

Note

De :	Jean MARSAULT	À :	
		Copie :	
Date :	19 décembre 2014	Réf. :	Reference
Objet :	Prérequis CERTitude		



1. Introduction

Différents prérequis sont nécessaires au bon fonctionnement de CERTitude, afin de permettre la communication entre le poste de l'analyste et les postes cibles.

Ces prérequis sont donc séparés en deux parties distinctes :

- Les prérequis à mettre en œuvre par l'analyste ;
- Les prérequis à mettre en œuvre par l'organisation possédant les postes à analyser, qui peuvent être déployés par GPO.

Certains de ces prérequis ne concernent que le chiffrement des communications entre l'analyste et les cibles, et sont donc facultatifs si cette fonctionnalité n'est pas requise.



2. Poste analyste

2.1. Prérequis nécessaires

Le poste réalisant l'analyse doit être en mesure de se connecter sur les postes cibles de l'analyse. Pour cela, l'analyste doit :

- Connecter son poste sur le même réseau que les postes à analyser ;
- Disposer d'un compte faisant partie du groupe « Administrateurs locaux » de chaque poste analysé. Pour cela, trois solutions s'offrent à l'analyste :
 - ▶ (1) : Créer un compte de domaine, ajouté par GPO au groupe « Administrateurs locaux » des postes ;
 - ▶ (2) : Créer un compte de domaine membre du groupe « Administrateurs du domaine » ;
 - ▶ (3) : Déployer par GPO un compte local membre du groupe « Administrateurs locaux » sur chaque poste (compte identique sur tous les postes).

En termes de sécurité, la solution (1) est à préférer.

2.2. Prérequis facultatifs

Les prérequis facultatifs concernent l'établissement de communications chiffrées. La solution retenue par CERTitude pour effectuer le chiffrement des messages est IPSec. Par conséquent :

- L'analyste devra s'assurer que le **port 500** (UDP) de son poste est ouvert en provenance des postes à analyser ;
- L'analyste devra déployer le politique de sécurité IPSec CERTitude (voir □) :
 - ▶ Sur **Windows XP / Server 2003**, en utilisant l'outil *ipseccmd* :

```
ipseccmd import reg certitude.ipsec
```

- ▶ Sur **Windows Vista** et **ultérieur** :

```
netsh ipsec static importpolicy certitude.ipsec
```



3. Postes analysés

3.1. Prérequis nécessaires

Lors de l'analyse, le poste de l'investigateur doit pouvoir déployer le service d'exécution de commandes à distance sur le poste cible. D'un point de vue technique, cela impose que :

- les partages d'administration par défaut soient activés ;
- les partages réseaux du poste cible autorisent l'authentification ;
- le poste cible soit joignable par le poste de l'analyste sur les ports 139 (NetBios Session Service) et 445 (Microsoft Directory Services, SMB).

3.1.1. Activation des partages d'administration par défaut

Les partages d'administration par défaut sont automatiquement activés dès lors que le service *lanmanserver* est activé :

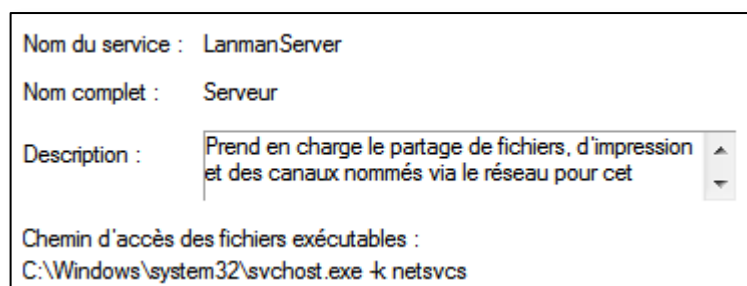


Figure 1 : Service « Serveur »

L'activation de ce service peut être **réalisée par GPO**.

3.1.2. Autorisation de l'authentification

L'explorateur de fichiers Windows propose, via le menu « Options des dossiers et de recherche > Affichage > Paramètres avancés > Utiliser le partage simple / l'assistant partage », de désactiver l'authentification lors de l'accès aux partages réseau :

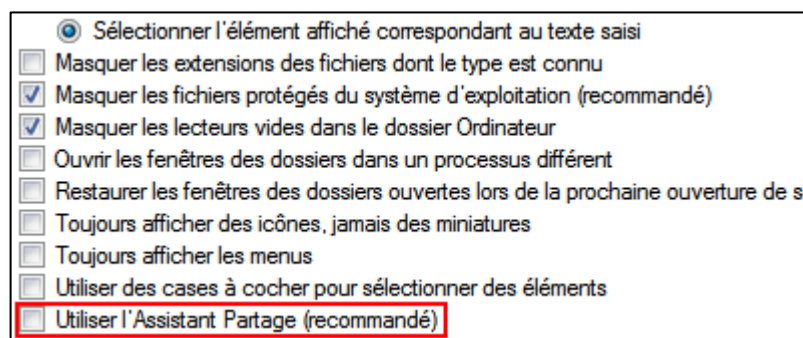


Figure 2 : Partage « simple » de fichiers



Cette option empêche l'authentification en tant que membre du groupe « Administrateurs locaux » et par conséquent l'accès aux partages d'administration par défaut.

La **désactivation par GPO** peut se faire en passant la valeur *force_guest* à 0 dans la clé de registre *HKLM\SYSTEM\ControlSet001\Control\Lsa* :

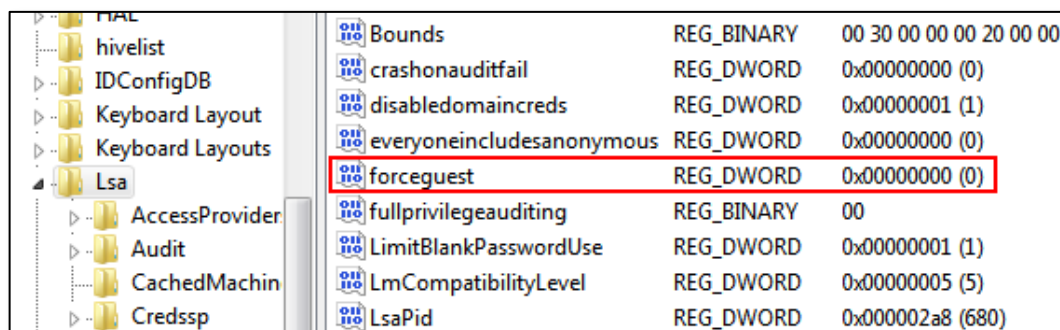


Figure 3 : Désactivation du « partage simple » par le registre

3.1.3. Configuration du pare-feu : ouverture des ports

Dans le cas où l'un des profils du pare-feu des machines cibles serait activé, il est nécessaire que les ports suivants soient ouverts :

- **139 TCP** : *NetBios Session Service*, requis pour l'ouverture des sessions distantes ;
- **445 TCP** : *Microsoft Directory Services*, utilisés pour le déploiement du service de communication à distance *RemComSvc* et les échanges de fichiers.

Ces paramètres peuvent être déployés par GPO depuis le composant suivant :

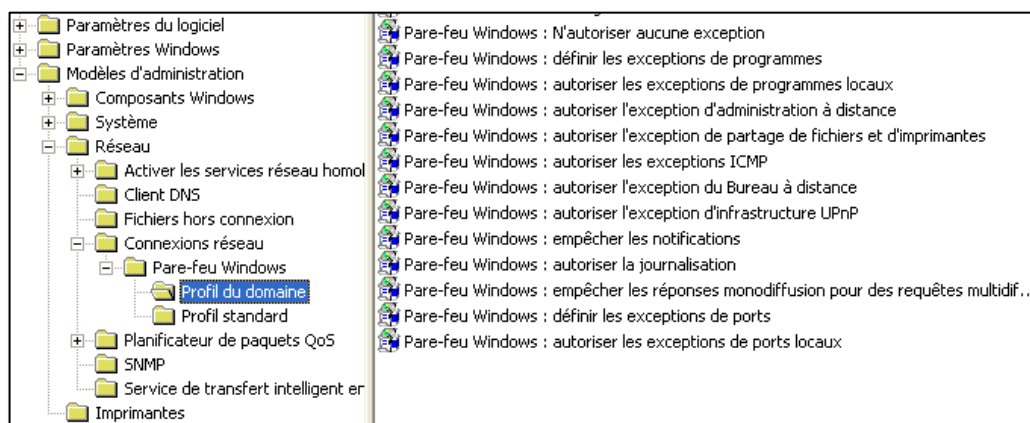


Figure 4 : Réglages du pare-feu Windows par GPO

Les exceptions à ajouter correspondent donc aux chaînes de caractères suivantes :

```
139:TCP:<ip_analyste>:enabled:Netbios-ssn
445:TCP:<ip_analyste>:enabled:Microsoft-ds
```



3.2. Prérequis facultatifs

Les prérequis facultatifs concernent l'établissement de communications chiffrées. La solution retenue par CERTitude pour effectuer le chiffrement des messages est IPSec. Par conséquent :

- Les postes analysés devront être en mesure de recevoir des communications chiffrées sur le port 500 (UDP), opération qui peut être déployée par GPO (voir partie **Erreur ! Source du renvoi introuvable.**), via la chaîne de caractères suivante :

```
500:UDP:<ip_analyste>:enabled:IPSec
```

- Ces postes devront déployer le politique de sécurité IPSec CERTitude (voir ☐). Cette opération est réalisable par GPO :

Racine de la console	Nom	Stratégie attribuée	Description
Stratégies de sécurité IP	CERTitude	Oui	Stratégie de sécurité permettant le chiffrem.

Figure 5 : Déploiement de la stratégie de sécurité par GPO



Annexe 1. Création de la politique de sécurité IPSec CERTitude


La politique de sécurité déployée par CERTitude permet de définir dans quels cas le chiffrement des communications doit être effectué. Elle spécifie également les paramètres d'échange des clés (via le protocole IKE), ainsi que les différents aspects du chiffrement (algorithmes utilisés, durée de vie des clés...).

Si l'analyste dispose d'un poste sous Windows XP SP2, le script « gen_sec_strat.bat » à disposition dans le répertoire « utils » sera suffisant pour créer les deux stratégies de sécurité IP.

Dans le cas contraire, la démarche suivante permettent la création pas-à-pas de la politique de sécurité CERTitude depuis une console MMC, ainsi que l'exportation de cette politique.



1.1. Ouverture de la console MMC et ajout du composant enfichable

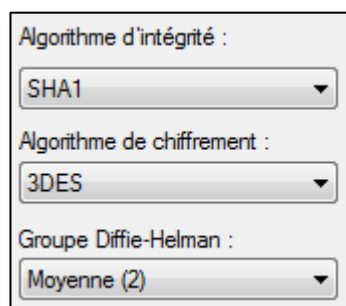
- Appuyez sur les touches  et R pour ouvrir la fenêtre « **Exécuter** » et lancez le programme « **mmc** ».
- Naviguez dans *Fichier > Ajouter/supprimer un composant logiciel enfichable* et ajoutez le composant « **Stratégies de sécurité IP** ».
- Cliquez sur *Action > Créer une règle de stratégie IP* :
 - Fournissez un nom et une description pour cette stratégie.
 - Ne cochez pas le paramètre « **Activer la règle de réponse par défaut** ».
 - Choisissez de « **Modifier les propriétés** ».

1.2. Paramètres de l'échange des clés (IKE)

- Rendez-vous dans l'onglet « **Général** ».
- Mettre la valeur de « **Vérifier les modifications de stratégie toutes les** » à **180 minutes**.
- Cliquez sur « **Paramètres** » et changez la valeur des paramètres suivants :

Paramètre	Valeur
Clé principale PFS	décoché
Authentifier et générer une nouvelle clé toutes les	480 minutes / 0 session(s)

- Cliquez sur « **Méthodes** » et ajoutez la méthode suivante :



Algorithme d'intégrité :
SHA1

Algorithme de chiffrement :
3DES

Groupe Diffie-Helman :
Moyenne (2)

Figure 6 : Paramètres de l'échange des clés



1.3. Configuration des filtres IP

- Revenez sur les propriétés principales et allez dans l'onglet « **Règles** ».
- Cliquez sur le bouton « **Ajouter...** » afin de créer une nouvelle règle.

1.3.1. Onglet « Liste des filtres IP »

- Ajoutez un filtre IP et nommez-le.
- Ajoutez une règle de filtre IP par port à ouvrir (139 et 445) :
 - Onglet « **Adresses** » :

Paramètre	Valeur
Adresse source	Mon adresse IP
Adresse de destination	Toutes les adresses IP OU Adresse du sous-réseau cible
Miroir	Coché

Tableau 1 : Paramètres du poste de l'investigateur

Paramètre	Valeur
Adresse source	<ip_investigateur>
Adresse de destination	Mon adresse IP
Miroir	Coché

Tableau 2 : Paramètres des postes cibles

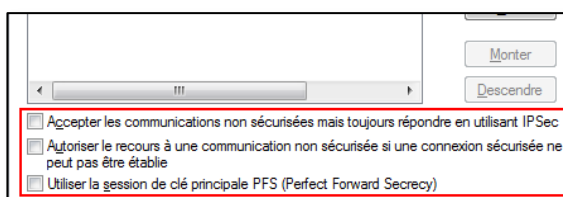
- Onglet « **Protocole** » :

Paramètre	Valeur
Type de protocole	TCP
Depuis le port	Depuis n'importe quel port
Vers le port	139 ou 445

- Onglet « **Description** » : entrez une brève description de la règle.

1.3.2. Onglet « Action de filtrage »

- Ajoutez une nouvelle action de filtrage et nommez-là dans son onglet « **Général** ».
- Choisissez l'option « **Négocier la sécurité** » et ne cochez aucune des trois options entourées en rouge :



- Ajoutez une méthode de sécurité « **Personnalisée** » comme suit :

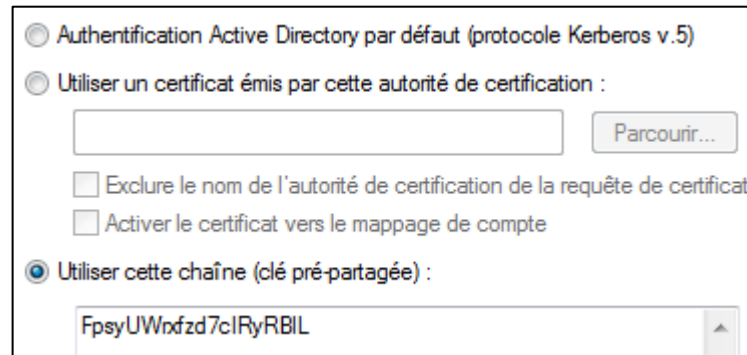
Paramètre	Valeur
Intégrité des adresses et des données sans chiffrement	décoché
Chiffrement et intégrité des données	SHA1 – 3DES
Générer une nouvelle clé tous les	100000Ko / 3600s



1.3.3. Onglet « Méthodes d'authentification »

Dans le cas de CERTitude, la méthode utilisée pour établir un canal de communication chiffré entre deux postes est la **clé pré-partagée** (PSK). Celle-ci doit être **aléatoire** et **différente** pour chaque vague d'analyse.

Ajoutez une seule et unique méthode d'authentification, définie comme suit :



The screenshot shows the 'Authentication Methods' tab in the Windows Security Policy console. It contains three radio button options: 'Authentication Active Directory par défaut (protocole Kerberos v.5)', 'Utiliser un certificat émis par cette autorité de certification :', and 'Utiliser cette chaîne (clé pré-partagée)'. The third option is selected. Below it is a text box containing the string 'FpsyUWxfzd7cIRyRBIL'. There are also checkboxes for 'Exclure le nom de l'autorité de certification de la requête de certificat' and 'Activer le certificat vers le mappage de compte', both of which are unchecked. A 'Parcourir...' button is next to the certificate authority text box.

Figure 7 : Méthode d'authentification utilisée par CERTitude présentant une clé aléatoire

1.3.4. Onglets « Paramètres du tunnel » et « Type de connexion »

Les options suivantes doivent être choisies :

- « Cette règle ne spécifie aucun tunnel IPSec » ;
- « Toutes les connexions réseaux ».

1.4. Exportation de la stratégie de sécurité

1.4.1. Sous Windows XP / Server 2003

Installez tout d'abord l'outil *ipseccmd*, puis exécutez la commande suivante :

```
ipseccmd export reg certitude.ipsec
```

1.4.2. Sous Windows Vista et ultérieur

Exécutez la commande suivante avec des privilèges administrateurs :

```
netsh ipsec static exportpolicy certitude.ipsec
```

