用户对IP映射在思科CDA中不再出现，在三月2017 Microsoft更新后

目录

简介

本文描述如何解决三月2017 Microsoft安全更新问题，即中断CDA功能用户映射在SWT上下文目录代理(CDA)不再出现。

背景信息

思科CDA依靠在所有Windows版本4768填充的事件ID 2008年和2012个域控制器。这些事件指示成功的用户登录事件。 如果成功登录事件在本地安全策略没有审计或，如果这些事件ID为其它原因没有填充然后从CDA的WMI查询这些事件的不会返回数据。结果，用户映射在CDA不会创建并且用户映射信息不会从CDA发送到可适应安全工具(ASA)。在客户有效利用用户或基于组的策略从AD在Cloud Web安全(CWS)处，用户信息在**whoami.scansafe.net**输出中没出现。

> **Note**:这不影响Firepower用户代理(UA)，因为有效利用事件ID 4624创建用户映射，并且那种事件没有由此安全更新影响。

问题：用户对IP映射在思科CDA中不再出现，在三月2017 Microsoft更新后

一次最近的Microsoft安全更新的几用户环境导致了问题，他们的域控制器停止记录这4768事件ID。 触犯的KBs如下是列出的：

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

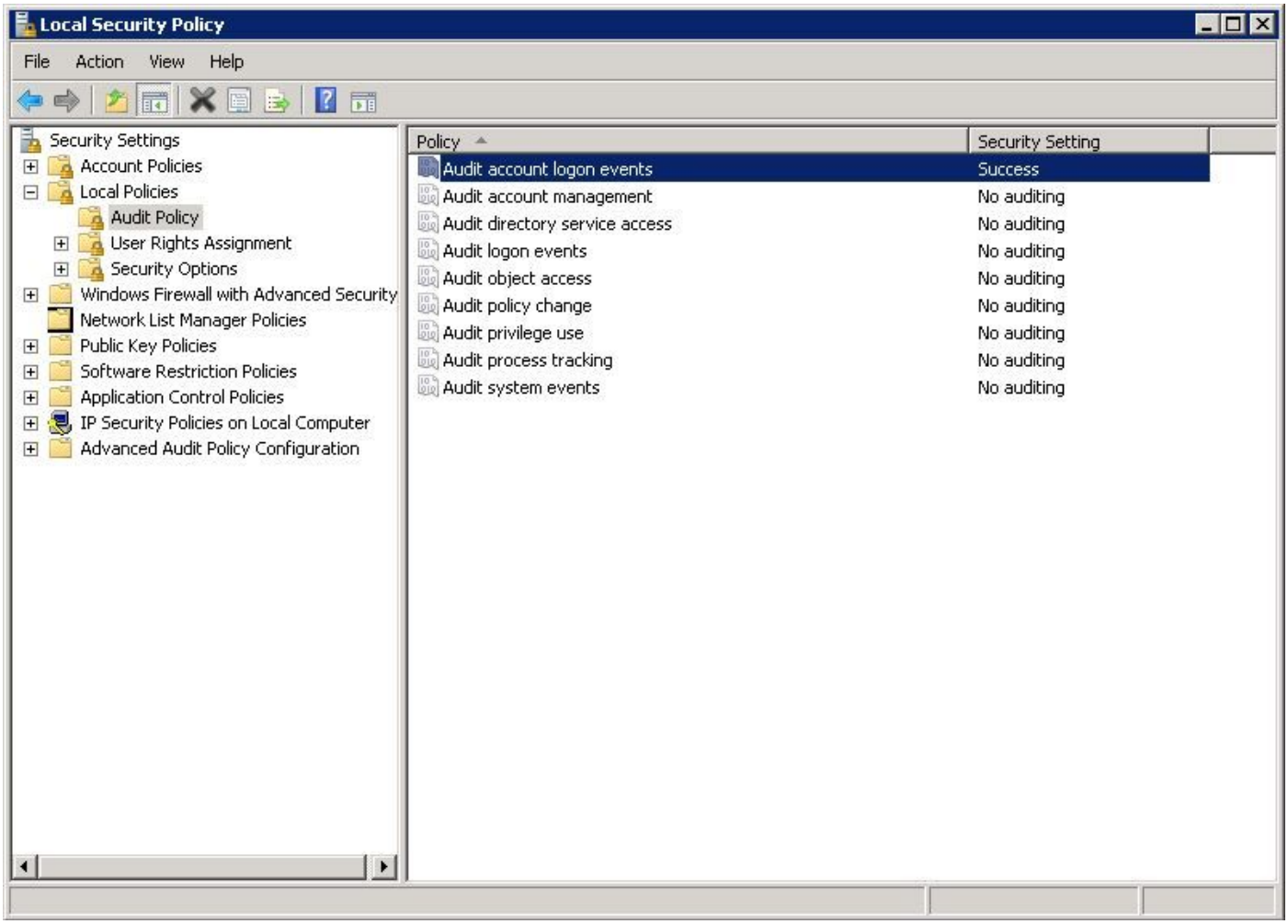
要确认此问题不是在域控制器的操作日志配置，请确保适当的审计日志在本地安全策略启用。 粗体项目在此输出中在为4768事件ID适当的记录日志启用的mustbe之下。应该从不是操作日志事件每个DC的prompt命令运行这：

```
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>
```

如果看到适当的审计日志没有配置，请导航对**本地安全策略> Security设置>本地策略>审计策略**并且保证**已审核的帐目登录事件**设置为**成功**，如镜像所显示， ：



潜在应急方案

(更新3/31/2017)

作为一当前应急方案，一些用户能卸载恢复的上述的KBs和4768事件ID记录日志。 这至今证明有效所有Cisco用户的。

Microsoft也提供了以下应急方案给点击此问题的一些客户如在支持论坛中看到。 注意这在思科实验室充分地未测试也未验证：

> 您需要启用的四项审计策略，当对bug的一应急方案在计算机配置\策略\ Windows设置\安全设置\先进的审计策略配置\审计策略\帐户登录下。应该为成败启用在该标题下的全部四项策略：
>
> 审计凭证验证
> 审计Kerberos认证服务
> 审计Kerberos服务票操作
> 审计其他帐户登录事件
>
> 当您启用那些四项策略时，您应该开始再看到4768/4769成功事件。

参考在那上的镜像在左窗格的底部显示**先进的审计策略配置**。

解决方案

自日期此最初的出版物(3/28/2017)，我们不知道从Microsoft的一个永久的修正。然而，他们知道此问题和工作在修正。

有跟踪此问题的几个线索：

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

本文更新，当更多信息变为联机或，如果Microsoft宣布此问题的一个永久的修正。