

Director and Windows Server 2008 (and 2003)

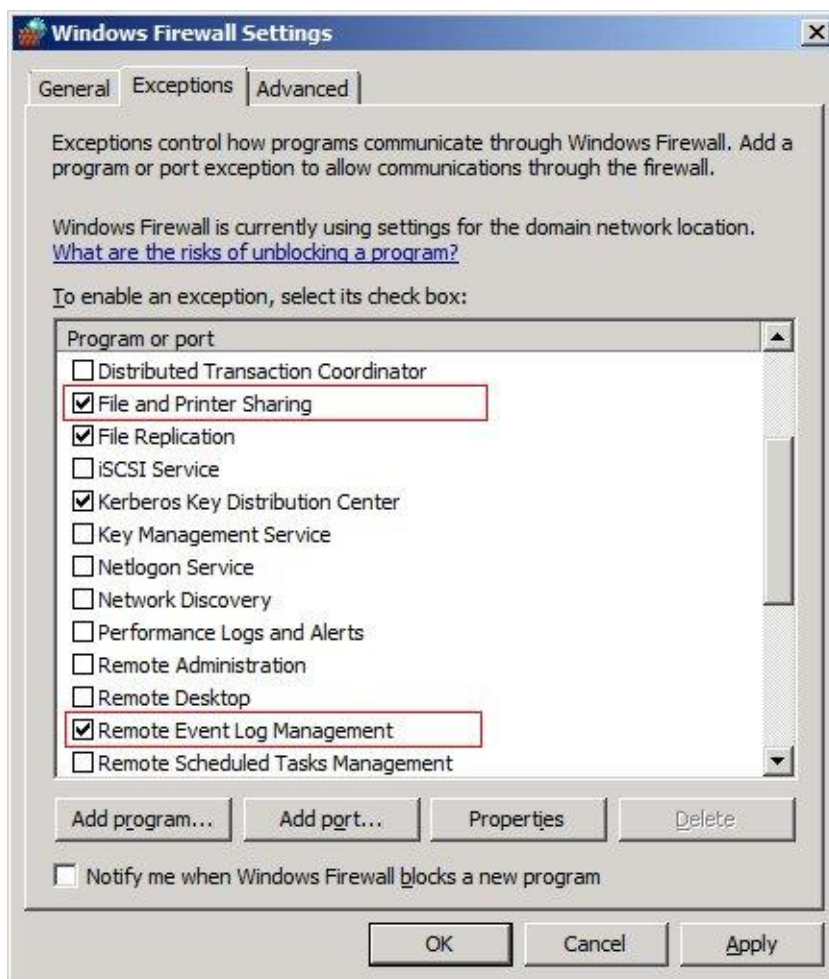
Windows Server 2008 as Domain Controller comes with several changes in the event logging and security area out-of-the-box. This makes it necessary to check for some requirements if you want to operate ChangeTracer in the same smooth way known from Windows Server 2000 and 2003 networks.

Windows Firewall Settings

The ChangeTracer Monitor service needs to have access to the Event Log on all Domain Controller servers in the domain.

If the Windows Firewall is enabled on a Domain Controller the following Exceptions have to be enabled:

- Remote Event Log Management
- File and Printer Sharing



Domain Level Auditing Settings

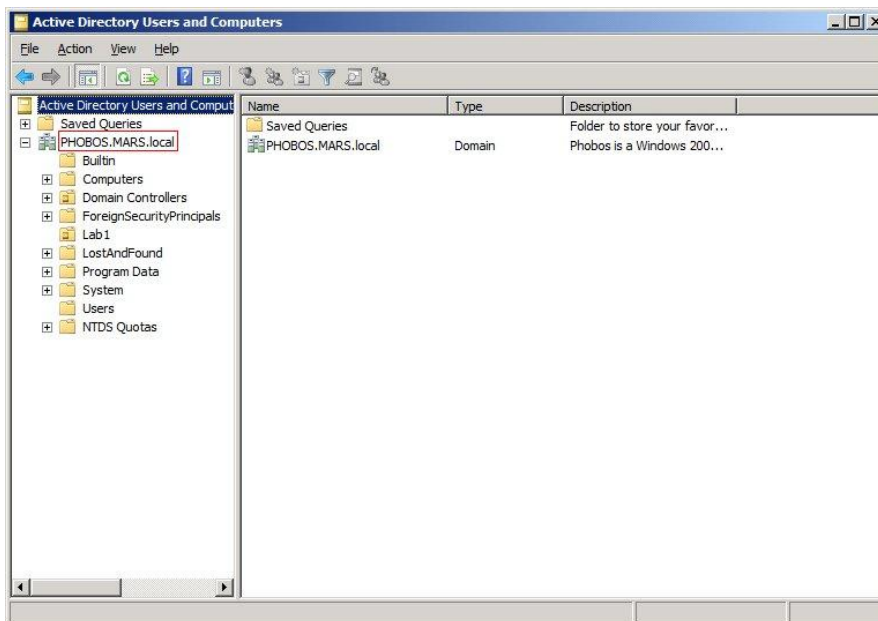
These settings are important for ChangeTracer to be able to retrieve the „WHO made a change“ information from the Windows Event Log.

Please read the following TechNet article:

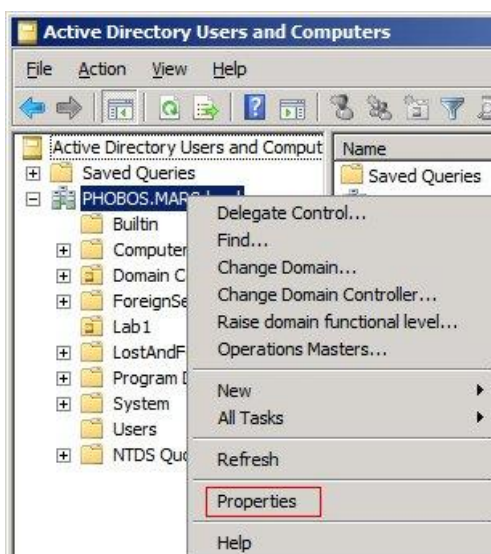
[http://technet.microsoft.com/en-us/library/cc731607\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx)

Open the *Active Directory Users and Computers* management tool and select the domain for which you want to change auditing settings.

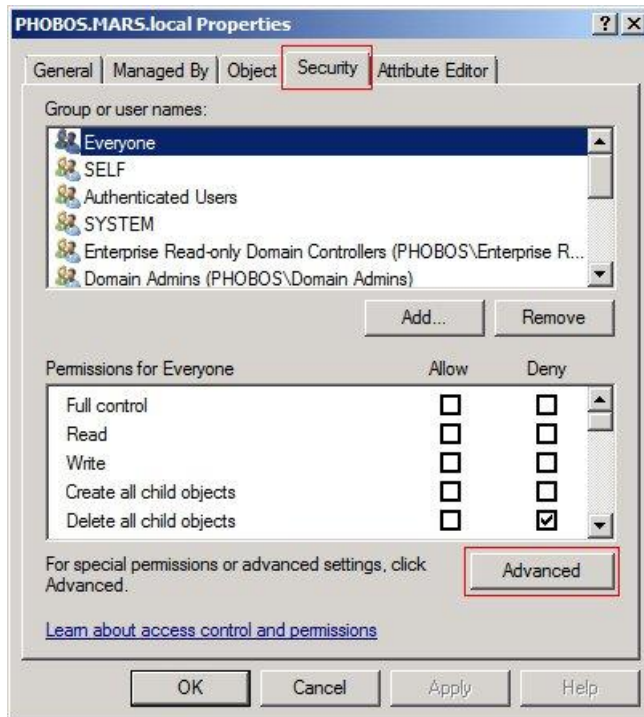
(in the example screenshots the domain is named: PHOBOS.MARS.local)



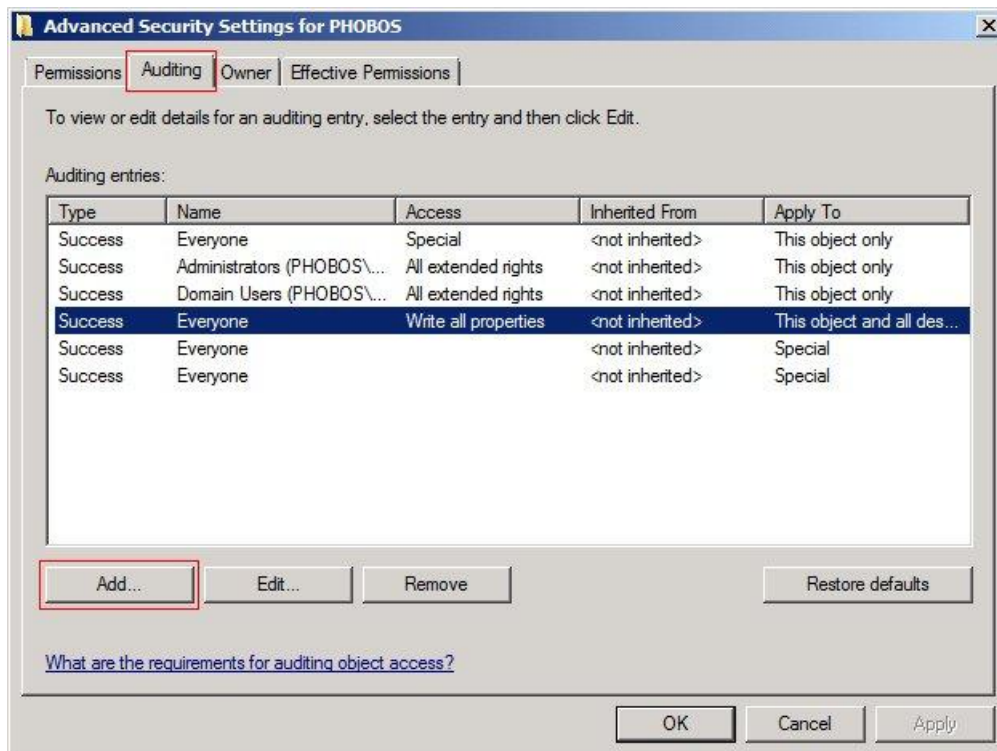
Push the right mouse button in the selected domain to open a popup-menu. Select *Properties* in the menu. A dialog <domain name> *Properties* opens.



Select the *Security* tab in the *Properties* dialog and push the *Advanced* button.
A dialog *Advanced Security Settings for <server>* opens.



Select the *Auditing* tab in the *Advanced Security Settings for <server>* dialog.
If there is no line similar to the marked one in the following screenshot push the *Add ...* button.
A dialog *Select User, Computer, or Group* opens.
(if you push *Edit ...* the *Select User, Computer, or Group* dialog does NOT appear)



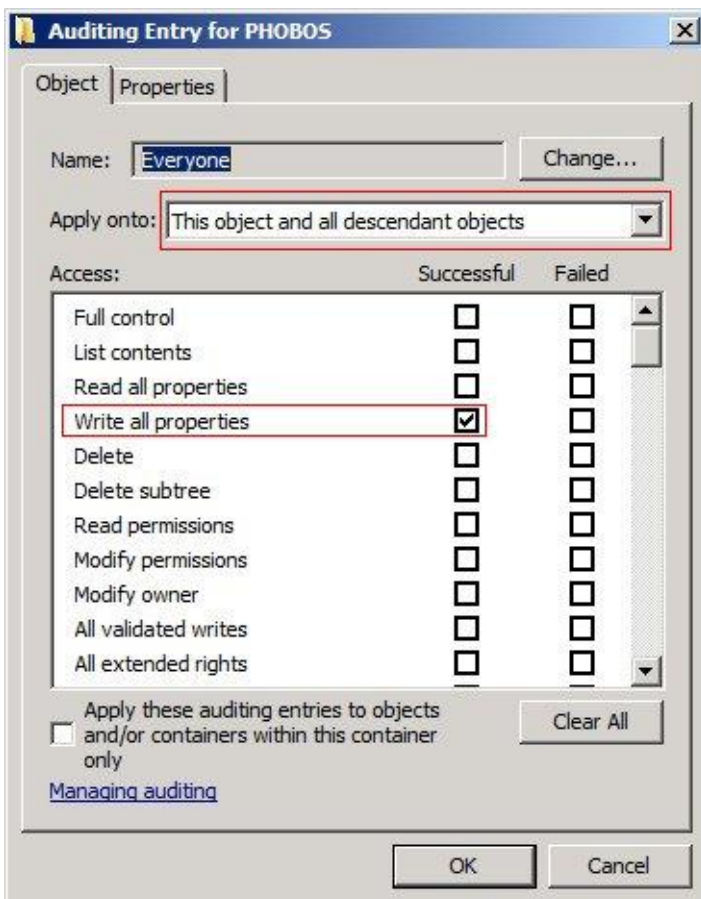
Enter *everyone* in the *Enter the object name ...* field and push *Check Names*. Push *OK* and the dialog *Auditing Entry for <server>* opens.



In the *Auditing Entry for <server>* dialog check that *Apply onto* contains *This object and all descendant objects* (or similar settings that comply with your auditing needs).

At least select and enable *Successful* auditing for *Write all properties* access.

Push *OK* and the SACL for domain auditing will be set for the domain.

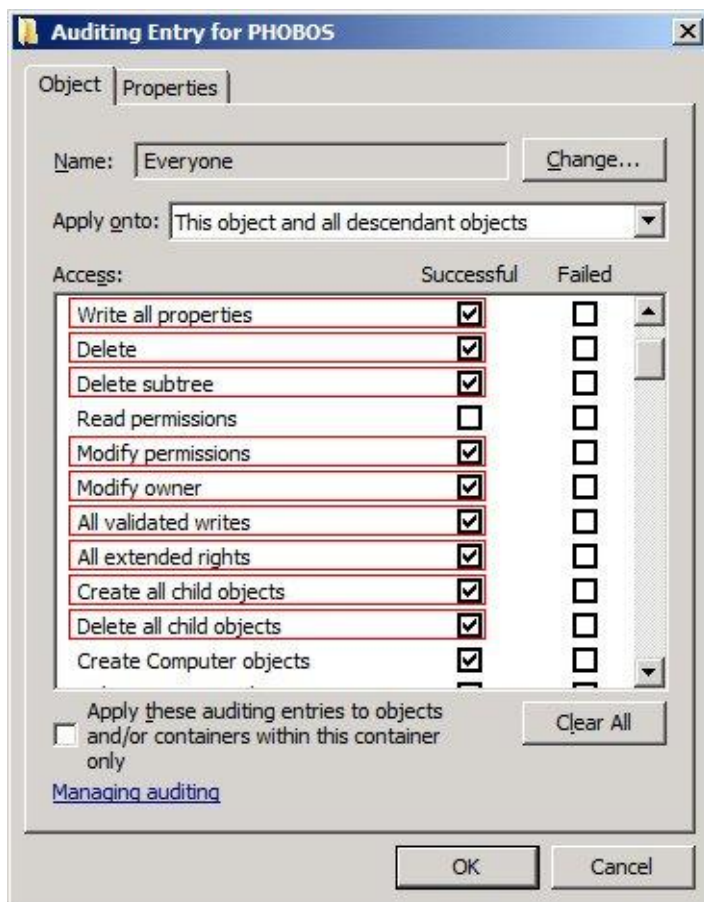


IMPORTANT :

If you want to retrieve the WHO for all changes made to all kind of objects and/or attributes in your AD domain you have to enable success auditing as follows.

Select and enable *Successful* auditing for the following access types:

- *Write all properties*
- *Delete*
- *Delete subtree*
- *Modify permissions*
- *Modify owner*
- *All validated writes*
- *All extended rights* (this also enables all access types beginning with *Add GUID*)
- *Create all child objects* (this also enables all subsequent *Create ... objects* access types)
- *Delete all child objects* (this also enables all subsequent *Delete ... objects* access types)



Of course auditing can be set as detailed as an administrator wishes to.

For example, there may be environments where auditing for some *Create ... objects* and some *Delete ... objects* access types is not needed, so simply enable *Create all child objects* and *Delete all child objects* and afterwards remove the mark from all the *Create ... objects* and *Delete ... objects* access types which are not needed.

PLEASE NOTE:

ChangeTracer does catch all changes to all objects (if no global monitoring filter is set) regardless of auditing settings which only affect the resolution of the WHO information.

Audit Policy Settings

Check that audit policy is correctly set. Otherwise no directory change events are generated and ChangeTracer is not able to extract the WHO information of a change to a directory object.

In Windows Server 2000 and 2003 server networks the audit policy was usually set by group policy. Windows Server 2008 has the same functionality but also delivers a new more granular way to setup audit policy.

Again see this very recommended TechNet article:

[http://technet.microsoft.com/en-us/library/cc731607\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx)

Use the built-in auditpol tool to find out the audit policy settings on each domain controller.

Enter the following command in a command prompt:

```
C:\>auditpol /get /category:"DS Access"
```

Look for the „*Directory Service Access*“ subcategory and check if it set to „*Success*“. **THIS IS A MUST !**

Also very recommended is to have ALL „*Account Management*“ subcategories set to at least „*Success*“.