

ユーザガイド
October 31, 2008

Novell® Identity Audit

1.0

www.novell.com



保証と著作権

米国 Novell, Inc., およびノベル株式会社は、本書の内容または本書を使用した結果について、いかなる保証、表明または約束も行っておりません。また、本書の商品性、および特定の目的への適合性について、いかなる黙示の保証も否認し、排除します。また、本書の内容は予告なく変更されることがあります。

米国 Novell, Inc. およびノベル株式会社は、すべてのノベル製ソフトウェアについて、いかなる保証、表明または約束も行っておりません。またノベル製ソフトウェアの商品性、および特定の目的への適合性について、いかなる黙示の保証も否認し、排除します。米国 Novell, Inc., およびノベル株式会社は、ノベル製ソフトウェアの内容を変更する権利を常に留保します。

本契約の下で提供される製品または技術情報はすべて、米国の輸出規制および他国の商法の制限を受けます。お客様は、すべての輸出規制を遵守して、製品の輸出、再輸出、または輸入に必要なすべての許可または等級を取得するものとします。お客様は、現在の米国の輸出除外リストに掲載されている企業、および米国の輸出管理規定で指定された輸出禁止国またはテロリスト国に本製品を輸出または再輸出しないものとします。お客様は、取引対象製品を、禁止されている核兵器、ミサイル、または生物化学兵器を最終目的として使用しないものとします。ノベル製ソフトウェアの輸出については、「[Novell International Trade Services \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/)」の Web ページをご参照ください。弊社は、お客様が必要な輸出承認を取得しなかったことに対し如何なる責任も負わないものとします。

Copyright © 2008 Novell, Inc. All rights reserved. 本ドキュメントの一部または全体を無断で複写・転載することは、その形態を問わず禁じます。

米国 Novell, Inc., およびノベル株式会社は、本書に記載されている製品内で実地されている技術に関連する知的所有権を有しています。これらの知的所有権は、「[Novell Legal Patents \(http://www.novell.com/company/legal/patents/\)](http://www.novell.com/company/legal/patents/)」の Web ページに記載されている 1 つ以上の米国特許、および米国ならびにその他の国における 1 つ以上の特許または出願中の特許を含む場合があります。

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

オンラインマニュアル: 本製品とその他の Novell 製品の最新のオンラインマニュアルにアクセスするには、[Novell のマニュアルの Web ページ \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) を参照してください。

Novell の商標

Novell の商標一覧については、「[商標とサービスの一覧 \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html)」を参照してください。

サードパーティ資料

サードパーティの商標は、それぞれの所有者に帰属します。

目次

このガイドについて	7
1 序文	9
1.1 製品の概要	9
1.1.1 Novell Audit 2.0.2 との比較	9
1.1.2 Novell Sentinel との比較	9
1.2 インタフェース	10
1.3 アーキテクチャ	11
2 システム要件	13
2.1 ハードウェア要件	13
2.2 対応オペレーティングシステム	14
2.3 対応ブラウザ	14
2.4 対応プラットフォームエージェント	14
2.5 対応イベントソース	15
3 インストール	17
3.1 Novell Identity Audit のインストール	17
3.1.1 クイックインストール (root として実行)	17
3.1.2 ルート以外のインストール	19
3.2 イベントソースの設定	21
3.2.1 プラットフォームエージェントのインストール	21
3.2.2 プラットフォームエージェントの設定	22
3.2.3 監査レベルの設定	22
3.3 はじめに	23
3.4 アンインストール	23
4 検索	25
4.1 イベント検索の概要	25
4.2 イベント検索の実行	26
4.2.1 基本検索	26
4.2.2 高度な検索	27
4.3 検索結果の表示	28
4.3.1 基本イベントビュー	28
4.3.2 詳細イベントビュー	29
4.3.3 検索結果の絞り込み	29
4.4 イベントフィールド	30
5 レポート機能	35
5.1 概要	35
5.2 レポートの実行	35
5.3 レポートの表示	37
5.4 レポートの管理	39
5.4.1 レポートの追加	39

5.4.2	レポート結果の名前の変更	41
5.4.3	レポートの削除	41
5.4.4	レポート定義の更新	41
6	データコレクション	43
6.1	イベントソースの設定	43
6.2	データコレクションステータス	43
6.2.1	監査サーバ	44
6.2.2	イベントソース	44
6.3	監査サーバのオプション	45
6.3.1	ポートの設定とポート転送	46
6.3.2	クライアント認証	47
6.4	イベントソース	50
7	データストレージ	53
7.1	データベースヘルス	53
7.2	データストレージの設定	54
8	ルール	57
8.1	ルールの概要	57
8.2	ルールの設定	58
8.2.1	フィルタ条件	58
8.2.2	ルールの追加	58
8.2.3	ルールの配列	59
8.2.4	ルールの削除	59
8.2.5	ルールの有効化または無効化	59
8.3	アクションの設定	59
8.3.1	電子メールに送信	60
8.3.2	Syslog に送信	60
8.3.3	ファイルに書き出し	61
9	ユーザ管理	63
9.1	ユーザの追加	63
9.2	ユーザの詳細の編集	64
9.2.1	自分のプロフィールを編集する	64
9.2.2	自分のパスワードを変更する	64
9.2.3	別のユーザのプロフィールを編集する (管理者のみ)	65
9.2.4	別のユーザのパスワードをリセットする (管理者のみ)	65
9.3	ユーザの削除	65
A	Truststore	67
A.1	キーストアの作成	67

このガイドについて

このガイドでは、Novell® Identity Audit のインストールと環境設定について説明します。

- ◆ 9 ページの第 1 章「序文」
- ◆ 13 ページの第 2 章「システム要件」
- ◆ 17 ページの第 3 章「インストール」
- ◆ 25 ページの第 4 章「検索」
- ◆ 35 ページの第 5 章「レポート機能」
- ◆ 43 ページの第 6 章「データコレクション」
- ◆ 53 ページの第 7 章「データストレージ」
- ◆ 57 ページの第 8 章「ルール」
- ◆ 63 ページの第 9 章「ユーザ管理」
- ◆ 67 ページの付録 A「Truststore」

対象読者

このガイドは、Novell Identity Audit の管理者を対象にしたドキュメントです。

フィードバック

本マニュアルおよびこの製品に含まれているその他のマニュアルについて、皆様のご意見やご要望をお寄せください。オンラインマニュアルの各ページの下部にあるユーザコメント機能を使用するか www.novell.com/documentation/feedback.html にアクセスしてコメントを記入してください。

マニュアルの更新

Novell Identity Audit 1.0 の最新バージョンのガイドについては、[Identity Audit マニュアルの Web サイト \(http://www.novell.com/documentation/identityaudit\)](http://www.novell.com/documentation/identityaudit) を参照してください。

マニュアルの表記規則

Novell のマニュアルでは、「より大きい」記号 (>) を使用して手順内の操作と相互参照パス内の項目の順序を示します。

商標記号 (®、™ など) は、Novell の商標を示します。アスタリスク (*) は、サードパーティの商標を示します。

Novell® Identity Audit は、Novell eDirectory™、Novell Identity Manager、Novell Access Manager、Novell Modular Authentication Services (NMAS™)、Novell SecureLogin、Novell SecretStore® など、Novell アイデンティティおよびセキュリティ管理環境に対応したイベントのレポート機能や監視機能を提供します。

- ◆ 9 ページのセクション 1.1 「製品の概要」
- ◆ 10 ページのセクション 1.2 「インタフェース」
- ◆ 11 ページのセクション 1.3 「アーキテクチャ」

1.1 製品の概要

Novell Identity Audit 1.0 は、Novell Identity Manager、Novell Access Manager、Novell eDirectory などの Novell アイデンティティおよびセキュリティ製品やテクノロジーから、イベントを収集、集計、格納できる便利な軽量ツールです。主な機能は次のとおりです。

- ◆ Web ベースの管理およびレポート機能のインタフェース
- ◆ イベントの全般的な検索ツールにより、複数のイベントフィールドを対象にした検索が可能
- ◆ 選択したイベントを複数のチャンネルに出力
- ◆ 組み込みの Jasper Reports エンジンにより、オープンソースのツールを使用して、付属レポートのカスタマイズやレポートの新規作成が可能
- ◆ ビルトインデータベースにより、外部データベースのライセンスや管理が不要
- ◆ シンプルで直感的なデータ管理ツール

1.1.1 Novell Audit 2.0.2 との比較

Novell Identity Audit 1.0 は、2009 年 2 月に一般サポートを終了する Novell Audit 製品群の代替製品として開発されました。Identity Audit は機能的には同等の製品ですが、アーキテクチャ、レポート機能、データ管理の面で大幅に改善されています。Novell Identity Audit 1.0 は、Novell アイデンティティおよびセキュリティ製品群向けの Novell Audit 2.0.2 セキュアログサーバと簡単に置き換えることができます。Novell Identity Audit は新たに組み込まれたデータベースを使用するため、Novell Audit の既存のイベントはアーカイブの Novell Audit データベースに保持できます。従来のデータを移行する必要はありません。

プラットフォームエージェントの役割も果たす Novell Audit クライアントコンポーネントは、Novell Identity Audit でもデータ伝送メカニズムとして使用されます。このコンポーネントに対するサポートは、引き続きそのプラットフォームエージェントを使用する Novell Identity および Access Management 製品のライフサイクルに合わせて継続されます。

1.1.2 Novell Sentinel との比較

Novell Identity Audit は堅牢な技術的基盤のもとで構築されており、その基本となるコードの多くは Novell Sentinel と共有されています。ただし、Sentinelの方がより広範囲のデバイスからデータを収集でき、高いイベント率にも対応し、ツールも充実しています。また

Sentinel は、SIEM (Security Information and Event Management) 機能も充実しており、リアルタイムダッシュボードやマルチイベントの関連付け、インシデントの追跡、自動修正、Novell 以外の製品からのデータ収集などが可能です。Identity Audit は、将来の Sentinel 環境への統合を踏まえて設計されています。

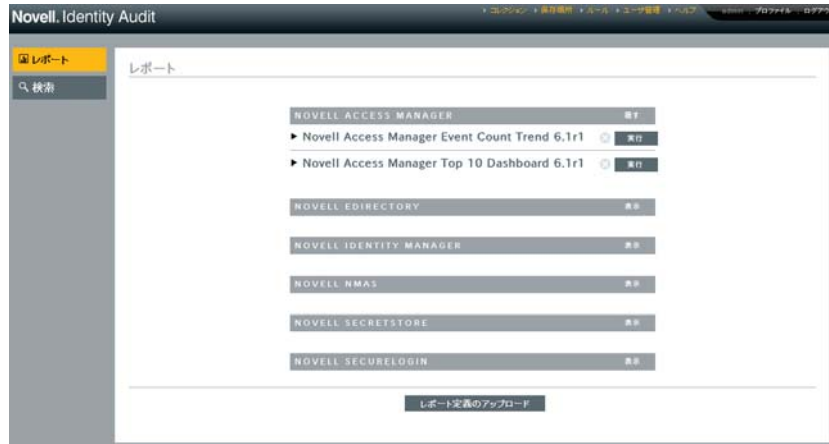
Novell Identity Audit 1.0 は Novell CMP (Compliance Management Platform) の一部ではなく、そのプラットフォームで提供される高度なアイデンティティおよびセキュリティ統合機能は備えていません。Sentinel 6.1 は現在のところ、CMP のアイデンティティ監査および監視コンポーネントです。

1.2 インタフェース

Novell Identity Audit の Web インタフェースでは、次のタスクを実行できます。

- ◆ レポートのアップロード、実行、表示、削除
- ◆ イベントの検索
- ◆ ユーザプロファイルの詳細の編集
- ◆ ユーザの作成、編集、削除、および管理権の割り当て (管理者のみ)
- ◆ データコレクションの設定、およびイベントソースのヘルスの表示 (管理者のみ)
- ◆ データストレージの設定、およびデータベースのヘルスの表示 (管理者のみ)
- ◆ 一致するイベントデータを出力チャンネルに送信するためのフィルタリングルールの作成および関連するアクションの設定 (管理者のみ)

図 1-1 Novell Identity Audit インタフェース (管理者ビュー)



このインタフェースは 30 秒ごとに自動的に更新され、他のユーザが更新処理を行った場合にその更新内容が表示されます。

このインタフェースは複数言語 (英語、フランス語、ドイツ語、イタリア語、日本語、ポルトガル語、スペイン語、簡体字中国語、繁体字中国語) に対応しています。デフォルトではブラウザのデフォルト言語が使用されますが、ログイン時に別の言語を選択することもできます。

注: このインタフェースは 2 バイト文字に対応するようにローカライズされていますが、Identity Audit の現行版では 2 バイトのイベントデータは処理されません。

1.3 アーキテクチャ

Identity Audit では、複数の Novell アイデンティティおよびセキュリティアプリケーションからデータを収集することができます。これらのアプリケーションサーバは、イベントレコードを生成するように設定されており、それぞれ Novell Audit アプリケーションに含まれるプラットフォームエージェントをホストしています。イベントデータは、プラットフォームエージェントによって、Identity Audit サーバに常駐する監査コネクタに転送されます。

監査コネクタがデータコレクションコンポーネントにイベントを渡し、そこで解析されたイベントが通信バスに置かれます。通信バスはシステムのバックボーンであり、コンポーネント間のすべての通信の橋渡しを行います。データコレクションの一環として、受信イベントは一連のフィルタリングルールによって評価されます。これらのルールによってイベントにフィルタが適用され、ファイルや syslog リレーなどの出力チャンネルにイベントが送信されます。

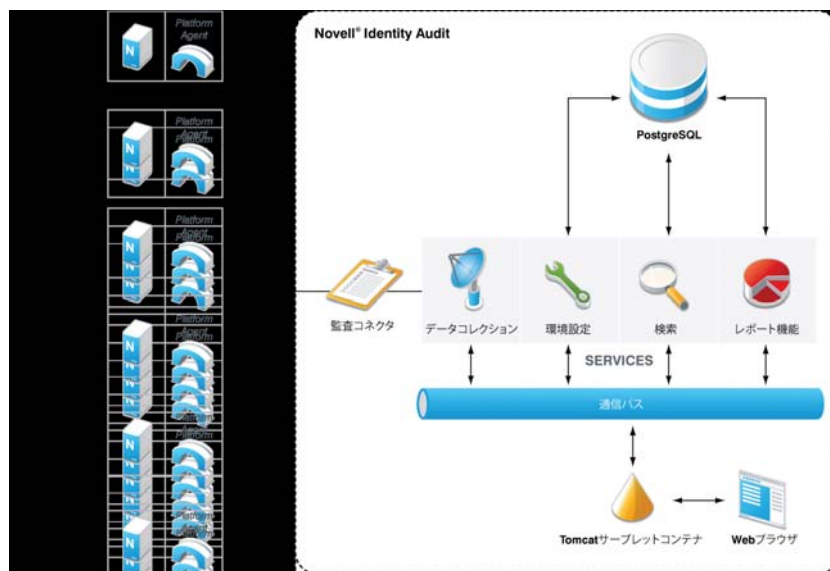
さらに、イベントはすべて Identity Audit データベース (PostgreSQL* を搭載) のパーティションテーブルに格納されます。

設定コンポーネントは、データコレクションとストレージ設定、ルール定義、レポート定義などの設定情報の取得、追加、および変更を行います。また、ユーザ認証も管理します。

検索コンポーネントはインデックスを使用した高速検索を実行し、データベースからイベントを取得して検索結果のセットを表示します。

レポートコンポーネントはレポートを実行し、レポート結果をフォーマットします。

図 1-2 Identity Audit のアーキテクチャ



ユーザは、Apache Tomcat Web サーバに接続した Web ブラウザを介して、Identity Audit サーバとそのすべての機能と対話します。Web サーバは、通信バスを介して、Identity Audit のさまざまなコンポーネントを呼び出します。

システム要件

インストールの際は、次のハードウェア、オペレーティングシステム、ブラウザ、およびイベントソースの互換性の要件に加えて、Identity Audit の実行中のプロセスを所有する novell ユーザと novell グループを作成するために、オペレーティングシステムへのルートアクセスが必要です。

- ◆ 13 ページのセクション 2.1 「ハードウェア要件」
- ◆ 14 ページのセクション 2.2 「対応オペレーティングシステム」
- ◆ 14 ページのセクション 2.3 「対応ブラウザ」
- ◆ 14 ページのセクション 2.4 「対応プラットフォームエージェント」
- ◆ 15 ページのセクション 2.5 「対応イベントソース」

2.1 ハードウェア要件

Novell Identity Audit™ は、64 ビット Intel Xeon* および AMD Opteron* ハードウェアに対応しています。Itanium には対応していません。90 日分のオンラインデータを保存する運用システムでは、次のハードウェアの使用をお勧めします。

- ◆ 1x Quad Core (x86-64)
- ◆ 16GB RAM
- ◆ 1.5TB の使用可能ディスク領域 - 3x 500GB (3 台使用可能)、10K RPM ドライブ (ハードウェア RAID 構成)
 - ◆ 使用可能ディスク領域の約 2/3 をデータベースファイルに使用
 - ◆ 使用可能ディスク領域の約 1/3 を検索インデックスと一時ファイルに使用
 - ◆ データベースから削除されたアーカイブデータ用にストレージの一部を使用することもできますが、アーカイブデータファイルは別のメディアに移動することをお勧めします。

表 2-1 パフォーマンス

メトリック	値	説明
1 秒当たりのイベント数 (eps) - 平常時	100	通常動作中の平均イベント率
1 秒当たりのイベント数 (eps) - ピーク時	500	急増時のピークイベント率 (最大 10 分)

メトリック	値	説明
1秒当たりのイベント数 (eps) - アプリケーション別のピーク時	300	Novell アプリケーション各種のピークイベント率 <ul style="list-style-type: none"> ◆ Identity Manager、SecureLogin、SecretStore®、NMASTM の場合、イベント率は一般的に低くなります (15 eps 未満)。 ◆ eDirectoryTM と Access Manager では、イベント率が非常に高くなる場合があります。イベント率を管理可能なレベルに維持するには、イベントフィルタリングを実装する必要があります。 ◆ イベントが急増しているときであっても、1つのアプリケーションで1秒当たりに送信可能なイベント数が、この値を超えることはありません。
オンラインデータ	90日または 7億5000万 イベント	推奨ストレージを使用して、約100 epsの平常時に Identity Audit が格納できるデータ量

2.2 対応オペレーティングシステム

Identity Audit は、64 ビット SuSE Linux Enterprise Server™ 10 SP1 および SP2 で動作することが保証されています。

2.3 対応ブラウザ

Identity Audit は次のブラウザに対応しています。その他のブラウザでは、情報が正しく表示されないことがあります。

表 2-2 Novell Identity Audit の対応 Web ブラウザ

Web ブラウザおよびバージョン

Mozilla Firefox 2

Mozilla Firefox 3

Microsoft Internet Explorer 7

検索とレポート表示のパフォーマンスは、ブラウザによって異なる場合があります。Mozilla Firefox 3 で特にパフォーマンスが優れていることが確認されています。

2.4 対応プラットフォームエージェント

Identity Audit 1.0 では、Novell Audit とそのプラットフォームエージェントが対応していた多数のアプリケーションから、ログイベントを収集できます。32 ビットのイベントソースの場合、Identity Audit ではプラットフォームエージェントのバージョン 2.0.2 FP6 (2.0.2.55) 以降が必要です。64 ビットのイベントソースの場合、プラットフォームエージェントのバージョン 2.0.2 FP6 が必要です。

注:一部の Novell アプリケーションは、以前のバージョンのプラットフォームエージェントにバンドルされています。プラットフォームエージェントについては、重要なバグ修正が施されている推奨バージョンへのアップグレードをお勧めします。

2.5 対応イベントソース

Identity Audit では、Novell アイデンティティおよびセキュリティアプリケーションからデータを収集することができます。一部のアプリケーションでは、データを正しく収集するために特定のパッチレベルが必要になります。

表 2-3 Novell Identity Audit によってサポートされているアプリケーション

アプリケーション

Novell Access Manager 3.0

Novell サポート Web サイト (http://download.novell.com/Download?buildid=RH_B5b3M6EQ~) にある eDirectory インストラメンテーションパッチを適用した Novell eDirectory 8.8.3

Novell Identity Manager 3.6

Novell NMAS 3.1

Novell SecretStore 3.4

Novell SecureLogin 6.0

この章では、Novell Identity Audit のインストール方法と、Identity Audit にデータを送信するためのイベントソースの設定方法について説明します。これらの手順は、各システムコンポーネントの最小要件が満たされていることを前提としています。詳細については、[13 ページの第 2 章「システム要件」](#)を参照してください。

- [17 ページのセクション 3.1 「Novell Identity Audit のインストール」](#)
- [21 ページのセクション 3.2 「イベントソースの設定」](#)
- [23 ページのセクション 3.3 「はじめに」](#)
- [23 ページのセクション 3.4 「アンインストール」](#)

3.1 Novell Identity Audit のインストール

Identity Audit のインストールパッケージでは、Identity Audit の実行に必要な環境 (Identity Audit アプリケーションとメッセージバス、イベントや環境設定の情報を格納するためのデータベース、Web ベースのユーザインタフェース、およびレポートサーバ) がすべてインストールされます。インストールには、ルートとして実行できるシンプルインストールと、ルートをなるべく使用しないマルチステップインストールという 2 つのオプションがあります。

3.1.1 クイックインストール (root として実行)

このシンプルインストールはルートとして実行する必要があります。

- 1 Identity Audit をインストールするサーバに root としてログインします。
- 2 `identity_audit_1.0_x86-64.tar.gz` を一時ディレクトリにダウンロードするかコピーします。
- 3 次のコマンドを使用して、そのファイルからインストールスクリプトを展開します。

```
tar xfz identity_audit_1.0_x86-64.tar.gz identity_audit_1.0_x86-64/setup/root_install_all.sh
```
- 4 次のコマンドを使用して、`root_install_all.sh` スクリプトを実行します。

```
identity_audit_1.0_x86-64/setup/root_install_all.sh  
identity_audit_1.0_x86-64.tar.gz
```
- 5 番号を入力して言語を選択します。
エンドユーザ使用許諾契約が、選択した言語で表示されます。
- 6 エンドユーザ使用許諾契約を読み、条件に同意する場合は「1」または「y」と入力してインストールを続行します。

インストールが開始されます。選択した言語にインストーラが対応していない場合 (ポーランド語など)、インストーラは英語で続行されます。

```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
Creating group novell ...
Creating user novell ...
Creating installation directory /opt/novell ...
Extracting files...
ソフトウェアのインストールを開始しています...

novell の環境を更新しています...
/opt/novell/identity_audit_1.0_x86-64/binをパスに追加しています...

Webサーバ証明書を生成しています...

JMSプロローカ証明書を生成しています...

JMSプロローカ証明書を生成しています...

「dbauser」に設定するパスワードを指定してください。 =>

```

novell ユーザと novell グループがまだ作成されていない場合は、その両方が作成されます。

- 7 データベース管理者 (dbauser) のパスワードを入力します。
- 8 確認のため、データベース管理者 (dbauser) のパスワードをもう一度入力します。
- 9 管理者ユーザのパスワードを入力します。
- 10 確認のため、管理者ユーザのパスワードをもう一度入力します。

```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
「dbauser」に設定するパスワードを指定してください。 =>
パスワードの確認 =>
「admin」に設定するパスワードを指定してください。 =>
パスワードの確認 =>
データベースおよび環境設定ファイルに新しいパスワードを設定しています...
初期パーティションをデータベースに追加しています...

Starting Identity Audit...

このソフトウェアの使用を開始するには、Webブラウザでhttps://linux-yyae.testoff.moravia-it.com:8443/novellidentityauditに移動します。
ユーザ名:: admin
パスワード: <上で入力したパスワードを使用してください>
サーバの起動中は、このURLにアクセスするまでに時間がかかる場合があります。
サービスがリッスンしているかどうかを確認するには、次のコマンドを使用します。
netstat -an | grep 'LISTEN' | grep 8443

完了しました。
Identity Auditサービスのインストールを開始しています...

以前のインストール設定をクリーンアップしています(存在する場合)...

起動スクリプトを /etc/init.d にインストールしています...

ブート時の自動起動を設定しています...
identity_audit      0:off 1:off 2:off 3:on  4:off 5:on  6:off

完了しました。

```

dbauser の資格情報を使用して、PostgreSQL データベースにテーブルとパーティションが作成されます。Identity Audit は、ランタイムレベル 3 および 5 (コンソールで起動するマルチユーザモードまたは X-Windows モード) で起動するように設定されます。

Identity Audit サービスが開始したら、インストールの出力で指定された URL にログインできます (<https://hostIP:8443/novellidentityaudit>)。システムは内部監査イベントの処理を直ちに開始し、Identity Audit にデータを送信するためのイベントソースを管理者が設定すると、Identity Audit が完全に機能するようになります。

3.1.2 ルート以外のインストール

お客様の組織のポリシーによって、root としてフルインストールプロセスを実行することが禁止されている場合は、インストールを2段階で実行することができます。インストール手順の最初の段階は、ルートレベルのアクセスで実行する必要があり、次の段階は、Identity Audit の管理者ユーザ (最初の段階で作成されるユーザ) として実行されます。

- 1 Identity Audit をインストールするサーバに root としてログインします。
- 2 `identity_audit_1.0_x86-64.tar.gz` を `/tmp` ディレクトリにダウンロードするかコピーします。
- 3 `novell` ユーザと `novell` グループがサーバにまだ作成されていない場合：
 1. Identity Audit の tar ファイルからスクリプトを展開して、`novell` ユーザと `novell` グループを作成します。例を次に示します。

```
tar xfz identity_audit_1.0_x86-64.tar.gz
identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
```
 2. 次のコマンドを使用して、root としてスクリプトを実行します。

```
identity_audit_1.0_x86-64/setup/root_create_novell_user.sh
```

`novell` ユーザと `novell` グループは、Identity Audit のインストールプロセスと実行プロセスを所有します。
- 4 Identity Audit 用のディレクトリを作成します。例を次に示します。

```
mkdir -p /opt/novell
```
- 5 `novell` ユーザと `novell` グループが所有するためのディレクトリを設定します。例を次に示します。

```
chown -R novell:novell /opt/novell
```
- 6 `novell` ユーザとしてログインします。

```
su novell
```
- 7 Identity Audit の tar ファイルを、先ほど作成したディレクトリに展開します。例を次に示します。

```
cd /opt/novell
tar xfz /tmp/identity_audit_1.0_x86-64.tar.gz
```
- 8 インストールスクリプトを実行します。例を次に示します。

```
/opt/novell/identity_audit_1.0_x86-64/setup/install.sh
```
- 9 番号を入力して言語を選択します。
エンドユーザ使用許諾契約が、選択した言語で表示されます。
- 10 エンドユーザ使用許諾契約を読み、条件に同意する場合は「1」または「y」と入力してインストールを続行します。
インストールが開始されます。選択した言語にインストーラが対応していない場合 (ポーランド語など)、インストーラは英語で続行されます。

```
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(T) ヘルプ(H)
ソフトウェアのインストールを開始しています...

novell の環境を更新しています...
/opt/novell/identity_audit_1.0_x86-64/binをパスに追加しています...

Webサーバ証明書を生成しています...

JMSプロローカ証明書を生成しています...

JMSプロローカ証明書を生成しています...

「dbauser」に設定するパスワードを指定してください。 =>
```

- 11 データベース管理者 (dbauser) のパスワードを入力します。
- 12 確認のため、データベース管理者 (dbauser) のパスワードをもう一度入力します。
- 13 管理者ユーザのパスワードを入力します。
- 14 確認のため、管理者ユーザのパスワードをもう一度入力します。
- 15 ログアウトした後に novell ユーザとしてログインし直します。この操作により、install.sh スクリプトで実行された PATH 環境変数の変更の内容がロードされます。
- 16 root_install_service.sh スクリプトを実行して、Identity Audit をサービスとして開始できるようにします。このステップには root レベルのアクセスが必要です。例を次に示します。

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

```
root's password:
完了しました。
Identity Auditサービスのインストールを開始しています...

以前のインストール設定をクリーンアップしています(存在する場合)...

起動スクリプトを /etc/init.d にインストールしています...

ブート時の自動起動を設定しています...
identity_audit      0:off 1:off 2:off 3:on  4:off 5:on  6:off

完了しました。
```

- 17 root のパスワードを入力します。

Identity Audit は、ランタイムレベル 3 および 5 (コンソールで起動するマルチユーザモードまたは X-Windows モード) で起動するように設定されます。

Identity Audit サービスが開始したら、インストールの出力で指定された URL にログインできます (<https://hostIP:8443/novellidentityaudit>)。システムは内部監査イベントの処理を直ちに開始し、Identity Audit にデータを送信するためのイベントソースを管理者が設定すると、Identity Audit が完全に機能するようになります。

3.2 イベントソースの設定

Identity Audit 1.0 では、以前の Novell Audit 製品とそのプラットフォームエージェントが対応していたアプリケーションから、ログイベントを収集できます。このセクションの手順を完了する前に、Novell 製品が対応されていることを確認してください。詳細については、[14 ページのセクション 2.4 「対応プラットフォームエージェント」](#)を参照してください。

- ◆ [21 ページのセクション 3.2.1 「プラットフォームエージェントのインストール」](#)
- ◆ [22 ページのセクション 3.2.2 「プラットフォームエージェントの設定」](#)
- ◆ [22 ページのセクション 3.2.3 「監査レベルの設定」](#)

3.2.1 プラットフォームエージェントのインストール

プラットフォームエージェントは、少なくとも Identity Audit に対して推奨されている最小バージョンを使用する必要があります。詳細については、[14 ページのセクション 2.4 「対応プラットフォームエージェント」](#)を参照してください。すべてのイベントソースコンピュータで、適切なプラットフォームエージェント (32 ビットまたは 64 ビット) をインストールするか更新する必要があります。プラットフォームエージェントは、[Novell ダウンロード Web サイト \(<http://download.novell.com>\)](#) からダウンロードできる Novell Audit に含まれています。

32 ビットのプラットフォームエージェントをインストールまたはアップグレードするには：

- 1 Audit 2.0.2 FP6 以降に対応する .iso ファイルを、イベントソースコンピュータの /tmp ディレクトリにダウンロードします。
- 2 Audit 用のディレクトリを作成します (例 : `mkdir -p audit202fp6`)。
- 3 root としてログインします。
- 4 Audit の .iso ファイルをマウントします。
`mount -o loop ./NAudit202.iso ./audit202fp6`
- 5 audit202fp6 ディレクトリに移動します。
- 6 イベントソース上のオペレーティングシステムで適切なディレクトリに移動します。例を次に示します。
`cd Linux`
- 7 `pinstall.lin` を実行します。
`./pinstall.lin`
- 8 使用許諾契約を読み、条件に同意する場合は「y」を入力します。
- 9 「P」と入力してプラットフォームエージェントをインストールします。
- 10 `logevent.conf` ファイルに対する以前の設定を保持するには、「Y」を入力します。
プラットフォームエージェントがインストールされます。
- 11 プラットフォームエージェントのバージョンが正しいことを確認するには、次のコマンドを入力します。
`rpm -qa | grep AUDT`

novell-AUDTplatformagent のバージョンは、少なくとも **14 ページのセクション 2.4 「対応プラットフォームエージェント」** に記載されている対応バージョンである必要があります。

64 ビットのプラットフォームエージェントをインストールまたはアップグレードするには、NAudit 2.0.2 FP6 をダウンロードして、パッチに付属する説明に従ってください。

3.2.2 プラットフォームエージェントの設定

プラットフォームエージェントをインストールしたら、Identity Audit サーバにデータを送信するように設定する必要があります。また必要に応じて、イベントソースからイベント署名を送信するように設定します。

警告: 署名を生成するようにプラットフォームエージェントを設定すると、イベントソースコンピュータのパフォーマンスが低下する場合があります。

プラットフォームエージェントを設定するには:

- 1 イベントソースコンピュータにログインします。
- 2 編集できるように `logevent` ファイルを開きます。このファイルがある場所は、オペレーティングシステムによって異なります。
 - ◆ Linux: `/etc/logevent.conf`
 - ◆ Windows: `C:\WINDOWS\logevent.cfg`
 - ◆ NetWare: `SYS:\etc\logevent.cfg`
 - ◆ Solaris: `/etc/logevent.conf`
- 3 LogHost を Identity Audit サーバの IP アドレスに設定します。
- 4 LogEnginePort を 1289 に設定します (このエントリがまだ存在しない場合は追加します)。
- 5 イベントソースがイベント署名を送信できるようにするには、「`LogSigned=always`」と入力します。
- 6 ファイルを保存します。
- 7 プラットフォームエージェントを再起動します。この方法は、オペレーティングシステムとアプリケーションによって異なります。コンピュータを再起動するか、[Novell マニュアルの Web サイト \(http://www.novell.com/documentation\)](http://www.novell.com/documentation) にあるアプリケーション固有のマニュアルを参照して詳細を確認してください。

3.2.3 監査レベルの設定

各アプリケーションがレコードを生成するイベントの設定は、Identity Audit が監視するアプリケーションによって異なります。次の URL では、各アプリケーションについてさらに詳細な情報を参照できます。

- ◆ [Access Manager \(http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd21.html#b8cvd21\)](http://www.novell.com/documentation/novellaccessmanager/adminguide/index.html?page=/documentation/novellaccessmanager/adminguide/data/b8cvd21.html#b8cvd21)
- ◆ [eDirectory \(http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html\)](http://www.novell.com/documentation/novellaudit20/index.html?page=/documentation/novellaudit20/novellaudit20/data/b296n3h.html)

- ◆ Identity Manager (http://www.novell.com/documentation/idm36/idm_sentinel/data/bookinfo.html)
- ◆ NMAS (<http://www.novell.com/documentation/nmas32/admin/index.html?page=/documentation/nmas32/admin/data/ahefojr.html>)
- ◆ SecretStore (<http://www.novell.com/documentation/secretstore33/index.html?page=/documentation/secretstore33/nssadm/data/bsqjxv.htm>)
- ◆ SecureLogin (<http://www.novell.com/documentation/securelogin60/index.html> (see the Auditing link))

3.3 はじめに

インストール中に作成された管理者ユーザは、Identity Audit アプリケーションにログインして、ユーザの追加作成、プリロードされているレポートの実行、新しいレポートのアップロード、イベント検索の実行などが可能です。

Identity Audit にログインするには：

- 1 対応 Web ブラウザを開きます。詳細については、**14 ページのセクション 2.3 「対応ブラウザ」**を参照してください。
- 2 Identity Audit のログインページ (<https://hostIP:8443/novellidentityaudit>) にアクセスします。
- 3 Identity Audit に初めてログインした場合は、証明書が提示されます。続行するには証明書を承認する必要があります。
- 4 「admin」と入力します。
- 5 インストールの際に設定した管理者パスワードを入力します。
- 6 Identity Audit インタフェースの言語を選択します (英語、ポルトガル語、フランス語、イタリア語、ドイツ語、スペイン語、日本語、繁体字中国語、または簡体字中国語)。
- 7 [ログイン] をクリックします。

3.4 アンインストール

Identity Audit のインストールを完全にクリーンアップするには、アンインストールスクリプトを実行してから、いくつかのクリーンアップ手順を手動で実行する必要があります。

- 1 Identity Audit サーバに root としてログインします。
- 2 Identity Audit サービスを停止します。
`/etc/init.d/identity_audit stop`
- 3 次のアンインストールスクリプトを実行します。
`/opt/novell/identity_audit_1.0_x86-64/setup/root_uninstall_service.sh`
- 4 Identity Audit のホームディレクトリとその内容を削除します。

```
rm -rf /opt/novell/identity_audit_1.0_x86-64
```

5 最後の手順は、**novell** ユーザやグループに関連する情報を保持するかどうかによって異なります。

- ◆ **novell** ユーザに関連する情報を保持しない場合は、次のコマンドを実行して、ユーザ、ユーザのホームディレクトリ、グループを削除します。

```
userdel -r novell && groupdel novell
```

- ◆ **novell** ユーザとユーザのホームディレクトリを保持し、すべての **Identity Audit** 関連の設定を削除するには、次の手順に従います。

1. `~novell/.bashrc` 内の **novell** ユーザのプロファイルから、**Identity Audit** 用の次の環境変数のエントリを削除します。

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

2. PostgreSQL ファイル (`~novell/.pgpass`) から `dbauser` のエントリを削除します。
::*:dbauser: パスワード

注 : `dbauser` パスワードは平文で表示されていますが、このファイルの内容を見ることができるのは **novell** ユーザと **root** ユーザだけです。これらのユーザは、**Identity Audit** サーバのすべての機能に対する完全なアクセス権を持っています。

検索

このセクションでは、Novell® Identity Audit の検索機能について説明します。

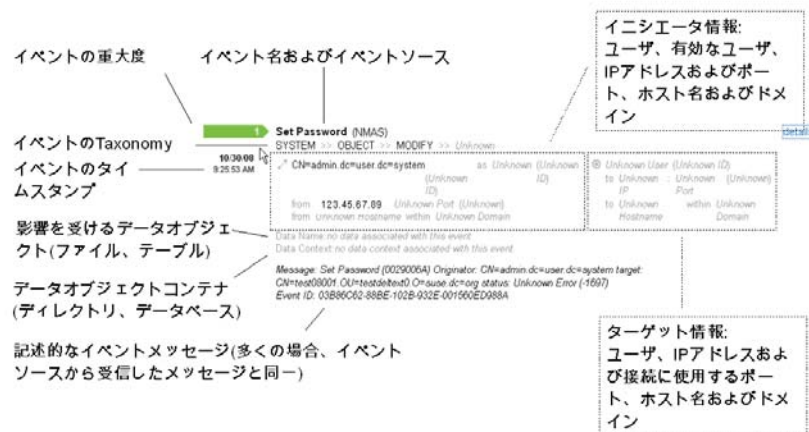
- ◆ 25 ページのセクション 4.1 「イベント検索の概要」
- ◆ 26 ページのセクション 4.2 「イベント検索の実行」
- ◆ 28 ページのセクション 4.3 「検索結果の表示」
- ◆ 30 ページのセクション 4.4 「イベントフィールド」

4.1 イベント検索の概要

Novell Identity Audit は、イベント検索を実行する機能を提供します。検索には、データベースに現在存在するすべてのオンラインデータが含まれますが、Identity Audit システムによって生成される内部イベントは、ユーザが [システムイベントの追加] を選択しない限り除外されます。デフォルトでは、イベントは検索エンジンの関連性アルゴリズムに基づいてソートされます。

基本的なイベント情報としては、イベント名、ソース、時間、重大度、イニシエータに関する情報 (矢印アイコンで表示)、ターゲットに関する情報 (ブルズアイアイコンで表示) などがあります。

図 4-1 イベントフィールド



4.2 イベント検索の実行

ユーザは簡単な検索と高度な検索を実行できます。

- ◆ 26 ページのセクション 4.2.1 「基本検索」
- ◆ 27 ページのセクション 4.2.2 「高度な検索」

4.2.1 基本検索

基本検索は 30 ページの 図表 4-1 のすべてのイベントフィールドに対して実行されます。いくつかの基本検索のサンプルには次のものが含まれています。

- ◆ root
- ◆ 127.0.0.1
- ◆ ロック *
- ◆ driverset0

注: エンドユーザのコンピュータと Identity Audit サーバの時間が同期されていない場合 (たとえば 1 台のコンピュータが 25 分遅れている場合)、検索によって予期しない結果が生じる可能性があります。過去 1 時間や過去 24 時間などの検索は、エンドユーザのコンピュータの時間に基づいています。

- 1 左側の [検索] リンクをクリックします。

Identity Audit は、ユーザが初めて [検索] リンクをクリックした場合は、重大度 3 ~ 5 のシステム外のイベントに対して、デフォルトで検索を実行するように設定されます。その他の場合は、ユーザが最後に入力した検索条件がデフォルトで適用されます。

The screenshot shows a search interface with the following elements:

- Search box: `sev:[3 TO 5]`
- Buttons: 検索 (Search), 検索のヒント (Search hints)
- Dropdown menu: 過去30日間 (Last 30 days)
- Checkboxes: システムイベントの追加 (Add system events), 時間でソート (Sort by time)
- Result message: 結果なし (No results) for [sev:[3 TO 5]]に対するイベントは見つかりませんでした (No events were found for [sev:[3 TO 5]])

- 2 別の条件で検索を行うには、検索フィールドに検索条件を入力します (たとえば admin)。この検索では大文字と小文字は区別されません。
- 3 検索対象となる期間を選択します。期間の設定値は見ればすぐ分かります。デフォルトは [過去 30 日間] です。
 - ◆ [カスタム] を指定すると、検索対象となる期間の開始日と終了日を選択できます。開始日には終了日より前の日付を設定する必要があります。時間は次の設定に基づいて指定されます。
 - ◆ [すべての時間] を指定すると、データベース内のすべてのデータが検索対象となります。
- 4 Identity Audit のシステム処理によって生成されるイベントを含めるには、[システムイベントの追加] を選択します。

5 最新のイベント順にデータを整列するには、[時間でソート] を選択します。

注: 時間によるソートは、関連性でソート(デフォルト)するよりも時間がかかり
ます。

6 [検索] をクリックします。

指定されたテキストに対して、インデックス内のすべてのフィールドが検索されま
す。回転しているアイコンは、検索が実行中であることを示します。

イベントの概要が表示されます。

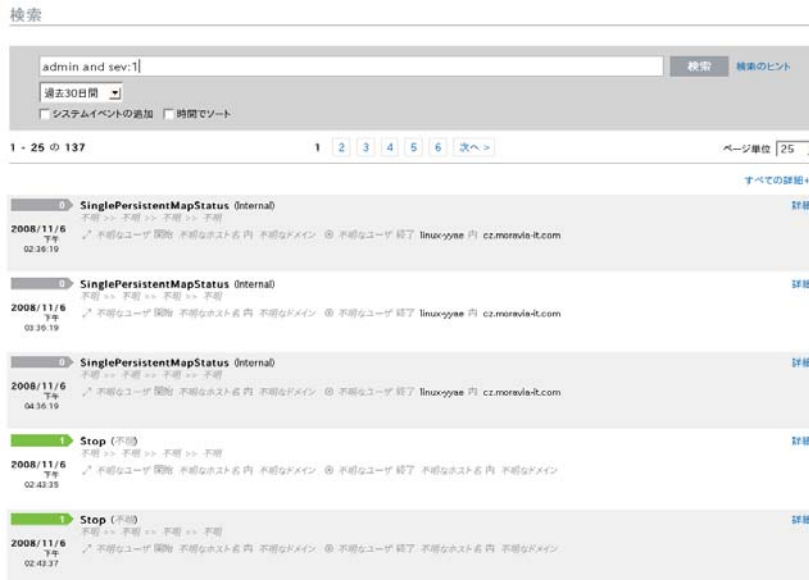


4.2.2 高度な検索

高度な検索では、特定のイベントフィールド(複数選択可)の値を検索できます。高度な
検索の条件は、各イベントフィールドの短縮名とインデックスの検索ロジックに基づいて
設定します。次の表は、各フィールドの説明と、高度な検索で使用される短縮名を記載す
るとともに、各フィールドが基本イベントビューや詳細イベントビューで表示されるかど
うかを示しています。

特定のフィールドの値を検索するには、フィールドの短縮名(詳細については [30 ページ](#)
の [図表 4-1](#) を参照)、コロン、値を使用します。たとえば、`user2` が `Identity Audit` に対
して試行した認証を検索するには、検索フィールドに次のテキストを入力します。

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



複数の高度な検索条件を結合するには、次の論理演算子を使用します。

- ◆ AND (大文字)

- ◆ OR (大文字)
- ◆ NOT (大文字、単独の検索条件としての使用は不可)
- ◆ +
- ◆ -

次の特殊文字は、\記号を使用してエスケープする必要があります。

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

高度な検索条件は、Apache Lucene オープンソースパッケージの検索条件に基づいてモデル化されています。検索条件の詳細については、Web の [Lucene Query Parser Syntax \(http://lucene.apache.org/java/2_3_2/queryparsersyntax.html\)](http://lucene.apache.org/java/2_3_2/queryparsersyntax.html) を参照してください。

4.3 検索結果の表示

検索では一連のイベントが返されます。ユーザは、イベントの基本情報や詳細な情報を表示したり、1 ページに表示する結果の件数を設定したりすることができます。検索結果はバッチ単位で返されます。デフォルトのバッチサイズは 25 件ですが、この値は簡単に設定できます。

- ◆ 28 ページのセクション 4.3.1 「基本イベントビュー」
- ◆ 29 ページのセクション 4.3.2 「詳細イベントビュー」
- ◆ 29 ページのセクション 4.3.3 「検索結果の絞り込み」

4.3.1 基本イベントビュー

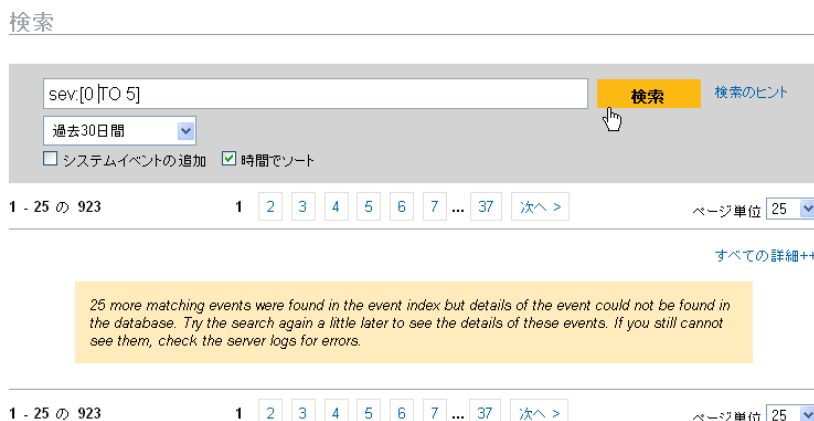
各イベントの情報は、イニシエータの情報とターゲットの情報にグループ化されます。特定のイベントフィールドのデータが利用できない場合、そのフィールドは「不明」と表示されます。

図 4-2 基本イベントビュー



場合によっては、イベントがデータベースに挿入されるよりも速く、検索エンジンがイベントのインデックスを作成することがあります。データベースに挿入されていないイベントを返す検索を実行すると、いくつかのイベントが検索クエリに一致しながらデータベースで見つからないというメッセージが表示されます。通常は、検索を後でもう一度実行すると、イベントがデータベースに存在することで検索が正常に行われます。

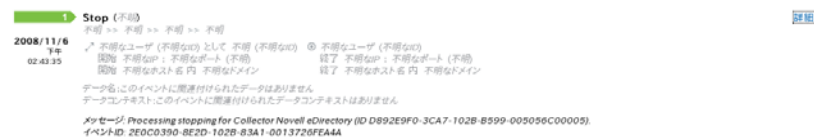
図 4-3 インデックスが作成されながらデータベースにまだ存在しないイベント



4.3.2 詳細イベントビュー

ページの右側にある [詳細] リンクをクリックすると、イベントの詳細情報を確認できません。ページ上のすべてのイベントの詳細は、[すべての詳細 ++] リンクを使用して展開したり、[すべての詳細 --] リンクを使用して折りたたんだりできます。この設定は、結果が表示される複数のページ間を移動したり、新しい検索を実行したりする際に維持されません。

図 4-4 詳細イベントビュー



このイベントは 28 ページの 図 4-2 と同じイベントを示していますが、ビューが拡張されているため、値が入力されている他のデータフィールドも表示されています。

4.3.3 検索結果の絞り込み

検索結果が表示された後に、検索結果の絞り込みや検索条件の追加が必要になる場合があります。たとえば、検索結果に特定のイニシエータユーザの名前が数回出現し、そのイニシエータによるイベントをさらに表示したい場合などです。

検索結果に出現する特定の値を使用して検索結果にフィルタを適用するには：

- 1 検索結果で、必要なフィルタ条件を特定します。
- 2 検索結果にフィルタを適用する値 (たとえばターゲットのホスト名 test1900) をクリックします。



ヒント: これにより、AND 演算子によってフィルタ条件に値が追加されます。NOT 演算子を使用してフィルタに値を追加するには、<Alt> キーを押しながら値をクリックします。

3 [検索] をクリックします。



次のフィールドは、この方法で詳細な検索を設定することができません。

- ◆ イベント時刻
- ◆ メッセージ
- ◆ レポーターに関連するすべてのフィールド
- ◆ オブザーバに関連するすべてのフィールド
- ◆ 値が [不明] であるすべてのフィールド

4.4 イベントフィールド

イベントの違いによって、値が入力されるフィールドと入力されないフィールドがあります。これらのイベントフィールドの値は、検索またはレポートを実行すると表示されます。各フィールドには、高度な検索で使用する短縮名があります。これらほとんどのフィールドの値は、詳細イベントビューに表示されます。その他の値は基本イベントビューにも表示されます。

表 4-1 イベントフィールド

フィールド	短縮名	説明	基本ビューでの表示	詳細ビューでの表示
重大度	sev	0(情報) ~ 5(重要) の基準に基づくイベントの重大度	X	X

フィールド	短縮名	説明	基本ビューでの表示	詳細ビューでの表示
イベント時刻	dt	イベントのタイムスタンプ。Identity Audit サーバのタイムスタンプまたはイベント発生元のイベントソースのタイムスタンプを設定可能 ([trust event time (信頼イベント時刻)] が有効になっている場合)。	X	X
イベント名	evt	イベントの短縮名	X	X
メッセージ	msg	詳細なイベントメッセージ		X
製品名	pn	イベントを生成した製品 (イベントソース)。 イベント名の後に表示されます。	X	X
InitUserName	sun	イベントを開始したユーザのユーザ名	X	X
InitUserID	iuid	イベントを開始したユーザのユーザ ID		X
InitUserDomain	rv35	イベントを開始したユーザのドメイン 検索は可能だが、どちらのイベントビューにも表示されない。		
InitHostName	shn	イベントが開始されたコンピュータのホスト名	X	X
InitHostDomain	rv42	イベントが開始されたコンピュータのドメイン	X	X
InitIP	sip	イベントが開始されたコンピュータの IP アドレス		X
InitServicePort	spint	イベントが開始されたポートの番号 (HTTP など)		X
InitServicePortName	sp	イベントが開始されたポートのタイプ (HTTP など)		X
TargetUserName	dun	イベントのターゲットであったユーザのユーザ名	X	X
TargetUserID	tuid	イベントのターゲットであったユーザのユーザ ID		X
TargetUserDomain	rv35	イベントのターゲットであったユーザのドメイン 検索は可能だが、どちらのイベントビューにも表示されない。		X
TargetHostName	dhn	イベントのターゲットであったコンピュータのホスト名	X	X
TargetHostDomain	rv45	イベントのターゲットであったコンピュータのドメイン	X	X
TargetIP	dip	イベントのターゲットであったコンピュータの IP アドレス		X

フィールド	短縮名	説明	基本ビューでの表示	詳細ビューでの表示
TargetServicePort	dpint	イベントのターゲットであったポートの番号 (80 など)		X
TargetServicePortName	dp	イベントのターゲットであったポートのタイプ (HTTP など)		X
TargetTrustName	ttn	イベントのターゲットであったユーザの役割 (FinanceAdmin など) 検索は可能だが、どちらのイベントビューにも表示されない。		
TargetTrustID	ttid	イベントのターゲットであったユーザの役割を表す数値 ID 検索は可能だが、どちらのイベントビューにも表示されない。		
TargetTrustDomain	ttd	検索は可能だが、どちらのイベントビューにも表示されない。		
EffectiveUserName	euname	InitUser がなりすましているユーザ (su を使用している root ユーザなど) の名前。 詳細イベントビューでの <i>Initiator Username (Initiator User ID)</i> に従う。		X
EffectiveUserID	euaid	InitUser がなりすましているユーザ (su を使用している root ユーザなど) の数値 ID		X
ObserverHostName	sn	イベントをセキュリティ情報イベント管理システムに転送したコンピュータのホスト名 (syslog サーバのホスト名など) 検索は可能だが、どちらのイベントビューにも表示されない。		
ObserverHostDomain	obsdom	イベントをセキュリティ情報イベント管理システムに転送したコンピュータのドメイン (syslog サーバのドメインなど) 検索は可能だが、どちらのイベントビューにも表示されない。		
ObserverIP	obsip	イベントをセキュリティ情報イベント管理システムに転送したコンピュータの IP アドレス (syslog サーバの IP アドレスなど) 検索は可能だが、どちらのイベントビューにも表示されない。		
ReporterHostName	rn	イベントをオブザーバに報告したコンピュータのホスト名 検索は可能だが、どちらのイベントビューにも表示されない。		

フィールド	短縮名	説明	基本ビューでの表示	詳細ビューでの表示
ReporterHostDomain	repdom	イベントをオブザーバに報告したコンピュータのドメイン 検索は可能だが、どちらのイベントビューにも表示されない。		
ReporterIP	repip	イベントをオブザーバに報告したコンピュータの IP アドレス 検索は可能だが、どちらのイベントビューにも表示されない。		
センサタイプ	st	センサタイプの 1 文字の指定子 (N= ネットワーク、H= ホスト、O= オペレーティングシステム、A および I=Identity Audit の監査イベント、P=Identity Audit のパフォーマンスイベント)。 検索は可能だが、どちらのイベントビューにも表示されない。		
DataName	fn	イベントで報告されたデータオブジェクト名 (ファイル名やデータベーステーブル名など)		X
データコンテキスト	rv36	FileName データオブジェクト (ファイルのディレクトリやデータベーステーブルのデータベースインスタンスなど) のコンテナ		X
TaxonomyLevel1	rv50	イベントのターゲット区分。イベント名の下に次の形式で表示される。 TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel2	rv51	イベントのサブターゲット区分。イベント名の下に次の形式で表示される。 TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel3	rv52	イベントのアクション情報。イベント名の下に次の形式で表示される。 TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X
TaxonomyLevel4	rv53	イベントの詳細な情報。イベント名の下に次の形式で表示される。 TaxonomyLevel1>> TaxonomyLevel2>> TaxonomyLevel3>> TaxonomyLevel4	X	X

一部のフィールドはトークン化されます。フィールドのトークン化により、ワイルドカードを使用せずにフィールド内の個々の単語を検索できます。フィールドはスペースとその他の特殊文字に基づいてトークン化されます。これらのフィールドでは、「a」または「the」などの冠詞は検索インデックスから除外されます。

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

レポート機能

この章では、Novell® Identity Audit でのレポートの実行、表示、および管理方法について説明します。

- ◆ 35 ページのセクション 5.1 「概要」
- ◆ 35 ページのセクション 5.2 「レポートの実行」
- ◆ 37 ページのセクション 5.3 「レポートの表示」
- ◆ 39 ページのセクション 5.4 「レポートの管理」

5.1 概要

Identity Audit は、Novell アプリケーションに関連付けられたレポートテンプレートの主要なセットとともにインストールされます。Identity Audit ユーザは、それぞれ必要なパラメータ (開始日や終了日など) を使用してレポートを実行することが可能で、レポート結果はユーザが選択した名前前で保存されます。レポートを実行すると、Identity Audit ユーザはその結果を取得して PDF ファイルで確認することができます。

レポートはカテゴリによって編成されます。Identity Audit には、各イベントソースに対応したレポートが付属しています。

図 5-1 カテゴリによって編成されたレポート

レポート

NOVELL ACCESS MANAGER		終了
▶ Novell Access Manager Event Count Trend 6.1r1	✕	実行
▶ Novell Access Manager Top 10 Dashboard 6.1r1	✕	実行
NOVELL EDIRECTORY		終了
▶ Novell eDirectory Account Trust Assignments 6.1r1	✕	実行
▶ Novell eDirectory Authentication by Server 6.1r1	✕	実行
▶ Novell eDirectory Authentication by User 6.1r1	✕	実行
▶ Novell eDirectory Event Count Trend 6.1r1	✕	実行

5.2 レポートの実行

Identity Audit には、複数の製品カテゴリに編成されたレポートのセットが付属しています。レポートは非同期に実行されるため、ユーザはレポートを実行しながらアプリケーションで他の作業を続けることができます。レポートの実行が完了した後に、ユーザは PDF 形式のレポート結果を確認できます。

レポート定義の多くにはパラメータが含まれています。レポートを実行する前に、これらのパラメータを設定するようメッセージが表示されます。レポートがどのように設計されているかによって、レポートのパラメータは、テキスト、数字、ブール値、または日付になります。パラメータにはデフォルト値がある場合もあれば、Identity Audit データベースの値に基づくピックリストがある場合もあります。

レポートを実行するには：

- 1 Identity Audit で [レポート] をクリックして、利用できるレポートを表示します。

レポート

NOVELL ACCESS MANAGER		隠す
▶ Novell Access Manager Event Count Trend 6.1r1	✕	実行
▶ Novell Access Manager Top 10 Dashboard 6.1r1	✕	実行
NOVELL EDIRECTORY		隠す
▶ Novell eDirectory Account Trust Assignments 6.1r1	✕	実行
▶ Novell eDirectory Authentication by Server 6.1r1	✕	実行
▶ Novell eDirectory Authentication by User 6.1r1	✕	実行
▶ Novell eDirectory Event Count Trend 6.1r1	✕	実行

必要に応じて、レポート定義をクリックして展開します。[サンプルレポート] が表示されたら、[表示] をクリックすると、レポートが最終的にどのように表示されるか、一連のサンプルデータで確認することができます。

- 2 実行するレポートを選択して、[実行] をクリックします。

Novell Access Manager Event Count Trend 6.1r1 を実行

実行オプション

名前:

Language:

Date Range:

From Date:

To Date:

Minimum Severity:

Maximum Severity:

Email Report To:

- 3 レポートを実行するスケジュールを設定します。レポートを後で実行する場合は、開始時刻を入力する必要があります。
 - ◆ [今] : デフォルトの設定です。レポートを直ちに実行します。
 - ◆ [1 回] : 指定した日時にレポートを 1 回実行します。
 - ◆ [日単位] : 1 日 1 回、指定した時刻にレポートを実行します。
 - ◆ [週単位] : 週 1 回、同じ曜日の指定した時刻にレポートを実行します。
 - ◆ [月単位] : 日時を指定して、毎月同じ日にレポートを実行します。たとえば、開始日時を 10 月 28 日午後 2 時に設定すると、毎月 28 日の午後 2 時にレポートが実行されます。

注: すべての時間設定は、ブラウザに設定されているローカル時間に基づいています。

- 4 レポート結果を特定する名前を入力します。
レポート結果を特定する際にユーザ名や日時も使用されるため、レポート名は一意の名前である必要はありません。
- 5 レポートを表示する言語を選択します (英語、フランス語、ドイツ語、イタリア語、日本語、繁体字中国語、簡体字中国語、スペイン語、ポルトガル語)。
- 6 レポートタイプを選択します。すべての時間は、ブラウザに設定されているローカル時間に基づいています。
 - ◆ [日単位]: 現在の日付の 0 時から 23 時 59 分までのイベントがレポートに表示されます。現在時刻が午前 8 時であれば、レポートには 8 時間分のデータが表示されます。
 - ◆ [週単位]: 現在の週の日曜 0 時から現在の日付が変わるまでのイベントがレポートに表示されます。
 - ◆ [月単位]: 現在の月の 1 日 0 時から現在の日付が変わるまでのイベントがレポートに表示されます。
 - ◆ [Custom Date Range (カスタム日付範囲)]: この設定を使用する場合のみ、開始日と終了日を設定する必要があります。
 - ◆ [Prior Day (前日)]: 前日の 0 時から午後 11 時 59 分までのイベントがレポートに表示されます。
- 7 [Custom Date Range (カスタム日付範囲)] を選択した場合は、レポートの開始日 (From Date) と終了日 (To Date) を設定します。

注: レポートのタイプとして [日単位]、[週単位]、[月単位]、または [Prior Day (前日)] を選択した場合、これらの時間設定は無視されます。

- 8 レポートに含まれるイベントの最低重大度を設定します。
- 9 レポートに含まれるイベントの最高重大度を設定します。
- 10 レポートをユーザに電子メールで送信する場合は、宛先の電子メールアドレスを入力します。複数のユーザに送信する場合は、電子メールアドレスをカンマで区切ります。

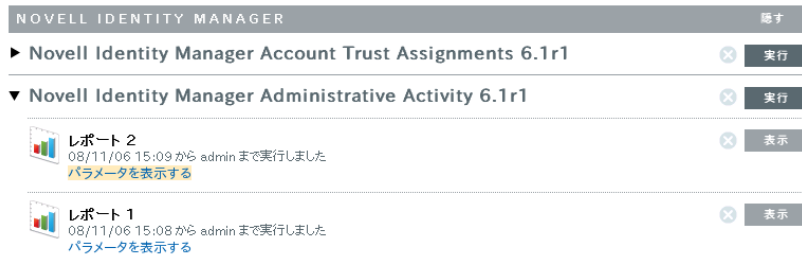
注: 電子メールによるレポートの送信を有効にするには、管理者は [ルール] > [環境設定] でメールリレーを設定する必要があります。

- 11 [実行] をクリックします。
レポート結果のエントリが作成され、指定した受信者に電子メールが送信されます。

5.3 レポートの表示

Identity Audit のユーザは、Identity Audit アプリケーションでレポートを表示することができます。その他のユーザはレポートの .pdf ファイルを電子メールで受信する場合があります。

- 1 レポート結果のリストを表示するには、[表示] をクリックします。以前実行されたすべてのレポートが、ユーザが定義したレポート名と、レポートの実行ユーザ、およびレポートの実行日時とともに表示されます。



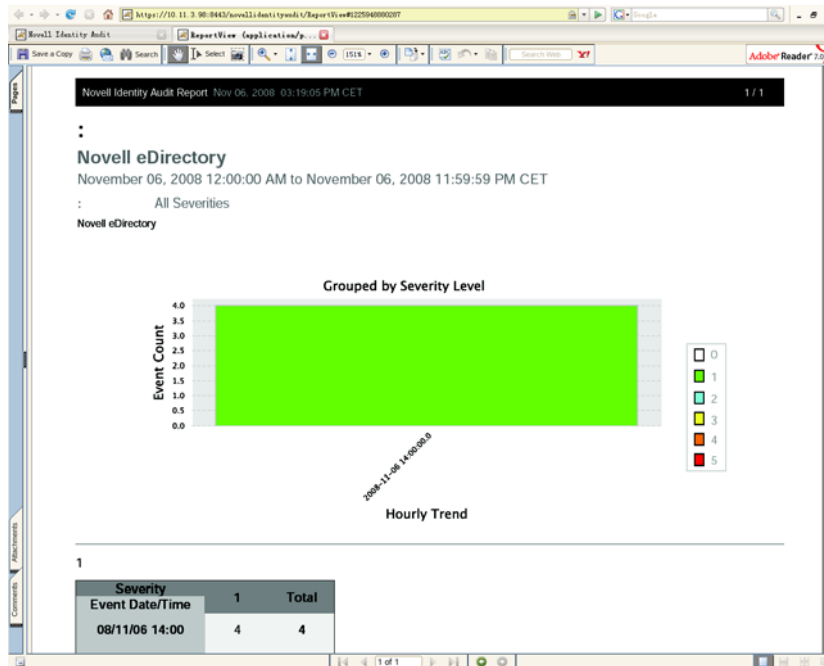
- 2 レポートを実行する際に使用された正確な値を確認するには、[パラメータを表示する] をクリックします。

▼ Novell Identity Manager Administrative Activity 6.1r1



Email Report To :
 Date Range : D
 To Date : 2008/11/06 15:08:52
 Language : ja
 From Date : 2008/11/06 15:08:52

- ◆ レポートタイプを示す値は、D= 日単位、W= 週単位、M= 月単位、DR=Custom Date Range (カスタム日付範囲)、PD=Prior Day (前日) です。
 - ◆ 言語を示す値は、en= 英語、fr= フランス語、de= ドイツ語、it= イタリア語、ja= 日本語、pt= ブラジルポルトガル語、es= スペイン語、zh= 簡体字中国語、zh_TW= 繁体字中国語です。
- 3 表示したいレポート結果の [表示] をクリックします。レポート結果は新しいウィンドウに .pdf 形式で表示されます。



ヒント：レポート結果は新しい結果から古い結果の順に並べられます。

5.4 レポートの管理

Identity Audit のユーザは、レポートの追加、削除、更新、およびスケジュール設定を行うことができます。

- ◆ 39 ページのセクション 5.4.1 「レポートの追加」
- ◆ 41 ページのセクション 5.4.2 「レポート結果の名前の変更」
- ◆ 41 ページのセクション 5.4.3 「レポートの削除」
- ◆ 41 ページのセクション 5.4.4 「レポート定義の更新」

5.4.1 レポートの追加

Identity Audit にはレポートがプリロードされていますが、新しいレポートプラグイン (レポート定義とメタデータが含まれる特別な .zip ファイル) をアップロードすることができます。システムにレポートが存在しない場合は、次の画面が表示されます。

図 5-2 ロード済みのレポートなし

レポート

現在、システムにはレポート定義がありません。1つ以上のレポート.zipファイルのアップロードから開始してください。

レポートを追加するには：

- 1 画面の左側にある [レポート] ボタンをクリックします。
- 2 [レポートのアップロード] ボタンをクリックします。
- 3 ローカルコンピュータ上のレポートプラグインの .zip ファイルの場所を指定します。
- 4 [開く] をクリックします。
- 5 [保存] をクリックします。
- 6 レポート固有の ID に基づいて、レポートリポジトリに同じレポートがすでに存在する場合は、システム内のレポートとインポートされたレポートの両方の詳細が Identity Audit に表示されます。ユーザは既存のレポートを置き換えるかどうかを決定できます。次のケースでは、インポートされたレポートと既存のレポートのバージョンが同じです。



レポート定義の置き換え

アップロードしようとしているレポート定義と同じIDのレポート定義があります。置き換えますか？

属性	リポジトリ内	インポートされているファイル内
名称	Novell-eDirectory_Password-Resets_6.1r1	Novell-eDirectory_Password-Resets_6.1r1
類型	JASPER_REPORT	JASPER_REPORT
バージョン	6.1r1	6.1r1
Release Date	Wed Oct 29 05:41:13 CET 2008	Wed Oct 29 05:41:13 CET 2008
説明	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.

キャンセル

置き換え

- 7 新しいレポート定義はアルファベット順でリストに追加され、必要な場合は直ちに実行することができます。

新しいレポートまたは更新されたレポートのダウンロード

Novell が提供する新しいレポートまたは更新されたレポートは、[Novell Content Web サイト \(http://support.novell.com/products/identityaudit/identityaudit10.html\)](http://support.novell.com/products/identityaudit/identityaudit10.html) からダウンロードできます。

新しいレポートの作成

ユーザは JasperForge* iReport を使用して、レポートの変更または書き込みを行うことができます。iReport は、Jasper レポート用のグラフィカルなレポートデザイナーです。iReport はオープンソースのレポート開発ツールで、このドキュメントの発行時点では [JasperForge.org \(http://jasperforge.org/plugins/project/project_home.php?group_id=83\)](http://jasperforge.org/plugins/project/project_home.php?group_id=83) からダウンロードできます。

新しいレポートまたは変更されたレポートには、Identity Audit の Web インタフェースにはないデータベースフィールドが追加されている場合があります。これらのデータベースフィールドは、レポートプラグインのファイルと形式に関する要件に従う必要があります。データベースフィールド、およびレポートプラグインのファイルと形式に関する要件の詳細については、[Sentinel SDK Web サイト \(http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel\)](http://developer.novell.com/wiki/index.php?title=Develop_to_Sentinel) を参照してください。

5.4.2 レポート結果の名前の変更

レポート結果は、Identity Audit のインタフェースで名前を変更することができます (レポート定義は変更できません)。

- 1 画面の左側にある [レポート] ボタンをクリックします。
- 2 レポート名をクリックして展開します。
- 3 変更するレポート結果の名前をクリックします。
- 4 新しい名前を入力します。
- 5 [名前変更] をクリックします。

5.4.3 レポートの削除

ユーザは、レポート結果セットまたはレポート定義を削除することができます。レポート定義が削除されると、関連するすべてのレポート結果も削除されます。

処理中のレポートが削除されると、データベースの検索がキャンセルされます。

5.4.4 レポート定義の更新

ユーザは既存のレポートの代わりに、更新されたレポートを Identity Audit にアップロードして置き換えることができます。詳細については、[39 ページのセクション 5.4.1 「レポートの追加」](#) を参照してください。

データコレクション

管理者は ?Novell® Identity Audit 用のデータコレクションの設定や監視を行うことができます。Identity Audit は、Novell Audit プラットフォームエージェントを使用して、さまざまな Novell アプリケーションからデータを収集する機能を備えています。対応されているプラットフォームエージェントのバージョンについては、[14 ページのセクション 2.4 「対応プラットフォームエージェント」](#) を参照してください。

- ◆ [43 ページのセクション 6.1 「イベントソースの設定」](#)
- ◆ [43 ページのセクション 6.2 「データコレクションステータス」](#)
- ◆ [45 ページのセクション 6.3 「監査サーバのオプション」](#)
- ◆ [50 ページのセクション 6.4 「イベントソース」](#)

6.1 イベントソースの設定

Identity Audit は、複数の Novell アプリケーションからデータを受け取るようにあらかじめ設定されていますが、アプリケーションサーバ自体 (イベントソース) は、データを Identity Audit サーバに送信するように設定する必要があります。これは Identity Audit の基本セットアップの一部です。詳細については、[21 ページのセクション 3.2 「イベントソースの設定」](#) を参照してください。

6.2 データコレクションステータス

管理者は、データコレクションをグローバルにまたはアプリケーションごとに有効または無効にすることができます。また、各アプリケーションのヘルス情報を表示することもできます。

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [コレクション] をクリックします。

データコレクション | ステータス 環境設定

■ 監査サーバ ○ オン ○ オフ

正常

イベントソース	オン	オフ
Novell Access Manager 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>
Novell eDirectory 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>
Novell Identity Manager 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>
Novell NMAS 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>
Novell SecretStore 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>
Novell SecureLogin 警告 (0.0 eps) 詳細を表示	<input checked="" type="radio"/>	<input type="radio"/>

- 3 監査サーバで、グローバルデータコレクションを有効または無効にします。
- 4 イベントソースから取得したアプリケーション固有のデータコレクションを有効または無効にします。
- 5 各アプリケーションのアクティブな接続の詳細を確認するには、[詳細を表示] をクリックしてください。

このページに対する変更は直ちに有効になります。

- ◆ 44 ページのセクション 6.2.1 「監査サーバ」
- ◆ 44 ページのセクション 6.2.2 「イベントソース」

6.2.1 監査サーバ

[監査サーバ] セクションで、管理者は [オン] または [オフ] オプションを使用して、データコレクションをグローバルレベルで有効または無効にすることができます。監査サーバのヘルス状態も表示されます。

正常: 緑色のインジケータは、監査サーバが正常 (監査サーバが動作中で、ポート上でリッスンしており、未解決のエラーがない状態) であることを示しています。

エラー: 赤色のインジケータは、監査サーバにエラーが発生していることを示しています。詳細については、server0.*.log ファイルを参照してください。

オフライン: 灰色のインジケータは、管理者が監査サーバをオフラインにしていることを示しています。

6.2.2 イベントソース

[イベントソース] セクションで、管理者はアプリケーションレベルのデータコレクションを有効にすることができます。これらの設定は、複数のサーバ (複数の eDirectory インスタンスなど) のデータコレクションに反映される場合があります。

注: これらの設定によって、一覧表示されているアプリケーションから取得した Identity Audit のデータコレクションが有効または無効になります。これによってイベントソースコンピュータ上のサービスが開始または停止されることはありません。

各アイコンでは、ヘルス状態が赤、黄、緑、または黒のアイコンで示されます。ほとんどのステータスについて、[詳細を表示] をクリックして詳細を確認することができます。

正常: 緑色のインジケータは、イベントソースが正常で、Identity Audit がイベントソースからデータを受信したことを示しています。

警告: 黄色のインジケータは、警告状態を示しています。よくある原因としては、アプリケーションが Identity Audit で動作していながらデータを送信していないことが考えられます。たとえばこれは、イベントソース上のプラットフォームエージェントが Identity Audit にデータを送信するように正しく設定されていないか、またはアプリケーションについてイベントログが有効になっていない場合に発生します。詳細を確認するには、[詳細を表示] をクリックしてください。

エラー: 赤色のインジケータは、Identity Audit サーバが、このアプリケーションとの接続、またはこのアプリケーションからのデータ受信について、エラーを報告していることを示しています。詳細を確認するには、[詳細を表示] をクリックしてください。

オフライン: 灰色のインジケータは、イベントソースがオフになっていることを示しています。Identity Audit はイベントソースから受信したデータを処理していません。

Identity Audit では、各オンラインデータソースについて、受信イベントに対して計算されたイベント率が表示されます。イベント率は 60 秒ごとに再計算されます。

6.3 監査サーバのオプション

管理者は Identity Audit がリッスンするポートや、イベントソースと Identity Audit 間の認証のタイプなど、Identity Audit がイベントソースのアプリケーションからデータをリッスンする方法に関して、設定を変更することができます。

- 1 Identity Audit に管理者としてログインします。
- 2 画面の一番上にある [コレクション] リンクをクリックします。
- 3 画面の右側にある [環境設定] リンクをクリックします。
- 4 [監査サーバ] が選択されていることを確認します。

データコレクション | 環境設定

- 5 Identity Audit サーバがイベントソースからのメッセージをリッスンするポートを入力します。詳細については、[46 ページのセクション 6.3.1 「ポートの設定とポート転送」](#)を参照してください。
- 6 適切なクライアント認証とサーバのキーペア設定を設定します。詳細については、[47 ページのセクション 6.3.2 「クライアント認証」](#)を参照してください。
- 7 バッファがイベントでいっぱいになった場合の、Identity Audit サーバの動作を選択します。

接続を一時的に停止する：この設定では、既存の接続を中断し、バッファに新しいメッセージ用の空き領域ができるまで、新しい接続を拒否します。同時に、イベントソースがメッセージをキャッシュします。

最も古いメッセージをドロップする：この設定では、新しいメッセージを受信するために最も古いメッセージをドロップします。

警告：[最も古いメッセージをドロップする] を選択した場合、ドロップされたメッセージを復元する方法はありません。

- 8 一定時間にわたってデータを送信していないイベントソースの接続を解除するには、[アイドル状態の接続] を選択します。

イベントソースの接続は、データの送信を再開した時点で再度自動的に確立されます。

- 9 アイドル状態の接続を解除するまでの時間数(分)を入力します。
- 10 イベントと合わせて署名を受け取るようにするには、[イベント署名] を選択します。

注: 署名を受け取るには、イベントソースのプラットフォームエージェントを正しく設定する必要があります。詳細については、[43 ページのセクション 6.1 「イベントソースの設定」](#) を参照してください。

- 11 [保存] をクリックします。

6.3.1 ポートの設定とポート転送

Identity Audit がプラットフォームエージェントからのメッセージをリッスンするデフォルトのポートは 1289 です。このポートが設定されると、システムはそのポートが有効で開いているかどうか確認します。

1024 未満のポートにバインドするには、ルート権限が必要になります。代わりに、1024 より大きいポートの使用をお勧めします。ソースデバイスを変更することで、より高位のポートへの送信、または Identity Audit サーバでのポート転送が可能になります。

イベントソースを変更して異なるポートに送信するには:

- 1 イベントソースコンピュータにログインします。
- 2 編集できるように `logevent` ファイルを開きます。このファイルがある場所は、オペレーティングシステムによって異なります。
 - ◆ Linux: `/etc/logevent.conf`
 - ◆ Windows: `C:\WINDOWS\logevent.cfg`
 - ◆ NetWare: `SYS:\etc\logevent.cfg`
 - ◆ Solaris: `/etc/logevent.conf`
- 3 `LogEnginePort` パラメータを目的のポートに設定します。
- 4 ファイルを保存します。
- 5 プラットフォームエージェントを再起動します。この方法は、オペレーティングシステムとアプリケーションによって異なります。コンピュータを再起動するか、[Novell マニュアルの Web サイト \(<http://www.novell.com/documentation>\)](#) にあるアプリケーション固有のマニュアルを参照して詳細を確認してください。

Identity Audit サーバでポート転送を設定するには:

- 1 Identity Audit サーバのオペレーティングシステムに `root` として (または `su` を使用した `root` として) ログインします。
- 2 編集できるように `/etc/init.d/boot.local` ファイルを開きます。
- 3 起動処理の末尾の部分に次のコマンドを追加します。

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

`protocol` は `tcp` または `udp`、`incoming port` はメッセージを受信するポート、`IP:rerouted port` はローカルコンピュータの IP アドレスと 1024 より大きい使用可能なポートを示します。

- 4 変更内容を保存します。
- 5 再起動します。すぐに再起動できない場合は、コマンドラインから `iptables` コマンドを実行します。

6.3.2 クライアント認証

イベントソースは SSL 接続を経由してデータを送信し、Identity Audit サーバの [クライアント認証] 設定では、イベントソース上のプラットフォームエージェントから受信した証明書に対して実行する認証の種類を決定します。

オープン: 認証は必要ありません。Identity Audit は、イベントソースからの証明書を要求しません。証明書を必要とすることも、検証することはありません。

非厳密: イベントソースからの有効な X.509 証明書が必要ですが、証明書は検証されません。認証局による署名は必要ありません。

厳密: イベントソースからの有効な X.509 証明書が必要で、信頼される認証局によって署名されている必要があります。イベントソースが有効な証明書を提示しない場合、Identity Audit はイベントデータを受け取りません。

- ◆ [47 ページの「Truststore の作成」](#)
- ◆ [48 ページの「Truststore のインポート」](#)
- ◆ [49 ページの「サーバのキーペア」](#)

Truststore の作成

厳密な認証では、イベントソースの証明書またはイベントソースの証明書に署名した認証局 (CA) の証明書を含む Truststore が必要です。DER 証明書または PEM 証明書を取得すると、Identity Audit に付属する `CreateTruststore` ユーティリティを使用して、Truststore を作成することができます。

- 1 Identity Audit サーバに `novell` としてログインします。
- 2 `/opt/novell/identity_audit_1.0_x86/data/updates/done` に移動します。
- 3 `audit_connector.zip` ファイルを解凍します。
`unzip audit_connector.zip`
- 4 証明書を持つコンピュータに `TruststoreCreator.sh` または `TruststoreCreator.bat` をコピーするか、`TruststoreCreator` ユーティリティがインストールされているコンピュータに証明書をコピーします。
- 5 `TruststoreCreator.sh` ユーティリティを実行します。
`TruststoreCreator.sh -keystore /tmp/my.keystore -password password1 -certs /tmp/cert1.pem,/tmp/cert2.pem`

この例では、`TruststoreCreator` ユーティリティによって、2つの証明書 (`cert1.pem` および `cert2.pem`) を含む `my.keystore` というキーストアファイルが作成されます。このファイルはパスワード `password1` によって保護されています。

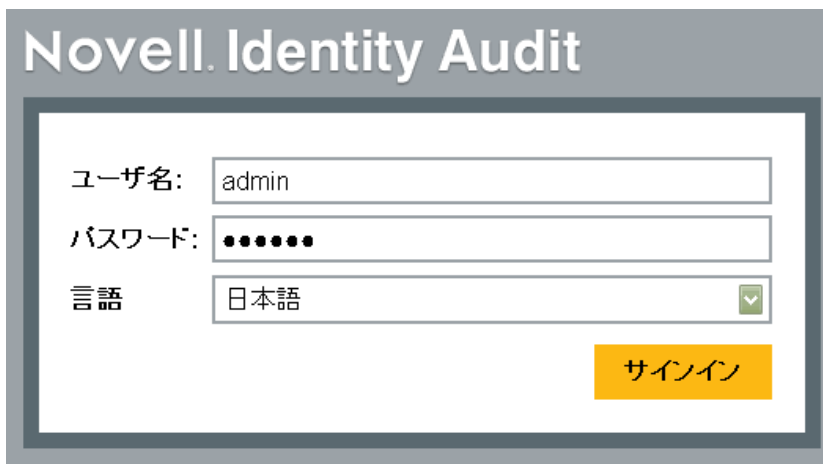
Truststore のインポート

厳密な認証では、管理者は [インポート] ボタンを使用して Truststore をインポートできます。これにより、認証されたイベントソースだけが Identity Audit にデータを送信できるようになります。Truststore には、イベントソースの証明書または署名した認証局の証明書のいずれかが含まれている必要があります。

次の手順は、Truststore があるコンピュータで実行する必要があります。Truststore があるコンピュータで Web ブラウザを開くか、Web ブラウザがある任意のコンピュータに Truststore を移動することができます。

Truststore をインポートするには：

- 1 Identity Audit に管理者としてログインします。
- 2 画面の一番上にある [コレクション] リンクをクリックします。
- 3 画面の右側にある [環境設定] リンクをクリックします。
- 4 [監査サーバ] タブが選択されていることを確認します。
- 5 [クライアント認証] の下にある [厳密] オプションを選択します。



- 6 [参照] をクリックして、Truststore ファイル (たとえば my.keystore) を指定します。
- 7 Truststore ファイルのパスワードを入力します。
- 8 [インポート] をクリックします。
- 9 Truststore の詳細を確認するには、[詳細] をクリックします。

- クライアント認証: オープン - 認証は必要ありません。
- 非厳密 - クライアント証明書が必要です。
- 厳密 - 認証局によって署名されたクライアント証明書が必要です。

原則	発行者
CN=sles10-scout,OU=client,O=.,L=.,ST=.,C=.	CN=sles10-sco
CN=sles10-scout,OU=client,O=.,L=.,ST=.,C=.	CN=sles10-sco

キャンセル

10 [保存] をクリックします。

Truststore を正しくインポートすると、[詳細] をクリックして Truststore に含まれる証明書を表示することができます。

サーバのキーペア

Identity Audit には、イベントソースに対して Identity Audit サーバを認証するための、組み込みの証明書が付属しています。この証明書は、公的な認証局 (CA) が署名した証明書で置き換えることができます。

組み込みの証明書を置き換えるには：

- 1 Identity Audit に管理者としてログインします。
- 2 画面の一番上にある [コレクション] リンクをクリックします。
- 3 画面の右側にある [環境設定] リンクをクリックします。
- 4 [監査サーバ] が選択されていることを確認します。
- 5 [サーバのキーペア] の下にある [カスタム] を選択します。
- 6 [参照] をクリックして、Truststore ファイルを指定します。
- 7 Truststore ファイルのパスワードを入力します。
- 8 [インポート] をクリックします。

ファイル内にパブリックキーとプライベートキーのペアが複数ある場合は、目的のキーペアを選択して [OK] をクリックします。

9 サーバのキーペアの詳細を確認するには、[詳細] をクリックします。

10 [保存] をクリックします。

6.4 イベントソース

管理者は [イベントソース] ページで、各イベントソースから受信するイベントのイベント時刻を決定する方法を設定できます。イベント時刻は、イベントソースからのタイムスタンプ (「信頼イベント時刻」)、または Identity Audit サーバからのタイムスタンプによって決定します。タイムスタンプは、検索結果を時間でソートした場合にイベントが表示される順序に影響します。またタイムスタンプは、レポートでの表示時間にも影響します。デフォルトでは Identity Audit サーバの時間が使用されます。

注: Identity Audit システム内のすべてのコンピュータで時刻同期を維持するために、NTP サーバの使用をお勧めします。NTP サーバを使用できる場合は、アプリケーションのイベント時刻を信頼することをお勧めします。NTP サーバを使用できない場合は、すべてのアプリケーションについて、Identity Audit サーバの時間を使用することをお勧めします (デフォルト設定)。これによって、コンピュータ間の時間の差分が修正されます。

イベント時刻のオプションを変更するには:

- 1 Identity Audit に管理者としてログインします。
- 2 画面の一番上にある [コレクション] リンクをクリックします。
- 3 画面の右側にある [環境設定] リンクをクリックします。
- 4 [イベントソース] をクリックします。
- 5 イベント発生元のアプリケーションのタイムスタンプを使用するアプリケーションをすべて選択します。

監視サーバ イベントソース

次のアプリケーションに関連付けられたイベント時刻を信頼する。(これは何ですか?):

- Novell Access Manager
- Novell eDirectory
- Novell Identity Manager
- Novell NMAS
- Novell SecretStore
- Novell SecureLogin

キャンセル 保存

その他のすべてのアプリケーションについては、**Identity Audit** サーバのタイムスタンプで、イベント発生元のアプリケーションのタイムスタンプが置き換えられます。

この変更内容は、新たに受信するすべてのイベントに対して直ちに反映されます。すでにキューに登録されているイベントについては、処理に時間がかかる場合があります。

データストレージ

Novell® Identity Audit のインストールでは、PostgreSQL データベースとともに、Identity Audit の実行に必要なすべてのテーブルとユーザがインストールされます。データベースには、データベースのパーティション管理や古いデータのアーカイブを実行するためのストアドプロシージャも含まれています。管理者は Web インタフェースを介して、データベースストレージやアーカイブの設定を管理できます。

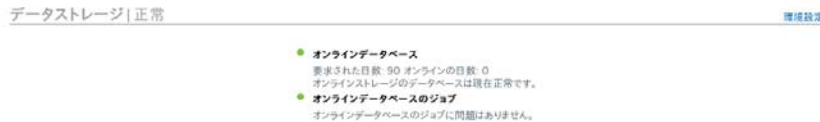
- 53 ページのセクション 7.1 「データベースヘルス」
- 54 ページのセクション 7.2 「データストレージの設定」

7.1 データベースヘルス

管理者だけが使用できる [データストレージ|正常] ページには、データベース内で使用できるパーティションの数や、パーティションの新規作成およびデータのアーカイブを実行するストアドプロシージャの成否に基づいて、データベースヘルスが表示されます。

データベースヘルスを参照するには：

- 1 Identity Audit に管理者としてログインします。
- 2 [保存場所] リンク (ページの右上隅) をクリックします。
[正常] ページが表示されます。



このページにはデータベースの各機能の状態が色分けされて示され、正常な状態は緑、警告の状態は黄、エラーの状態は赤で表示されます。

オンラインデータベース：このインジケータは、パーティション化されたテーブルごとに、想定される数のパーティションがデータベースに存在するかどうかを示します。想定されるパーティションの数は、オンラインになるように設定された日数に基づきます (新しいインストールの場合はインストールしてから経過した日数)。

パーティションの数が想定される数と異なる場合、このページにはそのテーブルの名前、想定されるパーティションの数、データベース内の実際のパーティションの数が表示されます。

オンラインデータベースのジョブ：このインジケータは、前回ストアドプロシージャによってパーティションが追加されデータが削除されたときにエラーが発生した場合に、赤に変わります。アーカイブを有効にしている場合は、パーティションを追加するジョブが前回実行されたときにエラーが発生した場合にだけ、インジケータが変わります。エラーが発生した場合は、失敗したジョブに関連する名前、タイムスタンプ、および詳細がページに表示されます。

アーカイブデータベース: このインジケータは、アーカイブが有効になっている場合のみ表示されます。インジケータは、データをアーカイブするストアドプロシージャが前回実行されたときにエラーが発生した場合に、赤に変わります。エラーが発生した場合は、失敗したジョブに関連する名前、タイムスタンプ、および詳細がページに表示されます。

7.2 データストレージの設定

データベースは、受信イベントや環境設定の情報、およびレポート結果を格納するためのリポジトリです。Identity Audit は、データベースがいっぱいになるのを防ぐためのデータベース管理手順を提供します。管理者だけがアクセスできる [データストレージ] ページには、データストレージに関するいくつかの設定を行う機能があります。

図 7-1 データストレージの設定

データストレージ | 環境設定

データをオンラインで保持する期間: 90 日

オンラインの期間が過ぎた後のアクション: データを削除する
 データをアーカイブする

毎日の保守の実行時間: 01 : 00 AM GMT+0100 (サーバ時間)

キャンセル 保存

データをオンラインで保持する期間: 管理者は、レポート機能で使用する目的でデータをデータベースに保持する日数を指定できます。この日数の最小値は 1 日で、小数ではなく整数を指定する必要があります。

オンラインの期間が過ぎた後のアクション: オンラインデータの保持期間が期限切れになると、指定した期間より古いイベントデータは削除されるか、データベースからアーカイブディレクトリに移動されます。

警告: 削除されたデータを復元することはできません。[削除] オプションは慎重に選択してください。

このデータベースディレクトリにアーカイブ: [データをアーカイブする] オプションを選択した場合、アーカイブデータが書き込まれる既存のディレクトリの場所を指定します。このディレクトリがすでに存在すること、およびこのディレクトリに対して novell ユーザが書き込み権を持っていることが必要です。デフォルトでは、この場所は Identity Audit のホームディレクトリの /data/db_archive に設定されます。このデフォルトディレクトリは、Identity Audit のインストール中に適切なパーミッションで作成されます。

重要: ハードディスクがいっぱいにならないように、定期的にアーカイブファイルを長期保管場所に移動することをお勧めします。

テスト: [データをアーカイブする] オプションを選択した場合は、[テスト] ボタンを使用して、アーカイブディレクトリが存在するかどうか、また novell ユーザが書き込み権を持っているかどうかを検証できます。

毎日の保守の実行時間 : 保守作業を実行する時刻を指定します。この時刻は Identity Audit サーバのローカル時刻に基づきます。スケジュールされた保守の実行時間になると、データベースにパーティションを追加するためのストアドプロシージャが実行されます。その 2 時間後、設定された日数よりも古いデータをアーカイブまたは削除するためのストアドプロシージャが実行されます。

データのアーカイブは、データベースの使用率が比較的低い時間に行うように計画する必要があります。

ルール

この章ではイベントチャネルについて説明します。イベントチャネルは、イベントを Identity Audit から別のシステムに送信する際に使用できます。

- ◆ 57 ページのセクション 8.1 「ルールの概要」
- ◆ 58 ページのセクション 8.2 「ルールの設定」
- ◆ 59 ページのセクション 8.3 「アクションの設定」

8.1 ルールの概要

[ルール] インタフェースでは、すべての受信イベントを評価して、指定した出力チャネルに選択したイベントを配信するルールを定義することができます。たとえば、重大度 5 の各イベントを、セキュリティアナリスト配信リストまたは管理者に電子メールで送信することができます。

注: すべてのイベントはデータベースにも配信されます。

受信イベントはそれぞれのフィルタリングルールに従って評価され、一致が見つかったら、そのルールに関連付けられている配信アクションが実行されます。

電子メールに送信: 設定された SMTP リレーを使用して、イベントをユーザに送信します。

ファイルに書き出し: Identity Audit サーバ上の指定されたファイルにイベントを書き出します。

Syslog に送信: 設定済みの Syslog サーバにイベントを転送します。

ヒント: 関連付けられているアクションによって、イベントが 1 件ずつ処理されます。したがって、イベントの送信先の出力チャネルを選択する場合は、パフォーマンスに対する影響を考慮する必要があります。たとえば、「ファイルに書き出し」アクションは使用するリソースが最も少ないため、大量のイベントを電子メールまたは Syslog に送信する前にデータ量を決定する、ルールの条件をテストする際に使用できます。

また、「電子メールに送信」アクションを設定する場合は、受信者が効率よく処理でき、ルールに従ってフィルタリングを調整できるイベント数を判断する必要があります。

イベント出力は、軽量なデータ交換形式である JavaScript Object Notation (JSON) 形式で送信されます。イベントは、フィールド名 (イベント名を示す「evt」など)、コロン、値 (「Start」など) をカンマで区切って構成されます。

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

8.2 ルールの設定

Identity Audit のルールを設定することにより、1 つ以上の検索可能フィールドに基づいてイベントにフィルタを適用することができます。Identity Audit の検索可能イベントフィールドの一覧については、30 ページの図表 4-1 を参照してください。各ルールは、設定済みの 1 つ以上のアクションに関連付けることができます。

- ◆ 58 ページのセクション 8.2.1 「フィルタ条件」
- ◆ 58 ページのセクション 8.2.2 「ルールの追加」
- ◆ 59 ページのセクション 8.2.3 「ルールの配列」
- ◆ 59 ページのセクション 8.2.4 「ルールの削除」
- ◆ 59 ページのセクション 8.2.5 「ルールの有効化または無効化」

8.2.1 フィルタ条件

ルールは、検索可能な任意のイベントフィールドに基づいて作成できます。これらのフィールドのリストは、30 ページの図表 4-1 を参照してください。使用できる演算子は、イベントフィールドのデータの種類によって異なります。たとえば、match subnet は IP アドレスに対して使用でき、match regex はテキストフィールドに対して使用できます。

8.2.2 ルールの追加

管理者はフィルタベースのルールを追加して、ルールの条件に適合するイベントを出力する 1 つ以上のチャンネルを定義できます。

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ルール] をクリックします。
- 3 [ルールを追加] をクリックします。
- 4 ルールの名前を入力します。
- 5 複数の条件を作成する場合は、[すべて] を選択し、AND 演算子を使用して条件を結合します。OR 演算子を使用して条件を結合するには、[任意] を選択します。
- 6 イベントフィールド、演算子、およびフィルタの値を選択します。

ルール名:

次の条件のうち すべて 次の条件を満たす場合:

=

次のアクションを実行する:

~ --- (設定を参照)

キャンセル 保存

- 7 フィルタ条件に適合するイベントを実行するアクションを選択します。
アクションの詳細は、[環境設定] リンクをクリックすると表示される設定情報に基づいています。

- 必要に応じてその他のアクションを設定します。
- [保存] をクリックします。

8.2.3 ルールの配列

イベントは配列されたルールによって一致が見つかるまで評価されるため、ルールを適切に配列することをお勧めします。より狭く定義されたルールや、より重要なルールは、リストの最初に配置する必要があります。複数のルールがある場合は、ルールの順序をドラッグアンドドロップで変更することができます。

ルールの順序を変更するには：

- Identity Audit に管理者としてログインします。
- ページの右上隅にある [ルール] をクリックします。
- ルール番号の左側にあるアイコンの上にカーソルを置くと、ドラッグアンドドロップが可能になります。このときカーソルは変化します。



- ルールをリスト内の適切な場所にドラッグアンドドロップします。

8.2.4 ルールの削除

ルールを削除するときアクション用のキューにイベントがすでに存在する場合、ルールが無効化されてからそのキューがフラッシュされるまで、しばらく時間がかかることがあります。

8.2.5 ルールの有効化または無効化

各ルールの左側の [オン] の列に、そのルールを有効化するチェックボックスがあります。新しいルールはデフォルトで有効になります。ルールを無効にすると、受信イベントがそのルールに従って評価されることはなくなります。アクション用のキューにイベントがすでに存在する場合、ルールが無効化されてからそのキューがフラッシュされるまで、しばらく時間がかかることがあります。

8.3 アクションの設定

イベントは、いずれかのルールで指定された条件に適合すると、1つ以上のチャンネルに配信されます。イベントをチャンネルに出力するには、そのチャンネルに送信するアクションを、適切な接続情報と併せて設定する必要があります (SMTP リレーが必要な場合は、認証資格情報も設定します)。Identity Audit システムでは、アクションタイプごとに設定済みの接続を1つだけ保持できます。たとえば、ファイルに書き込まれるすべてのイベントは同じファイルに書き込まれる必要があります。

- ◆ 60 ページのセクション 8.3.1 「電子メールに送信」

- ◆ 60 ページのセクション 8.3.2 「Syslog に送信」
- ◆ 61 ページのセクション 8.3.3 「ファイルに書き出し」

8.3.1 電子メールに送信

「電子メールに送信」アクションを設定するには ?SMTP リレーの接続情報 (IP アドレスとポート番号) ?宛先アドレス ?および送信元アドレスが必要です。カンマ区切りのリストを入力することにより ?複数の電子メールアドレスに送信することができます。

注 : SMTP リレーまたは電子メール受信者が受信可能なデータ量を超えないように、このアクションは生成するイベントの量が少ないルールで使用する必要があります。

この SMTP リレー設定は、ユーザにレポートを配信する場合にも使用されます。

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ルール] をクリックします。
- 3 [環境設定] をクリックします。
- 4 [電子メール] で、使用可能な SMTP リレーの名前とポートを入力します。必要に応じて [テスト] をクリックし、接続をテストします。

電子メール

SMTP: ポート:

テストが成功しました。 ✓

ユーザ名: パスワード:

開始:

送信先:

複数の電子メールアドレスをコンマで区切ります。

- 5 SMTP リレーで認証が必要な場合は、ユーザ名とパスワードを入力します。
- 6 電子メールメッセージの送信元のアドレスを入力します。
- 7 1 つ以上の電子メールアドレスをカンマで区切って入力します。
- 8 [保存] をクリックします。

? 「電子メールに送信」アクションが定義されているフィルタ条件を満たす Identity Audit のすべてのイベントは ? 同じ SMTP リレーおよび一連のアドレスに送信されます。

8.3.2 Syslog に送信

「Syslog に送信」アクションを設定するには、Syslog サーバの接続情報 (IP アドレスとポート番号) が必要です。

- 1 Identity Audit に管理者としてログインします。

- 2 ページの右上隅にある [ルール] をクリックします。
- 3 [環境設定] をクリックします。
- 4 [Syslog] で、名前または IP アドレスを入力し、Syslog サーバのポートを開きます。必要に応じて [テスト] をクリックし、送信先のサーバとポートが存在するかどうかをテストします。

Syslog

宛先:	<input type="text" value="localhost"/>	ポート:	<input type="text" value="514"/>	<input type="button" value="テスト"/>
-----	--	------	----------------------------------	------------------------------------

- 5 [保存] をクリックします。

?Syslog に送信」アクションが定義されているフィルタ条件を満たす Identity Audit のすべてのイベントは ? 同じ Syslog サーバに送信されます。

8.3.3 ファイルに書き出し

「ファイルに書き出し」アクションを設定するには ? イベントが書き込まれるファイルの名前とパスが必要です。このディレクトリがすでに存在すること、およびこのディレクトリに対して novell ユーザが書き込み権を持っていることが必要です。ファイルが存在しない場合は、Identity Audit によって作成されます。

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ルール] をクリックします。
- 3 [環境設定] をクリックします。
- 4 [ファイル名] で、イベントを書き込むファイルのパスを入力します。必要に応じて [テスト] をクリックし、接続をテストします。

ファイル名

宛先:	<input type="text" value=" ../data/log_to_file_events.txt"/>	<input type="button" value="テスト"/>
-----	--	------------------------------------

- 5 [保存] をクリックします。

? ファイルに書き出し」アクションが定義されているフィルタ条件を満たす Identity Audit のすべてのイベントは ? 同じファイルに書き込まれます。

ユーザ管理

管理者は ?Novell® Identity Audit でユーザの追加、編集、削除を行ったり、管理権を付与したりすることができます。ユーザは ? 各自のユーザプロファイルの詳細を編集することができます。

- ◆ 63 ページのセクション 9.1 「ユーザの追加」
- ◆ 64 ページのセクション 9.2 「ユーザの詳細の編集」
- ◆ 65 ページのセクション 9.3 「ユーザの削除」

9.1 ユーザの追加

Identity Audit システムでユーザを追加すると、Identity Audit アプリケーションにログインできるアプリケーションユーザが作成されます。

[管理権の付与] オプションを選択すると、そのユーザに Identity Audit システムでの管理権が与えられます。管理権には、次の機能を管理する権利が含まれています。

- ◆ ユーザ管理
- ◆ データコレクション
- ◆ データストレージ

ユーザを追加するには：

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ユーザ管理] をクリックします。
- 3 [ユーザの追加] をクリックします。
- 4 ユーザ情報を入力します。

ユーザ管理

ユーザの名前と電子メールアドレスを指定してください。

名:	<input type="text"/>
姓:	<input type="text"/>
電子メール:	<input type="text"/>
<input type="checkbox"/> 管理権の付与	

このユーザのユーザ名とパスワードを選択してください。

ユーザ名: *	<input type="text"/>
パスワード: *	<input type="password"/>
確認: *	<input type="password"/>

アスタリスク (*) が付いたフィールドは必須入力です。またユーザ名は一意である必要があります。

注: 電子メールアドレスの形式は指定されていますが、電話番号フィールドでは任意の形式を使用できます。正しい電話番号を入力してください。

- 5 必要に応じて [管理権の付与] を選択します。
- 6 [保存] をクリックします。

9.2 ユーザの詳細の編集

管理者は、システム内のすべてのユーザの情報を編集できます。ユーザは、ユーザ名と管理者ステータスを除き、自分のプロフィールの任意のフィールドを編集できます。また、パスワードを変更することもできます。

- ◆ 64 ページのセクション 9.2.1 「自分のプロフィールを編集する」
- ◆ 64 ページのセクション 9.2.2 「自分のパスワードを変更する」
- ◆ 65 ページのセクション 9.2.3 「別のユーザのプロフィールを編集する (管理者のみ)」
- ◆ 65 ページのセクション 9.2.4 「別のユーザのパスワードをリセットする (管理者のみ)」

9.2.1 自分のプロフィールを編集する

- 1 右上隅にある [プロフィール] をクリックします。

- 2 任意のフィールドを編集します。
- 3 [保存] をクリックします。

9.2.2 自分のパスワードを変更する

ユーザは、現在のパスワードを知っていれば、自分のパスワードを変更することができます。現在のパスワードがわからない場合は、管理者がパスワードをリセットする必要があります。

- 1 右上隅にある [プロフィール] をクリックします。
- 2 現在のパスワードを入力します。
- 3 新しいパスワードを入力します。
- 4 確認のため、新しいパスワードをもう一度入力します。
- 5 [保存] をクリックします。

9.2.3 別のユーザのプロファイルを編集する (管理者のみ)

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ユーザ管理] をクリックします。
- 3 編集するユーザに対応する [編集] をクリックします。
- 4 任意のフィールド (ユーザ名を除く) を編集します。
- 5 [保存] をクリックします。
[管理権の付与] に対する変更は、ユーザが次にログインしたときに有効になります。

9.2.4 別のユーザのパスワードをリセットする (管理者のみ)

別のユーザのパスワードをリセットする方法については、[65 ページのセクション 9.2.3 「別のユーザのプロファイルを編集する \(管理者のみ\)」](#) を参照してください。

9.3 ユーザの削除

管理者は、システムからユーザを削除できます。

- 1 Identity Audit に管理者としてログインします。
- 2 ページの右上隅にある [ユーザ管理] をクリックします。
- 3 削除するユーザに対応する [編集] をクリックします。
- 4 ページの右上隅にある [このユーザを削除] をクリックします。
- 5 確認して [削除] をクリックします。

Truststore

A

Identity Audit と、データを収集する Novell アプリケーション間の接続に対して厳密な認証を使用すると、データのセキュリティが向上します。

A.1 キーストアの作成

キーストアは、jre のインストールに付属している、Java の「keytool」実行可能ファイルを使用して作成できます。このキーストアには、Identity Audit に付属するデフォルトの証明書に代わる、パブリックキーとプライベートキーのキーペアが保存されています。基本的な手順を次に示しますが、keytool の詳細については、Sun の Web サイト (<http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html>) を参照してください。

- 1 Java の /bin ディレクトリに移動します (たとえば \$JAVA_HOME/bin)。
- 2 次のコマンドを実行します。
`keytool -genkey -alias alias -keystore .keystore`
- 3 キーストアのパスワードを入力します。このパスワードは Truststore をインポートする場合に使用します。
- 4 次の情報を入力します。
 - ◆ 氏名
 - ◆ 部門
 - ◆ 組織
 - ◆ 市または地域
 - ◆ 都道府県
 - ◆ 2 桁の国コード
- 5 情報を確認します。
- 6 キーストアのパスワードと同じパスワードを使用する場合は <Enter> キーを押します。
.keystore ファイルと、プライベートキーおよび対応するパブリックキー (証明書) が作成されます。