Les mappages Utilisateur-à-IP apparaissent plus dans la mise à jour de Cisco CDA après mars 2017 Microsoft

Contenu

Introduction

Ce document décrit comment surmonter la question mars 2017 de la mise à jour de sécurité de Microsoft, qui casse l'utilisateur de fonctionnalité CDA c.-à-d. que les mappages n'apparaissent plus dans l'agent de répertoire de contexte SWT (CDA).

Informations générales

Cisco CDA compte sur l'ID 4768 d'événement étant rempli sur toutes les versions de Windows 2008 et 2012 contrôleurs de domaine. Ces événements indiquent des événements réussis de connexion d'utilisateur. Si des événements de connexion de succès ne sont pas audités dans la stratégie de sécurité locale ou si ces id d'événement ne sont remplis pour aucune autre raison puis les requêtes WMI de CDA pour ces événements ne renverront aucune donnée. En conséquence, des mappages d'utilisateur ne seront pas créés dans CDA et donc les informations de mappage d'utilisateur ne seront pas envoyées de CDA à l'appliance de sécurité adaptable (ASA). Dans les cas où les clients accroissent l'utilisateur ou les stratégies basées sur groupe de l'AD dans la sécurité Web de nuage (CWS), les informations utilisateur n'apparaissent pas dans la sortie de **whoami.scansafe.net**.

> **Note**: Ceci n'affecte pas l'agent d'utilisateur de FirePOWER (uA) puisqu'il accroît l'ID 4624 d'événement pour créer des mappages d'utilisateur et ce type d'événement n'est pas affecté par cette mise à jour de sécurité.

Problème : Les mappages Utilisateur-à-IP apparaissent plus dans la mise à jour de Cisco CDA après mars 2017 Microsoft

Une mise à jour de sécurité récente de Microsoft a entraîné des questions dans plusieurs environnements de client où leurs contrôleurs de domaine cessent de se connecter ces 4768 id d'événement. Le KBS offensant sont répertoriés ci-dessous :

KB4012212 (2008)/KB4012213 (2012)

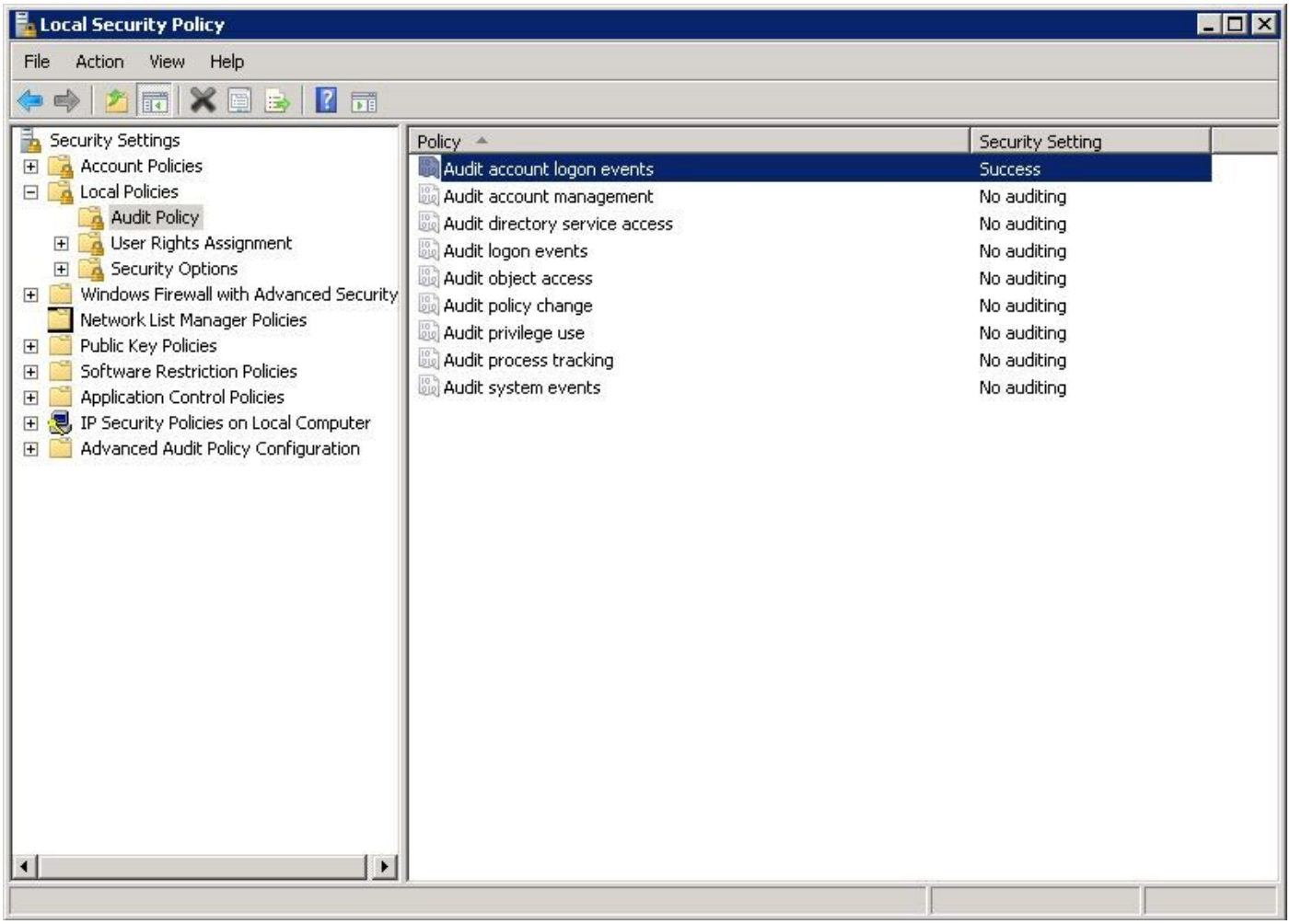
KB4012215 (2008)/KB4012216 (2012)

Pour confirmer que cette question n'est pas avec la configuration de journalisation sur le contrôleur de domaine, assurez-vous que se connecter approprié d'audit est activé dans la stratégie de sécurité locale. Les éléments gras dans cette sortie au-dessous du mustbe activé pour se connecter approprié de 4768 id d'événement. Ceci devrait être exécuté de l'invite de commande de chaque C.C qui n'est pas des loggings events :

```
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 voyez que se connecter approprié d'audit n'est pas configuré, naviguez vers la **stratégie > les paramètres de sécurité de sécurité locale > des stratégies locales > stratégie d'audit** et assurez-vous que des **événements de connexion de compte d'audit** est placés au **succès**, suivant les indications de l'image :



Contournements potentiels

(Mis à jour 3/31/2017)

Comme contournement en cours, quelques utilisateurs ont pu désinstaller le KBS mentionné ci-dessus et les 4768 id d'événement se connecter repris. Ceci a prouvé efficace pour tous les clients de Cisco jusqu'ici.

Microsoft a également fourni le contournement suivant à quelques clients frappant cette question comme vu dans des forum de support. Notez que ceci encore n'a pas été entièrement testé ou a été vérifié dans les TP Cisco :

> Les quatre stratégies d'audit que vous devez activer pendant qu'un contournement à la bogue sont sous la configuration de l'ordinateur \ stratégies \ paramètres de windows \ paramètres de sécurité \ la configuration de politique d'audit \ stratégies d'audit \ connexion avancées de compte. Chacune des quatre stratégies sous ce titre devrait être activé pour le succès et échec :
>
> Validation de laisser-passer d'audit
> Service d'authentification Kerberos d'audit
> Exécutions de ticket de service de Kerberos d'audit
> Apurez d'autres événements de connexion de compte

Quand vous activez ces quatre stratégies, vous devriez commencer à revoir les événements de succès de 4768/4769.

Référez-vous à l'image au-dessus de cela affiche la **configuration de politique avancée d'audit au** bas du volet gauche.

Solution

En date de la date de cette première publication (3/28/2017), nous ne savons pas encore d'une difficulté permanente de Microsoft. Cependant, ils se rendent compte de cette question et de fonctionner sur une difficulté.

Il y a plusieurs thread dépistant cette question :

Reddit :

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

TechNet de Microsoft :

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 pendant que plus d'informations deviennent disponibles ou si Microsoft annonce une difficulté permanente pour cette question.