

Re: ADAM object auditing

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-10/msg02063

- *From:* richwray <richwray@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 26 Oct 2006 12:00:02 -0700
-

Got it – thank you very much!!

Cheers!

"Lee Flight" wrote:

Hi

the Account Management audit in AD picks up a set of useful stuff but AFAIK it is mainly handled through the SAM logic in AD. Enabling the audit will not help for ADAM, I guess this stems from ADAM schema not having a default user class and a less rich concept of group and ADAM having it's own (pseudo) SAM logic.

Assuming that you have a user class in your schema then as a test you could try adding two ACEs to the SACL at the partition head or suitable child node:

Trustee: Everyone
Access Mask: Write Property, Create Child, Delete
ACE Flags: Inherit (checked), Success, Failure
Object type: group – class

and the same again but with

Object type: user – class

In the security policy of the server that has the ADAM instance you must enable
Audit directory service access, just as you would for Audit account management
etc.,

Lee Flight

Re: ADAM object auditing

"richwray" <richwray@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:3D476804-21FC-4D4C-B07B-9C747BBF13D9@xxxxxxxxxxxxxxxxxxxx

Thanks, I think that answers my question, however, I need to get the same type of output I get from enabling Account Management in AD (all creates, modifies and deletes on user/group objects). So, it's apparent this is not like AD in that I cannot just check an audit account management success box and have it work. Is there an "everyone" group or counterpart in ADAM that I could set auditing for at the top of the tree in order to catch similar output?

Thanks!

"Lee Flight" wrote:

Hi

audit is possible in ADAM SP1 but it's fairly coarse-grained. The tool to use is the security editor in the version of ldp.exe that comes with ADAM SP1.

Right-click a tree node ->Advanced -> Security Descriptor check the SACL box, click OK. Click in the SACL pane to add SACL. The windows (ADAM administrator) account you use to create/modify SACL must have Manage auditing and security log rights. This tool is very low level so if SACL or the SACL ACE setting do no mean much to you then careful study and testing are in order. In the security policy on the ADAM instance you will need to enable Directroy Service audit.

The key to audit of all objects is inheritance, *however* auditing success on all objects for everyone is going to be very noisy and may well hurt performance in production and so is not recommended.

Re: ADAM object auditing

Reading around the practices for AD audit should give you some pointers and then it's a case of deciding what's most important for your audit e.g. only child object creation.

HTH
Lee Flight

"richwray" <richwray@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>
wrote in message
news:8E87F946-1612-4ADA-A2F1-359167E204B8@xxxxxxxxxxxxxxxxxxxx

Is there anyway to enable object access auditing (or account management) on an ADAM partition, which would encompass ALL objects in the partition.

For example, if anyone changes a User or Group account in an ADAM partition it would record a success audit event in the Security log stating who did it, etc.

In the ADAM FAQ there is a sample script but it seems to only set auditing on a single object, whereas I'm looking for a way to do all user/group objects such that new objects being created would also trigger an entry in the log.

Thanks

Re: ADAM object auditing