# Atelier : Agent de récupération EFS dans un domaine

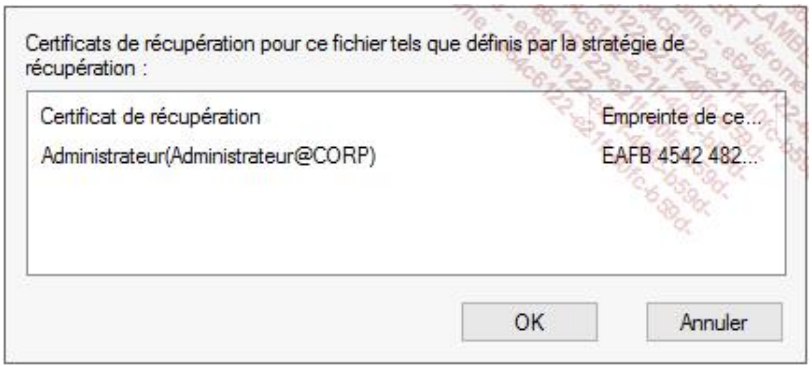
Nous allons implémenter le compte utilisateur Corp/Admin en tant qu'agent de récupération EFS de domaine et tester la récupération de fichiers chiffrés.

## 1. Supprimer l'ancien agent de récupération EFS

Nous allons supprimer le certificat autosigné d'agent de récupération généré automatiquement par le système d'exploitation Microsoft pour le remplacer par un certificat d'agent de récupération signé par notre autorité de certification.

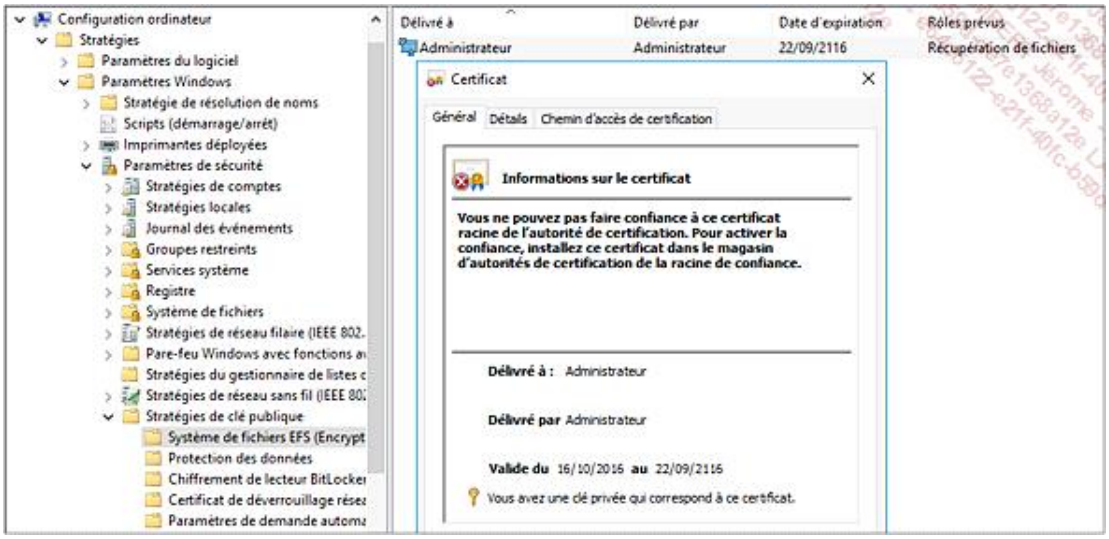
### Supprimer le certificat autosigné

- Faites un clic droit sur le fichier u1 et sélectionnez le menu **Propriétés**.
- Cliquez sur le bouton **Avancé** puis sur le bouton **Détails**.
- Vérifiez que la zone **Certificats de récupération pour ce fichier tels que définis par la stratégie de récupération** indique qu'il existe actuellement un certificat d'agent de récupération pour le compte administrateur du domaine Corp.




*Un certificat d'agent de récupération est présent par défaut dans le domaine.*

- Fermez toutes les fenêtres du certificat de l'utilisateur u1.
- 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\Système de fichiers EFS (Encrypting File System)**.
- Dans la zone de droite, double cliquez sur le certificat Administateur.
- Validez qu'il s'agit d'un certificat autosigné (délivré à Administrateur par Administrateur).




*Le certificat d'agents de récupération présent par défaut est autosigné !*

- Cliquez sur le bouton **OK** pour fermer le certificat.
- Supprimez le certificat autosigné (cliquez sur le bouton **Oui** pour supprimer définitivement le certificat autosigné).

## 2. Obtenir un certificat d'agent de récupération EFS

### Personnaliser le modèle Agent de récupération EFS

- Connectez-vous sur l'autorité de certification s2 en tant que Corp/admin.
- Ouvrez la console de gestion Autorité de certification et 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 **Agent de récupération EFS** 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.
- Sélectionnez l'onglet **Général**, saisissez **Corp Agent de récupération EFS** dans la zone **Nom complet du modèle**.
- Cochez les cases **Publier le certificat dans Active Directory** et **Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory**.
- Sélectionnez l'onglet **Sécurité**, sélectionnez le compte **Admin** puis cochez les autorisations **Lecture**, **Ecriture** et **Inscrire**.

L'autorisation **Ecriture** n'est pas obligatoire pour un agent de récupération de domaine. Elle n'est conservée ici que pour permettre de futures modifications du modèle par le compte Admin.

- Sélectionnez l'onglet **Extensions**, sélectionnez **Stratégies d'application** et validez que la zone **Description de Stratégies d'application** contient la stratégie **Récupération de fichiers**.

Ce modèle ne dispose que d'une stratégie et ne peut être utilisé que pour la récupération de fichiers chiffrés avec EFS.

- Sélectionnez **l'onglet Traitement de la demande** et cochez les cases **Autoriser l'exportation de la clé privée**.

Ce paramètre autorise une sauvegarde complète du certificat d'agent de récupération (avec sa clé privée).

- 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 Agent de récupération EFS** et cliquez sur le bouton **OK**.


Notre autorité de certification est prête à distribuer des certificats d'agent de récupération EFS.

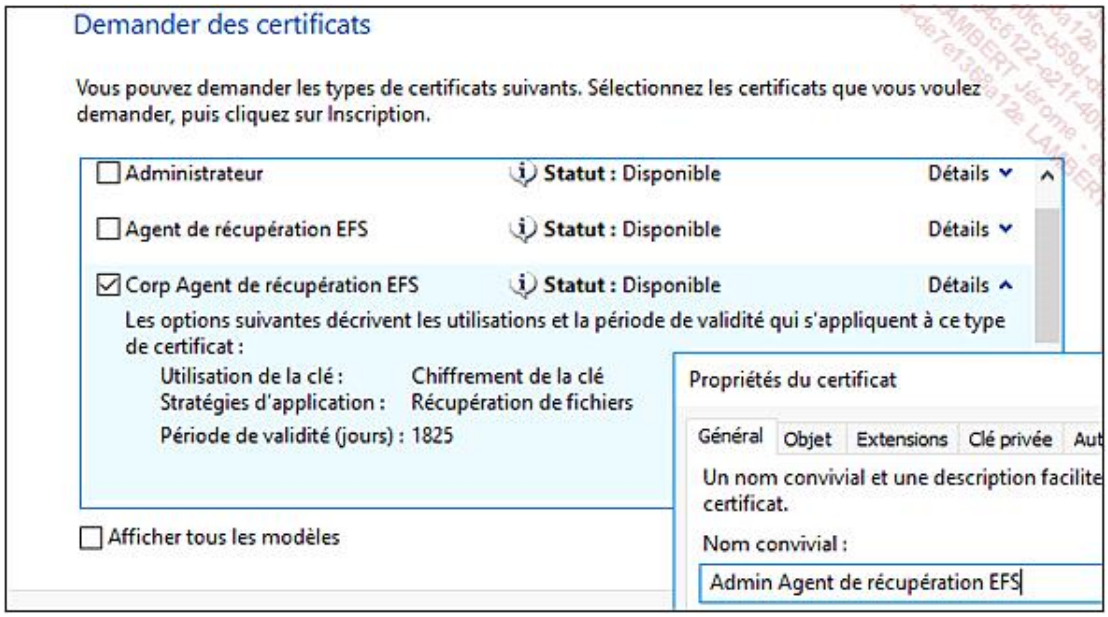
- Fermez la console de gestion Autorité de certification.

## Inscrire un certificat d'agent de récupération EFS

- Connectez-vous sur l'autorité de certification s2 en tant que Corp/admin.
- Ouvrez une invite de commande PowerShell et exécutez la commande :

```
Certmgr.exe
```

- Dans la console Certificats - Utilisateur Actuel, faites un clic droit sur le dossier **Personnel** et sélectionnez les menus **Toutes les taches\Demander un nouveau certificat**.
- Dans l'assistant Inscription de certificats, dans la fenêtre Avant de commencer, lisez les recommandations puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner la stratégie d'inscription de certificat, validez que la sélection par défaut est bien **Stratégie d'inscription à Active Directory** puis cliquez sur le bouton **Suivant**.
- Dans la fenêtre Demander des certificats, cochez le modèle **Corp Agent de récupération EFS**.
- Cliquez sur le l'icône flèche vers le bas à droite du menu **Détails** pour le développer, cliquez sur le bouton **Propriétés** et dans la zone **Nom convivial** de l'onglet **Général**, saisissez **Admin Agent de récupération EFS**.

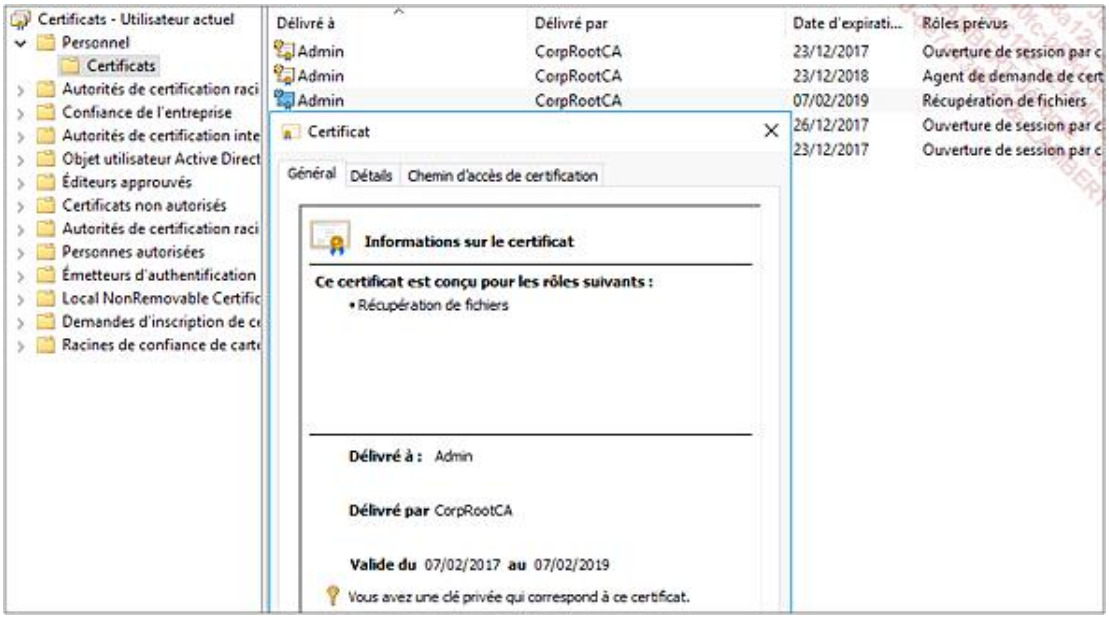



*Détails du modèle Corp agent de récupération EFS et ajout d'un nom convivial (Admin Agent de récupération EFS) à la demande de certificat d'Admin.*

- Cliquez sur les boutons **OK** et **Inscription**.
- Validez l'inscription du certificat.

## Valider les informations du certificat d'agent de récupération EFS

- Dans la console Certificats - Utilisateur Actuel, développez les dossiers **Personnel\Certificats** puis double cliquez sur le certificat obtenu (dans la zone de droite de la console).
- Dans l'onglet **Général**, validez que le certificat est délivré à **Admin** par l'autorité de certification **CorpRootCA**.




*Le certificat est bien délivré à Admin par CorpRootCA pour une durée de vie de deux années. Une clé privée est associée à ce certificat.*

- Sélectionnez l'onglet **Détails** et validez la présence des champs **Clé publique** et **Nom convivial**.
- Sélectionnez l'onglet **Chemin d'accès de certification** et validez que le certificat est bien délivré par l'autorité de certification **CorpRootCA**.

## 3. Activer l'agent de récupération

Nous allons modifier la stratégie par défaut du domaine afin d'activer le déploiement automatique du certificat de notre nouvel agent de récupération **Inscription** EFS sur tous les ordinateurs du domaine.

### Exporter le certificat d'agents de récupération EFS

- Faites un clic droit sur le certificat d'agent de récupération obtenu, sélectionnez le menu **Toutes les tâches** puis le menu **Exporter**.
- La boîte de dialogue Assistant exportation du certificat s'affiche, cliquez sur le bouton **Suivant**.
- Sélectionnez **Non, ne pas exporter la clé privée** puis cliquez sur le bouton **Suivant**.
- Acceptez le format de fichier par défaut (.cer) et cliquez sur le bouton **Suivant**.
- Dans la zone **Nom de fichier** saisissez C:\CertificatARAdmin, cliquez sur le bouton **Enregistrer** puis sur le bouton **Suivant** et sur le bouton **Terminer**.
- Cliquez sur **OK** sur le message indiquant que l'exportation a réussi.
- Transférez le fichier C:\CertificatARAdmin sur le contrôleur de domaine s1 (en utilisant le partage caché administratif \\s1\c$ par exemple…).

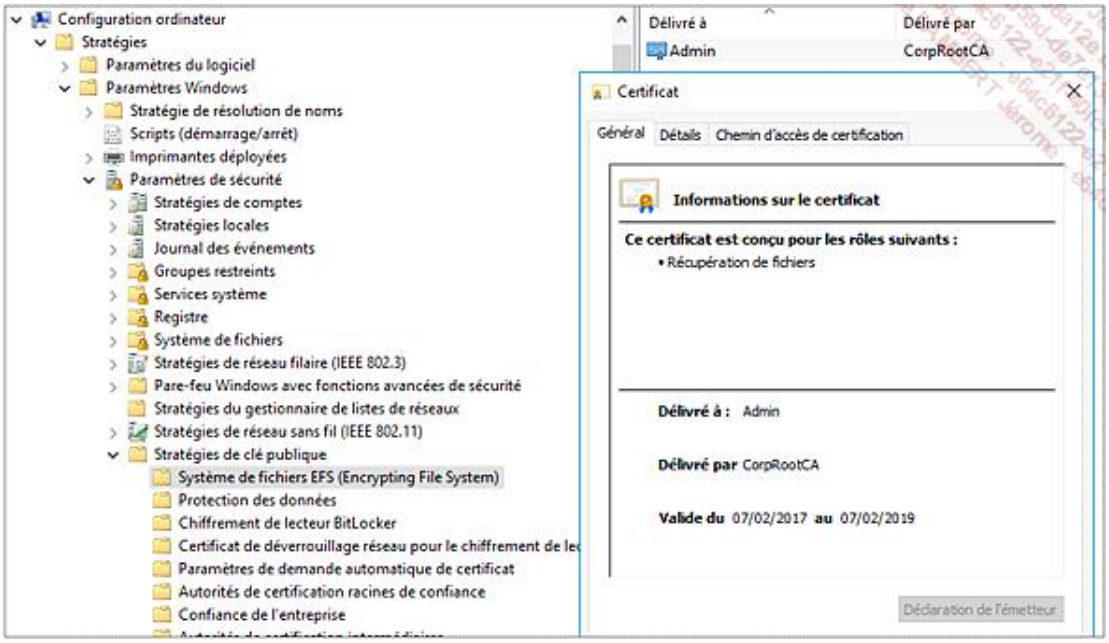
### Déployer le certificat de l'agent de récupération EFS

- 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 utilisateur\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 **Ajouter un agent de récupération de données**.


*Démarrage de l'assistant d'ajout d'un agent de récupération de données EFS pour le domaine corp.lan*

- Dans la fenêtre Bienvenue, cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sélectionner des agents de récupération, cliquez sur le bouton **Parcourir les dossiers** et sélectionnez le fichier C:\CertificatARAdmin.
- Cliquez sur les boutons **Suivant** et **Terminer**.
- Validez que le certificat de l'agent de récupération Admin s'affiche dans la fenêtre de droite de la

stratégie.




*Le certificat de notre nouvel agent de récupération EFS est prêt à être déployé par stratégie de groupe !*

- Fermez la console Gestion des stratégies de groupe.

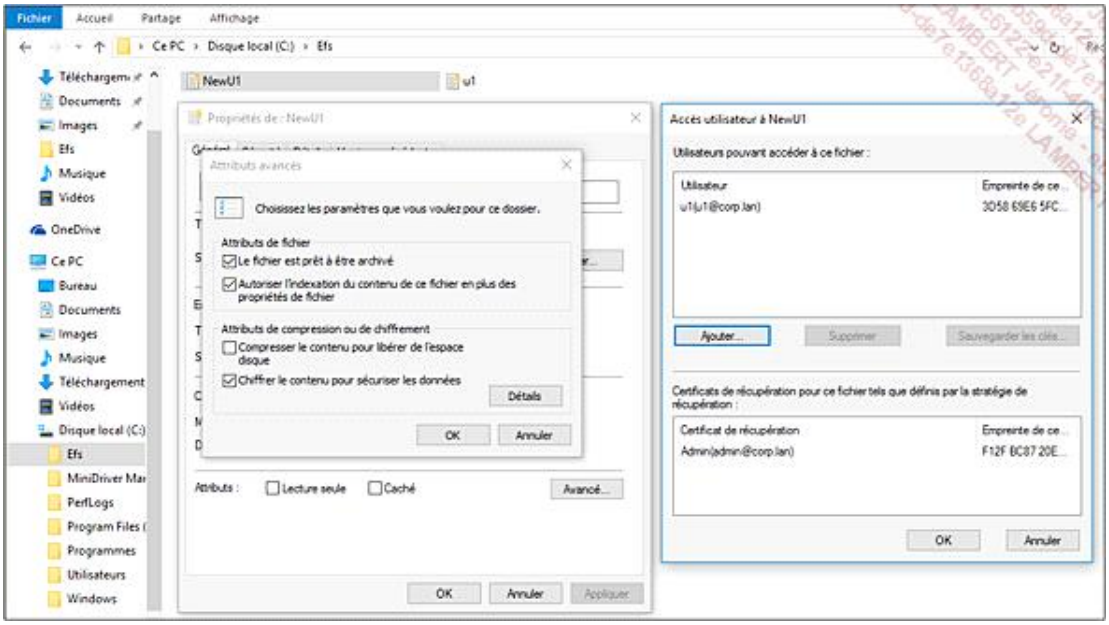
## 4. Récupération de fichiers chiffrés avec EFS

### Chiffrer un nouveau document

- Exécutez la commande **`Gpudate /force`** sur l'ordinateur client w10 afin d'appliquer les nouvelles stratégies de groupe.
- Connectez-vous sur l'ordinateur client w10 en tant que Corp/u1.
- Créez un nouveau document texte nommé NewU1 dans le dossier C:\Efs.
- Ouvrez le nouveau document texte nommé Newu1, ajoutez-y un contenu et sauvegardez-le.
- Faites un clic droit sur le fichier nommé Newu1 et utilisez le menu **Chiffrer** pour chiffrer ce nouveau document.

### Valider l'agent de récupération

- Faites un clic droit sur le fichier Newu1 et sélectionnez le menu **Propriétés**.
- Cliquez sur le bouton **Avancé** puis sur le bouton **Détails**.
- Vérifiez que la zone **Certificats de récupération pour ce fichier tels que définis par la stratégie de récupération** indique qu'il existe actuellement un certificat d'agent de récupération pour le compte Admin du domaine Corp.




*Le certificat de notre nouvel agent de récupération est maintenant reconnu sur l'ordinateur client w10.*

## Récupérer les fichiers chiffrés par u1

- Sur l'ordinateur client w10, fermez la session de l'utilisateur u1 et connectez-vous en tant que Corp/Admin.
- Validez que vous ne pouvez pas lire le contenu des deux documents chiffrés par l'utilisateur u1.

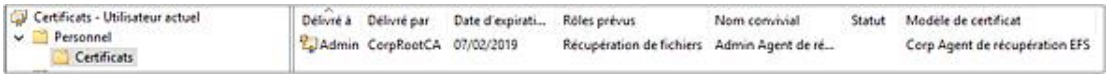
Vous ne disposez pas, sur l'ordinateur client w10, de la clé privée de déchiffrement de l'agent de récupération Admin.

## Exporter le certificat d'agents de récupération EFS sur w10

- Connectez-vous sur l'autorité de certification s2 en tant que Corp/admin.
- Ouvrez une invite de commande PowerShell et exécutez la commande **`Certmgr.msc`**.
- Faites un clic droit sur le certificat d'agent de récupération obtenu, sélectionnez le menu **Toutes les tâches** puis le menu **Exporter**.
- La boîte de dialogue Assistant exportation du certificat, cliquez sur le bouton **Suivant**.
- Sélectionnez **Oui, exporter la clé privée** puis cliquez sur le bouton **Suivant**.
- Acceptez le format de fichier d'exportation par défaut (.pfx) et cliquez sur le bouton **Suivant**.
- Dans la fenêtre Sécurité, cochez **Nom de groupes et d'utilisateurs (Recommandé)**, ajoutez le groupe Admins du domaine puis cliquez sur le bouton **Suivant**.
- Dans la zone **Nom de fichier**, saisissez **C:\CertificatARAdmin2**, cliquez sur le bouton **Enregistrer** puis sur le bouton **Suivant** et sur le bouton **Terminer**.
- Cliquez **OK** sur le message indiquant que l'exportation a réussi.
- Transférez le fichier C:\CertificatARAdmin2.pfx sur l'ordinateur client w10 (en utilisant le partage caché administratif \\w10\c$ par exemple…).

## Injecter la clé privée agent de récupération sur w10

- Connectez-vous sur l'ordinateur client w10 en tant que Corp/admin.
- Double cliquez sur le fichier transféré C:\CertificatARAdmin2.pfx afin de démarrer l'assistant d'installation du certificat d'agent de récupération.
- Validez toutes les fenêtres de l'assistant d'installation avec les paramètres par défaut.
- Ouvrez une invite de commande PowerShell et exécutez la commande **`Certmgr.msc`**.
- Développez **Certificats\Utilisateur actuel\Personnel\Certificats** et validez la présence du certificat de l'agent de récupération Admin.
- Double cliquez sur le certificat et validez qu'il possède une clé privée.




*La clé privée de l'agent de récupération est maintenant présente sur l'ordinateur client w10.*

- Validez que vous pouvez maintenant lire le contenu du dernier document chiffré par l'utilisateur u1 (le document NewU1) mais pas l'ancien document u1.txt.

L'ancien document a été créé après la déclaration de notre nouvel agent de récupération. Le fichier chiffré ne contient pas l'en-tête (avec la clé de chiffrement symétrique) pour l'agent de récupération.

- Connectez-vous sur l'ordinateur client w10 en tant que Corp/u1.
- Ouvrez puis fermez à nouveau le fichier u1.txt sans le modifier.

Cette simple manipulation crée un en-tête (avec la clé de chiffrement symétrique) pour l'agent de récupération.

- Connectez-vous sur l'ordinateur client w10 en tant que Corp/admin.
- Validez que vous pouvez maintenant lire le contenu de tous les documents chiffrés par l'utilisateur u1.