ManageEngine
ADAudit Plus

ADAudit Plus快速使用指导

内容

介绍:

安装设置:

检查列表:

介绍

什么是ADAudit Plus ?

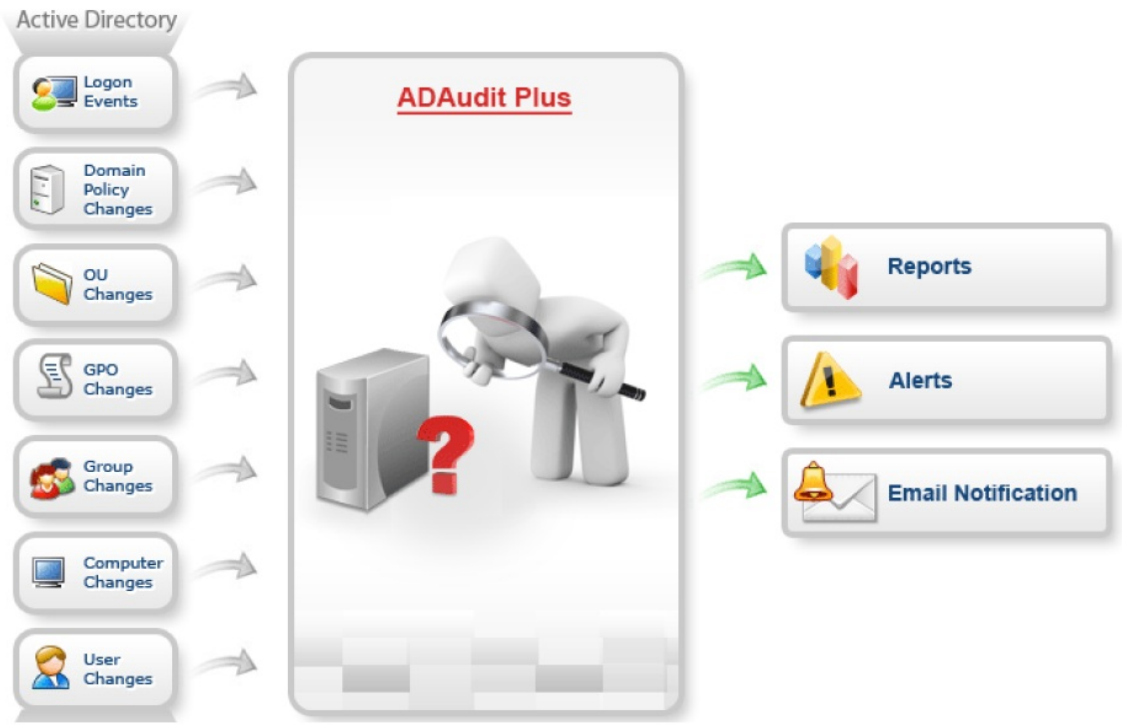
ADAudit Plus是一个企业范围的Active Directory和文件服务器变更审计软件，它提供报表和告警:

- 满足监管机构和政府机构提出的最需要的安全、审计和合规性要求。
- 为IT管理员提供正确的业务外接程序，以协助执行更改管理操作。

ADAuditPlus提供的解决方案是以综合报表和告警的形式提供的，即使是在技术上比较薄弱的用户也很容易理解。这些报表回答了Active Directory审核的四个关键W：“谁”执行了什么“操作”、“何时”和“从哪里”!

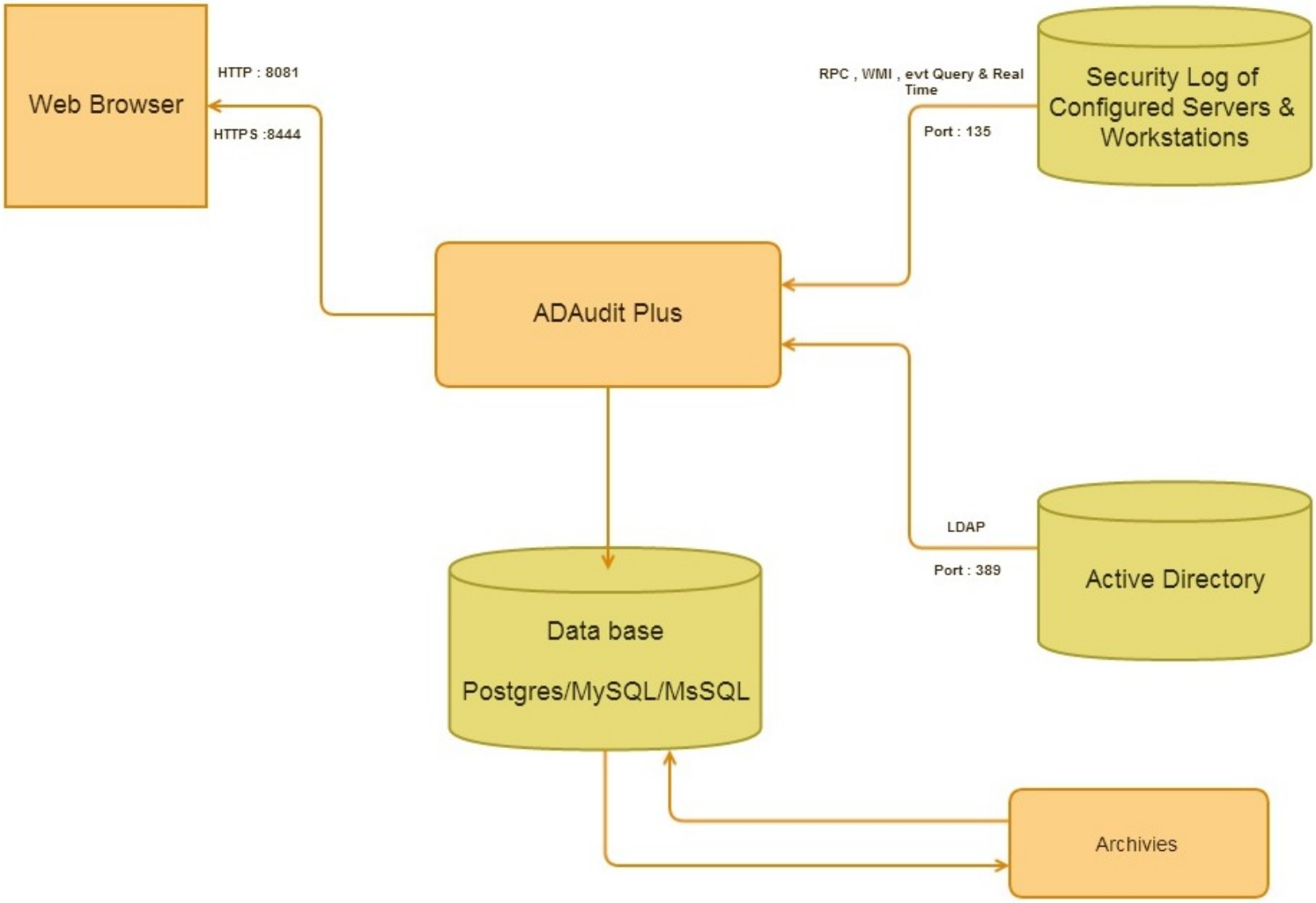
审计解决方案不仅显示与更改有关的数据，而且还允许将结果导出为XLS、html、pdf和csv格式，并提供打印列出的数据以协助解释的选项。

ADAudit Plus是如何工作的?



ADAuditPlus在本地审计的基础上工作。必须在域控制器和成员服务器上配置审核策略和SACL，才能启用审核。这可确保对Active Directory、登录活动所做的所有更改都记录在各自服务器的安全日志中。ADAuditPlus收集这些事件以报表更改。

ADAudit Plus的技术流程



安装设置

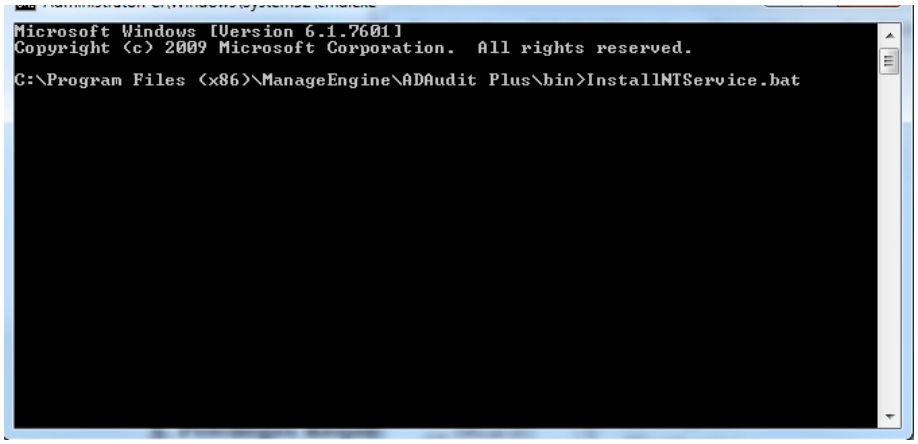
安装

ADAudit Plus以EXE格式发布。ADAuditPlus可以安装在域中具有指定系统要求的任何计算机上。ADAuditPlus可以安装在网络上的任何计算机上，也可以通过Web浏览器从网络上的任何客户端计算机上访问。

ADAudit Plus安装位Windows服务：

按照以下步骤以Windows服务运行**ADAudit Plus:**

- 停止ADAudit Plus(开始 -> 所有程序 -> ADAudit Plus -> 停止ADAudit Plus)
- 打开命令行(右键点击 --> 以管理员身份运行，如果是Windows server 2008)
- 进入<安装目录>\ADAudit Plus\bin [例如: C:\Program Files (x86)\ManageEngine\ADAudit Plus\bin]
- 执行"InstallNTService.bat"



- 打开services.msc -->"ManageEngine ADAudit Plus" Service --> 右键点击 --> 属性
- 点击"登录"标签，选择"此账户"并提供一个凭证(如果可以，请使用管理员账户)
- 启动ManageEngine ADAudit Plus

系统需求

硬件需求：

硬件	建议
处理器	**P4 - 1.5 GHz**或更高
RAM	**2 GB**或更高

磁盘大小	**20 GB**

注意: 数据库使用的额外磁盘空间将根据捕获的用户/文件和已审核事件的数量而有所不同。

软件需求：

支持的操作系统 - **ManageEngine ADAuditPlus**可在以下**Microsoft Windows**操作系统版本上安装和运行:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 2003 Server
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

支持的浏览器 - **ManageEngine ADAuditPlus**要求在系统中安装以下浏览器之一:

- Internet Explorer 6 and above
- Firefox 2.0 and above
- Chrome
- Preferred screen resolution 1024 x 768 pixels or higher

支持的平台:

- Active Directory 2003 and above
- Windows File Server 2003 and above
- NetApp Filer - Data ONTAP 7.2 and above
- Windows Failover Cluster with SAN

存储需求:

活动目录审计:

用户数量	天数	总大小
1	**1**	**15 KB**
10,000	**90**	**12*10000*90 = 13 GB**

文件服务器审计:

用户数量	文件数	天数	总大小
1	**1**	**1**	**4 KB**
100	**1**	**1**	**400 KB**
100	**100**	**1**	**40 MB**
100	**100**	**90**	**40000*90 = 3.5 GB**
100	**100**	**720 (2 Yrs)**	**40000*720 ~ 29 GB**

检查列表

需要打开的端口

事件收集的端口:

- 端口"389" - 与LDAP协议通讯
- 端口"135" - 与RPC通讯
- 端口"445"和"135" - 与NetBioS Session Service通讯

访问ADAudit Plus的端口:

- http :8081
- https :8444

配置审核策略

必须在任何Active Directory环境中配置审核策略; 这可确保将相关的审核数据记录到所需计算机/域控制器的安全日志中。ADAuditPlus只能为启用了审核策略的计算机收集和报表审核数据。

审核Active Directory

1. 默认域控策略必须配置。
2. 对象级别审核应该被启用。

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/manual-configuration-dc-auditing.html

http://www.manageengine.cn/products/active-directory-audit/help/reports/access-aduc-to-enable-audit-sacls.html

审核文件服务器

1. 必须为需要审核数据的特定文件服务器配置审核策略。
2. 对象基本审计必须启用

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/configure-object-access-auditing.html

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/linking-servers-to-gpo.html

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/sacls-to-audit-files-and-shares.html

审核成员服务器

必须为需要审核数据的特定成员服务器配置审核策略

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/configure-local-logon-auditing.html

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/configure-policy-member-server-auditing.html

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/linking-servers-to-gpo-ms.html

启用文件完整性监控[成员服务器]

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/fim-audit-policy.html

审核NetApp Filers

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/netapp-filer-manual-configuration.html

http://www.manageengine.cn/products/active-directory-audit/help/getting-started/sacls-to-audit-files-and-shares.html

2008 R2及以上域控制器和成员服务器的高级审核策略配置

域控审核	成员服务器审核	文件服务器审核	工作站审核
账户登录 * Kerberos 身份验证服务 账户管理 *计算机账户管理 *通讯组管理 *安全组管理 *用户账户管理 详细跟踪 *进程创建 *进程终止 **DS** 访问 *目录访问更改 *目录访问访问 登录/注销 *审核登录 *审核注销 *网络策略服务器 *其他登录/注销事件 对象访问 *其他对象访问事件	账户管理 *计算机账户管理 *通讯组管理 *安全组管理 *用户账户管理 详细跟踪 *进程创建 *进程终止 登录/注销 *审核登录 *审核注销 *网络策略服务器 *其他登录/注销事件 对象访问 *其他对象访问事件 策略更改 *身份验证测录更改 *授权策略更改 *审核策略更改 系统 *安全状态更改	登录/注销 *审核登录 *审核注销 *网络策略服务器 *其他登录/注销事件 对象访问 *文件系统 *句柄操作	登录/注销 *审核登录 *审核注销 *网络策略服务器 *其他登录/注销事件

策略更改 *身份验证策略更改 *授权策略更改 系统 *安全状态更改			

安全日志设置

ADAudit Plus定期从配置的服务器收集审核数据，并将信息存储在数据库中以供报表。为避免数据丢失，我S们建议使用以下事件日志设置。

服务器的操作系统	角色	安全日志大小**(Kb)**	安全日志保留
Windows Server 2003	域控	307200	按需覆盖日志
Windows Server 2008 及以上	域控	1048576	按需覆盖日志
Windows Server 2003	文件服务器	307200	按需覆盖日志
Windows Server 2008 及以上	文件服务器	4194304	按需覆盖日志
Windows Server 2003	成员服务器	307200	按需覆盖日志
Windows Server 2008 及以上	成员服务器	1048576	按需覆盖日志

使用ADAudit Plus的权限需求

ADAudit Plus需要某些权限才能从配置的服务器收集事件以报表更改。请单击以下链接，查找ADAuditPlus从配置的服务器收集审核数据所需权限的完整详细信息。

http://www.manageengine.com/products/active-directory-audit/audit-permissions-configuration-ad-audit-plus.html

ADAudit Plus 管理配置[管理标签]

告警:

“Alert Me”功能持续监控ADAuditPlus是否正在从配置的服务器的安全日志中收集事件日志数据。当ADAudit Plus停止收集事件日志数据时，它会向配置的电子邮件地址发送电子邮件告警。

该功能还监视安装ADAuditPlus的驱动器，并在可用空间低于设定阈值时发出告警。它还会在许可证到期时发出告警。

技术员/操作员:

组织的规模使单个管理员更难监视网络中发生的所有更改。需要将监控角色委派给域中的一个或多个用户，这可以使用ADAudit Plus中的技术人员委派功能有效地建立。

ADAudit Plus **允许委派两种不同的角色**:

1. 管理员角色：管理员角色将拥有ADAuditPlus设置和配置的完全权限。

2. 操作员角色：操作员角色将仅具有查看管理员配置的报表、告警和图形的权限。

除外用户账户:

服务帐户是一个Active Directory用户帐户，创建该帐户是为了为在Windows Server上运行的服务提供安全上下文。该帐户生成大量登录事件，反过来又消耗数据库中的大量空间，这些帐户发出的告警被证明是在浪费管理员的时间。

除外用户账户的步骤:

1. 点击管理标签
2. 选择管理中的"除外用户账户"
3. 选择域(“可用用户”中将会显示域中所有用户帐户的列表。)
4. 使用>>选项从可用用户列表中排除一个或多个用户。
5. 点击保存。

文件审核中的除外配置:

服务帐户是一个Active Directory用户帐户，创建该帐户是为了为在Windows Server上运行的服务提供安全上下文。该帐户生成大量登录事件，反过来又消耗数据库中的大量空间，这些帐户发出的告警被证明是在浪费管理员的时间。

从文件审核中除外指定的进程/用户/文件类型:

1. 点击文件审核标签
2. 选择配置中的“除外文件”
3. 指定进程/文件的名称，用逗号隔开
4. 点击保存

归档需求:

归档的需求不会随着合规性而停止。归档数据对于组织非常重要，以便:

- 协助Forensic分析和报表。
- 确保各种合规需求可能需要的审计数据安全、无变更。(SOX、HIPAA、GLBA等法规遵循要求，要求至少3年或更长时间的审计日志数据。)
- 分析Microsoft Windows Active Directory/File Server/Member Server未经授权的尝试，这些尝试导致内部安全漏洞，以及维护已建立的内部组织策略。
- 通过研究不同时期的资源利用模式来规划资源容量。隔离可疑用户(用户登录数据)，并使用他们的审计跟踪来证实他们参与了过去的任何安全攻击。

重新生成归档数据，ADAudit Plus的优势:

ADAudit Plus的优势在于，它可以帮助重新生成存档数据，包括:

- 允许在用户定义的位置归档审核数据，该位置可以是网络中任何位置的存储服务器。
- 帮助您仅归档所需的Active Directory更改数据，从而减少通常与次存储的本机方法相关的混乱。
- 对变更数据的各个日志进行编目降级，分组为多个压缩文件，按事件发生日期指定。这些压缩文件包含以纯格式存储的经过筛选的日志信息。
- 日志数据以一种格式存储，该格式允许在需要时根据需要在所需时间内进行恢复和重新生成。

启用归档的步骤:

- 点击"管理"标签 --> "管理"中的"归档事件"
- 根据所需的类别进行检查，并输入早于此日期的**“**天数**”**，处理后的数据将从直接数据库中清除并归档。

ADAudit Plus应用程序可以轻松地恢复和使用这些归档数据，用于**“**自定义报表**”**，用户可在其中确定报表周期。使用恢复后的数据，ADAuditPlus中始终可以对任何较早的日期进行自定义报表，因此这些自定义报表在取证、安全和合规性审计中起着至关重要的作用。

HTTP/HTTPS

ADAudit Plus和客户端通信之间的所有通信都通过一个简单且不言自明的Web浏览器界面进行。默认情况下，这些服务器-客户端交互发生在HTTP协议中。虽然在封闭的LAN中通过HTTP进行ADAudit Plus和客户端通信可能是安全的，但如果客户端位于LAN外部并将使用Internet访问ADAudit Plus，则必须在ADAudit Plus和客户端之间实施https协议。在地理位置不同的WAN或Internet上使用时，请应用启用SSL端口(Https)，以便对客户端-服务器通信进行加密。

步骤:

1. 点击管理标签 -->>连接设置。
2. 勾选启用ssl端口[https]以启用安全套接字层并输入端口号。
3. 点击保存。

使用ADAudit Plus，您可以做什么?

Active Directory审核:

* Active Directory审核报表
* 用户登录审核报表
* 跟踪用户管理动作
* 用户管理审核报表
* 所有AD变更审核报表
* Active Directory告警和邮件通知
* Active Directory审核和合规性
* 用户登录和注销
* 账户锁定分析
* DNS审核
* 架构审核
* 权限审核
* 实时报表和告警 - 2008 及以上的DC[新]

GPO变更:

* GPO变更审核
* 高级GPO审核报表

成员服务器审核:

* 登录/注销(域和本地)， 成员服务器和工作站上的登录持续时间
* 终端服务活动
* 计划任务活动
* 系统变更 - 启动/停止/审计日志清除
* 服务器上的进程跟踪
* 打印机审计[新]
* 文件完整性监控[新]

文件服务器审核:

* 文件/文件夹创建、修改、删除(成功和失败的尝试)
* 文件读取访问(成功和失败的尝试)
* 文件夹权限变更
* 文件夹审核设置变更(SACL)
* 文件移动/重命名
* 文件复制动作

NetApp Filer审核:

* 文件/文件夹创建、修改、删除(成功和失败的尝试)

* 文件读取访问(成功和失败的尝试)
* 文件夹权限变更
* 文件夹审核权限变更(SACL)
* 文件移动/重命名

EMC审核[新]:

* 文件/文件夹创建、修改、删除(成功和失败的尝试)
* 文件读取访问(成功和失败的尝试)
* 文件夹权限变更

报表:

ADAudit Plus有大量的报表可以从域中的任何位置有效地审计您的Active Directory。通过从客户端窗口选择报表选项卡，可以访问ADAudit Plus报表，默认情况下，报表被分组到以下类别中。

所有报表共有的功能:

- 为多个域生成报表
- 使用所有报表中提供的“添加/删除列”链接自定义列
- 允许从报表中显示的已可用属性列表中选择其他属性
- 通过输入列中显示的任何属性值来执行快速搜索
- 添加到收藏夹 —— 预定义报表用户输入添加书签并排序
- 打印报表
- 报表可以导出为CSV、PDF、XLS和HTML格式。
- 基于列出的和自定义的选定时间段查看报表的选项。
- 添加您自己的注释，以便在使用注释链接导出时显示。
- 每个报表都有一个图形显示，以帮助轻松访问更细粒度的审计信息。
- 选项选择要在报表的单个页中显示的行数。
- 报表可以采用以下任何一种格式存储：“pdf”、“xls”、“csv”或“html”。
- 可以选择一个或多个报表并将其计划在用户选择的时间运行
- 也可以通过电子邮件发送给一个或多个用户电子邮件ID
- 报表的柱状分类

告警:

使用ADAudit Plus，您可以为特定的更改事件配置和查看告警。例如:您可以配置并查看域中特定计算机上登录失败的告警。

创建一个新的告警配置文件:

- 点击“配置”标签 -->> 告警配置文件中的"创建新的告警配置文件"
- 将会显示创建告警配置文件的页面

- 输入告警配置文件的"名称"
- 输入告警配置文件的"描述"
- 选择告警配置文件的"严重度"(严重程度取决于告警的重要性，可以是"注意"、"麻烦"或"危急")
- 选择"报表配置文件"的域
- 点击"加号"图标
- 从下拉列表中选择"域"
- 从下拉列表中选择"类型"
- 选择一个或多个可用的"报表配置文件"，通过对它们进行检查来发出告警
- 点击确认
- 要添加告警消息，请单击告警消息框右侧的**[+]**链接。"告警消息"可以用常用告警消息输入，也可以配置自定义告警消息。点击"确认"
- 要发送电子邮件通知，请勾选"发送电子邮件通知"复选框，并在所提供的框中输入收件人的电子邮件地址
- 点击"保存"
- 一个新告警配置文件就创建完成了

自定义报表和告警:

可以自定义配置的基于报表概要的报表是一个高级特性。这是**ADAudit Plus**的一个亮点，它通过使用过滤器简化了对粒度细节的报表。变更审计事件是通过将审计操作和一个或多个帐户对象与报表概要关联起来来报表的，从而简化了粒度报表。使用基于报表概要文件的报表的优势使基于审计操作的粒度报表生成过程更加容易。

ADAudit Plus团队
ADAudit Plus的活动目录和文件服务器审核
邮箱 **: mes@zohocorp.com.cn**
免费电话**: 400-660-8680**