# Oracle® Fusion Cloud EPM

## Administration du contrôle d'accès

F28926-23

Oracle Fusion Cloud EPM Administration du contrôle d'accès,

F28926-23



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

Les environnements Oracle Fusion Cloud Enterprise Performance Management et Oracle Fusion Cloud Enterprise Data Management sont sécurisés par plusieurs couches de protection. L'accès est limité aux utilisateurs autorisés grâce à l'accès basé sur les rôles (rôles prédéfinis). Les affectations de rôle prédéfini sont gérées à l'aide de la console Oracle Cloud. Par exemple, pour que l'utilisateur `John Doe` puisse visualiser des rapports appartenant à un environnement de test Planning, il doit disposer du rôle Visualiseur de l'environnement. Pour plus d'informations, reportez-vous à la section Présentation des rôles prédéfinis du *Guide de mise en route pour les administrateurs*.

Pour permettre un contrôle plus précis de l'utilisation des processus métier Cloud EPM ou Cloud EDM, des rôles propres à une application peuvent être affectés aux utilisateurs via Contrôle d'accès. Par exemple, le rôle Administrateur des approbations peut être affecté à un utilisateur ou à un groupe dans une application Planning, ce qui lui permet d'effectuer des activités d'approbation.

L'affectation de rôles au niveau d'une application ne fait que renforcer les droits d'accès de l'utilisateur. Ces rôles d'application ne peuvent pas révoquer ni restreindre les privilèges accordés par des rôles prédéfinis.

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

- **Gestion des groupes**. Reportez-vous à la section Gestion des groupes.
- **Gestion des utilisateurs**. Reportez-vous à la section Affectation d'un utilisateur à plusieurs groupes.
- **Gestion des rôles d'application**. Reportez-vous à la section Gestion des affectations de rôle au niveau application.
- **Rapport sur l'affectation de rôle**. Reportez-vous aux sections suivantes :
  - Génération d'un rapport sur l'affectation de rôle pour un utilisateur ou un groupe
  - Affichage du rapport sur l'affectation de rôle pour l'environnement
- **Rapport sur les connexions utilisateur**. Reportez-vous à la section Affichage du rapport sur les connexions utilisateur.
- **Rapport sur le groupe d'utilisateurs**. Reportez-vous à la section Affichage du rapport sur le groupe d'utilisateurs.

Le **contrôle d'accès** pour Account Reconciliation offre des fonctionnalités spécifiques. Pour plus de détails, reportez-vous aux rubriques suivantes dans le guide *Administration d'Account Reconciliation* :

- Utilisation d'équipes
- Gestion des utilisateurs
- Sécurité de super utilisateur dans Account Reconciliation

**Lien de tutoriel**

Suivez le tutoriel Configuration de la sécurité dans les processus métier Cloud EPM pour en savoir plus sur les couches de sécurité dans les processus métier Cloud EPM, et sur la manière de gérer la sécurité à l'aide du contrôle d'accès et des autorisations d'accès.

# Ouverture du contrôle d'accès

Pour ouvrir Contrôle d'accès, procédez comme suit :

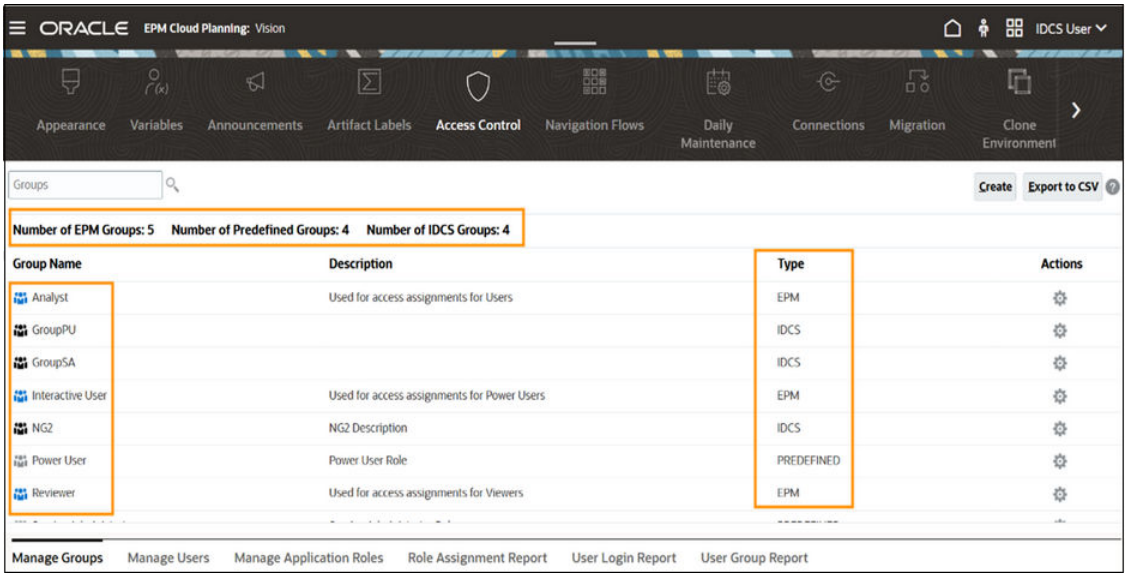
1. Accédez à l'environnement en tant qu'administrateur de service ou qu'utilisateur doté du rôle d'application Contrôle d'accès - Gérer.
2. Exécutez une étape :
   - Cliquez sur  (navigateur), puis sur **Contrôle d'accès**.
   - Cliquez sur **Outils**, puis sur **Contrôle d'accès**.
   - **Narrative Reporting uniquement :** cliquez sur **Contrôle d'accès**.

# Gestion des groupes

Oracle Fusion Cloud Enterprise Performance Management reconnaît trois types de groupe :

- PREDEFINED : ces groupes sont créés automatiquement pour chaque rôle prédéfini. Tous les utilisateurs sont ajoutés à un groupe PREDEFINED en fonction de leur rôle prédéfini (par exemple, Super utilisateur).
- EPM : il s'agit des groupes que vous créez dans le contrôle d'accès. Ils ne peuvent pas être créés dans la console de gestion des identités. Par ailleurs, ils n'y apparaissent pas non plus.
- IDCS : il s'agit des groupes que vous créez dans Oracle Identity Cloud. Ils peuvent être synchronisés avec un fournisseur d'identités (par exemple, Okta ou Azure AD). Ils figurent dans le contrôle d'accès mais vous ne pouvez pas les créer via le contrôle d'accès.

Dans l'onglet **Gérer les groupes**, les groupes sont catégorisés par type et image pour les différentier facilement. Pour savoir comment rechercher un groupe spécifique, reportez-vous à la section Utilisation de la recherche.




### Groupes PREDEFINED

Pour vous permettre de visualiser les affectations des utilisateurs, le contrôle d'accès répertorie les utilisateurs dans les rôles prédéfinis en tant que groupes PREDEFINED.

Remarques importantes :

- Les groupes PREDEFINED peuvent être affectés en tant que membres de groupes EPM.
- Les groupes PREDEFINED ne sont pas modifiables.
  Afin d'afficher un groupe PREDEFINED, sélectionnez **Afficher** sous Actions pour le groupe de votre choix. Vous pouvez voir la liste de tous les utilisateurs Cloud EPM affectés au groupe.

Pour plus d'informations sur les rôles prédéfinis, reportez-vous à la section Présentation des rôles prédéfinis du *Guide de mise en route pour les administrateurs*.

### Groupes EPM

Vous pouvez utiliser les options suivantes de l'écran **Gérer les groupes** pour créer et gérer des groupes EPM.

- Bouton **Créer** : permet de créer un groupe EPM. Reportez-vous à la section Création de groupes EPM.
- Bouton **Exporter dans un fichier CSV** : permet d'exporter des groupes EPM dans un fichier CSV. Reportez-vous à la section Export de groupes Cloud EPM dans un fichier CSV.
- **Modifier** (Action) : permet de modifier le groupe EPM de la ligne sélectionnée dans la liste des groupes. Reportez-vous à la section Modification de groupes EPM.
- **Supprimer** (Action) : permet de supprimer le groupe EPM de la ligne sélectionnée dans la liste des groupes. Reportez-vous à la section Suppression de groupes EPM.

Remarques importantes :

- Les groupes EPM peuvent être affectés en tant que membres à des groupes EPM plus importants.

- Vous ne pouvez pas utiliser le contrôle d'accès pour importer les informations de groupe d'un fichier afin de créer des groupes. Vous pouvez utiliser Migration ou la commande createGroups d'EPM Automate pour importer des groupes.

**Groupes IDCS**

Vous pouvez utiliser des groupes IDCS pour affecter des rôles prédéfinis à plusieurs utilisateurs Cloud EPM. Reportez-vous à Utilisation de groupes IDCS pour affecter des rôles prédéfinis à des utilisateurs dans le guide *Mise en route d'Oracle Enterprise Performance Management Cloud pour les administrateurs*

Remarques importantes :

- Les groupes IDCS ne sont pas modifiables.
  Afin d'afficher un groupe IDCS, sélectionnez **Afficher** sous Actions pour le groupe voulu. Vous pouvez voir la liste de tous les utilisateurs Cloud EPM affectés au groupe.
- Les groupes IDCS peuvent être affectés à des rôles d'application et à des groupes EPM.

> ⚠ **Attention**
>
> Si un groupe IDCS partage son nom avec un groupe EPM ou PREDEFINED, ou si le nom dépasse 256 caractères, il n'apparaît pas dans Contrôle d'accès. Il est essentiel de comprendre que les utilisateurs appartenant à de tels groupes IDCS ne peuvent pas se connecter.

**Dépannage**

Reportez-vous à la section Résolution des problèmes de gestion des utilisateurs, des rôles et des groupes du *Guide des opérations*.

# Création de groupes EPM

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent créer des groupes EPM. Les utilisateurs Oracle Fusion Cloud Enterprise Performance Management et les autres groupes peuvent être membres d'un groupe. Vous ne pouvez pas créer de groupe IDCS ou PREDEFINED à l'aide de cette option.

> ⓘ **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.

      Cloud EPM ne vous permet pas de créer des groupes avec des noms identiques à celui d'un groupe IDCS ou PREDEFINED.

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 de tous types répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **nom de groupe**.

   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 Cloud EPM 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.

      Les utilisateurs répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **connexion utilisateur**.

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

   d. Cliquez sur **Déplacer**.

6. Cliquez sur **Enregistrer**.

7. Cliquez sur **OK**.

## Modification de groupes EPM

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent modifier des propriétés de groupe EPM, 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. Vous ne pouvez pas modifier de groupe IDCS ou PREDEFINED à l'aide de cette option.

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.

   Les groupes de tous types répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **nom de groupe**.

> ⓘ **Remarque**
>
> Les noms de groupe ne peuvent pas contenir plus de 256 caractères. En fonction de la résolution d'écran, les caractères visibles, par exemple, dans la colonne **Groupes disponibles**, peuvent être tronqués.

3. Cliquez sur (Action) dans la ligne correspondant au groupe à modifier, puis sélectionnez **Modifier**.
4. **Facultatif :** modifiez le nom du groupe. La modification du nom de groupe n'influe pas sur les affectations de sécurité effectuées à l'aide du groupe. Vous ne pouvez pas renommer le groupe avec un nom identique à celui d'un groupe IDCS ou PREDEFINED répertorié.
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.

        Les groupes de tous types répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **nom de groupe**.
      - 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.

        Les utilisateurs répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **connexion utilisateur**.
      - 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 de groupes EPM

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent supprimer des groupes EPM. La suppression d'un groupe EPM ne supprime pas ses membres. Vous ne pouvez pas supprimer de groupe IAM ou PREDEFINED à l'aide de cette option.

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.

   Les groupes répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **nom de groupe**.

3. Cliquez sur (Action) dans la ligne correspondant au groupe EPM à supprimer, puis sélectionnez **Supprimer**.
4. Cliquez sur **Oui** pour confirmer la suppression.
5. Cliquez sur **OK**.

## Export de groupes Cloud EPM dans un fichier CSV

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent exporter les noms et descriptions de groupe EPM dans un fichier `Groups.csv` à l'aide de l'option **Exporter dans un fichier CSV**. Cette option ne permet pas d'exporter des groupes PREDEFINED ou IDCS.

L'option **Exporter dans un fichier CSV** est désactivée s'il n'existe aucun groupe EPM Cloud. Au moins un groupe EPM Cloud doit exister dans Contrôle d'accès pour que cette option puisse être utilisée.

1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.

   L'onglet **Gérer les groupes** répertorie tous les groupes disponibles.

2. Cliquez sur **Exporter dans un fichier CSV** pour exporter tous les groupes EPM Cloud.
3. Suivez les instructions qui s'affichent à l'écran pour ouvrir ou enregistrer le fichier `Groups.csv`.

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

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent importer des affectations de groupe EPM 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 Fusion Cloud Enterprise Performance Management 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 être semblable à celui-ci :

```
User Login,First Name,Last Name,Email,Direct,Group

jdoe,John,Doe,jdoe@example.com,Yes,AllRole
```

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 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 Fusion Cloud Enterprise Performance Management peuvent être membres de plusieurs groupes gérés à l'aide du contrôle d'accès. Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent affecter un utilisateur à plusieurs groupes.

> **Remarque**
>
> Un utilisateur peut être membre de 1 000 groupes à la fois au maximum, directement ou indirectement.

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

   Les utilisateurs répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **connexion utilisateur**.
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.

   Les groupes EPM répondant aux critères de recherche sont répertoriés. Par défaut, cette liste est triée par **nom de groupe**.
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. 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`.

L'option de recherche ne prend pas en charge les caractères génériques (*).

> **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.

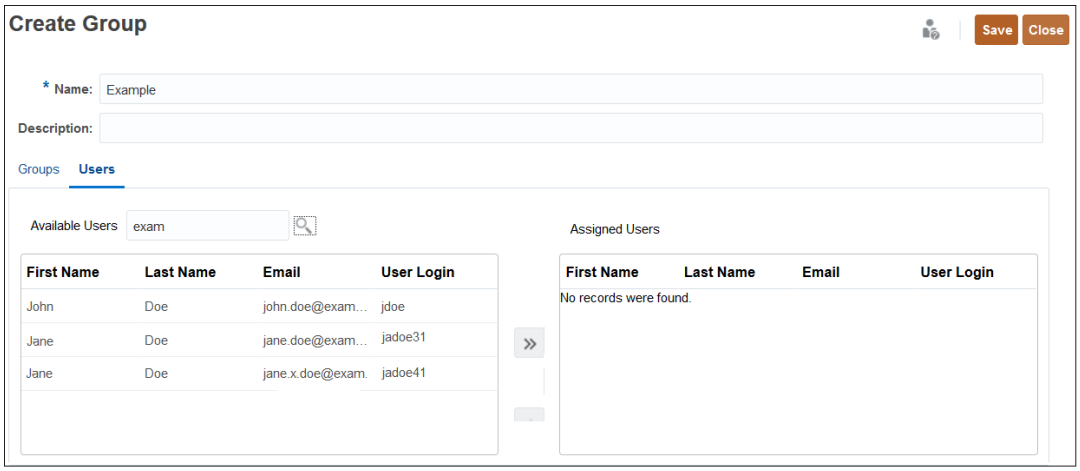
**Pour rechercher des utilisateurs, procédez comme suit :**

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. Par défaut, cette liste est triée par **connexion utilisateur**.

**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. Par défaut, cette liste est triée par **nom 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. Par défaut, cette liste est triée par **connexion utilisateur**.

2

# Gestion des affectations de rôle au niveau application

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

- Account Reconciliation
- Enterprise Profitability and Cost Management
- Financial Consolidation and Close
- FreeForm
- Narrative Reporting
- Oracle Fusion Cloud Enterprise Data Management
- Planning
- Profitability and Cost Management
- Tax Reporting

## Présentation de l'affectation des rôles d'application

Le contrôle d'accès vous permet d'étendre les capacités d'accès des utilisateurs Oracle Fusion Cloud Enterprise Performance Management au-delà de leurs rôles prédéfinis en leur affectant des rôles au niveau de l'application. Ces rôles sont appelés rôles d'application. Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent octroyer des autorisations de données et des rôles propres à une application à des utilisateurs et à des groupes créés et gérés dans Contrôle d'accès.

Par exemple, par défaut, seuls les administrateurs de service et les super utilisateurs peuvent accéder à l'intégration des données. Pour permettre aux utilisateurs dotés du rôle prédéfini Utilisateur ou Visualiseur de participer au processus d'intégration, les administrateurs de service peuvent leur affecter des rôles d'application Intégration des données - Créer.

> **Note**
>
> Les rôles d'application ne peuvent que renforcer les droits d'accès des utilisateurs. Aucun des privilèges octroyés par un rôle prédéfini ne peut être limité. Pour en savoir plus sur les rôles prédéfinis, reportez-vous à la section Présentation des rôles prédéfinis du *Guide de mise en route pour les administrateurs*.

Pour plus d'informations sur les rôles d'application Cloud EPM disponibles et les rôles prédéfinis avec lesquels ils sont mappés, reportez-vous aux sections suivantes :

- Account Reconciliation
- Enterprise Profitability and Cost Management
- Financial Consolidation and Close

- FreeForm
- Narrative Reporting
- Oracle Enterprise Data Management
- Planning
- Profitability and Cost Management
- Tax Reporting

> **Note**
>
> Si vous migrez des applications d'un environnement sur site vers Cloud EPM, reportez-vous à la section Mapping de rôles pour la migration vers Cloud EPM du guide *Administration de Migration*.

**Meilleure pratique pour l'affectation des rôles d'application**

La meilleure pratique recommandée est d'affecter le rôle de niveau le plus bas le plus adapté aux privilèges supplémentaires lorsque cela est nécessaire. Vous trouverez ci-dessous des exemples de situations dans lesquelles vous pourriez avoir besoin d'octroyer des rôles d'application à un utilisateur qui ne disposerait pas de ces privilèges à partir de son rôle prédéfini.

- Vous ajoutez le rôle d'application **Préparateur** à un visualiseur qui doit préparer des rapprochements.
- Vous disposez d'un concepteur de rapports qui travaille uniquement à la conception de rapports et n'utilise pas le reste des fonctionnalités de l'application. Vous pouvez lui octroyer le rôle Visualiseur, puis lui affecter le rôle d'application **Gérer les rapports**.
- Vous autorisez un super utilisateur à gérer les types d'alerte pour pouvoir affecter le rôle d'application **Gérer les types d'alerte**.

> **Note**
>
> L'octroi de privilèges est cumulatif uniquement. Cela signifie que vous pouvez ajouter des privilèges au rôle prédéfini d'un utilisateur, mais que vous ne pouvez pas enlever des privilèges qui sont automatiquement accordés à ce rôle prédéfini.

# Account Reconciliation

Le tableau suivant répertorie et décrit les rôles d'application Account Reconciliation, et les mappe avec des rôles prédéfinis.

> **Note**
>
> Tous les rôles prédéfinis peuvent effectuer une exploration amont vers les données détaillées de l'échange de données en fonction de leur accès aux données dans Account Reconciliation.

**Table 2-1 Rôles d'application Account Reconciliation**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet d'effectuer toutes les activités à l'aide du contrôle d'accès, y compris la gestion des groupes, l'affectation de rôles d'application à des utilisateurs ou à des groupes, la génération de rapports et la consultation des rapports disponibles. | Administrateur de service |
| Contrôle d'accès - Afficher | A l'aide du contrôle d'accès, permet de générer et de consulter des rapports relatifs à la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur, le rapport sur l'affectation de groupe et le rapport sur le groupe d'utilisateurs. Les utilisateurs dotés de ce rôle ne peuvent pas affecter de rôles d'application, gérer de groupes ni modifier de paramètres dans le contrôle d'accès. | Administrateur de service |
| Types d'alerte - Gérer | Permet de gérer les types d'alerte afin de définir une procédure à suivre lorsqu'un problème donné survient. | Administrateur de service |
| Annonces - Gérer | Permet de gérer les annonces que les utilisateurs visualisent sur le panneau Bienvenue. Elles peuvent indiquer des événements à venir, tels qu'une opération de maintenance du système ou l'exécution de jobs. | Administrateur de service |
| Audit - Afficher | Permet d'accéder à tous les détails d'audit. Toutefois, ce rôle d'application n'autorise pas le lancement de la boîte de dialogue Actions de rapprochement car les rapprochements ne font pas partie de sa portée de sécurité. | Administrateur de service |
| Devises - Gérer | Permet de configurer les devises, les types de taux et les catégories de devise. Les utilisateurs dotés de ce rôle peuvent déterminer les codes de devise qui sont actifs dans le système. | Administrateur de service |
| Tableaux de bord - Gérer | Permet de construire et de gérer les tableaux de bord personnalisés. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Configurer la conformité<br>• Ajouter, modifier, dupliquer et supprimer<br>• Importer et exporter | Administrateur de service |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données pour créer des mappings afin d'intégrer des données entre des systèmes source et cible. Les utilisateurs dotés de ce rôle peuvent définir des règles de données avec différentes options d'exécution. | Administrateur de service |

**Table 2-1 (Cont.) Rôles d'application Account Reconciliation**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Intégration des données - Exécuter | Les utilisateurs dotés de ce rôle se servent de l'intégration des données pour exécuter une intégration entre la source et la cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Administrateur de service |
| Chargements de données - Gérer | Permet d'établir des définitions de chargement de données afin de charger des données à l'aide de l'intégration des données et d'enregistrer ces paramètres de chargement de données.<br>Permet de consulter le statut le plus récent des chargements de données et de surveiller le traitement des demandes de modification des utilisateurs. | Administrateur de service |
| Jobs - Afficher | Permet d'afficher les jobs Account Reconciliation et leur statut. | • Super utilisateur<br>• Administrateur de service |
| Types de correspondance - Gérer | Permet de gérer les types de correspondance, les attributs d'ajustement, les attributs de prise en charge, les colonnes de journal et les attributs de groupe. | Administrateur de service |
| Types de correspondance - Afficher | Permet d'afficher les détails des types de correspondance, des attributs d'ajustement, des attributs de prise en charge et des colonnes de journal. | Administrateur de service |
| Migrations - Administrer | Permet d'exporter et d'importer des instantanés et des artefacts à partir de l'application, de créer des applications en migrant des instantanés et de supprimer les applications qui ont été créées. Les utilisateurs dotés de ce rôle peuvent également cloner l'environnement. Toutefois, pour cloner des utilisateurs et des rôles, l'utilisateur cible doit disposer des rôles Administrateur de domaine d'identité et Administrateur de service. En outre, les utilisateurs dotés de ce rôle peuvent afficher et ajuster le fuseau horaire et l'heure de début de la maintenance quotidienne. | Administrateur de service |
| Organisations - Gérer | Permet d'affecter une structure d'unité organisationnelle hiérarchique aux profils et aux rapprochements. | Administrateur de service |
| Périodes - Gérer | Permet de gérer les propriétés de période. Les utilisateurs dotés de ce rôle peuvent également définir le statut des périodes, charger des données et effectuer d'autres opérations sur les périodes existantes. | Administrateur de service |
| Périodes - Afficher | Les utilisateurs dotés de ce rôle peuvent visualiser (accès en lecture uniquement) le nombre de périodes associées aux rapprochements, mais aussi charger des données pour la période. | • Super utilisateur<br>• Administrateur de service |
| Profils - Afficher | Les utilisateurs dotés de ce rôle peuvent accéder aux profils pour lesquels des workflows leur ont été affectés, en fonction des rapprochements qu'ils peuvent voir. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |

**Table 2-1 (Cont.) Rôles d'application Account Reconciliation**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Profils et rapprochements - Gérer | Permet de gérer les profils, les rapprochements et les attributs.<br>Vous pouvez définir la portée de sécurité de ce rôle sur l'écran **Sécurité de super utilisateur**. | • Super utilisateur<br>• Administrateur de service |
| Vues et filtres publics - Gérer | Les filtres déterminent les enregistrements affichés dans les vues de liste et les rapports. Vous pouvez appliquer des filtres aux profils, aux rapprochements ou aux attributs de transaction des rapprochements, en incluant des attributs système, des soldes et des détails de solde. Les utilisateurs dotés de ce rôle peuvent créer des filtres complexes et des logiques déterminant l'ordre d'application des filtres. | Administrateur de service |
| Rapprochement - Commentateur | Permet de visualiser les rapprochements et d'ajouter des commentaires portant sur le rapprochement ou sur ses transactions. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Rapprochement - Préparateur | Les utilisateurs dotés de ce rôle préparent des rapprochements, affectent des panneaux, importent des données pré-mappées et ajoutent des pièces jointes pour soumettre, demander et libérer des rapprochements. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Rapprochement - Réviseur | Les utilisateurs dotés de ce rôle révisent les rapprochements, affectent des panneaux et ajoutent des pièces jointes pour approuver, rejeter, demander et libérer des rapprochements. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Rapports - Gérer | Permet de configurer les paramètres d'application pour afficher des rapports de rapprochement. | Administrateur de service |
| Equipes - Gérer | Les utilisateurs dotés de ce rôle peuvent ajouter, modifier ou enlever des équipes, et gérer les membres des équipes. | • Super utilisateur<br>• Administrateur de service |
| Utilisateurs - Gérer | Les utilisateurs dotés de ce rôle peuvent gérer les membres des équipes. | • Super utilisateur<br>• Administrateur de service |

# Enterprise Profitability and Cost Management

Le tableau suivant répertorie et décrit les rôles d'application Enterprise Profitability and Cost Management, et les mappe avec des rôles prédéfinis.

**Table 2-2 Rôles d'application Enterprise Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet d'effectuer toutes les activités à l'aide du contrôle d'accès, y compris la gestion des groupes, l'affectation de rôles d'application à des utilisateurs ou à des groupes, la génération de rapports et la consultation des rapports disponibles. | Administrateur de service |
| Contrôle d'accès - Afficher | A l'aide du contrôle d'accès, permet de générer et de consulter des rapports relatifs à la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur, le rapport sur l'affectation de groupe et le rapport sur le groupe d'utilisateurs. Les utilisateurs dotés de ce rôle ne peuvent pas affecter de rôles d'application, gérer de groupes ni modifier de paramètres dans le contrôle d'accès. | Administrateur de service |
| Ad hoc - Créer | Permet de créer, d'afficher, de modifier et d'enregistrer des grilles ad hoc. | Super utilisateur |
| Ad hoc - Utilisateur en lecture seule | Permet d'effectuer toutes les fonctions ad hoc mais pas de réécrire dans les grilles ad hoc ni de charger des données à l'aide de Data Management. | Non mappé. Voir la note de bas de page |
| Ad hoc - Utilisateur | Permet d'afficher et de modifier les grilles ad hoc, et d'effectuer des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc. | Utilisateur |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Annonces - Gérer | Permet de gérer les annonces que les utilisateurs visualisent sur le panneau Bienvenue. Elles peuvent indiquer des événements à venir, tels qu'une opération de maintenance du système ou l'exécution de jobs. | Administrateur de service |
| Approbations - Administrer | Permet de résoudre 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 Administrateur de service. Ils peuvent effectuer les tâches suivantes :<br>• Contrôler le processus des approbations<br>• Effectuer des actions sur les unités Planning auxquelles ils ont un accès en écriture<br>• Affecter des propriétaires et des réviseurs pour l'organisation dont ils sont responsables<br>• Modifier la dimension secondaire ou mettre à jour les règles de validation | Administrateur de service |

**Table 2-2 (Cont.) Rôles d'application Enterprise Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Approbations - Affecter les propriétés | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Affecter des propriétaires<br>• Affecter des réviseurs<br>• Indiquer les utilisateurs à avertir | Super utilisateur |
| Approbations - Concevoir le processus | Inclut le rôle Cédant de propriété des approbations. Par ailleurs, permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Modifier les dimensions secondaires et les membres des entités auxquelles l'utilisateur a accès en écriture<br>• Modifier l'affectation de scénario et de version pour une hiérarchie d'unité de planification<br>• Modifier les règles de validation des données des formulaires auxquels l'utilisateur a accès | Non mappé. Voir la note de bas de page |
| Approbations - Superviser | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un 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.<br>• Démarrer et arrêter une unité de planification<br>• Effectuer n'importe quelle action sur une unité de planification | Super utilisateur |
| Audit - Gérer | Permet d'afficher et de supprimer les enregistrements d'audit. | Administrateur de service |
| Audit - Afficher | Permet d'afficher les enregistrements d'audit. | Non mappé. Voir la note de bas de page |
| Calcul - Exécuter | Permet de calculer un modèle sur la page Contrôle de calcul. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Historique des calculs - Supprimer | Permet de supprimer une instance sélectionnée d'un calcul terminé de la page Analyse de calcul. La suppression de l'historique des calculs ne supprime aucune donnée. Elle supprime simplement l'instance enregistrée d'un calcul exécuté. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Historique des calculs - Afficher | Permet d'afficher les calculs terminés de la page Analyse de calcul. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |

**Table 2-2 (Cont.) Rôles d'application Enterprise Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Tableaux de bord - Gérer | Permet de construire et de gérer des tableaux de bord de planification et opérationnels. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des tableaux de bord en fonction des autorisations définies<br>• Importer et exporter des tableaux de bord | Administrateur de service |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données 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. | Super utilisateur |
| Intégration des données - Explorer en amont | Permet d'effectuer une exploration amont vers le système source des données. | • Super utilisateur<br>• Utilisateur |
| Intégration des données - Exécuter | Les utilisateurs dotés de ce rôle se servent de l'intégration des données pour exécuter une intégration entre la source et la cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Super utilisateur |
| Documents - Gérer | Permet de construire et de gérer des documents. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des documents en fonction des autorisations définies<br>• Importer et exporter des documents | Administrateur de service |
| IPM - Gérer | Permet de gérer et de configurer les jobs de gestion intelligente des performances (IPM), notamment les analyses, la prévision automatique et la prévision avancée. Les utilisateurs dotés de ce rôle :<br>• peuvent afficher, modifier et gérer uniquement les jobs qu'ils ont créés ;<br>• ne peuvent pas afficher ni gérer les jobs créés par d'autres utilisateurs. | Administrateur de service |
| Jobs - Gérer | Permet d'afficher et de supprimer des enregistrements de statut de job de n'importe quel utilisateur. | Administrateur de service |

**Table 2-2 (Cont.) Rôles d'application Enterprise Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Jobs - Afficher | Permet à l'utilisateur d'afficher les enregistrements de statut de job de tous les utilisateurs de l'environnement, mais de supprimer uniquement ses propres enregistrements de statut de job. | Non mappé. Voir la note de bas de page |
| Modèle - Créer | Permet de créer un modèle sur la page Modélisation. | • Super utilisateur<br>• Administrateur de service |
| Modèle - Supprimer | Permet de supprimer un modèle sur la page Modélisation. La suppression d'un modèle supprime également toutes les règles du modèle. | Administrateur de service |
| Modèle - Afficher | Permet d'afficher les modèles et les règles associées sur la page Concepteur. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur<br>• Visualiseur |
| Validation du modèle - Exécuter | Permet de valider les modèles sur la page Validation du modèle. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| PDV - Créer | Permet de créer un point de vue sur la page Contrôle de calcul. | • Super utilisateur<br>• Administrateur de service |
| PDV - Supprimer | Permet de supprimer un point de vue sur la page Contrôle de calcul. La suppression d'un point de vue supprime également les données associées, ainsi que la page d'historique des calculs pour ce point de vue. Cette opération enlève également le point de vue de la page Contrôle de calcul. | Administrateur de service |
| Données du PDV - Effacer | Permet d'effacer les données d'un point de vue sur la page Contrôle de calcul sans enlever le point de vue. | • Super utilisateur<br>• Administrateur de service |
| Données du PDV - Copier | Permet de copier les données d'un point de vue vers un autre sur la page Contrôle de calcul. | • Super utilisateur<br>• Administrateur de service |
| Statut du PDV - Modifier | Permet de modifier le statut d'un point de vue dans la boîte de dialogue **Modifier le point de vue** sur la page Contrôle de calcul. Statuts disponibles pour un point de vue : Brouillon, Publié et Archivé. | Administrateur de service |
| Courbe de profit - Créer | Permet de créer des courbes de profit dans l'onglet **Courbes de profit** du cluster d'aide à la décision. | • Super utilisateur<br>• Administrateur de service |
| Courbe de profit - Modifier | Permet de modifier des courbes de profit dans l'onglet **Courbes de profit** du cluster d'aide à la décision. | • Super utilisateur<br>• Administrateur de service |
| Courbe de profit - Exécuter | Permet d'exécuter des courbes de profit dans l'onglet **Courbes de profit** du cluster d'aide à la décision. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur<br>• Visualiseur |

**Table 2-2 (Cont.) Rôles d'application Enterprise Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Rapports - Gérer | Permet de créer et de gérer les artefacts de reporting (rapports, instantanés, liasses et définitions d'éclatement). Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des artefacts de reporting en fonction des autorisations définies.<br>• Importer et exporter des artefacts de reporting. | Administrateur de service |
| Règle - Créer/ Modifier | Permet de créer ou de modifier une règle d'allocation, une règle de calcul personnalisé ou un ensemble de règles sur la page Concepteur. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Règle - Supprimer | Permet de supprimer une règle d'allocation, une règle de calcul personnalisé ou un ensemble de règles sur la page Concepteur. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Equilibrage de règle - Exécuter | Permet d'afficher le rapport d'équilibrage de règle pour voir l'incidence de chaque règle. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Règles - Modifier en masse | Permet d'accéder à l'onglet **Modification en masse** de la page Concepteur pour modifier plusieurs règles à la fois. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Traçage d'allocation - Exécuter | Permet de tracer les montants d'allocation dans l'onglet **Tracer les allocations** du cluster d'aide à la décision. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur<br>• Visualiseur |
| Note de bas de page : ce rôle n'est mappé avec aucun rôle prédéfini, et nécessite d'être affecté à des utilisateurs ou à des groupes pour être activé. | | |

# Financial Consolidation and Close

Le tableau suivant répertorie et décrit les rôles Financial Consolidation and Close pour les applications suivantes, et les mappe avec des rôles prédéfinis :

**Tableau 2-3 Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |

**Tableau 2-3 (suite) Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Ad hoc - Créer | Permet de créer, d'afficher, de modifier et d'enregistrer des grilles ad hoc. | Super utilisateur |
| Ad hoc - Utilisateur en lecture seule | Permet d'effectuer toutes les fonctions ad hoc mais pas de réécrire dans les grilles ad hoc ni de charger des données à l'aide de Data Management. | Non mappé. Voir la note de bas de page |
| Ad hoc - Utilisateur | Permet d'afficher et de modifier les grilles ad hoc, et d'effectuer des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc. | Utilisateur |
| Annonces - Gérer | Permet de construire et de gérer des annonces. Les utilisateurs dotés de ce rôle peuvent ajouter, modifier, dupliquer et supprimer des annonces. | Administrateur de service |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Approbations - Administrer | Permet de résoudre 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 Administrateur de service. Ils peuvent effectuer les tâches suivantes :<br>• Contrôler le processus des approbations<br>• Effectuer des actions sur les unités Planning auxquelles ils ont un accès en écriture<br>• Affecter des propriétaires et des réviseurs pour l'organisation dont ils sont responsables<br>• Modifier la dimension secondaire ou mettre à jour les règles de validation | Administrateur de service |
| Approbations - Affecter les propriétés | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Affecter des propriétaires<br>• Affecter des réviseurs<br>• Indiquer les utilisateurs à avertir | Super utilisateur |

**Tableau 2-3 (suite) Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Approbations - Concevoir le processus | Inclut le rôle Cédant de propriété des approbations. Par ailleurs, permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Modifier les dimensions secondaires et les membres des entités auxquelles l'utilisateur a accès en écriture<br>• Modifier l'affectation de scénario et de version pour une hiérarchie d'unité de planification<br>• Modifier les règles de validation des données des formulaires auxquels l'utilisateur a accès | Non mappé. Voir la note de bas de page |
| Approbations - Superviser | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un 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.<br>• Démarrer et arrêter une unité de planification<br>• Effectuer n'importe quelle action sur une unité de planification | Super utilisateur |
| Audit - Gérer | Permet d'afficher et de supprimer les enregistrements d'audit. | Administrateur de service |
| Audit - Afficher | Permet d'afficher les enregistrements d'audit. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Approuver | Permet d'approuver un journal de consolidation soumis pour approbation ou de rejeter un journal soumis. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Imputer automatiquement après approbation | Permet l'imputation automatique d'un journal de consolidation une fois que l'approbateur l'a approuvé. L'utilisateur qui a approuvé le journal sera également indiqué comme l'ayant imputé. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Créer | Permet de créer, de modifier et de supprimer des journaux de consolidation et des modèles de journal de consolidation. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Gérer les périodes | Permet d'ouvrir des périodes pour les journaux de consolidation ou de fermer des périodes de journal. Si la période contient des journaux approuvés ou des journaux extournés automatiquement dont l'imputation a été annulée, vous ne pouvez pas la fermer. Si vous choisissez de fermer une période qui contient des journaux en cours d'utilisation ou soumis, un message d'avertissement apparaît et indique que des journaux non imputés ont été trouvés pour la période, mais que vous pouvez la fermer. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Imputer | Permet d'imputer un journal de consolidation terminé ou soumis et approuvé. Vous devez d'abord ouvrir la période de chaque scénario vers lequel des journaux de consolidation doivent être imputés. | Non mappé. Voir la note de bas de page |

**Tableau 2-3 (suite) Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Journaux de consolidation - Soumettre | Permet de soumettre un journal de consolidation pour approbation ou de rejeter un journal de consolidation présentant le statut Terminé. | Non mappé. Voir la note de bas de page |
| Journaux de consolidation - Annuler l'imputation | Permet d'annuler l'imputation d'un journal de consolidation. Vous devez disposer d'un accès en écriture aux membres du journal. | Non mappé. Voir la note de bas de page |
| Tableaux de bord - Gérer | Permet de construire et de gérer tous les tableaux de bord, y compris les tableaux de bord opérationnels. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des tableaux de bord<br>• Importer et exporter des tableaux de bord | • Administrateur de service<br>• Super utilisateur |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données 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. | Super utilisateur |
| Intégration des données - Explorer en amont | Permet d'effectuer une exploration amont vers le système source des données. | • Super utilisateur<br>• Utilisateur |
| Intégration des données - Exécuter | Les utilisateurs dotés de ce rôle se servent de l'intégration des données pour exécuter une intégration entre la source et la cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Super utilisateur |
| Documents - Gérer | Permet de construire et de gérer des documents. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des documents en fonction des autorisations définies<br>• Importer et exporter des documents | Administrateur de service |

**Tableau 2-3 (suite) Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| IPM - Gérer | Permet de gérer et de configurer les jobs de gestion intelligente des performances (IPM), notamment les analyses, la prévision automatique et la prévision avancée. Les utilisateurs dotés de ce rôle :<br>• peuvent afficher, modifier et gérer uniquement les jobs qu'ils ont créés ;<br>• ne peuvent pas afficher ni gérer les jobs créés par d'autres utilisateurs. | Administrateur de service |
| Jobs - Gérer | Permet d'afficher et de supprimer des enregistrements de statut de job de n'importe quel utilisateur. | Administrateur de service |
| Jobs - Afficher | Permet à l'utilisateur d'afficher les enregistrements de statut de job de tous les utilisateurs de l'environnement, mais de supprimer uniquement ses propres enregistrements de statut de job. | Non mappé. Voir la note de bas de page |
| Rapports - Gérer | Permet de créer et de gérer les artefacts de reporting (rapports, instantanés, liasses et définitions d'éclatement). Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des artefacts de reporting en fonction des autorisations définies.<br>• Importer et exporter des artefacts de reporting. | Administrateur de service |
| Liste des tâches - Gérer l'accès | Permet d'affecter des tâches à d'autres utilisateurs. | Super utilisateur |
| Task Manager - Approbateur | Peut être un approbateur sur des tâches Task Manager. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Task Manager - Artefacts - Gérer | Permet de gérer tous les artefacts Task Manager, tels que les alertes, les devises et l'organisation. | Administrateur de service |
| Task Manager - Personne affectée | Peut être une personne affectée sur des tâches Task Manager. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Task Manager - Audit - Afficher | Permet de consulter les informations d'historique d'audit. | Administrateur de service |
| Task Manager - Rapports personnalisés - Gérer | Permet de concevoir des rapports personnalisés. | Administrateur de service |
| Task Manager - Tableaux de bord opérationnels - Gérer | Permet de configurer un tableau de bord opérationnel. | Administrateur de service |
| Task Manager - Vues et filtres publics - Gérer | Permet de publier les filtres et les vues pour les rendre accessibles à tous les utilisateurs. | • Super utilisateur<br>• Administrateur de service |

**Tableau 2-3 (suite) Rôles d'application Financial Consolidation and Close**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Task Manager - Paramètres et services système - Gérer | Permet de définir les services système et les paramètres système d'une application. | Administrateur de service |
| Task Manager - Tâches - Gérer | Permet de concevoir et de gérer les tâches, les modèles et les planifications. | • Super utilisateur<br>• Administrateur de service |
| Task Manager - Utilisateurs et équipes - Gérer | Permet de gérer les utilisateurs et les équipes. | • Super utilisateur<br>• Administrateur de service |
| Note de bas de page : ce rôle n'est mappé avec aucun rôle prédéfini, et nécessite d'être affecté à des utilisateurs ou à des groupes pour être activé. | | |

# FreeForm

Le tableau suivant répertorie et décrit les rôles d'application FreeForm, et les mappe avec des rôles prédéfinis.

> **Note**
>
> Les rôles d'application qui ne sont mappés avec aucun rôle prédéfini nécessitent des affectations individuelles à des utilisateurs ou à des groupes. Sans ces affectations, les utilisateurs ne peuvent pas effectuer les activités liées à leurs rôles d'application. Par exemple, le rôle *Ad hoc - Utilisateur en lecture seule*, qui n'est associé à aucun rôle prédéfini dans le tableau ci-dessous, doit être explicitement octroyé à un utilisateur pour activer ses fonctionnalités. Cette fonctionnalité n'est pas automatiquement incluse dans les rôles prédéfinis.

**Table 2-4 Rôles d'application FreeForm**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Ad hoc - Créer | Permet de créer, d'afficher, de modifier et d'enregistrer des grilles ad hoc. | Super utilisateur |
| Ad hoc - Utilisateur en lecture seule | Permet d'effectuer toutes les fonctions ad hoc mais pas de réécrire dans les grilles ad hoc ni de charger des données à l'aide de Data Management. | Non mappé. Voir la note de bas de page |

**Table 2-4 (Cont.) Rôles d'application FreeForm**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Ad hoc - Utilisateur | Permet d'afficher et de modifier les grilles ad hoc, et d'effectuer des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc. | Utilisateur |
| Annonces - Gérer | Permet de construire et de gérer des annonces. Les utilisateurs dotés de ce rôle peuvent ajouter, modifier, dupliquer et supprimer des annonces. | Administrateur de service |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Audit - Gérer | Permet d'afficher et de supprimer les enregistrements d'audit. | Administrateur de service |
| Audit - Afficher | Permet d'afficher les enregistrements d'audit. | Non mappé. Voir la note de bas de page |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données 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. | Super utilisateur |
| Intégration des données - Explorer en amont | Permet d'effectuer une exploration amont vers le système source des données. | • Super utilisateur<br>• Utilisateur |
| Intégration des données - Exécuter | Les utilisateurs dotés de ce rôle se servent de l'intégration des données pour exécuter une intégration entre la source et la cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Super utilisateur |
| Tableaux de bord - Gérer | Permet de construire et de gérer des tableaux de bord de planification et opérationnels. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des tableaux de bord en fonction des autorisations définies<br>• Importer et exporter des tableaux de bord | Administrateur de service |

**Table 2-4 (Cont.) Rôles d'application FreeForm**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Documents - Gérer | Permet de construire et de gérer des documents. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des documents en fonction des autorisations définies<br>• Importer et exporter des documents | Administrateur de service |
| IPM - Gérer | Permet de gérer et de configurer les jobs de gestion intelligente des performances (IPM), notamment les analyses, la prévision automatique et la prévision avancée. Les utilisateurs dotés de ce rôle :<br>• peuvent afficher, modifier et gérer uniquement les jobs qu'ils ont créés ;<br>• ne peuvent pas afficher ni gérer les jobs créés par d'autres utilisateurs. | Administrateur de service |
| Jobs - Gérer | Permet d'afficher et de supprimer des enregistrements de statut de job de n'importe quel utilisateur. | Administrateur de service |
| Jobs - Afficher | Permet à l'utilisateur d'afficher les enregistrements de statut de job de tous les utilisateurs de l'environnement, mais de supprimer uniquement ses propres enregistrements de statut de job. | Non mappé. Voir la note de bas de page |
| Rapports - Gérer | Permet de créer et de gérer les artefacts de reporting (rapports, instantanés, liasses et définitions d'éclatement). Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des artefacts de reporting en fonction des autorisations définies.<br>• Importer et exporter des artefacts de reporting. | Administrateur de service |
| Liste des tâches - Gérer l'accès | Permet d'affecter des tâches à d'autres utilisateurs. | Super utilisateur |

Note de bas de page : ce rôle n'est mappé avec aucun rôle prédéfini, et nécessite d'être affecté à des utilisateurs ou à des groupes pour être activé.

# Narrative Reporting

Le tableau suivant répertorie et décrit les rôles d'application Narrative Reporting, et les mappe avec des rôles prédéfinis.

**Table 2-5 Rôles d'application Narrative Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |

**Table 2-5 (Cont.) Rôles d'application Narrative Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Bibliothèque - Administrer | Permet de créer des dossiers, y compris des dossiers de niveau racine. | • Administrateur de bibliothèque<br>• Super utilisateur<br>• Administrateur de service |
| Rapport - Administrer | Permet de créer des packages de rapports, des rapports, des liasses et des définitions d'éclatement. | • Super utilisateur<br>• Administrateur de rapport<br>• Administrateur de service |

# Oracle Enterprise Data Management

Le tableau suivant répertorie et décrit les rôles d'application Oracle Enterprise Data Management, et les mappe avec des rôles prédéfinis.

**Table 2-6 Rôles d'application Oracle Enterprise Data Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Application - Créer | Permet d'inscrire des applications dans Oracle Enterprise Data Management. 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. | Administrateur de service |
| Audit | Permet de consulter les informations liées à l'audit telles que l'historique des transactions et les demandes de modification de données dans Oracle Enterprise Data Management. | Administrateur de service |

**Table 2-6 (Cont.) Rôles d'application Oracle Enterprise Data Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Migrations - Administrer | Permet d'exporter et d'importer des instantanés et des artefacts à partir de l'application, de créer des applications en migrant des instantanés et de supprimer les applications qui ont été créées. Les utilisateurs dotés de ce rôle peuvent également cloner l'environnement. Toutefois, pour cloner des utilisateurs et des rôles, l'utilisateur cible doit disposer des rôles Administrateur de domaine d'identité et Administrateur de service. En outre, les utilisateurs dotés de ce rôle peuvent afficher et ajuster le fuseau horaire et l'heure de début de la maintenance quotidienne. | Administrateur de service |
| Vues - Créer | Les utilisateurs dotés de ce rôle peuvent créer des vues pour employer des métadonnées. Etant les propriétaires par défaut, ils peuvent octroyer l'autorisation d'accéder aux vues à d'autres utilisateurs également. Ils conservent le privilège de modifier ou de supprimer les vues. | Administrateur de service |

# Planning

Le tableau suivant répertorie et décrit les rôles d'application Planning, et les mappe avec des rôles prédéfinis. Les types d'application Planning sont les suivants : Personnalisé, FreeForm, Modules Planning, Prévision de trésorerie prédictive, Strategic Workforce Planning et Sales Planning.

**Table 2-7 Rôles d'application Planning**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Ad hoc - Créer | Permet de créer, d'afficher, de modifier et d'enregistrer des grilles ad hoc. | Super utilisateur |
| Ad hoc - Utilisateur en lecture seule | Permet d'effectuer toutes les fonctions ad hoc mais pas de réécrire dans les grilles ad hoc ni de charger des données à l'aide de Data Management. | Non mappé. Voir la note de bas de page |
| Ad hoc - Utilisateur | Permet d'afficher et de modifier les grilles ad hoc, et d'effectuer des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc. | Utilisateur |

**Table 2-7 (Cont.) Rôles d'application Planning**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Annonces - Gérer | Permet de construire et de gérer des annonces. Les utilisateurs dotés de ce rôle peuvent ajouter, modifier, dupliquer et supprimer des annonces. | Administrateur de service |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Approbations - Administrer | Permet de résoudre 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 Administrateur de service. Ils peuvent effectuer les tâches suivantes :<br>• Contrôler le processus des approbations<br>• Effectuer des actions sur les unités Planning auxquelles ils ont un accès en écriture<br>• Affecter des propriétaires et des réviseurs pour l'organisation dont ils sont responsables<br>• Modifier la dimension secondaire ou mettre à jour les règles de validation | Administrateur de service |
| Approbations - Affecter les propriétés | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Affecter des propriétaires<br>• Affecter des réviseurs<br>• Indiquer les utilisateurs à avertir | Super utilisateur |
| Approbations - Concevoir le processus | Inclut le rôle Cédant de propriété des approbations. Par ailleurs, permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Modifier les dimensions secondaires et les membres des entités auxquelles l'utilisateur a accès en écriture<br>• Modifier l'affectation de scénario et de version pour une hiérarchie d'unité de planification<br>• Modifier les règles de validation des données des formulaires auxquels l'utilisateur a accès | Non mappé. Voir la note de bas de page |
| Approbations - Superviser | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un 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.<br>• Démarrer et arrêter une unité de planification<br>• Effectuer n'importe quelle action sur une unité de planification | Super utilisateur |

**Table 2-7 (Cont.) Rôles d'application Planning**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Audit - Gérer | Permet d'afficher et de supprimer les enregistrements d'audit. | Administrateur de service |
| Audit - Afficher | Permet d'afficher les enregistrements d'audit. | Non mappé. Voir la note de bas de page |
| Tableaux de bord - Gérer | Permet de construire et de gérer des tableaux de bord de planification et opérationnels. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des tableaux de bord en fonction des autorisations définies<br>• Importer et exporter des tableaux de bord | Administrateur de service |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données 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. | Super utilisateur |
| Intégration des données - Explorer en amont | Permet d'effectuer une exploration amont vers le système source des données. | • Super utilisateur<br>• Utilisateur |
| Intégration des données - Exécuter | Permet d'utiliser l'intégration des données pour exécuter une intégration entre les systèmes source et cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Super utilisateur |
| Documents - Gérer | Permet de construire et de gérer des documents. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des documents en fonction des autorisations définies<br>• Importer et exporter des documents | Administrateur de service |

**Table 2-7 (Cont.) Rôles d'application Planning**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| IPM - Gérer | Permet de gérer et de configurer les jobs de gestion intelligente des performances (IPM), notamment les analyses, la prévision automatique et la prévision avancée. Les utilisateurs dotés de ce rôle :<br>• peuvent afficher, modifier et gérer uniquement les jobs qu'ils ont créés ;<br>• ne peuvent pas afficher ni gérer les jobs créés par d'autres utilisateurs. | Administrateur de service |
| Jobs - Gérer | Permet d'afficher et de supprimer des enregistrements de statut de job de n'importe quel utilisateur. | Administrateur de service |
| Jobs - Afficher | Permet à l'utilisateur d'afficher les enregistrements de statut de job de tous les utilisateurs de l'environnement, mais de supprimer uniquement ses propres enregistrements de statut de job. | Non mappé. Voir la note de bas de page |
| Rapports - Gérer | Permet de créer et de gérer les artefacts de reporting (rapports, instantanés, liasses et définitions d'éclatement). Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des artefacts de reporting en fonction des autorisations définies.<br>• Importer et exporter des artefacts de reporting. | Administrateur de service |
| Liste des tâches - Gérer l'accès | Permet d'affecter des tâches à d'autres utilisateurs. | Super utilisateur |
| Task Manager - Approbateur | Peut être un approbateur sur des tâches Task Manager. | • Administrateur de service<br>• Super utilisateur<br>• Utilisateur |
| Task Manager - Artefacts - Gérer | Permet de gérer tous les artefacts Task Manager, tels que les alertes, les devises et l'organisation. | Administrateur de service |
| Task Manager - Personne affectée | Peut être une personne affectée sur des tâches Task Manager. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Task Manager - Audit - Afficher | Permet de consulter les informations d'historique d'audit. | Administrateur de service |
| Task Manager - Rapports personnalisés - Gérer | Permet de concevoir des rapports personnalisés. | Administrateur de service |
| Task Manager - Tableaux de bord opérationnels - Gérer | Permet de configurer un tableau de bord opérationnel. | Administrateur de service |
| Task Manager - Vues et filtres publics - Gérer | Permet de publier les filtres et les vues pour les rendre accessibles à tous les utilisateurs. | • Super utilisateur<br>• Administrateur de service |

**Table 2-7 (Cont.) Rôles d'application Planning**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Task Manager - Paramètres et services système - Gérer | Permet de définir les services système et les paramètres système d'une application. | Administrateur de service |
| Task Manager - Tâches - Gérer | Permet de concevoir et de gérer les tâches, les modèles et les planifications. | • Super utilisateur<br>• Administrateur de service |
| Task Manager - Utilisateurs et équipes - Gérer | Permet de gérer les utilisateurs et les équipes. | • Super utilisateur<br>• Administrateur de service |
| Note de bas de page : ce rôle n'est mappé avec aucun rôle prédéfini, et nécessite d'être affecté à des utilisateurs ou à des groupes pour être activé. | | |

# Profitability and Cost Management

Le tableau suivant répertorie et décrit les rôles d'application Profitability and Cost Management, et les mappe avec des rôles prédéfinis.

**Table 2-8 Rôles d'application Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet de gérer des groupes, d'affecter des rôles d'application à un utilisateur ou à un groupe, et de générer des rapports sur la sécurité utilisateur. | Administrateur de service |
| Contrôle d'accès - Afficher | Permet de consulter des rapports sur la sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs, mais ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |

**Table 2-8 (Cont.) Rôles d'application Profitability and Cost Management**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Migrations - Administrer | Permet d'exporter et d'importer des instantanés et des artefacts à partir de l'application, de créer des applications en migrant des instantanés et de supprimer les applications qui ont été créées. Les utilisateurs dotés de ce rôle peuvent également cloner l'environnement. Toutefois, pour cloner des utilisateurs et des rôles, l'utilisateur cible doit disposer des rôles Administrateur de domaine d'identité et Administrateur de service. En outre, les utilisateurs dotés de ce rôle peuvent afficher et ajuster le fuseau horaire et l'heure de début de la maintenance quotidienne. | Administrateur de service |

# Tax Reporting

Le tableau suivant répertorie et décrit les rôles d'application Tax Reporting, et les mappe avec des rôles prédéfinis.

> **Note**
>
> Les rôles d'application qui ne sont mappés avec aucun rôle prédéfini nécessitent des affectations individuelles à des utilisateurs ou à des groupes. Sans ces affectations, les utilisateurs ne peuvent pas effectuer les activités liées à leurs rôles d'application. Par exemple, le rôle *Ad hoc - Utilisateur en lecture seule*, qui n'est associé à aucun rôle prédéfini dans le tableau ci-dessous, doit être explicitement octroyé à un utilisateur pour activer ses fonctionnalités. Cette fonctionnalité n'est pas automatiquement incluse dans les rôles prédéfinis.

**Table 2-9 Rôles d'application Tax Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Contrôle d'accès - Gérer | Permet d'effectuer toutes les activités à l'aide du contrôle d'accès, y compris la gestion des groupes, l'affectation de rôles d'application à des utilisateurs ou à des groupes, la génération de rapports et la consultation des rapports disponibles. | Administrateur de service |
| Contrôle d'accès - Afficher | A l'aide du contrôle d'accès, permet de consulter les rapports de sécurité utilisateur, tels que le rapport sur l'affectation de rôle, le rapport sur les connexions utilisateur et le rapport sur le groupe d'utilisateurs. Toutefois, ne permet pas d'affecter des rôles d'application, de gérer des groupes, ni d'effectuer toute autre opération de mise à jour dans le contrôle d'accès. | Administrateur de service |
| Ad hoc - Créer | Permet de créer, d'afficher, de modifier et d'enregistrer des grilles ad hoc. | Super utilisateur |

**Table 2-9 (Cont.) Rôles d'application Tax Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Ad hoc - Utilisateur en lecture seule | Permet d'effectuer toutes les fonctions ad hoc mais pas de réécrire dans les grilles ad hoc ni de charger des données à l'aide de Data Management. | Non mappé. Voir la note de bas de page |
| Ad hoc - Utilisateur | Permet d'afficher et de modifier les grilles ad hoc, et d'effectuer des opérations ad hoc. Les utilisateurs ad hoc ne peuvent pas enregistrer de grilles ad hoc. | Utilisateur |
| Annonces - Gérer | Permet de gérer les annonces que les utilisateurs visualisent sur le panneau Bienvenue. Elles peuvent indiquer des événements à venir, tels qu'une opération de maintenance du système ou l'exécution de jobs. | Super utilisateur |
| Application - Allouer en masse | Permet d'exécuter des règles d'allocation en masse dans des grilles de formulaire. | Administrateur de service |
| Approbations - Administrer | Permet de résoudre 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 Administrateur de service. Ils peuvent effectuer les tâches suivantes :<br>• Contrôler le processus des approbations<br>• Effectuer des actions sur les unités Planning auxquelles ils ont un accès en écriture<br>• Affecter des propriétaires et des réviseurs pour l'organisation dont ils sont responsables<br>• Modifier la dimension secondaire ou mettre à jour les règles de validation | Administrateur de service |
| Approbations - Affecter les propriétés | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Affecter des propriétaires<br>• Affecter des réviseurs<br>• Indiquer les utilisateurs à avertir | Super utilisateur |
| Approbations - Concevoir le processus | Inclut le rôle Cédant de propriété des approbations. Par ailleurs, permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un accès en écriture :<br>• Modifier les dimensions secondaires et les membres des entités auxquelles l'utilisateur a accès en écriture<br>• Modifier l'affectation de scénario et de version pour une hiérarchie d'unité de planification<br>• Modifier les règles de validation des données des formulaires auxquels l'utilisateur a accès | Non mappé. Voir la note de bas de page |

**Table 2-9 (Cont.) Rôles d'application Tax Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Approbations - Superviser | Permet d'effectuer les tâches suivantes pour tout membre de la hiérarchie d'unités de planification pour lequel l'utilisateur dispose d'un 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.<br>• Démarrer et arrêter une unité de planification<br>• Effectuer n'importe quelle action sur une unité de planification | Super utilisateur |
| Audit - Gérer | Permet d'afficher et de supprimer les enregistrements d'audit. | Administrateur de service |
| Audit - Afficher | Permet d'afficher les enregistrements d'audit. | Non mappé. Voir la note de bas de page |
| Tableaux de bord - Gérer | Permet de construire et de gérer les tableaux de bord personnalisés. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Configurer la conformité<br>• Ajouter, modifier, dupliquer et supprimer<br>• Importer et exporter | Administrateur de service |
| Intégration des données - Administrateur | Permet d'effectuer toutes les activités fonctionnelles dans l'intégration des données. Les utilisateurs dotés de ce rôle créent, effectuent et exécutent les opérations suivantes :<br>• Intégrations entre systèmes source et cible<br>• Activités de pipeline<br>• Extraction et transformation des données et des métadonnées des sources sur site à l'aide de l'agent d'intégration EPM | Administrateur de service |
| Intégration des données - Créer | Permet d'utiliser l'intégration des données 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. | Super utilisateur |
| Intégration des données - Explorer en amont | Permet d'effectuer une exploration amont vers le système source des données. | • Super utilisateur<br>• Utilisateur |
| Intégration des données - Exécuter | Les utilisateurs dotés de ce rôle se servent de l'intégration des données pour exécuter une intégration entre la source et la cible.<br>Si les utilisateurs sont dotés uniquement de ce rôle et qu'ils ne sont ni super utilisateurs ni administrateurs de service, ils peuvent également consulter les détails de l'intégration mais ne peuvent pas apporter de modifications. | Super utilisateur |

**Table 2-9 (Cont.) Rôles d'application Tax Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Documents - Gérer | Permet de construire et de gérer des documents. Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des documents en fonction des autorisations définies sur les documents<br>• Importer et exporter des documents | Administrateur de service |
| IPM - Gérer | Permet de gérer et de configurer les jobs de gestion intelligente des performances (IPM), notamment les analyses, la prévision automatique et la prévision avancée. Les utilisateurs dotés de ce rôle :<br>• peuvent afficher, modifier et gérer uniquement les jobs qu'ils ont créés ;<br>• ne peuvent pas afficher ni gérer les jobs créés par d'autres utilisateurs. | Administrateur de service |
| Jobs - Gérer | Permet d'afficher et de supprimer des enregistrements de statut de job de n'importe quel utilisateur. | Administrateur de service |
| Jobs - Afficher | Permet à l'utilisateur d'afficher les enregistrements de statut de job de tous les utilisateurs de l'environnement, mais de supprimer uniquement ses propres enregistrements de statut de job. | Non mappé. Voir la note de bas de page |
| Rapports - Gérer | Permet de créer et de gérer les artefacts de reporting (rapports, instantanés, liasses et définitions d'éclatement). Les utilisateurs dotés de ce rôle peuvent effectuer les opérations suivantes :<br>• Ajouter, modifier, dupliquer et supprimer des artefacts de reporting en fonction des autorisations définies.<br>• Importer et exporter des artefacts de reporting. | Administrateur de service |
| Liste des tâches - Gérer l'accès | Permet d'affecter des tâches à d'autres utilisateurs. | Super utilisateur |
| Task Manager - Approbateur | Peut être un approbateur sur des tâches Task Manager. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Task Manager - Artefacts - Gérer | Permet de gérer tous les artefacts Task Manager, tels que les alertes, les devises et l'organisation. | Administrateur de service |
| Task Manager - Personne affectée | Peut être une personne affectée sur des tâches Task Manager. | • Super utilisateur<br>• Administrateur de service<br>• Utilisateur |
| Task Manager - Audit - Afficher | Permet de consulter les informations d'historique d'audit. | Administrateur de service |
| Task Manager - Rapports personnalisés - Gérer | Permet de concevoir les rapports personnalisés. | Administrateur de service |

**Table 2-9 (Cont.) Rôles d'application Tax Reporting**

| Rôle d'application | Description | Inclus dans ce rôle prédéfini |
|---|---|---|
| Task Manager - Tableaux de bord opérationnels - Gérer | Permet de configurer le tableau de bord. | Administrateur de service |
| Task Manager - Vues et filtres publics - Gérer | Permet de publier les filtres et les vues pour les rendre accessibles à tous les utilisateurs. | • Super utilisateur<br>• Administrateur de service |
| Task Manager - Paramètres et services système - Gérer | Permet de définir les services système et les paramètres système d'une application. | Administrateur de service |
| Task Manager - Tâches - Gérer | Permet de concevoir et de gérer les tâches, les modèles et les planifications. | • Super utilisateur<br>• Administrateur de service |
| Task Manager - Utilisateurs et équipes - Gérer | Permet de gérer les utilisateurs et les équipes. | • Super utilisateur<br>• Administrateur de service |

Note de bas de page : ce rôle n'est mappé avec aucun rôle prédéfini, et nécessite d'être affecté à des utilisateurs ou à des groupes pour être activé.

# Affectation de rôles d'application à un groupe ou à un utilisateur

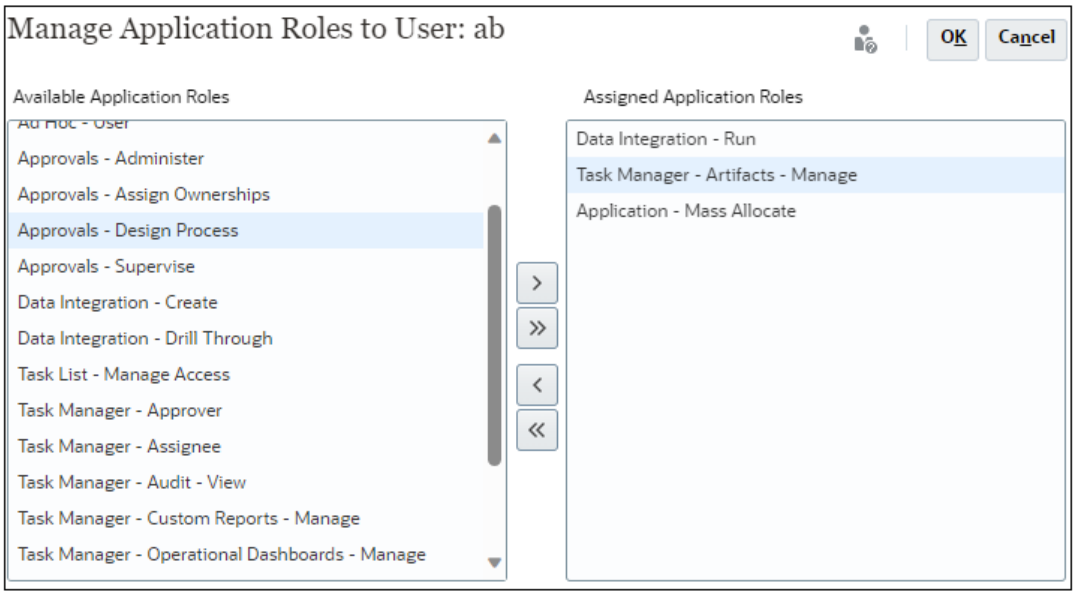
Lors de ce processus, les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent affecter ou annuler l'affectation des rôles d'application aux groupes EPM et IDCS ainsi qu'aux utilisateurs disposant d'un rôle prédéfini. Ils peuvent également s'affecter des rôles d'application.

Pour plus d'informations sur les groupes et les utilisateurs affectés à des groupes, reportez-vous à la section Gestion des groupes.

Pour affecter ou annuler l'affectation des rôles d'application à un groupe ou à un utilisateur, procédez comme suit :

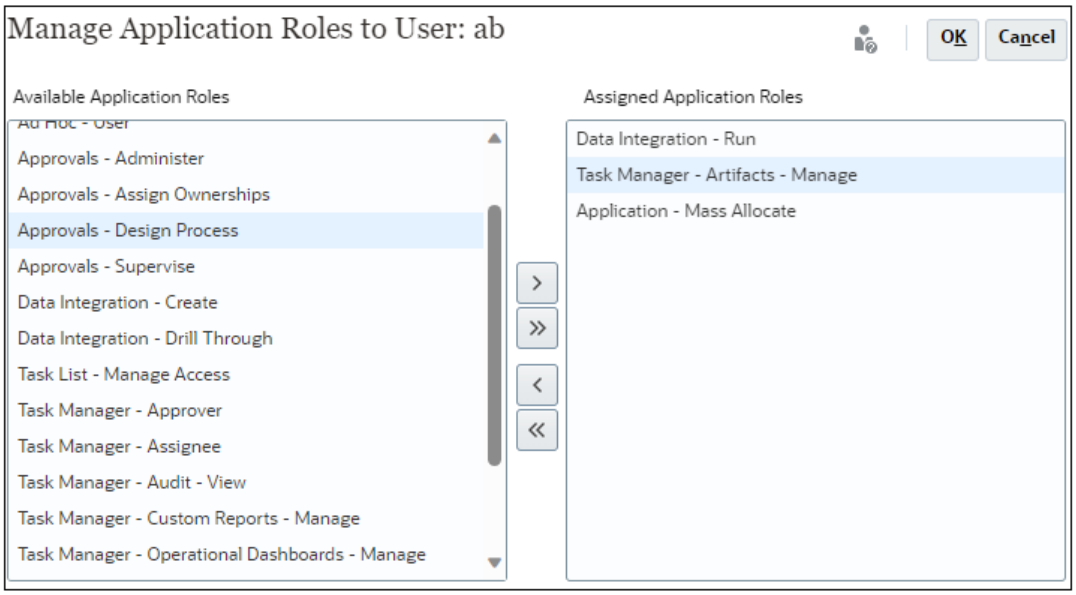
1. Ouvrez **Contrôle d'accès**. Reportez-vous à la section Ouverture du contrôle d'accès.
2. Cliquez sur l'onglet **Gérer les rôles d'application**.
3. Recherchez un utilisateur ou un groupe. Dans la liste déroulante, sélectionnez **Utilisateurs** ou **Groupes**. Pour plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

   Les utilisateurs ou les groupes (EPM ou IDCS) répondant aux critères de recherche sont répertoriés. Par défaut, la liste est triée par **connexion utilisateur**, puis par **nom de groupe** (pour les recherches de groupe).
4. Cliquez sur l'icône (**Actions**) correspondant à l'utilisateur ou au groupe, puis sélectionnez **Gérer les rôles**.
5. Pour affecter un rôle d'application à l'utilisateur ou au groupe, sélectionnez le rôle dans la liste des **rôles d'application disponibles**, puis cliquez sur la flèche orientée vers la droite.




Pour connaître les rôles d'application applicables à chaque processus métier, reportez-vous à la section Gestion des affectations de rôle au niveau application.

6. Si vous voulez annuler l'affectation d'un rôle d'application, sélectionnez-le dans la liste des **rôles d'application affectés**, puis cliquez sur la flèche orientée vers la gauche.




7. Cliquez sur **OK** pour terminer l'affectation de rôles d'application à l'utilisateur ou au groupe.
8. Cliquez sur **OK** à nouveau pour revenir à l'onglet **Gérer les rôles d'application**.

3

# Génération de rapports

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent générer les rapports ci-après pour analyser et gérer les affectations de rôle :

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

> **Remarque**
>
> Ces rapports sur le contrôle d'accès affichent uniquement les utilisateurs actifs. Les utilisateurs qui sont inactifs ou ont été enlevés d'IAM n'apparaissent pas dans les rapports.

### Fuseau horaire des rapports

L'heure de génération du rapport affichée dans les rapports reflète le fuseau horaire local du navigateur de l'utilisateur (en fonction de l'horloge système).

### 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 les utilisateurs sont affectés ne sont pas répertoriés 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.

### Dépannage

Reportez-vous à la section Résolution des problèmes de rapports du *Guide des opérations*.

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

Le rapport sur l'affectation de rôle permet de suivre l'accès utilisateur à des fins de reporting de conformité.

Ce rapport montre tous les utilisateurs actifs auxquels un rôle prédéfini a été affecté. Les utilisateurs désactivés ne figurent pas dans ce rapport. Les groupes IDCS ou EPM auxquels appartient un utilisateur ne sont pas répertoriés s'ils ne sont pas utilisés pour affecter des rôles d'application à l'utilisateur. Les administrateurs de service ou les utilisateurs dotés du rôle d'application Access Control - Gérer peuvent accéder au rapport sur l'affectation de rôle pour vérifier les rôles prédéfinis et les rôles d'application affectés à un utilisateur ou à un groupe. 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 l'onglet **Gérer les 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.

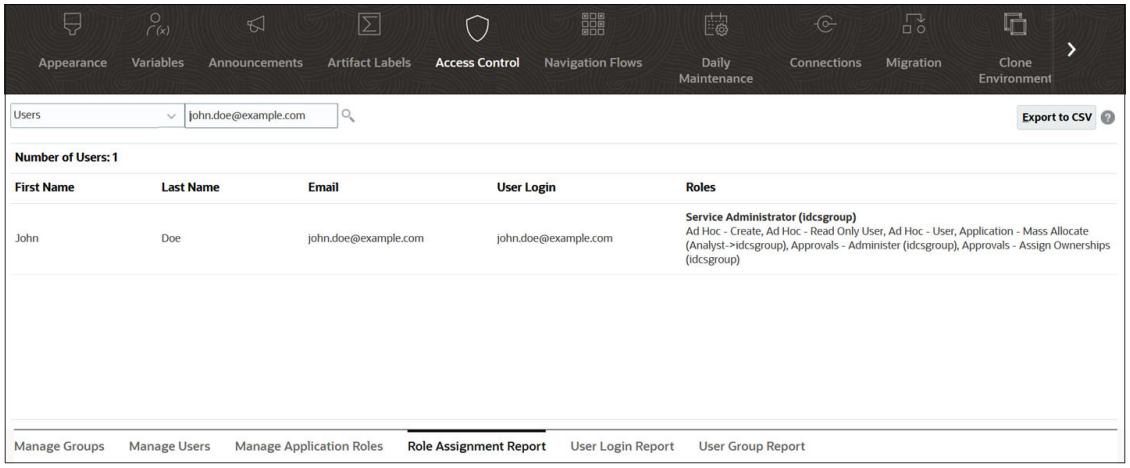
   Les utilisateurs ou les groupes répondant aux critères de recherche sont répertoriés. Par défaut, le rapport est trié par **connexion utilisateur**, puis par **nom de groupe** (pour les recherches de groupe).
4. Cliquez sur l'icône  correspondant à l'utilisateur ou au groupe, puis sélectionnez **Rapport sur l'affectation de rôle**.
5. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter le rapport dans un fichier CSV.

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

Les administrateurs de service ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer utilisent le rapport sur l'affectation de rôle pour vérifier l'accès de tous les utilisateurs, affecté via des rôles de niveau application et des rôles prédéfinis (en gras). Ce rapport montre tous les utilisateurs actifs auxquels un rôle prédéfini a été affecté. Les utilisateurs désactivés ne figurent pas dans ce rapport.

Les rôles hérités, ainsi que les informations relatives à l'héritage, sont affichés sur une ligne distincte pour chaque utilisateur.

Si un rôle prédéfini ou un rôle d'application est affecté à un groupe IDCS, le rapport indique que ce rôle prédéfini est affecté indirectement à l'utilisateur via le groupe IDCS. Par exemple, supposons que l'utilisateur John Doe soit affecté en tant que membre du groupe idcsgroup et que ce groupe soit affecté au rôle prédéfini Administrateur de service. 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 :




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.

| User Login | First Name | Last Name | Email | Role | Granted through Group |
|---|---|---|---|---|---|
| john.doe@example.com | John | Doe | john.doe@example.com | Service Administrator | idcsgroup |
| john.doe@example.com | John | Doe | john.doe@example.com | Ad Hoc - Create | |
| john.doe@example.com | John | Doe | john.doe@example.com | Ad Hoc - Read Only User | |
| john.doe@example.com | John | Doe | john.doe@example.com | Ad Hoc - User | |
| john.doe@example.com | John | Doe | john.doe@example.com | Application - Mass Allocate | Analyst->idcsgroup |
| john.doe@example.com | John | Doe | john.doe@example.com | Approvals - Administer | idcsgroup |
| john.doe@example.com | John | Doe | john.doe@example.com | Approvals - Assign Ownerships | idcsgroup |

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.

   Le rapport sur l'affectation de rôle apparaît. Par défaut, le rapport est trié par **connexion utilisateur**, puis par rôle d'application sous **Rôles** (pour les recherches par rôle). Les rôles prédéfinis sont affichés en caractères gras et les rôles d'application en caractères standard.

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 ou les utilisateurs dotés du rôle d'application Contrôle d'accès - Gérer peuvent régénérer ce rapport pour une plage de dates personnalisée ou pour les 30, 90 et 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 Fusion Cloud Enterprise Performance Management 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.

   Le rapport sur les connexions utilisateur apparaît. Par défaut, le rapport est trié par **date et heure d'accès**.
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 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 . Les administrateurs de service ou les utilisateurs dotés du rôle Contrôle d'accès - Gérer peuvent générer ce rapport.

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. Les groupes directs sont affichés en caractères gras et les groupes indirects en caractères standard.

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 générer 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 plus d'instructions sur l'utilisation de la fonctionnalité de recherche, reportez-vous à la section Utilisation de la recherche.

   Le rapport sur le groupe d'utilisateurs apparaît. Par défaut, le rapport est trié par **connexion utilisateur**.
4. Cliquez sur **Annuler** pour fermer le rapport.
5. **Facultatif :** cliquez sur **Exporter dans un fichier CSV** pour exporter les noms et descriptions de groupe EPM dans un fichier `Groups.csv`.

   Cette option ne permet pas d'exporter des groupes PREDEFINED ou IAM. L'option **Exporter dans un fichier CSV** est désactivée s'il n'existe aucun groupe EPM. Au moins un groupe EPM Cloud doit exister dans Contrôle d'accès pour que cette option puisse être utilisée.
6. **Facultatif :** cliquez sur **Importer à partir du fichier CSV** pour importer des affectations de groupe d'utilisateurs EPM à partir d'un fichier CSV dans Contrôle d'accès.

   Pour obtenir des informations sur le format de fichier CSV et d'autres détails, reportez-vous à la section Import d'affectations de groupe d'utilisateurs à partir d'un fichier.