

## RBAC Permissions

Date published: 2020-10-30

Date modified: 2024-05-30

# CLOUDERA

# Legal Notice

© Cloudera Inc. 2024. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

# Contents

<b>Permission levels for role-based access.....</b>	<b>4</b>
---	----------

## Permission levels for role-based access

Cloudera Data Visualization uses Role-Based Access Control (RBAC) permissions to regulate access to the different components and functionalities of the system. Administrators define these permissions while configuring roles, which are then assigned to the appropriate users or user groups.

### System-level permissions

#### Create workspaces

Allows users to create new workspaces that may be shared among users and user groups.

#### View roles and users

Enables users to view users, user groups, and roles.

#### Manage roles and users

Enables users to create users, user groups, and roles.

By default, includes the management of Filter Associations on the dataset management interface. Alternatively, you can configure Filter Associations as part of dataset management during individual dataset permission configuration. For more information on how to manage the filter association configuration for the dataset, see the *Manage dataset* permission below.

#### Manage settings

Permits users to manage global site settings.

#### Manage custom styles

Authorizes users to create new styles for dashboards and visuals.

#### Manage jobs, email templates

Enables users to manage scheduled jobs and create templates for email messages.

#### View activity logs

Allows users to view usage statistics and monitor the performance of Cloudera Data Visualization.

#### Manage data connections

Grants users the ability to create and manage connections to various data sources.

#### Additional system privilege

Enables users to perform the following actions:

- Set the homepage for all users. For more information, see *Setting a default homepage for all users*.
- Clone, delete, or edit dashboards in another user's private workspace.
- Perform administrative restart/stop work operations.
- Use Trusted Auth Get Ticket to request a ticket from the Cloudera Data Visualization Server. For more information, see *Embedding apps with trusted authentication*.

### Role-level permissions

#### Grant manage dataset

Enables users to grant Manage dataset privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

#### Grant manage dashboards

Enables users to grant Manage dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

**Grant view dashboards**

Enables users to grant View dashboard privileges to specific roles, provided the user has the Manage dataset permission for that dataset.

**Connection-level permissions****Manage AVs/Extracts**

Enables users to create and manage analytical views.

**Import data**

Allows users to import supplemental data into an existing connection.

**Create datasets, explore tables**

Allows users to create new datasets from existing tables, view sample data, and explore statistical reports on the data tables.

**Dataset-level permissions****Manage dataset**

Allows users to change the properties of datasets, create datasets over joined tables, modify the fields of the dataset, and more

To enable Filter Association (FA) configuration based on Manage dataset permission, modify the settings.py file by adding the following line:

```
MANAGE_DS_FA = True
```

**Manage dashboards**

Enables users to create and modify visuals and dashboards.

**View dashboards**

Used to limit users to view-only privileges for visuals and dashboards, while denying edit privileges.