True Continuous Auditing for Active Directory

by

Derek Melber
Group Policy and Active Directory MVP
ManageEngine ADSolutions Technical Evangelist

True Continuous Auditing for Active Directory

Today, most auditors perform a standard audit on Active Directory. This standard audit is very outdated, as it is a point-in-time solution that is only good for the day the reports were generated. Changed made to Active Directory can be made many times in between the standard audits, which are typically performed only once a year. These changes made to Active Directory are not tracked, not noticed, and put the entire enterprise at risk. There are, however, solutions that provide true continuous auditing of Active Directory and the changes that occur. The ideal solution will have built-in reports that are easy to read, separate of roles, custom reporting, and alerting. This white-paper will give you the insight into the ideal solution.

Standard Auditing of Active Directory

A standard audit of Active Directory is completed by gathering information of the existing infra-structure. I call this a point-in-time audit because the auditor asks the administrator to gather reports based on the current state of the servers. This means that the administrators must use tools (either built-in or third party) to discover and report on the controls that the auditor deems important for the audit.

The above summary is the end result, but what are the other moving components of a standard audit of Active Directory? Let's take a detailed look at each component.

Scoping the Audit

If you are performing an internal audit or external audit of Active Directory, you must first establish the size of the Active Directory, including all of the details related to the infrastructure. Here are the minimal details you will need to gather to scope the audit:

- Number of Active Directory forests
- Number of Active Directory domains
- Number of domain controllers per domain
- Number of trust relationships per domain
- NetBIOS and DNS names per domain
- Structure of the organizational units per domain

Most organizations also include Windows servers in their audits, which is a good idea.
In order to scope and choose the Windows servers, you need to know the following information:

- Number of Windows servers per domain
- List of key applications per server (HR, finance, intellectual property, private information, etc.)
- List of operating systems per Windows server
- List of physical locations for company being audited
- Breakdown of IT structure per location
- Design implementation of security using group policy and organizational units, if any

Development of Audit Program

The development of the audit program is usually based on four factors: scope, sampling, compliance requirements, and security controls. Changes to any of these factors can alter the audit program completely. Most audits are confined to both time and resources. Of course, both are tied to money, but the amount of time and number of people are the related physical issues that strap down an audit.

Most audits are driven primarily by compliance requirements. The end result must suffice the compliance requirements in order to avoid fines and additional time to meet the requirements. There is little that can be done to reduce compliance requirements, as they are mandated and must be met. Ideally, there needs to be a good balance between the four factors.

The more servers that can be sampled, the better the overall confidence of the results. If the scope is large (multiple domains), the overall audit time must be increased or the security controls will need to be reduced. If the scope is small and the sample is relatively small, the security controls can be increased to cover more areas of the Windows environment.

The end result of considering these four factors is the audit program. The audit program will consist of a list of reports needed for each server. Ideally, the audit program will include details such as:

- Tool being used to gather report
- Specifics regarding tool, such as command line example, location on server, menus and options to be selected, etc.
- Servers for which the tool should be run
- Report file format (.doc, .xls, .txt, etc)
- Report file name

Analysis and Audit Report

The analysis of the reports that you obtain will need to be evaluated based on many criteria. The criteria that you use for your analysis could vary drastically from company to company. The criteria could differ due to the fact that each company is willing to accept different levels of risk for each of the security controls that is being evaluated. In order to perform the analysis, you will need to obtain the following documentation:

- Notes taken from interview with administrator
- Company documentation regarding security configurations and controls
- Server build documentation
- Microsoft industry standards for security controls
- All reports related to the audit program

From these documents you will be able to perform your analysis. The outcome from the analysis will be a list of security controls that do not meet the security baselines and configurations that your company has set. These security controls that are not correct are usually written up in the final report as exceptions. In that final report, each exception should have details regarding the control and what was expected and what was found. This should be on a computer by computer basis, but in some cases when the exception is so widespread, the report could just indicate that. Most reports will have a listing of the security control, the issue that was found, background information describing the security control, and suggested resolution.

Concerns with Standard Auditing of AD

Most Active Directory audits follow the same procedures and processes, therefore auditors are subject to the similar circumstances no matter what environment they are dealing with. With this similarity in procedures and processes, most auditors have a laundry list of issues that concern them. Most of the issues and concerns are not warranted, but some are justified.

Security Controls Being Altered for Report Only

This concern is usually not justified, but there are vindictive administrators who would do something like this. There is little that can be done in order to overcome this issue. Even if you "observe" the administrator generating the report, there is no certainty that the change was made before you started your observation. The only true way to verify that this is not occurring is to perform continuous auditing on the controls to ensure that no changes have been made over time.

Text Documents are Not Reliable

This is a valid concern, but the premise is not valid. The premise is that, compared to a screen capture, a text file can "easily" be changed. This is wildly incorrect. Screen captures can just as easily be changed. In the end, if you are only receiving screen captures, your time to analyze information can be nearly doubled compared to obtaining text files, which can be searched.

Reports Are Incorrect

Auditors often are concerned that the information that they are provided is not correct. The concern could be that the administrator changed the information before generating the report (addressed above) or that the information provided is not the correct information. For example, I find that less than 5% of all auditors gather the correct information regarding the domain users' password policy. Not obtaining the correct information is a complete waste of time. Ensuring the information that is received is correct and accurate is essential.

It is essential that the reports that are being generated and provided are giving you the correct information. No matter if you are physically present, watching remotely, or trusting that the administrator is giving you the right information.

Changes Made Between Audits are Not Captured

A standard audit is a point in time only. This means that changes made before the report is run or after the report is run are not captured. In reality, changes can be made many times between audits, and the security controls for these changes would never be captured. This leaves the company and entire network at risk for attack. Figure 1 illustrates what a point-in-time audit actually means on a timeline.

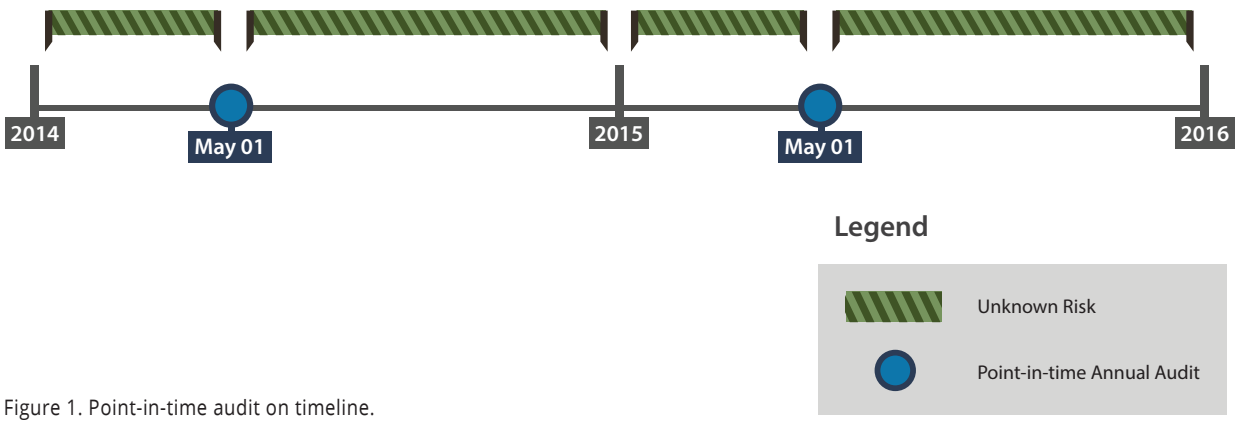

Figure 1. Point-in-time audit on timeline.

Continuous Auditing

As a solution to the shortcomings of point-in-time audits, the auditing community came up with the concept of continuous auditing. This concept is brilliant, but the typical implementation is not. Often, continuous auditing is accomplished by using existing, point-in-time tools that are simply run more often or scheduled to run periodically. The end result is close to continuous auditing, as multiple reports are run for the same security controls. Figure 2 illustrates typically continuous auditing on a timeline. However, the disparate results must be manually compared to the other reports to determine if there are any changes from one report to the other.

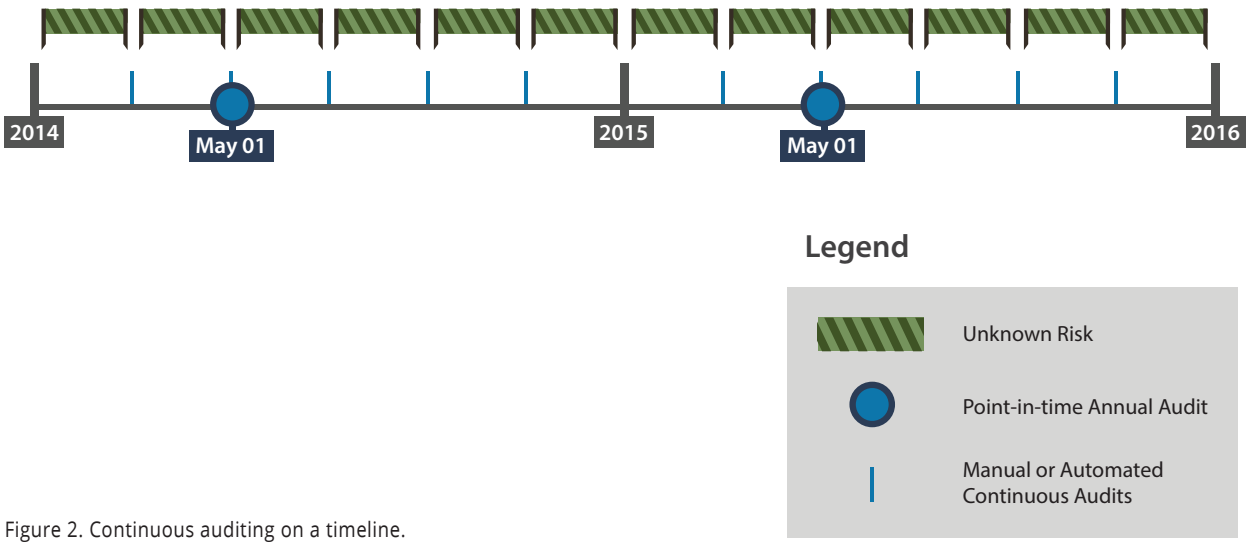

Figure 2. Continuous auditing on a timeline.

There are quite a few tools that can be used to generate periodic or schedule reports. These tools are typically free or very inexpensive, including:

- Active Directory Users and Computers: Saved Queries
- Dumpsec (both GUI and command line options)
- Powershell (basic PowerShell and the Active Directory Module for PowerShell)
- PowerGUI (A Dell/Quest tool based on their ActiveRoles Management Shell for Active Directory)
- Scheduled tasks (built into every Windows computer)

True Continuous Auditing

As you can see from the standard auditing and continuous auditing approaches above, there are too many chances for changes to occur to Active Directory without those changes being tracked, reported, or analyzed. This lack of reporting for changes that occur between audits and reports being generated exposes the environment to potentially high and devastating risks.

In reality, any point-in-time audit, whether standard or generated periodically, is only as good as that point in time. Point-in-time reports fail to generate constant changes that might occur to security controls. In an ideal continuous auditing world, point-in-time audits would be replaced with constant tracking and reporting on security controls.

The features of such a solution would include:

- Every change made in Active Directory would be tracked (See Figure 3.)
- Reports would clearly indicate if and when security controls were changed, including details
- regarding date, time, user making modification, modifications made, etc.
- Read only access would be granted, so auditors could generate reports at will
- Customized reports could be created to monitor and report on specific users, computers, and groups
- Alerts could be generated when key security controls change

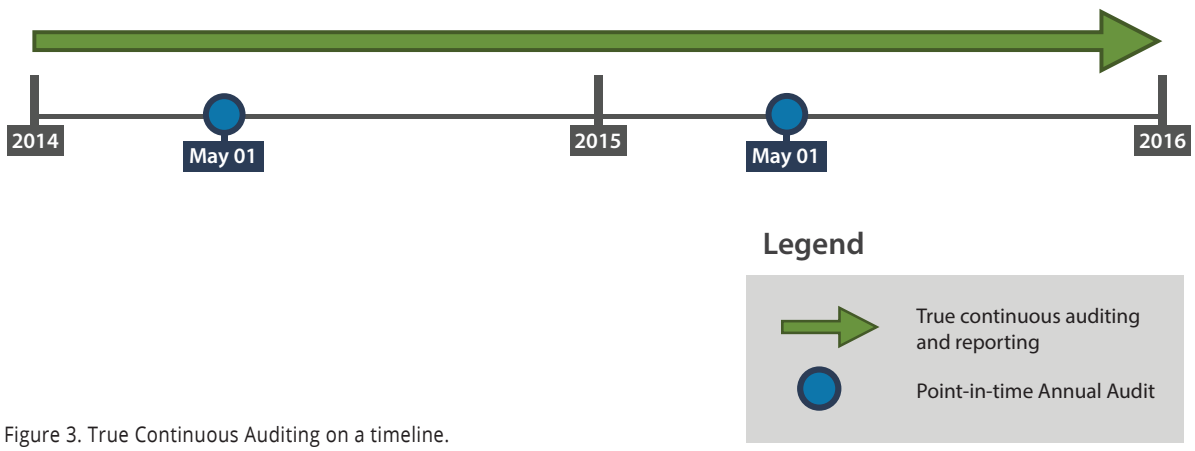

Figure 3. True Continuous Auditing on a timeline.

ADAudit Plus

True continuous auditing has not been obtainable until now. ManageEngine ADAudit Plus is the tool that makes true continuous auditing a reality. ADAudit Plus is powerful, comprehensive, easy to use, developed with reporting in mind, and completely integrated with alerting for key security controls.

Every Change to Active Directory Tracked

Every Windows domain controller provides extremely verbose auditing of every change that occurs to every object in Active Directory. ADAudit Plus taps into these logs and captures the information in a database before the Windows log is overwritten. The captured information is then organized for quick and efficient reporting. ADAudit Plus provides over 125 reports that give you insight into changes to users, groups, organizational units, group policy, and more. Figure 4 gives you a quick view of the multitude of areas that ADAudit Plus reports on.

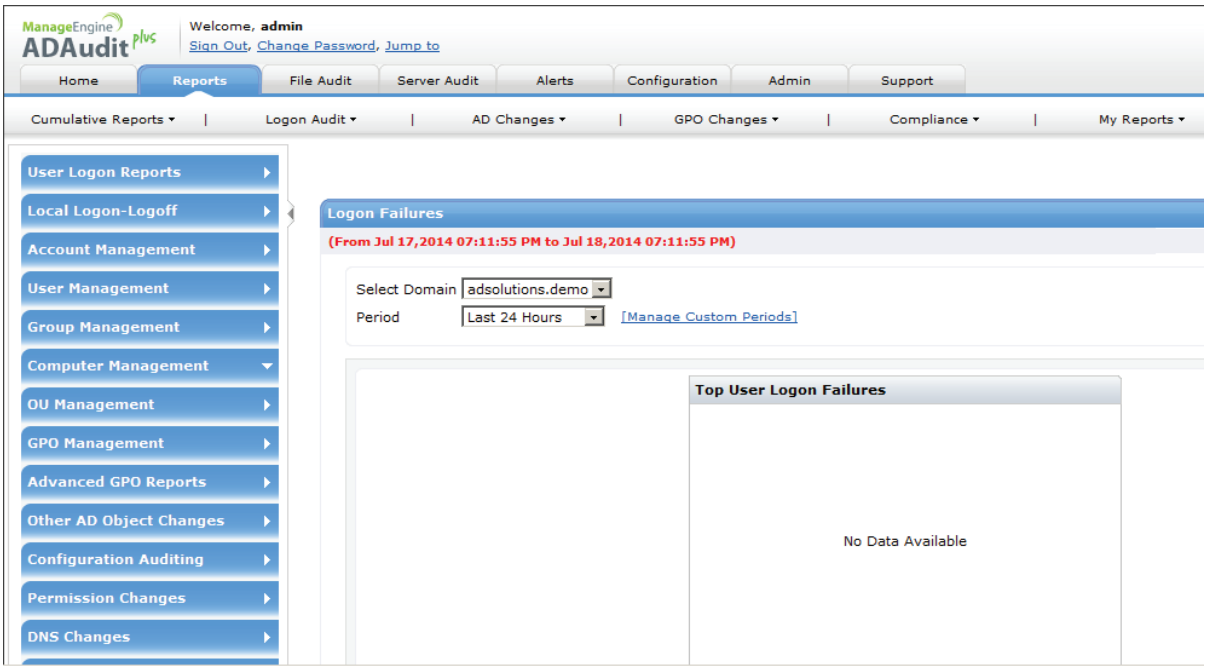

Figure 4. ADAudit Plus provides over 125 default reports.

Reports Are Verbose

Each report provides detailed information that can be used to determine exactly what was changed in Active Directory. Depending on the report, information will be provided as to who made the change, when the change was made, what change was made, as well as the old and new configurations where applicable. Figure 5 shows you a sample of such a report.

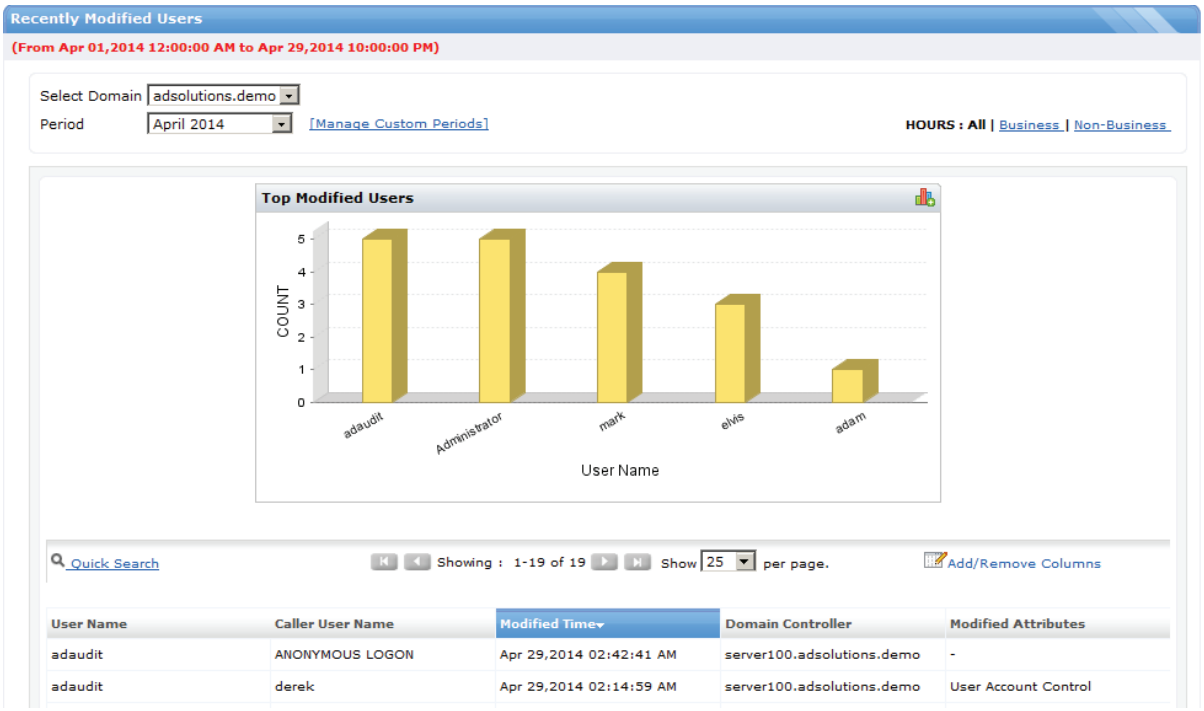

Figure 5. ADAudit Plus provides verbose reporting to give you insight into what was changed in Active Directory.

Read-only Access to All Reports

One of the most important aspects of auditing is the ability to separate the different roles and responsibilities of those involved with the security configuration, reporting, and auditing. Ideally, these different roles should be controlled through both Windows permissions and the tool being used to generate the true continuous auditing reporting. ADAudit Plus provides this separation with seamless effort. ADAudit Plus does not require any installation for the auditor, only that the auditors user account is granted “Operator” access, which allows for read-only access to every report as seen in Figure 6.

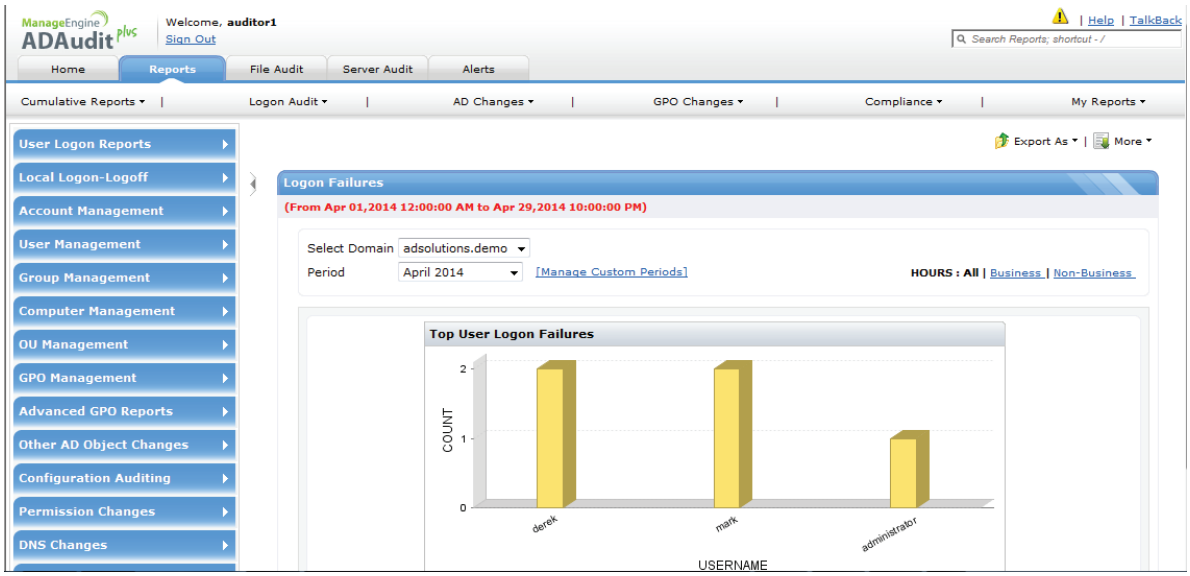

Figure 6. ADAudit Plus provide read-only access to reports.

Customized Reports are Easy to Create

Every Active Directory installation has custom users, groups, service accounts, and more. These accounts need to be monitored just like every other built-in user and group. ADAudit Plus provides customization of these custom users and groups, so special reports can be created to report on just what you want to see. For example, custom groups are created for many applications that are installed. These groups are granted elevated privileges and need to be monitored. Figure 7 shows you what a custom report for custom groups might look like.

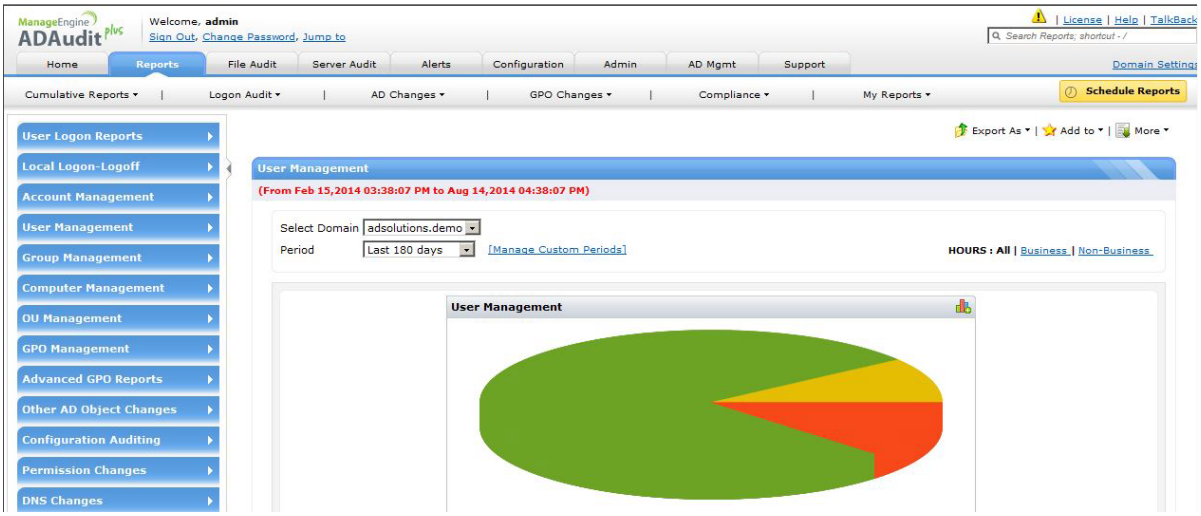

Figure 7. ADAudit Plus provides customization for your Active Directory enterprise of users and groups.

Alerts are Easy to Create

The key to true continuous auditing is not only the ability to track every change made to Active Directory and make it reportable but also to have an immediate alert generated when a key security control is changed. Alerts can be created to match every built-in and custom report, with the outcome being an event being generated, the ADAudit Plus interface indicating the alert, and an email being sent to your inbox. Figure 8 shows you how the alerts look in the interface.

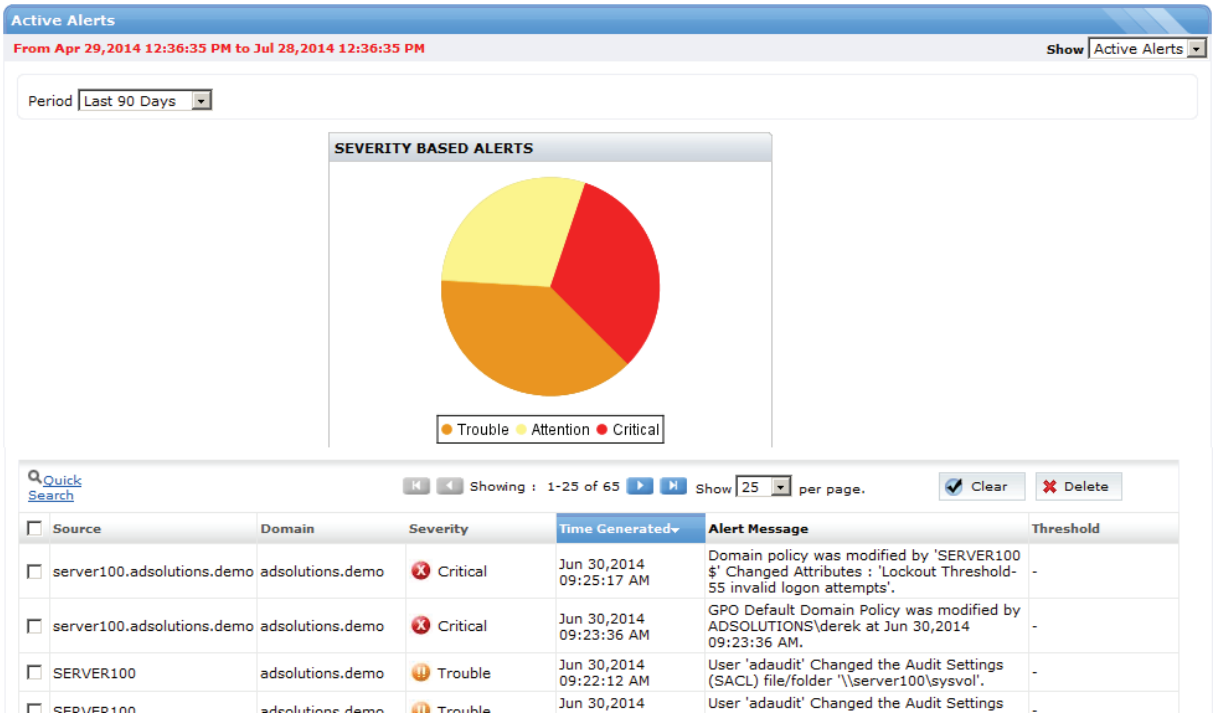

Figure 8. Alerts give you insight into changes made in real time to Active Directory.

Summary

Standard auditing is outdated, inefficient, and insufficient to provide enough information needed to truly audit and secure your Active Directory enterprise. However, ADAudit Plus from ManageEngine provides a true continuous auditing solution that is revolutionary, efficient, and complete. Reports are plentiful, insightful, and comprehensive; and they can be set for read-only mode. Custom reports can give you insight into your specific Active Directory installation. Alerts can be created to immediately Inform you of key security control changes that occur. ADAudit Plus can be downloaded and installed from http://www.manageengine.com/products/active-directory-audit/.

About ADAudit

ADAudit Plus is an IT security and compliance solution designed for Windows-based organizations. It provides in-depth knowledge about changes effected to both the content and configuration of Active Directory and servers. Additionally, it provides thorough access intelligence for desktops and file access in servers (including NetApp filers), enabling you to protect organization data.

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization's need for real-time services and support. Worldwide, more than 90,000 established and emerging customers - including more than 60 percent of the Fortune 500 - rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. Another 300,000-plus admins optimize their IT using the free editions of ManageEngine products. ManageEngine is a division of Zoho Corp.with offices worldwide, including the United States, United Kingdom, India, Japan and China.

For more information

Please visit:

www.manageengine.com/adsolutions

http://blogs.manageengine.com/

Follow us on:

Facebook: https://www.facebook.com/adsolutions.manageengine

Twitter: @me_adsolutions