AUTHORIZED DOCUMENTATION

用户指南

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

法律声明

Novell, Inc. 对本文档的内容或使用不作任何声明或担保，特别是对用于任何特定目的的适销性或适用性不作任何明示或暗示的担保。另外， Novell, Inc. 保留随时修改本出版物及其内容的权利，并且没有义务将这些修改通知任何个人或实体。

另外， Novell, Inc. 对任何软件不作任何声明或保证，特别是对适销性或用于任何特定目的的适用性不作任何明示或暗示的保证。另外， Novell, Inc. 保留随时修改 Novell 软件全部或部分内容的权利，并且没有义务将这些修改通知任何个人或实体。

依据本协议提供的任何产品或技术信息都将受到美国出口控制和其它国家 / 地区的贸易法律的约束。您同意遵守所有出口控制法规，并同意在出口、再出口或进口可交付产品之前取得所有必要的许可证或分类证书。您同意不出口或再出口至当前美国出口排除列表上所列的实体，或者美国出口法律中规定的任何被禁运的国家 / 地区或支持恐怖主义的国家 / 地区。您同意不将可交付产品用于禁止的核武器、导弹或生物化学武器等终端用途。有关出口 Novell 软件的详细信息，请访问 Novell International Trade Services 万维网页面 (http://www.novell.com/info/exports/)。如果您未能获得任何必要的出口许可， Novell 对此不负任何责任。

Novell, Inc. 对本文档中介绍的产品中所包含的相关技术拥有知识产权。这些知识产权特别包括但不限于 Novell 法律专利万维网页 (http://www.novell.com/company/legal/patents/) 上列出的一项或多项美国专利，以及美国和其它国家 / 地区的一项或多项其它专利或者正在申请的专利。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

*联机文档：*要访问该 Novell 产品及其它 Novell 产品的最新联机文档，请参见 Novell 文档万维网页 (http://www.novell.com/documentation)。

Novell 商标

有关 Novell 商标，请参见 Novell 商标和服务标记列表 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

第三方资料

所有第三方商标均属其各自所有者的财产。

目录

关于本指南

本指南包含 Novell® Identity Audit 的安装和配置。

适用对象

本指南的适用对象为 Novell Identity Audit 管理员。

反馈

我们希望听到您对本手册和本产品中包含的其它文档的意见和建议。请使用联机文档每页底部的 “用户意见”功能，或访问 www.novell.com/documentation/feedback.html 并输入您的意见。

文档更新

有关最新版本的 *《Novell Identity Audit 1.0 指南》*，请访问 Identity Audit 文档网站 (http://www.novell.com/documentation/identityaudit)。

文档约定

在 Novell 文档中，大于号 (>) 用于分隔步骤内的操作和交叉参照路径中的项目。

商标符号 （®、™ 等）代表一个 Novell 商标。星号 (*) 表示第三方商标。

简介

1

Novell® Identity Audit 为 Novell Identity 和 Security Management 环境提供事件报告和监视，环境包括 Novell eDirectory™、 Novell Identity Manager、 Novell Access Manager、 Novell Modular Authentication Services (NMAS™)、 Novell SecureLogin 和 Novell SecretStore®。

1.1 产品概述

Novell Identity Audit 1.0 是一个易于使用的轻型工具，用于收集、聚合和存储来自 Novell Identity Manager、 Novell Access Manager、 Novell eDirectory 以及其它 Novell 身份与安全产品与技术的事件。主要特性包括：

- 基于万维网的管理和报告界面
- 全事件搜索工具允许跨多个事件字段搜索
- 选中的事件输出到若干个通道
- 嵌入的 Jasper Reports 引擎允许使用开放源工具自定义包含的报告或创建新报告
- 内置数据库使得无需外部数据库许可或管理
- 简单直观的数据管理工具

1.1.1 与 Novell Audit 2.0.2 相比

Novell Identity Audit 1.0 设计作为 Novell Audit 产品系列的替代产品，这些 Novell Audit 产品系列的常规支持将在 2009 年 2 月终止。 Identity Audit 功能相当，但在体系结构、报告和数据管理方面获得了巨大改进。Novell Identity Audit 1.0 是 Novell Identity Audit 2.0 安全日志服务器的 Novell 身份与安全系列产品的随手可得的替代品。因为 Novell Identity Audit 使用新嵌入的数据库，所以客户应在存档的 Novell Audit 数据库中保存现有 Novell Audit 事件，而不是尝试迁移旧数据库。

Novell Audit 客户端组件 （也称为 Platform Agent）仍用作 Novell Identity Audit 的数据传输机制。根据仍使用 Platform Agent 的 Novell Identity 和 Access Management 产品的生命周期，还将继续支持该机制。

1.1.2 与 Novell Sentinel 相比

Novell Identity Audit 建立在功能强大的技术基础上，大部分基础代码与 Novell Sentinel 共享。但是， Sentinel 从更广泛的设备收集数据，提供更高的事件发生率，并提供比 Novell Identity Audit 更多的工具。Sentinel 提供其他安全信息和事件管理 (SIEM) 功能，例如实时仪表板、多事件关联、事件跟踪、自动修复和从非 Novell 产品收集数据。 Identity Audit 设计用于集成到未来 Sentinel 部署中。

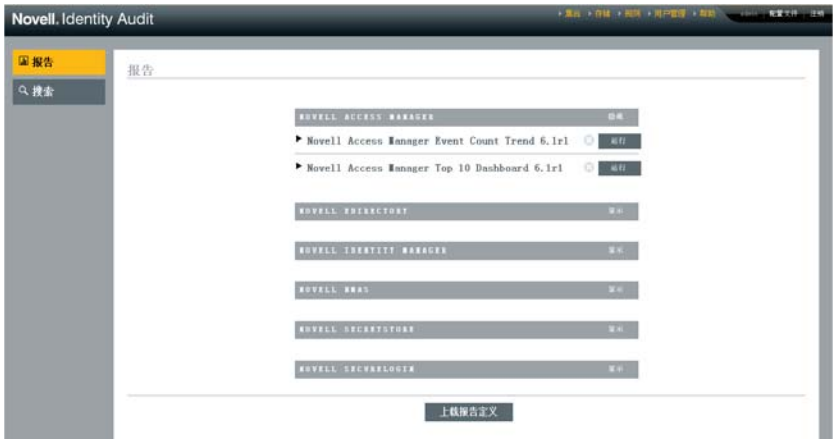
Novell Identity Audit 1.0 不是 Novell Compliance Management Platform (CMP) 的一部分，不包含该平台中提供的高级身份与安全集成功能。 Sentinel 6.1 现在是 CMP 的身份审计和监视组件。

1.2 界面

Novell Identity Audit 万维网界面提供执行以下任务的功能：

- 上载、运行、查看和删除报告
- 搜索事件
- 编辑用户配置文件详细信息
- 创建、编辑和删除用户，以及分配管理权限 （仅管理员）
- 配置数据收集和查看事件源的运行状况 （仅管理员）
- 配置数据存储和查看数据库的运行状况 （仅管理员）
- 创建过滤规则并配置将匹配事件数据发送到输出通道的相关操作 （仅管理员）

图 1-1 *Novell Identity Audit 界面 （管理员视图）*



界面每 30 秒钟自动刷新以显示其他用户所做的更新，如适用。

界面有多个语言版本 （英语、法语、德语、意大利语、日语、葡萄牙语、西班牙语、简体中文和繁体中文）。界面默认浏览器的默认语言，但用户在登录时可以选择其他语言。

注释 : 尽管界面已被本地化为双字节语言，但 Identity Audit 的当前版本并不处理双字节的事件数据。

1.3 体系结构

Identity Audit 从多个 Novell 身份与安全应用程序收集数据。这些应用程序服务器被配置为生成事件记录，并且每个都托管一个 Platform Agent， Platform Agent 是 Novell Audit 应用程序的一部分。事件数据由 Platform Agent 发送到 Identity Audit 服务器上的 Audit 连接器上。

Audit 连接器将事件传送到数据收集组件，数据收集组件分析事件并将它们放到通信总线上，通信总线是系统主干并负责中继组件间的所有通信。作为数据收集的一部分，传入事件由一组过滤规则来评估。这些规则过滤事件并将它们发送到输出通道，例如文件、系统日志中继或

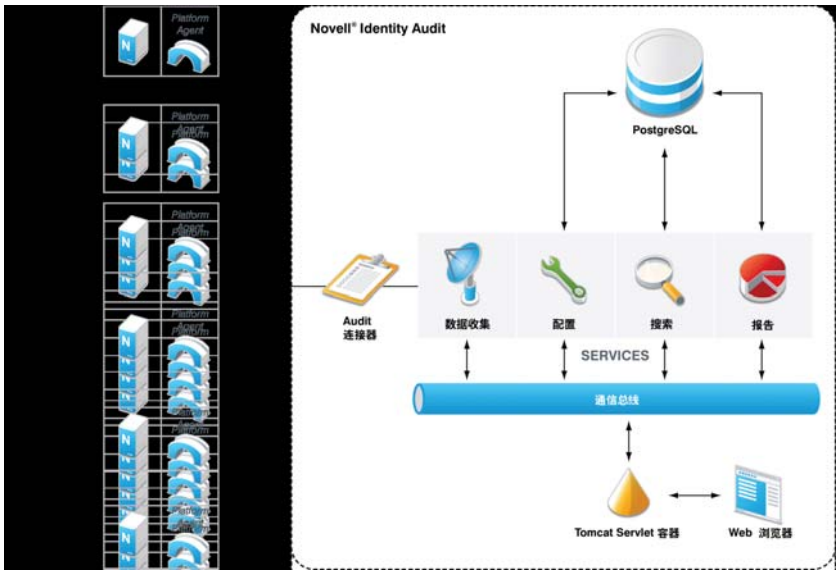
另外，所有事件存储在 Identity Audit 数据库 （基于 PostgreSQL*）的分区表中。

配置组件检索、添加和修改配置信息，例如：数据收集和存储设置、规则定义和报告定义。它还管理用户身份验证。

搜索组件执行快速的索引搜索并从数据库中检索事件，以便向用户显示搜索结果集。

报告组件运行报告并格式化报告结果。

图 1-2 *Identity Audit 的体系结构*



用户通过连接到 Apache Tomcat 万维网服务器的万维网浏览器与 Identity Audit 服务器及其所有功能进行交互。万维网服务器通过通信信息转移通路调用各个 Identity Audit 组件。

系统要求

2

除了以下介绍的硬件、操作系统、浏览器和事件源兼容性要求，安装还要求具有对操作系统的 root 访问权以创建 novell 用户和 novell 组，这些用户和组拥有 Identity Audit 的运行进程。

2.1 硬件要求

Novell Identity Audit™ 在 64 位 Intel Xeon* 和 AMD Opteron* 硬件上受支持。 Itanium 硬件上不支持。对于保存数据 90 天的生产系统， Novell 建议使用下列硬件：

- 1x Quad Core (x86-64)
- 16GB RAM
- 1.5 TB 可用磁盘空间 - 位于 RAID 硬件配置中 3x 500GB（3 可用）、10K RPM 的驱动器
  - 大约三分之二的可用磁盘空间用于数据库文件
  - 大约三分之一的可用磁盘空间用于搜索索引和临时文件
  - 有少量存储空间可用于从数据库移除的已存档数据，但 Novell 建议您将存档的数据文件移至其他介质。

表 2-1 *性能*

度量	值	说明
每秒钟的事件数 (eps) - 稳定状态	100	正常运行期间的平均事件发生率
每秒钟的事件数 (eps) - 最高	500	高峰期间 （最多 10 分钟）最高事件发生率
每秒钟的事件数 (eps) - 每个应用程序的最高值	300	每种 Novell 应用程序的最高事件发生率 ◆ Identity Manager、 SecureLogin、SecretStore® 和 NMAS™ 的事件发生率通常较低 （小于 15 eps）。 ◆ eDirectory™ 和 Access Manager 的事件发生率非常高。应执行事件过滤以确保一个易于控制的比率。 ◆ 即使在事件高峰期间，也没有一个应用程序可以每秒钟发送比这还多的事件。
联机数据	90 天或 7.5 亿个事件	Identity Audit 用建议的存储空间在稳定状态下以大约 100 eps 的速率可以存储的数据量

2.2 支持的操作系统

已证明 Identity Audit 可在 64 位 SuSE Linux Enterprise Server™ 10 SP 1 和 SP2 上运行。

2.3 支持的浏览器

Identity Audit 支持以下浏览器。其他浏览器可能无法按预期显示信息。

表 2-2 *Novell Identity Audit 支持的万维网浏览器*

万维网浏览器和版本
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

浏览器不同，搜索和报告查看性能也会有所不同。 Novell 发现使用 Mozilla Firefox 3 时的性能特别好。

2.4 支持的 Platform Agent

Identity Audit 1.0 支持从 Novell Audit 及其 Platform Agent 支持的多个应用程序收集日志事件。对于 32 位事件源，Identity Audit 需要 2.0.2 FP6 (2.0.2.55) 或更高版本的 Platform Agent。对于 64 位事件源，需要 2.0.2 FP6 版的 Platform Agent。

注释：一些 Novell 应用程序与以前版本的 Platform Agent 绑定。建议版本中包括重要 bug 修复，因此 Novell 建议升级 Platform Agent。

2.5 支持的事件源

Identity Audit 支持从 Novell 身份与安全应用程序收集数据。一些应用程序需要特定的增补程序级别以便正确收集数据。

表 2-3 *Novell Identity Audit 支持的应用程序*

应用程序
Novell Access Manager 3.0
在 Novell 支持网站 (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) 可以获取包含 eDirectory 工具增补程序的 Novell eDirectory 8.8.3
Novell Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

安装

3

本章介绍如何安装 Novell Identity Audit 以及如何配置事件源向其发送数据。这些说明假定已满足每个系统组件的最低要求。有关更多信息，请参见第 2 章 “系统要求”（第 13 页）。

3.1 安装 Novell Identity Audit

Identity Audit 安装程序包安装运行 Identity Audit 所需的所有内容：Identity Audit 应用程序和讯息总线，用于存储事件和配置信息的数据库，基于 web 的用户界面，以及报告服务器。共有两种安装选择，作为 root 运行的简单安装，或尽可能少使用 root 的多步骤安装。

3.1.1 快速安装 （作为 root）

这种简单安装必须以 root 运行。

1. 以 root 登录到要安装 Identity Audit 的服务器。
2. 将 identity_audit_1.0_x86-64.tar.gz 下载或复制到临时目录。
3. 使用以下命令从文件中解压缩安装脚本：

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```

4. 使用以下命令运行 root_install_all.sh 脚本：

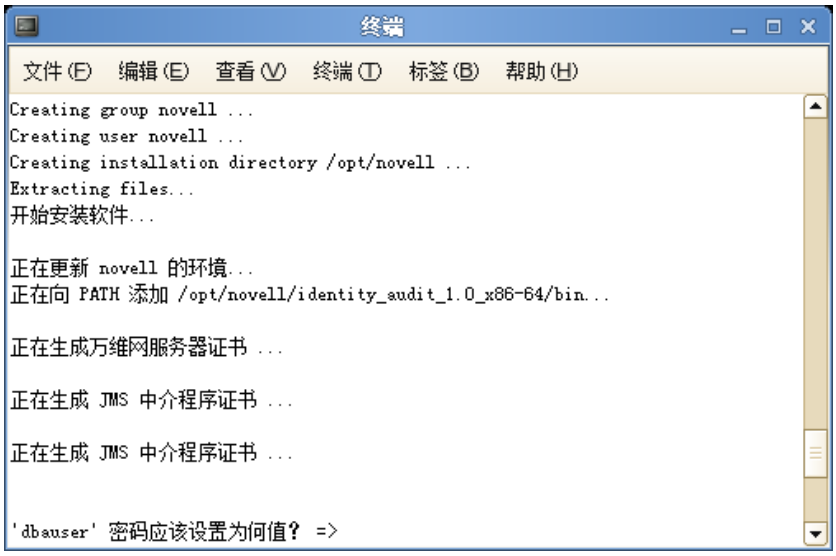
   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```

5. 输入数字选择语言。

   最终用户许可协议以选中的语言显示。

6. 阅读最终用户许可协议，如果您同意条款并想继续安装，请输入 1 或 y。

   安装随即开始。如果安装程序没有先前选择的语言 （例如，波兰语），安装程序将继续以英语安装。



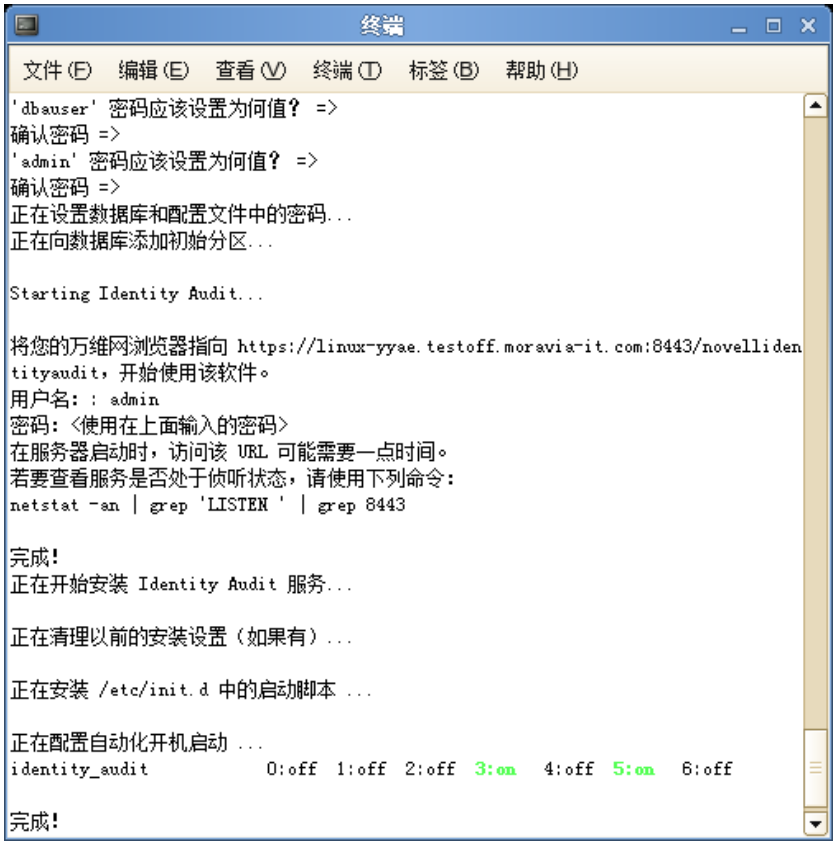
如果没有 novell 用户和 novell 组，则创建它们。

7 输入数据库管理员的口令 (dbauser)。

8 确认数据库管理员的口令 (dbauser)。

9 输入管理用户的口令。

10 确认管理用户的口令。



dbauser 身份凭证用于在 PostgreSQL 数据库中创建表和分区。 Identity Audit 已配置为以运行时级别 3 和 5 启动 （控制台中包含启动功能的多用户模式或 X-Windows 模式）。

Identity Audit 服务启动后，您可以登录到安装输出中指定的 URL (https://hostIP:8443/novellidentityaudit)。系统将立刻开始处理内部审计事件，并在您配置事件源向 Identity Audit 发送数据后发挥全部功能。

3.1.2 非 root 安装

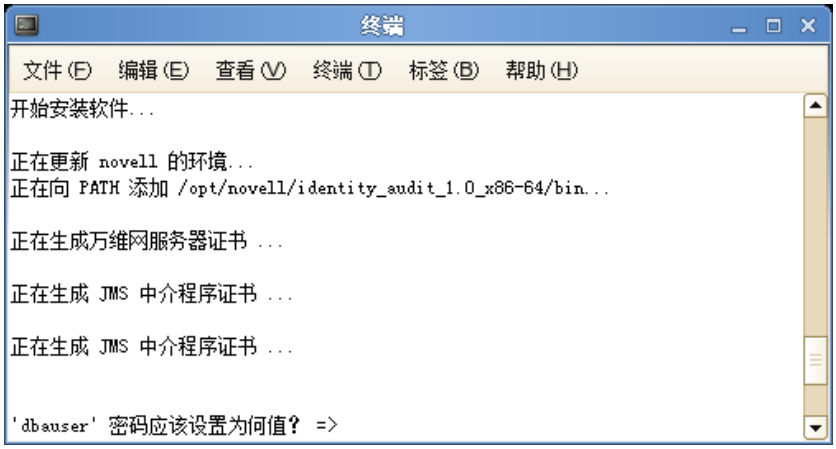
如果组织策略禁止以 root 运行完整安装过程，可以分两步运行安装。安装过程的第一部分必须以 root 级别访问权执行，第二部分以 Identity Audit 管理用户 （第一部分中创建）执行。

1. 以 root 登录要安装 Identity Audit 的服务器。
2. 将 identity_audit_1.0_x86-64.tar.gz 下载或复制到 /tmp 目录。
3. 除非服务器上已经存在 novell 用户和 novell 组：
   1. 否则，解压缩脚本从 Identity Audit tar 文件创建 novell 用户和 novell 组。例如：
      ```
      tar xfz identity_audit_1.0_x86-64.tar.gz
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
   2. 以 root 使用以下命令执行脚本：
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      Novell 用户和 novell 组将拥有 Identity Audit 的安装和运行进程。
4. 为 Identity Audit 创建目录。例如：

   mkdir -p /opt/*novell*
5. 设置目录由 novell 用户和 novell 组拥有。例如：
   ```
   chown -R novell:novell /opt/novell
   ```
6. 以 novell 用户登录：
   ```
   su novell
   ```
7. 将 Identity Audit tar 文件解压缩到刚创建的目录。例如：
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. 执行安装脚本。例如：
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. 输入数字选择语言。

   最终用户许可协议以选中的语言显示。
10. 阅读最终用户许可协议，如果您同意条款并想继续安装，请输入 1 或 y。

    安装随即开始。如果安装程序没有先前选中的语言 （例如，波兰语），安装程序将继续以英语安装。



11 输入数据库管理员的口令 (dbauser)。

12 确认数据库管理员的口令 (dbauser)。

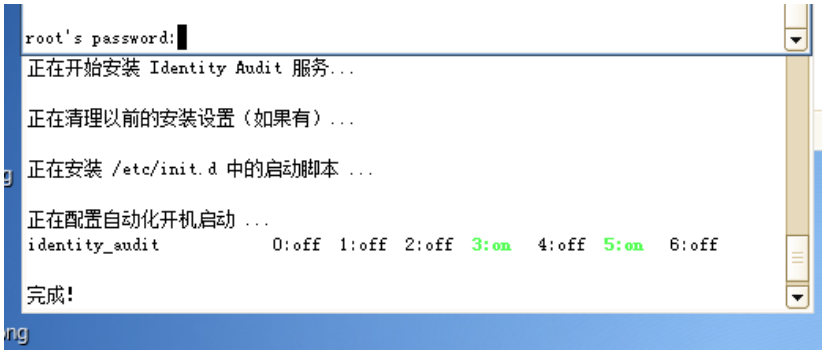
13 输入管理用户的口令。

14 确认管理用户的口令。

15 注销并以 novell 重新登录。这将加载 install.sh 脚本所作的 PATH 环境变量更改。

16 执行 root_install_service.sh 脚本使 Identity Audit 作为服务启动。此步骤需要 root 级别访问权。例如：

```
sudo /opt/novell/identity_audit_1.0_x86-64/setup/
root_install_service.sh
```



17 输入 root 口令。

Identity Audit 已配置为以运行时级别 3 和 5 启动（控制台中包含启动功能的多用户模式或 X-Windows 模式）。

Identity Audit 服务启动后，您可以登录到安装输出中指定的 URL (https://hostIP:8443/novellidentityaudit)。系统将立刻开始处理内部审计事件，并在您配置事件源向 Identity Audit 发送数据后发挥全部功能。

3.2 配置事件源

Identity Audit 1.0 可以从由 Novell Audit 以前产品及其 Platform Agent 支持的应用程序收集日志事件。在完成本部分的各个步骤之前，请确保您的 Novell 产品受到支持。有关更多信息，请参见第 2.4 节 “支持的 Platform Agent”（第 14 页）。

3.2.1 安装 Platform Agent

Platform Agent 必须至少为针对 Identity Audit 建议的最低版本。有关详细信息，请参见第 2.4 节 “支持的 Platform Agent”（第 14 页）。必须在所有事件源计算机上安装或更新相应的 Platform Agent （32 或 64 位）。 Platform Agent 包含在从 Novell 下载网站 (http://download.novell.com) 下载的 Novell Audit 中。

安装或升级 32 位 Platform Agent：

1. 下载 Audit 2.0.2 FP6 或更高版本的 iso 文件到事件源计算机上的 /tmp 目录中。
2. 为 Audit 创建目录。例如， mkdir -p audit202fp6
3. 以 root 身份登录。
4. 装入 Audit .iso 文件。

   mount -o loop ./NAudit202.iso ./audit202fp6
5. 转至 audit202fp6 目录。
6. 转至事件源操作系统中的相应目录。例如：

   cd Linux
7. 运行 pinstall.lin.

   ./pinstall.lin
8. 阅读许可协议，如果接受各项条款，则输入 y。
9. 输入 P 安装 Platform Agent。
10. 输入 Y 将先前的所有配置保留在 logevent.conf 文件中。

    已安装 Platform Agent。
11. 若要验证 Platform Agent 的版本是否正确，请输入下列命令：

    rpm -qa | grep AUDT

    novell-AUDTplatformagent 的版本应当至少为在第 2.4 节 “支持的 Platform Agent”（第 14 页）中列出的受支持的版本。

若要安装或升级 64 位 Platform Agent，请下载 NAudit 2.0.2 FP6 并按照增补程序中包含的说明执行操作。

3.2.2 配置 Platform Agent

安装之后，必须将 Platform Agent 配置为将数据发送到 Identity Audit 服务器，如果需要，从事件源发送事件签名。

警告：将 Platform Agent 配置为生成签名，会对事件源计算机的性能产生负面影响。

配置 Platform Agent：

1. 登录事件源计算机。
2. 打开 logevent 文件进行编辑。该文件的位置会有所不同，具体取决于操作系统：
   - Linux：/etc/logevent.conf
   - Windows：C:\WINDOWS\logevent.cfg
   - NetWare：SYS:\etc\logevent.cfg
   - Solaris：/etc/logevent.conf
3. 将 LogHost 设置为 dentity Audit 服务器的 IP 地址。
4. 设置 LogEnginePort=1289。（如果不存在，则添加该项。
5. 如果想要事件源发送事件签名，则输入 LogSigned=always。
6. 保存文件。
7. 重新启动 Platform Agent。操作系统和应用程序不同，方法也会有所不同。重新启动计算机，或者参考 Novell 文档网站 (http://www.novell.com/documentation) 上特定于应用程序的文档以获取更多说明。

3.2.3 配置审计级别

对于由 Identity Audit 监控的每个应用程序来说，每个应用程序为其生成记录的事件的配置方法会有所不同。下列 URL 提供有关每个应用程序的更多信息。

- Access Manager (http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd2l.html#b8cvd2l)
- eDirectory (http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)
- Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- NMAS (http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html)
- SecretStore (http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqdjxv.htm)
- 安全登录 (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 入门

在安装时创建的管理用户可以登录 Identity Audit 应用程序并创建其他用户，运行预加载的报告，上载新报告，执行事件搜索和其他操作。

登录到 Identity Audit：

1. 打开支持的万维网浏览器。有关更多信息，请参见第 2.3 节 “支持的浏览器”（第 14 页）。

2 转至 Identity Audit 登录页面 (https://hostIP:8443/novellidentityaudit)。

3 如果您是第一次登录 Identity Audit，则会显示一个证书。您必须接受该证书才能继续操作。

4 输入 admin。

5 输入安装过程中配置的 admin 口令。

6 选择 Identity Audit 界面的语言 （英语、葡萄牙语、法语、意大利语、德语、西班牙语、日语、繁体中文或简体中文）。

7 单击 “登录”。

3.4 卸载

要完全清除 Identity Audit 安装，必须运行卸载脚本，然后执行一些手动清理步骤。

1 以 root 登录 Identity Audit 服务器。

2 停止 Identity Audit 服务：
```
/etc/init.d/identity_audit stop
```

3 运行卸载脚本：
```
/opt/novell/identity_audit_1.0_x86-64/setup/
root_uninstall_service.sh
```

4 删除 Identity Audit 主目录及其内容。
```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

5 最后的步骤取决于您是否要保留有关 Novell 用户和组的任何信息。

- 如果您不想保留有关 Novell 用户的任何信息，请运行下列命令以删除该用户、其主目录和组：

  userdel -r novell && groupdel novell

- 如果您想保留 Novell 用户及其主目录，但要删除 Identity Audit 的所有相关设置，请执行下列步骤：

  1. 删除 Novell 用户的配置文件中用于 Identity Audit 的下列环境变量 （位于 ~novell/.bashrc 中）：

     APP_HOME=/opt/novell/identity_audit_1.0_x86-64 export PATH=$APP_HOME/bin:$PATH

  2. 从 PostgreSQL 文件 ~novell/.pgpass 删除 dbauser 项。 *:*:*:dbauser: *口令*

     注释：尽管 dbauser 口令显示为明文，但只有 Novell 和 root 用户才可以查看该文件，这些用户已有 Identity Audit 服务器上所有功能的完全访问权限。

搜索

4

本部分介绍 Novell® Identity Audit 的搜索功能。

4.1 事件搜索概述

Novell Identity Audit 提供对事件进行搜索的功能。搜索时会包括当前位于数据库中的所有联机数据，但不会包括由 Identity Audit 系统生成的内部事件，除非用户选择 *包括系统事件*。默认情况下，基于搜索引擎的关联算法对事件进行排序。

基本的事件信息包括事件名称、来源、时间、严重性、发起人信息 （通过箭头图标显示）和目标信息 （通过靶心图标显示）。

图 4-1 *事件字段*

4.2 运行事件搜索

用户可以运行简单和高级搜索。

4.2.1 基础搜索

会针对 表 4-1 在第 28 页 中的所有事件字段运行一个基本搜索。其中的基本搜索样例包括：

- root
- 127.0.0.1
- 锁定 *
- driverset0

注释：如果最终用户计算机和 Identity Audit 服务器的时间未实现同步 （例如，一台计算机延迟 25 分钟），则可能得到异常的搜索结果。*最后 1 小时*或*最后 24 小时*之类的搜索基于最终用户的计算机时间。

---

1 单击左侧的*搜索*链接。

Identity Audit 会被配置为在用户第一次单击*搜索*链接时，运行严重性为 3 到 5 的非系统事件的默认搜索。否则，默认设置为用户输入的最后一个搜索术语。

2 如果是其他搜索，则在搜索字段中键入一个搜索术语 （例如 admin）。该搜索不区分大小写。

3 选择执行搜索的时间段。大部分时间设置具有说明含义，默认值为 “过去 30 天”。

- “自定义”允许为查询选择开始日期和时间以及结束日期和时间。起始日期必须早于结束日期，时间基于
- *所有时间*会搜索数据库中的所有数据。

4 选择*包括系统事件*以包括 Identity Audit 系统操作生成的事件。

5 选择*按时间排序*，将最近事件的数据排在前面 .

注释：按时间排序比作为默认设置的按相关性排序的时间长。

---

6 单击 “搜索”。

将对索引中的所有字段搜索指定文本。旋转图标表明正在进行搜索。

显示事件摘要。

4.2.2 高级搜索

高级搜索可以在特定事件字段中搜索值。高级搜索条件以每个事件字段的短名称和索引的搜索逻辑为基础。下表介绍这些字段，提供用于高级搜索的短名称，并指示这些字段在基本视图和详细视图中是否可见。

若要搜索特定字段中的值，请使用字段的短名称 （有关更多信息，请参见 表 4-1 在第 28 页）、一个冒号和值。例如，要搜索 user2 对 Identity Audit 的身份验证尝试，请在搜索字段中输入以下文本：

- evt:authentication AND sun:user2
- pn:NMAS AND sev:5
- sip:123.45.67.89 AND evt: “Set Password”

可以使用布尔型运算符组合多个高级搜索条件：

- AND （必须大写）
- OR （必须大写）
- NOT （必须大写，并且不能用作唯一搜索条件）
- +
- -

必须使用 \ 符号转义特殊字符：

```
+ - && || ! ( ) { } [ ] ^ " ~ * ? : \
```

高级搜索条件以用于 Apache Lucene 开放源程序包的搜索条件为模型。有关搜索条件的更多详细信息，请访问网页：Lucene 查询分析器语法 (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html)。

4.3 查看搜索结果

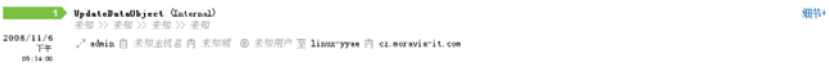
搜索返回一组事件。用户可以查看基本的或详细的事件信息，并配置每页显示的结果数量。搜索结果成批返回。默认批大小为 25 个结果，但可以容易配置它。

- 第 4.3.1 节 “基本事件视图”（第 25 页）
- 第 4.3.2 节 “具有详细信息的事件视图”（第 26 页）
- 第 4.3.3 节 “优化搜索结果”（第 26 页）

4.3.1 基本事件视图

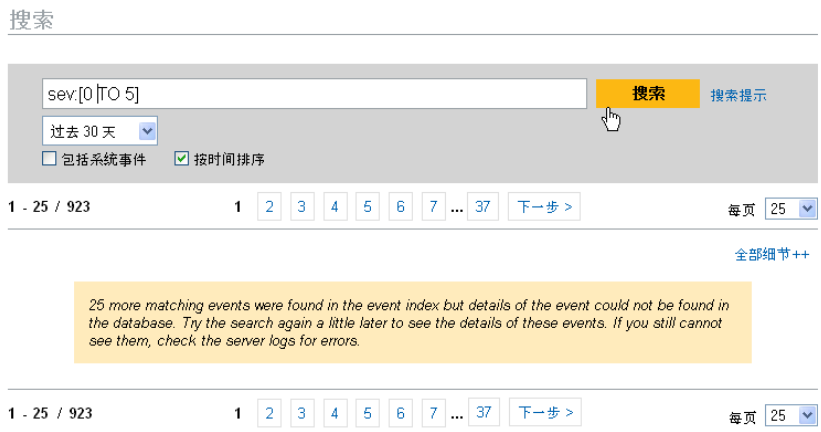
每个事件中的信息分组到 “发起人信息”和 “目标信息”中。如果特定事件字段中数据不可用，则字段标记为 “未知”。

图 4-2 *基本事件视图*



搜索引擎有时对事件编制索引可能会比将其插入到数据库中要快。如果用户运行的搜索返回未插入到数据库中的事件，用户则会收到一则信息，指出某些事件与搜索查询匹配，但在数据库中找不到该事件。一般来说，如果稍后再次运行该搜索，事件则会位于数据库中，搜索也会成功。

图 4-3 *已对事件编制索引，但事件尚不在数据库中。*



4.3.2 具有详细信息的事件视图

用户可以单击页面右侧的 “详细信息” 链接以查看任何事件的更多详细信息。使用 “所有详细信息 ++” 或 “所有详细信息 --” 链接可以展开或折叠页面上所有事件的详细信息。当您查看多个结果页面或执行新搜索时，此选择将保留。

图 4-4 *具有详细信息的事件视图*

以上事件显示图 4-2 在第 26 页中的同一事件，但包含其中显示可能已填充的其他数据字段的扩展视图。

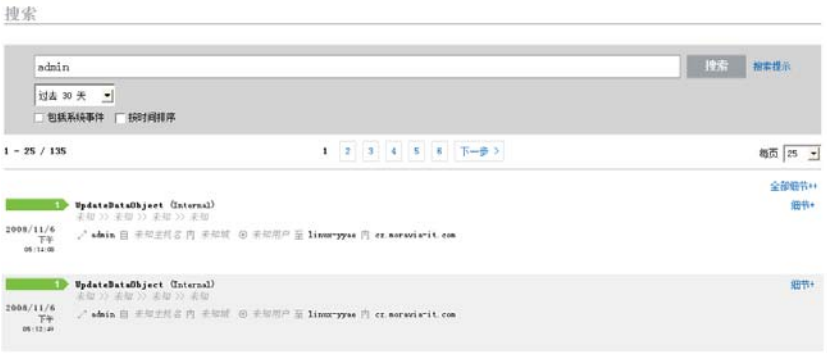
4.3.3 优化搜索结果

查看搜索结果后，可能需要优化搜索结果和添加更多搜索条件。例如，您可能看到一个发起人用户的名称在搜索结果中多次显示，并且希望查看该发起人的更多事件。

使用搜索结果中出现的特定值筛选搜索结果：

1 确定搜索结果中所需的过滤条件。

2 单击要通过其筛选结果的值 （例如，目标主机名 test1900）。



提示：这会将值添加到包含 AND 运算符的筛选器中。若要将值添加到包含 NOT 运算符的筛选器中，请在单击该值的同时按 Alt 键。

3 单击*搜索*。

选择某些值并不能这样优化搜索：

- 事件时间
- 讯息
- 与报告者相关的任意字段
- 与观察者相关的任意字段
- 包含未知值的任意字段

4.4 事件字段

每个事件都有填充或未填充的字段，取决于具体事件。通过使用搜索或运行报告可以查看这些事件字段的值。每个字段都有一个用于高级搜索的短名称。在事件的详细视图中会显示大多数字段的值，而在基本视图中也会显示其他值。

表 4-1 事件字段

字段	短名称	说明	可在基本视图中显示	可在详细视图中显示
严重性	sev	事件严重性 0 （信息型）至 5 （关键型）级	X	X
事件时间	dt	事件时间戳。可以是 Identity Audit 服务器时间戳，或原始事件源的时间戳 （如果启用 “信任事件时间”）	X	X
事件名	evt	事件的短名称	X	X
讯息	msg	详细事件信息		X
产品名	pn	生成事件的产品；事件源 显示在事件名称后。	X	X
InitUserName	sun	发起事件的用户的用户名	X	X
InitUserID	iuid	发起事件的用户的用户 ID		X
InitUserDomain	rv35	发起事件的用户的域 可以搜索，但不能在任一事件视图中显示		
InitHostName	shn	从中发起事件的计算机的主机名	X	X
InitHostDomain	rv42	从中发起事件的计算机的域	X	X
InitIP	sip	从中发起事件的计算机的 IP 地址		X
InitServicePort	spint	从中发起事件的端口号 （例如 HTTP）		X
InitServicePortName	sp	从中发起事件的端口类型 （例如 HTTP）		X
TargetUserName	dun	作为事件目标的用户的用户名	X	X
TargetUserID	tuid	作为事件目标的用户的用户 ID		X
TargetUserDomain	rv35	作为事件目标的用户的域 可以搜索，但不能在任一事件视图中显示		X
TargetHostName	dhn	作为事件目标的计算机的主机名	X	X
TargetHostDomain	rv45	作为事件目标的计算机的域	X	X
TargetIP	dip	作为事件目标的计算机的 IP 地址		X
TargetServicePort	dpint	作为事件目标的端口号 （例如 80）		X
TargetServicePortName	dp	作为事件目标的端口类型 （例如 HTTP）		X
TargetTrustName	ttn	作为事件目标的用户的角色 （例如 FinanceAdmin） 可以搜索，但不能在任一事件视图中显示		
TargetTrustID	ttid	表示作为事件目标的用户的角色的数字 ID 可以搜索，但不能在任一事件视图中显示		

字段	短名称	说明	可在基本视图中显示	可在详细视图中显示
TargetTrustDomain	ttd	可以搜索，但不能在任一事件视图中显示		
EffectiveUserName	euname	InitUser 扮演的用户的名称 （例如对于 root，使用 su）；在详细事件视图中的*发起人用户名 （发起人用户 ID） as* 后		X
EffectiveUserID	euid	InitUser 扮演的用户的数字 ID （例如对于 root，使用 su）		X
ObserverHostName	sn	将事件转发到安全信息事件管理系统的计算机的主机名 （例如 syslog 服务器的主机名）		
		可以搜索，但不能在任一事件视图中显示		
ObserverHostDomain	obsdom	将事件转发到安全信息事件管理系统的计算机的域 （例如 syslog 服务器的域）		
		可以搜索，但不能在任一事件视图中显示		
ObserverIP	obsip	将事件转发到安全信息事件管理系统的计算机的 IP 地址 （例如 syslog 服务器的 IP 地址）		
		可以搜索，但不能在任一事件视图中显示		
ReporterHostName	rn	将事件报告给观察者的计算机的名称		
		可以搜索，但不能在任一事件视图中显示		
ReporterHostDomain	repdom	将事件报告给观察者的计算机的域		
		可以搜索，但不能在任一事件视图中显示		
ReporterIP	repip	将事件报告给观察者的计算机的 IP 地址		
		可以搜索，但不能在任一事件视图中显示		
传感器类型	st	传感器类型的单字符批示名称 （N= 网络，H= 主机， O= 操作系统， A 和 I=Identity Audit 审核事件， P=Identity Audit 性能事件）。		
		可以搜索，但不能在任一事件视图中显示		
DataName	cs	事件中报告的数据对象名称 （例如，文件名或数据库表名称）		X
数据环境	rv36	FileName 数据对象的容器 （例如，文件的目录或数据库表的数据库实例）		X
TaxonomyLevel1	rv50	事件的目标分类。在事件名称下方以下面的格式显示：	X	X
		TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4		

字段	短名称	说明	可在基本视图中显示	可在详细视图中显示
TaxonomyLevel2	rv51	事件的子目标分类。在事件名称下方以下面的格式显示： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel3	rv52	事件的操作信息。在事件名称下方以下面的格式显示： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	事件的详细信息。在事件名称下方以下面的格式显示： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

一些字段被标记化。令牌化这些字段可以无需使用通配符即可搜索单个字。字段根据空格和其它特殊字符令牌化。对于这些字段，从搜索索引中删除 “a”或 “the”等冠词。

- 事件名
- 讯息
- 产品名
- 文件名
- 数据环境
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

报告

5

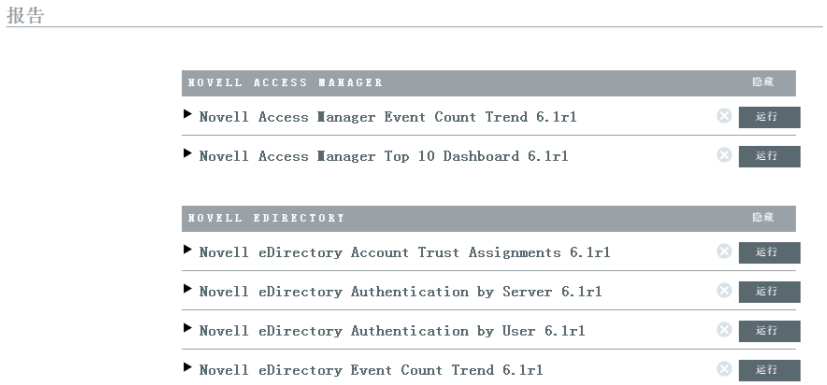
本章介绍如何在 Novell® Identity Audit 中运行、查看和管理报告。

5.1 概述

Identity Audit 安装时带有一组与 Novell 应用程序有关的核心报告模板。任何 Identity Audit 用户都可以使用他们所需的参数 （例如开始和结束日期）运行报告，并且报告结果将以用户选择的名称保存。报告运行后，任何 Identity Audit 用户都可以检索结果，并以 PDF 文件查看。

报告按类别组织。安装 Identity Audit 时会为每个支持的事件源包含报告。

图 5-1 *按类别组织的报告*



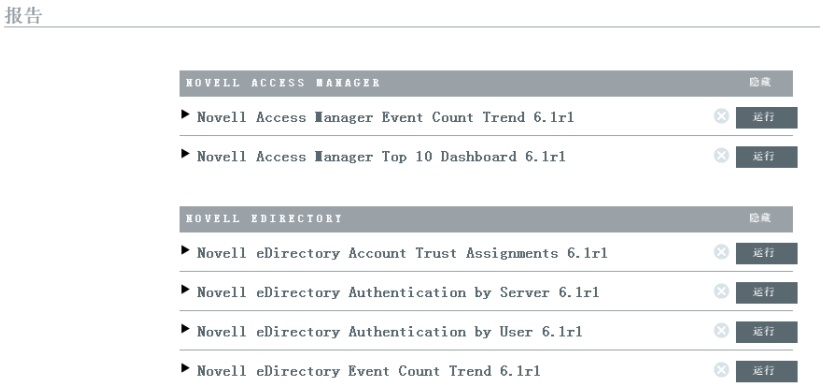
5.2 运行报告

安装 Identity Audit 时会包含一组报告，并且这些报告会被整理到若干个产品目录。报告异步运行，所以在运行报告时，用户可以在应用程序中继续做其他事情。报告完成运行后，任何用户都可以查看 PDF 报告结果。

很多报告定义含有参数。建议用户在运行报告之前设置这些参数。依据报告开发人员设计报告的方式的不同，报告参数可以是文本、数字、布尔值或日期。参数可能有一个默认值或基于 Identity Audit 数据库中的值的选取列表。

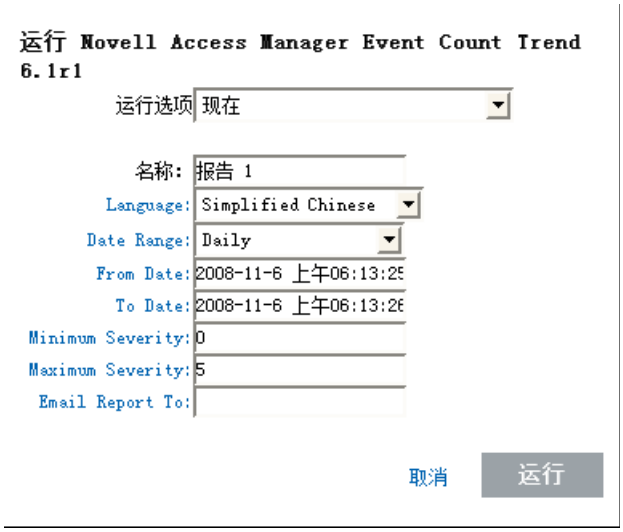
运行报告：

1 在 Identity Audit 中单击*报告*显示可用报告。



如需要，单击报告定义展开报告。如果您看到*样本报告*，可以单击*查看*来了解包含一组样本数据的完整报告的外观。

2 选择要运行的报告，然后单击*运行*。



3 设置运行报告的时间表。如果报告将在稍后运行，还必须输入开始时间。

- 现在：这是默认设置。它将立即运行报告。
- 一次：该设置在指定的日期和时间运行一次报告。
- 每天：该设置将在每天的指定时间运行一次报告。
- 每周：该设置将在每周同一天的指定时间运行一次报告。
- 每月：该设置将在每月的同一天，在指定日期和时间开始运行报告。例如，如果开始日期和时间是 10 月 28 日下午 2 时，报告将在每月第 28 天的下午 2 时运行。

注释：所有时间设置都基于浏览器的本地时间。

4 输入名称，确认报告结果。

因为用户名和时间也用于标识报告结果，所以报告名称不必唯一。

5 选择报告显示语言 （英语、法语、德语、意大利语、日语、繁体中文、简体中文、西班牙语或葡萄牙语）。

6 选择报告类型。所有时间期限都基于浏览器的本地语言。

- 每天：报告显示从当天凌晨到当天 11:59 的事件。如果当前时间是 8AM，报告将显示 8 小时的数据。
- 每周：报告显示从当周周日凌晨到当天结束的事件。
- 每月：报告显示从当月第一天凌晨到当天结束的事件。
- 自定义日期范围：您还需要在下面设置开始日期和结束日期 （仅限该设置）。
- 前一天：报告显示从昨天凌晨至昨天夜间 11:59 的事件。

7 如果您选择了 “自定义日期范围”，请设置报告的开始日期 （起始日期）和结束日期（终止日期）。

注释：如果为报告类型选择了 “每天”、“每周”、“每月”或 “前一天”，这些时间设置将被忽略。

8 设置要包含在报告中的 “最低严重性”事件。

9 设置要包含在报告中的 “最高严重性”事件。

10 如果要将报告发送给一个或多个用户，请输入他们的电子邮件地址，并用逗号分开。

注释：要启用用邮件发送报告功能，管理员必须在*规则* > *配置*下配置邮件中继。

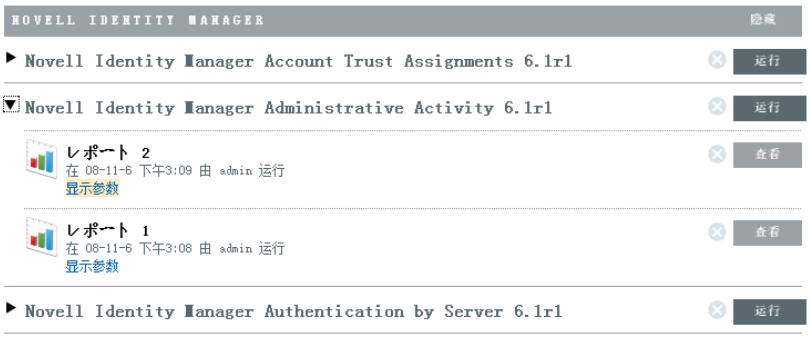
11 单击*运行*。

已创建报告结果项并发送给了指定收件人。

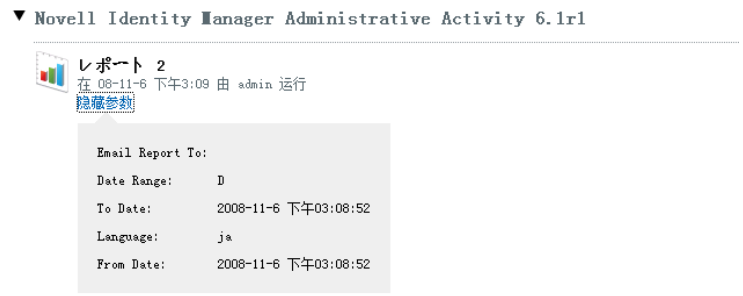
5.3 查看报告

Identity Audit 用户可以在 Identity Audit 应用程序中查看报告。其他用户可能会收到报告。邮件中的 pdf 文件。

1 要查看报告结果列表，请单击 “查看”。所有以前运行的报告将显示，并带有用户定义的报告名称、运行报告的用户以及运行报告的时间。

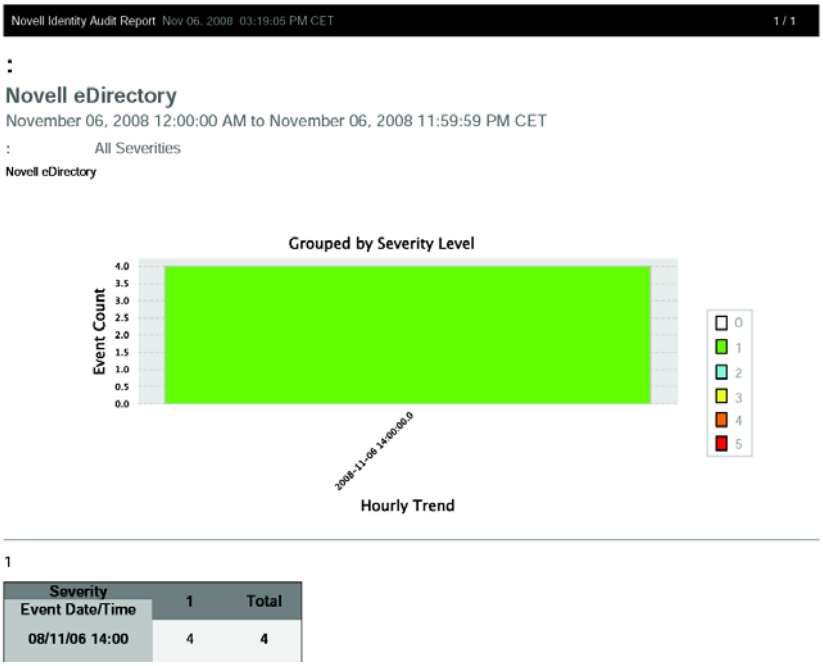


2 单击*显示参数*，查看用于显示报告的精确值。



- 对于报告类型，D= 每天，W= 每周，M= 每月，DR= 自定义日期范围，PD= 前一天。
- 对于语言，en= 英语，fr= 法语，de= 德语，it= 意大利语，ja= 日语，pt= 巴西葡萄牙语， es= 西班牙语， zh= 简体中文， zh_TW= 繁体中文。

3 对想看的报告结果单击*查看*。报告结果将显示在新的窗口中。 pdf 格式。



提示：报告结果从最新到最旧依次排列。

5.4 管理报告

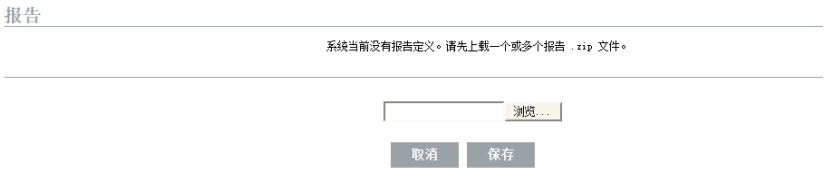
Identity Audit 用户可以添加、删除、更新和计划报告。

- 第 5.4.1 节 “添加报告”（第 35 页）
- 第 5.4.2 节 “重命名报告结果”（第 36 页）
- 第 5.4.3 节 “删除报告”（第 37 页）
- 第 5.4.4 节 “更新报告定义”（第 37 页）

5.4.1 添加报告

Identity Audit 本身预载了报告，但新报告插件 （尤其是包含报告定义和元数据的 zip 文件）也可以上载到 Identity Audit。如果系统中没有报告，将显示下面的屏幕：

图 5-2 *没有加载报告*



添加报告：

1. 单击屏幕左侧的*报告*按钮。
2. 单击*上载报告*按钮。
3. 浏览到本地机器上报告插件 zip 文件所在的位置。
4. 单击*打开*。
5. 单击*保存*。
6. 如果报告库中已经存在相同的报告 （基于报告的唯一 ID）， Identity Audit 将显示系统中的和正在导入的两个报告的详细信息。用户可以决定是否替换现有报告。在下面的情况下，导入的报告与现有报告版本相同。

7 新报告定义将以字母顺序添加到列表，如果需要，可立刻运行。

下载新报告或更新报告

N ovell 的新报告或更新报告可以从 Novell 内容网站 (http://support.novell.com/products/identityaudit/identityaudit10.html) 下载。

新建报告

用户可以使用 JasperForge* iReport. 修改或编写报告 （Jasper 报告的一种图形报告设计器）。iReport 是一种开放源报告开发工具，可以从 JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) 下载 （从本出版物发布时起）。

新报告或修改的报告可以包含 Identity Audit Web 界面没有显示的其他数据库字段。它们必须符合报告插件的文件和格式要求。有关数据库字段以及报告插件的文件和格式要求的更多信息，请参见 Sentinel SDK Web site (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)。

5.4.2 重命名报告结果

报告结果 （不是报告定义）可以在 Identity Audit 界面中重命名。

1 单击屏幕左侧的*报告*按钮。
2 单击报告名称展开报告。
3 单击要重命名的报告结果的名称。

4 输入新名称。

5 单击*重命名*。

5.4.3 删除报告

用户可以删除报告结果集或报告定义。如果删除报告定义，还将删除所有关联报告结果。

如果删除正在处理中的报告，将取消对数据库的查询。

5.4.4 更新报告定义

用户可以将更新的报告上载到 Identity Audit 来替换现有报告。有关更多信息，请参见第 5.4.1 节 “添加报告”（第 35 页）。

数据收集

6

管理员可以为 Novell® Identity Audit 配置和监视数据收集。 Identity Audit 安装时具有从各种使用 Novell Audit Platform Agent 的 Novell 应用程序收集数据的功能。有关 Platform Agent 支持版本的信息，请参见第 2.4 节 “支持的 Platform Agent”（第 14 页）。

6.1 配置事件源

尽管 Identity Audit 被预配置为接受多个 Novell 应用程序的数据，但应用程序服务器本身（事件源）必须配置为向 Identity Audit 服务器发送数据。这是 Identity Audit 基础设置的一部分。有关更多信息，请参见第 3.2 节 “配置事件源”（第 19 页）。

6.2 数据收集状态

管理员可以全局或按应用程序启用或禁用数据收集。他们还可以查看每个应用程序的运行状态信息。

1. 以管理员登录到 Identity Audit。
2. 单击 *页面右上角的收集*。

3. 启用或禁用由 Audit 服务器收集全局数据。
4. 启用或禁用从事件源收集应用程序特定数据。
5. 单击 *显示详细信息*，查看有关每个应用程序的活动连接的更多信息。

该页面将立即变化。

6.2.1 Audit 服务器

在 *Audit 服务器*部分，管理员可以使用 “开”和 “关”选项在全局级别启用或禁用数据收集。还会显示 Audit 服务器 的运行状态。

运行正常：绿色指示灯表示 Audit 服务器运行正常 （它亮起，正在监听端口，没有任何未解决的错误）。

错误：红色指示灯表示 Audit 发生了错误。详细信息，请查看 server0.*.log 文件。

脱机：灰色指示灯表示 Audit 服务器已经由管理员进行脱机处理。

6.2.2 事件源

在*事件源*部分，管理员可以在应用程序级别启用数据收集。这些设置会影响多个服务器的数据收集 （例如，多个 eDirectory 实例）。

注释 : 这些设置启用 （或禁用）从所列应用程序收集 Identity Audit 数据。它们不在事件源机器上开始或停止服务。

每个图标的运行状态由红色、黄色、绿色或黑色图标表示。更多状态，可以通过单击*显示详细信息*来查看更多信息。

运行正常：绿色指示灯表示事件源运行正常， Identity Audit 已接受其数据。

警告：黄色指示灯表示报警状态。常见原因是应用程序在 Identity Audit 中开启，但没有发送任何数据。例如，如果事件源上的 Platform Agent 没有正确配置为向 Identity Audit 发送数据，或者没有为应用程序启用事件日志，就会发生这种情况。单击*显示详细信息*可以查看更多信息。

错误：红色指示灯表示 Identity Audit 服务器正在报告连接应用程序或从其接收数据时出现的错误。单击*显示详细信息*可以查看更多信息。

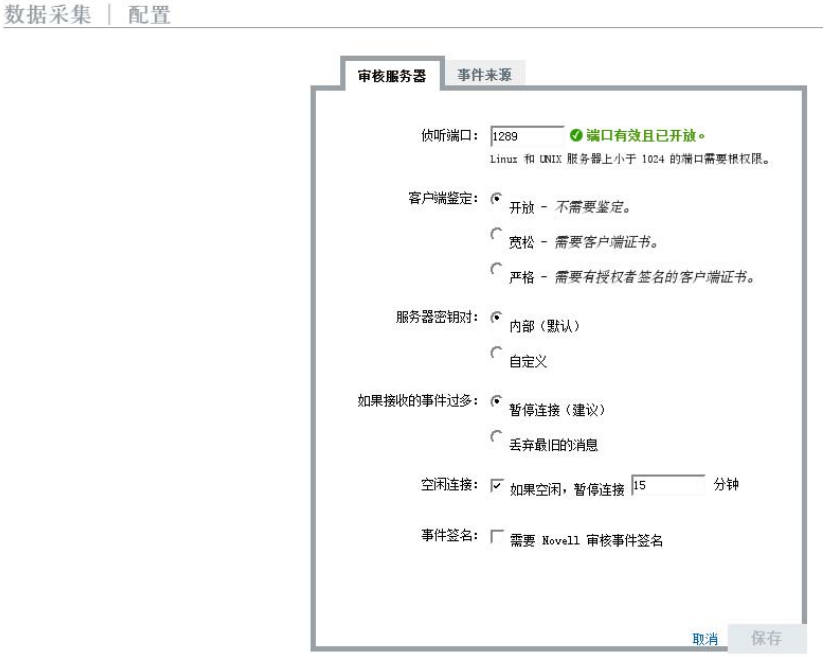
脱机 : 灰色指示灯表示事件源已关闭。 Identity Audit 没有处理来自事件源的任何数据。

对于每个联机数据源，Identity Audit 显示计算得出的传入事件的事件发生率。事件发生率每 60 秒钟重新计算一次。

6.3 Audit Server 选项

管理员可以更改 Identity Audit 侦听事件源应用程序数据的方式的一些设置，包括 Identity Audit 的侦听端口以及事件源和 Identity Audit 之间的身份验证类型。

1. 以管理员登录到 Identity Audit。
2. 单击屏幕顶部的 “收集”链接。
3. 单击屏幕右侧的 “配置”链接。
4. 确保选中 “Audit Server”。



5 输入 Identity Audit 服务器将要从事件源侦听消息的端口。有关更多信息，请参见第 6.3.1 节 “端口配置和端口转发”（第 41 页）。

6 设置合适的客户端身份验证和服务器密钥对设置。有关更多信息，请参见第 6.3.2 节 “客户端身份验证”（第 42 页）。

7 当缓冲区存储的事件过多时，选择 Identity Audit 服务器行为。

暂停连接：该设置中断现有连接并停止接受新连接，直到缓冲区内有存储新消息的空间。同时，事件源缓存消息。

丢弃最旧的消息：该设置按顺序丢弃最旧的消息以便接受新消息。

警告：如果选择*丢弃最旧的消息*，将无法恢复丢弃的消息。

---

8 选择*空闲连接*，可以断开在一定时间段内没有发送数据的事件源的连接。

事件源再次开始发送数据时，将自动重新创建连接。

9 在断开空闲连接之前，输入分钟数。

10 选择*事件签名*可接收事件的签名。

注释：只有正确配置事件源上的 Platform Agent 才能接收签名。有关更多信息，请参见第 6.1 节 “配置事件源”（第 39 页）. .

---

11 单击 “保存”。

6.3.1 端口配置和端口转发

Identity Audit 从 Platform Agent 侦听讯息的默认端口为端口 1289。设置端口后，系统将检查端口是否有效和打开。

将端口限制在 1024 以下需要根权限。相反， Novell 建议您使用大于 1024 的端口。您可以将源设备更改为向更高的端口发送或使用 Identity Audit 服务器上的端口转发功能。

更改事件源向不同的端口发送：

1. 登录到事件源机器。
2. 打开 logevent 文件进行编辑。根据操作系统的不同，文件会位于不同的位置。
   - Linux: /etc/logevent.conf
   - Windows: C:\WINDOWS\logevent.cfg
   - NetWare: SYS:\etc\logevent.cfg
   - Solaris: /etc/logevent.conf
3. 将 LogEnginePort 参数设置为所需端口。
4. 保存文件。
5. 重新启动 Platform Agent。方法因操作系统和应用程序的不同而有异。重新启动机器，或参阅 Novell 文档网站 (http://www.novell.com/documentation) 上的应用程序特定文档来了解更多说明。

配置 Identity Audit 服务器上的端口转发功能：

1. 作为 root （或 su to root）登录到 Identity Audit 服务器操作系统。
2. 打开文件 /etc/init.d/boot.local 进行编辑。
3. 在启动流程结束时添加下列命令：
   ```
   iptables -A PREROUTING -t nat -p protocol --dport incoming port -j
   DNAT --to-destination IP:rerouted port
   ```
   在这种情况下，*协议* 是 tcp 或 udp，*传入端口*是消息到达时所在的端口， *IP:rerouted 端口* 是本地机器的 IP 地址，并且可用端口大于 1024
4. 保存更改。
5. 重引导 . 如果不能立即重引导，从命令行运行上面的 iptables 命令。

6.3.2 客户端身份验证

事件源通过 SSL 连接来发送数据，并且 Identity Audit 服务器的*客户端身份验证*设置决定为来自事件源上的 Platform Agent 的证书执行哪种身份验证。

开放：无需身份验证。 Identity Audit 不请求、要求或验证来自事件源的证书。

松散：事件源要求有效的 X.509 证书，但该证书没有经过验证。它没有证书颁发机构的签名。

严格：事件源要求有效的 X.509 证书，并且必须有可靠的证书颁发机构的签名。如果事件源没有有效的证书， Identity Audit 将不会接受其数据。

- 创建可信存储区 （第 43 页）
- 导入可信存储区 （第 43 页）
- 服务器密钥对 （第 44 页）

创建可信存储区

对于严格身份验证，您必面有可信存储区，且其必须包含事件源的证书或为事件源证书签名的证书颁发机构的证书。拥有 DER- 或 PEM- 证书以后，就可以使用 Identity Audit 中的 CreateTruststore 程序创建可信存储区。

1. 作为 novell 登录到 Identity Audit 服务器。
2. 转至 /opt/novell/identity_audit_1.0_x86/data/updates/done。
3. 解压缩文件 audit_connector.zip。

   unzip audit_connector.zip
4. 用证书将 TruststoreCreator.sh 或 TruststoreCreator.bat 复制到机器，或用 TruststoreCreator 程序将证书复制到机器。
5. 运行 TruststoreCreator.sh 程序。

   TruststoreCreator.sh -keystore */tmp/my.keystore* -password *password1* -certs */tmp/cert1.pem,/tmp/cert2.pem*

   在这个例子中， TruststoreCreator 程序创建包含两个证书 (cert1.pem 和 cert2.pem）且名为 my.keystore 的关键存储区文件。该文件受密码 *password1* 的保护。

导入可信存储区

对于严格身份验证，管理员可以使用 *导入*按钮导入可信存储区。这有助于确保只有经过授权的事件源才可以向 Identity Audit 发送数据。可信存储区必须包含事件源的证书和为其签名的证书颁发机构的证书。

下列步骤必须在可信存储区所在的机器上运行。您可以打开可信存储区所在的机器上的 Web 浏览器，也可以将可信存储区移动到配有 Web 浏览器的任何一台机器。

导入可信存储区：

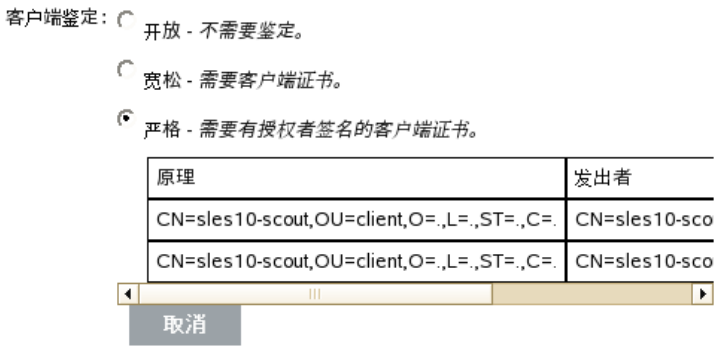
1. 以管理员登录到 Identity Audit。
2. 单击屏幕顶部的 “收集”链接。
3. 单击屏幕右侧的 “配置”链接。
4. 确保 *Audit Server* 选项卡被选中。
5. 选择*客户端身份验证*下的*严格*选项。

6 单击*浏览*，浏览到可信存储区文件 （例如 my.keystore）

7 输入可信存储区文件的密码。

8 单击*导入*。

9 单击*详细信息*



10 单击*保存*。

成功导入可信存储区后，可以单击*详细信息*查看可信存储区中包含的证书。

服务器密钥对

安装 Identity Audit 时会包含一个内置证书，用于 Identity Audit 到事件源的身份验证。该证书可以使用公共证书颁发机构签名的证书来废除。

替换内置证书：

1 以管理员登录到 Identity Audit。

2 单击屏幕顶部的 “收集”链接。

3 单击屏幕右侧的 “配置”链接。

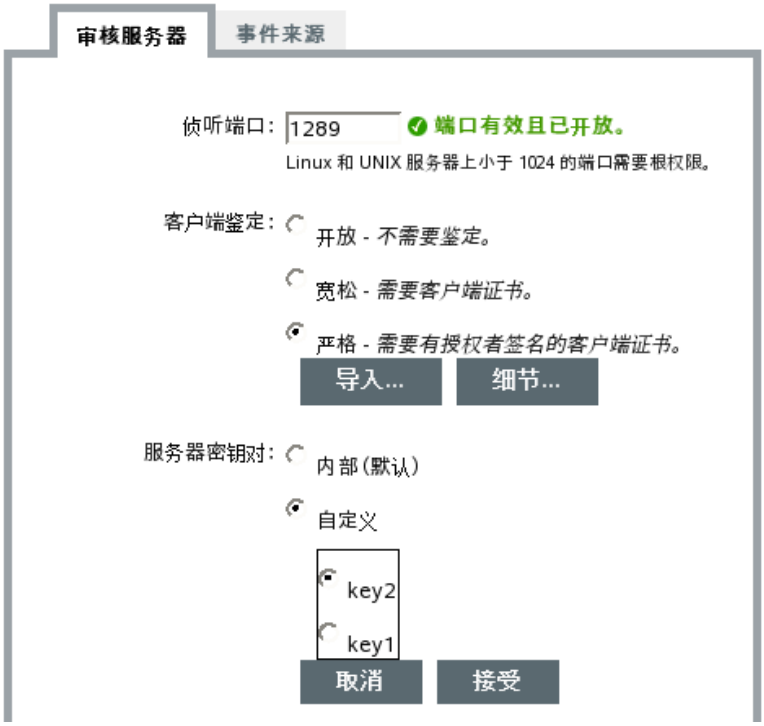
4 确保选中 “Audit Server”。

5 在*服务器密钥对*下，选择*自定义*。

6 单击*浏览*并浏览到可信存储区文件。

7 输入可信存储区文件的密码。

8 单击*导入*。



如果文件中有多个公 / 私钥对，选择所需密钥对并单击*确定*。

9 单击*详细信息*可了解有关服务器密钥对的更多信息。

10 单击*保存*。

6.4 事件源

管理员可以在*事件源*页面配置每个事件源的事件的时间确定方式。事件时间可以基于来自事件源的时间戳 （“信任时间早”），或基于来自 Identity Audit 服务器的时间戳。如果按时间排序，时间戳会影响搜索时事件的显示顺序。时间戳还会影响报告中的显示时间。默认使用 Identity Audit 服务器的时间。

注释：建议使用 NTP 服务器保持 Identity Audit 系统中所有计算机上的时间同步。如查 NTP 服务器可用， Novell 建议信任应用程序的事件时间。如果 NTP 服务器不可用， Novell 建议使用所有应用程序的 Identity Audit 服务器时间 （这是默认设置）来纠正两个机器之间的任何时差。

更改事件时间选项：

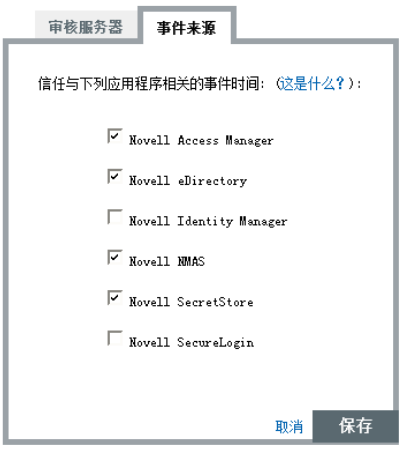
1 以管理员登录到 Identity Audit。

2 单击屏幕顶部的 “收集”链接。

3 单击屏幕右侧的 “配置”链接。

4 单击*事件源*。

5 选择 Identity Audit 将对其使用来自原始应用程序的事件时间戳的所有应用程序。



对于其他所有应用程序， Identity Audit 服务器时间戳将替换来自原始应用程序的时间戳。

更改将立刻对所有新传入的事件生效。可能需要一些时间来处理已经位于队列中的事件。

数据存储

7

Novell® Identity Audit 安装程序安装一个 PostgreSQL 数据库，并具有运行 Identity Audit 所需的所有表和用户。数据库还包含用于管理数据库分区和存档旧数据的存储过程。管理员可以通过万维网界面管理数据库存储和存档设置。

7.1 数据库运行状况

“数据库运行状况”页面仅对管理员可用，它显示数据库运行状况，即数据库上可用的分区数和存储过程创建新分区和存档数据成功与否 （如果配置）。

查看数据库运行状况：

1. 以管理员登录 Identity Audit。
2. 单击页面右上角的 “存储”链接。

   运行状况页面显示。

本页面显示是否有若干个数据库功能处于正常运行状态 （绿色）、报警状态 （黄色）或错误状态 （红色）。

联机数据库：此标志显示数据库中是否存在每个分区表的预期分区数。预期分区数基于配置的联机天数 （或已安装天数，如果是最近安装的）。

如果分区数不是预期值，页面将显示表名称、预期分区数和数据库中的实际分区数。

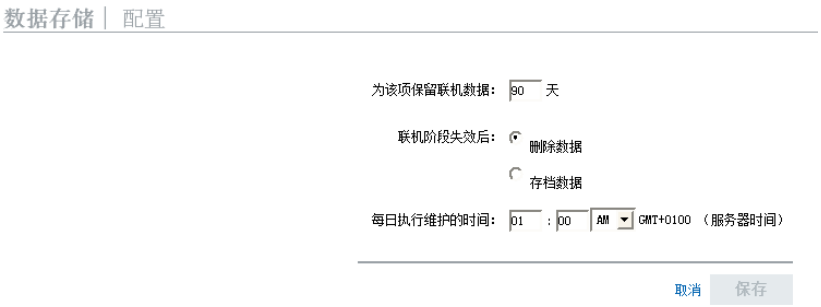
联机数据库作业：如果上次运行添加分区或删除数据的已存步骤时有任何错误，该指示灯将变为红色。如果启用存档，该指示灯将只显示上次运行添加分区的作业时是否有错误。如果有错误，页面将显示与失败作业相关的名称、时间戳和详细信息。

存档数据库：如果启用存档，将只显示该指示灯。如果上次运行存档数据的已存步骤时有任何错误，该灯将亮起红色。如果有错误，页面将显示与失败作业相关的名称、时间戳和详细信息。

7.2 数据存储配置

数据库是传入事件、配置信息和报告结果的储存库。 Identity Audit 提供数据库管理过程以避免数据库装满。仅供管理员访问的 “数据存储”页面提供配置数据存储多个方面的功能。

图 7-1 数据存储配置



为其保持数据联机：管理员可以指定保留数据库中的数据用于报告用途的天数。最小值为一天，数字必须为整数 （没有小数）。

联机期限到期后：联机数据保持期到期后，早于上述时间段的任何事件数据都将被删除或从数据库移至存档目录。

警告：Novell 不支持恢复已删除数据，所以请谨慎选择 “删除”选项。

存档到该数据库目录：如果选择 “存档数据”选项，请指定存档数据将写入到的现有目录位置。此目录必须已经存在， novell 用户必须具有对该目录的写入访问权。默认情况下此位置设置为 Identity Audit 主目录中的 /data/db_archive。Identity Audit 安装期间以相应权限创建默认目录。

重要：Novell 建议将存档文件定期移动到长期存储位置以避免装满硬盘。

测试：如果选中*存档数据*选项上，“测试”按钮将验证是否存在存档目录和 Novell 用户是否可以进行写入操作。

每天执行维护的时间：指定每天执行维护程序的时间：时间以 Identity Audit 服务器的本地时间为基础。在计划的维护时间，存档过程将运行以将分区添加到数据库。两小时后，存储过程将运行以存档或删除比天数更早的数据。

数据存档应计划在一天中数据库使用相对较低的时间执行。

规则

8

本章介绍用于将事件从 Identity Audit 发送到其它系统的事件通道。

8.1 规则概述

在 “规则”界面可以定义评估所有传入事件并将所选事件传输到指定输出通道的规则。例如，每个严重性为 5 级的事件可以通过电子邮件发送给安全分析师分发列表或管理员。

注释：所有事件也被传输到数据库。

按顺序对照每个过滤规则评估传入事件直到找到匹配项，然后执行与该规则相关的传输操作。

发送至电子邮件：使用配置的 SMTP 中断将事件发送给一个或多个用户

写入到文件：将事件写入到 Identity Audit 服务器上的指定文件

发送到系统日志：将事件转发到配置的系统日志服务器

提示：通过相关操作处理事件，一次一个。因此，在选择要将哪些事件发送到哪些输出通道时，应考虑性能的内在联系。例如，“写入到文件”操作的资源密集度最小，所以在将大量事件发送到电子邮件或系统日志之前，可以用它来测试规则标准，以此确定数据量。

另外，在设置 “发送到电子邮件”操作时，应考虑收件人可以有效处理的事件数量，并对过滤规则做相应调整。

事件输出是 JavaScript Object Notation (JSON) 格式，这是一个无足轻重的数据交换格式。事件由字段名称 （例如事件名称 “evt”）和紧随其后的冒号和值 （例如 “Start”）组成，中间用逗号隔开。

{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"CollectorManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agent":"Novell SecureLogin","obsassetid":"0","vul":"0","port":"Novell SecureLogin","msg":"Processing started for Collector Novell SecureLogin (ID D892E9F0-3CA7-102B-B5A1-005056C00005).","dt":"1224204655689","id":"751D97B0-7E13-112B-B933-000C29E8CEDE","src":"D892E9F0-3CA7-102B-B5A2-005056C00004"}

8.2 配置规则

可以配置 Identity Audit 规格以根据一个或多个可搜索字段过滤事件。有关 Identity Audit 可搜索字段列表，请参见表 4-1 在第 28 页。每个规则可以与配置的一个或多个操作相关联。

- 第 8.2.4 节 “删除规则”（第 51 页）
- 第 8.2.5 节 “激活或取消激活规则”（第 51 页）

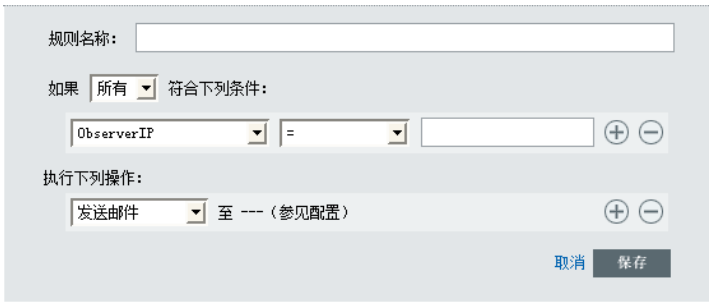
8.2.1 过滤条件

规则可基于任何可搜索的事件字段。这些字段的列表，请参见 表 4-1 在第 28 页。可用运算符取决于事件字段的数据类型。例如，匹配的子网适用于 IP 地址，而匹配的 regex 适用于文本字段。

8.2.2 添加规则

管理员可以添加基于过滤的规则，然后定义输出符合规则标准的事件的一条或多条通道。

1. 以管理员登录到 Identity Audit。
2. 单击 *页面右上角的规则*。
3. 单击*添加规则*。
4. 输入规则名称。
5. 如果您将创建多个条件，选择*全部*可用 AND 运算符将多个条件连接起来。选择*任何*可用 OR 运算符将多个条件连接起来。
6. 为过滤器选择事件字段、运算符和值。



7. 选择将要在符合过滤条件的每个事件上执行的操作。

   操作的详细情况基于单击*配置*链接时所看到的配置信息。
8. 根据需要配置其他操作。
9. 单击*保存*。

8.2.3 定制规则

由于是按顺序通过规则来评估事件，直到找到匹配项，所以 Novell 建议您根据情况定制规则。定义更细和更重要的规则应排在列表的开始位置。当有多个规则时，可以使用拖放功能重新定制规则。

重新定制规则：

1. 以管理员登录到 Identity Audit。
2. 单击 *页面右上角的规则*。
3. 将光标悬停在规则编号的左侧，启用拖放功能。光标将发生变化。

4 将规则拖放到定制清单中的正确位置。

8.2.4 删除规则

如果删除规则时已经有事件处于等待操作的队列中，则在停用规则后可能需要一些时间来清空该队列。

8.2.5 激活或取消激活规则

在每个规则的左侧，在标题为 “开”的列中，是激活该规则的复选框。新规则默认启用。如果停用规则，将不再按照该规则评估传入的事件。如果已经有事件处于等待操作的队列中，则在停用规则后可能需要一些时间来清空该队列。

8.3 配置操作

当某一事件符合其中一个规则规定的条件时，它就会被传输到一条或多条通道。在事件可以输出到通道之前，发送到该通道的操作必须配置合适的连接信息 （和身份验证凭证，如果 SMTP 中继需要）。 Identity Audit 系统对于每个操作类型只能有一个配置的连接 （例如，所有写入到文件的事件必须写入到同一文件）。

- 第 8.3.1 节 “发送到电子邮件”（第 51 页）
- 第 8.3.2 节 “发送到系统日志”（第 52 页）
- 第 8.3.3 节 “写入到文件”（第 53 页）

8.3.1 发送到电子邮件

若要配置发送到电子邮件操作，则需要 SMTP 中继的连接信息 （IP 址和端口号）、收件人和发件人地址。输入逗号分隔的列表可以发送到多个电子邮件地址。

注释：若要避免覆盖您的 SMTP 中继或电子邮件收件人，该操作仅可与生成少量事件的规则一起使用。

该 SMTP 中继配置也用于向用户传递报告。

1 以管理员登录到 Identity Audit。

2 单击 *页面右上角的规则*。

3 单击*配置*。

4 在*电子邮件*下面，输入可用 SMPT 中继的名称和端口。如果需要，则单击*测试*来测试连接情况。

5 如果 SMTP 中继需要身份验证，则输入用户名和口令。

6 输入电子邮件的发件人地址。

7 输入用逗号分隔的一个或多个电子邮件地址。

8 单击*保存*。

对于符合为其定义发送到电子邮件操作的筛选条件的所有 Identity Audit 事件，都会被发送到同一 SMTP 中继和地址组。

8.3.2 发送到系统日志

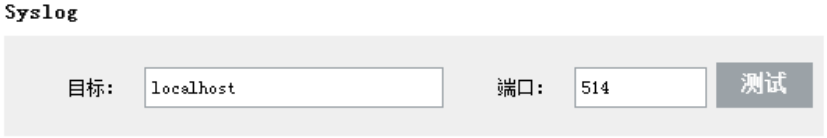
若要配置发送到系统日志操作，则需要系统日志服务器的连接信息 （IP 址和端口号）。

1 以管理员登录到 Identity Audit。

2 单击 *页面右上角中的规则*。

3 单击*配置*。

4 在*系统日志*下面，输入一个名称或 IP 地址并打开系统日志服务器的端口。如果需要，则单击*测试*以测试目标服务器和端口是否存在。



5 单击*保存*。

对于符合为其定义发送系统日志操作的筛选条件的所有 Identity Audit 事件，都会被发送到同一系统日志服务器。

8.3.3 写入到文件

要配置 “写入到文件”操作，您需要事件将写入到的文件的名称和路径。该目录必须已存在，并且 Novell 用户对其有写入权限。如果尚不存在该文件， Identity Audit 则会创建此文件。

1. 以管理员登录到 Identity Audit。
2. 单击 *页面右上角的规则*。
3. 单击*配置*。
4. 在*文件名*下面，输入要将事件写入到其听文件路径。如果需要，则单击*测试*来测试连接情况。

5. 单击*保存*。

对于符合为其定义写入到文件操作的筛选条件的所有 Identity Audit 事件，都会被写入到同一文件。

用户管理

9

管理员可以在 Novell® Identity Audit 中添加、编辑和删除用户，并授予管理权限。用户可以编辑自己的用户配置文件的详细信息。

9.1 添加用户

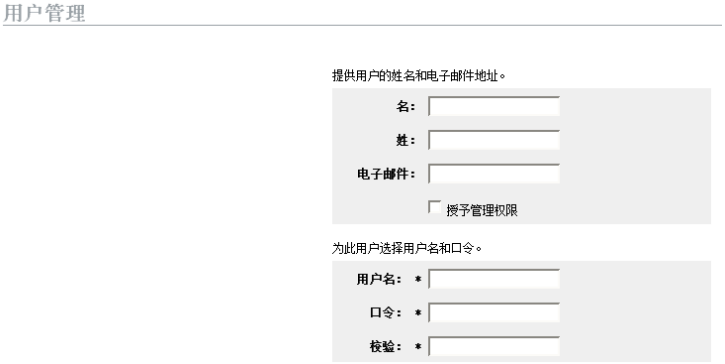
在 Identity Audit 系统中添加一个用户就会创建一个应用程序用户，该用户可以登录到 Identity Audit 应用程序。

如果选择*授予管理权限*选项，则会为用户提供 Identity Audit 系统中的管理权限。管理权限可以管理下列功能：

- 用户管理
- 数据收集
- 数据存储

添加用户：

1. 以管理员登录到 Identity Audit。
2. 单击 *页面右上角的 Admin 用户*。
3. 单击*添加用户*。
4. 输入用户信息。



带星号 (*) 的字段为填字段，并且用户名必须是唯一的。

注释：电子邮件地址已经过验证，而电话号码字段可以使用任意格式。确保输入一个有效的电话号码。

5. 如果需要，选择*授予管理权限*。
6. 单击*保存*。

9.2 编辑用户详细信息

管理员可以为系统中的任何用户编辑用户信息。除了用户名和管理员状态，任何用户还可以编辑其自己配置文件中的任意字段。用户还可以更改口令。

9.2.1 编辑您自己的配置文件。

1 单击右上角的*配置文件*。

2 编辑任意可用字段。

3 单击*保存*。

9.2.2 更改您自己的口令。

如果用户知道当前口令，就可以更改自己的口令。否则，必须由管理员重新设置口令。

1 单击右上角的*配置文件*。

2 输入您当前的密码。

3 输入新口令。

4 确认新口令。

5 单击 “保存”。

9.2.3 编辑另一个用户配置文件 （仅限 Admin)

1 以管理员登录到 Identity Audit。
2 单击 *页面右上角的 Admin 用户*。
3 单击要编辑的用户下面的*编辑*。
4 编辑任意字段 （除用户名以外）。
5 单击*保存*。

对*授予管理权限*的更改将在用户下次登录时生效。

9.2.4 重新设置另一个用户口令 （仅限 Admin)

若要重新设置另一个用户口令，请参见第 9.2.3 节 “编辑另一个用户配置文件 （仅限 Admin)”（第 57 页）。

9.3 删除用户

管理员可以从系统删除用户。

1 以管理员登录到 Identity Audit。
2 单击 *页面右上角的 Admin 用户*。
3 单击要删除的用户下面的*编辑*。
4 单击页面右上角的*删除该用户*。
5 单击*删除*以进行确认。

可信存储区

A

对 Identity Audit 及其从中收集数据的 Novell 应用程序之间的连接使用严格的身份验证，会提高数据安全性。

A.1 创建关键存储区

使用任何 JRE 安装程序中都包含的 Java “keytool”可执行文件可以创建关键存储区。该关键存储区包含一个公私密钥对，可用于替换 Identity Audit 自带的默认证书。下面是基本说明，若要获取有关 keytool 的更多信息，请参见 Sun 网站 (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html)。

1. 转至 Java 的 /bin 目录 （例如， $JAVA_HOME/bin）。
2. 运行以下命令：

   keytool -genkey -alias alias -keystore .keystore
3. 为关键存储区创建口令。当导入可信存储区时会使用该口令。
4. 输入下列信息：您的名和姓。
   - 名和性
   - 组织单位
   - 组织
   - 城市或地点
   - 州或省
   - 两位数国家代码
5. 验证该信息。
6. 按 Enter 以使用与关键存储区相同的口令。

   将创建一个包含私钥和相应公钥 （证书）的 .keystore 文件。