ANTRI Mohamed
Antrimohamed.fr

DS RM Password Synchronisation

Description

Lorsque nous souhaitons réparer ou restaurer notre Active Directory, il nous faut par moment entrer dans le DSRM (**D**irectory **S**ervices **R**estore **M**ode) sur nos contrôleurs de domaine. Pour entrer dans ce mode il nous faut un mot de passe qui a été spécifié lorsque nous avions promu un serveur en tant que contrôleur de domaine. Sur certains environnements Active Directory ancien ou de taille conséquente ce mot de passe aurait pu être spécifié par un administrateur qui a depuis quitté l'entreprise.

Malheureusement, certains services informatiques se rendent compte qu'ils ne possèdent pas ce mot de passe en plein incident de production ! A ce moment-là il est trop tard. Pour des raisons de sécurité évidente ce mot de passe doit aussi est changé régulièrement !

Nous allons donc voir comment synchroniser le mot de passe DSRM avec un compte Active Directory. Ainsi, ce mot de passe sera changé régulièrement et vous le maintiendrez constamment à jour.

Avantages

- Synchronisation avec un compte de l'AD.
- Mot de passe toujours à jour et régulièrement changé.
- Automatisation du processus.

Prérequis

- Un simple compte utilisateur AD.
- Une tâche planifiée.
- Un contrôleur de domaine étant en 2008 au minimum.

Pour les contrôleurs de domaine qui sont en 2008, vous devez appliquer le hotfix dont voici le lien :

http://support.microsoft.com/?kbid=961320

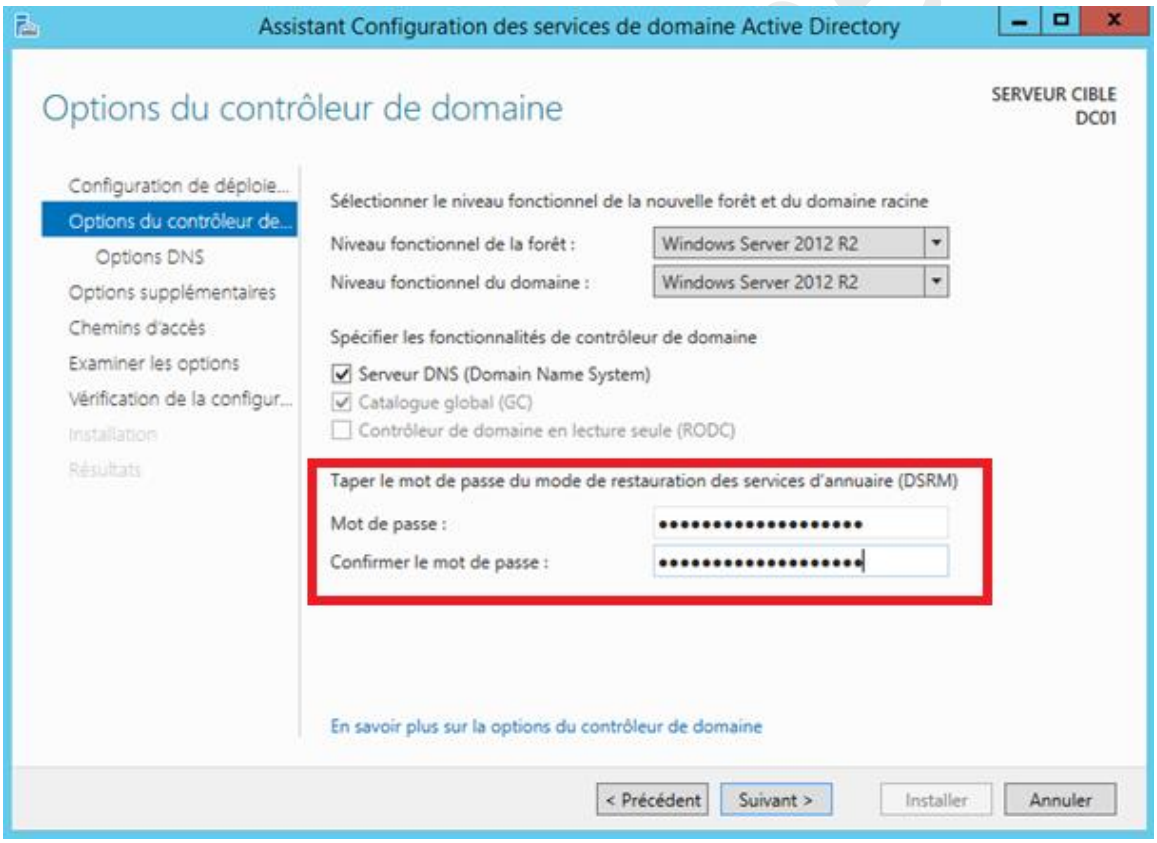
L'installation de ce hotfix nécessite un redémarrage de votre contrôleur de domaine !

Rappel

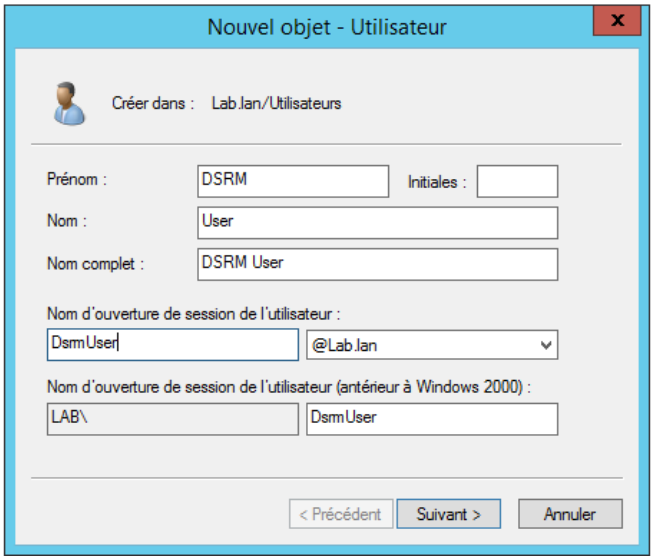
Il est important de rappeler que nous allons synchroniser le mot de passe d'un compte simple utilisateur avec le mot de passe DSRM. Cela signifie qu'à chaque fois que vous modifierez le mot de passe du compte simple utilisateur, il faudra alors de nouveau le synchroniser avec le mot de passe DSRM. Pour cela, dans notre exemple nous créerons une tâche planifiée qui sera exécutée quotidiennement.

Procédure

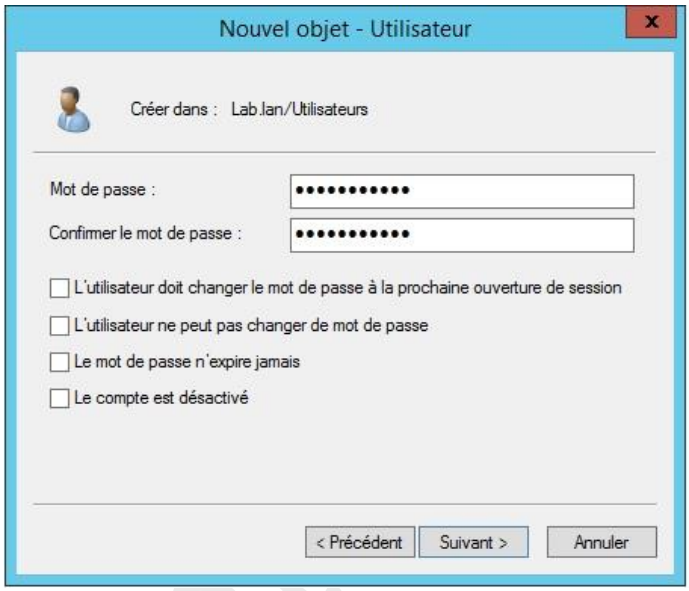
Pour commencer, voici l'endroit où indiquer le mot de passe DSRM pour la première fois lorsque nous avons promu notre serveur en tant que contrôleur de domaine.



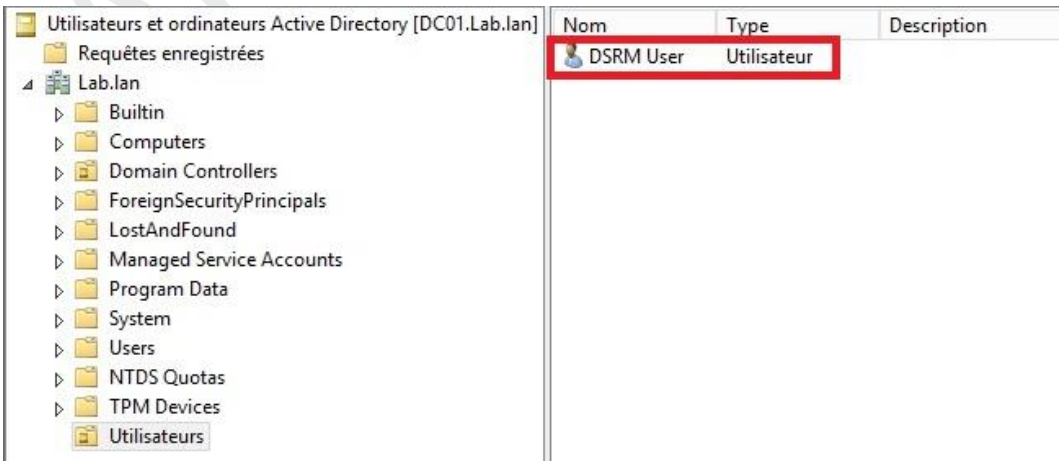
Nous allons ensuite créer notre compte qui sera utilisé pour la synchronisation du mot de passe DSRM.



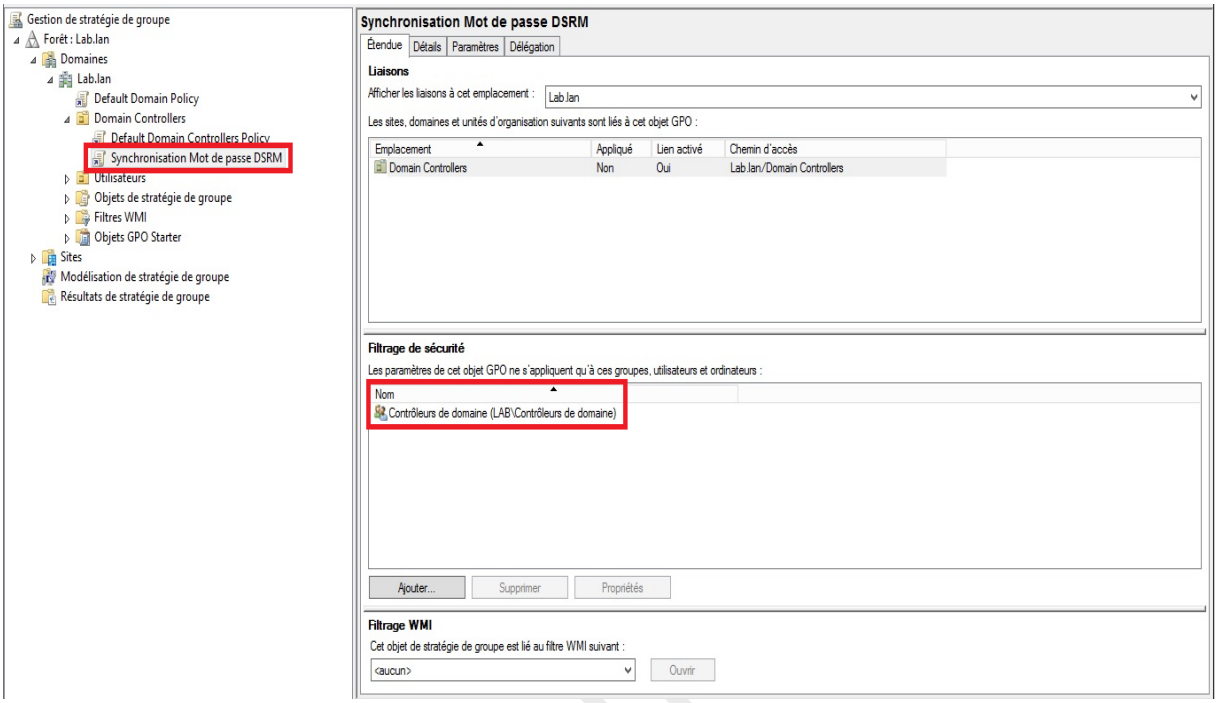
Puis nous lui spécifions un mot de passe :



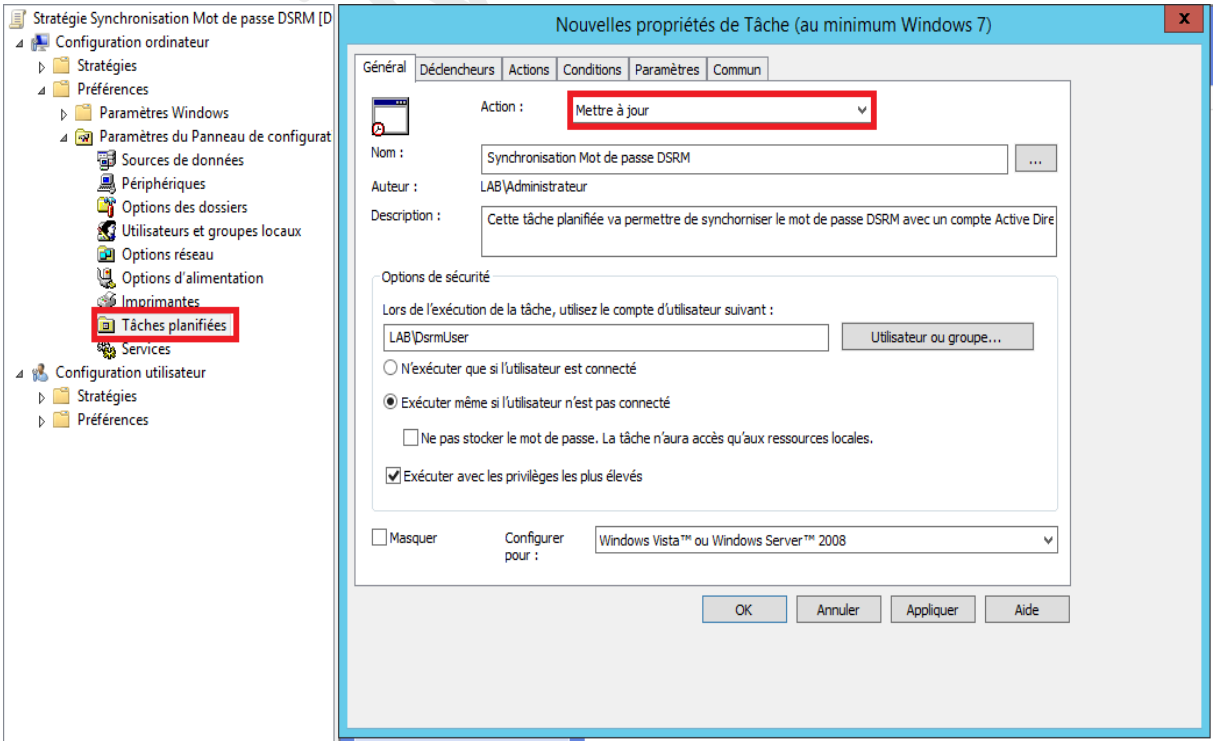
Voici donc le compte que nous avons créé :



Nous allons maintenant créer la tâche planifiée pour synchroniser automatiquement notre mot de passe DSRM avec le mot de passe du compte AD « DSRMUser » crée précédemment. Pour cela, nous allons commencer par créer une GPO que l'on appliquera à l'unité d'organisation « Domain Controllers ».



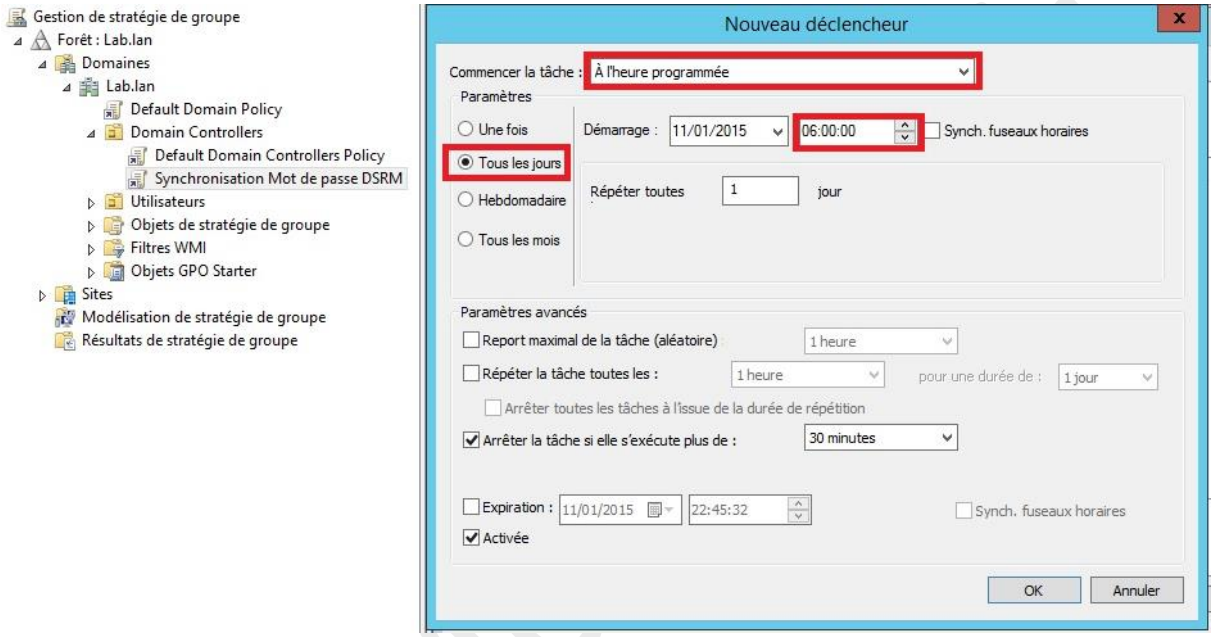
Il nous faut maintenant éditer notre GPO et créer la tâche planifiée. Nous utiliserons les stratégies de type « préférences » pour créer notre tâche planifiée.



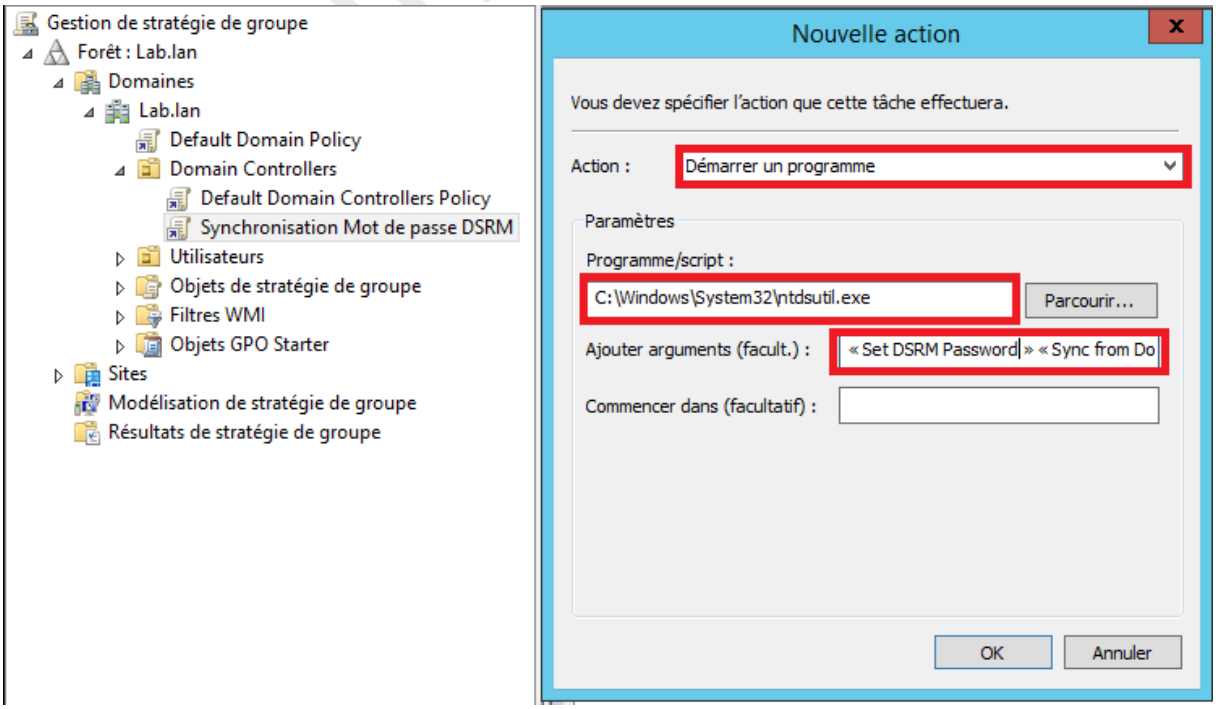
Nous utilisons le paramètre « Mettre à jour ». Ainsi si la stratégie n'est pas créée alors elle le sera.

Nous avons donné un nom à notre tâche planifiée et une description afin de pouvoir l'identifier rapidement.

Nous nous rendons maintenant sur l'onglet « Déclencheurs ». Nous créons un nouveau déclencheur et nous planifions un déclenchement tous les jours à 6h du matin. Ainsi, chaque jour le mot de passe de notre compte AD DSRM sera synchronisé avec le mot de passe du compte de domaine « DSRM User ».



Puis nous validons avec « OK ». Ensuite, nous nous rendons sur l'onglet « Actions » et nous créons une nouvelle action.



Puis, nous avons spécifié que la commande s'exécutera à partir de « **ntdsutil.exe** ».

Voici la commande passée en argument :

« Set DSRM Password » « Sync from Domain Account DSRMUser » Q Q

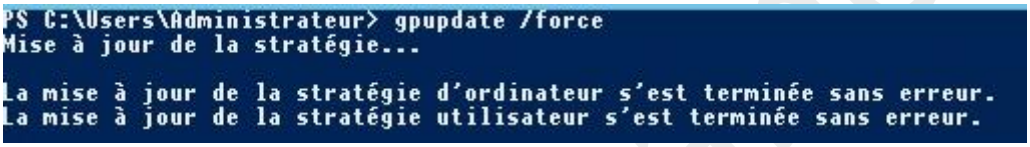
Copier / Coller la commande avec les guillemets !

Vous pouvez ensuite valider vos paramètres ou configurer d'autres options grâce aux autres onglets.

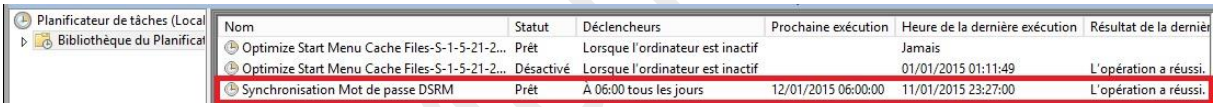
Une fois la stratégie configurée, il faut que celle-ci soit appliquée. Vous pouvez pour cela :

- Attendre 5 minutes. En effet, le « refresh » des GPO est d'environ 90 à 120 minutes sauf sur un contrôleur domaine ou le « refresh » est effectué toutes les 5 minutes.
- Redémarrer votre contrôleur de domaine. Les Gpo de type « Computer » sont appliquées à chaque fois que la machine redémarre.
- Effectuer un « gpupdate /force » pour appliquer immédiatement la GPO.

Dans notre exemple, nous exécutons un « gpupdate /force »

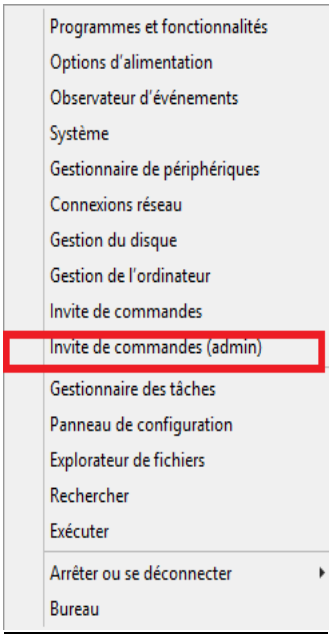


Nous pouvons ensuite vérifier que notre tâche planifiée a bien été créé :

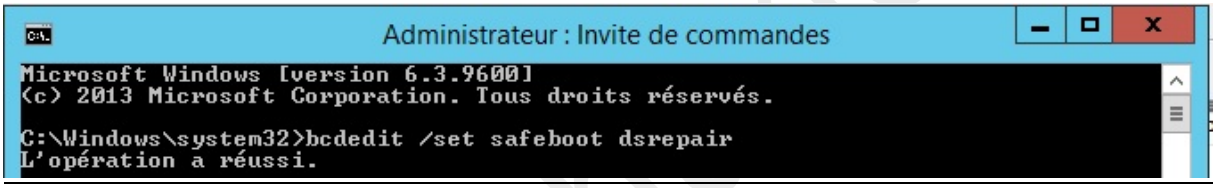


Il est important de rappeler que cette tâche planifiée sera créée sur l'ensemble des contrôleurs de domaine. Ainsi, chaque mot de passe DSRM sera synchronisé avec le mot de passe du compte simple utilisateur crée précédemment (DSRMUser). Veillez cependant à faire attention ! Synchroniser l'ensemble des comptes DSRM avec un compte AD peut compromettre l'intégrité de vos systèmes d'informations si le mot de passe de ce compte venait à être récupéré. N'hésitez pas à consulter des spécialistes sécurité !

Maintenant que notre mot de passe est synchronisé nous allons redémarrer notre contrôleur de domaine en mode DSRM. Pour cela, lancer votre « cmd.exe » **en tant qu'administrateur** :



Puis taper la commande suivante :



Vous pouvez ensuite redémarrer votre machine.

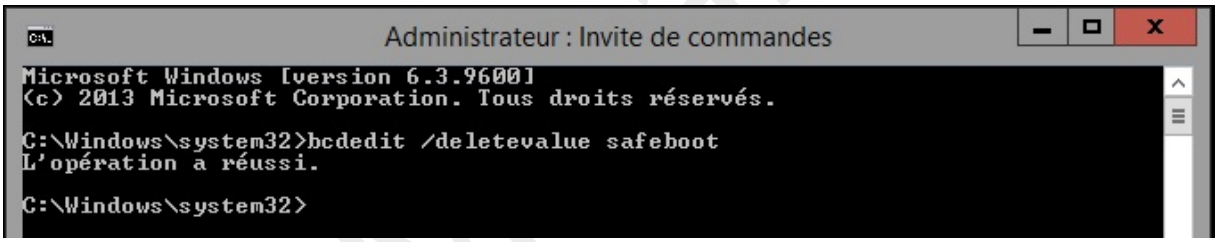
Puis vous pouvez vous connecter avec le compte Administrateur et saisir le mot de passe du compte DSRM que vous aviez saisie pour le compte « DSRM User ».

Cela fonctionne !

Le mot de passe du mode DSRM est maintenant synchronisé avec celui d'un compte du domaine.

Vous pouvez ainsi changer le mot de passe du compte simple utilisateur « DSRMUser » une fois par trimestre par exemple. Et celui-ci sera automatiquement synchronisé avec les différents contrôleurs de domaine. N'oubliez pas de mettre un mot de passe très complexe !

Pour quitter le mode DSRM vous devez lancer un invité de commande en mode admin et entrer la commande suivante :



Enfin, vous pouvez redémarrer votre machine.

Nous avons terminé !

Nous avons donc vu comment synchroniser le mot de passe DSRM entré initialement lors de l'installation de notre contrôleur de domaine avec le mot de passe d'un compte Active Directory classique.

Merci d'avoir suivi ce tutoriel !