2017 年 3 月の Microsoft 更新プログラムの適用後にユーザから IP へのマッピングが Cisco CDA に表示されない

内容

概要

このドキュメントでは、2017年3月のMicrosoftセキュリティアップデートの問題を解決する方法について説明します。この問題により、CDAの機能が中断されます。ユーザマッピングがSWT Context Directory Agent(CDA)に表示されなくなりました。

背景説明

Cisco CDA は、Windows 2008 および 2012 ドメイン コントローラのすべてのバージョンでイベント ID 4768 に値があることを前提としています。これらのイベントは、ユーザー・ログオンの成功を示します。成功ログオン・イベントがローカルのセキュリティ・ポリシーで監査されていない場合、またはこれらのイベントIDが他の理由で入力されていない場合は、CDAからこれらのイベントのWMIクエリーはデータを返しません。その結果、ユーザ マッピングが CDA で作成されず、ユーザ マッピング情報が CDA から適応型セキュリティ アプライアンス（ASA）に送信されません。 お客様がクラウド Web セキュリティ（CWS）で AD のユーザまたはグループ ベースのポリシーを使用している場合、**whoami.scansafe.net の出力にユーザ情報が表示されません。**

> **注**：これはFirepower User Agent(UA)には影響しません。これは、イベントID 4624を使用してユーザマッピングを作成し、このタイプのイベントがこのセキュリティアップデートの影響を受けないためです。

問題：2017 年 3 月の Microsoft 更新プログラムの適用後にユーザから IP へのマッピングが Cisco CDA に表示されない

最近公開された Microsoft セキュリティ更新プログラムが原因で、ドメイン コントローラがイベント ID 4768 を記録しなくなるという問題が多くの顧客環境で発生しています。 この問題を引き起こす KB を以下に示します。

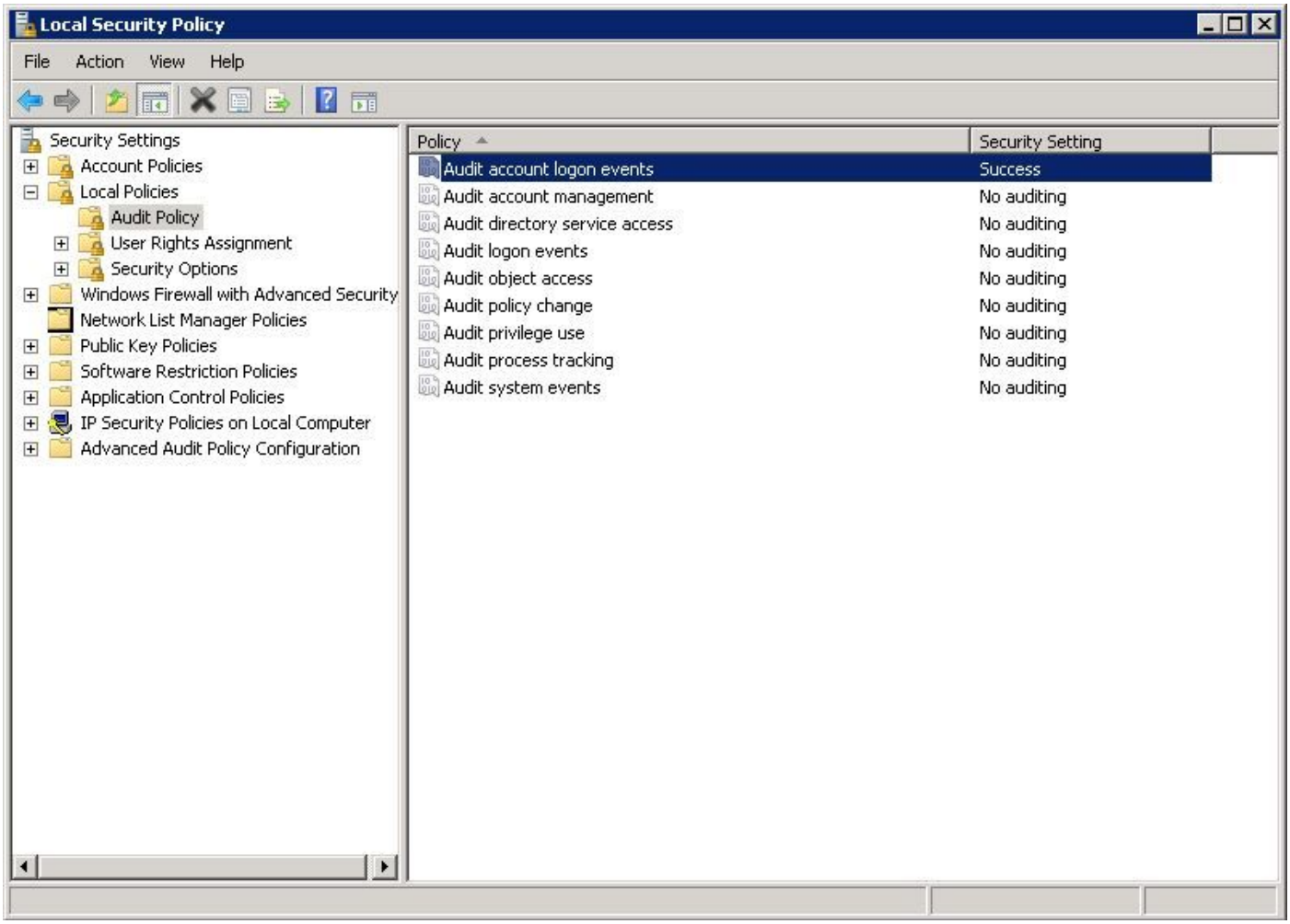
KB4012212（2008）/KB4012213（2012）
KB4012215（2008）/KB4012216（2012）

この問題がドメイン コントローラのロギング設定に関連していないことを確認するため、ローカル セキュリティ ポリシーで適切な監査ロギングが有効になっていることを確認してください。
次の出力では、イベント ID 4768 を適切にログに記録するために有効にする必要がある項目が太字で示されています。これは、イベントをログに記録しない各 DC のコマンド プロンプトから実行する必要があります。

```
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>
```

適切な監査ロギングが設定されていない場合には、[Local Security Policy] > [Security Settings] > [Local Policies] > [Audit Policy] に移動し、次の図に示すように [Audit account logon events] が [Success] に設定されていることを確認します。



考えられる回避策

(更新：2017 年 3 月 31 日)

現在の回避策として、前述のKBをアンインストールし、4768イベントIDのログを再開したユーザもいます。これは、シスコの全ての顧客にとって有効な方法です。

また、この問題が発生した一部のお客様に対し、Microsoft はサポート フォーラムで次の回避策を公開しました。 Cisco のラボではこの回避策を完全にテストまたは検証していないことに注意してください。

> このバグに対する回避策として、Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon にある次の 4 つの監査ポリシーを有効にする必要があります。このヘッダーの下にある 4 つのポリシーすべてを Success and Failure に設定する必要があります。
>
> Audit Credential Validation
> Audit Kerberos Authentication Service
> Audit Kerberos Service Ticket Operations
> Audit Other Account Logon Events
>
> この 4 つのポリシーを有効にすると、4768/4769 Success イベントが再び表示されるようになります。

左側のペインの下部に [Advanced Audit Policy Configuration] **がある上記の図を参照してください。**

解決方法

この記事の初回公開の時点（2017 年 3 月 28 日）では、Microsoft による正式な修正については不明です。ただし Microsoft はこの問題を認識しており、修正に取り組んでいます。

この問題を追跡するスレッドがいくつかあります。

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

このドキュメントは、追加の詳細が判明した時点、または Microsoft からこの問題に対する正式な修正が発表された時点で更新されます。