Atelier : Chiffrement EFS dans un domaine

1. Objectif

Dans l'atelier pratique de ce chapitre, nous allons revenir sur l'utilisation du système de chiffrement EFS. L'implémentation de ce système en mode Groupe de travail (Workgroup) nous a déjà permis de comprendre concrètement les notions de cryptographie de base et de certificat associées (voir chapitre Cryptographie). Le système EFS sera ici implémenté dans le contexte d'un domaine Active Directory afin d'illustrer le déploiement automatique de certificat pour les utilisateurs d'un domaine.

Les ordinateurs virtuels utilisés dans cet atelier sont les suivants :

S1 : contrôleur de domaine (Corp.lan)

S2 : autorité de certification (CorpRootCA)

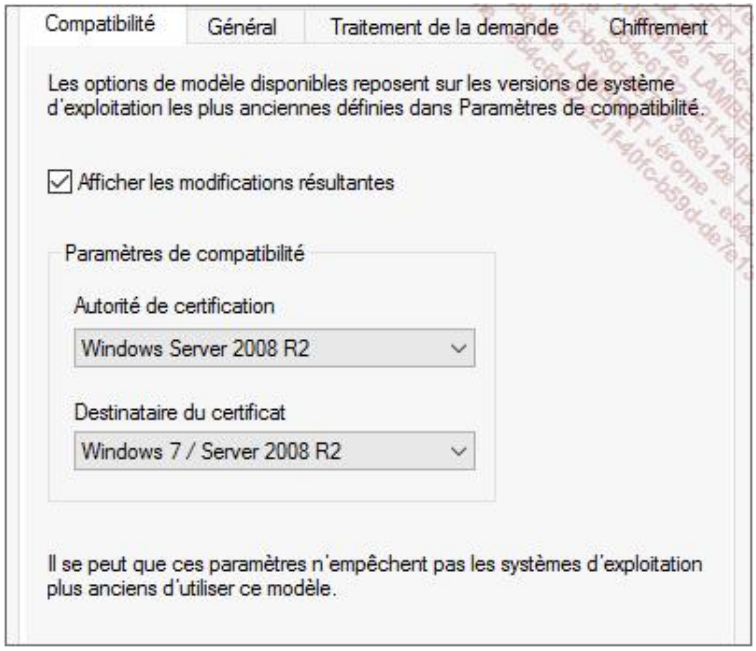
W10 : ordinateur client du domaine (Corp.lan)

2. Créer un nouveau modèle de certificats EFS Basique

- Ouvrez la console de gestion Autorité de certification.
- Développez CorpRootEntCA.
- Faites un clic droit sur **Modèles de certificats** et sélectionnez le menu **Gérer**.

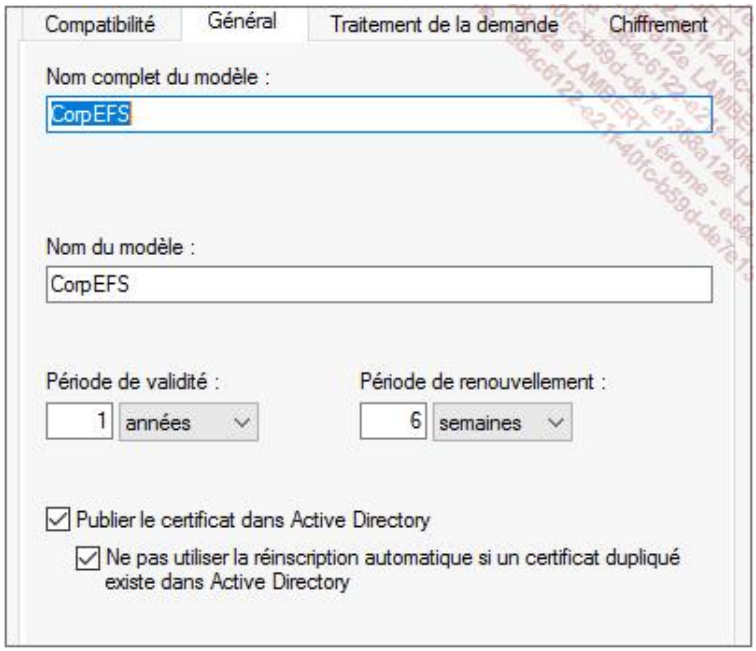
La console de gestion Modèles de certificats s'affiche.

- Faites un clic droit sur le modèle **EFS Basique** et sélectionnez le menu **Dupliquer le modèle**.
- Sélectionnez l'onglet **Compatibilité**, développez la liste déroulante **Autorité de certification**, sélectionnez **Windows 2008 r2** et cliquez le bouton **OK** pour accepter les modifications résultantes.
- Développez la liste déroulante **Destinataire du certificat**, sélectionnez **Windows 7 / Server 2008 R2** et cliquez le bouton **OK** pour accepter les modifications résultantes.



Attention, le niveau de compatibilité le plus élevé que l'on puisse appliquer sur le nouveau modèle est Windows 2008 R2 et client Windows 7. Voir https://social.technet.microsoft.com/Forums/windowsserver/en-US/59fbb2cb-8bde-4c9d-b61c-a11e1aa5bbd4/ws2012r2-gpmc-mmc-appcrash-when-trying-to-change-efs-certificate-template-in-gpo?forum=winserver8gen.

- Sélectionnez l'onglet **Général**, saisissez **Corp EFS** dans la zone **Nom complet du modèle** puis cochez les cases **Publier le certificat dans Active Directory** et **Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory**.

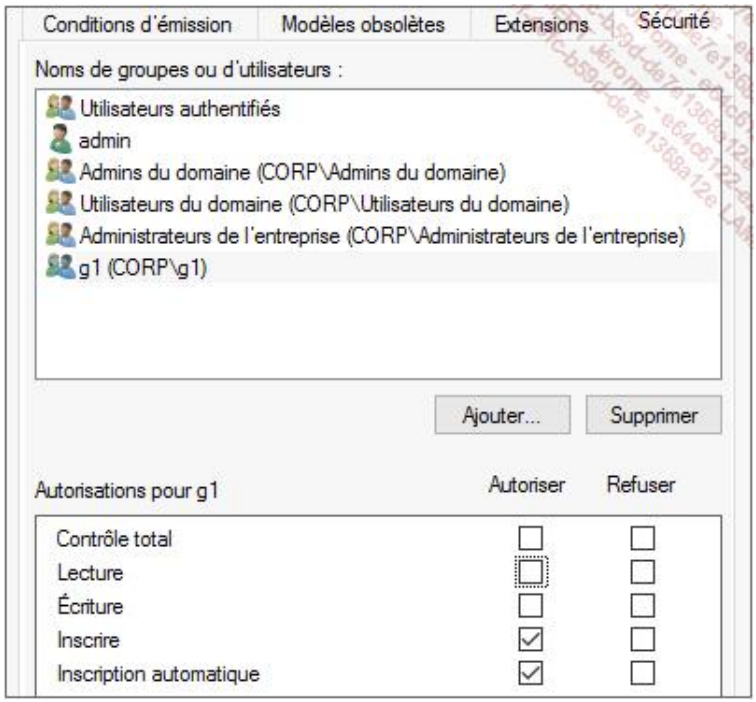


Les cases à cocher de publication garantissent l'utilisation d'un certificat unique pour EFS sur les ordinateurs clients.

- Sélectionnez l'onglet **Sécurité**, ajoutez le groupe g1 puis cochez les autorisations **Inscrire** et **Inscription automatique** pour ce groupe dans la zone **Autorisations pour g1**.

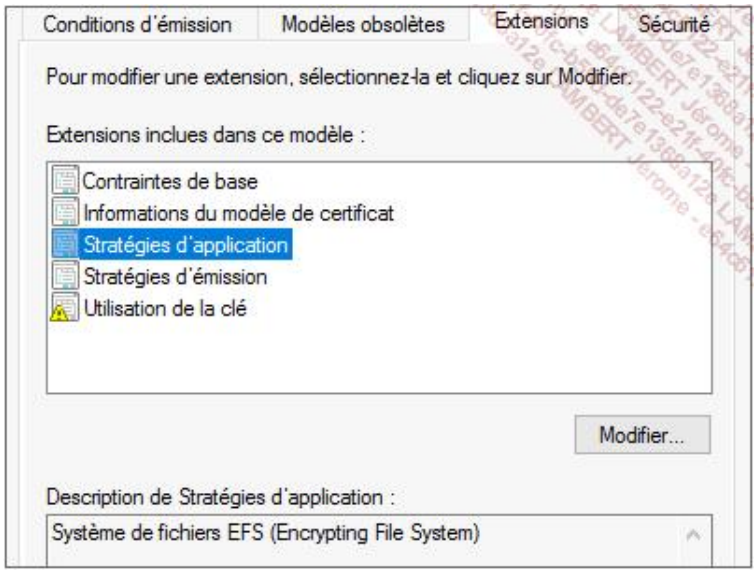
Ce groupe a été créé lors de la mise en place de la maquette de test et contient les utilisateurs du domaine u1, u2, u3 et u4.

- Décochez toutes les autorisations pour le groupe Utilisateurs du domaine.



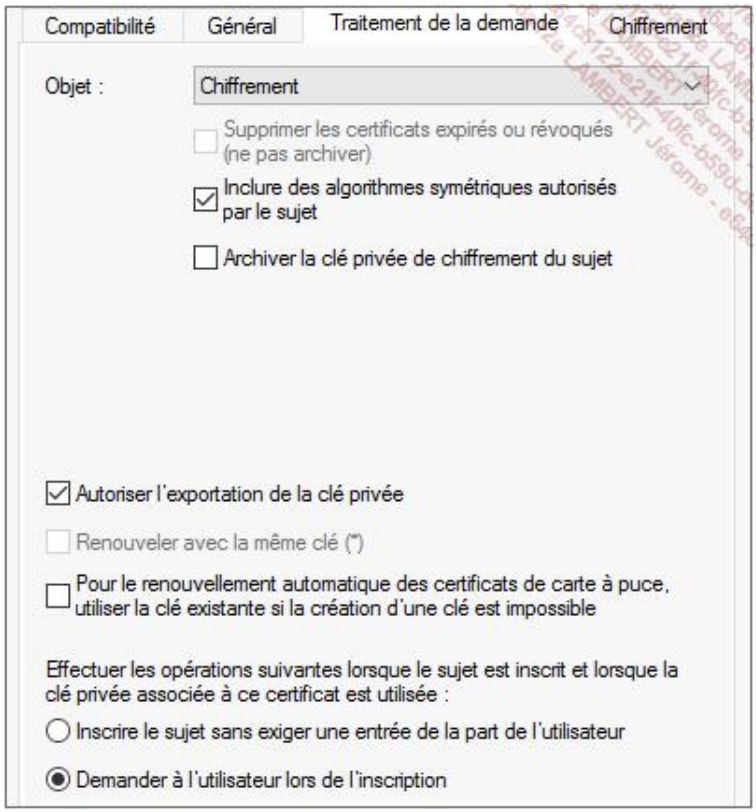
*Les utilisateurs obtiennent l'autorisation **Lecture** par le groupe Utilisateurs authentifiés qui dispose de cette autorisation par défaut.*

- Sélectionnez l'onglet **Extensions**, sélectionnez **Stratégies d'application** et validez que la zone **Description de stratégies d'application** contient la stratégie **Système de fichiers EFS (Encrypting File System)**.



Ce modèle ne dispose que d'une stratégie et ne peut être utilisé que pour le chiffrement de fichier EFS.

- Sélectionnez l'onglet **Traitement de la demande** et cochez les cases **Autoriser l'exportation de la clé privé** et **Demander à l'utilisateur lors de l'inscription**.



*L'option **Demander à l'utilisateur lors de l'inscription** affiche une notification dans la barre de tâches lors de l'inscription automatique d'un certificat. Elle n'est utilisée ici qu'à titre pédagogique et ne doit pas être utilisée en production.*

- Fermez la fenêtre de gestion Modèles de certificats.

Publier le nouveau modèle de certificat

- Dans la fenêtre Autorité de certification, faites un clic droit sur **Modèles de certificats** et sélectionnez les menus **Nouveau\Modèle de certificat à délivrer**.
- Dans la fenêtre Activer les modèles de certificats, sélectionnez le modèle de certificat **Corp EFS** et cliquez sur le bouton **OK**.

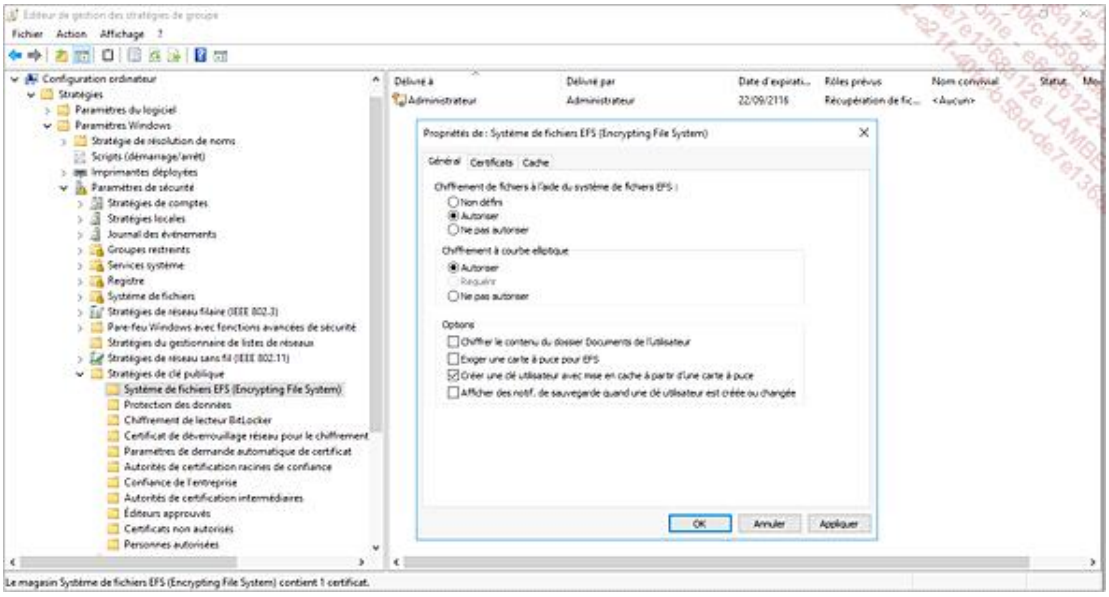
  Le nouveau modèle de certificat peut maintenant être distribué par l'autorité de certification.

3. Modifier le modèle de certificat utilisé pour EFS

Le modèle de certificat utilisé dans un domaine est codé en dur dans le système. Par défaut, seul le modèle EFS Basique est utilisable. Nous allons utiliser une stratégie de groupe pour forcer à la place l'usage de notre modèle personnalisé Corp EFS.

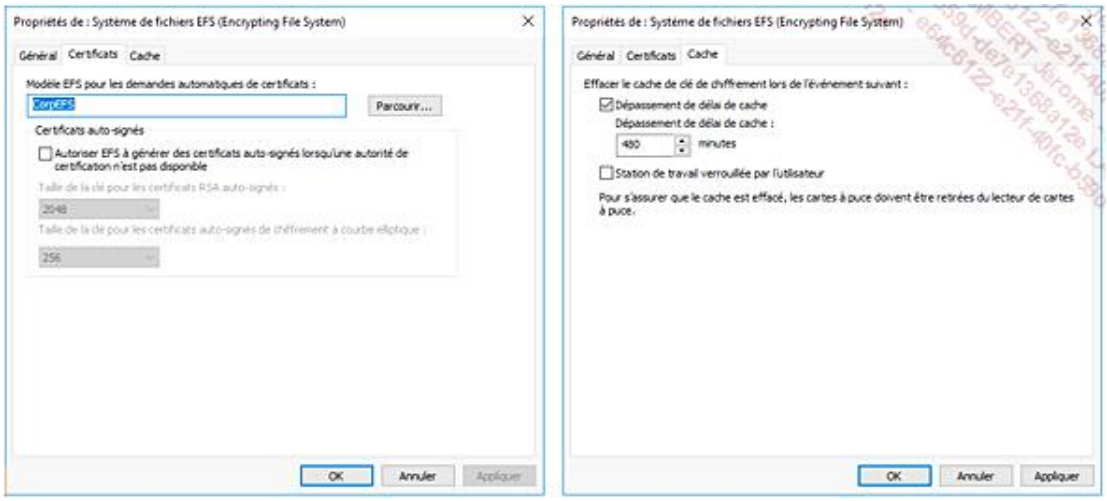
- Connectez-vous sur le contrôleur de domaine s1 en tant que Corp/admin.
- Ouvrez la console de gestion Gestion des stratégies de groupe et développez **Gestion de stratégie de groupe\Forêt:corp.lan\Domaines\corp.lan\Objets de stratégie de groupe**.
- Faites un clic droit sur **Default Domain Policy** et sélectionnez le menu **Modifier**.
- Dans la console Editeur des stratégies de groupe, développez **Configuration ordinateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**.

- Faites un clic droit sur **Système de fichiers EFS (Encrypting File System)** et sélectionnez le menu **Propriétés**.
- Dans la zone **Chiffrement de fichiers à l'aide du système de fichiers EFS**, cochez la case **Autoriser**.



Les paramètres de stratégies EFS permettent d'indiquer, entre autres, si le chiffrement EFS doit être autorisé ou refusé dans le domaine et si des cartes à puces doivent être utilisées.

- Sélectionnez l'onglet **Certificat**, cliquez sur le bouton **Parcourir** et sélectionnez le modèle de certificat **CorpEFS**.
- Décochez la case **Autoriser EFS à générer des certificats autosignés lorsqu'une autorité de certification n'est pas disponible**.



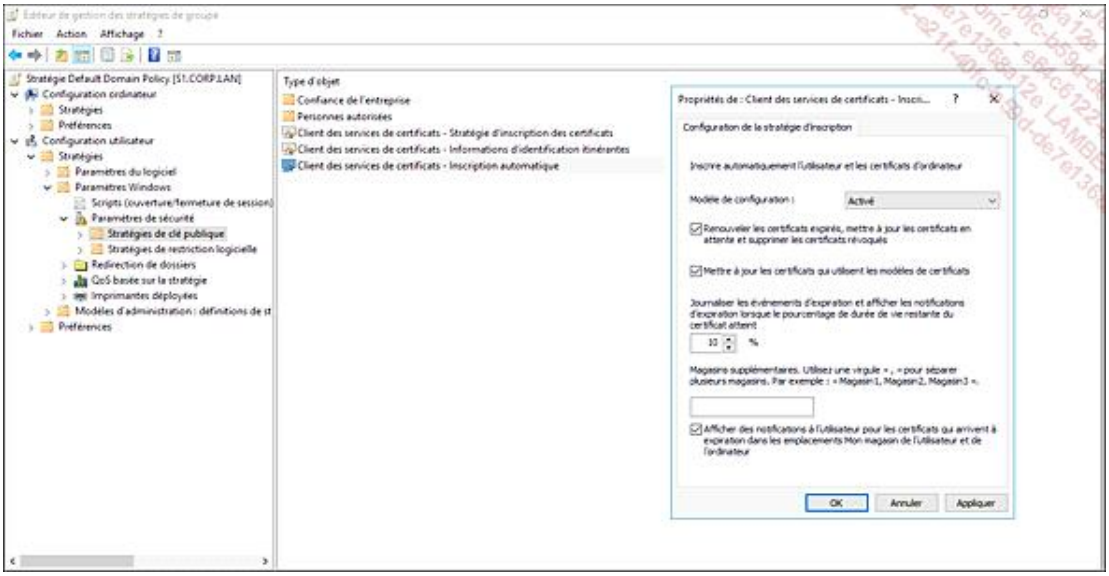
D'autres options permettent de contrôler le modèle EFS utilisé pour le chiffrement ainsi que les durées de mise en cache des clés de chiffrement.

- Cliquez sur le bouton **OK**.

4. Déploiement de certificat par stratégie de groupe

Nous allons modifier la stratégie par défaut du domaine afin d'activer le déploiement automatique de certificats par stratégies de groupe.

- Connectez-vous sur le contrôleur de domaine s1 en tant que Corp/admin.
- Ouvrez la console de gestion Gestion des stratégies de groupe et développez **Gestion de stratégie de groupe\Forêt:corp.lan\Domaines\corp.lan\Objets de stratégie de groupe**.
- Faites un clic droit sur **Default Domain Policy** et sélectionnez le menu **Modifier**.
- Dans la console Editeur des stratégies de groupe, développez **Configuration utilisateur\Stratégies\Paramètres Windows\Paramètres de sécurité\Stratégies de clé publique**.
- Faites un clic droit sur **Paramètres inscription automatique**.
- Développez la liste **Modèle de configuration** et sélectionnez **Activé**.
- Cochez la case **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués**.
- Cochez la case **Mettre à jour les certificats qui utilisent les modèles de certificats**.
- Cochez la case **Afficher des notifications à l'utilisateur pour les certificats qui arrivent à expiration dans les emplacements Mon magasin de l'utilisateur et de l'ordinateur**.
- Cliquez sur le bouton **OK**.
- Fermez les consoles de gestion Editeur de stratégies de groupe et Gestion des stratégies de groupe.



Activation du déploiement automatique des certificats utilisateur par stratégies de groupe.

5. Chiffrement EFS

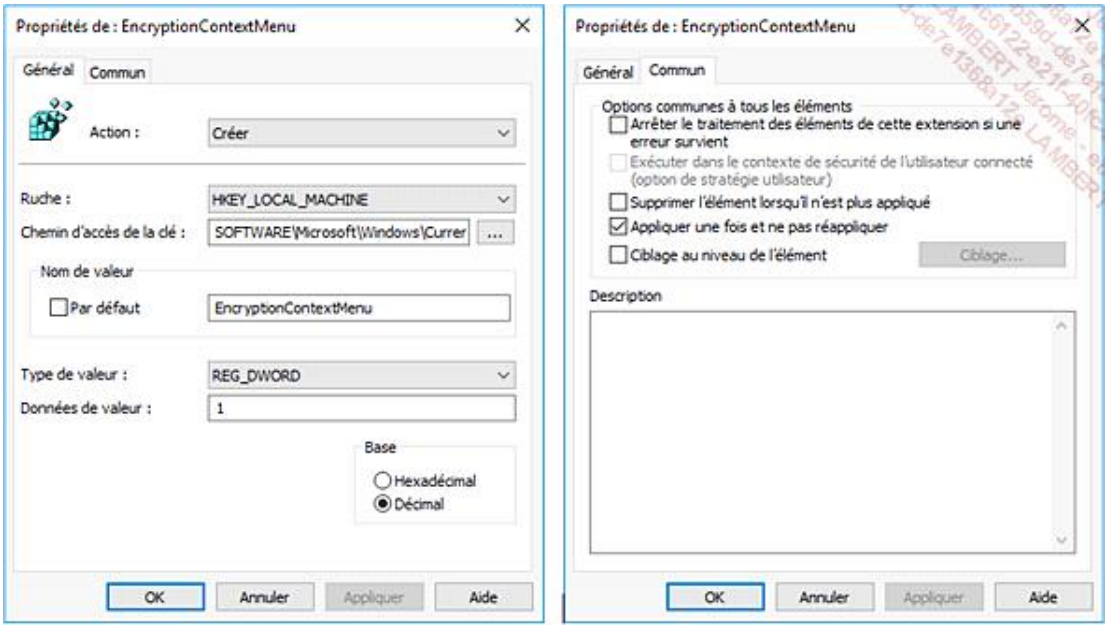
a. Menu contextuel pour le chiffrement

Afin de simplifier les manipulations de chiffrement de fichier, nous allons implémenter une stratégie de préférence permettant de disposer d'un menu contextuel pour le chiffrement.

- Connectez-vous sur le contrôleur de domaine s1 en tant que Corp/admin.
- Ouvrez la console de gestion Gestion des stratégies de groupe et développez **Gestion de stratégie de**

groupe\Forêt:corp.lan\Domaines\corp.lan\Objets de stratégie de groupe.

- Faites un clic droit sur **Default Domain Policy** et sélectionnez le menu **Modifier**.
- Dans la console Editeur des stratégies de groupe, développez **Configuration ordinateur\Préférences\Paramètres Windows**.
- Faites un clic droit sur **Registre** et sélectionnez les menus **Nouveau\Eléments registre**.
- Développez la liste déroulante **Action** puis sélectionnez **Créer**.
- Développez la liste déroulante **Ruche** puis sélectionnez **HKEY_LOCAL_MACHINE**.
- Dans la zone **Chemin d'accès de la clé**, cliquez sur le bouton … puis développez **HKLM\Software\Microsoft\Windows\Currentversion\Explorer\Advance**.
- Dans la zone **Nom de valeur**, saisissez **EncryptionContextMenu**.
- Développez la liste déroulante **Type de valeur** et sélectionnez **REG_DWORD**.
- Dans la zone **Données de valeur**, saisissez **1**.
- Sélectionnez l'onglet **Commun** puis cochez la case **Appliquer une fois et ne pas réappliquer**.



La stratégie de préférence crée le menu contextuel de chiffrement une seule fois.

b. Validation du certificat EFS

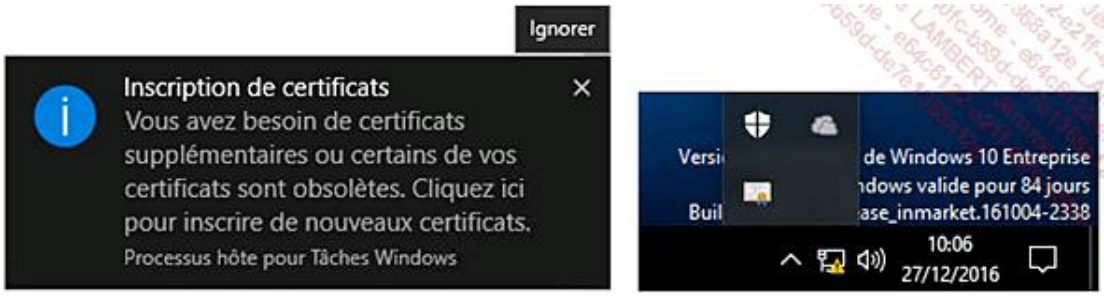
- Redémarrez l'ordinateur client w10.

  Toutes les nouvelles stratégies d'ordinateur s'appliquent au redémarrage.

- Connectez-vous sur le client w10 en tant que corp/u1.

  Attendez qu'une notification apparaisse à droite de la barre de tâches indiquant le déploiement d'un certificat pour le système EFS.

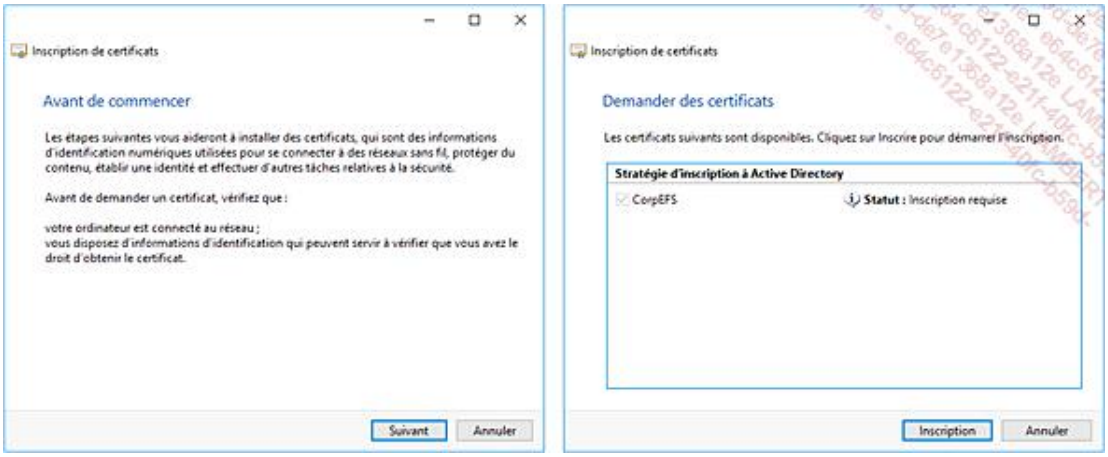
- Cliquez sur l'icône de notification **Inscription de certificats**.



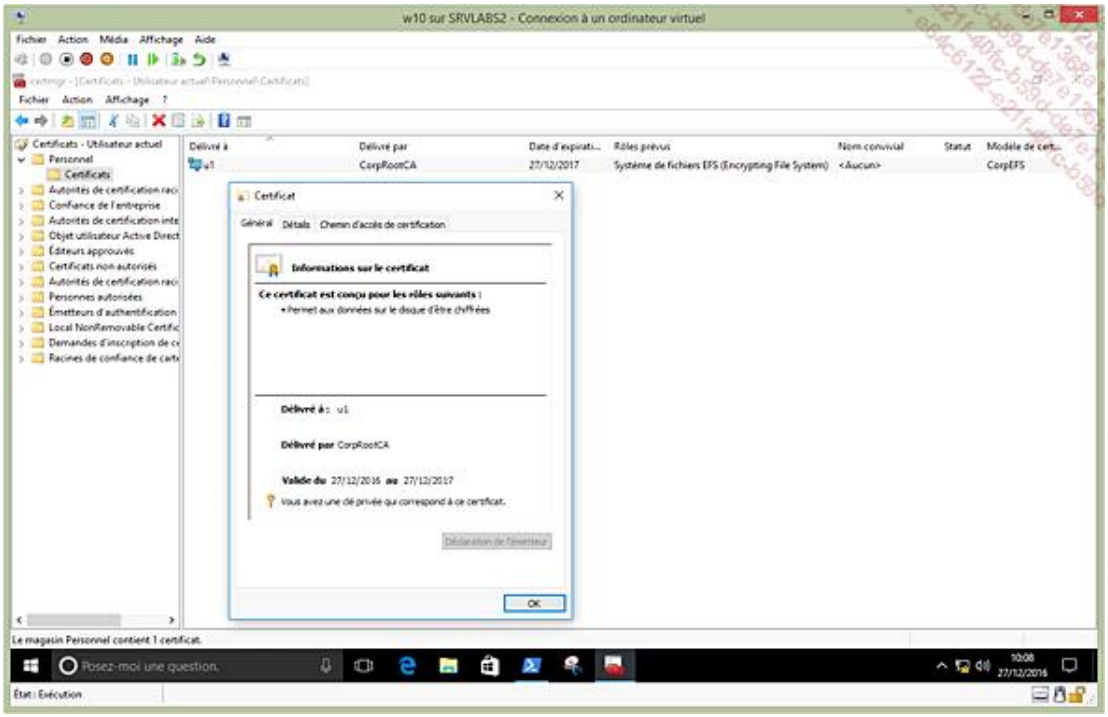
La notification d'inscription de certificat s'affiche après l'ouverture de session. Si vous l'avez ratée, cliquez sur ˆ (bouton afficher les icônes cachées de la zone de notification) et cliquez sur l'icône représentant un certificat.

Si l'icône de notification d'inscription de certificat ne s'affiche pas, vérifiez le paramétrage des stratégies de groupe, exécutez les commandes **`Gpupdate`** et **`Certutil -pulse`** sur le client w10 et redémarrez le client.

- Dans la fenêtre Inscription de certificat, cliquez sur le bouton **Suivant** puis sur les boutons **Inscription** et **Fermer**.



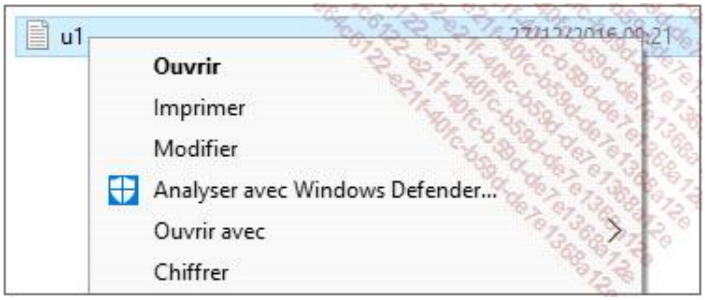
- Ouvrez une invite de commande et exécutez la commande **`Certmgr.msc`**.
- Développez **Certificat\Utilisateur Actuel\Personnel\Certificats** et validez que vous disposez bien d'un certificat valide pour le chiffrement EFS.



Le certificat obtenu est basé sur le modèle CorpEFS et délivré par notre autorité de certification CorpRootCA !

c. Chiffrement de fichiers EFS

- Créez un dossier c:\Efs et créez un fichier nouveau document texte nommé u1 dans le dossier c:\Efs.
- Ouvrez le nouveau document texte nommé u1, ajoutez-y un contenu et sauvegardez-le.
- Faites un clic droit sur le fichier nommé u1 et sélectionnez le menu **Chiffrer**.



Le nouveau menu contextuel ajouté par notre stratégie de groupe simplifie le chiffrement des fichiers !

- Dans la boîte de dialogue Avertissement de chiffrement, cochez **Chiffrer le fichier uniquement** puis cochez **Toujours chiffrer les fichiers uniquement**.
- Cliquez sur le bouton **OK.**

Le fichier u1 est maintenant chiffré. Le symbole cadenas apparaît en haut à gauche de l'icône (visible en mode affichage Grandes icônes).