AYI NEDJIMI Consultants

Adalanche — Audit Active Directory Open Source

Catégorie : Attaques Active Directory Lecture : 15 min Publié le : 12/04/2026 Auteur : Ayi NEDJIMI

Maîtrisez Adalanche pour l'audit Active Directory : analyse ACL par graphes, comparaison BloodHound, requêtes critiques, workflow pentest. Guide expert complet.

L'audit de sécurité d'un Active Directory ne se résume pas à lancer BloodHound et chercher un chemin vers Domain Admin. Les environnements AD d'entreprise accumulent des années de délégations mal configurées, de GPO redondantes, de comptes de service avec des privilèges excessifs et de trusts inter-forêts rarement revus. Adalanche, développé par Lars Karlslund, apporte une approche complémentaire à BloodHound en se concentrant sur l'analyse des permissions réelles — les ACL (Access Control Lists) et les droits effectifs — plutôt que sur les seuls chemins d'attaque basés sur les sessions et les appartenances de groupe. Cet outil open source, écrit en Go et déployable en quelques minutes, génère un graphe interactif de toutes les relations de contrôle dans l'AD, révélant des chemins d'élévation de privilèges que BloodHound ne détecte pas nativement. Ce guide couvre l'installation, la comparaison détaillée avec BloodHound, les requêtes clés pour identifier les failles de sécurité critiques, et l'intégration dans un workflow de pentest ou d'audit de conformité. Les exemples sont issus d'audits réels (anonymisés) réalisés sur des environnements de 500 à 50 000 objets AD.

Qu'est-ce qu'Adalanche ?

Adalanche est un outil d'analyse de sécurité Active Directory qui collecte les données de l'annuaire (objets, ACL, GPO, DNS, certificats) et les représente sous forme de graphe interactif dans un navigateur web. Contrairement à BloodHound qui nécessite un collecteur séparé (SharpHound) et une base de données Neo4j, Adalanche est un binaire unique qui fait tout : collecte, analyse et visualisation. Son moteur d'analyse se concentre sur les permissions effectives et les chemins de contrôle réels, offrant une vue complémentaire à BloodHound pour les auditeurs et les pentesters. Pour les techniques d'attaque AD associées, consultez notre guide d'exploitation Kerberos.

Architecture et fonctionnement

```
# Adalanche est un binaire Go unique — pas de dépendance externe
# Trois modes principaux :

# 1. Collecte (depuis une machine jointe au domaine ou avec credentials)
adalanche collect activedirectory --domain corp.local

# 2. Analyse et visualisation (lance un serveur web local)
adalanche analyze --domain corp.local

# 3. Export vers d'autres formats (BloodHound, JSON, XLSX)
adalanche analyze --domain corp.local --export bloodhound
```

Installation et configuration

```
# Installation depuis les releases GitHub
wget https://github.com/lkarlslund/Adalanche/releases/latest/download/adalanche-linux-
amd64
chmod +x adalanche-linux-amd64
mv adalanche-linux-amd64 /usr/local/bin/adalanche

# OU compilation depuis les sources (Go 1.21+)
git clone https://github.com/lkarlslund/Adalanche.git
cd Adalanche && go build -o adalanche ./cmd/adalanche

# Collecte depuis Linux avec credentials
adalanche collect activedirectory \
  --domain corp.local \
  --server dc01.corp.local \
  --username auditor@corp.local \
  --password 'AuditP@ss2026' \
  --tlsmode tls

# Collecte depuis une machine Windows jointe au domaine
adalanche.exe collect activedirectory --domain corp.local

# Les données sont stockées localement dans ./data/
ls -la data/
```

Droits minimaux pour la collecte

Adalanche fonctionne avec un compte utilisateur standard du domaine. Aucun privilège administrateur n'est nécessaire pour la collecte de base — les ACL et les objets AD sont lisibles par tout utilisateur authentifié (sauf si les permissions par défaut ont été restreintes). Pour une collecte complète incluant les LAPS passwords et les gMSA, un accès en lecture sur ces attributs est requis.

Comparaison avec BloodHound

Adalanche et BloodHound ne sont pas concurrents — ils sont complémentaires. Comprendre leurs forces respectives permet de choisir le bon outil pour chaque phase de l'audit. Pour une vision globale des techniques d'audit AD, consultez notre analyse des relais NTLM 2026.

Critère	Adalanche	BloodHound CE
Architecture	Binaire unique, sans dépendance	SharpHound + Neo4j + App web
Collecteur	Intégré (Go, multi-plateforme)	SharpHound (.NET, Windows)
Base de données	Fichiers locaux (embedded)	Neo4j (PostgreSQL en CE)
Focus principal	ACL et permissions effectives	Chemins d'attaque et sessions
Sessions utilisateurs	Non collectées	Collectées (NetSessionEnum)
Analyse de GPO	Complète (liens, permissions)	Partielle
Analyse de certificats (AD CS)	Oui (ESC1-ESC8)	Oui (depuis BH CE)
Requêtes personnalisées	Interface graphique + filtres	Cypher queries
Export	BloodHound, JSON, XLSX, GraphML	JSON, CSV
Facilité de déploiement	Immédiate (1 binaire)	Complexe (Docker ou install manuelle)
Open source	Oui (GPLv3)	Oui (Apache 2.0)

Stratégie d'audit recommandée
En audit AD, lancez **les deux outils**. Commencez par Adalanche pour un panorama rapide des ACL dangereuses et des délégations excessives — c'est l'outil de découverte initiale. Complétez ensuite avec BloodHound pour identifier les chemins d'attaque exploitables via les sessions actives et les appartenances de groupes imbriquées. Les résultats d'Adalanche alimentent la phase de recommandations (remédiation des ACL), tandis que BloodHound guide la phase offensive (démonstration des chemins d'exploitation).

Requêtes clés : identifier les failles critiques

ACL dangereuses (WriteDACL, GenericAll, WriteOwner)

Les ACL les plus dangereuses sont celles qui accordent un contrôle total ou la capacité de modifier les permissions d'un objet. Un utilisateur avec WriteDACL sur un groupe d'administration peut s'y ajouter. Un utilisateur avec GenericAll sur un compte peut réinitialiser son mot de passe.

```
# Dans l'interface web Adalanche (http://localhost:8080)
# Requête : qui peut modifier les ACL du groupe Domain Admins ?
# Navigation : Objects > Domain Admins > Incoming permissions > WriteDACL

# Requête : tous les objets avec GenericAll sur des comptes à privilèges
# Filter: target.type=group AND target.name contains "admin"
# Edge type: GenericAll

# Export des résultats pour le rapport
adalanche analyze --domain corp.local \
  --export xlsx \
  --filter "edge.type=GenericAll AND target.admincount=1"
```

Chemins de délégation (Constrained/Unconstrained)

La délégation Kerberos mal configurée est l'un des vecteurs d'élévation de privilèges les plus courants dans les AD d'entreprise. Adalanche identifie les comptes avec délégation non contrainte (capable d'extraire des TGT) et délégation contrainte vers des services sensibles. Consultez notre hub Active Directory pour approfondir.

```
# Identifier les comptes avec délégation non contrainte
# Dans Adalanche : Filter > Unconstrained Delegation
# Attention : les contrôleurs de domaine sont en délégation non contrainte par défaut

# Comptes de service avec constrained delegation vers LDAP/CIFS des DC
# Ce sont des cibles de haute valeur pour un attaquant
```

Chemins vers Domain Admin

```
# Adalanche calcule automatiquement les chemins les plus courts
# vers les groupes à privilèges

# Via l'interface web :
# 1. Sélectionner le nœud cible (Domain Admins, Enterprise Admins)
# 2. Cliquer "Shortest paths to here"
# 3. Analyser chaque hop du chemin

# Exemple de chemin typique trouvé en audit :
# User_HelpDesk → GenericAll → SVC_SQL → MemberOf → Server_Admins
#   → AdminTo → DC01 → DCSync → Domain
```

Intégration dans un workflow de pentest

Phase de reconnaissance

```
# 1. Collecte Adalanche (depuis la machine de l'attaquant)
adalanche collect activedirectory \
  --domain target.local \
  --server 10.0.1.10 \
  --username compromised_user@target.local \
  --password 'P@ssw0rd'

# 2. Analyse immédiate — pas besoin de Neo4j
adalanche analyze --domain target.local
# Ouvre http://localhost:8080

# 3. Identifier rapidement :
#    - Comptes Kerberoastable (SPN set, pas dans Protected Users)
#    - Comptes AS-REP Roastable (pre-auth disabled)
#    - Chemins WriteDACL/GenericAll vers Domain Admins
#    - Comptes avec mot de passe n'expirant jamais
#    - Comptes dormants avec privilèges
```

Automatisation pour les audits récurrents

```
#!/bin/bash
# audit_ad_automated.sh — Script d'audit AD récurrent
DOMAIN="corp.local"
DATE=$(date +%Y%m%d)
OUTPUT_DIR="/opt/audits/ad/$DATE"

mkdir -p "$OUTPUT_DIR"

# Collecte
adalanche collect activedirectory --domain "$DOMAIN" \
  --datapath "$OUTPUT_DIR/data"

# Analyse et export
adalanche analyze --domain "$DOMAIN" \
  --datapath "$OUTPUT_DIR/data" \
  --export xlsx \
  --exportpath "$OUTPUT_DIR/report.xlsx"

# Export BloodHound compatible (pour cross-référence)
adalanche analyze --domain "$DOMAIN" \
  --datapath "$OUTPUT_DIR/data" \
  --export bloodhound \
  --exportpath "$OUTPUT_DIR/bloodhound/"

# Diff avec l'audit précédent
PREV=$(ls -d /opt/audits/ad/20* | sort | tail -2 | head -1)
if [ -d "$PREV" ]; then
  echo "Comparaison avec l'audit du $(basename $PREV)"
  diff <(cat "$PREV/report.xlsx" | md5sum) <(cat "$OUTPUT_DIR/report.xlsx" | md5sum)
fi
```

Reporting et visualisation

L'interface web d'Adalanche offre un graphe interactif navigable où chaque nœud représente un objet AD (utilisateur, groupe, ordinateur, GPO) et chaque arête une relation de contrôle. Les couleurs indiquent le type de relation et le niveau de risque. L'export XLSX permet de générer des rapports structurés pour les comités de sécurité, avec des colonnes pré-formatées pour la source, la cible, le type de permission, et le niveau de criticité.

Usages avancés

Analyse multi-forêts et trusts

```
# Collecte sur plusieurs domaines/forêts
adalanche collect activedirectory --domain corp.local
adalanche collect activedirectory --domain partner.local

# Analyse combinée — inclut les relations cross-trust
adalanche analyze --domain corp.local,partner.local

# Identifier les chemins d'attaque cross-forest
# (SID History abuse, trust transitivity, etc.)
```

Analyse AD CS (Active Directory Certificate Services)

Adalanche détecte les templates de certificats vulnérables (ESC1 à ESC8) qui permettent à un utilisateur standard de demander un certificat au nom d'un administrateur. Ces vulnérabilités sont parmi les plus critiques et les plus fréquentes dans les AD d'entreprise. Pour les techniques de relais associées, voir notre analyse NTLM relay 2026.

FAQ — Questions fréquentes

Adalanche peut-il remplacer BloodHound dans un pentest ?

Non, et ce n'est pas son objectif. Adalanche excelle dans l'analyse des ACL et des permissions effectives, mais il ne collecte pas les sessions utilisateurs (NetSessionEnum, SMB sessions) qui sont essentielles pour les chemins d'attaque de type "session hop" dans BloodHound. Un pentest complet utilise les deux outils : Adalanche pour la surface d'attaque liée aux permissions, BloodHound pour les chemins d'exploitation via les sessions actives. En audit de conformité, Adalanche est souvent suffisant car l'objectif est de corriger les permissions excessives, pas de les exploiter.

Quelle est la volumétrie supportée par Adalanche ?

Adalanche traite des environnements de 100 000+ objets AD sans problème sur un poste de travail standard (16 Go RAM, SSD). La collecte d'un domaine de 50 000 objets prend typiquement 5 à 15 minutes selon la latence réseau et la profondeur de collecte (ACL, GPO, DNS, certificats).

L'analyse est quasi instantanée car les données sont stockées localement dans un format optimisé. Pour comparaison, la même analyse avec BloodHound CE nécessite l'import dans PostgreSQL qui peut prendre 30 minutes à 2 heures.

Comment détecter l'utilisation d'Adalanche sur notre AD ?

Adalanche effectue des requêtes LDAP standards sur les attributs publiquement lisibles de l'AD. Sa signature réseau est identique à celle de n'importe quel outil d'administration utilisant LDAP (dsquery, PowerShell Get-ADObject, ldapsearch). La détection repose sur l'analyse volumétrique : un seul compte effectuant des requêtes LDAP exhaustives sur l'ensemble des objets et ACL en quelques minutes est suspect. Supervisez les événements Windows 4662 (Directory Service Access) et 4624 (Logon) pour détecter des patterns de collecte massifs à partir de comptes non administrateurs.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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