Change hostname and certificates after an installation

Content Source:Article Number 000014456

Introduction

The hostname in Qlik Sense is determined by the content of host.cfg, to change the hostname you must change the value in this file. This will also result in all certificates being invalid and need to be recreated. In a single node site this is sufficient, in a multi-node system there are further steps that will be required.

Setup and Configurations

Single Node

Single Node

1. Change hostname in Windows as usual.
2. Restart the server as required by Windows.
3. Stop all the Qlik Sense services, except for the Qlik Sense Repository Database
4. Use Microsoft Management Console(MMC) to delete all the Qlik Sense related certificates.
5. Delete *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates*
6. Make a copy of *%ProgramData%\Qlik\Sense\Host.cfg* and rename the copy to *Host.cfg.old*
7. Host.cfg contains the hostname encoded in base64. Generate this string for the new hostname using a site like https://www.base64decode.org/
8. Open Host.cfg and replace the content with the new string

Scenario 1 using Qlik Sense v3.2.5, then start up the Qlik Services, which will re-create the certificates, and then start Qlik Sense. If running Sense 11.11.1 (June 2017) or newer, follow the instructions below to recreate the Qlik certificates before starting up the Qlik Services.

Scenario 2 using June 2017 or newer release, instead of starting the Repository Service directly you need to run "***C:\Program Files\Qlik\Sense\Repository\Repository.exe" -bootstrap -iscentral -restorehostname*** from an elevated Command Prompt. This is required in order to re-create local Qlik certificates in newer versions of sense, as this is due to changes in this version that introduces the floating central node concept. Please also see Changing the user account to run Qlik Sense services in our public documentation.

NB The central certificate is used to encrypt password strings being used in connectors, so changing this certificate means that you will need to recreate all connectors that include password information.

Multi Node

Multi-Node

There are two possible scenarios in a multi-node environment changing the hostname for a Rim node and for a Central node. Certificates are always generated by the central node and are based on hostname so changing hostnames here is more time consuming and will require redistribution and in some cases also the deletion and reading of node information.

Changing Rim Node Hostname

On the **Rim node**:

1. Change hostname in Windows as usual.
2. Restart the server as required by Windows.
3. Stop all the Qlik Sense services
4. Use Microsoft Management Console(MMC) to delete all the Qlik Sense related certificates.
5. Delete *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates*
6. For backup purposes, make a copy of *%ProgramData%\Qlik\Sense\Host.cfg* and rename the copy to *Host.cfg.old*
7. Host.cfg contains the hostname encoded in base64. Generate this string for the new hostname using a site like https://www.base64decode.org/
8. Open Host.cfg and replace the content with the new string
9. Start up Qlik Sense, when it fails to find the certificates it will enter set up mode

Unfortunately it is not possible to adjust the hostname of a node in QMC, so a when a Rim node's hostname is changed you have to then delete and read it to do this

On the **Central server**:

1. Open Qlik Management Console (QMC)
2. Click Nodes
3. Select the node whose hostname has changed
4. Click Delete
5. Confirm your decision
6. Click Create New
7. Fill in the node details as appropriate

You will need to recreate and/or modify any rules that specifically named the old node

Changing Central Node Certificate

All certificates used by Qlik Sense are created and signed by the central node and are based on its hostname, changing the hostname on the central node breaks this chain of trust and thus all certificates on all nodes will need to be recreated and redistributed.

On every rim node:

1. Stop all Qlik Sense services
2. Use Microsoft Management Console (MMC) to delete all the Qlik Sense related certificates
3. Start Qlik Sense services
4. Upon starting without certificates they will enter Setup mode, meaning they will be listening for new certificates

On the central node:

1. Change hostname in Windows as usual.
2. Restart the server as required by Windows.
3. Stop all the Qlik Sense services, except for the Qlik Sense Repository Database
4. Use Microsoft Management Console(MMC) to delete all the Qlik Sense related certificates.
5. Delete *%ProgramData%\Qlik\Sense\Repository\Exported Certificates\.Local Certificates*
6. Copy *%ProgramData%\Qlik\Sense\Host.cfg* to *Host.cfg.old*
7. Host.cfg contains the hostname encoded in base64. Generate this string for the new hostname using a site like https://www.base64decode.org/
8. Open Host.cfg and replace the content with the new string
9. If running Sense v3.2.5, then start up the Qlik Services, which will re-create the certificates, and then start Qlik Sense. If running Sense 11.11.1 (June 2017) or newer, follow the instructions below to recreate the Qlik certificates before starting up the Qlik Services.
    - If running June 2017 or newer, instead of starting the Repository Service directly you need to run "***C:\Program Files\Qlik\Sense\Repository\Repository.exe" -bootstrap -iscentral -restorehostname*** from an elevated Command Prompt. This is required in order to re-create local Qlik certificates in newer versions of sense, as this is due to changes in this version that introduces the floating central node concept. Please also see Changing the user account to run Qlik Sense services in our public documentation.
10. Confirm the new certificates are created and QMC is accessible
11. In the QMC, click Nodes
12. Select each rim node and click Redistribute
13. Follow the instructions displayed

NB The central certificates are also used to encrypt password strings in the database, changing the central node certificates will require recreating all connectors with saved login information

Home
Products
Onboarding Program
External Content
News & Update
Organization
Qlik Partners