CA Enterprise Log Manager

概要ガイド

r12.1 SP1

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 Enterprise Log Manager 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 Enterprise Log Manager 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 (15 ページ)
ポリシー違反アラート (53 ページ)
ドキュメントのマニュアル選択メニューによる検索 (63 ページ)

目次

第 1 章: 紹介 9

本書の内容 9
CA Enterprise Log Manager について 10
ネットワーク -- インストール前 11
インストール内容 12

第 2 章: クイック スタート展開 15

クイック スタートの概要 15
シングル サーバ システムのインストール 16
Windows の hosts ファイルの更新 22
最初の管理者の設定 22
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 33

エージェントのユーザ アカウントの作成 34
エージェント認証キーの設定 35
エージェント インストール プログラムのダウンロード 36
エージェントのインストール 37
NTEventLog に基づいたコネクタの作成 39
Windows イベント ソースの設定 43
Windows イベント ソースからのログの表示 43

第 4 章: 主な機能 47

ログ収集 47
ログ ストレージ 49
ログの標準化された表示 50
コンプライアンス レポート 51
ポリシー違反アラート 53
資格管理 54
ロールベースのアクセス 55
サブスクリプション管理 56

Out-of-the-Box コンテンツ 57

第 5 章: CA Enterprise Log Manager の詳細情報 59

ツールヒントの表示 59
オンライン ヘルプの表示 61
ドキュメントのマニュアル選択メニューによる検索 63

用語集 65

索引 91

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 (9 ページ)
CA Enterprise Log Manager について (10 ページ)

本書の内容

この「概要ガイド」では、CA Enterprise Log Manager 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 Enterprise Log Manager 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
CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager について

CA Enterprise Log Manager 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。

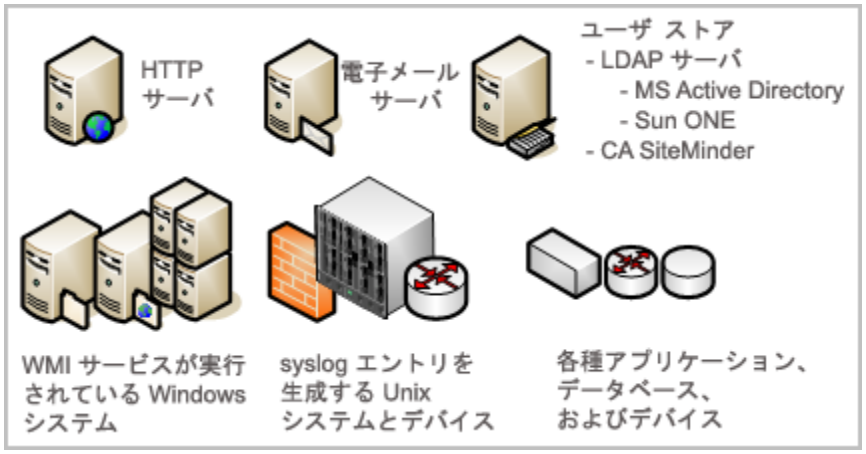
ネットワーク -- インストール前

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 Enterprise Log Manager 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

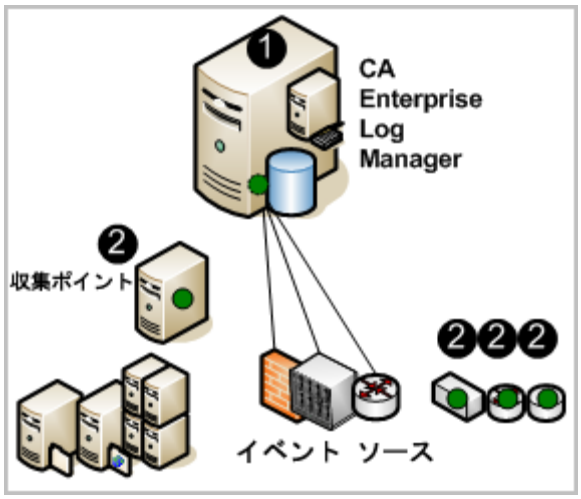
シングル サーバ ソリューションをセットアップし、イベントを収集し始めるのに多くの時間はかかりません。

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 Enterprise Log Manager サーバ
- CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager アプリケーションをインストールします。 CA Enterprise Log Manager 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(37 ページ)

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 (15 ページ)
シングル サーバ システムのインストール (16 ページ)
Windows の hosts ファイルの更新 (22 ページ)
最初の管理者の設定 (22 ページ)
Syslog イベント ソースの設定 (25 ページ)
Syslog コネクタの編集 (28 ページ)
Syslog イベントの表示 (31 ページ)

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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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

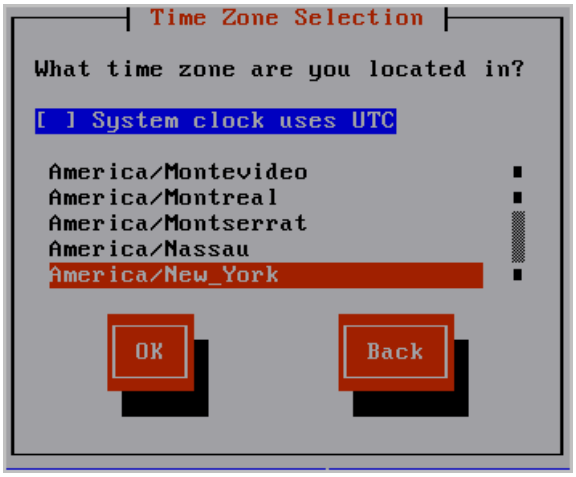
     注: インストールを完了するには、ネットワークの DNS サーバにドメインを登録する必要があります。
   - DNS サーバの IP アドレス
   - (オプション) NTP タイム サーバの IP アドレス
   - デフォルト インストールのスーパーユーザ名 EiamAdmin のパスワード
   - CAELM

     これは、CA Enterprise Log Manager 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。

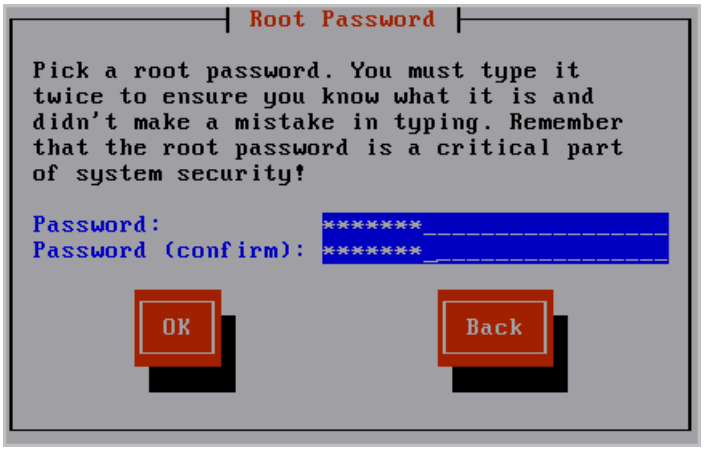
2. CA Enterprise Log Manager ダウンロード パッケージから作成したメディアを使用して、あらかじめ設定されたオペレーティング システムをインストールします。 オペレーティング システム インストール中に、以下を実行します。

   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 Enterprise Log Manager 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。

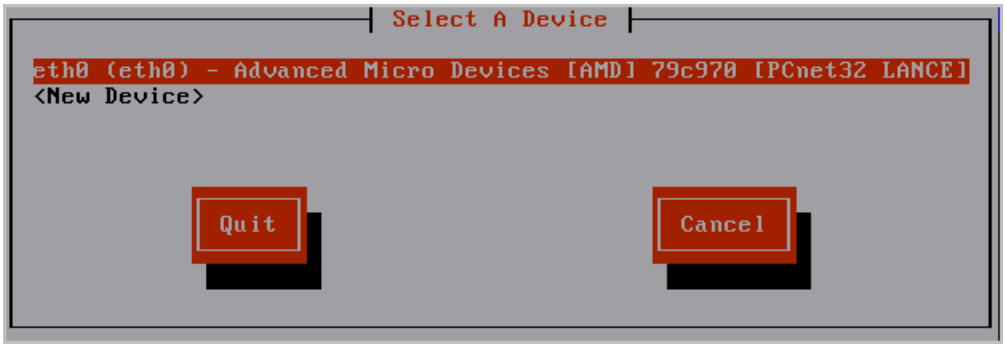
最適なパフォーマンスを得るために推奨される最小仕様を、システムが満たしているかどうかが確認されます。 満たさない場合、インストール プロセスを停止するかどうかを確認するプロンプトが表示されます。

以下のプロンプトが表示されます。

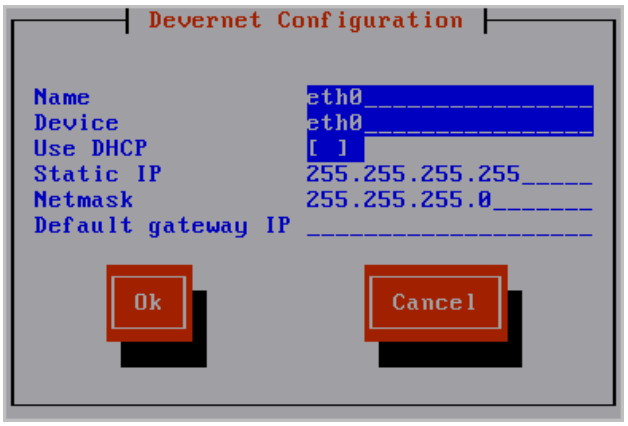
新しいホスト名を入力してください:

4. この CA Enterprise Log Manager 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 Enterprise Log Manager 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。

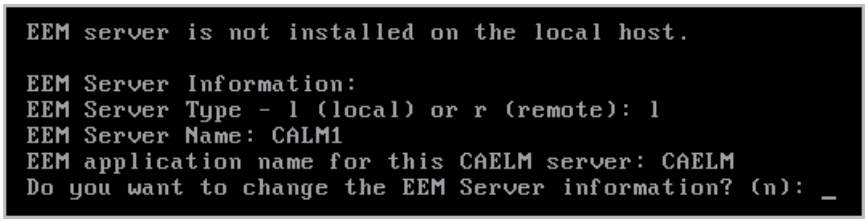
       EEM サーバの EiamAdmin ユーザのパスワードを入力します。
       EEM サーバの EiamAdmin ユーザのパスワードを確認します。

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 Enterprise Log Manager 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。



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 Enterprise Log Manager 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 Enterprise Log Manager サーバは FIPS モードで起動します。 n と入力すると、CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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。

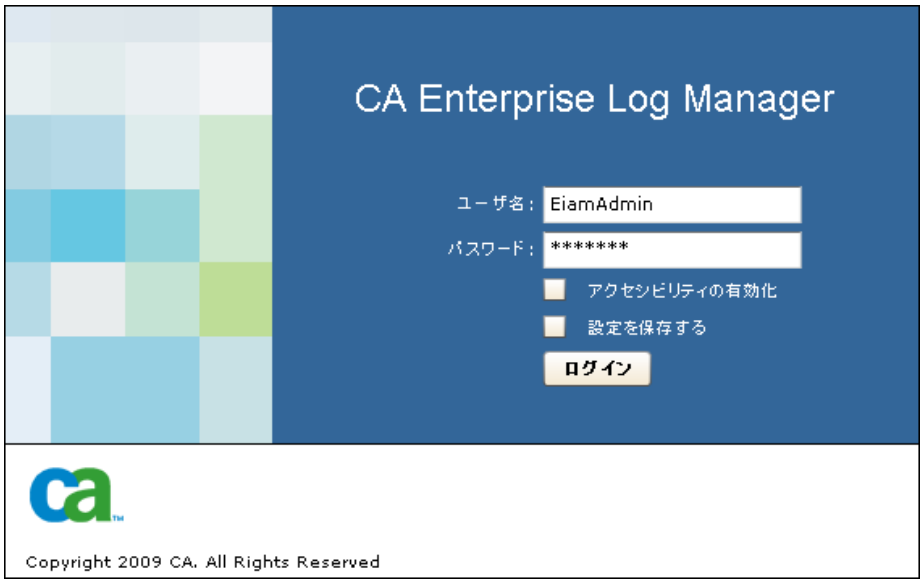
      [トラステッド証明書]ダイアログ ボックスが表示されます。

   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。

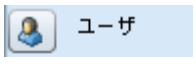
      ログオン ページが表示されます。

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。

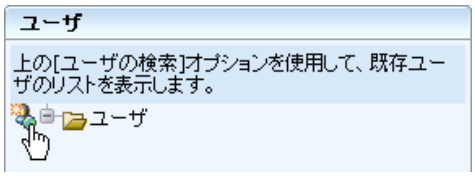


   アプリケーションでは、最初は[管理者]タブと[ユーザとアクセスの管理]サブタブのみがアクティブになっています。

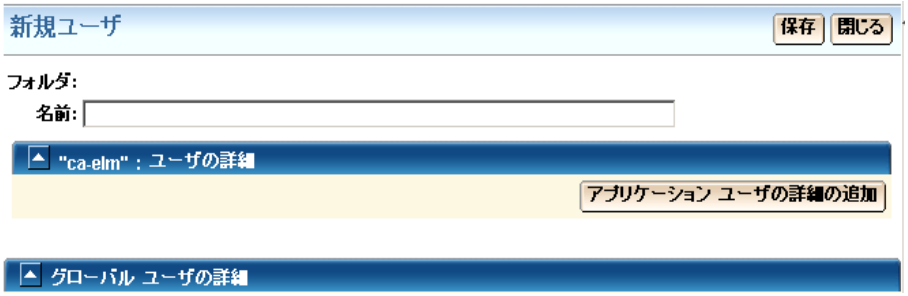
4. [ユーザ]をクリックします。



5. [新規ユーザの追加]をクリックします。

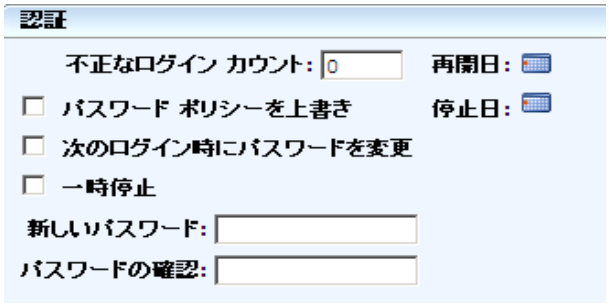


6. [名前]フィールドに名前を入力し、[アプリケーション ユーザの詳細の追加]をクリックします。



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 Enterprise Log Manager に再度ログインします。

    すべての機能が有効になって CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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。

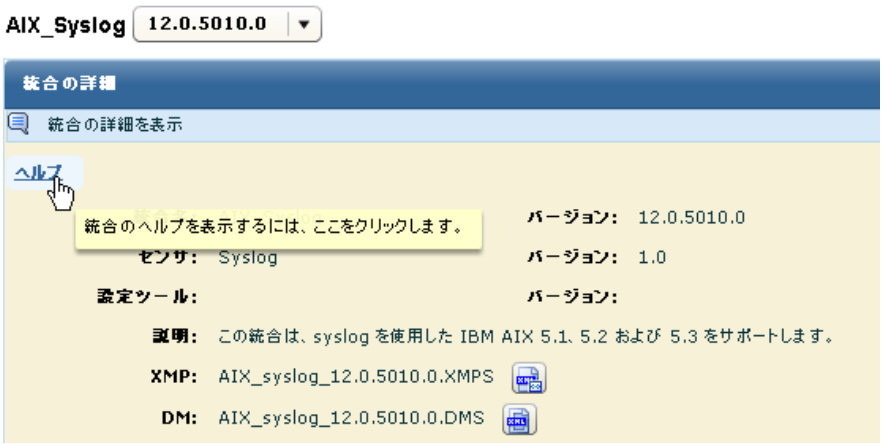
   ログ収集エクスプローラが表示されます。

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。

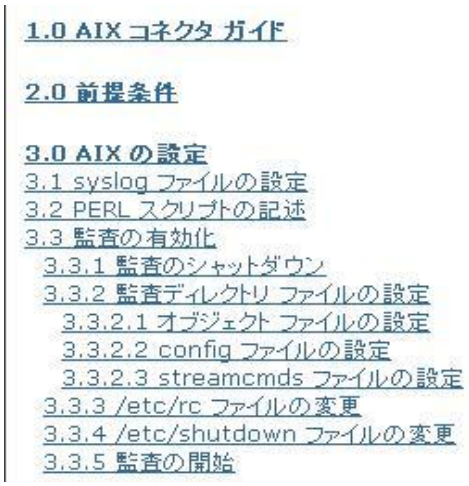
   統合の詳細が表示されます。



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。

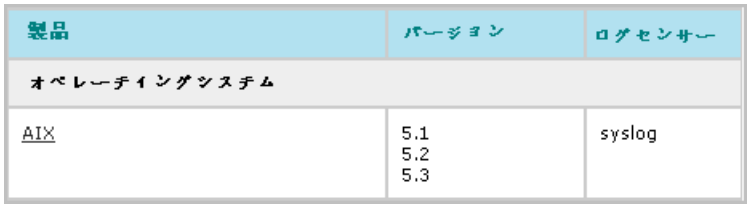
7. イベント ソースの設定要件についてのセクションをクリックします。 この例では、AIX オペレーティング システムのイベント ソースを設定して、その syslog を CA Enterprise Log Manager に送信する方法がドキュメントで説明されています。



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 Enterprise Log Manager 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 Enterprise Log Manager には、それぞれデフォルト エージェントがあります。 CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager が存在するユーザ定義グループを展開します。

3. CA Enterprise Log Manager 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 Enterprise Log Manager 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。

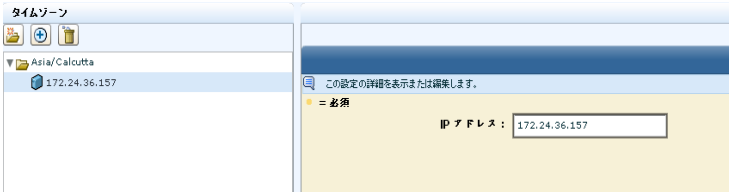
   通常は、デフォルト エージェントのデフォルト UPD および TCP ポートを受け入れることができます。

   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。

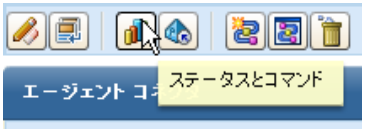
    b. フォルダの下にある空白のエントリを強調表示します。 このコネクタに設定したトラステッドホスト、または CA Enterprise Log Manager のインストールで指定した NTP タイム サーバのいずれかの IP アドレスを入力します。



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

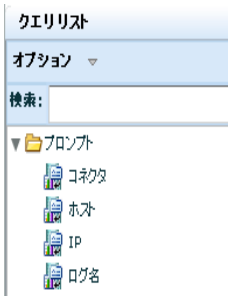
syslog リスナによって収集されたイベントのクエリ結果をすばやく表示する方法の 1 つは、ホストのプロンプトを使用する方法です。

syslog イベントを表示する方法

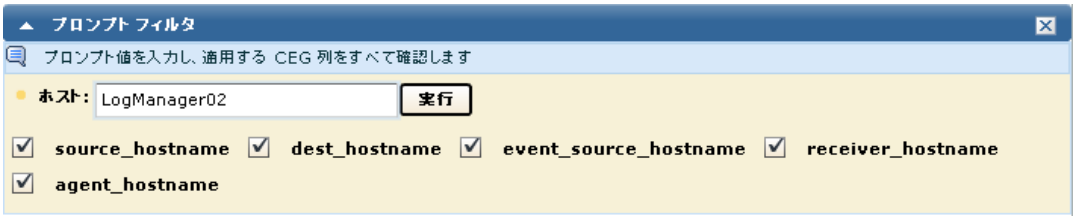
1. [クエリおよびレポート]タブを選択します。

   [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。



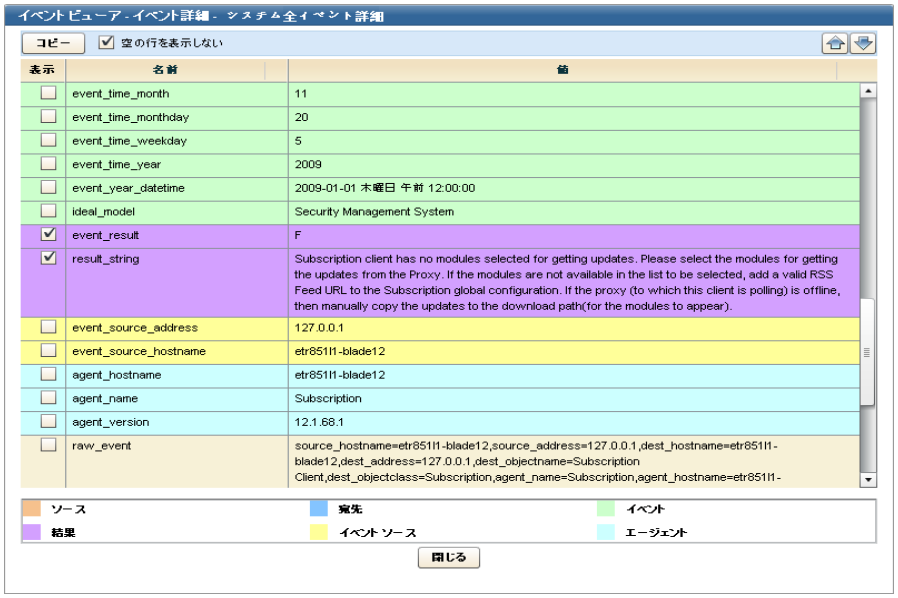
3. デフォルト エージェントによって収集されたイベントのクエリを送信します。
   a. [ホスト]フィールドに、デフォルト エージェント ホスト名 (このエージェントが存在する CA Enterprise Log Manager の名前でもあります)を入力します。
   b. agent_hostname を選択します。
   c. [実行]をクリックします。



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 Enterprise Log Manager 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 (34 ページ)
エージェント認証キーの設定 (35 ページ)
エージェント インストール プログラムのダウンロード (36 ページ)
エージェントのインストール (37 ページ)
NTEventLog に基づいたコネクタの作成 (39 ページ)
Windows イベント ソースの設定 (43 ページ)
Windows イベント ソースからのログの表示 (43 ページ)

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。

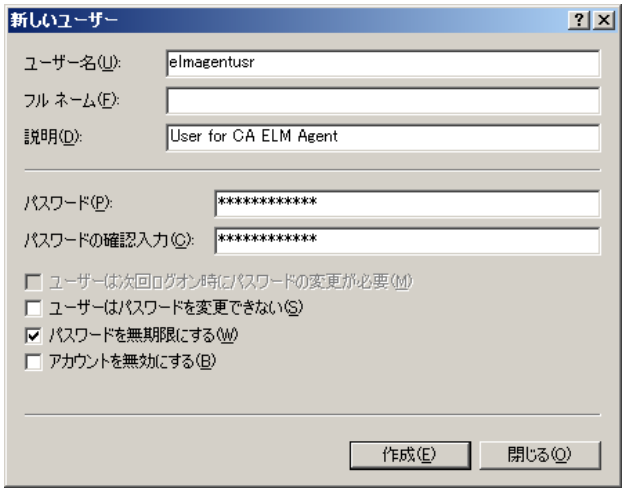
注: インストール時にこの手順を省略して、エージェントに管理者のドメイン認証情報を指定できますが、お勧めしません。

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 (37 ページ)

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

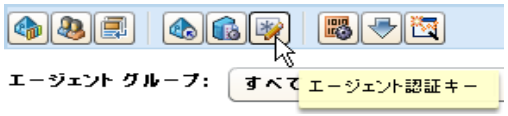
1. エージェントをインストールするホストでブラウザを開き、このエージェントの CA Enterprise Log Manager サーバの URL を入力します。 以下に例を示します。

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

2. CA Enterprise Log Manager 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。

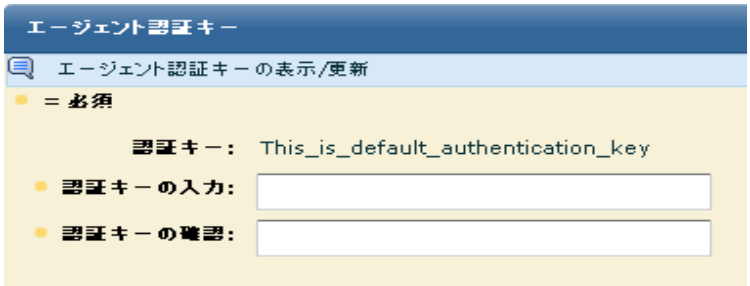
   左側ペインに、ログ収集エクスプローラが表示されます。
4. [エージェント エクスプローラ]フォルダを選択します。

   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。



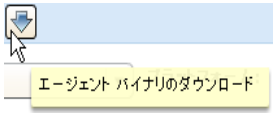
7. [保存]をクリックします。
8. 次のステップの「エージェント インストール プログラムのダウンロード」に進みます。

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 Enterprise Log Manager 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。

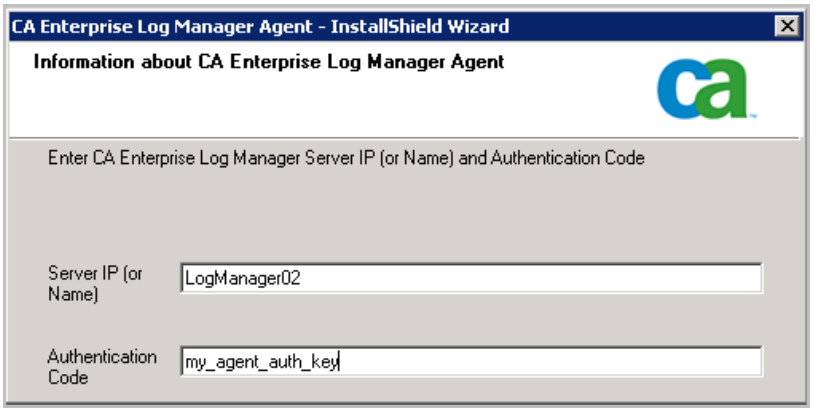
インストール ウィザードが起動します。

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 Enterprise Log Manager のホスト名を入力します。

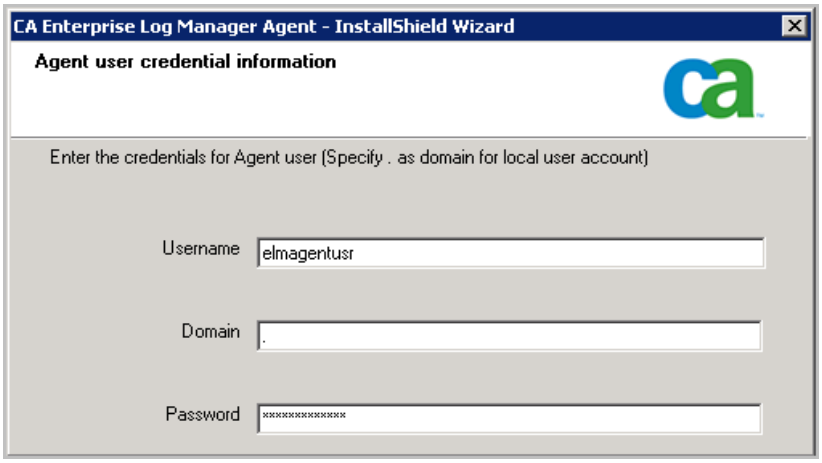
      注: このシナリオ例の CA Enterprise Log Manager では IP アドレス割り当てに DHCP が使用されているので、ここでは IP アドレスを入力しないでください。入力すると、サーバの IP アドレスが変わった場合にエージェントの再インストールが必要になるリスクが生じます。

   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 Enterprise Log Manager 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 (36 ページ)
エージェントのユーザ アカウントの作成 (34 ページ)
エージェント認証キーの設定 (35 ページ)

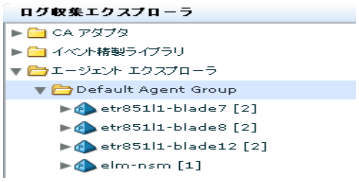
NTEventLog に基づいたコネクタの作成

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 Enterprise Log Manager 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。

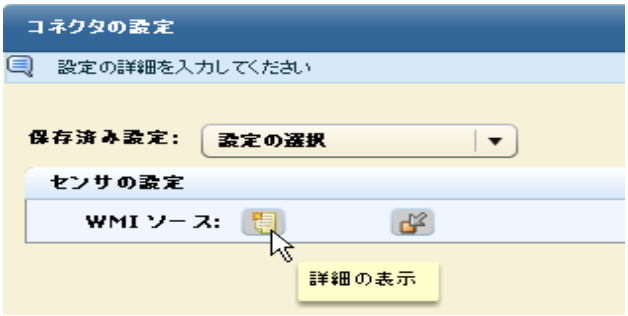
   [統合]の選択内容に基づいて、[コネクタ名]フィールドおよび[説明]フィールドに内容が入力されます。

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。



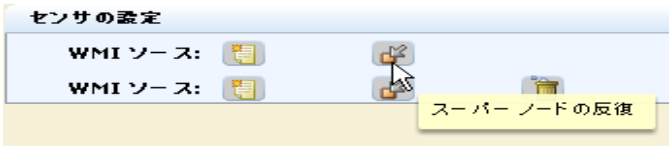
9. エージェントベースのログ収集を行うため、ローカル コンピュータの WMILogSensor 設定を設定します。 詳細については、[ヘルプ]リンクをクリックします。

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 Enterprise Log Manager 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 Enterprise Log Manager を最大化します。

Windows イベント ソースからのログの表示

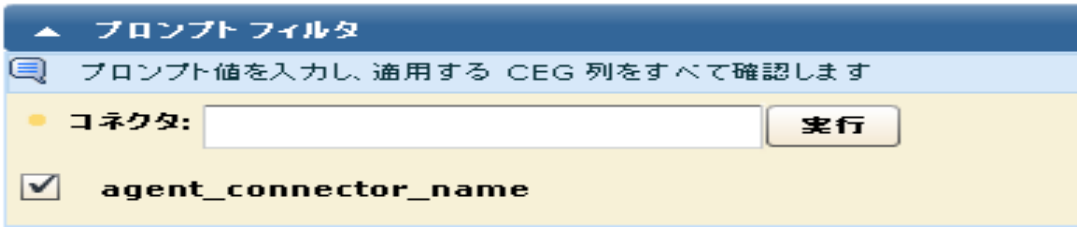
受信イベントのクエリ結果をすばやく表示する方法の 1 つは、ホストのプロンプトを使用する方法です。 さらに、クエリまたはレポートを選択することもできます。

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。



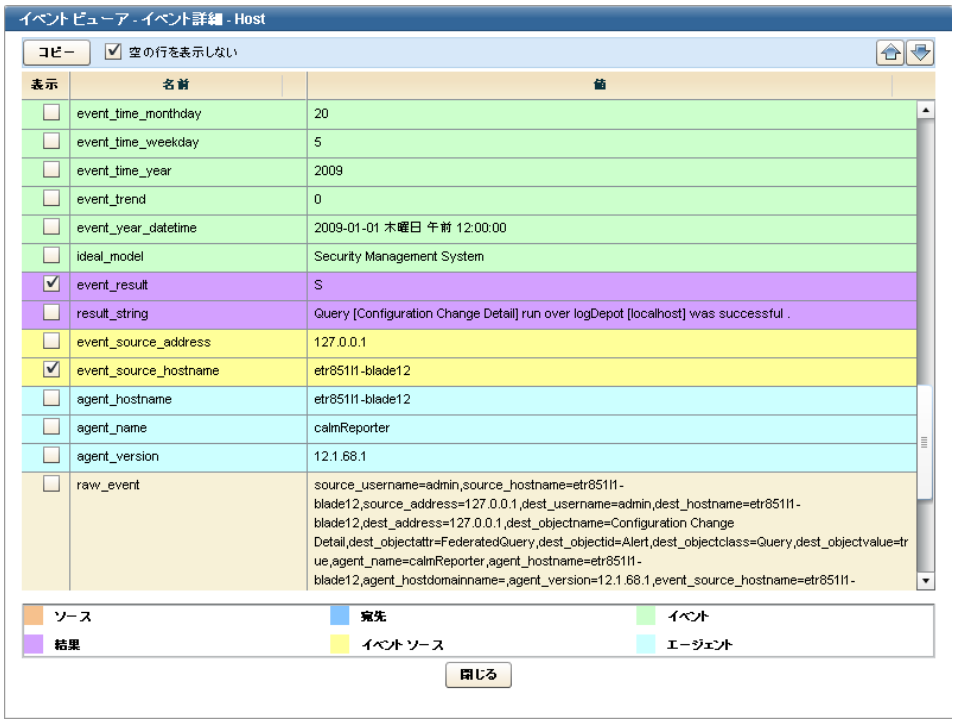
WMI サーバ イベント ソースからのイベントが表示されます。

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。

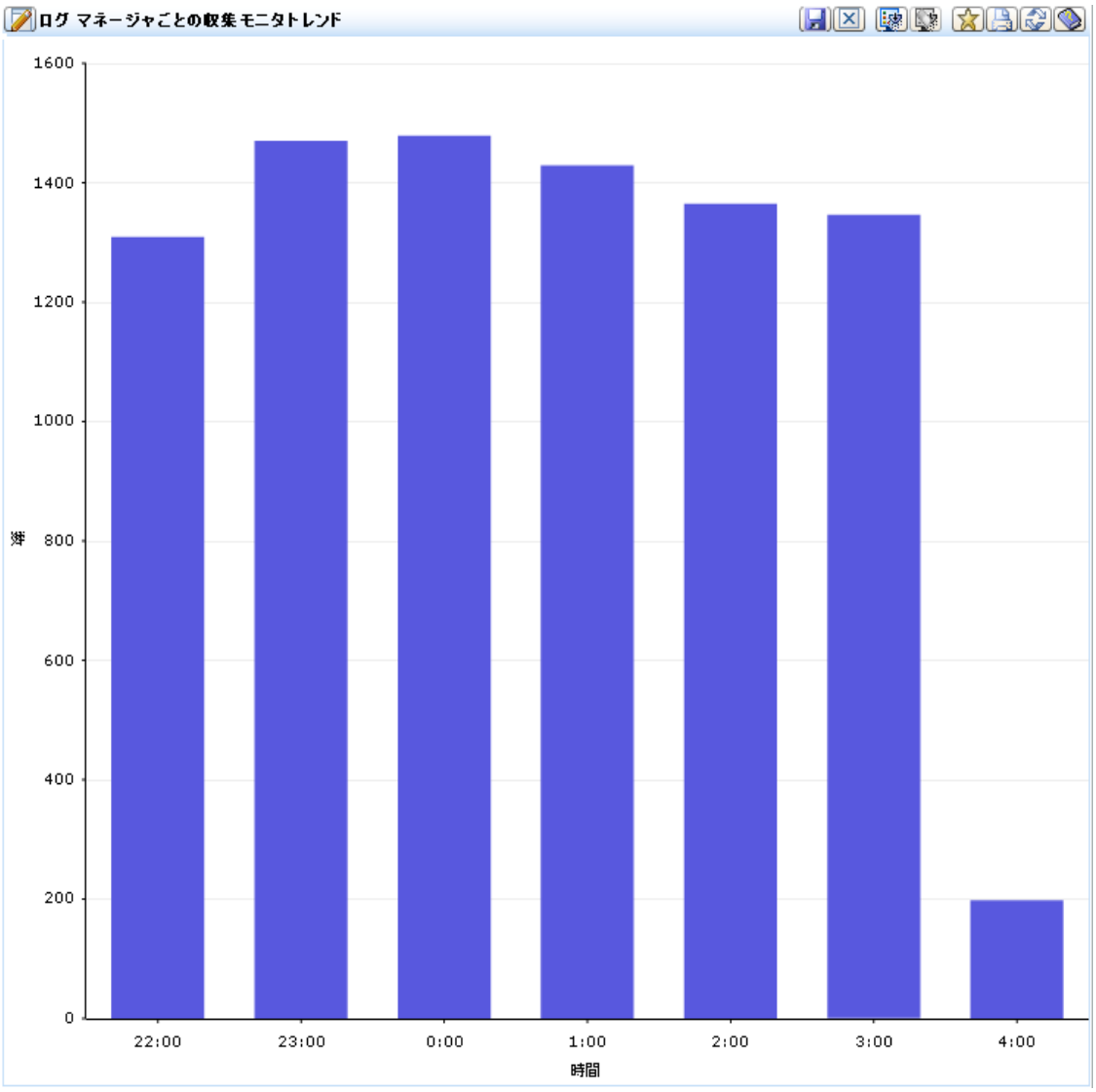
CA 重大度	日付	ソース...	結果	イベント ソース...	カテゴリ	アクション	ログ名
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access	Resource Modify	CALM
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access	Resource Creation	CALM
情報	2009-11-20 金曜日 午前 9:23:16	admin	S	etr851l1-blade12	Resource Access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

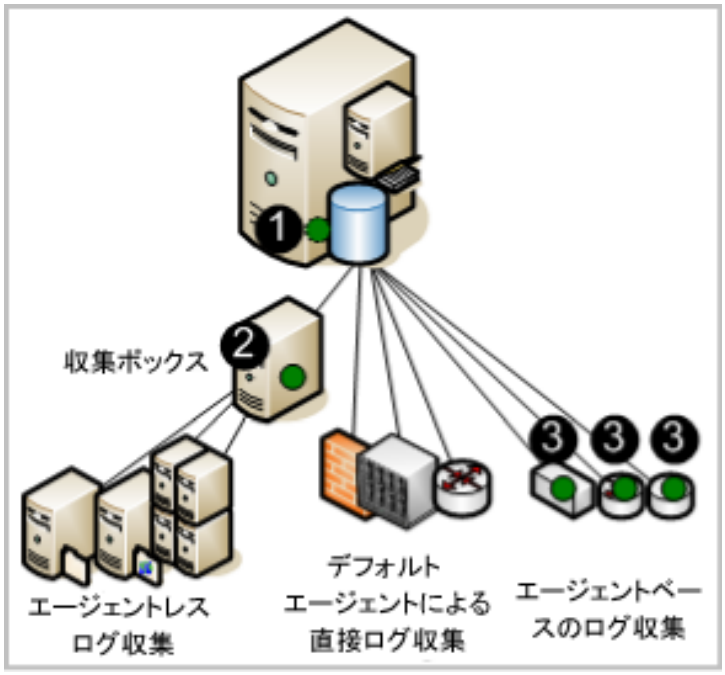
このセクションには、以下のトピックが含まれています。

ログ収集 (47 ページ)
ログ ストレージ (49 ページ)
ログの標準化された表示 (50 ページ)
コンプライアンス レポート (51 ページ)
ポリシー違反アラート (53 ページ)
資格管理 (54 ページ)
ロールベースのアクセス (55 ページ)
サブスクリプション管理 (56 ページ)
Out-of-the-Box コンテンツ (57 ページ)

ログ収集

CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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

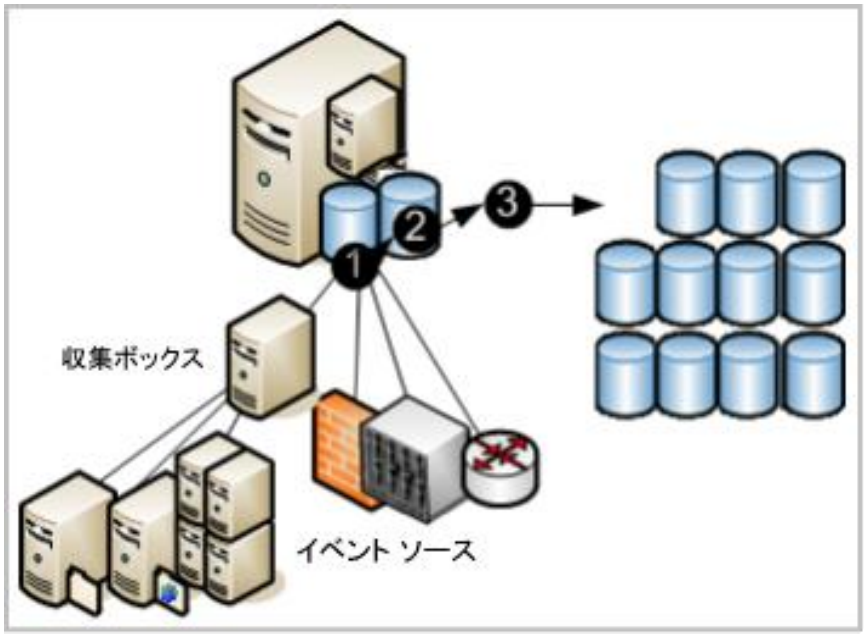
  エージェントベースの収集では、1 つ以上のイベント ソースが実行されていて、各イベント ソースのコネクタが設定されている場所にエージェントがインストールされます。

  利点: そのソースと CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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

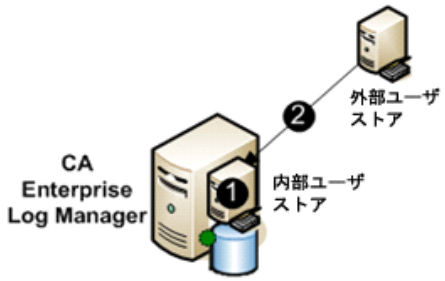
キー設定済みリストは、ファイルのインポートまたは CA IT PAM 動的値プロセスによって、手動で更新できます。

注: アクション アラートの詳細については、「CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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。

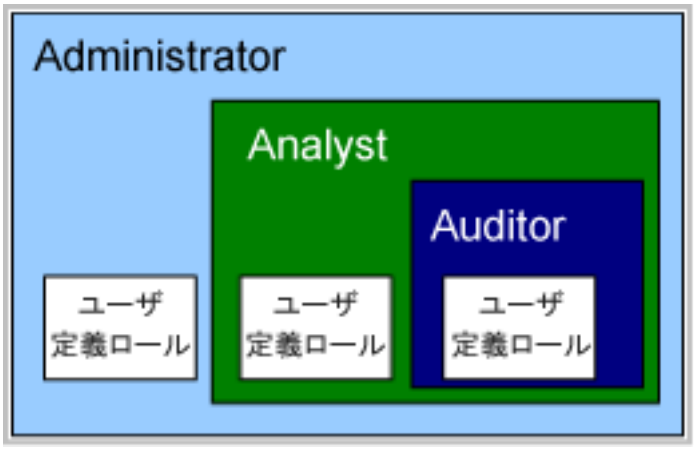
注: 基本的なユーザ アクセスの設定の詳細については、「CA Enterprise Log Manager 実装ガイド」を参照してください。 事前定義済みロールのサポート、ユーザ アカウントの作成、およびロール割り当てポリシーの詳細については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

ロールベースのアクセス

CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager サーバはバックアップを作成し、他のすべての CA Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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 Enterprise Log Manager 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。

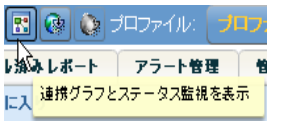
ツールヒントの表示 (59 ページ)
オンライン ヘルプの表示 (61 ページ)
ドキュメントのマニュアル選択メニューによる検索 (63 ページ)

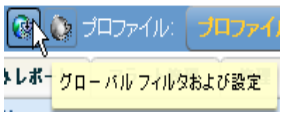
ツールヒントの表示

現在のビューの CA Enterprise Log Manager 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。



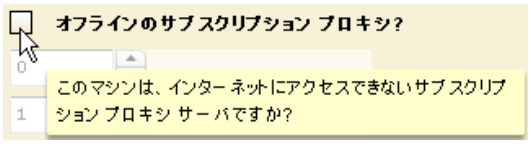


2. アクティブなボタンと非アクティブなボタンの違いに注意してください。

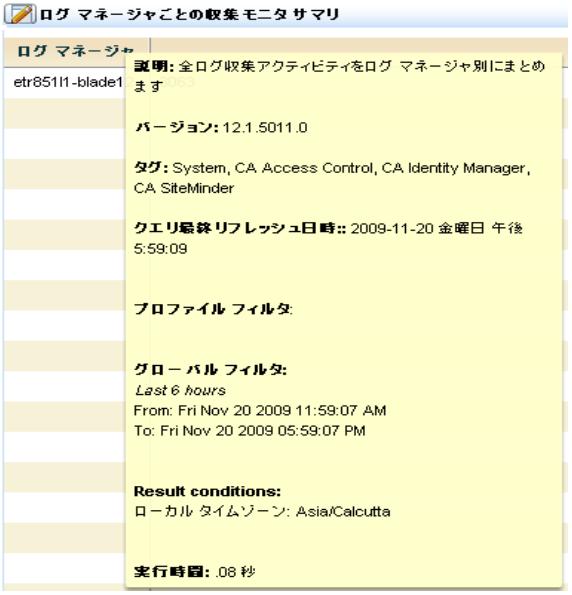
   有効な、つまりアクティブなボタンはカラーで表示されます。 たとえば、ユーザとアクセスの管理の管理者には、[アクセス フィルタ リスト]ボタンがカラーで表示されます。

   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。

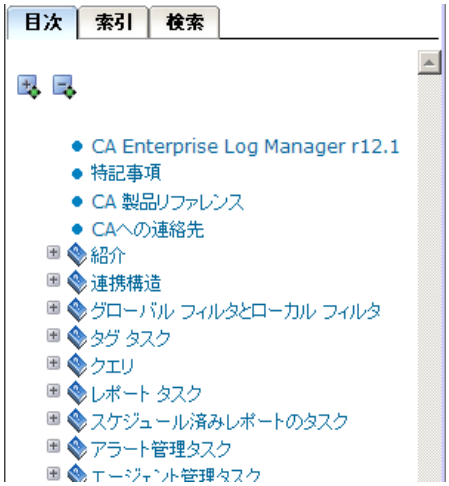
オンライン ヘルプの表示

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

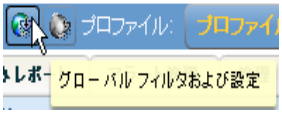
1. ツールバーの[ヘルプ]リンクをクリックし、CA Enterprise Log Manager のオンライン ヘルプ システムを表示します。

CA Enterprise Log Manager 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。

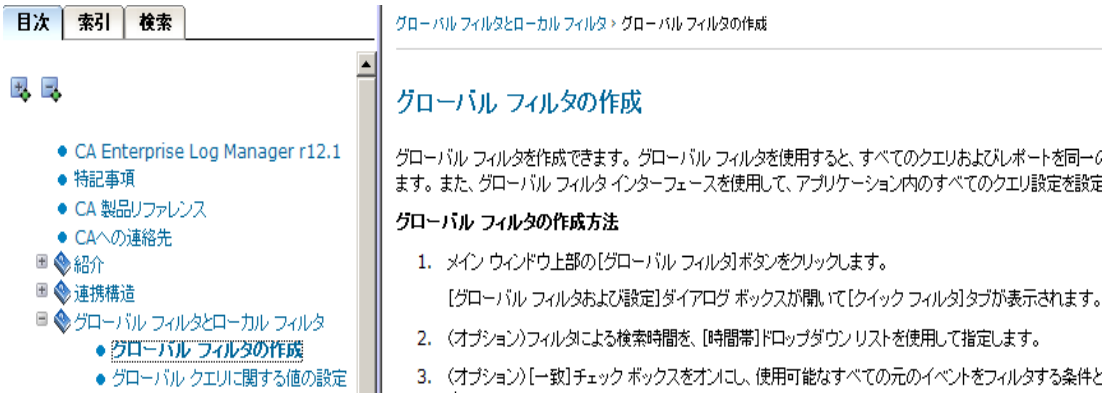
   a. [グローバル フィルタの表示/編集]ボタンをクリックします。

   [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 Enterprise Log Manager 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。

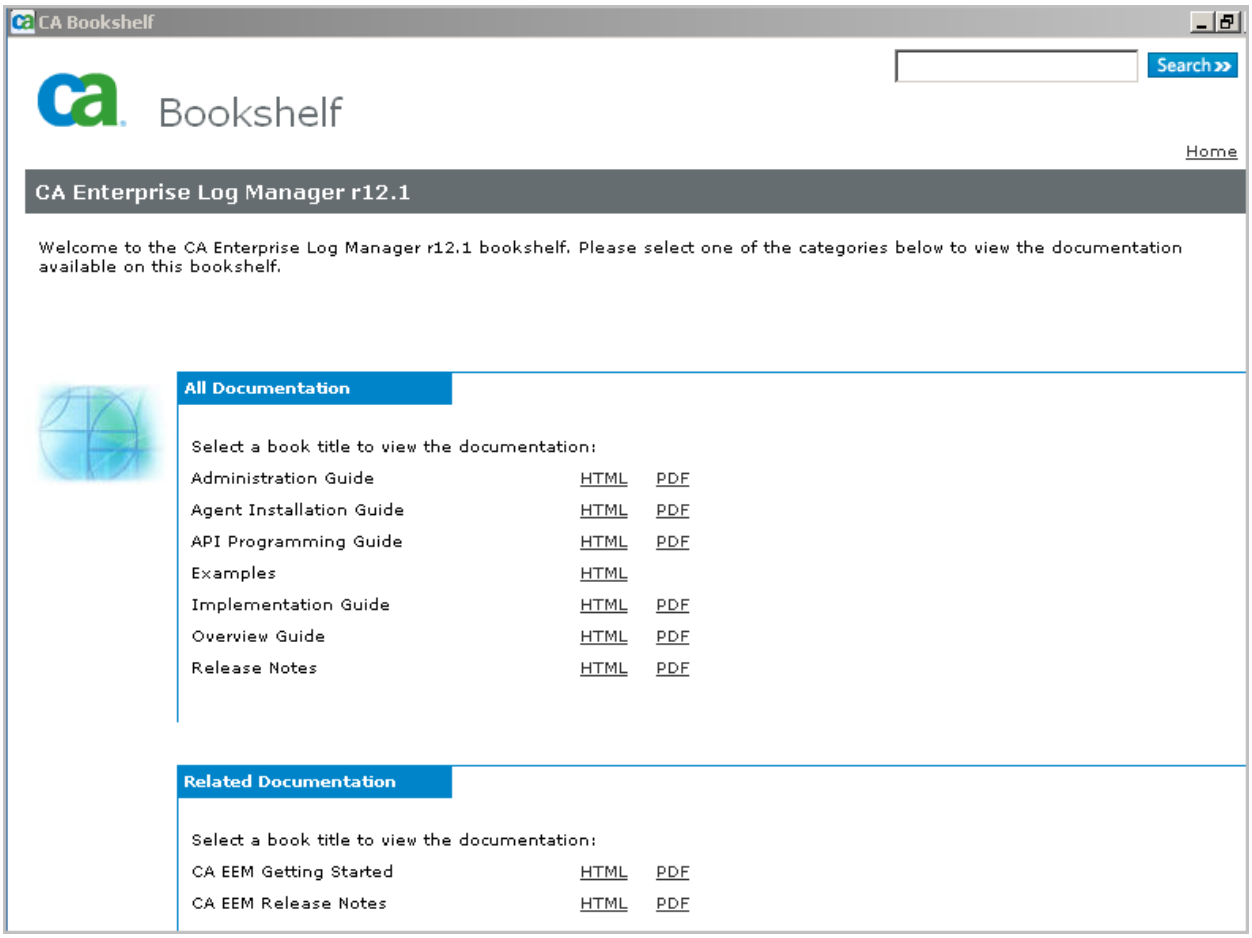
ドキュメントのマニュアル選択メニューによる検索

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。

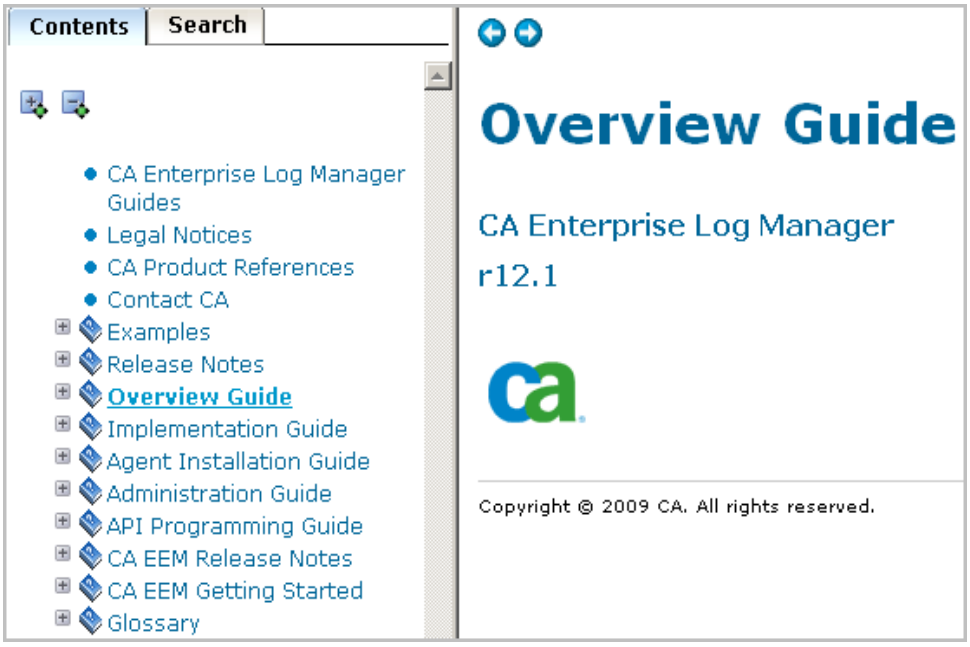
   次のようなページが表示されます。



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 Enterprise Log Manager 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。



用語集

(ダウンロードする)モジュール

モジュールは、サブスクリプションを通じてダウンロードが可能になるコンポーネント更新の論理グループです。 モジュールは、バイナリ更新またはコンテンツ更新、あるいはその両方を含む場合があります。 たとえば、すべてのレポートから構成されるモジュールもあれば、すべてのスポンサー バイナリ更新から構成されるモジュールもあります。 CA によって、各モジュールの構成要素が定義されます。

○証明書

CA Enterprise Log Manager によって使用される定義済みの証明書は、CAELMCert.cer と CAELM_AgentCert.cer です。 すべての CA Enterprise Log Manager サービスは、CAELMCert.cer を使用して管理サーバと通信します。 すべてのエージェントは、CAELM_AgentCert.cer を使用してそれぞれの収集サーバと通信します。

Administrator ロール

Administrator ロールは、すべての CA Enterprise Log Manager リソースへのすべての有効なアクションを実行する権限をユーザに付与します。 Administrator だけが、ログ収集およびサービスの設定や、ユーザ、アクセス ポリシー、およびアクセス フィルタの管理を許可されます。

Analyst ロール

Analyst ロールは、カスタム レポートおよびカスタム クエリの作成および編集、レポートの編集および注釈付け、タグの作成、レポートおよびアクション アラートのスケジュールを実行する権限をユーザに付与します。 Analyst は、すべての Auditor タスクも実行できます。

AppObjects

AppObjects、すなわちアプリケーション オブジェクトは、特定の製品のアプリケーション インスタンス下にある CA EEM に格納された製品固有のリソースです。 CAELM アプリケーション インスタンスの場合、これらのリソースには、レポートおよびクエリのコンテンツ、レポートおよびアラート用のスケジュール済みジョブ、エージェントのコンテンツおよび設定、サービス、アダプタ、および統合の設定、データ マッピングファイルおよびメッセージ解析ファイル、抑制ルールおよび集約ルールが含まれます。

Auditor ロール

Auditor ロールは、レポートおよびレポートに格納されているデータへのアクセス権をユーザに付与します。 Auditor は、レポート、レポート テンプレート リスト、スケジュール済みレポート ジョブ リスト、作成済みレポート リストを表示できます。 Auditor はレポートをスケジュールし、レポートに注釈を追加できます。 アクション アラートを表示する際に認証は不要と設定されていない限り、Auditor には RSS (Rich Site Summary)フィードへのアクセス権はありません。

CA Embedded Entitlements Manager の URL

CA Embedded Entitlements Manager（CA EEM）の URL は、https://<ip_address>:5250/spin/eiam です。 ログインするには、アプリケーションとして CAELM を選択し、EiamAdmin ユーザ名に関連付けられたパスワードを入力します。

CA Enterprise Log Manager

CA Enterprise Log Manager は、さまざまなタイプの広く分散したイベント ソースからログを収集し、クエリおよびレポートの準拠状況をチェックし、外部の長期用ストレージに移動した圧縮済みログのデータベースを記録するのに役立ちます。

CA Enterprise Log Manager の URL

CA Enterprise Log Manager の URL は、https://<ip_address>:5250/spin/calm です。 ログインするには、管理者によってアカウントに定義されたユーザ名および関連するパスワードを入力します。 または、デフォルトのスーパーユーザ名 EiamAdmin および関連するパスワードを入力します。

CA IT PAM

CA IT PAM は、CA IT Process Automation Manager の略です。 この CA 製品は、定義されたプロセスを自動化するものです。 CA Enterprise Log Manager では 2 つのプロセスを使用します。CA Service Desk などのローカル製品のイベント/アラート出力プロセスを作成するプロセスと、キー設定済み値としてインポートできるリストを動的に生成するプロセスです。 統合には CA IT PAM r2.1 が必要です。

CA Spectrum

CA Spectrum はネットワーク障害管理製品で、CA Enterprise Log Manager に統合して、SNMP トラップの形で送信されるアラートの宛先として使用することができます。

CA アダプタ

CA アダプタは、iTechnology を介してネイティブにイベントを送信するソースに加えて、CA Audit クライアント、iRecorders、SAPI レコーダなどの CA Audit コンポーネントからイベントを受信する、リスナのグループです。

CA サブスクリプション サーバ

CA サブスクリプション サーバは、CA からのサブスクリプション更新のソースです。

CAELM

CAELM は、CA EEM が CA Enterprise Log Manager に使用するアプリケーション インスタンス名です。 CA Embedded Entitlements Manager 内の CA Enterprise Log Manager 機能を使用するには、URL https://<ip_address>:5250/spin/eiam/eiam.csp を入力し、アプリケーション名として CAELM を選択し、EiamAdmin ユーザのパスワードを入力します。

caelmadmin

caelmadmin ユーザ名およびパスワードは、ソフトウェア アプライアンスのオペレーティング システムにアクセスするのに必要な認証情報です。 caelmadmin ユーザ ID は、このオペレーティング システムのインストール中に作成されます。 インストーラは、ソフトウェア コンポーネントのインストール中に、CA EEM スーパーユーザ アカウント EiamAdmin 用のパスワードを指定する必要があります。 caelmadmin アカウントには、これと同じパスワードが割り当てられます。 サーバ管理者は、caelmadmin ユーザとして ssh でログインし、このデフォルトのパスワードを変更することをお勧めします。 管理者は root として ssh でログインできませんが、必要な場合には、ユーザを root に切り替えることができます。

caelmservice

caelmservice は、iGateway およびローカル CA EEM サービスを root 以外のユーザとして実行できるようにするサービス アカウントです。 caelmservice アカウントは、サブスクリプション更新と共にダウンロードされたオペレーティング システム更新をインストールするために使用されます。

CALM

CALM は、Alert、ArchiveQuery、calmTag、Data、EventGrouping、Integration、および Report の CA Enterprise Log Manager リソースを含んでいる事前定義済みリソース クラスです。 このリソース クラスで許されるアクションは、注釈付け（Report）、作成（Alert、calmTag、EventGrouping、Integration、および Report）、データ アクセス（Data）、実行（ArchiveQuery）、およびスケジュール（Alert、Report）です。

calmTag

calmTag は、特定のタグに属するレポートとクエリにユーザを制限するスコープ ポリシーを作成する際に使用される AppObject の名前付き属性です。 すべてのレポートおよびクエリは AppObjects で、属性は calmTag になります （これはリソース Tag と混同されないようにするためです）。

CALM アプリケーション アクセス ポリシー

CALM アプリケーション アクセス ポリシーは、CA Enterprise Log Manager にログインできるユーザを定義するアクセス制御リストタイプのスコープ ポリシーです。 デフォルトでは、（グループの）Administrator、（グループの）Analyst、および（グループの）Auditor がアクセスを許可されています。

CEG フィールド

CEG フィールドは、異なるイベント ソースからの元のイベントのフィールド表示を標準化するために使用されるラベルです。 イベント精製中に、CA Enterprise Log Manager によって、元のイベント メッセージが一連の名前/値のペアに解析され、その後、元のイベントの名前が標準の CEG フィールドにマップされます。 この精製によって、元のイベントからの CEG フィールドと値で構成された名前/値ペアが作成されます。 つまり、同一のデータ オブジェクトやネットワーク要素に対して使用されている、元のイベント内の異なるラベルが、元のイベントを精製する際に、同じ CEG フィールド名に変換されるわけです。 CEG フィールドは SNMP トラップに使用された MIB 内の OID にマップされます。

EEM ユーザ

EEM ユーザは、イベント ログ ストアの[自動アーカイブ]セクションで設定し、アーカイブ クエリの実行、アーカイブ データベースのカタログ再作成、LMArchive ユーティリティの実行、および検査用にアーカイブ データベースを復元する restore-ca-elm シェル スクリプトの実行が可能なユーザを指定します。 このユーザには、事前定義済みの Administrator ロール、またはデータベース リソースへの編集アクションを許可するカスタム ポリシーに関連付けられたカスタム ロールが割り当てられている必要があります。

EiamAdmin ユーザ名

EiamAdmin は、CA Enterprise Log Manager サーバのインストール実施者に割り当てられるデフォルトのスーパーユーザ名前です。 最初に CA Enterprise Log Manager ソフトウェアをインストールする際に、リモート CA EEM サーバがまだ存在していない場合は、インストーラが、このスーパーユーザ アカウント用のパスワードを作成します。 存在する場合は、インストーラが既存のパスワードを入力する必要があります。 ソフトウェア アプライアンスをインストールした後、インストーラは、ワークステーションからブラウザを開き、CA Enterprise Log Manager 用の URL を入力し、関連するパスワードを使用して EiamAdmin としてログインします。 この最初のユーザが、ユーザ ストアを設定し、パスワード ポリシーを作成し、Administrator ロールを持つ最初のユーザ アカウントを作成します。 必要に応じて、EiamAdmin ユーザは、CA EEM によって制御された操作を実行できます。

EPHI 関連のレポート

EPHI 関連のレポートは、HIPAA セキュリティに焦点を合わせたレポートです。EPHI は、Electronic Protected Health Information（電子保護健康情報）を表します。 これらのレポートは、作成、管理、または送信される患者関連の個人医療情報がすべて電子的に保護されていることを証明するのに役立ちます。

event_action

event_action は、CEG によって使用されるイベント正規化の第 4 レベルのイベント専用のフィールドです。 一般的なアクションについて記述します。 イベント アクションのタイプには、プロセスの開始、プロセスの停止、アプリケーション エラーがあります。

event_category

event_category は、CEG によって使用されるイベント正規化の第 2 のレベルのイベント専用フィールドです。 これによって、特定の ideal_model を備えたイベントをさらに分類できます。 イベント カテゴリ タイプには、運用セキュリティ、ID 管理、設定管理、リソース アクセス、およびシステム アクセスがあります。

event_class

event_class は、CEG によって使用されるイベント正規化の第 3 レベルのイベント専用のフィールドです。 これによって、特定の event_category 内のイベントをさらに分類できます。

HTTP プロキシ サーバ

HTTP プロキシ サーバは、ファイアウォールと同様の働きをするプロキシ サーバで、インターネット トラフィックがプロキシ経由でない企業への出入りを阻止します。 送信トラフィックは、ID およびパスワードを指定して、プロキシ サーバをバイパスできます。 サブスクリプション管理でローカル HTTP プロキシ サーバを使用するかどうかを設定できます。

ID

CA Enterprise Log Manager の ID は、CAELM アプリケーション インスタンスおよびそのリソースへのアクセスが許可されるユーザまたはグループです。 CA 製品用の ID は、グローバル ユーザ、アプリケーション ユーザ、グローバル グループ、アプリケーション グループ、動的グループのいずれかです。

ID アクセス制御リスト

ID アクセス制御リストを使用すると、選択した ID が選択した各リソースに実行できるさまざまなアクションを指定できます。 たとえば、 ID アクセス制御リストを使用して、ある ID にレポートの作成を許可し、別の ID にレポートのスケジュールおよび注釈付けを許可することができます。 ID アクセス制御リストは、リソース中心ではなく ID 中心という点でアクセス制御リストと異なります。

ideal_model

ideal_model は、イベントを表現するテクノロジを表します。 これは、イベントの分類および正規化に使用されるフィールドの階層内で最初の CEG フィールドです。 推奨されるモデルの例には、アンチウイルス、DBMS、ファイアウォール、オペレーティング システム、Web サーバがあります。 Check Point、Cisco PIX、Netscreen/Juniper のファイアウォール製品は、フィールド「ideal_model」では「ファイアウォール」の値を使用して正規化されます。

iTech イベント プラグイン

iTech イベント プラグインは、選択したマッピング ファイルを使用して管理者が設定できる CA アダプタです。 リモート iRecorders、CA EEM、iTechnology 自身、または iTechnology を介してイベントを送信する製品からイベントを受信します。

LMArchive ユーティリティ

LMArchive ユーティリティは、CA Enterprise Log Manager サーバ上のイベント ログ ストアに対するアーカイブ済みデータベースのバックアップおよび復元を追跡するコマンド ライン ユーティリティです。 LMArchive を使用して、アーカイブが可能なウォーム データベース ファイルのリストを照会します。 リスト表示されたデータベースをバックアップし、長期的な(コールド)ストレージに移動させた後、このデータベースがバックアップされた CA Enterprise Log Manager に関する記録を作成する際にも LMArchive を使用します。 元の CA Enterprise Log Manager にコールド データベースを復元した後には、LMArchive を使用して CA Enterprise Log Manager に通知します。そこで、CA Enterprise Log Manager によってコールド データベース ファイルがクエリ可能な解凍済み状態に変更されます。

LMSEOSImport ユーティリティ

LMSEOSImport ユーティリティは、監査レポータ、ビューア、または監査コレクタからデータを移行する過程で、SEOSDATA (既存イベント)を CA Enterprise Log Manager にインポートするために使用されるコマンド ライン ユーティリティです。 このユーティリティは、Microsoft Windows および Sun Solaris Sparc 上でのみサポートされています。

MIB (management information base、管理情報ベース)

CA Enterprise Log Manager 用 MIB (management information base)である CA-ELM.MIB は、CA Enterprise Log Manager から SNMP トラップという形でアラートを受信する製品でインポートされコンパイルされる必要があります。 MIB では、SNMP トラップ メッセージで使用される各数値オブジェクト識別子(OID)の源が、そのデータ オブジェクトやネットワーク要素の説明と共に示されます。 CA Enterprise Log Manager によって送信された SNMP トラップの MIB では、各データ オブジェクトの説明は、関連する CEG フィールド用になっています。 MIB を使用すると、SNMP トラップで送信されたすべての名前/値ペアが、宛先で正しく解釈されるようになります。

NIST

アメリカ国立標準技術研究所(NIST)は、CA Enterprise Log Manager のベースとして使用された特別文書 800-92「Guide to Computer Security Log Management」で推奨事項を提供している米国連邦政府の科学技術機関です。

ODBC および JDBC のアクセス

CA Enterprise Log Manager イベント ログ ストアへの ODBC および JDBC のアクセスでは、サード パーティ レポート ツールを使用したカスタム イベントのレポートや、相関エンジンを使用したイベントの相関、侵入やマルウェアの検知製品を使用したイベント評価など、各種サード パーティ製品でのイベント データの使用をサポートしています。 Windows オペレーティング システムを備えたシステムでは、ODBC アクセスを使用します。UNIX や Linux オペレーティング システムを備えたシステムでは、JDBC アクセスを使用します。

ODBC サーバ

ODBC サーバは、ODBC や JDBC のクライアントと、CA Enterprise Log Manager サーバ間の通信に使用されるポートを設定し、SSL 暗号化を使用するべきかどうかを指定する設定済みサービスです。

OID（オブジェクト識別子）

OID（オブジェクト識別子）は、SNMP トラップ メッセージ内で値とペアになっているデータ オブジェクトの一意の数値識別子です。 CA Enterprise Log Manager によって送信された SNMP トラップ内で使用されている各 OID は、MIB 内のテキスト形式の CEG フィールドにマップされます。 CEG フィールドにマップされた OID の構文は、「1.3.6.1.4.1.791.9845.x.x.x、791」のようになっています。791 は CA の企業番号、9845 は CA Enterprise Log Manager の製品識別子です。

pozFolder

pozFolder は、AppObject の属性で、値は AppObject の親パスです。 pozFolder 属性および値は、レポート、クエリ、設定などのリソースへのアクセスを制限するアクセス ポリシー用フィルタで使用されます。

RSS イベント

RSS イベントは、サードパーティ製品やユーザにアクション アラートを送信するために CA Enterprise Log Manager によって生成されるイベントです。 このイベントは、各アクション アラート結果のサマリであり、結果ファイルへのリンクでもあります。 指定した RSS フィード項目の期間は設定可能です。

SafeObject

SafeObject は、CA EEM 内の事前定義済みリソース クラスです。 アプリケーションのスコープ下に保存された AppObjects が属するリソース クラスです。 AppObjects へのアクセスを許可するポリシーおよびフィルタを定義するユーザは、このリソース クラスを参照します。

SAPI コレクタ

SAPI コレクタは、CA Audit クライアントからイベントを受信する CA アダプタです。 CA Audit クライアントは、組み込みのフェイルオーバーを提供するコレクタ アクションを使用して通信します。 管理者は、選択した暗号および DM ファイルなどを使用して、CA Audit SAPI コレクタを設定します。

SAPI ルータ

SAPI ルータは、メインフレームなどの、統合からイベントを受信し、CA Audit ルータに送信する CA アダプタです。

SAPI レコーダ

SAPI レコーダは、iTechnology 以前に CA Audit に情報を送信するために使用されていた技術です。 SAPI は、Submit API（アプリケーション プログラミング インターフェース）を表しています。 SAPI レコーダの例としては、CA ACF2、CA Top Secret、RACF、Oracle、Sybase、DB2 用の CA Audit レコーダがあります。

scp ユーティリティ

scp セキュア コピー(リモート ファイル コピー プログラム)は、ネットワーク上の UNIX コンピュータ間でファイルを転送する UNIX ユーティリティです。 このユーティリティは、オンライン サブスクリプション プロキシからオフライン サブスクリプション プロキシにサブスクリプション更新ファイルを転送する際に使用できるよう、CA Enterprise Log Manager のインストール時に利用可能になります。

SNMP

SNMP は、Simple Network Management Protocol の頭字語で、エージェント システムから 1 つ以上の管理システムにアラート メッセージを SNMP トラップという形で送信するためのオープン スタンダードです。

SNMP トラップの宛先

アクション アラートをスケジュールする際に、1 つ以上の SNMP トラップの宛先は追加できます。 各 SNMP トラップの宛先には、IP アドレスとポートが設定されています。宛先は、通常 CA Spectrum や CA NSM などの NOC または管理サーバです。SNMP トラップは、スケジュールしたアラート ジョブのクエリによって結果が返されたときに、設定した宛先に送信されます。

SNMP トラップの内容

SNMP トラップは名前/値ペアで構成されます。各名前は OID (オブジェクト識別子)、各値はスケジュールしたアラートから返される値です。 アクション アラートから返されるクエリ結果は、CEG フィールドと値で構成されています。 SNMP トラップは、この名前/値ペアの名前に使用されている CEG フィールドを OID に置換して、生成されます。各 CEG フィールドの OID へのマッピングは、MIB に格納されています。 SNMP トラップには、アラートを設定する際に選択したフィールドの名前/値ペアが含まれます。

XMP ファイル分析

XMP ファイル分析は、メッセージ解析ユーティリティによって実行されるプロセスです。このプロセスでは、各事前一致文字列が含まれるすべてのイベントを検索し、一致したイベントを 1 つずつ解析して、同じ事前一致文字列を使用していると判明した最初のフィルタを使用しているイベントをトークンに変換します。

アーカイブ カタログ

「カタログ」を参照してください。

アーカイブ クエリ

アーカイブ クエリは、クエリを実行するために、復元して解凍する必要のあるコールド データベースを特定する際に使用されるカタログへのクエリです。 通常のクエリがホット データベース、ウォーム データベース、および解凍済みデータベースをターゲットにするのに対して、アーカイブ クエリは、コールド データベースをターゲットにするという点で、通常のクエリと異なります。 管理者は、[管理]タブ -[ログ収集]サブタブ -[カタログ クエリのアーカイブ]オプションから、アーカイブ クエリを発行できます。

アーカイブ ログ

ログ アーカイブは、ホット データベースが最大サイズに到達すると発生するプロセスで、このとき、行レベルで圧縮が実行され、状態がホットからウォームに変更されます。 削除のしきい値に達する前に、管理者は手動でウォーム データベースをバックアップし、LMArchive ユーティリティを実行して、バックアップ名を記録する必要があります。 その後に、この情報はアーカイブ クエリによって表示できるようになります。

アーカイブ済みデータベース

ある CA Enterprise Log Manager サーバ上で「アーカイブ済みデータベース」に含まれるデータベースとは、クエリの実行が可能だが有効期限が切れる前に手動でバックアップする必要があるすべてのウォーム データベース、バックアップ済みとして記録されているすべてのコールド データベース、およびバックアップから復元済みとして記録されているすべてのデータベースです。

アカウント

アカウントは、CALM アプリケーション ユーザでもあるグローバル ユーザです。 1 人の人が、1 つ以上のアカウントを持ち、それぞれに異なるユーザ定義ロールを設定することができます。

アクション アラート用の RSS フィード URL

アクション アラート用の RSS フィード URL は、https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp です。 この URL から、有効期間およびデータ量の最大値の設定に従ってアクション アラートを表示できます。

アクション クエリ

アクション クエリは、アクション アラートをサポートするクエリです。 アクション クエリは、繰り返しのスケジュールで実行され、関連付けられているアクション アラートによって規定された条件に対してテストします。

アクション アラート

アクション アラートは、スケジュール済みのクエリ ジョブです。ポリシー違反、使用状況、ログイン パターンなど、近い将来に注意が必要となるイベント アクションを検出するために使用できます。 デフォルトでは、アラート クエリから結果が返されたときに、CA Enterprise Log Manager［アラート］ページに結果が表示され、RSS フィードにも追加されます。 アラートをスケジュールする際に、電子メール、CA IT PAM イベント/アラート出力プロセス、SNMP トラップなどの宛先を追加指定できます。

アクセス フィルタ

アクセス フィルタは、管理者以外のユーザまたはグループが表示できるイベント データを制御するために、管理者が設定できるフィルタです。 たとえば、アクセス フィルタを設定して、指定した ID がレポートに表示できるデータを制限できます。 アクセス フィルタは自動的に責任ポリシーに変換されます。

アクセス ポリシー

アクセス ポリシーは、アプリケーション リソースへの ID（ユーザまたはユーザ グループ）のアクセス権を許可または拒否するルールです。 CA Enterprise Log Manager は、ID、リソース、リソース クラスを照合し、フィルタを評価して、特定のユーザにポリシーを適用するかどうかを決定します。

アプリケーション ユーザ

アプリケーション ユーザは、アプリケーション レベルの詳細を割り当てられたグローバル ユーザです。 CA Enterprise Log Manager アプリケーション ユーザの詳細には、ユーザ グループおよびアクセスへのすべての制限が含まれています。 ユーザ ストアがローカル リポジトリである場合、アプリケーション ユーザの詳細には、ログオン認証情報およびパスワード ポリシーも含まれています。

アプリケーション リソース

アプリケーション リソースは、CALM アクセス ポリシーによって、特定の ID に対する、作成、スケジュール、編集といったアプリケーション固有のアクションの実行が許可または拒否される CA Enterprise Log Manager 固有のリソースです。 たとえば、レポート、アラート、統合などがあります。 「グローバル リソース」も参照してください。

アプリケーション インスタンス

アプリケーション インスタンスは、すべての許可ポリシー、ユーザ、グループ、コンテンツ、および設定が格納されている CA EEM リポジトリ内の共用領域です。 通常、企業内のすべての CA Enterprise Log Manager サーバは、同じアプリケーション インスタンス（デフォルトでは CAELM）を使用します。 複数のアプリケーション インスタンスを備えた CA Enterprise Log Manager サーバをインストールできますが、連携できるのは、同じアプリケーション インスタンスを共有するサーバのみです。 同じ CA EEM サーバを使用するよう設定され、複数のアプリケーション インスタンスを備えたサーバでは、ユーザ ストア、パスワード ポリシー、およびグローバル グループのみが共有されます。複数の CA 製品には、複数のデフォルトのアプリケーション インスタンスがあります。

アプリケーション グループ

アプリケーション グループは、グローバル ユーザに割り当てることができる製品固有のグループです。 CA Enterprise Log Manager で使用される事前定義済みアプリケーション グループ、すなわちロールとは、Administrator、Analyst、および Auditor です。これらのアプリケーション グループ、は CA Enterprise Log Manager ユーザのみが使用できます。同じ CA EEM サーバに登録されたほかの製品のユーザへの割り当てには利用できません。 ユーザ定義アプリケーション グループは、そのユーザが CA Enterprise Log Manager にアクセスできるように、 CALM アプリケーション アクセス デフォルト ポリシーに追加する必要があります。

アラート サーバ

アラート サーバは、アクション アラートおよびアクション アラート ジョブ用のストアです。

イベント

CA Enterprise Log Manager の中のイベントは、指定した各イベント ソースによって生成されたログ レコードです。

イベント ログ ストレージ

イベント ログ ストレージは、アーカイブ処理の結果です。この処理では、ユーザがウォーム データベースをバックアップし、LMArchive ユーティリティを実行して CA Enterprise Log Manager に通知し、バックアップ済みデータベースをイベント ログ ストアから長期用ストレージに移動させます。

イベント/アラート出力プロセス

イベント/アラート出力プロセスは、CA Enterprise Log Manager で設定されたアラート データに応答するサードパーティ製品を呼び出す CA IT PAM プロセスです。 アラート ジョブをスケジュールする際に、宛先として CA IT PAM プロセスを選択できます。 CA IT PAM プロセスがアラートによって実行されると、CA Enterprise Log Manager によって CA IT PAM アラート データが送信され、CA IT PAM によって、イベント/アラート出力プロセスの一環として、アラート データが独自のプロセス パラメータと共にサード パーティ製品に転送されます。

イベント カテゴリ

イベント カテゴリは、CA Enterprise Log Manager によって使用されるタグで、イベント ストアに挿入する前にイベントを機能によって分類するためのものです。

イベント ソース

イベント ソースは、コネクタによるイベント収集元となるホストです。 イベント ソースに複数のログ ストアが含まれ、各ログ ストアが個別のコネクタによってアクセスされる場合があります。 新しいコネクタの展開には、通常、イベント ソースを設定する作業が伴います。エージェントがイベントソースにアクセスし、ログ ストアの 1 つから元のイベントを読み取れるように設定する必要があります。 オペレーティング システム、複数のデータベース、およびさまざまなセキュリティ アプリケーションのそれぞれの元のイベントが、イベント ソース上に別々に格納されます。

イベント転送ルール

イベント転送ルールによって、選択したイベントを、イベント ログ ストアへの保存後に、イベントの関連付けなどを行うサード パーティ製品に転送するよう指定します。

イベントの集約

イベント集約は、類似する複数のログ エントリを、イベント発生数が格納された単一のエントリに統合するプロセスです。 集約ルールによって、イベントの集約方法が定義されます。

イベント フィルタリング

イベント フィルタリングは、CEG フィルタに基づいてイベントを除外するプロセスです。

イベント ログ ストア

イベント ログ ストアは、受信イベントがデータベースに格納される CA Enterprise Log Manager サーバ上のコンポーネントです。 イベント ログ ストア内のデータベースは、手動でバックアップし、設定された削除時間に達する前に、リモート ログ ストレージ ソリューションに移動する必要があります。 アーカイブされたデータベースは、イベント ログ ストアに復元できます。

イベント収集

イベント収集は、元のイベント文字列をイベント ソースから読み取り、設定された CA Enterprise Log Manager に送信するプロセスです。 イベント収集の後に、イベント精製が実行されます。

イベント精製

イベント精製は、収集された元のイベント文字列が、構成要素のイベント フィールドに解析され、CEG フィールドにマッピングされるプロセスです。 クエリを実行して、結果として精製済みイベント データを表示できます。 イベント精製は、イベントの収集後、イベントの格納の前に実行されます。

イベント精製ライブラリ

イベント精製ライブラリは、事前定義済みおよびユーザ定義の統合、マッピング ファイルおよび解析ファイル、抑制ルールおよび集約ルールのストアです。

インストーラ

インストーラは、ソフトウェア アプライアンスとエージェントをインストールする個人です。インストール処理中に、caelmadmin と EiamAdmin というユーザ名が作成され、EiamAdmin に指定されたパスワードが、caelmadmin に割り当てられます。 これらの caelmadmin 認証情報は、オペレーティング システムに最初にアクセスする際に必要となります。EiamAdmin 認証情報は、CA Enterprise Log Manager ソフトウェアに最初にアクセスする際、およびエージェントをインストール際に必要になります。

ウォーム データベース状態

ウォーム データベース状態は、ホット データベースのサイズ(最大行数)を超えたとき、または新規イベントログ ストアへのコールド データベースの復元後にカタログ再作成が実行されたときに、イベント ログのホット データベースが移行する状態です。 ウォーム データベースは、経過日数が[アーカイブの最大日数]に設定された値を超えるまで、イベント ログ ストア内で圧縮されて保持されます。 ホット、ウォーム、および解凍済みの状態のデータベースに含まれるイベント ログにクエリを実行できます。

エージェント

エージェントは、コネクタによって設定される汎用サービスであり、それぞれが単一のイベント ソースから元のイベントを収集して、処理のために CA Enterprise Log Manager に送信します。 各 CA Enterprise Log Manager に、エージェントが 1 つ組み込まれています。 また、リモート収集ポイント上にエージェントをインストールし、エージェントをインストールできないホスト上のイベントを収集できます。 さらに、イベント ソースが実行されているホスト上にエージェントをインストールすると、抑制ルールの適用や CA Enterprise Log Manager への転送の暗号化などのメリットが得られます。

エージェント エクスプローラ

エージェント エクスプローラは、エージェント設定用のストアです（エージェントは、収集ポイント上、またはイベント ソースが存在するエンドポイント上にインストールできます）。

エージェント グループ

エージェント グループは、選択したエージェントに適用できるタグです。これによって、複数のエージェントに同時にエージェント設定を適用し、グループに基づいたレポートを取得することができます。 特定のエージェントは、一度に 1 つのグループにしか所属できません。 エージェント グループは、地理的地域や重要度など、ユーザ定義の基準をベースにします。

エージェント管理

エージェント管理は、連携されたすべての CA Enterprise Log Manager に関連付けられたすべてのエージェントを制御するソフトウェア プロセスです。 これによって、通信相手のエージェントが認証されます。

カタログ

カタログは、アーカイブされたデータベースの状態を管理する各 CA Enterprise Log Manager 上に格納されたデータベースで、すべてのデータベースについての高機能なインデックスとしても機能します。 状態情報（ウォーム、コールド、または解凍済み）には、これまでにこの CA Enterprise Log Manager 上に存在したすべてのデータベース、および解凍済みデータベースとしてこの CA Enterprise Log Manager に復元されたすべてのデータベースの状態が保持されます。 インデックス機能は、この CA Enterprise Log Manager 上のイベント ログ ストア内にあるすべてのホットおよびウォーム データベースを対象とします。

カタログ再作成

カタログ再作成は、強制的なカタログの再構築です。 カタログ再作成は、データが作成されたサーバとは異なるサーバ上のイベント ログ ストアにデータを復元する場合にのみ必要になります。 たとえば、CA Enterprise Log Manager の 1 つを、コールド データの調査用復元ポイントとして機能するよう指定すると、指定した復元ポイントにデータベースを復元した後、強制的なデータベースのカタログ再作成が必要になります。 必要な場合は、iGateway が再起動されたときに、カタログ再作成が自動的に実行されます。 単一のデータベース ファイルのカタログ再作成に、数時間かかる場合があります。

カレンダ

カレンダは、アクセス ポリシーが有効である時間を制限するための手段です。 ポリシーによって、指定した時間の、指定したリソースに対する指定したアクションの実行が、指定した ID に許可されます。

監査レコード

監査レコードには、認証の試行、ファイルへのアクセス、およびセキュリティ ポリシーや、ユーザ アカウント、権限への変更などの、セキュリティ イベントが記録されます。 管理者は、監査が必要なイベントのタイプ、およびログ記録の対象を指定します。

関数マッピング

関数マッピングは、製品統合用のデータ マッピング ファイルのオプション部分です。関数マッピングは、ソース イベントから必要な値を直接取得できない場合に CEG フィールドを挿入するために使用されます。 すべての関数マッピングは、CEG フィールド名、事前定義済みフィールド値またはクラス フィールド値、および値を取得または計算する際に使用される関数から構成されます。

キー値

キー値は、ユーザ定義値に割り当てられたユーザ定義リスト(キー グループ)です。 クエリがキー グループを使用する場合、検索結果には、キー グループ内のキー値のいずれかに一致するものが含まれます。 事前定義済みキー グループは複数あり、その中には事前定義済みキー値が含まれているものもあります。事前定義済みキー値は、事前定義済みクエリおよびレポートの中で使用されます。

クエリ

クエリは、アクティブな CA Enterprise Log Manager サーバ、および、指定した場合にはその連携サーバの、イベント ログ ストアを検索する際に使用される条件のセットです。クエリは、クエリの WHERE 句内で指定されたホット、ウォーム、または解凍済みデータベースをターゲットにします。 たとえば、WHERE 句によって、ある時間帯に source_username="myname" であるイベントにクエリが制限されていて、カタログ データベースに格納されている情報に基づくと、この条件に一致するレコードが 1000 個のデータベースのうち 10 にしか格納されていない場合、クエリはその 10 のデータベースに対してのみ実行されます。 クエリは、データの行を最大 5000 まで返すことができます。 事前定義済みロールを持つすべてのユーザが、クエリを実行できます。 Analyst および Administrator だけが、アクション アラートを配布するためのクエリのスケジュール、含めるクエリの選択によるレポートの作成、またはクエリの設計ウィザードを使用したカスタムクエリの作成を実行できます。 「アーカイブ クエリ」も参照してください。

クエリ ライブラリ

クエリ ライブラリは、事前定義済みおよびユーザ定義のクエリ、クエリ タグ、およびプロンプト フィルタをすべて格納するライブラリです。

グローバル グループ

グローバル グループは、同じ CA Enterprise Log Manager 管理サーバに登録されたアプリケーション インスタンス間で共有されるグループです。 すべてのユーザは、1 つ以上のグループに割り当てることができます。 アクセス ポリシーを定義する際に、選択したリソースに選択したアクションを実行する権限を許可または拒否された ID としてグローバル グループを使用できます。

グローバル設定

グローバル設定は、同じ管理サーバを使用するすべての CA Enterprise Log Manager サーバに適用される一連の設定です。

グローバル フィルタ

グローバル フィルタは、すべてのレポートの表示内容を制限するために指定できる条件のセットです。 たとえば、「過去 7 日間」というグローバル フィルタでは、過去 7 日間に生成されたイベントがレポートされます。

グローバル ユーザ

グローバル ユーザは、アプリケーション固有の詳細を除いたユーザ アカウント情報です。 グローバル ユーザの詳細およびグローバル グループ メンバシップは、デフォルトのユーザ ストアに統合されるすべての CA アプリケーションで共有されます。 グローバル ユーザの詳細は、組み込みリポジトリまたは外部ディレクトリに保存できます。

グローバル リソース

CA Enterprise Log Manager 製品のグローバル リソースは、ほかの CA アプリケーションと共有されるリソースです。 グローバル リソースに関するスコープ ポリシーを作成できます。 たとえば、ユーザ、ポリシー、カレンダなどがあります。「アプリケーション リソース」も参照してください。

コールド データベース状態

管理者が LMArchive ユーティリティを実行して、データベースがバックアップされたことを CA Enterprise Log Manager に通知すると、ウォーム データベースに、コールド データベース状態が適用されます。 管理者は、削除される前に、ウォーム データベースをバックアップし、このユーティリティを実行する必要があります。 ウォームデータベースは、経過日数が[アーカイブの最大日数]を超えたときか、設定された[アーカイブ ディスク領域]しきい値に達したときの、どちらか早いほうが発生したときに、自動的に削除されます。 アーカイブ データベースにクエリを実行し、ウォーム状態およびコールド状態にあるデータベースを特定することができます。

コネクタ

コネクタは、特定のエージェント上に設定された特定のイベント ソース用の統合です。 エージェントは、似たタイプまたは異なったタイプの複数のコネクタをメモリにロードできます。 コネクタによって、イベント ソースから元のイベントを収集したり、変換されたイベントをルールに基づいてイベント ログ ストアに転送して、ホット データベースに挿入したりすることが可能になります。 あらかじめ用意されている統合を使用すると、オペレーティング システム、データベース、Web サーバ、ファイアウォール、多種多様なセキュリティ アプリケーションなど、さまざまなタイプのイベント ソースからの収集を最適化することができます。 ゼロから、または統合をテンプレートとして使用して、独自に作成したイベント ソース用のコネクタを定義できます。

コンテンツ更新

コンテンツ更新は、CA Enterprise Log Manager 管理サーバ内に格納されているサブスクリプション更新の非バイナリ部分です。 コンテンツ更新には、XMP ファイル、DM ファイル、CA Enterprise Log Manager モジュール用の設定更新、公開鍵更新などのコンテンツが含まれています。

コンピュータ セキュリティ ログ管理

コンピュータ セキュリティ ログ管理は、NIST によって、「コンピュータ セキュリティ ログ データの生成、転送、格納、分析、および処理するプロセス」と定義されています。

サービス

CA Enterprise Log Manager サービスは、イベント ログ ストア、レポート サーバ、およびサブスクリプションです。 管理者はこれらのサービスをグローバル レベルで設定します。デフォルトで、すべての設定がすべての CA Enterprise Log Manager に適用されます。 サービスの大部分のグローバル設定は、ローカル レベルで、すなわち、指定されている CA Enterprise Log Manager について変更される可能性があります。

サブスクリプション クライアント

サブスクリプション クライアントは、サブスクリプション プロキシ サーバと呼ばれる別の CA Enterprise Log Manager サーバからコンテンツ更新を取得する CA Enterprise Log Manager サーバです。 サブスクリプション クライアントでは、設定されたサブスクリプション プロキシ サーバを定期的にポーリングし、利用可能な場合には新しい更新を取得します。 更新を取得したら、ダウンロードされたコンポーネントがクライアントによってインストールされます。

サブスクリプション プロキシ（オフライン）

オフライン サブスクリプション プロキシは、オンライン サブスクリプション プロキシから手動のディレクトリ コピー（scp を使用）によってサブスクリプション更新を取得する CA Enterprise Log Manager サーバです。 オフライン サブスクリプション プロキシは、要求しているクライアントにバイナリ更新をダウンロードし、コンテンツ更新の最新バージョンをまだ受信していない管理サーバに更新を送信するように設定できます。 オフライン サブスクリプション プロキシは、インターネットにアクセスする必要はありません。

サブスクリプション プロキシ（オンライン）

オンライン サブスクリプション プロキシは、インターネット アクセス権を持つ CA Enterprise Log Manager で、CA サブスクリプション サーバからサブスクリプション更新を反復スケジュールで取得します。 特定のオンライン サブスクリプション プロキシに、1 つ以上のクライアント用のプロキシ リストを保存することができます。クライアントは、リストに挙げられたプロキシにラウンド ロビン方式で接続し、バイナリ更新を要求します。別のプロキシによってまだ送信されていない場合に、管理サーバに新しいコンテンツ更新および設定更新を送信するよう、特定のオンライン プロキシを設定することができます。 オンライン プロキシのサブスクリプション更新ディレクトリを選択して、オフライン サブスクリプション プロキシに更新をコピーするためのソースとして使用できます。

サブスクリプション プロキシ（クライアント用）

クライアント用のサブスクリプション プロキシは、クライアントが CA Enterprise Log Manager ソフトウェアおよびオペレーティング システムの更新を取得する際に、ラウンド ロビン方式で接続するサブスクリプション プロキシ リストを構成します。 あるプロキシがビジーな場合は、リスト内の次のプロキシに接続します。 すべてが使用不可で、クライアントがオンラインの場合には、デフォルトのサブスクリプション プロキシが使用されます。

サブスクリプション プロキシ(コンテンツ更新用)

コンテンツ更新用のサブスクリプション プロキシは、CA サブスクリプション サーバからダウンロードされるコンテンツ更新がある CA Enterprise Log Manager 管理サーバを更新するために選択されたサブスクリプション プロキシです。 冗長性を持たせるために複数のプロキシを設定することをお勧めします。

サブスクリプション プロキシ(デフォルト)

デフォルトのサブスクリプション プロキシは通常、最初にインストールされた CA Enterprise Log Manager サーバで、プライマリ CA Enterprise Log Manager である場合もあります。 デフォルトのサブスクリプション プロキシは、オンライン サブスクリプション プロキシでもあるため、インターネットにアクセスできる必要があります。 ほかにオンライン サブスクリプション プロキシが定義されていない場合、このサーバは、CA サブスクリプション サーバからサブスクリプション更新を取得し、すべてのクライアントにバイナリ更新をダウンロードし、CA EEM にコンテンツ更新を送信します。 ほかのプロキシが定義されている場合でも、このサーバはサブスクリプション更新を取得しますが、更新を取得するためにクライアントによって接続されるのは、サブスクリプション プロキシ リストが設定されていない場合、または設定されているリストをすべて使用した場合のみです。

サブスクリプション モジュール

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、すべての CA Enterprise Log Manager サーバおよびすべてのエージェントに自動的にダウンロードおよび配布されるようにするサービスです。 グローバル設定は、ローカル CA Enterprise Log Manager サーバに適用されます。ローカル設定には、サーバがオフライン プロキシ、オンライン プロキシ、サブスクリプション クライアントのどれであるか、などが含まれます。

サブスクリプション更新

サブスクリプション更新は、CA サブスクリプション サーバによって使用可能にされた、バイナリ ファイルおよび非バイナリ ファイルを指します。 バイナリ ファイルとは、通常、CA Enterprise Log Manager にインストールされる製品モジュール更新です。 非バイナリ ファイルは、コンテンツ更新を指し、管理サーバに保存されます。

サブスクリプション用の RSS フィード URL

サブスクリプション用の RSS フィード URL は、サブスクリプション更新を取得するプロセスでオンライン サブスクリプション プロキシ サーバによって使用される、あらかじめ設定されたリンクです。 この URL は、CA サブスクリプション サーバのものです。

自己監視イベント

自己監視イベントは、CA Enterprise Log Manager によってログに記録されるイベントです。 このようなイベントは、ログインしたユーザによって実行された操作や、サービスおよびリスナなどの各種モジュールによって実行された機能によって、自動的に生成されます。 SIM 操作自己監視イベントの詳細レポートは、レポート サーバを選択し、[自己監視イベント]タブを開いて、表示することができます。

スコープ ポリシー

スコープ ポリシーはアクセス ポリシーの一種で、AppObjects、ユーザ、グループ、フォルダ、ポリシーなど、管理サーバに保存されたリソースへのアクセスを許可または拒否します。 スコープ ポリシーでは、指定されたリソースにアクセスできる ID を定義します。

ソフトウェア アプライアンス

ソフトウェア アプライアンスには、オペレーティング システム コンポーネントおよび CA Enterprise Log Manager ソフトウェア コンポーネントが含まれます。

タグ

タグは、同じビジネス関連グループに属するクエリやレポートを識別するために使用する言葉またはキー フレーズです。 タグを使用すると、ビジネス関連グループに基づいた検索を実行できます。 なお、Tag は、ユーザにタグを作成する権限を付与するポリシー内で使用されるリソース名です。

直接ログ収集

直接ログ収集は、イベント ソースと CA Enterprise Log Manager ソフトウェアの間に中間エージェントがないログ収集方法です。

データ アクセス

データ アクセスは、CALM リソース クラスに関するデフォルト データ アクセス ポリシーによってすべての CA Enterprise Log Manager に付与された許可の一種です。 すべてのユーザは、データ アクセス フィルタによって制限された場所以外にあるすべてデータにアクセスできます。

データ マッピング（DM）

データ マッピングは、キー値ペアを CEG にマッピングするプロセスです。 データ マッピングは DM ファイルによって実行されます。

データ マッピング（DM）ファイル

データ マッピング（DM）ファイルは XML ファイルです。CA 共通イベント文法（CEG）を使用して、イベントをソース形式から、イベント ログ ストア内でのレポートや分析用として格納できる CEG 準拠形式に変換します。 イベント データを保存するには、ログ名ごとに 1 つの DM ファイルが必要になります。 ユーザは、DM ファイルのコピーを変更して、指定したコネクタに適用できます。

データベースの状態

データベースの状態には、新規イベントの圧縮されていないデータベースを指す「ホット」、圧縮されたイベントのデータベースを指す「ウォーム」、バックアップされたデータベースを指す「コールド」、および、バックアップ元のイベント ログ ストアに復元されたデータベースを指す「解凍済み」があります。 ホット データベース、ウォーム データベース、および解凍済みデータベースにクエリを実行できます。 アーカイブ クエリには、コールド データベースに関する情報が表示されます。

デフォルト エージェント

デフォルト エージェントは、CA Enterprise Log Manager サーバと共にインストールされる組み込みエージェントです。 syslog イベントに加えて、CA Access Control r12 SP1、Microsoft Active Directory 証明書サービス、Oracle9i データベースなど、syslog 以外の各種イベント ソースからのイベントの直接収集用に設定することができます。

デフロスティング

デフロスティングは、データベースの状態をコールドから解凍済みに変更するプロセスです。 既知のコールド データベースが復元されたことが LMArchive ユーティリティによって通知されると、CA Enterprise Log Manager によってこのプロセスが実行されます（コールド データベースを元の CA Enterprise Log Manager に復元しない場合は、LMArchive ユーティリティは使用しません。デフロスティングの必要はありません。カタログ再作成によって、復元されたデータベースがウォーム データベースとして追加されます）。

統合

統合は、クエリおよびレポートに表示できるように、未分類のイベントを精製済みイベントに加工する手段です。 統合は、特定のエージェントおよびコネクタが多種多様なイベント ソースの 1 つからイベントを収集して、CA Enterprise Log Manager に送信できるようにする、要素のセットで実装されます。 この要素のセットには、ログ センサ、および特定の製品から読み込むよう設計された XMP ファイルと DM のファイルが含まれています。 事前定義済み統合の例には、syslog イベントおよび WMI イベントの処理用の統合などがあります。 未分類のイベントの処理を可能にするカスタム統合を作成できます。

動的値プロセス

動的値プロセスは、レポートやアラートで使用されている選択済みキーの値を登録または更新する際に呼び出される CA IT PAM プロセスです。 動的値プロセスへのパスは、IT PAM 設定の一部として、[管理]タブの[レポート サーバ サービス リスト]に入力します。 これと同じ UI ページの[キー値]に関連付けられた[値]セクションの[動的値リストのインポート]をクリックします。 動的値プロセスの呼び出しは、キーに値を追加する際に使用できる 3 つの方法のうちの 1 つです。

ネイティブ イベント

ネイティブ イベントは、元のイベントの発生要因となる状態またはアクションです。 ネイティブ イベントは、受信され、必要に応じて解析/マッピングされてから、元のイベントまたは精製済みイベントとして転送されます。 失敗した認証はネイティブ イベントです。

フィルタ

フィルタは、イベント ログ ストア クエリを制限する手段です。

フォルダ

フォルダは、CA Enterprise Log Manager オブジェクト タイプを格納するために CA Enterprise Log Manager 管理サーバが使用するディレクトリ パスの場所です。 指定したオブジェクトタイプにアクセスする権限を付与または拒否する際に、スコープ ポリシー内のフォルダを参照します。

プロファイル

プロファイルは、任意の、設定可能なタグおよびデータ フィルタのセットです。フィルタは、製品固有、テクノロジ固有、または選択したカテゴリ限定のいずれかになっています。たとえば、製品用のタグ フィルタを使用すると、リスト表示されるタグが、選択した製品タグに制限されます。 製品用のデータ フィルタを使用すると、作成するレポート、スケジュールするアラート、および表示するクエリ結果に、指定した製品のデータのみが表示されます。 必要なプロファイルを作成したら、ログイン時に常に有効になるようにプロファイルを設定できます。 複数のプロファイルを作成した場合は、セッション中のアクティビティに複数のプロファイルを 1 つずつ適用できます。 事前定義済みフィルタは、サブスクリプション更新と共に提供されます。

プロンプト

プロンプトとは、ユーザが入力した値、および選択した CEG フィールドに基づいて結果を表示する特殊なクエリです。 ユーザが入力した値が、選択された 1 つまたは複数の CEG フィールド内に存在するイベントについてのみ、行が返されます。

保存済み設定

保存済み設定は、新しい統合を作成する際にテンプレートとして使用できる統合のデータ アクセス属性の値と共に保存された設定です。

ホット データベース状態

ホット データベース状態は、新規イベントが挿入されるイベント ログ ストア内にあるデータベースの状態です。 ホット データベースは、収集サーバ上の設定可能なサイズに到達すると、圧縮され、カタログが作成され、レポート サーバ上のウォーム ストレージに移動されます。 さらに、ホット データベース内には、すべてのサーバによって新しい自己監視イベントが保存されます。

マッピング分析

マッピング分析は、データ マッピング（DM）ファイルをテストし、変更を加えるマッピング ファイル ウィザードの手順の 1 つです。 サンプル イベントが DM ファイルに対してテストされ、結果が CEG を使用して検証されます。

メッシュ統合

CA Enterprise Log Manager サーバのメッシュ統合は、サーバ間にピア関係を構築するトポロジです。 最も単純な形式では、サーバ 2 はサーバ 1 の子であり、サーバ 1 はサーバ 2 の子であります。 メッシュ型のサーバのペアには、双方向の関係があります。メッシュ統合では、多くのサーバがすべて相互のピアになるように定義できます。 連携クエリでは、選択したサーバおよびそのすべてのピアから結果が返されます。

メッセージ解析

メッセージ解析は、元のイベントログの分析にルールを適用して、タイム スタンプ、IP アドレス、ユーザ名などの関連情報を取得するプロセスです。 解析するルールでは、文字一致を使用して特定のイベント テキストを検索し、選択された値にリンクさせます。

メッセージ解析トークン（ELM）

メッセージ解析トークンは、CA Enterprise Log Manager メッセージ解析で使用される正規表現構文を構築するための再使用可能なテンプレートです。 トークンは、名前、タイプ、および対応する正規表現文字列で構成されます。

メッセージ解析ファイル（XMP）

メッセージ解析ファイル（XMP）は、解析ルールを適用する特定のイベント ソース タイプに関連付けられた XML ファイルです。 解析ルールによって、収集された元のイベント内の関連データから名前/値ペアが抽出され、さらなる処理のためにデータ マッピング ファイルに渡されます。 このファイル タイプは、すべての統合で使用され、統合に基づいてコネクタで使用されます。 CA アダプタの場合、XMP ファイルは CA Enterprise Log Manager サーバにも適用できます。

メッセージ解析ライブラリ

メッセージ解析ライブラリは、リスナ キューからイベントを受け取り、正規表現を使用して文字列を名前/値ペアにトークン化するライブラリです。

元のイベント

元のイベントは、監視エージェントによって Log Manager コレクタに送信されたネイティブ イベントがトリガとなる情報です。 元のイベントは、通常、syslog 文字列または名前/値ペアとしてフォーマットされます。 イベントを CA Enterprise Log Manager 内で元の形式で確認できます。

ユーザ グループ

ユーザ グループは、アプリケーション グループ、グローバル グループ、動的グループのいずれかです。 事前定義済み CA Enterprise Log Manager アプリケーション グループは、Administrator、Analyst、および Auditor です。 CA Enterprise Log Manager ユーザは、CA Enterprise Log Manager とは別のメンバシップを通して、グローバル グループに属している場合があります。 動的グループは、ユーザ定義のグループで、動的グループ ポリシーによって作成されます。

ユーザ ストア

ユーザ ストアは、グローバル ユーザ情報およびパスワード ポリシー用のリポジトリです。 CA Enterprise Log Manager ユーザ ストアは、デフォルトではローカル リポジトリですが、CA SiteMinder を参照したり、Microsoft Active Directory、Sun One、Novell eDirectory などのサポートされている LDAP ディレクトリを参照したりするよう設定できます。 ユーザ ストアの設定内容にかかわらず、管理サーバ上のローカル リポジトリには、ユーザ ロールや関連付けられたアクセス ポリシーなど、ユーザに関するアプリケーション固有の情報が格納されています。

ユーザ ロール

ユーザ ロールには、事前定義済みのアプリケーション ユーザ グループか、ユーザ定義のアプリケーション グループを指定できます。 事前定義済みアプリケーション グループ（Administrator、Analyst、および Auditor）では詳細な担当職務を十分カバーできない場合は、カスタム ユーザ ロールを作成する必要があります。 カスタム ユーザ ロールを作成するには、カスタム アクセス ポリシーを設定し、事前定義済みポリシーを変更して、この新しいロールを追加する必要があります。

抑制

抑制は、CEG フィルタに基づいてイベントを除外するプロセスです。 抑制は SUP ファイルによって実行されます。

抑制ルール

抑制ルールは、精製済みの特定のイベントをレポートに表示されないようにするために設定するルールです。 セキュリティ上問題のないルーチン イベントを抑制する永続的な抑制ルールを作成したり、多数の新規ユーザの作成などの計画されたイベントのログ記録を抑制する一時的なルールを作成したりすることができます。

リモート イベント

リモート イベントは、2 つの異なるホスト名（ソースおよび宛先）を含んだイベントです。 リモート イベントは、共通イベント文法（CEG）内で使用される 4 つのイベント タイプのタイプ 2 です。

リモート ストレージ サーバ

リモート ストレージ サーバは、1 つ以上のレポート サーバから自動アーカイブ済みデータベースを取得するサーバに割り当てられたロールです。 リモート ストレージ サーバでは、必要な年数の間コールド データベースが保存されます。 ストレージに使用されるリモート ホストには、通常、CA Enterprise Log Manager やほかの製品をインストールしません。 自動アーカイブの場合は、非対話型認証を設定します。

レポート

レポートは、フィルタを備えた事前定義済みクエリやカスタム クエリの実行によって生成されるイベント ログ データを、グラフィック形式や表形式で表示したものです。 データの取得先には、選択したサーバや、必要な場合はその連携サーバの、イベント ログ ストア内にあるホット データベース、ウォーム データベース、および解凍済みデータベースを指定できます。

レポート ライブラリ

レポート ライブラリは、事前定義済みおよびユーザ定義のレポート、レポート タグ、作成済みレポート、およびスケジュール済みレポートジョブをすべて格納したライブラリです。

レポート サーバ

レポート サーバは CA Enterprise Log Manager サーバによって実行されるロールです。レポート サーバは、1 つ以上の収集サーバから、自動アーカイブ済みウォーム データベースを取得します。 レポート サーバによって、クエリ、レポート、スケジュール済みアラート、およびスケジュール済みレポートが処理されます。

レポート サーバ

レポート サーバは、アラートを電子メールで送信する際に使用する電子メール サーバ、PDF 形式で保存されるレポートの外観、レポート サーバに保存するレポートや RSS フィードに送信するアラート用ポリシーの保持などの、設定情報を格納するサービスです。

ローカル イベント

ローカル イベントは、単一のエンティティを含んだイベントで、ここでは、イベントのソースおよび宛先が同じホスト マシンです。 ローカル イベントは、共通イベント文法 (CEG) 内で使用される 4 つのイベント タイプのタイプ 1 です。

ローカル フィルタ

ローカル フィルタは、現在のレポートに表示されているデータを制限するために、レポートの表示中に設定できる条件のセットです。

ログ

ログは、イベントまたはイベント コレクションの監査レコード、すなわち記録されたメッセージです。 ログは、監査ログ、トランザクション ログ、侵入ログ、接続ログ、システム パフォーマンス レコード、ユーザ アクティビティ ログ、またはアラートのいずれかです。

ログ エントリ

ログ エントリは、システム上またはネットワーク内で発生した特定のイベントについての情報が格納されているログ内のエントリです。

ログ センサ

ログ センサは、データベース、syslog、ファイル、SNMP などの特定のログ タイプから読み込むよう設計された統合コンポーネントです。 ログ センサは再利用されます。通常、ユーザはカスタム ログ センサを作成しません。

ログ レコード

ログ レコードは、個別の監査レコードです。

ログ解析

ログ解析は、ログ管理の後の段階で解析済み値を使用できるように、ログからデータを抽出するプロセスです。

ログ分析

ログ分析とは、対象のイベントを識別するためのログ エントリの検証です。 適切なタイミングで分析しないと、ログの価値はきわめて低くなります。

委任ポリシー

委任ポリシーは、ユーザが別のユーザ、アプリケーション グループ、グローバル グループ、または動的グループに自分の権限を委任できるようにするアクセス ポリシーです。 削除または無効化されたユーザによって作成された委任ポリシーを明示的に削除する必要があります。

解析

解析は、メッセージ解析（MP）とも呼ばれ、元のデバイス データを取得し、それをキー/値ペアに変換するプロセスです。 解析は XMP ファイルによって実行されます。 解析は、イベント ソースから収集された元のイベントを表示可能な精製済みイベントに変換する統合プロセスの手順の 1 つで、データ マッピングの前に実行されます。

解析ファイル ウィザード

解析ファイル ウィザードは、CA Enterprise Log Manager 管理サーバに格納された eXtensible Message Parsing （XMP）ファイルを作成、編集、および分析するために管理者が使用する CA Enterprise Log Manager の機能です。 受信イベント データの解析のカスタマイズには、事前一致文字列およびフィルタの編集が含まれます。 新規作成されたファイルおよび編集されたファイルは、[ログ収集エクスプローラ]、[イベント精製ライブラリ]、[解析ファイル]、[ユーザ フォルダ]に表示されます。

解凍済みデータベース状態

解凍済みデータベース状態は、アーカイブ ディレクトリに復元されたデータベースに適用される状態で、管理者が LMArchive ユーティリティを実行して CA Enterprise Log Manager に復元を通知した後に適用されます。 解凍済みデータベースは、[ポリシーのエクスポート]に設定された時間数の間保持されます。 ホット、ウォーム、および解凍済みの状態のデータベースに含まれるイベント ログにクエリを実行できます。

階層統合

CA Enterprise Log Manager サーバの階層統合は、サーバ間に階層関係を構築するトポロジです。 最も単純な形式では、サーバ 2 はサーバ 1 の子ですが、サーバ 1 はサーバ 2 の子ではありません。 すなわち、関係は一方向のみです。 階層統合は、複数のレベルの親子関係を持つことができ、1 つの親サーバが多数の子サーバを持つことができます。 連携クエリでは、選択したサーバおよびその子から結果が返されます。

管理サーバ

管理サーバは、最初にインストールされる CA Enterprise Log Manager サーバに割り当てられるロールです。この CA Enterprise Log Manager サーバには、すべての CA Enterprise Log Manager で共有されるポリシーなどのコンテンツが格納されるリポジトリが含まれています。 通常、このサーバは、デフォルトのサブスクリプション プロキシです。 管理サーバはすべてのロールを実行できますが、大部分の実稼働環境では推奨されません。

観察されたイベント

観察されたイベントは、ソース、宛先、およびエージェントを含んだイベントで、ここでは、イベントが、イベント収集エージェントによって観察および記録されます。

記録されたイベント

記録されたイベントは、データベースに挿入された後の元のイベント情報または精製済みイベント情報を指します。 抑制または集約されていない場合、元のイベントは、常に精製済みイベントです。 この情報は保存され、検索の対象になります。

共通イベント文法（CEG）

共通イベント文法（CEG）は、イベントがイベント ログ ストアに格納される前に、CA Enterprise Log Manager により解析ファイルおよびマッピング ファイルを使用して変換される標準形式を提供するスキーマです。 CEG は、さまざまなプラットフォームおよび製品からのセキュリティ イベントを定義するための一般的な正規化フィールドを使用します。 解析またはマッピングできないイベントは、元のイベントとして格納されます。

視覚化コンポーネント

視覚化コンポーネントは、表、グラフ（線グラフ、棒グラフ、縦棒グラフ、円グラフ）、イベント ビューアなど、レポート データを表示する際に使用できるオプションです。

資格管理

資格管理は、ユーザが認証され、CA Enterprise Log Manager インターフェースにログオンした後、実行を許可される内容を制御する手段です。 これは、ユーザに割り当てられたロールに関連付けられたアクセス ポリシーを使用して行います。 ロール、すなわちアプリケーション ユーザ グループと、アクセス ポリシーは、事前定義済みかユーザ定義のどちらかです。 資格管理は、CA Enterprise Log Manager 内部のユーザ ストアによって処理されます。

自動アーカイブ

自動アーカイブは、あるサーバから別のサーバへのアーカイブ データベースの移動を自動化する設定可能なプロセスです。 自動アーカイブの最初の段階で、収集サーバが、指定された間隔で新しくアーカイブされたデータベースをレポート サーバに送信します。 第 2 段階で、レポート サーバが、古くなったデータベースを長期保存用のリモート ストレージ サーバに送信します。これによって、手動によるバックアップおよび移動の手順が必要なくなります。 自動アーカイブでは、ソース サーバから宛先サーバへのパスワードを使用しない認証を設定する必要があります。

収集サーバ

収集サーバは、CA Enterprise Log Manager サーバによって実行されるロールです。収集サーバは、受信イベント ログを精製し、ホット データベースにそれらを挿入し、ホット データベースを圧縮し、関連するレポート サーバに自動アーカイブ、すなわちコピーします。 ホット データベースは、設定されたサイズに達すると、収集サーバによって圧縮され、設定されたスケジュールで自動アーカイブされます。

収集ポイント

収集ポイントは、エージェントがインストールされるサーバです。このサーバには、そのエージェントのコネクタに関連付けられたイベント ソースが含まれているすべてのサーバに対する、ネットワーク隣接性があります。

集約ルール

集約ルールは、同じタイプの複数のネイティブ イベントを結合して、単一の精製済みイベントとするルールです。 たとえば、集約ルールは、同じソースおよび宛先 IP アドレス/ポートを持つ重複イベントを最大 1000 まで、単一の集約イベントで置き換えるように設定できます。 このようなルールは、イベント分析を簡略化し、ログ トラフィックを軽減します。

精製済みイベント

精製済みイベントは、元のイベントまたは集約されたイベントから派生した、解析またはマッピングされたイベント情報です。 CA Enterprise Log Manager では、格納された情報を検索できるように、マッピングおよび解析を実行します。

責任ポリシー

責任ポリシーは、アクセス フィルタを作成したときに自動的に作成されるポリシーです。責任ポリシーを直接、作成、編集、または削除しようとしないでください。 代わりに、アクセス フィルタを作成、編集、または削除します。

統合の要素

統合の要素には、センサ、設定ツール、データ アクセス ファイル、1 つ以上の XMP メッセージ解析(XMP)ファイル、および 1 つ以上のデータ マッピング ファイルがあります。

動的ユーザ グループ

動的ユーザ グループは、1 つ以上の共通属性を共有するグローバル ユーザから構成されます。 動的ユーザ グループは、特殊な動的ユーザ グループ ポリシーによって作成されます。このポリシーでは、リソース名が動的ユーザ グループ名で、メンバシップのベースがユーザ属性およびグループ属性に設定されたフィルタ セットになります。

復元ポイント サーバ

復元ポイント サーバは CA Enterprise Log Manager サーバによって実行されるロールです。「コールド」イベントを調査するには、ユーティリティを使用して、リモート ストレージ サーバから復元ポイント サーバにデータベースを移動し、そのデータベースをカタログに追加し、クエリを実行します。 コールド データベースを専用の復元ポイントに移動するのは、調査のために元のレポート サーバに移動する必要がなくなります。

連携サーバ

連携サーバは、ログ データ収集を配布するためにネットワーク内で相互接続された CA Enterprise Log Manager サーバですが、収集されたデータをレポート用に集約することはしません。 連携サーバは、階層型トポロジまたはメッシュ型トポロジで接続することができます。 連携されたデータのレポートには、ターゲット サーバからのデータに加えて、そのサーバの子またはピアからのデータがすべて含まれます。

索引

C

CA Embedded Entitlements Manager
  定義済み - 54
CA Enterprise Log Manager
  インストール - 12
  オンライン ヘルプ - 61
  コンポーネント - 12
  ツールのヒント - 59
  ユーザ ロール - 55

S

syslog
  イベントの表示 - 31

あ

アーカイブ
  定義済み - 49
エージェント バイナリ
  Windows システム用のダウンロード - 36
エージェントのインストール
  マニュアル、Windows 用 - 37
エージェントのユーザ アカウント
  Windows 用の設定 - 34
エージェント認証キー
  更新 - 35

か

コネクタ
  設定 - 39

さ

サブスクリプション管理
  処理の説明 - 56
  定義済み - 56

た

ツールのヒント
  使い方 - 59
データ マッピング
  定義済み - 50
テスト環境
  インストールするもの - 12
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 - 43

ま

メッセージの解析
  定義済み - 50

や

ユーザ ロール
  定義済み - 55

ら

ログ収集
  定義済み - 47
ログ ストレージ
  定義済み - 49

漢字

共通イベント文法(CEG)
  定義済み - 50