2017년 3월 Microsoft Update 이후 Cisco CDA에 User-to-IP 매핑이 더 이상 표시되지 않음

목차

소개

이 문서에서는 CDA 기능을 중단하는 2017년 3월 Microsoft 보안 업데이트 문제를 해결하는 방법에 대해 설명합니다.사용자 매핑은 더 이상 SWT CDA(Context Directory Agent)에 나타나지 않습니다.

배경 정보

Cisco CDA는 Windows 2008 및 2012 도메인 컨트롤러의 모든 버전에서 채워지는 이벤트 ID 4768에 의존합니다.이러한 이벤트는 성공한 사용자 로그온 이벤트를 나타냅니다. 로컬 보안 정책에서 성공 로그온 이벤트가 감사되지 않거나 다른 이유로 이러한 이벤트 ID가 채워지지 않으면 CDA에서 이러한 이벤트에 대한 WMI 쿼리가 데이터를 반환하지 않습니다.따라서 사용자 매핑이 CDA에 생성되지 않으므로 사용자 매핑 정보가 CDA에서 ASA(Adaptive Security Appliance)로 전송되지 않습니다. 고객이 CWS(Cloud Web Security)에서 AD의 사용자 또는 그룹 기반 정책을 활용하는 경우 사용자 정보는 whoami.scansafe.**net** 출력에 나타나지 않습니다.

> **참고**:이벤트 ID 4624를 활용하여 사용자 매핑을 생성하므로 Firepower UA(User Agent)에는 영향을 주지 않으며 해당 이벤트 유형은 이 보안 업데이트의 영향을 받지 않습니다.

문제/장애:2017년 3월 Microsoft Update 이후 Cisco CDA에 User-to-IP 매핑이 더 이상 표시되지 않음

최근 Microsoft 보안 업데이트로 인해 도메인 컨트롤러가 이러한 4768 이벤트 ID의 로깅을 중지하는 고객 환경에서 문제가 발생했습니다. 문제가 되는 KB는 다음과 같습니다.

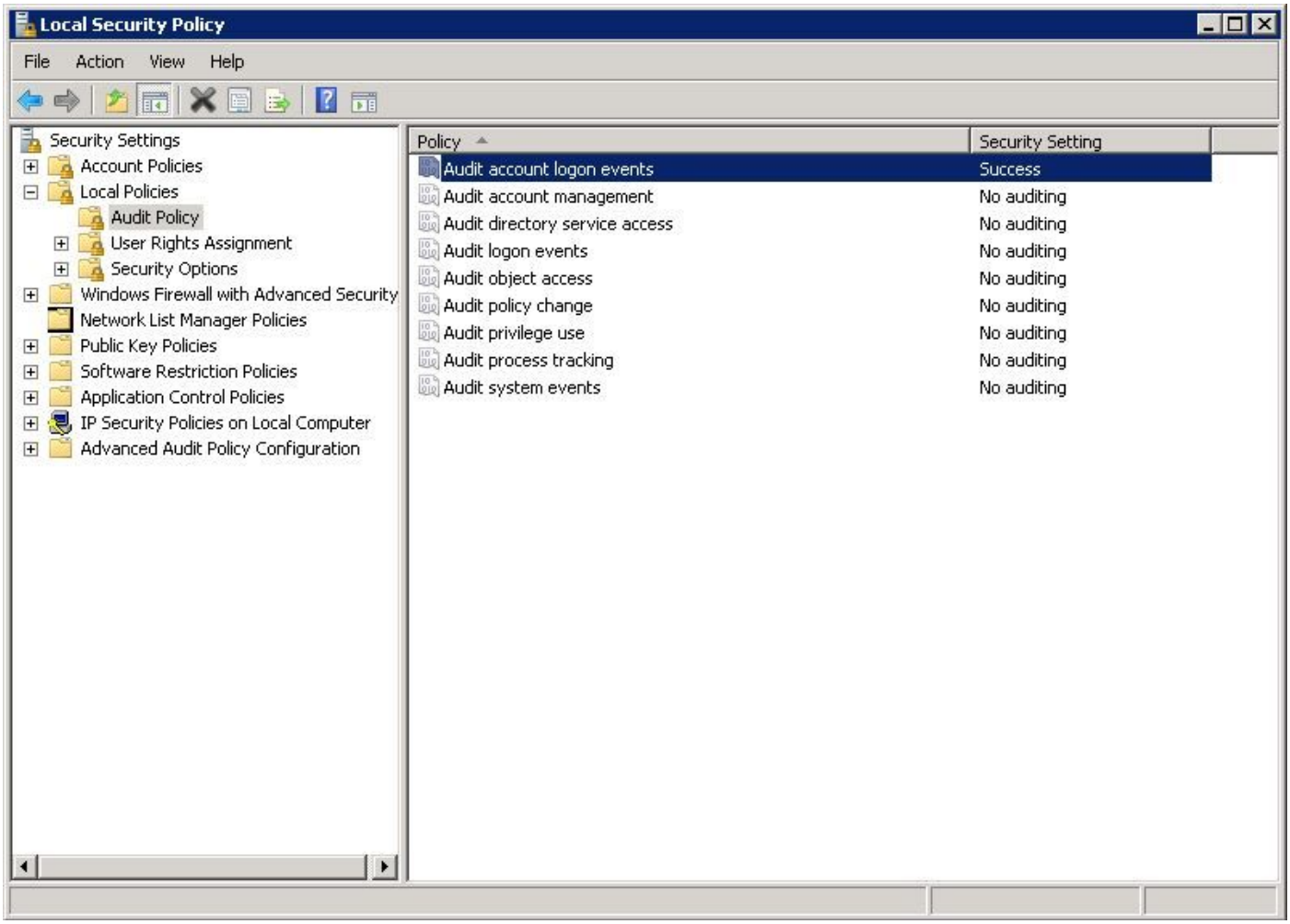
KB4012212(2008) / KB4012213(2012)
KB4012215(2008) / KB4012216(2012)

도메인 컨트롤러의 로깅 컨피그레이션에서 이 문제가 발생하지 않는지 확인하려면 로컬 보안 정책에서 적절한 감사 로깅이 활성화되어 있는지 확인하십시오. 4768 이벤트 ID의 적절한 로깅을 위해서는 아래 출력의 굵은 항목을 활성화해야 합니다.이벤트를 로깅하지 않는 각 DC의 명령 프롬프트에서 실행해야 합니다.

```
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>
```

적절한 감사 로깅이 구성되지 않은 경우 다음 이미지에 표시된 대로 **Local Security Policy(로컬 보안 정책) > Security Settings(보안 설정) > Local Policies(로컬 정책) > Audit Policy(감사 정책)로 이동하여 Audit account logon events(감사 계정 로그온 이벤트)**가 **Success(성공)**로 설정되었는지 확인합니다.



잠재적 해결 방법

(업데이트 3/31/2017)

현재 해결 방법으로, 일부 사용자는 위에서 언급한 KB를 제거하고 4768 이벤트 ID는 로깅을 다시 시작할 수 있었습니다. 지금까지 모든 Cisco 고객에게 효과가 입증된 것입니다.

또한 Microsoft는 지원 포럼에서 볼 수 있듯이 이 문제를 해결하는 일부 고객에게 다음과 같은 해결책을 제공했습니다. Cisco Labs에서는 아직 완전히 테스트되거나 검증되지 않았습니다.

> 버그에 대한 해결 방법으로 활성화해야 하는 4가지 감사 정책은 Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon에 있습니다.해당 제목 아래의 네 가지 정책 모두 성공 및 실패에 대해 활성화되어야 합니다.
>
> 자격 증명 검증 감사
> Kerberos 인증 서비스 감사
> Kerberos 서비스 티켓 작업 감사
> 기타 계정 로그온 이벤트 감사
>
> 이러한 4가지 정책을 활성화하면 4768/4769 성공 이벤트를 다시 볼 수 있습니다.

왼쪽 창 하단에 **Advanced Audit Policy Configuration(고급 감사 정책 컨피그레이션)**을 보여 주는 위

의 이미지를 참조하십시오.

솔루션

이 초기 발행일(3/28/2017)부터 Microsoft의 영구 수정 사항을 아직 알지 못합니다.그러나 이 문제를 인식하고 문제를 해결하기 위해 노력하고 있습니다.

이 문제를 추적하는 여러 스레드가 있습니다.

Redit:

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

이 문서는 더 많은 정보를 사용할 수 있게 되거나 Microsoft에서 이 문제에 대한 영구적인 수정 사항을 발표할 경우 업데이트됩니다.