AUTHORIZED DOCUMENTATION

使用者指南

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時修訂本說明文件或更改內容，而無義務向個人或團體告知這類修訂或變更。

此外，Novell, Inc. 不對軟體做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時變更部份或全部 Novell 軟體，而無義務向個人或團體告知這類變更。

此合約下提到的任何產品或技術資訊可能受美國出口管制法與其他國家 / 地區的貿易法的限制。您同意遵守所有出口管制規定，並同意取得出口、再出口或進口產品所需的一切授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列之實體，或是任何美國出口法所指定之禁運或恐怖主義國家。您同意不將交付產品用在禁止的核武、飛彈或生化武器等用途上。請參閱 Novell 國際貿易服務網頁 (http://www.novell.com/info/exports/)，以取得有關出口 Novell 軟體的詳細資訊。Novell 無需承擔您無法取得任何必要的出口核准之責任。

對於本文件中所述及之所有產品內附技術，Novell, Inc. 皆具有其智慧財產權。特別是 (但不限於) 這些智慧財產權可能包含 Novell 法律專利網頁 (http://www.novell.com/company/legal/patents/) 中所列的一或多項美國專利，以及在美國與其他國家 / 地區的一或多項其他專利或申請中的專利。

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

*線上文件：*若要存取本產品及其他 Novell 產品的最新線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

若要查看 Novell 商標，請參閱 Novell 商標和服務標誌清單 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

協力廠商資料

所有的協力廠商商標均爲其各別擁有廠商的財產。

目錄

關於本指南

本指南涵蓋 Novell® Identity Audit 的安裝與組態作業。

使用對象

本指南適用於 Novell Identity Audit 管理員。

意見反應

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。請使用線上文件中每頁底下的「使用者意見」功能，或造訪 www.novell.com/documentation/feedback.html，然後寫下您的意見。

文件更新

如需最新版的 *《Novell Identity Audit 1.0 指南》*，請造訪 Identity Audit 文件網站 (http://www.novell.com/documentation/identityaudit)。

文件慣例

在 Novell 文件中，大於符號 (>) 是用來分隔步驟中的動作，以及交互參照路徑中的項目。

商標符號 (®、™ 等) 表示 Novell 的商標。星號 (*) 則代表協力廠商的商標。

介紹

1

Novell® Identity Audit 爲 Novell Identity and Security Management 環境提供事件報告與監控功能，此處所述環境包括 Novell eDirectory™、Novell Identity Manager、Novell Access Manager、Novell Modular Authentication Services (NMAS™)、Novell 安全登入與 Novell SecretStore®。

1.1 產品綜覽

Novell Identity Audit 1.0 是一個容易使用的輕量型工具，可用來收集、彙整與儲存來自 Novell Identity Manager、Novell Access Manager、Novell eDirectory 與其他 Novell 身分及安全性產品及技術的事件。主要功能包括：

- 以網頁爲基礎的管理與報告介面
- 完整的事件搜尋工具，可讓您在多個事件欄位中進行搜尋
- 將選取的事件輸出到多個通道
- 內嵌 Jasper Reports 引擎，可讓您使用開放原始碼工具來自定隨附的報告或建立新報告
- 內建資料庫，可減少外部資料庫授權或管理需求
- 簡單、直覺化的資料管理工具

1.1.1 與 Novell Audit 2.0.2 的比較

Novell Identity Audit 1.0 是設計來取代 Novell Audit 產品線的產品，這些 Novell Audit 產品線產品的支援將在 2009 年 2 月終止。Identity Audit 功能與舊版產品類似，但在結構、報告與資料管理方面有大幅的改進。Novell Identity Audit 1.0 也可以用來取代 Novell Identity and Security 產品線中的 Novell Audit 2.0.2 安全登入伺服器。因爲 Novell Identity Audit 使用新的內嵌資料庫，客戶應該將現有的 Novell Audit 事件保留在歸檔的 Novell Audit 資料庫中，而不是嘗試移轉舊資料。

Novell Identity Audit 仍使用 Novell Audit 用戶端元件 (亦稱爲 Platform Agent) 做爲資料傳輸機制。在 Novell Identity and Access Management 產品仍使用 Platform Agent 的生命週期中，我們不會終止此支援。

1.1.2 與 Novell Sentinel 的比較

Novell Identity Audit 是建立在穩固的技術基礎上，且許多相依的程式碼都與 Novell Sentinel 共用。但是，Sentinel 可從更多裝置收集資料、支援更高的事件速率，並提供比 Novell Identity Audit 更多的工具。Sentinel 提供額外的 Security Information and Event Management (SIEM) 功能，例如即時儀表板、多重事件交互關聯、事件追蹤、自動修正，以及從非 Novell 產品收集資料。Identity Audit 是設計來整合至未來的 Sentinel 部署。

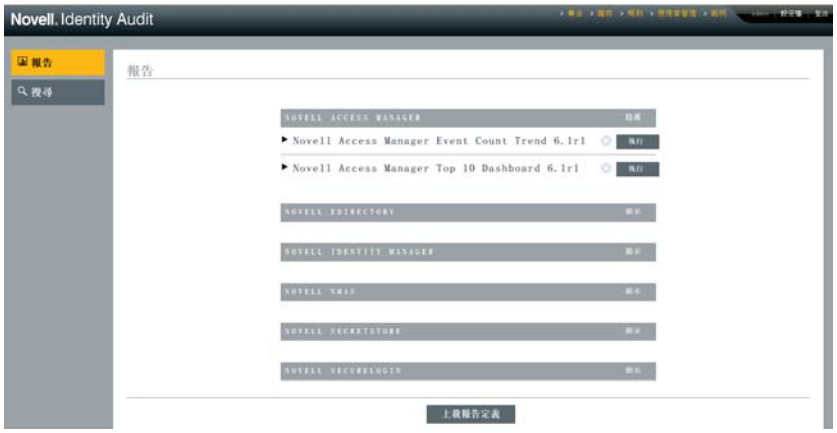
Novell Identity Audit 1.0 不是 Novell Compliance Management Platform (CMP) 的一部分，而且未包含該平台提供的進階身分與安全性整合功能。Sentinel 6.1 目前是 CMP 的身分稽核與監控元件。

1.2 介面

您可以使用 Novell Identity Audit 網頁介面來執行下列工作：

- 上載、執行、檢視與刪除報告
- 搜尋事件
- 編輯使用者設定檔詳細資料
- 建立、編輯與刪除使用者並指派管理權限 (僅限管理員)
- 設定資料集合與檢視事件來源的狀態 (僅限管理員)
- 設定資料儲存與檢視資料庫的狀態 (僅限管理員)
- 建立過濾規則並組態相關聯的動作，以傳送符合的事件資料到輸出通道 (僅限管理員)

圖 1-1 *Novell Identity Audit 介面 (管理員檢視)*



此介面每隔 30 秒會自動重新整理，以顯示由其他使用者執行的更新 (若適用)。

此介面提供多種語言 (英文、法文、德文、義大利文、日文、葡萄牙文、西班牙文、簡體中文與繁體中文)。此介面預設會使用瀏覽器的預設語言，但使用者可以在登入時選取其他語言。

附註：雖然此介面已翻譯爲雙位元語言，但目前的 Identity Audit 版本無法處理雙位元事件資料。

1.3 結構

Identity Audit 可從多種 Novell 身分識別及安全性應用程式收集資料。這些應用程式伺服器是組態爲產生事件記錄，而且每部伺服器都裝載 Platform Agent (Novell Audit 應用程式的一部分)。Platform Agent 會將事件資料轉送到 Identity Audit Server 上的「稽核連接器」。

「稽核連接器」會將事件傳遞到 「資料集合」元件，此元件會剖析事件並將事件放在 「通訊匯流排」(「通訊匯流排」是系統的骨幹，而且它是元件間所有通訊的仲介)。在 「資料集合」程序中，會由過濾規則集評估內送事件。這些規則會過濾事件並將事件傳送到輸出通道，例如檔案、syslog 傳送等。

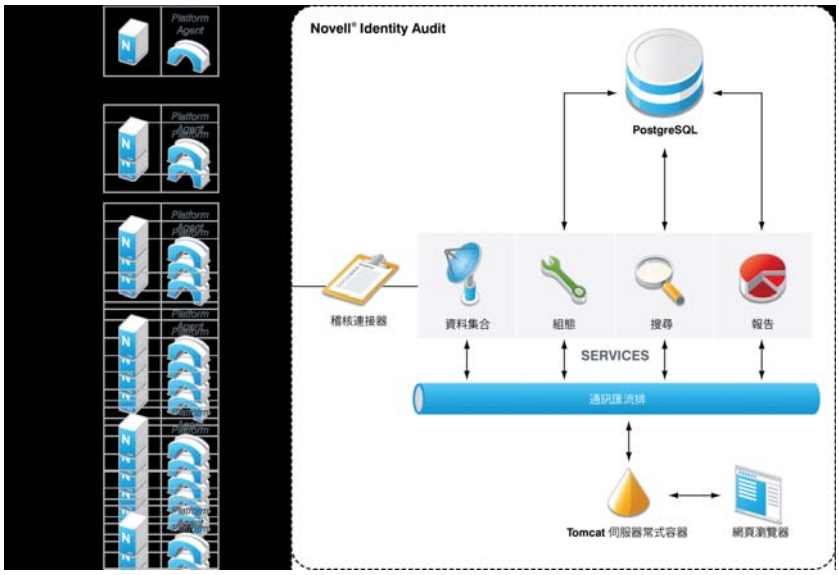
此外，所有事件都會儲存在 Identity Audit 資料庫 (PostgreSQL*) 的分割資料表中。

「組態」元件可擷取、新增與修改組態資訊 (例如資料集合與儲存設定、規則定義與報告定義)，它也負責管理使用者驗證。

「搜尋」元件可執行快速、已索引的搜尋並從資料庫擷取事件，爲使用者呈現搜尋結果集。

「報告」元件可執行報告並設定報告結果的格式。

圖 1-2 *Identity Audit 的結構*



使用者可透過網頁瀏覽器 (連接至 Apache Tomcat Web 伺服器) 與 Identity Audit 伺服器及其所有功能互動。Web 伺服器會透過 「通訊匯流排」呼叫各 Identity Audit 元件。

系統要求

2

除了以下所述的硬體、作業系統、瀏覽器與事件來源相容性要求之外，安裝也需要作業系統的 root 存取權，才能建立擁有 Identity Audit 執行中程序的 novell 使用者與 novell 群組。

2.1 硬體要求

64 位元 Intel Xeon* 與 AMD Opteron* 硬體都支援 Novell Identity Audit™。Itanium 硬體則不支援 Novell Identity Audit。Novell 建議您爲生產系統使用下列硬體 (可存放 90 天的線上資料):

- 1x Quad Core (x86-64)
- 16GB RAM
- 1.5 TB 可用磁碟空間 - 3x 500GB (3 可用)、10K RPM 硬碟機 (硬體 RAID 組態)
  - 大約 2/3 的可用磁碟空間會用於資料庫檔案
  - 大約 1/3 的可用磁碟空間會用於搜尋索引與暫存檔
  - 將使用一些儲存空間來存放從資料庫移除的歸檔資料，但 Novell 建議您將歸檔資料檔案移到其他媒體。

表格 2-1 *效能*

測量標準	數值	描述
每秒事件數 (eps) - 穩定狀態	100	正常操作期間的平均事件速率
每秒事件數 (eps) - 尖峰	500	事件突增期間的尖峰事件速率 (最長 10 分鐘)
個別應用程式每秒事件數 (eps) - 尖峰	300	來自每種 Novell 應用程式的尖峰事件速率 ◆ Identity Manager、SecureLogin、SecretStore® 與 NMAS™ 的事件速率通常很低 (小於 15 個事件 / 秒) ◆ eDirectory™ 與 Access Manager 的事件速率可能很高。您必須執行事件過濾以確保可管理的速率。 ◆ 即使在事件突增期間，也沒有任何應用程式能以超過此每秒事件數的速率傳送事件。
線上資料	90 天或 7.5 億個事件	使用建議的儲存裝置時，Identity Audit 在穩定速率狀態 (大約每秒 100 個事件) 下可儲存的資料量

2.2 支援的作業系統

Identity Audit 已證實可在 64 位元 SuSE Linux Enterprise Server™ 10 SP1 與 SP2 上執行。

2.3 支援的瀏覽器

Identity Audit 支援下列瀏覽器。其他瀏覽器可能無法正確地顯示資訊。

表格 2-2 *Novell Identity Audit 支援的網頁瀏覽器*

網頁瀏覽器與版本
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

搜尋與報告檢視效能因瀏覽器而異。Novell 發現使用 Mozilla Firefox 3 時會有最好的效能。

2.4 支援的 Platform Agent

Identity Audit 1.0 支援從 Novell Audit 與其 Platform Agent 所支援的許多應用程式收集記錄事件。對於 32 位元事件來源，Identity Audit 需要 Platform Agent 2.0.2 FP6 (2.0.2.55) 或更新版本。對於 64 位元事件來源，則需要 Platform Agent 2.0.2 FP6。

附註：某些 Novell 應用程式綑綁舊版的 Platform Agent。建議的版本包含重要的錯誤訂正，因此 Novell 建議您升級 Platform Agent。

2.5 支援的事件來源

Identity Audit 支援從 Novell 身分識別及安全性應用程式收集資料。某些應用程式需要安裝特定版本的修補程式，才能正確地收集資料。

表格 2-3 *Novell Identity Audit 支援的應用程式*

應用程式
Novell Access Manager 3.0
在 Novell 支援網站 (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) 上發現 Novell eDirectory 8.8.3 (含 eDirectory 儀器使用修補程式)
Novell Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell 安全登入 6.0

安裝

3

本章說明如何安裝 Novell Identity Audit 以及設定事件來源以傳送資料給它。這些指示假設每個系統元件都符合最低要求。如需詳細資訊，請參閱第 2 章 「系統要求」(第 13 頁)。

3.1 安裝 Novell Identity Audit

Identity Audit 安裝套件會安裝執行 Identity Audit 所需的所有元件：Identity Audit 應用程式與訊息匯流排、用來儲存事件與組態資訊的資料庫、Web 使用者介面，以及報告伺服器。安裝選項有兩個：可以使用 root 身分執行的簡易安裝，以及儘可能不使用 root 的多步驟安裝。

3.1.1 快速安裝 (以 root 身分執行)

您必須使用 root 身分才能執行此簡易安裝。

1. 以 root 身分登入要安裝 Identity Audit 的伺服器。
2. 下載或複製 identity_audit_1.0_x86-64.tar.gz 到暫存目錄。
3. 使用下列指令從檔案解壓縮安裝程序檔：
   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. 使用下列指令執行 root_install_all.sh 程序檔：
   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```
5. 輸入數字以選擇語言。

   使用者授權合約會以選取的語言顯示。
6. 閱讀使用者授權合約，若您同意合約中的條款而且要繼續安裝，請輸入 1 或 y。

   安裝即可開始。若安裝程式無法使用先前選取的語言 (例如，波蘭文)，則安裝程式將以英文繼續執行。

若系統上沒有 novell 使用者與 novell 群組，安裝程式會爲您建立。

7 輸入資料庫管理員 (dbauser) 的密碼。

8 確認資料庫管理員 (dbauser) 的密碼。

9 輸入 admin 使用者的密碼。

10 確認 admin 使用者的密碼。

dbauser 身分證明是用來在 PostgreSQL 資料庫中建立資料表與分割區。Identity Audit 是組態爲以執行時期層級 3 與 5 (含啓動於主控台或 X-Windows 模式的多使用者模式) 啓動。

當 Identity Audit 服務啓動後，您可以登入安裝輸出中指定的 URL (https://hostIP:8443/novellidentityaudit)。系統會立即開始處理內部稽核事件，而且當您設定事件來源以傳送資料到 Identity Audit 之後，它就可以完全地運作。

3.1.2 非 root 安裝

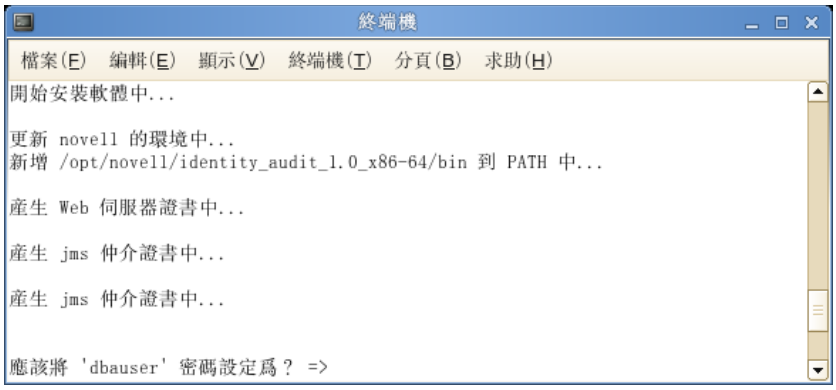
若組織規則禁止以 root 身分執行完整安裝程序，您可以使用兩個步驟來完成安裝。安裝程序的第一個部分必須以 root 層級的存取權執行，而第二個部分可以使用 Identity Audit 管理使用者 (在第一個部分所建立) 來執行。

1. 以 root 身分登入要安裝 Identity Audit 的伺服器。
2. 下載或複製 identity_audit_1.0_x86-64.tar.gz 到 /tmp 目錄。
3. 如果伺服器上沒有 novell 使用者與 novell 群組，請執行下列動作：
   1. 從 Identity Audit tar 檔案解壓縮程序檔以建立 novell 使用者與 novell 群組。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. 使用 root 身分以下列指令執行程序檔：
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      novell 使用者與 novell 群組將擁有 Identity Audit 的安裝與執行中程序。
4. 建立 Identity Audit 的目錄。例如：

   mkdir -p /opt/*novell*
5. 將該目錄的擁有者設定爲 novell 使用者與 novell 群組。例如：
   ```
   chown -R novell:novell /opt/novell
   ```
6. 以 novell 使用者的身分登入：
   ```
   su novell
   ```
7. 將 Identity Audit tar 檔案解壓縮到您剛建立的目錄。例如：
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. 執行安裝程序檔。例如：
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. 輸入數字以選擇語言。

   使用者授權合約會以選取的語言顯示。
10. 閱讀使用者授權合約，若您同意合約中的條款而且要繼續安裝，請輸入 1 或 y。

    安裝即可開始。若安裝程式無法使用先前選取的語言 (例如，波蘭文)，則安裝程式將以英文繼續執行。



11 輸入資料庫管理員 (dbauser) 的密碼。

12 確認資料庫管理員 (dbauser) 的密碼。

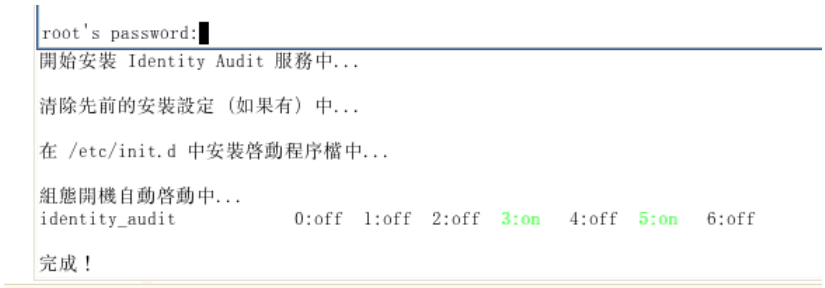
13 輸入 admin 使用者的密碼。

14 確認 admin 使用者的密碼。

15 登出並使用 novell 的身分重新登入。這樣會載入 install.sh 程序檔所做的 PATH 環境變數變更。

16 執行 root_install_service.sh 程序檔，讓 Identity Audit 以服務方式啓動。此步驟需要 root 層級的存取權。例如：

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



17 輸入 root 密碼。

Identity Audit 是組態爲以執行時期層級 3 與 5 (含啓動於主控台或 X-Windows 模式的多使用者模式) 啓動。

當 Identity Audit 服務啓動後，您可以登入安裝輸出中指定的 URL (https://hostIP:8443/novellidentityaudit)。系統會立即開始處理內部稽核事件，而且當您設定事件來源以傳送資料到 Identity Audit 之後，它就可以完全地運作。

3.2 設定事件來源

Identity Audit 1.0 支援從舊版 Novell Audit 產品與其 Platform Agent 所支援的應用程式收集記錄事件。完成本節中的步驟之前，請確定您的 Novell 產品已受支援。如需詳細資訊，請參閱 「支援的 Platform Agent」(第 14 頁)。

- 「安裝 Platform Agent」(第 19 頁)

- 「組態 Platform Agent」(第 19 頁)
- 「組態稽核層級」(第 20 頁)

3.2.1 安裝 Platform Agent

Platform Agent 必須符合 Identity Audit 所建議的最低版本需求。如需詳細資訊，請參閱「支援的 Platform Agent」(第 14 頁)。您必須在所有事件來源機器上安裝或更新適當的 Platform Agent (32 或 64 位元)。Platform Agent 內含於可從 Novell 下載網站 (http://download.novell.com) 下載的 Novell Audit 中。

安裝或升級 32 位元的 Platform Agent：

1. 將 Audit 2.0.2 FP6 或更新版本的 .iso 檔案下載到事件來源機器的 /tmp 目錄。
2. 建立 Audit 的目錄。例如，mkdir -p audit202fp6
3. 以 root 的身分登入。
4. 裝上 Audit .iso 檔案。

   mount -o loop ./NAudit202.iso ./audit202fp6
5. 移至 audit202fp6 目錄。
6. 移至事件來源上之作業系統的適當目錄。例如：

   cd Linux
7. 執行 pinstall.lin.

   ./pinstall.lin
8. 閱讀授權合約，若接受合約中的條款，請輸入 y。
9. 輸入 P 以安裝 Platform Agent。
10. 輸入 Y 可將所有先前的組態保留到 logevent.conf 檔案。

    這樣即可安裝 Platform Agent。
11. 若要驗證 Platform Agent 版本是否正確，請輸入下列命令：

    rpm -qa | grep AUDT

    novell-AUDTplatformagent 的版本至少必須是「支援的 Platform Agent」(第 14 頁) 所列的支援版本。

若要安裝或升級 64 位元的 Platform Agent，請下載 NAudit 2.0.2 FP6 並依照修補程式隨附的指示執行。

3.2.2 組態 Platform Agent

安裝 Platform Agent 之後必須進行組態以傳送資料到 Identity Audit 伺服器，如果需要也可以進行組態以從事件來源傳送事件簽名。

警告：組態 Platform Agent 以產生簽名會對事件來源機器的效能產生負面影響。

組態 Platform Agent：

1. 登入事件來源機器。

2 開啓 logevent 檔案以進行編輯。此檔案的位置在不同的作業系統上會不一樣：
   - Linux：/etc/logevent.conf
   - Windows：C:\WINDOWS\logevent.cfg
   - NetWare：SYS:\etc\logevent.cfg
   - Solaris：/etc/logevent.conf
3 將 LogHost 設定爲 Identity Audit 伺服器的 IP 位址。
4 設定 LogEnginePort=1289 (若此項目不存在，請自行新增)。
5 若要讓事件來源傳送事件簽名，請輸入 LogSigned=always。
6 儲存檔案。
7 重新啓動 Platform Agent。重新啓動方式視作業系統與應用程式而定。將機器重新開機，或參閱 Novell 文件網站 (http://www.novell.com/documentation) 的應用程式特定文件以取得詳細指示。

3.2.3 組態稽核層級

對於由 Identity Audit 監控的每個應用程式，Identity Audit 對於每個應用程式用以產生的記錄的事件會有不同組態。下列 URL 提供關於每個應用程式的詳細資訊。

- 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)
- SecureLogin (http://www.novell.com/documentation/securelogin60/index.html (see the Auditing link))

3.3 開始使用

安裝期間建立的管理使用者可登入 Identity Audit 應用程式並建立更多使用者、執行預先載入的報告、上載新報告，以及執行事件搜尋等。

登入 Identity Audit：

1 開啓支援的網頁瀏覽器。如需詳細資訊，請參閱 「支援的瀏覽器」(第 14 頁)。
2 移至 Identity Audit 登入頁面 (https://hostIP:8443/novellidentityaudit)。
3 若這是您第一次登入 Identity Audit，系統會提供證書。您必須接受它才能繼續。
4 輸入 admin。
5 輸入安裝期間設定的 admin 密碼。

6 選取 Identity Audit 介面的語言 (英文、葡萄牙文、法文、義大利文、德文、西班牙文、日文、繁體中文或簡體中文)。

7 點選「*登入*」。

3.4 解除安裝

若要完全清除 Identity Audit 安裝，您必須執行解除安裝程序檔，然後執行一些手動清除步驟。

1 以 root 的身分登入 Identity Audit 伺服器。

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

3 執行解除安裝程序檔：
```
/opt/novell/identity_audit_1.0_x86-64/setup/
root_uninstall_service.sh
```

4 刪除 Identity Audit 主目錄與其內容。
```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

5 最後一個步驟取決於您是否保留任何與 novell 使用者和群組相關的資訊。

- 若不要保留任何與 novell 使用者的相關資訊，請執行下列指令以移除使用者、使用者的主目錄以及群組：

  userdel -r novell && groupdel novell

- 若要保留 novell 使用者與其主目錄，但想要移除所有 Identity Audit 相關設定，請依照下列步驟執行：

  1. 從 novell 使用者的設定檔 (位於 ~novell/.bashrc) 移除 Identity Audit 的下列環境變數項目：

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

  2. 從 PostgreSQL 檔案 ~novell/.pgpass 移除 dbauser 項目。*:*:*:dbauser:*password*

     附註：雖然 dbauser 密碼是以明文顯示，但只有 novell 與 root 使用者 (這些使用者已經有 Identity Audit 伺服器上所有功能的完整存取權) 可以看到此檔案的內容。

搜尋

4

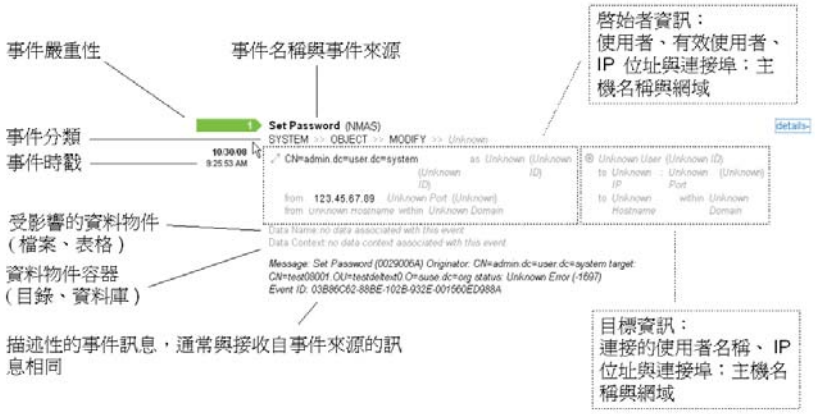
本節說明 Novell® Identity Audit 的搜尋功能。

4.1 事件搜尋綜覽

Novell Identity Audit 提供搜尋事件的功能。搜尋會包含目前在資料庫中的所有線上資料，但會排除 Identity Audit 系統產生的內部事件 (若使用者未選取「*包含系統事件*」。系統預設會根據搜尋引擎的相關演算法來排序事件。

基本事件資訊包含事件名稱、來源、時間、嚴重性、啓始者相關資訊 (以箭頭圖示表示) 與目標相關資訊 (以舷窗圖示表示)。

圖 4-1 *事件欄位*



4.2 執行事件搜尋

使用者可以執行簡易與進階搜尋。

4.2.1 基本搜尋

基本搜尋可針對表格 4-1 頁上 28 中的所有事件欄位執行搜尋。以下是一些基本搜尋範例：

- root
- 127.0.0.1
- Lock*
- driverset0

附註：若使用者機器與 Identity Audit 伺服器機器的時間並未同步 (例如，一部機器的時間比正確時間快 25 分鐘)，搜尋時可能會傳回未預期的結果。「*前 1 小時*」或「*前 24 小時*」等搜尋是以使用者機器的時間爲準。

---

1 點選左邊的「*搜尋*」連結。

Identity Audit 是組態爲在使用者首次點選「*搜尋*」連結時，執行預設搜尋以尋找嚴重性爲 3 到 5 的非系統事件。否則，它預設會以使用者上次輸入的搜尋條件執行搜尋。

2 若要執行不同的搜尋，請在搜尋欄位輸入搜尋條件 (例如，admin)。搜尋時不區分大小寫。

3 選取要搜尋的期間。大部分的時間設定都非常容易瞭解，應該不需要特別說明，而且預設值是「*前 30 天*」。

- 「*自定*」可讓您選取要查詢的開始日期及時間與結束日期及時間。開始日期必須在結束日前之前，而時間則是基礎
- 「*所有時間*」可搜尋資料庫中的所有資料。

4 選取「*包含系統事件*」可包含由 Identity Audit 系統操作所產生的事件。

5 選取「*依時間排序*」可依事件時間排序資料 (最新的事件排在最前面)。

附註：依時間排序 (預設值) 所需的時間比依嚴重性排序所需的時間久。

---

6 點選「*搜尋*」。

搜尋時會尋找索引中的所有欄位是否有指定的文字。旋轉的圖示表示正在進行搜尋。

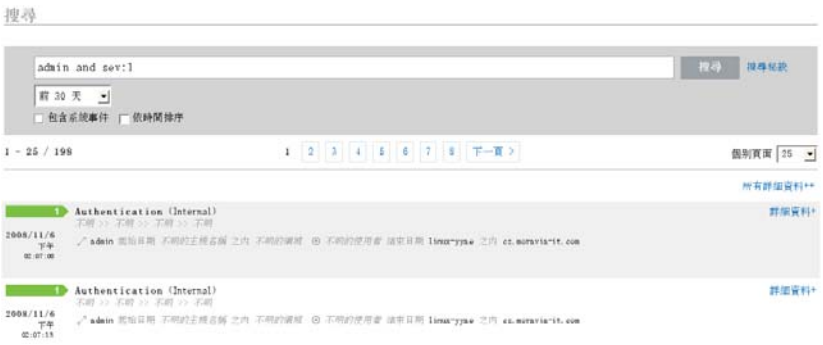
會顯示事件摘要。

4.2.2 進階搜尋

進階搜尋可搜尋一或多個特定事件欄位中是否有指定的值。進階搜尋準則是以每個事件欄位的簡稱與索引的搜尋邏輯爲基礎。下表說明搜尋欄位並提供用於執行進階搜尋的簡稱，而且會指出在基本與詳細資料事件檢視中是否會顯示特定欄位。

若要搜尋指定欄位的值，請使用欄位的簡稱 (如需詳細資訊，請參閱表格 4-1 頁上 28) 加上半形冒號與值。例如，若要搜尋 user2 對 Identity Audit 執行的驗證嘗試，請在搜尋欄位中輸入下列文字：

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



您可以使用下列布林運算子來結合多個進階搜尋準則：

- AND (必須全部大寫)
- OR (必須全部大寫)
- NOT (必須全部大寫，而且不能當成唯一的搜尋準則單獨使用)
- +
- -

特殊字元必須使用 \ 符號來進行逸出處理：

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

進階搜尋準則是以 Apache Lucene 開放原始碼套件的搜尋準則爲基礎而建立。您可以在下列網站找到更多關於搜尋準則的詳細資料：Lucene 查詢剖析器語法 (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html)。

4.3 檢視搜尋結果

搜尋會傳回一組事件。使用者可以檢視基本或詳細事件資訊，以及組態每頁的結果數目。搜尋結果是以批次方式傳回。預設批次大小是 25 個結果，但您可以輕鬆地設定批次大小。

- 「基本事件檢視」(第 26 頁)
- 「包含詳細資料的事件檢視」(第 26 頁)
- 「縮小搜尋結果範圍」(第 27 頁)

4.3.1 基本事件檢視

每個事件的資訊會根據啓始者資訊與目標資訊分組顯示。若特定事件欄位沒有資料可用，則該欄位會標示爲「*不明*」。

圖 4-2 *基本事件檢視*

有時搜尋引擎爲事件編製索引的速度可能比事件插入資料庫的速度還快。若使用者執行會傳回尚未插入資料庫之事件的搜尋，系統會顯示訊息通知使用者某些事件符合搜尋查詢，但在資料庫找不到那些事件。一般而言，若稍後再執行搜尋，就可以在資料庫中找到事件而且搜尋會成功。

圖 4-3 *已經爲事件編製索引，但事件尚未儲存至資料庫*

4.3.2 包含詳細資料的事件檢視

使用者可以點選頁面右邊的「*詳細資料*」連結，以檢視關於任何事件的其他詳細資料。使用「所有詳細資料 ++」或「*所有詳細資料 --*」連結則可以展開或摺疊頁面上所有事件的詳細資料。當您在多個搜尋結果頁面之間翻頁或執行新查詢時，會保留此優先設定。

圖 4-4 *包含詳細資料的事件檢視*

上面的事件顯示與圖 4-2 頁上 26 相同的事件，但具有展開的檢視，其中顯示可能已填入內容的額外資料欄位。

4.3.3 縮小搜尋結果範圍

檢視搜尋結果之後，您可能想要加入其他搜尋準則以縮小搜尋結果範圍。例如，您可能會看到一個啓始者使用者的名稱在搜尋結果中出現數次，而且想要檢視更多來自該啓始者的事件。

使用搜尋結果中顯示的特定值過濾搜尋結果：

1. 在搜尋結果中指出想要的過濾準則。
2. 點選要據以過濾結果的值 (例如，「目標主機名稱測試 1900」)。

提示：這樣會使用 AND 運算子將值新增至您的過濾條件。若要使用 NOT 運算子將值新增至您的過濾條件，請按住 Alt 鍵再點選值。

3. 點選 「*搜尋*」。

對於某些欄位，您無法使用此方式來縮小查詢範圍：

- EventTime
- 訊息
- 任何與 「報告人」相關的欄位
- 任何與 「觀察者」相關的欄位
- 任何具有 「不明」值的欄位

4.4 事件欄位

每個事件都會有預先填入或未預先填入內容的欄位，這取決於該特定事件。您可以使用搜尋或執行報告來檢視這些事件欄位的值。每個欄位都有可用於進階搜尋的簡稱。大部分這些欄位的的值都可以在詳細事件檢視中顯示，其他值也可以在基本事件檢視中顯示。

表格 4-1 *事件欄位*

欄位	簡稱	描述	基本檢視中可見	詳細資料檢視中可見
嚴重性	sev	事件的嚴重性，分成 0 (資訊) 到 5 (嚴重) 六個等級	X	X
EventTime	dt	事件的時戳。可以是 Identity Audit 伺服器時戳或來自原始事件來源的時戳 (若已啓用「信任事件時間」)	X	X
EventName	evt	事件的簡稱	X	X
訊息	msg	詳細的事件訊息		X
ProductName	pn	產生事件的產品；事件來源。 顯示在事件名稱後方。	X	X
InitUserName	sun	起始事件之使用者的使用者名稱	X	X
InitUserID	iuid	起始事件之使用者的使用者 ID		X
InitUserDomain	rv35	起始事件之使用者的網域 可搜尋但不會顯示在任一事件檢視		
InitHostName	shn	事件來源機器的主機名稱	X	X
InitHostDomain	rv42	事件來源機器的網域	X	X
InitIP	sip	事件來源機器的 IP 位址		X
InitServicePort	spint	事件來源的連接埠號碼 (例如，HTTP)		X
InitServicePortName	sp	事件來源的連接埠類型 (例如，HTTP)		X
TargetUserName	dun	事件目標使用者的使用者名稱	X	X
TargetUserID	tuid	事件目標使用者的使用者 ID		X
TargetUserDomain	rv35	事件目標使用者的網域 可搜尋但不會顯示在任一事件檢視		X
TargetHostName	dhn	事件目標機器的主機名稱	X	X
TargetHostDomain	rv45	事件目標機器的網域	X	X
TargetIP	dip	事件目標機器的 IP 位址		X
TargetServicePort	dpint	事件目標的連接埠號碼 (例如，80)		X
TargetServicePortName	dp	事件目標的連接埠類型 (例如，HTTP)		X
TargetTrustName	ttn	事件目標使用者的角色 (例如，FinanceAdmin) 可搜尋但不會顯示在任一事件檢視		
TargetTrustID	ttid	代表使用者爲事件之目標的角色的數值 ID 可搜尋但不會顯示在任一事件檢視		

欄位	簡稱	描述	基本檢視中可見	詳細資料檢視中可見
TargetTrustDomain	ttd	可搜尋但不會顯示在任一事件檢視		
EffectiveUserName	euname	InitUser 正在模擬之使用者的名稱 (例如，使用 su 模擬 root)；格式如詳細事件檢視中的*啓始者使用者名稱 (啓始者使用者 ID*)		X
EffectiveUserID	euid	InitUser 正在模擬之使用者的數字型 ID (例如，使用 su 模擬 root)		X
ObserverHostName	sn	將事件轉送至安全性資訊事件管理系統之機器的主機名稱 (例如，syslog 伺服器的主機名稱)		
		可搜尋但不會顯示在任一事件檢視		
ObserverHostDomain	obsdom	將事件轉送至安全性資訊事件管理系統之機器的網域 (例如，syslog 伺服器的網域)		
		可搜尋但不會顯示在任一事件檢視		
ObserverIP	obsip	將事件轉送至安全性資訊事件管理系統之機器的 IP 位址 (例如，syslog 伺服器的 IP 位址)		
		可搜尋但不會顯示在任一事件檢視		
ReporterHostName	rn	向觀察者報告事件之機器的主機名稱		
		可搜尋但不會顯示在任一事件檢視		
ReporterHostDomain	repdom	向觀察者報告事件之機器的網域		
		可搜尋但不會顯示在任一事件檢視		
ReporterIP	repip	向觀察者報告事件之機器的 IP 位址		
		可搜尋但不會顯示在任一事件檢視		
SensorType	st	感應器類型的單一字元指示項 (N= 網路、H= 主機、O= 作業系統、A 與 I=Identity Audit 稽核事件、P=Identity Audit 效能事件)。		
		可搜尋但不會顯示在任一事件檢視		
DataName	fn	事件中報告的資料物件名稱 (例如，檔案名稱或資料庫資料表名稱)		X
DataContext	rv36	FileName 資料物件 (例如，檔案的目錄，或資料庫資料表的資料庫例項) 的容器		X
TaxonomyLevel1	rv50	事件的目標類別。以下列格式顯示在事件名稱下方： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

欄位	簡稱	描述	基本檢視中可見	詳細資料檢視中可見
TaxonomyLevel2	rv51	事件的子目標類別。以下列格式顯示在事件名稱下方： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel3	rv52	事件的動作資訊。以下列格式顯示在事件名稱下方： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	事件的詳細資訊。以下列格式顯示在事件名稱下方： TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

某些欄位已記號化。將欄位記號化讓您無須使用萬用字元，即可搜尋欄位中的個別單字。欄位是根據空格與其他特殊字元來記號化。對於這些欄位，會從搜尋索引移除 “a” 或 “the” 之類的冠詞。

- EventName
- 訊息
- ProductName
- FileName
- DataContext
- TaxonomyLevel1
- TaxonomyLevel2
- TaxonomyLevel3
- TaxonomyLevel4

報告

5

本章說明如何在 Novell® Identity Audit 中執行、檢視與管理報告。

5.1 綜覽

安裝 Identity Audit 時會一併安裝一組與 Novell 應用程式相關的核心報告樣板。任何 Identity Audit 使用者都可以使用想要的參數 (例如開始與結束日期) 來執行報告，而報告結果會以使用者選擇的名稱儲存。執行報告之後，任何 Identity Audit 使用者都可以取回該報告並以 PDF 檔案的方式檢視。

報告會依類別組織。安裝 Identity Audit 時會一併安裝每個支援之事件來源的報告。

圖 5-1 依類別組織的報告

5.2 執行報告

安裝 Identity Audit 時會一併安裝一組分爲數個產品類別的報告。報告會以非同步方式執行，因此使用者可以在執行報告時繼續使用其應用程式執行其他作業。報告執行完成後，任何使用者都可以檢視 PDF 報告結果。

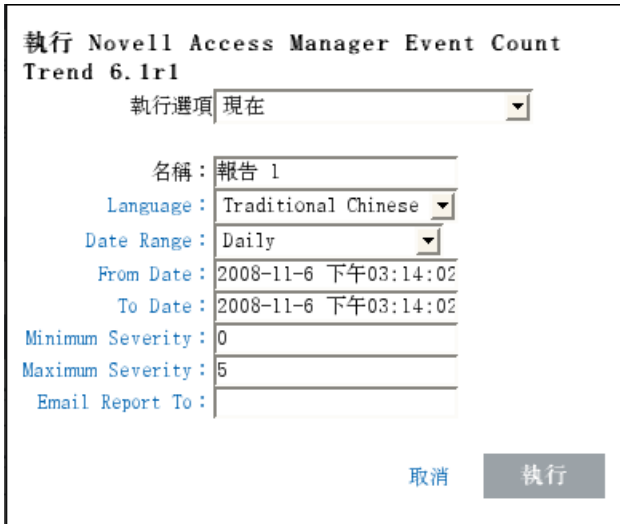
許多報告定義都包含參數。當使用者執行報告時，系統會提示使用者設定這些參數。視報告開發人員設計報告的方式而定，報告參數可以是文字、數字、布林值或日期。視 Identity Audit 資料庫中的值而定，參數可以是預設值或選擇清單。

執行報告：

1 在 Identity Audit 中，點選「*報告*」以顯示可用的報告。

您也可以點選報告定義將它展開。若看到「*範例報告*」，您可以點選「*檢視*」預覽範例資料在報告上的顯示方式。

2 選取您要執行的報告，並點選「*執行*」。



3 設定報告執行排程。若要稍後執行報告，您也必須輸入開始時間。

- 現在：這是預設值。選擇此設定可立即執行報告。
- 一次：選擇此設定會在指定的日期與時間執行一次報告。
- 每日：選擇此設定會每天執行報告 (在指定的時間)。
- 每週：選擇此設定會每週執行報告 (在每天指定的時間)。
- 每月：選擇此設定可在每月的同一天執行報告 (從指定的日期與時間開始)。例如，若開始日期與時間是 10 月 28 日下午 2 點，報告將會在每月第 28 天的下午 2 點執行。

附註：所有時間設定都是以瀏覽器的本機時間爲基礎。

4 輸入可用來識別報告結果的名稱。

因爲使用者名稱與時間也會用來識別報告結果，報告名稱不需要是唯一的。

5 選擇要用來顯示報告的語言 (英文、法文、德文、義大利文、日文、繁體中文、簡體中文、西班牙文或葡萄牙文)。

6 選擇報告類型。所有期間都是以瀏覽器的本機時間爲基礎。

- 每日：報告會顯示從當天凌晨到 23:59 的事件。若目前時間是上午 8 點，報告會顯示 8 小時的資料。
- 每週：報告會顯示從當週星期日凌晨到當天結束的事件。
- 每月：報告會顯示從當月第一天凌晨到當天結束的事件。
- 自定日期範圍：(僅適用於此設定) 您也必須在下面設定開始日期與結束日期。
- 前一日：報告會顯示從昨天凌晨到昨天晚上 23:59 的事件。

7 若選取「自定日期範圍」，請設定報告的「起始日期」與「結束日期」。

附註：若爲報告類型選取「每日」、「每週」、「每月」或「前一日」，會忽略這些時間設定。

8 設定要在報告中包含之事件的嚴重性層級下限。

9 設定要在報告中包含之事件的嚴重性層級上限。

10 若要使用電子郵件將報告寄給一或多個使用者，請輸入其電子郵件地址 (使用逗號分隔多個電子郵件地址)。

附註：若要啓用報告郵寄功能，管理員必須在「*規則* > *組態*」下組態郵件傳送。

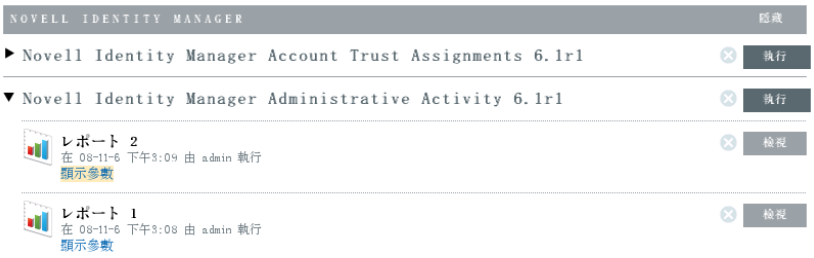
11 點選「*執行*」。

系統會建立報告結果項目，並使用電子郵件將報告寄給指定的收件人。

5.3 檢視報告

Identity Audit 使用者可以在 Identity Audit 應用程式中檢視報告。其他使用者可能可以接收以 .pdf 檔案格式傳送的報告。

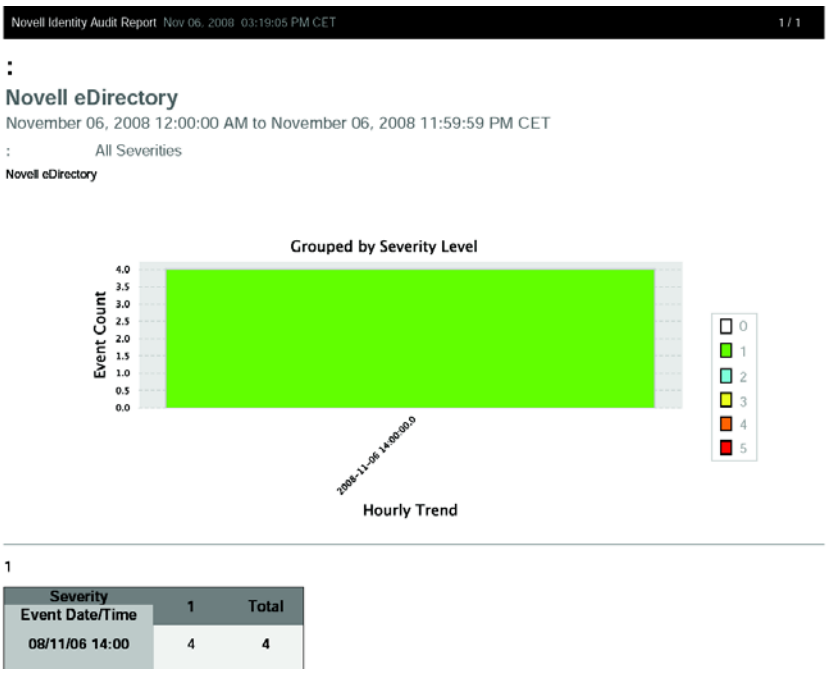
1 若要檢視報告結果清單，請點選「*檢視*」。顯示所有先前執行的報告時會一併顯示使用者定義的報告名稱、執行報告的使用者，以及執行報告的時間。



2 點選「*顯示參數*」以檢視用於執行報告的參數值。

- 對於「報告類型」，D= 每日、W= 每週、M= 每月、DR= 自定日期範圍，而 PD= 前一日。
- 對於「語言」，en= 英文、fr= 法文、de= 德文、it= 義大利文、ja= 日文、pt= 葡萄牙文 (巴西)、es= 西班牙文、zh= 簡體中文，而 zh_TW= 繁體中文。

3 針對您要檢視的報告結果點選「*檢視*」。報告結果會以 .pdf 格式顯示在新視窗中。



提示：報告結果是從最新到最舊排序。

5.4 管理報告

Identity Audit 使用者可以新增、刪除、更新與排程報告。

- 「新增報告」(第 35 頁)
- 「重新命名報告結果」(第 36 頁)
- 「刪除報告」(第 37 頁)
- 「更新報告定義」(第 37 頁)

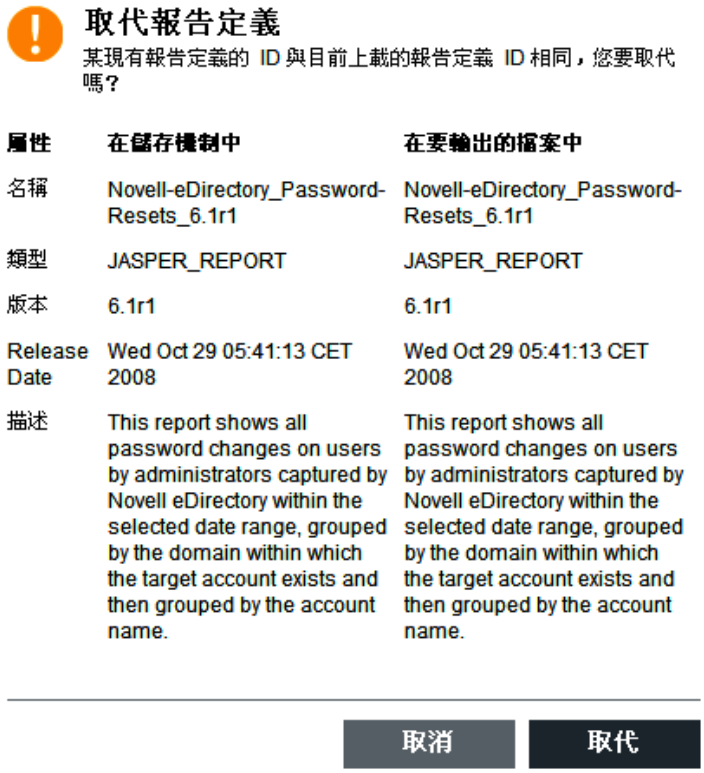
5.4.1 新增報告

Identity Audit 隨附一些報告，但您也可以將新的報告外掛程式 (包含報告定義與中繼資料的特殊 .zip 檔案) 上載到 Identity Audit。若系統中沒有報告，會顯示下列畫面：

圖 5-2 未載入任何報告

新增報告：

1. 點選畫面左邊的「*報告*」按鈕。
2. 點選「*上載報告*」按鈕。
3. 瀏覽至本機機器上報告外掛程式 .zip 檔案的位置。
4. 點選「*開啓*」。
5. 點選「*儲存*」。
6. 若報告儲存機制中已經有相同的報告 (以報告的唯一 ID 爲準)，Identity Audit 會顯示系統中的報告與要輸入的報告之詳細資料。使用者可以決定是否要取代現有的報告。在下面的案例中，輸入之報告的版本與現有報告的版本相同。



7 新的報告定義會以字母順序新增至清單，而且可以立即執行。

下載新報告或已更新的報告

您可以從 Novell 內容網站 (http://support.novell.com/products/identityaudit/identityaudit10.html) 下載 Novell 所提供的新報告或更新的報告。

建立新報告

使用者可以使用 JasperForge* iReport 修改或建立報告，這是一個適用於 Jasper 報告的報告設計工具。iReport 是一個開放原始碼報告開發工具，您可以從 JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) (此文件發佈當時) 下載此工具。

新報告或修改的報告可以包含 Identity Audit Web 介面中沒有的額外資料庫欄位。它們必須符合報告外掛程式的檔案與格式需求。如需有關適用於報告外掛程式之資料庫欄位與檔案和格式需求的詳細資訊，請參閱 Sentinel SDK 網站 (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel)。

5.4.2 重新命名報告結果

您可以在 Identity Audit 介面中重新命名報告結果 (但無法重新命名報告定義)。

1 點選畫面左邊的「*報告*」按鈕。
2 點選報告名稱將它展開。
3 點選您要重新命名的報告結果名稱。

4 輸入新名稱。

5 點選 *「重新命名」*。

5.4.3 刪除報告

使用者可以刪除報告結果組或報告定義。若刪除報告定義，也會刪除所有相關的報告結果。

若正在刪除報告，會取消在資料庫上執行的查詢。

5.4.4 更新報告定義

使用者可以上載更新的報告至 Identity Audit 以取代現有的報告。如需詳細資訊，請參閱「新增報告」(第 35 頁)。

資料集合

6

管理員可以設定並監控 Novell® Identity Audit 的資料集合。安裝 Identity Audit 時會一併安裝 Novell Audit Platform Agent，它可以讓您從各種 Novell 應用程式收集資料。如需支援之 Platform Agent 版本的詳細資訊，請參閱 「支援的 Platform Agent」(第 14 頁)。

6.1 組態事件來源

雖然 Identity Audit 預先組態爲從許多 Novell 應用程式接收資料，您必須設定應用程式伺服器 (事件來源) 將資料傳送給 Identity Audit 伺服器。這是 Identity Audit 基本安裝的一部分。如需詳細資訊，請參閱 「設定事件來源」(第 18 頁)。

6.2 資料集合狀態

管理員可以啓用或停用所有應用程式或個別應用程式的資料集合，也可以檢視每個應用程式的狀態資訊。

1 以管理員身分登入 Identity Audit。

2 點選頁面右上角的「*集合*」。

3 啓用或停用 Audit Server 從所有應用程式收集資料的功能。

4 啓用或停用從事件來源的個別應用程式收集資料的功能。

5 點選「*顯示詳細資料*」檢視關於每個應用程式之使用中連線的更多資訊。

在此頁面所做的變更會立即生效。

- 「Audit 伺服器」(第 40 頁)
- 「事件來源」(第 40 頁)

6.2.1 Audit 伺服器

管理員可以使用「*Audit Server*」區段中的「開啓」與「關閉」選項來啓用或停用全域層級的資料集合。也會顯示 Audit Server 的狀態。

狀態良好：綠色指示器表示 Audit Server 的狀態良好 (已開啓、正在監聽連接埠，而且沒有任何未解決的錯誤)。

錯誤：紅色指示器表示 Audit Server 發生錯誤。如需詳細資訊，請檢視 server0.*.log 檔案。

離線：灰色指示器表示管理員已將 Audit Server 離線。

6.2.2 事件來源

管理員可以在「*事件來源*」區段啓用應用程式層級的資料集合。這些設定可能會影響數部伺服器 (例如，數個 eDirectory 例項) 的資料集合。

附註：這些設定可啓用 (或停用) Identity Audit 從列出的應用程式收集資料的功能。它們不會啓動或停止事件來源機器的服務。

每個圖示的狀態都會以紅色、黃色、綠色或黑色圖示表示。對於大部分的狀態，您可以點選「*顯示詳細資料*」檢視詳細資訊。

狀態良好：綠色指示器表示事件來源的狀態良好，而且 Identity Audit 已從該事件來源接收資料。

警告：黃色指示器表示發生警告狀況。常見原因是應用程式已在 Identity Audit 開啓，但並未傳送任何資料。例如，若未正確地組態事件來源上的 Platform Agent 以傳送資料到 Identity Audit，或未針對應用程式啓用事件記錄功能，就會發生這種情況。點選「*顯示詳細資料*」，即可取得更多的資訊。

錯誤：紅色指示器表示 Identity Audit 伺服器連接到此應用程式或從此應用程式接收資料時發生錯誤。點選「*顯示詳細資料*」，即可取得更多的資訊。

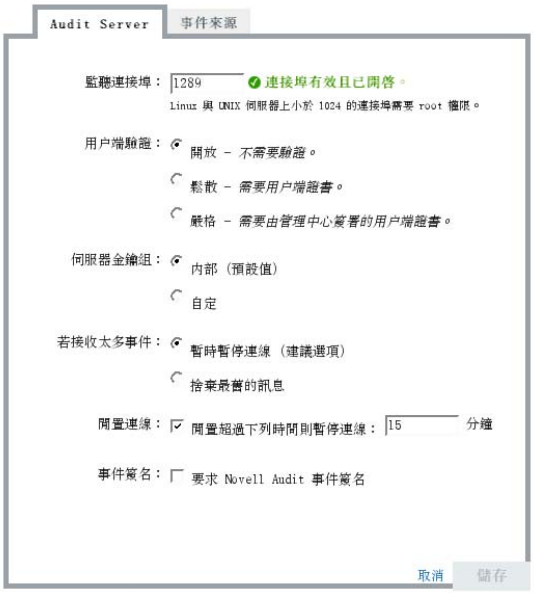
離線：灰色指示器表示事件來源已關閉。Identity Audit 並未處理來自該事件來源的任何資料。

對於每個線上資料來源，Identity Audit 會顯示內送事件的計算事件速率。事件速率每隔 60 秒會重新計算。

6.3 Audit Server 選項

管理員可以變更一些關於 Identity Audit 如何監聽來自事件來源應用程式之資料的設定，包括 Identity Audit 監聽的連接埠，以及事件來源與 Identity Audit 之間的驗證類型。

1. 以管理員身分登入 Identity Audit。
2. 點選畫面頂端的「*集合*」連結。
3. 點選畫面右邊的「*組態*」連結。
4. 確定已選取「*Audit Server*」。



5 輸入 Identity Audit 伺服器將用來監聽事件來源訊息的連接埠。如需詳細資訊，請參閱「連接埠組態與連接埠轉送」(第 41 頁)。

6 設定適當的用戶端驗證與伺服器金鑰組設定。如需詳細資訊，請參閱「用戶端驗證」(第 42 頁)。

7 選取 Identity Audit 伺服器偵測到緩衝區中塞滿太多事件時的處理方式。

暫時暫停連線：此設定會捨棄現有的連線並停止接受新連線，直到緩衝區有空間可以接受新訊息。同時，訊息會由事件來源放入快取。

捨棄最舊的訊息：此設定會捨棄最舊的訊息，以接受新訊息。

警告：若選取「*捨棄最舊的訊息*」，將沒有任何支援的方式可復原捨棄的訊息。

---

8 選取「*閒置連線*」可解除超過特定時間未傳送資料之事件來源的連線。

當事件來源開始重新傳送資料時，會自動建立事件來源連線。

9 輸入當連線閒置多久之後即中斷連線 (單位：分鐘)。

10 選取「*事件簽名*」即可隨著事件接收簽名。

附註：若要接收簽名，必須正確地組態事件來源上的 Platform Agent。有關更詳細的資訊，請參閱「組態事件來源」(第 39 頁)。

---

11 點選「*儲存*」。

6.3.1 連接埠組態與連接埠轉送

Identity Audit 預設使用連接埠 1289 來監聽來自 Platform Agent 的訊息。設定連接埠之後，系統會檢查該連接埠是否有效且已開啓。

繫結至小於 1024 的連接埠時需要 root 權限。因此，Novell 建議您使用大於 1024 的連接埠。您可以變更來源裝置，使其傳送到較高的連接埠，或在 Identity Audit 伺服器上使用連接埠轉送。

變更事件來源以傳送到不同的連接埠：

1. 登入事件來源機器。
2. 開啓 logevent 檔案以進行編輯。此檔案的位置在不同的作業系統上會不一樣：
   - Linux：/etc/logevent.conf
   - Windows：C:\WINDOWS\logevent.cfg
   - NetWare：SYS:\etc\logevent.cfg
   - Solaris：/etc/logevent.conf
3. 將 LogEnginePort 參數設定爲想要使用的連接埠。
4. 儲存檔案。
5. 重新啓動 Platform Agent。重新啓動方式視作業系統與應用程式而定。將機器重新開機，或參閱 Novell 文件網站 (http://www.novell.com/documentation) 的應用程式特定文件以取得詳細指示。

在 Identity Audit 伺服器上設定連接埠轉送。

1. 以 root (或 su 爲 root) 登入 Identity Audit 伺服器作業系統。
2. 開啓 /etc/init.d/boot.local 檔案以進行編輯。
3. 新增下面的指令到開機 (bootup) 程序的結尾附近：
   ```
   iptables -A PREROUTING -t nat -p protocol --dport incoming port -j
   DNAT --to-destination IP:rerouted port
   ```
   其中 *protocol* 是 tcp 或 udp，*incoming port* 是訊息送達的連接埠，而 *IP:rerouted port* 是本機機器的 IP 位址以及大於 1024 的可用連接埠
4. 儲存變更。
5. 重新開機。若無法立即重新開機，請從指令行執行上面的 iptables 指令。

6.3.2 用戶端驗證

事件來源會透過 SSL 連接傳送資料，而 Identity Audit 伺服器的「*用戶端驗證*」設定會決定要針對來自事件來源之 Platform Agent 的證書使用哪種驗證方式。

開放：不需要驗證。Identity Audit 不會要求、取得或驗證事件來源的證書。

鬆散：事件來源必須提供有效的 X.509 證書，但 Identity Audit 並不會驗證該證書。此外，該證書也不需要由證書管理中心簽署。

嚴格：事件來源必須提供有效的 X.509 證書，而且該證書必須已由信任的證書管理中心簽署。若事件來源未提供有效的證書，Identity Audit 將不會接受其事件資料。

- 「建立託管儲存」(第 43 頁)
- 「輸入託管儲存」(第 43 頁)
- 「伺服器金鑰組」(第 44 頁)

建立託管儲存

對於「嚴格」驗證方式，您必須有託管儲存，其中必須包含事件來源的證書，或是簽署事件來源證書之證書管理中心 (CA) 的證書。取得 DER- 或 PEM- 證書之後，您就可以使用 Identity Audit 隨附的 CreateTruststore 公用程式來建立託管儲存。

1. 以 novell 的身分登入 Identity Audit 伺服器。
2. 移至 /opt/novell/identity_audit_1.0_x86/data/updates/done。
3. 解除壓縮 audit_connector.zip 檔案。

   unzip audit_connector.zip
4. 將 TruststoreCreator.sh 或 TruststoreCreator.bat 複製到證書所在機器，或將證書複製到 TruststoreCreator 公用程式所在機器。
5. 執行 TruststoreCreator.sh 公用程式。

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

   在此範例中，TruststoreCreator 公用程式會建立名爲 my.keystore 的 keystore 檔案，其中包含兩個證書 (cert1.pem 與 cert2.pem)。此外，該檔案受密碼保護，密碼是 *password1*。

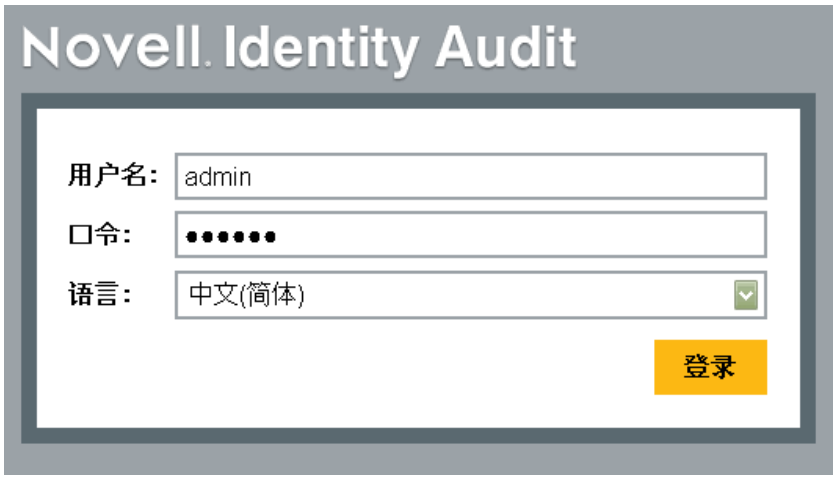
輸入託管儲存

對於「嚴格」驗證方式，管理員可以使用「*輸入*」按鈕輸入託管儲存。這可協助確保只有授權的事件來源可傳送資料到 Identity Audit。託管儲存必須包含事件來源的證書，或是簽署事件來源證書之證書管理中心的證書。

您必須在託管儲存所在機器上執行下列程序。您可以在託管儲存所在機器上開啓網頁瀏覽器，或將託管儲存移動到已安裝網頁瀏覽器的機器。

輸入託管儲存：

1. 以管理員身分登入 Identity Audit。
2. 點選畫面頂端的「*集合*」連結。
3. 點選畫面右邊的「*組態*」連結。
4. 確定已選取「*Audit Server*」索引標籤。
5. 選取「*用戶端驗證*」下的「*嚴格*」選項。

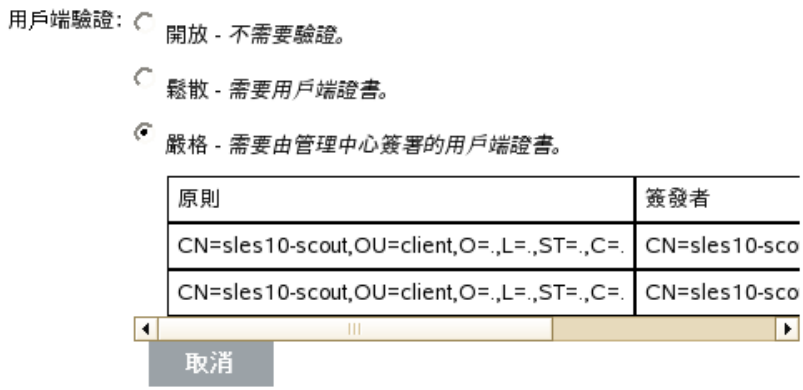


6 點選「*瀏覽*」並瀏覽到託管儲存檔案 (例如，my.keystore)

7 輸入託管儲存檔案的密碼。

8 點選「*輸入*」。

9 點選「*詳細資料*」以檢視關於託管儲存的詳細資訊。



10 點選「*儲存*」。

成功地輸入託管儲存之後，您可以點選「*詳細資料*」以檢視託管儲存中包含的證書。

伺服器金鑰組

安裝 Identity Audit 時會一併安裝內建的證書，Identity Audit 伺服器可使用此證書向來源伺服器證明自己的身分。您可以使用由公用證書管理中心 (CA) 所簽署的證書來覆寫此證書。

取代內建的證書：

1 以管理員身分登入 Identity Audit。

2 點選畫面頂端的「*集合*」連結。

3 點選畫面右邊的「*組態*」連結。

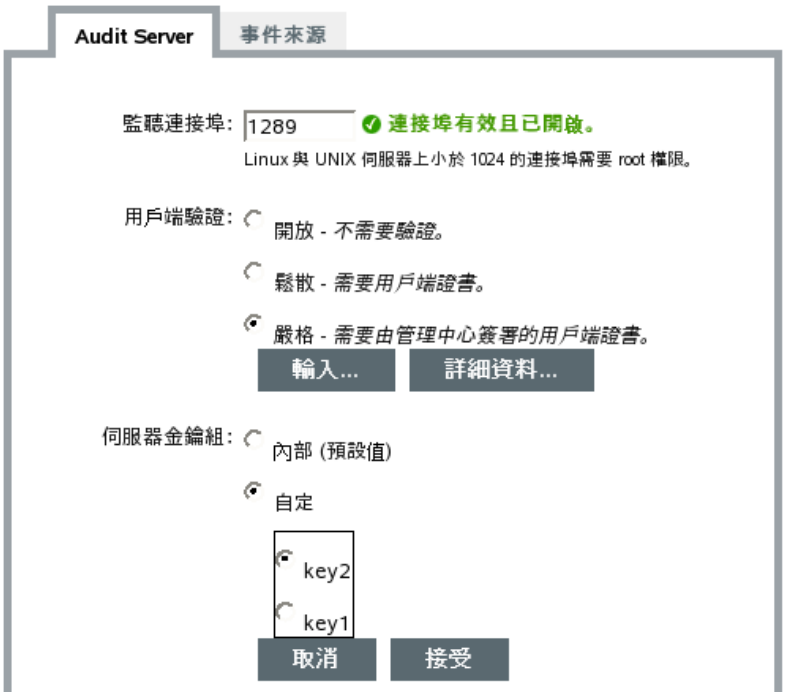
4 確定已選取「*Audit Server*」。

5 在「*伺服器金鑰組*」下，選取「*自定*」。

6 點選「*瀏覽*」並瀏覽至託管儲存檔案。

7 輸入託管儲存檔案的密碼。

8 點選「*輸入*」。



若檔案中有多個公用 - 私密金鑰組，請選取想要的金鑰組，然後點選「*確定*」。

9 點選「*詳細資料*」檢視關於伺服器金鑰組的詳細資訊。

10 點選「*儲存*」。

6.4 事件來源

管理員可以使用「*事件來源*」頁面來組態如何決定來自每個事件來源之事件的時間。事件時間能以事件來源的時戳爲基礎 (「信任事件時間」)，或以來自 Identity Audit 伺服器的時戳爲基礎。時戳會影響事件在搜尋結果中的顯示順序 (若您選擇依時間排序)。時戳也會影響報告中的顯示時間。預設值是使用 Identity Audit 伺服器時間。

附註：建議使用 NTP 伺服器來同步 Identity Audit 系統中所有機器的時間。若有 NTP 伺服器可以使用，Novell 建議您信任應用程式的事件時間。若沒有可用的 NTP 伺服器，Novell 建議您爲所有應用程式使用 Identity Audit 伺服器時間 (預設設定)，來校正機器之間的時間差異。

變更事件時間選項：

1 以管理員身分登入 Identity Audit。

2 點選畫面頂端的「*集合*」連結。

3 點選畫面右邊的「*組態*」連結。

4 點選「*事件來源*」。

5 選取要讓 Identity Audit 使用來自原始應用程式之事件時戳的所有應用程式。

對於所有其他項目，Identity Audit 伺服器時戳會取代原始應用程式的時戳。

您所做的變更會立即套用到所有新的內送事件。對於佇列中的待處理事件，則可能需要一些時間才會生效。

資料儲存

7

Novell® Identity Audit 安裝程式會安裝 PostgreSQL 資料庫，並建立執行 Identity Audit 所需的所有資料表與使用者。該資料庫也包含設計來管理資料庫分割區與將舊資料歸檔的預存程序。管理員可以透過網頁介面來管理資料庫儲存與歸檔設定。

- 「資料庫狀態」(第 47 頁)
- 「資料儲存組態」(第 47 頁)

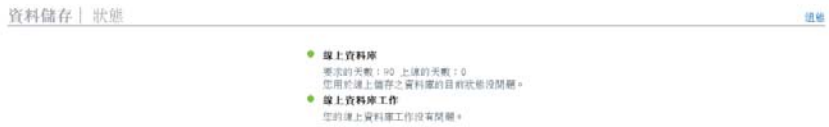
7.1 資料庫狀態

「資料儲存狀態」頁面 (只有管理員可存取) 可顯示資料庫的狀態，系統判斷資料庫狀態是否良好的條件包括資料庫中可用的分割區數目，以及建立新分割區與歸檔資料 (若已設定) 之預存程序的成功數目。

檢視資料庫狀態：

1. 以管理員身分登入 Identity Audit。
2. 點選頁面右上角的「儲存」連結。

   此時會顯示狀態頁面。



此頁面會顯示數個資料庫功能的狀態爲良好狀態 (綠色)、警告狀態 (黃色) 或錯誤狀態 (紅色)。

線上資料庫：此指示器顯示資料庫中每個已分割的資料表是否有預期的分割區數目。預期的分割區數目取決於設定要上線的天數 (對於最近的安裝，則是安裝之後經過的天數)。

若分割區數目不是預期的數目，此頁面會顯示資料表名稱、預期的分割區數目，以及資料庫中實際的分割區數目。

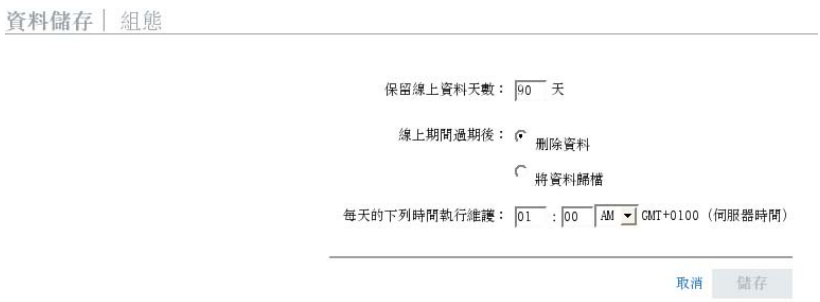
線上資料庫工作：若上次執行儲存程序以新增分割區並刪除資料時發生錯誤，此指示器會變成紅色。若啓用歸檔，此指示器只會顯示上次執行新增分割區的工作時是否發生錯誤。若發生錯誤，頁面會顯示與失敗之工作相關的名稱、時戳與詳細資料。

歸檔資料庫：只有啓用歸檔時才會顯示此指示器。若上次執行儲存程序以歸檔資料時發生錯誤，它會變成紅色。若發生錯誤，頁面會顯示與失敗之工作相關的名稱、時戳與詳細資料。

7.2 資料儲存組態

資料庫是一個儲存機制，可以儲存內送事件、組態資訊與報告結果。Identity Audit 提供資料庫管理程序，以防止資料庫被塞滿。「資料儲存」頁面 (只有管理員可存取) 可讓您設定數種資料儲存組態。

圖 7-1 資料儲存組態



保留線上資料天數：管理員可指定要在資料庫中保留報告用途資料的天數。最小值是一天，而且您只能指定整數 (不能指定含小數點的數字)。

線上期間過期後：線上資料的保留期間過期後，任何超過該期間的事件資料都會被刪除或從資料庫移至歸檔目錄。

警告：Novell 不支援復原已刪除的資料，因此選擇 「刪除」選項時請小心。

歸檔到此資料庫目錄：若選擇 「*將資料歸檔*」選項，請指定將用來寫入已歸檔資料的現有目錄位置。此目錄必須已存在，而且 novell 使用者必須具有此目錄的寫入存取權。根據預設，此位置是設定爲 Identity Audit 主目錄中的 /data/db_archive。具有適當許可的預設目錄是在 Identity Audit 安裝期間所建立。

重要：Novell 建議您定期將歸檔檔案移動到長期儲存位置，避免它們佔用硬碟空間。

測試：若選擇 「*將資料歸檔*」選項，可使用 「測試」按鈕來檢查歸檔目錄是否存在以及是否可供 novell 使用者寫入。

每天的下列時間執行維護：指定每天執行例行維護作業的時間。時間是以 Identity Audit 伺服器的本機時間爲準。在編程的維護時間，會執行預存程序以新增分割區到資料庫。兩個小時後，會執行預存程序以將存留時間超過指定保留期間的資料歸檔或刪除。

您應該將資料歸檔作業安排在每天資料庫使用量相對低的時間執行。

規則

8

本章說明可用來從 Identity Audit 傳送事件到另一個系統的事件通道。

8.1 規則綜覽

「規則」介面可讓您定義規則，以評估所有內送事件，並將選取的事件傳送到指定的輸出通道。例如，您可以將每個嚴重性層級爲 5 的事件以電子郵件寄給安全分析人員配送清單或管理員。

附註：所有事件也都會傳送到資料庫。

系統會根據每個過濾規則依序評估內送事件，直到發現符合的事件，然後執行與該規則相關的傳送動作：

傳送給電子郵件：使用組態的 SMTP 傳送將事件傳送給一或多個使用者

寫入檔案：將事件寫入 Identity Audit 伺服器上指定的檔案中

傳送給 Syslog：將事件轉送給設定的 syslog 伺服器

提示：相關的動作會一次處理多個事件。因此，選取將用來傳送事件的輸出通道時請考慮可能會對效能造成的負面影響。例如，「寫入檔案」動作使用最少系統資源，因此傳送大量事件到電子郵件或 syslog 之前，可以先使用此動作來測試規則準則以判斷資料量。

此外，當您設定「傳送給電子郵件」動作時，應該考慮收件人可有效處理的事件數量，然後據以調整過濾規則。

事件輸出是 JavaScript Object Notation (JSON) 格式，這是一種輕量型資料交換格式。事件是由欄位名稱 (例如 "evt" 代表「事件名稱」) 加上半形冒號和值 (例如 "Start") 組成，事件之間則以半形逗號分隔。

{"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 設定規則

您可以設定 Identity Audit 規則，根據一或多個可搜尋的欄位來過濾事件。如需 Identity Audit 的可搜尋的事件欄位清單，請參閱表格 4-1 頁上 28。每個規則可以與一或多個組態的動作相關聯。

- 「新增規則」(第 50 頁)
- 「排列規則順序」(第 50 頁)
- 「刪除規則」(第 51 頁)
- 「啓動或取消啓動規則」(第 51 頁)

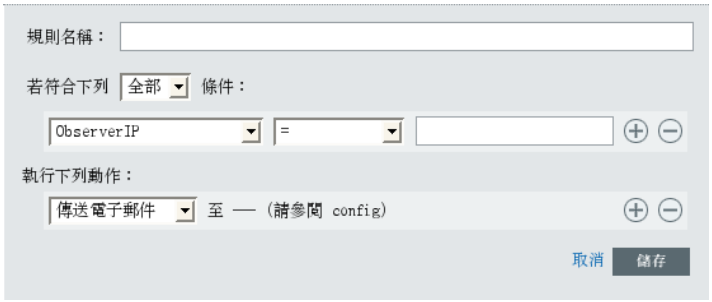
8.2.1 過濾準則

規則能以任何可搜尋的事件欄位爲基礎。如需這些欄位的清單，請參閱表格 4-1 頁上 28。可用的運算子取決於事件欄位的資料類型。例如，「符合子網路」適用於 IP 位址，而「符合正規運算式」則適用於文字欄位。

8.2.2 新增規則

管理員可以新增以過濾器爲基礎的規則，然後針對符合規則準則的事件定義一或多個輸出通道。

1. 以管理員身分登入 Identity Audit。
2. 點選頁面右上角的「*規則*」。
3. 點選「*新增規則*」。
4. 輸入規則名稱。
5. 若要建立多個條件，請選取「*全部*」以使用 AND 運算子來結合條件。選取「*任何*」，則可以使用 OR 運算子來結合條件。
6. 爲過濾器選取事件欄位、運算子與值。



7. 選取要在每個符合過濾準則之事件上執行的動作。

   點選「*組態*」連結可檢視以組態資訊爲基礎的動作詳細資料。
8. 視需要組態其他動作。
9. 點選「*儲存*」。

8.2.3 排列規則順序

因爲規則會依序評估事件直到發現符合的事件，Novell 建議您適當地排列規則順序。您應該將條件較嚴格的規則以及較重要的規則放在清單開頭。當清單中有多個規則時，您可以使用拖放方式來重新排列規則順序。

重新排列規則順序

1. 以管理員身分登入 Identity Audit。

2 點選頁面右上角的「*規則*」。

3 將滑鼠游標移到規則編號左邊的圖示上方可啓用拖放功能。游標會變更。

4 將規則拖放到已正確排列順序之清單中的適當位置。

8.2.4 刪除規則

刪除規則時，若佇列中已經有準備執行動作的事件，取消啓動規則之後可能需要一些時間才能衝洗該佇列。

8.2.5 啓動或取消啓動規則

每個規則的左邊 (欄標題爲「開啓」) 都有可用來啓動規則的核取方塊。新規則預設是啓動的。若取消啓動規則，則不會再根據該規則來評估內送事件。若佇列中已經有準備執行動作的事件，取消啓動規則之後可能需要一些時間才能衝洗該佇列。

8.3 設定動作

當事件符合任一規則指定的準則時，該事件會被傳送到一或多個通道。您必須先使用適當的連線資訊 (如果是 SMTP 傳送，您可能還必須設定驗證證書) 組態傳送到通道的動作，事件才能輸出到通道。在 Identity Audit 系統中，您只能針對每個動作類型設定一個連線 (例如，寫入至檔案的所有事件必須寫入至相同檔案)。

- 「傳送給電子郵件」(第 51 頁)
- 「傳送給 Syslog」(第 52 頁)
- 「寫入檔案」(第 53 頁)

8.3.1 傳送給電子郵件

若要設定「傳送給電子郵件」動作，您必須有 SMTP 傳送的連線資訊 (IP 位址與連接埠號碼)，以及「收件者」與「寄件者」地址。您可以輸入以逗號分隔的清單，來傳送給一個以上的電子郵件地址。

附註：爲避免造成 SMTP 郵件主機或電子郵件收件人的負擔，建議您不要在會產生大量事件的規則使用此動作。

系統也會使用 SMTP 傳送組態來傳送報告給使用者。

1 以管理員身分登入 Identity Audit。

2 點選頁面右上角的「*規則*」。

3 點選「*組態*」。

4 在「*電子郵件*」下，輸入可用之 SMTP 傳送的名稱與連接埠。您可以點選「*測試*」來測試連線。

5 若 SMTP 傳送需要驗證，請輸入使用者名稱與密碼。

6 輸入電子郵件訊息的寄件者。

7 輸入一或多個電子郵件地址 (若輸入多個地址，請使用逗號分隔每個地址)。

8 點選「*儲存*」。

符合已定義「傳送給電子郵件」動作之過濾準則的所有 Identity Audit 事件，都會傳送至相同的 SMTP 傳送與地址組。

8.3.2 傳送給 Syslog

若要組態「傳送給 Syslog」動作，您將需要 syslog 伺服器的連線資訊 (IP 位址與連接埠號碼)。

1 以管理員身分登入 Identity Audit。

2 點選頁面右上角的「*規則*」。

3 點選「*組態*」。

4 在「*Syslog*」下，輸入 syslog 伺服器的名稱或 IP 位址，以及開啓的連接埠。您可以點選「*測試*」，測試目的伺服器與連接埠是否存在。

5 點選「*儲存*」。

符合已定義「傳送給 Syslog」動作之過濾準則的所有 Identity Audit 事件，都會傳送至相同的 syslog 伺服器。

8.3.3 寫入檔案

若要設定「寫入檔案」動作，您需要將用來寫入事件之檔案的名稱與路徑。此目錄必須已存在，而且 novell 使用者必須具有此目錄的寫入許可。若該檔案不存在，Identity Audit 將會建立該檔案。

1. 以管理員身分登入 Identity Audit。
2. 點選頁面右上角的「*規則*」。
3. 點選「*組態*」。
4. 在「*檔名*」下，輸入要用來寫入事件之檔案的路徑。您可以點選「*測試*」來測試連線。

5. 點選「*儲存*」。

符合已定義「寫入檔案」動作之過濾準則的所有 Identity Audit 事件，都會寫入至相同的檔案。

使用者管理

9

管理員可以在 Novell® Identity Audit 中新增、編輯與刪除使用者，也可以授予管理權限。使用者可以編輯其使用者設定檔的詳細資料。

9.1 新增使用者

在 Identity Audit 系統新增使用者會建立應用程式使用者，接著該使用者便可以登入 Identity Audit 應用程式。

選取「*授予管理權限*」選項可將 Identity Audit 系統的管理權限授予使用者。管理權限包含管理下列功能的能力：

- 使用者管理
- 資料集合
- 資料儲存

若要新增使用者：

1. 以管理員身分登入 Identity Audit。
2. 點選頁面右上角的「*使用者管理*」。
3. 點選「*新增使用者*」。
4. 輸入使用者資訊。

具有星號 (*) 的欄位是必要欄位，而且使用者名稱必須是唯一的。

附註：系統會驗證電子郵件地址格式，但電話號碼欄位則接受任何格式。請確定您輸入有效的電話號碼。

5. 您可以視需要選取「*授予管理權限*」。
6. 點選「*儲存*」。

9.2 編輯使用者詳細資料

管理員可以編輯系統中任何使用者的使用者資訊。所有使用者都可以編輯其設定檔中的所有欄位，但使用者名稱與管理員狀態兩個欄位除外。使用者也可以變更密碼。

- 「編輯您自己的設定檔」(第 56 頁)
- 「變更您自己的密碼」(第 56 頁)
- 「編輯其他使用者的設定檔 (僅限管理員)」(第 57 頁)
- 「重設其他使用者的密碼 (僅限管理員)」(第 57 頁)

9.2.1 編輯您自己的設定檔

1 點選右上角的「*設定檔*」。

2 編輯任何可用的欄位。

3 點選「*儲存*」。

9.2.2 變更您自己的密碼

若使用者知道自己目前的密碼，就可以變更密碼。否則，必須要求管理員協助重設密碼。

1 點選右上角的「*設定檔*」。

2 輸入目前的密碼。

3 輸入新密碼。

4 確認您的新密碼。

5 點選「*儲存*」。

9.2.3 編輯其他使用者的設定檔 (僅限管理員)

1 以管理員身分登入 Identity Audit。
2 點選頁面右上角的「*使用者管理*」。
3 點選您要編輯之使用者下方的「*編輯*」。
4 編輯任何欄位 (「使用者名稱」除外)。
5 點選「*儲存*」。
對於「*授予管理權限*」所做的變更會在下次使用者登入時生效。

9.2.4 重設其他使用者的密碼 (僅限管理員)

若要重設其他使用者的密碼，請參閱「編輯其他使用者的設定檔 (僅限管理員)」(第 57 頁)。

9.3 刪除使用者

管理員可以將使用者從系統刪除。

1 以管理員身分登入 Identity Audit。
2 點選頁面右上角的「*使用者管理*」。
3 點選您要刪除之使用者下方的「*編輯*」。
4 點選頁面右上角的「*刪除此使用者*」。
5 點選「*刪除*」進行確認。

託管儲存

A

在 Identity Audit 與其資料收集來源 Novell 應用程式之間的連線使用「嚴格」驗證方式可提高資料安全性。

A.1 建立 Keystore

您可以使用 Java 的 "keytool" 可執行檔 (安裝 jre 時會一併安裝此可執行檔) 來建立 keystore。這個 keystore 儲存了公用與私密金鑰組，您可以使用此金鑰組來取代 Identity Audit 隨附的預設證書。以下是基本指示，如需關於 keytool 的詳細資訊，請參閱 Sun 網站 (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html)。

1. 移至 Java 的 /bin 目錄 (例如，$JAVA_HOME/bin)。
2. 執行以下指令：

   keytool -genkey -alias alias -keystore .keystore
3. 輸入 keystore 的密碼。輸入託管儲存時將需要使用此密碼。
4. 輸入下列資訊：您的名字與姓氏。
   - 名字與姓氏
   - 組織單位
   - 組織
   - 城市或地區
   - 州或省
   - 兩位數的國家代碼
5. 檢查資訊是否正確。
6. 按下 Enter 使用相同的密碼做爲 keystore 密碼。

   系統會建立 .keystore 檔案以及私密金鑰與對應的公用金鑰 (證書)。