

Re: auditing

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.active_directory/2004-02/2610.html

From: Tim Hines [MSFT] (*timhines_at_online.microsoft.com*)

Date: 02/29/04

Date: Sun, 29 Feb 2004 10:36:18 -0500

Enable auditing of account management will log the creation and changes to users and groups. I pasted a description from the help file for more info. You can audit Directory Service access to audit OU's. I've pasted info below about each audit setting.

Audit account management

Description

This security setting determines whether to audit each event of account management on a computer. Examples of account management events include:

- a.. A user account or group is created, changed, or deleted.
- b.. A user account is renamed, disabled, or enabled.
- c.. A password is set or changed.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when any account management event succeeds. Failure audits generate an audit entry when any account management event fails. To set this value to No auditing, in the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes.

Default:

- a.. Success on domain controllers.
- b.. No auditing on member servers

Configuring this security setting

You can configure this security setting by opening the appropriate policy and expanding the console tree as such: Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\

For specific instructions about how to configure auditing policy settings, see To define or modify auditing policy settings for an event category.

Account Management Events

624 A user account was created.

627 A user password was changed.

628 A user password was set.

- 630 A user account was deleted.
- 631 A global group was created.
- 632 A member was added to a global group.
- 633 A member was removed from a global group.
- 634 A global group was deleted.
- 635 A new local group was created.
- 636 A member was added to a local group.
- 637 A member was removed from a local group.
- 638 A local group was deleted.
- 639 A local group ac