

# Configuration de "*DIET file management system*"

19 octobre 2010

## 1 Configuration des serveurs

### 1.1 Tables d'utilisateurs et de groupes

*DIET file management system* permet d'utiliser les comptes d'un même utilisateur sur plusieurs systèmes sur lesquels il utilise des identifiants (*logins*) différents. Pour cela, le serveur utilise une table de correspondance entre un identifiant utilisateur *global* et l'utilisateur *local* correspondant. De même, les groupes d'utilisateurs peuvent varier d'une machine à l'autre, une table de correspondance des groupes peut également être renseignée pour permettre de maintenir tant que possible les droits d'accès aux fichiers d'un système à l'autre. Par ailleurs, les connexions aux comptes des utilisateurs s'effectuant par l'intermédiaire d'une connexion *ssh*, la table utilisateurs permet de définir la clé privée qui sera utilisée pour ces connexions. On précisera également le répertoire **HOME** utilisé pour les connexions.

#### 1.1.1 Exemple de table d'utilisateurs

Une table des utilisateurs exploitable par le serveur est un fichier texte contenant quatre colonnes. La première colonne correspond aux identifiants globaux des utilisateurs. La seconde correspond à l'identifiant local de l'utilisateur, la troisième colonne définit le répertoire **HOME** à utiliser et la dernière colonne le chemin vers la clé privée utilisée pour les connexions *ssh* de cet utilisateur.

pierre.dupont	pdupont	/home/lyon/pdupont	/opt/diet/dfms/etc/keys/pdupont_rsa
paul.dupuis	pdupuis	/home/paris/pdupuis	/opt/diet/dfms/etc/keys/pdupuis_rsa
jacques.duval	jduval	/home/papeete/jduval	/opt/diet/dfms/etc/keys/jduval_rsa
jean.duflot	jduflot	/home/lyon/jduflot	/opt/diet/dfms/etc/keys/jduflot_rsa

Avec le fichier exemple donné ci-dessus, lorsque Pierre Dupont voudra accéder à un fichier de son répertoire utilisateur, la connexion *ssh* s'effectuera avec l'identifiant **pdupont** dans le répertoire **/home/lyon/pdupont** à l'aide de la clé RSA stockée dans le fichier **/opt/diet/dfms/etc/keys/pdupont\_rsa**.

#### 1.1.2 Exemple de table des groupes

Une table des groupes utilisable par le serveur est un fichier texte contenant deux colonnes. La première correspond aux identifiants de groupes globaux et la seconde aux identifiants de groupes locaux.

lyon	users
paris	users
papeete	users
admins	admin
guests	temp

Avec le fichier exemple donné ci-dessus, un fichier appartenant au groupe d'identifiant global **admins** sera classé dans le groupe **admin** sur la machine locale. Il est à noter que lorsqu'il est impossible de maintenir une distinction de groupes d'utilisateurs existante au niveau globale sur la machine locale, les accès aux données peuvent être augmentés pour certains utilisateurs. Ainsi, avec la configuration donnée ici, un fichier du groupe **paris** dont les droits d'accès empêchaient l'accès à un utilisateur du groupe **lyon** verra cette restriction disparaître sur la machine locale. Le choix de correspondance des groupes

doit donc être effectué soigneusement et à défaut de pouvoir faire correspondre chaque groupe global à un groupe local au moins aussi restrictif, l'utilisateur veillera à réduire les droits d'accès à ses fichiers ou changer le groupe de ceux-ci.

Un utilitaire est fourni pour faciliter la génération d'une table des groupes en fonction de la configuration locale. Le programme **grp-config** parcourt la table des groupes du système en ignorant les groupes vides et demande l'identifiant global correspondant. L'option **-i** permet d'ignorer les groupes dont le nom commence par le caractère **\_** (certains systèmes UNIX utilisent de tels noms de groupe pour des services et fichiers systèmes qui n'ont pas d'intérêt à être "mappés" au niveau global).

### 1.1.3 Activation des tables users et groups

Par défaut, le serveur considère les groupes et utilisateurs locaux comme étant identiques aux groupes / utilisateurs globaux. Pour utiliser des tables d'utilisateurs ou de groupes, on utilisera les paramètres optionnels **--user-table** et **--grp-table**, ces options étant respectivement suivies du chemin vers le fichier contenant la table des utilisateurs et celui vers la table des groupes.

## 1.2 Configuration du nom d'hôte du serveur

Par défaut, le serveur prend le nom d'hôte de la machine comme nom lui permettant d'être retrouvé par les clients. Cependant, il peut s'avérer nécessaire de définir ce nom manuellement. Le paramètre optionnel **--hostname <name>** permet de définir un nom à utiliser pour la machine concernée.

## 1.3 Configuration d'un répertoire de dépôt temporaire

Les fichiers des utilisateurs étant récupérés par l'intermédiaire d'une commande *ssh*, ceux-ci sont déposés temporairement dans un répertoire accessible à l'application serveur. Ce répertoire est choisi grâce à l'option **--tmp-dir <dir>**. Il est recommandé d'utiliser un répertoire accessible en lecture, écriture et accès au seul utilisateur exécutant le serveur, les autres utilisateurs n'ayant des droits qu'en écriture/accès (mode octal 0733).

## 1.4 Configuration DIET du serveur

Le serveur doit être lancé avec l'option obligatoire **--config <config file>** pour se connecter à la hiérarchie DIET. Ce fichier doit au moins contenir un paramètre "parentName" permettant de définir à quel agent il doit se connecter. Il est également conseillé de fixer le paramètre "storageDirectory" en choisissant un répertoire temporaire en accès limité au processus du serveur (un répertoire **/tmp/DFMS** dont les droits d'accès sont fixés à 700 par exemple). Pour plus de détail quant à la configuration des serveurs DIET, se reporter au manuel de l'intergiciel.

## 2 Configuration des clients

L'ensemble des dix commandes de gestion de fichier prennent en paramètre obligatoire l'option **--config <config. file>** qui permet de définir le fichier de configuration DIET à utiliser. Ce fichier doit au moins contenir le paramètre **MAName** qui permet de se connecter au Master Agent de la hiérarchie DIET. Pour plus de détails sur les options disponibles pour les clients DIET, se reporter à la documentation de l'intergiciel.