LOSTE TRADI-FRANCE

Sécurisation des Scripts deSauvegarde PowerShell (DPAPI)

Procédure de migration INIT et bascule par site

Rédacteur	Paul Barrault-Gautier
Entreprise	Loste Tradi-France
Poste	Administrateur Réseau & Systèmes
Date	Avril 2026
Version	1.0
Classification	Usage interne — Confidentiel

1. Contexte et problématique

Loste Tradi-France dispose d'un parc de ~16 scripts PowerShell de sauvegarde basés sur Robocopy, déployés sur plusieurs sites de production. Ces scripts utilisaient initialement des identifiants (login/mot de passe NAS) stockés en clair dans les fichiers de configuration ou directement codés en dur dans les scripts.

Dans le cadre du renforcement de la sécurité des sauvegardes, ces scripts ont été refactorisés pour utiliser la DPAPI (Data Protection API) Windows via la cmdlet Export-Clixml / Import-Clixml de PowerShell. Les credentials sont désormais chiffrés et liés au compte de service du poste, rendant impossible leur réutilisation sur un autre poste ou par un autre utilisateur.

1.1 Avant / Après la migration

Aspect	Avant (ancienne version)	Après (version sécurisée)
Stockage des credentials	**En clair dans le script ou .txt**	**Chiffré DPAPI via Export-Clixml**
Protection	Aucune	Lié au compte + poste Windows
Réutilisable sur autre poste	Oui (danger)	Non (sécurité DPAPI)
Planification	Tâche planifiée manuelle (compte admin)	Register-ScheduledTask sans droits admin
Journalisation	Absente ou minimale	Fichier log + EventLog Windows
Supervision	Aucune	Dashboard HTML centralisé sur NAS

1.2 Périmètre de la migration

- 16 scripts Robocopy répartis sur les sites de production Loste
- Chaque site dispose d'un compte de service Windows dédié pour l'exécution des sauvegardes
- Destination des sauvegardes : NAS Loste (partage SMB sécurisé par site)
- Migration effectuée site par site pour limiter les risques

2. Principe de la sécurisation DPAPI

2.1 Comment fonctionne Export-Clixml / Import-Clixml

PowerShell permet de sérialiser un objet PSCredential (login + mot de passe chiffré) dans un fichier XML via Export-Clixml. Le chiffrement est assuré par la DPAPI Windows, qui lie le secret :

- Au compte Windows qui a exécuté Export-Clixml (compte de service)
- À la machine sur laquelle le chiffrement a été effectué

Seul le même compte sur la même machine peut déchiffrer le fichier XML avec Import-Clixml. Toute tentative de lecture depuis un autre contexte retourne une erreur.

```
# Créer et stocker le credential chiffré (à exécuter UNE SEULE FOIS par site)
# DOIT être exécuté sous le compte de service qui lancera les sauvegardes

$credential = Get-Credential   # Saisir le login/mdp NAS à la demande
$credential | Export-Clixml -Path 'C:\Scripts\Backup\creds\nas-cred.xml'

# Le fichier nas-cred.xml est chiffré par DPAPI
# Il ne peut être lu que par le compte de service sur CE poste
```

> ⚠ **L'étape Export-Clixml doit être exécutée en étant connecté (ou via Invoke-Command -ComputerName) sous le compte de service exact qui exécutera les tâches planifiées. Exécuté sous un autre compte, le fichier XML sera inutilisable.**

3. Procédure de migration INIT par site

3.1 Étapes préparatoires (à faire une seule fois par site)

1. Identifier le compte de service Windows utilisé pour les tâches planifiées sur le site (ex. : LOSTE\svc-backup-site1)
2. Se connecter au poste ou serveur du site sous ce compte de service
3. Créer le répertoire sécurisé pour les credentials

```
# Créer le dossier de stockage des credentials (accès restreint)
New-Item -Path 'C:\Scripts\Backup\creds' -ItemType Directory -Force

# Restreindre l'accès au dossier : uniquement le compte de service
$acl = Get-Acl 'C:\Scripts\Backup\creds'
$acl.SetAccessRuleProtection($true, $false)   # Désactiver l'héritage
$rule = New-Object System.Security.AccessControl.FileSystemAccessRule(
    'LOSTE\svc-backup-site1', 'FullControl', 'Allow')
$acl.SetAccessRule($rule)
Set-Acl -Path 'C:\Scripts\Backup\creds' -AclObject $acl
```

4. Générer le fichier de credentials chiffré

```
# Sous le compte de service : saisir les credentials NAS
$cred = Get-Credential -Message 'Entrez les credentials NAS Loste'
$cred | Export-Clixml -Path 'C:\Scripts\Backup\creds\nas-cred.xml'

# Vérifier que le fichier est bien créé
Test-Path 'C:\Scripts\Backup\creds\nas-cred.xml'
```

5. Tester la relecture du credential

```
# Vérifier que Import-Clixml fonctionne correctement
$testCred = Import-Clixml -Path 'C:\Scripts\Backup\creds\nas-cred.xml'
$testCred.UserName   # Doit afficher le login NAS
$testCred.GetNetworkCredential().Password   # Doit afficher le mot de passe
```

6. Déployer les scripts de sauvegarde sécurisés (voir DOC-PSB-02)
7. Enregistrer les tâches planifiées (voir DOC-PSB-03)
8. Valider une première exécution manuelle du script
9. Désactiver et archiver les anciens scripts non sécurisés

3.2 Bascule site par site — Tableau de suivi

Site	Compte de service	INIT effectué	Scripts déployés	Tâche planifiée
Siège Angers	svc-backup-siege	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non
Site Production 1	svc-backup-prod1	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non
Site Production 2	svc-backup-prod2	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non
Site Production 3	svc-backup-prod3	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non	[ ] Oui / [ ] Non

4. Gestion du renouvellement des credentials

En cas de changement du mot de passe du compte NAS, le fichier XML doit être régénéré sur chaque site. Procédure :

10. Se connecter sous le compte de service du site concerné
11. Supprimer l'ancien fichier XML : Remove-Item 'C:\Scripts\Backup\creds\nas-cred.xml'
12. Régénérer le fichier avec le nouveau mot de passe : même procédure que l'INIT
13. Valider une exécution manuelle du script de sauvegarde

> ⚠ **En cas de changement du compte de service (SID différent), le fichier XML doit obligatoirement être régénéré même si le mot de passe NAS n'a pas changé — DPAPI lie le secret au SID du compte.**