CHAPITRE 5

Travaux en laboratoire informatique

1 Gérer les accès et les privilèges appropriés

> Fiches savoirs technologiques 5 et 6

Vous avez fait plusieurs recommandations à M. Brillat pour améliorer la sécurité des données au sein du SI de la MSAP. Vous avez notamment proposé la modification des différents éléments d'habilitation et des droits d'accès. M. Jivon est intervenu pour la réalisation de ces modifications. Cependant, dans un souci de disponibilité des données, il souhaiterait installer un second serveur de fichiers (à l'identique du premier) pour remplacer le premier en cas de dysfonctionnement ou de panne.

1. **Préparez la machine virtuelle de tests (second serveur de fichiers) d'après les consignes.**
   > Document 1
   > Fiche méthode 3, p. 207
2. **Créez les différents partages en relevant les chemins d'accès qui servent à définir un lecteur réseau pour chaque compte.**
   > Documents 2 et 3
3. **Définissez les autorisations et les ACL (liste de contrôle d'accès) sur les partages en vous appuyant sur les recommandations données.**
   > Documents 4 et 5
4. **Réalisez les tests.**
   > Document 6

Document 1 Consignes pour la préparation de la machine virtuelle de tests

1. Installer le rôle serveur de fichiers sur une machine virtuelle Windows 2016.
2. Attribuer l'ensemble des privilèges au compte Administrateur.
3. Créer des comptes Enedis, MSA, CLIC et TRESOR en local sur le serveur à l'aide du compte Administrateur. Mot de passe pour chaque compte : **MSAP,connect1920**.
4. Valider la case à cocher «Modifier le mot de passe à la première connexion» pour chaque compte.

Document 2 Informations sur les dossiers de partage

1. Création d'un dossier nommé «Partages» à la racine du lecteur C du serveur de fichiers.
2. Création des différents dossiers de partage pour chaque utilisateur précédemment admis à l'intérieur du dossier «Partages». Chaque dossier de partage portera le même nom que le compte associé.

Document 3 Un exemple de partage sur un dossier

Le compte test et le dossier correspondant.

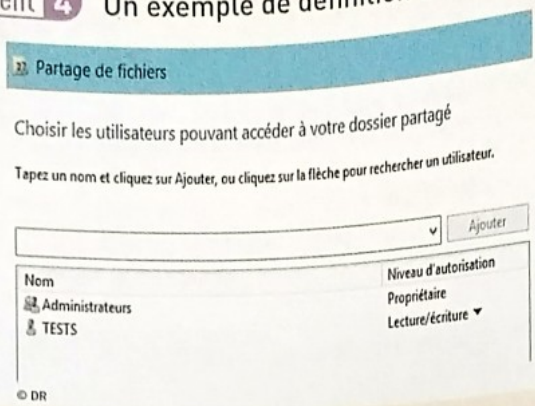
TESTS

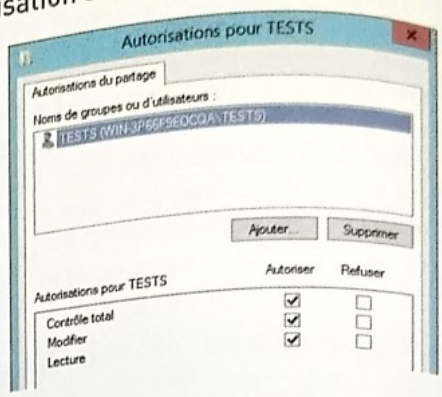
\\Desktop-579b371\tests

© DR

> Voir lexique BTS SIO, p. 221

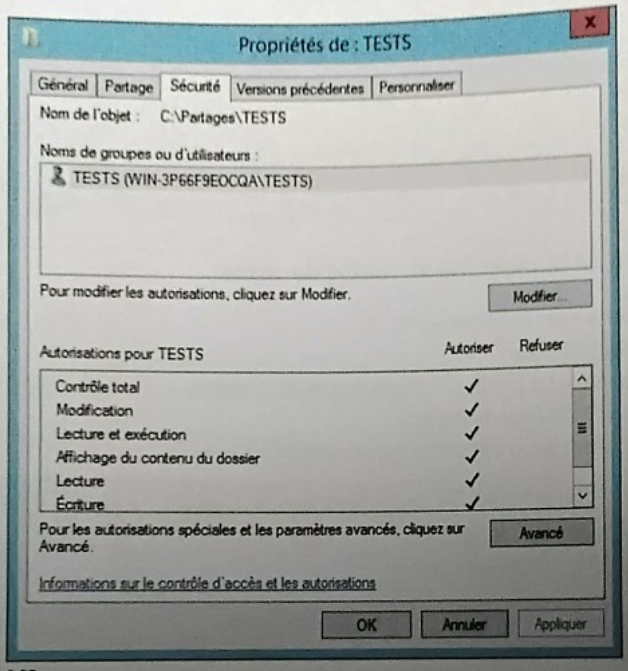
Document 4 Un exemple de définition d'une autorisation sur un partage





© DR

Document 5 Consignes pour la définition des ACL sur les partages



© DR

1. Créer l'accès au dossier (seul le compte portant le même nom que le dossier peut accéder au dossier).
2. Définir un contrôle total sur les données (on considère que les utilisateurs qui accèdent au partage sont les propriétaires des données).

Document 6 Tests à réaliser

- **Test 1**
  - Connexion avec le compte Enedis.
  - Définir le mot de passe de session. Celui-ci sera modifié par la suite.
  - Créer un lecteur réseau avec le chemin de partage relevé précédemment (question 2).
  - Ajouter un document dans le répertoire, le modifier, puis le supprimer.

Enedis1234

- **Test 2**
  - Se déconnecter du compte Enedis.
  - Ouvrir une session avec le compte MSA.
  - Créer un lecteur réseau avec le chemin de partage utilisé dans le test 1.
  - Identifier le message d'erreur (le commenter).

Fiche savoirs technologiques 5

Les authentifications, privilèges et habilitations des utilisateurs

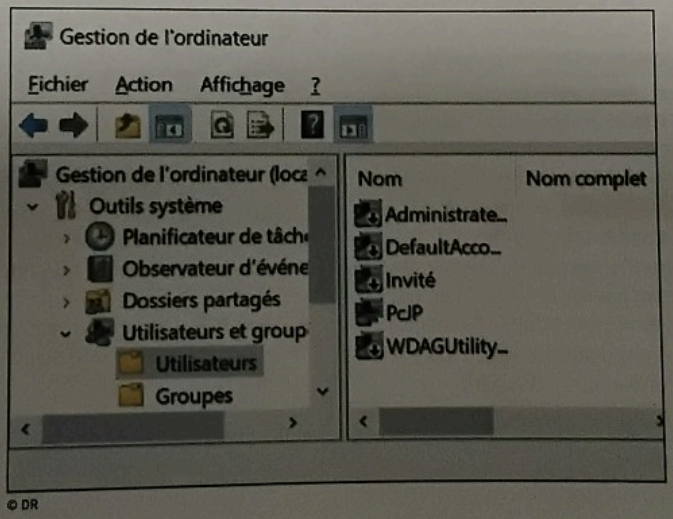
I Les principes de l'authentification et de l'habilitation

Authentification	Habilitation
Processus qui permet de vérifier si l'utilisateur est bien celui qu'il prétend être. • Elle permet de vérifier et de prouver l'identité d'un utilisateur qui veut ouvrir une session dans un SI, et de lui accorder les droits d'accès inhérents à son compte. • Elle s'appuie sur l'utilisation d'un identifiant (*login*) et d'un mot de passe (*password*). • Elle repose sur un compte utilisateur local ou un compte utilisateur sur un gestionnaire de domaine, comme *Active Directory*.	**Processus qui permet de savoir si un utilisateur a accès à une ressource ou non.** • Elle inclut l'autorisation, l'accréditation, les droits d'accès ou encore le contrôle d'accès. • Elle donne la permission à un utilisateur de réaliser des actions sur des ressources du SI : droit de consultation, droit de création, droit de modification, droit de suppression, etc. • Elle dépend des privilèges accordés. Le privilège est la délégation d'autorité sur un fichier ou un dossier dans un SI.

II Les techniques d'authentification

1. Le compte local

L'accès à un poste de travail s'effectue par des comptes utilisateurs. Ces comptes peuvent être nominatifs (chacun est associé à une seule personne) ou collectifs (des comptes sont associés à plusieurs personnes). Par défaut, le compte administrateur et le compte invité sont créés. L'ensemble des comptes locaux et des mots de passe sont stockés (sous forme d'empreintes numériques) dans la base SAM (*Security Accounts Manager* - %SystemRoot%\System32\Config\SAM).



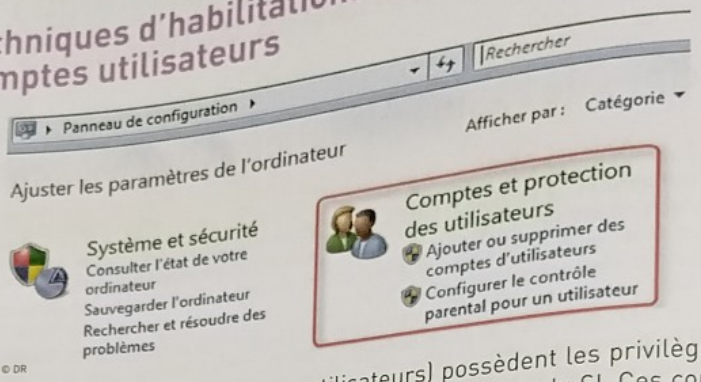
© DR

2. Les comptes itinérants

Les authentifications centralisées sur un contrôleur de domaine s'effectuent grâce à l'annuaire LDAP (*Lightweight Directory Access Protocol*) et au protocole Kerberos (protocole réseau d'authentification reposant sur un chiffrement symétrique et un système de tickets).

> Voir lexique BTS SIO, p. 221

III Les techniques d'habilitations associées aux comptes utilisateurs



© DR

Les **comptes administrateurs** (ou superutilisateurs) possèdent les privilèges les plus élevés. Ils ont un contrôle total sur l'ensemble des ressources du SI. Ces comptes sont par ailleurs habilités à créer, modifier et supprimer d'autres comptes.

Les **comptes utilisateurs** n'ont pas la possibilité de réaliser des opérations privilégiées, ni de créer des comptes. Ils peuvent cependant configurer le système et installer certains logiciels.

Les **comptes invités** sont des comptes génériques aux droits très restreints. Ils ne peuvent pas installer des logiciels et n'ont pas accès aux répertoires contenant des informations sensibles. Chaque compte utilisateur appartient à un groupe d'utilisateurs qui définit, par défaut, ses droits d'accès ou privilèges.

IV Les bonnes pratiques en matière d'authentification et d'habilitation

Authentification	Habilitation (valable pour l'ensemble des comptes)
Compte administrateur	
• Utiliser des comptes d'administration dédiés et non partagés entre différents utilisateurs : l'administrateur doit disposer de plusieurs comptes d'administration distincts selon les tâches qu'il doit réaliser. • Protéger (confidentialité et intégrité) l'accès aux annuaires des comptes administrateurs. • Ne pas autoriser l'ouverture de sessions de travail (activités qui ne sont pas de l'ordre de l'administration) sur des postes réservés aux actions d'administration. • Attribuer des droits d'administration à des groupes plutôt qu'à des utilisateurs individuels.	• Respecter le principe « du besoin d'en connaître » : habilitations nécessaires à la réalisation des tâches inhérentes à l'activité de l'utilisateur. • Respecter le principe « du moindre privilège » : mettre en place des habilitations strictement nécessaires aux activités liées à chaque compte. Ce principe ne doit pas être supérieur au « besoin d'en connaître ». • Gérer efficacement les mobilités : éviter l'accumulation des habilitations (fonctions successivement occupées). • Réaliser une revue annuelle des habilitations afin d'identifier et de supprimer les comptes non utilisés ou qui n'ont plus lieu d'exister. • Mettre en place des procédures d'attributions des habilitations à appliquer systématiquement à l'arrivée ainsi qu'au départ ou au changement d'affectation d'un utilisateur du SI. • Définir des mesures permettant de restreindre et de contrôler l'attribution et l'utilisation des accès.
Compte utilisateur	
• Doit être nominatif. • Ne pas utiliser de comptes partagés entre plusieurs utilisateurs. • Donner accès seulement aux données nécessaires aux activités et restreindre l'accès aux répertoires contenant des données sensibles. • Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour. • Ne pas donner accès aux disques et aux applications sensibles aux utilisateurs visiteurs.	

> Voir lexique BTS SIO, p. 221

CHAPITRE 5

Fiche savoirs technologiques 6

La gestion des droits d'accès aux données

Le contrôle d'accès précise qui (utilisateur) est autorisé à faire quoi (lectures, écritures, suppressions, modifications, etc.) sur quelles données.

I Les principes de la gestion des droits d'accès aux données

Elle a pour but de limiter les actions qui peuvent être réalisées sur les données (fichiers et dossiers), l'utilisation des applications et la gestion du système.
Le principe est de restreindre les privilèges des différents utilisateurs.

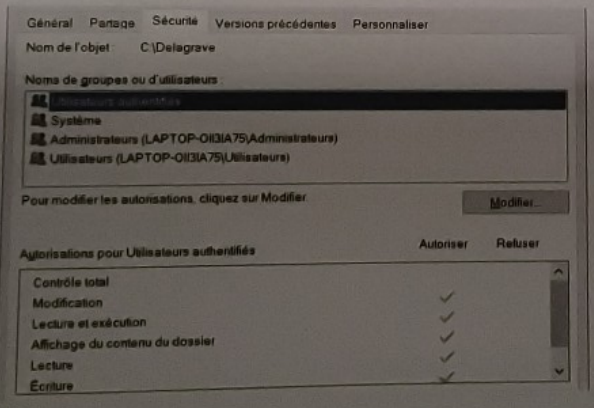
Exemple sous UNIX : la commande **ls -al** affiche les droits sur les fichiers et les répertoires, représentés par les lettres ci-dessous :

r - read	Lire un fichier/lister un répertoire
w – write	Ajouter, supprimer, modifier un fichier dans un répertoire
X – execute	Exécuter un fichier / traverser un répertoire

Droits	Utilisateurs	Ressources concernées
-rwxr-x---	1 root	apple.exe
drw-r-----	1 brows	Reports
-rw-rw-r--	1 darkness	gold.txt

La commande **chmod** munie des opérateurs **+**, **-**, **u**, permet de modifier et de changer les droits d'accès.

Exemple sous Windows : les droits d'accès s'appuient sur le système de fichiers NTFS pour pouvoir mettre en œuvre un modèle de moindre privilège grâce à des listes de contrôle d'accès (ACL). La gestion des autorisations se fait à partir de l'onglet « Sécurité » de chaque dossier ou fichier :



© DR

Les différents privilèges sont :
- l'accès au contenu du répertoire (Affichage du contenu du dossier) ;
- la lecture des fichiers, de leurs propriétés et de leurs répertoires (Lecture) ;
- l'exécution des programmes et des scripts (Lecture et exécution) ;
- l'écriture dans les fichiers et l'ajout des fichiers dans les répertoires (Écriture) ;
- l'affichage, la modification, la suppression des fichiers et répertoires (Modification) ;
- tous les droits (Contrôle total) habituellement réservés à l'administrateur : modification, ajout, déplacement ou suppression des fichiers et répertoires ;
- la modification des paramètres des autorisations pour tous les autres utilisateurs.

> Voir lexique BTS SIO, p. 221

II L'installation de VirtualBox

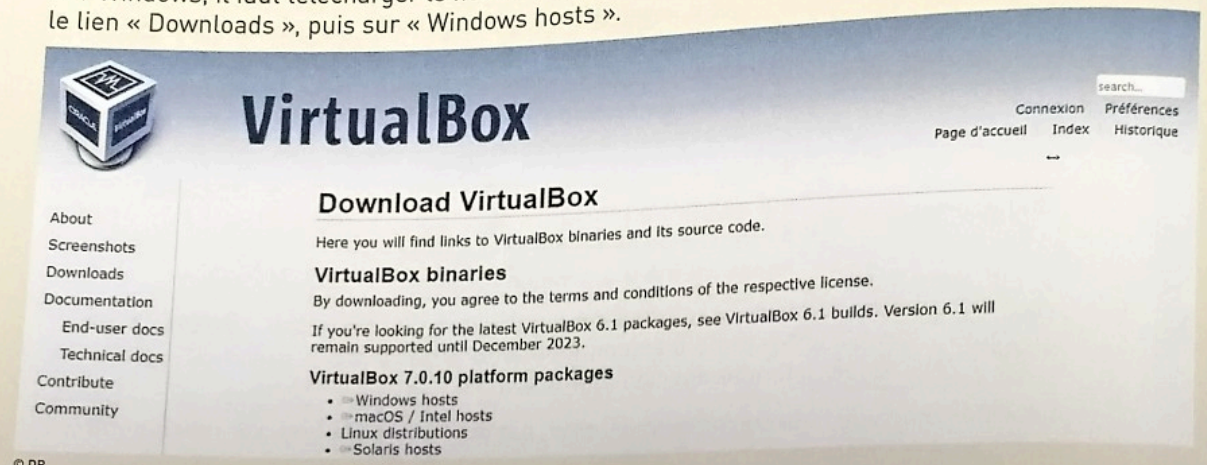
VirtualBox est le logiciel de virtualisation utilisé dans certains travaux en laboratoire de cet ouvrage. Pour l'installer, il faut suivre la procédure suivante.
L'utilisation d'un hyperviseur nécessite un ordinateur qui supporte la virtualisation. Il faut aussi vérifier que les fonctions de virtualisation sont activées dans le BIOS. Il convient aussi de disposer de suffisamment de mémoire vive afin que les machines virtuelles et le système hôte puissent fonctionner correctement.

1. Téléchargement

> VirtualBox à télécharger : www.lienmini.fr/882-11

VirtualBox est un logiciel libre édité par Oracle. Il est téléchargeable gratuitement depuis le site officiel.

Sur Windows, il faut télécharger le fichier d'installation avec l'extension .exe. Pour cela, cliquer sur le lien « Downloads », puis sur « Windows hosts ».



© DR

Sur Linux, il est possible d'installer directement VirtualBox à partir d'une commande exécutée depuis un terminal (voir ci-dessous).

2. Installation sur une machine hôte

Machine hôte Windows	Double cliquer sur le fichier .exe afin de lancer l'assistant d'installation.
Machine hôte Linux (Debian)	1. Ouvrir un terminal avec la combinaison des touches CTRL+ALT+T 2. Saisir la commande suivante : *sudo apt install virtualbox* Après validation de cette commande avec la touche ENTRÉE, saisir le mot de passe du compte administrateur afin de lancer l'installation du paquet.

La virtualisation

Le principe de la virtualisation

1. Définition

La virtualisation consiste à exécuter sur une machine hôte des systèmes d'exploitation (Windows, Linux...) différents de celui de la machine hôte. La virtualisation repose sur les éléments suivants.

Un système d'exploitation hôte	Il s'agit du système d'exploitation principal qui héberge l'outil de virtualisation et toutes les machines virtuelles. Ce système est hébergé sur une machine physique.	Exemples : Windows, Ubuntu
Un hyperviseur	Il s'agit du logiciel de virtualisation qui permet à plusieurs systèmes d'exploitation différents de travailler sur la même machine physique.	Exemples : VirtualBox, VMWare, KVM
Des machines virtuelles	Ces machines peuvent avoir un système d'exploitation différent et fonctionner en même temps.	Exemples : Windows, Debian

Ainsi, une machine hôte en Windows 10 peut, par exemple, héberger une machine virtuelle sous Linux et inversement.

2. Les deux types d'hyperviseur

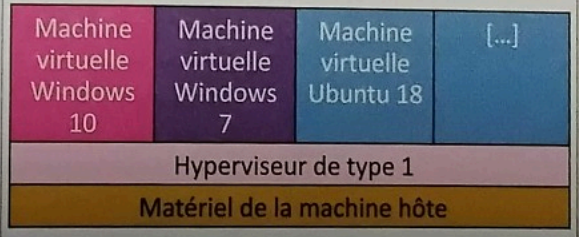
Il existe deux types d'hyperviseur :

Hyperviseur de type 1 : natif

Un hyperviseur de type 1, ou natif, est un logiciel qui s'exécute directement sur une plateforme matérielle.

Exemples : VMWare ESX, Proxmox

Schéma hyperviseur de type 1

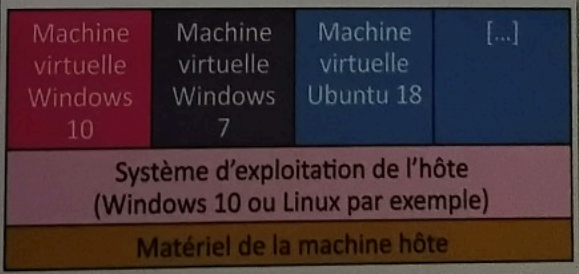


Hyperviseur de type 2 : hosted

Un hyperviseur de type 2 est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation.

Exemples : VirtualBox, VMWare Workstation

Schéma hyperviseur de type 2



II Les outils de la gestion des droits d'accès aux données

Différents modèles de gestion des droits d'accès sont possibles au sein d'un système d'information, mais leur finalité est la même : ne permettre l'accès et la modification des données qu'aux personnes autorisées. Les deux principaux modèles sont :

DAC ***(Discretionary Access Control)*** **Contrôle d'accès discrétionnaire**	**RBAC** ***(Role-Based Access Control)*** **Contrôle d'accès basé sur des rôles**
Le créateur d'une ressource est le propriétaire de celle-ci. Il fixe alors la politique de contrôle d'accès de cette ressource : il décide quel utilisateur peut réaliser quelle action. Exemple : En tant que propriétaire du fichier paie.xls, j'autorise uniquement Alice à lire le fichier.	Il convient de définir tout d'abord des rôles qui représentent un ensemble de privilèges. Les utilisateurs sont affectés à un rôle et héritent donc des droits inhérents à celui-ci. Exemple : Le rôle RH donne les droits d'accès en lecture et en écriture au fichier paie.xls. On attribue le rôle à Bob, qui pourra donc modifier le fichier.
Ce modèle de gestion est décentralisé. Il correspond à l'attribution de droits par un compte local sur un poste de travail.	Ce modèle de gestion est centralisé, comme dans un *Active Directory* où les utilisateurs appartiennent et héritent des groupes.

III La gestion dans le cadre d'un *Active Directory*

Dans un *Active Directory* (gestion centralisée des utilisateurs), des groupes de sécurité sont prédéfinis pour attribuer des droits particuliers aux différents comptes (utilisateurs) créés. Ci-dessous, un exemple de groupes présents dans l'*Active Directory* :

Administrateurs	Accès complet et illimité à l'ordinateur promu du domaine
Administrateur du domaine	Droits sur tous les objets du domaine et administration du domaine
Opérateurs de comptes	Création, modification et suppression des objets locaux
Utilisateurs du domaine	Groupe par défaut de tout nouvel utilisateur
Invité du domaine	Inclut le compte invité du domaine. Lorsque les membres de ce groupe se connectent, un profil de domaine est créé sur l'ordinateur