Las asignaciones de usuario a IP ya no aparecen en Cisco CDA después de marzo de 2017 Microsoft Update

Contenido

Introducción

Este documento describe cómo superar el problema de la actualización de seguridad de Microsoft de marzo de 2017, que interrumpe la funcionalidad de CDA, es decir, Las asignaciones de usuario ya no aparecen en el agente de directorio contextual (CDA) de SWT.

Antecedentes

Cisco CDA confía en que el ID de evento 4768 se rellene en todas las versiones de los controladores de dominio de Windows 2008 y 2012. Estos eventos indican eventos de inicio de sesión de usuario correctos. Si los eventos de inicio de sesión correctos no se auditan en la directiva de seguridad local o si estos ID de evento no se rellenan por ninguna otra razón, las consultas WMI de CDA para estos eventos no devolverán datos. Como resultado, no se crearán asignaciones de usuarios en CDA y, por lo tanto, la información de asignación de usuarios no se enviará desde CDA al dispositivo de seguridad adaptable (ASA). En los casos en que los clientes están aprovechando las políticas basadas en grupos o usuarios de AD en Cloud Web Security (CWS), la información del usuario no aparece en el resultado **whoami.scansafe.net**.

> **Nota**: Esto no afecta a Firepower User Agent (UA), ya que aprovecha la ID de evento 4624 para crear asignaciones de usuario y este tipo de evento no se ve afectado por esta actualización de seguridad.

Problema: Las asignaciones de usuario a IP ya no aparecen en Cisco CDA después de marzo de 2017 Microsoft Update

Una reciente actualización de seguridad de Microsoft ha causado problemas en varios entornos de clientes en los que sus controladores de dominio dejan de registrar estas ID de eventos 4768. Los KB infractores se enumeran a continuación:

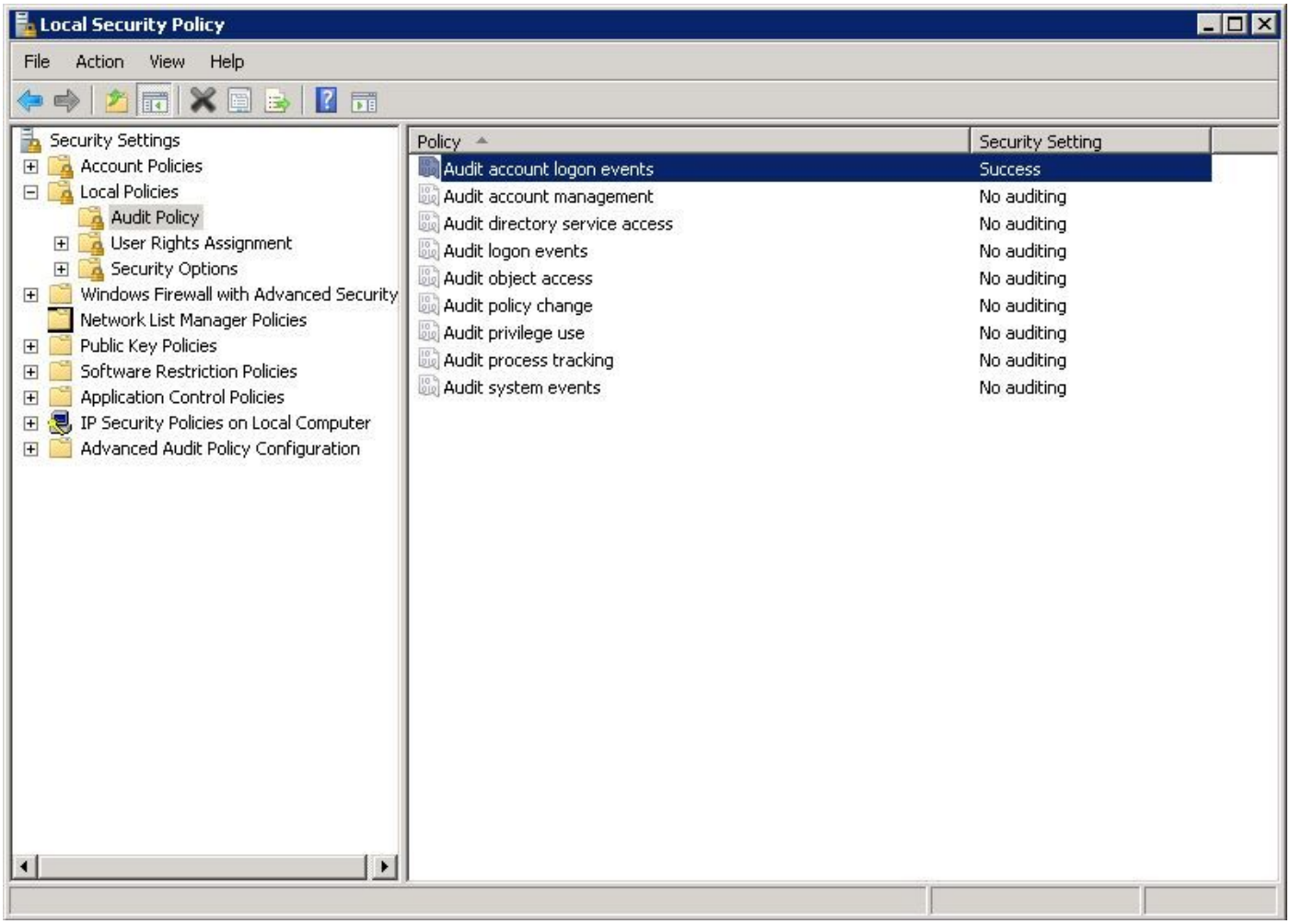
KB4012212 (2008) / KB4012213 (2012)
KB4012215 (2008) / KB4012216 (2012)

Para confirmar que este problema no está con la configuración de registro en el controlador de dominio, asegúrese de que el registro de auditoría adecuado esté habilitado en la política de seguridad local. Los elementos en negrita de esta salida deben estar habilitados para el registro correcto de 4768 ID de eventos. Esto debe ejecutarse desde el símbolo del sistema de cada DC que no esté registrando eventos:

```
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 ve que no se ha configurado el registro de auditoría adecuado, navegue hasta **Política de seguridad local > Configuración de seguridad > Políticas locales > Política de auditoría** y asegúrese de que **Eventos de inicio de sesión de cuenta de auditoría** esté establecido en **Éxito**, como se muestra en la imagen:



Soluciones alternativas potenciales

(Actualizado el 31/03/2017)

Como solución temporal actual, algunos usuarios han podido desinstalar los KB mencionados anteriormente y los ID de evento 4768 reanudaron el registro. Esto ha resultado eficaz para todos los clientes de Cisco hasta el momento.

Microsoft también ha ofrecido la siguiente solución a algunos clientes que han superado este problema, como se ve en los foros de soporte. Tenga en cuenta que esto todavía no se ha probado o verificado completamente en los laboratorios de Cisco:

> Las cuatro políticas de auditoría que debe habilitar como solución alternativa al error se encuentran en Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. Las cuatro políticas bajo ese encabezado deben estar habilitadas para el éxito y el fracaso:
>
> Validación de credenciales de auditoría
> Servicio de autenticación Kerberos de auditoría
> Auditoría de operaciones de notificaciones del servicio Kerberos
> Auditar eventos de inicio de sesión en otra cuenta
>
> Cuando habilita estas cuatro políticas, debe empezar a ver los eventos 4768/4769 Success

de nuevo.

Consulte la imagen anterior que muestra **Advanced Audit Policy Configuration** en la parte inferior del panel izquierdo.

Solución

A la fecha de esta publicación inicial (28/03/2017), todavía no conocemos una solución permanente de Microsoft. Sin embargo, son conscientes de este problema y están trabajando en una solución.

Hay varios subprocesos que siguen este problema:

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

Este documento se actualiza a medida que se dispone de más información o que Microsoft anuncia una solución permanente para este problema.