Mode Opératoire

Rotation périodique des mots de passe critiques

Code :	MO-AD-008
Version :	1.0
Date :	14 avril 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	14/04/2026	Création initiale — procédure exécutée et validée (Sprint 2 : T17, T18, T19)

1 Objet

Ce mode opératoire décrit la procédure de **rotation périodique des mots de passe critiques** de l'infrastructure BTS SIO : comptes administrateur Active Directory, comptes `root`/`admin` des firewalls OPNsense, du NAS QNAP et de la supervision Zabbix. Le compte `krbtgt` fait l'objet du mode opératoire dédié **MO-AD-002**.

Fréquence recommandée : tous les six mois, ou immédiatement après un soupçon de compromission (audit *password spraying*, fuite détectée, départ d'un administrateur).

⚠ Contexte initial

Avant la première exécution de cette procédure (14/04/2026), la majorité de ces mots de passe étaient identiques (« MDP unique réutilisé ») et inchangés depuis novembre 2022 (1 252 jours pour le compte *Administrateur* AD, 1 404 jours pour `krbtgt`). Le compte `Administrateur` était notamment découvert en moins d'une heure par un test *password spraying*.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Systèmes ciblés	DC1+DC2 (AD), OPNsense 1 (10.0.112.1), OPNsense 2 (10.0.112.101, si actif), NAS QNAP Scotty (10.0.112.5), Zabbix (10.0.112.190 web et SSH)
Outils	PowerShell + WinRM, `requests` (Python), Playwright (headless Chromium), Bitwarden CLI
Authentification	Compte Domain Admin pour AD, vault Vaultwarden pour le reste (admin@bts.sio)
Durée	90 minutes pour la séquence complète
Présentiel requis	Recommandé (accès LAN direct évite la rupture VPN/WinRM en cas d'incident sur OPNsense ou DC1)

3 Prérequis

Prérequis

— **MO-AD-005 exécuté** : réplication AD saine, FSMO accessibles, services AD UP
— **MO-AD-006 exécuté** : backup SystemState récent (< 7 jours) avant toute rotation AD
— Accès WinRM aux deux DCs (`10.0.112.2` et `10.0.112.3`)
— Vault Vaultwarden déverrouillé (`bw unlock -raw`)
— Connexion HTTP (et non HTTPS, voir dépannage) au firewall OPNsense
— Playwright Python installé sur le poste d'administration : `pip install playwright && playwright install chromium`
— Symétrie horaire : prévoir une fenêtre de 90 min sans cours pour minimiser l'impact d'une coupure

Cache NTLM

Après la rotation du mot de passe AD (étape 5.3), l'*ancien* mot de passe reste accepté pendant environ une heure via le cache NTLM des contrôleurs de domaine. C'est un comportement attendu de Windows et non une faille de la rotation. Ne pas confondre avec un échec de propagation.

4 Politique de génération des mots de passe

Règle	Justification
24 caractères minimum	Au-delà de la cible ANSSI (12) et FGPP-Admins (16)
Charset `[A-Za-z0-9!@#%_+=.]`	Évite les caractères problématiques (apostrophe, dollar, backslash) qui cassent l'échappement shell/PowerShell/SQL
Génération cryptographique	`secrets.choice` (Python) ou `openssl rand`, jamais `Math.random` ou `$RANDOM`
Un mot de passe par système	Aucun partage entre AD, OPNsense, NAS, Zabbix
Stockage exclusif Vaultwarden	Aucun fichier en clair, aucune note papier persistante

Génération en ligne de commande :

```
python3 -c "
import secrets, string
chars = string.ascii_letters + string.digits + '!@#%_+-=.'
print(''.join(secrets.choice(chars) for _ in range(24)))"
```

5 Procédure

⚠ Ordre d'exécution

Suivre l'ordre ci-dessous **périphériques avant AD** : si la rotation AD échoue, on conserve l'accès aux firewalls et au NAS pour intervenir. L'inverse n'est pas vrai.

5.1 Pré-vérifications (T00)

Étape 1 — Santé AD avant intervention

Sur DC1 via WinRM :

```
repadmin /replsummary        # 0 echec/0 erreur
Get-Service NTDS, kdc, DNS, Netlogon, W32Time
netdom query fsmo
wbadmin get versions         # backup SystemState < 7 jours
```

Toute anomalie (échec de réplication, service arrêté, backup ancien) doit être corrigée **avant** de continuer.

5.2 Rotation OPNsense (T18)

HTTP plutôt qu'HTTPS

Depuis le VLAN pédagogique (10.0.232.0/16), les requêtes HTTPS 443 vers `10.0.112.1` sont souvent en timeout (règle de filtrage). Le port HTTP 80 répond et permet le scripting. Pas de risque : la session reste interne au LAN d'administration.

Étape 2 — Anti-CSRF dynamique

OPNsense utilise un anti-CSRF dont **le nom du champ ET la valeur** sont aléatoires à chaque requête. Les extraire avant chaque POST :

```
import re, requests
s = requests.Session()
r = s.get('http://10.0.112.1/')
m = re.search(r'<input type="hidden" name="([A-Za-z0-9_-]+)"
    value="([A-Za-z0-9_-]+)"', r.text)
csrf_name, csrf_value = m.group(1), m.group(2)
```

Étape 3 — Login + changement de mot de passe

```
# 1. Login
s.post('http://10.0.112.1/', data={
    csrf_name: csrf_value,
    'usernamefld': 'admin',
    'passwordfld': OLD_PW,
    'login': '1',
})

# 2. Recuperer le formulaire de changement de mot de passe
r = s.get('http://10.0.112.1/system_usermanager_passwordmg.php')
m = re.search(r'<input type="hidden" name="([A-Za-z0-9_-]+)"
   value="([A-Za-z0-9_-]+)"', r.text)
csrf_name, csrf_value = m.group(1), m.group(2)

# 3. POST nouveau mot de passe
s.post('http://10.0.112.1/system_usermanager_passwordmg.php', data={
    csrf_name: csrf_value,
    'passwordfld0': OLD_PW,    # ancien
    'passwordfld1': NEW_PW,    # nouveau
    'passwordfld2': NEW_PW,    # confirmation
    'save': 'Sauvegarder',
})
# -> 302 Location: ?savemsg=Saved+settings+for+user
```

Étape 4 — Validation

Tester avec une session fraîche : login avec le *nouveau* MDP doit redirecter vers `/ui/core/dashboard`, login avec l'*ancien* MDP doit rester sur la page de login (HTTP 200 sans redirection).

Pour OPNsense 2 (10.0.112.101) : répéter la même procédure si le firewall est joignable (cluster CARP). En son absence (`ping` échoue), reporter et notifier.

5.3 Rotation NAS QNAP via Playwright (T19)

⚠ QTS 4.2.6 EOL

Le NAS Scotty fonctionne sous QTS 4.2.6, en fin de support. Les endpoints REST de modification d'utilisateur (`privRequest.cgi`, `userConfig.cgi`) renvoient HTTP 200 vide **sans appliquer** le changement. Le SSH (port 22) est fermé par défaut. Seule l'automation de l'UI ExtJS via Playwright fonctionne.

Étape 5 — Script Playwright headless

```
import asyncio
from playwright.async_api import async_playwright

async def run():
    async with async_playwright() as p:
        browser = await p.chromium.launch(headless=True,
            args=['--ignore-certificate-errors'])
        ctx = await browser.new_context(ignore_https_errors=True)
        page = await ctx.new_page()
        # Login
        await page.goto('https://10.0.112.5')
        await page.fill('input#username', 'admin')
        await page.fill('input[type="password"]', OLD_PW)
        await page.locator('button:has-text("Login")').first.click()
        await asyncio.sleep(5)              # laisser charger le desktop
    ExtJS
        # Ouvrir Panneau de configuration -> Utilisateurs
        await page.locator('text="Panneau de
    configuration"').first.dblclick()
        await asyncio.sleep(3)
        await page.locator('text="Utilisateurs"').first.click()
        # Ouvrir le dialog Changer mot de passe pour la ligne admin
        await page.locator('tr:has-text("admin") img').first.click()
        await asyncio.sleep(2)
        # Remplir les 3 champs et appliquer
        pwf = page.locator('input[type="password"]')
        await pwf.nth(0).fill(OLD_PW)
        await pwf.nth(1).fill(NEW_PW)
        await pwf.nth(2).fill(NEW_PW)
        await page.locator('button:has-text("Appliquer")').first.click()
        await asyncio.sleep(3)
        await browser.close()

asyncio.run(run())
```

Étape 6 — Validation

QTS déconnecte automatiquement la session après un changement de mot de passe. Tester directement :

```
import base64, requests
b64 = base64.b64encode(NEW_PW.encode()).decode()
r =
    requests.get(f'https://10.0.112.5/cgi-bin/authLogin.cgi?user=admin&pwd={b64}',
                 verify=False)
# Verifier <authPassed><![CDATA[1]]></authPassed>
```

5.4 Rotation Active Directory (T17)

Étape 7 — Set-ADAccountPassword via WinRM DC1

Sur DC1 via WinRM :

```
$Old = ConvertTo-SecureString $env:OLD_PW -AsPlainText -Force
$New = ConvertTo-SecureString $env:NEW_PW -AsPlainText -Force

Set-ADAccountPassword -Identity Administrateur `
    -OldPassword $Old -NewPassword $New `
    -Server (Get-ADDomainController -Discover).HostName[0]

# Forcer la replication immediate
Start-Sleep -Seconds 10
repadmin /syncall /AdeP

# Verifier la propagation sur tous les DCs
foreach ($dc in (Get-ADDomainController -Filter *)) {
    Get-ADUser Administrateur -Server $dc.HostName -Properties
    PasswordLastSet |
        Format-Table SamAccountName, PasswordLastSet
}
```

Étape 8 — Validation WinRM avec nouveau MDP

Tester depuis le poste d'administration :

```
python3 -c "
import winrm
s = winrm.Session('10.0.112.2', auth=('BTS\\\\Administrateur', NEW_PW),
                  transport='ntlm')
print(s.run_cmd('whoami').std_out.decode())"
```

Répéter sur DC2 (`10.0.112.3`). Les deux DCs doivent répondre `bts\administrateur`.

L'ancien MDP reste accepté environ une heure via le cache NTLM : c'est attendu, ne pas s'inquiéter.

5.5 Mise à jour des dépendances aval

Étape 9 — Vaultwarden

Pour chaque système dont le mot de passe vient de changer :

```
export NODE_TLS_REJECT_UNAUTHORIZED=0    # certificat self-signed
export BW_SESSION=$(bw unlock --raw)

# Identifier l'item via 'bw list items | jq'
ITEM_ID=$(bw list items --search "OPNsense 1" | jq -r '.[0].id')
bw get item $ITEM_ID | jq '.login.password = "<NOUVEAU_MDP>"' \
    | bw encode | bw edit item $ITEM_ID
bw sync
```

Items à mettre à jour : `DC1`, `DC2` (même MDP AD), `OPNsense 1`, `OPNsense 2`, `Scotty -- NAS QNAP TS-439`.

Étape 10 — Fichier `nas.cred` sur DC1

Si le mot de passe du NAS a changé, mettre à jour le fichier d'authentification utilisé par le script de backup : voir **MO-AD-006 §4.6**. Résumé :

```
$nouveau = "admin|<NOUVEAU_MDP_NAS>"
Set-Content -Path 'C:\Backups-AD\nas.cred' -Value $nouveau -NoNewline
# L'ACL existante (SYSTEM + Administrators) est preservee par
    Set-Content.
```

Tester immédiatement la connexion SMB pour valider : `net use Y: \\10.0.112.5\"Partage NAS" /user:admin <NOUVEAU>`.

6 Vérification — Grille récapitulative

Vérification

Cocher chaque point après la rotation :

OPNsense

- ☐ Login Web avec nouveau MDP → dashboard accessible
- ☐ Login Web avec ancien MDP → refusé
- ☐ Vaultwarden item *OPNsense 1* mis à jour
- ☐ OPNsense 2 traité ou explicitement reporté

NAS QNAP

- ☐ `authLogin.cgi` avec nouveau MDP → `authPassed=1`
- ☐ `authLogin.cgi` avec ancien MDP → `authPassed=0`
- ☐ Vaultwarden item *Scotty* mis à jour
- ☐ Fichier `C:\Backups-AD\nas.cred` mis à jour (ACL préservée)
- ☐ `net use` test réussi avec nouveau MDP

Active Directory

- ☐ `PasswordLastSet` sur les 2 DCs = aujourd'hui
- ☐ WinRM DC1 et DC2 répondent avec le nouveau MDP
- ☐ Vaultwarden items *DC1* et *DC2* mis à jour
- ☐ Backup SystemState planifié suivant pris en compte le nouveau MDP NAS (cf. `nas.cred`)

7 Rollback

Cible	Procédure de retour arrière
OPNsense	Console physique (option *3) Reset the root password* dans le menu CLI). Nécessite un accès clavier/écran sur le boîtier.
NAS QNAP	Bouton de reset physique sur le boitier (10 secondes appuyé). Réinitialise le mot de passe `admin` à la valeur d'usine **sans toucher aux données**.
Active Directory	Utiliser un autre compte Domain Admin pour réinitialiser `Administrateur` : `Set-ADAccountPassword -Identity Administrateur -Reset -NewPassword $X`. En dernier recours, mode DSRM via la console serveur.

Rollback Vaultwarden : Vaultwarden conserve l'historique des modifications par item (*Attachments & History* dans l'UI web). On peut copier la valeur précédente si on a fait une erreur de saisie.

8 Dépannage

Problème	Solution
OPNsense HTTPS 443 timeout depuis le VLAN pédagogique	Utiliser HTTP 80 (le serveur répond et la session reste interne au LAN). Si HTTP échoue aussi, basculer sur l'IP de management depuis le VLAN admin.
QNAP : le dialog « Changer mot de passe » ne se trouve pas par texte	L'icône est une `<img>` sans tooltip dans QTS 4.2. Cliquer la **première img** de la ligne `admin` : `page.locator('tr:has-text("admin") img').first.click()`.
QNAP : `authPassed=0` avec le nouveau MDP	Le caractère `&` ou `=` dans le MDP n'est pas accepté. Re-générer en restreignant à `[A-Za-z0-9!@#%_+=.]` (la police définie en section 4).
AD : `Set-ADAccountPassword` échoue (`Access denied`)	Vérifier que le compte WinRM utilisé a bien le droit de changer le MDP `Administrateur`. Le compte doit être Domain Admin et l'ACL `AdminSDHolder` ne doit pas être polluée.
AD : ancien MDP encore accepté après rotation	Cache NTLM : phénomène attendu pendant 1 heure. Pour purger immédiatement : redémarrer le service `Netlogon` sur les DCs (impacte les sessions actives).
Vaultwarden CLI : `self signed certificate`	Exporter `NODE_TLS_REJECT_UNAUTHORIZED=0` avant tout appel `bw`.
Backup T43 échoue après rotation NAS	Le fichier `nas.cred` n'a pas été mis à jour. Vérifier son contenu et l'ACL (cf. MO-AD-006 §4.6).