ManageEngine
ADAudit Plus

Group Policy change monitoring, reporting, and alerting

www.adauditplus.com

Group Policy change monitoring, reporting, and alerting

Every organization relies on Group Policy to control and manage users and computers in their Active Directory environment. Some organizations use Group Policy more than others, but no matter the level of use, Group Policy is a key component for ensuring the environment is stable and secure. With such a reliance on Group Policy, it only makes sense that changes made to Group Policy be monitored closely to ensure the settings don't drift and are kept consistent.

Not only should the changes to Group Policy be monitored, but you should also have reports and alerts on them. Microsoft provides limited monitoring, reporting, and alerting of Group Policy changes, but these measures are not sufficient for administrators to know, in real time, what is occurring in their Group Policy infrastructure.

This white paper will discuss the Group Policy monitoring options available from Microsoft. It will then look at solutions that fill in the gaps left by Microsoft to give every administrator real-time alerting on Group Policy changes, not to mention the ability to report on Group Policy changes over time.

Microsoft's monitoring of Group Policy changes

By default, Microsoft does not monitor changes made to Group Policy. Historically, Microsoft has not monitored the changes made to Active Directory due to concerns of overloading domain controllers with intensive logging and space concerns from the resulting logs. However, with technology surpassing these concerns, monitoring changes made to Active Directory should be incorporated by every administrator.

In order to monitor changes made to Active Directory, Group Policy changes specifically, auditing needs to be enabled. Auditing is a subset of Group Policy and should be configured so that all changes are tracked. To configure auditing, a new Group Policy Object (GPO) should be created and linked to the Domain Controllers organizational unit (OU). (The Default Domain Controllers GPO could be modified, however this is not a good practice.)

The configurations that need to be made in the Audit Policy to track Group Policy changes are shown in Figure 1.

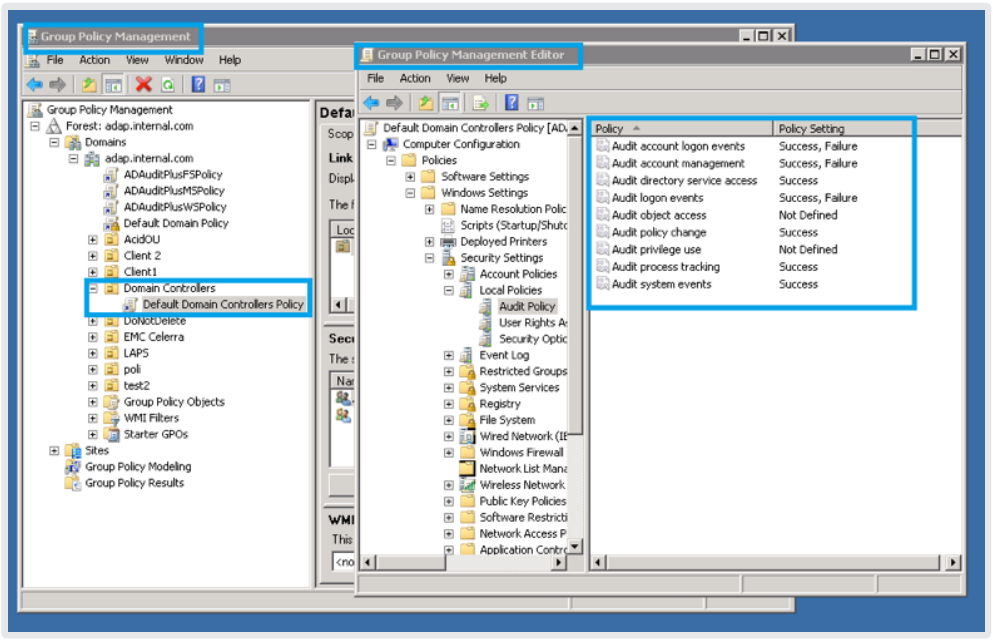

Figure 1. Audit Policy configurations to track Group Policy changes.

Not only does the Audit Policy need to be configured, but the security access control list (SACL) in Active Directory needs to be configured as well. These changes are listed in Figure 2.

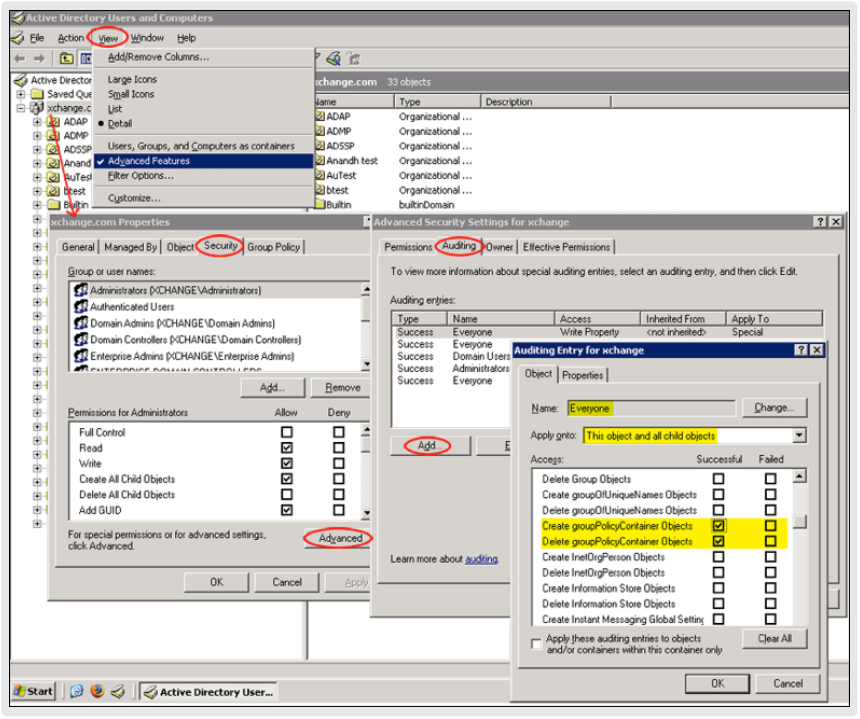

Figure 2. SACL configurations to track Group Policy changes.

Once the Audit Policy and the ACLs have been updated, all changes to Group Policy will be tracked and logged in the security log on each domain controller where the activity occurred. Figure 3 illustrates what a sample Security Log event looks like for Group Policy changes.

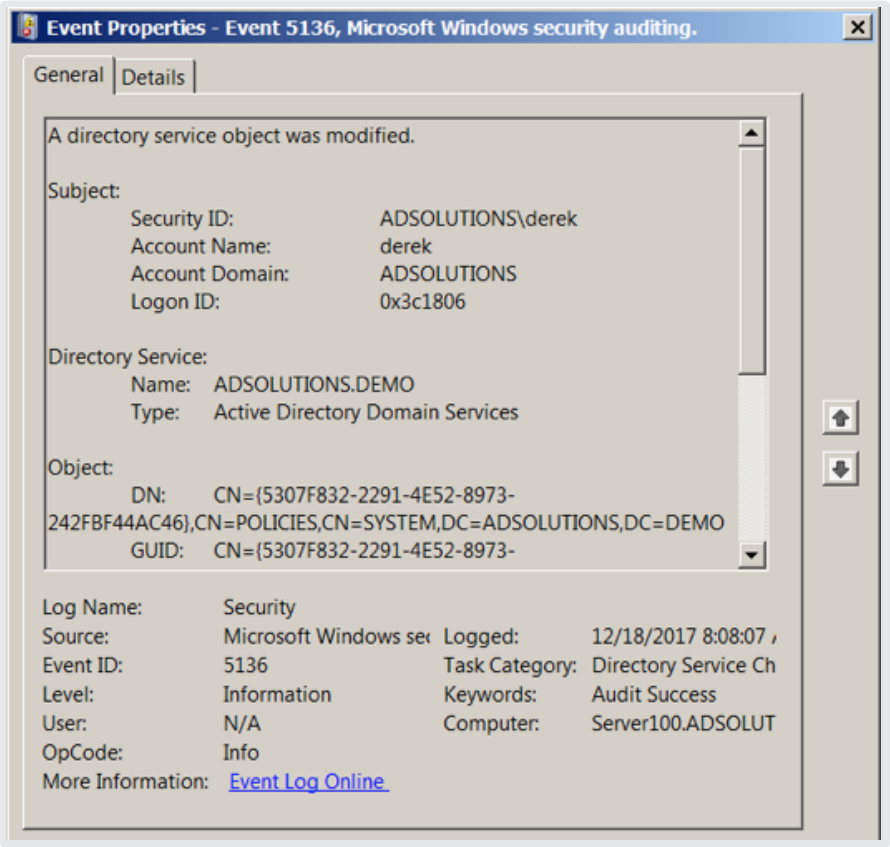

Figure 3. Security log entries for Group Policy changes.

Microsoft reporting of Group Policy changes

Most administrators use the Group Policy Management Console (GPMC) to manage and configure changes related to Group Policy. Everything from creating, editing, deleting, linking, and securing GPOs (and more) can be done in the GPMC. Unfortunately, the GPMC does not provide any reporting for the changes that occur in or to a GPO.

We already configured the Audit Policy and ACLs so that all GPO changes are tracked and located in the security log. Unfortunately, the Event Viewer, which is the tool used to view the security log, does not have any reporting mechanism. The closest option to reporting using the Event Viewer is to filter the security log or to use the Custom View. Neither option allows for a report to be generated from the information you are viewing.

Microsoft alerting of Group Policy changes

The GPMC does not provide any form of alerting when a GPO or any Group Policy-related change occurs.

The Event Viewer does have alerting capabilities. Therefore, an alert can be generated when a Group Policy change occurs. The alert options available using Event Viewer include running a program, sending an email, or displaying a message, which can all be seen in Figure 4.

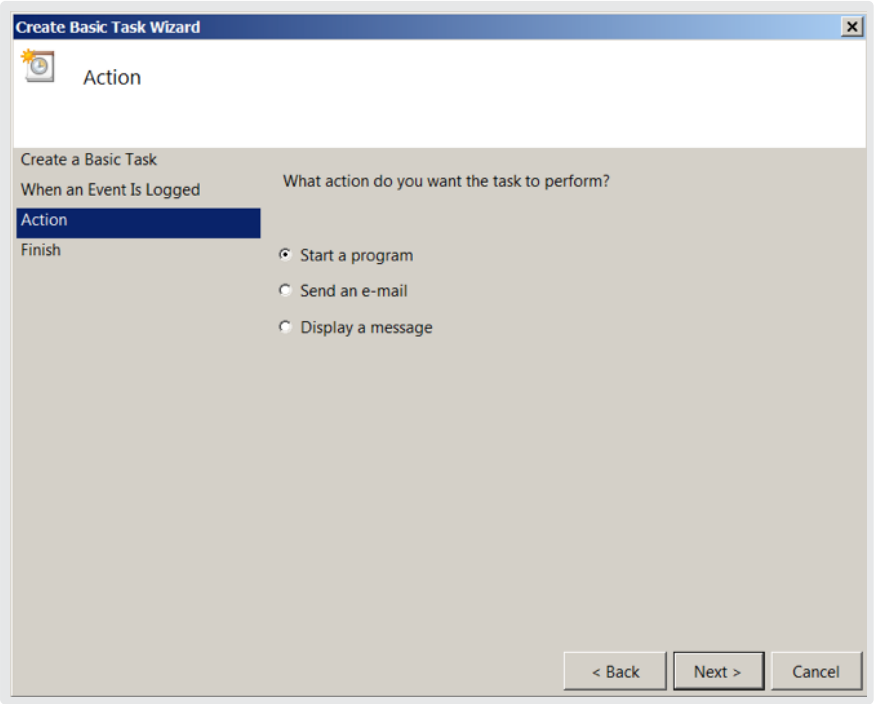

Figure 4. Event Viewer alert options.

The issue with using Event Viewer to send alerts is that the alert cannot be targeted to granular changes. The lowest level of alert is per event ID. So, any and all changes to Group Policy related to the event ID that you target will generate an alert.

Although Event Viewer can generate alerts, one must consider what the alert will produce to consider if the solution is valid. Running a program and displaying a message will not help the administrator determine what the change was with Group Policy. Only an email will indicate in any way what the change was. However, the default email notification in Event Viewer will not contain any details for the event. You must code the alert in the notification task to include any valuable information, as well as test it for nearly every situation when you might need to get details for Group Policy changes.

ADAudit Plus' monitoring, reporting, and alerting of Group Policy changes

Most administrators want a solution that is easy to install, efficient to manage, and generates results that are useful. ADAudit Plus is just that solution for changes that are occurring in Active Directory and to Group Policy. ADAudit Plus comes with over 125 canned reports, and more than 15 of those are dedicated to Group Policy.

Monitoring Group Policy changes is no simple task. Changes made to the settings in a GPO, modifications of GPO links, and even changes to the permissions on a GPO need to be monitored.

ADAudit Plus monitors all of these changes and much more. Below is a summary of what ADAudit Plus monitors with regard to Group Policy changes:

- Created GPOs
- Modified GPOs
- Deleted GPOs
- Permission changes to GPOs
- GPO link changes
- GPO History
- Undeleted GPOs
- Group Policy Settings changes
- Computer Configuration changes
- User Configuration changes
- Password Policy changes
- Account Lockout Policy changes
- Security Settings changes
- Administrative Template changes
- User Rights Assignment changes
- Group Policy Preferences changes
- Extended Attribute changes

Figure 5 illustrates what these monitored areas look like in ADAudit Plus.

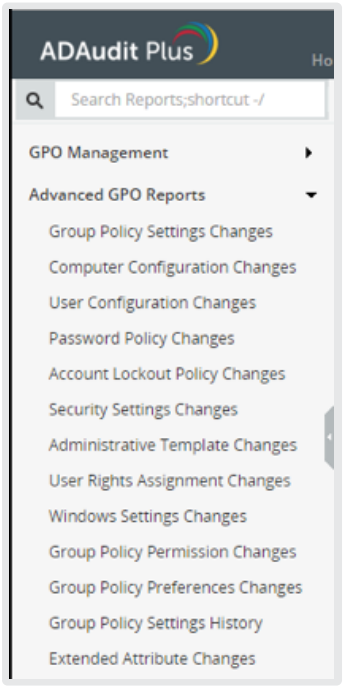

Figure 5. Group Policy-related areas in ADAudit Plus.

Monitoring changes to Group Policy is essential, but so is generating reports for these changes. Reports are required for documentation, not to mention for security professionals and auditors to meet compliance requirements. The ability to generate reports on specific aspects of Group Policy, especially over a given time frame, is an invaluable feature that all administrators require. This does not preclude the fact that reports can be automated to be created as often as every hour. Figure 6 illustrates what an automated report configuration looks like.

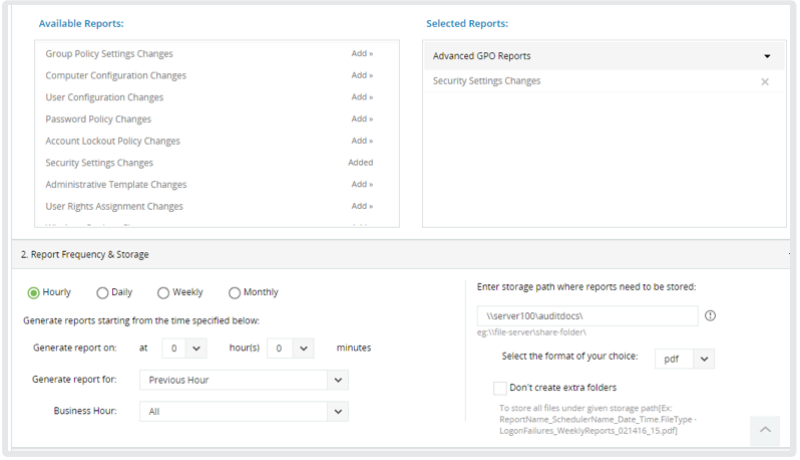

Figure 6. ADAudit Plus can automate the report generation of Group Policy changes.

Every administrator has limited time and very few administrators have the time to review reports. This is why ADAudit Plus provides detailed, granular, and automated alerting for all changes made to Group Policy. The alerts can be sent directly to the administrator's inbox, giving them full details on the changes that were made to Group Policy. Email alerts can also be sent when reports are automatically generated, so administrators are privy to when the reports are made available. Figure 7 illustrates what the alert configurations look like for Group Policy changes.

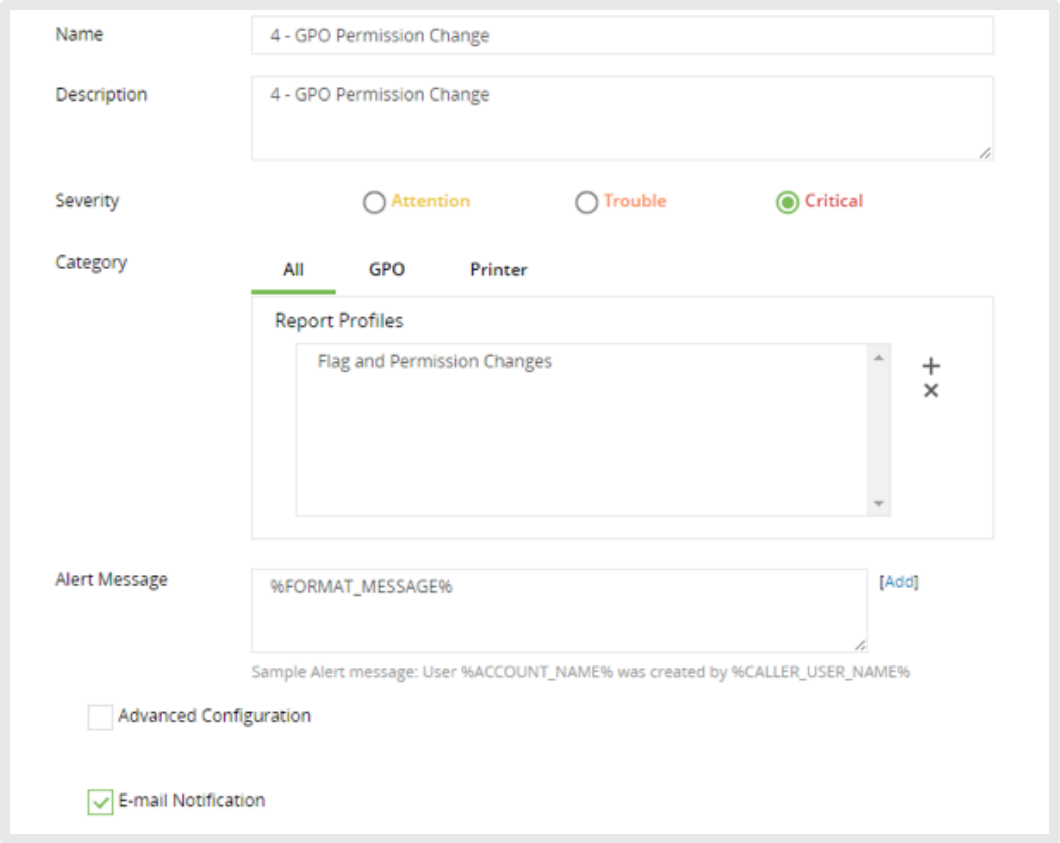

Figure 7. Group Policy changes can be sent to administrators in an email alert.

Of course, ADAudit Plus can also display alerts in a dashboard, and all historical alerts can be viewed and shown as a report.

Summary

Group Policy is complex. Changes made to Group Policy are nearly impossible to track, particularly without the right tools in place. Being able to monitor, report, and alert on all Group Policy changes will alter the way that you administer your Group Policy infrastructure. With a proper Group Policy change monitoring system in place, you will have a 360 degree view of all changes that are occurring to Group Policy, at all times. No longer will you need to troubleshoot for hours trying to discover what changed in Group Policy; you'll simply have email alerts indicating a change was made, with a complete history of the changes that were made to any and all Group Policy Objects.

ADAudit Plus provides a complete solution for organizations to monitor, report, and alert on Group Policy changes. Download ADAudit Plus today to start tracking your Group Policy changes.