Benutzer-zu-IP-Zuordnungen werden nach Microsoft Update vom März 2017 in Cisco CDA nicht mehr angezeigt

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie das Problem der Microsoft-Sicherheitsaktualisierung vom März 2017, die die CDA-Funktionalität (z. Benutzerzuordnungen werden nicht mehr im SWT Context Directory Agent (CDA) angezeigt.

Hintergrundinformationen

Cisco CDA setzt voraus, dass die Ereignis-ID 4768 in allen Versionen der Domänencontroller von Windows 2008 und 2012 eingetragen wird. Diese Ereignisse weisen auf erfolgreiche Benutzeranmeldeereignisse hin. Wenn Erfolgsanmeldeereignisse nicht in der lokalen Sicherheitsrichtlinie überprüft werden oder wenn diese Ereignis-IDs aus einem anderen Grund nicht eingetragen werden, werden von den WMI-Abfragen von CDA für diese Ereignisse keine Daten zurückgegeben. Aus diesem Grund werden in CDA keine Benutzerzuordnungen erstellt, und daher werden keine Benutzerzuordnungsinformationen von CDA an die Adaptive Security Appliance (ASA) gesendet. Wenn Kunden Benutzer- oder Gruppenrichtlinien von AD in Cloud Web Security (CWS) nutzen, werden die Benutzerinformationen nicht in der Ausgabe **whoami.scansafe.net** angezeigt.

> **Hinweis**: Dies betrifft den FirePOWER User Agent (UA) nicht, da die Ereignis-ID 4624 zum Erstellen von Benutzerzuordnungen verwendet wird und dieser Ereignistyp durch dieses Sicherheitsupdate nicht beeinflusst wird.

Problem: Benutzer-zu-IP-Zuordnungen werden nach Microsoft Update vom März 2017 in Cisco CDA nicht mehr angezeigt

Ein aktuelles Microsoft-Sicherheitsupdate hat in mehreren Kundenumgebungen Probleme verursacht, bei denen die Domänen-Controller die Protokollierung dieser 4768-Ereignis-IDs einstellen. Nachfolgend sind die zu verachtenden KBs aufgeführt:

KB4012212 (2008) / KB4012213 (2012)

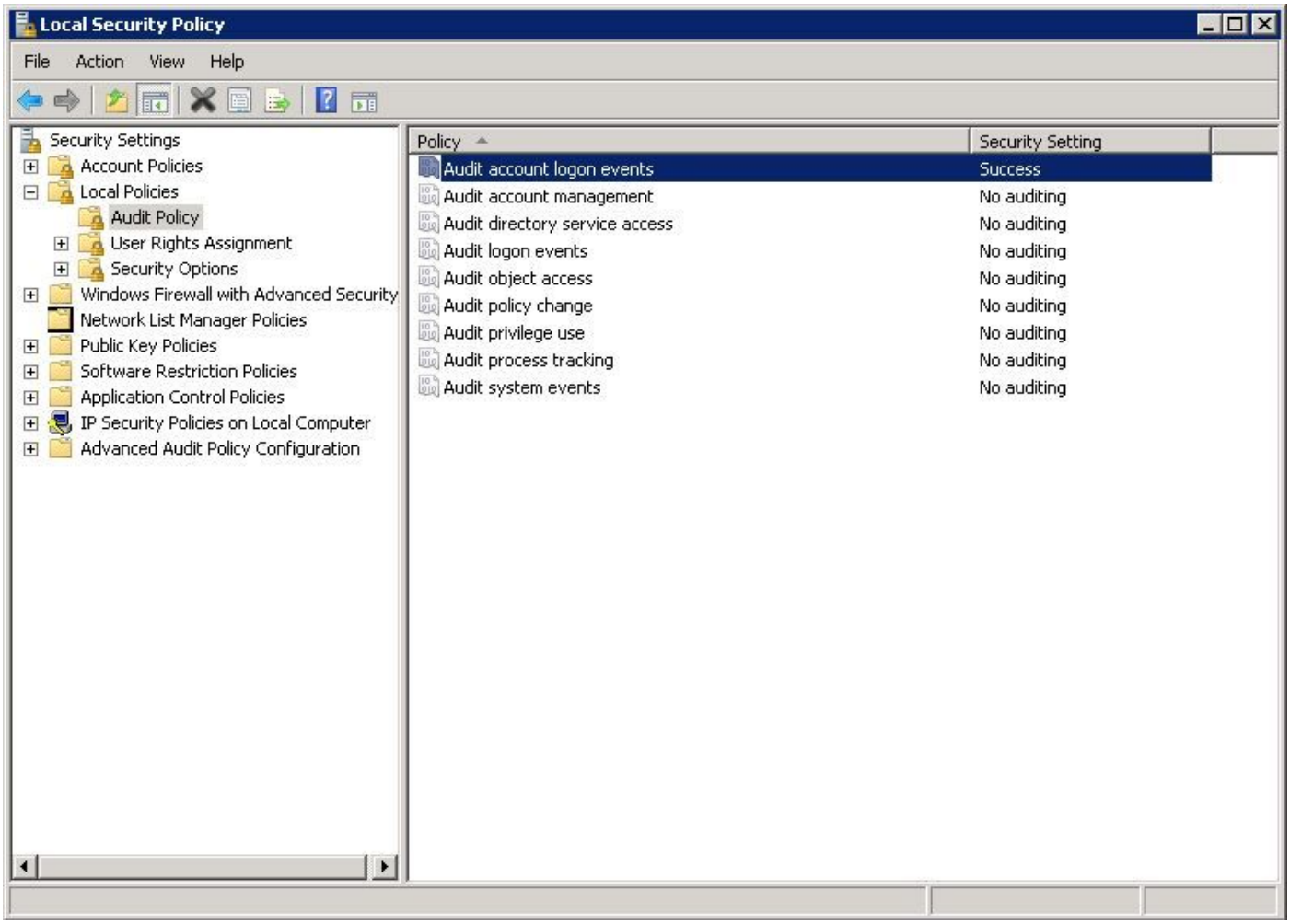
KB4012215 (2008) / KB4012216 (2012)

Um zu überprüfen, dass dieses Problem nicht mit der Protokollierungskonfiguration auf dem Domänencontroller auftritt, stellen Sie sicher, dass die ordnungsgemäße Überwachungsprotokollierung in der lokalen Sicherheitsrichtlinie aktiviert ist. Die fett formatierten Elemente in dieser Ausgabe unten müssen für die ordnungsgemäße Protokollierung von 4768 Ereignis-IDs aktiviert werden. Dies sollte über die Eingabeaufforderung jedes Rechenzentrums ausgeführt werden, das keine Ereignisse protokolliert:

```
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>
```

Wenn Sie sehen, dass die ordnungsgemäße Überwachungsprotokollierung nicht konfiguriert ist, navigieren Sie zu Lokale Sicherheitsrichtlinie > Sicherheitseinstellungen > Lokale Richtlinien > Überwachungsrichtlinie und stellen Sie sicher, dass die Anmeldeereignisse der Überwachungskonten auf Erfolgreich eingestellt sind, wie im Bild gezeigt:



Mögliche Workarounds

(Aktualisiert 31.03.2017)

Als aktuelle Problemumgehung konnten einige Benutzer die oben genannten KBs und die 4768 Ereignis-IDs wieder deinstallieren. Dies hat sich bisher für alle Cisco Kunden als effektiv erwiesen.

Microsoft hat auch einige Kunden, die dieses Problem beheben, wie in Support-Foren gezeigt, die folgende Problemumgehung angeboten. Beachten Sie, dass dies noch nicht vollständig in Cisco Labs getestet oder verifiziert wurde:

Die vier Audit-Richtlinien, die Sie als Problemumgehung für den Fehler aktivieren müssen, finden Sie unter Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. Alle vier Richtlinien in dieser Überschrift sollten für Erfolg und Misserfolg aktiviert sein:

Prüfung der Anmeldeinformationen
Kerberos-Authentifizierungsdienst überprüfen
Kerberos Service Ticket Operations überwachen
Anmeldeereignisse anderer Konten überprüfen

Wenn Sie diese vier Richtlinien aktivieren, sollten Sie die Erfolgsereignisse 4768/4769 erneut anzeigen.

Das Bild oben zeigt die **Konfiguration** der **erweiterten Überwachungsrichtlinie** unten im linken Bereich.

Lösung

Zum Zeitpunkt der Veröffentlichung dieser Erstveröffentlichung (28.03.2017) ist uns noch keine dauerhafte Behebung von Microsoft bekannt. Sie kennen dieses Problem jedoch und arbeiten an einer Lösung.

Es gibt mehrere Threads, die dieses Problem verfolgen:

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

Microsoft TechNet:

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

Dieses Dokument wird aktualisiert, sobald weitere Informationen verfügbar sind oder Microsoft eine dauerhafte Lösung für dieses Problem ankündigt.