BTS SIO PARCOURS SISR

Description d'une
RÉALISATION PROFESSIONNELLE
compétences E6 ■ Epreuve **E6**

UFITECH **SESSION 2025**

Logan Rochard
N° CANDIDAT : 02442782589

Recto

N°	INTITULÉ DE LA RÉALISATION PROFESSIONNELLE
2|2	**Gestion des stratégies de groupe Windows, entretien et support technique**

PÉRIODE DE RÉALISATION	MODALITÉ DE RÉALISATION	LIEU DE RÉALISATION
12-2024	[X] **Autonomie** [ ] **Groupe** [ ] **Mode projet**	Labo informatique **07**

COMPÉTENCES TRAVAILLÉES

[X] **Concevoir une solution d'infrastructure**	[X] **Installer, tester, déployer une solution d'infrastructure**	[X] **Exploiter, dépanner et superviser une solution d'infrastructure**

CONDITIONS DE RÉALISATION (RESSOURCES FOURNIES • RÉSULTATS ATTENDUS)

CONTEXTE GÉNÉRAL : Projet de la **société IGLOONET** fourni par notre professeur et joint en **Annexe 01**.

MÉTHODOLOGIE DE TRAVAIL : Regroupés par 3 étudiants sur un **laboratoire informatique** (schéma topologique joint en **Annexe 02**), notre professeur nous a fixé d'organiser notre travail ainsi :

- **Analyser** le contexte **IGLOONET** et l'expression des besoins en préambule.
- **Travailler**, autant que possible, dans un **mode "orienté projet"** avec, à minima, **l'affectation répartie et synchronisée des tâches** et la **détermination de deadline** (limite) pour chaque tâche.
- S'appuyer sur **une solution de suivi de projet** en ligne (exemple Trello).

OBJECTIFS ET RÉSULTATS ATTENDUS DE LA RÉALISATION :

Les objectifs attendus sont : Comprendre et maîtriser la gestion des stratégies de groupe Windows dans un environnement.
Configurer et appliquer des stratégies adaptées aux besoins d'IGLOONET pour optimiser la gestion des utilisateurs.
Assurer la maintenance et le dépannage des stratégies de groupe afin de garantir un fonctionnement optimal du réseau.
Mettre en place des mécanismes de sécurité et de contrôle des accès via les stratégies de groupe.
Élaborer une documentation détaillée pour assurer la pérennité des configurations et faciliter la prise en main par d'autres administrateurs.

RESSOURCES DOCUMENTAIRES UTILISÉES	RESSOURCES MATÉRIELLES MOBILISÉES	RESSOURCES LOGICIELLES MOBILISÉES
-Documentation UFITECH Performance -Articles techniques sur la gestion des stratégies de groupe	-Serveur Promox avec VM (Windows serveur) -Postes clients Windows 10/11(VM)	-Pack msi -BitLocker -console gpmc -Windows server 2022 -Monitoring des GPO

MODALITÉS D'ACCÈS AUX PRODUCTIONS ET A LEUR DOCUMENTATION

https://loganr06.odoo.com/

Logan Rochard
N° CANDIDAT : 02442782589

DESCRIPTIF DE LA RÉALISATION PROFESSIONNELLE, Y COMPRIS LES PRODUCTIONS RÉALISÉES ET SCHÉMAS EXPLICATIFS

Phase de conception :
Analyser les besoins et les contraintes du projet Igloonet en matière de gestion centralisée des configurations. (Annexe 3)
Rédiger un dossier présentant les choix d'automatisation de la configuration des environnements utilisateur et ordinateur via des stratégies de groupe (GPO), afin de répondre aux besoins actuels d'Igloonet ou d'anticiper ceux à venir. (Annexe 05)
Ce dossier devra notamment aborder les points suivants :

- **Le déploiement de logiciels via des packages MSI (ex. : agent GLPI)**
- **La mise en place de la sécurité, notamment avec BitLocker**
- **La configuration de lecteurs réseaux et de raccourcis sur le bureau**
- **L'utilisation de filtres WMI pour un ciblage précis des GPO**
- **La pertinence et les avantages d'utiliser des objets GPO de type Starter GPO**
-

Jeu de test des stratégies de groupe critiques avant déploiement. (Annexe 06)

Phase de configuration et de déploiement :

- **Mettre en place un serveur Active Directory avec la console de gestion des stratégies de groupe (GPMC).**
- **Configurer des GPO pour les postes utilisateurs et serveurs en fonction des besoins de l'entreprise.**
  - **Sécurité des comptes (mots de passe, verrouillage des sessions, restriction d'accès). (Annexe 05)**
  - **Déterminer un filtre WMI pour toute GPO d'installation de logiciel. (Annexe 05)**
  - **Configuration des paramètres réseau. (Annexe 05)**
  - **Déploiement automatique de logiciels via GPO en lien avec le déploiement d'un GLPI. (Annexe 05)**
- **Tester et valider l'application des stratégies sur différents environnements utilisateurs. (Annexe 06)**
- **Mettre en place un plan de reprise sur incident pour assurer la gestion et la restauration des GPO en cas de panne. (Annexe 06)**
- **Automatiser les sauvegardes et l'exportation des stratégies de groupe. (Annexe 06)**
- **Rédiger la documentation utilisateur sur la gestion et l'administration des GPO. (Annexe 06)**

Phase d'exploitation :

- **Surveiller et analyser l'application des GPO à l'aide des journaux d'événements et d'outils d'audit. (Annexe 07)**
- **Mettre en place des scripts PowerShell pour l'administration avancée et la gestion automatisée des stratégies. (Annexe 08)**
- **Documenter toute modification, incident ou problème rencontré lors de l'exploitation des GPO.**

BILAN DE RÉALISATION • AXES D'ÉVOLUTION | D'AMÉLIORATION

Bilan de réalisation :
Cette réalisation a permis à l'entreprise Igloonet d'avoir un aperçu de tous les équipements connectés à son réseau. Elle a également aidé l'équipe à identifier les pièces à remplacer ou le support à contacter en cas de panne de matériel.
Axe d'amélioration et d'évolution :
• Automatiser par GPO le déploiement de l'agent GLPI sur les postes et les serveurs Igloonet.
• Automatiser la sauvegarde de la base de données MySQL de GLPI.
• Maintenir l'inventaire du parc à jour.
• Établir un rapport à chaque ajout ou retrait d'équipement et le formaliser sous format Excel.

Annexe 1 :

I. Contexte général

La découverte récente d'un virus de type SRAS (Severe Acute Respiratory Syndrome ou Syndrome Respiratoire Aigu Sévère), le SARS-Cov-2, dont la forte propagation en France comme dans de très nombreux pays dans le monde, a créé un contexte pandémique depuis le début de l'année 2020.

Des centaines de milliers de personnes sont contaminées en quelques mois par ce coronavirus (maladie de la Covid-19). Le niveau symptomatique est très varié. Certains cas positifs sont totalement asymptomatiques, d'autres présentent des symptômes bénins mais force est de constater que de nombreux malades développent notamment des complications respiratoires sévères conduisant à leur hospitalisation avec, souvent, un placement en réanimation. Enfin et malheureusement, cette pandémie provoque de très nombreux décès.

a. Contexte sanitaire et dispositions imposées

Cette situation engendre inévitablement de très fortes tensions en milieu hospitalier avec un niveau de saturation rarement atteint. De nombreux états et gouvernements prennent et imposent alors des dispositions drastiques, dont le confinement des populations et la fermeture des commerces, des entreprises, des écoles et des lieux publics, ont été et sont l'un des aspects les plus marquants.

Le monde et ses acteurs font face à un contexte sanitaire, social et économique autant incertain qu'inédit.

b. Conséquences collatérales

Les conséquences d'un tel contexte sont prioritairement d'ordre sanitaire mais impacte fortement l'ordre économique. Les entreprises et les organisations qui le peuvent, envisagent et instaurent massivement le télétravail de leurs collaborateurs. En France notamment, plusieurs observateurs de l'immobilier d'entreprise notent que la répétition des périodes de confinement et la perspective de leur réapparition régulière dans le temps, posent de nouvelles questions stratégiques aux directions générales des entreprises quant à leur politique d'investissement et de gestion de leurs locaux et de leurs bureaux.

Le concept du télétravail, déjà existant mais plutôt marginal, est entré de force dans le mode de fonctionnement des entreprises. Un premier bilan acte qu'il est accepté, qu'il donne des résultats composites mais qui se révèlent néanmoins convenables voir même satisfaisants. Se pose alors mécaniquement la question de l'opportunité de réduire sensiblement les espaces loués et de réexaminer les projets d'extension de nouvelles surfaces locatives.
Il y a donc d'ores et déjà une tension palpable sur le marché de l'immobilier d'entreprises.

c. Opportunités pour Igloonet

C'est ce contexte qui pousse M. Xavier Froid et deux de ses associés, experts et investisseurs immobiliers de profession, à envisager le projet Igloonet.

Ce projet consiste à réaliser justement un investissement immobilier en région parisienne dans des conditions favorables et avantageuses compte tenu des tensions qui se dessinent clairement afin de créer un espace de coworking (espace d'affaires) original qui devra répondre aux nouvelles attentes des entreprises tant au niveau de leur surface d'exploitation que d'une proposition de services intégrés liée aux nouvelles technologies.

Igloonet sera un centre de coworking qui ciblera une clientèle d'entreprises demandeuses de surfaces de bureaux adaptées à des besoins plus restreints et recherchant une infrastructure informatique avancée, évolutive, personnalisée et agile dont elles bénéficieraient comme un service totalement géré.

Pour ce second objectif, Igloonet fonctionnera en quelques sortes comme un datacenter proposant à ses clients de l'IaaS (Infrastructure en tant que Service) avec un mode opérationnel hybride, autrement dit, avec des structures sur site (onpremise) et d'autres à distance (on cloud).

d. Historique

En juin 2020, M. Xavier Froid, Mme Frigide Ere et M. Sam Glace, s'associent et créent à la fois la Société Civile Immobilière (SCI) Igloonet et la Société par Actions simplifiées (SAS) éponyme.

La SCI Igloonet réalise l'acquisition d'un plateau de plein pied d'une surface 2000 m^2 dans le quartier d'affaires de Saint Denis Pleyel.

La SCI Igloonet loue l'intégralité des 2000 m^2 du plateau à la SAS Igloonet qui exploitera l'activité du centre de coworking.

II. L'appel à projet

Pour ce projet, la SAS IglooNet fait un appel concurrentiel à deux ESN (Entreprises de Services du Numérique) afin de répondre au mieux à ses besoins. Les informations fournies à chacune d'elle sont strictement identiques et sont exprimées ci-après :

a. Caractéristiques du plateau

Superficie : 2055 m2
Superficie bureaux : 1 880 m2

- 8 espaces de 40 m2 environ
- 9 espaces de 60 m2 environ
- 6 espaces de 100 m2 environ
- 2 espaces de 200 m2 divisibles en 4 espaces de 45 m2

Espaces communs	: 175 m2 (cuisine, accueil, salle de vie, couloirs…)
Emplacement	: Centre d'affaires de Saint Denis Pleyel (93200)
Niveau(x)	: Plein pied au second étage
Entrée(s)	: 2 entrées principales
Sorties de secours	4
Ascenseurs	2
Toilettes hommes	: 4 au second étage
Toilettes femmes	: 4 au second étage
Installation électrique	: Aux normes et entièrement contrôlée
Câblage réseau	: Oui. Type catégorie 6 FTP (Foiled Twisted Pair)
Prises Ethernet	: 470 (étiquetées et numérotées) - Moyenne : 1 par 4 m2
Brassage	: Oui. 5 baies 19" avec jarretières - Dans local technique de 16 m2

b. Téléphonie
La gestion de la téléphonie IP est exclue du présent appel à projet car elle est prise en charge par un autre prestataire.

c. Espace occupé par la SAS Igloonet
La SAS Igloonet occupera, outre le local technique, un des espaces de 60 m2 mitoyen au local technique.

d. Contraintes liées aux locaux
La SAS Igloonet fixe dans les contrats de location et de services de ses clients une contrainte liée à l'occupation des espaces de travail correspondant à 1 utilisateur par 4 m2 loués avec une tolérance de ± 5%.

e. Type de clients
Les clients de la SAS Igloonet pourront exercer toutes activités licites au regard des lois en vigueur en France et compatibles avec les conditions générales et les conditions détaillées du contrat de location.

Elles seront toutes, avant tout, des entreprises ne possédant pas leur propre système informatique et cherchant à disposer d'une infrastructure informatique réseaux et systèmes en tant que service totalement géré par Igloonet et/ou son prestataire expert habilité.

f. Connexion internet par FAI
La SAS Igloonet a contracté 2 abonnements fibres dédiés à 10Gb symétrique auprès de 2 FAI (Fournisseur d'Accès Internet) distincts, en l'occurrence SFR et ORANGE. En cas de dysfonctionnement, la garantie contractuelle de rétablissement est de 4 heures avec chacun des FAI.
Igloonet possède un pack de 6 adresses IP publiques fixes par FAI.

g. Gestion de projet
Le nom de code du projet est : Igloonet

• Le prestataire ESN retenu sera maitre d'œuvre (MOE) exclusif du projet Igloonet

• Le requérant, maitre d'ouvrage (MOA) seront collectivement M. Xavier Froid, Mme Frigide Ere et M. Sam Glace, associés fondateurs de la SAS Igloonet. Le MOA sera représenté par votre professeur référant.

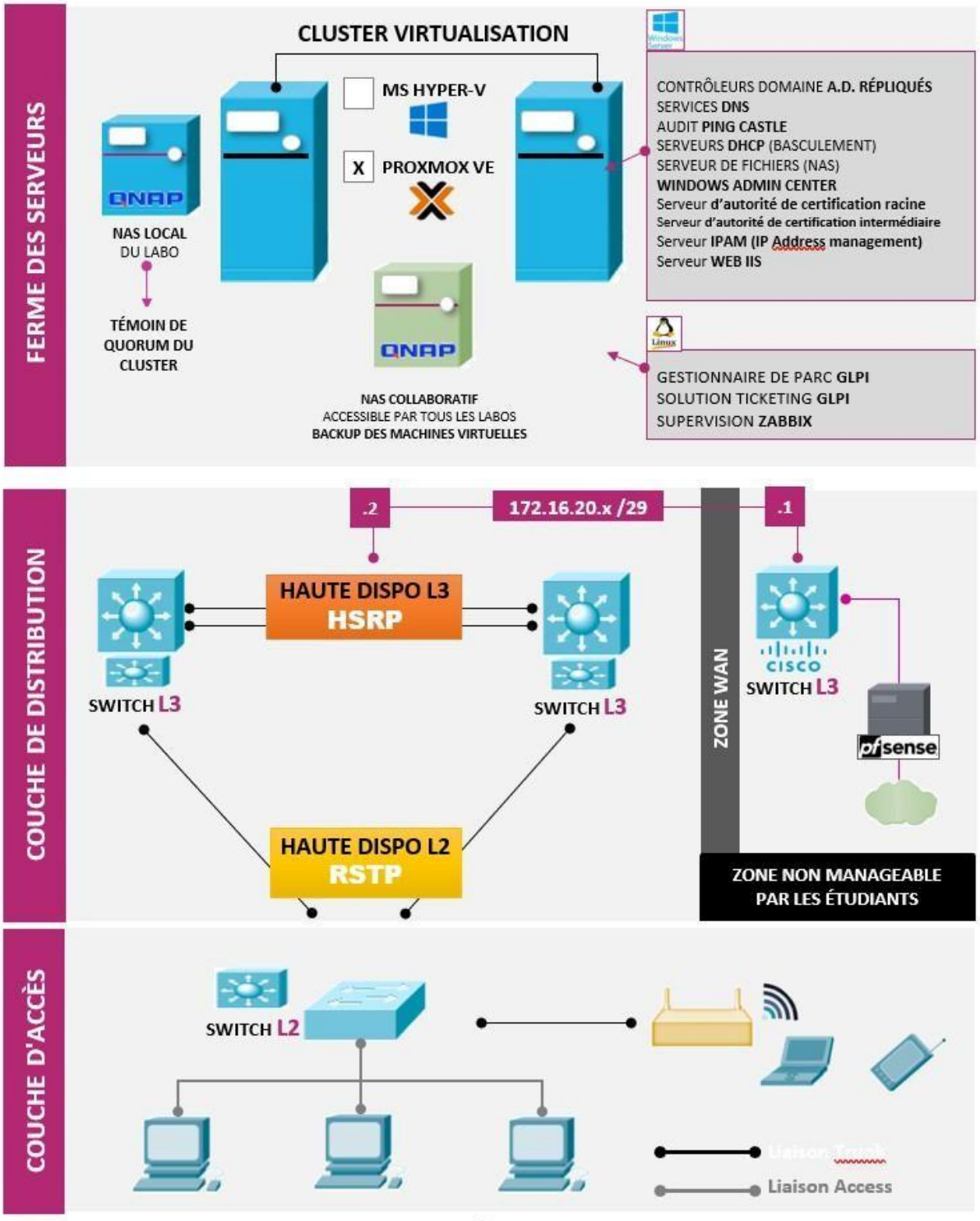
• Des réunions de projet entre le MOA et les membres de l'équipe projet (de manière individuelle ou globale) devront être programmées ainsi que des réunions de projet interne à l'équipe.

III. Expressions des besoins
En liminaire des points détaillés qui suivent, il convient de noter que les axes opérationnels primordiaux que devra intégrer l'infrastructure réseau et système élaborée pour Igloonet à l'attention de ses clients sont :

- La haute disponibilité de l'infrastructure.
- La haute disponibilité des services.
- La sécurisation des données, des accès et des échanges.
- L'archivage des données et des machines virtuelles des clients.
- L'isolation garantie des données et des accès par client.
- Permettre le télétravail en mode sécurisé
- Les performances
- L'agilité à produire à la demande des clients de nouveaux éléments d'infrastructure (commutateurs, machines virtuelles "on premise" ou "on cloud"…) par des outils et des technologies favorisant la méthodologie DevOps.
- L'agilité à faire évoluer à la demande les ressources et les services sollicités et consommés par les clients.
- L'automatisation des tâches d'administration.
- La supervision du système incluant notifications proactives
- Une gestion ITIL des incidents et des demandes d'assistance des clients

RÉALISATIONS PROFESSIONNELLES ■ EPREUVE E6 UFITECH

Annexe 02 **Schéma topologique** **LABO 07**



Plan d'adressage IPv4 • VLSM

VLAN Id	NOM DU VLAN	RÉSEAU IP / MASQUE	1ÈRE ADRESSE DISPONIBLE	DERNIÈRE ADRESSE DISPONIBLE	PASSERELLE SW L3 ACTIF / PASSERELLE SW L3 STANDBY	PASSERELLE HSRP	BROADCAST
200	Serveur	10.0.13.0 / 255.255.255.224	1	31	30 / 29	28	31
210	Infrastructure	10.0.13.32 / 255.255.255.240	33	47	46 / 45	44	47
220	Administration	10.0.13.48 / 255.255.255.240	49	63	62 / 61	60	63
100	Cisco	10.0.13.64 / 255.255.255.240	65	75	78 / 77	76	79
110	Alcatel	10.0.13.80 / 255.255.255.240	81	95	94 / 93	92	95
120	Libre	10.0.13.96 / 255.255.255.240	97	111	110 / 109	108	111
130	Libre bis	10.0.13.112 / 255.255.255.240	113	127	126 / 125	124	127
400	Pôle Communication	10.0.13.128 / 255.255.255.240	129	143	142 / 141	140	143
410	Pôle RH	10.0.13.144 / 255.255.255.240	145	159	158 / 157	156	159
420	Pôle Financier	10.0.13.160 / 255.255.255.240	161	175	174 / 173	172	175
430	Pôle Direction/ Gestion	10.0.13.176 / 255.255.255.240	177	191	190 / 189	188	191
230	Réplication	10.0.13.192 / 255.255.255.248	193	199	198 / 197	196	199
240	Backup	10.0.13.200 / 255.255.255.248	201	207	206 / 205	204	207
300	Télécommunication	10.0.13.208 / 255.255.255.248	209	215	214 / 213	212	215
310	Imprimantes	10.0.13.2016 / 255.255.255.248	217	223	222 / 221	220	223
10	Visiteur	10.0.13.224 / 255.255.255.248	225	231	230 / 229	228	231

Logan Rochard
N° CANDIDAT : 02442782589

Annexe 3 :

Dans le cadre des cours en laboratoire, le projet Igloonet vise à mettre en place une infrastructure sécurisée en s'appuyant sur les stratégies de groupe (GPO) sous Windows Server 2022.
L'objectif est de comprendre et appliquer les principes de gestion des GPO pour optimiser la configuration des postes et la sécurité du réseau. Nous allons voir les besoins pour notre réalisation.

Définition des GPO

- Une Stratégie de Groupe (GPO - Group Policy Object) est un ensemble de règles permettant d'administrer et de configurer de manière centralisée les postes et utilisateurs d'un domaine Windows.
- Les GPO sont appliquées via Active Directory et permettent de contrôler divers paramètres système, comme la sécurité, les restrictions d'accès, les configurations réseau et les logiciels installés.
- Elles facilitent la gestion des infrastructures informatiques en automatisant les configurations et en assurant une uniformité sur l'ensemble des postes utilisateurs.

Les rôles des GPO

Un environnement Active Directory utilise les GPO pour organiser et sécuriser les postes et utilisateurs grâce à différents types de stratégies :

- **GPO utilisateur** :
    - Applique des restrictions spécifiques aux utilisateurs.
    - Définit les paramètres des sessions, comme les scripts de connexion et les restrictions logicielles.
    - Gère les paramètres du bureau, des imprimantes et des profils itinérants.
- **GPO ordinateur** :
    - Configure les paramètres système des machines du réseau.
    - Applique des stratégies de sécurité avancées comme le verrouillage des sessions et les mises à jour automatiques.
    - Définit les configurations réseau et les paramètres des services Windows.

Remarque : Une GPO peut être appliquée à différents niveaux (site, domaine, unité d'organisation) et peut être héritée ou remplacée en fonction des priorités définies.

Les services et les configurations

Une GPO permet d'appliquer des services et configurations spécifiques :

- **Sécurité et authentification** : gestion des mots de passe, verrouillage des comptes, restrictions d'accès aux fichiers et aux applications.
- **Déploiement de logiciels** : installation automatique de programmes sur les postes clients.
- **Configuration du réseau** : attribution des paramètres IP, proxy et accès aux ressources partagées.
- **Maintenance et mises à jour** : application automatique des correctifs et des politiques de sauvegarde.

Réseau et communication

Les GPO facilitent la gestion réseau en permettant :

- **Le contrôle des connexions** : configuration des VPN, des partages réseau et des droits d'accès.
- **La sécurisation des postes** : restriction des accès non autorisés et configuration des pare-feu Windows.
- **La gestion des sessions** : limitation des temps de connexion et application des restrictions de bureau à distance.

Tolérance aux erreurs et scalabilité

- Si une GPO est corrompue ou mal appliquée, il est possible de restaurer les stratégies précédentes via les sauvegardes Active Directory.
- Une GPO peut être modifiée ou remplacée dynamiquement pour s'adapter aux nouvelles exigences du réseau.
- L'ajout ou le retrait d'utilisateurs/machines à une unité d'organisation applique automatiquement les GPO correspondantes sans intervention manuelle.

Besoins identifiés

- L'environnement de travail.
- Appliquer des restrictions et sécuriser l'accès aux postes.
- Automatiser l'installation des logiciels et des configurations réseau.
- Mettre en place une gestion centralisée des droits et accès.
- Assurer la sauvegarde et la restauration des configurations.

Contraintes techniques

- Utilisation d'un Active Directory en laboratoire.
- Compatibilité avec les versions Windows (10, 11, Server 2022).
- Respect des bonnes pratiques en matière de sécurité (RGPD).
- Planification des tests pour éviter les conflits.

Recommandations

- Analyser l'Active Directory existant.
- Structurer les Unités d'Organisation (OU) pour les tests.
- Prioriser les GPO essentielles à la sécurité et à l'organisation.
- Tester les configurations avant déploiement global.

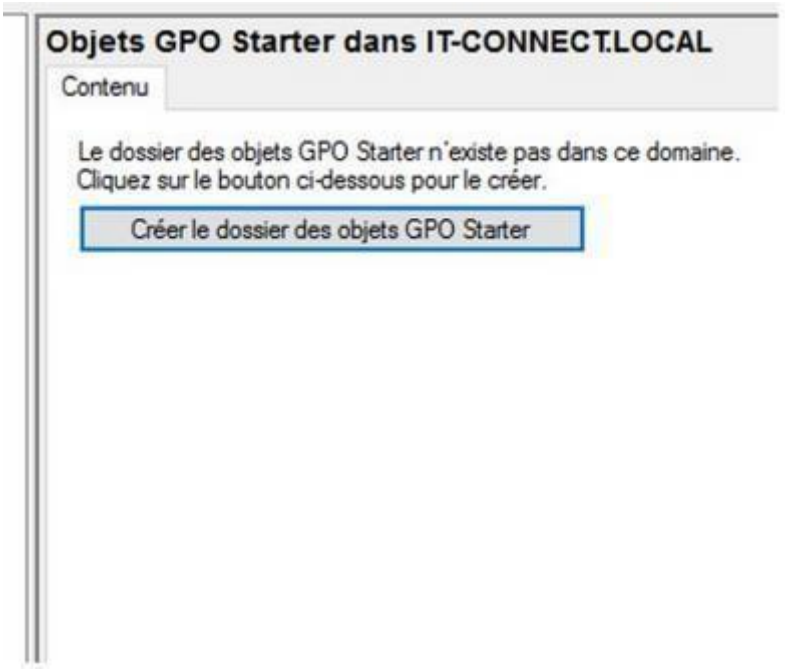
Annexe 4 :

I. Configurer des GPO pour les postes utilisateurs et serveurs en fonction des besoins de l'entreprise

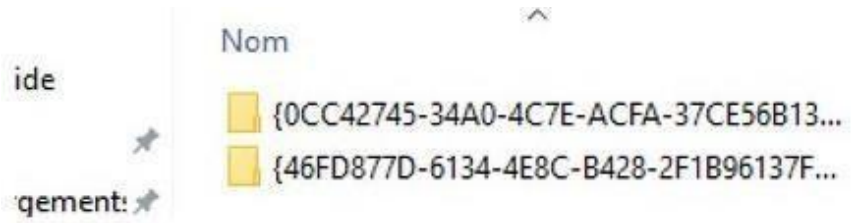
Dans ce contexte, je vais configurer une stratégie de groupe adaptées (intégrant un objet GPO Stater) aux postes utilisateurs, en appliquant des règles de sécurité.

a. Créer une GPO Starter

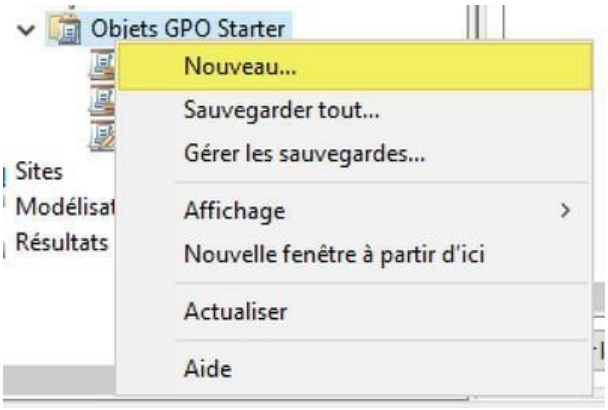
À l'aide de la console GPMC, on retrouve ces GPO sous le nom "**Objets GPO Starter**". De base, il faut initialiser les GPO Starter, il suffit de cliquer sur le bouton "**Créer le dossier des objets GPO Starter**".



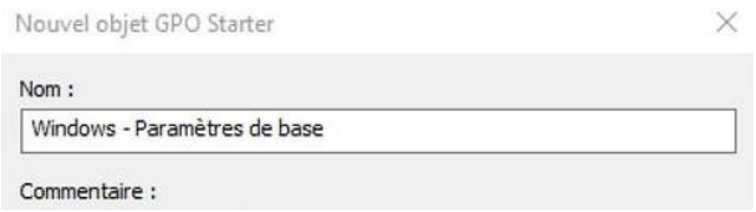
Concrètement, cela va générer un nouveau dossier au sein du SYSVOL de votre domaine :



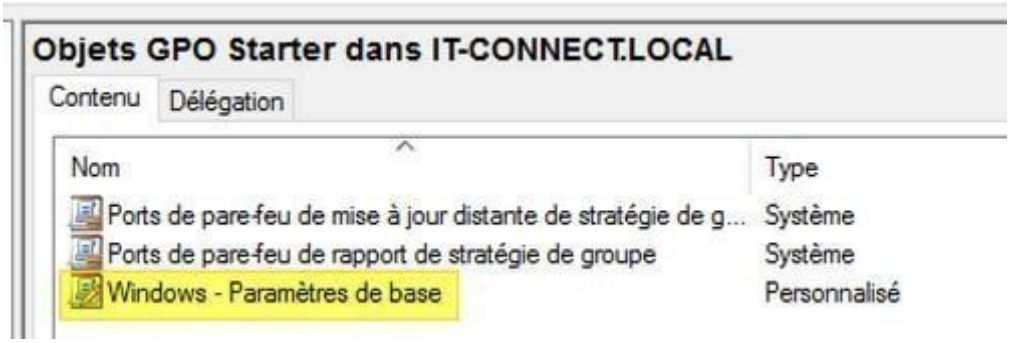
Ensuite, pour créer une nouvelle GPO Starter, il faudra faire: un clic droit sur "**Objets GPO Starter**" puis "**Nouveau**" pour ouvrir la fenêtre de création.



Donnez un nom à votre objet et pensez à indiquer un commentaire, puis validez.
La GPO va ensuite être listée dans la liste des GPO Starter.



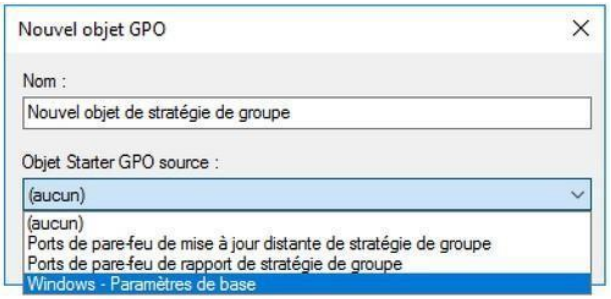
La GPO apparaît bien dans la liste.



Maintenant, il ne reste plus qu'à modifier cette GPO Starter et à la configurer comme n'importe quelle autre GPO. Néanmoins, les GPO Starter ne permettent pas de définir des paramètres de type "Préférences".

b. Créer une GPO à partir d'une GPO Starter

Si vous créez une GPO (classique) via la console GPMC, vous verrez qu'il y a l'option "**Objet Starter GPO source**" et que dans **la liste déroulante on retrouve bien la GPO Starter que l'on vient de créer.** Il suffit de la choisir et de valider.



Annexe 5 :

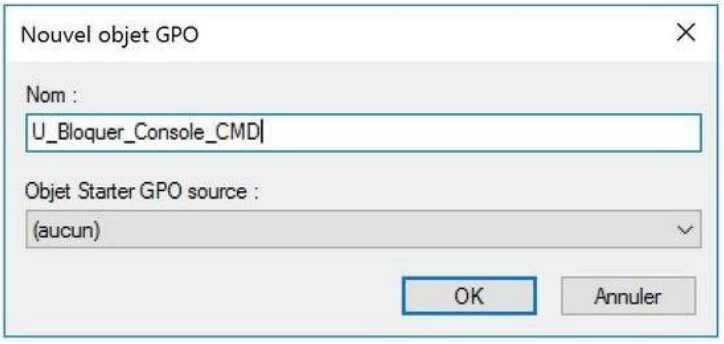
II. Créer une stratégie de groupe

Sur votre contrôleur de domaine, ouvrez la console GPMC.

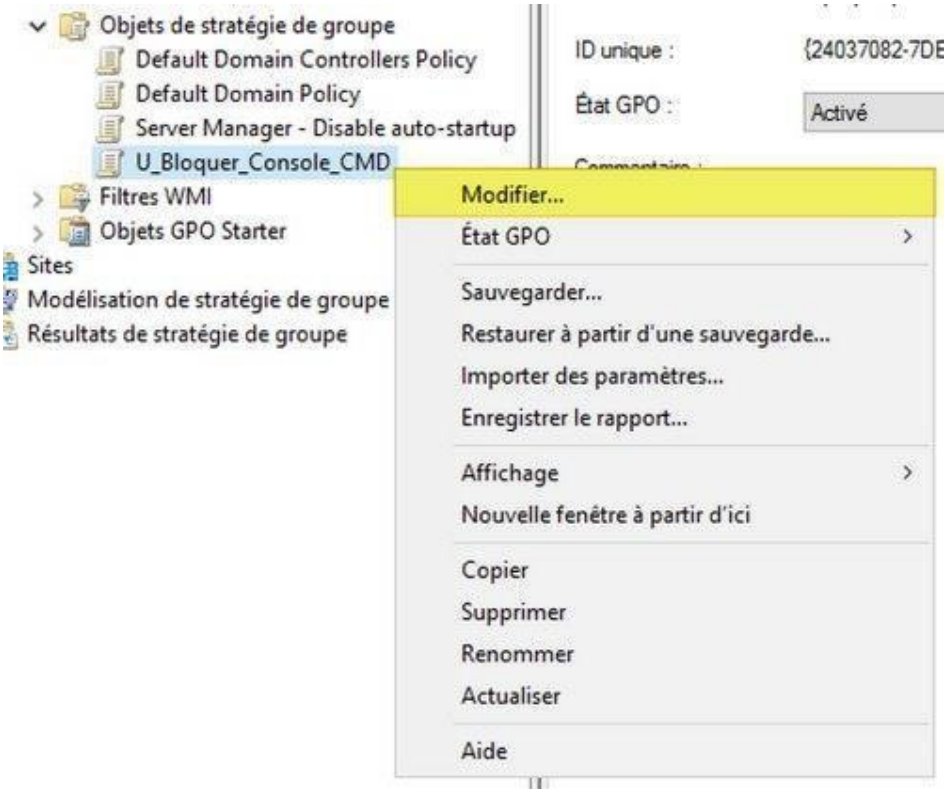
Sur "**Objets de stratégie de groupe**", effectuez un clic droit et cliquez sur "**Nouveau**".

Dans cet exemple, je vous propose de créer une stratégie de groupe pour bloquer l'utilisation de l'Invite de commande (*console cmd*) dans certaines sessions utilisateurs. Cette action simple est très répandue en entreprise.

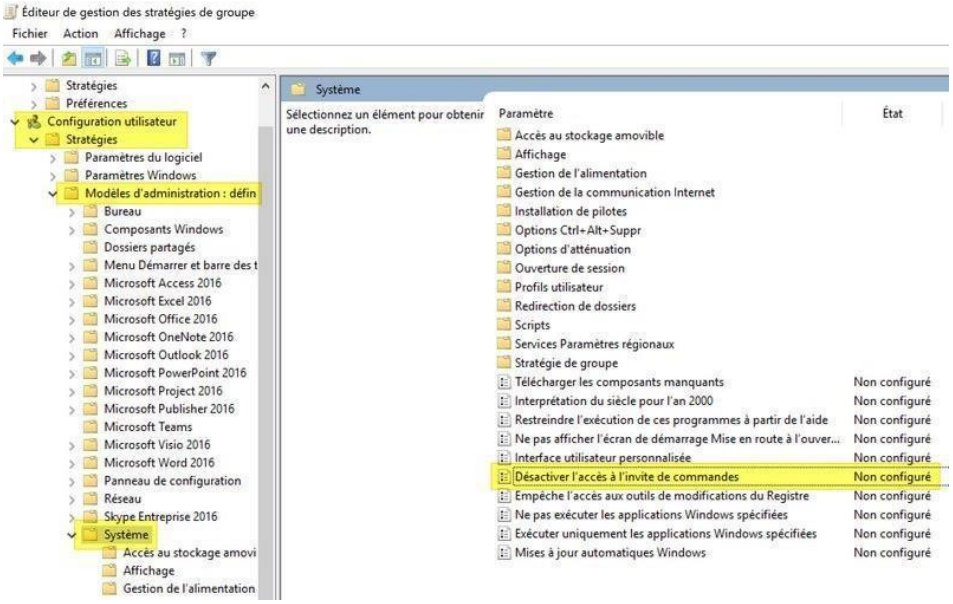
Indiquez un nom pour cette GPO, par exemple "*U_Bloquer_Console_CMD*" mais vous pouvez mettre ce que vous voulez. Le "U" étant là en préfixe pour indiquer qu'il s'agit d'une GPO qui va agir au niveau Utilisateur. Cliquez sur "OK" pour valider.



La GPO va s'afficher dans la liste, effectuez un clic droit dessus pour "*Modifier*".



Une fenêtre "**Éditeur de gestion des stratégies de groupe**" va s'ouvrir, cela permet de configurer la GPO. Autrement dit, c'est ici que l'on va activer ou configurer certains paramètres à appliquer sur les utilisateurs (ou les ordinateurs). L'objectif maintenant va être de trouver le paramètre qui permet de désactiver l'accès à l'invite de commandes. Voici le chemin vers notre fameux paramètre : **Configuration utilisateur > Stratégies > Modèles d'administration > Système > Désactiver l'accès à l'invite de commandes**. Double-cliquez dessus.

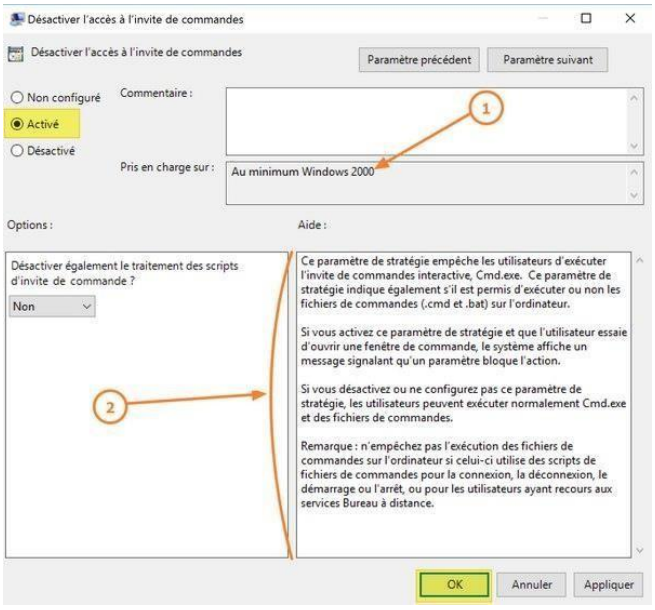


Les fenêtres de configuration sont présentées de la même façon pour la majorité des paramètres. Nous retrouvons tout d'abord dans le haut, deux boutons : "*Paramètre précédent*" et "*Paramètre suivant*" pour naviguer entre les paramètres sans fermer et rouvrir une nouvelle fenêtre.

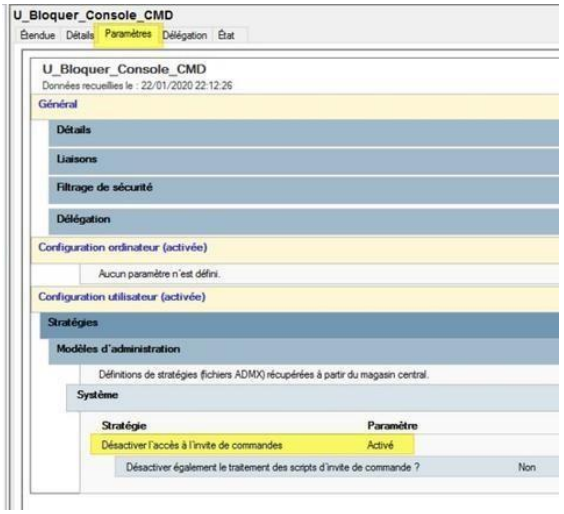
Nous avons également le champ "**Pris en charge sur :**" qui donne des indications (plus ou moins précises) sur la compatibilité de ce paramètre avec les différentes versions de Windows .

Juste à gauche, nous avons trois boutons, que vous retrouverez sur tous les paramètres que l'on pourrait qualifié de "booléen" : **soit on active, soit on désactive, ou alors on ne configure pas et dans ce cas c'est le paramétrage par défaut de Windows qui s'appliquera** (à moins que ce paramètre soit géré dans une autre GPO).

Enfin, certains paramètres proposent des options. C'est le cas de celui-ci. Si vous activez ce paramètre, il ne sera pas possible d'utiliser la console CMD avec les comptes utilisateurs ciblés. Néanmoins, l'option "**Désactiver également le traitement des scripts d'invite de commande**" est intéressante puisqu'elle permet (lorsqu'elle est définie sur "Non") d'autoriser l'exécution des scripts CMD.
Par exemple : si vos utilisateurs doivent exécuter un script de connexion qui va monter des lecteurs réseau, il ne faudra pas désactiver cette option.
Concernant, notre configuration, activez ce paramètre et validez.

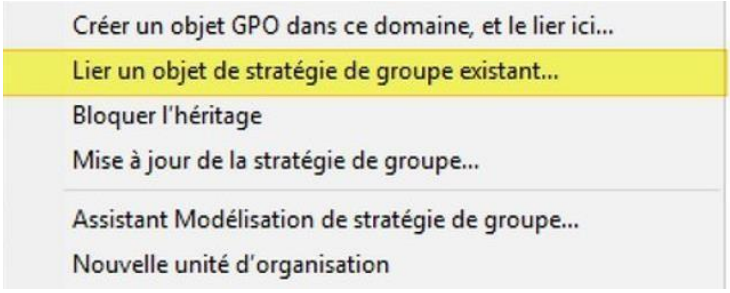


Vous pouvez fermer ensuite la console de modification de cette GPO.
Vous revoilà dans la console GPMC : cliquez sur la GPO "U_Bloquer_Console_CMD", puis sur la droite cliquez sur l'onglet "Paramètres". **Déroulez ensuite sous "Configuration utilisateur", vous verrez que cela offre la possibilité de voir rapidement la configuration contenue dans cette GPO.**

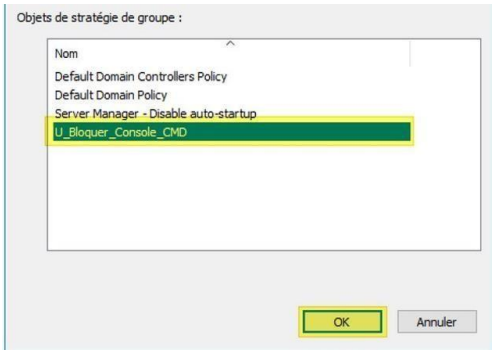


II. Créer une liaison

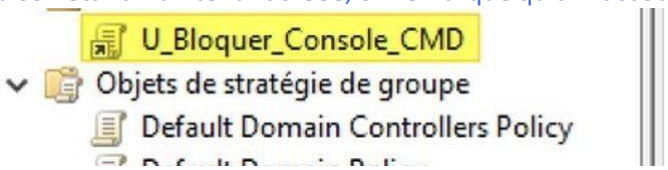
En l'état, notre stratégie de groupe ne sert à rien puisqu'elle s'applique sur aucun objet. Il va falloir la positionner au niveau de l'annuaire Active Directory : soit sur le domaine pour bloquer CMD dans toutes les sessions (pas top pour les sessions Administrateurs), soit sur une ou plusieurs OU spécifiques.
Il y a plusieurs méthodes pour créer une liaison, un simple glisser-déposer pourrait fonctionner aussi.



La liste des GPO de notre domaine va s'afficher, avec un classement par ordre alphabétique. Sélectionnez la GPO "U_Bloquer_Console_CMD" et cliquez sur "OK".



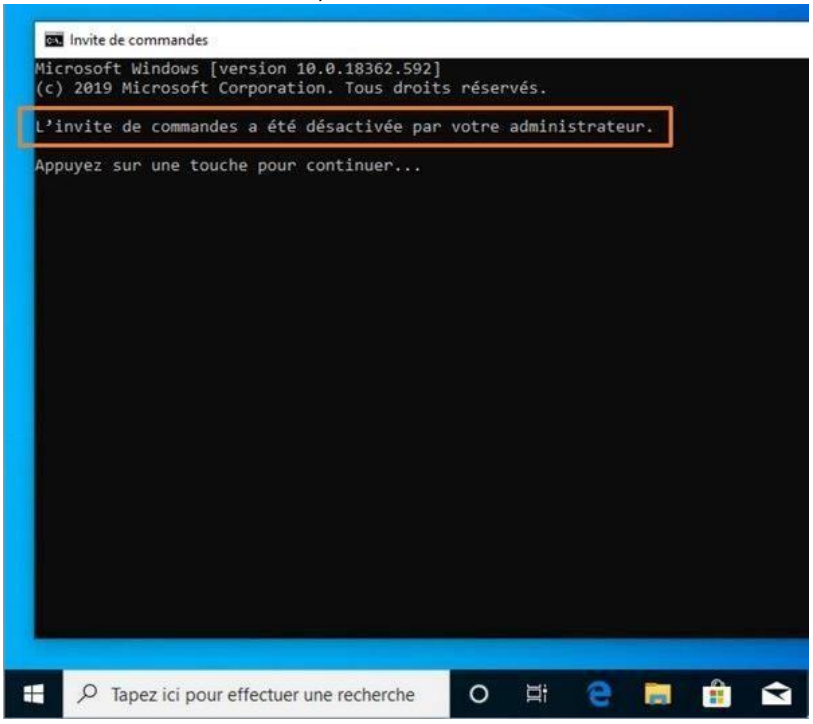
La liaison étant maintenant créée, on remarque qu'un raccourci s'est ajouté.



III. Tester la GPO

Sur un poste qui est dans le domaine, nous allons ouvrir une session d'un utilisateur dont le compte se situe dans l'OU ou je l'ai mise.

Une fois la session ouverte, il faut lancer une invite de commandes.



Conclusion : notre stratégie de groupe fonctionne bien !

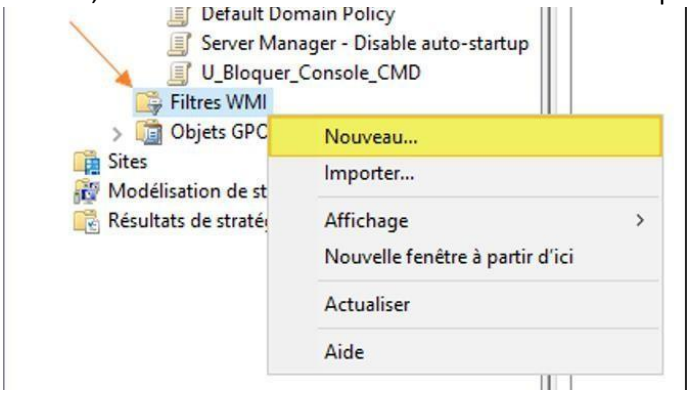
Il s'agissait de la première fois où cet utilisateur ouvrait la session sur ce poste de travail. Dans le cas où la session existerai déjà, il se peut que la GPO ne s'applique pas immédiatement. Il existe un temps de rafraîchissement pour les stratégies de groupe, ce qui est d'autant plus vrai pour les stratégies d'ordinateurs qui s'appliquent généralement au démarrage de la machine.

Pour forcer l'actualisation des stratégies de groupe sur un poste, que ce soit pour les paramètres ordinateurs ou utilisateurs, il y a une commande magique et qu'il est indispensable de connaître : gpupdate /force

II. Où créer un filtre WMI pour une GPO ?

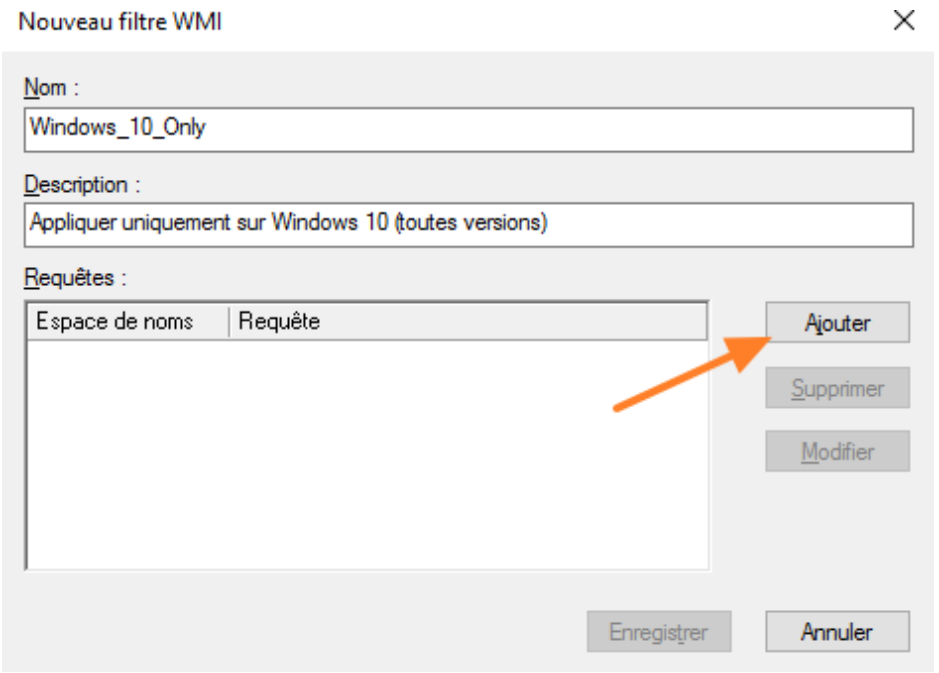
La première question que l'on se pose c'est : où est-ce que je vais pouvoir créer le filtre WMI ? Pour cela, rendez-vous dans la console GPMC (*Éditeur de stratégie de groupe*).

Ensuite, effectuez un clic droit sous "**Filtres WMI**" et cliquez sur "**Nouveau**".

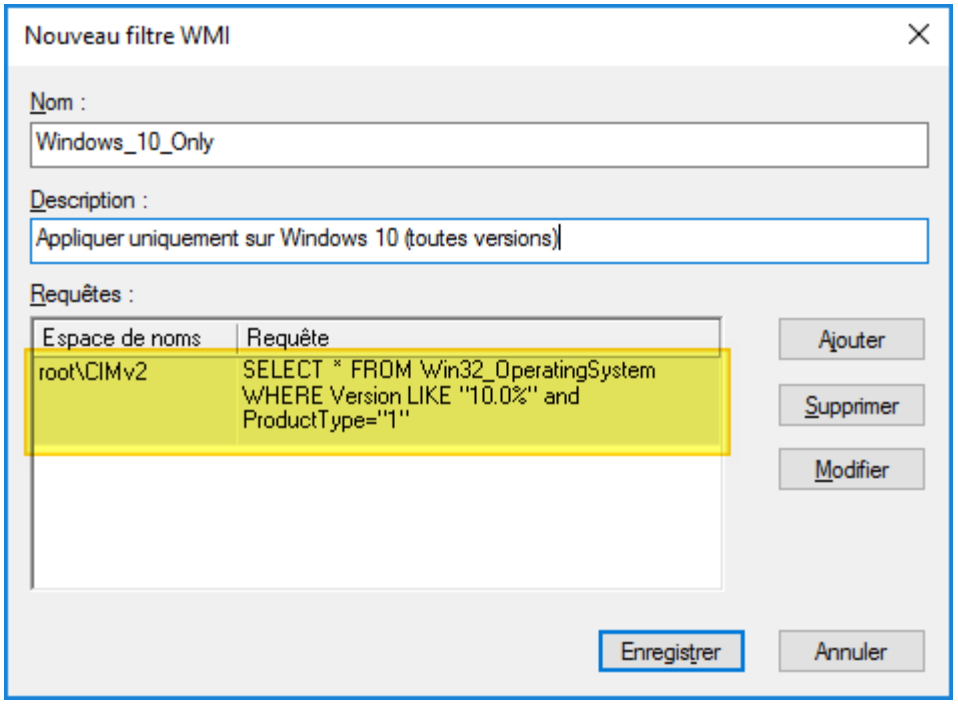


III. Filtre WMI pour cibler un système d'exploitation

Pour commencer, nous allons créer un filtre WMI qui va permettre de cibler une version spécifique de Windows, par exemple **cibler uniquement les postes sous Windows 10.**
Pour cibler une version précise de Windows, nous avons besoin de connaître son numéro de version.



La première chose consiste à définir l'espace de noms, mais pour la majorité des cas il n'est pas utile de changer la valeur par défaut : **root\CIMv2**.



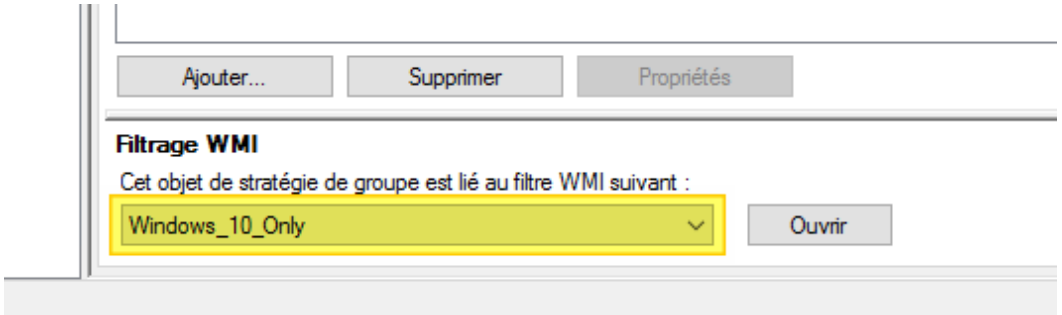
Pour tous les pc windows 10 la commande sera : SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0%" AND ProductType="1" .

Il ne reste plus qu'à voir comment l'associer à une GPO.

IV. Associer un filtre WMI à une GPO

Un filtre WMI ne s'applique à une GPO que lorsqu'il y a une liaison entre les deux. Pour réaliser cette opération, dans la console GPMC, cliquez sur votre GPO. Ensuite, vérifiez que vous êtes bien sur l'onglet "Étendue".

Dans le bas de la fenêtre, vous devriez voir la zone "*Filtrage WMI*". Grâce à la liste déroulante, sélectionnez votre filtre WMI et cliquez sur "Oui" sur la fenêtre qui s'affiche pour valider.

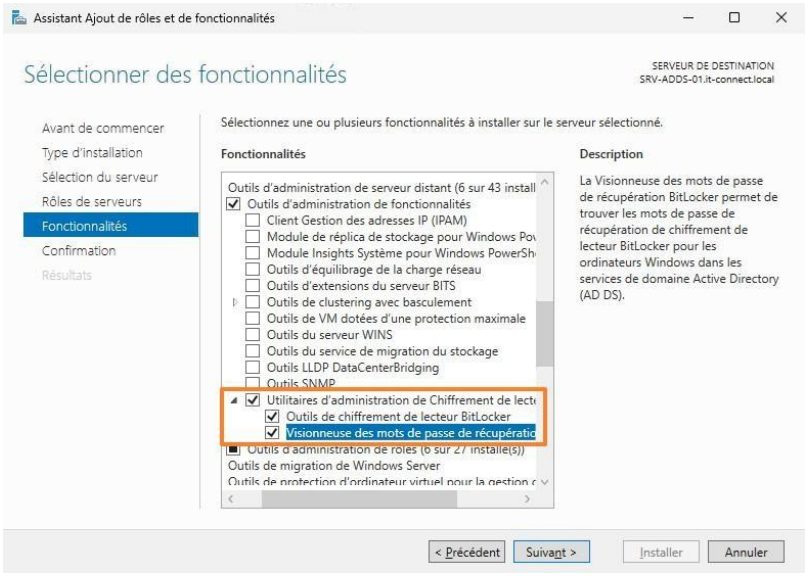


Annexe 6

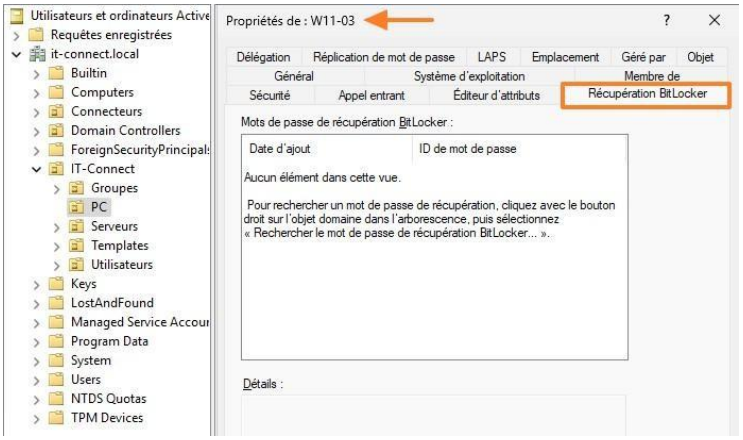
I. Configuration Bitlocker

a. Stocker les clés de récupération BitLocker dans l'Active Directory

Installation de nouvelles fonctionnalités.

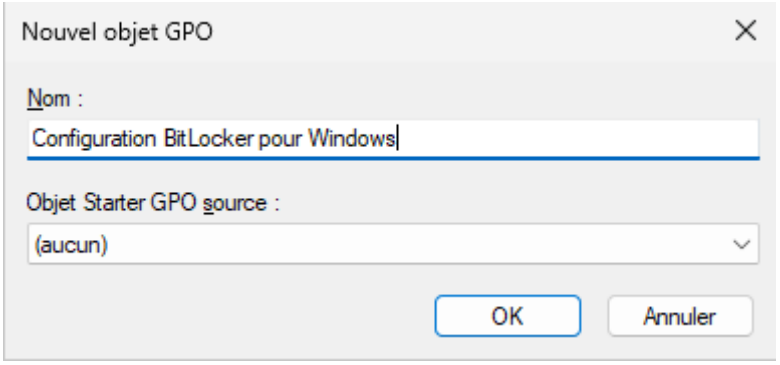


Désormais, si vous ouvrez la console "Utilisateurs et ordinateurs Active Directory", vous allez avoir du nouveau. Accédez aux propriétés d'un objet "Ordinateur" de votre annuaire et vous verrez un nouvel onglet : "Récupération BitLocker". C'est au sein de cet onglet que l'ordinateur viendra stocker son identifiant et la clé de récupération BitLocker associée. De cette façon, vous centralisez les clés de récupération BitLocker dans votre annuaire Active Directory.



II. GPO pour configurer BitLocker sur Windows

Toujours sur le contrôleur de domaine, ouvrez la console "Gestion de stratégie de groupe". Créez une nouvelle GPO et donnez-lui un nom, par exemple "Configuration BitLocker pour Windows".

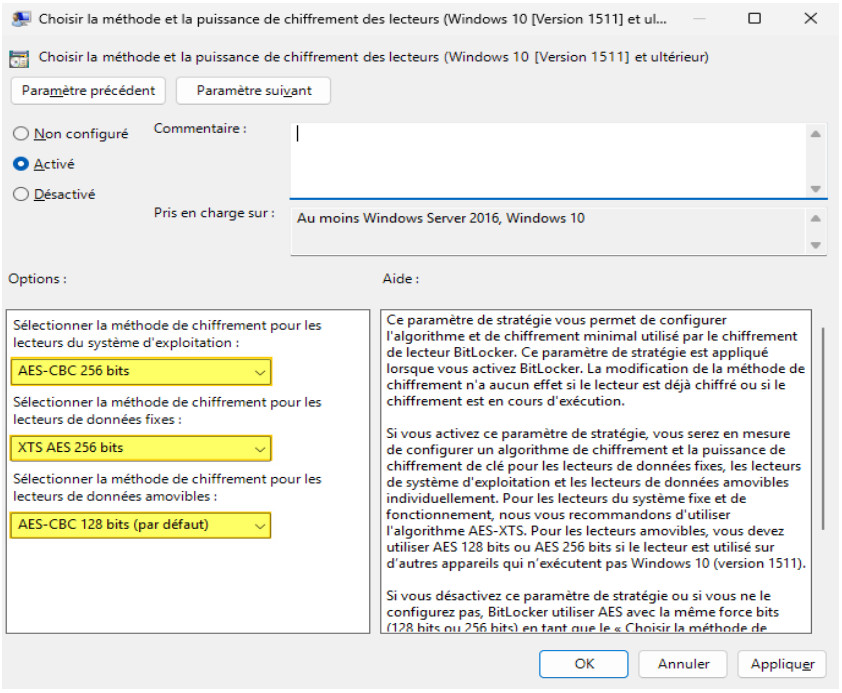


Lier cette GPO à une OU de test.

Commençons par le premier paramètre nommé "Choisir la méthode et la puissance de chiffrement des lecteurs)". Il sert à spécifier les méthodes de chiffrement à utiliser en fonction du type de lecteurs.

À ce sujet, Microsoft recommande d'utiliser l'algorithme XTS-AES pour les lecteurs fixes et les lecteurs de systèmes d'exploitation. Pour les disques amovibles, Microsoft recommande d'utiliser l'algorithme AES-CBC 128 bits ou AES-CBC 256 bits, si le disque est utilisé sur d'autres appareils qui ne fonctionnent pas sous Windows 10 (version 1511). Le fait de configurer les algorithmes ici va permettre d'uniformiser la configuration sur les postes.

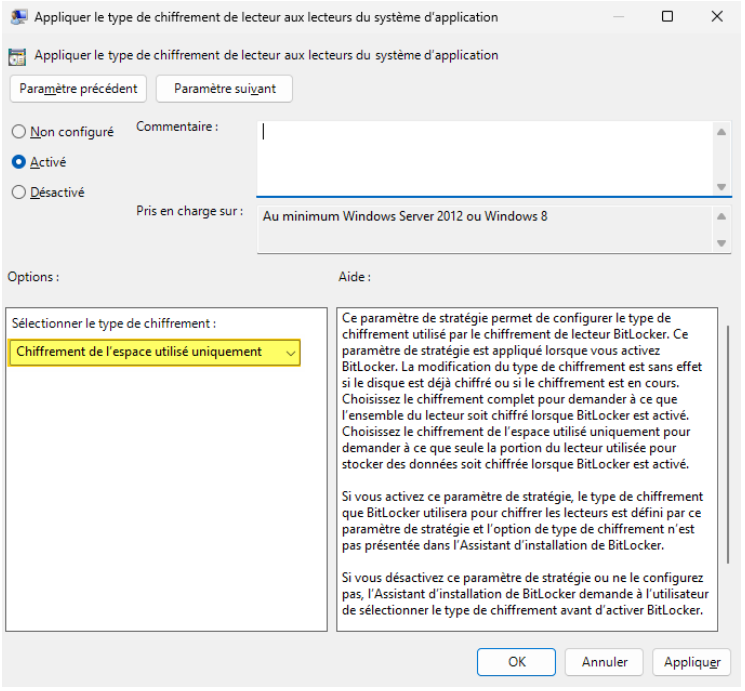
Voici la configuration de ce premier paramètre situé directement dans le dossier "Chiffrement de lecteur BitLocker" :



B. Paramètre n°2 - Appliquer le type de chiffrement de lecteur aux lecteurs du système d'application

Le second paramètre se situe dans "Lecteurs du système d'exploitation", comme ceux qui suivront après. Il se nomme : "Appliquer le type de chiffrement de lecteur aux lecteurs du système d'application" et permet d'indiquer comment BitLocker doit chiffrer le disque : tout le disque ou uniquement le contenu au fur et à mesure.

Activez ce paramètre et choisissez l'option "Chiffrement de l'espace utilisé uniquement", ce sera plus rapide sur les machines déjà en service depuis un moment, où le stockage est déjà sollicité

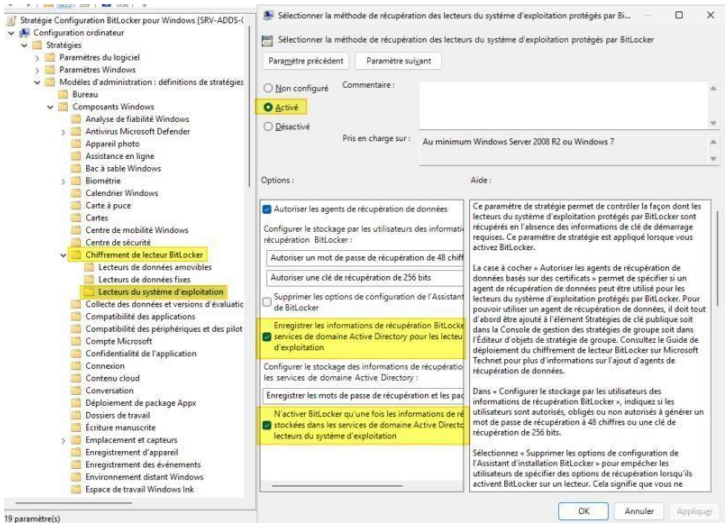


C. Paramètre n°3 - Sélectionner la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker

Le troisième paramètre à configurer se nomme : "Sélectionner la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker". Il va permettre d'indiquer aux postes qu'ils doivent sauvegarder leur clé de récupération dans l'Active Directory et de vérifier que la clé est bien sauvegardée dans l'annuaire AD avant de commencer à chiffrer le poste.

Activez ce paramètre, et veillez à ce que les deux options suivantes soient cochées (laissez les autres options par défaut) :

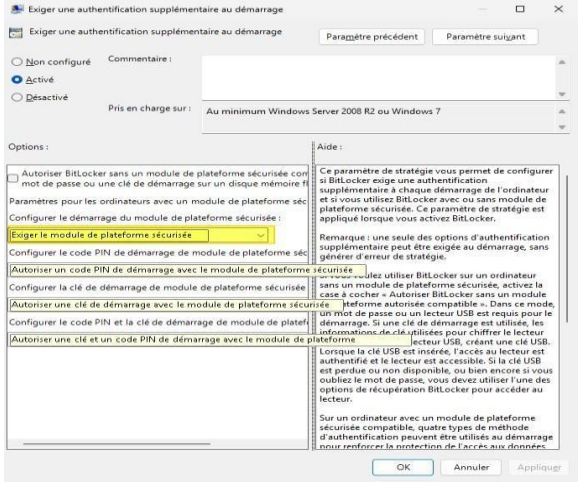
- **Enregistrer les informations de récupération de BitLocker dans les services de domaine Active Directory pour les lecteurs du système d'exploitation**
- **N'activer BitLocker qu'une fois les informations de récupération stockées dans les services de domaine Active Directory pour les lecteurs du système d'exploitation**



D. Paramètre n°4 - Exiger une authentification supplémentaire au démarrage

Le quatrième et dernier paramètre que nous allons configurer se nomme : "Exiger une authentification supplémentaire au démarrage". Sa configuration est facultative si vos machines ont une puce TPM. Sinon, configurez ce paramètre pour cocher la première option puisqu'elle permet d'activer BitLocker sans qu'il y ait de puce TPM (ce qui implique de définir un mot de passe ou une clé USB de démarrage).

Vous pouvez aussi le configurer pour exiger la présence de la puce TPM, en choisissant la valeur "Exiger le module de plateforme sécurisée", tel que présenté sur l'image ci-dessous.



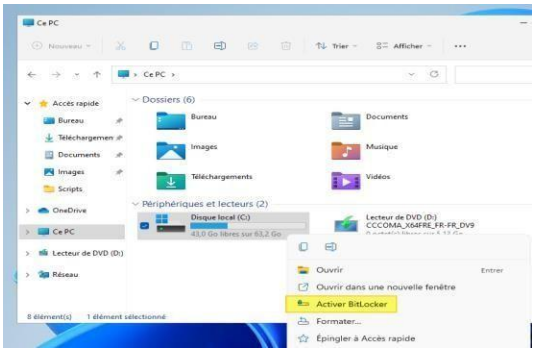
E. La GPO BitLocker est prête

La GPO pour configurer BitLocker est prête. Attention, cela ne va pas activer le chiffrement sur le disque système de vos postes. Par contre, BitLocker sera préconfiguré et prêt à être activé, en quelques clics. Nous allons voir dans la suite de cet article comment activer le chiffrement BitLocker via une GPO et un script PowerShell.

Pour le moment, nous allons tester notre GPO et la collecte des clés de récupération dans l'Active Directory.

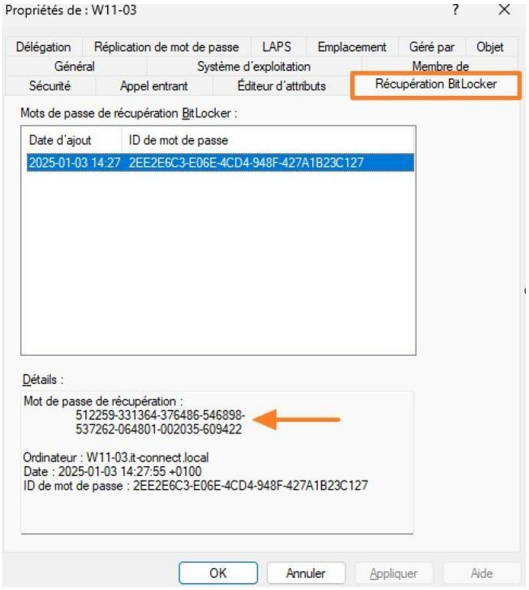
IV. Activer le chiffrement BitLocker sur Windows

Sur un poste client sur lequel s'applique la GPO, vous devez activer le chiffrement BitLocker sur le disque système pour voir ce qui se passe. Si vous utilisez Windows 11 24H2, vous n'aurez pas besoin d'effectuer cette action, car BitLocker est préactivé : la GPO créée précédemment est suffisante, ce qui facilite le travail de l'administrateur système.



Une fois le chiffrement démarré, retournez dans la console "Utilisateurs et ordinateurs Active Directory", accédez aux propriétés de l'ordinateur sur lequel vous venez d'activer le chiffrement et cliquez sur l'onglet "Récupération BitLocker".

Vous devez avoir une bonne surprise et visualiser la clé de récupération (champ "Mot de passe de récupération"), comme dans cet exemple :



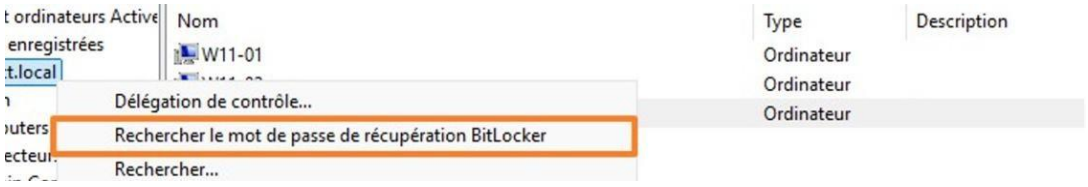
Notre configuration fonctionne très bien : les clés de récupération de nos postes seront centralisées dans l'Active Directory. Si un utilisateur vous appelle, car il a besoin de la clé de récupération, il suffira de se référer à l'Active Directory pour trouver l'information.

Si la configuration est régénérée sur le poste, une nouvelle clé de récupération sera générée. Elle viendra automatiquement s'ajouter dans l'Active Directory à la suite, sans supprimer les références de l'ancienne clé.

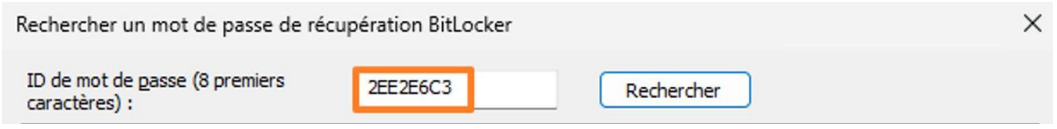
V. Comment retrouver une clé de récupération BitLocker ?

Dans le cas où un utilisateur est bloqué ou que vous n'avez pas le nom de la machine, retrouver la clé de récupération dans l'annuaire AD pourrait devenir un vrai casse-tête. Heureusement, grâce aux outils installés au début du tutoriel, nous pouvons rechercher une clé de récupération à partir des 8 premiers caractères de l'identifiant de l'ordinateur.

Toujours dans la console "Utilisateurs et ordinateurs Active Directory", effectuez un clic droit sur le nom de votre domaine et cliquez sur "Rechercher le mot de passe de récupération BitLocker".



Saisissez les 8 premiers caractères de l'identifiant du poste et cliquez sur "Rechercher".



VI. GPO - Script pour activer BitLocker sur plusieurs postes Windows

Nous allons voir créer une GPO qui va permettre d'activer BitLocker sur la partition système des postes Windows. Cela va éviter de devoir configurer les postes à la main.

Pour automatiser l'activation de BitLocker, nous allons utiliser le module PowerShell "BitLocker" qui est intégré à Windows et qui est plus dans l'air du temps que l'outil manage-bde.

A. Configurer BitLocker avec PowerShell

Lorsqu'un disque est protégé par BitLocker le statut est "FullyEncrypted", alors qu'à l'inverse le statut est "FullyDecrypted" si le disque n'est pas chiffré.

Si votre machine dispose d'un module TPM,il faudra utiliser cette commande :

```
Add-BitLockerKeyProtector -MountPoint $env:SystemDrive -TpmProtector
```

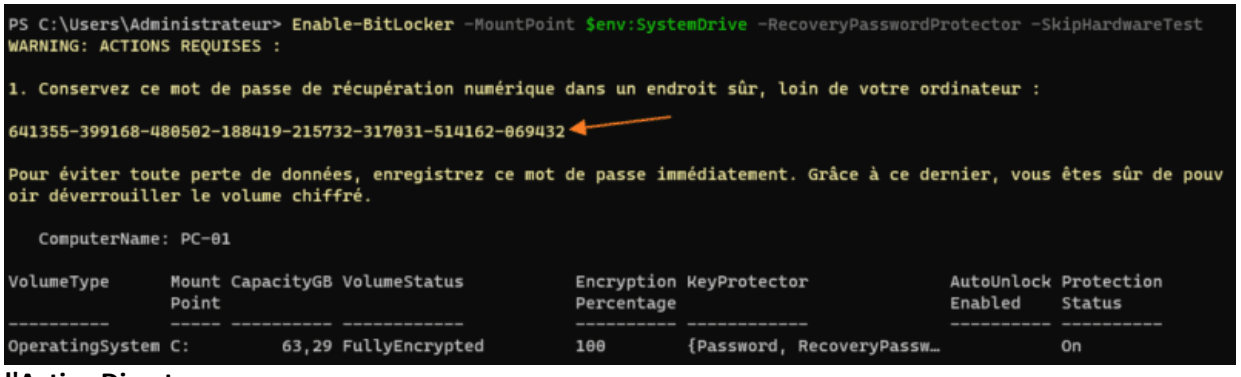
Sinon :

```
$BitLockerPwd = ConvertTo-SecureString "bonjour123" -AsPlainText -Force
Add-BitLockerKeyProtector -MountPoint $env:SystemDrive -PasswordProtector -Password $BitLockerPwd
```

Quand c'est fait, vous devez activer BitLocker sur la partition système grâce à la commande "Enable-BitLocker". Si vous souhaitez que le matériel soit vérifié avant que BitLocker commence à chiffrer, supprimez le paramètre "-SkipHardwareTest" de la commande ci-dessous. Cela implique qu'il faudra redémarrer, et que si tout est correct, alors le chiffrement BitLocker débutera.

```
Enable-BitLocker -MountPoint $env:SystemDrive -RecoveryPasswordProtector -SkipHardwareTest
```

Cette commande retourne la clé de récupération dans la sortie et c'est aussi cette clé que vous allez retrouver dans l'Active Directory :



Annexe 7

I. Jeu de test

N°	Titre	Description	Input	Résultat attendu
1	Blocage de l'invite de commandes	Vérifie si l'accès à CMD est bloqué	Lancer `cmd.exe`	Message de restriction / blocage complet
2	Application du filtre WMI	Vérifie si la GPO ne s'applique que sur des machines ciblées	Machine qui ne correspond pas au filtre	La GPO ne s'applique pas
3	Mise à jour automatique activée	Vérifie si Windows Update s'exécute automatiquement	`gpupdate /force` + `wuauclt /detectnow`	Téléchargement planifié automatique
4	Politique de verrouillage de compte	Vérifie le verrouillage du compte après plusieurs tentatives échouées	5 échecs de connexion	Compte verrouillé temporairement
5	Installation automatique GLPI Agent	Vérifie si l'agent GLPI est installé via le fichier MSI de la GPO	Redémarrer / forcer la GPO	Agent GLPI présent dans les programmes installés
6	Politique de mot de passe	Vérifie si le mot de passe respecte les règles définies	Créer un mot de passe faible / inchangé pendant >100 jours	Rejet du mot de passe faible / expiration à 100 jours
7	Montage lecteur réseau "partage"	Vérifie si le lecteur réseau est automatiquement monté	Se connecter à une session utilisateur	Le lecteur `P:\` (\serveur\partage) est visible