# I mapping utente-IP non vengono più visualizzati in Cisco CDA dopo il mese di marzo 2017 in Microsoft Update

## Sommario



## Introduzione

Questo documento descrive come superare il problema di marzo 2017 Microsoft Security Update, che rompe la funzionalità CDA, cioè. I mapping utente non vengono più visualizzati in CDA (Context Directory Agent) SWT.

## Premesse

Cisco CDA si basa sull'ID evento 4768 popolato su tutte le versioni dei controller di dominio Windows 2008 e 2012. Questi eventi indicano la riuscita degli eventi di accesso dell'utente. Se gli eventi di accesso riusciti non vengono controllati nei criteri di sicurezza locali o se questi ID di evento non vengono popolati per altri motivi, le query WMI da CDA per questi eventi non restituiranno alcun dato. Di conseguenza, i mapping degli utenti non verranno creati in CDA e pertanto le informazioni di mapping degli utenti non verranno inviate da CDA ad Adaptive Security Appliance (ASA). Nei casi in cui i clienti utilizzano criteri basati su utenti o gruppi di Active Directory in Cloud Web Security (CWS), le informazioni utente non vengono visualizzate nell'output di **whoami.scansafe.net**.

> **Nota**:questo non influisce su Firepower User Agent (UA), in quanto utilizza l'ID evento 4624 per creare mapping utente e il tipo di evento non è influenzato da questo aggiornamento della sicurezza.

## Problema: I mapping utente-IP non vengono più visualizzati in Cisco CDA dopo il mese di marzo 2017 in Microsoft Update

Un recente aggiornamento della protezione di Microsoft ha causato problemi in diversi ambienti dei clienti in cui i controller di dominio non registrano più questi 4768 ID evento.  Di seguito sono elencati i KB offensivi:

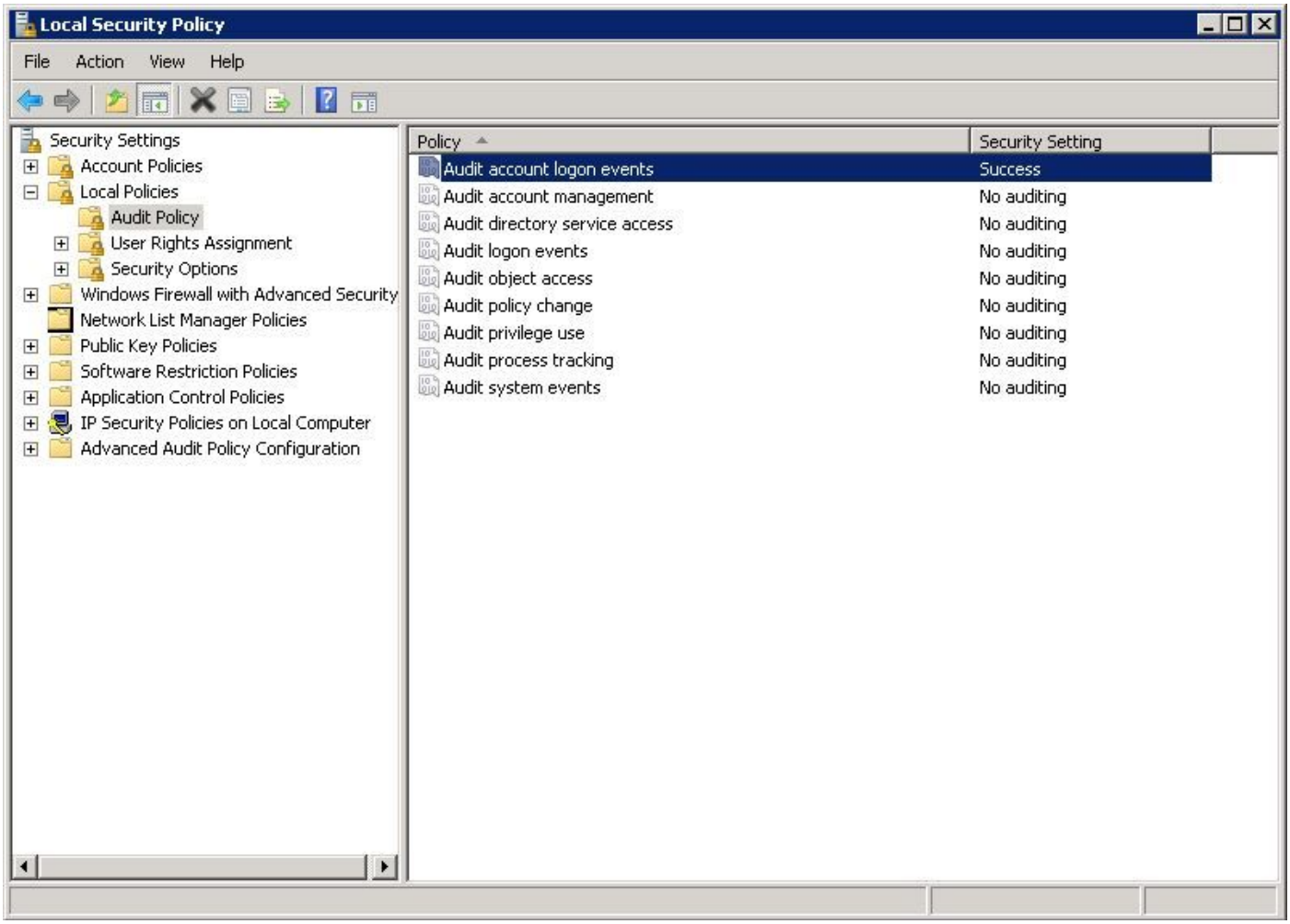
KB4012212 (2008) / KB4012213 (2012)
KB4012215 (2008) / KB4012216 (2012)

Per verificare che il problema non si verifichi con la configurazione della registrazione nel controller di dominio, verificare che la registrazione di controllo corretta sia attivata in Criteri di sicurezza locali.  Le voci in grassetto in questo output di seguito devono essere abilitate per la corretta registrazione di 4768 ID evento. Questa operazione deve essere eseguita dal prompt dei comandi di ogni controller di dominio che non registra gli eventi:

```
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>
```

Se la registrazione di controllo corretta non è configurata, passare a **Criteri di protezione locali > Impostazioni di protezione > Criteri locali > Criteri di controllo** e verificare che **Controlla eventi di accesso account** sia impostato su **Operazione riuscita**, come mostrato nell'immagine:




# Soluzioni potenziali

(Aggiornato il 31/03/2017)

Per ovviare al problema, alcuni utenti sono stati in grado di disinstallare le KB indicate in precedenza e la registrazione degli ID evento 4768 è stata ripresa. Ciò si è finora dimostrato efficace per tutti i clienti Cisco.

Microsoft ha inoltre fornito la soluzione seguente ad alcuni clienti che hanno riscontrato questo problema, come indicato nei forum di supporto.  Questa funzionalità non è stata ancora completamente testata o verificata nei laboratori Cisco:

> I quattro criteri di controllo da abilitare per risolvere il bug si trovano in Configurazione computer\Criteri\Impostazioni di Windows\Impostazioni sicurezza\Configurazione avanzata criteri di controllo\Criteri di controllo\Accesso account. Tutti e quattro i criteri di questa rubrica dovrebbero essere abilitati per il successo e il fallimento:
>
> Controlla convalida credenziali
> Controlla servizio di autenticazione Kerberos
> Controlla Operazioni ticket di servizio Kerberos
> Controlla altri eventi di accesso account
>
> Quando si attivano questi quattro criteri, è necessario ricominciare a visualizzare gli eventi di

successo 4768/4769.

Fare riferimento all'immagine precedente che mostra **Configurazione avanzata dei criteri di revisione** nella parte inferiore del riquadro sinistro.

# Soluzione

Alla data di questa pubblicazione iniziale (28/3/2017), non è ancora disponibile una correzione permanente da parte di Microsoft. Tuttavia, sono consapevoli del problema e stanno lavorando a una soluzione.

Sono disponibili diversi thread per tenere traccia del problema:

Modifica:

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

Questo documento viene aggiornato non appena si rendono disponibili ulteriori informazioni o se Microsoft annuncia una soluzione definitiva per il problema.