Administrateurs Diveline : configuration des listes de contrôle d’accès (ACL) – Bonnes pratiques

Description

Grouper les utilisateurs et appliquer un fichier ACL par défaut peut accélérer la configuration et la maintenance des contrôles d'accès aux données DiveLine.

Tous les objets sont contrôlés par une liste de contrôle d'accès (ACL). Dans le niveau de sécurité 2, un objet est inaccessible sauf si les utilisateurs ou groupes sont ajoutés à son ACL. En règle générale, dans les répertoires de projets DI il y a plusieurs fichiers de Modèle. Pour l'administrateur DiveLine, cela pourrait devenir un processus lourd. En regroupant les utilisateurs et en attribuant un ACL par défaut à ces groupes de fichiers, vous gagnez du temps. Comment? Tout d'abord, un groupe peut être assigné à un ACL et les utilisateurs peuvent être facilement déplacés dans ou hors du groupe. Deuxièmement, les limites et les suppressions peuvent être appliqués au niveau du fichier par défaut et la restriction peut être appliquée à tous les fichiers dans ce répertoire, aussi longtemps que le fichier ne possède pas son propre ACL.

Étape 1 : créer les groupes et ses membres (Figure 1).

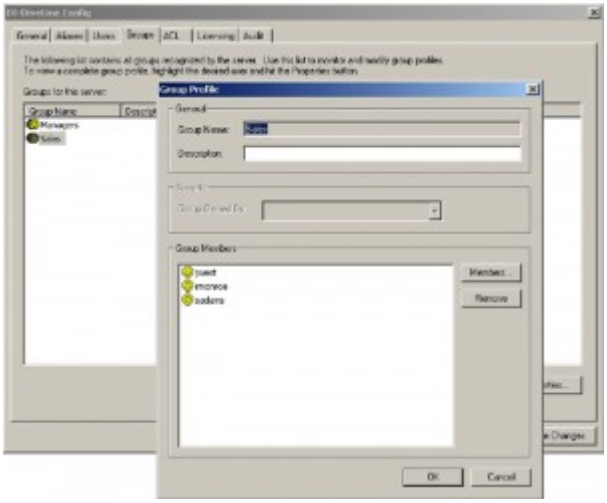

Figure 1

a) Ouvrez DI-Config en tant qu'administrateur.
b) Sélectionnez l'onglet ***Groups*** de DI-Config.
c) Cliquez sur le bouton ***New group...***
d) Saisissez un nom de groupe.
e) Cliquez sur le bouton ***Members...*** pour sélectionner des utilisateurs pour le Groupe. Dans cet exemple, le nom de groupe est ***Sales*** et de trois utilisateurs sont membres.

Maintenant, éditez l'ACL du fichier par défaut.

Etape 2 : Ajoutez le groupe à l'ACL du fichier par défaut (Figure 2).

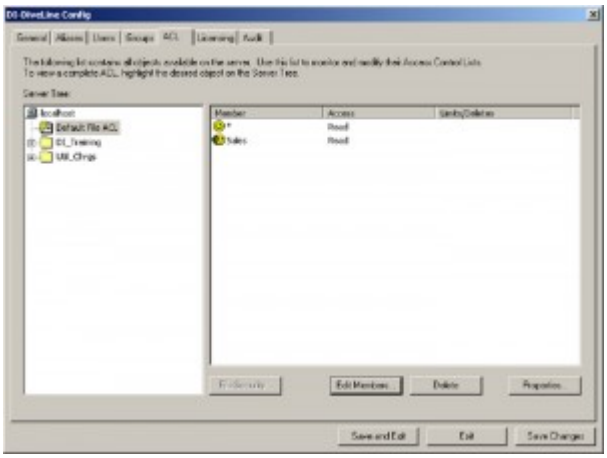

Figure 2

a) Sélectionnez l'onglet ***ACL*** de DI-Config.
b) Cliquez sur l'ACL du fichier par défaut dans l'arborescence du serveur.
c) Cliquez sur le bouton ***Edit members...*** pour sélectionner (ajouter) le Groupe.

Étape 3 : modifier les propriétés d'ACL du groupe ***Sales***, et l'accès aux données (Figure 3).

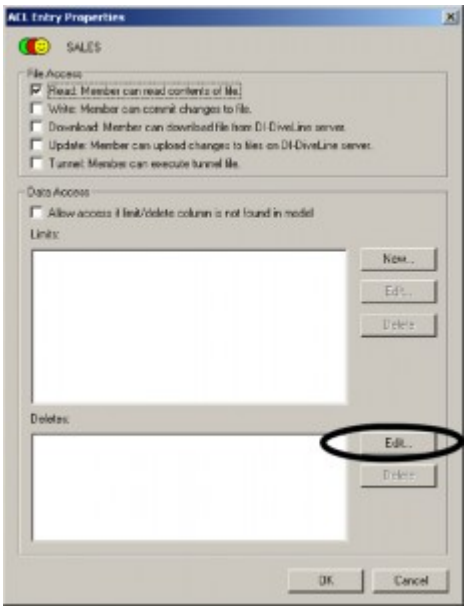

Figure 3

On y accède par un double clic sur l'entrée ***Sales*** dans la liste des membres.
Cliquez sur le bouton ***Edit...*** dans la section d'accès aux données, pour ouvrir la boîte de dialogue ***Edit ACL Entry Deletes.***
Maintenant, modifiez les suppressions de l'entrée ACL.
Parce que la suppression (et / ou la limitation) est ajoutée à partir du niveau de fichier par défaut, la liste des colonnes disponibles est vide. Toutefois, les colonnes de champ Somme peuvent être ajoutées en les saisissant.

Étape 4 : Ajouter / supprimer des valeurs (Figure 4).

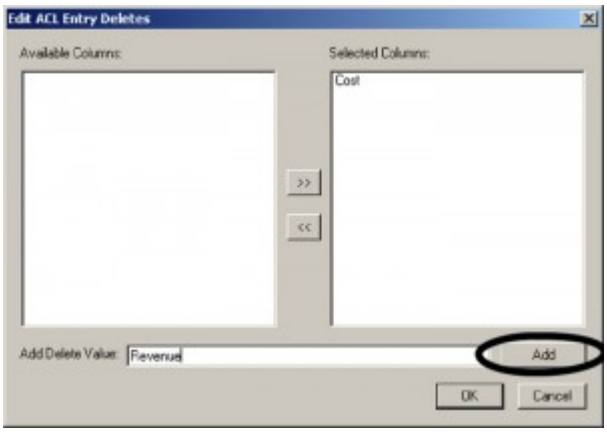

Figure 4

a) Dans la boîte de dialogue ***Edit ACL Entry Deletes***, tapez le nom de la colonne. Dans cet exemple, ***Revenue*** est ajouté. Toute Dimension, champ Somme ou champ Infos peuvent être ajoutés.
b) Cliquez sur le bouton ***Add***.
c) Cliquez sur le bouton ***OK*** pour fermer la boîte de dialogue ***Edit ACL Entry Deletes***.
d) Cliquez sur le bouton ***OK*** dans la boite de dialogue ***ACL Entry Properties*** pour la fermer.

Plusieurs colonnes peuvent être ajoutées en répétant les étapes 4a et 4b. La figure 5 montre deux suppressions qui ont été ajoutées. Des mesures similaires sont prises si les valeurs de Dimensions sont limitées.

Étape 5 : Revoir la configuration ACL (Figure 5).

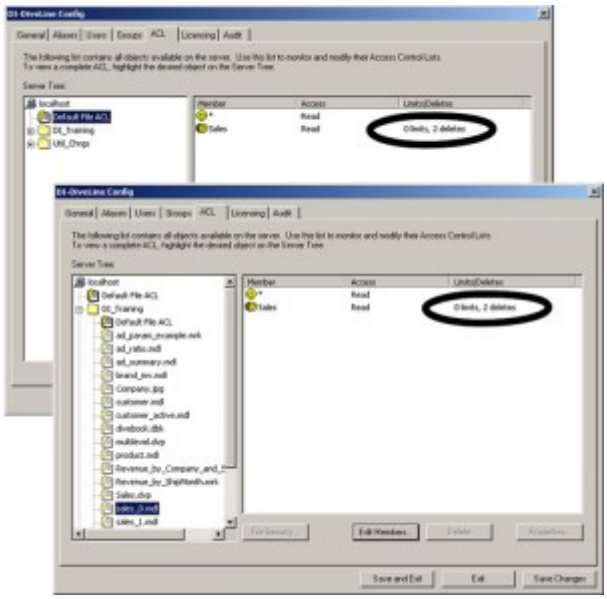

Figure 5

a) Notez la configuration des membres de l'ACL de fichier par défaut - Les limites / suppressions du groupe ***Sales*** indiquent: 0 limite, 2 suppressions.
b) Cliquez sur un fichier du Modèle. À condition qu'il ne possède pas son propre ACL, la configuration ACL de fichier par défaut est appliquée.

Étape 6 : Enregistrer les modifications

Cliquez sur le bouton ***Save and Exit***.

Pour les administrateurs DiveLine, l'attribution d'un groupe à un ACL de fichier et le maintien de son adhésion à l'utilisateur simplifie le processus de configuration des privilèges. Lorsque l'ACL est configuré au niveau ACL de fichier par défaut, les privilèges sont diffusés en cascade à travers l'arborescence des répertoires.

Bonus

Le processus DiveLine pour déterminer l'accès n'est pas le même pour les versions antérieures à la version 6.2 de DiveLine.

6.1 et versions antérieures :

a) Détermine si un ACL spécifique ou un ACL par défaut doit être utilisé.
b) Vérifie les accès accordés explicitement à un utilisateur et ses privilèges (limites et suppressions).
c) Si l'utilisateur ne figure pas explicitement, vérifie pour un groupe que l'utilisateur est répertorié à l'intérieur. Lorsque l'utilisateur est dans plus d'un groupe dans les ACL, les privilèges du premier groupe sont utilisés. Par conséquent, l'ordre de la liste des groupes sur un ACL de répertoire ou de fichiers est important.
d) Enfin, si l'utilisateur ne figure pas explicitement ou n'est pas un utilisateur listé dans un groupe, vérifie alors si l'"utilisateur étoile" a accordé l'accès et des privilèges respectifs.

6.2 :

a) Détermine si un ACL spécifique ou ACL par défaut doit être utilisé.
b) Détermine l'utilisateur et la liste des membres du groupe.
c) Vérifie l'accès accordé explicitement à un utilisateur et ses privilèges (limites et suppressions).
d) Si l'utilisateur ne figure pas explicitement, vérifie pour un groupe que l'utilisateur est répertorié à l'intérieur. Lorsque l'utilisateur est dans plus d'un groupe qui ont des privilèges différents sur le fichier, les décisions d'accès sont additifs de la manière suivante: les suppressions sont fusionnées; les limites sur la même dimension s'additionnent; les limites de dimensions différentes sont combinées.
e) Enfin, si l'utilisateur ne figure pas explicitement ou n'est pas un utilisateur dans un groupe listé, vérifie alors si l'"utilisateur étoile" a accordé l'accès et des privilèges respectifs.

Tags

1. DiveLine
2. droits accès