Qlik Sense Multi-node Setup Guide (DFAFT)

Introduction

This article explains how to add a rim node to an existing central node to build a Qlik Sense 1.0.2 multi-nodes environment. (This is NOT an official document distributed by QlikTech.)

Prerequisite

- Install the first Qlik Sense Server node as a central node. (standalone server)
- Install the second Qlik Sense Server node as a rim node. You can do it by unchecking "Central Node" option while installation. You can also choose services to install (Engine, Proxy, Repository and Scheduler) by selecting "CUSTOM INSTALL".
- The following ports need to be opened in Windows Firewall:
  - ✓ Central Node

Port	Description
443	Default Qlik Sense Proxy Service (QPS) API service port. This port uses https for communication.
4144	Default port for the internal authentication module in the Qlik Sense Proxy Service (QPS) when using NTLM in Microsoft Windows.
4241	Communication port within multi-node sites for QRS-to-QRS synchronization.
4242	Qlik Sense Repository Service (QRS) API service port. Also used as synchronization service port within multi-node sites for QRS-to-QRS synchronization.
4243	Qlik Sense Proxy Service (QPS) REST server.
5050	Qlik Sense Scheduler Service (QSS) master REST engine.
5051	Qlik Sense Scheduler Service (QSS) slave REST engine.

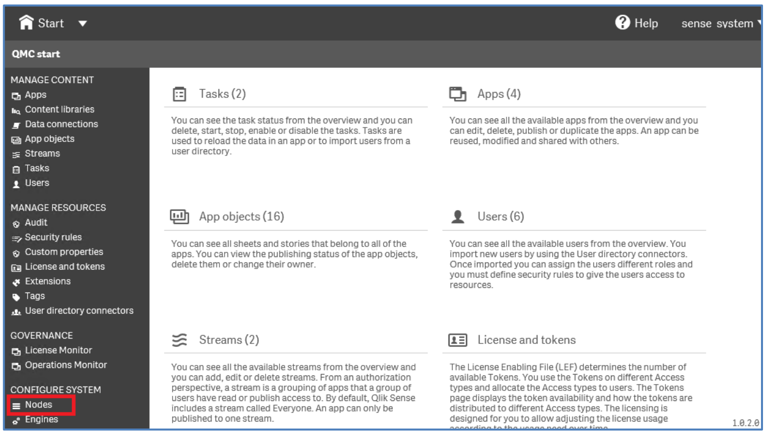
  - ✓ Rim Node

Port	Description
443	Default Qlik Sense Proxy Service (QPS) API service port. This port uses https for communication.
4144	Default port for the internal authentication module in the Qlik Sense Proxy Service

	(QPS) when using NTLM in Microsoft Windows.
4241	Communication port within multi-node sites for QRS-to-QRS synchronization.
4242	Qlik Sense Repository Service (QRS) API service port. Also used as synchronization service port within multi-node sites for QRS-to-QRS synchronization.
4243	Qlik Sense Proxy Service (QPS) REST server.
4444	Security distribution port, only used within multi-node sites by non-master Qlik Sense Repository Services (QRSs) to receive a certificate from the master QRS.
5051	Qlik Sense Scheduler Service (QSS) slave REST engine.

Setup Steps

1. Click [Configure System] > [Nodes] on the QMC.



Tasks (2)

You can see the task status from the overview and you can delete, start, stop, enable or disable the tasks. Tasks are used to reload the data in an app or to import users from a user directory.

Apps (4)

You can see all the available apps from the overview and you can edit, delete, publish or duplicate the apps. An app can be reused, modified and shared with others.

App objects (16)

You can see all sheets and stories that belong to all of the apps. You can view the publishing status of the app objects, delete them or change their owner.

Users (6)

You can see all the available users from the overview. You import new users by using the User directory connectors. Once imported you can assign the users different roles and you must define security rules to give the users access to resources.

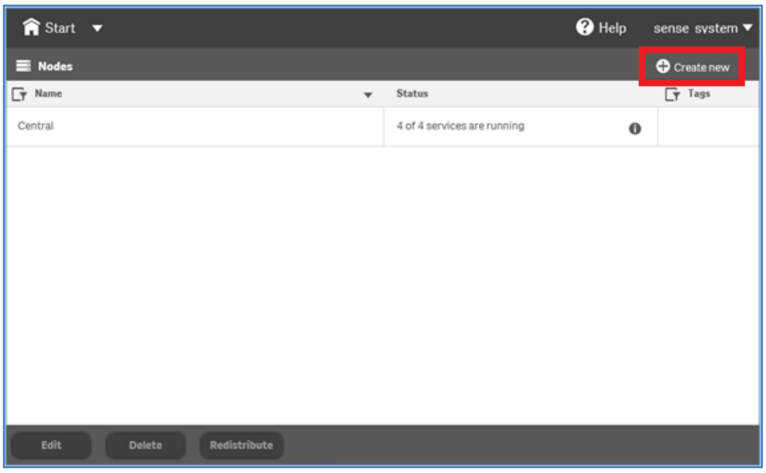
Streams (2)

You can see all the available streams from the overview and you can add, edit or delete streams. From an authorization perspective, a stream is a grouping of apps that a group of users have read or publish access to. By default, Qlik Sense includes a stream called Everyone. An app can only be published to one stream.

License and tokens

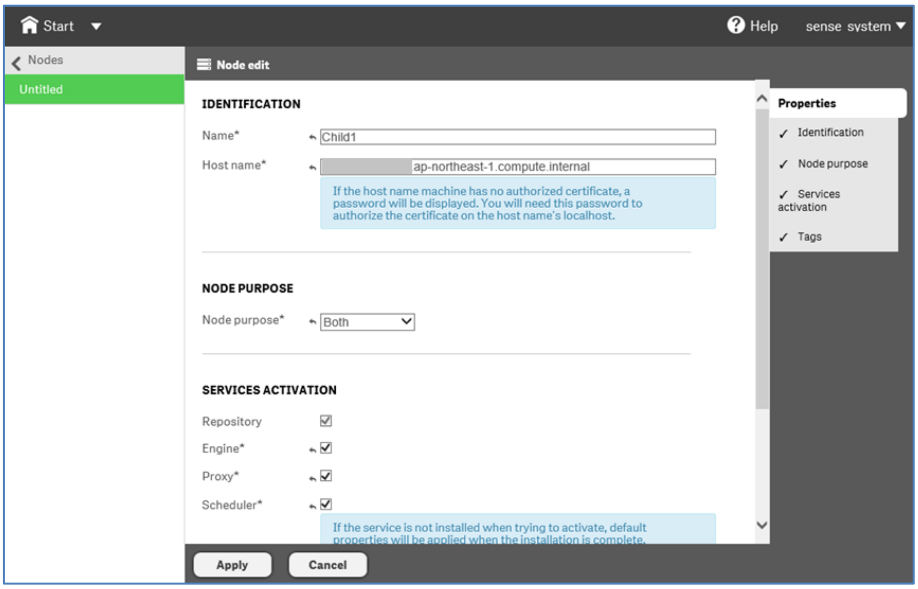
The License Enabling File (LEF) determines the number of available Tokens. You use the Tokens on different Access types and allocate the Access types to users. The Tokens page displays the token availability and how the tokens are distributed to different Access types. The licensing is designed for you to allow adjusting the license usage

2. Click [Create new].



Name	Status	Tags
Central	4 of 4 services are running	

3. Fill in the boxes and click [Apply].



IDENTIFICATION

Name* Child1

Host name* [redacted]ap-northeast-1.compute.internal

If the host name machine has no authorized certificate, a password will be displayed. You will need this password to authorize the certificate on the host name's localhost.

NODE PURPOSE

Node purpose* Both

SERVICES ACTIVATION

Repository ☑

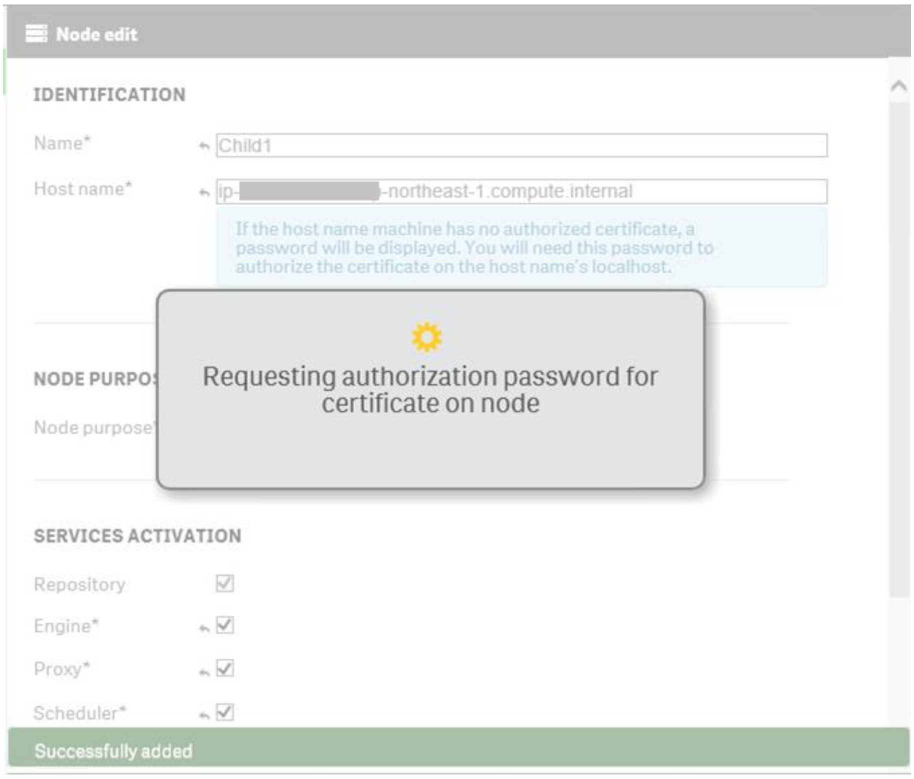
Engine* ☑

Proxy* ☑

Scheduler* ☑

If the service is not installed when trying to activate, default properties will be applied when the installation is complete.

4. The central node starts to communicate with the rim node.



IDENTIFICATION

Name* Child1

Host name* ip-[redacted]-northeast-1.compute.internal

If the host name machine has no authorized certificate, a password will be displayed. You will need this password to authorize the certificate on the host name's localhost.

NODE PURPO

Node purpose

Requesting authorization password for certificate on node

SERVICES ACTIVATION

Repository ☑

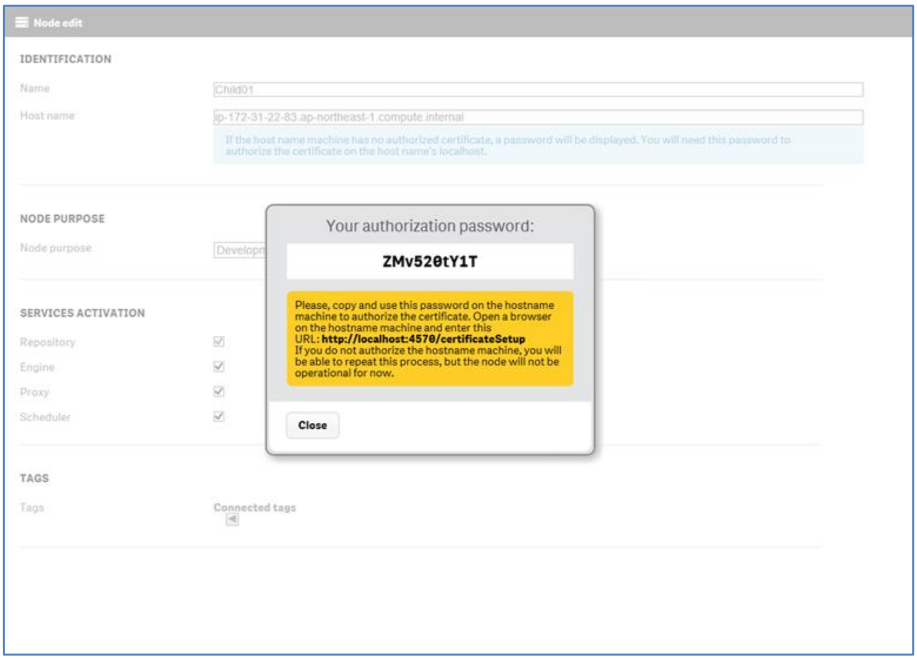
Engine* ☑

Proxy* ☑

Scheduler* ☑

Successfully added

5. After the communication with the rim node was established, a dialogue box which asks for authorization of the certificate is displayed.



Node edit

IDENTIFICATION

Name: Child01

Host name: ip-172-31-22-83.ap-northeast-1.compute.internal

If the host name machine has no authorized certificate, a password will be displayed. You will need this password to authorize the certificate on the host name's localhost.

NODE PURPOSE

Node purpose: Developn

SERVICES ACTIVATION

Repository ☑

Engine ☑

Proxy ☑

Scheduler ☑

TAGS

Tags: Connected tags

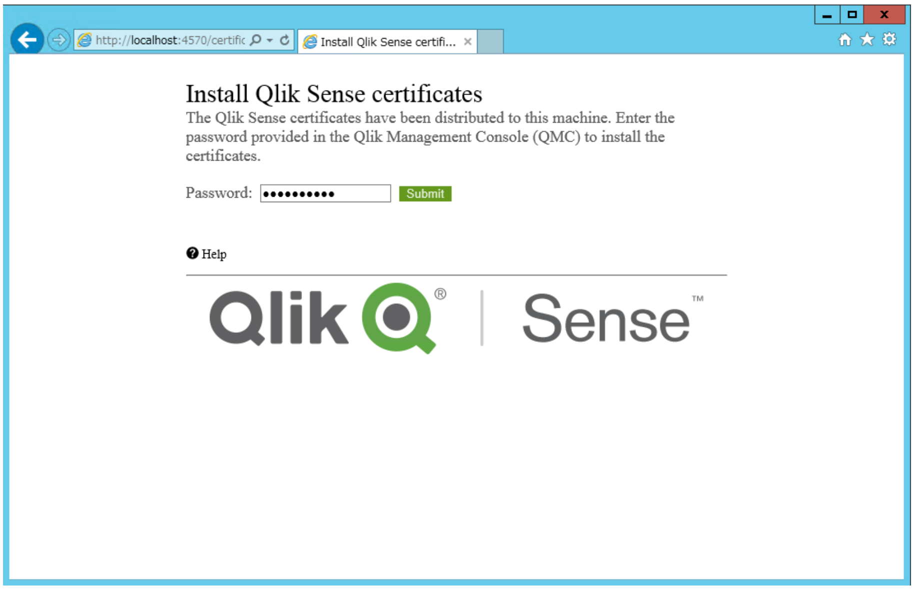
Your authorization password:

ZMv520tY1T

Please, copy and use this password on the hostname machine to authorize the certificate. Open a browser on the hostname machine and enter this URL: **http://localhost:4570/certificateSetup**
If you do not authorize the hostname machine, you will be able to repeat this process, but the node will not be operational for now.

6. Connect to the rim node on RDP and open a browser. Then, access to the following URL and submit the password displayed on the dialogue box in the previous step:

http://localhost:4570/certificateSetup



http://localhost:4570/certific

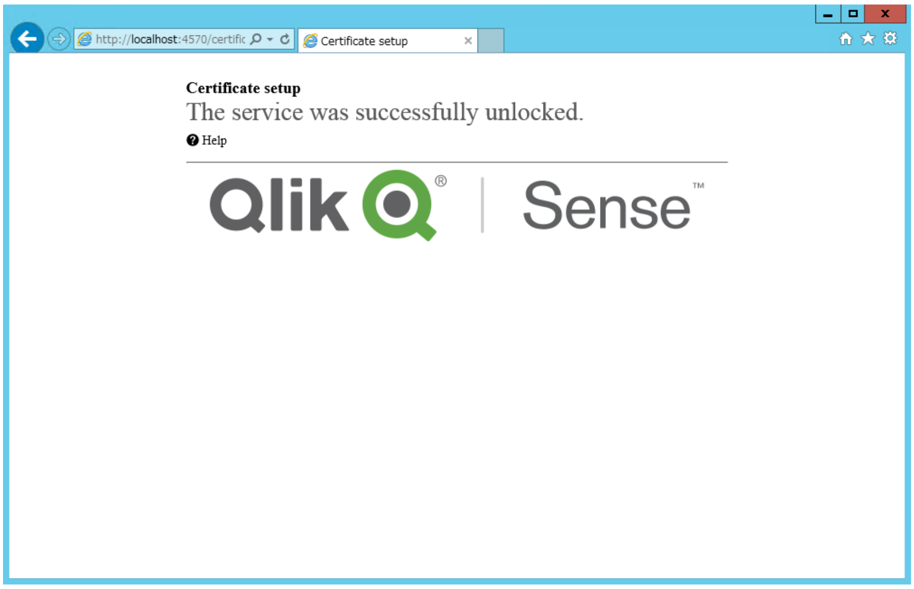
Install Qlik Sense certifi...

Install Qlik Sense certificates

The Qlik Sense certificates have been distributed to this machine. Enter the password provided in the Qlik Management Console (QMC) to install the certificates.

Password: ••••••••••

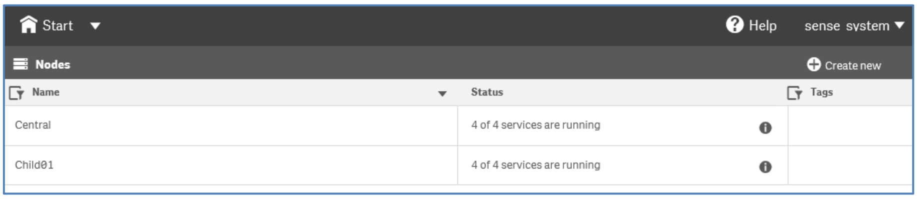
7. “The service was successfully unlocked.”



Certificate setup

The service was successfully unlocked.

8. You go back to QMC and make sure that the status of the added rim node is turned to “running”.

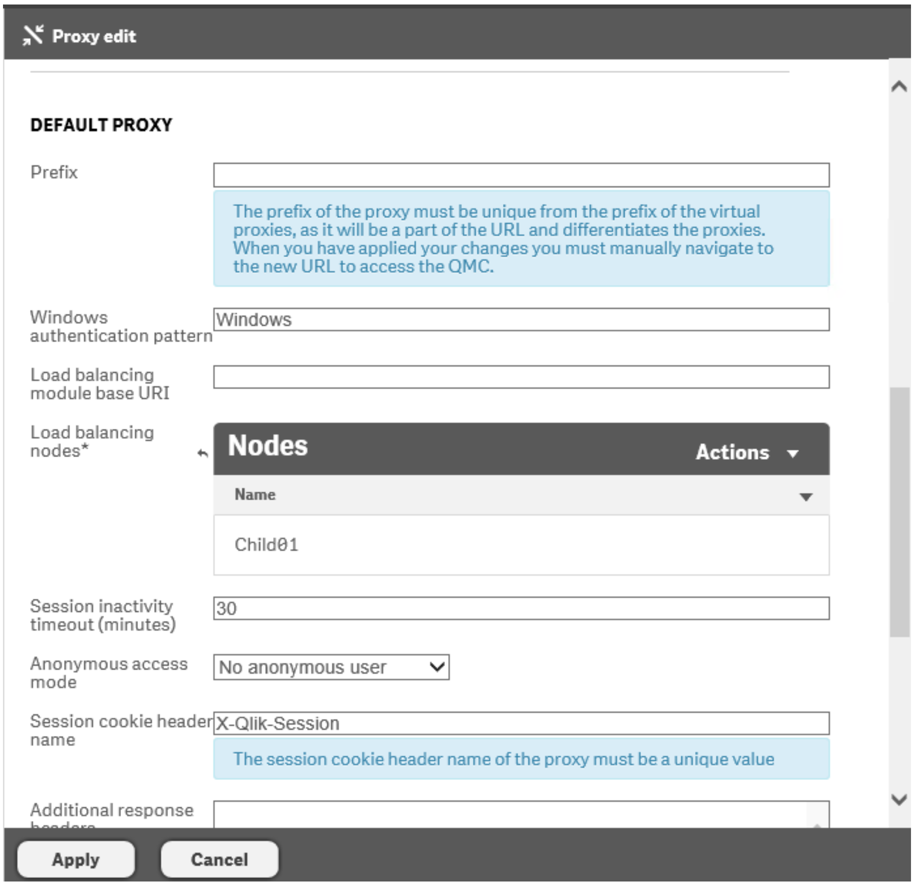


Name	Status	Tags
Central	4 of 4 services are running	
Child01	4 of 4 services are running	

9. You need to perform the following configuration on the proxy of the added rim node. (This is necessary only when you installed proxy service on the rim node.)

✓ Adding a node to “Load balancing nodes”.

✓ Adding entries to “Web socket origin white list”.



Proxy edit

DEFAULT PROXY

Prefix

The prefix of the proxy must be unique from the prefix of the virtual proxies, as it will be a part of the URL and differentiates the proxies. When you have applied your changes you must manually navigate to the new URL to access the QMC.

Windows authentication pattern: Windows

Load balancing module base URI:

Load balancing nodes*

Nodes — Actions

Name
Child01

Session inactivity timeout (minutes): 30

Anonymous access mode: No anonymous user

Session cookie header name: X-Qlik-Session

The session cookie header name of the proxy must be a unique value

Additional response headers