CA Enterprise Log Manager

リリース ノート

r12.1 SP1

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

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

CA への連絡先

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

マニュアルの変更点

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

- サブスクリプションによるアップグレード -- この既存のトピックは更新され、CA Enterprise Log Manager r12.1 SP1 に固有の情報が追加されました。サブスクリプションを使用してこのサービス パックを取得し、FIPS に対応するために CA Enterprise Log Manager をアップグレードします。
- r12.1 SP1 の新機能と変更された機能 -- この章では、CA Enterprise Log Manager の FIPS 互換性、使用される暗号化、制限、および Microsoft Internet Explorer と Mozilla Firefox からユーザ インターフェースにアクセスするために必要な設定変更について説明します。さらに、ISO イメージを使用した新しい展開、および、既存の展開への新しい CA Enterprise Log Manager サーバの追加についてのトピックを含んでいます。
- CA EEM サーバ システムの時間変更によって生じる証明書不一致エラー -- この既存トピックは、新しい証明書ファイル拡張子 .cer を反映するために変更されました。
- 特定の HP および IBM コンピュータの電力設定の前提条件 -- この新しいトピックでは、HP Proliant DL 380G5 シリーズ サーバおよび IBM X3650 シリーズ サーバのデフォルト電力設定の前提条件の変更について説明します。
- 以下の既知の問題は、この更新で修正されたか、該当しなくなったため削除されました。
  - エージェントでカスタム証明書を使用できない
  - syslog のセカンダリ ディスパッチャがロードで失敗する
  - 同じホストからのイベントが別の宛先ホストで表示される場合がある
  - PDF レポート仕様に対する制限
  - アップグレードの後に CA Enterprise Log Manager にログインできない
  - r12.1 M10 に直接更新するとセンサ バージョンが不正確に表示される
  - Audit ポリシー マネージャがインストールされていないというエラーが間違って表示される
  - CA Enterprise Log Manager との相互運用に必要な CA Audit へのアップグレード

詳細情報:

目次

第 1 章: はじめに

CA Enterprise Log Manager をご利用いただき、誠にありがとうございます。このドキュメントには、オペレーティング システムのサポート、強化された機能、既知の問題、および CA テクニカル サポートへの問い合わせに関する情報が含まれています。

サブスクリプションによるアップグレード

サブスクリプションで配信されるすべてのモジュールをダウンロードし、CA Enterprise Log Manager を最新リリース、またはサービス パックにアップグレードします。

重要 新しい CA Enterprise Log Manager サーバをネットワーク内にインストールする前に、管理 CA Enterprise Log Manager サーバをアップグレードしてください。これにより、新しいサーバを正常に登録できるようになります。

以下のガイドラインに従ってください。

1. サブスクリプション設定を確認して、基本設定が完了していることを検証します。
   a. [管理]タブ、[サービス]サブタブをクリックし、サブスクリプション モジュールを選択します。
   b. [OS 更新後に自動再起動]で[いいえ]を選択します。
   c. 選択リストに Log Manager モジュールを移動します(選択済みでない場合)。
   d. すべての必須値がグローバル レベルで設定されていることを確認します。
   e. すべての必須値が各 CA Enterprise Log Manager サーバ用に設定されることを確認します。

   注: 連携環境では、子を更新する前に親を更新します。

   サブスクリプションの更新がインストールされていることを示していた自己監視イベントが完了を示します。

2. サブスクリプション設定を確認して、基本設定が完了していることを検証します。

   a. [管理]タブ、[サービス]サブタブをクリックし、サブスクリプション モジュールを選択します。

   b. [OS 更新後に自動再起動]で[いいえ]を選択します。

   c. ダウンロードする残りのモジュールをすべて選択リストに移動します。

   注: 連携環境では、子を更新する前に親を更新します。

3. サブスクリプションの更新プロセスが完了したところで、各 CA Enterprise Log Manager サーバを再起動します。

   サブスクリプションの更新がインストールされていることを示していた自己監視イベントが完了を示します。

4. 以下の手順でエージェントとコネクタを更新します。

   a. [管理]タブをクリックし、[ログ収集]サブタブをクリックして[エージェント エクスプローラ]を選択します。

   b. サブスクリプションの更新を、エージェント エクスプローラ レベル、エージェント グループ レベル、エージェント レベルのどのレベルで適用するのか判断します。

   c. 該当するレベルを選択し、[サブスクリプション]ボタンをクリックします。

   d. エージェントがダウンロードされたモジュールの中に含まれていた場合は、エージェントに更新を適用します。

   e. もう一度、[サブスクリプション]ボタンをクリックします。

   f. 利用可能な場合は、コネクタに更新を適用します。

5. サードパーティ製品および他の CA 製品（CA Access Control など）を再登録します。これらの製品は、オープン API コールを使用して、それぞれのネイティブ インターフェースに CA Enterprise Log Manager レポートを表示します。

   この手順が完了すると、このリリースで変更された証明書が更新されます。詳細については、「CA Enterprise Log Manager API プログラミング ガイド」を参照してください。

注: サブスクリプション アップグレードに関連する既知の問題については、「リリース ノート」を参照してください。

詳細情報:

OS 更新後、SP のアップグレード時に自動的に再起動する (P. 67)
r12.1 SP1 で更新された syslog ログ センサにより Windows エージェント上の統合の更新が必要となる (P. 74)

第 2 章: 動作環境

このセクションには、以下のトピックが含まれています。

ハードウェアとソフトウェアの動作環境

CA Enterprise Log Manager の初期セットアップを実行すると、Red Hat Enterprise Linux オペレーティング システムがインストールされます。

CA Enterprise Log Manager 認定マトリックス インデックスは、以下を含むすべての CA Enterprise Log Manager 認定マトリックスのリンクを示します。

- サーバのハードウェアとソフトウェア

  CA Enterprise Log Manager サーバのハードウェアおよびソフトウェアの認定マトリックス

- エージェントのハードウェアとソフトウェア

  CA Enterprise Log Manager エージェントのハードウェアおよびソフトウェアの認定マトリックス

- ログ センサおよび関連するオペレーティング システムのサポート

  CA Enterprise Log Manager ログ センサの認定マトリックス

- 製品統合

  CA Enterprise Log Manager 製品統合マトリックス

- CA Audit iRecorders の認定

  CA Enterpise Log Manager Audit iRecorder 認定マトリックス

CA Enterprise Log Manager には、以下のブラウザと、Adobe Flash 9 または 10 Player を使ってアクセスできます。

- Internet Explorer 6 SP2（FIPS 非準拠モードのみ）
- Internet Explorer 7 または 8（FIPS モードまたは FIPS 非準拠モード）
- Mozilla Firefox 2.0.x および 3.0.x（FIPS 非準拠モードのみ）
- Mozilla Firefox 3.5.8 以降（FIPS モードおよび FIPS 非準拠モード）

注: Mozilla Firefox ブラウザで CA Enterprise Log Manager にアクセスした場合、ファイルのエクスポートは機能しません。

特定の HP および IBM コンピュータの電力設定の前提条件

CA Enterprise Log Manager が HP Proliant DL 380G5 シリーズ サーバおよび IBM X3650 シリーズ サーバにデフォルトの電力使用設定でインストールされた場合、iGateway に関する問題が発生し、その結果動作が低下するか、または手動によるサービスの再起動が必要になるその他の問題が発生する可能性があります。

この問題の発生を防ぐには、CA Enterprise Log Manager をインストールする前に設定を変更してください。

注: すでに CA Enterprise Log Manager をインストールした場合は、コンピュータを停止し、以下の説明に従って設定を変更してからコンピュータを再起動します。

HP Proliant DL 380G5 の電力使用設定を変更する方法

1. BIOS 設定メニューにアクセスします。
2. 電力使用設定に移動します。
3. オプションから[OS Control Mode]を選択します。

   注: デフォルト設定は[HP Dynamic Power Settings Mode]です。

IBM X3650 の電力使用設定を変更する方法

1. BIOS 設定メニューにアクセスします。
2. 電力使用設定に移動します。
3. 以下のパラメータを無効にします。
   - Active Energy Manager
   - Enhanced C1 Power State

モニタ解像度

モニタ解像度の最小要件は 1024 × 768 ピクセルです。最適な表示には、1280 × 1024 のモニタ解像度が推奨されます。

CA EEM サーバ リファレンス

既存の CA EEM サーバのオペレーティング システムのサポートについては、「CA Embedded Entitlements Manager 導入ガイド」を参照してください。*このガイドは CA Enterprise Log Manager マニュアル選択メニューに含まれています。*

また、このマニュアル選択メニューはテクニカル サポートからダウンロードできます。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

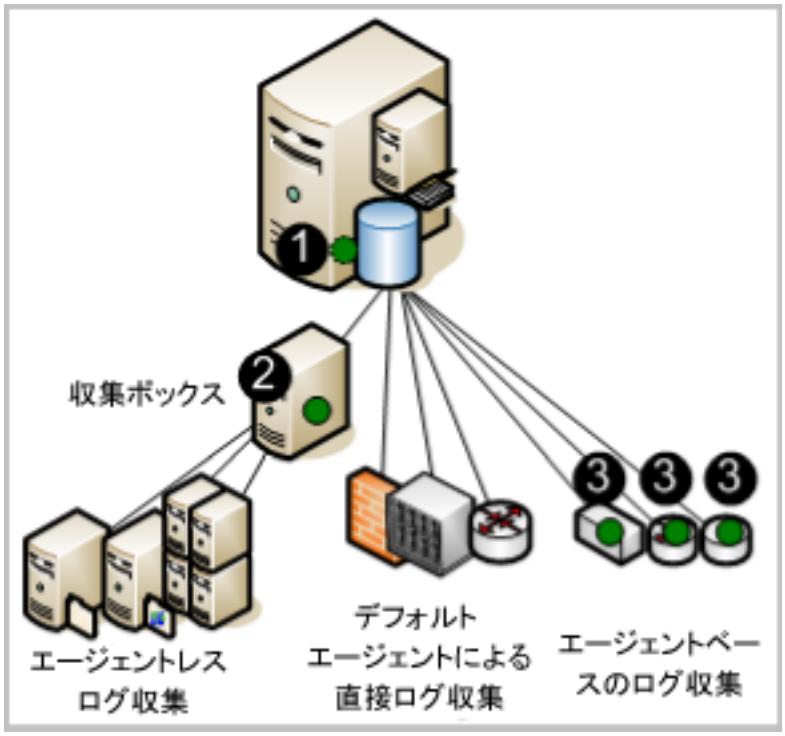
第 3 章: 機能

このセクションには、以下のトピックが含まれています。

ログ収集

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

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



図の番号は、次のステップを示しています。

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

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

各ログ収集方法には、次のような利点があります。

- 直接ログ収集

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

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

- エージェントレス収集

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

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

- エージェントベースの収集

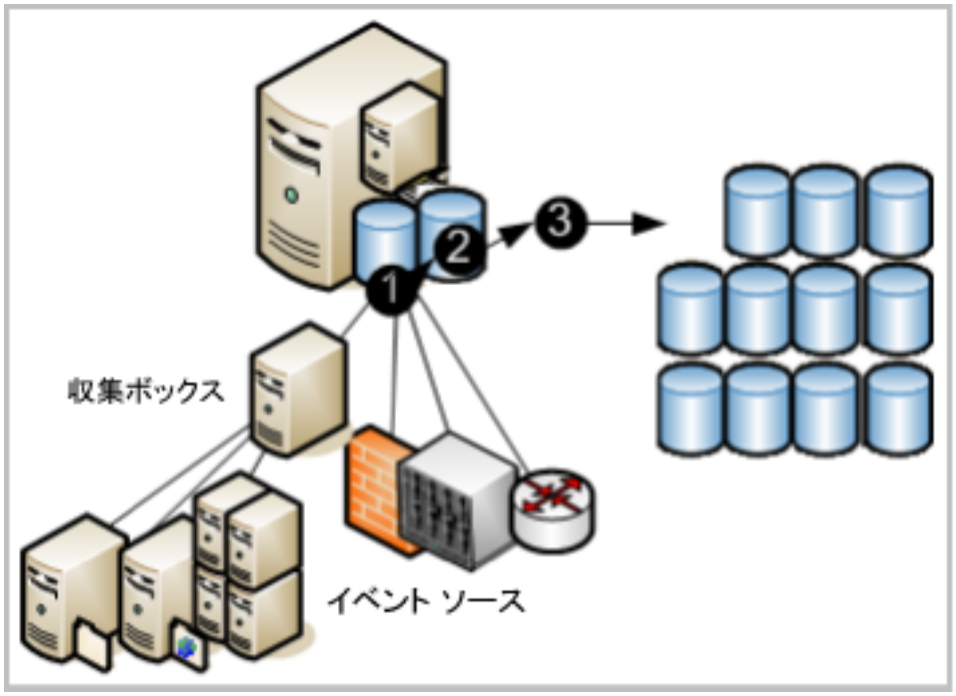
  エージェントベースの収集では、1 つ以上のイベント ソースが実行されていて、各イベント ソースのコネクタが設定されている場所にエージェントがインストールされます。

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

注: エージェント設定の詳細については、「管理ガイド」を参照してください。

ログ ストレージ

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



図の番号は、次のステップを示しています。

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

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

ログの標準化された表示

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

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

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

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

コンプライアンス レポート

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

システムには次の機能が備わっています。

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

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

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

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

ログ表示機能は、以下の機能によりサポートされています。

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

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

ポリシー違反アラート

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

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

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

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

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

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

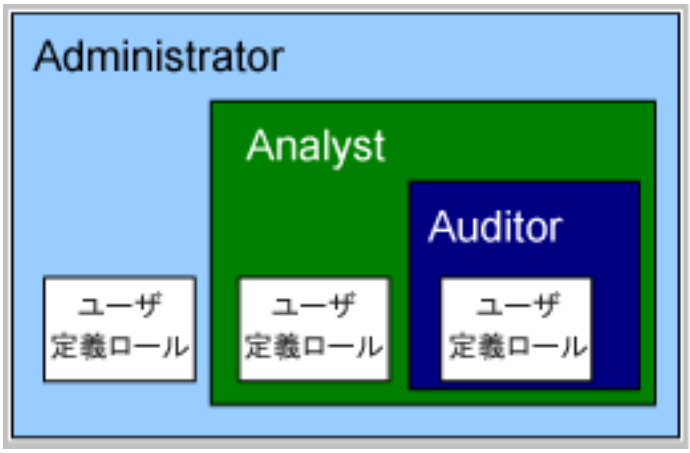
注: アクション アラートの詳細については、「CA Enterprise Log Manager 管理ガイド」を参照してください。

ロールベースのアクセス

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

- Administrator
- Analyst
- Auditor

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



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

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

サブスクリプション管理

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

次の図は、最も単純な直接インターネット接続シナリオを表しています。

図の番号は、次のステップを示しています。

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

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

IPv6 IP アドレスのサポート

従来は、IP アドレスの指定方法として、IPv4 のドット区切りの 10 進表記のみがサポートされていました。 現行リリースでは、IP アドレス フィールドに IPv6 アドレスを指定できます。 IPv6 は、IPv4 で使用される 32 ビット アドレスの代わりに 128 ビット IP アドレスを使用します。IP アドレスのバージョンを基にしたポリシーはすべて IPv4 および IPv6 をサポートします。

IPv4 マップ IPv6 アドレスと従来の IPv6 フォーマットの両方を使用できます。IPv4 マップ IPv6 アドレス フォーマットでは、以下のように IPv4 ノードの IPv4 アドレスを IPv6 アドレスとして表すことができます。

- IPv6 形式は、8 グループの 4 桁の 16 進数(x:x:x:x:x:x:x:x)で表すのが一般的です。x はそれぞれ、1 ～ 4 桁の 16 進数を表し、アドレスを 16 ビットずつに分けた 8 ブロックの内の 1 つに相当します。
- IPv4 射影 IPv6 アドレスは、IPv4 ノードと IPv6 ノードが混在する環境で使用する際に役立ちます。表記は、0:0:0:0:0:FFFF:d.d.d.d のようになります。d はそれぞれ、10 進数で表したアドレスです(IPv4 のドット区切りの 10 進表記)。

  重要: 0:0:0:0:0:0:d.d.d.d というフォーマットの IPv4 互換 IPv6 アドレスは、RFC 4291 によると、最新の IPv6 移行メカニズムでは使われなくなっているため、現在は推奨されていません。

以下は従来のフォーマットで記述された有効な IPv6 アドレスです。

2001:0db8:85a3:08d3:1319:8a2e:0370:7334

1 つ以上の 4 桁のグループが 0000 の場合、0 を省略して、2 つのコロン(::)で置き換えることができます。 グループ中の先頭の 0 も省略できます。次の例の IP アドレスはすべて同じです。

- 2001:0db8:0000:0000:0000:0000:1428:57ab
- 2001:0db8::1428:57ab
- 2001:db8:0:0:0:0:1428:57ab
- 2001:db8::1428:57ab

IPv4 アドレスを IPv4 マップ アドレスに置き換える場合、ガイドラインとして次の例を使ってください。

- 0:0:0:0:0:FFFF:192.168.2.128
- 0:0:0:0:0:FFFF:172.16.2.128

あるいは、次の圧縮した形式を使用できます。

- ::FFFF:192.168.2.128
- ::FFFF:172.16.2.128

第 4 章: r12.1 の新機能と変更された機能

このセクションには、以下のトピックが含まれています。

オープンな API アクセス

CA Enterprise Log Manager では、クエリおよびレポート メカニズムを使用し、API 呼び出によってイベント リポジトリのデータにアクセスし、Web ブラウザで表示することができます。また、CA またはサードパーティ製品のインターフェースに CA Enterprise Log Manager クエリまたはレポートを組み込むために API を使用することもできます。

CA Enterprise Log Manager API には以下の機能があります。

- 認証済みの安全な API
- シングルサインオン(SSO)の製品登録
- タグによってフィルタされたクエリまたはレポート リストの取得
- 対話型 CA Enterprise Log Manager インターフェースでのクエリやレポートの表示により、フィルタリングや、ユーザ インターフェースへの埋め込みが可能

API の詳細は、「API プログラミング ガイド」およびオンライン ヘルプを参照してください。

実用的なアラート: CA IT PAM 統合

CA Enterprise Log Manager は、ログ記録の量をクエリするスケジュール済みアラートによって、規制違反の可能性のある動作や、不審な IT アクティビティを検出します。CA Enterprise Log Manager は、個々のアラートを調査する IT のセキュリティ担当者に通知し、修正が必要かどうかの決定を可能にします。一般的な調査作業は、機械的な作業が多く、自動化に適しています。CA Enterprise Log Manager と CA IT PAM 間の緊密な統合によって、これら機械的なレスポンス作業は自動的に実行できます。IT セキュリティ担当者は、反復性の高い作業から解放され、最も重要な案件のみに集中できます。

CA IT PAM 統合によって、アラートから事前定義済み CA IT PAM イベント/アラート出力プロセスを実行することで、CA Service Desk でリクエストを作成できます。さらに、CA Enterprise Log Manager からも、不審なイベントへのその他のレスポンスを自動化するカスタム IT PAM イベント/アラート出力プロセスを実行できます。

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/アラート プロセスの使用」セクションを参照してください。

実用的なアラート: NSM 製品との SNMP 統合

スケジュール済みクエリが不審なアクティビティを表すイベントを取得すると、アラートが生成されます。このようなアラートは SNMP トラップとして CA Spectrum や CA NSM などのネットワーク セキュリティ モニタリング (NSM) 製品へ自動的に送信できます。CA Enterprise Log Manager から SNMP トラップを受信して変換するように送信先製品を準備し、次に送信先を設定して、送信するイベント情報を指定します。

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「SNMP トラップの使用」セクションを参照してください。

ODBC および JDBC アクセス

CA Enterprise Log Manager は、ODBC と JDBC を使用して収集されたイベントログ情報へ、読み取りアクセスのみを許可します。このアクセスによって、以下のような処理を実行できます。

- BusinessObjects Crystal Reports などのツールを使用した顧客レポートの作成
- 相関エンジンによる選択したログ情報の取得
- 侵入やマルウェアの検出のログの確認

ODBC および JDBC のアクセス機能では、ネットワーク内の適切なサーバにインストールされたクライアントを使用します。CA Enterprise Log Manager サーバは、サブスクリプションの更新およびインストールの処理中に自動的にサーバ側コンポーネントをインストールします。

インストールの情報については、「実装ガイド」を参照してください。設定の情報や例については、「管理ガイド」を参照してください。

ID とアセットの連携: CA IT PAM 統合

CA IT PAM 統合によって、CA IT PAM 動的値プロセスを実行することで、特定のキーの値を常に更新された状態で維持できます。動的値プロセスは、最新データを格納するリポジトリから現在の値を取得します。アセット ファイルまたはデータベースからクリティカル アセットの値を取得するプロセスを作成した場合、事前定義済みレポートおよびクエリでボタンをクリックすることで Critical_Asset キーを更新できます。

詳細については、「CA Enterprise Log Manager 管理ガイド」の「クエリおよびレポート」の章にある「動的な値のインポートの有効化」のセクションを参照してください。

拡張されたデフォルト エージェントによる直接ログ収集

CA Enterprise Log Manager のインストールでは、syslog イベントの収集を有効にするために、Syslog_Connector という名の syslog リスナがデフォルト エージェントに展開されます。さらに、Linux_localsyslog 統合と関連するコネクタの Linux_localsyslog_Connector も、syslog イベントの収集に使用できるようになります。

これにより、デフォルト エージェントでは、syslog イベント以外のイベントを直接収集可能になります。 WinRm コネクタを使用すると、デフォルト エージェントで、Microsoft Windows プラットフォームで実行されている製品からイベントを収集できます。たとえば、Active Directory Certificate Services や Microsoft Office Communication Server などから収集できます。ODBC コネクタを使用すると、デフォルト エージェントは、Oracle9i 、SQL Server 2005、およびこれらのデータベースにイベントを格納するアプリケーションなどの複数のデータベースからイベントを収集できます。

サブスクリプション クライアントの自動更新スケジュール

最初の CA Enterprise Log Manager サーバをインストールするときには、サブスクリプションを含むすべてのサービスに適用されるグローバル設定を設定します。サブスクリプションに関しては、最初にインストールしたサーバが、デフォルト サブスクリプション プロキシとなります。更新開始時刻、およびこのプロキシが更新用の CA サブスクリプション サーバを確認する頻度を設定します。追加のサーバをインストールするときには、それらの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インストールされます。追加のサーバを設定する際には、ローカル レベルで設定します。ローカル レベルでの設定は、設定するサーバの名前を選択したうえで、選択したグローバル設定よりローカル設定が優先されるように設定する、という手順で行います。

デフォルトでは、サブスクリプション クライアントの更新開始時刻はグローバル設定から継承されます。承継された設定よりローカル設定が優先されるよう手動で設定して遅延を生じさせないと、問題が生じます。この問題を防ぐために、現在はクライアントの更新スケジュールには自動的に 15 分の遅延が設定されるようになっています。よって、サブスクリプション クライアントの更新スケジュールを手動で設定する必要はなくなりました。

第 5 章: r12.1 SP1 の新機能と変更された機能

このセクションには、以下のトピックが含まれています。

FIPS 140-2 準拠の概要

FIPS（Federal Information Processing Standards: 連邦情報処理標準）140-2 は、製品が暗号化に使用すべき暗号のライブラリおよびアルゴリズムのセキュリティ標準です。FIPS 140-2 暗号化は、CA 製品のコンポーネント間、および CA 製品とサードパーティ製品間におけるすべての機密データの通信に影響を与えます。FIPS 140-2 では、機密性の高い未分類のデータを保護するセキュリティ システム内で暗号アルゴリズムを使用するための要件が指定されています。

CA Enterprise Log Manager では、FIPS モードで動作する場合に、FIPS 準拠のアルゴリズムを使用してイベント トラフィックを保護することにより、FIPS に対応しています。また、CA Enterprise Log Manager はデフォルトで FIPS 非準拠モードも提供しています。このモードでは、FIPS 準拠のアルゴリズムでイベント トラフィックが保護されません。連携ネットワーク内の CA Enterprise Log Manager サーバでは、2 つの動作モードを混在させることはできません。つまり、FIPS 非準拠モードで実行中のサーバが、FIPS モードで実行中のサーバとクエリおよびレポート データを共有することはできません。

FIPS モードの有効化および無効化に関する詳細は、「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、およびオンライン ヘルプのシステム ステータス サービスに関するセクションを参照してください。

詳細情報:

動作モード

CA Enterprise Log Manager は、FIPS モードと FIPS 非準拠モードの 2 つのモードで実行できます。暗号化の適用方法は両方のモードで同じですが、アルゴリズムは異なります。デフォルトでは、CA Enterprise Log Manager サーバは FIPS 非準拠モードで動作します。管理者ロールを持つユーザは、FIPS モードを有効にすることができます。

FIPS 非準拠モード

このモードでは、イベント転送と、CA Enterprise Log Manager と CA EEM サーバ間の他の通信(必ずしも FIPS 基準を満たしていない)において、暗号化アルゴリズムが混在します。

FIPS モード

このモードでは、イベント転送と、CA Enterprise Log Manager と CA EEM サーバ間の他の通信において、FIPS 認定された暗号化アルゴリズムを使用します。

管理者レベルのユーザは、[管理]タブの[ログ収集]サブタブで、エージェント エクスプローラ ノードからエージェント動作モードを確認できます。

FIPS モードと FIPS 非準拠モード間の切り替えの詳細については、オンライン ヘルプのシステム ステータス タスクのトピック、または「実装ガイド」のサービスの設定に関するセクションを参照してください。

暗号化ライブラリ

FIPS（Federal Information Processing Standards）140-2 は、機密性は高いが機密扱いではないデータを保護するセキュリティ システム内で暗号化アルゴリズムを使用するための要件を規定します。

CA Enterprise Log Manager ではまた、RSA の Crypto-C Micro Edition（ME）v2.1.0.2 暗号化ライブラリも組み込まれています。これは、FIPS 140-2 の暗号化モジュールのセキュリティ要件を満たしていることが確認されています。このモジュールの認証証明書番号は 865 です。

使用されるアルゴリズム

FIPS 140-2 認定の暗号化モジュールを FIPS モードで使用するコンピュータ製品は、FIPS によって承認されたセキュリティ機能のみを使用することができます。たとえば、AES（Advanced Encryption Algorithm）、SHA-1（Secure Hash Algorithm）、TLS v1.0 のような上位レベル プロトコルなどがあります。これらは、FIPS 140-2 標準および関連ガイドで明示的に許可されているものです。

FIPS 非準拠モードの場合、CA Enterprise Log Manager は以下のアルゴリズムを使用します。

- AES 128
- Triple DES（3DES）
- SHA-1
- MD5
- SSL v3

FIPS モードの場合、CA Enterprise Log Manager は以下のアルゴリズムを使用します。

- AES 128
- Triple DES（3DES）
- SHA-1
- TLS v1

CA Enterprise Log Manager は、SHA-1 をデフォルトのダイジェスト アルゴリズムとして使用して、パスワードの暗号化とサーバ リクエストの署名を行います。

CA Enterprise Log Manager で TLS v1.0 を使用するのは、外部 LDAP ディレクトリとの通信（LDAP 接続で TLS を使用している場合）、iTechnology コンポーネント間の通信、FIPS モードでのエージェントと iGateway サービスとの通信、エージェントと logDepot サービス間のイベント チャネルです。

証明書および鍵ファイル

FIPS 140-2 サポートについては、CA Enterprise Log Manager r12.1 SP1 へのアップグレードにより、既存の P12 形式の証明書が PEM 形式証明書に変換されます。この変換によって、以下のファイルが生成されます。

- 証明書ファイル（拡張子：.cer）
- 鍵ファイル（拡張子：.key）

鍵ファイルは暗号化されません。サーバおよびエージェント ホストの両方で不正なアクセスから鍵ファイルを保護することはユーザの責任で行われます。CA Enterprise Log Manager ソフト アプライアンスでは、さまざまなオペレーティング システムのハードニング技術を使用して、ファイル システムに格納された鍵および証明書を保護します。CA Enterprise Log Manager は、外部の鍵ストレージ デバイスの使用をサポートしていません。

CA Enterprise Log Manager では、以下の証明書および鍵ファイルを使用します。

証明書/鍵ファイル名	場所	説明
CAELMCert	/opt/CA/SharedComponents/iTechnology (このディレクトリは、より短い変数名 $IGW_LOC を使用して参照できます。)	すべての CA Enterprise Log Manager サービスは、CA Enterprise Log Manager サーバ間の通信、および CA Enterprise Log Manager サーバと CA EEM サーバ間の通信でこの証明書を使用します。 この証明書のエントリと、対応する鍵ファイルは、メインの環境設定ファイル CALM.cnf 内に存在します。タグのペアは、それぞれ <Certificate> および <KeyFile> で開始されます。
CAELM_AgentCert	エージェント ホスト サーバ上の $IGW_LOC	エージェントは、すべての CA Enterprise Log Manager サーバとの通信にこの証明書を使用します。CA Enterprise Log Manager 管理サーバは、この証明書をエージェントに提供します。この証明書は、指定されたアプリケーション インスタンス内のすべての CA Enterprise Log Manager サーバで有効です。
itpamcert	IT PAM サーバ	この証明書は、IT PAM との通信に使用されます。詳細については、CA IT PAM のドキュメントを参照してください。
rootcert	$IGW_LOC	この証明書は、インストール中に iGateway によって署名される自己署名ルート証明書です。
iPozDsa	$IGW_LOC	ローカルおよびリモートの両方の CA EEM サーバでこの証明書を使用します。詳細については、CA EEM のドキュメントを参照してください。

証明書/鍵ファイル名	場所	説明
iPozRouterDsa	$IGW_LOC	ローカルおよびリモートの両方の CA EEM サーバでこの証明書を使用します。詳細については、CA EEM のドキュメントを参照してください。
iTechPoz-trusted	/opt/CA/Directory/dxserver/config/ssld	CA Directory はこの証明書を使用します。
iTechPoz-<hostname>-Router	/opt/CA/Directory/dxserver/config/ssld	CA Directory はこの証明書を使用します。

FIPS サポートの制限事項

以下の CA Enterprise Log Manager 機能および製品の相互操作では、FIPS モードがサポートされません。

イベント ログ ストアへの ODBC および JDBC アクセス

CA Enterprise Log Manager 内の ODBC および JDBC は、FIPS 動作モードをサポートしない基本 SDK に依存しています。FIPS モードが必要となる連携ネットワークの管理者は、CA Enterprise Log Manager サーバごとに手動で ODBC サービスを無効にする必要があります。イベント ログ ストアへの ODBC/JDBC アクセスの無効化に関する詳細は、「実装ガイド」の該当セクションを参照してください。

CA EEM サーバの共有

CA Enterprise Log Manager r12.1 SP1 では、FIPS 対応の CA EEM r8.4 SP3 を使用しています。CA Enterprise Log Manager サーバで FIPS モードを有効にすると、共有されている CA EEM と、CA EEM r8.4 SP3 をサポートしないあらゆる製品の間で通信が無効になります。

たとえば、CA IT PAM は FIPS 対応ではありません。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。

CA Enterprise Log Manager r12.1 SP1 と CA IT PAM r2.1 SP2/SP3 の間で CA EEM サーバを共有するには、FIPS 非準拠モードでのみ共有できます。

お使いの CA IT PAM で同じ CA EEM サーバを共有していない場合、CA Enterprise Log Manager r12.1 SP1 は FIPS モードで実行できます。また、CA IT PAM と通信はできますが、それらの通信チャネルは FIPS 対応ではありません。

LDAP バインドで必要となる動作モードの一致

外部ユーザ ストアとの通信に成功するには、以下の両方の条件を満たす必要があります。

- CA Enterprise Log Manager サーバおよびその CA EEM 管理サーバは、同じ FIPS モードである必要があります。
- 接続に TLS v 1.0 を使用している場合、CA EEM サーバは、FIPS 対応の外部ユーザ ストアと同じ FIPS モードである必要があります。

  注: CA EEM サーバと外部ユーザ ストアの間で暗号化された通信を使用していない場合、または CA EEM サーバとユーザ ストアが異なる FIPS モードである場合、FIPS 対応は使用できません。

SNMP トラップ

SNMP V2 または SNMP V3 のいずれかを使用して、SNMP イベントを送信することができます。両方とも FIPS 非準拠モードでサポートされています。

SNMP トラップ送信先サーバが FIPS 対応である場合、V3 セキュリティを選択し、認証プロトコルとして SHA、暗号化プロトコルとして AES を選択する必要があります。これらの選択は、アクション アラートのスケジュール ウィザードの[宛先]ページで行います。

Microsoft Internet Explorer での CA Enterprise Log Manager への FIPS モード アクセスの設定

CA Enterprise Log Manager サーバを FIPS モードで実行する場合、ユーザ インターフェースを表示するには、ブラウザに追加の設定が必要とされる場合があります。Microsoft Internet Explorer 7 または 8 で、CA Enterprise Log Manager へのアクセスに必要なオプションを設定するには、以下の手順に従います。

注: FIPS モードで実行される CA Enterprise Log Manager サーバに Microsoft Internet Explorer 6 を使用してアクセスすることはできません。

Microsoft Internet Explorer 7 または 8 を設定する方法

1. ブラウザを開き、[ツール]-[インターネット オプション]を選択します。
2. [詳細設定]タブを選択し、[セキュリティ]セクションまでスクロールします。

3. 以下の各オプションを選択します。
   - SSL 2.0 を使用する
   - SSL 3.0 を使用する
   - TLS 1.0 を使用する
4. [OK]をクリックします。

Mozilla Firefox での CA Enterprise Log Manager への FIPS モード アクセスの設定

CA Enterprise Log Manager サーバを FIPS モードで実行する場合、ユーザ インターフェースを表示するには、ブラウザに追加の設定が必要とされる場合があります。Mozilla Firefox 3.5.8 以降のブラウザで、FIPS モードで実行される CA Enterprise Log Manager サーバへのアクセスに必要なオプションを設定するには、以下の手順に従います。

注: CA Enterprise Log Manager にアクセスするには、Adobe Flash 9 または 10 用の Mozilla Firefox プラグインをインストールする必要があります。

Mozilla Firefox を設定する方法

1. ブラウザを開き、[ツール]-[オプション]を選択します。
2. [詳細]タブ-[暗号化]サブタブをクリックします。
3. 以下の両方のオプションを選択します。
   - SSL 3.0 を使用する
   - TLS 1.0 を使用する
4. [セキュリティ]タブを選択し、[マスターパスワードを使用する]オプションを選択します。
5. [マスターパスワードを変更]をクリックします。ウィンドウが表示されたら、適切なパスワードを指定して[OK]をクリックします。
6. [詳細]タブを選択します。
7. [セキュリティ デバイス]をクリックします。

   [デバイス マネージャ]ウィンドウが表示されます。

8. 左ペインで NSS Internal PKCS#11 Module を選択します。

   選択すると、右ペインにデータがロードされます。

9. Module NSS Internal FIPS PKCS #11 Module の行を選択し、[FIPS を有効にする]をクリックします。
10. プロンプトが表示されたら、前の手順で指定したマスター パスワードを入力し、[OK]をクリックします。
11. [デバイス マネージャ]ウィンドウで[OK]をクリックします。
12. [オプション]ウィンドウで[OK]をクリックします。
13. ブラウザを再起動します。

詳細情報:

サブスクリプションによるアップグレード (P. 11)

新規インストール用の ISO イメージ

CA Enterprise Log Manager の展開、および既存の展開への新しい CA Enterprise Log Manager サーバの追加を迅速に行うため、サービス パックの ISO イメージが提供されています。ISO イメージは、Support Online の上の Downloads から利用可能です。

以下の場合は、最新の ISO イメージを使用することをお勧めします。

- CA Enterprise Log Manager を展開する場合。最新の ISO イメージからインストールすることで、適用が必要なサブスクリプション アップグレードの数を最小化し、展開をスピードアップします。
- 既存の展開においてサーバをアップグレードした後、新しい CA Enterprise Log Manager サーバを追加する場合。まず、現在の展開において、サーバおよびエージェントが正常にアップグレードされ、イベントを受信していることを確認します。次に、ISO イメージを使用して新しいサーバをインストールして、より多くの容量を追加し、かつ適用するサブスクリプション更新の数を最小化できるようにします。

注: インストール手順は変更されました。新しいプロンプトでは、FIPS モードを有効にしてインストールするかどうか尋ねられます。既存の FIPS 展開(CA Enterprise Log Manager 管理サーバまたはリモート CA EEM サーバは IPS モード)に新しい CA Enterprise Log Manager サーバを追加する場合は、インストール中に FIPS モードを有効にします。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。FIPS モードの詳細については、「実装ガイド」を参照してください。

第 6 章: 既知の問題

このセクションには、以下のトピックが含まれています。

エージェントおよび CA アダプタ

以下はエージェントおよび CA アダプタに関連する既知の問題です。

Red Hat Linux 4 にエージェントをインストールする際の必要条件

症状:

ユーザが Red Hat Enterprise Linux 4 システムに CA Enterprise Log Manager エージェントをインストールしようとすると、インストールは失敗し、必要な条件に関するエラー メッセージを表示します。

解決方法:

Red Hat Enterprise Linux 4 上の CA Enterprise Log Manager エージェントには、Legacy Software Development Package が必要です。エージェントをインストールする前に、Legacy Software Development パッケージをインストールします。

エージェント ステータス時間の精度が NTP サーバ設定に依存する

症状:

収集を実行する複数の CA Enterprise Log Manager サーバが異なるクロックに手動で設定されている場合、エージェント アクティビティに対するレポート時間に矛盾が発生する可能性があります。

解決方法:

ネットワーク内に各 CA Enterprise Log Manager をインストールする際に、NTP サーバを指定します。各サーバの NTP サーバの設定は、別のサーバによって管理されるエージェントに対してレポートされる時間と同期します。

コネクター括展開後、更新に時間がかかる

症状:

コネクター括展開後、即座に新しいコネクタがエージェント エクスプローラに表示されません。

解決方法:

コネクタおよびコネクタを展開するエージェントの数にもよりますが、すべてのコネクタがエージェント エクスプローラに更新されるには数分かかります。

コネクター括展開の IPv6 アドレスが正しくない

症状:

IPV6 フォーマットでサーバ アドレスを渡すコネクター括展開ウィザードで、コネクタの展開が予想通りに機能しません。しばらくすると、コネクタのステータスが実行中と表示されます。コネクタを編集する際、サーバ名に IPV6 アドレスの最初の 4 桁しか表示されていないことがわかります。ユーザ名、パスワードおよびドメイン フィールドは空白です。

解決方法:

現在、CA Enterprise Log Manager ユーザ インターフェースはソース ファイル コンテンツを送信する際、各ソースを区切るデリミタとして :: を使います。IPv6 アドレスにはダブル コロン文字(::)が含まれており、これが区切り文字として処理されてしまいます。コネクタ レコードは正しく保存されません。

コネクター括展開を実行する場合は、IPv6 アドレスを使わないでください。一括展開で使うコネクタの設定では、ホスト名を使うことが できます。また、新規コネクタの作成ウィザードを使えば、通常の手順で IPv6 コネクタを設定できます。

DVD マウント名にスペースを使用できない

症状:

Linux オペレーティング システムを搭載したコンピュータに製品の DVD-ROM メディアからエージェントを手動でインストールする場合、アクセス許可が拒否されたことを示すエラー メッセージが表示され、インストールが中止されます。

解決方法:

DVD メディアからエージェントをインストールするには、以下のコマンドで DVD ドライブをマウントします。

```
$ mount /dev/cdrom <local path>
```

DVD-ROM は、名前にスペースが含まれるローカル パス(ディレクトリ)にはマウントできません。スペースを含んでいないディレクトリ名に DVD-ROM をマウントし、エージェントをインストールします。

イベント ソースをドメイン レベルで正常に設定できない

症状:

任意のコネクタが Windows イベント ソースにアクセスしてそのログを読み取るように設定するには、最小限の権限を持つユーザ アカウントを作成し、それに必要な権限を割り当てる必要があります。イベント ソースが Windows Server 2003 SP1 ホストである場合、1 つの方法はローカル セキュリティ ポリシーを「認証後にクライアントを偽装」に設定することです。このユーザ権限がローカルに設定されている場合は、何ら問題は発生しません。しかし、この設定がドメイン ポリシーとしてすべてのサーバに適用されている場合、グローバルに適用されることにより、他のユーザ(管理者や SERVICE など)に対する既存のローカル割り当てが削除されることになります。

Microsoft のサポート記事には次のように記述されています。「...問題は、「認証後にクライアントを偽装」のユーザ権限を定義するグループ ポリシーがドメインにリンクされている場合に発生します。このユーザ権限は 1 つのサイトまたは組織単位(OU)のみにリンクされていなければなりません。」

解決方法:

Microsoft サポート技術情報の記事(ID 930220)に、IPSec サービスを無効にしてコンピュータを再起動することによりセキュリティ制限が適用されていない完全な TCP/IP 接続を復元するための推奨事項、および管理者と SERVICE のグループをグループ ポリシー設定として追加し直す手順が掲載されています。以下のリンク先を参照してください。

http://support.microsoft.com/kb/930220

また Microsoft では、「認証後にクライアントを偽装」設定をグループ ポリシーとして適用することによって発生する問題を解決する方法として、以下の方法も推奨しています。

- 方法 1:グループ ポリシー設定を変更する。
- 方法 2:レジストリを変更する。

Microsoft サポート技術情報の記事(ID 911801)に、推奨される 2 つの解決方法を実装する手順が掲載されています。以下のリンク先を参照してください。

http://support.microsoft.com/kb/911801

SSL 通信を有効にすると ODBC/JDBC 遅延が発生する

症状:

CA Enterprise Log Manager エージェントとサーバ間の通信が FIPS 非準拠モードである場合、SSL 通信を有効にすると ODBC/JDBC 通信が一時的に中断される場合があります。

解決方法:

ODBC または JDBC を使用している場合、SSL を有効にすると、CA Enterprise Log Manager サーバとすぐに通信できないことがあります。5 分ほど待機すると、通信が元に戻ります。

ファイル ログ センサ 4.0.0.0 統合で SUSE Linux がサポートされない

症状:

CA Enterprise Log Manager 12.1 から 12.1 SP1 に直接アップグレードした後、正しくないプラットフォーム サポート ステートメントが統合ウィザードに表示されます。ウィザードの最初の手順で、ファイル ログ センサ バージョン 4.0.0.0 を選択した場合、使用可能なプラットフォームのリストに「Linux_X86_32 SLES11」が表示されます。

解決方法:

この情報は正しくありません。SUSE Linux はファイル ログ センサ 4.0.0.0 でサポートされていません。このステートメントは無視してください。したがって、このログ センサを使用してカスタム統合を作成することはできません。

ポート設定に対する制限

症状:

Linux ホスト上で root 以外のユーザとして実行しているエージェント上で、syslog リスナがデフォルトの UDP ポートに設定されている場合、UDP ポート 514（syslog のデフォルト）はオープンにならないため、そのポート上で syslog イベントは収集されません。

解決方法:

エージェントを UNIX システム上で root 以外のユーザとして実行している場合は、syslog リスナ ポートを 1024 より大きいポート番号に変更するか、root として実行するサービスを変更します。

選択されている統合が多すぎる場合にパフォーマンスが低下する場合がある

症状:

デフォルト Syslog 統合のうちからコネクタ用に指定されたものが多すぎる合、デフォルト エージェントのパフォーマンスが低下します。この場合、パフォーマンスとは、1 秒あたりのイベント処理数（eps）を指します。

解決方法:

CA Enterprise Log Manager は、各統合について、メッセージ解析（XMP）およびデータ マッピング（DM）ファイルを読み込みます。処理の過程で、CA Enterprise Log Manager は受信イベントを正規表現のリストに照合してチェックします。ファイルの数が多いと、処理時間が長くなります。

syslog コネクタを作成する際に、不要な統合を削除することにより、パフォーマンスの低下を回避します。インストールの後、デフォルト syslog コネクタ用に設定された統合を確認し、必要でないものはすべて削除します。

連携からサーバを削除してもデフォルト エージェントは削除されない

症状:

連携サーバのグループから CA Enterprise Log Manager サーバを削除しても、削除したサーバのデフォルト エージェントは関連エージェント グループから削除されません。

解決方法:

[エージェント エクスプローラ]サブタブで、手動でグループからエージェントを削除します。

CA SAPI コレクタから集められたデータを含むレポートがイベントを正しく表示しない

症状:

CA Audit SAPI コレクタを使用して収集されたイベントは、すべてのイベント フィールドに正しく入力されるとは限りません。これにより、レポートのほとんどが想定外の方法でデータを表示します。

解決方法:

既存の CA Audit インフラストラクチャからイベントを収集する際は、CA Audit SAPI ルータを使用します。

SAPI ルータの詳細については、「実装ガイド」の「監査ユーザに関する考慮事項」セクションを参照してください。

UDP 上の syslog の送信は保証されない

症状:

保証された送信は、syslog リスナの UDP プロトコルを使った syslog の直接収集で問題になります。

解決方法:

保証された送信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。つまり、インストールされているエージェント上の syslog リスナを設定する際に、その syslog のイベント ソースも設定します。

注: エージェントを root として実行中の場合のみ、syslog の既知のポート、つまりポート 514 を使用します。エージェントを権限の低いユーザとして実行している場合(推奨)は、プライベート ポートを割り当てます。プライベート ポートは 49152 ー 65535 です。

UNIX 上の syslog サービスの競合

症状:

以下のシナリオの場合、CA Enterprise Log Manager は syslog イベントを受け取りません。

コンピュータ 1

コンピュータ 2 からの syslog イベントを待ち受ける CA Enterprise Log Manager サーバ

コンピュータ 2

syslog コネクタを含んでおり、syslog リスナを使用して、コンピュータ 1 にそのイベントを送るローカル エージェントを備えた RHEL 4.0 コンピュータ

コンピュータ 3

インストールされているコネクタを使用して、コンピュータ 2 にイベントを送る UNIX コンピュータ

この場合、OS syslog サービスおよび syslog コネクタが同じシステム上で実行されているため、エージェント コンピュータは、コンピュータ 3 からのイベントを取得することができません。

解決方法:

Computer 3 (UNIX コンピュータ)からイベントを受信するために Computer 2 の syslog サービスを停止します。また、ユーザは syslog サービスが同じコンピュータ上で競合しないように環境の構成を変えることができます。

WMI ログ センサによって複数のユーザ権限イベントが生成される

症状:

WMI ログ センサと共にコネクタを使用してイベントを収集している場合、「権限使用」に関連して複数のイベントが発生する場合があります。

解決方法:

このようなイベントは、ターゲット システム上で、正常に完了した権限使用アクションを記録するという Windows 監査ポリシーが有効になっている場合に発生します。これはイベント収集プロセスの副産物であり、発生しても何ら問題はありません。そのようなイベントが表示されることを望まない場合は、CA Enterprise Log Manager がそのようなイベントを受信しないようにする抑制ルールを作成することができます。

Solaris エージェント システム上で実行中のテキスト ファイル ログ センサがイベントの受信を停止する

症状:

Solaris エージェント システム上で実行中のテキスト ファイル ログ センサがイベントの受信を停止します。

コネクタ用のログ ファイルを確認したところ、以下のような、ライブラリ ファイル libssl.so.0.9.7 を開けないというエラーを発見しました。

```
[4] 10/07/20 18:55:50 ERROR :: [ProcessingThread::DllLoad] :Error is: ld.so.1:
caelmconnector: fatal: libssl.so.0.9.7: open failed: No such file or directory [4]
10/07/20 18:55:50 ERROR :: [ProcessingThread::run] Dll Load and Initialize failed,
stopping the connector ...
[3] 10/07/20 18:55:50 NOTIFY :: [CommandThread::run] Cmd_Buff received is START
```

解決方法:

ライブラリの場所を特定し、エージェントがイベントを受信できるようにします。

Solaris エージェント システム上のエラーを解決する方法

1. /etc フォルダに移動します。以下に例を示します。

   ```
   cd /etc
   ```

2. etc フォルダ内のプロファイル ファイルを開きます。以下に例を示します。

   ```
   vi /etc/profile
   ```

3. プロファイル ファイルの最後に、以下の 2 行を追加します。

   ```
   LD_LIBRARY_PATH=/usr/sfw/lib:$LD_LIBRARY_PATH
   ```

   ```
   export LD_LIBRARY_PATH
   ```

4. Solaris エージェント システムの現在のセッションを閉じます。
5. Solaris エージェント システムの新しいセッションを開始します。
6. Solaris システムの CA Enterprise Log Manager エージェントを停止します。以下に例を示します。

   ```
   /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

7. Solaris システムの CA Enterprise Log Manager エージェントを開始します。以下に例を示します。

   ```
   /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   テキスト ファイル ログ センサはイベントの受信を開始し、ログ ファイルにエラーが表示されなくなります。

非常に高いイベント フローによってエージェントが無応答になる

症状:

CA Enterprise Log Manager エージェントが無応答になり、イベント受信を停止します。以下のエラー メッセージが caelmdispatcher.log ファイルに表示されます。

```
[275] 10/07/12 14:32:05 ERROR :: FileQueue::PutEvents Unable to write to new event file
[275] 10/07/12 14:32:05 ERROR :: WriterThread::run Unable to push events to FileQueue, Retrying
[275] 10/07/12 14:32:10 NOTIFY :: FileQueue::UpdateCurrentWriterFile Reached Max files configured limit=10, Not creating any new files for now
```

解決方法:

これは、環境内のハードウェアに関するイベント受信レートが非常に高いことを示しています。この問題を解決するには、以下の手順に従ってエージェントを再設定します。

1. [管理]をクリックし、[ログ収集]サブタブをクリックして、エージェント エクスプローラ フォルダを展開します。
2. 再設定するエージェントを選択して[編集]ををクリックし、以下のパラメータを変更します。

   ファイルの最大数

   イベント受信ファイル キューに作成できるファイルの最大数を設定します。上限は 1000 ファイルです。デフォルト値は 10 です。

   1 ファイルあたりの最大サイズ

   イベント受信ファイル キュー内の各ファイルの最大サイズを MB 単位で設定します。ファイルが最大サイズに達すると、CA Enterprise Log Manager は新しいファイルを作成します。サイズの上限は 2048 MB です。デフォルト値は 100 MB です。

   現在の環境および秒あたりのイベント レートに基づいて、これらのパラメータ値を大きくします。

アプライアンス(UI 以外)

以下は、ソフトウェア アプライアンス(CA Enterprise Log Manager ユーザ インターフェースではない)に関連する既知の問題です。

EiamAdmin というユーザ名で CA Enterprise Log Manager サーバにログインできない

症状:

(ユーザ インターフェースからではなく)CA Enterprise Log Manager サーバにログインしようとすると、EiamAdmin というユーザ名およびパスワードは認識されません。

解決方法:

アーカイブの設定など、メンテナンス関連のタスクを実行するために、インストール時に別のユーザ名(caelmadmin)が作成され、インストーラが EiamAdmin に指定したのと同じパスワードが割り当てられています。CA Enterprise Log Manager サーバにログインするには caelmadmin というユーザ名とパスワードを使用します。

詳細については、「実装ガイド」の「デフォルトのユーザ アカウント」を参照してください。

ELM のアダプタログ ファイルの数が多すぎる

症状:

CA Enterprise Log Manager サーバ上に、大量のアダプタ ログ ファイルが生成される場合があります。ログ メッセージは通常、単一のログ ファイル内に追加されていくため、このような状態は異例です。この問題は、追跡を有効にすることにより発生する場合があります。

この問題が存在するかどうかを判定するには、以下の手順に従います。

1. レポートとアラートをスケジュールし、以下のような ODBC クエリを実行します。

   ```
   select event_logname,count(*) from view_event where event_time_gmt >=
   timestampadd(hh,-1,now()) AND event_time_gmt <= now() group by event_logname;
   ```

2. SSH を使用して CA Enterprise Log Manager サーバにログインし、caelmadmin のユーザ名とパスワードを指定します。
3. root に対して SU を実行し、パスワードを指定します。
4. iTechnology フォルダに移動します。

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

5. ODBC ドライバを通じてクエリを実行することにより過剰な数のログ ファイルが作成されたかどうかを判定します。これらのファイルには ELMAdapter_<oaserverpid>_-IP.log という名前が付けられます。

解決方法:

この問題が存在する場合は、以下の手順でエラー追跡が無効となるようにします。

1. SSH を使用して管理 CA Enterprise Log Manager サーバにログインし、caelmadmin のユーザ名とパスワードを指定します。
2. root に対して SU を実行し、パスワードを指定します。
3. iTechnology フォルダに移動します。

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ```

4. oaserver-dm.ini を開いて編集します。
5. [Service_0]までスクロールし、追跡が無効に設定されていることを確認します。無効になっていない場合は、以下の例のように変更します。

   ```
   ServiceDebugLogLevel=0
   ServiceIPLogOption=Disable All Tracing
   ```

6. 以下の手順で ODBC サービスを再起動します。
   a. [管理]タブ-[サービス]サブタブを選択します。
   b. [ODBC サーバ]をクリックします。
   c. 以下のいずれかの操作を実行します。
      - [サービスの有効化]が選択されていない場合は、[サービスの有効化]を選択し、[保存]をクリックします。
      - [サービスの有効化]が選択されている場合は、1 度[サービスの有効化]チェック ボックスをオフにし、[保存]をクリックしたうえで、再度[サービスの有効化]を選択し、[保存]をクリックします。

解析ファイルの手動インポートにタイムアウト値変更が必要となる場合

CA Enterprise Log Manager のインストール時、解析(.XMP)ファイルのインポート中に問題が発生する場合があります。この問題が最も発生しやすいのは、最小ハードウェア要件を満たさないサーバ上に、または遅いネットワーク内で CA Enterprise Log Manager をインストールしようとしている場合です。

症状:

インストール時、解析ファイルのインポート中にエラーが発生します。この問題はインストール完了後に解決できる場合があります。提供されたスクリプト *EEM/content/ImportCALMXMP.sh* を実行して、ファイルを手動でインポートします。(このスクリプトに関する詳細は、「実装ガイド」に掲載されています。)この操作を実行すると、通常エラーは解決されます。

ただし、CiscoRouter の XMP ファイルは、手動インポート スクリプトを実行しても正常にインポートされない場合があります。CA Enterprise Log Manager サーバのインストールは正常に完了しています。しかし、XMP インポートが失敗したことにより、デフォルトのコネクタがローカル エージェントに正常にインストールされなくなります。手動での XMP ファイルのインポートが正常に完了するまで、コネクタを展開することができなくなります。

解決方法:

EEMImportUtility.sh スクリプトでデフォルト タイムアウト値を上回ると、Cisco XMP ファイルのインポートに問題が発生します。*ImportCALMXMP.sh* スクリプトは *EEMImportUtility.sh* スクリプトを呼び出します。デフォルトのタイムアウト値は 4 分です。遅いサーバ上で手動インポートを行う場合でも十分な時間が確保されるように、デフォルト タイムアウトを 6 分に設定します。

デフォルト タイムアウト値を変更するには、以下の手順に従います。

1. /EEM/content ディレクトリに移動します。
2. ImportCALMXMP.sh ファイルを編集します。
3. 以下の行を見つけて、タイムアウト値を以下のように変更します。

   ```
   ./EEMImportUtility.sh -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP" to "./EEMImportUtility.sh -timeout 360000 -h simdemo01 -u EiamAdmin -m FgAMCQQJAllf -a CAELM -type xmp -l XMP
   ```

   注:タイムアウト値はミリ秒で表します。
4. ファイルを保存して閉じます。
5. 再びスクリプトを実行します。
6. デフォルト エージェント上で syslog 用および Linux_LocalSyslog 用のコネクタを手動で展開します。

イベント精製

以下はイベント精製に関連する既知の問題です。

文字列および数値のブロック マッピングでの異なる演算子の使用

症状:

マッピング ウィザードを使用する場合、数値またはテキスト文字列のブロック マッピング値は想定どおりの結果を返しません。

解決方法:

ブロック マッピングを作成する場合、「等しい」という演算子は数値列でのみ使用できます。すべてのテキスト文字列の列に「一致」演算子を使用します。

カスタム DM で epSIM（iTech）イベントをマップできない

症状：

epSIM（iTechnology）イベント用に作成されたカスタム データ マッピング（DM）ファイルでは、ログ収集エクスプローラの CA Adapter の下で iTechnology EventPlugin に適用された後、イベントをマップできません。

iTech イベントがカスタム DM ファイルに基づいてマップされたかどうかを判断するために「システム全イベント」クエリを確認すると、iTech イベントがマップされておらず、クエリ結果として返されていないことがわかります。「マップされたイベントはありません。イベントをマップできません。」という内容のメッセージが表示されます。

解決方法：

カスタム DM ファイルを開き、$EventLog を $Log に置き換えます。たとえば、以下のようにします。

次の行を変更：<DM_Field name="event_logname" type="string" value="$EventLog" mapping="direct"/>

変更後：<DM_Field name="event_logname" type="string" value="$Log" mapping="direct"/>

この変更により、イベントがマップされるようになります。 その後、マッピングの分析中に「マップされたイベントはありません」という内容のメッセージが表示されても無視します。

クエリおよびレポート

以下はクエリおよびレポートに関連する既知の問題です。

アクション アラートのクエリ結果が不完全な場合がある

症状:

アクション アラートが生成された場合、クエリ結果をすぐに CA Enterprise Log Manager で表示することができます。CA Enterprise Log Manager で結果を表示するには、[アラート管理]タブ-[アクション アラート]サブタブをクリックし、アラートの名前を選択します。結果がグラフ形式で表示されます。アクション アラートによって、CA Service Desk でヘルプ デスク チケットを発行する CA IT PAM イベント/アラート出力プロセスが起動された場合、ヘルプ デスクの問題として URL が表示されます。この URL にアクセスしてログインすると、アラートのクエリ結果が単一のページに表示されます。これらの結果を[アクション アラート]サブタブに表示された結果と比較したときに、クエリ結果が一致しないことに気づく場合があります。 たとえば、数についての結果が表示されている場合、アクセスした URL で表示されている数が CA Enterprise Log Manager で表示された数より大きい場合があります。この問題は、システムに高い負荷がかかっている場合において、アラートの[結果の条件]に設定されている動的終了時間が不適当であるときに、発生することがあります。不適当とは、データベースの読み取りが行われる前にデータベースの更新を実行する時間が十分に確保されていない、ということです。 この問題が発生する可能性は、[動的終了時間]のデフォルト値が、[過去 5 分間]となっている[事前定義済み範囲]について、[今すぐ]、[-2 分]に設定されるようになったことにより緩和されました。

解決方法:

アクション アラートの[結果の条件]手順で[動的終了時間]を、[今すぐ]、[-2 分]から、より長い時間が確保される値、たとえば[今すぐ]、[-10 分]に変更します。

複数検索語のクエリに対する制限

症状:

1 つの検索列に対するクエリを実行すると、大文字と小文字を区別して、問題なく検索が行われます。ただし、複数の検索列に対するクエリを実行すると、ワイルドカードとして解釈されるべきアスタリスク(*)が文字どおりに解釈され、大文字と小文字を区別して検索が実行されます。この問題は、内部で生成された SQL コードの where 句に OR 演算子が含まれている場合に発生します。

解決方法:

プロンプトを使用する場合は、クエリを一度に 1 列の検索に制限します。 複数の式を使って独自にクエリを作成する場合、複数の LIKE ワイルドカード式は、論理演算子の AND で結合します。

クエリ ウィザードの単純フィルタに特殊文字を使用すると正常に機能しない

症状:

クエリ ウィザードの単純フィルタで、単純フィルタのフィールド値の一部として特殊文字を入力すると、フィルタが正常に機能しません。以下の特殊文字を入力しても、クエリを保存したり実行したりすることは可能です。

(ページ) & * > < ? : } {

しかし、クエリはそのフィールドをフィルタとして使用せずに実行され、条件に一致しない場合でもデータが表示されます。

解決方法:

単純フィルタのフィールド値の一部として上記の特殊文字を使用しないようにします。

アップグレードの後にスケジュール済みジョブのステータスが表示されない

症状:

[スケジュール済みレポート]タブ、[レポートのスケジュール]サブタブでは、すべてのスケジュール済みのジョブとそのステータスを表示できます。[ステータス]列には、レポート生成プロセス中は[生成中]と表示され、ジョブがスケジュールされると[スケジュール済み]と表示されます。基本の r12.0 GA バージョンからのアップグレード後、レポートの[ステータス]列は、スタータスに関係なくクリアされます。スケジュール済みレポートが再生成されると、ステータスは再度表示されます。

解決方法:

スケジュール済みジョブの[ステータス]列の値の省略は、一時的な表示の問題です。処置を行う必要はありません。次回のレポート生成時に、正しいステータスが表示されます。

頻繁にスケジュールされた一部のアクション アラート ジョブが失敗する

症状:

指定された間隔内に生成されたイベントを照会するアクション アラートが、その間隔より頻繁に実行されるようスケジュールされている場合、重複するジョブは失敗します。その場合、「前のクエリが進行中であるためアラートを生成できませんでした」という内容のメッセージが表示されます。 たとえば、過去 3 時間以内に生成された特定のイベントを照会する場合に、毎時間実行されるクエリを設定すると、最初のジョブが完了する前に次のジョブが開始されることになります。この場合、CA Enterprise Log Manager では最初にスケジュールされたジョブの処理を続行し、2 番目にスケジュールされたジョブには失敗メッセージを送信します。3 時間が経過するとすぐに、クエリ基準を満たすイベントが発生した場合はアラートが送信され、このアラートの次の実行が開始されます。

解決方法:

[結果の条件]で、[日付の範囲選択]のみを指定した場合、[日付の範囲選択]に設定したのと同じ間隔を繰り返しの間隔として選択します。たとえば、過去 3 時間以内に生成された特定の基準を満たすイベントを照会する場合、[結果の条件]で以下のように[日付の範囲選択]を設定します:

動的終了時刻: 'now' '-2 minutes'

動的開始時刻: 'now' '-182 minutes'

スケジュールを定義する際は、ジョブのスケジュールの手順で、繰り返しの間隔に以下のように 3 時間(180 分)を設定します。

繰り返しの間隔: 3 時間

同じクエリ間隔および繰り返し間隔を設定することによって、クエリ基準を満たすイベントの発生すべてが、生成されるアラートに記録されるようになります。グループ化されたイベント用に間隔を指定する場合、この推奨事項は当てはまりません。

特殊文字を含むタグを削除できない

症状:

以下の特殊文字を含むクエリまたはレポートのタグを削除しようとしても、削除できません。~ ! @ # $ % ^ & * (ページ) _ + { } | : " < > ?

解決方法:

クエリやレポートのタグを作成する場合は、上記の特殊文字を使用しないようにします。

サブスクリプション

以下の既知の問題は、サブスクリプションに関するものです。

OS 更新後、SP のアップグレード時に自動的に再起動する

症状:

サブスクリプション オプション[OS 更新後に自動再起動]が[はい]に設定されている場合、サービス パックの更新を適用すると、オペレーティング システムが CA Enterprise Log Manager バイナリの更新が完了する前に再起動します。そのため、iGateway シャットダウン スクリプトの更新を完了できません。オペレーティング システムの再起動時に iGateway が正常にシャットダウンされるようにするため、この更新を適用する必要があります。

解決方法:

サービス パックの Log Manager モジュールの更新を適用する前に、[OS 更新後に自動再起動]サブスクリプション オプションを[いいえ]に設定します。

メモリ容量の少ないマシンでのメモリ不足エラー

症状:

推奨する 8 GB よりもメモリ搭載量が少ないコンピュータにサブスクリプション更新をダウンロードすると、メモリ不足による Java のエラーが発生し、ダウンロードに失敗します。Java Virtual Machine (JVM) のヒープ サイズを設定していないときに、大容量のパッケージが iGateway を使用してダウンロードされています。

解決方法:

推奨される 8 GB よりも少ないメモリを備えたハードウェアに CA Enterprise Log Manager をインストールする場合は、caelm-java.group ファイルを編集して JVM ヒープ サイズ設定を変更します。

JVM ヒープ サイズ設定を変更する方法

1. caelmadmin として CA Enterprise Log Manager サーバにログオンします。
2. iGateway フォルダに移動します。
3. caelm-java.group ファイルを開いて JVM 設定セクションを確認します。
4. 以下の太字に示されるように、新しい行を追加します。

```
<JVMSettings>
                <loadjvm>true</loadjvm>
                <javahome>/usr/java/latest/jre</javahome>
                <Properties
name="java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed">

<system-properties>java.endorsed.dirs=/opt/CA/SharedComponents/iTechnology/endorsed</system-properties>
                </Properties>
        <Properties
name="maxmemory"><jvm-property>-Xmx1250M</jvm-property></Properties>
        </JVMSettings>
```

5. caelm-java.group ファイルを保存して閉じます。

重要: 大きなデータ セットで[PDF にエクスポート]オプションを使用する場合、JVM ヒープ サイズの設定が原因で問題が生じることがあります。そのため、このオプションは低スペックのコンピュータでのみ使用するようにしてください。

プロキシ認証情報の変更によりドメイン アカウント ロックアウトが生じる

症状:

ドメインの認証情報が機能せず、ある環境の CA Enterprise Log Manager サーバでアカウントがロックされます。

解決方法:

CA Enterprise Log Manager サーバは、CA サブスクリプション サーバを定期的に問い合わせて製品の更新を確認します。プロキシの認証情報(ユーザ ID とパスワードなど)が期限切れになっているか、変更されている場合、CA Enterprise Log Manager はサブスクリプション サーバに問い合わせられないため、失敗したログインについて自己監視イベントを生成します。自己監視イベントは以下のようなメッセージを表示します。

サブスクリプション コンテンツ サーバに接続できませんでした。 サーバは停止しているか、接続が拒否されたか、プロキシ サーバの設定が間違っています。 プロキシ サーバの設定を確認してください。

失敗したログインがそのまま許可される場合、ドメイン アカウントはローカル ポリシーによってはロックされる場合があります。プロキシの認証情報が変更されていないこと、または期限が切れていないことを確認します。

サブスクリプション サーバへの問い合わせに使用するサーバ アカウントには、パスワードの有効期限ポリシーを設定しないようにしてください。

1 回だけ表示される再起動を求める自己監視イベント

症状:

サブスクリプションを通じてオペレーティング システム モジュールをダウンロードするよう選択し、再起動オプションなしでインストールするように指定すると、自己監視イベントが 1 回だけ生成されます。対象のホストには OS の更新がインストールされており、更新を有効にするにはマシンを再起動する必要があることを示すメッセージが表示されます。

解決方法:

サブスクリプションは、手動による再起動が必要な場合にオペレーティング システムの再起動を促すイベントを 1 回のみ生成します。このイベント用のアラートを作成しておくことをお勧めします。

アップグレード実行後、サブスクリプション モジュールを再度選択する必要がある

症状:

CA Enterprise Log Manager を r12.1 にアップグレードすると、以前選択したサブスクリプション モジュールは、インターフェース上の[選択済み]リストから削除され[使用可能]リストに移動します。そのため、アップグレード後にこれらのモジュールに対してサブスクリプションの更新を実行できません。

解決方法:

アップグレードした後、以下の手順に従って必要なモジュールを再度選択してください。

サブスクリプション モジュールを再度選択する方法

1. CA Enterprise Log Manager にログインし、[管理]タブをクリックした後、[サービス]サブタブをクリックします。
2. 更新対象とする各サーバの サブスクリプション モジュールを開きます。
3. [サブスクリプション]シャトル コントロールを使用し、更新に使用するモジュールを[使用可能]リストから[選択済み]リストに移動します。
4. [保存]をクリックします。

設定変更後に[プロキシのテスト ボタン]で誤検出が発生する

症状:

テストが成功した後に CA Enterprise Log Manager プロキシ サーバの設定を変更し、その後再び[プロキシのテスト]ボタンを使用してテストを実行すると、新しい設定が正しくても正しくなくても、確認メッセージが表示されます。

解決方法:

[プロキシのテスト]ボタンは、指定されたプロキシ設定を使用して、そのプロキシを経由して URL にアクセスします。プロキシ サーバは通常、クライアント認証が有効である場合にはこれをキャッシュし、一定の時間が経過するまでは以後の認証情報を無視します。

つまり、一旦[プロキシのテスト]ボタンによって設定が有効であることが正しく示されると、以後一定期間は、不適切な設定をチェックしても有効なものとして不正確に表示されることになります。

2 つの抑制ルールが正常に適用されない

症状:

以下の 2 つの抑制ルールは r12.0 の一部ですが、正常に適用されません。

- TMCM - ウイルス シグネチャ & ウイルス エンジン更新成功メッセージ
- McAfee ウイルス シグネチャ & ウイルス エンジン更新成功メッセージ

解決方法:

これらのルールは、タイトルにアンパサンド(&)が含まれているため、正常に適用されません。r12.1 アップグレードには、これらを置換する以下のルールが含まれています。

- TMCM - ウイルス シグネチャおよびウイルス エンジン更新成功メッセージ
- McAfee ウイルス シグネチャおよびウイルス エンジン更新成功メッセージ

アンパサンドを含む古いバージョンの代わりに、これらのルールを使用してください。

r12.1 へのアップグレードでは iGateway の再起動が必要

症状:

連携環境で r12.0 から r12.1 へのアップグレードを完了するには、iGateway を再起動する必要があります。

解決方法:

サブスクリプション クライアントは、アップグレード バイナリをコピーして抽出しますが、インストールは行いません。つまり、アップグレード バイナリは「/tmp/downloads」ディレクトリにそのまま残っています。これは、サブスクリプション アップグレード プロセスが完了していないことを示します。現時点では、以下のプロセスを使用して手動で iGateway を再起動する必要があります。

iGateway デーモンまたはサービスを再起動する方法

1. CA Enterprise Log Manager サーバの caelmadmin ユーザとしてログインします。
2. 以下コマンドでユーザを 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
   ```

4. 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
   ```

これにより、アップグレードを完了できます。

r12.1 SP1 へのアップグレードで iGateway の再起動が必要になる場合がある

症状:

r12.1 から r12.1 SP1 へのアップグレードが適切な方法で完了しないことがあります。サブスクリプション プロセスの完了までに 1 時間半以上かかった場合、iGateway の再起動が必要となる場合があります。

解決方法:

この問題を特定するには、以下の手順に従うことをお勧めします。

1. 12.1 GA からコンテンツのサブスクリプション(レポートと統合)を完了します。
2. SP1 へのバイナリのサブスクリプション(サーバ、エージェント、OS モジュール)を完了します。

これにより、各モジュールのダウンロードにかかった時間を区別することができます。モジュールのサイズに応じて時間は変わります。サブスクリプションの部分が完了までにあまりにも長くかかる場合は、CA Enterprise Log Manager ユーザインターフェースから iGateway を再起動します。

iGateway サービスを再起動する方法

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. [システム ステータス]エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
4. サービスの[管理]タブをクリックします。
5. [iGateway の再起動]をクリックします。

r12.1 SP1 で更新された syslog ログ センサにより Windows エージェント上の統合の更新が必要となる

症状:

r12.1 SP1 にアップグレードする際に、統合モジュール更新を適用しなかった場合、syslog ログ センサを使用するすべてのコネクタが機能しなくなります。エージェント ログ ファイルには以下のようなエラーが示されます。

```
[6072] 10/03/09 17:22:51 ERROR :: MySAX2Handler::fatalError: at line1
[6072] 10/03/09 17:22:51 ERROR :: XMLTree::ParseUsingSAX2:error parsing
stringintruvert/jsp/admin/Login.jsp
[6072] 10/03/09 17:22:51 ERROR :: XMLTree::Parse Exit ParseUsingSAX2 FAILURE
[6072] 10/03/09 17:22:51 ERROR :: HTTP_Processor::ParseRequestXML: Unknown request
format:intruvert/jsp/admin/Login.jsp
```

さらに、統合のバージョンを確認します。12.1.5104.0 より前である場合、アップグレードを適用する必要があります。

解決方法:

統合モジュール更新を適用し、次に、syslog ログ センサを使用する各統合をバージョン 12.1.5104.0 以降へアップグレードします。または、「管理ガイド」の「複数コネクタの設定の更新」の手順に従います。

syslog ログ センサを使用する統合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。

ユーザとアクセスの管理

以下はユーザとアクセスの管理に関連する既知の問題です。

Windows Vista でのブラウザからのアクセスの制限

症状:

IPv6 に対応した Windows Vista SP1 オペレーティング システムのコンピュータから CA Enterprise Log Manager にログオンする場合、[管理]タブ、[ユーザとアクセスの管理]サブタブ上のボタン機能にアクセスできません。

EiamAdmin 認証情報または Administrator ロールに割り当てられている CA Enterprise Log Manager ユーザ アカウントの認証情報でログインするユーザは、この機能にアクセスできる必要があります。この制限は、他の Windows オペレーティング システムから CA Enterprise Log Manager を参照するユーザには当てはまりません。Windows Vista コンピュータから https://[*ipv6-address*]:5250/spin/calm 形式の URL で CA Enterprise Log Manager を参照する場合のみ当てはまります。この URL の例を以下に示します。

```
https://[::FFFF:192.168.00.00]:5250/spin/eiam
```

解決方法:

この問題の回避策は、別の URL を使って[ユーザとアクセスの管理]機能にアクセスします。

1. ブラウザから次の URL を入力します。この URL は CA Enterprise Log Manager 管理サーバへの IPv6 アドレスです。

   ```
   https://[ipv6-address]:5250/spin/eiam
   ```

2. [アプリケーション]ドロップダウン リストから[CAELM]を選択します。
3. [ユーザ名]および[パスワード]フィールドに、EiamAdmin とこのアカウントのパスワード、または 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。
4. ユーザとグループを設定するには、[ID の管理]タブをクリックします。
5. テストまたはカレンダを設定するには、[アクセス ポリシーの管理]タブをクリックします。
6. グローバル ユーザ、グローバル グループ、またはパスワード ポリシーを設定するには、[設定]タブで EEM サーバを選択します。

アクセス ポリシーによるカレンダ使用に対する制限

症状:

明示的にアクセスを許可するポリシーを使って、カレンダ上の指定した日時に CA Enterprise Log Manager へのユーザのアクセス、またはグループのアクセスを制限できます。ただし、明示的にアクセスを拒否するポリシーでは期待どおりにカレンダが機能しません。

解決方法:

明示的な否認ポリシーではなく、明示的にアクセスを許可するタイプのポリシーで、グループにアクセス権を付与する時間を制限してください。

その他

以下はその他の既知の問題です。

CA Enterprise Log Manager が応答しないときがある

症状:

CA Enterprise Log Manager は応答しなくなることがあります。つまり、ユーザ インターフェースがユーザのリクエストに応答せず、エージェントからエージェント マネージャへの内部リクエストが停止します。ただし、ログ収集は継続します。

解決方法:

iGateway プロセスを停止して再起動するには、以下の手順に従います。

1. ssh を使用して、caelmadmin ユーザとして応答していない CA Enterprise Log Manager サーバにログオンします。
2. 以下のコマンドで root パスワードを指定して、ユーザを root アカウントに切り替えます。

   ```
   su -
   ```

3. $IGW_LOC ディレクトリに移動します。

   デフォルトで iGateway は、/opt/CA/SharedComponents/iTechnology ディレクトリに存在します。

4. 以下のコマンドで iGateway プロセスを停止します。

   ```
   ./S99igateway stop
   ```

5. 以下のコマンドで iGateway プロセスを開始します。

   ```
   ./S99igateway start
   ```

API クエリおよびレポートのコールが特定のブラウザで失敗する

症状:

Microsoft Internet Explorer 7 または 8、Mozilla Firefox 上で、オープン API getQueryViewer または getReportViewer コールを使用すると、結果が表示されません。

解決方法:

指定されたブラウザで、CA Enterprise Log Manager API は、API コール URL 内の "server" パラメータを認識できません。この問題を回避するには、getQueryViewer または getReportViewer のコールでサーバ パラメータを指定しません。CA Enterprise Log Manager インターフェースが表示されたら、メインページの最上部にある[ログ マネージャ サーバ]ドロップダウン リストから対象のサーバを選択します。

API コール URL の詳細については、「CA Enterprise Log Manager API プログラミング ガイド」を参照してください。

CAELM4Audit のサポート廃止

CA Enterprise Log Manager r12.1 SP1 では、CA Audit との使用が認定されていない CA EEM r8.4 SP3 を使用します。CA Enterprise Log Manager と CA Audit との統合では CA EEM サーバを共有することが必要とされるため、CA Audit は、サポートされていない環境設定で実行されることになります。

さらに、CA Audit は FIPS 対応ではないため、CA Enterprise Log Manager を FIPS モードに切り替えると、Audit 管理者ユーザ インターフェースが機能しなくなります。

アーカイブ クエリに対するカスタム アプリケーション名の影響

症状:

複数の CA Enterprise Log Manager サーバが同じ管理サーバを使っている環境では、通常、アーカイブ クエリはすべてのサーバのアーカイブ ディレクトリから結果を返します。 ただし、管理用の CA Enterprise Log Manager をインストールしたときにデフォルトの CAELM ではなくカスタム アプリケーション名を設定した場合は、アーカイブ クエリが予期したように機能しません。 つまり、アーカイブ クエリは、クエリを実行したサーバのみの結果を返します。その他のサーバからの結果には *<host>User CERT-custom: Access is denied* と表示されます。

解決方法:

アーカイブ カタログに対して各 CA Enterprise Log Manager から別々にクエリを実行します。

モニタ用のハイコントラスト設定

症状:

Windows でサポートされているハイコントラスト設定は、[ハイコントラスト 黒]のみです。他の 3 つのハイコントラスト オプションはサポートされていません。ハイコントラスト オプションには、[ハイコントラスト #1]、[ハイコントラスト #2]、[ハイコントラスト 黒]、[ハイコントラスト 白]があります。

解決方法:

ハイコントラスト設定が必要な場合は、[ハイコントラスト 黒]設定を選択します。このオプションを設定するためには、[コントロール パネル]で[画面]を選択します。このユーザ補助オプションは、[画面のプロパティ]ダイアログの[デザイン]タブにある[配色]ドロップダウン リストで設定します。

iGateway の継続的な停止と再起動

症状:

CA Enterprise Log Manager インターフェースは、操作中、まれに応答を停止します。CA Enterprise Log Manager サーバを確認すると、iGateway プロセスが停止して再起動した後、起動に失敗していることがわかります。iGateway プロセスを確認するには、以下のプロセスに従います。

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. 以下コマンドでユーザを root アカウントに切り替えます。

   ```
   su - root
   ```

4. 以下のコマンドで、iGateway プロセスが実行中であることを確認します。

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

   オペレーティング システムは iGateway プロセス情報、および iGateway の下で実行中のプロセスのリストを返します。

解決方法:

以下の回避策を使って、問題を解決します。

1. $IGW_LOC（/opt/CA/SharedComponents/iTechnology）に移動し、次のファイルを探します。

   ```
   saf_epSIM.*
   ```

   saf_epSIM.1、saf_epSIM.2、saf_epSIM.3 など、連続番号の付いた同じ名前のファイルが複数存在します。

2. 一番小さい番号が付いたファイルの名前を変更し、CA サポートに送信できるように別の場所に保存します。
3. iGateway が自動的に再起動しない場合は、再起動します。
   a. root ユーザとしてログインします。
   b. コマンド プロンプトを起動し、以下のコマンドを入力します。

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

仮想 CA Enterprise Log Manager 用の最大ディスク容量が小さすぎる

症状:

VMware ESX Server v3.5 では、512 GB のディスク容量を割り当てた仮想マシンを作成できない 仮想 CA Enterprise Log Manager サーバでは、イベント ボリュームの処理に 256 GB よりも多くの容量を必要とします。

解決方法:

VMWare ESX Server は、1 MB のデフォルト ブロック サイズを使用し、この値を使用して、最大のディスク容量を計算します。ブロック サイズが 1 MB に設定されている場合、最大のディスク容量はデフォルトで 256 GB になります。256 GB を超える仮想ディスク容量を設定する場合、デフォルトのブロック サイズを増やすことができます。

より大きな仮想ディスクを作成する方法

1. VMware ESX Server 上のサービス コンソールにアクセスします。
2. 以下コマンドでブロック サイズを 2 MB に増やします。

   ```
   vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   このコマンドで、値 2M は 512 GB(2 × 256)を意味します。
3. VMware ESX サーバを再起動します。
4. ディスク容量を 512 GB に設定して新しい仮想マシンを作成します。

このコマンドおよびその他のコマンドの詳細については、VMware ESX Server のマニュアルを参照してください。

ブラウザをリフレッシュするとユーザが CA Enterprise Log Manager からログアウトする

症状:

CA Enterprise Log Manager にログインしているときにブラウザをリフレッシュすると、セッションが終了して、ユーザがログアウトさせられます。

解決方法:

CA Enterprise Log Manager は、Flex 制限のためにブラウザのリフレッシュをサポートしていません。ブラウザのリフレッシュは避けてください。

iGateway の再起動後にサービスまたはエクスプローラ インターフェースのエラーが発生する場合がある

症状:

iGateway を再起動した直後に CA Enterprise Log Manager インターフェースのサービスまたはエクスプローラ ツリーでオブジェクトをクリックすると、要求したコンテンツの代わりに、「ネットワーク エラーを受信しました」というエラー メッセージが表示されることがあります。

解決方法:

このエラーが発生するのは、iGateway の再起動後に、まだ再ロード中であるオブジェクトを指定してアクセスしようとしたことが原因です。再ロードが完了するまで 5 分ほど待機してから、サービスまたはエクスプローラのアイテムをクリックしてください。

IE 以外のブラウザを使用すると、アップロードおよびインポートが失敗する

症状:

Mozilla Firefox、Safari あるいは Chrome を使用して CA Enterprise Log Manager を参照する場合、CA Enterprise Log Manager のほとんどのタスクを正常に実行することができます。ただし、これらのブラウザのいずれかを使用する場合、タスクのアップロードまたはインポートに失敗します。以下に例を示します。

- クエリ定義のインポートに失敗し、「IO エラー：リクエスト失敗」メッセージが表示される。
- コネクター括展開ウィザードを使用して CSV ファイルをアップロードすると、「ファイルをアップロードしています。」というメッセージが表示されるが、アップロードに失敗する。

解決方法:

ファイルのアップロードまたはインポートを実行する場合、Microsoft Internet Explorer を使用して CA Enterprise Log Manager を参照してください。

リモート EEM を使用したインストールにおいてユーザ インターフェースが予期しない理由で適切に表示されない

症状:

リモート EEM サーバ CA Enterprise Log Manager をインストールする場合、初期ログインでユーザ インターフェースが正常に表示されないことがあります。iGateway ログ ファイルを参照すると、agentmanager、calmreporter、subscclient および subscproxy サービスが開始されていないことを確認できます。

ログ ファイルに以下の構文に類似するメッセージが記録されていることを確認できます。

[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12 が失敗しました [エラーコード : -1]

[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12 が失敗しました [エラーコード : -1]

[1087523728] 09/23/09 20:35:32 ERROR :: Certificate::loadp12 : etpki_file_to_p12 が失敗しました [エラーコード : -1]

[1087527824] 09/23/09 17:00:07 ERROR :: OutProcessSponsorManager::stopSponsorGroup : SponsorGroup の safetynet プロセスが終了しました [caelm-msgbroker] が終了呼び出しに対して許可の応答をしません

[1087527824] 09/23/09 17:00:07 ERROR :: OutProcessSponsorManager::stopSponsorGroup : SponsorGroup の safetynet プロセスが終了しました [caelm-oaserver] が終了呼び出しに対して許可の応答をしません

[1087527824] 09/23/09 17:00:07 ERROR :: OutProcessSponsorManager::stopSponsorGroup : SponsorGroup の safetynet プロセスが終了しました [caelm-sapicollector] が終了呼び出しに対して許可の応答をしません

[1087527824] 09/23/09 17:07:46 ERROR :: OutProcessSponsorManager::start : SponsorGroup [caelm-java] の開始に失敗しました]

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [agentmanager] がロードに失敗しました

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [calmreporter] がロードに失敗しました

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [subscclient] がロードに失敗しました

[1087527824] 09/23/09 17:07:49 ERROR :: SponsorManager::start : Sponsor [subscproxy] がロードに失敗しました

解決方法:

iGateway を再起動しインターフェースへ再ログインすることにより、この問題を解決できます。

iGateway サービスを再起動するには、以下の手順に従います。

1. ［管理］タブをクリックし、［サービス］サブタブをクリックします。
2. ［システム ステータス］エントリを展開します。
3. 特定の CA Enterprise Log Manager サーバを選択します。
4. サービスの［管理］タブをクリックします。
5. ［iGateway の再起動］をクリックします。

第 7 章: 修正された問題

このセクションには、以下のトピックが含まれています。

r12.1 SP1 で修正された問題

お客様によって報告された以下の問題は、CA Enterprise Log Manager r12.1 SP1 で修正されています。

- 18789166-1
- 18790979-1
- 18955095-1
- 18973282-1
- 18982868-1
- 18988854-1
- 19005999-1
- 19066155-1
- 19077668-1
- 19087827-1
- 19127553-1
- 19176852-1
- 19182913-1
- 19188433-2

第 8 章: マニュアル

このセクションには、以下のトピックが含まれています。

マニュアル選択メニュー

マニュアル選択メニューを使用すると、すべての CA Enterprise Log Manager マニュアルに一箇所からアクセスできます。マニュアル選択メニューでは、以下の機能が提供されます。

- 展開可能な全マニュアルのリスト(HTML 形式)
- 全マニュアルにおける全文検索(検索結果はランク付けされ、検索語が強調表示されます)

  注: 数値のみを検索する場合は、検索語の前にアスタリスクを付けてください。
- 上位レベルのトピックへリンクするためのブレッドクラム機能
- 全マニュアルにわたる単一のインデックス
- ガイドの印刷用 PDF 版へのリンク

マニュアル選択メニューへのアクセス方法

CA 製品ドキュメントのマニュアル選択メニューは、「All Guides Including a Searchable Index」というタイトルの ZIP ファイルでダウンロードできます。

CA Enterprise Log Manager マニュアル選択メニューにアクセスする方法

1. ドキュメントの検索に移動します。
2. 製品名として「CA Enterprise Log Manager」を入力し、リリースと言語を選択して[Go]をクリックします。
3. デスクトップまたは他の場所へ ZIP ファイルをダウンロードします。
4. ZIP ファイルを開き、bookshelf フォルダをデスクトップにドラッグするか、別の場所に解凍します。
5. bookshelf フォルダを開きます。
6. bookshelf ファイルを開きます。
   - bookshelf がローカル システム上にあり、Internet Explorer を使用している場合は、Bookshelf.hta ファイルを開きます。
   - bookshelf が、リモート システム上にあるか、Mozilla Firefox を使用している場合は、Bookshelf.html ファイルを開きます。

   マニュアル選択メニューが開きます。

付録 A: サードパーティ製品の使用条件

このセクションには、以下のトピックが含まれています。

Adaptive Communication Environment（ACE）

ACE（TM）、TAO（TM）、CIAO（TM）に関する著作権およびライセンス情報

ACE(TM), TAO(TM) and CIAO(TM) are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University Copyright (c) 1993-2003, all rights reserved. Since ACE TAO CIAO are open-source, free software, you are free to use, modify, copy, and distribute--perpetually and irrevocably--the ACE TAO CIAO source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using ACE TAO CIAO.

You can use ACE TAO CIAO in proprietary software and are under no obligation to redistribute any of your source code that is built using ACE TAO CIAO. Note, however, that you may not do anything to the ACE TAO CIAO code, such as copyrighting it yourself or claiming authorship of the ACE TAO CIAO code, that will prevent ACE TAO CIAO from being distributed freely using an open-source development model. You needn't inform anyone that you're using ACE TAO CIAO in your software, though we encourage you to let us know so we can promote your project in the ACE TAO CIAO success stories.

ACE TAO CIAO are provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, ACE TAO CIAO are provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies provide commercial support for ACE and TAO, however. ACE, TAO and CIAO are Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by ACE TAO CIAO or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE, TAO and CIAO web sites are maintained by the Center for Distributed Object Computing of Washington University for the development of open-source software as part of the open-source software community. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the ACE, TAO and CIAO software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source ACE TAO CIAO projects or their designees.

The names ACE(TM), TAO(TM), CIAO(TM), Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE(TM), TAO(TM), or CIAO(TM) nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache ライセンスを利用するソフトウェア

この製品は、以下の Apache ソフトウェアを利用します。

- Ant 1.6.5
- Formatting Objects Processor（FOP）0.95
- Jakarta POI 3.0
- Log4cplus 1.0.2
- Log4j 1.2.15
- Quartz 1.5.1
- Xerces-C 2.6.0

Portions of this product include software developed by the Apache Software Foundation. The Apache software is distributed in accordance with the following license agreement:

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

'License' shall mean the terms and conditions for use, reproduction,and distribution as defined by Sections 1 through 9 of this document.

'Licensor' shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

'Legal Entity' shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, 'control' means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

'You' (or 'Your') shall mean an individual or Legal Entity exercising permissions granted by this License.

'Source' form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

'Object' form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and versions to other media types.

'Work' shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work(an example is provided in the Appendix below).

'Derivative Works' shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

'Contribution' shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, 'submitted' means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as 'Not a Contribution.'

'Contributor' shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s)with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a 'NOTICE' text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an 'AS IS' BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

boost 1.35.0

この製品は、次の使用許諾契約の下で配布されたソフトウェアを含んでいます。

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

JDOM 1.0

本製品には、JDOM Project（http://www.jdom.org/）によって開発されたソフトウェアが含まれています。The JDOM software is distributed in accordance with the following license agreement.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact .

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management .

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)." Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter and Brett McLaughlin . For more information on the JDOM Project, please see http://www.jdom.org.

PCRE 6.3

この製品の一部には、Philip Hazel によって開発されたソフトウェアが含まれています。University of Cambridge Computing Service ソフトウェアは、以下の使用許諾契約に従って配布されます。

THE BASIC LIBRARY FUNCTIONS

Written by: Philip Hazel

Email local part: ph10

Email domain: cam.ac.uk

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

THE C++ WRAPPER FUNCTIONS

Contributed by: Google Inc.

THE "BSD" LICENCE

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the University of Cambridge nor the name of Google Inc. nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

End

Zlib 1.2.3

この製品には、Jean-loup Gailly と Mark Adler が開発した zlib が含まれます。

ZThread 2.3.2

この製品の一部は、Eric Crahen によって開発されたソフトウェアが含まれています。ZThread ソフトウェアは以下の使用許諾契約に従って配布されます。

Copyright (c ページ) 2005, Eric Crahen

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software" ページ), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.