

---

# Cours - Active Directory - Focus sur les différents types de groupes

*BTS SIO - B1/U4 Support et mise à disposition des services informatiques*

*1.2 Répondre aux incidents et aux demandes d'assistance et d'évolution*

<b>1. Les groupes</b>	<b>3</b>
1.1. Introduction	3
<b>1.2. L'étendue du groupe</b>	<b>4</b>
<b>1.3. Le type du groupe</b>	<b>5</b>
<b>1.4. Les groupes par défaut</b>	<b>6</b>

# 1. Les groupes

## 1.1. Introduction

**Jusqu'ici, nous avons évoqué vaguement la notion de groupe, il va être temps de s'y mettre ! Comme je le disais précédemment, un groupe permet de regrouper plusieurs objets au sein d'un même objet.**

Pour vous convaincre de l'importance et de l'intérêt qu'il y a à utiliser les groupes, voici un exemple tout simple.

Je dispose d'un dossier partagé, accessible via le réseau aux utilisateurs du domaine. Ce dossier se nomme « *Comptabilité* » et je souhaite que toutes les personnes du service comptabilité de mon entreprise accèdent à ce dossier.

Plutôt que de donner les droits à chaque utilisateur du service comptabilité, tour à tour, on va créer un groupe. De ce fait, je vais créer un groupe nommé « comptabilité » dont les membres sont l'ensemble des utilisateurs correspondant aux collaborateurs du service comptabilité.

Il suffira ensuite d'ajouter sur le dossier partagé les autorisations pour le groupe « comptabilité », ce qui impliquera que les membres de ce groupe disposeront eux aussi des droits (comme ils font partie du groupe).

Non seulement ça permet de simplifier la liste des autorisations sur le répertoire (il y a moins d'éléments listés que si chaque utilisateur était ajouté de façon indépendante), mais aussi ça simplifie l'administration, car si un utilisateur change de service, il suffit de le changer de groupe. Il ne sera pas nécessaire de changer les autorisations de cet utilisateur sur des dossiers partagés tel que celui de la « comptabilité ».

Maintenant, il faut savoir qu'il existe différentes étendues pour les groupes et différents types de groupe, c'est ce que nous allons voir en détail maintenant.



## 1.2. L'étendue du groupe

L'étendue d'un groupe correspond à sa portée au niveau de l'arborescence Active Directory, les étendues peuvent aller d'une portée uniquement sur le domaine local, mais aussi s'étendre sur la forêt entière.

Il existe trois étendues différentes :

- **Domaine local**

Un groupe qui dispose d'une étendue « domaine local » peut être utilisé uniquement dans le domaine dans lequel il est créé. Avec ce type d'étendue, le groupe reste local au domaine où il est créé.

Cependant, les membres d'un groupe à étendue locale peuvent être bien sûr des utilisateurs, mais aussi d'[autres](#) groupes à étendues locales, globales ou universelles. Cette possibilité offre là encore une flexibilité dans l'administration.

Il peut être défini pour contrôler l'accès aux ressources uniquement au niveau du domaine local.

- **Globale**

Un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base. Ainsi, si un « domaine A » approuve via une relation un « domaine B », alors un groupe global créé dans le « domaine A » pourra être utilisé dans le « domaine B ».

Un groupe global pourra contenir d'[autres](#) objets du domaine, et être utilisé pour contrôler l'accès aux ressources sur le domaine local et tous les domaines approuvés.

- **Universelle**

Un groupe disposant de l'étendue « universelle » à une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

Un groupe universel peut contenir des groupes et objets provenant de n'importe quel domaine de la forêt. De la même manière, il est possible de l'utiliser pour définir l'accès aux ressources sur tous les domaines de la forêt.

Ainsi, avec ce type d'étendue on pourra consolider plusieurs groupes qui doivent avoir une portée maximale sur l'ensemble du [système](#).

Une particularité de ce type de groupe, c'est qu'il est défini au sein d'un catalogue global.

### Précisions sur les étendues

Les étendues sont dépendantes du niveau fonctionnel de la forêt et du domaine, ainsi que de la complexité de l'architecture en place, notamment au niveau des relations d'approbations entre les différents domaines et arbres. Si vous créez un groupe à étendue universelle, mais qu'il n'y a pas de relation avec un autre domaine ou une autre forêt, cela n'aura pas d'intérêt.

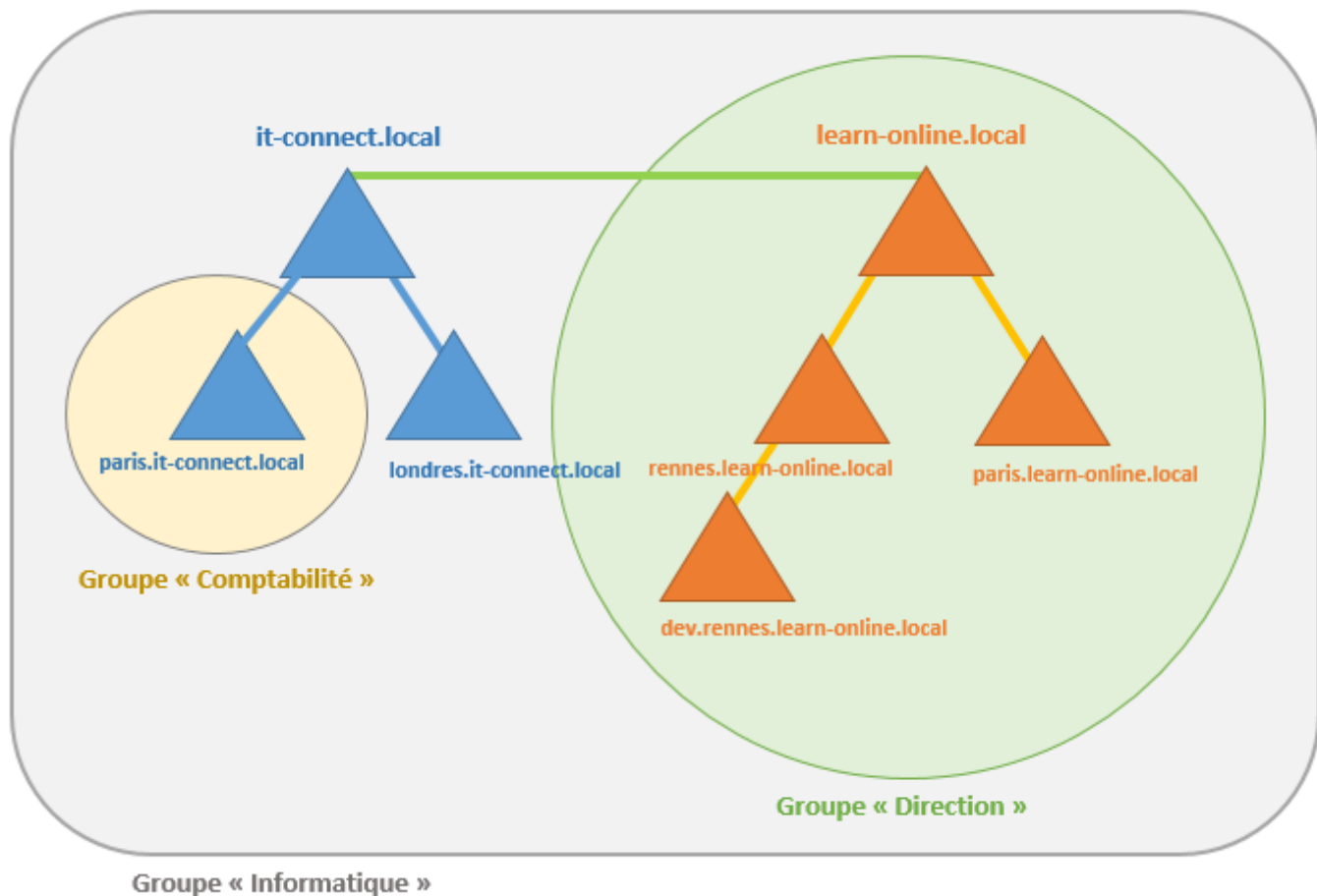
### Exemple

Reprenons l'arborescence que nous avons définie dans le module « Domaine, forêt et arbre », avec les deux domaines « it-connect.local » et « learn-online.local » contenant tous les deux des sous-domaines.

Imaginons trois groupes et leurs étendues cohérentes :

- *Comptabilité* : étendue « domaine local » sur « paris.it-connect.local »
- *Direction* : étendue « globale » sur « learn-online.local » qui approuve tous les sous-domaines
- *Informatique* : étendue « universelle » sur la forêt

Ainsi, la portée de ces groupes pourra être schématisée comme ceci au sein de la forêt :



### 1.3. Le type du groupe

Maintenant que vous êtes opérationnel sur la compréhension des étendues, nous allons voir le deuxième paramètre proposé lors de la création d'un groupe : le type.

Il existe deux types :

- **Sécurité**

Les groupes de sécurité sont les plus utilisés et ceux que vous manipulerez le plus souvent. Ils permettent d'utiliser les groupes pour gérer les autorisations d'accès aux ressources.

Par exemple, si vous avez un partage sur lequel vous souhaitez donner des autorisations d'accès, vous pourrez utiliser un « *groupe de sécurité* » pour donner des autorisations à tous les membres de ce groupe.

En résumé, ces groupes sont utilisés pour le contrôle d'accès, ce qui implique que chaque groupe de ce type dispose d'un identifiant de sécurité « SID ».

- **Distribution**

L'objectif de ce type de groupe n'est pas de faire du contrôle d'accès, mais plutôt des listes de distribution. Par exemple, créer une liste de distribution d'adresses e-mail en ajoutant des contacts.

De ce fait, ces groupes sont utilisés principalement par des applications de messagerie, comme Microsoft Exchange.

Comme il n'y a pas de notion de sécurité, ce type de groupe ne dispose pas d'identifiant de sécurité « SID ».

## Conclusion

Finalement, vous ne devez pas être étonné des définitions données ci-dessus quant aux deux types de groupe disponibles, car les noms sont assez explicites.



Il est à noter qu'il est possible de convertir à tout moment un groupe de sécurité en groupe de distribution, et vice-versa. Cependant, le niveau fonctionnel du domaine doit être au minimum « *Windows Server 2000 natif* » mais de nos jours, il est quasiment « impossible » de ne pas l'être.

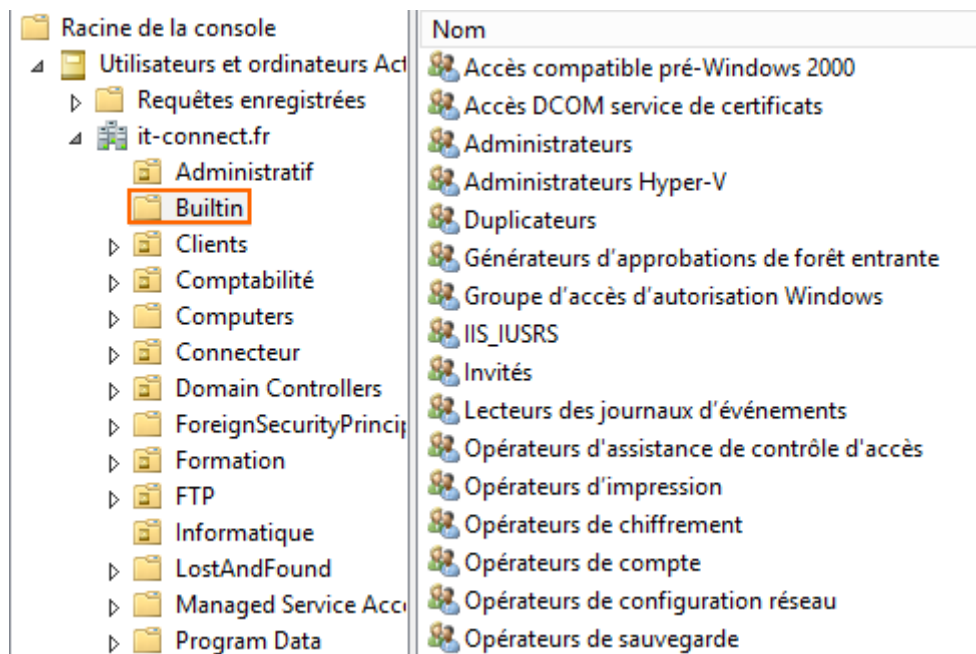
## 1.4. Les groupes par défaut

Lors de la création d'un domaine et de la création de l'annuaire Active Directory, différents groupes sont déjà présents, mais alors, à quoi servent-ils ? Intéressons-nous aux groupes intégrés, spéciaux et prédéfinis.

- **Les groupes intégrés (« Built-in »)**

Ce sont des groupes qui permettent d'assigner des autorisations d'administration, de façon générale ou sur des fonctionnalités précises afin de gérer la sécurité finement. Ces groupes sont directement intégrés et stockés dans l'annuaire Active Directory au sein du container « *Builtin* » accessible de la console « *Utilisateurs et ordinateurs Active Directory* ». Leur étendue est toujours de type local.

Par exemple, le groupe « *Administrateurs* [Hyper-V](#) » donnera un accès complet et illimité à toutes les fonctionnalités liées à Hyper-V. Autre exemple, le groupe « *Opérateurs de* [sauvegarde](#) » permet d'accéder aux fonctionnalités de sauvegarde et de restauration des fichiers.



### • Les groupes spéciaux :

Seul le système à la main sur ces groupes, qui sont pratiques et qui permettent d'englober les utilisateurs à différentes échelles. On trouve les groupes :

- Ouverture de session anonyme : utilisé pour les connexions à une ressource sans avoir fourni un nom d'utilisateur et un mot de passe.
- Tout le monde : ce groupe contient l'ensemble des groupes utilisateurs authentifiés et invité
- Utilisateurs authentifiés : contrairement aux utilisateurs anonymes, les membres de ce groupe sont les objets authentifiés par un contrôleur de domaine. Le compte invité n'est pas membre de ce groupe même s'il dispose d'un mot de passe.
- Interactif : lorsqu'un utilisateur accède à une ressource sur un ordinateur sur lequel il a ouvert une session localement, il est ajouté à ce groupe. Ce dernier contient également les utilisateurs qui ont ouvert une session via le bureau à distance.
- Réseau : contrairement au groupe précédent, celui-ci concerne les utilisateurs qui accèdent à une ressource sur le réseau.

Ces groupes peuvent être utilisés pour définir du contrôle d'accès (exemple : donner accès aux utilisateurs authentifiés l'accès à un partage).

Par ailleurs, il n'est pas possible de gérer les membres de ces groupes, le système gère ces groupes en exclusivité.

### • Les groupes prédéfinis

On les trouve dans l'unité d'organisation « Users » au sein de la console « Utilisateurs et ordinateurs Active Directory ». Ces groupes prédéfinis sont là en complément des groupes intégrés, sauf que pour eux il y a différents niveaux d'étendues qui sont prédéfinies et qu'on ne peut pas modifier.