Mapeamentos de usuário para IP não aparecem mais no Cisco CDA após março de 2017 Microsoft Update

Contents

Introduction

Este documento descreve como resolver o problema da atualização de segurança da Microsoft de março de 2017, que interrompe a funcionalidade do CDA, por exemplo: Os mapeamentos de usuário não aparecem mais no SWT Context Diretory Agent (CDA).

Informações de Apoio

O Cisco CDA confia no preenchimento da ID de evento 4768 em todas as versões dos controladores de domínio do Windows 2008 e 2012. Esses eventos indicam eventos de logon de usuário bem-sucedidos. Se os eventos de login bem-sucedidos não estiverem sendo auditados na política de segurança local ou se essas IDs de evento não forem preenchidas por qualquer outro motivo, as consultas WMI do CDA para esses eventos não retornarão nenhum dado. Como resultado, os mapeamentos de usuário não serão criados no CDA e, portanto, as informações de mapeamento de usuário não serão enviadas do CDA para o Adaptive Security Appliance (ASA). Nos casos em que os clientes estão utilizando políticas baseadas em grupo ou em usuário do AD no Cloud Web Security (CWS), as informações do usuário não aparecem na saída **whoami.scansafe.net**.

> **Nota**:Isso não afeta o Firepower User Agent (UA), pois ele aproveita o ID de evento 4624 para criar mapeamentos de usuário e esse tipo de evento não é afetado por essa atualização de segurança.

Problema: Mapeamentos de usuário para IP não aparecem mais no Cisco CDA após março de 2017 Microsoft Update

Uma atualização de segurança recente da Microsoft causou problemas em vários ambientes de clientes em que seus controladores de domínio param de registrar essas IDs de evento 4768. Os KBs ofensivos estão listados abaixo:

KB4012212 (2008) / KB4012213 (2012)

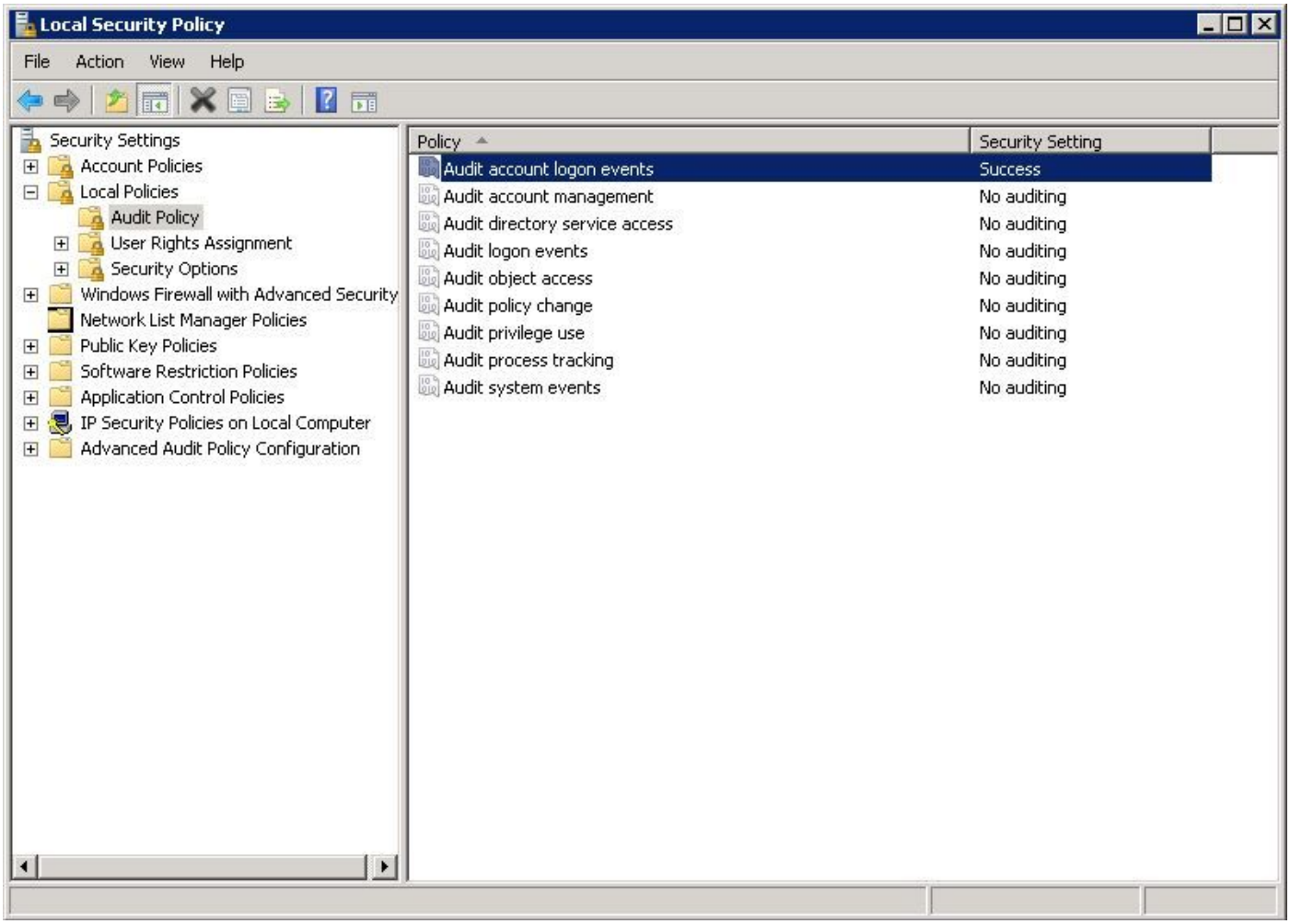
KB4012215 (2008) / KB4012216 (2012)

Para confirmar se esse problema não está na configuração de registro no Controlador de domínio, verifique se o registro de auditoria apropriado está habilitado na Diretiva de Segurança Local. Os itens em negrito nesta saída abaixo devem ser ativados para o registro correto de 4768 IDs de eventos. Isso deve ser executado a partir do prompt de comando de cada DC que não esteja 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>
```

Se você vir que o registro de auditoria correto não está configurado, navegue para **Diretiva de Segurança Local > Configurações de Segurança > Políticas Locais > Política de Auditoria** e certifique-se de que **Auditoria de eventos de logon de conta** esteja definida como **Êxito**, como mostrado na imagem:



Possíveis soluções alternativas

(Atualizado em 31/03/2017)

Como solução alternativa atual, alguns usuários puderam desinstalar os KBs mencionados acima e os IDs de evento 4768 retomaram o registro. Isso tem se mostrado eficaz para todos os clientes da Cisco até agora.

A Microsoft também forneceu a solução a seguir para alguns clientes que estão enfrentando esse problema, como visto nos fóruns de suporte. Observe que isso ainda não foi totalmente testado ou verificado nos laboratórios da Cisco:

> As quatro políticas de auditoria que você precisa ativar como solução alternativa para o bug estão em Computador Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. Todas as quatro políticas sob esse cabeçalho devem ser habilitadas para Êxito e Falha:
>
> Validação de credenciais de auditoria
> Serviço de Autenticação Kerberos de Auditoria
> Auditoria de operações de tíquete de serviço Kerberos
> Auditoria de outros eventos de login da conta
>
> Ao habilitar essas quatro políticas, você deve começar a ver os eventos 4768/4769 Success

novamente.

Consulte a imagem acima que mostra **Advanced Audit Policy Configuration** na parte inferior do painel esquerdo.

Solução

A partir da data desta publicação inicial (28/03/2017), ainda não sabemos de uma correção permanente da Microsoft. No entanto, eles estão cientes desse problema e trabalhando em uma solução.

Há vários processos rastreando esse 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 é atualizado à medida que mais informações ficam disponíveis ou se a Microsoft anunciar uma correção permanente para este problema.