Os mapeamentos USER-à-IP aparecem já não em Cisco CDA depois de março de 2017 Microsoft atualizam

Índice

Introdução

Este documento descreve como superar a introdução em março de 2017 da atualização da Segurança de Microsoft, que quebra o usuário que da funcionalidade CDA isto é os mapeamentos já não aparecem no agente de diretório do contexto SWT (CDA).

Informações de Apoio

Cisco CDA confia no ID do evento 4768 que está sendo povoado em todas as versões de janela 2008 e 2012 controladores de domínio. Estes eventos indicam eventos bem sucedidos do fazer logon do usuário. Se os eventos do fazer logon do sucesso não estão sendo examinados na política de segurança local ou se estes ID do evento não são povoados por qualquer outra razão então as perguntas WMI de CDA para estes eventos não retornarão nenhum dados. Em consequência, os mapeamentos do usuário não serão criados em CDA e consequentemente a informação de mapeamento do usuário não será enviada de CDA à ferramenta de segurança adaptável (ASA). Nos casos onde os clientes leveraging o usuário ou políticas grupo-baseadas do AD na Segurança da Web da nuvem (CWs), a informação sobre o usuário não aparece na saída de **whoami.scansafe.net**.

> Nota: Isto não afeta o agente de usuário da potência de fogo (UA) desde que leverages o ID do evento 4624 para criar mapeamentos do usuário e esse tipo de evento não é impactado por esta atualização da Segurança.

Problema: Os mapeamentos USER-à-IP aparecem já não em Cisco CDA depois de março de 2017 Microsoft atualizam

Uma atualização recente da Segurança de Microsoft causou edições em diversos ambientes de cliente onde seus controladores de domínio param de registrar estes 4768 ID do evento. O KBs de ofensa está listado abaixo:

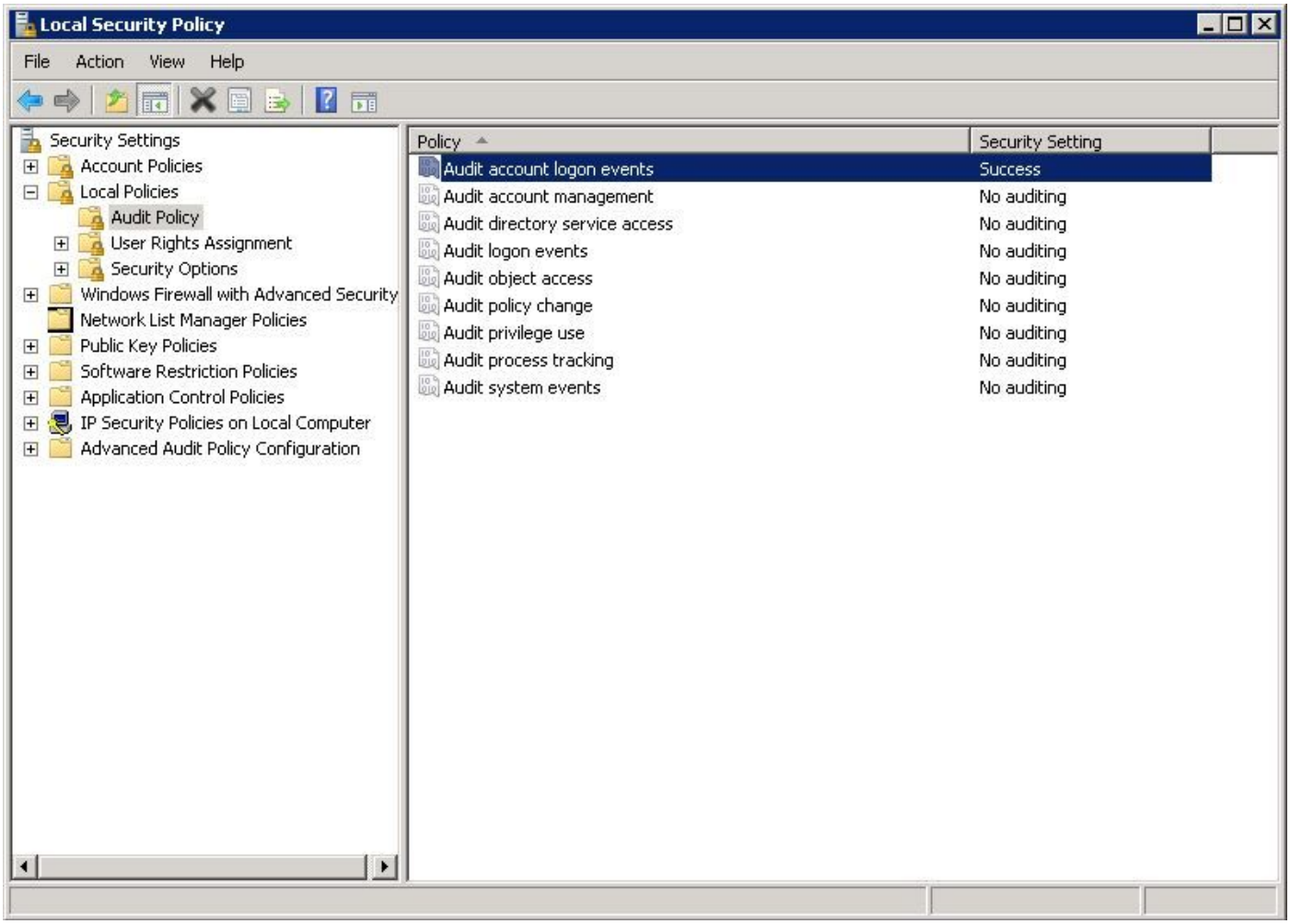
KB4012212 (2008)/KB4012213 (2012)

KB4012215 (2008)/KB4012216 (2012)

Para confirmar que esta edição não é com a configuração de registro no controlador de domínio, certifique-se de que o registro apropriado da auditoria está permitido na política de segurança local. Os itens em negrito nesta saída abaixo do mustbe permitido para um registro apropriado de 4768 ID do evento. Isto deve ser executado do comando prompt de cada DC que não é 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>
```

Se você vê que o registro apropriado da auditoria não está configurado, navegue aos **ajustes do > segurança da política de segurança local > às políticas local > à política da auditoria** e assegure-se de que os **eventos do fazer logon da conta de auditoria** estejam ajustados ao **sucesso**, segundo as indicações da imagem:



Ações alternativas potenciais

(Atualizado 3/31/2017)

Como uma solução alternativa atual, alguns usuários puderam desinstalar o KBs acima mencionado e os 4768 ID do evento registro recomeçado. Isto provou eficaz para todos os clientes Cisco até aqui.

Microsoft igualmente forneceu a seguinte ação alternativa a alguns clientes que batem esta edição como visto em fóruns do apoio. Note que isto não esteve testado ainda nem esteve verificado inteiramente nos laboratórios Cisco:

> As quatro políticas que da auditoria você precisa de permitir enquanto uma ação alternativa ao erro está sob a configuração de computador \ políticas \ ajustes de Windows \ configurações de segurança \ configuração das normas da auditoria \ políticas da auditoria \ fazer logon avançados da conta. Todas as quatro políticas sob esse título devem ser permitidas para o sucesso e falha:
>
> Validação das credenciais da auditoria
> Serviço de autenticação de Kerberos da auditoria
> Operações do bilhete do serviço de kerberos da auditoria
> Examine outros eventos do fazer logon da conta

Quando você permite aquelas quatro políticas, você deve começar ver outra vez os eventos do sucesso de 4768/4769.

Refira a imagem acima disso mostra **configuração das normas avançada da auditoria na** parte inferior do painel esquerdo.

Solução

Até à data da data desta publicação inicial (3/28/2017), nós não sabemos ainda de um reparo permanente de Microsoft. Contudo, estão cientes desta edição e do trabalho em um reparo.

Há diversas linhas que seguem esta edição:

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 está atualizado enquanto mais informação se torna disponível ou se Microsoft anuncia um reparo permanente para esta edição.