Las asignaciones Usuario-a-IP aparecen no más en Cisco CDA después de marzo de 2017 Microsoft Update

Contenido

Introducción

Este documento describe cómo superar la aplicación en marzo de 2017 la actualización de seguridad de Microsoft, que rompe al usuario de las funciones CDA es decir que las asignaciones aparecen no más en el agente de directorio del contexto SWT (CDA).

Antecedentes

Cisco CDA confía en el ID de evento 4768 que es poblado en todas las versiones de Windows 2008 y 2012 controladores de dominio. Estos eventos indican los eventos de inicio de sesión acertados del usuario. Si los eventos de inicio de sesión del éxito no están auditoría en Local Security (Seguridad local) la directiva o si estos ID de eventos no se pueblan por cualquier otro motivo entonces las interrogaciones WMI de CDA para estos eventos no devolverán ningún dato. Como consecuencia, las asignaciones del usuario no serán creadas en CDA y por lo tanto la información de mapeo del usuario no será enviada de CDA al dispositivo de seguridad adaptante (ASA). En caso de que los clientes leveraging el usuario o las directivas basadas en el grupo del AD en la Seguridad de la red de la nube (CWS), la información del usuario no aparece en la salida de **whoami.scansafe.net**.

> **Note**: Esto no afecta al agente de usuario de FirePOWER (UA) puesto que leverages el ID de evento 4624 para crear las asignaciones del usuario y esta actualización de seguridad no afecta a ese tipo de evento.

Problema: Las asignaciones Usuario-a-IP aparecen no más en Cisco CDA después de marzo de 2017 Microsoft Update

Una actualización de seguridad reciente de Microsoft ha causado los problemas en varios entornos del cliente en donde sus controladores de dominio paran el registrar de estos 4768 ID de eventos. El KBs que ofende es mencionado abajo:

KB4012212 (2008)/KB4012213 (2012)

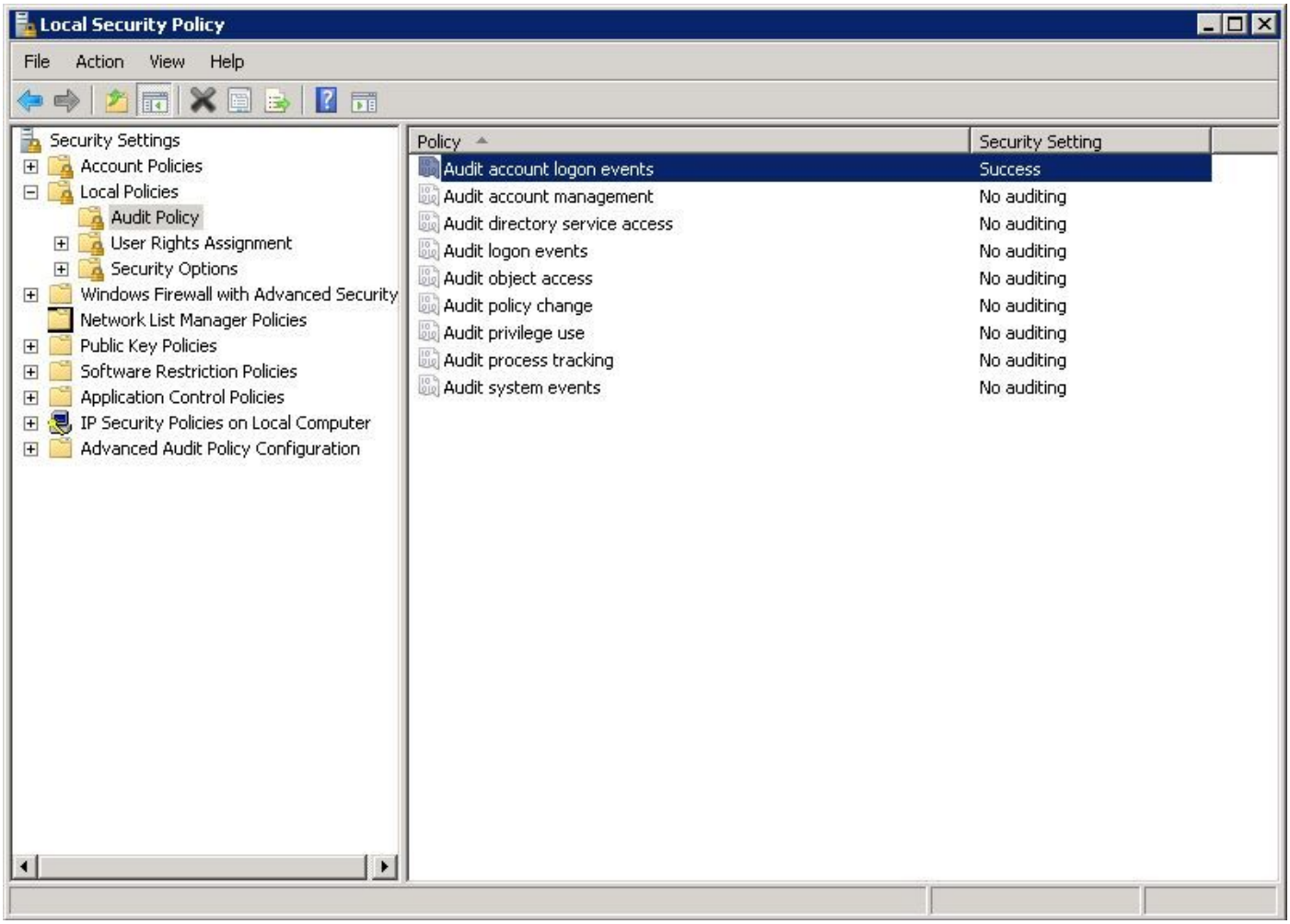
KB4012215 (2008)/KB4012216 (2012)

Para confirmar que este problema no está con la configuración de registro en el controlador de dominio, aseegurese que el registro de auditoría apropiado está habilitado en Local Security (Seguridad local) la directiva. Los elementos en negrita en esta salida debajo del mustbe habilitado para el registro apropiado de 4768 ID de eventos. Esto se debe ejecutar del comando prompt de cada DC que no es eventos de registro:

```
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 usted ve que el registro de auditoría apropiado no está configurado, navegue **Local Security (Seguridad local) a las configuraciones > a las políticas locales > a la directiva de auditoría del > Security (Seguridad) de la directiva** y asegúrese de que los **eventos de inicio de sesión de cuenta de la auditoría** están fijados al **éxito**, tal y como se muestra en de la imagen:



Soluciones alternativas potenciales

(Puesto al día 3/31/2017)

Como solución alternativa actual, algunos usuarios han podido desinstalar el KBs antedicho y los 4768 ID de eventos registración reanudada. Esto ha probado eficaz para todos los clientes de Cisco hasta el momento.

Microsoft también ha proporcionado a la solución alternativa siguiente a algunos clientes que golpeaban este problema como se ve en los foros del soporte. Observe que esto todavía no se ha probado ni se ha verificado completamente en los laboratorios de Cisco:

> Las cuatro directivas de auditoría que usted necesita habilitar mientras que una solución alternativa al bug está bajo la configuración de Computadora \ las directivas \ las configuraciones de Windows \ los ajustes de seguridad \ la configuración de la directiva de auditoría \ las directivas de auditoría \ inicio avanzados de la cuenta. Las cuatro directivas bajo ese título se deben habilitar para el éxito y fracaso:
>
> Validación de los credenciales de la auditoría
> Servicio de autenticación de Kerberos de la auditoría
> Operaciones del boleto del servicio Kerberos de la auditoría
> Auditoría otros eventos de inicio de sesión de cuenta

Cuando usted habilita esas cuatro directivas, usted debe comenzar a ver los eventos del éxito de 4768/4769 otra vez.

Refiera a la imagen sobre eso muestra la **configuración avanzada de la directiva de auditoría** en la parte inferior del panel izquierdo.

Solución

A partir de la fecha de esta publicación inicial (3/28/2017), todavía no sabemos de una corrección permanente de Microsoft. Sin embargo, son conscientes de este problema y del trabajo en un arreglo.

Hay varios hilos 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

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

Se pone al día este documento mientras que más información está disponible o si Microsoft anuncia una corrección permanente para este problema.