GS11 – TECHNIQUES DE SÉCURISATION

Configuration des GPOs

Projet SSI : Sécuriser l'infrastructure SI d'une entreprise

Préambule

Le présent document résume les différentes stratégies de groupe mises en place sur l'infrastructure. En effet, les GPO sont un atout important de l'administration du SI d'une entreprise et sont un véritable enjeu de la réduction des vulnérabilités système. Il est donc primordial de bien comprendre leur utilisation.

Nous couvrirons dans la première section les GPO demandées pour le projet. La seconde section sera quant à elle consacrée aux stratégies optionnelles déployées pour aller plus loin.

Les GPO sont positionnées au niveau du domaine puis filtrées par groupe. On utilisera les groupes prédéfinis (Utilisateurs authentifiés, Ordinateur du domaine) pour une couverture globale. D'autres groupes de sécurité ont été mis en place pour un déploiement plus précis, par fonction métier (Comptabilité, Management), ou par type d'équipement (Serveur, Ordinateurs du site principal).

Nous n'utilisons pas ici les fonctions de filtrage WMI d'une part puisque notre parc est homogène (nous n'avons déployé que des postes Windows 10 et des Serveurs 2016), et d'autre part, car cette fonctionnalité produit un surplus de calcul lors de l'application de GPO alors même que nous sommes déjà limités en ressources.

Axel NICOLAS

Antoine PINON

utt
UNIVERSITÉ DE TECHNOLOGIE
TROYES

Automne

Table des Matières

Table des Illustrations

1 Principales stratégies de groupe déployées

1.1 Politique de mot de passe

- **Nom de la GPO** : GPO_O_PolitiqueMotDePasse
- **Critère(s)** : Taille minimum de 10 caractères, au moins 1 majuscule, 1 minuscule et 1 chiffre.
- **Démarche** : Configuration de l'Ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de mot de passe

Stratégies de comptes/ Stratégie de mot de passe

Stratégie	Paramètre
Antériorité maximale du mot de passe	181 jours
Antériorité minimale du mot de passe	30 jours
Appliquer l'historique des mots de passe	5 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	10 caractères

Figure 1: GPO Politique de mot-de-passe

1.2 Mise en veille

- **Nom de la GPO** : GPO_O_PolitiqueMotDePasse
- **Critère(s)** : L'écran de veille s'active après 10 min d'inactivité et verrouille la session. Un mot de passe est alors - nécessaire pour accéder à la session.
- **Démarche** : Configuration ordinateur > Stratégie > Modèle d'administration > Composants Windows > Système > Gestion de l'alimentation > Paramètre de la veille.

Pour cette stratégie, nous utilisons un Modèle d'administration. Comme indiqué sur la capture d'écran, ces modèles proviennent de fichiers ADMX en local, mais beaucoup sont disponibles en ligne et permettent d'étendre d'autant plus les capacités d'administration.

Modèles d'administration masquer

Définitions de stratégies (fichiers ADMX) récupérées à partir de l'ordinateur local.

Système/ Gestion de l'alimentation/ Paramètres de l'affichage et de la vidéo masquer

Stratégie	Paramètre	Commentaire
Activer le diaporama de l'arrière-plan du Bureau (sur batterie)	Désactivé	
Activer le diaporama de l'arrière-plan du Bureau (sur secteur)	Désactivé	

Système/ Gestion de l'alimentation/ Paramètres de la veille masquer

Stratégie	Paramètre	Commentaire
Demander un mot de passe lorsqu'un ordinateur sort de la veille (sur batterie)	Activé	Activé par Admin, A. DeVigny, 14/ 12/ 2020
Demander un mot de passe lorsqu'un ordinateur sort de la veille (sur secteur)	Activé	

Figure 2: GPO Activation automatique de la veille

1.3 Stratégie de Restriction Logicielle (SRP)

- **Nom de la GPO** : GPO_O_SRP-Standard
- **Critère(s)** : Une restriction est appliquée sur les postes pour n'autoriser que les programmes des répertoires Windows sauf tmp.
- **Démarche** : Configuration de l'Ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégie de restriction logicielle

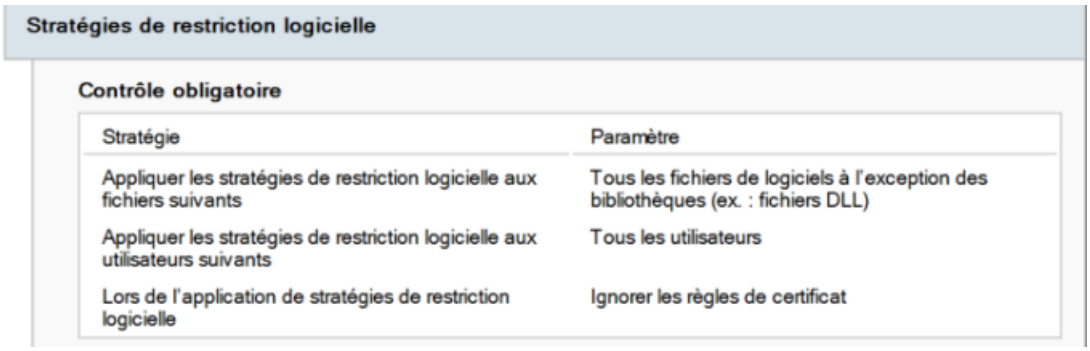

Figure 3: GPO SRP – Contrôle obligatoire (1)

Les contrôles obligatoires ainsi que les types de fichiers ont été conservés comme présent par défaut. Le reste de la stratégie consiste à restreindre tout par défaut avec le niveau de sécurité « Utilisateur standard » pour qu'un administrateur puisse toujours opérer, puis autoriser les répertoires que l'on souhaite, ici *Windows* et *ProgramFiles*. Puisque l'on souhaite exclure le dossier *Temp*, on rajoute une règle avec comme niveau de sécurité « Rejeté ». À noter qu'il existe aussi un modèle d'administration qui permet de définir une liste d'applications autorisées.

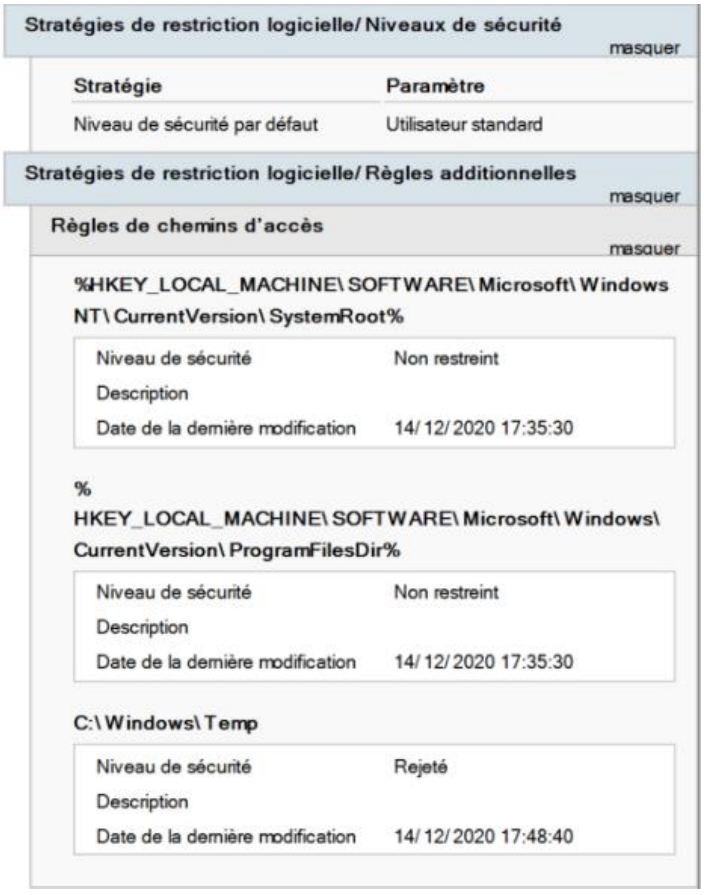

Figure 4: GPO SRP – Niveau de Sécurité et Règles additionnelles (2)

1.4 Accès à distances

- **Nom des GPO** : GPO_O_AuthRDP, GPO_O_DenyLocalAdminRDP
- **Critère(s)** : Le port 3389 est ouvert, et accessible aux administrateurs, mais l'administrateur local des postes n'est pas accessible à distance.

1.4.1 Ajout d'une règle de pare-feu pour autoriser le port 3389

- **Démarche** : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Pare-feu Windows avec sécurité avancée > Pare-feu Windows > Règles de Traffic entrant > Nouvelle Règle.

  La configuration de la règle est ensuite la même que sur un poste lambda :

Nom	G..	Profil	Activée	Action	Remplacer	Programme	Adresse locale	Adresse distante	Protocole	Port local	Port distant
Terminal Server		Domaine	Oui	Autoriser	Non	Tout	Tout	Tout	TCP	3389	Tout

Figure 5: GPO d'Autorisation du bureau à distance - Règle du Pare-feu

Règles de trafic entrant

Nom	Description
RDP	Terminal Server

Cette règle contient peut-être certains éléments qui ne peuvent pas être interprétés par la version actuelle du module de création de rapports de la console de gestion des stratégies de groupe (GPMC).	
Activé	Vrai
Programme	Tout
Action	Autoriser
Sécurité	Exiger l'authentification
Ordinateurs autorisés	
Utilisateurs autorisés	
Protocole	6
Port local	3389
Port distant	Tout
Paramètres ICMP	Tout
Étendue locale	Tout
Étendue distante	Tout
Profil	Tous
Type d'interface réseau	Tous
Service	Tous les programmes et services
Autoriser la traversée latérale	Faux
Groupe	

Figure 6: : GPO d'Autorisation du bureau à distance - Règle du Pare-feu (2)

Les autres paramètres n'ont pas été modifiés.

1.4.2 Autoriser les utilisateurs à se connecter à distance

- **Démarche** : Configuration ordinateur > Stratégies > Modèle d'administration > Composants Windows > Services Bureau à Distance > Hôte de la session Bureau à distance > Connexions.

Figure 7: GPO d'autorisation de bureau à distance - Autorisation des utilisateurs

1.4.3 Bloquer l'accès distant à l'administrateur local

- **Démarche** : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateur.

Figure 8: GPO de blocage d'accès distant à l'administrateur local

2 Stratégies de groupe optionnelles

D'autres GPO ont été ajoutés comme *PolitiqueAudit* et *SecuriteServeur-Global*. Elles implémentent les éléments de sécurité décrits dans le cours GS11 sur la sécurité des OS Windows et son annexe.

2.1 Verrouillage

- **Nom de la GPO** : GPO_O_Verrouillage
- **Critère(s)** : Verrouillage des comptes après 5 tentatives de connexion échouées en moins de 10 minutes.
- **Démarche** : Configuration ordinateur > Stratégies > Paramètres Windows > Composants Windows > Système > Gestion de l'alimentation > Paramètre de la veille.

Stratégies de comptes/ Stratégie de verrouillage du compte

Stratégie	Paramètre
Durée de verrouillage de comptes	0 minutes
Réinitialiser le compteur de verrouillages du compte après	10 minutes
Seuil de verrouillage de comptes	5 tentative d'ouverture de session non valides

Figure 9: GPO de Verrouillage pour parer au Bruteforce

2.2 Fond d'écran

- **Nom de la GPO** : GPO_U_FondEcran
- **Critère(s)** : Ajout d'un fond d'écran à l'image de l'entreprise, donner un indicateur visuel de l'application des GPO.
- **Démarche** : Configuration utilisateur > Stratégies > Modèle d'administration > Bureau > Bureau > Papier peint du Bureau.

Bureau/ Bureau masquer

Stratégie	Paramètre	Commentaire
Papier peint du Bureau	Activé	Ajouté par Admin Systeme - A. De Vigny, 14/ 12/ 2020.

Nom du papier peint :	\\srvdc1 \NETLOGON\ BKG_MonBeauReseau.png
Exemple : avec un chemin local : C:\ windows\ web\ wallpaper\ home.jpg	
Exemple : avec un chemin UNC : \\ Server\ Share\ Corp.jpg	
Style du papier peint :	Centrer

Figure 10: GPO Fond d'Ecran

2.3 Politique d'Audit

- **Nom de la GPO** : GPO_O_PolitiqueAudit
- **Critère(s)** : Pour obtenir un niveau de sécurité satisfaisant, il convient d'avoir une politique d'Audit cohérente pour pouvoir investiguer les incidents pouvant se produire sur le domaine.
- **Démarche** : Configuration utilisateur > Stratégies > Paramètres Windows > Paramètres de sécurité> Stratégie locale > Stratégie d'audit.

Stratégie locale/ Stratégie d'audit masquer

Stratégie	Paramètre
Auditer l'accès au service d'annuaire	Échec
Auditer l'accès aux objets	Échec
Auditer l'utilisation des privilèges	Échec
Auditer la gestion des comptes	Échec
Auditer le suivi des processus	Aucun audit
Auditer les événements de connexion	Échec
Auditer les événements de connexion aux comptes	Échec
Auditer les événements système	Opération réussie
Auditer les modifications de stratégie	Opération réussie

Figure 11: GPO Audit et journalisation

2.4 Politique de sécurité globale des serveurs

- **Nom de la GPO** : GPO_O_SecuriteServeur-Global
- **Critère(s)** : Implémentation des bonnes pratiques vues dans le cours GS11 sur le sujet.
- **Démarche** : Configuration ordinateur > Stratégies > Paramètres Windows > Paramètre de sécurité > *etc*. (Elles ne seront pas toutes présentées ici, mais toutes ont été implémentées.)

Stratégies de comptes/ Stratégie de mot de passe masquer

Stratégie	Paramètre
Antériorité maximale du mot de passe	30 jours
Antériorité minimale du mot de passe	15 jours
Appliquer l'historique des mots de passe	24 mots de passe mémorisés
Enregistrer les mots de passe en utilisant un chiffrement réversible	Désactivé
Le mot de passe doit respecter des exigences de complexité	Activé
Longueur minimale du mot de passe	10 caractères

Stratégies de comptes/ Stratégie de verrouillage du compte masquer

Stratégie	Paramètre
Durée de verrouillage de comptes	0 minutes
Réinitialiser le compteur de verrouillages du compte après	20 minutes
Seuil de verrouillage de comptes	3 tentative d'ouverture de session non valides

Figure 12: Sécurité des Serveurs - Mot de passe et Verrouillage

Stratégies locales/ Attribution des droits utilisateur masquer

Stratégie	Paramètre
Accéder à cet ordinateur à partir du réseau	AUTORITE NT\ Utilisateurs authentifiés, MONBEAURESEAU\ Contrôleurs de domaine, BUILTIN\ Administrateurs
Agir en tant que partie du système d'exploitation	
Ajuster les quotas de mémoire pour un processus	AUTORITE NT\ SERVICE RÉSEAU, AUTORITE NT\ SERVICE LOCAL, BUILTIN\ Administrateurs
Arrêter le système	BUILTIN\ Administrateurs
Augmenter la priorité de planification	BUILTIN\ Administrateurs
Autoriser l'ouverture de session par les services Terminal Server	BUILTIN\ Administrateurs
Charger et décharger les pilotes de périphériques	BUILTIN\ Administrateurs
Contourner la vérification de parcours	AUTORITE NT\ Utilisateurs authentifiés
Créer des liens symboliques	BUILTIN\ Administrateurs
Créer des objets globaux	AUTORITE NT\ SERVICE, BUILTIN\ Administrateurs
Créer des objets partagés permanents	
Créer un objet-jeton	
Déboguer les programmes	
Effectuer les tâches de maintenance de volume	BUILTIN\ Administrateurs
Emprunter l'identité d'un client après l'authentification	AUTORITE NT\ SERVICE, BUILTIN\ Administrateurs
Forcer l'arrêt à partir d'un système distant	BUILTIN\ Administrateurs

Figure 13: Sécurité des Serveurs – Attribution des droits utilisateur (1)

Générer des audits de sécurité	AUTORITE NT\ SERVICE RÉSEAU, AUTORITE NT\ SERVICE LOCAL
Gérer le journal d'audit et de sécurité	BUILTIN\ Administrateurs
Interdire l'accès à cet ordinateur à partir du réseau	Support_388945a0, BUILTIN\ Invités, AUTORITE NT\ ANONYMOUS LOGON
Interdire l'ouverture d'une session locale	Support_388945a0, BUILTIN\ Invités
Interdire l'ouverture de session en tant que service	
Interdire l'ouverture de session en tant que tâche	Support_388945a0, BUILTIN\ Invités
Interdire l'ouverture de session par les services Terminal Server	BUILTIN\ Invités
Modifier l'heure système	AUTORITE NT\ SERVICE LOCAL, BUILTIN\ Administrateurs
Modifier les valeurs de l'environnement du microprogramme	BUILTIN\ Administrateurs
Ouvrir une session en tant que service	AUTORITE NT\ SERVICE RÉSEAU
Permettre à l'ordinateur et aux comptes d'utilisateurs d'être approuvés pour la délégation	BUILTIN\ Administrateurs
Prendre possession de fichiers ou d'autres objets	BUILTIN\ Administrateurs
Processus unique du profil	BUILTIN\ Administrateurs
Remplacer un jeton de niveau processus	AUTORITE NT\ SERVICE RÉSEAU, AUTORITE NT\ SERVICE LOCAL
Restaurer les fichiers et les répertoires	BUILTIN\ Administrateurs
Retirer l'ordinateur de la station d'accueil	BUILTIN\ Administrateurs
Sauvegarder les fichiers et les répertoires	BUILTIN\ Administrateurs
Synchroniser les données du service d'annuaire	
Verrouiller les pages en mémoire	

Figure 14: Sécurité des Serveurs – Attribution des droits utilisateur (2)

Stratégies locales/ Options de sécurité masquer

Accès réseau masquer

Stratégie	Paramètre
Accès réseau : les autorisations spécifiques des utilisateurs appartenant au groupe Tout le monde s'appliquent aux utilisateurs anonymes	Désactivé
Accès réseau : les canaux nommés qui sont accessibles de manière anonyme	COMNAP, COMNODE, SQL\ QUERY, SPOOLSS, LLSRPC, BROWSER, netlogon, lsarpc, samr
Accès réseau : les chemins de Registre accessibles à distance	System\ CurrentControlSet\ Control\ ProductOptions, System\ CurrentControlSet\ Control\ Server Applications, Software\ Microsoft\ Windows NT\ CurrentVersion
Accès réseau : les partages qui sont accessibles de manière anonyme	
Accès réseau : modèle de partage et de sécurité pour les comptes locaux	Classique - les utilisateurs locaux s'authentifient eux-mêmes
Accès réseau : ne pas autoriser l'énumération anonyme des comptes et partages SAM	Activé
Accès réseau : ne pas autoriser l'énumération anonyme des comptes SAM	Activé
Accès réseau : restreindre l'accès anonyme aux canaux nommés et aux partages	Activé
Accès réseau : ne pas autoriser le stockage de mots de passe et d'informations d'identification pour l'authentification du réseau	Activé
Accès réseau : permet la traduction de noms/ SID	Désactivé

Figure 15: Sécurité des Serveurs – Options de sécurité

Arrêter le système masquer

Stratégie	Paramètre
Arrêt : effacer le fichier d'échange de mémoire virtuelle	Désactivé
Arrêt : permet au système d'être arrêté sans avoir à se connecter	Désactivé

Audit masquer

Stratégie	Paramètre
Audit : arrêter immédiatement le système s'il n'est pas possible de se connecter aux audits de sécurité	Activé
Audit : auditer l'accès des objets système globaux	Désactivé
Audit : auditer l'utilisation des privilèges de sauvegarde et de restauration	Désactivé

Chiffrement système masquer

Stratégie	Paramètre
Chiffrement système : utilisez des algorithmes compatibles FIPS pour le chiffrement, le hachage et la signature	Activé
Cryptographie système : force une protection forte des clés utilisateur enregistrées sur l'ordinateur	L'utilisateur doit entrer un mot de passe à chaque utilisation de la clé

Figure 16: Sécurité des Serveurs - Option de sécurité (2)

Client Réseau Microsoft masquer

Stratégie	Paramètre
Client réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)	Activé
Client réseau Microsoft : communications signées numériquement (toujours)	Activé
Client réseau Microsoft : envoyer un mot de passe non chiffré aux serveurs SMB tierce partie	Désactivé

Comptes masquer

Stratégie	Paramètre
Comptes : restreindre l'utilisation de mots de passe vides par le compte local à l'ouverture de session console	Activé
Comptes : état de compte d'administrateur	Activé
Comptes : état de compte d'invité	Désactivé

Figure 17: Sécurité des Serveurs - Option de sécurité (3)

...

Cf. Cours GS11, fichier SSl_apache_1.2.pdf