ADMINISTRATION WINDOWS SERVER

Romain Pillon – 2022 – Version 1

AGENDA

Semestre 1

1. Windows Server
2. Active Directory
3. Stratégie de groupe
4. DHCP
5. DNS
6. (Routage)

Semestre 2

MODULE 2 – ACTIVE DIRECTORY

Annuaire mais pas que

MODULE 2 - OBJECTIFS

- Découvrir l'annuaire Active Directory
- Savoir installer un AD
- Configurer la gestion des droits avec AGDLP

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Domaine Active Directory

- Pour quoi faire ?
  - Centraliser la gestion des identités et de l'authentification.
  - Centraliser la gestion des paramètres utilisateurs et ordinateurs.
  - Fournir une base de fonctionnement aux services et outils Microsoft.

- Utilisation de protocoles standardisés : **DNS** / **LDAP** / **Kerberos**
  - **DNS** : Résolution des noms de machines et localisation de services.
  - **LDAP** : Interrogation de l'annuaire le long de l'arborescence.
  - **Kerberos** : Protocole d'authentification reposant sur un mécanisme de clés secrètes et l'utilisation de tickets.

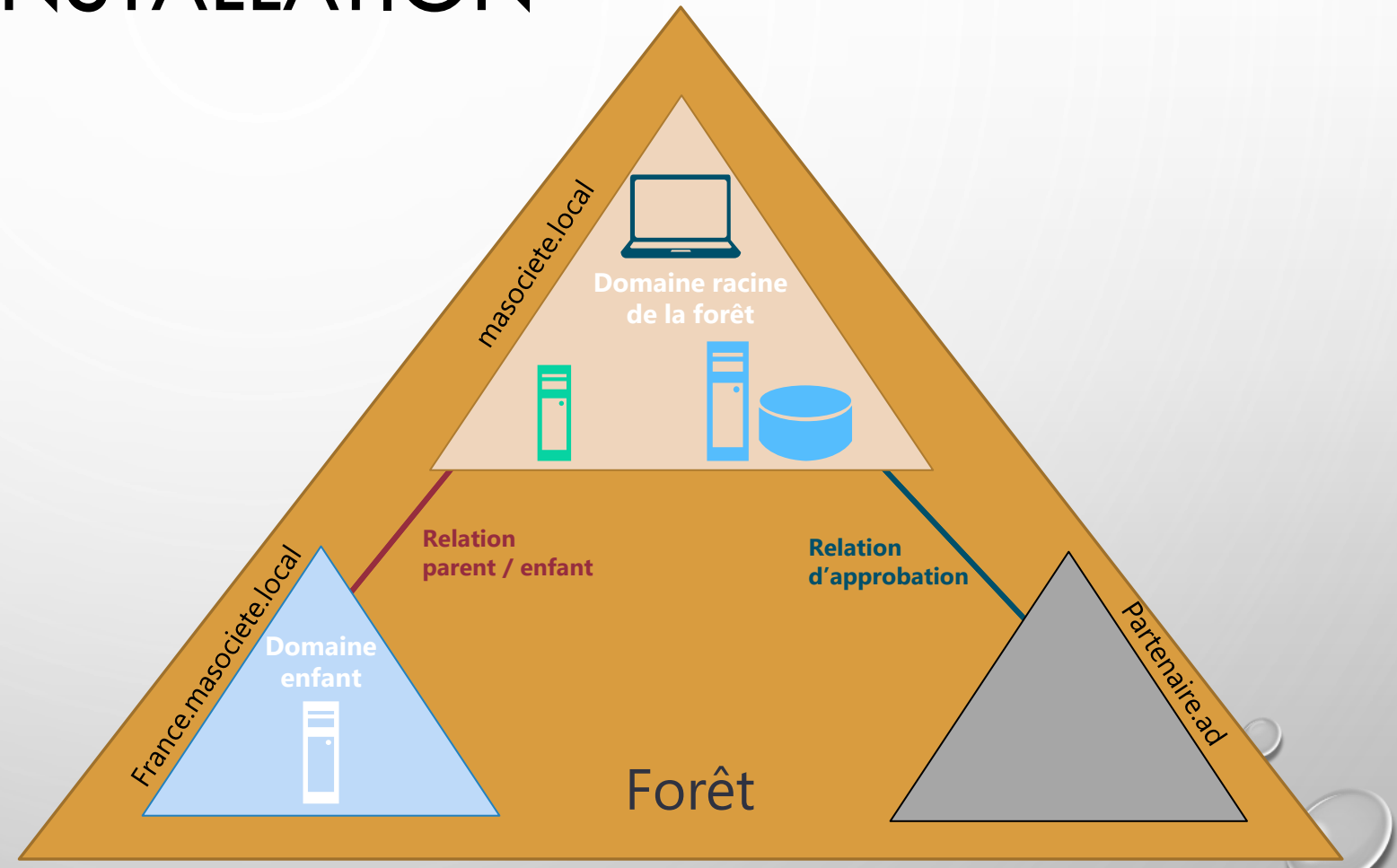
LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

La forêt Active Directory

Une forêt

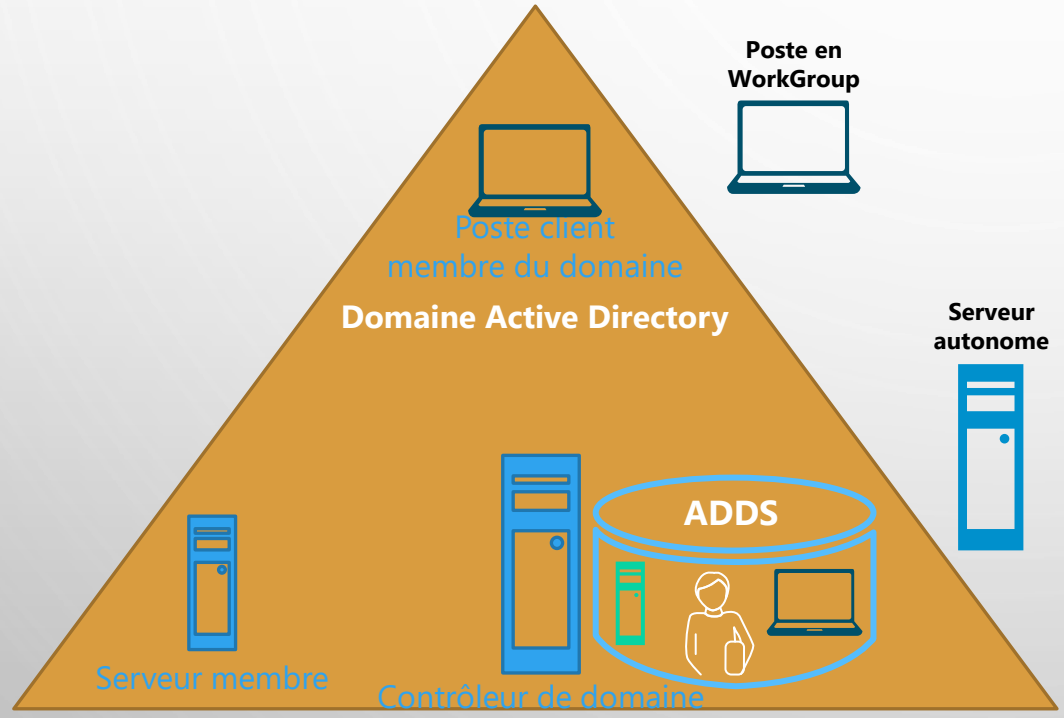
Comprend un ou plusieurs domaine AD partageant le même schéma, les mêmes informations de configuration et de recherche.

Les domaines d'une même forêt sont liés par une **relation d'approbation** transitive bidirectionnelle.



LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Le domaine



Un domaine Active Directory

Ensemble d'ordinateurs en réseau qui partagent une base de donnée commune.

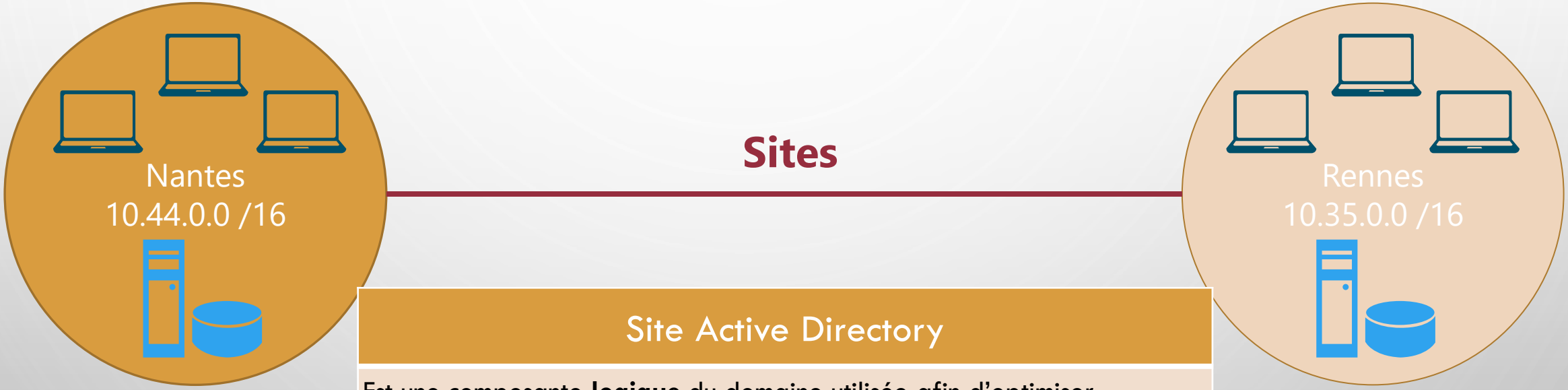
Un domaine est administré comme un ensemble, régi par des règles et procédures communes.

Le contrôleur de domaine

Les contrôleurs d'un domaine AD sont les serveurs qui assurent la gestion du domaine. Ils assurent les tâches d'hébergement et de gestion de la base AD, ainsi que l'authentification.

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Les sites



Site Active Directory

Est une composante **logique** du domaine utilisée afin d'optimiser :

- La réplication.
- L'accès aux ressources.

Il est composé d'un ou de plusieurs sous-réseaux TCP/IP.

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Prérequis pour un contexte de domaine

Avant de promouvoir un serveur en Contrôleur de Domaine, ces prérequis doivent être respectés :

Prérequis	Description
Nom d'hôte du poste	Le nom d'hôte et le suffixe DNS doivent être correctement définis.
Configuration réseau et adressage IP	Ces paramètres doivent être opérationnels.
Composants Windows	Les composants relatifs aux services ADDS doivent être installés.
Prise en compte de l'existant	Analyser l'infrastructure existante et déterminer les points essentiels.
Préparation de l'AD	La forêt ou le domaine peut être préparé lors de l'ajout d'un DC.

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Versions Active Directory

- Pour une forêt ou un domaine ciblé, les **niveaux fonctionnels** déterminent les **fonctionnalités** fournies au sein de la forêt et du domaine.
- Le choix des niveaux est **contraint** par les versions des **contrôleurs** présents au sein du domaine et de la forêt.

NF de domaine	2008 R2	2012 R2	2016
Version des CD	2008 R2		
	2012 R2	2012 R2	
	2016	2016	2016
	2019	2019	2019
NF de la forêt	**2008 R2**	**2012 R2**	**2016**

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Rétrograder / promouvoir un CD

- L'ajout et la suppression d'un contrôleur de domaine sont des actions qui impactent tous les contrôleurs de domaine de la forêt.
- Avant de rétrograder un contrôleur de domaine, on s'assurera qu'il ne dispose plus de rôles FSMO (voir diapo suivante)
- Sous Windows 2016 et ultérieur, afin de rétrograder un CD, utiliser la commande suivante :

```
PS C:\Windows\System32> Uninstall-AddsDomainController
```

LES SERVICES D'ANNUAIRE - PRÉSENTATION ET INSTALLATION

Les 5 rôles FSMO

	Rôles	Description
Forêt	**Maître de nom de domaine**	Il coordonne l'ajout ou suppression d'un domaine dans un forêt et le **renommage de domaine (Attention)**
	Maître de schéma	Peut modifier le schéma. Dans le schéma sont stockées les caractéristiques des objets. Les autres CD ont accès en lecture seul au schéma.
Domaine	**Maître RID**	Alloue les « bloc d'**ID**entificateurs **R**elatifs » aux autres CD. Ces derniers puisent dans le bloc pour attribuer les SID aux objets.
	Maître d'infrastructure	Responsable des objets des autres domaines de la forêt qui sont membres d'objets de son domaine.
	Maître émulateur PDC	Il coordonne au sein du domaine les mise à jour des mots de passe et des GPO ainsi que la synchronisation des horloges. Il gère également les incohérence de données (notamment les mot de passe)

MODULE 2 – TP3

- Objectifs:

Savoir créer un domaine et y intégrer des machines

- Consignes

Création d'un serveur et d'un client supplémentaire

Intégration dans le domaine

Vérification du fonctionnement

LES BASES DE GESTION D'UN DOMAINE

Objets de l'annuaire et outils de gestion

- Dans un contexte de domaine AD, les tâches courantes de gestion sont liées à l'administration des **principaux objets de l'annuaire**.

- La gestion de ces objets peut se faire :
  - Depuis la console Utilisateurs et ordinateurs Active Directory
  - Depuis le Centre d'administration Active Directory
  - En PowerShell

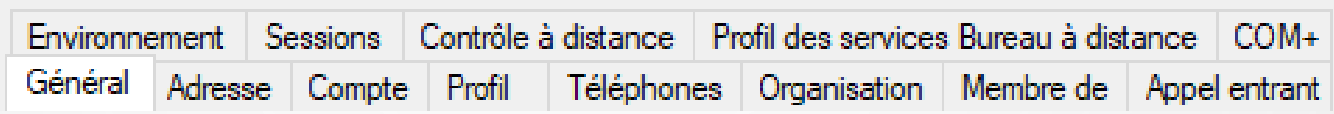
Entités de sécurité
Utilisateur
Ordinateur
Groupe

Conteneurs
Unité d'organisation
Conteneur système

LES BASES DE GESTION D'UN DOMAINE

Les caractéristiques de l'objet utilisateur

- Ces dernières sont regroupées graphiquement avec un ensemble de catégories.



- Elles sont relatives :
  - aux paramètres de l'utilisateur pour l'utilisation des services de bureau distant

Contrôle à distance	Environnement	Profil des services de bureau à distance	Sessions

  - aux informations générales concernant l'utilisateur

Adresse	Général	Organisation	Téléphones

  - aux informations nécessaires à sa connexion

Compte	Profil

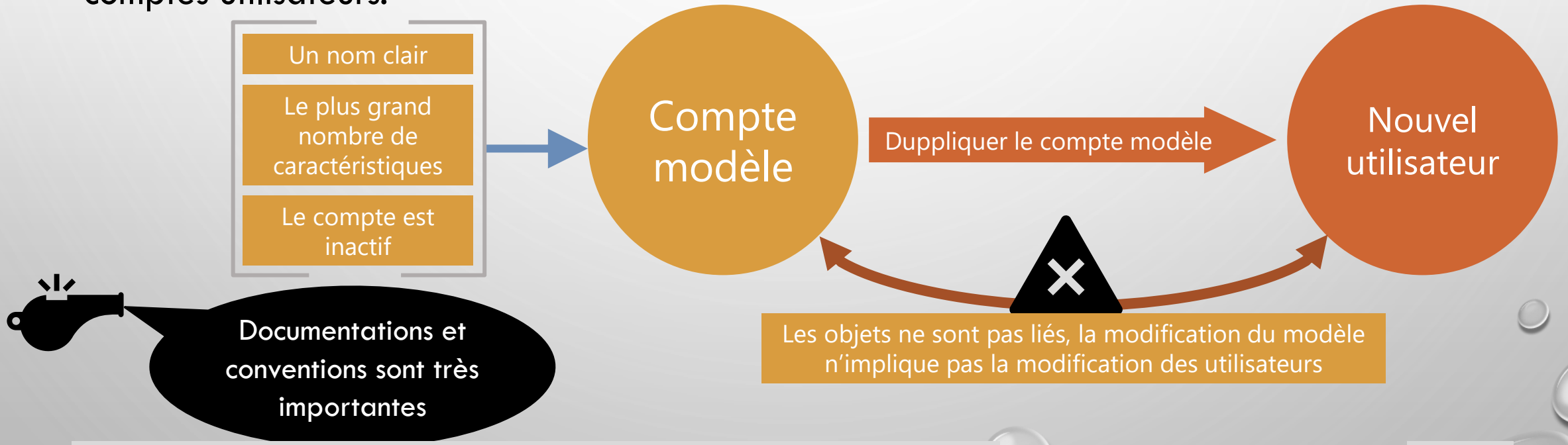
  - à l'appartenance aux groupes et aux paramètres utilisateur des connexions entrantes

Membres de	Appel entrant

LES BASES DE GESTION D'UN DOMAINE

Les modèles utilisateur

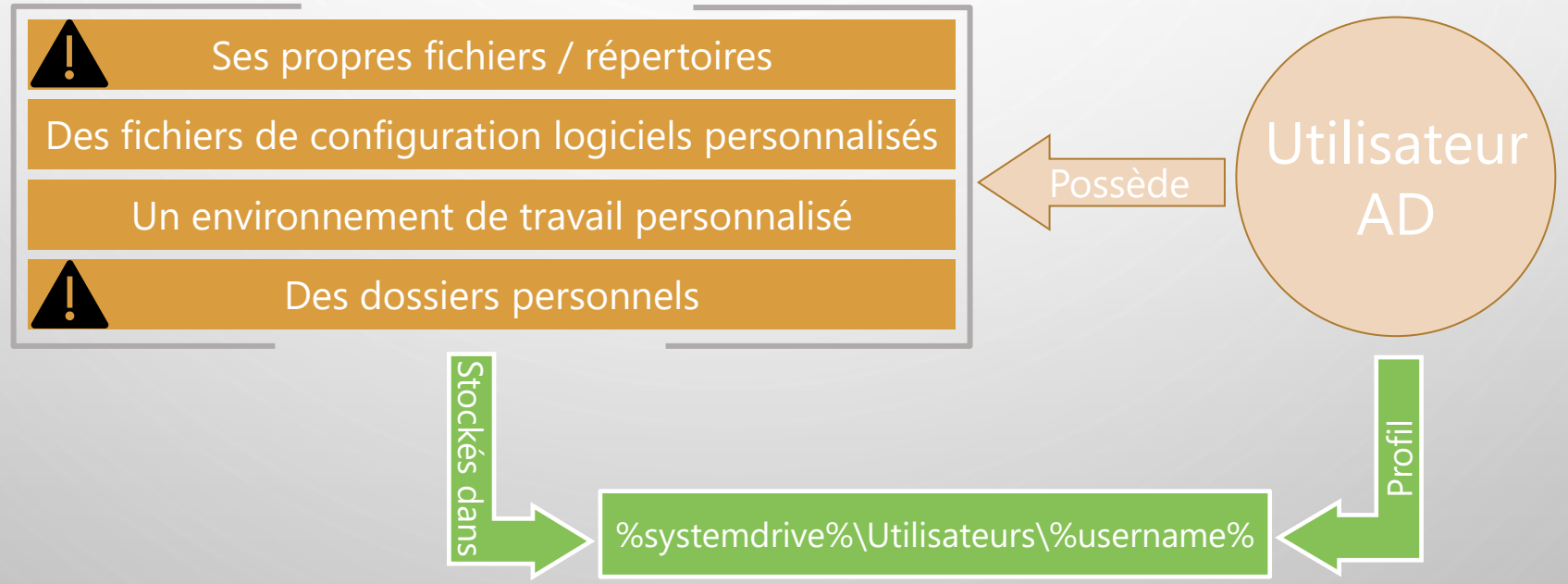
Il est conseillé d'utiliser des **modèles** de comptes pour simplifier la création de nouveaux comptes utilisateurs.



LES BASES DE GESTION D'UN DOMAINE

Les profils utilisateurs

Par défaut, les utilisateurs du domaine peuvent ouvrir une session sur les ordinateurs du domaine.



LES BASES DE GESTION D'UN DOMAINE

Les profils itinérants

Utilisés pour les utilisateurs ayant besoin de se connecter sur quel ordinateur du domaine et de retrouver leur environnement de travail.

1. Le profil est chargé sur l'ordinateur depuis un serveur de fichier
2. L'utilisateur travaille.
3. À la fermeture de session, le profil est synchronisé sur le serveur de fichier.

LES BASES DE GESTION D'UN DOMAINE

Les ordinateurs

- Dans un contexte de domaine, les membres s'authentifient afin de disposer d'un **jeton d'accès** permettant l'accès aux ressources du domaine.

- Ce processus est commun aux utilisateurs et aux ordinateurs.

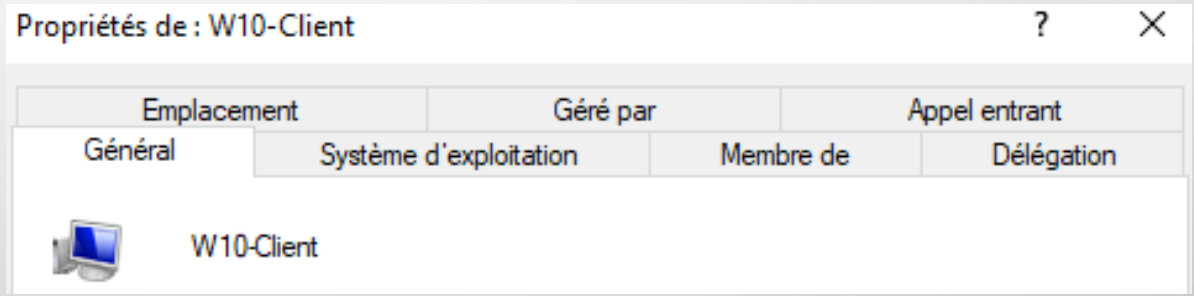
- Ceux-ci doivent donc disposer d'un **compte** dans le domaine.

LES BASES DE GESTION D'UN DOMAINE

Les caractéristiques de l'objet ordinateur

- Au même titre que l'objet utilisateur, l'objet ordinateur dispose de caractéristiques qui lui sont propres.

- Les principales caractéristiques d'un objet ordinateur sont :
  - Son nom et sa description
  - La version du SE
  - Ses groupes d'appartenance
  - …



LES BASES DE GESTION D'UN DOMAINE

Les groupes

- Les groupes sont des objets de l'annuaire.
- Tout groupe est caractérisé par un **type** et une **étendue**.
  - Il en existe deux types :

De **sécurité**	De **distribution**
Dispose d'un identifiant de sécurité (SID).	Ne dispose pas d'identifiant de sécurité.
Peut être utilisé pour répondre à un ensemble de besoins.	N'est utilisable qu'à des fins de messagerie.

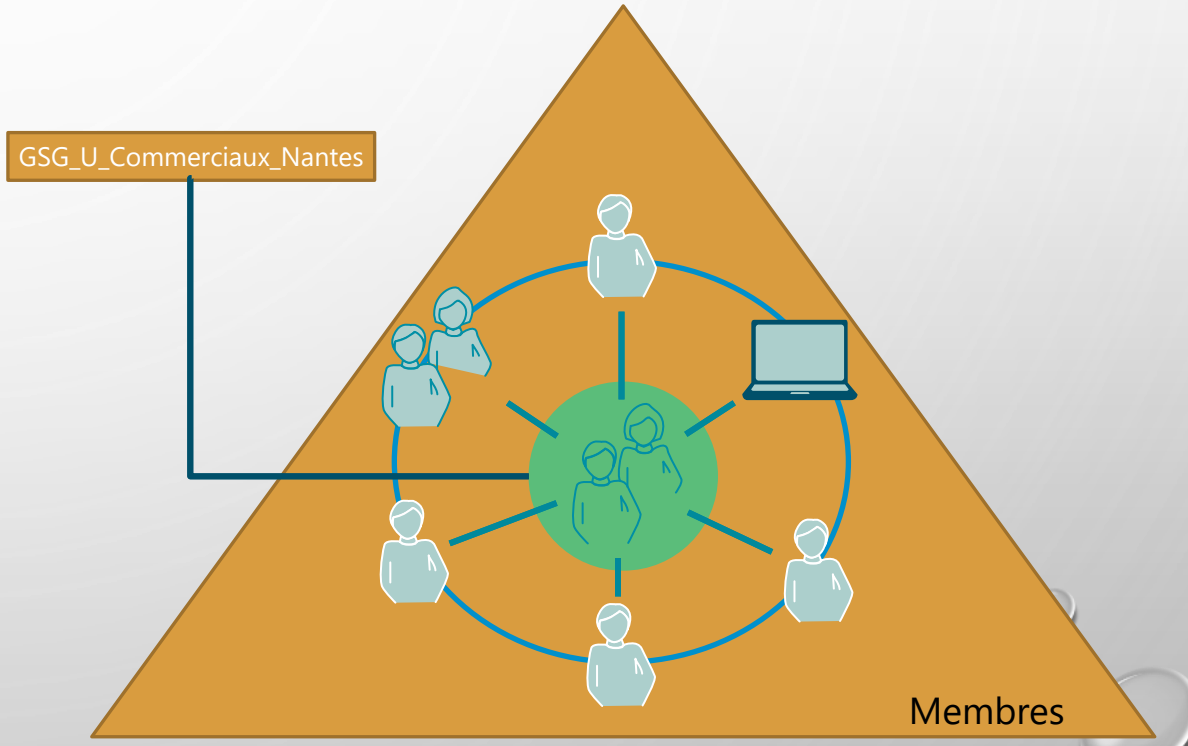
  - L'étendue du groupe détermine le périmètre d'appartenance des membres ainsi que celui d'utilisation.

Global	**Universel**	**De Domaine Local**	**Local**

LES BASES DE GESTION D'UN DOMAINE

Les groupes de sécurité globaux

Caractéristiques	
Utilité	Regrouper des objets qui possèdent des caractéristiques communes.
Contraintes d'appartenance	Ils ne peuvent contenir **que des objets** utilisateur, ordinateur ou groupe global **du même domaine.**
Contrainte d'utilisation	Ils peuvent être **utilisés** sur toute ressource du **domaine** ou approuvée (**forêt**).
Exemple de nom	GSG_U_Commerciaux_Nantes



LES BASES DE GESTION D'UN DOMAINE

Les groupes de sécurité de domaines locaux

Caractéristiques	
Utilité	Regrouper des objets qui requièrent un même privilège d'accès pour une ressource donnée.
Contraintes d'appartenance	Ils peuvent contenir **des objets** utilisateur, ordinateur ou groupe **de tout domaine de la forêt.**
Contrainte d'utilisation	Ils peuvent être **utilisés uniquement** sur les ressources de **leur domaine de création.**
Exemple de nom	DLSG_Comptabilite_Sur_SRVFIC_L

Ressource partagée

Marketing

Privilèges		Groupe de Domaine Local
CT		DLSG_Marketing_Sur_SRVFIC_CT
M		DLSG_Marketing_Sur_SRVFIC_M
L		DLSG_Marketing_Sur_SRVFIC_L
R		DLSG_Marketing_Sur_SRVFIC_R

LES BASES DE GESTION D'UN DOMAINE

Les groupes locaux

- On continue à les utiliser.
  - Les membres du domaine **conservent leur base SAM**.

- L'utilisation de ce type de groupe est **limitée et limitante**.
  - Ils ne peuvent être utilisés que sur leur poste d'appartenance.

- Cette limite peut être un atout pour certains besoins en termes de sécurité.

- C'est le **seul** type de groupe qui peut être utilisé **hors domaine**.

LES BASES DE GESTION D'UN DOMAINE

Les conteneurs système

- Les objets de l'annuaire AD sont stockés dans des conteneurs.
- Ces conteneurs système sont définis par défaut dans tout domaine AD.

Nom de l'objet	Fonction
Builtin	Eléments (utilisateurs et groupes locaux) présents dans la base SAM des CD avant leur promotion. Une fois la promotion faite, ces derniers sont déplacés dans ce conteneur.
Computers	Emplacement de stockage par défaut des comptes ordinateurs.
System	Emplacement de stockage des éléments nécessaires aux fonctionnement de l'AD et aux composants associés.
Users	Emplacement de stockage des groupes et utilisateurs existant par défaut dans un AD.

- Il n'est **pas** conseillé de conserver les comptes ordinateurs du domaine dans le conteneur Computer, de même pour les comptes utilisateurs dans le conteneur Users.

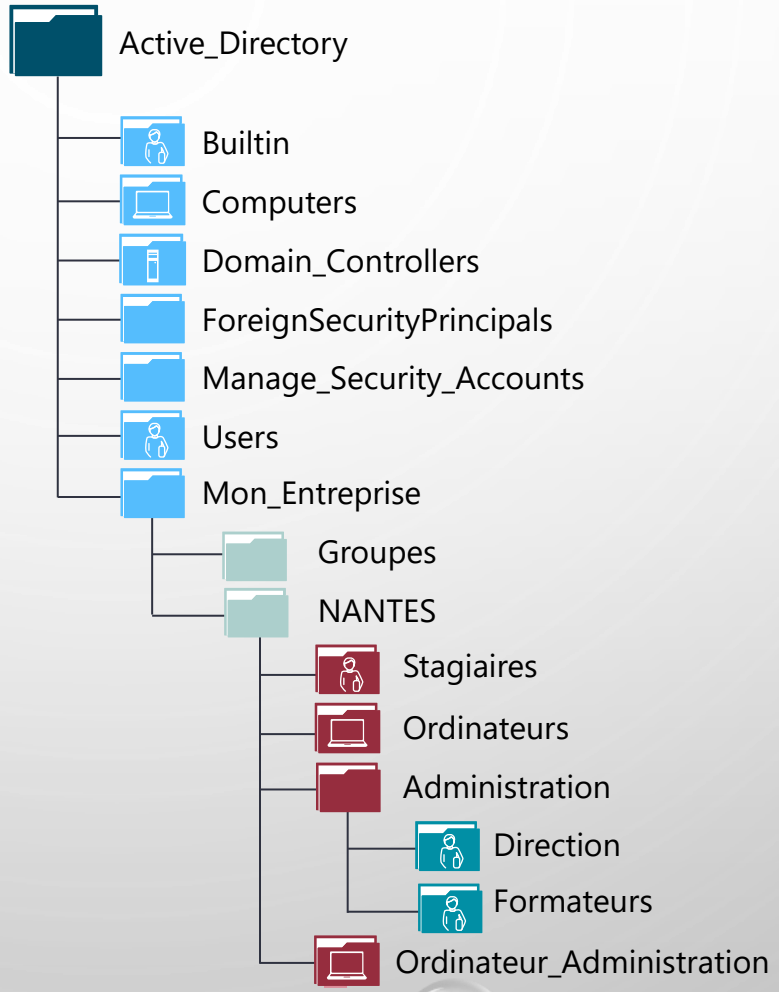
LES BASES DE GESTION D'UN DOMAINE

Les unités d'organisation

- Des conteneurs supplémentaires peuvent être créés :
  - **OU O**rganizational **U**nit / **UO U**nité d'**O**rganisation
- L'élaboration d'une structure organisationnelle doit prendre en considération les besoins suivants :
  - Les stratégies de groupe (**GPO G**roup **P**olicy **O**bject)
  - Les délégations administratives
  - L'organisation des objets dans l'arborescence
- Tout objet de l'annuaire ne peut être positionné directement que dans un seul conteneur.
- Attention :
  - **Sur les Contrôleurs de Domaine, les UO sont protégées contre toute suppression accidentelle (il est possible de modifier cela).**

LES BASES DE GESTION D'UN DOMAINE

Les unités d'organisation



LES BASES DE GESTION D'UN DOMAINE

Importation et exportation de comptes

- Quand un nombre important de comptes utilisateurs doit être créé, l'utilisation d'outils permet de **fiabiliser** et **réduire la durée de la tâche**.

- Ligne de commande : csvde
- PowerShell : `PS C:\Windows\System32> Import-Module -Name ActiveDirectory`

- Via des outils externes : IAM – Identity and Access management

MODULE 2 – TP4

- Objectifs

Se familiariser avec la gestions des utilisateurs, des groupes et des UO

- Consignes

Créer une arborescence et des groupes en fonction de l'organisation de l'entreprise

Créer des modèles d'utilisateurs

Instancier les utilisateurs

L'ACCÈS AUX RESSOURCES

Les ressources partagées

- Le **partage** de ressource est un service nécessaire aux utilisateurs.

- Sa mise en œuvre et sa gestion incombent à l'administrateur système qui doit respecter les exigences de **disponibilités** et de **sécurité**.

- Nous parlerons **d'espace disque partagé**.

L'ACCÈS AUX RESSOURCES

Utilité des autorisations NTFS

Sur un espace disque formaté en NTFS ou ReFS :

- Les autorisations NTFS permettent de définir quels sont les **privilèges d'accès**
- **Tous les dossiers et fichiers** d'un volume formaté y sont soumis

- Elles sont visualisables et/ou modifiables depuis l'onglet **Sécurité** des éléments

L'ACCÈS AUX RESSOURCES

Les caractéristiques des autorisations NTFS

- Deux niveaux de gestions sont disponibles :
  - Les autorisations **de base**
  - Les autorisations **avancées**
- La gestion des permissions est basée sur des règles **explicites**.
- Plusieurs règles d'accès peuvent s'appliquer à un même utilisateur.
- Chaque règle peut accorder des privilèges ou les ôter.
- Le mécanisme d'**héritage** s'applique aux autorisations positionnées sur des dossiers et s'appliquent aux objets enfants.
- Une règle de **refus** peut être explicite ou implicite.

L'ACCÈS AUX RESSOURCES

Les autorisations NTFS de base et avancées

- Pour répondre aux besoins courants, les autorisations **de base** permettent d'accorder les privilèges suivants :

Lecture	Liste de contenu	Lecture + exécution	Écriture	Modification	Contrôle Total

- Les privilèges complémentaires suivants peuvent être attribués, par les **autorisations avancées.**

Appropriation	Création de fichiers	Création de dossiers	Écriture des attributs étendus
Lecture des attributs étendus	**Modifier les autorisations**	**Suppression**	**Suppression de sous-dossiers et fichiers**

L'ACCÈS AUX RESSOURCES

Cumul d'autorisations

- Chaque autorisation s'applique à un objet **utilisateur** ou **groupe de sécurité**. Il est cependant préférable de n'appliquer des autorisations qu'aux **groupes**.
- Pour chaque entrée de contrôle d'accès, l'autorisation peut être appliquée :
  - **Autoriser** afin **d'accorder le privilège** correspondant
  - **Refuser** afin **d'ôter le privilège** correspondant
- À défaut de règle d'autorisation (explicite) le concernant, l'utilisateur est soumis à un **refus implicite**.
- Les autorisations sont **cumulatives**, la résultante des autorisations affectant un utilisateur correspond au cumul des autorisations le concernant.
- En cas de conflit, **le refus l'emporte**.

L'ACCÈS AUX RESSOURCES

L'héritage des autorisations NTFS

- L'héritage s'applique par défaut aux autorisations NTFS positionnées sur des dossiers.

- Il est conseillé d'affecter ces autorisations **en partant de la racine** d'une arborescence afin de bénéficier de l'héritage.

- L'héritage peut être rompu sur un point d'arborescence ou repropagé à partir d'un élément.

- Il y a néanmoins des contraintes :

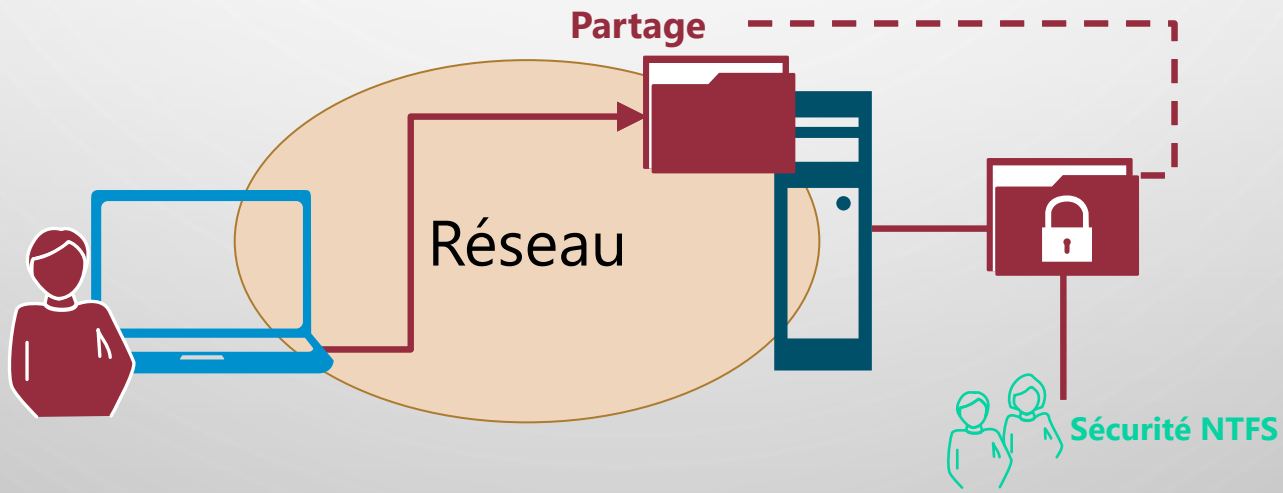
	Au sein d'une même partition	Entre deux partitions ou disques
Déplacement	**Conservation**	Héritage
Copie	Héritage	Héritage

L'ACCÈS AUX RESSOURCES

Le partage de fichiers

- Le partage vient en **complément** des autorisations NTFS.

- Un poste disposant de partages joue le rôle de serveur de fichiers.



L'ACCÈS AUX RESSOURCES

Les autorisations de partage

- Les autorisations permettent de définir :
  - Quels seront les privilèges
  - S'ils autoriseront ou interdiront
  - Pour qui
- Les trois types de privilèges de partage sont les suivants :

Lecture	Modification	Contrôle Total

- Pour chaque niveau, les privilèges correspondants pourront être :

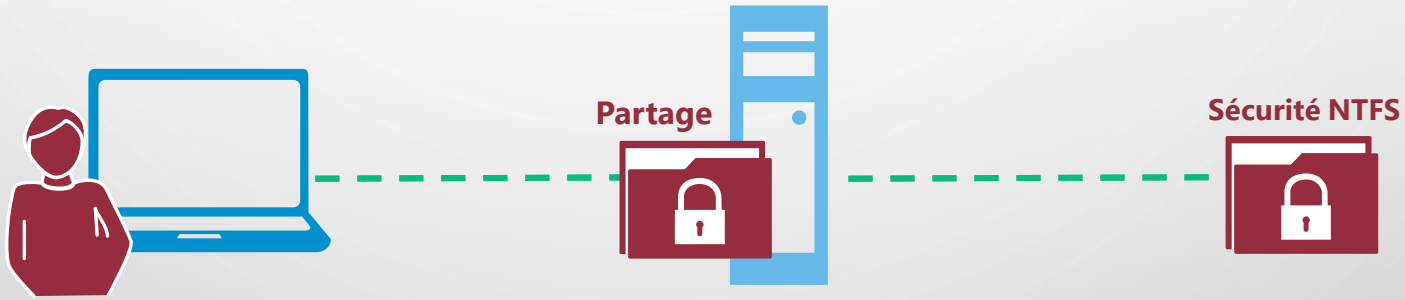
Autorisé	Refusé

- Chaque règle cible une ou plusieurs entités.
- Les règles de contrôles d'accès sont cumulatives et les refus prioritaires.

L'ACCÈS AUX RESSOURCES

Autorisations résultantes

- Quand l'utilisateur accède depuis son poste de travail à une ressource partagée :
  - Il est d'abord soumis aux autorisations du partage
  - Puis aux autorisations NTFS

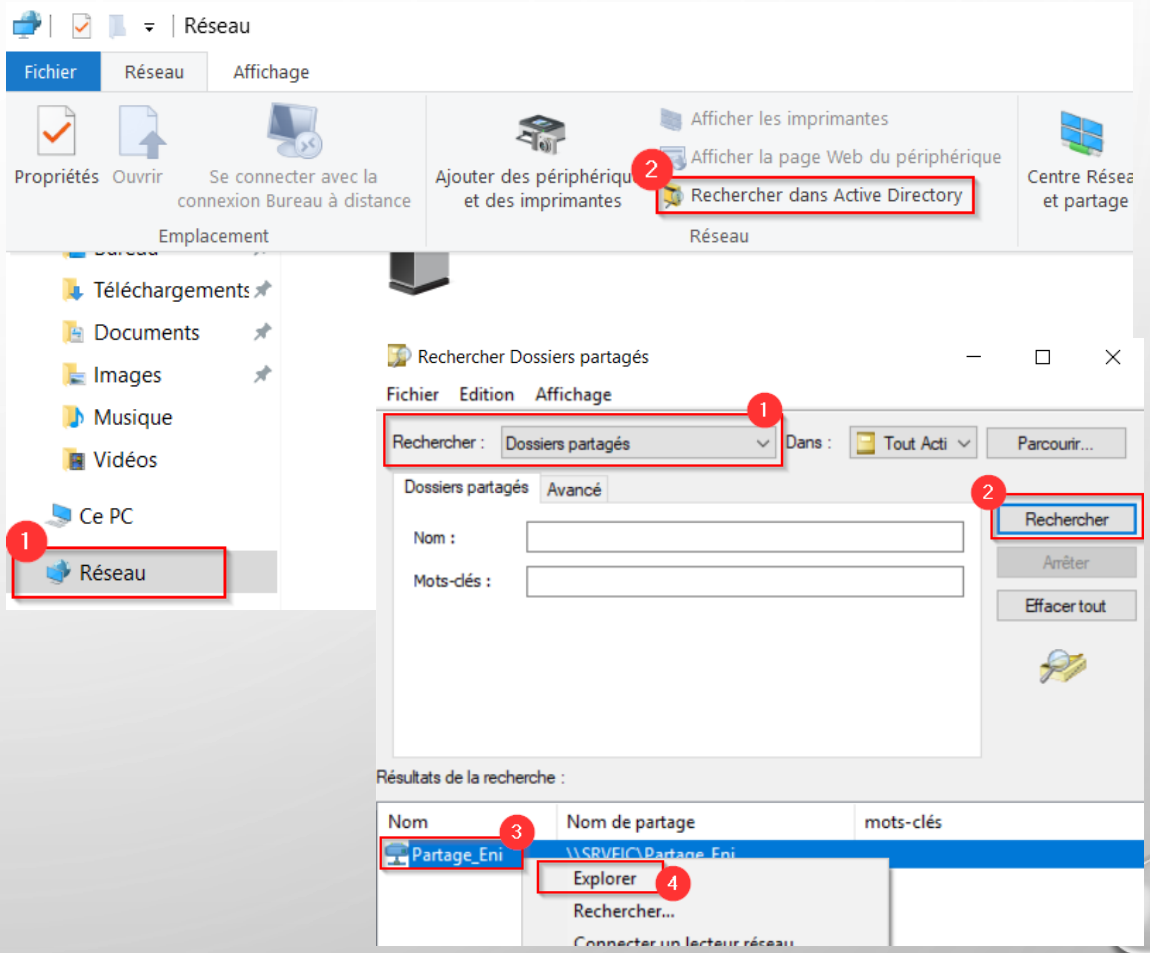


- Les privilèges les plus restrictifs prévalent.

L'ACCÈS AUX RESSOURCES

Les publications de partage

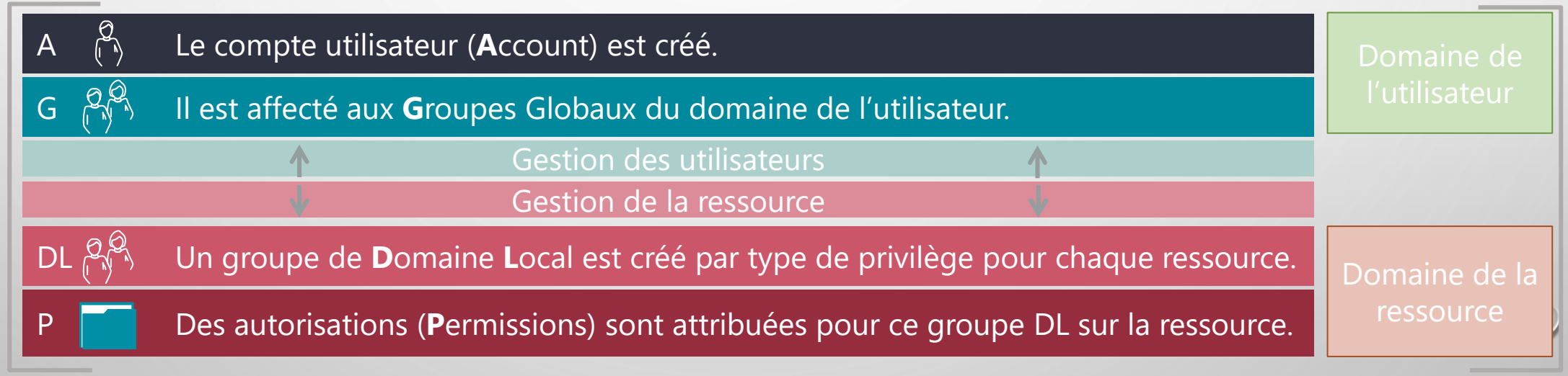
- Une fois créé, il est possible de le **publier** dans l'AD.
- L'objet **Partage** est soit lié à :
  - **L'objet ordinateur** auquel il est associé.
  - **Indépendant** et peut être déplacé dans un UO dédié.
- La publication de partage facilite la recherche pour les utilisateurs depuis leur poste client avec la fonction **Rechercher dans Active Directory**.



L'ACCÈS AUX RESSOURCES

Stratégie d'imbrication des groupes

- Afin de gérer efficacement l'accès aux ressources, Microsoft préconise l'imbrication des Groupes Globaux et de Domaines Locaux.



MODULE 2 – TP5

Objectifs

- Apprendre à créer des partage de fichiers
- Comprendre la gestion des droits

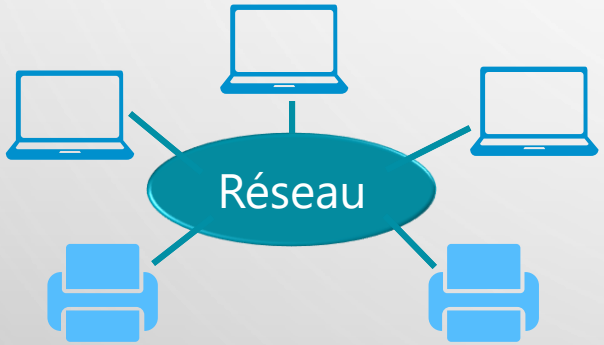
Consignes

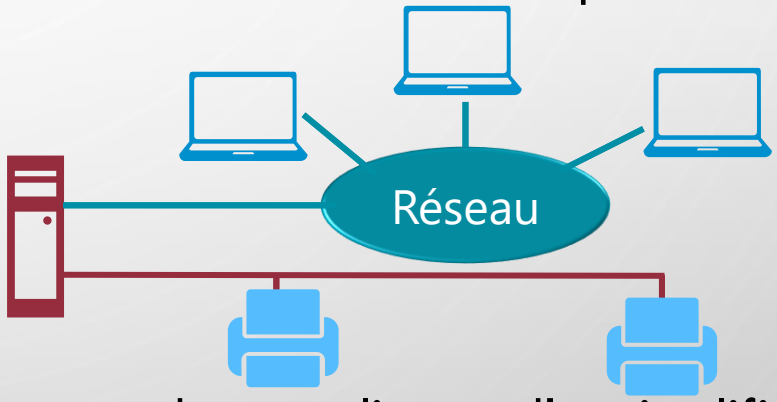
- Créer 3 partages de fichiers et appliquer les droits demandés
- Tester la bonne application des droits

LA GESTION DES IMPRESSIONS

Le service d'impression

- L'ajout du service de rôle **Serveur d'impression** permet de partager des imprimantes et centraliser la gestion de l'impression.
- Les imprimantes sont des ressources généralement raccordées au réseau de l'entreprise.





- Cependant la mise en place d'un serveur d'impression permet de centraliser et d'en simplifier la gestion.

LA GESTION DES IMPRESSIONS

Vocabulaire

Vocabulaire	Définition
Port d'impression	Lien qui permet la communication entre le périphérique d'impression et le serveur (ou à un poste client).
File d'attente	Liste des documents en attente de traitement par l'imprimante.
Imprimante locale	Imprimante dont la file d'attente est configurée sur un serveur ou à un poste client.
Imprimante partagée	Imprimante accessible sur le réseau • Elle peut être du type imprimante réseau • Elle peut être du type imprimante locale mais il faut que le poste ou le serveur qui la partage soit allumé pour qu'elle soit accessible
Imprimante réseau	Imprimante indépendante qui possède sa propre carte réseau, parfois un écran de configuration ou/et un petit serveur web embarqué pour l'administration à distance. Elle peut être configurée en locale ou partagée

LA GESTION DES IMPRESSIONS

Les tâches de gestion et outils

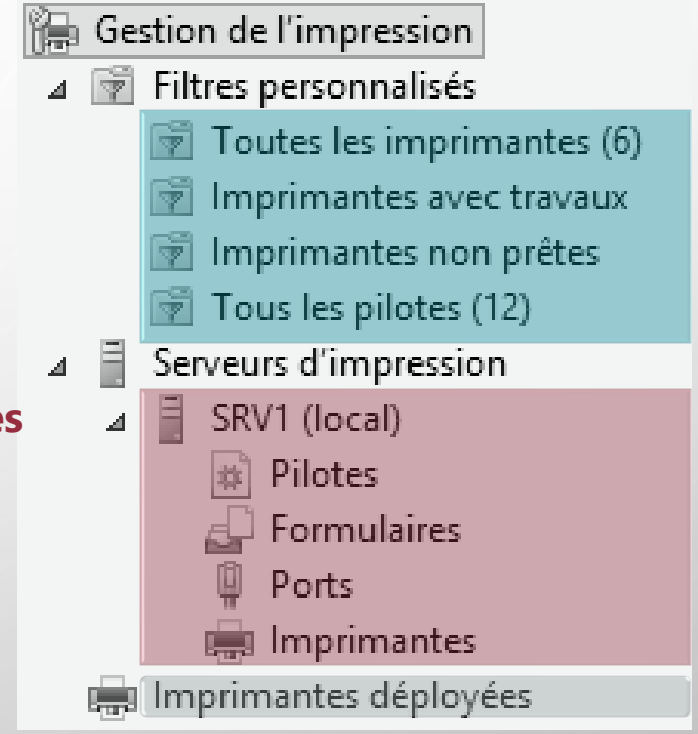
- L'ajout du service de rôle **Serveur d'impression** fournit la console de gestion **Gestionnaire d'impression.**

- Cette console rassemble les composants de gestion nécessaire :

Vue de l'état des imprimantes

Configuration des services d'impression

Gestion du déploiement par stratégies



LA GESTION DES IMPRESSIONS

La gestion des périphériques

- Comme pour les ressources disque, une imprimante doit être partagée pour être accessible via le réseau.
- L'attribution des privilèges se configure depuis les paramètres de sécurité :

Autorisation de base	Autorisation étendue
Imprimer	
Gérer l'imprimante	
Gérer les documents	
	Autorisation de lecture
	Modifier les autorisations

LA GESTION DES IMPRESSIONS

La gestion du déploiement

- Plusieurs méthodes peuvent être utilisées pour installer les imprimantes sur les ordinateurs :
  - Le déploiement manuel
  - L'utilisation de scripts
  - Le déploiement par stratégies de groupe (voir prochain module)

MODULE 2 – TP6

Objectifs

- Manipuler l'interface de création et de partage d'imprimantes
- Comprendre les droits sur le partage d'imprimante

Consignes

- Créer les imprimantes correspondant au besoin
- Les partager et positionner les droits d'accès

MODULE 2 – A RETENIR

- **Active Directory** est un **annuaire** regroupant des identités (utilisateur et ordinateurs) stockées dans une arborescence **d'unités d'organisation**
- Il permet de contrôler la sécurité d'accès aux ressources (partage de fichiers, partage d'imprimantes ou autres applications) via la logique **AGDLP**
- Active Direcory s'appuie sur des serveurs ayant le rôle de **Contrôleur de Domaine** pour fonctionner
- Les permissions NTFS définissent **qui** peut faire **quoi** sur un dossier (et éventuellement ce qu'il contient) ou un fichier