User-to-IP Maps wordt na Microsoft Update maart 2017 niet meer weergegeven in Cisco CDA

Inhoud

[Inleiding](#)
[Achtergrondinformatie](#)
[Probleem: User-to-IP Maps wordt na Microsoft Update maart 2017 niet meer weergegeven in Cisco CDA](#)
[Potentiele wonden](#)
[Oplossing](#)

Inleiding

In dit document wordt beschreven hoe de kwestie van de Microsoft Security Update van maart 2017, die de CDA-functionaliteit breekt, kan worden opgelost. Gebruikerspatronen verschijnen niet meer in SWT Context Directory Agent (CDA).

Achtergrondinformatie

Cisco CDA is afhankelijk van Event ID 4768 die wordt ingevuld op alle versies van Windows 2008 en 2012-domeincontrollers. Deze gebeurtenissen duiden op succesvolle openingstijden van gebruikers. Als de "succesopenings"-evenementen niet worden gecontroleerd in het lokale veiligheidsbeleid of als deze gebeurtenis-ID's om een andere reden niet worden ingevuld, zullen de WMI-vragen van CDA voor deze gebeurtenissen geen gegevens opleveren. Als resultaat hiervan zullen de gebruikerstoewijzing niet in CDA worden gemaakt en zal de informatie over gebruikerspatronen niet van CDA naar de adaptieve security applicatie (ASA) worden verzonden. In gevallen waarin klanten gebruik maken van op gebruikers of groepen gebaseerd beleid vanuit AD in Cloud Web Security (CWS), verschijnt de gebruikersinformatie niet in de output van **whoami.scansafe.net**.

> **Opmerking**: Dit heeft geen invloed op Firepower User Agent (UA), aangezien deze gebeurtenis ID 4624 gebruikt om gebruikersafbeeldingen te maken en dit type gebeurtenis niet door deze beveiligingsupdate wordt beïnvloed.

Probleem: User-to-IP Maps wordt na Microsoft Update maart 2017 niet meer weergegeven in Cisco CDA

Een recente Microsoft security update heeft problemen veroorzaakt in verscheidene klantomgevingen waar hun domeincontrollers stoppen met het registreren van deze 4768 gebeurtenis ID's. De betreffende KB's zijn hieronder opgesomd:

KB4012212 (2008) / KB4012213 (2012)

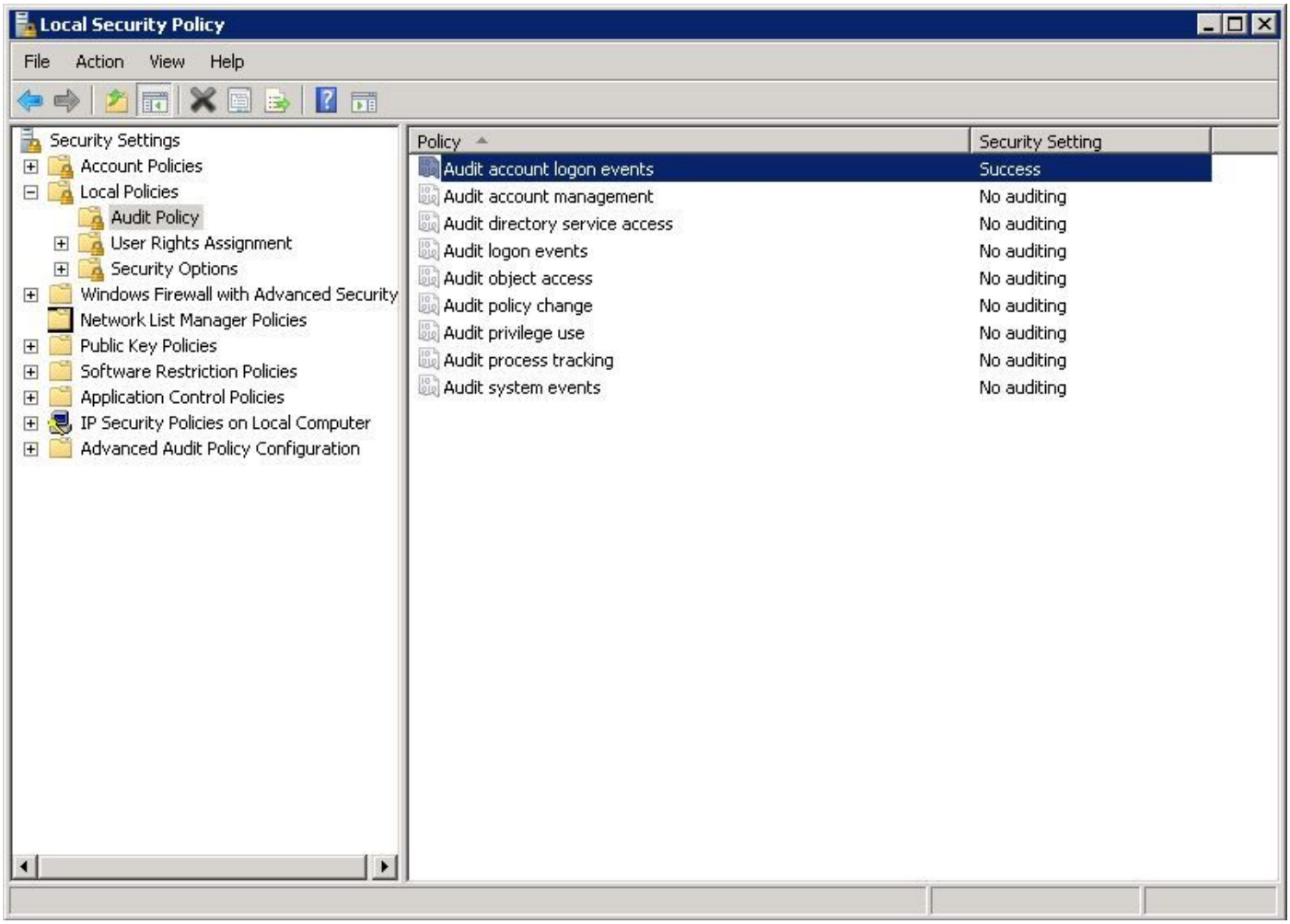
KB4012215 (2008) / KB4012216 (2012)

Om te bevestigen dat deze kwestie niet met de logconfiguratie op de controller van het domein is, zorg er dan voor dat de juiste controleloging is ingeschakeld in het Local Security Policy. De vetgedrukte items in deze hieronder weergegeven uitvoer moeten worden ingeschakeld voor een correcte houtkap van 4768 gebeurtenissen-IDs. Dit moet worden uitgevoerd vanuit de opdrachtmelding van elke DC die geen houtloggebeurtenissen is:

```
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>
```

Als u ziet dat de juiste controleloging niet is geconfigureerd, navigeer dan naar **Local Security Policy > Security Settings > Local Policy > Audit Policy** en zorg ervoor dat de **aanmeldingsgebeurtenissen** van de **account** op **Success** zijn ingesteld, zoals in de afbeelding:



Potentiele wonden

(Bijgewerkt 3/31/2017)

Als huidige tijdelijke oplossing zijn sommige gebruikers in staat geweest om de bovengenoemde KBs te verwijderen en de 4768 gebeurtenis IDs hervat houtkap. Dit is effectief gebleken voor alle klanten van Cisco tot nu toe.

Microsoft heeft ook de volgende gereedschappen geboden aan klanten die dit probleem aanpakken, zoals te zien is op ondersteuningsforums. Merk op dat dit nog niet volledig getest of geverifieerd is in Cisco labs:

> Het vier auditbeleid dat u als tijdelijke oplossing voor de bug moet inschakelen, wordt uitgevoerd onder Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. Alle vier de beleidslijnen in die rubriek moeten worden ingezet voor succes en mislukking:
>
> Verificatiekrediet-validatie
> Audit Kerberos-verificatieservice
> AuditKerberos-servicetechnieken - bewerkingen
> Audit van andere account Aangemelde gebeurtenissen
>
> Wanneer u deze vier beleidslijnen instelt, kunt u de 4768/4769 Success gebeurtenissen

opnieuw zien.

Raadpleeg de afbeelding hierboven die de **configuratie van het geavanceerde auditbeleid** onder in het linker deelvenster toont.

Oplossing

Op de datum van deze eerste publicatie (3/28/2017) weten we nog geen definitieve oplossing van Microsoft. Zij zijn zich echter bewust van deze kwestie en werken aan een oplossing.

Er zijn verschillende draden die dit probleem volgen:

Reddit:

https://www.reddit.com/r/sysadmin/comments/5zs0nc/heads_up_ms_kb4012213_andor_ms_kb4012216_disables/

leaving 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

Dit document wordt bijgewerkt zodra er meer informatie beschikbaar komt of als Microsoft een permanente oplossing voor dit probleem aankondigt.