DOCUMENT NUMBER: MTN-0053-19-NA
APC: 877
ISSUE DATE: 04-2019
EXPIRATION DATE: 30-04-2020
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: McAfee scan floods Windows security event log and SysLog server with messages, causes network congestion, and sluggish PC performance.

TECHNOLOGY: Windows Group Policy Object (GPO)

SYMPTOMS:
McAfee scan floods Windows security event log with event IDs such as 4656, 4658, 4663, and 4674 from Source=Microsoft Windows security auditing, which are generated by the following McAfee processes:

- C:\Program Files (x86)\McAfee\VirusScan Enterprise\x64\scan64.exe
- C:\Program Files\Common Files\McAfee\SystemCore\mcshield.exe

These messages in turn cause heavy network congestion, and the PC becomes sluggish in performance.

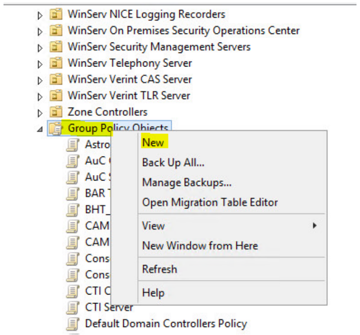
MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:
All PCs running Windows 10 operating systems / ASTRO 7.17.3 and 7.18 releases

SEVERITY RECOMMENDATION:
Medium / Operational - Schedule to implement

ROOT CAUSE / DEFINITIVE TEST:
Randomly, McAfee scan floods security event log. This is connected to default setting for GPO's Security Settings: "Audit: Audit the use of Backup and Restore privilege". This setting has different default value depending on the Windows 10 build.

WORKAROUNDS AND CORRECTIVE ACTIONS:
Follow these steps to create and apply a custom GPO that disables the security policy, "Audit: Audit the use of Backup and Restore privilege".

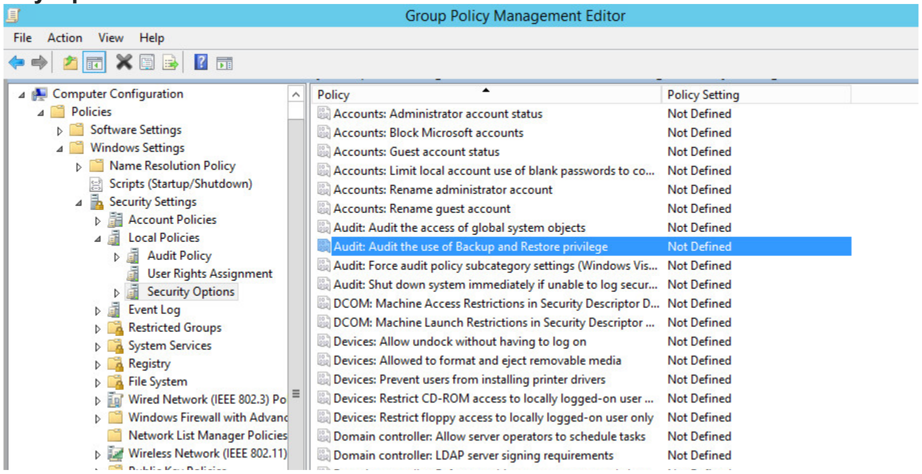
1. Login to System Level DC (UCS-DC01) as Domain Administrator.
2. Open **Group Policy Management Console**.
3. Expand **Forest** and **Domains** tree and find Active Directory **domain name** (e.g. ucs.astro).
4. Expand **this domain** and find **Group Policy Object OU**.
5. Right-click on **Group Policy Object** and choose "**New".**


WinServ NICE Logging Recorders
WinServ On Premises Security Operations Center
WinServ Security Management Servers
WinServ Telephony Server
WinServ Verint CAS Server
WinServ Verint TLR Server
Zone Controllers
Group Policy Objects
Astro
AuC
AuC
BAR
BHT_
CAM
CAM
Cons
Cons
CTI C
CTI Server
Default Domain Controllers Policy
New
Back Up All...
Manage Backups...
Open Migration Table Editor
View
New Window from Here
Refresh
Help

6. Provide the following name for new GPO: "**Win10 Custom GPO**".
7. Right-click on new GPO link and choose "**Edit**" to open GPO Editor.

ANY USE NOT APPROVED BY MOTOROLA SOLUTIONS IS PROHIBITED. This Motorola Technical Notification (MTN) is issued pursuant to Motorola's ongoing review of the quality, effectiveness, and performance of its products. The information provided in this bulletin is intended for use by trained, professional technicians only, who have the expertise to perform the service described in the MTN. Motorola disclaims any and all liability for product quality or performance if the recommendations in this MTN are not implemented, or not implemented in compliance with the instructions provided here. Implementation of these recommendations may be necessary for the product to remain compliant with applicable laws or regulations. Please be advised, that failure to implement these recommendations in the manner instructed may also invalidate applicable warranties, or otherwise impact any potential contractual rights or obligations. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

8. Navigate to **Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options.**

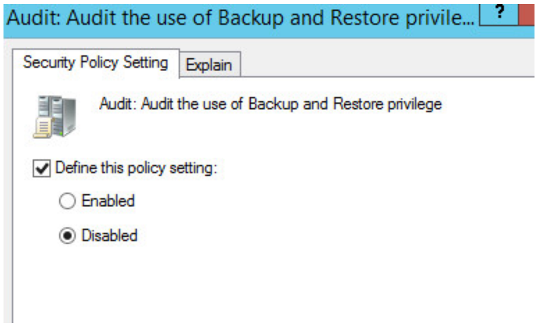


Group Policy Management Editor

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: LDAP server signing requirements	Not Defined

9. Double-click “**Audit: Audit the use of Backup and Restore privilege**” policy.

10. Mark **“Define this policy setting”** and select “**Disabled**”.



Audit: Audit the use of Backup and Restore privile...

Audit: Audit the use of Backup and Restore privilege

☑ Define this policy setting:

○ Enabled

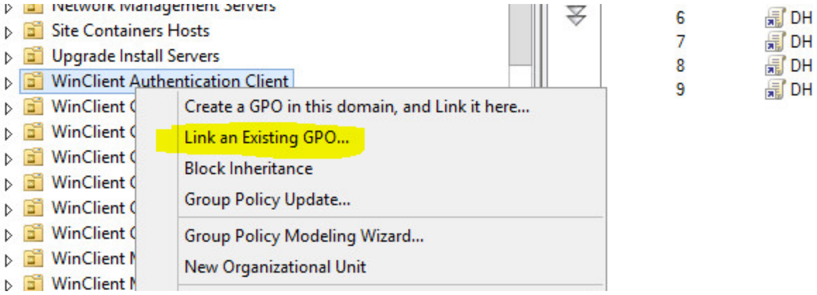
● Disabled

11. Choose **OK**.

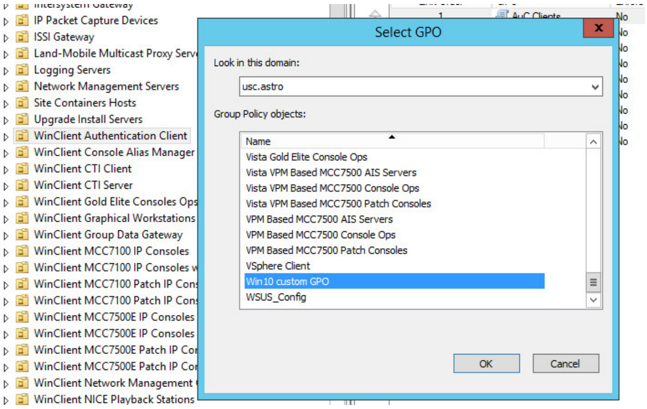
12. Close **Group Policy Management Editor**.

13. From the left pane, find the first OU whose name starts with “WinClient” (e.g. WinClient Authentication Client”.

14. Right-click on them and chose “Link an Existing GPO…”.



15. Find “**Win10 Custom GPO”** GPO, select it and click OK.



Select GPO

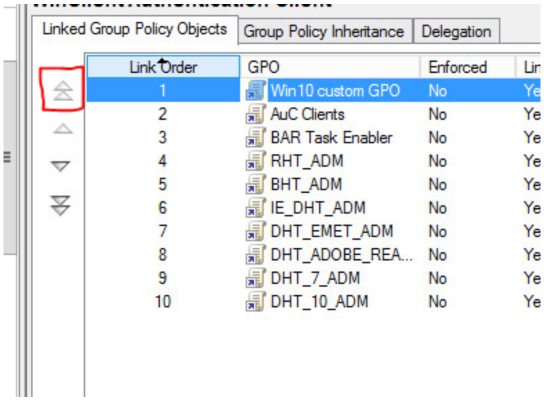
Look in this domain: usc.astro

Group Policy objects:

Name
Vista Gold Elite Console Ops
Vista VPM Based MCC7500 AIS Servers
Vista VPM Based MCC7500 Console Ops
Vista VPM Based MCC7500 Patch Consoles
VPM Based MCC7500 AIS Servers
VPM Based MCC7500 Console Ops
VPM Based MCC7500 Patch Consoles
VSphere Client
Win10 custom GPO
WSUS_Config

IP Packet Capture Devices
ISSI Gateway
Land-Mobile Multicast Proxy Serv
Logging Servers
Network Management Servers
Site Containers Hosts
Upgrade Install Servers
WinClient Authentication Client
WinClient Console Alias Manager
WinClient CTI Client
WinClient CTI Server
WinClient Gold Elite Consoles Ops
WinClient Graphical Workstations
WinClient Group Data Gateway
WinClient MCC7100 IP Consoles
WinClient MCC7100 IP Consoles w
WinClient MCC7100 Patch IP Con
WinClient MCC7100 Patch IP Con
WinClient MCC7500E IP Consoles
WinClient MCC7500E IP Consoles
WinClient MCC7500E Patch IP Co
WinClient MCC7500E Patch IP Co
WinClient Network Management
WinClient NICE Playback Stations
AuC Clients
No
OK
Cancel

16. Move this new policy to the first position, you can use the double arrow on the left side.



Link Order	GPO	Enforced	Lin
1	Win10 custom GPO	No	Ye
2	AuC Clients	No	Ye
3	BAR Task Enabler	No	Ye
4	RHT_ADM	No	Ye
5	BHT_ADM	No	Ye
6	IE_DHT_ADM	No	Ye
7	DHT_EMET_ADM	No	Ye
8	DHT_ADOBE_REA...	No	Ye
9	DHT_7_ADM	No	Ye
10	DHT_10_ADM	No	Ye

17. Repeat steps 14 to 17 for all "**WinClient…**" OUs.
18. Close **Group Policy Management Console**.

RESOLUTIONS AND REPAIR PROCEDURES:
Follow Workaround

PARTS REQUIRED (HARDWARE/SOFTWARE):
N/A

ADDITIONAL INFORMATION:
N/A

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:
N/A

WHEN TO APPLY RESOLUTION:
After reboot __
After (re)installation __
After upgrade __
After power cycle __
After database restoration __
After failure __
On FRU replacement __
During maintenance __
Immediately __
As instructed __
Information only x

LABOR ALLOWANCE:
This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

For assistance with this bulletin please contact your MSI Technical support centre
https://www.motorolasolutions.com/en_us/support.html