

# Comment effacer le mot de passe Administrateur du domaine sous Windows Server 2003

Soumis par PasswordOne

20-04-2006

Dernière mise à jour : 13-11-2006

## Comment effacer le mot de passe Administrateur du domaine sous Windows Server 2003

### Description

Si vous avez oublié le mot de passe du compte 'Administrateur' du domaine sous Windows Server 2003, les 2 utilitaires Srvany et Instsrv vont vous permettre de le réinitialiser.

Les mots de passe des comptes de domaine sont stockés dans la base de données Active Directory sous %systemroot%\NTFS\ntds.dit.

### Les prérequis

- Avoir accès au serveur Contrôleur de Domaine (DC)
- Connaître le mot de passe du compte local : Administrateur (si vous ne l'avez pas vous pouvez utiliser l'utilitaire Offline NT Password & Registry Editor)
- Utiliser les 2 utilitaires Srvany et Instsrv

### Utilisation

- Démarrer en 'Mode restauration Active Directory (Contrôleurs de domaine Windows)' à l'aide de la touche F8 sur le serveur DC

- Ouvrir une session avec le compte local 'Administrateur'
- Copier les 2 utilitaires compressés Srvany.exe et Instsrv.exe dans un dossier temporaire de votre choix (par exemple d:\temp)
- Lancer l'invite de commande et taper la commande :

```
instsrv PassRecovery "d:\temp\srvany.exe"
```

- Lancer la base de registre avec regedit, et aller dans la clé de registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PassRecovery.
```

- Créer une nouvelle clé : Parameters et ajouter les 2 nouvelles valeurs caractères :

nom : Application  
type : Valeur caractère  
valeur : d:\temp\cmd.exe

nom : AppParameters  
type : Valeur caractère  
valeur : /k net user administrateur nouveau\_mot\_de\_passe

- Remplacer la valeur 'nouveau\_mot\_de\_passe' par celle de votre choix
- Ouvrir le gestionnaire des services depuis la commande services.msc
- Aller dans les propriétés du service PassRecovery et vérifier que le mode de démarrage (Startup type) est en mode : Automatic
- Dans l'onglet Log On cocher l'option Allow service to interact with desktop
- Redémarrer le serveur en mode normal, Srvany changera le mot de passe du compte de domaine 'Administrateur'
- La connexion se fera automatiquement et une fenêtre d'invite de commande sera lancée
- Taper impérativement les 2 commandes :

```
net stop PassRecovery  
sc delete PassRecovery
```

- Supprimer le dossier temporaire d:\temp
- Pour finir changer le mot de passe du compte de domaine 'Administrateur'