International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 7 Issue 7, July - 2023, Pages: 9-24

Use of GPO as an optimization solution for the management of information system software resources within the University of "Notre-Dame-du-Kasayi (UKA)"

[1]BAKAJIKA NGANDU Léonard.

[1] *Licencié en Sciences Informatiques (orientation : Réseaux informatiques) et Assistant de Recherche à l'Université Notre Dame du Kasayi (U.KA.), Kasaï Central, Kananga (RDC).*

Abstract: *GPOs appeared with Windows 2000 and Active Directory. They have a very major role in the management of a computer park. Thus, they make it possible to apply configuration parameters to computers or even users and to be distributed by means of an Active Directory Domain. Mastering group policies in Windows environments means increasing the security capacity of the company. Countless policy settings related to the security of workstations and servers as well as network data are configurable with GPOs. This article is not an in-depth study of group strategies because it is such abundant material that needs to be synthesized to produce an essay such as ours. Indeed, we are going to target the essential points before moving on to the configuration which will only be possible with the involvement of Windows Server, all versions combined.*

Keywords: *Usage, GPO, Solution, Optimization, Management, Resources, Software, University, Windows Server, System, Information, UKA, etc.*

Utilisation des GPO comme solution d'optimisation de la gestion des ressources logicielles du Système d'Information au sein de l'Université Notre-Dame-du-Kasayi (UKA).

Résumé

Les GPO sont apparues avec Windows 2000 et Active Directory. Elles ont un rôle très majeur en ce qui concerne la gestion d'un parc informatique. Ainsi donc, elles permettent d'appliquer des paramètres de configuration sur les ordinateurs voire les utilisateurs et d'être distribuées au moyen d'un Domaine Active Directory. Maîtriser les stratégies de groupe dans les environnements Windows, c'est augmenter la capacité de sécurisation de l'entreprise. D'innombrables paramètres de stratégies liés à la sécurité des postes de travail et des serveurs ainsi que des données du réseau sont configurables avec les GPO. Cet article n'est pas une étude approfondie portant sur les stratégies des groupes car, c'est une matière tellement abondante qui nécessite d'être synthétisée pour produire une rédaction telle que la nôtre. En effet, nous allons cibler les points essentiels avant de passer à la configuration qui ne sera possible qu'avec l'implication de Windows Server toute version confondue.

Mots-clés : *Utilisation, GPO, Solution, Optimisation, Gestion, Ressources, Logiciel, Université, Windows Serveur, Système, Information, UKA, etc.*

I. INTRODUCTION

Dans le domaine informatique, la sécurité est un des éléments les plus sensibles. Le terme sécurité est large et il englobe une multitude de concepts. La sécurité physique des données de l'entreprise, l'intégrité des données informatiques, leur disponibilité et leur sauvegarde contribuent au maintien de l'existence de l'entreprise surtout dans le secteur académique où les informations à traiter sont innombrables. La majorité des réseaux d'entreprise sont aujourd'hui connectés à Internet. Ainsi donc, il existe deux grandes catégories : la sécurité domestique et la sécurité extérieure. **(3)**

La sécurité domestique relève de toutes les manipulations maladroites ou intentionnelles qui peuvent nuire à l'intégrité du réseau local. La sécurité extérieure doit empêcher les attaques, virus et autres programmes malveillants d'agir. Ceux-ci sont majoritairement issus de l'extérieur de l'entreprise. Ces intrusions proviennent le plus souvent d'Internet ou de supports amovibles. **(8)**

Maîtriser les stratégies de groupe dans les environnements Windows, c'est augmenter la capacité de sécurisation de l'entreprise. D'innombrables paramètres de stratégies liés à la sécurité des postes de travail et des serveurs ainsi que des données du réseau sont configurables avec les GPO (Group Policy Objet). C'est le pourquoi de cette rédaction qui porte sur la gestion centralisée de ressources dans un réseau au sein de l'Université Notre-Dame du Kasayi(UKA). Deux aspects sont visés : à priori nous allons parler de l'esquisse théorique et nous allons chuter par la mise en œuvre de la solution moins couteuse qui renforce la sécurité des ressources au sein du système informatique de l'UKA.

II. ESQUISSE THEORIQUE

Comme nous l'avons souligné sommairement, la présente partie va rassembler tout ce qui cadre avec la théorie portant d'une part sur l'administration d'un réseau informatique dans une entreprise qui se réfère aux activités, aux méthodes, aux procédures comme la surveillance du réseau et aux outils de mise en œuvre par l'administrateur réseaux ayant trait à l'exploitation, l'administration, la maintenance et la fourniture des réseaux informatiques. **(10)**

II.1. Administration Réseau

L'administration désigne plus spécifiquement les opérations de contrôle du réseau avec la gestion des configurations et de sécurité. De façon générale, une administration de réseaux a pour objectif d'englober un ensemble de techniques de gestion mises en œuvre pour **(1)** :

- Offrir aux utilisateurs une certaine qualité de service ;
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités ;
- Rendre opérationnel un système.

L'administration réseau englobe plusieurs idées qui peuvent faire objet d'un ouvrage dont le nombre de pages est innombrable. Cependant, nous allons nous limiter sur certains aspects importants qui vont nous conduire à trois types d'administration réseau. Nous allons en parler dans les lignes qui suivent. Certes, l'administration des réseaux informatiques peut se décomposer en trois types d'administration. Nous pouvons observer la figure ci-dessous qui décrit ces trois types d'administration :

Figure 1 : Typologie de l'administration des réseaux informatiques **(10)**.

a) L'administration des utilisateurs (consommateur de service)

L'administration des utilisateurs fournit l'ensemble des mécanismes nécessaires pour une personne afin d'utiliser le réseau, à savoir **(2)** :

- ***Accessibilité et Connectivité aux applications*** : l'utilisateur doit pouvoir se connecter aux différentes applications fournit par le réseau et doit disposer d'un ensemble d'outils lui assurant une certaine transparence au niveau des méthodes d'accès et connexions aux applications.

- ***L'accès aux serveurs de noms*** : afin de permettre la localisation des ressources et d'assurer à l'utilisateur l'existence et l'utilisation de ces ressources.

- ***la Confidentialité et la Sécurité*** : Le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.

b) L'administration des serveurs (ou fournisseur de service)

L'administration des serveurs fournit tous les mécanismes suivant **(2)** :

- ***La Connexion et la Distribution des applications sur tout le réseau*** : afin de permettre la relation entre les différents services.

- ***La Gestion et la Distribution des données*** **:** comme pour les utilisateurs, doivent garantir la fiabilité de transmission des informations et offrir des outils permettant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes.

c) L'administration de la machine de transport

L'administration de la machine de transport consiste à fournir **(9)** :

- ***Les opérations de réseau*** *:* dont le rôle est de permettre l'intervention sur le fonctionnement et la modification du réseau.

- ***La liste des incidents réseaux par la mise en place de protocoles de détection et de correction*** : lorsqu'une alerte est déclenchée, des actions vont être prises pour résoudre l'incident et de ce fait, réduire son influence et ses perturbations sur l'ensemble du réseau.

- ***Les performances fournies par le réseau*** *:* le but est d'afficher et d'évaluer le système par un ensemble de paramètres comme le temps de réponse ou la charge du système.

II.2. Active Directory

1. Principes

Active Directory est un service de répertoire développé par Microsoft pour les systèmes d'exploitation Windows. Il est utilisé pour stocker des informations sur les ressources réseau, telles que les ordinateurs, les utilisateurs, les groupes et les applications, et permet de fournir un moyen centralisé pour l'authentification et l'autorisation des utilisateurs et des ordinateurs sur le réseau. **(4)** Active Directory est basé sur le protocole LDAP (*Lightweight Directory Access Protocol*) et utilise un modèle hiérarchique pour organiser les objets de répertoire. Les informations stockées dans Active Directory peuvent être accessibles aux applications qui prennent en charge LDAP, telles que les serveurs de messagerie ou les applications de gestion des ressources humaines **(4)**.

Les avantages d'utiliser Active Directory incluent la centralisation de la gestion des comptes utilisateurs, la simplification de la gestion des autorisations et des accès aux ressources, la réduction des coûts de gestion et de maintenance du réseau, et l'amélioration de la sécurité en permettant une gestion centralisée des stratégies de sécurité.

2. Annuaire LDAP

L'annuaire LDAP regroupe tous les objets dans un arbre :

- La racine de cet arbre est le domaine (DNS).
- Les branches sont des unités d'organisations (pas des objets).
- Les feuilles sont des objets (utilisateurs, groupes, ordinateurs, ...).

Un exemple d'arbre pour le domaine uka.fr :

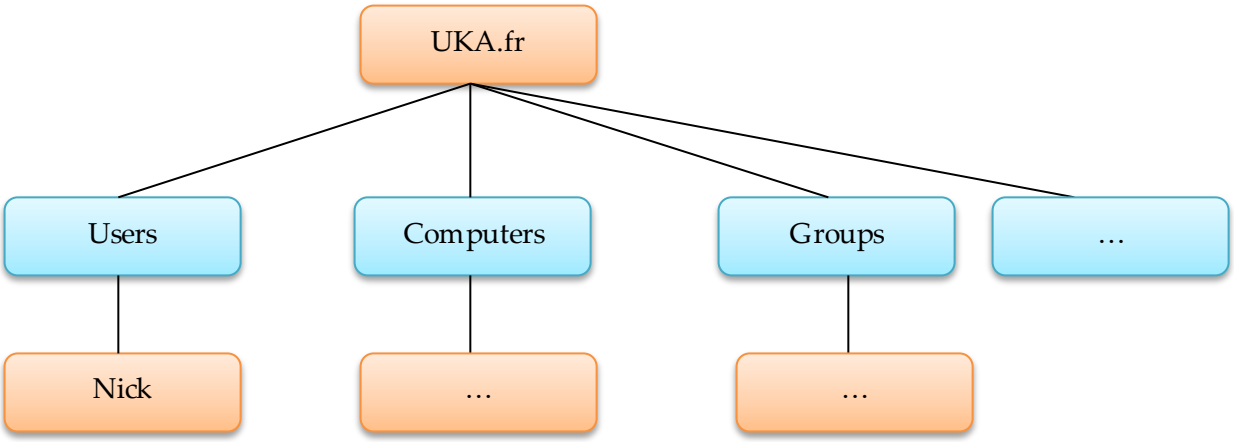


Figure 2 : Arbre pour le domaine de l'UKA.

3. Domaines, Arborescence, Forêts

Dans un contexte Active Directory, trois termes sont à retenir **(7)** :

- **Domaine (ou sous-domaine)** : Le domaine au sens de l'AD est le niveau le plus bas. Il contient au moins un contrôleur de domaine (Ldap + Kerberos). Il représente une organisation ou une partie d'une organisation.
- **Arborescence :** Ensemble d'un domaine et de tous ses sous-domaines.
- **Forêt :** Ensemble d'arborescences qui appartient à la même organisation. Au choix de l'architecte réseau, deux arborescences peuvent appartenir à une même forêt ou pas.

4. Rôles, Service de rôle et fonctionnalités

a) Rôles

Un rôle serveur est un ensemble de logiciels qui, lorsqu'ils sont installés et correctement configurés, permettent à un ordinateur d'exécuter une fonction spécifique pour plusieurs utilisateurs ou d'autres ordinateurs au sein d'un réseau. En général, les rôles partagent les caractéristiques suivantes **(9)** :

- Ils décrivent la fonction principale, le but ou l'utilisation d'un ordinateur. Un ordinateur spécifique peut être dédié à l'exécution d'un rôle unique qui est fortement utilisé dans l'entreprise, ou peut effectuer plusieurs rôles si chaque rôle n'est que légèrement utilisé dans l'entreprise.
- Ils permettent aux utilisateurs d'une organisation d'accéder à des ressources gérées par d'autres ordinateurs, telles que des sites Web, des imprimantes ou des fichiers stockés sur différents ordinateurs.

b) Service de rôle

Les services de rôle sont des logiciels qui fournissent les fonctionnalités d'un rôle. Lorsque vous installez un rôle, vous pouvez choisir les services de rôle qu'il fournit aux autres utilisateurs et ordinateurs de votre entreprise. Certains rôles, tels que Serveur DNS, n'ont qu'une seule fonction et ne disposent donc pas de services de rôle disponibles. D'autres rôles, tels que les services Bureau à distance, ont plusieurs services de rôle qui peuvent être installés, en fonction des besoins informatiques à distance de votre entreprise **(9)**. Vous pouvez considérer un rôle comme un regroupement de services de rôle complémentaires étroitement liés, pour lesquels, la plupart du temps, l'installation du rôle signifie l'installation d'un ou plusieurs de ses services de rôle.

c) Fonctionnalités

Les fonctionnalités sont des logiciels qui, bien qu'ils ne fassent pas directement partie des rôles, peuvent prendre en charge ou augmenter les fonctionnalités d'un ou de plusieurs rôles, ou améliorer les fonctionnalités du serveur, quels que soient les rôles installés. Par exemple, la fonctionnalité Telnet Client, vous permet de communiquer à distance avec un serveur Telnet via une connexion réseau, une fonctionnalité qui améliore les options de communication du serveur **(8)**.

5. Unité d'organisation(OU), Groupes, Utilisateurs

L'annuaire permet aussi de créer notamment **(7)** :

- Des unités d'organisation dans lesquelles on pourra créer des objets (utilisateurs, groupes, imprimantes, …) et sur lesquelles on pourra appliquer des stratégies de groupe (GPO).
- Des groupes qui permettent de regrouper les utilisateurs dans des ensembles sur lesquels on pourra définir des droits de sécurité NTFS.
- Des comptes utilisateurs qui permettent de définir individuellement le profil de chaque utilisateur.

6. Group POlicy (GPO)

GPO, une solution adéquate pour un contrôle de l'utilisation de ressources d'une entreprise. Il s'agit d'un ensemble de paramètres qui s'appliquent automatiquement à des utilisateurs ou des groupes sur des postes clients ou des serveurs. Ils sont un outil de gestion des stratégies de sécurité et de configuration pour les systèmes d'exploitation Windows, largement utilisé dans les environnements d'entreprise. Les GPO permettent aux administrateurs informatiques de configurer les paramètres de sécurité, les restrictions logicielles, les paramètres de réseau, les paramètres d'impression et bien d'autres fonctionnalités pour les ordinateurs et les utilisateurs dans un domaine « Active Directory ».

Dans l'ensemble, les GPO sont un outil puissant et efficace pour gérer les environnements Windows à grande échelle. Ils permettent aux administrateurs informatiques de configurer rapidement et facilement une grande variété de paramètres de sécurité et de configuration, et de les appliquer à des groupes d'utilisateurs ou d'ordinateurs spécifiques.

Cependant, les GPO peuvent également être complexes et difficiles à comprendre pour les administrateurs inexpérimentés, et peuvent causer des problèmes si elles sont mal configurées ou appliquées de manière incorrecte. Il est donc important que les administrateurs informatiques soient bien formés et aient une bonne compréhension des GPO avant de les utiliser dans un environnement de production **(3)**.

III. MISE EN PLACE DE LA SOLUTION ENVISAGEE

Nous avons déjà beaucoup écrit. Cependant, la présente partie va capitaliser la solution, qui est évidemment la mise en place des stratégies GPO pour garantir un bon usage des ressources logicielles et surtout renforcer leur sécurité au sein du système informatique de l'Université Notre-Dame-du-Kasayi.

1. Description du problème

De quoi s'agit-il concrètement pour penser à une telle solution au sein d'une Université ? Disons, UKA possède plusieurs services dans lesquels plusieurs machines sont installées pour des fins biens précis, concourant à l'évolution et à l'épanouissement de l'Université. Mais, un constat amer est à souligner dans l'utilisation de ces machines. Et surtout que la connexion internet est disponible, certains agents l'utilisent pour des fins inutiles, n'aidant à rien. Voir les films sur YouTube, télécharger des fichiers volumineux qui n'ont rien avoir pour gaspiller les forfaits que dispose l'Université, connecter les supports de masse vaille-que-vaille aux ordinateurs pour les exposer aux virus, sont en quelques sortes les exemples qui montrent noir-sur-blanc l'utilisation abusive des ressources. Donc, les ressources matérielles voire logicielles ne sont pas utilisées selon ce qui est demandé. Dommage ! Cela fait qu'au moins à la fin de chaque trimestre l'Université enregistre plus de pertes des matériels qu'elle dispose, parfois le forfait internet souscrit pour un mois s'épuise après une ou deux semaines.

Eu égard à ce qui précède, il a fallu que l'on centralise l'utilisation de ces ressources, puis limiter l'accès aléatoire aux ressources plus importantes, voire restreindre certaines fonctionnalités. C'est d'ailleurs la quintessence de cette rédaction.

2. Modélisation de la solution envisagée

a) Définition

La modélisation des données est l'analyse et la conception de l'information contenue dans le système afin de représenter la structure de ces informations et de structurer le stockage et les traitements informatiques **(6)**. Ainsi, pour arriver à modéliser, il sied d'opter une approche quelconque dont le langage de modélisation UML a été pour nous le choix.

b) Détermination des acteurs et leurs cas

Dans le langage UML, un acteur caractérise un rôle joué par un utilisateur humain ou un autre système qui interagit directement avec le système à représenter **(5)**. Un acteur participe à au moins un cas d'utilisation. « Un acteur peut consulter et/ou modifier directement l'état du système, en émettant et/ou en recevant des messages susceptibles d'être porteurs de données ». Nous avons pour notre cas les acteurs suivants :

→ **Administrateur :** il accède au système par authentification (comparaison de son nom et son mot de passe). Il peut exécuter les opérations suivantes :

- se connecter ;
- s'authentifier ;
- gérer les utilisateurs (ajouter, supprimer, restreindre d'autres fonctionnalités sur les comptes) ;
- configurer le système ;
- se déconnecter.

→ **Utilisateur :** comme l'administrateur, il accède aussi au système par authentification et il peut effectuer les opérations suivantes :

- se connecter ;
- s'authentifier ;
- utiliser les ressources se trouvant dans le système ;
- se déconnecter.

Toutes les opérations qu'effectuent l'administrateur et l'utilisateur peuvent être vues selon les différents diagrammes que nous dispose UML. Ils sont nombreux dont les quelques-uns sont soulevés dans le point suivant.

3. Déploiement de la solution envisagée

C'est dans ce volet que nous allons rester plus pragmatiques en mettant en place la solution dont nous avons beaucoup parlée. Pour ce faire, nous avons eu à utiliser le système d'exploitation Windows serveur 2019, qui est installé dans la machine serveur. De prime abord, nous allons mettre la maquette de le ladite solution comme le montre la figure ci-dessous.

a) Maquette de la solution GPO

Pour la réalisation de la maquette, nous avons fait recours au simulateur réseau Cisco Packet Tracer qui nous a aidés à trouver tous les outils possibles pour simuler la solution GPO entre un serveur et les ordinateurs d'autres services. Ladite maquette se présente de cette façon :

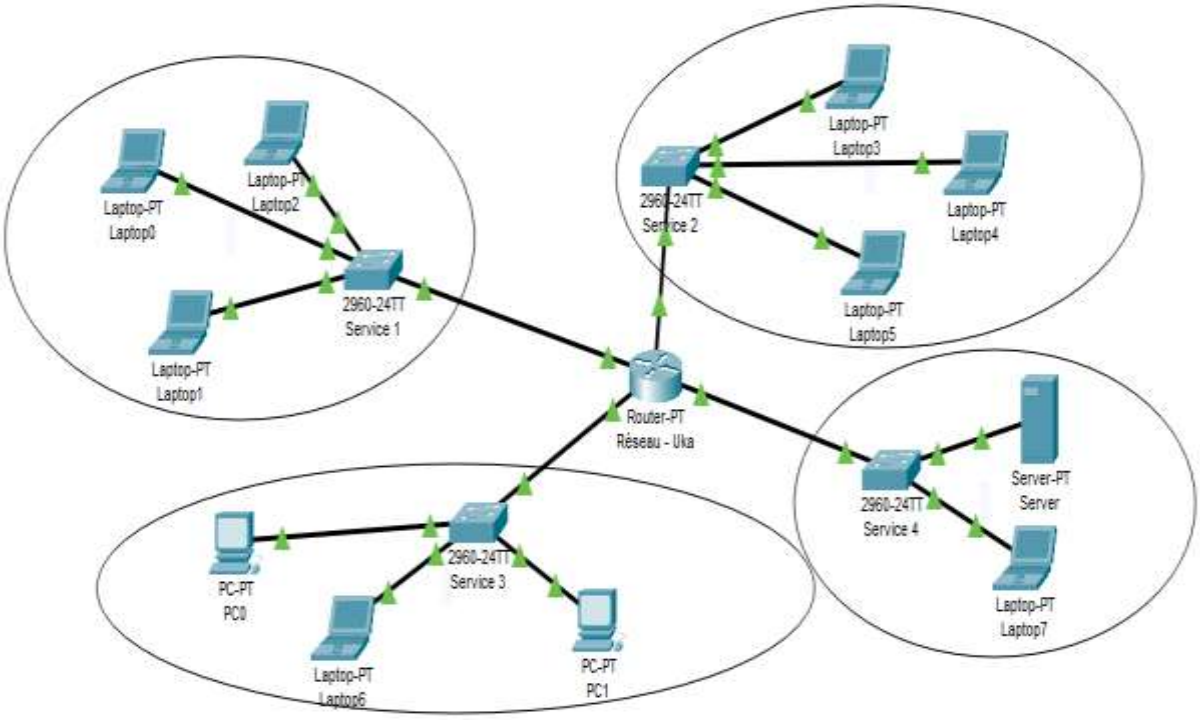


Figure 3. La maquette de la solution envisagée.

b) Présentation de la solution envisagée.

Avant toute chose, il sied que nous installions d'abord le logiciel serveur. Pour notre cas, nous avons eu à utiliser le Windows Server 2019 dont l'installation se fait comme toute autre installation. Nous allons mettre quelques captures pour illustrer cela :

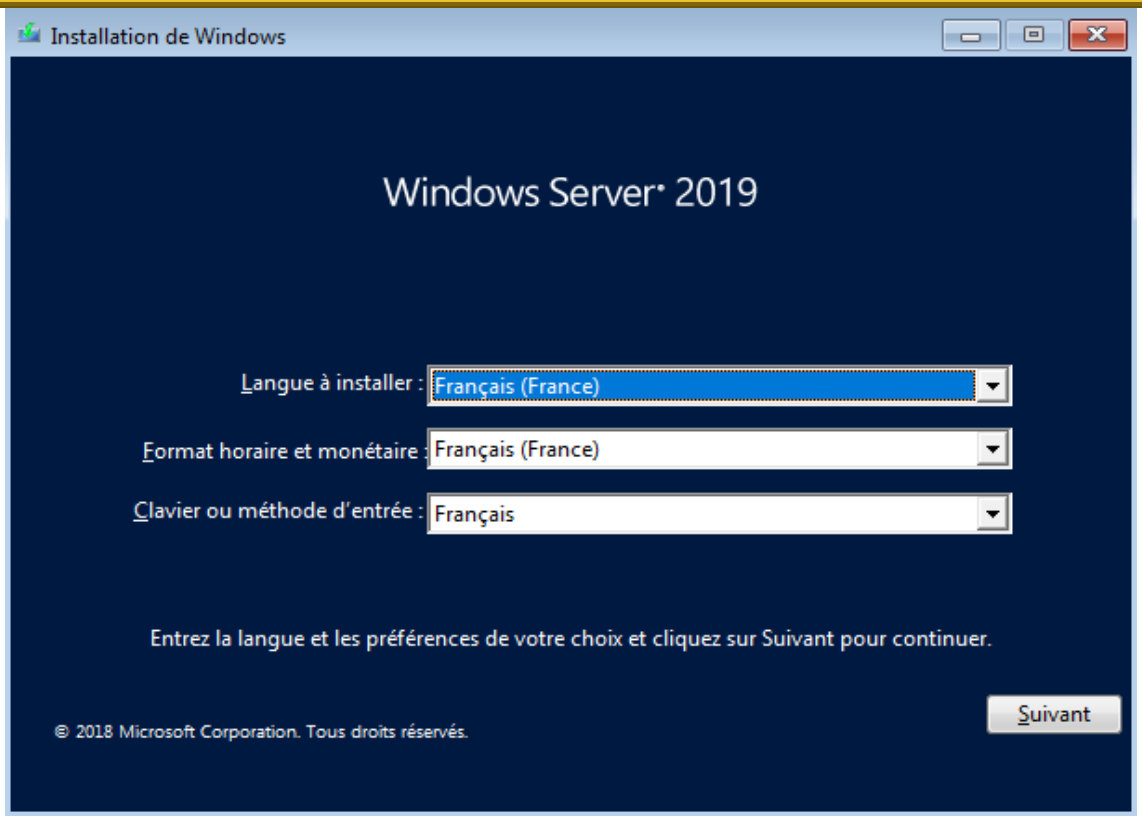


Figure 4 : Présentation de Windows server 2019 et son installation.

Après installation et configuration préalable du Windows Server 2019, cette interface pourra apparaitre demandant l'authentification pour accéder sur le bureau :

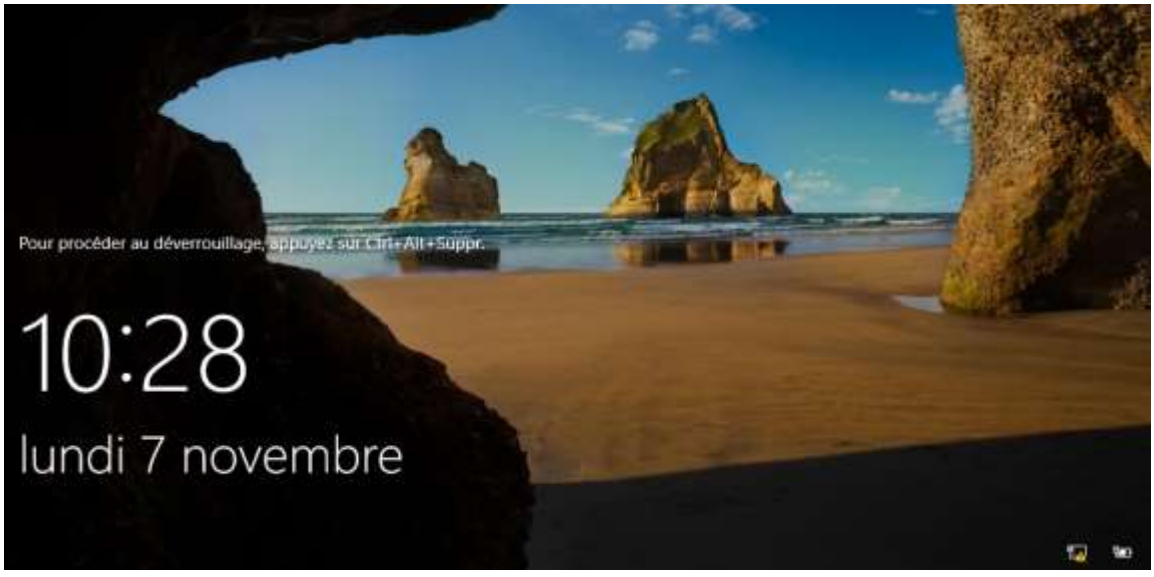


Figure 5 : Présentation de l'interface d'authentification du Windows Server 2019.

Le mot de passer qui a été saisi sera demandé encore. S'il est correct, alors le bureau apparaitra accompagné du tableau de bord sur lequel les configurations seront faites avec abnégation.

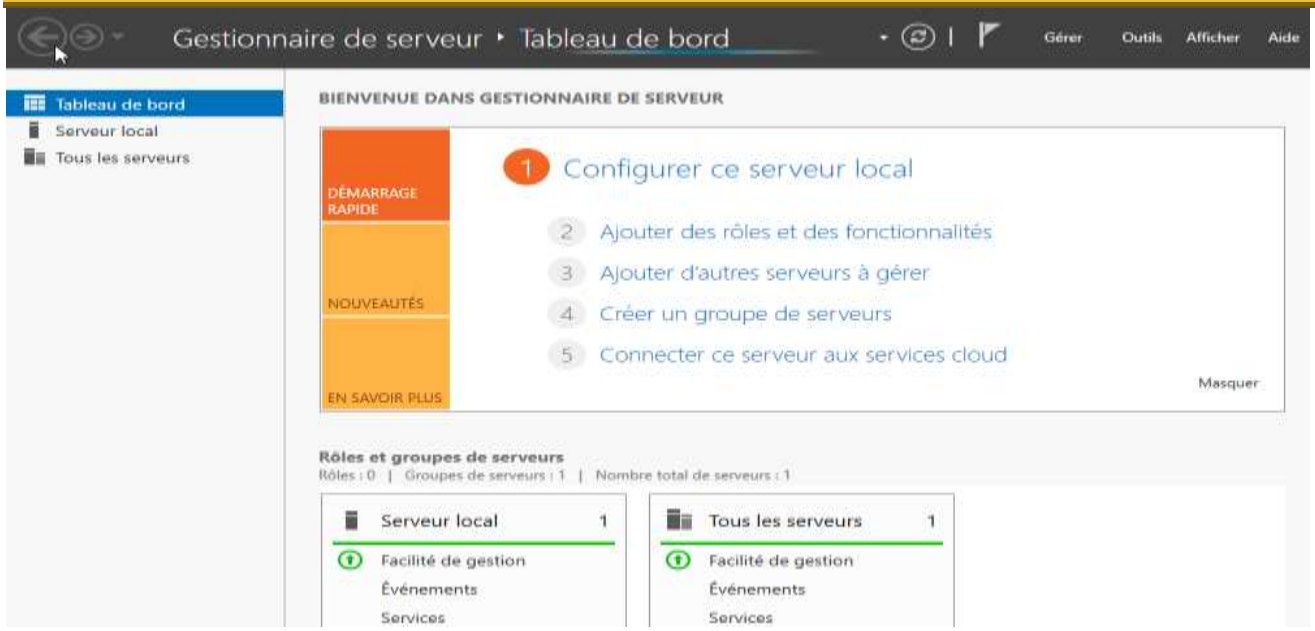
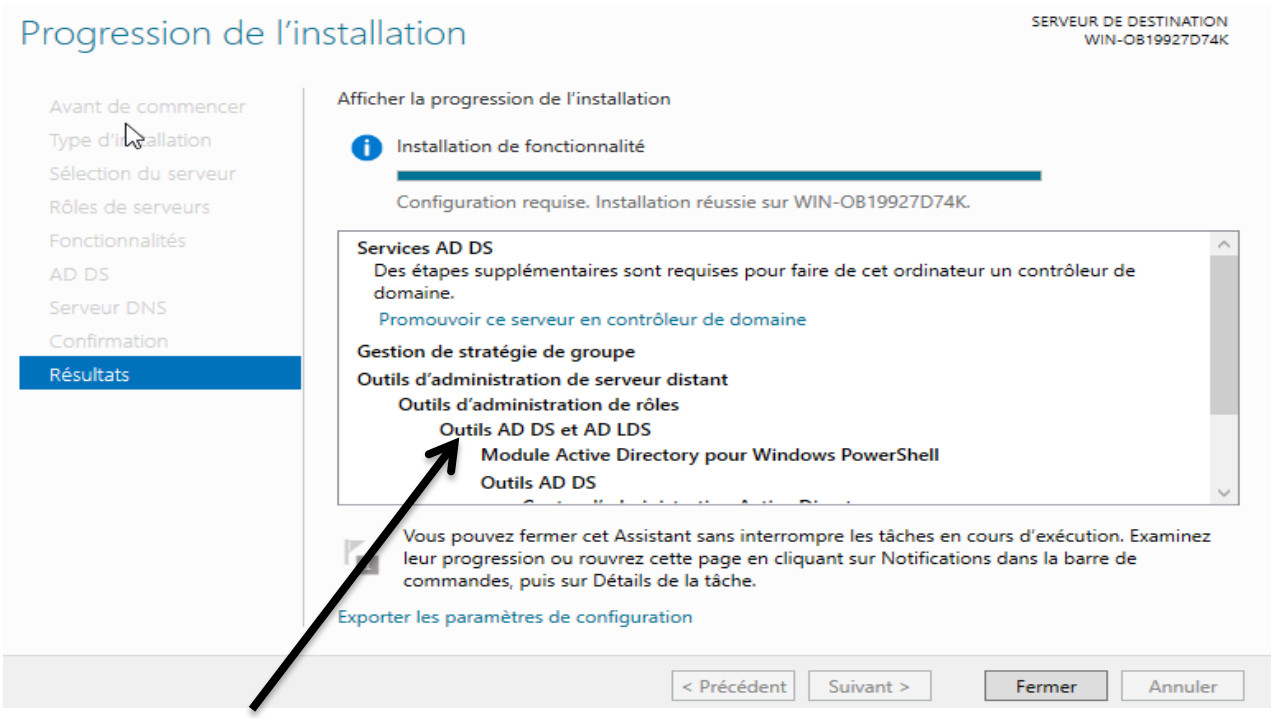


Figure 6 : Présentation du tableau de bord du Windows Server 2019.

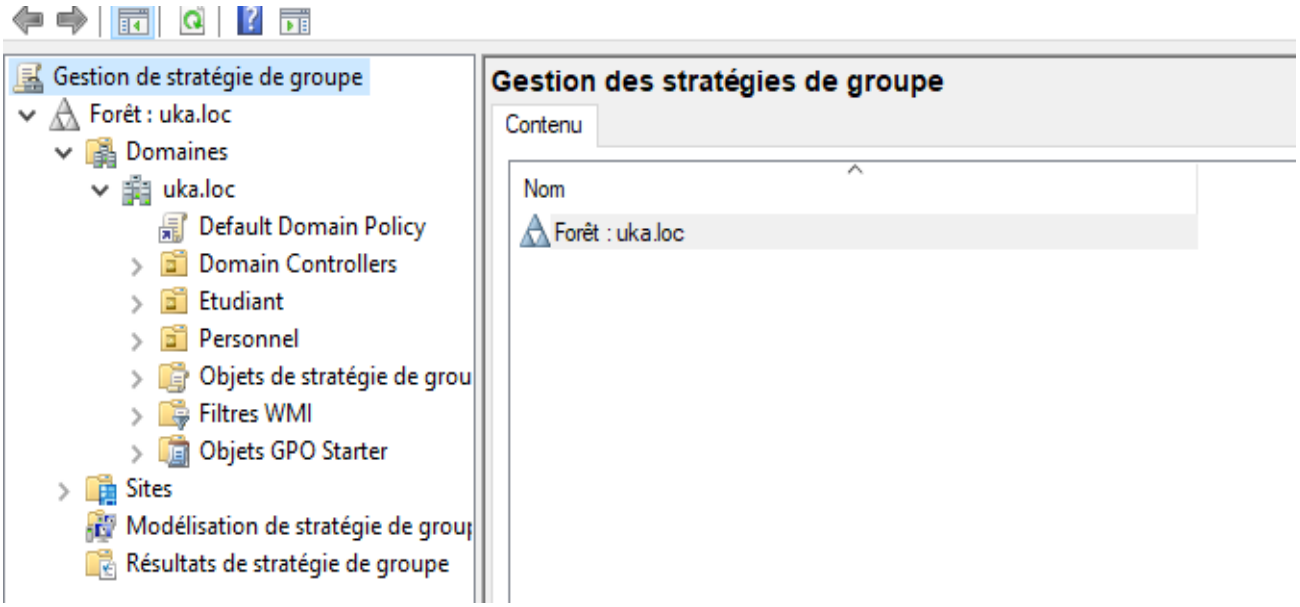
Certes, pour arriver à créer les stratégies, de prime abord il faut qu'on installe le rôle AD DS (Active Directory Domain Services) qui est un service de répertoire utilisé par le système d'exploitation Windows Server pour gérer les ressources d'un réseau, notamment les ordinateurs connectés, les utilisateurs, les groupes voire les unités d'organisations ; ce rôle permet la centralisation des comptes d'utilisateurs et les ordinateurs sur un réseau. L'installation du DNS sera un atout. Cela étant, il sera juste question de cliquer sur l'onglet Gérer puis aller sur ''Ajouter des rôles et fonctionnalités''. Cocher sur les deux rôles précités, puis installer après avoir configuré la carte réseau Ethernet par l'adresse IP statique.

Après l'installation, il faut promouvoir le serveur à contrôler le domaine. La capture ci-contre va l'expliquer.

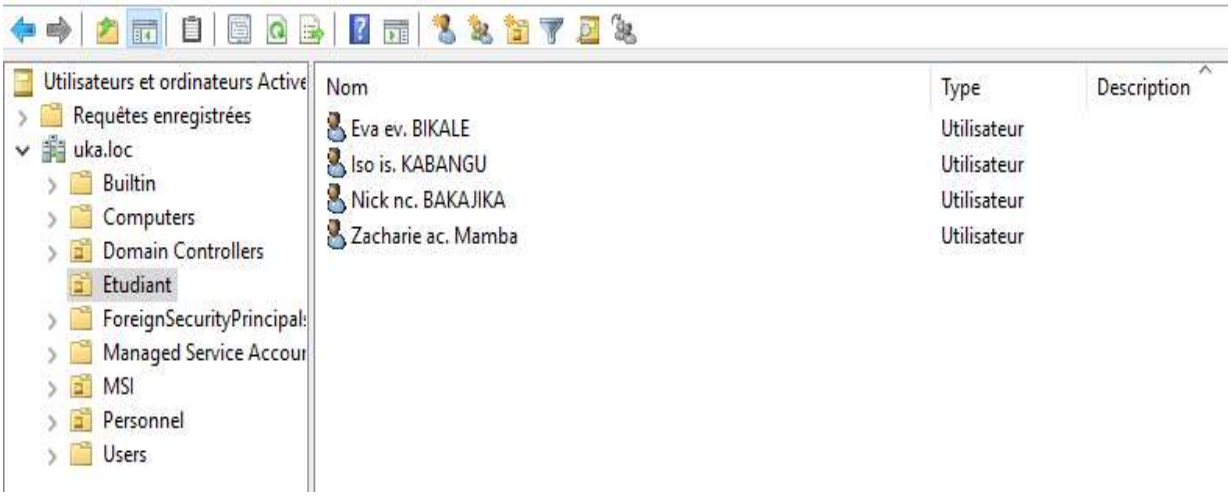


Le nom du domaine sera défini voire le mot de passe. Après la promotion, l'ordinateur pourra se redémarrer pour que les rôles installés soient pris en charge par le serveur.

Alors, comme il est de coutume, il faudrait aller créer les utilisateurs dans ''utilisateur et ordinateur Active Directory''. Pour notre cas, nous avons créé les utilités d'organisation sur lesquelles les différentes stratégies seront appliquées.



Comme on peut le constater, nous avons créé deux unités d'organisation pour illustrer : Etudiant et Personnel. Dans la première unité d'organisation, nous avons ajouté les utilisateurs suivants :



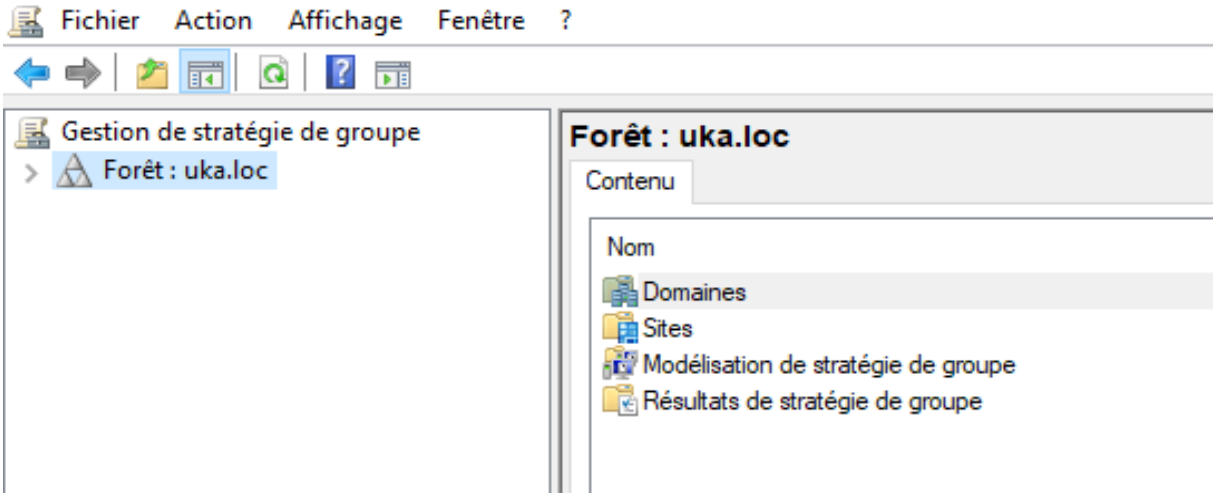
Alors, à cette unité d'organisation, on peut appliquer différentes stratégies GPO.

La création d'une stratégie de groupe au niveau local affecte tous ceux qui utilisent cette machine. Cependant, en utilisant Active Directory, vous disposez d'un nombre presque illimité d'objets de stratégie de groupe, avec la possibilité de choisir quels utilisateurs et quels ordinateurs seront assortis de quels paramètres. En réalité, vous ne pouvez appliquer que 999 GPO à un utilisateur ou un ordinateur avant que le système n'en refuse d'autres.

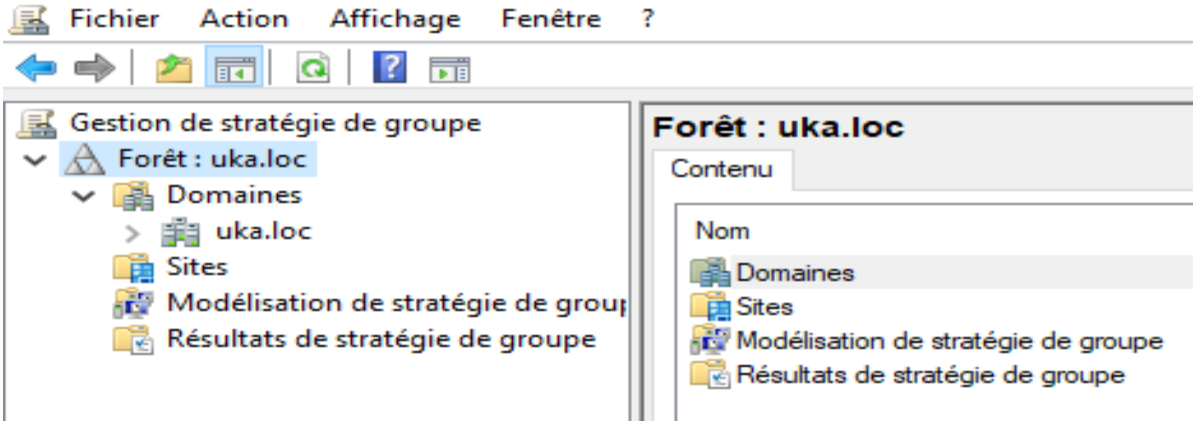
- Si un GPO est lié au niveau domaine, il affecte tous les utilisateurs et tous les ordinateurs du domaine, dans toutes les OU qui se situent à un niveau inférieur.

- Si un GPO est lié au niveau OU, il affecte tous les utilisateurs et ordinateurs de cette OU et toutes les OU en dessous. Comment alors procéder à la création d'un GPO ? Nous allons expliciter avec des captures dans les pages suivantes.

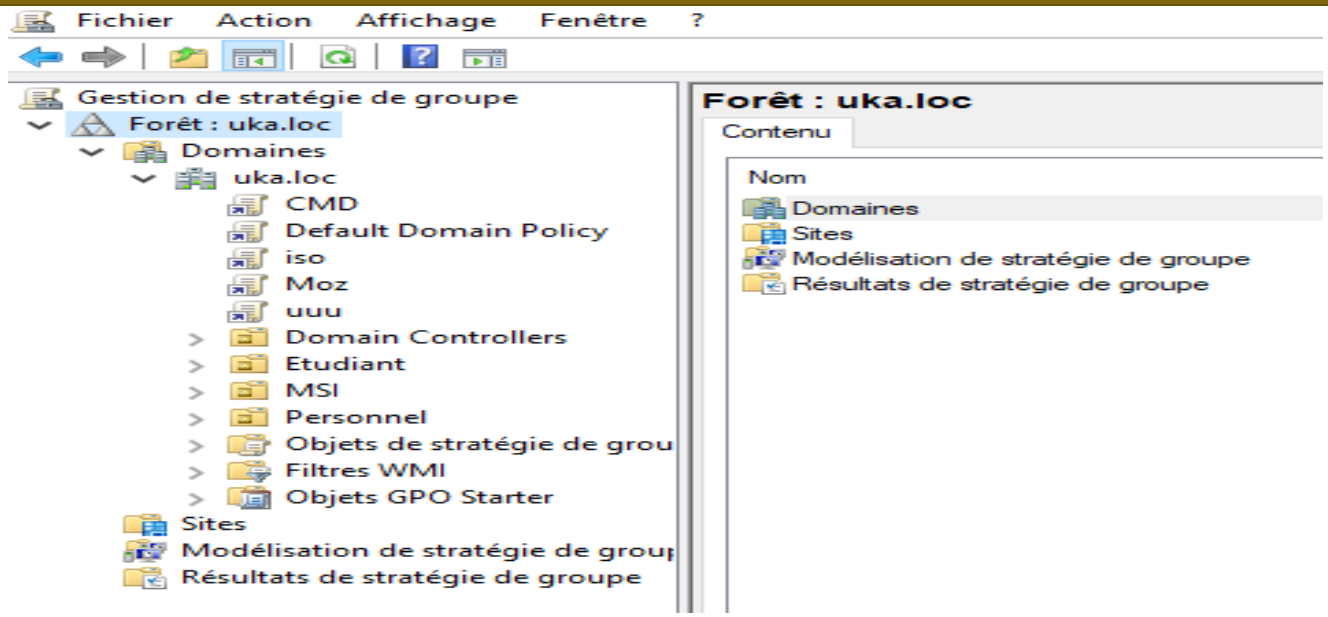
Plusieurs chemins peuvent être appliqués. Soit dans le gestionnaire de serveur, aller cliquer sur Gestion des stratégies de groupe. Puis l'interface suivante va apparaitre :



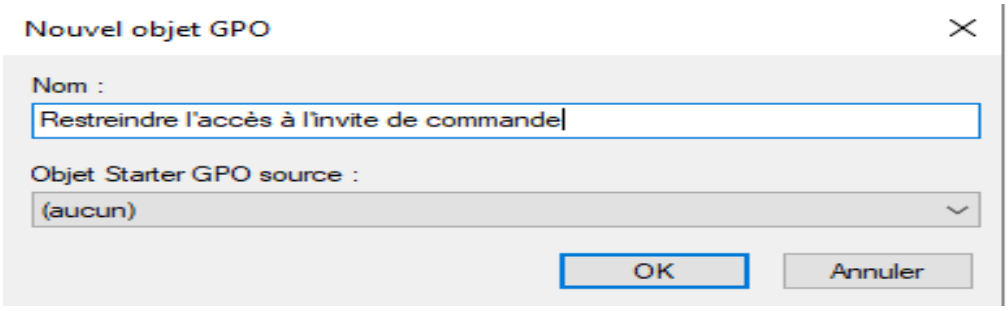
Il sied de cliquer sur la forêt, puis cette fenêtre deviendra comme suit :



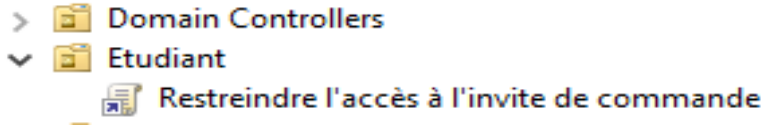
Puis, aller sur le domaine uka.loc pour voir les différents utilisateurs se trouvant dans diverses unités d'organisation. Voilà ce qui sera affiché cette fois-ci :



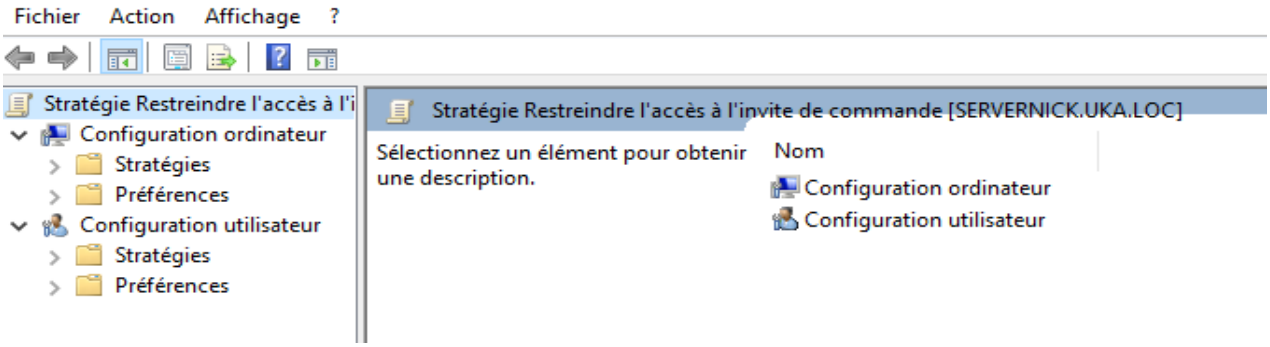
A ce niveau, il suffit de faire clic-droit sur l'OU Etudiant par exemple, puis cliquer sur le menu ''Créer un objet GPO dans ce domaine et le lier ici… '', Soudain la boîte de saisie apparaitra pour la définition du nom de nouvel objet GPO :



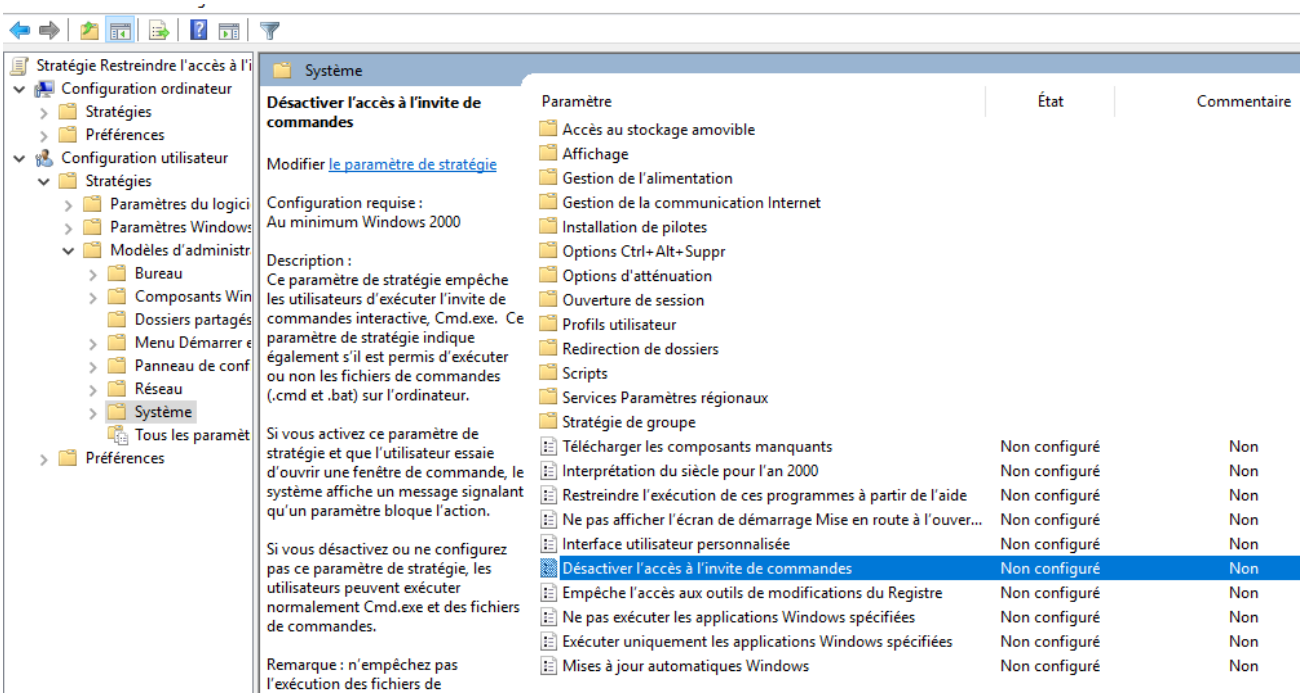
Notre premier objet GPO que nous avons créé pour expérimenter est celui de restreindre l'accès à l'invite de commande, comme nous pouvons le constater dans la capture ci-haut. Après avoir donné le nom, il sied de cliquer sur le bouton OK, ipso-facto l'objet sera ajouté à l'OU spécifiée :



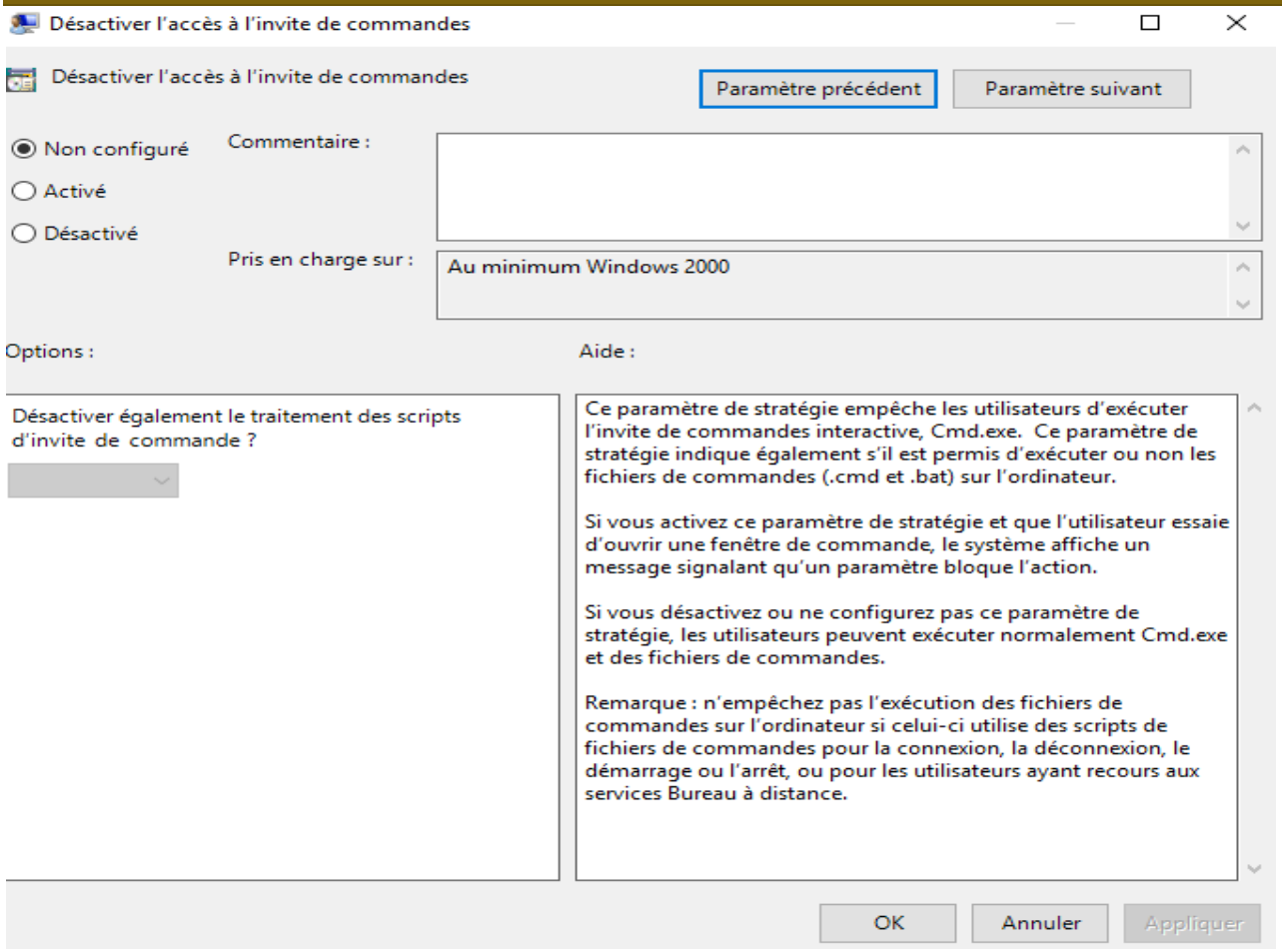
Alors, il sera question de faire le clic-droit sur ledit objet, puis cliquer sur le menu ''Modifier'' pour aller appliquer la stratégie en question. La fenêtre ci-après apparaitra :



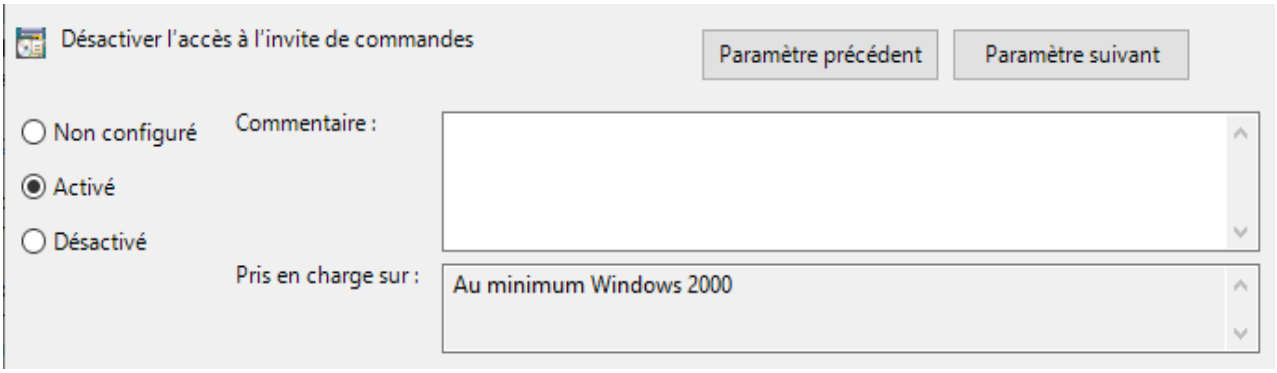
On pourra dérouler sur le menu ‘’Stratégies’’ de l’option Configuration utilisateur. Voilà d’ailleurs le schéma à suivre :



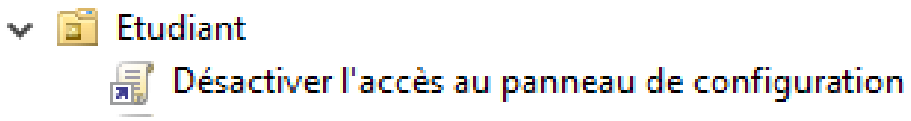
Au niveau d’ici, on pourra double-cliquer sur la stratégie sélectionnée, puis la boîte suivante va sortir :



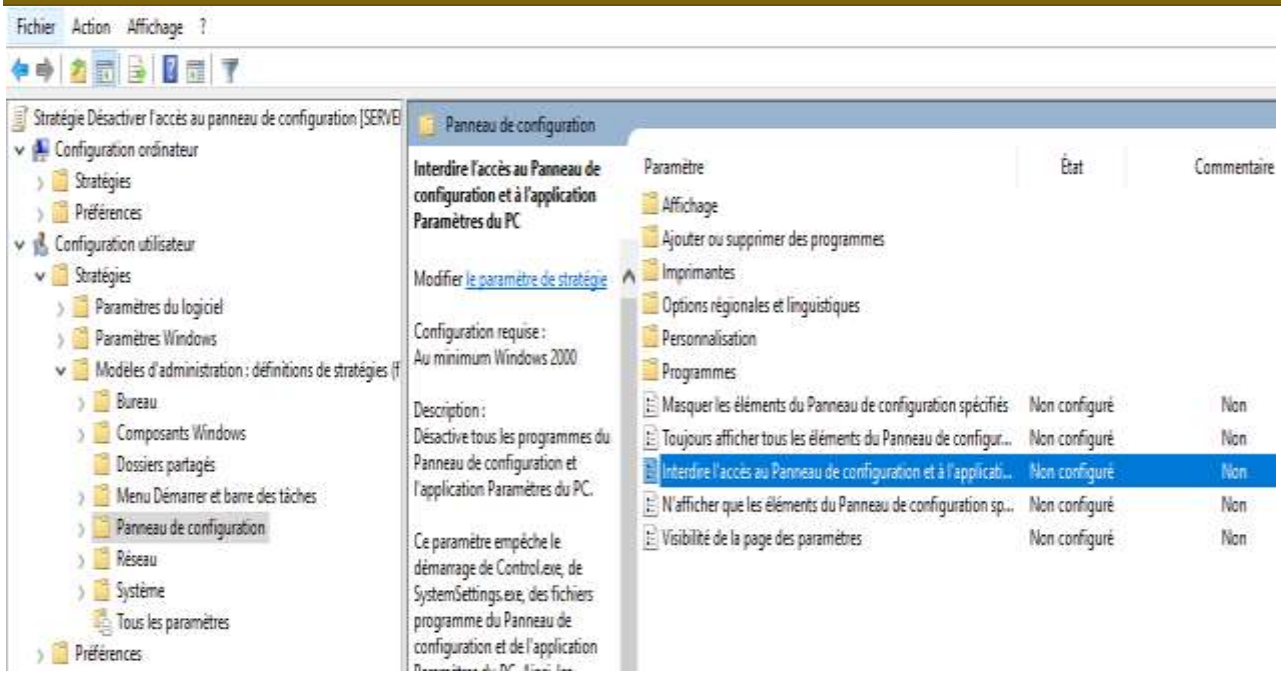
Sur l'image ci-haut, on a décrit la stratégie que l'on veut appliquer sur l'OU sélectionnée. Mais il faut l'activer à partir du bouton radio correspondant :



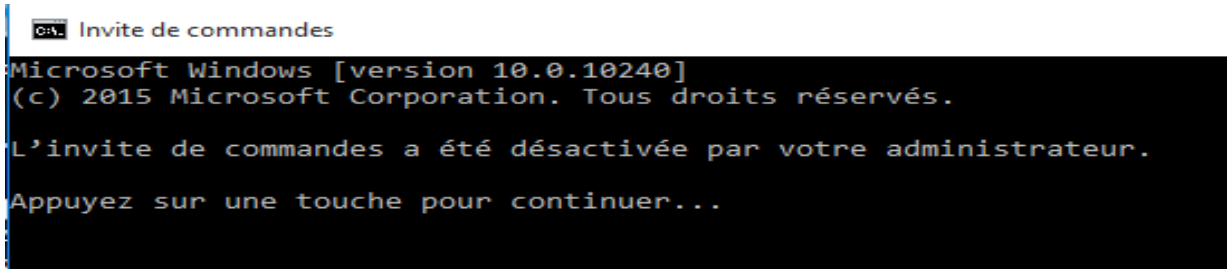
Après avoir coché, il sied d'appliquer puis OK directement la stratégie sera appliquée. Il y a plusieurs stratégies que nous pouvons appliquer, prenons un cas tel qu'interdire l'accès au panneau de configuration.



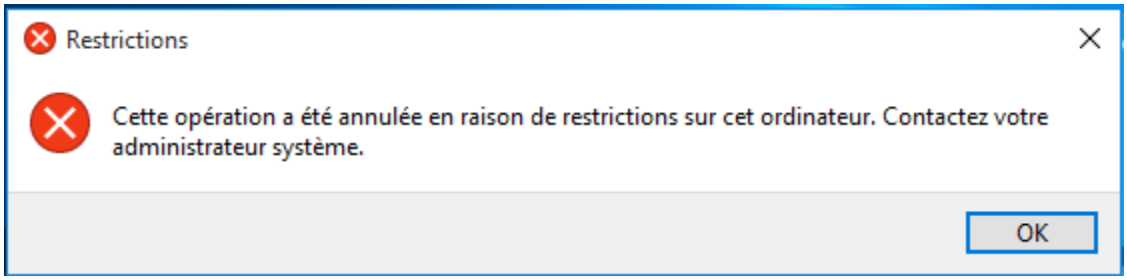
Même procédure, mais cette fois-ci en suivant le chemin-suivant :



Les autres étapes seront les mêmes que celles lors de la définition de stratégie pour la restriction à l'invite de commande. En effet, du côté utilisateur, voilà ce qui pourra apparaitre lorsqu'on voudra entrer en invite de commande ou accéder au panneau de configuration : Pour l'invite de commande, le tableau sera ouvert mais avec le message suivant :



Pour le panneau de configuration, on va réprimander l'utilisateur par un message suivant :



La liste de stratégies n'est pas exhaustive, il y a même la possibilité d'empêcher le déplacement de la barre de tâches et faire autres choses.

CONCLUSION

L'utilisation des politiques de groupe (GPO) comme solution d'optimisation de la gestion des ressources logicielles du système d'information au sein de l'UKA présente plusieurs avantages et participe activement à la sécurité des systèmes Windows. Tout d'abord, les GPO permettent de centraliser et de simplifier la gestion des ressources logicielles. En créant des politiques qui s'appliquent à des groupes d'utilisateurs ou d'ordinateurs, les administrateurs peuvent définir facilement les permissions d'accès aux logiciels et en contrôler l'installation et la désinstallation. Cela garantit une utilisation cohérente et sécurisée des applications à travers l'organisation.

De plus, les GPO offrent une granularité fine dans la gestion des ressources logicielles. Les administrateurs ont la possibilité de définir des conditions spécifiques pour l'installation ou l'exécution des logiciels, par exemple en se basant sur des critères tels que l'appartenance à un groupe, l'emplacement géographique ou le type d'ordinateur. Cela permet d'adapter les ressources logicielles en fonction des besoins de chaque utilisateur ou groupe d'utilisateurs. Les GPO permettent également de simplifier les mises à jour et les déploiements de logiciels. En créant des politiques de groupe spécifiques, les administrateurs peuvent automatiser le déploiement de nouvelles versions de logiciels, réduisant ainsi le temps et les efforts nécessaires pour maintenir les systèmes à jour. Enfin, les GPO offrent un niveau de sécurité supplémentaire en permettant de restreindre l'accès aux logiciels sensibles ou critiques. Les politiques de groupe peuvent être utilisées pour limiter l'accès à certaines applications ou pour empêcher leur installation ou leur exécution sur des ordinateurs non autorisés. Cela contribue à renforcer la sécurité du système d'information de l'UKA.

En conclusion, l'utilisation des politiques de groupe (GPO) comme solution d'optimisation de la gestion des ressources logicielles du système d'information au sein de l'UKA présente de nombreux avantages en termes de centralisation, de simplification, de granularité, de gestion des mises à jour et de sécurité. Elle permet d'assurer une utilisation cohérente et sécurisée des applications à travers l'organisation, tout en offrant une flexibilité et une adaptabilité aux besoins spécifiques des utilisateurs et des groupes d'utilisateurs.

REFERENCES

(1). E. HARTMANN, F. H., *Administration de réseaux locaux*, Addison-Wesley, 1994, p.390.
(2). G. MOURIER, *L'indispensable pour l'administration des réseaux locaux, l'essentiel pour bien débuter*, Marabout, 1996, p.658.
(3). J. BEZET-TORRES**,** *Les stratégies de groupe (GPO) sous Windows Server 2019 : Planification, Déploiement et Dépannage,* ENI, Saint-Herblain, 2019, p.291.
(4). J. FRANCOIS, Windows Server 2016 : Architecture et Gestion des services de domaine Active Directory (AD DS), Edition ENI, Saint-Herblain, 2016, p.345.
(5). O. GUIBERT, *Analyse et Conception des Systèmes d'Information – Méthodes Objet. Le langage de modélisation objet UML,* Paris, Département Informatique de l'Institut Universitaire de Technologie de l'Université Bordeaux 1, 2010, p.2.
(6). P. ROQUES, *Les cahiers du programmeur UML2*, 4eme Edition, Eyrolles, Paris, 2008, p. 10.
(7). W-R. STANEK, *Microsoft® Windows Server 2012: Guide de l'administrateur*, 5th Edition, Addison-Wesley, 2008, p.56.
(8). YENDE R. Grevisse & KASEKA K. Viviane, « *Divergence possible des processus de Data mining et Knowledge Discovery in Databases* », European Journal of Natural and Social Sciences, EJNSS-NOVUS, 01(10), Jan 2023.
(9). YENDE R. Grevisse et al., "*Operational approach to kernel system protection under Windows Server 2019: Optimization, QoS and Performance*", EJCSIT, 11(2), 70-99, 2023.
(10). YENDE R. Grevisse, *Administration des réseaux informatiques,* MédiasPaul, Kinshasa, 2019, p.9.