Microsoft® Official Course

Module 11

Configuration du chiffrement et de l'audit avancé

Microsoft

Vue d'ensemble du module

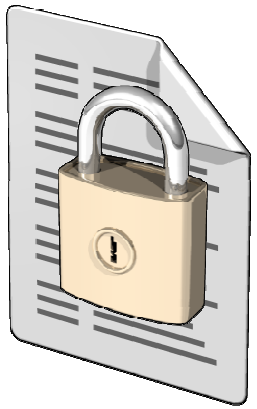
- Chiffrement des fichiers à l'aide du système EFS (Encrypting File System)
- Configuration de l'audit avancé

Leçon 1: Chiffrement des fichiers à l'aide du système EFS (Encrypting File System)

- Qu'est-ce que EFS ?
- Fonctionnement de la virtualisation des postes de travail (EFS)
- Récupération de fichiers chiffrés au format EFS
- Démonstration : Chiffrement d'un fichier à l'aide du système EFS

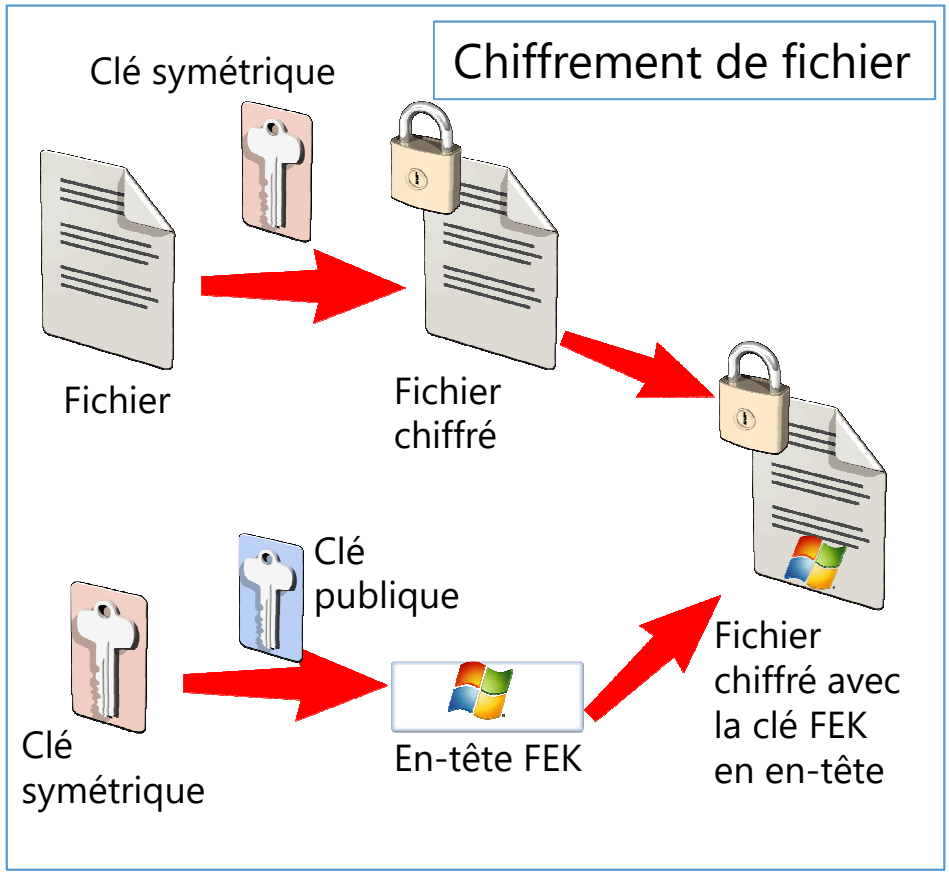
Qu'est-ce que EFS ?

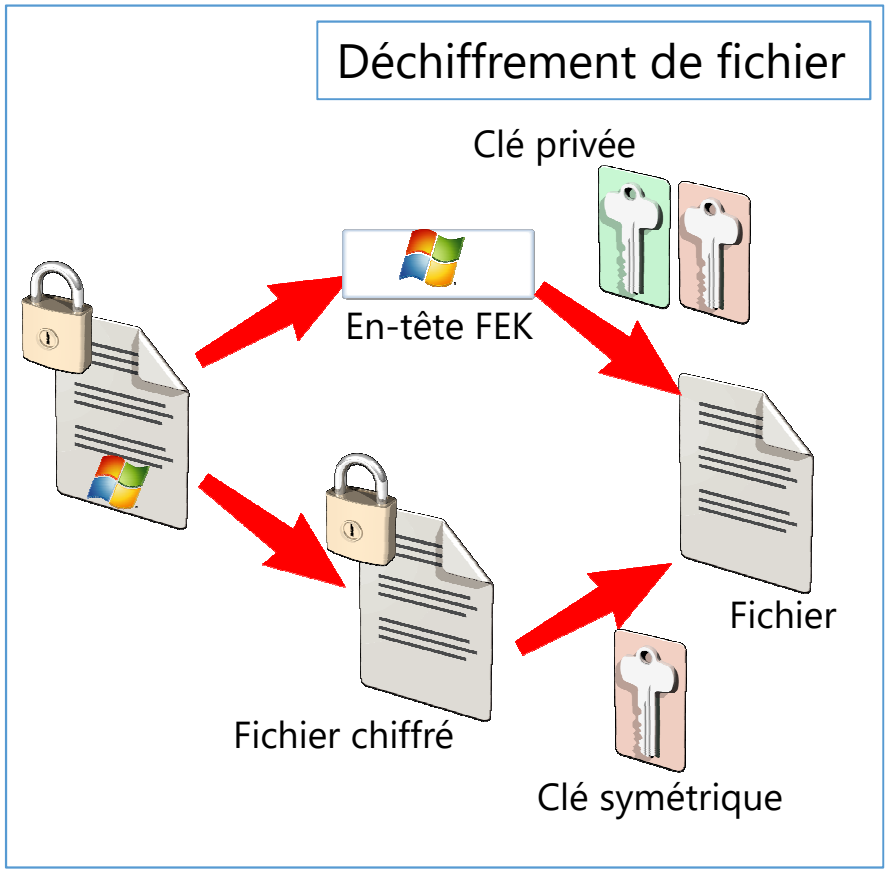
- Le système EFS est une fonctionnalité qui peut chiffrer des fichiers stockés sur une partition au format NTFS
- Le chiffrement EFS agit comme une couche de sécurité supplémentaire
- Le système EFS peut être utilisé sans configuration préalable



Fonctionnement de la virtualisation des postes de travail (EFS)

- Le chiffrement symétrique est utilisé pour protéger les données
- Le chiffrement par clé publique est utilisé pour protéger la clé symétrique





Récupération de fichiers chiffrés au format EFS

- Pour pouvoir récupérer des fichiers chiffrés au format EFS, vous devez :
  - Sauvegarder les certificats utilisateur
  - Configurer un agent de récupération
- Vous devez sauvegarder la clé de récupération pour :
  - Se protéger contre une défaillance du système
  - Rendre la clé de récupération portable

Démonstration : Chiffrement d'un fichier à l'aide du système EFS

- Dans cette démonstration, vous allez apprendre à :
  - Vérifier qu'un compte d'ordinateur prend en charge le système EFS sur un partage réseau
  - Utiliser le système EFS pour chiffrer un fichier sur un partage réseau
  - Afficher le certificat utilisé pour le chiffrement
  - Tester l'accès à un fichier chiffré

Leçon 2: Configuration de l'audit avancé

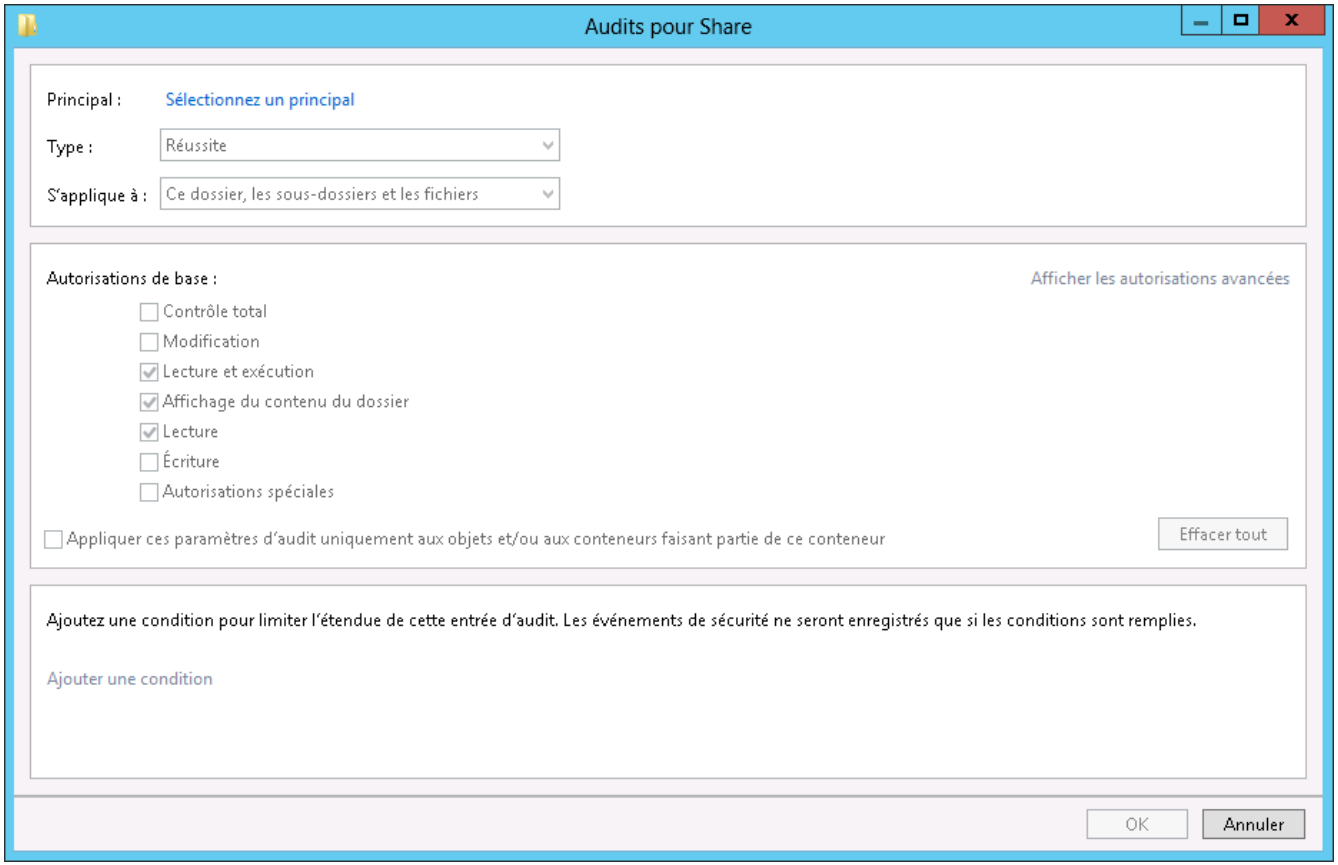
- Vue d'ensemble des stratégies d'audit
- Spécification des paramètres d'audit pour un fichier ou un dossier
- Activation de la stratégie d'audit
- Évaluation des événements du journal de sécurité
- Stratégies d’audit avancées
- Démonstration : Configuration de l'audit avancé

Vue d'ensemble des stratégies d'audit

- Auditez les événements dans une catégorie d'activités, telles que :
  - Accès aux fichiers et dossiers NTFS
  - Changements de compte ou d'objet dans AD DS
  - Ouverture de session
  - Attribution de l'utilisation des droits utilisateur
- Par défaut, les contrôleurs de domaine auditent les événements ayant réussi pour la plupart des catégories
- Objectif : aligner les stratégies d'audit sur les stratégies de sécurité de l'entreprise
  - Sur-audit : les journaux sont trop volumineux pour rechercher des événements importants
  - Sous-audit : les événements importants ne sont pas enregistrés

Spécification des paramètres d'audit pour un fichier ou un dossier

- **Les paramètres d'audit d'un fichier ou dossier sont spécifiés en modifiant la liste SACL :**



- Le contrôle total enregistre tous les événements associés
- Les événements d'audit ne sont pas enregistrés tant que la stratégie d'audit n'est pas activée

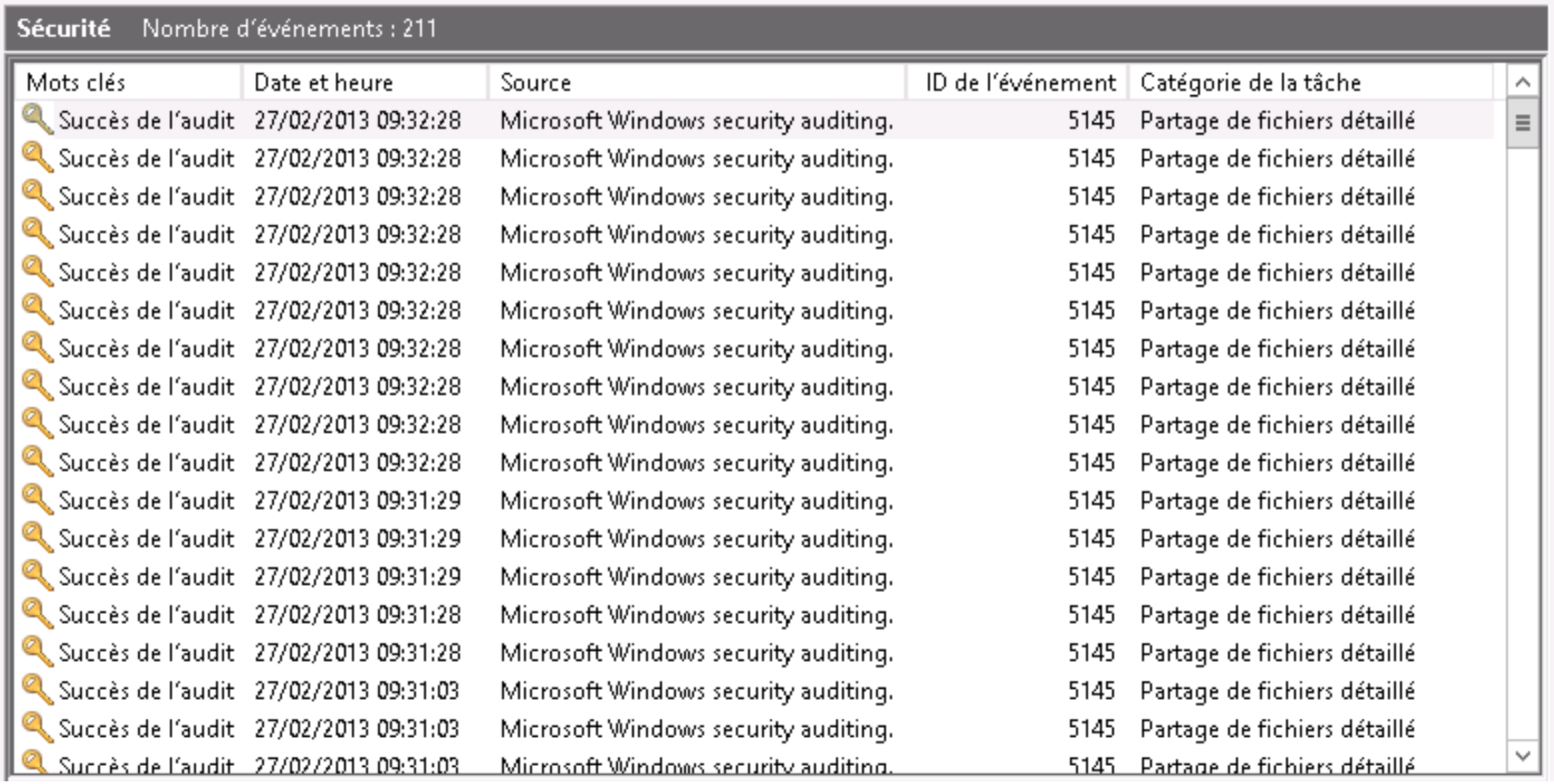
Activation de la stratégie d'audit

Pour activer la stratégie d'audit en configurant les paramètres de stratégie d'audit dans un objet de stratégie de groupe :

- Activez les paramètres appropriés dans l'objet de stratégie de groupe
- Appliquez l'objet de stratégie de groupe à l'emplacement AD DS où vos serveurs sont situés

Évaluation des événements du journal de sécurité

Affichez les événements d'audit dans le champ Détails du journal de sécurité, et appliquez un filtre pour réduire le nombre d'événements à examiner :

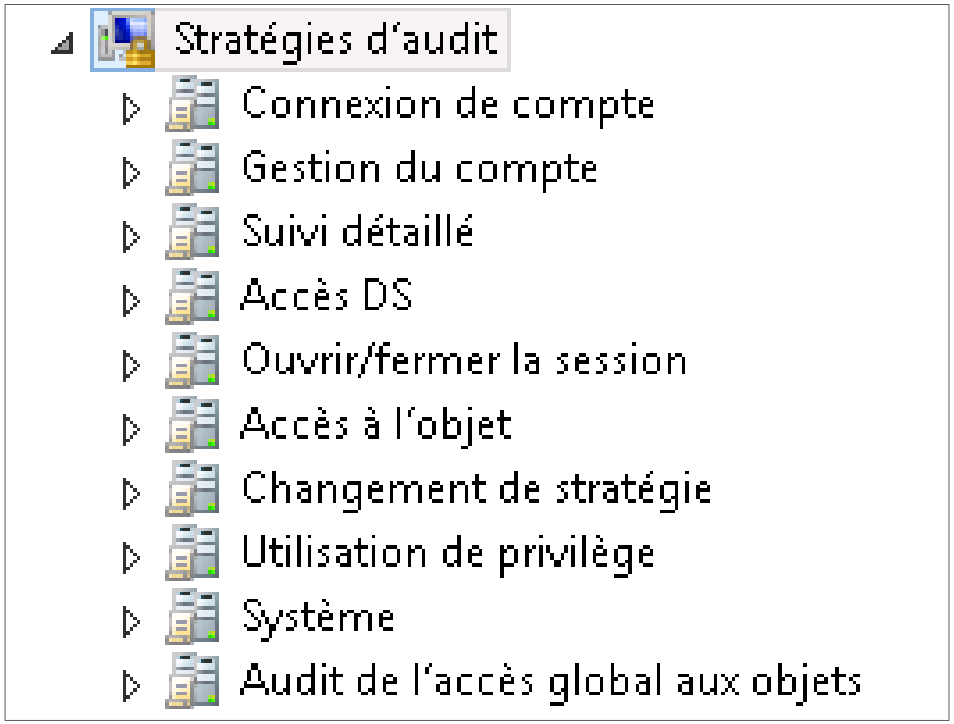


Sécurité Nombre d’événements : 211

Mots clés	Date et heure	Source	ID de l’événement	Catégorie de la tâche
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:32:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:29	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:29	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:29	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:28	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:03	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:03	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé
Succès de l’audit	27/02/2013 09:31:03	Microsoft Windows security auditing.	5145	Partage de fichiers détaillé

Stratégies d’audit avancées

Windows Server 2012 et Windows Server 2008 R2 fournissent un ensemble supplémentaire de stratégies d'audit à configurer :



Démonstration : Configuration de l'audit avancé

- Dans cette démonstration, vous apprendrez à créer et à modifier un objet de stratégie de groupe pour la configuration de la stratégie d'audit

Atelier pratique : Configuration du chiffrement et de l'audit avancé

- Exercice 1 : Chiffrement et récupération des fichiers
- Exercice 2 : Configuration de l'audit avancé

Informations d'ouverture de session

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-CL1 22411B-LON-SVR1
Nom d'utilisateur	**ADATUM\Administrateur**
Mot de passe	**Pa$$w0rd**

Durée approximative : 40 minutes

Scénario d'atelier pratique

A. Datum est une société internationale d’ingénierie et de fabrication, dont le siège social est basé à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour assister le siège social de Londres et d’autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012

Vous devez configurer l'environnement Windows Server 2012 pour protéger les fichiers sensibles, et vérifier que l'accès aux fichiers sur le réseau est audité convenablement. Vous devez également configurer l'audit du nouveau serveur

Révision de l'atelier pratique

- Dans l'exercice 1, tâche 1, pourquoi deviez-vous générer un nouveau certificat Agent de récupération de données à l'aide de l'autorité de certification (CA) AdatumCA ?
- Quels sont les avantages de placer des serveurs dans une unité d'organisation et d'appliquer des stratégies d'audit à cette unité d'organisation ?
- Quelle est la raison d'appliquer des stratégies d'audit à l'ensemble de l'organisation ?

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Outils