ユーザに IP マッピングは Cisco CDA にもはや後行進 2017 Microsoft アップデート現われました

目次

概要

この資料に CDA 機能性マッピングが SWT コンテキスト ディレクトリエージェント（CDA）にもはや現われないすなわちユーザを壊す行進 2017 Microsoft セキュリティ更新プログラムの問題を解決する方法を記述されています。

背景説明

Cisco CDA はすべての Windowsのバージョンで 2008 年および 2012 人の読み込まれるイベント ID 4768 にドメインコントローラ頼ります。 これらのイベントは正常なユーザ ログオン イベントを示します。 成功ログオン イベントがローカル セキュリティ ポリシーで監査されないか、またはこれらのイベント ID がそしてその他の理由で読み込まれなければこれらのイベントのための CDA からの WMI クエリはデータを返しません。 その結果、ユーザ マッピングは CDA で作成されないし、従ってユーザ マッピング情報は CDA から適応性があるセキュリティ アプライアンス モデル（ASA）に送信 されません。 顧客が Cloud Web セキュリティ（CWS）の AD からのユーザかグループ ベース ポリシーを活用 すれば、ユーザ情報は **whoami.scansafe.net** 出力に現われません。

> **注:** これはユーザ マッピングを作成するのにイベント ID 4624 を活用 し、イベントのその型がこのセキュリティ更新プログラムによって影響を与えられないので火力ユーザ エージェント（UA）に影響を与えません。

問題： ユーザに IP マッピングは Cisco CDA にもはや後行進 2017 Microsoft アップデート現われました

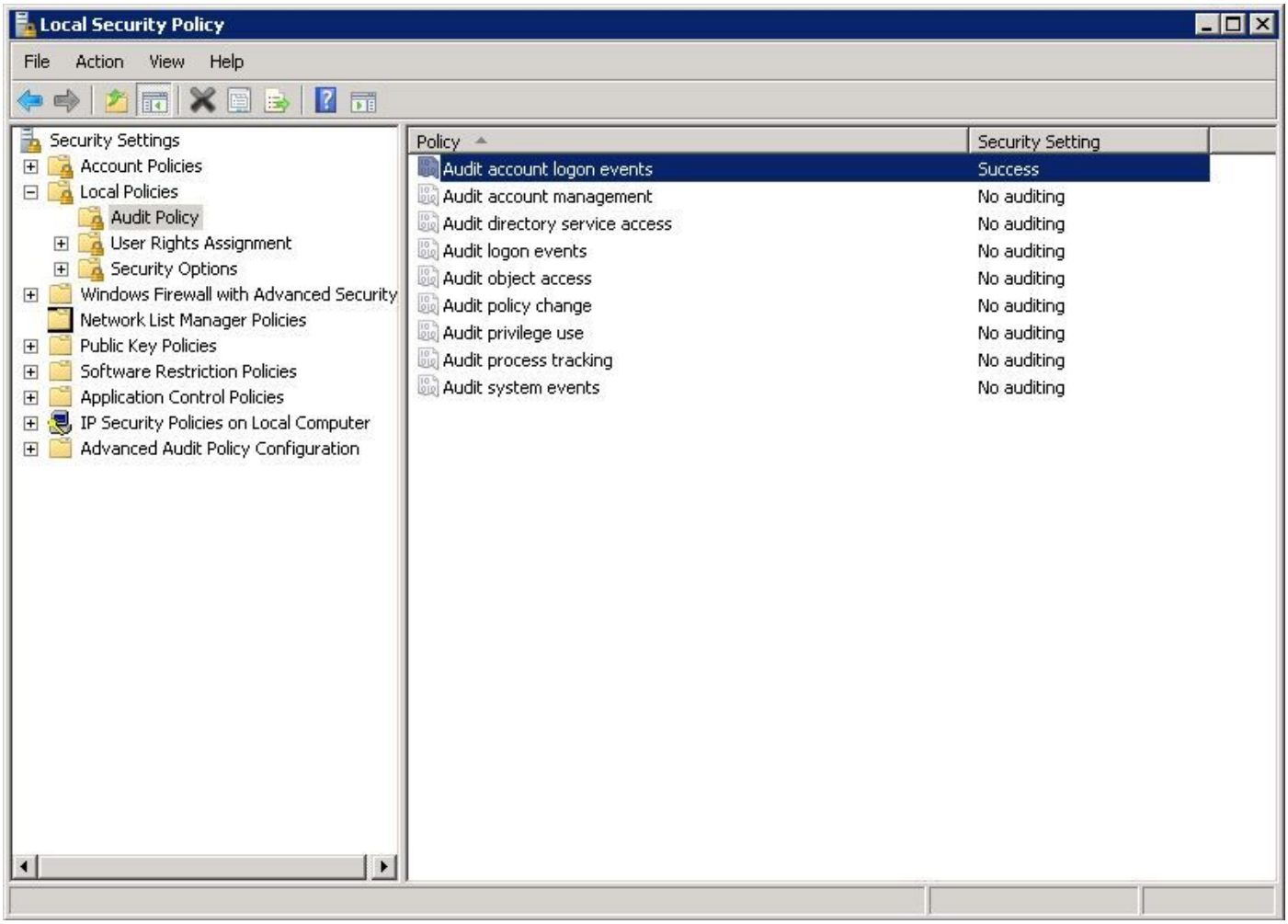
Microsoft 最近のセキュリティ更新プログラムは複数の顧客 の 環境でドメインコントローラがこの 4768 イベント ID を記録 することを止めるか問題を引き起こしていました。 おこる KB は下記のようにリストされています:

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

適切な監査 記録がローカル セキュリティ ポリシーで有効に なることをこの問題がドメインコントローラのログコンフィギュレーションとないことを確認するために、確かめて下さい。 4768 イベント ID の適切なロギングのために有効に なる mustbe の下のこの出力の太字の項目。 これはロギングイベントではない各 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 記録は設定されないことがわかったら、**ローカル セキュリティ ポリシー > Security 設定 > ローカル ポリシー > 監査 ポリシー**にナビゲート し、イメージに示すように、**監査済み勘定ログオン イベントが成功**に設定 されるようにして下さい:



可能性のある回避策

（3/31/2017 アップデートされる）

現在の回避策として、何人かのユーザは前述の KB および 4768 イベント ID をアンインストール ずっと再開された記録できます。 これはすべての Ciscoカスタマー向けの有効これまでに証明しました。

Microsoft はまたサポート フォーラムに見られるようにこの問題を見つけている何人かの顧客に次の回避策を提供しました。 これが Cisco ラボでまだ十分にテストされなかったし、または確認されなかったことに注目して下さい:

> 不具合への回避策がコンピューターの構成\ポリシー\ Windows 設定\セキュリティ設定\高度監査 ポリシー 設定\監査ポリシー\アカウント ログオンの下にあると同時に有効に する必要がある 4 つの監査ポリシー。 その見出しの下の 4 つのポリシーはすべて成功 および 失敗のために有効に する必要があります:
>
> 監査 資格情報 検証
> 監査 Kerberos認証サービス
> 監査 Kerberosサービス チケット オペレーション
> 他のアカウント ログオン イベントを監査して下さい
>
> それらの 4 つのポリシーを有効に するとき、4768/4769 成功イベントを再度参照し始める必要があります。

それの上のイメージを示します左ペインの下部の**で高度監査 ポリシー 設定を**参照して下さい。

解決策

この最初のパブリケーション（3/28/2017）の日付現在で、Microsoft からのパーマネント修正のまだ知っていません。 ただし、それらは修正でこの問題および動作に気づいています。

この問題をトラッキングする複数のスレッドがあります:

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

この資料は詳細が利用可能になると同時にまたは Microsoft がこの問題のためのパーマネント修

正をアナウンスすればアップデートされます。