CA Enterprise Log Manager

実装ガイド

リリース 12.5

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。

- イベント相関 -- 「サーバの計画」および「サービスの設定」の章が変更され、この新機能に関する説明が追加されました。変更内容には、専用の相関サーバ、サーバ ロールの計画、相関サーバおよびルールの設定が含まれます。
- サブスクリプション配布および監視の向上 -- 「サービスの設定」の章が変更され、サブスクリプション設定に関する説明が追加されました。
- 仮想化 -- 仮想化に関する章が変更され、OVF テンプレートを展開するための必須パラメータの変更が追加されました。

詳細情報:

サーバの計画 (P. 20)
相関サービスの設定 (P. 179)

目次

第 1 章: 概要

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

この「CA Enterprise Log Manager 実装ガイド」では、ネットワークのイベント ソースからイベント ログを受信する CA Enterprise Log Manager の計画、インストール、および設定に必要な手順について説明します。このガイドは、タスクがプロセスとその目標の説明から始まるように編成されています。通常はプロセスの後に関連する概念が続き、その次には目標を達成するための 1 つ以上の手順が続きます。

「CA Enterprise Log Manager 実装ガイド」は、ログ収集ソリューションのインストール、設定、および保守に加えて、ユーザの作成、ユーザのロールおよびアクセスの割り当てと定義、さらにバックアップ データの保持を担当するシステム管理者を対象としています。

また、このガイドは、次の作業方法についての情報を必要とする担当者を支援します。

- イベント データを収集するコネクタまたはアダプタの設定
- レポート、データの保存、バックアップ、およびアーカイブを制御するサービスの設定
- CA Enterprise Log Manager サーバの連携の設定
- コンテンツ、設定、およびオペレーティング システムの更新を取得するためのサブスクリプションの設定

内容の概要を次に示します。

セクション	Description
環境の計画	ログ収集、エージェント、連携、ユーザとアクセスの管理、サブスクリプションの更新、および惨事復旧などの領域の計画アクティビティについて説明します。

セクション	Description
CA Enterprise Log Manager のインストール	必要な情報を収集するためのワークシートと、CA Enterprise Log Manager をインストールし、インストールが適切に行われたかどうかを検証する方法に関する詳細な手順を説明します。
ユーザおよびアクセスの基本的な設定	ユーザ ストアを識別し、他のユーザとアクセスの詳細を設定するための最初の管理ユーザを作成する手順を説明します。
サービスの設定	グローバルおよびローカル フィルタ、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 オプションなどのサービスを設定する手順を説明します。
イベント収集の設定	マッピング ファイルや解析ファイルなどのイベント精製ライブラリコンポーネントと、CA アダプタの使用または設定に関する概念および手順を説明します。
連携の作成	さまざまなタイプの連携について説明し、CA Enterprise Log Manager サーバ間の連携関係を作成したり、連携グラフを表示したりするための手順を説明します。
イベント精製ライブラリの使用	メッセージ解析およびデータ マッピング ファイルの操作に関する高レベルな情報を提供します。
CA Audit ユーザに関する考慮事項	CA Enterprise Log Manager と CA Audit との間で実装可能な相互作用、iRecorder とポリシーの設定方法、および CA Audit コレクタ データベースからのデータのインポート方法について説明します。
CA Access Control ユーザに関する考慮事項	CA Access Control との統合方法、CA Enterprise Log Manager にイベントを送信する CA Audit ポリシーの変更方法、CA Enterprise Log Manager にイベントを送信する CA Access Control iRecorder の設定方法、および CA Audit コレクタ データベースを形成する CA Access Control イベントのインポート方法について説明します。
CA IT PAM に関する注意事項	管理 CA Enterprise Log Manager 上の EEM コンポーネントが認証を処理するように CA IT PAM をインストールするプロセスについて説明します。
惨事復旧	障害が発生した場合に、ログ管理ソリューションを確実にリカバリするためのバックアップ、リストア、および置換手順について説明します。
CA Enterprise Log Manager と仮想化	CA Enterprise Log Manager サーバを含む仮想マシンを作成して設定するために使用するプロセスについて説明します。

注: サポートするオペレーティング システムや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 の基本的な概要および使用のシナリオについては、「概要ガイド」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。

第 2 章: 環境の計画

このセクションには、以下のトピックが含まれています。

サーバの計画

環境の計画の最初の手順は、必要とする CA Enterprise Log Manager サーバの数と、各サーバが実行するロールを決定することです。ロールには次のものがあります。

- 管理

  事前定義済みおよびユーザ定義のコンテンツと設定を保存します。また、ユーザを認証し、機能へのアクセスを許可します。

- 収集

  エージェントからイベント ログを受信し、イベントを精製します。

- 相関

  エージェントまたは収集サーバからイベント ログを受信し、イベントをフィルタして、適用される相関ルールに基づいてインシデントを作成します。

- レポート

  収集されたイベントに対するクエリ、クエリとレポートの両方に対するオンデマンドのクエリ、さらにスケジュール済みアラートとレポートに対するクエリを処理します。

- 復元ポイント

  過去のイベントを検証する場合に、復元されたイベント ログ データベースを受信します。

最初にインストールされたサーバが管理サーバになります。このサーバは他のロールも実行できます。1 つの CA Enterprise Log Manager ネットワークには管理サーバを 1 つだけ持つことができます。CA Enterprise Log Manager のネットワークごとに、1 つの管理サーバを持つ必要があります。

使用可能なアーキテクチャには次のようなものがあります。

- 単一サーバのシステム。管理サーバが他のすべてのロールを実行します。
- 2 台のサーバによるシステム。管理サーバは収集以外のすべてのロールを実行します。収集は、このロール専用のサーバによって実行されます。
- 複数サーバ システム。各サーバが 1 つのロール専用になります。

サーバ ロールとアーキテクチャの詳細を次に説明します。

サーバ ロール

CA Enterprise Log Manager システムでは 1 つ以上のサーバを使用できます。さまざまなサーバをさまざまなロール専用にすると、パフォーマンスが最適化されます。ただし、各自の判断により、任意のサーバを使用して複数のロールを実行したり、すべてのロールを実行したりすることができます。インストールした各サーバを特定のロール専用にする方法を決定する場合、環境内の他の関連要因に関して、各サーバに関連付けられた処理の負荷を考慮します。

- 管理サーバ

  デフォルトでは、管理サーバ ロールは、最初にインストールされた CA Enterprise Log Manager サーバによって実行されます。管理サーバは主に次のような機能を実行します。

  - このサーバに登録されたすべてのサーバの共通のリポジトリとしての機能。特に、アプリケーション ユーザ、アプリケーション グループ (ロール)、ポリシー、カレンダ、および AppObjects を保存します。
  - ユーザ ストアを内部ストアに設定した場合は、グローバル ユーザ、グローバル グループ、およびパスワード ポリシーも保存します。設定されたユーザ ストアが外部ユーザ ストアを参照する場合、参照するユーザ ストアからグローバル ユーザ アカウントの詳細とグローバル グループの詳細をロードします。
  - 高速メモリにマッピングされたファイルを使用したユーザ資格情報の処理。ログイン時にはユーザとグループの設定に基づいてユーザを認証します。ポリシーとカレンダに基づいて、ユーザ インターフェースのさまざまな部分へのアクセスをユーザに許可します。
  - サブスクリプションを通じてダウンロードしたすべてのコンテンツと設定の更新の受信。

  CA Enterprise Log Manager サーバのネットワークでは 1 つの管理サーバのみを有効にできますが、フェイルオーバー用 (非アクティブ) の管理サーバを使用できます。複数の CA Enterprise Log Manager ネットワークを作成する場合は、それぞれのネットワークで有効な管理サーバを使用する必要があります。

- 収集サーバ

  単一のサーバ システムでは、管理サーバが収集サーバのロールを実行します。2 台以上のサーバ システムでは、専用の収集サーバの使用を検討してください。収集サーバは次のような機能を実行します。

  - コネクタの設定をサポートします。
  - エージェントのコネクタからの受信イベント ログを受け入れます。
  - 精製されたイベント ログを受信します。それらは解析されて CEG 形式にマップされるため、異なるイベント ソースからのイベント データを同一の形式で表示できるようになります。
  - イベント ログをホット データベースに挿入し、ホット データベースが設定したサイズに到達すると、それをウォーム データベースに圧縮します。
  - 自動アーカイブを許可して、ウォーム データベース情報を、設定されたスケジュールで関連するレポート サーバに移動できるようにします。

    重要： 収集およびレポーティング用に個別のサーバを割り当てた場合、収集サーバからレポート サーバに対して、非対話型の認証を設定し、1 時間ごとの自動アーカイブを設定する必要があります。

  イベントの収集と調整専用にサーバを割り当てるかどうかを決定する場合は、イベント ソースが生成するイベント ボリュームを考慮します。また、何台の収集サーバが 1 つのレポート サーバに対してデータの自動アーカイブを行うかについても検討します。

- 相関サーバ

  単一のサーバ システムでは、管理サーバが相関サーバのロールを実行します。2 台以上のサーバ システムでは、専用の相関サーバを使用することを検討してください。相関サーバは、以下の機能を実行します。

  - 相関ルールおよび通知の設定と適用をサポートします。
  - 収集サーバからイベント ログを受信します。
  - 受信イベントをフィルタし、相関ルール条件に従ってインシデントを作成します。
  - インシデントをインシデント データベースに格納し、それらのコンポーネント イベントをインシデント イベント データベースに格納します。

    重要：専用の相関サーバを使用する場合は、相関サービスを設定するときに、相関させるイベントが存在するすべての収集サーバを選択する必要があります。

- レポート サーバ

  1 台のサーバまたは 2 台のサーバ システムでは、管理サーバがレポート サーバのロールを実行します。多くのサーバを持つシステムでは、1 つ以上のサーバをレポート専用にすることを検討します。レポート サーバは次のような機能を実行します。

  - 非対話型認証と自動アーカイブが設定されている場合、その収集サーバから調整済みイベントの新しいデータベースを受信します。
  - オンデマンド プロンプト、クエリ、およびレポートを処理します。
  - スケジュール済みアラートやレポートを処理します。
  - カスタム クエリおよびレポートを作成するためのウィザードをサポートします。
  - レポーティング サーバからリモートのストレージ サーバに対して、非対話型の認証および自動アーカイブが設定されている場合、古いデータベースをリモート ストレージ サーバに移動します。

  オンデマンド アクティビティが多いサーバで多くの複雑なレポートやアラートを生成する予定である場合は、レポート専用のサーバを検討します。

- リモート ストレージ サーバ

  リモート ストレージ サーバ (CA Enterprise Log Manager サーバではない場合があります) は、以下の機能を実行します。

  - 有効期限や空きディスク領域の不足によってデータベースが削除される前に、高い圧縮率で自動アーカイブされたそれらのデータベースを設定された間隔でレポート サーバから受信します。自動アーカイブを設定すると、手動でデータベースを移動する手間を省くことができます。
  - コールド データベースをローカルに保存します。オプションで、これらのデータベースを、サイト外の長期保管用の場所に移動またはコピーできます。通常、コールド データベースは、政府の規制機関によって命令された数年間は保持されます。

  リモート ストレージ サーバは CA Enterprise Log Manager の連携の一部にはなりません。ただし、アーキテクチャを計画する場合は考慮する必要があります。

- 復元ポイント サーバ

  一般的に、レポート サーバは、以前保持したデータベースの復元ポイント サーバとして動作します。大規模なネットワークの場合は、このロール専用の CA Enterprise Log Manager サーバを用意することを検討します。復元ポイント サーバは次のような機能を実行します。

  - 古いイベント ログの検証に使用します。
  - すべてのコールド データベースを保持するリモート ストレージ サーバから復元されたデータベースを受信します。ストレージ サーバから復元ポイントに対して非対話型認証を最初に設定している場合は、restore-ca-elm.sh ユーティリティを使用して、データベースを復元ポイントに移動できます。
  - アーカイブ カタログを再作成して、復元されたデータベースをそのレコードに追加します。
  - 復元されたレコードを、復元の方法に応じて設定されたさまざまな期間にわたって保持します。

  専用の復元ポイントを持つ利点は、連携からこのサーバを除外して、復元された古いデータを含む連携レポートを作成しないようにすることができる点です。復元ポイント サーバで生成されたレポートはすべて、復元されたデータベースからのイベント データのみを反映します。

サーバを特定のロール専用にしても、他のロールに関連付けられたサーバから機能を実行できないわけではありません。専用の収集サーバとレポート サーバがある環境を考えてみます。できるだけ速く通知するにはスピードが重要であるため、収集サーバで状態をチェックするアラートを設定する場合は、そうした設定を行う柔軟性もあります。

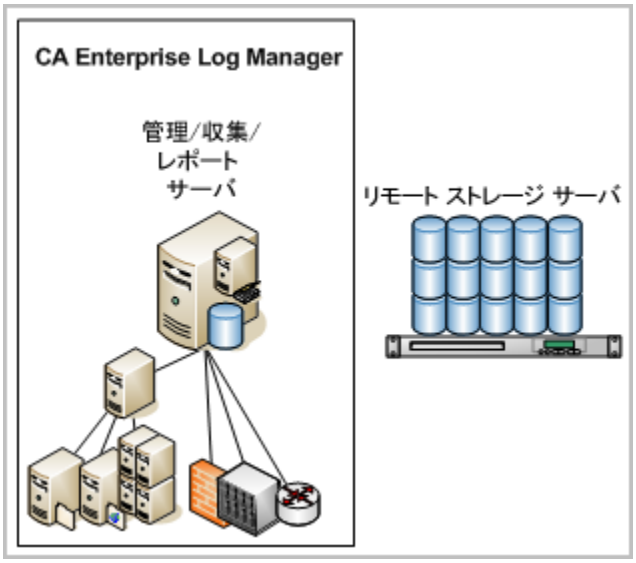
例: ネットワーク アーキテクチャ

CA Enterprise Log Manager の最も簡単なアーキテクチャは 1 台のサーバによるシステムです。この場合は 1 つの CA Enterprise Log Manager が次のすべてのロールを実行します。

- 管理、収集、レポート用の CA Enterprise Log Manager は、クエリとレポートに加えて設定/コンテンツ管理、イベント収集/精製、および相関を処理します。

  注: CA Enterprise Log Manager 以外のリモート サーバには、アーカイブされたイベント ログ データベースが保存されます。

このセットアップは、テスト システムなど、イベント ボリュームが少なく、スケジュール済みレポートの処理が少ない場合に適しています。

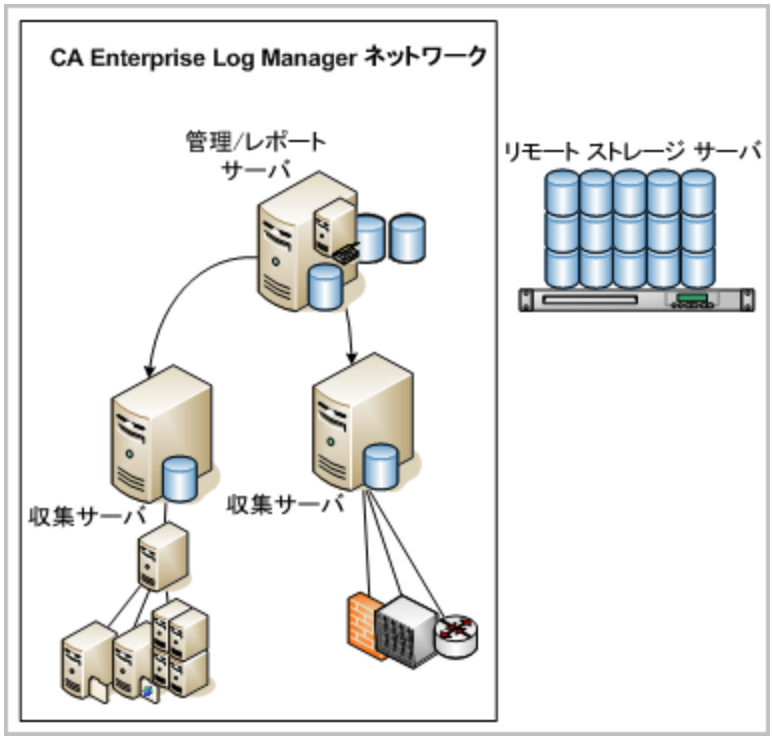


次に簡単なアーキテクチャは、最初にインストールされた CA Enterprise Log Manager がほとんどのロールを実行する、次のような複数のサーバ システムです。

- 管理、レポート用の CA Enterprise Log Manager は、クエリとレポートに加えて設定/コンテンツ管理およびイベント相関を処理します。
- 収集用 CA Enterprise Log Manager は、イベントの収集と精製を処理します。

注: CA Enterprise Log Manager 以外のリモート サーバは、イベント ログのアーカイブされたデータベースを保存するためにセット アップされます。

このアーキテクチャは、適度なイベント ボリュームを持つネットワークに適しています。矢印は、管理/レポート サーバの管理機能がすべてのサーバに適用されるグローバル設定を管理していることを示しています。収集サーバが多数ある場合、このアーキテクチャは「ハブとスポーク」と呼ばれます。

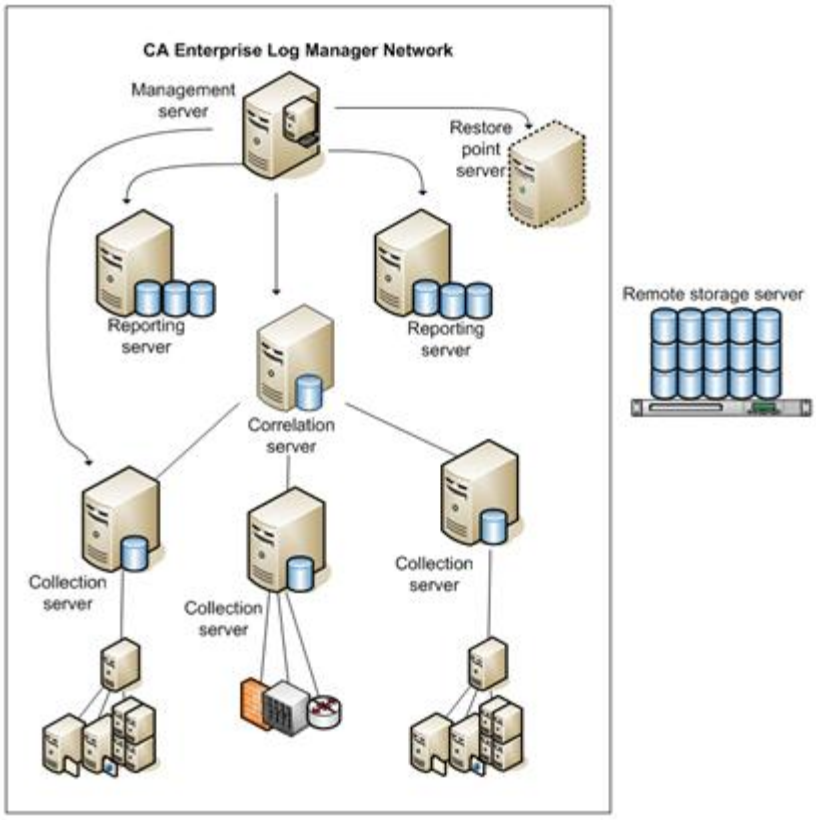


イベント ボリュームが大量で、多くの複雑なスケジュール済みレポートやアラートを使用し、カスタマイズが行われている大規模なネットワークでは、次のように 1 つ以上の CA Enterprise Log Manager サーバを 1 つのロール専用にすることができます。

- 管理用 CA Enterprise Log Manager は、設定/コンテンツ管理を行います。
- レポート用 CA Enterprise Log Manager は、クエリとレポートを処理します。
- 収集用 CA Enterprise Log Manager は、イベントの収集と精製を処理します。
- 相関 CA Enterprise Log Manager は、イベント相関を処理します。
- 任意で、復元ポイントの CA Enterprise Log Manager を使用して、復元されたアーカイブ データベースのイベントの検証を行います。

注: CA Enterprise Log Manager 以外のリモート サーバは、イベント ログのアーカイブされたデータベースを保存するためにセット アップされます。

このセットアップは大規模ネットワークにとって理想的です。矢印は、管理サーバが、すべてのサーバに適用されるグローバル設定を管理していることを示しています。



ログ収集の計画

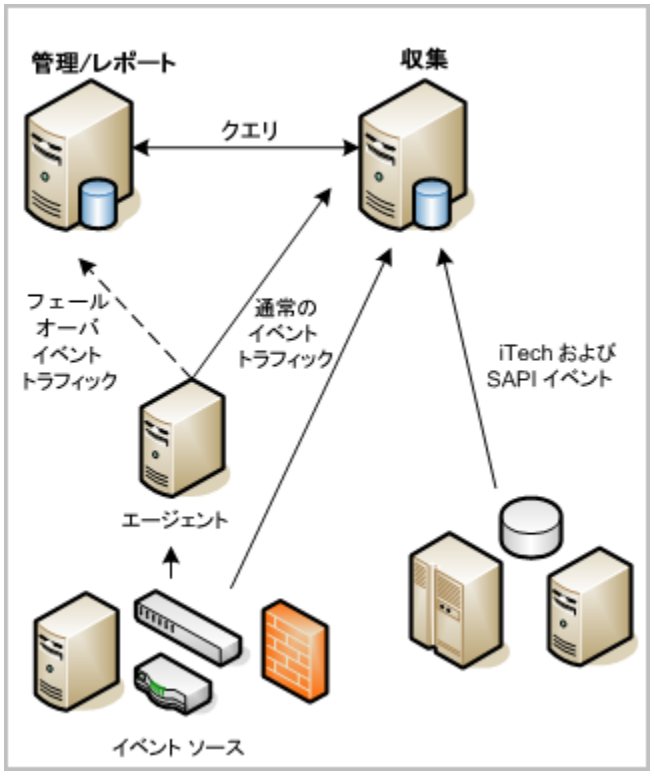
ネットワークのログ収集の計画では、処理して保存する必要のある 1 秒あたりのイベント数（eps）と、データをオンラインで保持する必要のある時間の長さを考慮する必要があります。（この意味では、オンラインとはすぐに検索できる状態であることを意味します。）通常は、30 ～ 90 日分のデータをオンラインで保持します。

各ネットワークには、ネットワーク デバイスやファイアウォールなどのアプリケーションを企業のイベント情報のニーズに合わせて調整する度合いや、デバイスの数、デバイス タイプに応じて、独自のイベント ボリュームがあります。 たとえば、一部のファイアウォールは、設定された方法に基づいて大量の不要なイベントを生成する場合があります。

全体的なイベント ボリュームが使用する CA Enterprise Log Manager サーバに均等に分配され、いずれかのサーバが通常の一定の作業の割合を超えることがないように、イベント収集を計画することをお勧めします。企業のイベント ボリュームで最高のパフォーマンスを維持するには、次のように少なくとも 2 つの連携された CA Enterprise Log Manager サーバをインストールすることをお勧めします。

- クエリとレポートの処理、アラートの表示とアラート管理、サブスクリプションの更新、およびユーザ認証と許可を行う 1 台のレポート用 CA Enterprise Log Manager サーバ。
- 特にデータベースの挿入を最大化するよう設定された、1 つ以上の収集用 CA Enterprise Log Manager サーバ。

次の図に、シンプルな連携された CA Enterprise Log Manager ネットワークの例を示します。2 つの CA Enterprise Log Manager サーバ (1 つはレポート用、もう一方は収集用) がさまざまなイベント ソースからのイベント トラフィックを処理します。どちらのサーバも、クエリ、レポート、およびアラート用にサーバ間でデータを共有できます。



収集サーバは、主に受信イベント ログ トラフィックを処理し、データベースへの挿入を中心に実行します。収集サーバは、24 時間以下の短いデータ保存ポリシーを使用します。 保存されたイベント ログは、自動化されたスクリプトによって、イベントのボリュームに応じて 1 日 1 回またはそれ以上の頻度でレポート サーバに移動されます。連携、および 2 つのサーバ間の連携クエリを使用すると、両方のサーバのイベント ログから正確なレポートを確実に受信できます。

レポート サーバは次のような複数の機能を実行します。

- クエリとレポートの処理
- アラートのスケジュール設定と管理
- リモートのストレージ サーバへのアーカイブ ファイルの移動
- 収集サーバのコネクタが収集した一連のイベントのフェイルオーバーの実行

自動化されたバックアップ スクリプトによって、レポート サーバからリモート サーバ(コールド ストレージ)にデータが移動されます。コールド ストレージからデータを復元することを決定した場合、通常はレポート サーバに復元します。レポート サーバにスペースの制約がある場合は、収集サーバにも復元できます。収集サーバには大量のデータを保存できませんが、連携によって同じレポート結果を得ることができます。

さらに、レポート サーバは、収集サーバが何らかの理由でイベントの受信を停止した場合に、リモート エージェントのコネクタによって収集されたイベントのフェイルオーバー用の受信先として利用できます。エージェント レベルでフェイルオーバーを設定することも可能です。フェイルオーバー処理によって、1 つ以上の代替 CA Enterprise Log Manager サーバにイベントが送信されます。イベント収集のフェイルオーバーは、SAPI および iTech リスナによって収集されたレガシーのイベント ソースからのイベントには使用できません。

詳細情報:

CA Enterprise Log Manager と仮想化 (P. 309)

ディスク容量の計画

環境を計画する場合、大量のイベントをサポートするのに十分なディスク容量を準備します。つまり、収集サーバの場合は、各収集サーバが標準的なイベントボリュームに加えてピーク時に負荷を共有するのに十分なディスク容量であることを意味します。レポート サーバの場合は、イベント ボリュームとオンラインで保存する必要がある期間に基づいて、ディスク容量を計算します。

ホット データベースは圧縮されません。 ウォーム データベースが圧縮されます。ホット データベースとウォーム データベースは、両方ともオンラインであるとみなされます。これらのデータベースのデータを使用して、検索やレポート作成を実行できます。通常は、いつでもレポートを作成したり、すぐに検索したりできるように、30 日から 90 日分のデータを保持します。それより古いレコードはリモートサーバに保存されます。必要に応じて、検索やレポートのためにそのレコードを復元できます。

収集サーバはホット データベースとウォーム データベースの両方をサポートします。収集サーバの保存期間は 1 ～ 23 時間と非常に短いため、長期の保存は関係しません。

ホット データベースは自己監視イベント メッセージを挿入するために管理サーバに存在します。

レポート サーバでは、小さいホット データベースと多くのウォーム データベースをサポートします。また、レポート サーバには一定期間復元されたファイルをサポートするのに十分な追加容量が必要です。直接接続されたストレージを使用する場合、ストレージの容量を増やせるようにパーティションが自動的に拡張されます。

CA EEM サーバについて

CA Enterprise Log Manager は、内部的には CA Embedded Entitlements Manager（CA EEM）サーバを使用し、設定の管理、ユーザの許可と認証、コンテンツとバイナリに対するサブスクリプションの更新の調整、およびその他の管理機能を実行します。基本的な CA Enterprise Log Manager 環境では、管理用 CA Enterprise Log Manager サーバをインストールするときに CA EEM をインストールします。CA EEM は、そこからすべての収集用 CA Enterprise Log Manager サーバの設定とエージェントおよびコネクタを管理します。

さらに、アプリケーション インストール ディスクで提供されているインストール パッケージを使用して、リモート サーバに CA EEM サーバをインストールすることもできます。または、他の CA 製品と一緒に使用している場合に、CA EEM サーバが存在する場合は、既存の CA EEM サーバを使用できます。

CA EEM サーバは独自の Web インターフェースを提供しています。ただし、設定とメンテナンスのほとんどすべてのアクティビティは CA Enterprise Log Manager ユーザ インターフェースで実行します。フェイルオーバーの設定、および惨事復旧の一部であるバックアップと復元を除いて、通常は組み込みの CA EEM サーバの機能と直接対話する必要はありません。

注: CA Enterprise Log Manager サーバのインストールでは、CA Enterprise Log Manager サーバを適切に登録するために、CA EEM のデフォルトの管理者アカウント EiamAdmin のパスワードを使用する必要があります。最初の管理用 CA Enterprise Log Manager サーバをインストールするときに、インストールの一部でこの新しいパスワードを作成します。同じアプリケーション インスタンス名を使用して後続の CA Enterprise Log Manager サーバをインストールすると、後で CA Enterprise Log Manager サーバ間の連携関係をセット アップできるネットワーク環境が自動的に作成されます。

ログ収集のガイドライン

計画段階では、ログ収集に関する次のガイドラインに考慮してください。

- ログ収集にエージェントを使用するか使用しないかにかかわらず、エージェントから CA Enterprise Log Manager サーバへのトラフィックは常に暗号化されます。
- 送信の保証に関する潜在的な問題の回避策として、syslog のローカル収集メカニズムを使用することを検討してください。

デフォルト エージェントによる直接収集、エージェントがイベント ソースを持つホストにインストールされた場合のエージェントベースの収集、またはエージェントがイベント ソースから離れた収集ポイントにインストールされた場合のエージェントレス収集のうち、どの方法を使用するかを決定する場合は、以下の要因を考慮します。

- プラットフォームのサポート

  たとえば、WMI は Windows のログ センサのみに作用します。
- 特定のログ センサ用のドライバ サポート

  たとえば、ODBC が動作するには ODBC ドライバが必要です。
- ログ ソースにリモートからアクセスできるかどうか

  たとえば、ファイル ベースのログの場合、リモートで動作するには共有ドライブが必要です。

連携の計画

CA Enterprise Log Manager の連携とは、イベント データの保存、レポート、およびアーカイブを行うサーバのネットワークです。連携を使用すると、ネットワークでデータをグループ化したり確認する方法を制御できます。サーバをお互いに関連付ける方法と、あるサーバから別のサーバにクエリを送信する方法を設定できます。さらに、必要に応じて、特定のクエリのために連携クエリをオンまたはオフにすることができます。

連携を使用するかどうかの決定は、必要なイベントのボリュームと、ログ データの区分とレポート作成に関するビジネス ニーズの組み合わせに基づきます。CA Enterprise Log Manager では、階層統合およびメッシュ統合と、この 2 つのタイプを融合させた設定をサポートしています。連携させるすべての CA Enterprise Log Manager サーバは、CA EEM で同じアプリケーション インスタンス名を使用する必要があります。各 CA Enterprise Log Manager サーバのインストールは、アプリケーション インスタンス名を使用して CA EEM サーバに自動的に登録されます。

最初の CA Enterprise Log Manager サーバと少なくとも 1 つの追加サーバをインストールしたら、いつでも連携を設定できます。ただし、最適な結果を得るにはインストールする前に連携を計画します。詳細な連携マップを作成すると、設定タスクを迅速かつ正確に実行できます。

ネットワーク レベルでは、複数の CA Enterprise Log Manager サーバを使用すると大量のイベントを処理できます。レポートの観点からは、連携を使用すると、イベント データにアクセスできるユーザや、どのくらいの量のイベント データを表示できるかを制御できます。

基本的な 2 台のサーバの環境では、管理サーバがレポート サーバの役割を担います。管理用 CA Enterprise Log Manager サーバの内部の CA EEM サーバは、連携の設定を集中的かつ全体的に管理します（ネットワーク内の任意の CA Enterprise Log Manager サーバから設定オプションを変更できます）。クエリとレポートに最新のデータが含まれるように、収集用 CA Enterprise Log Manager サーバをレポート サーバの子として設定できます。

注: CA Enterprise Log Manager と一緒に使用する予定の既存の CA EEM サーバがある場合は、同じ方法で CA Enterprise Log Manager サーバを設定します。リモートにある専用の CA EEM サーバにこれらの設定を保存します。

さらに、ローカルの設定オプションを有効にして、グローバル設定を一時的に書き換えることができます。これにより、選択した CA Enterprise Log Manager サーバが他のサーバとは異なる動作を実行できます。たとえば、電子メール レポートやアラートを別のメール サーバから送信したり、ネットワークのあるブランチ固有のレポートを異なる時間帯でスケジュール設定します。

詳細情報:

階層統合 (P. 226)
メッシュ統合 (P. 227)
連携環境のクエリとレポート (P. 225)
CA Enterprise Log Manager の連携の設定 (P. 229)

連携マップの作成

連携マップの作成は、連携の設定の計画や実装を行う場合に便利な手順です。ネットワークが大きいほど実際の設定タスクを行う際にこのマップが役立ちます。市販のグラフィック プログラムまたは図面プログラムを使用したり、手作業でマップを作成できます。マップに多くの詳細を追加するほど、設定時間を短縮できます。

連携マップを作成する方法

1. 2 つの基本的な CA Enterprise Log Manager サーバ（管理用および収集用）のマップ作成から開始し、各サーバの詳細を記入します。
2. 追加の収集サーバが必要かどうか、そのサーバを階層の最上位とするのか、またはメッシュ統合の 1 要素とするのかを決定します。
3. ニーズに最適な連携のタイプは階層構造なのか、あるいはメッシュ状なのかを決定します。
4. レポート、コンプライアンス、およびイベントのスループットなどのビジネスのニーズに基づいて、階層、ブランチ、または相互接続の条件を識別します。

   たとえば、会社のオフィスが 3 つの大陸にある場合、3 つの階層統合を作成するよう決定できます。さらに、経営者やセキュリティ管理者がネットワーク全体のレポートを作成できるように、上位レベルの階層をメッシュ構造とするように決定できます。少なくとも、基本的な環境で CA Enterprise Log Manager サーバの挿入とクエリを連携させる必要があります。
5. 導入する必要がある CA Enterprise Log Manager サーバの総数を決定します。

   この値は、ネットワーク内のデバイスの数と、それらが生成するイベント ボリュームに基づきます。
6. 必要とする連携サーバの階層数を決定します。

   この数は、手順 2 および 3 で行った決定の一部に基づきます。

7. 連携の各 CA Enterprise Log Manager サーバが受信するイベント タイプを識別します。

   ネットワークに多くの syslog ベースのデバイスと数台の Windows サーバがある場合、Windows イベント収集用に特別に 1 つの CA Enterprise Log Manager サーバを割り当てるように決定できます。syslog イベントのトラフィックを処理するには、複数のサーバが必要になる場合あります。どの CA Enterprise Log Manager サーバがどの種類のイベントを受信するかを前もって計画しておくと、ローカルのリスナとサービスの設定がより簡単になります。

8. 連携された(子の)CA Enterprise Log Manager サーバの設定時に使用するネットワークのマップを作成します。

   わかる場合は、DNS 名と IP アドレスをマップに含めます。CA Enterprise Log Manager サーバの DNS 名を使用してサーバ間の連携関係を設定します。

例: 大企業向けの連携マップ

連携マップを作成する場合、さまざまな統合データ セットを必要とするレポートのタイプを考慮します。たとえば、3 つのタイプのサーバ グループを使用した統合データが必要な場合のシナリオを考えてみます。

- すべてのサーバ

  自己監視イベントに関するシステム レポートの場合、すべてのサーバを含めると、CA Enterprise Log Manager ネットワーク全体のサーバの健全性を一度に評価することができます。

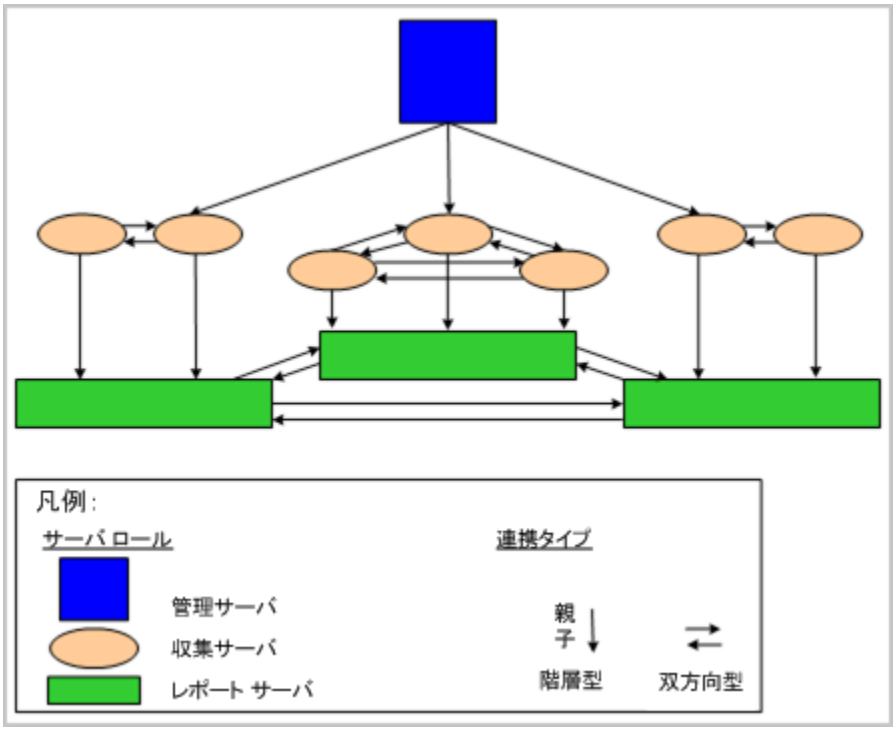
- すべてのレポート サーバ

  サマリ レポートおよびトレンド レポートでは、収集サーバが最新のイベントに対するクエリを処理しないようにしている間に、すべての収集サーバにデータを送信するすべてのエージェントが収集したデータを検査する場合、レポート サーバのみを含む連携レポートを実行する必要があります。

- レポート サーバを持つ一連の収集サーバ

  あるレポート サーバを持つ場所に限定されたデータを必要とするレポートで、収集サーバがそのサーバにまだ送信していないイベントをそのレポートに含める場合は、このサーバのサブセットに対して連携レポートを実行する必要があります。

これらのレポートの目的に合った連携マップの例を次に示します。



この連携マップの設計を実装するには、次のアクションを実行します。

- 管理サーバから各レポート サーバに関連する 1 つの収集サーバへの階層統合を作成します。この場合、管理サーバが親となり、各収集サーバは子となります。
- 各レポート サーバの収集サーバ間に、完全なメッシュ統合を作成します。
- 各収集サーバからレポート サーバへの階層統合を作成します。この場合、収集サーバが親となり、レポート サーバが子となります。
- レポート サーバ間に、完全なメッシュ統合を作成します。

特定のレポートの目的に合わせるには、連携マップの特定の場所に存在するサーバからレポートを実行することが重要です。以下に例を示します。

- ネットワーク内の各 CA Enterprise Log Manager で発生した自己監視イベントに関するシステム レポートを生成するには、管理サーバからレポートを実行します。
- ネットワーク内のすべてのレポート サーバからサマリ レポートとトレンド レポートを生成するには、任意のレポート サーバからレポートを実行します。
- レポート サーバとその収集サーバに存在するデータに関するレポートを生成するには、その収集サーバの 1 つからレポートを実行します。

例: 中規模企業向けの連携マップ

連携マップを作成する前に、各サーバ ロールに当てる予定のサーバ数を決定します。次の例では、1 つのサーバが管理とレポート専用になっており、残りのサーバは収集専用になっています。 中規模環境用にはこの設定を推奨します。管理/レポート用のサーバと収集サーバのアーキテクチャは、ハブとスポークと見なすことができます。ここでは、管理/レポート用のサーバがハブになります。連携マップ図にはこの設定が反映されていません。代わりに、階層を示すことで、階層的に連携するペアと、メッシュ状に連携するペアを簡単に区別できるようになっています。

連携マップを作成する場合、さまざまな統合データ セットを必要とするレポートとアラートを考慮します。たとえば、2 つのタイプのサーバ グループを使用した統合データが必要な場合のシナリオを考えてみます。

- 管理/レポート サーバのみ

  ほとんどのレポートでは、最近アーカイブした(ウォーム)イベントの確認が必要です。同時に、新しい(ホット)イベントのクエリの処理には、収集サーバを使用しないようにします。

  注: イベントは通常、収集サーバ(スポーク)からレポート サーバ(ハブ)に 1 時間ごとにアーカイブされます。

- すべてのサーバ

  自己監視イベントのシステム レポートでは、すべての CA Enterprise Log Manager サーバの健全性を一度に評価することが求められます。

  アラートでは、すべての収集サーバからの新規イベントに問い合わせることが重要です。

これらのレポートの目的に合った連携マップの例を次に示します。

@

この連携マップの設計を実装するには、次のアクションを実行します。

- 収集サーバ間に、完全なメッシュ統合を作成します (すべての収集サーバが他の収集サーバの親となり、子にもなります)。
- 各収集サーバから管理/レポート サーバへの階層統合を作成します。この場合、収集サーバが親となり、管理/レポート サーバが子となります。

所定の目的を満たすためには、連携マップの特定の場所で表されるサーバからのレポートまたはアラートを実行し、連携が必要かどうかを正しく指定することが重要です。以下に例を示します。

- ネットワーク内の各 CA Enterprise Log Manager で発生した自己監視イベントに関するシステム レポートをスケジュールするには、管理/レポート サーバからレポートを実行し、連携済みであることを指定します。
- 最近の(ウォーム)イベントに関するレポートをスケジュールするには、管理/レポート サーバからレポートを実行し、連携の要求をクリアします。そうしたレポートには、すべての収集サーバによって収集され、最近アーカイブされたデータが含まれます。連携は必要ではありません。
- 各収集サーバからの新しい(ホット)イベントと、管理/レポート サーバに関するアーカイブ済みの(ウォーム)イベントを含むアラートをスケジュールするには、任意の収集サーバからアラートを実行し、連携を指定します。最後の 1 時間内に、結果の条件として事前定義済み範囲を指定することにより収集サーバに返されるものを制限できます。

More information:

子サーバとしての CA Enterprise Log Manager サーバの設定 (P. 229)
例: 3 つのサーバ間の自動アーカイブ (P. 171)

ユーザとアクセスの計画

最初の CA Enterprise Log Manager サーバをインストールして EiamAdmin ユーザとしてアクセスしたら、ユーザ ストアを設定し、管理者としてユーザを設定し、パスワード ポリシーを設定できます。

ユーザとアクセスの計画は次のように制限されています。

- この CA Enterprise Log Manager サーバのデフォルトのユーザ ストアを受け入れるか、外部ユーザ ストアを設定するかを決定します。 設定する必要がある場合は、提供されたワーク シートに必要な値を記録します。
- 最初の管理者を割り当てるユーザを決定します。CA Enterprise Log Manager の設定を変更できるのは Administrator だけです。
- CA Enterprise Log Manager ユーザのパスワード強化を目的としたパスワード ポリシーを定義します。

  注: この CA Enterprise Log Manager のユーザ ストアをユーザ ストアとして設定する場合に限り、パスワード ポリシーを設定できます。

詳細情報:

外部の LDAP ディレクトリ用のワークシート (P. 42)
CA SiteMinder ワークシート (P. 44)

ユーザ ストアの計画

最初の CA Enterprise Log Manager サーバをインストールしたら、CA Enterprise Log Manager にログインしてユーザ ストアを設定します。設定されたユーザ ストアには、認証に使用されるユーザ名とパスワード、およびその他のグローバルな詳細情報が保存されます。

アプリケーション ユーザの詳細は、すべてのユーザ ストア オプションと一緒に CA Enterprise Log Manager ユーザ ストアに保存されます。これには、ロール、ユーザのお気に入り、および最後のログイン時刻などの情報が含まれます。

ユーザ ストアの設定を計画する場合は、次の内容を考慮します。

- CA Enterprise Log Manager のユーザ ストアを使用(デフォルト)

  ユーザは CA Enterprise Log Manager で作成されたユーザ名とパスワードを使用して認証されます。パスワード ポリシーを設定します。ユーザは自分のパスワードを変更し、他のユーザ アカウントのロックを解除できます。

- CA SiteMinder から参照

  ユーザ名、パスワード、およびグローバル グループは、CA SiteMinder から CA Enterprise Log Manager ユーザ ストアにロードされます。ユーザは参照されたユーザ名およびパスワードを使用して認証されます。 新規または既存のポリシーにグローバル グループを割り当てることができます。新規ユーザの作成、パスワードの変更、パスワード ポリシーの設定は実行できません。

- LDAP(Lightweight Directory Access Protocol)ディレクトリから参照

  ユーザ名とパスワードは LDAP ディレクトリから CA Enterprise Log Manager ユーザ ストアにロードされます。ユーザは参照されたユーザ名およびパスワードを使用して認証されます。ロードされたユーザ アカウント情報はグローバル ユーザ アカウントになります。そのグローバル ユーザに対して、CA Enterprise Log Manager で持つべきアクセス許可に対応するユーザ ロールを割り当てることができます。新規ユーザの作成とパスワード ポリシーの設定は実行できません。

重要: ユーザまたは任意の管理者が使用を開始する前に、CA Enterprise Log Manager に付属の事前定義済みアクセス ポリシーをバックアップすることをお勧めします。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。

詳細情報:

デフォルトのユーザ ストアの受け入れ (P. 138)
LDAP ディレクトリの参照 (P. 139)
CA SiteMinder のユーザ ストアとしての参照 (P. 141)

外部の LDAP ディレクトリ用のワークシート

外部の LDAP ディレクトリを参照する前に、次の設定情報を集めます。

必要な情報	値	コメント
タイプ		使用しているディレクトリのタイプに注意します。CA Enterprise Log Manager では、Microsoft Active Directory と Sun ONE Directory などの複数のさまざまなディレクトリをサポートしています。 サポートされているディレクトリの完全なリストについては、ユーザ インターフェースを参照してください。
ホスト		外部ユーザ ストアまたはディレクトリのサーバのホスト名を記録します。
ポート		外部ユーザ ストアまたはディレクトリ サーバが待ち受けるポート番号を記録します。ポート 389 は LDAP (Lightweight Directory Access Protocol) の Well-Known ポートです。レジストリ サーバがポート 389 を使用しない場合は、正しいポート番号を記録します。
ベース DN		ベースとして使用される LDAP 識別名 (DN) を記録します。DN とは、LDAP ディレクトリ ツリー構造にあるエントリの一意の識別子です。ベース DN にスペースは使用できません。この DN の下で検出されるグローバル ユーザとグループのみがマッピングされ、CA Enterprise Log Manager のアプリケーション グループまたはロールが割り当てられます。

必要な情報	値	コメント
パスワード		[ユーザ DN]行にリスト表示されたユーザのパスワードを入力し、確認します。
ユーザ DN		ユーザ レコードが検索可能なユーザ レジストリにある任意の有効なユーザの有効なユーザ認証情報を入力します。ユーザの完全な識別名（DN）を入力します。 Administrator ロールを持つ任意のユーザ ID を使用してログインできます。User DN および関連するパスワードは、外部ディレクトリのホストに接続する際に使用される認証情報です。
トランスポート レイヤ セキュリティ（TLS）の使用		プレーン テキストの転送を保護するためにユーザ ストアで TSL フレームワークを使用するかどうかを指定します。選択した場合、外部ディレクトリに LDAP 接続が行われる場合に TLS が使用されます。
未知の属性を含む		LDAP ディレクトリと同期されないフィールドを含むかどうかを指定します。マッピングされない外部属性は、検索のために、およびフィルタとして使用できます。
グローバル ユーザをキャッシュ		すぐにアクセスできるように、メモリにグローバル ユーザを保存するかどうかを指定します。これを選択するとより高速な検索を実行できますが、スケーラビリティは低下します。小さいテスト環境の場合は、選択することをお勧めします。
キャッシュ更新時間		グローバル ユーザをキャッシュするよう選択した場合、キャッシュされたグローバル グループおよびユーザに新しいレコードや変更されたレコードが含まれるように更新する頻度を分単位で指定します。
グローバル ユーザ グループとして Exchange グループを取得		外部ディレクトリのタイプが Microsoft Active Directory である場合、このオプションでは Microsoft Exchange のグループ情報からグローバル グループを作成するかどうかを指定します。選択された場合、配布リストのメンバに対するポリシーを作成できます。

CA SiteMinder ワークシート

ユーザ ストアとして CA SiteMinder を参照する前に、次の設定情報を集めます。

必要な情報	値	コメント
ホスト		参照する CA SiteMinder システムのホスト名または IP アドレスを定義します。IPv4 または IPv6 の IP アドレスを使用できます。
管理者名		システムとドメイン オブジェクトを管理する CA SiteMinder のスーパー ユーザのユーザ名。
管理者のパスワード		関連付けられたユーザ名のパスワード。
エージェント名		ポリシー サーバ対して提供されたエージェントの名前。この名前では大文字と小文字は区別されません。
エージェント パスワード		CA SiteMinder に定義されている、大文字と小文字を区別する共有のパスワード。エージェント パスワードは大文字と小文字を区別します。
グローバル ユーザをキャッシュ		メモリにグローバル ユーザをキャッシュするかどうかを指定します。これにより高速な検索を実行できますが、スケーラビリティは低下します。 **注**: グローバル ユーザ グループは常にキャッシュされます。
キャッシュ更新時間		ユーザのキャッシュが自動的に更新される間隔（分）。
未知の属性を含む		フィルタとして、または検索で使用するために、マッピングされていない外部属性を含むかどうかを指定します。
グローバル ユーザ グループとして Exchange グループを取得		外部ディレクトリのタイプが Microsoft Active Directory である場合、このオプションでは Microsoft Exchange のグループ情報からグローバル グループを作成するかどうかを指定します。選択された場合、配布リストのメンバに対するポリシーを作成できます。
許可ストア タイプ		使用するユーザ ストアのタイプを定義します。

必要な情報	値	コメント
許可ストア名		[許可ストア タイプ]フィールドで参照されるユーザ ストアに割り当てられた名前を指定します。

Administrator ロールを持つユーザ

Administrator ロールを割り当てられたユーザだけが CA Enterprise Log Manager コンポーネントを設定できます。

最初の CA Enterprise Log Manager をインストールした後に、ブラウザを使用して CA Enterprise Log Manager にアクセスし、EiamAdmin 認証情報を使用してログインしてユーザ ストアを設定します。

次の手順では、設定を行うユーザ アカウントに Administrator アプリケーション グループを割り当てます。デフォルトの CA Enterprise Log Manager ユーザ ストアをユーザ ストアとして設定したら、新しいユーザ アカウントを作成してそのユーザに Administrator ロールを割り当てます。外部のユーザ ストアを参照する場合は、新規ユーザを作成できません。 この場合、管理者にする予定の個人のユーザ レコードを検索し、このユーザ アカウントを Administrator アプリケーション グループに追加します。

パスワード ポリシーの計画

デフォルトのユーザ ストアを受け入れたら、新しいユーザを定義し、CA Enterprise Log Manager からこのユーザ アカウントのパスワード ポリシーを設定します。強力なパスワードを使用すると、ユーザのコンピュータ リソースを保護できます。パスワード ポリシーによって、強力なパスワードの作成を支援し、脆弱なパスワードを使用しないようにすることができます。

CA Enterprise Log Manager で使用されるデフォルトのパスワード ポリシーは、非常に柔軟性の高いパスワード保護機能を提供します。たとえば、デフォルトのポリシーでは、ユーザがパスワードとしてユーザ名を使用することができます。また、ユーザがパスワードのロックを解除することもできます。パスワードの有効期限が切れないようにすることができ、ログインの失敗に基づいてロックされません。デフォルトのオプションは、独自のカスタム パスワード ポリシーを作成できるように、意図的に非常に低いレベルのパスワード セキュリティが設定されています。

重要: 自分の会社で使用しているパスワード制限と一致するように、デフォルトのパスワード ポリシーを変更する必要があります。稼働環境でデフォルトのパスワード ポリシーを使用して CA Enterprise Log Manager を実行することはお勧めしません。

これらのアクティビティを禁止し、長さ、文字のタイプ、有効期限、および再利用できるかどうかなどのパスワード属性に関するポリシーを適用し、カスタム パスワード ポリシーの一部として設定可能な失敗したログインの試行回数に基づいてロック ポリシーを作成できます。

詳細情報:

パスワード ポリシーの設定 (P. 142)

パスワードとしてのユーザ名

強力なパスワードを作成するために、セキュリティのベスト プラクティスとして、パスワードはユーザ名を含まない、またはユーザ名と一致させないようにする必要があります。デフォルトのパスワード ポリシーでは、このオプションは有効です。新規ユーザ用の一時パスワードを設定する場合にはこのオプションが便利に思えますが、このパスワード ポリシーの選択をオフにしておくほうが適しています。このオプションをオフにすると、ユーザがこのような脆弱なパスワードを使用するのを防止します。

パスワードの有効期限と再利用

有効期限と再利用のポリシーを決定する場合は、次のガイドラインを考慮します。

- パスワードの再利用のポリシーでは、必ず特定のパスワードが頻繁に再利用されないようにすることができます。このポリシーではパスワードの履歴を作成します。0 という設定は、パスワード履歴が作成されないことを意味します。0 より大きい値に設定すると、変更したパスワードを指定した数だけ保存し、比較用に使用することができます。パスワード ポリシーを強力にするには、ユーザが少なくとも 1 年間はパスワードを再利用しないようにする必要があります。

- パスワードに推奨される最長有効期限は、パスワードの長さと複雑さに応じて変わります。一般的なルールでは、パスワードの最長有効期限までの間に総当り攻撃でも見破られないパスワードが最適なパスワードです。最長有効期限に適した基準は、30 日から 60 日です。
- 最短有効期限を設定すると、再利用を制限するポリシーが適用されるため、1 つのセッションで何回もパスワードをリセットすることはできません。一般的なベスト プラクティスで推奨されているのは 3 日です。
- パスワードの有効期限を設定する場合は、パスワードのリセットをユーザに警告することをお勧めします。有効期限の中間点または有効期限の終了時に警告が発生するように設定できます。
- ユーザが適当な回数ログインに失敗したら、ユーザ アカウントをロックする必要があります。これによって、ハッカーによるパスワードの推測が成功しないようにすることができます。アカウントをロックする標準的な回数は、3 ～ 5 回の試行です。

パスワードの長さと形式

パスワード長を制限するべきかどうかを決定する場合は、次のガイドラインを考慮します。

- パスワードの暗号化方式の観点から、最も安全なパスワードは 7 文字または 14 文字です。
- ネットワーク上にある古いオペレーティング システムによって適用されたパスワード長の制限を超えないように注意します。

文字の最大繰り返し回数、または最小文字数、または数字に関するポリシーを強制するかどうかを決定する場合は、次のガイドラインを考慮します。

- 辞書に載っている用語は、強力なパスワードにはなりません。
- 強力なパスワードには、小文字、大文字、数字、および特殊文字の 4 つのセットのうち、少なくとも 3 種類から 1 つ以上の文字が含まれます。

サブスクリプションの更新の計画

このセクションでは、CA Enterprise Log Manager 環境用にサブスクリプション更新を計画するための情報および手順について説明します。

詳細情報:

サブスクリプション サービス (P. 49)
サブスクリプションの仕組み (P. 50)
サブスクリプション更新を計画する方法 (P. 52)
サブスクリプション アーキテクチャ (P. 53)
オフライン サブスクリプション アーキテクチャ (P. 57)

サブスクリプション サービス

運用環境では、1 つのサーバによってすべてのタスクが実行されるようにすることも、複数のサーバを設定して各サーバに特定のロール（収集、相関、レポートなど）の実行を割り当てることもできます。サブスクリプション サービスを使用することにより、すべてのサーバが最新のコンテンツ、オペレーティング システム、および製品の更新で常に最新の状態に維持されるようにすることができます。

サブスクリプション サービスは、プロキシ/クライアント システムを使用して更新を配布します。CA は、CA サブスクリプション サーバに、モジュールにパッケージ化された更新を発行します。環境内の 1 つ以上のサーバはサブスクリプション プロキシとして機能します。これらのプロキシは、インターネットを介して CA サブスクリプション サーバにアクセスし、更新モジュールをダウンロードして自己インストールを行います。環境内の他のすべてのサーバは、サブスクリプション クライアントとなり、プロキシから更新を順番にダウンロードします。

一部の環境では、セキュリティ ポリシーまたは他の考慮事項によって、インターネットへのネットワーク アクセスが制限されています。そのような場合は、オフライン サブスクリプションを通じて CA Enterprise Log Manager 環境を更新します。オフライン サブスクリプションでは、CA オフライン サブスクリプション FTP サイトから更新をダウンロードする必要があります。ダウンロードした更新は、インターネット アクセスのない CA Enterprise Log Manager プロキシ（オフライン プロキシ）に手動でコピーします。その後は、このオフライン プロキシからサブスクリプション クライアントが更新をダウンロードしてインストールするという通常の方法で更新が続行されます。

注: デフォルトでは、サブスクリプション サービスは自動更新を実行するように設定されていません。サブスクリプション サービスを使用するには、モジュールの選択や更新スケジュール設定など、特定の設定を行う必要があります。

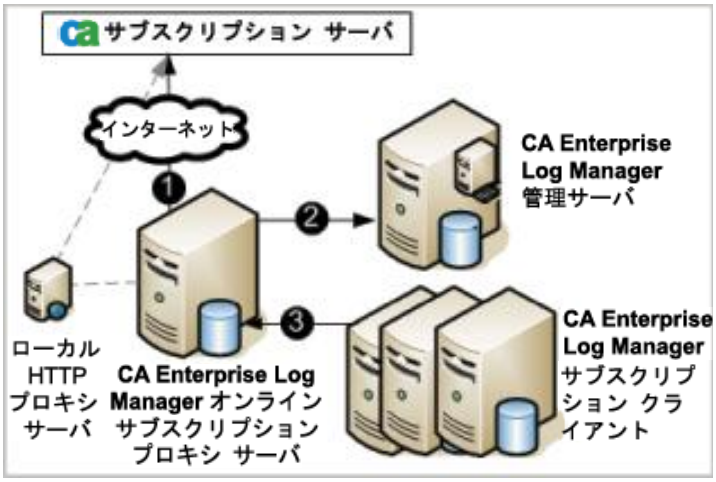
サブスクリプションの仕組み

サブスクリプションには、以下のコンポーネントが含まれます。

- CA サブスクリプション サーバ
- HTTP プロキシ サーバ（オプション）
- CA Enterprise Log Manager サブスクリプション プロキシ サーバ
- CA Enterprise Log Manager 管理サーバ
- CA Enterprise Log Manager サブスクリプション クライアント

設定したサブスクリプション スケジュールに従って、自動的にサブスクリプション更新が行われるよう設定できます。または必要に応じて手動で更新プロセスを開始し、サブスクリプション更新をオンデマンドで実行することもできます。

以下の図は、サブスクリプション サービスのプロセスを詳細に示したものです。



1. サブスクリプション プロキシ サーバは、CA サブスクリプション サーバにアクセスします。プロキシ サーバがサブスクリプション サーバに直接接続するか、またはローカルの HTTP プロキシを介して接続するかを設定できます。プロキシから CA サブスクリプション サーバへのアクセスは、設定されたスケジュールに従って自動的に、または必要に応じて手動で開始することによってオンデマンドで実行されます。プロキシ サーバは、オペレーティング システムおよび製品の更新をダウンロードして自己インストールします。

   オフライン サブスクリプションを使用している場合、CA Enterprise Log Manager 環境とは別のシステムに更新ファイルを手動でダウンロードし、オフライン プロキシ サーバにコピーします。

2. サブスクリプション プロキシは、コンテンツと統合の更新を管理サーバにプッシュします。デフォルトでは、最初にインストールされた CA Enterprise Log Manager サーバが管理サーバとなり、レポート、統合、相関ルールなど、その環境用のすべてのコンテンツ情報を格納します。

3. 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 プロキシに自動またはオンデマンドで接続し、更新を確認します。クライアントは更新をダウンロードして自己インストールします。

   注: サブスクリプション プロキシでダウンロードした更新をインストールすると、クライアントがそれらの更新を使用できるようになります。

サブスクリプション更新を計画する方法

使用している CA Enterprise Log Manager 環境用にサブスクリプション更新の方法を計画することにより、すべてのサーバで適宜かつ安全な方法で更新を確実に受信できるようにします。

CA Enterprise Log Manager 環境用にサブスクリプション更新を計画するには、以下を実行します。詳細については、関連する手順を参照してください。

1. 最初に、CA Enterprise Log Manager サーバ用のプロキシ/クライアント構造を設計します。プロキシとして使用するサーバおよびクライアントとして使用するサーバを決定します。その際、各サーバのロールやネットワークトラフィックに関する懸念事項を考慮します。
2. 環境におけるインターネット アクセスの制約を考慮し、オフライン プロキシが必要かどうかを判断します。
3. インターネット セキュリティおよびトラフィックの懸念事項を考慮し、サブスクリプション アーキテクチャにローカルの HTTP プロキシを含むかどうかを決定します。オンライン サブスクリプション プロキシは、CA サブスクリプション サーバに直接アクセスするか、またはローカルの HTTP プロキシを使用してアクセスできます。
4. 設定されたサブスクリプション スケジュールに従ってすべての更新を自動的にダウンロードするか、または更新のタイプによっては手動でダウンロードするかどうかを検討します。たとえば、内部セキュリティ ポリシーの場合は、環境に適用する前に特定のアップグレードをテストする必要がある場合があります。
5. CA Enterprise Log Manager 環境を更新する頻度を検討します。更新は定期的に利用可能です。頻度は、更新のタイプに依存します。更新タイプの詳細については、「詳細情報」の「ダウンロードするモジュールについて」を参照してください。

   注: サブスクリプション更新を続行する前に、各 CA Enterprise Log Manager サーバにサブスクリプション更新をダウンロードするのに十分なディスク容量があることを確認します。サーバ上の利用可能なディスク容量が 5GB 未満である場合、サブスクリプション サービスは自己監視イベントを発行し、ダウンロード プロセスを一時停止します。

詳細情報:

サブスクリプション アーキテクチャ (P. 53)
オフライン サブスクリプション アーキテクチャ (P. 57)
ダウンロードするモジュールについて (P. 197)

サブスクリプション アーキテクチャ

CA Enterprise Log Manager 環境としては、1 つのサーバが存在する場合、または複数のサーバが存在する場合のどちらも考えられます。環境内の CA Enterprise Log Manager サーバの数およびロールに基づいてサブスクリプション アーキテクチャを設計してください。以下のサブスクリプション アーキテクチャが可能です。

- 単一サーバ環境
- 1 つのサブスクリプション プロキシを含む複数サーバの環境
- 複数のサブスクリプション プロキシを含む複数サーバの環境

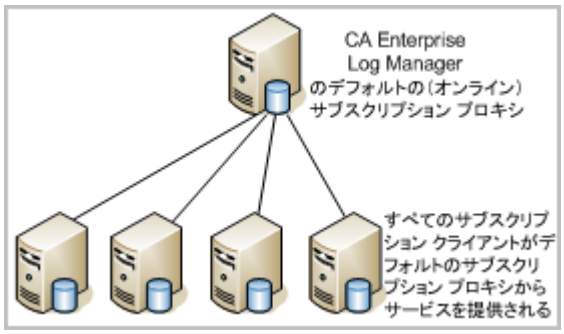
注: サブスクリプション アーキテクチャを選択する際は、オフライン プロキシが必要かどうかを検討してください。詳細については、「詳細情報」の「オフライン サブスクリプション アーキテクチャ」を参照してください。

最初にインストールする CA Enterprise Log Manager サーバは、インストール時にデフォルトのサブスクリプション プロキシとして設定されます。これは、他のプロキシが設定されていないか利用可能でない場合、サブスクリプション更新をダウンロードしてインストールします。後続の CA Enterprise Log Manager サーバは、デフォルトでは、サブスクリプション クライアントとして設定されます。任意の CA Enterprise Log Manager サーバの設定を変更して、オンラインまたはオフラインのサブスクリプション プロキシ、サブスクリプション クライアントとして機能するようにできます。また、環境内のいずれかのオンライン サブスクリプション プロキシをデフォルトのサブスクリプション プロキシとして機能するよう設定できます。

コンテンツ サーバは、コンテンツおよび統合の更新を管理サーバに提供します。管理サーバは、環境用のアプリケーション コンテンツを格納して取得します。このサーバは、デフォルトのサブスクリプション プロキシとして使用できます。環境内のいずれかのオンライン サブスクリプション プロキシをコンテンツ サーバとして機能するよう設定することも可能です。

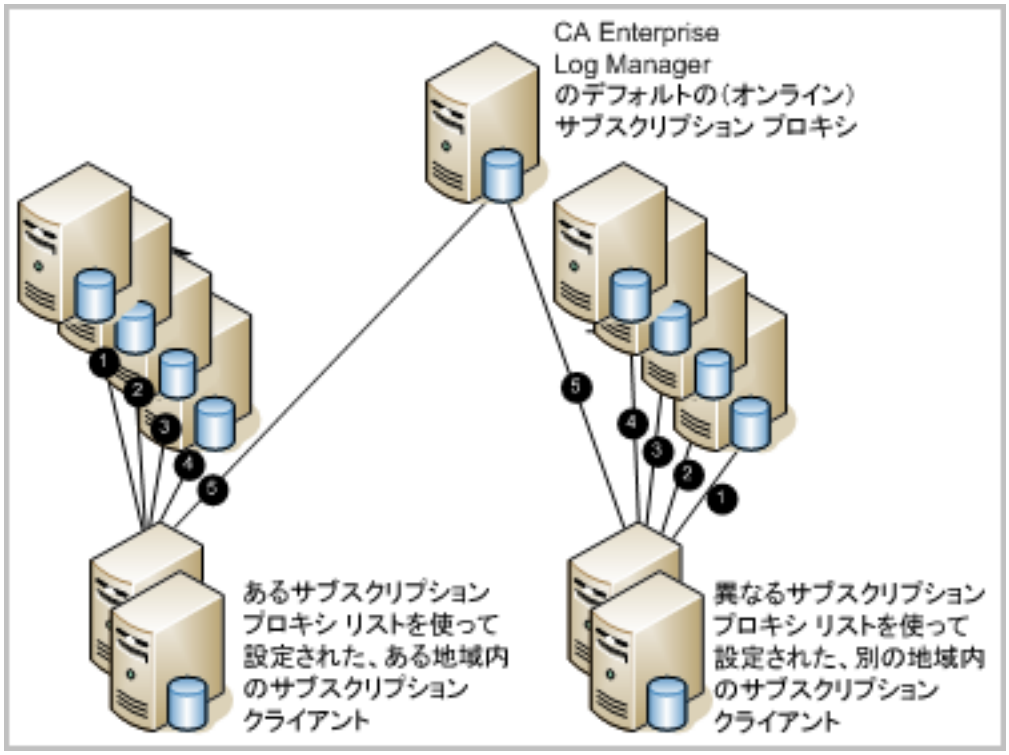
単一サーバ環境では、唯一の CA Enterprise Log Manager サーバがサブスクリプション プロキシとして設定されます。このサーバはサブスクリプション サービスによって CA Enterprise Log Manager 更新をダウンロードして自己インストールします。このサーバは、その環境用のコンテンツ サーバとしても機能します。

2 つ以上のサーバを備えた小規模な環境では、1 つのサーバをサブスクリプション プロキシおよびコンテンツ サーバの両方として設定し、他のすべてのサーバをサブスクリプション クライアントとして設定できます。デフォルトのサブスクリプション プロキシをサブスクリプション プロキシとして機能させることを選択できます。またはどの CA Enterprise Log Manager サーバでもプロキシとして選択可能です。サブスクリプション プロキシは、CA Enterprise Log Manager 更新をダウンロードして自己インストールします。サブスクリプション クライアントは、プロキシにアクセスしてそれらの更新を順にダウンロードします。 クライアントでは、プロキシがダウンロードした更新と同じものをダウンロードするか、そのグループのサブセットをダウンロードするよう設定できます。



大規模な複数サーバ環境では、複数のサーバをサブスクリプション プロキシとして設定し、それぞれのサーバが特定のサブスクリプション クライアントのグループに更新を提供するよう設定することもできます。これにより、サブスクリプション プロキシへのトラフィックが分散され、サブスクリプション サービスが効率よく機能することが可能になります。

複数のプロキシを使用する場合、サブスクリプション プロキシ リストを設定できます。プロキシ リストを設定することにより、CA Enterprise Log Manager サーバが最新の更新を適宜確実に受信できるようになります。クライアントが CA Enterprise Log Manager 更新を要求したときに、指定されたプロキシが利用不可能である場合、クライアントはそのプロキシ リスト内の各プロキシに順番にアクセスし、更新をダウンロードできるまで続けます。お使いの CA Enterprise Log Manager 環境全体に対して、クライアント更新用およびコンテンツ更新用にグローバルのプロキシ リストを設定できます。また、各 CA Enterprise Log Manager サーバごとにクライアント更新用のカスタム プロキシ リストを設定することもできます。



詳細情報

サブスクリプション更新を計画する方法 (P. 52)
オフライン サブスクリプション アーキテクチャ (P. 57)

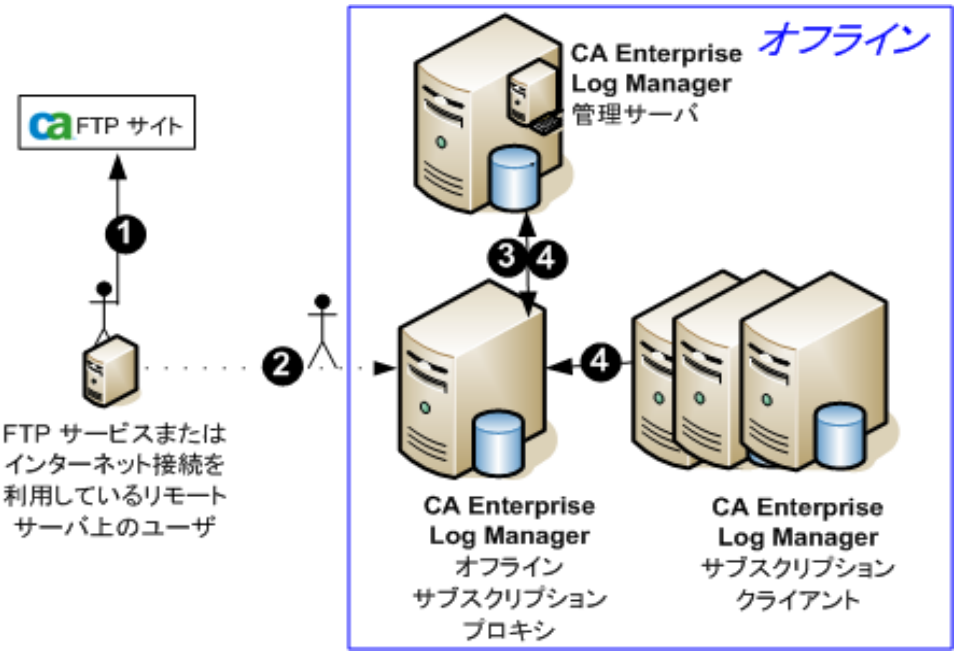
オフライン サブスクリプション アーキテクチャ

セキュリティ ポリシーまたは他の懸念事項によってインターネットへのネットワーク アクセスが制限されている場合、オフライン サブスクリプションを通じて CA Enterprise Log Manager 環境を更新できます。オフライン サブスクリプションによって、サーバの一部またはすべてをインターネットに接続しなくても、CA Enterprise Log Manager 環境を最新の状態に保つことが可能になります。オフライン サブスクリプションの設定が必要となる状況として以下の場合があります。

- CA Enterprise Log Manager 環境内のどのサーバにもインターネット アクセスが許可されていない。
- ネットワーク内の一部のサーバにはインターネット アクセスが許可されているが、他のサーバにはインターネット アクセスが可能なサーバへの接続さえも許可されていない。

オンラインとオフラインのサブスクリプションの唯一の違いは、更新ファイルがサブスクリプション プロキシに配布される方法です。オンライン サブスクリプションの場合、プロキシは、インターネット経由で CA サブスクリプション サーバにアクセスします。オフライン サブスクリプションの場合、CA FTP サイトから更新をダウンロードし、それをオフライン プロキシとして設定された CA Enterprise Log Manager サーバに手動でコピーします。

以下の図は、オフライン サブスクリプション プロセスを示しています。この例では、CA Enterprise Log Manager 環境全体がオフラインです。



1. システム管理者は、CA FTP サイトから、インターネットまたは FTP アクセスが許可されているシステムに更新をダウンロードします。
2. システム管理者は、オフライン CA Enterprise Log Manager プロキシに更新ファイルを手動でコピーします。ディスクなどの物理メディアまたは CA Enterprise Log Manager に含まれている scp を使用してファイルを転送できます。
3. その後はオンライン サブスクリプションと同じ様に更新が続行します。オフライン プロキシは、更新を自己インストールして、コンテンツ更新を管理サーバにプッシュします。

   注: スケジュールに従ってオフライン プロキシが自身を更新するように設定できます。新規ファイルを転送した場合はオフライン プロキシ上で手動更新を実行することをお勧めします。そうすることにより、サブスクリプション クライアントで更新が要求された場合にその更新が使用可能な状態であることが保証されます。
4. オフライン プロキシのクライアントが、設定したスケジュールに従って、またはユーザが手動更新を実行することによって、更新をダウンロードします。

   注: オフライン サブスクリプション クライアントは、オフライン プロキシ サーバに手動でインストールされるすべての更新を常に受信します。ローカル レベルでオフライン サブスクリプション クライアントに選択されたサブスクリプション モジュールは関係ありません。

サブスクリプション アーキテクチャには「混在」の場合もあります。たとえば、1 つのプロキシをオフラインとして割り当て、他のプロキシをオンラインとして使用できます。その場合、オフライン プロキシとそれに割り当てられたクライアントはインターネットから隔離されたままになる一方で、CA Enterprise Log Manager 環境の残りの部分はオンライン サブスクリプションを通じて更新を受信します。混在アーキテクチャは、複雑過ぎるためベスト プラクティスにはなり得ません。このアーキテクチャを実装する場合は、全体のサブスクリプション戦略を慎重に検討して計画してください。

重要: 混在サブスクリプション環境では、オンライン サブスクリプション クライアント用のプロキシ リストにオフライン プロキシを含めないでください。含めた場合、オンライン サブスクリプション クライアントは、CA Enterprise Log Manager 環境またはそのクライアントに対してローカルに選択されたモジュールではなく、手動でインストールされたすべての更新を自動的に受信します。

詳細情報

サブスクリプション更新を計画する方法 (P. 52)
サブスクリプション アーキテクチャ (P. 53)

例: 6 台のサーバによるサブスクリプションの設定

サブスクリプションの設定に着手する場合、サブスクリプション ロールを決定する前に、サーバが実行している他のロールを考慮します。デフォルトでは、最初にインストールしたサーバである管理サーバは、デフォルトのサブスクリプション プロキシになります。他のすべてのサーバは、デフォルトのサブスクリプション プロキシのサブスクリプション クライアントになります。この設定を受け入れることもできますが、オンライン サブスクリプション プロキシを設定して、デフォルトのプロキシをフェイルオーバー用または冗長プロキシとして動作させることをお勧めします。最も使用頻度の低いサーバに、オンライン プロキシとしてのロールを割り当てるのも良い方法です。

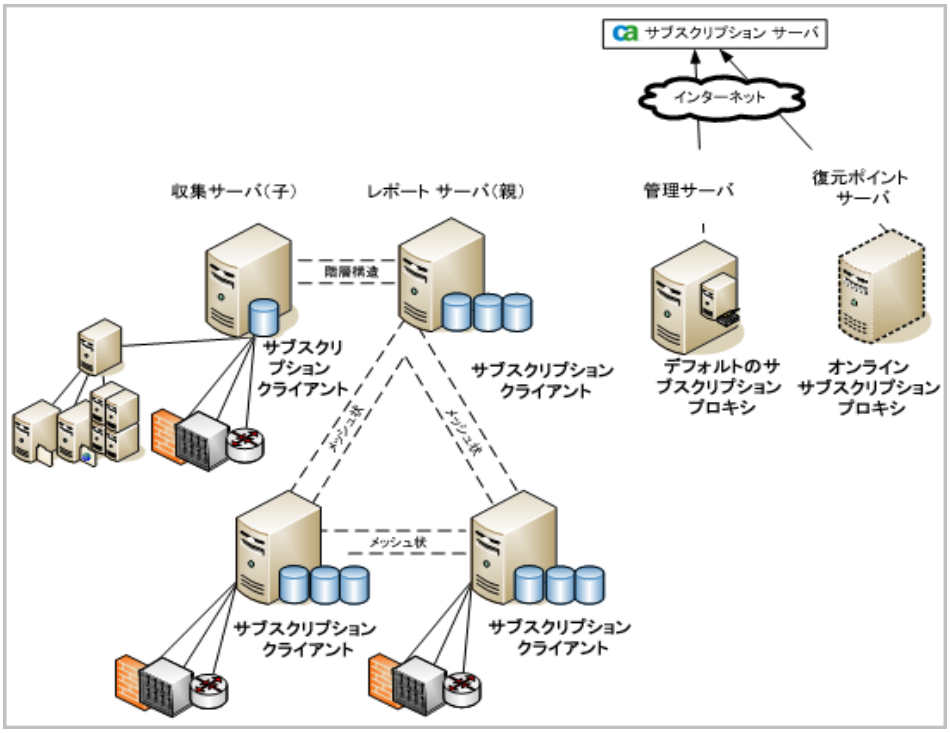
例: 最もビジーでないサーバがオンライン サブスクリプション プロキシである場合の 6 台のサーバ

6 台の CA Enterprise Log Manager サーバのシナリオを考えてみます。管理サーバは、ログイン時のユーザの認証と許可、およびアプリケーション コンテンツの保存専用のサーバです。連携した 4 台のサーバは、イベント処理およびレポート処理を行います。6 番目のサーバは、復元されたデータベースからのイベントを調査するための専用復元ポイントです。専用復元ポイントを使用する利点は、連携にこのサーバを含めないことで、古いデータが最新のレポートに含まれないようにできる点です。

この例では、「収集」と「レポート」とラベル付けされた 2 台のサーバが、他のサーバよりも高負荷の処理要件を持つように設定されています。これらのサーバは階層構成で連携され、収集サーバはレポート サーバの子になっています。収集サーバおよびレポート サーバの両方として動作する 2 台のサーバは、通常のイベント ボリュームとスケジュール済みレポートを提供するように設定されています。これらは互いに連携し、メッシュ統合で専用のレポート サーバとして機能しています。つまり、3 台のサーバがピアになっています。サーバを連携させる目的は、連携したサーバからもクエリの結果が得られるように機能を拡張することです。 メッシュ構成にしたサーバの任意のサーバから連携クエリを実行すると、そのサーバ自身と連携内の他の 3 つのサーバからのイベントが返されます。

注: 自己監視イベントに関する統合レポートを実行する場合は、連携に管理サーバを含めます。

このシナリオで推奨されるソリューションは、復元ポイントをオンライン サブスクリプション プロキシとして設定することですが、それは、復元ポイントが最も使用頻度の低いサーバであるためです。次に、各クライアントがこのオンライン プロキシを参照するように設定し、オンライン プロキシがビジー状態や使用不可能な状態の場合でも、デフォルトのプロキシがバックアップとして動作できるようにします。



詳細情報:

CA Enterprise Log Manager の連携の設定 (P. 229)

エージェントの計画

エージェントはコネクタを使用してイベントを収集し、CA Enterprise Log Manager サーバにそのイベントを転送します。CA Enterprise Log Manager サーバと一緒にインストールされたデフォルトのエージェントにコネクタを設定できます。あるいは、ネットワークのサーバまたはイベント ソースにエージェントをインストールできます。外部エージェントを使用するかどうかの決定は、イベント ボリューム、エージェントの場所、ニーズをフィルタリングするデータ、およびその他の考慮事項に基づきます。エージェントのインストールの計画には次の内容が含まれます。

- 次のコンポーネントの関係を理解する
  - 統合とリスナ
  - エージェント
  - コネクタ
- ネットワークのサイズを決定し、インストールするエージェント数を決定する

イベント ログを収集するイベント ソースの比較的近くにエージェントをインストールする必要があります。ほとんどのコネクタは 1 つのイベント ソースのみからイベントを収集します。syslog イベントの場合は、1 つの syslog リスナが複数のイベント ソース タイプからのイベントを受信できます。エージェントは複数のコネクタからのイベント トラフィックを制御および処理できます。

Syslog イベントの収集について

CA Enterprise Log Manager では、syslog ソースからイベントを直接受信できます。複数の異なるログ ソースが CA Enterprise Log Manager に同時にイベントを送信できるため、syslog の収集は他の収集方法とは異なります。2 つの使用可能なイベント ソースとして、ネットワーク ルータと VPN コンセントレータについて考えてみます。いずれも syslog を使用して CA Enterprise Log Manager に直接イベントを送信できますが、ログ形式と構造が異なります。syslog エージェントは、提供された syslog リスナを使用して、同時に両方の種類のイベントを受信できます。

一般的に、イベント収集は次の 2 つのカテゴリに分類されます。

- CA Enterprise Log Manager は設定可能なポートで syslog イベントを待ち受けます。
- CA Enterprise Log Manager は、たとえば WMI を使用して Windows イベントを収集するなど、他のイベント ソースのイベントを監視します。

リスナは指定されたポートのすべてのトラフィックを受信するため、複数の syslog イベント ソースが 1 つのコネクタを使用してイベントを転送できます。CA Enterprise Log Manager は任意のポートで syslog イベントを待ち受けることができます（root 以外のユーザでエージェントを実行している場合は、1024 より小さいポートの使用に対する制限がある場合があります）。標準ポートでは、さまざまなタイプの syslog イベントで構成されるイベント ストリームを受信する場合があります。このイベントには、UNIX、Linux、Snort、Solaris、CiscoPIX、Check Point Firewall 1 などが含まれます。CA Enterprise Log Manager は、専用のタイプの統合コンポーネントであるリスナを使用して syslog イベントを処理します。リスナと統合に基づいて、次のように syslog コネクタを作成します。

- リスナは、ポートまたはトラステッド ホストなどの接続情報を提供します。
- 統合は、メッセージ解析（XMP）ファイルおよびデータ マッピング（DM）ファイルを定義します。

1 つの syslog コネクタが多くのイベント ソースからのイベントを受信する場合があるため、そのタイプやソースに基づいて、syslog イベントをルーティングするべきかどうかを検討する必要があります。次のように、環境のサイズおよび複雑さによって、syslog イベントの受信のバランスをどのように保つかを判断します。

多数の syslog タイプ：1 つのコネクタ

1 つのコネクタがさまざまな syslog ソースからのイベントを処理する必要があり、イベント ボリュームも多い場合、コネクタは、イベントに一致するものを見つけるまで、適用されたすべての統合（XMP ファイル）を使用して解析する必要があります。処理量が非常に多くなるため、パフォーマンスが低下する場合があります。一方で、イベント ボリュームがそれほど多くない場合は、保存する必要のあるすべてのイベントを収集するのに、デフォルト エージェントの 1 つのコネクタを使用すれば十分である場合があります。

1 つの syslog タイプ: 1 つのコネクタ

1 つの syslog タイプからのイベントを処理するために一連の単一のコネクタを設定する場合、負荷を複数のコネクタに分散させることによって、処理の負荷を軽くすることができます。一方で、各コネクタは個別の処理を必要とする別々のインスタンスであるため、1 つのエージェントで実行するコネクタが多すぎると、パフォーマンスが低下する場合があります。

複数の syslog タイプ: 1 つのコネクタ

環境内で特定のタイプの syslog イベントのボリュームが多い場合、コネクタがそのタイプだけを収集するように設定することも可能です。環境内でイベント ボリュームが少ない複数のタイプの syslog イベントを 1 つ以上の他のコネクタで収集するように設定できます。この方法を使用すれば、少数のコネクタ間で syslog イベント収集の負荷を分散でき、パフォーマンスを改善できます。

必ずしも独自の syslog リスナを作成する必要はありませんが、必要に応じて独自のリスナを作成することもできます。別の syslog リスナを作成して、ポートに異なるデフォルト値を使用したり、トラステッド ホストなどを使用できます。これによって、たとえばたくさんのコネクタを syslog イベントのタイプごとに作成する場合、コネクタの作成が簡略化されます。

詳細情報:

デフォルトのユーザ アカウント (P. 107)
syslog イベント用のファイアウォール ポートのリダイレクト (P. 115)

エージェントおよびエージェント証明書

事前定義された CAELM_AgentCert.cer 証明書は、すべてのエージェントが CA Enterprise Log Manager サーバとの通信に使用します。

この証明書をカスタムの証明書で置き換える場合は、エージェントをインストールする前に置き換えておくことをお勧めします。エージェントがインストールされ CA Enterprise Log Manager サーバに登録された後にカスタム証明書を実装した場合、各エージェントをアンインストールし、エージェント エクスプローラからエージェント エントリを削除し、エージェントを再インストールしてコネクタを再設定する必要があります。

エージェントについて

エージェントは、インストール後にサービスまたはデーモンとして動作するオプションの製品コンポーネントで、次のうちの 1 つ以上の状況下で使用されます。

- 小規模のリモート サイトでイベント データを収集する必要があるが、完全な CA Enterprise Log Manager ソフトウェア アプライアンスは不要である。
- ネットワーク トラフィックまたは保存するデータの量を削減するために、イベント ソースでデータをフィルタする必要がある。
- コンプライアンスのために、イベント ログ ストアへのイベント配信を確実に実行する必要がある。
- ネットワーク全体で、データの暗号化を使用してログの転送をセキュリティ保護する必要がある。

エージェントは、特定のアプリケーション、オペレーティング システム、またはデータベースからイベント データを収集するコネクタのプロセス マネージャとして動作します。また、CA Enterprise Log Manager のエージェント エクスプローラ インターフェースで、開始、停止、再起動などのコネクタ管理コマンドを提供しています。さらに、コネクタの設定変更やバイナリの更新を適用します。

個々のイベント ソースにエージェントをインストールできます。あるいは、エージェントをリモート ホスト サーバにインストールして、複数のイベント ソースからイベントを収集できます。CA Enterprise Log Manager サーバをインストールすると、自動的に自身のエージェントがインストールされます。このデフォルト エージェントを使用して syslog イベントを直接収集できます。

また、ネットワークの任意の CA Enterprise Log Manager サーバのエージェント エクスプローラから、任意のエージェントのステータスを表示できます。エージェントには、突然停止した場合にエージェントを再起動するウォッチドッグ サービスがあり、エージェントとコネクタのバイナリの更新が監視されます。また、変更とステータスを追跡するために、自己監視イベントをイベント ログ ストアに送信します。

エージェント グループについて

エージェント グループも作成できます。エージェント グループは、管理を容易にするためのエージェントの論理グループです。エージェントをエージェント グループに入れたら、設定を変更して、グループ内のすべてのコネクタを同時に開始したり停止したりできます。たとえば、物理的および地理的な地域ごとにエージェントをグループ化するように決定する場合があります。

エージェント エクスプローラでグループを作成したり、グループ間でエージェントを移動できます。エージェント グループを定義しない場合、すべてのエージェントは CA Enterprise Log Manager をインストールしたときに作成されたデフォルトのグループに属します。

エージェントの設定およびエージェント グループのレコードは管理サーバに保存されます。エージェントをインストールするたびに、管理サーバは、同じアプリケーション インスタンス名の下に登録されたすべての CA Enterprise Log Manager サーバがエージェント エクスプローラで新しいエージェントを使用できるようにします。これによって、ネットワーク内の任意の CA Enterprise Log Manager サーバから任意のエージェントを設定して制御できます。

エージェントのユーザ アカウントの権限

エージェントは権限レベルの低いユーザ アカウントで実行できます。エージェントをインストールする前に、ターゲット ホストでグループとサービス ユーザ アカウントを作成する必要があります。エージェントのインストール時にユーザ名を指定すると、インストール プログラムによって適切なアクセス権が設定されます。Linux システムでは、エージェント ユーザは root ユーザが所有するウォッチドッグのバイナリ以外のすべてのエージェント バイナリを所有します。

統合について

統合の既定のセットとは、本質的にはテンプレートのライブラリです。これらのテンプレートは、特定の種類のログ ソースからのイベント収集に特化されたコードを提供します。ライブラリから取得され、設定され、イベント ソースに適用されると、統合はコネクタになります。統合には次の種類の情報が含まれます。

- 特定の種類のイベント ソースに関する情報を持つデータ アクセス ファイル
- 収集されたイベント ログから名前と値のペアを作成するメッセージ解析ファイル
- 解析された名前と値のペアを、CA Enterprise Log Manager サーバのイベント ログ ストアのデータベース スキーマを形成する共通イベント文法にマッピングするデータ マッピング ファイル

CA Enterprise Log Manager では、CA 製品、一般的なファイアウォール、データベース、オペレーティング システム、アプリケーションなど、一般的に普及しているイベント ソース用のさまざまな統合を提供しています。次の方法を使用すると追加の統合を入手できます。

- 新しい統合または既存の統合の新しいバージョンを含む、サブスクリプションの更新
- 提供されたウィザードを使用した、カスタム統合の作成

コネクタを設定する場合に、統合を使用して実行するイベント収集の種類を指定します。

コネクタについて

コネクタはイベントを待ち受け、CA Enterprise Log Manager サーバに転送するためにステータス イベントを定期的にエージェントに送信します。コネクタとは、ログ センサと統合を使用して、特定のイベント ソースからイベントを収集するための設定を作成するプロセスです。コネクタは統合を設定テンプレートとして使用します（syslog を除く）。Syslog コネクタはリスナをベースにしています。

エージェントはコネクタを使用してイベントを収集します。エージェントをインストールしたら、任意の CA Enterprise Log Manager サーバのエージェント エクスプローラを使用して、そのエージェントに 1 つ以上のコネクタを設定できます（この方法でエージェントを設定するには、CA Enterprise Log Manager サーバを同じ管理サーバ（あるいは外部の CA EEM サーバ）に同じアプリケーション インスタンス名で登録する必要があります）。

注: 理論上は指定のエージェントに最大で 256 までのコネクタを設定できますが、コネクタ数が多いとパフォーマンスは低下します。パフォーマンスを最適化するには、1 つのエージェントに設定するコネクタ数は 70 までに制限することをお勧めします。

通常は、ネットワーク内のイベント ソースごとに 1 つのコネクタを使用します。syslog イベントの場合、設定の選択によっては、多くのイベント ソースに対して 1 つのコネクタを使用する場合があります。同じ統合を使用して複数のコネクタを作成できます。一方で、別のイベント ソースにアクセスするために少し異なる詳細設定を持つ複数のコネクタを作成することもできます。一部のコネクタでは、イベント ソースへのアクセスに必要な情報を収集する設定ツールを提供しています。現在統合が提供されていないコネクタが必要になった場合は、統合ウィザードを使用して統合を作成できます。

ログ センサについて

ログ センサは、イベント ソースにアクセスする方法を解釈するコネクタ内のコンポーネントです。CA Enterprise Log Manager は次のようなさまざまなタイプのイベント ソースとログ形式用のログ センサを提供しています。

ACLogsensor

このログ センサは、CA Access Control がイベントのルーティングのために selogrd を使用する際、CA Access Control イベントを読み取ります。

FileLogSensor

このログ センサは、ファイルからイベントを読み取ります。

LocalSyslog

このログ センサは任意の UNIX サーバのローカル syslog ファイルからイベントを収集します。

ODBCLogSensor

このログ センサは、ODBC を使用してデータベース イベント ソースに接続し、そのデータベース イベント ソースからイベントを取得します。

OPSECLogSensor

このログ センサは、Check Point OPSEC イベント ソースからのイベントを読み取ります。

SDEELogSensor

このログ センサは、Cisco デバイスからイベントを読み取ります。

syslog

このログ センサは syslog イベントを待ち受けます。

TIBCOLogSensor

このログ センサは、CA Access Control 実装環境で、TIBCO Event Message Service（EMS）のキューからイベントを読み取ります。

W3CLogSensor

このログ センサは、W3C のログ形式のファイルからイベントを読み取ります。

WinRMLinuxLogSensor

このログ センサを使用すると、CA Enterprise Log Manager サーバ上のデフォルト（Linux）エージェントが Windows イベントを収集できます。

WMILogSensor

このログ センサは、Windows Management Instrumentation（WMI）を使用して、Windows イベント ソースからイベントを収集します。

その他のログ センサは、サブスクリプションの更新によって使用可能になる場合があります。ログ センサの設定の詳細については、オンライン ヘルプおよび「管理ガイド」で説明しています。

CA Enterprise Log Manager のネットワークのサイズ決定

必要なエージェント数を計画する場合、次のような簡単な方法で数を決定できます。最初に、必要なコネクタ数を決定します。すべてのイベント ソースにエージェントをインストールする必要はありません。ただし、syslog 以外のイベント ソースで、イベントを収集する予定のものは、それぞれにコネクタを 1 つ設定する必要があります（イベント ソースごとにログ センサを追加すると、単一のコネクタ上の複数のイベント ソースから WMI イベントを収集することができます。コネクタをこのように設定する場合は、必ずイベントの総ボリュームを考慮します）。

syslog コネクタはさまざまな方法で設定できます。たとえば、1 つの syslog コネクタを設定して、タイプにかかわらずすべての syslog イベントを受信できます。ただし、syslog コネクタは、特定の syslog イベント ソースからのイベント ボリュームに基づかせることをお勧めします。

エージェントは個々のイベント ソースにインストールできます。この方法は、そのソースからのイベント数が多い場合に推奨します。計画の際は、イベント ソース上にあるエージェントと、別の種類のイベントのコレクタとして動作する、ホスト上のエージェントを区別する必要があります。

抑制ルールによる影響

抑制ルールを使用すると、イベント ログ ストアへのイベントの挿入や、コネクタによるイベントの収集が抑制されるため、抑制ルールの計画中には、その影響を考慮する必要があります。抑制ルールは、常にコネクタに添付されます。エージェントまたはグループ レベルで、あるいは CA Enterprise Log Manager サーバ自体に抑制ルールを適用できます。配置した場所にはさまざまな影響があります。

- エージェント レベルまたはグループ レベルで抑制ルールが適用されると、イベントの収集が抑制され、CA Enterprise Log Manager サーバに送信されるネットワーク トラフィックの量が削減されます。
- CA Enterprise Log Manager サーバに抑制ルールが適用されると、データベースへのイベントの挿入が抑制され、保存される情報の量が削減されます。

特に、複数の抑制ルールを作成する場合や、イベントの発生量が多い場合、イベントが CA Enterprise Log Manager サーバに到達した後でイベントに抑制ルールを適用する際に起こりうる、パフォーマンスに関する注意事項があります。

たとえば、ファイアウォールからのイベントや、同じアクションに重複したイベントを作成する一部の Windows サーバからのイベントには、抑制が必要となる場合があります。これらのイベントを収集しなければ、保存が必要なイベント ログの送信処理を速めることができ、CA Enterprise Log Manager サーバの処理時間を短縮できます。このような場合には、エージェント コンポーネントに 1 つ以上の適切な抑制ルールを適用します。

複数のプラットフォーム、または環境全体で発生する特定のタイプのイベントをすべて抑制する必要がある場合は、CA Enterprise Log Manager サーバに 1 つ以上の適切な抑制ルールを適用します。イベントが CA Enterprise Log Manager サーバに到達すると、抑制に関連するイベント評価が行われます。サーバに多数の抑制ルールを適用すると、サーバはイベント ログ ストアへのイベント挿入に加えて、抑制ルールの適用を実行する必要が生じるため、パフォーマンスが低下する恐れがあります。

小規模な環境では、CA Enterprise Log Manager サーバで抑制を実行できます。また、集約（集合）が使用されている導入環境でも、サーバへの抑制の適用を選択できます。大量のイベント情報を生成するイベント ソースから少数のイベントのみを挿入する場合には、エージェント レベルまたはエージェント グループ レベルで不要なイベントを抑制するよう選択すれば、CA Enterprise Log Manager サーバ上の処理時間を短縮できます。

第 3 章: CA Enterprise Log Manager のインストール

このセクションには、以下のトピックが含まれています。

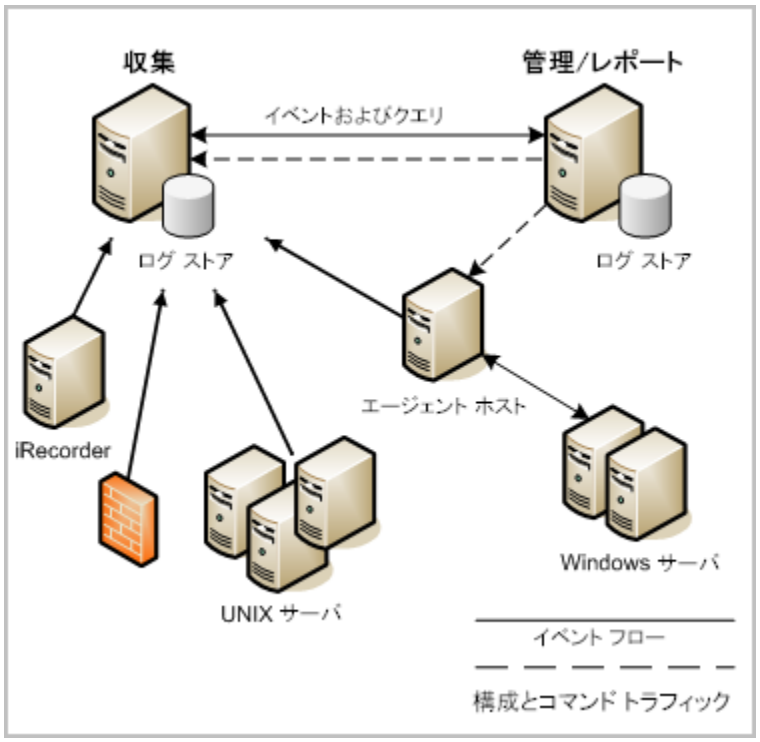
CA Enterprise Log Manager の環境について

CA Enterprise Log Manager は、インストールの開始から製品がログ情報を収集してレポートを生成するまで、短時間で起動し実行できるように設計されています。CA Enterprise Log Manager ソフトウェア アプライアンスは、専用のシステムにインストールする必要があります。

重要: CA Enterprise Log Manager サーバは高性能のイベント ログ収集専用であるため、ホストするサーバに他のアプリケーションをインストールしないでください。他のアプリケーションをインストールすると、パフォーマンスが低下することがあります。

環境を設定するにはさまざまな方法があります。エンタープライズ環境で大量のイベント処理できるようにするには、次のような特定の設定を行うことをお勧めします。

基本的なエンタープライズレベル（稼働環境）では、既存のネットワークに少なくとも 2 つの CA Enterprise Log Manager サーバをインストールします。CA Enterprise Log Manager サーバはネットワーク内の既存 DNS サーバを使用して指定されたイベント ソースとエージェント ホストと連携します。1 つのサーバは収集を重点的に行い、もう一方のサーバは収集されたイベント ログのレポート作成を集中的に行います。 2 台のサーバ環境では、最初にインストールした管理サーバがレポート サーバの役割を担います。 このサーバは管理サーバとしてユーザ認証や許可、およびその他の管理機能を実行します。次の図に、いくつかのイベント ソースを持つ基本的な環境を表示します。



この図にある実線は、イベント ソースから収集サーバ、またはエージェント ホストへ、そしてその後には収集サーバに向かうイベント フローを表しています。収集用 CA Enterprise Log Manager サーバのデフォルト エージェントを使用して、syslog イベントを直接収集できます。また、別のエージェント ホストに 1 つ以上のコネクタを設定して、複数の syslog ソースから収集することもできます（この図では示されていません）。

Windows のイベント収集では、Windows Management Instrumentation（WMI）を使用して、そのイベントの Windows サーバを監視します。これには、Windows ホストにインストールされたエージェントに、イベント収集ポイントとしての WMI コネクタを設定する必要があります。 その他のイベント タイプの中には、ホスト サーバのスタンド アロンの CA iRecorder を使用する場合もあります。

ネットワークの任意の CA Enterprise Log Manager サーバからのイベント ソース用に、エージェントとコネクタを設定して管理できます。図内の点線は、管理サーバとエージェント、および他の CA Enterprise Log Manager サーバ間の設定および制御トラフィックを表します。この図に示した環境では、管理サーバから設定を実行します。これによって収集サーバはイベントの処理に集中することができます。

CA Enterprise Log Manager サーバをインストールするログ収集環境には次のような特徴があります。

- 管理用 CA Enterprise Log Manager サーバは、ユーザ認証と許可の処理に加えて、ネットワーク内でローカルの CA EEM サーバを使用しているすべての CA Enterprise Log Manager サーバ、エージェント、およびコネクタの設定を管理します。

  ネットワークのサイズとイベント ボリュームによっては、複数の管理サーバをインストールし、それぞれの管理サーバの下で収集サーバの連携を構築する場合もあります。あるいは、複数のサーバをレポート専用にして、すべてのレポート サーバを 1 つの管理サーバに登録することもできます。 このシナリオのイベント フローでは、イベント ソースから設定済みの収集サーバまで通過し、さらに設定済みのレポート サーバまで通過します。

- 1 つ以上の収集用 CA Enterprise Log Manager サーバでは、受信イベントを処理して保存します。
- 対応するコネクタまたはアダプタを設定した後は、イベントはさまざまなイベント ソースからログ収集ネットワークを通って流れます。

インストール DVD の作成

CA Enterprise Log Manager ソフトウェアは、ダウンロード可能で圧縮された ISO イメージとして使用できます。ソフトウェアをダウンロードしたら、インストールできるようにする前に DVD メディアを作成する必要があります。ISO イメージをダウンロードしてインストール ディスクを作成するには、以下の手順に従います。

インストール DVD を作成する方法

1. インターネットに接続されたコンピュータから、ダウンロード サーバ (http://www.ca.com/jp/support/t) にアクセスします。
2. [CA サポート]リンクをクリックし、次に[ダウンロード]リンクをクリックします。
3. [製品の選択]フィールドで CA Enterprise Log Manager を選択し、[リリースの選択]フィールドでリリースを選択します。

4. ［Select all components］チェック ボックスをオンにして、［Go］をクリックします。

   ［Published Solutions Downloads］ページが表示されます。

5. ダウンロードするパッケージを選択します。

   ソリューションのドキュメント ページが表示されます。

6. ページの下までスクロールし、パッケージ名前の反対側にある［Download］リンクを選択します。

   パッケージのダウンロードが開始されます。

   注: 接続のスピードによっては、ダウンロードが完了するまでにある程度の時間がかかる場合があります。

7. 2 つのインストール イメージを解凍します。

8. オペレーティング システムと CA Enterprise Log Manager の ISO ディスク イメージを別の DVD-RW メディアに書き込むことにより、2 つの個別のインストール ディスクを作成します。

   2 つのインストール ディスクには、それぞれ、CA Enterprise Log Manager 環境用のオペレーティング システムと製品コンポーネントがすべて含まれます。その環境で SAPI レコーダまたは iRecorder などの他のコンポーネントを使用することもできます。これらのコンポーネントは CA のサポート Web サイトから入手可能で、個別にダウンロードします。

9. インストールには新しく作成したインストール ディスクを使用します。

CA Enterprise Log Manager サーバのインストール

インストール プロセスには、以下の手順が含まれます。

- CA Enterprise Log Manager サーバのワークシートの記入
- CA Enterprise Log Manager 管理サーバのインストール

  注: SAN ストレージを使用する場合は、SAN ドライブにインストールされないよう、事前に注意する必要があります。

- 1 つ以上の CA Enterprise Log Manager 収集サーバのインストール
- (オプション) 1 つ以上のレポート サーバのインストール

  注: レポート専用のサーバをインストールしない場合は、レポート サーバのロールに管理サーバを使用できます。
- (オプション) 復元ポイント サーバのインストール
- インストールの確認
- 自己監視イベントの表示

重要: CA Enterprise Log Manager のインストールを開始する前に、RAID アレイのストレージ ディスクを構成してください。最初の 2 つのディスクを RAID 1 として設定し、このアレイをブート可能なアレイにします。残りのディスクは単体の RAID 5 アレイとして設定します。RAID アレイの構成に失敗すると、データの損失につながる場合があります。

CA Enterprise Log Manager サーバ自体の全体的セキュリティの一部として、インストール時に Grand Unified Boot-loader (GRUB) ユーティリティはパスワード保護されています。

CA Enterprise Log Manager サーバのワークシート

CA Enterprise Log Manager サーバをインストールする前に、次の表の情報を集めます。ワークシートを記入したら、インストール時のプロンプトに対してそのワークシートを使用できます。インストールする予定の CA Enterprise Log Manager サーバごとに、個別のワークシートを印刷して記入できます。

CA Enterprise Log Manager の情報	値	コメント
OS ディスク		
キーボードのタイプ	*適切な値*	国の言語設定ごとに使用するキーボード タイプを指定します。 デフォルト値には、サーバの起動時にサーバに接続されているキーボード用のハードウェア設定が使用されます。
タイム ゾーンの選択	*希望するタイム ゾーン*	このサーバが存在する地域のタイム ゾーンを選択します。

CA Enterprise Log Manager の情報	値	コメント
ルート パスワード	*新しい root のパスワード*	このサーバ用の新しい root のパスワードを作成し、確認します。
アプリケーション ディスク		
新しいホスト名	*この CA Enterprise Log Manager サーバのホスト名* 例: CA-ELM1	ホストでサポートされている文字のみを使用して、このサーバのホスト名を指定します。業界基準では、A ～ Z（大文字と小文字を区別しない）、0 ～ 9、およびハイフンを使用し、最初の文字には英字、最後の文字には英数字を使用することを推奨しています。ホスト名にはアンダースコア文字を使用しないでください。 **注**: ホスト名の値にはドメイン名を追加しないでください。
デバイスの選択	*device name*	イベント ログの収集および通信に使用するネットワーク アダプタの名前を選択します。 デバイスの設定を入力するには、Space キーを押します。
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	*関連する IP の値*	このサーバ用の有効な IP アドレスを入力します。 このサーバで使用する有効なサブネット マスクおよびデフォルト ゲートウェイを入力します。
ドメイン名	*ドメイン名*	mycompany.com など、このサーバが動作する完全修飾ドメイン名を入力します。 **注**: IP アドレスに対するホスト名を解決できるようにするために、ネットワーク内の Domain Name Server（DNS）サーバにドメイン名を登録する必要があります。

CA Enterprise Log Manager の情報	値	コメント
DNS サーバのリスト	*関連する IPv4 または IPv6 のアドレス*	ネットワークで使用している 1 つ以上の DNS サーバの IP アドレスを入力します。 このリストはカンマで区切り、エントリ間にスペースは挿入しません。 DNS サーバが IPv6 のアドレス割り当てを使用している場合は、その形式でアドレスを入力します。
システムの日付と時刻	*ローカルの日付と時刻*	必要に応じて、新しいシステムの日付と時間を入力します。
NTP を使用して時刻を更新するか。	はい（推奨） いいえ	設定済みの Network Time Protocol（NTP）サーバからの日付と時刻を更新するように CA Enterprise Log Manager サーバを設定するかどうか示します。 **注**: 時間を同期することにより、確実にアラートに完全なデータが含まれるようになります。
NTP のサーバ名またはアドレス	*関連するホスト名または IP アドレス*	この CA Enterprise Log Manager サーバが日付および時刻の情報を取得する NTP サーバのホスト名または有効な IP アドレスを入力します。
Sun Java JDK の EULA	はい	使用許諾契約書を読み、「使用許諾契約書の条項に同意しますか? [はい/いいえ]」という質問が表示されるまで、ページを下にスクロールします。
CA EULA	はい	使用許諾契約書を読み、「使用許諾契約書の条項に同意しますか? [はい/いいえ]」という質問が表示されるまで、ページを下にスクロールします。

CA Enterprise Log Manager の情報	値	コメント
CA Embedded Entitlements Manager サーバはローカルか、リモートか。	ローカル: 最初にインストールされたサーバ(管理サーバ)の場合 リモート: 追加サーバの場合	ローカルの CA EEM サーバを使用するのか、リモートの CA EEM サーバを使用するのかを示します。 管理用 CA Enterprise Log Manager サーバの場合は、ローカルを選択します。インストール中に、デフォルトの EiamAdmin ユーザ アカウントのパスワードを作成するように求めるプロンプトが表示されます。 個々の追加サーバについては、リモートを選択します。インストール中に、管理サーバ名を入力するように求めるプロンプトが表示されます。 ローカルを選択したかリモートを選択したかにかかわらず、最初は EiamAdmin アカウントの ID およびパスワードを使用して各 CA Enterprise Log Manager サーバにログインする必要があります。
CA EEM サーバ名の入力	*IP アドレスまたはホスト名*	このプロンプトは、ローカル サーバかリモート サーバを指定するプロンプトで、リモート サーバを選択した場合にのみ表示されます。 最初にインストールした管理用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。 ホスト名を DNS サーバに登録する必要があります。

CA Enterprise Log Manager の情報	値	コメント
CA EEM サーバの管理者のパスワード	*EiamAdmin アカウントのパスワード*	デフォルトの管理者アカウント EiamAdmin のパスワードを記録します。 CA Enterprise Log Manager サーバに初めてログインする場合には、このアカウント認証情報が必要です。 管理サーバをインストールしている場合は、ここで EiamAdmin の新しいパスワードを作成して確認します。 他の CA Enterprise Log Manager サーバやエージェントをインストールするときに再び使用するため、このパスワードを書き留めておきます。 **注**: ここで入力したパスワードは、ssh を使用して CA Enterprise Log Manager サーバに直接アクセスするために使用するデフォルトの caelmadmin アカウントの初期パスワードでもあります。 必要に応じて、インストール後に追加の管理者アカウントを作成して CA EEM の機能にアクセスできます。

CA Enterprise Log Manager の情報	値	コメント
アプリケーションのインスタンス名	CAELM	ネットワークに最初の CA Enterprise Log Manager サーバをインストールするときに、このプロンプトでアプリケーション インスタンスの値を作成します。 その後の CA Enterprise Log Manager サーバでもこの値を使用して管理サーバに登録します。 デフォルトのアプリケーション インスタンス名は CAELM です。 この値には任意の名前を使用できます。後で CA Enterprise Log Manager のインストールで使用するために、アプリケーションのインスタンス名を書き留めておきます。
CAELM サーバを FIPS モードで 実行するか。	Yes、または No	CA Enterprise Log Manager サーバが FIPS モードで開始するかどうかを決定します。 **注**: 既存の CA Enterprise Log Manager 展開にサーバを追加する場合は、CA Enterprise Log Manager 管理サーバまたはリモート CA EEM サーバも FIPS モードである必要があります。そうしないと新しいサーバは登録できないため、再インストールする必要があります。

注: インストール時に、接続を試行する前に CA EEM サーバの詳細を確認して変更する機会が与えられます。

インストール プログラムが指定した管理サーバに接続できない場合にインストールを続行すると、組み込みの CA EEM 機能を使用して CA Enterprise Log Manager サーバを手動で登録できます。このような状況が発生した場合は、コンテンツ、CEG、およびエージェント管理ファイルも手動でインポートする必要があります。詳細および手順については、インストールに関するトラブルシューティングについてのセクションを参照してください。

詳細情報:

CA Enterprise Log Manager サーバの CA EEM サーバへの登録 (P. 129)
CA EEM サーバからの証明書の取得 (P. 130)
CA Enterprise Log Manager レポートのインポート (P. 130)
CA Enterprise Log Manager データ マッピング ファイルのインポート (P. 131)
共通イベント文法ファイルのインポート (P. 132)
共通のエージェント管理ファイルのインポート (P. 133)

CA Enterprise Log Manager のインストール

CA Enterprise Log Manager サーバのインストール手順は次のとおりです。

CA Enterprise Log Manager ソフトウェアをインストールする方法

1. OS のインストール DVD を使用してサーバを起動します。

   オペレーティング システムのインストールが自動的に開始されます。

2. CA Enterprise Log Manager サーバのワークシートに書き込んだ情報を使用して、プロンプトに応答します。

   使用許諾契約に同意しない場合はインストールが停止し、サーバがシャットダウンされます。

3. まずメディアを取り出し、[再起動]をクリックして、再起動を要求するプロンプトに応答します。

4. CA Enterprise Log Manager アプリケーションのディスクを挿入するよう要求されたら、ディスクを挿入して Enter キーを押します。

5. ワークシートに書き込んだ情報を使用して、プロンプトに応答します。

   インストールが続行されます。CA Enterprise Log Manager のインストールに成功したことを示すメッセージが表示されたら、インストールは完了です。

   注: 2 台目以降の CA Enterprise Log Manager サーバをインストールすると、インストール ログに、インストール時に CA EEM サーバに登録しようとしたアプリケーション名がすでに存在することを示すエラー メッセージが記録される場合があります。これは、CA Enterprise Log Manager をインストールするたびに、毎回アプリケーション名を新規のアプリケーションとして作成しようとするために起こるエラーであり、無視しても問題はありません。

インストールが完了したら、イベントを受信できるように CA Enterprise Log Manager サーバを設定する必要があります。必要に応じ、syslog イベントを受信するデフォルト エージェントのコネクタ設定を併せて実行します。

詳細情報

インストールに関するトラブルシューティング (P. 126)
デフォルト エージェントの設定 (P. 207)

iGateway プロセスの実行確認

インストール後に CA Enterprise Log Manager サーバの Web インターフェースにアクセスできず、ネットワーク インターフェース ポートが正しく設定されていることが確認できた場合は、iGateway プロセスが実行されていない可能性があります。

次の手順を使用して、iGateway プロセスのステータスを簡単に確認できます。iGateway プロセスは、CA Enterprise Log Manager サーバがイベントを収集し、ユーザ インターフェースにアクセスできるようにするために実行する必要があります。

iGateway デーモンを確認する方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root アカウントに切り替えます。

   ```
   su - root
   ```

4. iGateway プロセスが実行中であることを確認するには、次のコマンドを使用します。

   ```
   ps -ef | grep igateway
   ```

   オペレーティング システムによって、iGateway のプロセス情報と iGateway の下で実行されているプロセスのリストが返されます。

詳細情報:

ネットワーク インターフェースの設定エラーの解決 (P. 128)

iGateway デーモンまたはサービスの開始

iGateway デーモンまたはサービスは、CA EEM と CA Enterprise Log Manager の両方のユーザ インターフェースに対するすべての呼び出しを処理するプロセスです。そのプロセスは、いずれかのアプリケーションにアクセスする際に実行されている必要があります。プロセスが実行されていない場合に iGateway プロセスを開始するには、次の手順を使用します。

注: iGateway を開始できない場合は、「/」フォルダに使用可能なディスクの空き容量があることを確認してください。ディスクの空き容量が不足すると、iGateway を開始できない場合があります。

iGateway デーモンまたはサービスを開始する方法

1. CA Enterprise Log Manager サーバの caelmadmin ユーザとしてログインします。
2. 次のコマンドを使用してユーザを root アカウントに切り替えます。

   ```
   su -
   ```

3. 次のコマンドを使用して iGateway プロセスを開始します。

   ```
   $IGW_LOC/S99igateway start
   ```

   S99igateway は iGateway プロセスのスタートアップ スクリプトで、root アカウントが所有しています。iGateway プロセスを開始する場合、このプロセスは caelmservice ユーザ アカウントで実行されます。

iGateway デーモンまたはサービスの停止

iGateway デーモンまたはサービスは、CA EEM と CA Enterprise Log Manager の両方のユーザ インターフェースに対するすべての呼び出しを処理するプロセスです。そのプロセスは、いずれかのアプリケーションにアクセスする際に実行されている必要があります。iGateway プロセスを停止するには、次の手順を使用します。この作業は、プロセスを再起動するための準備、あるいはネットワークから CA Enterprise Log Manager サーバを削除する場合に行います。

iGateway デーモンまたはサービスを停止する方法

1. CA Enterprise Log Manager サーバの caelmadmin ユーザとしてログインします。
2. 次のコマンドを使用してユーザを root アカウントに切り替えます。

   ```
   su -
   ```

3. 次のコマンドを使用して iGateway プロセスを停止します。

   ```
   $IGW_LOC/S99igateway stop
   ```

   S99igateway は iGateway プロセスのシャット ダウン スクリプトで、root アカウントが所有しています。iGateway プロセスを開始する場合、このプロセスは caelmservice ユーザ アカウントで実行されます。

CA Enterprise Log Manager エージェントのデーモンまたはサービスの開始

CA Enterprise Log Manager エージェントのデーモンまたはサービスは、収集されたイベントを CA Enterprise Log Manager サーバに送信するコネクタを管理するプロセスです。コネクタがイベントを収集できるようにするには、このプロセスが実行されている必要があります。プロセスが実行されていない場合に CA Enterprise Log Manager エージェント プロセスを開始するには、次の手順を使用します。

CA ELM エージェントのデーモンまたはサービスを開始する方法

1. root または Windows の管理者ユーザとしてログインします。
2. コマンド プロンプトにアクセスして、次のコマンドを入力します。

   Linux、UNIX、Solaris の場合: `/opt/CA/ELMAgent/bin/S99elmagent start`

   Windows の場合: `net start ca-elmagent`

CA Enterprise Log Manager エージェントのデーモンまたはサービスの停止

CA Enterprise Log Manager エージェントのデーモンまたはサービスは、収集されたイベントを CA Enterprise Log Manager サーバに送信するコネクタを管理するプロセスです。コネクタがイベントを収集できるようにするには、このプロセスが実行されている必要があります。CA Enterprise Log Manager エージェントのプロセスを停止するには、次の手順を使用します。通常、開始および停止コマンドは、任意の CA Enterprise Log Manager サーバのエージェント エクスプローラから発行します。エージェント プロセスとそのすべてのコネクタを再起動するための準備段階で、このコマンドを使用する場合があります。

CA ELM エージェントのデーモンまたはサービスを停止する方法

1. root または Windows の管理者ユーザとしてログインします。
2. コマンド プロンプトにアクセスして、次のコマンドを入力します。

   Linux、UNIX、Solaris の場合: `/opt/CA/ELMAgent/bin/S99elmagent stop`

   Windows の場合: `net stop ca-elmagent`

CA Enterprise Log Manager サーバのインストールの確認

Web ブラウザを使用して CA Enterprise Log Manager サーバのインストールを確認できます。CA Enterprise Log Manager サーバにログインすることにより、インストールの最初の確認を実行できます。

注: 初めて CA Enterprise Log Manager アプリケーションにログインする場合は、CA Enterprise Log Manager サーバをインストールしたときに使用した EiamAdmin のユーザ認証情報を使用する必要があります。このユーザ アカウントでログインすると、特定のユーザのみを表示および使用して、各種管理機能にアクセスできます。その後でユーザ ストアを設定し、CA Enterprise Log Manager の新しいユーザ アカウントを作成して、CA Enterprise Log Manager の他の機能にアクセスする必要があります。

CA Enterprise Log Manager サーバを確認する方法

1. Web ブラウザを開いて、次の URL を入力します。

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

   CA Enterprise Log Manager のログイン画面が表示されます。

2. EiamAdmin 管理者ユーザとしてログインします。

   [管理]タブの[ユーザとアクセスの管理]サブタブが表示されます。CA Enterprise Log Manager サーバにログインすることができれば、インストールが成功したとみなすことができます。

   注: イベント データを受信してレポートを表示できるようにするには、1 つ以上のイベント ソース サービスを設定する必要があります。

自己監視イベントの表示

自己監視イベントを使用して、CA Enterprise Log Manager サーバが正常にインストールされていることを確認できます。CA Enterprise Log Manager がネットワークからイベント ログ データを収集してレポートできるようにする前に実行すべき設定タスクがいくつかありますが、その間にも CA Enterprise Log Manager サーバによってすぐに生成される自己監視イベントを確認することができます。

インストールが成功したかどうかの 1 番最初の最適なテストは、CA Enterprise Log Manager サーバにログインすることです。自己監視イベントでは、別の方法で CA Enterprise Log Manager サーバのステータスをチェックします。使用可能な自己監視イベントのタイプはたくさんあります。CA Enterprise Log Manager サーバ自体によって生成されたイベントからの追加のイベント データを表示するには、以下の手順に従います。

自己監視イベントを表示する方法

1. CA Enterprise Log Manager サーバにログインします。
2. [レポート]タブにアクセスします。
3. [システム]タグをクリックしてレポートを選択し、[自己監視イベント詳細]を選択します。

   自己監視イベントのレポートがロードされます。

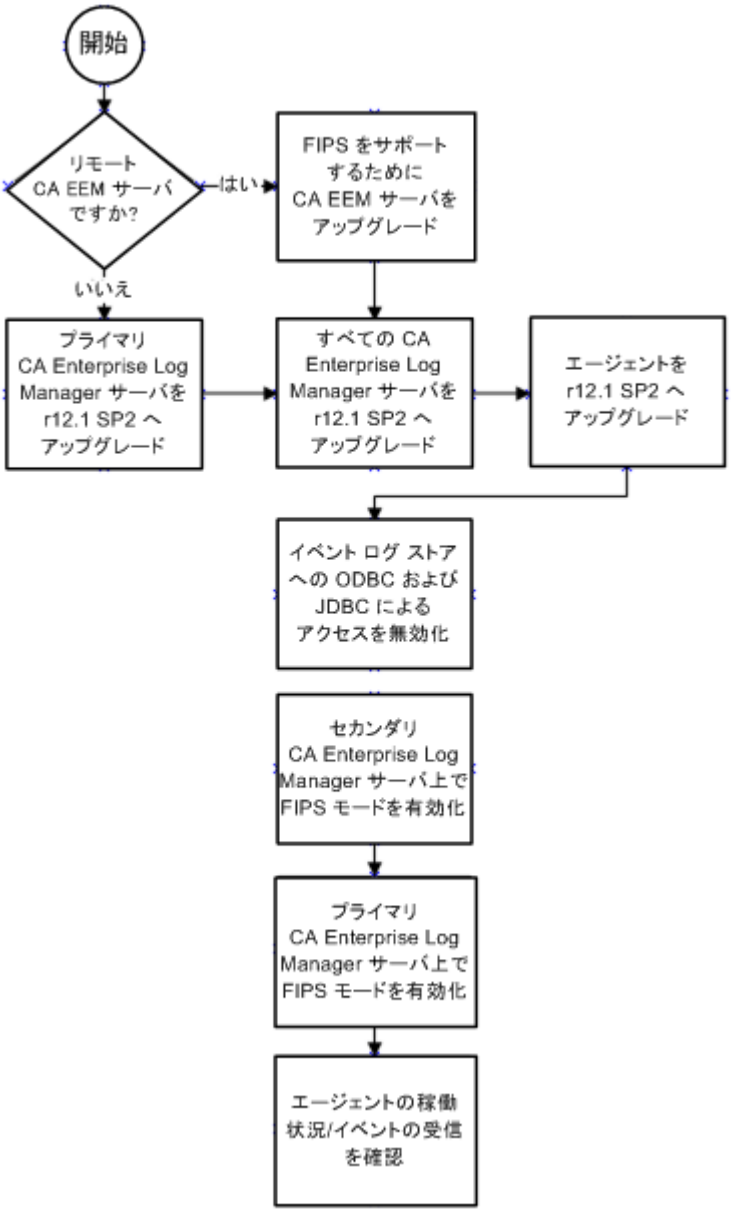
4. レポートに、ログインおよびその他の準備設定アクションの自己監視イベントがあることを確認します。

FIPS サポートのための既存の CA Enterprise Log Manager サーバおよびエージェントのアップグレード

既存の CA Enterprise Log Manager サーバおよびエージェントは、FIPS サポートのため、サブスクリプション サービスを使用してアップグレードできます。このアップグレード処理は、以下を前提としています。

- CA Enterprise Log Manager r12.1 をインストールしたか、または r12.0 SP3 からそのレベルにアップグレードした。
- CA Enterprise Log Manager 連携のために FIPS モードを有効にする必要がある。

以下のプロセスに従って、サーバをアップグレードします。



アップグレードおよび FIPS の有効化には、以下の手順が含まれます。

1. プライマリ サーバまたは管理サーバを r12.1 SP1 にアップグレードします。

   リモート CA EEM サーバを使用している場合は、FIPS をサポートするリリース レベルであることを確認します。FIPS サポートのためのアップグレードの詳細については、「CA EEM リリース ノート」を参照してください。

   サブスクリプション モジュールを使用して CA Enterprise Log Manager サーバおよびエージェントの両方をアップグレードするための手順については、「管理ガイド」のサブスクリプションのセクションを参照してください。

2. r12.1 SP1 との連携内の他のすべての CA Enterprise Log Manager サーバをアップグレードします。

3. すべてのエージェントを r12.1 SP1 にアップグレードし、必要に応じてコネクタ ログ センサを更新します。

   重要: Windows ホスト上で syslog ログ センサを使用するコネクタを展開した場合は、これらのコネクタ設定をすべて更新し、FIPS モードで実行中に本リリースの最新の syslog センサが使用されるようにする必要があります。syslog ログ センサを使用する統合の最新のリストについては、CA Enterprise Log Manager 製品統合マトリックス https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html を参照してください。

4. イベント ログ ストアに対する ODBC および JDBC アクセスを無効にします。

5. 連携内の CA Enterprise Log Manager セカンダリ サーバごとに、FIPS モードを有効にします。

   エージェントは、エージェントを管理する CA Enterprise Log Manager サーバから動作モードを自動的に検出します。

6. プライマリ サーバまたは管理サーバ上で FIPS モードを有効にします。

7. エージェント エクスプローラ ダッシュボードを使用して、エージェントが FIPS モードで実行されていることを確認します。

   エージェントがクエリまたはレポートを使用してイベントを送信していることも確認できます。または、システム ステータス サービス領域で自己監視イベント タブを確認します。

既存のエージェントを r12.1 SP1 にアップグレードする場合、サブスクリプション処理では、デフォルトでエージェントが FIPS 非準拠モードで更新されます。エージェントを管理する CA Enterprise Log Manager サーバに対しては FIPS モードを設定します。エージェントは、エージェントを管理しているサーバが FIPS モードであることを検出し、必要に応じて対応するモードで自身を再起動します。管理者ユーザ権限を持っている場合は、CA Enterprise Log Manager ユーザ インターフェースでエージェント エクスプローラ ダッシュボードを使用し、エージェントの FIPS モードを参照します。アップグレードの詳細については、「実装ガイド」の CA Enterprise Log Manager のインストールに関するセクションを参照するか、オンライン ヘルプでエージェント管理タスクに関する説明を参照してください。

詳細情報:

FIPS モードでの操作の有効化 (P. 92)
エージェント ダッシュボードの表示 (P. 94)

FIPS サポートのためのアップグレードの前提条件

以下は、FIPS 140-2 をサポートするために CA Enterprise Log Manager をアップグレードするための前提条件です。

- CA Enterprise Log Manager r12.0 SP3 または r12.1 のいずれかのインストールから開始する
- サブスクリプションを通じて CA Enterprise Log Manager r12.1 SP1 にアップグレードする

詳細情報:

既存の FIPS モード連携への新規 CA Enterprise Log Manager サーバの追加 (P. 96)

アップグレードのガイドライン

以下は、FIPS をサポートする CA Enterprise Log Manager をアップグレードするためのガイドラインです。

- 連携内に複数の CA Enterprise Log Manager サーバがある場合は、プライマリ サーバまたは CA Enterprise Log Manager 管理サーバをまず r12.1 SP1 にアップグレードします。その後は、任意の順序で他のすべてのサーバをアップグレードできます。アップグレードされたサーバは、FIPS 非準拠 ードでのみ開始されます。FIPS モードを有効にするには、管理者が動作モードを手動で設定する必要があります。

  重要: サブスクリプション処理中に CA Enterprise Log Manager セカンダリ サーバ上で FIPS モードに切り替えることはしないでください。切り替えるとサブスクリプションが失敗する可能性があります。

- CA Enterprise Log Manager r12.1 SP1 サーバは、r12.1 エージェントと通信できますが、r12.1 SP1 にアップグレードしないと、エージェント レベルで FIPS はサポートされません。

- FIPS モードを有効にした場合、r12.1 SP1 以降の FIPS 対応エージェントのみが CA Enterprise Log Manager サーバと通信できます。FIPS 非準拠モードを有効にした場合、CA Enterprise Log Manager サーバは、古いエージェントと完全に後方互換性がありますが、FIPS モードは使用できません。CA Enterprise Log Manager サーバを r12.1 SP1 にアップグレードした後は、r12.1 SP1 エージェントのみをインストールすることをお勧めします。

- CA Enterprise Log Manager サーバと関連付けられているエージェントは、サーバ モードの変更を自動的に検出し、対応するモードで自身を再起動します。

- 新しい CA Enterprise Log Manager サーバを、FIPS モードで実行されている既存の連携に追加する場合は、特別な対応が必要になります。既存の連携への新しい CA Enterprise Log Manager サーバの追加については、「実装ガイド」の該当セクションを参照してください。

リモート CA EEM サーバのアップグレード

CA Enterprise Log Manager インストールを含む CA EEM スタンドアロン サーバを使用している場合は、CA Enterprise Log Manager サーバまたはエージェントにアップグレードする前に FIPS サポートのためにアップグレードする必要があります。詳細および手順については、「CA EEM 導入ガイド」を参照してください。

イベント ログ ストアへの ODBC/JDBC アクセスの無効化

ODBC サービス環境設定ダイアログ ボックスのオプションを使用して、イベント ログ ストア内のイベントへの ODBC/JDBC アクセスを防ぐことができます。連携されたネットワークを FIPS モードで実行する場合は、連携標準との互換性を維持するために ODBC/JDBC アクセスを無効にする必要があります。

ODBC および JDBC アクセスを無効にする方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブを開きます。
2. [サービス]サブタブをクリックし、「ODBC サービス」ノードを展開します。
3. 対象のサーバを選択します。
4. [サービスを有効化]チェック ボックスをオフにして[保存]をクリックします。

   注: 連携内の CA Enterprise Log Manager サーバごとに、ODBC オプションを無効にして、ODBC/JDBC が無効になっていることを確認します。

FIPS モードでの操作の有効化

[システム ステータス]サービスの[FIPS モード]オプションを使用すると、FIPS モードのオン/オフを切り替えることができます。デフォルトの FIPS モードは FIPS 非準拠です。管理者ユーザは、連携内にある各 CA Enterprise Log Manager サーバに対して FIPS モードを設定する必要があります。

重要: 同じサーバ連携内では、混合モードで操作することはできません。連携内のあるサーバが別のモードで稼働している場合、他のサーバからのクエリやレポートのデータの収集、リクエストへの応答は実行できません。

FIPS モードと FIPS 非準拠モードを切り替える方法

1. CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックし、[サービス]サブタブをクリックします。
3. [システム ステータス]サービス ノードを展開し、必要な CA Enterprise Log Manager サーバを選択します。

   システム ステータスのサービスを設定するダイアログ ボックスが表示されます。

4. ドロップダウン リストから、必要な FIPS モードとして「オン」または「オフ」を選択します。
5. [保存]をクリックします。

   選択したモードで CA Enterprise Log Manager サーバが再起動します。再度ログインすると、エージェント エクスプローラからエージェントの FIPS モードを表示できます。
6. サーバの再起動後に[システム ステータス]サービス ダイアログ ボックスをチェックし、CA Enterprise Log Manager サーバの操作モードを確認してください。

   また、自己監視イベントを使用し、CA Enterprise Log Manager サーバが必要なモードで開始したことを確認することができます。[システム ステータス]ダイアログ ボックスの[自己監視イベント]タブで以下のイベントを探します。

   Successfully turned Server FIPS mode ON（FIPS モードが正常にオンに設定されました）
   Successfully turned Server FIPS mode OFF（FIPS モードが正常にオフに設定されました）
   Failed to turn Server FIPS mode ON（FIPS モードをオンに設定できませんでした）
   Failed to turn Server FIPS mode ON（FIPS モードをオフに設定できませんでした）

プライマリ サーバまたは管理サーバに対して FIPS モードを無効にすると、データを返す連携クエリおよびレポートがすべて停止されます。また、スケジュール済みレポートは実行されません。この状態は、連携内のすべてのサーバが再度同じモードで稼働するまで続きます。

注: 管理サーバまたはリモートの CA EEM サーバ上での FIPS の無効化は、新しい CA Enterprise Log Manager サーバを FIPS モードで稼働する連携に追加する際の要件の 1 つです。

エージェント ダッシュボードの表示

エージェント ダッシュボードを表示して、お使いの環境のエージェントのステータスを表示することができます。また、ダッシュボードには、現在の FIPS モード（FIPS または FIPS 非準拠）などの詳細情報および使用状況の詳細情報が表示されます。この詳細情報には、1 秒あたりに読み込むイベント数、CPU 使用率、最終更新日と最終更新時刻が含まれます。

エージェント ダッシュボードを表示するには、以下の手順に従います。

1. ［管理］タブをクリックし、［ログ収集］サブタブをクリックします。

   ［ログ収集］フォルダ リストが表示されます。

2. ［エージェント エクスプローラ］フォルダを選択します。

   詳細ペインにエージェント管理ボタンが表示されます。

3. [エージェント ステータス モニタ/ダッシュボード]をクリックします。 

   エージェントの検索パネルが表示され、詳細なグラフ内に利用可能なすべてのエージェントのステータスが表示されます。以下に例を示します。

   合計: 10 実行中: 8 保留: 1 停止済み: 1 応答なし: 0

4. (オプション)エージェント検索条件を選択し、表示されたエージェントのリストを絞り込みます。以下の条件を 1 つ以上選択できます。

   - エージェント グループ— 選択したグループに割り当てられたエージェントのみが返されます。
   - プラットフォーム— 選択したプラットフォーム上で実行されているエージェントのみが返されます。
   - ステータス— 「実行中」など、選択したステータスのエージェントのみが帰されます。
   - エージェント名パターン— 指定したパターンを含むエージェントのみが返されます。

5. [ステータスの表示]をクリックします。

   検索条件に一致するエージェントのリストが表示されます。表示には、以下の情報が含まれます。

   - ローカル コネクタの名前およびバージョン
   - 現在の CA Enterprise Log Manager サーバ
   - エージェントの FIPS モード(FIPS または FIPS 非準拠)
   - 最後に記録された、エージェントによって処理される 1 秒あたりのイベント数負荷
   - 最後に記録された CPU 使用率の値
   - 最後に記録されたメモリ使用率の値
   - 最新の設定更新
   - 設定の更新ステータス

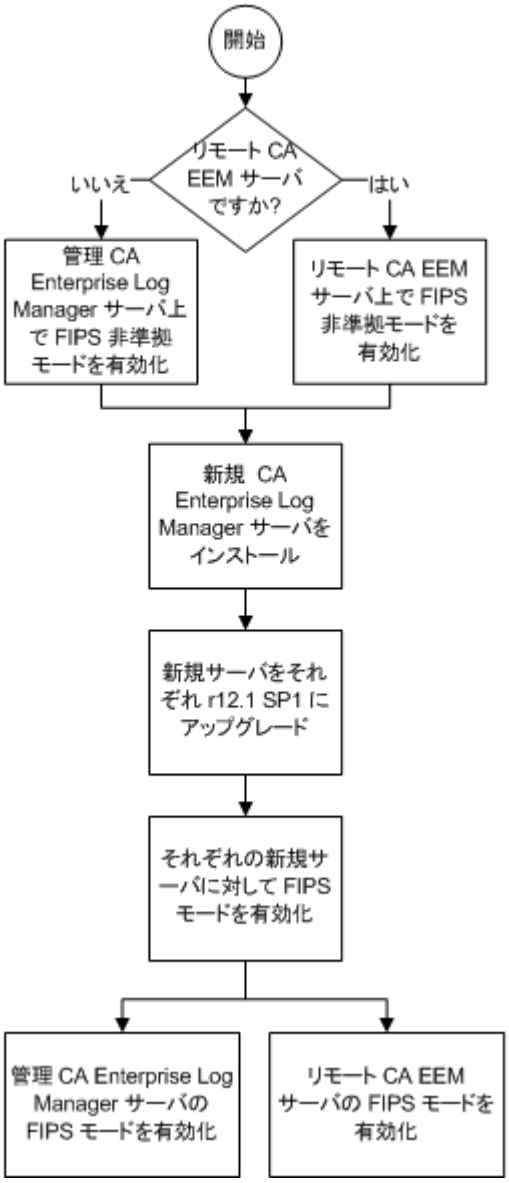
既存の FIPS モード連携への新規 CA Enterprise Log Manager サーバの追加

すでに FIPS モードで実行されているサーバの連携に対して、新しい CA Enterprise Log Manager サーバを追加するためには、いくつかの特別のガイドラインがあります。インストール中に FIPS モードを指定しない場合、新しくインストールされた CA Enterprise Log Manager サーバはデフォルトでは FIPS 非準拠モードで実行されます。FIPS 非準拠モードで実行されるサーバは、FIPS モードで実行されるサーバと通信できません。

インストールの一環として、新しい CA Enterprise Log Manager サーバは、管理サーバ上でローカルの組み込まれた CA EEM サーバに登録するか、スタンドアロンの CA EEM リモート サーバに登録する必要があります。既存のネットワークにサーバを追加す手順は、管理する CA EEM サーバの場所に基づいています。

以下のワークフローを考えてみてください。

FIPS のみのモードで実行中の連携への ELM サーバの追加



新しいサーバを追加するプロセスには、以下の手順が含まれます。

1. 管理(プライマリ) CA Enterprise Log Manager サーバ、またはリモート CA EEM サーバ上で FIPS モードが有効になっていることを確認してください。
2. CA Enterprise Log Manager12.1 SP1 以上の ISO のイメージまたは DVD を使用して、1 つ以上の新しい CA Enterprise Log Manager セカンダリ サーバをインストールします。

   重要: インストール中に FIPS モードを必ず指定してください。そうしないと、新しくインストールされたサーバは管理サーバまたはリモート CA EEM サーバと通信することができず、新しい CA Enterprise Log Manager サーバを再インストールする必要があります。

CA Enterprise Log Manager 管理サーバまたはリモート CA EEM サーバが FIPS モードで作動しているため、新しい CA Enterprise Log Manager サーバによる連携の登録および追加が可能になります。

詳細情報:

FIPS モードでの操作の有効化 (P. 92)
エージェント ダッシュボードの表示 (P. 94)

SAN ドライブを備えたシステムのインストールに関する考慮事項

SAN ドライブを備えたシステムに CA Enterprise Log Manager 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する場合、CA Enterprise Log Manager が SAN ドライブにインストールされないよう事前に注意する必要があります。そうしないと、インストールに失敗します。

以下のいずれかの方法を実行して、インストールが確実に成功するようにします。

- SAN ドライブを無効にします。オペレーティング システムおよび CA Enterprise Log Manager アプリケーションを通常の手順どおりにインストールします。その後、CA Enterprise Log Manager 用に SAN ドライブを設定し、CA Enterprise Log Manager をリサイクルして SAN ドライブ設定を有効にします。
- SAN ドライブは有効なままにします。オペレーティング システムのインストールを開始します。キックスタート ファイルに定義されているオペレーション順序を変更するために、この手順を終了します。説明されているとおり、インストールを再開して完了します。

SAN ドライブが無効な状態でのインストール

CA Enterprise Log Manager では、Dell、IBM、HP によって提供される修正されたハードウェア設定の使用が現在サポートされています。以下の例では、HP Blade サーバから構成されるハードウェアが QLogic ファイバ チャネル カードを使用して、SAN（Storage Area Network）のデータ ストレージに接続すると仮定します。HP Blade サーバには、RAID-1（ミラーリング）が設定された SATA ハード ドライブが付いています。

キックスタート ブート ファイルをそのまま使用する場合は、インストールを開始する前に必ず SAN ドライブを無効にしてください。OS5 DVD でインストール処理を開始し、ドキュメントの説明どおりにインストールを完了します。

注: SAN ドライブを無効にした状態でインストールを開始しなかった場合、CA Enterprise Log Manager は SAN にインストールされます。その場合、CA Enterprise Log Manager が再起動した後、赤い画面で Illegal Opcode というメッセージが表示されます。

以下の手順に従って、SAN ドライブを備えたシステムに CA Enterprise Log Manager アプライアンスをインストールします。その際、オペレーティング システムをインストールする前に SAN ドライブを無効にします。

1. SAN ドライブを無効にします。
2. アプライアンスにオペレーティング システムをインストールします。
3. CA Enterprise Log Manager サーバをインストールします。
4. SAN ストレージ用にマルチパスを設定します。
5. 論理ボリュームを作成します。
6. CA Enterprise Log Manager 用に論理ボリュームを準備します。
7. CA Enterprise Log Manager をリサイクルします。
8. インストールが成功したことを確認します。

SAN ドライブが無効な状態でオペレーティング システムをインストールする場合は、以下のファイルを使用します。

lvm.conf

Linux Logical Volume Manager（LVM2）用の環境設定ファイル

multipath.conf（/etc/multipath.conf）

Linux マルチパス用の環境設定ファイル。

fstab（/etc/fstab）

Linux システム内のディレクトリにデバイスをマップするファイル システム テーブル ファイル。

SAN ドライブの無効化

お使いの SAN ドライブ ベンダーによって推奨される手順を使用して、ソフト アプライアンスをインストールする予定のハードウェア上で SAN ドライブを無効にします。

ソフト アプライアンスのオペレーティング システムまたは CA Enterprise Log Manager アプリケーションをインストールする前に SAN ドライブを無効にする必要があります。

SAN ストレージ用のマルチパスの設定

SAN ストレージを使用する RAID システムにインストールされた CA Enterprise Log Manager システムには、マルチパスの設定が必要になります。SAN 上の物理ディスクは論理装置番号（LUN）という名前の論理的なパーティションに分割されます。

SAN ストレージ用のマルチパスの設定

1. CA Enterprise Log Manager アプライアンスにログオンし、su によって root になります。
2. （オプション）/dev/mapper のディレクトリ リスティングを実行し、マルチパスおよび論理ボリュームを設定する前に設定の状態を確認します。結果は以下のようになります。

```
drwxr-xr-x  2 root root     120 Jun 18 12:09 .
drwxr-xr-x 11 root root    3540 Jun 18 16:09 ..
crw-------  1 root root  10, 63 Jun 18 12:09 control
brw-rw----  1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw----  1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw----  1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. .../etc/multipath.conf ファイルを編集できる形で開き、以下の手順を実行します。

   a. SAN 管理者によって提供される各 LUN の "device {" の下に以下のセクションを追加します。

```
device {
    vendor                "NETAPP"
    product               "LUN"
    path_grouping_policy  multibus
    features              "1 queue_if_no_path"
    path_checker          readsector0
    path_selector         "round-robin 0"
    failback              immediate
    no_path_retry         queue
         }
```

   b. すべてのデバイスについて 'blacklist' のコメントを解除します。blacklist セクションは、デフォルト デバイスでマルチパスを有効にします。

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

   c. multipath.conf ファイルを保存して閉じます。

4. 以下を実行し、マルチパスが有効で、LUN がリストされることを確認します。

```
multipath -l
```

   注: パスは 'mpath0' および 'mpath1' として表示されます。LUN が表示されない場合は、再起動して multipath を再度実行してください。

5. 使用可能なドライブを表示します。

```
fdisk -l
```

6. 使用可能なパーティションをリスト表示し、'mpath0' および 'mpath1' が表示されることを確認します。

```
ls -la /dev/mapper
```

7. 最初のパーティションを以下のようにマップします。

```
kpartx -a /dev/mapper/mpath0
```

8. 2 つ目のパーティションを以下のようにマップします。

```
kpartx -a /dev/mapper/mpath1
```

論理ボリュームの作成

ボリューム マネージャ ソフトウェアを使用して、複数の LUN を CA Enterprise Log Manager がアクセスできる論理ボリュームに結合します。論理ボリューム マネージャ（LVM）は、Linux オペレーティング システム上でディスク ドライブおよび同様の大容量ストレージ デバイスを管理します。LVM の下で作られたストレージ カラムは、SAN ストレージのようなバックエンド デバイスに移動するかサイズを調整することができます。

論理ボリュームを作成する方法

1. 最初の物理ボリュームを作成します。

   ```
   pvcreate /dev/mapper/mpath0
   ```

2. 2 つ目の物理ボリュームを作成します。

   ```
   pvcreate /dev/mapper/mpath1
   ```

3. システム上のすべての物理ボリュームを表示します。

   ```
   pvdisplay
   ```

4. VolGroup01 ボリューム グループを作成します。（VolGroup00 ボリューム グループは存在します。）

   ```
   vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
   ```

   注: このコマンドは、ボリュームを作成し、2 つの物理ボリュームをグループに含めます。

5. ボリューム グループ内に論理ボリュームを作成します。

   ```
   lvcreate –n LogVol00 –l 384030 VolGroup01
   ```

6. ファイル システムを作成します。

   ```
   mkfs –t ext3 /dev/VolGroup01/LogVol00
   ```

CA Enterprise Log Manager 用の論理ボリュームの準備

論理ボリュームを作成したら、適切なディレクトリ構造を読み込み、CA Enterprise Log Manager によって必要となる所有権とグループの関連付けを割り当てます。vi を使用して fstab ファイルを変更し、作成した論理ボリュームを参照するようにします。次に、新しいデータ ディレクトリをマウントします。

CA Enterprise Log Manager 用の論理ボリュームを準備する方法

1. 一時ディレクトリ(/data1)を作成し、/data1 ディレクトリの所有権を caelmservice に変更し、このディレクトリに関連付けられているグループを caelmservice に変更します。

   ```
   mkdir /data1
   chown caelmservice /data1
   chgrp caelmservice /data1
   ```

2. CA Enterprise Log Manager サーバ iGateway プロセスを停止します。

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   ```

3. CA Enterprise Log Manager エージェントが実行されているディレクトリに移動してエージェントを停止し、すべてのサービスが停止されていることを確認します。

   ```
   cd /opt/CA/ELMAgent/bin/
   ./caelmagent –s
   ps –ef | grep /opt/CA
   ```

4. / ディレクトリに移動します。

5. 新しいファイル システムを /data1 にマウントし、/data ディレクトリのコンテンツを /data1 ディレクトリにコピーします。2 つのディレクトリの中身が同じであることを確認します。

   ```
   mount –t ext3 /dev/VolGroup01/LogVol00 /data1
   cp –pR /data/* /data1
   diff –qr /data /data1
   ```

6. 既存のデータ マウント ポイントをマウント解除し、data1 マウント ポイントをマウント解除します。

   ```
   umount /data
   umount /data1
   ```

7. /data ディレクトリを削除し、/data1 ディレクトリの名前を /data に変更します。

   ```
   rm –rf /data
   mv /data1 data
   ```

8. /data ディレクトリを参照する /etc/fstab 内の行を変更し、新しい論理ボリュームを参照するようにします。つまり、/dev/VolGroup00/LogVol02 を /dev/VolGroup01/LogVol00 に変更します。変更されたデータは、サンプル fstab ファイルの内容を表す以下で、太字のスタイルで示されています。

device name	mount point	fs-type	options	dump-freq pass-num
none	/dev/VolGroup00/LogVol00/	ext3	defaults	1 1
none	**/dev/VolGroup01/LogVol00/data**	ext3	defaults	1 2
LABEL=/boot	/boot	ext3	defaults	1 2
tmpfs	/dev/shm	tmpfs	defaults	0 0
devpts	/dev/pts	devpts	gid=5,mode=620	0 0
sysfs	/sys	sysfs	defaults	0 0
proc	/proc	proc	defaults	0 0
none	/dev/VolGroup00/LogVol01	swap	defaults	0 0

9. 新しいデータ ディレクトリをマウントし、/etc/fstab 内のすべてのパーティションがマウントされたことを確認します。

```
mount -a
mount
```

CA Enterprise Log Manager サーバのリサイクル

論理ボリュームを作成したら、論理ボリュームを使用できるように CA Enterprise Log Manager をリサイクルします。成功を確認するには、CA Enterprise Log Manager にアクセスし、「システム全イベント詳細」クエリによって返されたイベントを参照します。

CA Enterprise Log Manager サーバをリサイクルする方法

1. CA Enterprise Log Manager サーバ iGateway プロセスを開始します。

```
/opt/CA/SharedComponents/iTechnology/S99igateway start
```

2. ELMAgent サービスを開始します。

```
/opt/CA/ELMAgent/bin/caelmagent –b
```

3. CA Enterprise Log Manager サーバを再起動します。

SAN ドライブが有効な状態でのインストール

「CA Enterprise Log Manager 用の SAN ストレージの設定」などのトピックには、CA Enterprise Log Manager アプライアンスにオペレーティング システムをインストールする前に SAN ドライブ（LUN）を無効にするための推奨手順が含まれています。

それ以外の方法としては、SAN ドライブを有効にしたままで、オペレーティング システムのインストールを開始した後にキックスタート ファイル ca-elm-ks.cfg を ISO 編集ツールで変更する方法があります。この変更により、インストールおよび起動が SAN ではなくローカルのハードディスクから実行されるようにすることができます。

SAN ではなくローカル ディスクから起動する方法

1. OS のインストール DVD を使用してサーバを起動します。
2. キーボード タイプに関する最初のプロンプトに応答します。
3. Alt+F2 キーを押して、Anaconda/Kickstart プロンプトを表示します。
4. 次のように入力します。

   ```
   list-hardrives
   ```

   使用可能なドライブのリストが表示されます。以下のようなリストになります。

   ```
   cciss/c0d0 – 68GB RAID 1 (cciss is HP Smart Array)
   Sda – 500GB SAN  (sda – h is the SAN Multipathed)
   Sdb – 500GB SAN
   Sdc – 500GB SAN
   Sdd – 500GB SAN
   Sde – 500GB SAN
   Sdf – 500GB SAN
   Sdg – 500GB SAN
   Sdh – 500GB SAN
   ```

5. ローカル ハードドライブを特定します。この場合は cciss/c0d0 です。

6. 以下の手順を実行します。
   a. CA Enterprise Log Manager オペレーティング システム キックスタート ファイル ca-elm-ks.cfg を編集できる形で開きます。ISO エディタを使用します。
   b. 以下の行を確認します。

      ```
      bootloader --location=mbr --driveorder=sda,sdb
      ```

      以下のように変更します。

      ```
      bootloader --location=mbr --driveorder=cciss/c0d0
      ```

      この変更により、ローカル ディスクからのみ起動するように指定されます。
   c. 以下の行を確認します。

      ```
      clearpart --all --initlabel
      part /boot --fstype "ext3" --size=100
      part pv.4 --size=0 –grow
      ```

      以下のように変更します。

      ```
      part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0
      part pv.4 --size=0 --grow --ondisk cciss/c0d0
      ```

      パーティション定義行をこのように変更することにより、パーティションが名前によって cciss/c0d0 ディスク上に作成されるようになります --ondisk を使用して、既存の $disk1 および $disk2 変数を置き換えます。
   d. 必要に応じて、ディスクドライブの数に関する IF/When 句を削除し、ディスク コマンドの最初のセットだけを保持します（行 57 - 65）。
   e. 新しい ISO イメージを保存します。
7. Anaconda プロンプトを終了し、オペレーティング システムのインストール プロンプトに戻ります。
8. ドキュメントに説明されている手順どおりにインストールを続行します。

CA Enterprise Log Manager サーバの初期設定

CA Enterprise Log Manager サーバの初期インストールでは、デフォルト値の CAELM というアプリケーション名が作成されます。この名前は、インストール時に組み込みの CA EEM サーバに登録されます。後続のインストールで同じアプリケーション インスタンス名を使用すると、管理用 CA Enterprise Log Manager サーバはすべての設定を同じアプリケーション インスタンス名の下で管理します。

インストールが完了すると、サーバにはオペレーティング システムと CA Enterprise Log Manager サーバの両方が存在します。32 ビットのオペレーティング システムは、32 ビットと 64 ビットの両方のハードウェアをサポートします。初期設定には次の領域が含まれます。

- デフォルトのユーザ アカウント
- デフォルトのディレクトリ構造
- カスタマイズされたオペレーティング システム イメージ
- デフォルトのポート割り当て

デフォルトのユーザ アカウント

CA Enterprise Log Manager のインストールでは、独自のパスワードを持つデフォルトの管理者ユーザ caelmadmin が作成されます。ホスト サーバに直接アクセスする必要がある場合、インストール後は root アカウントのログイン機能が制限されるため、このアカウントを使用してログインする必要があります。caelmadmin アカウントはログイン アクションのみを許可されています。ログインしてから、別のパスワードを使用してユーザを root アカウントに切り替え、OS レベルのシステム管理用ユーティリティにアクセスする必要があります。

このアカウントのデフォルトのパスワードは、EiamAdmin アカウント用に作成したものと同じパスワードです。インストール後すぐに caelmadmin アカウントのパスワードを変更することをお勧めします。

また、インストールを実行すると、デフォルトのサービス ユーザ アカウントの caelmservice が作成されます。このユーザを使用してシステムにログインすることはできません。必要に応じてユーザをこのユーザに切り替えて、プロセスを起動または停止することができます。iGateway プロセスと組み込みの CA EEM サーバ（CA Enterprise Log Manager サーバにインストールされている場合）は、このユーザ アカウントで実行され、セキュリティの追加のレイヤを提供します。

iGateway プロセスは root ユーザ アカウントでは実行されません。ポートの転送は自動的に有効になり、ポート 80 および 443 の HTTPS 要求がポート 5250 と CA Enterprise Log Manager ユーザ インターフェースにアクセスできるようになります。

デフォルトのディレクトリ構造

CA Enterprise Log Manager のインストールでは、ソフトウェアのバイナリをディレクトリ構造 /opt/CA の下に配置します。システムに 2 つ目のディスクドライブがある場合は、/data として設定されます。インストール時に /opt/CA/LogManager/data ディレクトリから /data ディレクトリへのシンボリック リンクが作成されます。次の表に、デフォルトのインストール ディレクトリ構造を示します。

ファイル タイプ	ディレクトリ
iTechnology 関連のファイル（iGateway）	/opt/CA/SharedComponents/iTechnology
CA Enterprise Log Manager EEM サーバ関連のファイル	/opt/CA/LogManager/EEM
CA Enterprise Log Manager のインストール関連のファイル	/opt/CA/LogManager/install
データ ファイル（複数ドライブの場合は /data にリンク）	/opt/CA/LogManager/data
ログ ファイル	/opt/CA/SharedComponents/iTechnology

アーカイブ ファイルをバックアップまたは長期保管するために移動するか、ディスクドライブを追加する場合を除き、通常の状況下では、CA Enterprise Log Manager サーバの *ssh* ユーティリティにアクセスする必要はありません。

カスタマイズされたオペレーティング システム イメージ

最小のイメージを作成し、チャネルをできるだけ少なくしてアクセスを制限することにより、インストール プロセスでオペレーティング システムをカスタマイズします。必要でないサービスはインストールされません。CA Enterprise Log Manager サーバはごく少数の待ち受けポートを使用し、未使用のポートは個別にオフにされます。

オペレーティング システムのインストール中に、root アカウントのパスワードを作成します。CA Enterprise Log Manager のインストールが完了したら、root はその後のログインで使用できないように制限されます。CA Enterprise Log Manager をインストールするとデフォルト ユーザ *caelmadmin* が作成されます。このユーザにはログインだけが許可され、他のアクセス権は与えられていません。

CA Enterprise Log Manager サーバに root レベルでアクセスする場合は、このアカウントを使用してサーバにアクセスし、管理ツールを使用する場合にはユーザを root アカウントに切り替えます。つまり、root ユーザとしてシステムにアクセスするには、*caelmadmin* と *root* の両方のパスワードを知っている必要があります。

CA Enterprise Log Manager には他の特定のセキュリティ関連のソフトウェアはインストールされません。最高のパフォーマンスを維持するには、CA Enterprise Log Manager サーバに他のアプリケーションをインストールしないでください。

デフォルトのポート割り当て

CA Enterprise Log Manager サーバは、デフォルトでポート 5250 を待ち受け、HTTPS プロトコルを使用する場合は、ポート 80 および 443 を待ち受けるように設定されています。CA Enterprise Log Manager のプロセスおよびデーモンは root アカウントでは実行されません。そのため、ポート 1024 より小さい番号のポートを開くことはできません。その結果、ポート 80 および 443 に対するユーザ インターフェース要求を受信するために、インストール時に iptable を使用してポート 5250 へのリダイレクトが自動的に作成されます。

CA Enterprise Log Manager はシステム ステータスを追跡する際に自己監視イベントを使用するため、CA Enterprise Log Manager サーバのローカル オペレーティング システムの syslog デーモンは設定されません。自己監視イベントを使用して、他のローカル イベントや、ローカルの CA Enterprise Log Manager サーバで実行されたアクションに関するレポートを表示できます。

CA Enterprise Log Manager 環境で使用されるポートのリストを以下に示します。

ポート	コンポーネント	説明
53	CA Enterprise Log Manager サーバ	サーバのホスト名を IP アドレスに解決するための DNS 通信に使用する必要がある TCP/UDP ポート。サーバには、たとえば、CA Enterprise Log Manager サーバ、リモート CA EEM サーバ（設定されている場合）、NTP サーバ（インストール時に NTP 時間同期を選択した場合）などがあります。ローカルの /etc/hosts ファイルにホスト名から IP アドレスへのマッピングを指定している場合、DNS 通信は不要です。
80	CA Enterprise Log Manager サーバ	HTTPS を介した CA Enterprise Log Manager サーバのユーザ インターフェースとの TCP 通信。自動的にポート 5250 にリダイレクトされる。
111	ポートマップ機能（SAPI）	監査クライアントとポートマップ機能のプロセスとの通信。動的なポート割り当てを受信する。
443	CA Enterprise Log Manager サーバ	HTTPS を介した CA Enterprise Log Manager サーバのユーザ インターフェースとの TCP 通信。自動的にポート 5250 にリダイレクトされる。
514	syslog	デフォルトの UDP syslog 待ち受けポート。このポート値は設定可能です。 デフォルト エージェントを root 以外のユーザとして実行するために、デフォルト ポートを 40514 に設定します。また、インストールの際、CA Enterprise Log Manager サーバにファイアウォール ルールを適用します。
1468	syslog	デフォルトの TCP syslog 待ち受けポート。このポート値は設定可能です。
2123	DXadmin	CA の LDAP ディレクトリの DXadmin 用ポート（CA Enterprise Log Manager サーバ（管理サーバ）と同じ物理サーバ上で CA EEM サーバを使用している場合）

ポート	コンポーネント	説明
5250	CA Enterprise Log Manager サーバ	iGateway を使用している CA Enterprise Log Manager サーバのユーザ インターフェースとの TCP 通信 以下の TCP 通信が含まれます。 ■ CA Enterprise Log Manager サーバと CA EEM サーバ間 ■ 連携された CA Enterprise Log Manager サーバ間 ■ エージェントと CA Enterprise Log Manager サーバ間（ステータス更新用）
6789	Agent	エージェントのコマンドと管理用の待ち受けポート **注**: 送信トラフィックを許可しない場合は、操作を適切に実行できるように、このポートをオープンにする必要があります。
17001	Agent	CA Enterprise Log Manager サーバに通信する安全なエージェント。このポート値は設定可能です。 **注**: 送信トラフィックを許可しない場合は、操作を適切に実行できるように、このポートをオープンにする必要があります。
17002	ODBC/JDBC	ODBC または JDBC ドライバと、CA Enterprise Log Manager イベント ログ ストア間の通信に使用されるデフォルトの TCP ポート
17003	Agent	r12.1 エージェント用の Qpid メッセージ バスによる通信に使用される TCP ポート
17200	ディスパッチャ SME リスナ	エージェント ローカル ホスト上のディスパッチャ サービスに使用される TCP ポート。エージェント プロセス間の自己監視イベントを待ち受けます。
17201	ディスパッチャ イベント リスナ	エージェント ローカル ホスト上のディスパッチャ サービスに使用される TCP ポート。クライアント コネクタからのイベントを待ち受けます。
random	SAPI	ポートマッピング機能によって割り当てられた、イベント収集に使用される UDP ポート。1024 よりも番号の大きい任意の固定ポートを使用するように SAPI ルータおよびコレクタを設定できます。

関連プロセスのリスト

次の表は、CA Enterprise Log Manager の実装の一部として実行されるプロセスのリストを表します。リストには、基礎となるオペレーティング システムに関連するシステム プロセスは含まれません。

プロセス名	デフォルトのポート	説明
caelmagent	6789、17001	CA Enterprise Log Manager エージェントのプロセスです。
caelmconnector	リスン対象、または接続先により異なります。	CA Enterprise Log Manager コネクタのプロセスです。エージェントで設定されたコネクタごとに、個別のコネクタ プロセスが実行されます。
caelmdispatcher		この CA Enterprise Log Manager プロセスは、コネクタとエージェント間のイベント送信およびステータス情報を処理します。
caelmwatchdog	None	操作の継続性を確実にするために他のプロセスを監視する CA Enterprise Log Manager のウォッチドッグ プロセスです。
caelm-agentmanager		この CA Enterprise Log Manager プロセスは、ステータスやサブスクリプションなどのエージェント管理タスクを処理します。
caelm-alerting		この CA Enterprise Log Manager プロセスは、電子メール、IT PAM および SNMP トラップを介して送信されるアラート メッセージを処理します。
caelm-correlation		この CA Enterprise Log Manager プロセスは、相関ルールがトリガされた場合に相関サービスと通信し、相関ルールを処理します。
caelm-eemsessionsponsor		CA Enterprise Log Manager サーバのセーフティネットの下で実行しているローカル スポンサーの CA EEM への全通信を管理する CA EEM のメイン プロセスです。 このプロセスはセーフティネットの下で実行できます。

プロセス名	デフォルトのポート	説明
caelm-incidentservice		この CA Enterprise Log Manager プロセスは、相関ルールがトリガされた場合に相関サービスからの情報を処理し、インシデント生成およびログ記録設定に対応します。
caelm-logdepot	17001	イベントの保存、アーカイブ ファイル作成、およびその他の機能を処理する CA Enterprise Log Manager のイベント ログ ストアのプロセスです。 このプロセスはセーフティネットの下で実行できます。
caelm-queryservice		この CA Enterprise Log Manager プロセスは、クエリの設定および管理を処理します。
caelm-reporter		この CA Enterprise Log Manager プロセスは、スケジュール済みレポート、レポートのエクスポート、およびアクション アラートの設定および管理を処理します。
caelm-ruletest		この CA Enterprise Log Manager プロセスは、アドホック ベースで実行されるルール テストを管理します。
caelm-sapicollector		SAPI コレクタ サービスのプロセスです。 このプロセスはセーフティネットの下で実行できます。
caelm-sapirouter		SAPI ルータ サービスのプロセスです。 このプロセスはセーフティネットの下で実行できます。
caelm-systemstatus		このプロセスは、CA Enterprise Log Manager ユーザ インターフェースに表示するシステム ステータスを収集します。 このプロセスはセーフティネットの下で実行できます。
dxadmind		CA EEM がインストールされているサーバで実行される CA Directory のプロセスです。
dxserver		CA EEM がインストールされているサーバで実行される CA Directory のプロセスです。

プロセス名	デフォルトのポート	説明
iGateway	5250	CA Enterprise Log Manager メイン プロセスです。イベントを収集して保存するにはこのプロセスを実行する必要があります。
message broker		イベントの送信にあたって、エージェントと CA Enterprise Log Manager サーバ間の通信を処理する CA Enterprise Log Manager プロセスです。
oaserver	17002	ODBC および JDBC がイベント ログ ストアにアクセスするための要求に対して、サーバ側での処理を実行する CA Enterprise Log Manager プロセスです。
safetynet		操作の継続性を確実にするために実行される CA Enterprise Log Manager プロセスのフレームワークです。
ssld		CA EEM がインストールされているサーバで実行される CA Directory のプロセスです。

OS ハードニング

CA Enterprise Log Manager ソフト アプライアンスには、Red Hat Linux オペレーティング システムの合理化されハードニングされたコピーが含まれています。以下のハードニング手法が適用されます。

- root ユーザとして SSH にアクセスすることはできません。
- ログインせずに、コンソールから Ctrl+Alt+Del キー シーケンスを使用してサーバを再起動することはできません。
- リダイレクトは、IP テーブルで以下のポートに対して適用されます。
  - TCP Port 80 および 443 は 5250 にリダイレクトされます。
  - UDP ポート 514 は 40514 にリダイレクトされます。

- GRUB パッケージはパスワード保護されます。
- インストールによって、権限の低い以下のユーザが追加されます。
  - caelmadmin - CA Enterprise Log Manager サーバ コンソールへのログイン権限を持つオペレーティング システム アカウント。
  - caelmservice - iGateway およびエージェントのプロセスを実行するサービス アカウント。このアカウントを使用して直接ログインすることはできません。

syslog イベント用のファイアウォール ポートのリダイレクト

エージェントと CA Enterprise Log Manager サーバの間にファイアウォールを使用している場合は、標準ポートのトラフィックを別のポートへリダイレクトできます。

セキュリティに関するベスト プラクティスでは、アプリケーション プロセスおよびデーモンを実行するのに必要なのは最小限のユーザ権限です。root 以外のアカウントで実行している UNIX と Linux のデーモンは、1024 より小さいポートをオープンにすることができません。標準的な UDP の syslog ポートは 514 です。そのため、標準以外のポートを使用できないルータやスイッチなどのデバイスで問題が発生する場合があります。

この問題を解決するには、受信トラフィックをポート 514 で待ち受け、他のポートで CA Enterprise Log Manager サーバに送信するようにファイアウォールを設定します。リダイレクトは syslog リスナと同じホストで実行します。代わりに標準以外のポートを使用するように選択した場合は、そのポートにイベントを送信するように各イベント ソースを再設定する必要があります。

ファイアウォールを使用してイベントのトラフィックをリダイレクトする方法

1. root ユーザとしてログインします。
2. コマンド プロンプトにアクセスします。
3. 特定のファイアウォール用にポートをリダイレクトするコマンドを入力します。

Red Hat Linux オペレーティング システムで実行する netfilter または iptables パケット フィルタリング ツールのコマンド ライン入力の例を次に示します。

```
chkconfig --level 345

iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to <yournewport>

service iptables save
```

4. 変数 *<yournewport>* の値を、使用可能な 1024 より大きいポート番号に置き換えます。

   その他の実装については、ファイアウォール ベンダーが提供しているポート処理の手順を参照してください。

ODBC クライアントのインストール

Windows システムに ODBC クライアントをインストールするには、次の手順を実行します。

1. 必要な権限を持っており、ODBC クライアント ドライバのライセンス キーが取得できることを確認します（前提条件）。
2. ODBC クライアントをインストールします。
3. Windows Data Source（ODBC）ユーティリティを使用して、データ ソースを作成します。
4. ODBC クライアントの接続の詳細を設定します。
5. データベースへの接続をテストします。

前提条件

イベント ログ ストアへの ODBC アクセスは、CA Enterprise Log Manager r12.1 以降のリリースでのみ利用可能です。インストールを開始する前に、ODBC データ ソースの注意事項で必要な情報を参照します。

この機能のユーザは、（CALM アクセス ポリシーの）デフォルト データ アクセス ポリシーで、データ アクセス権限を保持しているユーザ グループに属す必要があります。*アクセス ポリシーの詳細については、「CA Enterprise Log Manager r12.1 管理ガイド」を参照してください。*

ODBC クライアントについては、次の前提条件が適用されます。

- ODBC クライアントを Windows サーバにインストールするには、管理者権限を保持している必要があります。
- ODBC クライアントのインストールには、Microsoft Windows Installer サービスが必要です。このサービスが見つからない場合はメッセージが表示されます。
- CA Enterprise Log Manager で ODBC サーバ サービスを設定して、[サービスの有効化]チェック ボックスがオンになっていることを確認します。
- [コントロール パネル]のデータ ソース(ODBC)ユーティリティを使用して、ODBC データ ソースを Windows システム向けに設定します。
- UNIX および Linux システムにクライアントをインストールする場合は、インストール先のディレクトリに対して、ファイル作成の権限を持っている必要があります。

ODBC および JDBC 機能をサポートする特定のプラットフォームの詳細については、CA Enterprise Log Manager サポート サイトの互換性マトリクス（http://www.ca.com/Support）を参照してください。

ODBC サーバ サービスの設定

この手順を使用すると、CA Enterprise Log Manager イベント ログ ストアへの ODBC および JDBC アクセスを設定できます。

ODBC および JDBC アクセスを設定する方法

1. 管理者ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックし、[サービス]サブタブをクリックします。
3. [ODBC サーバ サービス]をクリックしてグローバル設定を開きます。または、ノードを展開して特定の CA Enterprise Log Manager サーバを選択します。
4. デフォルト値以外のポートを使用する場合は、[サービス ポート]フィールドにポート値を設定します。
5. SSL を有効にして、ODBC クライアントと CA Enterprise Log Manager サーバ間のデータ伝送を暗号化するかどうかを指定します。

   注: サービス ポートおよび SSL 有効化の設定は、サーバと ODBC クライアントの両方で一致している必要があります。ポートのデフォルト値は 17002 です。また、SSL 暗号化はデフォルトで有効です。この設定が ODBC クライアントの設定と一致していないと、接続の試行に失敗します。

Windows システムへの ODBC クライアントのインストール

Windows システムに ODBC クライアントをインストールするには、この手順を使用します。

注: ODBC クライアントのインストールには、Windows 管理者アカウントが必要です。

ODBC クライアントのインストール方法

1. アプリケーション DVD またはインストール イメージ内の ODBC クライアント ディレクトリを、ディレクトリ ¥CA¥ELM¥ODBC に置きます。
2. アプリケーション（setup.exe）をダブルクリックします。
3. 使用許諾契約に同意して［次へ］をクリックします。

   ［インストール先の選択］パネルが表示されます。
4. インストール先を入力するか、またはデフォルトの場所を受け入れて［次へ］をクリックします。

   ［プログラム フォルダの選択］パネルが表示されます。
5. プログラム フォルダを選択するか、またはデフォルト選択を受け入れて［次へ］をクリックします。

   ［ファイルのコピーを開始］パネルが表示されます。
6. ［次へ］をクリックしてファイルのコピーを開始します。

   ［セットアップステータス］パネルに、インストールの進行状況が表示されます。インストールのファイルのコピーが完了すると、［InstallShield ウィザードの完了］パネルが表示されます。
7. ［完了］をクリックして、インストールを終了します。

Windows システムへの ODBC データ ソースの作成

Windows システムに、必要な ODBC データ ソースを作成するには、この手順を使用します。データ ソースはユーザ DSN またはシステム DSN のいずれかとして作成できます。

データ ソースの作成方法

1. Windows の[コントロール パネル]にアクセスし、[管理ツール]を開きます。
2. ユーティリティ(データ ソース(ODBC))をダブルクリックします。[ODBC データ ソース アドミニストレータ]ウィンドウが表示されます。
3. [追加]をクリックして、[データ ソースの新規作成]ウィンドウを表示します。
4. [CA Enterprise Log Manager ODBC ドライバ]を選択し、[完了]をクリックします。

   [CA Enterprise Log Manager ODBC ドライバ セットアップ]ウィンドウが表示されます。
5. フィールドに、ODBC データ ソースの注意事項セクションで説明している値を入力し、[OK]をクリックします。

ODBC データ ソースの注意事項

以下は、CA Enterprise Log Manager に関連している ODBC データ ソース フィールドの説明です。

データ ソース名

このデータ ソースの名前を作成します。このデータを使用するクライアント アプリケーションがデータ ソースに接続する際に、この名前を使用します。

サービス ホスト

クライアントが接続する CA Enterprise Log Manager サーバの名前を指定します。ホスト名または IPv4 アドレスのいずれかを使用できます。

サービス ポート

CA Enterprise Log Manager サーバが ODBC クライアント接続をリスンする TCP サービス ポートを指定します。デフォルト値は 17002 です。ここで設定した値は、ODBC サーバ サービスの設定と一致する必要があります。一致しない場合、接続は失敗します。

サービス データ ソース

このフィールドは空白のままにします。そうでない場合、接続の試行は失敗します。

暗号化 SSL

クライアントと CA Enterprise Log Manager サーバ間の通信で暗号化を使用するかどうかを指定します。デフォルト値では SSL は有効です。ここで設定した値は、ODBC サーバ サービスの設定と一致する必要があります。一致しない場合、接続は失敗します。

カスタム プロパティ

イベント ログ ストアで使用するための接続プロパティを指定します。プロパティ間の区切り文字は、スペースのないセミコロンです。推奨されるデフォルト値には、以下のものがあります。

querytimeout

この時間データの返信がない場合にクエリが終了するタイムアウト値を秒単位で指定します。以下は、このプロパティで使用する構文です。

```
querytimeout=300
```

queryfederated

連携クエリを実行するかどうかを指定します。この値を false に指定すると、データベース接続が確立された CA Enterprise Log Manager サーバ上でのみクエリが実行されます。以下は、このプロパティで使用する構文です。

```
queryfederated=true
```

queryfetchrows

クエリが成功した場合に、1 回のフェッチ操作で取得する行数を指定します。最小値は 1 で、最大値は 5000 です。デフォルト値は 1000 です。以下は、このプロパティで使用する構文です。

```
queryfetchrows=1000
```

offsetmins

この ODBC クライアントのタイムゾーンのオフセットを指定します。値を 0 に指定すると、GMT が使用されます。お使いのタイムゾーンの GMT からのオフセットを設定する際に、このフィールドを使用できます。 以下は、このプロパティで使用する構文です。

```
offsetmins=0
```

suppressNoncriticalErrors

データベースが応答しない、ホストが応答しないなどの、クリティカルでないエラーが発生した場合のインターフェース プロバイダの動作を示します。

以下は、このプロパティで使用する構文です。

```
suppressNoncriticalErrors=false
```

ODBC クライアントのデータベース接続のテスト

ODBC クライアントのインストールには、コマンド ラインによる対話型の SQL クエリ ツール(ISQL)を使用します。このツールを使用して、構成設定および ODBC クライアントと CA Enterprise Log Manager イベント ログ ストア間の接続性をテストすることもできます。

データベースへのクライアント接続をテストする方法

1. コマンド プロンプトにアクセスし、ODBC クライアントをインストールしたディレクトリへ移動します。
2. ISQL ユーティリティ、odbcisql.exe を開始します。
3. 次のコマンドを入力して、データベースへのクライアント接続をテストします。

   ```
   connect User*Password@DSN_name
   ```

   DSN_name の値には、データベースへの ODBC 接続用として今回作成したデータ ソース名を使用します。接続パラメータが正しい場合、次のようなメッセージが返されます。

   ```
   SQL: connecting to database: DSN_name
   Elapsed time 37 ms.
   ```

注: パスワードに @ 記号が含まれる場合、iSQL ユーティリティは、「@」の後の部分すべてを DSN 名と解釈するため、正しく実行されません。この問題を回避するには、パスワードを引用符で囲みます。

```
Connect User*"Password"@DSN_name
```

データベースからのサーバ取得のテスト

このテスト クエリを使用して、ODBC クライアント アプリケーションが、確立されたデータベース接続を使用して、CA Enterprise Log Manager イベント ログ ストアからデータを取り戻すことができるかどうかを確認します。この手順では、ODBC 接続のテストに使用したものと同じ ISQL ユーティリティを使用します。

注: ODBC 接続のテストには、CA Enterprise Log Manager クエリおよびレポートで提供された SQL クエリをコピーして使用しないでください。この SQL ステートメントは CA Enterprise Log Manager サーバ専用で、イベント ログ ストアと共に使用するものです。ODBC SQL クエリは、ANSI SQL 標準に従った標準的な設計で作成します。

サーバ コンポーネントのデータ取得のテスト方法

1. コマンド プロンプトにアクセスし、ODBC クライアントをインストールしたディレクトリへ移動します。
2. ISQL ユーティリティ、odbcisql.exe を開始します。
3. 次の SELECT ステートメントを入力し、イベント ログ ストアからの取得をテストします。

```
select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from
view_event where event_time_gmt < now() and event_time_gmt >
timestampadd(mi,-15,now()) GROUP BY receiver_hostname, event_logname;
```

JDBC クライアントのインストール

JDBC クライアントは、任意の Java 対応アプレット、アプリケーション、またはアプリケーション サーバを介した JDBC アクセスを提供します。JDBC アクセスでは、データ ソースに対して、高パフォーマンスなポイント ツー ポイントの n 層アクセスが実現します。クライアントは Java 環境向けに最適化されているため、Java テクノロジを組み込んで、既存のシステムの機能とパフォーマンスを拡張することができます。

JDBC クライアントは 32 ビットと 64 ビットのプラットフォームで実行されます。64 ビットプラットフォームの場合、既存のアプリケーションを実行するための変更は必要ありません。

JDBC クライアントをインストールするには、次の手順を実行します。

1. 接続プール設定機能を備えた Web アプリケーション サーバがインストールされ、実行されていることを確認します。
2. DBC クライアント ドライバのライセンス キーを取得します。
3. JDBC クライアントをインストールします。
4. Web アプリケーション サーバの接続プール管理機能を使用して、データベースへの接続を設定します。
5. データベースへの接続をテストします。

JDBC クライアント前提条件

イベント ログ ストアへの JDBC アクセスは、CA Enterprise Log Manager r12.1 以降のリリースでのみ利用可能です。JDBC クライアントは Windows と UNIX のシステムにインストールできます。

この機能のユーザは、(CALM アクセス ポリシーの) デフォルト データ アクセス ポリシーで、データ アクセス権限を保持しているユーザ グループに属す必要があります。アクセス ポリシーの詳細については、「CA Enterprise Log Manager r12.1 管理ガイド」を参照してください。

JDBC クライアントについては、次の前提条件が適用されます。

- JDBC クライアントを Windows サーバにインストールするには、管理者権限を保持している必要があります。
- [ODBC サーバ設定]ウィンドウで、[サービスの有効化]チェック ボックスが選択されている (オンになっている) ことを確認します。
- UNIX および Linux システムにクライアントをインストールする場合は、インストール先のディレクトリに対して、ファイル作成の権限を持っている必要があります。
- J2SE v 1.4.2.x で作動するアプリケーションについては、特定のアプリケーションで定義されているように、プログラミングでデータベース接続を設定します。
- J2EE 1.4.2.x 以降のバージョンで動作するアプリケーションについては、Oracle WebLogic や Red Hat JBoss などの Web アプリケーション サーバを使用して接続プール管理を設定します。

ODBC および JDBC 機能をサポートする特定のプラットフォームの詳細については、CA Enterprise Log Manager サポート サイトの互換性マトリクス (http://www.ca.com/Support) を参照してください。

Windows システムへの JDBC クライアントのインストール

Windows システムに JDBC クライアントドライバをインストールするには、この手順を使用します。

JDBC ドライバをインストールする方法

1. アプリケーション DVD またはインストール イメージ内にある以下の 2 つの .jar ファイルを、ディレクトリ CA/ELM/JDBC に置きます。

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. 宛先サーバの希望するディレクトリにこの .jar ファイルをコピーし、コピー先をメモします。

UNIX システムへの JDBC クライアントのインストール

UNIX システムに JDBC クライアントドライバをインストールするには、この手順を使用します。

JDBC ドライバをインストールする方法

1. アプリケーション DVD またはインストール イメージ内にある以下の 2 つの .jar ファイルを、ディレクトリ CA/ELM/JDBC に置きます。

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. 宛先サーバの希望するディレクトリにこの .jar ファイルをコピーし、コピー先をメモします。

3. UNIX 上の JDBC 用に JDBC クライアントをインストールしたら、インストール ディレクトリから以下の（または以下と同様の）コマンドを手動で実行します。

   ```
   chmod -R ugo+x file_location
   ```

   file_location に入る値は、JDBC クライアントをインストールしたディレクトリです。この手順によって、インストール済みのクライアントで提供されるシェル スクリプトを実行できます。

JDBC 接続パラメータ

さまざまなアプリケーションでは、JDBC クライアントドライバを使用するために所定の接続パラメータが必要となります。通常のパラメータには以下が含まれます。

- 接続文字列または接続 URL
- クラス名

JDBC 接続文字列（URL）は次の形式になります。

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

JDBC ドライバ クラス名は次のとおりです。

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

JDBC URL の注意事項

JDBC クライアントを使用して CA Enterprise Log Manager に格納されているイベント データにアクセスする場合、JDBC クラスパスおよび JDBC URL の両方が必要となります。JDBC クラスパスは、ドライバ JAR ファイルの場所を指定したものです。JDBC URL は、ロードする際に JAR 内のクラスが使用するパラメータを定義したものです。

以下は、完全な JDBC URL の例です。

```
jdbc:ca-elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout
=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

以下で、URL コンポーネントについて説明します。

jdbc:ca-elm:

CA Enterprise Log Manager と共に提供されている JDBC ドライバを指定する、プロトコル：サブプロトコルの文字列を定義します。

//IP Address:Port;

アクセスするデータが格納された CA Enterprise Log Manager サーバを表す IP アドレスを指定します。ポート番号は、通信に使用するポートで、CA Enterprise Log Manager［ODBC サービスの設定］パネルの設定と一致する必要があります。ポートが一致しない場合、接続の試行は失敗します。

encrypted=0|1;

JDBC クライアントと CA Enterprise Log Manager サーバ間の通信に SSL 暗号化を使用するかどうかを決定します。デフォルト値は 0 で、暗号化されず、URL 内での指定が必要ありません。encrypted=1 と設定すると、暗号化が有効になります。 接続の暗号化が明示的に設定されます。 また、この設定は、CA Enterprise Log Manager [ODBC サービス]ダイアログ ボックスで設定したものと一致する必要があります。一致しない場合は、接続の試行は失敗します。

ServerDataSource=Default

データ ソースの名前を指定します。CA Enterprise Log Manager イベント ログ ストアへのアクセスの場合は、この値を「Default」に設定します。

CustomProperties=（x; y; z）

このプロパティは ODBC カスタム プロパティと同じものです。明示的に指定しない場合、URL 例で示されたデフォルト値が適用されます。

詳細情報

ODBC データ ソースの注意事項 (P. 119)

インストールに関するトラブルシューティング

次のインストール ログ ファイルを確認して、インストールのトラブルシューティングを開始できます。

製品	ログ ファイルの場所
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log /tmp/install_ca-elm.<*timestamp*>.log /tmp/install_ca-elmagent.<*timestamp*>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log
CA Directory	/tmp/etrdir_install.log

CA Enterprise Log Manager のインストールでは、CA EEM サーバに管理用のコンテンツやその他のファイルをコピーします。CA EEM サーバ側から見ると、CA Enterprise Log Manager のレポートやその他のファイルがインポートされます。インストール時に CA EEM サーバに接続できない場合、CA Enterprise Log Manager のインストールはコンテンツ ファイルをインポートせずに続行します。インストールが完了したら、コンテンツ ファイルを手動でインポートできます。

インストール中にエラーが発生した場合、インストールを完了するには次の 1 つ以上のアクションを実行しなければならない場合があります。この各アクションを行うには、デフォルトのアカウント caelmadmin を使用して CA Enterprise Log Manager サーバにログインし、その後に root アカウントにユーザを切り替えます。

- ネットワーク インターフェースの設定エラーの解決
- rpm パッケージがインストールされたかどうかの確認
- iGateway デーモンが実行されているかどうかの確認
- CA EEM サーバでの CA Enterprise Log Manager アプリケーションの登録
- デジタル証明書の取得
- CA Enterprise Log Manager レポートのインポート
- データ マッピング ファイルのインポート
- メッセージ解析ファイルのインポート
- 共通イベント文法（CEG）ファイルのインポート
- 共通のエージェント管理ファイルのインポート

ネットワーク インターフェースの設定エラーの解決

インストール後に、CA Enterprise Log Manager サーバのユーザ インターフェースにアクセスできない場合は、ネットワーク インターフェースに設定エラーがある可能性があります。エラーを解決するには 2 つのオプションがあります。

- 物理ネットワーク ケーブルを取り除き、それを別のポートに挿入します。
- コマンド ラインから、論理的なネットワーク インターフェース アダプタを再設定します。

コマンド ラインからネットワーク アダプタのポートを再設定する方法

1. caelmadmin ユーザとしてソフトウェア アプライアンスにログインし、コマンド プロンプトにアクセスします。
2. 次のコマンドを使用して、ユーザを root ユーザに切り替えます。

   ```
   su -
   ```

3. root ユーザのパスワードを入力して、システムへのアクセスを確認します。
4. 以下のコマンドを入力します。

   ```
   system-config-network
   ```

   ネットワーク アダプタを設定するためのユーザ インターフェースが表示されます。
5. 必要なポート設定を行って、終了します。
6. 次のコマンドを使用して、ネットワーク サービスを再起動して変更を有効にします。

   ```
   service network restart
   ```

RPM パッケージのインストールの確認

適切な rpm パッケージがインストールされていることを確認して、インストールの簡単なチェックを実行できます。

rpm パッケージを確認する方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root アカウントに切り替えます。

   ```
   su - root
   ```

4. 次のコマンドを使用して、ca-elm-<version>.i386.rpm パッケージがインストールされていることを確認します。

   ```
   rpm -q ca-elm
   rpm -q ca-elmagent
   ```

   インストールされていれば、オペレーティング システムによってパッケージのフル ネームが返されます。

CA Enterprise Log Manager サーバの CA EEM サーバへの登録

症状:

インストール中に、CA Enterprise Log Manager アプリケーションが CA EEM サーバに正常に登録されませんでした。CA Enterprise Log Manager アプリケーションは、ユーザ アカウントとサービス設定の管理を CA EEM サーバに依存しています。CA Enterprise Log Manager アプリケーションが登録されないと、ソフトウェアは正常に動作しません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

CA EEM サーバに CA Enterprise Log Manager アプリケーションを手動で登録します。

CA Enterprise Log Manager アプリケーションを登録する方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./EEMRegister.sh
   ```

   シェル スクリプトによって CA Enterprise Log Manager アプリケーションが CA EEM サーバに登録されます。

CA EEM サーバからの証明書の取得

症状:

インストール中に、CA EEM サーバからデジタル証明書を正常に取得できませんでした。デジタル証明書は CA Enterprise Log Manager アプリケーションを起動して実行するために必要です。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

CA EEM サーバから証明書を手動で取得します。

デジタル証明書を取得する方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./EEMAcqCert.sh
   ```

   シェル スクリプトによって、必要なデジタル証明書を得るための処理が実行されます。

CA Enterprise Log Manager レポートのインポート

症状:

インストール中に、CA EEM サーバは CA EEM サーバからのレポートの内容を正常にインポートできませんでした。イベント ログ ストアに保存された後にイベント データを表示するには、レポートの内容をインポートする必要があります。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

レポートの内容を手動でインポートします。

レポートの内容をインポートする方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMContent.sh
   ```

   シェル スクリプトによって CA EEM サーバからレポートの内容がダウンロードされます。

CA Enterprise Log Manager データ マッピング ファイルのインポート

症状:

インストール中に、CA EEM サーバはデータ マッピング (DM) ファイルを正常にインポートできませんでした。受信イベント データをイベント ログ ストアにマッピングするには DM ファイルが必要です。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

DM ファイルを手動でインポートします。

DM ファイルをインポートする方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMDM.sh
   ```

   シェル スクリプトによって、CA EEM サーバから DM ファイルがインポートされます。

共通イベント文法ファイルのインポート

症状:

インストール中に、CA EEM サーバは共通イベント文法(CEG)ファイルを正常にインポートできませんでした。CEG は、イベント ログ ストアの基礎となるデータベース スキーマを形成します。CEG ファイルがないと、CA Enterprise Log Manager イベント ログ ストアにイベントを保存できません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

CEG ファイルを手動でインポートします。

CEG ファイルをインポートする方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMCEG.sh
   ```

   シェル スクリプトによって、共通イベント文法ファイルがインポートされます。

相関ルール ファイルのインポート

症状:

インストール中に、CA EEM サーバが相関ルール ファイルを正常にインポートできませんでした。相関ルールは、調査が必要なイベントのパターンを特定できるようにします。相関グループまたはルールをインポートできます。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

相関ルール ファイルを手動でインポートします。

相関ルール ファイルをインポートする方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 以下のいずれかのコマンドを実行します。

   ```
   ./ImportCALMCorrelationGroups.sh
   ```

   シェル スクリプトが相関ルール グループをインポートします。

   ```
   ./ImportCALMCorrelationRules.sh
   ```

   シェル スクリプトが相関ルール ファイルをインポートします。

共通のエージェント管理ファイルのインポート

症状:

CA EEM サーバは、インストール中に、共通のエージェント管理ファイルを正常にインポートできませんでした。このファイルがないと、CA Enterprise Log Manager ユーザ インターフェースでエージェントを管理することができません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

エージェント管理ファイルを手動でインポートします。

共通のエージェント管理ファイルのインポート方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMAgentContent.sh
   ```

   シェル スクリプトによって、共通のエージェント管理ファイルがインポートされます。

CA Enterprise Log Manager 設定ファイルのインポート

症状:

CA EEM サーバは、インストール中に、設定ファイルを正常にインポートできませんでした。CA Enterprise Log Manager は開始できますが、一定の設定および値がサービス設定領域に見当たりません。これらのファイルがないため、個々のホストを中央で設定することができません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

設定ファイルを手動でインポートします。

設定ファイルをインポートする方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMConfig.sh
   ```

   シェル スクリプトによって設定ファイルがインポートされます。

抑制および集約ファイルのインポート

症状:

CA EEM サーバは、インストール中に、抑制および集約ファイルを正常にインポートできませんでした。これらのファイルがないと、CA Enterprise Log Manager ユーザ インターフェースでは既定の抑制および集約ルールを使用することができません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

抑制および集約ファイルを手動でインポートします。

抑制および集約ファイルのインポート方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMSAS.sh
   ```

   シェル スクリプトによって抑制および集約ファイルがインポートされます。

解析トークン ファイルのインポート

症状:

インストール中に、CA EEM サーバは解析トークン ファイルを正常にインポートできませんでした。これらのファイルがないと、メッセージ解析ウィザードで既定の解析トークンを使用することができません。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

解析トークン ファイルを手動でインポートします。

解析トークン ファイルのインポート方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMTOK.sh
   ```

   シェル スクリプトによって解析トークン ファイルがインポートされます。

CA Enterprise Log Manager ユーザ インターフェース ファイルのインポート

症状:

CA EEM サーバは、インストール中に、ユーザ インターフェース ファイルを正常にインポートできませんでした。これらのファイルがないと、[動的時間帯]ドロップダウン フィールドに値が表示されなくなります。

この後の手順に示すシェル スクリプトは、インストール中に指定されたディレクトリに自動的にコピーされます。

解決方法:

ユーザ インターフェース ファイルを手動でインポートします。

ユーザ インターフェース ファイルのインポート方法

1. CA Enterprise Log Manager サーバのコマンド プロンプトにアクセスします。
2. caelmadmin アカウントの認証情報を使用してログインします。
3. 次のコマンドを使用してユーザを root ユーザに切り替えます。

   ```
   su -
   ```

4. /opt/CA/LogManager/EEM/content ディレクトリに移動します。
5. 次のコマンドを実行します。

   ```
   ./ImportCALMFlexFiles.sh
   ```

   シェル スクリプトによってユーザ インターフェース ファイルがインポートされます。

第 4 章: ユーザおよびアクセスの基本的な設定

このセクションには、以下のトピックが含まれています。

基本的なユーザとアクセスについて

ユーザ ストアの設定、事前定義済みの Administrator ロールを持つ 1 人以上のユーザの作成、およびパスワード ポリシーの設定から設定作業を開始します。通常、この設定はインストーラによって実行されます。インストーラは EiamAdmin 認証情報を使用して CA Enterprise Log Manager にログオンできます。この設定が完了したら、Administrator として定義されたユーザが CA Enterprise Log Manager を設定します。

デフォルトのユーザ ストアの設定を受け入れる場合、EiamAdmin ユーザは最低限、最初の管理者アカウントの設定を完了する必要があります。最初の管理者は、他の CA Enterprise Log Manager コンポーネントを設定する前にパスワード ポリシーを設定できます。

注: 他のユーザの作成方法や、カスタム アクセス ポリシーを持つカスタム ロール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。

ユーザ ストアの設定

ユーザ ストアとは、グローバル ユーザ情報のリポジトリです。CA Enterprise Log Manager サーバをインストールしたらすぐに、ユーザ ストアを設定できます。EiamAdmin ユーザだけがユーザ ストアを設定できます。通常、これは最初のログオン直後に行われます。

次のいずれかの方法でユーザ ストアを設定します。

- デフォルトの[内部データ ストアに保存]を受け入れます。

  注: インストール中にスタンド アロンの CA EEM を指定した場合、デフォルト オプションを CA の管理データベースとして表示できます。

- 外部ディレクトリの参照を選択します。外部ディレクトリには、Microsoft Active Directory、Sun One、または Novell CA Directory などの LDAP ディレクトリを使用できます。

- CA SiteMinder の参照を選択します。

ユーザ ストアを外部ディレクトリに設定した場合は、新規ユーザを作成できません。事前定義済みおよびユーザ定義のアプリケーション グループまたはロールのみを、読み取り専用のグローバル ユーザ レコードに追加できます。外部のユーザ ストアに新規ユーザを追加してから、CA Enterprise Log Manager の権限をグローバル ユーザ レコードに追加する必要があります。

デフォルトのユーザ ストアの受け入れ

デフォルトの内部データストアを受け入れる場合は、ユーザ ストアを設定する必要はありません。参照する外部ユーザ ストアがない場合は、デフォルトを適用します。

デフォルトのリポジトリがユーザ ストアとして設定されていることを確認する方法

1. 管理者権限を持つユーザ、または EiamAdmin というユーザ名のユーザとして、関連するパスワードを使用して CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックします。

   EiamAdmin ユーザとしてログインすると、このタブが自動的に表示されます。

3. [ユーザとアクセスの管理]サブタブを選択し、次に、左側のペインにある[ユーザ ストア]ボタンをクリックします。

   [EEM サーバのグローバル ユーザ/グローバル グループ設定]が表示されます。

4. オプションの[内部データ ストアに保存]が選択されていることを確認します。

5. [保存]をクリックして[閉じる]をクリックします。

注: デフォルトのユーザ ストアが設定されている場合は、新規ユーザを作成し、一時パスワードを設定し、パスワード ポリシーを設定できます。

詳細情報:

ユーザ ストアの計画 (P. 41)

LDAP ディレクトリの参照

グローバル ユーザの詳細が Microsoft Active Directory、Sun One、または Novell Directory に保存されている場合は、LDAP ディレクトリを参照するようにユーザ ストアを設定します。

注: アプリケーションの詳細はデフォルトのリポジトリに格納されます。 外部のユーザ ストアを参照する場合、そのユーザ ストアは更新されません。

LDAP ディレクトリをユーザ ストアとして参照する方法

1. 管理者権限を持つユーザ、または EiamAdmin ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックします。

   EiamAdmin ユーザとしてログインすると、このタブが自動的に表示されます。

3. [ユーザとアクセスの管理]サブタブを選択し、次に、左側のペインにある[ユーザ ストア]をクリックします。

   [CA EEM サーバのユーザ ストア設定]が表示されます。

4. [外部ディレクトリから参照]を選択します。

   LDAP 設定用のフィールドが表示されます。

5. 外部ディレクトリ用のワークシートで計画したとおりに、これらのフィールドに入力します。

   次のバインディング文字列を使用して、Active Directory オブジェクトにバインディングする例を考えてみます。

   Set objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com") ここで、cn は共有名、ou は組織単位、dc は完全な DNS 名を構成する 2 つのドメイン コンポーネントで構成されます。User DN については、次のように入力します。

   ```
   cn=Bob,cn=Users,ou=Sales,dc=MyDomain,dc=com
   ```

6. [保存]をクリックします。

   この参照を保存すると、ユーザ アカウント情報が CA EEM にロードされます。これによって、グローバル ユーザとしてユーザ レコードにアクセスし、アプリケーション ユーザ グループやユーザ ロール名などのアプリケーション レベルの詳細を追加できます。

7. 表示ステータスを確認し、外部ディレクトリのバインドが成功してデータがロードされたことを確認します。

   ステータスに警告が表示される場合は、[ステータスの更新]をクリックします。ステータスにエラーが表示される場合は、設定を修正して[保存]をクリックし、この手順を繰り返します。

8. [閉じる]をクリックします。

詳細情報:

ユーザ ストアの計画 (P. 41)
外部の LDAP ディレクトリ用のワークシート (P. 42)

CA SiteMinder のユーザ ストアとしての参照

ユーザ アカウントがすでに CA SiteMinder に定義されている場合は、ユーザ ストアを設定するときにこの外部ディレクトリを参照します。

CA SiteMinder をユーザ ストアとして参照する方法

1. 管理者権限を持つユーザ、または EiamAdmin ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックします。

   EiamAdmin ユーザとしてログインすると、このタブが自動的に表示されます。
3. [ユーザとアクセスの管理]サブタブを選択し、次に、左側のペインにある[ユーザ ストア]ボタンをクリックします。

   [CA EEM サーバのユーザ ストア設定]が表示されます。
4. [CA SiteMinder からの参照]オプションを選択します。

   CA SiteMinder の特定のフィールドが表示されます。

   a. SiteMinder のワークシートで計画したとおりに、これらのフィールドに入力します。

   b. CA SiteMinder が使用する接続とポートを表示または変更するには、省略記号をクリックして[接続属性]パネルを表示します。
5. [保存]をクリックします。

   この参照を保存すると、ユーザ アカウント情報が CA EEM にロードされます。これによって、グローバル ユーザとしてユーザ レコードにアクセスし、アプリケーション ユーザ グループやユーザ ロール名などのアプリケーション レベルの詳細を追加できます。
6. 表示ステータスを確認し、外部ディレクトリのバインドが成功してデータがロードされたことを確認します。

   ステータスに警告が表示される場合は、[ステータスの更新]をクリックします。ステータスにエラーが表示される場合は、設定を修正して[保存]をクリックし、この手順を繰り返します。
7. [閉じる]をクリックします。

詳細情報:

ユーザ ストアの計画 (P. 41)
CA SiteMinder ワークシート (P. 44)

パスワード ポリシーの設定

パスワード ポリシーを設定して、自分のために作成したパスワードが設定された基準を満たし、設定された頻度で変更されるようにすることができます。内部ユーザ ストアを設定した後にパスワード ポリシーを設定します。EiamAdmin ユーザまたは Administrator ロールを割り当てたユーザだけが、パスワード ポリシーを設定または変更できます。

注: CA Enterprise Log Manager のパスワード ポリシーは外部のユーザ ストアに作成されたユーザ アカウントには適用されません。

パスワード ポリシーを設定する方法

1. 管理者権限を持つユーザ、または EiamAdmin ユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブをクリックします。

   EiamAdmin ユーザとしてログインすると、このタブが自動的に表示されます。
3. [ユーザとアクセスの管理]サブタブを選択し、次に左側のペインにある[パスワード ポリシー]ボタンをクリックします。

   [パスワード ポリシー]パネルが表示されます。
4. パスワードをユーザ名と同じにできるかどうかを指定します。
5. パスワード長を制限するかどうかを指定します。
6. 文字の最大繰り返し回数、または最小文字数、または数字に関するポリシーを適用するかどうかを指定します。
7. ポリシーの有効期限と再利用するかどうかを指定します。
8. 設定を確認してから、[保存]をクリックします。
9. [閉じる]をクリックします。

   設定されたパスワード ポリシーは、すべての CA Enterprise Log Manager ユーザに適用されます。

詳細情報:

パスワード ポリシーの計画 (P. 45)
パスワードとしてのユーザ名 (P. 46)
パスワードの有効期限と再利用 (P. 46)
パスワードの長さと形式 (P. 47)

事前定義済みのアクセス ポリシーの保存

事前定義済みのアプリケーション ユーザ グループやロールと関連する事前定義済みのポリシーだけを使用する場合は、事前定義済みポリシーが削除されたり破損したりするリスクはほとんどないでしょう。ただし、管理者がユーザ定義のロールや関連するアクセス ポリシーを作成する予定の場合には、事前定義済みポリシーを開いたり編集したりすることで、意図せず変更されることがあります。必要に応じて復元できるように、元の事前定義済みポリシーのバックアップを保持することをお勧めします。

エクスポート機能を使用して、各タイプの事前定義済みポリシーを含むバックアップ ファイルを作成します。これらのファイルを外部メディアにコピーしたり、エクスポートを起動したサーバのディスクに残しておくことができます。

注: 事前定義済みポリシーのバックアップの手順については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

最初の管理者の作成

最初に作成するユーザには Administrator ロールを割り当てる必要があります。Administrator ロールを割り当てたユーザだけが設定を実行できます。Administrator ロールは、作成した新しいユーザ アカウント、または CA Enterprise Log Manager に取得された既存のユーザ アカウントに割り当てることができます。

次の手順に従います。

1. デフォルトの EiamAdmin ユーザとして CA Enterprise Log Manager サーバにログインします。
2. 最初の管理者を作成します。

   CA Enterprise Log Manager の最初の管理者を作成するために使用する方法は、ユーザ ストアを設定する方法によって決まります。

   - 内部ユーザ ストアを使用するように CA Enterprise Log Manager を設定した場合は、Administrator ロールを使用して新しいユーザ アカウントを作成します。
   - 外部ユーザ ストアを使用するように CA Enterprise Log Manager を設定した場合は、既存の LDAP ユーザを使用してディレクトリにバインドします。外部ディレクトリにバインドしたら、外部ユーザ ストアから CA Enterprise Log Manager のロールを割り当てるユーザ アカウントを取得します。外部ユーザ ストアのユーザ アカウントはグローバル ユーザとして取得されます。 既存のユーザ アカウント情報は変更できませんが、新しい CAELM アプリケーション ユーザ グループやロールを追加できます。最初のユーザに Administrator ロールを割り当てます。

   注: 外部ユーザ ストアを設定した場合は、CA Enterprise Log Manager から新規ユーザを作成することができません。
3. CA Enterprise Log Manager サーバからログオフします。
4. 新しいユーザ アカウントの認証情報を使用して、CA Enterprise Log Manager サーバにもう一度ログインします。

   これで設定タスクを実行する準備が整います。

新規ユーザ アカウントの作成

CA Enterprise Log Manager を使用する予定の各個人にユーザ アカウントを作成できます。ユーザが初めてログオンするときに使用する認証情報を提供し、そのロールを指定します。事前定義済みの 3 つのロールには、Administrator、Analyst、および Auditor があります。Analyst ロールまたは Auditor ロールが割り当てられた新規ユーザがログオンすると、CA Enterprise Log Manager は保存された認証情報を使用してユーザを認証し、割り当てられたロールに基づいてさまざまな機能の使用を許可します。

新規ユーザを作成する方法

1. デフォルトの EiamAdmin ユーザとして CA Enterprise Log Manager サーバにログインします。

   [管理]タブと[ユーザとアクセスの管理]サブタブが表示されます。

2. 左側のペインで[ユーザ]をクリックします。
3. [ユーザ]フォルダの左側の[新規ユーザ]をクリックします。

   [新規ユーザ]の詳細画面がウィンドウの右側に表示されます。

4. [名前]フィールドにユーザ名を入力します。ユーザ名では大文字と小文字が区別されません。
5. [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。
6. このユーザが実行するタスクに関連するロールを選択します。シャトル コントロールを使用して、そのロールを[選択されたユーザ グループ]リストに移動します。
7. 必要に応じて、画面の残りのフィールドに値を入力します。[認証]グループ ボックスには、確認のためにパスワードを入力する必要があります(大文字と小文字が区別されます)。
8. [保存]をクリックして[閉じる]をクリックします。

詳細情報:

グローバル ユーザへのロールの割り当て (P. 146)

グローバル ユーザへのロールの割り当て

既存ユーザ アカウントを検索し、対象のユーザが実行するロールのアプリケーション ユーザ グループを割り当てることができます。外部ユーザ ストアを参照する場合は、検索によってそのユーザ ストアからロードされたグローバル レコードが返されます。設定したユーザ ストアが CA Enterprise Log Manager ユーザ ストアである場合は、検索によって CA Enterprise Log Manager 内のユーザ用に作成されたレコードが返されます。

ユーザ アカウントを編集できるのは、Administrator だけです。

ロール(アプリケーション ユーザ グループ)を既存ユーザに割り当てる方法

1. [管理]タブをクリックし、[ユーザとアクセスの管理]サブタブをクリックします。
2. 左側ペインの[ユーザ]をクリックします。

   [ユーザの検索]ペインおよび[ユーザ]ペインが表示されます。
3. [グローバル ユーザ]を選択し、検索条件を入力して、[実行]をクリックします。

   ロードされたユーザ アカウントの検索の場合、[ユーザ]ペインにはパスが表示され、パス ラベルには参照された外部ディレクトリが反映されます。

   重要: 外部ユーザ ストア内にあるすべてのエントリが表示されるのを避けるには、検索のたびに条件を入力してください。
4. CA Enterprise Log Manager アプリケーション グループのメンバシップを持っていないグローバル ユーザを選択します。

   [ユーザ]ペインに、フォルダ名およびグローバル ユーザの詳細と、該当する場合はグローバル グループ メンバシップが表示されます。
5. [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。

   「CAELM」ユーザの詳細ペインが展開されます。
6. [使用可能なユーザ グループ]から目的のグループを選択し、右方向矢印をクリックします。

   選択したグループが、[選択されたユーザ グループ]ボックスに表示されます。
7. [保存]をクリックします。

8. 追加を確認します。
   a. [ユーザの検索]ペインで、[アプリケーション ユーザの詳細]をクリックし、[実行]をクリックします。
   b. 表示された結果に、新規アプリケーション ユーザの名前が表示されていることを確認します。
9. [閉じる]をクリックします。

第 5 章: サービスの設定

このセクションには、以下のトピックが含まれています。

イベント ソースと設定

ほとんどのネットワークには Windows デバイスと syslog ベースのデバイスがあり、これらのイベント ログを収集、保存、監視、および監査する必要があります。また、ネットワークには、アプリケーション、データベース、バッジ読み取り装置、バイオメトリック装置、または既存の CA Audit レコーダや iRecorder など、他のデバイス タイプがある場合もあります。CA Enterprise Log Manager サービス、アダプタ、エージェント、およびコネクタは、これらのイベント ソースに接続してイベント データを受信できるように、必要な設定がなされています。

CA Enterprise Log Manager サービスには次の設定領域と設定が含まれます。

- グローバル設定
- グローバル フィルタおよび設定
- アラート サービス
- 相関サービス
- イベント ログ ストアの設定

- インシデント サービス
- ODBC サーバの設定
- レポート サーバの設定
- ルール テスト サービス
- サブスクリプション サービスの設定
- システム ステータス アクセス パネル

サービスの設定はグローバルに行うことができます。これは、管理サーバの単一のアプリケーション インスタンス名の下にインストールされたすべての CA Enterprise Log Manager サーバに、この設定が影響することを意味します。選択されたサーバだけに影響するように、設定をローカルにすることもできます。設定は、収集用 CA Enterprise Log Manager サーバのローカル コピーを使用して管理サーバに保存されます。ネットワークの接続が失われたり、管理サーバが何らかの理由でダウンした場合は、この方法で、イベントのログ記録は収集サーバ上で中断することなく続行されます。

システム ステータス アクセス パネルは、CA Enterprise Log Manager サーバおよびそのサービスに影響し、またサポートに必要な情報を収集するツールを提供します。この領域に関する詳細は、「管理ガイド」およびオンライン ヘルプで説明しています。

グローバル設定の編集

すべてのサービスのグローバル設定を設定できます。有効範囲外の値を保存しようとすると、CA Enterprise Log Manager によって、デフォルトの最小値または最大値のどちらか適切なほうに設定されます。設定の一部は相互に依存しています。

グローバル設定の編集方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。

   [サービス リスト]が表示されます。

2. [サービス リスト]内の[グローバル設定]をクリックします。

   [グローバル サービス設定]詳細ペインが開きます。

3. 以下の設定項目のうち、必要なものを変更します。

更新間隔

サーバ コンポーネントが設定の更新を適用する間隔を秒単位で指定します。

最小: 30

最大: 86400

セッション タイムアウト

非アクティブ セッションの最大長を指定します。自動リフレッシュが有効に設定されている場合は、セッションはタイムアウトになりません。

最小: 10

最大: 600

自動リフレッシュを許可

レポートまたはクエリを自動リフレッシュできるようにします。この設定により、管理者は自動リフレッシュをグローバルに無効にすることができます。

自動リフレッシュ間隔

レポート表示がリフレッシュされる間隔を秒単位で指定します。この設定は、[自動リフレッシュを許可]の選択に依存します。

最小: 1

最大: 60

自動リフレッシュの有効化

すべてのセッションで自動リフレッシュを設定します。自動リフレッシュはデフォルトでは有効になっていません。

アクション アラートの参照には認証が必要

監査者またはサードパーティ製品にアクション アラート RSS フィードを表示しないようにします。この設定は、デフォルトでは有効になっています。

デフォルトのレポート

デフォルトのレポートを指定します。

デフォルトのレポートの起動を有効化

[レポート]サブタブをクリックしたときにデフォルトのレポートを表示します。この設定は、デフォルトでは有効になっています。

4. 以下のレポートまたはクエリ タグ設定のうち、必要なものを変更します。

   レポート タグを隠す

   指定されたタグが任意のタグ リストに表示されないようにします。レポート タグを非表示にすると、使用可能なレポートのビューを単純化できます。

   クエリ タグを隠す

   選択されたタグを非表示にします。非表示にされたタグは、メインのクエリ リストまたはアクション アラートのスケジュールのクエリ リストには表示されません。クエリ タグを非表示にすることにより、使用可能なクエリのビューをカスタマイズできます。

5. 以下のダッシュボード設定項目のうち、必要なものを変更します。

   デフォルト ダッシュボードの起動を有効化

   [クエリおよびレポート]タブをクリックしたときに、デフォルトのレポートを表示します。この設定は、デフォルトでは有効になっています。

   デフォルト ダッシュボード

6. 以下のプロファイル設定のうち、必要なものを変更します。

   デフォルト プロファイルの有効化

   デフォルト プロファイルを設定します。

   デフォルト プロファイル

   デフォルト プロファイルを指定します。

   プロファイルを隠す

   選択されたプロファイルを非表示にします。インターフェースがリフレッシュされるか更新間隔が期限切れになると、非表示のプロファイルは表示されなくなります。プロファイルを非表示にすることにより、使用可能なプロファイルのビューをカスタマイズできます。

   注: [リセット]をクリックすると、最後に保存した値に戻すことができます。変更を保存するまで、1 回の変更でも複数の変更でもリセットすることができます。変更を保存したら、変更を個々にリセットします。

7. [保存]をクリックします。

グローバル フィルタおよび設定の操作

CA Enterprise Log Manager サーバの設定の一部として、グローバル フィルタの設定を行うことができます。 グローバル設定は現在のセッションのみで保存され、[デフォルトとして使用]オプションを選択しない限り、ユーザがサーバからログオフするとこの設定は残りません。

グローバルなクイック フィルタでは、最初のレポートを実行する時間間隔を制御し、一致するテキストのシンプルなフィルタリングを実行し、特定のフィールドとその値を使用してレポートに表示するデータに反映できます。

グローバルな詳細フィルタを使用すると、SQL 構文や演算子を使用してレポートデータの対象範囲をさらに広げることができます。グローバル設定を使用すると、タイム ゾーンを設定したり、連携内の他の CA Enterprise Log Manager サーバからデータを取得したりできるほか、表示中にレポートを自動的にリフレッシュする専用のクエリを使用できます。

複数のレポート領域で使用しても機能するグローバル フィルタを設定する必要があります。グローバル フィルタを絞り込むオプションを設定すると、レポートに表示するデータの量を制御できます。グローバル フィルタおよび設定の最初のタスクには、以下のような内容が含まれます。

- CA Enterprise Log Manager サーバから表示するレポートに影響を与える開始時間を提供するグローバル クイック フィルタの設定
- [設定]タブで連携クエリを選択し、このサーバの下で連携している CA Enterprise Log Manager サーバからのデータを表示する
- レポートを自動的にリフレッシュするかどうかを決定する
- レポートのデータをリフレッシュする間隔を設定する

注: グローバル フィルタの設定を絞りすぎたり、厳密にしすぎたりすると、一部のレポートではデータが表示されなくなる場合があります。

グローバル フィルタとその使用法の詳細については、オンライン ヘルプで説明しています。

連携クエリの使用の選択

連携されたデータにクエリを実行するかどうか選択できます。連携されたネットワークで複数の CA Enterprise Log Manager サーバを使用する予定である場合は、[連携クエリの使用]チェック ボックスをオンにすることもできます。このオプションを使用すると、この CA Enterprise Log Manager サーバに連携された(子として動作する)すべての CA Enterprise Log Manager サーバから、レポート用のイベント データを収集できます。

また、現在の CA Enterprise Log Manager サーバのみからのデータを表示する場合は、特定のクエリに対して連携クエリをオフにするよう選択できます。

連携クエリの使用を設定する方法

1. CA Enterprise Log Manager サーバにログインします。
2. [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。

   このボタンは、現在の CA Enterprise Log Manager サーバ名の右側にあるメイン タブの真上にあります。
3. [設定]タブをクリックします。
4. 連携クエリを使用するかどうか選択します。

   連携クエリ オプションの選択をオフにすると、表示するレポートにはこのサーバの子として設定されたサーバからのイベント データが含まれません。

詳細情報:

CA Enterprise Log Manager の連携の設定 (P. 229)
子サーバとしての CA Enterprise Log Manager サーバの設定 (P. 229)

グローバル更新間隔の設定

CA Enterprise Log Manager サービスが設定の変更をチェックする間隔を設定できます。インストール直後のデフォルト値は 5 分で、秒単位で表されます。この値にあまり長い間隔を設定すると、アプリケーションで必要な設定変更が遅れる場合があります。

更新間隔を設定する方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブをクリックします。
2. [サービス]タブをクリックして、[グローバル設定]サービス ノードをクリックします。
3. 更新間隔の新しい値を入力します。

   デフォルト値および推奨値は 300 秒です。

イベント ログ ストアの設定

イベント ログ ストアは基礎となる専用のデータベースで、収集されたイベントログを含みます。イベント ログ ストア サービス用に設定するオプションは、グローバルまたはローカルとして設定でき、CA Enterprise Log Manager サーバのストレージやにイベントのアーカイブに影響します。イベント ログ ストアを設定する処理には、次のような作業が含まれます。

- イベント ログ ストア サービスの理解
- イベント ログ ストアがアーカイブ ファイルを処理する方法の理解
- イベント ログ ストアの設定(グローバルまたはローカルの値)

  これには、データベース サイズ、基本的なアーカイブ ファイルの保持値、集約ルール、抑制ルール、連携関係、相関設定、データ整合性チェック、自動アーカイブ オプションの設定が含まれます。

アクティブなデータベースがこのサービス用に定義された容量に達した場合、CA Enterprise Log Manager は自動的にアクティブなデータベース ファイルを閉じて、アーカイブ ファイルを作成します。その後、CA Enterprise Log Manager は新しくアクティブになったファイルを開き、イベントのログ記録処理を続行します。このようなファイルを処理するために自動アーカイブ オプションを設定できますが、各 CA Enterprise Log Manager サーバのローカル設定としてのみ設定できます。

イベント ログ ストア サービスについて

イベント ログ ストア サービスは次のようなデータベース操作を処理します。

- 新しいイベントを現在の(ホット)データベースに挿入する
- クエリおよびレポートで使用するために、ローカルおよびリモートの連携データベースからイベントを取得する
- 現在のデータベースが満杯になった場合に新しいデータベースを作成する
- 新しいアーカイブ ファイルを作成し、古いアーカイブ ファイルを削除する
- アーカイブ クエリ キャッシュを管理する
- 選択した要約ルールおよび抑制ルールを適用する
- 選択したイベント転送ルールを適用する
- この CA Enterprise Log Manager サーバの連携の子として動作する CA Enterprise Log Manager サーバを定義する

アーカイブ ファイルについて

ホット データベースがイベント ログ ストア サービスに指定した[最大行数]の設定に到達した場合、CA Enterprise Log Manager サーバは、アーカイブ ファイルと呼ばれるウォーム データベース ファイルを自動的に作成します。ホット データベース ファイルは圧縮されません。

収集サーバからレポート サーバへの自動アーカイブを設定すると、データベースがレポート サーバにコピーされた後に、収集サーバのウォーム データベースが削除されます。 [アーカイブの最大日数]はここでは適用されません。

レポート サーバからリモートのストレージ サーバへの自動アーカイブを設定すると、レポート サーバのウォーム データベースはリモートのストレージ サーバにコピーされた後に削除されません。もっと正確に言えば、[アーカイブの最大日数]の値に達するまで、ウォーム データベースはレポート サーバ上で保持されます。 その後、ウォーム データベースが削除されます。ただし、削除されたコールド データベースのレコードは保持されるため、復元するためにこの情報が必要な場合は、アーカイブ データベース対して詳細に関するクエリを実行できます。

[アーカイブの最大日数]の設定方法を決める場合は、レポート サーバ上の使用可能なディスク容量を考慮します。[アーカイブ ディスク領域]にはしきい値を設定します。使用可能なディスク容量が設定された割合を下回った場合、そのデータの[アーカイブの最大日数]が経過していない場合でも、より多くの領域を確保するためにイベント ログ データが削除されます。

レポート サーバからリモートのストレージ サーバへの自動アーカイブを設定しない場合、手動でウォーム データベースをバックアップし、そのコピーを[アーカイブの最大日数]に設定された日数よりも多い頻度でリモートの保存場所に手動で移動する必要があります。 これを行わないと、データが失われる恐れがあります。アーカイブ ファイルを毎日バックアップして潜在的なデータ損失を回避し、適切なディスク容量を維持することをお勧めします。 イベント ログ ストア サービスはアーカイブされたデータベースでクエリを実行するための独自の内部キャッシュを管理し、繰り返されるクエリや非常に広範囲のクエリを実行する場合のパフォーマンスを改善します。

アーカイブ ファイルの操作に関する詳細は、「CA Enterprise Log Manager 管理ガイド」で説明しています。

詳細情報:

例: 3 つのサーバ間の自動アーカイブ (P. 171)

自動アーカイブについて

保存されたイベント ログの管理では、ファイルのバックアップと復元を慎重に処理する必要があります。イベント ログ ストア サービスの設定は、内部データベースのサイズの設定と調整、保持、および自動アーカイブ オプションを設定するための中心となる場所を提供します。CA Enterprise Log Manager では、これらのタスクに役立つ次のようなスクリプトを提供しています。

- backup-ca-elm.sh
- restore-ca-elm.sh
- monitor-backup-ca-elm.sh

注: これらのスクリプトを使用する場合は、2 つのサーバ間に RSA キーを使用した非対話型の認証が確立されていることを前提とします。

バックアップと復元のスクリプトでは、リモート ホストとのウォーム データベースのコピーを簡単にするために、LMArchive ユーティリティを使用します。タスクが完了すると、スクリプトは自動的に適切なカタログ ファイルを更新します。リモート サーバ、または他の CA Enterprise Log Manager サーバにコピーできます。ファイルを送信するリモート ホストが CA Enterprise Log Manager サーバである場合、このスクリプトによって受信サーバのカタログ ファイルも自動的に更新されます。また、連携レポートでの重複を避けるために、スクリプトによってローカル マシンからアーカイブ ファイルが削除されます。これによって、クエリやレポートでデータを使用できます。システムから離れた場所にあるストレージは、コールド ストレージと呼ばれます。コールド ストレージに移動されたファイルを、クエリやレポート用に復元できます。

監視スクリプトは、イベント ログ ストア サービス設定の自動アーカイブに関する設定を使用して、自動的にバックアップ スクリプトを実行します。

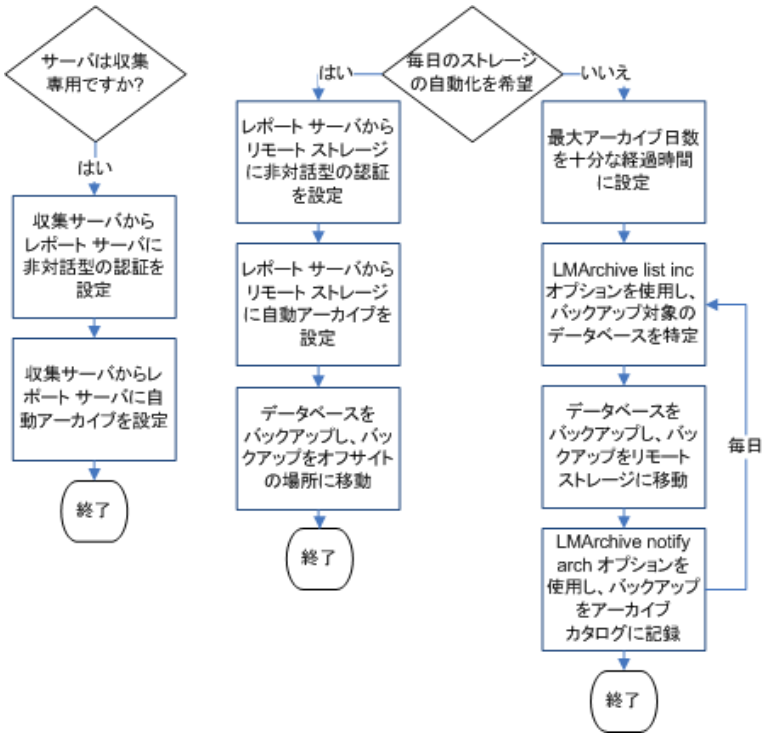
詳細情報:

例: 3 つのサーバ間の自動アーカイブ (P. 171)

データベース移動およびバックアップ戦略のフローチャート

各 CA Enterprise Log Manager サーバ上でイベント収集およびレポーティングの両方を実行するか、収集とレポーティングにそれぞれ別のサーバを割り当てることができます。収集用にサーバを割り当てる場合、収集サーバからレポート サーバに 1 時間ごとにデータが自動的に移動するよう設定する必要があります。専用のサーバ ロールがない場合は、「レポートからリモート ストレージ」の箇所を「専用でない CA Enterprise Log Manager サーバからリモート ストレージ」と読み換えます。

バックアップ戦略とは、各データベースのコピーを 2 つ持つことで、1 つがバックアップであると見なされます。この場合、リモート ストレージ サーバへの自動アーカイブは設定してもしなくてもかまいません。自動アーカイブが設定されたバックアップ戦略では、元のデータベースがリモート ストレージ サーバ上、バックアップがオフサイトのロケーション上に存在することになります。自動アーカイブが設定されていないバックアップ戦略では、元のデータベースが CA Enterprise Log Manager サーバ上、バックアップがリモート ストレージ サーバ上に存在することになります。元のデータベースを最初にアーカイブされた CA Enterprise Log Manager に格納できるかどうかは、長期保管用の空き容量およびストレージ ポリシーによって決まります。これらの条件が満たされている場合は、個人の裁量によって決まります。



自動アーカイブ用の非対話型認証の設定

異なるロールを持つサーバ間で、自動アーカイブを設定できます。以下に例を示します。

- 1 つ以上の収集サーバから 1 つのレポート サーバへ。
- 1 つ以上のレポート サーバから 1 つのリモート ストレージ サーバへ。

あるサーバから別のサーバへの自動アーカイブを設定する前に、1 つのソース サーバから宛先サーバに対して非対話型の ssh 認証を設定する必要があります。非対話型とは、1 つのサーバがパスワードを使用せずに別のサーバにファイルを移動できることを意味します。

- 収集サーバ、レポート サーバ、およびリモート ストレージ サーバの 3 つのサーバしか使用しない場合は、非対話型認証を以下のとおり 2 回設定します。
  - 収集サーバからレポート サーバへ。
  - レポート サーバからリモート ストレージ サーバへ。
- 4 つの収集サーバ、1 つのレポート サーバ、1 つのリモート ストレージ サーバの 6 つのサーバを使用する場合、非対話型の認証を以下のとおり 5 回設定します。
  - 収集サーバ 1 からレポート サーバへ。
  - 収集サーバ 2 からレポート サーバへ。
  - 収集サーバ 3 からレポート サーバへ。
  - 収集サーバ 4 からレポート サーバへ。
  - レポート サーバからリモート ストレージ サーバへ。

2 つのサーバ間で非対話型 ssh 認証を設定するには、RSA 鍵のペア、秘密鍵、および公開鍵を使用します。生成した最初の公開鍵は、authorized_keys として宛先サーバにコピーします。非対話型認証の複数のインスタンスを同じ宛先レポート サーバに設定する場合、元の authorized_keys が上書きされないようにするため、ほかの公開鍵にそれぞれ一意のファイル名を使用してコピーします。その後、これらのファイルを authorized_keys にまとめます。たとえば、authorized_keys_ELM-C2 および authorized_keys_ELM-C3 を ELM-C1 からの authorized_keys ファイルに追加します。

例: ハブとスポーク用の非対話型認証の設定

2 つのサーバ間で非対話型認証を使用することは、ソース サーバから宛先サーバへの自動アーカイブを行うための前提条件です。非対話型認証を設定するための一般的なシナリオとして、収集に割り当てられた複数のソース サーバが、レポーティング/管理に割り当てられている共通の宛先サーバにアクセスする場合があります。この例では、1 つのレポート/管理サーバ(ハブ)、4 つの収集サーバ(スポーク)、1 つのリモート ストレージ サーバから成る中規模の CA Enterprise Log Manager 連携を使用します。各サーバ ロール内のサーバの名前は以下のとおりです。

- CA Enterprise Log Manager レポート/管理サーバ: ELM-RPT
- CA Enterprise Log Manager 収集サーバ: ELM-C1、ELM-C2、ELM-C3、ELM-C4
- リモート ストレージ サーバ: RSS

CA Enterprise Log Manager 連携のために非対話型認証を有効にするには、以下の手順に従います。

1. 最初の収集サーバから、caelmservice として RSA 鍵のペアを生成し、公開鍵を authorized_keys として宛先レポート サーバ上の /tmp ディレクトリにコピーします。
2. 追加の収集サーバごとに、RSA 鍵のペアを生成し、公開鍵を authorized_keys_n としてコピーします。n によってソースを一意に識別できるようにします。
3. レポート サーバ上の /tmp ディレクトリで、これらの公開鍵の中身を元の authorized_keys に追加してまとめます。.ssh ディレクトリを作成し、ディレクトリの所有権を caelmservice に変更します。authorized_keys を .ssh ディレクトリに移動し、鍵ファイルの所有権および必要な権限を設定します。
4. 各収集サーバとレポート サーバとの間で非対話型認証が存在することを確認します。
5. リモート ストレージ サーバで、.ssh ディレクトリ用のディレクトリ構造を作成します(デフォルトは /opt/CA/LogManager)。宛先サーバ上で .ssh ディレクトリを作成し、所有権を caelmservice に変更します。
6. レポート サーバで、RSA 鍵のペアを caelmservice として生成し、公開鍵を authorized_keys として宛先リモート ストレージ サーバ上の /tmp ディレクトリにコピーします。

7. リモート ストレージ サーバで、authorized_keys を /tmp から .ssh ディレクトリに移動し、鍵ファイルの所有権を caelmservice に設定して必要な権限を付与します。
8. レポート サーバとリモート ストレージ サーバとの間に非対話型認証が存在することを確認します。

最初の収集/レポート ペア用の鍵の設定

ハブとスポークのアーキテクチャ用に非対話型認証を設定するための最初の手順は、収集サーバ上で RSA 公開鍵/秘密鍵ペアを生成し、公開鍵を宛先レポート サーバにコピーすることです。公開鍵は authorized_keys という名前でコピーします。この鍵は、指定されたレポート サーバにコピーされた最初の公開鍵であると仮定します。

最初の収集サーバで RSA 鍵のペアを生成し、公開鍵をレポート サーバにコピーする方法

1. ssh を使用して caelmadmin ユーザとして ELM-C1 にログインします。
2. ユーザを root に切り替えます。

   ```
   su –
   ```

3. ユーザを caelmservice アカウントに切り替えます。

   ```
   su – caelmservice
   ```

4. RSA 鍵のペアを生成します。

   ```
   ssh-keygen –t rsa
   ```

5. 以下のプロンプトが表示されるたびに、Enter キーを押してデフォルトを使用します。
   - 鍵を保存するファイルを入力します（/opt/CA/LogManager/.ssh/id_rsa）。
   - パスフレーズを入力します（パスフレーズを使用しない場合は空にします）。
   - 同じパスフレーズを再度入力します。
6. ディレクトリを /opt/CA/LogManager に変更します。
7. 次のコマンドを使用して、.ssh ディレクトリの権限を変更します。

   ```
   chmod 755 .ssh
   ```

8. id_rsa.pub 鍵が保存されている .ssh に移動します。

   ```
   cd .ssh
   ```

9. 以下のコマンドを使用して、id_rsa.pub ファイルを宛先の CA Enterprise Log Manager サーバにコピーします。

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
   ```

   これにより、レポート サーバ上に authorized_keys ファイルが作成され、公開鍵のコンテンツが含まれます。

追加の収集/レポート ペア用の鍵の設定

ハブとスポークのアーキテクチャ用に非対話型認証を設定するための 2 番目の手順は、追加の収集サーバごとに RSA 鍵のペアを生成し、共通のレポート サーバの /tmp ディレクトリに authorized_keys_n としてコピーすることです。n によってソースの収集サーバが一意に識別できるようにします。

追加の収集サーバ上で RSA 鍵のペアを生成し、公開鍵を共通レポート サーバにコピーする方法

1. 2 つ目の収集サーバ ELM-C2 に、ssh を使用して caelmadmin としてログインします。
2. ユーザを root に切り替えます。
3. ユーザを caelmservice アカウントに切り替えます。

   ```
   su – caelmservice
   ```

4. RSA 鍵のペアを生成します。

   ```
   ssh-keygen –t rsa
   ```

5. 以下のプロンプトが表示されるたびに、Enter キーを押してデフォルトを使用します。
   - 鍵を保存するファイルを入力します（/opt/CA/LogManager/.ssh/id_rsa）。
   - パスフレーズを入力します（パスフレーズを使用しない場合は空にします）。
   - 同じパスフレーズを再度入力します。
6. ディレクトリを /opt/CA/LogManager に変更します。
7. 次のコマンドを使用して、.ssh ディレクトリの権限を変更します。

   ```
   chmod 755 .ssh
   ```

8. id_rsa.pub 鍵が保存されている .ssh に移動します。

9. 以下のコマンドを使用して、id_rsa.pub ファイルを宛先の CA Enterprise Log Manager サーバにコピーします。

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
   ```

   これにより、レポート サーバ上に authorized_keys_ELM-C2 ファイルが作成され、公開鍵のコンテンツが含まれます。

10. 「yes」と入力し、ELM-RPT に対する caelmadmin のパスワードを入力します。
11. 「exit」と入力します。
12. 収集サーバ ELM-C3 に対して手順 1 から 11 までを繰り返します。手順 9 では、以下を指定します。

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
    ```

13. 収集サーバ ELM-C4 に対して手順 1 から 11 までを繰り返します。手順 9 では、以下を指定します。

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
    ```

レポート サーバでの 1 つの公開鍵ファイルの作成と所有権の設定

シナリオのこれまでの手順では、収集サーバごとに鍵のペアを生成し、公開鍵を以下のファイルとしてレポート サーバにコピーしました。

- authorized_keys
- authorized_keys_ELM-C2
- authorized_keys_ELM-C3
- authorized_keys_ELM-C4

3 つ目の手順として、これらのファイルを連結し、連結された RSA 公開鍵ファイルを適切なディレクトリに移動し、ディレクトリとファイルの所有権を caelmservice に設定します。

連結された公開鍵ファイルをレポート サーバの適切な場所に作成してファイル所有権を設定する方法

1. ssh を使用して、caelmadmin として CA Enterprise Log Manager レポート サーバにログインします。
2. ユーザを root に切り替えます。

3. ディレクトリを CA Enterprise Log Manager フォルダに変更します。

   ```
   cd /opt/CA/LogManager
   ```

4. .ssh フォルダを作成します。

   ```
   mkdir .ssh
   ```

5. 新しいフォルダの所有権を caelmservice ユーザとグループに変更します。

   ```
   chown caelmservice:caelmservice .ssh
   ```

6. ディレクトリを /tmp に変更します。

7. 収集サーバ ELM-C2、ELM-C3、ELM-C4 から、ELM-C1 からの公開鍵を含んでいる authorized_keys ファイルに公開鍵のコンテンツを追加します。

   ```
   cat authorized_keys_ELM-C2 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C3 >> authorized_keys
   ```

   ```
   cat authorized_keys_ELM-C4 >> authorized_keys
   ```

8. ディレクトリを opt/CA/LogManager/.ssh に変更します。

9. tmp フォルダから現在のフォルダ .ssh に authorized_keys ファイルをコピーします。

   ```
   cp /tmp/authorized_keys
   ```

10. authorized_keys ファイルの所有権を caelmservice アカウントに変更します。

    ```
    chown caelmservice:caelmservice authorized_keys
    ```

11. ファイルの権限を変更します。

    ```
    chmod 755 authorized_keys
    ```

    755 を指定すると、すべてのユーザに読み取りおよび実行の権限が付与され、ファイルの所有者に読み取り、実行、書き込みの権限が付与されます。

これにより、パスワード不要の認証が、収集サーバとレポート サーバの間で設定されました。

収集サーバとレポート サーバ間での非対話型認証の検証

自動アーカイブの両方の段階のソース サーバと宛先サーバ間で使用する非対話型の認証設定を検証できます。

収集サーバとレポート サーバ間の設定を検証する方法

1. ssh を使用して caelmadmin として収集サーバ ELM-C1 にログインします。
2. ユーザを root に切り替えます。
3. ユーザを caelmservice アカウントに切り替えます。

   ```
   su – caelmservice
   ```

4. 以下のコマンドを入力します。

   ```
   ssh caelmservice@ELM-RPT
   ```

   パスフレーズを入力せずに ELM-RPT にログインできたことにより、ELM-C1 と ELM-RPT の間で非対話型認証が存在することが確認されました。
5. ELM-C2 にログインして同じ手順を繰り返します。
6. ELM-C3 にログインして同じ手順を繰り返します。
7. ELM-C4 にログインして同じ手順を繰り返します。

リモート ストレージ サーバ上での所有権を備えたディレクトリ構造の作成

以下の手順では、リモート ストレージ サーバが CA Enterprise Log Manager サーバではないという前提で、新しいユーザ、グループ、およびディレクトリ構造を作成して CA Enterprise Log Manager サーバのユーザ、グループ、ディレクトリ構造をコピーしておく必要があります。これは、レポート サーバから鍵を送信する前に行う必要があります、caelmadmin アカウントを使用してリモート ストレージ サーバへの scp を行うからです。

リモート ストレージ サーバ上でファイル構造を作成してファイル所有権を設定する方法

1. ssh を使用して root としてリモート ストレージ サーバにログインします。
2. caelmadmin という名前の新しいユーザを作成します。
3. caelmservice という名前のグループを作成し、次に、caelmservice という名前の新しいユーザを作成します。

4. リモート ロケーションとして使用するディレクトリを作成します。デフォルトは /opt/CA/LogManager です。

   注: 別のディレクトリを使用する場合、自動アーカイブ用のリモート ロケーションを設定する際にそのディレクトリを指定するようにしてください。

5. caelmservice のホーム ディレクトリを /opt/CA/LogManager または適切なリモート ロケーション ディレクトリに変更します。以下の例ではデフォルトのディレクトリを使用します。

   ```
   usermod -d /opt/CA/LogManager caelmservice
   ```

6. caelmservice のファイル権限を設定します。以下の例ではデフォルトのリモート ロケーション ディレクトリを使用します。

   ```
   chown -R caelmservice:caelmservice /opt/CA/LogManager
   ```

7. ディレクトリを /opt/CA/LogManager または適切なリモート ロケーションに変更します。
8. .ssh フォルダを作成します。
9. .ssh フォルダの所有権を caelmservice ユーザとグループに変更します。

   ```
   chown caelmservice:caelmservice .ssh
   ```

10. リモート ストレージ サーバからログオフします。

レポート/リモート ストレージ ペア用の鍵の設定

各収集サーバからレポート サーバへの非対話型認証の設定および検証したら、レポート サーバからリモート ストレージ サーバへの非対話型認証を設定および検証します。

このシナリオ例の最初の手順として、レポート サーバ ELM-RPT 上で新しい RSA 鍵のペアを生成し、公開鍵を authorized_keys としてリモート ストレージ サーバ RSS の /tmp ディレクトリにコピーします。

レポート サーバ上で RSA 鍵のペアを生成してリモート ストレージ サーバにコピーする方法

1. caelmadmin としてレポート サーバにログインします。
2. ユーザを root に切り替えます。

3. ユーザを caelmservice アカウントに切り替えます。

   ```
   su – caelmservice
   ```

4. 次のコマンドを使用して、RSA 鍵のペアを生成します。

   ```
   ssh-keygen –t rsa
   ```

5. 以下のプロンプトが表示されるたびに、Enter キーを押してデフォルトを使用します。

   - 鍵を保存するファイルを入力します（/opt/CA/LogManager/.ssh/id_rsa）。
   - パスフレーズを入力します（パスフレーズを使用しない場合は空にします）。
   - 同じパスフレーズを再度入力します。

6. ディレクトリを /opt/CA/LogManager に変更します。
7. 次のコマンドを使用して、.ssh ディレクトリの権限を変更します。

   ```
   chmod 755 .ssh
   ```

8. .ssh フォルダに移動します。
9. 以下のコマンドを使用して、id_rsa.pub ファイルを宛先リモート ストレージ サーバの RSS にコピーします。

   ```
   scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
   ```

   これにより、リモート ストレージ サーバ上の /tmp ディレクトリに authorized_keys ファイルが作成され、公開鍵のコンテンツが含まれます。

リモート ストレージ サーバ上での鍵ファイル所有権の設定

レポート サーバで鍵のペアを生成し、公開鍵をリモート ストレージ サーバにコピーしたら、リモート ストレージ サーバで鍵ファイルの所有権と権限を設定できます。

リモート ストレージ サーバの適切な場所に公開鍵ファイルを移動してファイルの所有権を設定する方法

1. caelmadmin としてリモート ストレージ サーバにログインします。
2. ユーザを root に切り替えます。

3. ディレクトリを /opt/CA/LogManager/.ssh に変更します。
4. /tmp ディレクトリからカレント ディレクトリ.ssh に authorized_keys ファイルをコピーします。

   ```
   cp /tmp/authorized_keys
   ```

5. 次のコマンドを使用して、authorized_keys ファイルの所有権を変更します。

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

6. authorized_keys ファイルについて権限を変更します。

   ```
   chmod 755 authorized_keys
   ```

   非対話型認証が、CA Enterprise Log Manager レポート サーバとストレージ用のリモート ホスト間に設定されました。

レポート サーバとストレージ サーバ間での非対話型認証の検証

レポート サーバとリモート ストレージ サーバの間で非対話型認証が設定されていることを確認します。このシナリオ例では、リモート ストレージ サーバに RSS という名前が付いています。

CA Enterprise Log Manager レポート サーバとストレージ サーバ間の非対話型認証を検証する方法

1. レポート サーバに root としてログインします。
2. ユーザを caelmservice に切り替えます。

   ```
   su – caelmservice
   ```

3. 以下のコマンドを入力します。

   ```
   ssh caelmservice@RSS
   ```

   これにより、パスフレーズを入力せずに、リモート ストレージ サーバにログインします。

例: 3 つのサーバ間での非対話型認証の設定

自動アーカイブの前提条件として非対話型認証を設定するための最も単純なシナリオは、2 つの CA Enterprise Log Manager サーバ、1 つの収集サーバ、1 つのレポート/管理サーバ、1 つのリモート ストレージ システム(UNIX または Linux のサーバ上)を使用する場合です。 この例では、以下の 3 つのサーバが自動アーカイブ用に用意されているものとします。

- NY-Collection-ELM
- NY-Reporting-ELM
- NY-Storage-Svr

非対話型認証を有効にするための手順は以下のとおりです。

1. NY-Collection-ELM で、caelmservice として RSA 鍵のペアを生成し、このペアの公開鍵を authorized_keys として NY-Reporting-ELM 上の /tmp ディレクトリにコピーします。
2. NY-Reporting-ELM 上に .ssh ディレクトリを作成し、所有権を caelmservice に変更し、authorized_keys を /tmp ディレクトリから .ssh ディレクトリに移動します。鍵ファイルの所有権を caelmservice に設定し、必要な権限を設定します。
3. NY-Collection-ELM から NY-Reporting-ELM に対して非対話型認証が存在することを検証します。
4. NY-Reporting-ELM で、別の RSA 鍵のペアを caelmservice として生成し、公開鍵を authorized_keys として NY-Storage-Svr の /tmp ディレクトリにコピーします。
5. NY-Storage-Svr で、ディレクトリ構造 /opt/CA/LogManager を作成します。このパスに .ssh ディレクトリを作成し、所有権を caelmservice に変更し、authorized_keys をこのディレクトリに移動します。鍵ファイルの所有権を caelmservice に設定して必要な権限を設定します。
6. NY-Reporting-ELM から NY-Storage-Svr に対して非対話型認証が存在することを検証します。

これらの手順の詳細は、ハブとスポークを使用したシナリオの場合と似ています。3 つのサーバのシナリオの場合は、追加の収集/レポート ペアに対する手順 2 をスキップし、authorized_keys へのファイルの連結に関する手順 3 をスキップします。

例: 3 つのサーバ間の自動アーカイブ

収集 - レポート アーキテクチャを使用している場合、収集サーバからレポート サーバへの自動アーカイブを設定する必要があります。この設定によって、収集および精製済みイベント ログ データのウォーム データベースを、レポートの実行が可能なレポート サーバに自動的に送信できるようになります。この自動アーカイブを、日単位ではなく時間単位で反復されるようスケジュールし、毎日大量のデータの転送に長時間が当てられる事態を回避することをお勧めします。作業の負荷や処理を集中させるか、1 日の間に分散するかに応じてスケジュールを選択します。自動アーカイブによってデータベースが収集サーバからレポート サーバにコピーされると、そのデータベースは収集サーバから削除されます。

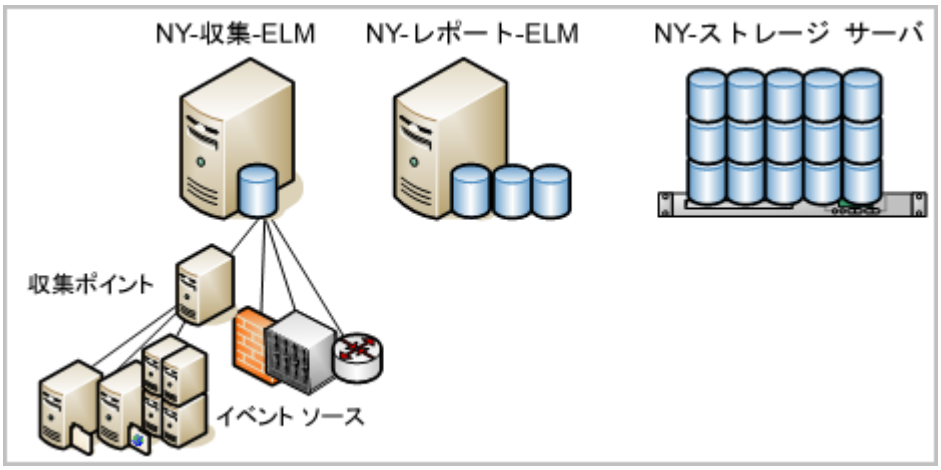
ストレージ領域が豊富なローカル サーバを特定し、その後レポート サーバからこのリモート ストレージ サーバに自動アーカイブを設定することができます。自動アーカイブによってデータベースがレポート サーバからリモート ストレージ サーバにコピーされると、レポート サーバ上のデータベースは、[アーカイブの最大日数]に設定されている期間が経過するまでは削除されません。設定期間が経過した時点で、データベースは削除されます。自動アーカイブのこのフェーズのメリットは、アーカイブ済みデータベースが自動削除の前に長期保存場所に手動で移動されていないために失われてしまうことからデータベースを保護することです。

注: 自動アーカイブされたデータベースを受信するようリモート サーバを設定する前に、ソース CA Enterprise Log Manager サーバなどの宛先サーバ上のディレクトリ構造を設定し、認証のための各種所有権および権限を割り当てる必要があります。詳細については、「実装ガイド」の「非対話型認証の設定」を参照してください。必ず「リモート ホストでの鍵ファイルの所有権の設定」で説明されている手順に従ってください。

このシナリオ例では、ニューヨーク データ センターの CA Enterprise Log Manager 管理者を想定しています。このデータ センターのネットワークは、豊富なストレージ容量を備えた 1 台のリモート サーバと、それぞれが専用のロールを持つ複数の CA Enterprise Log Manager サーバから構成されています。自動アーカイブで使用されるサーバの名前は、以下のとおりです。

- NY- 収集 -ELM
- NY- レポート -ELM
- NY- ストレージ -Svr

注: この例は、サーバの CA Enterprise Log Manager システム管理を専門とする管理サーバが存在していることを想定しています。自動アーカイブでは直接的なロールがないため、このサーバはここでは示していません。



収集サーバからレポート サーバ、その後レポート サーバからリモート ストレージ サーバへの自動アーカイブを設定するには、ガイドとして以下の例を使用します。

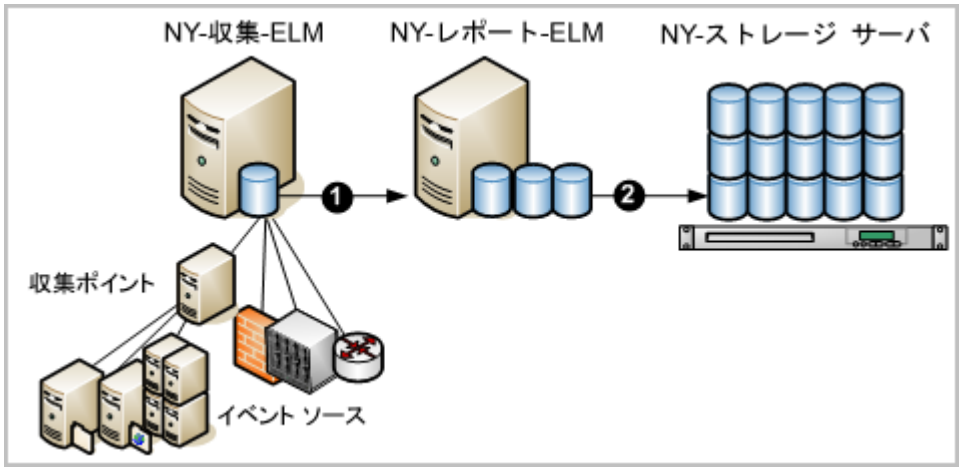
1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
2. [イベント ログ ストア]フォルダを展開し、収集サーバを選択します。

3. 宛先がレポート サーバである場合は、時間単位で反復するよう自動アーカイブを指定します。Administrator ロールを持つ CA Enterprise Log Manager ユーザの認証情報を入力します。カスタム ポリシーを使用する際は、データベース リソースへの編集権限を持つユーザである必要があります。この権限によって、アーカイブされたデータベースを削除することが許可されます。

4. サービス リストからレポート サーバを選択します。

5. 保存用のリモート サーバが宛先の場合は、日単位で反復するよう自動アーカイブを指定します。Administrator ロールを持つユーザ アカウントの認証情報を入力します。必要に応じて、データベース リソースに対する編集アクションを備えた CALM アクセス ポリシーを作成し、[ID]にユーザを割り当てます。ここでは、権限レベルの低いユーザの認証情報を入力します。

以下の図の数字は、自動アーカイブの 2 つの設定を示しています。1 つは、収集サーバからレポート サーバへのもの、もう 1 つは、レポート サーバからネットワーク上のリモート サーバへのものです。

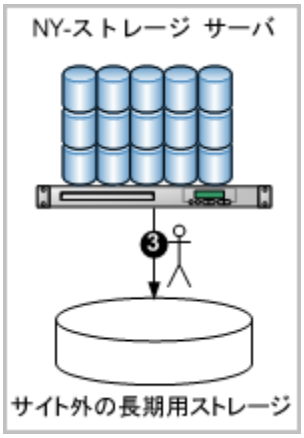


このような設定を行った後、自動処理が以下の要領で実行されます。

1. NY- 収集 -ELM、すなわち収集 CA Enterprise Log Manager サーバによって、イベントが収集および精製され、ホット データベースに挿入されます。設定されたレコード数に達すると、ホット データベースは圧縮されてウォーム データベースになります。自動アーカイブが時間単位で反復するようスケジュールされているため、毎時間、ウォーム データベースがシステムによってコピーされ、NY- レポート -ELM、すなわちレポート CA Enterprise Log Manager サーバに移動されます。移動されると、ウォーム データベースは NY- 収集 -ELM から削除されます。
2. NY- レポート -ELM にはデータベースが保持され、[アーカイブの最大日数] で設定された日数に達するまでクエリを実行できます。設定日数が経過すると削除されます。自動アーカイブが日単位で反復するようスケジュールされているため、毎日、ウォーム データベースがシステムによってコピーされ、NY- ストレージ -Svr にコールド データベースとして移動されます。コールド データベースは、長期間リモート ストレージ サーバに保持される場合があります。

3. ネットワークの NY- ストレージ -Svr 上に保存されたコールド データベースを、義務付けられた年数保持が可能なオフサイトの長期保存ソリューションに移動させます。

   アーカイブの目的は、復元の際に使用できるよう、イベント ログを保存することです。ログに記録された古いイベントを調査する必要性が生じた場合は、コールド データベースを復元できます。オンサイトのストレージ サーバからオフサイトの長期保存場所にアーカイブ済みデータベースを手動で移動する手順を、以下の図に示します。

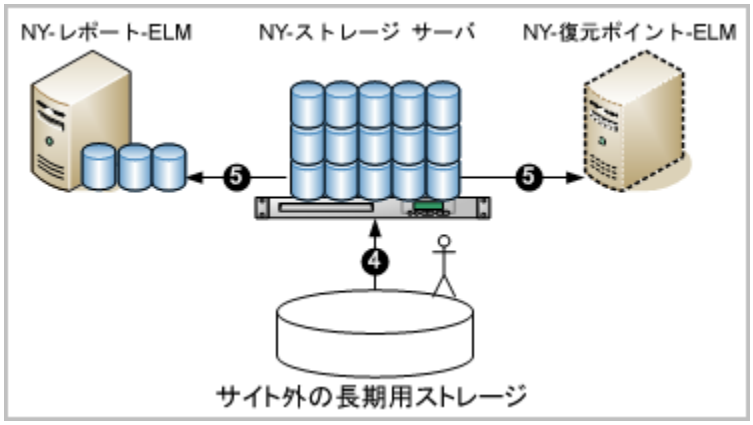


4. バックアップされ、オフサイトに移動されたログの検査が必要な状況が発生したと仮定します。復元するアーカイブ済みデータベースの名前を特定するために、NY- レポート -ELM 上のローカル アーカイブ カタログを検索します ([管理]タブをクリックし、[ログ収集エクスプローラ]から[カタログ クエリのアーカイブ]を選択し、[クエリ]をクリックします)。

5. オフサイトのストレージから、特定したアーカイブ済みデータベースを取得します。NY- ストレージ -Svr 上の元の /opt/CA/LogManager/data/archive ディレクトリにコピーします。次に、アーカイブ ディレクトリの所有権を caelmservice ユーザに変更します。

6. データベースを元のレポート サーバか、復元されたデータベースからのログの調査に使用する専用の復元ポイントのどちらかに、以下の要領で復元します。

   - NY- レポート -ELM に復元する場合は、リモート ホストに NY- ストレージ -Svr を指定して、NY- レポート -ELM から restore-ca-elm.sh スクリプトを実行します。
   - NY- 復元ポイント -ELM に復元する場合は、リモート ホストに NY- ストレージ -Svr を指定して、NY- 復元ポイント -ELM から restore-ca-elm.sh スクリプトを実行します。



注: これで、復元されたデータにクエリおよびレポートを実行できます。

詳細情報:

自動アーカイブについて (P. 157)
アーカイブ ファイルについて (P. 156)
基本的な環境でのイベント ログ ストアの設定 (P. 176)
例: 大企業向けの連携マップ (P. 37)

基本的な環境でのイベント ログ ストアの設定

収集サーバとレポート サーバのロールを個別の CA Enterprise Log Manager サーバで実行する環境では、イベント ログ ストアをローカルの設定として個別に設定する必要があります。 また、レポート サーバを使用してフェイルオーバー トラフィックを処理するように選択した場合、テーブルに表示される数よりも[最大行数]フィールドの値を増やすと便利な場合があります。管理サーバをレポート サーバとして使用する場合は、管理サーバで一部のイベント情報を自己監視イベントとして生成することを検討します。

注: 自動アーカイブの設定を正常に動作させるには、非対話型認証の自動アーカイブに参加する各ペアのサーバを設定する必要があります。

以下の表は、ある基本的な設定を示す例です。収集用 CA Enterprise Log Manager サーバは CollSrvr-1 という名前です。レポート用 CA Enterprise Log Manager サーバは、RptSrvr-1 という名前です。この例では、コールド データベース ファイルを保存する RemoteStore-1 という名前のリモート ストレージ サーバが存在し、そのコールド ファイルは /CA-ELM_cold_storage ディレクトリに配置されています。

イベント ログ ストア フィールド	[収集サーバ] の値	[レポート サーバ]の値
最大行数	2000000（デフォルト）	自動アーカイブには適用できない。
最大アーカイブ日数	1（自動アーカイブには適用できない）	30（自動アーカイブに適用可能。自動アーカイブが設定されていない場合）
アーカイブ ディスク領域	10	10
ポリシーのエクスポート	24	72
セキュリティで保護されたサービス ポート	17001	17001
自動アーカイブ オプション		
有効	Yes	Yes
バックアップ タイプ	増分	増分
間隔	毎時間	毎日
開始時間	0	23
EEM ユーザ	<CA Enterprise Log Manager_Administrator>	<CA Enterprise Log Manager_Administrator>
EEM パスワード	*<password>*	*<password>*
リモート サーバ	RptSrvr-1	RemoteStore-1
リモート ユーザ	caelmservice	user_X
リモート ロケーション	/opt/CA/LogManager	/CA-ELM_cold_storage
リモート CA-ELM サーバ	Yes	No

この例の自動アーカイブ オプションは、収集サーバのアーカイブ ファイル（ウォーム データベース ファイル）を 1 時間おきにレポート サーバに移動します。これによって、受信イベントに使用可能なディスク空き容量を確保します。どちらのサーバも、増分バックアップを使用するため、一度に大量のデータを移動する必要はありません。ウォーム データベースがレポート サーバに移動されると、収集サーバから自動的に削除されます。

注: バックアップの[間隔]が[時間単位]に設定されている場合、[開始時間]の値に 0 を設定しても影響はありません。

[EEM ユーザ]と[EEM パスワード]については、事前定義済みの Administrator ロールを割り当てた CA Enterprise Log Manager ユーザ、またはデータベース リソースのアクションを編集する実行権限を付与するカスタム ポリシーに関連付けられたカスタム ロールを割り当てた CA Enterprise Log Manager ユーザの認証情報を指定します。

レポート サーバからリモート ストレージ サーバへの自動アーカイブを行う場合、レポート サーバには、[リモート ロケーション]に /opt/CA/LogManager を指定し、[リモート ユーザ]に caelmservice を指定します。これらのサーバ間に非対話型認証を設定する場合は、このパスとこのユーザを作成します。

この例の自動アーカイブ オプションは、レポート サーバからリモート ストレージ サーバへのアーカイブ ファイルの移動を、毎日午後 11 時に開始します。データベースがリモート サーバのコールド ストレージに移動されると、[アーカイブの最大日数]の期間はレポート サーバに保持されます。

自動アーカイブが有効でない場合、ウォーム データベースは、[アーカイブの最大日数]と[アーカイブ ディスク領域]に設定されたしきい値に基づいて保持されます（先に到達するのはどちらの値でもかまいません）。アーカイブされたデータベースは、ディスクの空き容量が 10% 未満にならなければ、削除されるまで 30 日間はレポート サーバで保持されます。空き容量が 10% 未満になると、レポート サーバは自己監視イベントを生成し、使用可能なディスク空き容量が 10% 以上になるまで、最も古いデータベースを削除します。このような状況が発生した場合に、電子メールまたは RSS フィードによってユーザに通知するアラートを作成できます。

リモート ストレージ サーバから元のレポート サーバにデータベースを復元すると、そのデータベースは 3 日間（72 時間）保持されます。

これらの各フィールドと値の詳細については、オンライン ヘルプで説明しています。

イベント ログ ストア オプションの設定

[イベント ログ ストアの設定]ダイアログ ボックスを使用して、すべての CA Enterprise Log Manager サーバのグローバル オプションを設定できます。また、エントリの隣の矢印をクリックすると[イベント ログ ストア]ノードを展開できます。このアクションによって、ネットワーク内の個々の CA Enterprise Log Manager サーバが表示されます。表示されたサーバ名をクリックすると、必要に応じて各サーバに固有のローカルの設定オプションを設定できます。

Administrator ロールを持つユーザは、他の CA Enterprise Log Manager サーバから任意の CA Enterprise Log Manager サーバを設定できます。

イベント ログ ストア オプションを設定する方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブを選択します。

   デフォルトでは[ログ収集]サブタブが表示されます。

2. [サービス]サブタブをクリックします。

3. [イベント ログ ストア]エントリを選択します。

   デフォルトでは、平均的なスループットの中規模ネットワークで初期設定として使用するのに適したオプションが選択されています。

   各フィールドの詳細については、オンライン ヘルプで説明しています。

   注: 個々の CA Enterprise Log Manager サーバのローカル オプションを表示する場合に限り、[連携の子]テーブルおよび[自動アーカイブ]テーブルが表示されます。

相関サービスの設定

相関サービスは、環境内で相関ルールが適用される方法および条件を制御します。相関サービスを設定するばときには、以下のことを考慮する必要があります。

- 専用の相関サーバの導入を計画するかどうか。
- 相関用のイベントを提供する収集サーバの名前および場所。
- 環境内で適用する相関ルールのタイプおよび名前。
- 環境用に策英した通知の宛先。

相関ルールおよびインシデント通知の適用

相関ルールを環境内で有効にするには、それらを適用する必要があります。相関ルールを適用するときには、各ルールの通知の宛先を関連付けることができます。

相関ルールを適用して通知の宛先を設定する方法

1. [管理]をクリックし、[サービス]サブタブをクリックして、[相関サービス]ノードを展開します。
2. 相関ルールを適用する CA Enterprise Log Manager サーバを選択します。

   相関サーバの詳細が右ペインに表示されます。
3. [追加]をクリックします。

   ルールおよびバージョン ダイアログ ボックスが表示されます。
4. 適用するルール カテゴリまたはルールの隣にあるチェック ボックスをオンにします。カテゴリ フォルダ全体、個々のルール、またはそれらの組み合わせを自由に選択できます。
5. 適用する各ルールのルール バージョンを選択します。
6. (オプション)適用するルールの通知の宛先を選択します。宛先を選択しない場合、このルールでは自動通知が行われません。その場合、ルールによって生成されたインシデントの通知を手動で設定できます。
7. 収集サーバを選択して、利用可能なサーバのリストから相関イベントをルーティングする必要があります。相関イベントの送信先となるすべてのサーバを選択する必要があります。サーバが選択されていない場合、相関イベントは転送されません。
8. [OK] または [適用] をクリックします。

定義済み相関ルールの使用

CA Enterprise Log Manager には、ユーザの環境で使用するさまざまな定義済み相関ルールが用意されており、これらはタイプまたは規制要件別に整理されています。たとえば、ライブラリ インターフェースの相関ルール フォルダには PCI というフォルダがあります。このフォルダには、さまざまな PCI 要件のルールが格納されています。また、ID というフォルダには、許可および認証に関する汎用ルールが含まれています。

ルールには 3 つのタイプがあり、各カテゴリにはそれらのいずれかまたはすべてが含まれています。このトピックでは、各タイプの 1 つを選択および適用する例を示します。

例 - 単純ルールの選択および適用

単純相関ルールは、1 つの状態または発生の存在を検出します。たとえば、通常の営業時間外のアカウント作成アクティビティを警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

通常の営業時間外のアカウント作成ルールを選択および適用する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、相関ルール フォルダを展開します。
2. [PCI]フォルダ、[要件 8]フォルダの順に展開して、[通常の営業時間外のアカウント作成ルールを選択します。

   ルールの詳細が右ペインに表示されます。
3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、フィルタはアカウント作成アクションを定義し、通常の営業時間を時間および曜日で設定します。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックしてフィルタ設定を変更します。たとえば、通常の労働時間を変更して現地の仕様に合わせることができます。

   [ルールの管理]ウィザードが開き、ルールの詳細がロードされます。
5. [ルールの管理]ウィザードに通知の詳細を追加します。通知の詳細では、通知の宛先で指定された宛先に送信されるメッセージの内容を指定します。
6. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は自動的に新しいバージョンを作成し、元のバージョンを保存します。

7. [サービス]サブタブをクリックし、[相関サービス]ノードを展開します。
8. ルールを適用するサーバを選択します。相関サーバを識別した場合は、そのサーバを選択する必要があります。
9. [ルール設定]領域の[適用]をクリックし、[通常の営業時間外のアカウント作成]ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
10. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにします。

例 - カウント ルールの選択および適用

カウント相関ルールは、一連の同一状態または発生を識別します。たとえば、管理者アカウントによる 5 回以上のログイン失敗を警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

[管理者アカウントによる 5 回失敗したログイン]ルールを選択および適用する方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、相関ルール フォルダを展開します。
2. [脅威管理]フォルダ、[不審なアカウントおよびログイン アクティビティ]フォルダの順に展開し、[管理者アカウントによる 5 回失敗したログイン]ルールを選択します。

   ルールの詳細が右ペインに表示されます。
3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、フィルタは、キー設定済みリスト「Administrators」に属するユーザ名として管理者アカウントを定義し、カウントしきい値を 60 分内に 5 つのイベントに設定します。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックしてフィルタ設定を変更します。たとえば、時間しきい値を 30 分内に 3 つのイベントに変更できます。

   [ルールの管理]ウィザードが開き、ルールの詳細がロードされます。
5. [ルールの管理]ウィザードに通知の詳細を追加します。通知の詳細では、通知の宛先で指定された宛先に送信されるメッセージの内容を指定します。

6. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は自動的に新しいバージョンを作成し、元のバージョンを保存します。
7. [サービス]サブタブをクリックし、[相関サービス]ノードを展開します。
8. ルールを適用するサーバを選択します。相関サーバを識別した場合は、そのサーバを選択する必要があります。
9. [ルール設定]領域の[適用]をクリックし、[管理者アカウントによる 5 回失敗したログイン]ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
10. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにします。

例 - 状態の移行ルールの選択および適用

状態の移行相関ルールは、一連の状態または発生を識別します。たとえば、同じユーザ アカウントによるログイン失敗後のログイン成功を警告するルールを適用できます。ルールを適用する前に、適切な通知の宛先を作成しておく必要があります。

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、相関ルール フォルダを展開します。
2. [ID]フォルダ、[認証]フォルダの順に展開し、[失敗したログイン、その後成功]ルールを選択します。

   ルールの詳細が右ペインに表示されます。
3. ルールの詳細を参照して、対象の環境内でルールが適切であることを確認します。この場合、詳細ペインにはルールで追跡する 2 つの状態が表示されます。最初の状態は、同じユーザ アカウントまたは ID による 5 回以上のログイン失敗です。2 番目の状態は、同じユーザまたは ID によるログイン成功です。
4. (オプション) 必要な場合は、ペインの上部にある[編集]をクリックして状態設定を変更します。

   [ルールの管理]ウィザードが開き、ルールを構成する 2 つの状態が表示されます。
5. 変更する状態をダブル クリックします。

   [状態定義]ウィザードが開き、状態の詳細が表示されます。

6. 必要に応じて状態を変更したら、[保存して閉じる]をクリックして[ルールの管理]ウィザードに戻ります。たとえば、最初の状態は 10 分以内の 5 回のログイン失敗をチェックします。ログイン失敗しきい値または時間、あるいはその両方を変更できます。
7. [ルールの管理]ウィザードに通知の詳細を追加します。通知の詳細では、通知の宛先で指定された宛先に送信されるメッセージの内容を指定します。
8. ルールの作成が完了したら、ウィザードの[保存して閉じる]をクリックします。定義済み相関ルールを編集して保存すると、CA Enterprise Log Manager は自動的に新しいバージョンを作成し、元のバージョンを保存します。
9. [サービス]サブタブをクリックし、[相関サービス]ノードを展開します。
10. ルールを適用するサーバを選択します。相関サーバを識別した場合は、そのサーバを選択する必要があります。
11. [ルール設定]領域の[適用]をクリックし、[失敗したログイン、その後成功]ルールの新バージョンおよびそれに関連付ける通知の宛先を選択します。
12. [OK]をクリックして、ダイアログ ボックスを閉じてルールをアクティブにします。

詳細情報:

相関ルールおよびインシデント通知の適用 (P. 180)

収集サーバの設定

収集サーバを設定して、複数サーバ環境内で相関用のイベントをルーティングできます。収集サーバを設定すると、1 つのサーバ(専用サーバか共有サーバかに関係なく)で相関ルールを管理および実行できます。その後、選択された収集サーバからインシデントを参照できます。

収集サーバを設定する方法

1. [管理]をクリックし、[サービス]サブタブをクリックして、[相関サービス]ノードを展開します。
2. 相関用のイベントの転送先となる CA Enterprise Log Manager サーバを選択します。専用の相関サーバが存在する場合は、そのサーバ名を選択します。

   相関サーバの詳細が右ペインに表示されます。
3. 相関サーバ シャトル コントロールを使用して、目的のサーバを選択します。相関用のイベントを収集するすべてのサーバが[選択済み]列にあることを確認します。

インシデント通知を設計および適用する方法

相関ルール用の通知をセットアップできます。通知を使用すると、検出されたインシデントについてのキー情報を指定のスタッフに渡すか、または CA IT PAM サービス デスク チケットを自動的に作成できます。

環境内で通知を設定するには、以下の手順に従います。

1. 通知の宛先を計画および作成します。
2. 定義済みの相関ルールを選択するか、または環境内で使用するカスタム ルールを作成します。
3. 設定する通知の詳細を相関ルールに追加します。
4. CA Enterprise Log Manager サーバに相関ルールを適用し、通知の宛先を割り当てます。

詳細情報:

通知の宛先を設定する方法 (P. 186)
相関ルールおよびインシデント通知の適用 (P. 180)

通知の宛先を設定する方法

相関ルールで使用する通知の宛先オブジェクトを作成できます。宛先を使用すると、共通の送信設定をさまざまなルールに適用できます。つまり、必要に応じて 1 つの宛先を複数のルールに割り当てることができます。宛先は、相関ルールの適用中、またはインシデントの作成後に割り当てることができます。

通知の宛先オブジェクトを作成するには、以下の手順に従います。

1. 通知の管理ウィザードを開き、宛先名および説明を設定します。
2. 必要な宛先タイプのパラメータを設定します。
   a. 電子メール
   b. CA IT PAM プロセス
   c. SNMP トラップ

   通知の宛先オブジェクトには複数の通知タイプがあります。

詳細情報:

通知の管理ウィザードの開き方 (P. 186)
電子メールの宛先の設定 (P. 187)
プロセスの宛先の設定 (P. 187)
SNMP の宛先の設定 (P. 188)

通知の管理ウィザードの開き方

通知の宛先を作成するには、ウィザードを開く必要があります。

通知の管理ウィザードを開く方法

1. [管理]タブをクリックし、[ライブラリ]サブタブをクリックして、[通知の宛先]フォルダを展開します。
2. [新規通知]をクリックします。

   [通知の管理]ウィザードが開きます。

詳細情報:

電子メールの宛先の設定 (P. 187)
プロセスの宛先の設定 (P. 187)
SNMP の宛先の設定 (P. 188)

電子メールの宛先の設定

通知用の電子メール宛先を設定して、適切な担当者に対してそのジョブのロールまたは責任に関連するインシデントを通知できます。

電子メールの宛先を設定する方法

1. 通知の管理ウィザードを開きます
2. ID 情報の詳細を設定し、[通知]ステップに進みます。
3. [電子メール]タブをクリックし、[電子メール通知を有効化]を選択します。
4. 少なくとも 1 人の受信者の電子メール アドレスを入力します。複数のアドレスをカンマで区切って入力できます。
5. (オプション) 送信者の電子メール アドレスを入力します。
6. 必要な他の宛先を追加して、[保存して閉じる]をクリックします。

プロセスの宛先の設定

通知の宛先として IT PAM プロセスを設定できます。通知は、IT PAM を使用して CA Enterprise Log Manager インシデント情報を CA ServiceDesk または サードパーティ アプリケーションに渡します。プロセスの宛先は、有効な IT PAM プロセスを識別することによって設定します。通知の詳細を使用して、プロセス パラメータを構成するインシデント情報を定義します。

IT PAM プロセスの詳細については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

プロセスの宛先を設定する方法

1. 通知の管理ウィザードを開き、ID 情報の詳細を設定して[通知]ステップに進みます。
2. [プロセス]タブをクリックし、[プロセス自動化の有効化]を選択します。
3. 以下のように、インシデント情報の送り先となる IT PAM プロセスの名前を入力します。

   ```
   /CA_ELM/EventAlertOutput
   ```

4. 必要な他の宛先を追加して、[保存して閉じる]をクリックします。

SNMP の宛先の設定

SNMP トラップを設定すると、SNMP トラップを使用してインシデント情報をサードパーティ管理システムに送信できます。SNMP トラップの詳細については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

SNMP の宛先を設定する方法

1. 通知の管理ウィザードを開き、ID 情報の詳細を設定して[通知]ステップに進みます。
2. SNMP タブをクリックし、[SNMP トラップの有効化]を選択します。
3. (オプション) SNMP v3 を使用するアラートを送信するには[SNMP Version 3]を選択します。デフォルトは[SNMP Version 2]です。
4. (オプション) SNMP バージョン 3 を選択した場合は、[V3 セキュリティ]ボタンをクリックし、セキュリティ パラメータ ダイアログ ボックスで認証または暗号化を設定します。
5. 宛先サーバおよび宛先ポートの情報を入力して、SNMP 転送されるイベントのターゲットを指定します。
6. (オプション) 別の宛先サーバ/宛先ポート行を選択し、別のサーバ/ポート値を入力します。
7. 必要な他の宛先を追加して、[保存して閉じる]をクリックします。

インシデント サービスに関する注意事項

選択した CA Enterprise Log Manager サーバについて、インシデント サービスがイベントを格納し、インシデントを作成する方法を制御できます。以下の値を設定できます。

有効期限

サービスがインシデント データベース内のインシデントを保持する日数を指定します。値が 0 の場合、イベントは削除されません。期限切れになったインシデントは表示されません。

インシデント生成制限

単一の相関ルールがインシデントを作成する頻度を指定して、不要なインシデントを減らします。インシデント生成制限の目的のため、ルールの異なるバージョンは別個のルールと見なされます。したがって、環境内にルールの複数のバージョンを適用した場合は、それらは個別に制限されます。制限値は以下のとおりです。

有効

インシデント生成制限が適用されるかどうかを示します。

カウント

単一のルールによって生成されるインシデント数のしきい値を設定します。値が 0 より大きい場合、この値は[時間]値と一緒に機能します。指定された数に達すると、インシデント サービスは[ブロックされた時間]制限値を適用します。したがって、[カウント]を 3 に設定し、[時間]を 10 に設定した場合は、単一のルールが 10 秒内に 3 つを超えるインシデントを生成した後に制限が適用されます。

時間

単一のルールによって生成されるインシデント数のしきい値を秒単位で設定します。値が 0 より大きい場合、この値は[カウント]値と一緒に機能します。指定された数に達すると、インシデント サービスは[ブロックされた時間]制限値を適用します。したがって、[カウント]を 3 に設定し、[時間]を 10 に設定した場合は、単一のルールが 10 秒内に 3 つを超えるインシデントを生成した後に制限が適用されます。

ブロックされた時間

ルールによるインシデントの作成をブロックする期間を秒単位で指定します。この制限に達すると、期間が経過するまでルールはインシデントを作成しません。

ODBC サーバの注意事項

SAP Business Objects の Crystal Reports のような外部アプリケーションから CA Enterprise Log Manager イベント ログ ストアにアクセスするには、ODBC クライアントまたは JDBC クライアントをインストールします。

この設定領域では、以下のタスクを実行できます。

- ODBC および JDBC によるイベント ログ ストアへのアクセスを有効にします。
- ODBC または JDBC クライアントと CA Enterprise Log Manager サーバの間の通信に使用されるサービス ポートの設定。
- ODBC または JDBC クライアントと CA Enterprise Log Manager サーバの間の通信を暗号化するかどうかの指定。

フィールドの説明は以下のとおりです。

[サービスの有効化]

ODBC と JDBC のクライアントがイベント ログ ストアのデータにアクセスできるかどうかを示します。このチェック ボックスをオンにすると、外部からのイベントへのアクセスが有効になります。 外部からのアクセスを無効にするには、チェック ボックスをオフにします。

現在、ODBC サービスは FIPS と互換性はありません。FIPS モードで実行する場合は、ODBC および JDBC のアクセスを無効にするために、このチェック ボックスをオフにします。これによって、非準拠の場合はアクセスできなくなります。FIPS モードでの操作向けに ODBC サービスおよび JDBC サービスを無効にする場合、この値を連携内の各サーバに設定したことを確認してください。

[サーバ リスニング ポート]

ODBC サービスまたは JDBC サービスで使用するポート番号を指定します。デフォルト値は 17002 です。Windows のデータ ソースまたは JDBC の URL 文字列に異なる値が指定された場合、CA Enterprise Log Manager サーバは接続の試行を拒否します。

[暗号化 (SSL)]

ODBC クライアントと CA Enterprise Log Manager サーバの間の通信に暗号化を使用するかどうか示します。Windows のデータ ソースまたは JDBC の URL 文字列の対応する値がこの設定と一致しない場合、CA Enterprise Log Manager サーバは接続の試行を拒否します。

[セッション タイムアウト (分)]

自動的に終了する前に、アイドル セッションを開いておく時間(分)の長さを指定します。

ログ レベル

ログ記録ファイルに記録される詳細情報のタイプおよびレベルを定義します。ドロップダウン リストは、詳細さのレベル順に並んでおり、最も詳細でない選択肢が最初になっています。

すべてのロガーに適用

ログ レベル設定が、ログのプロパティ ファイルによるすべてのログ設定より優先されるかどうかを制御します。この設定は、ログ レベル設定がデフォルト設定より低い(より詳細に表示される)場合にのみ適用されます。

レポート サーバに関する注意事項

レポート サーバは、自動配信レポートの管理、それらのレポートの PDF 形式のレイアウト、およびアクション アラートとレポート保持を制御します。レポート サーバ設定領域では、以下のタスクを実行できます。

- [レポート設定]領域に、会社名とロゴ、フォント、およびその他の PDF レポート設定を設定する。
- [アラート保持]領域に、保持される全アクション アラートおよび保持される日数を設定する。

  最大アクション アラート数

  レポート サーバがレビュー用に保持するアクション アラートの最大数を定義します。

  最小: 50

  最大: 1000

  アクション アラート保持

  アクション アラートが保持される日数を定義します。最大日数まで保持されます。

  最小: 1

  最大: 30
- [レポート保持]領域に、スケジュール済みレポートの反復タイプごとに保持ポリシーを設定する。

- 保持ユーティリティがレポートを検索し、保持ポリシーに基づいて自動的に削除するかどうか、削除する場合はその頻度を設定する。たとえば、レポート保持ユーティリティを日単位で実行する場合、指定した最長有効期間を過ぎたレポートが日単位で削除されます。

サブスクリプションの設定方法

サブスクリプション アーキテクチャを計画したら、サブスクリプション更新を実装するために CA Enterprise Log Manager 環境を設定できます。

以下は、サブスクリプション設定プロセスの概要です。各手順の詳細については、関連する手順を参照してください。

1. 計画したサブスクリプション アーキテクチャに基づいて、各サーバをサブスクリプション プロキシまたはクライアントとして設定します。必要に応じて、1 つまたは複数のプロキシをオフライン プロキシとして指定します。サーバはローカル レベルでプロキシまたはクライアントとして指定します。
2. クライアント更新およびコンテンツ更新の両方にプロキシ リストを設定します。クライアント更新用のプロキシ リストは、環境全体に対してグローバルに指定するか、またはサーバごとにローカルのプロキシ リストを設定します。コンテンツ更新については、グローバル レベルでのみプロキシ リストを指定できます。
3. ダウンロードするモジュールを選択します。モジュールはグローバルに選択するか、またはサーバごとにローカルに選択できます。
4. サブスクリプション スケジュールを設定します。スケジュールはグローバルに設定するか、またはサーバごとにローカルに設定できます。

詳細情報:

オンライン サブスクリプション プロキシの設定 (P. 193)
オフライン サブスクリプション プロキシの設定 (P. 194)
サブスクリプション クライアントの設定 (P. 195)
プロキシ リストの設定 (P. 196)
オンライン サブスクリプション用のモジュールの選択 (P. 199)
オフライン サブスクリプション用のモジュールのダウンロードと選択 (P. 201)
サブスクリプション スケジュールの設定 (P. 203)

オンライン サブスクリプション プロキシの設定

オンライン サブスクリプション プロキシは、CA サブスクリプション サーバにアクセスして最新の CA Enterprise Log Manager 更新をダウンロードし、それらをサブスクリプション クライアントに順に配布します。

他のプロキシが設定されていないか利用可能でない場合は、デフォルトのオンライン サブスクリプション プロキシが更新をサブスクリプション クライアントにダウンロードします。最初にインストールされる CA Enterprise Log Manager サーバが、インストール時にデフォルトのサブスクリプション プロキシとして設定されます。ただし、どのオンライン プロキシでもデフォルトのサブスクリプション プロキシとして指定できます。デフォルトのサブスクリプション プロキシは、グローバル レベルでのみ設定できます。

オンライン サブスクリプション プロキシを設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

   [グローバル サービス設定]-[サブスクリプション サービス]ウィンドウが表示されます。

   注: インストール時に設定されたものとは別のデフォルト サブスクリプション プロキシを指定するには、[管理]をクリックし、[デフォルトのサブスクリプション プロキシ]フィールドにサーバ名を入力します。
3. [サービス リスト]で、[サブスクリプション サービス]を展開し、設定するサーバを選択します。

   選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス設定]が表示されます。
4. [管理]タブをクリックします。
5. [サブスクリプション プロキシ]チェック ボックスをオンにして、[オンラインのサブスクリプション プロキシ]を選択します。
6. サブスクリプション更新用の RSS フィード URL が正しいことを確認します。このプロキシで、グローバル設定とは別の RSS フィードを使用する場合は、ローカル設定に切り替えて、正しい RSS URL を入力します。
7. このサーバで、継承したものとは異なる HTTP プロキシ サーバを使用して CA サブスクリプション サーバに接続するには、ローカル設定に切り替えて該当する HTTP プロキシを設定します。
8. [保存]をクリックします。

詳細情報:

サブスクリプションの設定方法 (P. 192)

オフライン サブスクリプション プロキシの設定

オフライン サブスクリプション プロキシは、インターネットに接続せずに、クライアントに CA Enterprise Log Manager 更新を提供します。この設定により、CA Enterprise Log Manager サーバの一部またはすべてをインターネットから隔離することが可能になります。

オフライン サブスクリプション更新を実行する前に、オフライン更新ファイルを CA FTP サイトから、物理メディアを使用して、または CA Enterprise Log Manager に含まれている scp 経由で、オフライン プロキシに手動でコピーします。更新ファイルは次のパスにコピーします:
/opt/CA/LogManager/data/subscription/offline

オフライン プロキシ サーバのサブスクリプション クライアントは、設計上、オフライン プロキシに手動でインストールされたすべての更新を自動的に受信します。この場合、クライアントにローカル レベルで選択されているモジュールは関係がありません。そのため、オンラインとオフラインの両方のサブスクリプション プロキシが混在している環境では、オンライン サブスクリプション クライアントのプロキシ リストにオフライン プロキシを含めないようにしてください。含めた場合、オンライン サブスクリプション クライアントでは、そのクライアントに選択されているモジュールではなく、オフライン プロキシ サーバに手動でインストールされるすべての更新を自動的に受信します。

オフライン サブスクリプション プロキシを設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]を展開し、設定するサーバを選択します。

   選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス設定]が表示されます。
3. [管理]タブをクリックします。
4. [サブスクリプション プロキシ]チェック ボックスをオンにして、[オフラインのサブスクリプション プロキシ]を選択します。

5. インストールするオフライン サブスクリプション ファイルが含まれる .zip ファイルを[ファイル]ドロップダウン リストから選択します。

   注: この手順は、オフライン サブスクリプション パッケージがこのサーバ上の適切な場所にすでにコピーされていることを前提としています。まだの場合、プロンプトが表示されます。

6. [保存]をクリックします。

詳細情報:

サブスクリプションの設定方法 (P. 192)

サブスクリプション クライアントの設定

サブスクリプション クライアントは、最新の CA Enterprise Log Manager 更新をサブスクリプション プロキシからダウンロードします。 更新を取得したクライアントは、ダウンロードしたコンポーネントをインストールします。

サブスクリプション プロキシとして設定されていないすべての CA Enterprise Log Manager サーバは、デフォルトでサブスクリプション クライアントとなります。グローバルに設定されたサブスクリプション設定を使用しない場合を除いて、サーバをクライアントとしてローカルに設定する必要はありません。

サブスクリプション プロキシが更新を完全にダウンロードしてプロキシ自身にインストールするまで、サブスクリプション クライアントはその更新を取得できません。クライアントは、設定されたプロキシ リスト内の各サーバから順に更新の取得を試行します。クライアントの要求する更新のインストールを完了したプロキシがない場合、クライアントは更新に成功するまで再試行を 5 分おきに繰り返します。 1 時間経っても更新をダウンロードできない場合、更新はキャンセルされ、クライアントは次のスケジュールされた時間に再度更新を試行します。このプロセスの間、自己監視イベント ログにメッセージが表示され、更新のステータスをユーザに警告します。

サブスクリプション クライアントを設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]を展開し、設定するサーバを選択します。

   選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス設定]が表示されます。

3. [サブスクリプション プロキシ]チェック ボックスはオフにしたままで、選択されたサーバをクライアントとして特定します。
4. サブスクリプション クライアントは内部ネットワークを通してサブスクリプション プロキシに接続するため、個別のクライアント サーバ用のローカル HTTP プロキシ設定を指定する必要はありません。
5. [保存]をクリックします。

詳細情報:

サブスクリプションの設定方法 (P. 192)

プロキシ リストの設定

環境に複数のサブスクリプション プロキシを設定する場合、クライアント更新用のプロキシ リストを設定できます。クライアントが更新を要求したときに、指定されたプロキシが利用不可能である場合、クライアントはそのプロキシ リスト内の各プロキシに順番にアクセスします。これは、更新のダウンロードに成功するまで続けられます。クライアント更新用のプロキシ リストは、CA Enterprise Log Manager 環境全体に対してグローバルに設定するか、またはサブスクリプション クライアントごとにローカルに設定できます。

複数のサブスクリプション プロキシがある場合、コンテンツ更新用のプロキシ リストを設定することもできます。 このリストに含まれるプロキシは、クエリ、レポート、相関ルールなどのコンテンツ更新を受信して管理サーバに配布します。管理サーバでは、CA Enterprise Log Manager で使用するためにコンテンツ更新を格納します。コンテンツ更新用のプロキシ リストは、グローバル レベルでのみ設定できます。

プロキシ リストを使用すると、サブスクリプション更新を確実に適宜取得および配布できるようになります。小規模な CA Enterprise Log Manager 環境でも、プライマリ プロキシが利用不可能である場合に備えて、クライアント更新とコンテンツ更新の両方に対して少なくとも 1 つのバックアップ プロキシを設定しておくことをお勧めします。

プロキシ リストを設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

   サブスクリプション サービス用の[グローバル サービス設定]が表示されます。

3. 以下のいずれかを行います。

   - CA Enterprise Log Manager 環境全体に対するグローバルなプロキシ リストを指定するには、[管理タブ]をクリックします。

または

   - 特定のサブスクリプション クライアント用にローカルのプロキシ リストを指定するには、サーバ名をクリックし、[管理]タブをクリックしてローカル設定に切り替えます。

4. 該当するプロキシ サーバをプロキシ リストに追加します。

   重要: オンラインとオフラインの両方のサブスクリプション プロキシが混在して設定されている環境では、オンライン サブスクリプション クライアント用のプロキシ リストにオフライン プロキシを含めないようにしてください。含めた場合、オンライン サブスクリプション クライアントでは、選択されているモジュールではなく、オフライン プロキシ サーバに手動でインストールされたすべての更新を自動的に受信します。

5. [保存]をクリックします。

詳細情報:

サブスクリプションの設定方法 (P. 192)

ダウンロードするモジュールについて

更新はモジュールとしてパッケージ化され、CA サブスクリプション サーバを通じてダウンロードされます。使用可能なモジュールのリストには、CA が提供する RSS フィード URL を使用してアクセスするか、オフライン サブスクリプションの場合は CA FTP サイト経由でアクセスします。各モジュールに何が含まれるかは CA によって決定されます。

以下の表に、各モジュール、その機能、および CA が更新を提供する頻度を示します。

モジュールのタイプ	説明	頻度
コンテンツ	クエリ リスト、レポート リスト、および相関ルールの内容を更新します。コンテンツ更新用プロキシによって、このコンテンツが自動的に管理サーバのリポジトリに送信されます。	毎月

モジュールのタイプ	説明	頻度
統合	サブスクリプション ウィザードが実行され、[コネクタの更新] が選択された場合に、コネクタを更新します。	毎月
オペレーティング システム	各 CA Enterprise Log Manager サーバにインストールされたオペレーティング システムを更新します。	定期的
エージェント	サブスクリプション ウィザードが実行され、[エージェントの更新] が選択された場合に、エージェントを更新します。	定期的
Log Manager サービス パック	各サーバの CA Enterprise Log Manager 製品を該当するサービス パックで更新します。	四半期
Log Manager バージョン	各システムの CA Enterprise Log Manager 製品を該当するバージョンで更新します。	定期的

CA Enterprise Log Manager 環境に対してダウンロードするモジュールのリストをグローバル レベルで選択できます。個々のサブスクリプション プロキシおよびクライアント サーバは、これらのグローバル設定を継承します。グローバル設定を使用しないようにするには、個別の CA Enterprise Log Manager サーバに対して、ダウンロードするモジュールのローカル リストを設定します。

注: サブスクリプション プロキシは、プロキシ自身にインストールされていないモジュールをクライアントに配布することはできません。サブスクリプション プロキシ用のモジュールを選択する場合は、少なくともプロキシのクライアントに選択されているすべてのモジュールが含まれているようにしてください。

CA Enterprise Log Manager 環境の更新は、以下のいずれかまたは両方の方法で実行できます。

1. 自動: モジュールをあらかじめ選択し、ダウンロードのスケジュールを指定します。サブスクリプション サービスは、指定したスケジュールに従って、選択したモジュールを自動的にダウンロードおよびインストールします。
2. 手動: 必要に応じてモジュールを選択し、サブスクリプション サービスの [今すぐ更新] 機能を使用して、それらのモジュール適宜ダウンロードおよびインストールします。

コンテンツ、統合、オペレーティング システム、エージェントのモジュールは定期的に更新されるため、少なくとも月に 1 度はこれらのモジュールを自動的にダウンロードするようサブスクリプション スケジュールを設定することを検討してください。ログ マネージャ サービス パックおよびバージョン更新の頻度はそれほど高くなく、CA Enterprise Log Manager 環境にそれらを適用する前に考慮および計画が必要になる場合があります。必要に応じて、これらのタイプの更新は手動でダウンロードします。

新しいモジュールが利用可能になると、サブスクリプション RSS フィードに表示されます。オフライン サブスクリプションの場合は CA オフライン サブスクリプション FTP サイト上に表示されます。ダウンロードが可能なモジュールは、更新サイクルによって異なります。そのため、使用可能なリストを監視し、必要とするモジュールがすべて選択されていることを確認してください。また、CA サポート サイト(http://ca.com/support)をチェックして、新しい Log Manager サービス パックおよびバージョンが使用可能であるかどうかを確認してください。

詳細情報:

オンライン サブスクリプション用のモジュールの選択 (P. 199)
オフライン サブスクリプション用のモジュールのダウンロードと選択 (P. 201)
サブスクリプション更新を計画する方法 (P. 52)
サブスクリプションの設定方法 (P. 192)

オンライン サブスクリプション用のモジュールの選択

現在利用可能な CA Enterprise Log Manager サブスクリプション更新は、CA によって提供される RSS フィードに表示されます。RSS フィード URL は、インストール時にサブスクリプション サービス管理タブにデフォルトで提供されます。

新しいモジュールが利用可能になると、それらがサブスクリプション RSS フィードに表示されます。利用可能なモジュールのリストを定期的にチェックして、必要なすべてのモジュールが選択されていることを確認します。また、CA サポート サイト(http://ca.com/support)をチェックして、新しい Log Manager サービス パックおよびバージョンが使用可能であるかどうかを確認してください。

ダウンロードするモジュールを選択する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

   サブスクリプション サービス用の[グローバル サービス設定]が表示されます。

3. 以下のいずれかの操作を行います。

   - CA Enterprise Log Manager 環境全体に対してグローバルにダウンロードするモジュールを選択するには、[管理]タブをクリックします。

   または

   - 特定のサーバに対してローカルにダウンロードするモジュールを選択するには、サーバ名をクリックし、[管理]タブをクリックして、[ダウンロード用に選択したモジュール]のローカル設定に切り替えます。

4. [RSS フィード URL]フィールドに正しい RSS アドレスが表示されていることを確認します。または特定のサーバ用にカスタムの RSS アドレスを設定するには、ローカル設定に切り替えて、RSS URL を入力します。

5. [参照]をクリックします。

   [ダウンロード可能なモジュール]ダイアログ ボックスが表示されます。

6. ダウンロードするモジュールを選択します。

   注: 新しい更新を利用可能になると同時に CA から受信するようにするには、月単位および定期的に更新されるモジュールを選択し、少なくとも月に 1 度は自動的に更新するようサブスクリプション スケジュールを設定します。サービス パックおよびバージョン更新の頻度はそれほど高くなく、CA Enterprise Log Manager 環境にそれらを適用する前に考慮および計画が必要になる場合があります。必要に応じて、これらのタイプの更新は手動でダウンロードします。

   注: クライアントモジュールをダウンロードするには、そのプロキシにまずダウンロードされている必要があります。サブスクリプション プロキシに選択されたモジュールには、少なくともそのプロキシのクライアントのダウンロード リストで選択されたすべてのモジュールが含まれているようにしてください。

7. [OK]をクリックします。

   [ダウンロード可能なモジュール]ダイアログ ボックスが閉じられ、選択したモジュールが[ダウンロード用に選択したモジュール]リストに表示されます。

8. [保存]をクリックします。

詳細情報:

サブスクリプションの設定方法 (P. 192)
ダウンロードするモジュールについて (P. 197)

オフライン サブスクリプション用のモジュールのダウンロードと選択

オフライン サブスクリプション更新ファイルは、CA オフライン サブスクリプション FTP サイトで、.zip ファイルのパッケージで提供されています。新しいモジュールが利用可能になると、FTP フィードに表示されます。使用可能なモジュールのリストを定期的にチェックして、最新の更新がダウンロードされていることを確認します。また、CA サポート サイト(http://ca.com/support)をチェックして、新しい Log Manager サービス パックおよびバージョンが使用可能であるかどうかを確認してください。

オフライン サブスクリプション プロキシ用にダウンロードするモジュールを選択するには、CA FTP サイトからオフライン更新ファイル パッケージをダウンロードし、お使いのオフライン プロキシに手動でコピーする必要があります。その後、どのモジュールをダウンロードしてインストールするかを選択できます。反対に、オフライン サブスクリプション クライアントは、そのオフライン プロキシに手動でインストールされたすべての更新を自動的に受信します。ローカル レベルでそのクライアントにどのモジュールが選択されているかは関係ありません。

オフライン サブスクリプション モジュールをダウンロードおよび選択する方法

1. インターネットまたは FTP アクセスに対応するシステムで、FTP オフライン サブスクリプション サイトへ移動します:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   ディレクトリ インデックスには、主な CA Enterprise Log Manager リリースごとにフォルダが表示されます。

2. 実行する更新用の適切な .zip ファイルをダウンロードします。

   注: CA Enterprise Log Manager r12.5 リリース用のフォルダには、サブフォルダと .zip ファイルが含まれています。サブフォルダには、旧バージョンから r12.5 にアップグレードするためのモジュールが含まれます。.zip ファイルには、バージョン r12.5 への定期的なルーチン更新を実行するためのモジュールが含まれます。オフライン サブスクリプションを使用して旧バージョンから r12.5 にアップグレードする場合は、「リリース ノート」の「CA Enterprise Log Manager へのアップグレード」を参照してください。ルーチン更新を実行している場合は、.zip ファイルを選択します。

3. ディスクなどの物理メディア、または scp を使用する場合は、オフライン プロキシ上の以下のファイル パスに .zip ファイルを手動でコピーします。

   /opt/CA/LogManager/data/subscription/offline

4. CA Enterprise Log Manager 環境内のシステムにログインします。

5. [管理]タブをクリックし、[サービス]サブタブをクリックします。
6. [サブスクリプション サービス]を展開し、設定するオフライン プロキシ サーバを選択します。

   選択した CA Enterprise Log Manager サーバの[サブスクリプション サービス設定]が表示されます。

   注: オフライン サブスクリプション クライアントは、そのオフライン プロキシに手動でインストールされたすべてのモジュールを自動的に受信します。プロキシ サーバのコンテンツによって、サブスクリプション クライアントがどの更新を受信するかが制御されます。オフライン クライアントに対してローカル レベルで選択されたモジュールは関係しません。
7. [管理]タブをクリックします。
8. [ファイル]ドロップダウンで、サーバにコピーしたオフライン更新用 .zip ファイルを選択し、[参照]をクリックします。

   [ダウンロード可能なモジュール]ダイアログ ボックスが表示されます。
9. ダウンロードするモジュールを選択します。
10. [OK]をクリックします。

    [ダウンロード可能なモジュール]ダイアログ ボックスが閉じられ、選択したモジュールが[ダウンロード用に選択したモジュール]リストに表示されます。
11. [保存]をクリックします。

    オフライン サブスクリプション クライアントでこれらのモジュールをダウンロードできるようになりました。これは、設定されたサブスクリプション スケジュールに従って自動的に行われるか、またはユーザが手動更新を開始することによってオンデマンドで実行されます。
12. (オプション)[今すぐ更新]をクリックします。

    オフライン プロキシ サーバが、選択されたモジュールで自身を更新します。

    注: オフライン プロキシによる更新は、設定したサブスクリプション スケジュールに従って自動的に行われるようにできますが、新しいファイルを転送した場合は常に手動更新を実行することをお勧めします。これにより、オフライン サブスクリプション クライアントで更新が要求された場合にその更新が使用可能な状態であることが保証されます。

詳細情報

サブスクリプションの設定方法 (P. 192)
ダウンロードするモジュールについて (P. 197)

サブスクリプション スケジュールの設定

サブスクリプション スケジュールを設定して、サブスクリプション サービスが自動更新を実行するタイミングおよび頻度を定義することができます。サブスクリプション スケジュールは、CA Enterprise Log Manager 環境全体に対してグローバルに設定できます。または、個別のサブスクリプション プロキシおよびクライアントに対してカスタムのスケジュールを設定できます。

サブスクリプション スケジュールを設定する方法

1. [管理]タブをクリックし、[サービス]サブタブをクリックします。
2. [サブスクリプション サービス]をクリックします。

   サブスクリプション サービス用の[グローバル サービス設定]が表示されます。
3. 以下のいずれかを行います。
   - CA Enterprise Log Manager 環境全体に対するグローバルなサブスクリプション スケジュールを指定するには、[管理タブ]をクリックします。

または

   - 特定のサーバに対するローカルのサブスクリプション スケジュールを指定するには、サーバ名をクリックし、[管理]タブをクリックしてローカル設定に切り替えます。
4. サブスクリプション スケジュールを設定します。タイムゾーンおよび更新の開始時刻を選択し、更新の頻度を指定します。

詳細情報

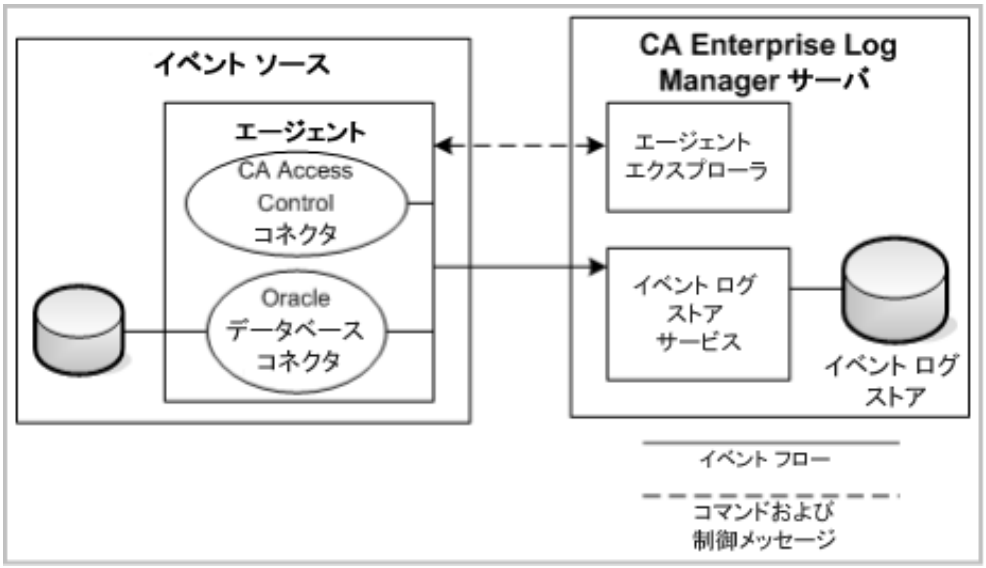
サブスクリプションの設定方法 (P. 192)

第 6 章: イベント収集の設定

このセクションには、以下のトピックが含まれています。

エージェントのインストール

CA Enterprise Log Manager エージェントを特定のプラットフォームに対して個別にインストールすることで、トランスポート層でイベント ソースから CA Enterprise Log Manager サーバのイベント ログ ストアにイベントを取得できます。エージェントは、コネクタを使用してさまざまなイベント ソースからイベント ログを収集します。次の図に、エージェントと CA Enterprise Log Manager サーバ間の相互作用を示します。



イベント ソースにエージェントをインストールしたら、1 つ以上のコネクタを設定して、デバイス、アプリケーション、オペレーティング システム、およびデータベースなどのイベント ソースからイベントを収集できます。図内の例には、CA Access Control および Oracle データベース用のコネクタが含まれています。通常はホスト サーバまたはイベント ソースごとにエージェントを 1 つだけインストールしますが、そのエージェントには複数のタイプのコネクタを設定できます。CA Enterprise Log Manager サーバの一部であるエージェント エクスプローラを使用して、エージェントの管理や設定、エージェントのコネクタの管理を行うことができます。また、エージェント エクスプローラを使用して、管理や制御をより簡単にするためのエージェント グループを作成できます。

統合またはリスナのいずれかに基づいてコネクタを設定します。これは、データアクセス、メッセージ解析、およびデータ マッピング用ファイルを含むことができるテンプレートです。CA Enterprise Log Manager では、よく使用されるイベント ソース用の多くの統合を標準装備で提供しています。

エージェントのインストールに関する詳細と手順については、「CA Enterprise Log Manager 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:

エージェントまたはコネクタのステータスの表示と管理 (P. 222)

エージェント エクスプローラの使用

CA Enterprise Log Manager サーバをインストールするとすぐに、エージェント エクスプローラにデフォルトのエージェントがリスト表示されます。エージェントは CA Enterprise Log Manager サーバをインストールするときにインストールされ、直接 syslog イベント収集に使用されます。

ネットワークにエージェントをインストールすると、エージェント エクスプローラはエージェントの追跡とリスト表示を行い、エージェントとコネクタの設定、コマンド、および制御の中心となる場所を提供します。エージェントは、初めて起動するときに、指定した CA Enterprise Log Manager サーバに登録されます。登録されると、エージェント エクスプローラにエージェント名が表示され、イベント ログの収集を開始するコネクタを設定できるようになります。コネクタはイベント ログを収集して、CA Enterprise Log Manager サーバに送信します。1 つのエージェントに多くのコネクタを制御できます。

エージェント エクスプローラを使用したコネクタおよびエージェントのインストール、設定、および制御には、次の基本的な手順が含まれます。

1. エージェント バイナリをダウンロードします。
2. 1 つ以上のエージェント グループを作成します（オプション）。
3. コネクタを作成して設定します（抑制ルールと集約ルールの作成または適用を含む）。
4. エージェントまたはコネクタのステータスを表示します。

エージェント グループとコネクタの作成と操作、およびエージェントに抑制ルールを適用する方法については、「CA Enterprise Log Manager 管理ガイド」で詳細を参照してください。

詳細情報:

エージェントについて (P. 64)
エージェント グループについて (P. 64)
ログ センサについて (P. 67)
抑制ルールによる影響 (P. 69)

デフォルト エージェントの設定

CA Enterprise Log Manager をインストールすると、CA Enterprise Log Manager サーバにデフォルト エージェントが作成されます。このエージェントには、使用可能な 2 つのコネクタ、syslog_Connector および Linux_local Connector が備わっています。syslog コネクタを使うと、CA Enterprise Log Manager サーバに送信される syslog イベントを収集できます。Linux_local コネクタは、CA Enterprise Log Manager 物理サーバ、または syslog ファイルからの OS レベルのイベントの収集に利用できます。

2 台のサーバを使用する基本的な環境では、収集サーバに 1 つ以上の syslog コネクタを設定してイベントを受信する必要があります。

デフォルト エージェントを使用するプロセスには、次の手順が含まれます。

1. （オプション）syslog の統合とリスナを確認します。
2. syslog のコネクタを作成します。
3. CA Enterprise Log Manager サーバが syslog イベントを受信しているかどうかを確認します。

syslog の統合とリスナの確認

コネクタを作成する前に、デフォルトの syslog の統合とリスナを確認できます。リスナは、基本的には syslog コネクタのテンプレートであり、CA Enterprise Log Manager サーバに標準で付属している特定の syslog 統合を使用します。

syslog の統合を確認する方法

1. CA Enterprise Log Manager にログインして、[管理]タブにアクセスします。
2. [ライブラリ]サブタブをクリックし、[イベント精製ライブラリ]ノードを展開します。
3. [統合]ノードと[サブスクリプション]ノードの両方を展開します。
4. 名前が「..._Syslog」で終わる統合を選択します。

   右側のウィンドウに統合の詳細が表示されます。統合が使用するメッセージ解析ファイルやデータ マッピング ファイルと、バージョンや抑制ルールと集約ルールのリストなどのその他の詳細を確認できます。

syslog リスナを確認する方法

1. [リスナ]ノードと[サブスクリプション]ノードの両方を展開します。
2. [syslog リスナ]を選択します。

   右側のウィンドウにデフォルトリスナの詳細が表示されます。バージョン、抑制ルールと集約ルールのリスト、デフォルトのリスニング ポート、トラステッド ホストのリスト、およびリスナのタイムゾーンなどの詳細を確認できます。

デフォルト エージェントの syslog コネクタの作成

CA Enterprise Log Manager サーバのデフォルト エージェントを使用して、syslog イベントを受信する syslog コネクタを作成します。

デフォルト エージェントの syslog コネクタを作成する方法

1. CA Enterprise Log Manager にログインして、[管理]タブにアクセスします。
2. [エージェント エクスプローラ]と[エージェント グループ]を展開します。

   デフォルト エージェントは、自動的にデフォルト エージェント グループにインストールされます。このエージェントは別のグループに移動させることもできます。

3. エージェント名を選択します。

   デフォルト エージェントは、インストール中に CA Enterprise Log Manager サーバに指定したものと同じ名前です。

4. [コネクタの新規作成]をクリックして、コネクタ ウィザードを開きます。
5. [リスナ]オプションをクリックして、このコネクタの名前を入力します。
6. ウィザードの 2 ページ目と 3 ページ目で、必要に応じて抑制ルールを適用します。
7. このコネクタと一緒に使用する 1 つ以上のターゲットの syslog 統合を[使用可能]リストから選択し、それを[選択済み]リストに移動します。
8. デフォルトを使用していない場合は UDP と TCP のポートの値を設定し、実装でトラステッド ホストを使用している場合はそのリストを入力します。

   注: CA Enterprise Log Manager エージェントが root として実行されない場合、1024 より小さい番号のポートは開くことができません。そのため、デフォルト syslog コネクタは UDP ポート 40514 を使用します。インストールの際に、CA Enterprise Log Manager サーバにファイアウォール ルールを適用して、トラフィックをポート 514 から 40514 にリダイレクトします。

9. タイムゾーンを選択します。
10. [保存して閉じる]をクリックするとコネクタが完成します。

    コネクタは、指定したポートで、選択した統合と一致する syslog イベントの収集を開始します。

CA Enterprise Log Manager が syslog イベントを受信しているかどうかの確認

次の手順を使用して、デフォルト エージェントのコネクタが syslog イベントを収集しているかどうかを確認できます。

syslog イベントの受信を確認する方法

1. CA Enterprise Log Manager にログインして、[クエリおよびレポート]タブにアクセスします。
2. [システム]クエリ タグを選択して、[システム全イベント詳細]クエリを開きます。

   コネクタが正しく設定され、イベント ソースがアクティブにイベントを送信していれば、デフォルト エージェントがリストしたイベントが表示されます。

例：ODBCLogSensor を使用した直接収集の有効化

ODBCLogSensor を使用して、特定のデータベースおよび CA 製品によって生成されたイベントの直接収集を有効にすることができます。そのためには、ODBCLogSensor を使用する統合に基づいてデフォルト エージェント上にコネクタを作成します。多くの統合でこのセンサを使用します。たとえば、CA_Federation_Manager、CAIdentityManager、Oracle10g、Oracle9i、MS_SQL_Server_2005 などです。

以下は、CA Enterprise Log Manager サーバ上のデフォルト エージェントによって直接収集可能なイベントを生成する製品の一部を示しています。製品ごとに固有のコネクタが使用され、各コネクタが ODBCLogSensor を使用します。

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i および 10g
- Microsoft SQL Server 2005

完全なリストについては、サポート オンライン上の製品統合マトリックスを参照してください。

この例では、Microsoft SQL Server データベースからのイベントの直接収集を有効にする方法を示します。デフォルト エージェント上に展開されたコネクタは、MS_SQL_Server_2005 統合に基づいています。この例では、SQL Server データベースが ODBC サーバ上に存在しています。CA Enterprise Log Manager エージェントに展開されたコネクタは、MSSQL_TRACE テーブルからイベントを収集します。Microsoft SQL Server データベースからのイベント収集を有効にするには、選択されたイベントがこのトレース テーブルに送信されるようにする必要があります。このための具体的な手順については、Microsoft SQL Server コネクタ ガイドを参照してください。

Microsoft SQL Server イベント ソースを設定する方法

1. [管理]タブ-[ライブラリ]サブタブを選択します。
2. [イベント精製ライブラリ]を展開し、統合、サブスクリプションを展開して、MS_SQL_Server_2005 を選択します。

   [統合の詳細を表示]に、センサ名 ODBCLogSensor が表示されます。サポートされているプラットフォームには Windows と Linux の両方が含まれます。
3. [統合の詳細を表示]上で[ヘルプ]リンクをクリックします。

   Microsoft SQL Server コネクタ ガイドが表示されます。
4. 前提条件および Microsoft SQL Server 設定のセクションを確認します。

イベント ソースを設定してログ記録を確認する方法

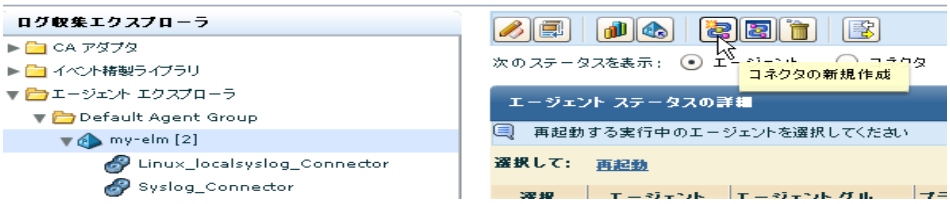
1. 次の詳細を収集します: ODBC サーバの IP アドレス、データベース名、サーバへのログオンに必要な管理者ユーザ名とパスワード、SQL Server 認証に使用される権限レベルの低いユーザの認証情報 (これはトレース テーブルに対して読み取り専用アクセス権限を持つよう定義されたユーザです)。
2. 管理者ユーザ名とパスワードで ODBC サーバにログオンします。
3. Microsoft SQL Server コネクタ ガイドに指定されたとおり、TCP/IP 接続を確認します。
4. SQL Server を設定し、Microsoft SQL Server コネクタ ガイドに指定されたとおり、トレース テーブルにイベントが送信されることを確認します。

   注: 作成するトレース テーブルが含まれるデータベースの名前を記録しておいてください。このデータベース名は接続文字列に指定する必要があります。例: master

ODBC サーバ上の SQL Server データベースによって生成されるイベントを取得するためにデフォルト エージェント上にコネクタを作成する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
2. [エージェント エクスプローラ]を展開し、CA Enterprise Log Manager デフォルト エージェントが含まれるエージェント グループを展開します。
3. デフォルト エージェント、つまり CA Enterprise Log Manager という名前を持つエージェントを選択します。

   デフォルト エージェントには、他のコネクタが展開されている場合があります。
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]ウィザードが開きます。

5. [統合]ドロップダウン リストから MS_SQL_Server_2005 を選択します。

   この選択によって、[コネクタ名]フィールドに「MS_SQL_Server_2005_Connector」が自動入力されます。
6. (オプション) デフォルトの名前を、コネクタの特定が容易になるような名前に変更します。この同じエージェントで複数の SQL Server データベースをモニタしている場合は、一意の名前を指定することを検討します。

7. (オプション) [抑制ルールの適用]をクリックし、サポートされるイベントに関連付けられるルールを選択します。

   たとえば、MSSQL_2005_Authorization 12.0.44.12 を選択します。

8. [コネクタの設定]手順をクリックし、[ヘルプ]リンクをクリックします。

   この手順には、Windows と Linux の両方で必要となる CA Enterprise Log Manager のセンサの設定が含まれます。

9. デフォルト エージェントのプラットフォームである Linux 用の手順を確認し、指定されたとおりに接続文字列および他のフィールドを設定します。

   a. 「センサの設定 -- Linux」に指定されているように接続文字列を入力します。アドレスにはイベント ソースのホスト名または IP アドレスを指定します。データベースは MSSQLSERVER_TRACE が作成される SQL Server データベースです。

      DSN=SQLServer Wire Protocol;Address=*IPaddress*,*port*;Database=*databasename*

   b. 読み取り専用のイベント収集アクセス権を持つユーザの名前を入力します。読み取り専用アクセス権を付与するには、db_datareader ロールと public ロールをユーザに割り当てる必要があります。

   c. 指定したユーザ名のパスワードを入力します。

   d. データベースのタイム ゾーンを、GMT に対する相対値として指定します。

      注: Window サーバで、この情報は[日付と時刻]プロパティの[タイム ゾーン]タブに表示されます。システム トレイ上のクロックを開きます。

   e. [最初から読み取り開始]をオンまたはオフにします。これにより、ログ センサがデータベースの最初からイベントを読み取るかどうかが決まります。

   以下に例を一部示します。

10. [保存して閉じる]をクリックします。

    新しいコネクタ名が[エージェント エクスプローラ]のエージェントの下に表示されます。

11. MS_SQL_Server_2005_Connector をクリックして、ステータス詳細を表示します。

    最初は、ステータスに[設定保留中]が表示されます。そのステータスに[実行中]が表示されるまで待ちます。

コネクタ	エージェント	エージェント グループ	プラットフォーム	統合	ステータス
MS_SQL_Server_2005_コネクタ	my-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	実行中

12. コネクタを選択して[実行中]をクリックし、イベント収集詳細を参照します。

    注: レポートを実行して、このデータベースからのデータを参照することもできます。

デフォルト エージェントがターゲット イベント ソースからイベントを収集していることを確認する方法

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]で[プロンプト]を展開し、[コネクタ]を選択します。
3. コネクタ名を入力し、[実行]をクリックします。

   収集されたイベントが表示されます。最初の 2 つは内部イベントです。続くイベントは、設定した MS SQL トレース テーブルから収集されたイベントです。

   注: 予期されるイベントが表示されていない場合、メイン ツールバーで[グローバル フィルタおよび設定]をクリックし、[時間範囲]を[制限なし]に設定して設定を保存する。
4. (オプション)[元のイベントの表示]を選択し、最初の 2 つのイベントの結果文字列を確認します。結果文字列は元のイベントの最後に表示されます。以下の値は正常に開始されたことを示します。
   - result_string=ODBCSource initiated successfully - MSSQL_TRACE
   - result_string=<connector name> Connector Started Successfully

例：WinRMLinuxLogSensor を使用した直接収集の有効化

Windows アプリケーションまたは Windows Server 2008 オペレーティング システムによって生成されたイベントの直接収集を WinRMLinuxLogSensor で有効にすることができます。そのためには、WinRMLinuxLogSensor を使用する統合に基づいてデフォルト エージェント上にコネクタを作成します。多くの統合でこのセンサを使用します。たとえば Active_Directory_Certificate_Services、Forefront_Security_for_Exchange_Server、Hyper-V、MS_OCS、WinRM などです。WinRMLinuxLogSensor によって取得可能なイベントを生成する Microsoft Windows アプリケーションとオペレーティング システムは、Windows リモート管理が有効なものです。

以下は、CA Enterprise Log Manager サーバ上のデフォルト エージェントによって直接収集可能なイベントを生成する製品の一部を示しています。製品ごとに固有のコネクタが使用され、各コネクタが WinRMLinuxLogSensor を使用します。

- Microsoft Active Directory 証明書サービス
- Microsoft Forefront Security for Exchange Server
- Microsoft Forefront Security for SharePoint
- Microsoft Hyper-V Server 2008
- Microsoft Office Communication Server
- Microsoft Windows Server 2008

完全なリストについては、サポート オンライン上の製品統合マトリックスを参照してください。

以下の例は、WinRM 統合に基づいたコネクタを使用して、イベントの直接収集を有効にする方法を示しています。 そのようなコネクタが展開された場合、Windows Server 2008 オペレーティング システムのイベント ソースからイベントが収集されます。収集が開始されるのは、Windows イベント ビューアにイベントが記録されるようイベント ソースを設定し、サーバに Windows リモート管理を有効にした後です（手順については、この統合に関連するコネクタ ガイドに記載されています）。

Windows Server 2008 イベント ソースの設定方法を確認する方法

1. ［管理］タブ-［ライブラリ］サブタブを選択します。
2. ［イベント精製ライブラリ］を展開し、統合、サブスクリプションを展開して、WinRM を選択します。

   ［統合の詳細を表示］に、センサ名 WinRMLinuxLogSensor が表示されます。サポートされているプラットフォームには Windows と Linux の両方が含まれます。
3. WinRM の［統合の詳細を表示］上の［ヘルプ］リンクをクリックします。

   Microsoft Windows Server 2008 コネクタ ガイド - WinRM が表示されます。

イベント ソースを設定してログ記録を確認する方法

1. Windows Server 2008 オペレーティング システムのターゲット ホストにログオンします。
2. Microsoft Windows Server 2008 CA コネクタ ガイドの説明に従って、イベントが Windows イベント ビューアに表示されること、および Windows リモート管理がターゲット サーバ上で有効であることを確認します。

   注: このプロセスの一環として、コネクタの設定で入力する必要があるユーザ名とパスワードを作成します。これらの認証情報によって、イベント ソースと CA Enterprise Log Manager の間の接続を確立するために必要な認証が有効になります。
3. ログ記録を確認します。
   a. [ファイル名を指定して実行]ダイアログ ボックスから eventvwr を開きます。

      イベント ビューアが表示されます。
   b. Windows ログを展開し、「セキュリティ」をクリックします。

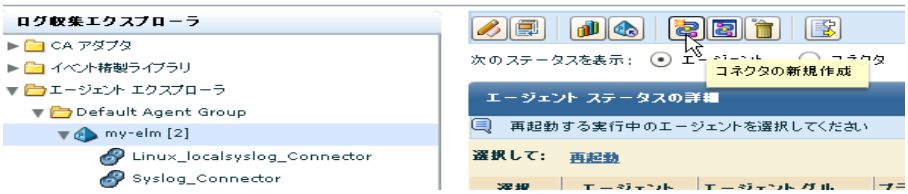
      以下のように表示されていれば、ログ記録が発生していることを示します。

Windows イベント ソースからのイベントの直接収集を有効にする方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。
2. [ログ収集エクスプローラ]で、[エージェント エクスプローラ]を展開し、CA Enterprise Log Manager デフォルト エージェントが含まれるエージェント グループを展開します。
3. デフォルト エージェント、つまり CA Enterprise Log Manager という名前を持つエージェントを選択します。

   デフォルト エージェントには、他のコネクタが展開されている場合があります。

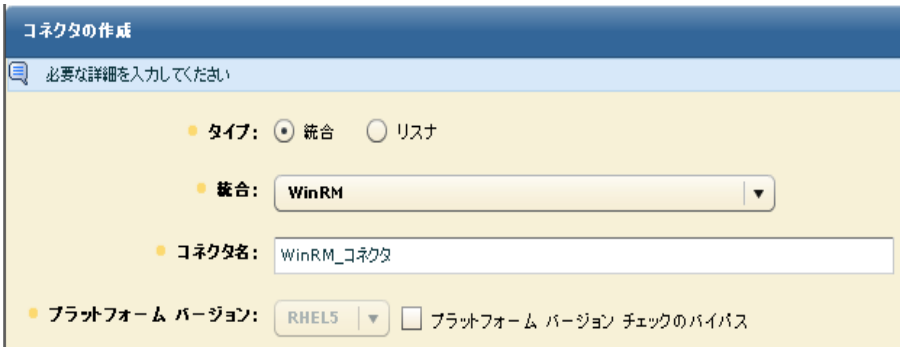
4. [コネクタの新規作成]をクリックします。



[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]ウィザードが開きます。

5. [統合]ドロップダウン リストから WinRM ログ センサを使用する統合を選択します。

たとえば、WinRM を選択します。



この選択によって、[コネクタ名]フィールドに「WinRM_Connector」が自動入力されます。

6. (オプション)[抑制ルールの適用]をクリックし、サポートされるイベントに関連付けられるルールを選択します。

7. [コネクタの設定]手順をクリックし、[ヘルプ]リンクをクリックします。

「CA Enterprise Log Manager センサの設定 -- WinRM」に手順が含まれています。

5.0 CA Enterprise Log Manager センサの設定 - WinRM
5.1 固定パラメータ

8. このコネクタ ガイドの手順に従って、センサを設定します。Windows リモート管理を設定したホストのホスト名ではなく IP アドレスを入力します。ユーザ名とパスワードのエントリには、Windows リモート管理の設定中に追加した認証情報が反映されます。

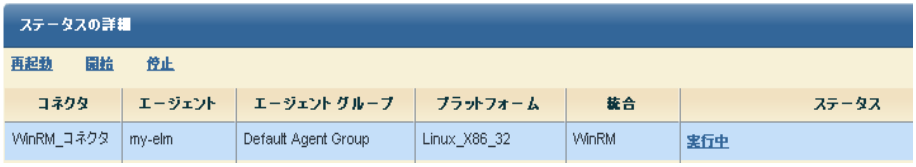
   以下に例を示します。

9. [保存して閉じる]をクリックします。

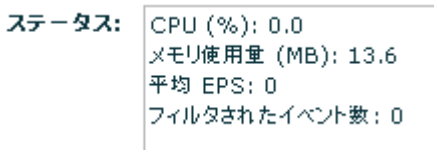
10. 新しいコネクタ名が[エージェント エクスプローラ]のエージェントの下に表示されます。

11. WinRM_Connector をクリックして、ステータス詳細を表示します。

    最初は、ステータスに[設定保留中]が表示されます。そのステータスに[実行中]が表示されるまで待ちます。



12. [実行中]をクリックし、EPS（毎秒イベント）などのサマリ データを取得します。



デフォルト エージェントがターゲット イベント ソースからイベントを収集していることを確認する方法

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]で[プロンプト]を展開し、[コネクタ]を選択します。
3. コネクタ名を入力し、[実行]をクリックします。
4. 収集されたイベントを参照します。

エージェントまたはコネクタのステータスの表示と管理

必要に応じて、環境内のエージェントまたはコネクタのステータスを監視したり、エージェントを再起動したり、コネクタを起動、停止および再起動することができます。

エージェント エクスプローラのフォルダ階層のさまざまなレベルからエージェントまたはコネクタを表示できます。必要に応じて、使用可能なビューを次のようにレベルごとに絞り込みます。

- エージェント エクスプローラ フォルダからは、現在の CA Enterprise Log Manager サーバに割り当てられたすべてのエージェントまたはコネクタを表示できます。
- 特定のエージェント グループ フォルダからは、そのエージェント グループに割り当てられたエージェントとコネクタを表示できます。
- 個々のエージェントからは、そのエージェントに割り当てられたエージェントとコネクタだけを表示できます。

3 つのすべてのレベルからエージェント用の FIPS モード (FIPS または FIPS 非準拠) を指定できます。

エージェントまたはコネクタのステータスを表示する方法

1. [管理]タブをクリックし、[ログ収集]サブタブをクリックします。

   [ログ収集]フォルダ リストが表示されます。
2. [エージェント エクスプローラ]フォルダを選択します。

   詳細ペインにエージェント管理ボタンが表示されます。
3. [ステータスとコマンド]をクリックします。 

   [ステータス]パネルが表示されます。
4. [エージェント]または[コネクタ]を選択します。

   エージェントまたはコネクタの検索パネルが表示されます。

5. (オプション)エージェントまたはコネクタの更新の検索条件を選択します。検索語を入力しない場合は、使用可能な更新がすべて表示されます。検索を絞り込むには、次の条件を 1 つ以上選択できます。
   - [エージェント グループ]: 選択したグループに割り当てられたエージェントおよびコネクタだけを返します。
   - [プラットフォーム]: 選択したオペレーティング システムで実行されているエージェントおよびコネクタだけを返します。
   - エージェントの名前パターン: 指定したパターンを含むエージェントおよびコネクタだけを返します。
   - (コネクタのみ)[統合]: 選択した統合を使用しているコネクタだけを返します。
6. [ステータスの表示]をクリックします。

   詳細なグラフが表示され、検索と一致するエージェントまたはコネクタのステータスが表示されます。以下に例を示します。

   合計: 10 実行中: 8 保留: 1 停止済み: 1 応答なし: 0
7. (オプション)ステータス表示をクリックして、グラフの下にある[ステータス]ペインに詳細を表示します。

   注: エージェントまたはコネクタの[オンデマンド]ボタンをクリックすると、ステータス表示をリフレッシュすることができます。
8. (オプション)コネクタを表示している場合は、任意のコネクタを選択して、[再起動]、[開始]、または[停止]をクリックします。エージェントを表示している場合は、任意のエージェントを選択して、[再起動]をクリックします。

第 7 章: 連携の作成

このセクションには、以下のトピックが含まれています。

連携環境のクエリとレポート

単体の CA Enterprise Log Manager サーバでは、内部のイベント データベースからデータを返してクエリの応答およびレポートの生成を行います。CA Enterprise Log Manager サーバが連携されている場合、連携関係を設定する方法でクエリとレポートがどのようにイベント情報を返信するかを制御できます。また、[連携クエリの使用]グローバル設定を無効にすることにより、1 つのサーバからのクエリ結果を保持できます。

デフォルトでは、グローバル設定[連携クエリの使用]は有効です。これによって、親の CA Enterprise Log Manager サーバからのクエリがすべての子の CA Enterprise Log Manager サーバに送信されます。子の各 CA Enterprise Log Manager サーバは、すべての子の CA Enterprise Log Manager サーバにクエリを実行するほか、アクティブなイベント ログ ストアやアーカイブ カタログにもクエリを実行します。そして、子の CA Enterprise Log Manager サーバは、それぞれ 1 つの結果セットを作成して、要求した親の CA Enterprise Log Manager サーバに送信します。メッシュ構成を実現するため、CA Enterprise Log Manager には循環的なクエリに対する保護が組み込まれています。

一般的な企業では、1 ～ 5 台の CA Enterprise Log Manager サーバを実装します。大企業では、10 台以上のサーバを実装する場合があります。連携を設定する方法によって、クエリを発行する CA Enterprise Log Manager サーバ対してどれくらいの情報を表示するかを制御します。最も単純なクエリ タイプは主要な CA Enterprise Log Manager サーバから送信され、その下に設定されたすべての子サーバからの情報が返されます。

子サーバから連携に対してクエリを実行する場合、表示される結果は連携がどのように設定されたかによって決まります。階層統合では、1 つのサーバの子として設定されたサーバはすべて、親のサーバにクエリ結果を返します。メッシュ統合では、相互接続されたサーバはすべて、クエリを発行したサーバにデータを返します。

階層統合

階層統合では、トップダウンの階層構造を使用して、広い領域にイベント収集の負荷を分散します。この構造は組織図に似ています。作成しなければならないレベル数はありません。ビジネスのニーズに最も適したレベルを作成できます。

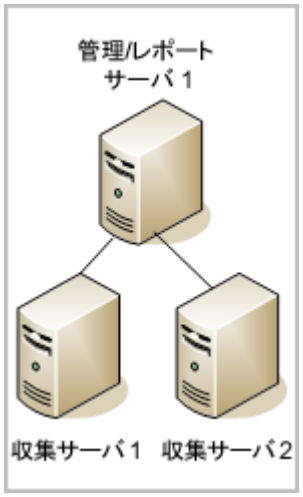
階層統合では、任意の CA Enterprise Log Manager サーバに接続して、そのサーバとその下の任意の子サーバのイベント データに関するレポートおよびデータを表示することができます。アクセス可能なデータのスコープは、階層のどの場所で開始するかによって制限されます。階層の中間で開始すると、そのサーバのデータと、その子サーバのデータのみを表示できます。階層統合の上位ほど、対象のネットワーク データのスコープが広くなります。最上位レベルでは、階層環境全体のすべてのデータにアクセスできます。

階層統合は、地域ごとに展開する場合などに便利です。ローカルのリソースにネットワークの特定の階層またはブランチ内のイベント データにアクセスさせ、同階層の他のブランチのイベント データにはアクセスさせないようにする場合を考えてみます。同階層に 2 つ以上のブランチを持つ階層統合を作成し、各地域のデータを含めます。各ブランチは、すべてのイベント ログ レポートの全体的なビューを作成するために、本社のオフィスにある管理用 CA Enterprise Log Manager サーバにレポートします。

階層統合の例

次の図に示す連携マップのネットワークでは、レポート サーバとして管理用 CA Enterprise Log Manager サーバと、組織図に似た設定の複数の収集サーバを使用しています。管理サーバおよびレポート サーバは親の CA Enterprise Log Manager サーバとして動作し、クエリ、レポートおよびアラートを処理するレポート機能に加えてユーザ認証、許可、および主な管理機能も提供します。この例の収集サーバは、管理/レポート サーバ 1 の子になります。階層に追加のレベルを用意する場合もあります。 一方で、管理サーバは 1 台しか配置できません。追加のレベルは、収集サーバの親としてのレポート サーバで構成します。

このスタイルの連携の例では、管理/レポート サーバ 1 は本社に配置し、収集サーバ 1 および 2 として表された収集サーバは地方または支社に配置できます。 各ブランチでは自分のデータに関するレポート情報を取得できますが、別のブランチからのデータは取得できません。たとえば、収集サーバ 1 では、収集サーバ 1 のみのデータに対してクエリおよびレポートを実行できます。一方で、管理/レポート サーバ 1 では、管理/レポート サーバ 1、収集サーバ 1、および収集サーバ 2 からのデータに対してクエリおよびレポートを実行できます。



階層統合では、各 CA Enterprise Log Manager サーバは 1 つ以上の子を持つことができますが、親は 1 つだけです。このタイプの連携は、管理サーバから始まるトップダウン形式で設定されます。そして下の各階層に移動し、子のレポート サーバおよび収集サーバを設定します。連携の設定で重要なのは、先にサーバのマップと目的とする関係を作成することです。その後に CA Enterprise Log Manager サーバを子サーバとして設定し、そのサーバ間の関係を実装します。

メッシュ統合

メッシュ統合は、階層を作成できるという点で階層統合に似ています。主な違いは、サーバ間の接続の設定にあります。メッシュ統合では、ネットワーク内の任意の CA Enterprise Log Manager サーバが他のすべての CA Enterprise Log Manager サーバのデータに対してクエリを実行し、そのデータのレポートを作成できます。レポート機能はサーバ間に作成された関係に依存します。

たとえばメッシュ統合では、サーバは垂直方向のブランチ内のみで相互に接続できます。つまり、そのブランチのすべての CA Enterprise Log Manager サーバが、同じブランチの他のすべての CA Enterprise Log Manager サーバにアクセスできます。これは階層統合の CA Enterprise Log Manager サーバとは正反対です。階層統合の CA Enterprise Log Manager サーバは、階層内で自分の下位にあるサーバのみに関するレポートを作成できます。

リング型またはスター型では、すべての CA Enterprise Log Manager サーバは他のすべてのサーバの子として設定されます。任意の 1 つの CA Enterprise Log Manager サーバにレポート データを要求すると、ネットワークのすべての CA Enterprise Log Manager サーバのデータが表示されます。

メッシュ統合では、2 つ以上の CA Enterprise Log Manager サーバをプライマリとして割り当てて、ネットワーク内の配置を考慮せずに連携内のサーバを使用します。子として設定されたサーバも、サーバに連携されると、同じブランチまたは他のブランチにある子を表示するように設定されます。たとえば、2 つの CA Enterprise Log Manager サーバ A と B があり、B を A の子にし、かつ A を B の子にすることで、メッシュ統合を作成できます。これは、2 つ以上の管理サーバを使用している場合を想定した設定です。

メッシュ統合の例

次の完全なメッシュ統合の図を考えてみます。

この図に示されているメッシュ統合では、4 つの収集サーバが互いに連携され、さらに 2 つのレポート サーバとも連携されています。連携内では、すべてのサーバが他のサーバの親となり、子にもなります。

厳密な階層統合に対してメッシュ統合を展開する場合の潜在的な利点とは、階層を意識せずにメッシュ内の任意のポイントからデータにアクセスでき、そのメッシュ内の他のすべての CA Enterprise Log Manager サーバから結果を得ることができるという点です。

メッシュ統合と階層統合を組み合わせることで、ニーズに合った任意の構成を作ることができます。たとえば、単一のブランチ内でメッシュ状の構成を使用すると、グローバルな展開の場合に非常に便利です。親のレポート サーバからはデータをグローバルに俯瞰できる一方で、地域クラスタ(ブランチ)を作成して、対象地域のデータにだけアクセスするようにできます。

CA Enterprise Log Manager の連携の設定

連携関係にある CA Enterprise Log Manager サーバはすべて、管理サーバ上の同じアプリケーション インスタンス名を参照する必要があります。 管理サーバは、この方法で、すべての設定をグローバル設定として一緒に保存して管理できます。

連携はいつでも設定できますが、統合されたレポートが必要な場合は、レポートのスケジュールを開始する前に設定すると便利です。

連携の設定には以下のアクティビティが含まれます。

1. 連携マップを作成します。
2. 最初の CA Enterprise Log Manager を管理サーバとしてインストールします。
3. 1 つ以上の追加のサーバをインストールします。
4. 親/子関係を設定します。たとえば最初に、このサーバのイベント ログ ストアの設定から、管理サーバの連携の子を選択します。

   階層統合を設定する場合、この子サーバの最初のグループが連携の 2 番目の層を形成します。
5. [連携グラフ]を表示して、親の層と子の層で、サーバ間の構造が意図したとおりになっていることを確認します。

子サーバとしての CA Enterprise Log Manager サーバの設定

ある CA Enterprise Log Manager サーバを別のサーバの子として設定することは、連携を作成する場合の重要な手順です。連携にサーバを追加するには、常に以下の手順に従います。設定のこの部分を実行する前に、登録済みの同じアプリケーション インスタンス名の下で連携する CA Enterprise Log Manager サーバをすべてインストールする必要があります。新しいサーバをそれぞれインストールすると、連携で使用可能なサーバのリストにその名前が表示されます。この手順は、必要な連携構造を作成するのに何度でも実行できます。

子サーバとして CA Enterprise Log Manager サーバを設定する方法

1. 目的の連携で、同じアプリケーション インスタンス名で登録された複数の CA Enterprise Log Manager サーバのいずれかにログインします。
2. [管理]タブをクリックして、[サービス]サブタブを選択します。

3. [イベント ログ ストア]サービスのフォルダを展開し、親の CA Enterprise Log Manager サーバのサーバ名を選択します。
4. [連携の子]リストまでスクロールします。
5. [使用可能]リスト内のサーバから、上記の親サーバの子として設定するサーバ名を 1 つ以上選択します。
6. 矢印ボタンを使用して、選択対象を[選択されたサーバ]リストに移動します。

   選択し、リストに移動した CA Enterprise Log Manager サーバが、親サーバに連携された子になります。

詳細情報:

連携クエリの使用の選択 (P. 154)

連携グラフおよびサーバ ステータス監視の表示

グラフを表示して、環境内にある CA Enterprise Log Manager サーバ、その連携関係、および個々のサーバのステータス情報を確認できます。連携グラフを使用すると、現在の連携構造を表示したり、各サーバの詳細を表示したりできます。また、そのセッション内でクエリを実行するローカル サーバを選択し、そのローカル サーバを親サーバとして設定できます。

連携グラフを表示するには、画面の一番上にある[連携グラフの表示]と[ステータス監視]をクリックします。 

ウィンドウが開き、現在の管理サーバに登録されているすべてのイベント ストア ホストがグラフィカルに表示されます。

- 連携の子を持つイベント ストアは水色で表示され、連携関係は黒い接続線で表示されます。
- 連携の子を持たないイベント ストアは薄い緑色で表示されます。

クエリを行う現在のローカル サーバを選択できます。

また、表示されたサーバについては、どれもステータス詳細を表示できます。連携グラフ内のサーバをクリックすると、以下のようなステータス詳細を表示できます。

- CPU 使用率(%)
- 使用可能なメモリの使用率(%)
- 使用可能なディスク容量の使用率(%)
- 秒あたりの受信イベント数
- イベント ログ ストア ステータスのマスタ グラフ

詳細情報:

例: 中規模企業向けの連携マップ (P. 39)
例: 大企業向けの連携マップ (P. 37)

第 8 章: イベント精製ライブラリの使用

このセクションには、以下のトピックが含まれています。

イベント精製ライブラリについて

イベント精製ライブラリは、新しい解析ファイルやマッピング ファイルを作成するほか、新しいデバイスやアプリケーションなどをサポートするために既存のファイルのコピーを変更するツールを提供します。このライブラリには次のオプションがあります。

- 統合
- リスナ
- 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

抑制ルールは、データが収集されないようにしたり、データがイベント ログ ストアに挿入されないようにしたりします。集約ルールは、タイプの似たイベントまたはアクションの挿入回数を減らすために、イベントを集約できるようにします。抑制ルールと集約ルールはネットワークとデータベースの両方のパフォーマンスを調整するのに役立つため、ライブラリで最も頻繁に使用される機能です。

統合の領域を使用して、事前定義済み統合を表示したり、カスタムまたは専用のデバイス、アプリケーション、ファイルまたはデータベース用の新しい統合を作成したりできます。詳細は、「CA Enterprise Log Manager 管理ガイド」およびオンライン ヘルプで説明しています。

イベント精製ライブラリによる新規イベント ソースのサポート

まだサポートされていないデバイス、アプリケーション、データベース、またはその他のイベント ソースをサポートするには、マッピングのウィザードや解析ファイルのウィザードおよび統合ウィザードを使用して、必要なコンポーネントを作成します。

このプロセスには、次のような一般的な手順が含まれます。

1. 解析ファイルを作成し、イベント データを名前と値のペアとして収集する
2. マッピング ファイルを作成し、名前と値のペアを共通イベント文法にマッピングする
3. 新しい統合とリスナを作成し、イベント ソースからデータを収集する

統合、解析ファイルとマッピング ファイル、および抑制と集約のルールについては、「CA Enterprise Log Manager 管理ガイド」とオンライン ヘルプを参照してください。

マッピング ファイルおよび解析ファイル

CA Enterprise Log Manager は、実行中に受信イベントを読み取り、それを解析と呼ばれるアクションでセクションに分割します。さまざまなデバイス、オペレーティング システム、アプリケーション、およびデータベースに対して個別のメッセージ解析ファイルがあります。 受信イベントが名前と値のペアに解析されると、そのデータはデータベースのフィールドにイベント データを配置するマッピング モジュールを経由します。

マッピング モジュールは、メッセージ解析ファイルと同様に、特定のイベント ソース用に作成されたデータマッピング ファイルを使用します。データベース スキーマには CA Enterprise Log Manager の中心的な機能の 1 つである共通イベント文法が使用されます。

解析およびマッピングは、イベント タイプやメッセージ フォーマットにかかわらず、共にデータを標準化して共通のデータベースに保存するための手段です。

統合ウィザードと CA アダプタ モジュールの一部にはマッピング ファイルおよび解析ファイルを設定し、コネクタまたはアダプタが待ち受けるイベント データの種類について最適な記述をする必要があります。これらのコントロールが表示される設定パネルでは、メッセージ解析ファイルの順序が受信されるそのタイプのイベントの相対的な数を反映しています。また、データ マッピング ファイルの順序は、特定のソースから受信したイベントの量を反映しています。

たとえば、特定の CA Enterprise Log Manager サーバの syslog リスナ モジュールが受信した大部分が Cisco PIX ファイアウォールのイベントである場合、それぞれの対応するリストには CiscoPIXFW.XMPS ファイルおよび CiscoPIXFW.DMS ファイルが 1 番目に入ります。

付録 A: CA Audit ユーザに関する考慮事項

このセクションには、以下のトピックが含まれています。

アーキテクチャの違いについて

ICA Audit と CA Enterprise Log Manager を一緒に使用する方法を計画する場合は、最初にアーキテクチャの違いとネットワーク構造に与える影響を理解する必要があります。

CA Enterprise Log Manager は組み込みのイベント ログ ストアを使用し、エージェントを設定して管理するためのエージェント エクスプローラを提供します。共通イベント文法と組み合わされた新技術を使用すると、多くのイベント ソースをサポートする一方で、ストレージへのイベント スループットをより速くすることができます。CA Enterprise Log Manager は共通イベント文法を使用してさまざまなイベント ソースからのイベントを単一のデータベース スキーマに標準化できます。

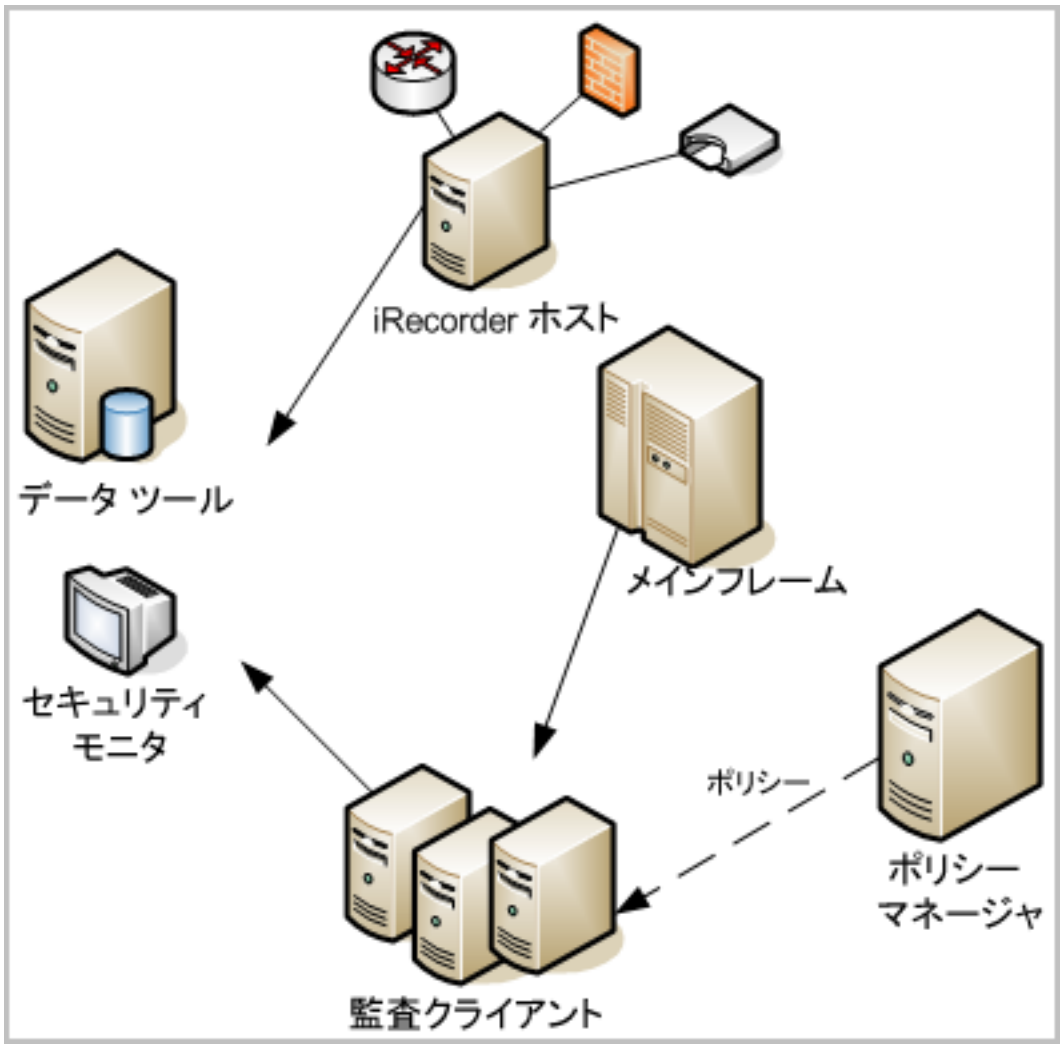
CA Enterprise Log Manager は一定のレベルで CA Audit を統合しています。しかし、意図的に完全には相互運用可能ではありません。CA Enterprise Log Manager は、CA Audit と並行して実行できる新しい個別のサーバ インフラストラクチャですが、イベント処理に関しては次の考慮事項があります。:

CA Enterprise Log Manager で実行されること	CA Enterprise Log Manager では実行されないこと
設定可能なリスナを使用して、CA Audit クライアントおよび iRecorder から送信されたイベント ログを受信します。	CA Audit コレクタ データベースに保存されたイベント ログに直接アクセスします。
CA Audit コレクタ データベース（SEOSDATA テーブル）に保存されたイベント ログ データをインポートするためのユーティリティを提供します。	

CA Enterprise Log Manager で実行されること	CA Enterprise Log Manager では実行されないこと
エージェントを使用して、CA Enterprise Log Manager サーバ インフラストラクチャにのみイベント ログを送信します。	
CA Enterprise Log Manager エージェントおよび iRecorder を持つ CA Audit クライアントを同じ物理ホスト上で実行できます。	CA Enterprise Log Manager エージェントおよび同じホストに iRecorder を持つ CA Audit クライアントが、同じログ ソースに同時にアクセスできます。
組み込みのエージェント エクスプローラを使用して、CA Enterprise Log Manager エージェントのみを管理します。2 つのシステムが同時に操作を行っている間、CA Audit はポリシー マネージャを使用して CA Audit クライアントの管理のみを行います。	
	テーブル コレクタに保持された CA Audit データ、レポート テンプレートまたはカスタム レポート、アラート ポリシー、収集/フィルタリング ポリシー、またはロールベースのアクセス制御ポリシーを移行します。

CA Audit のアーキテクチャ

次の図は、簡略化された CA Audit の実装を示しています。



一部の企業の CA Audit の展開では、イベント データはデータ ツール サーバで実行されているリレーショナル データベースのコレクタ サービスによって保存されます。データベース管理者はこのデータベースを監視して管理し、システム管理者と協力して、必要なイベントを収集し不要なイベントを除外するための適切なポリシーが確実に実施されるようにします。

この図にある実線は、CA Audit クライアント、レコーダ、および iRecorder ホストからデータ ツール サーバまで、場合によってはオプションのセキュリティ モニタ コンソールまでのイベント フローを示しています。点線は、ポリシー マネージャ サーバとポリシーを使用しているクライアントの間の制御フローを表します。

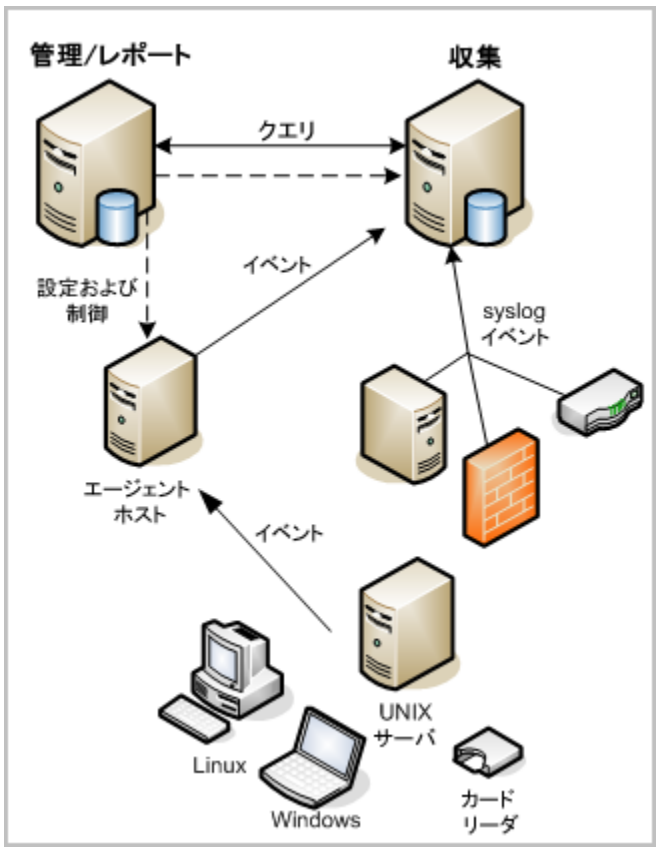
データ ツール サーバは、イベントの保存に加えて、基本的なレポートと視覚化ユーティリティも提供します。企業の実装ではカスタム クエリとレポートは標準的で、作成と管理には多くの時間が必要です。

このネットワークトポロジを使用すると、多様なデバイス、アプリケーション、およびデータベースからのさまざまなイベント タイプの収集できます。収集されたイベントの集中ストレージがあり、通常は一部のレポートを提供するデータ ツール サーバの一部であるか、データ ツール サーバによって管理されます。

ただし、急速に増加するイベント ボリュームを処理するには、ソリューションの規模を大きくする追加の機能が必要です。さまざまな連邦規制および国際規制へのコンプライアンスを実証するレポートを生成する必要があります。また、それらのレポートを迅速かつ容易に見つけることができる必要があります。

CA Enterprise Log Manager アーキテクチャ

次の図は、2 台のサーバを使用する CA Enterprise Log Manager の基本的な実装を示しています。



CA Enterprise Log Manager システムでは 1 つ以上のサーバを使用することができ、最初にインストールされたサーバが管理サーバになります。1 つのシステムでは 1 つの管理サーバしか使用できませんが、複数のシステムを作成できます。管理サーバはすべての CA Enterprise Log Manager サーバのコンテンツと設定を管理し、ユーザ認証と許可を実行します。

また、2 台のサーバを使用する基本的な実装では、管理サーバはレポート サーバとしての役割も果たします。レポート サーバは、1 つ以上の収集サーバの精製済みイベントを受信します。レポート サーバは、スケジュール済みアラートやレポートに加えて、オンデマンドのクエリやレポートも処理します。収集サーバは、収集したイベントの精製を実行します。

各 CA Enterprise Log Manager サーバには、独自の内部イベント ログ ストア データベースがあります。イベント ログ ストアは、ストレージ容量を増やすために圧縮された専用のデータベースで、アクティブなデータベース ファイル、アーカイブするようにマーク付けされたファイル、および解凍されたファイルのクエリを実行できます。イベントを保存するためにリレーショナル DBMS パッケージは必要ありません。

収集用 CA Enterprise Log Manager サーバは、デフォルト エージェントを使用するか、イベント ソースに存在するエージェントから、直接イベントを受信できます。また、VPN コンセントレータまたはルータ ホストに関しては、ネットワークの他のイベント ソースのコレクタとして動作するホストでエージェントを使用できます。

この図にある実線は、イベント ソースからエージェント、収集サーバ、管理サーバ/レポート サーバのレポート ロールまでのイベント フローを表しています。点線は、CA Enterprise Log Manager サーバ間、および管理サーバ/レポート サーバの管理ロールからエージェントへの設定および制御トラフィックを示しています。インストール時に CA Enterprise Log Manager サーバが管理サーバに同じアプリケーション インスタンス名で登録されている限り、ネットワーク内の任意の CA Enterprise Log Manager サーバを使用してネットワーク内の任意のエージェントを制御できます。

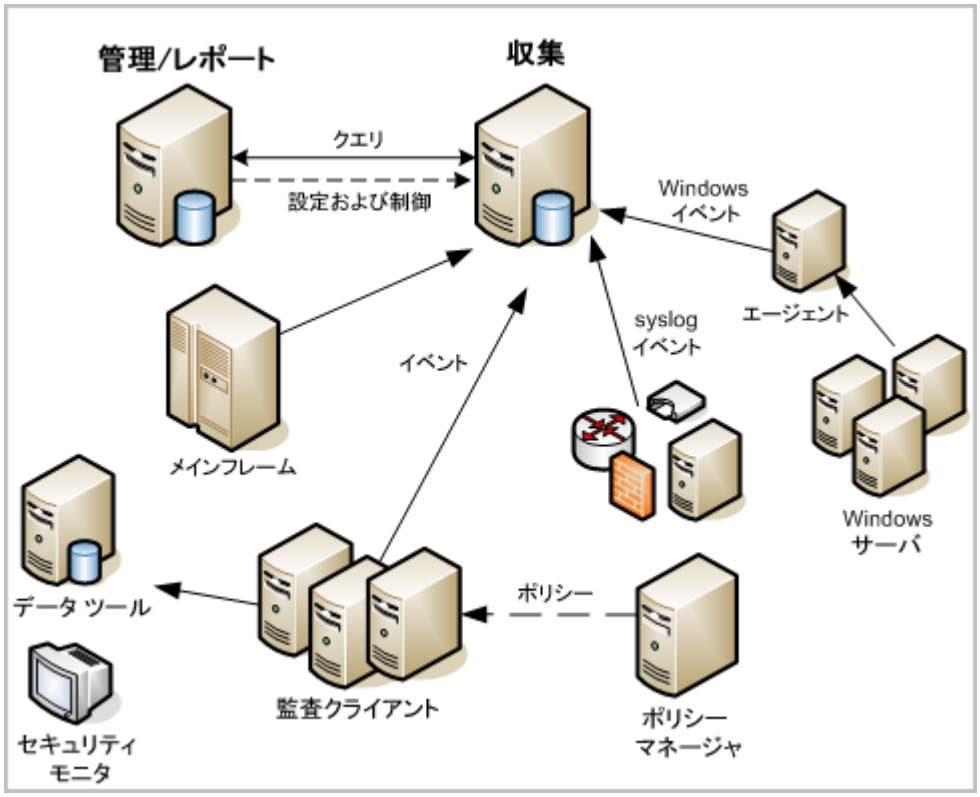
エージェントは、コネクタを使用してイベントを収集します（図では示されていません）。1 つのエージェントが複数のコネクタを管理し、同時に複数の異なるタイプのイベントを収集できます。つまり、個々のイベント ソースに導入された 1 つのエージェントで、さまざまなタイプの情報を収集できます。また、CA Enterprise Log Manager サーバは、CA Audit ネットワークから既存の iRecorder および SAPI レコーダを使用して他の CA アプリケーションからのイベントを収集できるリスナを提供します。

CA Enterprise Log Manager サーバを連携させてソリューションを拡張したり、領域外にそのデータを転送せずに、サーバ間のレポート データを共有することができます。これにより、データの物理的な保存場所の管理に関する規制に従いながら、コンプライアンスに関するネットワーク全体のビューを表示できます。

事前定義済みクエリとレポートに対してサブスクリプションの更新を行うことにより、手動でクエリとレポートを管理する必要はありません。付属のウィザードを使用すると、サードパーティ デバイスやまだサポートされていないアプリケーションの独自のカスタム統合を作成できます。

統合のアーキテクチャ

次の図に、大量のイベント処理およびコンプライアンス ベースのレポート機能を活用するために追加された CA Enterprise Log Manager を備えた、典型的な CA Audit ネットワークを示します。



CA Enterprise Log Manager では、統合されたエージェント エクスプローラ、組み込みのイベント ログ ストア、および 1 つのユーザ インターフェースを使用して、ログ収集を集中化および簡略化しています。共通イベント文法と組み合わされた CA Enterprise Log Manager エージェントの技術を使用すると、多くのイベント ソースを処理する一方で、ストレージへのイベント スループットをより高速化できます。1 つのエージェントはイベント ソースへの複数のコネクタを処理し、エージェント管理作業を簡略化したり、よく使用されるイベント ログ ソースまたは共通のイベント ログ ソースの事前定義済み統合を利用できます。

この実装では、CA Enterprise Log Manager 収集サーバは syslog イベント、iTechnology ベースのイベント、および SAPI レコーダのイベントを直接受信します。収集サーバは、個別の Windows ベースの CA Enterprise Log Manager エージェントを使用して、Windows イベント ソースからイベントを受信します。ネットワークに複数のエージェントを展開できます。各エージェントはコネクタを使用してさまざまな種類のイベント データを収集できます。これによって、SEOSDATA データベースへのイベントトラフィックを削減し、CA Enterprise Log Manager で使用可能なクエリおよびレポートを活用できます。単純なポリシー ルールの変更によって、CA Audit クライアントはデータ ツール サーバと CA Enterprise Log Manager サーバの両方で収集されたイベントを送ることができます。

CA Enterprise Log Manager では多くのスループットに加えて標準装備のクエリおよびレポートを提供し、PCI（DSS）や SOX などの複数の基準に関するコンプライアンスを実証できます。事前定義済みのクエリとレポートを既存の CA Audit と CA Security Command Center の実装に結び付ける場合、CA Enterprise Log Manager レポートと多くのスループットを利用しながら、カスタム ソリューションへの投資を活用できます。

CA アダプタの設定

CA アダプタとはリスナのグループで、iTechnology を使用してネイティブでイベントを送信するイベント ソースに加えて、CA Audit クライアント、iRecorder、および SAPI レコーダなどのレガシー コンポーネントからイベントを受信します。

CA Audit ポリシーまたは iRecorder の設定を変更する前に、CA アダプタのオプションを設定します。これによって、イベントが到着する前に確実にリスナ プロセスが動作している状態になります。また、イベント データが誤ってマッピングされることを防ぎます。

iRecorder を使用して CA Audit にイベントを送信する場合、または iRecorder を持つ CA Audit クライアントを使用する場合は、CA Enterprise Log Manager SAPI アダプタを使用してイベントを受信します。CA Enterprise Log Manager にイベントを送信するには、CA Access Control イベント用の既存の CA Audit ポリシーを変更します。既存のルールに、コレクタ アクションまたはルート アクションのいずれかを追加できます。

- 既存の CA Audit ポリシーのルールにコレクタ アクションを作成する場合は、SAPI コレクタの CA アダプタを設定してイベントを受信します。
- 既存の CA Audit ポリシーのルールにルート アクションを作成する場合は、SAPI ルータの CA アダプタを設定してイベントを受信します。

CA Enterprise Log Manager に直接イベントを送信するように再設定する方法の手順については、SAPI のソースドキュメントを参照してください。

スタンド アロンの iRecorder をインストールする場合、または既存の iRecorder を使用する場合は、iTech イベント プラグインを設定してイベントを受信します。たとえば、CA Audit をインストールしておらず、一方で CA iRecorder を使用してサポートされているイベント ソースからイベントを収集する場合は、このアプローチを使用します。このプロセスには次のような手順が含まれます。

- iTechnology イベント プラグインの設定
- CA Enterprise Log Manager サーバに直接イベントを送信する iRecorder または iTechnology ベースの製品の設定

SAPI ルータおよびコレクタについて

通常、SAPI サービスは既存の CA Audit クライアントと統合された製品からのイベントを受信するために使用されます。CA Enterprise Log Manager は、SAPI リスナ サービスの 2 つのインスタンスを使用します。一方 SAPI コレクタとしてインストールされ、もう一方は SAPI ルータとしてインストールされます。

SAPI モジュールでは、コマンドおよび管理に iGateway デーモンを使用します。このモジュールは SAPI ルータおよび SAPI コレクタとして動作し、静的なポートまたはポートマップ機能を使用した動的ポートのいずれかを使用します。

監査コレクタのアクションで組み込みのフェイルオーバー サポートを使用できるように、CA Audit クライアントからイベントを送信する場合に SAPI コレクタを使用します。

CA Audit クライアントからルート アクションを使用してイベントを送信する場合、あるいは <SAPI レコーダまたは CA Audit クライアントにイベントを直接送信できる統合からイベントを送信する場合は、SAPI ルータを使用します。この場合は、まるで CA Enterprise Log Manager サーバが CA Audit クライアントであるかのようにリモート送信者を設定します。

SAPI リスナは自身のポートをパッシブ オープンにして、新しいイベントが送信されるのを待ち受けます。SAPI モジュールの各インスタンスには、次の内容を指定する独自の設定があります。

- 待ち受けポート
- ロードするデータ マッピング（DM）ファイル
- 使用する暗号化ライブラリ

イベントを受信したら、モジュールはそれをマッピング ライブラリに送信し、CA Enterprise Log Manager はそれをデータベースに挿入します。

重要: データ マッピング ライブラリには、同じ名前である一方でバージョン番号が異なる 1 つ以上のマッピング ファイルが含まれることがあります。オペレーティング システム、データベースなど、同じイベント ソースでリリース レベルが異なる場合は別々のファイルでサポートします。SAPI コレクタまたはルータを設定する場合は、バージョンに関連するマッピング ファイルを 1 つだけ選択することが重要です。

選択されたマッピング ファイルのリストの中に同じ名前を持つファイルが 2 つある場合、マッピング エンジンはリストの最初のファイルだけを使用します。それが受信イベントのストリームにとって適切なファイルでない場合は、マッピング エンジンがイベントを正しくマッピングできません。これによって、誤ってマッピングされたイベントを含まない情報、またはイベントがまったく含まれない情報がクエリやレポートに表示される可能性があります。

SAPI コレクタ サービスの設定

SAPI コレクタ サービスを設定するには、以下の手順に従います。

コレクタ アクションを使用する CA Audit ポリシー を変更して、CA Audit コレクタ データベースへのイベントの送信に加えて(またはその代わりに)、CA Enterprise Log Manager サーバにイベントを送信できます。イベントの消失を防ぐため、監査ポリシーを変更する前にこのサービスを設定します。

SAPI コレクタ サービスを設定する方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブを選択します。

   デフォルトでは[ログ収集]サブタブが表示されます。
2. CA アダプタのエントリを展開します。
3. [SAPI コレクタ]サービスを選択します。
4. 各フィールドの説明については、オンライン ヘルプを参照してください。
5. 設定が終了したら、[保存]をクリックします。

SAPI ルータ サービスの設定

SAPI ルータ サービスを設定するには、以下の手順に従います。

他の宛先へのイベントのルーティングに加えて(またはその代わりに)、ルート アクションを使用する CA Audit ポリシーを変更して CA Enterprise Log Manager サーバにイベントを送信できます。また、設定ファイルを変更することにより、SAPI ルータリスナに直接送信するように SAPI レコーダ イベントをリダイレクトすることもできます。イベントの消失を防ぐため、監査ポリシーまたは SAPI レコーダの設定を変更する前にこのサービスを設定します。

SAPI ルータ サービスを設定する方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブを選択します。

   デフォルトでは[ログ収集]サブタブが表示されます。
2. CA アダプタのエントリを展開します。
3. SAPI ルータ サービスを選択します。
4. 各フィールドの説明については、オンライン ヘルプを参照してください。
5. 設定が終了したら、[保存]をクリックします。

iTechnology イベント プラグインについて

iTechnology イベント プラグインは、iGateway イベントの処理メカニズムを使用して送信されたイベントを受信します。環境が次のいずれかに該当する場合は、iTechnology イベント プラグインを設定します。

- 同じシステムに CA Audit クライアントが存在しないネットワークに、既存の iRecorder がある
- iTechnology によってイベントを転送できる CA EEM などの他の製品が存在する

このサービスは、イベントを受信するとそれをマッピング ライブラリに送信し、その後に CA Enterprise Log Manager はマッピングされたイベントをイベント ログ ストアに挿入します。

iTechnology イベント プラグインの設定

iRecorder および他の iTechnology イベント ソースから受信するための iTechnology イベント プラグインを設定するには、以下の手順に従います。

iTechnology プラグインは、イベントを CA Enterprise Log Manager サーバに送信するようにスタンドアロンの iRecorder を設定する場合に使用します。イベントの消失を防ぐため、iRecorder を設定またはインストールする前に、このサービスを設定します。

注: 外部クライアントから iTechnology イベント プラグイン リスナにイベントを送信する場合、これらのイベントはセカンダリ CA Enterprise Log Manager サーバにのみ送信する必要があります。

iTechnology イベント プラグインを設定する方法

1. CA Enterprise Log Manager サーバにログインして、[管理]タブを選択します。

   デフォルトでは[ログ収集]サブタブが表示されます。

2. CA アダプタのエントリを展開します。

3. iTechnology イベント プラグインサービスを選択します。
4. [使用可能な DM ファイル]リストから 1 つ以上のデータ マッピング(DM)ファイルを選択し、矢印を使用してそのファイルを[選択した DM ファイル]リストに移動します。

   イベント プラグイン サービスは、主なデータ マッピング ファイルの大部分を含むようにあらかじめ設定されています。
5. [保存]をクリックして管理サーバの設定ファイルへの変更を保存します。

CA Enterprise Log Manager への CA Audit イベントの送信

次の方法で、既存の CA Audit の実装に CA Enterprise Log Manager を統合できます。

- CA Enterprise Log Manager にイベントを送信するには、CA Audit クライアントと同じホストに存在しない iRecorder を再設定します
- CA Audit と CA Enterprise Log Manager の両方にイベントを送信するように、既存の CA Audit ポリシーを変更します

イベントを CA Enterprise Log Manager に送信するための iRecorder の設定

CA Enterprise Log Manager は iRecorder から iTech イベント プラグイン リスナを経由してイベントを受信します。iRecorder の設定を変更する前に、リスナを設定する必要があります。設定しない場合、イベント データが失われることがあります。リスナを設定したら、次の手順を使用して CA Enterprise Log Manager サーバにイベントを送信するように iRecorder を設定します。

CA Audit クライアントと同じコンピュータにインストールされる iRecorder は、クライアントにイベントを直接送信します。これらのマシンについては、SAPI コレクタまたはルータのアダプタを使用する必要があります。

重要: スタンド アロンの iRecorder は、1 つの宛先のみにイベントを送信することができます。次に示す手順を使用して iRecorder を再設定すると、イベントが CA Enterprise Log Manager イベント ログ ストアにのみ保存されます。イベント ログ ストアと CA Audit コレクタ データベースの両方にイベントを保持する必要がある場合は、既存のポリシーのルール アクションを変更するか、CA Audit クライアントに新しいポリシーを作成します。

CA Enterprise Log Manager にイベントを送信するように iRecorder を設定する方法

1. 管理者権限を持つユーザとして、iRecorder をホストするサーバにログインします。
2. オペレーティング システムの次のディレクトリに移動します。
   - UNIX または Linux の場合: /opt/CA/SharedComponents/iTechnology
   - Windows の場合: ¥Program Files¥CA¥SharedComponents¥iTechnology
3. 次のコマンドを使用して、iGateway デーモンまたはサービスを停止します。
   - UNIX または Linux の場合: ../S99igateway stop
   - Windows の場合: net stop igateway
4. iControl.conf ファイルを編集します。
5. RouteEvent の値を次のように指定します。

   ```
   <RouteEvent>true</RouteEvent>
   ```

   このエントリは、すべての iRecorder イベントを含むイベントを RouteHost タグのペアに指定されたホストに送信するように、iGateway に指示します。
6. RouteHost の値を次のように指定します。

   ```
   <RouteHost>CA_ELM_hostname</RouteHost>
   ```

   このエントリは、DNS 名を使用して CA Enterprise Log Manager サーバにイベントを送信するように iGateway に指示します。
7. 次のコマンドを使用して、iGateway デーモンまたはサービスを再起動します。
   - UNIX または Linux の場合: ./S99igateway start
   - Windows の場合: net start igateway

   このアクションによって iRecorder は強制的に新しい設定を使用し、iRecorder から CA Enterprise Log Manager サーバへのイベント フローを開始します。

詳細情報:

SAPI ルータおよびコレクタについて (P. 242)
SAPI コレクタ サービスの設定 (P. 244)
SAPI ルータ サービスの設定 (P. 244)

CA Enterprise Log Manager にイベントを送信するための既存の CA Audit ポリシーの変更

CA Audit クライアントが CA Enterprise Log Manager と CA Audit コレクタ データベースの両方にイベントを送信できるようにするには、次の手順を使用します。既存のルールのルート アクションまたはコレクタ アクションに新しいターゲットを追加すると、収集されたイベントを両方のシステムに送信できます。または、特定のポリシーまたはルールを変更して、CA Enterprise Log Manager サーバのみにイベントを送信することもできます。

CA Enterprise Log Manager は CA Audit SAPI ルータおよび CA Audit SAPI コレクタのリスナを使用して CA Audit クライアントからのイベントを収集します。収集されたイベントは、ポリシーをクライアントにプッシュした後、ポリシーが有効になってから CA Enterprise Log Manager のイベント ログ ストアに保存されます。

重要: ポリシーを変更して有効にする前に、CA Enterprise Log Manager リスナがイベントを受信するように設定する必要があります。この設定を最初に行わないと、ポリシーが有効になった時間とリスナがイベントを正しくマッピングできるようになった時間との間にイベントを受信した場合に、イベントが正確にマッピングされない可能性があります。

既存のポリシー ルールのアクションが CA Enterprise Log Manager にイベントを送信するように変更する方法

1. ポリシー マネージャ サーバにログインし、左側のペインの[マイ ポリシー]タブにアクセスします。
2. 必要なポリシーが表示されるまで、ポリシー フォルダを展開します。
3. ポリシーをクリックして、右側の[詳細]ペインに基本情報を表示します。
4. ポリシーのルールに追加するには、[詳細ペインで編集]をクリックします。ルール ウィザードが起動します。
5. ウィザードの手順 3 で、矢印の隣の[アクションの編集]をクリックします。ウィザードの[ルール アクション]ページが表示されます。
6. 左側の[アクションの参照]ペインで[コレクタ]アクションをクリックします。右側に[アクション リスト]が表示されます。

   さらに、ルート アクションを使用して CA Enterprise Log Manager サーバにイベントを送信するルールを作成できます。
7. [新規]をクリックして新しいルールを追加します。

8. 収集用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。

   2 つ以上のサーバを使用する CA Enterprise Log Manager 実装の場合、[代替ホストの名前]フィールドに異なる CA Enterprise Log Manager のホスト名または IP アドレスを入力して、<Aus> の自動フェイルオーバー機能を利用できます。最初の CA Enterprise Log Manager サーバが使用できない場合、CA Audit は自動的に[代替ホストの名前]フィールドに指定されたサーバにイベントを送信します。

9. [代替ホストの名前]フィールドに管理用 CA Enterprise Log Manager サーバの名前を入力してから、この新しいルール アクションの説明を作成します。

10. [このアクションをリモート サーバで実行]チェック ボックスがオンの場合は、このチェック ボックスをオフにします。

11. [追加]をクリックして新しいルール アクションを保存し、ウィザード ウィンドウで[完了]をクリックします。

12. 右下のペインの[ルール]タブを選択してから、チェックするルールを選択します。

13. [ポリシーのチェック]をクリックして、新しいアクションを追加して変更したルールをチェックし、正常にコンパイルされることを確認します。

    ルールに対して必要な変更を行い、ルールを有効にする前に正常にコンパイルされることを確認します。

14. [有効にする]をクリックして、追加した新しいルール アクションを含むチェック済みのポリシーを配布します。

15. CA Enterprise Log Manager に送信するイベントを収集するルールおよびポリシーのそれぞれに対して、この手順を繰り返します。

詳細情報:

SAPI ルータおよびコレクタについて (P. 242)
SAPI コレクタ サービスの設定 (P. 244)
SAPI ルータ サービスの設定 (P. 244)

CA Enterprise Log Manager にイベントを送信するための r8 SP2 ポリシーの変更

r8 SP2 の CA Audit クライアントが CA Enterprise Log Manager と CA Audit コレクタ データベースの両方にイベントを送信できるようにするには、次の手順を使用します。既存のルールのルート アクションまたはコレクタ アクションに新しいターゲットを追加すると、収集されたイベントを両方のシステムに送信できます。または、特定のポリシーまたはルールを変更して、CA Enterprise Log Manager サーバのみにイベントを送信することもできます。

ポリシーの使用に関する詳細は、「CA Audit r8 SP2 実装ガイド」で説明しています。この後の処理手順の実行の詳細については、その資料を参照してください。

CA Enterprise Log Manager は CA Audit SAPI ルータおよび CA Audit SAPI コレクタのリスナを使用して CA Audit クライアントからのイベントを収集します。収集されたイベントは、ポリシーをクライアントにプッシュした後、ポリシーが有効になってから CA Enterprise Log Manager のイベント ログ ストアに保存されます。

重要: ポリシーを変更して有効にする前に、CA Enterprise Log Manager リスナがイベントを受信するように設定する必要があります。この設定を最初に行わないと、ポリシーが有効になった時間とリスナがイベントを正しくマッピングできるようになった時間との間に、イベントが正確にマッピングされない可能性があります。

既存の r8 SP2 のポリシー ルールのアクションが CA Enterprise Log Manager にイベントを送信するように変更する方法

1. 「作成者」ロールを持つユーザとして、ポリシー マネージャ サーバにログインします。
2. [ポリシー]ペインのフォルダを展開して適切なポリシーを選択し、編集するルールにアクセスします。

   [詳細]ペインにポリシーが表示され、そのルールが表示されます。
3. 編集するルールをクリックします。

   [詳細]ペインにルールが表示され、そのアクションも表示されます。

4. ［編集］をクリックします。

   ［ルールの編集］ウィザードが表示されます。

5. 現在の宛先に加えて（あるいはその代わりに）CA Enterprise Log Manager サーバにイベントを送信できるように、［ルールの編集］ウィザードを使用してルールを変更し、終了したら［完了］をクリックします。

6. 「確認者」ロールを持つユーザが承認できるように、「作成者」ユーザとしてポリシーを確認し、コミットします。

7. 会社で職務の分離機能を使用している場合は、ログアウトしてから「確認者」ロールを持つユーザとしてポリシー マネージャ サーバにもう一度ログインします。

8. 変更したポリシーとルールを含むポリシー フォルダを確認して承認します。

   ポリシーが承認されると、ポリシー マネージャの配布サーバの設定によって、新規ポリシーが監査ノードに配布されるタイミングが決まります。ポリシーの有効化ステータスを確認するには、有効化ログを確認します。

9. CA Enterprise Log Manager に送信するイベントを収集するルールおよびポリシーのそれぞれに対して、この手順を繰り返します。

イベントをインポートするタイミング

コレクタ データベースを持つ既存の CA Audit データ ツール サーバが存在する場合は、イベント データを含む SEOSDATA テーブルも存在します。CA Audit および CA Enterprise Log Manager システムを同時に実行し、すでに収集されたデータに関するレポートを表示するために、SEOSDATA テーブルからデータをインポートする場合があります。

SEOSDATA インポート ユーティリティを実行して、コレクタ データベースからのイベント データを CA Enterprise Log Manager イベント ログ ストアにインポートできます。通常は、CA Enterprise Log Manager サーバを導入した直後にイベント データをインポートします。2 つのシステムを統合している場合、使用状況とネットワークの設定に応じて、データのインポートを複数回実行する場合もあります。

注: SEOSDATA テーブルからデータをインポートしても、そのテーブルに保存されたデータはいずれも削除または変更されません。インポート機能とは、データをコピーしてそれを解析し、CA Enterprise Log Manager イベント ログ ストアにマップすることです。

SEOSDATA インポート ユーティリティについて

インポート ユーティリティ LMSeosImport は、コマンド ライン インターフェースを使用して、Windows と Solaris の両方のオペレーティング システムをサポートします。このユーティリティは次のアクションを実行します。

- SEOSDATA テーブルに接続し、指定した方法でイベントを抽出します。
- 選択した SEOSDATA のイベントを名前と値のペアに解析します。
- イベント ログ ストアに挿入する場合に、SAPI イベント スポンサー または iTech イベント スポンサーを使用して CA Enterprise Log Manager にイベントを送信します。

イベントは、イベント ログ ストアのデータベース テーブルの基礎を形成する共通イベント文法（CEG）にマッピングされます。そして事前定義済みのクエリとレポートを使用して、保存されたイベントから情報を収集できます。

ライブ SEOSDATA テーブルからのインポート

ライブ SEOSDATA テーブルに対して LMSeosImport ユーティリティを実行することはお勧めしませんが、避けられない場合もあります。実際のデータベースに対してこのユーティリティを実行しなければならない場合は、ユーティリティで特定のセクションのデータだけをインポートします。このような状況は、LMSeosImport ユーティリティの起動後にデータベースに追加されたイベントが、インポート セッション中にインポートされないために発生します。

たとえば、ユーティリティの起動時にコマンド ラインで -minid および -maxid パラメータを指定しない場合、既存のエントリ ID の最小値と最大値がデータベースに照会されます。その後、ユーティリティでは、クエリとインポート アクティビティの実行時にその値を基にします。ユーティリティの起動後にデータベースに挿入されたイベントは、その範囲外のエントリ ID を持つため、インポートされません。

ユーティリティは、インポート セッションの完了時に、処理された最後のエントリ ID を表示します。すべてのイベントを取得するには、インポート セッションを複数回実行しなければならない場合があります。あるいは、ネットワークの使用やイベント アクティビティが少ない時間を待って、インポート ユーティリティを実行することもできます。必要に応じて、前回のセッションの最後のエントリ ID を新しいセッションの -minid の値として使用して、追加のインポート セッションを実行できます。

SEOSDATA テーブルからのデータのインポート

コレクタ データベース(SEOSDATA テーブル)からのデータをインポートして最適な結果を確実に得るには、以下の手順に従います。

1. LMSeosImport ユーティリティを CA Audit データ ツール サーバの iTechnology フォルダにコピーします。

   注: LMSeosImport ユーティリティには、*etsapi* および *etbase* のサポート ライブラリが必要です。これらは CA Audit クライアントに提供されます。

2. LMSeosImport のコマンド ラインとオプションを理解します。
3. [イベント]レポートを作成して、イベント タイプとイベント数、およびエントリ ID の範囲を検出します。
4. 使用する予定のパラメータを使用したインポート結果をプレビューします。

   必要に応じて、もう一度インポートのプレビューを実行してコマンド ライン オプションを再設定できます。

5. 再設定されたコマンド ライン オプションを使用して、コレクタ データベースからイベントをインポートします。

Solaris データ ツール サーバへのイベント インポート ユーティリティのコピー

SEOSDATA テーブルからデータをインポートできるようにするには、CA Enterprise Log Manager アプリケーションのインストール DVD-ROM から Solaris データ ツール サーバに LMSeosImport ユーティリティをコピーする必要があります。

注: LMSeosImport ユーティリティには、*etsapi* と *etbase* のライブラリが必要です。これらのファイルは、データ ツール サーバの基本インストールに含まれます。LMSeosImport ユーティリティを使用する前に、CA Audit インストール ディレクトリがシステムの PATH 文に含まれていることを確認してください。デフォルトのディレクトリは、opt/CA/eTrustAudit/bin です。

ユーティリティを実行する前に、*env* コマンドで次の環境変数を設定します。

- ODBC_HOME=<*CA Audit データ ツールのインストール ディレクトリ*>/odbc
- ODBCINI=<*CA Audit データ ツールのインストール ディレクトリ*>/odbc/odbc.ini

ユーティリティをコピーする方法

1. Solaris データ ツール サーバのコマンド プロンプトにアクセスします。
2. CA Enterprise Log Manager アプリケーションのインストール DVD-ROM を挿入します。
3. /CA/ELM/Solaris_sparc ディレクトリに移動します。
4. LMSeosImport ユーティリティを、CA Audit データ ツール サーバの iTechnology ディレクトリ /opt/CA/SharedComponents/iTechnology にコピーします。

   指定されたディレクトリにユーティリティをコピーして必要な環境変数を設定したら、このユーティリティを使用できます。個別のインストールは実行しません。

Windows データ ツール サーバへのインポート ユーティリティのコピー

SEOSDATA テーブルからデータをインポートできるようにするには、CA Enterprise Log Manager アプリケーションのインストール DVD-ROM から Windows データ ツール サーバに LMSeosImport ユーティリティをコピーする必要があります。

注: LMSeosImport ユーティリティには、*etsapi* と *etbase* のダイナミック リンク ライブラリが必要です。これらのファイルは、データ ツール サーバの基本インストールに含まれます。LMSeosImport ユーティリティを使用する前に、Program Files¥CA¥eTrust Audit¥bin ディレクトリがシステムの PATH 文に含まれていることを確認してください。

ユーティリティをコピーする方法

1. Windows データ ツール サーバのコマンド プロンプトにアクセスします。
2. CA Enterprise Log Manager アプリケーションのインストール DVD-ROM を挿入します。
3. ¥CA¥ELM¥Windows ディレクトリに移動します。
4. LMSeosImport.exe ユーティリティを、CA Audit データ ツール サーバの iTechnology ディレクトリ（<ドライブ>:¥Program Files¥CA¥SharedComponents¥iTechnology）にコピーします。

   指定されたディレクトリにユーティリティをコピーしたら、このユーティリティを使用できます。個別のインストールは実行しません。

LMSeosImport コマンド ラインについて

LMSeosImport ユーティリティでは、移行するイベントを制御できるさまざまなコマンド ライン引数を提供しています。SEOSDATA テーブルの各イベントは 1 行になっており、それを識別するための一意のエントリ ID を持っています。インポート ユーティリティを使用すると、複数の異なる種類の便利な情報をリスト表示するレポートを取得できます。そのレポートには、SEOSDATA テーブルのイベント数（エントリ ID の数として表示）、ログ タイプごとのイベント数、およびイベントの日付範囲がリスト表示されます。イベントのインポート中にエラーが発生した場合のために、このユーティリティでは再試行オプションが提供されています。

また、プレビュー ジョブを実行して、特定のコマンド構造を使用した場合のインポート結果を確認できます。プレビュー ジョブでは実際にはデータをインポートしません。これによって、実際の移行を行う前にコマンド ライン オプションを調整できます。

さまざまな種類のデータをインポートするために、異なるパラメータを使用して移行ユーティリティを複数回実行できます。たとえば、ある範囲のエントリ ID、ログ タイプ、または特定の日付範囲に基づいて調整した数回のセッションで、データを移行することもできます。

注: このユーティリティでは、前のセッションのインポートを追跡しません。同じパラメータを使用したコマンドを複数回実行すると、CA Enterprise Log Manager データベースのデータを複製できます。

最適な結果を得るには、-log オプションを使用してログ タイプごとにインポートを分割するか、-minid および -maxid オプションを使用してエントリ ID ごとにインポートを分割して、インポートのパフォーマンスを改善します。イベントのインポート中に発生する可能性のあるエラーから回復できるようにするには、-retry オプションを使用します。このユーティリティでは、インポートをできるだけ成功させるために、-retry のデフォルト値 300 秒を使用します。

インポート ユーティリティ コマンドおよびオプション

LMSeosImport ユーティリティは、以下のコマンド ライン構文とオプションをサポートしています。

```
LMSeosImport -dsn dsn_name -user user_name -password password -target target_name
{-sid nnn -eid nnnn -stm yyyy-mm-dd -etm yyyy-mm-dd -log logname -transport
(sapi|itech) -chunk nnnn -pretend -verbose -delay -report -retry}
```

-dsn

SEOSDATA テーブルが存在するホスト サーバの名前を指定します。このパラメータは必須です。

-user

少なくとも SEOSDATA テーブルへの読み取りアクセス権を持っている有効なユーザ ID を指定します。このパラメータは必須です。

-password

-user パラメータで指定されたユーザ アカウントのパスワードを指定します。このパラメータは必須です。

-target

SEOSDATA テーブルから移行されたイベントを受信する CA Enterprise Log Manager サーバのホスト名または IP アドレスを指定します。このパラメータは必須です。

-minid nnnn

SEOSDATA テーブルからイベントを選択するときに使用する、開始 ENTRYID を示します。このパラメータは任意です。

-maxid nnnn

SEOSDATA テーブルからイベントを選択するときに使用する、終了 ENTRYID を示します。このパラメータは任意です。

-mintm YYYY-MM-DD

SEOSDATA テーブルからイベントを選択するときに使用する、開始時刻（YYYY-MM-DD 形式）を示します。このパラメータは任意です。

-maxtm YYYY-MM-DD

SEOSDATA テーブルからイベントを選択するときに使用する、終了時刻（YYYY-MM-DD 形式）を示します。このパラメータは任意です。

-log logname

このユーティリティが、指定されたログ名を持つイベント レコードのみを選択するように指定します。このパラメータは任意です。ログ名にスペースが含まれる場合は、二重引用符で囲む必要があります。

-transport <sapi | itech >

インポート ユーティリティと CA Enterprise Log Manager の間で使用する転送方法を指定します。デフォルトの転送方法は sapi です。

-chunk nnnn

1 回のパスで SEOSDATA テーブルから選択するイベント レコードの数を指定します。デフォルト値は 5000 イベント(行)です。このパラメータは任意です。

-preview

イベント レコードの選択結果を STDOUT に出力しますが、実際のデータ インポートは行われません。このパラメータは任意です。

-port

SAPI への転送オプションを設定し、ポートマップ機能を使用せずに固定ポートの値を使用するように CA Enterprise Log Manager SAPI ルータを設定した場合は、使用するポート番号を指定します。

-verbose

ユーティリティが詳細な処理メッセージを STDOUT に送信するように指定します。このパラメータは任意です。

-delay

各イベントの処理の間に一時停止する秒数を指定します。このパラメータは任意です。

-report

SEOSDATA テーブルの時間範囲、ENTRYID の範囲、およびログ数のレポートを表示します。このパラメータは任意です。

-retry

イベントのインポート中にエラーが発生するたびに、再試行を試みる秒数の合計を指定します。そのイベントの送信が再び成功すると、処理が続行されます。ユーティリティは、自動的に 300 秒のデフォルト値を使用します。別の値を指定しない場合は、このパラメータを入力する必要はありません。再試行のステータスに関連するメッセージは STDOUT に送信されます。

LMSeosImport コマンド ラインの例

次のコマンド ラインの例を使用して、SEOSDATA のインポート ユーティリティを使用する場合のカスタム コマンドを独自に作成できます。

ENTRYID が 1000 ～ 4000 のレコードのインポートを実行する方法

次のコマンド ラインを入力します。

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –minid 1000 –maxid 4000
```

NT アプリケーション イベントのみのレコードのインポートを実行する方法

次のコマンド ラインを入力します。

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –log NT-Application
```

イベント レポートの作成

実際にデータをインポートする前に SEOSDATA イベント レポートを実行すると、テーブルのイベントに関する必要な情報が提供されます。レポートには、イベントの時間範囲、ログ タイプごとのイベント数、およびエントリ ID の範囲が表示されます。レポートに表示された値を使用して、プレビュー コマンドまたは実際のインポート コマンドのコマンド ライン オプションを調整できます。

Windows で現在の SEOSDATA のイベント情報のレポートを表示する方法

1. CA Audit データ ツール サーバのコマンド プロンプトにアクセスします。
2. ¥Program Files¥CA¥SharedComponents¥iTechnology ディレクトリに移動します。
3. 次のコマンド ラインを入力します。

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa -target <Log_Manager_host_name> –report
```

次の例のようなレポートが生成されます。

```
SEOSProcessor::InitOdbc: successfully attached to source [eAudit_DSN]

---------- SEOSDATA Event Time Range ----------

Minimum TIME = 2007-08-27
Maximum TIME = 2007-10-06

---------- Event Count Per Log ----------

com.ca.iTechnology.iSponsor : 3052
EiamSdk : 1013
NT-Application : 776
NT-System : 900

---------- SEOSDATA EntryID Range ----------

Minimum ENTRYID : 1
Maximum ENTRYID : 5741

Report Completed.
```

インポート結果のプレビュー

実際にデータをインポートまたは移行せずに、STDOUT に出力してインポートのテストを実行し、インポートの結果をプレビューできます。この方法は、一度だけの移行または定期的にスケジュールされたインポート バッチ ジョブ用に入力したコマンド ライン パラメータをテストする場合に適しています。

インポートのテストを実行してインポート結果をプレビューする方法

1. CA Audit データ ツール サーバのコマンド プロンプトにアクセスします。
2. 次の適切なディレクトリに移動します。

   Solaris の場合: /opt/CA/SharedComponents/iTechnology

   Windows の場合: ¥Program Files¥CA¥SharedComponents¥iTechnology

3. 次のコマンド ラインを入力します。

   Solaris の場合:

   ```
   ./LMSeosImport.sh –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_host_name_or_IP> –minid 1000 –maxid 4000 -preview
   ```

   Windows の場合

   ```
   LMSeosImport.exe –dsn eAudit_DSN –user sa –password sa –target
   <Log_Manager_host_name_or_IP> –minid 1000 –maxid 4000 -preview
   ```

Windows コレクタ データベースからのイベントのインポート

Windows のデータ ツール サーバにあるコレクタ データベースからイベント データをインポートするには、次の手順に従います。

Windows サーバの SEOSDATA テーブルからイベントをインポートする方法

1. SEOSDATA テーブルが存在するサーバの名前を検索します。
2. そのサーバ用のユーザ アクセス認証情報と、少なくとも SEOSDATA テーブルへの読み取りアクセス権を持っていることを確認します。
3. CA Audit データ ツール サーバのコマンド プロンプトにアクセスします。
4. ¥Program Files¥CA¥Shared Components¥iTechnology ディレクトリに移動します。
5. 次のコマンド構文を使用してインポート ユーティリティを起動します。

   ```
   LMSeosImport.exe -dsn <dsnname> -user <UID> -password <password> -target
   <targethostname> <optional flags>
   ```

Solaris コレクタ データベースからのイベントのインポート

Solaris のデータ ツール サーバにあるコレクタ データベースからイベント データをインポートするには、以下の手順に従います。

Solaris サーバの SEOSDATA テーブルからイベントをインポートする方法

1. SEOSDATA テーブルが存在するサーバの名前を検索します。
2. そのサーバ用のユーザ アクセス認証情報と、少なくとも SEOSDATA テーブルへの読み取りアクセス権を持っていることを確認します。
3. CA Audit データ ツール サーバのコマンド プロンプトにアクセスします。

4. /opt/CA/SharedComponents/iTechnology ディレクトリに移動します。
5. 次のコマンド構文を使用してインポート ユーティリティを起動します。

```
./LMSeosImport -dsn <dsnname> -user <UID> -password <password> -target
<targethostname> <optional flags>
```

付録 B: CA Access Control ユーザに関する考慮事項

このセクションには、以下のトピックが含まれています。

CA Access Control との統合

複数の異なるリリース レベルの 1 つを使用して、CA Access Control に CA Enterprise Log Manager を統合できます。一般的なアプローチは次のとおりです。

イベントのルーティングに TIBCO メッセージ サーバを使用する CA Access Control リリースについては、以下の手順を実行します。

- CA Enterprise Log Manager エージェントをインストールします
- AccessControl_R12SP1_TIBCO_Connector コネクタを使用するコネクタを設定します

CA Access Controlr12.5 については、「CA Access Control r12.5 実装ガイド」および「CA Enterprise Log Manager CA Access Control コネクタ ガイド」を参照してください。

CA Access Controlr12. SP1 については、「CA Access Control r12 SP1 実装ガイド」第 3 版および「CA Enterprise Log Manager コネクタ ガイド CA Access Control 用」を参照してください。

注: 上記の実装では、CA Access Control Premium Edition に含まれるコンポーネントを使用します。

イベントのルーティングに selogrd を使用する CA Access Control リリースについては、以下の手順を実行します。

- CA Enterprise Log Manager エージェントをインストールします
- ACSelogrd 統合を使用するコネクタを設定します

CA Access Control イベントを収集するコネクタの詳細な設定方法については、「CA Access Control コネクタ ガイド」で説明しています。

現在 CA Access Control イベントを CA Audit に送信している場合は、以下の方法を使用すると CA Enterprise Log Manager にイベントを送信できます。

- CA Audit iRecorder を使用してイベントを収集する場合は、CA Audit および CA Enterprise Log Manager の両方にイベントを送信するように、既存の CA Audit ポリシーを変更します。また、必要に応じて、CA Enterprise Log Manager サーバにのみイベントを送信するようにポリシーを変更することもできます。
- control.conf ファイルを設定すると、iRecorder が CA Enterprise Log Manager に直接イベントを送信することができます。

注: eTrust Access Control が iRecorder をサポートしないバージョンである場合は、CA Audit ルータにイベントを直接送信できます。詳細については、「eTrust Access Control r5.3 管理ガイド」にある CA Audit の統合に関する情報を参照してください。

以下のガイドラインでは、Policy Manager のユーザ インターフェースに r8 SP2 シリーズを使用します。ユーザ インターフェースは異なりますが、一般的な手順は、以前の CA Audit リリースで使用していたものと同じです。

CA Enterprise Log Manager にイベントを送信するように CA Audit ポリシーを変更する方法

CA Enterprise Log Manager にイベントを送信するように既存の CA Audit ポリシーを変更する処理には、次の手順が含まれます。

- 必要な情報を収集します。
  - ポリシーの作成、チェック、および有効化の権限を持つ CA Audit ポリシー マネージャのユーザ認証情報を持っていることを確認します。
  - Audit アドミニストレータのユーザ インターフェースにアクセスするために、必要な IP アドレスまたはホスト名を取得します。r8 SP2 シリーズのポリシー マネージャ サーバ Web アプリケーションにアクセスする URL は、次の形式になります。

    `https://<IP_address_of_CA Audit_PM>:5250/spin/auditadmin`
- ルール アクションをどのように作成するかによって、CA Enterprise Log Manager SAPI コレクタまたは SAPI ルータ サービスを設定します。

  コレクタ アクションを作成する予定である場合は、SAPI コレクタを設定します。ルート アクションを設定する予定である場合は、SAPI ルータを設定します。

  注: このセクションの例ではコレクタ アクションを使用します。
- 既存の CA Access Control ポリシーを検索し、CA Enterprise Log Manager にイベントを送信するように変更します。
- 変更したポリシーを確認して有効化し、監査ノードにそれを配布します。

必要に応じてこのプロセスを繰り返し、他のポリシー ルールに新しいルール アクションを追加します。

詳細情報:

SAPI ルータおよびコレクタについて (P. 242)

CA Access Control イベントを受信するための SAPI コレクタのアダプタの設定

CA Audit の実装から CA Access Control イベントを受信するように SAPI コレクタのアダプタを設定するには、次の手順を使用します。

CA Audit コレクタ データベースへのイベントの送信に加えて(またはその代わりに)、コレクタ アクションを使用する CA Audit ポリシー を変更して CA Enterprise Log Manager サーバにイベントを送信できます。イベントの消失を防ぐため、CA Audit ポリシーを変更する前にこのサービスを設定します。

(非常によく似た方法で SAPI ルータ サービスを設定できます。ルータ サービスとコレクタ サービスの両方を使用する場合は、リスト表示されたポートが異なること、またはこれらのサービスがポート マッピング サービスによって制御されていることを確認してください。)

SAPI コレクタ サービスを設定する方法

1. 管理者ユーザとして CA Enterprise Log Manager サーバにログインし、[管理]タブを選択します。

   デフォルトでは[ログ収集]サブタブが表示されます。

2. CA アダプタのエントリを展開します。

3. [SAPI コレクタ]サービスを選択します。

4. [リスナの有効化]チェック ボックスをオンにして、CA Audit が使用する値と同じ値に SAPI ポート値を設定します。

   デフォルトの CA Enterprise Log Manager 値、0 は、ポートのマッピングにポートマップ サービスを利用します。CA Audit で定義されたポートがある場合は、ここでその設定を使用します。

5. その他のフィールドのデフォルト値を受け入れて、[マッピング ファイル]のリストまでスクロールします。

   [登録]チェック ボックスをオンにする場合は、SAPI ポート値を指定します。

6. アクセス制御のマッピング ファイルが存在しない場合はこのファイル エントリを追加して、[選択済み]マッピング ファイルのリストから他のマッピング ファイルの選択を削除します。

7. [保存]をクリックします。

CA Enterprise Log Manager にイベントを送信するための既存の CA Audit ポリシーの変更

CA Audit クライアントが CA Enterprise Log Manager と CA Audit コレクタ データベースの両方にイベントを送信できるようにするには、次の手順を使用します。既存のルールのルート アクションまたはコレクタ アクションに新しいターゲットを追加すると、収集されたイベントを両方のシステムに送信できます。または、特定のポリシーまたはルールを変更して、CA Enterprise Log Manager サーバのみにイベントを送信することもできます。

CA Enterprise Log Manager は CA Audit SAPI ルータおよび CA Audit SAPI コレクタのリスナを使用して CA Audit クライアントからのイベントを収集します。(いずれの iRecorder も CA Enterprise Log Manager サーバに直接送信するように設定している場合、CA Enterprise Log Manager では iTech プラグインを直接使用してイベントを収集することもできます。)クライアントにポリシーを適用し、それがアクティブになると、初めて、収集されたイベントが CA Enterprise Log Manager イベント ログ ストアに格納されます。

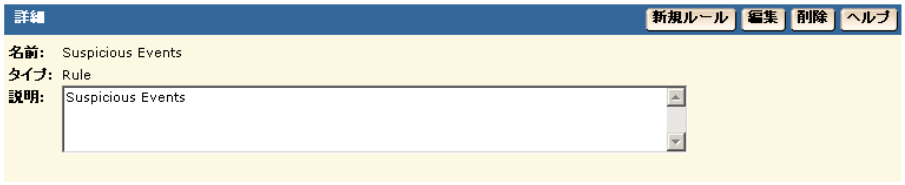
重要: ポリシーを変更して有効にする前に、CA Enterprise Log Manager リスナがイベントを受信するように設定します。この設定を最初に行わないと、ポリシーが有効になる時間とリスナがイベントを正しくマッピングできるようになる時間との間で、イベントが正確にマッピングされなくなる可能性があります。

既存のポリシー ルールのアクションが CA Enterprise Log Manager にイベントを送信するように変更する方法

1. ポリシー マネージャ サーバにログインし、左側のペインの[マイ ポリシー]タブにアクセスします。

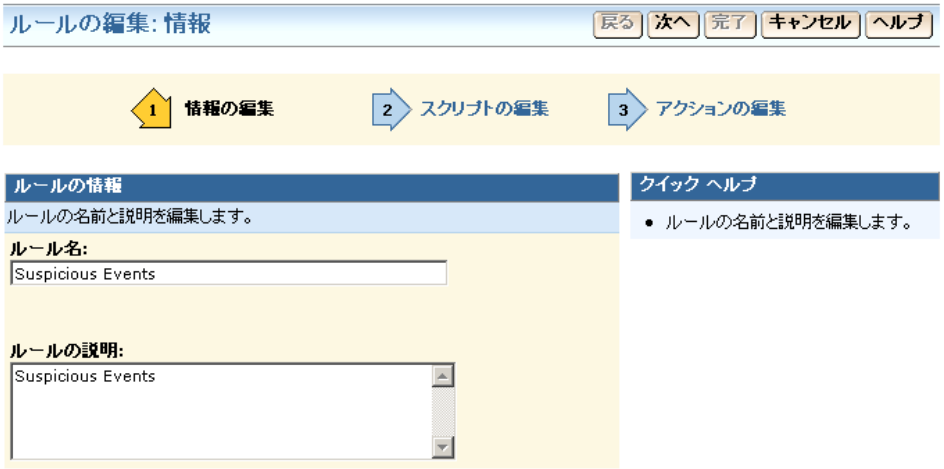
2. 必要なポリシーが表示されるまで、ポリシー フォルダを展開します。

3. ポリシーをクリックして、右側の[詳細]ペインに基本情報を表示します。



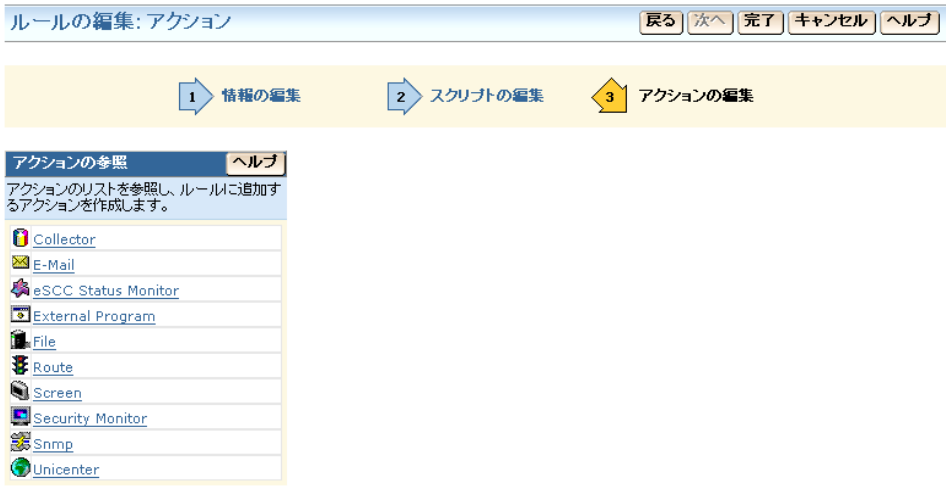
4. ポリシー ルールを追加するには、[詳細]ペインで[編集]をクリックします。

ルール ウィザードが起動します。

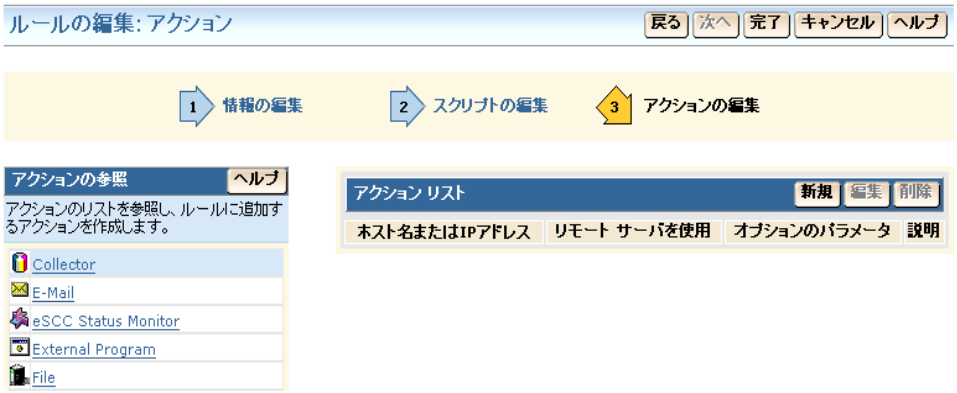


5. 手順 3 を示す矢印の横にある[アクションの編集]をクリックします。

   ルール ウィザードの[アクション]ページが表示されます。



6. [アクションの参照]ペインで[コレクタ]アクションをクリックすると、右側に[アクション リスト]が表示されます。



   ルート アクションも使用できますが、コレクタ アクションには、基本的なフェイルオーバー処理の代替ホスト名を提供するという追加の利点もあります。

7. [新規]をクリックして新しいルールを追加します。
8. 収集用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。

2 つ以上のサーバを使用する CA Enterprise Log Manager 実装の場合、[代替ホストの名前]フィールドに異なる CA Enterprise Log Manager のホスト名または IP アドレスを入力できます。こうすることで、CA Audit の自動フェイルオーバー機能を利用できます。最初の CA Enterprise Log Manager サーバが使用できない場合、CA Audit は自動的に[代替ホストの名前]フィールドに指定されたサーバにイベントを送信します。

9. [代替ホストの名前]フィールドに管理用 CA Enterprise Log Manager サーバの名前を入力してから、この新しいルール アクションの説明を作成します。
10. [このアクションをリモート サーバで実行]チェック ボックスがオンの場合は、このチェック ボックスをオフにします。
11. [追加]をクリックして新しいルール アクションを保存し、ウィザード ウィンドウで[完了]をクリックします。

注: 次に、ポリシーを確認して有効にします。そのため、CA Audit ポリシー マネージャからログアウトしないでください。

詳細情報:

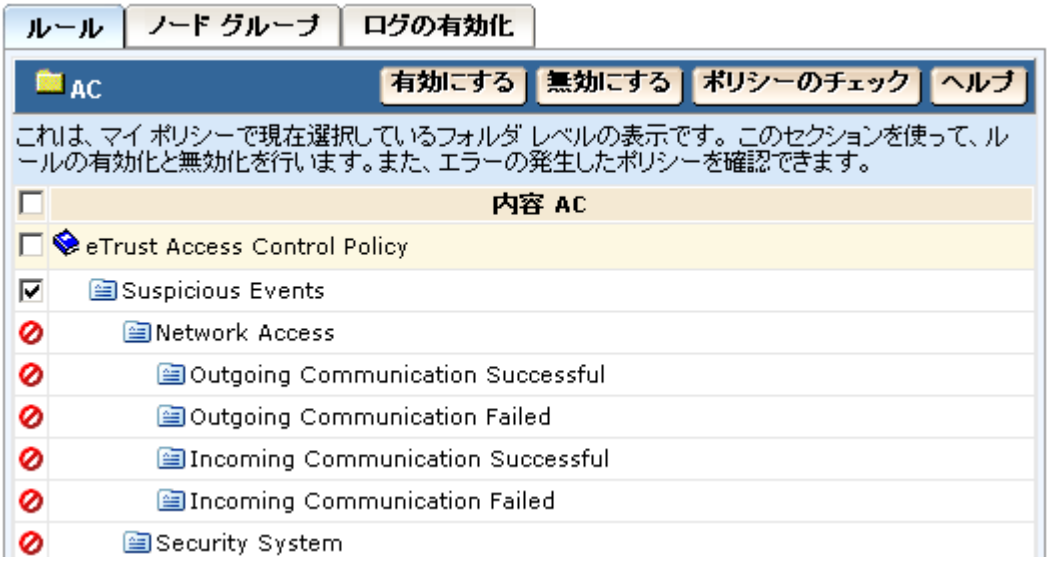
CA Enterprise Log Manager にイベントを送信するための r8 SP2 ポリシーの変更 (P. 250)

変更されたポリシーの確認と有効化

既存のポリシーを変更してルール アクションを追加したら、そのポリシーを確認(コンパイル)して有効にします。

CA Access Control のポリシーを確認および有効化する方法

1. 右下のペインの[ルール]タブを選択してから、チェックするルールを選択します。



2. [ポリシーのチェック]をクリックして、新しいアクションを追加して変更したルールをチェックし、正常にコンパイルされることを確認します。

   ルールに対して必要な変更を行い、ルールを有効にする前に正常にコンパイルされることを確認します。

3. [有効にする]をクリックして、追加した新しいルール アクションを含むチェック済みのポリシーを配布します。

4. CA Enterprise Log Manager に送信するイベントを収集するルールおよびポリシーのそれぞれに対して、この手順を繰り返します。

CA Enterprise Log Manager にイベントを送信するように CA Access Control iRecorder を設定する方法

スタンド アロンの CA Access Control iRecorder を設定して、収集したイベントを CA Enterprise Log Manager サーバに直接送信し、保存およびレポートに使用することができます。このプロセスには次のような手順が含まれます。

1. CA Access Control iRecorder からの情報を受信するように iTech イベント プラグイン リスナを設定します。
2. CA Access Control iRecorder をダウンロードしてインストールします。
3. 収集したイベントを直接 CA Enterprise Log Manager に送信するように iRecorder を設定します。
4. CA Enterprise Log Manager がイベントを受信していることを確認します。

注: iRecorder がイベントを送信できる宛先は 1 つのみです。この手順を使用して設定を行うと、宛先は指定した CA Enterprise Log Manager サーバのみになります。

CA Access Control イベント用の iTech イベント プラグインの設定

CA Enterprise Log Manager に直接イベントを送信するように iRecorder を再設定する前に、それらのイベントを受信するようにリスナを設定する必要があります。

リスナを設定する方法

1. Administrator ロールを持つユーザとして CA Enterprise Log Manager サーバにログインします。
2. [管理]タブにアクセスしてから、[CA アダプタ]ノードを展開します。

3. iTechnology イベント プラグイン ノードを展開します。
4. 現在の CA Enterprise Log Manager サーバを選択して、ローカルの設定を表示します。
5. AccessControl マッピング ファイルが[選択済み]マッピング ファイル リストの最初にあり、最も効率的な処理が実行されることを確認します。
6. すべてのイベント レベルを収集するには、[ログ レベル]の値が[NOTSET]に設定されていることを確認します。
7. [保存]をクリックします。

CA Access Control iRecorder のダウンロードとインストール

CA Audit をインストールしていなくても、CA Access Control イベントを収集して CA Enterprise Log Manager サーバに送信できます。この方法でイベントを収集する場合は、スタンドアロン モードで iRecorder を使用します。iRecorder は CA サポート Web サイトから取得できます。

注: iRecorder は CA Access Control r8 以降のリリースのみでサポートされています。

iRecorder をダウンロードおよびインストールする方法

1. 次の CA Web サイトにアクセスします。

   `https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec`

2. 使用している CA Access Control のバージョンに適した iRecorder を選択します。
3. マトリクス内の統合ガイドリンクから、使用可能なインストール手順を表示してそれに従います。

スタンドアロンの CA Access Control iRecorder の設定

CA Enterprise Log Manager に CA Access Control イベントを送信するように iRecorder を設定するには、次の手順を使用します。

重要: スタンド アロンの iRecorder は、1 つの宛先のみにイベントを送信することができます。次の手順を使用して iRecorder を設定すると、このシステムにインストールされたすべての iRecorder が指定された CA Enterprise Log Manager イベント ログ ストアのみにイベントを送信します。

CA Audit クライアントと同じコンピュータにインストールされる iRecorder は、クライアントにイベントを直接送信します。それらのサーバでは、CA Enterprise Log Manager SAPI コレクタまたはルータ アダプタを設定後に、既存の CA Audit ポリシーを変更してルール アクションを追加する必要があります。

CA Enterprise Log Manager にイベントを送信するように iRecorder を設定する方法

1. 管理者または root の権限を持つユーザとして、iRecorder をホストするサーバにログインします。
2. オペレーティング システムの次のディレクトリに移動します。
   - UNIX または Linux の場合: /opt/CA/SharedComponents/iTechnology
   - Windows の場合: ¥Program Files¥CA¥SharedComponents¥iTechnology
3. 次のコマンドを使用して、iGateway デーモンまたはサービスを停止します。
   - UNIX または Linux の場合: ../S99igateway stop
   - Windows の場合: net stop igateway
4. iControl.conf ファイルを編集します。

   変更する必要のあるセクションを太字で示した iControl のサンプル ファイルを次に示します。

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
    <Name>iControl</Name>
    <ImageName>iControl</ImageName>
    <Version>4.5.0.2</Version>
    <DispatchEP>iDispatch</DispatchEP>
    <ISType>DSP</ISType>
    <Gated>false</Gated>
    <PreLoad>true</PreLoad>
    <RouteEvent>false</RouteEvent>
    <RouteEventHost>localhost</RouteEventHost>
    <EventsToCache>100</EventsToCache>
    <EventUseHttps>true</EventUseHttps>
    <EventUsePersistentConnections>true</EventUsePersistentConnections>
    <EventUsePipeline>false</EventUsePipeline>
    <StoreEventHost max="10000">localhost</StoreEventHost>
    <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
    <UID>ef1f44ef-r8sp1cr3596a1052-abcd28-2</UID>
    <PublicKey>Public_Key_Value</PublicKey>
    <PrivateKey>Private_Key_Value</PrivateKey>
    <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. RouteEvent の値を次のように指定します。

```
<RouteEvent>true</RouteEvent>
```

   このエントリは、すべての iRecorder イベントを含むイベントを、RouteEventHost タグのペアで指定されたホストに送信するよう iGateway に指示します。

6. RouteEventHost の値を次のように指定します。

   <RouteEventHost>*Your_CA_Enterprise_Log_Manager_hostname*</RouteEventHost>

   このエントリは、DNS 名を使用して CA Enterprise Log Manager サーバにイベントを送信するように iGateway に指示します。

7. ファイルを保存して閉じます。
8. 次のコマンドを使用して、iGateway デーモンまたはサービスを再起動します。

   - UNIX または Linux の場合: ./S99igateway start
   - Windows の場合: net start igateway

   このアクションによって iRecorder は強制的に新しい設定を使用し、iRecorder から CA Enterprise Log Manager サーバへのイベント フローを開始します。

CA Audit コレクタ データベースから CA Access Control イベントをインポートする方法

既存の SEOSDATA テーブルから CA Access Control イベントをインポートする処理には、次の手順が含まれます。

1. LMSeosImport ユーティリティを CA Audit データ ツール サーバにコピーします。
2. CA Access Control イベントがデータベースに存在するかどうか判断するために、イベント レポートを作成します。
3. CA Access Control 固有のパラメータを使用して、インポートのプレビューを実行します。
4. CA Access Control イベントをインポートします。
5. インポートされたイベントに対して CA Enterprise Log Manager のクエリとレポートを実行します。

CA Access Control のイベントをインポートするための前提条件

LMSeosImport ユーティリティを使用する前に、以下の手順に従います。

- 少なくとも CA Audit SEOSDATA テーブルへの読み取りアクセスを持つデータベース ユーザ アカウントを取得します
- LMSeosImport ユーティリティを CA Audit データ ツール サーバにコピーします
- データ ツール サーバのコマンド プロンプトにアクセスして、次の適切なディレクトリに移動します。

  Solaris の場合: /opt/CA/SharedComponents/iTechnology

  Windows の場合: ¥Program Files¥CA¥SharedComponents¥iTechnology

Windows データ ツール サーバへのインポート ユーティリティのコピー

SEOSDATA テーブルからデータをインポートできるようにするには、CA Enterprise Log Manager アプリケーションのインストール DVD-ROM から Windows データ ツール サーバに LMSeosImport ユーティリティをコピーする必要があります。

注: LMSeosImport ユーティリティには、*etsapi* と *etbase* のダイナミック リンク ライブラリが必要です。これらのファイルは、データ ツール サーバの基本インストールに含まれます。LMSeosImport ユーティリティを使用する前に、Program Files¥CA¥eTrust Audit¥bin ディレクトリがシステムの PATH 文に含まれていることを確認してください。

ユーティリティをコピーする方法

1. Windows データ ツール サーバのコマンド プロンプトにアクセスします。
2. CA Enterprise Log Manager アプリケーションのインストール DVD-ROM を挿入します。
3. ¥CA¥ELM¥Windows ディレクトリに移動します。
4. LMSeosImport.exe ユーティリティを、CA Audit データ ツール サーバの iTechnology ディレクトリ (<ドライブ>:¥Program Files¥CA¥SharedComponents¥iTechnology) にコピーします。

   指定されたディレクトリにユーティリティをコピーしたら、このユーティリティを使用できます。個別のインストールは実行しません。

Solaris データ ツール サーバへのイベント インポート ユーティリティのコピー

SEOSDATA テーブルからデータをインポートできるようにするには、CA Enterprise Log Manager アプリケーションのインストール DVD-ROM から Solaris データ ツール サーバに LMSeosImport ユーティリティをコピーする必要があります。

注: LMSeosImport ユーティリティには、*etsapi* と *etbase* のライブラリが必要です。これらのファイルは、データ ツール サーバの基本インストールに含まれます。LMSeosImport ユーティリティを使用する前に、CA Audit インストール ディレクトリがシステムの PATH 文に含まれていることを確認してください。デフォルトのディレクトリは、opt/CA/eTrustAudit/bin です。

ユーティリティを実行する前に、*env* コマンドで次の環境変数を設定します。

- ODBC_HOME=<*CA Audit データ ツールのインストール ディレクトリ*>/odbc
- ODBCINI=<*CA Audit データ ツールのインストール ディレクトリ*>/odbc/odbc.ini

ユーティリティをコピーする方法

1. Solaris データ ツール サーバのコマンド プロンプトにアクセスします。
2. CA Enterprise Log Manager アプリケーションのインストール DVD-ROM を挿入します。
3. /CA/ELM/Solaris_sparc ディレクトリに移動します。
4. LMSeosImport ユーティリティを、CA Audit データ ツール サーバの iTechnology ディレクトリ /opt/CA/SharedComponents/iTechnology にコピーします。

   指定されたディレクトリにユーティリティをコピーして必要な環境変数を設定したら、このユーティリティを使用できます。個別のインストールは実行しません。

CA Access Control のイベントの SEOSDATA イベント レポートの作成

既存の SEOSDATA テーブルに CA Access Control のイベントが含まれるかどうかを判断し、インポート方法を決定するには、イベント レポートを実行する必要があります。CA Access Control のイベントのログ名は *eTrust Access Control* です。このレポートには、ログ名ごとに区切られたデータベースのすべてのイベントがリスト表示されます。CA Access Control のイベントをインポートする最も簡単な方法は、ログ名に基づいてインポートすることです。

イベント レポートを作成する方法

1. SEOSDATA テーブルに存在する CA Access Control イベントを確認できるように、イベント レポートを作成します。

   ```
   LMSeosImport –dsn My_Audit_DSN –user sa –password sa –report
   ```

   処理の後に、ユーティリティによって次のようなレポートが表示されます。

   ```
   Import started on Fri Jan  2 15:20:30 2009


   No transport specified, defaulting to SAPI...

   Preparing ODBC connections...

   Successfully attached to source [My_Audit_DSN]

   ---------- SEOSDATA Event Time Range ----------

   Minimum TIME = 2008-05-27
   Maximum TIME = 2009-01-02

   ---------- Event Count Per Log ----------

   Unix : 12804
   ACF2 : 1483
   eTrust AC : 143762
   com.ca.iTechnology.iSponsor : 66456
   NT-Application : 5270
   CISCO PIX Firewall : 5329
   MS IIS : 6765
   Netscape : 530
   RACF : 14
   Apache : 401
   N/A : 28222
   SNMP-recorder : 456
   Check Point FW-1 : 1057
   EiamSdk : 2790
   MS ISA : 609
   ORACLE : 2742
   eTrust PCM : 247
   NT-System : 680
   eTrust Audit : 513
   NT-Security : 14714
   CISCO Device : 41436
   SNORT : 1089

   ---------- SEOSDATA EntryID Range ----------
   ```

```
Minimum ENTRYID : 1
Maximum ENTRYID : 10000010243


Report Completed.

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

2. CA Access Control からのイベントが存在することをレポートで確認します。

   次に示すレポートの抜粋の太字の行は、この SEOSDATA テーブルに CA Access Control のイベントが含まれていたことを示します。

```
---------- Event Count Per Log ----------

Unix : 12804
ACF2 : 1483
eTrust AC : 143762
com.ca.iTechnology.iSponsor : 66456
NT-Application : 5270
...
```

CA Access Control のイベントのインポートのプレビュー

インポート プレビューを使用して、インポート パラメータを調整できます。この例では、特定の期間のイベントをインポートする必要性に基づいて、2 つのプレビュー パスについて説明します。この例は、以下の内容を前提としています。

- CA Audit データ ツール サーバは Windows コンピュータに存在します。
- SEOSDATA テーブルのデータベース名は My_Audit_DSN です。
- データベース ユーザ名は sa で、パスワードは sa です。
- インポートのプレビューでは、検索およびインポートの条件としてログ名のみを使用します。

-preview オプションを使用したコマンドの出力では、インポート結果の例が STDOUT に送信されます（この例では CA Enterprise Log Manager サーバ名を表すために *My_CA-ELM_Server* という値を使用します）。

インポートをプレビューする方法

1. 次のコマンドを使用して CA Access Control イベントのインポートをプレビューします。

```
LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server
–log "eTrust Access Control" -preview
```

-preview コマンドによって次のような情報が表示されます。

```
Import started on Fri Jan  2 15:35:37 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import (preview) running, please wait...

.........

Import (preview) Completed (143762 records in 4 minutes 12 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     143762

Last EntryId processed: 101234500

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

プレビュー結果では、インポートする CA Access Control イベントがかなり多く存在することを示しています。この例では、2 か月間に発生したイベントのみをインポートする必要があると仮定します。日付ごとに小さなグループのイベントをインポートするように、プレビュー コマンドを調整できます。

2. 次のコマンドを使用して、日付範囲を含むようにインポート パラメータを変更し、再びプレビューを実行します。

```
LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server
–log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31 -preview
```

修正されたコマンドによって、次のような情報が表示されます。

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import (preview) running, please wait...

.........

Import (preview) Completed (143762 records in 4 minutes 37 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2349

Last EntryId processed: 5167810102

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

このインポート プレビューでは、日付範囲によってインポートするイベントがより小さなサブセットになったことを示しています。これで実際のインポートを実行する準備ができました。

詳細情報:

LMSeosImport コマンド ラインについて (P. 255)
インポート結果のプレビュー (P. 259)

CA Access Control イベントのインポート

イベント レポートおよびインポートのプレビューを実行すると、SEOSDATA テーブルから CA Access Control のイベントをインポートする準備が整います。

CA Access Control のイベントをインポートする方法

指定された日付範囲の CA Access Control イベントを取得するには、-preview オプションを使用しないで、プレビューから次のコマンドを使用します。

```
LMSeosImport.exe –dsn [My_Audit_DSN] –user sa –password sa -target [My-CA-ELM-Server]
–log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

このユーティリティによって次のような結果が表示されます。

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import running, please wait...

.........

Import Completed (143762 records in 5 minutes 18 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2241

Last EntryId processed: 5167810102

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

詳細情報:

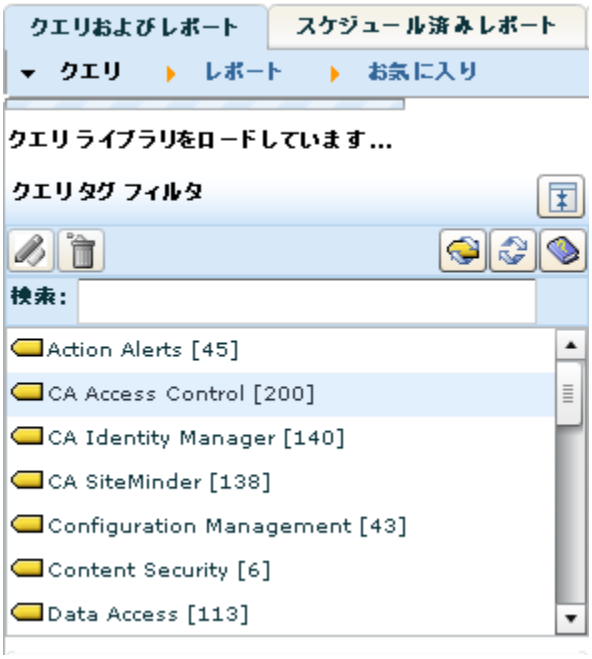
LMSeosImport コマンド ラインについて (P. 255)
Windows コレクタ データベースからのイベントのインポート (P. 260)
Solaris コレクタ データベースからのイベントのインポート (P. 260)

CA Access Control イベントを確認するためのクエリおよびレポートの表示

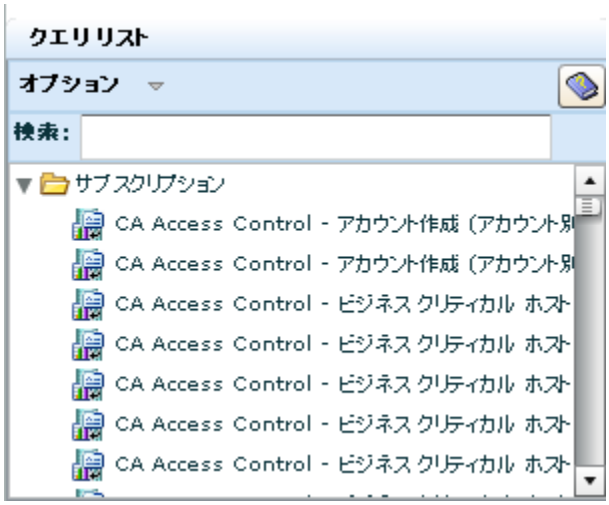
CA Enterprise Log Manager は、CA Access Control から収集されたイベントを検査するための多くのクエリとレポートを提供しています。CA Access Control のクエリおよびレポートにアクセスするには、次の手順を使用します。

CA Access Control のクエリにアクセスする方法

1. クエリとレポートを表示する権限を持つユーザとして CA Enterprise Log Manager サーバにログインします。
2. [クエリおよびレポート]タブの[クエリ]サブタブがまだ表示されていない場合は、このサブタブにアクセスします。



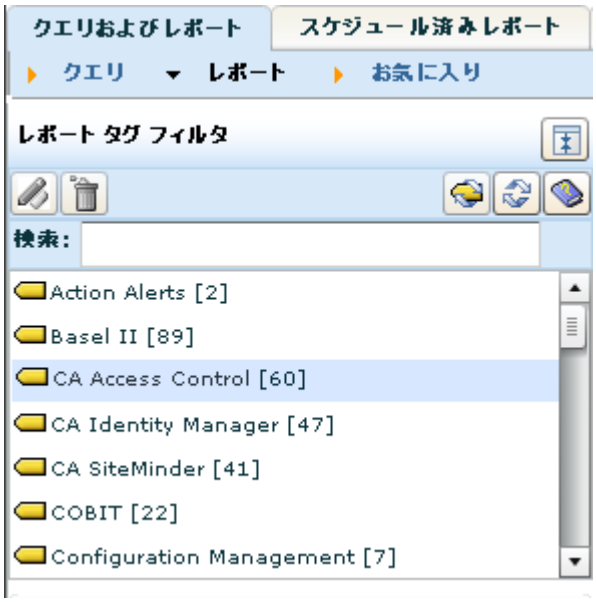
3. CA Access Control クエリ タグをクリックして、左側のリストに使用可能なクエリを表示します



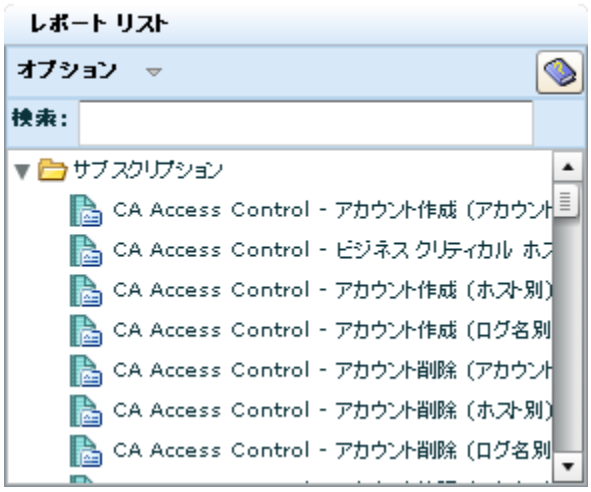
4. クエリを選択してイベント データを表示します。

CA Access Control のレポートにアクセスする方法

1. クエリとレポートを表示する権限を持つユーザとして CA Enterprise Log Manager サーバにログインします。
2. [クエリおよびレポート]タブの[レポート]サブタブがまだ表示されていない場合は、このサブタブにアクセスします。



3. CA Access Control レポート タグをクリックして、左側のリストに使用可能なレポートを表示します。



4. レポートを選択してイベント データを表示します。

付録 C: CA IT PAM の注意事項

このセクションには、以下のトピックが含まれています。

シナリオ: CA IT PAM 認証に CA Enterprise Log Manager 上で CA EEM を使用する方法

この付録では、Windows サーバに CA IT PAM をインストールし、認証用に CA Enterprise Log Manager サーバ上で CA EEM を共有するためのシナリオについて説明します。これらの手順は、「CA IT Process Automation Installation Guide」に記載されている内容を補足するものです。

重要: CA IT PAM は FIPS 互換でないため、CA EEM の共有は FIPS モードではサポートされていません。CA Enterprise Log Manager サーバを FIPS モードにアップグレードした場合、CA IT PAM との統合はできなくなります。

注: CA IT PAM を UNIX サーバにインストールするか、LDAP またはローカル CA EEM を認証に使用する場合、この付録の内容は該当しません。いずれの場合も、同じ CA EEM サーバを共有することにはなりません。CA Enterprise Log Manager r12.1 SP1 は FIPS モードで実行でき、CA IT PAM と通信できますが、それらの通信チャネルは FIPS 互換ではありません。

あらゆるインストール シナリオについては、サポート オンラインから CA IT Process Automation Manager r2.1 SP03 用のインストール ガイドをダウンロードしてください。また、PDF ファイルを参照するために Adobe Acrobat Reader が必要になります。

CA IT PAM 認証用に CA Enterprise Log Manager 上で CA EEM を使用するためには、2 つの手順を手動で実行する必要があります。1 つのファイルは Windows サーバからアプライアンスにコピーし、別のファイルはアプライアンスから Windows サーバにコピーします。これらの手順は、この付録で説明されています。CA IT PAM のドキュメントでは説明されていません。

CA IT PAM 認証の実装プロセス

CA Enterprise Log Manager 管理サーバ上で CA EEM を使用して、CA IT PAM 認証を実装するには、以下の手順に従います。

1. CA IT PAM 認証を実装する準備をします。
   a. CA IT PAM インストール パッケージをインストール先の Windows サーバにロードします。
   b. (オプション) itpamcert.p12 証明書のデフォルトのパスワードを変更します。

2. ITPAM_eem.xml ファイルを、CA IT PAM のインストール先のホストから、CA EEM を含む CA Enterprise Log Manager アプライアンスにコピーします。
3. CA Enterprise Log Manager が使用するのと同じ CA EEM 上で、ITPAM をアプリケーション インスタンスとして登録します。safex コマンドを実行すると、itpamcert.p12 証明書および ITPAM アプリケーション インスタンスが、2 つのユーザ アカウント itpamadmin および itpamuser で生成されます。

   注: safex コマンドの使用について参照するには、./safex を入力します。
4. itpamcert.p12 ファイルを、CA Enterprise Log Manager アプライアンスら、CA IT PAM ドメインのインストール先 Windows ホストにコピーします。
5. ITPAM アプリケーションにアクセスし、itpamadmin および itpamuser のパスワードをリセットします。
6. Windows サーバにログオンし、「CA IT Process Automation Manager Installaion Guide」で説明されている手順に従って、サードパーティ コンポーネントをインストールします。
7. この付録に示されているガイドライン、および CA IT PAM インストール手順を使用して、CA IT PAM ドメインをインストールします。
8. CA ITPAM Server サービスを開始します。
9. CA IT PAM コンソールを起動してログインします。

共有 CA EEM 上での CA IT PAM 認証の実装準備

CA IT PAMドメインのインストール先の Windows サーバにインストール パッケージをロードしたら、itpamcert.cer 証明書のパスワードを設定できます。

CA Enterprise Log Manager 管理サーバ上での CA IT PAM 認証の実装を準備する方法

1. CA IT PAM のインストール先の Windows Server 2003 ホストに、CA IT PAM の ISO イメージを展開します。

   注: CA IT PAM ISO イメージは、CA IT PAM インストール ソースの CD 2 に含まれています。

2. (オプション) IT PAM 証明書用のデフォルトのパスワードを変更します。
   a. <インストール パス>¥eem フォルダに移動します。
   b. ITPAM_eem.xml ファイルを開きます。
   c. 以下の行で「itpamcertpass」を置換します。

      ```
      <Register certfile="itpamcert.p12" password="itpamcertpass"/>
      ```

   d. ファイルを保存します。

管理 CA Enterprise Log Manager への XML ファイルのコピー

safex コマンドは、ITPAM_eem.xml ファイルから CA IT PAM セキュリティ オブジェクトを生成します。このファイルは、safex 処理中にアクセス可能な CA Enterprise Log Manager アプライアンスにコピーする必要があります。

ITPAM_eem.xml ファイルを CA Enterprise Log Manager アプライアンスにコピーする方法

CA IT PAM インストール ディスク内の ITPAM_eem.xml ファイルを、CA EEM が含まれる CA Enterprise Log Manager アプライアンスにコピーします。Windows サーバ上に iso ファイルを解凍した場合は、Winscp を使用して、アプライアンスの /tmp ディレクトリに ITPAM_eem.xml をコピーします。

- CA IT PAM インストール ディスク内のソース ファイル:

  ```
  ITPAM_eem.xml
  ```

- 管理 CA Enterprise Log Manager 上の宛先パス:

  ```
  /opt/CA/SharedComponents/iTechnology
  ```

共有される CA EEM での CA IT PAM の登録

CA Enterprise Log Manager 管理サーバに組み込まれている CA EEM に CA IT PAM を登録することができます。CA EEM を登録すると、CA IT PAM セキュリティ オブジェクトが追加されます。

登録中に CA EEM に追加される CA IT PAM セキュリティ オブジェクトには以下が含まれます。

- アプリケーション インスタンス ITPAM
- CA IT PAM のアクセスに関連するポリシー
- グループおよびユーザ（事前定義された ITPAMAdmins、ITPAMUsers、itpamadmin、itpamuser を含む）
- 証明書 itpamcert.p12

CA IT PAM セキュリティ オブジェクトは、CA Enterprise Log Manager 管理サーバ上に作成できます。始める前に、caelmadmin パスワードがわかっていない場合は取得する必要があります。

CA Enterprise Log Manager 管理サーバ上の CA EEM に CA IT PAM を登録する方法

1. ssh を使用して、caelmadmin ユーザとして CA Enterprise Log Manager アプライアンスにログオンします。
2. 次のコマンドを使用して、ユーザを root アカウントに切り替えます。

   ```
   su -
   ```

3. ディレクトリをターゲット パスに変更し、コンテンツをリスト表示します。

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ls
   ```

4. 以下のファイルが存在することを確認します。
   - ITPAM_eem.xml
   - safex

5. 次のコマンドを実行します。

   ```
   ./safex -h <ELM_hostname> -u EiamAdmin -p <password> -f ITPAM_eem.xml
   ```

   このプロセスは、CA Enterprise Log Manager 管理サーバ内に CA IT PAM アプリケーションを作成し、デフォルト ユーザを追加し、IT PAM のインストールで必要とされる証明書を生成します。この証明書は、ITPAM_eem.xml ファイルに指定されたパスワード、または変更されていない場合は itpamcertpass で生成されます。

   注: safex コマンドの使用について参照するには、./safex を入力します。

6. ディレクトリのコンテンツをリスト表示し、itpamcert.cer が存在することを確認します。

7. CA IT PAM の XML 設定ファイルを削除します。これは、セキュリティ上の理由から推奨される手順です。

   ```
   rm ITPAM_eem.xml
   ```

CA IT PAM サーバへの証明書のコピー

CA IT PAM を CA EEM に登録するために CA Enterprise Log Manager から safex コマンドを実行した場合、このプロセスによって itpamcert.p12 証明書が生成されました。この証明書は、CA IT PAM ドメインのインストール先の Windows サーバにコピーする必要があります。CA IT PAM ドメインのインストール中に、この証明書ファイルを使用します。

CA Enterprise Log Manager アプライアンスからターゲットの Windows サーバに証明書をコピーする方法

itpamcert.p12 ファイルを、CA EEM が含まれる CA Enterprise Log Manager アプライアンスから、CA IT PAM のインストール先のホストにコピーします。

- CA Enterprise Log Manager 管理サーバ上のソース ファイル:

  ```
  /opt/CA/SharedComponents/iTechnology/itpamcert.p12
  ```

- ターゲット Windows サーバ上の宛先パス:

  <インストール パス>

  注: このファイルは、指定したパスにコピーできます。このファイルは、CA IT PAM ドメインをインストールする際に、その場所から選択します。

事前定義された CA IT PAM ユーザ アカウントのパスワードの設定

safex コマンドを実行すると、以下が作成されます。

- IT PAM セキュリティ グループ
  - ITPAMAdmins
  - ITPAMUsers
- IT PAM ユーザ
  - itpamadmin（デフォルト パスワードを使用）
  - itpamuser（デフォルト パスワードを使用）

これらの事前定義済みの 2 つの IT PAM ユーザに対しては、パスワードをリセットする必要があります。

CA EEM 上の IT PAM アプリケーションで itpamadmin および itpamuser のパスワードをリセットする方法

1. CA Enterprise Log Manager によって使用される CA EEM がインストールされているサーバの URL にアクセスします。CA Enterprise Log Manager 管理サーバの例:

   `https://<ELM_managementserver>5250/spin/eiam`

   CA EEM ログオン画面が表示されます。[アプリケーション]のドロップダウンリストには <グローバル>、CAELM、ITPAM が含まれます。

2. IT PAM アプリケーションにログインします。
   a. アプリケーションとして ITPAM を選択します。
   b. ユーザ名として EiamAdmin を入力します。
   c. EiamAdmin ユーザ アカウントのパスワードを入力します。
   d. [Log In]をクリックします。
3. [Manage Identities]タブをクリックします。
4. [Search Users]ダイアログ ボックスで、値に itpam を入力し、[Go]をクリックします。

   リストに以下のユーザが表示されます。
   - itpamadmin
   - itpamuser

5. itpamadmin のパスワードをリセットします。
   a. リストから itpamadmin を選択し、右ペインで［Authentication］にスクロールします。
   b. ［Reset Password］を選択します。
   c. このアカウントの新しいパスワードを入力し、確認用に再度入力します。
   d. ［Save］をクリックします。
6. itpamuser のパスワードをリセットします。
   a. リストから itpamuser を選択し、右ペインで［Authentication］にスクロールします。
   b. ［Reset Password］を選択します。
   c. このアカウントの新しいパスワードを入力し、確認用に再度入力します。
   d. ［Save］をクリックします。
7. ［Log Out］をクリックします。

CA IT PAM が必要とするサードパーティコンポーネントのインストール

サードパーティコンポーネントをインストールする前に、JDK 1.6 以上をシステムにインストールする必要があります。CA IT PAM をインストールする Windows サーバで Third_Party_Installer_windows.exe を実行します。詳細については、「*CA IT Process Automation Manager Installation Guide*」を参照してください。

CA IT PAM ドメインのインストール

CA IT PAM ウィザードを、ここで説明する手順どおりに実行すると、証明書がリンクされ、CA Enterprise Log Manager 管理サーバ上で CA IT PAM および CA EEM の信頼が確立します。

次の情報を用意します。

- EEM 証明書ファイル itpamcert.p12 のパスワード。「共有 CA EEM 上での CA IT PAM 認証の実装準備」の手順で、ITPAM_eem.xml ファイル内のデフォルトを変更している場合があります。
- CA Enterprise Log Manager 管理サーバのホスト名。これは、「共有 CA EEM への CA IT PAM の登録」の手順でログインしたサーバです。
- itpamadmin パスワード(「事前定義された CA IT PAM ユーザ アカウントのパスワードの設定」の手順で設定)。
- パスワードの暗号化に使用される鍵へのアクセスを制御するための証明書パスワード。これは新しい設定です(既存のものではありません)。

CA IT PAM ドメインのインストール手順については、ソフトウェアに付随する「CA IT Process Automation Manager Installation Guide」を参照してください。EEM セキュリティ設定を指定するには、以下の手順に従います。

CA IT PAM ドメインをインストールする方法

1. サードパーティ コンポーネントのインストールの一環として IT PAM インストール ウィザードが起動しない場合は、CA_ITPAM_Domain_windows.exe を起動します。
2. CA IT PAM ドキュメントの手順に従い、セキュリティ サーバ タイプの選択まで進みます。
3. [Select Security Server Type]ダイアログ ボックスが表示されたら、セキュリティ サーバとして EEM を選択し、[Next]をクリックします。

   [EEM Security Settings]ページが表示されます。

4. EEM セキュリティ設定を以下の手順で完了します。
   a. EEM サーバ フィールドに CA Enterprise Log Manager 管理サーバのホスト名を入力します。
   b. EEM アプリケーション フィールドに ITPAM を入力します。
   c. [Browse]をクリックし、itpamcert.p12 が含まれているフォルダに移動します。
   d. itpamcert.p12 を選択します。
   e. 以下のいずれかの方法で、[EEM Certificate Password]フィールドに入力します。
      - 準備の手順で、ITPAM_eem.xml ファイル内で置き換えたパスワードを入力します。
      - デフォルトのパスワード itpamcertpass を入力します。
5. [EEM 設定のテスト]をクリックします。

   「テストを実行するには数分かかる場合があります。」という内容のメッセージが表示されます。
6. [OK]をクリックします。

   [EEM 設定の検証]ダイアログ ボックスが表示されます。
7. ユーザ名として itpamadmin を入力します。 itpamadmin ユーザ アカウントに設定したパスワードを入力し、[OK]をクリックします。
8. [次へ]をクリックします。IT PAM ドキュメント内の説明に従って、ウィザードの残りの手順を完了します。

CA ITPAM Server サービスの開始

CA IT PAM サーバを起動できるように、CA ITPAM Server サービスを開始します。

CA ITPAM Server サービスの開始

1. CA IT PAM ドメインをインストールした Windows サーバにログオンします。
2. [スタート]メニューから、[すべてのプログラム]-[ITPAM Domain]-[Start Server Service]を選択します。

   注: このメニュー オプションが表示されない場合、[管理ツール]-[コンポーネント サービス]を選択します。[Services]をクリックし、[CA IT PAM Server]をクリックして[Start the service]をクリックします。

CA IT PAM サーバ コンソールの起動とログイン

CA IT PAM サーバは、Java JRE 1.6 または JDK 1.6 api がインストールおよび統合されているシステムのブラウザから起動できます。

CA IT PAM 管理コンソールを起動する方法

1. ブラウザのアドレス バーに以下の URL を入力します。

   `http://<itpam_server_hostname>:8080/itpam/`

   CA IT Process Automation Manager のログオン画面が表示されます。

2. [User Login]フィールドに itpamadmin を入力します。
3. [Password]フィールドに、このユーザ アカウントに割り当てたパスワードを入力します。
4. [Log In]をクリックします。

   CA Enterprise Log Manager アプライアンスの CA EEM はユーザのログイン認証情報を認証し、CA IT Process Automation Manager を開きます。

CA IT PAM と CA Enterprise Log Manager の統合および使い方の詳細については、「*CA Enterprise Log Manager 管理ガイド*」のアクション アラートの章にある、「CA IT PAM イベント/出力プロセスの使用」セクションを参照してください。

付録 D: 惨事復旧

このセクションには、以下のトピックが含まれています。

惨事復旧計画

惨事復旧計画は、優れたネットワーク管理計画に欠かすことのできない要素です。CA Enterprise Log Manager の惨事復旧計画は比較的単純で簡単です。CA Enterprise Log Manager の惨事復旧を成功させる鍵は、定期的なバックアップを維持することにあります。

次の情報のバックアップを作成する必要があります。

- 管理サーバの CA Enterprise Log Manager アプリケーション インスタンス
- 各 CA Enterprise Log Manager サーバ上の /opt/CA/LogManager/data フォルダ
- 各 CA Enterprise Log Manager サーバ上の /opt/CA/SharedComponents/iTechnology フォルダの証明書ファイル

実装において高いレベルのスループットを維持することが重要である場合、他の CA Enterprise Log Manager サーバをインストールしたものと同じハードウェア特性を備えた予備サーバを用意しておくこともできます。1 つの CA Enterprise Log Manager サーバが使用できなくなった場合、まったく同じ名前を使用して別の CA Enterprise Log Manager サーバをインストールできます。新しいサーバが起動するときに、管理サーバから必要な設定ファイルを受信します。実装においてこのレベルのパフォーマンスが重要ではない場合、基本的なオペレーティング システムをホストすることができ、メモリおよびハード ディスクの最小要件を満たした未使用のサーバに CA Enterprise Log Manager サーバをインストールできます。

ハードウェアとソフトウェアの要件に関する詳細については、「CA Enterprise Log Manager リリース ノート」で説明しています。

また、管理サーバにインストールされた内部の CA EEM サーバには、操作を確実に継続するための独自のフェイルオーバー設定プロセスがあり、「CA EEM 導入ガイド」で詳細に説明しています。

CA EEM サーバのバックアップについて

クエリ、レポート、アラートなどに加えて、各 CA Enterprise Log Manager サーバ、エージェント、およびコネクタの設定は、管理用 CA Enterprise Log Manager サーバの CA EEM リポジトリに個別に保持されます。サーバのリカバリを成功させるために重要なのは、CA Enterprise Log Manager アプリケーション インスタンスに保存された情報の定期的なバックアップを維持することです。

アプリケーション インスタンスは、CA EEM リポジトリの共用の領域にあります。このリポジトリでは次の情報を保存します。

- ユーザ、グループ、およびアクセス ポリシー
- エージェント、統合、リスナ、コネクタ、および保存済み設定
- カスタマイズされたクエリ、レポート、および抑制ルールと集約ルール
- 連携関係
- バイナリ コードの管理情報
- 暗号化鍵

CA EEM Web ブラウザ インターフェース内から、CA EEM のバックアップ処理を実行できます。通常は、企業内のすべての CA Enterprise Log Manager サーバが同じアプリケーション インスタンスを使用します。CA Enterprise Log Manager アプリケーション インスタンスのデフォルト値は CAELM です。別のアプリケーション インスタンスを使用して CA Enterprise Log Manager サーバをインストールできますが、同じアプリケーション インスタンスを共有するサーバだけが連携できます。同じ CA EEM サーバを使用し、一方で別のアプリケーション インスタンスを使用するように設定されたサーバは、ユーザ ストア、パスワード ポリシー、およびグローバル グループのみを共有します。

「CA EEM 導入ガイド」では、バックアップと復元処理の詳細について説明しています。

CA EEM アプリケーション インスタンスのバックアップ

管理サーバ内部の CA EEM サーバから、CA Enterprise Log Manager アプリケーション インスタンスのバックアップを実行できます。

アプリケーション インスタンスをバックアップする方法

1. 次の URL を使用して CA EEM サーバにアクセスします。

   `https://<servername>:5250/spin/eiam`

2. ログイン ページの[アプリケーション]リストを展開し、CA Enterprise Log Manager サーバをインストールしたときに使用したアプリケーション インスタンス名を選択します。

   CA Enterprise Log Manager のデフォルトのアプリケーション インスタンス名は CAELM です。

3. EiamAdmin ユーザまたは CA EEM の Administrator ロールを持つユーザとしてログインします。

4. [設定]タブにアクセスして、[EEM サーバ]サブタブを選択します。

5. 左側のナビゲーション ペインで[アプリケーションのエクスポート]の項目を選択します。

6. [最大検索サイズの上書き]チェック ボックス以外のすべてのオプションをオンにします。

   注: 外部ディレクトリを使用している場合は、[グローバル ユーザ]、[グローバル グループ]、および[グローバル フォルダ]オプションを選択しないでください。

7. [エクスポート]をクリックして、アプリケーション インスタンスの XML エクスポート ファイルを作成します。

   [ファイルのダウンロード]ダイアログ ボックスに、ファイル名 *<AppInstanceName>*.xml.gz (たとえば CAELM.xml.gz)と[保存]ボタンが表示されます。

8. [保存]をクリックし、マッピングされたリモート サーバにあるバックアップの保存場所を選択します。 あるいは、ファイルをローカルに保存して、別のサーバのバックアップの保存場所にこのファイルをコピーまたは移動します。

CA Enterprise Log Manager と併用する CA EEM サーバの復元

CA Enterprise Log Manager アプリケーション インスタンスを管理サーバに復元できます。管理サーバの CA EEM 機能の復元には、バックアップされたアプリケーション インスタンスをインポートする safex ユーティリティの実行が含まれます。

バックアップから管理サーバの CA EEM 機能を復元する方法

1. 新しいハードウェア サーバに CA Enterprise Log Manager ソフト アプライアンスをインストールします。
2. コマンド プロンプトにアクセスし、/opt/CA/LogManager/EEM ディレクトリに移動します。
3. バックアップ ファイル *<AppinstanceName>*.xml.gz を外部のバックアップ サーバからこのディレクトリにコピーします。
4. 次のコマンドを実行して XML のエクスポート ファイルを取得します。

   `gunzip <AppinstanceName>.xml.gz`
5. 次のコマンドを実行して、新しい管理サーバにエクスポート ファイルを復元します。

   `./safex –h eemserverhostname –u EiamAdmin –p password –f AppinstanceName.xml`

   FIPS モードで実行している場合は、必ず -fips オプションを指定してください。
6. /opt/CA/ELMAgent/bin ディレクトリに移動します。
7. デフォルトの AgentCert.cer ファイルをバックアップ ファイルの CAELM_AgentCert.cer で置き換え、エージェントが正しくセットアップされるようにします。

CA Enterprise Log Manager サーバのバックアップ

/opt/CA/LogManager/data フォルダから CA Enterprise Log Manager サーバ全体をバックアップできます。このデータ フォルダは、ルート ディレクトリの下の data フォルダ（/data）へのシンボリック リンクです。

CA Enterprise Log Manager サーバをバックアップする方法

1. caelmadmin ユーザとして CA Enterprise Log Manager サーバにログインします。
2. su ユーティリティを使用して、root アカウントにアクセスします。
3. /opt/CA/LogManager ディレクトリに移動します。
4. 次の TAR コマンドを実行して CA Enterprise Log Manager サーバ ファイルのバックアップ コピーを作成します。

   ```
   tar –hzcvf backupData.tgz /data
   ```

   このコマンドは、/data ディレクトリのファイルを使用して、圧縮された出力ファイル backupData.tgz を作成します。
5. /opt/CA/SharedComponents/iTechnology ディレクトリに移動します。
6. 次の TAR コマンドを実行して、デジタル証明書（.cer というファイル拡張子を持つすべてのファイル）のバックアップ コピーを作成します。

   ```
   tar –zcvf backupCerts.tgz *.cer
   ```

   このコマンドは、圧縮された出力ファイル backupCerts.tgz を作成します。

   ```
   tar –hzcvf backupCerts.tgz /data
   ```

バックアップ ファイルからの CA Enterprise Log Manager サーバの復元

新しいサーバに CA Enterprise Log Manager ソフトウェア アプライアンスをインストールしたら、バックアップ ファイルから CA Enterprise Log Manager サーバを復元できます。

バックアップから CA Enterprise Log Manager サーバを復元する方法

1. 新しいサーバの iGateway プロセスを停止します。

   停止するには、/opt/CA/SharedComponents/iTechnology フォルダに移動して、次のコマンドを実行します。

   ```
   ./S99igateway stop
   ```

2. backupData.tgz と backupCerts.tgz のファイルを新しいサーバの /opt/CA/LogManager ディレクトリにコピーします。
3. 次のコマンドを使用して、backupData.tgz ファイルの内容を展開します。

   ```
   tar –xzvf  backupData.tgz
   ```

   このコマンドは、データ フォルダの内容をバックアップ ファイルの内容で上書きします。
4. /opt/CA/SharedComponents/iTechnology ディレクトリに移動します。
5. 次のコマンドを使用して backupCerts.tgz ファイルのコンテンツを展開します。

   ```
   tar –xzvf  backupCerts.tgz
   ```

   このコマンドは、現在のフォルダにある証明書(.p12)ファイルをバックアップ ファイルの証明書ファイルで上書きします。
6. iGateway プロセスを開始します。

   開始するには、次のコマンドを実行します。

   ```
   ./S99igateway start
   ```

サブスクリプション更新後の CA Enterprise Log Manager サーバの復元

サブスクリプション更新が失敗したか、または望まないサブスクリプション更新が行われた場合は、CA Enterprise Log Manager サーバを復元できます。各サブスクリプション ダウンロードではバックアップ ファイルが作成され、そのラベルとしてバックアップの日付が付けられます。以下の手順では、EEM または他のコンポーネントではなく、ログ マネージャ サーバのみが復元されます。

サブスクリプション更新後にサーバを復元する方法

1. 新しいサーバの iGateway プロセスを停止します。

   停止するには、/opt/CA/SharedComponents/iTechnology フォルダに移動して、次のコマンドを実行します。

   ```
   ./S99igateway stop
   ```

2. /opt/CA/SharedComponents/iTechnology ディレクトリに移動します。
3. 以下のコマンドを入力します。

   ```
   sh ./restore.sh <backupdate> <backupversion>
   ```

   例:

   ```
   sh ./restore.sh 22-Sep-2010 12.0.45.10
   ```

4. /opt/CA/SharedComponents/iTechnology ディレクトリに移動します。
5. iGateway プロセスを開始します。

   開始するには、次のコマンドを実行します。

   ```
   ./S99igateway start
   ```

CA Enterprise Log Manager サーバの交換

大きな災害や障害の後に収集用 CA Enterprise Log Manager サーバを交換する場合は、以下の手順に従います。この手順を使用すると、障害が発生したサーバの代わりにイベント収集を再開するための新しい CA Enterprise Log Manager サーバを作成することによって、障害状況から回復できます。

注: この手順では、障害が発生したサーバのイベント ログ ストアに存在するイベント データの回復は行いません。ダウンしたサーバのイベント ログ ストアからイベント データを取得するには、通常のデータ リカバリ テクニックを使用します。

使用できなくなった CA Enterprise Log Manager サーバを回復する方法

1. ダウンしたサーバに割り当てたのと同じホスト名を使用して、別のサーバに CA Enterprise Log Manager ソフトウェアをインストールします。

   インストール時に CA EEM アプリケーション インスタンス名を要求されたら、必ず古いサーバが使用したのと同じアプリケーション インスタンスを使用します。登録が成功すると、CA EEM サーバは設定を同期できます。

2. 新しい CA Enterprise Log Manager サーバを起動し、デフォルトの管理者ユーザ EiamAdmin としてログインします。

   新しい CA Enterprise Log Manager サーバを起動すると、自動的に CA EEM サーバに接続して設定ファイルをダウンロードします。設定ファイルを受信すると、新しい CA Enterprise Log Manager サーバはログ収集を再開します。

付録 E: CA Enterprise Log Manager と仮想化

このセクションには、以下のトピックが含まれています。

展開の前提条件

仮想環境で CA Enterprise Log Manager を使用する場合、または装置クラスと仮想サーバの両方を含む混合環境を使用する場合は、次の内容を前提としています。

- すべての仮想環境に、管理サーバとして少なくとも 1 つの CA Enterprise Log Manager サーバをインストールします。この管理サーバは設定、サブスクリプション コンテンツ、ユーザ定義コンテンツを管理し、エージェントと通信します。管理サーバではイベント ログを受信せず、クエリとレポートの処理は行いません。
- 混合環境では、認定されたハードウェアに管理用 CA Enterprise Log Manager サーバをインストールします。
- 仮想マシンホストには専用プロセッサがそれぞれ 4 つ必要です。これは、VMware ESX Server 3.5 で許可される最大数になります。

注意事項

8 つ以上のプロセッサを備えた専用の CA Enterprise Log Manager サーバを使用すると、最適なパフォーマンスが得られます。VMware ESX Server では、単一の仮想マシンに最大 4 つまでプロセッサを使用できます。8 つのプロセッサを持つ専用サーバと同様のパフォーマンスを得るには、2 つ以上の仮想マシンに CA Enterprise Log Manager をインストールし、統合レポート用にそのサーバを連携させます。

VMware ESX Server v3.5 の下でゲストとして 2 つの CA Enterprise Log Manager サーバを実行すると、1 台の専用の CA Enterprise Log Manager サーバの能力に近くなります。次の表を使用すると、仮想ネットワークを計画する場合に役立ちます。

CA Enterprise Log Manager サーバのロール	プロセッサ数（最小）	CPU 速度 - GHz（CPU 当たり）	合計メモリ - GB（最小要件）
管理	8	3	8
レポート	8	3	8
収集	4	3	8

注: 1 秒あたりの最大イベントは 1K、中程度の展開設定では 1K、大規模な展開設定では 5K になります。

仮想マシンを使用した CA Enterprise Log Manager サーバの作成

次のシナリオを使用して、イベント ログ収集環境用の仮想 CA Enterprise Log Manager サーバを作成できます。

- 既存の CA Enterprise Log Manager 環境に仮想サーバを追加: 混合環境を作成します。
- 仮想ログ収集環境の作成
- 迅速な拡張に向けた仮想 CA Enterprise Log Manager サーバのクローニングと展開
- 仮想アプライアンスを使用した CA Enterprise Log Manager サーバの作成

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

使用している環境への仮想サーバの追加

すでに CA Enterprise Log Manager が実装されている場合は、ネットワークに仮想の CA Enterprise Log Manager 収集サーバを追加して、増加したイベント ボリュームを処理できます。このシナリオでは、すでに CA Enterprise Log Manager 管理サーバと 1 つ以上の収集およびレポート用 CA Enterprise Log Manager サーバがインストールされていることを前提とします。

注: 最高のパフォーマンスを得るには、仮想サーバに CA Enterprise Log Manager サーバをインストールして、収集タスクとレポート タスクのみを処理します。

環境に仮想収集サーバを追加するプロセスには、次の手順が含まれます。

1. 新しい仮想マシンを作成します。
2. 仮想ディスクドライブを追加します。
3. 仮想マシンに CA Enterprise Log Manager をインストールします。
4. インストール セクションの説明に従って CA Enterprise Log Manager サーバを設定します。

仮想収集サーバをインストールしたら、クエリとレポートを実行できるようにそのサーバを連携に追加できます。

新しい仮想マシンの作成

VMware Infrastructure Client を使用して新しい仮想マシンを作成するには、次の手順を使用します。満足できるパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバごとに 4 つのプロセッサを使用します。

仮想マシンを作成する方法

1. VMware Infrastructure Client にアクセスします。
2. 左側のペインの ESX ホストを右クリックし、[新規仮想マシン]を選択して新しい仮想マシンのウィザードを呼び出します。このアクションによって、設定タイプのダイアログ ボックスが表示されます。
3. [カスタム設定]を選択して、[次へ]をクリックします。名前と場所を示すダイアログ ボックスが表示されます。

4. この仮想マシンにインストールする CA Enterprise Log Manager サーバの名前を入力し、[次へ]をクリックします。
5. 仮想マシンの保存設定を指定して、[次へ]をクリックします。

   保存設定が CA Enterprise Log Manager サーバに対して十分な大きさであることを確認します。少なくとも 500 GB を設定することをお勧めします。

   注: 他の手順で収集されたイベント ログを保存するには、追加の仮想ディスク ドライブをセット アップします。
6. ゲスト オペレーティング システムとして Red Hat Enterprise Linux 5 (32 ビット)を選択し、[次へ]をクリックします。
7. [仮想プロセッサの数]ドロップダウン リストから、仮想プロセッサの数として[4]を選択します。

   物理ホスト サーバは、この CA Enterprise Log Manager インスタンスだけに 4 つの物理 CPU を割り当てることができる必要があります。[次へ]をクリックします。
8. 仮想マシンのメモリ サイズを設定して、[次へ]をクリックします。CA Enterprise Log Manager の許容可能な最小メモリ サイズは、8 GB (すなわち 8,192 MB)です。
9. ネットワーク インターフェース接続 (NIC)を設定します。CA Enterprise Log Manager には少なくとも 1 つのネットワーク接続が必要です。使用可能な NIC のリストから NIC を選択し、[アダプタ]の値を[フレキシブル]に設定します。

   注: この物理サーバにホストされた各 CA Enterprise Log Manager サーバに対して、個別の NIC を設定する必要はありません。ただし、サーバごとに静的な IP アドレスを割り当てる必要があります。
10. [電源投入時に接続]オプションを選択して、[次へ]をクリックします。[I/O アダプタのタイプ]ダイアログ ボックスが表示されます。
11. [I/O アダプタ]に[LSI ロジック]を選択して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。
12. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。ディスク容量と場所を入力するダイアログ ボックスが表示されます。

13. ディスク容量および場所を指定して、[次へ]をクリックします。詳細設定オプションを指定するダイアログ ボックスが表示されます。

    仮想マシンを使用してこのディスクに保存できます。あるいは、別の場所を指定することもできます。少なくとも 500 GB を設定することをお勧めします。

14. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。

15. 設定を確認して[完了]をクリックし、新しい仮想マシンを作成します。

仮想ディスクドライブの追加

イベント ログの保存用に仮想ディスクドライブを追加するには、次の手順を使用します。特定の CA Enterprise Log Manager サーバがネットワーク内で担当するロールにかかわらず、同じ設定を使用します。

設定を編集する方法

1. VMware Infrastructure Client の仮想マシンを右クリックし、[設定の編集]を選択します。

   [仮想マシンのプロパティ]ダイアログ ボックスが表示されます。

2. [CD/DVD ドライブ 1]のプロパティを強調表示します。

3. [ホスト デバイス]オプション ボタンをクリックし、ドロップダウン リストから DVD-ROM ドライブを選択します。

4. [デバイスのステータス]オプションの[電源投入時に接続]を選択します。

5. [追加]をクリックして[ハードウェアの追加]ウィザードを起動し、2 つ目のハード ディスクを追加します。

6. デバイス リストで[ハード ディスク]を強調表示して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。

7. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。

8. 新しいディスクのサイズを指定して、[データストアを指定して場所を設定する]オプションを選択します。

   CA Enterprise Log Manager はインストール中にこの追加のドライブを検出し、そのドライブをデータ ストレージに割り当てます。CA Enterprise Log Manager が使用可能なストレージの量を最大にすることをお勧めします。

   注: VMware ESX Server のデフォルトのブロック サイズ設定は 1 MB であるため、作成可能な最大ディスク容量が 256 GB までに制限されます。さらに多くの容量が必要な場合は、次のコマンドを使用して、ブロック サイズの設定を 2 MB に増やします(最大 512 GB)。

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   新しい設定を有効にするには、ESX Server を再起動します。このコマンドとその他のコマンドの詳細については、VMware ESX Server のドキュメントで説明しています。

   [次へ]をクリックして[詳細オプションの指定]ダイアログ ボックスを表示します。

9. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。作業完了を示すダイアログ ボックスが表示されます。

10. [完了]をクリックして、この仮想マシンへの変更を保存します。このアクションで VMware Infrastructure Client のダイアログ ボックスに戻ります。

仮想マシンでの CA Enterprise Log Manager のインストール

事前に作成した仮想マシンに CA Enterprise Log Manager をインストールするには、次の手順を使用します。

インストール後に、仮想または専用の CA Enterprise Log Manager サーバが、管理、収集、またはレポートといった複数の機能ロールの 1 つを担当するように設定できます。CA Enterprise Log Manager 管理サーバをインストールする場合は、イベント ログの受信やクエリおよびレポートの実行に管理サーバを使用しないでください。最高のパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバを個別にインストールして、レポート サーバおよび収集サーバとして動作させます。

仮想環境に CA Enterprise Log Manager をインストールする前に、通常のインストール手順を確認します。インストールのワークシートを使用すると、必要な情報を収集できます。

仮想マシンに CA Enterprise Log Manager をインストールする方法

1. 物理 DVD-ROM ドライブで CA Enterprise Log Manager の OS インストール ディスクをロードするか、インストール イメージをコピーしたディレクトリを検索します。
2. 仮想マシンのインベントリ リストで仮想マシンを強調表示し、それを右クリックして[電源投入]を選択します。
3. 通常の CA Enterprise Log Manager のインストールを続行します。
4. CA Enterprise Log Manager サーバのインストールに関するセクションの情報を使用して、目的の機能のロールをインストールされた CA Enterprise Log Manager サーバに設定します。

詳細情報

CA Enterprise Log Manager のインストール (P. 81)

完全な仮想環境の作成

まだ CA Enterprise Log Manager 環境を実装していない場合は、すべてを仮想化したログ収集環境を作成できます。このシナリオでは、目的の各 CA Enterprise Log Manager サーバをインストールするために、十分な数の物理サーバが使用可能で、その各サーバに少なくとも 4 つのプロセッサ グループがあることを前提としています。

管理サーバとして動作する CA Enterprise Log Manager サーバを 1 台インストールします。 設定中にこのサーバにイベント ログを送信しないでください。または、このサーバを使用してレポートを生成しないでください。この方法で環境を設定すると、エンタープライズ レベルの本稼働環境に必要なイベント ログ収集のスループットを維持できます。

一般的には、認定されたハードウェアを使用する場合に通常インストールする各装置クラス サーバの代わりに、4 つのプロセッサを 2 つ持つ CA Enterprise Log Manager サーバをインストールします (アプライアンスクラスのサーバには、最低 8 つのプロセッサがあります)。

仮想環境を作成するプロセスには、次の手順が含まれます。

1. インストールする予定の各 CA Enterprise Log Manager サーバに新しい仮想マシンを作成します。
2. 仮想ディスクドライブを追加します。
3. 仮想マシン ホストのうちの 1 つに、管理機能用の仮想 CA Enterprise Log Manager サーバをインストールします。
4. 収集およびレポート用に、2 つ以上の CA Enterprise Log Manager サーバをインストールします。
5. CA Enterprise Log Manager サーバのインストールに関するセクションの説明に従って、CA Enterprise Log Manager サーバを設定します。

新しい仮想マシンの作成

VMware Infrastructure Client を使用して新しい仮想マシンを作成するには、次の手順を使用します。満足できるパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバごとに 4 つのプロセッサを使用します。

仮想マシンを作成する方法

1. VMware Infrastructure Client にアクセスします。
2. 左側のペインの ESX ホストを右クリックし、[新規仮想マシン]を選択して新しい仮想マシンのウィザードを呼び出します。このアクションによって、設定タイプのダイアログ ボックスが表示されます。
3. [カスタム設定]を選択して、[次へ]をクリックします。名前と場所を示すダイアログ ボックスが表示されます。
4. この仮想マシンにインストールする CA Enterprise Log Manager サーバの名前を入力し、[次へ]をクリックします。
5. 仮想マシンの保存設定を指定して、[次へ]をクリックします。

   保存設定が CA Enterprise Log Manager サーバに対して十分な大きさであることを確認します。少なくとも 500 GB を設定することをお勧めします。

   注: 他の手順で収集されたイベント ログを保存するには、追加の仮想ディスクドライブをセット アップします。
6. ゲスト オペレーティング システムとして Red Hat Enterprise Linux 5 (32 ビット)を選択し、[次へ]をクリックします。

7. [仮想プロセッサの数]ドロップダウン リストから、仮想プロセッサの数として[4]を選択します。

   物理ホスト サーバは、この CA Enterprise Log Manager インスタンスだけに 4 つの物理 CPU を割り当てることができる必要があります。[次へ]をクリックします。

8. 仮想マシンのメモリ サイズを設定して、[次へ]をクリックします。CA Enterprise Log Manager の許容可能な最小メモリ サイズは、8 GB(すなわち 8,192 MB)です。

9. ネットワーク インターフェース接続(NIC)を設定します。CA Enterprise Log Manager には少なくとも 1 つのネットワーク接続が必要です。使用可能な NIC のリストから NIC を選択し、[アダプタ]の値を[フレキシブル]に設定します。

   注: この物理サーバにホストされた各 CA Enterprise Log Manager サーバに対して、個別の NIC を設定する必要はありません。ただし、サーバごとに静的な IP アドレスを割り当てる必要があります。

10. [電源投入時に接続]オプションを選択して、[次へ]をクリックします。[I/O アダプタのタイプ]ダイアログ ボックスが表示されます。

11. [I/O アダプタ]に[LSI ロジック]を選択して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。

12. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。ディスク容量と場所を入力するダイアログ ボックスが表示されます。

13. ディスク容量および場所を指定して、[次へ]をクリックします。詳細設定オプションを指定するダイアログ ボックスが表示されます。

    仮想マシンを使用してこのディスクに保存できます。あるいは、別の場所を指定することもできます。少なくとも 500 GB を設定することをお勧めします。

14. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。

15. 設定を確認して[完了]をクリックし、新しい仮想マシンを作成します。

仮想ディスクドライブの追加

イベント ログの保存用に仮想ディスクドライブを追加するには、次の手順を使用します。特定の CA Enterprise Log Manager サーバがネットワーク内で担当するロールにかかわらず、同じ設定を使用します。

設定を編集する方法

1. VMware Infrastructure Client の仮想マシンを右クリックし、[設定の編集]を選択します。

   [仮想マシンのプロパティ]ダイアログ ボックスが表示されます。

2. [CD/DVD ドライブ 1]のプロパティを強調表示します。
3. [ホスト デバイス]オプション ボタンをクリックし、ドロップダウン リストから DVD-ROM ドライブを選択します。
4. [デバイスのステータス]オプションの[電源投入時に接続]を選択します。
5. [追加]をクリックして[ハードウェアの追加]ウィザードを起動し、2 つ目のハード ディスクを追加します。
6. デバイス リストで[ハード ディスク]を強調表示して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。
7. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。
8. 新しいディスクのサイズを指定して、[データストアを指定して場所を設定する]オプションを選択します。

   CA Enterprise Log Manager はインストール中にこの追加のドライブを検出し、そのドライブをデータ ストレージに割り当てます。CA Enterprise Log Manager が使用可能なストレージの量を最大にすることをお勧めします。

   注: VMware ESX Server のデフォルトのブロック サイズ設定は 1 MB であるため、作成可能な最大ディスク容量が 256 GB までに制限されます。さらに多くの容量が必要な場合は、次のコマンドを使用して、ブロック サイズの設定を 2 MB に増やします(最大 512 GB)。

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   新しい設定を有効にするには、ESX Server を再起動します。このコマンドとその他のコマンドの詳細については、VMware ESX Server のドキュメントで説明しています。

   [次へ]をクリックして[詳細オプションの指定]ダイアログ ボックスを表示します。

9. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。作業完了を示すダイアログ ボックスが表示されます。
10. [完了]をクリックして、この仮想マシンへの変更を保存します。このアクションで VMware Infrastructure Client のダイアログ ボックスに戻ります。

仮想マシンでの CA Enterprise Log Manager のインストール

事前に作成した仮想マシンに CA Enterprise Log Manager をインストールするには、次の手順を使用します。

インストール後に、仮想または専用の CA Enterprise Log Manager サーバが、管理、収集、またはレポートといった複数の機能ロールの 1 つを担当するように設定できます。CA Enterprise Log Manager 管理サーバをインストールする場合は、イベント ログの受信やクエリおよびレポートの実行に管理サーバを使用しないでください。最高のパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバを個別にインストールして、レポート サーバおよび収集サーバとして動作させます。

仮想環境に CA Enterprise Log Manager をインストールする前に、通常のインストール手順を確認します。インストールのワークシートを使用すると、必要な情報を収集できます。

仮想マシンに CA Enterprise Log Manager をインストールする方法

1. 物理 DVD-ROM ドライブで CA Enterprise Log Manager の OS インストール ディスクをロードするか、インストール イメージをコピーしたディレクトリを検索します。
2. 仮想マシンのインベントリ リストで仮想マシンを強調表示し、それを右クリックして[電源投入]を選択します。
3. 通常の CA Enterprise Log Manager のインストールを続行します。
4. CA Enterprise Log Manager サーバのインストールに関するセクションの情報を使用して、目的の機能のロールをインストールされた CA Enterprise Log Manager サーバに設定します。

詳細情報

CA Enterprise Log Manager のインストール (P. 81)

仮想 CA Enterprise Log Manager サーバの迅速な展開

仮想 CA Enterprise Log Manager サーバをクローンして展開可能なイメージを作成し、ログ収集環境を迅速に拡張することができます。

注: 最高のパフォーマンスを得るには、仮想サーバに CA Enterprise Log Manager サーバをインストールして、収集タスクのみを処理することを推奨します。管理 CA Enterprise Log Manager サーバを含んでいる仮想マシンのクローンは作成しないでください。

このシナリオで始める前に、既存の環境があることを確認します。または、CA Enterprise Log Manager サーバをインストールして、専用サーバもしくは仮想サーバで管理機能が実行されるようにします。さらに、クローニング機能をサポートするために、VMware ソフトウェアの適切なバージョンを所有している必要もあります。

収集用に仮想 CA Enterprise Log Manager サーバを作成しクローンを作るためには、以下の手順に従います。

1. 新しい仮想マシンを作成します。
2. 仮想ディスクドライブを追加します。
3. 仮想マシンに CA Enterprise Log Manager をインストールします。
4. ベンダー提供の手順を使用して、新しい CA Enterprise Log Manager サーバを含んでいる仮想マシンのクローンを作成します。

   注: 完全なクローン イメージだけを作成します。CA Enterprise Log Manager を使用したリンク クローンは使用しないでください。
5. クローンの仮想マシンを物理ターゲット サーバへインポートします。
6. クローンの仮想マシンを更新し、その後ネットワークに接続します。
7. 「実装ガイド」の説明に従って CA Enterprise Log Manager サーバを設定します。

新しい仮想マシンの作成

VMware Infrastructure Client を使用して新しい仮想マシンを作成するには、次の手順を使用します。満足できるパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバごとに 4 つのプロセッサを使用します。

仮想マシンを作成する方法

1. VMware Infrastructure Client にアクセスします。
2. 左側のペインの ESX ホストを右クリックし、[新規仮想マシン]を選択して新しい仮想マシンのウィザードを呼び出します。このアクションによって、設定タイプのダイアログ ボックスが表示されます。
3. [カスタム設定]を選択して、[次へ]をクリックします。名前と場所を示すダイアログ ボックスが表示されます。
4. この仮想マシンにインストールする CA Enterprise Log Manager サーバの名前を入力し、[次へ]をクリックします。
5. 仮想マシンの保存設定を指定して、[次へ]をクリックします。

   保存設定が CA Enterprise Log Manager サーバに対して十分な大きさであることを確認します。少なくとも 500 GB を設定することをお勧めします。

   注: 他の手順で収集されたイベント ログを保存するには、追加の仮想ディスク ドライブをセット アップします。
6. ゲスト オペレーティング システムとして Red Hat Enterprise Linux 5 (32 ビット) を選択し、[次へ]をクリックします。
7. [仮想プロセッサの数]ドロップダウン リストから、仮想プロセッサの数として[4]を選択します。

   物理ホスト サーバは、この CA Enterprise Log Manager インスタンスだけに 4 つの物理 CPU を割り当てることができる必要があります。[次へ]をクリックします。
8. 仮想マシンのメモリ サイズを設定して、[次へ]をクリックします。CA Enterprise Log Manager の許容可能な最小メモリ サイズは、8 GB (すなわち 8,192 MB) です。

9. ネットワーク インターフェース接続(NIC)を設定します。CA Enterprise Log Manager には少なくとも 1 つのネットワーク接続が必要です。使用可能な NIC のリストから NIC を選択し、[アダプタ]の値を[フレキシブル]に設定します。

   注: この物理サーバにホストされた各 CA Enterprise Log Manager サーバに対して、個別の NIC を設定する必要はありません。ただし、サーバごとに静的な IP アドレスを割り当てる必要があります。

10. [電源投入時に接続]オプションを選択して、[次へ]をクリックします。[I/O アダプタのタイプ]ダイアログ ボックスが表示されます。

11. [I/O アダプタ]に[LSI ロジック]を選択して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。

12. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。ディスク容量と場所を入力するダイアログ ボックスが表示されます。

13. ディスク容量および場所を指定して、[次へ]をクリックします。詳細設定オプションを指定するダイアログ ボックスが表示されます。

    仮想マシンを使用してこのディスクに保存できます。あるいは、別の場所を指定することもできます。少なくとも 500 GB を設定することをお勧めします。

14. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。

15. 設定を確認して[完了]をクリックし、新しい仮想マシンを作成します。

仮想ディスクドライブの追加

イベント ログの保存用に仮想ディスクドライブを追加するには、次の手順を使用します。特定の CA Enterprise Log Manager サーバがネットワーク内で担当するロールにかかわらず、同じ設定を使用します。

設定を編集する方法

1. VMware Infrastructure Client の仮想マシンを右クリックし、[設定の編集]を選択します。

   [仮想マシンのプロパティ]ダイアログ ボックスが表示されます。

2. [CD/DVD ドライブ 1]のプロパティを強調表示します。

3. [ホスト デバイス]オプション ボタンをクリックし、ドロップダウン リストから DVD-ROM ドライブを選択します。

4. [デバイスのステータス]オプションの[電源投入時に接続]を選択します。
5. [追加]をクリックして[ハードウェアの追加]ウィザードを起動し、2 つ目のハード ディスクを追加します。
6. デバイス リストで[ハード ディスク]を強調表示して、[次へ]をクリックします。[ディスクの選択]ダイアログ ボックスが表示されます。
7. [新しい仮想ディスクを作成する]オプションを選択して、[次へ]をクリックします。
8. 新しいディスクのサイズを指定して、[データストアを指定して場所を設定する]オプションを選択します。

   CA Enterprise Log Manager はインストール中にこの追加のドライブを検出し、そのドライブをデータ ストレージに割り当てます。CA Enterprise Log Manager が使用可能なストレージの量を最大にすることをお勧めします。

   注: VMware ESX Server のデフォルトのブロック サイズ設定は 1 MB であるため、作成可能な最大ディスク容量が 256 GB までに制限されます。さらに多くの容量が必要な場合は、次のコマンドを使用して、ブロック サイズの設定を 2 MB に増やします(最大 512 GB)。

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   新しい設定を有効にするには、ESX Server を再起動します。このコマンドとその他のコマンドの詳細については、VMware ESX Server のドキュメントで説明しています。

   [次へ]をクリックして[詳細オプションの指定]ダイアログ ボックスを表示します。
9. [詳細設定オプション]のデフォルト値を受け入れ、[次へ]をクリックします。作業完了を示すダイアログ ボックスが表示されます。
10. [完了]をクリックして、この仮想マシンへの変更を保存します。このアクションで VMware Infrastructure Client のダイアログ ボックスに戻ります。

仮想マシンでの CA Enterprise Log Manager のインストール

事前に作成した仮想マシンに CA Enterprise Log Manager をインストールするには、次の手順を使用します。

インストール後に、仮想または専用の CA Enterprise Log Manager サーバが、管理、収集、またはレポートといった複数の機能ロールの 1 つを担当するように設定できます。CA Enterprise Log Manager 管理サーバをインストールする場合は、イベント ログの受信やクエリおよびレポートの実行に管理サーバを使用しないでください。最高のパフォーマンスを得るには、仮想 CA Enterprise Log Manager サーバを個別にインストールして、レポート サーバおよび収集サーバとして動作させます。

仮想環境に CA Enterprise Log Manager をインストールする前に、通常のインストール手順を確認します。インストールのワークシートを使用すると、必要な情報を収集できます。

仮想マシンに CA Enterprise Log Manager をインストールする方法

1. 物理 DVD-ROM ドライブで CA Enterprise Log Manager の OS インストール ディスクをロードするか、インストール イメージをコピーしたディレクトリを検索します。
2. 仮想マシンのインベントリ リストで仮想マシンを強調表示し、それを右クリックして[電源投入]を選択します。
3. 通常の CA Enterprise Log Manager のインストールを続行します。
4. CA Enterprise Log Manager サーバのインストールに関するセクションの情報を使用して、目的の機能のロールをインストールされた CA Enterprise Log Manager サーバに設定します。

詳細情報

CA Enterprise Log Manager のインストール (P. 81)

仮想 CA Enterprise Log Manager サーバのクローン作成

仮想 CA Enterprise Log Manager サーバのクローン作成には、この手順を使用します。この手順では、新しい仮想マシンが作成済みで、ディスクドライブが追加されており、CA Enterprise Log Manager がインストール済みであることが前提となっています。

仮想サーバのクローン作成方法

1. VMware VirtualCenter にアクセスし、CA Enterprise Log Manager を含んでいる仮想マシンを検索します。
2. 仮想マシンが実行中の場合は、マシンの電源をオフにします。
3. エクスポート オプションを選択し、対象の仮想マシンのエクスポート先を指定します。

   VMware ESX Server では、仮想マシンのクローニングに別な方法が提供されています。詳細は、VMware のドキュメントを参照してください。

クローンの仮想マシンをターゲット サーバへインポートします。

クローン仮想マシンを別のサーバへインポートして有効にするには、この手順を使用します。

クローン VM のインポート方法

1. ターゲット ホスト サーバにネットワークでアクセスできることを確認します。
2. VMware ESX をホストするサーバから VMware VirtualCenter にアクセスします。
3. インポート オプションを選択してターゲット サーバを検索し、必要に応じて追加のプロンプトに応答します。

   インポート アクションにより、ターゲット サーバにクローン仮想マシンを移動させます。詳しい情報は、VMware ESX のドキュメントに記載されています。

展開の前にクローン CA Enterprise Log Manager サーバを更新

クローンの仮想 CA Enterprise Log Manager サーバの更新には、この手順を使用します。

クローンの仮想 CA Enterprise Log Manager サーバは、インストール時に与えられたホスト名を保持しています。ただし、アクティブな CA Enterprise Log Manager サーバそれぞれのホスト名は、ログ収集の実装環境内で一意である必要があります。そこで、クローンの仮想サーバを有効にする前に、*Rename_ELM.sh* スクリプトを使用してサーバのホスト名と IP アドレスを変更します。

更新スクリプトで実行されるアクションは以下のとおりです。

- デフォルト エージェントの自動停止と自動再起動
- iGateway サービス自動停止と自動再起動
- ホスト名、IP アドレスおよび DNS IP アドレスの変更を要求
- 暗号化されたパスワードで設定ファイルを自動更新し、各種の証明書に対応

クローンの仮想 CA Enterprise Log Manager サーバを更新する方法

1. 物理ターゲット サーバに root としてログインします。
2. アプリケーションの ISO イメージまたは DVD にアクセスし、ディレクトリ、/CA/Linux_x86 に移動します。

   インストールした CA Enterprise Log Manager サーバのファイル システムで、スクリプトを検索することもできます。スクリプトは、ディレクトリ、opt/CA/LogManager にあります。
3. ターゲット サーバに、スクリプト（Rename_ELM.sh）をコピーします。
4. 次のコマンドで、仮想 CA Enterprise Log Manager サーバの情報を変更します。

   ```
   ./Rename_ELM.sh
   ```
5. プロンプトに応答します。
6. 更新済みの仮想サーバを含んでいる仮想マシンを起動します。

仮想アプライアンスを使用した CA Enterprise Log Manager サーバの作成

CA Enterprise Log Manager は仮想アプライアンスとして OVF（Open Virtualization Format）で展開できます。仮想アプライアンスのプロビジョニングに必要な時間は、仮想マシンでの CA Enterprise Log Manager サーバのインストールまたはクローニングに必要な時間より少なくてすみます。

CA Enterprise Log Manager 仮想アプライアンスの概要

OVF は、仮想アプライアンスのパッケージ化および配布のためのオープン標準です。CA Enterprise Log Manager は、OVF を基にした仮想マシン ディスク（VMDK）ファイル形式を使用します。OVF パッケージには以下のファイルが含まれます。

OVF 記述子 XML ファイル

拡張子が「.ovf」である OVF 記述子 XML ファイル。このファイルには、仮想ハードウェア仕様、CA Enterprise Log Manager 設定パラメータ、および使用許諾契約が含まれます。

仮想ディスク ファイル

仮想アプライアンスの展開に使用されるディスク イメージ ファイルを含む、以下の VMware vSphere 仮想ディスク ファイル。

- CA Enterprise Log Manager 1.vmdk
- CA Enterprise Log Manager 2.vmdk
- CA Enterprise Log Manager 3.vmdk

マニフェスト ファイル

すべてのファイルのシグネチャが含まれる CA Enterprise Log Manager.mf ファイル。

注: 仮想ディスク ファイルまたはマニフェスト ファイルを変更しないでください。これらを変更すると、仮想アプライアンスのパフォーマンスに影響する可能性があります。

デフォルトでは、VMware vSphere Client は、OVF テンプレートを使用してインポートされた詳細を読み取り、仮想アプライアンスのプロビジョニングを行います。

仮想アプライアンスを使用する方法

次のシナリオで、仮想アプライアンスを使用して、イベント ログ収集環境用の仮想 CA Enterprise Log Manager サーバを作成できます。

- 既存の CA Enterprise Log Manager 環境に仮想サーバを追加: 混合環境を作成します。
- 仮想ログ収集環境の作成
- 迅速な拡張に向けた仮想 CA Enterprise Log Manager サーバの展開

VMware vSphere Client を使用して、仮想アプライアンスの手動またはサイレント インストールを実行します。OVF 記述子ファイルには、CA Enterprise Log Manager を設定するための設定パラメータが含まれます。インストール中に、各設定パラメータの値を入力します。

仮想アプライアンス インストール ワークシート

仮想アプライアンスをインストールする前に、以下の表にある情報を集めます。ワークシートを記入したら、インストール時のプロンプトに対してそのワークシートを使用できます。インストールする予定の CA Enterprise Log Manager サーバごとに、個別のワークシートを印刷して記入できます。

必要な情報	値	コメント
ホスト固有の設定		
ホスト名	*この CA Enterprise Log Manager サーバのホスト名* 例: CA-ELM1	ホストでサポートされている文字のみを使用して、このサーバのホスト名を指定します。業界基準では、A ～ Z(大文字と小文字を区別しない)、0 ～ 9、およびハイフンを使用し、最初の文字には英字、最後の文字には英数字を使用することを推奨しています。ホスト名内にアンダースコア文字を使用したり、このホストにドメイン名を追加したりしないでください。 **注**: ホスト名は 15 文字以内である必要があります。
ルート パスワード	*新しい root のパスワード*	このサーバ用の新しい root のパスワードを作成し、確認します。

必要な情報	値	コメント
IP アドレス	*関連する IPv4 アドレス*	このサーバ用の有効な IP アドレスを入力します。
サブネット マスク	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクを入力します。
デフォルト ゲートウェイ	*関連する IP アドレス*	このサーバで使用する有効なデフォルト ゲートウェイを入力します。
DNS サーバ	*関連する IPv4 アドレス*	ネットワークで使用している 1 つ以上の DNS サーバの IP アドレスを入力します。 このリストはカンマで区切り、エントリ間にスペースは挿入しません。 DNS サーバが IPv6 のアドレス割り当てを使用している場合は、その形式でアドレスを入力します。
ドメイン名	*ドメイン名*	mycompany.com など、このサーバが動作するドメイン名を入力します。 **注**: IP アドレスに対するホスト名を解決できるようにするために、ネットワーク内の Domain Name Server (DNS) サーバにドメイン名を登録する必要があります。
EULA	Accept	CA 使用許諾契約を読み、質問箇所までスクロール ダウンし、[Accept]をクリックして承諾します。
タイムゾーン	*希望するタイム ゾーン*	このサーバが存在する地域のタイム ゾーンを選択します。
アプリケーション固有の設定		

必要な情報	値	コメント
CA EEM サーバの場所	ローカル: 最初にインストールされたサーバ(管理サーバ)の場合 リモート: 追加サーバの場合	ローカルの CA EEM サーバを使用するのか、リモートの CA EEM サーバを使用するのかを示します。 管理用 CA Enterprise Log Manager サーバの場合は、ローカルを選択します。インストール中に、デフォルトの EiamAdmin ユーザ アカウントのパスワードを作成するように求めるプロンプトが表示されます。 個々の追加サーバについては、リモートを選択します。インストール中に、管理サーバ名を入力するように求めるプロンプトが表示されます。 ローカルを選択したかリモートを選択したかにかかわらず、最初は EiamAdmin アカウントの ID およびパスワードを使用して各 CA Enterprise Log Manager サーバにログオンする必要があります。
CA EEM サーバのホスト名または IP アドレス。	*IP アドレスまたはホスト名*	ローカル/リモート サーバ オプションでリモートを選択した場合のみ、この値を入力します。 最初にインストールした管理用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。 ホスト名を DNS サーバに登録する必要があります。 ローカル CA EEM サーバを使用する場合、デフォルト値は「**なし**」です。

必要な情報	値	コメント
CA EEM サーバのパスワード	*EiamAdmin アカウントのパスワード*	デフォルトの管理者アカウント EiamAdmin のパスワードを記録します。 CA Enterprise Log Manager サーバに初めてログインする場合には、このアカウント認証情報が必要です。 管理サーバをインストールしている場合は、ここで EiamAdmin の新しいパスワードを作成して確認します。 他の CA Enterprise Log Manager サーバやエージェントをインストールするときに使用するため、このパスワードを書き留めておきます。 **注**: ここで入力したパスワードは、ssh を使用して CA Enterprise Log Manager サーバに直接アクセスするために使用するデフォルトの caelmadmin アカウントの初期パスワードでもあります。 必要に応じて、インストール後に追加の管理者アカウントを作成して CA EEM の機能にアクセスできます。
FIPS	はい、またはいいえ	仮想アプライアンスを FIPS モードで実行するか非 FIPS モードで実行するかを指定します。ローカル CA EEM サーバを使用する場合、いずれのモードも選択できます。リモート CA EEM サーバを使用する場合、リモート CA EEM サーバが使用するモードを選択する必要があります。

使用している環境への仮想サーバの追加

すでに CA Enterprise Log Manager が実装されている場合は、ネットワークに仮想の CA Enterprise Log Manager 収集サーバを追加して、増加したイベント ボリュームを処理できます。このシナリオでは、すでに CA Enterprise Log Manager 管理サーバと 1 つ以上の収集およびレポート用 CA Enterprise Log Manager サーバがインストールされていることを前提とします。

注: 最高のパフォーマンスを得るには、仮想サーバに CA Enterprise Log Manager サーバをインストールして、収集タスクとレポート タスクのみを処理します。

環境に仮想収集サーバを追加するプロセスには、次の手順が含まれます。

1. CA Enterprise Log Manager 仮想アプライアンス パッケージをダウンロードします。
2. 仮想アプライアンスを使用して CA Enterprise Log Manager サーバをインストールします。
3. インストール セクションの説明に従って CA Enterprise Log Manager サーバを設定します。

仮想収集サーバをインストールしたら、クエリとレポートを実行できるようにそのサーバを連携に追加できます。

重要: 仮想装アプライアンスを使用して CA Enterprise Log Manager サーバをプロビジョンする場合、プライマリ CA Enterprise Log Manager サーバのアプリケーション インスタンス名は CAELM である必要があります。

仮想アプライアンス パッケージをダウンロードします。

CA Enterprise Log Manager 仮想アプライアンスの配布イメージは、Support Online のダウンロード用リンクから入手可能です。5 つのファイルをダウンロードする必要があります。

- マニフェスト ファイル
- .ovf ファイル
- 3 つの仮想ディスク ファイル

CA Enterprise Log Manager サーバの手動インストール

仮想アプライアンスを手動でインストールする場合は、以下タスクを実行します。

1. OVF テンプレートを展開します。
2. Paravirtualization と Resource を設定します。
3. プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れます。

OVF テンプレートの展開

OVF テンプレートで仮想アプライアンスのプロパティを指定できます。VMware は、このテンプレートを使用して CA Enterprise Log Manager サーバをセットアップします。VMware vSphere クライアントを使用して、OVF テンプレートを展開します。

注: 以下の手順で使用されているスクリーンショットには、参考のためのサンプル データが含まれます。これらのサンプル スクリーンショットは VMware vSphere Client 4.0.0 のものです。お使いの環境に合わせてデータを指定してください。

OVF テンプレート展開方法

1. VMware vSphere クライアントがインストールされているコンピュータで、[スタート]-[すべてのプログラム]-[VMware vSphere Client]を選択します。

   [VMware vSphere Client]ダイアログ ボックスが表示されます。

2. [IP address/Name]フィールドに、接続する VMware vCenter サーバの IP アドレスまたはホスト名を入力します。

3. [User Name]フィールドおよび[Password]フィールドにログイン認証情報を入力します。

4. [Logon]ボタンをクリックします。

   アプリケーション ウィンドウが開きます。

5. 左ペインの[Datacenter]の下で、CA Enterprise Log Manager サーバをセットアップする場所を選択します。

6. [File]-[Deploy OVF Template]をクリックします。

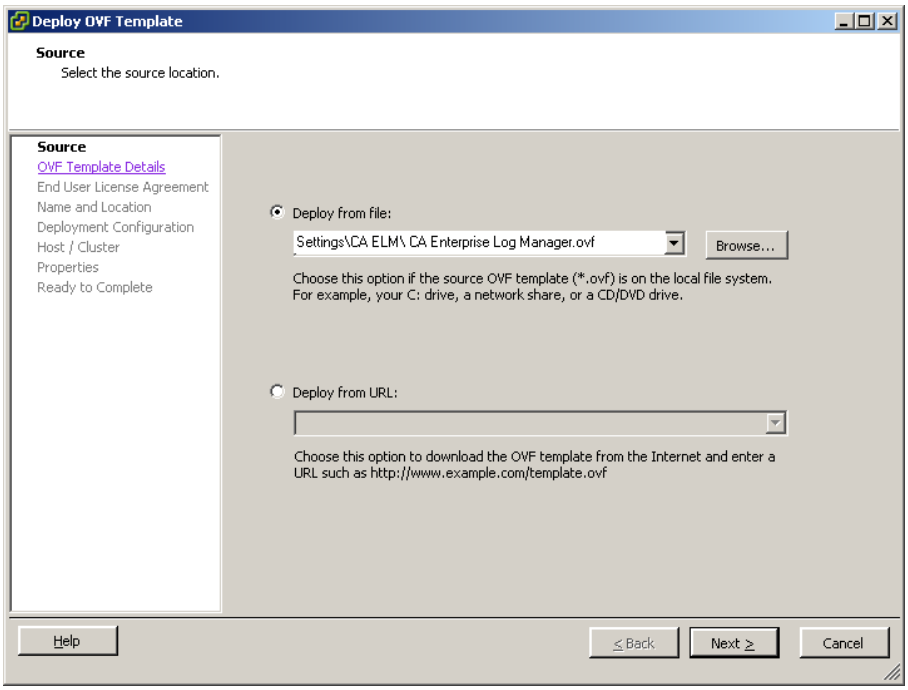
   [Deploy OVF Template]ウィンドウが表示されます。デフォルトでは、[Deploy OVF Template]ウィンドウにはソース ページが表示されます。このページで OVF テンプレートの場所を入力する必要があります。

   注: [Deploy OVF Template]ウィンドウで表示されるページは、使用している VMware vSphere クライアントのバージョンおよび設定によって異なります。OVF テンプレートを展開する詳細については、www.vmware.com を参照してください。

7. ファイル オプションから[Deploy]を選択し、[Browse]をクリックして、OVF テンプレートの場所を選択します。

8. [Open]ダイアログ ボックスで OVF テンプレートの場所へ移動し、OVF テンプレートを選択し、[Open]をクリックします。

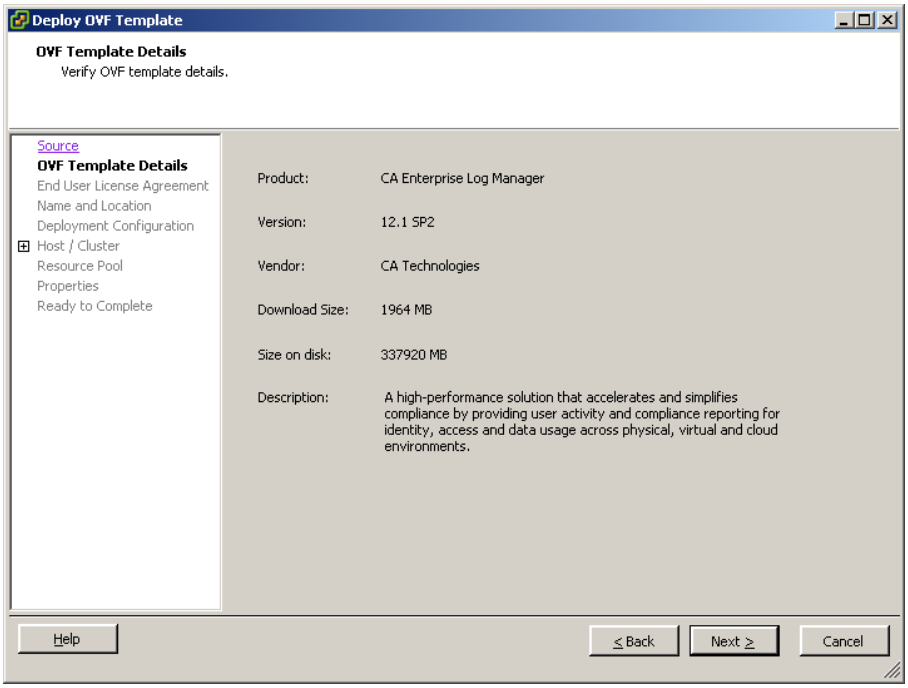
OVF テンプレートの場所のパスが[Deploy from file]フィールドに表示されます。



9. ［Next］をクリックします。

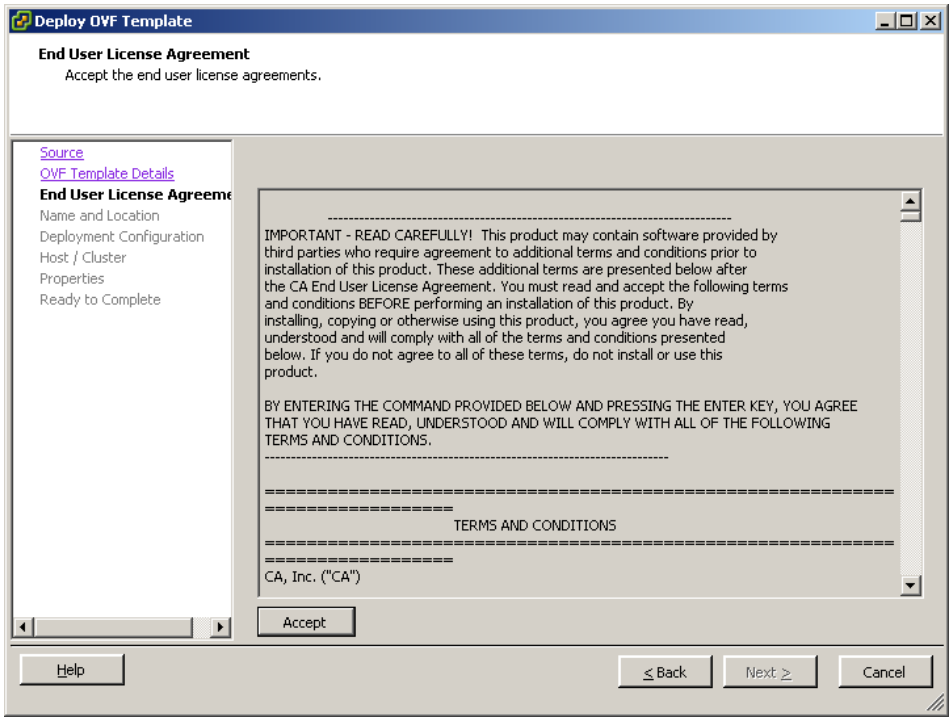
   ［OVF Template Details］が開きます。このページは、ダウンロード サイズ、利用可能なディスク サイズ、ベンダー名などの、OVF テンプレートに格納された詳細を表示します。

10. 350GB 以上の空きディスク容量が VMware サーバ上にあることを確認して、［Next］をクリックします。



[End User License Agreement]ページが表示されます。このページには、サードパーティ製品の使用許諾契約が表示されます。CA Enterprise Log Manager をインストールするには、この使用許諾契約を承諾する必要があります。

11. エンド ユーザ使用許諾契約の内容を読みます。

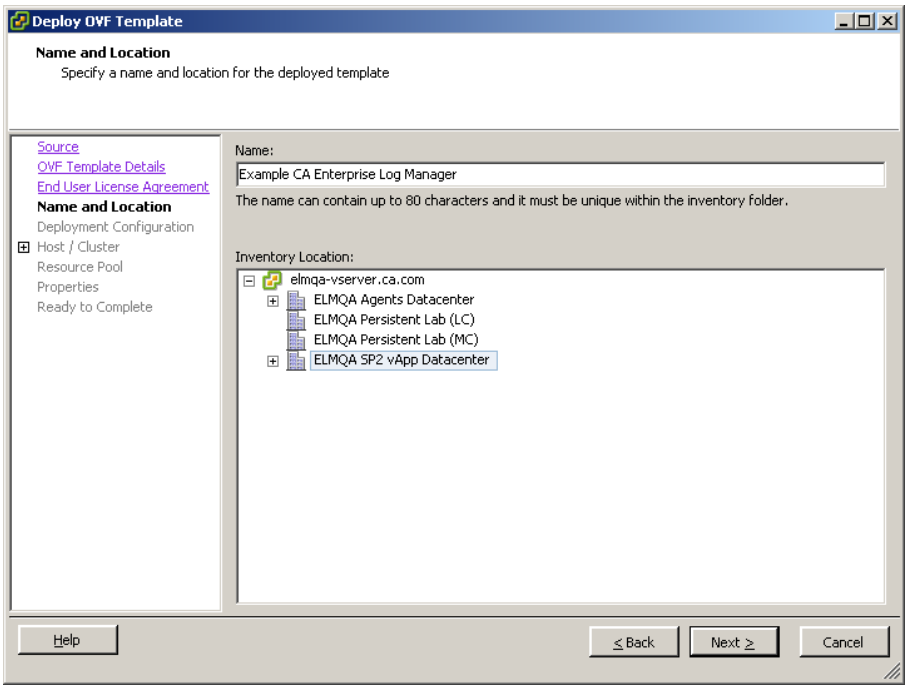


12. [Accept]をクリックして、[Next]をクリックします。

    [Name and Location]ページが開きます。このページでは、CA Enterprise Log Manager サーバを識別する名前を入力し、CA Enterprise Log Manager サーバのプロビジョニングをするデータセンターを指定します。

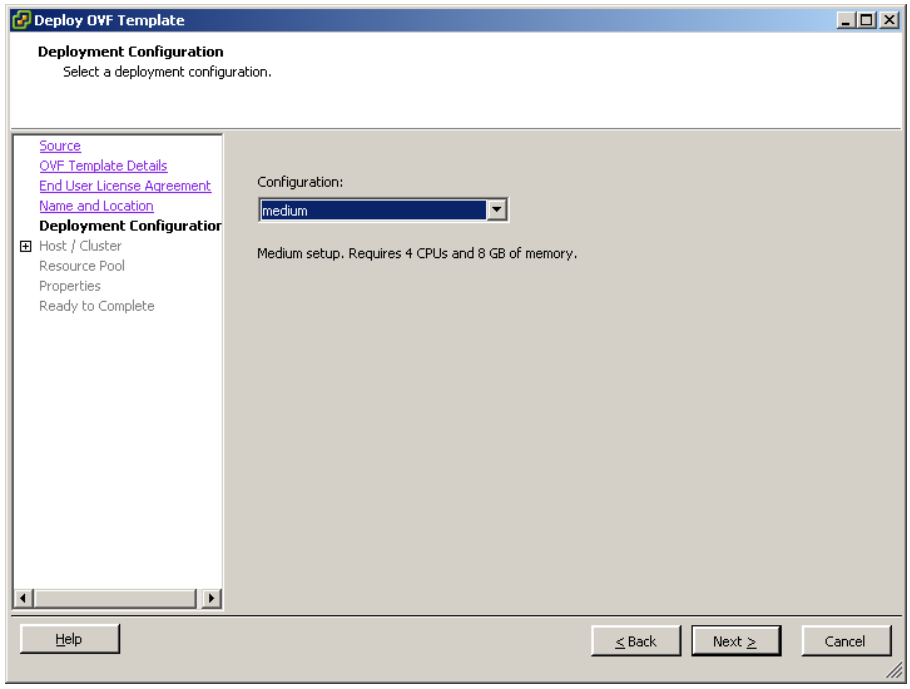
13. [Name]フィールドに CA Enterprise Log Manager サーバ名を入力し、[Inventory Location]でデータセンターを選択して、[Next]をクリックします。

    注: デフォルトでは、[Name]フィールドには、OVF テンプレートに指定された名前が表示されます。



［Deployment Configuration］ページが開きます。［Deployment Configuration］ページでは、プロビジョニングする CA Enterprise Log Manager サーバの設定モードを指定します。

14. ［Configuration］ドロップダウンから「Medium」または「Large」を選択し、［Next］をクリックします。

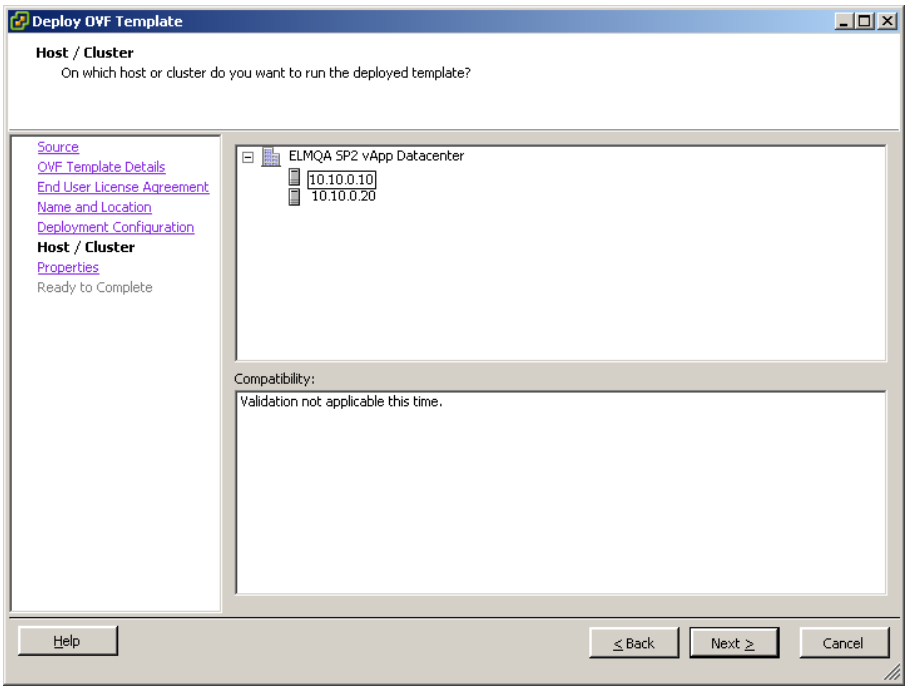


「Medium」を選択した場合、VMware は 4 つの CPU（各 CPU につき 8 GB の RAM）を提供します。「Large」を選択した場合、VMware は 8 つの CPU（各 CPU につき 8 GB の RAM）を提供します。

注: 収集サーバのプロビジョニングには Medium 展開設定を使用し、管理またはレポート サーバのプロビジョニングには Large 展開設定を使用することを強くお勧めします。

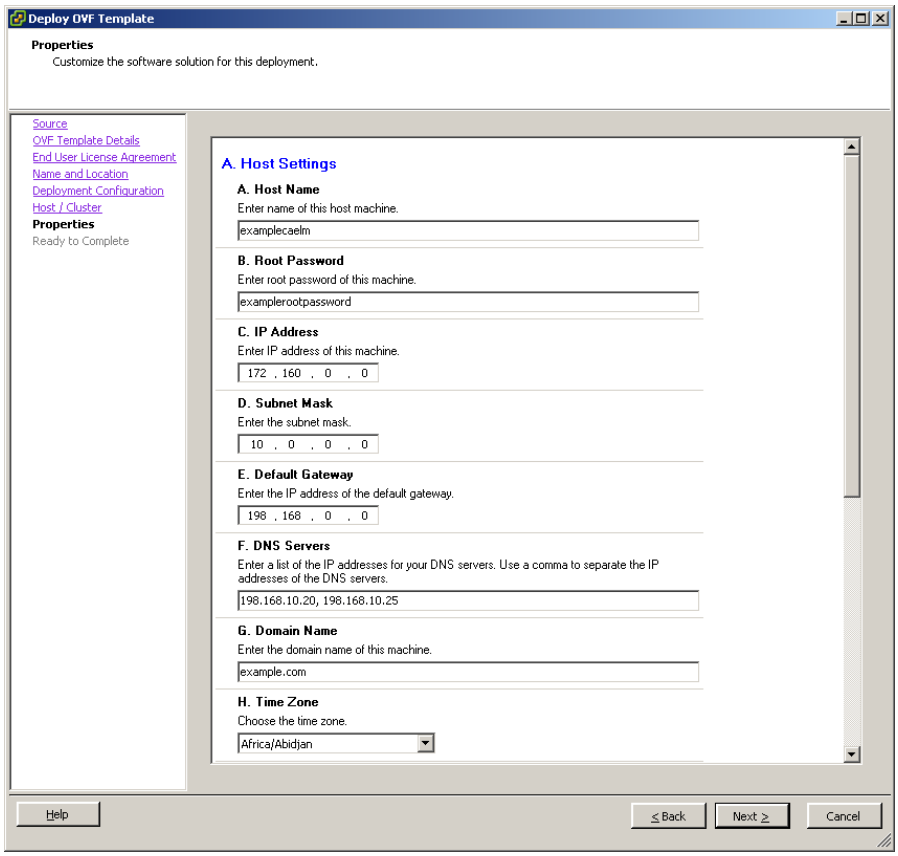
[Host/Cluster]ページが開きます。このページは、OVF テンプレートのインポート開始前にリソース プールを選択していない場合にのみ表示されます。[Host/Cluster]ページは、選択したデータセンターおよびその利用可能なクラスタを表示します。データセンター下で、CA Enterprise Log Manager サーバをプロビジョニングするクラスタの場所を指定する必要があります。

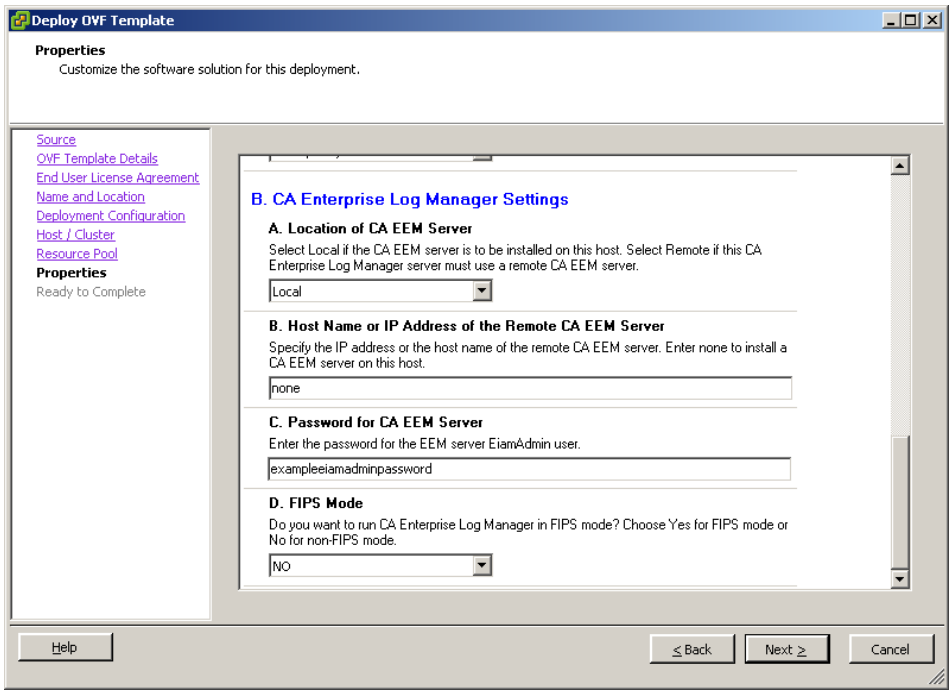
15. データセンター下でクラスタを選択し、[Next]をクリックします。



［Properties］ページが表示されます。このページにはホスト設定および CA Enterprise Log Manager 設定が含まれます。

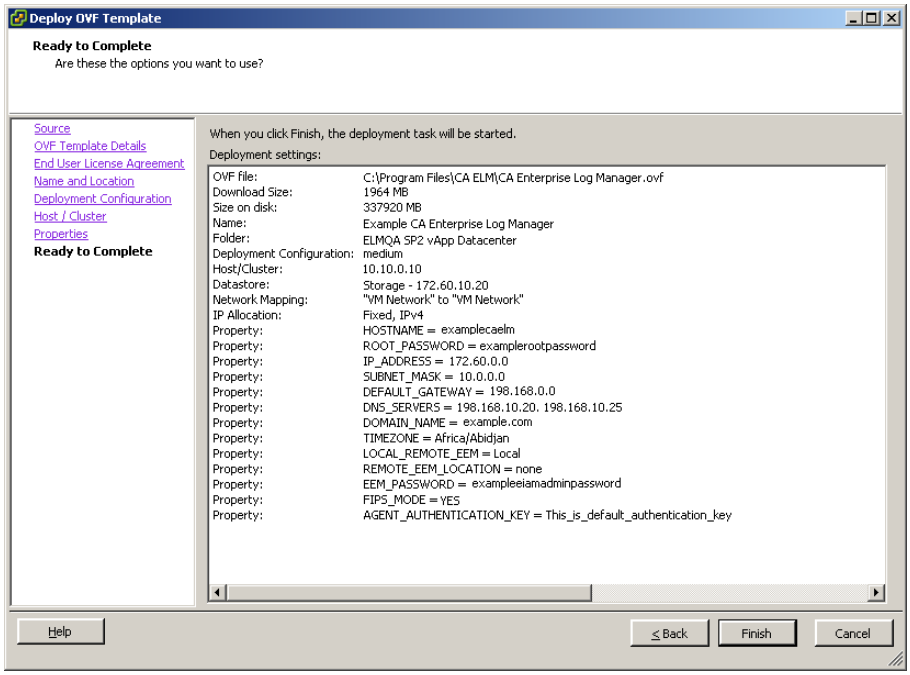
16. インストール ワークシートに集めた情報を使用して各フィールドの値を入力し、［Next］をクリックします。





[Ready to Complete]ページが開きます。このページには、今までのページで入力した詳細のサマリが表示されます。

17. 入力された詳細を確認し、[Finish]をクリックします。



メッセージ「Opening VI target」が表示されます。仮想アプライアンスの展開ステータスが表示されます。インストールが成功すると、左ペインの選択したデータ ストアの下に仮想アプライアンスがリスト表示されます。

18. （オプション）入力された詳細を変更する場合は、以下の手順に従います。

    a. 関連するページに移動するまで、[Deploy OVF Template]ウィンドウで繰り返し[Back]をクリックします。

    b. 必要な変更を行います。

    c. [Ready to Complete]ページに移動するまで、[Deploy OVF Template]ウィンドウで繰り返し[Next]をクリックします。

Paravirtualization と Resource の設定

OVF テンプレートをインポートした後、プロビジョニングされた CA Enterprise Log Manager サーバのパフォーマンスを改善するため、手動で Paravirtualization と Resource を設定する必要があります。

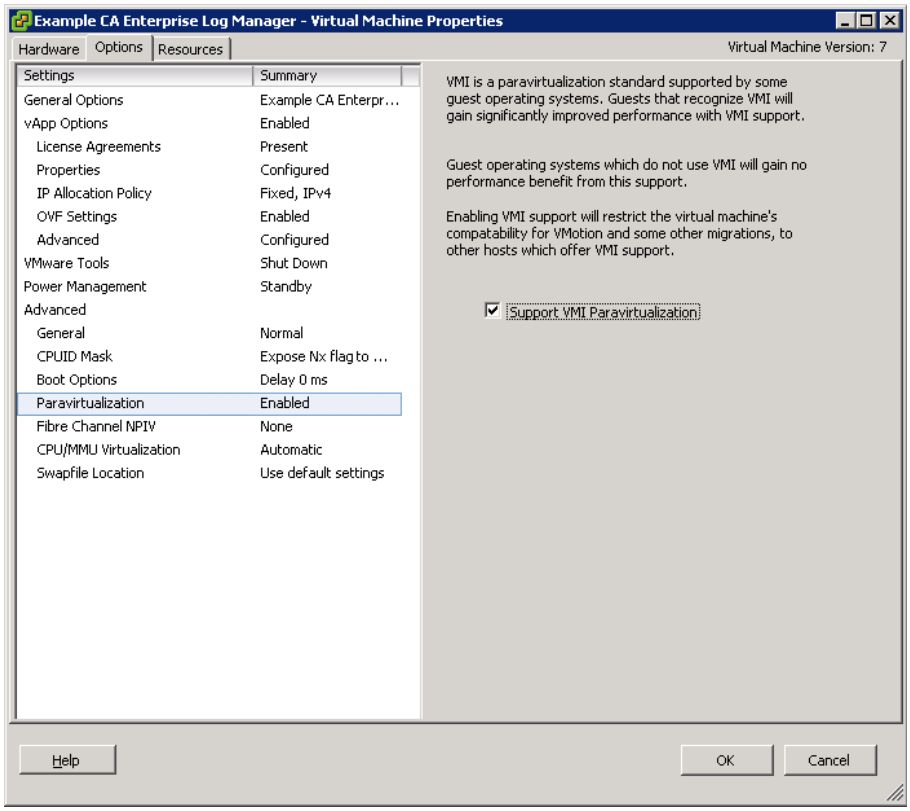
注: CD/DVD ドライブがクライアント デバイスに設定されていることを確認します。

Paravirtualization と Resource を設定する方法

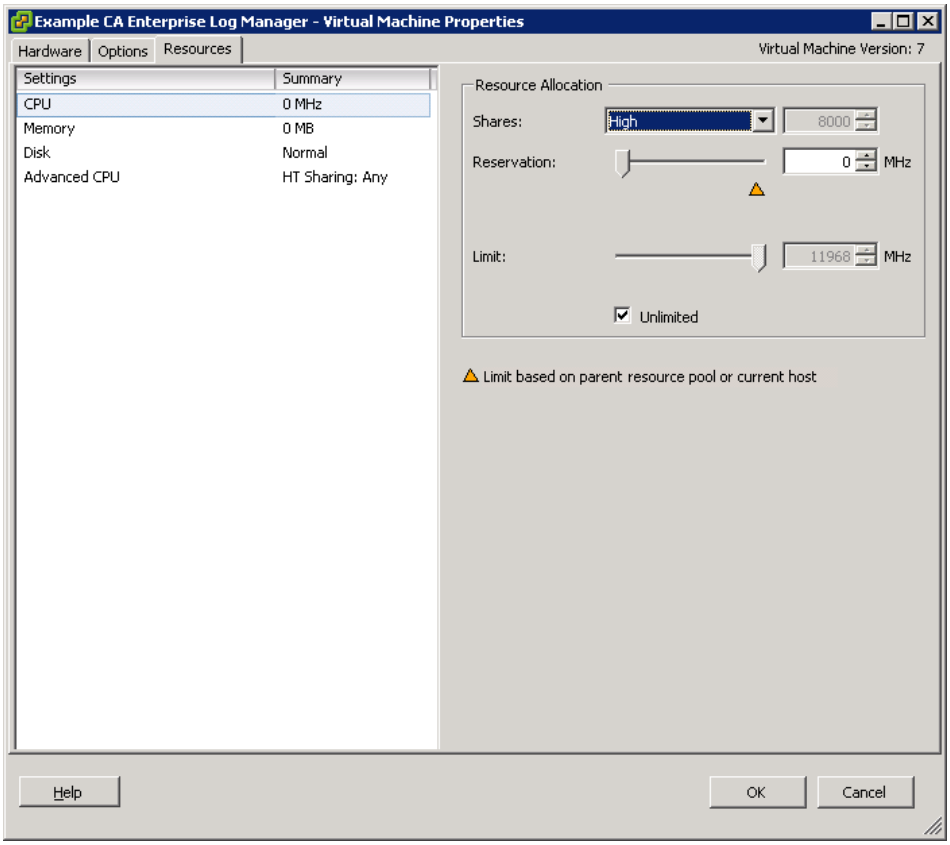
1. 左ペインの新しい[CA Enterprise Log Manager Virtual Appliance]を右クリックし、[Edit Settings]をクリックします。

   <*CA Enterprise Log Manager 仮想アプライアンス名* -> - [Virtual Machine Properties]ウィンドウが表示されます。

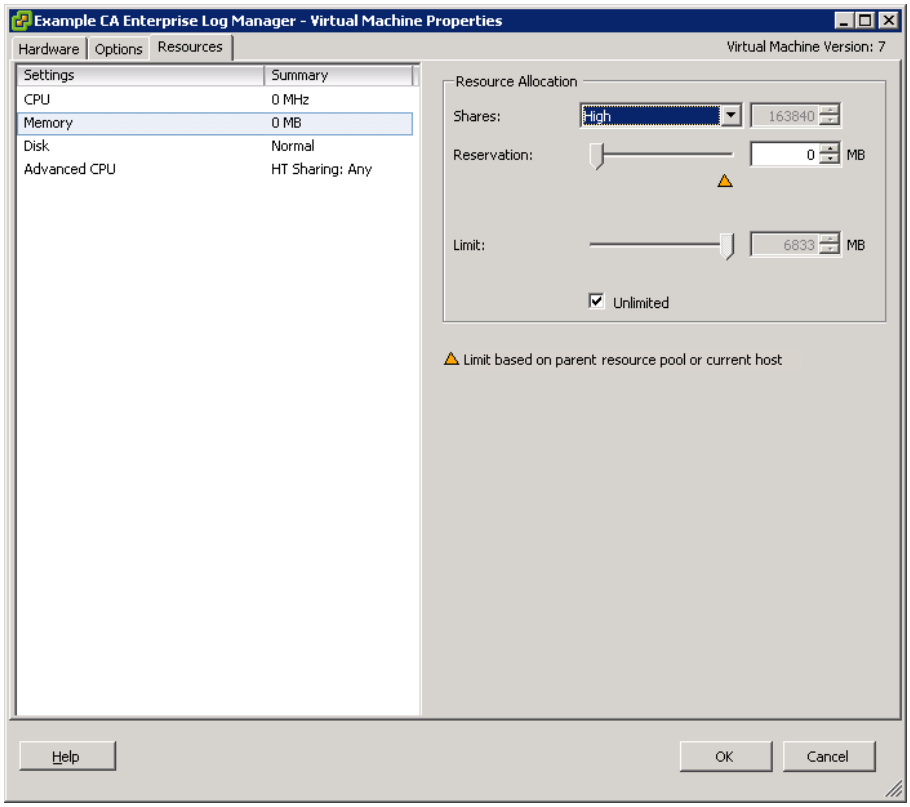
2. ウィンドウの[Option]タブをクリックします。
3. 左ペインで[Paravirtualization]設定を選択し、右ペインで[Support VMI Paravirtualization]オプションを選択します。



4. ウィンドウの[Resources]タブをクリックします。
5. [Settings]列から[CPU]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



6. [Settings]列から[Memory]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



7. [OK]をクリックします。

8. **注**: 準仮想化の詳細については、www.vmware.com を参照してください。

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れる

CA Enterprise Log Manager サーバを実行するため、電源を入れる必要があります。

CA Enterprise Log Manager サーバの電源を入れる方法

1. VMware アプリケーション ウィンドウの左ペインで新しい CA Enterprise Log Manager サーバを選択します。
2. 右ペインの[Getting Started]タブの[Basic Tasks]の下の[Power On]オプションをクリックします。

   CA Enterprise Log Manager サーバの電源が入ります。

注: セカンダリ CA Enterprise Log Manager サーバの電源を入れる前にプライマリ CA Enterprise Log Manager サーバが作動していることを確認してください。

CA Enterprise Log Manager サーバのサイレント インストール

仮想アプライアンスのサイレント インストールを実行するには、以下のタスクを実行する必要があります。

1. OVF ツールを起動します。
2. Paravirtualization と Resource を設定します。
3. プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れます。

以下の表では、OVF ツールを使用して CA Enterprise Log Manager を展開する際に使用するパラメータについて説明します。これらのパラメータは、コマンドラインでコマンド ライン引き数として指定する必要があります。

必要な情報	値	コメント
ホスト固有の設定		

必要な情報	値	コメント
HOSTNAME	*この CA Enterprise Log Manager サーバのホスト名* 例: CA-ELM1	ホストでサポートされている文字のみを使用して、このサーバのホスト名を指定します。業界基準では、A ～ Z(大文字と小文字を区別しない)、0 ～ 9、およびハイフンを使用し、最初の文字には英字、最後の文字には英数字を使用することを推奨しています。ホスト名内にアンダースコア文字を使用したり、このホストにドメイン名を追加したりしないでください。 **注**: ホスト名は 15 文字以内である必要があります。
ROOT_PASSWORD	*新しい root のパスワード*	このサーバ用の新しい root のパスワードを作成し、確認します。
IP_ADDRESS	*関連する IPv4 アドレス*	このサーバ用の有効な IP アドレスを入力します。
SUBNET_MASK	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクを入力します。
DEFAULT_GATEWAY	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクおよびデフォルト ゲートウェイを入力します。
DNS_SERVERS	*関連する IPv4 アドレス*	ネットワークで使用している 1 つ以上の DNS サーバの IP アドレスを入力します。 このリストはカンマで区切り、エントリ間にスペースは挿入しません。 DNS サーバが IPv6 のアドレス割り当てを使用している場合は、その形式でアドレスを入力します。
DOMAIN_NAME	*ドメイン名*	mycompany.com など、このサーバが動作するドメイン名を入力します。 **注**: IP アドレスに対するホスト名を解決できるようにするために、ネットワーク内の Domain Name Server (DNS)サーバにドメイン名を登録する必要があります。
acceptAllEulas	Accept	CA Enterprise Log Manager サーバのプロビジョニングを継続するには、CA 使用許諾契約を承諾します。

必要な情報	値	コメント
deploymentOption	「Medium」または「Large」	「Medium」を選択した場合、VMware は 4 つの CPU（各 CPU につき 8 GB の RAM）を提供します。「Large」を選択した場合、VMware は 8 つの CPU（各 CPU につき 8 GB の RAM）を提供します。
TIMEZONE	*希望するタイム ゾーン*	このサーバが存在する地域のタイム ゾーンを選択します。
アプリケーション固有の設定		
LOCAL_REMOTE_EEM	ローカル: 最初にインストールされたサーバ(管理サーバ)の場合 リモート: 追加サーバの場合	ローカルの CA EEM サーバを使用するのか、リモートの CA EEM サーバを使用するのかを示します。 管理用 CA Enterprise Log Manager サーバの場合は、ローカルを選択します。インストール中に、デフォルトの EiamAdmin ユーザ アカウントのパスワードを作成するように求めるプロンプトが表示されます。 個々の追加サーバについては、リモートを選択します。インストール中に、管理サーバ名を入力するように求めるプロンプトが表示されます。 ローカルを選択したかリモートを選択したかにかかわらず、最初は EiamAdmin アカウントの ID およびパスワードを使用して各 CA Enterprise Log Manager サーバにログオンする必要があります。
REMOTE_EEM_LOCATION	*IP アドレスまたはホスト名*	ローカル/リモート サーバ オプションでリモートを選択した場合のみ、この値を入力します。 最初にインストールした管理用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。 ホスト名を DNS サーバに登録する必要があります。 ローカル CA EEM サーバを使用する場合、デフォルト値は「**なし**」です。

必要な情報	値	コメント
EEM_PASSWORD	*EiamAdmin アカウントのパスワード*	デフォルトの管理者アカウント EiamAdmin のパスワードを記録します。 CA Enterprise Log Manager サーバに初めてログインする場合には、このアカウント認証情報が必要です。 管理サーバをインストールしている場合は、ここで EiamAdmin の新しいパスワードを作成して確認します。 他の CA Enterprise Log Manager サーバやエージェントをインストールするときに使用するため、このパスワードを書き留めておきます。 **注**: ここで入力したパスワードは、ssh を使用して CA Enterprise Log Manager サーバに直接アクセスするために使用するデフォルトの caelmadmin アカウントの初期パスワードでもあります。 必要に応じて、インストール後に追加の管理者アカウントを作成して CA EEM の機能にアクセスできます。
FIPS_MODE	はい、またはいいえ	仮想アプライアンスを FIPS モードで実行するか非 FIPS モードで実行するかを指定します。ローカル CA EEM サーバを使用する場合、いずれのモードも選択できます。リモート CA EEM サーバを使用する場合、リモート CA EEM サーバが使用するモードを選択する必要があります。

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

コマンド ラインからの OVF ツールの呼び出し

注: サイレント インストールを実行する前に、OVF Tool 1.0.0.0 をインストールする必要があります。OVF ツールの詳細については、VMware の「*OVF Tool User Guide*」または www.vmware.com を参照してください。

OVF ツールを呼び出すには、設定パラメータをコマンド ライン引き数として渡す必要があります。

注: 収集サーバのプロビジョニングには Medium 展開設定を使用し、レポート サーバのプロビジョニングには Large 展開設定を使用することを強くお勧めします。また、VMware のドキュメントで説明されているとおり、シック展開手法を使用することをお勧めします。

コマンド ラインからの OVF ツールの呼び出し方法

1. VMware vSphere クライアントがインストールされているコンピュータのコマンド プロンプトを開きます。
2. 以下のコマンドを実行して、OVF ツールを呼び出します。

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value
--prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value
--prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value
--prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value
--prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value
--prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host
name
```

メッセージ「Opening VI target」が表示されます。CA Enterprise Log Manager サーバの展開ステータスが表示されます。インストールが成功すると、左ペインの選択したデータ ストアの下に CA Enterprise Log Manager サーバがリスト表示されます。

注: プロパティ値にスペースが含まれる場合は、ダブルクォート("") でプロパティ値を囲みます。たとえば、OVF 名が CA ELM である場合は、値を "CA ELM.ovf" として入力します。OVF ツールの詳細については、「*OVF Tool User Guide*」を参照してください。

例

```
ovftool -dm=thick --acceptAllEulas --name="example_server"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA
ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Paravirtualization と Resource の設定

OVF テンプレートをインポートした後、プロビジョニングされた CA Enterprise Log Manager サーバのパフォーマンスを改善するため、手動で Paravirtualization と Resource を設定する必要があります。

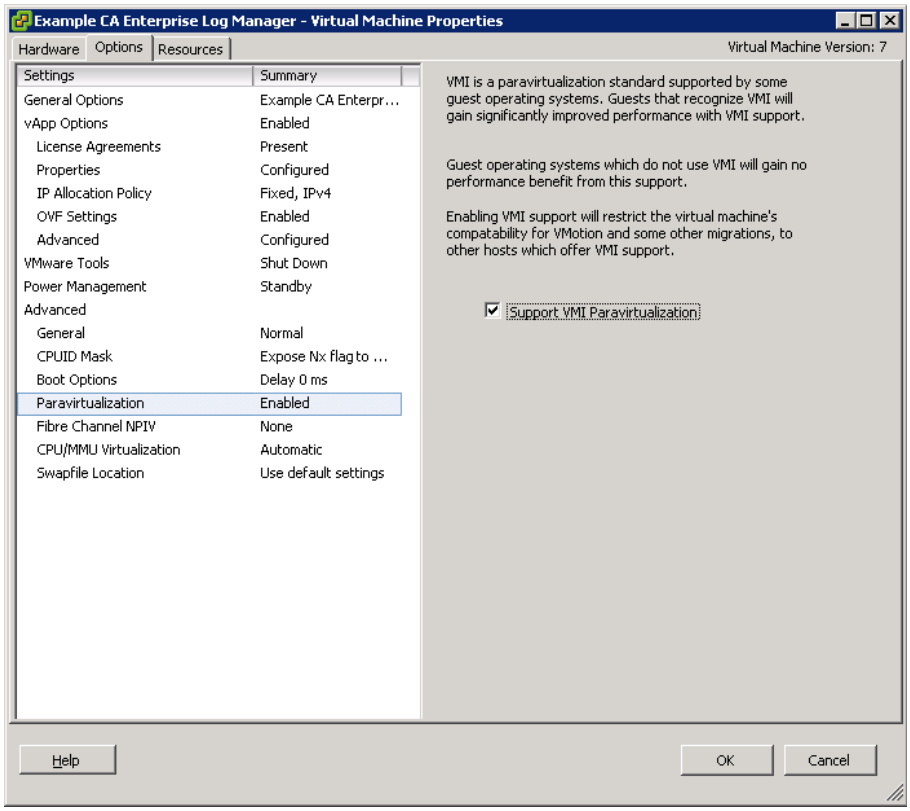
注: CD/DVD ドライブがクライアント デバイスに設定されていることを確認します。

Paravirtualization と Resource を設定する方法

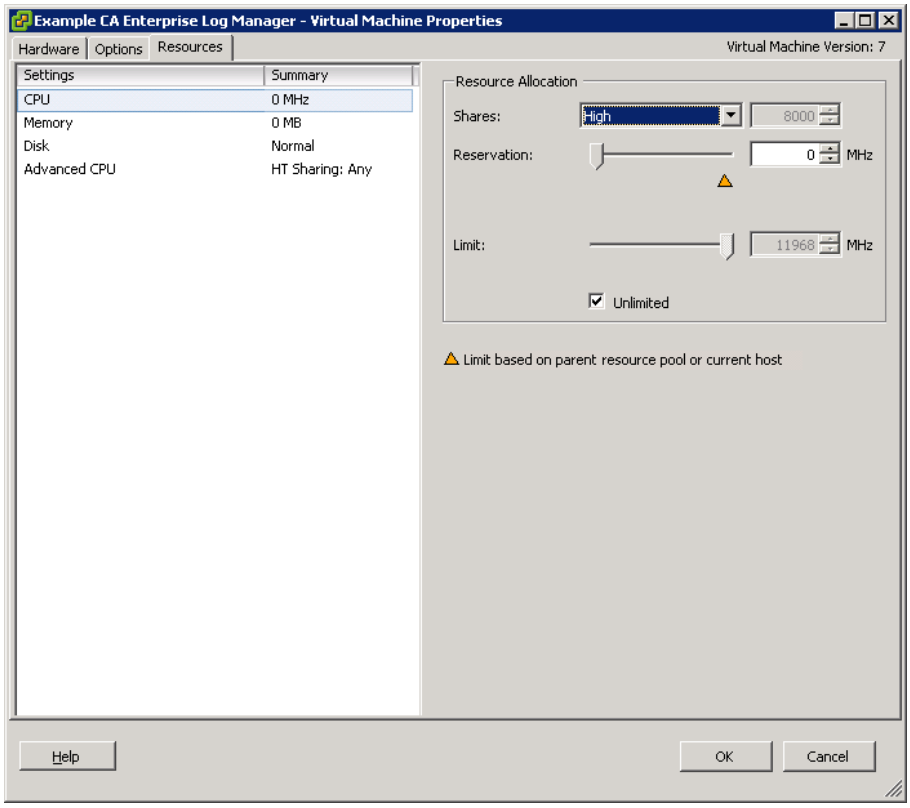
1. 左ペインの新しい[CA Enterprise Log Manager Virtual Appliance]を右クリックし、[Edit Settings]をクリックします。

   <*CA Enterprise Log Manager 仮想アプライアンス名* -> - [Virtual Machine Properties]ウィンドウが表示されます。

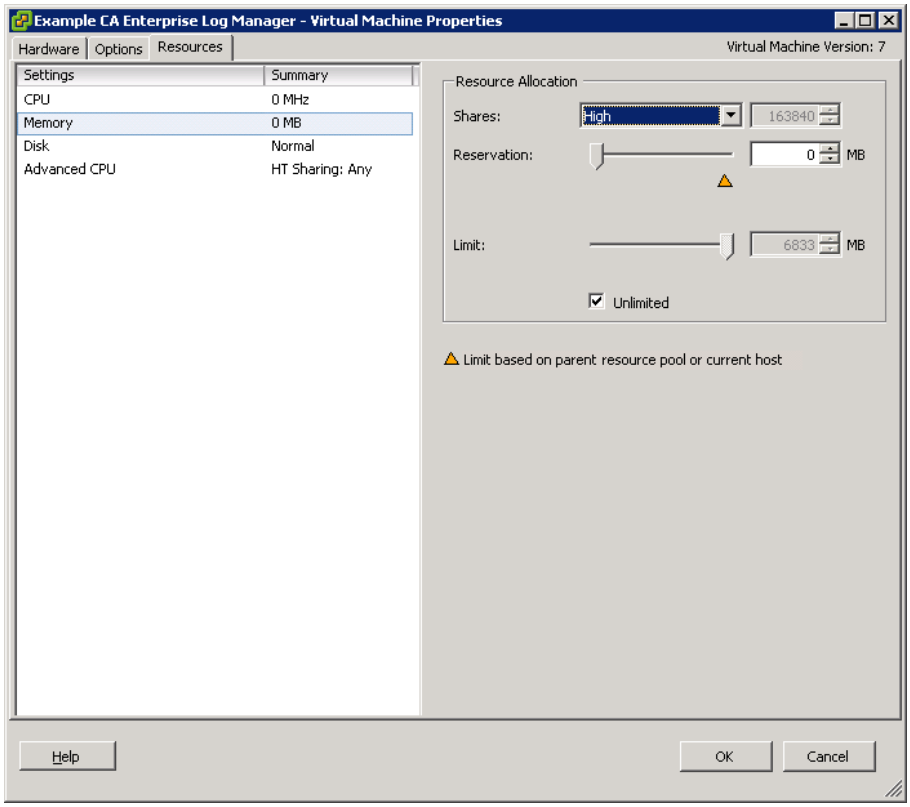
2. ウィンドウの[Option]タブをクリックします。
3. 左ペインで[Paravirtualization]設定を選択し、右ペインで[Support VMI Paravirtualization]オプションを選択します。



4. ウィンドウの[Resources]タブをクリックします。
5. [Settings]列から[CPU]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



6. [Settings]列から[Memory]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



7. [OK]をクリックします。
8. **注**: 準仮想化の詳細については、www.vmware.com を参照してください。

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れる

CA Enterprise Log Manager サーバを実行するため、電源を入れる必要があります。

CA Enterprise Log Manager サーバの電源を入れる方法

1. VMware アプリケーション ウィンドウの左ペインで新しい CA Enterprise Log Manager サーバを選択します。
2. 右ペインの[Getting Started]タブの[Basic Tasks]の下の[Power On]オプションをクリックします。

   CA Enterprise Log Manager サーバの電源が入ります。

注: セカンダリ CA Enterprise Log Manager サーバの電源を入れる前にプライマリ CA Enterprise Log Manager サーバが作動していることを確認してください。

仮想 CA Enterprise Log Manager サーバのインストールの確認

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れると、CA Enterprise Log Manager にアクセスする URL が[VMware vSphere Client]ウィンドウの[Console]タブに表示されます。CA Enterprise Log Manager にアクセスするには、この URL および以下のデフォルト ログイン認証情報を使用します。

デフォルト ユーザ名 : EiamAdmin

デフォルト パスワード : CA Enterprise Log Manager サーバのインストール中に入力したパスワード

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

完全な仮想環境の作成

まだ CA Enterprise Log Manager 環境を実装していない場合は、すべてを仮想化したログ収集環境を作成できます。このシナリオでは、目的の各 CA Enterprise Log Manager サーバをインストールするために、十分な数の物理サーバが使用可能で、その各サーバに少なくとも 4 つのプロセッサ グループがあることを前提としています。

管理サーバとして動作する CA Enterprise Log Manager サーバを 1 台インストールします。 設定中にこのサーバにイベント ログを送信しないでください。または、このサーバを使用してレポートを生成しないでください。この方法で環境を設定すると、エンタープライズ レベルの本稼働環境に必要なイベント ログ収集のスループットを維持できます。

一般的には、認定されたハードウェアを使用する場合に通常インストールする各装置クラス サーバの代わりに、4 つのプロセッサを 2 つ持つ CA Enterprise Log Manager サーバをインストールします (アプライアンスクラスのサーバには、最低 8 つのプロセッサがあります)。

仮想アプライアンスを使用して仮想環境を作成するプロセスには、以下の手順が含まれます。

1. 仮想アプライアンス パッケージをダウンロードします。
2. 管理機能用に CA Enterprise Log Manager 仮想サーバをインストールします。
3. 収集およびレポート用に、2 つ以上の仮想アプライアンス サーバをインストールします。
4. CA Enterprise Log Manager サーバのインストールに関するセクションの説明に従って、仮想アプライアンス サーバを設定します。

重要: 仮想装アプライアンスを使用して CA Enterprise Log Manager サーバをプロビジョンする場合、プライマリ CA Enterprise Log Manager サーバのアプリケーション インスタンス名は CAELM である必要があります。

仮想アプライアンス パッケージをダウンロードします。

CA Enterprise Log Manager 仮想アプライアンスの配布イメージは、Support Online のダウンロード用リンクから入手可能です。5 つのファイルをダウンロードする必要があります。

- マニフェスト ファイル
- .ovf ファイル
- 3 つの仮想ディスク ファイル

CA Enterprise Log Manager サーバの手動インストール

仮想アプライアンスを手動でインストールする場合は、以下タスクを実行します。

1. OVF テンプレートを展開します。
2. Paravirtualization と Resource を設定します。
3. プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れます。

OVF テンプレートの展開

OVF テンプレートで仮想アプライアンスのプロパティを指定できます。VMware は、このテンプレートを使用して CA Enterprise Log Manager サーバをセットアップします。VMware vSphere クライアントを使用して、OVF テンプレートを展開します。

注: 以下の手順で使用されているスクリーンショットには、参考のためのサンプル データが含まれます。これらのサンプル スクリーンショットは VMware vSphere Client 4.0.0 のものです。お使いの環境に合わせてデータを指定してください。

OVF テンプレート展開方法

1. VMware vSphere クライアントがインストールされているコンピュータで、[スタート]-[すべてのプログラム]-[VMware vSphere Client]を選択します。

   [VMware vSphere Client]ダイアログ ボックスが表示されます。

2. [IP address/Name]フィールドに、接続する VMware vCenter サーバの IP アドレスまたはホスト名を入力します。

3. [User Name]フィールドおよび[Password]フィールドにログイン認証情報を入力します。

4. [Logon]ボタンをクリックします。

   アプリケーション ウィンドウが開きます。

5. 左ペインの[Datacenter]の下で、CA Enterprise Log Manager サーバをセットアップする場所を選択します。

6. [File]-[Deploy OVF Template]をクリックします。

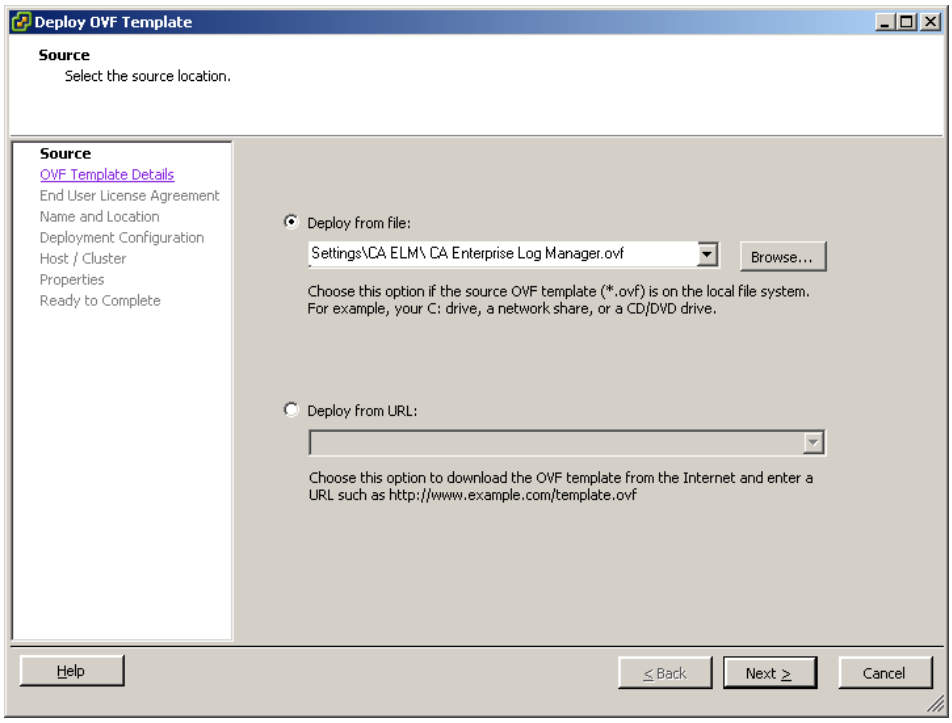
   [Deploy OVF Template]ウィンドウが表示されます。デフォルトでは、[Deploy OVF Template]ウィンドウにはソース ページが表示されます。このページで OVF テンプレートの場所を入力する必要があります。

   注: [Deploy OVF Template]ウィンドウで表示されるページは、使用している VMware vSphere クライアントのバージョンおよび設定によって異なります。OVF テンプレートを展開する詳細については、www.vmware.com を参照してください。

7. ファイル オプションから[Deploy]を選択し、[Browse]をクリックして、OVF テンプレートの場所を選択します。

8. [Open]ダイアログ ボックスで OVF テンプレートの場所へ移動し、OVF テンプレートを選択し、[Open]をクリックします。

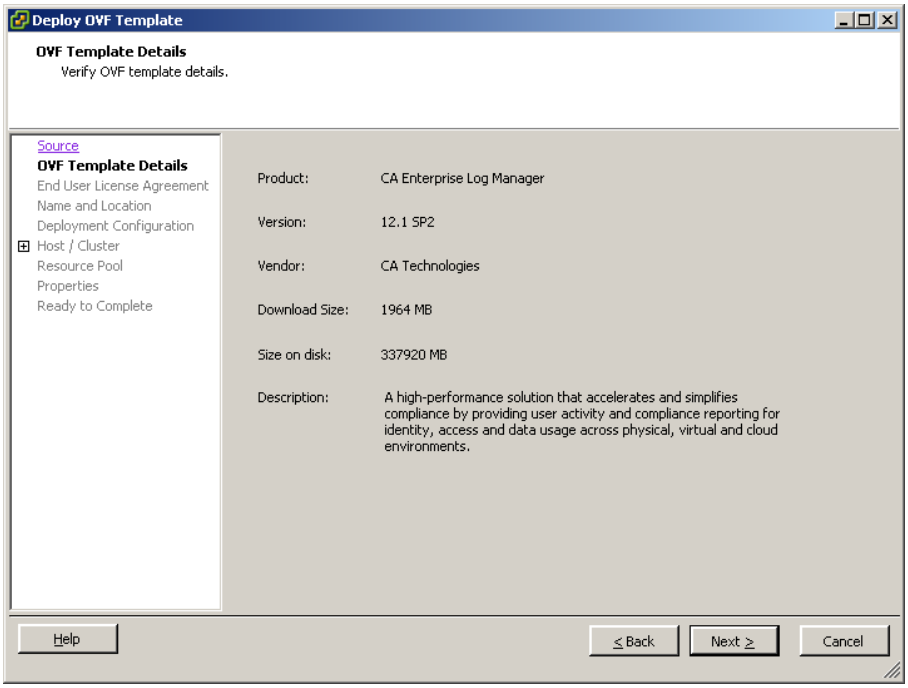
OVF テンプレートの場所のパスが[Deploy from file]フィールドに表示されます。



9. ［Next］をクリックします。

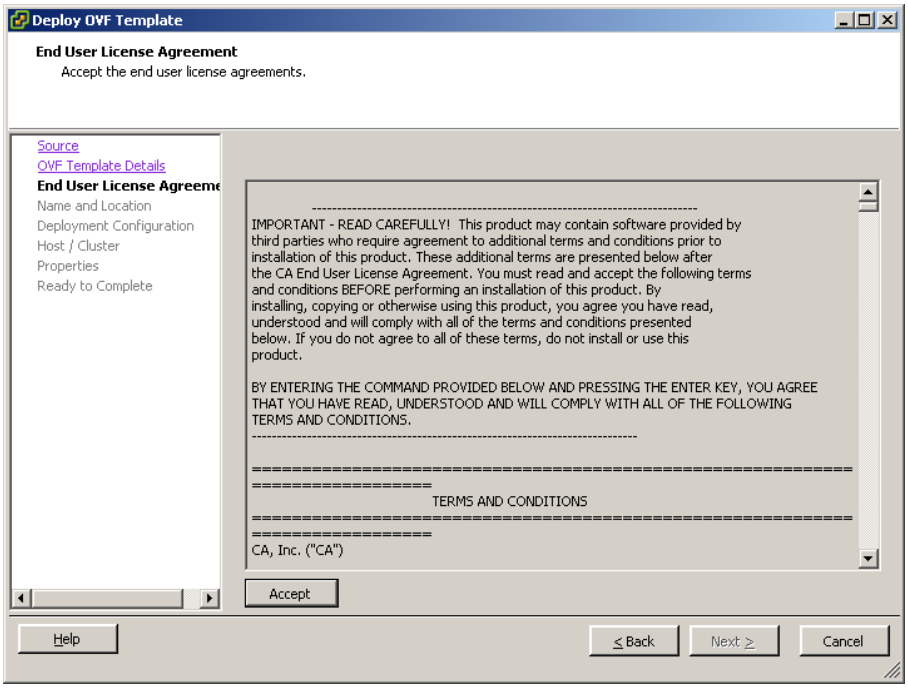
   ［OVF Template Details］が開きます。このページは、ダウンロード サイズ、利用可能なディスク サイズ、ベンダー名などの、OVF テンプレートに格納された詳細を表示します。

10. 350GB 以上の空きディスク容量が VMware サーバ上にあることを確認して、［Next］をクリックします。



[End User License Agreement]ページが表示されます。このページには、サードパーティ製品の使用許諾契約が表示されます。CA Enterprise Log Manager をインストールするには、この使用許諾契約を承諾する必要があります。

11. エンド ユーザ使用許諾契約の内容を読みます。

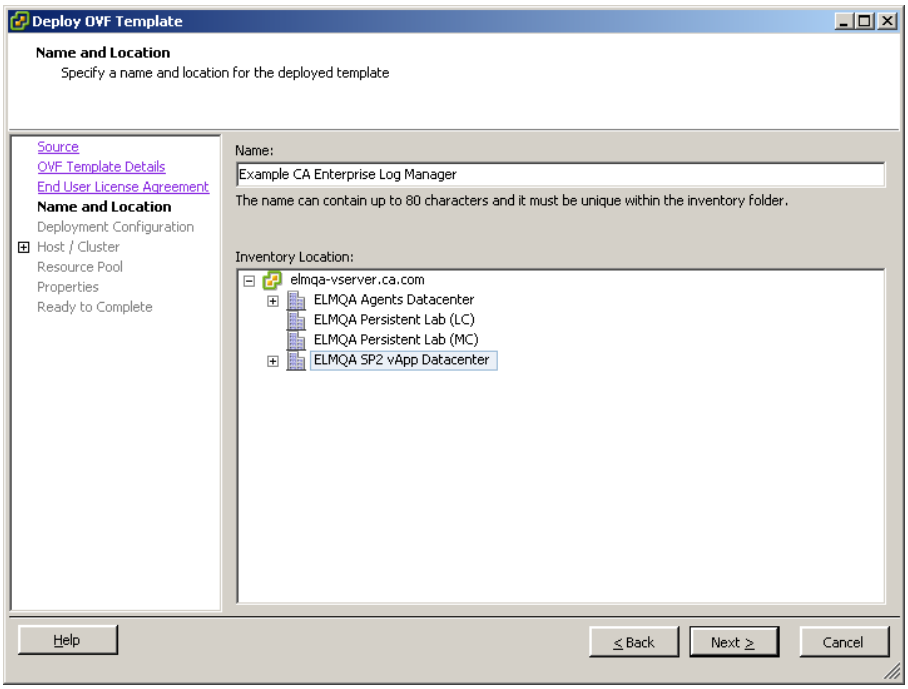


12. [Accept]をクリックして、[Next]をクリックします。

    [Name and Location]ページが開きます。このページでは、CA Enterprise Log Manager サーバを識別する名前を入力し、CA Enterprise Log Manager サーバのプロビジョニングをするデータセンターを指定します。

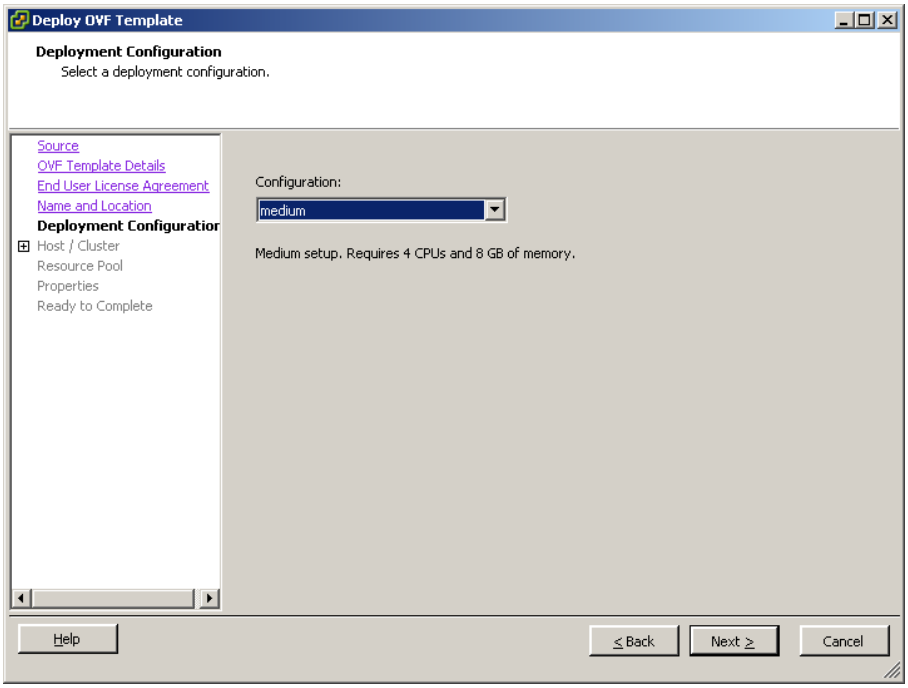
13. [Name]フィールドに CA Enterprise Log Manager サーバ名を入力し、[Inventory Location]でデータセンターを選択して、[Next]をクリックします。

    注: デフォルトでは、[Name]フィールドには、OVF テンプレートに指定された名前が表示されます。



［Deployment Configuration］ページが開きます。［Deployment Configuration］ページでは、プロビジョニングする CA Enterprise Log Manager サーバの設定モードを指定します。

14. ［Configuration］ドロップダウンから「Medium」または「Large」を選択し、［Next］をクリックします。

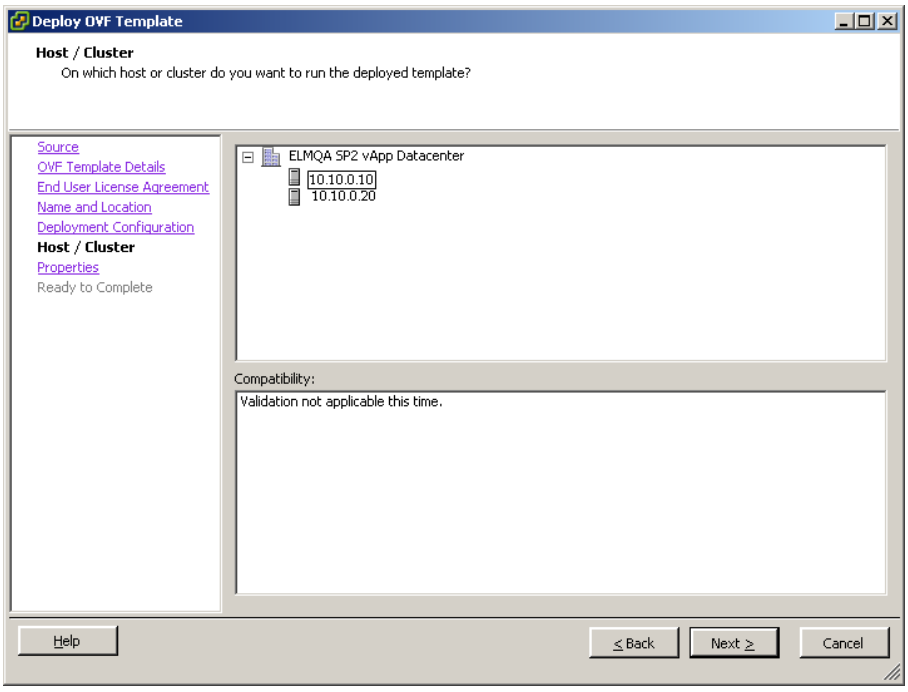


「Medium」を選択した場合、VMware は 4 つの CPU（各 CPU につき 8 GB の RAM）を提供します。「Large」を選択した場合、VMware は 8 つの CPU（各 CPU につき 8 GB の RAM）を提供します。

注: 収集サーバのプロビジョニングには Medium 展開設定を使用し、管理またはレポート サーバのプロビジョニングには Large 展開設定を使用することを強くお勧めします。

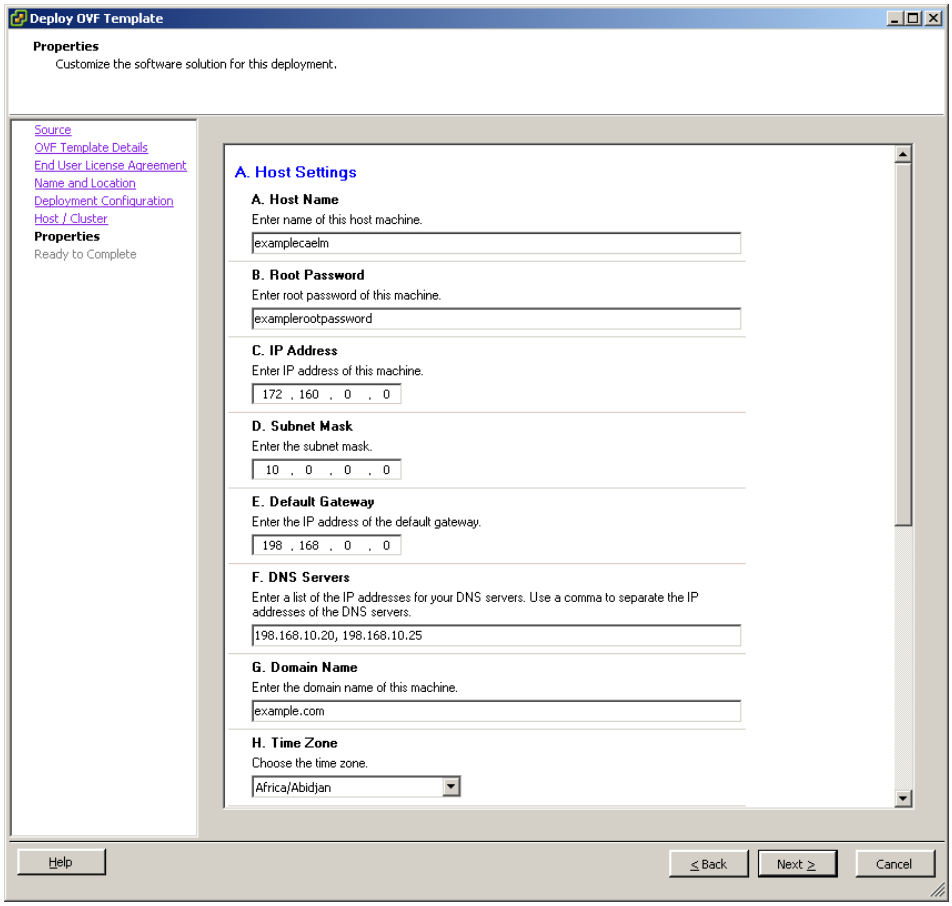
[Host/Cluster]ページが開きます。このページは、OVF テンプレートのインポート開始前にリソース プールを選択していない場合にのみ表示されます。[Host/Cluster]ページは、選択したデータセンターおよびその利用可能なクラスタを表示します。データセンター下で、CA Enterprise Log Manager サーバをプロビジョニングするクラスタの場所を指定する必要があります。

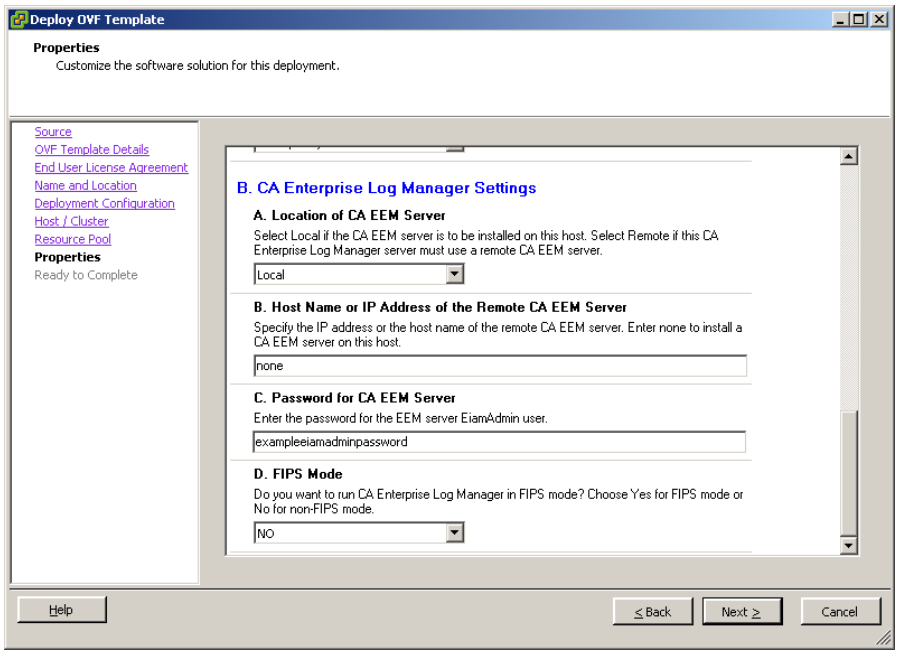
15. データセンター下でクラスタを選択し、[Next]をクリックします。



［Properties］ページが表示されます。このページにはホスト設定および CA Enterprise Log Manager 設定が含まれます。

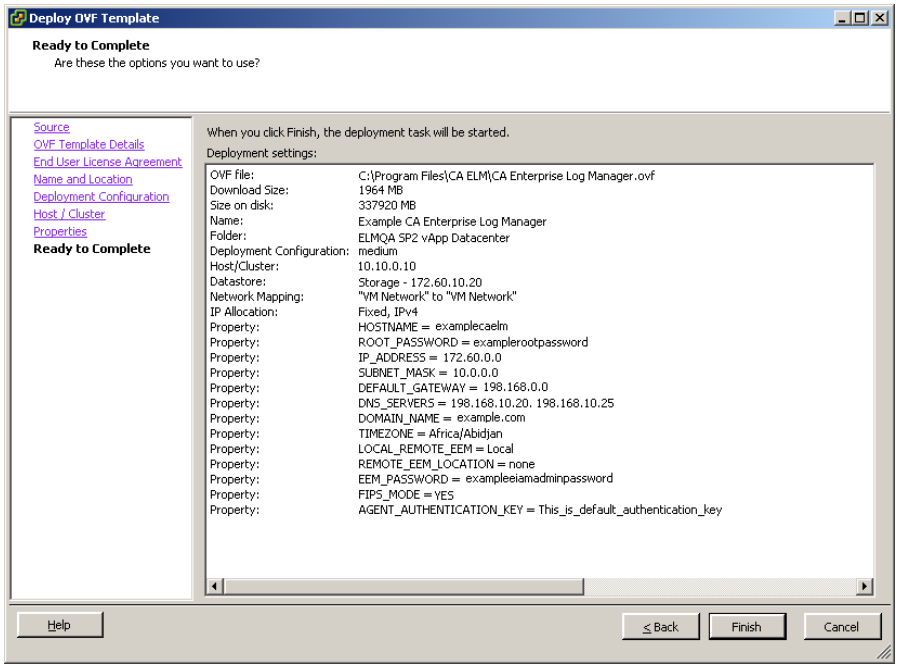
16. インストール ワークシートに集めた情報を使用して各フィールドの値を入力し、［Next］をクリックします。





[Ready to Complete]ページが開きます。このページには、今までのページで入力した詳細のサマリが表示されます。

17. 入力された詳細を確認し、[Finish]をクリックします。



メッセージ「Opening VI target」が表示されます。仮想アプライアンスの展開ステータスが表示されます。インストールが成功すると、左ペインの選択したデータ ストアの下に仮想アプライアンスがリスト表示されます。

18. （オプション）入力された詳細を変更する場合は、以下の手順に従います。

    a. 関連するページに移動するまで、[Deploy OVF Template]ウィンドウで繰り返し[Back]をクリックします。

    b. 必要な変更を行います。

    c. [Ready to Complete]ページに移動するまで、[Deploy OVF Template]ウィンドウで繰り返し[Next]をクリックします。

Paravirtualization と Resource の設定

OVF テンプレートをインポートした後、プロビジョニングされた CA Enterprise Log Manager サーバのパフォーマンスを改善するため、手動で Paravirtualization と Resource を設定する必要があります。

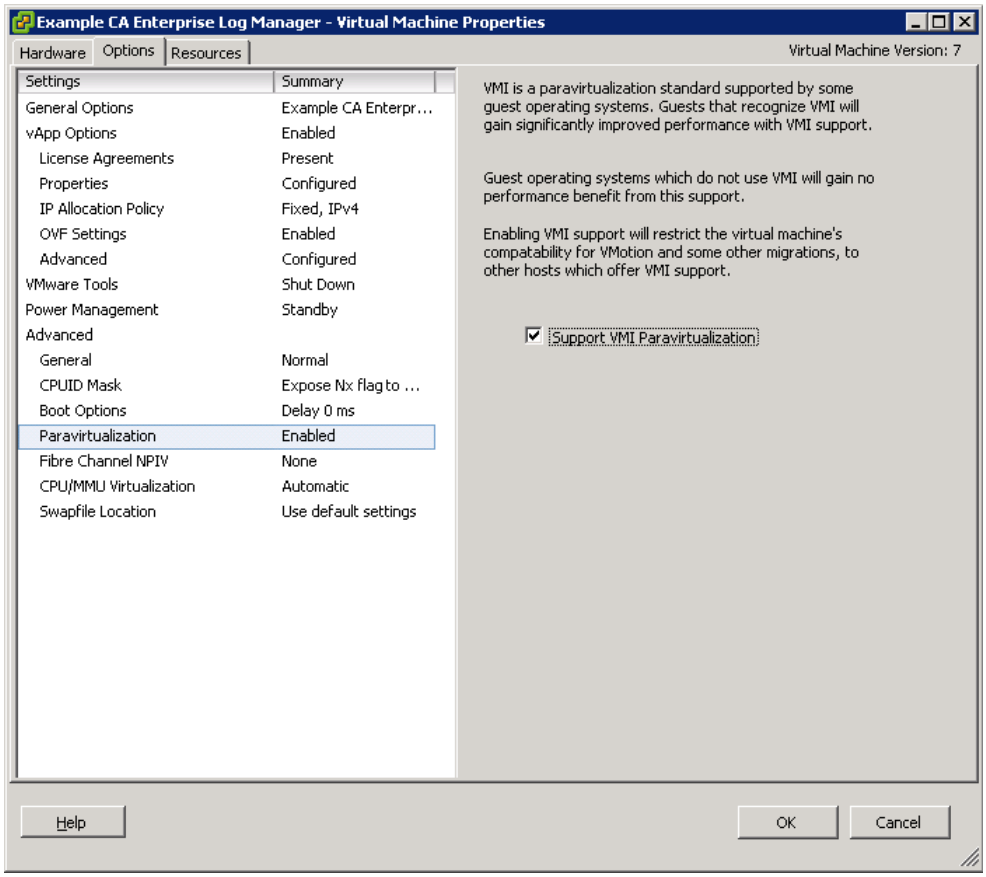
注: CD/DVD ドライブがクライアント デバイスに設定されていることを確認します。

Paravirtualization と Resource を設定する方法

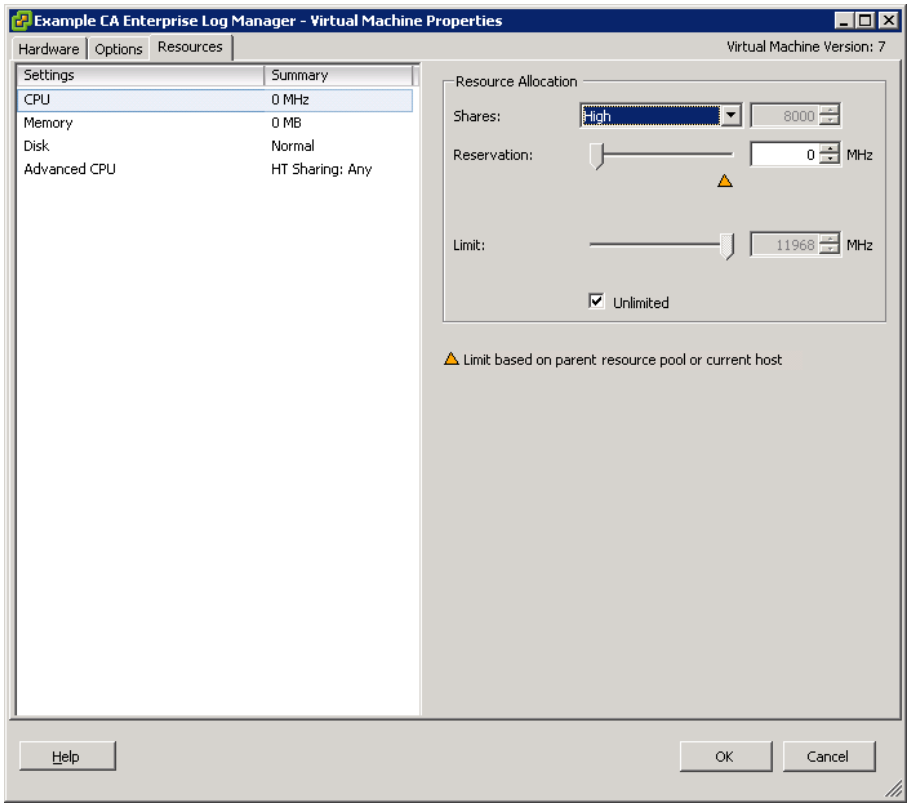
1. 左ペインの新しい[CA Enterprise Log Manager Virtual Appliance]を右クリックし、[Edit Settings]をクリックします。

   <*CA Enterprise Log Manager 仮想アプライアンス名* -> - [Virtual Machine Properties]ウィンドウが表示されます。

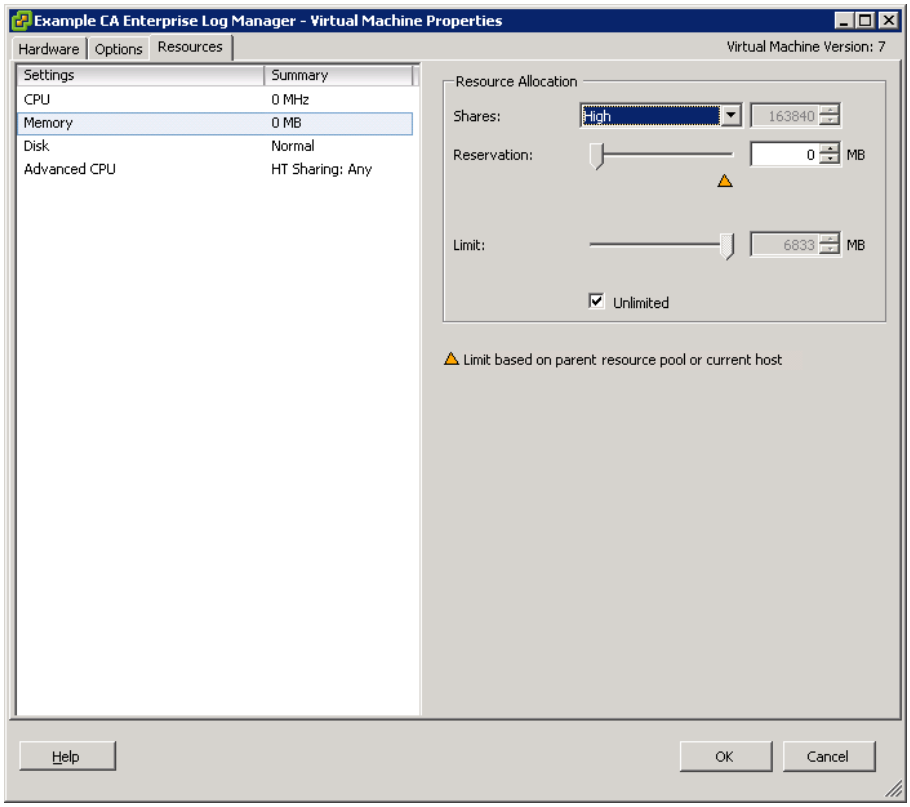
2. ウィンドウの[Option]タブをクリックします。
3. 左ペインで[Paravirtualization]設定を選択し、右ペインで[Support VMI Paravirtualization]オプションを選択します。



4. ウィンドウの[Resources]タブをクリックします。
5. [Settings]列から[CPU]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



6. [Settings]列から[Memory]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



7. [OK]をクリックします。
8. **注**: 準仮想化の詳細については、www.vmware.com を参照してください。

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れる

CA Enterprise Log Manager サーバを実行するため、電源を入れる必要があります。

CA Enterprise Log Manager サーバの電源を入れる方法

1. VMware アプリケーション ウィンドウの左ペインで新しい CA Enterprise Log Manager サーバを選択します。
2. 右ペインの[Getting Started]タブの[Basic Tasks]の下の[Power On]オプションをクリックします。

   CA Enterprise Log Manager サーバの電源が入ります。

注: セカンダリ CA Enterprise Log Manager サーバの電源を入れる前にプライマリ CA Enterprise Log Manager サーバが作動していることを確認してください。

CA Enterprise Log Manager サーバのサイレント インストール

仮想アプライアンスのサイレント インストールを実行するには、以下のタスクを実行する必要があります。

1. OVF ツールを起動します。
2. Paravirtualization と Resource を設定します。
3. プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れます。

以下の表では、OVF ツールを使用して CA Enterprise Log Manager を展開する際に使用するパラメータについて説明します。これらのパラメータは、コマンドラインでコマンド ライン引き数として指定する必要があります。

必要な情報	値	コメント
ホスト固有の設定		

必要な情報	値	コメント
HOSTNAME	*この CA Enterprise Log Manager サーバのホスト名* 例: CA-ELM1	ホストでサポートされている文字のみを使用して、このサーバのホスト名を指定します。業界基準では、A ～ Z(大文字と小文字を区別しない)、0 ～ 9、およびハイフンを使用し、最初の文字には英字、最後の文字には英数字を使用することを推奨しています。ホスト名内にアンダースコア文字を使用したり、このホストにドメイン名を追加したりしないでください。 **注**: ホスト名は 15 文字以内である必要があります。
ROOT_PASSWORD	*新しい root のパスワード*	このサーバ用の新しい root のパスワードを作成し、確認します。
IP_ADDRESS	*関連する IPv4 アドレス*	このサーバ用の有効な IP アドレスを入力します。
SUBNET_MASK	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクを入力します。
DEFAULT_GATEWAY	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクおよびデフォルト ゲートウェイを入力します。
DNS_SERVERS	*関連する IPv4 アドレス*	ネットワークで使用している 1 つ以上の DNS サーバの IP アドレスを入力します。 このリストはカンマで区切り、エントリ間にスペースは挿入しません。 DNS サーバが IPv6 のアドレス割り当てを使用している場合は、その形式でアドレスを入力します。
DOMAIN_NAME	*ドメイン名*	mycompany.com など、このサーバが動作するドメイン名を入力します。 **注**: IP アドレスに対するホスト名を解決できるようにするために、ネットワーク内の Domain Name Server (DNS)サーバにドメイン名を登録する必要があります。
acceptAllEulas	Accept	CA Enterprise Log Manager サーバのプロビジョニングを継続するには、CA 使用許諾契約を承諾します。

必要な情報	値	コメント
deploymentOption	「Medium」または「Large」	「Medium」を選択した場合、VMware は 4 つの CPU（各 CPU につき 8 GB の RAM）を提供します。「Large」を選択した場合、VMware は 8 つの CPU（各 CPU につき 8 GB の RAM）を提供します。
TIMEZONE	*希望するタイム ゾーン*	このサーバが存在する地域のタイム ゾーンを選択します。
アプリケーション固有の設定		
LOCAL_REMOTE_EEM	ローカル: 最初にインストールされたサーバ(管理サーバ)の場合 リモート: 追加サーバの場合	ローカルの CA EEM サーバを使用するのか、リモートの CA EEM サーバを使用するのかを示します。 管理用 CA Enterprise Log Manager サーバの場合は、ローカルを選択します。インストール中に、デフォルトの EiamAdmin ユーザ アカウントのパスワードを作成するように求めるプロンプトが表示されます。 個々の追加サーバについては、リモートを選択します。インストール中に、管理サーバ名を入力するように求めるプロンプトが表示されます。 ローカルを選択したかリモートを選択したかにかかわらず、最初は EiamAdmin アカウントの ID およびパスワードを使用して各 CA Enterprise Log Manager サーバにログオンする必要があります。
REMOTE_EEM_LOCATION	*IP アドレスまたはホスト名*	ローカル/リモート サーバ オプションでリモートを選択した場合のみ、この値を入力します。 最初にインストールした管理用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。 ホスト名を DNS サーバに登録する必要があります。 ローカル CA EEM サーバを使用する場合、デフォルト値は「**なし**」です。

必要な情報	値	コメント
EEM_PASSWORD	*EiamAdmin アカウントのパスワード*	デフォルトの管理者アカウント EiamAdmin のパスワードを記録します。 CA Enterprise Log Manager サーバに初めてログインする場合には、このアカウント認証情報が必要です。 管理サーバをインストールしている場合は、ここで EiamAdmin の新しいパスワードを作成して確認します。 他の CA Enterprise Log Manager サーバやエージェントをインストールするときに使用するため、このパスワードを書き留めておきます。 **注**: ここで入力したパスワードは、ssh を使用して CA Enterprise Log Manager サーバに直接アクセスするために使用するデフォルトの caelmadmin アカウントの初期パスワードでもあります。 必要に応じて、インストール後に追加の管理者アカウントを作成して CA EEM の機能にアクセスできます。
FIPS_MODE	はい、またはいいえ	仮想アプライアンスを FIPS モードで実行するか非 FIPS モードで実行するかを指定します。ローカル CA EEM サーバを使用する場合、いずれのモードも選択できます。リモート CA EEM サーバを使用する場合、リモート CA EEM サーバが使用するモードを選択する必要があります。

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

コマンド ラインからの OVF ツールの呼び出し

注: サイレント インストールを実行する前に、OVF Tool 1.0.0.0 をインストールする必要があります。OVF ツールの詳細については、VMware の「*OVF Tool User Guide*」または www.vmware.com を参照してください。

OVF ツールを呼び出すには、設定パラメータをコマンド ライン引き数として渡す必要があります。

注: 収集サーバのプロビジョニングには Medium 展開設定を使用し、レポート サーバのプロビジョニングには Large 展開設定を使用することを強くお勧めします。また、VMware のドキュメントで説明されているとおり、シック展開手法を使用することをお勧めします。

コマンド ラインからの OVF ツールの呼び出し方法

1. VMware vSphere クライアントがインストールされているコンピュータのコマンド プロンプトを開きます。
2. 以下のコマンドを実行して、OVF ツールを呼び出します。

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value
--prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value
--prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value
--prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value
--prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value
--prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host
name
```

メッセージ「Opening VI target」が表示されます。CA Enterprise Log Manager サーバの展開ステータスが表示されます。インストールが成功すると、左ペインの選択したデータ ストアの下に CA Enterprise Log Manager サーバがリスト表示されます。

注: プロパティ値にスペースが含まれる場合は、ダブルクォート("") でプロパティ値を囲みます。たとえば、OVF 名が CA ELM である場合は、値を "CA ELM.ovf" として入力します。OVF ツールの詳細については、「*OVF Tool User Guide*」を参照してください。

例

```
ovftool -dm=thick --acceptAllEulas --name="example_server"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_server1"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA
ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Paravirtualization と Resource の設定

OVF テンプレートをインポートした後、プロビジョニングされた CA Enterprise Log Manager サーバのパフォーマンスを改善するため、手動で Paravirtualization と Resource を設定する必要があります。

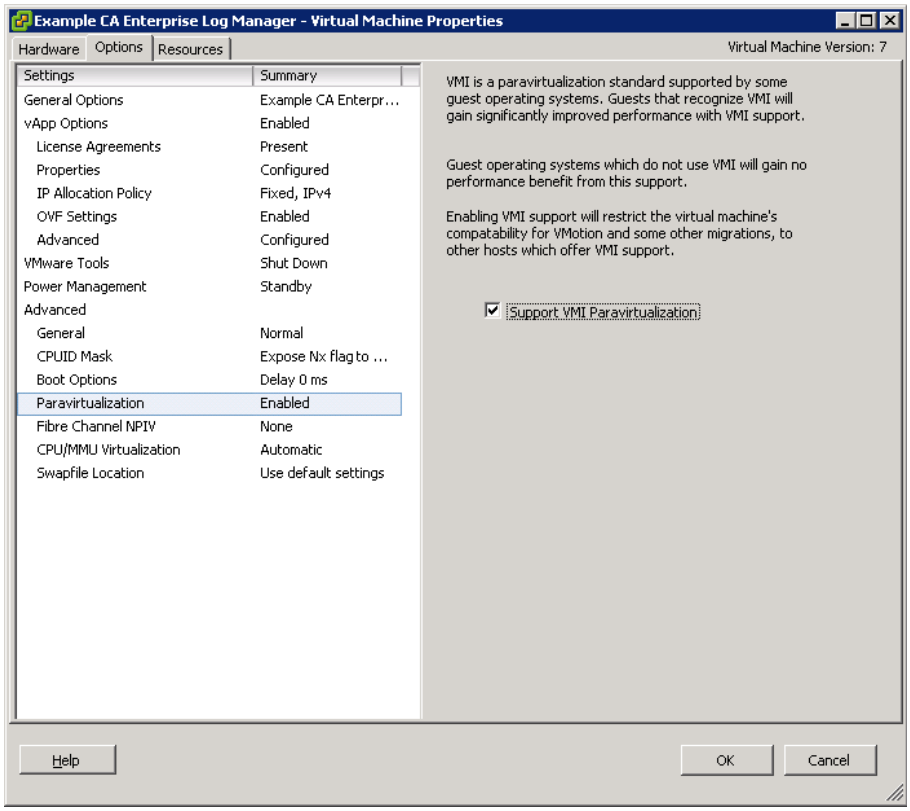
注: CD/DVD ドライブがクライアント デバイスに設定されていることを確認します。

Paravirtualization と Resource を設定する方法

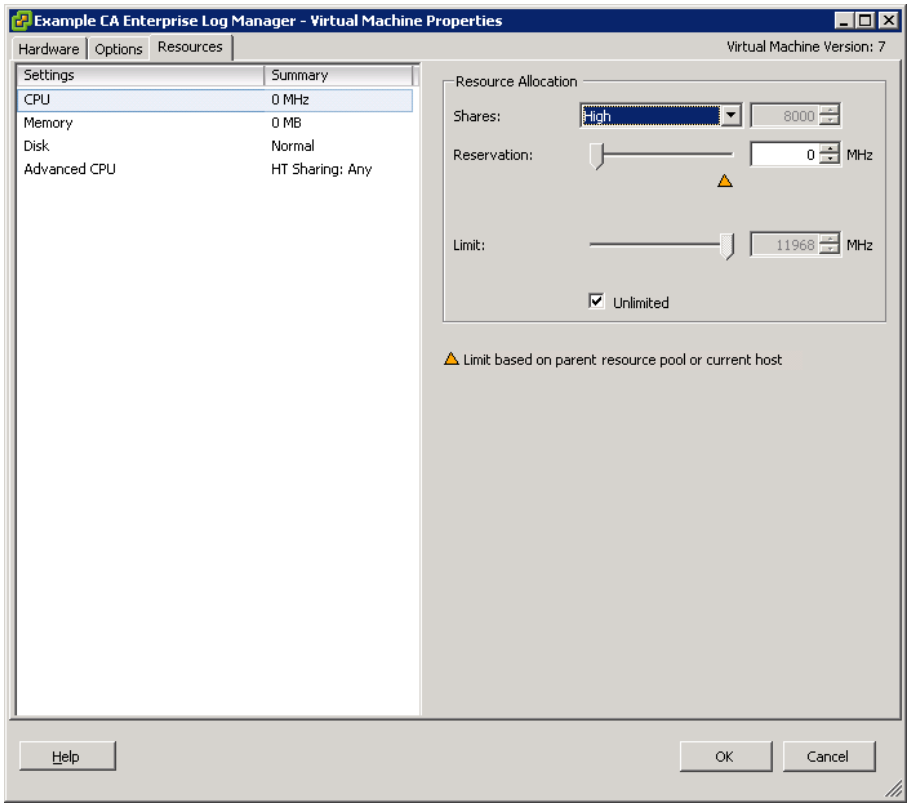
1. 左ペインの新しい[CA Enterprise Log Manager Virtual Appliance]を右クリックし、[Edit Settings]をクリックします。

   <*CA Enterprise Log Manager 仮想アプライアンス名* -> - [Virtual Machine Properties]ウィンドウが表示されます。

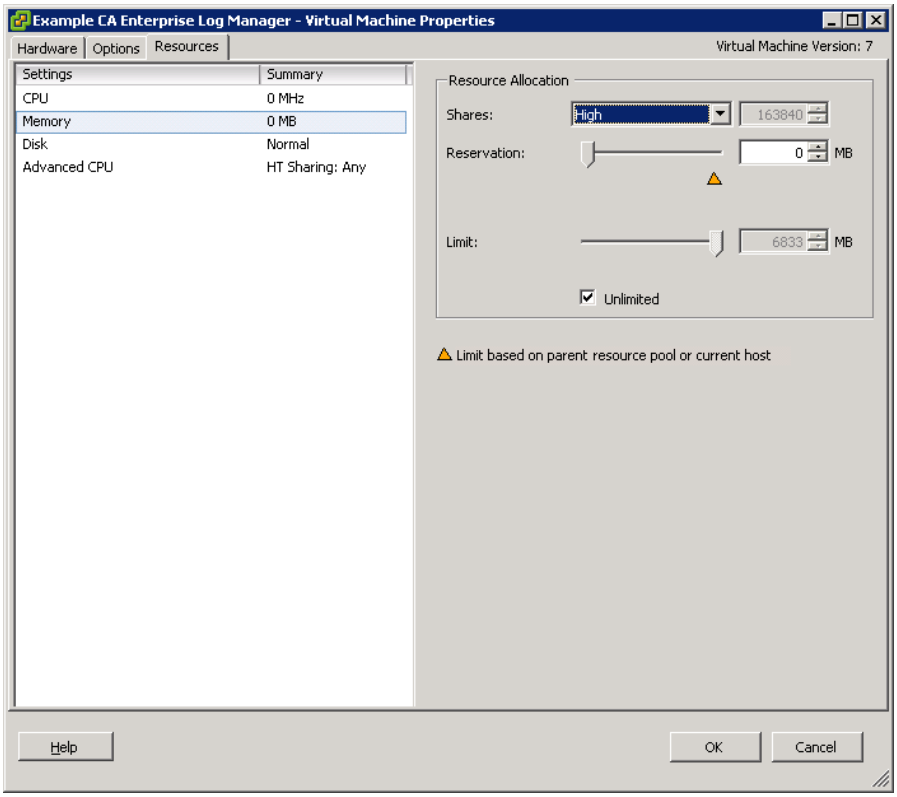
2. ウィンドウの[Option]タブをクリックします。
3. 左ペインで[Paravirtualization]設定を選択し、右ペインで[Support VMI Paravirtualization]オプションを選択します。



4. ウィンドウの[Resources]タブをクリックします。
5. [Settings]列から[CPU]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



6. [Settings]列から[Memory]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



7. [OK]をクリックします。
8. **注**: 準仮想化の詳細については、www.vmware.com を参照してください。

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れる

CA Enterprise Log Manager サーバを実行するため、電源を入れる必要があります。

CA Enterprise Log Manager サーバの電源を入れる方法

1. VMware アプリケーション ウィンドウの左ペインで新しい CA Enterprise Log Manager サーバを選択します。
2. 右ペインの[Getting Started]タブの[Basic Tasks]の下の[Power On]オプションをクリックします。

   CA Enterprise Log Manager サーバの電源が入ります。

注: セカンダリ CA Enterprise Log Manager サーバの電源を入れる前にプライマリ CA Enterprise Log Manager サーバが作動していることを確認してください。

仮想 CA Enterprise Log Manager サーバのインストールの確認

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れると、CA Enterprise Log Manager にアクセスする URL が[VMware vSphere Client]ウィンドウの[Console]タブに表示されます。CA Enterprise Log Manager にアクセスするには、この URL および以下のデフォルト ログイン認証情報を使用します。

デフォルト ユーザ名 : EiamAdmin

デフォルト パスワード : CA Enterprise Log Manager サーバのインストール中に入力したパスワード

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

仮想サーバの迅速な展開

収集用に仮想 CA Enterprise Log Manager サーバを迅速に展開するには、以下の手順に従います。

1. CA Enterprise Log Manager 仮想アプライアンス パッケージをダウンロードします。
2. CA Enterprise Log Manager サーバのサイレント インストール
3. CA Enterprise Log Manager サーバのインストールに関するセクションの説明に従って、仮想アプライアンス サーバを設定します。

重要: 仮想装アプライアンスを使用して CA Enterprise Log Manager サーバをプロビジョンする場合、プライマリ CA Enterprise Log Manager サーバのアプリケーション インスタンス名は CAELM である必要があります。

仮想アプライアンス パッケージをダウンロードします。

CA Enterprise Log Manager 仮想アプライアンスの配布イメージは、Support Online のダウンロード用リンクから入手可能です。5 つのファイルをダウンロードする必要があります。

- マニフェスト ファイル
- .ovf ファイル
- 3 つの仮想ディスク ファイル

CA Enterprise Log Manager サーバのサイレント インストール

仮想アプライアンスのサイレント インストールを実行するには、以下のタスクを実行する必要があります。

1. OVF ツールを起動します。
2. Paravirtualization と Resource を設定します。
3. プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れます。

以下の表では、OVF ツールを使用して CA Enterprise Log Manager を展開する際に使用するパラメータについて説明します。これらのパラメータは、コマンド ラインでコマンド ライン引き数として指定する必要があります。

必要な情報	値	コメント
ホスト固有の設定		
HOSTNAME	*この CA Enterprise Log Manager サーバのホスト名* 例: CA-ELM1	ホストでサポートされている文字のみを使用して、このサーバのホスト名を指定します。業界基準では、A ～ Z（大文字と小文字を区別しない）、0 ～ 9、およびハイフンを使用し、最初の文字には英字、最後の文字には英数字を使用することを推奨しています。ホスト名内にアンダースコア文字を使用したり、このホストにドメイン名を追加したりしないでください。 **注**: ホスト名は 15 文字以内である必要があります。
ROOT_PASSWORD	*新しい root のパスワード*	このサーバ用の新しい root のパスワードを作成し、確認します。

必要な情報	値	コメント
IP_ADDRESS	*関連する IPv4 アドレス*	このサーバ用の有効な IP アドレスを入力します。
SUBNET_MASK	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクを入力します。
DEFAULT_GATEWAY	*関連する IP アドレス*	このサーバで使用する有効なサブネット マスクおよびデフォルト ゲートウェイを入力します。
DNS_SERVERS	*関連する IPv4 アドレス*	ネットワークで使用している 1 つ以上の DNS サーバの IP アドレスを入力します。 このリストはカンマで区切り、エントリ間にスペースは挿入しません。 DNS サーバが IPv6 のアドレス割り当てを使用している場合は、その形式でアドレスを入力します。
DOMAIN_NAME	*ドメイン名*	mycompany.com など、このサーバが動作するドメイン名を入力します。 **注**: IP アドレスに対するホスト名を解決できるようにするために、ネットワーク内の Domain Name Server (DNS) サーバにドメイン名を登録する必要があります。
acceptAllEulas	Accept	CA Enterprise Log Manager サーバのプロビジョニングを継続するには、CA 使用許諾契約を承諾します。
deploymentOption	「Medium」または「Large」	「Medium」を選択した場合、VMware は 4 つの CPU (各 CPU につき 8 GB の RAM) を提供します。「Large」を選択した場合、VMware は 8 つの CPU (各 CPU につき 8 GB の RAM) を提供します。
TIMEZONE	*希望するタイム ゾーン*	このサーバが存在する地域のタイム ゾーンを選択します。
アプリケーション固有の設定		

必要な情報	値	コメント
LOCAL_REMOTE_EEM	ローカル: 最初にインストールされたサーバ(管理サーバ)の場合 リモート: 追加サーバの場合	ローカルの CA EEM サーバを使用するのか、リモートの CA EEM サーバを使用するのかを示します。 管理用 CA Enterprise Log Manager サーバの場合は、ローカルを選択します。インストール中に、デフォルトの EiamAdmin ユーザ アカウントのパスワードを作成するように求めるプロンプトが表示されます。 個々の追加サーバについては、リモートを選択します。インストール中に、管理サーバ名を入力するように求めるプロンプトが表示されます。 ローカルを選択したかリモートを選択したかにかかわらず、最初は EiamAdmin アカウントの ID およびパスワードを使用して各 CA Enterprise Log Manager サーバにログオンする必要があります。
REMOTE_EEM_LOCATION	*IP アドレスまたはホスト名*	ローカル/リモート サーバ オプションでリモートを選択した場合のみ、この値を入力します。 最初にインストールした管理用 CA Enterprise Log Manager サーバの IP アドレスまたはホスト名を入力します。 ホスト名を DNS サーバに登録する必要があります。 ローカル CA EEM サーバを使用する場合、デフォルト値は「**なし**」です。

必要な情報	値	コメント
EEM_PASSWORD	*EiamAdmin アカウントのパスワード*	デフォルトの管理者アカウント EiamAdmin のパスワードを記録します。 CA Enterprise Log Manager サーバに初めてログインする場合には、このアカウント認証情報が必要です。 管理サーバをインストールしている場合は、ここで EiamAdmin の新しいパスワードを作成して確認します。 他の CA Enterprise Log Manager サーバやエージェントをインストールするときに使用するため、このパスワードを書き留めておきます。 **注**: ここで入力したパスワードは、ssh を使用して CA Enterprise Log Manager サーバに直接アクセスするために使用するデフォルトの caelmadmin アカウントの初期パスワードでもあります。 必要に応じて、インストール後に追加の管理者アカウントを作成して CA EEM の機能にアクセスできます。
FIPS_MODE	はい、またはいいえ	仮想アプライアンスを FIPS モードで実行するか非 FIPS モードで実行するかを指定します。ローカル CA EEM サーバを使用する場合、いずれのモードも選択できます。リモート CA EEM サーバを使用する場合、リモート CA EEM サーバが使用するモードを選択する必要があります。

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

スクリプトを使用した OVF ツールの呼び出し

注: サイレント インストールを実行する前に、OVF Tool 4.0.0 をインストールする必要があります。OVF ツールの詳細については、VMware の「*OVF Tool User Guide*」を参照するか、www.vmware.com を参照してください。

OVF ツールを呼び出すコマンドを含むスクリプトを作成すし、実行することにより、複数の CA Enterprise Log Manager サーバを同時にインストールできます。スクリプトを作成するには、いずれのスクリプト言語を使用しても構いません。

スクリプトを使用した OVF ツールの呼び出し方法

1. OVF ツールを呼び出すためのスクリプトを作成します。
2. VMware vSphere クライアントがインストールされているコンピュータのコマンド プロンプトを開きます。
3. スクリプトが保存されているパスに移動します。
4. スクリプトを実行します。

   メッセージ「Opening VI target」が表示されます。各 CA Enterprise Log Manager サーバの展開ステータスが表示されます。インストールが成功すると、左ペインの選択したデータ ストアの下に CA Enterprise Log Manager サーバがリスト表示されます。

例 1: プライマリ CA Enterprise Log Manager サーバおよびセカンダリ CA Enterprise Log Manager サーバを作成するためのバッチ スクリプト

```
REM Primary CA Enterprise Log Manager Server
ovftool -dm=thin --acceptAllEulas --name="example_primaryserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.162.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_primary_server"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA
ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"

REM Secondary CA Enterprise Log Manager Server
```

```
ovftool -dm=thin --acceptAllEulas --name="example_secondaryserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password1"
--prop:LOCAL_REMOTE_EEM="Remote"
--prop:REMOTE_EEM_LOCATION="example_primaryserver" --prop:EEM_PASSWORD="calmr12"
--prop:FIPS_MODE="Yes" --prop:IP_ADDRESS="172.168.10.10"
--prop:SUBNET_MASK="10.0.10.10" --prop:HOSTNAME="example_secondary_server"
--prop:DEFAULT_GATEWAY="198.168.10.30"
--prop:DNS_SERVERS="198.168.20.20,198.168.20.25" --prop:DOMAIN_NAME="example.com"
--prop:TIMEZONE="Asia/Kolkata" "C:¥Program Files¥CA ELM¥CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

例 2: 管理サーバおよび 2 つの収集サーバを作成するためのバッチ スクリプト

```
REM CA Enterprise Log Manager Management Server
ovftool -dm=thin --acceptAllEulas --name="example_managementserver"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password"
--prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none
--prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.0.0
--prop:SUBNET_MASK=10.0.0.0 --prop:HOSTNAME="example_management_server"
--prop:DEFAULT_GATEWAY=198.168.0.0 --prop:DNS_SERVERS=198.168.10.20,198.168.10.25
--prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA
ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"

REM CA Enterprise Log Manager Collection Server 1
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver1"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password1"
--prop:LOCAL_REMOTE_EEM=Remote
--prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12
--prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.10 --prop:SUBNET_MASK=10.0.10.10
--prop:HOSTNAME="example_collection_server1" --prop:DEFAULT_GATEWAY=198.168.10.30
--prop:DNS_SERVERS=198.168.20.20,198.168.20.25 --prop:DOMAIN_NAME=example.com
--prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"

REM CA Enterprise Log Manager Collection Server 2
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver2"
--deploymentOption=medium --prop:ROOT_PASSWORD="example_password2"
--prop:LOCAL_REMOTE_EEM=Remote
--prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12
--prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172.168.10.30 --prop:SUBNET_MASK=10.0.10.40
--prop:HOSTNAME="example_collection_server2" --prop:DEFAULT_GATEWAY=198.168.10.40
--prop:DNS_SERVERS=198.168.30.30,198.168.30.25 --prop:DOMAIN_NAME=example.com
--prop:TIMEZONE=Asia/Kolkata "C:¥Program Files¥CA ELM¥CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0.10.0
"
```

Paravirtualization と Resource の設定

OVF テンプレートをインポートした後、プロビジョニングされた CA Enterprise Log Manager サーバのパフォーマンスを改善するため、手動で Paravirtualization と Resource を設定する必要があります。

注: CD/DVD ドライブがクライアント デバイスに設定されていることを確認します。

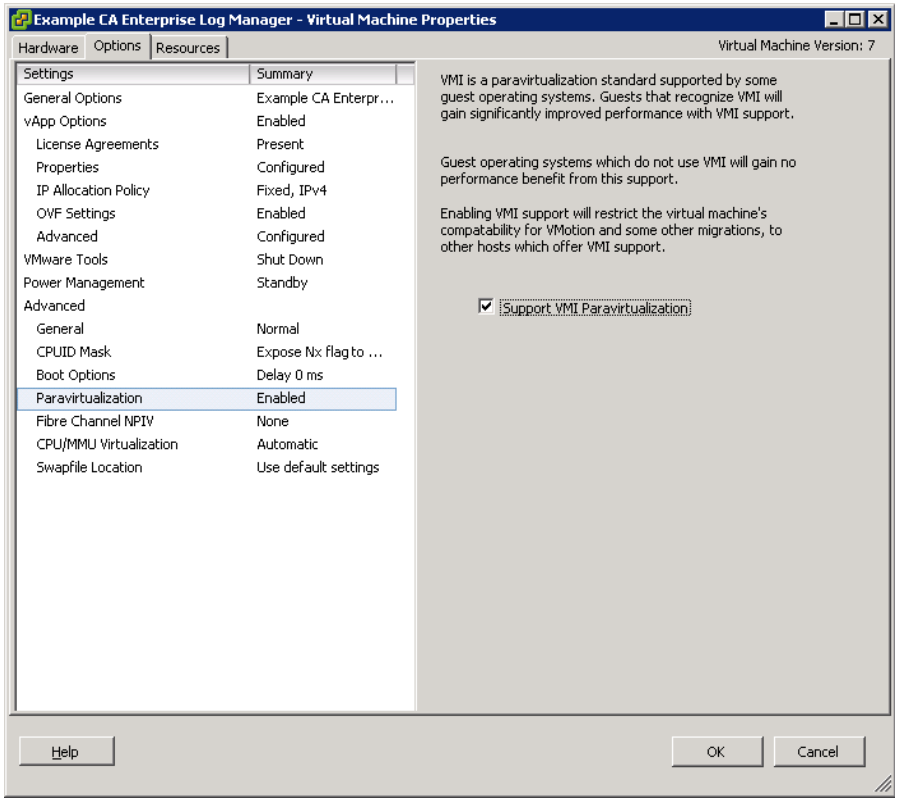
Paravirtualization と Resource を設定する方法

1. 左ペインの新しい[CA Enterprise Log Manager Virtual Appliance]を右クリックし、[Edit Settings]をクリックします。

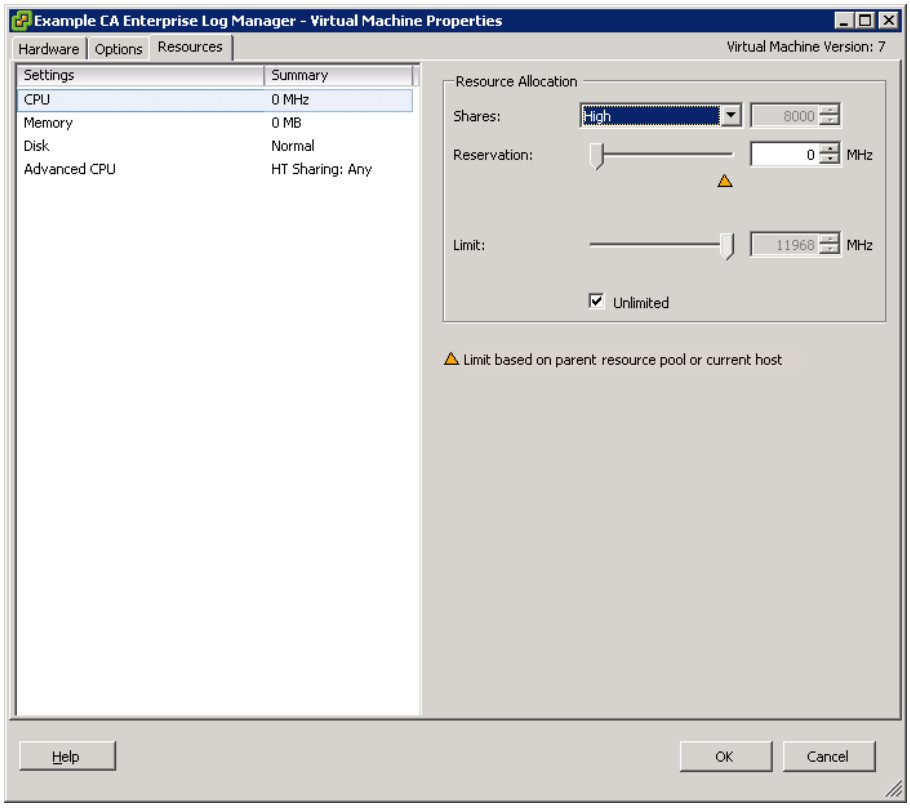
   <CA Enterprise Log Manager 仮想アプライアンス名 -> - [Virtual Machine Properties]ウィンドウが表示されます。

2. ウィンドウの[Option]タブをクリックします。

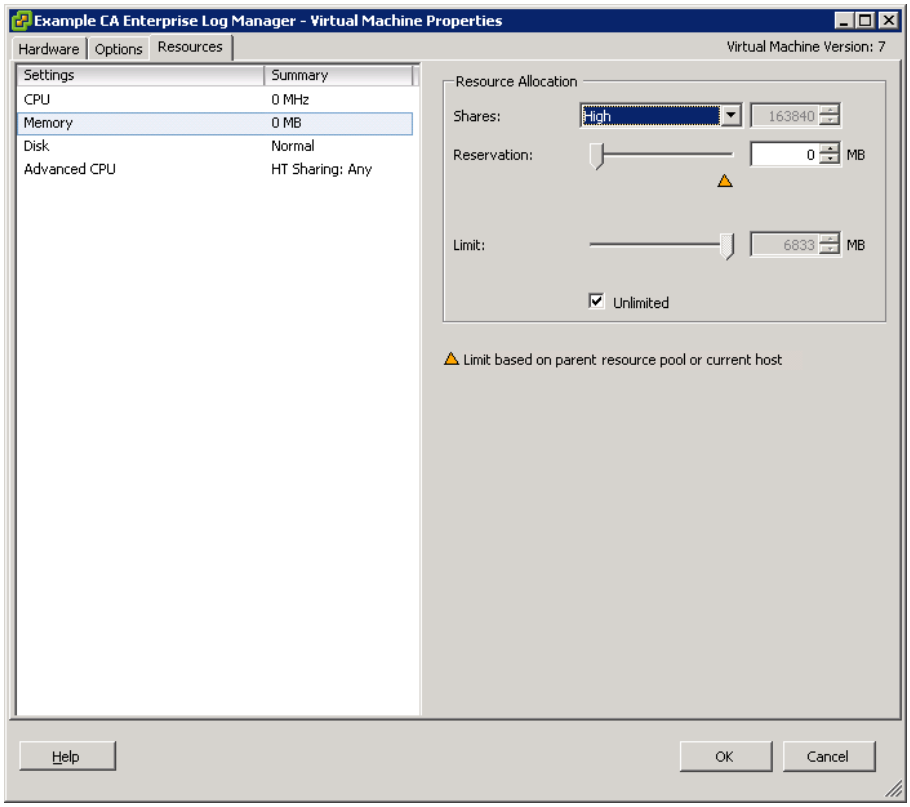
3. 左ペインで[Paravirtualization]設定を選択し、右ペインで[Support VMI Paravirtualization]オプションを選択します。



4. ウィンドウの[Resources]タブをクリックします。
5. [Settings]列から[CPU]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



6. [Settings]列から[Memory]オプションを選択し、[Resource Allocation]セクションの[Shares]ドロップダウンから「High」を選択します。



7. [OK]をクリックします。
8. **注**: 準仮想化の詳細については、www.vmware.com を参照してください。

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れる

CA Enterprise Log Manager サーバを実行するため、電源を入れる必要があります。

CA Enterprise Log Manager サーバの電源を入れる方法

1. VMware アプリケーション ウィンドウの左ペインで新しい CA Enterprise Log Manager サーバを選択します。
2. 右ペインの[Getting Started]タブの[Basic Tasks]の下の[Power On]オプションをクリックします。

   CA Enterprise Log Manager サーバの電源が入ります。

注: セカンダリ CA Enterprise Log Manager サーバの電源を入れる前にプライマリ CA Enterprise Log Manager サーバが作動していることを確認してください。

仮想 CA Enterprise Log Manager サーバのインストールの確認

プロビジョニングされた CA Enterprise Log Manager サーバの電源を入れると、CA Enterprise Log Manager にアクセスする URL が[VMware vSphere Client]ウィンドウの[Console]タブに表示されます。CA Enterprise Log Manager にアクセスするには、この URL および以下のデフォルト ログイン認証情報を使用します。

デフォルト ユーザ名 : EiamAdmin

デフォルト パスワード : CA Enterprise Log Manager サーバのインストール中に入力したパスワード

詳細情報

使用している環境への仮想サーバの追加 (P. 331)
完全な仮想環境の作成 (P. 355)
仮想サーバの迅速な展開 (P. 380)

インストール後のタスク

CA Enterprise Log Manager サーバの電源を入れた後、以下の操作が実行できます。

- キーボード タイプの変更
- NTP サーバの追加

キーボード タイプの変更

デフォルトでは、プロビジョニングされた CA Enterprise Log Manager サーバは標準 US キーボードを使用します。国の言語設定を変更して、使用するキーボード タイプを変更できます。

キーボード タイプの変更方法

1. root ユーザとして CA Enterprise Log Manager コンソールにログインします。
2. 以下のコマンドを実行します。

   ```
   vi /etc/sysconfig/keyboard
   ```

   キーボード ファイルが編集モードで開きます。既存のキーボード タイプの詳細が表示されます。
3. KEYTABLE 値の「US」を希望する国の言語設定に変更します。

   たとえば、UK キーボードを使用するには、KEYTABLE 値を KEYTABLE="UK" と入力します。

   注: 国の言語設定の詳細については、RHEL インストール ドキュメント セットを参照してください。
4. ファイルを保存して閉じます。
5. コンピュータを再起動します。

   これでキーボード タイプが変更されます。

NTP サーバの追加

CA Enterprise Log Manager サーバの日付および時間を更新するために NTP サーバを追加することを強くお勧めします。

NTP サーバの追加方法

1. root ユーザとして CA Enterprise Log Manager コンソールにログインします。
2. 以下のコマンドを実行します。

   ```
   crontab -e
   ```

   ```
   00 0 * * * /usr/sbin/ntpdate NTPserver_hostname
   ```

   cron ジョブが追加されます。
3. 変更を保存し、コンソールを終了します。

   これで NTP サーバが追加されました。

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。

FIPS 140-2

FIPS 140-2 は、連邦情報処理標準（Federal Information Processing Standard）です。この連邦標準は、SBU（sensitive but unclassified：取扱注意だが機密扱いなし）情報を保護するセキュリティ システムで使用される暗号モジュールのセキュリティ要件を規定しています。この標準は、広範囲のアプリケーションおよび環境に対応するために 4 つのセキュリティ品質レベルを定義しています。

FIPS 140-2 互換

FIPS 140-2 互換とは、オプションで FIPS 準拠の暗号ライブラリおよびアルゴリズムを使用して機密データを暗号化および復号化できる製品の呼称です。CA Enterprise Log Manager は、FIPS 準拠のログ収集製品です。CA Enterprise Log Manager では、FIPS モードまたは FIPS 非準拠モードを選択できます。

FIPS 140-2 準拠

FIPS 140-2 準拠とは、認定された暗号モジュール テスト(CMT)機関によって認証された暗号化アルゴリズムのみをデフォルトで使用する製品の呼称です。CA Enterprise Log Manager は、認証された RSA BSAFE Crypto-C ME および Crypto-J ライブラリに基づく暗号化モジュールを FIPS モードで使用できますが、デフォルトでは使用しない場合があります。

FIPS 非準拠モード

FIPS 非準拠モードはデフォルトの設定です。この設定では、CA Enterprise Log Manager サーバおよびエージェントが FIPS 準拠でない技術を含む暗号化技術を組み合わせて使用できます。代わりに使用される設定は FIPS モードです。

FIPS モード

FIPS モードの設定では、CA Enterprise Log Manager サーバおよびエージェントは RSA の FIPS 準拠の暗号モジュールを使用して暗号化を行う必要があります。代わりに使用される設定は FIPS 非準拠モードです。

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。

varbind

varbind は SNMP 変数バインディングです。各 varbind は、OID、タイプ、および値から構成されています。varbind はカスタム MIB に追加します。

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。

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。

カスタム MIB

カスタム MIB は、CA NSM などの SNMP トラップ宛先に送信されるアクション アラート用に作成する MIB です。アクション アラートで指定されたカスタム トラップ ID は、トラップとして送信される選択された CEG フィールドを定義する MIB の存在を前提としています。

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。

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。

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 アプライアンスは、ソフトウェアに加えて基盤となるオペレーティング システムおよびすべての依存パッケージで構成される、必要な機能をすべて備えたフトウェア パッケージです。このパッケージは、ソフトウェア アプライアンス インストール メディアから起動することで、エンド ユーザのハードウェアにインストールされます。

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。

非対話型の ssh 認証

非対話型の認証を使用すると、認証用の*パスフレーズを入力することなく、あるサーバ上のファイルを別のサーバに移動できます。ソース サーバから宛先サーバへの非対話型の認証の設定は、自動アーカイブの設定前または restore-ca-elm.sh スクリプトの使用前に行います。*

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。

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

I

L

S

あ

か

さ

た

は

や

ら

わ