Administrateurs Diveline : configuration des listes de contrÃ´le dâ??accÃ¨s (ACL) â?? Bonnes pratiques

Description

Grouper les utilisateurs et appliquer un fichier ACL par dÃ©faut peut accÃ©lÃ©rer la configuration et la maintenance des contrÃ´les d'accÃ¨s aux donnÃ©es DiveLine.

Tous les objets sont contrÃ´lÃ©s par une liste de contrÃ´le d'accÃ¨s (ACL). Dans le niveau de sÃ©curitÃ© 2, un objet est inaccessible sauf si les utilisateurs ou groupes sont ajoutÃ©s Ã son ACL. En rÃ¨gle gÃ©nÃ©rale, dans les rÃ©pertoires de projets DI il y a plusieurs fichiers de ModÃ¨le. Pour l'administrateur DiveLine, cela pourrait devenir un processus lourd. En regroupant les utilisateurs et en attribuant un ACL par dÃ©faut Ã ces groupes de fichiers, vous gagnez du temps. Comment? Tout d'abord, un groupe peut Ãªtre assignÃ© Ã un ACL et les utilisateurs peuvent Ãªtre facilement dÃ©placÃ©s dans ou hors du groupe. DeuxiÃ¨mement, les limites et les suppressions peuvent Ãªtre appliquÃ©s au niveau du fichier par dÃ©faut et la restriction peut Ãªtre appliquÃ©e Ã tous les fichiers dans ce rÃ©pertoire, aussi longtemps que le fichier ne possÃ¨de pas son propre ACL.

Ã?tape 1 : crÃ©er les groupes et ses membres (Figure 1).

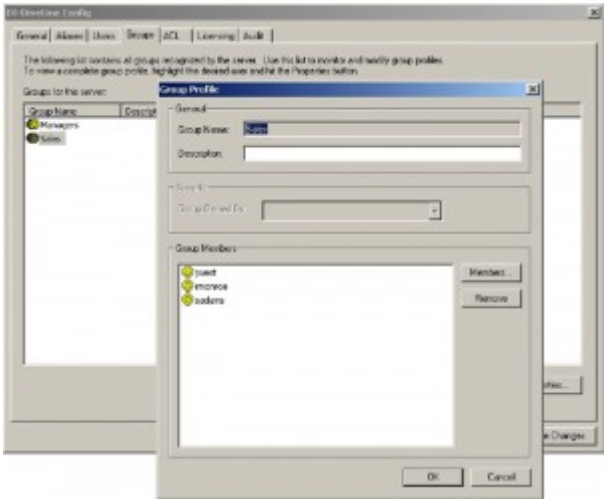

Figure 1

a) Ouvrez DI-Config en tant qu'administrateur.
b) SÃ©lectionnez 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 sÃ©lectionner des utilisateurs pour le Groupe. Dans cet exemple, le nom de groupe est ***Sales*** et de trois utilisateurs sont membres.

Maintenant, Ã©ditez l'ACL du fichier par dÃ©faut.

Etape 2 : Ajoutez le groupe Ã l'ACL du fichier par dÃ©faut (Figure 2).

Â© Bimaxis - Tous droits rÃ©servÃ©s

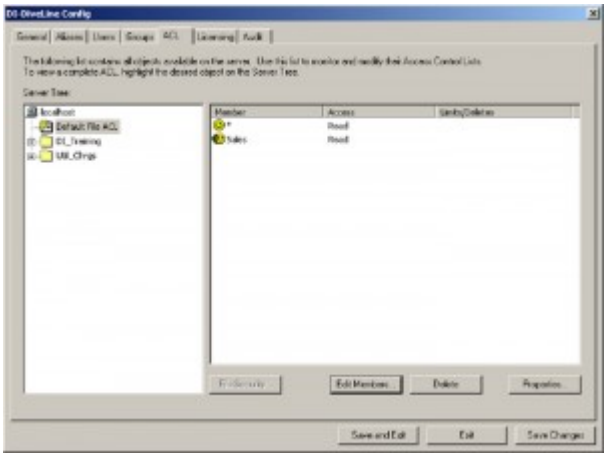

Figure 2

a) SÃ©lectionnez l'onglet ***ACL*** de DI-Config.
b) Cliquez sur l'ACL du fichier par dÃ©faut dans l'arborescence du serveur.
c) Cliquez sur le bouton ***Edit members...*** pour sÃ©lectionner (ajouter) le Groupe.

Ã?tape 3 : modifier les propriÃ©tÃ©s d'ACL du groupe ***Sales***, et l'accÃ¨s aux donnÃ©es (Figure 3).

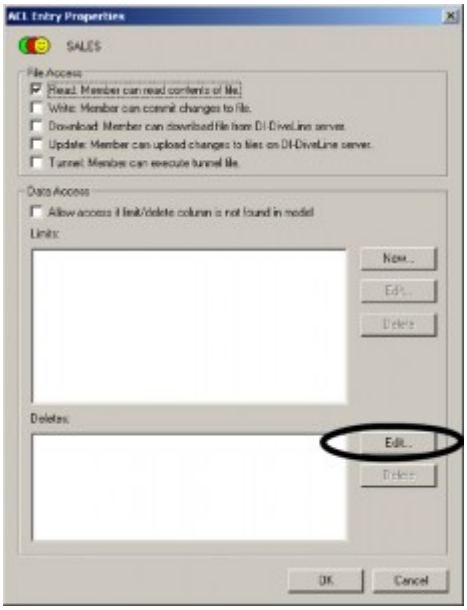

Figure 3

On y accÃ¨de par un double clic sur l'entrÃ©e ***Sales*** dans la liste des membres.
Cliquez sur le bouton ***Edit...*** dans la section d'accÃ¨s aux donnÃ©es, pour ouvrir la boÃ®te de dialogue ***Edit ACL Entry Deletes.***
Maintenant, modifiez les suppressions de l'entrÃ©e ACL.
Parce que la suppression (et / ou la limitation) est ajoutÃ©e Ã partir du niveau de fichier par dÃ©faut, la liste des colonnes disponibles est vide. Toutefois, les colonnes de champ Somme peuvent Ãªtre ajoutÃ©es en les saisissant.

Ã?tape 4 : Ajouter / supprimer des valeurs (Figure 4).

Â© Bimaxis - Tous droits rÃ©servÃ©s

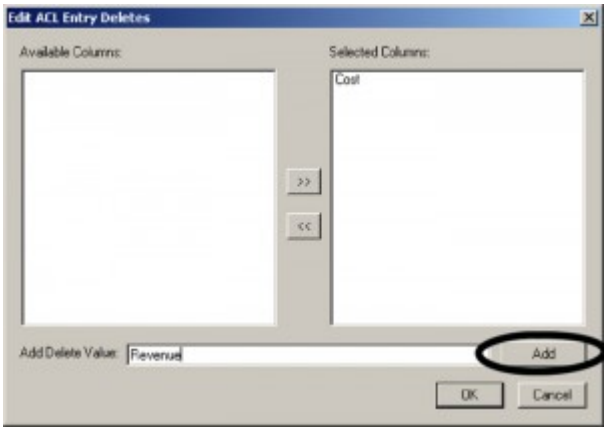

Figure 4

a) Dans la boÃ®te de dialogue ***Edit ACL Entry Deletes***, tapez le nom de la colonne. Dans cet exemple, ***Revenue*** est ajoutÃ©. Toute Dimension, champ Somme ou champ Infos peuvent Ãªtre ajoutÃ©s.
b) Cliquez sur le bouton ***Add***.
c) Cliquez sur le bouton ***OK*** pour fermer la boÃ®te 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 Ãªtre ajoutÃ©es en rÃ©pÃ©tant les Ã©tapes 4a et 4b. La figure 5 montre deux suppressions qui ont Ã©tÃ© ajoutÃ©es. Des mesures similaires sont prises si les valeurs de Dimensions sont limitÃ©es.

Ã?tape 5 : Revoir la configuration ACL (Figure 5).

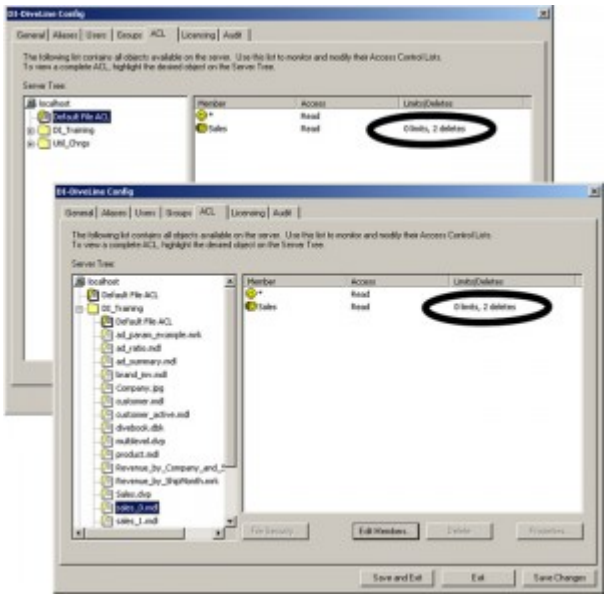

Figure 5

a) Notez la configuration des membres de l'ACL de fichier par dÃ©faut - Les limites / suppressions du groupe ***Sales*** indiquent: 0 limite, 2 suppressions.
b) Cliquez sur un fichier du ModÃ¨le. Ã? condition qu'il ne possÃ¨de pas son propre ACL, la configuration ACL de fichier par dÃ©faut est appliquÃ©e.

Â© Bimaxis - Tous droits rÃ©servÃ©s

Ã?tape 6 : Enregistrer les modifications

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

Pour les administrateurs DiveLine, l'attribution d'un groupe Ã un ACL de fichier et le maintien de son adhÃ©sion Ã l'utilisateur simplifie le processus de configuration des privilÃ¨ges. Lorsque l'ACL est configurÃ© au niveau ACL de fichier par dÃ©faut, les privilÃ¨ges sont diffusÃ©s en cascade Ã travers l'arborescence des rÃ©pertoires.

Bonus

Le processus DiveLine pour dÃ©terminer l'accÃ¨s n'est pas le mÃªme pour les versions antÃ©rieures Ã la version 6.2 de DiveLine.

6.1 et versions antÃ©rieures :

a) DÃ©termine si un ACL spÃ©cifique ou un ACL par dÃ©faut doit Ãªtre utilisÃ©.
b) VÃ©rifie les accÃ¨s accordÃ©s explicitement Ã un utilisateur et ses privilÃ¨ges (limites et suppressions).
c) Si l'utilisateur ne figure pas explicitement, vÃ©rifie pour un groupe que l'utilisateur est rÃ©pertoriÃ© Ã l'intÃ©rieur. Lorsque l'utilisateur est dans plus d'un groupe dans les ACL, les privilÃ¨ges du premier groupe sont utilisÃ©s. Par consÃ©quent, l'ordre de la liste des groupes sur un ACL de rÃ©pertoire ou de fichiers est important.
d) Enfin, si l'utilisateur ne figure pas explicitement ou n'est pas un utilisateur listÃ© dans un groupe, vÃ©rifie alors si l'"utilisateur Ã©toile" a accordÃ© l'accÃ¨s et des privilÃ¨ges respectifs.

6.2 :

a) DÃ©termine si un ACL spÃ©cifique ou ACL par dÃ©faut doit Ãªtre utilisÃ©.
b) DÃ©termine l'utilisateur et la liste des membres du groupe.
c) VÃ©rifie l'accÃ¨s accordÃ© explicitement Ã un utilisateur et ses privilÃ¨ges (limites et suppressions).
d) Si l'utilisateur ne figure pas explicitement, vÃ©rifie pour un groupe que l'utilisateur est rÃ©pertoriÃ© Ã l'intÃ©rieur. Lorsque l'utilisateur est dans plus d'un groupe qui ont des privilÃ¨ges diffÃ©rents sur le fichier, les dÃ©cisions d'accÃ¨s sont additifs de la maniÃ¨re suivante: les suppressions sont fusionnÃ©es; les limites sur la mÃªme dimension s'additionnent; les limites de dimensions diffÃ©rentes sont combinÃ©es.
e) Enfin, si l'utilisateur ne figure pas explicitement ou n'est pas un utilisateur dans un groupe listÃ©, vÃ©rifie alors si l'"utilisateur Ã©toile" a accordÃ© l'accÃ¨s et des privilÃ¨ges respectifs.

Tags

1. DiveLine
2. droits accÃ¨s

Â© Bimaxis - Tous droits rÃ©servÃ©s