AUTHORIZED DOCUMENTATION

Benutzerhandbuch

October 31, 2008

Novell®
Identity Audit

1.0

www.novell.com

Rechtliche Hinweise

Novell, Inc. leistet keinerlei Gewähr bezüglich des Inhalts oder Gebrauchs dieses Handbuchs. Insbesondere werden keine ausdrücklichen oder stillschweigenden Gewährleistungen hinsichtlich der handelsüblichen Qualität oder Eignung für einen bestimmten Zweck übernommen. Novell, Inc. behält sich weiterhin das Recht vor, diese Dokumentation zu revidieren und ihren Inhalt jederzeit und ohne vorherige Ankündigung zu ändern.

Des Weiteren übernimmt Novell, Inc. für Software keinerlei Haftung und schließt insbesondere jegliche ausdrücklichen oder impliziten Gewährleistungsansprüche bezüglich der Marktfähigkeit oder der Eignung für einen bestimmten Zweck aus. Außerdem behält sich Novell, Inc. das Recht vor, Novell-Software ganz oder teilweise jederzeit inhaltlich zu ändern, ohne dass für Novell, Inc. die Verpflichtung entsteht, Personen oder Organisationen von diesen Überarbeitungen oder Änderungen in Kenntnis zu setzen.

Alle im Zusammenhang mit dieser Vereinbarung zur Verfügung gestellten Produkte oder technischen Informationen unterliegen möglicherweise den US-Gesetzen zur Exportkontrolle sowie den Handelsgesetzen anderer Länder. Sie erkennen alle Ausfuhrkontrollbestimmungen an und erklären sich damit einverstanden, alle für ausstehende Exporte, Re-Exporte oder Importe erforderlichen Lizenzen bzw. Klassifizierungen einzuholen. Sie erklären sich damit einverstanden, nicht an juristische Personen, die in der aktuellen US-Exportausschlussliste enthalten sind, oder an in den US-Exportgesetzen aufgeführte terroristische Länder oder Länder, die einem Embargo unterliegen, zu exportieren oder zu reexportieren. Sie stimmen zu, keine Lieferungen für verbotene nukleare oder chemisch-biologische Waffen oder Waffen im Zusammenhang mit Flugkörpern zu verwenden. Weitere Informationen zum Export von Novell-Software finden Sie auf der Webseite "Novell International Trade Services" (http://www.novell.com/info/exports/). Novell übernimmt keine Verantwortung für das Nichteinholen notwendiger Exportgenehmigungen.

Novell, Inc. besitzt Anrechte auf geistiges Eigentum für Technologie, die in das in dieser Dokumentation beschriebene Produkt integriert ist. Diese Rechte auf geistiges Eigentum umfassen möglicherweise insbesondere ein oder mehrere Patente in den USA, die auf der Webseite "Legal Patents" von Novell (http://www.novell.com/company/legal/patents/) aufgeführt sind, sowie ein oder mehrere andere Patente oder laufende Patentanträge in den USA und in anderen Ländern.

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

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite von Novell (http://www.novell.com/documentation).

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch beschreibt, wie Novell® Identity Audit installiert und konfiguriert wird.

Zielgruppe

Dieses Handbuch richtet sich an Novell Identity Audit-Administratoren.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Benutzerkommentarfunktion unten auf der jeweiligen Seite der Online-Dokumentation oder wählen Sie www.novell.com/documentation/feedback.html, und geben Sie dort Ihre Kommentare ein.

Dokumentationsaktualisierungen

Die neueste Version des *Novell Identity Audit 1.0-Benutzerhandbuchs* finden Sie auf der Website zur Identity Audit-Dokumentation (http://www.novell.com/documentation/identityaudit).

Konventionen in der Dokumentation

In dieser Novell-Dokumentation wird ein „Größer als“-Zeichen (>) verwendet, um verschiedene Aktionen innerhalb eines Schritts und Meldungen in einem Querverweispfad voneinander zu trennen.

Ein Markensymbol (®, ™ usw.) kennzeichnet eine Novell-Marke. Ein Sternchen (*) kennzeichnet eine Drittanbieter-Marke.

Einführung

1

Novell® Identity Audit bietet Ereignisberichts- und Überwachungsfunktionen für die Umgebung von Novell Identity and Security Management, zu der Novell eDirectory™, Novell Identity Manager, Novell Access Manager, Novell Modular Authentication Services (NMAS™), Novell SecureLogin und Novell SecretStore® gehören.

1.1 Produktübersicht

Novell Identity Audit 1.0 ist ein benutzerfreundliches, unkompliziertes Tool zur Sammlung, Zusammenfassung und Speicherung von Ereignissen aus Novell Identity Manager, Novell Access Manager, Novell eDirectory und anderen Identitäts- und Sicherheitsprodukten und -technologien von Novell. Zu den Schlüsselfunktionen zählen:

- Webbasierte Verwaltung und Berichtschnittstellen
- Suchwerkzeug für umfassende Ereignisse zur Suche in mehreren Ereignisfeldern
- Ausgewählte Ereignisausgabe an mehrere Kanäle
- Die Embedded Jasper Reports-Engine ermöglicht die Verwendung von Open Source-Tools zur individuellen Anpassung bereits vorhandener Berichte oder zur Erstellung neuer Berichte.
- Die integrierte Datenbank macht Lizenzen oder die Verwaltung von externen Datenbanken überflüssig.
- Einfache, intuitive Tools zur Datenverwaltung

1.1.1 Vergleich mit Novell Audit 2.0.2

Novell Identity Audit 1.0 löst die Produktlinie von Novell Audit ab, für die der Support im Februar 2009 eingestellt wird. Identity Audit ist vergleichbar in der Funktionalität, bietet jedoch erhebliche Verbesserungen in der Architektur, Berichterstellung und Datenverwaltung. Novell Identity Audit 1.0 ist ein integrierter Ersatz für den Novell Audit 2.0.2 Secure Logging Server für Produkte der Produktfamilie Novell Identity and Security. Da Novell Identity Audit eine neue integrierte Datenbank verwendet, sollten Kunden ihre vorhandenen Novell Audit-Ereignisse besser in der archivierten Novell Audit-Datenbank aufbewahren, statt zu versuchen, alte Daten zu migrieren.

Die Client-Komponente von Novell Audit, die auch als Plattformagent bekannt ist, wird auch bei Novell Identity Audit als Methode zum Datentransport verwendet. Für diese Methode wird weiterhin entsprechend den Produktlebenszyklen der Novell Identity- und Access Management-Produkte, die den Plattformagenten weiterhin verwenden, Support angeboten.

1.1.2 Vergleich mit Novell Sentinel

Novell Identity Audit baut auf einer stabilen technologischen Grundlage auf, denn der zugrunde liegende Code entstammt weitgehend einer gemeinsamen Nutzung mit Novell Sentinel. Sentinel erfasst allerdings Daten einer breiteren Palette an Geräten, unterstützt eine höhere Ereignisverarbeitungsrate und bietet mehr Tools als Novell Identity Audit. Sentinel bietet auch zusätzliche Funktionen zur Verwaltung von Sicherheitsinformationen und Ereignissen (SIEM), wie zum Beispiel Echtzeit-Dashboards, Mehrfachereigniskorrelation, Vorfallprotokollierung sowie automatische Korrektur und Datensammlung von nicht-Novell-Produkten. Bei der Entwicklung von Identity Audit wurde auf Integrationsfähigkeit mit künftigen Sentinel-Implementierungen geachtet.

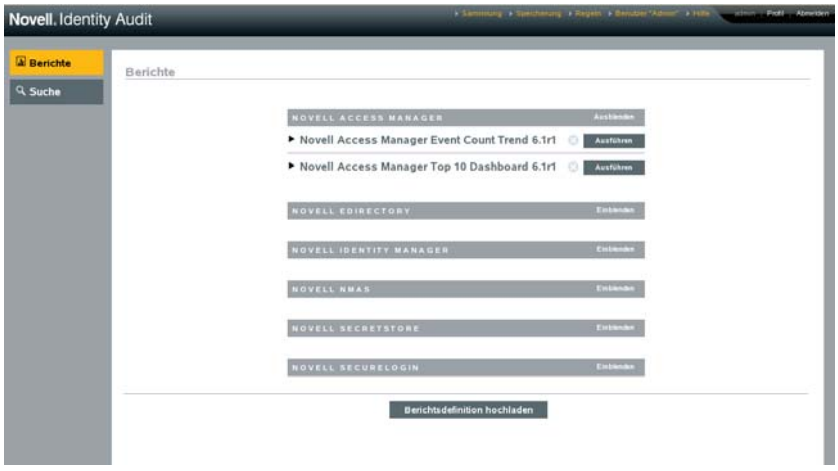
Novell Identity Audit 1.0 ist nicht Teil der Novell Compliance Management Platform (CMP) und enthält keine der im Lieferumfang dieser Plattform enthaltenen erweiterten Funktionen zur Identitäts- und Sicherheitsintegration. Sentinel 6.1 ist gegenwärtig die Komponente, die in der CMP für die Identitätsprüfung und -überwachung zuständig ist.

1.2 Schnittstelle

Die Web-Oberfläche von Novell Identity Audit ermöglicht die Durchführung der folgenden Aufgaben:

- Berichte hochladen, ausführen, anzeigen und löschen
- Ereignisse suchen
- Detailinformationen des Benutzerprofils bearbeiten
- Benutzer erstellen, bearbeiten und löschen und Verwaltungsrechte zuweisen (nur Administratoren)
- Datensammlungen konfigurieren und Status der Ereignisquellen anzeigen (nur Administratoren)
- Datenspeicher konfigurieren und Status der Datenbank anzeigen (nur Administratoren)
- Filterregeln erstellen und dazugehörige Aktionen konfigurieren, um übereinstimmende Ereignisdaten an Ausgabekanäle zu senden (nur Administratoren)

Abbildung 1-1 *Oberfläche von Novell Identity Audit (Administratoransicht)*



Die Oberfläche wird alle 30 Sekunden aktualisiert, um gegebenenfalls durch andere Benutzer vorgenommene Änderungen anzuzeigen.

Die Oberfläche steht in mehreren Sprachen zur Verfügung (Deutsch, Englisch, Französisch, Italienisch, Japanisch, Portugiesisch, Spanisch, Vereinfachtes und Traditionelles Chinesisch). Die Oberfläche wird in der Standardsprache des Browsers angezeigt, der Benutzer kann jedoch bei der Anmeldung eine andere Sprache auswählen.

Hinweis: Obwohl die Oberfläche in Doppelbyte-Sprachen lokalisiert wurde, verarbeitet das aktuelle Identity Audit-Release keine Doppelbyte-Ereignisdaten.

1.3 Architektur

Identity Audit sammelt Daten aus mehreren Novell Identity and Security-Anwendungen. Diese Anwendungsserver werden zum Generieren von Ereignisdatensätzen konfiguriert. Jeder Server ist Host eines Plattformagenten, der wiederum Teil der Novell Audit-Anwendung ist. Der Plattformagent leitet Ereignisdaten an den Audit Connector weiter, der sich auf dem Identity Audit-Server befindet.

Der Audit Connector leitet Ereignisse an die Datensammlungskomponente weiter und parst sie auf den Kommunikationsbus. Dieser ist das Backbone des Systems, der sämtliche Kommunikationen zwischen den Komponenten verwaltet. Im Zuge der Datensammlung werden eingehende Ereignisse von einer Reihe von Filterregeln ausgewertet. Diese Regeln filtern Ereignisse und senden sie an Ausgabekanäle wie eine Datei, einen Syslog-Server oder ein .

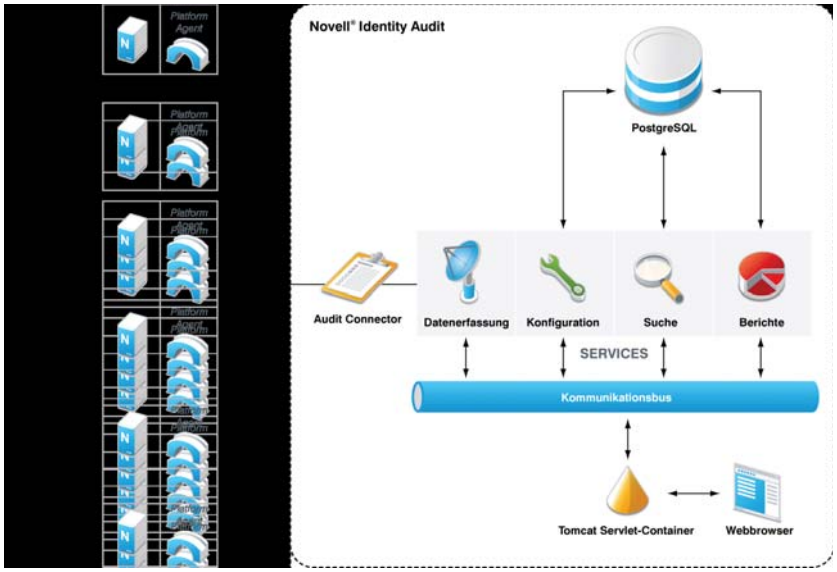
Zusätzlich werden alle Ereignisse in der Identity Audit-Datenbank (unterstützt von PostgreSQL*) in partitionierten Tabellen gespeichert.

Die Konfigurationskomponente ruft Konfigurationsinformationen ab, fügt sie hinzu und ändert sie. Bei diesen Informationen kann es sich um Datensammlungen, Speichereinstellungen, Regeldefinitionen und Berichtdefinitionen handeln. Des Weiteren verwaltet diese Komponente die Benutzerauthentifizierung.

Mit der Suchkomponente können Sie schnelle und indizierte Suchen durchführen. Die Komponente ruft Ereignisse aus der Datenbank ab und gibt dem Benutzer das Suchergebnis aus.

Die Berichtkomponente führt Berichte aus und stellt Berichtergebnisse zusammen.

Abbildung 1-2 *Architektur für Identity Audit*



Benutzer interagieren über einen Webbrowser, der eine Verbindung zu einem Apache Tomcat-Webserver herstellt, mit dem Identity Audit-Server und seinen Funktionen. Über den Kommunikationsbus ruft der Webserver die verschiedenen Identity Audit-Komponenten an.

Systemanforderungen

2

Zusätzlich zu den nachfolgend beschriebenen Anforderungen an die Hardware, das Betriebssystem, den Browser und die Kompatibilität mit den Ereignisquellen ist zur Installation root-Zugriff auf das Betriebssystem erforderlich, um den Novell-Benutzer und die Novell-Gruppe erstellen zu können, die Eigentümer der Ausführungsvorgänge von Identity Audit sind.

2.1 Hardwareanforderungen

Novell Identity Audit™ wird auf 64-Bit Intel Xeon*- und AMD Opteron*-Hardware unterstützt. Das Programm wird nicht auf Itanium-Hardware unterstützt. Novell empfiehlt die folgende Hardware für ein Produktionssystem, das Online-Daten der letzten 90 Tage speichert:

- 1 x Quad Core (x86-64)
- 16 GB RAM
- 1,5 TB verwendbarer Festplattenspeicher - 3 x 500 GB (3 verwendbar), 10K RPM-Laufwerke in einer Hardware-RAID-Konfiguration
  - Ungefähr zwei Drittel des verwendbaren Festplattenspeichers werden für Datenbankdateien verwendet.
  - Ungefähr ein Drittel des verwendbaren Festplattenspeichers wird für den Suchindex und temporäre Dateien verwendet.
  - Ein kleiner Teil des Speichers steht für archivierte Daten zur Verfügung, die aus der Datenbank entfernt wurden. Novell empfiehlt jedoch, die archivierten Datendateien auf einen anderen Datenträger zu speichern.

Tabelle 2-1 *Leistung*

Metrik	Wert	Beschreibung
Ereignisse pro Sekunde (eps) - Steady State	100	Durchschnittliche Ereignisverarbeitungsrate bei normalem Betrieb
Ereignisse pro Sekunde (eps) - Peak	500	Höchste Ereignisverarbeitungsrate bei kurzzeitig erhöhtem Verarbeitungsaufkommen (bis zu 10 Minuten)

Metrik	Wert	Beschreibung
Ereignisse pro Sekunde (eps) - Peak pro Anwendung	300	Höchste Ereignisverarbeitungsrate jedes Novell-Anwendungstyps ◆ Ereignisverarbeitungsraten sind für Identity Manager, SecureLogin, SecretStore® und NMAS™) normalerweise niedrig (weniger als 15 eps). ◆ Für eDirectory™ und Access Manager können die Ereignisverarbeitungsraten extrem hoch sein. Verwenden Sie auf jeden Fall die Ereignisfilterung, um eine übersichtliche und zu bewältigende Rate zu erstellen. ◆ Auch bei einem kurzzeitigen Mehraufkommen von Ereignissen kann eine Anwendung immer nur die angegebene Anzahl von Ereignissen pro Sekunde senden.
Onlinedaten	90 Tage oder 750 Millionen Ereignisse	Datenmenge, die Identity Audit bei einer Steady State-Rate von ungefähr 100 eps bei Verwendung des empfohlenen Speicherplatzes speichern kann.

2.2 Unterstützte Betriebssysteme

Identity Audit ist zertifiziert zur Ausführung auf 64-Bit SUSE Linux Enterprise Server™ 10 SP 1 und SP 2.

2.3 Unterstützte Browser

Identity Audit unterstützt die nachfolgend aufgeführten Browser. Andere Browser zeigen Informationen möglicherweise nicht wie erwartet an.

Tabelle 2-2 *Von Novell Identity Audit unterstützte Webbrowser*

Webbrowser und Version
Mozilla Firefox 2
Mozilla Firefox 3
Microsoft Internet Explorer 7

Die Leistung der Suchausführung und der Berichtanzeige ist anscheinend abhängig vom verwendeten Browser. Eine extrem gute Leistung wird nach Aussagen von Novell mit Mozilla Firefox 3 erzielt.

2.4 Unterstützter Plattformagent

Identity Audit 1.0 unterstützt die Sammlung von Protokollierungsereignissen von vielen Anwendungen, die auch schon seitens Novell Audit und dessen Plattformagenten unterstützt wurden. Für 32-Bit-Ereignisquellen ist für Identity Audit Plattformagent Version 2.0.2 FP6 (2.0.2.55) oder höher erforderlich. Für 64-Bit-Ereignisquellen ist Plattformagent Version 2.0.2 FP6 erforderlich.

Hinweis: Einige Novell-Anwendungen sind im Lieferumfang einer früheren Version des Plattformagenten enthalten. Die empfohlene Version enthält Fehlerbehebungen, weshalb Novell empfiehlt, den Plattformagenten zu aktualisieren.

2.5 Unterstützte Ereignisquellen

Identity Audit unterstützt die Datensammlung aus den Novell Identity and Security-Anwendungen. Für manche Anwendungen ist ein bestimmter Patch-Level erforderlich, um die Datensammlung korrekt ausführen zu können.

Tabelle 2-3 *Von Novell Identity Audit unterstützte Anwendungen*

Anwendung
Novell Access Manager 3.0
Novell eDirectory 8.8.3 mit dem eDirectory-Ausrüstungs-Patch finden Sie auf der Website des Novell-Kundendiensts (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~)
Novell Identity Manager 3.6
Novell NMAS 3.1
Novell SecretStore 3.4
Novell SecureLogin 6.0

Installation

3

In diesem Kapitel wird beschrieben, wie Novell Identity Audit installiert wird und wie die Ereignisquellen zum Senden von Daten an das Programm konfiguriert werden. Diese Anleitungen gehen davon aus, dass die Mindestanforderungen für jede Systemkomponente erfüllt sind. Weitere Informationen finden Sie unter Kapitel 2, „Systemanforderungen“, auf Seite 13.

3.1 Installieren von Novell Identity Audit

Das Installationspaket von Identity Audit installiert alles, was zur Ausführung von Identity Audit erforderlich ist: die Anwendung und den Nachrichtenbus von Identity Audit, die Datenbank zur Speicherung von Ereignissen und Konfigurationsinformationen, die webbasierte Benutzeroberfläche sowie den Berichtsserver. Es stehen zwei Installationsoptionen zur Verfügung, nämlich eine einfache Installation, die als root ausgeführt werden kann, oder eine Installation in mehreren Schritten, die root möglichst wenig in Anspruch nimmt.

3.1.1 Schnellinstallation (als root)

Diese einfache Installation muss als root ausgeführt werden.

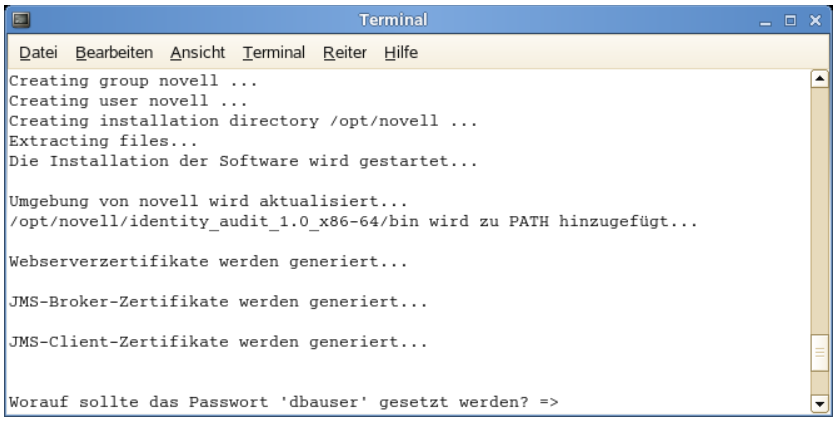
1. Melden Sie sich am Server, auf dem Identity Audit installiert werden soll, als `Root` an.
2. Laden Sie die Datei `identity_audit_1.0_x86-64.tar.gz` in ein temporäres Verzeichnis herunter oder kopieren Sie es dorthin.
3. Extrahieren Sie das Installationsskript in der Datei mithilfe des folgenden Befehls:

   ```
   tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
   ```
4. Führen Sie das Skript `root_install_all.sh` mithilfe des folgenden Befehls aus:

   ```
   identity_audit_1.0_x86-64/setup/root_install_all.sh identity_audit_1.0_x86-64.tar.gz
   ```
5. Geben Sie eine Zahl ein, um eine Sprache auszuwählen.

   Die Endbenutzerlizenz-Vereinbarung wird in der ausgewählten Sprache angezeigt.
6. Lesen Sie die Endbenutzerlizenz-Vereinbarung und geben Sie `1` oder `y` ein, um der Vereinbarung zuzustimmen und mit der Installation fortzufahren.

   Die Installation beginnt. Falls die zuvor ausgewählte Sprache nicht für das Installationsprogramm zur Verfügung steht (z. B. Polnisch), wird das Installationsprogramm in englischer Sprache fortgeführt.



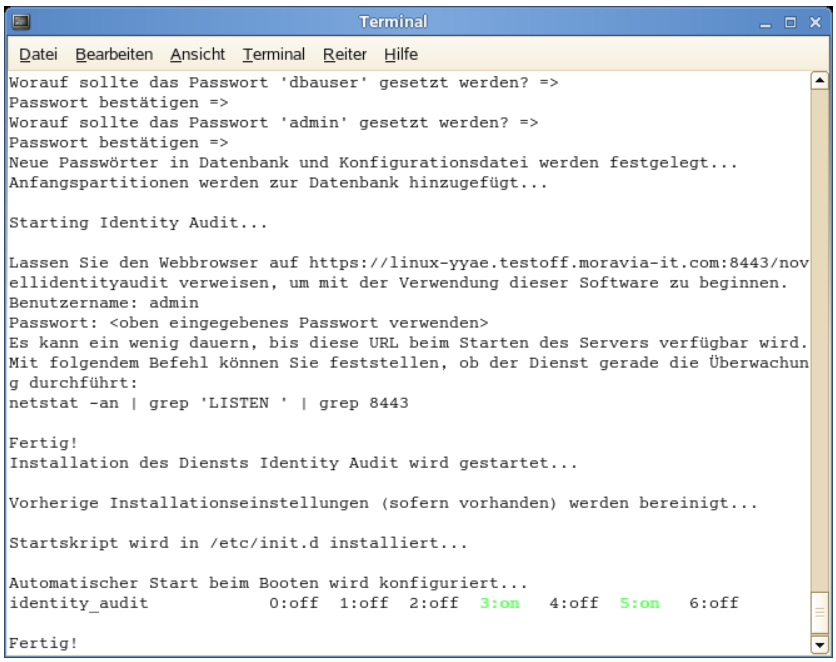
Der Novell-Benutzer und die Novell-Gruppe werden erstellt, falls nicht bereits vorhanden.

7 Geben Sie das Passwort für den Datenbankadministrator (dbauser) ein.

8 Bestätigen Sie das Passwort für den Datenbankadministrator (dbauser).

9 Geben Sie das Passwort für den Admin-Benutzer ein.

10 Bestätigen Sie das Passwort für den Admin-Benutzer.



Der dbauser-Berechtigungsnachweis wird zur Erstellung von Tabellen und Partitionen in der PostgreSQL-Datenbank verwendet. Identity Audit ist so konfiguriert, dass es beim Start mit den Laufzeit-Levels 3 und 5 ausgeführt wird (Multi-User-Modus beim Start in der Konsole oder im X-Windows-Modus).

Nach dem Starten des Identity Audit-Service melden Sie sich bei der URL an, die in der Installationsausgabe angegeben ist (https://hostIP:8443/novellidentityaudit). Das System beginnt umgehend damit, interne Audit-Ereignisse zu verarbeiten und ist nach der Konfiguration der Ereignisquellen zum Senden von Daten an Identity Audit voll funktionsfähig.

3.1.2 Nicht-root-Installation

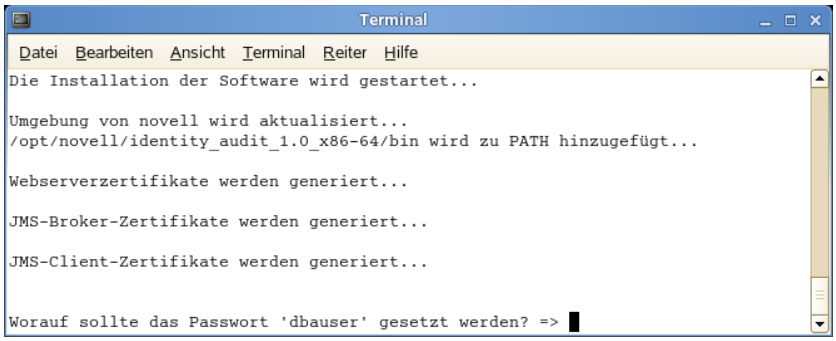
Falls organisatorische Richtlinien die Ausführung des gesamten Installationsvorgangs als `root` verbieten, kann die Installation auch in zwei Schritten durchgeführt werden. Der erste Teil des Installationsvorgangs muss mit Zugriff auf die root-Ebene durchgeführt werden. Der zweite Teil wird als verwaltungsbefugter Benutzer von Identity Audit (der im ersten Schritt erstellt wurde) durchgeführt.

1. Melden Sie sich am Server, auf dem Identity Audit installiert werden soll, als `Root` an.
2. Laden Sie die Datei `identity_audit_1.0_x86-64.tar.gz` in das Verzeichnis `/tmp` herunter oder kopieren Sie sie dorthin.
3. Falls der Novell-Benutzer und die Novell-Gruppe noch nicht vorhanden sind:
   1. Extrahieren Sie das Skript zur Erstellung des Novell-Benutzers und der Novell-Gruppe aus der TAR-Datei von Identity Audit. Beispiel:
      ```
      tar xfz identity_audit_1.0_x86-64.tar.gz
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
   2. Führen Sie das Skript als `root` mithilfe des folgenden Befehls aus:
      ```
      identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
      ```
      Der Novell-Benutzer und die Novell-Gruppe sind Eigentümer der Installations- und Ausführungsvorgänge von Identity Audit.
4. Erstellen Sie ein Verzeichnis für Identity Audit. Beispiel:

   mkdir -p /opt/*novell*
5. Legen Sie das Verzeichnis als Eigentum des Novell-Benutzers und der Novell-Gruppe fest. Beispiel:
   ```
   chown -R novell:novell /opt/novell
   ```
6. Melden Sie sich als Novell-Benutzer an:
   ```
   su novell
   ```
7. Extrahieren Sie die TAR-Datei von Identity Audit im gerade erstellten Verzeichnis. Beispiel:
   ```
   cd /opt/novell
   tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
   ```
8. Führen Sie das Installationsskript aus. Beispiel:
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/install.sh
   ```
9. Geben Sie eine Zahl ein, um eine Sprache auszuwählen.

   Die Endbenutzerlizenz-Vereinbarung wird in der ausgewählten Sprache angezeigt.
10. Lesen Sie die Endbenutzerlizenz-Vereinbarung und geben Sie `1` oder `y` ein, um der Vereinbarung zuzustimmen und mit der Installation fortzufahren.

    Die Installation beginnt. Falls die zuvor ausgewählte Sprache nicht für das Installationsprogramm zur Verfügung steht (z. B. Polnisch), wird das Installationsprogramm in englischer Sprache fortgeführt.



11 Geben Sie das Passwort für den Datenbankadministrator (dbauser) ein.

12 Bestätigen Sie das Passwort für den Datenbankadministrator (dbauser).

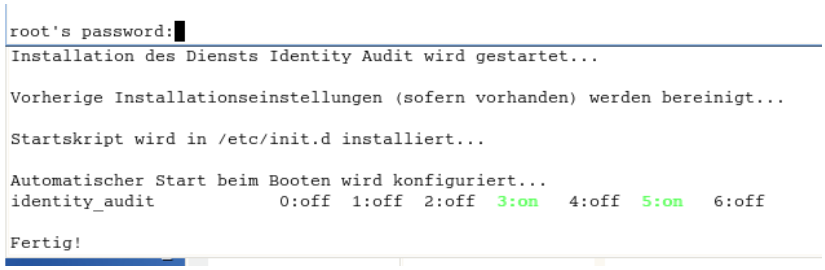
13 Geben Sie das Passwort für den Admin-Benutzer ein.

14 Bestätigen Sie das Passwort für den Admin-Benutzer.

15 Melden Sie sich ab und erneut als novell an. Dadurch werden die Änderungen an der PATH-Umgebungsvariable geladen, die durch das Skript `install.sh` vorgenommen wurden.

16 Führen Sie das Skript `root_install_service.sh` aus, damit Identity Audit als Service starten kann. Bei diesem Schritt ist Zugriff auf die `root`-Ebene erforderlich. Beispiel:

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



17 Geben Sie das `root`-Passwort ein.

Identity Audit ist so konfiguriert, dass es beim Start mit den Laufzeit-Levels 3 und 5 ausgeführt wird (Multi-User-Modus beim Start in der Konsole oder im X-Windows-Modus).

Nach dem Starten des Identity Audit-Service melden Sie sich bei der URL an, die in der Installationsausgabe angegeben ist (https://hostIP:8443/novellidentityaudit). Das System beginnt umgehend damit, interne Auditereignisse zu verarbeiten und ist nach der Konfiguration der Ereignisquellen zum Senden von Daten an Identity Audit voll funktionsfähig.

3.2 Konfigurieren von Ereignisquellen

Identity Audit 1.0 unterstützt die Sammlung von Protokollierungsereignissen von Anwendungen, die auch schon seitens Novell Audit und dessen Plattformagenten unterstützt wurden. Bevor Sie die in diesem Abschnitt aufgeführten Schritte durchführen, stellen Sie sicher, dass Ihre Novell-Produkte auch unterstützt werden. Weitere Informationen finden Sie unter Abschnitt 2.4, „Unterstützter Plattformagent“, auf Seite 15.

- Abschnitt 3.2.1, „Installation des Plattformagenten“, auf Seite 21

- Abschnitt 3.2.2, „Konfigurieren des Plattformagenten“, auf Seite 21
- Abschnitt 3.2.3, „Konfigurieren des Revisionslevels“, auf Seite 22

3.2.1 Installation des Plattformagenten

Sie müssen die für Identity Audit empfohlene Mindestversion des Plattformagenten verwenden. Weitere Informationen finden Sie unter Abschnitt 2.4, „Unterstützter Plattformagent“, auf Seite 15. Der entsprechende Plattformagent (32- oder 64-Bit) muss auf allen Ereignisquellen-Computern installiert sein oder aktualisiert werden. Der Plattformagent ist Teil des Novell Audit-Downloads von der Novell Download-Website (http://download.novell.com).

So installieren oder aktualisieren Sie den 32-Bit-Plattformagenten:

1. Laden Sie die Datei `.iso` für Audit 2.0.2 FP6 oder höher in das Verzeichnis /tmp auf dem Ereignisquellen-Computer herunter.
2. Erstellen Sie ein Verzeichnis für Audit. Beispiel: `mkdir -p audit202fp6`
3. Melden Sie sich als `root`-Benutzer an.
4. Laden Sie die Audit-Datei `.iso`.

   ```
   mount -o loop ./NAudit202.iso ./audit202fp6
   ```
5. Navigieren Sie zum Verzeichnis `audit202fp6`.
6. Navigieren Sie zum entsprechenden Verzeichnis für das Betriebssystem auf Ihrer Ereignisquelle. Beispiel:

   ```
   cd Linux
   ```
7. Führen Sie die Datei `pinstall.lin` aus.

   ```
   ./pinstall.lin
   ```
8. Lesen Sie die Lizenzvereinbarung und geben Sie `y` ein, um die Vereinbarung zu akzeptieren.
9. Geben Sie `P` ein, um den Plattformagenten zu installieren.
10. Geben Sie `Y` ein, um alle vorherigen Konfigurationen in der Datei `logevent.conf` zu behalten.

    Der Plattformagent wird installiert.
11. Geben Sie zum Überprüfen der korrekten Version des Plattformagenten den folgenden Befehl ein:

    ```
    rpm -qa | grep AUDT
    ```

    Die Version des novell-AUDTplatformagent sollte mindestens die in Abschnitt 2.4, „Unterstützter Plattformagent“, auf Seite 15 aufgeführte unterstützte Version sein.

Zum Installieren oder Aufrüsten des 64-Bit-Plattformagenten laden Sie NAudit 2.0.2 FP6 herunter und befolgen die im Patch enthaltene Anleitung.

3.2.2 Konfigurieren des Plattformagenten

Nach der Installation muss der Plattformagent konfiguriert werden, um Daten an den Identity Audit-Server zu senden und, falls gewünscht, Ereignissignaturen von den Ereignisquellen zu senden.

Warnung: Wenn Sie den Plattformagenten für die Generierung von Signaturen konfigurieren, kann dies negative Auswirkungen auf die Leistung der Ereignisquellen-Computer haben.

So konfigurieren Sie den Plattformagenten:

1. Melden Sie sich am Ereignisquellen-Computer an.
2. Öffnen Sie die Datei `logevent` zur Bearbeitung. Je nach Betriebssystem befindet sich diese Datei in den folgenden Verzeichnissen:
   - Linux: `/etc/logevent.conf`
   - Windows: `C:\WINDOWS\logevent.cfg`
   - NetWare: `SYS:\etc\logevent.cfg`
   - Solaris: `/etc/logevent.conf`
3. Legen Sie für LogHost die IP-Adresse des Identity Audit-Servers fest.
4. Legen sie folgenden Wert fest: LogEnginePort=1289. (Fügen Sie diesen Eintrag hinzu, falls er noch nicht vorhanden ist.)
5. Falls Sie die Ereignisquelle zum Senden von Ereignissignaturen konfigurieren möchten, geben Sie Folgendes ein: LogSigned=always.
6. Speichern Sie die Datei.
7. Starten Sie den Plattformagenten neu. Dieser Vorgang ist abhängig vom Betriebssystem und der Anwendung. Booten Sie den Computer neu. Weitere Anleitungen finden Sie auf der Novell Documentation-Website (http://www.novell.com/documentation) in der anwendungsspezifischen Dokumentation.

3.2.3 Konfigurieren des Revisionslevels

Die Ereignisse, für die jede Anwendung Datensätze generiert, werden für jede von Identity Audit überwachte Anwendung separat und unterschiedlich konfiguriert. Unter den im Folgenden aufgeführten URLs finden Sie weitere Informationen zu jeder Anwendung.

- 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 verwendet (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 Einführung

Der bei der Installation erstellte verwaltungsbefugte Benutzer kann sich in der Identity Audit-Anwendung anmelden und weitere Benutzer erstellen, zuvor geladene Berichte ausführen, neue Berichte hochladen, Ereignissuchen durchführen und vieles mehr.

So melden Sie sich bei Identity Audit an:

1. Öffnen Sie einen unterstützten Webbrowser. Weitere Informationen finden Sie unter Abschnitt 2.3, „Unterstützte Browser“, auf Seite 14.
2. Wechseln Sie zur Identity Audit-Anmeldeseite (https://hostIP:8443/novellidentityaudit).
3. Falls Sie sich zum ersten Mal bei Identity Audit anmelden, wird ein Zertifikat angezeigt. Sie müssen dieses akzeptieren, um fortzufahren.
4. Geben Sie `admin` ein.
5. Geben Sie das Admin-Passwort ein, das Sie bei der Installation konfiguriert haben.
6. Wählen Sie die Sprache für die Oberfläche von Identity Audit aus (Englisch, Portugiesisch, Französisch, Italienisch, Deutsch, Spanisch, Japanisch, traditionelles Chinesisch oder vereinfachtes Chinesisch).
7. Klicken Sie auf *Anmelden*.

3.4 Deinstallation

Um eine Installation von Identity Audit vollständig zu entfernen, müssen Sie das Deinstallationsskript ausführen und anschließend einige manuelle Schritte zur Bereinigung durchführen.

1. Melden Sie sich als `root`-Benutzer am Identity Audit-Server an.
2. Stoppen Sie den Identity Audit-Service:
   ```
   /etc/init.d/identity_audit stop
   ```
3. Führen Sie das Deinstallationsskript aus:
   ```
   /opt/novell/identity_audit_1.0_x86-64/setup/
   root_uninstall_service.sh
   ```
4. Löschen Sie das Identity Audit-Basisverzeichnis mit allen Inhalten.
   ```
   rm -rf /opt/novell/identity_audit_1.0_x86-64
   ```
5. Welche letzten Schritte Sie ausführen, ist abhängig davon, ob Sie Informationen bezüglich des Novell-Benutzers und der Novell-Gruppe behalten möchten.
   - Falls Sie keine Informationen bezüglich des Novell-Benutzers behalten möchten, führen Sie den folgenden Befehl aus. Mit diesem Befehl löschen Sie den Benutzer, sein Basisverzeichnis und die Gruppe.
     ```
     userdel -r novell && groupdel novell
     ```
   - Falls Sie die Informationen bezüglich des Novell-Benutzers und sein Basisverzeichnis behalten möchten und nur die Identity Audit-bezogenen Einstellungen löschen möchten, gehen Sie wie folgt vor:
     1. Entfernen Sie die folgenden Einträge der Umgebungsvariable für Identity Audit aus dem Profil des Novell-Benutzers (in `~novell/.bashrc`):

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

2. Entfernen Sie den dbauser-Eintrag aus der PostgreSQL-Datei `~novell/.pgpass`. `*:*:*:dbauser:`*`password`*

Hinweis: Auch wenn das dbauser-Passwort im Klartext angezeigt wird, können nur der Novell- und der root-Benutzer, die bereits vollen Zugriff auf alle Funktionen auf dem Identity Audit-Server haben, den Inhalt der Datei anzeigen.

Suchvorgänge

4

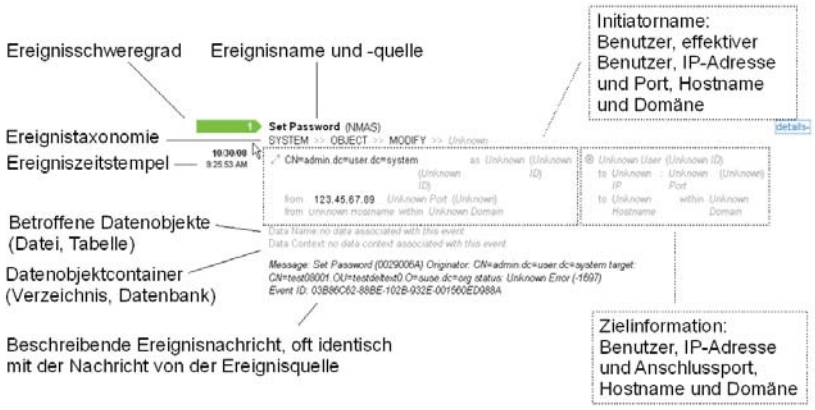
In diesem Abschnitt werden die Suchmöglichkeiten von Novell® Identity Audit beschrieben.

4.1 Überblick zur Ereignissuche

Novell Identity Audit bietet die Möglichkeit, eine Suche nach Ereignissen durchzuführen. Die Suche umfasst alle Online-Daten, die sich zurzeit in der Datenbank befinden. Allerdings werden interne Ereignisse, die durch das Identity Audit-System generiert wurden, dabei ausgeschlossen, es sei denn, der Benutzer wählt die Option *Systemereignisse einbeziehen* aus. Standardmäßig werden Ereignisse basierend auf dem Relevanzalgorithmus der Suchengine sortiert.

Zu den Grundinformationen von Ereignissen gehören Ereignisname, Quelle, Zeit, Schweregrad, Informationen zum Initiator (angegeben durch ein Pfeilsymbol) sowie Informationen zum Ziel (angegeben durch ein Bullaugensymbol).

Abbildung 4-1 *Ereignisfelder*



4.2 Ausführen einer Ereignissuche

Benutzer haben die Möglichkeit, einfache und erweiterte Suchvorgänge auszuführen.

- Abschnitt 4.2.1, „Basissuche“, auf Seite 26
- Abschnitt 4.2.2, „Erweiterte Suche“, auf Seite 27

4.2.1 Basissuche

Eine Basissuche wird für alle Ereignisfelder in Tabelle 4-1 auf Seite 31 ausgeführt. Zu einigen Grundsuchen gehört Folgendes:

- `Root`
- `127.0.0.1`
- `Sperren*`
- `driverset0`

Hinweis: Falls die Zeit zwischen dem Endbenutzer-Computer und dem Identity Audit-Server nicht synchronisiert ist (die Zeiteinstellung des einen Computers geht beispielsweise 25 Minuten nach), erhalten Sie unter Umständen unerwartete Suchergebnisse. Suchen wie *Letzte 1 Stunde* oder *Letzte 24 Stunden* basieren auf der Zeiteinstellung des Endbenutzer-Computers.

---

1. Klicken Sie links auf den Link *Suchen*.

   Identity Audit ist so konfiguriert, dass beim ersten Klicken des Benutzers auf den Link *Suche* eine Standardsuche für Nicht-Systemereignisse mit einem Schweregrad von 3 bis 5 ausgeführt wird. Anderenfalls wird standardmäßig nach dem letzten vom Benutzer eingegebenen Suchbegriff gesucht.

2. Geben Sie für einen anderen Suchtyp einen Suchbegriff in das Suchfeld ein, z. B. `Admin`). Die Suche unterscheidet nicht zwischen Groß- und Kleinschreibung.
3. Wählen Sie einen Zeitabschnitt aus, in dem die Suche durchgeführt werden soll. Die meisten Zeiteinstellungen sind selbsterklärend; standardmäßig ist *Die letzten 30 Tage* festgelegt.
   - Mithilfe der Option *Benutzerdefiniert* können Sie für eine Abfrage ein Start- und ein Enddatum sowie eine Uhrzeit auswählen. Das Anfangsdatum muss vor dem Enddatum liegen und die Zeit is based.
   - Mithilfe der Option *Jederzeit* werden alle Daten in der Datenbank durchsucht.
4. Wählen Sie *Systemereignisse einbeziehen*, um Ereignisse einzubeziehen, die durch Systemoperationen von Identity Audit generiert wurden.

5 Mit der Option *Nach Zeit sortieren* können Sie die Daten beginnend mit dem zuletzt aufgetretenen Ereignis sortieren.

Hinweis: Das Sortieren nach Zeit dauert länger als das Sortieren nach Relevanz, welches die Standardeinstellung ist.

---

6 Klicken Sie auf *Suchen*.

Alle Felder im Index werden nach dem entsprechenden Text durchsucht. Ein sich drehendes Symbol gibt an, dass die Suche ausgeführt wird.

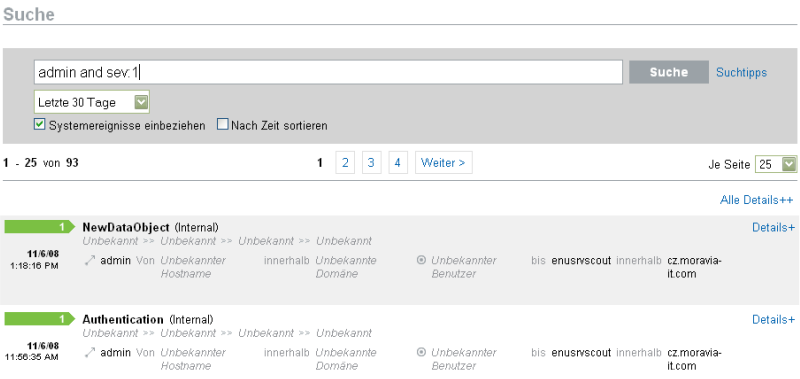
Die Ereigniszusammenfassungen werden angezeigt.

4.2.2 Erweiterte Suche

Bei einer erweiterten Suche wird nach einem Wert in mindestens einem bestimmten Ereignisfeld gesucht. Die Kriterien der erweiterten Suche basieren auf den Kurznamen der einzelnen Ereignisfelder sowie der Suchlogik für den Index. In der folgenden Tabelle werden die Felder beschrieben, die Kurznamen für die erweiterte Suche genannt und es wird angegeben, ob die Felder in der Basisansicht bzw. der Detailansicht für Ereignisse angezeigt werden.

Verwenden Sie für die Suche nach einem Wert in einem bestimmten Feld den Kurznamen des Feldes (weitere Informationen siehe Tabelle 4-1 auf Seite 31), einen Punkt und den Wert. Um beispielsweise nach einem Authentifizierungsversuch von Benutzer2 zu suchen, geben Sie den folgenden Text in das Suchfeld ein:

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



Mehrere erweiterte Suchkriterien können mithilfe der folgenden Booleschen Operatoren kombiniert werden:

- UND (Großschreibung beachten)
- ODER (Großschreibung beachten)

- NICHT (Großschreibung beachten; kann nicht als einziges Suchkriterium verwendet werden)
- +
- -

Sonderzeichen müssen durch das Symbol \ ersetzt werden:

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

Die erweiterten Suchkriterien sind den Suchkriterien für das Open Source-Paket Apache Lucene nachgebildet. Weitere Details zu den Suchkriterien finden Sie im Internet unter Lucene Query Parser Syntax (http://lucene.apache.org/java/2_3_2/queryparsersyntax.html).

4.3 Anzeigen von Suchergebnissen

Suchvorgänge geben einen Satz an Ereignissen zurück. Benutzer können Basisinformationen oder ausführliche Informationen zu Ereignissen anzeigen und die Anzahl der Ergebnisse pro Seite konfigurieren. Suchergebnisse werden stapelweise zurückgegeben. Die Standardstapelgröße beträgt 25 Ergebnisse, kann jedoch leicht konfiguriert werden.

- Abschnitt 4.3.1, „Basisereignisansicht“, auf Seite 28
- Abschnitt 4.3.2, „Ereignisansicht mit Details“, auf Seite 29
- Abschnitt 4.3.3, „Verfeinern der Suchergebnisse“, auf Seite 29

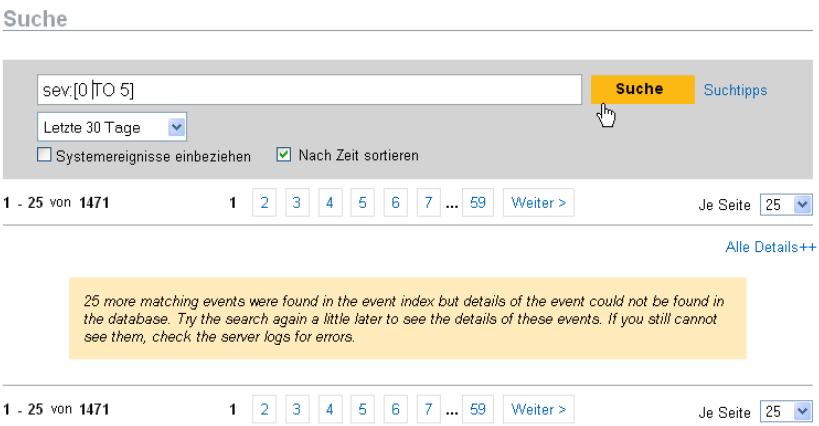
4.3.1 Basisereignisansicht

Die Informationen in jedem Ereignis werden nach Initiatorinformationen und Zielinformationen gruppiert. Wenn für ein bestimmtes Ereignisfeld keine Daten verfügbar sind, werden die Felder mit *Unbekannt* gekennzeichnet.

Abbildung 4-2 *Basisereignisansicht*

Es kann vorkommen, dass die Suchengine Ereignisse schneller indiziert als diese in die Datenbank eingefügt werden. Falls ein Benutzer eine Suche ausführt, die noch nicht in die Datenbank eingefügte Ereignisse ausgibt, gibt das System eine Meldung aus, dass eine Anzahl von Ereignissen der Suchabfrage entsprechen, jedoch nicht in der Datenbank gefunden wurden. Im Allgemeinen sind die Ereignisse in der Datenbank, wenn Sie die Suche zu einem späteren Zeitpunkt erneut ausführen. Die Suche wird dann erfolgreich ausgeführt.

Abbildung 4-3 *Indizierte, jedoch nicht in der Datenbank enthaltene Ereignisse*



4.3.2 Ereignisansicht mit Details

Durch Klicken auf den Link *Details* rechts auf der Seite können Benutzer zusätzliche Details zu den Ereignissen anzeigen. Die Details für alle Ereignisse auf einer Seite können durch Klicken auf den Link "Alle Details++" oder *Alle Details--* maximiert oder minimiert werden. Diese Einstellung bleibt erhalten, während Sie durch mehrere Ergebnisseiten blättern oder neue Suchvorgänge durchführen.

Abbildung 4-4 *Ereignisansicht mit Details*

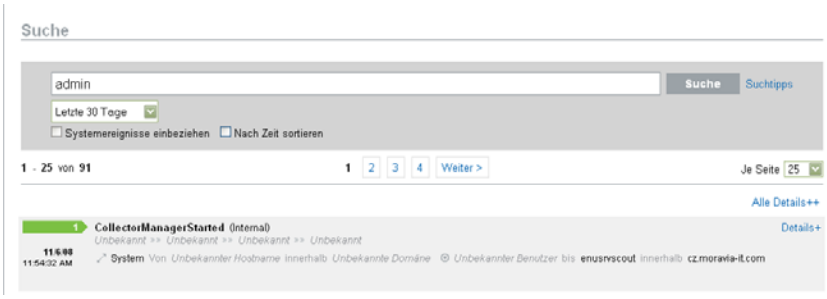
Das obige Ereignis entspricht dem Ereignis in Abbildung 4-2 auf Seite 28, jedoch verfügt das obige Ereignis über eine erweiterte Ansicht mit zusätzlichen Datenfeldern, die möglicherweise gefüllt wurden.

4.3.3 Verfeinern der Suchergebnisse

Nach der Anzeige der Ergebnisse einer Suche ist es eventuell erforderlich, die Suchergebnisse zu verfeinern und zusätzliche Suchkriterien hinzuzufügen. Der Name eines Initiatorbenutzers könnte beispielsweise in den Suchergebnissen mehrmals erscheinen, weshalb weitere Ereignisse dieses Initiators angezeigt werden sollen.

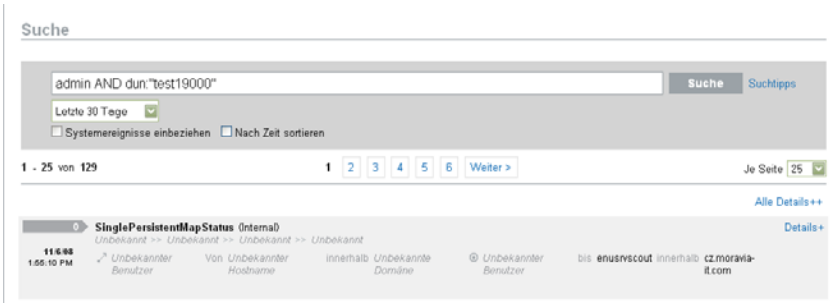
So filtern Sie die Suchergebnisse nach einem bestimmten Wert, der in den Suchergebnissen erscheint:

1. Suchen Sie das gewünschte Filterkriterium in den Suchergebnissen.
2. Klicken Sie auf den Wert (Beispiel: Ziel-Hostname test1900), nach dem die Ergebnisse gefiltert werden sollen.



Tipp: Der Wert wird jetzt mit einem AND-Operator dem Filter hinzugefügt. Sie können den Wert auch mit einem NOT-Operator hinzufügen. Drücken Sie dabei die Alt-Taste, wenn Sie auf den Wert klicken.

3 Klicken Sie auf *Suchen*.



Einige Felder können zum Optimieren der Suche auf diese Weise nicht ausgewählt werden:

- EventTime
- Message
- Alle mit dem Reporter verknüpften Felder
- Alle mit dem Observer verknüpften Felder
- Alle Felder mit dem Wert `Unbekannt`

4.4 Ereignisfelder

Abhängig vom jeweiligen Ereignis verfügt jedes Ereignis über Felder, die nicht ausgefüllt sein müssen. Die Werte für diese Ereignisfelder können Sie anzeigen, indem Sie eine Suche durchführen oder einen Bericht ausführen. Jedes Feld verfügt über einen Kurznamen, der in der erweiterten Suche verwendet wird. Die Werte für die meisten dieser Felder werden in der detaillierten Ereignisansicht angezeigt. Andere Werte werden ebenfalls in der Basisereignisansicht angezeigt.

Tabelle 4-1 *Ereignisfelder*

Feld	Kurzname	Beschreibung	Anzeige in der Basisansicht	Anzeige in der Detailansicht
Schweregrad	sev	Schweregrad eines Ereignisses auf einer Skala von 0 (informativ) bis 5 (kritisch)	X	X
EventTime	dt	Zeitstempel des Ereignisses. Hierbei handelt es sich entweder um den Zeitstempel von Identity Audit oder um den Zeitstempel der ursprünglichen Ereignisquelle (falls "Verbürgte Ereigniszeit" aktiviert wurde)	X	X
EventName	evt	Kurzname des Ereignisses	X	X
Meldung	msg	Detaillierte Ereignismeldung		X
ProductName	pn	Produkt, das das Ereignis generiert hat; die Ereignisquelle. Wird nach dem Ereignisnamen angezeigt.	X	X
InitUserName	sun	Benutzername des Benutzers, der das Ereignis initiiert hat	X	X
InitUserID	iuid	Benutzer-ID des Benutzers, der das Ereignis initiiert hat		X
InitUserDomain	rv35	Domäne des Benutzers, der das Ereignis initiiert hat Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
InitHostName	shn	Hostname des Computers, auf dem das Ereignis initiiert wurde	X	X
InitHostDomain	rv42	Domäne des Computers, auf dem das Ereignis initiiert wurde	X	X
InitIP	sip	IP-Adresse des Computers, auf dem das Ereignis initiiert wurde		X
InitServicePort	spint	Portnummer, von der aus das Ereignis initiiert wurde (z.B. HTTP)		X
InitServicePortName	sp	Typ des Ports, von dem aus das Ereignis initiiert wurde (z.B. HTTP)		X
TargetUserName	dun	Benutzername des Benutzers, der als Ziel des Ereignisses diente	X	X
TargetUserID	tuid	Benutzer-ID des Benutzers, der als Ziel des Ereignisses diente		X

Feld	Kurzname	Beschreibung	Anzeige in der Basisansicht	Anzeige in der Detailansicht
TargetUserDomain	rv35	Domäne des Benutzers, der als Ziel des Ereignisses diente Durchsuchbar, aber in keiner Ereignisansicht angezeigt		X
TargetHostName	dhn	Hostname des Computers, der als Ziel des Ereignisses diente	X	X
TargetHostDomain	rv45	Domäne des Computers, der als Ziel des Ereignisses diente	X	X
TargetIP	dip	IP-Adresse des Computers, der als Ziel des Ereignisses diente		X
TargetServicePort	dpint	Portnummer, die als Ziel des Ereignisses diente (z.B. 80)		X
TargetServicePortName	dp	Typ des Ports, der als Ziel des Ereignisses diente (z.B. HTTP)		X
TargetTrustName	ttn	Funktion des Benutzers, der als Ziel des Ereignisses diente (z.B. FinanceAdmin) Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
TargetTrustID	ttid	Nummerische ID, die die Funktion des Benutzers darstellt, der als Ziel des Ereignisses diente Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
TargetTrustDomain	ttd	Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
EffectiveUserName	euname	Name des Benutzers, den der InitUser verkörpert (z.B. `root` mit dem Kürzel `su`); folgt dem *Benutzernamen des Initiators (Benutzer-ID des Initiators*) *wie* in der detaillierten Ereignisansicht		X
EffectiveUserID	euid	Nummerische ID des Benutzers, den der InitUser verkörpert (z.B. `root` mit dem Kürzel `su`)		X
ObserverHostName	sn	Hostname des Computers, der das Ereignis an das Verwaltungssystem für Sicherheitsinformationsereignisse weitergeleitet hat (z.B. der Hostnamen eines Syslog-Servers). Durchsuchbar, aber in keiner Ereignisansicht angezeigt		

Feld	Kurzname	Beschreibung	Anzeige in der Basisansicht	Anzeige in der Detailansicht
ObserverHostDomain	obsdom	Domäne des Computers, der das Ereignis an das Verwaltungssystem für Sicherheitsinformationsereignisse weitergeleitet hat (z.B. die Domäne eines Syslog-Servers). Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
ObserverIP	obsip	IP-Adresse des Computers, der das Ereignis an das Verwaltungssystem für Sicherheitsinformationsereignisse weitergeleitet hat (z.B. die IP-Adresse eines Syslog-Servers). Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
ReporterHostName	rn	Hostname des Computers, der das Ereignis an einen Beobachter gemeldet hat Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
ReporterHostDomain	repdom	Domäne des Computers, der das Ereignis an einen Beobachter gemeldet hat Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
ReporterIP	repip	IP-Adresse des Computers, der das Ereignis an einen Beobachter gemeldet hat Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
SensorType	st	Der Einzelbuchstabenbezeichner für den Sensortyp (N=Netzwerk, H=Host, O=Betriebssystem, A und I=Audit-Ereignisse von Identity Audit, P=Identity Audit-Leistungsereignisse). Durchsuchbar, aber in keiner Ereignisansicht angezeigt		
DataName	fn	Im Ereignis gemeldeter Datenobjektname (z.B. der Dateiname oder der Name der Datenbanktabelle)		X
DataContext	rv36	Container für das FileName-Datenobjekt (z. B. ein Verzeichnis für eine Datei oder eine Datenbankinstanz für eine Datenbanktabelle)		X

Feld	Kurzname	Beschreibung	Anzeige in der Basisansicht	Anzeige in der Detailansicht
TaxonomyLevel1	rv50	Zielklassifikation für das Ereignis. Angezeigt unter dem Ereignisnamen im Format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	Unterzielklassifikation für das Ereignis. Angezeigt unter dem Ereignisnamen im Format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel3	rv52	Aktionsinformationen für das Ereignis. Angezeigt unter dem Ereignisnamen im Format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	Detailinformationen für das Ereignis. Angezeigt unter dem Ereignisnamen im Format: TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

Einige Felder sind in Tokens übersetzt. Wenn Felder in Tokens übersetzt werden, ist es möglich, nach einem einzelnen Wort im Feld ohne Platzhalter zu suchen. Die Felder werden auf der Basis von Leerzeichen und anderen Sonderzeichen in Tokens übersetzt. Für diese Felder werden Artikel wie "ein" oder "der" aus dem Suchindex entfernt.

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

Berichte

5

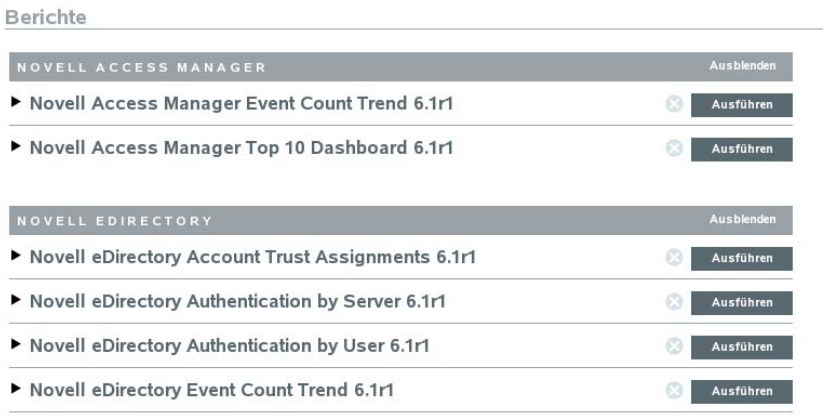
In diesem Kapitel wird beschrieben, wie Berichte in Novell® Identity Audit ausgeführt, angezeigt und verwaltet werden.

5.1 Überblick

Identity Audit wird mit einem Kernsatz an Berichtvorlagen installiert, die sich auf Novell-Anwendungen beziehen. Jeder Benutzer von Identity Audit kann einen Bericht ausführen und dabei die gewünschten Parameter (wie Start- und Enddatum) verwenden. Die Berichtergebnisse werden mit dem Namen gespeichert, den der Benutzer dafür wählt. Nach Ausführung des Berichts können die Ergebnisse von jedem Identity Audit-Benutzer abgerufen und als PDF-Datei angezeigt werden.

Berichte werden in Kategorien organisiert. Identity Audit wird mit Berichten für jede unterstützte Ereignisquelle installiert.

Abbildung 5-1 *Nach Kategorie organisierte Berichte*



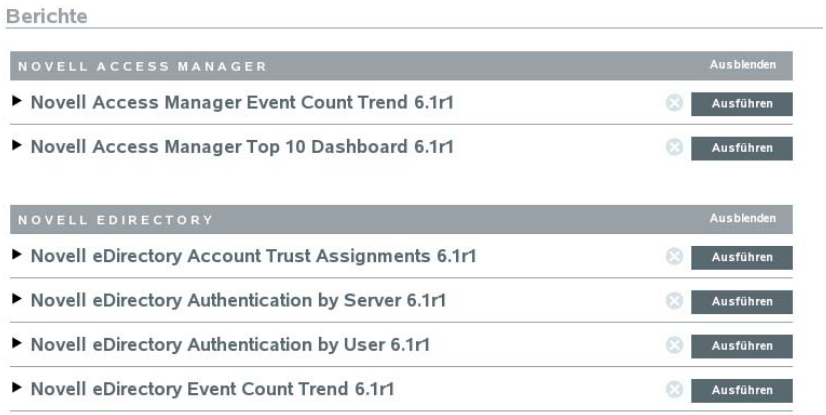
5.2 Ausführen von Berichten

Identity Audit wird mit einer Reihe von Berichten für die einzelnen Produktkategorien installiert. Die Ausführung von Berichten erfolgt asynchron, damit Benutzer in der Anwendung weiterarbeiten können, während der Bericht ausgeführt wird. Die PDF-Berichtergebnisse können nach Fertigstellung des Berichts von jedem Benutzer angezeigt werden.

Viele Berichtdefinitionen enthalten Parameter. Vor dem Ausführen der Berichte wird der Benutzer aufgefordert, diese Parameter festzulegen. Abhängig davon, wie der Entwickler den Bericht konzipiert hat, kann es sich bei den Berichtparametern um Text, Zahlen, Boolsche Werte oder Daten handeln. Für einen Parameter kann ein Standardwert definiert sein oder Sie können aus einer Liste bestehend aus Werten der Identity Audit-Datenbank Werte auswählen.

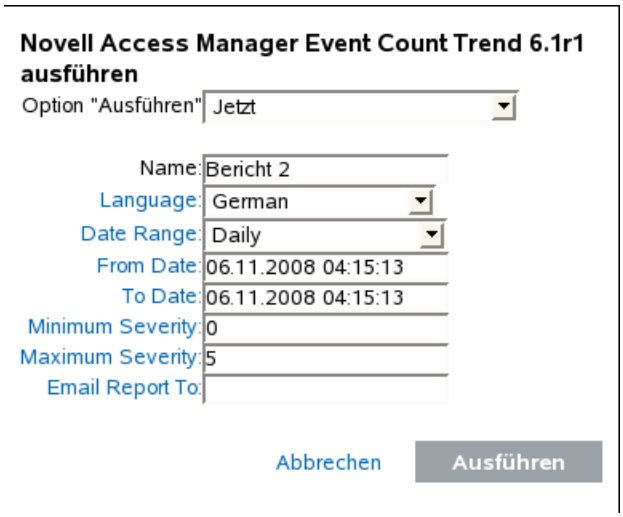
So führen Sie einen Bericht aus:

1 Klicken Sie in Identity Audit auf *Berichte*, um die verfügbaren Berichte anzuzeigen.



Klicken Sie bei Bedarf auf eine Berichtdefinition, um sie zu erweitern. Wenn *Beispielbericht* angezeigt wird, können Sie auf *Anzeigen* klicken, um eine Vorschau des vollständigen Berichts mit Beispieldaten anzuzeigen.

2 Wählen Sie den Bericht aus, der ausgeführt werden soll, und klicken Sie auf *Ausführen*.



3 Legen Sie den Zeitplan für die Ausführung des Berichts fest. Soll der Bericht zu einem späteren Zeitpunkt ausgeführt werden, müssen Sie eine Anfangszeit eingeben.

- Jetzt: Dies ist der Standard. Der Bericht wird sofort ausgeführt.
- Einmal: Bei dieser Einstellung wird der Bericht einmal zum festgelegten Datum und Zeitpunkt ausgeführt.

- Täglich: Bei dieser Einstellung wird der Bericht einmal täglich zur festgelegten Zeit ausgeführt.
- Wöchentlich: Bei dieser Einstellung wird der Bericht einmal pro Woche am gleichen Tag zur festgelegten Zeit ausgeführt.
- Monatlich: Bei dieser Einstellung wird der Bericht jeden Monat am festgelegten Datum und zum festgelegten Zeitpunkt ausgeführt. Beispiel: Wenn das Anfangsdatum der 28. Oktober und die Zeit 14.00 Uhr ist, wird der Bericht jeden Monat am 28. des Monats um 14.00 Uhr ausgeführt.

Hinweis: Alle Zeiteinstellungen basieren auf den lokalen Zeiteinstellungen des Browsers.

---

4 Geben Sie einen Namen zur Identifikation der Berichtergebnisse ein.

Da der Benutzername und die Uhrzeit auch verwendet werden, um die Berichtergebnisse zu identifizieren, braucht der Berichtname nicht eindeutig zu sein.

5 Wählen Sie die Sprache, in der der Bericht angezeigt werden soll (Englisch, Französisch, Deutsch, Italienisch, Japanisch, Traditionelles Chinesisch, Vereinfachtes Chinesisch, Spanisch oder Portugiesisch).

6 Wählen Sie den Berichtstyp aus. Alle Zeiträume basieren auf den lokalen Zeiteinstellungen des Browsers.

- Täglich: Der Bericht zeigt Ereignisse ab Mitternacht des aktuellen Tages bis 23.59 Uhr des aktuellen Tages an. Ist der aktuelle Zeitpunkt 8.00 Uhr, zeigt der Bericht Daten über einen Zeitraum von 8 Stunden an (von Mitternacht bis 8.00 Uhr).
- Wöchentlich: Der Bericht zeigt Ereignisse von Sonntag Mitternacht der aktuellen Woche bis zum Ende des aktuellen Tages an.
- Monatlich: Der Bericht zeigt Ereignisse von Mitternacht des ersten Tages des Monats bis zum Ende des aktuellen Tages an.
- Benutzerdefinierter Datumsbereich: Bei dieser Einstellung müssen Sie ein Anfangs- und ein Enddatum eingeben.
- Vortag: Der Bericht zeigt Ereignisse von gestern Mitternacht bis 23.59 Uhr gestern an.

7 Wenn Sie "Benutzerdefinierter Datumsbereich" ausgewählt haben, geben Sie ein Anfangs- ("Von") und ein Enddatum ("Bis") für den Bericht ein.

Hinweis: Wenn Sie "Täglich", "Wöchentlich", "Monatlich" oder "Vortag" für den Berichtstyp gewählt haben, werden diese Zeiteinstellungen ignoriert.

---

8 Legen Sie für die Ereignisse, die im Bericht aufgeführt werden sollen, den "Mindestschweregrad" fest.

9 Legen Sie für die Ereignisse, die im Bericht aufgeführt werden sollen, den "Höchstschweregrad" fest.

10 Möchten Sie den Bericht an einen oder mehrere Benutzer senden, geben Sie die Email-Adressen durch Kommata getrennt ein.

Hinweis: Um Berichte zu versenden, muss der Administrator den Mailserver unter *Regeln* > *Konfiguration* konfigurieren.

---

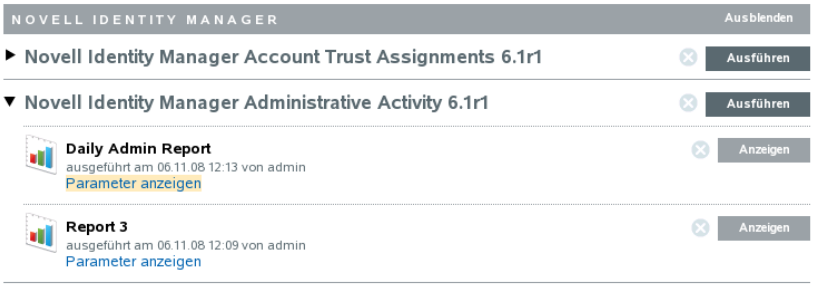
11 Klicken Sie auf *Ausführen*.

Ein Eintrag mit Berichtergebnissen wird erstellt und per Email an die festgelegten Empfänger gesendet.

5.3 Anzeigen von Berichten

Identity Audit-Benutzer können Berichte in der Identity Audit-Anwendung anzeigen. Andere Benutzer erhalten den Bericht unter Umständen als `.pdf`-Datei per Email.

1 Klicken Sie zum Anzeigen der Berichtergebnisliste auf *Anzeigen*. Alle vorher ausgeführten Berichte werden mit dem benutzerdefinierten Berichtnamen, dem Benutzer, der sie ausgeführt hat und mit der Uhrzeit der Ausführung des Berichts angezeigt.



2 Klicken Sie auf *Parameter anzeigen*, um die genauen Werte anzuzeigen, die zur Ausführung des Berichts verwendet wurden.

- Für den Berichtstyp gelten die folgenden Abkürzungen: D=Täglich, W=Wöchentlich, M=Monatlich, DR=Benutzerdefinierter Zeitraum und PD=Vortag.
- Für die Sprachen gelten die folgenden Abkürzungen: en=Englisch, fr=Französisch, de=Deutsch, it=Italienisch, ja=Japanisch, pt=Brasilianisches Portugiesisch, es=Spanisch, zh=Vereinfachtes Chinesisch und zh_TW=Traditionelles Chinesisch.

3 Klicken Sie auf *Anzeigen*, um die gewünschten Berichtergebnisse anzuzeigen. Die Berichtergebnisse werden in einem neuen Fenster im `.pdf`-Format angezeigt.

Tipp: Die Berichtergebnisse sind von neu nach alt sortiert.

5.4 Verwalten von Berichten

Identity Audit-Benutzer können Berichte hinzufügen, löschen, aktualisieren und einplanen.

- Abschnitt 5.4.1, „Hinzufügen von Berichten“, auf Seite 39
- Abschnitt 5.4.2, „Umbenennen von Berichtergebnissen“, auf Seite 41
- Abschnitt 5.4.3, „Löschen von Berichten“, auf Seite 41
- Abschnitt 5.4.4, „Aktualisieren von Berichtdefinitionen“, auf Seite 41

5.4.1 Hinzufügen von Berichten

Im Lieferumfang von Identity Audit sind Berichte enthalten, Sie können jedoch neue Bericht-Plugins (bestimmte `ZIP`-Dateien, die die Berichtdefinition und Metadaten enthalten) in Identity Audit hochladen. Wenn im System keine Berichte vorhanden sind, wird der folgende Bildschirm angezeigt:

Abbildung 5-2 *Keine Berichte geladen*

So fügen Sie einen Bericht hinzu:

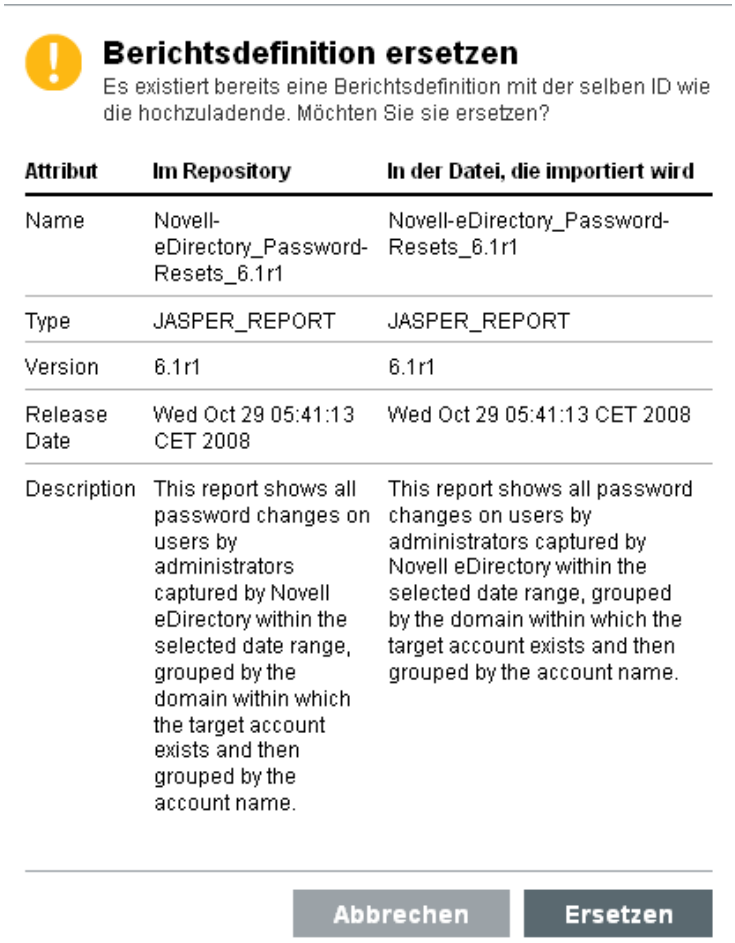
1. Klicken Sie links im Bildschirm auf die Schaltfläche *Berichte*.
2. Klicken Sie auf die Schaltfläche *Bericht hochladen*.

3 Navigieren Sie zu dem Speicherort der `ZIP`-Datei für das Bericht-Plugin auf Ihrem lokalen Computer.

4 Klicken Sie auf *Öffnen*.

5 Klicken Sie auf *Speichern*.

6 Falls derselbe Bericht bereits im Bericht-Repository vorhanden ist (basierend auf der eindeutigen Bericht-ID), zeigt Identity Audit die Details beider Berichte, also des Berichts im System und des importierten Berichts, an. Sie entscheiden, ob Sie den vorhandenen Bericht ersetzen möchten. Im unten angezeigten Fall handelt es sich bei dem importierten Bericht um die gleiche Version des bereits vorhandenen Berichts.



Berichtsdefinition ersetzen

Es existiert bereits eine Berichtsdefinition mit der selben ID wie die hochzuladende. Möchten Sie sie ersetzen?

Attribut	Im Repository	In der Datei, die importiert wird
Name	Novell-eDirectory_Password-Resets_6.1r1	Novell-eDirectory_Password-Resets_6.1r1
Type	JASPER_REPORT	JASPER_REPORT
Version	6.1r1	6.1r1
Release Date	Wed Oct 29 05:41:13 CET 2008	Wed Oct 29 05:41:13 CET 2008
Description	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.	This report shows all password changes on users by administrators captured by Novell eDirectory within the selected date range, grouped by the domain within which the target account exists and then grouped by the account name.

7 Die neue Berichtdefinition wird der Liste in alphabetischer Reihenfolge hinzugefügt und kann gegebenenfalls sofort ausgeführt werden.

Herunterladen neuer oder aktualisierter Berichte

Sie können neue oder von Novell aktualisierte Berichte von der Novell Content-Website (http://support.novell.com/products/identityaudit/identityaudit10.html) herunterladen.

Erstellen neuer Berichte

Mithilfe von JasperForge* iReport können Sie Berichte ändern oder selber verfassen. JasperForge* iReport ist ein grafisches Berichterstellungsprogramm für Jasper-Berichte. iReport ist ein Open Source-Tool zur Berichtentwicklung, das Sie von der Website JasperForge.org (http://jasperforge.org/plugins/project/project_home.php?group_id=83) herunterladen können (ab dem Zeitpunkt dieser Veröffentlichung).

Neue oder geänderte Berichte können zusätzliche Datenbankfelder enthalten, die nicht in der Identity Audit Web-Benutzeroberfläche angezeigt werden. Sie müssen den Datei- und Formatanforderungen des Bericht-Plugins entsprechen. Weitere Informationen zu Datenbankfeldern, Datei- und Formatanforderungen für Bericht-Plugins erhalten Sie auf der Sentinel SDK-Website (http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel).

5.4.2 Umbenennen von Berichtergebnissen

Berichtergebnisse (jedoch keine Berichtdefinitionen) können über die Identity Audit-Benutzeroberfläche umbenannt werden.

1. Klicken Sie links im Bildschirm auf die Schaltfläche *Berichte*.
2. Klicken Sie auf einen Berichtnamen, um den Bericht zu erweitern.
3. Klicken Sie auf den Namen des Berichts, den Sie umbenennen möchten.
4. Geben Sie den neuen Namen ein.
5. Klicken Sie auf *Umbenennen*.

5.4.3 Löschen von Berichten

Benutzer können entweder einen Berichtergebnissatz oder eine Berichtdefinition löschen. Wird eine Berichtdefinition gelöscht, so werden alle verknüpften Berichtergebnisse ebenfalls gelöscht.

Wenn ein Bericht gelöscht wird, der gerade in Bearbeitung ist, wird die Abfrage in der Datenbank abgebrochen.

5.4.4 Aktualisieren von Berichtdefinitionen

Sie können aktualisierte Berichte in Identity Audit hochladen, um vorhandene Berichte zu ersetzen. Weitere Informationen finden Sie unter Abschnitt 5.4.1, „Hinzufügen von Berichten“, auf Seite 39.

Datensammlung

6

Administratoren können die Datensammlung für Novell® Identity Audit konfigurieren und überwachen. Identity Audit wird mit der Möglichkeit zur Sammlung von Daten aus einer Vielzahl an Novell-Anwendungen mithilfe des Novell Audit-Plattformagenten installiert. Informationen zu den unterstützten Versionen des Plattformagenten finden Sie unter Abschnitt 2.4, „Unterstützter Plattformagent“, auf Seite 15.

6.1 Konfigurieren von Ereignisquellen

Obwohl Identity Audit so vorkonfiguriert wurde, dass es Daten aus mehreren Novell-Anwendungen akzeptiert, müssen die Anwendungsserver (Ereignisquellen) noch dahingehend konfiguriert werden, dass sie Daten an den Identity Audit-Server senden. Dies geschieht beim Einrichten von Identity Audit. Weitere Informationen finden Sie unter Abschnitt 3.2, „Konfigurieren von Ereignisquellen“, auf Seite 20.

6.2 Status der Datensammlung

Administratoren können die Datensammlung global oder nach Anwendung aktivieren oder deaktivieren. Des Weiteren können die Administratoren auch Zustandsinformationen zu jeder Anwendung anzeigen.

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie auf *Sammlung* in der oberen rechten Ecke der Seite.

3 Aktivieren oder deaktivieren Sie die globale Datensammlung durch den Audit-Server.

4 Aktivieren oder deaktivieren Sie anwendungsspezifische Datensammlungen der Ereignisquellen.

5 Klicken Sie auf *Details anzeigen*, um weitere Informationen zu den aktiven Verbindungen für jede Anwendung anzuzeigen.

Änderungen auf dieser Seite werden sofort wirksam.

- Abschnitt 6.2.1, „Audit-Server“, auf Seite 44
- Abschnitt 6.2.2, „Ereignisquellen“, auf Seite 45

6.2.1 Audit-Server

Unter *Audit-Server* können Administratoren mithilfe der Optionen "Ein" und "Aus" die globale Datensammlung aktivieren bzw. deaktivieren. Der Zustand des Audit-Servers wird ebenfalls angezeigt.

Fehlerfrei: Ein grünes Kennzeichen gibt an, dass der Audit-Server in fehlerfreiem Zustand ist: Er ist eingeschaltet, überwacht einen Port und es liegen keine ungelösten Fehler vor.

Fehler: Ein rotes Kennzeichen gibt an, dass auf dem Audit-Server ein Fehler aufgetreten ist. Weitere Informationen finden Sie in den `server0.*.log`-Dateien.

Offline: Ein graues Kennzeichen gibt an, dass der Audit-Server von einem Administrator in den offline-Modus gestellt wurde.

6.2.2 Ereignisquellen

Unter *Ereignisquellen* können Administratoren die Datensammlung auf Anwendungsebene aktivieren. Diese Einstellungen können die Datensammlung für mehrere Server (z. B. mehrerer eDirectory-Instanzen) beeinflussen.

Hinweis: Über diese Einstellungen wird die Identity Audit-Datensammlung für die aufgelisteten Anwendungen aktiviert oder deaktiviert. Durch die Einstellungen werden keine Services auf den Computern der Ereignisquellen gestartet oder angehalten.

Der Zustand für jedes Symbol wird durch ein rotes, gelbes, grünes oder schwarzes Symbol angezeigt. Für die meisten Statusanzeigen können Sie durch Klicken auf *Details anzeigen* weitere Informationen aufrufen.

Fehlerfrei: Ein grünes Kennzeichen gibt an, dass die Ereignisquelle sich in einem fehlerfreien Zustand befindet und Identity Audit Daten von der Quelle erhalten hat.

Warnung: Ein gelbes Kennzeichen gibt eine Warnmeldung an. Häufige Ursache für die Warnmeldung ist, dass die Anwendung in Identity Audit zwar eingeschaltet ist, jedoch noch keine Daten gesendet hat. Beispiel: Dieser Fall tritt ein, wenn der Plattformagent auf der Ereignisquelle nicht ordnungsgemäß konfiguriert wurde, um Daten an Identity Audit zu senden, oder wenn die Ereignisprotokollierung für die Anwendung nicht aktiviert wurde. Klicken Sie auf *Details anzeigen*, um weitere Informationen zu erhalten.

Fehler: Bei einem roten Kennzeichen gibt der Identity Audit-Server einen Fehler beim Herstellen einer Verbindung zur Anwendung oder beim Empfangen der Daten von der Anwendung aus. Klicken Sie auf *Details anzeigen*, um weitere Informationen zu erhalten.

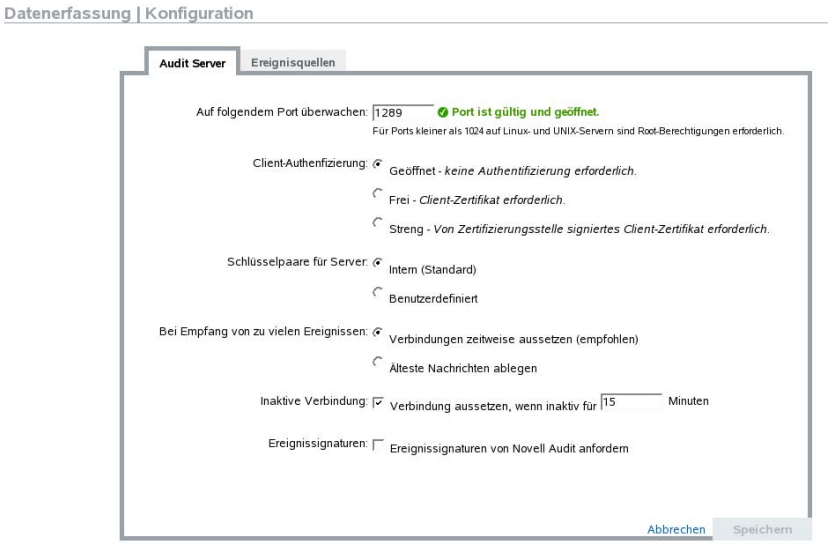
Offline: Ein graues Kennzeichen gibt an, dass die Ereignisquelle ausgeschaltet wurde. Identity Audit verarbeitet keine Daten von dieser Quelle.

Für jede Online-Datenquelle zeigt Identity Audit die berechnete Ereignisverarbeitungsrate für eingehende Ereignisse an. Die Ereignisverarbeitungsrate wird alle 60 Sekunden neu berechnet.

6.3 Audit Server-Optionen

Administratoren können einige Einstellungen ändern, die die Überwachung der Daten von den Ereignisquellenanwendungen durch Identity Audit betrifft, einschließlich des Ports, auf dem Identity Audit die Überwachung durchführt, sowie die Art der Authentifizierung zwischen der Ereignisquelle und Identity Audit.

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie oben am Bildschirm auf den Link *Sammlung*.
3. Klicken Sie rechts am Bildschirm auf den Link *Konfiguration*.
4. Vergewissern Sie sich, dass *Audit Server* ausgewählt ist.



5 Geben Sie den Port ein, den der Identity Audit-Server auf Meldungen von den Ereignisquellen hin überwachen soll. Weitere Informationen finden Sie unter Abschnitt 6.3.1, „Konfiguration des Ports und Port-Weiterleitung“, auf Seite 47.

6 Legen Sie die entsprechenden Einstellungen für die Schlüsselpaare für Client-Authentifizierung und Server fest. Weitere Informationen finden Sie unter Abschnitt 6.3.2, „Client-Authentifizierung“, auf Seite 47.

7 Wählen Sie das Verhalten des Identity Audit-Servers aus, wenn der Puffer mit zu vielen Ereignissen gefüllt ist.

Verbindungen zeitweise aussetzen: Diese Einstellung unterbricht die vorhandenen Verbindungen und stoppt das Akzeptieren neuer Verbindungen, bis der Puffer wieder über Speicher für neue Meldungen verfügt. In der Zwischenzeit werden die Meldungen in den Ereignisquellen zwischengespeichert.

Älteste Nachrichten ablegen: Diese Einstellung verwirft die ältesten Meldungen, um neue Meldungen akzeptieren zu können.

Warnung: Es ist keine unterstützte Methode verfügbar, um nach Wählen der Option *Älteste Nachrichten ablegen* die verworfenen Meldungen wiederherzustellen.

---

8 Wählen Sie *Inaktive Verbindung*, um die Verbindung zu Ereignisquellen zu trennen, die über einen bestimmten Zeitraum keine Daten gesendet haben.

Die Verbindungen zu den Ereignisquellen werden automatisch wieder hergestellt, wenn erneut Daten gesendet werden.

9 Geben Sie die Anzahl der Minuten ein, bevor eine ruhende Verbindung getrennt wird.

10 Wählen Sie *Ereignissignaturen*, um zusammen mit dem Ereignis eine Signatur zu erhalten.

Hinweis: Sie können nur Signaturen erhalten, wenn der Plattformagent auf der Ereignisquelle ordnungsgemäß konfiguriert wurde. Weitere Informationen finden Sie unter Abschnitt 6.1, „Konfigurieren von Ereignisquellen“, auf Seite 43.

---

11 Klicken Sie auf *Speichern*.

6.3.1 Konfiguration des Ports und Port-Weiterleitung

Port 1289 ist der Standardport, auf dem Identity Audit die Nachrichten der Plattformagenten überwacht. Wenn der Port festgelegt ist, überprüft das System, ob der Port gültig und offen ist.

Für die Bindung an Ports kleiner als 1024 sind root-Berechtigungen erforderlich. Novell empfiehlt, dass Sie einen Port größer als 1024 verwenden. Sie können die Quellgeräte an einen höheren Port senden oder die Port-Weiterleitung auf dem Identity Audit-Server verwenden.

So ändern Sie die Ereignisquelle, damit sie an einen anderen Port sendet:

1. Melden Sie sich am Ereignisquellen-Computer an.
2. Öffnen Sie die Datei `logevent` zur Bearbeitung. Je nach Betriebssystem befindet sich diese Datei in den folgenden Verzeichnissen:
   - Linux: `/etc/logevent.conf`
   - Windows: `C:\WINDOWS\logevent.cfg`
   - NetWare: `SYS:\etc\logevent.cfg`
   - Solaris: `/etc/logevent.conf`
3. Stellen Sie den Parameter "LogEnginePort" auf den gewünschten Port ein.
4. Speichern Sie die Datei.
5. Starten Sie den Plattformagenten neu. Dieser Vorgang ist abhängig vom Betriebssystem und der Anwendung. Booten Sie den Computer neu. Weitere Anleitungen finden Sie auf der Novell Documentation-Website (http://www.novell.com/documentation) in der anwendungsspezifischen Dokumentation.

So konfigurieren Sie die Port-Weiterleitung auf den Identity Audit-Server:

1. Melden Sie sich als `root`-Benutzer (oder `su` an `root`) am Betriebssystem des Identity Audit-Servers an.
2. Öffnen Sie die Datei `/etc/init.d/boot.local` im Bearbeitungsmodus.
3. Fügen Sie gegen Ende des Boot-Vorgangs den folgenden Befehl hinzu:

   `iptables -A PREROUTING -t nat -p` *`protocol`* `--dport` *`incoming port`* `-j DNAT --to-destination` *`IP`*`:`*`rerouted port`*

   wenn *protocol* tcp oder udp ist, ist der *incoming port (eingehender Port)* der Port, an dem die Meldungen ankommen, und *IP:rerouted port (IP umgeleiteter Port)* die IP-Adresse des lokalen Computers und ein verfügbarer Port größer als 1024.
4. Speichern Sie die Änderungen.
5. Booten Sie den Computer neu. Falls Sie den Computer nicht sofort rebooten können, führen Sie in einer Befehlszeile den Befehl `iptables` aus.

6.3.2 Client-Authentifizierung

Ereignisquellen senden ihre Daten über eine SSL-Verbindung. Die Einstellung *Client-Authentifizierung* für den Identity Audit-Server legt fest, welche Art von Authentifizierung für die vom Plattformagenten für die Ereignisquellen ausgegebenen Zertifikate durchgeführt wird.

Offen: Keine Authentifizierung erforderlich. Identity Audit benötigt, erfordert oder bewertet kein Zertifikat von der Ereignisquelle.

Frei: Ein gültiges X.509-Zertifikat von der Ereignisquelle ist zwar erforderlich, wird jedoch nicht validiert. Das Zertifikat muss nicht von einer Zertifizierungsstelle signiert sein.

Streng: Ein gültiges X.509-Zertifikat von der Ereignisquelle ist erforderlich und muss von einer verbürgten Zertifizierungsstelle signiert sein. Falls die Ereignisquelle nicht über ein gültiges Zertifikat verfügt, akzeptiert Identity Audit die Ereignisdaten dieser Quelle nicht.

- „Erstellen eines Truststore“ auf Seite 48
- „Importieren eines Truststore“ auf Seite 48
- „Serverschlüsselpaar“ auf Seite 49

Erstellen eines Truststore

Für die strenge Authentifizierung muss ein Truststore vorhanden sein. Dieser muss entweder das Zertifikat der Ereignisquelle oder das Zertifikat für die Zertifizierungsstelle, welches das Zertifikat der Ereignisquelle signiert hat, enthalten. Wenn Sie über ein DER- oder PEM-Zertifikat verfügen, können Sie mithilfe des in Identity Audit mitgelieferten CreateTruststore-Dienstprogramms den Truststore erstellen.

1. Melden Sie sich als novell am Identity Audit-Server an.
2. Navigieren Sie zu `/opt/novell/identity_audit_1.0_x86/data/updates/done`.
3. Dekomprimieren Sie die Datei `audit_connector.zip`.

   ```
   unzip audit_connector.zip
   ```
4. Kopieren Sie entweder `TruststoreCreator.sh` oder `TruststoreCreator.bat` auf den Computer mit den bzw. dem Zertifikat(en) oder kopieren Sie die Zertifikate auf den Computer mit dem TruststoreCreator-Dienstprogramm.
5. Führen Sie das `TruststoreCreator.sh`-Dienstprogramm aus.

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

   In diesem Beispiel erstellt das TruststoreCreator-Dienstprogramm eine Keystore-Datei namens `my.keystore`. Diese Datei enthält die zwei Zertifikate `cert1.pem` und `cert2.pem`. Die Datei ist durch das Passwort *password1* geschützt.

Importieren eines Truststore

Für die strenge Authentifizierung kann der Administrator über die Schaltfläche *Importieren* einen Truststore importieren. So wird sichergestellt, dass nur autorisierte Ereignisquellen Daten an Identity Audit senden. Der Truststore muss entweder das Zertifikat der Ereignisquelle oder das Zertifikat der Zertifizierungsstelle, die das Zertifikat signierte, enthalten.

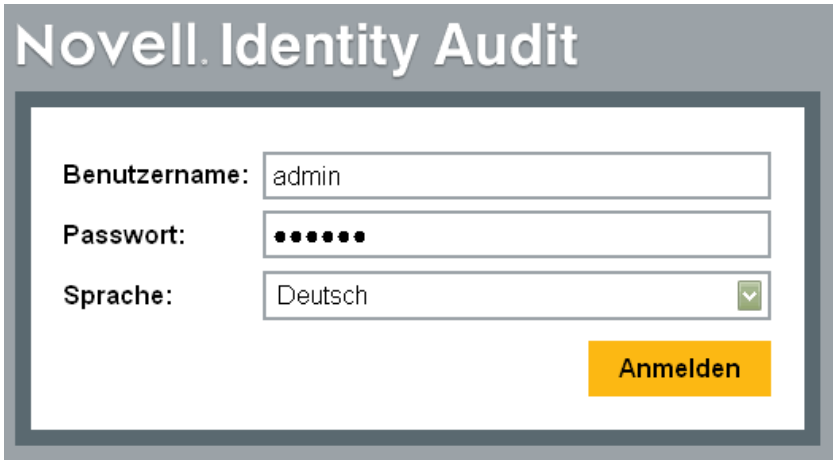
Der folgende Vorgang muss auf dem Computer mit dem Truststore ausgeführt werden. Sie können auf dem Computer mit dem Truststore einen Webbrowser öffnen oder den Truststore auf einen Computer mit einem Webbrowser verschieben.

So importieren Sie einen Truststore:

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie oben am Bildschirm auf den Link *Sammlung*.
3. Klicken Sie rechts am Bildschirm auf den Link *Konfiguration*.

4 Vergewissern Sie sich, dass die Registerkarte *Audit Server* ausgewählt ist.

5 Wählen Sie unter *Client-Authentifizierung* die Option *Streng*.

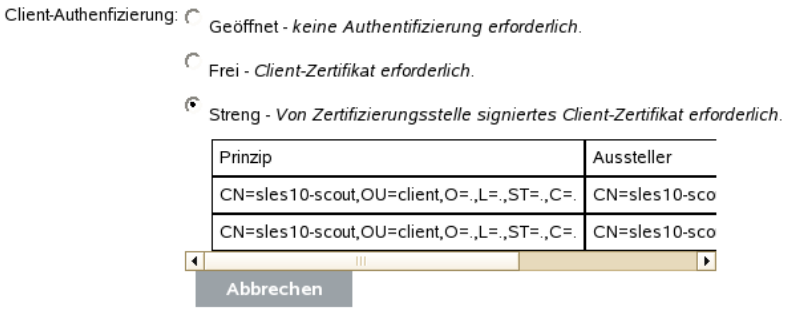


6 Klicken Sie auf *Durchsuchen*, und navigieren Sie zur Truststore-Datei, z. B. `my.keystore`.

7 Geben Sie das Passwort für die Truststore-Datei ein.

8 Klicken Sie auf *Importieren*.

9 Klicken Sie auf *Details*, um weitere Informationen zum Truststore aufzurufen.



10 Klicken Sie auf *Speichern*.

Nachdem der Truststore erfolgreich importiert wurde, können Sie auf *Details* klicken, um die im Truststore enthaltenen Zertifikate anzuzeigen.

Serverschlüsselpaar

Identity Audit wird mit einem integrierten Zertifikat installiert. Anhand dieses Zertifikats wird der Identity Audit-Server für die Ereignisquellen authentifiziert. Sie können dieses Zertifikat mit einem von einer öffentlichen Zertifizierungsstelle signierten Zertifikat überschreiben.

So ersetzen sie das integrierte Zertifikat:

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie oben am Bildschirm auf den Link *Sammlung*.

3 Klicken Sie rechts am Bildschirm auf den Link *Konfiguration*.

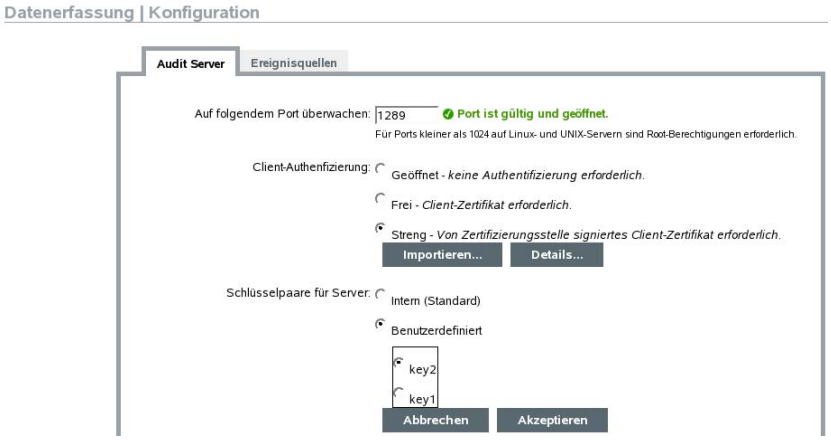
4 Vergewissern Sie sich, dass *Audit Server* ausgewählt ist.

5 Wählen Sie unter *Schlüsselpaare für Server* die Option *Benutzerdefiniert*.

6 Klicken Sie auf *Durchsuchen* und navigieren Sie zur Truststore-Datei.

7 Geben Sie das Passwort für die Truststore-Datei ein.

8 Klicken Sie auf *Importieren*.



Falls die Datei mehrere öffentlich-private Schlüsselpaare enthält, wählen Sie das gewünschte Schlüsselpaar aus und klicken Sie auf *OK*.

9 Klicken Sie auf *Details*, um weitere Informationen zum Serverschlüsselpaar anzuzeigen.

10 Klicken Sie auf *Speichern*.

6.4 Ereignisquellen

Auf der Seite *Ereignisquellen* können Administratoren konfigurieren, wie die Zeit von Ereignissen von jeder Ereignisquelle ermittelt wird. Die Ereigniszeit kann auf dem Zeitstempel der Ereignisquelle (verbürgte Ereigniszeit) oder dem Zeitstempel des Identity Audit-Servers basieren. Der Zeitstempel wirkt sich auf die Reihenfolge aus, in der Ereignisse bei einer Suche angezeigt werden, wenn Sie die Ereignisse nach Zeit sortieren. Der Zeitstempel hat außerdem Auswirkungen auf die Anzeigezeit in Berichten. Standardmäßig wird die Identity Audit-Serverzeit verwendet.

Hinweis: Es wird empfohlen, einen NTP-Server zur ständigen Zeitsynchronisierung auf allen Computern im Identity Audit-System zu verwenden. Falls ein NTP-Server verfügbar ist, empfiehlt Novell, der Ereigniszeit für die Anwendungen zu vertrauen. Steht kein NTP-Server zur Verfügung, empfiehlt Novell, für alle Anwendungen die Identity Audit-Serverzeit zu verwenden (dies ist die Standardeinstellung), um alle Zeitunterschiede zwischen den Computern zu korrigieren.

So ändern Sie die Ereigniszeitoptionen:

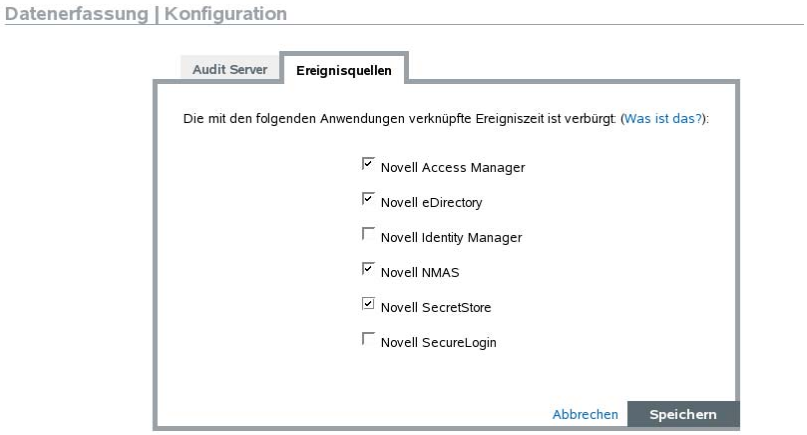
1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie oben am Bildschirm auf den Link *Sammlung*.

3 Klicken Sie rechts am Bildschirm auf den Link *Konfiguration*.

4 Klicken Sie auf *Ereignisquelle*.

5 Wählen Sie alle Anwendungen aus, für die Identity Audit den Ereigniszeitstempel der ursprünglichen Anwendung verwenden soll.



Für alle anderen ersetzt der Zeitstempel des Identity Audit-Servers den Zeitstempel der ursprünglichen Anwendung.

Die Änderungen werden sofort für alle neuen eingehenden Ereignisse wirksam. Möglicherweise dauert es einige Zeit, bis die Ereignisse, die sich bereits in der Warteschlange befinden, verarbeitet werden.

Datenspeicherung

7

Zusammen mit Novell® Identity Audit wird eine PostgreSQL-Datenbank mit allen erforderlichen Tabellen und Benutzern zur Ausführung von Identity Audit installiert. Die Datenbank enthält auch gespeicherte Vorgänge, die zur Verwaltung von Datenbankpartitionen und zur Archivierung alter Daten entwickelt wurden. Administratoren können die Einstellungen zur Datenbankspeicherung und Archivierung über die Weboberfläche verwalten.

7.1 Zustand der Datenbank

Auf der Seite "Zustand der Datenbank", die nur Administratoren zur Verfügung steht, wird der Zustand der Datenbank angezeigt basierend auf der Anzahl an Partitionen, die in der Datenbank verfügbar sind, und darauf, ob die gespeicherten Vorgänge erfolgreich neue Partitionen erstellen und Daten archivieren können (falls konfiguriert).

So zeigen Sie den Zustand der Datenbank an:

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie oben rechts auf der Seite auf den Link "Speicher".

   Die Zustandsseite wird angezeigt.

Auf dieser Seite wird angezeigt, ob verschiedene Datenbankfunktionen fehlerfrei funktionieren (grün), eine Warnmeldung (gelb) oder eine Fehlermeldung (rot) anzeigen.

Online-Datenbank: In dieser Anzeige sehen Sie, ob die erwartete Anzahl an Partitionen für jede der partitionierten Tabellen in der Datenbank vorhanden ist. Die erwartete Anzahl von Partitionen basiert auf der Anzahl an Tagen, die das System laut Konfiguration online ist (oder die Anzahl an Tagen seit der Installation, falls die Installation erst kürzlich erfolgte).

Falls die Anzahl an Partitionen nicht den Erwartungen entspricht, so wird auf der Seite der Name der Tabelle, die Anzahl an erwarteten Partitionen sowie die tatsächliche Anzahl der Partitionen in der Datenbank angezeigt.

Online-Datenbankaufträge: Dieses Kennzeichen ist rot, wenn bei der letzten Ausführung der gespeicherten Vorgänge zum Hinzufügen von Partitionen und zum Löschen von Daten Fehler auftraten. Wurde die Archivierung aktiviert, zeigt dieses Kennzeichen nur an, ob beim letzten

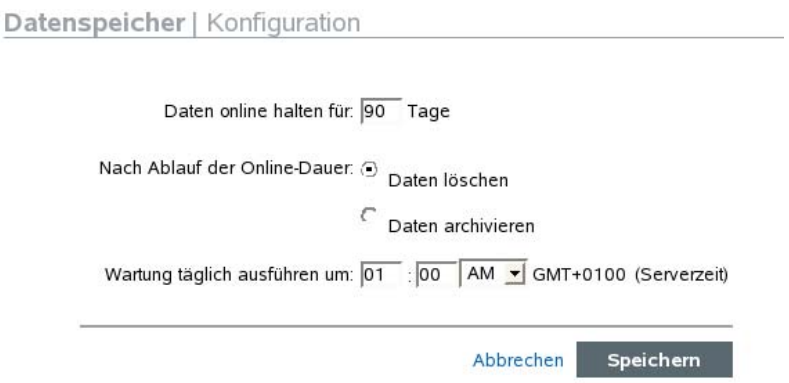
Ausführen des Auftrags zum Hinzufügen von Partitionen Fehler auftraten. Wenn Fehler auftraten, werden auf dieser Seite Name, Zeitstempel und weitere Details für den fehlerhaft ausgeführten Auftrag angezeigt.

Archivdatenbank: Dieses Kennzeichen wird nur angezeigt, wenn die Archivierung aktiviert ist. Es wird rot angezeigt, wenn bei der letzten Ausführung des gespeicherten Vorgangs zum Archivieren von Daten Fehler auftraten. Wenn Fehler auftraten, werden auf dieser Seite Name, Zeitstempel und weitere Details für den fehlerhaft ausgeführten Auftrag angezeigt.

7.2 Konfiguration der Datenspeicherung

Die Datenbank fungiert als Repository für eingehende Ereignisse, Konfigurationsinformationen und Berichtergebnisse. Identity Audit stellt Vorgänge zur Datenbankverwaltung zur Vefügung, die verhindern sollen, dass die Datenbank überfüllt wird. Auf der Seite "Datenspeicherung", auf die nur Administratoren Zugriff haben, können verschiedene Aspekte der Datenspeicherung konfiguriert werden.

Abbildung 7-1 *Konfiguration der Datenspeicherung*



Daten online halten für: Administratoren können den Zeitraum in Tagen angeben, für den die Daten zu Berichtszwecken in der Datenbank gehalten werden sollen. Es muss mindestens ein Tag angegeben werden und die Zahl muss eine Ganzzahl sein (keine Dezimalzahlen).

Nach Ablauf der Online-Dauer: Wenn der Zeitraum zur Online-Datenaufbewahrung abgelaufen ist, werden alle Ereignisdaten, die älter als dieser Zeitraum sind, entweder gelöscht oder aus der Datenbank in ein Archivverzeichnis verschoben.

Warnung: Novell unterstützt die Wiederherstellung gelöschter Daten nicht. Gehen Sie also beim Verwenden der Löschoption extrem vorsichtig vor.

In diesem Datenbankverzeichnis archivieren: Wenn die Option *Daten archivieren* gewählt wurde, geben Sie den Speicherort für ein vorhandenes Verzeichnis an, in den die archivierten Daten geschrieben werden sollen. Dieses Verzeichnis muss bereits vorhanden sein und Novell-Benutzer müssen Schreibzugriff darauf haben. Dieser Speicherort ist standardmäßig mit /data/db_archive im Basisverzeichnis von Identity Audit festgelegt. Das Standardverzeichnis wird mit den entsprechenden Berechtigungen bei der Installation von Identity Audit erstellt.

Wichtig: Novell empfiehlt Ihnen, die Archivdateien von Zeit zu Zeit an einen langfristigen Speicherort zu verschieben, um die Überfüllung der Festplatte zu vermeiden.

Test: Wenn die Option *Daten archivieren* gewählt wird, kann durch Klicken auf die Schaltfläche "Test" überprüft werden, ob das Archivverzeichnis vorhanden ist und der Novell-Benutzer Schreibzugriff darauf hat.

Wartung täglich durchführen um: Geben Sie die Uhrzeit ein, zu der die Wartungsroutinen durchgeführt werden sollen. Die Uhrzeit basiert auf der Ortszeit des Identity Audit-Servers. Zur geplanten Wartungszeit wird ein gespeicherter Vorgang zum Hinzufügen von Partitionen zur Datenbank ausgeführt. Zwei Stunden später wird ein gespeicherter Vorgang zur Archivierung oder Löschung von Daten ausgeführt, die älter als die konfigurierte Anzahl an Tagen sind.

Die Datenarchivierung sollte für einen Zeitpunkt geplant werden, zu dem die Datenbankauslastung relativ gering ist.

Regeln

8

In diesem Kapitel werden die Ereigniskanäle beschrieben, die zum Senden von Ereignissen von Identity Audit an ein anderes System verwendet werden können.

8.1 Regelüberblick

Mit der Regel-Benutzeroberfläche können Sie Regeln zur Bewertung der eingehenden Ereignisse definieren sowie Regeln zur Zustellung der Ereignisse an die festgelegten Ausgabekanäle. Beispiel: Alle Ereignisse mit dem Schweregrad 5 können per Email an einen Verteiler von Sicherheitsanalysten oder an einen Administrator gesendet werden.

Hinweis: Alle Ereignisse werden außerdem der Datenbank zugestellt.

Ein eingehendes Ereignis wird anhand einer Filterregel bewertet, bis eine Übereinstimmung gefunden wurde. Danach werden die zu dieser Regel gehörenden Zustellungsaktionen ausgeführt:

An Email senden: Das Ereignis wird an einen oder mehrere Benutzer gesendet. Dazu wird ein konfigurierter SMTP-Server verwendet.

In Datei schreiben: Das Ereignis wird in eine bestimmte Datei auf dem Identity Audit-Server geschrieben.

An Syslog senden: Das Ereignis wird an einen konfigurierten Syslog-Server weitergeleitet

---

Tipp: Ereignisse werden nacheinander mithilfe der verknüpften Aktionen verarbeitet. Berücksichtigen Sie daher bei der Auswahl der Ausgabekanäle, an die die Ereignisse gesendet werden, die Auswirkung auf die Leistung. Beispiel: Die Aktion "In Datei schreiben" benötigt am wenigsten Ressourcen. Sie können diese Aktion zum Testen von Regelkriterien zur Ermittlung von Datenmengen verwenden, bevor Sie eine große Anzahl von Ereignissen per Email oder an das Syslog senden.

Wenn Sie die Aktion "An Email senden" wählen, berücksichtigen Sie, wie viele Ereignisse der Empfänger bearbeiten kann. Passen Sie die Filteroption der Regel entsprechend an.

Die Ereignisausgabe erfolgt in JavaScript Object Notation (JSON). Dies ist ein leicht lesbares Datenaustauschformat. Ereignisse bestehen aus Feldnamen (z. B. “evt” für Ereignisname), gefolgt von einem Punkt und einem Wert (z. B. “Start”), getrennt durch Kommata.

```
{"st":"I","evt":"Start","sev":"1","sres":"Collector","res":"Collec
torManager","rv99":"0","rv1":"0","repassetid":"0","rv77":"0","agen
t":"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 Konfigurieren von Regeln

Identity Audit-Regeln können zum Filtern von Ereignissen basierend auf mindestens einem der durchsuchbaren Felder konfiguriert werden. Eine Liste der mit Identity Audit durchsuchbaren Ereignisfelder finden Sie unter Tabelle 4-1 auf Seite 31. Jede Regel kann mit einer oder mehreren konfigurierten Aktionen verknüpft werden.

- Abschnitt 8.2.1, „Filterkriterien“, auf Seite 58
- Abschnitt 8.2.2, „Hinzufügen einer Regel“, auf Seite 58
- Abschnitt 8.2.3, „Sortieren von Regeln“, auf Seite 59
- Abschnitt 8.2.4, „Löschen von Regeln“, auf Seite 59
- Abschnitt 8.2.5, „Aktivieren oder Deaktivieren einer Regel“, auf Seite 59

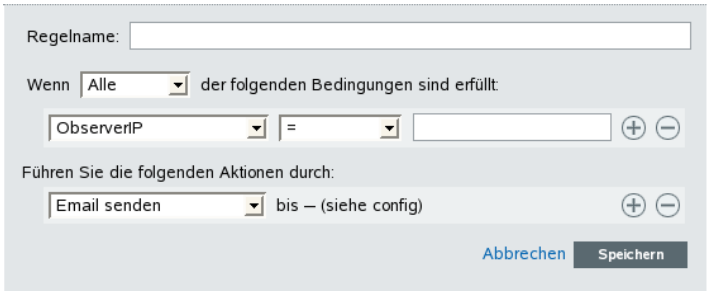
8.2.1 Filterkriterien

Regeln können auf allen suchbaren Ereignisfeldern basieren. Eine Auflistung dieser Felder finden Sie unter Tabelle 4-1 auf Seite 31. Die verfügbaren Operatoren sind abhängig vom Datentyp des Ereignisfelds. Beispiel: `match subnet` ist für IP-Adressen verfügbar, `match regex` ist für Textfelder verfügbar.

8.2.2 Hinzufügen einer Regel

Administratoren können eine filterbasierte Regel hinzufügen und dann einen oder mehrere Kanäle definieren, an die die Ereignisse ausgegeben werden, die den Regelkriterien entsprechen.

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie auf *Regeln* in der oberen rechten Ecke der Seite.
3. Klicken Sie auf *Regel hinzufügen*.
4. Geben Sie einen Regelnamen ein.
5. Wenn Sie mehrere Bedingungen erstellen, wählen Sie *Alle*, um die Bedingungen mit einem AND-Operator zu verknüpfen. Wählen Sie *Beliebige*, um die Bedingungen mit einem OR-Operator zu verknüpfen.
6. Wählen Sie das Ereignisfeld, den Operator und den Wert für den Filter aus.



7 Wählen Sie eine Aktion aus, die für jedes Ereignis, welches den Filterkriterien entspricht, ausgeführt wird.

   Die Details der Aktion basieren auf den Konfigurationsinformationen. Diese können Sie über den Link *Konfiguration* anzeigen.

8 Konfigurieren Sie bei Bedarf weitere Aktionen.

9 Klicken Sie auf *Speichern*.

8.2.3 Sortieren von Regeln

Da Ereignisse der Reihe nach von Regeln bewertet werden, bis eine Übereinstimmung gefunden wurde, empfiehlt Novell, dass Sie die Regeln entsprechend sortieren. Stellen Sie genauer definierte und wichtige Regeln an den Anfang der Liste. Wenn mehrere Regeln vorhanden sind, können Sie über Ziehen-und-Ablegen die Regeln neu sortieren.

So sortieren Sie Regeln neu:

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie auf *Regeln* in der oberen rechten Ecke der Seite.

3 Ziehen Sie den Mauszeiger über das Symbol links neben der Regelnummerierung, um die Ziehen-und-Ablegen-Funktion zu aktivieren. Der Cursor ändert sich.

4 Ziehen Sie die Regel an die gewünschte Stelle in der Sortierungsliste und legen Sie sie dort ab.

8.2.4 Löschen von Regeln

Wenn sich Ereignisse beim Löschen einer Regel bereits in der Warteschlange für eine oder mehrere Aktionen befinden, dauert es möglicherweise einige Zeit, bis diese Warteschlange nach dem Deaktivieren der Regel geleert ist.

8.2.5 Aktivieren oder Deaktivieren einer Regel

Links neben jeder Regel in der Spalte "Ein" befindet sich ein Kontrollkästchen zum Aktivieren der Regel. Neue Regeln werden standardmäßig aktiviert. Wenn Sie eine Regel deaktivieren, werden eingehende Ereignisse nicht länger entsprechend dieser Regel bewertet. Wenn sich Ereignisse bereits in der Warteschlange für eine oder mehrere Aktionen befinden, dauert es möglicherweise einige Zeit, bis diese Warteschlange nach dem Deaktivieren der Regel geleert ist.

8.3 Konfigurieren von Aktionen

Wenn das Ereignis den Kriterien einer der Regeln entspricht, wird es an einen oder mehrere Kanäle zugestellt. Bevor die Ereignisse an einen Kanal ausgegeben werden, muss die Aktion zum Senden des Ereignisses an diesen Kanal mit den entsprechenden Verbindungsinformationen (und Authentifizierungsberechtigungen, falls diese für den SMTP-Server erforderlich sind) konfiguriert werden. Das Identity Audit-System darf nur eine konfigurierte Verbindung pro Aktionstyp besitzen (beispielsweise müssen alle Ereignisse, die in eine Datei geschrieben werden, in dieselbe Datei geschrieben werden).

- Abschnitt 8.3.1, „An Email senden“, auf Seite 60
- Abschnitt 8.3.2, „An Syslog senden“, auf Seite 61
- Abschnitt 8.3.3, „In Datei schreiben“, auf Seite 61

8.3.1 An Email senden

Zum Konfigurieren der Aktion "An Email senden" sind die Verbindungsinformationen für einen SMTP-Server (IP-Adresse und Portnummer) erforderlich sowie die Adressen unter "An" und "Von". Sie können Nachrichten mithilfe einer kommagetrennten Liste an mehrere Email-Adressen senden.

Hinweis: Um den SMTP-Server oder die Email-Empfänger nicht zu überlasten, verwenden Sie diese Aktion nur mit Regeln, die eine geringe Anzahl von Ereignissen generieren.

Diese SMTP-Serverkonfiguration wird auch zum Zustellen von Berichten an Benutzer verwendet.

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie auf *Regeln* in der oberen rechten Ecke der Seite.
3. Klicken Sie auf *Konfiguration*.
4. Geben Sie unter *Email* den Namen und Port eines verfügbaren SMTP-Servers ein. Klicken Sie auf *Test*, um die Verbindung zu testen.

5. Falls für den SMTP-Server eine Authentifizierung erforderlich ist, geben Sie einen Benutzernamen und ein Passwort ein.
6. Geben Sie eine Adresse ein, von der die Email-Nachrichten versendet werden.

7 Geben Sie mindestens eine Email-Adresse ein. Trennen Sie bei mehreren Email-Adressen die Adressen durch Kommata.

8 Klicken Sie auf *Speichern*.

Alle Identity Audit-Ereignisse, die den Filterkriterien entsprechen und für die eine Aktion "An Email senden" definiert wurde, werden an denselben SMTP-Server und denselben Adressensatz gesendet.

8.3.2 An Syslog senden

Um die Aktion "An Syslog senden" zu konfigurieren, benötigen Sie die Verbindungsinformationen für den Syslog-Server (IP-Adresse und Portnummer).

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie auf *Regeln* in der oberen rechten Ecke der Seite.

3 Klicken Sie auf *Konfiguration*.

4 Geben Sie unter *Syslog* einen Namen oder eine IP-Adresse ein und öffnen Sie den Port eines Syslog-Servers. Klicken Sie bei Bedarf auf *Test*, um zu testen, ob der Zielserver und der Zielport vorhanden sind.

5 Klicken Sie auf *Speichern*.

Alle Identity Audit-Ereignisse, die den Filterkriterien entsprechen und für die eine Aktion "An Syslog senden" definiert wurde, werden an denselben Syslog-Server gesendet.

8.3.3 In Datei schreiben

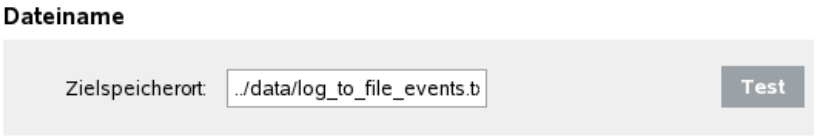
Zum Konfigurieren der Aktion "In Datei schreiben" ist der Name und der Pfad der Datei erforderlich, in die die Ereignisse geschrieben werden sollen. Dieses Verzeichnis muss bereits vorhanden sein und der Novell-Benutzer muss Schreibzugriff darauf haben. Falls die Datei noch nicht vorhanden ist, wird sie von Identity Audit erstellt.

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie auf *Regeln* in der oberen rechten Ecke der Seite.

3 Klicken Sie auf *Konfiguration*.

4 Geben Sie unter *Dateiname* den Pfad zu der Datei an, in die die Ereignisse geschrieben werden sollen. Klicken Sie auf *Test*, um die Verbindung zu testen.



5 Klicken Sie auf *Speichern*.

Alle Identity Audit-Ereignisse, die den Filterkriterien entsprechen und für die die Aktion "In Datei schreiben" definiert wurde, werden in dieselbe Datei geschrieben.

Benutzerverwaltung

9

Administratoren können Benutzer in Novell® Identity Audit hinzufügen, bearbeiten und löschen und ihnen Administratorrechte erteilen. Benutzer können die Details ihrer Benutzerprofile selbst bearbeiten.

9.1 Hinzufügen eines Benutzers

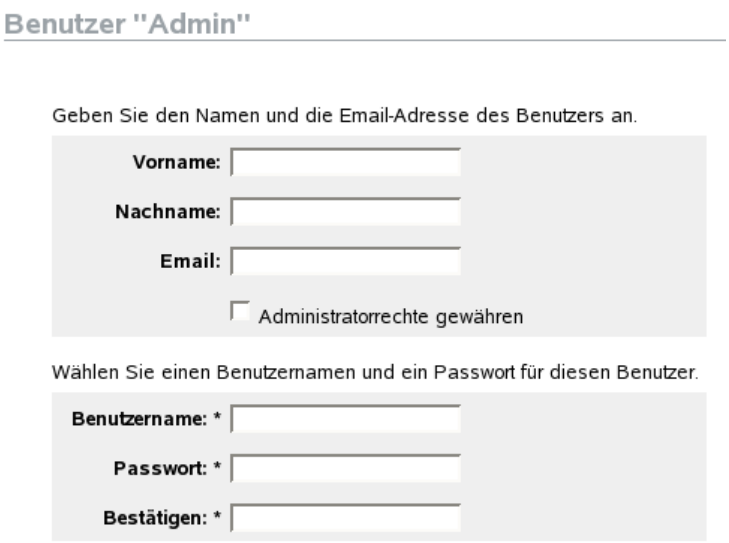
Durch Hinzufügen eines Benutzers im Identity Audit-System wird ein Benutzer erstellt, der sich anschließend bei der Identity Audit-Anwendung anmelden kann.

Durch Auswahl der Option *Administratorrechte gewähren* erhält der Benutzer Administratorrechte im Identity Audit-System. Zu den Verwaltungsrechten gehören die Verwaltung der folgenden Funktionen:

- Benutzerverwaltung
- Datensammlung
- Datenspeicherung

So fügen Sie einen Benutzer hinzu:

1. Melden Sie sich bei Identity Audit als Administrator an.
2. Klicken Sie auf *Benutzerverwaltung* in der oberen rechten Ecke der Seite.
3. Klicken Sie auf *Einen Benutzer hinzufügen*.
4. Geben Sie die Benutzerinformationen ein.



Sie müssen alle Felder mit einem Sternchen (*) ausfüllen. Der Benutzername muss eindeutig sein.

Hinweis: Das Format der Email-Adresse wird überprüft, die Telefonnummernfelder akzeptieren ein beliebiges Format. Achten Sie darauf, eine gültige Telefonnummer einzugeben.

5 Wählen Sie bei Bedarf *Administratorrechte gewähren*.

6 Klicken Sie auf *Speichern*.

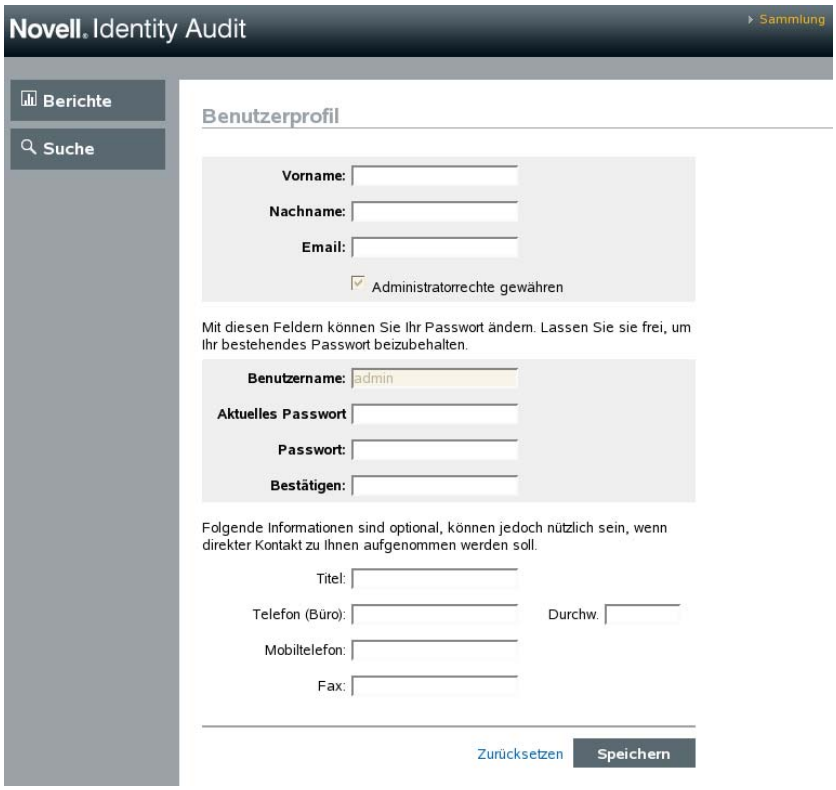
9.2 Bearbeiten von Benutzerdetails

Administratoren können die Benutzerinformationen für alle Benutzer im System bearbeiten. Alle Benutzer können alle Felder in ihrem eigenen Profil bearbeiten. Ausgenommen sind Benutzername und Administratorstatus. Benutzer können auch ihr Passwort ändern.

- Abschnitt 9.2.1, „Bearbeiten des eigenen Profils“, auf Seite 64
- Abschnitt 9.2.2, „Ändern des eigenen Passworts“, auf Seite 65
- Abschnitt 9.2.3, „Bearbeiten des Profils eines anderen Benutzers (nur Admin)“, auf Seite 65
- Abschnitt 9.2.4, „Zurücksetzen des Passworts eines anderen Benutzers (nur Admin)“, auf Seite 65

9.2.1 Bearbeiten des eigenen Profils

1 Klicken Sie auf *Profil* in der rechten oberen Ecke.



2 Bearbeiten Sie die verfügbaren Felder beliebig.

3 Klicken Sie auf *Speichern*.

9.2.2 Ändern des eigenen Passworts

Benutzer können ihr eigenes Passwort ändern, wenn ihnen das aktuelle Passwort bekannt ist. Anderenfalls muss ein Administrator das Passwort zurücksetzen.

1 Klicken Sie auf *Profil* in der rechten oberen Ecke.

2 Geben Sie Ihr aktuelles Passwort ein.

3 Geben Sie das neue Passwort ein.

4 Bestätigen Sie das neue Passwort.

5 Klicken Sie auf *Speichern*.

9.2.3 Bearbeiten des Profils eines anderen Benutzers (nur Admin)

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie auf *Benutzerverwaltung* in der oberen rechten Ecke der Seite.

3 Klicken Sie unter dem zu bearbeitenden Benutzer auf *Bearbeiten*.

4 Bearbeiten Sie die Felder wie gewünscht (mit Ausnahme des Benutzernamens).

5 Klicken Sie auf *Speichern*.

   Änderungen mit der Funktion *Administratorrechte gewähren* werden bei der nächsten Anmeldung des Benutzers wirksam.

9.2.4 Zurücksetzen des Passworts eines anderen Benutzers (nur Admin)

Weitere Informationen zum Zurücksetzen des Passworts eines anderen Benutzers finden Sie unter Abschnitt 9.2.3, „Bearbeiten des Profils eines anderen Benutzers (nur Admin)“, auf Seite 65.

9.3 Löschen von Benutzern

Administatoren können einen Benutzer im System löschen.

1 Melden Sie sich bei Identity Audit als Administrator an.

2 Klicken Sie auf *Benutzerverwaltung* in der oberen rechten Ecke der Seite.

3 Klicken Sie unter dem zu löschenden Benutzer auf *Bearbeiten*.

4 Klicken Sie auf *Diesen Benutzer löschen* in der oberen rechten Ecke der Seite.

5 Klicken Sie zur Bestätigung auf *Löschen*.

Truststore

A

Eine Verbesserung der Datensicherheit ist möglich, wenn Sie für die Verbindung zwischen Identity Audit und den Novell-Anwendungen, aus denen Identity Audit Daten sammelt, die strenge Authentifizierung verwenden.

A.1 Erstellen eines Keystore

Sie können mithilfe der ausführbaren Datei "keytool" von Java einen Keystore erstellen. Diese Datei ist Teil aller jre-Installationen. Dieser Keystore enthält ein öffentliches und ein privates Schlüsselpaar, mit dem Sie die in Identity Audit enthaltenen Standardzertifikate ersetzen können. Im Folgenden werden einige grundlegende Anweisungen beschrieben. Ausführliche Informationen zum Keytool finden Sie auf der Sun-Website (http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html).

1. Navigieren Sie in das /bin-Verzeichnis für Java (Beispiel: `$JAVA_HOME/bin`).
2. Führen Sie den folgenden Befehl aus:

   ```
   keytool -genkey -alias alias -keystore .keystore
   ```

3. Geben Sie ein Passwort für den Keystore ein. Dieses Passwort wird beim Import des Truststore verwendet.
4. Geben Sie die folgenden Informationen ein: Vor- und Nachname.
   - Vor- und Nachname
   - Organisatorische Einheit
   - Organisation
   - Stadt oder Standort
   - Bundesland/-staat
   - Zweistelliger Ländercode
5. Überprüfen Sie die Informationen.
6. Drücken Sie die Eingabetaste, um dasselbe Passwort wie das Keystore-Passwort zu verwenden.

   Es wird eine .keystore-Datei mit einem privaten Schlüssel und dem entsprechenden öffentlichen Schlüssel (Zertifikat) erstellt.