ManageEngine ADAudit Plus

Workbook

Table of Contents

Active Directory Auditing with ADAudit Plus

Address the most-needed security, audit and compliance demands; arm yourself with easily comprehendible thorough reports and alerts- the right business add-ons to assist in the execution of a change management action and export the results to xls, html, pdf and csv formats to assist in interpretation and computer forensics.

For security reasons critical resources in the network like the Domain Controllers, access rights are crucial, ADAudit Plus lists the entire information on users who have last logged on / logged off or have attempted to breach access critical resources in the domain. Track user, GPO, Computer, OU changes with 150+ detailed event specific reports and instant email alerts.

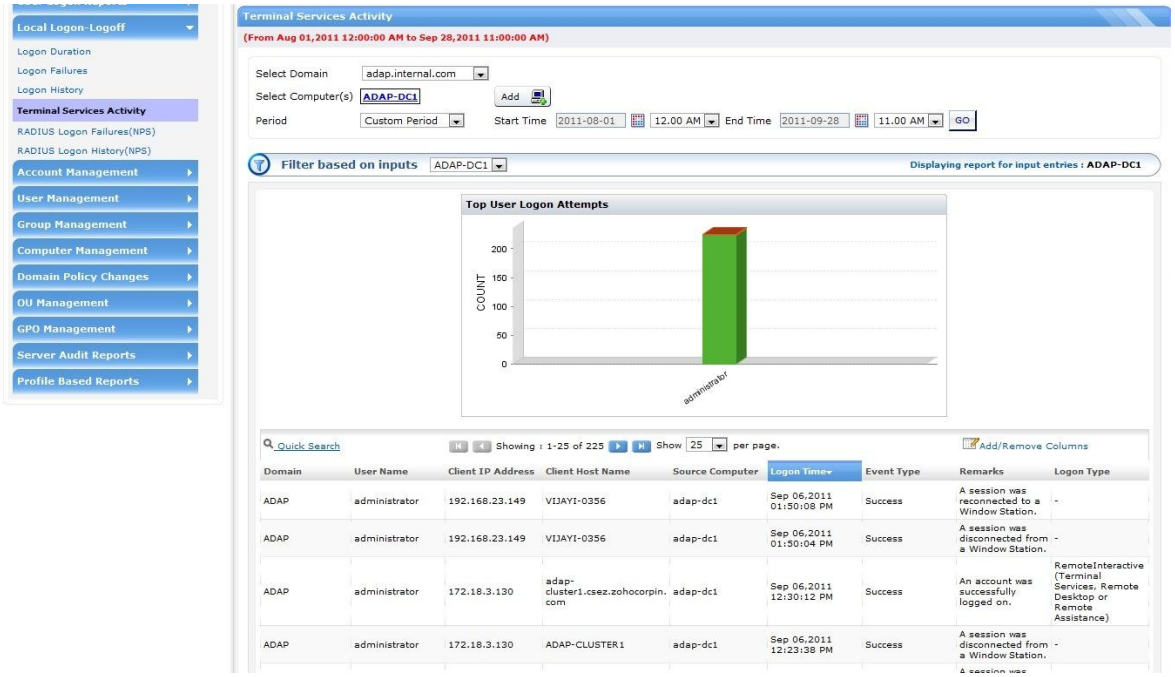
- Track users Logon / Logoff, GPO, OU and Audit User Management Actions.
- Delegate User Management Tasks to Support Staff
- View **user object life cycle changes** - creation, modification and deletion of a user object.
- **Admin** can assign helpdesk tasks to track and monitor account changes in the domain with reports and alerts.
- View reports specific to any / every Active Directory change.
- Monitor important user account changes in the recent past.
- Export the reports to desired formats xls, csv, pdf and html.
- Maintain accountability of actions done by administrators, helpdesk technicians, human resource staff or any selected user in the organization with reports from archived information.

Logon Auditing with ADAudit Plus

Customer Use Case:

Need to capture who logged in recently on which computer in the domain using terminal services.

ADAudit Plus Terminal Services logon reports can be advantageously used to overcome user terminal services logon audit challenges. With a host of pre-configured reports to provide answers to logon audit questions in the format desired and enhance Active Directory auditing experience.



Summary of Terminal Services Activity for a Selected period

A bar graph is displayed. Each bar denotes an audit action on the server. The size of the bar shows the number of events. Click on the bar graph to filter and view desired audit change on the Terminal Servers.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the ‘Local Logon-Logoff’ Report Category from the Available list.
3. Select ‘Terminal Services Activity’ Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.

Critical ADAudit Plus Reporting Features

Detailed reports based on Domain, User Name, Client IP Name, Client Host Name, Source Computer, Logon Time, Event Type, Remarks, Logon Type, Quick Search (Filter based) and many more…

Other Logon Auditing Reports

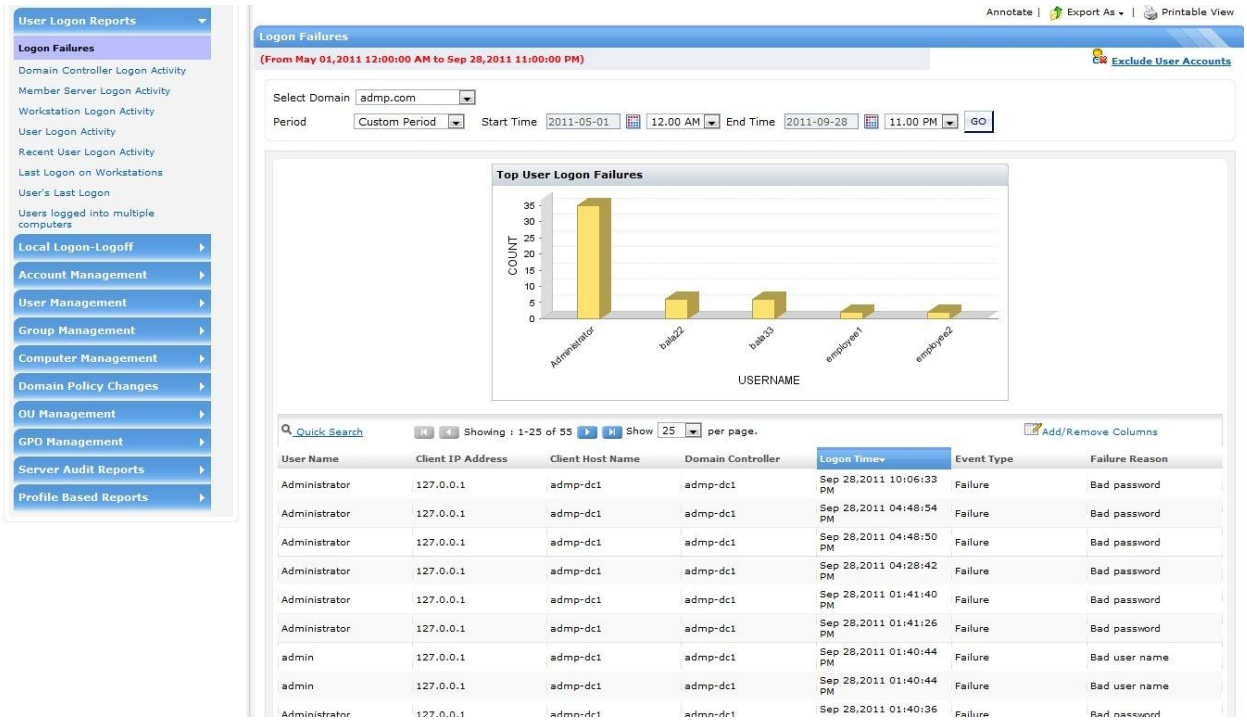
Logon Duration | Logon Failures | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | **Terminal Services Activity** | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Logon Auditing with ADAudit Plus

Customer Use Case:

Have to check whether any user tried logging in to the computers they don't have permissions.

Logon Failure Report provides information on the reason for logon failures over a selected period of time. Multiple logon failure attempts (bad logon attempts) on User accounts in the selected period of time equip administrators with information on possible attacks on "intruder attack susceptible" accounts. Information on logon failure alike when a logon failure occured, logon failed account, and possible failure reasons is reported.



Summary of User Logon Failures for a Selected period

A bar graph is displayed. Each bar denotes an audit action on the server. The size of the bar shows the number of events. Click on the bar graph to filter and view desired audit change on the Domain Controller.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'User Logon' Report Category from the Available list.
3. Select 'Logon Failures' Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Client IP Name, Client Host Name, Domain Controller, Logon Time, Event Type, Failure Reason, Quick Search (Filter based) and many more…

Other Logon Auditing Reports

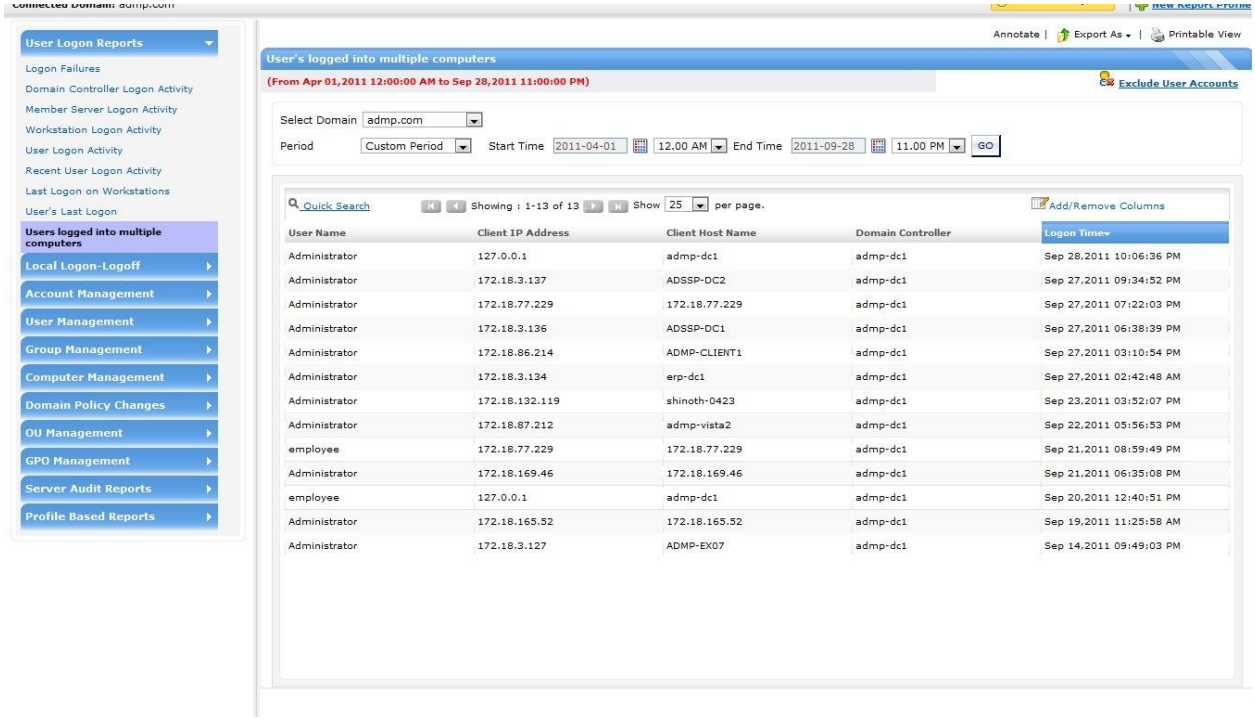
Logon Duration | **Logon Failures** | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Logon Auditing with ADAudit Plus

Customer Use Case:

What if any one logged into multiple computers at a time.

Windows Active Directory allows its domain users to login into multiple computers at any given instant. Administrators, auditors and managers require advanced tools to track these logons to ensure that resources are used as desired. '**Users logged into multiple computers' report** provide the last logon data of user/users into multiple computers within a given time frame.



Summary of Users logged into multiple computers for a Selected period

The multiple computers access events are presented as refined data for a descriptive format to ease in auditing who-did-what-from-where along with many filter options to help single-out the user in question. Each event is an audit action on the server.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the ‘User Logon’ Report Category from the Available list.
3. Select ‘Users logged into multiple computers’ Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Client IP Name, Client Host Name, Domain Controller, Logon Time, SID, Logon Service, Event Type, Failure Reason, Quick Search (Filter based) and many more…

Other Logon Auditing Reports

Logon Duration | Logon Failures | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | **Users logged into multiple computers**

Logon Auditing with ADAudit Plus

Customer Use Case:

I want to see a report on failure logins for a particular Group.

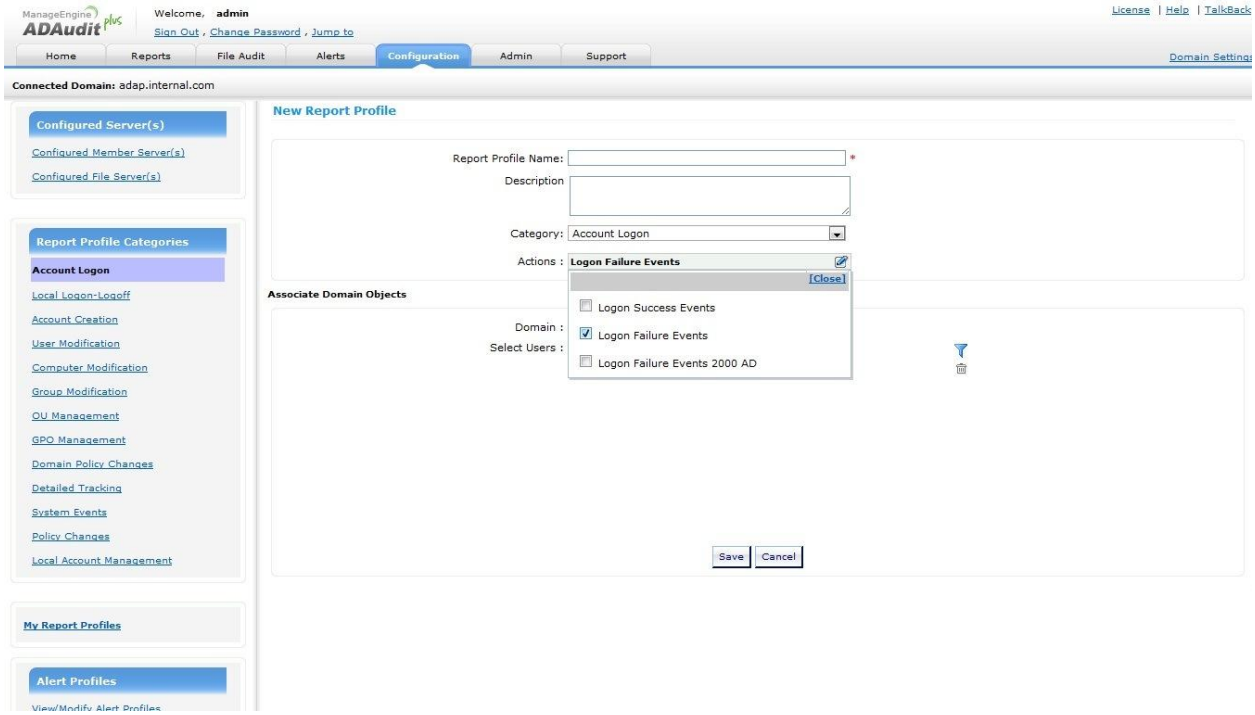
Windows Active Directory allows its domain users to login into multiple computers at any given instant. Administrators, auditors and managers require advanced tools to track these logons to ensure that resources are used as desired. '**Users logged into multiple computers' report** provide the last logon data of user/users into multiple computers within a given time frame.

Steps to create the Custom Report

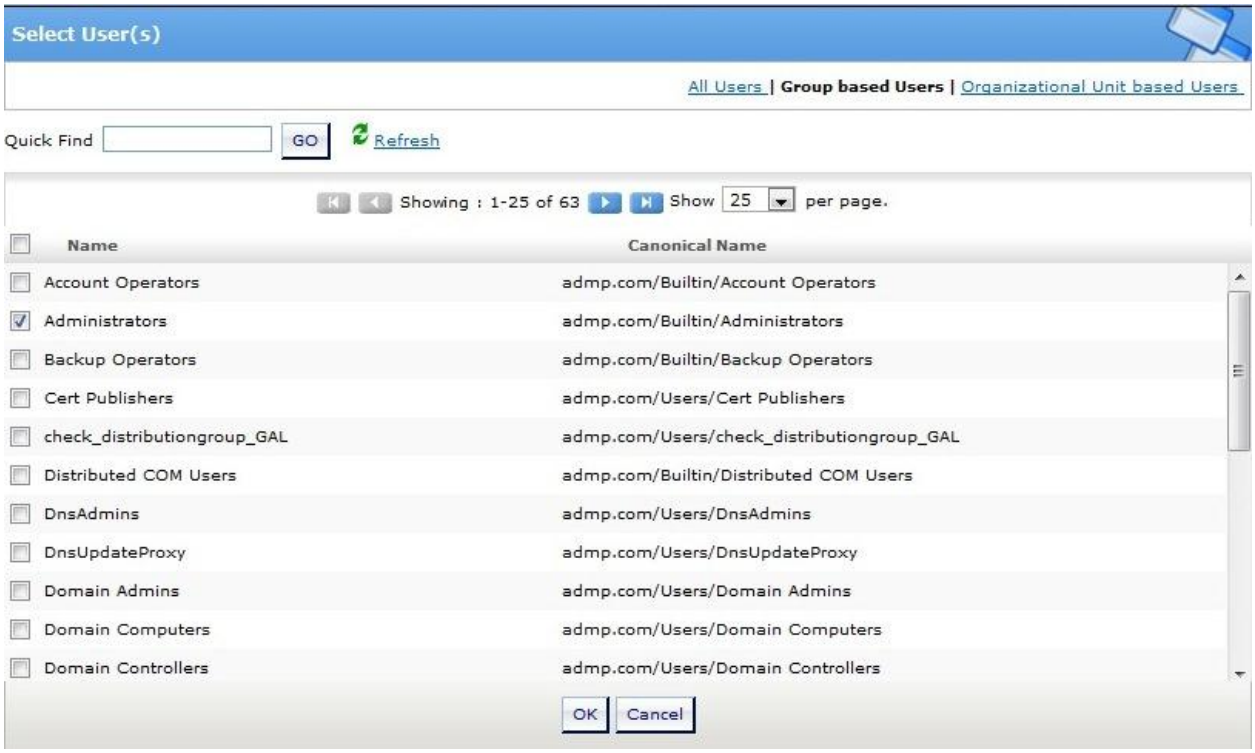
Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the New Report Profile option on the top-right.
3. Choose 'Logon Failure Events' from the pre-listed report categories.
4. Select the Domain and Click on Group Based Users.
5. Select the Group(s) to be Audited and Click Save.
6. **To View,** select the configured Report from the Profile Based Reports.
7. Select the Period. Custom Period can also be selected.

New Report Profile



Simply choose from the Pre-listed report categories



Click on Group Based Users and Select the Group(s) to be Audited

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Client IP Name, Client Host Name, Domain Controller, Logon Time, Source Computer, Remarks, Logon Service, Event Type, Failure Reason, Quick Search (Filter based) and many more…

Other Logon Auditing Reports

Logon Duration | Logon Failures | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

User Object Change Auditing

Customer Use Case:

Report when Administrator's password is changed.

One of the most critical reports, to help pin-point the authorized or unauthorized password change for an administrator's account! With the many filter attributes on offer, interpreting and solving an otherwise bleak situation is very simple.

Steps to create the Custom Report

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 

option on the top-right.
3. Choose 'User Modification' from the pre-listed report categories.
4. Choose the preferred event to be audited- 'User Password was changed'.
5. Select the Domain and Select the User 'Administrator' and Click Save.
6. **To View,** select the configured Report from the Profile Based Reports.
7. Select the Period. Custom Period can also be selected.

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Client IP Name, Client Host Name, Domain Controller, Logon Time, SID, Logon Service, Event Type, Failure Reason, Quick Search (Filter based) and many more…

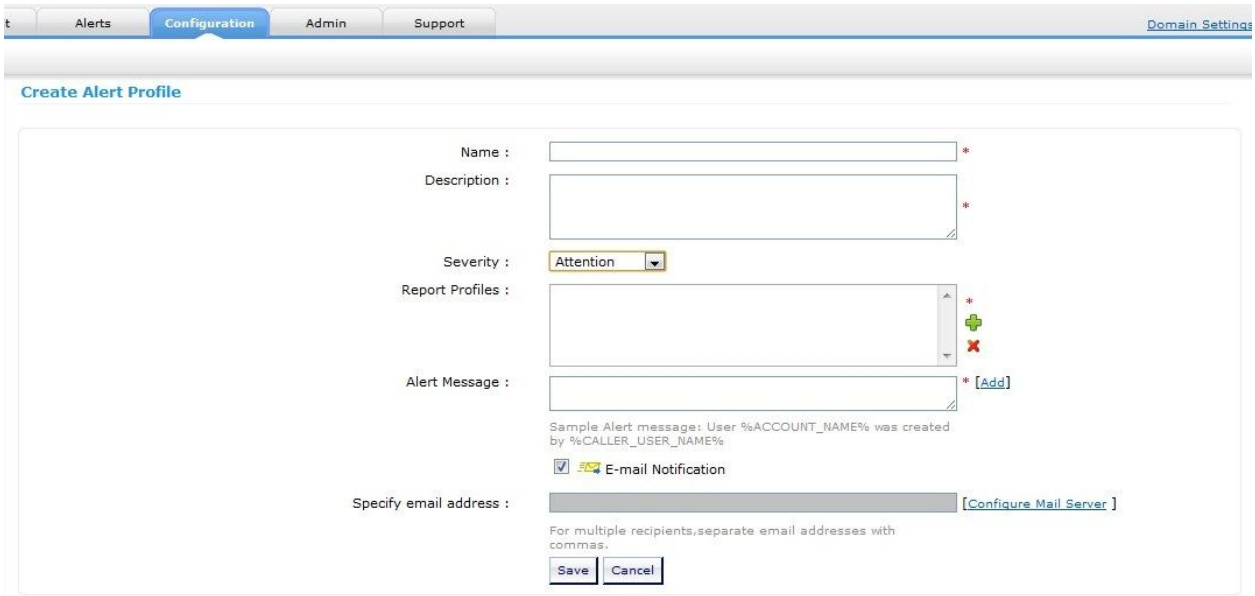
Alerts

Instant Event Alerts can be created, when the criticality is of the highest order in addition to the scheduled emailing of reports.

Steps to create the Event Alerts

Assuming ADAudit Plus Server is running, we will proceed:

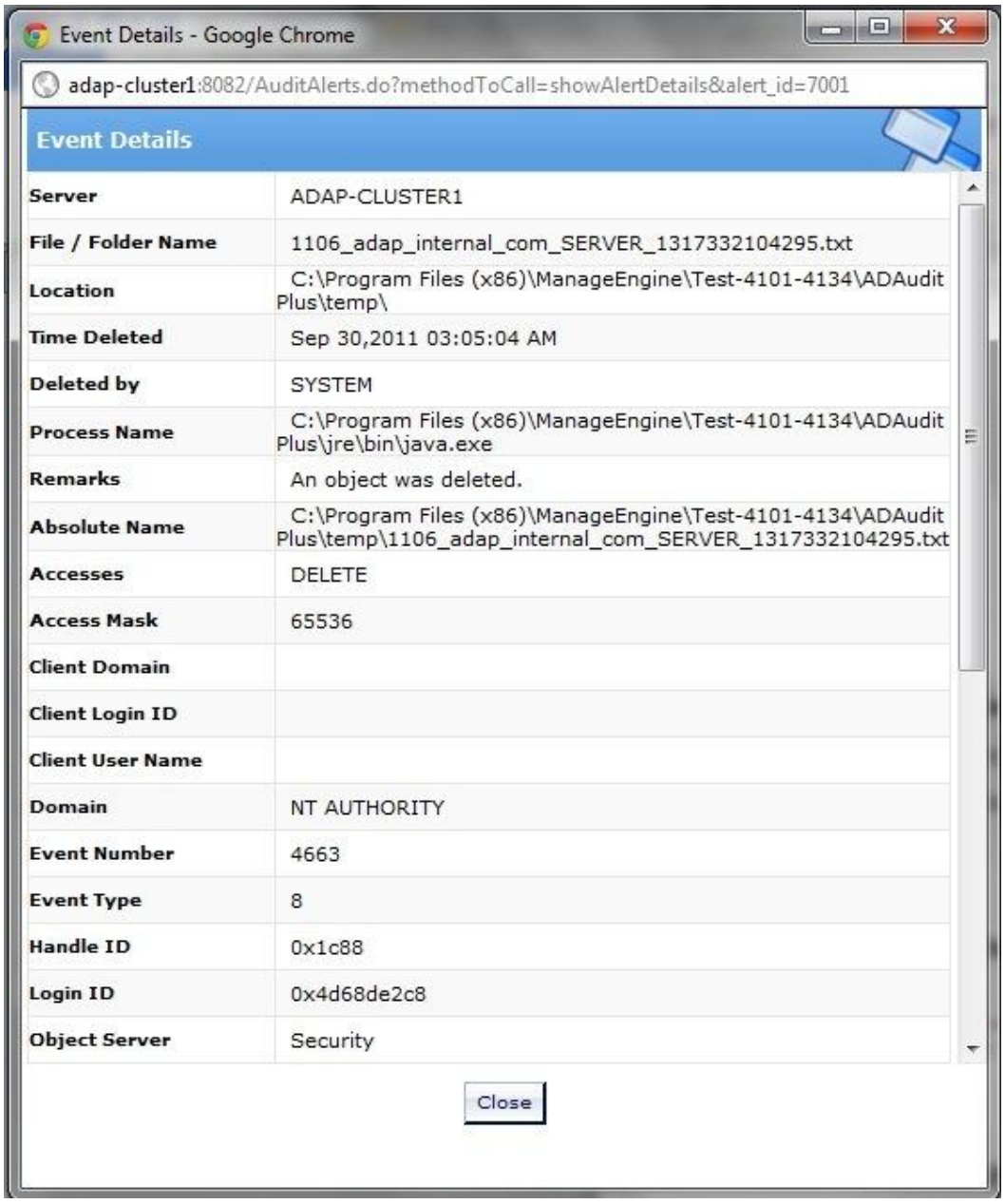
1. Click on 'Alerts' tab.
2. Select New Alert Profile option on the top-right.
3. Enter event identification details (name, description).
4. Select the Severity from the available- Attention, Trouble, Critical.
5. Choose the Report Profiles or create a new one at ease.
6. Choose Email Notification for instant email alerts.
7. Configure mail server with a few clicks.
8. Click on Save.



Create New Alert Profile screen

Critical ADAudit Plus Alert Features

Source, Domain, Severity, Alert Message; Click on an Alert to get the comprehensive details of the authorized / unauthorized event.



Comprehensive Event Details responsible for the Alert

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain

Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

User Object Change Auditing

Customer Use Case:

To know when a user is set with "Password never expires"

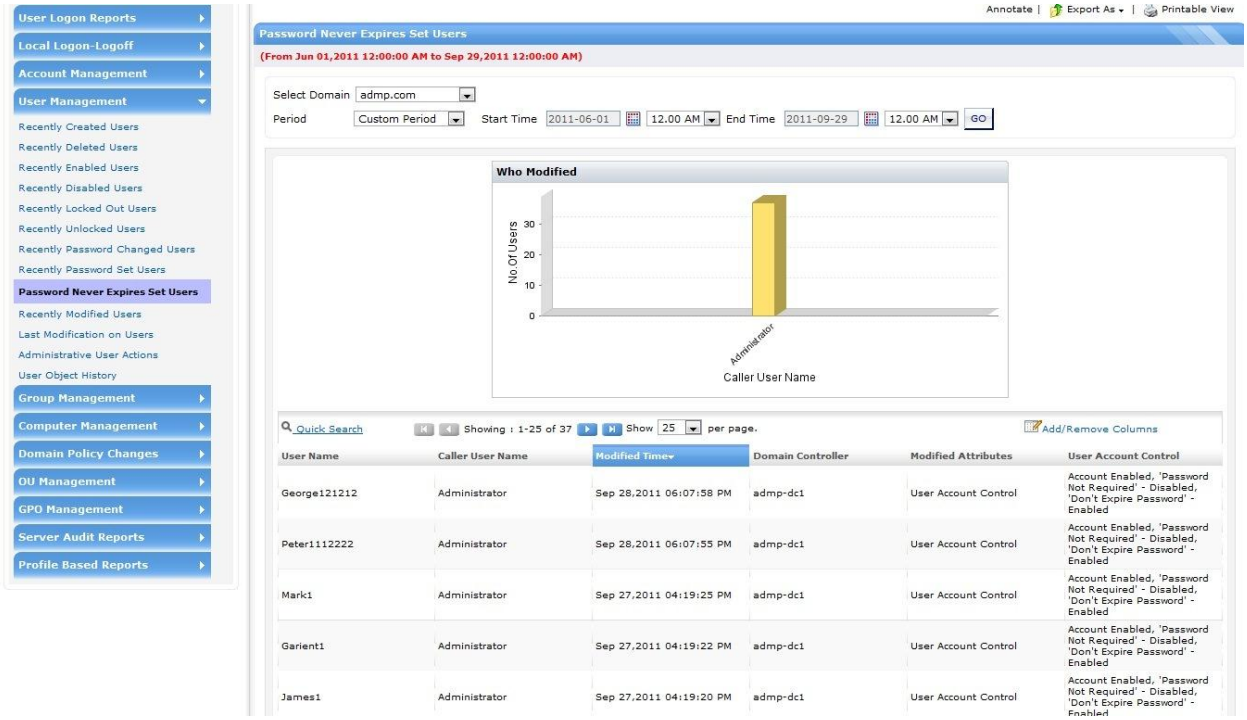
In an organization there are a mix of 'Periodic Password Change users' and 'Password never expires', the differentiating factor between the two being 'Security'.

Note: A secure Active Directory password policy demands users to change their passwords on a periodic basis. This is with a motive to ensure security of user logins and prevent attacks by any intruder.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'User Management' Report Category from the Available list.
3. Select 'Password Never Expires Set Users' Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.



Report listing the Password Never Expires Set Users

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Caller User Name, Modified Time, Domain Controller, Modified Attributes, User Account Control, Client IP Name, Client Host Name, Domain Controller, Logon Hours, SAM Account Name, SID, Logon Service, Event Type, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Group Object Change Auditing

Customer Use Case:

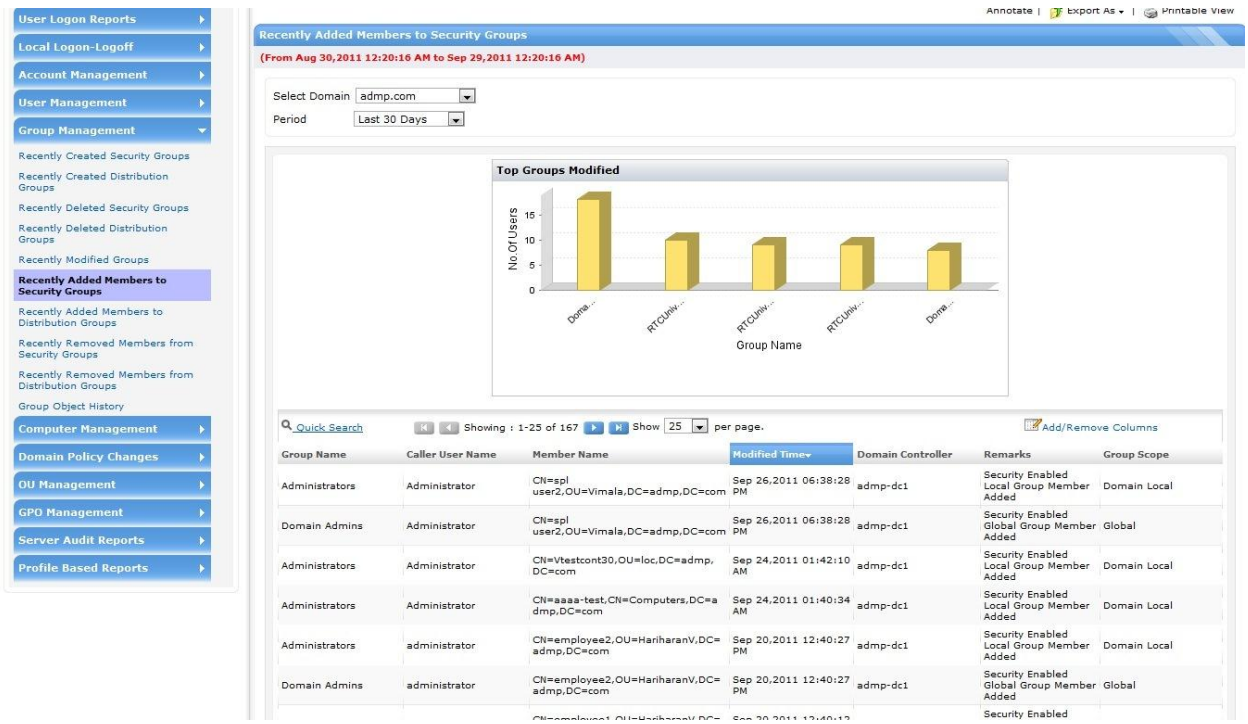
Need to show when a user is added/removed from a security group.

'Security to user, computers and other objects', in an organization is implemented with the help of Security groups where the appropriate permissions to specific resources (such as file shares and printers) are specified. A simple user addition / deletion in the crucial security groups can be with many privileges.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'Group Management' Report Category from the Available list.
3. Select 'Recently Added Members to Security Groups' Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.



Report listing the Recently Added Members to Security Groups

Critical ADAudit Plus Reporting Features

Detailed reports based on Group Name, Member Name, Group Scope, Privileges, Caller User Domain, SAM Account Name, Modification Type, Caller Logon ID, Old Group Name, SID History, SID, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Computer Object Change Auditing

Customer Use Case:

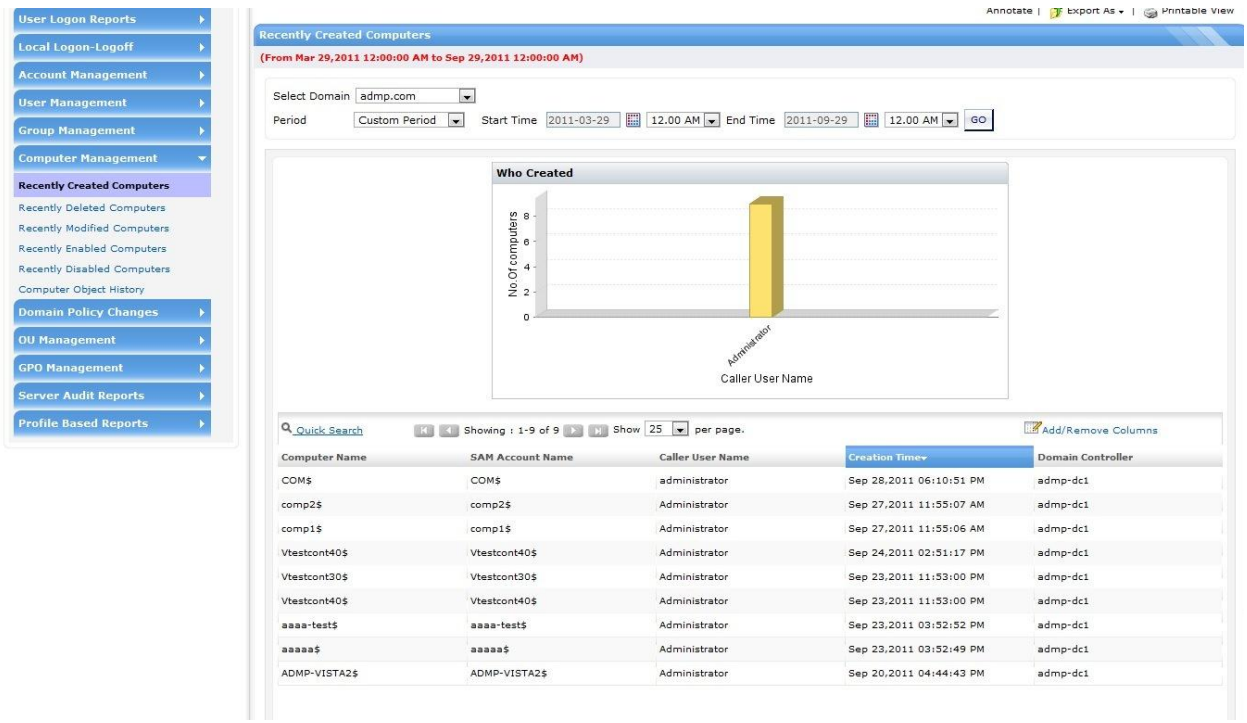
Every day we add few computers and we want to maintain the data for at least 6 months.

Like user accounts, computer accounts provide a means for authenticating and auditing the computer's access to the network and its access to critical domain resources. Auditing and keeping a tab on the 'access resources' plays a vital role in curtailing unauthorized access and in forensics.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'Computer Management' Report Category from the Available list.
3. Select 'Recently Created Computers' Report.
4. Select the Domain.
5. Select the Period. Custom Period (6 months) can also be selected.



Report listing the Recently Created Computers, Period Selected is 6 months

Critical ADAudit Plus Reporting Features

Detailed reports based on Group Name, Member Name, Group Scope, Privileges, Caller User Domain, SAM Account Name, Modification Type, Caller Logon ID, Old Group Name, SID History, SID, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Organizational Unit Change Auditing

Customer Use Case:

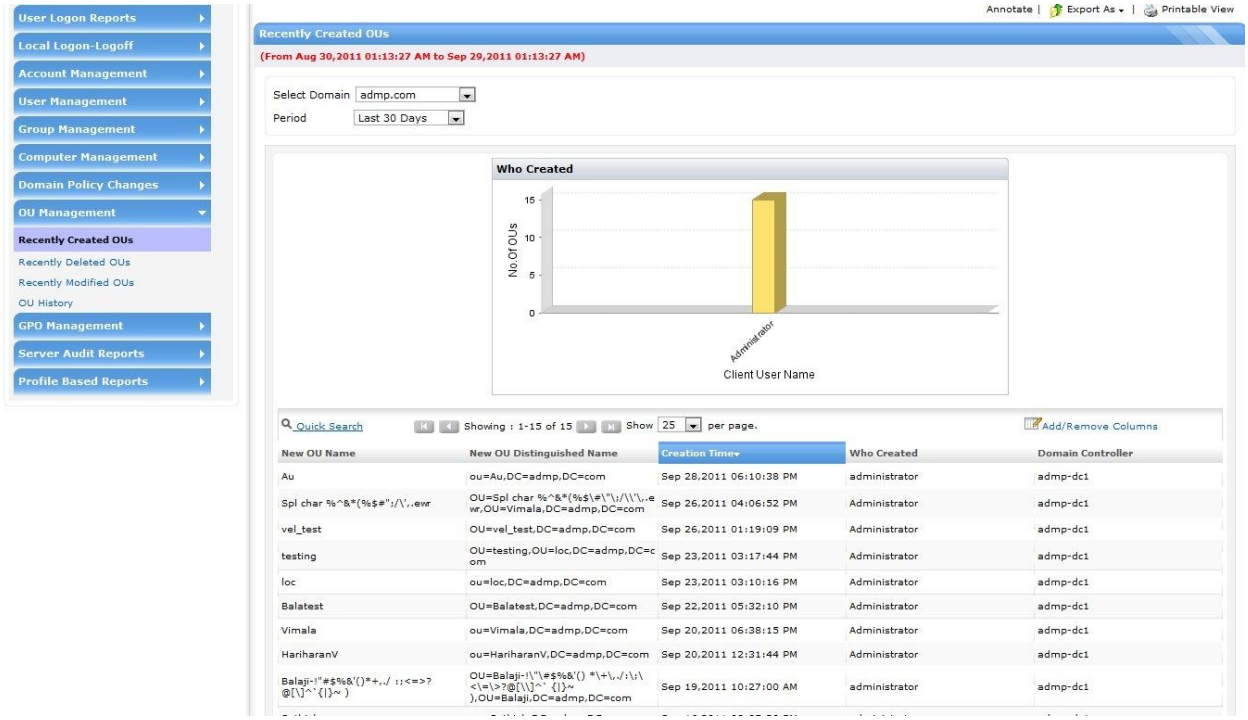
Need to know what are all the OU's added recently in the domain and get a report for the last one month.

Auditing the organizational units, the smallest scope or unit to which Group Policy settings can be assigned or to delegate administrative authority. Know when an OU was Created / Modified / Deleted. The History of OU Changes can be viewed in a single report.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'OU Management' Report Category from the Available list.
3. Select 'Recently Created OUs' Report.
4. Select the Domain.
5. Select the Period. Custom Period (Last 30 Days) can also be selected.



Report listing the Recently Created OUs, Period Selected is Last 30 Days

Critical ADAudit Plus Reporting Features

Detailed reports based on New OU Name, New OU Distinguished Name, Creation Time, Who Created, Domain Controller, Parent Object, Primary User Name, Primary Domain, Event Type, Client Domain, Caller User SID, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Group Policy Object Change Auditing

Customer Use Case:

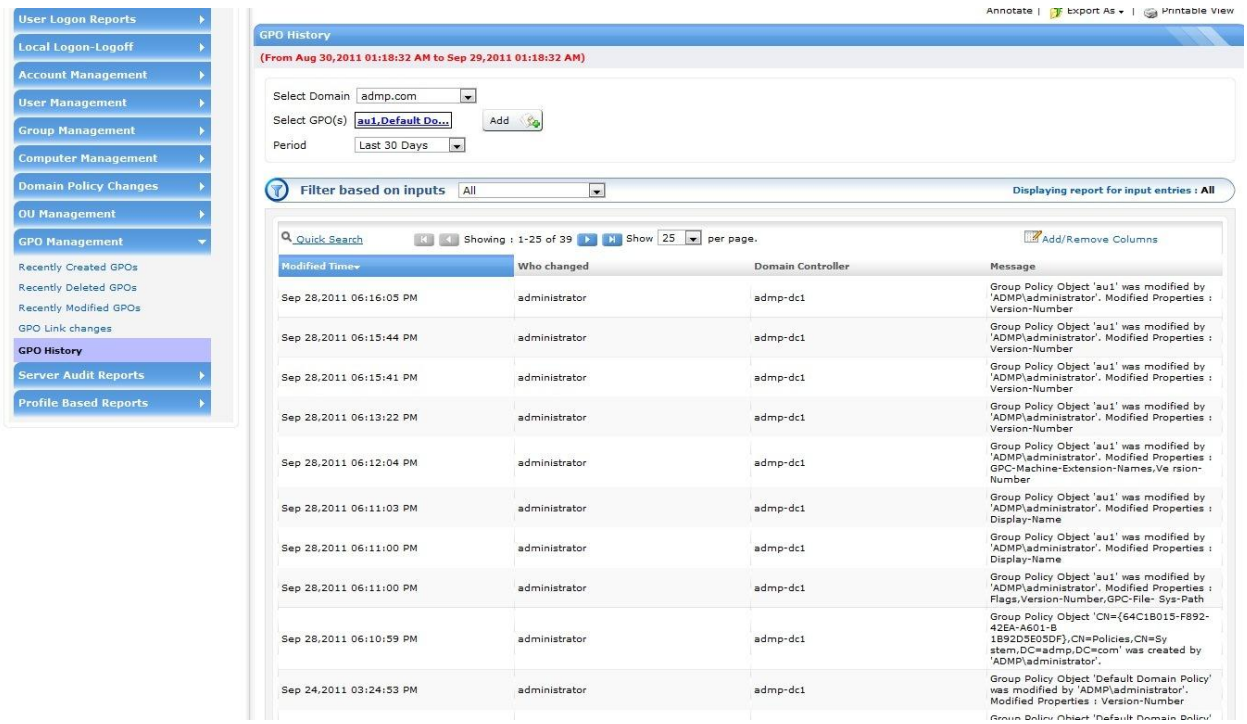
I have already set a GPO for desktop customizations on all servers in the domain and would like to generate a report on frequent changes especially " who" did and " When" .

Group Policy Objects comprises of top most critical 'Group policies' of user or computer settings for an entire group of users or computers. Further, associated with Active Directory objects such as sites, domains, or organizational units. Auditing this complex setup is indeed very simple with ADAudit Plus.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'GPO Management' Report Category from the Available list.
3. Select 'GPO History' Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.



Report listing the GPO History Events

The GPO History events are presented as refined data for a descriptive format to ease in auditing who-did-what-from-where along with many filter options to help single-out the user in question. Each event is an audit action on the server.

Critical ADAudit Plus Reporting Features

Detailed reports based on Object Name, Modified Attributes, Modified Time, Who Changed, Domain Controller, Message, Caller User SID, Accesses, Primary User Name, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

Domain Policy Change Auditing

Customer Use Case:

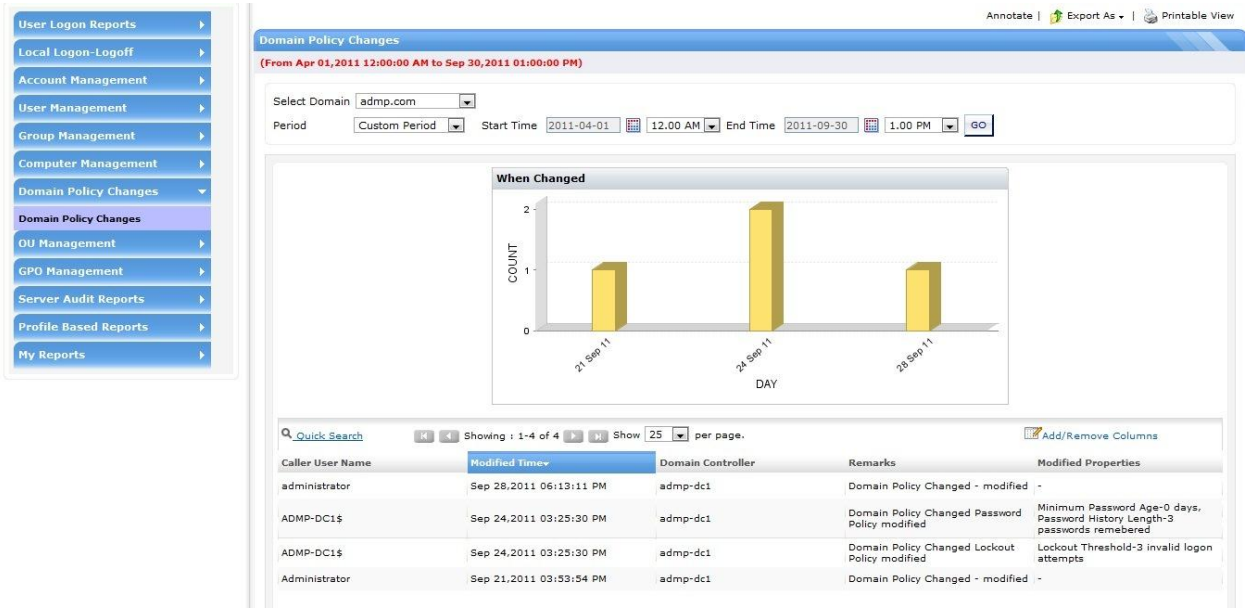
My account got locked out yesterday due to invalid logon attempt but I know that it was just 2 attempts, however I came to know later that someone had changed the domain policy, I want to find out who.

Domain Policy Changes holds the Domain-wide Security settings for handling authentication and authorization of Active Directory security principals and helps streamline the user, computers settings. The main policies under a domain policy are Password Policy, Account Lockout Policy an Kerberos Policy. Domain policy is applied to all security principal accounts in the domain, unless inheritance is specifically blocked or overridden by another policy.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'Domain Policy Changes' Report Category from the Available list.
3. Select 'Domain Policy Changes' Report.
4. Select the Domain.
5. Select the Period. Custom Period can also be selected.



Report listing the Domain Policy Changes

A bar graph is displayed. Each bar denotes an audit action on the server. The size of the bar shows the number of events. Click on the bar graph to filter and view desired audit change on the Domain Controller.

Critical ADAudit Plus Reporting Features

Detailed reports based on Caller User Name, Modified Time, Remarks, Modified Properties, Domain, Privileges, Lockout Threshold, Machine Account Quota, Password Property, Minimum Password Length, Quick Search (Filter based) and many more…

Other Active Directory Auditing Reports (A few from the 150+ Reports)

Logon Duration | Logon Failures | Recently Deleted Security Groups | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | Account Management (User, OU, Group, GPO, Computer) | User Object History | Domain Policy Changes | GPO Link Changes | Logon Activity | Recent User Logon Activity | Last Logon on Workstations | User's Last Logon | Users logged into multiple computers

File Server Auditing with ADAudit Plus

Customer Use Case:

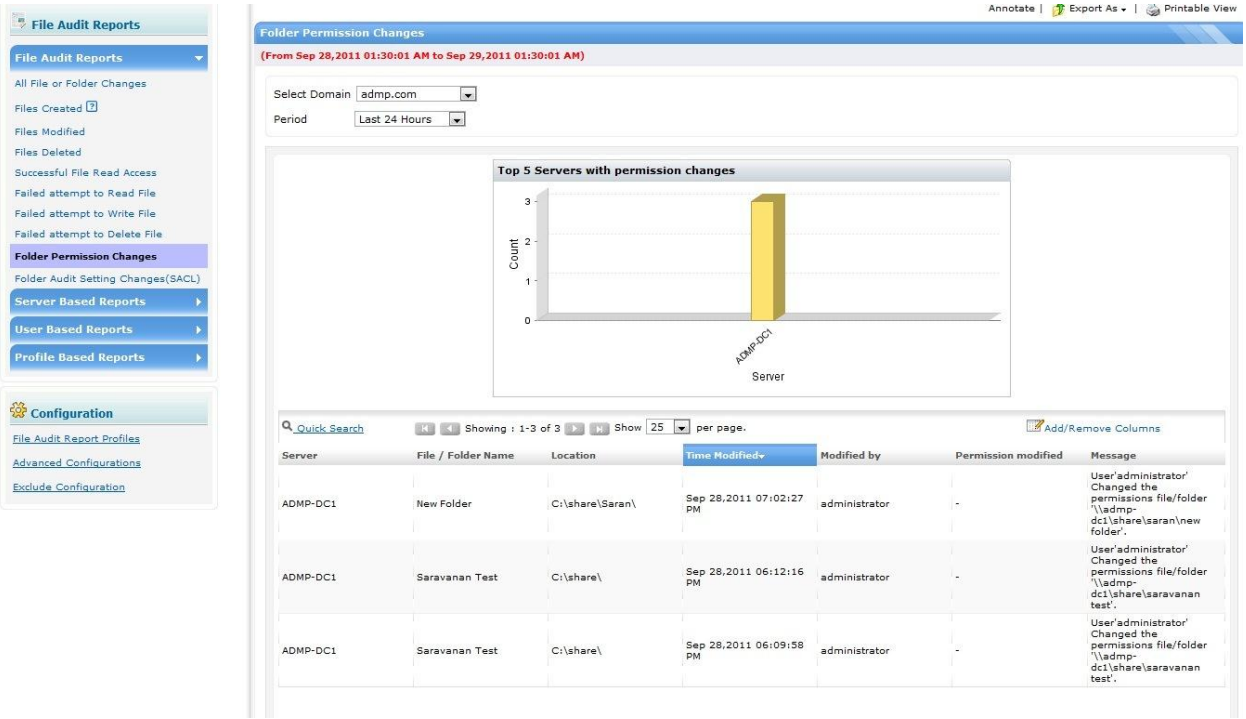
Have to configure a report of share permission changes on folders and sub folders.

In Real-Time, centrally Track-Audit-Secure the business-critical File Servers in a Windows Server Environment! Securely track the authorized / unauthorized access, changes to the documents in their files and folder structure, shares and permissions. This Report sheds light on the permission changes.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "File Audit" tab.
2. Select ‘Folder Permission Changes’ Report.
3. Select the Domain.
4. Select the Period. Custom Period can also be selected.



Report listing the File Server Folder Permission Changes

A bar graph is displayed. Each bar denotes an audit action on the server. The size of the bar shows the number of events. Click on the bar graph to filter and view desired audit change on the Domain Controller.

Critical ADAudit Plus Reporting Features

Detailed reports based on Caller User Name, Modified Time, Remarks, Modified Properties, Domain, Privileges, Lockout Threshold, Machine Account Quota, Password Property, Minimum Password Length, Quick Search (Filter based) and many more…

Other File Server Reports (File Audit | Server Based | User Based | Profile Based)

All File or Folder Changes | Files Created | Files Modified | Files Deleted | Successful File Read Access | Failed attempt to Read File | Failed attempt to Write File | Failed attempt to Delete File | Folder Permission Changes | Folder Audit Setting Changes (SACL)

Member Server Auditing with ADAudit Plus

Customer Use Case:

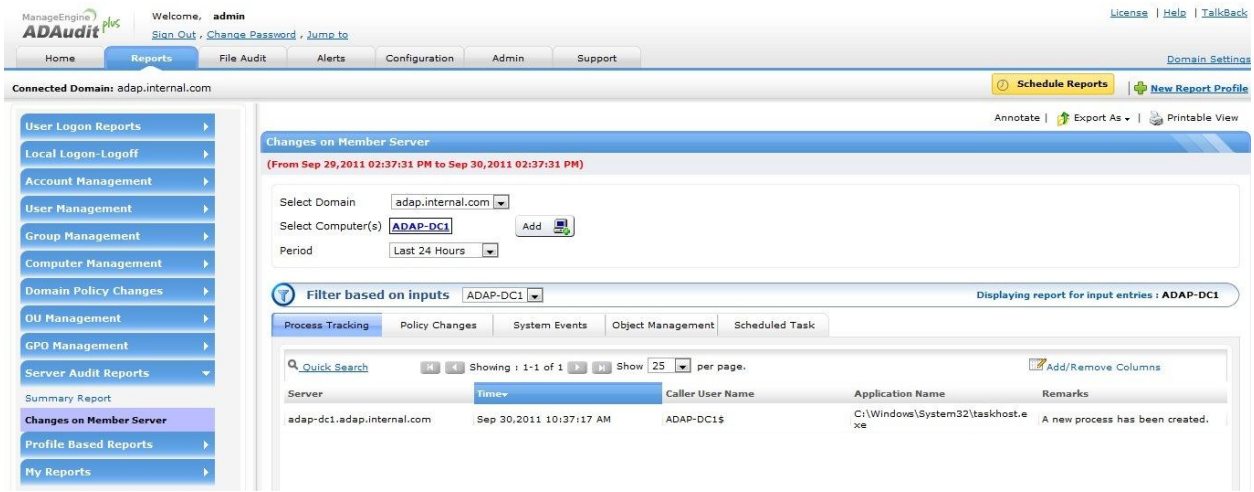
Is there a way to a get report on process tracking on a particular server for a particular time.

It is important to secure the member servers by diligently tracking server logons. This commands for a setting that is not only secure internally but also audits every 'event' logged in to the security log of Member Servers and reports them as and when in demand. Now an administrator can audit much more on a Member Server.

Steps to generate the Reports

Assuming ADAudit Plus Server is running, we will proceed:

1. Click on "Reports" tab.
2. Select the 'Server Audit' Report Category from the Available list.
3. Select 'Changes on Member Server' Report.
4. Select the Domain and Computer(s).
5. Select the Period. Custom Period can also be selected.



Report listing the categorized Summary of Member Server Changes

A bar graph is displayed. Each bar denotes an audit action on the server. The size of the bar shows the number of events. Click on the bar graph to filter and view desired audit change on the Domain Controller.

Critical ADAudit Plus Reporting Features

Detailed reports based on User Name, Logon Process Name, Server, Time, Remarks, Logon ID, File Name, SAM Account Name, Home Directory, Home Drive, Script Path, Caller User SID, Rights Value, Quick Search (Filter based) and many more…

Other Member Server Reports

Logon/Logoff | Logon Duration | Logon History | Terminal Services Activity | Schedule Tasks Activity | System Changes - Start/Stop/Audit Log cleared | Process Tracking on Servers | Policy Changes | Object Management | Summary Report