\_EFS est un outil de chiffrement de fichier intégré pour Windows :

Permet un chiffrement et un déchiffrement transparents des fichiers

Assure la récupération des fichiers chiffrés

\_Scénarios d’utilisation fréquente pour EFS :

Protéger les fichiers sur les ordinateurs partagés

Protéger les fichiers contre tout accès par des utilisateurs privilégiés

\_Comment fonctionne EFS :

Le chiffrement EFS se produit au niveau du système de fichiers

Si un utilisateur qui possède la clé requise tente d’ouvrir un fichier, le fichier s’ouvre

\_Solutions d’entreprise pour gérer EFS

Déployer une autorité de certification permet la gestion centralisée des :

Clés EFS

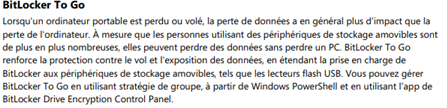
Agents de récupération de données EFS

Agents de récupération de clés EFS

\_BitLocker chiffre les données stockées sur le système d’exploitation et d’autres volumes en :

Fournissant une protection des données hors connexion

Protégeant toutes les données stockées sur le volume chiffré



\_Modes BitLocker : Windows 10 prend en charge deux modes de fonctionnement BitLocker :

-Le mode TPM

-Le mode Non-TPM

\_La configuration matérielle requise pour BitLocker est la suivante :

Un environnement BIOS ou UEFI qui est compatible avec un module de plateforme sécurisée (TPM) 1.2 ou un périphérique plus récent ou qui prend en charge les périphériques USB pendant le démarrage de l’ordinateur

Un espace suffisant sur le disque dur pour que BitLocker puisse créer deux partitions

\_Récupération des lecteurs chiffrés BitLocker

-Lorsqu’un ordinateur compatible avec BitLocker démarre :

-BitLocker vérifie s’il existe des problèmes indiquant un risque pour la sécurité dans le système d’exploitation

-Le mot de passe de récupération BitLocker :

* + - Est un mot de passe à 48 chiffres qui déverrouille un système en mode de récupération
    - Est spécifique à un chiffrement BitLocker particulier