CA User Activity Reporting Module

概要ガイド

リリース 12.5.03

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。 いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負います。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2011 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager（CA EEM）
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager（CA IT PAM）
- CA NSM
- CA Security Command Center（CA SCC）
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

マニュアルの変更点

以下のドキュメントのアップデートは、本書の最新のリリース以降に行われたものです。

- クイック スタートの概要 — 既存のトピックが更新され、CA User Activity Reporting Module サーバ上のデフォルトのエージェントによって収集される追加のイベントのタイプが確認できます。
- ポリシー違反アラート — 既存のトピックが更新され、ヘルプ デスク チケットを作成する機能など、直接アラートを送信して IT PAM イベント/アラート出力プロセスを実行する機能やネットワーク セキュリティ監視システムに SNMP トラップとしてアラートを送信する機能について確認できます。
- ドキュメントのマニュアル選択メニューによる検索 — 既存のトピックが更新され、CA User Activity Reporting Module マニュアル選択メニューに表示されている新しい API プログラミング ガイドを確認できます。

詳細情報:

クイック スタートの概要 (P. 13)
ポリシー違反アラート (P. 59)
ドキュメントのマニュアル選択メニューによる検索 (P. 69)

目次

第 1 章: 紹介 7

本書の内容 7
CA User Activity Reporting Module について 8
ネットワーク -- インストール前 9
インストール内容 10

第 2 章: クイック スタート展開 13

クイック スタートの概要 13
シングル サーバ システムのインストール 14
Windows の hosts ファイルの更新 21
最初の管理者の設定 21
Syslog イベント ソースの設定 25
Syslog コネクタの編集 28
Syslog イベントの表示 31

第 3 章: Windows エージェント展開 35

エージェントのユーザ アカウントの作成 36
エージェント認証キーの設定 38
エージェント インストール プログラムのダウンロード 39
エージェントのインストール 41
NTEventLog に基づいたコネクタの作成 43
Windows イベント ソースの設定 48
Windows イベント ソースからのログの表示 48

第 4 章: 主な機能 51

ログ収集 52
ログ ストレージ 54
ログの標準化された表示 56
コンプライアンス レポート 57
ポリシー違反アラート 59
資格管理 60

ロールベースのアクセス 61
サブスクリプション管理 62
Out-of-the-Box コンテンツ 63

第 5 章: CA User Activity Reporting Module の詳細情報 65

ツールヒントの表示 65
オンライン ヘルプの表示 67
ドキュメントのマニュアル選択メニューによる検索 69

索引 73

第 1 章: 紹介

このセクションには、以下のトピックが含まれています。

本書の内容 (P. 7)
CA User Activity Reporting Module について (P. 8)

本書の内容

この「概要ガイド」では、*CA User Activity Reporting Module について紹介します。まず、製品をすぐに実際に体験できるクイック チュートリアルから始めます。最初のチュートリアルでは、シングル サーバの CA Enterprise Log Manager の運用を開始し、隣接するネットワークの UNIX デバイスから収集された syslog を表示する手順を説明します。2 番目のチュートリアルでは、Windows オペレーティング システムにエージェントをインストールし、ログ収集を設定し、結果として生成されるイベント ログを表示する手順を説明します。その後、主な機能や、詳細な手順を学習する方法について説明します。このガイドはすべてのユーザを対象としています。*

内容の概要は以下のとおりです。

セクション	説明内容
CA Enterprise Log Manager について	現在のネットワーク環境に CA User Activity Reporting Module を統合する方法
クイック スタート展開	シングル サーバ システムをインストールする方法、syslog イベント ソースを設定する方法、デフォルト エージェント用の syslog コネクタを更新する方法、精製済みイベントを表示する方法
Windows エージェント展開	エージェントのインストールを準備する方法、Windows オペレーティング システム用のエージェントをインストールする方法、エージェントベースの収集用の 1 つのコネクタを設定する方法、イベント ソースを更新する方法、生成されたイベントを表示する方法
主な機能	ログ収集、ログ ストレージ、コンプライアンス レポートおよびアラートなど、主な機能の利点

セクション	説明内容
CA User Activity Reporting Module の詳細情報	ツールヒント、オンライン ヘルプ、およびドキュメント マニュアル選択メニューに関して必要な情報

注: オペレーティング システムのサポートまたはシステム要件の詳細については、「リリース ノート」を参照してください。*CA User Activity Reporting Module のインストールおよび初期設定の実行についての詳細な手順については、「実装ガイド」を参照してください。*エージェントのインストールの詳細については、「エージェント インストール ガイド」を参照してください。*製品の使用および保守の詳細については、「管理ガイド」を参照してください。*CA User Activity Reporting Module ページの使用方法については、オンライン ヘルプを参照してください。

CA User Activity Reporting Module について

CA User Activity Reporting Module は、IT のコンプライアンスおよび保証に重点的に取り組んでいます。 これを使用することによって、IT アクティビティを収集し、標準化し、集約して報告し、コンプライアンス違反が発生した場合にアクションを必要とするアラートを生成することができます。異なるセキュリティ デバイスおよびセキュリティ以外のデバイスからデータを収集できます。

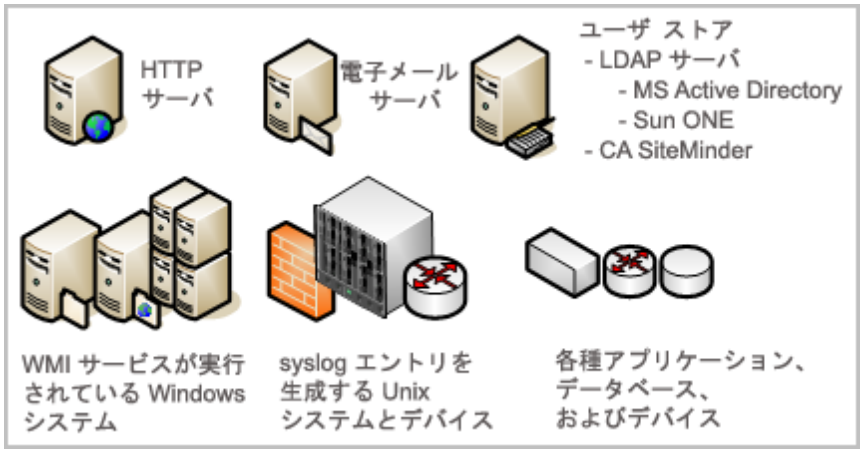
ネットワーク -- インストール前

米国の連邦規制および指令では、ログ レコード管理が義務付けられています。これに従うために、以下のことを行う必要があります。

- 監査の際にログを確認できるようにする。
- ログを長期間保存する。
- 要求に応じてログを復元する。

ログ レコードの管理が困難となるのは、その数の多さ、その場所、およびその一時的な性質のためです。ログは、ユーザおよびソフトウェアのプロセス アクティビティによって絶えず生成されています。生成の速さは 1 秒あたりのイベント数（eps）で測定されます。元のイベントは、ネットワーク内のあらゆるアクティブなシステム、データベース、およびアプリケーション上に記録されます。ログ レコードが上書きされる前に、各イベント ソースで保存のためのログ レコードのバックアップを行う必要があります。さまざまなイベント ソースからのバックアップが別々の場所に保存されていると、イベント ログの復元が困難となります。

元のイベントの解釈が煩雑になるのは、イベントの重大度がわかりにくい文字列形式のためです。さらに、各種システムからの類似のデータがシステムによって異なることもその原因となります。



運用の効率性を高めるには、すべてのログを統合し、ログを読みやすくし、ストレージへのアーカイブを自動化し、ログの復元を簡略化するソリューションが必要です。CA User Activity Reporting Module には、これらの利点が備わっており、クリティカルなイベントが発生した場合に個人とシステムにアラートを送ることが可能です。

インストール内容

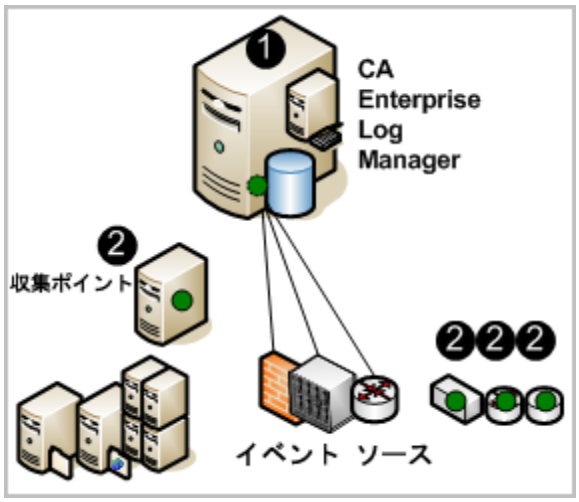
シングル サーバ ソリューションをセットアップし、イベントを収集し始めるのに多くの時間はかかりません。

インストール ディスクには、以下のコンポーネントが含まれています。

- ソフトウェア アプライアンス用オペレーティング システム（Red Hat Enterprise Linux）
- CA User Activity Reporting Module サーバ
- CA User Activity Reporting Module エージェント（以下「エージェント」と呼びます）

次の図では、CA User Activity Reporting Module は、小さいサーバ、濃い（緑色の）円、およびデータベースを含むサーバとして示されています。小さいサーバは、アプリケーション レベルのコンテンツを格納するローカル リポジトリを表します。濃い円はデフォルト エージェントを表し、データベースはイベント ログ ストアを表します。このイベント ログ ストアでは、クエリやレポートに使用できるよう、受信イベント ログが処理されます。

収集ポイントおよび他のイベント ソース上の濃い（緑色の）円は、別々にインストールされたエージェントを表します。エージェントのインストールはオプションです。必須の設定を完了した後、デフォルト エージェントを使用して UNIX 互換のイベント ソースから syslog を収集できます。



図の番号は、次のステップを示しています。

1. ソフトウェア アプライアンス用のオペレーティング システムをインストールし、次に CA User Activity Reporting Module アプリケーションをインストールします。CA User Activity Reporting Module に syslog がプッシュされるようにソースを設定し、デフォルト エージェントのコネクタ設定で syslog ターゲットを指定するとすぐに、syslog が収集され、処理しやすい形に精製されます。
2. (オプション) エージェントは、収集ポイントとして指定したホストにインストールするか、収集するイベントを生成するソースが存在するホストに直接インストールできます。

注: ソフトウェア アプライアンスのインストールの詳細については、「実装ガイド」*を参照してください。エージェントのインストールの詳細については、「エージェント インストール ガイド」を参照してください。*

詳細情報:

エージェントのインストール (P. 41)

第 2 章: クイック スタート展開

このセクションには、以下のトピックが含まれています。

クイック スタートの概要 (P. 13)
シングル サーバ システムのインストール (P. 14)
Windows の hosts ファイルの更新 (P. 21)
最初の管理者の設定 (P. 21)
Syslog イベント ソースの設定 (P. 25)
Syslog コネクタの編集 (P. 28)
Syslog イベントの表示 (P. 31)

クイック スタートの概要

1 つのソフトウェア アプライアンスを使用して、簡単で機能的な CA User Activity Reporting Module 展開を実現できます。定義済み syslog コネクタを使用することで、デフォルト エージェントが、生成された syslog イベントを受信することが可能になります。必要なのは、CA User Activity Reporting Module に syslog イベントをプッシュするように syslog ソースを設定し、syslog ターゲットを識別するように syslog コネクタ設定を編集することだけです。受信される内容は、サーバと syslog ソースの間の帯域幅、および遅延時間によって異なります

WinRM と ODBC を含むログ センサは、20 種類以上の syslog 以外のイベント ソースから直接ログを収集できます。WinRM ログ センサでは、Forefront Security for Exchange Server、Forefront Security for SharePoint Server、Microsoft Office Communication Server、Active Directory 証明書サービスなどで利用される Hyper-V 仮想化サーバなど、Windows オペレーティング システムを実行しているサーバから直接イベントを収集できます。ODBC ログ センサは、Oracle9i または SQL Server 2005 のデータベースで生成されたイベントのキャプチャが可能です。詳細については、CA Enterprise Log Manager 製品統合マトリクスを参照してください。

CA User Activity Reporting Module をインストールするには、EiamAdmin 認証情報が必要です。EiamAdmin スーパーユーザとして、設定に使用する管理者アカウントを設定します。管理者認証情報でログオンした場合、自己監視イベントを表示することで、セットアップが正常に実行されていることを確認できます。

シングル サーバ システムのインストール

照会したイベントを表示できる最もシンプルな導入環境は、シングル サーバ システムです。必ず、CA User Activity Reporting Module ソフトウェア アプライアンスの最小ハードウェア要件以上のマシンを選択します。

注: 認定されたハードウェア リスト、オペレーティング システムのサポート、およびシステム ソフトウェアとサービスの要件については、「リリース ノート」を参照してください。

シングル サーバ システムに CA User Activity Reporting Module をインストールする方法

1. 次の情報を用意します。
   - root パスワードとして使用するパスワード
   - アプライアンスのホスト名
   - DHCP を使用していない場合は、アプライアンスの静的 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ
   - アプライアンスのドメイン

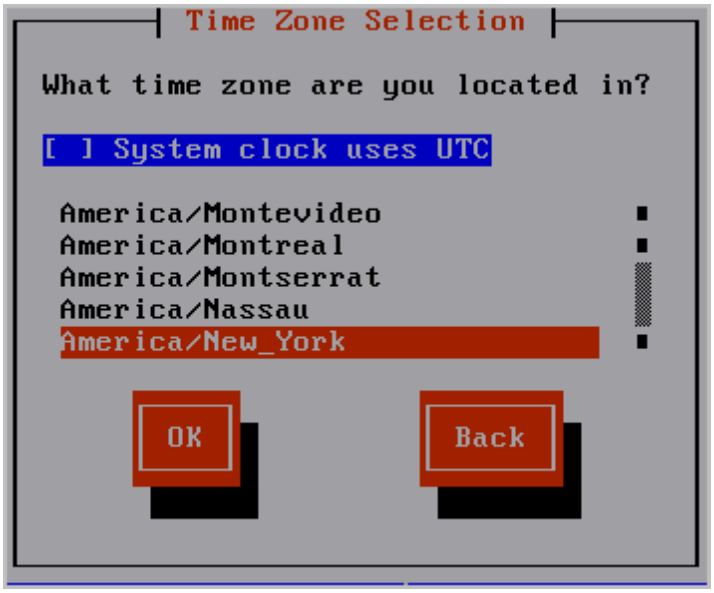
     注: インストールを完了するには、ネットワークの DNS サーバにドメインを登録する必要があります。
   - DNS サーバの IP アドレス
   - (オプション) NTP タイム サーバの IP アドレス
   - デフォルト インストールのスーパーユーザ名 EiamAdmin のパスワード
   - CAELM

     これは、CA User Activity Reporting Module アプリケーションのデフォルト アプリケーション名です。

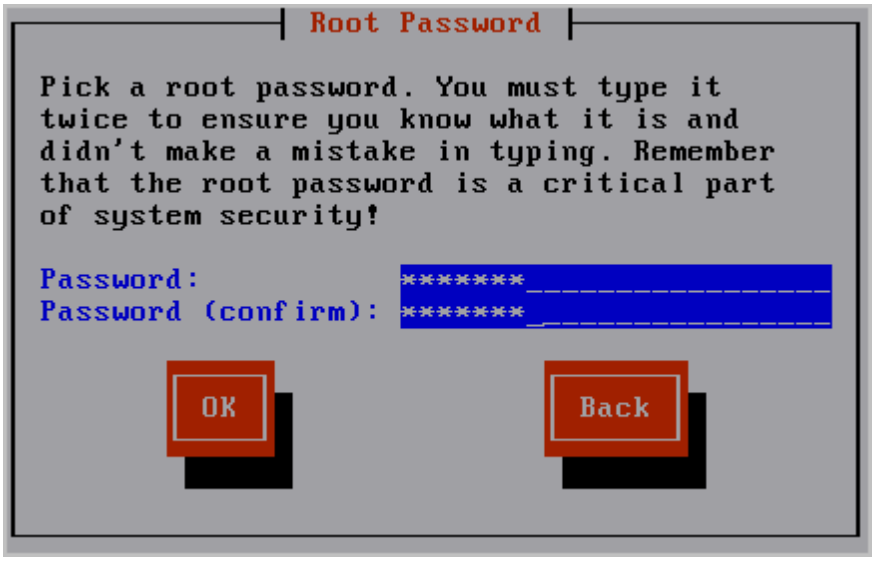
2. CA User Activity Reporting Module ダウンロード パッケージから作成したメディアを使用して、あらかじめ設定されたオペレーティング システムをインストールします。オペレーティング システム インストール中に、以下を実行します。

   a. キーボード配列を選択します。デフォルトは英語キーボード配列(US)です。

   b. タイム ゾーン(たとえば、アメリカ/ニューヨークなど)を選択し、[OK]を選択します。



   c. root パスワードとして使用するパスワードを入力し、再入力して確認します。[OK]を選択します。



インストールの進捗状況が表示されます。

d. オペレーティング システムのインストール ディスクを取り出し、Enter キーを押してシステムを再起動します。

システムが再起動し、非対話型のスタートアップ画面が表示されます。インストールの進捗状況を示すメッセージが表示されます。このインストールに関する詳細情報は、/tmp/PRE-install_ca-elm.log ファイルに保存されます。

以下のプロンプトが表示されます。

CA Enterprise Log Manager r12 - アプリケーション インストール ディスクを挿入し、Enter キーを押してください。

3. CA User Activity Reporting Module アプリケーション ディスクを挿入します。Enter キーを押します。

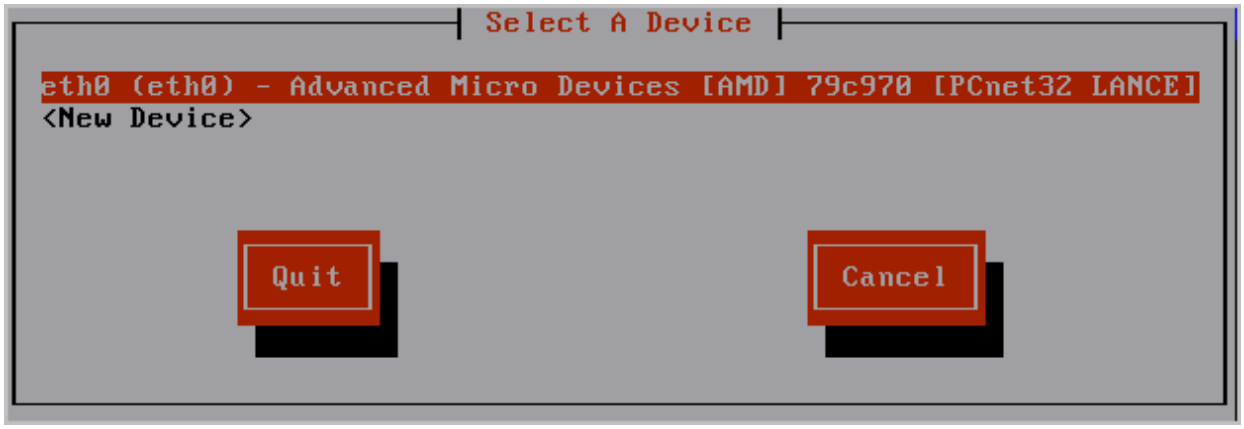
最適なパフォーマンスを得るために推奨される最小仕様を、システムが満たしているかどうかが確認されます。満たさない場合、インストール プロセスを停止するかどうかを確認するプロンプトが表示されます。

以下のプロンプトが表示されます。

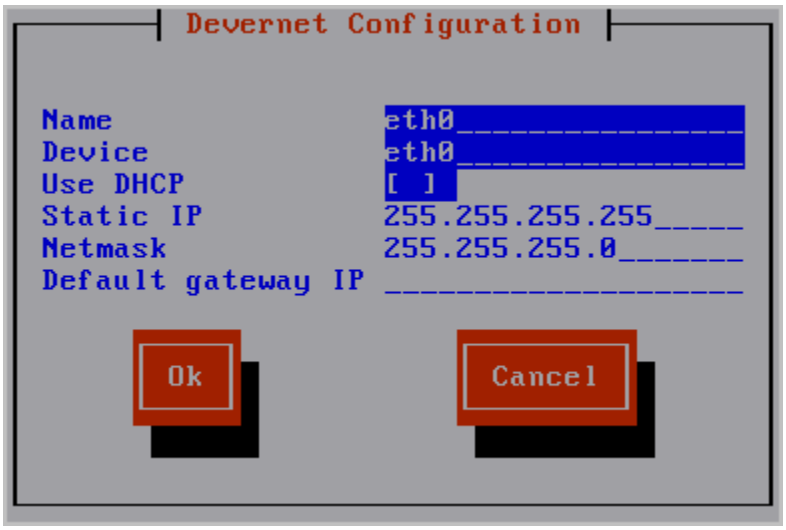
新しいホスト名を入力してください:

4. この CA User Activity Reporting Module ソフトウェア アプライアンスのホスト名を入力します。たとえば、「CALM1」と入力します。

5. デフォルト デバイス eth0 を受け入れます。Enter キーを押して次の画面に移動します。



6. 以下のいずれかを実行し、[OK]を選択します。
   - [DHCP を使用](スタンド アロンのテスト システムにのみ使用可能なオプション)を選択します。
   - 入力したホスト名に関連付ける静的 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイ IP アドレスを入力します。



ネットワーク サービスが新しい設定で再起動され、それらの設定が表示されます。

以下のメッセージが表示されます。

ネットワーク設定を変更しますか? (n):

7. ネットワーク設定を確認します。問題ない場合は、ネットワーク設定を変更できることを示すメッセージが表示されたら、「n」と入力するか Enter キーを押します。

   以下のメッセージが表示されます。

   このシステムのドメイン名を入力してください。

8. <yourcompany>.com のようなドメイン名を入力します。

   以下のメッセージが表示されます。

   使用する DNS サーバのリストをカンマで区切って入力してください:

9. 内部 DNS サーバの IP アドレスを、スペースを入れずにカンマで区切って入力します。

   次のメッセージと共にシステムの日付と時刻が表示されます。

   システムの日付と時刻を変更しますか? (n):

10. 表示されたシステムの日付と時刻を確認します。問題ない場合は、「n」と入力するか Enter キーを押します。

    以下のメッセージが表示されます。

    システムを設定して、NTP 経由で時刻を更新しますか?

11. Network Time Protocol (NTP) サーバを使用する場合は、以下のように続けます。あるいは、「no」と指定して次の手順に進みます。

    a. メッセージに「yes」と応答します。

       「yes」を指定した場合、次のメッセージが表示されます。

       NTP サーバ名または IP アドレスを入力してください

    b. NTP サーバのホスト名または IP アドレスを入力します。

       「システムは、<yourntpserver> にある NTP サーバを使用して午前 0 時に時刻を更新するように設定されています」というような確認メッセージが表示されます。

12. 表示されたエンド ユーザ使用許諾契約(EULA)を読み、次のように応答します。

    a. Sun Java Development Kit(JDK)の EULA を読みます。

       EULA の末尾に、以下のメッセージが表示されます。

       使用許諾契約書の条項に同意しますか? [はい/いいえ]:

    b. 条件に同意する場合は、「yes」と入力します。

       次のメッセージの後に製品登録情報が表示されます。

       Enter キーを押して続行します...

    c. Enter キーを押します。

       メッセージは、CA User Activity Reporting Module のインストールの準備中に、システム設定が設定されることを示しています。CA エンド ユーザ使用許諾契約が表示されます。

    d. CA EULA を読みます。

       ライセンスの末尾に、以下のメッセージが表示されます。

       使用許諾契約書の条項に同意しますか? [はい/いいえ]:

    e. 条件に同意する場合は、「yes」と入力します。

       CA EEM サーバ情報が表示されます。

13. 次のプロンプトに応答し、CA EEM を設定します。

    ローカルまたはリモートの EEM サーバを使用しますか?
    「l」(ローカル)または「r」(リモート)を入力してください:

    a. スタンドアロンのテスト システムを作成するには、ローカルを示す「l」を入力します。

       EEM サーバの EiamAdmin ユーザのパスワードを入力します。
       EEM サーバの EiamAdmin ユーザのパスワードを確認します。

    b. EiamAdmin デフォルト スーパーユーザに割り当てるパスワードを入力します、再度入力します。

       この CAELM サーバ(CAELM)のアプリケーション名を入力します。

c. Enter キーを押して、CAELM（CA User Activity Reporting Module のデフォルト アプリケーション名）を受け入れます。

これまでに入力した EEM サーバ情報が、変更するかどうかを尋ねるメッセージと共に表示されます。

```
EEM server is not installed on the local host.

EEM Server Information:
EEM Server Type - l (local) or r (remote): l
EEM Server Name: CALM1
EEM application name for this CAELM server: CAELM
Do you want to change the EEM Server information? (n): _
```

d. Enter キーを押すか、「n」と入力して、入力した CA EEM サーバ情報を受け入れます。

インストール プロセスが開始します。各 CA User Activity Reporting Module コンポーネントの正常なインストール、登録の完了、証明書の取得、ファイルのインポート、およびコンポーネントの設定について、進捗状況を示すメッセージが表示されます。CA ELM のインストールの成功を示すメッセージが表示されます。インストールが完了すると、システムにコンソール ログオン アドレスが表示されます。

14. 以下のプロンプトに応答します。

```
Do you want to run CAELM Server in FIPS mode?
「YES」または「NO」と入力します。
```

y と入力すると CA User Activity Reporting Module サーバは FIPS モードで起動します。n と入力すると、CA User Activity Reporting Module サーバは FIPS 非準拠モードで起動します。

15. このアドレスを書き留めます。これは、この CA User Activity Reporting Module サーバにアクセスするブラウザで入力するアドレスです。つまり、https://<hostname>:5250/spin/calm です。

<hostname> のログイン プロンプトが表示されます。これは無視してもかまいません。

注: 何らかの理由で、このログイン プロンプトからオペレーティング システム プロンプトを表示する場合、caelmadmin とデフォルトのパスワード（EiamAdmin ユーザ アカウントに割り当てたパスワード）を入力することで表示できます。caelmadmin アカウントを使用すると、コンソールまたは SSH 経由でアプライアンスにログインできます。

16. 以下のように続けます。
    - 静的 IP アドレスを設定した場合、必ず手順 9 で指定した DNS サーバにこの IP アドレスを登録します。
    - DHCP を設定した場合は、このサーバの参照に使用するマシン上の hosts ファイルを更新します。
    - 手順 14 で書き留めた URL を参照し、最初の管理者を設定します。

Windows の hosts ファイルの更新

CA User Activity Reporting Module のインストール時に、1 つ以上の DNS サーバを識別するか、[DHCP を使用]を選択できます。DHCP を選択した場合、ブラウザを使用して CA User Activity Reporting Module にアクセスするコンピュータで、Windows の hosts ファイルを更新する必要があります。

ブラウザを使用してホスト上の hosts ファイルを更新する方法

1. Windows エクスプローラを開き、C:¥WINDOWS¥system32¥drivers¥etc に移動します。
2. メモ帳などのエディタを使用して hosts ファイルを開きます。
3. CA User Activity Reporting Module サーバの IP アドレスと対応するホスト名を含むエントリを追加します。
4. [ファイル]メニューから[保存]を選択し、ファイルを閉じます。

最初の管理者の設定

シングル サーバの CA User Activity Reporting Module をインストールしたら、リモート ワークステーションから CA User Activity Reporting Module の URL に参照してログオンし、設定の実行に使用可能な管理者アカウントを作成することで、設定を準備します。

注: このクイック スタート展開では、デフォルトのユーザ ストアおよびデフォルトのパスワードポリシーを使用します。通常、これらは最初の管理者を追加する前に設定します。

最初の管理者を設定する方法

1. ブラウザからの次の URL に接続します。hostname は、CA User Activity Reporting Module をインストールしたサーバのホスト名または IP アドレスです。

   ```
   https://<hostname>:5250/spin/calm
   ```

2. セキュリティ アラートが表示された場合は、以下の作業を行います。

   a. [証明書の表示]をクリックします。

   b. [証明書のインストール]をクリックし、デフォルト値を受け入れて、インポート ウィザードを完了します。

      CA User Activity Reporting Module サーバのホスト名を表すと主張する証明書がインストールされることを示す、セキュリティ警告が表示されます。

   c. [はい]をクリックします。

      ルート証明書がインストールされ、インポート成功メッセージが表示されます。

   d. [OK]をクリックします。

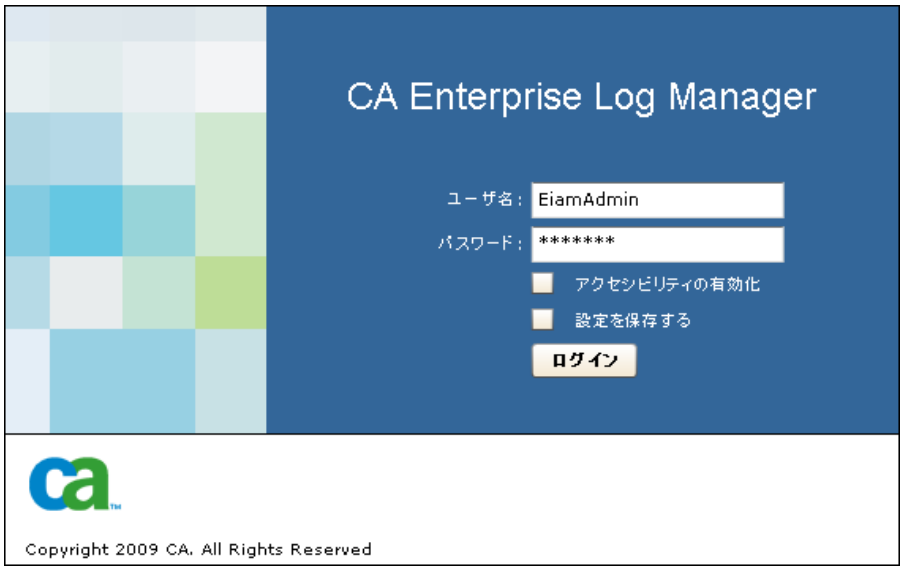
      [トラステッド証明書]ダイアログ ボックスが表示されます。

   e. (オプション) [証明書パス]をクリックし、証明書ステータスにこの証明書が OK であると示されていることを確認します。

   f. [OK]をクリックし、[はい]をクリックします。

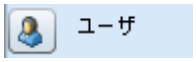
      ログオン ページが表示されます。

3. ソフトウェアのインストール時に作成した EiamAdmin のユーザ名およびパスワードでログオンします。[ログイン]をクリックします。

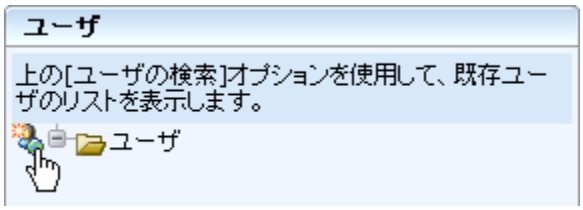


アプリケーションでは、最初は[管理者]タブと[ユーザとアクセスの管理]サブタブのみがアクティブになっています。

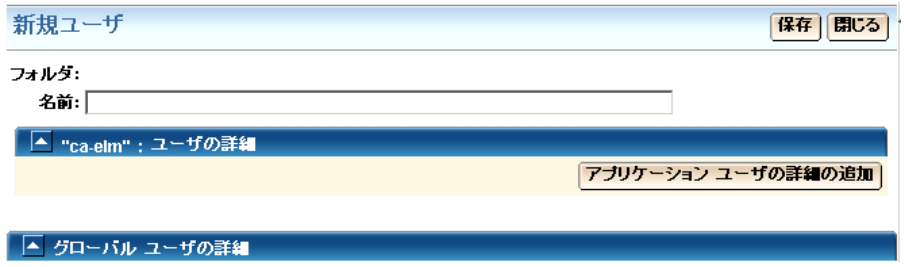
4. [ユーザ]をクリックします。



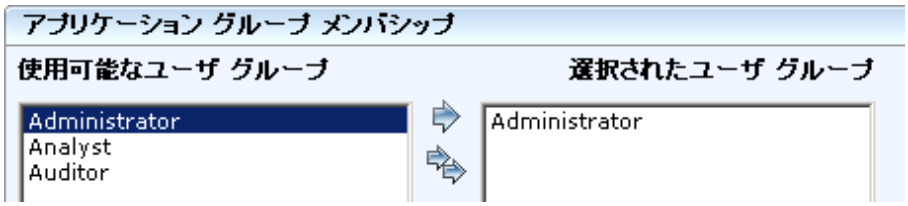
5. [新規ユーザの追加]をクリックします。



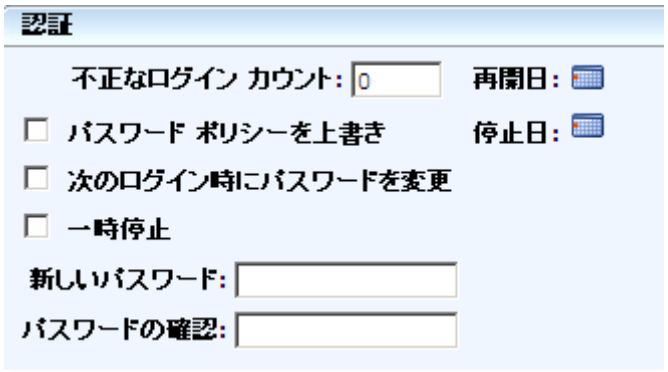
6. [名前]フィールドに名前を入力し、[アプリケーション ユーザの詳細の追加]をクリックします。



7. [管理者]を選択し、[選択されたユーザ グループ]に移動します。



8. [認証]の下で、入力用と確認用の 2 つのフィールドにこの新規アカウントのパスワードを入力します。



9. [保存]をクリックし、[閉じる]をクリックします。[閉じる]をクリックします。

10. ツールバーの[ログアウト]リンクをクリックします。

    ログオン ページが表示されます。

11. ここで定義した管理者認証情報で CA User Activity Reporting Module に再度ログインします。

    すべての機能が有効になって CA User Activity Reporting Module が開きます。[クエリおよびレポート]タブと[クエリ]サブタブが表示されます。

12. (オプション) 次のようにして、ログイン試行を表示します。

    a. クエリ タグ リストから[システム アクセス]を選択します。

    b. クエリ リストから[システム アクセスの詳細]を選択します。

    クエリ結果に 2 つのログイン試行が表示されます。1 つ目は EiamAdmin としてのログイン試行で、ログイン試行に成功した場合は「S」というマークが付いて管理者名が表示されます。

CA 重大度	日付	アカウント	実行ユ...	ホスト	ログ名	カテゴリ	アクション	結果
情報	2009-11-20 金曜日 午後 2:20:15	admin	admin	etr851l1-blade12	CALM	System Access	Login Attempt	S
情報	2009-11-20 金曜日 午後 2:18:42	admin	admin	etr851l1-blade12	CALM	System Access	Login Attempt	S
情報	2009-11-20 金曜日 午後 2:09:42	admin	admin	etr851l1-blade12	CALM	System Access	Login Attempt	S
情報	2009-11-20 金曜日 午後 2:09:36	song	song	etr851l1-blade12	CALM	System Access	Login Attempt	F

Syslog イベント ソースの設定

各 CA User Activity Reporting Module サーバに存在するデフォルト エージェントによって syslog イベントを直接収集できるようにするには、まずイベントの収集元に使用する syslog イベント ソースを特定して、関連する統合を決定します。その後、次の 2 つの操作を実行します（順序はどちらでもかまいません）。

- syslog イベント ソースを設定します。 syslog イベント ソースが実行されている各ホストにログオンし、コネクタ ガイドで説明されているとおりにその syslog 統合を設定します。
- デフォルト エージェントで syslog コネクタを設定し、設定されたイベント ソースに関連付けられたターゲットの syslog 統合を追加します。

この 2 段階の設定を完了するとすぐに、イベント収集と精製が開始されます。その後、CA User Activity Reporting Module を使用して、管理対象のイベントを標準化された形式で表示またはレポートできます。さらに、特定のイベントが発生したときにアラートを生成することもできます。

選択された syslog イベント ソースを設定する方法

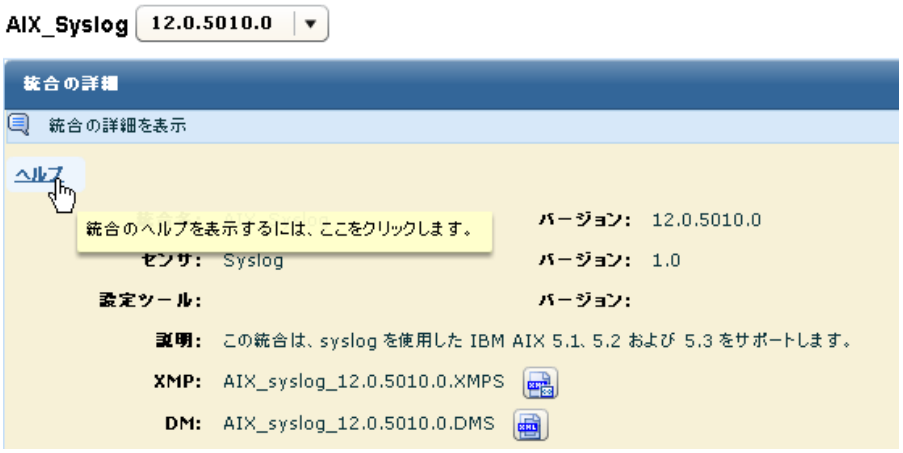
1. ターゲットの syslog イベント ソースが存在するホストにログオンします。
2. このホストのブラウザから CA User Activity Reporting Module を起動します。
3. [管理]タブおよび[ログ収集]サブタブをクリックします。

   ログ収集エクスプローラが表示されます。
4. [イベント精製ライブラリ]、[統合]、[サブスクリプション]を展開します。

   定義済み統合のリストが表示されます。 簡単な例を次に示します。

5. 設定する必要があるイベント ソースの統合を選択します。たとえば、AIX オペレーティング システムにより生成される syslog を収集する場合は、AIX_Syslog を選択します。

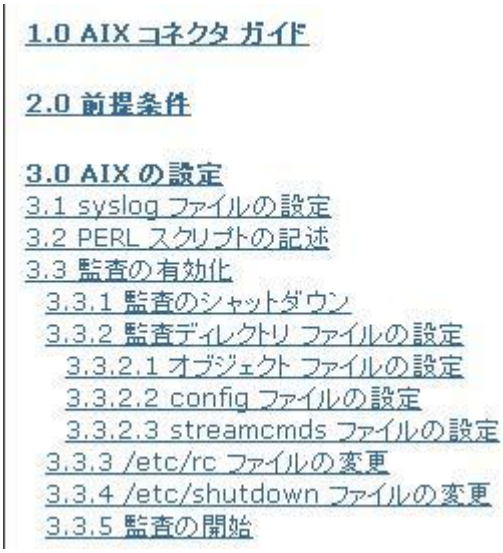
   統合の詳細が表示されます。



6. 右側ペインの統合名のすぐ上にある[ヘルプ]ボタンをクリックします。

   選択した統合のコネクタ ガイドが表示されます。

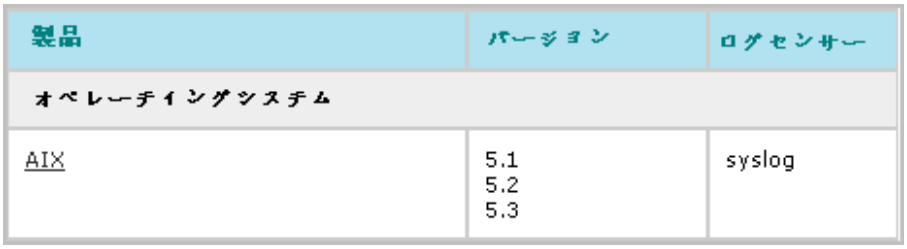
7. イベント ソースの設定要件についてのセクションをクリックします。この例では、AIX オペレーティング システムのイベント ソースを設定して、その syslog を CA User Activity Reporting Module に送信する方法がドキュメントで説明されています。



例 -- コネクタ ガイドの代替ソース: Support Online

選択したコネクタ ガイドは、CA User Activity Reporting Module ユーザ インターフェース内または CA Support Online から開くことができます。この代替ソースからコネクタ ガイドを開く方法を以下の例に示します。

1. CA Support Online にログオンします。
2. [製品の選択]ページのドロップダウン リストから[CA Enterprise Log Manager]を選択します。
3. [製品のステータス]までスクロールし、[CA Enterprise Log Manager の証明書マトリクス]を選択します。
4. [製品統合マトリクス]を選択します。
5. 設定しているイベント ソースに関連付けられた統合のカテゴリを見つけます。たとえば、イベント ソースが AIX オペレーティング システムである場合は、[オペレーティング システム]カテゴリまでスクロールし、[AIX]リンクをクリックします。



製品	バージョン	ログセンサー
オペレーティングシステム		
AIX	5.1 5.2 5.3	syslog

Syslog コネクタの編集

CA User Activity Reporting Module には、それぞれデフォルト エージェントがあります。CA User Activity Reporting Module がインストールされると、そのデフォルト エージェントには Syslog_Connector と呼ばれる部分的に設定されたコネクタが付与されます。これは、リスナである Syslog に基づいています。CA User Activity Reporting Module に syslog が送信されるようにイベント ソースを設定するとすぐ、このリスナはデフォルト ポートに関する元の syslog イベントを受信します。ただし、CA User Activity Reporting Module でこれらの元のイベントを精製するには、この Syslog_Connector を編集する必要があります。必須の編集とオプションの編集があります。

- このコネクタを編集するには、syslog ターゲットを識別する必要があります。syslog ターゲットとして、設定した、または設定する予定の 1 つ以上のイベント ソースに対応する各統合を選択します。syslog ターゲットを識別することで、CA User Activity Reporting Module が正しくイベントを精製できます。
- オプションで、抑制ルールの適用、トラステッドホストへの syslog の受け入れの制限、Well-Known syslog UDP ポートの 514 およびデフォルト TCP ポートである 1468 以外の待機ポートの指定、トラステッドホストの新しいタイムゾーンの追加を行うことができます。

デフォルト エージェントの syslog コネクタを編集する方法

1. [管理]タブをクリックします。

   [ログ収集]サブタブが表示されます。

2. [エージェント エクスプローラ]を展開し、次に、[デフォルトのエージェント グループ]または設定する CA User Activity Reporting Module が存在するユーザ定義グループを展開します。

3. CA User Activity Reporting Module サーバの名前を選択します。

   Syslog_Connector という名のコネクタが表示されます。

4. [編集]をクリックします。

   [コネクタの詳細]ステップが選択された状態で、[コネクタの編集]ウィザードが表示されます。

5. (オプション)[抑制ルールの適用]をクリックします。いずれかの syslog イベント タイプを抑制する(つまり収集しない)*場合、そのイベント タイプを使用可能リストから選択済みリストに移動します。移動するイベントを選択して、移動ボタンをクリックします。*

6. [コネクタの設定]ステップをクリックします。

   使用可能なすべての統合がデフォルトで選択されます。

7. ターゲットにする syslog 統合を使用可能リストから選択済みリストに移動することにより、syslog ターゲットを選択します。

   たとえば、ネットワーク上のホストの AIX オペレーティング システムを設定した場合、syslog ターゲット(AIX_Syslog)を使用可能リストから選択済みリストに移動します。

8. (オプション) syslog コネクタが受信イベントを受け入れる、トラステッドホストを特定します。入力フィールドに IP アドレスを入力し、[追加]をクリックします。トラステッドホストごとに繰り返します。その後、トラステッドホストとして設定されていないホストからイベントを受信すると、そのイベントは拒否されます。

   注: トラステッドホストを設定することをお勧めします。通常、CA User Activity Reporting Module に syslog を送信するようにイベント ソースを設定したすべてのホストを設定します。トラステッドホストを指定すると、攻撃者が syslog リスナにイベントを送信するように設定した悪質なシステムからのイベントをデフォルト エージェントが受け入れなくなります。

9. （オプション）ポートを追加します。

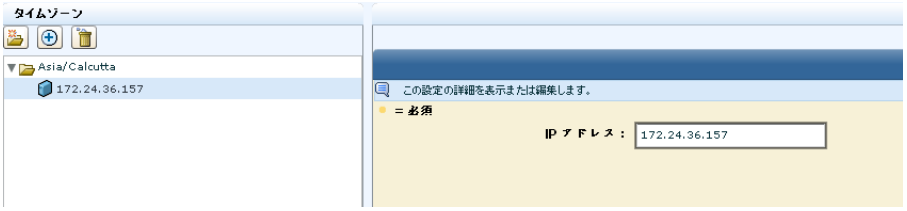
   通常は、デフォルト エージェントのデフォルト UPD および TCP ポートを受け入れることができます。

   注: さまざまなイベント タイプの syslog コネクタを定義し、それぞれに別のポートを指定することで、パフォーマンスが向上します。新しいポートを割り当てる場合は、必ず未使用のポートを選択してください。

10. （オプション）ソフトウェア アプライアンスとは異なるタイム ゾーンのマシンから syslog を収集する場合のみ、タイム ゾーンを追加します。

    a. ［フォルダの作成］をクリックし、フォルダを展開します。

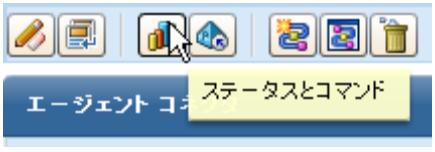
    b. フォルダの下にある空白のエントリを強調表示します。このコネクタに設定したトラステッドホスト、または CA User Activity Reporting Module のインストールで指定した NTP タイム サーバのいずれかの IP アドレスを入力します。



11. ［保存して閉じる］をクリックします。

12. ステータスを表示します。

    a. ［ステータスとコマンド］をクリックします。



[エージェントのステータス表示]が選択されます。デフォルト エージェントはこのサーバ上にあるため、インストールしたサーバのホスト名が[エージェント]列に表示されます。ステータスは[実行中]と表示されます。

b. 詳細を表示するには、[実行中]リンクをクリックします。

c. コネクタのステータスを表示するには、[コネクタ]ボタンをクリックします。

d. [実行中]リンクをクリックします。

CPU 使用率、メモリ使用量、1 秒あたりの平均イベント数(EPS)、およびフィルタされたイベント数が表示されます。

Syslog イベントの表示

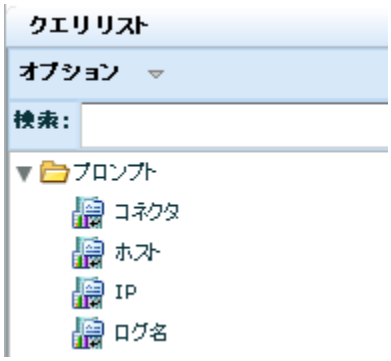
syslog リスナによって収集されたイベントのクエリ結果をすばやく表示する方法の 1 つは、ホストのプロンプトを使用する方法です。

syslog イベントを表示する方法

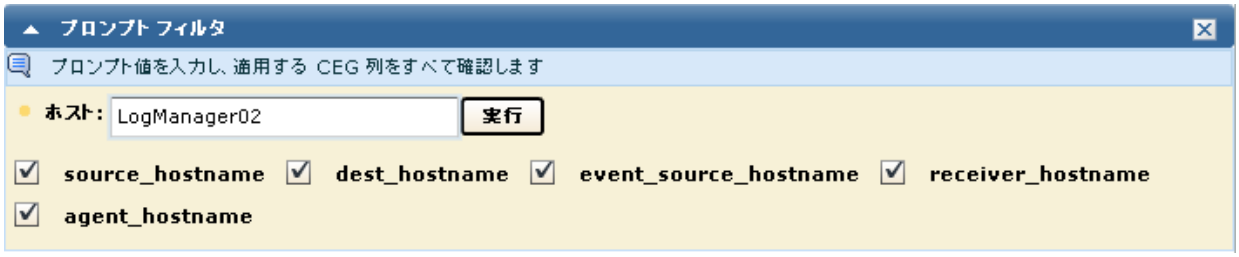
1. [クエリおよびレポート]タブを選択します。

   [クエリ]サブタブが表示されます。

2. [クエリ リスト]の下の[プロンプト]を展開し、[ホスト]を選択します。



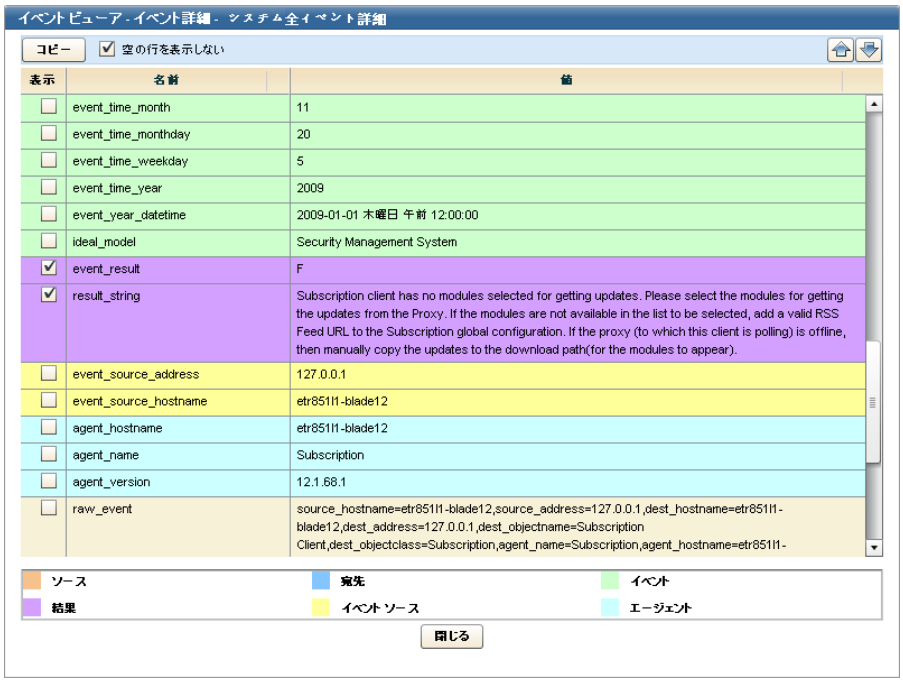
3. デフォルト エージェントによって収集されたイベントのクエリを送信します。
   a. [ホスト]フィールドに、デフォルト エージェント ホスト名 (このエージェントが存在する CA User Activity Reporting Module の名前でもあります) を入力します。
   b. agent_hostname を選択します。
   c. [実行]をクリックします。



4. 検証する結果を表示します。
   a. [結果]列をクリックして、結果別に並べ替えます。
   b. 失敗を表す F の最初の結果までスクロールします。これは、カテゴリ「設定管理」の設定の警告であるとします。
   c. 行をダブルクリックして選択し、詳細を表示します。

   イベント ビューアが表示されます。

5. ［結果］が表示される領域にスクロールします。この例では、エラーはサブスクリプション モジュールを設定する必要があるという警告です。 この警告は、インストールするすべての CA User Activity Reporting Module サーバのインストールが終了するまで無視してください。



第 3 章: Windows エージェント展開

このセクションには、以下のトピックが含まれています。

エージェントのユーザ アカウントの作成 (P. 36)
エージェント認証キーの設定 (P. 38)
エージェント インストール プログラムのダウンロード (P. 39)
エージェントのインストール (P. 41)
NTEventLog に基づいたコネクタの作成 (P. 43)
Windows イベント ソースの設定 (P. 48)
Windows イベント ソースからのログの表示 (P. 48)

エージェントのユーザ アカウントの作成

Windows オペレーティング システムにエージェントをインストールする前に、[Windows ユーザー]フォルダにエージェントの新規アカウントを作成します。このとき、できるだけ低い権限でエージェントを実行できるようにするため、エージェントに権限レベルの低いアカウントを作成します。エージェントをインストールする際には、ここで作成するユーザ名およびパスワードを指定します。

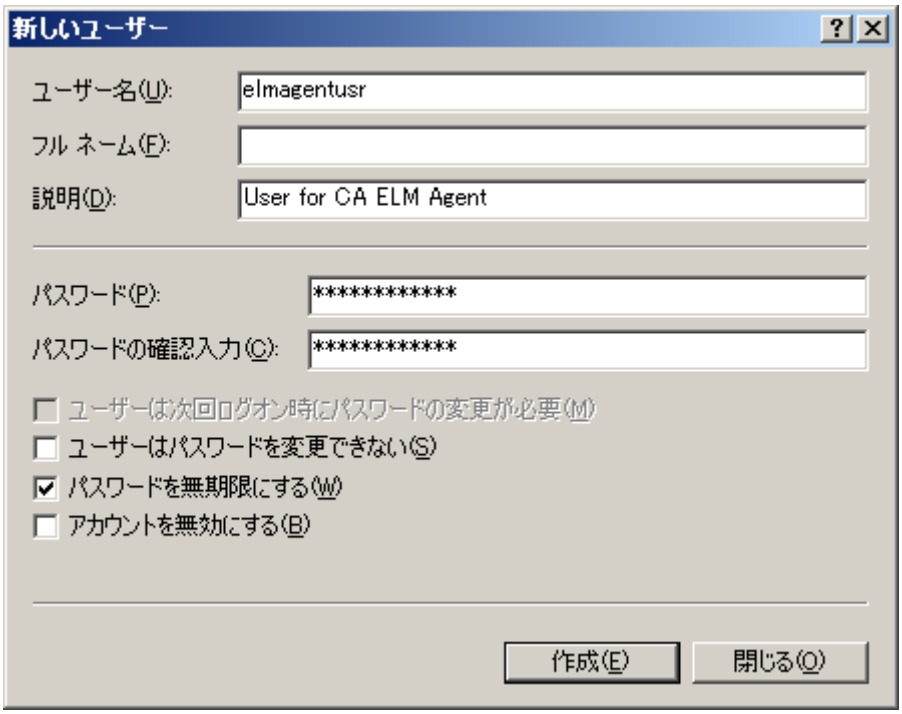
注: インストール時にこの手順を省略して、エージェントに管理者のドメイン認証情報を指定できますが、お勧めしません。

エージェントの Windows ユーザ アカウントを作成する方法

1. エージェントをインストールするホストにログオンします。管理用の認証情報を使用します。
2. [スタート]、[プログラム]、[管理ツール]、[コンピュータの管理]をクリックします。
3. [ローカル ユーザーとグループ]を展開します。
4. [ユーザー]を右クリックし、[新しいユーザー]を選択します。

   Windows の[新しいユーザー]ダイアログ ボックスが表示されます。
5. ユーザ名を入力し、パスワードを 2 回入力します。アルファベット、数字、および特殊文字を組み合わせると、強力なパスワードになります。たとえば、calmr12_agent などです。任意で説明を入力します。

   重要: この名前とパスワードを記憶するか、記録します。エージェントのインストール時に入力する必要があります。



6. ［Create］をクリックします。［閉じる］をクリックします。

詳細情報:

エージェントのインストール (P. 41)

エージェント認証キーの設定

最初のエージェントをインストールするには、エージェント認証キーを知っている必要があります。 キーが設定されていない場合はデフォルトのキーを使用でき、設定されている場合は現在のキーを使用できます。または、新しいキーを設定できます。ここで設定するエージェント認証キーは、各エージェントのインストール時に入力する必要があります。Administrator のみがこのタスクを実行できます。

エージェント認証キーを設定する方法

1. エージェントをインストールするホストでブラウザを開き、このエージェントの CA User Activity Reporting Module サーバの URL を入力します。以下に例を示します。

   ```
   https://<IP address>:5250/spin/calm/
   ```

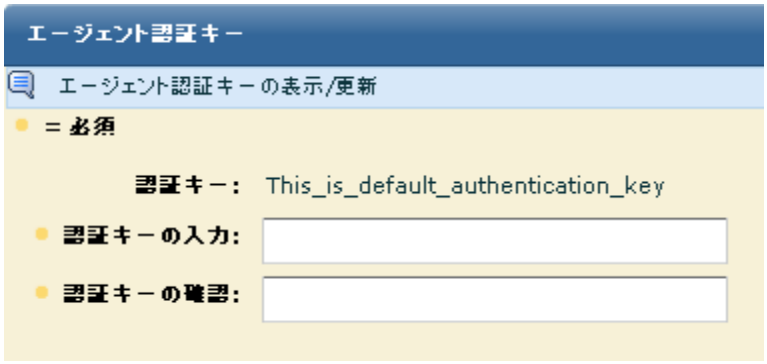
2. CA User Activity Reporting Module にログオンします。ユーザ名とパスワードを入力し、[ログオン]をクリックします。
3. [管理]タブをクリックします。

   左側ペインに、ログ収集エクスプローラが表示されます。
4. [エージェント エクスプローラ]フォルダを選択します。

   ツールバーがメイン ペインに表示されます。
5. [エージェント認証キー]をクリックします。

6. エージェントのインストールに使用するエージェント認証キーを入力するか、現在のエントリを書き留めます。

   重要: このキーは、覚えるか記録してください。エージェントのインストール時に必要となります。



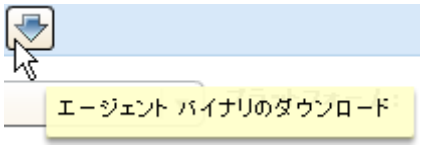
7. [保存]をクリックします。
8. 次のステップの「エージェント インストール プログラムのダウンロード」に進みます。

エージェント インストール プログラムのダウンロード

前の手順でエージェント認証キーを設定した場合、デスクトップ上にエージェント インストール プログラムをダウンロードする状態になります。

エージェント インストール プログラムをダウンロードする方法

1. エージェント エクスプローラに表示されたツールバーから[エージェント バイナリのダウンロード]をクリックします。



   使用可能なエージェント バイナリのリンクがメイン ペインに表示されます。

2. Windows リンクをクリックして、Window Server 2003 オペレーティング システムが実行されているサーバにエージェントをインストールします。

[<IP アドレス> によるダウンロード先の選択]ダイアログ ボックスが表示されます。

3. デスクトップを選択し、[保存]をクリックします。

選択したエージェント バイナリのダウンロードの進捗状況を示すメッセージが表示され、その後に確認メッセージが表示されます。

4. [OK]をクリックします。

5. ブラウザを最小化します。ただし、完了後にインストールをすぐに確認できるように接続は開いておきます。

エージェント インストール プログラムのセットアップ ランチャがデスクトップに表示されます。

エージェントのインストール

開始する前に、以下の情報を確認しておきます。

- エージェント プログラムをダウンロードした CA User Activity Reporting Module サーバの IP アドレス
- エージェント用に作成したユーザ アカウントのユーザ名およびパスワード
- 設定したエージェント認証キー

Windows ホスト用のエージェントをインストールする方法

1. エージェント インストール ランチャをダブルクリックします。

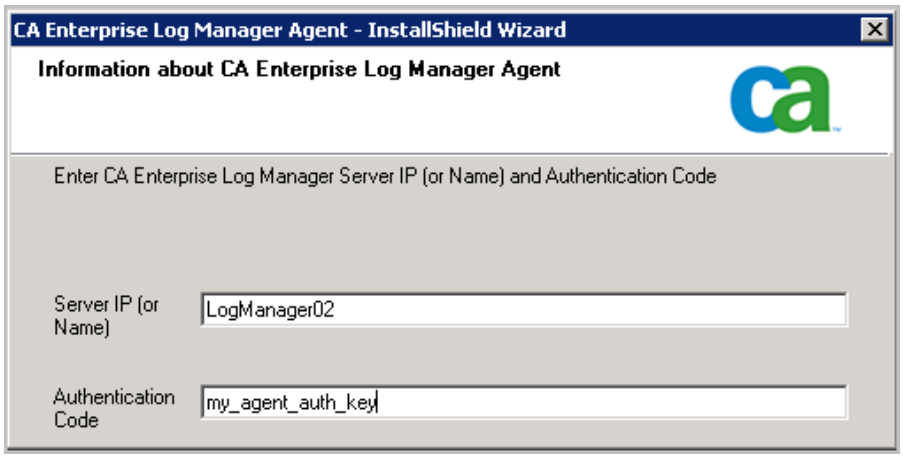
   

   インストール ウィザードが起動します。
2. [次へ]をクリックし、続行するには[使用許諾契約の条件に同意する]をクリックして[次へ]をクリックします。
3. インストール パスを受け入れるか、変更後に[次へ]をクリックします。
4. 以下のように、必要な情報を入力します。
   a. このエージェントが収集したログを転送する CA User Activity Reporting Module のホスト名を入力します。

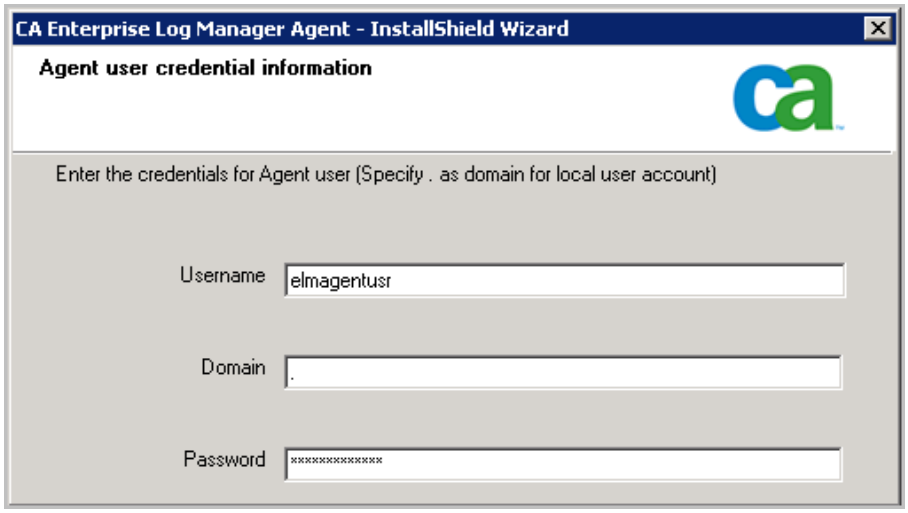
      注: このシナリオ例の CA User Activity Reporting Module では IP アドレス割り当てに DHCP が使用されているので、ここでは IP アドレスを入力しないでください。入力すると、サーバの IP アドレスが変わった場合にエージェントの再インストールが必要になるリスクが生じます。

   b. エージェント認証キーを入力します。

以下に例を示します。



5. エージェント用に設定したユーザ アカウントに定義された名前およびパスワードを入力し、[次へ]をクリックします。



6. ［次へ］をクリックします。エクスポートされるコネクタ ファイルの指定はオプションです。

   ［ファイルのコピーを開始］ページが表示されます。

7. ［次へ］をクリックします。

   エージェント インストール プロセスが完了します。

8. ［終了］をクリックします。

9. 続いて、このエージェントのコネクタを設定します。

   コネクタを設定すると、収集されたイベントはポート 17001 経由で CA User Activity Reporting Module イベント ログ ストアに送信されます。

   重要: エージェントをインストールしたホストからの送信トラフィックを許可しておらず、Windows ファイアウォールを使用している場合は、Windows ファイアウォールでこのポートを開く必要があります。

詳細情報:

エージェント インストール プログラムのダウンロード (P. 39)
エージェントのユーザ アカウントの作成 (P. 36)
エージェント認証キーの設定 (P. 38)

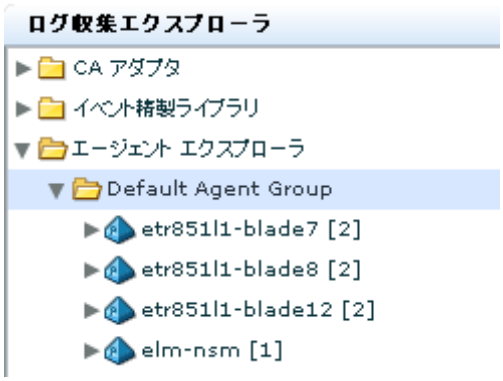
NTEventLog に基づいたコネクタの作成

エージェントをインストールしたら、コネクタを作成して、収集するイベントのイベント ソースを指定します。Windows オペレーティング システムが実行されているサーバにエージェントをインストールしたので、NTEventLog 統合に基づいてコネクタを作成し、WMILogSensor の設定を指定します。［新規コネクタの作成］ウィザードから開いたコネクタ ガイドで説明されている手順に従います。エージェントベースのログ収集のためにエージェントがインストールされるホストの名前を指定します。オプションで、このコネクタ用の別の WMI ログ センサを追加し、エージェントがインストールされたホスト以外のホストを指定できます。これにより、エージェントレスのログ接続が可能になります。追加のホストは同じドメインにあり、追加した最初のホストと同じ Windows 管理者が設定されている必要があります。

NTEventLog に基づいてコネクタを設定する方法

1. CA User Activity Reporting Module エージェント エクスプローラが表示されているブラウザを最大化します。
2. [エージェント エクスプローラ]を展開し、次に、[デフォルトのエージェント グループ]を展開します。

   エージェントをインストールしたコンピュータの名前が表示されます。



3. このエージェントを選択します。

   [エージェント コネクタ]ペインが表示されます。

4. [コネクタの新規作成]をクリックします。

   [コネクタの詳細]ステップが選択された状態で、[新規コネクタの作成]ウィザードが表示されます。

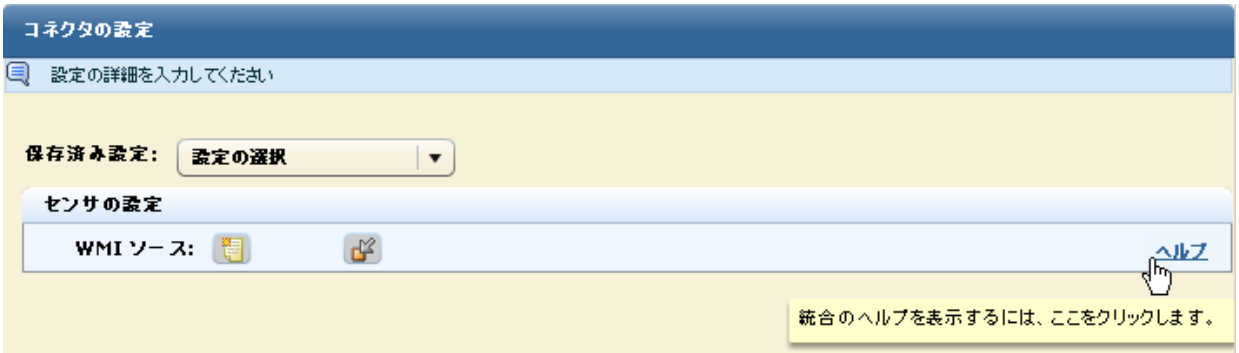
5. [統合]を選択したままにし、[統合]ドロップダウン リストから NTEventLog を選択します。

   [統合]の選択内容に基づいて、[コネクタ名]フィールドおよび[説明]フィールドに内容が入力されます。

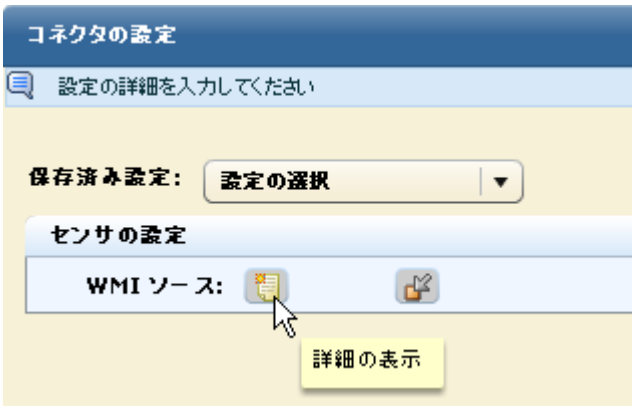
6. コネクタ名を編集して一意にします。たとえば、NTEventLog_Connector_USER001LAB のようにターゲット サーバ名でこの名前を拡張することを検討してください。

7. [コネクタの設定]ステップを選択します。

[センサの設定]ペインが表示されます。[ヘルプ]ボタンをクリックすると、センサの設定用のフィールドについて説明する NTEventLog のコネクタ ガイドが表示されます。

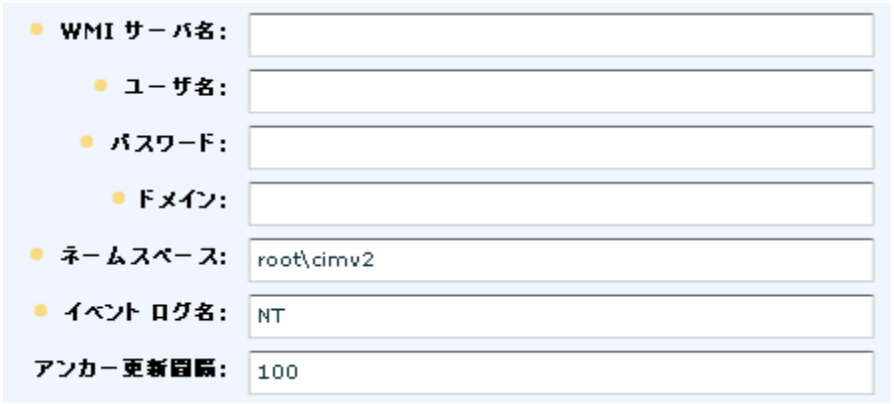


8. WMI ソースの[詳細の表示]ボタンをクリックします。



9. エージェントベースのログ収集を行うため、ローカル コンピュータの WMILogSensor 設定を設定します。詳細については、[ヘルプ]リンクをクリックします。

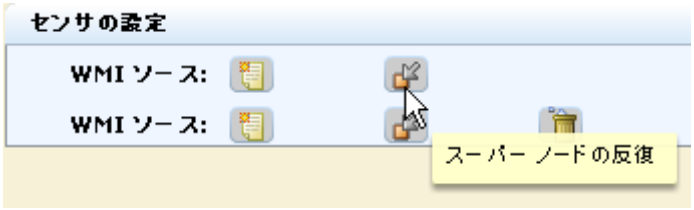
   次の例は、ユーザが指定された WMI サーバの Windows 管理者となっている設定を示しています。ドメインは WMI サーバのものです。



10. (オプション)この同じコネクタを使用してエージェントレス ログ収集を行うために、別のコンピュータの WMI センサを設定します。

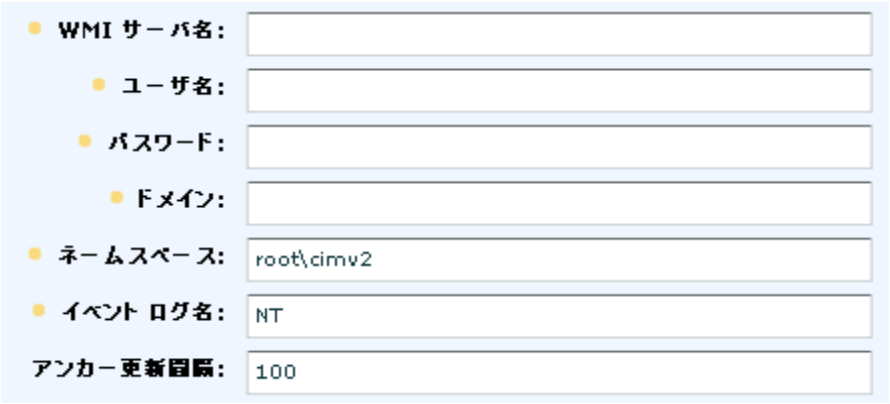
    a. [スーパー ノードの反復]ボタンをクリックします。

       次の図は、2 つの WMI ソースが存在する設定を示しています。



b. 別のコンピュータの WMILogSensor 設定を設定します。

次の例は、同じドメインに存在し、同じ管理者認証情報を持つ 2 番目の WMI ログ センサの設定を示しています。



11. [保存して閉じる]をクリックします。
12. 設定したコネクタのステータスを表示するには、以下の作業を行います。
    a. 左側ペインにあるエージェントを選択します。
    b. [ステータスとコマンド]をクリックします。
    c. [コネクタのステータス表示]を選択します。

    [ステータスの詳細]ペインが表示されます。

13. [実行中]リンクをクリックします。

    コネクタで設定されたターゲットの表示されるステータスは、CPU 使用率、メモリ使用量、および 1 秒あたりの平均イベント数(EPS)などです。

Windows イベント ソースの設定

エージェントで NTEventLog 統合を使用してコネクタを設定した後、イベント ビューアを使用してイベントを見ることができる必要があります。イベントがイベント ビューアに転送されない場合、イベント ソースでローカル ポリシーの Windows 設定を変更する必要があります。

NTEventLog コネクタのイベント ソースでローカル ポリシーを設定する方法

1. ログ収集エクスプローラがまだ表示されていない場合は、[管理]タブをクリックします。
2. [イベント精製ライブラリ]を展開して[統合]を展開し、[サブスクリプション]を展開して NTEventLog を選択し、[統合の詳細を表示]ペインの[統合名]の上にある[ヘルプ]リンクをクリックします。

   NT イベント ログ (セキュリティ、アプリケーション、システム) のコネクタ ガイドが表示されます。
3. CA User Activity Reporting Module ユーザ インターフェースを最小化し、コネクタ ガイドの指示に従って、Windows オペレーティング システムで実行されているイベント ソースのローカル ポリシーを編集します。

   注: システムが Windows Server 2003 である場合、[コントロール パネル]、[管理ツール]、[ローカル セキュリティ ポリシー]の順に選択し、[ローカル ポリシー]を展開します。
4. (オプション) 2 番目の WMI サーバ用に WMI センサを設定した場合は、そのサーバでもローカル ポリシーを編集します。
5. CA User Activity Reporting Module を最大化します。

Windows イベント ソースからのログの表示

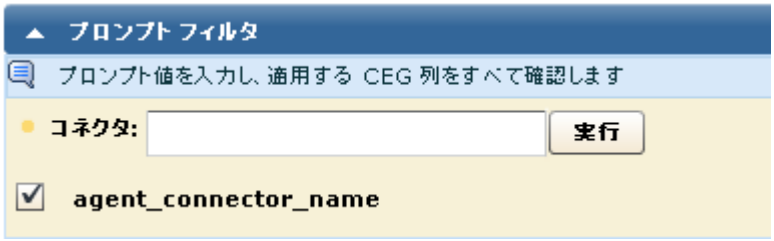
受信イベントのクエリ結果をすばやく表示する方法の 1 つは、ホストのプロンプトを使用する方法です。さらに、クエリまたはレポートを選択することもできます。

受信イベント ログを表示する方法

1. [クエリおよびレポート]タブを選択します。

   [クエリ]サブタブが表示されます。
2. [クエリ リスト]の下の[プロンプト]を展開し、[ホスト]を選択します。

3. [ホスト]フィールドに、センサに設定された WMI サーバ名を入力します。他のチェック マークをクリアし、[実行]をクリックします。



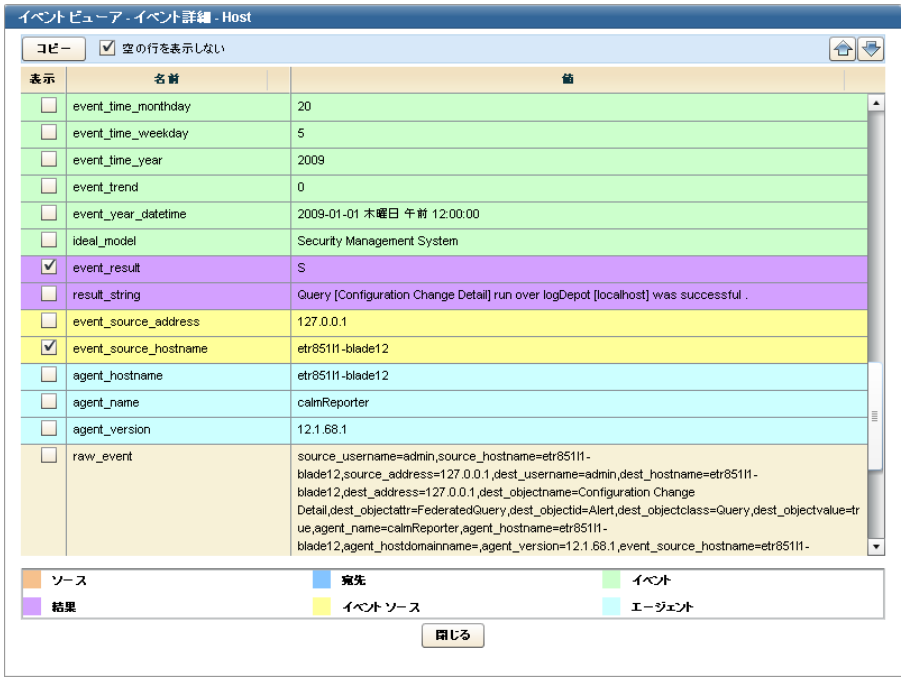
WMI サーバ イベント ソースからのイベントが表示されます。

4. [CA 重大度]をクリックし、スクロールして警告を見つけます。[日付]列と[イベント ソース]列を省略した簡単な例を次に示します。

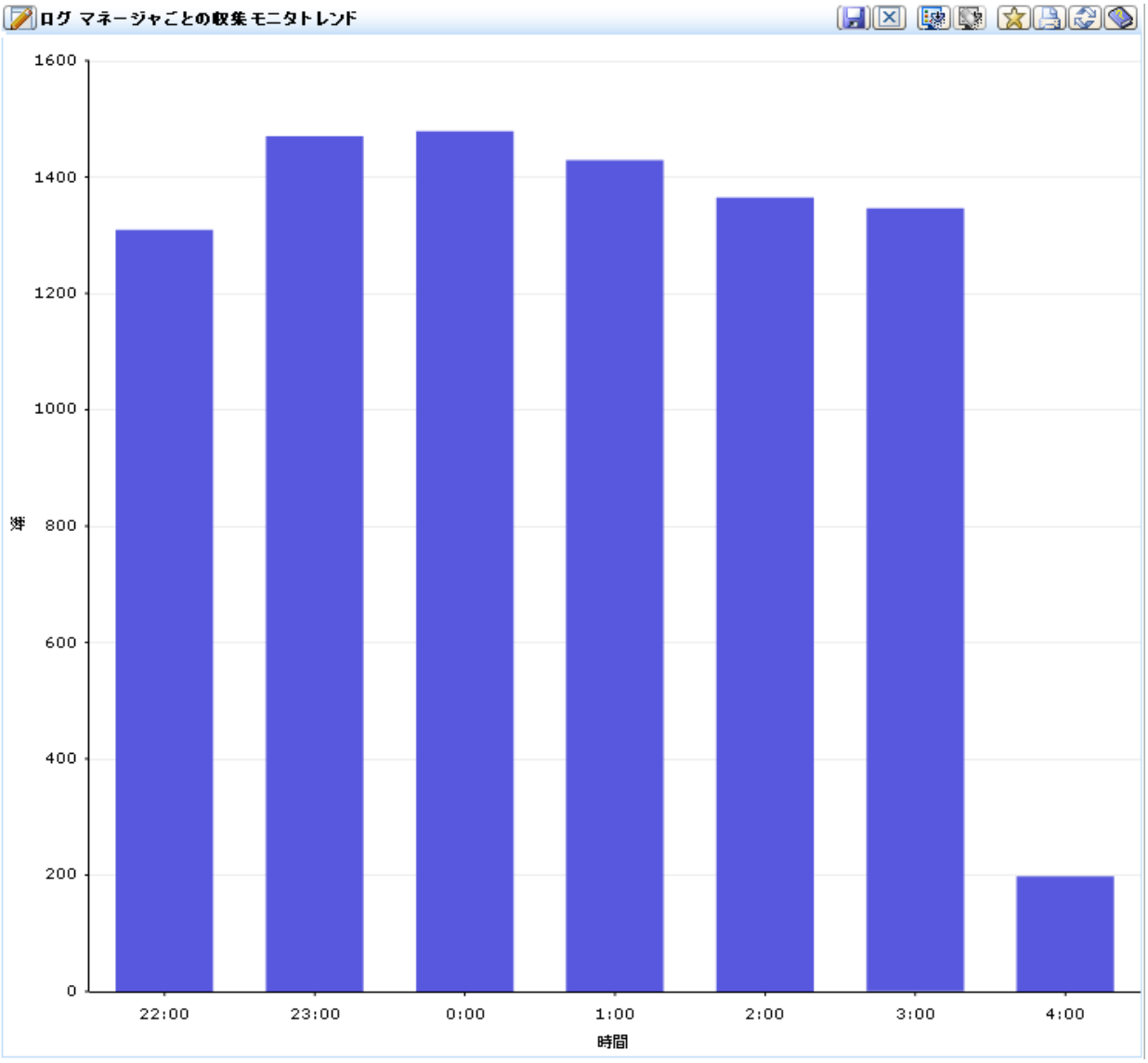
CA 重大度	日付	ソース...	結果	イベント ソース...	カテゴリ	アクション	ログ名
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access	Resource Modify	CALM
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access	Resource Creation	CALM
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access	Resource Execution	CALM

5. [元のイベントの表示]をクリックして、警告の元のイベントを表示します。

6. 警告をダブルクリックして、イベント ビューアにさらに多くのデータを表示します。サンプル データのいくつかの行を次に示します。



7. [クエリおよびレポート]タブをクリックし、[クエリ リスト]からクエリ([ログ マネージャごとの収集モニタトレンド]など)をクリックします。生成される棒グラフを表示します。



8. [レポート]をクリックします。[レポート リスト]の下で、[検索]フィールドに「自己」と入力して、レポート名[システム自己監視イベント]を表示します。このレポートを選択して、CA User Activity Reporting Module サーバによって生成されるイベントのリストを表示します。

注: 分析対象の情報に関し、レポートをスケジュール設定する方法の詳細については、オンライン ヘルプまたは「管理ガイド」を参照してください。

第 4 章: 主な機能

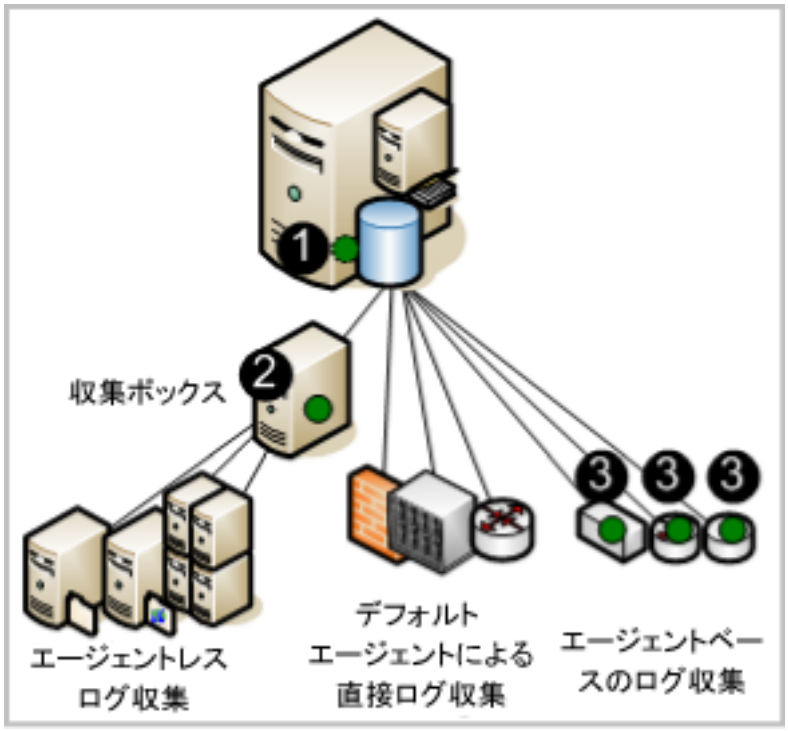
このセクションには、以下のトピックが含まれています。

ログ収集 (P. 52)
ログ ストレージ (P. 54)
ログの標準化された表示 (P. 56)
コンプライアンス レポート (P. 57)
ポリシー違反アラート (P. 59)
資格管理 (P. 60)
ロールベースのアクセス (P. 61)
サブスクリプション管理 (P. 62)
Out-of-the-Box コンテンツ (P. 63)

ログ収集

CA User Activity Reporting Module サーバは、サポートされる 1 つ以上の方法を使用して、ログを収集するように設定できます。方法は、ログを待ち受け、収集するコンポーネントのタイプおよび場所によって異なります。これらのコンポーネントは、エージェント上で設定されます。

次の図は、シングル サーバ システムを表しており、エージェントの位置が濃い（緑色の）円で示されています。



図の番号は、次のステップを示しています。

1. CA User Activity Reporting Module でデフォルト エージェントを設定して、指定した syslog ソースからイベントを直接取得するようにします。
2. Windows 収集ポイントにインストールされたエージェントを設定して、指定した Windows サーバからイベントを収集して、CA User Activity Reporting Module にそれらを転送するようにします。
3. イベント ソースの実行ホスト上でインストール済みのエージェントを設定し、所定のタイプのイベント収集や抑制を実行するようにします。

注: エージェントから宛先 CA User Activity Reporting Module サーバまでのトラフィックは常に暗号化されます。

各ログ収集方法には、次のような利点があります。

- 直接ログ収集

  直接ログ収集では、デフォルト エージェント上に syslog リスナを設定し、指定した信頼できるソースからイベントを受信するようにします。さらに、ソフトウェア アプライアンス オペレーティング システムと互換性を持つどのイベント ソースからもイベントを収集するように、他のコネクタを設定することもできます。

  利点: CA User Activity Reporting Module サーバの隣接するネットワークに存在するイベント ソースからログを収集するために、エージェントをインストールする必要はありません。

- エージェントレス収集

  エージェントレス収集では、イベント ソース上にローカル エージェントはありません。その代わりに、エージェントは専用の収集ポイントにインストールされます。各ターゲット イベント ソースのコネクタは、そのエージェント上で設定されます。

  利点: 企業ポリシーによってエージェントが禁止されているサーバなど、エージェントをインストールできないサーバ上で実行されているイベント ソースからログを収集できます。設定が適切であれば、ODBC ログ収集などが確実に配信されます。

- エージェントベースの収集

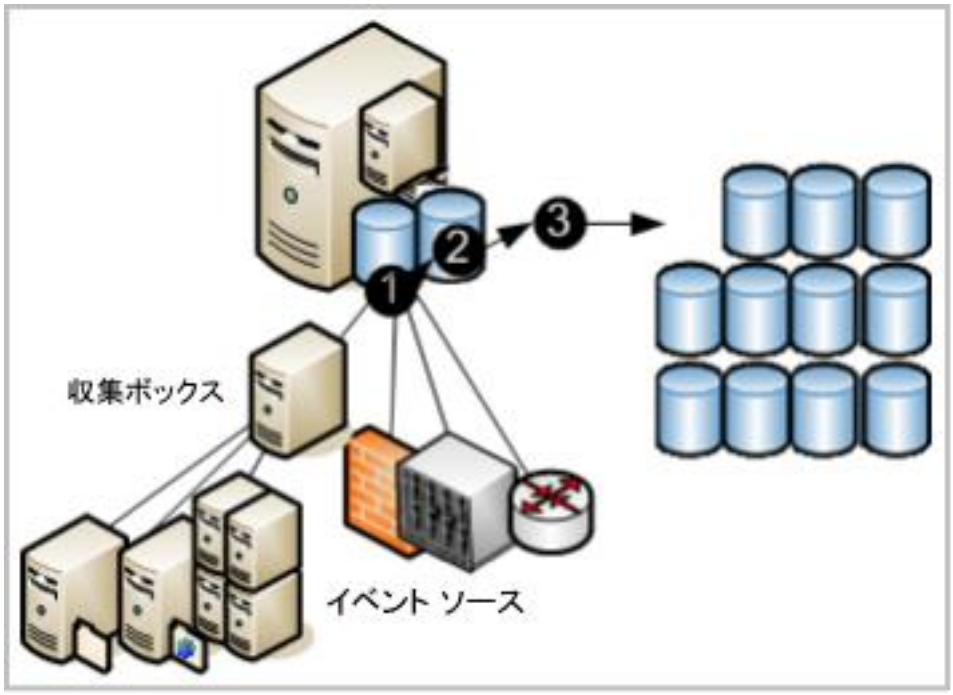
  エージェントベースの収集では、1 つ以上のイベント ソースが実行されていて、各イベント ソースのコネクタが設定されている場所にエージェントがインストールされます。

  利点: そのソースと CA User Activity Reporting Module の間のネットワーク帯域幅が不足していて直接ログ収集をサポートできないソースからログを収集できます。エージェントを使用してイベントをフィルタできるため、ネットワークを介して送信されるトラフィックが減少します。イベント配信が保証されます。

注: エージェント設定の詳細については、「管理ガイド」を参照してください。

ログ ストレージ

CA User Activity Reporting Module には、最近アーカイブされたデータベース用の管理された埋め込みログ ストレージが用意されています。エージェントによってイベント ソースから収集されたイベントは、次の図に示すようなストレージ ライフサイクルをたどります。



図の番号は、次のステップを示しています。

1. いずれかの方法によって収集された新規イベントは、CA User Activity Reporting Module に送信されます。受信イベントの状態は、収集に使用される方法によって異なります。受信イベントは、データベースに登録する前に精製する必要があります。
2. 精製済みレコードのデータベースは所定のサイズに達すると、すべてのレコードがデータベースに圧縮され、一意の名前で保存されます。ログ データを圧縮すると、移動コストが下がり、ストレージのコストが下がります。圧縮されたデータベースは、自動アーカイブ設定に基づいて自動的に移動することも、削除対象として設定された時間が経過する前にバックアップして手動で移動することもできます（自動的にアーカイブされたデータベースは、移動後すぐにソースから削除されます）。
3. 自動アーカイブを設定して、圧縮されたデータベースを毎日リモート サーバに移動する場合は、都合の良いときにそれらのバックアップをサイト外の長期ログ ストレージに移動できます。ログのバックアップを保持すると、ログを安全に収集して一定の年数まとめて保管し、確認できるようにしておくことを定めた規制に準拠できます（データベースは、いつでも長期データベースから復元できます）。

注: 自動アーカイブの設定など、イベント ログ ストアの設定の詳細については、「実装ガイド」を参照してください。*調査およびレポート用にバックアップを復元する方法の詳細については、「管理ガイド」を参照してください。*

ログの標準化された表示

アプリケーション、オペレーティング システム、およびデバイスによって生成されたログでは、すべて独自のフォーマットが使用されます。CA User Activity Reporting Module は、収集されたログを精製して、データの報告方法を標準化します。 フォーマットを標準化することで、監査担当者および上級管理者による、異なるソースから収集されたデータの比較が容易になります。技術的には、CA 共通イベント文法(CEG)によって、イベントの正規化と分類が行われます。

CEG には、以下のようなイベントのさまざまな側面の正規化に使用されるいくつかのフィールドが用意されています。

- 推奨されるモデル(アンチウイルス、DBMS、およびファイアウォールなどのテクノロジのクラス)
- カテゴリ(たとえば、ID 管理およびネットワーク セキュリティなど)
- クラス(たとえば、アカウント管理およびグループ管理など)
- アクション(たとえば、アカウント作成およびグループ作成など)
- 結果(たとえば、成功および失敗など)

注: イベント精製で使用されるルールとファイルの詳細については、「CA User Activity Reporting Module 管理ガイド」を参照してください。イベントの正規化と分類の詳細については、オンライン ヘルプで CEG についてのセクションを参照してください。

コンプライアンス レポート

CA User Activity Reporting Module では、セキュリティ関連データを収集し、内部または外部の監査担当者に適したレポートに変換できます。調査のためにクエリやレポートを操作できます。レポート ジョブをスケジュールすることで、レポート プロセスを自動化できます。

システムには次の機能が備わっています。

- タグを使用した使いやすいクエリ機能
- ほぼリアルタイムのレポート
- 重要なログの、中央で検索可能な分散アーカイブ

その焦点は、イベントとアラートのリアルタイムの関連付けではなく、コンプライアンス レポートに置かれています。業界関連の各種規制に準拠していることを証明するため、各法令ではレポートの提出が義務付けられています。CA User Activity Reporting Module では、識別しやすくするため、次のタグを使用してレポートが生成されます。

- Basel II（バーゼル II）
- COBIT
- COSO
- EU Directive - Data Protection（EU 指令 - データ保護）
- FISMA
- GLBA
- HIPAA
- ISO¥IEC 27001¥2
- JPIPA
- JSOX
- NERC
- NISPOM
- PCI
- SAS70
- SOX

事前定義済みログ レポートを確認するか、指定した基準に基づいて検索を実行できます。新規レポートは、サブスクリプション更新で提供されます。

ログ表示機能は、以下の機能によりサポートされています。

- 事前定義済みクエリまたはユーザ定義クエリによるオンデマンド クエリ機能（最高 5000 のレコードが生成される可能性があります）
- 指定されたホスト名、IP アドレス、ポート番号、またはユーザ名の、プロンプトを使用したクイック検索
- 標準装備のレポート コンテンツが含まれるスケジュール済みレポートとオンデマンド レポート
- スケジュール済みクエリおよびアラート
- トレンド情報が含まれる基本レポート
- 対話型のグラフィカルなイベント ビューア
- 電子メールの添付ファイルを使用した自動レポート
- 自動レポート保持ポリシー

注意: 事前定義済みクエリおよびレポートの使用、または独自のクエリおよびレポートの作成の詳細については、「CA User Activity Reporting Module 管理ガイド」を参照してください。

ポリシー違反アラート

CA User Activity Reporting Module では、すぐに注意が必要なイベントが発生したときにのアラート送信を自動化できます。さらに、直近 5 分間から直近 30 日間までのように、時間間隔を指定することで、いつでも CA User Activity Reporting Module からのアクション アラートを監視できます。アラートは、Web ブラウザからアクセスできる RSS フィードに自動送信されます。オプションで、電子メール アドレス、CA IT PAM プロセス(ヘルプ デスク チケットの生成など)、1 つ以上の SNMP トラップの宛先 IP アドレスを別の宛先として指定できます。

すぐに使い始めることができるように、多くのクエリがあらかじめ定義されているため、そのままアクション アラートとしてスケジュールできます。たとえば、以下のような情報が含まれます。

- 過剰なユーザ アクティビティ
- CPU 高使用率平均
- 使用可能なディスク領域が少ない
- 過去 24 時間に消去されたセキュリティ イベント ログ
- 過去 24 時間に変更された Windows 監査ポリシー

一部のクエリでは、クエリで使用される値を指定するキー設定済みリストが使用されます。いくつかのキー設定済みリストには、補足可能な事前定義済み値が含まれます。たとえば、デフォルト アカウントや権限グループなどです。ビジネス クリティカルなリソースなど、他のキー設定済みリストにはデフォルト値がありません。それらを設定した後、次のような事前定義済みクエリのアラートをスケジュールできます。

- グループ メンバシップの追加または削除(権限グループ別)
- デフォルトのアカウントで成功したログイン
- ビジネス クリティカル ソースが受信したイベントはありません

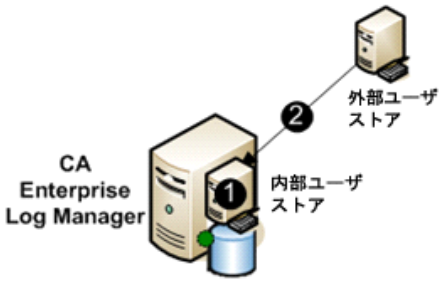
キー設定済みリストは、ファイルのインポートまたは CA IT PAM 動的値プロセスによって、手動で更新できます。

注: アクション アラートの詳細については、「CA User Activity Reporting Module 管理ガイド」を参照してください。

資格管理

ユーザ ストアを設定するとき、ユーザ アカウントを設定したり、ユーザ アカウントがすでに定義されている外部ユーザ ストアを参照したりするために、CA User Activity Reporting Module でデフォルト ユーザ ストアを使用するかどうかを選択します。基礎となるこのデータベースは CA User Activity Reporting Module 専用であり、市販の DBMS を使用しません。

サポートされる外部ユーザ ストアは、CA SiteMinder、および Microsoft Active Directory、Sun One、Novell eDirectory のような LDAP ディレクトリなどです。外部ユーザ ストアを参照する場合、次の図の矢印が示すように、ユーザ アカウント情報が読み取り専用形式で自動的にロードされます。選択したアカウントには、アプリケーション固有の詳細のみを定義します。データが内部ユーザ ストアから参照先外部ユーザ ストアに移動することはありません。



図の番号は、次のステップを示しています。

1. 内部ユーザ ストアは、ログイン時にユーザが入力した認証情報を認証し、そのユーザ アカウントに割り当てられたロールに関連付けられたポリシーに基づいて、ユーザ インターフェースのさまざまな機能にアクセスする権限をユーザに与えることで、資格管理を実行します。ログインしようとするユーザのユーザ名およびパスワードが、外部ユーザ ストアによってロードされた場合、入力された認証情報はロードされた認証情報と一致する必要があります。
2. 外部ユーザ ストアには、内部ユーザ ストアにそのユーザ アカウントをロードすること以外の機能はありません。ユーザ ストアへの参照が保存されると、これらのアカウントは自動的にロードされます。

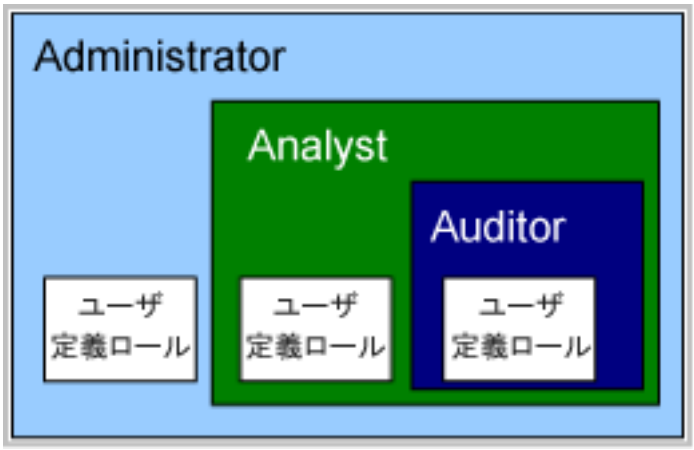
注: 基本的なユーザ アクセスの設定の詳細については、「CA User Activity Reporting Module 実装ガイド」*を参照してください。事前定義済みロールのサポート、ユーザ アカウントの作成、およびロール割り当てポリシーの詳細については、「CA User Activity Reporting Module 管理ガイド」を参照してください。*

ロールベースのアクセス

CA User Activity Reporting Module には、3 つの事前定義済みアプリケーション グループまたはロールが用意されています。管理者は、次のロールをユーザに割り当てることで、CA User Activity Reporting Module 機能に対するアクセス権を指定します。

- Administrator
- Analyst
- Auditor

Auditor は、すべての機能にアクセスできます。Analyst は、すべての Auditor 機能に加えて、いくつかの機能にアクセスできます。Administrator は、すべての機能にアクセスできます。 リソースへのユーザ アクセスをビジネス ニーズに合う方法で制限するポリシーを関連付けた、カスタム ロールを定義できます。



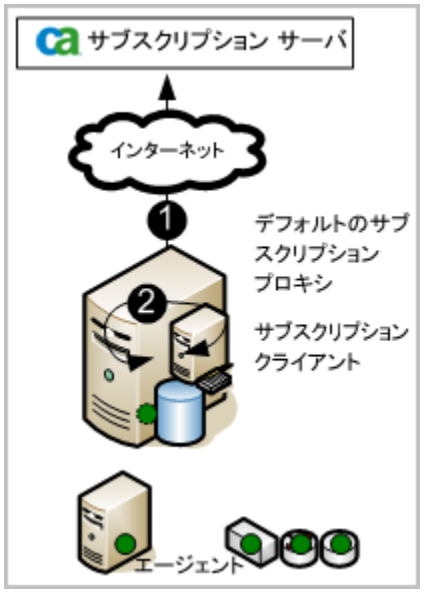
Administrator は、ポリシーが関連付けられたカスタム アプリケーション グループを作成し、そのアプリケーション グループ (つまりロール) をユーザ アカウントに割り当てることにより、任意のリソースへのアクセスをカスタマイズできます。

注: カスタム ロール、カスタム ポリシー、およびアクセス フィルタの計画および作成の詳細については「CA User Activity Reporting Module 管理ガイド」を参照してください。

サブスクリプション管理

サブスクリプション モジュールは、CA サブスクリプション サーバからのサブスクリプション更新が、スケジュールされた間隔で自動的にダウンロードされて CA User Activity Reporting Module サーバに配信されるようにするサービスです。サブスクリプション更新にエージェント用のモジュールが含まれている場合、ユーザはエージェントにこれらの更新を適用できます。サブスクリプション更新では、CA User Activity Reporting Module ソフトウェア コンポーネントの更新、オペレーティング システムの更新（パッチ）、レポートなどのコンテンツの更新が行われます。

次の図は、最も単純な直接インターネット接続シナリオを表しています。



図の番号は、次のステップを示しています。

1. CA User Activity Reporting Module サーバは、デフォルト サブスクリプション サーバとして CA サブスクリプション サーバに更新があるかどうかを問い合わせ、使用可能な新しい更新をすべてダウンロードします。次に CA User Activity Reporting Module サーバはバックアップを作成し、他のすべての CA User Activity Reporting Module 用のコンテンツ更新を格納する管理サーバの埋め込みコンポーネントにコンテンツ更新をプッシュします。
2. CA User Activity Reporting Module サーバは、サブスクリプション クライアントとして、必要な製品とオペレーティング システムの更新を自動的にインストールします。

注: サブスクリプションの計画および設定の詳細については、「実装ガイド」を参照してください。サブスクリプション設定の調整および変更と、エージェントに対する更新の適用の詳細については、「管理ガイド」を参照してください。

Out-of-the-Box コンテンツ

CA User Activity Reporting Module には、製品をインストールして設定するだけですぐに使用できる事前定義済みコンテンツが用意されています。サブスクリプション プロセスによって、定期的に新しいコンテンツの追加と既存のコンテンツの更新が行われます。

事前定義済みコンテンツのカテゴリには次のものがあります。

- タグを使用したレポート
- タグを使用したクエリ
- 関連付けられたセンサ、解析ファイル（XMP）、マッピング（DM）ファイルとの統合（一部、抑制ルールとの統合を含む）
- 抑制ルールおよび集約ルール

第 5 章: CA User Activity Reporting Module の詳細情報

このセクションには、以下のトピックが含まれています。

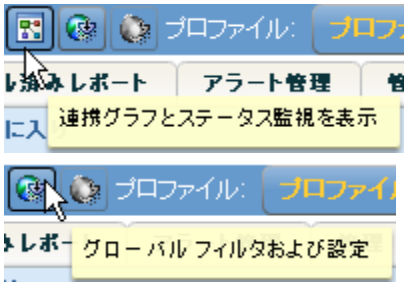
ツールヒントの表示 (P. 65)
オンライン ヘルプの表示 (P. 67)
ドキュメントのマニュアル選択メニューによる検索 (P. 69)

ツールヒントの表示

現在のビューの CA User Activity Reporting Module ページでは、ボタン、チェック ボックス、およびレポートの目的を確認できます。

ツールヒントおよび他のヘルプを表示する方法

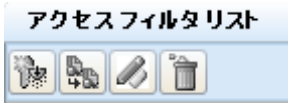
1. ボタンの上にカーソルを移動すると、ボタン機能の説明が表示されます。どのボタンの機能もこの方法で表示できます。



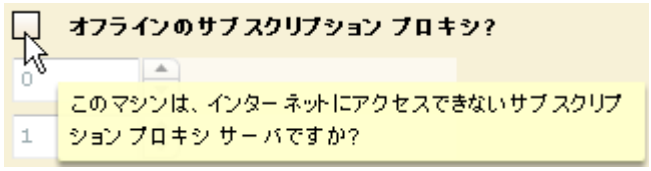
2. アクティブなボタンと非アクティブなボタンの違いに注意してください。

   有効な、つまりアクティブなボタンはカラーで表示されます。たとえば、ユーザとアクセスの管理の管理者には、[アクセス フィルタ リスト]ボタンがカラーで表示されます。

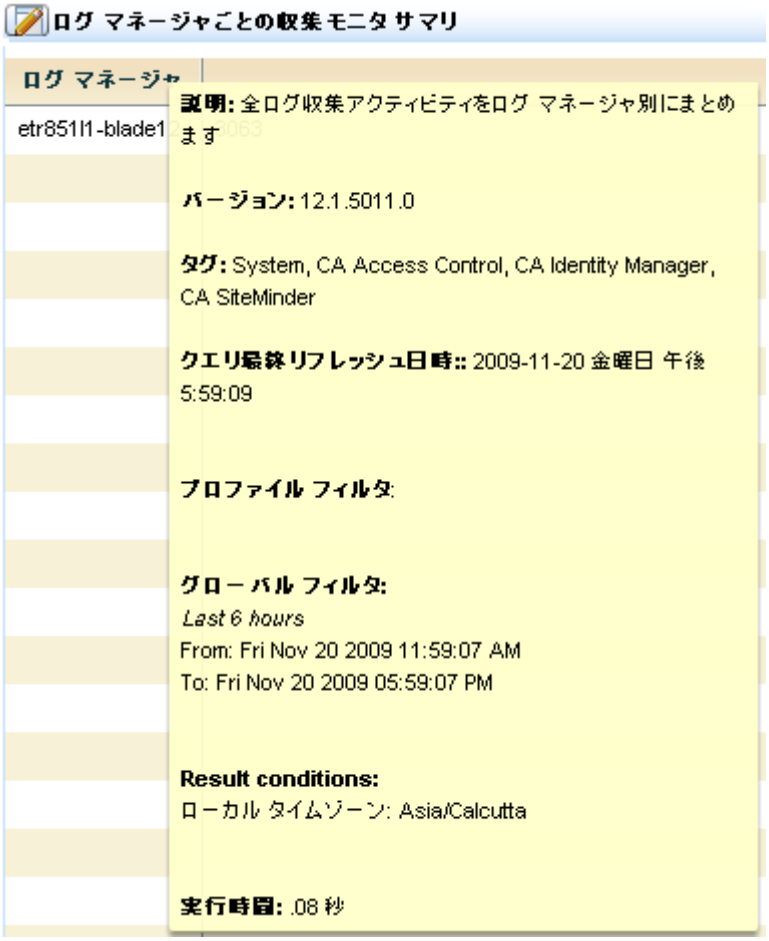
無効な、つまり非アクティブなボタンは白黒で表示されます。たとえば、Auditor には[アクセス フィルタ リスト]ボタンが白黒で表示されます。



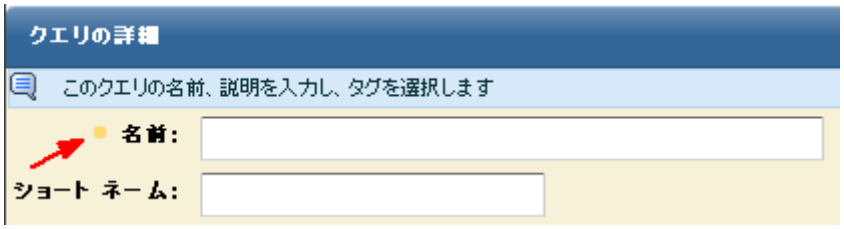
3. カーソルをフィールド名の上に移動すると、入力フィールドまたはチェックボックスの説明が表示されます。



4. レポート名の上にカーソルを移動すると、レポートの説明が表示されます。



5. 一部のフィールドには、左側にオレンジ色の点が表示されます。この点は、フィールドが必須であることを示します。保存可能な設定の場合、すべての必須フィールドに入力するまで保存できません。



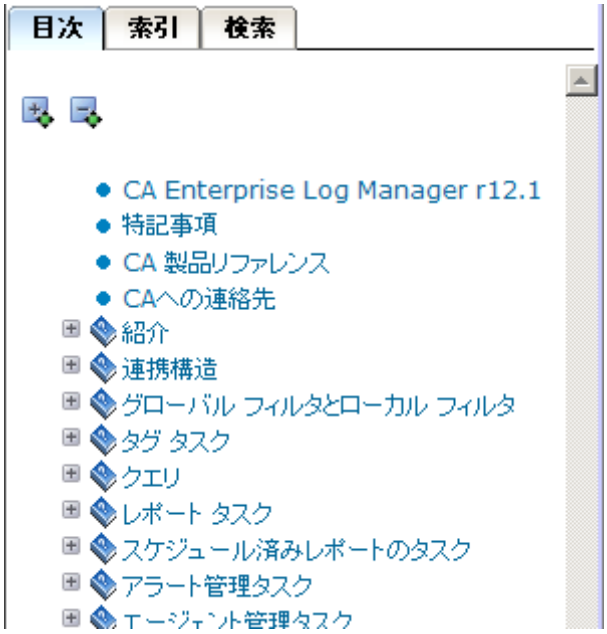
オンライン ヘルプの表示

表示しているページのヘルプや、実行する任意のタスクのヘルプを表示できます。

オンライン ヘルプを表示する方法

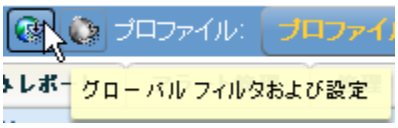
1. ツールバーの[ヘルプ]リンクをクリックし、CA User Activity Reporting Module のオンライン ヘルプ システムを表示します。

CA User Activity Reporting Module ヘルプ システムが表示され、左側ペインに目次が表示されます。



2. 次の例に示すように、[ヘルプ]ボタンからコンテキスト依存ヘルプにアクセスします。

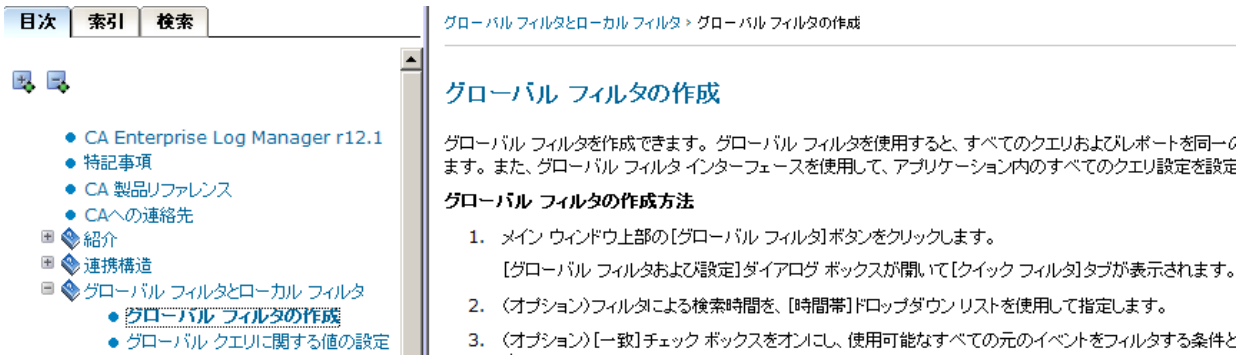
   a. [グローバル フィルタの表示/編集]ボタンをクリックします。

   [グローバル フィルタおよび設定]ウィンドウが、[ヘルプ]ボタンと共に表示されます。

   b. [ヘルプ]ボタンをクリックします。現在のページ、ペイン、またはダイアログ ボックスで実行できる手順のオンライン ヘルプが、2 つ目のウィンドウに表示されます。



c. 実行するタスクはわかっているが、CA User Activity Reporting Module で対応するページにアクセスする方法がわからない場合、目次で見つけることができます。 タスク タイトルをクリックすると、ページが表示されます。

注: 必要なタスクが目次で見つからない場合は、ドキュメントのマニュアル選択メニューを参照してください。

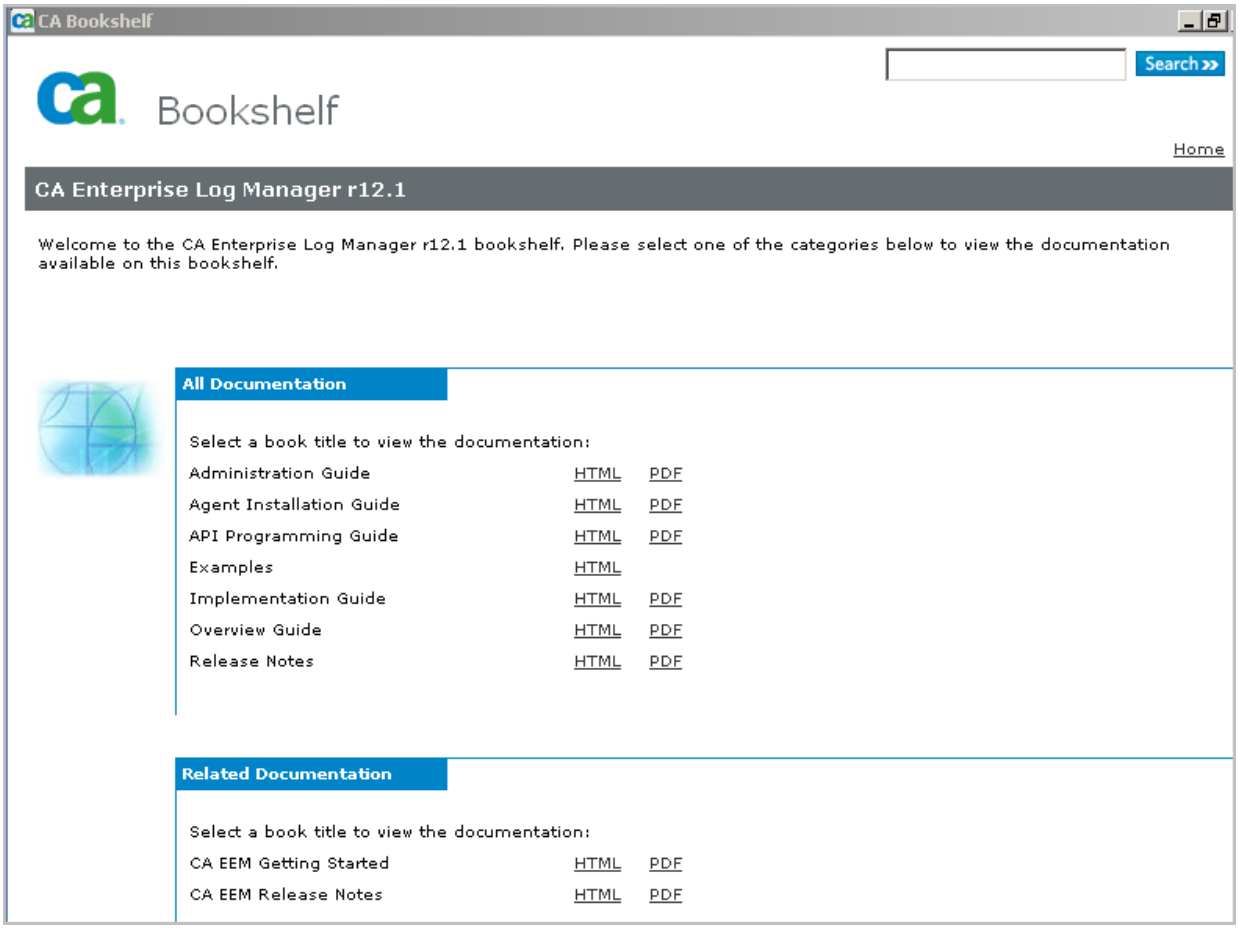
ドキュメントのマニュアル選択メニューによる検索

ローカル ドライブにマニュアル選択メニューをコピーし、すべてのマニュアルを HTML 形式または PDF 形式で参照できます。 HTML 形式のマニュアルには、マニュアル間の相互参照が含まれています。

マニュアル選択メニューによる検索方法

1. マニュアル選択メニューを、アプリケーションのインストール DVD からローカル ドライブにコピーするか、CA カスタマ サポート Web サイトからダウンロードします。 Bookshelf.hta または Bookshelf.html をダブルクリックして、マニュアル選択メニューを開きます。

   次のようなページが表示されます。



主なガイドおよび例について、内容の説明を次に示します。

ガイド	説明内容
エージェント インストール ガイド	エージェントをインストールする方法
実装ガイド	CA User Activity Reporting Module システムをインストールして設定する方法
管理ガイド	設定のカスタマイズ、ルーチン管理タスクの実行、およびクエリ、レポート、アラートを操作する方法
API プログラミング ガイド	API を使用して、Web ブラウザ内のイベント データを表示したり、CA の別の製品やサードパーティ製品のレポートを埋め込んだりする方法
例	よくあるビジネス上の問題を解決する方法と、ドキュメントのトピックへのリンク

2. [検索]入力フィールドに値を入力し、[検索]ボタンをクリックして、ドキュメント内の、入力内容が含まれるすべての箇所を表示します。
3. 印刷リンクをクリックすると、選択したガイドの PDF が開きます。
4. HTML リンクをクリックすると、統合ドキュメント セットが開きます。統合セットには、HTML 形式のすべてのガイドが含まれています。「概要ガイド」の HTML リンクを選択した場合、そのガイドが表示されます。

索引

C

CA Embedded Entitlements Manager
　定義済み - 60
CA Enterprise Log Manager
　インストール - 10
　オンライン ヘルプ - 67
　コンポーネント - 10
　ツールのヒント - 65
　ユーザ ロール - 61

S

syslog
　イベントの表示 - 31

あ

アーカイブ
　定義済み - 54
エージェント バイナリ
　Windows システム用のダウンロード - 39
エージェントのインストール
　マニュアル、Windows 用 - 41
エージェントのユーザ アカウント
　Windows 用の設定 - 36
エージェント認証キー
　更新 - 38

か

コネクタ
　設定 - 43

さ

サブスクリプション管理
　処理の説明 - 62
　定義済み - 62

た

ツールのヒント
　使い方 - 65
データ マッピング
　定義済み - 56
テスト環境
　インストールするもの - 10
デフォルト エージェント
　syslog コネクタの設定 - 28

は

プロンプト
　syslog イベントを表示するための使用 - 31
　Windows イベント ソースのログを表示するための使用 - 48

ま

メッセージの解析
　定義済み - 56

や

ユーザ ロール
　定義済み - 61

ら

ログ収集
　定義済み - 52
ログ ストレージ
　定義済み - 54

漢字

共通イベント文法（CEG）
　定義済み - 56