Monitor Qlik Sense sites

Qlik Sense®
September 2018
Copyright © 1993-2018 QlikTech International AB. All rights reserved.

Copyright © 1993-2018 QlikTech International AB. All rights reserved.

Qlik®, QlikTech®, Qlik Sense®, QlikView®, Sense® and the Qlik logo are trademarks which have been registered in multiple countries or otherwise used as trademarks by QlikTech International AB. Other trademarks referenced herein are the trademarks of their respective owners.

Contents

1 About this document ... **6**

2 Monitoring a Qlik Sense site ... **7**

2.1 Monitoring apps ... 7

2.2 Configuring the Monitoring apps ... 7

Configuring single node environments ... 7

Configuring multi-node environments ... 8

Default virtual proxy with prefix ... 9

Importing the new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor ... 9

Customizing the apps ... 10

2.3 Starting the Monitoring apps from the QMC ... 10

2.4 Upgrading the Monitoring apps ... 10

Upgrading from Qlik Sense 3.2.x to Qlik Sense June 2017 ... 10

Upgrading from Synchronized persistence to Shared persistence ... 10

3 Operations Monitor ... **12**

3.1 Operations Monitor sheets ... 12

3.2 24-Hour Summary ... 13

Overview table ... 14

Last 24 Hours of Activity table ... 14

3.3 Performance ... 15

Performance measures ... 15

3.4 Task Overview ... 16

3.5 Task Planning ... 17

Tables ... 17

Reload Heatmap: Reload Count ... 17

Reload Heatmap: Reload CPU Spent ... 17

Task Chain: Paths ... 18

Task Chain: Median Reload Duration (Last 28 Days) ... 18

3.6 Task Details ... 18

Reload Summary Statistics ... 18

Reload Details ... 19

3.7 Session Overview ... 20

Bar charts and Combo chart ... 20

3.8 Session Details ... 20

Tables ... 21

App Session Summary ... 21

User Session Summary ... 21

Session Details ... 21

3.9 Export Overview ... 22

Tables ... 22

App Object Export Summary ... 22

User Export Summary ... 23

Export Details ... 23

3.10 QMC Change Log ... 23

Change Summary ... 24

Users making changes 24
Change details 25
3.11 Apps 25
Tables 25
App Owners 25
App Details 25
App Object Owners 25
App Object Details 25
3.12 Log Details 26
3.13 Operations Monitor assets panel 26
3.14 Analyzing operations data 27
Diagnosing reload task failures 27
Diagnosing slow system response 29
4 License Monitor 31
4.1 License Monitor sheets 31
4.2 Overview 32
KPIs (token-based license) 32
KPIs (user-based license) 32
Tables 33
Overview 33
Allocation Changes in Last 7 Days 34
Charts 34
User Timeline 34
4.3 User Detail 34
User License Session Summary 34
Denied Access 34
Unused Access 35
Sessions per User 35
Quarantined Access 35
4.4 Usage by App 35
Token Consumption by Stream > App 35
Token Consumption by Stream 35
Token Consumption by App 35
Token Consumption Timeline 35
4.5 Timeline 36
Token Consumption Timeline 36
Token Consumption by Month 36
First Time Access (New Users) 36
4.6 User Access History 36
4.7 Login Access History 37
Login access pass usage 37
Login access pass users 38
Access denied 38
4.8 Allocation History 38

License Allocation Change History ... 38
4.9 Log Details ... 39
4.10 License Monitor assets panel ... 40
4.11 Analyzing license data ... 41
Diagnosing login access overutilization ... 41
Scenario 1: Appropriate utilization ... 41
Scenario 2: Overutilization ... 41
User access underutilization ... 42
Scenario 1: Appropriate allocation ... 42
Scenario 2: Underutilization of user access ... 43
Diagnosing problems with login pass denials ... 43
A solution ... 44
5 Log Monitor ... 46
5.1 Importing the Log Monitor app to the Monitoring apps in the QMC ... 46
5.2 Log Monitor sheets ... 46
6 Reloads Monitor ... 48
6.1 Importing the Reloads Monitor app to the Monitoring apps in the QMC ... 48
6.2 Reloads Monitor sheets ... 48
7 Sessions Monitor ... 49
7.1 Importing the Sessions Monitor app to the Monitoring apps in the QMC ... 49
7.2 Sessions Monitor sheets ... 49
8 Troubleshooting - Monitoring a Qlik Sense site ... 50
8.1 The Monitoring apps are not backed up correctly ... 50
8.2 I have accidentally deleted the Monitoring apps ... 50
8.3 The Monitoring apps have become corrupted ... 51
8.4 Reload of the Monitoring apps failed ... 51
Insufficient administration rights in the QMC ... 51
Reload is performed on rim nodes ... 51
Message: “Error: Field not found…” ... 52
Message: “Error: Table 'tempDateTimeList' not found…” ... 52
Message: "Error: QVX_UNEXPECTED_END_OF_DATA..." ... 52
Customized proxy port ... 52
Changes made to the user account under which the Qlik Sense services are running ... 53
8.5 The Monitoring apps fail to reload in a multi-node environment ... 53
The central node is not a reload node ... 53
The repository database is on a separate machine ... 54
8.6 Operations Monitor App fails to reload after turning off database logging ... 54
8.7 Failed to connect to the QRS via the Qlik REST Connector ... 55

1 About this document

This guide documents the *Operations Monitor*, *License Monitor*, *Log Monitor*, *Sessions Monitor*, and *Reloads Monitor*, the apps used to monitor a Qlik Sense site. This document is derived from the online help for Qlik Sense. It is intended for those who want to read parts of the help offline or print pages easily, and does not include any additional information compared with the online help. Use the online help or the other documents to learn more.

The Monitoring apps are accessed from the QMC start page. The **Monitoring apps** link under **GOVERNANCE** in the navigation panel takes you to the **Monitoring apps** stream where you can start the individual apps.

The *Operations Monitor* app provides information about hardware utilization, such as server memory and CPU usage, active users, and reload task activity. It also provides summary and detailed information about errors, warnings, and log activities in the Qlik Sense server environment that can be used for troubleshooting.

The *License Monitor* app tracks license usage, and it facilitates monitoring changes to license allocation.

The *Log Monitor* app presents nearly all log data available and enables trend analysis and troubleshooting.

The *Sessions Monitor* app shows log data about usage of apps.

The *Reloads Monitor* app presents detailed information about reload data, both from the QMC and apps open in the hub.

The Monitoring apps provide historical status and trending data. Real-time status is provided by QMC management resources. Actions taken in response to issues revealed by the Monitoring apps are also performed in the QMC.

2 Monitoring a Qlik Sense site

2.1 Monitoring apps

The Qlik Management Console (QMC) provides apps for monitoring system performance and usage on Qlik Sense server nodes and for monitoring license usage.

The Monitoring apps are accessed from the QMC start page. The **Monitoring apps** link under **GOVERNANCE** in the navigation panel takes you to the **Monitoring apps** stream where you can start the individual apps.

The *Operations Monitor* app provides information about hardware utilization, such as server memory and CPU usage, active users, and reload task activity. It also provides summary and detailed information about errors, warnings, and log activities in the Qlik Sense server environment that can be used for troubleshooting.

The *License Monitor* app tracks license usage, and it facilitates monitoring changes to license allocation.

The *Log Monitor* app presents nearly all log data available and enables trend analysis and troubleshooting.

The *Sessions Monitor* app shows log data about usage of apps.

The *Reloads Monitor* app presents detailed information about reload data, both from the QMC and apps open in the hub.

The Monitoring apps provide historical status and trending data. Real-time status is provided by QMC management resources. Actions taken in response to issues revealed by the Monitoring apps are also performed in the QMC.

2.2 Configuring the Monitoring apps

All installations of Qlik Sense require some level of configuration of the Monitoring apps.

Configuring single node environments

Do the following:

1. Update the data connections *ArchivedLogFolder* by replacing *C:\ProgramData\Qlik\Sense* with the fully-qualified domain name (FQDN) path to the shared folder for Qlik Sense: *\\<FQDN>\<QlikShare>\ArchivedLogs*.
2. Update the `monitor_apps_REST_` data connections by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with the FQDN of the node where the repository resides.
3. If the virtual proxy uses a prefix, the `monitor_apps_REST_` data connections must be updated to include the prefix used.
   See: *Default virtual proxy with prefix (page 9)*

Data in the Operations Monitor and License Monitor is not live, it is updated when the apps are reloaded. Reload frequency can be changed by editing the triggers for the task.

Configuring multi-node environments

Do the following:

1. Update the data connections *ArchivedLogFolder* by replacing *C:\ProgramData\Qlik\Sense* with the fully-qualified domain name (FQDN) path to the shared folder for Qlik Sense: \\<*FQDN*>\<*QlikShare*>*ArchivedLogs*.
2. Update the data connections *ServerLogFolder*, by replacing *C:\ProgramData\Qlik\Sense\Log* with the FQDN path to the central node: \\<*FQDN*>\<*UNC_Share*>*Log*.
3. Update the `monitor_apps_REST_` data connections by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with the FQDN of the node where the central Qlik Sense repository service is running.
4. If the virtual proxy uses a prefix, the `monitor_apps_REST_` data connections must be updated to include the prefix used.
   See: *Default virtual proxy with prefix (page 9)*
5. If you are using centralized logging, you need to update the `QLogs` data connection by replacing *localhost* in the connection string URL with the FQDN of the machine where the centralized logging database resides.

   The centralized logging database may or may not be enabled and may or may not be in the same PostgreSQL database as the Qlik Sense Repository Database.
6. Share the Qlik Sense log folder on all RIM nodes.
7. Add a new data connection to the *Log* folder for each rim node. This can be accomplished by opening an app, accessing the data load editor, and creating a new data connection. If you have five RIM nodes, you need to create five data connections.
   For example, the data connection for RIM1 points to folder *rim_node_1*\<*UNC_Share*>*Log* and is called RIM1.
8. Rename the new data connections in the QMC to remove the *(username)*, which is appended to the data connection name. Example: *RIM1 (user_183)* is changed to *RIM1*.
9. Update the load script of the *Operations Monitor* in section *logFolderList* on line 5 by adding the names of all the new data connections created in step 7 and 8.
   Do the following:
   i. Duplicate the *Operations Monitor* app in the QMC.
   ii. Open the duplicate app in the Qlik Sense hub.
   iii. Edit the load script: Each new data connection name needs to be enclosed in single quotes (') and separated by a comma.
   Example: *FOR each node in 'ServerLogFolder','RIM1','RIM2'*.

iv. Save the app.

v. Replace the existing *Operations Monitor* app by publishing the duplicate app to the **Monitoring apps** stream and selecting **Replace existing app**.

10. Perform step 9 in the *License Monitor*.

If you encounter problems when the central node is not a reload node, see: The Monitoring apps fail to reload in a multi-node environment (page 53).

Default virtual proxy with prefix

For the *Operations Monitor* and *License Monitor* to reload correctly when the default virtual proxy uses a prefix, you need to manually add the prefix to the `qrs` data connections. The default URL is *https://<FQDN>/qrs/app/full*, where the FQDN refers to the node where the repository resides. If the virtual proxy prefix is "qlik", the URL needs to be as follows: *https://<FQDN>/qlik/qrs/app/full*.

The following data connections need to be updated:

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license_access`
- `monitor_apps_REST_license_login`
- `monitor_apps_REST_task`
- `monitor_apps_REST_user`
- `monitor_apps_REST_license_user`

Importing the new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor

The three new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor are not by default available in the QMC. You need to import them to make them appear in the QMC.

Do the following:

1. From the QMC start page, open **Apps**.
2. Click **Import** in the action bar.
3. Click **Choose File** and navigate to *%ProgramData%\Qlik\Sense\Repository\DefaultApps*
4. Select the app to import and click **Import**.
   The app is imported and can be published to the *Monitoring apps* stream.
5. Repeat steps 2-4 for the remaining apps.

Customizing the apps

It is possible to extend the Monitoring apps with visualizations you find useful in your particular environment. The Monitoring apps provide assets panels with the dimensions and measures they use. You can use those dimensions and measures to create customized visualizations on separate sheets that you can add to the apps.

The assets panels may also include extra visualizations that are not used on any of the apps' sheets, but which can be useful in a particular environment.

Operations Monitor assets panel (page 26)

License Monitor assets panel (page 40)

2.3 Starting the Monitoring apps from the QMC

The apps for operations and license monitoring are started by going to the QMC start page. The Monitoring apps are accessed from the **Monitoring apps** link under **GOVERNANCE** in the navigation panel.

Do the following:

1. Start the QMC.
2. Allocate user access to users who will use QMC apps or allocate login access to groups whose users can use apps with login passes.
3. Click the **Monitoring apps** link under **GOVERNANCE** in the navigation panel.
   This takes you to the **Monitoring apps** stream where you can start the individual apps.

*The first time the Monitoring apps are started, they may not contain data to display because they have not yet been reloaded. In the case of the License Monitor, it has no data until at least one license token has been allocated or an access denial has taken place, so it might display no data even if it has been reloaded. To get fresh data for the apps before their next scheduled reload, return to the Apps overview in the QMC and click **More actions > Reload now**.*

2.4 Upgrading the Monitoring apps

Upgrading from Qlik Sense 3.2.x to Qlik Sense June 2017

When you upgrade from Qlik Sense 3.2.x to June 2017, or later releases, eight new REST data connections are introduced (`monitor_app_REST_`). The existing `qrs_` data connections will no longer function due to functional changes to the REST connector. These `qrs_` data connections therefore can be removed.

Upgrading from Synchronized persistence to Shared persistence

If you upgrade from Synchronized persistence to Shared persistence, you may need to move the archived logs from the earlier version to the Shared persistence ArchivedLogs share.

Do the following:

1. Create a new folder called *OlderLogs* (or the name of your choice) in the Service Cluster *ArchivedLogs* folder. You can find this in QMC > Service cluster.
2. Move or copy the following subfolders from *Archived Logs* (in the older version) to this new *OlderLogs* folder in step 1.
    a. Default *Archived Logs* folder is *c:\programdata\qlik\sense\repository\archived logs*.
    b. Copy the following folders to the new location:
        i. Engine
        ii. Repository
        iii. Proxy
        iv. Scheduler
        v. Printing

    The reason to just move/copy these folders is that other log folders (like AppMigration and Script) are not loaded into the Monitoring apps and can be quite large in size.
3. Verify in the *ArchivedLogs* folder (for the service cluster) that this *OlderLogs* folder is present, as well as folders for each node in your environment.
4. Update the *ArchivedLogsFolder* data connection in QMC to point to the *ArchivedLogs* folder (as defined in QMC > ServiceCluster).
5. Versions prior to 7.x of the governance*.QVDs located in *c:\Programdata\Qlik\Sense\Log* can be removed if wanted (optional).
6. Reload the *new* Monitoring apps from the QMC.

3 Operations Monitor

The *Operations Monitor* loads service logs to populate charts covering performance history of hardware utilization, active users, app sessions, results of reload tasks, and errors and warnings. It also tracks changes made in the QMC that affect the *Operations Monitor*.

With the *Operations Monitor*, you can track system performance and investigate activity that might adversely affect it. For example, by analyzing reload tasks and sessions, you can find bottlenecks that might be alleviated by rescheduling reloads or redistributing sessions. Or you can use the **QMC Change Log** sheet to review changes that might explain changes in system performance.

3.1 Operations Monitor sheets

The *Operations Monitor* sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 8)*), the app includes information across all nodes.

24-hour Summary	Displays hardware utilization, active users, active apps, and reload tasks over the last twenty-four hours.
Performance	Allows the user to select a time period over which to display hardware utilization, concurrent users, and concurrent apps.
Task Overview	Provides a statistical overview of the success, duration, and failure of reload tasks.
Task Planning	Provides details about reload count, reload CPU spent, and task dependencies.
Task Details	Provides details about the success and failure of individual app reloads, including execution details about duration and start and end times.
Session Overview	Provides summary information about apps, app sessions, and app users over selected periods to show which users use which apps when.
Session Details	Provides details about individual user and app sessions, including number, average duration, days since last session, start and end times, reasons for ending sessions, and the type of client on which the app was run.
Export Overview	Provides summary information about apps, app objects, and app users to show which users export which app objects when.
Apps	Provides details about the apps in the Qlik Sense Repository Service (QRS), including name and ID of app objects, owners, publishing, and streams.
QMC Change Log	Displays changes made in the QMC that affect a range of factors from system performance to user access, including changes by QMC resource type, by specific QMC resources, by users who made changes, or by a type of action performed in the QMC.

Log Details	Provides details about reloads of the *Operations Monitor*, including the time of reloads, results, error messages and warnings, and log entries.

The *Operations Monitor* provides charts for the following:

- Server CPU
- Server RAM usage
- number of active users
- reload tasks statistics and execution details
- errors and warnings

It also reports the following:

- average and maximum RAM usage in the period
- average and maximum CPU usage in the period
- average and maximum number of active users in the period
- average and maximum number of active sessions in the period
- number of errors and warnings
- warnings and error entries
- number of reloads and their average and maximum duration
- number of reload failures
- reload task execution details

Data in the Operations Monitor is updated when the app is reloaded. Data is not live.

3.2 24-Hour Summary

The *24-hour Summary* provides an overview of system performance during the 24 hours prior to the latest reload. It displays hardware utilization, active users, active documents, task reloads, failures and average duration, user sessions, and errors and warnings over the last twenty-four hours on the current node.

Data comes from all nodes in a multi-node environment. The average and maximum usage is for all nodes combined.

Six KPI visualizations highlight important performance indicators, and each of the KPI visualizations link to sheets in the *Operations Monitor* that provide details about the indicator. The following list shows the KPI visualizations included, and the linked sheets for each KPI is shown in parentheses:

- Max CPU (Performance)
- Max RAM (Performance)
- Reloads and Failures (Task Overview)
- Avg Reload Duration and Max duration (Task Overview)

- Max Concurrent Users and Max Concurrent Apps (Session Overview)
- Errors and Warnings (Log Details)

Overview table

In addition, the *Overview* table provides columns with data for the previous 7-day and 28-day periods to compare to the column with the 24-hour values.

> *During the first 7 days, the 28-day average will probably show a higher daily average than the 7-day, because it calculates how many days have had activity, whereas the 7-day average always divides by seven, regardless the number of days that actually had activity during that 7-day period.*

The Overview table rows show the following:

Max CPU	Maximum CPU load on the QES process, given as a percentage.
Max RAM	Maximum virtual memory committed by the QES process, given in GB.
Max Concurrent Users	Maximum number of concurrently active users during the periods.
Max Concurrent Apps	Maximum number of apps running concurrently during the periods.
User Sessions	Total number of user sessions started during the periods.
Reloads	Count of reload tasks started during the periods.
Reload Failures	Count of reload tasks that failed to complete during the periods, either because they failed or were aborted.
Avg Reload Duration	Average length of time reload tasks took to complete during the periods.
Errors & Warnings	Total number of errors and warnings during the periods.

Last 24 Hours of Activity table

The Last 24 Hours table shows metrics by the hour for the last 24 hours:

- Maximum CPU
- Maximum RAM (in GB)
- Percent of RAM committed
- Concurrent apps
- Concurrent users
- Reloads
- Errors and warnings

3.3 Performance

The *Performance* sheet displays the history of hardware utilization, active users, and active documents on the current node over a period selected by the user. In a multi-node environment, data comes from all nodes, unless specific nodes have been selected. The average and maximum usage is for all nodes combined or all selected nodes. The user can select on months, weeks, dates, and days of the week. Selections can also be made by hour, ten-minute time period, and by hostname.

The performance charts and summary table can highlight periods of peak CPU and RAM usage and help identify concurrent events that might be contributing to the high usage. They can also help diagnose trends for concurrent users and apps that could contribute to periods of high activity that cause problems reflected in RAM or CPU usage.

Performance measures

The line charts contain different options for both measures and dimensions. By default, the dimensions are the drill-down Month > Date > Hour and Hostname, but both of these have the alternative dimensions Hour Timeline, Ten-Minute Timeline, and Five-Minute Timeline.

Chart name	Measure	Measure definition
Qlik SenseServer CPU	Max CPU	Maximum value in each hour of CPU load on the QES process and is given as a percentage. Threshold line at 90% provides visual cue to times when CPU usage approaches maximum usage.
	CPU Above 95%	Displays periods when CPU load has been above 95%.
	Average CPU	Averages the CPU load on the Qlik Sense Engine Service (QES) process by hour and is given as a percentage.
	CPU Spent (ms) on Apps	CPU time (in milliseconds) that was spent handling requests during the finished engine session. Hover over an arrow to show the value when the line is out of range.
Qlik SenseServer RAM	Average RAM	Average virtual memory committed by the Qlik Sense Engine Service process, given in Gigabytes.
	Max RAM	Maximum virtual memory committed by the QES process, given in Gigabytes. The Max Free line near the top of the chart shows the maximum amount of RAM that can be used by Qlik Sense.

Concurrent Users & Apps	Concurrent User	Number of active users in the QES at the given point in time.
	Concurrent Apps	Number of active apps in the QES at the given point in time.
	Max Active Doc Sessions	Maximum number of active doc sessions in the QES at the given point in time.

The *Performance Summary* pivot table at the bottom provides additional average and maximum values for the granular time period selected. The summary can be used to illuminate issues observed in the line charts. For example, are there hours during each day that exhibit high activity or load?

Date, Hostname	Dates selected are super headings for the table's columnar data headings. Hostnames are subheadings.
Measures	Measures are the subheadings (with calculated values), such as Max CPU, Max RAM, and Concurrent Users.
Hour, Ten-Minute Timeline, Five-Minute Timeline	The table rows are hourly data for the dates selected. Hourly rows can be expanded to display data by five-minute or ten-minute period.
Max CPU	Maximum CPU load for the selected period given as a percentage.
Max RAM (GB)	Average RAM load for the selected period in Gigabytes.
% RAM Committed	Percentage of available RAM that is committed to Qlik Sense and other processes.
Concurrent Apps	Number of active app sessions in the Qlik Sense Engine Service at the given point in time.
Concurrent Users	Number of active users at the given point in time.
Reloads	Number of reload tasks at the given point in time.
Errors & Warnings	Number of errors and warnings at the given point in time.
CPU Spent (ms) on Apps	CPU time that was spent handling requests during the finished engine session.

For additional details about engine performance, namely caching metrics, consider using the performance with cache chart or the cache metrics master item measures in the library.

3.4 Task Overview

The *Task Overview* sheet provides a summary view of reload task activity. KPI visualizations highlight reload totals, with failures, reloads per day and per hour, average duration of the reloads, with the maximum duration, and the number of reloads and reload failures the last 24 hours. Double-clicking any of the KPI visualizations opens the *Task Details* sheet.

The *Reload Count* horizontal stacked bar chart displays the number of successful and failed reload tasks, during the selected period, for the *License Monitor*, *Operations Monitor*, and all other apps. The stacked bars make it easy to identify reload tasks that experience a high failure rate.

Reloads by Hour also charts the number of reload tasks (successful, failed, and aborted) by hour of the days during the selected time period. The alternative dimension *Weekday* is available. The chart can be used to identify peak reload times as well as periods when the number of reloads is low and when perhaps more reloads could be executed.

A third chart, *Reload Count and Duration Trend*, displays reload totals and the average amount of time taken by reload tasks during the selected period. It can be used to identify reloads that are taking longer than expected or are increasing over time. Or are there some reloads that take longer than the average time to complete. Alternative measures and dimensions are available.

When a user reloads an unpublished app in the client (hub), this reload is not listed under the general "task reloads" statistics and information. It is logged as a Reload App entry. These client app reloads can be found in the Log Details sheet of the Operations Monitor by searching for "App Reload".

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

3.5 Task Planning

The *Task Planning* sheet contains two heatmaps (pivot tables) that enable users to drill into details about reload count and CPU spent during reload. The cell color indicates the level of activity during a period: the darker the color, the more activity.

The task chain tables show task paths, task chain depths, and the median reload duration for the last four weeks for each task in a task chain.

This sheet can be used to monitor and plan your reloads to avoid busy periods with high CPU workload. You can also identify reload times that are slower than expected.

Tables

Reload Heatmap: Reload Count

The *Reload Heatmap: Reload Count* table can help identify periods that are suitable for reloads. You can change the positions of the dimensions (Hour, Weekday, and Date) to get new views of the data.

Reload Heatmap: Reload CPU Spent

The *Reload Heatmap: Reload CPU Spent* table uses the same dimensions as *Reload Heatmap: Reload Count*, but presents the CPU workload instead of reload count. Normally, there should be some correspondence between the number of reloads and the CPU workload.

Task Chain: Paths

The *Task Chain: Paths* table shows the full task path for a reload together with the task depth. When you select a task path, the *Task Chain: Median Reload Duration (Last 28 Days)* displays the reload duration for all the tasks in the task chain.

Task Chain: Median Reload Duration (Last 28 Days)

The *Task Chain: Median Reload Duration (Last 28 Days)* table lists the Task Chain Total (the median reload duration during the last four weeks) for all tasks in a task chain (hh:mm:ss). The darker the cell color, the longer the duration. Long reload times may indicate issues with the reload (or high CPU workload). Compare with the Task Chain Total value to see if the value deviates considerably from the median value.

3.6 Task Details

The *Task Details* sheet contains two tables that enable users to drill into details about apps and their reload tasks. The filter panes allow users to specify periods by month, week, date, day of the week, hour, and reload duration.

In addition to time periods, reload tasks can be selected based on the following:

- Hostname of the system on which the reload tasks are run.
- Task type to isolate a specific type of tasks for analysis.
- User directory connector.
- Enabled tasks.
- Task name to isolate individual tasks for analysis.
- Reload status to analyze tasks according to results of their reloads: FinishedFailed, FinishedSuccess, and Aborted.
- App name to analyze the reload results of individual apps.

When a task is executed in the QMC, the reload is logged and displayed in the *Operations Monitor* statistics. When an unpublished app in the client (Hub) is reloaded, however, the reload task is not included in the reload statistics. Client app reloads can be found in the Log Details sheet by searching for “App Reload.”

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Reload Summary Statistics

The *Reload Summary Statistics* table can help identify tasks that have a high failure rate or take a long time to complete. You can also use it to identify tasks that have not been executed for a long time.

Task Name	Name of the reload task
App Name	Name of the app for which the task reloads data
Reloads	Count of reload start times

Reload Failures	Number of reloads that terminated with FinishedFail or Aborted
Failure Rate	Percentage of reload attempts ending in failure or abort
Avg Reload Duration	Average length of time reloads took to complete, either successfully or failing
Max Duration	Longest duration of a reload task
Last Reload	Time the last reload task started
Last Reload Failure	Time the last reload task failed
Next Execution	Time of the next reload task execution
Enabled	Task status
App ID	Unique ID of the app

Reload Details

The *Reload Details* table lists reload task status and details such as task name and duration. When tasks fail, you can examine details to see how long it took to fail and which other tasks were executing when it failed.

Task Name	The name of the reload task
App Name	The name of the app for which the task reloads data
Hostname	The name of the node to which the task execution details apply.
Reload Status	The result of the execution of the task. The status reported is “Success,” “Failed,.” and “Aborted.” All other status, such as skipped, is shown as “error code 65=finished failed.” *When Reload Status for an app is FinishedFail or Aborted, the Level of the message for the reload task on the Log Details sheet may be INFO instead of ERROR. The number of reload failures reported is, however, the same on both sheets.*
Start Time	The time when the execution of the task started.
End Time	The time when the execution of the task stopped.
Duration	The time (in seconds) for the execution of the task to be completed. Blank when the task terminates due to error or due to timing of the system monitor reload.
Message	The reason for the reload task failure. When the reload finishes successfully, the message can indicate the nature of the reload (for example, “Changing task state from Started to FinishedSuccess”).

3.7 Session Overview

The *Session Overview* sheet provides summary and detailed information (apps, app sessions, and their users over selected periods) to show which users use which apps when.

Four KPI visualizations highlight key data about users, apps, and sessions.

- Max Concurrent Users and Max Concurrent Apps
- Avg Session Duration and Avg Selections
- Users per Day and Users per Hour
- Apps Accessed per Day and Apps per Hour

Double-clicking any of the KPI visualizations opens the *Session Details* sheet.

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Bar charts and Combo chart

The following charts all contain alternative measures and three charts also have alternative dimensions.

Top 50 Apps	Displays the number of sessions each of the fifty most frequently used apps has run during a selected time period. The bar chart contains several alternative measures.
Top 50 Users	Displays the number of sessions each of the fifty most active users has run during a selected time period. When users have run multiple apps, each app's usage total is indicated in the stacked bars. The bar chart contains several alternative measures.
Sessions Over Time	Displays the session over time. You can drill down from weekday to Hour > Minute Drill. For example, when a month is selected, Sessions Over Timer displays the total session activity by hour during that month. It is not the average session activity by hour. The bar chart contains several alternative measures.
User and App Count Trend	Displays the total number of users and apps used over the selected period.

3.8 Session Details

The *Session Details* sheet provides detailed information (apps, app sessions, and their users over selected periods) to show which users use which apps when. The user can select on months, weeks, dates, days of the week, hours of the day, length of sessions, and session CPU spent.

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Tables

App Session Summary

Displays session activity by apps. The *App Session Summary* can be used to identify apps that have high session counts but low user counts and apps that have not been used recently.

App	Name of an app that has been used in at least one session.
Stream	Name of the stream, if any, that the app has been published to.
Users	Number of users who have started sessions with the app.
Sessions	Number of sessions started with the app.
Days Since Last Session	Number of days since the last session with the app.
Avg Session Duration	Average length of time for sessions with the app.
Avg CPU Spent (ms)	Average CPU time (in milliseconds) that was spent handling requests during the session.
Avg KB Transferred	Average amount of data (in KB) that was sent and received during the session.
Avg Selections	Average number of selections made in the app.
AppID	Unique ID of the app.

User Session Summary

Displays session activity by users. The *User Session Summary* can be used to identify users who are accessing a large number of apps. The table can also identify users who open apps for only very short sessions.

User	Directory from which the user started sessions.
User Name	Name of the user that started sessions.
Apps	Number of apps started by the user.
Sessions	Number of sessions started by the user.
Days Since Last Session	Number of days since the user last started a session.
Avg Session Duration	Average duration for sessions run by the user.
Avg Selections	Average number of selections made by the user.

Session Details

Displays details contained in *App Session Summary* and *User Session Summary* tables on a per session basis. This can help isolate apps or users that consistently show long duration or a high number of selections. Such session statistics can be used to evaluate app content and design.

Session Start	Date and time at which a session started.
Session Finish	Date and time at which the session finished.
User ID	ID of the user who started the session.
User Name	Name of the user who started the session.
App	Name of the app run in the session.
App Stream	Name of the stream where the app was published, or, if not published, value **Unpublished**.
Hostname	Name of the node to which the session details apply.
Duration	Length of time the session lasted.
Selections	Number of selections made in the app during the session.
CPU Spent (ms)	CPU time (in milliseconds) that was spent handling requests during the session.
KB Transferred	Amount of data (in KB) that was sent and received during the session.

3.9 Export Overview

The *Export Overview* sheet provides information (app object export summary, user export summary, and export details) to show which app objects that have been exported, and by whom. The user can select on months, weeks, dates, days of the week, hours of the day, and length of export.

In a multi-node environment, the data in the charts represents all nodes combined, unless specific nodes have been selected.

Tables

App Object Export Summary

Displays export activity by apps. The *App Object Export Summary* can be used to identify app objects that have high export counts but low user export counts, and apps that have long export duration.

App	Name of the app containing the exported app object.
Object Type	Type of app object exported.
Object	Name of the exported app object.
Output Format	The output format of the exported object.
Exports	Number of exports of the app object.
Users	Number of users that have exported the app object.
Avg Export Duration	Average length of time for export of the app object.

User Export Summary

Displays session activity by users. The *User Export Summary* can be used to identify users who are exporting a large number of app objects, and/or very small app objects.

User	The user who has exported the app objects.
User Name	Name of the user who has exported the app objects.
Apps	Number of apps exported by the user.
Exports	Number of exports by the user.
Average Export Duration	Average duration for exports run by the user.

Export Details

Displays details contained in *App Object Export Summary* and *User Export Summary* tables on a per export basis. This can help isolate app objects or users that consistently show long export duration, or a high number of selections. Such statistics can be used to evaluate app object content and design.

Start	Date and time at which an export started.
Finish	Date and time at which an export finished.
Hostname	ID of the app object host.
User ID	ID of the user who started the export.
User Name	Name of the user who started the export.
App	Name of the app that the app object belongs to.
Object	Name of the app object.
Object Type	Type of app object.
Output Format	Output format of the exported app object.
Export Duration	Length of time the export lasted.
Message	Summary of the export activity.

3.10 QMC Change Log

The *QMC Change Log* sheet displays changes made in the QMC. It enables administrators to analyze operations that might have a range of effects, from system performance to user access. You can explore changes by QMC resource type, by specific QMC resources, by users who made changes, or by a type of action performed in the QMC.

Change Summary

The table at the top of the *QMCChange Log* sheet is titled *Change Summary*. It summarizes changes by resource type, shows the latest change, and whom it was made by.

Resource Type	The following resource types are listed: • Analyzer access • App • App content • App object • Application access • Certificates • Content library • Content library content • Extension • License • Rule • Stream • Task • User • User access • User access from license
Changes	Number of changes made to the resource type.
Latest Change	Most recent change to the resource type.
Changed by	User who made the most recent change.

Users making changes

The *Change Users* table on the right side of the sheet lists the QMC users who have made changes. It includes the total number of changes made and the date of the latest change. It can be used to track users making a large number of changes.

UserID	ID of the QMC user who made changes.
User Name	Name of the QMC user who made changes.
User Role	User role of the QMC user who made changes.
Changes	Number of changes made by the user.
Latest Change	Date of the latest change made by the user.

Change details

Details of changes made in the QMC are contained in a table named *QMC Change Log*. The QMC *Change Log* can be particularly useful for tracking changes to security rules. It can also help identify apps that have been added, published or exported inappropriately.

Timestamp	The date and time the log file containing the change action was created.
Resource Type	The type of resource that made the change.
Resource	The specific resource that made the change.
Command	The type of action the resource made, such as Add, Delete, or Update.
User ID	The ID of the user who made changes.
User Name	The name of the user who made changes.
User Role	The admin role of the user who made changes.
Change Detail	The details of the change. For example, if a system rule has been added, the detail includes the category of the rule, such as security, the name of the rule, the rule, actions permitted by the rule, the context of the rule, and version.

3.11 Apps

The *Apps* sheet provides detailed information about apps and app objects, such as, ID, owner, stream, and time and date of publishing.

Tables

App Owners

Displays the app owner and the number of apps owned.

App Details

Displays the details of the apps in the Qlik Sense Repository Service (QRS). If an app never has been published, the value in the *Stream* column is *Unpublished* and the value in the *Published* column is *Never*. Published apps display the stream name and a time stamp for when the app was published.

App Object Owners

Displays the app object owner and the number of objects owned.

App Object Details

Displays the details of the app objects in the QRS. When an app object has the value *Not approved* in the *Approved* column, it means that the app object was added to an already published app. When the value is *Approved*, the app object belonged to the app when the app was published.

3.12 Log Details

The *Log Details* sheet displays the current version of the *Operations Monitor* and the copyright notice. It also provides status of the most recent reload of the *Operations Monitor*, including errors and messages. The sheet contains three tables that list servers monitored and display the errors, warnings, and log details during the selected period.

For a more complete view of all the logs, refer to the Log Monitor app.

Qlik SenseServers	Lists the servers from which log details have been collected. It can highlight servers that are generating high numbers of log entries.
Errors & Warnings	Provides a consolidated list of errors and warnings by Qlik services. When a specific service message is selected, the *Log Details* table displays log entries associated with that service message. This table can highlight services (for example, Proxy or Engine) that are producing numerous errors.
Log Details	Lists log entries by host name and service. The Date and Hour fields can be useful for filtering. The Timestamp field shows the exact date and time the message was logged. You can search for "*Synchronization*" in the Command column to see the status of sync activities in the Message column. *When Task Status for an app is reported as FinishedFail or Aborted on the Task Details sheet, the Level of the message for the reload task on the Log Details sheet may be INFO instead of ERROR. The number of task failures reported is, however, the same on both sheets.*

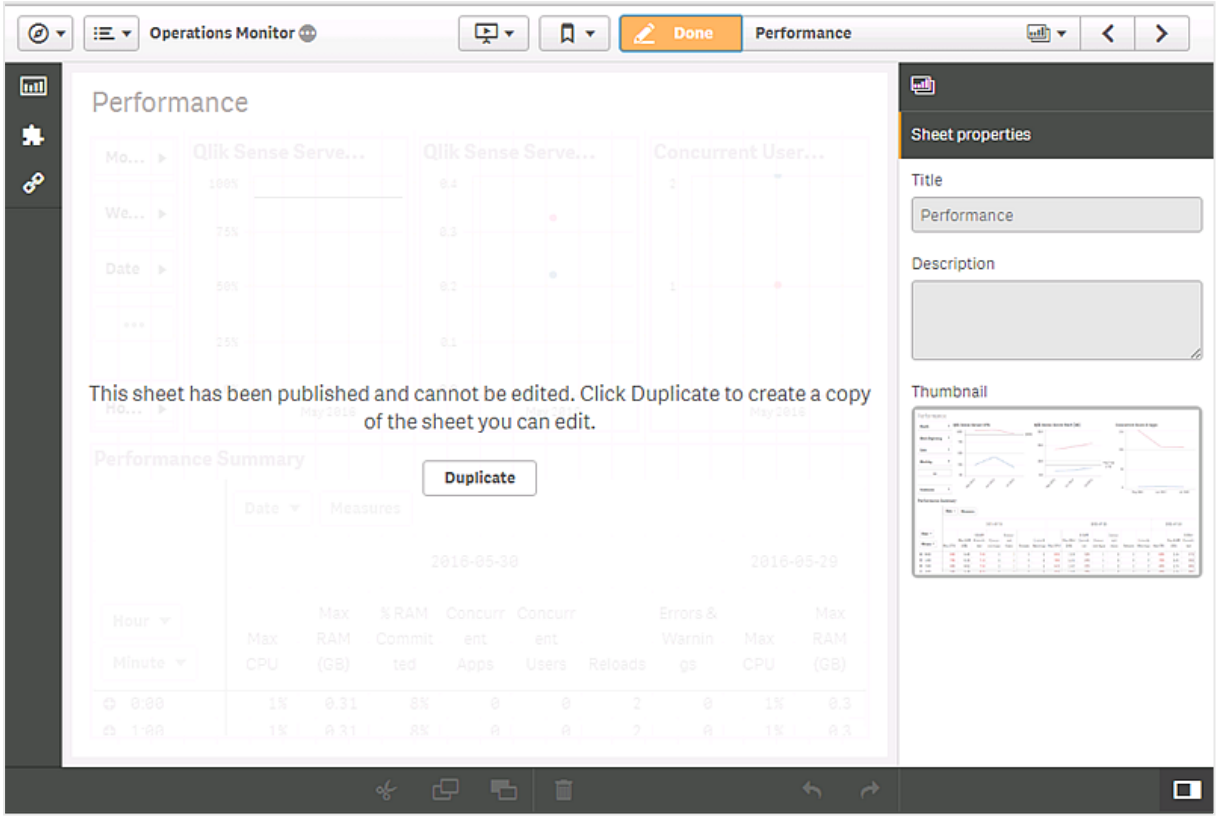
The *Operations Monitor* creates a log for that contains the status of each of its reloads. The log file, named “Operations_Monitor_Reload_Stats.txt,” is located in the Log folder: *%ProgramData%\Qlik\Sense\Log*.

3.13 Operations Monitor assets panel

The *Operations Monitor* includes an assets panel that provides access to charts, custom objects, and master items used in the app. You can use these objects to create additional visualizations for your particular environment.

The assets panel may also contains extra visualizations that are not used on the *Operations Monitor* sheets. These visualizations can be used on customized sheets that you create for your particular environment. You can use the visualizations as is or customize them for your environment.

To access the assets panel, open one of the *Operations Monitor* sheets and click **Edit** in the toolbar. In the illustration below, the *Performance* sheet is open in edit mode. You cannot edit the *Performance* sheet, but you can make a copy of it and then customize it by adding new visualizations or altering or removing the existing visualizations.



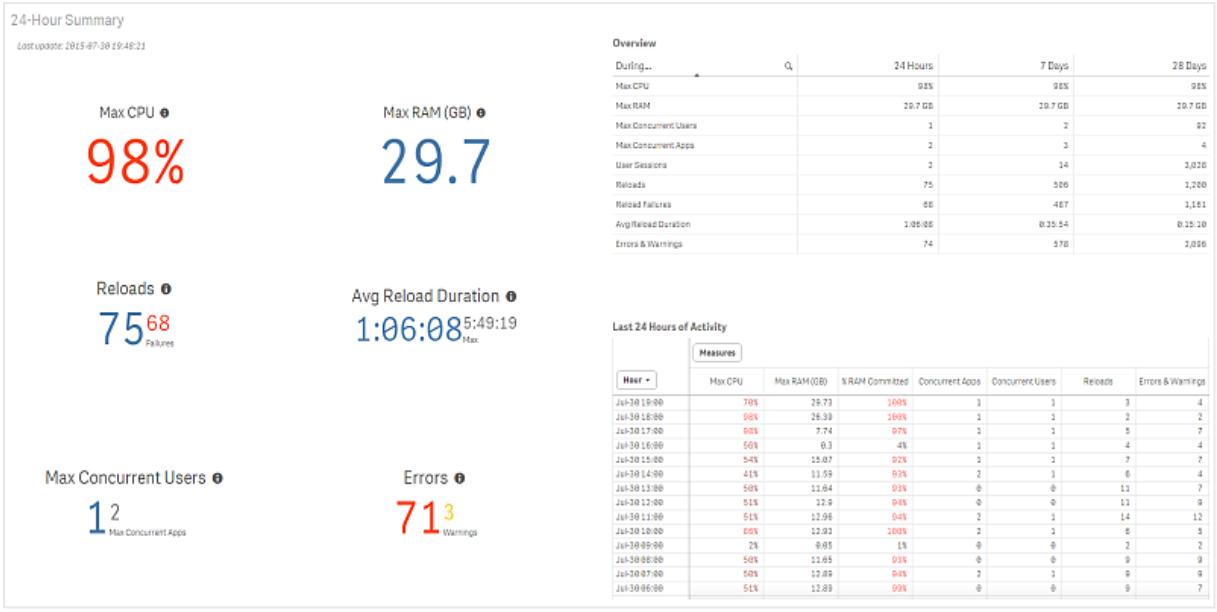
When you click a dimension, measure, or visualizations in the assets panel, a pop-up is displayed with a description of the object.

3.14 Analyzing operations data

The *Operations Monitor* gathers a large amount of data about Qlik Sense systems and operations and organizes the data in charts and tables that enable the data discovery typical of Qlik Sense apps. The scenarios outlined in this section of the documentation offer approaches to analyzing operations data to diagnose problems and better understand how a Qlik Sense environment is performing.

Diagnosing reload task failures

The following scenario explores approaches to analyzing operations data that shows a high number of reload task failures in the last 24 hours. This condition would be identified by checking the *Reloads* KPI on the *24-Hour Summary* sheet. The *Reloads* KPI indicates how many reload tasks have been started and how many have failed.



If the KPI shows 75 reload task and 68 failures, that is high failure rate, and in most cases, you would want to find out why it is so high. The steps below offer one analytical path that might lead to a diagnosis.

Do the following:

1. Double-click the *Reloads* KPI to open the *Task Overview* sheet in the *Operations Monitor* app.
2. Review the *Reloads per Hour* chart to see if the failure rate is high over a particular time period during the last 24 hours.
   If you find that a large percentage of the failures occurred during a limited period of the day, you might be able to identify an isolated event. If the failures are spread out over the 24-hour period, you should compare the recent period to other periods.
3. Open the *Task Details* sheet and select a time period to examine.
4. If the current month shows a significant number of failures, select the month to see its specific data.
5. Select specific dates in the month to isolate the time periods in which a significant number of failures occurs.
6. Switch to the *Log Details* sheet and examine the types of errors in the *Errors & Warnings* table to find out if there is problem that affects multiple tasks.
   It is possible that there is an underlying problem with one of the services, such as the Engine or Scheduler, that affects a number of the reload tasks.
7. Switch back to the *Task Details* sheet and select individual tasks in the *Reload Summary Statistics* table, particularly tasks that have a high failure rate.
   When a task is selected, the *Reload Details* table displays the individual reload attempts for that task.
8. Examine reload attempts with **`FinishedFail`** status and their reasons for failure.

The *Operations Monitor* might not indicate directly what the problem is, but by understanding the types of errors or the reload tasks that are failing, you can investigate causes. For example, a load script may have been changed and introduced an error that causes it to fail.

Diagnosing slow system response

The following scenario explores approaches to analyzing slow system response for apps and reload tasks. This condition might be identified on the *24-Hour Summary* or *Performance* sheets if there is a very high average server CPU usage or on the *Task Details* sheet if average load duration time goes up significantly. Neither of these indicators are necessarily definitive. The changes shown might be normal variations, such as a series of reload tasks that normally run longer. Another indication might be that users complain that their system response time is unusually slow. The *Operations Monitor* can then be used to diagnose the problem.

When slow system response appears to be a problem, the steps below offer one analytical path that might lead to a diagnosis.

Do the following:

1. Switch to the *24-Hour Summary* sheet in the *Operations Monitor* app.
2. Review the *Last 24 Hours of Activity* pivot table to see if there is high average usage for an extended time during the 24-hour period. High CPU usage could indicate a hardware problem, or it could be a symptom of problems or conditions elsewhere on the server, such as reload failures, system errors, or increased usage.
3. Review the *Last 24 Hours of Activity* pivot table to see if memory usage is unusually high. Memory usage of 90% or above should be considered high. Average RAM and maximum RAM usage are usually quite similar over a 24-hour period.
4. If memory usage is high during some part of the 24-hour period, check the *Overview* table to see if average RAM is higher for the 24-hour period compared to the 7-day and 28-day periods. Higher current RAM usage could indicate that something unusual is occurring and could be causing the slow system problems.
5. Check *Concurrent Users & Apps* chart on the *Performance* sheet to see the number of users is high during the period when response has been slow.
6. If the number of users is high, switch to the *Session Overview* sheet to see if there is a correlation between the number of user sessions and the period of slow response.
7. Select the time period in which the slowdown occurs and review the *Sessions by Hour* chart and *Avg Session Duration* KPI to see if there is a large number of sessions or sessions that last a long time. Sessions with long duration times could be running apps that are very active (many selections), perhaps a meeting presentation or deep analysis. It is also possible that a session was left open without ongoing activity in the app, or an app got stuck or did not close properly. Usually a "frozen" session does not consume a lot of resources. Long session duration could be caused by users accessing apps during long meetings or doing extended analysis.
8. Switch to the *Session Details* sheet and review the *App Session Summary* table to see if there are specific apps running in a number of sessions. It is possible that one user has an app open in multiple browsers but is only actively using it in one place.
9. Switch to the *Task Details* sheet and select the date or dates for which slow system response is occurring to see if there is an extraordinarily large number of reloads being performed during the period or if there is a large number of reload failures occurring.

10. Switch to the *Task Overview* sheet and check the *Avg Reload Duration* KPI to see if the average duration is high during the slow response period.
11. Switch back to the *Task Details* and check the *Reload Summary Statistics* table to see how many reload tasks have high average durations and how many reload attempts those tasks have made. If there are one or two apps reloading data frequently and whose reloads take a long time, you might have to move those app reloads to another server or reduce the number of reload tasks to free up CPU time for other apps that are negatively affected.
12. Check the Reload Failures column in the *Reload Summary Statistics* table to see if the apps that have long average reload durations are failing frequently. Reload tasks that are failing frequently could be experiencing connection problems with their data source and are left in a wait state for long periods, or they are being rerun immediately after failures. Problems with the reload tasks might have to be fixed to reduce load that is slowing system performance. The most recent data load execution logs are available in *Qlik\Sense\Log\Script* and are listed in the app GUID.
13. Check the *Reload Details* table to see if tasks that fail have long durations or if they take a long time to run successfully. If the reload tasks run a long time and then fail, the problems with the task will have to be fixed to improve system performance. If the tasks take a long time to run successfully, they may have to be moved to a system with more resources to prevent them from blocking other apps.
14. Switch to the *Log Details* sheet to see the types of errors and warnings generated during the slow response time. If the errors are concentrated in one or two services, or perhaps one or two types of errors recur many times, then you can see whether one of the services has to be fixed or perhaps a particular type of error will point to a problem with a reload task that can addressed.

There are multiple issues that could cause poor system response time, and the preceding review of the *Operations Monitor* objects could reveal one or more problems that are affecting your systems.

4 License Monitor

The *License Monitor* loads service logs to populate charts and tables covering token allocation, usage of login and user passes, and errors and warnings.

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

> *If you have a user-based license with professional and analyzer access, you will instead see figures relevant to that license type.*

4.1 License Monitor sheets

The License Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 8)*), the app includes information across all nodes.

Overview	Displays summary data about login and user access sessions over the last 7, 28, and 90 days, changes in the allocation of license tokens over the last 7 days, and license usage over time.
User Detail	Allows the user to select a time period over which to display user access pass sessions, the number of users starting sessions, and the individual users starting sessions.
Usage by App	Allows the user to select a time period over which to display the apps for which access passes are being used and the number of tokens consumed by each app.
Timeline	The *Timeline* sheet displays token usage over time so administrators can monitor usage and anticipate future token allocation needs.
User Access History	Allows the user to select a time period over which to display user access pass sessions, the number of users starting sessions, and the individual users starting sessions. *Only valid for token-based license.*
Login Access History	Allows the user to select a time period over which to display login pass utilization, login access users, and denials of login access. *Only valid for token-based license.*
Allocation History	Displays the latest changes and changes over selected times to the allocation of license tokens to login and user access passes.

Log Details	Lists servers in the cluster and provides details about license usage entered in server's logs.

Data in the License Monitor is updated when the app is reloaded. Data is not live.

4.2 Overview

The *Overview* sheet provides an overview of license changes and user access in the last 7, 28, and 90 days. Charts and tables contain information about user access and user-specific access history. There are two license types: token-based license (with login access and user access), and user-based license (with professional access or analyzer access). The charts will show data that is relevant to your license type.

For a user-based license, you will see figures for access instead of tokens, and figures for professional and analyzer access, instead of login and user access.

Data comes from all nodes in a multi-node environment.

KPIs (token-based license)

There are eight KPIs to provide high-level summary information about license usage.

Unallocated Tokens	Percentage of tokens that have not yet been allocated. Double-click to see the *Allocation History* sheet.
Total Tokens	Total number of tokens that are available. Double-click to see the *Allocation History* sheet.
Available User Access	Percentage of user access available.
Available User Access	Total number of user access available.
Available Login Access	Percentage of login access available.
Allocated Login Access	Total number of login accesses that have allocated.
Access Denials	Total number of access denials over the last 90 days. Double-click to see the *User Detail* sheet.
All-time Users Accessing Apps	Total number of users ever accessing the apps. Double-click to see the *User Detail* sheet.

KPIs (user-based license)

There are eight KPIs to provide high-level summary information about license usage.

Unallocated Access	Percentage of access (professional or analyzer) that has not yet been allocated. Double-click to see the *Allocation History* sheet.
Total Access	Total access (professional or analyzer) that is available. Double-click to see the *Allocation History* sheet.
Unallocated Professional Access	Percentage of professional access available.
Licensed Professional Users	Number of professional access allocations available.
Unallocated Analyzer Access	Percentage of analyzer access available.
Licensed Analyzer Users	Number of analyzer access allocations available.
Access Denials	Total number of access denials over the last 90 days. Double-click to see the *User Detail* sheet.
All-time Users Accessing Apps	Total number of users ever accessing the apps. Double-click to see the *User Detail* sheet.

Tables

Overview

During the first 7 days, the 28-day average will probably show a higher daily average than the 7-day because it calculates how many days have had activity whereas the 7-day average always divides by seven, regardless the number of days that actually had activity during that 7-day period. The same is true for the 28-day average compared to the 90-day average.

Total Users	Total number of users who have used either a login access token or a user access token over the last 7, 28, and 90 days.
Total Tokens Used	Total number of tokens used over the last 7, 28, and 90 days.
User Access Tokens Used	Number of user access tokens used over the last 7, 28, and 90 days.
Login Access Tokens Used	Number of tokens used over the last 7 or 28 days. The Last 90 Days measure uses the last 28 days due to the 28-day renewal process of login access passes.
Avg Daily Tokens Used	Average number of tokens used on a daily basis over the last 7, 28, and 90 days.
Max Daily Tokens Used	Highest number of tokens used on a daily basis over the last 7, 28, and 90 days.

Access Denials	Number of times access was denied over the last 7, 28, and 90 days. Denials can be for login or user access. A user is denied login access when all the login access tokens for the group to which the user belongs have been used. User access is denied when a user access token has not been allocated to the user.
Allocation Changes	Number of changes over the last 7, 28, and 90 days, in the way tokens are allocated.

Allocation Changes in Last 7 Days

This table lists the date changes were made, the type of change, such as adding more passes, the user and group affected by the change, and the user who made the change. When login access passes are allocated, they are allocated in groups of ten. That is because 10 login access passes are granted for 1 token. Login passes are allocated to groups, and then users in that group can access those passes.

A single user access pass requires one token. User access passes are allocated to specific users.

The *Allocation Changes in Last 7 Days* table can be used to detect unexpected changes made to token allocation.

Charts

User Timeline

This line chart shows the number of users accessing apps, and the distribution between login access user access on a monthly basis. Select a month to display the distribution per day.

4.3 User Detail

The *User Detail* sheet shows more detailed information about licensed Qlik Sense users.

For a user-based license, you will see figures for access instead of tokens, and figures for professional and analyzer access, instead of login and user access.

Data comes from all nodes in a multi-node environment.

User License Session Summary

The table shows user, access type, and when the access was allocated. The *Total Sessions Count* gives an indication of how frequently Qlik Sense is used.

Denied Access

This pivot table lists users who have been denied access. Have the access denials anything to do with recent changes in access allocations?

Unused Access

Users in this list with the access type user access, may not need user access, but could instead have login access.

Sessions per User

Use the filter box *Session Threshold* to filter out users who are above a certain number of sessions. Users below the threshold can be perhaps be assigned a different access type?

Quarantined Access

Shows users who have been quarantined and when the quarantined access is available again.

4.4 Usage by App

The *Usage by App* sheet shows the apps for which access passes are being used. The usage values are the passes that have been used, not the number of passes allocated. The period of history shown can be selected by month, by week, by a specific date, by days of the week, and also by specific app streams or apps.

For a user-based license, you will see figures for access instead of tokens, and figures for professional and analyzer access, instead of login and user access.

Token Consumption by Stream > App

The *Token Consumption by Stream > App* table displays the number of tokens used for each app and corresponding stream, and the distribution between users with login access and user access for the selected period. The *Totals* row shows the total number of tokens used and the percentage of total tokens.

Token Consumption by Stream

The *Token Consumption by Stream* bar chart displays the number of user access passes used for each stream, and the distribution between the two access types. You can quickly get an overview of the most popular streams.

Token Consumption by App

The *Token Consumption by App* bar chart displays the number of access passes used for each app, and the distribution between the two access types. You can quickly get an overview of the most popular apps.

Token Consumption Timeline

The *Token Consumption Timeline* line chart shows the consumption of tokens over time. You have a *Month > Date* drill-down option that enables closer review of a certain month. You can also switch between viewing the consumption per *Access Type*, *App*, or *App Stream*.

4.5 Timeline

The *Timeline* sheet is intended to display token usage over time so administrators can monitor usage and also anticipate future token allocation needs – such as adding more tokens to specific login access rules.

The period of history shown can be selected by month, week, or date. Selections can also be filtered by access type, app stream, app, user ID or user name.

For a user-based license, you will see figures for access instead of tokens, and figures for professional and analyzer access, instead of login and user access.

Token Consumption Timeline

The *Token Consumption Timeline* line chart shows the number of tokens consumed during the selected time period. You can drill down from month to date for a more detailed view. Token consumption can be displayed by access type, app stream, or app.

The chart is only valid when viewed by month. Login access passes renew every 28 days, and token usage by, for example, quarter, would therefore be incorrect, because each token for login access would renew a couple of times during that 3-month period.

Token Consumption by Month

The *Token Consumption by Month* pivot table displays token usage by month, app stream, app and access type. By default, token usage is displayed by month and access type. Expand to show stream and app details. With a pivot table, you can also move the dimensions and measure around for different views of the data.

The chart is only valid when viewed by month. Login access passes renew every 28 days, and token usage by, for example, quarter, would therefore be incorrect, because each token for login access would renew a couple of times during that 3-month period.

First Time Access (New Users)

The *First Time Access (New Users)* bar chart displays token usage of users who are accessing apps and streams for the first time. The users are presented by access type.

4.6 User Access History

This page is only relevant if you have a token-based license.

The *User Access History* sheet shows the number of non-concurrent sessions started by users with user access passes and the number of users who started non-concurrent sessions. The period of history shown can be selected by month, by week, by a specific date, by days of the week, or by hour of the day. Individual users can also be selected, and selections can be made by number of sessions.

The *User Access Sessions* chart shows the number of sessions started and the number of users who started them during the selected period of time. It is useful to track the ratio of unique users to user passes over time.

The *Unused User Access Passes* shows the users who have not used their user access pass, when their user access pass was granted, and by whom the user access pass was last modified. Unused access passes constitute an unnecessary cost, and users who have not used their user access pass could be quarantined and, in time, their token reallocated to a login access rule or to another user access pass.

The *User Access Sessions per User* table lists individual users who have started sessions during the selected period and the total number of sessions they started.

The table also lists the number of sessions each user started in the last 28 days and the date of the last session. Knowing how often a user has started sessions in the last 28 days allows you to determine whether or not a user is making full use of his or her user pass. Users who have not started at least ten sessions in the last 28 days might be able to use login access passes instead of user access passes because login passes are allocated to groups on a basis of ten passes per license token. User access passes are allocated to individual users on a basis of one pass per token.

The session numbers here are not exactly the same as the session numbers by user in the *Operations Monitor*. The user access sessions shown in the *Session Details* do not count concurrent sessions. If a user has more than one app open concurrently, only one user pass session is counted.

The *Quarantined User Access Passes* table shows the users, when the quarantine ends, and when and by whom the user access passes were modified. If the quarantine period has not reached its end, the original allocation of the access pass can be reinstated, so that the user can start using the access pass again.

4.7 Login Access History

This page is only relevant if you have a token-based license.

The *Login Access History* sheet shows the totals of login pass usage and the usage by individual users. The usage values are the passes that have been used, not the number of passes allocated. The period of history shown can be selected by month, week, by a specific date, by days of the week, or a specific date and time. Selections can also be made based on users, login access rules, and number of login passes used.

Login access pass usage

The *Used Login Access Passes* stacked bar chart displays, by default, a month-by-month breakdown of login access passes used by groups. When different log dates and times are selected, the chart displays login access usage by group for those selected times. Because the bar chart is stacked, it is easy to see how usage across different groups is changing.

The *Login Access Rule Usage* stacked bar chart displays the total number of access passes and the distribution between used and available passes. The subheading shows the date and time when the data was retrieved.

Login access pass users

The *Login Access Passes per User* table is a sortable list of users, who have used login access passes in total and over the last 28 days. It displays the number of login passes each user has used and the last time the user accessed the system.

Users who use more than ten login passes in a 28-day period might be candidates for getting user access passes. User access passes allow the assigned user to login as many times as necessary during a 28-day period, but they require the allocation of a whole license token. Login access passes, on the other hand, are allocated to groups on a basis of ten passes per license token.

The table also enables you to find inactive users who have not used Qlik Sense recently.

Access denied

The *User Denied Access* pivot table shows, users, by name and ID, who were denied login access, when they were denied, and how many times they were denied on a particular date. Examining access denials can help administrators understand whether recent token allocation changes have caused or resolved denials.

4.8 Allocation History

The *Allocation History* sheet provides status of the access allocated and the history of license allocation changes over the selected time period. Status and history can also be displayed according to the operation performed, a login access rule, and the user who performed an operation.

The *Allocation Changes* KPI shows how many changes have been during the selected period.

The *Allocation Users* pivot table allows you to examine user allocation changes by the type of action and the administrator who took the action.

The *Affected Objects* table lists the user group affected by the changes. Each change is listed with the date the change was made.

For a user-based license, you will see figures for access instead of tokens, and figures for professional and analyzer access, instead of login and user access.

License Allocation Change History

This table shows how licenses have been allocated to login and user access and the details of the allocations. Here it is easy to see which users have recently been allocated User Access Passes and how often tokens are being reallocated among Login Access Groups.

Timestamp	The date and time of the allocation change.
Modified By	The administrator who performed the allocation operation.
User Role	The admin role of the administrator.
Affected Object	The group to which login access was granted or the user to whom user access was granted.
Command	The specific operation that took place with this command. • **Add rule**: a rule was created for the entity in the **Affected Object** column. • **Delete rule**: a rule was deleted for the entity in the **Affected Object** column. • **Add user access**: user access was added for the entity in the **Affected Object** column. • **Update user access**: the entity in **Affected Object** was allocated additional access passes or the number of access passes allocated was reduced. • **Update license**: the license for the entity in **Affected Object** was updated.
Message	The details of the command performed.

4.9 Log Details

The *Log Details* sheet displays the current version of the *License Monitor* and the copyright notice. It also provides status of the most recent reload of the *License Monitor*, including errors and messages.

The *Qlik Sense Servers* table lists the nodes in a multi-node environment on which licensing activity has taken place in the last 24 hours.

The *License Log Details* table shows events recorded in the license log file.

Date	The date of the activity related to licensing.
Hour	The hour of the activity related to licensing.
Timestamp	The date and time of the activity related to licensing.
Hostname	The name of the server on which the activity took place.
User Id	The user who initiated the activity.
Object	The user who is the object of the activity.
Description	A description of the activity, such as license maintenance or user access request.
Command	The type of action that caused the log to be generated.

Message	A detailed description of the activity, including the type of operation (for example, Timeout).

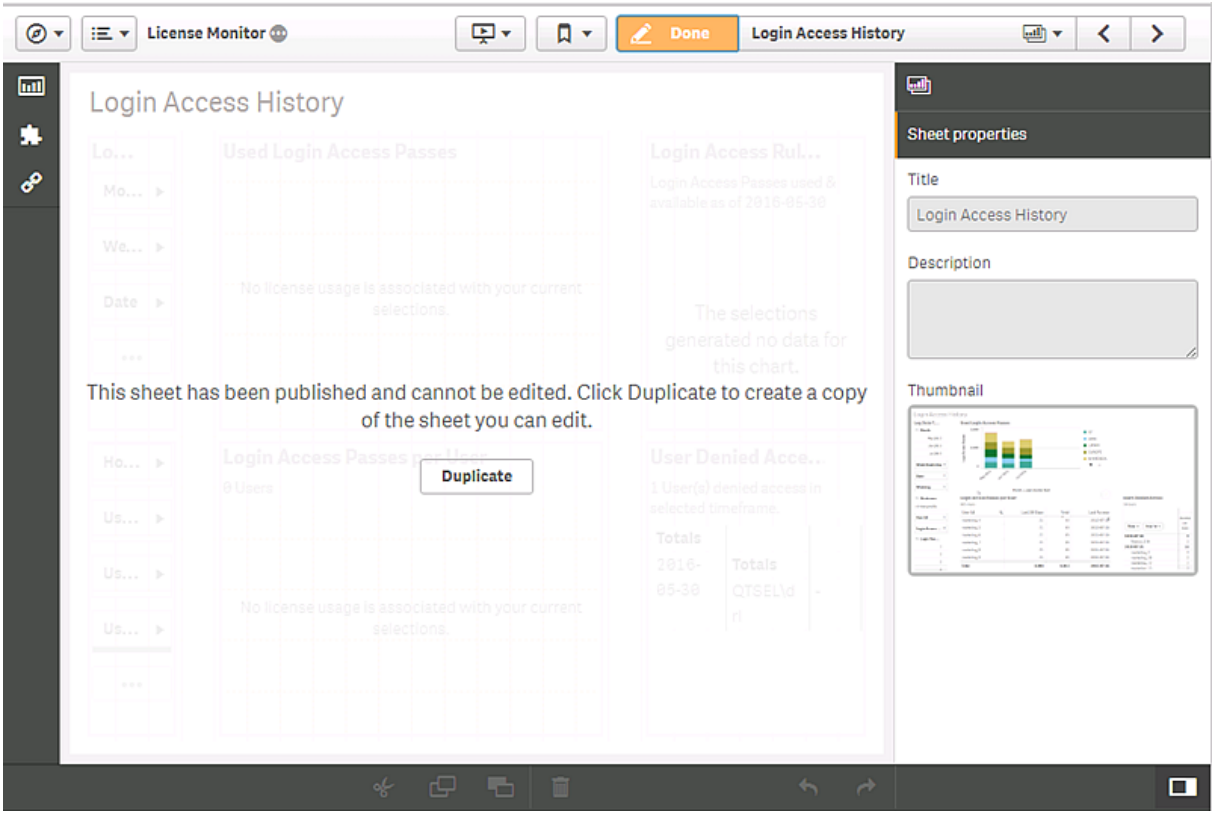
The *License Monitor* creates a log that contains the status of each of its reloads. The log file, named "License_Monitor_Reload_Stats.txt," is located in the Log folder: *%ProgramData%\Qlik\Sense\Log*.

4.10 License Monitor assets panel

The *License Monitor* includes an assets panel that provides access to charts, custom objects, and master items used in the app. You can use these objects to create additional visualizations for your particular environment.

The assets panel may also contain extra visualizations that are not used on the *License Monitor* sheets. These visualizations can be used on customized sheets that you create for your particular environment. You can use the visualizations as is or customize them for your environment.

To access the assets panel, open one of the *License Monitor* sheets and click **Edit** in the toolbar. In the illustration below, the *Login Access History* sheet is open in edit mode. You cannot edit the *Login Access History* sheet, but you can make a copy of it and then customize it by adding new visualizations or altering or removing the existing visualizations.



When you click a dimension, measure, or visualizations in the assets panel, a pop-up is displayed with a description of the object.

4.11 Analyzing license data

The *License Monitor* gathers a large amount of data about how Qlik Sense license tokens are allocated and used and organizes the data in charts and tables that enable the natural analytics typical of Qlik Sense apps.The scenarios outlined in this section of the documentation offer approaches to analyzing license data to better understand how access passes are being used. That knowledge can then be used to allocate access passes most efficiently.

Diagnosing login access overutilization

When managing login access passes, it is important to monitor the number of login passes used in the 28-day period to find users who exceed the threshold (10 passes).

Open the *Login Access History* sheet and sort the *Login Access Passes per User* table in descending order to see the high-frequency users at the top of the list. The high-frequency users who use more than 10 login access passes in 28 days can be managed more efficiently by giving them user access passes.

Scenario 1: Appropriate utilization

In this case, the *Login Access Passes per User* table shows that all the login access users have used fewer than 10 sessions in the last 28 days. It requires fewer license tokens to service these users than it would be to allocate user access passes to any of them.

Login Access Passes per User

932 Users

User Id	Last 28 Days	Total	Last Access
finance_403	4	25	2015-09-25
finance_400	4	24	2015-09-25
finance_408	4	24	2015-09-25
marketing_37	5	123	2015-10-13
marketing_49	5	102	2015-09-27
marketing_30	5	88	2015-10-13
finance_73	5	85	2015-09-25
finance_37	5	83	2015-09-25
finance_83	5	81	2015-09-25
finance_84	5	80	2015-09-25
Total	**2,585**	**22,941**	**2015-10-19**

Scenario 2: Overutilization

In this case, the *Login Access Passes per User* table shows that several users have accessed well over 10 times in the last 28 days. These users are candidates for dedicated user access passes. The number of login passes freed up by reassigning the high-frequency users would be the sum of the passes the users used in the last 28 days.

Login Access Passes per User

932 Users

User Id	Last 28 Days	Total	Last Access
marketing_init_2	21	87	2015-10-17
marketing_22	22	98	2015-10-13
marketing_20	24	92	2015-10-13
finance_5	26	106	2015-10-19
finance_init_2	26	78	2015-10-19
finance_2	26	69	2015-10-19
finance_6	29	109	2015-10-19
marketing_5	40	161	2015-10-19
marketing_2	42	115	2015-10-19
marketing_6	45	168	2015-10-19
Total	**2,585**	**22,941**	**2015-10-19**

User access underutilization

When managing user access passes, it is important to monitor the number of passes used in the 28-day period to find users who are not making sufficient use of passes allocated to them.

Open the *User Access History* sheet and sort the *User Access Sessions per User* table in ascending order to see the low-frequency users at the top of the list. The low-frequency users can be managed more efficiently by giving them login access passes.

Scenario 1: Appropriate allocation

In this case, the *User Access Sessions per User* table shows that even the lowest frequency user access pass users are accessing Qlik Sense more than 10 times in the last 28 days. None of these users should be converted to login access passes.

User Access Sessions per User

543 Users

User Id	Last 28 Days	Total	Last Session
marketing_17	15	114	2015-10-13
marketing_18	15	114	2015-10-13
marketing_19	15	114	2015-10-13
marketing_21	15	114	2015-10-13
marketing_31	15	110	2015-10-13
finance_init_1	22	149	2015-10-19
finance_1	23	105	2015-10-19
marketing_1	27	128	2015-10-19
marketing_init_1	27	158	2015-10-19
finance_10	28	110	2015-10-19
Totals	**2,241**	**16,317**	**2015-10-20**

Scenario 2: Underutilization of user access

In this case, the *User Access Sessions per User* table shows that a number of users listed at the top of the table have accessed Qlik Sense far fewer times than the threshold for a user access pass. These users could be added to login pass groups, and their user access passes could be reallocated to high-frequency users who do not currently have user access passes. Or the license tokens used for the user access passes could be converted to login access passes.

User Access Sessions per User

543 Users

User Id	Last 28 Days	Total	Last Session
marketing_140	1	8	2015-09-22
marketing_141	1	8	2015-09-22
marketing_142	1	8	2015-09-22
marketing_143	1	8	2015-09-22
marketing_144	1	8	2015-09-22
marketing_145	1	8	2015-09-22
marketing_146	1	8	2015-09-22
marketing_147	1	8	2015-09-22
marketing_148	1	8	2015-09-22
marketing_149	1	8	2015-09-22
Totals	**2,241**	**16,317**	**2015-10-20**

Diagnosing problems with login pass denials

From the *Overview* table on the *7-Day Summary* sheet it is evident that there have been a number of access denials in the past seven days and many more in the past 28 days. Has this affected a number of different users, or are there specific users who are being denied access frequently?

Overview

2015-10-13 to 2015-10-20

Measure	Last 7 Days	Last 28 Days
Total Users	31	642
Avg Daily Login Access Passes	12	93
Max Daily Login Access Passes	29	483
Total Login Passes	84	2,585
User Access Sessions	65	1,996
Access Denials	18	1,262
Allocation Changes	0	0

To investigate this issue, review the *Users Denied Access* table on the *Login Access History* sheet. The table lists users who were denied access, when they were last denied, and how many times each user was denied access.

User Denied Access

73 User(s) denied access in selected timeframe.

Date	User Id	User Name	Access Denials
Totals			**135**
2016-02-23	**Totals**		**80**
	QT\santiago_15000	santiago_15000	2
	QT\santiago_15001	santiago_15001	2
	QT\santiago_15005	santiago_15005	2
	QT\santiago_15006	santiago_15006	2
	QT\santiago_15007	santiago_15007	2
	QT\santiago_15008	santiago_15008	2
	QT\santiago_15010	santiago_15010	2
	QT\santiago_15011	santiago_15011	2
	QT\santiago_15015	santiago_15015	2
	QT\santiago_15016	santiago_15016	2
	QT\santiago_15017	santiago_15017	2

A solution

Check the *Login Access Passes per User* table on the *Login Access History* sheet to see if any users are exceeding the 28-day access threshold. Those users would be candidates for a dedicated user access pass.

Login Access Passes per User

932 Users

User Id	Last 28 Days	Total	Last Access
finance_403	4	25	2015-09-25
finance_400	4	24	2015-09-25
finance_408	4	24	2015-09-25
marketing_37	5	123	2015-10-13
marketing_49	5	102	2015-09-27
marketing_30	5	88	2015-10-13
finance_73	5	85	2015-09-25
finance_37	5	83	2015-09-25
finance_83	5	81	2015-09-25
finance_84	5	80	2015-09-25
Total	**2,585**	**22,941**	**2015-10-19**

In this case, however, no login pass users have exceeded the threshold in last 28 days.

Because there are no login pass users who should be given user pass access, resolving the problem of login access denials can probably be handled by allocating more tokens to the specific groups whose users are being denied access. License tokens are allocated in the Qlik Management Console.

5 Log Monitor

The *Log Monitor* loads and visualizes almost all available Qlik Sense log data. This gives you the possibility to discover trends and analyze and troubleshoot issues in your Qlik Sense environment. Compared to the Operations Monitor, the Log Monitor loads more log files, but for a shorter period of history (default seven days).

For a more detailed description of the sheets and visualizations, visit the story About the Log Monitor that is available from the app overview page, under ***Stories****.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

5.1 Importing the Log Monitor app to the Monitoring apps in the QMC

The Log Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing the new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor (page 9)*

5.2 Log Monitor sheets

The Log Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 8)*), the app includes information across all nodes.

Overview	Summarizes the activities during the last couple of hours and days and enables you to quickly identify irregularities.
Timeline	The Activity Timeline bar chart gives an overview of the logging activities during the last week. Use the alternative dimensions to see how the measures vary over time and find diverging values that may require investigation.
Trends	Shows a collection of timelines displaying performance (CPU and RAM), usage (apps and users), as well as errors and reload status.
Errors & Warnings	Shows a timeline together with a summary and a detailed view of errors and warnings.
Filters	Contains filter panes with a large number of key fields from the logs. Make selections to make discoveries in your data.
Log Details	Shows errors, warnings, and information log entries for the servers in the deployment.

Data in the Log Monitor is updated when the app is reloaded. Data is not live.

6 Reloads Monitor

The *Reloads Monitor* loads and presents log data about reloads. Reload data is collected both from QMC tasks and apps open in the hub. You can see which apps are updated, and details about when, where, and how often they are updated.

*For a more detailed description of the sheets and visualizations, visit the story About the Reloads Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

6.1 Importing the Reloads Monitor app to the Monitoring apps in the QMC

The Reloads Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing the new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor (page 9)*

6.2 Reloads Monitor sheets

The Reloads Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 8)*), the app includes information across all nodes.

Dashboard	Gives an overview of the reload task history. Get different views by using the alternative dimensions and measures that are available for the Reloads by Hour bar chart and the Reload Count and Duration Trend combo chart.
Task Planning	Shows when tasks are reloaded and the associated duration and failure rate. Use the data to re-schedule reloads and thereby optimize performance.
Reload Summary	Gives detailed information about reload history statistics and recently completed reloads.
Log Details	Shows details about specific log events and times.
Intermediate Details	Presents the intermediate states of a task reload, such as Triggered, Started, and Queued.

Data in the Reloads Monitor is updated when the app is reloaded. Data is not live.

7 Sessions Monitor

The *Sessions Monitor* loads and displays log data about users' app sessions.

*For a more detailed description of the sheets and visualizations, visit the story About the Sessions Monitor that is available from the app overview page, under **Stories**.*

The log files are located in *%ProgramData%\Qlik\Sense\Log\Repository\Trace*.

7.1 Importing the Sessions Monitor app to the Monitoring apps in the QMC

The Sessions Monitor is not available by default from the QMC. To make it available, you need to import the app.

Follow the instructions in the section *Importing the new Monitoring apps: Log Monitor, Reloads Monitor, and Sessions Monitor (page 9)*

7.2 Sessions Monitor sheets

The Sessions Monitor sheets display Qlik Sense performance on the current node, and, when properly configured for multi-node (as described in *Configuring multi-node environments (page 8)*), the app includes information across all nodes.

Dashboard	Gives an overview of the session activity. Get different views by using the alternative dimensions and measures that are available for the Sessions Over Time bar chart and the User and App Count Trend combo chart.
Session Heatmap	Shows when session activity is at its highest and lowest. Use the data to understand peak usage times or optimal times for server maintenance.
Session Details	Gives a more detailed view of the session activity and helps identifying unused apps and extensive users of apps.
Apps	Shows metadata about apps and app objects.
Log Details	Shows details about specific log events and times.

Data in the Sessions Monitor is updated when the app is reloaded. Data is not live.

8 Troubleshooting - Monitoring a Qlik Sense site

This section describes problems that can occur when monitoring a Qlik Sense site.

8.1 The Monitoring apps are not backed up correctly

When upgrading Qlik Sense, the Monitoring apps are not backed up correctly.

Normally, when upgrading Qlik Sense, the existing version number of the Monitoring apps is replaced by the corresponding version number appended to the app name. Then, the latest Monitoring apps are also available under **Apps**.

Possible cause

The upgrade process of the Monitoring apps was unsuccessful.

Proposed action

Manually import the latest apps from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*.

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*.
   If prompted, do not rename the app.
3. Publish the newly imported License Monitor app to the Monitoring apps stream, replacing the existing License Monitor.
4. Repeat step 2 for the Operations Monitor.qvf.
5. Publish the newly imported Operations Monitor app to the Monitoring apps stream, replacing the existing Operations Monitor.
6. Repeat steps 2 and 3 for Log Monitor, Reloads Monitor, and Sessions Monitor.

8.2 I have accidentally deleted the Monitoring apps

I accidentally deleted the Monitoring apps and cannot find them in the QMC.

Possible cause

Accidental or intentional removal of the Monitoring apps.

Proposed action

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from

%ProgramData%\Qlik\Sense\Repository\DefaultApps\.
If prompted, do not rename the app.

3. Publish the newly imported License Monitor app to the Monitoring apps stream.
4. Repeat step 2 and 3 for any of the affected Monitoring apps.

8.3 The Monitoring apps have become corrupted

The Monitoring apps have become corrupted and are no longer functional.

Possible cause

Technical failure.

Proposed action

Do the following:

1. In the QMC, open **Apps**.
2. Click **Import** and select License Monitor.qvf from *%ProgramData%\Qlik\Sense\Repository\DefaultApps*\.
   If prompted, do not rename the app.
3. Publish the newly imported License Monitor app to the Monitoring apps stream, replacing the existing, corrupt License Monitor.
4. Repeat step 2 for Operations Monitor.qvf.
5. Publish the newly imported Operations Monitor app to the Monitoring apps stream, replacing the existing, corrupt Operations Monitor.

8.4 Reload of the Monitoring apps failed

There is more than one possible cause when the reload fails.

Insufficient administration rights in the QMC

Possible cause

The service account running the Qlik Sense services does not have the required RootAdmin role in the QMC.

Proposed action

For the Monitoring apps to successfully retrieve all data, the service account running the Qlik Sense services must be given the role of RootAdmin in the QMC.

Reload is performed on rim nodes

Possible cause

The load balancing rule *ResourcesOnNonCentralNodes* causes the reloads to fail on rim nodes.

Proposed action

Edit the load balancing rule *ResourcesOnNonCentralNodes*.

Do the following:

1. From the QMC start page, open **Load balancing rules**.
2. Select *ResourcesOnNonCentralNodes* and click **Edit**.
3. Under **Advanced**, edit the **Conditions**, so that they read as follows:
   `((node.iscentral="false"))`
4. Click **Apply**.

Message: "**Error: Field not found...**"

Possible cause

Some fields that are used by the Monitoring apps are missing in the log files.

Proposed action

Upgrade to 2.1.1 or later.

Message: "**Error: Table 'tempDateTimeList' not found...**"

This error can occur after an upgrade, especially if the environment changes from synchronized persistence to shared persistence, or if the Qlik Sense cluster share where Archived Logs are stored is changed.

Possible cause

The app cannot find license history data in the log files because the *ArchivedLogsFolder* data connection is incorrect.

Proposed action

Fix the *ArchivedLogsFolder* data connection to point to the correct folder location.

Message: "**Error: QVX_UNEXPECTED_END_OF_DATA...**"

This error can have different causes.

Customized proxy port

Possible cause

The proxy's HTTPS port has been customized.

Proposed action

Change all the `monitor_apps_REST_` data connections to use the customized port.

Example:

CUSTOM CONNECT TO*"provider=QvRestConnector.exe;url=https://localhost:4443/qrs..."*.

Data connections affected include the following:

- monitor_apps_REST_app
- monitor_apps_REST_appobject
- monitor_apps_REST_event
- monitor_apps_REST_license_access
- monitor_apps_REST_license_login
- monitor_apps_REST_task
- monitor_apps_REST_user
- monitor_apps_REST_license_user

Changes made to the user account under which the Qlik Sense services are running

Error message: **Error: QVX_UNEXPECTED_END_OF_DATA: HTTP protocol error 401 (Unauthorized): Requested resource requires authentication.**

Possible cause

During installation, a user account is created under which the Qlik Sense services run. If the credentials for that account changes, or a different account is selected for the Qlik Sense services to run under, the data connections must be updated accordingly.

Proposed action

Do the following:

1. Open the **Data connections** overview page in the QMC.
2. For each monitor_apps_REST_ data connection, click **Edit** and enter the new **User ID** and **Password** credentials.
3. Save the changes.

8.5 The Monitoring apps fail to reload in a multi-node environment

There is more than one possible cause when the reload fails.

The central node is not a reload node

The Monitoring apps with default monitor_apps_REST_ data connection strings fail to reload in a multi-node environment where the central node is not a reload node.

Possible cause

The reload node where the Monitoring apps are reloaded does not have any proxy set up.

Proposed action

Change all the `monitor_apps_REST_` data connections to point to the fully qualified domain name (FQDN) of the central node. This is accomplished by replacing *localhost* in the connection strings URL and *trustedLocation* parameters with FQDN of the central node.

Example:

CUSTOM CONNECT TO *"provider=QvRestConnector.exe;url=https://centralnodeserver.company.com/qrs..."*.

Data connections affected include the following:

- `monitor_apps_REST_app`
- `monitor_apps_REST_appobject`
- `monitor_apps_REST_event`
- `monitor_apps_REST_license_access`
- `monitor_apps_REST_license_login`
- `monitor_apps_REST_task`
- `monitor_apps_REST_user`
- `monitor_apps_REST_license_user`

The repository database is on a separate machine

Possible cause

The REST data connections point to the FQDN of the Qlik Sense Repository Database and not the Qlik Sense Repository Service.

Proposed action

In any multi-node or “remote” Qlik Sense Repository Database situation, you need to update the REST data connections to point to the FQDN of the Qlik Sense Repository Service, regardless of where the actual Qlik Sense Repository Database resides.

8.6 Operations Monitor App fails to reload after turning off database logging

The Operations Monitor reload task fails after the database logging is turned off.

The following error message is displayed:

```
Error: Table 'time_range_working' not found
```

Possible cause

The Monitoring apps continue to check for recent logs in the database and use these logs for approximately ten hours after the last log message is written in the database. If the database logging is turned off, no new log entries for the load script can be found, and this can cause the reload process to fail.

Proposed action

The reload fail can be prevented by manually updating the Operations Monitor app's load script.

1. Make sure file logging is enabled.
2. Update the Operations Monitor load script. Because this is a published app, you need to duplicate it first.
   Do the following:
   i. Duplicate the Operations Monitor app in the QMC.
   ii. Open the duplicate app in the Qlik Sense hub.
   iii. Update the load script at line 9 by changing the variable `db_v_file_override` from `0` (default value) to `1` as follows:
   `SET db_v_file_override = 1`
   By setting this variable to `1`, the script will not check for log entries in the database logging.
   iv. Save the app.
   v. Replace the existing Operations Monitor app by publishing the duplicate app to the Monitoring apps stream and selecting **Replace existing app**.
3. Launch the Operations Monitor reload task again. If it does not work immediately, wait a few minutes and reload again.

By following this procedure, the database logging can be turned off safely.

8.7 Failed to connect to the QRS via the Qlik REST Connector

This problem will only occur when you have apps that work with the Qlik REST Connector.

An error message is displayed that there is a problem connecting to the QRS via the Qlik REST Connector.

Possible cause

The Qlik REST Connector is unavailable, because it has been uninstalled or corrupted.

Proposed action

If the error message appears during a reload, you need to verify that the Qlik Sense installation is working properly. Consider repairing or upgrading Qlik Sense.