|  |
| --- |
| Alfresco – Gestion des droits  CAPITALISATION SMU |
| DCNS |

Historique du document

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Auteur | Description |
| X.X prél X | AAAA-MM-JJ |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Réviseurs**

Chaque réviseur atteste avoir révisé ce document et affirme être en accord avec son contenu, en vertu de son rôle au sein de l’entente.

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Rôle | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Propriétaire**

Le propriétaire est responsable de la création de ce document, et atteste que ce dernier satisfait aux normes de qualité et qu’il est prêt à être soumis pour approbation finale.

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Rôle | Signature | Date |
|  |  |  |  |

**Approbation par CGI**

Le représentant de CGI atteste que ce document satisfait à toutes les exigences et qu’il répond adéquatement à tous les objectifs du document tels que décrits dans l’article , Objectifs du document, sauf indication contraire précisée par le client ou communiquée au client.

|  |  |  |  |
| --- | --- | --- | --- |
| Nom | Rôle | Signature | Date |
|  |  |  |  |

Table des matières

[1 Présentation 3](#_Toc447033036)

[2 Gestion des droits dans Alfresco (Eureka, GedIndus) 4](#_Toc447033037)

[2.1 Gestion des droits d’accès sur les fichiers/dossiers (Eureka) 4](#_Toc447033038)

[2.1.1 Fonctionnement d’Eureka sur les droits 4](#_Toc447033039)

[2.1.2 Recherche des fichiers/dossiers 5](#_Toc447033040)

[2.1.1 Explication des droits génériques 6](#_Toc447033041)

[**2.1.1.1** Pour information 6](#_Toc447033042)

[2.1.1.2 Explication des droits génériques 6](#_Toc447033043)

# Présentation

Le but de ce document est de regrouper ici les explications et piste de recherches toutes applications confondu, aussi bien à destination du support qu’à destination de la TMA.

# Gestion des droits dans Alfresco (Eureka, GedIndus)

## Gestion des droits d’accès sur les fichiers/dossiers (Eureka)

### Fonctionnement d’Eureka sur les droits

Les droits d’accès/recherches et autres se font sur le principe de l’héritage maximum. Pour un sous-dossier particulier, l’application fera la liste des droits disponibles pour un utilisateur donné se trouvant au niveau N-1 (soit le dossier juste au dessus, soit le site si on est déjà à la racine), auquel on y ajoute les droits propres au fichier/document courant. De façon récursive, le dossier N-1 récupèrera les droit du N-2 augmenté de ses propres droits…

Suivant le principe précédent, l’héritage de droit ne peut s’appliquer UNIQUEMENT si à chaque niveau de dossier, l’option « Hériter des droits d’accès » a été cochée. Si ce n’est pas le cas, et que les droits « site\_###\_siteCollaborateur », « site\_###\_SiteConsumer » et « site\_###\_SiteContributor » sont présent (avec les droits correspondant), il y aura une modification en cascade des droits d’accès sur tous les dossiers et sous-dossiers. Sinon, les utilisateurs ayant l’un de ces droits n’aura tout simplement pas accès (ni aucune visibilité de présence) à ces dossiers/sous-éléments.

* **Exemple :** 
  + **Site :** M. XXX est déclaré comme « Contributeur » (que ce soit directement ou au travers un groupe quelconque)
  + **Arborescence du site :**

Site

/usr

/home

/usr/aft

/usr/aft/test.txt

/home/test2.txt

* + **Droits déclarés :**
    - usr : l’héritage est supprimé. Le droit du contributeur est définit comme rôle « lecteur » (pas de modification pour les autres rôles)
    - aft : l’héritage est retiré. Seul les droits du gestionnaire est conservé
    - home : l’héritage est conservé
    - test.txt : l’héritage est conservé. Les droits d’accès spécifique ont été rajouté à M. XXX (en tant que « Contributeur »)
    - test2.txt : l’héritage est conservé
  + **Droits lors de l’utilisation :**
    - usr : A partir de ce dossier, tous les sous-dossiers/fichiers considéreront les contributeurs **du site** comme des « Lecteurs » (pas de modification ou création possible pour eux sur tous les fichiers et sous-dossiers). Des droits spécifiques pourront être appliqué plus tard aux sous-éléments présents.
    - aft : à partir de ce dossier, plus aucun utilisateur (en dehors du gestionnaire et des administrateurs) n’aura accès aux dossiers/fichiers. Les recherches ne retourneront pas les éléments contenus dans ce dossier (et sous-dossiers) si l’utilisateur n’est pas gestionnaire/admin.
    - home : ce sont les droit définit au niveau du site qui font loi. M. XXX pourra agir suivant le rôle « Contributeur » (comme défini au niveau du site)
    - test.txt : M. XXX n’aura pas accès à ce fichier, et sa recherche ne retournera pas ledit fichier (coupure de droit au niveau du dossier « /usr/aft »).
    - test2.txt : ce sont les droit définit au niveau du site qui font loi. M. XXX pourra agir suivant le rôle « Contributeur » (comme défini au niveau du site)

### Recherche des fichiers/dossiers

La recherche est appliqué par le principe de « **recherche en profondeur** ».

* **Pour chaque site :**
  + Dans ceux ou l’utilisateur a au moins un droit « lecteur », l’application continuera sa recherche aux sous-dossiers/fichiers.
  + Si ce n’est pas le cas, il ignorera ce site pour passer au suivant.
* **Pour chaque fichier trouvé :**
  + l’application vérifiera les droits d’accès de l’utilisateur sur ces derniers, et si les droit sont suffisants, il contrôlera le nom par rapport à la recherche
  + Si les droit sont suffisant et que le nom correspond, le fichier apparaitra dans le résultat de recherche. Si l’un des deux cas n’est pas bon, le fichier n’apparaitra pas.
* **Pour chaque dossier trouvé :**
  + l’application vérifiera les droits d’accès de l’utilisateur sur ces dernier, et si les droits sont suffisants, il contrôlera le nom par rapport à la recherche, et continuera sa recherche dans les sous-dossiers/fichiers qu’il contient.
  + Si les droits ne sont pas suffisant, il arrêtera sa recherche pour ce dossier et continuera sa recherche sans faire de contrôle dans son contenu.

Ainsi, en reprenant l’exemple ci-dessus, si l’utilisateur XXX recherche le mot « test », il n’obtiendra que le fichier « test2.txt ». « test.txt » ne sera pas retourné, malgré les droits spécifiques de l’utilisateur dessus car l’utilisateur n’a pas accès au dossier « /usr/arf »

### Explication des droits génériques

#### Pour information

Afin de simplifier la compréhension, pour une arborescence « **/usr/aft/log/test.txt** », si on se place dans le dossier « **aft** » :

* « **aft** » est au niveau N
* « **usr** » est au niveau N-1
* « **log** » est au niveau N+1
* « **test.txt** » est au niveau N+2

#### Explication des droits génériques

Lors de la création d’un fichier/dossier, le principe d’héritage de droit est appliqué. Par ce principe, des groupes génériques apparaissent automatiquement dans la liste des droits d’accès pour chaque éléments, bien que personne n’apparait dans ces groupes.

Dans Eureka, il y en a 4 :

* **« site\_###\_SiteCollaborator » :** il s’agit du droit générique des coordinateurs.
* **« site\_###\_SiteConsumer » :** il s’agit du droit générique des lecteurs.
* **« site\_###\_SiteContributor » :** il s’agit du droit générique des contributeurs
* **« site\_###\_SiteManager » :** il s’agit du droit générique des gestionnaires du site (et administrateurs de l’application). Il ne peut pas être modifié ou supprimé.

Pour ces 4 groupes génériques, les « ### » correspondent au nom du site ou ils sont appliqués (par exemple, « site\_rde\_SiteCollaborator » définit les droits des coordinateurs pour le site « rde »).

Il faut bien faire attention entre ces groupes génériques et les groupes d’utilisateurs. Ainsi :

* les groupes génériques ne contiennent aucun utilisateur.
* Les groupes génériques n’existent que pour servir de « **passe-plat** » entre le niveau N-1 (site ou dossier englobant suivant la position de l’élément sur lequel sont appliqués les droits), et l’ensemble des éléments se trouvant directement dans le dossier courant (fichiers/sous-dossiers, niveau N+1).
* Ils ont pour but :
  + Soit de conserver les droits précédents (niveau N-1) pour les éléments suivant (niveau N+1)
  + Soit de modifier les droits entre les niveaux précédents (N-1) et les suivants (N+1). On peut ainsi définir que tous les « contributeurs » au niveau N-1 seront considéré comme « lecteurs » au niveau N+1 (par exemple).
* Si un groupe générique n’est pas présent à un niveau N, pour tous les utilisateurs ayant les droits correspondants au niveau précédent (N-1) :
  + Ils ne verront pas l’élément courant (niveau N)
  + Ils n’auront pas accès aux éléments suivants (niveau N+1 et suivant), même si les droits spécifiques sont rajoutés sur les sous-éléments (N+1 et suivant)
  + Leurs recherches n’impliqueront pas l’élément N et suivants (N+1, N+2, …), même si des droits spécifiques sont rajoutés sur les sous-éléments (N+1 et suivant)

Les groupes génériques ne servent que de **passe-plat**. S’ils ne sont pas définis à un niveau donné (niveau N), mais que le groupe d’utilisateur (ou les utilisateurs de façon nominatives) sont présents, les droits des utilisateurs spécifiés seront conservés pour la suite.

**/!\ Si l’héritage des droits est retiré, il est donc important que les droits soient fournit via les groupes ou nominativement, et ce à chaque niveau afin que la chaine d’accès ne soit pas coupée /!\**