

RE: Auditing Workstation logons from DC

Source:

<http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.sbs/2006-01/msg04589.html>

- *From:* v-stezhu@xxxxxxxxxxxxxxxxxxxxxx (Steven Zhu [MSFT])
 - *Date:* Thu, 26 Jan 2006 09:26:19 GMT
-

Hi,

Thanks for posting here.

>From your post, my understanding of this issue is that you want to see workstation interactive logins in the Event Log in Windows Server 2003 DC. You have already configured Domain Security Settings for Audit account logon to Success and Audit logon events to Success. You have also configured Domain Controller Setting for Audit account logon to Success and Failure and Audit Logon to Success and Failure. But you still didn't see the relevant events. If I am off base, please feel free to let me know.

I know you have enabled Audit Logon Event and Audit account Logon Event in the both Default Domain Controllers Policy and Default Domain Security Policy. But to make sure the configuration you have made is correct, please refer to the following steps:

Configure Default Domain Controllers Policy:

1. Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
2. Right-click Domain Controllers Organizational Unit, and then click Properties.
3. Click the Group Policy tab, select Default Domain Controllers Policy, and then click Edit.
4. Under Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Audit Policy.
5. In the right pane, double-click Audit Account Logon Event and Audit Logon Event.
6. Click to select the Define the policy settings check box, click to select the Success check box, click to select the Failure check box, and then click OK.
7. Quit the Group Policy Object Editor snap-in, and then click Close.

Configure Default Domain Policy:

1. Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
2. Right-click Domain, and then click Properties.

RE: Auditing Workstation logons from DC

3. Click the Group Policy tab, select Default Domain Policy, and then click Edit.
4. Under Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Audit Policy.
5. In the right pane, double-click Audit Account Logon Event and Audit Logon Event.
6. Click to select the Define the policy settings check box, click to select the Success check box, click to select the Failure check box, and then click OK.
7. Quit the Group Policy Object Editor snap-in, and then click Close.

Then, you should be able to see security logs in the security Event Log in the Event Viewer as an administrator or as a member of the Administrators. After you correctly configured auditing in both Default Domain Controllers Policy and Default Domain Security Policy, but the related events still don't appear in Security Event Log in the Event Viewer. This behavior can occur for any of the following reasons:

1. A domain, or an organizational unit policy setting overrides the audit policy that you configured. To troubleshoot this issue, follow these steps:
 - A): Click Start, and then click Run.
 - B): In the Open box, type gpedit.msc, and then click OK
 - C): Under Computer Configuration, expand Windows Settings, expand Security Settings, expand Local Policies, and then click Audit Policy.
 - D): In the right pane, view the item in the Security Setting column of the policy that you want to use.If the security setting of the policy is No auditing, a higher-level GPO may be overriding the audit policy setting that you configured. To confirm this behavior, view the higher-level GPO items that are linked to either the organizational unit or to the domain for possible conflicts.
 - E): Click to select the Define this policy settings check box, click to select the Success check box, click to select the Failure check box, and then click OK.
 - F): Quit the Group Policy Object Editor snap-in.

2. A GPO that overrides the audit policy setting has a higher priority. To troubleshoot this issue, follow these steps:
 - A): Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
 - B): In the console tree, right-click your domain, and then click Properties.
 - C): Click the Group Policy tab. View the Group Policy Objects Links list. Items that are higher in the list override other lower-level items.
 - D): If the GPO that contains your audit policy setting is listed below a higher-priority GPO item that turns off auditing, do the following steps: Click the GPO that contains the audit policy setting that you want to use, and then click Up to move it above the higher-priority item in the list.
 - E): When you are finished, click OK, and then click Exit on the File menu.

3. The domain, or the organizational unit policy setting that contains the audit policy setting has not replicated to other computers. To resolve this issue, use the gpupdate.exe command-line utility to force Group Policy to

be refreshed.

4. The security log is limited in size, so carefully select the events to be audited and consider the amount of disk space you are willing to devote to the security log.

Please let me know the results above so that I can provide further assistance on this problem. I am looking forward to your reply.

Have a nice day.

Best Regards,

Steven Zhu
MCSE
Microsoft Online Partner Support

=====
Business–Critical Phone Support (BCPS) provides you with technical phone support at no charge during critical LAN outages or "business down" situations. This benefit is available 24 hours a day, 7 days a week to all Microsoft technology partners in the United States and Canada.

This and other support options are available here:

BCPS:

<https://partner.microsoft.com/US/technicalsupport/supportoverview/40010469>

Others: <https://partner.microsoft.com/US/technicalsupport/supportoverview/>

If you are outside the United States, please visit our International Support page: <http://support.microsoft.com/common/international.aspx>.

=====
This posting is provided "AS IS" with no warranties, and confers no rights.

• **References:**

◆ **[Auditing Workstation logons from DC](#)**

◇ From: harlanandrew28

• Prev by Date: **[Re: Exchange NDR Reports](#)**

• Next by Date: **[DNS / Cache problem](#)**

• Previous by thread: **[Auditing Workstation logons from DC](#)**

• Next by thread: **[Re: remote using and connecting to exchange](#)**

• Index(es):

◆ **[Date](#)**

◆ **[Thread](#)**