User-to-IP Mappings No Longer Appear in Cisco CDA after March 2017 Microsoft Update

Contents

Introduction

This document describes how to overcome the issue of March 2017 Microsoft security update, which breaks CDA functionality i.e. User mappings no longer appear in SWT Context Directory Agent (CDA).

Background Information

Cisco CDA relies on Event ID 4768 being populated on all versions of Windows 2008 and 2012 domain controllers. These events indicate successful user logon events. If success logon events are not being audited in the local security policy or if these event IDs are not populated for any other reason then the WMI queries from CDA for these events will return no data. As a result, user mappings will not be created in CDA and therefore user mapping information will not be sent from CDA to the Adaptive Security Appliance (ASA). In cases where customers are leveraging user or group-based policies from AD in Cloud Web Security (CWS), the user information does not appear in the **whoami.scansafe.net** output.

> **Note**:This does not affect Firepower User Agent (UA) since it leverages event ID 4624 to create user mappings and that type of event is not impacted by this security update.

Problem: User-to-IP Mappings No Longer Appear in Cisco CDA after March 2017 Microsoft Update

A recent Microsoft security update has caused issues in several customer environments wherein their domain controllers stop logging these 4768 event IDs. The offending KBs are listed below:

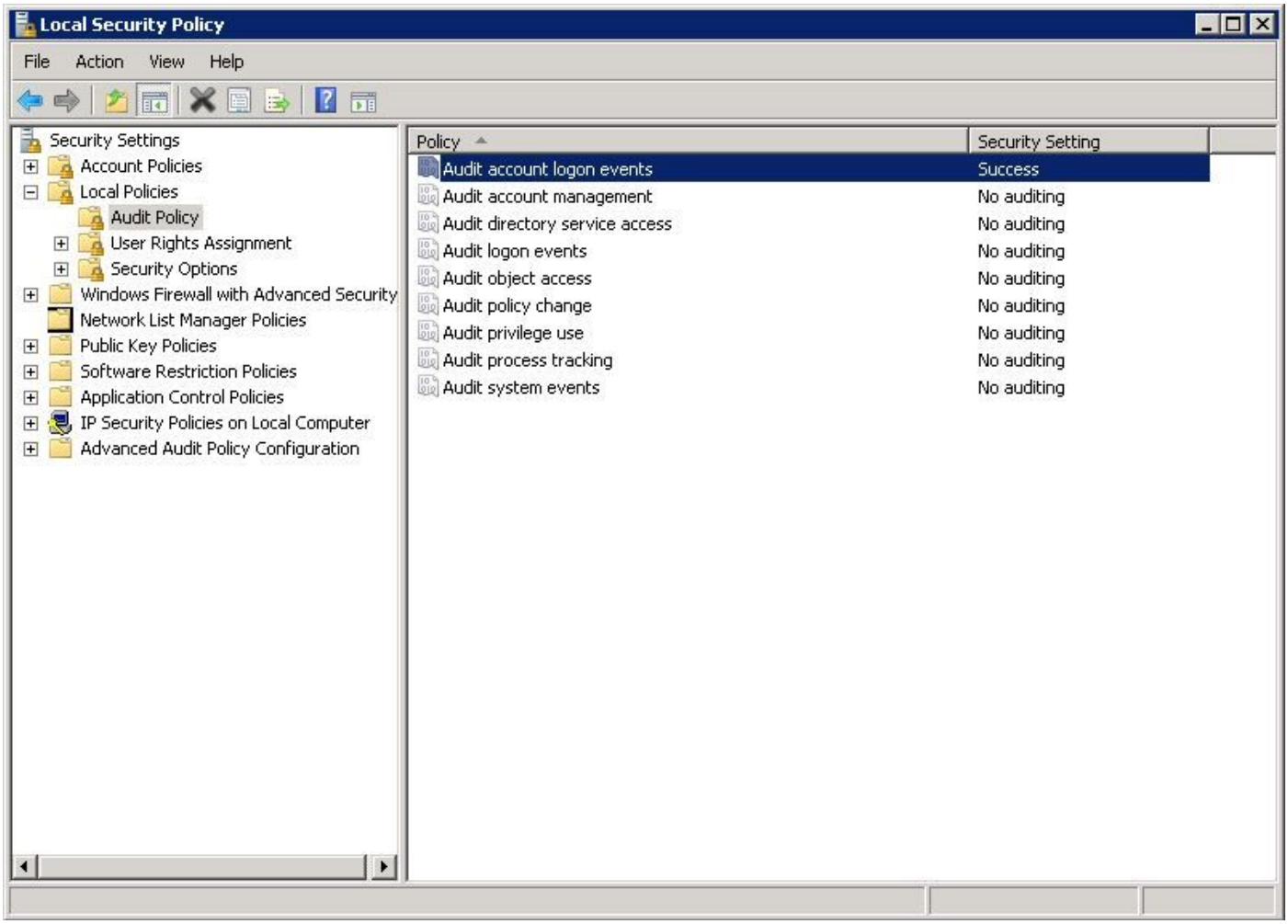
KB4012212 (2008) / KB4012213 (2012)
KB4012215 (2008) / KB4012216 (2012)

To confirm that this issue is not with the logging configuration on the Domain Controller, make sure that the proper audit logging is enabled in the Local Security Policy. The bold items in this output below mustbe enabled for proper logging of 4768 event IDs. This should be run from the

command prompt of each DC that is not logging events:

```
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>
```

If you see that the proper audit logging is not configured, navigate to **Local Security Policy > Security Settings > Local Policies > Audit Policy** and ensure that **Audit account logon events** is set to **Success**, as shown in the image:



Potential Workarounds

(Updated 3/31/2017)

As a current workaround, some users have been able to uninstall the above mentioned KBs and

the 4768 event IDs resumed logging. This has proven effective for all Cisco customers thus far.

Microsoft has also provided the following workaround to some customers hitting this issue as seen in support forums. Note that this has not yet been fully tested or verified in Cisco labs:

> The four audit policies you need to enable as a workaround to the bug are under Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon. All four policies under that heading should be enabled for Success and Failure:
>
> Audit Credential Validation
> Audit Kerberos Authentication Service
> Audit Kerberos Service Ticket Operations
> Audit Other Account Logon Events
>
> When you enable those four policies, you should start to see the 4768/4769 Success events again.

Refer to the image above that shows **Advanced Audit Policy Configuration** at the bottom of the left pane.

Solution

As of the date of this initial publication (3/28/2017), we do not yet know of a permanent fix from Microsoft. However, they are aware of this issue and working on a fix.

There are several threads tracking this issue:

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

This document is updated as more information becomes available or if Microsoft announces a permanent fix for this issue.