Сопоставления пользователя к IP Больше Не Появляются в Cisco CDA после марта 2017 Microsoft Update

Содержание

Введение

Этот документ описывает , как преодолеть проблему обновления Защиты Microsoft марта 2017, которое ломает функциональность CDA , т.е. Пользовательские сопоставления больше не появляются в Агенте каталога контекста (CDA) SWT.

Общие сведения

Cisco CDA полагается на Идентификатор события 4768 заполняемый на всех версиях контроллеров домена Windows 2008 и 2012. Эти события указывают на успешные пользовательские события входа в систему. Если события входа в систему успеха не будут контролироваться в политике локального уровня безопасности или если эти идентификаторы события не будут заполнены ни по какой другой причине тогда, то запросы WMI от CDA для этих событий не возвратят данных. В результате пользовательские сопоставления не будут созданы в CDA, и поэтому пользовательские данные сопоставления не будут передаваться от CDA до Устройства адаптивной защиты (ASA). В случаях, где клиенты усиливают пользователя или основанную на группе политику от AD в Облачной веб-безопасности (CWS), сведения о пользователе не появляются в выходных данных **whoami.scansafe.net**.

> **Примечание:** Это не влияет на Клиента User Agent (UA) Огневой мощи, так как он усиливает идентификатор события 4624 для создания пользовательских сопоставлений, и на тот тип события не влияет это обновление системы защиты.

Проблема: Сопоставления пользователя к IP Больше Не Появляются в Cisco CDA после марта 2017 Microsoft Update

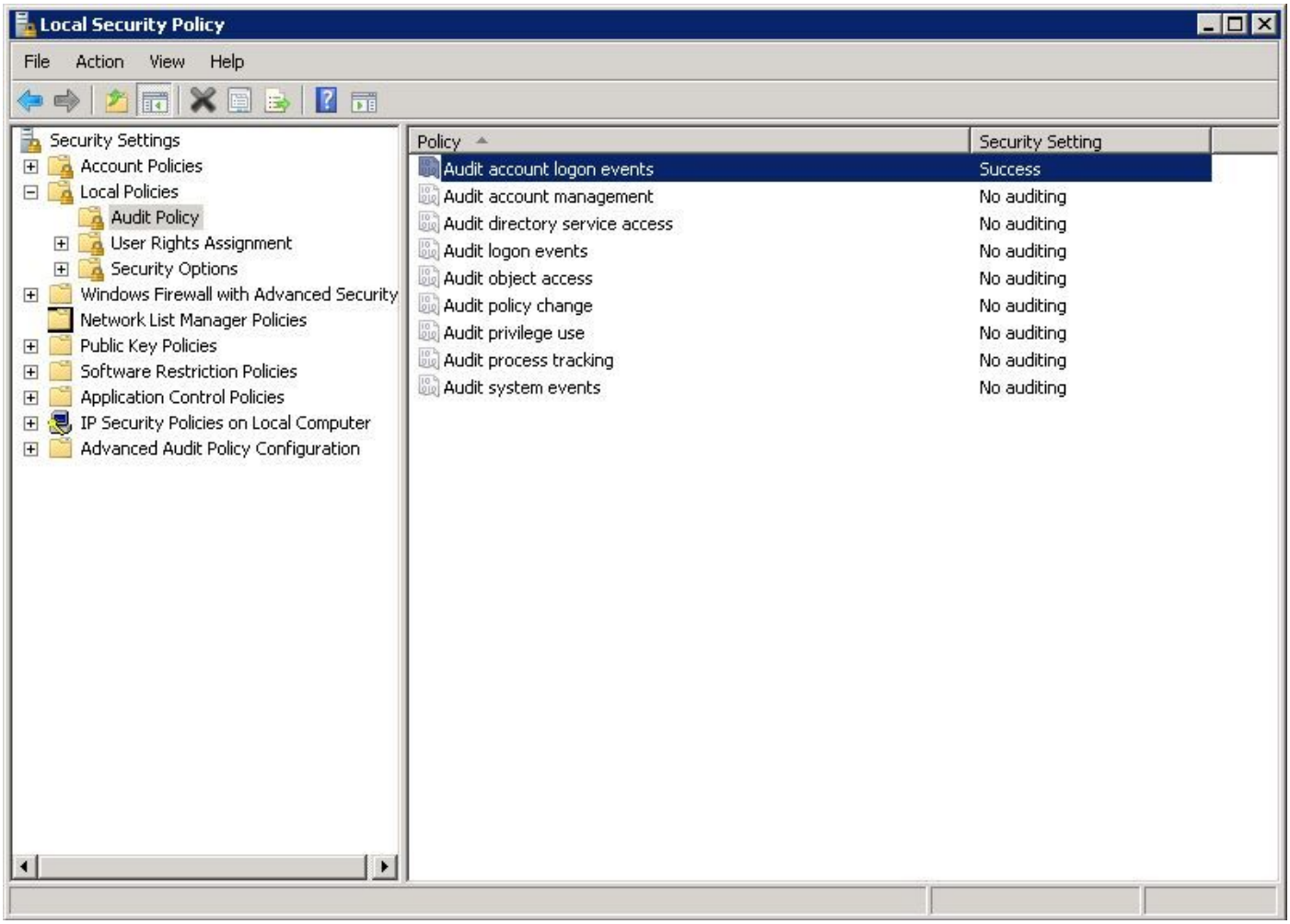
Недавнее обновление Защиты Microsoft вызвало проблемы в нескольких пользовательских окружениях в чем, их контроллеры домена прекращают регистрировать эти 4768 идентификаторов события. Незаконные КБИТЫ упомянуты ниже:

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

Чтобы подтвердить, что эта проблема не с конфигурацией журнала на Контроллере домена, удостоверьтесь, что надлежащая контрольная регистрация включена в Политике Локального уровня безопасности. Элементы, выделенные полужирным шрифтом в этих выходных данных ниже неизбежности включены для надлежащей регистрации 4768 идентификаторов события. Это должно быть выполнено от командной строки каждого DC, который не является событиями регистрации:

```
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>
```

Если вы видите, что надлежащая контрольная регистрация не настроена, перейдите к**> Security Политики Локального уровня безопасности Параметры настройки> Локальная политика> Политика аудита** и гарантируйте, что **Контрольные события входа в систему учетной записи** установлены в **Успех**, как показано в образе:



Потенциальные обходные пути

(Обновленный 31.03.2017)

Как текущее решение проблемы, некоторые пользователи были в состоянии деинсталлировать вышеупомянутые КБИТЫ, и эти 4768 идентификаторов события продолжили регистрировать. Это оказалось эффективным для всех Клиентов Cisco к настоящему времени.

Microsoft также предоставила следующий обходной путь некоторым клиентам, поражающим эту проблему, как замечено в форумах поддержки. Обратите внимание на то, что это еще не было полностью протестировано или проверено в лабораториях Cisco:

> Эти четыре политики аудита, которую необходимо включить как обходной путь к дефекту, находится под Компьютером Политика аудита Configuration\Policies\Windows Settings\Security Settings\Advanced Вход в систему Configuration\Audit Policies\Account. Все четыре политики под тем заголовком должна быть включена для Успеха или неудачи:
>
> Контрольная учетная проверка
> Контрольный сервис проверки подлинности Kerberos
> Контрольные операции билета сервиса Kerberos
> Контролируйте другие события входа в систему учетной записи

При включении тех четырех политики необходимо начать видеть 4768/4769 события Success снова.

См. образ выше этого показывает **Усовершенствованную Конфигурацию Политики аудита** у основания левой панели.

Решение

С даты этой начальной публикации (3/28/2017) мы еще не знаем о Долговремменном исправлении от Microsoft. Однако они знают об этой проблеме и работают на исправление.

Существует несколько потоков, отслеживающих эту проблему:

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

Этот документ обновлен, поскольку дополнительные сведения становятся доступными или если Microsoft объявляет о Долговремменном исправлении для этой проблемы.