审核策略设置

2021-04-19

审核策略设置

在默认状态下，Windows Server 2003操作系统的审核机制并没有启动，需要网络管理员手工或者使用“安全分析和配置”MMC管理控制台加载安全模板的方式启动审核策略。下面将分别介绍审核策略的设置。

1．审核账户登录事件

审核账户登录事件审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器上对域用户账户进行身份验证时，将产生账户登录事件。该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件。该事件记录在本地安全日志中，不产生账户注销事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。当某个账户的登录成功时，成功审核会生成审核项。当某个账户的登录失败时，失败审核会生成审核项。

以“审核账户登录事件”为例说明如何设置审核策略。

第1步，在组策略控制台中依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“审核策略”，在右侧窗口中可以看到系统默认的所有策略，如图5-13所示。

在“组策略编辑器”窗口中，双击“审核账户登录事件”选项，显示“审核账户登录事件 属性”对话框，如图5-14所示。

选择“定义这些策略设置”复选框，然后根据需要选择“成功”或者“失败”复选框，单击“确定”按钮即可完成策略的设置。建议，在实际的网络应用中，选择“失败”即可，有两方面的原因如下。

 通常情况下，外来***不会一次就能够登录成功，因此，一般只需记录“失败”事件即可。当然，为了更为安全起见，也可以一同记录“成功”事件。

 可以节约日志空间，存储更多的日志信息。

图 5-13 显示审核策略窗口

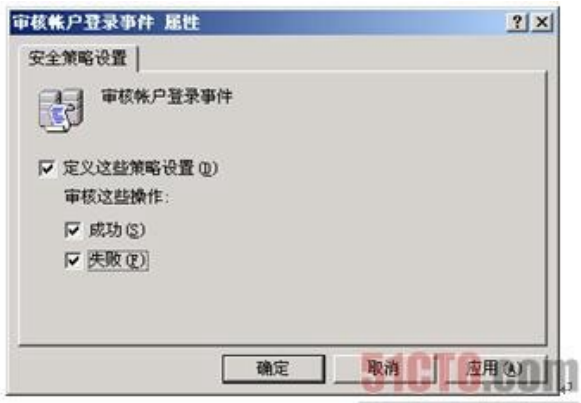

图 5-14 “审核账户登录事件 属性”对话框

定义该策略设置可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。当某个账户的登录成功时，成功审核会生成审核项。当某个账户的登录失败时，失败审核会生成审核项。

单击“确定”按钮，保存对该策略的设置。

其他审核策略设置用“审核账户登录事件”策略。

2．审核账户管理

审核账户管理设置确定是否审核计算机上的每一个账户管理事件。账户管理事件包括以下几种。

 创建、更改或删除用户账户或组。

 重命名、禁用或启用用户账户。

 设置或更改密码。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。任何账户管理事件成功时，成功审核都会生成审核项。任何账户管理事件失败时，失败审核也都会生成审核项。

3．审核目录服务访问

审核目录服务访问设置审核用户访问那些指定自己的系统访问控制列表（SACL）的Active Directory对象的事件。

默认情况下，在“默认域控制器组策略对象（GPO）”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它保持未定义状态。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。用户成功访问指定了SACL的Active Directory对象时，成功审核会生成审核项。用户尝试访问指定了SACL的Active Directory对象失败时，失败审核会生成审核项。

4．审核登录事件

审核登录事件设置审核每一个登录或注销计算机的用户实例。

在域控制器上将生成域账户活动的账户登录事件，并在本地计算机上生成本地账户活动的账户登录事件。如果同时启用账户登录和账户审核策略类别，那么使用域账户的登录将生成登录或注销工作站或服务器的事件，而且将在域控制器上生成一个账户登录事件。此外，在用户登录而检索登录脚本和策略时，使用域账户的成员服务器或工作站的交互式登录将在域控制器上生成登录事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。登录成功时，成功审核会生成审核项。登录失败时，失败审核会生成审核项。

5．审核对象访问

审核对象访问设置审核用户访问某个对象的事件，如文件、文件夹、注册表项和打印机等，它们都有自己特定的系统访问控制列表（SACL）。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。当用户成功访问指定了合适SACL的对象时，成功审核将生成审核项。当用户访问指定有SACL的对象失败时，失败审核会生成审核项。

6．审核策略更改

审核策略更改设置审核用户权限分配策略、审核策略或信任策略更改的每一个事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。对用户权限分配策略、审核策略或信任策略所作更改成功时，成功审核会生成审核项。对用户权限分配策略、审核策略或信任策略所作更改失败时，失败审核会生成审核项。

7．审核特权使用

审核特权使用设置审核用户实施其用户权利的每一个实例。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对这种事件类型进行审核。用户权利实施成功时，成功审核会生成审核项。用户权利实施失败时，失败审核会生成审核项。

8．审核过程跟踪

审核过程跟踪设置审核事件（例如，程序**、进程退出、句柄复制和间接对象访问等）的详细跟踪信息。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。所跟踪的过程成功时，成功审核会生成审核项。所跟踪的过程失败时，失败审核会生成审核项。

9．审核系统事件

当用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。系统事件执行成功时，成功审核会生成审核项。系统事件执行失败时，失败审核会生成审核项。

注意:Windows Server 2003里各种策略的应用先后顺序是：“本地计算机组策略”、“默认域策略”、“默认域控制器策略”、“组织单元策略”。后面的策略会覆盖掉前面应用的策略的!!

转载于:https://blog.51cto.com/yerik/336974

分类:

技术点:

相关文章:

Fabric设置背书策略 2021-05-15

Windows Server 2008 R2之八目录服务审核策略 2021-10-28

Go ASP.net core git CSS 后端 k8s mybatis Nginx 爬虫 多线程 React Django Spring Boot golang 云计算 容器 分布式 devops 架构 云原生 深度学习

常用小工具 更多

JSON格式美化工具

在线XML转JSON/JSON转XML工具

JSON格式化编辑和美化工具

密码安全性在线检测

在线计算器

在线高级科学计算器

贷款计算器/房贷计算器

在线RGB、HEX颜色代码生成器

在线WEB安全色查询工具

网页颜色搭配表及颜色搭配技巧

组策略与安全设置 2021-12-14

Infopath的策略设置问题 2021-10-27

AD账户频繁被锁定-开启日志审核策略 2021-11-07

谁动了账号，AD\exchange行为记录启用审核策略 2021-08-13

CentOS 设置密码策略 2022-03-08

组策略设置及导出导入方法[附上设置好的组策略] 2021-11-25

SQL Server 审核（Audit）-- 审核组件 2021-05-03

In - App Purchase，苹果内购商品，审核时的设置 2021-10-11

组策略设置IE 11的Compatible View 2021-09-15