White Paper

Qlik Sense® Enterprise security overview

July, 2018

Platform

Qlik Sense is Qlik's next-generation platform for modern, self-service oriented analytics, supporting the full spectrum of analytics use cases from visualization to reporting, all within a governed multi-cloud architecture that offers scalability, trust and ongoing choice for the organization. It delivers broad value for all types of users, offering unmatched associative exploration, accelerated self-service creation, collaboration and reporting, online and offline mobility, customization and extension, data integration, and governed, multi-cloud scalability supporting the entire enterprise ecosystem. Qlik Sense runs on the patented Qlik associative engine, which allows users of all skill levels to explore information freely without the limitations of query-based tools.

Qlik Sense® Enterprise for Windows

Qlik Sense Enterprise for Windows provides self-service visualization that is scalable, secure, and governable. It can be deployed on-premise or in a customer-or partner-managed cloud, and users can perform a variety of analytic activities ranging from consumption to data preparation to creation of visualizations. To ensure platform security, Qlik Sense leverages internal and external resources to manage access, authentication, authorization, and data governance on four levels.

- **Network security:** All communication between Qlik Sense services and web clients use web protocols using Transport Layer Security (TLS). TLS uses digital certificates to encrypt information exchanged between services, servers, and clients. Encrypted information flows through tunnels requiring two certificates to secure the connection; a server certificate to identify the correct server and a client certificate to allow the client to communicate with the identified server.
- **Server security:** The operating system security system controls access to certificates, storage, memory, and CPU resources. Qlik Sense uses these controls to protect the platform by only allowing authorized users and processes access to required resources.[1]
- **Process security:** Qlik Sense goes through a rigorous testing process during development to mitigate security risks and handle unanticipated events. Additional testing verifies Qlik Sense can stand up against known security threats toward the software.
- **App security:** Attribute based access control provides a comprehensive framework to govern user capabilities within the platform. Row and column level data reduction through section access dynamically manages the data which users view and select in applications.

[1] For more information about Qlik Sense architecture, review the Qlik Sense Architecture & Scalability whitepaper.

Authentication

Qlik Sense Proxy

All authentication in a Qlik Sense deployment is managed by the Qlik Sense Proxy Service (QPS), including clients connecting to the Hub or the Qlik Management Console (QMC). Qlik Sense requires an external identity provider to verify an individual user's identity. Upon verification, Qlik Sense transfers the user to Hub or QMC, encrypting traffic using TLS and certificates with the following methods:

- **SAML** integration with Qlik Sense acts as a service provider integrating with an identity provider.
- **Windows Integrated Authentication** allows for NTLM or Kerberos based authentication.
- **JSON Web Tokens (JWT)** enable secure transmission between two parties as a JavaScript Object Notation (JSON) object.
- **Ticket/Session APIs** transfer the user and user's attributes using a one-time ticket allowing for integration with websites and portals.
- **HTTP Headers** in solutions with trusted systems that transfer user information using this method.
- **Anonymous** users can be configured to access Qlik Sense.

Qlik Sense - three step authentication

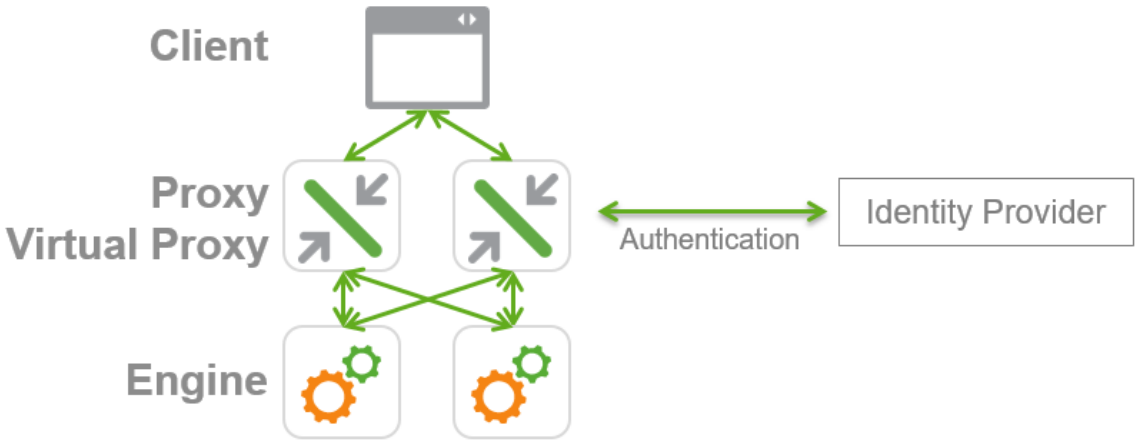
1. Authentication module gets the user identity and credentials.

2. Authentication module requests an external system to verify the user identity using the credentials.

3. User transferred to Qlik Sense using the Ticket API, Session API, HTTP headers, or SAML.

Virtual Proxies

Each QPS in a Qlik Sense deployment uses Virtual Proxies to support authentication. Virtual Proxies allow one proxy to support multiple authentication schemes, perform session management, and load balancing across multi-node deployments. Virtual Proxies may link to one or many QPS nodes to direct traffic, load balance between engines, or provide specific access to administrative layers of a deployment.



Authorization

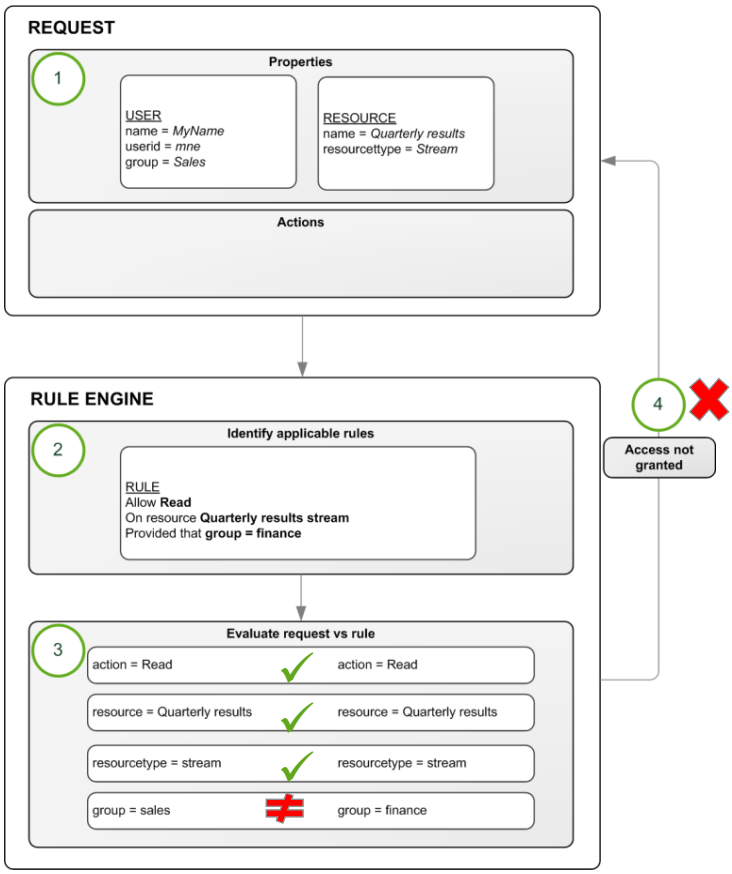
After a user authenticates and gains access to Qlik Sense, authorization through an attribute based access control (ABAC)[2] model enforces application visibility and self-service capabilities within applications.

Attribute Based Access Control (ABAC)

In Qlik Sense, ABAC is defined as an access control method where **user** requests to perform **actions** on **resources** are granted based on assigned attributes of the **user**, assigned attributes of the **resource**, **environment** conditions, and a set of **security rules** that are specified in terms of those attributes and conditions. Attributes from Active Directory, LDAP, and databases are loaded into Qlik Sense. In addition, attributes may be defined and managed directly within Qlik Sense as well.

Security Rules

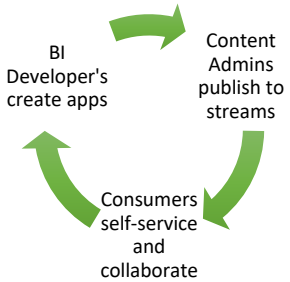
Qlik Sense security rules define user capabilities on Qlik Sense resources provided a condition. Access is provided if at least one rule returns true based on attributes like the roles or groups of the user and resources.



Security rules control access to application streams in the hub, capabilities within applications (sheet, story, bookmark creation), and administrative capabilities in the QMC (publish apps, set stream access, create and run tasks).

The security rules framework comes with several predefined rules enabling administrators to scale security across users leveraging existing roles and groups in the enterprise.

In a roles based enterprise, BI authors are responsible for app creation and have data access. Content Admins do not create, but publish applications to streams aimed at groups of consumers. Consumers can extend their own analysis with sheets and stories within an application; sharing new found insights with their teammates without compromising the integrity of the core application.



These capabilities and corresponding rules are delivered out of the box with Qlik Sense.

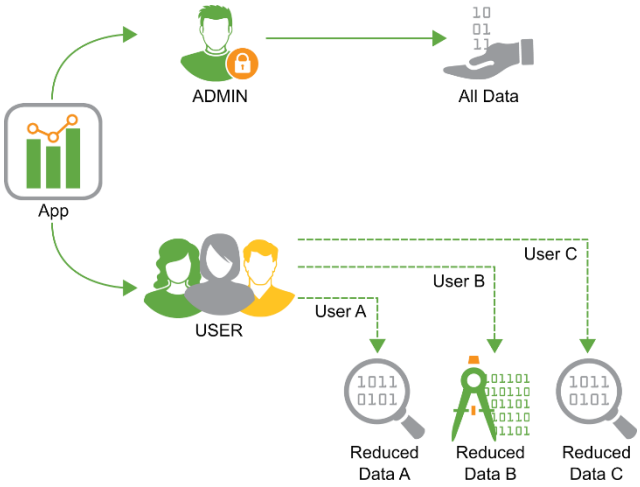
[2] ABAC is a special publication of the National Institute of Standards and Technology (NIST) catalogued as NIST Special Publication 800-162.

Data Reduction

Data reduction in Qlik Sense determines what data users and groups are allowed to see when they enter a Qlik Sense application. In Qlik Sense, data reduction is known as section access.

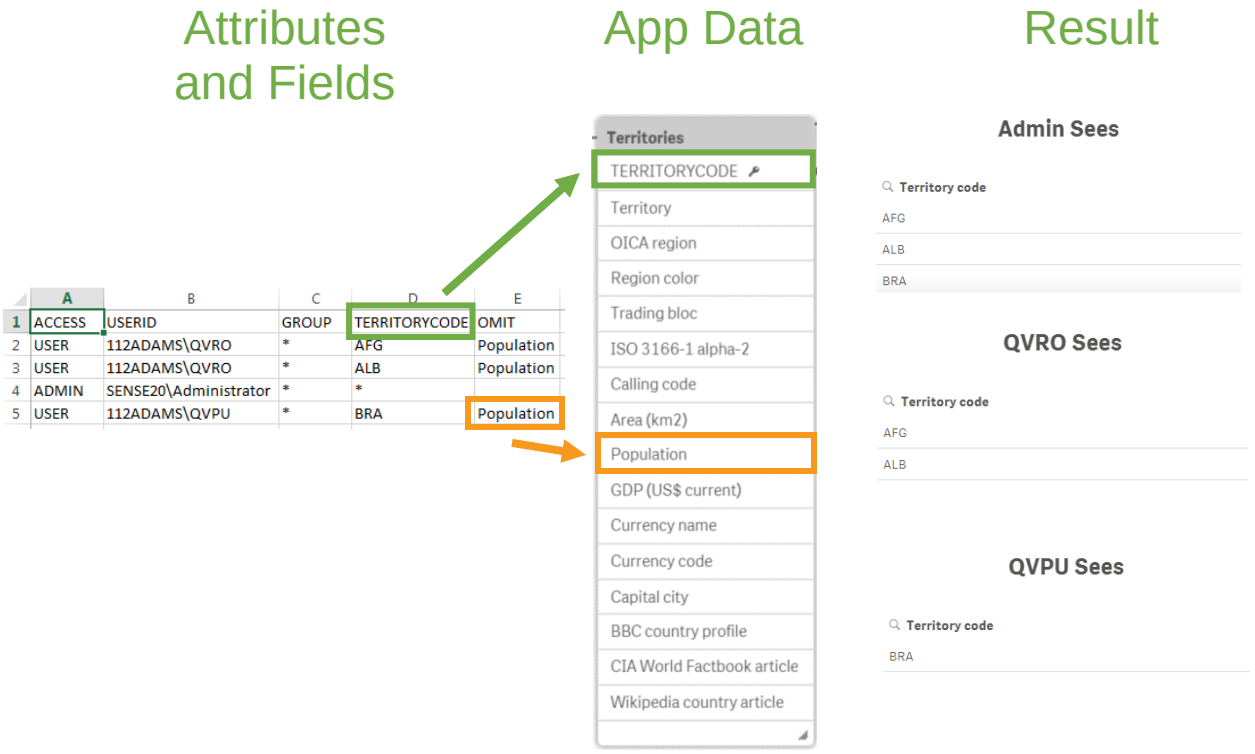
Section Access

Section access performs row and column level security in a Qlik Sense application. With section access, a single Qlik Sense application may hold data for multiple users or groups. Through the authentication and authorization process, user information is sent into the application to dynamically reduce the data so that users access only the data they are allowed to view. Section access may use attributes and fields from external databases, directories, lookup tables, or created tables to enforce user visibility to data.



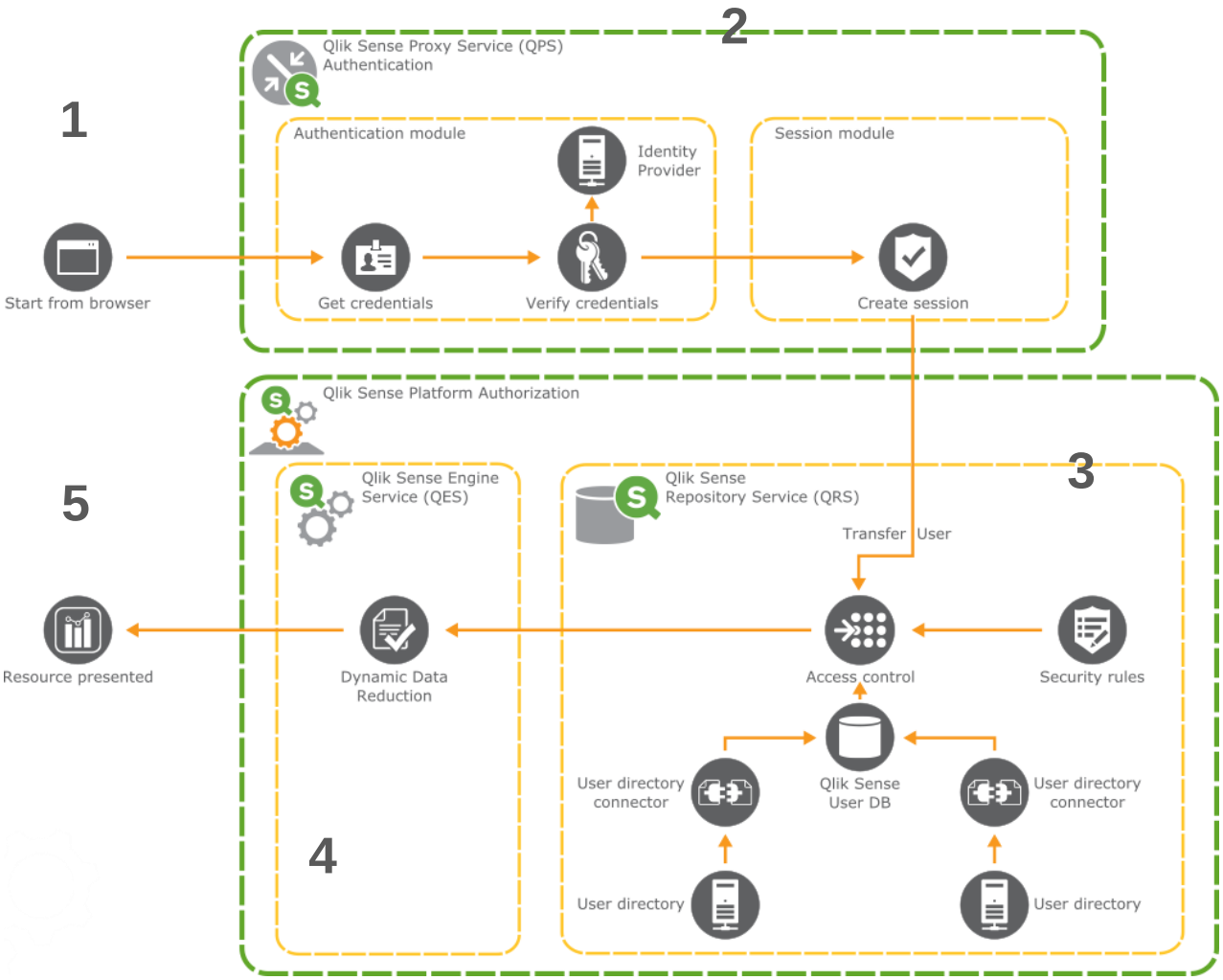
Dynamic Data Reduction

Section access reduces data in an application dynamically by associating section access data with the business data loaded into the application with a single defined relationship. Using common field names, rows of data are excluded from the user during application interaction. In addition, columns of data may be hidden from view by specifying field names to omit for each user.



Qlik Sense Security User Access Workflow

Combining authentication, authorization, and data reduction is a seamless experience for a user accessing Qlik Sense.

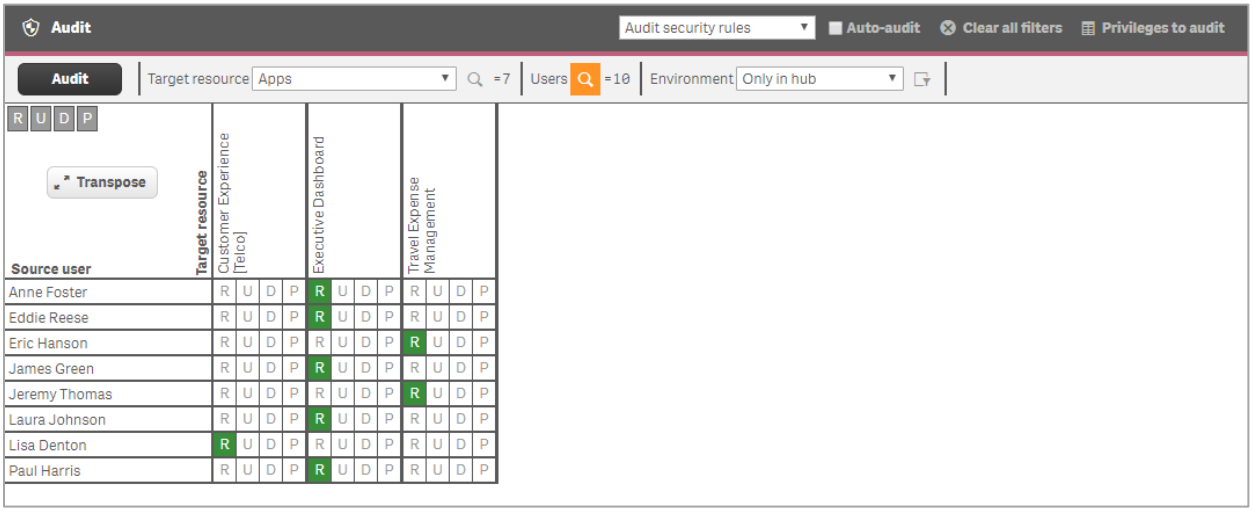


1. A user makes a request for Qlik Sense content.
2. The Qlik Sense proxy service authenticates the user and creates a session cookie in the browser.
3. The session cookie identifies the user to Qlik Sense and synchronizes with a user directory to import attributes. At the same time the rules engine authorizes the user to Qlik Sense content using the attribute based access control model.
4. The session state for the user is created in the engine. The engine performs dynamic data reduction using section access.
5. The engine sends content through a web socket connection to the client to render Qlik Sense content.

Auditing

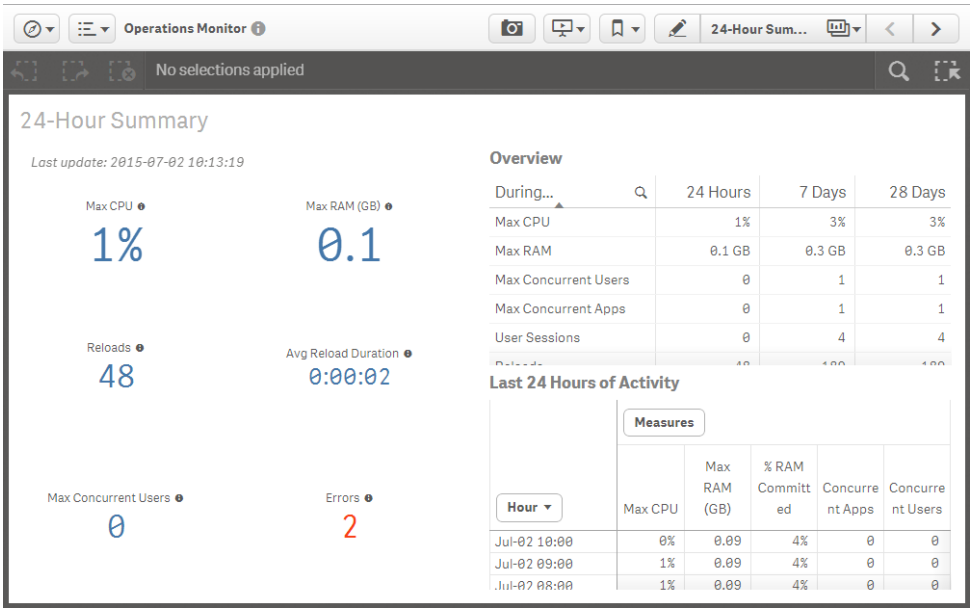
Governance is critical in enterprise business intelligence. Qlik Sense delivers auditing, monitoring and logging using the QMC, applications, and log files to inform administrators and mitigate risks in deployments.

- **Audit** security rules using the Audit tab built into the Qlik Management Console.



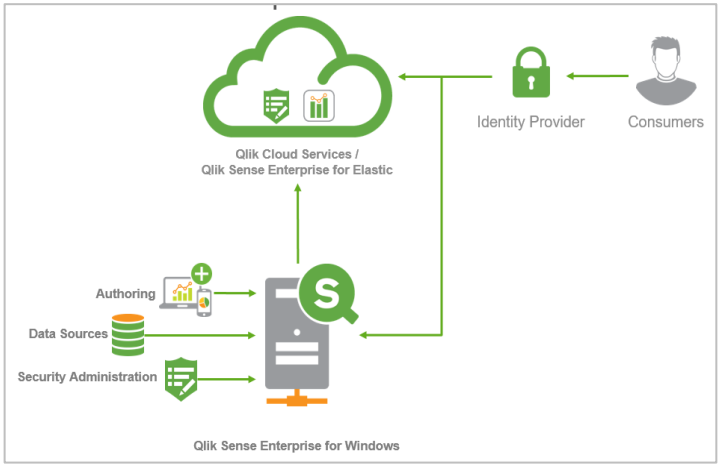
Using the filters at the top of the audit screen, administrators can evaluate user access control for applications. Administrators can use inline auditing when creating security rules for streams, content libraries, and data connections to preview access control based on rules they write.

- **Monitor** Qlik Sense using the built-in Operations Monitor and License Monitor applications. These applications present information related to uptime, sessions, resource utilization, change logging, and license compliance and management.
- **Logging** to text files runs in the background in a Qlik Sense. All services include audit, system, and trace logs for deployment monitoring and management.



Qlik Operations Monitor

Qlik Sense Enterprise with Multi-Cloud Deployment



The optional multi-cloud capability of Qlik Sense Enterprise allows organizations to broadly scale policy-driven deployments to expand the reach of analytics to new users, while retaining flexibility to choose where analytic consumption takes place. Organizations can use multi-cloud capabilities to distribute apps from Qlik Sense Enterprise for Windows deployments to managed container services using Qlik Sense Enterprise for Elastic or hosted by Qlik using Qlik Cloud Services. Both capabilities are technically similar, Qlik Sense Enterprise for Elastic (QSEfE) is customer-deployed while the Qlik Cloud Services is a fully managed hosted service by Qlik. The underlying architecture is microservices-based and delivered through Docker and Kubernetes.[3] The following is an overview of the relevant services as used in both QCS and QSEfE highlighting the differences where appropriate.

Ingress

[*container name: qsefe-nginx-ingress-controller*]

All client communication and Qlik Sense Enterprise from Windows communication is routed through an NGINX-Ingress controller named qsefe-ngnix-ingress-controller. This ensures a single point of entry to the multi-cloud environment, and by leveraging the capabilities of Kubernetes, NGINX-Ingress can take advantage of edge devices within managed container services such as a load balancer.

Authentication

[*container name: qsefe-edge-auth*]

Users access content in the multi-cloud environment using a web based portal and analytics client. The client is protected an Identity Provider (IdP) conforming to OpenID Connect, such as Auth0 or Okta, and integration between the IdP and the multi-cloud environment is handled via a container called qsefe-edge-auth. All communication between the IdP and qsefe-edge-auth is encrypted using TLS. Customers should ensure they are using an IdP that supports both SAML to connect to Qlik Sense Enterprise for Windows and OpenID to connect to the multi-cloud environment. With this, users can login using the same credentials and leverage a single license and consistent entitlements throughout.

Similarly, service communication between Qlik Sense Enterprise for Windows and the multi-cloud environment is encrypted using TLS and authenticates using the same IdP integration as above.

[3] For more information about Qlik Sense architecture, review the Qlik Sense Architecture & Scalability whitepaper.

Authorization

[*container name: qsefe-policy-decisions*]

The relevant entitlements defined using the Security Rules in Qlik Sense Enterprise for Windows are automatically pushed to a multi-cloud environment and enforced with a container called qsefe-policy-decisions. Other containers within the deployment leverage qsefe-policy-decisions to determine the permissions of a user, such as which applications and collections of applications (e.g., Sales, Finance) the user can access. Additionally, section access, which provides row and column level security, is enforced in the multi-cloud environment.

Data Access

Distribution Policies

With Distribution Policies that are defined and managed in the Qlik Sense Management Console, it is possible to specify which applications that are to be delivered to the multi-cloud environment. Those applications are transmitted using TLS and stored in a persistent volume using Kubernetes. Encryption of persistent volumes are managed by the host operating system.

Secrets

Secrets such as MongoDB credentials, IdP configuration, SSL certificates are stored using Kubernetes Secrets.

Qlik Cloud Services

With multi-cloud capabilities, apps can be distributed from Qlik Sense Enterprise for Windows deployments to Qlik Cloud Services, a fully managed service provisioned and administrated by Qlik, using the distribution policies described above.

Qlik Cloud Services is hosted on Amazon AWS infrastructure in three regions; United States East (Virginia), Europe West (Ireland), and APAC (Sydney). Customers may choose the region in which their data resides, and data will not leave that region. Qlik leverages the AWS shared responsibility model as a secure foundation upon which Qlik Cloud Services is built.

Qlik follows security best practices within Qlik Cloud Services such as strong authentication, the principle of least privilege, encrypted data at rest and in transit, disaster recovery testing, and more.

Qlik is Privacy Shield approved and adheres to GDPR requirements, for more details please see the below links;
Qlik Privacy Shield Policy: https://www.qlik.com/us/legal/privacy-shield-policy
Qlik and GDPR: http://qlik.com/gdpr

Summary

Qlik Sense security provides comprehensive security at multiple levels to ensure only permissible users have access to allowable data via a secure connection.

- **Authentication** handled by the Qlik Sense Proxy Service (QPS) using certificates and Transport Layer Security (TLS) to encrypt network traffic.
- **Authorization** using an attribute based access control (ABAC) system for managing user access and content, and using section access for data reduction.
- **Auditing** the Qlik Sense platform tracking changes in the repository database, comprehensive audit and security logging, and monitoring applications.
- **Confidentiality** by encrypting network connections with TLS, leveraging the operating system file system and server access controls to protect content on Qlik Sense nodes, protecting memory using operating system controls, securing application access at the resource level, encrypting sensitive information (e.g. passwords and data connection strings), and protecting app data using data reduction.
- **Integrity** through operating system controls like the file system to protect data at rest, encrypt sensitive information, and prevent data write back to the source system.
- **Multi-Cloud** allows for secure deployment to a hosted or customer managed deployment leveraging the same authentication and authorization schemes as defined in Qlik Sense Enterprise for Windows.

To learn more, please visit Qlik.com.