Stratégies de Groupe

Active Directory — centresio.local

Version : 1.0

Rédacteur : Florian Besse

Date : Mai 2026

Formation : BTS SIO option SISR

Domaine : centresio.local

1. Présentation

L'infrastructure Centre SIO applique dix-huit objets de stratégie de groupe (GPO) distribués sur l'ensemble des unités organisationnelles du domaine centresio.local. Ces stratégies couvrent la sécurité des postes, la gestion des mises à jour, le déploiement des agents de supervision et de gestion, ainsi que le mappage des lecteurs réseau selon les profils utilisateurs.

Contrôleur principal : **SRV-AD-SIO — 10.0.90.11**
Contrôleur secondaire : **SRV-AD2-SIO — 10.0.90.6**
Domaine : **centresio.local**
Console de gestion : **GPMC — gpmc.msc**

2. Structure des unités organisationnelles

Les GPO sont liées aux OU suivantes, reflétant l'organisation logique du parc :

OU Postes : **Stations de travail pédagogiques et administratives**
OU Serveurs : **Ensemble des serveurs membres du domaine**
OU Utilisateurs : **Comptes utilisateurs rattachés aux services**
OU Admins : **Comptes administrateurs du domaine**

3. Détail des GPO appliquées

3.1 — Sécurité des mots de passe

Nom : **GPO_MotDePasse**
Étendue : **Domaine entier**
Longueur minimale : **10 caractères**
Complexité : **Activée — majuscule, minuscule, chiffre, caractère spécial**
Durée maximale : **60 jours**
Historique : **5 anciens mots de passe mémorisés**
Verrouillage de compte : **5 tentatives échouées — déverrouillage après 30 minutes**

3.2 — LAPS (Local Administrator Password Solution)

Nom : **GPO_LAPS**
Étendue : **OU Postes**
Complexité du mot de passe local : **Activée**
Durée de vie : **30 jours**
Compte cible : **Administrateur local**
Stockage : **Attribut ms-MCS-AdmPwd dans Active Directory**

> *Le mot de passe de l'administrateur local est renouvelé automatiquement et lisible depuis la console LAPS par les administrateurs du domaine.*

3.3 — BitLocker

Nom : **GPO_BitLocker**

Étendue : **OU Postes**

Chiffrement : **AES 256 bits — XTS-AES**

Mode de démarrage : **TPM uniquement**

Stockage de la clé de récupération : **Active Directory — attribut ms-FVE-RecoveryPassword**

Lecteur système : **Chiffrement obligatoire avant démarrage**

3.4 — Restriction des ports USB

Nom : **GPO_USB**

Étendue : **OU Postes**

Périphériques de stockage USB : **Désactivés en écriture**

Stratégie appliquée : **Refus d'installation des pilotes de stockage amovible**

3.5 — Déploiement de l'agent Zabbix

Nom : **GPO_Zabbix_Agent**

Étendue : **OU Postes + OU Serveurs**

Type de déploiement : **Installation MSI via stratégie logicielle (Computer Configuration)**

Paramètre Server : **10.0.90.10 (SRV-ZABBIX-SIO)**

Paramètre Hostname : **Résolu automatiquement via variable %COMPUTERNAME%**

3.6 — Déploiement de l'agent GLPI

Nom : **GPO_GLPI_Agent**

Étendue : **OU Postes + OU Serveurs**

Type de déploiement : **Installation MSI via stratégie logicielle**

URL du serveur GLPI : **http://10.0.90.8**

Fréquence d'inventaire : **Toutes les 24 heures**

3.7 — WSUS — Postes

Nom : **GPO_WSUS_PC**

Étendue : **OU Postes**

Serveur WSUS : **http://SRV-WSUS-SIO:8530**

Détection des mises à jour : **Toutes les 22 heures**

Installation automatique : **Tous les jours à 03h00**

Redémarrage automatique : **Activé si aucun utilisateur connecté**

3.8 — WSUS — Serveurs

Nom : **GPO_WSUS_SRV**
Étendue : **OU Serveurs**
Serveur WSUS : **http://SRV-WSUS-SIO:8530**
Détection des mises à jour : **Toutes les 22 heures**
Installation automatique : **Désactivée — validation manuelle requise**
Groupe WSUS cible : **Serveurs**

3.9 — Mappage des lecteurs réseau

Nom : **GPO_LecteurReseau_Users**
Étendue : **OU Utilisateurs**
Lecteur H: : **\\centresio.local\DFS\Personnel\%USERNAME%**
Lecteur S: : **\\centresio.local\DFS\Commun**
Application : **Item-level targeting — selon le groupe de sécurité AD**

3.10 — Fond d'écran et personnalisation

Nom : **GPO_Fond_Ecran**
Étendue : **OU Postes**
Fond d'écran : **Imposé depuis le partage SYSVOL**
Personnalisation utilisateur : **Désactivée**

3.11 — Pare-feu Windows

Nom : **GPO_Firewall**
Étendue : **OU Postes + OU Serveurs**
Profil Domain : **Activé**
Profil Private : **Activé**
Profil Public : **Activé — règles entrantes bloquées par défaut**
Exceptions autorisées : **RDP (3389 TCP), WinRM (5985 TCP), ICMP, agent Zabbix (10050 TCP)**

3.12 — Gestion des sessions utilisateurs

Nom : **GPO_Session**
Étendue : **OU Postes**
Verrouillage de session : **Après 10 minutes d'inactivité**
Déconnexion automatique : **Après 60 minutes d'inactivité**
Ctrl+Alt+Suppr : **Requis pour déverrouiller**

4. Ordre d'application et héritage

L'application des GPO suit l'ordre LSDOU : Local, Site, Domaine, Unité Organisationnelle. Aucun blocage d'héritage n'est configuré sur les OU de l'infrastructure. Les stratégies liées aux OU feuilles prennent le dessus sur celles liées au niveau domaine en cas de conflit de paramètre.

Traitement loopback : **Désactivé**
Filtre WMI : **Aucun filtre WMI actif**
Liens forcés : **Aucun lien en mode Enforced**