Oracle® Cloud

Administration du contrôle d'accès pour Oracle Enterprise Performance Management Cloud

F28926-05

ORACLE

Oracle Cloud Administration du contrôle d'accès pour Oracle Enterprise Performance Management Cloud

F28926-05

Auteur principal : EPM Information Development Team

Table des matières

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité de la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Commentaires sur la documentation

Pour envoyer des commentaires sur cette documentation, cliquez sur le bouton Commentaires situé en bas de la page de chaque rubrique du centre d'aide Oracle. Vous pouvez également envoyer un courriel à l'adresse epmdoc_ww@oracle.com.

1

Présentation du contrôle d'accès

L'accès aux composants Oracle Enterprise Performance Management Cloud est contrôlé par les rôles prédéfinis dans le domaine d'identité auquel les utilisateurs sont affectés. Les administrateurs de service peuvent affecter des rôles propres aux applications de planification, de consolidation et de gestion des données à des utilisateurs afin de leur permettre d'effectuer des tâches supplémentaires dans un environnement.

Par exemple, les administrateurs de service peuvent affecter le rôle Administrateur des approbations d'une application de planification ou de consolidation à un utilisateur afin de lui permettre d'effectuer des activités liées aux approbations.

En outre, les administrateurs de service peuvent créer, à partir du contrôle d'accès, des groupes comprenant des utilisateurs ayant le rôle Domaine d'identité ou d'autres groupes. L'affectation de rôles à de tels groupes permet aux administrateurs de service d'octroyer simultanément des rôles à de nombreux utilisateurs, réduisant ainsi les frais généraux de gestion.

L'affectation de rôles au niveau application peut uniquement améliorer les droits d'accès des utilisateurs. Aucun des privilèges octroyés par un rôle prédéfini ne peut être limité par des rôles affectés au niveau application.

Le contrôle d'accès permet de réaliser les activités suivantes dans un environnement :

- Gestion des groupes
- Affectation de rôles à un groupe ou à un utilisateur
- Génération d'un rapport sur l'affectation de rôle pour un utilisateur ou un groupe
- Affichage du rapport sur l'affectation de rôle pour votre environnement
- Affichage du rapport sur les connexions utilisateur

A propos de ce guide

Le contrôle d'accès s'applique aux processus métier Oracle Enterprise Performance Management Cloud suivants :

- Planning
- Modules Planning
- Financial Consolidation and Close
- Tax Reporting
- Profitability and Cost Management
- Account Reconciliation

- Oracle Enterprise Data Management Cloud
- Narrative Reporting
- Oracle Strategic Workforce Planning Cloud
- Oracle Sales Planning Cloud

Ouverture du contrôle d'accès

Vous pouvez affecter des rôles propres à une application aux groupes et aux utilisateurs à partir de **Contrôle d'accès**, disponible dans la carte **Outils** sur la page d'accueil.

Pour ouvrir Contrôle d'accès, procédez comme suit :

1. Accédez à l'environnement en tant qu'administrateur de service.
2. Exécutez une étape :
   - Cliquez sur  (navigateur), puis sur **Contrôle d'accès**.
   - Cliquez sur **Outils**, puis sur **Contrôle d'accès**.
   - **Oracle Enterprise Data Management Cloud et Narrative Reporting uniquement :** cliquez sur **Contrôle d'accès**.

Gestion des groupes

Oracle Enterprise Performance Management Cloud utilise un référentiel interne afin de prendre en charge les affectations de rôle au niveau application et de stocker les informations relatives aux groupes que vous utilisez lors du processus d'affectation de rôle.

Les utilisateurs EPM Cloud et les autres groupes peuvent être membres de groupes gérés à l'aide du contrôle d'accès. Les utilisateurs peuvent obtenir des rôles d'application par l'affectation du rôle donné au groupe.

Pour vous permettre de visualiser les affectations des utilisateurs, le contrôle d'accès répertorie les rôles prédéfinis en tant que groupes. Vous ne pouvez ni les modifier ni les affecter aux groupes à partir du contrôle d'accès. Par ailleurs, les utilisateurs EPM Cloud, qui disposent de rôles prédéfinis, sont répertoriés dans le contrôle d'accès afin de pouvoir être ajoutés en tant que membres de groupe. Reportez-vous à la section Présentation des rôles prédéfinis du guide *Mise en route d'Oracle Enterprise Performance Management Cloud pour les administrateurs*.

- Création de groupes
- Modifications des groupes
- Suppression des groupes

Remarque : Vous ne pouvez pas utiliser le contrôle d'accès pour importer les informations de groupe d'un fichier afin de créer des groupes. De même, vous ne pouvez pas exporter d'informations de groupe à l'aide du contrôle d'accès. Vous pouvez utiliser Migration ou la commande createGroups d'EPM Automate pour importer des groupes.

Création de groupes

Seuls les administrateurs de service peuvent créer et gérer des groupes. Les utilisateurs Oracle Enterprise Performance Management Cloud et les autres groupes peuvent être membres d'un groupe.

> **Remarque :** Vous pouvez également utiliser Migration ou la commande createGroups d'EPM Automate pour importer les informations de groupe d'un fichier afin de créer des groupes.

Pour créer des groupes, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Dans **Gérer les groupes**, cliquez sur **Créer**.
3. Dans **Créer un groupe**, suivez la procédure ci-dessous :
   a. Dans **Nom**, entrez un nom de groupe unique (256 caractères maximum).

      Les noms de groupe ne sont pas sensibles à la casse. Pour éviter toute ambiguïté dans les rapports de sécurité, EPM Cloud ne vous permet pas de créer des groupes avec des noms identiques aux noms de rôle prédéfini en cours ou précédents (Administrateur de service, Super utilisateur, Utilisateur, Visualiseur, Planificateur, Administrateur système, Administrateur d'application, Administrateur de bibliothèque, Administrateur de rapport).

   b. **Facultatif :** entrez une description du groupe.
4. **Facultatif :** ajoutez des groupes pour créer un groupe imbriqué.
   a. Dans **Groupes disponibles**, recherchez des groupes. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

      Les groupes répondant aux critères de recherche sont répertoriés sous **Groupes disponibles**.

   b. Dans **Groupes disponibles**, sélectionnez les groupes membres du nouveau groupe.

   c. Cliquez sur **Déplacer**.

      Les groupes sélectionnés sont répertoriés sous **Groupes affectés**. Pour enlever des groupes affectés, dans **Groupes affectés**, sélectionnez le groupe à enlever et cliquez sur **Enlever**.
5. **Facultatif :** ajoutez des utilisateurs EPM Cloud en tant que membres du groupe. Seuls les utilisateurs disposant d'un rôle prédéfini peuvent être ajoutés en tant que membres de groupe.
   a. Cliquez sur **Utilisateurs**.

   b. Dans **Utilisateurs disponibles**, recherchez des utilisateurs. Reportez-vous à la section Utilisation de la recherche pour obtenir des instructions.

   c. Dans **Utilisateurs disponibles**, sélectionnez les utilisateurs à ajouter au groupe.

d. Cliquez sur **Déplacer**.

6. Cliquez sur **Enregistrer**.
7. Cliquez sur **OK**.

Modifications des groupes

Les administrateurs de service peuvent modifier les propriétés de groupe, y compris le nom de groupe. Renommer un groupe n'a pas d'incidence sur les rôles d'application affectés au groupe et sur les autres affectations de sécurité.

Pour modifier des groupes, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. **Facultatif :** dans **Gérer les groupes**, localisez le groupe à modifier. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

> **Remarque :** Les noms de groupe ne peuvent pas contenir plus de 71 caractères. Toutefois, seuls les 34 premiers caractères apparaissent dans la liste affichée dans la colonne **Groupes disponibles**.

3. Cliquez sur  (Action) dans la ligne correspondant au groupe à modifier, puis sélectionnez **Modifier**.
4. **Facultatif :** modifiez le nom de groupe. La modification du nom de groupe n'influe pas sur les affectations de sécurité effectuées à l'aide du groupe.
5. Modifiez l'affectation de groupe en procédant comme suit :
   a. **Facultatif :** ajoutez des groupes imbriqués de la manière suivante :
      - Dans **Groupes disponibles**, recherchez des groupes. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
      - Dans **Groupes disponibles**, sélectionnez des groupes et cliquez sur **Déplacer**.

        Les groupes sélectionnés sont répertoriés dans la liste **Groupes affectés**.

   b. **Facultatif :** enlevez des groupes imbriqués de la manière suivante :
      - Dans **Groupes affectés**, sélectionnez le groupe à supprimer.
      - Cliquez sur **Enlever**.
6. Modifiez l'affectation d'utilisateur en procédant comme suit :
   a. Cliquez sur **Utilisateurs**.
   b. **Facultatif :** ajoutez des utilisateurs à un groupe de la manière suivante :
      - Dans **Utilisateurs disponibles**, recherchez les utilisateurs que vous pouvez affecter en tant que membres de groupe. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

- Dans **Utilisateurs disponibles**, sélectionnez des utilisateurs et cliquez sur **Déplacer**.

  Les utilisateurs sélectionnés sont répertoriés dans la liste **Utilisateurs affectés**.

c. **Facultatif :** enlevez des utilisateurs du groupe de la manière suivante :

- Dans **Utilisateurs affectés**, sélectionnez les utilisateurs à supprimer.
- Cliquez sur **Enlever**.

7. Cliquez sur **Enregistrer**.
8. Cliquez sur **OK**.

Suppression des groupes

La suppression d'un groupe ne supprime pas ses membres.

Pour supprimer un groupe :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. **Facultatif :** dans **Gérer les groupes**, recherchez le groupe à supprimer. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
3. Cliquez sur  (Action) dans la ligne correspondant au groupe à supprimer, puis sélectionnez **Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression.
5. Cliquez sur **OK**.

Import d'affectations de groupe d'utilisateurs à partir d'un fichier

Les administrateurs de service peuvent importer des affectations de groupe d'utilisateurs à partir d'un fichier CSV (valeurs séparées par des virgules) pour créer des affectations dans un groupe de contrôle d'accès existant. Oracle Enterprise Performance Management Cloud applique les affectations de sécurité de niveau application et de niveau artefact en fonction des nouvelles affectations de groupe.

Remarque : Toutes les connexions utilisateur identifiées dans le fichier d'import doivent exister dans le domaine d'identité et tous les noms de groupe inclus dans le fichier doivent exister dans le contrôle d'accès. Vous ne pouvez pas créer de groupe en utilisant ce processus d'import.

Vous pouvez uniquement créer des affectations de groupe. Vous ne pouvez pas enlever les affectations de groupe en cours des utilisateurs.

Le format de fichier d'import CSV peut se présenter comme dans les illustrations suivantes :

```
User Login,Group
jdoe, Example_grp1
jane.doe@example.com, Example_grp2
```

```
User Login,First Name,Last Name,Email,Direct,Group
jdoe, John, Doe, jdoe@example.com, Yes, Example_grp1
jane.doe@example.com, Jane, Doe, jane.doe@example.com, No, Example_grp2
```

Ce format est identique à la version CSV du rapport sur le groupe d'utilisateurs. Si vous utilisez ce format, le processus d'import ignore toutes les colonnes autres que Connexion utilisateur et Groupe. Pour créer facilement un fichier d'import, vous pouvez exporter le rapport sur le groupe d'utilisateurs en cours, puis le modifier selon vos besoins. Reportez-vous à la section Affichage et export du rapport sur le groupe d'utilisateurs.

Pour importer des affectations de groupe d'utilisateurs, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Rapport sur le groupe d'utilisateurs**.
3. Cliquez sur **Importer à partir du fichier CSV**.
4. A l'aide de l'option **Parcourir** dans **Importer le fichier CSV d'affectation de groupe d'utilisateurs**, sélectionnez le fichier d'import.
5. Cliquez sur **Importer**.
6. Cliquez sur **Oui**.

   Une fois le processus d'import terminé, une boîte de dialogue de confirmation indiquant le statut et le nombre total d'affectations traitées apparaît.

Affectation d'un utilisateur à plusieurs groupes

Les utilisateurs Oracle Enterprise Performance Management Cloud peuvent être membres de plusieurs groupes gérés à l'aide du contrôle d'accès.

Pour affecter un utilisateur à plusieurs groupes, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Gérer les utilisateurs**.

   La liste de tous les utilisateurs de l'environnement en cours apparaît.
3. Recherchez l'utilisateur à affecter à des groupes . Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
4. Cliquez sur  (Action) dans la ligne voulue de la liste d'utilisateurs, puis sélectionnez **Modifier**.

   L'écran **Modifier l'utilisateur** apparaît. Il répertorie des informations utilisateur détaillées, dont les appartenances actuelles aux groupes (dans **Groupes affectés**). Sur cet écran, vous pouvez uniquement modifier les affectations de groupe.

5. Recherchez les groupes à affecter à l'utilisateur. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

6. Effectuez l'une des actions suivantes :

   - Pour affecter d'autres groupes à l'utilisateur, sélectionnez-les dans **Groupes disponibles** et cliquez sur (**Déplacer**) afin de les déplacer vers **Groupes affectés**. Vous pouvez également cliquer sur (**Déplacer tout**) pour déplacer tous les groupes dans **Groupes disponibles** vers **Groupes affectés**.

   - Pour enlever des groupes affectés à l'utilisateur, sélectionnez-les dans **Groupes affectés** et cliquez sur (**Enlever**) afin de les déplacer vers **Groupes disponibles**. Vous pouvez également cliquer sur (**Enlever tout**) pour déplacer tous les groupes dans **Groupes affectés** vers **Groupes disponibles**.

7. Cliquez sur **Enregistrer**.

8. Cliquez sur **OK**.

Utilisation de la recherche

La recherche intelligente des artefacts d'utilisateur et de groupe fonctionne de la même manière dans le contrôle d'accès.

Vous utilisez une chaîne de l'un des attributs de l'utilisateur (nom d'utilisateur, prénom, nom de famille ou ID de messagerie), ou le nom du groupe ou du rôle afin de rechercher des utilisateurs, des groupes ou des rôles spécifiques. Vous n'avez pas besoin d'utiliser de caractères génériques dans les chaînes de recherche. Par exemple, la chaîne `st` dans une recherche de groupes affiche tous les noms de groupe contenant `st`, par exemple : TestGroup, Strategic_Planner ou AnalystsGroup. De même, la chaîne `jd` dans une recherche d'utilisateurs répertorie les utilisateurs dont le nom d'utilisateur, le prénom, le nom de famille ou l'adresse électronique contient la chaîne `jd`.

Remarque : Certains écrans du contrôle d'accès, comme **Affecter des rôles d'application**, **Rapport sur l'affectation de rôle** et **Rapport sur le groupe d'utilisateurs**, proposent une option de recherche. Sélectionnez l'option appropriée avant de démarrer une recherche.

Pour rechercher des utilisateurs, procédez comme suit :

1. Accédez à un écran, par exemple **Gérer les utilisateurs**, où la fonctionnalité de recherche d'utilisateur est disponible.

2. Dans le champ de recherche, saisissez partiellement un attribut utilisateur (nom d'utilisateur, prénom, nom de famille ou ID de messagerie).

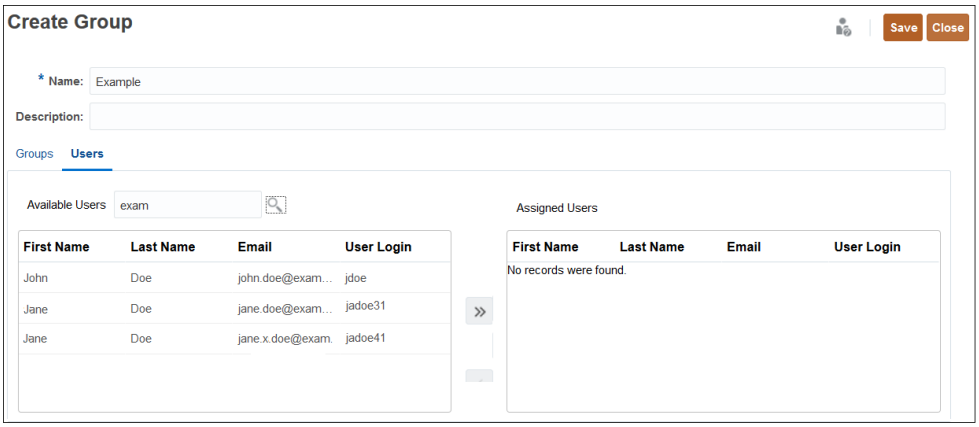
3. Cliquez sur (Rechercher).

   Les résultats de la recherche affichent toutes les propriétés disponibles pour les utilisateurs correspondant au critère de recherche. Vous pouvez trier la liste des utilisateurs extraits en cliquant sur l'un des en-têtes de colonne.

Pour rechercher des groupes :

- Accédez à un écran, par exemple **Gérer les groupes**, où la fonctionnalité de recherche de groupe est disponible.
- Dans le champ de recherche, saisissez partiellement un nom de groupe.
- Cliquez sur (Rechercher).

  Les résultats de la recherche affichent le nom et la description des groupes correspondant au critère de recherche. Vous pouvez trier la liste des groupes extraits en fonction du nom ou de la description de groupe.



Pour rechercher des utilisateurs en fonction de leurs rôles dans le rapport sur l'affectation de rôle, procédez comme suit :

- Accédez à l'onglet **Rapport sur l'affectation de rôle**.
- Sélectionnez **Utilisateurs** ou **Rôles** dans la liste déroulante de recherche.
- Dans le champ de recherche, saisissez une chaîne de recherche.
- Cliquez sur (Rechercher).

  Les résultats de la recherche affichent toutes les informations disponibles sur les utilisateurs disposant des rôles correspondant au critère de recherche.

2

Gestion des affectations de rôle au niveau application

L'affectation de rôle au niveau application est prise en charge pour les applications de planification, de consolidation et de clôture, de déclaration fiscale et Oracle Profitability and Cost Management Cloud. Les applications de planification, de consolidation et Oracle Enterprise Data Management Cloud utilisent des rôles granulaires propres à l'application pour améliorer les privilèges d'accès octroyés via les rôles prédéfinis tandis que Profitability and Cost Management affecte des autorisations d'accès aux données de niveau utilisateur et groupe afin de sécuriser l'accès aux données d'application.

Présentation

Tandis que les droits d'accès globaux sont contrôlés par des rôles prédéfinis d'Oracle Enterprise Performance Management Cloud, les administrateurs de service peuvent octroyer des autorisations de données et des rôles propres à l'application à des utilisateurs et à des groupes créés et gérés dans le contrôle d'accès. Par exemple, par défaut, les droits de conception du processus des approbations ne sont pas octroyés aux utilisateurs, mais aux super utilisateurs et aux administrateurs de service. Dans le contrôle d'accès, les administrateurs de service peuvent affecter le rôle Administrateur des approbations pour permettre à l'utilisateur d'effectuer des activités liées aux approbations.

Les affectations de rôle au niveau application peuvent uniquement améliorer les droits d'accès des utilisateurs. Aucun des privilèges octroyés par un rôle prédéfini ne peut être limité par l'affectation d'un rôle au niveau application.

Vous pouvez gérer le processus d'affectation de rôle à l'aide du contrôle d'accès. Vous pouvez effectuer les tâches suivantes :

- Créer des groupes et ajouter des utilisateurs EPM Cloud ou d'autres groupes en tant que membres
- Ajouter ou supprimer des membres dans les groupes
- Affecter des rôles d'application Planning et Consolidation à des groupes ou à des utilisateurs
- Afficher la liste des utilisateurs qui sont membres d'un groupe

Utilisateurs EPM Cloud

Vous créez et gérez les utilisateurs EPM Cloud dans le domaine d'identité associé à l'environnement auquel appartient le processus métier. Vous pouvez affecter des rôles de niveau application uniquement aux utilisateurs disposant de rôles prédéfinis afin d'améliorer leur accès pour effectuer des tâches dans un processus métier.

Rôles d'application Planning et Consolidation

Les rôles suivants concernent les applications Planning, Consolidation et Tax Reporting uniquement. Reportez-vous au guide *Administration de Profitability and Cost Management* pour plus d'informations sur l'affectation des autorisations de données à partir de l'application Profitability and Cost Management.

Par défaut, seuls les administrateurs de service et les superutilisateurs ont accès à Data Management pour manipuler le processus d'intégration de données. Pour permettre aux utilisateurs dotés du rôle de domaine d'identité Utilisateur ou Visualiseur de participer au processus d'intégration, les administrateurs de service doivent leur affecter des rôles Gestion des données (Créer une intégration, Exécuter l'intégration et Explorer en amont).

Administrateur des approbations

Résout les problèmes d'approbation en s'appropriant manuellement le processus. Se compose des rôles suivants : Cédant de propriété des approbations, Concepteur du processus des approbations et Superviseur des approbations.

Généralement, ce rôle est affecté aux utilisateurs en entreprise qui sont responsables d'une région et qui ont besoin de contrôler le processus des approbations pour cette région, sans avoir besoin de disposer du rôle d'administrateur de Planning. Ils peuvent effectuer les tâches suivantes :

- Contrôler le processus des approbations
- Effectuer des actions sur les unités Planning auxquelles ils ont un accès en écriture
- Affecter des propriétaires et des réviseurs pour l'organisation dont ils sont responsables
- Modifier la dimension secondaire ou mettre à jour les règles de validation

Cédant de propriété des approbations

Effectue toutes les tâches réalisables par les utilisateurs dotés du rôle Planificateur. En outre, il effectue les tâches suivantes pour tout membre de la hiérarchie d'unités de planification auquel il a accès en écriture :

- Affecter des propriétaires
- Affecter des réviseurs
- Indiquer les utilisateurs à avertir

Concepteur du processus des approbations

Effectue toutes les tâches réalisables par les utilisateurs dotés du rôle Planificateur et Cédant de propriété des approbations. En outre, il effectue les tâches suivantes pour tout membre de la hiérarchie d'unités de planification auquel il a accès en écriture :

- Modifier les dimensions secondaires et les membres des entités auxquelles l'utilisateur a accès en écriture
- Modifier l'affectation de scénario et de version pour une hiérarchie d'unité de planification

- Modifier les règles de validation des données des formulaires auxquels l'utilisateur a accès

Superviseur des approbations

Effectue les tâches suivantes pour tout membre de la hiérarchie d'unités de planification auquel l'utilisateur a accès en écriture, même si l'utilisateur n'est pas propriétaire de l'unité de planification. Cet utilisateur ne peut pas modifier les données des unités de planification dont il n'est pas propriétaire.

- Démarrer et arrêter une unité de planification
- Effectuer n'importe quelle action sur une unité de planification

Créateur de grille ad hoc

Crée, affiche, modifie et enregistre les grilles ad hoc.

Utilisateur ad hoc

Affiche et modifie les grilles ad hoc, et effectue des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc.

Utilisateur ad hoc en lecture seule

Effectue toutes les fonctions ad hoc, mais ne peut pas réécrire dans les grilles ad hoc ni charger des données à l'aide de Data Management.

Allocation en masse

Exécute des règles d'allocation en masse dans des grilles de formulaire.

Gestionnaire d'accès à la liste des tâches

Affecte des tâches à d'autres utilisateurs.

Créer une intégration

Utilise Data Management pour créer des mappings afin d'intégrer des données entre des systèmes source et cible. Les utilisateurs peuvent définir des règles de données avec différentes options d'exécution.

Exécuter l'intégration

A partir de Data Management, exécute des règles de données avec des paramètres d'exécution et visualise des journaux d'exécution.

Explorer en amont

Effectue une exploration amont jusqu'au système source des données.

Rôles d'application Oracle Enterprise Data Management Cloud

Ces rôles concernent seulement les applications Oracle Enterprise Data Management Cloud.

Créateur de l'application

Inscrit les applications dans Oracle Enterprise Data Management Cloud. L'utilisateur qui inscrit une application reçoit l'autorisation Propriétaire de l'application. Cet utilisateur devient également le propriétaire de la vue d'application par défaut.

Auditeur

Visualise les informations liées à l'audit telles que l'historique des transactions et les demandes de modification de données dans Oracle Enterprise Data Management Cloud.

Créateur de vues

Crée des vues dans une application Oracle Enterprise Data Management Cloud. L'utilisateur qui crée une vue reçoit l'autorisation Propriétaire de la vue.

Affectation de rôles à un groupe ou à un utilisateur

Lors du processus, les administrateurs de service affectent des rôles de niveau application aux groupes et aux utilisateurs disposant d'un rôle prédéfini.

Remarque :

Vous ne pouvez pas affecter de rôles d'application à votre propre compte d'utilisateur.

Pour que vous puissiez visualiser les affectations de rôle, le contrôle d'accès répertorie les rôles Oracle Enterprise Performance Management Cloud prédéfinis en tant que groupes. Vous ne pouvez pas leur affecter des rôles de niveau application à partir du contrôle d'accès.

Pour affecter des rôles de niveau application à un groupe ou à un utilisateur, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Affecter des rôles d'application**.
3. Recherchez un utilisateur ou un groupe. Dans la liste déroulante, sélectionnez **Utilisateurs** ou **Groupes**. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
4. Cliquez sur l'icône  (**Actions**) correspondant à l'utilisateur ou au groupe, puis sélectionnez **Affecter des rôles**.
5. Dans **Rôles disponibles**, sélectionnez les rôles à affecter à l'utilisateur ou au groupe, puis cliquez sur **Déplacer**.

   Pour avoir une description des rôles qui peuvent être affectés aux utilisateurs et aux groupes, reportez-vous aux sections suivantes :

   - Rôles d'application Planning et Consolidation
   - Rôles d'application Oracle Enterprise Data Management Cloud

Les rôles sélectionnés sont répertoriés sous **Rôles affectés**. Pour enlever des rôles affectés, dans **Rôles affectés**, sélectionnez le rôle à enlever, puis cliquez sur **Enlever**.

6. Cliquez sur **OK**.
7. Cliquez sur **OK**.

Suppression de rôles de niveau application affectés à un groupe ou à un utilisateur

Ce processus entraîne la suppression de tous les rôles d'application affectés au groupe ou à l'utilisateur. La suppression de l'affectation de rôle de niveau application n'a aucune incidence sur les rôles prédéfinis de l'utilisateur.

Pour enlever les rôles de niveau application d'un groupe ou d'un utilisateur, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Affecter des rôles d'application**.
3. Recherchez un utilisateur ou un groupe. Dans la liste déroulante, sélectionnez **Utilisateurs** ou **Groupes**. Pour obtenir des instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
4. Cliquez sur l'icône  (Actions) correspondant à l'utilisateur ou au groupe, puis sélectionnez **Annuler l'affectation des rôles**.
5. Cliquez sur **Oui**.
6. Cliquez sur **OK**.

3

Génération de rapports

Vous pouvez utiliser les rapports pour analyser et gérer les affectations de rôle de la façon suivante :

- Génération d'un rapport sur l'affectation de rôle pour un utilisateur ou un groupe
- Affichage du rapport sur l'affectation de rôle pour votre environnement
- Affichage du rapport sur les connexions utilisateur
- Affichage et export du rapport sur le groupe d'utilisateurs

L'heure de génération de rapport indiquée sur les rapports reflète l'heure en fonction du fuseau horaire du navigateur (horloge système locale).

A propos de la version CSV du rapport

Vous pouvez exporter un rapport pour créer une version CSV (valeurs séparées par une virgule) de celui-ci. Outre le nombre d'utilisateurs disposant de rôles prédéfinis, la version CSV du rapport répertorie les éléments suivants :

- Les rôles prédéfinis affectés à chaque utilisateur. Chaque rôle prédéfini affecté à un utilisateur apparaît sur une ligne distincte. Les rôles d'application inclus dans des rôles prédéfinis ne sont pas indiqués.
- Les rôles d'application affectés directement ou via un groupe à un utilisateur. Chaque rôle d'application affecté à un utilisateur apparaît sur une ligne distincte.
- Les groupes auxquels un utilisateur est affecté ne sont pas répertoriés, même si les groupes en question ne sont affectés à aucun rôle.
- Seules les informations de la vue en cours du rapport sont exportées dans le fichier CSV. Par exemple, si vous filtrez le rapport afin d'afficher les affectations de rôle d'un utilisateur spécifique, le fichier CSV exporté contient uniquement les affectations de cet utilisateur.

Génération d'un rapport sur l'affectation de rôle pour un utilisateur ou un groupe

Les administrateurs de service utilisent le rapport sur l'affectation de rôle pour vérifier les rôles prédéfinis et les rôles d'application affectés aux utilisateurs. Les groupes auxquels appartient l'utilisateur ne sont pas répertoriés s'ils ne sont pas utilisés pour affecter des rôles d'application à l'utilisateur. Ce rapport permet de suivre l'accès utilisateur à des fins de reporting de conformité.

Afin de générer un rapport sur l'affectation de rôle pour un utilisateur ou un groupe, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Affecter des rôles d'application**.
3. Recherchez un utilisateur ou un groupe. Dans la liste déroulante, sélectionnez **Utilisateurs** ou **Groupes**. Pour obtenir des instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
4. Cliquez sur l'icône **Action** (**Actions**) correspondant à l'utilisateur ou au groupe pour lequel un rapport doit être généré, puis sélectionnez **Rapport sur l'affectation de rôle**.
5. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter le rapport dans un fichier CSV.
6. Cliquez sur **Fermer** pour fermer le rapport.

Affichage du rapport sur l'affectation de rôle pour votre environnement

Les administrateurs de service utilisent le rapport sur l'affectation de rôle pour vérifier l'accès, affecté via des rôles de niveau application et des rôles prédéfinis, de tous les utilisateurs. Le rapport répertorie les rôles prédéfinis (par exemple, Super utilisateur) et les rôles d'application (par exemple, Allocation en masse, qui est un rôle d'application Planning) affectés à l'utilisateur.

Les rôles hérités, ainsi que les informations relatives à l'héritage, sont affichés sur une ligne distincte pour chaque utilisateur. Par exemple, supposons que l'utilisateur `John Doe` dispose du rôle prédéfini `User` et que `User` est membre du groupe `example` auquel le rôle d'application Planning `Approvals Administrator` est affecté. Dans ce scénario, le rapport sur l'affectation de rôle affiche les éléments suivants en tant qu'informations relatives à l'affectation de rôle pour `John Doe` :

`Approvals Administrator (example->User)`.

Le rapport sur l'affection de rôle identifie également le nombre d'utilisateurs autorisés à accéder à l'environnement en fonction de leurs rôles prédéfinis. Il ne répertorie pas les rôles d'application inclus dans les rôles prédéfinis ou les rôles de composant des rôles d'application affectés à l'utilisateur. Si vous avez besoin d'un rapport présentant ces informations, vous pouvez générer la version classique du rapport à l'aide de la commande provisionReport d'EPM Automate.

Vous pouvez exporter le rapport sur l'affectation de rôle sous la forme d'un fichier CSV, que vous pouvez ensuite ouvrir à l'aide d'un programme tel que Microsoft Excel ou enregistrer sur votre ordinateur. Le rapport sur l'affectation de rôle au format CSV indique chaque affectation de rôle sur une ligne distincte.

	A	B	C	D	E	F
1	User Login	First Name	Last Name	Email	Role	Granted through Group
2	Jdoe	John	Doe	jdoe@example.com	Planner	
3	jdoe	John	Doe	jdoe@example.com	Power User	
4	Jdoe	John	Doe	jdoe@example.com	Service Administrator	
5	jdoe	John	Doe	jdoe@example.com	Viewer	
6	Jdoe	John	Doe	jdoe@example.com	Mass Allocation	example->Power User
7	jdoe	John	Doe	jdoe@example.com	Run Integration	
8	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Planner	
9	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Power User	
10	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Viewer	
11	jane.doe@example.com	Jane	Doe	jane.doe@example.com	Mass Allocation	example

Pour ouvrir le rapport sur l'affectation de rôle, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Rapport sur l'affectation de rôle**.

   Le rapport sur l'affectation de rôle apparaît.
3. **Facultatif :** filtrez le rapport afin d'afficher les éléments ci-dessous.
   - Affectations de rôle d'un utilisateur spécifique. Sélectionnez **Utilisateurs** dans la liste déroulante et entrez une chaîne de recherche partielle. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
   - Utilisateurs affectés à un rôle spécifique. Sélectionnez **Rôles** dans la liste déroulante et entrez un nom de rôle partiel. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

   Remarque : Les utilisateurs peuvent disposer de plusieurs rôles. Dans ce cas, le rapport répertorie tous les rôles de l'utilisateur, même si vous le filtrez sur un rôle spécifique.
4. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter le rapport dans un fichier CSV. Seules les informations du rapport en cours d'affichage sont exportées dans le fichier CSV.

Affichage du rapport sur les connexions utilisateur

Par défaut, le rapport sur les connexions utilisateur contient des informations sur les utilisateurs qui se sont connectés à l'environnement au cours des dernières 24 heures. Il répertorie l'adresse IP de l'ordinateur à partir duquel l'utilisateur s'est connecté, ainsi que la date et l'heure (au format UTC) auxquelles il a accédé à l'environnement.

Les administrateurs de service peuvent régénérer ce rapport pour une plage de dates personnalisée ou pour les 30 derniers jours, les 90 derniers jours et les 120 derniers jours. Ils peuvent également filtrer le rapport afin d'afficher uniquement les informations d'utilisateurs spécifiques en saisissant partiellement le prénom, le nom ou l'ID des utilisateurs comme chaîne de recherche.

Remarque : Oracle Enterprise Performance Management Cloud conserve l'historique d'audit des connexions utilisateur des 120 derniers jours uniquement.

Pour régénérer le rapport sur les connexions utilisateur, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Rapport sur les connexions utilisateur**.

   Un rapport répertoriant tous les utilisateurs qui se sont connectés à l'environnement au cours du jour précédent s'affiche.
3. Sélectionnez une période (Dernier jour, 30 derniers jours, 90 derniers jours, 120 derniers jours) pour laquelle générer le rapport. Pour indiquer une plage de dates personnalisée, sélectionnez **Plage de dates**, puis choisissez une date de début et une date de fin.
4. **Facultatif :** sélectionnez les utilisateurs à inclure dans le rapport. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
5. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter le rapport affiché sous forme de fichier CSV.
6. Cliquez sur **Annuler** pour fermer le rapport.

Affichage et export du rapport sur le groupe d'utilisateurs

Le rapport sur le groupe d'utilisateurs répertorie les appartenances directes ou indirectes des utilisateurs affectés à des groupes dans le contrôle d'accès.

Les utilisateurs sont considérés comme des membres directs d'un groupe s'ils y sont affectés et comme des membres indirects, s'ils sont affectés à un groupe enfant d'un autre groupe. Pour chaque utilisateur affecté à un groupe, le rapport répertorie des informations telles que l'ID de connexion, le nom de famille et le prénom, l'ID de messagerie et dresse la liste des groupes (séparés par une virgule) auxquels l'utilisateur est affecté directement ou indirectement. La version CSV du rapport indique si l'utilisateur est affecté directement ou indirectement à un groupe avec `Yes` ou `No`.

Remarque : Ce rapport n'est pas applicable à Account Reconciliation et Narrative Reporting.

Pour régénérer le rapport sur le groupe d'utilisateurs, procédez comme suit :

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur **Rapport sur le groupe d'utilisateurs**.
3. **Facultatif :** filtrez le rapport. Dans la liste déroulante, sélectionnez **Utilisateurs** ou **Groupes**. Pour obtenir des instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.
4. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter le rapport dans un fichier CSV.
5. Cliquez sur **Annuler** pour fermer le rapport.