

PROCÉDURE DE DÉPLOIEMENT

GPO Active Directory

Agents Zabbix et GLPI — Domaine sio.local — Infrastructure SISR 2026

Auteur	CHADHOULI EL-Anrif
Domaine	sio.local — SRV-AD-01 (10.11.3.18)
Date	Mars 2026
GPO couvertes	GPO_DEPLOY_ZABBIX_AGENT GPO_DEPLOY_GLPI_AGENT
OUs cibles	Service_RH, Service_INFO, Service_COMPTA + CL-WIN11-01/02
Prérequis	Partage SYSVOL accessible, MSI téléchargés sur SRV-AD-01

1. Contexte et Prérequis

1.1 Objectif

Cette procédure décrit le déploiement automatique des agents Zabbix et GLPI sur tous les postes Windows du domaine sio.local via des stratégies de groupe (GPO). L'objectif est d'éviter toute installation manuelle poste par poste : dès qu'un poste rejoint le domaine ou redémarre, les agents s'installent automatiquement sans intervention.

i INFO : Cette méthode remplace l'installation manuelle précédente. Les GPO sont créées sur SRV-AD-01 (10.11.3.18) et s'appliquent à toutes les OUs contenant des postes clients.

1.2 Architecture des GPO

GPO	Logiciel déployé	OUs cibles
GPO_DEPLOY_ZABBIX_AGENT	zabbix_agent2-7.x- windows.msi	Service_RH, Service_INFO, Service_COMPTA

GPO_DEPLOY_GLPI_AGENT	glpi-agent-1.x-x64.msi	Service_RH, Service_INFO, Service_COMPTA
-----------------------	------------------------	---

1.3 Prérequis avant de commencer

- SRV-AD-01 (10.11.3.18) est opérationnel, rôle AD DS actif
- Les OUs Service_RH, Service_INFO, Service_COMPTA existent dans sio.local
- Les postes CL-WIN11-01 (10.11.3.25) et CL-WIN11-02 (10.11.4.24) sont joints au domaine
- Les fichiers .msi sont téléchargés et stockés sur SRV-AD-01

2. Préparation des Fichiers MSI sur SRV-AD-01

2.1 Création du dossier de partage réseau

Les MSI doivent être accessibles via un chemin UNC depuis tous les postes du domaine. On crée un partage dédié sur SRV-AD-01 :

```
# Sur SRV-AD-01 — PowerShell en administrateur

# Créer le dossier de déploiement
New-Item -ItemType Directory -Path 'C:\Deploiement\MSI' -Force

# Partager le dossier en lecture seule pour les ordinateurs du domaine
New-SmbShare -Name 'Deploiement' -Path 'C:\Deploiement' `
  -Description 'Partage MSI pour GPO' `
  -ReadAccess 'Domain Computers','Domain Users' `
  -FullAccess 'Domain Admins'

# Vérifier que le partage est actif
Get-SmbShare -Name 'Deploiement'
```

 **CAPTURE REQUISE** : SRV-AD-01 PowerShell — Get-SmbShare montrant le partage 'Déploiement' actif avec les droits corrects

```
PS C:\Users\Administrateur> get-SmbShare -Name 'Deploiement'
```

Name	ScopeName	Path	Description
Deploiement	*	C:\Deploiement	

2.2 Téléchargement et placement des MSI

Agent Zabbix

URL de téléchargement : https://www.zabbix.com/download_agents → Windows → MSI 64-bit

```
# Copier le MSI Zabbix dans le dossier de déploiement
# (télécharger manuellement ou via PowerShell si accès Internet sur SRV-AD-01)
Copy-Item 'zabbix_agent2-7.x.x-windows-amd64-openssl.msi' `
  -Destination 'C:\Deploiement\MSI\zabbix_agent.msi'
```

Agent GLPI

URL de téléchargement : <https://github.com/glpi-project/glpi-agent/releases> → glpi-agent-X.x-x64.msi

```
Copy-Item 'glpi-agent-1.x-x64.msi' `
-Destination 'C:\Deploiement\MSI\glpi_agent.msi'
```

```
# Vérifier la présence des deux MSI
Get-ChildItem 'C:\Deploiement\MSI\'

# Tester l'accès UNC depuis SRV-AD-01
Test-Path '\\10.11.3.18\Deploiement\MSI\zabbix_agent.msi'
Test-Path '\\10.11.3.18\Deploiement\MSI\glpi_agent.msi'
```

 **CAPTURE REQUISE :** SRV-AD-01 PowerShell — Get-ChildItem montrant zabbix_agent.msi et glpi_agent.msi présents + Test-Path retournant True pour les deux

```
PS C:\Users\Administrateur> Get-ChildItem 'C:\Deploiement\MSI\'
```

Répertoire : C:\Deploiement\MSI

Mode	LastWriteTime		Length	Name
----	-----	-----	-----	----
-a----	06/12/2025	04:03	1996800	7z2501-x64.msi
-a----	09/12/2025	17:44	22568960	glpi_agent.msi
-a----	15/12/2025	11:16	147	install_glpi.bat
-a----	25/03/2026	09:39	9756672	zabbix_agent.msi

```
PS C:\Users\Administrateur> Test-Path '\\10.11.3.18\Deploiement\MSI\zabbix_agent.msi'
True
```

```
PS C:\Users\Administrateur> Test-Path '\\10.11.3.18\Deploiement\MSI\glpi_agent.msi'
True
```

3. Création de la GPO — Agent Zabbix

3.1 Créer la GPO dans la console GPMC

1. Sur SRV-AD-01, ouvrir : Outils d'administration → Gestion des stratégies de groupe (gpmc.msc)
2. Dans l'arborescence, faire un clic droit sur l'OU Service_INFO → Créer un objet GPO dans ce domaine
3. Nommer la GPO : GPO_DEPLOY_ZABBIX_AGENT
4. Cliquer OK

CAPTURE REQUISE : Console GPMC — GPO_DEPLOY_ZABBIX_AGENT créée visible dans l'arborescence sous Service_INFO

Service_INFO						
Objets de stratégie de groupe liés Héritage de stratégie de groupe Délégation						
Ordre des liens	Objet de stratégie de groupe	Appliqué	Lien activé	État GPO	Filtre WMI	Modifié le
1	GPO_DEPLOY_ZABBIX_AGENT	Non	Oui	Activé	Aucun(e)	25/03/2026 09:25:34
2	GPO_DEPLOY_GLPI_AGENT	Non	Oui	Activé	Aucun(e)	25/03/2026 09:25:34

3.2 Configurer le déploiement MSI

5. Faire un clic droit sur GPO_DEPLOY_ZABBIX_AGENT → Modifier
6. Dans l'éditeur GPO, naviguer vers :

Configuration ordinateur → Paramètres → Paramètres du logiciel → Installation du logiciel

7. Clic droit dans le panneau droit → Nouveau → Package
8. Dans la fenêtre qui s'ouvre, saisir le chemin UNC :

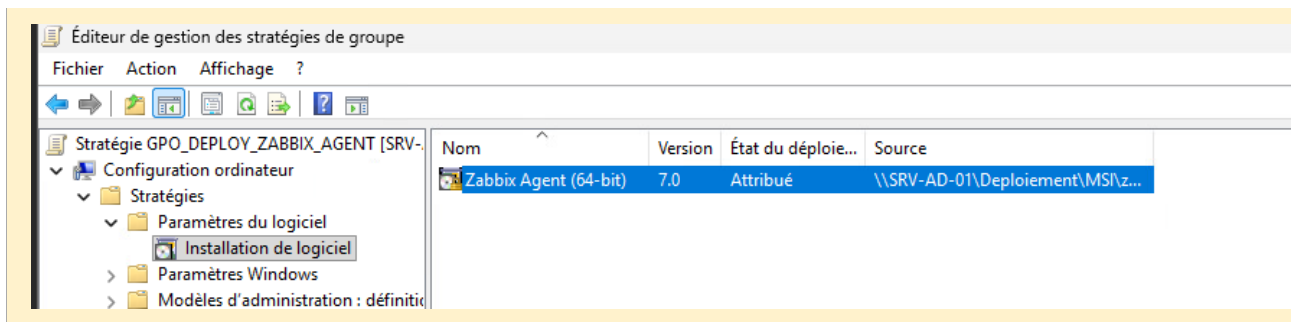
\\10.11.3.18\Deploiement\MSI\zabbix_agent.msi

⚠ ATTENTION : Il est impératif d'utiliser le chemin UNC (\\serveur\partage\...) et non un chemin local (C:\...). Un chemin local ne sera pas accessible depuis les postes clients.

9. Dans 'Méthode de déploiement', choisir : Assigné
10. Cliquer OK

i INFO : 'Assigné' signifie que l'installation se fait automatiquement au démarrage du poste, sans action de l'utilisateur. C'est le mode recommandé pour les agents de supervision.

CAPTURE REQUISE : Éditeur GPO — Installation du logiciel avec zabbix_agent.msi assigné visible dans la liste, chemin UNC \\10.11.3.18\Deploiement\MSI\zabbix_agent.msi



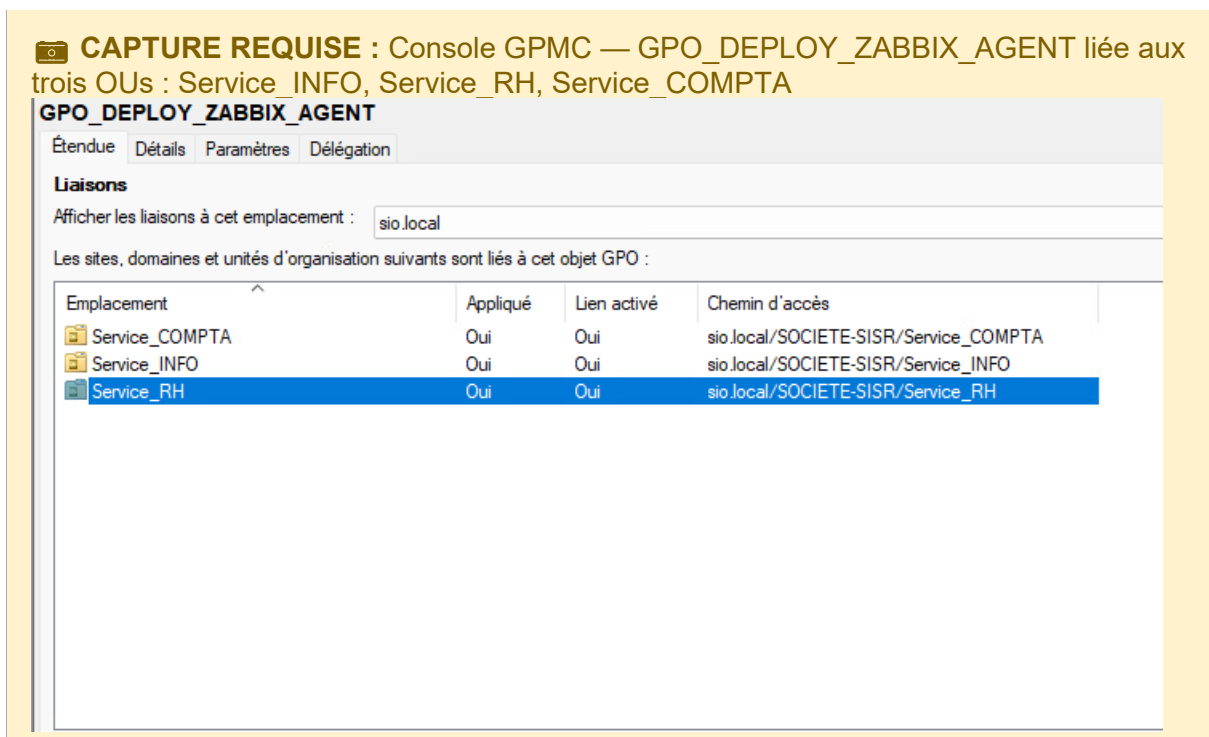
3.3 Configurer les propriétés du package Zabbix

11. Double-cliquer sur le package zabbix_agent dans la liste
12. Onglet Déploiement : vérifier que 'Assigné' est coché
13. Onglet Modifications : laisser vide (pas de fichier .mst de transformation nécessaire)
14. Cliquer OK

3.4 Lier la GPO aux autres OUs

La GPO doit être liée à toutes les OUs contenant des postes clients, pas seulement Service_INFO :

15. Dans GPMC, faire un clic droit sur Service_RH → Lier un objet GPO existant
16. Sélectionner GPO_DEPLOY_ZABBIX_AGENT → OK
17. Répéter pour Service_COMPTA



4. Création de la GPO — Agent GLPI

4.1 Créer la GPO GLPI

18. Dans GPMC, clic droit sur Service_INFO → Créer un objet GPO
19. Nommer la GPO : GPO_DEPLOY_GLPI_AGENT
20. Cliquer OK

4.2 Configurer le déploiement MSI GLPI

21. Clic droit sur GPO_DEPLOY_GLPI_AGENT → Modifier
22. Naviguer vers Configuration ordinateur → Paramètres → Paramètres du logiciel → Installation du logiciel
23. Clic droit → Nouveau → Package
24. Saisir le chemin UNC :
`\\10.11.3.18\Deploiement\MSI\glpi_agent.msi`
25. Méthode de déploiement : Assigné → OK

4.3 Configurer les options de l'agent GLPI (serveur cible)

L'agent GLPI doit connaître l'adresse de son serveur. On peut le configurer via les propriétés du package MSI ou via un fichier de transformation (.mst). La méthode la plus simple est de modifier les paramètres après installation via une clé de registre GPO :

26. Dans l'éditeur GPO de GPO_DEPLOY_GLPI_AGENT, naviguer vers :

`Configuration ordinateur → Préférences → Paramètres Windows → Registre`

27. Clic droit → Nouveau → Élément registre
28. Renseigner :

Champ	Valeur
Action	Mettre à jour
Ruche	HKEY_LOCAL_MACHINE
Chemin de la clé	SOFTWARE\GLPI-Agent
Nom de la valeur	server
Type de valeur	REG_SZ
Données de la valeur	http://10.11.3.22/glpi

29. Cliquer OK

CAPTURE REQUISE : Éditeur GPO — glpi_agent.msi assigné + clé de registre 'server = http://10.11.3.22/glpi' visible dans Préférences > Registre

Stratégie GPO_DEPLOY_GLPI_AGENT [SRV-AD-01.SIO.LOCAL]	Nom	Version	État du déploie...	Source
Configuration ordinateur	GLPI Agent 1.15	1.15	Attribué	\\SRV-AD-01\Deploiement\MSI\g...
Stratégies				
Paramètres du logiciel				
Installation de logiciel				
Paramètres Windows				
Modèles d'administration : définitions de stratégies (fich				

Propriétés de : server

Général Commun

Action : Mettre à jour

Ruche : HKEY_LOCAL_MACHINE

Chemin d'accès de la clé : SOFTWARE\GLPI-Agent

Nom de valeur

☐ Par défaut server

Type de valeur : REG_SZ

Données de valeur : http://10.11.3.22/glpi

OK Annuler Appliquer Aide

4.4 Lier la GPO GLPI aux OUs

30. Lier GPO_DEPLOY_GLPI_AGENT à Service_RH, Service_INFO, Service_COMPTA (même procédure que pour Zabbix)

CAPTURE REQUISE : Console GPMC — GPO_DEPLOY_GLPI_AGENT liée aux trois OUs, visible en dessous de GPO_DEPLOY_ZABBIX_AGENT

GPO_DEPLOY_GLPI_AGENT

Étendue Détails Paramètres Délégation

Liaisons

Afficher les liaisons à cet emplacement : sio.local

Les sites, domaines et unités d'organisation suivants sont liés à cet objet GPO :

Emplacement	Appliqué	Lien activé	Chemin d'accès
Service_COMPTA	Oui	Oui	sio.local/SOCIETE-SISR/Service_COMPTA
Service_INFO	Oui	Oui	sio.local/SOCIETE-SISR/Service_INFO
Service_RH	Oui	Oui	sio.local/SOCIETE-SISR/Service_RH

5. Application des GPO et Validation

5.1 Forcer l'application sur CL-WIN11-01

Se connecter sur CL-WIN11-01 (10.11.3.25) avec un compte du domaine administrateur :

```
# Forcer la mise à jour des GPO immédiatement (sans redémarrage)
gpupdate /force

# Vérifier quelles GPO sont appliquées sur ce poste
gpresult /r
```

 **CAPTURE REQUISE** : CL-WIN11-01 PowerShell — gpupdate /force terminé sans erreur + gpresult /r montrant GPO_DEPLOY_ZABBIX_AGENT et GPO_DEPLOY_GLPI_AGENT dans la liste des GPO appliquées

```
C:\Users\Administrateur>gpresult /r

Outil de résultat du système d'exploitation Microsoft (R) Windows (R) v2.0
© Microsoft Corporation. Tous droits réservés.

Créé le 25/03/2026 à 12:24:41

Données RSOP pour SIO\Administrateur sur CL-W11-01 : mode journalisation
-----

Configuration du système d'exploitation : Station de travail membre
Version du système d'exploitation..... : 10.0.26100
Nom du site..... : Default-First-Site-Name
Profil itinérant : N/A
Profil local..... : C:\Users\Administrateur
Connexion via une liaison lente ? : Non

Paramètre de l'ordinateur
-----
CN=CL-W11-01,OU=Ordinateur,OU=Service_INFO,OU=SOCIETE-SISR,DC=sio,DC=local
Heure de la dernière application de la stratégie de groupe : 25/03/2026 à 11:14:09
Stratégie de groupe appliquée depuis : SRV-AD-01.sio.local
Seuil de liaison lente dans la stratégie de groupe : 500 kbps
Nom du domaine..... : SIO
Type de domaine..... : Windows 2008 ou supérieur

Objets Stratégie de groupe appliqués
-----
Default Domain Policy
GPO_Deploy_7Zip
GPO_DEPLOY_ZABBIX_AGENT
GPO_DEPLOY_GLPI_AGENT

Les objets stratégie de groupe n'ont pas été appliqués
car ils ont été refusés
-----
```

 **ATTENTION** : gpupdate /force applique les préférences mais les déploiements MSI (Installation du logiciel) nécessitent un redémarrage complet du poste pour s'installer.

5.2 Redémarrer CL-WIN11-01 et vérifier l'installation

31. Redémarrer CL-WIN11-01

32. Après redémarrage, ouvrir PowerShell et vérifier les installations :

```
# Vérifier que l'agent Zabbix est installé
Get-Service -Name 'Zabbix Agent 2'
# → Status doit être 'Running'

# Vérifier que l'agent GLPI est installé
Get-Service -Name 'GLPI-Agent'
# → Status doit être 'Running'

# Vérifier dans la liste des programmes installés
Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like '*Zabbix*' -or $_.Name -like '*GLPI*'} | Select-Object Name, Version
```

 **CAPTURE REQUISE : CL-WIN11-01 PowerShell — Get-Service : Zabbix Agent 2 = Running + GLPI-Agent = Running**

```
PS C:\Users\Administrateur> Get-Service -Name "Zabbix Agent"
```

Status	Name	DisplayName
Running	Zabbix Agent	Zabbix Agent

```
PS C:\Users\Administrateur> Get-Service -Name "GLPI-Agent"
```

Status	Name	DisplayName
Running	GLPI-Agent	GLPI Agent

 **CAPTURE REQUISE : CL-WIN11-01 PowerShell — Get-WmiObject montrant Zabbix Agent et GLPI-Agent dans la liste des programmes installés avec leurs versions**

```
PS C:\Users\Administrateur> Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -like "*Zabbix*" -or $_.Name -like "*GLPI*"} | Select-Object Name, Version, InstallDate
```

Name	Version	InstallDate
Zabbix Agent (64-bit)	7.0.24.2400	20260325
GLPI Agent 1.15	1.15	20260325

5.3 Vérification côté serveurs

Vérification Zabbix

Sur SRV-ZABBIX (10.11.3.19), dans l'interface web Zabbix :

33. Se connecter à <http://10.11.3.19/zabbix>

34. Aller dans Configuration → Hôtes

35. Vérifier que CL-WIN11-01 (10.11.3.25) apparaît avec un statut 'ZBX' vert

 **CAPTURE REQUISE : Interface web Zabbix — CL-WIN11-01 visible dans la liste des hôtes avec icône ZBX verte (agent connecté)**

Nom ▲	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableau
CL-W11-01	10.11.3.23:10050	ZBX	class: os target: windows	Activé	Dernières données 117	1 1	Graphiques 15	Tableau
CL-W11-02	10.11.4.22:10050	ZBX	class: os target: windows	Activé	Dernières données 115	2	Graphiques 12	Tableau
PF-SENSE-01	10.11.3.17:10050	ZBX	class: os target: freebsd	Activé	Dernières données 151	Problèmes	Graphiques 44	Tableau
PF-SENSE-02	10.11.4.17:161	SNMP	class: software target: pfsense	Activé	Dernières données 100	1	Graphiques 10	Tableau
SRV-AD-01	10.11.3.18:10050	ZBX	class: os target: windows	Activé	Dernières données 134	2 1	Graphiques 16	Tableau
SRV-AD-02	10.11.4.18:10050	ZBX	class: os target: windows	Activé	Dernières données 121	1 1	Graphiques 12	Tableau
SRV-GLPI	10.11.3.22:10050	ZBX	class: os target: linux	Activé	Dernières données 68	1	Graphiques 14	Tableau
SRV-WEB-01	10.11.3.2:10050	ZBX	class: os target: linux	Activé	Dernières données 43	Problèmes	Graphiques 8	Tableau
Zabbix server	10.11.3.19:10050	ZBX	class: os target: linux	Activé	Dernières données 75	1	Graphiques 16	Tableau

Vérification GLPI

Sur SRV-GLPI (10.11.3.22), dans l'interface web GLPI :

36. Se connecter à <http://10.11.3.22/glpi>
37. Aller dans Parc → Ordinateurs
38. Vérifier que CL-WIN11-01 apparaît avec son inventaire automatiquement rempli

 **CAPTURE REQUISE** : Interface web GLPI — CL-WIN11-01 visible dans Parc > Ordinateurs avec inventaire automatique (matériel, OS, logiciels) rempli

5.4 Répéter sur CL-WIN11-02 (Site B)

Répéter les mêmes vérifications sur CL-WIN11-02 (10.11.4.24). Ce poste étant sur le Site B, il récupère les GPO via le tunnel IPsec et la réplication AD depuis SRV-AD-02.