RODC Windows Server 2025 : Déploiement Sécurisé et Durcissement

RODC Windows Server 2025 : déploiement sécurisé, Password Replication Policy, KRBTGT isolé, attaques possibles et durcissement. Guide expert ANSSI 2026.

Le Read-Only Domain Controller (RODC) est une variante du contrôleur de domaine Active Directory introduite avec Windows Server 2008 et consolidée dans Windows Server 2025 avec des améliorations notables en matière de sécurité et de résilience. En 2026, dans un contexte de multiplication des sites distants, des filiales industrielles déconnectées et des architectures zero-trust imposées par NIS 2, le RODC n'est plus un simple compromis de bande passante : il est devenu un composant stratégique de défense en profondeur. Son principe fondamental — ne stocker en local que les secrets strictement nécessaires, refuser toute écriture non répliquée, présenter une surface d'attaque réduite — répond directement aux exigences de l'ANSSI en matière de segmentation des privilèges Active Directory. Pour un RSSI gérant des sites industriels à Lyon, Toulouse ou Bordeaux, comprendre le RODC, c'est maîtriser la frontière entre un DC compromis qui reste isolé et un DC compromis qui devient une tête de pont vers l'annuaire central. Ce guide expert couvre l'architecture, la Password Replication Policy, le compte KRBTGT isolé, les vecteurs d'attaque réels et le durcissement complet pour un déploiement conforme aux recommandations ANSSI 2025-2026.

📋 EN BREF

ATTAQUES ACTIVE DIRECTORY

RODC Windows Server 2025 : Sécurité et Durcissement

Prérequis et architecture RODC

Le déploiement d'un RODC sous Windows Server 2025 requiert un niveau fonctionnel de domaine (DFL) minimum de Windows Server 2003, mais exploiter l'ensemble des fonctionnalités de sécurité modernes — notamment la granularité de la PRP fine et les améliorations Kerberos de Windows Server 2025 — impose un DFL Windows Server 2016 ou supérieur. Le niveau fonctionnel de forêt (FFL) doit lui aussi atteindre au moins Windows Server 2003.

> ⚡ **Retour terrain**
>
> Dans mes missions de hardening Active Directory, le point le plus sous-estimé est la gestion du groupe 'Opérateurs de compte' et des délégations personnalisées créées au fil des années. Pour un groupe logistique de 1 500 utilisateurs, j'ai trouvé 312 ACL personnalisées dont 89 accordaient des permissions d'écriture sur des attributs sensibles (adminCount, memberOf sur groupes privilégiés) à des comptes d'utilisateurs standards. La dette technique en sécurité AD est souvent invisible jusqu'au premier audit sérieux.

Positionnement réseau

Le RODC se déploie dans des contextes où le contrôleur de domaine en lecture-écriture (RWDC) ne peut ou ne doit pas être installé :

Critère	RWDC	RODC
Sécurité physique du site	Datacenter sécurisé	Filiale, usine, agence
Écriture dans AD	Oui	Non (renvoi vers RWDC)
Stockage credentials	Tous les comptes du domaine	Uniquement comptes PRP-allowed révélés
Compte KRBTGT	KRBTGT partagé domaine	KRBTGT_RxxxxX dédié
Impact compromission	Domaine entier en danger	Limité aux comptes révélés + site local
Administration locale	Domain Admins	Groupe RODC dédié (non DA)

En termes de topologie réseau, le RODC doit pouvoir joindre un RWDC via le port 389 (LDAP), 636 (LDAPS), 88 (Kerberos), 53 (DNS) et 135/dynamique (RPC réplication). Il est recommandé de filtrer ce flux via un pare-feu applicatif, en n'autorisant que les flux de réplication AD depuis le RWDC hub vers le RODC, et non l'inverse.

Différences fonctionnelles clés RWDC vs RODC

Le RODC ne traite pas les modifications d'attributs AD. Toute tentative d'écriture (changement de mot de passe, modification d'objet) est renvoyée — via un referral LDAP — vers le RWDC hub le plus proche dans le site AD. Cette caractéristique protège l'intégrité de l'annuaire central mais impose une connectivité réseau minimale vers le hub pour les opérations d'authentification de comptes non encore cachés localement.

Le RODC expose un filtre d'attributs (*Filtered Attribute Set*, FAS) qui lui permet d'exclure certains attributs sensibles de la réplication descendante. Cela signifie que même si un attaquant extrait le NTDS.dit du RODC, des attributs comme `ms-Mcs-AdmPwd` (LAPS) ou des attributs d'applications métier sensibles peuvent être absents de la copie locale.

Password Replication Policy (PRP)

La Password Replication Policy est le mécanisme central qui détermine quels comptes peuvent avoir leurs credentials mis en cache localement sur le RODC. Une PRP mal configurée est le

vecteur d'attaque le plus fréquent sur les déploiements RODC : trop permissive, elle expose des comptes à privilèges ; trop restrictive, elle génère une charge réseau excessive et des délais d'authentification.

Groupes par défaut

À l'installation, Windows crée deux groupes de domaine :

Allowed RODC Password Replication Group — vide par défaut. Les membres peuvent voir leurs credentials mis en cache sur n'importe quel RODC du domaine.

Denied RODC Password Replication Group — contient par défaut : Domain Admins, Enterprise Admins, Group Policy Creator Owners, Domain Controllers, Read-only Domain Controllers, Schema Admins, Cert Publishers, Account Operators, Server Operators, Backup Operators, Replicator et le compte KRBTGT principal.

Ces groupes s'appliquent à l'échelle du domaine. Pour une granularité par RODC, il faut configurer la PRP directement sur l'objet ordinateur du RODC dans AD, via les attributs `msDS-RevealOnDemandGroup` (allowed) et `msDS-NeverRevealGroup` (denied).

Stratégie PRP recommandée par l'ANSSI

L'ANSSI recommande dans son guide AD 2024 une approche minimaliste :

Créer un groupe de sécurité dédié par RODC : `RODC-Site-Lyon-PRP-Allowed`

N'y placer que les comptes utilisateurs et de service du site local

Exclure explicitement tous les comptes Tier 0 et Tier 1 (voir modèle de tiering AD)

Jamais ajouter de compte avec droits d'administration domaine dans le groupe allowed

Auditer mensuellement la liste des comptes révélés (*revealed accounts*)

Comptes cachés vs comptes révélés

La distinction est critique : un compte est *cached* (dans la PRP allowed) si sa politique l'autorise, mais il devient *revealed* uniquement lorsque le RODC a effectivement demandé et stocké son

hash au RWDC. L'audit des comptes révélés est donc plus représentatif du risque réel qu'un audit de la PRP seule.

```
 # Vérifier le cache PRP sur un RODC
Get-ADDomainControllerPasswordReplicationPolicy -Identity "RODC-SITE01" -AllowedList
Get-ADDomainControllerPasswordReplicationPolicy -Identity "RODC-SITE01" -DeniedList

# Voir les comptes dont le mot de passe est caché dans le RODC
Get-ADDomainControllerPasswordReplicationPolicyUsage -Identity "RODC-SITE01" -AuthenticatedAccoun

# Lister les comptes RÉVÉLÉS (credentials cachés sur le RODC)
Get-ADDomainControllerPasswordReplicationPolicyUsage -Identity "RODC-SITE01" -RevealedAccounts

# Réinitialiser le KRBTGT du RODC (rotation)
$rodc = Get-ADDomainController -Identity "RODC-SITE01"
$krbAcct = $rodc.ComputerObjectDN | Get-ADObject -Properties msDS-KrbTgtLink | Select -Expand msD
Set-ADAccountPassword -Identity $krbAcct -Reset -NewPassword (ConvertTo-SecureString -AsPlainText

# Promouvoir un RODC Windows Server 2025
Install-ADDSDomainController `
    -DomainName "corp.example.fr" `
    -ReadOnlyReplica `
    -SiteName "Site-Filiale-Lyon" `
    -AllowPasswordReplicationAccountName @("RODC-PRP-Allowed") `
    -DenyPasswordReplicationAccountName @("Domain Admins","Enterprise Admins","KRBTGT") `
    -InstallDns:$true `
    -NoGlobalCatalog:$false `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "C0mpl3x!DSRM#2025" -AsPlainText -Forc
```

Le compte KRBTGT isolé de chaque RODC

C'est l'une des protections les plus importantes — et les moins comprises — de l'architecture RODC. Chaque RODC possède un compte KRBTGT dédié, nommé `KRBTGT_RxxxxX` où *RxxxxX* est l'identifiant numérique du RODC dans Active Directory. Ce compte est distinct du compte KRBTGT principal du domaine.

Pourquoi deux comptes KRBTGT ?

Lorsqu'un utilisateur s'authentifie auprès d'un RODC, le Ticket Granting Ticket (TGT) qu'il reçoit est signé avec la clé du `KRBTGT_RxxxxX` local, pas avec la clé du KRBTGT domaine. Ce TGT est marqué avec un flag spécial indiquant qu'il a été émis par un RODC. Lorsque ce TGT est présenté à un RWDC pour obtenir un Service Ticket, le RWDC vérifie ce flag et re-valide le TGT auprès du RWDC hub si nécessaire.

Conséquence directe : si un attaquant compromet un RODC et extrait la clé du `KRBTGT_RxxxxX`, il peut forger des Golden Tickets — mais uniquement valables pour les services du site local servis par ce RODC. Le KRBTGT principal du domaine reste intact. Contrairement à une compromission classique décrite dans notre article sur les attaques Golden Ticket Kerberos, le rayon d'action reste limité au périmètre du site.

Rotation indépendante du KRBTGT RODC

La rotation du `KRBTGT_RxxxxX` est indépendante de la rotation du KRBTGT principal. En cas de compromission avérée d'un RODC, la procédure est :

Isoler réseau le RODC compromis immédiatement

Réinitialiser le mot de passe du `KRBTGT_RxxxxX` deux fois à 10 heures d'intervalle (durée de vie max d'un TGT)

Nettoyer la liste des comptes révélés — réinitialiser les mots de passe de chaque compte exposé

Audit des mouvements latéraux depuis le site compromis vers le hub (voir protection NTDS.dit)

Ne pas réintégrer le RODC sans réinstallation complète de l'OS

Pour la rotation préventive régulière du KRBTGT RODC, consultez notre procédure détaillée dans l'article rotation KRBTGT sécurisée par PowerShell.

Lien objet msDS-KrbTgtLink

L'attribut `msDS-KrbTgtLink` sur l'objet ordinateur du RODC dans AD pointe vers le Distinguished Name du compte `KRBTGT_RxxxxX` associé. Cet attribut est en lecture seule pour les administrateurs et ne peut être modifié manuellement. Sa valeur permet d'identifier sans

ambiguïté quel compte KRBTGT appartient à quel RODC, utile lors des investigations forensiques.

Déploiement pas à pas d'un RODC Windows Server 2025

Étape 1 : Préparation de l'infrastructure

Avant la promotion, vérifier que le schéma AD est bien à la version Windows Server 2016+ (`adprep /forestprep` si nécessaire), que le site AD du site distant est créé dans Sites and Services, et que le lien de site avec le hub est configuré avec un coût et une fréquence de réplication appropriés.

```
 # Vérifier la version du schéma AD
Get-ADObject (Get-ADRootDSE).schemaNamingContext -Property objectVersion | Select objectVersion
# objectVersion 88 = Windows Server 2019/2022, 87 = Windows Server 2016

# Créer le site AD si absent
New-ADReplicationSite -Name "Site-Filiale-Lyon"
New-ADReplicationSubnet -Name "10.10.20.0/24" -Site "Site-Filiale-Lyon"
New-ADReplicationSiteLink -Name "Hub-Lyon" -SitesIncluded @("Default-First-Site-Name","Site-Filia

# Créer les groupes PRP dédiés au RODC
New-ADGroup -Name "RODC-Lyon-PRP-Allowed" -GroupScope DomainLocal -GroupCategory Security
New-ADGroup -Name "RODC-Lyon-PRP-Denied" -GroupScope DomainLocal -GroupCategory Security
# Ajouter les comptes Tier0/Tier1 dans Denied
Add-ADGroupMember -Identity "RODC-Lyon-PRP-Denied" -Members "Domain Admins","Enterprise Admins","
```

Étape 2 : Installation du rôle AD DS et promotion RODC

```
 # Installer le rôle AD DS sur Windows Server 2025
Install-WindowsFeature AD-Domain-Services -IncludeManagementTools

# Promouvoir en RODC
Import-Module ADDSDeployment
Install-ADDSDomainController `
    -DomainName "corp.example.fr" `
    -ReadOnlyReplica `
    -SiteName "Site-Filiale-Lyon" `
    -AllowPasswordReplicationAccountName @("RODC-Lyon-PRP-Allowed") `
    -DenyPasswordReplicationAccountName @("RODC-Lyon-PRP-Denied","Domain Admins","Enterprise Admi
    -DelegatedAdministratorAccountName "RODC-Lyon-LocalAdmin" `
    -InstallDns:$true `
    -NoGlobalCatalog:$false `
    -CriticalReplicationOnly:$false `
    -SafeModeAdministratorPassword (ConvertTo-SecureString "C0mpl3x!DSRM#2025" -AsPlainText -Forc
    -Force:$true
```

Étape 3 : Vérification post-déploiement

```
 # Vérifier que le DC est bien en ReadOnly
Get-ADDomainController -Identity "RODC-SITE01" | Select IsReadOnly, Site, OperationMasterRoles

# Vérifier le compte KRBTGT dédié
$rodc = Get-ADDomainController -Identity "RODC-SITE01"
$krbLink = Get-ADObject $rodc.ComputerObjectDN -Properties "msDS-KrbTgtLink" | Select -Expand "ms
Write-Host "KRBTGT RODC: $krbLink"

# Tester la réplication depuis le RWDC
repadmin /showrepl RODC-SITE01
repadmin /replsummary

# Vérifier la PRP effective
Get-ADDomainControllerPasswordReplicationPolicy -Identity "RODC-SITE01" -AllowedList
Get-ADDomainControllerPasswordReplicationPolicy -Identity "RODC-SITE01" -DeniedList
```

Attaques possibles sur un RODC

Le RODC réduit significativement la surface d'attaque mais ne l'élimine pas. Comprendre les vecteurs d'attaque spécifiques au RODC est essentiel pour dimensionner correctement les contre-mesures. Pour une vision complète des attaques sur l'Active Directory, consultez notre guide de sécurisation AD.

1. Extraction du NTDS.dit local

Le NTDS.dit du RODC contient les hashes des comptes *révélés*. Un attaquant avec accès physique ou administrateur local peut extraire ce fichier avec les mêmes techniques que sur un RWDC (VSS shadow copy, ntdsutil, framework comme Impacket). La différence : seuls les hashes des comptes dans la PRP-allowed **et** qui se sont authentifiés sur ce RODC sont présents. Si la PRP est correctement configurée avec uniquement des comptes locaux non-privilégiés, l'impact reste limité au site compromis.

La protection contre ce vecteur passe par BitLocker (voir section durcissement) et la supervision de l'accès physique. Pour les techniques d'extraction et de protection du NTDS.dit, référez-vous à notre article dédié sur l'extraction et la protection des secrets AD.

2. Extraction et utilisation du KRBTGT_RxxxxX

Si un attaquant obtient les droits SYSTEM sur le RODC (via exploit local, RCE, ou accès physique), il peut extraire le hash du `KRBTGT_RxxxxX` via mimikatz (`lsadump::dcsync /domain:corp.example.fr /dc:RODC-SITE01 /user:KRBTGT_R1234`) et forger des Golden Tickets valables pour le site. Ces tickets sont rejetés par les RWDC pour les ressources du domaine central, mais acceptés localement.

Le risque est d'utiliser ces tickets forgés pour élever les privilèges dans le périmètre local du RODC — notamment si des comptes de service avec accès au hub sont présents dans la PRP-allowed.

3. Attaque depuis le site compromis vers le hub

Un scénario d'attaque sophistiqué consiste à compromettre le RODC, puis à utiliser les flux de réplication AD autorisés pour tenter une attaque DCSync partielle vers le RWDC. Par défaut, le RODC ne peut pas initier une réplication vers un RWDC (la réplication est unidirectionnelle RWDC → RODC), mais des configurations firewall incorrectes ou des vulnérabilités dans le protocole de réplication peuvent créer des opportunités.

De plus, si des comptes de service ayant accès aux ressources hub ont leur hash caché sur le RODC, l'attaquant peut usurper leur identité via Pass-the-Hash depuis le réseau de la filiale.

4. Attaque sur l'administration locale déléguée

Le paramètre `-DelegatedAdministratorAccountName` lors de la promotion RODC désigne un groupe ayant des droits d'administration locale sur ce RODC **sans être Domain Admin**. Si ce groupe est compromis, l'attaquant obtient un accès élevé au RODC sans pour autant avoir de droits sur le reste du domaine — mais c'est suffisant pour déclencher les attaques 1 et 2 décrites ci-dessus.

Durcissement du RODC Windows Server 2025

BitLocker avec TPM 2.0 — Obligatoire

Le chiffrement intégral du disque est la première ligne de défense contre le vol physique du NTDS.dit. Windows Server 2025 impose TPM 2.0 comme prérequis matériel, rendant BitLocker plus fiable. La configuration minimale recommandée :

```
 # Activer BitLocker avec TPM + PIN (protection maximale)
Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 `
    -TpmAndPinProtector -Pin (ConvertTo-SecureString "DSRM-BitLocker-PIN-2025" -AsPlainText -Forc

# Sauvegarder la clé de récupération dans AD
Backup-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId (Get-BitLockerVolume -MountPoint "C
# Ou sauvegarder dans Azure AD si hybride
BackupToAAD-BitLockerKeyProtector -MountPoint "C:" -KeyProtectorId (Get-BitLockerVolume -MountPoi
```

Filtered Attribute Set (FAS)

Configurer le Filtered Attribute Set permet d'exclure des attributs sensibles de la réplication vers le RODC. Les attributs contenant des secrets d'applications (tokens, clés API chiffrées) et `ms-Mcs-AdmPwd` (LAPS) doivent impérativement figurer dans le FAS. La configuration se fait via le schéma AD (attribut `searchFlags` avec le bit 9 = 0x200).

Sécurisation de la réplication DFS-R

Si SYSVOL est répliqué via DFS-R (obligatoire en niveau fonctionnel Windows Server 2008 R2+), sécuriser les flux DFS-R entre le RWDC hub et le RODC :

Activer le chiffrement RPC pour DFS-R :

`HKLM\SYSTEM\CurrentControlSet\Services\DFSR\Parameters\RPC Use Encryption = 1`

Restreindre les connexions DFS-R aux seules adresses IP du RWDC hub autorisé

Surveiller les modifications de GPO répliquées vers le RODC (un attaquant RWDC peut pousser des GPO malveillantes)

Hardening Windows Server 2025 spécifique RODC

```
 # Désactiver les services inutiles sur un RODC (non nécessaires en site distant)
Stop-Service -Name "CertPropSvc","KtmRm","NetLogon" -Force  # Vérifier avant de désactiver NetLog
Set-Service -Name "CertPropSvc" -StartupType Disabled

# Activer le pare-feu Windows avec règles strictes
Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True

# Restreindre RDP aux seuls administrateurs du site
$rdpRule = Get-NetFirewallRule -DisplayName "Remote Desktop*" | Where-Object {$_.Direction -eq "I
Set-NetFirewallRule -InputObject $rdpRule -RemoteAddress "10.0.0.0/8"  # Adapter à la plage résea

# Configurer le Local Administrator Password Solution (LAPS) v2
Set-LapsADComputerSelfPermission -Identity "OU=RODC,DC=corp,DC=example,DC=fr"

# Activer Windows Defender Credential Guard si matériel compatible
# (protège les secrets LSASS contre mimikatz)
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name "EnableVirtuali
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\DeviceGuard" -Name "RequirePlatfor
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LsaCfgFlags" -Value 1
```

Supervision de la réplication depuis le RWDC

Le flux de réplication AD vers le RODC est unidirectionnel (RWDC → RODC). Surveiller ce flux permet de détecter les anomalies :

```
 # Vérifier l'état de réplication depuis le hub
repadmin /showrepl RODC-SITE01 /csv | ConvertFrom-Csv | Where-Object {$_.'Number of Failures' -gt

# Rapport de réplication global
repadmin /replsummary *

# Vérifier les objets répliqués récemment
Get-ADReplicationPartnerMetadata -Target "RODC-SITE01" | Select-Object Partner, LastReplicationSu

# Alerter si la dernière réplication dépasse 4h
$lastRepl = (Get-ADReplicationPartnerMetadata -Target "RODC-SITE01").LastReplicationSuccess
if ((Get-Date) - $lastRepl -gt [TimeSpan]::FromHours(4)) {
    Write-Warning "ALERTE: Réplication RODC-SITE01 en retard de plus de 4 heures"
}
```

Monitoring et audit — Événements Windows spécifiques RODC

La supervision d'un RODC nécessite des politiques d'audit spécifiques, distinctes de celles des RWDC. Les événements suivants sont particulièrement significatifs :

Événement ID	Signification	Criticité
4738	Modification d'un compte utilisateur (inclut les révélations PRP)	Haute
4769	Demande de ticket de service Kerberos (TGS request) — authentifications sur le RODC	Moyenne
4649	Replay Attack détecté — ticket Kerberos réutilisé	Critique
4771	Échec pré-authentification Kerberos	Moyenne
4625	Échec d'ouverture de session NTLM — force brute potentielle	Haute
4741/4742	Création/modification compte ordinateur — RODC ajouté/modifié dans AD	Haute
4706	Nouvelle relation de confiance de domaine créée	Critique
5136	Modification d'un attribut AD — surveiller msDS-RevealOnDemandGroup et msDS-NeverRevealGroup	Haute

Configuration de l'audit sur le RODC

```
 # Activer l'audit avancé sur le RODC via GPO (ou localement)
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Service Ticket Operations" /success:enable /failure:enable
auditpol /set /subcategory:"Computer Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Access" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Changes" /success:enable /failure:enable

# Vérifier la configuration d'audit active
auditpol /get /category:*
```

Intégration SIEM

Pour les filiales industrielles françaises sous obligation NIS 2, les logs du RODC doivent être centralisés vers le SIEM de l'organisation dans les 24 heures. Configurer Windows Event Forwarding (WEF) depuis le RODC vers un Event Collector sur le hub, avec les abonnements filtrés sur les Event IDs critiques listés ci-dessus.

Cas terrain France — Exemples de déploiement RODC

Filiale industrielle à Lyon — Site OT/IT convergé

Un équipementier automobile lyonnais déploie un RODC dans son usine pour authentifier les opérateurs sur les postes SCADA. Contraintes : réseau OT segmenté, bande passante WAN limitée à 10 Mbps partagés avec la téléphonie, accès physique au datacenter local limité mais non-nul.

Configuration retenue : PRP contenant uniquement les 45 comptes opérateurs (pas de comptes IT ni de comptes de service avec accès au hub), BitLocker TPM+PIN, administrateur local délégué = compte de service IT dédié au site (non DA), réplication toutes les 4h pendant les heures de

bureau. Surveillance : WEF vers SIEM central, alerte sur tout événement 4769 avec compte hors PRP-allowed.

Agence gouvernementale à Bordeaux — Faible connectivité

Une préfecture régionale avec 80 agents et une liaison WAN 4 Mbps vers le datacenter ministériel. Le RODC permet l'authentification locale même en cas de panne WAN, avec un cache PRP couvrant 100% des agents du site. Particularité : le poste RODC est dans un local technique verrouillé, mais la clé est partagée avec le responsable logistique — risque physique identifié, compensé par BitLocker TPM+PIN avec le PIN conservé par la DSI centrale.

Entreprise de services numériques à Toulouse — DMZ partenaires

Un intégrateur IT déploie un RODC dans une DMZ pour permettre l'authentification des comptes partenaires externes (prestataires, clients) sans exposer un RWDC dans la zone démilitarisée. PRP strictement vide (aucun compte mis en cache — authentification toujours renvoyée vers le RWDC hub), FAS complet. Le RODC sert ici de proxy d'authentification Kerberos, non de cache de credentials.

Checklist durcissement RODC

À RETENIR

Checklist durcissement RODC Windows Server 2025

☐ **PRP minimale** : uniquement les comptes utilisateurs du site dans le groupe PRP-Allowed dédié par RODC

☐ **Zéro compte Tier 0/Tier 1** dans la PRP-Allowed (vérifier avec `Get-ADDomainControllerPasswordReplicationPolicyUsage -RevealedAccounts`)

☐ **BitLocker XTS-AES 256** avec TPM 2.0 + PIN activé sur le volume système

☐ **Clé BitLocker sauvegardée** dans AD (ou Azure AD) avant chiffrement

☐ **Credential Guard** activé si le matériel supporte la virtualisation (VBS)

☐ **LAPS v2** configuré pour le compte administrateur local du RODC

☐ **Filtered Attribute Set** configuré pour exclure ms-Mcs-AdmPwd et attributs secrets métier

☐ **Administrateur local délégué** = compte de service dédié, non-DA, avec MFA

☐ **RDP restreint** aux seules plages IP du hub d'administration

☐ **DFS-R chiffré** (RPC encryption) pour la réplication SYSVOL

☐ **Pare-feu Windows** activé, règles sortantes restrictives vers le RWDC hub

☐ **Windows Event Forwarding** configuré vers le SIEM central

☐ **Audit mensuel** des comptes révélés et de la liste PRP-Allowed

☐ **Rotation KRBTGT_RxxxxX** annuelle minimum (semestrielle recommandée)

☐ **Plan de compromission documenté** : procédure d'isolation, réinitialisation KRBTGT, reset mots de passe révélés

☐ **Test de restauration** depuis sauvegarde testé semestriellement

FAQ — Questions fréquentes sur le RODC

Un RODC peut-il être compromis même avec la PRP configurée ?

Oui. La PRP limite l'impact d'une compromission mais ne la prévient pas. Un attaquant avec accès physique ou droits SYSTEM sur le RODC peut extraire le NTDS.dit local (contenant les hashes des comptes révélés), le hash du KRBTGT_RxxxxX (permettant des Golden Tickets locaux), et potentiellement utiliser les comptes révélés pour se déplacer latéralement depuis la filiale. La PRP réduit le rayon d'explosion — elle ne remplace pas la sécurité physique, BitLocker, et la supervision active.

Faut-il un KRBTGT différent pour chaque RODC ?

Oui, et c'est automatique. Windows Active Directory crée un compte KRBTGT_RxxxxX unique pour chaque RODC lors de la promotion. Il est impossible — et déconseillé — de partager un compte KRBTGT entre plusieurs RODC. Cette architecture garantit qu'une compromission du KRBTGT d'un RODC n'affecte pas les autres sites ni le domaine central. La rotation de ce compte se fait indépendamment de la rotation du KRBTGT principal du domaine.

Quelle différence entre un RODC et un DC en lecture seule via Syslog ?

La confusion est courante. Un "DC en lecture seule via Syslog" n'existe pas comme concept AD : ce que certains architectes décrivent ainsi est généralement une configuration de journal ou une solution tierce. Le RODC est une fonctionnalité native d'Active Directory avec un compte KRBTGT dédié, une PRP configurable, un NTDS.dit partiel, et des mécanismes de délégation d'administration locale. Il authentifie réellement les utilisateurs en local via Kerberos, alors qu'une solution de journalisation passive ne participe pas au processus d'authentification.

BitLocker est-il obligatoire sur un RODC en filiale ?

Oui, sans exception. Le NTDS.dit d'un RODC, même partiel, contient des hashes de mots de passe. Sans BitLocker, le vol physique du serveur (ou du disque) permet l'extraction offline de ces hashes en quelques minutes, contournant toute protection logicielle. L'ANSSI le recommande explicitement dans son guide AD pour tout contrôleur de domaine hors datacenter sécurisé. Sur Windows Server 2025, BitLocker XTS-AES 256 avec TPM 2.0 est la configuration de base — y ajouter un PIN pour les sites à risque physique élevé.

Comment vérifier qu'aucun compte admin n'est caché sur le RODC ?

Deux vérifications complémentaires sont nécessaires. D'abord, auditer la PRP : `Get-ADDomainControllerPasswordReplicationPolicy -Identity "RODC-SITE01" -AllowedList` pour la liste théorique. Ensuite, et surtout, vérifier les comptes réellement révélés : `Get-ADDomainControllerPasswordReplicationPolicyUsage -Identity "RODC-SITE01" -RevealedAccounts`. Croiser cette liste avec les membres des groupes à privilèges (Domain

Admins, Enterprise Admins, Schema Admins, Tier 0 assets). Si un compte privilégié apparaît dans les comptes révélés, réinitialiser son mot de passe immédiatement et investiguer comment il s'est authentifié sur ce RODC.

Références et documentation

Microsoft Learn — Sécurité Windows Server

ANSSI — Guide de sécurisation Active Directory

MITRE ATT&CK — Techniques Active Directory