Chapitre 1 : Introduction aux Réseaux

Deux grandes branches principales :

- **Mise en place** : installation physique et logique du réseau.
- **Administration du réseau** : gestion des utilisateurs, des ressources et de la sécurité.

1/Types de Réseaux

Réseau non-administré

- **Définition** : Petit réseau simple, sans configuration avancée, ne nécessitant pas un administrateur réseau.
- **Exemple** : Réseau domestique entre un PC, une imprimante et une box Internet.

Réseau administré

- **Définition** : Réseau de grande taille avec de nombreux utilisateurs et ressources, nécessitant un administrateur pour la gestion.
- **Exemple** : Réseau d'une université ou d'une entreprise, avec contrôle centralisé des accès et des services.

2/Administration Réseau

- Gère les utilisateurs et les ressources en leur attribuant des **droits et privilèges**.
- **Exemple** : Autoriser l'utilisateur *user1* à accéder au dossier partagé *dp1*.

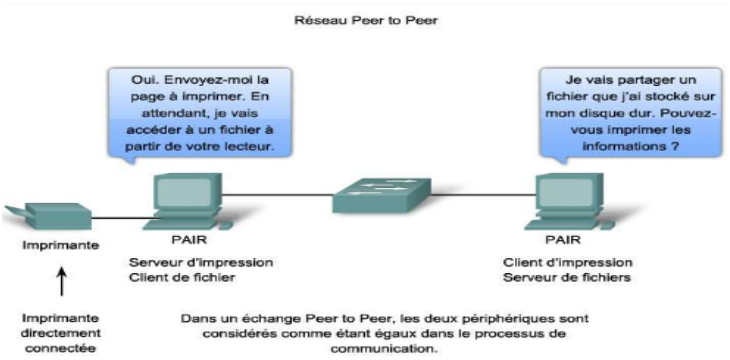
3/Modèles de Réseaux

Peer-to-Peer (P2P)

- **Définition** : Modèle décentralisé où chaque machine peut agir comme client et serveur.

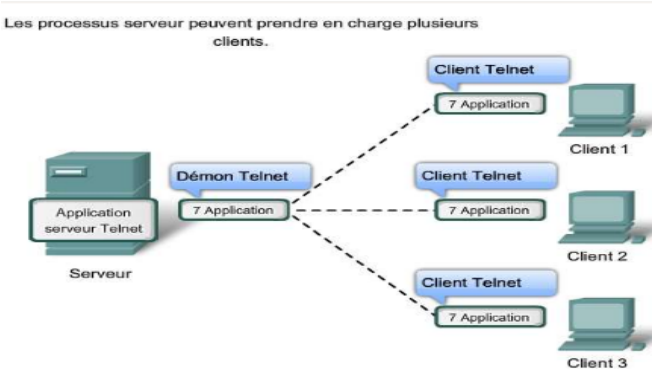
- **Caractéristiques** :
  - Sécurité limitée
  - Authentification non centralisée
  - Partage de fichiers non structuré (type "Tout ou Rien")
  - Pas d'administrateur nécessaire

- **Exemple** : Partage de fichiers entre étudiants via un réseau local sans serveur central.



Client/Serveur

- **Définition** : Modèle centralisé où des clients (utilisateurs) accèdent à des services fournis par un ou plusieurs serveurs.
- **Exemple** : Un poste étudiant qui se connecte à un serveur de fichiers pour accéder à des documents.



4/Services dans un Réseau Client/Serveur

- **Serveur Web (HTTP)** : héberge des sites web.
- **Serveur DHCP** : attribue automatiquement des adresses IP.
- **Serveur DNS** : traduit les noms de domaine en adresses IP.
- **Serveur de fichiers** : partage et gère des fichiers à travers le réseau.
- **Serveur d'annuaire** : gère les utilisateurs, ordinateurs et ressources.

5/Qu'est-ce qu'un Annuaire ?

- **Définition** : Base de données contenant des **objets du réseau** (utilisateurs, ordinateurs, imprimantes, groupes).
- **Fonction** : Centralise l'authentification, facilite la gestion et l'accès aux ressources.

6/Active Directory (AD)

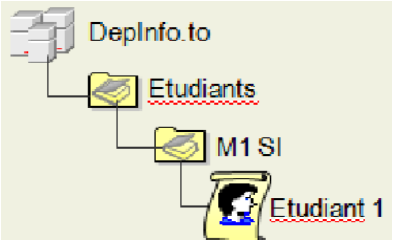
- **Définition** : Service d'annuaire de Microsoft utilisé dans les environnements Windows Server.
- **Fonctionnalités** :
  - Centralisation de la gestion du réseau
  - Organisation hiérarchique des objets
  - Authentification unique pour les utilisateurs
- **Exemple concret** : Dans un lycée, chaque élève a un seul identifiant pour se connecter à n'importe quel poste informatique via Active Directory.

7/Objets d'Active Directory

- Serveurs
- Domaines
- Sites
- Utilisateurs (DR)
- Ordinateurs (R ou DR)
- Imprimantes (R)
- Groupe (DR)

D = Défini dans l'annuaire (Active Directory),R = Ressource du réseau

8/Hiérarchie et Schéma Active Directory



- **Schéma AD** : définit les classes d'objets et leurs attributs dans le système.
- **Exemple** de classe :
  Classe **User** → objet **user1**
  Attributs : Nom, Prénom, Adresse, Fonction, etc.

9/Notion de Domaine

- **Définition** : Unité de base dans AD, un **domaine** regroupe des utilisateurs et ordinateurs qui partagent la même base de données d'annuaire.
- **Exemple** : Domaine **Depinfo.to**

10/Contrôleur de Domaine (DC)

- **Définition** : Serveur sur lequel est installée une copie de la base de données Active Directory.
- Il valide les connexions et applique les règles de sécurité.

11/Administrateur de Domaine

- Compte utilisateur avec tous les privilèges sur le domaine.
- Par défaut, ce compte existe dans chaque domaine créé dans Active Directory.

12/Relation Domaine / Contrôleur de Domaine

- Un **domaine** peut être servi par plusieurs **contrôleurs de domaine** (DC1, DC2, DC3).
- Ces contrôleurs coopèrent pour authentifier les utilisateurs et fournir les services du domaine.
- **Exemple** : Le domaine *Depinfo.to* est géré par les serveurs *DC1*, *DC2*, *DC3*.

13/Situation d'un Ordinateur dans un Domaine

Un ordinateur peut avoir l'un des trois statuts :

- **Indépendant** : ne fait pas partie d'un domaine.
- **Membre du domaine** : utilisateur authentifié par le contrôleur du domaine.
- **Contrôleur de domaine** : serveur hébergeant Active Directory.

Cas Pratique – Gestion des Salles de TP

Problème :

- Chaque étudiant doit avoir un compte **différent sur chaque ordinateur** du département informatique.

Solution :

- Mettre en place **un service d'annuaire (Active Directory)** :
    - Un seul **compte unique par étudiant**
    - Accès à **tous les postes** du département
    - Authentification **centralisée**
    - Meilleure sécurité et facilité de gestion

QCM

1. Quelle est la différence principale entre un réseau administré et un réseau non-administré ?
a) Le réseau administré ne partage pas de fichiers
b) Le réseau administré nécessite un administrateur et une configuration centralisée
c) Le réseau non-administré utilise des serveurs DNS
d) Le réseau non-administré est plus sécurisé
✅ **Réponse : b**

2. Quel est un exemple typique de réseau non-administré ?
a) Réseau d'entreprise avec Active Directory
b) Réseau d'un hôpital centralisé
c) Réseau domestique entre un PC, une imprimante et une box Internet
d) Réseau client/serveur avec plusieurs domaines
✅ **Réponse : c**

3. Dans un modèle Peer-to-Peer, chaque machine peut :
a) Uniquement agir comme client
b) Accéder uniquement à Internet
c) Être à la fois client et serveur
d) Gérer l'annuaire central
✅ **Réponse : c**

4. Quelle est une caractéristique du modèle Peer-to-Peer ?
a) Centralisation de l'authentification
b) Administration hiérarchique
c) Partage structuré des fichiers
d) Sécurité limitée
✅ **Réponse : d**

5. Le serveur DHCP a pour rôle principal de :
a) Traduire les noms de domaine en adresses IP
b) Stocker des fichiers en réseau
c) Attribuer automatiquement des adresses IP
d) Fournir un accès à Internet
✅ **Réponse : c**

6. Quelle est la fonction principale d'un annuaire dans un réseau ?
a) Gérer les connexions Internet
b) Sauvegarder les données utilisateurs

c) Centraliser l’authentification et la gestion des ressources
d) Bloquer les accès non autorisés
✅ **Réponse : c**

7. Quel service Microsoft permet la gestion hiérarchique des utilisateurs dans un réseau ?
a) DNS
b) Active Directory
c) DHCP
d) FTP
✅ **Réponse : b**

8. Dans Active Directory, qu’est-ce qu’un objet “Utilisateur” contient ?
a) Le mot de passe administrateur seulement
b) Un nom, prénom, fonction, etc.
c) L'adresse IP de l'ordinateur
d) Un fichier partagé
✅ **Réponse : b**

9. Quel est le rôle du Contrôleur de Domaine (DC) ?
a) Configurer le routeur
b) Partager des imprimantes
c) Authentifier les utilisateurs et appliquer les règles de sécurité
d) Installer des mises à jour logicielles
✅ **Réponse : c**

10. Quel statut peut avoir un ordinateur dans un domaine Active Directory ?
a) Exclusivement un contrôleur de domaine
b) Indépendant, membre du domaine ou contrôleur de domaine
c) Serveur uniquement
d) Uniquement client local
✅ **Réponse : b**

Chapitre 2 : Administration des comptes d’utilisateurs

1/Introduction

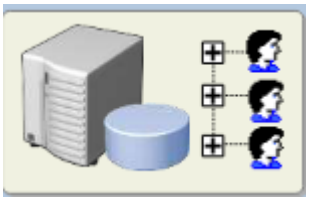
- **Administrer** = Gérer des **entités de sécurité** (utilisateurs, ordinateurs, groupes) par rapport à des **ressources réseau**.

- Ces entités sont appelées **objets de sécurité** :

    - **Utilisateur** (Classe *User*)
    - **Ordinateur** (Classe *Computer*)
    - **Groupe** (Classe *Group*)

2/Types de comptes d'utilisateurs

a. Comptes locaux

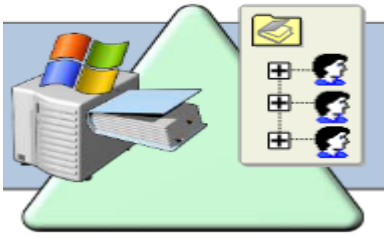


- Stockés localement sur un ordinateur (dans **SAM** – *Security Account Manager*).
- Chaque poste a ses propres comptes indépendants.
- **Problème** : un compte doit être créé **sur chaque PC**, ce qui complique la gestion.

Scénario 1 : Comptes locaux

- Entreprise avec 3 PC : PC1, PC2, PC3.
- Pierre a un compte local sur PC1 uniquement.
- Il peut se connecter **sur PC1** avec ses identifiants.
- Sur PC2 et PC3, impossible de se connecter car son compte n'existe pas.
- Pour que Pierre puisse utiliser tous les PCs, il faudrait créer un compte Pierre différent sur chaque machine, avec des mots de passe différents.
- **Inconvénient** : gestion difficile, plusieurs comptes à gérer.

b. Comptes d'utilisateurs de domaine



- Stockés dans **Active Directory** (base centralisée).
- Un **seul compte** permet à l'utilisateur de se connecter sur **tous les postes du domaine**.
- **Exemple** : Pierre@entreprise.local peut se connecter à PC1, PC2 et PC3 avec le **même identifiant et mot de passe**.
- **Comparaison** :
  - Compte local = **une clé différente** pour chaque porte.
  - Compte de domaine = **un badge unique** pour toutes les portes.

Scénario 2 : Compte de domaine

- Pierre possède un compte de domaine Pierre@entreprise.local.
- Il se connecte avec ces mêmes identifiants sur PC1, PC2 et PC3.
- Un seul compte à gérer pour tous les ordinateurs du domaine.
- **Analogie** : compte local = une clé différente par porte ; compte de domaine = un badge unique ouvrant toutes les portes.
- Le **contrôleur de domaine** gère l'authentification centralisée.

3. Hiérarchie et organisation des comptes

- Les comptes peuvent être organisés selon deux logiques :
  - **Géopolitique** : par région (Amérique du Nord, Amérique du Sud…)
  - **Organisationnelle** : par service (Comptabilité, Ventes…)

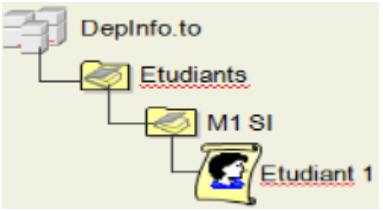
4. Noms et identifiants des comptes de domaine

- **Nom d'ouverture de session** : *Etudiant 1*
- **Nom complet** (UPN) : *Etudiant1@depInfo.to*
- **Chemin LDAP** (utilisé pour accéder aux objets dans AD) :

  CN=Etudiant 1,OU=M1 SI,OU=Etudiants,DC=DepInfo,DC=TO

  - **CN** : *Common Name* (nom de l'objet) //dans le cours c'est command name mais d'après chatgpt,deep seek c'est faux.
  - **OU** : *Organizational Unit* (Unité d'organisation)
  - **DC** : *Domain Component* (nom du domaine, pas "Contrôleur de domaine")

5. Exemples de chemins LDAP



- Domaine : DC=DepInfo,DC=to
- Unité Etudiants : OU=Etudiants,DC=DepInfo,DC=to
- Unité M1 SI : OU=M1 SI,OU=Etudiants,DC=DepInfo,DC=to
- Utilisateur : CN=Etudiant 1,OU=M1 SI,OU=Etudiants,DC=DepInfo,DC=to

6. Options de mot de passe utilisateur

- **L'utilisateur doit changer le mot de passe** à la prochaine session.
- **L'utilisateur ne peut pas changer son mot de passe** (restriction).
- **Le mot de passe n'expire jamais** (souvent utilisé pour des comptes de service).

7. Création de comptes utilisateurs

a. Méthodes disponibles :

- **Console graphique** : DSA.MSC
- **Ligne de commande** : DSADD

b. Syntaxe DSADD

DSADD Classe "Chemin LDAP"

- Exemple – Créer une unité d'organisation :

  DSADD OU "OU=Etudiants,DC=DepInfo,DC=to"

- Exemple – Créer un utilisateur :

  DSADD User "CN=Etudiant 1,OU=M1 SI,OU=Etudiants,DC=DepInfo,DC=to"

QCM

1. Où sont stockés les comptes utilisateurs locaux ?
a) Dans Active Directory
b) Dans la base SAM locale de chaque ordinateur
c) Sur le serveur DNS
d) Dans le dossier "Comptes Utilisateurs" du Panneau de configuration
✅ **Réponse : b**

2. Quel est le principal inconvénient des comptes locaux ?
a) Ils nécessitent un accès Internet
b) Ils ne peuvent pas être supprimés
c) Il faut les recréer manuellement sur chaque ordinateur
d) Ils expirent automatiquement
✅ **Réponse : c**

3. Que permet un compte d'utilisateur de domaine ?
a) De se connecter uniquement sur le PC principal
b) D'installer des logiciels sur tous les ordinateurs
c) De se connecter à tous les postes du domaine avec un seul identifiant
d) De modifier tous les mots de passe du réseau
✅ **Réponse : c**

4. Lequel de ces éléments correspond à un identifiant de connexion complet (UPN) ?
a) Pierre.localhost
b) user@entreprise.local
c) CN=Pierre,DC=local
d) admin/password
✅ **Réponse : b**

5. Dans le chemin LDAP, que signifie "OU" ?
a) Output Unit
b) Operational Usage
c) Organizational Unit
d) Object Utility
✅ **Réponse : c**

6. Quel est le rôle du contrôleur de domaine dans un domaine Windows ?
a) Sauvegarder tous les fichiers des utilisateurs
b) Gérer l'authentification centralisée des utilisateurs
c) Modifier les mots de passe automatiquement
d) Analyser les disques durs
✅ **Réponse : b**

7. Quelle commande permet de créer un utilisateur via la ligne de commande ?
a) DSGET User
b) DSA.MSC
c) DSADD User

d) LDAPADD CN
✅ **Réponse : c**

8. Quel chemin LDAP est correct pour un utilisateur ?
a) OU=Etudiants,CN=Etudiant 1,DC=DepInfo,DC=to
b) CN=Etudiant 1,OU=M1 SI,OU=Etudiants,DC=DepInfo,DC=to
c) DC=Etudiant 1,OU=SI,OU=Etudiants,DC=DepInfo
d) User=Etudiant1@DepInfo.to
✅ **Réponse : b**

9. Quelle option empêche un utilisateur de modifier son mot de passe ?
a) Le mot de passe expire
b) L'utilisateur ne peut pas changer son mot de passe
c) Réinitialisation forcée
d) Authentification temporaire
✅ **Réponse : b**

10. Quelle interface graphique permet de gérer les comptes utilisateurs ?
a) DNS.MSC
b) DHCP.MSC
c) DSA.MSC
d) DSADD
✅ **Réponse : c**

Chapitre 3 : Administration des groupes

1/ Introduction

L'administration des groupes concerne la gestion des **entités de sécurité** suivantes :

- Utilisateurs
- Ordinateurs
- Groupes

2/Utilité des groupes

Les groupes permettent de **simplifier la gestion des autorisations** d'accès aux ressources.
⚠️ *Un groupe n'est pas un conteneur* : un utilisateur **appartient** à un groupe, il n'est pas *stocké* dedans.

Un groupe est défini par :

- **Un type** (Sécurité ou Distribution)
- **Une étendue** (Globale, Domaine local ou Universelle)

3/ Types de groupes

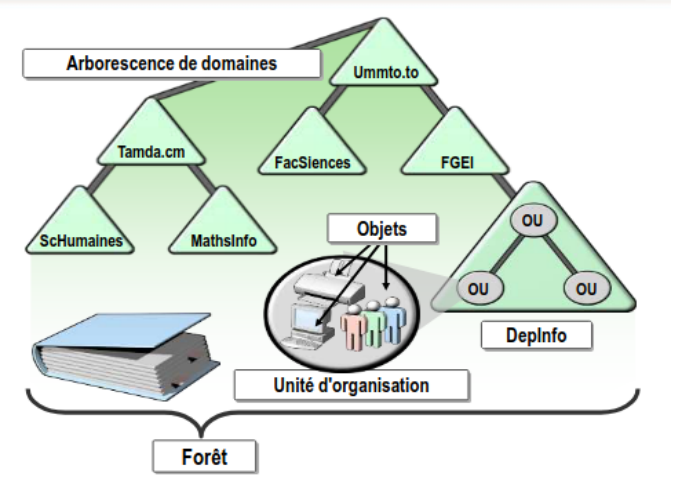
Type	Description
Sécurité	Utilisé pour gérer les **droits et autorisations** d'accès aux ressources.
Distribution	Utilisé uniquement pour la **messagerie** (ex. listes de diffusion). Pas utilisable pour les autorisations.

4/Étendue des groupes

Étendue	Membres admis	Portée des autorisations
Global	Utilisateurs & ordinateurs du même domaine	Tous les domaines de la **forêt**
Domaine local	Utilisateurs, ordinateurs & groupes globaux **de toute la forêt**	Uniquement dans **le domaine local**
Universel	Utilisateurs, ordinateurs & groupes globaux **de tout domaine**	Tous les domaines de la **forêt**

5/Notion de forêt

Une **forêt** est une structure hiérarchique de domaines dans Active Directory.
Elle peut contenir plusieurs **domaines**, **unités d'organisation (OU)** et **objets**.



Exemple :

Forêt : Ummto.to
├── Domaine : FGEIFacSciences
├── Domaine : MathsInfo
├── Domaine : ScHumaines
└── OU : DepInfo

6/Stratégies de regroupement

Trois modèles d'organisation des groupes :

1. C → G → A

Comptes → Groupe Global → Autorisations

- On crée un groupe global regroupant les utilisateurs d'un service.

- Ce groupe est ensuite affecté à une ressource avec des autorisations.

Exemple :

- `G_Compta` → groupe global contenant tous les utilisateurs du service comptabilité.
- On donne à `G_Compta` un accès en lecture/écriture sur le dossier partagé `\\serveur\compta`.

🔸 **2. C → DL → A**

Comptes → Groupe Domaine Local → Autorisations

- Les comptes utilisateurs sont ajoutés directement dans un **groupe de domaine local**.
- Ce groupe reçoit ensuite les autorisations.

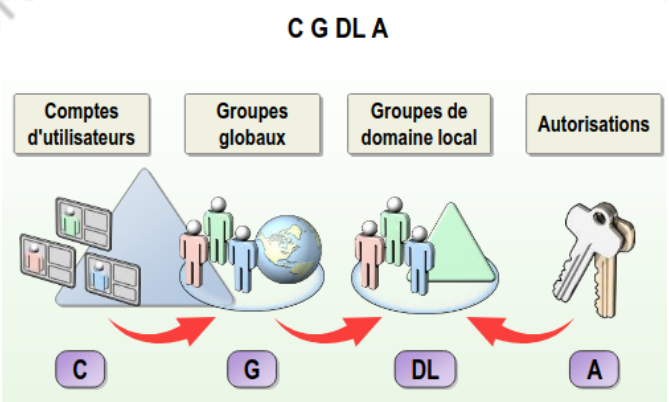
Exemple :

- `DL_Réseau` → groupe de domaine local.
- On y ajoute les utilisateurs `Ali`, `Sami`, `Amel`, etc.
- On donne à `DL_Réseau` un accès sur l'imprimante du département Réseau.

🔸 **3. C → G → DL → A**

Comptes → Groupe Global → Groupe Domaine Local → Autorisations

- On regroupe les utilisateurs dans un **groupe global** (par service ou par site).
- Ce groupe est ensuite **ajouté dans un groupe de domaine local**, qui est responsable de l'accès à une ressource spécifique.



Exemple :

- `G_Dev` contient tous les développeurs.
- `DL_Applications` est un groupe de domaine local responsable de l'accès à `\\serveur\app`.
- `G_Dev` est membre de `DL_Applications`, qui a l'autorisation d'accès à ce partage.

📌 Cette méthode est recommandée pour **simplifier la gestion dans les grandes entreprises**.

7/Convention de nommage des groupes

Inclure l'étendue dans le nom :

- **G** : Groupe global → `G_Compta`
- **DL** : Domaine local → `DL_Reseau`
- **U** : Universel → `U_Technique`

Le nom doit refléter **la fonction ou l'équipe** concernée (ex. `G_Marketing`, `DL_Professeurs`).

8/Création de groupes

Deux méthodes :

- **Interface graphique** : via la console `DSA.MSC`
- **Ligne de commande** : via `DSADD`

Syntaxe DSADD :

```
DSADD Group "Chemin_LDAP" -secgrp {yes|no} -scope {G|L|U}
```

Exemple DSADD :
DSADD Group "CN=G_M1SI,OU=M1SI,OU=Etudiants,DC=DepInfo,DC=to" -secgrp yes -scope G

- `-secgrp yes` → groupe de **sécurité**
- `-scope G` → groupe **global**

9/Affectation d'un responsable à un groupe

Permet de :

- Identifier clairement le responsable du groupe
- **Déléguer** à ce responsable le droit d'ajouter/supprimer des membres dans le groupe

Exemple :

- Le groupe `G_Admins` est géré par l'utilisateur `Samy`
- `Samy` pourra ajouter/supprimer des membres dans ce groupe via la console

QCM

1. Quel type de groupe est utilisé pour gérer les droits et autorisations d'accès aux ressources ?
a) Groupe Distribution
b) Groupe de travail

c) Groupe Sécurité
d) Groupe Local
✅ **Réponse : c**

2. Quelle étendue de groupe permet d'avoir des membres uniquement du même domaine ?
a) Universel
b) Global
c) Domaine local
d) Forêt
✅ **Réponse : b**

3. Quelle étendue de groupe peut contenir des utilisateurs, ordinateurs et groupes globaux de toute la forêt ?
a) Domaine local
b) Global
c) Universel
d) Local
✅ **Réponse : c**

4. Quelle est la portée des autorisations d'un groupe de domaine local ?
a) Toute la forêt
b) Tous les domaines du réseau
c) Uniquement dans le domaine local
d) Partout dans le monde
✅ **Réponse : c**

5. Dans le modèle de regroupement C → G → A, que représente "G" ?
a) Groupe de domaine local
b) Groupe global
c) Groupe universel
d) Groupe de travail
✅ **Réponse : b**

6. Quelle méthode de gestion des groupes est recommandée pour simplifier la gestion dans les grandes entreprises ?
a) C → DL → A
b) C → G → A
c) C → G → DL → A
d) C → A → G
✅ **Réponse : c**

7. Quel préfixe est utilisé pour un groupe universel dans la convention de nommage ?
a) G_
b) DL_
c) U_
d) UG_
✅ **Réponse : c**

8. Quelle commande ligne permet de créer un groupe de sécurité global ?
a) DSADD Group "CN=G_M1SI,OU=M1SI,DC=DepInfo" -secgrp no -scope L
b) DSADD Group "CN=G_M1SI,OU=M1SI,OU=Etudiants,DC=DepInfo,DC=to" -secgrp yes -scope G
c) DSADD User "CN=G_M1SI" -secgrp yes -scope U
d) ADDGROUP -name G_M1SI -scope global
✅ **Réponse : b**

9. Quelle fonction permet d'identifier et déléguer un responsable à un groupe ?
a) Gestionnaire de domaine
b) Contrôleur de domaine
c) Responsable du groupe
d) Propriétaire du groupe
✅ **Réponse : c**

10. Un groupe de distribution peut être utilisé pour :
a) Gérer les autorisations sur les fichiers
b) Créer des listes de diffusion pour la messagerie
c) Autoriser l'accès aux imprimantes
d) Gérer les comptes utilisateurs
✅ **Réponse : b**

Chapitre 4 : Administration des accès aux ressources (Dossiers partagés)

1/Introduction

Administrer signifie gérer les **entités de sécurité** (utilisateurs, groupes, ordinateurs) en leur attribuant des **autorisations** (accès à des ressources) ou des **droits** (actions système).

🔎 **Exemple :**
Dans une entreprise, l'administrateur décide que :

- L'équipe RH peut lire les fichiers "Salaires".
- Le directeur peut les modifier.
- Le personnel technique ne peut pas y accéder.

2/Autorisations

- **Définissent le type d'accès** accordé à une entité sur un objet.
- Attribuées aux **utilisateurs, ordinateurs et groupes**.
- Appliquées sur : fichiers, dossiers partagés, imprimantes.

3/Autorisations vs Droits

Type	Description	Exemples
Autorisation	Action sur une ressource	Imprimer, accéder à un dossier…
Droit	Action sur le système d'exploitation	Ouvrir une session, arrêter l'ordi

4/Nature des autorisations

- **Autorisation explicite :** accordée directement à l'entité.
- **Refus explicite :** refus direct → **prioritaire**.
- **Autorisation héritée :** transmise depuis un dossier parent.
- **Refus hérité :** transmis depuis un parent sans être explicite.
- **Refus implicite :** défaut si aucune autorisation définie.

🔁 ⚠️ **Le refus explicite l'emporte toujours.**

🔎 **Exemple (conflit d'autorisations) :**

- Imprimante partagée
- G1 : autorisé à imprimer
- G2 : refus explicite d'imprimer
- U1 ∈ G1 et G2 → **U1 sera refusé** car le refus explicite de G2 domine.

5/Contrôle d'accès

Le **contrôle d'accès** dans Windows Server garantit la sécurité des ressources (fichiers, dossiers, imprimantes).
Le contrôle d'accès repose sur :

- **Entités de sécurité** (utilisateur, ordinateur, groupe)
- **SID** (Security Identifier) : identifiant unique de chaque entité
- **DACL** (Discretionary Access Control List)
- **TGT** (Ticket Granting Ticket) : fourni lors de la connexion

6/Entités de sécurité

Ce sont les objets pouvant demander un accès à une ressource :

- Utilisateurs
- Groupes
- Ordinateurs

Chacune a un **identifiant unique** appelé **SID**.

7/SID (Security Identifier)

- **SID = identifiant unique** d'une entité.
- **Lié à la vie de l'objet** : s'il est supprimé puis recréé, il aura un **nouveau SID**.
- **Structure :** `SID_domaine + RID` (Relatif Identifier)

Exemple :
SID du domaine : `S-1-5-21-123456789-987654321-1112131415`
Utilisateur A reçoit le RID 1001 → SID final :
`S-1-5-21-123456789-987654321-1112131415-1001`

8/DACL

- Chaque ressource possède une DACL avec des **ACE** (Access Control Entry).
- Chaque ACE contient :
  - SID de l'entité
  - Type d'accès (Lecture, Écriture…)
  - Type d'entrée (Autoriser ou Refuser)
  - Héritage éventuel

Exemple :

- G1 (SID : FF01) → autorisé en **Modification**
- G2 (SID : E8F2) → refusé en **Lecture**

9/TGT (Ticket Granting Ticket)

À **chaque ouverture de session**, le système attribue à l'utilisateur un **TGT**, contenant :

- Son **SID**
- Les **SID de tous les groupes** auxquels il appartient

→ Ce TGT est comparé à la DACL pour valider l'accès à une ressource.

🔎 **Exemple :**
U1 (SID : FF01) ∈ G1 (SID : FF02) et G2 (SID : FF03)
TGT(U1) = {FF01, FF02, FF03}

10/Niveaux d'autorisations

Sur les dossiers partagés :

- **Lecture (L) :** Voir contenu uniquement
- **Modification (M) :** Lecture + Modifier/Supprimer
- **Contrôle total (CT) :** Modification + Modifier les autorisations

11/Autorisations standards vs spéciales

- **Standards :** prédéfinies (Lecture, Modification, CT…)
- **Spéciales :** personnalisées (ex : suppression sans écriture)

12/Dossiers partagés

- Permettent l'accès réseau à leur contenu.
- Par défaut, le groupe **Tout le monde** a la **Lecture**.
- Pour masquer un dossier → ajouter **$** (ex : `Finances$`).

13/Création de dossiers partagés

Méthodes :

- **Gestion de l'ordinateur**
- **Explorateur Windows**
- **Ligne de commande :** net share NomPartage=Lecteur:Chemin

14/Dossiers partagés publiés

Un **dossier partagé publié** est un objet dans **Active Directory (AD)**.

📌 **Avantages :**

- Les clients peuvent **chercher dans l'AD** les partages disponibles.
- **Pas besoin de connaître le nom du serveur**.

15/ Types d'accès à un dossier partagé

Type d'accès	Description
Accès local	Accès direct depuis l'ordinateur hébergeant le dossier
Accès réseau	Accès à distance via le réseau (depuis un autre PC)

📎 **Méthodes :**

- **Favoris réseau :** créer un raccourci vers un partage distant
- **Exécuter :** taper `\\NomServeur\NomPartage` ou `\\@IP\Partage`

16/Autorisations NTFS (système de fichiers)

- Appliquées localement sur fichiers/dossiers.
- Cumulées avec les autorisations de partage pour les accès réseau.

Fichiers	Dossiers
Contrôle total	Contrôle total
Modification	Modification
Lecture et exécution	Lecture et exécution
Écriture	Écriture
Lecture	Lecture
	Affichage du contenu

17/Cumul des autorisations

- Un utilisateur hérite des autorisations de **tous ses groupes**.
- Les autorisations **se cumulent** :
    - L + M = M
    - L + CT = CT
    - L + M + CT = CT

⚠️ **Refus explicite > toute autre autorisation**

- Refus(L) + CT = Refus(L)

18/Calcul des autorisations effectives

Contexte	Calcul
Accès local	Autorisations **NTFS uniquement**
Accès réseau	Comparer **NTFS vs Partage** → Prendre la **plus restrictive**

Exemple 1 :

- NTFS = Contrôle total
- Partage = Lecture
  → Résultat = **Lecture** (plus restrictive)

Exemple 2:

Soit un dossier partagé qui possède la liste des autorisations suivantes et **U** un utilisateur qui demande l'accès au dossier partagé

	Autorisations Partage	Autorisations NTFS
G1	L(ok)	CT(ok)
G2	M(ok)	L(ok)

1) Si un utilisateur U ϵ G1
   - Si U accède en local on aura : **CT** (Contrôle total)
   - Si U accède en réseau on aura : L vs CT = **L** (Lecture)
2) Si un utilisateur U ϵ G2
   - Si U accède en local on aura : **L** (Lecture)
   - Si U accède en réseau on aura : M vs L = **L** (Lecture)
3) Si un utilisateur U ϵ (G1 et G2)
   - Si U accède en local on aura : CT + L = CT (contrôle total)
   - Si U accède en réseau on aura : (CT + L) vs (L+M)=CT vs M= **M** (Modification)

QCM

1. Que signifie un refus explicite dans les autorisations d'accès ?
a) Autorisation donnée par défaut
b) Autorisation héritée d'un dossier parent
c) Refus direct prioritaire sur toute autre autorisation
d) Refus implicite par défaut
✅ **Réponse : c**

2. Quelle entité possède un SID (Security Identifier) unique ?
a) Utilisateur uniquement
b) Groupe uniquement
c) Ordinateur uniquement
d) Utilisateur, groupe et ordinateur
✅ **Réponse : d**

3. Que contient une DACL (Discretionary Access Control List) ?
a) Une liste de tous les utilisateurs
b) Les SID des entités autorisées et refusées avec type d'accès
c) Un mot de passe de sécurité
d) Le chemin du dossier partagé
✅ **Réponse : b**

4. Quel est le rôle du TGT (Ticket Granting Ticket) lors de la connexion ?
a) Stocker le mot de passe utilisateur
b) Contenir les SID de l'utilisateur et de ses groupes pour vérifier l'accès
c) Accorder un accès total à tous les dossiers
d) Servir uniquement aux imprimantes partagées
✅ **Réponse : b**

5. Quelle autorisation correspond au niveau "Modification" sur un dossier partagé ?
a) Lecture uniquement
b) Lecture + Modifier/Supprimer
c) Contrôle total
d) Écriture seule
✅ **Réponse : b**

6. Que fait le symbole $ à la fin du nom d'un dossier partagé (exemple : Finances$) ?
a) Donne un accès complet
b) Rend le dossier accessible à tous
c) Masque le dossier partagé sur le réseau
d) Crée une copie du dossier
✅ **Réponse : c**

7. Lors d'un accès réseau, quelles autorisations sont prises en compte ?
a) Uniquement les autorisations NTFS
b) Uniquement les autorisations de partage
c) Les deux : NTFS et partage, la plus restrictive est appliquée
d) Aucune, accès libre
✅ **Réponse : c**

8. Quelle commande permet de créer un dossier partagé en ligne de commande ?
a) net user NomPartage=Lecteur:Chemin
b) net share NomPartage=Lecteur:Chemin
c) share net NomPartage=Lecteur:Chemin
d) create share NomPartage=Lecteur:Chemin
✅ **Réponse : b**

9. Quelle différence existe-t-il entre autorisations et droits ?
a) Autorisations = actions sur le système, Droits = actions sur une ressource
b) Autorisations = actions sur une ressource, Droits = actions sur le système
c) Pas de différence
d) Droits ne concernent que les utilisateurs locaux
✅ **Réponse : b**

10. Quelle est la portée d'un refus explicite dans la gestion des accès ?
a) Il est moins prioritaire qu'une autorisation explicite
b) Il est prioritaire et bloque l'accès même si d'autres groupes autorisent
c) Il n'a aucune importance
d) Il s'applique uniquement sur les imprimantes
✅ **Réponse : b**

Chapitre 5 : Implémentation des stratégies de groupe (GPO)

1/Introduction

Pour gérer et contrôler l'environnement des utilisateurs et ordinateurs dans un réseau, on applique des **règles et configurations** via :

- **Stratégies locales** : sans Active Directory, sur un seul PC.
- **Stratégies de groupe (GPO)** : avec Active Directory, à l'échelle du domaine.

🔒 **Objectifs :**

- Restreindre l'accès à des paramètres.
- Bloquer l'installation de logiciels.
- Définir des paramètres système (fond d'écran, page d'accueil, etc.).

2/Qu'est-ce qu'une GPO ?

Une **GPO (Group Policy Object)** est un **objet qui regroupe un ou plusieurs paramètres** permettant de configurer et contrôler l'environnement des utilisateurs et/ou des ordinateurs dans un réseau Active Directory.

- Une GPO contient **des paramètres de configuration** qui s'appliquent soit aux **comptes utilisateurs**, soit aux **ordinateurs**, ou aux deux.

3/Exemples de paramètres

👩‍💻 **Paramètres utilisateur :**

- Interdire l'accès au Panneau de configuration
- Désactiver le gestionnaire de tâches
- Définir la page d'accueil Internet Explorer
- Définir l'adresse du serveur proxy

💻 **Paramètres ordinateur :**

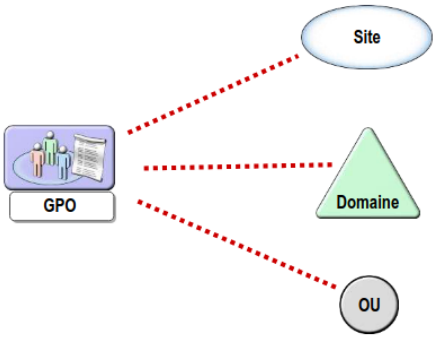
- Désactiver les ports USB
- Imposer un fond d'écran
- Interdire l'installation de logiciels

4/Catégories de paramètres GPO

- **Modèles d'administration** (Bureau, Panneau de config, Menu Démarrer, etc.)
- **Sécurité** (mots de passe complexes)
- **Installation logicielle** (ex : déployer MS Office)
- **Scripts** (connexion/déconnexion avec messages)
- **Internet Explorer** (page d'accueil par défaut)
- **Redirection de dossiers** (ex : "Mes Documents" vers un serveur)

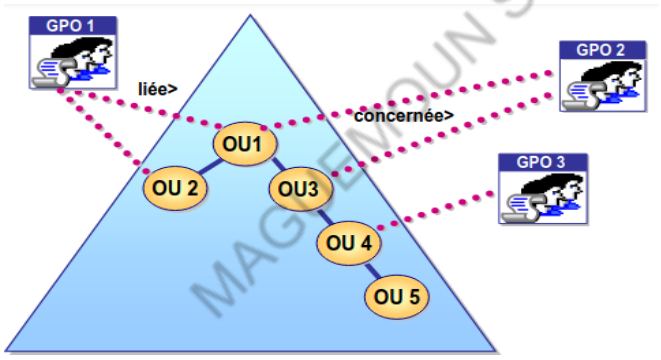
5/Lien d'une GPO

Une GPO peut être liée à :



- Un **site**
- Un **domaine**
- Une **unité d'organisation (OU)**

Schéma possible :



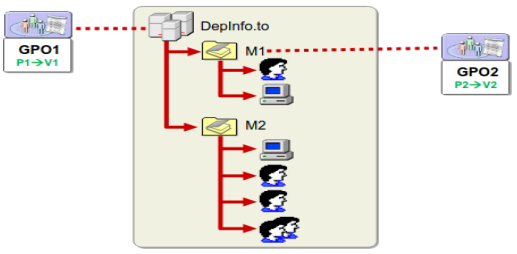
6/Outil de gestion des GPO

🛠️ **GPMC.MSC** : Console de gestion des stratégies de groupe
Permet de **créer, lier, modifier, supprimer, bloquer ou forcer** les GPO.

7/Héritage des GPO

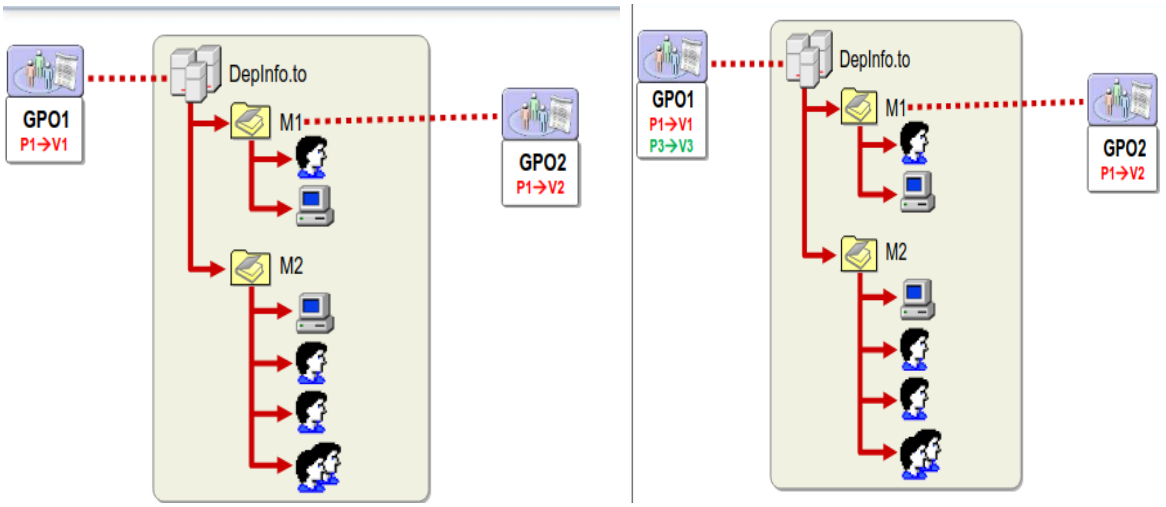
✅ **Sans conflit :**

Les paramètres hérités s'appliquent dans l'ordre hiérarchique (Domaine → OU).



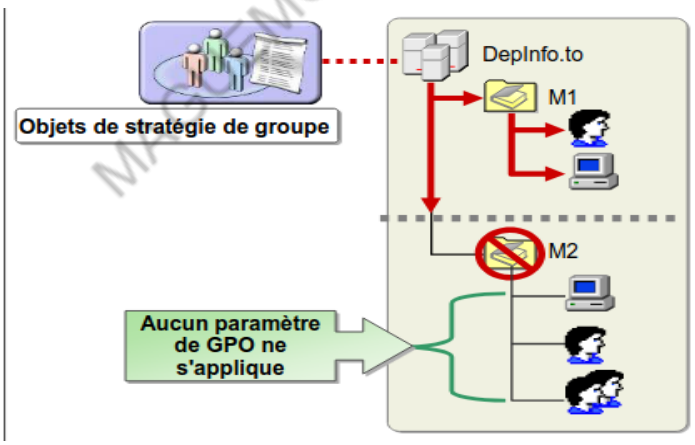
⚠️ **Avec conflit :**

Si deux GPO définissent le **même paramètre**, la **GPO la plus proche** de l'objet (ex : OU) **prend le dessus**.



8/Options d'héritage

- **Héritage activé par défaut**
- On peut **bloquer l'héritage** d'une OU (aucune GPO parentale ne s'applique).
- Option **"Appliquer" (force)** peut écraser un blocage.



9/Actualisation des GPO

🖥️ Pour appliquer ou réactualiser une stratégie de groupe :

gpupdate

QCM

1. Qu'est-ce qu'une GPO ?
a) Un programme antivirus
b) Un objet regroupant des paramètres pour configurer utilisateurs et ordinateurs dans AD

c) Une unité d’organisation
d) Un dossier partagé
✅ **Réponse : b**

2. Quel outil permet de gérer les stratégies de groupe ?
a) DSA.MSC
b) GPMC.MSC
c) CMD.EXE
d) REGEDIT
✅ **Réponse : b**

3. À quoi peut-on lier une GPO ?
a) Un fichier
b) Un site, un domaine, ou une unité d’organisation (OU)
c) Un utilisateur uniquement
d) Une imprimante réseau
✅ **Réponse : b**

4. Quelle catégorie de paramètres GPO permet de rediriger des dossiers comme "Mes Documents" vers un serveur ?
a) Sécurité
b) Modèles d’administration
c) Redirection de dossiers
d) Installation logicielle
✅ **Réponse : c**

5. Que se passe-t-il si deux GPO définissent un même paramètre sur une unité d’organisation (OU) ?
a) La première GPO appliquée est prioritaire
b) La GPO la plus proche de l’objet (ex : OU) a la priorité
c) Aucune GPO est appliquée
d) Les deux paramètres sont fusionnés automatiquement
✅ **Réponse : b**

6. Quelle commande permet de forcer l’actualisation des stratégies de groupe sur un poste ?
a) gpresult
b) gpupdate
c) net share
d) dsadd
✅ **Réponse : b**

7. Parmi ces paramètres, lequel est un paramètre utilisateur GPO ?
a) Désactiver les ports USB
b) Imposer un fond d’écran
c) Désactiver le gestionnaire de tâches
d) Interdire l'installation de logiciels
✅ **Réponse : c**

8. Quelles sont les deux grandes catégories de paramètres dans une GPO ?
a) Utilisateur et Ordinateur
b) Réseau et Sécurité
c) Local et Global
d) Active Directory et NTFS
✅ **Réponse : a**

9. Qu'est-ce qu'on peut faire avec l'option "Appliquer" (force) sur une GPO ?
a) Bloquer la GPO
b) Empêcher l'héritage
c) Forcer l'application de la GPO même si l'héritage est bloqué
d) Supprimer la GPO
✅ **Réponse : c**

10. Quelle est la différence principale entre une stratégie locale et une GPO ?
a) La stratégie locale s'applique à tout le domaine, la GPO seulement à un PC
b) La stratégie locale s'applique à un seul PC, la GPO s'applique à l'échelle du domaine via Active Directory
c) La stratégie locale est une GPO avancée
d) Il n'y a pas de différence
✅ **Réponse : b**

Chapitre 6 : Déploiement des logiciels via les GPO

1/Introduction

- Le déploiement manuel des logiciels est **complexe et chronophage**.
- **Active Directory + GPO** permettent de **centraliser, automatiser et sécuriser** l'installation, la maintenance et la suppression des logiciels.

2/Cycle de vie des logiciels

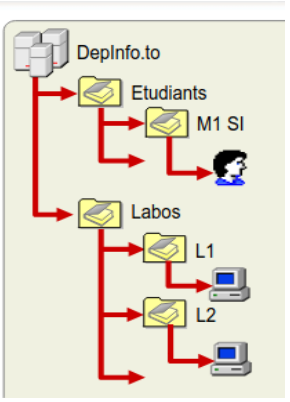
1. **Préparation**
2. **Déploiement**
3. **Maintenance (mises à jour)**
4. **Suppression**

3/Windows Installer

Windows Installer est un **service** de Windows permettant de :

- Automatiser l'installation, la configuration et la réparation des applications.
- Offrir une **suppression propre** et une **personnalisation** de l'installation.

4/Prérequis au déploiement



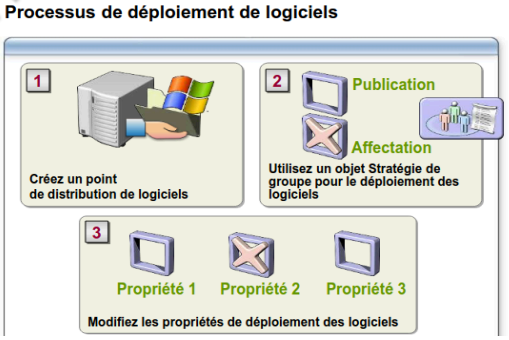
Pour un déploiement réussi, il faut :

- Une **bonne structure Active Directory** (OU par groupes d'utilisateurs/machines).
- Créer un **point de distribution** (partage réseau contenant le fichier `.msi`).
- Utiliser un **package logiciel au format `.MSI`** (Microsoft Installer).
- Lier une **GPO de déploiement** aux OU appropriées.

5/Outils de création de packages .MSI

- **Inno Setup**
- **EMCO MSI Package Builder**
- **Smart Packager**
- **Advanced Installer**
- **MSIX Packaging Tool**

6/Processus de déploiement logiciel via GPO



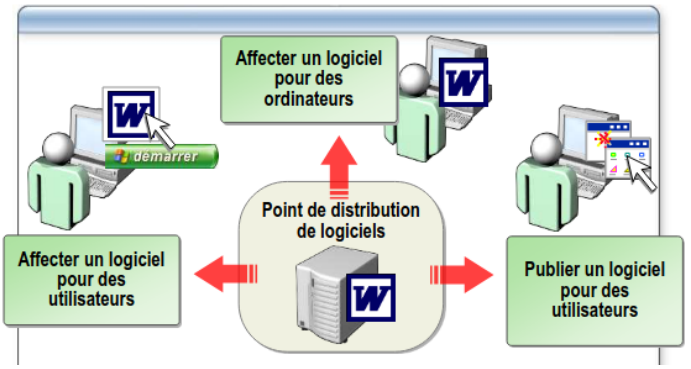
1. Créer un **point de distribution** (partage réseau accessible)
2. Créer une **GPO** avec un paramètre de déploiement
3. **Modifier les propriétés du déploiement** selon le mode choisi

7/Techniques de déploiement

✅ Affectation (Attribution)

- Installation automatique.
- **À un utilisateur** : installée au premier lancement.
- **À un ordinateur** : installée au démarrage de Windows.

Affectation de logiciels et publication de logiciels



📤 Publication

- L'utilisateur **voit** le logiciel dans *Ajouter/Supprimer des programmes* et **choisit de l'installer**.
- Ne fonctionne **que pour les utilisateurs**, pas pour les ordinateurs.

8/Suppression des logiciels

- **Suppression manuelle** depuis la GPO
- **Suppression forcée** : désinstallation automatique sans interaction de l'utilisateur

9/Problèmes courants et solutions

Symptôme	Cause	Solution
L'application n'apparaît pas dans *Ajouter/Supprimer des programmes*	L'application a été **affectée**, pas **publiée**	Modifier la stratégie
L'application n'apparaît pas dans le menu Démarrer	L'application a été **publiée**, pas **affectée**	Modifier la stratégie
L'application s'affiche mais ne peut pas être installée	Le **point de distribution** n'est pas accessible	Vérifier les autorisations réseau
Aucune application ne s'affiche	La GPO n'a pas été appliquée	Vérifier l'application de la GPO avec `gpresult` ou `gpupdate`

QCM

1. Quel est l'avantage principal d'utiliser GPO pour déployer des logiciels ?
a) Rendre l'installation manuelle plus rapide
b) Centraliser, automatiser et sécuriser le déploiement
c) Installer uniquement les logiciels gratuits
d) Supprimer automatiquement tous les logiciels
✅ **Réponse : b**

2. Quel format de package est requis pour le déploiement via GPO ?
a) .exe
b) .msi
c) .zip
d) .bat
✅ **Réponse : b**

3. Quel service Windows permet d'automatiser l'installation et la réparation des applications ?
a) Windows Defender
b) Windows Installer
c) Windows Update

d) Task Scheduler
✅ **Réponse : b**

4. Quelle condition est nécessaire avant de déployer un logiciel via GPO ?
a) Créer un point de distribution réseau contenant le fichier .msi
b) Installer le logiciel sur chaque poste client
c) Utiliser uniquement des fichiers .exe
d) Ne pas utiliser Active Directory
✅ **Réponse : a**

5. Quelle technique de déploiement installe automatiquement le logiciel au démarrage d'un ordinateur ?
a) Publication
b) Affectation à un utilisateur
c) Affectation à un ordinateur
d) Installation manuelle
✅ **Réponse : c**

6. La publication d'un logiciel via GPO permet à l'utilisateur de :
a) Installer automatiquement sans interaction
b) Voir le logiciel dans Ajouter/Supprimer des programmes et choisir de l'installer
c) Installer uniquement au démarrage de l'ordinateur
d) Installer seulement les mises à jour
✅ **Réponse : b**

7. Quelle est la différence principale entre l'affectation et la publication d'un logiciel ?
a) L'affectation est manuelle, la publication automatique
b) L'affectation installe automatiquement, la publication laisse le choix à l'utilisateur
c) La publication fonctionne pour les ordinateurs, l'affectation non
d) Il n'y a aucune différence
✅ **Réponse : b**

8. Que faut-il vérifier si une application n'apparaît pas dans le menu Démarrer après déploiement ?
a) Le point de distribution est inaccessible
b) L'application a été publiée mais pas affectée
c) La GPO n'est pas liée au domaine
d) L'ordinateur n'est pas allumé
✅ **Réponse : b**

9. Comment peut-on forcer la suppression automatique d'un logiciel via GPO ?
a) Suppression manuelle uniquement
b) Suppression forcée (désinstallation automatique sans interaction)
c) Désinstaller via le menu Démarrer
d) Par redémarrage de l'ordinateur
✅ **Réponse : b**

10. Quelle commande permet de forcer l'actualisation des stratégies de groupe sur un poste ?

a) gpresult

b) gpupdate

c) net share

d) ipconfig

✅ **Réponse : b**