

# Les mappages utilisateur-IP n'apparaissent plus dans Cisco CDA après mars 2017 Microsoft Update

## Contenu

[Introduction](#)

[Informations générales](#)

[Problème : Les mappages utilisateur-IP n'apparaissent plus dans Cisco CDA après mars 2017 Microsoft Update](#)

[Solutions potentielles](#)

[Solution](#)

## Introduction

Ce document décrit comment surmonter le problème de la mise à jour de sécurité Microsoft de mars 2017, qui rompt la fonctionnalité CDA i.e. Les mappages utilisateur n'apparaissent plus dans l'agent CDA (Context Directory Agent) SWT.

## Informations générales

Cisco CDA s'appuie sur l'ID d'événement 4768 renseigné sur toutes les versions des contrôleurs de domaine Windows 2008 et 2012. Ces événements indiquent que les événements de connexion utilisateur ont réussi. Si les événements d'ouverture de session réussis ne sont pas vérifiés dans la stratégie de sécurité locale ou si ces ID d'événement ne sont pas renseignés pour une autre raison, les requêtes WMI de CDA pour ces événements ne retourneront aucune donnée. Par conséquent, les mappages utilisateur ne seront pas créés dans CDA et par conséquent, les informations de mappage utilisateur ne seront pas envoyées de CDA à l'ASA (Adaptive Security Appliance). Dans les cas où les clients exploitent des stratégies utilisateur ou de groupe à partir d'AD dans Cloud Web Security (CWS), les informations utilisateur n'apparaissent pas dans la sortie `whoami.scansafe.net`.

**Remarque** : ceci n'affecte pas l'agent utilisateur Firepower, car il utilise l'ID d'événement 4624 pour créer des mappages utilisateur et ce type d'événement n'est pas affecté par cette mise à jour de sécurité.

## Problème : Les mappages utilisateur-IP n'apparaissent plus dans Cisco CDA après mars 2017 Microsoft Update

Une mise à jour récente de la sécurité Microsoft a causé des problèmes dans plusieurs environnements clients où leurs contrôleurs de domaine arrêtent de consigner ces ID d'événement 4768. Les Ko incriminés sont répertoriés ci-dessous :

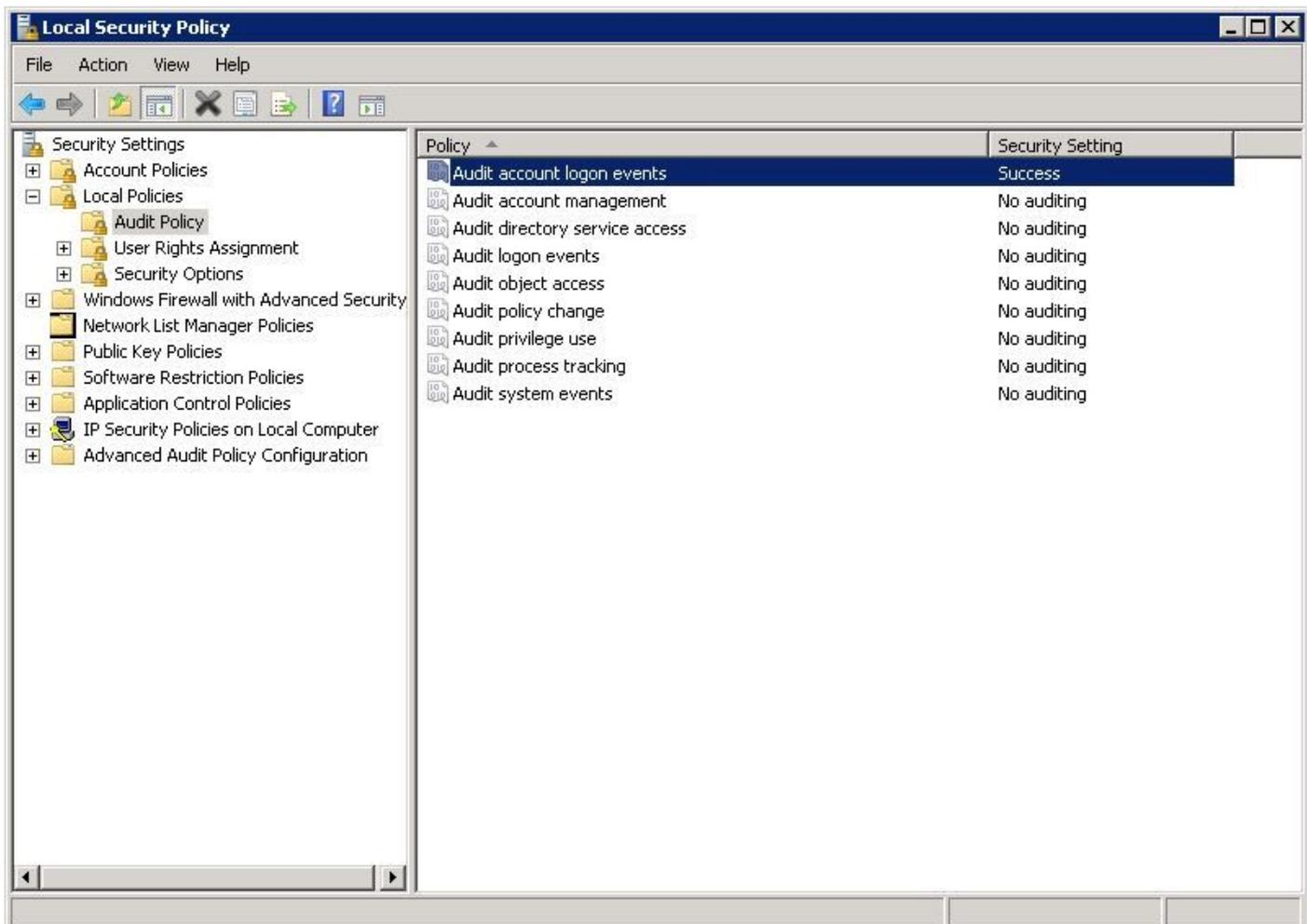
KB4012212 (2008) / KB4012213 (2012)

Pour confirmer que ce problème ne concerne pas la configuration de journalisation sur le contrôleur de domaine, assurez-vous que la journalisation d'audit appropriée est activée dans la stratégie de sécurité locale. Les éléments en gras de cette sortie ci-dessous doivent être activés pour la journalisation correcte des ID d'événement 4768. Cette opération doit être exécutée à partir de l'invite de commande de chaque contrôleur de domaine qui ne consigne pas les événements :

```
C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory                Setting
System
  Security System Extension          No Auditing
  System Integrity                   Success and Failure
  IPsec Driver                       No Auditing
  Other System Events                Success and Failure
  Security State Change              Success
Logon/Logoff
  Logon                             Success and Failure
  Logoff                             Success
  Account Lockout                    Success
  IPsec Main Mode                    No Auditing
  IPsec Quick Mode                   No Auditing
  IPsec Extended Mode                No Auditing
  Special Logon                      Success
  Other Logon/Logoff Events          No Auditing
  Network Policy Server              Success and Failure
...output truncated...
Account Logon   Kerberos Service Ticket Operations   Success and Failure
  Other Account Logon Events          Success and Failure
  Kerberos Authentication Service     Success and Failure
  Credential Validation                Success and Failure
```

C:\Users\Administrator>

Si vous constatez que la journalisation d'audit appropriée n'est pas configurée, accédez à **Stratégie de sécurité locale > Paramètres de sécurité > Stratégies locales > Stratégie d'audit** et assurez-vous que les **événements d'ouverture de session du compte d'audit** sont définis sur **Réussite**, comme l'illustre l'image :



## Solutions potentielles

(Mise à jour le 31/03/2017)

Comme solution de contournement actuelle, certains utilisateurs ont pu désinstaller les Ko mentionnés ci-dessus et les ID d'événement 4768 ont repris la journalisation. Jusqu'à présent, cela s'est avéré efficace pour tous les clients Cisco.

Microsoft a également fourni la solution de contournement suivante à certains clients qui abordent ce problème, comme le montrent les forums de support. Notez que ceci n'a pas encore été entièrement testé ou vérifié dans les laboratoires Cisco :

Les quatre stratégies d'audit que vous devez activer pour contourner le bogue sont sous Ordinateur Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. Les quatre stratégies sous cette rubrique doivent être activées pour Réussite et Échec :

- Validation des identifiants d'audit
- Service d'authentification Kerberos d'audit
- Audit des opérations de ticket de service Kerberos
- Audit des autres événements de connexion au compte

Lorsque vous activez ces quatre stratégies, vous devriez recommencer à voir les événements

4768/4769 Success.

Reportez-vous à l'image ci-dessus qui montre **Configuration avancée de la stratégie d'audit** en bas du volet gauche.

## Solution

À la date de cette publication initiale (3/28/2017), nous ne connaissons pas encore de correctif permanent de Microsoft. Cependant, ils sont conscients de ce problème et travaillent à une solution.

Plusieurs threads suivent ce problème :

Reddit :

[https://www.reddit.com/r/sysadmin/comments/5zs0nc/heads\\_up\\_ms\\_kb4012213\\_andor\\_ms\\_kb4012216\\_disables/](https://www.reddit.com/r/sysadmin/comments/5zs0nc/heads_up_ms_kb4012213_andor_ms_kb4012216_disables/)

UltimateWindowsSecurity.com:

<http://forum.ultimatewindowssecurity.com/Topic7340-276-1.aspx>

Microsoft TechNet :

<https://social.technet.microsoft.com/Forums/systemcenter/en-US/4136ade9-d287-4a42-b5cb-d6042d227e4f/kb4012216-issue-with-event-id-4768?forum=winserver8gen>

Ce document est mis à jour à mesure que davantage d'informations deviennent disponibles ou si Microsoft annonce une correction permanente pour ce problème.