



Qlik Sense 3.1 SR2 Shared Persistence

Configuration Guide

November 22, 2016





Table of Contents

Shared persistence overview	4
Benefits	4
Limitations	4
Security considerations	5
Planning a shared persistence deployment	6
Preparations	7
Preparing shared folders for files	7
Running Qlik Sense services as a user without local Administrator privileges	7
Using the database and file share on one of the nodes	8
Installing the central node and creating a cluster	8
Installing and adding more nodes to the cluster	10
Using a database and file share on a dedicated machine	12
Preparing the database server	12
Prepare the file share	13
Installing the central node and creating a cluster	13
Installing and adding more nodes to the cluster	14
Upgrading a multi-node deployment to Qlik Sense 3.1 SR2 with shared persistence	16
Migrating a site running Qlik Sense 3.1 SR1 or older using synchronized persistence	16
Migrating a site running Qlik Sense 3.1 SR2 using synchronized persistence	17
Upgrading a Qlik Sense 3.1/3.1 SR1 using shared persistence	18
Backing up and restoring a site deployed with shared persistence	19
Backing up a site deployed with shared persistence	19
Restoring a site deployed with shared persistence	19
Configuring Monitoring apps for shared persistence	20

Update <i>ArchivedLogsFolder</i> data connection	20
Configure sync rules	20
Manual configuration procedures	21
<hr/>	
Save username and password from the existing repository	21
Copying content to shared folders	21
Configuring the Repository Service for shared persistence	22
Setting the repository service database connection string	22
Configuring the Postgres database to accept connections from other nodes	23
Setting up database traffic encryption	25
<hr/>	
Maintaining database password integrity	25
Mutual authentication configuration	25
Optional: Setting up database replication and failover	27
<hr/>	
Setting up replication to standby nodes for failover	27
Database failover	28
Known Issues	29
<hr/>	
Logs	29
Operations monitor	29
Uninstalling Qlik Sense	29

Shared persistence overview

In a Qlik Sense multi-node site with synchronized persistence each node has its own repository database and set of application files. Both the database and the application files are synchronized from the central node to the rim nodes by the Qlik Sense Repository Service (QRS).

This document describes an alternative multi-node deployment where the nodes form a cluster that shares a single repository database and a network folder for the application files. This type of deployment is referred to as “shared persistence”.

Benefits

The benefits of using shared persistence instead of the multi-node synchronized persistence setup include:

- Use of a high availability database cluster is possible.
- Higher volumes of changes, such as reloads, is possible.
- Improved stability during high volume of content creation.
- Improved resiliency.
- No sync delay.

Limitations

There are some limitations to shared persistence deployments. In addition to these limitations, see also Known issues.

Geographical deployments

Shared persistence does not support geographical deployments, as Qlik Sense servers need to be located in the same local network as the database and the file share

Capacity and performance

Shared persistence supports up to a maximum of 8 machines. In addition to the number of nodes, there are other factors that will contribute to total capacity:

- workload
- hardware speed
- network speed

For example, if the disk speed of the file share and the central node is too slow, you may expect low performance during some operations, such as importing or duplicating apps.

We recommend scalability testing and engaging with Qlik Consulting for large deployments.

DMZ deployments

All machines in a site, including machines without an engine, require access to both the database and file share. In DMZ deployments this may require opening additional ports, or taking an alternative approach, compared to a DMZ deployment with synchronized persistence,

Central node dependencies

The central node is responsible for handling a number of vital operations in the site. When the central node is put offline, those operations are prevented from running, including:

- master scheduler, responsible for triggering reloads
- allowing new users to obtain a license
- using extension objects

Security considerations

In shared persistence deployments the network traffic between the servers, the database and the file share is not encrypted by default after an installation. We recommend applying the settings described in the following sections:

- Setting up database traffic encryption
- Optional: Setting up database replication and failover

Planning a shared persistence deployment

Qlik Sense supports two types of shared persistence deployments:

- Using a database and storing files on one of the nodes in the site
This type of deployment requires no extra installation or additional hardware.
- Using a database and a file share on one or more dedicated machines
This type of deployment requires one or more additional servers for running a PostgreSQL cluster and for hosting file shares, but provides more options for high availability deployments and more flexibility in terms of server deployments.

The functionality is the same with both options, and the set up steps are very similar, with a few additional steps required when using a dedicated machine.

If the deployment is small, such as 2-3 nodes, or there are no specific high availability requirements, we recommend using the database and file storage on one of the server machines. In larger deployments we recommend that you separate the database and file storage, which in addition will provide high availability options.

Preparations

Preparing shared folders for files

The files that are persisted in a Qlik Sense deployment must be available to all nodes. They can be stored on any of the nodes in the cluster, or on a separate server.

For either type of shared persistence deployment, do the following on the server that you want to use to store shared content:

1. Create a folder for all file content to be shared, for example, c:\QlikShare.
2. Create a Windows share for this folder and set read/write access to this share for the service account that is used to run the Qlik Sense services.

This file share should now be accessible from all machines as \\<servername>\QlikShare.

Note: We recommend that you enable SMB encryption for the file share to protect data from manipulation or tampering. More information about enabling SMB 3 encryption in Windows 2012 Server is available on <https://blogs.technet.microsoft.com/filecab/2012/05/03/smb-3-security-enhancements-in-windows-server-2012/>.

If you use SMB 3.0 encryption on the file share, all nodes in the cluster need to run Windows 2012.

Running Qlik Sense services as a user without local Administrator privileges

It is possible to run Qlik Sense as a user without local Administrator privileges, but there are some additional steps to perform in the installation and configuration process of a shared persistence deployment.

The user account that is used to run the Qlik services will need read and write access to the file share. We recommend that you use a specific domain user account on all machines, and set permissions for the file share on this account. This requires that all servers are part of the same Windows domain. If the servers are not part of a Windows domain, you must create an identical user name and password on all machines, including the machine hosting the file share, and use this account to apply file permissions.

Before installing you need to set up a service user account according to this section on every node in the site. You also need to perform the installation steps marked with **(Optional, only required for service user accounts without local Administrator privileges)**.

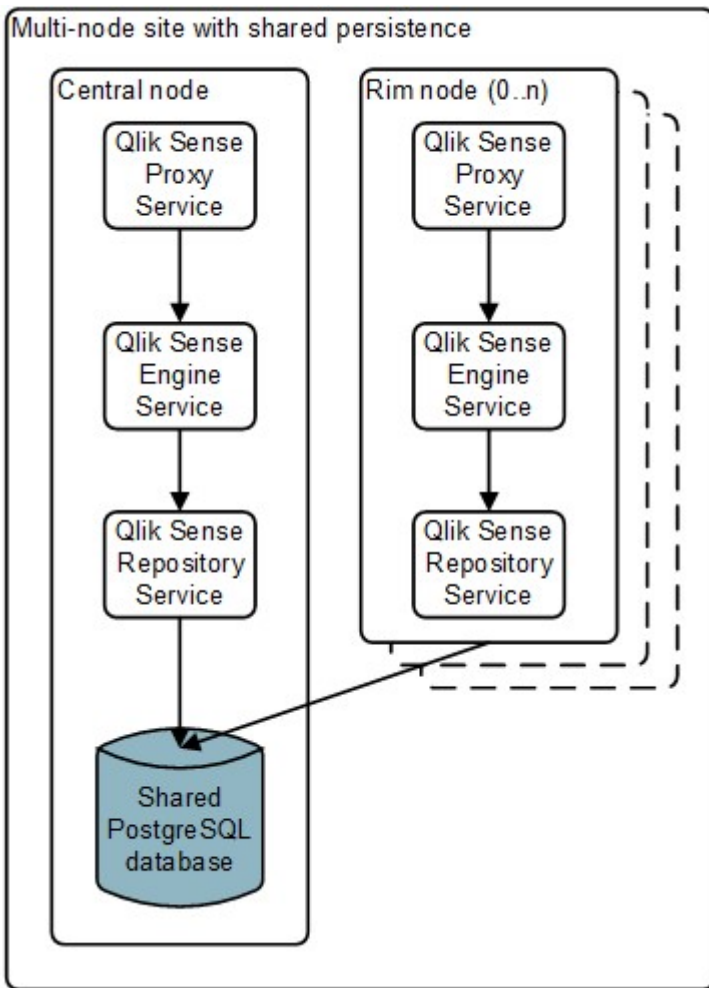
Setting up a service user account without local Administrator privileges

1. Create the group *Qlik Sense Service Users* in **Computer Management > System Tools > Local Users and Groups > Groups**.
2. Create a dedicated service user account which is a member of the following groups:
 - Performance Monitor Users
 - Qlik Sense Service Users

Using the database and file share on one of the nodes

This section describes how to set up shared persistence using the repository database on one of the nodes in the site, as well as sharing some of the file content. Any machine could be used. However, the method documented here uses the central node as the starting point.

Note: If you want to run Qlik Sense service using a service user account without local Administrator privileges, you first need to prepare a service user account on all nodes. See **Setting up a service user account without local Administrator privileges**.



Installing the central node and creating a cluster

These instructions describe how you install a node and create a new cluster with a new local database installed on the node. The database and file share will be shared with other nodes in the cluster.

Note: If you want to run Qlik Sense service using a service user account without local Administrator privileges, you need to prepare a service user account on the central node. See **Setting up a service user account without local Administrator privileges**.

Do the following on the machine dedicated to be a central node:

1. Log on with Administrator rights using an account that has an actual password defined (that is, not a blank password) on operating systems with User Account Control (UAC) disabled.

2. Start the installation program (Qlik_Sense_setup.exe). On the first screen, select **Shared persistence**, and accept the license agreement. Click **Next**.
3. Select **Create cluster**.
4. Select **Install a local database** and enter the following settings:
 - **Database port** - this is the port that the local database will listen for connections on.
 - **Database user** - this user will be created in the local database, and set as owner of the database.
 - **Database password** and **Confirm password**

Make a note of the settings, as you will need them when you add additional nodes to the cluster.

Click **Next**.
5. In **Root folder**, state where to store data and resources that should be accessible from all nodes in the cluster. This should be a file share in the form \\share\path. Sub folders for apps, archived logs, custom data, and static content will be created automatically, but you can also edit the separate folder paths individually.

Click **Next**.
6. Define the Qlik Sense **Installation Location**. The default is: `%ProgramFiles%\Qlik\Sense`. Click **Next**.
7. In the **Database Credentials** screen, add the password of the super user of the database.
8. In the **Service Credentials** screen, enter the **Username** and **Password** for the dedicated service account to run the Qlik Sense services.
9. In the **Host Name** screen, ensure that the address matches the correct DNS entry that other machines will use to connect to this machine. Click **Next**.
10. In the **Ready to install** screen, make sure that you select not to start the Qlik Sense services when the installation has completed.

Then click **Install**.

11. When the installation has completed, you need to configure the repository database. See **Configuring the Postgres database to accept connections from other nodes**.
12. **(Optional, only required for service user accounts without local Administrator privileges)**
 - a) Set full access to all folders needed by Qlik Sense services for the *Qlik Sense Service Users* group. Make sure that permissions are inherited and replaced on sub folders and shared resources, such as User Directory connectors. This includes folders:
 - `C:\ProgramData\Qlik\Sense`
 - The file share for shared folders
 - b) Run the following commands as administrator from an elevated command prompt.


```
Proxy.exe -bootstrap=install
Scheduler.exe -bootstrap=install
Repository.exe -bootstrap=install -iscentral
```
 - c) Change the **Log On** credentials for the Qlik Sense Repository Database service from **Local System** to the service user account you created.
13. Start the Qlik Sense Service Dispatcher (QSD).
14. Start the Qlik Sense Repository Service (QRS).

Before proceeding, make sure that the QRS starts up properly by checking its Service log (usually stored in `%ProgramData%\Qlik\Sense\Log\Repository\System`). It may take one to two minutes for the first startup to complete.
15. Start all other Qlik Sense services.
16. Open the Qlik Management Console (QMC) and apply the site licence.

You have now successfully installed a Qlik Sense node with a local database and created a new cluster.

Installing and adding more nodes to the cluster

These instructions describe how you install a node that connects to an existing cluster.

Note: If you want to run Qlik Sense service using a service user account without local Administrator privileges, you first need to prepare a service user account on all rim nodes. See **Setting up a service user account without local Administrator privileges**.

Do the following on the machine dedicated to be a rim node:

1. Log on with Administrator rights using an account that has an actual password defined (that is, not a blank password) on operating systems with User Account Control (UAC) disabled.
2. Start the installation program (Qlik_Sense_setup.exe). On the first screen, select **Shared persistence**, and accept the license agreement. Click **Next**.
3. Select **Join cluster**.
4. Enter the following settings according to the database settings you entered when you created the cluster:
 - **Database host name** - the address to the central node running a local database.
 - **Database port** -this is the port that the database listens for connections on.
 - **Database user**
 - **Database password** and **Confirm password**.

Click **Next**.

5. Define the Qlik Sense **Installation Location**. The default is: `%ProgramFiles%\Qlik\Sense`. Click **Next**.
6. In the **Service Credentials** screen, enter the **Username** and **Password** for the dedicated service account to run the Qlik Sense services.
7. In the **Ready to install** screen:
 - Service user account with local Administrator privileges:* select to automatically start the Qlik Sense services when the installation has completed.
 - Service user account without local Administrator privileges:* select not to start the Qlik Sense services when the installation has completedThen click **Install**.
8. **(Optional, only required for service user accounts without local Administrator privileges)**
 - a) Set full access to all folders needed by Qlik Sense services for the *Qlik Sense Service Users* group. Make sure that permissions are inherited and replaced on sub folders and shared resources, such as User Directory connectors. This includes folders:
 - `C:\ProgramData\Qlik\Sense`
 - The file share for shared folders
 - b) Run the following commands as administrator from an elevated command prompt.

```
Proxy.exe -bootstrap=install
Scheduler.exe -bootstrap=install
Repository.exe -bootstrap
```
9. Open the Qlik Management Console (QMC) on the central node and add the rim node you just installed.
For more information, see *Managing a Qlik Sense site > Configuring the node* in the Qlik Sense help.

10. **(Optional, only required for service user accounts without local Administrator privileges)**

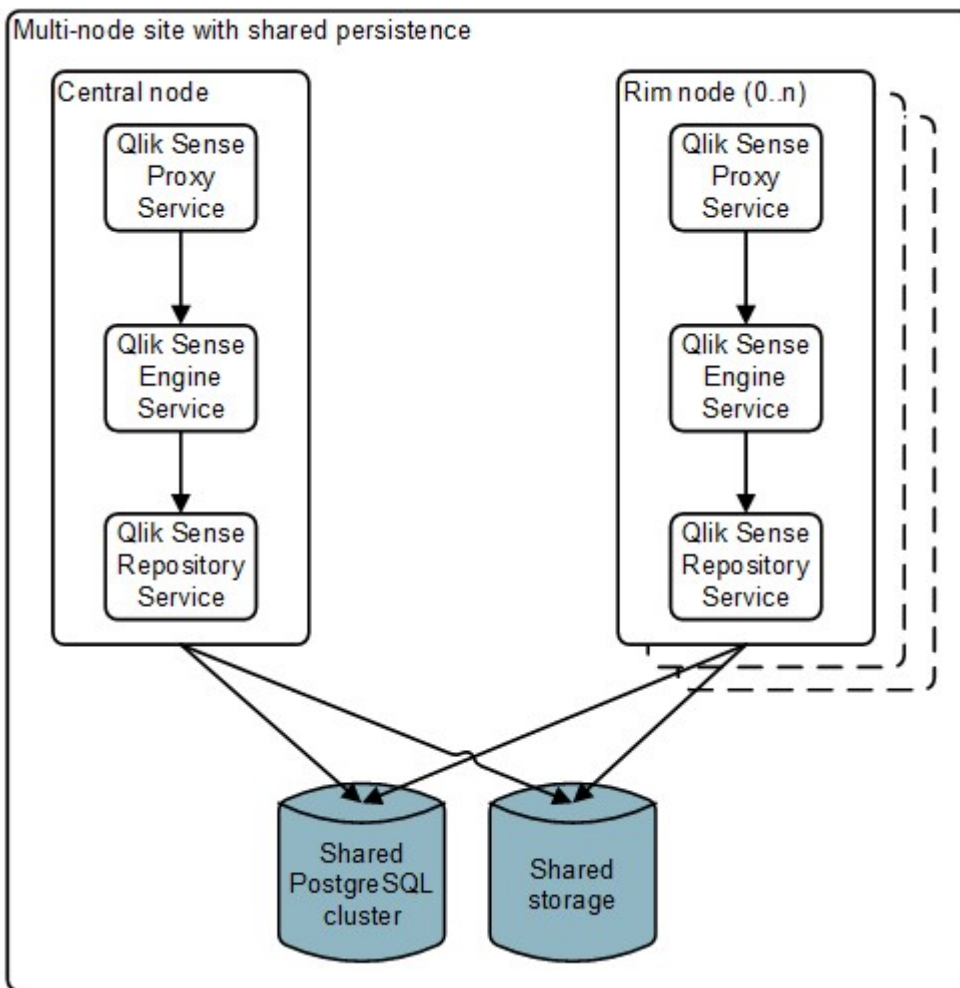
Start all Qlik Sense services.

You have now successfully installed a Qlik Sense node that connects to an existing cluster.

Using a database and file share on a dedicated machine

You can also separate machines to host the database and file share instead of using one of the nodes in the Qlik Sense site. Database and file share can be placed physically on the same machine or on different machines.

Note: If you want to run Qlik Sense service using a service user account without local Administrator privileges, you need to prepare a service user account. See **Setting up a service user account without local Administrator privileges**



Preparing the database server

You need to prepare the database server to be able to connect to Qlik Sense. To do this, you need to know how many nodes are planned for the site, as well as subnet specifications in the network.

Do the following:

1. Install PostgreSQL version 9.3.14 or a later version on the 9.3.x track, which can be obtained from <https://www.postgresql.org/>. It is important that you specify port 4432 during installation.
2. Create a PostgreSQL role named *qliksenserepository*, and assign a password.
3. Create a new database named QSR and set the *qliksenserepository* role as owner.
4. Copy the file *C:\Program Files\PostgreSQL\9.3\data\postgresql.conf* to another folder and open it in a text editor.
 - Uncomment the `listen_addresses` line and change it to `listen_addresses = '*'`.

- Set the maximum number of database connections to 100 x number of nodes in the Qlik Sense site with the `max_connections` setting,
Example: `max_connections = 200 # example for a site with 2 nodes.`
 - Save the `postgresql.conf` file and copy it to `C:\Program Files\PostgreSQL\9.3\data\`, replacing the existing file.
5. Copy the file `C:\Program Files\PostgreSQL\9.3\data\pg_hba.conf` to another folder and open it in a text editor.
 - Locate the following line:


```
host    all             all             127.0.0.1/32          md5
```

 This line determines which servers can access the server that the repository database runs on. The default setting, `127.0.0.1/32`, only allows localhost to access the database.
 - Replace `127.0.0.1/32` with a subnet specification that covers the IP addresses of all nodes in your site. Either add one row for each node, using `/32` as suffix for each address, or add a subnet that covers all addresses using, for example, `/24` as suffix. To allow all servers to access the repository database, use `0.0.0.0/0`.
 - Save the `pg_hba.conf` file and copy it to `C:\Program Files\PostgreSQL\9.3\data\`, replacing the existing file.
 6. The database server is now prepared for creating a new cluster that connects to the database.
 7. Restart `postgresql-x64-9.3` service from Windows Services.

Note: The database owner setup is different compared to a Qlik Sense deployment with a local database, where the owner role is **postgres**.

Prepare the file share

Prepare a network file share that can be used to store app content and logs that should be available to all nodes in the cluster.

See section Preparing shared folders for files

Installing the central node and creating a cluster

These instructions describe how you install a Qlik Sense node and create a new cluster with a new local database installed on the node. The database and storage share will be shared with other nodes in the cluster.

Do the following on the machine dedicated to be a central node:

1. Log on with Administrator rights using an account that has an actual password defined (that is, not a blank password) on operating systems with User Account Control (UAC) disabled.
2. Start the installation program (`Qlik_Sense_setup.exe`). On the first screen, select **Shared persistence**, and accept the license agreement. Click **Next**.
3. Select **Create cluster**.
4. Make sure that **Install a local database** is not selected, and enter the following settings:
 - **Database host name** - the address to the database server
 - **Database port** - this is the port that the local database will listen for connections on, usually 4432.
 - **Database user** – the user you created in the database, `qliksenserepository`.
 - **Database password** and **Confirm password** – the password for the database user.
 Click **Next**.
5. State where to store data and resources that should be accessible from all nodes in the cluster in Root folder. This is the network share that you prepared earlier, in the form `\\share\path`. Sub folders for apps, archived logs, custom data, and static content will be

created automatically, but you can also edit the separate folder paths individually.

Click **Next**.

6. Define the Qlik Sense Installation location either by entering the installation location, or browse for the location, or leave it to be installed at the predefined location. The default is: *%ProgramFiles%\Qlik\Sense*. Click **Next**.
7. In the **Service Credentials** screen, enter the **Username** and **Password** for the dedicated service account to run the Qlik Sense services.
8. In the **Host Name** screen, ensure that the address matches the correct DNS entry that other machines will use to connect to this machine.
Click **Next**.
9. In the **Ready to install** screen:
Service user account with local Administrator privileges: select to automatically start the Qlik Sense services when the installation has completed.
Service user account without local Administrator privileges: select not to start the Qlik Sense services when the installation has completed
Then click **Install**.
10. **(Optional, only required for service user accounts without local Administrator privileges)**
 - a) Set full access to all folders needed by Qlik Sense services for the *Qlik Sense Service Users* group. Make sure that permissions are inherited and replaced on sub folders and shared resources, such as User Directory connectors. This includes folders:
 - *C:\ProgramData\Qlik\Sense*
 - The file share for shared folders
 - b) Run the following commands as administrator from an elevated command prompt.
`Proxy.exe -bootstrap=install`
`Scheduler.exe -bootstrap=install`
`Repository.exe -bootstrap`
 - c) Change the Log On credentials for the Qlik Sense Repository Database service from Local System to the service user account you created.
10. **(Optional, only required for service user accounts without local Administrator privileges)**
 - a. Start the Qlik Sense Service Dispatcher (QSD).
 - b. Start the Qlik Sense Repository Service (QRS).
Before proceeding, make sure that the QRS starts up properly by checking its Service log (usually stored in *%ProgramData%\Qlik\Sense\Log\Repository\System*). It may take one to two minutes for the first startup to complete.
 - c. Start all other Qlik Sense services.
11. When the installation has completed, open the Qlik Management Console (QMC) and apply the site licence.

You have now successfully installed a Qlik Sense node that connects to a dedicated database server, and created a new cluster.

Installing and adding more nodes to the cluster

These instructions describe how you install a node that connects to an existing cluster,

Do the following on the machine dedicated to be a rim node:

1. Log on with Administrator rights using an account that has an actual password defined (that is, not a blank password) on operating systems with User Account Control (UAC) disabled.
2. Start the installation program (*Qlik_Sense_setup.exe*). On the first screen, select **Shared persistence**, and accept the license agreement. Click **Next**.

3. Select **Join cluster**.
4. Enter the following settings according to the database settings you entered when you created the database:
 - **Database host name** - the address to the database server
 - **Database port** - this is the port that the local database will listen for connections on, usually 4432.
 - **Database user** – the user you created in the database, *qliksenserepository*.
 - **Database password** and **Confirm password** – the password for the database user.
 Click **Next**.
5. Define the Qlik Sense **Installation location** either by entering the installation location, or browsing for the location. You can also leave it to be installed at the predefined location: *%ProgramFiles%\Qlik\Sense*. Click **Next**.
6. In the **Service Credentials** screen, enter the **Username** and **Password** for the dedicated service account to run the Qlik Sense services.
7. In the **Ready to install** screen:

Service user account with local Administrator privileges: select to automatically start the Qlik Sense services when the installation has completed.

Service user account without local Administrator privileges: select not to start the Qlik Sense services when the installation has completed

 Then click **Install**
11. **(Optional, only required for service user accounts without local Administrator privileges)**
 - a) Set full access to all folders needed by Qlik Sense services for the *Qlik Sense Service Users* group. Make sure that permissions are inherited and replaced on sub folders and shared resources, such as User Directory connectors. This includes folders:
 - *C:\ProgramData\Qlik\Sense*
 - The file share for shared folders
 - b) Run the following commands as administrator from an elevated command prompt.


```
Proxy.exe -bootstrap=install
Scheduler.exe -bootstrap=install
Repository.exe -bootstrap
```
8. Open the Qlik Management Console (QMC) on the central node and add the rim node you just installed.

For more information, see *Managing a Qlik Sense site > Configuring the node* in the Qlik Sense help.
9. **(Optional, only required for service user accounts without local Administrator privileges)**

Start all Qlik Sense services.

You have now successfully installed a Qlik Sense node that connects to an existing cluster.

Upgrading a multi-node deployment to Qlik Sense 3.1 SR2 with shared persistence

You can convert an existing multi-node deployment to Qlik Sense 3.1 SR2 with shared persistence.

The upgrade scenario is different depending on your existing deployment:

- Qlik Sense 3.1 SR1 or older using synchronized persistence
- Qlik Sense 3.1 SR2 using synchronized persistence
- Qlik Sense 3.1 or 3.1 SR1 using shared persistence

These scenarios assume that the existing central node is to be used as the shared data base and file share. If you want to move data to separate servers, additional steps are required. During this process no data or settings will be lost.

Migrating a site running Qlik Sense 3.1 SR1 or older using synchronized persistence

Do the following on the central node:

1. Before starting the migration, take a backup of central node data. See the Qlik Sense help section **Backing up and restoring** for more information.
2. Save the repository user password from the connection string.
See **Save username and password from the existing repository**
3. Prepare file share according to section Preparing shared folders for files
4. Copy content to the shared folders according to section **Copying content to shared folders**.
5. Uninstall Qlik Sense.
Make sure that **Remove Qlik Sense certificates and data folders** is not selected in the confirmation screen
6. Install Qlik Sense. You should be alerted that **An existing database has been detected**, select to use that database. Select **Shared persistence** and **Create cluster**.
Select **Install a local database** and use the password that you retrieved from the existing repository in step 2.
Use the file shares you created in steps 3 and 4.
In the **Ready to install** screen, make sure that you select not to start the Qlik Sense services when the installation has completed.
Then click **Install** and finalize the installation.
7. Configure the Postgres database according to section **Configuring the Postgres database to accept connections from other nodes**.
8. Make sure that the centralized database service ('QlikSenseRepositoryDatabase') is running.
9. Run the following command from the command line:

```
(echo TRUNCATE "AppAvailabilities", "SyncSessions",  
"BinaryDownloadProperties", "BinaryDownloads",  
"BinaryDeleteProperties", "BinaryDeletes",  
"BinarySyncRuleEvaluations" CASCADE;) | "C:\Program  
Files\Qlik\Sense\Repository\PostgreSQL\9.3\bin\psql.exe" -U postgres  
-p 4432 -d QSR
```
10. **(Optional)**
If you want to use a service user account without local Administrator privileges, perform the configuration steps described in online help topic **Running Qlik Sense services as a user without local Administrator privileges**.
11. Start the Qlik Sense Service Dispatcher (QSD) and then Qlik Sense Repository Service (QRS)
12. Start up the remaining services and verify operation of the QMC and Hub.

Do the following on all rim nodes:

1. Uninstall Qlik Sense and select to delete all data and certificates. Settings and data will not be lost as these will be stored on the central node.

2. Install Qlik Sense, selecting **Shared persistence** and **Join cluster**.
Use the fully qualified domain name of the central node as **Host name**, and set same **User name** and **Password** as on the central node.
In the **Ready to install** screen, select to automatically start the Qlik Sense services when the installation has completed. Then click **Install and finalize the installation**.
3. Re-add the rim nodes to the QMC. Do the following on the central node for each rim node:
 - a. Go to **QMC -> Nodes**, select the rim node and click **Redistribute**.
 - b. Complete the node registration by entering the password to the location indication in the QMC as normal.
4. **(Optional)**
If you want to use a service user account without local Administrator privileges, perform the configuration steps described in online help topic **Running Qlik Sense services as a user without local Administrator privileges**.

After registering all nodes, verify that all nodes work correctly.

Migrating a site running Qlik Sense 3.1 SR2 using synchronized persistence

Do the following on the central node:

1. Before starting the migration, take a backup of central node data. See the Qlik Sense help section **Backing up and restoring** for more information.
2. Save the repository user password from the connection string.
See **Save username and password from the existing repository**
3. Prepare file share according to section **Preparing shared folders for files**
4. Copy content to the shared folders according to section **Copying content to shared folders**.
5. Uninstall Qlik Sense.
Make sure that **Remove Qlik Sense certificates and data folders** is not selected in the confirmation screen
6. Install Qlik Sense, selecting **Shared persistence** and **Create cluster**.
You should be alerted that **An existing database has been detected**, select to use that database.
Select **Install a local database** and use the password that you retrieved from the existing repository in step 2.
Use the file shares you created in steps 3 and 4.
In the **Ready to install** screen, make sure that you select not to start the Qlik Sense services when the installation has completed.
Then click **Install** and finalize the installation.
7. Configure the Postgres database according to section **Configuring the Postgres database to accept connections from other nodes**.
8. Make sure that the centralized database service ('QlikSenseRepositoryDatabase') is running.
9. Run the following command from the command line:

```
(echo TRUNCATE "AppAvailabilities", "SyncSessions",
"BinaryDownloadProperties", "BinaryDownloads",
"BinaryDeleteProperties", "BinaryDeletes",
"BinarySyncRuleEvaluations" CASCADE;) | "C:\Program
Files\Qlik\Sense\Repository\PostgreSQL\9.3\bin\psql.exe" -U postgres
-p 4432 -d QSR
```
10. **(Optional)**
If you want to use a service user account without local Administrator privileges, perform the configuration steps described in online help topic **Running Qlik Sense services as a user without local Administrator privileges**.
11. Start the Qlik Sense Service Dispatcher (QSD) and then Qlik Sense Repository Service (QRS).
12. Configure the repository service for shared persistence, using the password retrieved in step 2 and adjusted paths to the file share folders.
See **Configuring the Repository Service for shared persistence**
13. Restart the Qlik Sense Service Dispatcher (QSD) and then Qlik Sense Repository Service (QRS).
14. Start up the remaining services and verify that paths are correct in **QMC > Service cluster**.

Do the following on all rim nodes:

1. Uninstall Qlik Sense and select to delete all data and certificates. Settings and data will not be lost as these will be stored on the central node.
2. Install Qlik Sense, selecting **Shared persistence** and **Join cluster**.
Use the fully qualified domain name of the central node as **Host name**, and set same **User name** and **Password** as on the central node.
In the **Ready to install** screen, select to automatically start the Qlik Sense services when the installation has completed. Then click **Install and finalize the installation**.
3. Re-add the rim nodes to the QMC. Do the following on the central node for each rim node:
 - a. Go to **QMC -> Nodes**, select the rim node and click **Redistribute**.
 - b. Complete the node registration by entering the password to the location indication in the QMC as normal.
4. **(Optional)**
If you want to use a service user account without local Administrator privileges, perform the configuration steps described in online help topic **Running Qlik Sense services as a user without local Administrator privileges**.

After registering all nodes, verify that all nodes work correctly.

Upgrading a Qlik Sense 3.1/3.1 SR1 using shared persistence

If you have an existing shared persistence deployment on Qlik Sense 3.1/3.1 SR1, you need to follow this procedure to upgrade to Qlik Sense 3.1 SR2.

Do the following on the central node:

1. Before starting the migration, take a backup of central node data. See the Qlik Sense help section **Backing up and restoring** for more information.
2. Save the repository user password from the connection string.
See **Save username and password from the existing repository**
3. Uninstall Qlik Sense, and make sure that **Remove Qlik Sense certificates and data folders** is not selected in the confirmation screen.
4. Install Qlik Sense selecting **Shared persistence**, and **Create cluster**.
You should be alerted that **An existing database has been detected**, select to use that database.
Select **Install a local database** and use the password that you retrieved from the existing repository in step 2.
Use the existing file shares.
In the **Ready to install** screen, select to start the Qlik Sense services when the installation has completed.
Then click **Install** and finalize the installation.

Do the following on all rim nodes:

1. Uninstall Qlik Sense and select to delete all data and certificates. Settings and data will not be lost as these will be stored on the central node.
2. Install Qlik Sense, selecting **Shared persistence** and **Join cluster**.
Use the fully qualified domain name of the central node as **Host name**, and set same **User name** and **Password** as on the central node.
In the **Ready to install** screen, select to automatically start the Qlik Sense services when the installation has completed. Then click **Install and finalize the installation**.
3. Re-add the rim nodes to the QMC. Do the following on the central node for each rim node:
 - a. Go to **QMC -> Nodes**, select the rim node and click **Redistribute**.
 - b. Complete the node registration by entering the password to the location indication in the QMC as normal.

After registering all nodes, verify that all nodes work correctly.

Backing up and restoring a site deployed with shared persistence

You can back up and restore a site deployed with shared persistence using the same manual procedures described in the Qlik Sense help section **Backing up and restoring**, with a few differences described in this section.

Note! It is not possible to use the Repository Snapshot Manager on shared persistence deployments.

Backing up a site deployed with shared persistence

Follow the procedure in the help topic **Backing up a site manually**, but with the following exceptions:

- In step 2 you need to stop the services on all rim nodes as well, not just the central node.
- If you deployed PostgreSQL and app storage on a dedicated machine, steps 3 and 4 need to be performed on that machine, using the path that was used when installing PostgreSQL.

Restoring a site deployed with shared persistence

Follow the procedure in the help topic **Restoring a site manually**, but with the following exceptions:

- Install nodes according to the procedure in this document.
- If you deployed PostgreSQL and app storage on a dedicated machine, steps 4 and 5 need to be performed on that machine, using the path that was used when installing PostgreSQL.
- Step 8 is not applicable, as rim nodes do not contain data in a shared persistence deployment.

Configuring Monitoring apps for shared persistence

If you want to use the monitoring apps in a shared persistence deployment, you need to make some configuration changes in QMC.

Update data connections

You need to update the **Connection string** of some data connections:

- **ArchivedLogsFolder**: make sure that the **Connection string** points to the shared folder containing archived logs.
- REST connectors: make sure that the **Connection string** points to the shared folder containing the database.

Configure load balancing rules

1. Open **Start>Load balancing rules**.
2. Select the rule *ResourcesOnNonCentralNodes* and click Edit.
Select **Disabled** and click **Apply**.
3. Create a new rule with the following settings:
 - a. **Resource filter**: App_*
 - b. **Actions**: Load balancing enabled
 - c. **Conditions**: ((node.isCentral = "false"))

Manual configuration procedures

These manual configuration procedures are referred to in upgrade scenarios.

Save username and password from the existing repository

In some cases, you need to retrieve the username and password from the repository, as you will need it in the installation procedure. To do this you need the ConnectionString editor, which is located in `%Program Files%\Qlik\Sense\Repository\Util\ConnectionStringEditor\ConnectionStringEditor.exe`.

ConnectionString editor is installed with Qlik Sense 3.1 SR2. If you need the tool to perform an upgrade to Qlik Sense 3.1 SR2, you can either:

- Install Qlik Sense 3.1 SR2 on a separate machine to copy the tool.
- Contact Qlik Support to obtain the tool.

Do the following on the central node:

1. Open the ConnectionString editor. You need to run the executable as an Administrator.
2. Open the file `%Program Files%\Qlik\Sense\Repository\Repository.exe` in the ConnectionString editor.
The decrypted database connection string is displayed.
3. Take note of the username and password.

Note: The password copied from the 'ConnectionStringEditor' tool may contain escape characters used in XML/HDF5, such as:

- quote (") "
- apostrophe (') '
- ampersand (&) &
- less than (<) <
- greater than (>) >

If this happens, it is important to make sure that you replace the escaped characters with the actual characters when pasting the password in the installer dialog.

Example: `I^! ?0&163j` is actually `I^! ?0&163j`

Copying content to shared folders

Do the following on the file share created according to **Prepare the file share**:

1. Create the following sub-folders in the shared folder:
 - *Apps*
 - *StaticContent*
 - *ArchivedLogs*
 - *CustomData*
2. Copy all files and folders from `%ProgramData%\Qlik\Sense\Apps` to *Apps* in the *QlikShare* folder.

3. Copy all content from `%ProgramData%\Qlik\Custom Data` to `CustomData` Restart all the Qlik Sense services. If you are running multi-deployed environment, please restart the Qlik Sense services on all machines.
4. Copy all connectors from `%ProgramFiles%\Common Files\Qlik\Custom Data` to `CustomData` in the `QlikShare` folder.
5. Copy all content from `%ProgramFiles%\Common Files\Qlik\ Archived Logs` to `ArchivedLogs` in the `QlikShare` folder if you want to keep your old log files in the shared folder.
6. Copy the following folders from `%ProgramData%\Qlik\Sense\Repository` to `StaticContent` in the `QlikShare` folder:
 - `AppContent`
 - `Content`
 - `DefaultContent`
 - `Extensions`
 - `DefaultApps`

Note: The folders are created by Qlik Sense when needed. So, if any folder is missing, you can safely ignore it.

Configuring the Repository Service for shared persistence

The configuration file for the repository may need to be edited to enable shared persistence. You need to modify read/write permissions for the Repository folder to be able to save it. You need the `ServiceClusterTool.exe` tool available in `%Program Files%\Qlik\Sense\Repository\Util..`

1. Start `ServiceClusterTool.exe` as an Administrator.
2. Edit the following settings. Replace `<server>` with the name of the server that hosts the file share used for storing app content.
 - **user ID:** `<user ID to use when logging in to PostgreSQL database, default is qliksenserepository>`
 - **password:** `<password for qliksenserepository user>`
 - **Port:** `<port for PostgreSQL database, default is 4432>`
 - **Host:** `<hostname where PostgreSQL database is located>`
 - **Root Folder:** `\\< server>\QlikShare`
 - **Apps:** `\\< server>\QlikShare\Apps`
 - **Archived Logs:** `\\< server>\QlikShare\ArchivedLogs`
 - **Custom Data:** `\\< server>\QlikShare\CustomData`
 - **Static Content:** `\\< server>\QlikShare\StaticContent`
3. Click **Save**
4. Restart all Qlik Sense services on all nodes of the deployment.

Setting the repository service database connection string

You may need to set the repository database connection string to point to the central node instead of localhost. As the connection string is encrypted in the config file, you need to use the ConnectionString editor, supplied by Qlik, to decrypt the string, edit it, and write back an encrypted string.

Do the following:

1. Open the ConnectionString editor, *ConnectionStringEditor.exe* which is located in *%Program Files%\Qlik\Sense\Repository\Util\ConnectionStringEditor*. You need to run the executable as Administrator.
2. Open the file *%Program Files%\Qlik\Sense\Repository\Repository.exe* in the ConnectionString editor.

The decrypted database connection string is displayed.

3. Edit these connection string properties:
Host: replace localhost with the machine name of the server running the shared repository database.
4. Save the changes to the file

Configuring the Postgres database to accept connections from other nodes

By default, the Postgres database installed by the Qlik Sense installer will only listen to requests from the local machine. This may need to be configured to allow database access to the rim nodes.

- If you installed a local database, the files are located in *%ProgramData%\Qlik\Sense\Repository\PostgreSQL<version>*
- If you set up a dedicated Postgres server, the files are located in *%ProgramFiles%\PostgreSQL9.3\data*.

Do the following:

1. Copy the file *postgresql.conf* to another folder and open it in a text editor.
2. Locate the `listen_addresses` setting, uncomment it by removing the # symbol at the start of the line, and then set it to *:

```
listen_addresses = '*'
```

3. Set the maximum number of database connections to 100 x number of nodes in the Qlik Sense site:

```
max_connections = 200 # this example is for a site with 2 nodes
```

4. Save the *postgresql.conf* file and copy it, replacing the existing file.
5. Copy the file *pg_hba.conf* to another folder and open it in a text editor.

6. Locate the following line:

```
host all all 127.0.0.1/32 md5
```

This line determines which servers can access the server that the repository database runs on. The default setting, `127.0.0.1/32`, only allows localhost to access the database.

7. Add a subnet specification that covers the IP addresses of all nodes in your site. Either add one row for each node, using `/32` as suffix for each address, or add a subnet that covers all addresses using, for example, `/24` as suffix. To allow all servers to access the repository database, use `0.0.0.0/0`.

Note: If you do not know which addresses to add, check with your system administrator.

8. Save the *pg_hba.conf* file and copy it, replacing the existing file.
9. If you installed a local database, restart Qlik Sense Repository Database.
If you set up a dedicated Postgres server, restart postgresql-x64-9.3 service from Windows Services.

Setting up database traffic encryption

Qlik Sense supports database traffic encryption using SSL, but you need to consider password security and perform some manual configuration in a shared persistence deployment.

We recommend that the configuration in this section is performed by someone with sufficient skills in PostgreSQL database configuration.

Maintaining database password integrity

Here are some guidelines to maintain password integrity in a Qlik Sense shared persistence deployment.

- It is important that you disable the **Store password** option for your user in PostgreSQL. If this option is enabled, the password is stored in a file, and incoming connections without a password will be able to connect to the database.
- Change password by executing this query in the PostgreSQL database:

```
ALTER USER {User} PASSWORD 'newPassword'
```

Do not change password in the PostgreSQL user interface for the same reasons as above.
- Use md5 hashing.
- Do not set your password to PASSWORD "", that is, an empty string, since this is not handled well in PostgreSQL.

Mutual authentication configuration

You need to perform the following steps to setup SSL and MD5 password protection:

1. Edit the following values in *postgresql.conf*:

```
listen_addresses = '*'  
port = 4432  
ssl = on  
ssl_cert_file = 'server.pem'  
ssl_key_file = 'server_key.pem'  
#ssl_ca_file = ''  
#ssl_crl_file = ''
```
2. Add the following lines in *pg_hba.conf*

```
hostssl all all all md5
```
3. Remove any other lines starting with hostssl or host in *pg_hba.conf*
4. Copy *server.pem*, and *server_key.pem* from
`%PROGRAMDATA%\Qlik\Sense\Repository\Exported Certificates\Local Certificates to
%PROGRAMDATA%\Qlik\Sense\Repository\PostgreSQL\9.3`
5. Use the ConnectionString editor to make the following setting in *repository.exe.config* on the central node and all rim nodes that belong to the cluster. *ConnectionStringEditor.exe* is located in `%Program Files%\Qlik\Sense\Repository\Util\ConnectionStringEditor`. You need to run the executable as Administrator.:
Add `'Ssl Mode=Require;'` to the QSR connection string:

```
<add name="QSR" connectionString="User  
ID=qliksenserepository;Password='randompass'; Ssl  
Mode=Require;Host=fullhostname.com;Port=4432;Database=QSR;Pooling=true;  
Min Pool Size=0;Max Pool Size=90;Connection  
Lifetime=3600;Unicode=true;"providerName="Devart.Data.PostgreSql"/>
```
6. Start all Qlik Sense services and verify that everything works.

7. Verify the authentication using the pgAdmin tool in PostgreSQL:
 - Users postgres and qliksenserepository must enter a valid password to connect.

Optional: Setting up database replication and failover

Note: The instructions in this section are optional.

This section describes how to set up database replication and failover in a shared persistence environment. Additionally, the file storage content will also need to be replicated.

Note: When editing text files related to the Qlik Sense installation, do the following:

1. Copy the file to another location on the server.
2. Edit the file and save the changes.
3. Copy the updated file back to its original location.

Setting up replication to standby nodes for failover

To fail over to a standby node in case the central database or node is lost, one or more standby databases can be configured for streaming replication from the database on the primary node. The instructions in this section describe how to set up asynchronous streaming replication to one or more standby nodes.

Before starting, ensure that the environment is configured and running, and install PostgreSQL on a standby machine.

Configure the primary database server

On the primary database server, do the following:

1. Open the file *C:\Program Files\PostgreSQL\9.3\data\postgresql.conf*
2. Locate and set the following settings

```
wal_level = hot_standby  
  
max_wal_senders = 3  
  
checkpoint_segments = 8  
  
wal_keep_segments = 8  
  
hot_standby = on
```

3. Create a user account that can be used for replication. To do so from a command prompt, run the following command. Adjust the hostname as needed, and specify a suitable password. You may be prompted for a password, this is the password that was specified during installation.

```
"C:\Program Files\PostgreSQL\9.3\bin\psql.exe" -h <machinename>  
-p 4432 -W -c "CREATE USER replicator REPLICATION LOGIN  
ENCRYPTED PASSWORD 'secretpassword';"
```

4. Open the file *C:\Program Files\PostgreSQL\9.3\data\pg_hba.conf*.
5. At the bottom of the file add...

```
host      replication      replicator      0.0.0.0/0md5
```

You can restrict the subnet access further, if required.

6. Restart the Postgres service.

Configure the standby database server

On the standby Postgres database server, do the following:

1. Stop the Postgres service.
2. Delete all content from *C:\Program Files\PostgreSQL\9.3\data*.
3. From the command line run the following command adjusted to use the name of the primary server:

```
"C:\Program Files\PostgreSQL\9.3\bin\pg_basebackup" -h  
<primaryServer> -D "C:\Program Files\PostgreSQL\9.3\data" -U  
replicator -v -P -p 4432 -W
```

You can ignore any warnings about copying files manually.

4. In a text editor, create a file called *recovery.conf* and place it in *C:\Program Files\PostgreSQL\9.3\data*.
5. Open *recovery.conf* and add the following text, adjusting the hostname and port

```
standby_mode = 'on'  
  
primary_conninfo = 'host=< primaryServer > port=4432  
user=replicator password=secretpassword'  
  
trigger_file = 'failover'  
  
recovery_target_timeline = 'latest'
```

6. Start the Postgres service.

You should now be able to connect to the database and view the data being streamed over from the primary node in read only mode.

Database failover

If the database on primary node is lost, a standby node needs to take over.

Do the following:

1. On the standby node that is to become the new primary node, create a file called *failover* in the folder *C:\Program Files\PostgreSQL\9.3\data*
Note: *The failover file should have no file extension!*

The file triggers PostgreSQL to cease recovery and enter read/write mode. PostgreSQL also changes the name of the file *recovery.conf* to *recovery.done* to reflect the transition.

2. On each node open the ConnectionString editor and change the connection string to point to the hostname or IP address of the new central node.

Known issues

Database availability

If the PostgreSQL database is unreachable for a period of time, repository services may shutdown and need to be restarted.

Logs

The following Qlik Sense logs are not automatically archived:

- Broker Service log
- Data Profiling Service log
- Hub Service log
- Migration Service log

Operations monitor

The steps for reconfiguring the Operations Monitor are obsolete in shared persistence deployments.

For more information, see *Monitoring a Qlik Sense site > Multi-node environments* in the Qlik Sense help.

TLS configuration

Do not disable SSL 3.0 support in the TLS configuration of the database, due to a limitation in the current version of the database connector driver.

Uninstalling Qlik Sense

When uninstalling Qlik Sense, both from the central node and from rim nodes, no information is removed from the shared folder even if you select **Remove Qlik Sense certificates and data folders**.



150 N. Radnor Chester Road
Suite E120
Radnor, PA 19087
Phone: +1 (888) 828-9768
Fax: +1 (610) 975-5987

qlik.com

