GÉNÉRATION D'HISTORIQUES D'OUVERTURES ET FERMETURES DE SESSIONS

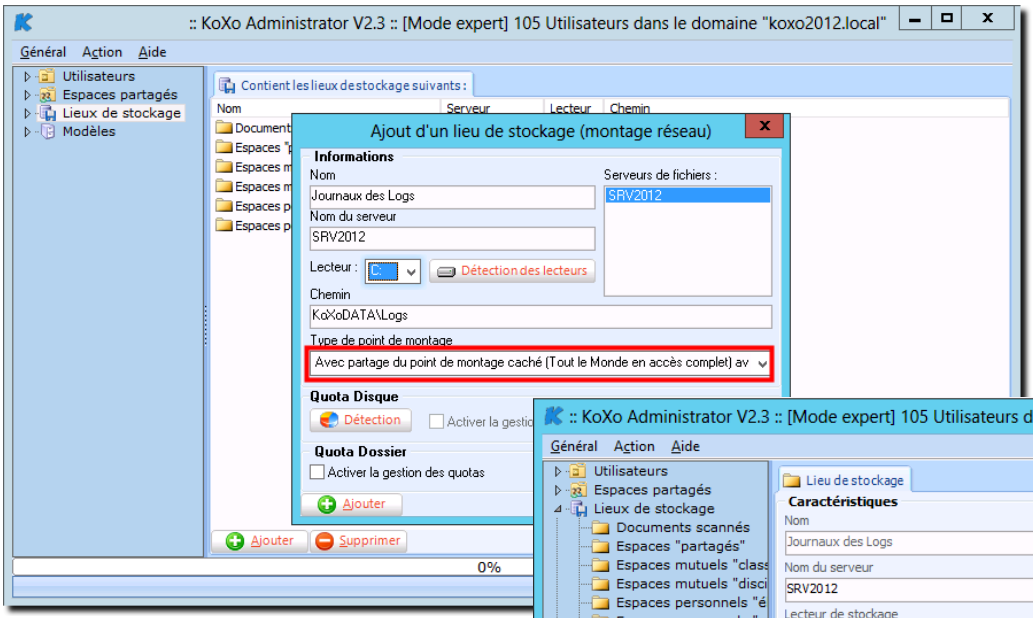
KOXO LOG SESSIONS

1 – Avant-propos

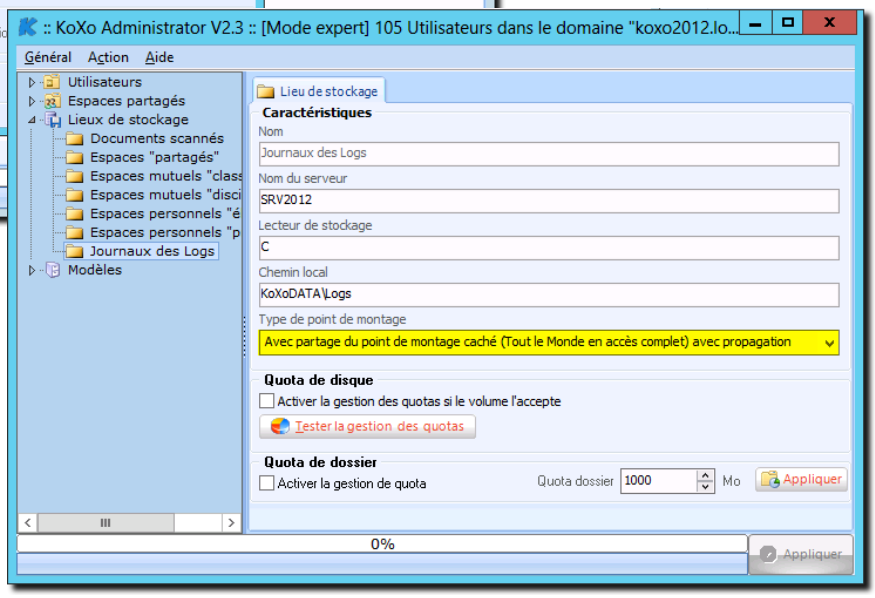
Ce document est destiné aux administrateurs de réseaux à base de serveurs Microsoft qui désirent réaliser un historique simple des ouvertures et fermetures de sessions des utilisateurs. L'outil proposé s'appuie sur le mécanisme natif des stratégies de groupe. Deux dossiers seront générés, un contiendra les historiques par machine et l'autre par utilisateur. Un outil de visualisation est fourni.

2 – Création du stockage

Le moyen le plus simple est de passer par KoXo Administrator, il suffit de créer un lieu de stockage que l'on nommera comme on le souhaite en prenant un point de montage « **avec partagé caché et accès en complet** » pour tout le monde :



Création du stockage



Vérification du stockage et partage associé

NB : Pour des raisons de sécurité il vaut mieux ne pas utiliser le même nom de dossier (et donc de partage associé) que celui de l'exemple (Logs).

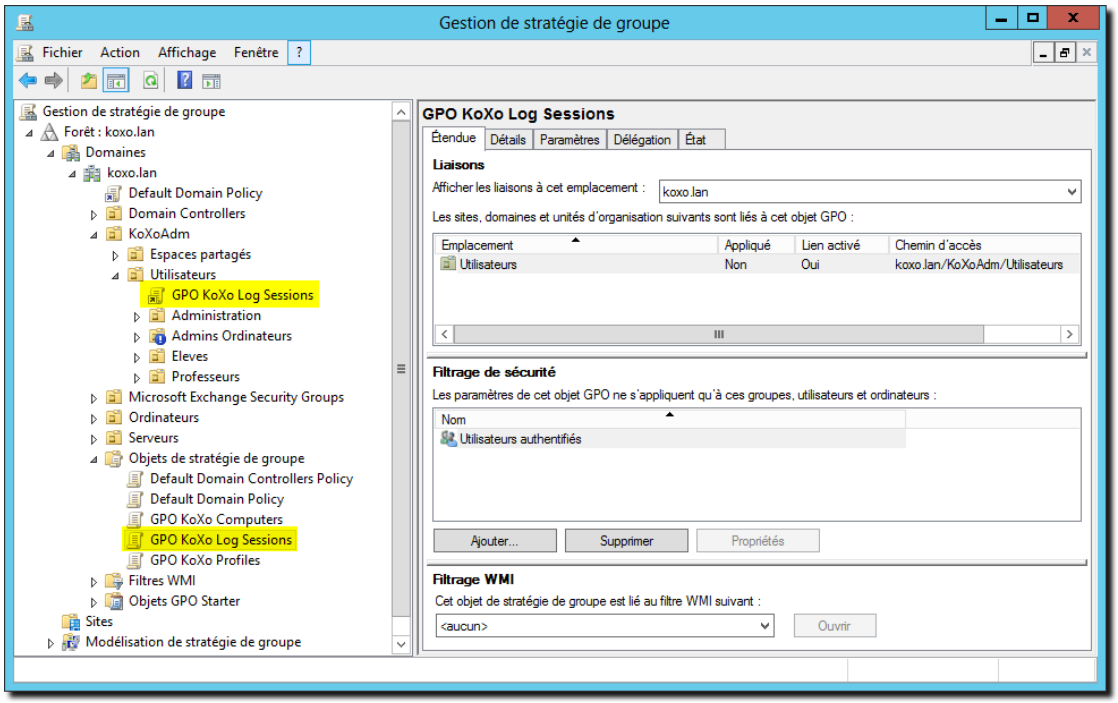
© 2006-2022 KoXo Développement

3 – Mise en place de la stratégie de groupe

Une stratégie de groupe toute faite est fournie, il suffit de l'importer et de la lier à l'unité d'organisation « racine » des utilisateurs. (Une telle démarche est décrite dans le manuel de KoXo Computers). **Il ne faudra pas oublier de modifier le nom du partage s'il a été modifié et éventuellement le nom du serveur s'il n'est pas le serveur ayant le rôle « émulateur PDC ».**

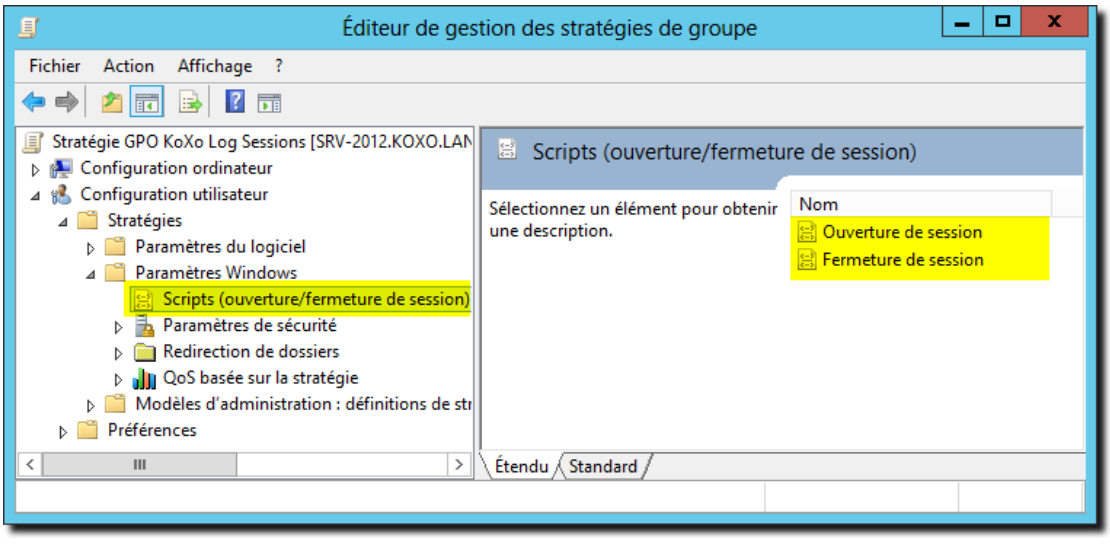
Voici cependant la méthode manuelle :

Dans la console de stratégie de groupe, créer un objet nommé « **GPO KoXo Log Session** » et le lier à l'unité d'organisation contenant les utilisateurs :



Objet de stratégie de groupe et lien

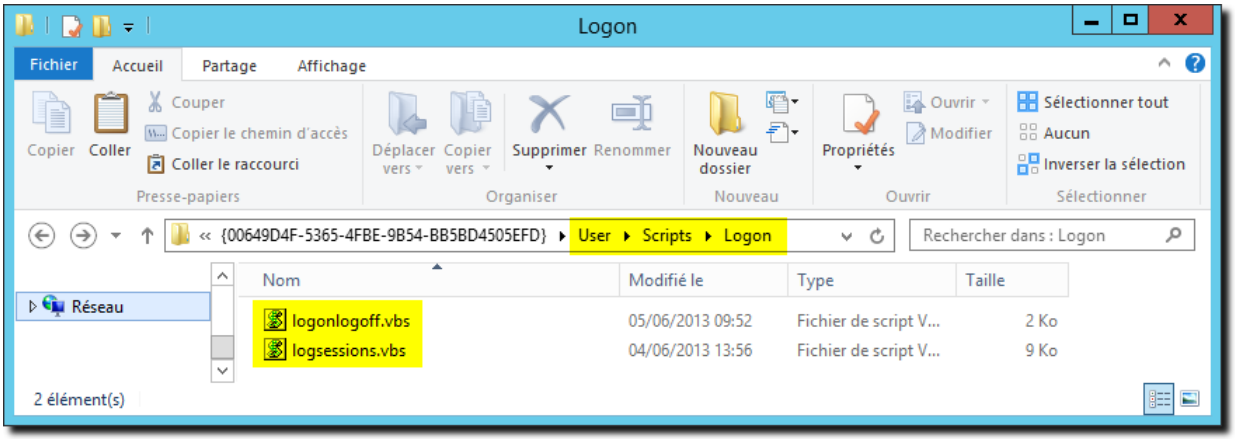
Editer en suite cet objet et se positionner sur les scripts liés à l'utilisateur :



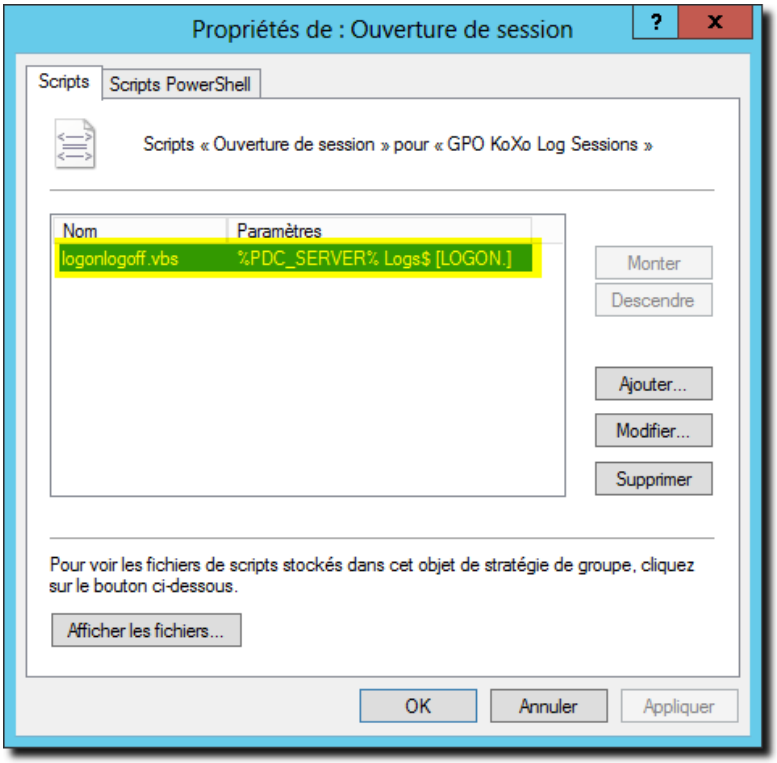
Scripts des utilisateurs

© 2006-2022 KoXo Développement

Cliquer sur l'ouverture de session, faire parcourir, copier-coller les scripts fournis « **logonlogoff.vbs** » et « **logsessions.vbs** » et indiquer le nom du script à exécuter : « **logonlogoff.vbs** » :



Copie des scripts « logonlogoff.vbs » et « logsession.vbs »



Configuration du script d'ouverture de session

Entrer le nom du script : « **logonlogoff.vbs** » et les paramètres « **%PDC_SERVER% Logs$ [LOGON.]** ».

Refaire exactement la même manipulation avec le même script pour la fermeture de session, entrer les paramètres « **%PDC_SERVER% Logs$ [LOGOFF]** ». La variable %LOGON_SERVER% existe aussi et désigne de serveur qui a servi à l'ouverture de session.

N.B. : Le script « **logonlogoff.vbs** » appelle le script « **logsessions.vbs** » avec les paramètres nécessaires. Si le serveur hébergeant le dossier de stockage des journaux n'est pas le serveur ayant le rôle FSMO émulateur PDC il faudra entrer son nom au lieu de la variable « **%PDC_SERVER%** », idem pour le nom du partage. **Ne pas oublier de modifier le nom du partage « Logs$ » s'il a été modifié.**

© 2006-2022 KoXo Développement

Il existe des options supplémentaires pour faire apparaitre le serveur de logon, l'adresse IP, l'adresse MAC et le nom LDAP (FQDN). Il suffit d'indiquer un « 1 » ou un « 0 » en fin de la ligne de paramètres. Si on souhaite rajouter au moins un de ces paramètres il faut saisir les quatre commutateurs (0 ou 1), sachant que l'ordre est : « Serveur de logon » « Adresse IP » « Adresse MAC » « FQDN ».

La ligne : `%PDC_SERVER% Logs$ "[LOGON.] 1 1 1 1"`

Nom	Paramètres
logonlogoff.vbs	%PDC_SERVER% Logs$ "[LOGON.] 1 1 1 1"

➔ Affichera le serveur de logon, puis l'adresse IP, puis l'adresse MAC, puis le nom LDAP (FQDN).

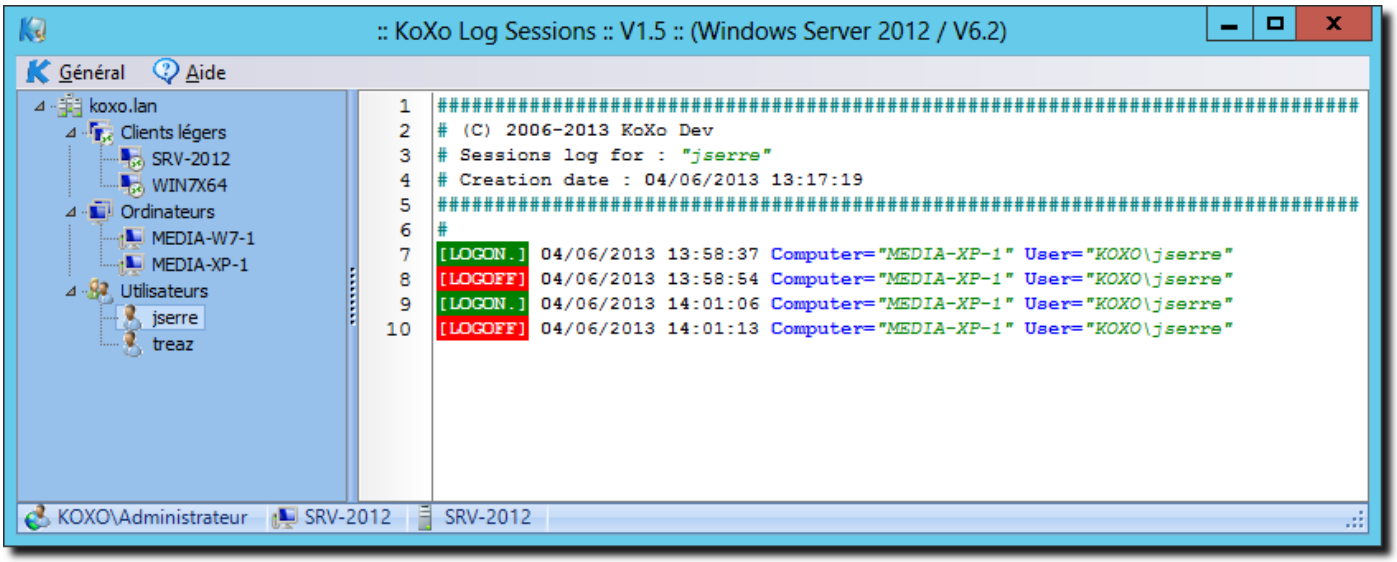
Si on ne souhaite pas avoir le serveur de logon, on entre :

```
%PDC_SERVER% Logs$ "[LOGON.] 0 1 1 1"
```

N.B. : Le point juste après le mot « **[LOGON.]** », permet d'avoir la même longueur que « **[LOGOFF]** » et d'avoir donc un alignement des messages. **Ne pas oublier les guillemets !**

3 – Visualisation des journaux

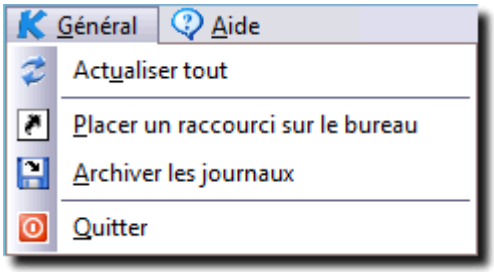
L'outil de visualisation doit être copié dans le dossier racine contenant les historiques. L'utilisation est des plus simples, un arbre fait apparaitre une branche pour les ordinateurs, une branche pour les clients légers et une branche pour les utilisateurs, dès qu'un journal est présent il est affiché dans l'arbre :



Visualisation du journal pour un ordinateur

N.B. : Le journal peut être exporté sous forme colorisée via un clic droit / Export au format RTF. Un clic droit sur un objet de l'arbre permet d'obtenir des informations « Annuaire ».

Le menu général permet de placer un raccourci sur le bureau pour lancer l'application plus facilement, et aussi de faire un archivage de tous les journaux au format ZIP, un dossier « **BACKUP** » est alors généré.



© 2006-2022 KoXo Développement