在2017年3月Microsoft Update之後，使用者到IP的對映不再出現在Cisco CDA中

目錄

簡介

本文檔介紹如何克服2017年3月發佈的Microsoft安全更新問題。使用者對映不再出現在SWT上下文目錄代理(CDA)中。

背景資訊

思科CDA依賴於所有版本的Windows 2008和2012域控制器上填充的事件ID 4768。這些事件指示成功的使用者登入事件。如果本地安全策略中未稽核成功登入事件，或者這些事件ID由於任何其他原因未填充，則從CDA對這些事件的WMI查詢將不返回任何資料。因此，不會在CDA中建立使用者對映，因此使用者對映資訊不會從CDA傳送到自適應安全裝置(ASA)。 如果客戶在Cloud Web Security(CWS)中使用AD中的使用者或基於組的策略，則使用者資訊不會顯示在**whoami.scansafe.net輸出**中。

> **注意**：這不會影響Firepower使用者代理(UA)，因為它利用事件ID 4624建立使用者對映，並且該型別的事件不受此安全更新的影響。

問題：在2017年3月Microsoft Update之後，使用者到IP的對映不再出現在Cisco CDA中

最近的Microsoft安全更新導致多個客戶環境出現問題，其中他們的域控制器停止記錄這些4768事件ID。 有問題的KB如下所示：

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

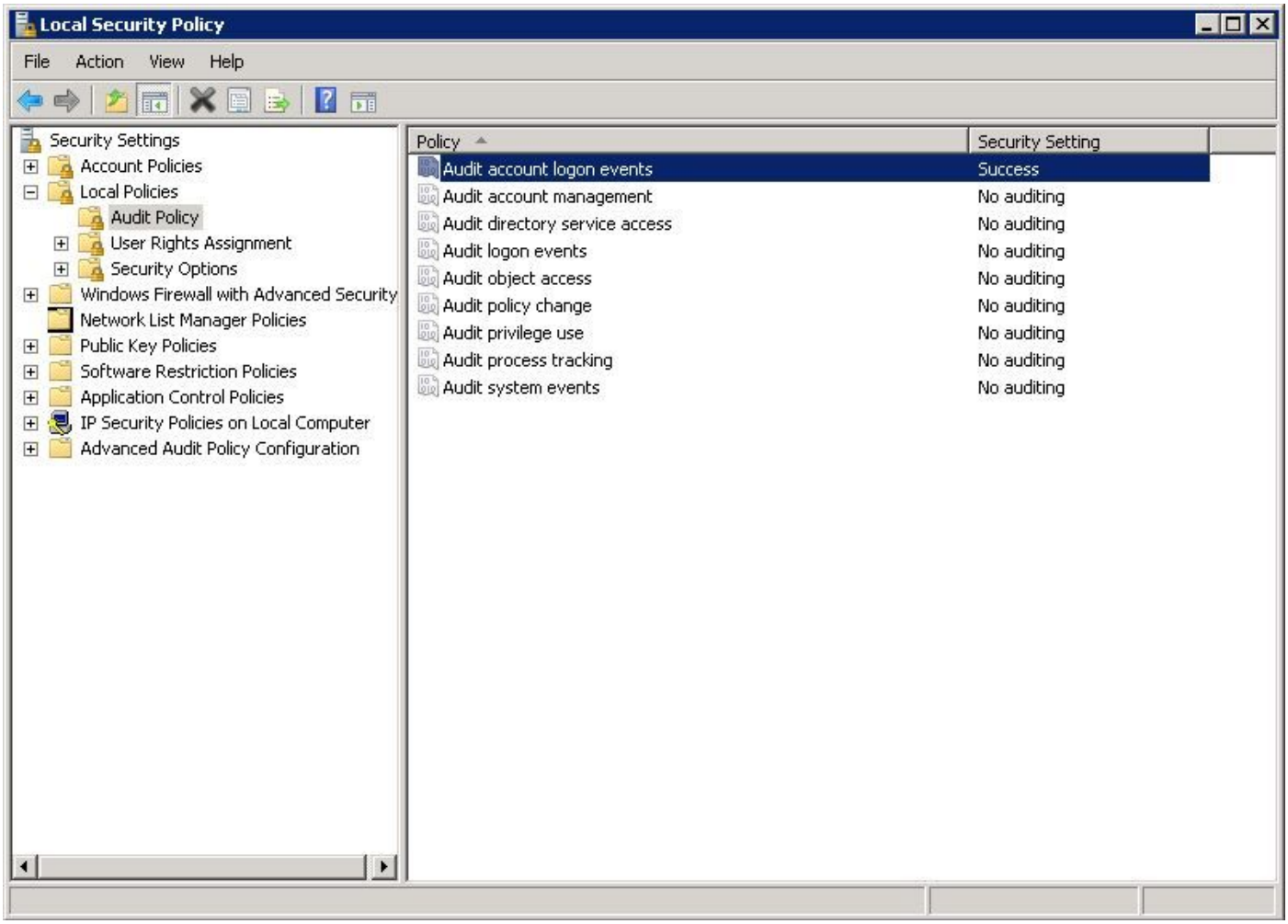
要確認此問題與域控制器上的日誌記錄配置無關，請確保在本地安全策略中啟用了正確的稽核日誌記錄。 必須啟用以下輸出中的粗體專案，才能正確記錄4768事件ID。此操作應從每個未記錄事件的DC的命令提示符運行：

```
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確的稽核日誌記錄，請導航到**Local Security Policy > Security Settings > Local Policies > Audit Policy**，並確保**Audit account logon events**設定為**Success**，如下圖所示：



可能的變通辦法

（2017年3月31日更新）

目前的解決方法是，某些使用者能夠解除安裝上述知識庫，而4768事件ID恢復日誌記錄。迄今為止，此方法對所有思科客戶均有效。

Microsoft還為某些遇到此問題的客戶提供了以下解決方法，這在支援論壇中可見。 請注意，這尚未在思科實驗室中經過充分測試或驗證：

> 您需要啟用作為錯誤解決方法的四個審計策略位於「電腦配置\策略\Windows設定\安全設定\高級審計策略配置\審計策略\帳戶登入」下。該標題下的所有四個策略都應啟用「成功」和「失敗」：
>
> 稽核憑據驗證
> 審計Kerberos身份驗證服務
> 稽核Kerberos服務票證操作
> 稽核其他帳戶登入事件
>
> 啟用這四個策略後，您應該開始再次看到4768/4769成功事件。

請參閱左窗格底部的**Advanced Audit Policy Configuration**上圖。

解決方案

截至本首次發佈日期（2017年3月28日），我們還不知道Microsoft提供永久修補程式。但是，他們知道此問題並正在處理修復。

有多個執行緒跟蹤此問題：

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

當更多資訊可用或Microsoft宣佈永久修復此問題時，將更新此文檔。