# Windows Events à Surveiller sur un Contrôleur de Domaine : Guide SOC 2026

> Les 50 Windows Event IDs critiques à surveiller sur vos contrôleurs de domaine : Kerberos, DCSync, PowerShell. Règles Wazuh et KQL Sentinel incluses.

📋 EN BREF


## En bref

- Event ID 4625 (échec authentification) : première alerte brute-force et password spray sur vos contrôleurs de domaine
- Event ID 4768/4769/4771 (Kerberos) : détection AS-REP Roasting, Kerberoasting, Pass-the-Ticket et Golden Ticket

- Event ID 4672 (attribution droits sensibles) : surveillance élévation de privilèges et comptes à hauts droits
- Event ID 4742 : modification compte ordinateur — vecteur d'attaque RBCD et machine account takeover
- Event ID 5136 (modification objet AD) : détection AdminSDHolder, ACL abuse et préparation DCSync
- Event ID 4662 + réplication DS : signature d'une attaque DCSync avec Mimikatz ou Impacket
- Event ID 1102 : journal d'audit effacé — indicateur de compromission ou d'effacement de traces

Les contrôleurs de domaine (DC) sont le cœur névralgique de toute infrastructure Active Directory et, par extension, la cible prioritaire des attaquants sophistiqués opérant en France et en Europe. En 2025-2026, les équipes SOC françaises font face à une recrudescence des attaques ciblant spécifiquement l'annuaire Active Directory : DCSync pour exfiltrer les hachages NTLM, Kerberoasting pour compromettre les comptes de service, Pass-the-Ticket pour du mouvement latéral discret, ou encore les attaques Golden Ticket qui persistent des mois après la compromission initiale. La directive NIS 2, transposée en droit français et applicable aux OIV et OSE, impose désormais une supervision renforcée des systèmes critiques, dont les contrôleurs de domaine font partie intégrante. L'ANSSI, dans ses guides de recommandations Active Directory, insiste sur la nécessité d'activer une politique d'audit granulaire et de centraliser les Windows Event Logs dans un SIEM. Ce guide SOC 2026 recense les 50 Event IDs Windows incontournables sur les DCs, détaille les techniques d'attaque associées, et fournit des règles de détection prêtes à l'emploi pour Wazuh et Microsoft Sentinel. À destination des analystes SOC, RSSI et ingénieurs sécurité des entreprises françaises, il constitue une référence opérationnelle pour construire un monitoring AD efficace et conforme aux exigences réglementaires.

## Pourquoi surveiller les Events sur les Contrôleurs de Domaine ?

Un contrôleur de domaine traite des milliers d'événements par heure dans un environnement de taille moyenne. Sans filtre ni règle de corrélation, ce volume noie les signaux d'attaque dans le bruit. Pourtant, contrairement aux endpoints classiques, les DCs génèrent des events d'une richesse exceptionnelle : chaque tentative d'authentification Kerberos, chaque modification d'objet Active Directory, chaque réplication entre DCs laisse une trace précise dans les journaux Windows.

> ⚡ **Retour terrain**
>
> Dans les SOC que j'accompagne, le principal problème n'est pas le manque d'alertes mais l'excès : 'alert fatigue' systématique, analysts qui désactivent des règles jugées trop bruyantes sans documentation, et faux positifs récurrents qui masquent les vrais incidents. J'ai développé un tableau de bord simple — 3 métriques : taux de faux positifs par règle, MTTD (mean time to detect) sur incidents réels, et ratio alertes/analyst — qui permet en une réunion hebdomadaire de 30 minutes d'identifier les règles à tuner en priorité.

La spécificité des attaques AD modernes est qu'elles exploitent des fonctionnalités légitimes du protocole : DCSync utilise l'API de réplication, Kerberoasting demande des tickets TGS valides, Pass-the-Hash s'appuie sur l'authentification NTLM standard. Ces attaques ne génèrent pas d'anomalie binaire évidente mais des patterns statistiques et contextuels que seule une supervision fine des Event Logs peut révéler.

Les trois raisons opérationnelles de surveiller intensément les DCs :

**Réduction du temps de détection (MTTD)** : Les attaques APT sur AD durent en moyenne 207 jours avant détection selon les rapports sectoriels. Une supervision des Event IDs critiques permet de détecter les techniques en quelques minutes.

**Conformité NIS 2 / ANSSI** : La directive impose la journalisation, la centralisation et l'analyse des événements de sécurité sur les systèmes critiques. Les DCs sont explicitement dans le périmètre.

**Investigation forensique** : En cas d'incident, les Event Logs du DC constituent la source de vérité pour reconstituer la chaîne d'attaque et identifier le patient zéro.

Pour aller plus loin sur la configuration de Sysmon sur les contrôleurs de domaine, consultez notre article sur la configuration Sysmon pour contrôleurs de domaine en 2026, qui complète ce guide avec la télémétrie au niveau des processus.

## Events d'Authentification Critiques (Kerberos et NTLM)

Les events d'authentification sont le premier vecteur de détection des attaques sur Active Directory. Ils couvrent aussi bien les succès que les échecs, et révèlent les patterns d'attaque les plus courants.

### Event ID 4624 — Ouverture de session réussie

**Canal** : Security | **Priorité** : MEDIUM
Enregistre chaque connexion réussie. Le champ *LogonType* est crucial : type 3 (réseau) depuis un poste inhabituel, type 10 (RemoteInteractive/RDP) depuis une IP externe, ou type 9 (NewCredentials / Pass-the-Hash via runas /netonly). Surveiller les types 3 depuis des comptes à hauts privilèges en dehors des plages horaires habituelles.

### Event ID 4625 — Échec d'authentification

**Canal** : Security | **Priorité** : HIGH
Indicateur principal de brute-force et password spray. Le sous-code *Status/SubStatus* précise la cause : 0xC000006A (mauvais mot de passe), 0xC0000064 (compte inexistant), 0xC000006D (restrictions logon). Un password spray génère de nombreux 4625 avec SubStatus 0xC000006A sur des comptes différents depuis une même IP source.

### Event ID 4627 — Appartenance aux groupes

**Canal** : Security | **Priorité** : LOW
Complément du 4624, liste les groupes du compte au moment de la connexion. Utile pour vérifier les droits effectifs d'un compte lors d'une investigation.

### Event ID 4648 — Connexion avec credentials explicites

**Canal** : Security | **Priorité** : HIGH
Généré lors d'un `runas` ou d'une connexion avec credentials différents. Technique utilisée dans le mouvement latéral (Pass-the-Hash avec `runas /netonly`). Alerter si le compte source est un compte de service ou si l'IP destination est un DC.

### Event IDs Kerberos : 4768, 4769, 4770, 4771

**4768 — Demande de Ticket TGT (AS-REQ)** | Canal : Security | Priorité : HIGH
Enregistre chaque demande de Ticket Granting Ticket. L'AS-REP Roasting cible les comptes avec l'attribut `DONT_REQUIRE_PREAUTH` : la demande TGT réussit sans authentification préalable, livrant un hash craquable offline. Indicateur : *PreAuthType = 0* dans le champ d'audit.

**4769 — Demande de Ticket de Service (TGS-REQ)** | Canal : Security | Priorité : CRITICAL
Event le plus surveillé pour le Kerberoasting. Champs critiques :

*TicketEncryptionType = 0x17* (RC4-HMAC) : type de chiffrement faible, signe de Kerberoasting

*ServiceName* : si c'est un compte avec SPN, demande de ticket suspecte

Nombreuses demandes TGS RC4 en quelques secondes depuis un même client = Kerberoasting automatisé

Le Pass-the-Ticket se manifeste par des demandes TGS depuis une IP source différente de la machine du compte propriétaire du TGT.

**4770 — Renouvellement de Ticket TGT** | Canal : Security | Priorité : MEDIUM
Un Golden Ticket expirera normalement après 10 ans (durée configurée par Mimikatz par défaut). Des renouvellements de tickets avec des durées anormales (> 10h standard) méritent investigation.

**4771 — Échec d'authentification Kerberos (KDC)** | Canal : Security | Priorité : HIGH
Équivalent Kerberos du 4625 NTLM. Code d'erreur 0x18 = mauvais mot de passe (brute-force Kerberos). Code 0x25 = horloge désynchronisée (> 5 min, souvent signe de manipulation). Code 0x6 = compte inexistant (enumération de comptes).

### Event ID 4776 — Authentification NTLM (NTLM Validate)

**Canal** : Security | **Priorité** : HIGH
Généré lors d'une authentification NTLM sur le DC. Les attaques NTLM Relay (ntlmrelayx) génèrent des authentifications NTLM depuis des sources inattendues. Surveiller aussi les downgrades NTLM v1 : *PackageName = NTLM V1* indique un client négociant en NTLMv1, vulnérable au cracking avec des tables arc-en-ciel.

Pour comprendre la relation entre ces events et Wazuh, notre article sur la détection des attaques Active Directory avec Wazuh détaille les règles de corrélation.

---

## Events de Modifications Active Directory (Objets et Permissions)

Les modifications d'objets Active Directory sont particulièrement sensibles car elles permettent aux attaquants d'établir une persistance ou de préparer une élévation de privilèges. Ces events proviennent du canal Security et nécessitent l'activation de la catégorie d'audit "DS Access".

### Events de gestion des comptes utilisateurs (472x)

**4720** — Création d'un compte utilisateur | Priorité : HIGH — Alerter si créé hors processus ITSM, surtout en dehors des heures ouvrées

**4722** — Compte activé | Priorité : MEDIUM — Activation d'un compte dormant peut indiquer une réactivation de backdoor

**4723** — Changement de mot de passe (par l'utilisateur) | Priorité : LOW

**4724** — Réinitialisation de mot de passe (par admin) | Priorité : HIGH — Si réalisé sur un compte privilégié par un compte non-helpdesk

**4725** — Compte désactivé | Priorité : MEDIUM — Désactivation du compte KRBTGT pourrait indiquer une attaque DC

**4726** — Suppression d'un compte | Priorité : HIGH — Suppression de compte admin = effacement de traces

### Events de gestion des groupes (4728-4756)

**4728** — Membre ajouté à un groupe de sécurité global | Priorité : CRITICAL — Addition à Domain Admins, Enterprise Admins, Schema Admins

**4729** — Membre retiré d'un groupe de sécurité global | Priorité : HIGH

**4730** — Groupe de sécurité global supprimé | Priorité : HIGH

**4732** — Membre ajouté à un groupe local | Priorité : HIGH — Addition au groupe local Administrators sur un DC

**4733** — Membre retiré d'un groupe local | Priorité : MEDIUM

**4735** — Groupe de sécurité local modifié | Priorité : HIGH

**4756** — Membre ajouté à un groupe universel | Priorité : HIGH — Groupes universels utilisés dans les forêts multi-domaines

### Events de gestion des comptes machine (4741-4743)

**4741** — Création d'un compte ordinateur | Priorité : HIGH — MAQ (Machine Account Quota) abuse : un utilisateur standard peut créer jusqu'à 10 comptes machine par défaut

**4742** — Modification d'un compte ordinateur | Priorité : CRITICAL — Modification de l'attribut *msDS-AllowedToActOnBehalfOfOtherIdentity* = configuration RBCD (Resource-Based Constrained Delegation) pour élévation de privilèges

**4743** — Suppression d'un compte ordinateur | Priorité : HIGH

Events de modification d'objets AD (4738, 5136, 5137, 5138, 5139)

**4738 — Modification d'un compte utilisateur** | Priorité : CRITICAL
Champs critiques à surveiller : modification de l'attribut *userAccountControl* (activation DONT_REQUIRE_PREAUTH = AS-REP Roasting backdoor), modification du *SIDHistory* (escalade vers d'autres domaines), changement de *scriptPath* (GPO logon script persistence).

**5136 — Modification d'un attribut d'objet DS** | Priorité : CRITICAL
L'event le plus riche pour détecter l'AD abuse. Champs à surveiller :

Modification de *nTSecurityDescriptor* sur OU ou Domain Root = ACL abuse, préparation DCSync

Modification d'AdminSDHolder (*CN=AdminSDHolder,CN=System*) = persistence via SDProp

Ajout d'un SPN sur un compte utilisateur = préparation Kerberoasting

Modification de *msDS-KeyCredentialLink* = Shadow Credentials attack (ADCS abuse)

**5137** — Création d'objet DS | Priorité : HIGH — Création d'une nouvelle GPO ou OU suspecte
**5138** — Désuppression d'objet DS (undelete) | Priorité : HIGH
**5139** — Déplacement d'objet DS | Priorité : MEDIUM

La sécurisation du LDAP signing et channel binding empêche certaines de ces modifications via LDAP non sécurisé. Voir notre guide sur le LDAP signing et channel binding dans Active Directory.

---

## Events de Réplication et DCSync

La réplication Active Directory est un mécanisme légitime entre contrôleurs de domaine. Les attaques DCSync exploitent cette mécanique pour extraire les hachages NTLM de tous les comptes, y compris KRBTGT et les comptes admin, sans avoir besoin d'accès direct aux fichiers NTDS.dit.

### Event ID 4662 — Opération effectuée sur un objet AD

**Canal** : Security | **Priorité** : CRITICAL
C'est l'event clé pour détecter DCSync. Une attaque DCSync génère des 4662 avec :

**ObjectType** : `19195a5b-6da0-11d0-afd3-00c04fd930c9` (domainDNS)

**Properties** incluant : `1131f6aa-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes) ET `1131f6ad-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes-All)

**SubjectUserName** : un compte utilisateur (non DC) effectuant ces opérations = compromission

Les contrôleurs de domaine légitimes génèrent aussi ces events lors de la réplication normale, mais le *SubjectUserName* sera un compte de machine DC (se terminant par $).

### Events de session de réplication DS (4928, 4929, 4932, 4933)

**4928** — Établissement d'une source de nommage de réplication AD | Priorité : HIGH — Un DC inconnu demandant une réplication est suspect

**4929** — Suppression d'une source de nommage de réplication | Priorité : MEDIUM

**4932** — Synchronisation d'un réplica de nommage AD | Priorité : HIGH — Volume anormal de synchronisations depuis un DC peut indiquer DCShadow

**4933** — Fin de synchronisation d'un réplica | Priorité : MEDIUM

**Détection DCShadow** : L'attaque DCShadow (Mimikatz) enregistre temporairement un faux DC dans Active Directory. Elle génère des 4928/4932 depuis une machine non-DC. Corrélation nécessaire avec le registre des DCs légitimes dans l'environnement.

### XPath Query pour DCSync

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">
      *[System[(EventID=4662)]]
      and
      *[EventData[Data[@Name='Properties'] and
        (Data[contains(text(),'1131f6aa-9c07-11d1-f79f-00c04fc2dcd2')] or
         Data[contains(text(),'1131f6ad-9c07-11d1-f79f-00c04fc2dcd2')])]]
    </Select>
  </Query>
</QueryList>
```

---

## Events Système et Services Critiques

Les events système sur les DCs révèlent des techniques de persistance et d'effacement de traces souvent négligées par les équipes SOC focalisées sur les events d'authentification.

### Event ID 4697 — Installation d'un nouveau service

**Canal** : Security | **Priorité** : CRITICAL
Un attaquant ayant compromis un DC peut installer un service malveillant pour la persistance. Champs à surveiller : *ServiceFileName* (chemin inhabituel, UNC path, fichier dans %TEMP%), *ServiceType* (kernel driver = rootkit potentiel), *ServiceAccount* (LocalSystem avec un service suspect).

### Event ID 7045 — Nouveau service installé (System log)

**Canal** : System | **Priorité** : CRITICAL
Complément du 4697, généré dans le canal System. Les outils comme Metasploit, Cobalt Strike

ou PsExec créent des services temporaires. Un service avec un nom aléatoire (ex: `BTOBTO`, `PSEXESVC`) ou un chemin UNC est hautement suspect.

### Event ID 1102 — Journal d'audit de sécurité effacé

**Canal** : Security | **Priorité** : CRITICAL
L'effacement du journal Security Log est une tactique d'effacement de traces (MITRE T1070.001). Cet event lui-même doit déclencher une alerte immédiate P1. À corréler avec les events précédents pour identifier ce qui a été effacé. La politique ANSSI recommande de rendre l'effacement impossible via des permissions restrictives sur le journal.

### Event ID 4719 — Modification de la politique d'audit système

**Canal** : Security | **Priorité** : CRITICAL
Un attaquant cherchant à passer inaperçu peut désactiver la politique d'audit. Toute modification de la politique d'audit sur un DC doit déclencher une alerte immédiate et une investigation.

### Event ID 4906 — Valeur CrashOnAuditFail modifiée

**Canal** : Security | **Priorité** : HIGH
La clé de registre *CrashOnAuditFail* contrôle le comportement du DC si le journal est plein. Sa modification peut indiquer une tentative de saturation du journal pour masquer des activités.

---

## Events PowerShell et WMI (LOLBins sur DC)

PowerShell est l'outil de prédilection des attaquants pour la phase post-exploitation sur les DCs en raison de sa puissance et de son intégration profonde à Windows et Active Directory. Le logging PowerShell doit être activé explicitement via GPO.

### Configuration du logging PowerShell

Trois niveaux de logging PowerShell à activer :

**Module Logging** (Event 4103) : enregistre les sorties de pipeline et paramètres de modules

**ScriptBlock Logging** (Event 4104) : enregistre le code PowerShell déobfusqué — le plus précieux pour la détection

**Transcription** : sauvegarde complète des sessions dans des fichiers texte

### Event ID 4104 — Exécution de ScriptBlock PowerShell

**Canal** : Microsoft-Windows-PowerShell/Operational | **Priorité** : CRITICAL
Cet event enregistre le code PowerShell tel qu'il est réellement exécuté, après déobfuscation.
Patterns suspects à détecter :

`Invoke-Mimikatz`, `Invoke-DCSync`, `Get-ADReplAccount`

`IEX` / `Invoke-Expression` combiné avec `DownloadString` (fileless malware)

`Net.WebClient`, `Invoke-WebRequest` vers des IP externes depuis un DC

Encodage base64 : `-EncodedCommand` ou `[Convert]::FromBase64String`

`Add-DomainGroupMember`, `Set-DomainObject` (PowerView)

### Event ID 4103 — Module PowerShell invoqué

**Canal** : Microsoft-Windows-PowerShell/Operational | **Priorité** : HIGH
Enregistre l'exécution de chaque commande PowerShell avec ses paramètres. Utile pour détecter l'utilisation de modules comme *ActiveDirectory*, *PowerSploit*, ou *PowerView* dans un contexte suspect.

### Events 400, 403, 500, 600, 800 (Windows PowerShell log)

**Canal** : Windows PowerShell | **Priorité** : MEDIUM
Ces events plus anciens enregistrent le cycle de vie des pipelines PowerShell. L'Event 400

(*Engine Lifecycle Started*) avec un *HostApplication* inhabituel (ex: encodé en base64) est un indicateur de lancement de PowerShell malveillant.

### Détection WMI (Windows Management Instrumentation)

WMI est utilisé pour le mouvement latéral et la persistance. Sur les DCs, surveiller :

**Event ID 5857** (Microsoft-Windows-WMI-Activity/Operational) : activité provider WMI

**Event ID 5858** : erreur WMI — peut indiquer une tentative de connexion WMI échouée

**Event ID 5860/5861** : inscription de subscription WMI permanente = persistance WMI

# Tableau de Référence : Top 50 Event IDs à Surveiller

| Event ID | Nom | Canal | Priorité | Attaque associée | Action recommandée |
|---|---|---|---|---|---|
| 4624 | Logon Success | Security | MEDIUM | Pass-the-Hash (type 9), RDP bruteforce (type 10) | Alerter sur LogonType 9 hors heures ouvrées |
| 4625 | Logon Failure | Security | HIGH | Brute-force, Password Spray | Seuil : >10 échecs/minute sur comptes différents |
| 4627 | Group Membership | Security | LOW | Audit des droits effectifs | Archiver pour investigation forensique |
| 4648 | Explicit Credentials Logon | Security | HIGH | Pass-the-Hash, Runas abuse | Alerter si source = compte de service |
| 4662 | DS Object Operation | Security | CRITICAL | DCSync, DCShadow | Alerte immédiate si SubjectUser non-DC |
| 4672 | Special Privileges Assigned | Security | HIGH | Élévation de privilèges | Surveiller SeDebugPrivilege, SeTcbPrivilege |
| 4697 | Service Installed | Security | CRITICAL | Persistance via service (Cobalt Strike, Meterpreter) | Alerte immédiate sur chemin UNC ou %TEMP% |
| 4719 | Audit Policy Changed | Security | CRITICAL | Désactivation audit (T1070) | Alerte P1 immédiate |
| 4720 | User Account Created | Security | HIGH | Backdoor account creation | Alerter si hors heures ouvrées / hors ITSM |
| 4722 | User Account Enabled | Security | MEDIUM | Réactivation compte dormant | Corréler avec 4624 dans les minutes suivantes |
| 4723 | Password Change (self) | Security | LOW | — | Log pour audit RH |
| 4724 | Password Reset (admin) | Security | HIGH | Prise de contrôle de compte | Alerter si cible = compte admin |
| 4725 | User Account Disabled | Security | MEDIUM | Sabotage compte admin | Alerter si cible = KRBTGT ou compte DA |
| 4726 | User Account Deleted | Security | HIGH | Effacement de traces | Alerte si cible = compte récemment créé |
| 4728 | Member Added to Global Group | Security | CRITICAL | Élévation Domain Admins | Alerte P1 si groupe = Domain/ Enterprise/Schema Admins |
| 4730 | Global Group Deleted | Security | HIGH | Destruction groupes de sécurité | Alerter systématiquement |

| Event ID | Nom | Canal | Priorité | Attaque associée | Action recommandée |
|---|---|---|---|---|---|
| 4732 | Member Added to Local Group | Security | HIGH | Élévation admin local sur DC | Alerter si groupe = Administrators sur DC |
| 4735 | Local Group Changed | Security | HIGH | Modification groupes sensibles | Surveiller groupes Backup Operators, Account Operators |
| 4738 | User Account Changed | Security | CRITICAL | AS-REP Roasting setup, SIDHistory abuse | Alerter sur changement UAC ou SIDHistory |
| 4741 | Computer Account Created | Security | HIGH | MAQ abuse, RBCD preparation | Alerter si créé par compte non-admin |
| 4742 | Computer Account Changed | Security | CRITICAL | RBCD attack, machine account takeover | Alerter sur modification msDS-AllowedToActOnBehalfOf |
| 4743 | Computer Account Deleted | Security | HIGH | Nettoyage de traces | Alerter si DC account supprimé |
| 4756 | Member Added to Universal Group | Security | HIGH | Élévation multi-domaines | Alerter sur groupes universels admin |
| 4768 | TGT Requested (AS-REQ) | Security | HIGH | AS-REP Roasting, énumération comptes | Alerter sur PreAuthType=0 |
| 4769 | TGS Requested | Security | CRITICAL | Kerberoasting, Pass-the-Ticket, Golden Ticket | Alerter sur EncryptionType=0x17 en masse |
| 4770 | TGT Renewed | Security | MEDIUM | Golden Ticket (durée anormale) | Alerter si durée > 10h |
| 4771 | Kerberos Pre-auth Failed | Security | HIGH | Brute-force Kerberos, énumération | Seuil : >5 échecs/minute même compte |
| 4776 | NTLM Validation | Security | HIGH | NTLM Relay, NTLMv1 downgrade | Alerter sur PackageName=NTLM V1 |
| 4906 | CrashOnAuditFail Changed | Security | HIGH | Saturation journal d'audit | Alerter immédiatement |
| 4907 | Audit Settings Changed on Object | Security | HIGH | Désactivation audit objet spécifique | Surveiller modifications sur objets admin |
| 4928 | AD Replica Source Established | Security | HIGH | DCShadow | Alerter si source n'est pas un DC connu |
| 4929 | AD Replica Source Removed | Security | MEDIUM | DCShadow cleanup | Corréler avec 4928 |

| Event ID | Nom | Canal | Priorité | Attaque associée | Action recommandée |
|---|---|---|---|---|---|
| 4932 | AD Replica Synchronization Begin | Security | HIGH | DCShadow, réplication anormale | Alerter si source non-DC |
| 4933 | AD Replica Synchronization End | Security | MEDIUM | — | Archiver pour corrélation |
| 5136 | DS Object Attribute Modified | Security | CRITICAL | ACL abuse, AdminSDHolder, Shadow Credentials | Alerter sur nTSecurityDescriptor / msDS-KeyCredentialLink |
| 5137 | DS Object Created | Security | HIGH | Création GPO/OU malveillante | Alerter si créé par compte non-admin |
| 5138 | DS Object Undeleted | Security | HIGH | Résurrection d'objets supprimés | Alerter systématiquement |
| 5139 | DS Object Moved | Security | MEDIUM | Déplacement hors OU protégée | Surveiller déplacements hors OUs admin |
| 1102 | Security Log Cleared | Security | CRITICAL | Effacement de traces (T1070.001) | Alerte P1 immédiate, escalade SOC |
| 4104 | PS ScriptBlock Executed | PS/ Operational | CRITICAL | Fileless malware, PowerView, Mimikatz PS | Alerter sur keywords Mimikatz/ DCSync/IEX+Download |
| 4103 | PS Module Invoked | PS/ Operational | HIGH | PowerSploit, Empire, PowerView | Alerter sur modules offensifs connus |
| 400 | PS Engine Started | Windows PS | MEDIUM | Lancement PS en mode encodé | Alerter si HostApplication contient base64 |
| 7045 | Service Installed (System) | System | CRITICAL | Persistance service (PsExec, CS, Metasploit) | Alerter sur PSEXESVC, noms aléatoires, UNC paths |
| 5857 | WMI Activity | WMI/ Operational | MEDIUM | WMI lateral movement | Surveiller connexions WMI vers DCs |
| 5861 | WMI Subscription Created | WMI/ Operational | CRITICAL | WMI persistence (T1546.003) | Alerte immédiate — toute subscription est suspecte sur DC |
| 4670 | Permissions Changed on Object | Security | CRITICAL | ACL modification, Shadow Admin création | Alerter sur permissions Domain Object, AdminSDHolder |

| Event ID | Nom | Canal | Priorité | Attaque associée | Action recommandée |
|---|---|---|---|---|---|
| 4673 | Privileged Service Called | Security | HIGH | SeDebugPrivilege pour injection mémoire | Alerter sur SeDebugPrivilege hors processus légitimes |
| 4674 | Privileged Object Operation | Security | HIGH | Abus de privilèges sur objets système | Surveiller opérations sur LSASS |
| 4688 | Process Created | Security | HIGH | Exécution d'outils offensifs sur DC | Alerter sur mimikatz.exe, rubeus.exe, sharphound.exe |
| 4698 | Scheduled Task Created | Security | HIGH | Persistance via tâche planifiée | Alerter si TaskName contient chemin inhabituel |
| 4702 | Scheduled Task Updated | Security | HIGH | Modification tâche planifiée légitime | Alerter sur modification tâches système |

# Implémentation dans un SIEM : Wazuh et Microsoft Sentinel

## Règles Wazuh pour la détection AD

```
 <!-- Règles Wazuh custom pour Windows DC monitoring -->
<!-- Fichier: /var/ossec/etc/rules/active_directory_rules.xml -->

<group name="windows,active_directory,">

  <!-- DCSync Detection: Event 4662 with DS-Replication-Get-Changes-All -->
  <rule id="100100" level="15">
    <if_group>windows</if_group>
    <id>4662</id>
    <field name="win.eventdata.properties" type="pcre2">
      1131f6ad-9c07-11d1-f79f-00c04fc2dcd2
    </field>
    <description>CRITICAL: DCSync detected - DS-Replication-Get-Changes-All from non-DC account</
    <mitre>
      <id>T1003.006</id>
    </mitre>
  </rule>

  <!-- Kerberoasting: TGS request with RC4 encryption -->
  <rule id="100101" level="12">
    <if_group>windows</if_group>
    <id>4769</id>
    <field name="win.eventdata.ticketEncryptionType">0x17</field>
    <field name="win.eventdata.ticketOptions">0x40810000</field>
    <description>HIGH: Kerberoasting - TGS requested with RC4 encryption (T1558.003)</description
    <mitre>
      <id>T1558.003</id>
    </mitre>
  </rule>

  <!-- AS-REP Roasting: TGT without pre-authentication -->
  <rule id="100102" level="12">
    <if_group>windows</if_group>
    <id>4768</id>
    <field name="win.eventdata.preAuthType">0</field>
    <description>HIGH: AS-REP Roasting - Kerberos pre-authentication disabled account (T1558.004)
    <mitre>
      <id>T1558.004</id>
    </mitre>
  </rule>

  <!-- Password Spray: Multiple 4625 on different accounts -->
  <rule id="100103" level="10" frequency="10" timeframe="60">
```

```
    <if_matched_group>windows</if_matched_group>
    <id>4625</id>
    <same_field>win.eventdata.ipAddress</same_field>
    <different_field>win.eventdata.targetUserName</different_field>
    <description>HIGH: Password spray detected - 10 failures from same IP on different accounts</
    <mitre>
      <id>T1110.003</id>
    </mitre>
  </rule>

  <!-- Security Log Cleared -->
  <rule id="100104" level="15">
    <if_group>windows</if_group>
    <id>1102</id>
    <description>CRITICAL: Security Event Log cleared - Possible evidence tampering (T1070.001)</
    <mitre>
      <id>T1070.001</id>
    </mitre>
  </rule>

  <!-- Domain Admins Group Modified -->
  <rule id="100105" level="14">
    <if_group>windows</if_group>
    <id>4728</id>
    <field name="win.eventdata.groupName" type="pcre2">
      Domain Admins|Enterprise Admins|Schema Admins
    </field>
    <description>CRITICAL: Member added to privileged AD group</description>
    <mitre>
      <id>T1098.007</id>
    </mitre>
  </rule>

  <!-- PowerShell ScriptBlock with offensive keywords -->
  <rule id="100106" level="13">
    <if_group>windows</if_group>
    <id>4104</id>
    <field name="win.eventdata.scriptBlockText" type="pcre2" negate="no">
      [Ii]nvoke-[Mm]imikatz|Invoke-DCSync|Get-ADReplAccount|
      Invoke-Kerberoast|Get-NetDomainController|Add-DomainGroupMember|
      Set-DomainObject|[Ii]nvoke-[Ee]xpression.*[Dd]ownload
    </field>
    <description>CRITICAL: Offensive PowerShell detected on DC (Mimikatz/PowerView/Empire)</descr
    <mitre>
```

```
      <id>T1059.001</id>
    </mitre>
  </rule>

  <!-- RBCD Attack: Computer account msDS-AllowedToActOnBehalfOf modified -->
  <rule id="100107" level="14">
    <if_group>windows</if_group>
    <id>5136</id>
    <field name="win.eventdata.attributeLDAPDisplayName">
      msDS-AllowedToActOnBehalfOfOtherIdentity
    </field>
    <description>CRITICAL: RBCD attack setup - msDS-AllowedToActOnBehalfOf modified</description>
    <mitre>
      <id>T1134.001</id>
    </mitre>
  </rule>

</group>
```

Requêtes KQL Microsoft Sentinel

```
// ===== KERBEROASTING DETECTION =====
// Détecte les demandes TGS avec chiffrement RC4 en masse
SecurityEvent
| where EventID == 4769
| where TicketEncryptionType == "0x17"  // RC4-HMAC
| where TicketOptions == "0x40810000"
| where AccountName !endswith "$"  // Exclure comptes machine
| summarize
    RequestCount = count(),
    TargetServices = make_set(ServiceName, 20)
  by AccountName, IpAddress, bin(TimeGenerated, 1m)
| where RequestCount > 3
| extend AlertSeverity = "High"
| extend MITRE_Technique = "T1558.003 - Kerberoasting"
| project TimeGenerated, AccountName, IpAddress, RequestCount, TargetServices, MITRE_Technique

// ===== DCSYNC DETECTION =====
// Détecte les opérations de réplication DS depuis des comptes non-DC
SecurityEvent
| where EventID == 4662
| where Properties has "1131f6aa-9c07-11d1-f79f-00c04fc2dcd2"
    or Properties has "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2"
| where SubjectUserName !endswith "$"  // Non machine account
| where ObjectType contains "19195a5b"  // domainDNS
| extend AlertSeverity = "Critical"
| extend MITRE_Technique = "T1003.006 - DCSync"
| project TimeGenerated, SubjectUserName, SubjectDomainName,
          ObjectName, Properties, Computer, MITRE_Technique

// ===== PASSWORD SPRAY DETECTION =====
// Fenêtre glissante : >10 échecs depuis même IP sur comptes différents
SecurityEvent
| where EventID == 4625
| where SubStatus == "0xc000006a"  // Wrong password
| summarize
    FailureCount = count(),
    DistinctAccounts = dcount(TargetUserName),
    Accounts = make_set(TargetUserName, 10)
  by IpAddress, bin(TimeGenerated, 5m)
| where DistinctAccounts > 5 and FailureCount > 10
| extend AlertSeverity = "High"
| extend MITRE_Technique = "T1110.003 - Password Spray"
```

```
// ===== SECURITY LOG CLEARED =====
SecurityEvent
| where EventID == 1102
| extend AlertSeverity = "Critical"
| extend MITRE_Technique = "T1070.001 - Clear Windows Event Logs"
| project TimeGenerated, Computer, Account, Activity, MITRE_Technique

// ===== DCSHADOW DETECTION =====
// Réplication depuis une machine qui n'est pas un DC connu
let KnownDCs = toscalar(
    SecurityEvent
    | where EventID == 4928
    | where TimeGenerated > ago(30d)
    | summarize make_set(SubjectUserName)
);
SecurityEvent
| where EventID in (4928, 4932)
| where SubjectUserName !in (KnownDCs)
| where SubjectUserName !endswith "$"
| extend AlertSeverity = "Critical"
| extend MITRE_Technique = "T1207 - Rogue Domain Controller (DCShadow)"
```

## Politique d'Audit Windows : Configuration via GPO

L'activation de l'Advanced Audit Policy Configuration est indispensable pour capturer les Event IDs décrits dans ce guide. La politique d'audit basique (Basic Audit Policy) ne suffit pas — elle ne génère pas les events DS Access nécessaires pour détecter DCSync.

Activation via auditpol (ligne de commande)

```
 # === ACCOUNT LOGON ===
auditpol /set /subcategory:"Kerberos Service Ticket Operations" /success:enable /failure:enable
auditpol /set /subcategory:"Kerberos Authentication Service" /success:enable /failure:enable
auditpol /set /subcategory:"Credential Validation" /success:enable /failure:enable
auditpol /set /subcategory:"Other Account Logon Events" /success:enable /failure:enable

# === ACCOUNT MANAGEMENT ===
auditpol /set /subcategory:"User Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Computer Account Management" /success:enable /failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable /failure:enable
auditpol /set /subcategory:"Distribution Group Management" /success:enable /failure:enable
auditpol /set /subcategory:"Other Account Management Events" /success:enable /failure:enable

# === DS ACCESS - CRITIQUE POUR DCSYNC ===
auditpol /set /subcategory:"Directory Service Access" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Changes" /success:enable /failure:enable
auditpol /set /subcategory:"Directory Service Replication" /success:enable /failure:enable
auditpol /set /subcategory:"Detailed Directory Service Replication" /success:enable /failure:enab

# === LOGON/LOGOFF ===
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Logoff" /success:enable /failure:enable
auditpol /set /subcategory:"Special Logon" /success:enable /failure:enable
auditpol /set /subcategory:"Other Logon/Logoff Events" /success:enable /failure:enable

# === OBJECT ACCESS ===
auditpol /set /subcategory:"SAM" /success:enable /failure:enable

# === POLICY CHANGE ===
auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable
auditpol /set /subcategory:"Authentication Policy Change" /success:enable /failure:enable
auditpol /set /subcategory:"Authorization Policy Change" /success:enable /failure:enable

# === PRIVILEGE USE ===
auditpol /set /subcategory:"Sensitive Privilege Use" /success:enable /failure:enable

# === SYSTEM ===
auditpol /set /subcategory:"Security System Extension" /success:enable /failure:enable
auditpol /set /subcategory:"Security State Change" /success:enable /failure:enable

# === PROCESS CREATION (pour 4688) ===
auditpol /set /subcategory:"Process Creation" /success:enable /failure:enable
```

```
# Activer la ligne de commande dans 4688 via registre
reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Audit" ^
    /v ProcessCreationIncludeCmdLine_Enabled /t REG_DWORD /d 1 /f

# Vérification de la configuration
auditpol /get /category:*

# === POWERSHELL LOGGING ===
# Module Logging
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging" ^
    /v EnableModuleLogging /t REG_DWORD /d 1 /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames" ^
    /v * /t REG_SZ /d * /f

# ScriptBlock Logging
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" ^
    /v EnableScriptBlockLogging /t REG_DWORD /d 1 /f
reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging" ^
    /v EnableScriptBlockInvocationLogging /t REG_DWORD /d 1 /f
```

### Configuration GPO recommandée

Dans la GPO liée aux Unités d'Organisation des Domain Controllers :

Chemin : **Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration**

Activer toutes les sous-catégories listées ci-dessus en Success et Failure

Augmenter la taille des journaux Security : minimum **1 Go** sur les DCs (4 Go recommandé)

Configurer la politique de rétention : **Overwrite events as needed** (les logs sont envoyés au SIEM en temps réel)

Activer **Command Line Process Auditing** pour enrichir les Event 4688

La configuration des Authentication Silos Windows Server 2025 permet de restreindre encore davantage les authentifications sensibles. Voir notre guide sur les Authentication Silos Windows Server 2025 pour compléter cette configuration.

# Conformité NIS 2 et ANSSI : Quels Events sont Obligatoires ?

La directive NIS 2 (Network and Information Security Directive 2), transposée en droit français par la loi n°2023-703 du 1er août 2023 et les décrets d'application en cours, impose aux entités essentielles et importantes de mettre en place des mesures de supervision de leurs systèmes d'information critiques. Les contrôleurs de domaine Active Directory entrent pleinement dans ce périmètre.

## Events obligatoires selon les référentiels ANSSI

Le guide ANSSI "Recommandations de sécurité relatives à Active Directory" (version 2.0, 2023) identifie les journaux suivants comme indispensables :

| Catégorie ANSSI | Event IDs requis | Justification réglementaire |
|---|---|---|
| Authentifications | 4624, 4625, 4648, 4768, 4769, 4771, 4776 | Traçabilité des accès aux SI sensibles |
| Gestion des comptes | 4720, 4722, 4724, 4725, 4726, 4728, 4732, 4738 | Contrôle des identités et des droits |
| Modifications AD | 5136, 5137, 4662, 4742 | Intégrité de l'annuaire |
| Politique de sécurité | 4719, 4907, 4906 | Non-répudiation des changements de configuration |
| Effacement de logs | 1102, 4904, 4905 | Détection de l'effacement de preuves |
| Services et processus | 4697, 7045, 4688, 4698 | Détection de persistance |

## Exigences de rétention et de centralisation

**Rétention minimum** : 12 mois (NIS 2, Article 21) — les logs doivent être conservés dans un système immuable

**Centralisation SIEM** : les logs des DCs doivent être transmis en temps réel à un SIEM centralisé, inaccessible depuis les DCs eux-mêmes

**Intégrité des logs** : mécanisme de détection de modification ou suppression (1102 surveillé)

**Délai de notification** : en cas d'incident affectant les DCs, notification ANSSI sous 24h (incident majeur) ou 72h (incident significatif)

### Lien avec DNSSEC sur les DCs

La sécurisation DNS des contrôleurs de domaine est également un prérequis NIS 2. Notre guide sur DNSSEC avec Windows Server 2025 détaille l'implémentation pour les zones DNS hébergées sur les DCs.

---

## Questions fréquentes sur la supervision des Contrôleurs de Domaine

### Quels sont les Event IDs Windows les plus critiques à surveiller sur un contrôleur de domaine ?

Les Event IDs les plus critiques sont : 4625 (échec authentification / brute-force), 4768/4769/4771 (tickets Kerberos / Kerberoasting / AS-REP Roasting), 4662 (opérations sur objets AD / DCSync), 4672 (attribution de droits sensibles), 5136 (modification objet AD / ACL abuse), 1102 (journal d'audit effacé) et 4697 (nouveau service installé). Ces events couvrent les principales techniques d'attaque Active Directory documentées dans MITRE ATT&CK.

### Comment détecter une attaque DCSync via les Event Logs Windows ?

Une attaque DCSync se détecte principalement via l'Event ID 4662 avec les propriétés `1131f6aa-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes) et `1131f6ad-9c07-11d1-f79f-00c04fc2dcd2` (DS-Replication-Get-Changes-All). Si ces réplications proviennent d'un compte non-DC (vérifier que l'IP source n'est pas un contrôleur de domaine légitime), c'est une forte indication d'un outil comme Mimikatz ou Impacket secretsdump. Les Events 4928 et 4929 couvrent aussi les sessions de réplication DS suspectes.

### Quelle politique d'audit GPO activer pour capturer tous les events critiques sur un DC ?

Il faut activer l'Advanced Audit Policy Configuration via GPO. Les catégories essentielles sont : Account Logon (Kerberos, NTLM), Account Management (création/modification comptes), DS Access (objets AD — indispensable pour DCSync), Logon/Logoff (ouvertures de session), Policy Change et Privilege Use. La commande `auditpol /set /subcategory` permet un contrôle granulaire. Pour PowerShell, activer le Module Logging et le ScriptBlock Logging dans les clés de registre dédiées ou via GPO (Administrative Templates > Windows Components > Windows PowerShell).

### Comment configurer Wazuh pour alerter sur les attaques Kerberoasting depuis un contrôleur de domaine ?

Dans Wazuh, créer une règle personnalisée qui filtre l'Event ID 4769 avec le champ *TicketEncryptionType=0x17* (RC4-HMAC, déprécié depuis Windows Server 2019). Le seuil de fréquence est crucial : plus de 5 demandes TGS en RC4 depuis un même compte en moins de 60 secondes indique un Kerberoasting automatisé (Rubeus, Impacket GetUserSPNs). Configurer aussi la règle sur l'Event 4768 avec PreAuthType=0 pour détecter l'AS-REP Roasting sur les comptes sans pré-authentification Kerberos.

### Quels Event IDs Windows sont requis par la réglementation NIS 2 et les recommandations ANSSI pour les contrôleurs de domaine ?

Le cadre NIS 2 et le guide ANSSI "Recommandations de sécurité relatives à Active Directory" imposent la journalisation des authentifications (4624/4625), des modifications de comptes privilégiés (4728/4732/4756), des changements de politique de sécurité (4719/4907), et des effacements de journaux (1102/4904). L'ANSSI recommande également la supervision des réplications AD (4662/4928) et des nouvelles installations de services (4697/7045) pour détecter la persistance. Ces logs doivent être centralisés dans un SIEM avec une rétention minimale de 12 mois, dans un système immuable inaccessible depuis les DCs.

Pour centraliser et corréler ces events dans le cloud, notre guide sur la détection des attaques Active Directory avec Microsoft Sentinel couvre les requêtes KQL, les règles analytiques et les playbooks SOAR.

À RETENIR

## Points clés à retenir

Les Event IDs 4625, 4768, 4769 et 4771 couvrent 80% des attaques d'authentification sur les DCs (brute-force, Kerberoasting, AS-REP Roasting)

L'Event ID 4662 avec les GUIDs de réplication DS est la signature principale d'une attaque DCSync — alerter immédiatement si le compte source n'est pas un DC

L'Event 5136 permet de détecter les abus ACL, la modification d'AdminSDHolder et les Shadow Credentials avant qu'ils ne soient exploités

L'Event 1102 (journal effacé) doit toujours déclencher une alerte P1 — c'est un indicateur fort de compromission ou d'effacement de traces

Le ScriptBlock Logging PowerShell (Event 4104) est indispensable pour détecter les outils offensifs comme Mimikatz, PowerView et Empire exécutés directement en mémoire

L'Advanced Audit Policy Configuration via GPO est obligatoire — la Basic Audit Policy ne génère pas les events DS Access nécessaires à la détection DCSync

NIS 2 et l'ANSSI exigent une rétention de 12 mois minimum, une centralisation SIEM en temps réel, et une surveillance active des effacements de journaux sur les DCs

## Sources


ANSSI CERT-FR — Publications et alertes

MITRE ATT&CK — Framework des techniques d'attaque

CISA — Advisories de cybersécurité

 