..

Security

Date published: 2020-10-30
Date modified: 2022-09-21

https://docs.cloudera.com/

Legal Notice

Contents

Security model

Security in CDP Data Visualization means authentication and permission granularity. It involves many components, including role-based access control, which enables fine-grain control over data and feature access.

As an administrator, you can configure roles, privileges, and members. For more information, see *Working with user roles*. You can manage privileges and members of a role witth the help of *Role-based access control*. User roles are further leveraged to enable dataset creators and managers to share curated datasets with their organization, while exercising three levels of access control. For more information, see *Publishing datasets*. You can also restrict a user's access to defined data segments. For more information, see *Setting segments*. Additionally, you can also configure LDAP authentication. For more information, see *Enabling LDAP authentication*.

Related Information

Role-based access control
Working with user roles
Publishing datasets
Setting segments
Enabling LDAP authentication

Role-based access control

Role-based access control (RBAC) is a mechanism that restricts system access. It involves setting permissions and privileges to enable access to authorized users only. Access rights and actions are assigned according to a user's role within CDP Data Visualization.

Note: This feature is only available to users with administrative privileges.

RBAC enables administrators to exercise fine-grain control over data and feature access based on roles. Everyone who holds a certain role has the same set of rights. Those who hold different roles have different rights. For more information, see *Role privileges*.

RBAC consists of the following components:

Permissions

Permissions define access to visuals, datasets, data connections, and system-level functions. There are four categories of permissions: system, role, connection, and dataset. For more information, see the *List of permissions*.

Privileges

Privileges are sets of permissions of a particular type and the associated components on which the permissions are granted. For example, a privilege may consist of the permission View visuals and dashboards on component specifier Connection default / All datasets.

Members

Members are a list of users and groups that are assigned to a particular role.

Roles

Roles are collections of privileges and associated members who have these privileges.

Related Information

Role privileges
List of permissions

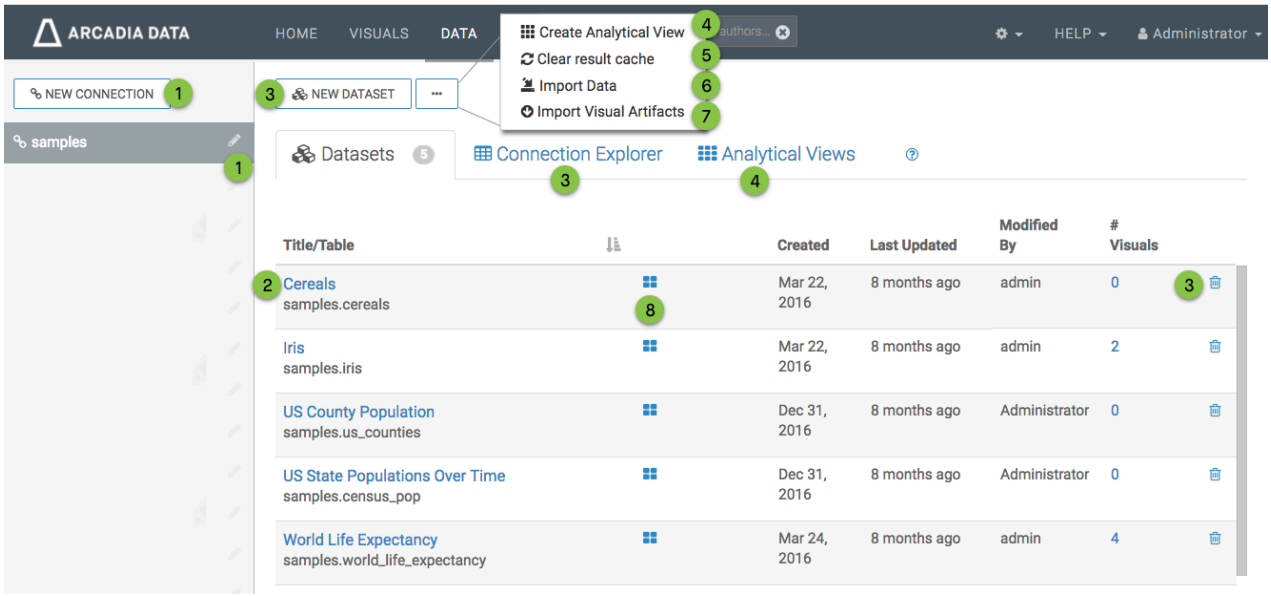
List of permissions

When defining privileges, the following default permissions exist at each level:

System-level permissions	Role-level permissions	Connection-level permissions	Dataset-level permissions
Site-level capabilities: • Create workspaces • Manage roles and users • Manage site settings • Manage custom styles • Manage jobs, email templates • View activity logs • Manage data connections	Defined separately for each role: • Grant manage datasets • Grant manage dashboards • Grant view dashboards	Defined separately for each data connection: • Manage analytical views • Import data • Create datasets, explore tables	Defined separately for each dataset: • Manage dataset • Manage dashboards • View dashboards

To connect the permissions to what options are available in the DATA interface of CDP Data Visualization, consider the following:

1. System-level Manage data connections permission is necessary to see the NEW CONNECTION button and to see the Pencil icon to edit existing connections.
2. Dataset-level View visuals and dashboards permission is necessary for a particular dataset to appear in the list of datasets for the selected connection.
3. Connection-level Create datasets, explore tables permission is necessary to see the NEW DATASET button over the list of datasets, the Connection Explorer tab, and the Delete icon on the dataset row.
4. Connection-level Manage data connections and dataset-level Manage dataset permissions are necessary to see the Clear result cache option in the Supplemental menu.
5. Connection-level Import data permission is necessary to see the Import Data option in the Supplemental menu.
6. System-level Manage styles and settings, connection-level Create datasets, explore tables, and dataset-level Manage dataset and Manage visuals and dashboards may all be required to see the Import Visual Artifacts option in the Supplemental menu. This depends on the type of import.
7. Dataset-level Manage visuals and dashboards permission is necessary to see the New Dashboard and New Visual links on the specified dataset rows.



Role privileges

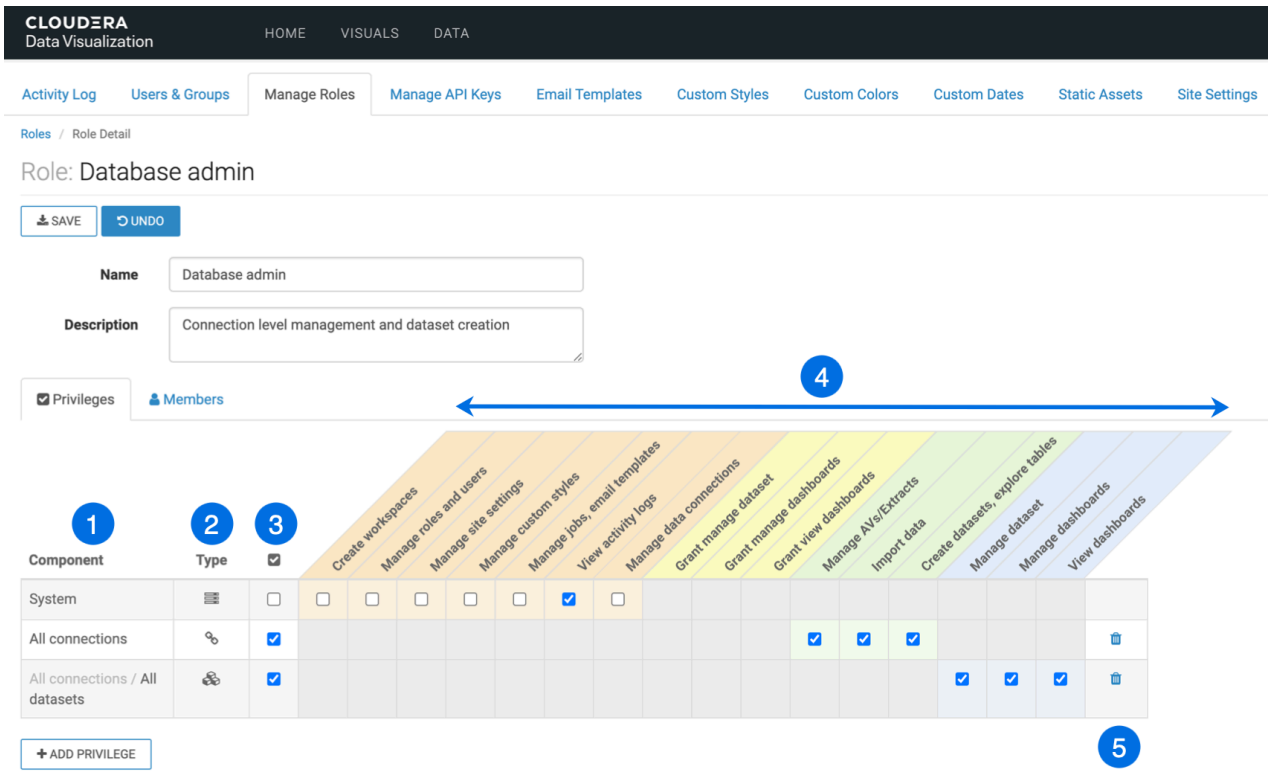
Privileges for a role may be defined on one of the following levels:

- System privileges
- Role privileges
- Connection privileges
- Dataset privileges

Note: This feature is only available to users with administrative privileges.

The Role Detail interface shows a table matrix of privilege components and the specific permissions granted to the role for that component. Each row shows one privilege, with following detail:

1. Set of components such as specific connection name(s), or specific dataset name(s)
2. Type of privilege component indicated by an icon, such as
    - System
    - Role
    - Connection
    - Dataset
3. Whole or partial; if granting all privileges for the specified component type, a check mark appears
4. Permissions enabled on the specified components, which include:
    - System privileges: Create workspaces, Manage roles and users, Manage site settings, Manage custom styles, Manage jobs and email templates, View activity logs, and Manage data connections
    - Role privilages: Grant manage dataset, Grant manage dashboard, and Grant view dashboard.
    - Connection privileges: Manage analytical views, Import data, and Create datasets, explore tables.
    - Dataset privileges: Manage dataset, Manage dashboards, and View dashboards.
5. Available actions on components, such as Edit and Delete.



See the following sections on how to add or change privileges defined for a specific role:

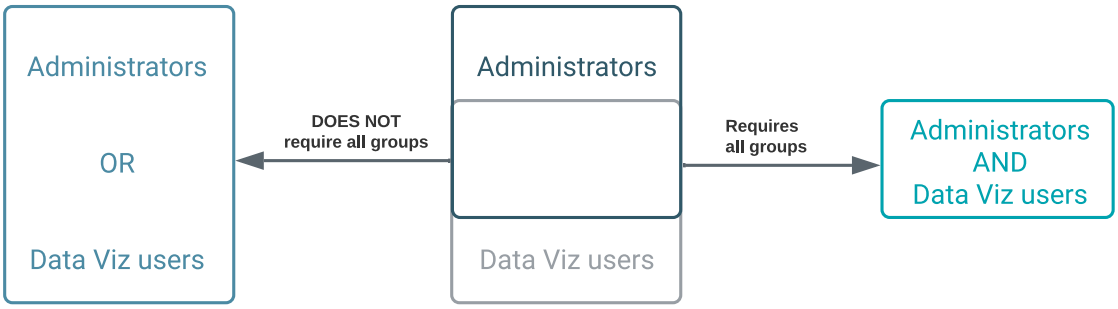
Related Information

Adding privileges
Setting system privileges
Setting role privileges
Setting connection privileges
Setting dataset privileges
Creating new roles

All groups requirement

The Require all groups option ensures that only members of ALL groups listed in the role membership fields have the role's defined access.

In this example, the role Administrators Only is shared by members of both Administrators and Data Viz users user groups. If you do not select the Require all groups option, all members of either group get the privileges of the role. However, if you check the Require all groups options, only users who are members of BOTH Administrators and Data Viz users user groups get the privileges of the role.



There are two other ways a user can be a member of the role, even when the Require all groups option is on:

- If the user is named specifically in the Users section of the membership page.
- For roles that are imported, if the Groups section is empty, and the user is a member of ANY imported group.

RBAC setup for dataset publishing

RBAC gives dataset creators an opportunity to 'publish' or share their datasets through a set of grants based role-based privileges. They can grant access to specific roles though the Grant manage dataset, Grant manage dashboards, and Grant view dashboards permissions.

Note:

- Only users with Manage roles and users role privileges (typically system administrators) can set up the roles and permissions, and define users and user groups.

For the purpose of demonstrating how dataset publishing works, consider this relatively simple scenario:

- There are three teams: Marketing, Sales, and Operations.
- There are three distinct access levels in each team: Data Admins, Analysts, and Visual Consumers.

To set up the required permissions, roles, groups, and users, read these topics:

1. Setting the dataset recipient roles
2. Setting the dataset publisher role
3. Define groups for teams and access levels
4. Assign groups to roles
5. Assign users to groups

After you complete these steps, Data Admins may publish their datasets, as described in Publishing datasets.

Related Information

Setting the dataset recipient roles
Setting the dataset publisher role
Define groups for teams and access levels
Assign groups to roles
Assign users to groups
Publishing datasets