

# Pivotal Greenplum® Command Center

Version 4.5.0

## User Guide

Rev: 01

## Table of Contents

Table of Contents	2
Pivotal Greenplum Command Center 4.5.0 Documentation	4
Pivotal Greenplum® Command Center 4.5.0 Release Notes	5
About Pivotal Greenplum Command Center	11
Installing the Greenplum Command Center Software	14
Creating the gpperfmon Database	15
Installing Pivotal Greenplum Command Center	17
Upgrading Greenplum Command Center	23
Uninstalling Greenplum Command Center	24
About the Command Center Installation	25
Setting the Greenplum Command Center Environment	26
Connecting to the Greenplum Command Center Console	27
Administering the Command Center Web Server	28
Administering Command Center Agents	30
Administering the gpperfmon Database	31
gpcc	32
gpmetrics Schema Reference	34
Configuration Files Reference	36
Command Center Agent Parameters	37
Command Center Console Parameters	39
gpmetrics Configuration File Reference	41
Setup Configuration File	42
Greenplum Database Server Configuration Parameters	44
Securing Greenplum Command Center	45
Managing Greenplum Command Center Authentication	47
Managing Greenplum Command Center Permissions	49
Securing the gpmon Database User	51
Enabling Authentication with Kerberos	53
Monitoring the Greenplum Database System	58
Dashboard	59
Greenplum Database Cluster State	62
Segment Status	65
Cluster Metrics	68
Host Metrics	69
Storage Status	71
Monitoring and Managing Greenplum Database Queries	72
Query Monitor	73
Query Details	75
History	79
Alerts	82
Managing Greenplum Database Workloads	86
About Greenplum Command Center Workload Management	87
Workload Management	89
Importing Resource Queues to Resource Groups	93
Accessing the Workload Configuration Programmatically	96
Troubleshooting Enabling Resource Groups	99
Query Monitor Help Topics	101
CPU	102

CPU Skew	103
Locks	104
Memory	106
Query Plan Execution	108
Spill Files	111

## Pivotal Greenplum Command Center 4.5.0 Documentation

[PDF](#) [↗](#)

[Greenplum Command Center 4.5.0 Release Notes](#)

[About Greenplum Command Center](#)

### Installing Greenplum Command Center

- [Installing Greenplum Command Center](#)
- [About the Command Center Installation](#)
- [Setting the Greenplum Command Center Environment](#)

### Administration

- [Administering the Command Center Web Server](#)
- [Administering Command Center Agents](#)
- [Administering the gpperfmon Database](#)
- [gpcc Command Reference](#)
- [Configuration File Reference](#)
- [Securing Greenplum Command Center](#)

### Using Greenplum Command Center

- [Monitoring the Greenplum Database System](#)
  - [Overall Cluster State](#)
  - [Segment Status](#)
  - [Cluster Metrics](#)
  - [Host Metrics](#)
  - [Storage Status](#)
- [Monitoring and Managing Greenplum Database Queries](#)
  - [Query Monitor](#)
  - [Query Details](#)
  - [Query History](#)
- [Managing Workloads](#)
  - [About Workloads](#)
  - [Managing Workloads with Command Center](#)
  - [Troubleshooting Command Center Workload Management](#)

### Command Center Help Topics

- [CPU](#)
- [CPU Skew](#)
- [Locks](#)
- [Memory](#)
- [Query Optimization](#)
- [Spill Files](#)

## Pivotal Greenplum® Command Center 4.5.0 Release Notes

### About This Release

This document contains release information about Pivotal Greenplum Command Center 4.5.0. Greenplum Command Center 4.5.0 is a minor release that adds some features and resolves some issues.

See [Enhancements and Changes in Greenplum Command Center 4.5.0](#) for information about new features and changes in this Command Center release.

### Supported Platforms

Greenplum Command Center 4.5.0 is compatible with the following platforms.

- Pivotal Greenplum Database 5.14.0 and higher
- Red Hat Enterprise Linux 6.x<sup>1</sup> and 7.x
- CentOS 6.x<sup>1</sup> and 7.x
- SUSE Enterprise Linux 11 SP4<sup>2</sup>

<sup>1</sup>If you use resource groups and workload management on Red Hat or CentOS 6.x, upgrade your kernel to 2.6.32-696 or higher to benefit from improvements in the Linux cgroups service.

<sup>2</sup>Greenplum Command Center workload management features are not supported on SUSE Enterprise Linux 11.

### Enhancements and Changes in Greenplum Command Center 4.5.0

Greenplum Command Center 4.5.0 contains the following new features:

#### Alert Rules

On the new **Admin> Alerts** page, Command Center users with superuser permission can configure alert rules. When an alert rule is matched, a record is logged in the `gpmetrics.gpcc_alert_log` table and, optionally, an email is sent to a list of addresses you specify. You can also write a custom shell script to send alerts to other messaging systems.

Alert rules can detect the following events:

- Segment failure
- Out of memory errors
- Average memory usage percentage of segment hosts exceeds a specified percentage for a specified number of minutes
- Memory usage on the master host exceeds a specified percentage for a specified number of minutes
- Total disk space used on all hosts exceeds a specified percentage
- Number of Greenplum Database connections exceeds a specified percentage
- Average CPU usage of segment hosts exceeds a specified percentage for a specified number of minutes
- Spill files for an active query exceed a specified number of gigabytes
- Runtime for a query exceeds a specified number of minutes
- A query is blocked for more than a specified number of minutes

#### Query Text Download for Long Queries

On the **Query Details** page, if the query text is longer than 100K characters, Command Center only shows the first 100K characters and, when you click **COPY**, copies only the first 100K characters to the clipboard. When the query text is longer than 100K characters, Command Center adds a button, **Retrieve full query text**, which you can click to download a text file containing the entire text of the query. The file is available to download for 24 hours, or until the query is saved to history, when history collection is enabled.

## Fixed Issues

- 161436520 - Panels displaying help text can now be scrolled vertically when the text does not fit in the window.
- 158278655 - The displayed metrics for a query could be inaccurate if Command Center received the query “done” status before the final metrics arrived. Now the final metrics are updated even when they arrive after the “done” status.
- 161074984 - Repeated assertion errors logged in the `agent.log` file caused log files to grow quickly and consume too much disk space. This is fixed. Each type of assertion error will be logged no more than once every 10 minutes.
- 162114428 - When a user visits Command Center with a browser, the Command Center web server (gpccws process) establishes a websocket connection and runs two goroutines to service the websocket. When the websocket closes, one of the goroutines does not exit. After many connections the gpccws process can occupy gigabytes of memory. This memory leak is fixed.

## Enhancements and Changes in Greenplum Command Center 4.4.2

- The Greenplum Database metrics collector extension is now enabled only when Command Center agents are running. Previously, if an agent process terminated, the metrics collector continued to collect and send data.

Greenplum Command Center 4.4.2 contains the following resolved issues:

- 160195564 - When Command Center is restarted after a user has submitted a query, and the user submits another query in the same session, the database name and user name are missing from the second query in the Command Center interface. This is fixed.
- 161077294 - The Authentication view now prevents the user from saving an undefined entry to the `pg_hba.conf` file.
- 161274227 - The Command Center installer, `gpccinstall`, no longer prints errors to the `pg_log` log file about missing `iterators` and `emc_connect_history` tables.
- 161273865 - The Query Monitor no longer shows runtimes flashing to 0 seconds when a query is cancelled through the user interface.

## Enhancements and Changes in Greenplum Command Center 4.4.1

- The **Admin> Authorization** view allows entering host names in the **Address** field.
- On the visual query plan, a data motion showed a finished status when the send data operation completed. This is changed so that the node completes only after the corresponding data receive operation has also completed.
- Enabled cross-site request forgery prevention during login.

## Resolved Issues in Greenplum Command Center 4.4.1

- 160679694 - If Command Center is restarted while on the Query Monitor view and the browser is then refreshed, an extra web socket connection is created. This is fixed.
- MPP-29539 - Command Center agent (ccagent) logging is disabled for a known issue with PL/pgSQL queries.

## Enhancements and Changes in Greenplum Command Center 4.4.0

Greenplum Command Center 4.4.0 contains the following features and enhancements.

### Workload Management

- Command Center has a new user interface to assist administrators in enabling resource groups in Greenplum Database, importing existing resource queues to resource groups, and enabling workload management with Command Center. The option to import resource queues to resource groups is presented if no resource groups have been created (other than `default_group` and `admin_group`) and Greenplum Database has resource queues to convert (other than `pg_default`). Once the administrator has imported resource queues, or chosen to skip importing resource queues, the option to import queues is no longer presented.
- The resource group list on the Workload Management view has a new column to show the minimum (fixed) amount of memory that will be allocated to a query for each resource group. This value is recalculated when you enter new values while editing resource groups.
- Administrators can now define resource group assignment rules and idle session kill rules with an interactive interface. It is no longer necessary to edit the JSON document for workload management rules. The JSON text field is removed.
- The Workload Management view changed to a light theme.

## Permissions

- Command Center users with the Self Only permission level can:
  - see all queries on the query monitor, including queries owned by other users
  - cancel their own queries
  - access the query details view for their own queries
  - hover on a query to see query text for their own queries
  - hover on locking/blocking queries and access details of locking/blocking queries that do not belong to other users

Users with Self Only permission level cannot see query text or access the details views of others' queries.

- The Greenplum Database roles `gpcc_basic`, `gpcc_operator`, and `gpcc_operator_basic` are created during Command Center installation if they do not already exist.

## Query Monitor

- Fixed a bug where the database name and role name were missing from query details when queries are executed in a session after restarting Command Center.

## Enhancements and Changes in Greenplum Command Center 4.3.0

Greenplum Command Center 4.3.0 contains the following enhancements.

### Resource Group Management

The **Admin>Workload Mgmt** view has a new user interface you can use to add and remove resource groups and to change the Concurrency, CPU %, and Memory % attributes of resource groups.

### Resource Group Role Assignments

The **Admin>Workload Mgmt** view has a new user interface you can use to view and change Greenplum Database roles' default resource groups.

### Details Added to Visual Query Plan Steps

The metrics collector extension in Greenplum Database release 5.9 is updated to submit additional information about each step in the query plan to the Command Center backend. Command Center displays this information in the visual query plan when you expand a step in the query plan. The new information displayed depends on the operation the step performs and includes details such as hash key, merge key, join condition, or filter condition. Previously, you could only see this information by generating the textual query plan.

## Enhancements and Changes in Greenplum Command Center 4.2.0

Greenplum Command Center 4.2.0 contains the following enhancements.

### Visual Query Plan

The Command Center Query Details view now includes a visual query plan.

### Idle Session Kill Rules

Idle session kill rules can include optional `exemptedRoles` and `message` parameters.

- The value of the `exemptedRoles` parameter is a list of Greenplum Database roles that are exempted from the rule. The list can include Posix regular expressions to match Greenplum Database role names.

- The value of the `message` parameter is a string to include in the message that is displayed when a session is killed.

## Command Center Can Run on the Master Host or Standby Master Host

The Greenplum Command Center web server and backend may now be executed on the master host or on the standby master host. Running GPCC on the standby master host is recommended to avoid adding load to the master server, but it is no longer a requirement. After the GPCC software is installed, log in to the host where you want to run GPCC, source the `gpcc_path.sh` file in the GPCC installation directory, and run the `gpcc start` command.

## Enhancements and Changes in Greenplum Command Center 4.1.0

Greenplum Command Center 4.1.0 contains the following enhancements.

- Command Center administrators can set permission levels for Command Center users. Permissions are enforced as described in the documentation.
- On the **Query Detail** view, clicking **Copy** in the query text or query plan panel copies the text in the panel to the clipboard.
- A help icon and in-app help have been added on the **Query Monitor** and **Query Detail** views.

The following workload management features, improvements, and bug fixes have been added in the workload management extension included with Greenplum Database 5.8.0.

- On the **Admin>Workload Mgmt** view, you can add idle session kill rules for each resource group. When you add these rules, the Greenplum Database workload management extension kills a session after it has been idle for the number of seconds you specify. See [Workload Management](#) for syntax and examples.
- Optimizations have been implemented to reduce the impact on Greenplum Database when the workload management extension is disabled.
- The workload management extension takes advantage of resource group name-to-id caching added in Greenplum Database.
- Fixed a bug in the workload management extension that caused errors to print to the `psql` prompt, even when the extension was disabled.

Greenplum Command Center 4.1.0 contains the following bug fixes.

- In the **History Detail** view, when either of the **Disk R** or **Disk W** metrics is 0, both are reported to be 0. This is fixed.
- When using the Kerberos gpmon-only authentication mode, generating an explain plan failed. This is fixed.
- The Command Center agent failed with the message “Error: can’t find gpcc.query\_metrics\_port, metrics\_collector is not correctly installed.” This occurs when running Command Center on a Greenplum Database system that was upgraded from an earlier Greenplum Database 5.x release. The `metrics_collector` and `gp_wlm` extensions are installed with the upgrade, but the upgrade process does not perform the required configuration changes in the `postgresql.conf` configuration file. The Command Center installation instructions now include steps to manually configure and restart an upgraded Greenplum Database system.
- When Command Center starts, an error message is written in the Greenplum Database log file: “function gpcc\_schema.read\_pghba(unknown) does not exist.” This is fixed.
- A change to time zone handling in Greenplum Database 5.7 can cause Greenplum Command Center 4.0.0 to display an incorrect time if the master host operating system time and Greenplum Database use different time zones. Now Command Center times are displayed using the time zone of the Greenplum Database master host operating system. The current time, last sync time, and timestamps in alert logs, cluster metrics, and query history are all displayed using the master host’s system time zone.
- On the **Admin> Authorization** view, when the authorization method is `gss` and the options field contains text, changing the method to `trust` does not clear the options field and it is not possible to save changes to the `pg_hba.conf` file.
- The Command Center web server, `gpccws`, spawns ssh processes but does not reap them in a timely manner, leading to many zombie processes. This is fixed.
- On the **Admin> Authentication** view, if the number of users listed in the user column is longer than can be displayed, Command Center truncates the list and adds ellipsis ( `...` ) to the end. Only administrators can view the complete value, by editing the field. Now any user with access to the view can see the full list of users by hovering over the field.

## Enhancements and Changes in Greenplum Command Center 4.0.0



## Command Center Installation Changes

Greenplum Command Center 4.x software, unlike previous releases, is installed on every host in the Greenplum Database cluster. The Command Center web server and backend run on the standby master, if your Greenplum Database cluster has a standby master. If there is no standby master, Command Center runs on the master host instead.

To modify the Command Center installation—for example to enable or disable SSL or install Command Center on new or replaced hosts—just re-execute the installer and restart Command Center. It is not necessary to uninstall Command Center before reinstalling.

There is one Command Center installation per Greenplum Database cluster. It is no longer necessary to create Command Center instances after installing the software.

The `gpccmdr` command-line utility is replaced with the new `gpcc` utility. Use the `gpcc` utility to start and stop Command Center and metrics collection agents, check Command Center status, and enable or disable Kerberos authentication.

In previous releases, the `gpmon` role required only local connections to databases on the Greenplum master host. In Greenplum Command Center 4.x, the `gpmon` user must be able to connect to databases from the host running the Command Center web server and backend, which requires adding a host entry to the `pg_hba.conf` authentication configuration file.

## Real-time Query Metrics

Greenplum Command Center 4.0 introduces real-time query metrics for Pivotal Greenplum Database 5.7 and above. This new feature combines the following new features in Greenplum Database and Greenplum Command Center:

- Greenplum Database saves query execution metrics in shared memory while queries execute.
- A new Greenplum Database metrics collection extension, included with Pivotal Greenplum Database, emits the saved metrics as UDP datagrams.
- A new Greenplum Command Center metrics collection agent running on each Greenplum Database host receives the datagrams and posts metrics to the Greenplum Command Center backend. The Command Center backend starts and manages the metrics collection agents.

The Command Center Query monitor view updates in real time so you can see queries that are waiting to execute and the current status and resource usage for queries that are running.

Metrics collection now includes lock and spill file information. On the Query Monitor, you can see which queries are blocked and which queries hold the locks blocking them. The Query Monitor shows the total size of spill files created on all segments for each query.

Installing the `gpperfmon` database remains a prerequisite for Command Center. The `gpperfmon` database is the source for query history displayed in the Command Center user interface. The new real-time metrics are not persisted and are not directly related to the metrics collected and persisted in the `gpperfmon` database.

## Workload Management

Workload management is now an integrated Command Center feature rather than a separate product. Workload management is available in Command Center only after resource groups have been enabled in Greenplum Database by changing the `gp_resource_manager` server configuration parameter from `'queue'` to `'group'` and enabling Linux control groups (cgroups).

In Command Center 4.0, workload management allows you to assign transactions to Greenplum Database resource groups at execution time by evaluating the current database role and *query tags* against workload assignment filters you define in Command Center. Query tags are user-defined `name=value` parameters that you define in the `gpcc.query_tags` database session parameter. You can define multiple query tags separated by semicolons. Set query tags in a Greenplum Database session either as a parameter in the database connection URL or by executing

```
SET gpcc.query_tags TO '<tag1>=<val1>;<tag2>=<val2>;...' in the database session.
```

When a transaction is about to execute, the current database role and query tags are compared to the workload assignment filters that you have created in Command Center. If a match is found, the transaction is assigned to a resource group according to the workload management filter. Otherwise, the transaction is assigned to the database user's resource group, which is the default behavior when Command Center workload management is not enabled.

Workload management uses the `gp_wlm` database extension included with Pivotal Greenplum Database.

## Unimplemented Features

Some features available in previous Greenplum Command Center releases have been removed or are not yet implemented in Command Center 4.x.

- The ability for a Command Center admin to post a message to the Query Monitor view is not yet implemented.
- The multi-cluster view has been removed.

## Known Issues

The following are known issues in the current Greenplum Command Center release.

### Unable to View Real Time Queries After Upgrading From a Previous Command Center Release

If you install a new version of Greenplum Command Center using the same port number as the previous version, and you use the Chrome web browser, you may be unable to view real-time queries until after you clear the browser's cache. See the note in [Connecting to the Command Center Console](#) for steps to clear the browser cache.

## About Pivotal Greenplum Command Center

Pivotal Greenplum Command Center is a management tool for the Pivotal Greenplum Database Big Data Platform. This topic introduces key concepts about Greenplum Command Center and its components.

## Greenplum Command Center Features

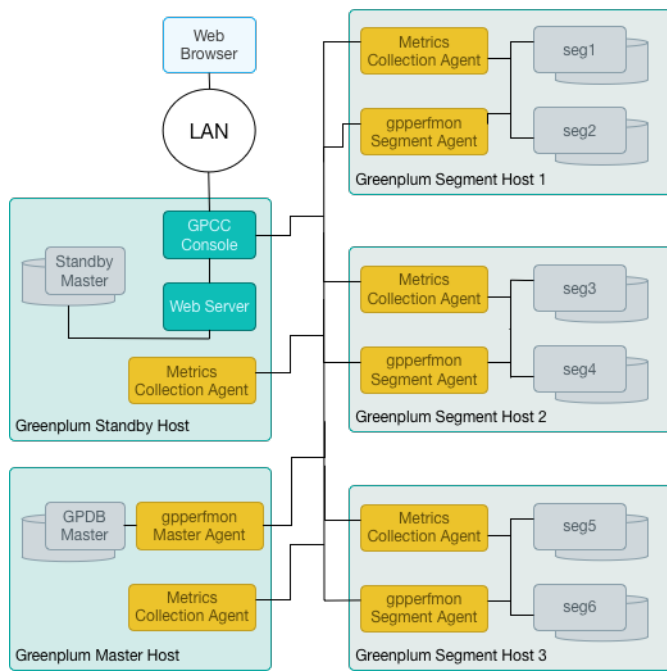
Greenplum Command Center monitors system performance metrics, analyzes cluster health, and enables database administrators to perform management tasks in a Greenplum Database environment.

Greenplum Command Center provides a browser-native HTML5 graphical console for viewing Greenplum Database system metrics and performing certain database administrative tasks. The Command Center application provides the following functionality:

- Interactive overview of realtime system metrics. Drill down to see details for individual cluster hosts and segments.
- Detailed realtime statistics for the cluster and by server.
- Query Monitor view lists queries executing, waiting to execute, and blocked by locks held by other queries.
- Query Detail view shows query metrics, query text, and the execution plan for the query.
- Workload Management view allows administrators to:
  - Create and manage workloads to manage concurrency and allocate CPU and memory resources.
  - Change default resource groups for Greenplum Database roles.
  - Create assignment rules to assign transactions to resource groups.
  - Create idle session timeout rules to set the amount of time before an idle session is killed.
- Four permission levels allow users to view or cancel their own or others' queries, and to view or manage administrative information.
- Cluster Metrics view shows synchronized charts of historical system metrics.
- History view lists completed queries and system metrics plotted over a selected time period.
- Permissions view to see or manage Command Center permission levels.
- Authentication view to see or edit the `pg_hba.conf` host-based authentication configuration file.
- Segment Status view with summaries and details by segment.
- Storage Status view with summaries and details by segment data directory.

## Greenplum Command Center Architecture

The following figure illustrates the Greenplum Command Center architecture.



## Greenplum Command Center Web Server and Web Application

The Greenplum Command Center web server and backend application can run on the master, standby master, or any segment host in the Greenplum Database cluster—the standby master host is recommended. The web server, gpccws, is a custom HTTP server designed for Command Center. The web application is an HTML5 and Go language application.

The Command Center web server authenticates users with the Greenplum Database authentication system. Administrators can edit the Greenplum Database host-based authentication file, `pg_hba.conf`, in the Command Center Console. Command Center can also be configured to authenticate users in a Kerberos environment.

Command Center defines four user authorization levels to manage users' access to the Query Monitor, and to administrative information and operations. User authorization is managed in the Administrative area of the Command Center user interface.

Greenplum Command Center displays information derived from several sources:

- Greenplum Database performance monitoring database (gpperfmon)
- Operating system process accounting
- Greenplum Database system catalog tables
- Real-time query metrics collection extension
- Workload management extension

Greenplum Database is instrumented to enable capturing performance metrics and tracking query execution. The performance monitoring database and the query metrics collection extension deploy agents—processes running on each host to collect metrics. The gpperfmon agents forward collected data to an agent on the Greenplum Database master. The real-time query metrics agents submit collected data directly to the Command Center rpc port. The agents also collect data from the host operating system so that query performance can be correlated with CPU and memory utilization and disk space can be monitored in Command Center.

## Greenplum Database Performance Monitoring Database

The gpperfmon performance monitoring database stores current and historical query status and system information collected from agents running on the master and segment hosts. Greenplum Command Center uses gpperfmon for historical data only; it uses the real-time query metrics to monitor active and queued queries. Greenplum Database sends UDP packets at various points during query execution. The `gpsmon` process on each segment host collects the data. Periodically, every 15 seconds by default, a `gpmmon` agent on the master host signals the `gpsmon` process to forward the collected data. The agent on the master host receives the data and adds it to the gpperfmon database.

The Command Center database consists of three sets of tables:

- `now` tables store data on current system metrics such as active queries

- *history* tables store data on historical metrics
- *tail* tables are for data in transition. Tail tables are for internal use only and should not be queried by users.

The now and tail data are stored as text files on the master host file system, and the Command Center database accesses them via external tables. The history tables are regular database tables stored within the gpperfmon database.

You can run SQL queries on the data stored in the gpperfmon database. Greenplum Command Center runs queries on the database for information presented in the Command Center Console. The *Greenplum Database Reference Guide* contains references for the tables in the gpperfmon database.

Greenplum Database provides a management utility, `gpperfmon_install`, to create the gpperfmon database and enable the gpperfmon agents on the master and segment hosts. Creating the gpperfmon database is a prerequisite for installing Greenplum Command Center. See the *Greenplum Database Utility Guide* for details of running the `gpperfmon_install` management utility.

## Real-Time Query Metrics Collection

The data collected by real-time query metrics collection is more detailed and more current than statistics recorded in the gpperfmon database. Command Center users can observe queries as they execute and, with sufficient permissions, cancel problem queries to allow other queries to complete.

The Greenplum Database query metrics extension and the metrics collection agent work together to collect real-time metrics and update the Command Center application.

Greenplum Database calls the query metrics extension when a query is first submitted, when a query's status changes, and when a node in the query execution plan initializes, starts, or finishes. The query metrics extension sends metrics to the metrics collection agent running on each segment host. The extension also collects information about the locks queries hold so that you can see which queries hold locks that block other queries. The agent posts the metrics to the Greenplum Command Center rpc port.

The `metrics_collection` extension is included with Pivotal Greenplum Database. The extension is enabled by setting the `gp_enable_query_metrics` server configuration parameter to on and restarting the Greenplum Database cluster. The metrics collection agent is installed on each host when you install Greenplum Command Center. The Command Center application monitors the agent and restarts it if needed.

## Command Center Workload Management

Workloads set concurrency, memory, and CPU resource limits for database transactions they manage. A Greenplum Command Center workload corresponds to a Greenplum Database resource group, but adds additional capabilities that are not available with resource groups.

Command Center allows administrators greater flexibility in assigning transactions to workloads. Every Greenplum Database role is assigned to a single resource group and, by default, transactions are managed by the role's resource group. With Command Center workload management, administrators can define criteria to assign transactions to workloads based on attributes other than the role submitting the transaction. Currently, assignment criteria can evaluate query tags and roles in combination with query tags.

A *query tag* is a key-value pair defined in the `gpcc.query_tags` parameter of a database session. The parameter has the format `<tag1>=<value1>;<tag2>=<value2>`, where tags and values are user-defined values. For example, if you want to run ETL operations in a workload named "etl", you could define a tag named "xact-type" and set it to "etl": `xact-type=etl`. The `gpcc.query_tags` parameter can be set as a connection parameter on Greenplum Database clients that allow it, or with a `SET` command inside the session after the connection has been established, for example

```
SET gpcc.query_tags='xact-type=etl'.
```

The `gp_wlm` extension in Pivotal Greenplum Database provides support for Command Center workloads. The extension is included with Pivotal Greenplum Database, but is not enabled by default. Initially, Greenplum Database uses resource queues to manage resources. Using Command Center workloads requires enabling resource groups in Greenplum Database. Resource groups are based on the Linux control groups (cgroups) service, which must first be enabled in the operating system.

## Installing the Greenplum Command Center Software

This section contains the following topics:

- [Creating the gpperfmon Database](#)
- [Installing Greenplum Command Center](#)
- [Upgrading Greenplum Command Center](#)
- [Uninstalling Greenplum Command Center](#)
- [Setting the Command Center Environment](#)

## Creating the gpperfmon Database

This topic describes how to create the Command Center gpperfmon database and enable the gpperfmon data collection agents. This task must be completed one time for the Greenplum Database system, before you install Greenplum Command Center.

When the data collection agents are enabled, their processes are started and stopped (using `gpstart` and `gpstop`) on the Greenplum segment hosts along with the Greenplum Database server processes.

Greenplum Database includes a `gpperfmon_install` utility that performs the following tasks:

- Creates the Command Center database (gpperfmon).
- Creates the Command Center superuser role (`gpmon`).
- Configures Greenplum Database server to accept connections from the `gpmon` role (edits the `pg_hba.conf` and `.pgpass` files).
- Sets the Command Center server configuration parameters in the Greenplum Database server `postgresql.conf` files.

The `gpperfmon_install` utility and the agents are part of the Greenplum Database software. The tasks in this topic can be performed before or after the Command Center software is installed.

## Enabling the Collection Agents

1. Log in to the Greenplum master host as the `gpadmin` user.

```
$ su - gpadmin
```

2. Source the path file from the Greenplum Database installation directory:

```
# source /usr/local/greenplum-db/greenplum_path.sh
```

3. Run the `gpperfmon_install` utility with the `--enable` option. You must supply the connection port of the Greenplum Database master server process, and set the password for the `gpmon` superuser that will be created. For example:

```
$ gpperfmon_install --enable --password changeme --port 5432
```

### Note:

The `gpperfmon_install` utility creates entries for the `gpmon` user in the `$MASTER_DATABASE/pg_hba.conf` file. See [gpmon User Authentication](#) for notes about restricting the gpmon user's access to databases.

The password you specify is saved in a `.pgpass` file in the `gpadmin` user's home directory. See [Changing the gpmon Password](#) for steps to change the `gpmon` password.

4. When the utility completes, restart Greenplum Database server. The data collection agents do not start until the database is restarted.

```
$ gpstop -r
```

5. Using the `ps` command, verify that the data collection process is running on the Greenplum master. For example:

```
$ ps -ef | grep gpmon
```

6. Run the following command to verify that the `gpmon` user can authenticate and that the data collection processes are writing to the Command Center database. If all of the segment data collection agents are running, you should see one row per segment host.

```
$ psql -U gpmon gpperfmon -c 'SELECT * FROM system_now;'
```

The data collection agents are now running, and your Greenplum system now has a gpperfmon database installed. This is the database where historical Command Center data is stored. You can connect to it as follows:

```
$ psql gpperfmon
```

## Configuring a Standby Master Host (if enabled)

1. Copy the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file from your primary master host to your standby master host. This ensures that the required connection options are also set on the standby master.
2. Copy your `~/.pgpass` file from your primary master host to your standby master host. This file usually resides in the `gpadmin` user's home directory. Note that the permissions on `.pgpass` must be set to 600 (for example: `chmod 0600 ~/.pgpass`).

## gpmon User Authentication

The `gpperfmon_install` utility adds entries for the `gpmon` user to the `pg_hba.conf` file, which allows the `gpmon` user to make a local connection to any database in the Greenplum cluster.

```
local  gpperfmon gpmon      md5
host   all      gpmon      127.0.0.1/28 md5
host   all      gpmon      ::1/128  md5
```

For Greenplum Command Center, the `gpmon` user must also have host access from the host where the Command Center web server and backend run. This requires that you add an entry for the Command Center host. Edit the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file and add a line like the following.

```
host   all      gpmon      <cc-host-ip>/32 md5
```

Since the `gpmon` role is a Greenplum Database superuser, you may wish to restrict the role from accessing other databases. Edit these lines:

List `gpperfmon` and the databases you want to monitor with Command Center in the second field:

```
local  gpperfmon,userdb1,userdb2 gpmon      md5
host   gpperfmon,userdb1,userdb2 gpmon      127.0.0.1/28 md5
host   gpperfmon,userdb1,userdb2 gpmon      ::1/128  md5
host   gpperfmon,userdb1,userdb2 gpmon      <cc-host-ip>/32 md5
```

See [Changing the gpmon Password](#) for steps to change the `gpmon` user's password.



## Installing Pivotal Greenplum Command Center

The Pivotal Greenplum Command Center installation utility installs the Command Center files on all hosts in the Greenplum Database cluster.



Run the Greenplum Command Center installer on the Greenplum Database master host. The installer installs the Command Center software on every host in your Greenplum Database cluster. It retrieves the list of hosts in your Greenplum Database cluster from the `gp_segment_configuration` system table.

After you have run the installer you can start Greenplum Command Center on the master host or on the standby master host. Running Command Center on the standby master avoids adding load to the master host.

## Prerequisites

Before installing Greenplum Command Center, ensure the following requirements are met:

- Greenplum Database must be installed and running. See the Pivotal Greenplum Command Center release notes for compatible Greenplum Database versions.
- The Greenplum Database `MASTER_DATA_DIRECTORY` environment variable must be set.
- The gpperfmon database and gpmon role must be created and the gpperfmon agents must be running. See [Creating the gpperfmon Database](#).
- The directory where Greenplum Command Center will be installed, `/usr/local/` by default, must be writable by the gpadmin user on all Greenplum Database hosts. Alternatively, you can install Command Center as root and, when done, change ownership of all files in the installation directory to the gpadmin user. See [Selecting and Preparing an Installation Directory for Command Center](#) for options.



**Important!** If you upgraded to Pivotal Greenplum Database release 5.7 or later from an earlier Greenplum Database 5.x release, you must follow steps at [Set Up the Metrics Collection and Workload Management Extensions](#) before you start Greenplum Command Center.

## Prepare the Standby Master Host

After the Command Center software is installed, you start the Command Center web server and backend on the standby master host or on the master host. Some preparation is required to enable Command Center to run on the standby master host.

1. On the master host, edit the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file and add the following entry to allow the gpmon user to authenticate from any host in the Greenplum Database cluster.

```
host all gpmon <IP_of_host>/32 md5
```

Run `gpstop -u` to have Greenplum Database reload the file.

2. Copy the `.pgpass` file from the master host to the standby master host. Run these commands from the master:

```
$ ssh gpadmin@<standby_host>
$ scp gpadmin@<master_host>:~/.pgpass ~
$ chmod 600 ~/.pgpass
```



**NOTE** There are two alternative methods you can use to supply the gpmon user's password so that you do not have to put the `.pgpass` file on the host. Command Center only requires the gpmon password when you run `gpcc start`, `gpcc stop`, or `gpcc status`.

1. Set the `PGPASSWORD` environment variable before you run `gpcc` commands. Example:

```
$ PGPASSWORD=changeme gpcc status
```

2. Add the `-W` option to `gpcc` commands to have the command prompt you for the password. Example:

```
$ gpcc start -W
```

3. If the Greenplum Command Center web server is to support TLS/SSL, a server certificate must be obtained and installed on the Command Center host in a location readable by the `gpadmin` user. The default path is `/etc/ssl/certs/cert.pem`.
4. If Greenplum Command Center is to support Kerberos authentication, Greenplum Database must have Kerberos authentication set up and the required principals and keytabs must be installed on the Command Center host. See [Enabling Authentication with Kerberos](#) for Kerberos setup instructions. You can install Command Center without Kerberos authentication initially and then enable Kerberos later by running the `gpcc krbenable` command.

## Selecting and Preparing an Installation Directory for Command Center

The Command Center installation directory must exist and be writable on every host in the Greenplum Database cluster by the Linux user who runs the Command Center installer. That user must also have passwordless ssh access to all hosts in the cluster. The Command Center installer creates a directory named `greenplum-cc-web-<version>` in the installation directory on every host in the Greenplum Database cluster. When Command Center installation is complete the `greenplum-cc-web-<version>` directory and all of its contents must be owned by the `gpadmin` user.

The default installation directory for Command Center is `/usr/local`. In a standard Linux system, the `/usr/local` directory is owned by `root` and is only writable by `root`. If you choose the default installation directory or another directory where `gpadmin` does not have write permission, you can use one of the following methods to install Command Center.

- Temporarily change permissions on the installation directory to allow the `gpadmin` user to install Command Center.
- As `root`, create the `greenplum-cc-web-<version>` directory in the installation directory on all hosts in the Greenplum Database cluster and change the directory's ownership to `gpadmin`.
- Run the Command Center installer as `root` and then change the ownership of the `greenplum-cc-web-<version>` directory and its contents to `gpadmin`.

All of these options require `root` to execute shell commands on every Greenplum Database host. The Greenplum Database utilities `gpssh-exkeys` and `gpssh` make this much easier.

## Setting up Passwordless ssh for the root User

The root user must have passwordless ssh access to all Greenplum Database hosts in order to run the Command Center installer or to execute shell commands on Greenplum hosts using the `gpssh` utility. Follow this procedure to set up passwordless ssh access with the `gpssh-exkeys` utility.

1. Log in to the master host as the `root` user.
2. Create a text file, for example `allhosts.txt`, containing a list of all Greenplum Database cluster hosts, including the master and standby master host, one name per line.
3. Source the Greenplum Database environment setup script in the Greenplum Database installation directory.

```
# source /usr/local/greenplum-db-<version>/greenplum-db_path.sh
```

4. Run the `gpssh-exkeys` utility, specifying the hosts file with the `-f` option.

```
# gpssh-exkeys -f allhosts.txt
```

## Create the Installation Directory and Install Command Center Software

Create the Command Center installation directory on all Greenplum Database hosts and assign permissions so that you can run the Command Center installer as the `gpadmin` user.

1. Log in to the master host as the `root` user.
2. Source the Greenplum Database environment setup script in the Greenplum Database installation directory.

```
# source /usr/local/greenplum-db-<version>/greenplum-db_path.sh
```

3. Use the `gpssh` utility to create the directory and set ownership on all hosts.

```
# gpssh -f allhosts.txt
=> mkdir /opt/greenplum-cc-web-4.4.0
=> chown gpadmin:gpadmin /opt/greenplum-cc-web-4.4.0
=> exit
```

- As the `gpadmin` user, run the Command Center installer as described in [Installation Steps](#). When prompted for the installation directory, enter `/opt`.

## Change Ownership of the Command Center Directory Post-Installation

If you instead installed Command Center installer as the `root` user, then you must follow these steps to change the ownership of the installation directory and its contents to the `gpadmin` user. This example assumes you have installed Command Center as `root` in the `opt` directory, following the steps in [Installation Steps](#). The files in the `greenplum-cc-web-<version>` directory and its contents are currently owned by `root`.

- Log in to the master host as `root`.
- Source the Greenplum Database environment setup script in the Greenplum Database installation directory.

```
# source /usr/local/greenplum-db-<version>/greenplum-db_path.sh
```

- Run the following commands, providing the path to your Command Center installation.

```
# gpssh -f allhosts.txt
=> chown -R gpadmin:gpadmin /opt/greenplum-cc-web-<version>
exit
```

Now you can log in to the standby master or master host as `gpadmin` and start Command Center.

## Installation Steps

You can run the Greenplum Command Center installer on the Greenplum Database master host. The software will be copied to all other hosts in the cluster.

Perform these steps as the `gpadmin` user, if `gpadmin` has write permission in the installation directory, or as `root`.

If you install Command Center as `root`, make sure `root` has passwordless ssh access to all hosts in the Greenplum Database cluster. (See [Setting up Passwordless ssh for the root User](#).) When installation is complete, be sure to change the ownership of the Greenplum Command Center directory and contents to `gpadmin`. (See [Change Ownership of the Command Center Directory Post-Installation](#).)

- Download Greenplum Command Center 4.x from [Pivotal Network](#).
- Extract the installer from the zip file.

```
$ unzip greenplum-cc-web-<version>-LINUX-x86_64.zip
```

Extracting the installer creates a `greenplum-cc-web-<version>` directory containing the `gpccinstall-<version>` installation utility.

- Source the `greenplum_path.sh` script in the Greenplum Database installation directory to ensure the `GPHOME` environment variable is set.

```
$ source /usr/local/greenplum-db/greenplum_path.sh
```

- Run the Greenplum Command Center installer.

```
$ cd greenplum-cc-web-<version>
$ ./gpccinstall-<version> -W
```

The installer has three options.

- The `-c <config-file>` option specifies the path to an installation configuration file to use for a non-interactive installation. See [Install with a Configuration File](#).
- The `-w` option instructs the installer to prompt for the gpmon user's password. The installer attempts to retrieve the gpmon password from the `PGPASSWORD` environment variable, if set, or from the `~gpadmin/.pgpass` file, if present. If neither of these options is available, include the `-W` option to instruct the installer to prompt for the password.

- The `--ssh_path` option allows you to specify the full path to a custom ssh program. If you do not supply this option, the installer uses the ssh command on the path.

```
$ ./gpccinstall-<version> --ssh_path /usr/local/bin/ssh -W
```

5. Read through the license agreement and enter `y` to accept.

6. **Where would you like to install Greenplum Command Center?**

The default installation directory is `/usr/local`. Press Enter to accept the default or enter the desired path. The directory must exist on all hosts in the Greenplum Database cluster and must be writable by gpadmin.

7. **What would you like to name this installation of Greenplum Command Center?**

Enter a name to display on Command Center web pages to identify this Greenplum Database system.

8. **On which port would you like to install the Greenplum Command Center web server?**

The default Command Center listen port is 28080. Press Enter to accept the default or enter another port number.

9. **Would you like to enable SSL?**

Enter `y` if you want to enable SSL/TLS (HTTPS) encryption for client connections to the Command Center web server. The installation utility prompts for the location of the SSL certificate.

**Provide the file path for the SSL certificate**

Enter the path to the certificate installed on the Command Center host. The default is `/etc/ssl/certs/cert.pem`. The certificate must be readable by the gpadmin user.

10. **Would you like to enable Kerberos?**

Enter `y` if you want to enable client authentication with Kerberos. Kerberos must already be enabled for Greenplum Database. (If you enter `n`, you can set up Kerberos authentication later using the `gpcc krbenable` command.) The installer prompts for information about your Kerberos installation.

**Choose Kerberos mode (1.normal/2.strict/3.gpmon\_only)**

Greenplum Command Center supports three different Kerberos authentication schemes.

**1 - normal mode** (default) – The Command Center Kerberos keytab file contains the Command Center principal and may contain principals for Command Center users. If the principal in the client's connection request is in the Command Center's keytab file, Command Center uses the client's principal for database connections. Otherwise, Command Center uses the `gpmon` user for database connections.

**2 - strict mode** – Command Center has a Kerberos keytab file containing the Command Center service principal and a principal for every Command Center user. If the principal in the client's connection request is in the keytab file, the web server grants the client access and the web server connects to Greenplum Database using the client's principal name. If the principal is not in the keytab file, the connection request fails.

**3 - gpmon\_only mode** – Command Center uses the `gpmon` database role for all Greenplum Database connections. No client principals are needed in the Command Center's keytab file.

**Provide the path to the keytab file**

Enter the path to the keytab file containing the Kerberos principal for the Command Center web server and, optionally, Command Center user principals.

**What is the name of the GPDB Kerberos service?**

The default service name for Greenplum Database is `postgres`. You can check the value of the service name for your Greenplum Database cluster with the `gpconfig` utility:

```
$ gpconfig -s krb_srvname
```

**What is the URL of the Command Center web server?**

The Kerberos keytab file must contain a principal for the Command Center web server. The principal name is of the format `HTTP/<gpcc-host>@<realm>`, where `<gpcc-host>` is the host name clients use in URLs when connecting to the Command Center web server.

If you ran the installer as `root`, change the ownership of the Greenplum Command Center directory and contents to `gpadmin`. See [Change Ownership of the Command Center Directory Post-installation](#).

## Install With a Configuration File

You can provide a configuration file to the Greenplum Command Center installer to perform a non-interactive Command Center installation. Note that you must still view and accept the license agreement.

```
$ cd greenplum-cc-web-<version>
$ ./gpccinstall-<version> -c <config-file> -W
```

The following table contains the names of the parameters corresponding to the interactive installation prompts and their default values. Define parameters in a configuration file for any parameters that have no default value or to override default values.

Installer Prompt	Default	Parameter
Where would you like to install Greenplum Command Center?	/usr/local	path
What would you like to name this installation of Greenplum Command Center?	gpcc	display_name
On which port would you like to install the Greenplum Command Center web server?	28080	web_port
Would you like to enable SSL?	false	enable_ssl
Please provide the file path for the SSL certificate:	/etc/ssl/certs/cert.pem	ssl_cert_file
Would you like to enable Kerberos?	false	enable_kerberos
Choose Kerberos mode (1.normal/2.strict/3.gpmon_only):	1	krb_mode
Please provide the path to the keytab file:		keytab
What is the name of the GPDB Kerberos service?	postgres	krb_service_name
What is the URL of the Command Center web server?	gpcc	webserver_url

If the `enable_ssl` parameter is true, the `ssl_cert_file` parameter is required.

If the `enable_kerberos` parameter is true, the `keytab` parameter is required and the `webserver_url`, `krb_mode`, and `krb_service_name` must be set to values from your Kerberos installation.

The following installation configuration file example sets all parameters to their default values.

```
path = /usr/local
# Set the display_name param to the string to display in the GPCC UI.
# The default is the hostname of the Greenplum master host
# display_name = localhost

master_port = 5432
web_port = 28080
rpc_port = 8899
enable_ssl = false
# Uncomment and set the ssl_cert_file if you set enable_ssl to true.
# ssl_cert_file = /etc/certs/mycert
enable_kerberos = false
# Uncomment and set the following parameters if you set enable_kerberos to true.
# webserver_url = <webserver_service_url>
# krb_mode = 1
# keytab = <path_to_keytab>
# krb_service_name = postgres
```

## Set Up Command Center and Workload Management Extensions

You must follow the steps in this section only if you have upgraded your Pivotal Greenplum Database system from a 5.x release earlier than 5.7.0.

The Greenplum Database metrics collection and workload management extensions are installed when you upgrade to Pivotal Greenplum Database 5.7.0 or later. However, the upgrade procedure preserves your previous `postgresql.conf` configuration file, so you must manually set the server configuration parameters that enable the extensions. You must restart Greenplum Database if you change any configuration parameters.

To set up the Command Center and workload management extensions, log in to the master host as `gpadmin` and follow these steps.

1. Add the metrics collector and workload management shared libraries to the `shared_preload_libraries` configuration parameter. Check the current value of the `shared_preload_libraries` configuration parameter.

```
$ gpconfig -s shared_preload_libraries
Values on all segments are consistent
GUC      : shared_preload_libraries
Master value:
Segment value:
```

Add the Command Center and workload management libraries to the parameter. (If there were existing libraries in the parameter, append the new libraries, separated with a comma.)

```
$ gpconfig -c shared_preload_libraries -v '$libdir/metrics_collector,$libdir/gp_wlm'
```

2. Make sure the `gp_enable_query_metrics` configuration parameter is on.

```
gpconfig -s gp_enable_query_metrics  
gpconfig -c gp_enable_query_metrics -v on
```

3. If you changed any configuration parameters, restart Greenplum Database.

```
gpstop -r
```

## Next Steps

- [Setting the Greenplum Command Center Environment](#)
- [Starting and Stopping Greenplum Command Center](#)
- [Connecting to Greenplum Command Center](#)

## Upgrading Greenplum Command Center

To upgrade Greenplum Command Center, you install the new Command Center software release, stop the old version, and start the new version. You can then remove the older Command Center release from your Greenplum Database hosts.

### Upgrading From Greenplum Command Center 3.x to 4.x

The Greenplum Command Center architecture changed between Command Center 3.x and 4.x.

With Command Center 3.x, you installed the Greenplum Command Center software one time on the Command Center host. You then created a Command Center instance for each Greenplum Database cluster you monitored with Command Center.

Command Center 4.x does not have instances; you install the Command Center software on the master or standby master of the Greenplum Database cluster you want to monitor with Command Center. The installer copies the software to every host in the Greenplum Database cluster. To monitor additional Greenplum Database clusters you must install the Command Center software again, on a different master or standby host. Monitoring multiple Greenplum Database clusters running on the same hardware cluster is not supported.

To upgrade to a new release of Greenplum Command Center 4.x:

1. Download and install the new Command Center release by following the instructions in [Installing Greenplum Command Center](#).

2. Stop the current Command Center release.

Command Center 3.x:

```
$ gpccmdr --stop <instance_name>
```

Command Center 4.x:

```
$ gpcc stop
```

3. Source the `gpcc_path.sh` script in the new Command Center installation directory.

```
$ source /usr/local/greenplum-cc-web-<version>/gpcc_path.sh
```

**Note:** Also update the source command in your shell start-up script, for example `~/bashrc.sh` or `~/bash_profile.sh`.

4. Start the new Command Center release.

```
$ gpcc start
```

5. Uninstall the older Command Center release. See “Uninstalling Greenplum Command Center” in the Greenplum Command Center documentation for the release you are uninstalling.

## Uninstalling Greenplum Command Center

To uninstall Greenplum Command Center, you must stop both the Command Center Console and disable the data collection agents. Optionally, you may also remove any data associated with Greenplum Command Center by removing your Command Center Console installation and the gpperfmon database.

1. Stop Command Center Console if it is currently running. For example:

```
$ gpcc --stop
```

2. Remove the Command Center installation directory from all hosts. For example:

```
$ rm -rf /usr/local/greenplum-cc-web-version
```

3. Disable the data collection agents.

- a. Log in to the master host as the Greenplum administrative user (`gpadmin`):

```
$ su - gpadmin
```

- b. Disable the data collection agents by setting the `gp_enable_gpperfmon` server configuration parameter off:

```
$ gpconfig -c gp_enable_gpperfmon -v off
```

- c. Remove or comment out the gpmon entries in `pg_hba.conf`. For example:

```
#local  gpperfmon  gpmon  md5
#host   gpperfmon  gpmon  0.0.0.0/0  md5
```

- d. Drop the Command Center superuser role from the database. For example:

```
$ psql template1 -c 'DROP ROLE gpmon;'
```

- e. Restart Greenplum Database:

```
$ gpstop -r
```

- f. Clean up any uncommitted Command Center data and log files that reside on the master file system:

```
$ rm -rf $MASTER_DATA_DIRECTORY/gpperfmon/data/*
$ rm -rf $MASTER_DATA_DIRECTORY/gpperfmon/logs/*
```

- g. If you do not want to keep your historical Command Center data, drop the gpperfmon database:

```
$ dropdb gpperfmon
```



## About the Command Center Installation

The installation procedure creates a software installation directory for Greenplum Command Center. This directory is copied to all hosts in the Greenplum Cluster. Versions of Greenplum Database that are compatible with Greenplum Command Center include pre-packaged files that support the Command Center real-time metrics and workload management features.

## Software Installation Directory

The following files and first-level subdirectories are copied into the installation directory you specify when you install Greenplum Command Center. This location can be referenced with the `$GPCC_HOME` environment variable when you have [set the Command Center environment](#).

- `gpcc_path.sh` – file containing environment variables for Greenplum Command Center
- `bin/` – program files for Greenplum Command Center
  - `gpcc-agent` – real-time query metrics collection agent
  - `gpccws` – the Greenplum Command Center web server
  - `static/` – static files for the Command Center application
- `conf/`
  - `app.conf` – configuration file for the Command Center web server
- `logs/` – web server access and error log files
- `open_source_licenses_GPCC.txt` – licenses for open source components used by Greenplum Command Center

## Greenplum Database Artifacts

The Command Center real-time metrics and workload management features depend on the `gp_wlm` and `metrics_collection` Greenplum Database extensions. These extensions are included with compatible versions of Greenplum Database.

## Setting the Greenplum Command Center Environment

To enable the `gpadmin` user to execute Command Center utilities such as `gpcc` at the command line, source the `gpcc_path.sh` file in the Greenplum Command Center installation directory. For example:

```
$ source /usr/local/greenplum-cc-web-<version>/gpcc_path.sh
```

The `gpcc_path.sh` script sets the `GPCC_HOME` environment variable to the Command Center installation directory and adds the `$GPCC_HOME/bin` directory to the path.

To automatically source the `gpcc_path.sh` each time you log in, add the above source command to your start-up script, for example `~/.bashrc` or `~/.bash_profile`.

## Connecting to the Greenplum Command Center Console

Sign in to the Command Center Console with a name and password. If the Guest Access to Query Monitor feature is enabled, you can sign in anonymously to see just the **Query Monitor** view.

Open the Command Center Console in a supported browser using the host name and port configured for the Command Center web server. For example, to open a secure Command Center connection on a host named `smdw` at port 28080, enter this URL into your browser:

`https://smdw:28080`

- If the **View Query Monitor** link is present, you can click it to view the **Query Monitor** page without signing in. This takes you immediately to the [Query Monitor](#) view. To access additional Command Center features, click **Sign In** on the **Query Monitor** view and sign in with a valid Command Center user name and password. If the link is not present on the sign-in page, a Command Center administrator has disabled the anonymous query monitor feature.
- To sign in as a Command Center user, enter the user name and password of a Greenplum role that has been configured to allow authentication to Greenplum Command Center, then click **Sign In**. This opens the **Dashboard** page of the Command Center Console, which provides a graphical system snapshot and a summary view of active queries. See the [Dashboard](#) for information about the Dashboard view.

### Note to Chrome Browser Users

If you install a new version of Greenplum Command Center using the same port number as the previous version, and you use the Chrome web browser, you may be unable to view real-time queries until after you clear the browser's cache. Follow these steps.

1. Choose **Settings** from the Chrome menu.
2. Scroll to the bottom and click **Advanced**.
3. Under **Privacy and security**, click **Clear browsing data**.
4. Click the **Basic** tab and select **Cached images and files**. You do not have to clear **Browsing history** or **Cookies and other site data**.
5. Click **CLEAR DATA** and then log in to Command Center.

## Administering the Command Center Web Server

The gpccws web server binary and web application files are installed in the `bin` directory of your Greenplum Command Center installation.

### Starting and Stopping the Web Server

Starting the Command Center Web Server runs the gpccws web server, starts the metrics collection agents on the segment servers, and starts a listener on the Command Center rpc port.

You can run the `gpcc` command as the gpadmin user on the standby master host (recommended) or on the master host.

To ensure the `gpcc` command is on your path, source the `gpcc_path.sh` file in the Command Center installation directory or add it to the startup script for your command shell. See [Setting the Greenplum Command Center Environment](#) for instructions.



#### NOTE

The `gpcc` command uses the gpmon role to connect to Greenplum Database. It looks for the gpmon password in the `PGPASSWORD` environment variable or in the `.pgpass` file in the gpadmin user's home directory. You can instead append the `-W` flag to the `gpcc` commands below to have `gpcc` prompt you to enter the password.

#### To start Greenplum Command Center

Log on to the standby master host or the master host.

To log on to the standby from the master host:

```
$ ssh <standby-host>
```

Source the Command Center environment variables.

```
$ source /usr/local/greenplum-cc-<version>/gpcc_path.
```

Start the Command Center web server and the metrics collection agents.

```
$ gpcc start
Starting the gpcc agents and webserver...
2018/03/22 17:35:06 Agent successfully started on 7/8 hosts
2018/03/22 17:35:06 View Greenplum Command Center at http://smdw:28080
```

#### To stop Greenplum Command Center

```
$ gpcc stop
2018/03/22 17:36:23 Gpcc webserver and metrics collection agents have been stopped. Use gpcc start to start them again
```

#### To check the Greenplum Command Center status

```
$ gpcc status
Starting the gpcc agents and webserver...
2018/03/22 17:36:55 Agent successfully started on 7/8 hosts
2018/03/22 17:36:55 View Greenplum Command Center at http://smdw:28080
```

See the [gpcc](#) reference page for full syntax for the `gpcc` command.

### Configuring the Command Center Web Server

The web server configuration file is stored in `$GPCC_HOME/conf/app.conf`. The parameters in this configuration file are set when you install Greenplum Command Center. The installer copies the Command Center installation directory, including this configuration file, to every Greenplum Database host.

See the *Web Server Parameters* section of [Configuration File Reference](#) for a description of the parameters in this file.

You can see a summary of the current configuration using the `gpcc --settings` command.

```
$ gpcc --settings
Install path: /usr/local
Display Name: gpcc
GPCC port: 28080
Kerberos: disabled
SSL: disabled
```

If you modify the file on one host you should copy it to every other host. Be sure to restart the web server after you change the configuration. Rather than modifying the configuration directly, you can just stop Command Center and re-run the `gpccinstall-<version>` installation command. This ensures the configuration is consistent on all hosts.

You can use the `gpcc krbenable` command to add Kerberos authentication to the Command Center configuration. See [Enabling Authentication with Kerberos](#) for details about setting up Kerberos on the Command Center host. The `gpcc krbenable` command prompts for the Kerberos principal names and artifacts and updates the configuration.

The `gpcc krbdisable` command removes Kerberos parameters from the Command Center configuration.

## Viewing and Maintaining Web Server Log Files

Web server access and error log messages are written to `$GPCC_HOME/logs/gpccws.log`.

If you experience errors viewing the Greenplum Command Center Console, refer to this file for more information.

To prevent the web server log from growing to excessive size, you can set up log file rotation using `logrotate` or `cronolog`.

## Administering Command Center Agents

The Command Center metrics collection agent, `ccagent`, runs on segment hosts and receives real-time metrics emitted by the metrics collection database extension. Each segment host has one `ccagent` process. The metrics collection extension connects to `ccagent` using Unix Domain Sockets (UDS) to transfer metrics from Greenplum Database. Starting Greenplum Command Center with the `gpcc start` command starts the Command Center agent on

each segment host. Stopping Command Center with `gpcc stop` ends these processes. The Command Center backend monitors these agents and restarts them when necessary.

Installing the `gpperfmon` database configures Greenplum Database to run agents on the master host and each segment host. The agents are started automatically when the database system starts up. The Greenplum Database postmaster process monitors the agents and restarts them when necessary.

`gpmmmon`

The `gpmmmon` agent runs on the Greenplum Database master host. It collects initial query information from the master. Every 15 seconds, by default, it prompts the `gpsmon` agents to send their accumulated data. The `gpmmmon` process saves the metrics data and logs to CSV text files that feed the external tables in the `gpperfmon` database.

`gpsmon`

The `gpsmon` agent runs on each Greenplum Database segment host. It listens on a UDP port for metrics emitted by Greenplum Database, gathers additional metrics from the operating system, and forwards data to the `gpmmmon` agent when requested.

This topic describes basic agent administration tasks, including adding hosts and viewing agent log files.

## Adding and Removing Hosts

When you add or replace Greenplum Database hosts, you must reinstall the Greenplum Command Center software to ensure the software is installed on the new hosts. It is not necessary to uninstall Command Center before reinstalling. Stop Command Center and restart it to start agents on the new hosts.

The `gpperfmon` `gpsmon` agents on new hosts are detected automatically by the master agent, `gpmmmon`. Whenever the `gp_enable_gpperfmon` server configuration parameter is enabled on the master, the `gpmmmon` agent automatically detects, starts, and begins harvesting data from new segment agents.

## Viewing and Maintaining Agent Log Files

Log messages for the Command Center metrics collector agents are saved in the `logs` directory of the Command Center installation directory.

Log messages for the `gpperfmon` master agent are written to the following file by default:

```
$MASTER_DATA_DIRECTORY/gpperfmon/logs/gpmmmon.log
```

To change the `gpperfmon` log file location, edit the `log_location` parameter in `gpperfmon.conf`.

On the segment hosts, `gpperfmon` agent log messages are written to a `gpsmon.log` file in the segment instance's data directory. For a host with multiple segments, the agent log file is located in the data directory of the first segment, as listed in the `gp_configuration` table by `dbid`. If the segment agent is unable to log into this directory, it will log messages to the home directory of the user running Command Center (typically `gpadmin`).

## Configuring gpperfmon Log File Rollover

At higher logging levels, the size of the `gpperfmon` log files may grow dramatically. To prevent the log files from growing to excessive size, you can add an optional log rollover parameter to `gpperfmon.conf`. The value of this parameter is measured in bytes. For example:

```
max_log_size = 10485760
```

With this setting, the log files will grow to 10MB before the system rolls over the log file. The timestamp is added to the log file name when it is rolled over. Administrators must periodically clean out old log files that are no longer needed.

## Administering the gpperfmon Database

Data collected by gpmmon and gpsmon agents is stored in a dedicated database called gpperfmon. This database requires the typical database maintenance tasks, such as clean up of old historical data and periodic `ANALYZE`.

See the [gpperfmon Database Reference](#) section for a reference of the tables and views in the gpperfmon database.

## Connecting to the gpperfmon Database

Database administrators can connect directly to the gpperfmon database using any Greenplum Database-compatible client program (such as `psql`). For example:

```
$ psql -d gpperfmon -h master_host -p 5432 -U gadmin
```

## Backing Up and Restoring the gpperfmon Database

The history tables of the gpperfmon database can be backed up and restored using the Greenplum Database backup and restore utilities. See the *Greenplum Database Utility Guide* for more information.

## Maintaining the Historical Data Tables

All of the `*_history` tables stored in the gpperfmon database are partitioned into monthly partitions. A January 2010 partition is created at installation time as a template partition. It can be deleted once some current partitions are created. The Command Center agents automatically create new partitions in two month increments as needed. Administrators must periodically drop partitions for the months that are no longer needed in order to maintain the size of the database.

See the *Greenplum Database Administrator Guide* for more information on dropping partitions of a partitioned table.

## gpcc

Manages the Greenplum Command Center web service and metrics collection agents.

```
gpcc <action> [-W]

gpcc [--version | -v ]

gpcc [--help | -h]

gpcc [--settings]
```

## Actions

### start

Starts the Command Center web service and metrics collection agents. Add the `-W` flag to force a prompt for the gpmon user password.

### stop

Stops the Command Center web service and metrics collection agents. Add the `-W` flag to force a prompt for the gpmon user password.

### status

Displays the status, either `Running` or `Stopped`, of the web server and metrics collection agents. Add the `-W` flag to force a prompt for the gpmon user password.

### krbenable

Enables Kerberos authentication for Command Center.

Use the `gpcc krbenable` command to set up Kerberos authentication for Command Center users if Command Center was initially installed without enabling Kerberos. When you run `gpcc krbenable`, `gpcc` prompts for:

- the web server name
- the name of the Greenplum Database Kerberos service
- the Command Center Kerberos authentication mode
- the path to the keytab file on the Command Center host.

Before you run `gpcc krbenable`, see [Enabling Authentication with Kerberos](#) to check prerequisites and for help preparing the Command Center host to allow Kerberos authentication.

### krbdisable

Disables Kerberos authentication for Command Center.

### help

Displays syntax and help text for the `gpcc` command.

## Options

### --settings

Displays the current values of the Command Center configuration parameters. See [Setup Configuration File](#) for a list of the configuration parameters.

### --version or -v

Displays the Greenplum Command Center version.

### -W <password>

The optional `-W` option specifies the password for the gpmon user. The `gpcc` command normally gets the password from the `$PGPASSWD` environment variable or the `.pgpass` file in the gpadmin user's home directory. If the password is not available with either of these methods, the `-W` option must be included to specify the password whenever you run `gpcc`.



## Description

Once started, the Command Center backend monitors the metrics agents with a heartbeat. If a failed agent is detected, the backend spawns a new agent process.

## Examples

Start Command Center and the metrics agents, prompting for the gpmon password.

```
S gpcc start -W
Password for GPDB user gpmon:
Starting the gpcc agents and webserver...
2018/03/22 17:51:51 Agent successfully started on 7/8 hosts
2018/03/22 17:51:51 View Greenplum Command Center at http://smdw:28080
```

## gpmetrics Schema Reference

Greenplum Command Center creates the `gpmetrics` schema in the Greenplum Database `gpcc` database to save data related to the Greenplum Database metrics collection extension. Command Center creates the following tables in the Greenplum Database `gpcc` database:

- The `gpcc_alert_rule` table holds alert rules configured on the Command Center **Admin> Alerts** page.
- The `gpcc_alert_log` table records an event when an alert rule is triggered.

### gpmetrics.gpcc\_alert\_rule Table

The `gpcc_alert_rule` table records the alert rules configured in the Command Center UI. It has the following columns.

Column	Type	Description
<code>rule_id</code>	integer	Unique id for the rule.
<code>rule_type</code>	integer	Reserved for future use.
<code>rule_description</code>	character varying(512)	Text of the rule.
<code>rule_config</code>	json	JSON string containing parameters for user-specified values.
<code>ctime</code>	timestamp(0) without time zone	Time the rule was created.
<code>etime</code>	timestamp(0) without time zone	Time the rule became inactive, or null if rule is active.

The `gpcc_alert_rule` table keeps a history of alert rule configurations. When a rule becomes active, a new row is inserted and the `ctime` timestamp column is set to the current time; the `etime` timestamp is null, indicating that the rule is still active. When a rule is either disabled or superseded by a new rule, the `etime` timestamp column is set to the current time. Thus, the set of currently active rules is all rows where the `etime` column is null. A row that has timestamps in both `ctime` and `etime` columns is an historical record of the period of time during which the rule was active.

The `rule_id` column, a unique integer, is the distribution key for the table and is used to identify a single alert rule configuration. This column can be joined with the `rule_id` column in the `gpcc_alert_log` table to identify the rule that triggered each recorded alert event.

The `rule_description` column contains a string that describes the event that matches the rule. It is the text displayed in the Command Center UI for the rule, with user-specified values inserted.

The `rule_config` column contains a JSON string with parameters for the values entered for each of the rule's fields in the Command Center UI.

### gpmetrics.gpcc\_alert\_log Table

The `gpcc_alert_log` table is an append-only table, partitioned by month on the `ctime` column. Command Center creates new partitions as needed. The table has the columns shown in the following table.

Column	Type	Description
<code>id</code>	integer	Unique ID for the alert.
<code>rule_id</code>	integer	The ID of the rule that triggered this alert.
<code>transaction_time</code>	timestamp(0) without time zone	Time the alert was raised.
<code>content</code>	json	Contains parameters specifying values that triggered the alert.

A row is added to the `gpcc_alert_log` table whenever an alert rule is matched.

The `id` column, a unique integer, is the distribution key for the table.

The `rule_id` column can be joined with the `rule_id` column in the `gpcc_alert_rule` table to access data for the rule that triggered the alert.

The `transaction_time` column is set to the current time when a row is created.

The `content` column contains a JSON string with parameters specifying details about the event that triggered the alert. The JSON parameters vary with the type of the alert.

## Example Query

This query lists the ten most recent alerts, including the configuration of the rule that triggered each event.

```
gpperfinon=# SELECT l.transaction_time, l.rule_id, r.rule_description, l.content
FROM gpmetrics.gpcc_alert_log AS l, gpmetrics.gpcc_alert_rule AS r
WHERE l.rule_id = r.rule_id
ORDER BY l.transaction_time
LIMIT 10;
```

## Configuration Files Reference

Configuration parameters for Greenplum Command Center are stored in the following files.

`$MASTER_DATA_DIRECTORY/gpperfmon/conf/gpperfmon.conf`, on Greenplum Database master host

Stores configuration parameters for the Greenplum Command Center agents.

`$GPCC_HOME/conf/app.conf`, on Command Center host.

Stores configuration parameters for the Command Center web application and web server.

`$MASTER_DATA_DIRECTORY/gpmetrics/gpcc.conf`

Stores configuration parameters for Command Center interface options and alert emails.

`$MASTER_DATA_DIRECTORY/postgresql.conf`

Stores configuration parameters to enable the Greenplum Command Center features for Greenplum Database server. These parameters are normally set using the `gpconfig` Greenplum Database management utility.

`$GPCC_HOME/bin/ssh-wrapper`

Greenplum Command Center normally finds the `ssh` command on the path. If your environment has an incompatible implementation of this command on the path, you can provide the absolute path to your version in the `ssh-wrapper` script, located at `$GPCC_HOME/bin/ssh-wrapper`.

For example:

```
ssh="/opt/bin/myssh"
```

## Command Center Agent Parameters

The `$MASTER_DATA_DIRECTORY/gpperfmon/conf/gpperfmon.conf` file on the Greenplum Database master host stores configuration parameters for the Command Center agents. For configuration changes to these options to take effect, you must save `gpperfmon.conf` and then restart Greenplum Database server ( `gpstop -r` ).

To enable the Command Center agents within Greenplum Database server, you must also set the Greenplum Database Server Configuration Parameters. See the `gpperfmon_install` reference in the *Greenplum Database Utility Guide* for details.

### log\_location

Specifies a directory location for Command Center log files. Default is `$MASTER_DATA_DIRECTORY/gpperfmon/logs`.

### min\_query\_time

Specifies the minimum query run time in seconds for statistics collection. Command Center logs all queries that run longer than this value in the `queries_history` table. For queries with shorter run times, no historical data is collected. Defaults to 20 seconds.

If you know that you want to collect data for all queries, you can set this parameter to a low value. Setting the minimum query run time to zero, however, collects data even for the numerous queries run by Command Center itself, creating a large amount of data that may not be useful.

### min\_detailed\_query\_time

Specifies the minimum iterator run time in seconds for statistics collection. Command Center logs all iterators that run longer than this value in the `iterators_history` table. For iterators with shorter run times, no data is collected. Minimum value is 10 seconds.

This parameter's value must always be equal to, or greater than, the value of `min_query_time`. Setting `min_detailed_query_time` higher than `min_query_time` allows you to log detailed query plan iterator data only for especially complex, long-running queries, while still logging basic query data for shorter queries.

Given the complexity and size of iterator data, you may want to adjust this parameter according to the size of data collected. If the `iterators_*` tables are growing to excessive size without providing useful information, you can raise the value of this parameter to log iterator detail for fewer queries.

### max\_log\_size

This parameter is not included in `gpperfmon.conf`, but it may be added to this file for use with Greenplum Command Center.

To prevent the log files from growing to excessive size, you can add the `max_log_size` parameter to `gpperfmon.conf`. The value of this parameter is measured in bytes. For example:

```
max_log_size = 10485760
```

With this setting, the log files will grow to 10MB before the system rolls over to a new log file.

### partition\_age

The number of months that Greenplum Command Center statistics data will be retained. The default is 0, which means we won't drop any data.

### quantum

Specifies the time in seconds between updates from Command Center agents on all segments. Valid values are 10, 15, 20, 30, and 60. Defaults to 15 seconds.

If you prefer a less granular view of performance, or want to collect and analyze minimal amounts of data for system metrics, choose a higher quantum. To collect data more frequently, choose a lower value.

### ignore\_qexec\_packet

When set to true, Greenplum Command Center agents do not collect performance data in the `gpperfmon` database `queries_*` tables: `rows_out`, `cpu_elapsed`, `cpu_currpct`, `skew_cpu`, and `skew_rows`. The default setting, true, reduces the amount of memory consumed by the `gpmmon` process. Set this parameter to false if you require this additional performance data.

### smdw\_aliases

This parameter allows you to specify additional host names for the standby master. For example, if the standby master has two NICs, you can enter:

```
smdw_aliases= smdw-1,smdw-2
```

This optional fault tolerance parameter is useful if the Greenplum Command Center loses connectivity with the standby master. Instead of continuously retrying to connect to host `smdw`, it will try to connect to the NIC-based aliases of `smdw-1` and/or `smdw-2`. This ensures that the Command Center Console can continuously poll and monitor the standby master.



## Command Center Console Parameters

The Command Center Console configuration file is on the Command Center host at `$GPCC_HOME/webserver/conf/app.conf`.

After editing this file, reload the configuration by restarting the Command Center Console.

```
$ gpcc --stop
$ gpcc --start
```

`appname = gpccws`

The web server binary file. Do not change.

`listentcp4 = [true | false]`

When `true`, the address type is tcp4. The default is `true`.

`runmode = [prod | dev | test]`

The application mode, which can be `dev`, `prod` or `test`. The default is `dev`. In `dev` mode Command Center shows user friendly error pages. User friendly error pages are not rendered in `prod` mode.

`session = [true | false]`

Use sessions to manage user experience. The default is `true`. Sessions are stored in memory.

`enablexsrif = [true | false]`

Enable CSRF protection.

`xsrifexpire = <seconds>`

CSRF expire time. The default is `2592000` seconds.

`xsrifkey = <token_string>`

The CSRF token.

`rendertype = json`

The render type of web server. Do not change.

`printallsqls = [true | false]`

Print all backend gpccfm SQL to the web server console. The default is `false`.

`path = /usr/local`

Path to the directory where Greenplum Command Center is installed.

`display_name = <display_name>`

The display name for console.

`enable-kerberos = [true | false]`

True if Kerberos authentication is enabled for Command Center. The default is `false`.

`HTTPSCertFile = </path/to/cert.pem>`

The full path to the server's SSL certificate, if SSL is enabled.

`HTTPSKeyFile = </path/to/cert.pem>`

The server's private key file if SSL is enabled.

`EnableHTTPS = [true | false]`

Enable listening on the secure SSL port. The default is `true`.

`EnableHTTP = [true | false]`

Enable listening on the HTTP port. Default is `false`.

`httpport = <port>`

The web server port. The default is 28080.

`rpcport = <port>`

The port on which the Command Center backend receives data from metrics collector agents. The default is 8899.

`master_host = <hostname>`

The Greenplum Database host name. The default is `localhost` .

`master_port = <port>`

The Greenplum Database master port. The default is `5432` .



## gpmetrics Configuration File Reference

Greenplum Command Center uses the `gpcc.conf` configuration file to save configuration information entered in the Command Center user interface. You should not normally edit the `gpcc.conf` file directly. Instead, modify configuration information in the Command Center user interface.

The `gpcc.conf` file is created in the `$MASTER_DATA_DIRECTORY/gpmetrics/` directory on the Greenplum Database master or standby host where you start Command Center. The file is an INI-format configuration file, containing properties defined as `key = value` entries, one property per line.

Property	Description
<code>allow_anonymous</code>	If <code>true</code> , Command Center users can access the Query Monitor view without logging into Command Center. You can change this setting on the Command Center <b>Admin&gt; Permissions</b> page.
<code>resource_queue_import_status</code>	Command Center uses this property to determine whether to offer to import Greenplum Database resource queues to resource groups when you access the <b>Admin&gt; Workload Mgmt</b> view. The default is <code>false</code> .
<code>emailFrom</code>	The email address to set on the "From:" line of alert emails. The default is <code>noreply-gpcc-alerts@pivotal.io</code> .  Note: Set the email and smtp properties on the Command Center <b>Admin&gt; Alerts</b> page.
<code>emailTo</code>	A comma-separated list of email addresses to send alert emails.
<code>smtpUsername</code>	The account name to use when authenticating with the SMTP server.
<code>smtpServer</code>	The address and port of the SMTP server to use for alert emails.
<code>smtpPassword</code>	The password used to authenticate the SMTP user with the SMTP server, base 64-encoded.

## Setup Configuration File

A setup configuration file contains properties used to configure Greenplum Command Center when you perform a non-interactive Command Center installation. The file is passed to the `gpccinstall` command with the `-c` option:

```
$ ./gpccinstall-<version> -c <config_file>
```

The configuration file contains `name: value` or `name=value` entries, one per line. Comments begin with a `#` or `;` character and continue through the end of the line.

See [Installing Pivotal Greenplum Command Center](#) for more information about installing Command Center with a configuration file.

## Parameters

`path`

The path to the directory where Greenplum Command Center software will be installed. The directory must be writable by the `gadmin` user on all hosts in the Greenplum Cluster.

`display_name`

The name to display in the Command Center user interface. The default display name is `gpcc`.

`master_port`

The Greenplum Database master port. Default: `5432`.

`web_port`

The listen port for the Command Center web server. The default is `28080`.

`enable_ssl`

`True` if client connections to the Command Center web server are to be secured with SSL. The default is `false`. If `true` the `ssl_cert_file` parameter must be set and the SSL certificate must be installed on the host where you run Command Center.

`ssl_cert_file`

If `enable_ssl` is `true`, set this parameter to the full path to a valid certificate in PEM file format. The certificate must be installed on the host where you run Command Center.

`enable_kerberos`

Set to `true` to enable Kerberos authentication.

`krb_mode`

The Kerberos authentication scheme to use. The default is `1`.

- **1 - normal mode (default)** - The Command Center Kerberos keytab file contains the Command Center principal and may contain principals for Command Center users. If the principal in the client's connection request is in the Command Center's keytab file, Command Center uses the client's principal for database connections. Otherwise, Command Center uses the `gpmon` user for database connections.
- **2 - strict mode** - Command Center has a Kerberos keytab file containing the Command Center service principal and a principal for every Command Center user. If the principal in the client's connection request is in the keytab file, the web server grants the client access and the web server connects to Greenplum Database using the client's principal name. If the principal is not in the keytab file, the connection request fails.
- **3 - gpmon\_only mode** - Command Center uses the `gpmon` database role for all Greenplum Database connections. No client principals are needed in the Command Center's keytab file.

`webserver_url`

The web server hostname, from the Kerberos HTTP service principal.

`keytab`

Path to the keytab file containing Kerberos principals for the Command Center web server and users.

## Examples

```
#####  
# GPCC 4.0 setup configuration file  
#####  
path = /opt  
display_name = Greenplum Database Production Cluster  
master_port = 5432  
webserver_port = 28081  
EnableHTTP = true    ; allow both HTTP and HTTPS  
EnableHTTPS = true  
ssl_cert_file = /etc/ssl/cert.pem  
enable_kerberos = false
```

## Greenplum Database Server Configuration Parameters

### Greenplum Database gpperfmon Database

The following Greenplum Database configuration parameters must be uncommented and set in the server configuration file ( `postgresql.conf` ) to enable the Command Center data collection agents:

- `gp_enable_gpperfmon` and `gpperfmon_port` must be set in both the master and segment `postgresql.conf` files.
- `gp_enable_gpperfmon` and `gp_enable_gpperfmon` only need to be set in the master `postgresql.conf` file.

After changing these settings, the Greenplum Database instance must be restarted for the changes to take effect.

#### `gp_enable_gpperfmon`

Turns on the Command Center data collection agent for a segment. Must be set in all `postgresql.conf` files (master and all segments).

#### `gpperfmon_port`

The default port for the Command Center agents is 8888, but you can set this parameter to a different port if required (master and all segments).

#### `gp_gpperfmon_send_interval`

Sets the frequency in seconds that the Greenplum Database server processes send query execution updates to the Command Center agent processes.

#### `gp_external_enable_exec`

This parameter is enabled by default and must remain enabled. It allows the use of external tables that execute OS commands or scripts on the segment hosts. The Command Center agents use this type of external tables to collect current system metrics from the segments.

#### `gpperfmon_log_alert_level`

Controls which message levels are written to the gpperfmon log. Each level includes all the levels that follow it. The later the level, the fewer messages are sent to the log. The default value is warning.

#### `shared_preload_libraries`

A comma-separated list of shared libraries that are to be preloaded when Greenplum Database starts. The workload management and query metrics extension libraries must be included in this configuration parameter to use Greenplum Command Center.

#### `gp_enable_query_metrics`

When on, enables query metrics collection. The default is off. After setting this configuration parameter, Greenplum Database must be restarted for the change to take effect.

#### `gp_instrument_shmem_size`

The amount of shared memory, in kilobytes, allocated for query metrics. The default is 5120 and the maximum is 131072. At startup, if `gp_enable_query_metrics` is set to on, Greenplum Database allocates space in shared memory to save query metrics. This memory is organized as a header and a list of slots. The number of slots needed depends on the number of concurrent queries and the number of execution plan nodes per query. The default value, 5120, is based on a Greenplum Database system that executes a maximum of about 250 concurrent queries with 120 nodes per query. If the `gp_enable_query_metrics` configuration parameter is off, or if the slots are exhausted, the metrics are maintained in local memory instead of in shared memory.

## Securing Greenplum Command Center

Greenplum Command Center Console can be secured by encrypting network traffic between the web server and users' browsers, authenticating Command Center users, and managing users' permissions to access Command Center features.

### SSL/TLS Encryption

Greenplum Command Center supports SSL/TLS encryption to secure connections between browsers and the Command Center web server. When SSL is enabled, Command Center uses the WebSockets API, enabling long-lived, full-duplex connections, in addition to encryption.

To enable SSL, you should have a signed certificate for the Command Center web server in place when you install Command Center. Place your certificate on the server where Command Center is installed, for example in the `/etc/ssl/certs` directory of the Greenplum master host. You import the certificate when you install Command Center. The locations of the certificate and private key files are saved in the `$GPCC_HOME/conf/app.conf` configuration file for the Command Center. See [Command Center Console Parameters](#) for details.

You can request a certificate from your organization's internal certificate authority or a commercial certificate authority, or you can use a self-signed certificate you create yourself with a cryptography suite such as OpenSSL. If you create a self-signed certificate, note that clients will have to override a security warning when they first connect to the Command Center web server.

### Authentication Options

Users logging in to Greenplum Command Center are authenticated with the Greenplum Database host-based authentication system. Users can enter credentials as a user name and password or, if Kerberos authentication is configured, by authenticating with Kerberos on their workstation before browsing to the Command Center web server.

**Note:** Greenplum Command Center does not accept logins from the `gadmin` user, or from users configured with trust authentication in the `pg_hba.conf` file.

Database users must first be added to the Greenplum Database by using commands such as `CREATE ROLE` or `CREATE USER`. The `LOGIN` privilege is required. This example creates a login user with an encrypted password:

```
CREATE ROLE cc_user WITH LOGIN ENCRYPTED PASSWORD 'changeme';
```

The `pg_hba.conf` configuration file determines how authentication will proceed. This file contains a list of entries that are compared to attributes of the user's connection request, including the type of connection, network location of the originating host, database name, and login user name. When a match is found, the authentication method specified in the entry is applied.

The `pg_hba.conf` file can be viewed by Operators and edited by Admins in the Command Center console on the [Admin>Authentication](#) page.

The `md5` and `password` authentication methods authenticate the user name and password with the Greenplum Database `pg_roles` system table. The `md5` method requires the password to be MD5-encoded when sent over the network, so it is preferred over the `password` method, which sends the password in clear text.

The `ldap` authentication method authenticates the user name and password with an LDAP server. The LDAP server and parameters are specified in the options field of the `pg_hba.conf` entry. See the PostgreSQL [LDAP authentication](#) documentation for the format of the LDAP options.

The `gss` authentication method is used for Kerberos authentication. To use Kerberos with Command Center, Kerberos authentication must be enabled for the Greenplum Database system and Command Center must also be configured. Users authenticate with the Kerberos KDC on their workstations (using `kinit`, for example) before connecting to the Command Center web server. The role name in Command Center is the user's Kerberos principal name.

For details about setting up Kerberos authentication, see [Enabling Kerberos Authentication with Greenplum Command Center](#).

See the PostgreSQL [Authentication methods](#) documentation for additional details of the authentication options.

### Authorization

 **Note:** The functionality described in this section has not been fully implemented in Greenplum Command Center 4.0.0. Only Admin and Self Only

permission levels are available.

Command Center manages permission levels using Greenplum Database roles and groups. The Basic, Operator Basic, and Operator permission levels correspond to the `gpcc_basic`, `gpcc_operator_basic`, and `gpcc_operator` group roles in the database. The Admin permission level is conferred to roles that have the `SUPERUSER` privilege. A user who has not been added to any of the groups and does not have `SUPERUSER` privilege has the most restrictive permission level, Self Only.

Greenplum Database superusers can manage permission levels on the Command Center [Admin>Permissions](#) page. Superusers can also directly assign users roles in the database by using the `ALTER USER`, `ALTER GROUP`, and related commands to add or remove users from groups and add or remove the `SUPERUSER` privilege. If a role is configured for more than one permission level, Command Center uses the highest permission level.

Command Center users have the following capabilities, according to their permission levels:

## Self Only

Users can view metrics and view and cancel their own queries.

Any Greenplum Database user successfully authenticated through the Greenplum Database authentication system can access Greenplum Command Center with Self Only permission. Higher permission levels are required to view and cancel other's queries and to access the System and Admin Control Center screens.

## Basic

Allows users to view metrics, view all queries, and cancel their own queries.

Users with Basic permission are members of the Greenplum Database `gpcc_basic` group.

## Operator Basic

Allows users to view metrics, view their own and others' queries, cancel their own queries, and view the System and Admin screens.

Users with Operator Read-only permission are members of the Greenplum Database `gpcc_operator_basic` group.

## Operator

Allows users to view their own and others' queries, cancel their own and other's queries, and view the System and Admin screens.

Users with Operator permission are members of the Greenplum Database `gpcc_operator` group.

## Admin

Allows users access to all views and capabilities in the Command Center.

Greenplum Database users with the `SUPERUSER` privilege in Greenplum Database have Superuser permissions in Command Center.

## Managing Greenplum Command Center Authentication

The **Admin> Authentication** screen allows users with Operator Basic, Operator, and Admin permission to view the Greenplum Database host-based authentication file, `pg_hba.conf`.

**Host-Based Authentication** Controls user access for all GPDB activity on this server

For guidance on managing `pg_hba.conf` consult the [postgres documentation](#)

`pg_hba.conf` This version 2018-09-25, 12:10 **LOAD VERSION...** **ABANDON CHANGES** **SAVE CONFIG AND UPDATE GPDB**

Type	Database	User	Address (CIDR/Hostname)	Method	Comment
local	all	gpadmin		ident	
host	all	gpadmin	127.0.0.1/28	trust	
host	all	gpadmin	192.168.1.144/32	trust	
host	all	gpadmin	::1/128	trust	
host	all	gpadmin	2605:a601:4199:bb00:a00:27ff:f...	trust	
host	all	gpadmin	fe80::a00:27ff:fe6c:43b4/128	trust	
local	replication	gpadmin		ident	
host	replication	gpadmin	same-net	trust	
local	gpmon	gpmon		md5	
host	all	gpmon	127.0.0.1/28	md5	
host	sales	nickd	nickd-pc	md5	
host	all	gpmon	::1/128	md5	

Type Database User Address (CIDR/Hostname) Method Comment

host all gpmon 192.168.1.144/28 md5

**DONE** Cancel

Users with Admin permission can add, remove, change, and move entries in the file. The Command Center UI validates entries to ensure correct syntax. Previous versions of the file are archived so that you can restore an earlier version or audit changes.

See [Authentication Options](#) for an overview of user authentication options for Greenplum Database and Greenplum Command Server.

See [Configuring Client Authentication](#) in the *Greenplum Database Administrator Guide* for a detailed description of the contents of the `pg_hba.conf` file.



## Viewing the Host-Based Authentication File






Choose **Admin>Authentication** to display the content of the Greenplum Database `pg_hba.conf` file.

The `pg_hba.conf` file contains a list of entries that specify the characteristics of database connection requests and authentication methods. When Greenplum Database receives a connection request from a client, it compares the request to each entry in the `pg_hba.conf` entry in turn until a match is found. The request is authenticated using the specified authentication method and, if successful, the connection is accepted.

## Editing the Host-Based Authentication File

Command Center users with the *Admin* permission can edit the `pg_hba.conf` file. Note that any changes you make are lost if you move to another screen before you save them.

- To change an existing entry, click anywhere on the entry. Edit the fields and click **Save** to save your changes, or **Cancel** to revert changes.
- To move an entry up or down in the list, click on the  symbol, drag the line to the desired location, and release.
- To add a new entry to the end of the file, click **Add New Entry** at the bottom of the screen. Edit the fields and click **Save** to save your changes, or **Cancel** to abandon the new entry.
- To add a new entry after an existing entry, highlight the existing entry and click . Edit the fields and click **Save** to save your changes, or **Cancel** to abandon the new entry.

- To copy an entry, select the entry and click . A copy of the selected entry is added below the selected entry and displayed for editing. Edit the fields and click **Save** to save your changes, or **Cancel** to abandon the copy.
- To add a comment to the file, add an entry by clicking **Add New Entry** or  and then choose  from the **Type** list.
- To toggle an entry between active and inactive, select the line and click the **active/inactive** toggle control to the right. This action adds or removes a comment character () at the beginning of the entry.
- To remove an entry, highlight the line and click . The entry is displayed with strikethrough text. You can restore the entry by highlighting it and clicking **undelete**. The entry is permanently removed when you click **Save config and update GPDB**.
- To finish editing, click **Save config and update GPDB**. Then click **Save and Update** to save your changes or click **Cancel** to return with your edits intact.

When you select **Save and Update**, the `pg_hba.conf` file is saved and refreshed in Greenplum Database. Note that existing client connections are unaffected.

## Loading a Previous Version of the Host-Based Authentication File

When you save a new version of the `pg_hba.conf` file, a copy is saved in the Greenplum Database `$MASTER_DATA_DIRECTORY/pg_hba_archive` directory as `pg_hba.conf-<timestamp>`.

To view an archived version of the `pg_hba.conf` file, click **Load versions...** and click the timestamp for the version to display.

To revert to a previous version of the file, load the previous version and then click **Save config and update GPDB**. The configuration is refreshed in Greenplum Database and saved as a new version in the archive directory.



## Managing Greenplum Command Center Permissions

The **Permissions Levels for GPCC Access** screen allows users with Operator Basic, Operator, or Admin permission to view Command Center user permissions for Greenplum Database users. Users with Admin permission can set permissions for any user.

Users with Operator Basic, Operator, and Admin permission can also see if the Guest Access to Query Monitor feature is enabled or disabled, and Admin users can toggle this feature on and off.

**Permission Levels for GPCC Access** Controls access to various aspects of GPCC on this server

**GPCC Access** Change Selected to... ▾

<input type="checkbox"/>	Role Name ▾ Filter by...	Permission Level Filter by...
<input type="checkbox"/>	sallyg	Admin (superuser) ▾
<input type="checkbox"/>	richd	Operator Basic ▾
<input type="checkbox"/>	ralphp	Operator Basic ▾
<input type="checkbox"/>	nickd	Operator Basic ▾
<input type="checkbox"/>	kristiem	Self Only ▾
<input type="checkbox"/>	katrinab	Self Only ▾
<input type="checkbox"/>	jillianr	Operator ▾
<input type="checkbox"/>	brentd	Operator ▾
<input type="checkbox"/>	anny	Self Only ▾

**Permission Levels**

*See Queries & Metrics only* *See all screens*

**Self Only (default)**  
See all queries (no details)  
See own query details  
Cancel own  
*group: none*

**Operator Basic**  
See all queries, cancel own  
Cannot perform admin tasks  
*group: gpcc\_operator\_basic*

**Operator**  
See all/cancel any query  
Cannot perform admin tasks  
*group: gpcc\_operator*

**Basic**  
See all queries, cancel own  
*group: gpcc\_basic*

**Admin (superuser)**  
See all/cancel any query  
Perform admin tasks  
*group: none*  
*role attribute: superuser*

**Query Monitor Guest Access**  
*Provides access to Query Monitor without sign in*  
☒ **Allow guests to view Query Monitor**

*Users must also have entry in pg\_hba.conf (see [Authentication](#)) to sign in to GPCC*



## Viewing User Permissions

Initially, all Greenplum Database login users are included in the list of roles with their current permission levels.

- To filter by role name, enter all or part of the user's database role name in the *Role Name* field. The filter performs a simple substring search and displays users with matching role names. Click the **Role Name** label to reverse the search order.
- To filter for users with a specific permission level, choose the permission level from the **Permission Level** list.
- Role Name and Permission Level filters can be used together.
- To reset the filters, remove all text from the *Role Name* field and choose **Filter by...** from the **Permission Level** list.

## Changing User Permission Levels

Users with Admin permission can change permission levels.

- Use the **Role Name** and **Permission Level** filters to display the roles you want to change.
- Check the box next to a role name to select the user, or check the box in the heading to select all displayed users.
- Select the new permissions level for each user from the list in the **Permission Level** column, or select a new permission level for all selected users

from the **Change Selected to...** list.

## Enabling or Disabling Guest Access to Query Monitor

When enabled, the **Guest Access to Query Monitor** feature allows anyone with access to the Greenplum Command Center web server to click **View Query Monitor** on the Command Center sign-in screen and see the **Query Monitor** page without logging in. These anonymous users cannot cancel queries and cannot access any other Command Center features.

When this feature is off, the **View Query Monitor** link does not appear on the sign-in screen and anonymous users cannot see the **Query Monitor** page.

Command Center users with Admin permission can toggle the feature on an off with a mouse click. Users with Operator or Operator Basic permission see a message reporting if the feature is on or off.

## Securing the gpmon Database User

The Greenplum Database `gpmon` user is a superuser role used to manage the gpperfmon database. The `gpperfmon_install` utility, which must be run before you install Greenplum Command Center Console, creates the `gpmon` role.

Greenplum Database uses the `gpmon` role to update the gpperfmon database with data collected by agents running on the segment hosts. The Command Center web server uses the `gpmon` role to connect to the gpperfmon database as well as databases monitored by the Command Center.

When `gpperfmon_install` creates the `gpmon` role, it prompts for a password, which it then adds to the `.pgpass` file in the `gpadmin` user's home directory. The entry in the `.pgpass` file is similar to the following:

```
*:5432:gpperfmon:gpmon:changeme
```

See [The Password File](#) in the PostgreSQL documentation for details about the `.pgpass` file.

The `.pgpass` file is required on the Greenplum Database master host to start the gpperfmon data collection agents. If you run Greenplum Command Center on a different host, you can copy the `.pgpass` file to that host, or you can run the Command Center `gpcc` management utility with the `-W` option to request password entry each time you start or stop Command Center or request status.

In the `$MASTER_DATA_DIRECTORY/pg_hba.conf` authentication file, `gpperfmon_install` creates these entries:

```
local  gpperfmon  gpmon  md5
host   all      gpmon   127.0.0.1/28  md5
host   all      gpmon   ::1/128      md5
```

If you authenticate users with Kerberos, you can also set up Kerberos authentication for the `gpmon` role on the Greenplum master and standby hosts. Kerberos authentication is supported with TCP connections only; `local` entries use Linux sockets and authenticate with the `.pgpass` file password, even if you have enabled Kerberos for `host` entries.

## Changing the gpmon Password

To change the `gpmon` password, follow these steps:

1. Log in to Greenplum Database as a superuser and change the `gpmon` password with the `ALTER ROLE` command:

```
# ALTER ROLE gpmon WITH ENCRYPTED PASSWORD 'new_password';
```

2. On the Greenplum master host, update the password in the `.pgpass` file in the `gpadmin` home directory (`~/.pgpass`). Replace the existing password in the line or lines for `gpmon` with the new password.

```
*:5432:gpperfmon:gpmon:new_password
```

3. Ensure that the `.pgpass` file is owned by `gpadmin` and RW-accessible by `gpadmin` only.

```
$ chown gpadmin:gpadmin ~/.pgpass
$ chmod 600 ~/.pgpass
```

4. Restart Greenplum Command Center with the `gpcc` utility.

```
$ gpcc stop
$ gpcc start
```

💡 Be sure to also update the `.pgpass` file on the standby master host.

## Authenticating gpmon with Kerberos

If you authenticate Greenplum Database and Command Center users with Kerberos, you can also authenticate the `gpmon` user with Kerberos.

To prepare for installing Command Center with Kerberos authentication, follow these steps:

1. Create the gpperfmon database using the Greenplum Database `gpperfmon-install` management utility. See [Creating the gpperfmon Database](#).
2. On the KDC, create a keytab file containing the Kerberos principal for the `gpmon` user, just as you would for any Kerberos-authenticated client. Install the file on the Greenplum master and standby hosts.
3. Update the entries for `gpmon` in the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file to use the `gss` authentication method.

```
host all gpmon 0.0.0.0/0 gss include_realm=0 krb_realm=GPDB.EXAMPLE.COM
```

Note that `local` entries in `pg_hba.conf` cannot be authenticated with Kerberos. If there is a `local` entry for the `gpmon` user, it will use the `.pgpass` file to authenticate with the database. See [The pg\\_hba.conf file](#) in the PostgreSQL documentation for complete `pg_hba.conf` file documentation.

4. Log in to the master host as `gpadmin` and authenticate the `gpmon` user.

```
$ kinit gpmon
```

5. Install Greenplum Command Center to set up the Kerberos-enabled Command Center.

## Enabling Authentication with Kerberos

If you have enabled Kerberos authentication for Greenplum Database, you can set up Greenplum Command Center to accept connections from Kerberos-authenticated users.

Greenplum Database and Command Center include support for the Generic Security Service Applications Program Interface (GSS-API) standard. A related standard, Simple and Protected GSS-API Negotiation Mechanism (SPNEGO), describes the protocol GSS-API clients and servers use to agree on the method of authentication.

With a SPNEGO-compliant web application such as Command Center, the client and server agree on the authentication method on the client's initial HTTP request. If Kerberos authentication is not supported on both ends of the connection the server falls back to basic authentication, and displays a login form requesting a user name and password. If a user has authenticated on the workstation with Kerberos and has a valid ticket granting ticket, the web browser offers the user's credential to the Command Center web server. A Kerberos-enabled Command Center web server is configured to handle the authenticated user's connection request in one of three modes, called strict, normal, or gpmon-only.

### Strict

Command Center has a Kerberos keytab file containing the Command Center service principal and a principal for every Command Center user. If the principal in the client's connection request is in the keytab file, the web server grants the client access and the web server connects to Greenplum Database using the client's principal name. If the principal is not in the keytab file, the connection request fails.

### Normal

The Command Center Kerberos keytab file contains the Command Center principal and may contain principals for Command Center users. If the principal in the client's connection request is in Command Center's keytab file, it uses the client's principal for database connections. Otherwise, Command Center uses the `gpmon` user for database connections.

### gpmon-only

The Command Center uses the `gpmon` database role for all Greenplum Database connections. No client principals are needed in the Command Center's keytab file.

If you have set up Kerberos authentication for Greenplum Database, most of the configuration required to enable Command Center Kerberos authentication has been done. The Command Center Kerberos configuration builds upon the Greenplum Database Kerberos setup.

Kerberos authentication can be enabled by responding to prompts when you install Command Center, or you can use the `gpcc --krbenable` command to enable Kerberos after Command Center has been installed.

## Before You Begin

Kerberos authentication must be enabled for Greenplum Database. See [Using Kerberos Authentication](#) for instructions. Make sure the following prerequisites are met before you continue:

- The `krb5-workstation` package and associated libraries (`libkrb5*`) must be installed on the Greenplum master host and each client workstation.
- The date and time on the Greenplum master host and all client workstations must be synchronized with the KDC.
- The `krb5.conf` configuration file must be the same on the KDC host, the Greenplum Database master host, and client workstations.
- The KDC database must have a service principal for Greenplum Database. The default service name for Greenplum Database is `postgres/<master-host>@<realm>`. You can choose a service name other than `postgres`, but it must match the value of the `krb_srvname` parameter in the `$MASTER_DATA_DIRECTORY/postgresql.conf` file.
- A keytab file with the Greenplum Database principal must be installed on the Greenplum master host and identified by the `krb_server_keyfile` parameter in the `$MASTER_DATA_DIRECTORY/postgresql.conf` file.
- Each client workstation can have a keytab file containing their Kerberos principal, `<username>@<realm>`.

## Add Command Center Principals to the KDC Database

Before you configure Command Center for Kerberos authentication, you must create the required Kerberos principals. All of the principals used with Command Center are created in the Greenplum Database Kerberos realm. Command Center users can use the same Kerberos principal to authenticate with Command Center and Greenplum Database.

### Command Center Service Principal

A service principal is needed for the Command Center web server. This principal has the format `HTTP/<host>@<realm>`. For example, if users access

Command Center at the URL `http://mdw.example.com:28080`, the `<host>` part of the service key is `mdw.example.com` and the `<realm>` part is the Greenplum Database Kerberos realm, for example `GPDB.KRB`.

Note that Kerberos authentication only works if Command Center users enter the host in the same format specified in the Kerberos service principal. If the principal specifies the FQDN, for example, using the host's IP address in the browser URL will not work; the web server will fall back to basic authentication.

## Greenplum Database gpmon User

Command Center uses the `gpmon` Greenplum role to access the `gpmon` database, which contains data presented in the Command Center UI.

You can choose to authenticate the `gpmon` user with Kerberos or with basic authentication. To use Kerberos, you must create a principal for the `gpmon` user.

If you choose to use basic authentication you do not need a Kerberos principal for the `gpmon` user. The `gpmon` user will authenticate with Greenplum Database using the password saved in the `~gpadmin/.pgpass` file on the host running Command Center. If you run Command Center on a host other than the Greenplum Database master host, you must copy the `~gpadmin/.pgpass` file from the master host to the Command Center host. See [Changing the gpmon Password](#) for instructions to manage the `gpmon` password.

## Command Center Users

Add Kerberos principals for any Command Center users who do not already have principals in the KDC for Greenplum Database.

## Adding Kerberos Principals

To add the required principals, perform the following steps as root on the KDC server.

1. Add a principal for the Command Center web service. Be sure to specify the `<gpcc-host>` in the same format that users should enter the host in their browsers.

```
# kadmin.local -q "addprinc -randkey HTTP/<gpcc-host>@<realm>"
```

2. If you want the `gpmon` database user to use Kerberos authentication, add a `gpmon` principal.

```
# kadmin.local -q "addprinc gpmon@<realm>"
```

3. Add principals for any new Command Center users.

```
# kadmin.local -q "addprinc cc_user1@<realm>"
```

Repeat for each new Command Center user.

## Set Up Keytab Files

After you have created all of the Kerberos principals needed, you create and distribute keytab files. Keytab files contain Kerberos principals and encrypted keys based on the principals' Kerberos passwords. Keytab files are needed for the Greenplum Database master and standby hosts and the Command Center host.

You can also create a keytab file for each Greenplum Database or Command Center user containing just the user's principal. This keytab file is installed on the user's workstation to enable the user to authenticate to Kerberos. Note that all keytab files must contain the most recent versions of the principals' keys.

## Command Center Running on the Greenplum Master Host

If the Greenplum Command Center web server is running on the Greenplum Database master host, Command Center can share the Greenplum Database keytab file. You need to create a keytab file that contains the following principals:

- Service key for the `postgres` process on the Greenplum Database master host, for example `postgres/mdw.example.com@GPDB.EXAMPLE`.
- Service key created for Command Center in the previous section, for example `HTTP/mdw.example.com@GPDB.KRB`.
- A principal for every Kerberos-authenticated Greenplum Database or Command Center user.

All service keys and principals should be in the Greenplum Database realm.

To create a keytab file for Greenplum Database and Command Center, perform the following steps as root on the KDC server.

1. Create a keytab file containing the Greenplum Database service key, the command center service key, and all database and Command Center users.

```
kadmin.local -q "ktadd -k gpdb-kerberos.keytab postgres/mdw.example.com@GPDB.KRB HTTP/mdw.example.com@GPDB.KRB"
```

You can enter one or more principals with each `ktadd` command. You can specify a wildcard using the `-glob` option. For example this command adds all principals in the `GPDB.KRB` realm, including service principals and admin users.

```
kadmin.local -q "ktadd -k gpdb-kerberos.keytab -glob */GPDB.KRB"
```

2. Copy the keytab you created to the Greenplum Database master host, replacing the old keytab file. The location of the file is given by the `krb_server_keyfile` parameter in the `$MASTER_DATA_FILE/postgresql.conf` file. Set the permissions on the file so that it can be read only by the `gpadmin` user.
3. Update any entries required for new Greenplum Database principals in the `pg_hba.conf` file and `pg_ident.conf` files. See [Update the Greenplum Database `pg\_hba.conf` File](#) for details.

## Command Center Running on the Standby Master

If the Command Center web server is on a different host than the Greenplum Database master, you need separate keytab files for Greenplum Database and Command Center. The keytab file for Greenplum Database may not require any updates, but you will need to create a keytab file for Command Center.

- The Greenplum Database keytab file must contain the Greenplum Database service key and all principals for users with database access.
- The Command Center keytab file contains the Command Center service key and principals for users that have Command Center access. Users with Command Center access must also have Greenplum Database access, so user principals in the Command Center keytab file must also be in the Greenplum Database keytab file.

Update the Greenplum Database keytab if you created new database roles and principals for Command Center. For example, if you want to use Kerberos authentication for the `gpmon` user, you must create a principal and add it to both the Greenplum Database and Command Center keytab files.

To create the keytab file for Command Center, perform the following steps as root on the KDC host.

1. Create a keytab file and add the Command Center service key.

```
kadmin.local -q "ktadd -k gpcc-kerberos.keytab HTTP/smdw.example.com@GPDB.KRB"
```

2. If you want to authenticate the `gpmon` user with Kerberos, add the `gpmon` principal.

```
kadmin.local -q "ktadd -k gpcc-kerberos.keytab gpmon@GPDB.KRB"
```

3. Add principals for all Command Center users:

```
kadmin.local -q "ktadd -k gpcc-kerberos.keytab cc_user1@GPDB.KRB cc_user2@GPDB.KRB"
```

You can enter one or more principals with each `ktadd` command.

4. Enter `quit` to exit `kadmin.local`.
5. Copy the keytab you created to the the host running Command Center, for example:

```
$ scp gpcc-kerberos.keytab gpadmin@<host-name>:/home/gpadmin
```

6. Update any entries required for new principals in the `pg_hba.conf` file and `pg_ident.conf` files on the Greenplum master. See [Update the Greenplum Database `pg\_hba.conf` File](#).

## Update the Greenplum Database pg\_hba.conf File

The Greenplum Database `$MASTER_DATA_DIRECTORY/pg_hba.conf` configuration file determines which authentication methods to use to allow database access.

If you created new Command Center users, you may need to add an entry to allow access via Command Center. The entry for an individual user has this format:

```
host database <user-name> <gpcc CIDR> gss [options]
```

Authentication for the `gpmon` user needs to be set up in the `pg_hba.conf` file in one of the following ways.

### Basic authentication

The `/home/gpadmin/.pgpass` file contains the password for `gpmon` to use. See [Changing the gpmon Password](#) for details. An entry in the `pg_hba.conf` file specifies the md5 authentication method for `gpmon`:

```
local all gpmon md5
```

### Trust authentication

On the Greenplum Database master host only, the `gpmon` user can access databases without authentication:

```
local all gpmon trust
```

The `/home/gpadmin/.pgpass` file is not needed.

### Kerberos authentication

A Kerberos principal has been created for the `gpmon` user and added to the Greenplum Database and Command Center keytab files.

```
host all gpmon <gpcc CIDR> gss [options]
```

Remove any existing reject rules for `gpmon`:

```
host all gpmon <auth-method> reject
```

See [Using Kerberos Authentication](#) for more information about the `pg_hba.conf` file.

## Enable Kerberos for Command Center

Set up Command Center to use the Command Center keytab file you created.

If you are adding Kerberos authentication to an existing Command Center, use the `gpcc` command. For example:

```
$ gpcc --krbenable
```

Enter the Command Center host name and path to the keytab file at the prompts. See the [gpcc Reference](#) for more information.

## Authenticating With Kerberos on the Client Workstation

To use Kerberos Command Center authentication, the user must have authenticated with Kerberos using the `kinit` command-line tool.

The user then accesses the Command Center web server with a URL containing the host name in the format specified in the Command Center service principal and the port number, for example `http://mdw.example.com:28080`.

The user's web browser must be configured to use the SPNEGO protocol so that it offers the user's Kerberos principal to the web browser. The method for configuring web browsers varies with different browsers and operating systems. Search online to find instructions to enable SPNEGO with your browser and OS.





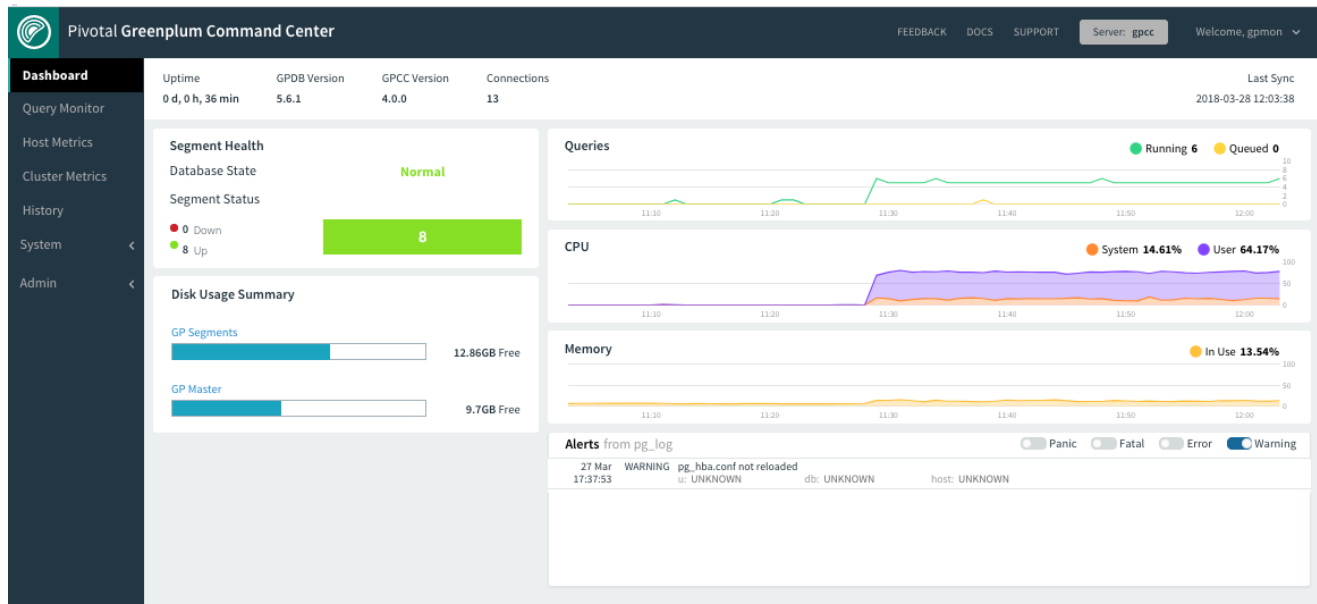
## Monitoring the Greenplum Database System

- [Dashboard](#)
- [Cluster State](#)
- [Segment Status](#)
- [Cluster Metrics](#)
- [Host Metrics](#)
- [Storage Status](#)

## Dashboard

The **Dashboard** displays when you first sign in to Pivotal Greenplum Command Center. The **Dashboard** provides a quick view of the current system status, Segment Health, Queries, CPU, Memory, and Disk usage.

Clicking on a panel provides more detailed information about the metric. The Alerts panel shows the most recent messages from the Greenplum Database log file. Some information is available only to Command Center users with Admin or Operator permission level.



## System Information

The following system information is displayed at the top of the page.

### Uptime

The elapsed time since the Greenplum Database system was last started.

### GPDB Version

The version of the Greenplum Database software the monitored cluster is running.

### GPCC Version

The version of the Greenplum Command Center software.

### Connections

The number of active Greenplum Database sessions (client connections).

### Server

The display name for this Greenplum Command Center.

### Last Sync

Date and time the data was last synchronized. The Command Center user interface updates views with live data every 15 seconds.

## Segment Health

The **Segment Health** section of the Dashboard provides a quick overview of the status of the database system and segments this Command Center monitors.

## Database State

**Database State** is the current state of the Greenplum Database system. The state can be one of the following:

- **Normal:** The database is functioning with no major errors or performance issues.
- **Segment(s) Down:** The database is in change-tracking mode or resync mode. Overall performance and system reliability is greatly reduced. See the *Pivotal Greenplum Database System Administrator Guide* for information about resolving this condition.
- **Database Unreachable:** The Greenplum Performance Monitor agent cannot connect to the database. The database is likely down. See the *Pivotal Greenplum Database System Administrator Guide* for troubleshooting information.
- **Unbalanced:** Some segments are not running in their preferred roles. That is, primaries are running as mirrors and mirrors are running as primaries, resulting in unbalanced processing.
- **Resyncing:** The database is performing a recovery or rebalance operation.

## Segment Status

The bar graph in the **Segment Status** section shows the up or down status of all database segments in your Pivotal Greenplum Database system. A color indicator and associated number indicate the number of database segments that are currently in that particular state. Segments can have the following states:

- **Up** (Green)
- **Down** (Red)

Clicking the **Segment Status** panel displays the [Segment Status](#) Command Center page.

## Disk Usage Summary

This chart displays total disk usage and disk available for the Greenplum master host and segment hosts at the last synchronization. Hover over the chart to see the amount of disk used, free, and total.

## Queries

This graph displays a summary view of active and queued queries for the last 60 minutes. Click on the colored dot next to the **Running** or **Queued** label to toggle the line on or off. At least one line must be visible at all times. Hover over the graph to display the number of queries for each visible line at that point in time.

## CPU

This graph displays average CPU usage across the entire cluster, for the last 60 minutes. The graph displays separate lines for system processes and user processes. The user CPU usage includes the Greenplum database master, standby, and segment processes. Click on the colored dot next to the **System** or **User** label to toggle that line on or off. At least one line must be visible at all times.

Hovering the cursor over a line in the graph displays a small window with the percentage of CPU used at that point in time for the visible lines and the total if both the system and user lines are visible.

## Memory

This graph displays the average percent of memory used across the entire cluster over the last 60 minutes. Hover over the line to display the percent of memory used at that point in time.

## Alerts

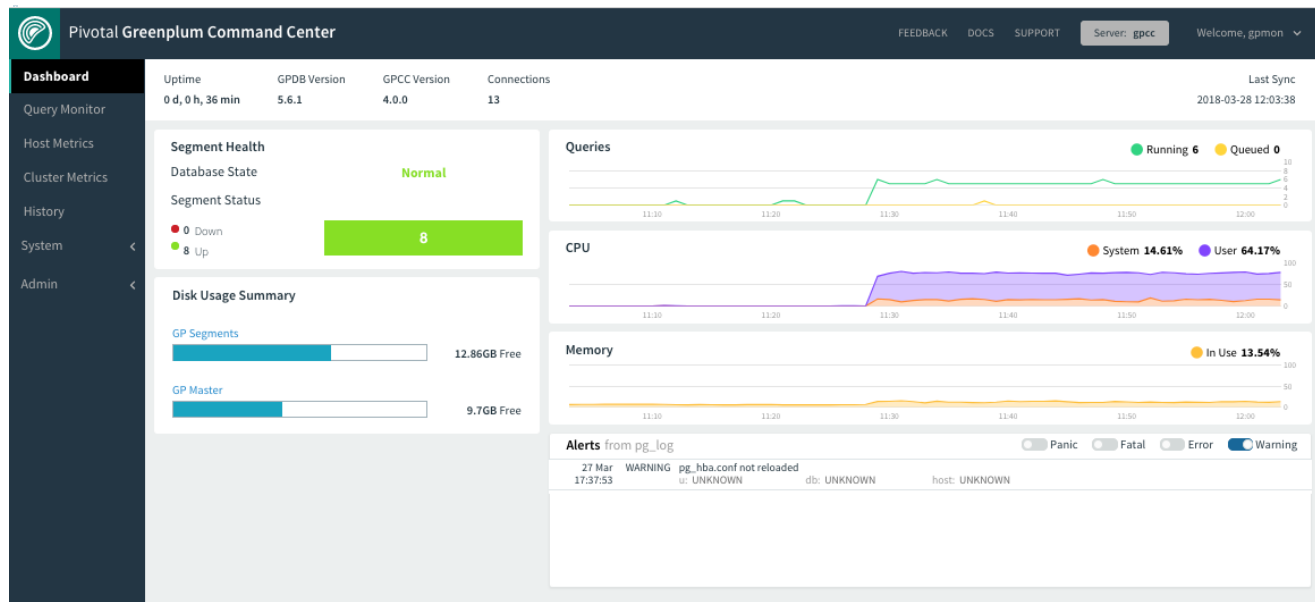
*Admin and Operator permission levels only*

The **Alerts** panel displays recent messages from the Greenplum Database `pg_log` log file. The panel is updated at each synchronization. Filter the messages by severity level using the controls at the top right of the panel.



## Greenplum Database Cluster State

The Greenplum Command Center **Dashboard** provides a quick view of the current system status, Segment Health, Queries, CPU, Memory, and Disk usage. Clicking on a panel provides more detailed information about that metric. The **Alerts** panel shows the most recent messages from the Greenplum Database log file. Some information is available only to Command Center users with Admin or Operator permission level.



## System Information

The following system information is displayed at the top of the page.

### Uptime

The elapsed time since the Greenplum Database system was last started.

### GPDB Version

The version of the Greenplum Database software the monitored cluster is running.

### GPCC Version

The version of the Greenplum Command Center software.

### Connections

The number of active Greenplum Database sessions (client connections).

### Server

The display name for this Greenplum Command Center.

### Last Sync

Date and time the data was last synchronized. The Command Center user interface updates views with live data every 15 seconds.

## Segment Health

The **Segment Health** section of the Dashboard provides a quick overview of the status of the database system and segments this Command Center monitors.

## Database State

**Database State** is the current state of the Greenplum Database system. The state can be one of the following:

- **Normal:** The database is functioning with no major errors or performance issues.
- **Segment(s) Down:** The database is in change-tracking mode or resync mode. Overall performance and system reliability is greatly reduced. See the *Pivotal Greenplum Database System Administrator Guide* for information about resolving this condition.
- **Database Unreachable:** The Greenplum Performance Monitor agent cannot connect to the database. The database is likely down. See the *Pivotal Greenplum Database System Administrator Guide* for troubleshooting information.
- **Unbalanced:** Some segments are not running in their preferred roles. That is, primaries are running as mirrors and mirrors are running as primaries, resulting in unbalanced processing.
- **Resyncing:** The database is performing a recovery or rebalance operation.

## Segment Status

The bar graph in the **Segment Status** section shows the up or down status of all database segments in your Pivotal Greenplum Database system. A color indicator and associated number indicate the number of database segments that are currently in that particular state. Segments can have the following states:

- **Up** (Green)
- **Down** (Red)

Clicking the **Segment Status** panel displays the [Segment Status](#) Command Center page.

## Disk Usage Summary

This chart displays total disk usage and disk available for the Greenplum master host and segment hosts at the last synchronization. Hover over the chart to see the amount of disk used, free, and total.

## Queries

This graph displays a summary view of active and queued queries for the last 60 minutes. Click on the colored dot next to the **Running** or **Queued** label to toggle the line on or off. At least one line must be visible at all times. Hover over the graph to display the number of queries for each visible line at that point in time.

## CPU

This graph displays average CPU usage across the entire cluster, for the last 60 minutes. The graph displays separate lines for system processes and user processes. The user CPU usage includes the Greenplum database master, standby, and segment processes. Click on the colored dot next to the **System** or **User** label to toggle that line on or off. At least one line must be visible at all times.

Hovering the cursor over a line in the graph displays a small window with the percentage of CPU used at that point in time for the visible lines and the total if both the system and user lines are visible.

## Memory

This graph displays the average percent of memory used across the entire cluster over the last 60 minutes. Hover over the line to display the percent of memory used at that point in time.

## Alerts

*Admin and Operator permission levels only*

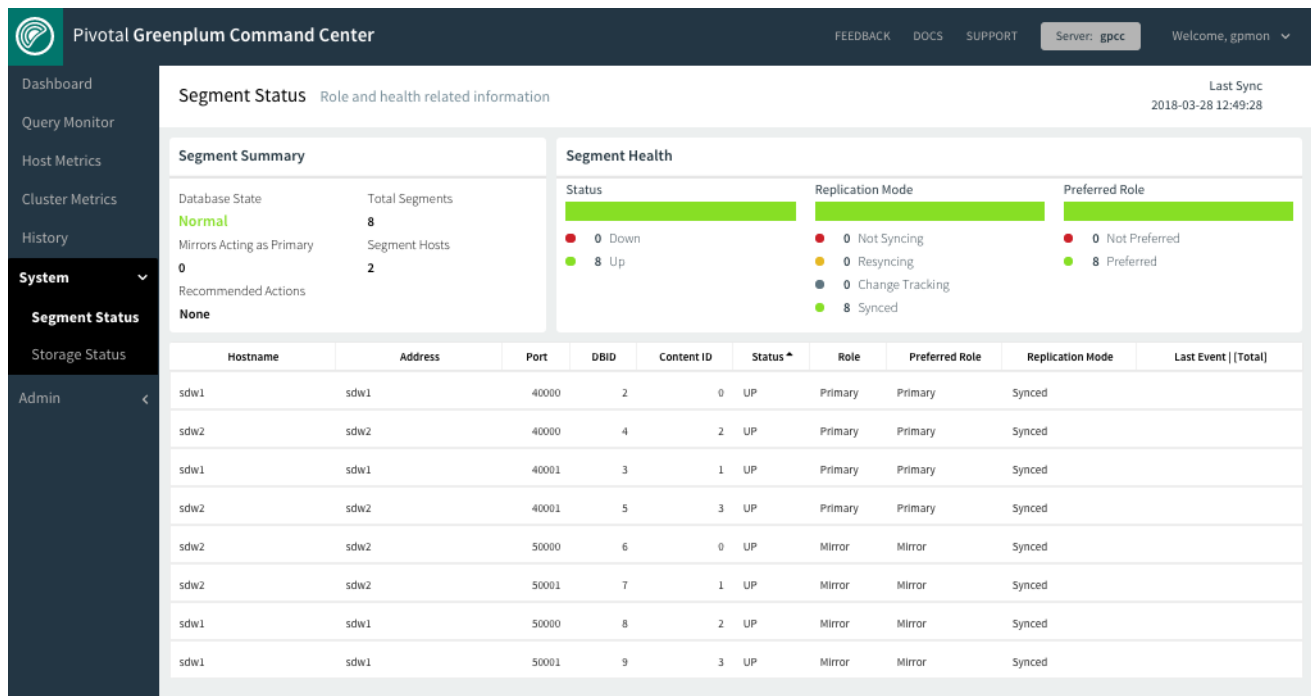
The **Alerts** panel displays recent messages from the Greenplum Database `pg_log` log file. The panel is updated at each synchronization. Filter the messages by severity level using the controls at the top right of the panel.





## Segment Status

The **Segment Status** page provides a health overview for the Greenplum Database segments and details for each primary and mirror segment.



## Segment Summary

Greenplum Database is most efficient when all segments are operating in their preferred roles. The **Segment Summary** panel tells you the overall segment status and if any mirrors are acting as primaries.

The **Segment Summary** panel provides the following information:

### Database State

The database state can be one of the following:

- **Normal:** The database is functioning with no major errors or performance issues.
- **Segment(s) Down:** The database is in change-tracking mode or resync mode. Overall performance and system reliability is greatly reduced. See the *Pivotal Greenplum Database System Administrator Guide* for information about resolving this condition.
- **Database Unreachable:** The Greenplum Performance Monitor agent cannot connect to the database. The database is likely down. See the *Pivotal Greenplum Database System Administrator Guide* for troubleshooting information.
- **Unbalanced:** Some segments are not running in their preferred roles. That is, primaries are running as mirrors and mirrors are running as primaries, resulting in unbalanced processing.
- **Resyncing:** The database is performing a recovery or rebalance operation.

### Mirrors Acting as Primary

The number of mirror segments acting as primary segments.

### Recommended Actions

Suggests actions to perform to restore the cluster to balance. These include:

- Recover and Rebalance
- Rebalance

These actions are executed from the command line using the `gprecoverseg` Greenplum management utility. See `gprecoverseg` in the *Pivotal Greenplum Database Utility Reference* for more information.

## Total Segments

The total number of primary and mirror segments in the Greenplum cluster.

## Segment Hosts

The total number of segment hosts in the Greenplum cluster.

## Segment Health

The **Segment Health** panel contains charts for Greenplum Database segments' status, replication mode, and preferred roles.

### Status

Numbers of segments that are down and up.

### Replication Mode

A chart that shows the number of segments in each of the possible replication modes.

- **Not Syncing:** The primary segment and mirror segment are active and all changes to the primary segment have been copied to the mirror using a file block replication process.
- **Change Tracking:** If a primary segment is unable to copy changes to its mirror segment using the file replication process, it logs the unsent changes locally so they can be replicated when the mirror again becomes available. This can happen if a mirror segment goes down or if a primary segment goes down and its mirror segment automatically assumes the primary role.
- **Resyncing:** When a down segment is brought back up, administrators initiate a recovery process to return it to operation. The recovery process synchronizes the segment with the active primary and copies the changes missed while the segment was down.
- **Synced:** Once all mirrors and their primaries are synchronized, the system state becomes synchronized.

## Preferred Roles

The red portion of the Preferred Role chart shows the numbers of segments that not operating in their preferred primary or mirror roles. If the chart is not solid green, the performance of the Greenplum cluster is not optimal.

Primary and mirror segments are distributed evenly among the segment hosts to ensure that each host performs an equivalent share of the work and primary segments and their mirror segments reside on different segment hosts. When a primary segment goes down, its mirror on another host in the cluster automatically assumes the primary role, increasing the number of primary segments running on that host. This uneven distribution of the workload will affect query performance until the down segment is restored and the segments are returned to their original, preferred, roles.

## Segment Table

The table at the bottom of the **Segment Status** page contains a detailed row for every primary and mirror segment in the Greenplum Cluster. The table has the following columns for each segment:

### Hostname

The name of the segment host where the segment is running.

### Address

The network interface on the segment host for the segment.

### Port

The port number assigned to the segment.

### DBID

The unique identifier for the segment instance.

### ContentID

The content identifier for the segment, from 0 to the number of segments minus 1. A primary segment and its mirror have the same ContentID. The master and standby master, which have ContentID -1, are excluded from the table.

### Status

"UP" if the segment is running, "DOWN" if the segment has failed or is unreachable.

### Role

The segment's current role, either "primary" or "mirror".

## Preferred Role

The segment's intended role, either "primary" or "mirror".

## Replication Mode

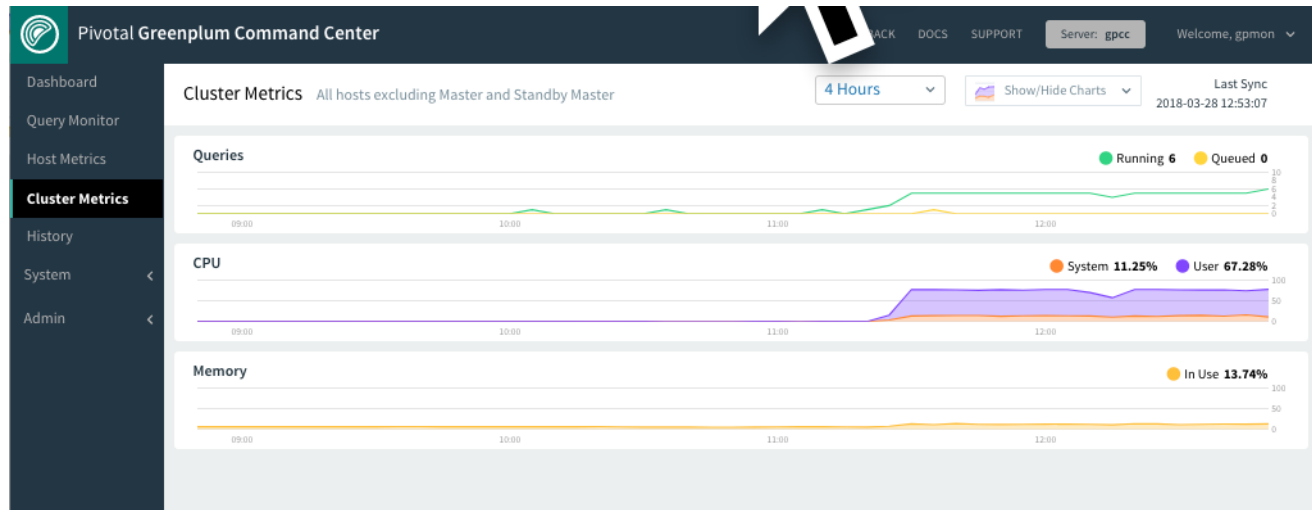
The replication status for the segment. See [Segment Health](#) for possible values.

## Last Event[Total]

The date and time of last segment health-related activity. Click to display a list of recent events.

## Cluster Metrics

The **Cluster Metrics** page shows consolidated statistics for all segment hosts in the Greenplum cluster. Master and standby master hosts are excluded from the metrics.



The charts display metrics for the last time period set by the control in the top right corner of the screen.

Use the **Show/hide Charts** control to choose which metrics to display.

Hover over any of the charts to see values for the metrics at a point in time in pop-up boxes. The charts are synchronized so that hovering over any chart shows the same point in time in all charts.

The current value of a metric is shown in the upper right corner of its chart.

On charts with multiple metrics, toggle the display for a line on or off by clicking the line's label in the legend at the top right of the chart. At least one line must be displayed. All lines are redisplayed at the next quantum interval.

The page has charts for the following metrics:

### Queries

The number of queries running and the number of queries queued to run.

### CPU

The percentage CPU used by system processes and the percentage CPU used by user processes.

### Memory

Percentage of memory in use.

Memory is calculated as follows:

Total = MemTotal

Free = MemFree + Buffers + Cached

Used = MemTotal - Free

### Disk I/O

Disk read and write rates in megabytes per second.

### Network

Network I/O read and write rates in megabytes per second. Network metrics include traffic over all NICs (network interface cards), including internal interconnect and administrative traffic.

### Load

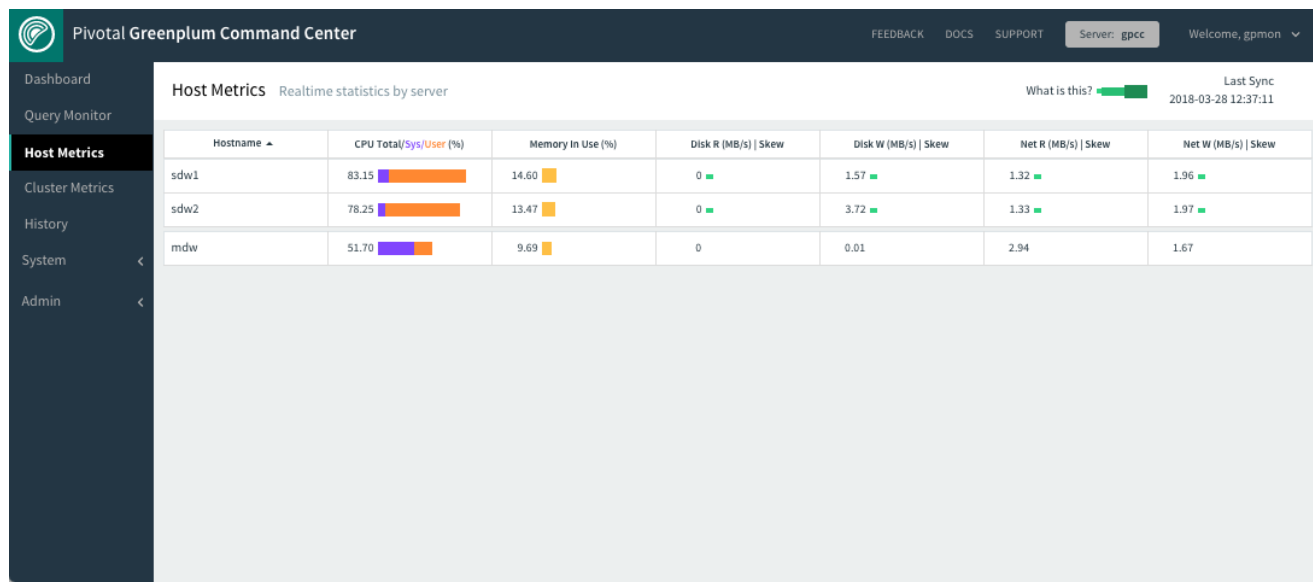
System load average for 1-minute, 5-minute, and 15-minute periods.

### Swap

Percentage of swap space used.

## Host Metrics

The **Host Metrics** page displays a table of the hosts in the cluster with statistics collected at the most recent quantum interval.



At the top, **Last Sync** displays the time the statistics were last updated.

Click a column header to sort the table by that column. Click again to toggle between ascending and descending sort. Master and standby hosts are not included in the sort and are always displayed following the sorted list of segment hosts.

For each server, the following columns are displayed:

### Hostname

The hostname name of the server.

### CPU Total/Sys/User (%)

The total percentage of CPU in use is displayed next to a graph illustrating the CPU used for system and user processes. Hover over the table cell to show the percentages used for system and user processes and the percentage CPU idle.

### Memory In Use (%)

The percentage of host memory in use is displayed next to a graph illustrating the memory in use and available. Hover over the table cell to see memory used and available in gigabytes.

Memory is calculated as follows:

Total = MemTotal

Free = MemFree + Buffers + Cached

Used = Total - Free

### Disk R (MB/s) | Skew

Disk read rate in megabytes per second is displayed next to a graph of calculated disk read skew. Hover over the table cell to see a Low/Medium/High rating for disk skew.

### Disk W (MB/s) | Skew

Disk write rate in megabytes per second is displayed next to a graph of calculated disk write skew. Hover over the table cell to see a Low/Medium/High rating for disk write skew.

### Net R (MB/s) | Skew

Network read rate in megabytes per second is displayed next to a graph of calculated network read skew. Hover over the table cell to see a Low/Medium/High rating for network read skew.

### Net W (MB/s) | Skew

Network write rate in megabytes per second is displayed next to a graph of calculated network write skew. Hover over the table cell to see a Low/Medium/High rating for network write skew.

## About Skew Calculations

Disk and Network skew ratings are calculated as each server's standard deviation from the mean calculated from all segment hosts.

#### Low

Value is within 1 standard deviation from the mean. (Note: if the variance of the set is less than 3, skew is considered low regardless of deviation from mean.)

#### Moderate

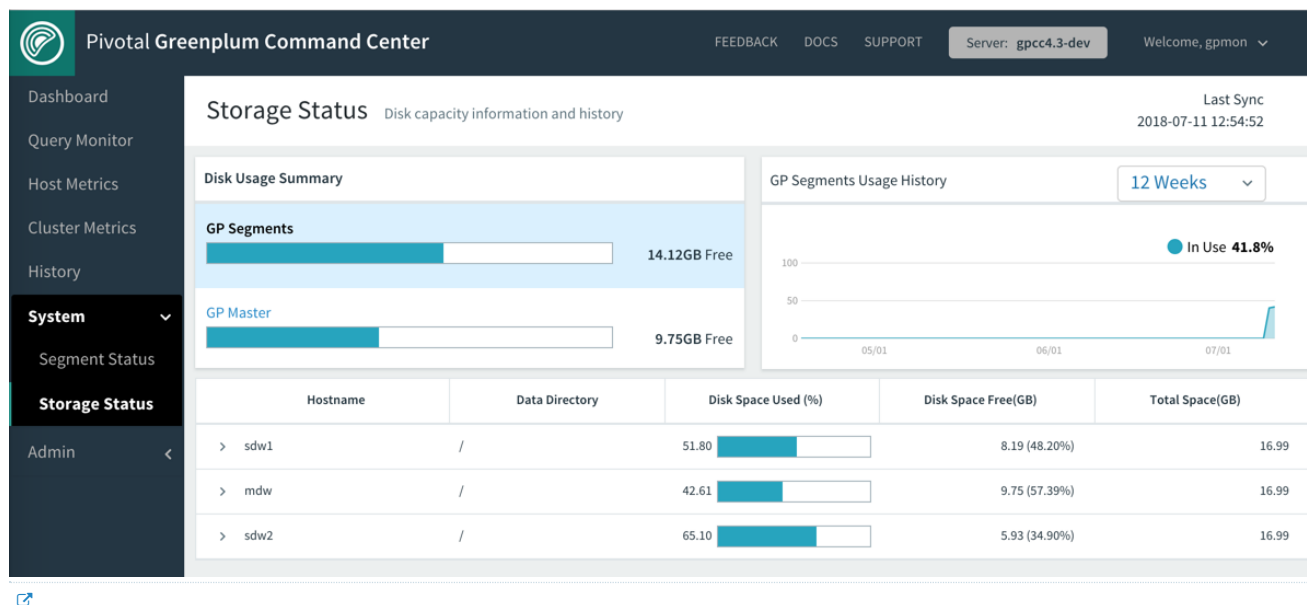
Value is between 1 and 2 standard deviations from the mean.

#### Very High

Value is greater than 3 standard deviations from the mean.

## Storage Status

The **Storage Status** page shows current historical disk usage for Greenplum master and segment hosts.



## Disk Usage Summary

You can see current disk space in use, space free, and total space in the Disk Usage Summary panel. Disk space metrics for the segment hosts (GP Segments) and the master (GP Master) are shown in separate bar charts.

The GP Segments bar chart shows combined disk space for all segments.

The GP Masters bar chart shows combined disk space for master and standby master.

Hover over either of the charts to see the space used, free, and total in gigabytes and as a percentage of the total.

## GP Segments Usage History

The GP Segments Usage History panel presents a chart of percentage of disk space in use for the time period set by the control in the panel header.

Hover over the chart to see the percentage disk in use on any given point.

## Storage Status Table

The Storage Status table provides current disk space usage metrics for each host and by data directory within hosts.

## Monitoring and Managing Greenplum Database Queries

- [Query Monitor](#)
- [Query Details](#)
- [Query History](#)



## Query Monitor

The **Query Monitor** view allows you to view information for all Greenplum Database server queries, including details about queries running, queued to run, and blocked by other queries. Users with Admin or Operator permission can see and cancel all users' queries.

**Query Monitor** Current queries by all users

Current Time: 2018-07-11 15:42:05

25 Running 0 Queued 2 Blocked

Query ID	Status	User	Database	Workload	Submitted	Queued Time	Run Time	Spill Files	Blocked by
1531266727-13954-2	Running	gpadmin	gpadmin	admin_gr...	15:35:48	4m 53s	1m 35s	--	--
1531266727-13956-2	Running	tpch_1	gpadmin	default_g...	15:35:54	4m 50s	1m 32s	352.80 MB	--
1531266727-13968-2	Running	tpch_1	gpadmin	default_g...	15:36:20	4m 24s	1m 32s	179.79 MB	--
1531266727-14005-2	Running	tpch_1	gpadmin	default_g...	15:39:01	1m 43s	1m 32s	158.94 MB	--
1531266727-14011-2	Running	tpch_4	gpadmin	benchmark	15:39:34	1m 11s	1m 31s	216.40 MB	--
1531266727-14033-2	Running	tpch_1	gpadmin	benchmark	15:40:12	32s	1m 32s	102.81 MB	--
1531266727-14034-2	Running	tpch_1	gpadmin	benchmark	15:40:13	1s	2m 2s	102.72 MB	--
1531266727-14035-2	Running	tpch_1	gpadmin	benchmark	15:40:13	4s	1m 59s	406.96 MB	--
1531266727-14036-2	Running	tpch_1	gpadmin	benchmark	15:40:13	2s	2m 1s	143.46 MB	--
1531266727-14037-2	Running	tpch_1	gpadmin	benchmark	15:40:13	2s	2m 1s	98.08 MB	--
1531266727-14038-2	Running	tpch_1	gpadmin	benchmark	15:40:13	2s	2m 1s	129.43 MB	--
1531266727-14039-2	Running	tpch_4	gpadmin	benchmark	15:40:14	31s	1m 31s	95.54 MB	--
1531266727-14040-2	Running	tpch_4	gpadmin	benchmark	15:40:14	2s	2m 0s	135.91 MB	--
1531266727-14041-2	Running	tpch_1	gpadmin	benchmark	15:40:14	1s	2m 1s	99.39 MB	--

If a Command Center administrator has enabled Query Monitor Guest Access, anyone able to access the Command Center web server can view the system status and query list on this page without signing in to Command Center. Anonymous users, however, cannot cancel queries or access any other Command Center features.

With the information available in this view, Greenplum Database administrators can easily:

- Understand how the system is being used — both in real-time and trending over time.
- Identify and diagnose problem queries while they are running, detect skew, find runaway queries, and so on.
- Review and balance the query load on the system by better optimizing and scheduling the query load.
- Cancel queries that disrupt system performance.

## Query Metrics

The Query Monitor table displays the following columns for queries.

### Query ID

An identification string for the query. If the column is blank, no query ID has been assigned yet. In the Console, this looks like "1295397846-56415-2". Command Center generates this ID by combining the query record's `tmid`, `ssid`, and `ccnt` fields.

- `tmid` is a time identifier for the query.
- `ssid` is the session id.
- `ccnt` is the number of the command within the session.

### Status

The status of the query. This can be one of the following:

- Queued: the query has not yet started to execute
- Running: execution has started, but is not yet complete
- Blocked: the query is waiting for one or more other queries to release locks
- Done: completed successfully
- Cancelling: cancel request sent, cancel pending
- Cancelled: terminated, no longer running
- Idle Transaction: the transaction is open, but idle, for example, waiting while a user in an interactive session enters a statement

## User

The Greenplum Database role that submitted the query.

## Database

The name of the database that was queried.

## Workload

The resource group or resource queue that is managing the query.

## Submitted

The time the query was submitted to the query planner.

## Queued Time

The amount of time the query has been (or was) in queue awaiting execution.

## Run Time

The amount of time since query execution began.

## Spill Files

The total size of spill files created for the query. Greenplum Database creates spill files when there is insufficient memory to execute the query in memory. See [Managing Spill Files Generated by Queries](#) for information about spill files.

## Blocked by

Shows the number of locks blocking the query. Hover over the column to display details of the locks. The tip shows the type of each lock, the ID of the transaction or query that holds the lock, the Greenplum Database role holding the lock, and the amount of time the query has been blocked.

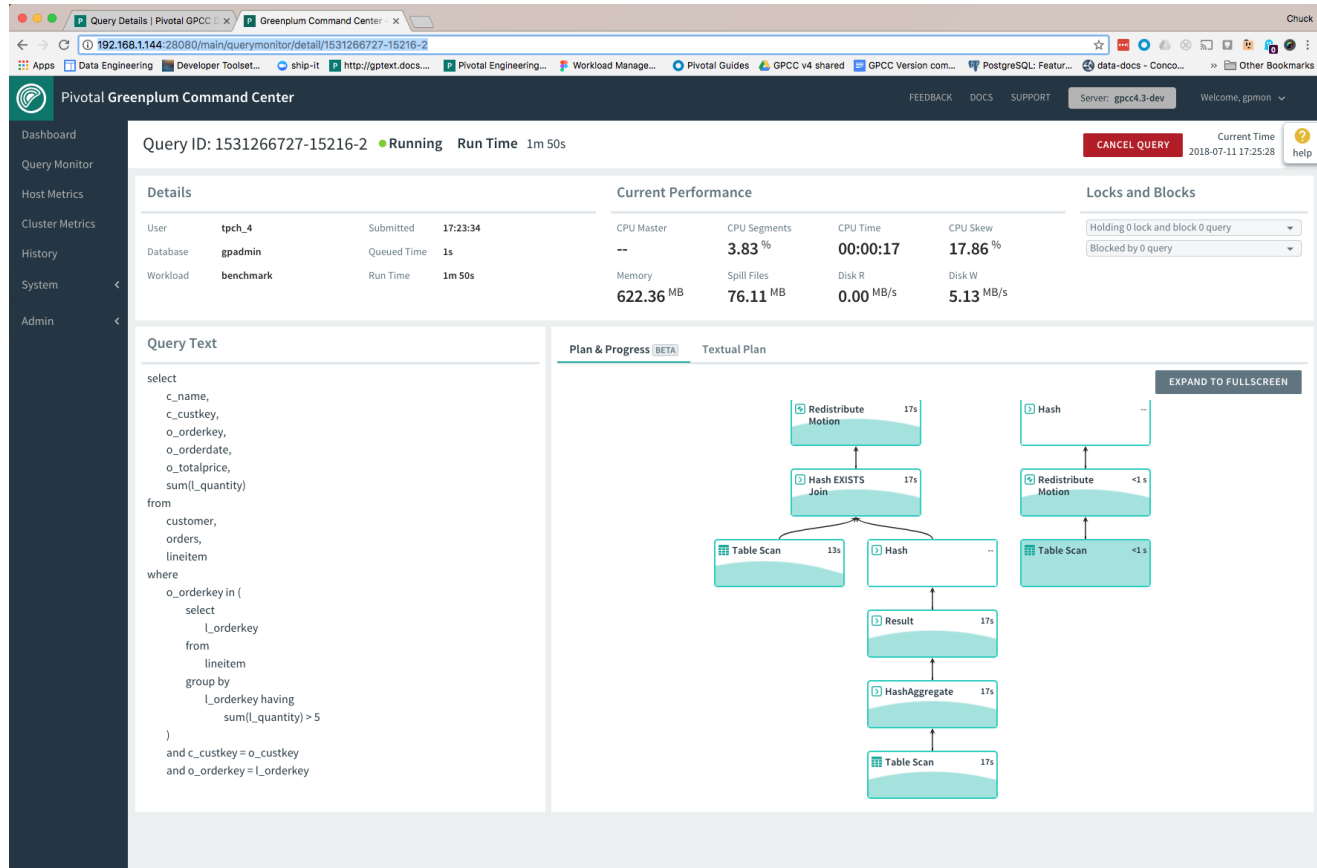
4s	--	--	1 Blockers
0s	1m 14s		Access Exclusive 1531266727-14058-2
0s	1m 7s	60	User gpadmin
1s	1m 6s	52	Query blocked for 1m 27s

## Using the Query Monitor Controls

- Click a column heading to sort the rows on that column in ascending or descending order.
- Click the checkbox at the left of a row to choose a query to cancel or export. Click the checkbox in the heading row to choose all queries.
- Click **Cancel Query** to cancel selected queries.
- Click **Export** to download a comma-separated values (CSV) text file containing rows for the selected queries. When no queries are selected, all rows are exported. The default file name is `spreadsheet.csv`.
- Click any query ID to see the [Query Details](#), including metrics, the text of the query, and the query plan.

## Query Details

The **Query Details** view displays query metrics, the text of the query, and the query plan and progress for a single query selected from the [Query Monitor](#) view.



## Query Execution Metrics

The Query ID, execution status, and run time of the query are displayed at the top.

The following metrics are displayed for the query.

### User

The Greenplum Database role that submitted the query.

### Database

The name of the database that was queried.

### Workload

The name of the resource group or resource queue that is managing the query.

### Submitted

The time the query was submitted to the query planner.

### Queued Time

The amount of time the query has been (or was) in queue awaiting execution.

### Run Time

The amount of time since query execution began.

### CPU Master

Current CPU percent on the Greenplum Database master host for this query.

## CPU Segments

(Active queries only.) Current CPU percent average for all segment processes executing this query. The percentages for all processes running on each segment are averaged, and then the average of all those values is calculated to render this metric. Current CPU percent average is always zero in historical and tail data. The master and standby master are excluded from the calculation.

## CPU Time

Total CPU time consumed by all processes on all segments executing this query.

## CPU Skew

The amount of CPU skew. CPU skew occurs when query executor processes for one segment use a disproportionate amount of CPU compared to processes for other segments executing the query. This value is calculated as

$$1 - (\text{average\_segment\_CPU} / \text{maximum\_segment\_CPU})$$

## Memory

Memory consumed by all segment processes executing the query.

## Spill Files

The total size of spill files created for the query. Greenplum Database creates spill files when there is insufficient memory to execute the query in memory. See [Managing Spill Files Generated by Queries](#) for information about spill files.

## Disk R

The current average disk read rate for all segment hosts.

## Disk W

The current average disk write rate for all segment hosts.

## Locks and Blocks

Contains two lists of locks currently blocking transactions. Click a list to expand and view the contents.

- A list of locks held by this query, including the type of each lock and the queries blocked by that lock.

### Locks and Blocks

Holding <b>1</b> lock and block <b>3</b> query	
Access Exclusive	<a href="#">1531266727-15345-2</a>
--	<a href="#">1531266727-15341-2</a>
	<a href="#">1531266727-15342-2</a>
Blocked by <b>12</b> query	



- A list of queries that hold locks that block this query and the lock type.

### Locks and Blocks

Holding <b>1</b> lock and block <b>3</b> query	
Blocked by <b>12</b> query	
<a href="#">1531266727-15295-2</a>	Access Share
<a href="#">1531266727-15157-2</a>	Access Share
<a href="#">1531266727-15160-2</a>	Access Share



## Query Text and Execution Plan

The query text and the query's plan and execution progress are shown in the lower panels of the Query Details view. The text of the query is displayed in the left panel, and the plan and progress is displayed in the right panel.

### Query Text

The **Query Text** panel displays the text of the query as it was submitted to Greenplum Database.

Command Center can display up to 100K characters. If you click **COPY**, up to 100K characters of the query text are copied to the clipboard.

If the query text is longer than 100K characters, a message is displayed with a link you can use to download the full text of the query. The name of the text file is the ID of the query with a `.txt` extension. The file is available to download for 24 hours after the query completes, or until the query has been saved to history, once history collection is enabled.

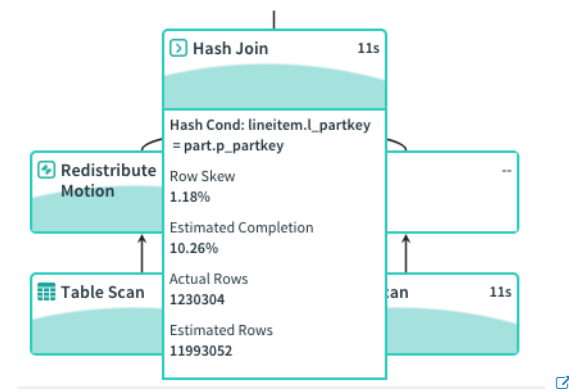
## Query Plan and Progress

The **Plan & Progress** tab in the lower right panel is a graphical representation of the query plan with animation and real-time metrics to show execution progress. Each box in the tree represents a step in the query execution plan. The boxes are labeled with the operation they represent and have a CPU usage metric. Query execution begins at the bottom of the tree and ends at the top.

Before a step begins to execute, the box has a solid white fill. When the step becomes active, the box is animated with a green and white fill to indicate that the operator is working. When the step has completed, the box has a solid green fill.

Query execution plans are executed in “slices,” portions of the query plan that segments can work on independently in parallel. The plan is sliced wherever a data motion operator occurs. The time displayed in the upper right corner of each box is the amount of CPU time used for all steps in the slice to which the step belongs. The visual query plan does not illustrate slices, but you can find information about slices in the textual plan.

If you click a step, the box expands to show additional details.



The expanded plan box contains the following metrics.

- The type of operator. When the operator is a table scan, the name of the scanned table is included. See [Query Plan Execution](#) for descriptions of the operators.
- Information related to the current operation, such as the hash key, merge key, join condition, or filter condition.
- Row Skew - the amount of row skew for the current operator, a value from 0% to 100%. Row skew occurs when some segments process more rows than other segments. The percentage is calculated as  $(1 - (\text{average\_segment\_rows} / \text{maximum\_segment\_rows})) * 100$ .
- Estimated Completion - the current percentage of actual rows to estimated rows for this plan step. The percentage can exceed 100% if the operation produces more rows than the optimizer's estimate. The percentage changes to “Completed” when the operation completes.
- Actual Rows - The current number of rows produced by this step. Note that for nested join operators, the Actual Rows is estimated since the actual row counts are not available while the join is executing.
- Estimated Rows - The estimated number of rows the operator will produce.

## Textual Plan

Select the **Textual Plan** tab and click **RUN EXPLAIN** to generate the text representation of the explain plan.



The **RUN EXPLAIN** button is dimmed if Command Center is unable to generate the explain plan. Command Center is unable to generate the explain plan if the size of the query text is greater than 100K or if the query text contains multiple statements.

Query ID: 1527709348-39-3 ● Running Run Time 4m 9s

CANCEL QUERY

Current Time  
2018-05-30 14:47:53

help

Details	Current Performance		Blocking (0)	Blocked by (0)
User: <b>tpch_4</b>	CPU: <b>11.08 %</b>	CPU Skew: <b>41.67 %</b>		
Database: <b>gpadmin</b>	Memory: <b>511.64 MB</b>	Spill Files: <b>608.69 MB</b>		
Res Queue: <b>pg_default</b>	Disk R: <b>0.00 MB/s</b>	Disk W: <b>2.06 MB/s</b>		
Submitted: <b>14:43:51</b>				
Queued Time: <b>0s</b>				
Run Time: <b>4m 9s</b>				

### Query Text

```

select
  c_name,
  c_custkey,
  o_orderkey,
  o_orderdate,
  o_totalprice,
  sum(l_quantity)
from
  customer,
  orders,
  lineitem
where
  o_orderkey in (
    select
      l_orderkey
    from
      lineitem
    group by
      l_orderkey having
        sum(l_quantity) > 5
  )
  and c_custkey = o_custkey
  and o_orderkey = l_orderkey
group by
  c_name,
  c_custkey,
  o_orderkey,
  o_orderdate,
  o_totalprice
order by
  o_totalprice desc,
  o_orderdate
;

```

### Plan & Progress BETA

#### Textual Plan

```

Gather Motion 4:1 (slice3; segments: 4) (cost=0.00..6554.33 rows=2402130 width=49)
Merge Key: orders.o_totalprice, orders.o_orderdate
-> GroupAggregate (cost=0.00..6160.61 rows=600533 width=49)
  Group By: orders.o_totalprice, orders.o_orderdate, customer.c_name, customer.c_custkey, orders.o_orderkey
  -> Sort (cost=0.00..6115.27 rows=600533 width=48)
    Sort Key: orders.o_totalprice, orders.o_orderdate, customer.c_name, customer.c_custkey, orders.o_orderkey
    -> Hash Join (cost=0.00..2977.88 rows=600533 width=48)
      Hash Cond: public.lineitem.l_orderkey = orders.o_orderkey
      -> Table Scan on lineitem (cost=0.00..558.99 rows=1501332 width=11)
      -> Hash (cost=1888.16..1888.16 rows=124319 width=41)
        -> Redistribute Motion 4:4 (slice2; segments: 4) (cost=0.00..1888.16 rows=124319 width=41)
          Hash Key: orders.o_orderkey
          -> Hash Join (cost=0.00..1872.21 rows=124319 width=41)
            Hash Cond: orders.o_custkey = customer.c_custkey
            -> Redistribute Motion 4:4 (slice1; segments: 4) (cost=0.00..1371.15 rows=124319 width=22)
              Hash Key: orders.o_custkey
              -> Hash EXISTS Join (cost=0.00..1362.59 rows=124319 width=22)
                Hash Cond: orders.o_orderkey = public.lineitem.l_orderkey
                -> Table Scan on orders (cost=0.00..459.64 rows=374619 width=22)
                -> Hash (cost=784.20..784.20 rows=124319 width=4)
                  -> Result (cost=0.00..784.20 rows=124319 width=4)
                    Filter: (sum(public.lineitem.l_quantity)) > 5::numeric
                    -> HashAggregate (cost=0.00..773.98 rows=310798 width=12)
                      Group By: public.lineitem.l_orderkey
                      -> Table Scan on lineitem (cost=0.00..558.99 rows=1501332 width=11)
                  -> Hash (cost=434.95..434.95 rows=37596 width=23)
                    -> Table Scan on customer (cost=0.00..434.95 rows=37596 width=23)

```

Settings: optimizer=on  
Optimizer status: PQO version 2.58.0

The textual plan is the output of the Greenplum Database `EXPLAIN` command for the query. The query plan steps are labeled with arrows (`->`) and the structure of the query plan tree is indicated with indentation.

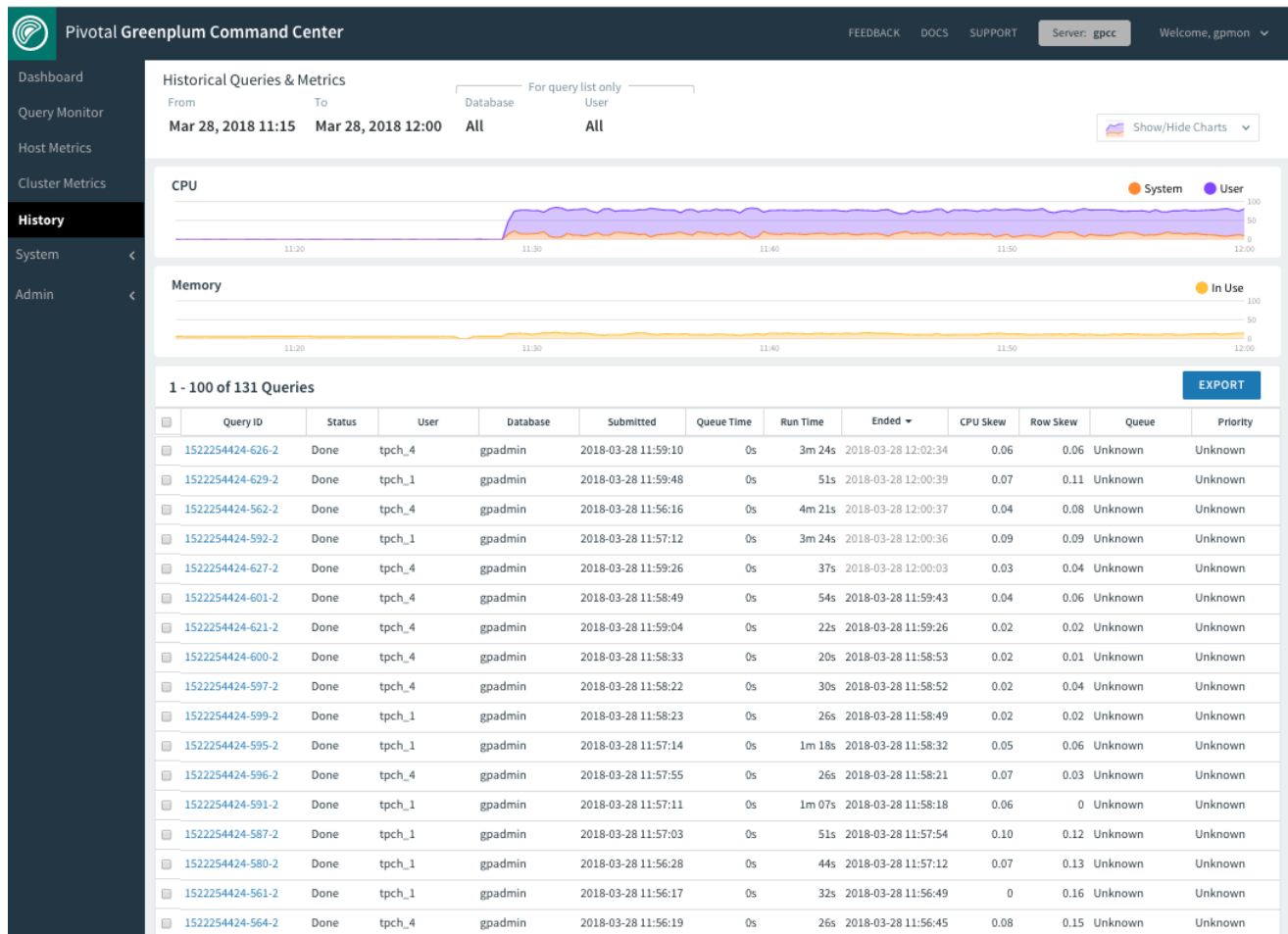
The `Optimizer status:` line at the bottom of the textual plan reports whether the explain plan was generated using the GPORCA optimizer (PQO) or the legacy query optimizer.

For help reading the textual explain plan see the [EXPLAIN](#) command in the *Greenplum Database Reference Guide* and [Query Profiling](#) in the *Greenplum Database Administrator Guide*. See [Query Execution](#) for descriptions of the query operators.

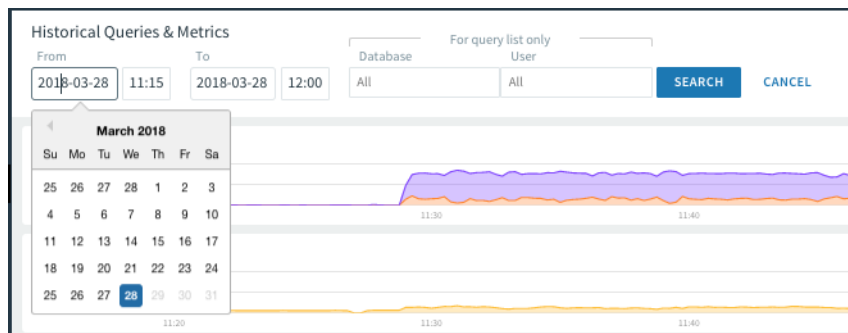
## History

The **History** page allows you to display system metrics and queries executed during a specified time period. Queries may also be filtered by database and/or user.

**Note:** The History data is not derived from the real-time metrics displayed by the Query Monitor and Query Detail view. History is collected and saved in the gppeermon database by the `gpmmmon` and `gpsmon` agents. Variations should be expected due to the different data collection methods.



Set the time period to display by entering dates and times in the **From** and **To** date and time fields. You can enter dates by typing them into the date field or by choosing from the pop-up calendar. Enter 24-hour times in HH:MM format.



To restrict queries that display in the query table at the bottom of the page, enter a Greenplum database name in the **Database** field, a user name in the **User** field, or both. Filtering by database and user only affects the queries displayed in the table. The metrics displayed in charts include all activity during the selected time period.

Click **Search** to display results that match your criteria.

You can click and drag on a chart to zoom in on a time range. Click **Search** to update the query list and charts to the selected range.

Scroll charts left or right by hovering over the edge of the chart and clicking an arrow. Click ‹ or › to move in half steps. Click ‹‹ or ›› to move in full steps.

In the query list, select or hover over a query to highlight its queued and run time in the charts.

Charts of the following metrics are available. Show or hide them at any time with the checklist at the upper right of the view.

#### Queries

The number of queries running and the number of queries queued to run.

#### CPU

The percentage of CPU used by system processes and the percentage of CPU used by user processes.

#### Memory

Percentage of memory in use.

#### Disk I/O

Disk read and write rates in megabytes per second.

#### Network

Network I/O read and write rates in megabytes per second. Network metrics include traffic over all NICs (network interface cards), including internal interconnect and administrative traffic.

#### Load

System load average for 1-minute, 5-minute, and 15-minute periods.

#### Swap

Percentage of swap space used.

## Query Metrics

The Query table displays queries that were active during the specified time period, including queries that started before or finished after the specified time. However, queries that are still active are not included in the table; these queries can be viewed on the [Query Monitor](#) page.

The query table has the following columns:

#### Query ID

An identification string for the query. In the Console, this looks like “1295397846-56415-2”.

#### Status

The final status of the query. This can be one of the following:

- Done
- Cancelled

#### User

The Greenplum Database user who submitted the query.

#### Database

The name of the database that was queried.

#### Submit Time

The time the query was submitted to the query planner.

#### Queued Time

The amount of time a query spent in the queue before it was executed.

#### Run Time

The amount of time the query required to produce a result.

#### End Time

The time the query completed or was cancelled.

#### CPU Skew

The amount of CPU skew. CPU skew occurs when query executor processes for one segment use a disproportionate amount of CPU compared to processes for other segments executing the query. This value is the coefficient of variation for the CPU used by processes running this query on each segment, multiplied by 100. For example, a value of .95 is shown as 95.

#### Row Skew



A measure of row skew in the system. Row skew occurs when one segment produces a disproportionate number of rows for a query. This value is the coefficient of variation for the Rows Out metric of all iterators across all segments for this query, multiplied by 100. For example, a value of .95 is shown as 95.

#### Queue

The name of the resource queue for the query.

#### Priority

Each query inherits the priority assigned to its resource queue.

For more information about Resource Queues and Query Plans, refer to the *Greenplum Database Administrator Guide*.

## Alerts

On the **Admin > Alerts** page, an administrator can set up **alert rules** to detect and respond to events occurring in the Greenplum Database system and in currently executing database queries. When a rule is matched, Command Center logs a record.

You can set up email alerts by configuring an SMTP server in Greenplum Database or in Command Center. Additionally, you can create a `send-alert.sh` shell script to forward alerts to other destinations, such as an SMS gateway or a Slack channel. If the script is present, Command Center runs it whenever an alert is raised.

Command Center creates the `gpmetrics` schema in the `gpcc` database to store both rules and log records. See [gpmetrics Schema Reference](#) for information about the `gpcc_alert_rule` and `gpcc_alert_log` tables in the `gpmetrics` schema.

This topic contains the following subtopics:

- [Configuring Alert Rules](#)
- [Configuring Alert Email](#)
- [Creating a Send Alert Script](#)

## Configuring Alert Rules

Click **EDIT** to manage alert event rules. To enable an alert rule, enter any data required in the fields and check the box. Uncheck the box to disable the rule. Click **SAVE** when you have finished making changes to the alert configuration.

Alerts events

CANCEL SAVE

Receive email alerts for selected events:

☒ Segment failure

☒ Out of memory errors

☒ Average memory (segment hosts) exceeds 65 % for 10 min

☒ Spill files for a query exceeds 250 GB

☐ Memory (master) exceeds % for min

☐ Query runtime exceeds min

☐ Total disk space exceeds % full

☒ Query is blocked for 15 min

☒ Number of connections exceeds 5

☐ Average CPU (segment hosts) exceeds % for min

☐ CPU (master) exceeds % for min

### Segment failure

An alert is raised when one or more failed segments are detected. After the alert email is raised, Command Center will raise the alert every 30 minutes until the segments are recovered.

### Average memory (segment hosts) exceeds [%] for [N] min

An alert is raised when the average memory for all segment hosts exceeds the specified percentage for the specified number of minutes. Command Center samples all segment hosts every 15 seconds and calculates the mean of the samples. Only memory in use is considered; memory for buffers and cache is not included.

### Memory (master) exceeds [%] for [N] min

An alert is raised when the percent of memory used on the master host exceeds the specified percentage for the specified number of minutes. Command Center samples memory usage on the master host every 15 seconds and calculates the mean of the samples. Only memory in use is considered; memory for buffers and cache is not included.

### Total disk space exceeds [%] full

An alert is raised when the total of disk space in use for all segment hosts exceeds the specified percentage. Command Center gathers the *available disk space* and *total disk space* from each segment host in the Greenplum Database cluster. The *percent of total disk space in use* is calculated by the following formula:

```
100 - sum(<available disk space>) / sum(<total disk space>) * 100
```

A disk space alert is raised no more than once every 24 hours.

Number of connections exceeds [N]

An alert is raised when the total number of database connections exceeds the number specified. The number of connections is checked every 30 seconds. After an alert is raised, the metrics collector checks the number of connections every 30 minutes until the number of connections drops below the threshold, and then it resumes checking every 30 seconds.

Average CPU (segment hosts) exceeds [%] for [N] min

An alert is raised when the average percent of CPU used for all segment hosts exceeds the specified percentage for the specified number of minutes. Command Center samples all segment hosts every 15 seconds and calculates the mean of the samples.

CPU (master) exceeds [%] for [N] min

An alert is raised when the CPU usage on the master host exceeds the specified percentage for the specified number of minutes. Command Center samples CPU usage on the master host every 15 seconds and calculates the mean of the samples.

Out of memory errors

An alert is raised when an executing query fails with an out of memory (OOM) error. Note that no alert is raised if there is insufficient memory to start the query.

Spill files for a query exceeds [GB]

An alert is raised when the total disk space consumed by a running query's spill files exceeds the specified number of gigabytes. An alert is raised only once per query.

Query runtime exceeds [N] min

An alert is raised when a query runtime exceeds the number of minutes specified. This alert is raised just once for a query.

Query is blocked for [N] min

An alert is raised if a query remains in a blocked state for longer than the specified number of minutes. If an alert is raised, and then the query unblocks, runs, and blocks again for the specified time, an additional alert is raised. Blocked time excludes the time a query is queued before it runs. It is possible for a "Query runtime exceeds [N] min" rule to also trigger while a query is blocked.

## Configuring Alert Email

Command Center requires an SMTP server to send alert emails. If SMTP has been configured for Greenplum Database, Command Center will use the configured SMTP server, SMTP user, and password. You must enter values for the fields in the right column, **Send emails to** and **From**, whether you use the Greenplum Database SMTP server or enter another one.

## Configuring email With Command Center

Click **EDIT** in the **Manage email configuration** panel.

Manage email configuration

CANCEL

SAVE

SMTP Server address

smtp.example.com:465

Username

gpcc-alerts@example.com

Password

\*\*\*\*\*

Send emails to

gpcc-admin@example.com × gpdb-admin@example.com ×

From

noreply-gpcc-alerts@example.com ×

Emails will be sent from this address. If left blank, default noreply email will be used.

The alert email configuration is set with the following Greenplum Database server configuration parameters:

## SMTP Server address

The name or IP address of the SMTP server and the SMTP port number. The port number is typically 587 for connections with TLS encryption or 465 without encryption. If the `gp_email_smtp_server` configuration parameter is set in Greenplum Database, it is prefilled here. Ask your system admin for the correct values to enter. Example: `smtp.example.com:465`

## Username

The username of the account to authenticate with the SMTP server. If the `gp_email_smtp_password` configuration parameter is set in Greenplum Database, it is prefilled here. Example: `gpcc-alerts@example.com`

## Password

The password for the SMTP username. For security, the password is masked. If the `gp_email_smtp_password` configuration parameter is set in Greenplum Database, that value is used here.

## Send emails to

To add an address to the list, enter the address and press Enter. To remove an email address, click the `x` on the address.

## From

The email address to use for the `From:` address in the alert email. Example: `do-not-reply@example.com`. If you leave this field blank, Command Center uses the default value, `noreply-gpcc-alerts@pivotal.io`.

When you click **SAVE**, Command Center sends a test email to the addresses in the **Send emails to** field. The email contains a list of the currently configured alert rules. If there is an error in the SMTP server or username/password configuration and the email cannot be sent, Command Center displays an error message.

## Configuring email for Greenplum Database

The following server configuration parameters are used to configure SMTP email for Greenplum Database.

### gp\_email\_smtp\_server

The SMTP server and port. Example: `smtp.example.com:465`

### gp\_email\_smtp\_userid

The name of a user to authenticate with the SMTP service. Example: `gpcc-alerts@example.com`

### gp\_email\_smtp\_password

The password for the SMTP user.

### gp\_email\_from

The email address to set as the email sender. Example: `noreply-gpcc-alerts@example.com`

### gp\_email\_to

A semicolon-separated list of email addresses to receive alert messages. Example: `gpcc-admin@example.com;gpdb-admin@example.com`

Command Center uses the `gp_email_smtp_server`, `gp_email_smtp_userid`, and `gp_email_smtp_password` parameters if they are set. It ignores the remaining parameters.

You can check the current value of a configuration parameter by running the `gpconfig -s` command on the master host, for example:

```
gpconfig -s gp_email_smtp_server
```

Use the `gpconfig -c` option to set the values of server configuration parameters, for example:

```
$ gpconfig -c gp_email_smtp_server -v "smtp.example.com:465"
$ gpconfig -c gp_email_smtp_userid -v "gpcc-alerts@example.com"
$ gpconfig -c gp_email_smtp_password -v "changeme"
$ gpconfig -c gp_email_from -v "gpcc-alerts@example.com"
$ gpconfig -c gp_email_to -v "gpcc-admin@example.com:gpdb-admin@example.com"
```

Run `gpstop -u` to reload the configuration files after changing these configuration parameters.

## Creating a Send Alert Script

The send alert script is a shell script that you can use to send Command Center alerts to destinations such as SMS gateways, pagers, team collaboration tools like Slack, chat servers, archive files, alternative email servers, and so on. You can use the send alert script in addition to sending email from Command Center, or as an alternative to sending alert emails from Command Center.

Command Center looks for the script `$MASTER_DATA_DIRECTORY/gpmetrics/send-alert.sh` on the host where Command Center is running—either the master host or standby host. If the file exists and is executable by the `gpadmin` user, Command Center executes the script. The following variables are set on the command line when the script runs.

Variable	Description
LINK	URL of the Greenplum Command Center web server.
QUERYID	ID of the query, if the alert was triggered by a query.
SERVERNAME	Name of the Greenplum Command Center server.
QUERYTEXT	The text of the query, if the alert was triggered by a query.
ACTIVERULENAME	Current text the of rule, with user-specified values included.
LOGID	Value of this alert's <code>id</code> column in the <code>gpmetrics.gpcc_alert_log</code> table.
RULEDESCRIPTION	Text of the rule, including user-specified values, at the time the alert was raised.
ALERTDATE	Date the alert was raised.
ALERTTIME	Time the alert was raised.
SUBJECT	Subject line for email.

An example script that you can customize is provided at `$GPCC_HOME/alert-email/send_alert.sh.sample`. The example formats the alert as HTML email text and pipes it through the Linux `mail` command.

To set up a send alert script:

1. Copy the `$GPCC_HOME/alert-email/send_alert.sh.sample` file to `$MASTER_DATA_DIRECTORY/gpmetrics/send-alert.sh`.
2. Customize the script with code to format and deliver the alert to your desired destination.
3. Run `gpcc start` to restart Command Center and enable the script.

## Managing Greenplum Database Workloads

[About Workloads](#)

[Managing Greenplum Database Resource Groups](#)

[Importing Resource Queues to Resource Groups](#)

[Accessing the Workload Management Configuration Programmatically](#)

[Troubleshooting Enabling Resource Groups](#)

## About Greenplum Command Center Workload Management

Greenplum Database segment hosts have a set amount of memory, CPU, I/O, and network resources. If these resources start to run short due to heavy database load, queries can fail or the entire database system can become unacceptably slow. For this reason, it is important to manage database requests to prevent resource depletion.



Greenplum Database has two resource management systems: *resource queues* and *resource groups*. Command Center workload management is based on resource groups, the resource management system introduced in Greenplum Database version 5. Resource groups require enabling Linux control groups (cgroups), so Greenplum Database initially is set to perform resource management using resource queues.

When Command Center starts, it checks the resource management system enabled in your Greenplum Database system. If you have not yet enabled resource groups in your Greenplum Database system, the Command Center workload management view displays a message encouraging you to enable resource groups, including a link to documentation with the procedure for completing the task. When you start Command Center after enabling resource groups, click the **ENABLE WORKLOADS** button. Command Center presents a view to help you set the initial resource group configuration by importing your existing resource queues to resource groups.

See [Using Resource Groups](#) in the *Greenplum Database Administrator Guide* for a full description of resource management features available with resource groups and instructions to enable resource groups in Greenplum Database.

On the Command Center **Admin> Workload Mgmt** view, you can perform the following tasks:

- Create new resource groups in Greenplum Database
- Delete existing resource groups
- Change the number of concurrent transactions each resource group allows
- Change the percentages of available system CPU and memory each resource group manages
- Change Greenplum Database roles' default resource groups
- Write query assignment rules to override a user's default resource group when a transaction executes
- Write idle session timeout rules for each resource group to set the amount of time a session can be idle before it is killed

For more information about Linux cgroups and Greenplum Database resource groups see [Using Resource Groups](#) in the *Greenplum Database Administrator Guide*.

Query assignment rules is a Greenplum Command Center resource group enhancement that you can use to more flexibly assign transactions to resource groups. With idle session timeout rules you can set the amount of time a session managed by a resource group is idle before it is terminated. The following sections provide more information about these Command Center features.

## About Query Assignment Rules

Greenplum Database defers to the workload management database extension to assign transactions to resource groups. Command Center users with Admin permission level can create assignment rules in Command Center to assign transactions to resource groups.

When a transaction begins, Greenplum Database calls the workload management extension to determine the resource group. The extension evaluates the assignment rules and, if a matching rule is found, returns that rule's resource group. If no assignment rule matches, Greenplum Database falls back to the default behavior, assigning the transaction to the resource group specified for the current user in the `pg_authid` system table.

Assignment rules can redirect a transaction to a resource group based on query tags or a combination of query tags and the Greenplum Database role executing the transaction.


A query tag is a user-defined *name=value* pair that you can set in a Greenplum Database session when the workload management database extension is enabled. Query tags are defined by setting the `gpcc.query_tags` parameter on the connect string when requesting a database connection or in the session with `SET gpcc.query_tags TO '<query-tags>'`. Multiple query tags can be set by separating them with a semicolon. Query tags are set before a transaction begins and cannot be changed inside of a transaction.

See [Workload Management](#) for details about creating assignment rules and for examples that use query tags.

## About Timeout Rules

Command Center administrators can create session timeout rules for resource groups that specify the maximum time that a session can remain idle before it is terminated. When the session process on the Greenplum Database master becomes idle and the specified time has elapsed, the session terminates itself. Sessions that become idle while inside of a transaction are not subject to timeout rules.

Session timeout rules are per resource group, allowing you to determine how long to wait for different classes of transactions. You can include a list of Greenplum Database roles to exempt from the rule and a custom message to add to the session termination error output.

 Creating timeout rules for the `admin_group` resource group is not recommended. Avoid creating rules that kill sessions started by Greenplum Database client applications that are designed to have a long-lasting or persistent session. For example, the `gpmmmon` process creates a session as the `gpmon` role to update the `gpperfmon` database. An idle session timeout rule that kills idle `gpmon` sessions too quickly could cause Greenplum Database to log many session termination messages and unnecessarily create new sessions. See [Workload Management](#) for details about creating timeout rules.



## Workload Management

### Defining Resource Groups and Resource Attributes

Command Center allows you to view resource groups that have been created in Greenplum Database, to add or delete resource groups, and to edit the resource group attributes **Concurrency**, **CPU %**, and **Memory %**.

To change values of the `MEMORY_AUDITOR`, `CPuset`, `MEMORY_SHARED_QUOTA`, or `MEMORY_SPILL_RATIO` resource group attributes, use the `ALTER RESOURCE GROUP` SQL command.

Resource Groups					EDIT
Name	Concurrency	CPU %	Memory %	Min Mem per query	
default_group	10	10	10	57.44MB	
admin_group	5	10	10	114.88MB	
etl	10	10	10	91.90MB	
priority_low	12	20	12	91.90MB	
priority_high	25	30	40	147.05MB	

1. Click **EDIT** to open the Resource Group editor.
2. To delete a resource group, select the resource group, and click the minus sign that appears at the right.  
You cannot delete the `default_group` or `admin_group` resource groups. You cannot delete a resource group that is assigned to any Greenplum Database role.
3. To add a resource group, click **ADD RESOURCE GROUP** and enter a name for the resource group in the **Name** column. Resource group names must be unique and are case-sensitive.
4. Adjust the values of the **Concurrency**, **CPU %**, and **Memory %** resource group attributes.

#### Concurrency

The maximum number of concurrent transactions, including active and idle transactions, that are permitted in the resource group.

**Concurrency** sets the `CONCURRENCY` attribute of the resource group. The total of the **Concurrency** columns cannot exceed the value of the Greenplum Database `max_connections` master server configuration parameter.

#### CPU %

The percentage of CPU resources available to this resource group. The percentage is the portion of the total CPU percentage allocated for all resource groups (reserved CPUs excluded), which is set with the `gp_resource_group_cpu_limit` server configuration parameter. **CPU %** sets the `CPU_RATE_LIMIT` attribute of the resource group.

#### Memory %

The percentage of memory resources available to this resource group. The percentage is the portion of the total memory allocated for all resource groups, which is set with the `gp_resource_group_memory_limit` Greenplum Database configuration parameter. Changing the **Memory %** value sets the `MEMORY_LIMIT` attribute of the resource group.

#### Min memory per query

The minimum amount of memory allocated to a query. This column is recalculated as you adjust **Concurrency** and **Memory %** settings. The value is the resource group's total share of system memory, less the resource group's shared memory pool (20% by default), divided by the value in the **Concurrency** column. The percentage of memory allocated to the shared memory pool can be changed by setting the `MEMORY_SHARED_QUOTA` attribute of the resource group using the `ALTER RESOURCE GROUP` SQL command. Each query managed by the resource queue is allocated this amount of memory. If a query needs more memory, it is allocated from the resource group shared memory pool and the global shared memory pool, if available.

The totals of the **CPU %** and **Memory %** columns must not exceed 100%. You should not allow the total of the **CPU %** column to exceed 90%, because this could cause resource-intensive queries to consume nearly all CPU, starving other Greenplum Database processes. If the total of the **Memory %** column is less than 100%, the unreserved memory is part of the resource group shared global memory pool. See "Global Shared Memory" in [Using Resource Groups](#) in the *Greenplum Database Administrator Guide* for information about the global resource group shared memory pool.

5. Click **Apply** to save your changes or click **Cancel** to abandon your changes.

## Assigning Roles to Resource Groups

Every Greenplum Database role is assigned to a single resource group in the `pg_roles` system table. Transactions executed by a role are managed by its assigned resource group, unless you create an assignment rule to override the default.

You can view the current resource group assignments for all roles and change a role's resource group by adding it to a different resource group.

**Assignment by Role**  
 Queries are routed to Resource Group based on gpdb role, unless diverted by Query Tag filter(below)

default_group(3)	admin_group(2)	etl(1)	priority_low(2)	priority_high(1)
<div>ralph</div> <div>sallyr</div> <div>cashk</div>	<div>gpadmin</div> <div>gpmon</div>	<div>nickd</div>	<div>tpch_4</div> <div>tpch_1</div>	<div>kristiem</div>
<input type="text" value="add role"/>	<input type="text" value="add role"/>	<input type="text" value="add role"/>	<input type="text" value="add role"/>	<input type="text" value="add role"/>



To move a role to a different resource group:

1. Enter all or part of the role name in the **add role** field beneath the new resource group.
2. Choose the role from the list that is displayed and press Enter.

The change is immediately applied to the Greenplum Database `pg_roles` system table.

## Defining Workload Management Rules

Workload management rules include *query assignment* rules and *timeout* rules.

Query assignment rules allow you assign transactions to a resource group based on user-defined query tags and, optionally, the current role in the database session. When no rule matches, the transaction is assigned to the role's default resource group. See [About Assignment Rules](#) for more information about assignment rules.

Timeout rules set the amount of time a session can be idle before it is terminated. You create a timeout rule for each resource group. See [About Timeout Rules](#) for more information about timeout rules.

See [Accessing the Workload Configuration Programmatically](#) for information about retrieving and setting rules programmatically with database functions.

**Workload Management Rules**
CANCEL
APPLY

Queries matching a filter's query tag connection attributes will be diverted, overriding its role's assigned Resource Group. Drag to change filter order.

**If matching query tags**
**Assign to Resource Group**

fdsa=2

AND

cc\_selfonly

default\_group

⊕ ADD ASSIGNMENT RULE

Automatically terminate connections when idle for prescribed period of time

Resource Group	Time before idle connections killed	Exempted roles	Message
test_queue1	75 minutes	cc_admin2	Session terminated by timeout role.

⊕ ADD TIMEOUT RULE



1. Click **EDIT** to open the Workload Management Rules editor.
2. To delete a rule, select the rule and click the minus sign that appears at the right.
3. To add an assignment rule, click **ADD ASSIGNMENT RULE** and fill in the fields.

## Query Tags

The first field is a list of query tags to match against the `gpcc.query_tags` parameter in the Greenplum Database session. A query tag is a user-defined `<name>=<value>` pair. Separate multiple query tags with semicolons. See [Defining and Setting Query Tags](#) for more information about query tags.

## Role

(Optional) If you enter a role name in this field, the rule matches only if both the query tags and role match the tags and current role in the database session.

## Resource Group

Choose a resource group from the list.

- Change the order of the assignment rules by dragging a rule's handle (at the left) up or down. Assignment rules are evaluated from top to bottom. Greenplum Database applies the first rule that matches.
- Use the **Active/Inactive** toggle to make a rule active or inactive.

4. To add a timeout rule, click **ADD TIMEOUT RULE** and fill in the fields.

## Resource Group

Choose a resource group from the list.

## Time before idle connections killed

The amount of time before an idle session is terminated. Enter an integer value for the number of seconds or minutes and choose **minutes** or **seconds** from the list. A value of 600 seconds, for example, terminates the session after it has been idle for 10 minutes. See [About Timeout Rules](#) for warnings about setting timeouts for the `admin_group` resource group and resource groups with roles that require persistent sessions.

## Exempted roles

The rule is not applied to roles added to this field. Open the list to choose roles to exempt from the rule. Only roles for the selected resource group are included in the list. To remove a role from the field, click the **x** next to the role name.

## Message

Enter the message to log when a session is killed by this rule.

5. Click **APPLY** to save your changes.

## Defining and Setting Query Tags

A query tag is a user-defined `<name>=<value>` pair, set in the Greenplum Database `gpcc.query_tags` parameter in the Greenplum Database session. The `gpcc.query_tags` parameter is defined when the `gp_wlm` database extension is enabled in the postgres database. If you try to set query tags when the `gp_wlm` extension is not enabled, you get an unrecognized configuration parameter error. To see if the extension is enabled, run the following command.

```
$ psql postgres -c "\dx"
          List of installed extensions
  Name | Version | Schema | Description
-----+-----+-----+-----
 gp_wlm | 0.1     | gpcc   | Greenplum Workload Manager Extension
(1 row)
```

When you submit a transaction and the `gp_wlm` extension is enabled, Greenplum Database calls the `gp_wlm` extension to determine the resource group for the transaction. The extension evaluates the current role and query tags set in the session against the rules you have defined in Command Center. If there is a match, the extension returns the rule's resource group. If there is no match, Greenplum Database assigns the transaction to the role's default resource group.

The following command, executed in the Greenplum Database session, sets the `appName` and `appUser` query tags to "tableau" and "bi\_sales", respectively.

```
=# SET gpcc.query_tags TO 'appName=tableau;appUser=bi_sales';
```

To match a rule, all tags in the rule's query tag field must be present in the `gpcc.query_tags` parameter in the database session. The order of the tags is not significant, and the `gpcc.query_tags` parameter can have a superset of the tags defined in the `queryTags` value.

If you set the `gpcc.query_tags` parameter inside of a transaction, you must commit the transaction before the new query tags are used to evaluate assignment rules.

You can set the value of the `gpcc.query_tags` parameter using the `SET` command, as in the example above, or as a connection parameter with database clients that support it, such as `psql`. Following are two examples that show how to specify query tags on the `psql` command line.

```
$ PGOPTIONS="-c gpcc.query_tags='appName=tableau;appUser=bi_sales'" psql
```

```
$ psql postgresql://mdw:5432/postgres?options="-c gpcc.query_tags%3D'appName%3Dtableau;appUser%3Dbi_sales'"
```

In the second example, it is necessary to code the equals signs as `%3D` to prevent `psql` from interpreting the query tags as command-line arguments.

## Importing Resource Queues to Resource Groups

Greenplum Command Center workload management works with resource groups, the new Greenplum Database resource management system. The default resource management system for Greenplum Database is resource queues. To use the Command Center workload management features, you must first enable resource groups in Greenplum Database.

Command Center can assist you in enabling resource groups and in importing existing resource queues to resource groups.

### Step One: Enable Resource Groups in Greenplum Database

If your Greenplum Database system is still configured to use resource queues, the Command Center **Admin> Workload Mgmt** view describes the benefits of resource groups and workload management with Command Center and provides a link to the Greenplum Database documentation to help you enable resource groups.

**Workload Management** Manage your workload through Resource Groups

**With Resource Groups and Command Center, you can**

**Handle mixed workloads**  
Assign queries to Resource Groups based on role or custom query tags

**Use system resources more efficiently**  
Control memory, CPU, and concurrency allocation for each Resource Group

**Support SLAs**  
Protect resources for privileged groups to ensure queries complete on time

**Improve memory management**  
Prevent over subscription and isolate memory between Resource Groups and transactions

[VIEW RESOURCE GROUP SET UP GUIDE](#)

Name	Concurrency	CPU %	Memory %	Estimated Mem per query
admin_group	2	10	10	241MB
default_group	20	10	10	241MB
BI_Analytics	20	12	12	723MB
ETL_Load	20	25	25	723MB
Adhoc	20	12	12	482MB
Global	20	5	5	120MB
Special_VIP	20	5	5	120MB

Click **VIEW RESOURCE GROUP SET UP GUIDE** for instructions to enable resource groups in your Greenplum Database system.

### Step Two: Preview and Configure Resource Group Imports

After you have enabled resource groups and restarted Greenplum Database, restart Command Center (`gpcc start`), log in, and choose **Admin> Workload Mgmt**.

The workload management view now displays a preview of resource groups converted from your existing resource queues. You can use this one-time view to convert your Greenplum Database resource queues to resource groups.

## Workload Management Manage your workload through Resource Groups

Here is a preview of your resource groups converted from your resource queues. Please input the resource allocations. Your roles will be matched with the assigned resource groups.

Resource Group	Concurrency	CPU %	Memory %	Min mem per query
default_group	<input type="text" value="20"/>	<input type="text" value="30"/>	<input type="text" value="30"/>	86.16MB
admin_group	<input type="text" value="20"/>	<input type="text" value="30"/>	<input type="text" value="30"/>	86.16MB
vip	<input type="text"/>	<input type="text"/>	<input type="text"/>	--
etl	<input type="text"/>	<input type="text"/>	<input type="text"/>	--
adhoc	<input type="text"/>	<input type="text"/>	<input type="text"/>	--
bi_analytics	<input type="text"/>	<input type="text"/>	<input type="text"/>	--
		60	60	Total CPU and Memory must be less than or equal to 100%

IMPORT RESOURCE GROUPS

SKIP IMPORT

Your roles will be imported to the matching resource groups. [Close preview.](#)

default\_group (0)

admin\_group (2)

gpmon  
gpadmin

vip (3)

nickd  
ralphs  
katrinab

etl (2)

kristiem  
richd

adhoc (0)

bi\_analytics (4)

jillianr  
brentd  
sallyg  
anny



The resource group list includes the required `admin_group` and `default_group` resource groups, and a row for each of your existing resource queues.

Roles are assigned to the resource group matching the resource queue to which they are assigned. Click the **Preview roles** link to see the role assignments.

Your roles will be imported to the matching resource groups. [Close preview.](#)

default\_group (0)

admin\_group (2)

gpmon  
gpadmin

vip (3)

nickd  
ralphs  
katrinab

etl (2)

kristiem  
richd

adhoc (0)

bi\_analytics (4)

jillianr  
brentd  
sallyg  
anny



If you want to set up resource groups later, you can click **SKIP IMPORT**. Only the `default_group` and `admin_group` resource groups are created. Roles with the superuser attribute are assigned to the `admin_group` resource group; roles without superuser privilege are assigned to the `default_group` resource group.

If you want Command Center to import resource queues to resource groups, you must complete the resource allocation fields for all resource groups.

Set the **Concurrency**, **CPU %**, and **Memory %** resource group attributes to allocate Greenplum Database resources to the resource queues. The **Concurrency** fields must each contain a positive integer. The **CPU %** and **Memory %** fields must each contain positive integers between 1 and 99 and the totals for the **CPU %** and **Memory %** columns must not exceed 100%. See [Defining Resource Groups and Resource Attributes](#) for help determining the values to enter.

The **IMPORT RESOURCE GROUPS** button is disabled until you have entered valid values in the allocation fields for every resource group.

When you are ready to import the resource groups, click **IMPORT RESOURCE GROUPS** to create the resource groups.

## Step Three: Enable Command Center Workload Management

After you import (or skip importing) resource queues to resource groups, you can enable Command Center workload management.

Resource Groups

EDIT

Name	Concurrency	CPU %	Memory %	Min mem per query
default_group	5	2	5	86.16MB
admin_group	5	2	5	57.44MB
vip	10	10	15	137.86MB
etl	5	5	5	91.90MB
adhoc	5	2	3	55.14MB
bi_analytics	50	30	30	55.14MB

Assignment by Role

Queries are routed to Resource Group based on gpdb role, unless diverted by Query Tag filter (below)

default\_group (0)

admin\_group (2)

vip (3)

etl (2)

adhoc (0)

bi\_analytics (4)

Workload Management Rules

EDIT

Queries matching a filter's query tag connection attributes will be diverted, overriding its role's assigned Resource Group. Drag to change filter order.

If matching query tags

Assign to Resource Group

no assignment rules

ENABLE WORKLOAD MANAGEMENT

Automatically terminate connections when idle for prescribed period of time

Enable Workload Management will allow you set query tags and idle session rules.

Resource Group

Time before idle connections killed

Exempted roles

Message

no timeout rules

Click **ENABLE WORKLOAD MANAGEMENT** to enable workload management in Greenplum Command Center. Greenplum Command Center creates the `gp_wlm` extension, the `gpcc.workload_config` table, and the associated user-defined functions in Greenplum Database.

You are now able to use the Command Center Workload Management interface to add, remove, and configure resource groups; change role assignments; and define workload management rules.

See [Workload Management](#) for help using the Command Center Workload Management view.

© Copyright Pivotal Software Inc, 2013-2018

95

4.5.0

## Accessing the Workload Configuration Programmatically

The Greenplum Database workload management extension `gp_wlm` creates a table in the postgres database to store the workload management rules, and user-defined functions to get or set the workload management rules.

The `gpcc.workload_config` table stores the workload management rules as a JSON value. You can use the `gpcc.get_workload_config()` and `gpcc.set_workload_config()` functions to read and write this JSON value.

This topic is a reference for the workload management configuration JSON document and the get and set functions.



**Warning!** The `gpcc.workload_config` table should only be accessed by using the `gpcc.get_workload_config()` and `gpcc.set_workload_config()` functions or the Command Center user interface. Do not drop the table while the workload management extension is enabled.

The `gpcc.set_workload_config()` function requires valid JSON syntax, but does not validate the workload management rules. You must ensure that the JSON value contains a `version` variable, and correctly specified assignment and idle session timeout rules.

## Workload Management Rules JSON Format

This section describes the JSON object that stores the resource group assignment and idle session timeout rules. The object has three members:

- a `version` key/value pair
- an `assignmentRules` array containing one element for each assignment rule
- an `idleSessionKillRules` list containing one key/value pair for each resource group

### version pair

version

The `version` value is an integer. It is reserved for future use. It can be set to `1`.

### assignmentRules array

assignmentRules

The `assignmentRules` array has one element for each assignment rule. Each element maps the rule to a resource group in Greenplum Database and defines the conditions that assign a transaction to that resource group.

Greenplum Command Center evaluates each rule in the `assignmentRules` array from top to bottom and stops at the first match, so the order is important.

The elements in the `assignmentRules` array can have the following key/value pairs.

resourceGroupName

The name of the Greenplum Database resource group. The resource group must already exist or have been created in Greenplum Database with the `CREATE RESOURCE GROUP` SQL statement.

roleName

The name of a Greenplum Database role to match against the current role identifier in the Greenplum Database session. The current role is initially the database role that authenticated with the Greenplum Database system to begin the session. A user with sufficient privileges can change the current role in the database session using the `SET ROLE` SQL command.

If no role is specified in the assignment rule and the query tags match, the transaction is assigned to the specified resource group. If the `roleName` value is present, however, the current database user must match the specified role.

queryTags

A list of query tags to match against the `gpcc.query_tags` parameter in the Greenplum Database session. A query tag is a user-defined `<name>=<value>` pair. Separate multiple query tags with semicolons. For example, the following statement, executed in the Greenplum Database session, sets the `appName` and `appUser` query tags to “tableau” and “bi\_sales”, respectively.



```
==# SET gpcc.query_tags TO 'appName=tableau;appUser=bi_sales';
```

To match, all tags in the assignment rule's `queryTags` value must be present in the `gpcc.query_tags` parameter in the database session. The order of the tags is not significant, and the `gpcc.query_tags` parameter can be a superset of the tags defined in the `queryTags` value.

If the `queryTags` value is empty, or the parameter omitted, the rule will match every session for the `roleName` database role.

If you set the `gpcc.query_tags` parameter inside of a transaction, you must commit the transaction before the new query tags are used to evaluate assignment rules.

The `gpcc.query_tags` parameter can be specified using the `SET` command, as above, or as a connection parameter with database clients that support it, such as `psql`. Here are two examples that show how to specify query tags on the `psql` command line:

```
$ PGOPTIONS="-c gpcc.query_tags='appName=tableau;appUser=bi_sales'" psql
$ psql postgresql://mdw:5432/postgres?options="-c gpcc.query_tags=%3D'appName%3Dtableau;appUser%3Dbi_sales'"
```

In the second example, it is necessary to code the equals signs as `%3D` to prevent `psql` from interpreting the query tags as command-line arguments.

disabled

If set to `true`, the assignment rule is ignored when Command Center evaluates rules to assign transactions to workloads. This parameter is optional and its default value is `"false"`.

## gpcc.get\_workload\_config()

Retrieves the current workload assignment rules as a JSON value.


### Example

```
postgres=# SELECT gpcc.get_workload_config();
           get_workload_config
-----
{
  "version": 1,
  "assignmentRules": [
    {
      "resourceGroupName": "default_group",
      "roleName": "gpadmin",
      "queryTags": "appName=tableau;appUser=bi_sales"
    },
    {
      "resourceGroupName": "admin_group",
      "roleName": "gpadmin",
      "queryTags": "appName=tableau;appUser=bi_acct",
      "disabled": true
    }
  ],
  "idleSessionKillRules": {
    "admin_group": {
      "timeoutSeconds": 600
    },
    "default_group": {
      "timeoutSeconds": 3600
    }
  }
}

(1 row)
```

## gpcc.set\_workload\_config()

Sets the workload assignment rules. The argument is a valid JSON value containing the assignment rules. See [JSON Parameters](#) for descriptions of the parameters.

 The `gpcc.set_workload_config()` function accepts any valid JSON value. You must ensure that the value contains a `version` element and properly specified assignment and idle session timeout rules.

If you call `gpcc.set_workload_config()` within a transaction, you must commit the transaction before the workload management extension applies the new rules.

## Example

```
postgres=# SELECT gpcc.set_workload_config(
,
  { "version": 1,
    "assignmentRules":
    [
      {
        "resourceGroupName": "default_group",
        "roleName": "gpadmin",
        "queryTags": "appName=tableau;appUser=bi_sales"
      },
      {
        "resourceGroupName": "admin_group",
        "roleName": "gpadmin",
        "queryTags": "appName=tableau;appUser=bi_acct",
        "disabled": true
      }
    ],
    "idleSessionKillRules":
    {
      "admin_group":
      { "timeoutSeconds": 600 },
      "default_group":
      { "timeoutSeconds": 3600 }
    }
  },
);
set_workload_config
-----
t
(1 row)
```

## Troubleshooting Enabling Resource Groups

If you experience problems enabling resource groups in Greenplum Command Center, review the following list to ensure prerequisites are met and all of the dependencies are properly configured.

- Red Hat 6.x and 7.x and CentOS 6.x and 7.x are currently supported.
- You must be running Greenplum Database version 5.7.0 or later.
- Configure the Linux cgroups kernel feature on your hosts by following the instructions at “Prerequisite” in [Using Resource Groups](#).
- Make sure the `/etc/cgconfig.d/gpdb.conf` file contains the objects `perm`, `cpu`, and `cpuacct`. If the document is incorrect and the `gp_resource_manager` configuration parameter is set to `"group"`, Greenplum Database can hang at startup.

```
group gpdb {
  perm {
    task {
      uid = gpadmin;
      gid = gpadmin;
    }
  }
  admin {
    uid = gpadmin;
    gid = gpadmin;
  }
}
cpu {
}
cpuacct {
}
```

- On Red Hat 7, make sure you run `cgconfigparser -L /etc/cgconfig.d` to parse changes to the `/etc/cgconfig.d/gpdb.conf` file. This command must also be set up to run at boot time.
- Set the Greenplum Database `gp_resource_manager` server configuration parameter to `"group"`.

```
$ gpconfig -c gp_resource_manager -v "group"
```

Verify by showing the value of the parameter:

```
$ gpconfig -s gp_resource_manager
Values on all segments are consistent
GUC      : gp_resource_manager
Master value: group
Segment value: group
```

- After installing a Pivotal Greenplum Database distribution, the `shared_preload_libraries` configuration parameter contains the metrics collector and workload manager extension shared libraries. Make sure these libraries are still present:

```
$ gpconfig -s shared_preload_libraries
Values on all segments are consistent
GUC      : shared_preload_libraries
Master value: $libdir/metrics_collector,$libdir/gp_wlm
Segment value: $libdir/metrics_collector,$libdir/gp_wlm
```

Check that the shared libraries exist at `$GPHOME/lib/postgresql/metrics_collector.so` and `$GPHOME/lib/postgresql/gp_wlm.so`. If the libraries do not exist, make sure you have installed the Pivotal Greenplum Database distribution. These extensions are not available in the Greenplum Database Open Source version.

If the shared library files exist in the `$GPHOME/lib/postgresql` directory, but not in the `shared_preload_libraries` parameter, add them with the `gpconfig` command:

```
$ gpconfig -c shared_preload_libraries -v '$libdir/metrics_collector,$libdir/gp_wlm'
```

Note that adding the libraries to the `shared_preload_libraries` parameter does not enable the `metrics_collector` or `gp_wlm` extensions, but is a prerequisite for enabling them.

- The `gpmon` user must be able to connect to databases from the Command Center host. Make sure to add a `host` entry like the following in the `$MASTER_DATA_DIRECTORY/pg_hba.conf` file.

```
host all gpmon <IP_of_host>/32 md5
```

- Check whether the `gp_wlm` extension is installed. The extension is added when you click **Enable Workloads** in the Greenplum Command Center

Admin> Workload Mgmt view.

```
$ psql postgres
\dx
postgres=# \dx
          List of installed extensions
  Name | Version | Schema | Description
-----+-----+-----+-----
 gp_wlm | 0.1    | gpcc   | Greenplum Workload Manager Extension
```

- Make sure the `gpcc.workload_config` table and functions are present in the postgres database:

```
$ psql postgres
postgres=# \d gpcc.*
Table "gpcc.workload_config"
  Column | Type | Modifiers
-----+-----+-----
 dist_col | integer |
 config | json |
Distributed by: (dist_col)
postgres=# \df gpcc.*
          List of functions
 Schema | Name | Result data type | Argument data types | Type
-----+-----+-----+-----+-----
 gpcc | get_workload_config | json | | normal
 gpcc | set_workload_config | boolean | wlm_json_config json | normal
(2 rows)
```

If the `gpcc.workload_config` table or the functions are not present, dropping and recreating the `gp_wlm` extension will create them. Note that any assignment rules saved in the `gpcc.workload_config` table will have to be recreated in Command Center.

```
$ psql postgres
postgres=# DROP EXTENSION gp_wlm;
DROP EXTENSION
postgres=# CREATE EXTENSION gp_wlm;
CREATE EXTENSION
```

## Query Monitor Help Topics

- [CPU](#)
- [CPU Skew](#)
- [Locks](#)
- [Query Optimization](#)
- [Memory](#)
- [Spill Files](#)

## CPU

The **CPU percent** metric is the average current CPU percentage for all backend processes executing this query. The percentages for all processes running a query on each segment are averaged, and then the average of all those values is calculated to render this metric.

You can manage the percentage of CPU that queries can consume by creating workloads and specifying the maximum percent of CPU each workload can consume. That percentage is further divided among the segments running on each host and then among the concurrent queries the workload can execute.

CPU allocated to idle workloads is reallocated to active queries and reclaimed when the idle workload becomes active again. This means that the **CPU percent** value for a query can exceed limits defined for workloads and can increase and decrease as other queries start or finish.

Memory and disk I/O resources are more likely causes for degraded query performance than lack of CPU cycles. The ways to reduce CPU contention mirror the solutions for insufficient memory:

- Reduce concurrency of workloads to make more CPU available to each query.
- Reduce the number of workloads and reallocate CPU to the remaining workloads.

If CPU is not constrained and the size of spill files for some queries is very large, make sure that the `gp_workfile_compress_algorithm` server configuration parameter is set to `zlib` and not `none`. Compressing spill files reduces disk I/O, but uses CPU cycles to compress and decompress the data.

See [Using Resource Groups](#) for more about managing performance with resource groups.

If your Greenplum Database system is configured to manage resources with resource queues, see [Using Resource Queues](#).

## CPU Skew

### What is CPU Skew?

CPU skew occurs when the work to execute a query is not distributed evenly among the segments.

The **CPU** metric is the average of the CPU percentages used by each process executing the query. The **CPU skew** metric is a variance statistic based on the difference between the average and each segment's current **CPU** metric. The smaller the **CPU skew**, the more equally the work is distributed. The **CPU skew** metric varies between 0.0 (no skew) and 1.0. The lower the skew metric the more fully the database cluster's resources are utilized.

CPU skew is usually related to the volume of data processed by the segments while executing the query execution plan. There are two types of skew you should investigate: data skew and computational skew.

### Data Skew

A high CPU skew may be an indication of data skew, where tables used by the query are distributed unevenly, so that some segments have more data to process than their peers. You can check for data skew in a table by running a query like this one:

```
=# SELECT gp_segment_id, COUNT(*) FROM <table-name> GROUP BY gp_segment_id;
```

The row count should be approximately equal for each segment. If the rows are distributed unevenly, check the distribution key for the table. A good distribution key is a column or list of columns with unique or nearly unique values, such as the table's primary key. Setting the distribution policy to `DISTRIBUTED RANDOMLY` also ensures a well-distributed table, but precludes taking advantage of performance-enhancing strategies such as co-location for tables with equivalent primary keys.

### Computational Skew

High CPU skew can be the result of computational skew, which occurs during query execution. Some of the operations in the query plan can cause some segments to do more work than others. For example, joins, sorts, or aggregations on columns with low cardinality or unevenly distributed values can contribute to CPU skew by causing some segments to process many more tuples than others.

See [Distribution and Skew](#) in the *Greenplum Database Administrator Guide* and [Tuning SQL Queries](#) in the *Greenplum Database Best Practices* guide for more help finding the causes of skew.

## Locks

Greenplum Command Center displays the locks currently held by queries and queries blocked by locks.

A block occurs when one query needs to acquire a lock that conflicts with a lock held by another query. If a query is blocked for a long period of time, you can investigate the blocking query and, if necessary, cancel one of the queries.

Locks can be acquired using the `LOCK TABLE` SQL statement. Some SQL commands acquire locks automatically. Following are descriptions of the lock modes, the Greenplum Database commands that acquire them, and which lock modes conflict with them.

### ACCESS SHARE

Acquired by `SELECT` and `ANALYZE` commands.

Conflicts with ACCESS EXCLUSIVE locks.

In general, any query that only reads a table and does not modify it acquires this lock mode.

### ROW SHARE

Acquired by `SELECT FOR SHARE` command.

Conflicts with EXCLUSIVE and ACCESS EXCLUSIVE locks.

A ROW SHARE lock is placed on the specified table and an ACCESS SHARE lock on any other tables referenced in the query.

### ROW EXCLUSIVE

Acquired by `INSERT` and `COPY` commands.

Conflicts with SHARE, SHARE ROW EXCLUSIVE, EXCLUSIVE, and ACCESS EXCLUSIVE locks.

A ROW EXCLUSIVE lock is placed on the specified table and ACCESS SHARE locks are placed on any other referenced tables.

### SHARE UPDATE EXCLUSIVE

Acquired by `VACUUM` and `VACUUM FULL`.

Conflicts with the SHARE UPDATE EXCLUSIVE, SHARE, SHARE ROW EXCLUSIVE, EXCLUSIVE, and ACCESS EXCLUSIVE locks.

SHARE UPDATE EXCLUSIVE protects a table against concurrent schema changes and `VACUUM` runs.

### SHARE

Acquired by `CREATE INDEX`.

Conflicts with ROW EXCLUSIVE, SHARE UPDATE EXCLUSIVE, SHARE ROW EXCLUSIVE, EXCLUSIVE, and ACCESS EXCLUSIVE locks.

Protects a table against concurrent data changes.

### SHARE ROW EXCLUSIVE

This lock mode is not automatically acquired by any Greenplum Database command.

Conflicts with ROW EXCLUSIVE, SHARE UPDATE EXCLUSIVE, SHARE, SHARE ROW EXCLUSIVE, EXCLUSIVE, and ACCESS EXCLUSIVE locks.

### EXCLUSIVE

Acquired by `UPDATE`, `SELECT FOR UPDATE`, and `DELETE` commands in Greenplum Database.

Conflicts with ROW SHARE, ROW EXCLUSIVE, SHARE UPDATE EXCLUSIVE, SHARE, SHARE ROW EXCLUSIVE, EXCLUSIVE, and ACCESS EXCLUSIVE locks.

This lock mode allows only concurrent ACCESS SHARE locks - a table can be read by another transaction while this lock is held. This is more restrictive locking than in regular PostgreSQL.

### ACCESS EXCLUSIVE

Acquired by the `ALTER TABLE`, `DROP TABLE`, `TRUNCATE`, `REINDEX`, `CLUSTER`, and `VACUUM FULL` commands. Default lock mode for `LOCK TABLE` statements that do not specify a lock mode. Also briefly acquired by `VACUUM` (without `FULL`) on append-optimized tables during processing.

Conflicts with all locks.

This lock mode guarantees that the holder is the only transaction accessing the table in any way.

For more on locks in Greenplum Database queries, see the [LOCK](#) command Reference. See also [Tuning SQL Queries](#).





## Memory

The Greenplum Command Center Query Monitor reports the current total memory consumed by all processes executing a query. When there is insufficient memory available for a query to complete, the query has an error status in the query monitor and an out of memory error is logged.

If you have enabled resource groups in Greenplum Database, you can manage the amount of memory available to queries by tuning resource group parameters, and by setting Greenplum Database configuration parameters that affect resource group memory.

- For a detailed description of resource group memory management, see [Using Resource Groups](#) in the *Greenplum Database Administrator Guide*.
- If you are using resource queues, see [Memory and Resource Management with Resource Queues](#) and [Using Resource Queues](#) for ways to troubleshoot memory problems with resource queues.
- See [Tuning SQL Queries](#) for help with query optimization.

The following summary describes the resource group parameters and related Greenplum Database server configuration parameters that determine the amount of memory available to database queries and how configuration choices affect concurrency, spill file usage, and query performance.

## Resource Group Memory Configuration Parameters

A resource group has parameters `CONCURRENCY`, `MEMORY_LIMIT`, `MEMORY_SHARED_QUOTA`, and `MEMORY_SPILL_RATIO`, which determine how much memory is allocated to execute a query. The `CPU_LIMIT` parameter has no effect on memory allocation. See the [CREATE RESOURCE GROUP](#) SQL reference for command syntax and information about these parameters.

### `MEMORY_LIMIT`

This parameter sets the amount of memory the resource group manages as a percentage of the memory available to resource groups. The sum of all resource groups' `MEMORY_LIMIT`s must not exceed 100. If the sum of all resource groups' `MEMORY_LIMIT`s is less than 100, the remaining, unallocated memory is *global resource group shared memory*, available to queries from all resource groups on a first-come, first-served basis.

### `MEMORY_SHARED_QUOTA`

A resource group divides the memory it manages into a fixed portion and a shared portion, called *resource group shared memory*. This parameter specifies the percentage of a resource group's memory that is shared. The default is 20 and the value can range from 0 to 100.

### `CONCURRENCY`

This parameter limits the number of concurrent transactions a resource group allows. The fixed portion of the memory the resource group manages is divided equally among `CONCURRENCY` transaction slots. Every transaction starts with this fixed portion of memory and, if needed, Greenplum Database uses additional memory from the resource group shared memory and global resource group shared memory.

### `MEMORY_SPILL_RATIO`

This parameter sets a limit for the amount of memory a query can use before it spills to disk. The parameter value is expressed as a percentage of the fixed memory allocation. The default is 20 and the value can range from 0 to 100. A higher value uses more memory, but can improve query performance. A transaction can override this value by setting the `memory_spill_ratio` configuration parameter in the session.

When a query executes, Greenplum Database allocates memory to it from the fixed portion of the resource group's memory. If the query needs more memory and the resource group has available shared memory, Greenplum Database allocates additional memory. If insufficient shared memory is available, Greenplum Database allocates additional memory from global shared memory, if available. If the required memory is not available the transaction fails.

## Greenplum Database Memory Configuration Parameters

The following Greenplum Database configuration parameters affect resource group memory allocation and concurrency.

### `gp_resource_group_memory_limit`

This Greenplum Database server configuration parameter sets the percentage of each host's system memory to be managed by resource groups. The default is `0.7` (70%). This memory is divided equally among the primary segments on each host, and further divided among resource groups with the `MEMORY_LIMIT` resource group parameter. Any memory not allocated to resource groups becomes global shared memory available to queries from all resource groups. See [gp\\_resource\\_group\\_memory\\_limit](#) for a complete reference for this parameter.

### `gp_resgroup_memory_policy`

This parameter determines how Greenplum Database allocates memory to query operators. The default value, `eager_free`, re-allocates memory from completed operators to operators later in the query plan. The alternative value for this parameter, `auto`, allocates a fixed amount of memory to operators that are not memory-intensive and the rest to the memory-intensive operators. The default value is usually the optimal setting. See [gp\\_resgroup\\_memory\\_policy](#) for a complete reference for this parameter.


## `memory_spill_ratio`

A transaction can override the resource group's `MEMORY_SPILL_RATIO` value by setting the `memory_spill_ratio` configuration parameter in the session. The value is a percentage of the fixed memory allocation for transactions in the resource group, expressed as an integer from 0 to 100. The performance of queries with low memory requirements can be improved by setting the `memory_spill_ratio` parameter in the session to a low setting, for example 0 to 2. See [memory\\_spill\\_ratio](#) [↗](#) for more information about this parameter.

## Query Plan Execution

The Greenplum Database legacy and GPORCA query optimizers generate execution plans that produce the results requested by the query. A plan is a sequence of operators, such as table scans, joins, sorts, aggregates, and data motions.

When you select a query on the Command Center **Query Monitor** view, a [Query Details](#) view presents a graphical representation of the execution plan.

You can switch between the graphical and textual representations of the query execution plan by selecting the **Plan & Progress** tab or the **Textual Plan** tab. In the textual format, each plan node is flagged with an arrow (). In the graphical view, the nodes are represented by boxes that fill as the plan executes.

A query execution plan executes from the bottom up. Each node in the plan performs an operation and passes results up to the next node in the plan.

The **Optimizer status:** line on the **Textual Plan** tab reports whether the explain plan was generated using the GPORCA optimizer or the legacy query optimizer.

## Slices and Gangs

Segments can work on portions of a query in parallel, each segment executing operators independently on their local data. When the plan requires exchanging data between segments, a data motion operator coordinates the data transfer between segments. The plan is divided into “slices” where these data motions occur.

A data motion node in a textual query plan identifies the slice and the number of segments participating in the motion.

Example:

```
-> Broadcast Motion 4:4 (slice2; segments: 4) (cost=0.00..867.15 rows=10000 width=30)
```

In a broadcast motion, each segment broadcasts all of its rows for a table over the network so that every segment has a complete copy of the table. In this example, the broadcast motion marks the completion of **slice2** with four segments sending and four segments receiving.

Each segment has one or more backend processes working on a slice. Backend processes working on the same slice are called a “gang”.

## Operators

Operators are processes that take as input database tables or the output from other operators, and perform some action to produce a transformed output.

### Scan Operators

#### Init plan

A query that runs before the main query is optimized to find the partitions to scan.

#### Sequential scan

The optimizer may choose a sequential table scan if there is no index on the condition column or if most rows are expected to satisfy the condition. Because each segment scans an equal portion of the data in parallel with other segments, a table scan in Greenplum Database is very efficient. A query on a partitioned table may be able to eliminate partitions to make the scan even faster.

#### Append-only scan

Scans rows in a row-oriented, append-optimized table.

#### Append-only columnar scan

Scans rows in a column-oriented, append-optimized table.

#### Dynamic table scan

Scans selected partitions in a partitioned table.

#### Function scan

A Function Scan node selects the partitions to scan. The function can be one of the following:

- `gp_partition_expansion` - chooses all nodes
- `gp_partition_selection` - chooses a partition with an equality expression
- `gp_partition_inversion` - chooses partitions with a range expression

## Index scan

Scans a B-tree index on a table to find rows. The rows are then retrieved from disk.

## Bitmap index scan

A Bitmap Index Scan is an index scan optimized by storing rows in a bitmap instead of retrieving them from the table immediately. When the scan is complete, rows in the bitmap are retrieved with a Bitmap Heap Scan operation.

## BitmapAnd and BitmapOr

Generates a new bitmap by running logical AND or OR on multiple bitmaps.

## Bitmap heap scan

Retrieves rows from heap storage using a bitmap generated by a Bitmap index scan or BitmapAnd or BitmapOr operation.

## Nested loop with inner sequential scan join

For each row in the first table, the operator tests every row in the second table with a sequential scan.

One table must be broadcast so that every segment can compare all rows of one table with the rows it has from the other table. This is expensive and is best used only for small tables.

## Nested loop with inner index scan

For each row in the first table, the operator searches an index on the second table.

One table must be broadcast so that every segment can compare all rows of one table with the rows it has from the other table.

## Append

Concatenates data sets. For example, combines rows scanned from multiple partitions.

## Filter

Selects rows using a `WHERE` clause.

## Limit

Limits the number of rows returned.

## Materialize

Saves results from a subselect so that it is not necessary to process the inner table for every row in the outer table.

## Join Operators

### Hash join

Creates a hash table on the join key of the smaller table. Scans the larger table and looks up matching rows in the hash table. Hash join is very fast. The hash table is held in memory, so a hash join can use a lot of memory, depending on the size of the smaller table.

### Sort merge join

The tables to be joined are sorted on the join attribute and then scanned in parallel to find the matching values. This is a good join method for tables that are too large to use a hash join.

### Product join

Joins every qualifying row in the first table with every qualifying row in the second table. This type of join can be very expensive if spill files must be used.

## Sort and Aggregate Operators

### Sort

Sorts rows to prepare for operations such as an aggregation or merge join.

### Group by

Groups rows by one or more columns.

### Group / hash aggregate

Aggregates rows using a hash.

## Motion Operators

### Broadcast motion

Every segment sends its own local data to all other segment instances so that every segment instance has a complete local copy of the table.

### Redistribution motion

Sends data from one table to another segment so that matching rows are located together, enabling a local join.

### Gather motion

All segments send rows to the master where they are gathered into a single result set.

## DML Operators

### Assert

Performs constraints checking.

### Split

Used for update operations.

## Spill Files

Greenplum Command Center reports the total size for all spill files created for a query.

Greenplum Database creates spill files, also called workfiles, to save intermediate results when there is insufficient memory to execute a query in memory. Disk I/O is much slower than memory access, so a query that creates spill files will take longer to complete.

## Investigating Spill File Usage

The `gp_toolkit` schema contains views you can use to see details about spill file usage for current queries. You can see the number and sizes of spill files created for each operator in a query execution plan, and totals by query and segment. This is useful information to detect data skew and to help tune queries.

See the [gp\\_toolkit Administrative Schema](#) reference for descriptions of these views.

## Eliminating or Reducing Spill Files

You can work to eliminate spill files by increasing the amount of memory available to the query or by optimizing the query to use the memory available more efficiently.

You may be able to revise the query to prevent spilling by eliminating or postponing memory-intensive operators.

Following are some ways to increase memory available to queries when resource group resource management is enabled in Greenplum Database.

- Decrease the resource group's concurrency so that each query's share of memory increases.
- Increase the resource group's `MEMORY_SHARED_QUOTA` parameter to increase the amount of resource group shared memory.
- Decrease the percentage of memory allocated to all resource groups to increase the amount of global shared memory.

When resource queue resource management is active, Greenplum Database can detect and terminate “runaway” queries that consume a high percentage of available memory. You can prevent runaway queries by limiting the number of spill files created or the total size of spill files created. See the `gp_workfile_limit*` configuration parameters below for more information.

If you cannot prevent queries from spilling, it is important to ensure that the number of spill files created is minimized and that problems such as CPU or data skew are found and corrected. Skew can create excessive numbers of spill files on one or more segments.

To minimize disk usage and I/O when spill files are created, make sure the `gp_workfile_compress_algorithm` configuration parameter is set to 'zlib' and not 'none'.

## Limiting Spill Files with Server Configuration Parameters

Greenplum Database by default limits the number of spill files allowed per query for each segment to 100,000. You can raise or lower this limit, and you can also limit the number of spill files for all queries on a segment, and limit the disk space consumed by spill files per query and per segment. Use the following Greenplum Database server configuration parameters to manage spill files.

`gp_workfile_limit_files_per_query`

Sets the maximum number of spill files allowed per query per segment. Default is 100,000.

`gp_workfile_limit_per_query`

Sets the maximum disk size an individual query is allowed to use for spill files at each segment. The default value is 0, which means no limit is enforced.

`gp_workfile_limit_per_segment`

Sets the maximum total disk size that all running queries are allowed to use for creating spill files at each segment. The default value is 0, which means a limit is not enforced.

`gp_workfile_compress_algorithm`

Specifies the compression algorithm to use for spill files when a hash aggregation or hash join operation spills to disk during query processing. The default is 'none'. Set to 'zlib' to enable compression. Using compression reduces the number of I/O operations at the expense of increased CPU.

See also [Managing Spill Files Generated by Queries](#).