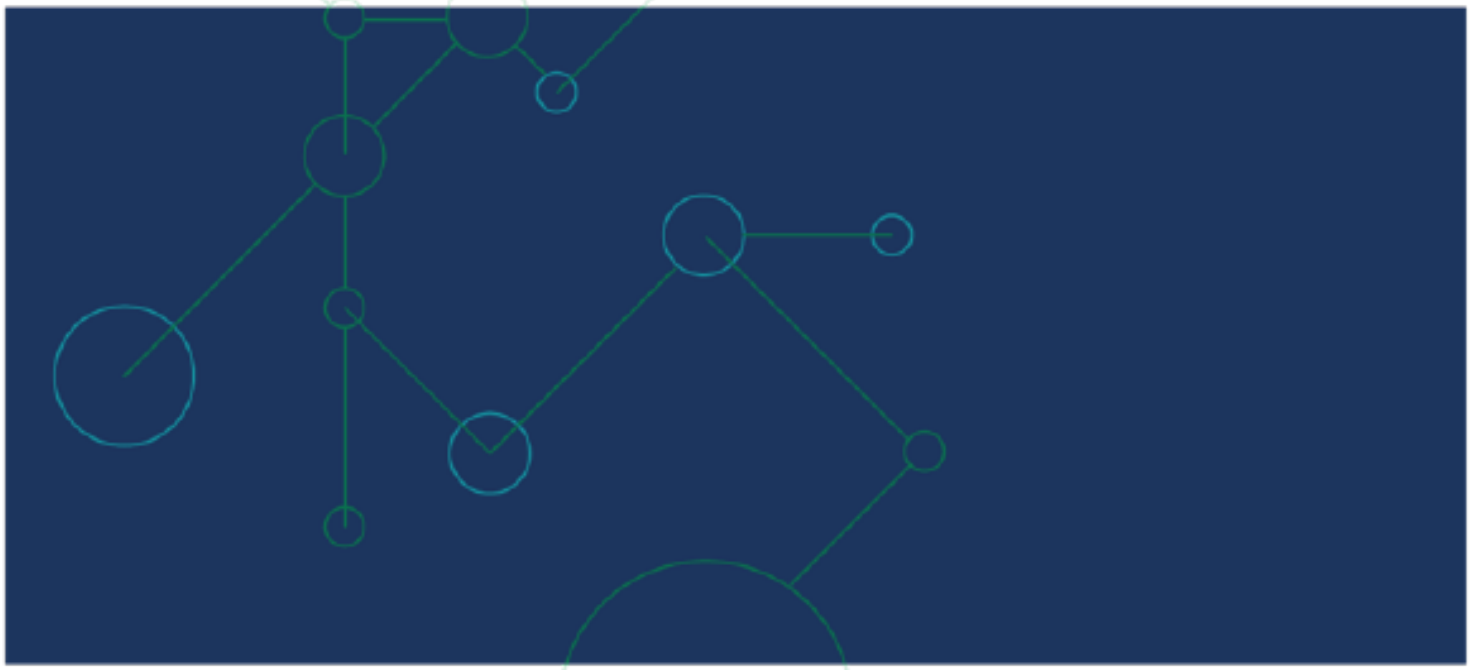
WHITE PAPER

Qlik Sense use of certificates

Architectural overview



SUMMARY

- Qlik Sense Enterprise is a data analytics platform
- The platform leverages a distributed architecture based on web technologies
- Qlik protects customer information using industry standards
- For protection of information in transit Qlik Sense makes use of TLS (Transport Layered Security) for encryption and certificates for authentication of clients
- Qlik Sense Enterprise implements two main use cases for certificates; HTTPS encryption and authentication of servers for client access and for mutual authentication of service to service communication.
- For client access, externally generated certificates can be used
- For service to service authentication, Qlik Sense Enterprise implements an internal Certificate Authority to issue certificates

INTRODUCTION

When Qlik Sense Enterprise was designed, a key design decision was to use standard security components where possible to solve different aspects of security. Protecting communication is a good example of this, as we used standard components to protect against rogue servers and eavesdropping.

When Qlik Sense Enterprise needs to exchange information between different services, the Qlik services need to trust each other, and Qlik services need a way to talk without others listening to the conversation.

In Qlik Sense Enterprise, all communication between services and clients use web protocols. With these we get the option of using a widely deployed standard for building trust and protecting the communication from eavesdropping. The way of achieving secure communication is tightly knit together by two components:

• TLS (Transport Layer Security), the protocol for encryption and exchange of information/keys

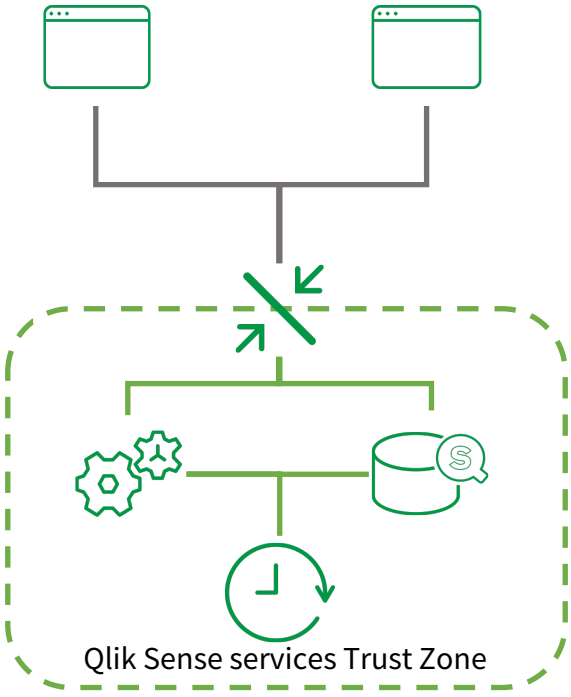
• Certificates for authentication of the servers that need to communicate

What TLS supplies is a way to build protected tunnels between two identified servers using encryption. The identification of the servers that communicate is done using certificates. Each tunnel needs two certificates, one to prove to the one starting the communication that they talk to the correct recipient and one to prove to the recipient that the one wanting to communicate is allowed to do so, i.e. mutual authentication.

So how do we know if the certificates are valid for communication between the servers? All certificates that belong to a trust zone (unique for each deployment of Qlik Sense) are signed by the same signature (root certificate) and only this signature will be accepted as proof of belonging to the trust zone.

The root certificate is unique to each Qlik Sense deployment and generated during installation and protected by the operating system's certificate store.

When these protected tunnels are in place and we have the right certificates in place, we can build a trust zone for all Qlik Sense services to work within. Within the Qlik Sense trust zone only the services belonging to that specific Qlik Sense installation can communicate.



Outside this trust zone we have the clients running in the user's browser (Qlik Management Console and the Analytic Client). These components are running on less trusted end user devices; therefore, we do not allow them to be part of the Qlik Sense trust zone. The only component that can bridge the two zones is the proxy (but there may exist more than one bridge in an installation). The criteria required to cross the bridge and communicate in a controlled way with the servers in the trust zone,

is to authenticate (show who you are) to the system so it can determine if you are allowed to cross the bridge.

Even though the clients are not part of the Qlik Sense trust zone, protected tunnels (TLS) play a vital role in securing the communication between the client and the proxy, because sensitive information is sent across this connection. Since this is a different trust zone, a certificate with a different signature issued by a different certificate authority should be used for the client communication.

End user access

Overview

Qlik Sense uses web protocols for users to access the platform and analyze information. The web protocols can use TLS as the method to protect the communication from the client's browser/device to the platform's entry point (Qlik Sense Proxy). If TLS is used to protect the communication, there is also a need for the client to authenticate that the server it builds trust with is the server that you as a user want to connect with. For this purpose, Qlik Sense uses certificates. The trust of certificate is based on its issuance by an external certificate authority trusted by the browser used to access Qlik Sense. Qlik Sense allows for customers to install and use a certificate of their choice.

Certificate use

The client uses one externally generated certificate that is installed into the Windows certificate store and referenced in the Qlik Management Console as the external certificate to use for server authentication for client communication.

More information

https://help.qlik.com/en-US/sense/June2019/Subsystems/AdministerQSEoK/Content/Sense_QMC/change-to-signed-server-proxy-certificate.htm

Building trust zones

Overview

Qlik Sense is using TLS and certificates to build a trust zone for the services of a Qlik Sense deployment. TLS is used to protect the communication and certificates are used to implement mutual authentication (the server knows that it talks to the right client and the client knows it talks to the right server).

To achieve the trust zone Qlik Sense deploys a Certificate Authority with the installation of the product that uses a deployment unique root certificate to sign all other certificates needed to build up the trust relation between the services.

Certificate types

Root certificate

The top level certificate is used by the Certificate Authority to sign all other certificates belonging to a deployments trust zone for services. All certificates signed by the root certificate are trusted by other services in a deployment

Client certificate

The client certificate is used to authenticate the service connecting to another service.

Server certificate

The server certificate is used to authenticate the service receiving a connection.

Certificates

The root certificate is created at install time and used to create new certificates (client and server) when new servers are joined to the deployment.

The joining of a server to a deployment initiates the needed distribution of certificates to the other nodes for secure communication to be used. The distribution of certificates uses out of band exchange of secrets to protect the distribution.

All certificates distributed are stored and secured using the Windows Certificate Store and its protective measures.

Information in the certificates are also used for encryption of secrets in the Qlik Sense database (Postgres).

More information

https://help.qlik.com/en-US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Certificate-Trust.htm

https://help.qlik.com/en-US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Certificate-Trust-Architecture.htm

https://help.qlik.com/en-US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Server-Security-Authentication-Certificate-Trust-Using-MMC.htm

Qlik LEAD WITH DATA

About Qlik

Qlik is on a mission to create a data-literate world, where everyone can use data to solve their most challenging problems. Only Qlik's end-to-end data management and analytics platform brings together all of an organization's data from any source, enabling people at any skill level to use their curiosity to uncover new insights. Companies use Qlik producs to see more deeply into customer behavior, reinvent business processes, discover new revenue streams, and balance risk and reward. Qlik does business in more than 100 countries and serves over 48,000 customers around the world.

qlik.com