How-To Library

Using Groups and Roles to Manage Informatica Access Control

Abstract

When you use groups and roles to organize Informatica access control, you simplify user management and create a more secure environment. This article describes how to identify groups and roles and examines the benefits of using groups and roles.

Supported Versions

- PowerCenter Advanced Edition 8.5.x - 8.6.x
- Informatica Data Quality 9.0 - 9.0.1
- Informatica Data Services 9.0 - 9.0.1
- PowerCenter 9.0 - 9.0.1

Table of Contents

Overview

When you manage hundreds of Informatica users, a common challenge is handling changes in personnel. When employees leave, employees change their position, or new employees join, you need to change Informatica access control.

If you directly assign privileges and permissions to users, managing personnel changes can be a tedious and time consuming task. For example, if a user changes positions within your organization, you must remove privileges and permissions that the user no longer needs, and then assign the user new privileges and permissions. If a new user joins your organization, you create the user in Informatica, assign privileges to the user, and then assign permissions to the user in each application client that the user accesses.

If you organize users into groups and then assign roles and permissions to the groups, you can more effectively manage personnel changes. For example, if a user changes positions within your organization, you move the user to another group. If a new user joins your organization, you add the user to a group. The users automatically inherit the privileges, roles, and permissions assigned to the group. You do not need to reassign the privileges, roles, and permissions.

When you use groups and roles to organize access control, you simplify and automate daily user administration tasks. In addition, you can complete the following tasks:

- Assign privileges and permissions to many users at once.

  Roles are collections of privileges. When you assign a role to a group, you assign the collection of privileges belonging to the role.

  Groups are collections of users. When you assign a role to a group, the group and all subgroups and users belonging to the group inherit the privileges belonging to the role. When you assign permissions to a group, all subgroups and users that belong to the group inherit the permissions.
- Place a label on a user that identifies the user's position in the organization.

  When you assign a user to the Developers group, you identify the user as a developer. When you directly assign privileges to a user, you can identify the user by name only. You have to examine the privileges assigned to the user to determine the user's position in the organization. If you have multiple Informatica administrators who manage access control, placing a label on each user enables the administrators to collaborate more effectively.

To manage access control using groups and roles, you first must identify the groups and roles that you need.

Note: In versions 8.5.x and 8.6.x, you use the Administration Console to manage users. Effective in version 9.0, the Administration Console is renamed to Informatica Administrator. This article refers to the tool as the Administrator tool.

Identifying Groups

Organize users who complete the same tasks into a group. For example, you can organize users into the following groups: Administrators, Developers, and Analysts.

Optimize groups so that each group contains a significant number of users. If you create groups that contain one or two users, you do not simplify the role, privilege, and permission assignment process.

When you identify groups, consider using the following features:

- Nested groups
- Users assigned to multiple groups
- Default Everyone group

Nested Groups

You can create groups that contain other groups. Use nested groups when part of a group needs additional privileges.

For example, you have a group of PowerCenter developers in India and another group of developers in Germany. The development group in India creates PowerCenter workflows, and another group in India creates and manages connection objects. The development group in Germany creates workflows and connection objects. You create the following nested groups:

Developers group. Assigned the predefined PowerCenter Developer role.

- India Developers group. Inherits the privileges belonging to the predefined PowerCenter Developer role.
- Germany Developers group. Inherits the privileges belonging to the predefined PowerCenter Developer role. Directly assigned the predefined PowerCenter Connection Administrator role.

Users Assigned to Multiple Groups

An individual in a group might need to perform additional tasks not granted to the entire group. As a best practice, assign the user to an additional group and then assign a role with the additional privileges to that group.

For example, an Informatica 9 Analyst tool user also administers the Analyst Service in the Administrator tool. Assign the user to the following groups:

- Analyst group. Assign a role that includes privileges to create projects and run profiles and scorecards in the Analyst tool.
- Analyst Administrator group. Assign a role that includes privileges to manage services in the Informatica domain.

Default Everyone Group

Effective in version 9.0, the Informatica domain includes a default group named Everyone. All users in the domain belong to the group. Use the Everyone group to grant general access to all users in the domain.

Assign roles and permissions to the Everyone group to grant the same access to all users. For example, in a PowerCenter development environment, you might want to create a role that includes all privileges in the PowerCenter Repository Service Tools privilege group. Assign the role to the Everyone group. You then grant all users access to all PowerCenter Client tools and command line programs.

As a best practice, use the Everyone group in the development environment. Do not use the Everyone group in the production environment. To maintain security in the production environment, limit the access granted to users.

Identifying Roles

Create roles that define the tasks that a group of users must complete. For example, you can create an Analyst role that includes privileges to create projects and run profiles and scorecards in the Informatica 9 Analyst tool. Assign the Analyst role to the Analyst group.

When you identify roles, consider using the following features:

- Predefined custom roles
- Roles for multiple service types

Predefined Custom Roles

Examine the predefined roles in the Administrator tool to determine whether you can assign these roles to your groups. Predefined roles include custom roles for the PowerCenter Repository Service, Metadata Manager Service, and Reporting Service.

The PowerCenter Repository Service roles are designed to create a secure production environment. You might want to assign the predefined PowerCenter Repository Service roles to groups to ensure that users access only what they need. Along with the roles, assign repository object permissions to define a group's level of access to repository objects.

The following table describes how you can use the PowerCenter Repository Service custom roles to create a secure environment:

PowerCenter Repository Service Custom Role	Description
PowerCenter Connection Administrator	Designed for administrators who create connection objects in the Workflow Manager. These administrators have access to source and target databases and applications. Assign this role to a small number of users to maintain source and target security.
PowerCenter Repository Folder Administrator	Designed for administrators who manage repository folders, deployment groups, labels, and queries. These administrators have access to metadata across repository folders. Assign this role to a small number of users to maintain repository folder security.
PowerCenter Developer	Designed for a developer who creates source definitions, target definitions, design objects, and workflows, and who runs and monitors workflows. Assign this role along with folder and global object permissions to restrict user access to the repository metadata that they need.
PowerCenter Operator	Designed for a workflow operator who runs and monitors workflows. In a production environment, you might want to assign this role to an automated user that a script uses to run and monitor workflows. If the automated user's login credentials are accessed, the user account cannot be used to change repository metadata.

If the predefined custom roles do not meet your needs, you can edit the privileges in the predefined custom roles or create your own custom roles.

Note: The Administrator role is a system-defined role that you cannot edit or delete. The role includes all privileges for the domain and each application service type. In addition, the role bypasses permission checking. Users with the Administrator role can access all objects. To maintain security, limit the number of users assigned the Administrator role.

Roles for Multiple Service Types

If a group needs to access multiple Informatica application clients, create a single role that includes privileges for multiple application service types.

For example, PowerCenter developers need to run data lineage on design objects, source definitions, and target definitions in the PowerCenter Client. When they launch data lineage on the PowerCenter repository objects, the PowerCenter Client launches Metadata Manager.

Create a single role that includes privileges for the following application service types:

- PowerCenter Repository Service. Includes privileges to create source definitions, target definitions, design objects, and workflows and to run and monitor workflows in the PowerCenter Client.
- Metadata Manager Service. Includes the privilege to view data lineage in Metadata Manager.

Tips for Using Groups and Roles

Create a collaborative development environment and a secure production environment.

In a development environment, encourage user collaboration by granting users more access to data. For example, you might want to use the default Everyone group in the development environment to grant all users access to all client tools or read permission on all objects.

In a production environment, ensure that data is secure by granting users a limited access to data. As a best practice, do not use the default Everyone group in the production environment.

Note: The default Everyone group is available effective in version 9.0.

Create a group named Exceptions to handle users who need a privilege temporarily or who need a privilege not assigned to any of their groups.

An individual in a group might need to perform additional tasks not granted to the entire group. As an exception, you can directly assign privileges and permissions to the user. However, you might forget to remove these privileges when the user no longer needs them.

As a best practice, create a group named Exceptions and add all users needing exceptions to the group. Assign a temporary privilege to the group so that all users inherit the privilege. Or, if you have multiple users in the Exceptions group that require different privileges, you can directly assign privileges to the users.

Periodically monitor and clean up the Exceptions group to ensure that users have the minimum privileges required to complete their tasks.

View which privileges are directly assigned to a user or group and which are inherited.

If you have not used an Exceptions group to handle exceptions, you might need to clean up privilege assignments. In the Administrator tool, the Privileges tab for a user displays all inherited privileges and all directly assigned privileges. The tooltip for an inherited privilege displays which role or group the user inherited the privilege from.

Use the information on the Privileges tab to determine which privileges are exceptions to the user's position in the organization.

View all domain objects that a user or group has permission on.

When you select a user or group in the following locations in the Administrator tool, you can view all domain objects that the user or group has permission on:

- Permissions tab in versions 8.5.x and 8.6.x
- Manage Permissions dialog box in versions 9.0 and 9.0.1

You can assign domain object permissions in these locations. Or, you can navigate to a domain object to assign permissions.

In an environment with a large number of users, use the infacmd command line program to automate repetitive user management tasks.

If you have a large number of users to manage, you can use the infacmd command line program to automate repetitive tasks. Automating repetitive user management tasks is easier when you use groups and roles. Because group and role names rarely change, you can consistently reference them by name within infacmd scripts.

After you organize users into well-defined groups and organize privileges into standardized roles, you can create command line scripts to assign roles and permissions to groups.

Common User Administration Tasks

When you use groups and roles to organize Informatica access control, daily user administration tasks are simpler to manage. This section examines common administration tasks and compares completing the tasks when Informatica access control is organized by users and privileges or by groups and roles. It examines the following administration tasks:

- Adding users
- Moving users to another Informatica domain
- Securing data in a multi-tenant environment

Case Study: Adding Users

A department within your organization needs to use Informatica. You need to add all 15 users within the department to the Informatica domain.

Organized by Users and Privileges

The Informatica domain contains users with privileges and permissions directly assigned to the users.

1. Log in to the Administrator tool and create 15 users.
2. In the Administrator tool, assign privileges to 15 users.
3. In the Administrator tool, assign permissions to 15 users.
4. Log in to each Informatica application client and assign permissions to 15 users.

Organized by Groups and Roles

The Informatica domain contains users that are organized into the following three groups: Developers, Analysts, and Administrators. Roles and permissions are assigned to the groups. The users that you need to add are analysts. You can assign the users to the existing Analysts group.

1. Log in to the Administrator tool and create 15 users.
2. In the Administrator tool, navigate to the Analyst group and assign 15 users to the group.

   The users inherit all privileges belonging to the roles assigned to the group and all permissions assigned to the group.

Case Study: Moving Users to Another Informatica Domain

You need to move users from a development to a test Informatica domain.

You can use the infacmd isp ExportUsersAndGroups and ImportUsersAndGroups commands to export and import users and groups. However, you cannot move privilege, role, and permission assignments across domains. After moving users and groups, you must reassign all privileges, roles, and permissions in the new domain.

Note: If you your domain contains LDAP users, configure the new domain to synchronize with the same LDAP directory service. After synchronization, you must reassign all privileges, roles, and permissions in the new domain.

Organized by Users and Privileges

The Informatica domain contains 100 users with privileges and permissions directly assigned to the users.

1. Use infacmd to export and import the users.
2. Log in to the Administrator tool and assign privileges to 100 users.
3. In the Administrator tool, assign permissions to 100 users.
4. Log in to each Informatica application client and assign permissions to 100 users.

Organized by Groups and Roles

The Informatica domain contains 100 users organized into the following three groups: Developers, Analysts, and Administrators. Roles and permissions are assigned to the groups.

1. Use infacmd to export and import the users and groups.
2. Log in to the Administrator tool and create roles for the migrated groups if the roles do not exist in the new domain.

3. In the Administrator tool, assign roles to three groups.
4. In the Administrator tool, assign permissions to three groups.
5. Log in to each Informatica application client and assign permissions to three groups.

Case Study: Securing Data in a Multi-tenant Environment

You have a multi-tenant environment where multiple departments access a single PowerCenter repository. The repository contains sensitive data that must not be shared across departments.

The following departments access the repository: Development, Sales, and Finance. Each department owns a set of folders in the repository. Some of the folders are shared with other departments, but most are accessed by a single department. The following table lists each folder in the repository and the departments that need to access the folder:

Folder	Departments that Access the Folder
Development1	Development
DevelopmentShared	Development, Sales, and Finance
Finance1	Finance
Finance2	Finance
Sales1	Sales
SalesShared	Sales and Finance

The departments have frequent employee turnover. You need to ensure that each department's data remains secure.

Organized by Users and Privileges

The Informatica domain contains 100 users with privileges and permissions directly assigned to the users.

1. In the Repository Manager, navigate to the properties of each folder.
2. Assign 100 users the appropriate permissions on the folder.

   For example, assign all users in the Development department write and execute permission on the Development1 folder. Do not assign users in the other departments permission on the Development1 folder.

When a user changes position in the organization or a new employee joins, navigate to each repository folder to assign the user the appropriate permissions.

Organized by Groups and Roles

The Informatica domain contains 100 users organized into the following three groups: Development, Sales, and Finance.

1. In the Repository Manager, navigate to the properties of each folder.
2. Assign three groups the appropriate permissions on the folder.

   For example, assign the Development group write and execute permission on the Development1 folder. Do not assign other groups permission on the Development1 folder.

When a user changes position in the organization or a new employee joins, add the user to the appropriate group. The user inherits the permissions assigned to the group.

Author

Alison Taylor

Acknowledgements

The author would like to acknowledge Sean Ma for his contributions to this article.