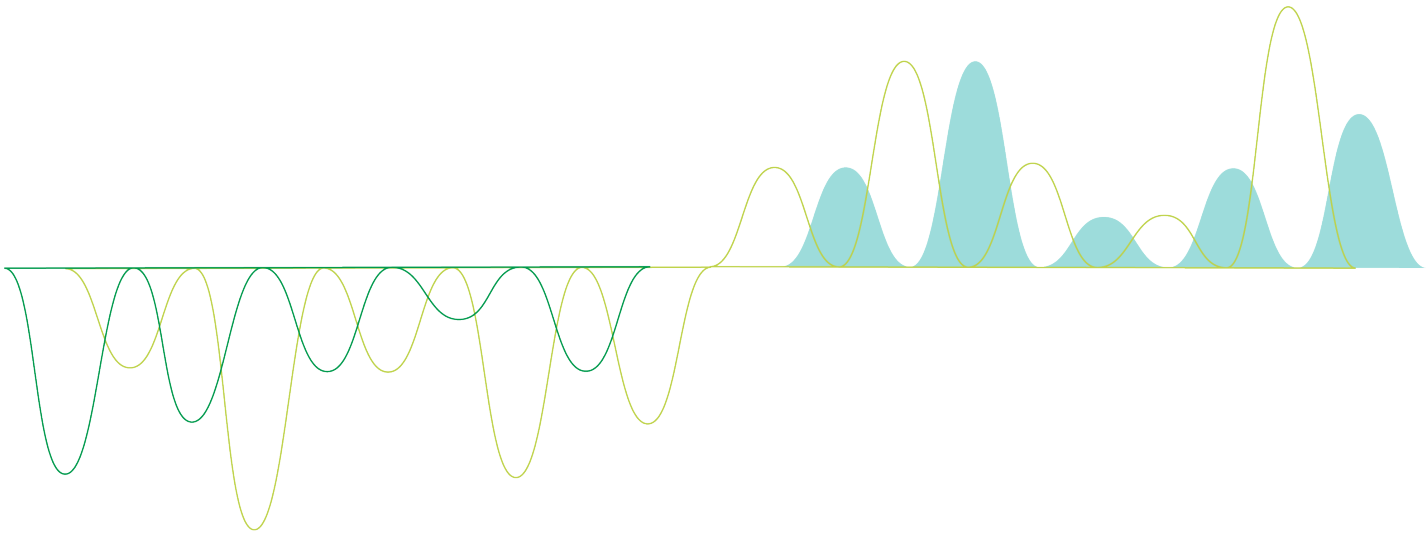
Administer Qlik Sense Enterprise on Kubernetes

Qlik Sense®
June 2020



Contents

Contents

1 Management console

The management console is used for managing licenses, user assignments, manage spaces, themes, and extensions in SaaS editions of Qlik Sense. The management console should not be confused with the Qlik Management Console (QMC), which is used for managing Qlik Sense Enterprise on Windows. Only users with Tenant Admin role have access to the management console.

The management console user interface is made up of four conceptual sections, each consisting of a number of different pages:

- **Governance**: manage users, licenses, spaces, schedules, events and links
- **Content**: manage custom content, such as themes and extensions
- **Integration**: manage security aspects for integration
- **Configuration**: enable feature settings and configure identity providers

1.1 Accessing the management console

You access the management console by adding */console* to your tenant address: *https://<your tenant address>/console*, or by using the navigation link **Administration** under user profile in the hub.

1.2 Users

The users page displays all the users that have logged into the tenant. If a user has a certain role (tenant admin), it is displayed in the roles field.

1.3 License

The license allocation section has three tabs: **Overview**, **Assigned users**, and **License key**.

1.4 Spaces

The spaces page displays information of all the spaces created in the tenant as well as lets you create new spaces and edit existing ones.

1.5 Schedules

With scheduling, you can view and delete reload schedules for apps in your system. Schedules can only be created from the hub.

1.6 Events

On the events page, you can follow up on events in your system and get information about the event type and the user who initiated the event.

1.7 Generic links

If you have a multi-cloud deployment consisting of QlikView or Qlik Sense Enterprise on Windows in combination with Qlik Sense Enterprise SaaS or Qlik Sense Enterprise on Kubernetes, generic links offer an easy way to make on-premise apps available in the cloud.

1.8 Apps

The apps page lets you manage all apps in the tenant.

1.9 Extensions

The extensions page lets you manage all the extensions in the tenant, as well as uploading new ones.

1.10 Themes

The themes page lets you manage all the extensions in the tenant, as well as uploading new ones.

1.11 API keys

An API key is a unique identifier used for authentication of a user, developer, or calling program to an API. API keys are often used for tracking and controlling how the interface is used, to prevent abuse of the API.

1.12 Content Security Policy

Content Security Policy (CSP) provides an extra layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

In Qlik Sense, CSP allows tenant admins to control resources an extension or a theme is allowed to load for a given page. With a few exceptions, policies mostly involve specifying server origins and script endpoints. If an extension or theme contain links to external resources, these must have its origins whitelisted in the Content Security Policy.

1.13 Web

You can create web integrations to add origins that are whitelisted to access the tenant. The web integration containing the whitelist is connected to an ID used in for example a mashup that is connecting to your tenant. When a request arrives, Qlik Sense confirms that the request derives from a whitelisted domain and then approves the request, else not.

1.14 Settings

The settings page lets you manage the following sections:

- On-demand data
- Groups
- Dynamic license assignment
- API keys

2 Licensing Qlik Sense Enterprise on Kubernetes

When you buy a new license for Qlik Sense Enterprise SaaS, the license key is set automatically during on-boarding. If needed, you can change the license key manually at a later moment.

The user who enters the tenant for the first time becomes tenant admin. The tenant admin can assign the role tenant admin to other users. It is required to have at least one tenant admin. To prevent accidental removal of the last tenant admin, you cannot remove the role tenant admin from yourself.

It is possible to lose the ability to repair or modify the identity provider configuration in Qlik Sense Enterprise SaaS if the account owner has been removed as a tenant admin. If the identity provider (IdP) in use in a tenant is no longer functional and needs to be modified, it is necessary for the original tenant account owner to access the management console through the recovery URL. This will fail if this user is no longer an administrator. For more information, see Repairing or modifying your IdP when the account owner is removed as tenant admin*.*

Qlik Sense Enterprise on Kubernetes is licensed using a signed key. You apply your license for a Qlik Sense Enterprise on Kubernetes installation in the management console.

For an overview of the License section of the management console, see: *Management console (page 6)*.

2.1 Applying the Qlik Sense Enterprise on Kubernetes license

Do the following:

1. In the management console, navigate to the **Licenses** section.
2. In the **Overview** tab, enter the signed key in the **License key** input box.
3. Select **Submit** to apply the license.

3 Assigning access to users

Users are managed in the Management console on the **Users** and the **Lisense** pages.

3.1 Users overview

The users page displays all the users that have logged into the tenant. If a user has a certain role (tenant admin and developer), it is displayed in the roles field.

Use search for the fields **Name**, **User ID**, and **Email**. The IdP subject field can be used for distinguishing one user from another if the names are identical and the email field is not visible. For each user in the table, you have a button to the far right where you can assign and remove the tenant admin role, and activate or disable users. If you have the invite users license, you also have options for resending or deleting user invitations.

User status

The following are the available user statuses.

Status	Description	Status can be changed to
Active	User is fully registered and can consume according to the assigned license.	Disabled
Pending	User is invited but has not yet registered.	Active
Disabled	User license is removed and that user cannot access their account or use the product.	Active

3.2 License overview

The license section has three tabs: **Overview**, **Assigned users**, and **License key**.

Overview tab

Overview shows basic information about the license. In the Overview tab you can also add a license if needed.

License item	Description
Professional	**Consumed**: number of users with professional access. **Total**: Total availability of professional access.
Analyzer	**Consumed**: number of users with analyzer access.

	Total: Total availability of analyzer access.
Analyzer capacity (minutes)	**Consumed**: amount of minutes spent.
	Total: Total amount of minutes available per month. Overage is required after the total amount has been spent.
	Overage. Overage can either be limited, to the amount stated, or unlimited.
Expires	Date of license expiration.
Quotas	
Shared spaces	**Consumed**: number of shared spaces. **Quota limit**: Quota limit can either be limited, to the amount stated, or unlimited.
Managed spaces	**Consumed**: number of managed spaces. **Quota limit**: Quota limit can either be limited, to the amount stated, or unlimited.
In-memory app size	Maximum app memory size.

Assigned users tab

Assigned users shows information about users and license types. There are also buttons for removing assignments and assigning analyzer or professional access.

License item	Description
Name	Name of user.
User ID	Unique ID for the user.
IdP subject	User identifier in the identity provider (IdP). This value is populated from the IdP user database when users log in.
License	License type assigned to the user: professional, analyzer, or analyzer capacity (also known as analyzer time).
Status	When the number of allocated assignments is larger than defined by the license, some users will be excluded. The users will then no longer have access to the hub or the management console. The **Status** column for the users will show *Excluded*. Those who most recently were assigned access will be excluded. They will remain excluded until the number of allocations matches the number

defined by the license. If more access assignments are made available, or if the admin removes access for others, access will be reallocated to excluded users.

License key tab

In the License key tab you can change a license if needed. To change the license: paste the license key in the text box and click **Submit**.

3.3 Invite users

There are two ways to add users to your deployment. If you have an IdP, you can create an IdP configuration in the **Identity provider** section. If you do not have an IdP, you can add users by sending invite emails. Use the **Invite** button in the **Users** section. You can also invite users from your profile. In the invite form, you add email addresses of the users separated by comma or space. The email contains a link (button), which is only valid for a limited period. The invite expiry date is displayed in the table. When the user clicks the button an account registration page is opened.

When the invite has been sent, the status field in the **Users** table displays *invited*. When the user has registered, the status is changed to *active*. If needed, you can resend the invite. You can also delete an invite. In that case the user cannot register, even if the link has not expired.

Your license only includes one of the options to add users, either through an IdP or by sending email invites.

Do the following:

1. In the management console, go to the **Users** section and click **Invite**.
2. Enter the email addresses of the users that you want to invite, and click **Send invitation**.
3. On the Invitation sent page you can choose **Manage invites** to go to the management console, **Invite more users**, or click **Done** to exit.

   You can remove an invitation from the management console.

Tenant admins can also invite users from the hub by selecting **Invite users** in their profile in the top right corner.

3.4 Add access type to a user

Tenant admins can assign and remove access for users in the management console.

Do the following:

1. In the management console, go to the **License** section and select the **Assigned users** tab.
2. Click **Add assignment**.
3. Select a user from the **Search for a user** field.
4. Select the **Access type**.
5. Click **Add**.
6. Add more users if needed and when finished click **Close**.

3.5 Remove assignment

Licenses can be removed for users.

Do the following:

1. Select the user from the list.

   You can select multiple users at the same time.

2. Click **Remove assignment**.
3. Click **Delete** to confirm the license removal.

3.6 Assign professional access to a user with analyzer access

You can assign professional access to users with analyzer access.

Do the following:

1. Select the user from the list.

   You can select multiple users at the same time.

2. Click **Assign professional access**.
3. Click **Confirm** to confirm the assignment.

3.7 Enable dynamic license assignment

Dynamic license assignment can be used to simplify the assignment of access to users and is enabled in the management console on the **Settings** page.

Property	Description
Enable dynamic assignment of professional access	When enabled, users who log in are

	automatically assigned professional access, if available.
Enable dynamic assignment of analyzer access	When enabled, and no professional access is available, users who log in are automatically assigned analyzer access, if available.

Choose between four options:

- Dynamic assignment enabled for both professional and analyzer access:

  Professional access is assigned, if available, otherwise analyzer access. If neither of those are available, analyzer capacity is assigned, if available.

- Dynamic assignment enabled only for professional access:

  Professional access is assigned, if available, otherwise analyzer capacity is assigned, if available.

- Dynamic assignment enabled only for analyzer access:

  Analyzer access is assigned, if available, otherwise analyzer capacity is assigned, if available.

- Dynamic assignment disabled for both professional and analyzer access:

  Analyzer capacity access is assigned, if available.

You can upgrade from analyzer access to professional access, but not downgrade from professional to analyzer.

If you change to a new license key, all your assignments are removed, because they are associated with the license, not the tenant. However, if you start using the old license key again, the assignments will be present.

4 Managing tenant admins

Tenant admins are administered from the management console on the **Users** page.

The users page displays all the users that have logged into the tenant. If a user has a certain role (tenant admin and developer), it is displayed in the roles field.

Use search for the fields **Name**, **User ID**, and **Email**. The IdP subject field can be used for distinguishing one user from another if the names are identical and the email field is not visible. For each user in the table, you have a button to the far right where you can assign and remove the tenant admin role, and activate or disable users. If you have the invite users license, you also have options for resending or deleting user invitations.

4.1 Assign tenant admin

A tenant admin can assign the tenant admin role to other users.

Do the following:

1. In the management console, go to the **Users** section and select a name from the list.
2. Click the **Assign tenant admin** button.
3. Confirm the role assignment.

4.2 Remove tenant admin

A tenant admin can remove the tenant admin role from other users.

Tenant admins cannot remove the tenant admin role from themselves.

Do the following:

1. In the management console, go to the **Users** section and select a name from the list.
2. Click the **Remove tenant admin** button.
3. Confirm the role removal.

5 Working in shared spaces

A shared space is a section of the cloud hub used to develop apps collaboratively and control access to apps. You can find your shared spaces using the spaces drop-down in **Explore.**

Any user with a professional license can create a space. Apps within a space can have sheets, stories, and bookmarks added to them by multiple users. Shared spaces are restricted to the members. Apps in the space can only be viewed by space members.

Permissions are assigned to members when they are added to a shared space. Permissions define what members can do in the shared space. There are four permissions in shared spaces:

- **Owner**: You are the first administrator that can manage the space and its members as well as create content in the space.
- **Is admin**: You can manage the space and its members as well as create content in the space.
- **Can edit**: You can add and edit content in apps. You cannot manage the space and its membership.
- **Can view**: You can view apps in the space, but cannot create content or manage the space.

Member permissions can be changed, giving them a different role in the space or removing them from the space.

You can create new apps directly in a shared space. You can also move apps from your personal space to your shared space so other members can work on them.

5.1 Creating shared spaces

A space's owner is the user who created the space. The owner of a space cannot be changed in the cloud hub. Space owners can be changed in the Management Console.

Space names must be unique within a cloud hub.

Do the following:

1. Click the spaces drop-down and select **Add a space**.
2. Enter a name for the space and a description for the space.
3. Click **Create**.

5.2 Adding members to shared spaces

Members can be added to the space by the owner or members with **Is admin** permission. If your tenant administrator has enabled groups, you can also add groups of members to your space.

If a member has individual permission and group permission in a space, the highest permission level is applied.

Do the following:

1. In the space, click and then **Manage members**.
   In Qlik Sense Enterprise on Kubernetes, click **Manage members**.
2. Search for members by name and select the members you want to add to the space.
3. Select a permission for the members and click **Add members**.
4. Click **Done**.

5.3 Editing the names and descriptions of shared spaces

You can change the name and description of the space.

Do the following:

1. In the space,click and then **Edit spaces**.
   In Qlik Sense Enterprise on Kubernetes, click the **Edit spaces** icon.
2. Change the name and description and click **Save**.

5.4 Deleting shared spaces

You can delete a space. Only the owner or a user with **Is admin** permission can delete a space.

1. In the space, click and then **Edit spaces**.
   Qlik Sense Enterprise on Kubernetes click the **Edit spaces** icon.
2. Click **Delete**.
3. Click **Delete**.

5.5 Developing and sharing apps with shared spaces

There are different ways of developing apps collaboratively and sharing them with other members of your cloud hub. Here is a sample workflow for using shared spaces:

Create an app

Create an app in your personal space. Add data sources, create a data model, and create scheduled reloads for the app.
The creator of an app is the only user who can manage the data in an app, so the data model must be complete before the app can be collaboratively developed with other users.

Create a shared space

Add a shared space to your cloud hub for collaborative development of your app.

Move your app to the space
: Once the app is ready for collaboration, move your app to your shared space.
Using apps in shared spaces (page 18)

Add users to the space
: Add collaborators to your space and assign them **Can edit** permission. Collaborators must have a professional license.

Develop apps in the space collaboratively
: All **Can edit** users can add sheets, stories, and bookmarks to the app. Their content is private until they chose to make it public in the app.
Granting access to sheets, bookmarks, and stories

Update your app
: You may receive feedback from your app audience. An app in a space can be updated at any time with changes to the data model or content in the app.

Retire an app from the shared space
: When the app is no longer required, you can delete it from the cloud hub.

Retire the space
: When the space is no longer required, you can delete it from the cloud hub.

5.6 Using apps in shared spaces

Apps can be created, developed, and shared with other members of the cloud hub in a shared space.

Apps can be created and developed in a similar way to how apps are created and shared in a personal space. Depending on your space permissions and your license, you can create and develop apps in the space. If you have **Can view** permission, you can only view the apps in the space.

Creating apps in a shared space

Users can create or upload apps in a shared space by clicking **Create** and selecting **Create app** or **Upload app**. You cannot duplicate apps to a space, but you can move apps to a space.

Tags you add to an app are shared with other members of the cloud hub, but only if they have access to your app.

Data connections and data files can be created, modified, and deleted by users with **Can edit** permissions in a shared space.

Users with **Can edit** permission can read, write, and load data connections and load scripts in **Data manager** or **Data load editor**. They can also create data connections to external sources and load data from those connections.

You can create on-demand selection apps in a shared space. Selection apps and template apps must be in the same space. For more information, see Creating an on-demand selection app.

Adding content to apps in shared spaces

Users with **Can edit** or **Is admin** permissions can add sheets, stories, and bookmarks to apps in the shared space. Sheets, stories, and bookmarks added to the app are private. Only the creator of the private content can see it in the app. When they are ready to be shared, the creator makes them public.

Only the space owner can edit data in the app, but other shared space members can create, edit, and delete:

- Master items
- Variables
- Media library content

Snapshots taken for stories are not shared with other users.

Shared space members with **Owner**, **Can edit**, or **Is admin** permissions can modify the following app properties:

- Selected theme
- Enable right-to-left reading order
- Setting a bookmark as app default
- Sheet title styling

Reloading apps in a shared space

Users with **Owner**, **Is admin**, and **Can edit** permissions can manually reload apps and create scheduled reloads in the space.

Moving apps between spaces

You can move apps between shared spaces as well as between a shared space and a personal space.

If you create an app in a shared space, the data connections related to it will stay in that space, even if the app moves. For example, you create an app called *QuarterlyAnalysis* in the Data Team shared space. If you move *QuarterlyAnalysis* to a different shared space, the data connections will remain in the Data Team shared space. If the data needs to be edited or reloaded, it must be done by a user with **Can edit** rights in the Data Team shared space. The same would apply if you created an app in a personal space and moved it to a shared or space.

Do the following:

1. Click on the app and select **Move**.
2. Select the new space from **Space**.

3. To open the new space, select **Navigate to space**.
4. Click **Move**.

Duplicating apps in a shared space

You can duplicate apps in a shared space.

If an app uses section access for data, you cannot duplicate the app.

Do the following:

- Click on the app and select **Duplicate**.

Exporting apps from shared spaces

You can export an app from a shared space as a .qvf file. Exported apps do not include any private sheets in the app.

If an app uses section access for data, you cannot export the app.

Do the following:

- Click on the app and select **Export with data** or **Export without data**.

Sharing apps from shared spaces

You can add members to a space and give them **Can view** permission so they can view the apps in a space. You cannot share individual apps from a space. If you do not want to share a space with viewers, you can move the app to a space you have created for app viewers.

5.7 Managing spaces in the management console

Spaces are managed in the management console on the **Spaces** page.

The spaces page has two tabs:

- **Overview** shows the current number of shared and managed spaces, and the creation date of the latest space.
- **Spaces** shows a table with space name, space type, space owner, description of the space, and the space creation date. You also have buttons for deleting a space, changing the owner, editing the space, and creating a new space.

The following are the space types:

- Personal spaces: In personal spaces, only the owner can edit apps, that is, you cannot co-develop in personal spaces. You can share apps outside your space, but only for viewing.

- Shared spaces: Shared spaces allow for easy co-development of apps within a closed group of users. What actions you can perform with an app in a space is determined by permissions and your license. With a professional license you can create a shared space in the hub. You can then add new members to your shared space and assign them permissions.
- Managed spaces: Managed spaces enable governed access to apps. Managed spaces are restricted to members. Permissions are assigned to members when they are added to a managed space. Permissions define what members can access in a space. Apps that you develop in a personal or shared space can be published to a managed space. Only space owners and target app consumers can open apps in a managed space. Other users can open apps if they have viewing permissions. Managed spaces can only be created by tenant administrators.

Changing the owner of a space

Do the following:

1. Select the spaces for which you want to change owner.
2. Click **Change owner**.
   A dialog is displayed.
3. Search for a user who will be the new owner.
4. Click **Apply**.

6 Managing reload schedules

With scheduling, you can view and delete reload schedules for apps in your system. From the hub users can edit existing and create new reload schedules.

6.1 Reloading app data in the management console

Apps in the cloud hub do not automatically update when their data sources are updated. Reloading an app updates it with the latest data from the app data sources. From the cloud hub, you can manually reload your apps or schedule reloads for your apps.

In addition to this, tenant admins can view and delete reload schedules from the management console. This is done on the **Schedules** tab.

Viewing a reload schedule

Tenant admins can view existing reload schedules from the management console. Select the reload schedule from the list and then click **View**.

Deleting a reload schedule

Do the following:

1. Select the reload task you want to remove and then click **Delete**.

   You can remove several items at a time.

2. Confirm that you want to delete the reload task.

6.2 Reloading app data in the cloud hub

Apps in the cloud hub do not automatically update when their data sources are updated. Reloading an app updates it with the latest data from the app data sources. You can manually reload your apps or schedule reloads for your apps.

You cannot reload data in the cloud hub for apps published to the cloud hub from a Qlik Sense Enterprise deployment. Apps published from Qlik Sense Enterprise can be reloaded using the QMC in Qlik Sense Enterprise.

You can only reload apps you own.

You can view the status of current and past reloads for an app from **Reload history** in **Details**.

Scheduling reloading app data

You can create a schedule for data reloading in your app. Qlik Sense adds a reload to the reload queue at the frequency, date, and time you schedule. You can schedule a single reload of the data or schedule a repeating reload of app data.

When you schedule a single reload, you can pick a specific date and time for the reload. When you schedule a repeating reload, you can pick the interval and time of the reload. Repeating reloads can be set at the following intervals:

- Hourly
- Daily
- Weekly
- Monthly
- Yearly

You can remove a scheduled reload from an app by setting the schedule to **Inactive** and saving.

The dates and times in the schedule reload dialog use your current time zone. Qlik Sense determines your current time zone based on your browser settings.

Do the following:

1. Click on the app and select **Schedule reload**.
2. Set the schedule to active and create your schedule.

   If you cannot see the AM option when setting the reload time, use the scroll bar.
3. Click **Save**.

Manually reloading app data

You can reload an app manually, adding a reload task to the reload queue.

Do the following:

- Click on the app and select **Reload**.

Viewing reload history for your app

Reload history contains the reload history for the selected app. You can view the status, start and end times, and duration of past and current reloads. For failed reloads, you can also view error logs.

To view the reload history for an app, click on the app, select **Details**, and click **Reload history**.

7 Managing events

Events are managed in the management console on the **Events** page.

On the events page, you can follow up on events in your system and get information about the event type and the user who initiated the event.

Property	Description
Date	Date and time in UTC format.
Source	Source of the event information. See examples.
Event type	Type of event. See examples.
User	User initiating the event. If the user name cannot be displayed, the user ID is displayed instead. Click the arrow to the far right to display additional information from the source or event.

In the table, sort by using the arrows in the properties header and filter by using the funnel. There are buttons for refreshing and resetting after filtering.

Examples of sources:

- `com.qlik/licenses`
- `com.qlik/engine`
- `com.qlik/edge-auth`

Examples of events:

- `app.created`
- `user-session.begin`
- `assignment.added`
- `assignment.revoked`

7 Managing generic links

If you are a tenant admin, you can create and edit generic links from the hub or the management console. The following procedures describe how to create, edit, and delete generic links in the management console. You can either create a single link or upload a CSV file with one or more links.

Qlik Sense only supports UTF-8 encoding for generic link CSV files.

In the Management console, generic links are administered on the **Generic links** page.

7.1 Generic links overview

If you have a multi-cloud deployment consisting of QlikView or Qlik Sense Enterprise on Windows in combination with Qlik Sense Enterprise SaaS or Qlik Sense Enterprise on Kubernetes, generic links offer an easy way to make on-premise apps available in the cloud. A tenant admin can add generic links from the hub, and from the management console. The linked apps are presented in the same way as the native apps, but they are opened in their respective environments.

Currently, only app links can be uploaded, and a link can only be uploaded to one space. However, a space can have more than one link.

You can upload a CSV file to add several links at the same time.

The following properties are present:

Property	Description
Name	Name of the app. This field is required when uploading a CSV file.
Type	Type of app: QlikView, Qlik Sense, or Other.
URL	URL to the app. This field is required when uploading a CSV file.
Space	Name of the space where the app is added.
Description	Description of the app.

7.2 Creating a single generic link

Do the following:

1. In the management console, open the **Generic links** section.
2. In the top right corner, click **Create new**.
3. Enter name, URL, description (optional), and type, and select a space.

7.3 Editing a generic link

Do the following:

1. In the management console, open the **Generic links** section.
2. To the far right on the row you want to edit, click **...** and select **Edit**.
3. Make your edits. **Type** cannot be edited.

*To edit multiple links, select the check boxes for the links to delete and click **Edit**.*

7.4 Uploading a CSV file with one or several generic links

Do the following:

1. In the management console, open the **Generic links** section.
2. In the top right corner, click **Upload CSV file** and add your CSV file.
   Name and *URL* are required fields and must be present in the CSV file.

7.5 Deleting a generic link

Do the following:

1. In the management console, open the **Generic links** section.
2. To the far right on the row you want to edit, click **...** and select **Delete**.

*To delete multiple links, select the check boxes for the links to delete and click **Delete**.*

7 Managing apps

If you are a tenant admin, you can move apps between managed spaces, move apps between self-managed (personal or shared) spaces, change owner of apps, and delete apps.

7.6 Apps overview

The **Apps** page in the management console consists of tabs for the following types of apps: **Self-managed**, **Managed**, and **Staged**.

Self-managed apps

Self-managed apps are apps that are in personal or shared spaces. As a tenant admin, you can perform the following actions on self-managed apps:

- Delete
- Change space
- Change owner

Managed apps

Managed apps are apps that are in managed spaces. As a tenant admin, you can perform the following actions on managed apps:

- Delete
- Change space

Staged apps

Staged apps are apps that does not have an owner and does not belong to a space. Staged apps are not visible in the hub. As a tenant admin, you can perform the following actions on staged apps:

- Delete
- Set space

7.7 Changing owner of an app

As a tenant admin, you can change owner of a self-managed app.

Do the following:

1. In the management console, on the **Self-managed** tab of the **Apps** page, select one or more apps.
2. In the top right corner, click **Change owner**.
3. In the Change owner dialog, select the user to whom you want to assign ownership of the app. Click **Apply**.

7.8 Changing space of an app

As a tenant admin, you can change the space that an app belongs to.

Do the following:

1. In the management console, on either of the **Self-managed** or **Managed** tabs of the **Apps** page, select one or more apps.
2. In the top right corner, click **Change space**.
3. In the Change space dialog, select the space to which you want to move the app. Click **Apply**.

> *If you are changing the space of an app, you might need elevated privileges. If you do, select the **Get elevated privileges** check-box before clicking **Apply**.*
> *Elevated privileges are needed if you are not the owner of the app or if you do not have Can manage permission for the space the app is moved from or moved to. The elevated privileges are restored as soon as the change space action has been performed.*

7.9 Setting the space for an app

As a tenant admin, you can set the space for staged apps.

Do the following:

1. In the management console, on the **Staged** tab of the **Apps** page, select one or more apps.
2. In the top right corner, click **Set space**.
3. In the Change space dialog, select the space to which you want to add the app. Click **Apply**.

7.10 Deleting an app

As a tenant admin, you can delete apps.

Do the following:

1. In the management console, on any of the tabs of the **Apps** page, select one or more apps.
2. In the top right corner, click **Delete**.

8 Managing extensions

Extensions are managed in the management console on the **Extensions** page.

Extensions that contain resource requests to external resources must have its origins whitelisted in the Content Security Policy, else the extension will be blocked from rendering.

We recommend reviewing extensions and their code before uploading. See Visualization extensions for more information.

8.1 Extensions overview

In the **Extensions** page of the management console, the following properties are shown.

Property	Description
Name	This is the metadata name contained in the QEXT file, which is different from the QEXT filename.
Description	Short description of the extension.
Tags	Tags for filtering.
Author	Creator of the extension.
QEXT filename	Identifier that must be unique. Filename of the extension definition file. Different from the name of the extension.
QEXT version	Metadata version contained in the QEXT file.
Published	Date of publishing.

In the table, sort by using the arrows in the properties header. Filter by using the **Tags** drop-down menu, or by selecting the tags in the table.

Extensions with external resources

Extensions that contain resource requests to external resources must have its origins whitelisted in the Content Security Policy, else the extension will be blocked from rendering.

Microsoft Internet Explorer 11 does not support Content Security Policy. Extensions, themes and maps that uses external resources will be blocked when using that browser due to this limitation in Microsoft Internet Explorer 11.

Unsupported file formats

Maximum size of a file within an extension folder is 250 MB.

Due to security, extensions are not allowed to contain files with disallowed MIME types. Upload will fail if your extension for example contains a executable file or a zip file. The following MIME types are disallowed:

- 'application/octet-stream'
- 'application/x-coredump'
- 'application/x-dosexec'
- 'application/x-executable'
- 'application/x-java-applet'
- 'application/x-object'
- 'application/x-sharedlib'
- 'application/zip'
- 'text/x-shellscript'
- 'text/x-awk'
- 'text/x-gawk'
- 'text/x-msdos-batch'
- 'text/x-nawk'
- 'text/x-php'

All files in an extension must have a file name and a file extension. Files that are not complying to this will be ignored. Examples of ignored files: `.gitignore` *and* `README`.

8.2 Adding a new extension

Do the following:

1. In the management console, go to the **Extensions** section and click **Add** in upper the right-hand corner.
2. In the pop-up, click **Browse** to select an extension file, or drop a file in the designated area.

   You cannot upload an extension with the same QEXT filename as an existing one.
3. Optionally, add tags.
4. Click **Publish**.
5. If the extension you just uploaded contain external resources, you need to whitelist the origins in the Content Security Policy.

8.3 Editing an extension

You can edit one extension at a time.

Do the following:

1. To the left in the table, select the check box for the extension you want to edit.
2. In the upper the right-hand corner, click **Edit**.
   The editing panel is displayed with options for replacing the existing extension and adding or removing tags.
3. Make your edits and save.

8.4 Deleting an extension

Do the following:

1. To the left in the table, select the check boxes for the extensions you want to delete.
2. In the upper the right-hand corner, click **Delete**.

Deletion of extensions can affect all resources. All users within a tenant are affected by a deletion.

9 Managing themes

Themes are managed in the management console, on the **Themes** page.

9.1 Themes overview

The following properties are present.

Property	Description
Name	This is the metadata name contained in the QEXT file, which is different from the QEXT filename.
Description	Short description of the theme or extension.
Tags	Tags for filtering.
Author	Creator of the theme or extension.
QEXT filename	Identifier that must be unique. Filename of the theme or extension definition file. Different from the name of the theme or extension.
QEXT version	Metadata version contained in the QEXT file.
Published	Date of publishing.
Updated	Date of last update.

In the table, sort by using the arrows in the properties header. Filter by using the **Tags** drop-down menu, or by selecting the tags in the table.

Themes with external resources

Themes that contain links to external resources must have its origins whitelisted in the Content Security Policy.

Microsoft Internet Explorer 11 does not support Content Security Policy. Extensions, themes and maps that uses external resources will be blocked when using that browser due to this limitation in Microsoft Internet Explorer 11.

Supported file formats and size

Themes only support HTML files, CSS, JSON, and images (PNG, JPEG, GIF, and SVG), along with QEXT metadata files and font files.

Maximum size of a file within a theme folder is 250 MB.

Uploading of themes that contain files with the following disallowed MIME types will fail:

- 'application/octet-stream'
- 'application/x-coredump'
- 'application/x-dosexec'
- 'application/x-executable'
- 'application/x-java-applet'
- 'application/x-object'
- 'application/x-sharedlib'
- 'application/zip'
- 'text/x-shellscript'
- 'text/x-awk'
- 'text/x-gawk'
- 'text/x-msdos-batch'
- 'text/x-nawk'
- 'text/x-php'

All files in a theme must have a file name and a file extension. Files that are not complying to this will be ignored. Examples of ignored files: `.gitignore` *and* `README`.

9.2 Adding a new theme

Do the following:

1. In the management console, go to the **Themes** section and Click **Add** in upper the right-hand corner.
2. In the pop-up, click **Browse** to select a theme file, or drop a file in the designated area.

   You cannot upload a theme with the same QEXT filename as an existing one.
3. Optionally, add tags.
4. Click **Publish**.
5. If the theme you just uploaded contain external resources, you need to whitelist the origins in the Content Security Policy.

9.3 Editing a theme

You can edit one theme at a time.

Do the following:

1. In the management console, go to the **Themes** section and select the check box for the theme you want to edit.
2. In the upper the right-hand corner, click **Edit**.

The editing panel is displayed with options for replacing the existing theme and adding or removing tags.

3. Make your edits and save.

9.4 Deleting a theme

Do the following:

1. In the management console, go to the **Themes** section and select the check boxes for the themes you want to delete.
2. In the upper the right-hand corner, click **Delete**.

Deletion of themes can affect all resources. All users within a tenant are affected by a deletion.

9 Managing Content Security Policy

SaaS editions of Qlik Sense utilizes Content Security Policy (CSP) Level 2, which provides an extra layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement to distribution of malware.

In Qlik Sense Enterprise, CSP allows tenant admins to control resources an extension or a theme is allowed to load for a given page. With a few exceptions, policies mostly involve specifying server origins and script endpoints. If an extension or theme contain resource requests to external resources, these must have its origins whitelisted in the Content Security Policy.

Microsoft Internet Explorer 11 does not support Content Security Policy. Extensions, themes and maps that uses external resources will be blocked when using that browser due to this limitation in Microsoft Internet Explorer 11.

To manage content security policies in the management console, navigate to the **Content Security Policy** page.

For more information, see MDN Web Docs: Content Security Policy (CSP).

9.5 Content Security Policy overview

In the **Content Security Policy** page of the management console, the following properties are shown:

Property	Description
Name	Name of the content security policy entry.
Origin	Domain origin to whitelist.
Directive	Directive applicable to the origin.
Last updated	Displays when the entry was last updated.
Date created	Displays when the entry was created.

Directives

The directives control locations from which certain resource types may be loaded. The following directives are supported in Qlik Sense Enterprise:

Directive	Description
child-src	Defines the valid sources for web workers and nested browsing contexts loaded using elements such as `<frame>` and `<iframe>`.

	*If you wish to regulate nested browsing contexts and workers, use the **`frame-src`** and **`worker-src`** directives, respectively.*
form-action	Restricts the URLs which can be used as the target of a form submissions from a given context.
media-src	Specifies valid sources for loading media using the `<audio>`, `<video>` and `<track>` elements.
style-src	Specifies valid sources for stylesheets.
connect-src	Restricts the URLs which can be loaded using script interfaces.
frame-src	Specifies valid sources for nested browsing contexts loading using elements such as `<frame>` and `<iframe>`.
frame-ancestors	Specifies valid sources for embedding the resource using `<frame>`, `<iframe>`, `<object>`, `<embed>` and `<applet>`.
object-src	Specifies valid sources for the `<object>`, `<embed>`, and `<applet>` elements.
	*Elements controlled by **`object-src`** are perhaps coincidentally considered legacy HTML elements and are not recieving new standardized features (such as the security attributes sandbox or allow for `<iframe>`). Therefore it is recommended to restrict this fetch-directive (for example explicitly set **`object-src 'none'`** if possible).*
worker-src	Specifies valid sources for `Worker`, `SharedWorker`, or `ServiceWorker` scripts.
font-src	Specifies valid sources for fonts loaded using `@font-face`.
image-src	Specifies valid sources of images and favicons.
script-src	Specifies valid sources for JavaScript.

Content Security Policy entries and header length considerations

The maximum number of Content Security Policy entries allowed per tenant is 256. If you receive an error message for exceeding the number of allowed Content Security Policy entries, you can remove redundant Content Security Policy entries and then add your new Content Security Policy entry.

The maximum length of the Content Security Policy header is 2048 characters. If you receive an error message for exceeding the Content Security Policy header length when adding a new Content Security Policy entry, you can remove redundant Content Security Policy entries and then add your new Content Security Policy entry.

The maximum number of characters allowed in the CSP header default value and the maximum number of CSP entries allowed per tenant default value are built-in and cannot be changed in Qlik Sense Enterprise SaaS.

9.6 Creating a Content Security Policy entry

Maximum 256 Content Security Policy entries are allowed per tenant.

Do the following:

1. In the management console, go to the **Content Security Policy** section and Click **Add** in upper the right-hand corner.
2. In the dialog, give the Content Security Policy a name.
3. Type the address of the origin in the following format: *domain.com*.
   Qlik Sense enforces HTTPS.
4. Select the directive applicable for the origin.

   You can add several directives.

5. Click **Add**.

Users who are using the client when a Content Security Policy is created or edited need to refresh their browser for the changes to take effect.

9.7 Editing a Content Security Policy entry

Do the following:

1. In the management console, go to the **Content Security Policy** section and select the CSP entry you want to edit and then click **Edit**.
2. In the dialog, change the CSP entry options as wanted.
3. Click **Save**.

Users who are using the client when a Content Security Policy is created or edited need to refresh their browser for the changes to take effect.

9.8 Deleting a Content Security Policy entry

Do the following:

1. In the management console, go to the **Content Security Policy** section and select the CSP entry you want to remove and then click **Delete**.

   You can remove several items at a time.

2. Confirm that you want to delete the CSP entry.

9.9 Copying the Content Security Policy header

Maximum 2048 characters are allowed in the Content Security Policy header.

Do the following:

1. In the management console, go to the **Content Security Policy** section and click **View header**.
2. In the dialog, click **Copy to clipboard**.
3. Click **Done**.

9 Managing API keys

An API key is a unique identifier used for authentication of a user, developer, or calling program to an API. API keys are often used for tracking and controlling how the interface is used, to prevent abuse of the API.

9.10 API keys overview

By default, the API keys are disabled in the management console. To enable the API keys, go to the **Settings** section. A tenant admin can revoke API keys and edit the API keys settings, but to generate or delete API keys, you must have the role *developer*. A tenant admin assigns the role *developer* to a user. If you are a tenant admin, you can assign the role developer to yourself.

The API keys table shows the following information about the API keys: name, ID, owner, last update, creation date, expiry date, and status. Use the search field to search in the first three fields: **Key name**, **Key ID**, and **Owner**.

API key statuses

API keys can have the following statuses:

- Active: the API key is in use.
- Expired: the expiry date has been reached.
- Revoked: the API key has been revoked and can no longer be used.

As an admin, you can review the API key activities registered in the **Events** section in the management console. If suspicious activities are detected, such as, extensive use of a certain API key, you can revoke that API key. Open the detailed list by clicking the arrow to the far right in the table and copy the ID of the API key. You can then search for the ID in the **API keys** section to find the API key to revoke.

To revoke a single API key, click the button **...** to the far right and select **Revoke**. You can only revoke keys with the status *Active*. To revoke multiple keys, select the check boxes to the left of the keys to revoke and click **Revoke** in the top right corner. Revocation is irreversible, a revoked API key cannot be re-activated.

In addition to revocation there is the delete option. You can delete an API key from the hub, but not in the management console.

9.11 Enabling API keys in the tenant

The setting **Enable API keys** is turned on in the management console on the **Settings** page. By default, the API keys are disabled in the management console.

Property	Description
Enable API keys	This switch enables or disables all the API keys in the tenant. Only the tenant admin can enable the API keys.

Change maximum token expiration	By changing the token expiration value, all new tokens will have the new expiration value. Already existing APIs will not be affected by the change, they will have the same expiration value as before.
Change maximum of API keys per user	This setting only affects new API keys. If a new API key makes the total number exceed the maximum number, creation is denied.

Do the following:

1. In the management console, go to the **Settings** page.
2. Under the **API keys** section, switch on the **Enable API keys** button.
3. If applicable, change the **Change maximum token expiration** and the **Change maximum of API keys per user** settings.

9.12 Generating an API key from the hub

You can generate API keys from the hub. Before you start, make sure that the following two requirements are fulfilled:

- The setting **Enable API keys** is turned on in the management console.
- The tenant admin has assigned the role *developer* to you.

Do the following:

1. Log onto your tenant, for example, *https://<tenantname>.com*.
2. Click your profile in the top right corner and select **Settings**.
3. Select **API keys**.
4. Click **Generate new API keys**.
5. Enter an API key description and select when the API key should expire.
6. Click **Generate**.
   An API key is generated.
7. Copy the API key and store it in a safe place.

After creation, you can edit the name of the API key. You can also delete it.

10 Managing web integrations

You can create web integrations to add origins that are whitelisted to access the tenant. The web integration containing the whitelist is connected to an ID used in for example a mashup that is connecting to your tenant. When a request arrives, Qlik Sense confirms that the request derives from a whitelisted domain and then approves the request, else not.

Web integrations are administered by tenant admins from the management console on the **Web** page.

10.1 Web integration overview

You can create web integrations to add origins that are whitelisted to access the tenant. The web integration containing the whitelist is connected to an ID used in for example a mashup that is connecting to your tenant. When a request arrives, Qlik Sense confirms that the request derives from a whitelisted domain and then approves the request, else not.

Click **...** to the far right to reach options for copying the ID, editing, or deleting the web integration.

Property	Description
Name	Name of the web integration.
ID	Unique ID assigned to the web integration when it is created.
Number of origins	Number of domains contained in the white-list.
Last updated	Displays when the web integration was last updated.
Date created	Displays when the web integration was created.

10.2 Creating a new web integration

Do the following:

1. In the management console, go to the **Web** section and click **Create new** in upper the right-hand corner.
2. In the dialog, give the web integration a name.
3. Type the address of the origin in the following format: *https://domain.com*. Then click **Add** to add the origin to the whitelist.

   You can add several origins.
4. Click **Create**.

10.3 Editing a web integration

Do the following:

1. In the management console, go to the **Web** section and select the web integration you want to edit and then click **Edit**.
2. In the dialog, change the web integration options as wanted.
3. Click **Save**.

10.4 Deleting a web integration

Do the following:

1. In the management console, go to the **Web** section and select the web integration you want to remove and then click **Delete**.

   You can remove several items at a time.

2. Confirm that you want to delete the web integration.

10.5 Copying a web integration ID for use in mashups

Do the following:

1. Select the web integration you want to copy the ID for, click **...** and then select **Copy ID**.

   The ID is copied to the clipboard.

10 Managing email sharing

Chart sharing lets Qlik Sense users share static Qlik Sense charts with anyone regardless of whether they are Qlik Sense users or not. When this feature is enabled, users have the option to send Qlik Sense charts to any email address.

Email settings and chart sharing are administered by tenant admins from the management console under **Configuration** > **Settings**.

10.6 Email server overview

In the **Email server** section of the **Settings** page in the management console, enter the outgoing email settings for sharing content via email.

Property	Description
Server Address (SMTP)	The server address (SMTP) from which to send email notifications.
Port	The port number for the email server.
Security	Select the appropriate security type. One of: • StartTLS • SSL/TLS • None
Sender email address	The email address the emails are sent from.
Password	The password of the email account.

10.7 Creating an email server

You must provide an email server from which emails are sent. You can use a dedicated email server or use an SMTP provider like G Suite or Office 365.

Do the following:

1. Enter the server address (SMTP) from which to send email notifications.
2. Enter the port number for the email server.
3. Chose the appropriate security type:
    - StartTLS
    - SSL/TLS
    - None
4. Enter the email address.
5. Enter the email password.

6. Click **Test** to check whether the SMTP settings are correct.
   When you click next, a window opens where you can enter an email address where you will receive a test email.
   If the email server is working, you should receive an email with the title: **Test email from Qlik Management Console**. The sender will be the email address you entered above.

*If you use one of the G Suite SMTP servers, you are required to enable **less secure apps** whenever OAuth is not used. Although Qlik authenticates over a secure communication channel, we use email address and password as authentication credentials.*

10.8 Email sharing

Tenant admins can allow users to share static charts with other users via email.

When **Chart sharing via email** is enabled, users can share a chart by right-clicking a chart and selecting **Share**. When this feature is disabled, the option is not visible to app users.

11 Managing on-demand app generation

On-demand apps are generated in the hub from navigation links that connect selection apps to template apps. The On-Demand App Service must be enabled in the management console to generate on-demand apps.

On-demand app generation is controlled by the On-Demand App Service. Tenant admins can enable the On-Demand App Service in the management console, on the **Settings** tab. The service is disabled by default and must be enabled before selection and template apps can be linked and on-demand apps generated.

When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps will be accepted nor will developers be able to create or edit new On-demand app navigation links. These capabilities are restored once the service is re-enabled.

11.1 Enabling and disabling on-demand app generation

To enable or disable on-demand app generation, in the management console navigate to the **Settings** page. In the **On-demand app generation (ODAG)** tab, manage the following setting:

Property	Description
On-demand app generation	When the service is switched from enabled to disabled, any pending requests to generate on-demand apps are allowed to finish. But once the service has been disabled, no new requests to generate apps are accepted. This service is disabled by default.
Dynamic views	Turn on dynamic views to allow app sheets to contain charts that are loaded from data sources on-demand. If you have apps whose sheets contain charts based on dynamic views and the **Dynamic views** setting is disabled for the tenant, the apps will continue to function with the following limitations: • All dynamic charts appear dimmed (and without data) to indicate that the dynamic view functionality has been disabled. • The sheet editor does not expose the dynamic view assets.

All charts and features not related to dynamic views will continue to function normally.

12 Enabling auto-creation of groups

Enable auto-creation of groups is enabled or disabled on in the management console on the **Settings** page.

Groups are used for access control of users, and can optionally be automatically created from *idp-groups*.

Property	Description
Enable auto-creation of groups	When enabled, groups are inherited from the identity provider so that access can be granted to the same groups of users that exist in the IdP. This simplifies access administration compared to granting access to one user at a time. It is required that you use single sign-on and have administrative access to your IdP to configure groups. Note that new IdP groups will show up in Qlik Sense Enterprise as users log in (or log in again) to the Qlik Sense Enterprise tenant. IdP groups are not imported all at the same time. Instead, IdP groups are discovered at login time. Further, only groups associated with users in Qlik Sense Enterprise will be available as described earlier.

13 Viewing logs in Qlik Sense Enterprise on Kubernetes

All services in Qlik Sense Enterprise on Kubernetes emit log data that can be used for debugging issues and activity. Logs can be read on demand or they can be collated and pushed to a log aggregation product for further analysis and use.

13.1 Viewing service logs

To inspect the recent logs of a service, for example to debug an issue, the Kubernetes CLI (or other Kubernetes management tools) can be used to quickly view log data.

The following assumes you have the **kubectl** tool installed and connected to your Kubernetes cluster.

Run the following to get a list of all the services running, this will also list if any services are reporting themselves as having issues.

```
Kubectl get pods
```

Identify the service you want to inspect the logs for from the list and run the following adjusting as needed.

```
Kubectl log qliksense-engine-xxxxxxx
```

This will render the recent log entries to the console in JSON format.

If a pod is not running, for example it is in a pending state, then it may not issue any log entries. You can use the following command to see what issue Kubernetes is reporting with that pods configuration:

```
kubectl describe pod qliksense-engine-XXXXX
```

There are two common reasons for a pod to not start:

- Wrong storage configuration - this will report issues about the availability of its volume claims.
- Insufficient resources - depending on the Kubernetes provider there can be insufficient resources or a limitation on how many pods can run on a node. In this instance it will report errors about pods being “unschedulable”

13.2 Collating and forwarding logs

The logs produced can be forwarded to be gathered, stored, searched and viewed all the system logs on mass in log aggregation tools.

Below is an example of using 3rd party tools including:

- Gathering your system logs in **fluentd**
- Storing your log files in **Elasticsearch**

> *Elasticsearch requires a significant amount of resources and is therefore not recommended to be executed on your local machine unless your Kubernetes cluster has a lot of available memory and CPU.*

- Consuming your log files in **Kibana**

13.3 Installing Elasticsearch

Elasticsearch is a search engine that provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

In this example we install a minimum setup of **Elasticsearch**, that does not include any persistence.

1. Create a file named **elasticsearch.yaml** to configure your installation preferences, and add the following:

```
image:
  tag: "6.1.4"

client:
  replicas: 1
  resources:
    limits:
      cpu: "0.5"
      memory: "1024Mi"  ## not setting a limit here can take down the cluster using all
available memory
    # requests:   # use defaults
    #   cpu: "25m"
    #   memory: "512Mi"

master:
  persistence:
    enabled: false
  replicas: 2
  # heapSize: "512m"    ## use default, should be less than request, MUST be less than limit
  resources:
    limits:
      cpu: "0.5"
      memory: "1024Mi"  ## set a limit
    # requests:   # use defaults
    #   cpu: "25m"
    #   memory: "512Mi"

data:
  persistence:
    enabled: false
  replicas: 1
  heapSize: "512m"
  resources:
    limits:
      cpu: "0.5"
```

```
      memory: "1024Mi"
    requests:
      cpu: "25m"
      memory: "512Mi"
```

2. Run the following command to install **Elasticsearch**:
   ```
   helm upgrade --install elasticsearch incubator/elasticsearch -f ./elasticsearch.yaml
   ```

13.4 Installing fluentd

Fluentd is an open source data collector for unified logging layer. It allows you to unify data collection and consumption for a better use and understanding of data. Follow these steps to install **fluentd**.

1. Create a file named **fluentd.yaml** to configure your installation preferences, and add the following:
   ```
   elasticsearch:
     host: elasticsearch-elasticsearch-client
   ```
2. Run the following command to install **fluentd**:
   ```
   helm upgrade --install fluentd incubator/fluentd-elasticsearch -f fluentd.yaml
   ```

13.5 Installing Kibana

Kibana lets you visualize your **Elasticsearch** data and navigate the Elastic Stack. You can use it to view and search your logs. Follow these steps to install **Kibana**.

1. Create a file named **kibana.yaml** to configure your installation preferences, and add the following:
   ```
   env:
     ELASTICSEARCH_URL: http://elasticsearch-elasticsearch-client:9200
   ```
2. Run the following command to install **Kibana**:
   ```
   helm upgrade --install kibana stable/kibana -f kibana.yaml
   ```

13.6 Accessing Kibana

Run the following command to access **Kibana**:

```
export POD_NAME=$(kubectl get pods --namespace default -l "app=kibana,release=kibana" -o jsonpath="
{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:5601 to access Kibana"
kubectl port-forward $POD_NAME 5601
```

In **Kibana** you can run the following query to test your setup:

```
kubernetes.container_name:engine
```

14 Monitoring metrics in Qlik Sense Enterprise on Kubernetes

All Qlik Sense Enterprise on Kubernetes services expose metrics that can be used to monitor activities, health and performance data.

The data can be surfaced and collated using open source components. The example below shows how to use Prometheus and Grafana to scrape and analyze metrics in real time.

14.1 Viewing metrics with Prometheus

Prometheus is a system monitoring and alerting toolkit that can be used for scraping and storing metrics. It collects metrics from configured targets at given intervals, evaluates rule expressions, displays the results, and can trigger alerts if some condition is observed to be true.

Prometheus finds the metrics by looking for Kubernetes annotations that have been added to the services.

```
prometheus.io/port=8080
prometheus.io/scrape=true
```

Installing the Prometheus chart

Run the following command to install the **stable/prometheus** chart.

Adjust the configuration of your cluster settings, such as RBAC.

```
helm upgrade --install prometheus stable/prometheus --
set=rbac.create=true,alertmanager.enabled=false,pushgateway.enabled=false
```

Viewing the metrics

View the metrics with the following command:

```
export POD_NAME=$(kubectl get pods --namespace default -l
"app=prometheus,release=prometheus,component=server" -o jsonpath="{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:9090 to access prometheus"
kubectl port-forward $POD_NAME 9090
```

14.2 Viewing metrics with Grafana

Grafana is another tool for monitoring and analyzing metrics.

Installing Grafana

Run the following command to install Grafana:

```
helm upgrade --install grafana stable/grafana -f grafana.yaml
```

The example YAML file referenced in the command above provides the following abilities:

- Configure Grafana to look at Prometheus metrics.
- Preload a GO Services dashboard for exposing Golang metrics.
- Preload a Kubernetes dashboard with general metrics.
- Preload a Kubernetes container details dashboard with more specific POD metrics.

See the Online help for full code example.

Viewing the metrics

Run the following command to retrieve your admin user password:

```
kubectl get secret --namespace default grafana -o jsonpath="{.data.admin-password}" | base64 --decode
; echo
```

In the same shell, run the following command to retrieve the Grafana URL:

```
export POD_NAME=$(kubectl get pods --namespace default -l "app=grafana,release=grafana" -o jsonpath="
{.items[0].metadata.name}")
echo "Visit http://127.0.0.1:3000 to access grafana"
export GRAFANA_PASSWORD=$(kubectl get secret --namespace default grafana -o jsonpath="{.data.admin-
password}" | base64 --decode ; echo)
echo "Login as admin:$GRAFANA_PASSWORD"
kubectl port-forward $POD_NAME 3000
```