2017年3月Microsoft更新后，Cisco CDA中不再显示用户到IP的映射

目录

简介

本文档介绍如何克服2017年3月Microsoft安全更新问题，该问题中断了CDA功能，即用户映射不再显示在SWT情景目录代理(CDA)中。

背景信息

思科CDA依赖于在所有Windows 2008和2012域控制器版本上填充的事件ID 4768。这些事件表示成功的用户登录事件。如果在本地安全策略中未审核成功登录事件，或者由于任何其他原因未填充这些事件ID，则来自CDA的这些事件的WMI查询将不返回任何数据。因此，用户映射不会在CDA中创建，因此用户映射信息不会从CDA发送到自适应安全设备(ASA)。 如果客户在云网络安全(CWS)中利用AD中的基于用户或基于组的策略，则用户信息不会显示在**whoami.scansafe.net输**出中。

> **注意**：这不会影响Firepower用户代理(UA)，因为它利用事件ID 4624创建用户映射，并且该类型的事件不受此安全更新的影响。

问题：2017年3月Microsoft更新后，Cisco CDA中不再显示用户到IP的映射

最近的Microsoft安全更新在几个客户环境中导致其域控制器停止记录这些4768事件ID的问题。 违规知识库列于下面：

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

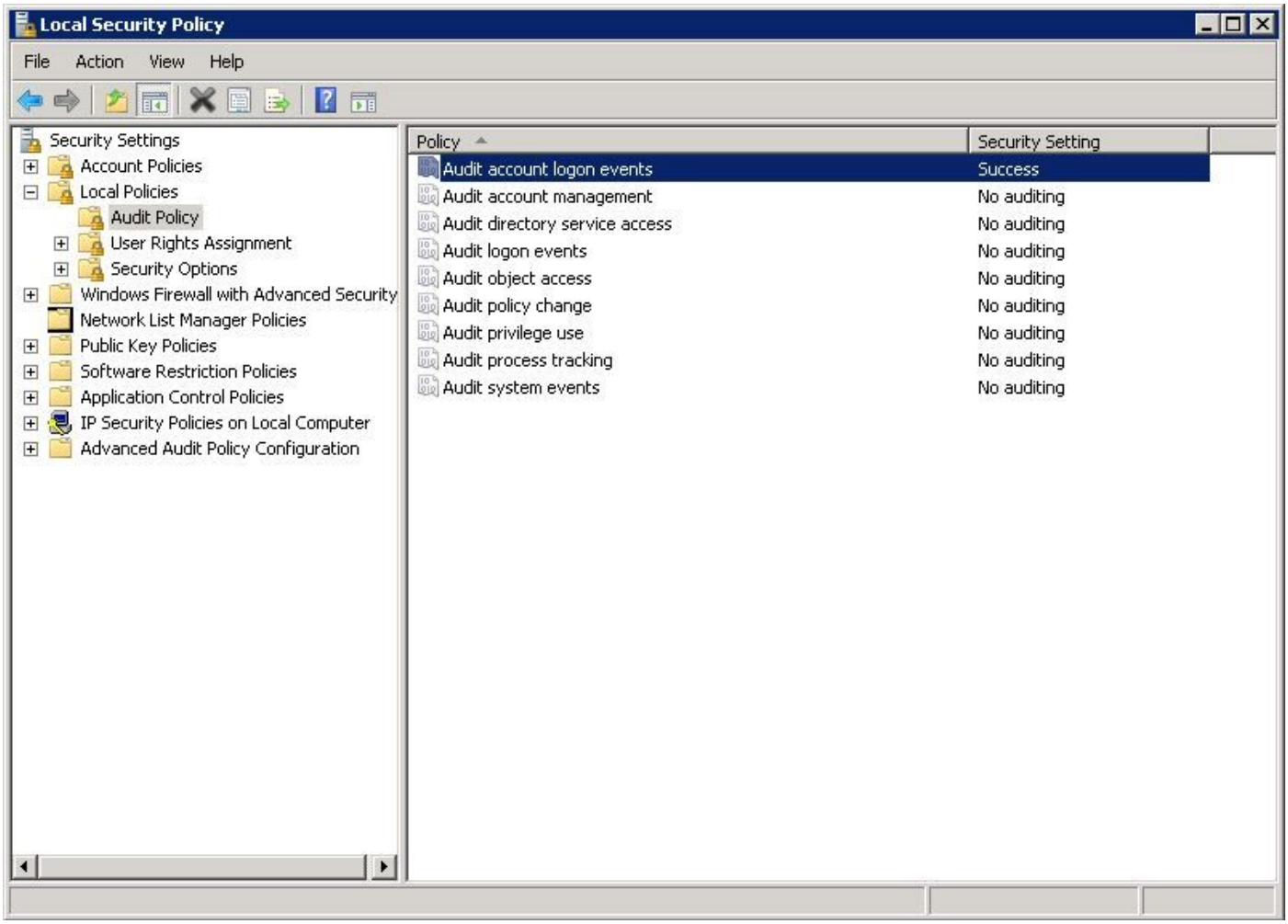
要确认此问题与域控制器上的日志记录配置无关，请确保在本地安全策略中启用了正确的审核日志记录。 必须启用下面此输出中的粗体项，才能正确记录4768个事件ID。应从未记录事件的每个DC的命令提示符运行以下命令：

```
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>
```

如果您看到未配置正确的审核日志记录，请导航到**Local Security Policy > Security Settings > Local Policies > Audit Policy**，并确保**Audit account logon events**设置为**Success**，如图所示：



潜在解决方法

(更新3/31/2017)

作为当前的解决方法，一些用户已能卸载上述知识库，4768个事件ID已恢复日志记录。事实证明，这对迄今为止所有思科客户都有效。

Microsoft还为一些遇到此问题的客户提供了以下解决方法，如支持论坛中所示。 请注意，这尚未在思科实验室中完全测试或验证：

> 您需要启用的四个审计策略作为对漏洞的解决方法，位于计算机Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon下。标题下的所有四个策略都应启用“成功和失败：
>
> 审核凭证验证
> 审核Kerberos身份验证服务
> 审核Kerberos服务票证操作
> 审核其他帐户登录事件
>
> 启用这四个策略后，您应开始再次看到4768/4769 Success事件。

请参阅左窗格底部**显示高级审**核策略配置的上图。

解决方案

截至本初始发布日期(3/28/2017)，我们尚不知道Microsoft提供的永久性修复。但是，他们了解此问题，并正在解决问题。

跟踪此问题的线程有多个：

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

当更多信息可用或Microsoft宣布永久修复此问题时，本文档会更新。