

ManageEngine ADAudit Plus
Workbook

Table of Contents

Table of Contents	1
Active Directory Auditing with ADAudit Plus	2
Logon Auditing with ADAudit Plus	3
Need to capture who logged in recently on which computer in the domain using terminal services.	3
Have to check whether any user tried logging in to the computers they don't have permissions.	5
What if any one logged into multiple computers at a time.	7
I want to see a report on failure logins for a particular Group.	9
User Object Change Auditing	12
Report when Administrator's password is changed.	12
To know when a user is set with "Password never expires"	16
Group Object Change Auditing	18
Need to show when a user is added/removed from a security group.	18
Computer Object Change Auditing	20
Every day we add few computers and we want to maintain the data for at least 6 months.	20
Organizational Unit Change Auditing	22
Need to know what are all the OU's added recently in the domain and get a report for the last one month.	22
Group Policy Object Change Auditing	24
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" .	24
Domain Policy Change Auditing	26
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.	26
File Server Auditing with ADAudit Plus	28
Have to configure a report of share permission changes on folders and sub folders.	28
Member Server Auditing with ADAudit Plus	30
Is there a way to a get report on process tracking on a particular server for a particular time.	30

Active Directory Auditing with ADAudit Plus

Address the most-needed security, audit and compliance demands; arm yourself with easily comprehensible 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.

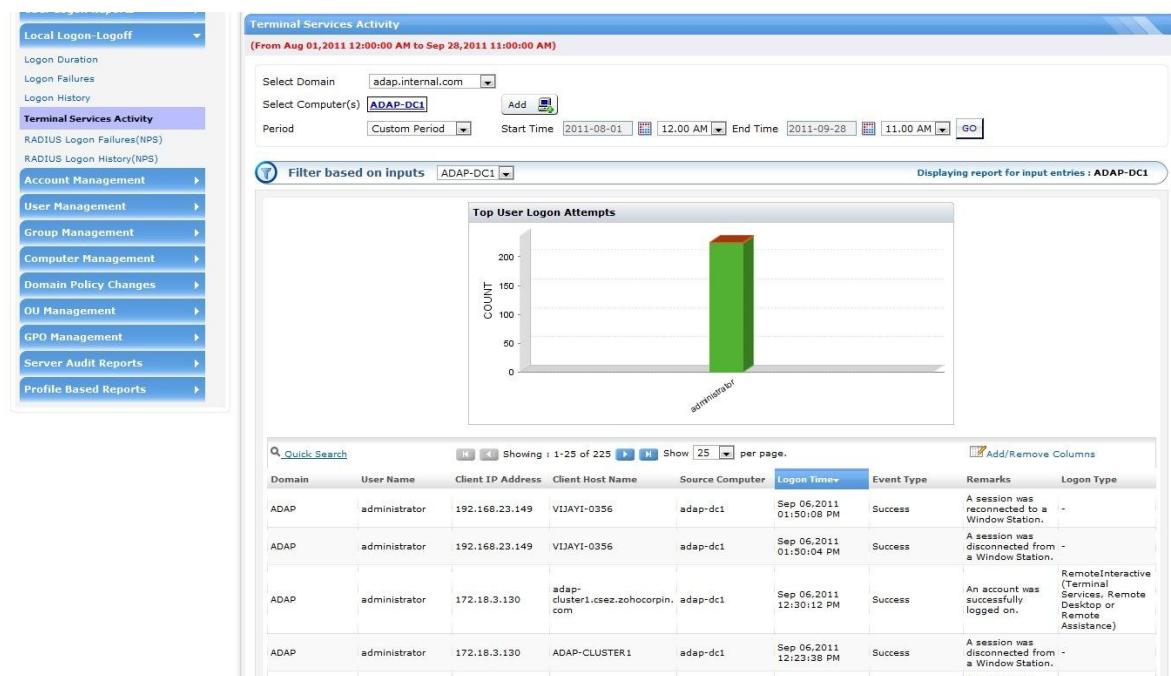
- Track users Logon / Logoff, GPO, OU and Audit User Management Actions.
- Delegate User Management Tasks to Support Staff
- View **user object life cycle changes** - creation, modification and deletion of a user object.
- **Admin** can assign helpdesk tasks to track and monitor account changes in the 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

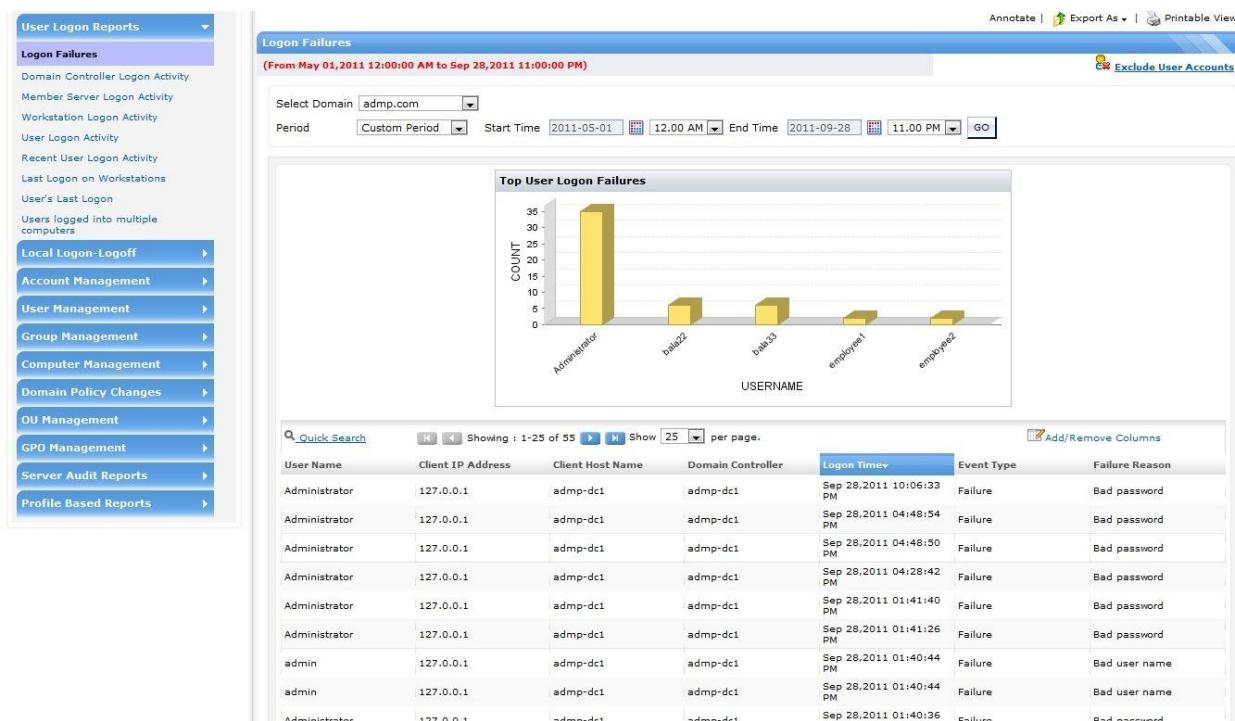
Logon Duration | Logon Failures | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | **Terminal Services Activity** | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on 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 occurred, 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

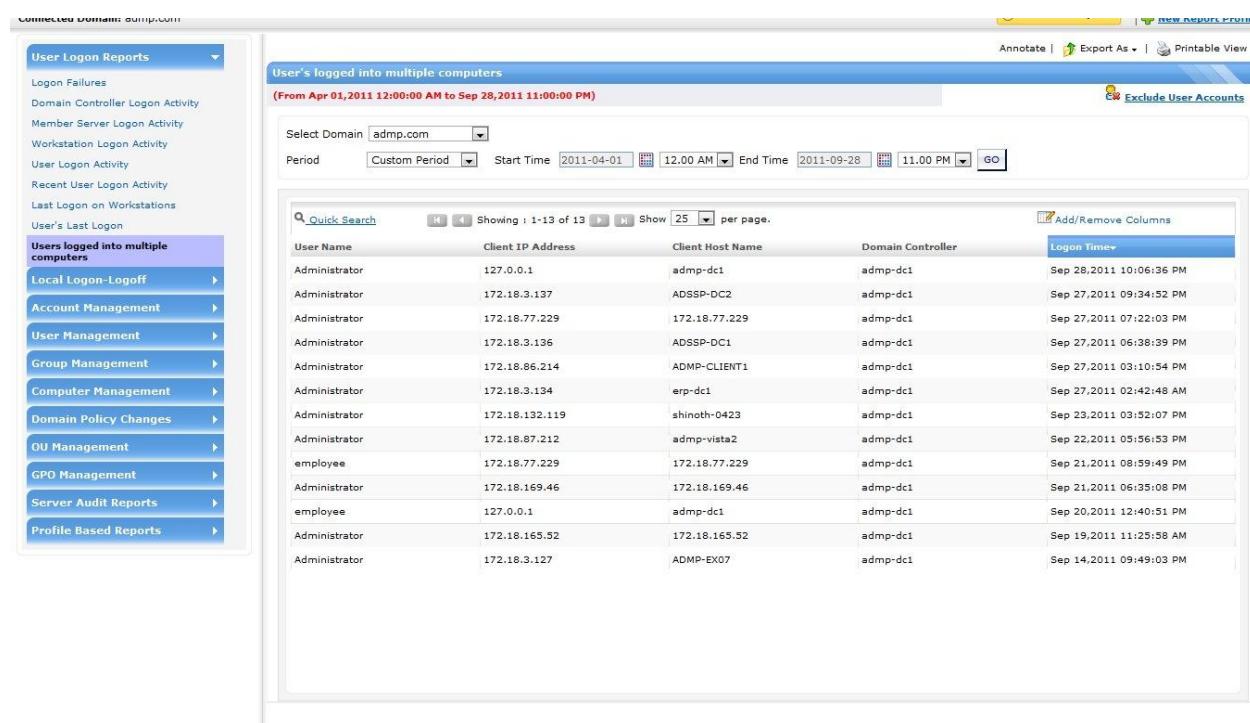
Logon Duration | **Logon Failures** | Logon History | RADIUS Logon Failures (NPS) | RADIUS Logon History (NPS) | Terminal Services Activity | Domain Controller Logon Activity | Member Server Logon Activity | Workstation Logon Activity | User Logon Activity | Recent User Logon Activity | Last Logon on 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.



The screenshot shows the ADAudit Plus interface for User Logon Reports. The left sidebar has a tree view with 'User Logon Reports' expanded, showing 'Logon Failures', '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', and 'Users logged into multiple computers' (which is selected and highlighted in purple). The main content area has a title 'User's logged into multiple computers (From Apr 01, 2011 12:00:00 AM to Sep 28, 2011 11:00:00 PM)'. It includes filter options for 'Select Domain' (admp.com), 'Period' (Custom Period, Start Time: 2011-04-01, End Time: 2011-09-28, 12:00 AM to 11:00 PM), and a 'GO' button. Below these is a table with columns: User Name, Client IP Address, Client Host Name, Domain Controller, and Logon Time. The table lists 13 entries for users like Administrator and employee from various IP addresses and hosts, with logon times ranging from Sep 14, 2011 to Sep 28, 2011.

User Name	Client IP Address	Client Host Name	Domain Controller	Logon Time
Administrator	127.0.0.1	admp-dc1	admp-dc1	Sep 28, 2011 10:06:36 PM
Administrator	172.18.3.137	ADSSP-DC2	admp-dc1	Sep 27, 2011 09:34:52 PM
Administrator	172.18.77.229	172.18.77.229	admp-dc1	Sep 27, 2011 07:22:03 PM
Administrator	172.18.3.136	ADSSP-DC1	admp-dc1	Sep 27, 2011 03:38:39 PM
Administrator	172.18.86.214	ADMP-CLIENT1	admp-dc1	Sep 27, 2011 03:10:54 PM
Administrator	172.18.3.134	erp-dc1	admp-dc1	Sep 27, 2011 02:42:48 AM
Administrator	172.18.132.119	shinoth-0423	admp-dc1	Sep 23, 2011 03:52:07 PM
Administrator	172.18.87.212	admp-vista2	admp-dc1	Sep 22, 2011 05:56:53 PM
employee	172.18.77.229	172.18.77.229	admp-dc1	Sep 21, 2011 08:59:49 PM
Administrator	172.18.169.46	172.18.169.46	admp-dc1	Sep 21, 2011 06:35:08 PM
employee	127.0.0.1	admp-dc1	admp-dc1	Sep 20, 2011 12:40:51 PM
Administrator	172.18.165.52	172.18.165.52	admp-dc1	Sep 19, 2011 11:25:58 AM
Administrator	172.18.3.127	ADMP-EX07	admp-dc1	Sep 14, 2011 09:49:03 PM

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

Active Directory Auditing with ADAudit Plus

Connected Domain: adap.internal.com

New Report Profile

Report Profile Name: *

Description:

Category: Account Logon

Actions : Logon Failure Events

Associate Domain Objects

Domain :

Select Users :

Logon Success Events

Logon Failure Events

Logon Failure Events 2000 AD

Save Cancel

Simply choose from the Pre-listed report categories

Select User(s)

All Users | Group based Users | Organizational Unit based Users

Quick Find GO Refresh

Showing : 1-25 of 63 Show 25 per page.

<input type="checkbox"/>	Name	Canonical Name
<input type="checkbox"/>	Account Operators	admp.com/Builtin/Account Operators
<input checked="" type="checkbox"/>	Administrators	admp.com/Builtin/Administrators
<input type="checkbox"/>	Backup Operators	admp.com/Builtin/Backup Operators
<input type="checkbox"/>	Cert Publishers	admp.com/Users/Cert Publishers
<input type="checkbox"/>	check_distributiongroup_GAL	admp.com/Users/check_distributiongroup_GAL
<input type="checkbox"/>	Distributed COM Users	admp.com/Builtin/Distributed COM Users
<input type="checkbox"/>	DnsAdmins	admp.com/Users/DnsAdmins
<input type="checkbox"/>	DnsUpdateProxy	admp.com/Users/DnsUpdateProxy
<input type="checkbox"/>	Domain Admins	admp.com/Users/Domain Admins
<input type="checkbox"/>	Domain Computers	admp.com/Users/Domain Computers
<input type="checkbox"/>	Domain Controllers	admp.com/Users/Domain Controllers

OK Cancel

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  **New Report Profile** 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...

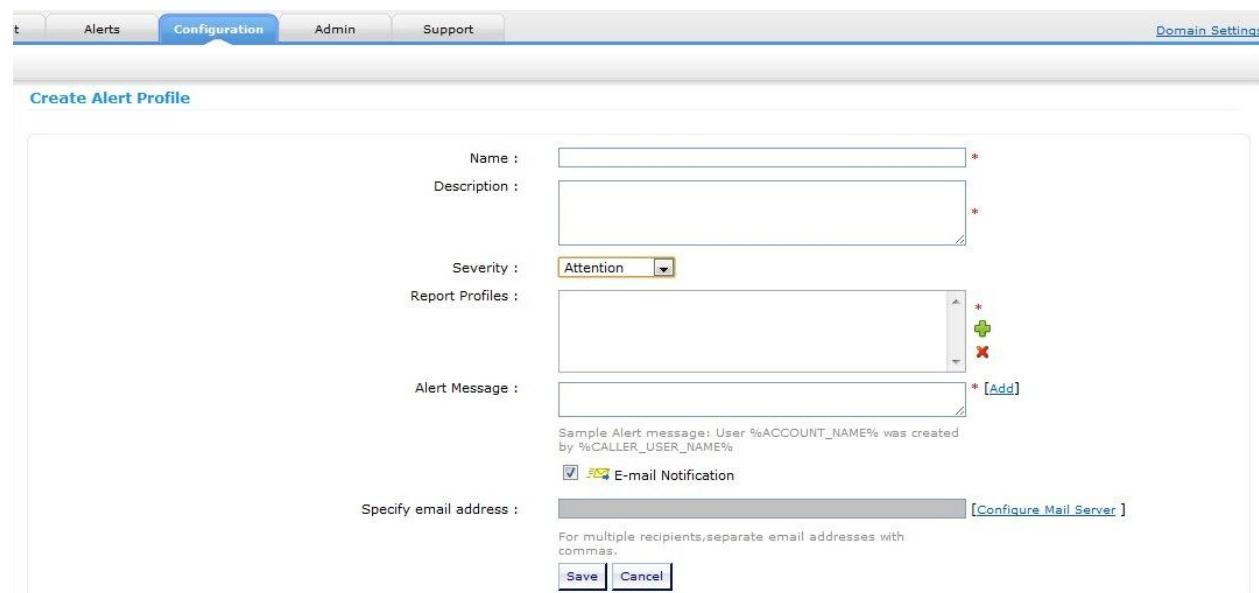
Alerts

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 Alert Profile

Name : *

Description : *

Severity :

Report Profiles :

Alert Message :
Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%
  E-mail Notification

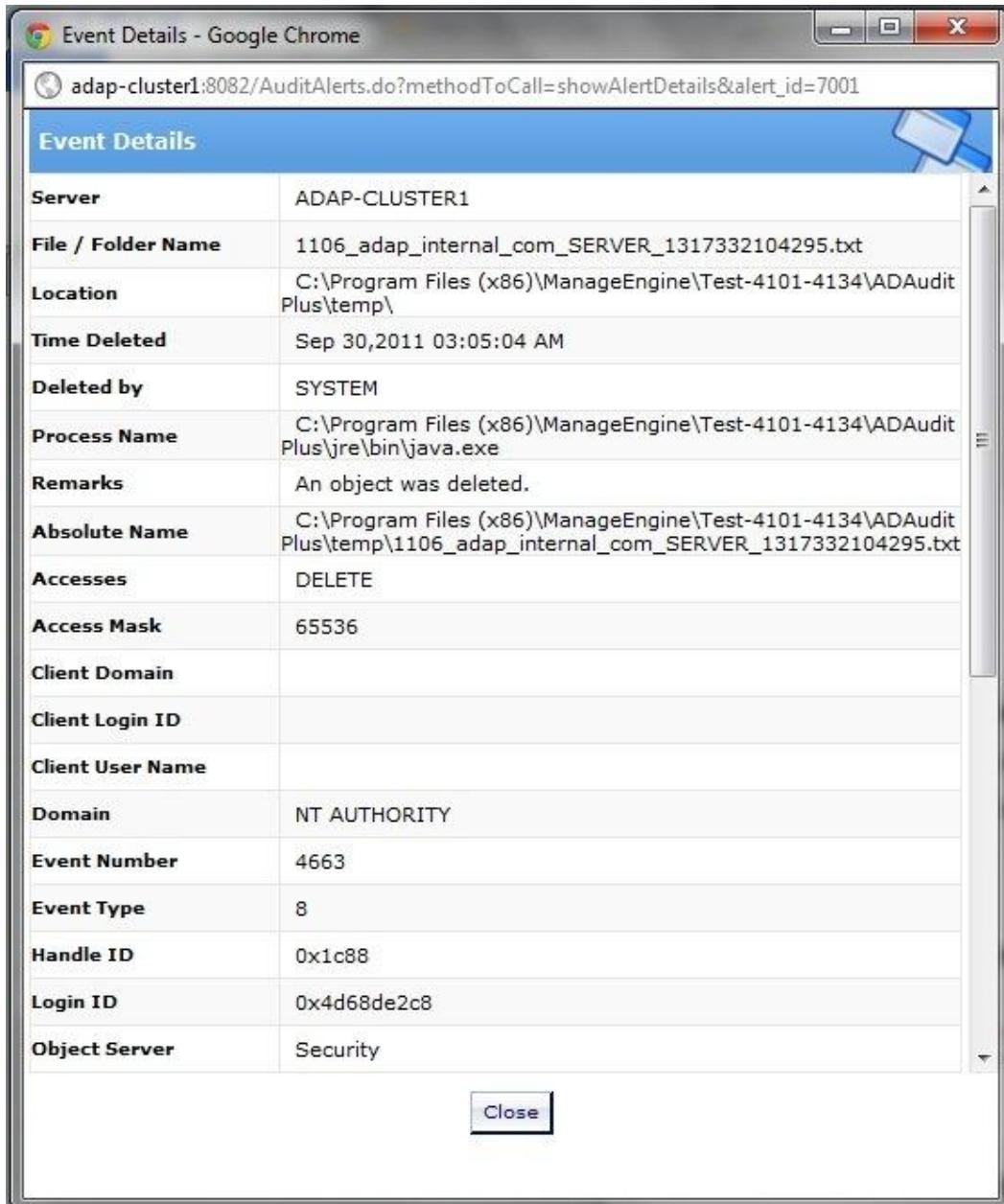
Specify email address : [Configure Mail Server](#)

For multiple recipients, separate email addresses with commas.

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.



The screenshot shows a Google Chrome window titled "Event Details - Google Chrome" with the URL "adap-cluster1:8082/AuditAlerts.do?methodToCall=showAlertDetails&alert_id=7001". The main content is a table titled "Event Details" with the following data:

Server	ADAP-CLUSTER1
File / Folder Name	1106_adap_internal_com_SERVER_1317332104295.txt
Location	C:\Program Files (x86)\ManageEngine\Test-4101-4134\ADAAudit Plus\temp\
Time Deleted	Sep 30, 2011 03:05:04 AM
Deleted by	SYSTEM
Process Name	C:\Program Files (x86)\ManageEngine\Test-4101-4134\ADAAudit Plus\jre\bin\java.exe
Remarks	An object was deleted.
Absolute Name	C:\Program Files (x86)\ManageEngine\Test-4101-4134\ADAAudit Plus\temp\1106_adap_internal_com_SERVER_1317332104295.txt
Accesses	DELETE
Access Mask	65536
Client Domain	
Client Login ID	
Client User Name	
Domain	NT AUTHORITY
Event Number	4663
Event Type	8
Handle ID	0x1c88
Login ID	0x4d68de2c8
Object Server	Security

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.

Active Directory Auditing with ADAudit Plus

Report listing the Password Never Expires Set Users

User Name	Caller User Name	Modified Time	Domain Controller	Modified Attributes	User Account Control
George121212	Administrator	Sep 28,2011 06:07:58 PM	admp-dc1	User Account Control	Account Enabled, 'Password Not Required' - Disabled, 'Don't Expire Password' - Enabled
Peter1112222	Administrator	Sep 28,2011 06:07:55 PM	admp-dc1	User Account Control	Account Enabled, 'Password Not Required' - Disabled, 'Don't Expire Password' - Enabled
Mark1	Administrator	Sep 27,2011 04:19:25 PM	admp-dc1	User Account Control	Account Enabled, 'Password Not Required' - Disabled, 'Don't Expire Password' - Enabled
Garient1	Administrator	Sep 27,2011 04:19:22 PM	admp-dc1	User Account Control	Account Enabled, 'Password Not Required' - Disabled, 'Don't Expire Password' - Enabled
James1	Administrator	Sep 27,2011 04:19:20 PM	admp-dc1	User Account Control	Account Enabled, 'Password Not Required' - Disabled, 'Don't Expire Password' - Enabled

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.

Active Directory Auditing with ADAudit Plus

Recently Added Members to Security Groups
(From Aug 30, 2011 12:20:16 AM to Sep 29, 2011 12:20:16 AM)

Select Domain: admp.com | Period: Last 30 Days

Top Groups Modified

Group Name	No of Users
Domain	18
RTGUniv	10
RTGUniv	10
RTGUniv	10
Domain	8

Group Name	Caller User Name	Member Name	Modified Time	Domain Controller	Remarks	Group Scope
Administrators	Administrator	CN=spluser2,OU=Vimalsa,DC=admp,DC=com	Sep 26, 2011 06:38:28 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Domain Admins	Administrator	CN=spluser2,OU=Vimalsa,DC=admp,DC=com	Sep 26, 2011 06:38:28 PM	admp-dc1	Security Enabled Global Group Member Added	Global
Administrators	Administrator	CN=vtestcont30,OU=loc,DC=admp,DC=com	Sep 24, 2011 01:42:10 AM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Administrators	Administrator	CN=aaaa-test,CN=Computers,DC=aadmp,DC=com	Sep 24, 2011 01:40:34 AM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Administrators	administrator	CN=employee2,OU=HarisharanV,DC=admp,DC=com	Sep 20, 2011 12:40:27 PM	admp-dc1	Security Enabled Local Group Member Added	Domain Local
Domain Admins	administrator	CN=employee2,OU=HarisharanV,DC=admp,DC=com	Sep 20, 2011 12:40:27 PM	admp-dc1	Security Enabled Global Group Member Added	Global
		CN=employee2,OU=HarisharanV,DC=admp,DC=com	Sep 20, 2011 12:40:19		Security Enabled	

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.

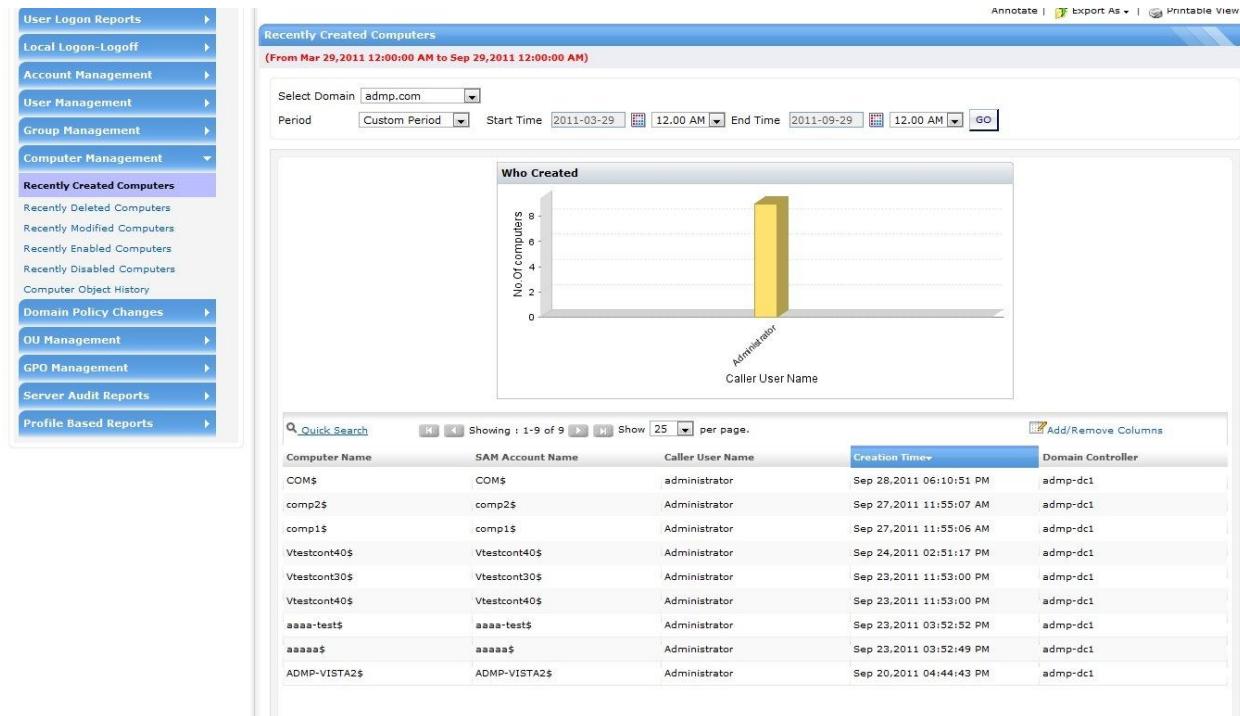
Like user accounts, computer accounts provide a means for authenticating and auditing the computer's access to the network and its access to critical domain resources. Auditing and keeping a tab on the 'access resources' plays a vital role in curtailing unauthorized access and in forensics.

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.

Active Directory Auditing with ADAudit Plus



Recently Created Computers
(From Mar 29, 2011 12:00:00 AM to Sep 29, 2011 12:00:00 AM)

Select Domain: admp.com | Period: Custom Period | Start Time: 2011-03-29 | 12:00 AM | End Time: 2011-09-29 | 12:00 AM | GO

Who Created

Caller User Name	No Of Computers
Administrator	8

Quick Search | Show: 1-9 of 9 | Show: 25 per page. | Add/Remove Columns

Computer Name	SAM Account Name	Caller User Name	Creation Time	Domain Controller
COM\$	COM\$	administrator	Sep 28, 2011 06:10:51 PM	admp-dc1
comp2\$	comp2\$	Administrator	Sep 27, 2011 11:55:07 AM	admp-dc1
comp1\$	comp1\$	Administrator	Sep 27, 2011 11:55:06 AM	admp-dc1
Vtestcont40\$	Vtestcont40\$	Administrator	Sep 24, 2011 02:51:17 PM	admp-dc1
Vtestcont30\$	Vtestcont30\$	Administrator	Sep 23, 2011 11:53:00 PM	admp-dc1
Vtestcont40\$	Vtestcont40\$	Administrator	Sep 23, 2011 11:53:00 PM	admp-dc1
aaaa-test\$	aaaa-test\$	Administrator	Sep 23, 2011 03:52:52 PM	admp-dc1
aaaaa\$	aaaaa\$	Administrator	Sep 23, 2011 03:52:49 PM	admp-dc1
ADMP-VISTA2\$	ADMP-VISTA2\$	Administrator	Sep 20, 2011 04:44:43 PM	admp-dc1

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.

New OU Name	New OU Distinguished Name	Creation Time	Who Created	Domain Controller
Au	ou=Au,DC=admp,DC=com	Sep 26,2011 06:10:38 PM	administrator	admp-dc1
Spl char %^&(%\$#";/\',.ewr	OU=Spl char %^&(%\$#";/\',.ewr,OU=Vimala,DC=admp,DC=com	Sep 26,2011 04:06:52 PM	Administrator	admp-dc1
vel_test	OU=vel_test,DC=admp,DC=com	Sep 26,2011 01:19:09 PM	Administrator	admp-dc1
testing	OU=testing,OU=loc,DC=admp,DC=com	Sep 23,2011 03:17:44 PM	Administrator	admp-dc1
loc	ou=loc,DC=admp,DC=com	Sep 23,2011 03:10:16 PM	Administrator	admp-dc1
Balatest	OU=Balatest,DC=admp,DC=com	Sep 22,2011 05:32:10 PM	Administrator	admp-dc1
Vimala	ou=Vimala,DC=admp,DC=com	Sep 20,2011 06:38:15 PM	Administrator	admp-dc1
HarisharanV	ou=HarisharanV,DC=admp,DC=com	Sep 20,2011 12:31:44 PM	Administrator	admp-dc1
Balaji-!"#\$%&(')=+,./;:=>?@{}`~`{}`~`	OU=Balaji-!"#\$%&(')=+,./;:=>?@{}`~`{}`~`,OU=Balaji,DC=admp,DC=com	Sep 19,2011 10:27:00 AM	administrator	admp-dc1

 The chart has a single bar for 'Administrator' reaching the value of 15 on the y-axis.

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.

Modified Time	Who changed	Domain Controller	Message
Sep 28,2011 06:16:05 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : Version-Number
Sep 28,2011 06:15:44 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : Version-Number
Sep 28,2011 06:15:41 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : Version-Number
Sep 28,2011 06:13:22 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : Version-Number
Sep 28,2011 06:12:04 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : GPC-Machine-Extension-Names,Version-Number
Sep 28,2011 06:11:03 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : DisplayName
Sep 28,2011 06:11:00 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : DisplayName
Sep 28,2011 06:11:00 PM	administrator	admp-dc1	Group Policy Object 'au1' was modified by 'ADMP\Administrator'. Modified Properties : DisplayName,Version-Number,GP-File-Sys-Path
Sep 28,2011 06:10:59 PM	administrator	admp-dc1	Group Policy Object 'CN={64C1B015-F892-42EA-AE01-B1B92D5E93DF},CN=Policies,CN=System,DC=admp,DC=com' was created by 'ADMP\Administrator'.
Sep 24,2011 03:24:53 PM	administrator	admp-dc1	Group Policy Object 'Default Domain Policy' was modified by 'ADMP\Administrator'. Modified Properties : Version-Number

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.

Domain Policy Changes
(From Apr 01, 2011 12:00:00 AM to Sep 30, 2011 01:00:00 PM)

Select Domain: admp.com

Period: Custom Period | Start Time: 2011-04-01 | 12.00 AM | End Time: 2011-09-30 | 1.00 PM | GO

When Changed

DAY	COUNT
21 Sep 11	1
24 Sep 11	2
28 Sep 11	1

Report listing the Domain Policy Changes

Caller User Name	Modified Time	Domain Controller	Remarks	Modified Properties
administrator	Sep 28,2011 06:13:11 PM	admp-dc1	Domain Policy Changed - modified -	
ADMP-DC1\$	Sep 24,2011 03:25:30 PM	admp-dc1	Domain Policy Changed Password Policy modified	Minimum Password Age-0 days, Password History Length-3 passwords remembered
ADMP-DC1\$	Sep 24,2011 03:25:30 PM	admp-dc1	Domain Policy Changed Lockout Policy modified	Lockout Threshold-3 invalid logon attempts
Administrator	Sep 21,2011 03:53:54 PM	admp-dc1	Domain Policy Changed - modified -	

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.

Active Directory Auditing with ADAudit Plus

The screenshot shows the ADAudit Plus interface. On the left, a sidebar menu includes 'File Audit Reports' (selected), 'File Audit Reports' (dropdown), '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' (selected), 'Folder Audit Setting Changes(SACL)', 'Server Based Reports', 'User Based Reports', and 'Profile Based Reports'. Below this is a 'Configuration' section with 'File Audit Report Profiles', 'Advanced Configurations', and 'Exclude Configuration'. The main content area is titled 'Folder Permission Changes' (From Sep 28, 2011 01:30:01 AM to Sep 29, 2011 01:30:01 AM). It shows a bar chart titled 'Top 5 Servers with permission changes' with a single bar for 'ADMP-DC1' reaching a count of 3. Below the chart is a table with columns: Server, File / Folder Name, Location, Time Modified, Modified by, Permission modified, and Message. The table data is as follows:

Server	File / Folder Name	Location	Time Modified	Modified by	Permission modified	Message
ADMP-DC1	New Folder	C:\share\Saran\	Sep 28, 2011 07:02:27 PM	administrator	-	User 'administrator' Changed the permissions file/folder '\\admp- dc1\share\saran\new folder'.
ADMP-DC1	Saravanan Test	C:\share\	Sep 28, 2011 06:12:16 PM	administrator	-	User 'administrator' Changed the permissions file/folder '\\admp- dc1\share\saravanan test'.
ADMP-DC1	Saravanan Test	C:\share\	Sep 28, 2011 06:09:58 PM	administrator	-	User 'administrator' Changed the permissions file/folder '\\admp- dc1\share\saravanan test'.

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 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.

The screenshot shows the ADAudit Plus web interface. The left sidebar has a 'Reports' tab selected. Under 'Server Audit Reports', the 'Changes on Member Server' report is selected. The main content area shows a table with the following data:

Server	Time	Caller User Name	Application Name	Remarks
adap-dc1.adap.internal.com	Sep 30, 2011 10:37:17 AM	ADAP-DC1\$	C:\Windows\System32\taskhost.exe	A new process has been created.

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