


UTILISATION DU SYSTEME EFS

PARCOURS

SISR ☒

SLAM ☐

Lieu de réalisation	Campus Montsouris	
Période de réalisation	Du : 19.01.2024	Au :
Modalité de réalisation	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

Intitulé de la mission	Utilisation du système EFS
Description du contexte de la mission	Chiffrer des données et gérer leur accès

Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu
	Windows Server 2022, Laptop, Hyper V
Productions associées	Liste des documents produits et description

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

Configuration et utilisation du système Windows EFS

La mission débute avec la création des utilisateurs. On crée des utilisateurs dans le serveur avec les fonctionnalités Windows.

La suite consiste au chiffrement des dossiers et fichiers en allant dans les propriétés du dossier.

La gestion des accès aux fichiers et dossiers chiffrés se fait, soit à l'aide de clés, soit à l'aide d'un agent de récupération.

A. Permettre l'accès à certains fichiers : utilisation des clés

1. Exportation d'une clé

Chercher "gérer les certificats de recherche" dans la barre Windows. Par la suite, le système nous propose la création d'un certificat. Il faut nommer et sauvegarder la future clé de format pfx dans un dossier. Enfin, choisir les fichiers et dossiers chiffrés que nous voulons associer à cette clé. Lorsque ceci est fait, le système nous informe de la réussite de la procédure, que nous pouvons vérifier en cliquant sur "afficher le journal", qui ouvre un fichier texte renseignant la réussite ou non de la procédure fichier par fichier.

2. Importation d'une clé

La suite de la procédure consiste en l'importation de la clé. Se connecter sur la session de l'autre utilisateur, puis accéder au fichier de la clé. Double-cliquer dessus. Cliquer sur "utilisateur actuel". Cliquer sur suivant. Le fichier à importer est rentré par défaut. Cliquer sur suivant. Rentrer le mot de passe précédemment configuré. Cliquer sur suivant. La prochaine fenêtre indique le magasin de certificats concerné. Cliquer sur suivant. Le système nous informe de la réussite de la procédure. Tester la procédure en tentant d'accéder à un fichier chiffré.

Permettre l'accès à tous les fichiers de tous les utilisateurs : création d'un agent de récupération

1. Création d'un certificat d'agent de récupération de données

Créer un dossier, ici "AgentRecup", destiné à contenir la future clé dans le volume C:\. Accéder à la console cmd. Taper la commande "cipher /r:C:\AgentRecup\certificat-agent", qui signifie que le système va créer une clé d'agent dans le dossier. Créer un mot de passe.

Accéder au dossier. 2 clés ont été créées. Double-cliquer sur la clé d'échange d'information pour entamer la procédure d'importation. Celle-ci est identique à celles précédentes. La procédure est un succès.

2. Création d'un agent de récupération de données

Ouvrir exécuter, taper "secpol.msc", cliquer sur ok. Dérouler successivement Paramètres de sécurité > Stratégies de clé publique > Système de fichiers EFS. Double-cliquer. Parcourir les dossiers pour accéder à celui qui contient les clés. Sélectionner le fichier CER. L'utilisateur concerné a été rentré par défaut. Le certificat de l'agent de récupération a été ajouté à la liste, et délivré à l'utilisateur. Tester la réussite de la procédure en créant 2 nouveaux fichiers dans le dossier chiffré "Chiffré" à l'aide des utilisateurs Sabine et Maxime. Par la suite, se connecter sur l'utilisateur, et lire les fichiers.

