NOMS et PRENOMS :

- ✓ OUSMANE ALASSANE SOULTANA
- ✓ KAMGUIA KOUAM ERIC STEPHANE

Thème : Microsoft Active Directory pour le contrôle d'accès et de flux

Résumé

Le présent rapport expose notre projet trimestriel dans le cadre du programme de la Maitrise en sciences et technologies de l'information au sein de l'Université du Québec en Outaouais. Ce projet intitulé « Microsoft Active Directory pour le contrôle d'accès et de flux » vise à expliquer et à mettre en œuvre l'utilisation de Microsoft Active Directory (AD) au sein d'un environnement informatique. L'objectif principal est de renforcer l'efficacité de la gestion des accès et du workflow des ressources (matériels, logiciels et humains) au sein d'une organisation.

I. Introduction

Microsoft Active Directory (AD) est une pierre angulaire du contrôle d'accès et de flux de données au sein des organisations. Les services de domaine active directory (ou AD DS pour Active Directory Domain Services) constituent le noyau de l'Active Directory concernant la gestion des autorisations et des fluctuations des entités (usagers ou utilisateurs, sujets, objets, ressources). Ils offrent une gestion centralisée des ressources et des identités dans les réseaux. Ce système d'Active Directory Domain Services s'appuie sur quelques modèles de contrôle d'accès et de flux. Parmi ces modèles, nous avons : le modèle de contrôle d'accès basé sur des rôles (ou **RBAC** pour Rôle Based Access Control) principalement, le modèle de contrôle d'accès discrétionnaire (ou **DAC** pour Discretionary access control), le modèle de contrôle d'accès obligatoire (ou **MAC** pour Mandatory Access Control). Ces modèles conceptuels permettent aux services de domaine Active Directory de contrôler les entités (usagers ou utilisateurs, sujets, objets, ressources) et garantir la sécurité de manière concrète. Dans ce qui suit, nous présenterons dans un premier temps, les modèles de contrôles de flux et dans un second temps, nous passerons a une revue des modèles de contrôles d'accès des services de domaine Active Directory, en se basant sur les principales notions abordées en classe.

II. Problématique

Plusieurs problématiques posent des défis aux administrateurs informatiques dans les domaines de l'accès et du contrôle de flux. Parmi ces problématiques, nous pouvons citer entre autres :

- ➢ **Sécurité des ressources :** La sécurité des ressources est un défi constant, car les menaces évoluent rapidement. Les administrateurs doivent mettre en œuvre des

mécanismes de sécurité tels que, les solutions de droits d'accès, les politiques de sécurité, etc., pour protéger les données, les systèmes et les réseaux contre les vulnérabilités et les attaques, mais aussi à l'accès effective à qui de droits à une information.

- **Hiérarchisation :** La hiérarchisation des ressources informatiques est essentielle pour garantir que les ressources critiques soient accessibles en priorité, en particulier à qui de droits à une information dans les environnements où les ressources sont limitées. Les administrateurs doivent déterminer quelles ressources sont essentielles pour les opérations de l'entreprise et attribuer des priorités en fonction de la disponibilité, de la performance et du niveau dans la hiérarchie du sujet au sein de l'organisation.

- **Mouvement des ressources (flux) :** La gestion efficace du mouvement des ressources, y compris le transfert de données et d'applications entre différents composants du système, est cruciale pour maintenir un environnement informatique fluide et efficace, tout cela en restant optimale.

III. Contrôle d'accès et de flux dans Active Directory de Microsoft

Les solutions proposées pour résoudre nos problématiques est **l'Active Directory de Microsoft**. Ce dernier possède un ensemble de sous outils, à travers lequel il effectue le contrôle d'accès et le contrôle de flux.

III.1 Contrôle de flux

Le contrôle de flux est une pratique technique dont la connaissance permanente à ses questionnements est primordiale dans la gestion du canal ; De qui fais quoi ? A quel moment ? Et qui vois quoi ? A partir de cette définition on peut dire sans ambiguïté que la maitrise d'un contrôle de flux passe obligatoirement par un contrôle d'accès. Pour effectuer un contrôle de flux Active Directory, il est nécessaire de connaitre les éléments présents dans le flux, à savoir : les sujets (usagers, sessions), les objets (fichiers, imprimantes…etc.), le canal (liaison physique, liaison logique). Le contrôleur de domaine qui est une machine physique à partir duquel est déployé Active Directory, est le coffret qui renferme les clés du monde Active Directory, car il joue les rôles de central annuaire, centrale d'authentification et bien d'autre encore.

S'agissant du contrôle de flux dans AD on peut avoir plusieurs mécanismes. Tout d'abord, commençons par la topologie choisit pour notre implémentation:

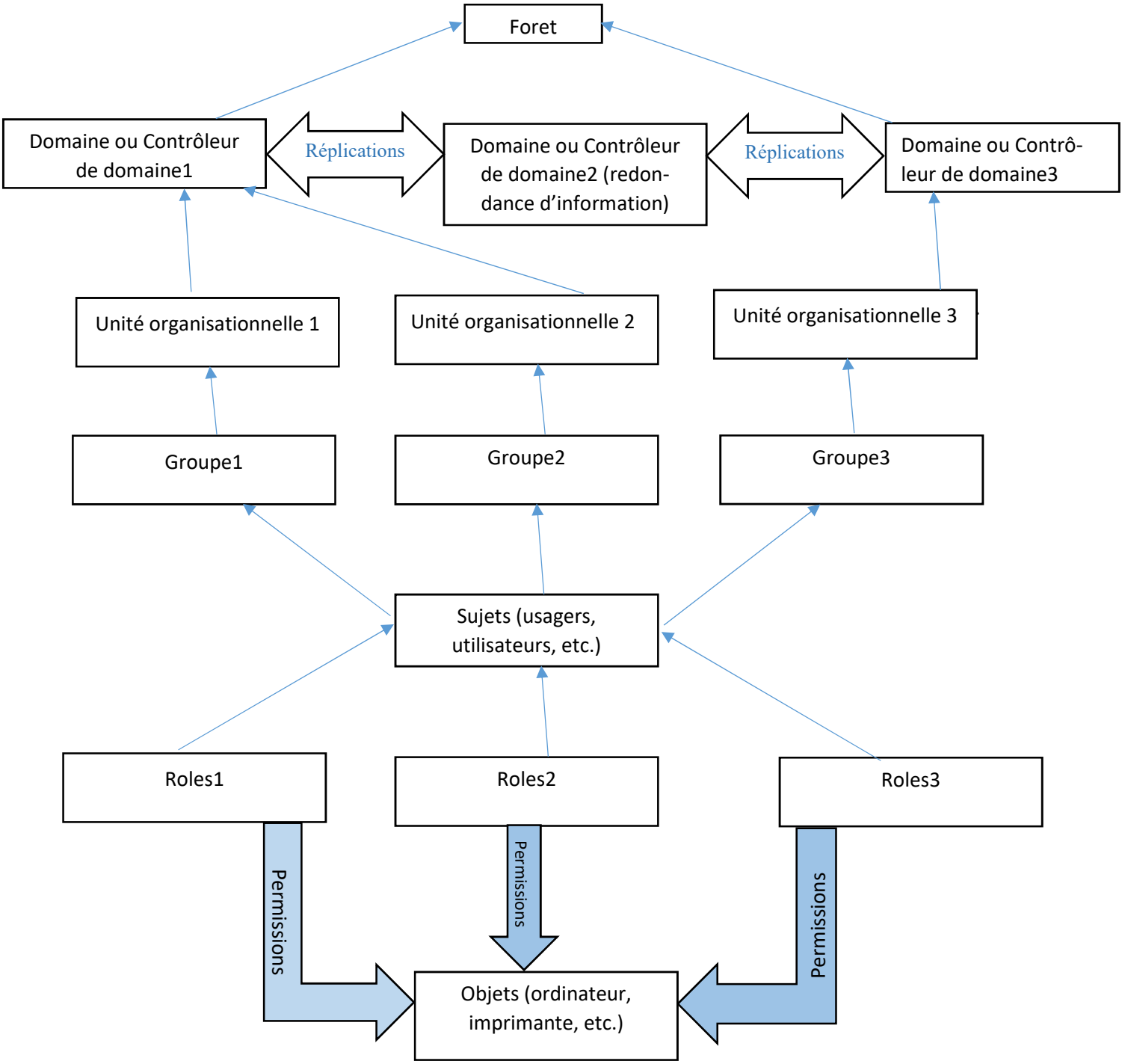

Figure 1 : Architecture d'implémentation (Source : réalisé par nous)

Pour la gestion du flux, la topologie a adopté dans une organisation est un élément très essentiel dans le contrôle de flux car il définit la méthode de circulation des données. Dans active directory le choix de topologie est d'autant plus important qu'il montre le schéma communicationnel, la redondance des données soit dans le sens de gestion des défaillances ou l'accès permanent et optimal aux ressources désirées. On peut faire un choix de topologie parmi celles qu'on va proposer ci-dessous, et cela en fonction de l'organisation. Aussi, on peut

mutualiser des topologies pour avoir celle qui s'adapte la plus à notre besoin. Les topologies possibles sont :

- **Modèle de Domaine Unique :** Dans cette topologie nous avons un seul domaine que partagent les objets et les sujets. Cette topologie est axée pour les petites entreprises et en plus elle à une flexibilité et scalabilité très limitées dans le temps. Donc, elle est limitée aussi par le flux de données qu'elle peut gérer. Elle est inadéquate pour une entreprise qui veut vivre au minimum 99ans.

- **Forêt Unique, Multiples Domaines :** Comme le nom l'indique, dans cette topologie, on a une seule forêt et plusieurs domaines, mais nom hiérarchisé. Elle fournit une autonomie très accrue aux départements et garde tout de même une gestion centralisée. Ce qui rend l'attribution des permissions assez difficile et complexe et même impossible d'attribuer des permissions transitives.

- **Multiples Forêts :** Il y'a plusieurs forêts active directory qui partagent entre elles ou pas, des relations de confiance. Pour une organisation active directory elle sera lourde et peut flexible, mais offre une sécurité accrue et une très bonne autonomie.

- **Modèle d'Arborescence :** Ce modèle de topologie est très hiérarchisé et facilement administrable. Très équilibré entre la structure organisationnelle et flexibilité.

- **Modèle Hub and Spoke :** Elle a un domaine centrale appelé **Hub** et des domaines gravitationnelles appelés **Spoke**. Tout le réseau Active directory est centralisé au domaine central Hub, ce qui crée une dépendance du réseau au Hub.

- **Modèle de Forêt de Ressources :** Cette topologie réserve une forêt aux objets et une autre forêt aux sujets. On peut remarquer avec cette topologie une frontière bien marquée entre les objets et les sujets. Mais elle n'est pas appropriée pour un contrôle de flux optimal, pour une organisation aux regards de l'énorme charge dans la gestion de ce type de topologie.

- **Modèle Géographique :** Ici les domaines sont organisés en fonction de l'emplacement géographique. Elle est bonne pour les structures avec succursale (ou bureau) situées dans plusieurs territoires différents. Sauf que dans cette topologie, le trafic de réplication est énorme et pourrait y avoir du temps de latence.

Dans notre projet nous avons utilisés une mutualisation entre le model arborescent et géographique pour avoir de la flexibilité et de la hiérarchisation ainsi présenté dans notre schéma1.

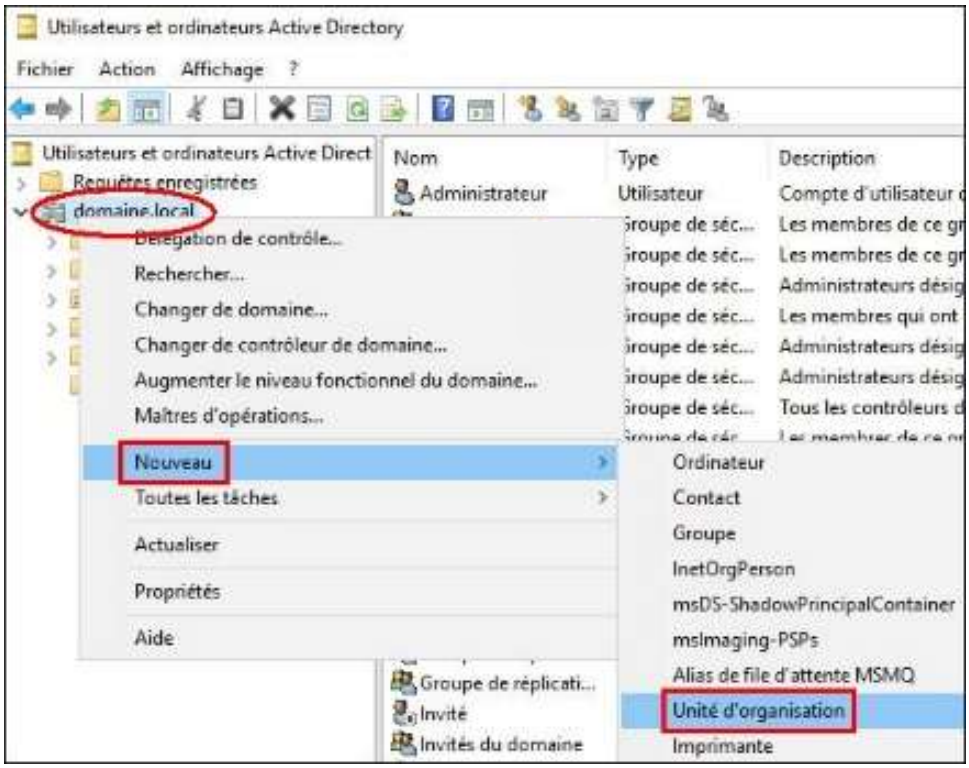

Figure 2 : Création de domaine, unité organisationnelle

Comme autre mécanisme de gestion de flux dans un environnement Active directory, on peut parler de la réplication. La réplication est un mécanisme au cours duquel il y'a redondance des données dans un environnement organisationnel Active directory. Cela, à travers ses deux mécanismes principaux à savoir : La réplication inter site et intra-site. Comment est-ce que cela fonctionne et impacte le contrôle de flux dans active directory ? Pour que la réplication soit optimale et en adéquation avec le choix de notre topologie, nous avons supprimé une réplication des données inter domaines et l'avons centralisé pour diminuer le flux de données répliqué. S'agissant de la scalabilité de notre environnement nous avons prévu deux à trois domaines de backup pour assurer la disponibilité permanente de tout notre réseau.

La réplication inter et intra-site créent un système de redondance des données d'un contrôleur de domaine à l'autre. C'est-à-dire, les données administrées présentent ou mises à jour dans un contrôleur de domaine, sont répercuter dans tous les autres contrôleurs de domaine présentent dans le réseau. Ceci permet de garder la cohérence des données administrées au sein de la structure Active Directory tout en distribuant la charge de travail dans tous les contrôleurs. La cohérence, la distribution de charge rendent la disponibilité des données permanente et à partir de tous les contrôleurs de domaine. Le contrôle de flux est plus spécifiquement marqué ici par la distribution de la charge de travail.
Exemple : Tout cet exemple n'est valable que si le rôle, l'attribut ou même contrôle d'accès que l'utilisateur possède dans cette organisation lui permet d'avoir la permission d'accéder à ce service. Dans le cas contraire, tout ce qui n'est pas permit est interdit.
Supposons un utilisateur du **groupe1** de **role2** appartenant à l'**unité organisationnelle1** veut une information présente dans le **contrôleur de domaine3**. Sans réplication, il y'aurait au minimum 8 flux de messages (en aller et retour) du **groupe1** au **domaine3**. Tandis qu'avec une réplication il y'aurait au maximum 4 flux de messages.

A côté de la topologie et de la réplication, on a aussi le Groupe Policy Object (GPO) qui permet le contrôle de flux à travers les stratégies telles que les <groupes retreints> dans lesquels on peut implémenter des règles sur des groupes avec des attributs, par importance pour cette journée. Exemple : Nous sommes dans une structure qui a besoin de se connecter sur internet pour faire les payements de factures, supposons à un moment lambda de la journée, le débit est mauvais et le réseau est très lent. L'administrateur à ce moment dans le groupe restreint crée une règle ne permettant plus aux clients de se connecter à internet. De plus on peut configurer des règles de trafic entrantes et sortantes, l'administrateur, peut selon le besoin, décider de rendre indisponible un certain service tel que l'accès au bureau à distance et au téléchargement, etc. Avec la GPO, le contrôle de flux est très précis et flexible comme nous le montre ce schéma qui identifie un lieu précis pour appliquer une règle.

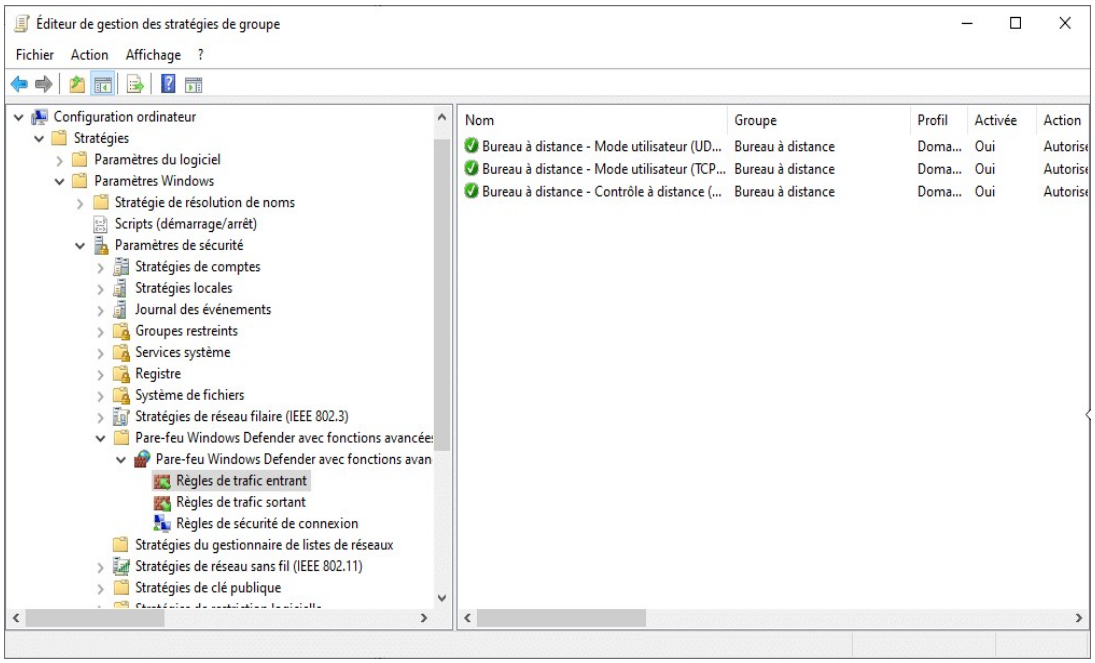

Figure 3 : Configuration des GPO (Source : réalisé par nous)

Les stratégies de groupes (ou GPO pour Group Policy Object) sont un ensemble d'outils intégrés à Windows Server qui permet au service informatique de centraliser la gestion de l'environnement utilisateur et la configuration des machines grâce à l'application de politiques. Il est un élément clé dans la politique de gestion du flux dans un environnement Active Directory. A travers la GPO, on peut définir des politiques sur les utilisateurs leurs permettant d'ouvrir plusieurs sessions qui ont des permissions différentes pour ne pas créer d'autre utilisateurs avec les même permissions, qui par la suite, viendrons augmenter la charge de circulation des données. Avec la GPO, on peut aussi définir des paramètres de configuration automatique sur des utilisateurs et objets qui changent de rôles, groupe ou permissions. Ainsi, pour gérer la fluctuation permanente dans une organisation des entités, la GPO peut aussi implémenter des méthodes de fonctionnement semblable a RBAC a l'instar de la DSD et SSD (Dynamic Separation of Duties et Static Saperation of Duties). A côté de la GPO, nous avons aussi les outils ADUC (Active Directory Users and Computers) ou ADAC (Active Directory Administrative Center) qui sont des approches graphiques qui permettent aux administrateurs

réseaux d'effectuer des mouvements d'entités (utilisateurs, ordinateurs, objet, etc.) lorsque celle-ci changent de rôles ou de niveau hiérarchique pour les sujets et lorsqu'elles changent de niveau d'accès pour les objets.

III.2 Contrôle d'accès

III.2.1 Modèles de contrôle d'accès utilisés par Active Directory

Comme nous l'avons mentionné dans l'introduction, les services de domaine Active Directory (ou **AD DS**) qui est le noyau de Microsoft Active Directory, s'appuie sur des modèles pour contrôler l'accès aux ressources, au sein d'une organisation. Parmi ces modèles figure le modèle de contrôle d'accès basé sur des rôles (ou **RBAC** pour Role Based Access Control). Tout d'abord, le modèle RBAC est un concept de sécurité selon lequel un système accorde des autorisations aux usagers (utilisateurs) en fonction de leur rôle dans une organisation, simplifiant ainsi la gestion des autorisations et renforçant la sécurité. Le modèle RBAC est la méthode de contrôle d'accès la plus utilisée. Nous allons voir, par la suite, les étapes nécessaires de la conception et de l'implémentation du modèle RBAC dans Active Directory.

Pour implémenter le modèle **RBAC** dans **Microsoft Active Directory**, la première étape consiste à définir les rôles et les permissions qu'on souhaite attribuer aux utilisateurs, dans une organisation. Un rôle, comme nous l'avons vu en classe, c'est un type de poste dans une organisation (par exemple, à l'UQO[1], on pourrait avoir les rôles suivants : étudiant, professeur, administrateur, etc.). Tandis qu'une permission, c'est une autorisation ou un droit qui permet à un utilisateur d'effectuer une action ou d'accéder à une ressource. Par exemple, à l'UQO, un utilisateur ayant le rôle ''Professeur'' pourrait avoir les permissions suivantes : déposer les notes de cours dans Moodle, déposer les devoirs dans Moodle, etc. Les permissions d'un utilisateur sur les ressources d'une organisation doit dépendre du rôle de l'utilisateur dans l'organisation. Pour créer et gérer des rôles et des permissions, on peut utiliser l'outil Utilisateurs et ordinateurs Active Directory (ou ADUC pour Active Directory Users and Computers) ou le Centre d'administration Active Directory (ou ADAC pour Active Directory Administrative Center).

La deuxième étape de l'implémentation du modèle RBAC dans Microsoft Active Directory consiste à créer des groupes et à leur attribuer des rôles. Un groupe est un ensemble d'utilisateurs qui partagent le même rôle ou ont les mêmes besoins d'accès. Par exemple, on peut créer un groupe pour les étudiants de l'UQO et attribuer à ce groupe le rôle ''étudiant'' qui devait être défini à l'étape précédente. Dans Active Directory on a plusieurs niveaux de subdivision des entités en fonction de leurs rôles, pour définir leurs permissions collectives, à l'instar d'un ou des unités organisationnelle (organizational unit) qui sont des subdivisions logiques utilisées pour organiser les objets active directory (Utilisateur, groupe, etc.), un ou des domaines et une forêt dont les utilisateurs appartenant à ses différents niveaux hiérarchiques ont le même niveau d'étiquetages. En effet, l'utilisation des groupes permet de simplifier l'administration des droits d'accès, car on aura juste besoin d'attribuer des rôles à

UQO[1] : Université du Québec en Outaouais.

des groupes plutôt qu'à des utilisateurs individuellement. Les outils ADUC et ADAC peuvent être utilisé pour créer et gérer des groupes et leur attribuer des rôles.

La troisième étape de l'implémentation du modèle RBAC dans Microsoft Active Directory consiste à configurer des stratégies de contrôle d'accès qui appliquent les rôles et les permissions qui ont été définis dans les étapes précédentes. Une stratégie de contrôle d'accès est une règle qui détermine qui peut accéder à quelles ressources et dans quelles conditions. Par exemple, on peut créer une stratégie de contrôle d'accès qui autorise uniquement les étudiants de l'UQO à déposer leurs devoirs dans Moodle, et uniquement avant la date limite de la soumission. Pour créer et gérer des stratégies de contrôle d'accès, on peut utiliser l'outil éditeur de sécurité Active Directory (ou ADSE pour Active Directory Security Editor) ou l'outil ADAC.

La quatrième étape de l'implémentation du modèle RBAC dans Microsoft Active Directory consiste à tester et à surveiller le modèle RBAC qui a été créé dans les étapes précédentes. Les tests et la surveillance sont essentiels pour s'assurer que le modèle RBAC fonctionne comme prévu, qu'il répond aux différentes exigences de sécurité et de conformité de l'organisation et qu'il ne cause aucun problème de performances ou de fonctionnalités. On peut utiliser l'outil Active Directory Rights Management Services (ADRMS) ou bien l'outil Active Directory Audit Policy (ADAP), pour tester et surveiller le modèle RBAC.

La cinquième étape de l'implémentation du modèle RBAC dans Microsoft Active Directory consiste à examiner et à mettre à jour le modèle RBAC de façon périodique. L'examen et la mise à jour sont nécessaires pour maintenir le modèle RBAC aligné sur les besoins et les objectifs changeants d'une organisation.

En effet, mis à part le modèle RBAC, le domaine de service Active Directory s'appuie également sur le modèle de contrôle d'accès discrétionnaire (ou **DAC** pour Discretionary Access Control). Le modèle DAC permet aux propriétaires de ressources (fichiers par exemple) de décider qui et qui peuvent accéder à leurs ressources et quel type d'accès est accordé. Dans Active Directory, les autorisations DAC sont souvent définies par les administrateurs pour les fichiers, les dossiers et d'autres ressources partagées. Le modèle DAC voit son empreinte dans AD par le fait que chaque machine possède une ACL qui répertorie les entrés qui définissent les autorisations des utilisateurs et des groupes cités plus haut.

Par la centralisation de la gestion des ressources et entités dans un ou des contrôleurs de domaines tel que, les noms d'utilisateurs, mots de passe d'utilisateurs dans le contrôleur de domaine, on constate qu'Active Directory utilise également le modèle de contrôle d'accès identique à celui du modèle de contrôle d'accès obligatoire (MAC).

III.2.2 Conception et implémentation pratique de RBAC dans Active Directory

Nous allons voir dans cette partie, la conception et l'implémentation **pratique** du modèle RBAC dans Microsoft Active Directory. Autrement dit, nous allons voir comment se présentent de **manière pratique**, les étapes d'implémentation de RBAC dans Active Directory vues précédemment.

Tout d'abord, comme mentionné précédemment, au sein d'une organisation, l'administrateur doit définir les rôles et les permissions qui doivent être attribués aux usagers (utilisateurs). Il est très important à savoir que les permissions d'un utilisateur sur les ressources d'une organisation doivent dépendre du rôle de l'utilisateur dans l'organisation. Les rôles quant à eux, peuvent être définis soit pendant la création des groupes (que nous verrons plus tard), soit pendant la création des domaines, soit pendant la création des unités organisationnelles, dépendamment de la structure organisationnelle de l'entreprise.

Après la définition des rôles et permissions, l'administrateur va créer des groupes auxquels il va attribués les rôles définis. La création de groupe peut être faite de deux (2) manières : soit à partir de l'interface graphique ou bien avec PowerShell.

- Création de groupe Active Directory à partir de l'interface graphique

Pour créer un groupe dans l'environnement Active Directory, on doit exécuter le «Gestionnaire de serveur». Ensuite, on ouvre «Outils» et on sélectionne «Utilisateurs et ordinateurs Active Directory», puis on clique avec le bouton droit sur «Utilisateurs» dans l'arborescence de gauche et on sélectionne «Nouveau» - «Groupe ». *(Voir l'image ci-dessous).*

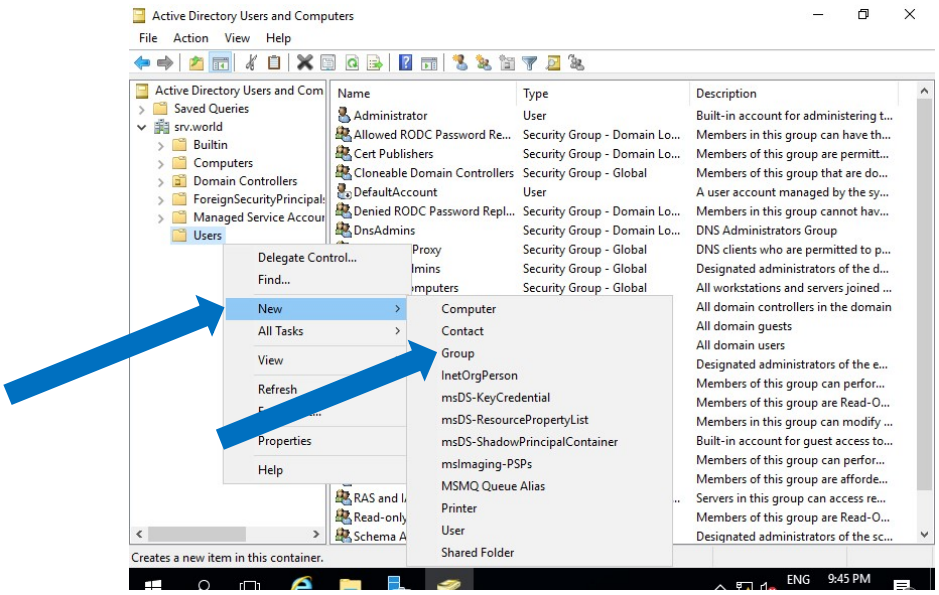

Figure 4 : Processus de création de groupe à partir de l'interface graphique (source : réalisé par nous)

Après avoir effectué les étapes précédentes, on doit choisir le nom du groupe qu'on souhaite ajouter. L'image ci-dessous présente un groupe nommé *''EtudiantUqo''* qui est en train d'être ajouté ou créé. Tous les utilisateurs contenus dans le groupe *''EtudiantUqo''* auront donc le rôle *''EtudiantUqo''* avec les permissions spécifiques à ce rôle.

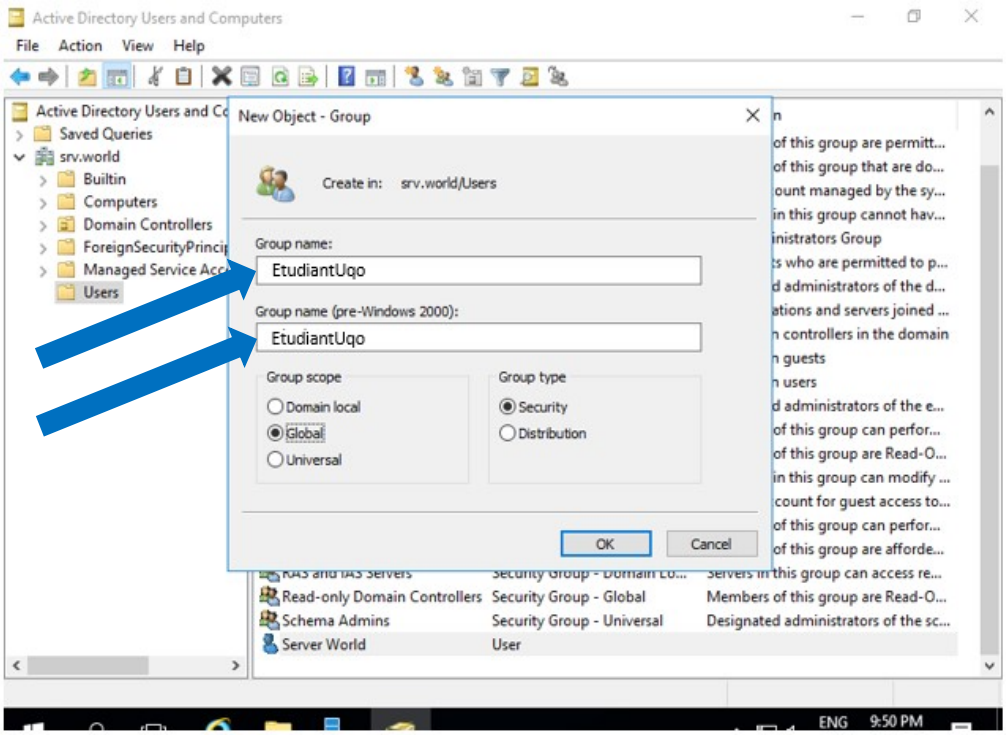

Figure 5 : Interface pour l'ajout ou la création d'un groupe (source : réalisé par nous)

On pourrait finalement voir dans l'image ci-dessous que le groupe ''EtudiantUqo'' a été bien ajouté ou créé.

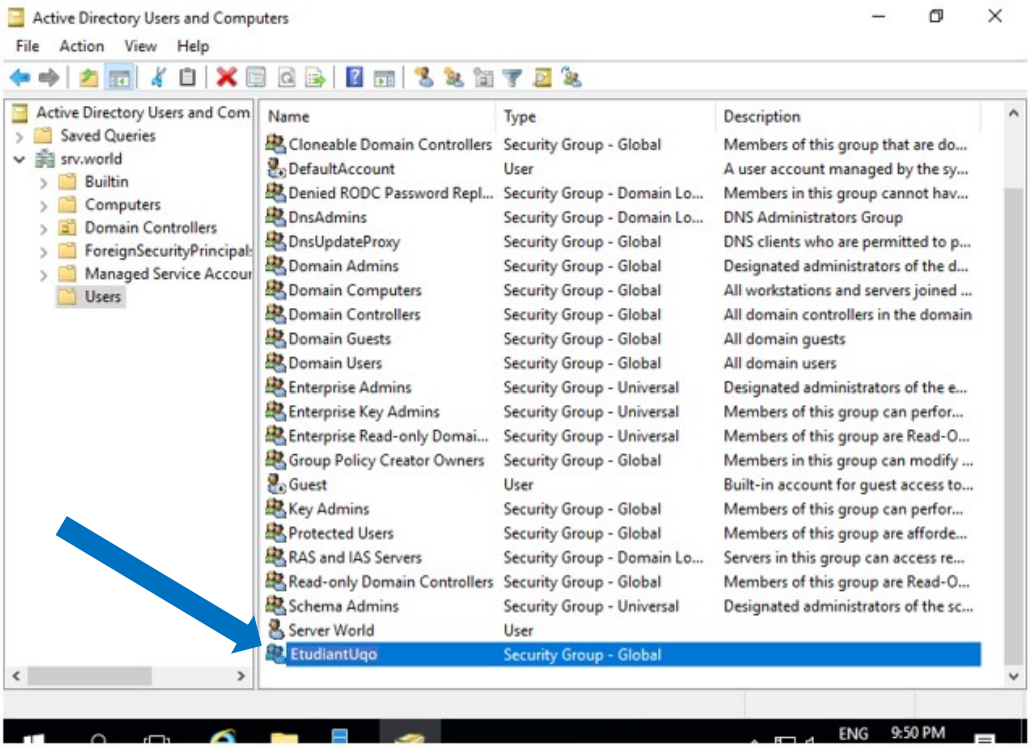

Figure 6 : Interface montrant la réussite de la création du groupe (source : réalisé par nous)

- Création de groupe Active Directory avec PowerShell

Pour créer un groupe Active Directory avec PowerShell, on utilise le cmdlet **New-ADGroup**. La syntaxe complète peut être obtenue en exécutant la commande suivante: **Get-Command New-ADGroup –Syntax.** Mais, le moyen le plus simple de créer un groupe est d'exécuter ce court script : **New-ADGroup "Nom du groupe".** Le système demandera de spécifier le paramètre « GroupScope », puis créera un nouveau groupe. Toutefois, ce groupe sera assorti de valeurs par défaut, telles que :

- Il sera créé dans le conteneur LDAP par défaut appelé « Utilisateurs ».
- Ce groupe sera du type « Sécurité ».
- Les champs Membres, Description, E-mail et Notes seront tous vides.

III.2.3 Configuration des stratégies de groupe ou GPO (Group Policy Object)

Bien qu'on a eu à parler un peu de GPO dans la partie de contrôle de flux ci-dessus, dans cette partie nous allons voir plus en détails qu'est-ce que c'est que GPO et à quoi ça sert.

Alors, qu'est-ce que c'est que GPO ?

Les stratégies de groupe ou GPO (pour Group Policy Object) sont une fonctionnalité clé de Microsoft Active Directory et sont utilisées pour gérer les configurations et les paramètres des ordinateurs et des utilisateurs dans un environnement Windows.

Les GPO servent à quoi exactement ?

Les GPO permettent aux administrateurs de définir des paramètres de configuration spécifiques pour les ordinateurs membres d'un domaine Active Directory. Ces paramètres peuvent être appliqués à des utilisateurs, des groupes d'utilisateurs ou des ordinateurs dans un domaine Windows, offrant un contrôle centralisé sur la manière dont ces systèmes fonctionnent et interagissent dans le réseau.

Comment créer une GPO ?

Pour créer une GPO, on aura besoin d'un contrôleur de domaine opérationnel et d'un poste client Windows qui sera utilisé pour vérifier que la GPO créée fonctionne bien. Dans ce qui suit nous allons créer une GPO pour bloquer l'utilisation de l'Invite de commande (*console cmd*) dans certaines sessions utilisateurs. L'image ci-dessous montre le processus de création d'une GPO.

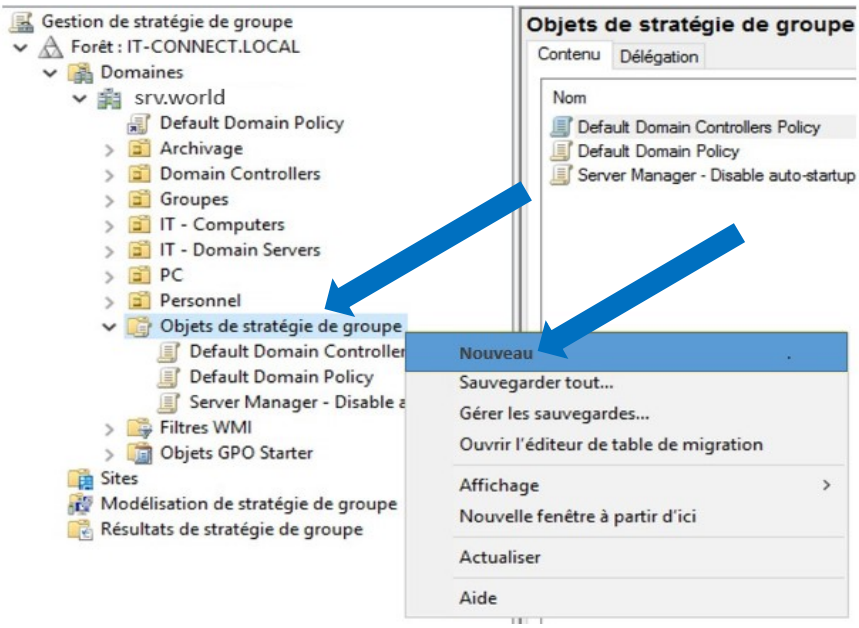

Figure 7 : Processus de création de groupe de GPO (source : réalisé par nous)

Après avoir sélectionné « Nouveau » indiqué par la flèche bleue dans l'image précédente, par la suite, on doit indiquer un nom pour cette GPO. Par exemple, dans l'image ci-dessous, le nom de la GPO est "*U_Bloquer_console_UQO*". Le "*U*" étant là en préfixe pour indiquer qu'il s'agit d'une GPO qui va agir au niveau Utilisateur. Et on clique sur "OK" pour valider.

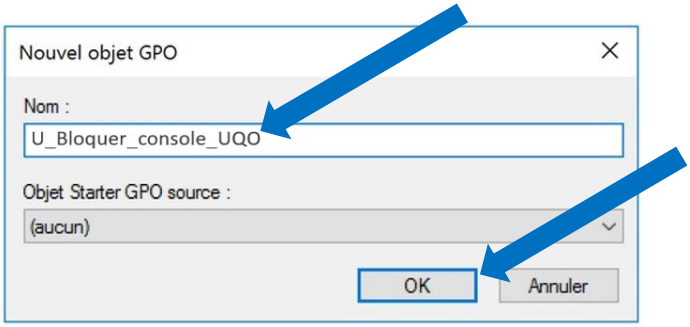

Figure 8 : Processus de création de groupe de GPO (source : réalisé par nous)

IV. Conclusion

Suite aux deux (2) rapports précédents, ce dernier présente la pratique de notre projet. En effet, nous avons présenté pratiquement la création des groupes auxquels sont attribués les rôles, facilitant ainsi la gestion des droits d'accès. Par la suite, nous avons abordé la gestion des stratégies de groupes qui sont une fonctionnalité clé de Microsoft Active Directory. Concernant le contrôle de flux, on a principalement utilisé trois mécanismes pour pouvoir gérer la gestion de flux dans l'environnement Active Directory, à savoir : une topologie de model arborescent et géographique, la réplication et la GPO. Ce rapport clôture notre travail, malgré que beaucoup de notions n'ont pas été assez détaillées comme nous le souhaitons, car nous somme limiter non seulement par le temps, mais aussi par le volume du rapport demandé. Toutes fois, il est clair qu'Active Directory est un thème vaste et surtout très intéressant en ce qui concerne tout ce qui est la gestion des autorisations, ainsi le contrôle de mouvements des données au sein d'une organisation.

Référence :

[1]: By Dishan Francis, (31 mars 2023) Mastering Active Directory, Third Edition: Design, Deploy, and Protect Active Directory Domain Services. Packt Publishing

[2]: By Jordan Krause, (30 Nov 2018). Mastering Windows Group Policy: Control and secure your Active Directory. Packt Publishing

[3]: By Will Willis, David Watts (18 Sept 2006). MCSA/MCSE 70-294 Exam Cram: Planning, Implementing, and Maintaining. Pearson IT Certification

[4]: Derek Melber(25 juin 2005. Microsoft Group Policy Guide. Microsoft Press

[5]: Jean-François. Windows server 2008 ; Architecture et gestion des services de domaine Active Directory (AD DS). APREA Edition ENI

[6]: Ravi S Sandhu, Pierangela Samarati. Access control: principle and practice, Volume 32. Edit by IEEE.