

CA Asset Portfolio Management

実装ガイド

リリース 12.9.00



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により隨時、変更または撤回されることがあります。本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けて本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

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

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

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

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

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2013 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

このドキュメントセットには以下の CA Technologies ブランドと製品についての記述があります。

- CA Asset Converter
- CA Asset Portfolio Management (CA APM)
- CA Business Intelligence
- CA Client Automation
 - (旧称 : CA IT Client Manager)
- CA Configuration Management Database (CA CMDB)
- CA Embedded Entitlements Manager (CA EEM)
- CA 管理データベース (CA MDB)
- CA Process Automation™
- CA Service Catalog
- CA Service Desk Manager
- CA Software Asset Manager (CA SAM)
- CA SiteMinder®

このドキュメントセットには、以下のコンポーネントについての記述もあります。
このコンポーネントには以前は別の名前が使用されていました。

- Common Asset Viewer
 - (以前のアセット管理システム (AMS))

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。

目次

第 1 章: はじめに	9
概要.....	9
対象読者.....	9
CA APM のデフォルト管理者.....	10
第 2 章: 計画	11
インストールの計画.....	11
Internet Information Services がインストールされているかどうかの確認.....	13
CA iTechnology iGateway の削除.....	13
Java Development Kit (JDK) のインストール.....	15
Pentaho データ統合 (Kettle) のインストール.....	15
リリース 12.8 からのマイグレーションステータスの保持.....	17
以前のバージョンの製品のアンインストール.....	18
CA SAM インポートおよびエクスポートサービスのアンインストール.....	19
第 3 章: インストール	21
ソフトウェアの実装方法.....	21
前提条件の確認.....	21
CA APM のインストール.....	22
Apache Tomcat 設定ファイルの更新.....	23
サービスの開始.....	24
Web インターフェースの開始.....	25
インストールの確認.....	27
CA Business Intelligence のインストールの確認.....	27
CA SAM インポートおよびエクスポートサービスをインストールする。.....	29
セキュリティで保護されたネットワーク通信の設定.....	30
製品コンポーネントの設定.....	31
CA APM の修復.....	40
CA APM のアンインストール.....	40

第 4 章: リリース 11.3.4 から リリース 12.9 に CA APM データをマイグレートする方法

43

リリース 11.3.4 から リリース 12.9 に CA APM データをマイグレートする方法.....	43
前提条件の確認.....	47
CA APM マイグレーションツールキットを起動します。	53
マイグレーション前レポートの実行.....	53
アセット名変更設定の指定.....	61
マイグレーションユーティリティの実行	63
手動マイグレーション用のマイグレーション後レポートの実行	69
参照と分析用のマイグレーション レポート データ	71
CA APM Web インターフェースの開始	76
手動マイグレーションの実行.....	77
マイグレーション後検証の実行.....	95
トラブルシューティング.....	96

第 5 章: マルチテナントの実装

99

マルチテナント	99
サービス プロバイダ	100
マルチテナントの仕組み	100
ユーザ インターフェースの影響	102
テナント ユーザ	102
マルチテナントを実装する方法	103
マルチテナントの有効化	104
テナント、サブテナント、およびテナント グループの管理	105
テナントの定義	105
テナントの更新	106
テナントのアクティブ化	107
新しいテナントを初期化する方法	108
テナント グループの定義	108
テナント グループの更新	108
テナント 階層	109
サブテナントの定義	110
サブテナントの更新	110
製品によって維持されるテナント グループ	111

第 6 章: その他の製品の統合

113

CA Business Intelligence の統合	113
------------------------------------	-----

CA APM と CA Business Intelligence の統合方法	114
レポートの設定および製品の更新	116
CA EEM 統合	116
CA CMDB の統合	117
CA APM と CA CMDB の統合方法	118
アセットと構成アイテムの監査履歴レコードの共有	118
アセットと構成アイテムのレコードの分類	118
アセット拡張フィールドの定義	121
共有フィールドに対するイベントの定義	123
CA Service Desk Manager および CA CMDB からの管理データ リポジトリ (MDR) の定義	123
通知プロセスのための CA Process Automation 統合	124
CA Process Automation 通知プロセスのセットアップ方法	124
ワークフロー プロバイダ通知プロセス ファイルのインポート	125
CA Process Automation メール サーバの設定	126
CA Process Automation ワークフロー プロセス パラメータの変更	127
CA APM ユーザに対する CA Process Automation の使用の許可	130
パラメータ用の必須インジケータおよび複数行テキスト フィールド	131
Data Importer プロセスのための CA Process Automation 統合	132
CA Process Automation Data Importer プロセスのセットアップ方法	132
CA Process Automation ワークフロー プロセス パラメータの変更	133
CA Service Catalog インテグレーション	135

第 7 章: CA APM への CA SAM の実装	137
概要	137
CA APM および CA SAM データ同期	138
データ同期の設定方法	139
CA APM で CA SAM を実装する方法	144
前提条件の確認	144
Internet Information Services がインストールされているかどうかの確認	145
CA SAM インポートおよびエクスポート サービスをインストールする。	146
CA SAM インポートおよびエクスポート サービスの設定	147
CA SAM の CA APM イベント サービスを設定します。	149
SAM インポート ドライバの設定	152
ハードウェア インポート用 Windows タスクのスケジュール	153
CA APM イベント サービスの開始	153
ソフトウェア アセット管理機能の有効化	154
CA SAM への CA APM データのロード	158
データ管理の推奨事項	159
手動データ同期	160

コストセンターのデータ管理.....	160
在庫の測定単位.....	161
自動データ同期のフィールド要件.....	162
未定義オペレーティングシステムを持ったアセット.....	163
CA Software Compliance Manager をアンインストールする方法.....	164

第 8 章: トラブルシューティング 167

「インストールが開始されない」または「サーバが見つからない」というエラーが表示される	167
テナント管理ページを表示できないというブラウザ エラーが表示される	168
テナント管理ページが表示されない	168
Web サーバ名にアンダースコア文字が使われている	168
拡張文字が含まれるユーザ名を使うとログインに失敗する	169
IIS 7 が Windows 2008 にインストールされると WCF サービスが失敗する	169
「含まれていないオペレーティング システム」というメッセージがメッセージ キューに表示される	170

第1章: はじめに

このセクションには、以下のトピックが含まれています。

[概要 \(P. 9\)](#)

[対象読者 \(P. 9\)](#)

[CA APM のデフォルト管理者 \(P. 10\)](#)

概要

このガイドでは、CA APM を正しく実装するために必要な情報について説明します。これには、以下のタスクの実行方法が含まれます。

- 新規インストールを計画および準備する
- 必要な製品コンポーネントをインストールおよび設定する
- その他の CA 製品と統合する

注: システム要件が記載された最新のリリース ノートは、CA サポート オンラインの [CA APM 製品ページ](#)で参照できます。

対象読者

このガイドは、CA APM のインストールと設定の方法を習得したいと思っているユーザを対象としています。以下のユーザは、このガイドに記載された情報を利用して特定のタスクを実行します。

- システム管理者と管理者はこのガイドの情報を使用して、製品を初めてインストールし、実装要件に基づいて製品を設定します。
- インテグレータは、このガイドの情報および CA Technologies 製品に関する自身の知識を活用して、CA APM をその他の CA Technologies 製品と統合します。
- ユーザ: 必要な場合にはこのガイド内の情報を使用して、製品とコンポーネントをインストールできます。

このガイドの情報を使用するには、Windows オペレーティング システムに関する実用的な知識、およびオペレーティング システムの基本的な管理タスクに関する実用的な知識が必要です。

CA APM のデフォルト管理者

デフォルトの CA APM システム管理者ユーザおよび役割は、CA APM のインストール時に自動的に作成されます。このユーザは、製品のすべての部分を完全に制御できます。CA APM システム管理者ユーザのデフォルトのユーザ名とパスワードは **uapmadmin** です。

注: セキュリティ上の理由により、リリース 12.9 インストールを完了した後にデフォルトパスワードを変更することをお勧めします。

インストールが完了したら、すべてのサービスが開始されていることを確認します。次に、CA APM システム管理者ユーザのログイン認証情報を使用して Web インターフェースを起動し、製品が使用可能な状態にあることを確認します。

第 2 章: 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。

[インストールの計画 \(P. 11\)](#)

インストールの計画

CA APM のインストールを計画するときは、以下の情報を使って調査を行い、情報を収集すると、作業を効率的に進めることができます。

■ **調査** - 以下の手順を実行します。

- リリース ノートを参照します。この情報を参照して理解するまでは、インストールを開始しないでください。

注: 最新のリリース ノートは、CA サポートオンラインの CA APM 製品ページ（マニュアル選択メニュー セクション）で参照できます。

- インストール ファイルがあることを確認します。

注: コンピュータにインストール メディア用の適切なドライブがない場合は、CA APM をインストールするコンピュータにインストール ファイルをコピーします。その後、インストールを開始します。ネットワークを経由したリモートインストールの場合でも、ネットワーク上でドライブまたはフォルダを共有できます。ネットワーク経由で接続してインストールを開始します。

- CA APM との使用を認定されたサードパーティ製ソフトウェア製品のリスト用の **Certification Matrix** を確認します。

注: 最新の **Certification Matrix** は、<http://ca.com/jp/support/> で参照できます。

- ネットワークの可用性、使用帯域幅、および応答性を考慮します。
- [製品コンポーネント \(P. 31\)](#) の情報に目を通し、概要を把握します。

■ **データベース** - 以下の手順を実行します。

- 「CA 管理データベース概要ガイド」を確認します。CA MDB に関する知識を深めます。展開計画を決定し、CA MDB を使用するために対処する必要のある SQL Server または Oracle の問題を認識します。
- CA APM で使用するデータベース（SQL Server または Oracle）を決定し、そのデータベースをインストールします。

- Oracle または SQL Server を設定します。
- (SQL Server) SQL Server クライアントツールが SQL Server データベースにアクセスするすべてのサーバにインストールされていることを確認してください。
- (Oracle) 32 ビットの Oracle クライアントツールが Oracle データベースにアクセスするすべてのサーバにインストールされていることを確認してください。

注: 64 ビット Oracle データベース サーバをホストする 64 ビット コンピュータには、CA MDB を除いて、CA APM コンポーネントをインストールすることをお勧めしません。

- **CA Business Intelligence** - CA Business Intelligence をインストールし、ログイン認証情報と接続情報を記録します。 [CA Business Intelligence のインストールを確認します](#) (P. 27)。

注: CA Business Intelligence の実装の詳細については、「CA Business Intelligence 実装ガイド」を参照してください。

- **Internet Information Services (IIS)** - [すべてのアプリケーションサーバおよび Web サーバに Internet Information Services がインストールされていることを確認](#) (P. 13) します。

- **CA EEM** - CA EEM 12.51 をインストールします。 CA APM インストールメディアにあるインストーラ プログラムを使用して、CA EEM をインストールできます。

注: CA EEM の以前のバージョンがある場合は、CA EEM インストーラを使用して、リリース 12.51 にアップグレードします。

CA EEM と共にインストールされる CA iTechnology iGateway は、さまざまな CA Technologies 製品で使用される共有コンポーネントです。 CA iTechnology iGateway は、HTTP プロトコルを使用してリクエストを送信し、応答を受信する Web サーバです。

CA iTechnology iGateway は、その他の製品と共にインストールされる場合もあります。 CA iTechnology iGateway が CA EEM をインストールするコンピュータに存在する場合は、32 ビットか 64 ビットかを確認します。 CA iTechnology iGateway および CA EEM 12.51 サーバが、両方とも 32 ビットまたは両方とも 64 ビットである場合、対応は必要ありません。ただし、2 つの製品が一致しない(たとえば、一方が 32 ビットで、他方が 64 ビット)場合は、[CA iTechnology iGateway を削除します](#) (P. 13)。その後、CA EEM のインストールを開始します。 CA EEM のインストールを完了すると、正しいバージョンの CA iTechnology iGateway がインストールされます。

- **Common Asset Viewer** - CA APM をインストールする前に、Common Asset Viewer をインストールするアプリケーションサーバに [Java Development Kit \(JDK\) をインストール](#) (P. 15) します。
- **CA Software Compliance Manager (CA SCM)** - CA SCM リリース 12.6 を CA APM リリース 12.9 に統合する場合、CA APM をインストールする前に CA SCM (およびすべての累積リリース) をインストールします。
- **Pentaho データ統合 (Kettle)** - CA APM をインストールする前またはインストールした後に、Pentaho データ統合 (Kettle) 4.x をインストールします。CA APM をインストールするローカルコンピュータに Kettle をインストールします。Kettle は、リリース 11.3.4 データをマイグレートするために使用するマイグレーションツールキットに必要です。
注: リリース 11.3.4 から リリース 12.9 にアップグレードする場合、または以前にリリース 11.3.4 から リリース 12.8 にアップグレードした場合にのみ、Kettle が必要です。

Internet Information Services がインストールされているかどうかの確認

CA APM のインストールを開始する前に、Internet Information Services (IIS) 7.0、7.5、または 8.0 がすべてのアプリケーションサーバと Web サーバにインストールされていることを確認します。このサービスがサーバ上にない場合は、インストールを開始する前に、サービスを追加します。

次の手順に従ってください:

1. 各々のアプリケーションサーバおよび Web サーバにログインします。
2. コントロールパネル ([管理ツール] - [サービス]) を開きます。
3. IIS 管理サービスがサーバにインストールされていることを確認します。

CA iTechnology iGateway の削除

CA EEM と共にインストールされる CA iTechnology iGateway は、さまざまな CA Technologies 製品で使用される共有コンポーネントです。CA iTechnology iGateway は、HTTP プロトコルを使用してリクエストを送信し、応答を受信する Web サーバです。

CA iTechnology iGateway は、その他の製品と共にインストールされる場合もあります。CA iTechnology iGateway が CA EEM をインストールするコンピュータに存在する場合は、32 ビットか 64 ビットかを確認します。CA iTechnology iGateway および CA EEM 12.51 サーバが、両方とも 32 ビットまたは両方とも 64 ビットである場合、対応は必要ありません。ただし、2 つの製品が一致しない（たとえば、一方が 32 ビットで、他方が 64 ビット）場合は、CA iTechnology iGateway を削除します。その後、CA EEM のインストールを開始します。CA EEM のインストールを完了すると、正しいバージョンの CA iTechnology iGateway がインストールされます。

注: 各種 CA Technologies 製品やコンポーネントが、64 ビット CA Technologies eTrustITM エージェントを含む、CA iTechnology iGateway の 64 ビットバージョンをインストールします。

次の手順に従ってください:

1. CA EEM をインストールするコンピュータで、CA iTechnology iGateway を削除します。

注: CA iTechnology iGateway を正常にアンインストールするために、まず CA iTechnology iGateway に依存する製品をすべてアンインストールする必要があります。

- a. コントロールパネルを開きます（[スタート] - [設定] - [コントロールパネル] など）。
- b. [プログラムの追加と削除] をダブルクリックします。
- c. [CA iTechnology iGateway] を選択し、[削除] をクリックします。

2. 以下の場所から iGateway および iTechnology のレジストリ キーフォルダを削除します。

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\

3. IGW_LOC 環境変数を削除します。
 - a. [スタート] メニューから、[マイコンピュータ] を右クリックし、[プロパティ] を選択します。
 - b. [詳細設定] タブをクリックします。
 - c. [環境変数] をクリックします。
 - d. [システム環境変数] 一覧で [IGW_LOC] を選択し、[削除] - [OK] をクリックします。

4. コンピュータを再起動します。
5. CA APM をインストールします。
6. CA APM インストールが完了すると、CA EEM がインストールされたコンピュータ上に、アンインストールしたコンポーネントが再インストールされています。

注: 64 ビット Oracle データベース サーバをホストする 64 ビット コンピュータには、CA MDB を除いて、CA APM コンポーネントをインストールすることをお勧めしません。

Java Development Kit (JDK) のインストール

CA APM のインストールを開始する前に、Common Asset Viewer のインストール先のアプリケーションサーバに Java Development Kit (JDK) 1.7.0_40 (32 ビット版) をインストールします。CA APM をインストールすると、アプリケーションサーバに Common Asset Viewer が自動的にインストールされます。

次の手順に従ってください:

1. アプリケーションサーバにログインします。
2. Web ブラウザで、Oracle の Web サイト (<http://www.oracle.com>) から JDK 1.7.0_40 (32 ビット版) をダウンロードして、インストールします。
3. JDK 1.7.0.40 (32 ビット版) のインストールディレクトリを参照するように JAVA_HOME 環境変数を設定します。
4. JDK 1.7.0_40 (32 ビット版) のインストールディレクトリの \$bin ディレクトリを参照するように Path 環境変数を更新します。

Pentaho データ統合 (Kettle) のインストール

CA APM をインストールするローカル コンピュータに Pentaho データ統合 (Kettle) 4.x をインストールします。リリース 11.3.4 から リリース 12.9 にアップグレードする場合、または以前にリリース 11.3.4 から リリース 12.8 にアップグレードした場合のみ、Kettle が必要です。

注: CA APM をインストールする前またはインストールした後に Kettle をインストールできます。ただし、CA APM をインストールする前に Kettle 4.x をインストールすることをお勧めします。

次の手順に従ってください:

1. CA APM をインストールするコンピュータに管理者としてログインします。
2. CA サポート Web サイトから Kettle をダウンロードし、CA APM リリース 12.9 がインストールされているサーバにインストールします。以下の手順に従って Kettle をダウンロードします。
 - a. 以下のリンクをクリックしてください。
ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_8/pentaho-kettle-4.4.0.zip
 - b. 希望のディレクトリに pentaho-kettle-4.4.0.zip 保存します。
3. 以下の手順を実行して、Kettle 用の環境変数を作成します。
 - a. [スタート] - [ファイル名を指定して実行] をクリックし、「sysdm.cpl」と入力して [システムのプロパティ] にアクセスします。
 - b. [詳細設定] タブをクリックします。
 - c. [環境変数] をクリックします。
 - d. システム環境変数セクションの [新規] をクリックし、以下の情報を入力します。

変数名

KETTLE_HOME

変数値

Kettle フォルダへのパス。

注: 「data-integration」フォルダが含まれる親フォルダ (C:\Program Files (x86)\CA\ITAM\Kettle など) にパスが設定されていることを確認してください。

- a. [OK] をクリックし、[システムのプロパティ] を終了します。

リリース 12.8 からのマイグレーションステータスの保持

マイグレーションユーティリティは、リリース 11.3.4 から現在のリリースに CA APM データ オブジェクトを移動させます。各オブジェクトのマイグレーションステータス（[完了] など）はマイグレーションユーティリティに表示されます。以前にリリース 11.3.4 データをリリース 12.8 にマイグレートしている場合、リリース 12.9 を使用して、リリース 12.8 でマイグレートできなかったオブジェクトをマイグレートできます。ただし、リリース 12.8 でマイグレートしたオブジェクトのマイグレーションステータスを保持するには、リリース 12.9 にアップグレードする前に、以下の手順に従います。

重要: 以下の手順は、リリース 12.8 をアンインストールする前に実行してください。

次の手順に従ってください:

1. リリース 12.8 がインストールされているサーバにログインします。
2. マイグレーションユーティリティの `resources` フォルダに移動します。

例：

`[ITAM Root Path]\Migration Toolkit\migration-utility\resources\`

3. 任意のテキストエディタ（メモ帳など）で `mu_db_delete.bat` ファイルを開きます。
4. ファイルの内容をすべて削除します。
5. `mu_db_delete.bat` ファイルを保存し、テキストエディタを終了します。

これで、リリース 12.9 のアップグレードに進むことができます。マイグレーションユーティリティは、リリース 12.8 でマイグレートしたオブジェクトのステータスを保持します。

注: まずこれらの手順を実行せずに、リリース 12.8 をアンインストールした場合でも、リリース 12.9 のインストールを続けることができます。マイグレーションユーティリティを開くと、以前にマイグレートしたオブジェクトには [Not Started] のステータスが表示されます。ステータスを手動で更新します。オブジェクトを選択して右クリックし、[Move to Completed] を選択します。

以前のバージョンの製品のアンインストール

CA APM リリース 12.9 を以前のバージョンの製品がインストールされたコンピュータにインストールする場合、インストールによってデータベースのみが更新されます。インストールによって CA APM はリリース 12.9 にアップグレードされません。まず CA APM の以前のバージョンを手動でアンインストールし、次にリリース 12.9 をインストールします。

注: 製品の以前のバージョンをアンインストールする前に、Apache Tomcat Common Asset Viewer サービスを停止してください。

次の手順に従ってください:

1. 現在のリリースの **Storage** フォルダをバックアップします（現在のリリースがリリース 12.6、12.7、または 12.8 のバージョンである場合にのみ、この手順は適用されます）。

- a. ストレージマネージャ サービスがインストールされているアプリケーションサーバの以下の場所に移動します。

[ITAM Root Path]/Storage/

- b. Storage フォルダの内容をコピーし、安全なロケーション（ただし、いずれの ITAM ルートパス フォルダにもない）にそれらを貼り付けます。

注: 製品のインストールを完了したら、Storage フォルダの内容をリストアします。詳細については、「[インストールの確認 \(P. 27\)](#)」を参照してください。

2. 製品の以前のリリースまたはバージョンをアンインストールします。

注: CA APM の以前のバージョンのアンインストールについては、そのバージョンの「実装ガイド」を参照してください。

3. 以前のリリースでインストールされている場合は、[CA SAM インポートおよびエクスポート サービスをアンインストール \(P. 19\)](#) します。

これで、CA APM リリース 12.9 をインストールできます。

注: リリース 12.9 のインストールについては、「[インストール \(P. 21\)](#)」を参照してください。

CA SAM インポートおよびエクスポート サービスのアンインストール

以前のリリースで CA APM および CA SAM を実装している場合、CA SAM サーバに CA SAM インポートおよびエクスポート サービスのコンポーネントがインストールされています。リリース 12.9 をインストールする前に、CA SAM サーバから CA SAM インポートおよびエクスポート サービスをアンインストールします。

次の手順に従ってください:

1. CA SAM サーバにログインします。
2. [スタート] メニューから、コントロールパネルを開きます (たとえば、[スタート] - [設定] - [コントロールパネル] をクリックします)。
3. [プログラムと機能] をクリックします。
4. [CA ITAM SAM Import Export Service] をダブルクリックします。
5. 画面の指示に従って、アンインストールプロセスを実行します。

第3章: 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。

[ソフトウェアの実装方法 \(P. 21\)](#)

[CA APM の修復 \(P. 40\)](#)

[CA APM のアンインストール \(P. 40\)](#)

ソフトウェアの実装方法

リリース 12.9 を実装するには、以下の手順に従います。

1. [前提条件を確認します \(P. 21\)](#)。
2. [CA APM をインストール \(P. 22\)](#) します。
3. [Apache Tomcat 設定ファイルを更新します \(P. 23\)](#)。
4. [サービスを開始します \(P. 24\)](#)。
5. [Web インターフェースを開始 \(P. 25\)](#) します。
6. [インストールを確認します \(P. 27\)](#)。

前提条件の確認

リリース 12.9 をインストールする前に、インストール先のコンピュータが最小システム要件を満たしていることを確認します。システム要件の詳細については、「CA Asset Portfolio Management リリース ノート」を参照してください。

製品をインストールするコンピュータに以下のコンポーネントがインストールされていることを確認します。以下のコンポーネントのいずれもインストールされていない場合は、インストール処理は開始されません。

- Microsoft .NET 3.5 の機能 (Windows Server 2012 のみ)
- Microsoft .NET Framework 4.0
- Microsoft WSE 3.0 Runtime

注: インストーラは、製品をインストールするコンピュータ上で以下のコンポーネントを検出しなかった場合、Microsoft .NET Framework 4.0 および Microsoft WSE 3.0 Runtime をインストールします。

- Internet Information Services (IIS) 7.0、7.5、または 8.0
- SQL Server クライアントまたは Oracle クライアント
- Java Development Kit (JDK) 1.7.0_40 (32 ビット版)

注: JAVA_HOME 環境変数を適切なインストールディレクトリに設定してください。

インストーラが以下のコンポーネントを検出しなくても、インストール処理は開始されます。ただし、作成する設定がこれらのコンポーネントを必要とする場合、インストールは停止します。

- Pentaho データ統合 (Kettle) 4.4
注: KETTLE_HOME 環境変数を適切なインストールディレクトリに設定してください。
- CA EEM 12.51
- CA Business Intelligence 接続

CA APM のインストール

前提条件となるコンポーネントおよび製品を正しく計画およびインストールした後、インストールメディアを使用して CA APM をローカルコンピュータにインストールします。インストーラは、CA APM と統合するコンポーネントおよび製品情報を入力するようにユーザに促します。正しい情報を入力していることを確認します。

次の手順に従ってください:

1. リリース 12.9 をインストールするコンピュータに管理者としてログインします。
2. インストールファイルが含まれるフォルダを開き、ルートディレクトリ内の Setup.exe ファイルをダブルクリックします。
インストール ウィザードが起動します。
3. ウィザードの画面の指示に従います。

重要: Oracle データベースがある場合は、有効な表領域パスを指定していることを確認します。このパスが無効な場合、データベースのインストールは失敗します。次のパスは、有効な Oracle 表領域パスの例です：

C:\app\Administrator\oradata\Oracle_Service_Name。

注: Web フーム セットアップで、Web フーム内のサーバのいずれかにすでにこれらのコンポーネントがインストールされている場合、[CA Business Intelligence の詳細] パネルおよび[CA EEM の詳細] パネルは表示されません。

4. インストールが完了したら、[完了] をクリックします。

製品コンポーネント

インストール時に、インストール ウィザードは、以下の製品コンポーネントに関する情報を入力するようにユーザに促します。この情報にはサーバ ロケーション および設定が含まれます。

- [データベース サーバ](#) (P. 33)
- [Web サーバ](#) (P. 34)
- [アプリケーション サーバ](#) (P. 34)
- [CA EEM](#) (P. 36)
- [CA Business Intelligence](#) (P. 36)

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

Apache Tomcat 設定ファイルの更新

Common Asset Viewer を使用すると、照合を通してリンクされているアセットの検出データと所有データを表示できます。このデータには、システム構成、オペレーティング システム、システム デバイス、およびファイル システムが含まれます。

Common Asset Viewer は、CA APM のインストールを開始する前に [Java Development Kit \(JDK\) をインストール](#) (P. 15)することを必要とします。Common Asset Viewer は Apache Tomcat サーバを必要とします。このサーバは CA APM のインストールに含まれています。この値はインストール後に変更できます。最初に Apache Tomcat 設定ファイル内でポートを更新します。次に、製品内でポートを変更します（[管理] - [システム構成] - [Common Asset Viewer]）。

重要: CA APM の Tomcat ポート番号は、デフォルトで 9080 です。CA APM と統合する別の製品がこのポート番号を使用する場合、競合が発生しないように CA APM 内のポート番号を変更してください。

次の手順に従ってください:

1. Common Asset Viewer がインストールされているアプリケーション サーバで、以下のいずれかのフォルダに移動します（サーバによって異なります）。


```
C:\Program Files\CA\SC\AMS\Tomcat\conf (32 ビット オペレーティング システムの場合)
```

```
C:\Program Files (x86)\CA\SC\AMS\Tomcat\conf (64 ビット オペレーティング システムの場合)
```
2. `server.xml` ファイルを選択して開きます。

3. server.xml ファイルの以下のセクションに移動します。

```
<Connector port="9080" protocol="HTTP/1.1"
           connectionTimeout="20000"
           redirectPort="8443" />
```

4. Tomcat ポート番号を、CA APM が使用するものと同じ番号で更新します（[管理] - [システム構成] - [Common Asset Viewer]）。
5. server.xml ファイルを保存します。

サービスの開始

インストールが完了した後、すべてのサービスを開始します。

注: 状況によっては、製品をインストールした後、CA Business Intelligence はインストールされたが Web サーバを再起動する必要があることを伝えるメッセージが表示される場合があります。CA Business Intelligence サービスが開始されていることを確認する前に、Web サーバを再起動してください。

次の手順に従ってください:

1. コントロールパネルを開きます（[スタート] - [設定] - [コントロールパネル] など）。
2. [管理ツール] をダブルクリックします。
3. [サービス] をダブルクリックします。
4. 以下の各サービスを見つけて開始します。
 - Apache Tomcat Common Asset Viewer
 - CA Asset Portfolio Management - Data Importer エンジン
 - CA Asset Portfolio Management - イベント サービス
 - CA Asset Portfolio Management - エクスポート サービス
 - CA Asset Portfolio Management - 登録サービス
 - CA Asset Portfolio Management - ハードウェア照合エンジン
 - CA Asset Portfolio Management - LDAP インポート サービス
 - CA CASM

重要: パフォーマンス上の理由により、マルチテナントを使用しないときは CA CASM サービスを開始しないことをお勧めします。

 - CA iTechnology iGateway 4.6

5. セントラル設定マネージャを使って CA Business Intelligence サービスを確認するには、[スタート] - [プログラム] - [BusinessObjects XI Release] - [BusinessObjects Enterprise] - [Central Configuration Manager] を選択します。セントラル設定マネージャが開きます。サービスが開始されていない場合は、サービスを右クリックし、[開始] を選択します。

Web インターフェースの開始

インストールの完了後は、Web インターフェースを開始して、CA APM が使用可能な状態にあるかどうかを確認できます。Web インターフェースが開始されていることを確認したら、すべての管理者に URL とログイン認証情報を提供し、ユーザのために製品を準備します。その後で各管理者は、セキュリティのセットアップ、ユーザインターフェースの設定、ハードウェア照合のセットアップ、また必要であれば、製品コンポーネントの設定を行うことができます。管理者は、製品の準備が終わった後、URL とログイン認証情報をユーザに提供できます。ユーザのための製品の管理および準備の詳細については、「[管理ガイド](#)」を参照してください。

注: Web インターフェースを起動する前に、[IIS に ASP.NET を登録](#) (P. 26) していることを確認してください。

以下のいずれかの方法を使用して、Web インターフェースを起動します。

- サポートされている Web ブラウザを開き、以下の URL を入力します。

`http://servername:port/itm`

servername および port を CA APM Web サーバをホストしているサーバおよびポートの名前に置き換えます。

注: Internet Explorer ブラウザのセキュリティが「高」に設定されている場合、Web インターフェースを開始すると、コンテンツに関する警告メッセージが表示されます。このメッセージが表示されないようにするには、Web サイトを信頼済みサイトに追加するか、セキュリティのレベルを下げます。

Web サーバ上には、URL の場所を参照する [スタート] メニューのショートカットが作成されています。

- [スタート]-[プログラム]-[CA]-[Asset Portfolio Management]-[Asset Portfolio Management] をクリックします。

CA APM にログインするには、以下のデフォルト認証情報を入力します。

ユーザ名

uapmadmin

パスワード

uapmadmin

注: インストール中にパスワードを変更した場合は、作成したパスワードを使用します。

状況によっては、ブラウザ エラーまたは[ユーザ名エラー](#) (P. 169)が表示されます。これらのエラーは、トラブルシューティングの指示に従って解決できます。

ASP.NET の IIS への登録

CA APM をインストールするコンピュータに IIS および ASP.NET をインストールした後、IIS に ASP.NET を登録します。

次の手順に従ってください:

1. Windows Server 2008 では、以下の手順に従います。
 - a. コマンドプロンプトで、適切な Microsoft.NET Framework フォルダに移動します。たとえば、C:\Windows\Microsoft.Net\Framework64\v4.0.30319 や C:\Windows\Microsoft.Net\Framework\v4.0.30319 などです。
 - b. 以下の実行可能ファイルを実行します。
`aspnet_regiis.exe`

これで、ASP.NET は IIS に登録されます。
2. Windows Server 2012 では、以下の手順に従います。
 - a. サーバー マネージャを開きます。
 - b. [管理] メニューの下で、[役割と機能の追加] を選択します。
[役割と機能の追加 ウィザード] が開きます。
 - c. 画面上の指示に従い、インストール タイプおよびインストール先サーバを選択します。
 - d. [サーバーの役割の選択] ペインで、[役割] の下の [アプリケーション開発] を展開し、適切な ASP.NET バージョンを選択して、[次へ] をクリックします。
 - e. 画面上の指示に従って、インストールを実行します。

これで、ASP.NET は IIS に登録されます。

インストールの確認

インストール手順をすべて完了した後、リリース 12.9 が正常にインストールされたことを確認できます。

次の手順に従ってください:

1. CA APM リリース 12.9 をインストールしたサーバにログインします。
2. (Windows Server 2008 または Windows Server 2012) [スタート] メニューから、[コントロールパネル] - [プログラムと機能] を選択します。
3. すべての該当するサーバで以下のコンポーネントが利用可能であることを確認します。

CA Asset Portfolio Management

インストールの確認が完了しました。

注: リリース 12.9 をインストールする前に Storage フォルダの内容をバックアップした場合は、ここでその内容をリストアします。コピーした Storage フォルダの内容を使用し、以下のロケーションへそれらを貼り付けます。

[ITAM Root Path]/Storage/

すでに存在するフォルダに関するメッセージが表示されたら、フォルダをマージします。

Storage フォルダのバックアップの詳細については、「[以前のバージョンの製品のアンインストール \(P. 18\)](#)」を参照してください。

CA Business Intelligence のインストールの確認

インストール手順をすべて完了した後、CA Business Intelligence が正常にインストールされたことを確認できます。

次の手順に従ってください:

1. BiConfig.log ファイルを確認します。
 - a. CA APM がインストールされているアプリケーションサーバ上の以下のフォルダに移動します。

[ITAM Root Path]¥ITAM¥BIAR¥biconfig¥

- b. テキストエディタ (メモ帳など) で BiConfig.log ファイルを開きます。

- c. レポートサーバへの BIAR ファイルのエクスポートに関するエラーを検索します。
 - エラーが存在しない場合、CA Business Intelligence は正常にインストールされています。手順 3（共通ホーム ページでの CA Business Intelligence の確認）に進みます。
 - エラーが存在する場合は、レポートサーバに BIAR ファイルを手動でインポートします（以下の手順に進みます）。
2. BIAR ファイルを手動でインポートします（エラーがログ ファイルに存在する場合）。
 - a. CA APM がインストールされているアプリケーションサーバの [スタート] メニューからコマンドプロンプト ウィンドウを開きます。
 - b. 以下のフォルダに移動します。

```
[ITAM Root Path]\ITAM\BIAR\biconfig
```
 - c. テキストエディタ（メモ帳など）で ItamBoSetup-InstallBiar.xml ファイルを開きます。
 - CA MDB データベースのパスワードを入力します。
 - CA Business Intelligence サーバのパスワードを入力します。
 - d. ItamBoSetup-InstallBiar.xml ファイルを保存して閉じます。
 - e. 以下のコマンドを実行します。

```
biconfig -h CA Business Intelligence サーバ名 -u CA Business Intelligence 管理者ユーザ名  
-p CA Business Intelligence 管理者パスワード -f ItamBoSetup-InstallBiar.xml
```
 - f. BiConfig.log ファイルをもう一度開き、CA Business Intelligence が正常にインストールされたことを確認します。
 - g. 手順 3（共通ホーム ページでの CA Business Intelligence の確認）に進みます。
3. 共通ホーム ページで CA Business Intelligence を確認します。
 - a. [スタート] メニュー（[すべてのプログラム] - [CA] - [Asset Portfolio Management] - [CA IT Asset Manager]）から共通ホーム ページを開きます。
 - b. CA Business Intelligence に関する警告メッセージが表示されないことを確認します。
 - 警告が表示されない場合、CA Business Intelligence は正常にインストールされています。以下の手順に進む必要はありません。
 - 警告が表示される場合は、CA Business Intelligence レポートサーバのポートが正しいことを確認します（以下の手順に進みます）。

4. CA Business Intelligence レポート サーバのポートを確認します（共通ホーム ページに警告が表示される場合）。
 - a. CA APM ユーザインターフェースの [管理] - [システム構成] をクリックします。
 - b. 左側の [Web サーバ] を選択します。
 - c. [レポート サーバ ポート] フィールドに実装の正しい値が含まれていることを確認します。
 - ポートの値が正しくない場合は、正しい値を入力します。CA APM Web サーバおよびアプリケーション サーバで `iisreset` コマンドを実行してインターネットインフォメーション サービス (IIS) を再起動します。
 - ポートの値が正しく、警告が共通ホーム ページに表示される場合は、CA サポートにお問い合わせください。

CA SAM インポートおよびエクスポート サービスをインストールする。

CA APM および CA SAM を実装する場合は、CA SAM インポートおよびエクスポート サービス コンポーネントを CA SAM サーバにインストールします。

注: ソフトウェアアセット管理システムとして CA SAM を実装しない場合、CA SAM インポートおよびエクスポート サービスをインストールする必要はありません。

重要: CA SAM インポートおよびエクスポート サービスをインストールする前に、Microsoft .NET Framework 4.0 を CA SAM サーバにインストールする必要があります。

次の手順に従ってください:

1. CA SAM サーバにログインします。
2. CA APM インストール メディア上の SAMImportExportSetup フォルダに移動します。そのフォルダとすべての内容を CA SAM サーバ上のローカル フォルダにコピーします。
3. CA SAM サーバ上の SAMImportExportSetup フォルダで、`CAITAMSAMImportExportServiceInstaller.msi` をダブルクリックします。
インストール ルート パス用のプロンプトが表示されます。

4. CA SAM インポートおよびエクスポート サービス コンポーネントのインストール先 ITAM ルートパスを入力します。

以下の例は、推奨のパスを示しています。

例：

C:\Program Files\CA\ITAM

CA SAM インポートおよびエクスポート サービスのインストールが完了しました。

セキュリティで保護されたネットワーク通信の設定

インストールが完了した後、製品はセキュリティで保護されないネットワーク通信 (http) 用に設定されます。セキュリティで保護されたネットワーク通信 (https) 用に製品を設定するには、まずセキュアソケットレイヤ (SSL) プロトコルをサポートするように製品サーバ上の IIS を設定します。その後、セキュリティで保護されたネットワーク通信用の CA APM 設定パラメータを設定します。

以下のアクションを実行します。

1. [セキュリティで保護されたネットワーク通信のために IIS を設定します \(P. 30\)](#)。
2. [セキュリティで保護されたネットワーク通信のために CA APM を設定します \(P. 31\)](#)。

セキュリティで保護されたネットワーク通信のための IIS の設定

セキュアソケットレイヤ (SSL) プロトコルをサポートするように製品サーバ上の IIS を設定します。

次の手順に従ってください：

1. CA APM Web サーバ上でインターネットインフォメーションサービス (IIS) マネージャを起動します。
2. [サーバー証明書] を選択します。
3. [自己署名入り証明書の作成] をクリックし、証明書名を指定します。
4. (左側にある) CA APM がインストールされている Web サイト (たとえば既定の Web サイト) を選択します。
5. 右側の [操作] の下の [バインド] をクリックします。
[サイトバインド] ダイアログ ボックスが表示されます。
6. [追加] をクリックします。
7. [種類] に https を選択します。

8. ポートおよび SSL 証明書名を指定します。
9. CA APM アプリケーションサーバでこれらの同じ手順を実行します。

セキュリティで保護されたネットワーク通信のための CA APM の設定

セキュア ソケット レイヤ (SSL) プロトコルをサポートするように製品サーバ上の CA APM を設定します。

次の手順に従ってください:

1. 製品にログインし、[管理] - [システム構成] に移動します。
2. 左側の [Web サーバ] をクリックします。
3. サーバプロトコルを https に変更し、[保存] をクリックします。
4. 左側の [WCF サービス] をクリックします。
5. サーバプロトコルを https に変更し、[保存] をクリックします。
6. 左側の [アプリケーションサーバ] をクリックし、[詳細オプションを表示] チェック ボックスをオンにして設定パラメータをすべて表示します。
7. サーバプロトコルを https に変更します。
8. サーバポートおよびコンポーネントサーバポートを https プロトコルのポート (デフォルトでは 443) に変更し、[保存] をクリックします。
9. Web サーバおよびアプリケーションサーバ上の IIS をリセットします。

これで、セキュリティで保護されたネットワーク通信を使用して製品の Web インターフェースを起動できます。サポートされている Web ブラウザを開き、以下の URL を入力します。

`https://servername/ITAM/Pages/UserLogin.aspx`

servername を、CA APM Web サーバをホストしているサーバの名前に置き換えます。

製品コンポーネントの設定

製品のインストール後は、コンポーネント設定の変更および追加コンポーネントの設定が可能です。

以下のコンポーネントを設定できます。

- [Web サーバ \(P. 34\)](#)
- [アプリケーションサーバ \(P. 34\)](#)

- [ハードウェア照合エンジン](#) (P. 35)
- [CA EEM](#) (P. 36)
- [CA Business Intelligence](#) (P. 36)
- [エクスポート サービス](#) (P. 36)
- [Data Importer エンジン サービス](#) (P. 36)
- [インポート ドライバ](#) (P. 37)
- [LDAP データインポートおよび同期サービス](#) (P. 37)
- [ストレージマネージャ サービス](#) (P. 37)
- [CA APM 登録サービス](#) (P. 38)
- [サービス管理用の共通管理 \(CASM\)](#) (P. 38)
- [イベント サービス](#) (P. 38)
- [Common Asset Viewer](#) (P. 38)
- [WCF サービス](#) (P. 39)
- [Software Asset Management \(SAM\)](#) (P. 40)

次の手順に従ってください:

1. 管理者として CA APM にログインします。
2. 「管理」 - 「システム構成」をクリックします。
3. 左側で、設定する製品コンポーネントをクリックします。
4. 設定を行い、[保存]をクリックします。
5. アプリケーションプール内の設定をリサイクルします。

詳細については、「[アプリケーションプール内の設定のリサイクル \(P. 33\)](#)」を参照してください。

6. サービスを再起動します。

詳細については、「[サービスの開始 \(P. 24\)](#)」を参照してください。

注: [システム構成] ページからは、データベース サーバを設定できません。データベース サーバ設定用の対応する設定ファイルを更新します。

コンポーネント構成の変更およびサーバの追加の詳細については、「[管理ガイド](#)」を参照してください。

アプリケーション プール内の設定のリサイクル

[システム構成] で製品コンポーネントを設定した後、アプリケーション プール内の設定をリサイクルします。

次の手順に従ってください:

1. [スタート] メニューから、[コントロール パネル] を開きます。
2. [管理ツール] をダブルクリックし、次に、[インターネット インフォメーション サービス (IIS) マネージャー] をダブルクリックします。
3. [接続] ペインでサーバ名を展開し、[アプリケーション プール] をクリックします。
4. [アプリケーション プール] ペインで、[ITAM] を選択します。
5. [操作] ペインで [停止] をクリックし、次に [開始] をクリックします。

データベース サーバ

データベース サーバは、CA APM 用の Oracle または SQL Server データベース管理システムをホストする製品コンポーネントです。CA MDB はデータベース サーバにインストールされます。アプリケーション サーバ、ハードウェア照合エンジン、および他の製品コンポーネントは、CA MDB からデータを取得し、CA MDB にデータを格納します。

以下のフィールドについて説明します。

MS SQL Server インスタンス

構成中の MS SQL Server インスタンスの名前を定義します。SQL Server の名前付きインスタンスが複数存在する場合に限り、インスタンス名を入力します。インスタンスが 1 つだけ（デフォルト）の場合は、フィールドを空白のままにします。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

Web サーバ

Web サーバは、Web アプリケーションをホストし、CA APM ユーザ インターフェースを構築するメインサーバです。このサーバはユーザおよびアプリケーションサーバと通信します。

以下のフィールドについて説明します。

Web サーバまたはロード バランサの IP/ホスト

CA APM インストールでは、デフォルトで、このフィールドに Web サーバのホスト名が設定されます。

- Web サーバが 1 台の環境では、Web サーバのホスト名または IP アドレスを入力できます。
- Web サーバが複数台の環境では、Web サーバのホスト名またはロード バランサの IP アドレスを入力できます。

注: Web サーバをドメインネームシステム (DNS) に登録する際、Web サーバホスト名として登録されている名前とは別の名前を使用できます。そのような場合、このフィールドにはその別名を指定してください。

製品のインストール後に、追加の Web サーバ コンポーネントを構成できます。

注: コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

アプリケーション サーバ

アプリケーションサーバは、CA APM のデータベース サーバと Web サーバとを接続するサーバです。ビジネスおよびデータアクセス ロジックはアプリケーションサーバに配置されます。スケーラビリティを考慮して、アプリケーションサーバと Web サーバは 2 台の別個のサーバに配置されます。

複数のアプリケーションサーバをインストールできます。エクスポート サービス コンポーネントとストレージ マネージャ サービス コンポーネントは、いずれか 1 台のアプリケーションサーバに必ずインストールする必要があります。ただし、同じサーバである必要はありません。

以下のフィールドについて説明します。

アプリケーション サーバまたはロード バランサの IP/ホスト

CA APM インストールでは、デフォルトによって、このフィールドにアプリケーション サーバのホスト名が設定されます。

- アプリケーション サーバが 1 台の環境では、アプリケーション サーバのホスト名または IP アドレスを入力できます。
- アプリケーション サーバが複数台の環境では、アプリケーション サーバのホスト名またはロード バランサの IP アドレスを入力できます。

注: アプリケーション サーバをドメインネーム システム (DNS) に登録する際、アプリケーション サーバホスト名として登録されている名前とは別の名前を使用できます。 そのような場合、このフィールドにはその別名を指定してください。

製品のインストール後に、別のアプリケーション サーバコンポーネントを設定できます。

注: コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

ハードウェア照合エンジン

ハードウェア照合エンジンは、検出されたアセットを、別の論理リポジトリ内の対応する所有アセットに一致させるサービスです。ビジネス プラクティスに基づいてアセットを管理できます。ハードウェア照合エンジンは、データの取得と保存を CA MDB で行います。ハードウェア照合エンジンは 1 台以上のサーバにインストールできます。

製品のインストール後に、追加のハードウェア照合エンジン コンポーネントを構成できます。

注: コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

CA EEM

CA APM では、認証に CA EEM を使用します。認証に CA EEM を必要とする他の製品は、CA APM が使用する CA EEM サーバと同じサーバを使用できます。

- 複数の CA Technologies 製品についてセキュリティを一元管理するには、既存の CA EEM サーバの名前、場所、およびログイン認証情報を指定します。
- CA APM のセキュリティを他の CA Technologies 製品と分けて管理するには、既存の CA EEM がインストールされているサーバとは別の、任意の 1 台のアプリケーションサーバまたは Web サーバに CA EEM をインストールします。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

CA Business Intelligence

CA Business Intelligence はレポート環境を管理、監視、および設定します。CA APM は CA Business Intelligence を使用して、効果的な企業 IT 管理に必要な情報を統合、分析、および提示します。

CA Business Intelligence コンポーネントについて入力するログイン認証情報および接続情報の詳細については、「[CA APM と CA Business Intelligence の統合方法 \(P. 114\)](#)」を参照してください。

エクスポート サービス

エクスポート サービスは、CA APM のデータをエクスポートし、カンマ区切り値 (CSV) ファイルなどの形式で結果を保存します。このタスクを実行するため、エクスポート サービスはストレージマネージャ サービスと対話します。これにより、エクスポートファイルの保存先を指定できるようになります。

注: エクスポート サービスの詳細については、「ユーザ ガイド」を参照してください。

Data Importer エンジン サービス

Data Importer エンジン サービスは、列とフィールドをマッピングすることにより、大量の製品情報を CA MDB にインポートします。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

インポート ドライバ

インポート ドライバは、検出されたハードウェア データを CA SAM からエクスポートする作業を処理します。CA APM は、検出されたハードウェア データを使用して、所有権と検出のデータをリンクします。CA APM は、所有権データをエクスポートして CA SAM に戻します。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

LDAP データ インポートおよび同期サービス

LDAP データ インポートおよび同期サービスは、CA EEM または外部データ ソース (LDAP または CA SiteMinder) から CA APM にデータをインポートします。LDAP データ インポートおよび同期サービスをいずれかの Data Importer サーバ上にインストールします。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

ストレージ マネージャ サービス

ストレージ マネージャ サービスは、エクスポート済みファイル、添付ファイル、データインポートデータとマップのファイル、およびデータインポートと大量変更のログファイルを保存します。現在の製品リリースがリリース 12.6、12.7、または 12.8 のいずれかのバージョンである場合、現在のリリースをアンインストールする前に Storage フォルダの内容をバックアップする必要があります。リリース 12.9 のインストールが完了したら、フォルダの内容をリストアします。詳細については、「[以前のバージョンの製品のアンインストール \(P. 18\)](#)」を参照してください。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

CA APM 登録サービス

CA APM 登録サービスは、個々の CA APM CORA サービスを 1 つの主要サービスに統合します。CORA API を使用する別の CA Technologies 製品をインストールすることもできます。CA APM 環境で CORA API に変更を加えても、他の CA Technologies 製品による CORA API の使用には影響しません。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

サービス管理用の共通管理(CASM)

サービス マネージャの共通管理 (CASM) は、マルチテナント管理などの管理機能を CA APM に提供します。マルチテナントでは、複数の独立したテナント（およびそのユーザ）が CA APM の単一の実装を共有できます。

注: マルチテナントの実装の詳細については、「マルチテナントの実装方法」を参照してください。

イベント サービス

イベント サービスは、CA APM 内のイベントと通知のプロセスを管理します。イベントは、追跡の対象となる重要なアクティビティまたはデータ変更であり、CA APM 内で定義します。定義されたイベントが発生すると、イベントについて警告するため、適切なユーザまたは管理者に通知が送信されます。

通知機能を実行するため、イベント サービスは Web サービスを利用してワークフロー プロバイダ (CA Process Automation など) と対話します。ワークフロー プロバイダは自動化されたプロセスを管理します。ワークフロー プロバイダが CA Process Automation である場合、インストール時に CA Process Automation の既存のインスタンスを指定できます。また、CA Service Desk Manager および CA Service Catalog と CA Process Automation を共有することもできます。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

Common Asset Viewer

Common Asset Viewer を使用すると、照合を通してリンクされているアセットの検出データと所有データを表示できます。システム構成、オペレーティングシステム、システム デバイス、ファイル システムなどのアセットがあります。[アセットの詳細] ページでこのようなデータを表示するには、[所有済みの情報] リンクまたは [検出された情報] リンクをクリックします。

Common Asset Viewer を正常にインストールして実行するには、以下のコンポーネントが必要です。

- Apache Tomcat サーバ。このサーバは CA APM のインストールに含まれています。Apache Tomcat サーバポートのデフォルト値は 9080 です。この値はインストール後に変更できます。最初に [Apache Tomcat 設定ファイル内でポートを更新](#) (P. 23) します。次に、製品内でポートを変更します（[管理] - [システム構成] - [Common Asset Viewer]）。
- Java Development Kit (JDK) CA APM のインストールを開始する前に、Common Asset Viewer をインストールするアプリケーションサーバに [JDK をインストール](#) (P. 15) します。

Common Asset Viewer のインストール後、このコンポーネントはセキュリティで保護されないネットワーク通信 (http) 用に設定されます。セキュリティで保護されたネットワーク通信 (https) 用にコンポーネントを設定するには、最初に、セキュアソケットレイヤ (SSL) プロトコルがサポートされるように Apache Tomcat サーバ (Common Asset Viewer がインストールされている) を設定します。次に、Web 設定ファイル内で Common Asset Viewer コンポーネントの設定を変更する必要があります。

重要: CA APM の Tomcat ポート番号は、デフォルトで 9080 です。CA APM と統合する別の製品がこのポート番号を使用する場合、競合が発生しないように CA APM 内のポート番号を変更してください。

WCF サービス

Windows Communications Foundation (WCF) サービスは、CA APM に Web サービスを実装します。Web サービスによって、標準ベースのインターフェースを使用して、CA APM と統合するクライアントアプリケーションを構築できます。

Web サービスを通じて、外部クライアントアプリケーションから CA APM オブジェクトの作成、検索、更新、コピー、および削除を実行できます。割り当てられているユーザ役割によって、CA APM の Web サービスにアクセスする権限の有無が決定されます。また、役割によって表示や変更を実行できるオブジェクトとデータ (クラスと属性) が制限されます。

WCF サービスコンポーネント用のサーバ名を指定します。WCF サービスプロトコル設定を変更できます。製品のインストール後、WCF サービスコンポーネントの設定を変更できます。

注: コンポーネント構成の変更およびサーバの追加の詳細については、「[管理ガイド](#)」を参照してください。

Software Asset Management (SAM)

ソフトウェアアセット管理コンポーネントを使用すると、CA SAMを通してソフトウェアアセット管理能力を有効にできます。CA APMおよびCA SAMの両方を実装すると、組織内のハードウェアおよびソフトウェアアセットの両方の管理を調整できます。CA APMはハードウェアアセットデータを管理し、CA SAMはソフトウェアアセットとライセンスデータを管理します。両方の製品で必要な共通のデータは共有されます。

製品インストールでは、ソフトウェアアセット管理コンポーネントを設定しません。製品をインストールした後、[システム構成]でこのコンポーネントを設定します。

注: 製品のインストール後は、会社のニーズに合わせて、コンポーネント構成の変更および追加コンポーネントの構成が可能です。コンポーネント構成の変更およびサーバの追加の詳細については、「管理ガイド」を参照してください。

CA APM の修復

CA APMをインストールしている場合、インストールプログラムを使用してインストールエラーを修復できます。これらのエラーは製品またはそのコンポーネントのいずれかに関連している可能性があります。

次の手順に従ってください:

1. CA APMをインストールしたコンピュータに管理者としてログインします。
2. インストールファイルが含まれるフォルダを開き、ルートディレクトリ内の `Setup.exe` ファイルをダブルクリックします。
インストール ウィザードが起動します。
3. [修復] をクリックします。
4. 修復プロセスの画面の指示に従います。

CA APM のアンインストール

さまざまな理由によって、CA APMをコンピュータからアンインストールすることができます。たとえば、コンピュータを別の目的に使用する場合や、コンポーネントを別のコンピュータに移動する場合に、CA APMをアンインストールすることができます。

次の手順に従ってください:

1. CA APM をインストールしたコンピュータに管理者としてログインします。
2. インストール ファイルが含まれるフォルダを開き、ルートディレクトリ内の **Setup.exe** ファイルをダブルクリックします。
インストール ウィザードが起動します。
3. [アンインストール] をクリックします。
アンインストールが開始されます。
4. 画面の指示に従って、アンインストール プロセスを実行します。

第4章: リリース 11.3.4 から リリース 12.9 に CA APM データをマイグレートする方法

このセクションには、以下のトピックが含まれています。

[リリース 11.3.4 から リリース 12.9 に CA APM データをマイグレートする方法 \(P. 43\)](#)

リリース 11.3.4 から リリース 12.9 に CA APM データをマイグレートする方法

システム管理者は、リリース 11.3.4 から リリース 12.9 に CA APM データを移動する場合はデータのマイグレーションを行います。リリース 12.9 のインストール後、CA 管理データベース (CA MDB) 構造がアップグレードされます。また、データのマイグレーションを求めるメッセージが表示されます。

重要: リリース 12.9 では、リリース 12.8 でマイグレートされなかったオブジェクトをマイグレートできます。これらのオブジェクトとは、コストと支払いの拡張および監査、カスタム関係と監査、および関係の拡張および監査です。このリリースでは、カスタム関係および製品提供されなかった関係を含むすべての関係がマイグレートされます。以前リリース 11.3.4 からデータをマイグレートした場合は、これらのオブジェクトのデータのみをマイグレートできます。再度完全なデータマイグレーションを実行する必要はありません。

アップグレードのインストールとデータのマイグレートは個別のプロセスです。

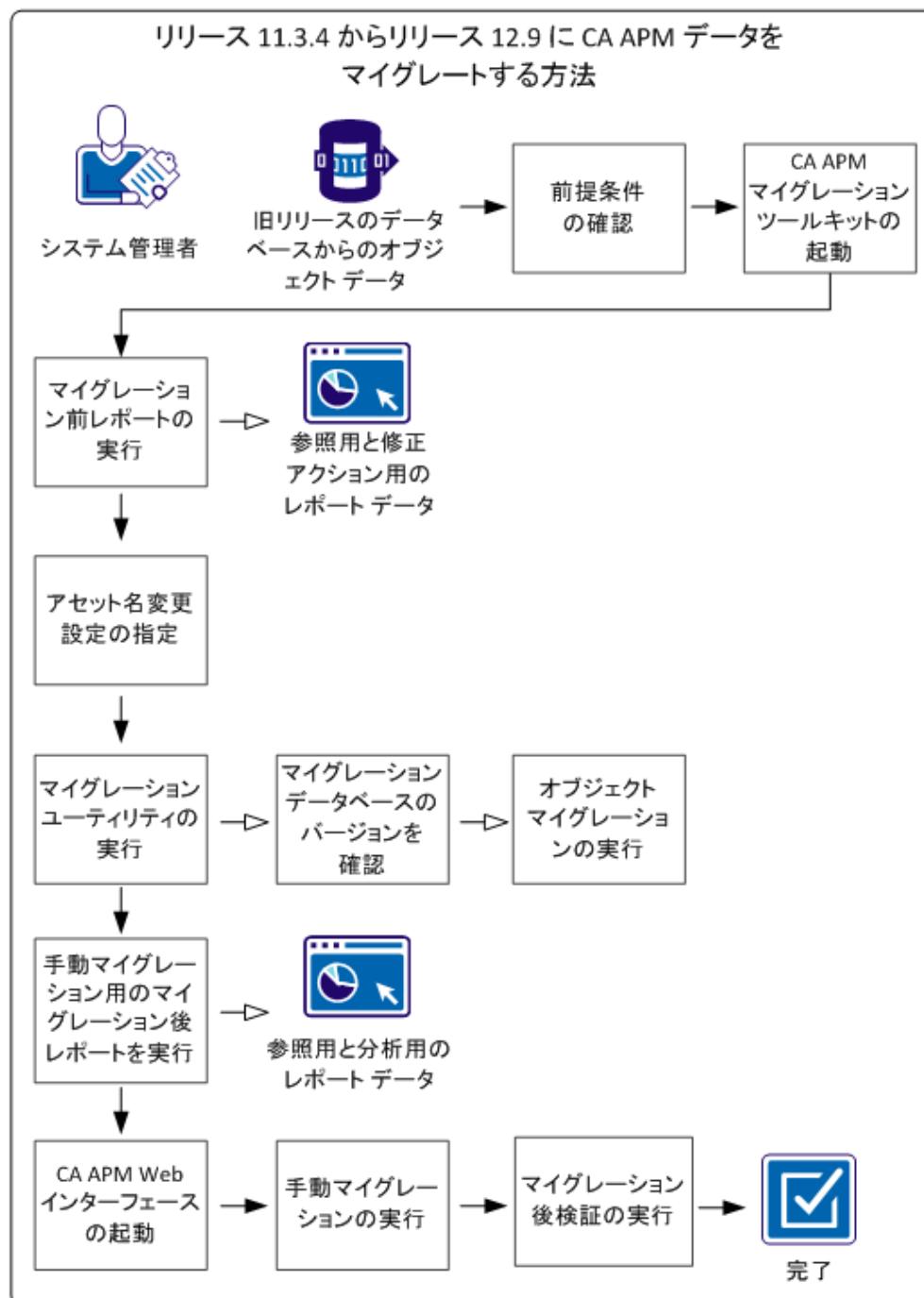
- **アップグレード。** アプリケーションおよびデータベース構造を新しいバージョンに更新します。
- **マイグレート。** 古いデータベース構造からアップグレード中に作成された新しいデータベース構造にデータを変換または移動します。

CA APM マイグレーションツールキットには、リリース 11.3.4 データベース構造から新しいリリース 12.9 データベース構造に CA APM データをマイグレートするための以下のツールが含まれています。

- **マイグレーション ドキュメント。** マイグレーション レポートの生成、マイグレーションユーティリティの実行、および手動によるオブジェクトマイグレーションの手順が記載されています。

- **マイグレーション レポート。**マイグレーション プロセス中にユーザに役立つレポートを生成します。マイグレーション中に発生する可能性のある問題を回避するために、[マイグレーションユーティリティ \(P. 63\)](#)を実行する前に[マイグレーション前レポート \(P. 53\)](#)を生成します。マイグレーションユーティリティを実行した後に、[マイグレーション後レポート \(P. 69\)](#)を生成します。マイグレーション後レポートは、マイグレーションユーティリティを使用してマイグレートできない古いデータベース構造を手動でマイグレートするときに役立ちます。
- **重複アセット名コンフィギュレータ。**重複するアセット名に適用する名称変更設定を指定します。
- **マイグレーションユーティリティ。**古いデータベース構造内の選択したオブジェクトを新しいデータベース構造に移動する自動手順を提供します。

以下の図は、システム管理者がデータをマイグレートする手順を示します。



CA APM データをマイグレートするには、以下の手順に従います。

1. [前提条件を確認します](#) (P. 47)。
2. [CA APM マイグレーションツールキットを起動します](#) (P. 53)。
3. [マイグレーション前レポートを実行します](#) (P. 53)。
参照用と修正アクション用 (P. 55) のマイグレーション前レポートデータを使用します。
4. [アセット名変更設定を指定します](#) (P. 61)。
5. [マイグレーションユーティリティを実行します](#) (P. 63)。
 - a. [マイグレーションデータベースのバージョンを確認します](#) (P. 65)。
 - b. [オブジェクトマイグレーションを実行します](#) (P. 67)。
6. [手動マイグレーション用のマイグレーション後レポートを実行します](#) (P. 69)。
参照用と分析用 (P. 71) にマイグレーション後レポートデータを使用します。
7. [CA APM Web インターフェースを起動します](#) (P. 76)。
8. [手動マイグレーションを実行します](#) (P. 77)。
9. [マイグレーション後検証を実行します](#) (P. 95)。

例: リリース 11.3.4 から リリース 12.9 への CA APM データのマイグレーション

ミリアムは Document Management Company で CA APM システム管理を担当しています。ミリアムは CA APM リリース 11.3.4 を リリース 12.9 にアップグレードし、古いデータ構造からアップグレードしたデータ構造にデータをマイグレートしたいと考えています。ミリアムは、新リリースへのマイグレーションおよびアップグレードを開始するための前提条件を確認します。

ミリアムは、CA APM マイグレーションツールキットを起動します。まず、マイグレーション前レポートを生成して確認します。このレポートは、マイグレーションユーティリティを実行する前に、古いデータ構造で修正する必要があるオブジェクトを識別する上で役立ちます。レポートの一部は、後で同じ名前を持つアセットの新しい名前を設定したり、手動マイグレーションを実行したりするために使用します。

古いデータ構造の修正を行った後、ミリアムは重複するアセット名を識別するために、重複アセット名レポートを確認します。ミリアムは重複アセット名コンフィギュレータを開き、重複するアセット名用の名称変更設定を選択します。マイグレーションユーティリティを実行すると、これらのアセット名が変更されます。

ミリアムはマイグレーションユーティリティを開きます。次に、データベース接続をテストして、正しい CA APM 旧データベース バージョンが正しい新リリースデータベース バージョンにマイグレートされることを確認します。

ミリアムはマイグレートするオブジェクトを選択し、マイグレーションユーティリティを実行します。進捗状況とステータス メッセージを参照して、マイグレーションプロセスを監視します。すべてのオブジェクトがマイグレートされたら、マイグレーションの監査履歴オブジェクトが使用可能になります。ミリアムは監査履歴オブジェクトを選択し、マイグレーションユーティリティを再実行します。

マイグレーションユーティリティ プロセスが完了したら、マイグレーション後レポートを生成します。このレポートには、正常にマイグレートされたデータとマイグレートされなかったデータが示されます。マイグレートされなかったデータは、手動でマイグレートする必要があります。

手動マイグレーションは、アップグレードされた CA APM リリース 12.9 Web インターフェースを使用して実行します。ミリアムは Web インターフェースを起動します。マイグレーション後レポートの情報を使用して、手動マイグレーションを実行します。マイグレートされたデータを確認し、マイグレーション処理を完了します。

前提条件の確認

データを正しくマイグレートできるように、以下の順番で前提条件を満たしていることを確認します。

注: マイグレーションの前提条件の多くは リリース 12.9 のインストール中に満たされます。「実装ガイド」では、インストールに関する詳しい情報を提供します。

1. 以下の情報に目を通します。
 - [CA IT Asset Manager 製品ロードマップ](#)
 - [CA IT Asset Manager 12.9 と旧リリース \(CA IT Asset Manager 12 および CA Asset Portfolio Management 11.3.4\) の相違点](#)
 - [CA APM 製品ページ](#)で公開されている既知の問題。
 - [リリース 11.3.4 と リリース 12.9 との関係の相違点 \(P. 50\)](#)

2. 現在のリリース 11.3.4 パッチ レベルが累積パッチ 14 以上であることを確認します。現在のパッチ レベルが不明であるか、または累積パッチ 14 以上ではない場合、CA サポート Web サイトから最新の CA APM リリース 11.3.4 累積パッチをダウンロードして適用します。
3. CA サポート Web サイトから Kettle をダウンロードし、CA APM リリース 12.9 がインストールされているサーバにインストールします。以下の手順に従って Kettle をダウンロードします。
 - a. 以下のリンクをクリックしてください。
ftp://ftp.ca.com/pub/ca_itam/ca_apm/apm12_8/pentaho-kettle-4.4.0.zip
 - b. 希望のディレクトリに pentaho-kettle-4.4.0.zip 保存します。
例: C:¥Program Files (x86)¥CA¥ITAM¥
 - c. pentaho-kettle-4.4.0.zip の内容を展開します。
Kettle という名前の新しいフォルダが作成されます。フォルダのパスを変更します。
4. 以下の手順を実行して、Kettle 用の環境変数を作成します。
 - a. [スタート] - [ファイル名を指定して実行] をクリックし、「sysdm.cpl」と入力して [システムのプロパティ] にアクセスします。
 - b. [詳細設定] タブをクリックします。
 - c. [環境変数] をクリックします。
 - d. システム環境変数セクションの [新規] をクリックし、以下の情報を入力します。

変数名

KETTLE_HOME

変数値

Kettle フォルダへのパス。

注: 「data-integration」フォルダが含まれる親フォルダ (C:¥Program Files (x86)¥CA¥ITAM¥Kettle など) にパスが設定されていることを確認してください。

5. CA APM および他の統合サービス マネジメント製品用の以下のサービスおよびスケジュールされたタスクを停止します。
 - CA Unicenter Asset Portfolio Management (CA APM)
 - CA APM キャッシュ サービス
 - CA APM 通知サービス
 - 自動照合タスク
 - CA Service Catalog リリース 12.8 および リリース 12.9
 - CA Service Catalog
 - CA Service Accounting
 - CA Service Catalog リリース 12.7
 - CA Service Accounting
 - CA Service Fulfillment
 - CA Service Repository Agent
 - CA Service View
 - CA Service Desk Manager
 - CA Service Desk Manager サーバ
 - CA Client Automation
 - マイグレートする CA MDB を直接共有する CA Client Automation エンタープライズマネージャおよびドメインマネージャに対して、*caf stop* を使用して CA Client Automation サービスを停止します。
 - マイグレートする CA MDB に対する補足エンジン プロセスを実行するその他のサービスに対して、*caf stop* を使用して CA Client Automation を停止します。
 - マイグレートする CA MDB に対してデータベース同期タスクを実行するエンジン プロセスに対して、DSM エクスプローラを使用してデータベース同期を停止します。
 - エンタープライズにレポートする各 CA Client Automation ドメインマネージャに対して、DSM エクスプローラを使用してエンタープライズに対するエンジン レプリケーションタスクを停止します。

6. CA APM リリース 11.3.4 データベースをバックアップします。
 7. CA APM リリース 12.9 インストールメディアのヘルス チェック ユーティリティ フォルダにある CA マイグレーション ヘルス チェック ユーティリティを見つけています。CA APM リリース 11.3.4 データベース上でこのユーティリティを実行します。

重要: ユーティリティの実行について詳細は、「CA マイグレーション ヘルス チェック ユーティリティ ユーザ ガイド」(インストール メディアにあります) を参照してください。
 8. Oracle の Web サイト (<http://www.oracle.com>) から JRE 1.7 をダウンロードし、CA APM リリース 12.9 をインストールするサーバに JRE をインストールします。
 9. CA MDB 用の Microsoft SQL Server トランザクション ログ シーケンス 設定を確認し、設定が一括ロード向けに設定されていることを確認します。以下の手順を実行して、この情報を取得します。
 - a. Web ブラウザで、Microsoft の Web サイト (<http://www.microsoft.com>) を開き、「トランザクション ログ の管理」を検索します。
 - b. 記事の指示に従います。
 10. リリース 11.3.4 データベースに リリース 12.9 をインストールします。
- 注:** 以前に リリース 11.3.4 のデータを リリース 12.8 にマイグレートした場合は、マイグレートされたオブジェクトのマイグレーション ステータスを保持する手順を実行する必要があります。マイグレーション ステータスを保持する方法の詳細については、「実装ガイド」のインストールの計画セクションを参照してください。
11. リリース 12.9 サービスが実行されていないことを確認します。データ マイグレーション ユーティリティを実行するか、または手動マイグレーションのためにレポートを生成する前に CA APM マイグレーション ツールキットを終了した場合、これらのサービスがまだ実行されている場合があります。

リリース 11.3.4 と リリース 12.9 との関係の相違点

CA APM リリース 11.3.4 には、標準の関係があらかじめ用意されています。また、新しいカスタム関係を追加できます。関係のサポートは リリース 12.9 で変更されました。

リリース 12.9 で製品提供されていない関係

リリース 11.3.4 で提供されている以下の関係および関連リンクは、リリース 12.9 では製品提供されていません。ただし、これらの関係は リリース 12.9 のカスタム関係にマイグレートされます。

- アクティビティ概要
- 連絡先（予算マネージャ、サポート元、ユーザ）
- 依存（依存）
- 製品展開（発展）
- 製品アップグレード（アップグレード）
- ユーザ配置（配置先）
- ソフトウェア配置（配置）

リリース 12.9 で製品提供されている関係

リリース 12.9 で製品提供されているリリース 11.3.4 の関係は以下のとおりです。

- アセットの割り当て（ライセンス供与先）
- 企業買収（買収先（親会社））
- 会社の割り当て（ライセンス供与先）
- 連絡先の割り当て（ライセンス供与先）
- 管理ドキュメント（管理元）
- イメージパーティション（パーティショニングされた CPU）
- 法改正（改正）
- ロケーションの割り当て（ライセンス供与先）
- ハードウェアアセット構成（一般コンポーネント、特定のコンポーネント）
- ハードウェアモデル構成（一般コンポーネント）

関係情報を格納するデータ構造が変更されました。リリース 11.3.4 から リリース 12.9 に関係情報を移動するには、マイグレーションユーティリティは関係テンプレート名および関係テンプレートリンク名によって関係を識別する必要があります。

必要な作業：マイグレーションユーティリティを実行する前に、関係テンプレートまたは関係テンプレートリンク名の変更された名前を元のリリース 11.3.4 の値に変更します。

ユーザ インターフェースの変更

CA APM リリース 11.3.4 では、関係およびリンクはユーザ インターフェース内の別個のセクションで表示および変更されます。リリース 12.9 では、関係およびリンクは単一のエンティティに統合され、ユーザ インターフェース内の同じセクションで表示および変更されます。

リリース 12.9 の関係名のメニュー項目の一部は、リリース 11.3.4 とは異なります。以下の表に、リリース 11.3.4 の関係、およびそれらと関連付けられたリリース 12.9 の関係メニュー項目を示します。反対方向から関係を表示する場合、一部の関係メニュー項目のラベルは異なります。たとえば、[会社の割り当て] 関係は、ソフトウェアから表示したときは [会社配置]、会社から表示したときは [ソフトウェア配置] と表示されます。

リリース 11.3.4 関係	リリース 12.9 エンティティ	リリース 12.9 関係
アセットの割り当て	アセット (ソフトウェア)	アセット配置
アセットの割り当て	アセット (ハードウェア)	ソフトウェア配置
企業買収	会社	企業買収
会社の割り当て	アセット (ソフトウェア)	会社配置
会社の割り当て	会社	ソフトウェア配置
連絡先の割り当て	アセット (ソフトウェア)	連絡先配置
連絡先の割り当て	連絡先	ソフトウェア配置
管理ドキュメント	リーガルドキュメント	規程リーガルドキュメント
イメージパーティション	アセット	イメージパーティション
法律改正	リーガルドキュメント	法律改正
ロケーションの割り当て	アセット (ソフトウェア)	ロケーション配置
ロケーションの割り当て	ロケーション	ソフトウェア配置
ハードウェアアセット構成 (一般コンポーネント)	アセット	モデル構成
ハードウェアアセット構成 (特定のコンポーネント)	アセット	アセット構成
ハードウェアモデル構成	モデル	モデル構成

CA APM マイグレーションツールキットを起動します。

リリース 11.3.4 を リリース 12.9 にアップグレードするときに、アップグレードを実行しているコンピュータに CA APM マイグレーションツールキットがインストールされます。アップグレードが完了したら、すぐに新しいリリースのデータ構造に CA MDB データをマイグレートすることをお勧めします。

アップグレードを実行したコンピュータで、CA APM マイグレーションツールキットを起動します。

次の手順に従ってください:

- [スタート]、[すべてのプログラム]、[Asset Portfolio Management]、[CA APM マイグレーションツールキット] の順番にクリックします。

マイグレーション前レポートの実行

CA MDB をマイグレートする前に、マイグレーション前レポートを実行します。マイグレーション前レポートは、以下のタイプのデータを識別します。

- データマイグレーション中に問題を引き起こす可能性のあるデータ。[マイグレーションユーティリティ](#) (P. 63) を実行する前に、CA MDB 内のデータを修正します。たとえば、リリース 11.3.4 で提供された関係テンプレートの名前が変更されていると、関係のマイグレーション中に問題が発生する場合があります。マイグレーションを開始する前に、関係レポートで名前が変更されたテンプレートを確認して、製品提供の元のテンプレート名に戻します。
- マイグレーション設定を決定するために分析を必要とするデータ。
- マイグレーションユーティリティではマイグレートしないが、更新された製品の機能により手動でマイグレートできるデータ。このデータは、マイグレーションユーティリティの実行後、[手動マイグレーション](#) (P. 77) 時に参照します。このデータはリリース 12.9 データベース構造にマイグレートされないので、古いデータをマイグレートする前にこれらのレポートでデータをキャプチャする必要があります。これらのレポートを保存しておき、後でリリース 12.9 の[手動マイグレーション](#) (P. 77) を実行するときに参照してください。
- リリース 11.3.4 でサポートされているがリリース 12.9 ではサポートされないデータ。このデータはマイグレーションユーティリティでマイグレートすることはできません。また、リリース 12.9 を使用して追加することもできません。これらのレポートはサポートされないデータを識別し、古い参照情報を提供します。

注: リリース 12.9 でサポートされる機能の詳細については、CA サポート Web サイトで、「[CA IT Asset Manager 製品ロードマップ](#)」および「[CA IT Asset Manager 12.8 と旧リリース \(CA IT Asset Manager 12 および CA Asset Portfolio Management 11.3.4\) の相違点](#)」というドキュメントを参照してください。

次の手順に従ってください:

1. CA Asset Portfolio Management マイグレーションツールキットのメイン ウィンドウで、[マイグレーション レポート] をクリックします。

[マイグレーション前レポート] 領域の以下のチェック ボックスがオンになっています。

- カスタム インデックス
- 重複アセット名
- 照合
- 関係

注: 作成したくないレポートがある場合は、作成するレポート タイプのみを選択します。

2. [レポート出力フォルダ] 領域で [参照] をクリックして、レポートを保存する出力フォルダを選択します。

3. [レポートの生成] をクリックします。

ステータス メッセージが [メッセージ] 領域に表示され、レポート生成プロセスをモニタできます。

レポート出力フォルダを開いてレポートを表示するかどうかをたずねられます。

4. [はい] をクリックします。

Windows エクスプローラが開きます。レポート ツールは、前の手順で選択した各レポート チェック ボックスに対応するフォルダを作成します。

5. レポート フォルダに移動し、フォルダを開きます。

レポートはカンマ区切り値 (CSV) 形式で表示されます。

6. レポートを右クリックして、[プログラムから開く]、[Excel] を順番に選択して、レポートを表形式で開いて表示します。

[レポート データ](#) (P. 55)が表形式で表示されます。テーブルの見出しへ最初の行に表示されます。

注: レポートをクリックして、テキスト エディタで CSV フォーマットのレポートを表示できます。

参照用と修正アクション用のマイグレーション前レポート データ

レポートツールは、テキストエディタで開くことができる CSV 形式でレポートを生成します。レポートのフィールド名およびフィールド値はカンマで区切られます。Excel でレポートを開くこともできます。その場合、表形式でデータが表示されます。Excel でレポートを開くと、フィールド名は列見出しとなり、フィールド値は各見出しの下の行に表示されます。

以下のマイグレーション前レポートは、マイグレーションの前に CA MDB で変更する必要があるデータに関する情報を提供します。これにより、関連するオブジェクトを リリース 12.9 CA MDB データ構造に正常にマイグレートできます。

- [カスタムインデックス レポート](#) (P. 56)
- [関係レポート](#) (P. 56)

以下のレポートは、マイグレーション設定を決定するために分析するデータを識別します。

- [重複アセット名 レポート](#) (P. 59)
- 照合レポート：
 - [主要変換リスト クエリ レポート](#) (P. 60)

以下のマイグレーション前レポートは、マイグレーションユーティリティ [リティ](#) (P. 63) の実行後、[手動マイグレーションを実行](#) (P. 77) する際に使用するデータを識別します。これらのレポートを保存して、手動マイグレーション中に参照します。

- 照合レポート：
 - [主要タスク クエリ レポート](#) (P. 60)
 - [タスク追加アセット レポート](#) (P. 60)
 - [カスタマイズ検索レポート](#) (P. 61)

以下のレポートは、リリース 12.9 でサポートされない、古い参照情報を提供するデータを識別します。

- 照合レポート：
 - [変換リスト使用廃止 レポート](#) (P. 61)
 - [変換リスト未変換 レポート](#) (P. 61)

カスタム インデックス レポート

カスタム インデックス レポートは、リリース 11.3.4（または旧リリース）のフィールドにカスタマイズされて追加されたインデックスを識別します。これらのインデックスは、リリース 12.9 でパフォーマンスの問題を引き起こす可能性があります。[データベースからカスタム インデックスを削除する \(P. 56\)](#) ことをお勧めします。このレポートには、カスタム インデックスを削除するために使用できる SQL ステートメントが付属します。

データベースからカスタム インデックスを削除する

パフォーマンスの問題を回避するために、データベースからカスタム インデックスを削除することをお勧めします。マイグレーションユーティリティを実行する前に、インデックスを削除してください。[カスタム インデックス レポート \(P. 56\)](#) は、カスタム インデックスを削除するために使用できる情報を提供します。

次の手順に従ってください:

1. カスタム インデックス レポートを開きます。
2. レポートの ドロップ SQL という列から SQL ステートメントをコピーします。
注: ステートメントの最初と最後の引用符は削除してください。
3. SQL ステートメントをお好みのツール（Microsoft SQL Server Management Studio、Oracle SQL Developer など）にペーストして実行します。
以下の項目が削除されます。
 - カスタム インデックス
 - arg_index_member テーブルのインデックス定義
 - arg_index_def テーブルのインデックス情報

関係レポート

関係レポートは、11.3.4 に用意されている元の製品提供の関係テンプレート名が変更された関係テンプレートを識別します。マイグレーション前に、CA MDB に存在するこのデータを変更します。

このツールは、複数の言語で関係レポートを生成します。リリース 11.3.4 で設定されている言語に対応するレポートを使用します。

このレポートには、関係テンプレートまたは関係テンプレートリンクの以下のステータスが示されます。

カスタマイズ

関係テンプレートまたは関係テンプレートリンクが、リリース 11.3.4 でユーザによって追加されたか、その名前が変更されたことを示します。

- 関係がリリース 11.3.4 で追加された場合、その関係は リリース 12.9 で製品提供されたものではありません。ただし、この関係はカスタム関係にマイグレートされます。
- 関係がリリース 11.3.4、および リリース 12.9 で製品提供されている場合、関係を リリース 12.9 で製品提供された関係にマイグレートできます。また、関係テンプレートまたは関係テンプレートリンクの名前をそれらの元の値に変更します。

マイグレーション ユーティリティでマイグレート

関係テンプレートまたは関係テンプレートリンクが リリース 12.9 でサポートされており、ユーティリティによってマイグレートされることを示します。

サポートされていません

リリース 12.9 で製品提供されていない関係テンプレートまたは関係テンプレートリンクであることを示します。Migration Utility は、これらの環境をカスタム関係にマイグレートします。

見つからない

リリース 11.3.4 の製品提供の関係テンプレートまたは関係テンプレートリンクがユーザのデータベースに見つからないことを示します。関係テンプレートまたは関係テンプレートリンクの名前が変更されており、リリース 12.9 で製品提供されている場合、関係テンプレートまたは関係テンプレートリンクの名前を元の値に変更してから関係を リリース 12.9 にマイグレートします。

マイグレーション前の名前変更

リリース 11.3.4 で名前が変更された関係テンプレートまたは関係テンプレートリンクを元の名前に戻してからマイグレートする必要があることを示します。

名前が変更された製品提供の関係テンプレートをマイグレーションに追加する場合は、以下のアクションを完了します。

- [名前が変更された関係テンプレートを元の製品提供の名前に変更します](#) (P. 58)。
- [名前が変更された関係テンプレートリンクを元の製品提供の名前に変更します](#) (P. 58)。

名前が変更された関係テンプレートを元の製品提供の名前に変更する

[マイグレーションユーティリティを実行する](#) (P. 63)前に、変更された関係テンプレート名をリリース 11.3.4 から元の製品提供の関係テンプレート名に変更します。

関係テンプレート名を変更するには SQL ステートメントを実行します。以下の手順は、関係レポートで [マイグレーション前の名前変更] ステータスを持つ各エントリ、および [関係テンプレートの名前変更] に指定されている値に対して実行します。

次の手順に従ってください:

1. お好みのツール (Microsoft SQL Server Management Studio、Oracle SQL Developer など) から以下の SQL ステートメントを実行します。

注: かっこおよびかっこ内のテキストはプレースホルダです。プレースホルダ名は関係レポート上の列名を表します。

```
UPDATE arg_actiondf
SET adtext = '{関係テンプレートの名前変更}'
WHERE adtext = '{関係テンプレートの名前変更}'
    AND adlobty IN (SELECT slentry
                     FROM arg_strlst
                     WHERE slid = 9
                     AND slvalue1 = '{関係オブジェクト タイプ}')
```

2. プレースホルダを関係レポート上の同名の列の値に置換します。たとえば、レポート [関係テンプレートの名前変更] 列は、製品提供の名前アクティビティ サマリを識別します。{関係テンプレートの名前変更} を [アクティビティ サマリ] に置換します。

名前が変更された関係テンプレートリンクを元の製品提供の名前に変更する

[マイグレーションユーティリティを実行する](#) (P. 63)前に、変更された関係テンプレートリンク名をリリース 11.3.4 から元の製品提供の関係テンプレートリンク名に変更します。

関係テンプレートリンク名を変更するには SQL ステートメントを実行します。以下の手順は、関係レポートで [マイグレーション前の名前変更] ステータスを持つ各エントリ、および [リンクの名前変更] に指定されている値に対して実行します。

次の手順に従ってください:

1. お好みのツール (Microsoft SQL Server Management Studio、Oracle SQL Developer など) から以下の SQL ステートメントを実行します。

注: かつこおよびかつこ内のテキストはプレースホルダです。プレースホルダ名は関係レポート上の列名を表します。

```
UPDATE arg_linkdef
SET ndtext = '{リンクの名前変更}'
WHERE ndtext = '{リンク名}'
    AND nd2objt IN (SELECT slentry
                     FROM arg_strlst
                     WHERE slid = 9
                     AND slvalue1 = '{リンク オブジェクト タイプ}')
```

2. プレースホルダを関係レポート上の同名の列の値に置換します。たとえば、レポートでは、[リンクの名前変更] 列は製品提供のテンプレートリンク名を承認ユーザとして識別します。{リンクの名前変更} を [承認ユーザ] に置換します。

重複アセット名レポート

重複アセット名レポートは、重複するアセット名を識別します。

注: 同じアセット名を共有していて、以下の登録フィールドに値が設定されていないアセットだけが対象になります。

- シリアル番号
- 代替アセット ID
- ホスト名
- DNS 名
- Mac アドレス
- シリアル番号

マイグレーション中、CA APM マイグレーションツールキットは、CA MDB 内の重複アセット名に自動で一意のアセット名を設定できます。重複アセット名レポートを使用して、[アセット名変更設定の指定 \(P. 61\)](#)方法を決定してください。

照合レポート

レポートツールは以下の照合レポートを生成します。

- [主要変換リスト クエリ レポート \(P. 60\)](#)
- [変換リスト使用廃止レポート \(P. 61\)](#)
- [変換リスト未変換レポート \(P. 61\)](#)
- [主要タスク クエリ レポート \(P. 60\)](#)
- [タスク追加アセットレポート \(P. 60\)](#)
- [カスタマイズ検索レポート \(P. 61\)](#)

主要変換リスト クエリ レポート

主要変換リスト クエリ レポートは、会社、オペレーティング システムおよびモデル用の古い変換リストデータを識別します。このレポートでデータを分析して、マイグレーションユーティリティを使用して旧型の変換リストを対応するリリース 12.9 正規化ルールへ移行するか、手動でリストを移行するか決定します。

[変換リストを手動でマイグレートする \(P. 93\)](#)場合は、主要変換リスト クエリ レポートのデータを使用します。

主要タスク クエリ レポート

マイグレーション前主要タスク クエリ レポートは、[マイグレーションユーティリティ \(P. 63\)](#)を実行した後に参照するデータを識別します。このレポートは、リリース 11.3.4 のレガシー照合タスクに関する情報を提供します。このレポートを保存しておき、[ハードウェア照合タスクの手動マイグレーション \(P. 92\)](#)時に参照して、リリース 12.9 で照合ルールを作成します。

タスク追加アセットレポート

タスク追加アセット レポートは、[マイグレーションユーティリティ \(P. 63\)](#)の実行後、手動マイグレーションを実行する時に使用するデータを提供します。このレポートは、リリース 11.3.4 の所有アセットを追加する古い照合タスクを識別します。このレポートを保存しておき、[ハードウェア照合タスクの手動マイグレーション \(P. 92\)](#)時に参照してください。

カスタマイズ検索レポート

カスタマイズ検索レポートは、[マイグレーション ユーティリティ \(P. 63\)](#)の実行後、手動マイグレーションを実行するときに使用するデータを提供します。このレポートは、リリース 11.3.4 の古いハードウェア照合カスタマイズ検索を識別します。リリース 12.9 は事前定義済みハードウェア照合レポートを提供します。これらのレポートは、リリース 12.9 でも提供される CA Business Intelligence を使用してカスタマイズできます。レポートを保存し、[ハードウェア照合検索の手動マイグレーション \(P. 94\)](#)中にそれを参照してください。

変換リスト使用廃止レポート

変換リスト使用廃止レポートは、廃止されて リリース 12.9 ではサポートされない、リリース 11.3.4 のハードウェア照合の古い変換リストを識別します。このレポートは参考用です。対処は不要です。

変換リスト未変換レポート

変換リスト未変換レポートは、見つからないか、無効なため リリース 12.9 に移行されないエントリを持つリリース 11.3.4 のハードウェア照合レガシー変換リストを識別します。変換リストは移行されますが、サポートするデータが古いデータベースにないエントリは移行されません。

移行後に変換リスト未変換レポートおよび[主要変換リスト クエリ レポート \(P. 60\)](#)のデータを使用して、[欠けているエントリを正規化リストに追加 \(P. 94\)](#)してください。

アセット名変更設定の指定

リリース 12.9 で、登録にはアセット名、シリアル番号の代替アセット ID、ホスト名、DNS 名および MAC アドレスが含まれます。一意のアセット名は各アセットオブジェクトに必要です。この要件は リリース 11.3.4 にありませんでした。したがって、ユーザの CA MDB はアセット登録に一意でないアセット名を持つことができました。CA APM マイグレーションツールキットは、マイグレーション中にユーザの CA MDB 内の各重複したアセット名に対して自動的に一意のアセット名を設定できます。

CA APM マイグレーションツールキットは、重複したアセット名の名前を変更するために設定を使用します。 [CA APM マイグレーション ユーティリティ重複アセット名の設定] ダイアログ ボックス上の設定を選択します。マイグレーション ユーティリティを実行すると、重複したアセットは リリース 12.9 データベースで名前を変更されます。

注: 一意のアセット名は、リリース 12.9 の Common Registration API (CORA) によるアセット登録の要件です。CORA を有効にしない場合は、アセット登録は発生しません。そのため、アセット名前変更の設定を指定する必要はありません。

次の手順に従ってください:

1. [重複アセット名レポート](#) (P. 59) を確認します。
2. CA Asset Portfolio Management Migration Toolkit のメイン ウィンドウで、[重複アセット名コンフィギュレータ] をクリックします。
3. 以下の名前変更設定のいずれかを選択します。

置換

重複したアセット名を別のフィールドの値に置換します。ドロップダウンリスト内のこのフィールドを選択します。

注: ドロップダウンリスト内のフィールドは、[重複アセット名レポート](#) (P. 59) の見出しと同じフィールドです。

増分設定は自動的に選択されロックされます。置換設定が重複アセット名をもたらす場合は、増分を設定に追加することで名前変更が一意であることが保証されます。

連結

重複アセット名の最後に 1 つ以上のフィールドの値を追加します。ドロップダウンリスト内の 4 つまでのフィールドを選択します。

注: ドロップダウンリスト内のフィールドは、[重複アセット名レポート](#) (P. 59) の見出しと同じフィールドです。

増分設定は自動的に選択されロックされます。連結設定が重複アセット名をもたらす場合は、増分を設定に追加することで名前変更が一意であることが保証されます。

増分

重複アセット名の最後に一意の整数値を追加し、それに続く重複アセット名それぞれに対し 1 だけ整数をインクリメントします。[整数基礎値] に開始整数を入力します。

なし

重複アセット名は名前を変更されません。CORA を有効にしていない場合、またはマイグレーション後にアセットを手動で修正する場合は、このオプションを選択できます。

4. (オプション) 増分および連結設定において各フィールド間、およびフィールドと増分整数間に表示される 1 文字のフィールド区切りを入力します。

5. [保存] をクリックします。

注: レコード数によっては、設定の保存に時間がかかる場合があります。進捗バーに、完了のステータスが示されます。

6. [終了] をクリックします。

マイグレーション ユーティリティの実行

マイグレーションユーティリティは、1 つの CA APM リリースから別のアップグレードされたデータベース構造に監査、オブジェクト、およびイベントをマイグレートします。

【CA APM マイグレーションユーティリティ】 ウィンドウ上の選択領域にあるオブジェクトの階層構造により、1 つの階層レベル内のすべてのオブジェクトを選択したり、または 1 レベル内の個別のオブジェクトを選択することができます。ステータス アイコンは、各オブジェクトまたはオブジェクト レベルのマイグレーションステータスを表示します。

ウィンドウの上部にあるアイコン キーは、ステータスを示します。オブジェクトステータスが [完了] のときは、オブジェクトを選択できません。

[メッセージ] および [サマリ] タブで [マイグレーションプロセスをモニタし \(P. 69\)](#)、マイグレーションの実行結果を確認できます。

重要: 「[前提条件 \(P. 47\)](#)」で説明したサービスおよびスケジュール タスクに加えて、リリース 12.9 サービスが実行されていないことをマイグレーション ユーティリティの実行前に確認してください。

ウィンドウを最初に開くと、[マイグレーションデータベースバージョンを確認する \(P. 65\)](#) ように求められます。このタスクを完了した後で、[オブジェクトマイグレーションを実行 \(P. 67\)](#) できます。

重要: リリース 12.9 では、リリース 12.8 でマイグレートされなかったオブジェクトをマイグレートできます。これらのオブジェクトとは、コストと支払いの拡張および監査、カスタム関係と監査、および関係の拡張および監査です。このリリースでは、カスタム関係および製品提供されなかった関係を含むすべての関係がマイグレートされます。以前リリース 11.3.4 からデータをマイグレートした場合は、これらのオブジェクトのデータのみをマイグレートできます。再度完全なデータマイグレーションを実行する必要はありません。

マイグレーションユーティリティを使用すると、以下のオブジェクトおよび関連イベントをマイグレートできます。

- アセット
 - CORA の一意のアセット名
 - アセットの現在のステータス履歴
- コストと支払い
 - 請求コード
 - 價格タイプ
 - コストタイプ
 - 通貨タイプ
- コストおよび支払いの拡張（および関連する監査）
- リーガルドキュメント
 - リーガル定義
 - ドキュメントロケーション
 - リーガルステータス
 - リーガルドキュメントステータス履歴
- 特記事項
 - 特記事項タイプ
- OOTB 関係（元の製品指定の関係）
- カスタム関係（および関連する監査）
- 拡張機能
 - 単純な拡張
 - リスト拡張
 - ロケーション階層

- 関係の拡張（および関連する監査）
- 添付ファイル
- 役割
- 照合変換リスト（サポート対象のタイプのみ）
 - オペレーティング システム変換リスト
 - システム モデル変換リスト
 - 製造元変換リスト
- アーカイブテーブルを監査するレガシー監査 他のオブジェクトをマイグレートした後、監査履歴オブジェクトが有効になり、イベント用の監査生成に完了ステータスが表示されます。

注: イベントが製品で正常に動作することを保証するには、マイグレーション オブジェクトのリストから [イベント用の監査生成] を選択します。イベント用の監査生成は、ベースライン監査レコードを作成します。

マイグレーション データベース バージョンの確認

データベース接続テストを行うことにより、マイグレーションデータベースのバージョンを確認します。マイグレーションユーティリティを初めて実行すると、[CA APM マイグレーションユーティリティの設定] ダイアログ ボックスが自動的に表示されます。ダイアログ ボックス フィールドにはリリース 12.9 インストール中に指定したデータベース構成設定が入力されています。

注: マイグレーションデータベース バージョンを確認した後に、マイグレーションユーティリティ ウィンドウの [設定] をクリックします。

データベース接続をテストすると、マイグレーションユーティリティは、データをマイグレートする元の製品リリース バージョンとデータをマイグレートする先のリリース バージョンを検出します。ユーティリティは、ダイアログ ボックス上の [バージョン元] および [バージョン先] フィールドに検出された製品リリース バージョンを入力します。ダイアログ ボックス上のリリース バージョンを変更できません。

検出された [バージョン元] はリリース 11.3.4 である必要があります。また、検出された [バージョン先] はリリース 12.9 である必要があります。マイグレーションユーティリティが別のリリース バージョンを検出した場合は、マイグレーションを続けることができません。

次の手順に従ってください:

1. データベース パスワードを入力します。
2. [接続のテスト] をクリックします。
確認メッセージは、接続テストの成否を示します。
3. 接続テストが成功したことが確認メッセージに表示された場合は、[CA APM マイグレーションユーティリティ設定] ダイアログ ボックスで [保存] をクリックします。
ダイアログ ボックスが閉じます。
4. データベース接続テストが失敗したことを確認メッセージが示した場合は、マイグレーションユーティリティがデータベース設定に接続できなかつた原因を特定します。その問題を解決した後、接続テストを繰り返します。

注: [CA APM マイグレーションユーティリティ設定] ダイアログ ボックス上で、製品リリースバージョンがマイグレーションユーティリティに接続しようとしているリリースバージョンと一致しない場合、データベース接続テストは失敗します。マイグレーションを続行できません。

後日データベース構成設定を変更する場合は、「[マイグレーションデータベースの設定 \(P. 66\)](#)」を参照してください。

マイグレーション データベースの設定

マイグレーション中にマイグレーションデータベースを設定する必要はありません。データベースは、リリース 12.9 インストール中に指定された設定で構成されます。

後で CA MDB のロケーションを変更する場合は、マイグレーションデータベースを新しいロケーションに設定した後でマイグレーションユーティリティの実行が可能になります。

次の手順に従ってください:

1. [マイグレーションユーティリティ] ウィンドウの [設定] をクリックします。
2. 構成設定を入力します。
3. [接続のテスト] をクリックします。

確認メッセージは、接続テストの成否を示します。

4. 接続テストが成功したことが確認メッセージに表示された場合は、[CA APM マイグレーションユーティリティ設定] ダイアログ ボックスで [保存] をクリックします。
[CA APM マイグレーションユーティリティ設定] ダイアログ ボックスが閉じます。
5. データベース接続テストが失敗したことを確認メッセージが示した場合は、マイグレーションユーティリティがデータベース設定に接続できなかった原因を特定します。その問題を解決した後、接続テストを繰り返します。

オブジェクトマイグレーションの実行

重要: 「[前提条件 \(P. 47\)](#)」で説明したサービスおよびスケジュールタスクに加えて、リリース 12.9 サービスが実行されていないことをマイグレーションユーティリティの実行前に確認してください。

[CA APM マイグレーションユーティリティ] ウィンドウでは、[CA APM オブジェクト] 領域の階層構造にあるマイグレーション オブジェクトがリスト表示されます。マイグレートするオブジェクトを選択します。データを段階的にマイグレートできます。階層構造により、1 つの階層レベル内のすべてのオブジェクトを選択したり、または 1 レベル内の個別のオブジェクトを選択することができます。

マイグレートするオブジェクトを選択すると、そのオブジェクトの階層内のすべてのオブジェクトが選択されます。これらのオブジェクトはセカンダリ オブジェクトと呼ばれます。階層内のセカンダリ オブジェクトが最初にマイグレートされ、選択したトップレベル オブジェクトが最後にマイグレートされます。たとえば、[コストと支払い] トップレベル オブジェクトを選択すると、[コストと支払い] オブジェクト階層内の [請求コード]、[価格タイプ]、および [コストタイプ] セカンダリ オブジェクトも選択されます。そのセカンダリ オブジェクトを参照するにはトップレベル オブジェクトを展開します。マイグレーションでは、[請求コード]、[価格タイプ] および [コストタイプ] を最初にマイグレートします。トップレベル オブジェクト [コストと支払い] はそのセカンダリ オブジェクトの後にマイグレートします。

マイグレートしないオブジェクトについては、隣のチェック ボックスをオフにできます。マイグレートする 1 つのオブジェクト、オブジェクトのグループまたはすべてのオブジェクトを選択できます。

すでにマイグレートされたオブジェクトは、[完了] ステータスとなっているため、それらのチェック ボックスは無効です。このように、マイグレーションユーティリティは、すでにマイグレートされたオブジェクトをマイグレートできないようになっています。

実行するために選択できるオプションを表示するにはオブジェクトを右クリックします。利用可能なオプションは、オブジェクトの現在のステータスに依存します。オブジェクトを右クリックしたときに、以下のオプションを選択できます。

- セカンダリ オブジェクト用のチェック ボックスをオフにする
- 完了へ移動
- 開始前へ移動

監査履歴オブジェクトは最初は無効になっています。最初は、非監査オブジェクトのマイグレートから開始します。マイグレーションが正常に完了すると、監査履歴オブジェクトが有効になり、イベントの監査生成に完了ステータスが示されます。オプションが有効になり、すべてのアプリケーションおよびサービスがオンラインに復帰したら、監査履歴オブジェクトをいつでもマイグレートできます。

重要: データのサイズによっては、監査履歴オブジェクトのマイグレートに時間がかかる場合があります。監査履歴のレコード数が約 100 万件の場合、オフピーク時間にマイグレートすることをお勧めします。

次の手順に従ってください:

1. [CA APM マイグレーションユーティリティ] ウィンドウで、マイグレートするオブジェクトの隣のチェック ボックスをオンにします。

注: イベントが製品で正常に動作するには、マイグレーション オブジェクトのリストからイベントの監査生成を選択します。イベント用の監査生成は、ベースライン監査レコードを作成します。

2. [開始] をクリックします。

[マイグレーション進捗状況をモニタする](#) (P. 69)には [メッセージ] タブ内の情報を見ます。

マイグレーションが正常に完了すると、ウィンドウの選択領域内のオブジェクトのステータスが [完了] となります。

注: マイグレーションが失敗した場合、以下の場所にあるオブジェクトマイグレーションログファイルで詳細を確認してください。

`[ITAM Root Path]¥Migration Toolkit¥migration-utility¥logs`

3. (オプション) マイグレーションが成功した場合、監査履歴オブジェクトを選択し、手順 2 を繰り返します。
4. [終了] をクリックします。

[CA APM マイグレーションユーティリティ] ウィンドウが閉じます。

マイグレーションが完了した場合、以下のサービス マネジメント製品用のサービスを再起動します。

- CA Service Catalog
- CA Service Desk Manager
- CA Client Automation
- CA APM リリース 12.9

マイグレーションプロセスのモニタ

[CA APM マイグレーションユーティリティ] ウィンドウ上の [メッセージ] タブには、現在のマイグレーションプロセスの進捗状況が表示されます。メッセージを表示することによりマイグレーションプロセスをモニタします。メッセージは、マイグレーション中の各オブジェクトのステータスの変化を示します。

マイグレーションが終了すると、[サマリ] タブ上で成功、保留中および失敗したマイグレーションの概要を確認できます。[サマリ] タブには、セッション中に実行されたすべてのマイグレーションのステータスが表示されます。

オブジェクトマイグレーションログファイルは以下の場所から参照できます。

[ITAM Root Path]¥Migration Toolkit¥migration-utility¥logs

ログファイルに表示される失敗メッセージについては、CA サポートにお問い合わせください。

手動マイグレーション用のマイグレーション後レポートの実行

マイグレーションユーティリティを実行した後に、手動マイグレーションで使用するマイグレーション後レポートを実行します。マイグレーション後レポートは、リリース 12.9 に入力する必要があるオブジェクトデータを識別します。データと関連付けられている機能が変更されたため、マイグレーションユーティリティでは一部のデータをマイグレートできません。

次の手順に従ってください:

1. CA Asset Portfolio Management マイグレーションツールキットのメイン ウィンドウで、[マイグレーション レポート] をクリックします。

2. [マイグレーション前レポート] 領域のチェックボックスをすべてオフにし、[マイグレーション後レポート] 領域で以下のレポートを選択します。

- 詳細検索
- 添付ファイル
- 基本の検索結果返却フィールド
- イベント
- フィルタ
- 役割のセキュリティ (フィールドおよび機能の権限)

注: 一部のマイグレーション後レポートタイプのみを生成する場合は、目的のレポートタイプのみを選択します。

3. [レポート出力フォルダ] 領域で、[参照] をクリックし、レポートを保存する出力フォルダを選択します。

4. [レポートの生成] をクリックします。

ステータスマッセージが [メッセージ] 領域に表示され、レポート生成プロセスをモニタできます。

レポートを表示するためにレポート出力フォルダを開くように促されます。

5. [はい] をクリックします。

Windows エクスプローラが開きます。レポートツールは、ユーザが以前に選択した各マイグレーション後レポートチェックボックスのフォルダを作成します。

6. レポートフォルダに移動し開きます。

レポートはカンマ区切り値 (CSV) 形式で表示されます。

7. レポートを右クリックして、[プログラムから開く]、[Excel] を順番に選択して、レポートを表形式で開いて表示します。

レポートデータ (P. 71)が表形式で表示されます。テーブルの見出しへ最初の行に表示されます。

注: レポートを開き、テキストエディタで CSV フォーマットのレポートを表示できます。

参照と分析用のマイグレーションレポートデータ

レポートツールは、テキストエディタで開くことができる CSV 形式でレポートを生成します。レポートのフィールド名およびフィールド値はカンマで区切られます。Excel でレポートを開くこともできます。その場合、表形式でデータが表示されます。Excel でレポートを開くと、フィールド名は列見出しとなり、フィールド値は各見出しの下の行に表示されます。

マイグレーション後レポートは、マイグレーション後に リリース 12.9 に入力したデータに関する情報を提供します。このデータは、マイグレーションユーティリティを使用してマイグレートできませんでした。

以下のマイグレーション後レポートには、[手動マイグレーションの実行 \(P. 77\)](#)に使用する情報が表示されます。

- [詳細検索レポート \(P. 71\)](#)
- [添付レポート \(P. 72\)](#)
- [基本検索レポート \(P. 73\)](#)
- [イベント レポート \(P. 73\)](#)
- [フィルタリング レポート \(P. 75\)](#)
- [役割のセキュリティ \(フィールドおよび機能の権限\) レポート \(P. 75\)](#)

詳細検索レポート

詳細検索レポートには、各詳細検索の概要および[各詳細検索の詳細レポート \(P. 72\)](#)のロケーション情報が提示されます。レポートの [詳細] 列には、各詳細検索詳細レポートのロケーションと名前が提示されます。

以下のレポートフィールドについて説明します。

エクスポートタイプ

検索結果のエクスポートフォーマットを示します。

リフレッシュ間隔

エクスポートスケジュールの開始時刻および頻度を識別します。

オブジェクトタイプ

セキュリティ検索設定に 1 つ以上の役割がある場合の役割アクセスを示します。

割り当て

検索へのアクセス権限がある役割名または連絡先を識別します。

作成者

検索を最後に更新したユーザの名前を識別します。詳細検索の手動マイグレーション（再作成）を委任するにはこの情報を使用します。このフィールドを詳細検索での設定には割り当てません。

作成者 ID

検索を最後に更新したユーザの名前を識別します。詳細検索の手動マイグレーション（再作成）を委任するにはこの情報を使用します。このフィールドを詳細検索での設定には割り当てません。

[詳細検索を リリース 12.9 に手動でマイグレートする \(P. 79\)](#)には詳細検索レポートを使用します。

詳細検索詳細レポート

詳細検索詳細レポートはそれぞれ、1つの詳細検索に対するデータを識別します。リリース 11.3.4 で作成された詳細検索に関する情報を確認します。

[これらの詳細検索を リリース 12.9 に手動でマイグレートする \(P. 79\)](#)には詳細検索レポートを使用します。

添付レポート

添付レポートは、[ファイル添付を手動でマイグレートする \(P. 85\)](#)ために使用する情報を識別します。マイグレーションユーティリティは、完全な Web URL リンク添付ファイルおよびリモートサーバとローカル添付ファイルのメタデータをマイグレートします。マイグレーション後に、物理添付ファイルをストレージマネージャサービスに移動します。

添付レポートには、ファイルの場所と説明、および各添付の以下の情報が提示されます。

UUID

ユニバーサル識別子はオブジェクトを識別し、同じ名前を持つ2つのオブジェクトを区別します。

オブジェクトタイプ

ファイルが添付されるオブジェクトのタイプを識別します。

割り当て

ファイルが添付されるオブジェクトの名前を識別します。

基本検索レポート

リリース 11.3.4 で作成された検索に関する以下の情報を表示し、[これらの基本検索をリリース 12.9 に手動でマイグレートする](#) (P. 77)には基本検索レポートを使用します。

- 検索結果が返すオブジェクトタイプ
- 検索結果返却フィールドを表示することが許可されている役割（存在する場合）
- 検索結果返却フィールド。これはリリース 11.3.4 では表示フィールドという名前でした。

イベントレポート

[通知履歴イベント レポート](#) (P. 73)には、確認用としてリリース 11.3.4 からの履歴情報が提示されます。以下のイベントレポートは、手動マイグレーションを実行するときに、[マイグレーションユーティリティ](#) (P. 63)を実行した後に使用するデータを識別します。[イベントの手動マイグレーション](#) (P. 86)時にこれらのレポートを参照してください。

- [日付イベント レポート](#) (P. 74)
- [監視と変更イベント レポート](#) (P. 74)

通知履歴イベント レポート

通知履歴イベント レポートには、確認用としてリリース 11.3.4 からの履歴情報が提示されます。対処は不要です。

このレポートは、昨年処理されたイベントを識別します。以下のフィールドについて説明します。

イベントが有効

値が TRUE であるときにイベントが有効で非アクティブではないことを示します。値が FALSE であるときにイベントが非アクティブであることを示します。

イベントフィールド名

イベントはこのオブジェクトフィールドの値に基づいています。

イベント受信者

現在のイベント通知の電子メールアドレス。

イベント通知定義テキスト

現在のイベント通知の電子メールメッセージテキスト。

通知タイプ

受信者が受信する通知のタイプを示します。「初期イベント」は、最初の通知の受信者を示します。「エスカレーション」は、未確認の通知の受信者を示します。

通知テキスト

過去のイベント通知の電子メール メッセージ テキスト。

通知受信者

過去のイベント通知の電子メール アドレス。

「実装ガイド」には、CA Process Automation で指定されるワークフロー プロバイダ プロセス パラメータに関する情報が記載されています。通知プロセス パラメータの詳細については、ワークフロー プロバイダのドキュメントを参照してください。

日付イベントレポート

日付イベント レポートは、[マイグレーションユーティリティ](#) (P. 63) の実行後、手動マイグレーションを実行するときに使用するデータを識別します。このレポートは日付イベントと通知を識別します。このレポートは、[イベントの手動マイグレーション](#) (P. 86) 時に参照します。

「実装ガイド」には、CA Process Automation で指定されるワークフロー プロバイダ プロセス パラメータに関する情報が記載されています。通知プロセス パラメータの詳細については、ワークフロー プロバイダのドキュメントを参照してください。

監視と変更イベントレポート

監視と変更イベント レポートは、[マイグレーションユーティリティ](#) (P. 63) の実行後、手動マイグレーションを実行するときに使用するデータを識別します。このレポートでは、リリース 11.3.4 から、監視イベントと通知、および変更イベントと通知に関する情報が提示されます。このレポートは、[手動マイグレーション](#) (P. 77) 中に参照します。

注: 手動イベントは リリース 11.3.4 で利用可能でしたが、リリース 12.9 ではサポートされていません。手動イベントは、監視と変更イベント レポートに含まれていません。

「実装ガイド」には、CA Process Automation で指定されるワークフロー プロバイダ プロセス パラメータに関する情報が記載されています。通知プロセス パラメータの詳細については、ワークフロー プロバイダのドキュメントを参照してください。

フィルタリング レポート

フィルタリング レポートでは、[各フィルタの詳細レポート \(P. 75\)](#)に関する各フィルタおよびロケーション情報の概要が提示されます。レポートの[詳細]列には、各フィルタ詳細レポートのロケーションと名前が提示されます。

連絡先フィルタリング詳細レポート

各フィルタリング詳細レポートは、1つのフィルタに対するデータを識別します。リリース 11.3.4 で作成されたフィルタに関する情報を表示し、[フィルタを手動でマイグレートする \(P. 87\)](#)にはフィルタリング詳細レポートを使用します。

役割セキュリティ(フィールドおよび機能の権限)レポート

各役割セキュリティ レポートは、1つのフィールド上、機能上、または表示できるリンクしたオブジェクトセキュリティ設定のデータを識別します。Migration Toolkit は以下のタイプの役割セキュリティ レポートを生成します。

- **フィールドセキュリティ レポート。** 役割セキュリティ設定がある各オブジェクトにつき 1 つのフィールドセキュリティ レポートを生成します。そのレポートは、役割、オブジェクト、オブジェクトフィールド、およびフィールドの役割に割り当てられる権限を識別します。更新権限レポートの列ラベルおよび新規権限の追加レポートの列ラベルは、リリース 11.3.4 の機能を参照します。リリース 12.9 はオブジェクトの更新および作成の権限を区別しません。
- **機能セキュリティ レポート。** 役割セキュリティ設定がある各オブジェクトにつき 1 つの機能セキュリティ レポートを生成します。そのレポートは、役割、オブジェクト、オブジェクトに関連する機能、およびその機能の役割に割り当てられる権限を識別します。
- **フィールドセキュリティリンク オブジェクト表示可能レポート。** 役割セキュリティ設定がある各オブジェクトにつき 1 つのフィールドセキュリティ表示可能リンク済みオブジェクト レポートを生成します。このレポートは、役割、オブジェクト、およびオブジェクトの割り当てられたフィールドを識別します。

CA APM リリース 11.3.4 で作成された役割セキュリティ設定に関する情報を表示し、[役割セキュリティ設定を手動でマイグレートする \(P. 89\)](#)には役割セキュリティ レポートを使用します。

以下のオブジェクト、フィールドおよび機能は リリース 12.9 でサポートされていません。それらは、参照用として リリース 11.3.4 データベース レポートに表示されます。

- アセットバージョン
- アセットバージョンステータス履歴
- モデルバージョン
- Keywords

CA APM Web インターフェースの開始

リリース 12.9 アップグレード製品を実行し、手動でデータを リリース 12.9 データベースにマイグレートするには CA APMWeb インターフェースを開始します。

[手動マイグレーションを実行する \(P. 77\)](#)前に、マイグレーションユーティリティ (P. 63)で自動マイグレーションを完了し、[マイグレーション後レポートを実行する \(P. 69\)](#)必要があります。

Web インターフェースを開始するには、Web ブラウザを開き、以下の URL を入力します。

`http://servername/itam`

servername を、CA APM Web サーバをホストしているサーバの名前に置き換えてください。

注: Internet Explorer ブラウザのセキュリティが「高」に設定されている場合、Web インターフェースを開始すると、コンテンツに関する警告メッセージが表示されます。このメッセージが表示されないようにするには、Web サイトを信頼済みサイトに追加するか、セキュリティのレベルを下げます。

Web サーバ上には、URL の場所を参照する [スタート] メニューのショートカットが作成されています。

URL を開いた後 CA APM にログインするには、以下のデフォルト認証情報を入力します。

ユーザ名

uapmadmin

パスワード

uapmadmin

注: 状況によっては、ブラウザ エラーまたはユーザ名エラーが表示されます。これらのエラーは、[トラブルシューティングの指示 \(P. 96\)](#)に従って解決できます。

手動マイグレーションの実行

以下のタスクを完了した後で、リリース 12.9 へのデータの手動マイグレーションを実行できます。

- マイグレーションユーティリティを使用してデータをマイグレートした。
- マイグレーション後レポートを生成した。

データを手動でマイグレートする場合は、リリース 12.9 を使用してデータを新しいリリースのデータ構造に入力します。マイグレーション レポートは、入力するフィールドおよび値を指定します。

重要: データの手動マイグレーションを実行するには、マイグレーション ツール キットを終了し、[Web インターフェースを起動 \(P. 76\)](#) しておく必要があります。

以下の手動マイグレーションを実行します。

- [基本検索のマイグレート \(P. 77\)](#)
- [詳細検索のマイグレート \(P. 79\)](#)
- [ファイル添付のマイグレート \(P. 85\)](#)
- [イベントのマイグレート \(P. 86\)](#)
- [フィルタのマイグレート \(P. 87\)](#)
- [役割セキュリティのマイグレート \(フィールドおよび機能の権限\) \(P. 89\)](#)
- [ハードウェア照合のタスクおよびルールのマイグレート \(P. 92\)](#)
- [ハードウェア照合の変換リストのマイグレート \(P. 93\)](#)
- [ハードウェア照合検索のマイグレート \(P. 94\)](#)

基本検索のマイグレート

リリース 11.3.4 では、ユーザが参照できる検索結果フィールドは、役割ごとにセキュリティ機能に設定されています。リリース 12.9 では基本検索機能が強化され、詳細検索とより密接に連携しています。すべてのフィールドを基本検索で使用できます。リリース 12.9 では、ユーザが検索機能で表示できる検索結果フィールドを設定します。新しい検索を作成し、設定した検索を保存するときに、特定のユーザ役割および設定を選択することによって検索にセキュリティを適用できます。

デフォルトでは、作成する検索のセキュリティによって、作成者のみが使用できるようになります。役割および設定を検索に割り当てて、それらの役割および設定に割り当てられているユーザにアクセス権を付与します。

注: 検索の詳細については、「ユーザ ガイド」を参照してください。

これらの変更は、マイグレーション ユーティリティではマイグレートできません。手動マイグレーション中に基本検索レポートのデータを使用します。

次の手順に従ってください:

1. 基本検索レポートで検索のオブジェクト タイプを特定します。
2. CA APM で、検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
3. 左側で、[新規検索] をクリックします。
[フィールドの追加] ダイアログ ボックスが表示されます。
注: オブジェクト タイプによっては、テンプレート、ファミリまたは他の属性を選択して検索範囲を絞り込むように促されます。
4. 検索結果フィールド レポートを使用して、検索に追加するフィールドを選択します。リリース 11.3.4 では、これらのフィールドは表示フィールドというラベルが付けられていました。
5. ダイアログ ボックスの下部にある [フィールドの追加先] 領域で、[検索条件と検索結果] を選択します。
6. [OK] をクリックします。
フィールドは検索条件と検索結果の両方に追加されます。[フィールドの追加] ダイアログ ボックスが閉じます。
7. ページの一番上にある [設定の検索: オフ] をクリックします。
検索の設定が完了しました。
8. [検索情報] 領域で、検索タイトルおよび他の記述情報 (たとえば、カテゴリおよび説明) を入力します。
9. (オプション) [セキュリティの検索] 領域を開きます。
10. (オプション) [セキュリティの検索] 領域で、検索を実行できるユーザ ロールを選択します。
注: 基本検索レポート (P. 73) で識別されるユーザ ロールを選択することを推奨します。
11. (オプション) [セキュリティの検索] 領域で、検索を実行できる設定を選択します。
注: 役割も設定も選択しない場合は、検索の作成者のみが検索を実行できます。
12. [検索条件] 領域、および入力した条件フィールドを特定します。

13. 各 [検索条件] フィールドには、フィールド値を入力します。検索アイコンをクリックして値を検索できます。
14. (オプション) [追加設定] 領域を開いて、他の設定 (並べ替えの設定など) を追加します。
15. [保存] をクリックします。
検索が保存されます。
16. [セキュリティの検索] 領域でユーザ ロールを選択した場合は、各役割に対して以下の手順を実行します。
 - a. [管理] - [ユーザ/役割管理] をクリックします。
 - b. 左側の [役割管理] メニューを展開します。
 - c. [役割の検索] をクリックします。
 - d. 役割を検索および選択します。
役割の詳細が表示されます。
 - e. [デフォルト検索] 領域で、[新規に選択] をクリックします。
 - f. 先ほど作成した検索を検索します。
 - g. 検索を役割のデフォルト検索として割り当てます。
 - h. [保存] をクリックします。
更新した役割が保存されます。

詳細検索のマイグレート

CA APM リリース 11.3.4 では、ユーザが参照できる検索結果フィールドは、役割ごとにセキュリティ機能に設定されています。リリース 12.9 では、検索は追加されるセキュリティ レベルをサポートしています。ユーザが検索機能で表示できる検索結果フィールドを設定します。設定した検索を保存するときに、特定のユーザ ロールおよび設定を選択することによって検索にセキュリティを適用できます。

デフォルトでは、作成する検索のセキュリティによって、作成者のみが使用できるようになります。役割および設定を検索に割り当てて、それらの役割および設定に割り当てられているユーザにアクセス権を付与します。

注: 検索の詳細については、「ユーザ ガイド」を参照してください。

これらの変更はマイグレーション ユーティリティではマイグレートできません。

詳細検索を移行するときに、以下の手順を実行します。

- [詳細検索の作成 \(P. 80\)](#)
- [検索のスケジューリングおよび結果のエクスポート \(P. 83\)](#)

詳細検索の作成

手動での移行中に、[詳細検索レポート \(P. 71\)](#)および[詳細検索の詳細レポート \(P. 72\)](#)のデータを使用します。

次の手順に従ってください:

1. 詳細検索の詳細レポートで検索のオブジェクト タイプを特定します。
2. CA APM で、検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
3. 左側で、[新規検索] をクリックします。
[フィールドの追加] ダイアログ ボックスが表示されます。
注: オブジェクト タイプによっては、テンプレート、ファミリまたは他の属性を選択して検索範囲を絞り込むように促されます。
4. 詳細レポートで、[結果フィールド] および [選択済み条件フィールド] の両方にあるフィールドを特定します。
5. [フィールドの追加] ダイアログ ボックスで、レポートで特定した共通のフィールドを選択します。
6. ダイアログ ボックスの下部にある [フィールドの追加先] 領域で、[検索条件と検索結果] を選択します。
7. [OK] をクリックします。
[検索条件] と [検索結果] の両方のフィールドが検索に追加され、[フィールドの追加] ダイアログ ボックスが閉じます。
8. [フィールドの追加] をクリックします。
[フィールドの追加] ダイアログ ボックスが表示されます。

9. 詳細レポートで [結果フィールド] および [選択済み条件フィールド] に共通しない [結果フィールド] を選択します。
10. ダイアログ ボックスの下部にある [フィールドの追加先] 領域で、[検索結果のみ] を選択します。
11. [OK] をクリックします。
[検索結果のみ] フィールドが検索に追加され、[フィールドの追加] ダイアログ ボックスが閉じます。
12. [フィールドの追加] をクリックします。
[フィールドの追加] ダイアログ ボックスが表示されます。
13. 詳細レポートで [結果フィールド] および [選択済み条件フィールド] に共通しない [選択済み条件フィールド] を選択します。
14. ダイアログ ボックスの下部にある [フィールドの追加先] 領域で、[検索条件のみ] を選択します。
15. [OK] をクリックします。
[検索条件のみ] フィールドが検索に追加され、[フィールドの追加] ダイアログ ボックスが閉じます。
16. ページの一番上にある [設定の検索: オフ] をクリックします。
検索の設定が完了しました。
17. [検索情報] 領域で、検索タイトルおよびレポートの他の情報を入力します。
たとえば、カテゴリや説明などです。

18. (オプション) [セキュリティの検索] 領域を展開します。
19. (オプション) [セキュリティの検索] 領域で、以下の手順を実行して検索を実行できるユーザ ロールを選択します。
 - a. [役割アクセス] 領域で [新規に選択] をクリックします。
[役割の検索] ダイアログ ボックスが表示されます。
 - b. 詳細検索レポートの [割り当て] フィールドで識別される役割名を入力します。役割名は役割の名前または連絡先名である場合があります。
 - c. 必要に応じて、説明を入力します。
 - d. 新しい役割の検索に非アクティブ レコードを含むかどうかを選択します。
 - e. [実行] をクリックします。
検索結果が表示されます。
 - f. 検索を実行できる役割または連絡先を選択します。
 - g. [OK] をクリックします。
[役割の検索] ダイアログ ボックスが閉じます。
20. (オプション) [セキュリティの検索] 領域で、検索を実行できる設定を選択します。
注: 役割も設定も選択しない場合、検索はすべてのユーザ および設定に対して実行可能になります。
21. [検索条件] 領域、および選択した条件フィールドを特定します。
22. [詳細設定] をクリックします。
詳細な [検索条件] 領域が開きます。
23. 各検索条件に対して、以下の手順を実行します。
 - a. 検索条件の隣の [レコード編集] アイコンをクリックします。
 - b. レポートに関する条件情報を特定します。
 - c. 詳細レポートで示されるように、演算子、値、コネクタ および 丸かっこを入力します。
 - d. [レコード編集を完了] アイコンをクリックします。
24. (オプション) [追加設定] 領域を開いて、他の検索設定 (並べ替えなど) を追加します。
注: 詳細レポートの [並べ替え順序] 領域で識別されるように、[検索結果の並べ替え] 領域で、[選択したフィールド] および [並べ替え方向] の値を選択します。
25. [保存] をクリックします。
詳細検索が保存されます。

検索のスケジューリングおよび結果のエクスポート

定期的に処理するように検索をスケジュールして、検索結果を CSV ファイルまたはデータベース ビューにエクスポートできます。

次の手順に従ってください:

1. CA APM で、検索するオブジェクトのタブおよびオプションのサブタブをクリックします。
2. 左側の [検索の管理] をクリックします。
3. 保存した検索を検索して選択します。
4. 左側で、[新規エクスポート] をクリックします。
5. 詳細レポートのエクスポート情報に基づいて、基本的なエクスポート情報を入力します。
6. 以下のフィールドについて説明します。

エクスポート名

エクスポート名を指定します。

エクスポート形式

エクスポートされた検索結果の形式を選択します。

ビューネ名

データベース ビューネ名を指定します。

注: [エクスポートフォーマット] に [データベース ビュー] を選択する場合、ビューネ名は必須です。名前は有効なデータベース ビューネ名である必要があります。

説明

エクスポートされた検索結果の説明を指定します。

保管日数

エクスポートされた検索結果がページされるまで保管する日数を指定します。

フォルダ名

エクスポートされた CSV ファイル検索結果用のフォルダを指定します。

失効なし

CSV ファイルまたはデータベース ビューをページしないように指定します。

7. [エクスポートスケジュール] 領域で検索をスケジュールします。 詳細レポートの [リフレッシュ間隔] の値を使用して、検索をスケジュールします。 以下のフィールドについて説明します。

実行時刻

CA APM アプリケーションサーバのローカルタイムゾーンで、検索を処理する時刻を指定します。

間隔タイプ

検索の間隔のタイプ（日、月、四半期、週、または年）を指定します。

間隔日

間隔中に検索を処理する日を指定します。たとえば、[間隔タイプ] が [月] で、[間隔日] が「1」である場合、検索は月の1日に処理されます。

初回実行日

最初の検索処理を開始する日付を指定します。

間隔

選択した間隔タイプに基づいて、検索処理の頻度を指定します。たとえば、[間隔タイプ] が [週] で、[間隔] が「2」である場合、検索は2週間ごとに処理されます。

間隔の最終日

検索が選択された間隔タイプの最終日に処理されるように指定します。

8. 検索に割り当てられたすべての役割と設定に、エクスポートされた検索結果を送信するかどうかを指定します。

9. [保存] をクリックします。

検索が保存されます。スケジュールされた時刻に検索が処理され、検索結果がエクスポートされます。

添付ファイルのマイグレート

リリース 12.9 では、ストレージマネージャ サービスによってすべての添付ファイルが処理されます。2 種類の添付ファイルを指定できます。

- **Web URL リンク。** URL で指定されたページに直接アクセスできます。このタイプの添付ファイルを追加する場合は、リンクが正常に機能するように、先頭に `http://` を付けます。
- **ファイルパス。** ファイルへの直接アクセスを提供します。ファイルは、ファイルタイプ用のデフォルトプログラムを使用して開きます。この添付ファイルタイプを作成する際、現在のファイルシステムから CA APM サーバのファイルシステムにファイルがコピーされます。

注: 複数の添付ファイルを (1 つのオブジェクトや複数のオブジェクトに) 追加する場合、各添付ファイルの名前とファイルパスまたは URL はすべてのオブジェクトで一意である必要があります。

リリース 11.3.4 では、添付ファイルは共通の共有フォルダに格納されました。

マイグレーションユーティリティは、完全な Web URL 添付ファイルおよびリモートサーバとローカル添付ファイルのメタデータを移行します。メタデータには添付ファイル説明情報およびファイルパス ロケーション情報が含まれます。マイグレーションユーティリティによって、ファイルパス ロケーションはストレージマネージャ サービスに変更されます。マイグレーション後に、物理的な添付ファイルをストレージマネージャ サービスに移動します。

マイグレーションユーティリティを実行した後、リリース 11.3.4 の添付ファイルを共有フォルダおよびローカルサーバからリリース 12.9 ストレージマネージャ サービスにコピーします。Web URL 添付ファイルは、マイグレーションユーティリティによってマイグレートされます。

注: 添付ファイルの詳細については、「ユーザ ガイド」を参照してください。

手動でのマイグレーション中に [添付ファイル レポート](#) (P. 72) のデータを使用します。

次の手順に従ってください:

1. レポートで識別される添付ファイルの場所に移動します。
2. 添付ファイルをコピーして、アプリケーションサーバ上のストレージマネージャ サービスの以下の場所に貼り付けます。
 - `[ITAM Root Path]¥Storage¥Common Store¥Attachment¥attachment.extn`

attachment.extn を添付ファイル名と拡張子に置換します。

以下のように添付ファイルへの完全パスを入力します。

C:\Program Files (x86)\ITAM\Storage\Common Store\Attachment\legaldoc1.docx

3. レポート上の各リモート サーバまたはローカル添付ファイルに対してこの手順を繰り返します。

注: ストレージマネージャ マシンの場所に移動しないファイルは、本製品では利用できません。

4. CA APM ではなくリモート サーバまたはローカルマシンから添付ファイルを削除した場合、マイグレーションユーティリティによって添付ファイルのメタデータがマイグレートされます。物理的に存在しなくなった添付ファイルがレポートによって識別される場合は、リリース 12.9 を使用して添付ファイルのメタデータを削除します。

イベントのマイグレート

ユーザ インターフェースを使用して、日付、変更および監視イベントを定義できます。ハードコードされたテキストおよび CA APM オブジェクト値を使用して、通知をセットアップできます。たとえば、通知の件名で、「要承認:」に続いて CA APM リーガルドキュメント識別子オブジェクトの値が含まれるように指定できます。イベントが発生すると、特定の受信者に電子メール通知を送信することができます。受信確認されない通知はエスカレートできます。

イベントおよび通知を手動でマイグレートするときは、「[日付イベント レポート \(P. 74\)](#)」のデータ、「[監視および変更イベント レポート \(P. 74\)](#)」のデータを使用します。

次の手順に従ってください:

1. 「ユーザ ガイド」のイベントおよび通知の作成手順に従います。
2. イベントおよび通知を作成するには、「日付イベント レポート」のデータおよび「監視および変更イベント レポート」のデータを使用します。

注: 「実装ガイド」には、CA Process Automation で指定されるワークフロー プロバイダ プロセス パラメータに関する情報が記載されています。通知プロセス パラメータの詳細については、ワークフロー プロバイダのドキュメントを参照してください。

フィルタのマイグレート

CA APM リリース 11.3.4 では、表示されるフィルタは役割別にセキュリティ機能で設定されます。このリリースでは、フィルタは新しいセキュリティ レベルをサポートしています。フィルタ機能でユーザに表示されるフィルタを設定します。フィルタを設定するときには、特定のユーザの役割およびフィルタを表示する権限を持つユーザを選択することにより、フィルタにセキュリティを適用できます。

デフォルトでは、作成するフィルタに適用されるセキュリティにより、すべての役割およびユーザにフィルタが利用可能になります。作成したフィルタに固有のセキュリティを適用することで、フィルタ内の機密情報を特定のユーザが表示できないように設定できます。

これらの変更はマイグレーション ユーティリティではマイグレートできません。手動マイグレーション時に「[フィルタ詳細レポート \(P. 75\)](#)」のデータを使用します。

次の手順に従ってください:

1. フィルタ詳細レポートのフィルタのオブジェクトを特定します。
2. CA APM で、[管理] タブおよび[フィルタ管理] サブタブをクリックします。
3. [新規フィルタ] をクリックします。
[フィルタ詳細] ページが表示されます。
4. [フィルタ情報] 領域で、フィルタ詳細レポートの情報を使用して以下の手順を実行します。
 - a. フィルタ名およびフィルタするオブジェクトを入力します。
 - b. (オプション) 説明を入力します。
 - c. (オプション) すべてのユーザがフィルタ データを参照できるようにする場合は、[すべてのユーザへのフィルタの割り当て] を選択します。フィルタにセキュリティを適用する場合は、以下の手順に従って [フィルタのセキュリティ] 領域に入力します。

5. [フィルタのセキュリティ] 領域で、以下のアクションを実行します（複数可）。
 - フィルタを参照できる役割を入力するには
 - [役割] 領域の [新規に選択] をクリックします。
[役割の検索] ダイアログ ボックスが表示されます。
 - フィルタの参照が許可される役割を検索および選択します。
 - [OK] をクリックします。
 - フィルタを参照できるユーザを入力するには
 - [ユーザ] 領域の [新規に選択] をクリックします。
[検索] ダイアログ ボックスが表示されます。
 - フィルタの参照が許可されるユーザを検索および選択します。
 - [OK] をクリックします。
6. [フィールドの追加] をクリックします。
[フィールドの追加] ダイアログ ボックスが表示されます。
7. [選択された条件フィールド] セクションで、レポートに表示するフィールドを選択します。
8. [OK] をクリックします。
[フィールドの追加] ダイアログ ボックスが閉じ、選択したフィールドが [フィルタ条件] 領域に表示されます。
9. 詳細レポートの [条件] 領域の情報を使用して、フィルタ条件ごとに以下の手順を実行します。
 - a. [フィルタ条件] の隣の [レコード編集] アイコンをクリックします。
 - b. レポートの指示に従って、演算子、値、コネクタ、および丸かつこを入力します。
 - c. [レコード編集を完了] アイコンをクリックします。
10. [保存] をクリックします。
フィルタが保存されます。

役割セキュリティのマイグレート

マイグレーションユーティリティは、役割のセキュリティ設定ではなく、ユーザの役割をマイグレートします。役割のセキュリティ（フィールド、機能、表示可能なリンク済みオブジェクト権限）は、手動で移行します。

ユーザの役割は、セキュリティおよびユーザインターフェース ナビゲーションを制御するプライマリ レコードです。ユーザがタスク（通常、ビジネス組織内での役割に対して割り当てられているもの）を実行するために必要な機能のみを公開することによって、役割ごとに製品の限定ビューが定義されます。ユーザのデフォルトの役割とユーザインターフェース設定の組み合わせにより、ユーザがログインしたときに表示される内容が決定されます。ユーザは1つの役割のみに属することができます。

機能およびフィールドレベルのリポジトリ アクセス権を適用するには、ユーザの役割を定義します。各役割に必要なアクセス権のレベルを決定し、割り当てます。役割を割り当てることで、データの追加や削除といった許可されていないタスクをユーザが実行できないようにします。

フィールドセキュリティは、オブジェクトフィールドに対する役割の権限（たとえば、フル コントロールなど）を定義します。機能セキュリティは、オブジェクトの機能に対する役割の権限（たとえば、アセットのコピーなど）を定義します。表示可能リンク済みオブジェクトセキュリティは、オブジェクトのフィールドを定義します。

オブジェクトローカル設定で、オブジェクトのセキュリティ権限設定を作成します。その後、オブジェクト設定の1つを役割に割り当てます。役割のフィールドセキュリティ権限および機能セキュリティ権限は、その役割に割り当てられたオブジェクト設定によって決まります。それぞれの役割のオブジェクト設定は、オブジェクトの「[役割セキュリティ レポート \(P. 75\)](#)」上で識別されます。

役割セキュリティをマイグレートするには、以下の手動マイグレーションを実行します。

- [役割フィールドセキュリティのマイグレート \(P. 90\)](#)
- [役割機能セキュリティのマイグレート \(P. 90\)](#)
- [役割表示可能リンク済みオブジェクトセキュリティのマイグレート \(P. 91\)](#)

役割フィールドセキュリティ、役割機能セキュリティ、および役割表示可能リンク済みフィールドのセキュリティを手動でマイグレートするには、「[役割セキュリティ レポート \(P. 75\)](#)」の情報を使用します。

役割フィールド セキュリティのマイグレート

役割フィールドセキュリティを手動でマイグレートするには、「[役割セキュリティ レポート \(P. 75\)](#)」の情報を使用します。

次の手順に従ってください:

1. 役割フィールドセキュリティ セキュリティ権限をマイグレートするには、オブジェクトのフィールドセキュリティ レポートで、フィールドおよびフィールドの役割権限を特定します。
 2. オブジェクトフィールドのローカル設定を作成し、名前を付けます。以下のフィールドセキュリティ設定が利用可能です。
 - **フル コントロール。** その役割によるフィールドの編集が許可されます。
 - **非表示。** その役割に対して非表示になり、ユーザインターフェースから削除されます。
 - **読み取り専用。** その役割に対してフィールドは読み取り専用になります。
- 注:** ユーザインターフェースの設定については、「[管理ガイド](#)」を参照してください。

役割機能セキュリティのマイグレート

役割機能セキュリティを手動でマイグレートするには、「[役割セキュリティ レポート \(P. 75\)](#)」の情報を使用します。

次の手順に従ってください:

1. 役割機能セキュリティ セキュリティ権限を移行するには、オブジェクトの機能セキュリティ レポートで、機能および機能の役割権限を特定します。
2. オブジェクト機能のローカル設定を作成し、名前を付けます。機能セキュリティ設定は、ユーザにアセットモデルの変更を許可するなど、多くの機能の中の1つでもかまいません。機能セキュリティ設定には、「付与済みの権限」や「拒否された権限」があります。

注: ユーザインターフェースの設定については、「[管理ガイド](#)」を参照してください。
3. オブジェクト設定を保存します。
4. [管理] - [ユーザ/役割管理] をクリックします。
5. 左側の [役割管理] 領域を展開します。

6. [役割の検索] をクリックします。
7. セキュリティ レポートに示された役割を検索します。
8. [検索結果] 領域の役割名リンクをクリックします。
[基本情報] 領域が開きます。
9. 左側の [役割の設定] をクリックします。
[役割の設定] 領域が表示されます。
10. [新規の選択] をクリックします。
保存された設定のリストが表示されます。
11. 役割に割り当てるオブジェクト設定を選択します。
12. [OK] をクリックします。
オブジェクト設定が役割に割り当てられます。

役割表示可能リンク済みオブジェクト セキュリティのマイグレート

役割表示可能リンク済みオブジェクト セキュリティを手動でマイグレートするには、[「役割セキュリティ レポート \(P. 75\)」](#) の情報を使用します。

次の手順に従ってください:

1. 役割表示可能リンク済みオブジェクトセキュリティ権限の場合、フィールドセキュリティ表示可能リンク済みオブジェクトレポートで、リンク済みオブジェクトおよびオブジェクトの役割を見つけます。
2. オブジェクトのローカル設定を作成し、名前を付けます。レポート内のオブジェクトの割り当て済みフィールドとして定義されるフィールドをリンクします。
3. オブジェクト設定を保存します。
4. [管理] - [ユーザ/役割管理] をクリックします。
5. 左側の [役割管理] 領域を開きます。
6. [役割の検索] をクリックします。
7. セキュリティ レポートに示された役割を検索します。
8. [検索結果] 領域の役割名リンクをクリックします。
[基本情報] 領域が開きます。
9. 左側の [役割の設定] をクリックします。
10. [新規の選択] をクリックします。
11. 役割に割り当てるオブジェクト設定を選択し、[OK] をクリックします。

オブジェクト設定が役割に割り当てられます。レポート内の各役割に対して手順を繰り返します。

ハードウェア照合のタスクおよびルールのマイグレート

ハードウェア照合プロセスでは、以下の手順が必要となります。

1. データの正規化ルールを確立し、検出リポジトリと製品間でデータの値をマップします。
2. 処理対象のデータの制限方法および検出されたレコードの処理方法を指定するには、照合ルールを定義します。

注: この手順の照合ルールは、リリース 11.3.4 の照合タスクに代わるもので、手動マイグレーション中、照合ルールは、リリース 11.3.4 のタスクに基づいて、「[主要タスク クエリ レポート \(P. 60\)](#)」および「[タスク追加アセット レポート \(P. 60\)](#)」から作成します。

3. (オプション) 照合更新オプションを定義し、ハードウェア照合エンジンによって、対応する検出されたアセットで見つかった変更を使用して所有アセットフィールドが自動的に更新されるようにします。
4. 所有アセットと検出されたアセットを一致させるため、照合ルールのアセット一致基準を定義します。
5. メッセージ キュー内の照合結果を表示します。

タスクから照合ルールに手動で移行する際に、「[主要タスク クエリ レポート \(P. 60\)](#)」および「[タスク追加アセット レポート \(P. 60\)](#)」のデータを使用します。

次の手順に従ってください:

1. 「[管理ガイド](#)」の「照合ルールの定義」で説明されている照合ルール定義手順に従います。
2. 照合ルールを作成するには、「[主要タスク クエリ レポート](#)」および「[タスク追加アセット レポート](#)」のデータを使用します。

ハードウェア照合変換リストのマイグレート

マイグレーションユーティリティを使用してハードウェア照合変換リストを移行しない場合は、リストを手動でマイグレートします。この決定をするには、「[主要変換リスト クエリ レポート \(P. 60\)](#)」を分析します。

リリース 12.9 は、同じタイプの複数の変換リストを、モデル、製造元、およびオペレーティング システムに対する正規化ルールに置換します。

変換リストから正規化ルールに手動移行する際に、「[メイン変換リスト クエリ レポート \(P. 60\)](#)」のデータを使用します。

次の手順に従ってください:

1. 「[管理ガイド](#)」の「データの正規化」で説明されている正規化ルールの作成手順に従います。
2. 正規化ルールを作成するには、「[主要変換リスト クエリ レポート](#)」のデータを使用します。

注: 同じタイプのすべてのリストをマージし、重複したエントリを除去した後、結合リストを対応する正規化ルールに移行します。

ハードウェア照合変換リストから欠落したエントリのマイグレート

CA APM リリース 11.3.4 のハードウェア照合レガシー変換リストで、欠落しているか無効なためにリリース 12.9 に移行されないエントリのあるリストは、変換リスト未変換レポートで識別されます。変換リストはマイグレートされますが、リスト内のエントリの一部はマイグレートされません。これは、レガシーデータベース内にサポートするデータが存在しないためです。

同じタイプの複数の変換リストは、モデル、製造元、およびオペレーティングシステム用の正規化ルールに置換されます。

レガシー変換リスト上の欠落したエントリを リリース 12.9 正規化ルールに追加するには、「[変換リスト未変換レポート \(P. 61\)](#)」および「[主要変換リストクエリレポート \(P. 60\)](#)」のデータを使用します。

次の手順に従ってください:

1. 「[管理ガイド](#)」の「データの正規化」で説明されている正規化ルールの更新手順に従います。
2. 「[変換リスト未変換レポート \(P. 61\)](#)」のデータを使用して、リリース 12.9 の正規化ルールを更新し、レポートで特定された欠落エントリに反映します。

注: 同じタイプのすべてのリストをマージし、重複したエントリを除去した後、結合リストを対応する正規化ルールに移行します。

ハードウェア照合検索のマイグレート

ハードウェア照合カスタム検索を CA APM リリース 11.3.4 から リリース 12.9 ハードウェア照合レポートに移行します。CA Business Intelligence ソフトウェアによって生成された事前定義済みハードウェア照合レポートが用意されています。これらのレポートは、この製品に含まれている CA Business Intelligence を使用してカスタマイズできます。

ハードウェア照合レポートは、以下の情報を提供します。

- 検出された在庫とネットワーク ディスカバリ レコードの両方を含め、検出されたアセットに照合された所有アセット
- 請求されたアセット（有効なインボイス コードがあるアクティブ アセットまたは受信アセット）でディスカバリ レコードと一致しないもの
- 所有アセットに照合されていない検出されたアセット
- データの損失または無効なデータのために処理されない、検出されたアセット
- 現在の検出データ ボリュームの数
- ディスカバリ レコードに一致した所有アセット

- レコードに一致しない所有アセット
- ネットワーク検出データとエージェント検出データ間の一致
- 請求されていないが検出されたアセットなど、潜在的な収益の損失。このレポートには、請求されているアセットの数に基づいて収益機会が示されます。このレポートの情報を使用して、アセットがアクティブで検出されていることを証明できます。
- 対応する検出された在庫に一致していないネットワーク ディスカバリ レコード。ネットワークディスカバリによって、ネットワーク上のアセットの特定用に制限されたデータが提供されます。ディスカバリでは、アセットに関する詳細なハードウェアおよびソフトウェアの情報を提供されます。

どのハードウェア照合レポートを生成し、最大限カスタマイズするかを決定するには、「[カスタマイズ済み検索レポート \(P. 61\)](#)」のリリース 11.3.4 検索情報を使用します。

次の手順に従ってください:

1. 「ユーザ ガイド」の「レポート」セクションで説明されているハードウェア照合レポートの生成手順に従います。
2. カスタマイズ済み検索レポートの情報を使用して、関連するハードウェア照合レポートを特定し、検索条件を入力します。

注: レポートの結果を生成してエクスポートした後、Data Importer でレポート結果をインポートすることにより未照合のアセットを追加するには、「[管理ガイド](#)」の「未照合検出レポートからのアセットの追加」で説明されている手順に従います。

マイグレーション後検証の実行

データマイグレーションの前に CA Service Desk Manager および CA Service Catalog との統合が存在していた場合は、これらの統合のトマイグレーション後検証を実行します。この検証は、すべてのデータをリリース 12.9 にマイグレートした後に実行します。

次の手順に従ってください:

1. [ファイル名を指定して実行] をクリックし、services.msc を実行します。
2. CA Service Desk Manager サービスが実行されていない場合は、このサービスを選択して開始します。

3. CA Service Desk Manager ディレクトリに移動します。
4. CA Service Desk Manager PDM Tomcat サービスが実行されていない場合は、このサービスを選択して開始します。
5. CA Service Catalog にログインします。
6. [管理] に移動して [設定] をクリックします。
7. CA APM Services ハイパーリンクをクリックします。
8. CA APM Web サーバ名の編集鉛筆アイコンをクリックします。
9. CA APM Web サーバ名を入力します。
10. CA APM ポート番号の編集鉛筆アイコンをクリックします。
11. ポート番号を入力して [保存] をクリックします。
12. ログアウトして、services.msc で CA Service View サービスを開始します。

CA Service Desk Manager および CA Service Catalog と CA APM との統合が正常に動作することを確認します。

トラブルシューティング

このセクションには、以下のトピックが含まれます。

- [名前にアンダースコア文字を含む Web サーバ \(P. 96\)](#)
- [監査履歴マイグレーションが失敗する \(P. 97\)](#)
- [マイグレーションユーティリティのクラス エラー \(P. 97\)](#)
- [重複アセット名コンフィギュレータ リンクの起動に失敗する \(P. 97\)](#)

名前にアンダースコア文字を含む Web サーバ

問題の状況:

Web サーバのホスト名にアンダースコア文字を使用すると、製品にログインするときや、CA EEM を使用してユーザ設定を行うときに問題が発生する場合があります。

解決方法:

仮想システムまたはゴーストシステムを使用している場合は、アンダースコア文字を含まない別のイメージを作成して、新しいホスト名を設定します。実稼働システムの場合は、別の URL で製品にアクセスできるように、内部ドメインネームシステム (DNS) に新しいホスト名を追加します。

監査履歴のマイグレーションが失敗する

問題の状況:

マイグレーションユーティリティの実行後、監査履歴のステータスアイコンが「エラー」を示し、マイグレーションが失敗したこと通知します。また、マイグレーションユーティリティログに以下のメッセージが記録されます。

`Audit History migration has aborted due to a history data conflict with the Group Separator.` 一意のグループ区切り文字については、CA サポートにお問い合わせください。

解決方法:

CA サポートにお問い合わせください。

マイグレーション ユーティリティのクラス エラー

問題の状況:

ツールキットまたはコマンドプロンプトからのマイグレーションユーティリティを起動しようとすると、以下のエラーメッセージが表示されます。

`Could not find the main class: com.ca.core.gui.Application`

解決方法:

このエラーは、`KETTLE_HOME` のパスが正しく設定されていない場合に発生します。`KETTLE_HOME` 環境変数に、`data-integration` フォルダが含まれている Kettle の正しいパスが設定されていることを確認してください。例：`C:\Program Files\Pentaho\Kettle\`

重複アセット名コンフィギュレータリンクの起動に失敗する

Windows 2008 および Windows 7 オペレーティング システムで有効

問題の状況:

ユーザ アクセス制御(UAC)設定を有効にした状態で重複アセット名コンフィギュレータを実行できません。

解決方法:

ユーザ アクセス制御(UAC)設定を有効にした状態で重複アセット名コンフィギュレータを実行するには、管理者として UI を起動します。

- `LaunchUI.bat` を右クリックし、`[Run as Administrator]` を選択します。

第5章: マルチテナントの実装

このセクションには、以下のトピックが含まれています。

- [マルチテナント \(P. 99\)](#)
- [サービス プロバイダ \(P. 100\)](#)
- [マルチテナントの仕組み \(P. 100\)](#)
- [ユーザインターフェースの影響 \(P. 102\)](#)
- [マルチテナントを実装する方法 \(P. 103\)](#)
- [マルチテナントの有効化 \(P. 104\)](#)
- [テナント、サブテナント、およびテナント グループの管理 \(P. 105\)](#)

マルチテナント

マルチテナントでは、複数の独立したテナント（およびそのユーザ）が CA APM の単一の実装を共有できます。テナント同士は、それぞれの役割とテナント階層によって指定されるとおり、定義された方法で対話するだけです。通常は、役割またはテナント階層によってアクセスが許可されない限り、各テナントは CA APM の実装を、それ自身の使用のためだけに表示します。別のテナントのデータを更新または表示することはできません。

マルチテナントでは、テナントがハードウェアとアプリケーションのサポートリソースを共有できます。これにより、独立した実装の多くの利点を活かしながら、両方のコストを下げるることができます。

マルチテナントは CA APM のインストール時に自動的にインストールされます。CA APM をインストールした後は、このセクションの手順に従ってマルチテナントを実装します。

関連項目：

- [マルチテナントを実装する方法 \(P. 103\)](#)

サービス プロバイダ

サービス プロバイダは、CA APM のマルチテナント実装におけるプライマリ テナント（オーナー）です。CA APM の実装に追加される最初のテナントは、常にサービス プロバイダ テナントです。サービス プロバイダ テナントは、親テナントを持つことができません。

CA APM は、権限のあるユーザ（通常は `uapmadmin`）をサービス プロバイダ テナントに関連付けます。

以下の CA APM タスクをどれでも実行できるのは、サービス プロバイダ テナントのみです。

- テナントの定義、編集、または削除
- テナントがサブテナントを持つことの許可
- テナントのある公開データの更新

注: CA APM 管理者は、テナントユーザに対し、自分のデータ以外のデータへのアクセスを許可できます。また、ユーザの役割では、その役割内のユーザに対し、特定のテナント グループへの読み取りおよび書き込みアクセスを個別に指定できます。ユーザの役割の作成およびユーザへの役割の割り当ての詳細については、「管理ガイド」を参照してください。

マルチテナントの仕組み

[マルチテナントを有効にする](#) (P. 104) と、各連絡先に対し、すべてのテナント（パブリック）、単一テナント、またはテナント グループ（ユーザ定義または製品によって維持されるもの）へのアクセスを許可できます。連絡先の役割はアクセス権を制御し、このアクセス権によって読み取りと書き込みの権限が別々に指定されます。

注: ユーザの役割の作成およびユーザへの役割の割り当ての詳細については、「管理ガイド」を参照してください。

マルチテナントを有効にした場合、ほとんどの CA APM オブジェクトには、そのオブジェクトを所有するテナントを指定するテナント属性が含まれます。オブジェクトは、テナント属性とオブジェクトの使用方法に基づいて、以下の 3 つのグループに分類されます。

テナントなし

テナント属性を使用しないでオブジェクトを定義します。これらのオブジェクト内のデータはすべて公開データであり、すべてのユーザはテナントのない公開データを作成および更新できます。

テナント必須

(DBMS ではなく CA APM によって強制される) `null` にできないテナント属性を使用してオブジェクトを定義します。これらのオブジェクト内のデータはすべて、個々のテナントに関連付けられます。パブリック データはありません。

テナント任意

`null` にできるテナント属性を使用してオブジェクトを定義します。これらのオブジェクトは、「テナントあり」または「パブリック」として作成できます。テナントのドロップダウンリストでテナントを選択してオブジェクトを作成するとき、そのオブジェクトはテナントのあるオブジェクトになります。ただし、テナントのドロップダウンリストで「[公開データ] オプションを選択するとき、そのオブジェクトはテナントのあるパブリック オブジェクトになります。1つのテナントを公開するだけの役割に割り当てられているユーザには、データの入力時にテナントのドロップダウンリストが表示されません。

ユーザがデータベースに対してクエリを実行すると、その結果は、ユーザがアクセスを許可されているテナントに属するオブジェクトに制限されます。つまり、表示されるのは、アクセスが許可されているテナントに属するデータのみで、テナントが必要なテーブル内のデータは表示されません。テナントのある公開データの場合は、公開データでもあるので、テナントがオプションのテーブル内で見ることができます。

テナント ユーザがデータベース オブジェクトの作成または更新を要求するときは、そのユーザの現在の役割が更新できるテナントにオブジェクトが属しているかどうかが確認されます。また、そのオブジェクトから他のオブジェクトへのすべての参照も確認されます。つまり、パブリック (テナントなし) オブジェクトへの参照、同じテナントのオブジェクトへの参照、またはオブジェクトのテナントの上位テナント階層内のテナントのオブジェクトへの参照であるかどうかが確認されます。テナントのあるオブジェクトは、その親テナントに属するオブジェクトや、その親の親に属するオブジェクトなどを参照できるということです。

オブジェクトを作成するユーザが複数のテナントに対して更新アクセス権を持っている場合、そのユーザはテナントを明示的に指定する必要があります (直接的または間接的に)。

注: 参照されるオブジェクトの制限には例外が 1 つあります。一部の参照では、包含オブジェクトのテナント階層内のテナントに属しているオブジェクトへの参照が許可されます。このような参照は CA APM オブジェクトスキーマで `SERVICE_PROVIDER_ELIGIBLE` として指定されます。`SERVICE_PROVIDER_ELIGIBLE` フラグが重要な意味を持つのは、サービス プロバイダ テナントが、オブジェクトのテナントの上位テナント階層にない場合だけです。サービス プロバイダ テナントがこの階層内にある場合は、テナント検証ルールによってサービス プロバイダ の参照が許可されます。

オブジェクトの作成または更新を要求しているサービス プロバイダ ユーザには、テナント ユーザと同じ制限が適用されます。ただし、そのサービス プロバイダ ユーザには、テナントのあるパブリック オブジェクトを作成または更新する権限を与えることができます。この権限は、サービス プロバイダ ユーザについて定義された役割によって制御されます。テナントのあるオブジェクトを作成している複数のテナントに対する権限を持つサービス プロバイダ ユーザは、テナントを直接的または間接的に指定する必要があります。

ユーザ インターフェースの影響

マルチテナント機能を実装すると、ユーザの役割に関連付けられた権限およびテナント アクセス権に応じて、ユーザ インターフェースが変わります。

注: ユーザの役割の作成およびユーザへの役割の割り当ての詳細については、「管理ガイド」を参照してください。

テナント ユーザ

1 つのテナントに制限され、管理者でないテナント ユーザの場合、ユーザ インターフェースは以下のように変更されます。

- 複数のテナントに属するすべてのユーザは、情報の入力時およびレポートの生成時に、ドロップダウンリストからテナントを選択できます。
注: レポートの生成時にユーザがテナントを選択することを望まない場合は、レポートからテナント ドロップダウンリストを削除できます。テナント ドロップダウンリストの削除の詳細については、「ユーザ ガイド」を参照してください。
- 複数のテナントに対する読み取りアクセス権を持つすべてのユーザには、検索結果内に [テナント名] の列が表示されます。

マルチテナントを実装する方法

マルチテナントでは、複数の独立したテナント（およびそのユーザ）が CA APM の単一の実装を共有できます。テナント同士は、それぞれの役割とテナント階層によって指定されるとおり、定義された方法で対話するだけです。通常は、役割またはテナント階層によってアクセスが許可されない限り、各テナントは CA APM の実装を、それ自身の使用のためだけに表示します。別のテナントのデータを更新または表示することはできません。

CA APM でマルチテナントを実装するには、以下の手順に従います。

1. CA CASM サービスが開始されていることを確認します。
2. マルチテナントを実装するユーザが、マルチテナント管理アクセス権が有効になっている役割に割り当てられていることを確認します。
注: 役割の定義およびユーザへの役割を割り当ての詳細については、「管理ガイド」を参照してください。
3. [マルチテナントを有効化](#) (P. 104) します。
4. [テナント、サブテナント、およびテナント グループを定義](#) (P. 105) します。
5. CA APM Web サーバおよびアプリケーションサーバを再起動します。
6. 権限のあるユーザ名（通常は *uapmadmin*）を使って製品にログインし、以下の手順に従います。
 - a. テナントアクセス権を備えたユーザの役割を定義します。
 - b. 連絡先を定義します。つまりユーザをインポートして同期します。
注: ユーザのインポートおよび同期の詳細については、「管理ガイド」を参照してください。
 - c. 製品を使用する権限をユーザに付与します。
注: ユーザへの権限付与の詳細については、「管理ガイド」を参照してください。
 - d. 連絡先をユーザの役割に割り当てます。
7. 権限のあるユーザ名を使って製品にログインし、マルチテナント制限が適用されていることを確認します。

マルチ テナントの有効化

複数の独立したテナント（およびそのユーザ）が CA APM の単一の実装を共有できるように、マルチテナントを有効にします。マルチテナントを有効にする前に、テナント、サブテナント、テナント グループの定義、ユーザの役割の作成、および役割へのユーザの割り当てを行います。マルチテナントを有効にすると同時に、マルチテナント実施が有効になります。マルチテナント実施とは、オブジェクトがテナントを必要としているとき、テナント制限を満たさないとレコードを保存できないことを意味します。

注: ユーザの役割の作成およびユーザへの役割の割り当ての詳細については、
「管理ガイド」を参照してください。

マルチテナントを有効にする方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. [編集] をクリックします。
3. [ステータス] ドロップダウンリストから、以下のオプションのいずれかを選択します。

オフ

マルチテナントを無効にします。

オン

マルチテナントを有効にします。

4. テナントの最大深度を定義するフィールドに、テナント階層に許可される最大深度を指定します。
5. [保存] をクリックします。
マルチテナントが有効になります。
6. Web サーバおよびアプリケーション サーバを再起動します。

関連項目:

[テナント管理ページを表示できないというブラウザ エラーが表示される \(P. 168\)](#)

テナント、サブテナント、およびテナント グループの管理

CA APM の単一の実装を共有するには、テナント、サブテナント、およびテナント グループを定義します。マルチテナントでは、テナントがハードウェアとアプリケーションのサポートリソースを共有できます。これにより、独立した実装の多くの利点を活かしながら、両方のコストを下げるることができます。

テナントの定義

テナントは、顧客にサポートを提供する複数の個別の企業を管理するために必要な数だけ定義できます。テナントを必要とするオブジェクトのインスタンスを更新する前に、テナントを定義します。

重要: 最初に作成されるテナント（サービス プロバイダ）は、CA APM のマルチテナント実装におけるプライマリ テナント（オーナー）です。サービス プロバイダ テナントは、親テナントを持つことができません。サービス プロバイダ テナントを定義したら、製品からログアウトし、サービス プロバイダのメンバとして再度ログインします。権限のあるユーザ（uapmadmin）としてログインすることをお勧めします。このユーザは自動的にサービス プロバイダ テナントのメンバになるからです。

テナントを定義する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント] をクリックします。
[テナント] ページが表示されます。
3. [テナントの作成] をクリックします。
[テナントの新規作成] ページが表示されます。
4. テナント情報を入力します。以下のフィールドについて説明します。

テナント番号

(情報のみ) テナント番号が表示されます。CA APM では、このフィールドを使用しません。

レコード ステータス

テナントをアクティブまたは非アクティブに設定します。サービス プロバイダ テナントを定義した後、このオプションはテナントに対して読み取り専用になります。

使用条件

(情報のみ) テナントに対する使用条件を表示します。CA APM では、このフィールドを使用しません。

親テナント

このテナントの上に別のテナントを指定して、このテナントをテナント階層におけるサブテナントにします。

サブテナントを許可

このテナントがサブテナントを持つことができるようになります。テナントは設定を変更することができません。

テナントの深さ

(情報のみ) このテナントの深さを指定します。

ロゴ

(情報のみ) テナントのロゴを含む画像ファイルの URL を表示します。任意の種類の Web 画像を使用できます。CA APM では、このフィールドを使用しません。

連絡先

連絡先ルックアップ ページを表示します。

ロケーション

ロケーションルックアップ ページを表示します。

5. [保存] をクリックします。

テナントが定義されます。

テナントの更新

既存のテナントの情報は、必要に応じて更新できます。

テナントを更新する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント] をクリックします。
[テナント] ページが表示されます。

3. 更新するテナントを検索して見つけます。
検索条件に一致するすべてのテナントが、[テナント] リストに表示されます。
4. 更新するテナントをクリックします。
テナント情報が表示されます。
5. [編集] をクリックします。
6. テナントの新しい情報を入力します。
7. [保存] をクリックします。
テナントが更新されます。

テナントのアクティブ化

非アクティブな特定のテナントの情報を参照または入力する必要があるときは、そのテナントをアクティブにすることができます。たとえば、サービスプロバイダが、特定のテナントに提供したサービスに対する支払いをまだ受け取っていないとします。サービスアグリーメントに基づいて、サービスプロバイダはテナントを非アクティブにし、支払いが行われるまでサービスの提供を停止します。テナントがサービスの支払いを行ったら、サービスプロバイダはテナントをアクティブにします。

テナントをアクティブにする方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント] をクリックします。
[テナント] ページが表示されます。
3. アクティブにするテナントを検索して見つけます。
検索条件に一致するすべてのテナントが、[テナント] リストに表示されます。
4. アクティブにするテナントをクリックします。
テナント情報が表示されます。
5. [編集] をクリックします。
6. [レコードステータス] ドロップダウンリストで、[アクティブ] を選択します。
7. [保存] をクリックします。
テナントがアクティブになります。

新しいテナントを初期化する方法

サービス プロバイダは、コストセンター、コストタイプ、部門など、新しいテナントのための標準的なデータ セットを定義できます。テナント用のデータをインポート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。

テナント グループの定義

テナントへのアクセスを分類、管理、および制御するために、テナント グループを定義できます。たとえば、特定の地理的な場所に属するテナントを含むテナント グループに、アセット マネージャを割り当てることができます。

テナント グループを定義する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント グループ] をクリックします。
[テナント グループ] ページが表示されます。
3. [テナント グループの作成] をクリックします。
新規テナントのグループ詳細ページが表示されます。
4. テナント グループ情報を入力します。
5. [保存] をクリックします。
テナント グループが定義されます。
6. [テナントの割り当て] をクリックします。
[テナントの検索] ページが表示されます。
7. グループに追加するテナントを検索して選択します。
テナントがグループに追加されます。

テナント グループの更新

テナント グループのメンバと詳細情報を管理するために、テナント グループを更新できます。

テナント グループを更新する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント グループ] をクリックします。
[テナント グループ] ページが表示されます。
3. 更新するテナント グループを検索して見つけます。
検索条件に一致するすべてのテナント グループが、[テナント グループ] リストに表示されます。
4. リスト内のテナント グループをクリックします。
テナント グループの詳細ページが表示されます。
5. [編集] をクリックします。
6. テナント グループの新しい情報を入力します。
7. (オプション) [テナントの割り当て] をクリックして、グループにテナントを追加します。
注: テナントを追加または削除すると、そのテナントのサブテナントも追加または削除されます。
8. [保存] をクリックします。
テナント グループが更新されます。

テナント階層

テナント階層とは、テナントに親テナントを割り当てるシステムによって作成または変更される、構造化されたテナント グループです。テナントは親のサブテナントになり、その階層においてより高いテナント(存在する場合)になります。

注: サービス プロバイダは複数の独立した階層を作成できます。またはまったく作成しないことも可能です。テナント階層のあるシステム内にも、スタンドアロンテナントを定義できます。

CA APM がサポートするテナント階層の深さは無制限です。ただし、サービス プロバイダは、テナントの総数およびテナント階層の深さ(デフォルトは4 レベル)を制限できます。また、サービス プロバイダは、各テナントがサブテナントを持つことができるかどうかを決定します。

注: 必ずしも必要ではありませんが、サービス プロバイダはテナント階層に参加できます。サービス プロバイダが親テナントを持つことはできません。

サブテナントの定義

サブテナントを使用すると、組織の目的およびデータ共有の目的のために、テナント階層を定義および変更できます。テナントをテナント階層内に配置するには、そのテナントの親テナントを指定します。

サブテナントを定義する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント] をクリックします。
[テナント] ページが表示されます。
3. [テナントの作成] をクリックします。
テナントの新規作成ページが表示されます。
4. サブテナント情報を入力します。以下のフィールドについて説明します。

親テナント

このテナントの上に別のテナントを指定して、このテナントをテナント階層におけるサブテナントにします。

注: [親テナント] ドロップダウンには、サブテナントを持つことを許可されたテナントのみが表示されます。

5. [保存] をクリックします。
テナントは親テナントのサブテナントです。
- 注: サブテナントになったテナントは、親テナントの他のサブテナントなど（ある場合）と共に、親テナントのサブテナント グループに所属します。親テナントは、親テナントの他のスーパー テナントなど（ある場合）と共に、その新しいサブテナントのスーパー テナント グループを結合します。それぞれが、他方に関連するテナント グループを結合します。

サブテナントの更新

既存のサブテナントの情報は、必要に応じて更新できます。

サブテナントを更新する方法

1. [管理] - [テナント管理] をクリックします。
マルチテナント管理ページが表示されます。
2. 左側で、[テナント] をクリックします。
[テナント] ページが表示されます。

3. 更新するテナントを検索して見つけます。
検索条件に一致するすべてのテナントが、[テナント] リストに表示されます。
4. リスト内のテナントをクリックします。サブテナント名が [テナント] リストの [名前] 列に表示されます。
テナント情報が表示されます。
5. [編集] をクリックします。
6. サブテナントの新しい情報を入力します。
7. [保存] をクリックします。
サブテナントが更新されます。

製品によって維持されるテナント グループ

製品では、テナント階層内の各テナントについて以下のテナント グループが自動的に生成および維持されます (*tenant* はテナント名)。

- *tenant_subtenants* (テナント、その子テナント、およびそれぞれの下位のサブテナント)
- *tenant_supertenants* (テナント、親テナント、およびそれぞれの上位スーパー テナント)
- *tenant_relatedtenants* (単一の階層全体)

システムによって維持されるテナント グループは、ユーザ定義のテナント グループと同じように使用できます。ただし、名前と説明しか変更できません。

第6章: その他の製品の統合

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 Business Intelligence の統合 \(P. 113\)](#)

[CA EEM 統合 \(P. 116\)](#)

[CA CMDB の統合 \(P. 117\)](#)

[通知プロセスのための CA Process Automation 統合 \(P. 124\)](#)

[Data Importer プロセスのための CA Process Automation 統合 \(P. 132\)](#)

[CA Service Catalog インテグレーション \(P. 135\)](#)

CA Business Intelligence の統合

CA Business Intelligence は、情報を提示し、ビジネス上の意思決定をサポートするために複数 CA 製品によって使用される、一連のレポートおよび分析ソフトウェアです。このような CA 製品は CA Business Intelligence を使用して、効果的な企業 IT 管理に必要な重要な情報を統合、分析、および提示します。

CA Business Intelligence では、情報管理、レポート、クエリ、および解析の各ツールが揃った包括的なスイートを提供するスタンダードアロン製品として、SAP BusinessObjects Enterprise がインストールされます。インストールされた製品は他の CA 製品から独立して動作するため、CA 製品間で同じ CA Business Intelligence サービスを共有することができます。

CA 製品は、BusinessObjects Enterprise テクノロジを使用したレポート、クエリ、分析などの幅広い一連のビジネスインテリジェンス機能を活用します。CA APM には、事前定義された BusinessObjects Enterprise レポートが用意されています。事前定義済みレポートの詳細については、「ユーザガイド」を参照してください。CA Business Intelligence はほかにも設定可能なレポート機能をユーザーに提供します。

BusinessObjects Enterprise のインストールメディアとマニュアルは、CA APM のインストールメディアとマニュアルと共に提供されます。

重要: CA APM をインストールする前に、CA Business Intelligence をインストールする必要があります。

CA APM と CA Business Intelligence の統合方法

重要: CA APM をインストールする前に、CA Business Intelligence をインストールする必要があります。

CA APM は、BusinessObjects Enterprise レポートの使用を開始するために必要なデータを提供します。BusinessObjects Enterprise と CA APM をインストールした後で、レポートを使用する前に必要なセットアップタスクを実行します。CA APM を BusinessObjects Enterprise に統合するには、以下の手順に従います。

1. 製品を管理および使用できるように、マニュアルなどで BusinessObjects Enterprise に関する知識を深めます。少なくとも以下の機能を実行できる必要があります。
 - CA Business Intelligence をインストールする。これによって BusinessObjects Enterprise がインストールされます。
 - BusinessObjects Enterprise に含まれる事前定義済みレポートを使用する。
2. CA Business Intelligence BusinessObjects Enterprise をインストールし、以下のログイン認証情報と接続情報を書き留めます。これらの情報は CA APM のインストール中に入力を求められます。
 - BusinessObjects Enterprise 管理者 ID
 - BusinessObjects Enterprise 管理者パスワード
 - BusinessObjects Enterprise Central Management Server (CMS) ポート。CMS は、CA Business Intelligence と共に使用する BusinessObjects に関する情報のデータベースを維持します。デフォルトの CMS ポートは 6400 です。
3. CA MDB として Oracle を使用している場合は、CA Business Intelligence がインストールされているサーバ上で Oracle ネットサービス名 (NSN) を定義します。NSN を書き留めます。NSN は CA APM のインストール中に入力を求められます。
4. BusinessObjects Enterprise を起動して、BusinessObjects Enterprise がインストールされていることを確認します。

5. CA APM をインストールします。CA APM をインストールすると、Oracle および SQL Server データベースの両方の BIAR ファイルがインストール、設定されます。BIAR ファイルには、CA Business Intelligence ユニバース、事前定義済みレポート、および CA APM デフォルト管理者ユーザ (uapmadmin) が含まれます。

注: CA APM をインストールするときは、書き留めておいた BusinessObjects Enterprise ログイン認証情報、BusinessObjects Enterprise CMS ポート、および Oracle NSN を入力します。CA Business Intelligence サーバに .NET フレームワークがインストールされていない場合は、CMS ポートの入力を求められたときに「6400」と入力します。

6. 事前定義済みレポートについて理解したうえで、レポートを使用します。CA APM の事前定義済みレポートの詳細については、「ユーザガイド」を参照してください。
7. BusinessObjects Enterprise を管理および使用するときは、以下のベストプラクティスに従います。
 - 各 CA 製品につき 1 つのユニバースをインストールして管理します。
 - デフォルトのユニバースは変更しないでください。代わりに、ユニバースをコピーし、コピーに変更を加えます。そうしないと、サービスパック、パッチ、およびその他の更新を適用したときに、すべてのカスタム変更が失われる可能性があります。
 - サービスパック、パッチ、およびその他の更新をカスタムユニバースに適用する前に、変更をバックアップします。
 - レポートが正しく機能しない場合は、CMS が動作しているかどうかを確認します。
 - 事前定義済みレポートを上書きしないでください。
 - 事前定義済みレポートは常に、カスタムレポートを作成するためのベースとして使用します。ベースとして使用することで、すべてのレポートで一貫したフォーマットを維持しやすくなります。
 - 管理者はすべてのレポートを変更でき、既存のユニバースに基づいて新規レポートを作成できることを覚えておいてください。ただし、管理者は、既存の CA APM フォルダにレポートを追加することはできません。
 - 管理者とエンドユーザは事前定義済みレポートを変更するべきではありません。事前定義済みレポートに対する変更はすべて、同じ CA Business Intelligence インスタンスを使用しているその他すべてのユーザに適用されてしまうからです。代わりに、カスタムフォルダを作成し、カスタムフォルダにレポートをコピーします。次に、レポートの名前を変更し、レポートをカスタマイズします。
 - 管理者とユーザはどちらも、自分で作成した新規レポートを、自分のカスタムフォルダに追加する必要があります。

レポートの設定および製品の更新

CA APM に更新（パッチ、サービス パック、またはその他の更新）をインストールするときは、更新プロセスによって既存の製品コンポーネントが上書きされます。場合によっては、レポートコンポーネントも上書きされます。その結果、以前に行ったレポート設定がすべて失われる可能性があります。ただし、CA Technologies では、CA APM の更新を適用するときにレポート設定が保持されるようにするための方法を用意しています。CA Technologies が提供するホワイトペーパーの指示に従ってください。このホワイトペーパーは <http://ca.com/jp/support> で見ることができます。

[テクニカル サポート] で、CA Technologies IT Asset Manager の製品ページに移動します。推奨される読み物リストで「*White Paper: Reporting Components Upgrade and Version Control to Retain Customizations*」を検索します。このホワイトペーパーに記載された方法に従うことで、レポート設定を保護できます。

注: レポートの設定の詳細については、「CA Business Intelligence 実装ガイド」を参照してください。

CA EEM 統合

CA APM では、認証に CA EEM を使用します。製品インストールを開始する前に CA EEM をインストールする必要があります。

認証に CA EEM を必要とする他の製品は、CA APM が使用する CA EEM サーバと同じサーバを使用できます。

- CA EEM を使用して、複数の CA Technologies 製品に対してセキュリティを中央的に管理できます。CA APM インストール処理中に既存のサーバの名前、ロケーションおよびログイン認証情報を指定します。
- また、CA APM セキュリティを他の CA Technologies 製品から独立して管理できます。既存の CA EEM がインストールされているもの以外の任意の単一アプリケーションまたは Web サーバに CA EEM をインストールします。

CA CMDB の統合

このセクションは、CA CMDB リリース 12.7 および CA Service Desk Manager リリース 12.7 に含まれる CA CMDB と CA APM を統合する方法について説明します。

CA CMDB は、異種コンピューティング環境において、企業内の IT コンポーネント、サービス、およびコンポーネントとサービスとの関係を管理するための包括的な統合ソリューションです。CA CMDB は、構成アイテム (CI) と呼ばれるアセットについて、およびアセット間の相互関係について、信頼性の高い最新情報を提供および保存することを可能にします。このような関係は、組織内の変更を制御するための重要なツールである影響分析の基盤となります。

CA CMDB は、以下のような複数の分野で CA APM と統合されています。

- CA APM 監査履歴レコードには、CA Service Desk Manager、CA CMDB、および CA APM によってアセット/CI レコードに対して行われたすべての変更を含めることができます。
- CA Service Desk Manager と CA CMDB がインストールされているとき、アセット/CI 監査履歴レコードには、CA CMDB の [Versioning] タブ上の CA APM 監査履歴レコードがすべて含まれます。
- CA APM 内でアセットを定義するときは、[アセット] チェックボックスと [CI] チェックボックスのオン/オフを切り替えることで、アセット/CI レコードを分類および制御できます。この柔軟性が提供されているのは、CA CMDB が作成する CI が CA APM に関連しない場合があるためです。逆に、CA APM が作成するアセットは CA CMDB に関連しない場合があります。
- CA APM では、アセットファミリのコンテキストの中でアセット/CI に関するフィールドを拡張できます。拡張したフィールドは CA APM 内で共有できます。たとえば、CA APM 管理者は、[アセット] ページを設定し、アセット拡張フィールドを定義することで、CA Service Desk Manager と CA CMDB 内で作成される CI をユーザーに表示および更新させることができます。
- CA APM 内で CA CMDB と共有されるフィールドに対してイベントを定義し、CA APM または CA CMDB 内でそのイベントをトリガできます。イベントと通知の管理の詳細については、ユーザガイドを参照してください。
- CA Service Desk Manager および CA CMDB ユーザは、管理データリポジトリ (MDR) を定義し、CA CMDB CI による CA APM 内の対応するアセットの起動を許可することができます。

CA APM と CA CMDB の統合方法

CA APM と CA CMDB を統合すると、CA APM が管理するアセットと、CA CMDB が管理する構成アイテム (CI) は、単純かつ正確な方法で統合および区別されます。CA APM ユーザは、アセットと CI の共有分類モデルに移行できます。CA APM と CA CMDB を統合するには、以下の手順に従います。

1. [アセットと構成アイテムの監査履歴レコードを共有](#) (P. 118) します。
2. [アセットと構成アイテムのレコードを分類](#) (P. 118) します。
3. [アセットの拡張フィールドを定義](#) (P. 121) します。
4. [共有フィールドに対してイベントを定義](#) (P. 123) します。
5. [CA Service Desk Manager および CA CMDB から管理データ リポジトリ \(MDR\) を定義](#) (P. 123) します。

アセットと構成アイテムの監査履歴レコードの共有

CA APM と CA CMDB を統合するために、CA APM の監査履歴レコードに、CA Service Desk Manager、CA CMDB、および CA APM によってアセット/CI レコードに対して行われたすべての変更を含めることができます。また、CA Service Desk Manager、CA CMDB、またはその両方がインストールされているとき、CA CMDB 内のアセット/CI 監査履歴レコード (バージョン管理タブ) には、CA APM のすべての監査履歴レコードが含まれます。

CA CMDB 11.2 以降では、CA APM の監査履歴レコードが含まれます。CA Asset Portfolio Management のイベントサービスを開始すると、監査履歴レコードは CA CMDB と CA APM の両方で更新されます。詳細については、「[サービスの開始](#) (P. 24)」を参照してください。

アセットと構成アイテムのレコードの分類

CA APM と CA CMDB を統合するこの手順では、CA APM 内でアセットを定義するときに、[アセット] チェック ボックスと [CI] チェック ボックスのオン/オフを切り替えることで、アセットと CI のレコードを分類および制御できます。CA CMDB によって作成される CI が CA APM に関連しない場合があることと、反対に、CA APM によって作成されるアセットが CA CMDB に関連しない場合があることによって、このような柔軟性が実現します。

これらのチェック ボックスを使用するときは、以下の情報を考慮してください。

デフォルト値

- CA APM によって作成されるすべての新規アセット レコードは、あらかじめ、[an Asset only] および [CA APM で管理] の両方として設定されます。CA APM の [新規アセット] ページで、[アセット] チェック ボックスはオン、[CA APM で管理] チェック ボックスはオフ、および [CI] チェック ボックスはオフになっています。
- CA CMDB によって作成される (CA Service Desk Manager の有無にかかわらず) すべてのアセット レコードは、あらかじめ [CI only] に設定されます。CA CMDB の [CI] ページで、[CI] 列見出しが [はい] に、[アセット] 列見出しが [いいえ] にそれぞれ設定されます。
- CA APM と CA CMDB ではいずれも、[新規アセット] ページと [CI] ページに [アセット] フィールドと [CI] フィールドが表示されます。ただし、[CA APM で管理] チェック ボックスが表示されるのは CA APM だけです。各製品の既存の監査およびセキュリティ機能は、これらのチェック ボックスに適用されます。

デザイン

- 他の CA Technologies 製品がインストールされても、CA APM と CA CMDB には [アセット] フィールドと [CI] フィールドが表示されます。CA CMDB がインストールされていないとき、CA Service Desk Manager に [アセット] フィールドと [CI] フィールドは表示されません。
 - CA APM 管理者は、ユーザインターフェースを設定し、[アセット] フィールドと [CI] フィールドを新しい場所に移動できます。また、これらのフィールドを、読み取り専用、必須、オプション、または非表示にすることができます。
- 注:** ユーザインターフェースの設定の詳細については、「管理ガイド」を参照してください。

表示および更新

CA CMDB

- デフォルトでは、CA CMDB アナリストおよび管理者は、[アセット] フィールドと [CI] フィールドの値を更新できます。
- CA CMDB ではデフォルトで、[アセット] の値が [はい] に設定されているとき、[アセット] の値を変更することは許可されません。

CA APM

- デフォルトでは、CA APM にはアセットと CI のレコードが表示されます。
- CA APM 管理者は、ユーザインターフェースを設定し、[アセット] チェック ボックスと [CI] チェック ボックスを新しい場所に移動できます。また、これらのチェック ボックスを、読み取り専用、必須、オプション、または非表示にすることができます。[CI] チェック ボックスをオンにしてアセットを保存すると、[CI] チェック ボックスは非表示になり、設定を変更することができなくなります。

重要: CA APM の [CI] チェック ボックスを読み取り専用に設定し、チェック ボックスの設定を変更できる権限を CA CMDB アナリストおよび管理者のみに制限することを強くお勧めします。

- [CA APM で管理] チェック ボックスがオンになっている CA APM 内のアセットは、常にアセットです。[CA APM で管理] チェック ボックスがオンになっている CA APM 内のアセットを保存するには、[アセット] チェック ボックスもオンにする必要があります。

検索

CA CMDB

- CA CMDB 検索ではデフォルトで、すべてのレコードが初期表示されます。ただし、レコードをフィルタするためのオプションが用意されています。
- 注:** CA Service Desk Manager をインストールした場合、同じデフォルト検索ルールが適用されます。

CA APM

- デフォルトのアセット検索には、[CA APM で管理]、[CI]、および [アセット] の値を持つドロップダウンリストが含まれます。この柔軟性が提供されている理由は、アセットと CI を区別できるようにするためです。

ハードウェア照合

ハードウェア照合では、すべてのアセット レコードと CI レコードが分析されます。ハードウェア照合によって検出されたアセットに関連する任意の CI を表示する方法には、検索を利用します。CA APM ユーザは例外を表示し、[アセット] チェック ボックスをオンにするかどうかを決定できます。[アセット] チェック ボックスをオンにすると、CA APM アセット検索でアセット レコードを利用できるようになります。

アセット拡張フィールドの定義

CA APM と CA CMDB を統合するこの手順では、CA APM で、アセットファミリのコンテキストの中でアセットに関するフィールドを拡張できます。拡張したフィールドは CA APM 内で共有できます。たとえば、CA APM 管理者は、[アセット] ページを設定し、アセット拡張フィールドを定義することで、CA Service Desk Manager と CA CMDB 内で作成される CI をユーザに表示および更新させることができます。

重要: これらの手順が当てはまるのは、初めてウィザードを実行し、アセット拡張フィールドを定義するときだけです。拡張フィールドを定義する前に、参照用の CA CMDB 内の `usp_owned_resource` テーブルに次の情報があることを確認します：テーブル名、形式（文字、ブール、通貨、日付、小数、または整数）、フィールド名、属性名、およびフィールドサイズ。ウィザードを完了した後、CA APM では、他のすべてのフィールドと同じように拡張フィールドを設定できます。

例: 「保証開始日」のアセット拡張フィールドの定義

この例では、「保証開始日」のアセット拡張フィールドを定義します。CA Service Desk Manager/CA CMDB 内の [在庫] タブで、CI 内のラベルを「保証開始日」として表示します。次に、CA CMDB 内の `usp_owned_resource` テーブルで、関連する `nr_wrty_st_dt` 列の情報を表示します。この例で、`nr_wrty_st_dt` 列形式は整数、フィールド名は `nr_wrty_st_dt`、属性名は `nr_wrty_st_dt`、フィールドサイズは 4 です。この情報を記録し、ウィザード内の適切な [形式]、[フィールド名]、[属性名]、および [フィールドサイズ] フィールドに、表示されるとおりに入力します。混乱を避けるため、ウィザード内の [ラベル] フィールドでは、CI と同じラベル（「保証開始日」）を使用することをお勧めします。

アセット拡張フィールドを定義する方法

1. CA Service Desk Manager と CA CMDB の拡張テーブル名とデータベース フィールド名を決定するには、CA Service Desk Manager と CA CMDB のスキーマ ファイルを確認します。

注: CA Service Desk Manager と CA CMDB のスキーマ ファイルの詳細については、CA Service Desk Manager と CA CMDB のマニュアルを参照してください。

2. 拡張を定義する権限のあるログイン認証情報をを使って CA APM にログインします。
 3. [アセット] - [新規アセット] をクリックします。
 4. 左側の [設定: オン] をクリックします。
- ページの設定が有効になります。

5. ページの [構成情報] 領域で、グローバル設定を定義して保存します。
 6. [拡張の追加] をクリックします。
ウィザードが表示されます。
 7. 画面の指示に従って、拡張フィールドの情報を入力します。
 8. ウィザードの [タイプ] ページで、以下の手順に従います。
 - a. [単純型のフィールド] オプションを選択します。
 - b. 新しいフィールドが表示されるページの一部を選択します。
 - c. [すべての拡張タイプ] タイプチェック ボックスをオンにします。
 - d. [次へ] をクリックします。
 9. ウィザードの [フィールド] ページで、以下の手順に従います。

重要: CA CMDB 内の `usp_owned_resource` テーブルの列情報を入力します。また、混乱を避けるため、[ラベル] フィールドでは、CI と同じラベルを使用することをお勧めします。

 - a. [フィールドの追加] をクリックします。
 - b. ページに表示するフィールド ラベルを入力します。
 - c. データ形式を選択します。
 - d. データベース フィールド名を入力します。
 - e. 属性名を入力します。
 - f. フィールド サイズを入力します。
 - g. (オプション) フィールドの説明を入力します。
 - h. フィールドへの入力が必須かどうかを指定します。
 - i. チェックマーク アイコンをクリックして、フィールドを保存します。
入力したフィールド情報が製品で表示されます。
 - j. [次へ] をクリックします。
 10. ウィザードの [概要] ページで、フィールド情報を確認し、[保存して終了] をクリックします。
 11. フィールドが [アセット] ページに表示されることを確認します。
 12. [設定の保存] をクリックします。
- ページ上の拡張フィールドがすべてのユーザに表示されます。CA APM 内でイベントを定義し、CA APM または CA CMDB 内でそのイベントをトリガできます。イベントの管理の詳細については、「ユーザ ガイド」を参照してください。

共有フィールドに対するイベントの定義

CA APM と CA CMDB の間で共有される任意のフィールドに対して、CA APM 内でイベントを定義できます。CA Service Desk Manager/CA CMDB または CA APM 内の変更によってイベントの条件が満たされると、イベントが実行され、通知が送信されます。たとえば、[アセット] ページの [連絡先] フィールドに対してイベントを定義できます。イベントが変更イベントである場合、アセットまたは関連する構成アイテム (CI) で [連絡先] フィールドを変更すると、イベントを実行できます。イベントが実行されると、通知が送信されます。

注: イベントと通知の管理の詳細については、「ユーザ ガイド」を参照してください。

CA Service Desk Manager および CA CMDB からの管理データリポジトリ (MDR) の定義

CA APM と CA CMDB を統合するこの手順では、CA Service Desk Manager および CA CMDB ユーザが管理データリポジトリ (MDR) を定義し、CA CMDB CI によって CA APM 内の対応するアセットをコンテキストの中で起動できるようにすることができます。

CA Service Desk Manager および CA CMDB から MDR を定義する方法

1. CA Service Desk Manager Web インターフェースで、管理者としてログインします。
2. [管理] タブを選択します。[管理] ブラウザで、[CA CMDB] - [MDR 管理] - [MDR リスト] を選択します。
3. [新規作成] をクリックします。
MDR プロバイダ定義が表示されます。
4. 以下の、必要な MDR プロバイダ情報を入力します。

ボタン名

ボタン名として「ITAM」を指定します。

MDR 名

MDR 名として「ITAM」を指定します。

MDR クラス

MDR クラスとして「**GLOBAL**」を指定します。

ホスト名

CA APM Web サーバのネットワーク アドレスまたは DNS 名を使用して、CA APM サーバ名を指定します。

重要: MDR プロバイダ フォームでは、入力した情報に基づいて [コンテキストで起動する URL] フィールドが自動的に入力されます。したがって、このフィールドには値を入力しません。

5. [保存] をクリックします。
CA APM MDR プロバイダが定義されます。
6. CA CMDB で、CI を定義します。
7. CI 詳細フォームの [属性] タブをクリックします。
8. 事前に定義した [ITAM] ボタンをクリックします。
CA APM 内の対応するアセットが表示されます。

通知プロセスのための CA Process Automation 統合

CA APM と CA Process Automation を統合すると、定義されたイベントが発生した後に特定の受信者に対して通知を配信する通知プロセスをセットアップおよび設定できます。CA APM は電子メール通知プロセスの製品を提供します。このようなプロセスは、製品のインストールメディアに含まれているファイルで提供されます。CA Process Automation 内にファイルをインポートし、CA Process Automation および CA APM 内でプロセス パラメータを指定します。

CA Process Automation 通知プロセスのセットアップ方法

CA APM で提供される電子メール通知プロセスをセットアップするには、以下の手順に従います。

1. CA APM と CA Process Automation をインストールします。
2. CA Process Automation で、[ワークフロープロバイダ通知プロセス ファイルをインポート](#) (P. 125) します。

3. CA Process Automation で、[メール サーバを設定](#) (P. 126) します。
4. CA Process Automation で、[ワークフロー プロセス パラメータの設定を変更](#) (P. 127) します。
 - a. 管理者のデフォルトの電子メール アドレスを変更して (Admin_Email_To パラメータ) 、必要な設定を指定します。
 - b. CA APM のデフォルトの URL を変更して (ITAM_URL パラメータ) 、必要な設定を指定します。
 - c. CA Process Automation のデフォルトの URL を変更して (ITPAM_URL パラメータ) 、必要な設定を指定します。
 - d. (オプション) 必要な設定を指定したい他のパラメータをすべて変更します。
5. CA APM と CA EEM で、[CA APM ユーザに対して CA Process Automation の使用を許可](#) (P. 130) します。
6. CA EEM で、CA APM ユーザ以外のユーザの CA Process Automation ユーザ アカウントを作成します。
7. CA APM で、イベントを定義するときのワークフロー プロセス パラメータを指定します。

注: CA APM 内でのイベント定義の詳細については、「ユーザ ガイド」を参照してください。注: CA Process Automation と CA EEM の使用の詳細については、CA Process Automation と CA EEM のマニュアルを参照してください。

ワークフロー プロバイダ通知プロセス ファイルのインポート

CA APM には、デフォルトの電子メール通知プロセス ファイルが用意されています。これらのファイルを CA Process Automation にインポートした後に、製品内で電子メール通知をセットアップおよび設定できるようになります。

注: ファイルのインポートおよび操作の詳細については、CA Process Automation のドキュメントを参照してください。

次の手順に従ってください:

1. 管理者として CA Process Automation にログインします。
2. CA Process Automation クライアントに移動します。

3. 以下のパスを使用して、CA APM インストール メディア上の ITAM.xml ファイルを探します。

CD1¥SetupFiles¥ITPAM¥

4. ITAM.xml ファイルを / ノードへインポートします。

注: CA Process Automation リリース 3.1 では、クライアントから XML ファイルをインポートします。リリース 4.0 SP1 では、[ライブラリ] タブから XML ファイルをインポートします。

インポートしたバージョンを現在のバージョンとして設定し、インポートしたカスタム演算子とセンサを利用可能にするためのインポート オプションを選択します。

通知プロセス ファイルがデフォルトの /ITAM フォルダへインポートされます。

CA Process Automation メール サーバの設定

CA Process Automation と CA APM 間に電子メール通知を実装するには、CA Process Automation に対してメール サーバを設定します。

注: メール サーバをセットアップするために CA Process Automation アラート モジュールを設定する具体的な手順については、「*CA IT Process Automation Manager Administration Guide*」を参照してください。

1. 管理者として CA Process Automation にログインします。
2. CA Process Automation クライアントに移動します。
3. ライブラリ ブラウザに移動します。
4. デフォルト環境を特定し、ロックします。
5. アラート モジュールを特定し、継承のチェック ボックスをオフにします。
6. SMTP (メール) サーバを指定します。

例: mail.company.com

7. 送信元アドレスを指定します。
例 : admin@company2.com
8. 変更を保存します。
9. デフォルト環境をロック解除します。
変更が有効になるまで数分かかります。

注: SMTP (メール) サーバの設定で外部アドレスへの電子メール配信が許可されている場合、外部電子メールアドレスに電子メール通知を送信することができます。メールサーバの設定を確認して、電子メールを外部アドレスに送信できるかどうかを確認します。

CA Process Automation ワークフロー プロセス パラメータの変更

CA APM と CA Process Automation をインストールし、通知プロセス ファイルを CA Process Automation にインポートすると、デフォルトのワークフロー プロセス パラメータが CA Process Automation 内に定義されます。必要な設定を含めるために、デフォルトのプロセス パラメータを変更できます。プロセス パラメータの実際の (ハードコードされた) 値を入力します。入力した値が有効であることを確認する必要があります。

すべての通知プロセスに適用されるデータ セット内または個々のプロセス開始リクエスト フォーム内の通知プロセス パラメータを変更できます。個々のプロセスについて指定するパラメータは、そのプロセスのメイン データ セット内のパラメータを上書きします。

注: CA APM 内でイベントを定義するときは、ワークフロー プロバイダ用の一部の通知プロセス パラメータを指定します。CA APM でのプロセス パラメータの指定の詳細については、「ユーザ ガイド」を参照してください。

CA Process Automation ワークフロー プロセス パラメータを変更する方法

重要: CA APM および CA Process Automation では、パラメータに入力した情報は検証されません。入力が有効で、正しいフォーマットでデータを入力したことを確認してください。

1. CA Process Automation にログインし、CA Process Automation クライアントに移動します。
2. ITAM フォルダで、Dataset と名前の付いたデータ セットを探します。

3. パラメータの情報を入力します。

以下のフィールドについて説明します。

Ack_Interaction_Form_Full_Path

CA Process Automation 内の確認対話フォームが含まれるファイルのフルパス。電子メール通知受信者は、このフォームを使用して、通知の受信を確認します。個々のワークフロープロセスには、一意のユーザ対話フォームと、フォームへの一意のパスが必要です。製品に付属の確認対話フォームは、プロセスとメインデータセットが格納されているフォルダにあります (/ITAM またはプロセスのインポート先のフォルダ)。

Admin_Email_CC

通知エラーが発生したときに管理者に送信される電子メールの、コピー受信者の電子メールアドレス。

Admin_Email_To

通知エラーが発生したときに管理者に送信される電子メールの、管理者の電子メールアドレス。デフォルト値を必要な設定に変更します。

Log_Folder_Path

通知プロセスでエラーが発生したときに作成されるエラーログファイルのフルパス。パスを指定しない場合、デフォルトの CA Process Automation ログファイルパスが使用されます。

ITAM_Username

CA APM にログインするユーザの名前。CA Process Automation は、通知受信者とエスカレーションに関する情報を取得するため、CA APM へのアクセスを必要とします。

ITAM_Password

CA APM にログインするユーザのパスワード。CA Process Automation は、通知受信者とエスカレーションに関する情報を取得するため、CA APM へのアクセスを必要とします。

Admin_Email_Subject

通知エラーが発生したときに管理者に送信される電子メールの件名。このパラメータは、メインデータセットまたは個々のプロセス開始リクエストフォームで設定できます。

Admin_Email_Header

通知エラーが発生したときに管理者に送信される電子メールのヘッダまたは導入部（「こんにちは」など）。このパラメータは、メインデータセットまたは個々のプロセス開始リクエストフォームで設定できます。

Admin_Email_Footer

通知エラーが発生したときに管理者に送信される電子メールのシグネチャ（「ありがとう」など）。このパラメータは、メインデータセットまたは個々のプロセス開始リクエストフォームで設定できます。

Log_File_Name

通知プロセスでエラーが発生したときに作成されるエラーログファイルの名前。通知エラーが発生したときに管理者に送信される電子メールに、ログファイル名が記載されます。名前を指定しない場合、次のような CA Process Automation のデフォルトログファイル名が使用されます。

`プロセス名_プロセス インスタンス番号.log`

ITAM_URL

通知受信者とエスカレーションに関する情報を取得するために CA Process Automation が CA APM にアクセスするときに使用する CA APM の URL。デフォルト値を必要な設定に変更します。

例：

`http://ITAMAPP SERVER:99/ITAMService/Service.asmx`

ITPAM_URL

電子メール通知メッセージに含まれる CA Process Automation の URL。デフォルト値を必要な設定に変更します。

例：

`http://PAMSERVER:8080/itpam`

4. CA Process Automation の変更を保存します。

注: 通知プロセスのセットアップの詳細については、ワークフロー プロバイダのマニュアルを参照してください。

CA APM ユーザに対する CA Process Automation の使用の許可

通知を受信する CA APM ユーザは、通知を確認するために CA Process Automation にアクセスする必要があります。このようなユーザは、CA Process Automation を使用する権限を持っている必要があります。CA Process Automation の使用をユーザに対して許可するには、最初に CA APM 内の手順を実行し、次に CA EEM 内の手順を実行します。CA APM では、CA APM にログインして CA APM を使用するユーザを定義し、権限を付与します。CA EEM では、権限を付与された CA APM ユーザに対して CA Process Automation の使用を許可します。

CA APM ユーザに対して CA Process Automation の使用を許可する方法

1. CA APM にログインします。
2. 新規ユーザと既存ユーザの両者に、CA APM にログインして CA APM を使用する権限があることを確認します。

注: CA APM で新規ユーザを定義して権限を付与する操作と、既存ユーザに権限を付与する操作の詳細については、「管理ガイド」を参照してください。

CA APM ユーザが定義され、権限が付与されます。CA EEM の利用可能ユーザのリストに CA APM ユーザが含まれています。

- CA EEM にログインし、アプリケーション ドロップダウン リストから CA Process Automation を選択します。

重要: CA EEM にログインして CA APM ユーザに対して CA Process Automation の使用を許可するときは、CA Process Automation アプリケーションを選択する必要があります。

- すべてのユーザのリストから CA APM ユーザを選択し、ユーザのアプリケーション ユーザ詳細をクリックします。
- ユーザの CA Process Automation ユーザ グループを選択し、選択内容を保存します。

注: CA EEM を使用してユーザ詳細にアプリケーションを追加する操作の詳細については、CA EEM のマニュアルを参照してください。

これで CA APM ユーザは、CA Process Automation にアクセスし、製品を使用できます。

パラメータ用の必須インジケータおよび複数行テキストフィールド

製品に付属のデフォルト通知プロセスには、製品のイベント定義ユーザ インターフェースに表示されるパラメータと、ワークフロー プロバイダ内で指定するパラメータが含まれます。デフォルトのプロセスには、製品ユーザ インターフェース上に必須インジケータおよび複数行テキストフィールドを表示できるようにする XML フォーマットも含まれます。これらの項目は、ワークフロー プロバイダから常に利用できるわけではないため、プロセス内で指定されます。各デフォルト プロセスの CA Process Automation 開始リクエスト フォームでは、以下の XML ステートメントが各ユーザ インターフェース パラメータの説明の前に表示されます。

```
<FieldDescriptor><IsRequired>true または false</IsRequired><Length>数値
</Length></FieldDescriptor>
```

IsRequired

パラメータが必須 (true) または不要 (false) であることを指定します。パラメータが必須の場合、製品ユーザ インターフェースには標準的な必須インジケータが表示されます。

例 : <FieldDescriptor><IsRequired>true</IsRequired></FieldDescriptor>

Length

パラメータ テキスト入力フィールドの長さを指定します。複数行テキスト フィールドを定義するには、255 より大きい値を指定します。

例 : <FieldDescriptor><Length>275</Length></FieldDescriptor>

製品に付属のデフォルト通知プロセスは変更できます。独自の新しい通知プロセスを作成することもできます。必須インジケータに関する情報と、変更されたプロセスまたは新しいプロセス内のフィールド長に関する情報を含めるには、プロセス内の各ユーザインターフェースパラメータの説明の前に XML ステートメントを挿入する必要があります。

注: 新しい通知プロセスを作成する場合は、そのプロセス用の、対応する開始リクエストフォームが必要になります。通知プロセスの変更または作成の詳細については、ワークフロープロバイダのマニュアルを参照してください。

Data Importer プロセスのための CA Process Automation 統合

CA APM と CA Process Automation の統合により、Data Importer プロセスをセットアップして設定することができます。この統合では、CA Process Automation にインポートし、プロセス ワークフロー全体に統合されるサンプルデータインポート XML ファイルを使用します。Data Importer プロセスは Data Importer を起動し、データインポートを実行します。

注: この統合では、CA Process Automation、および会社提供されるサンプルデータインポート XML ファイルを使用します。また、その他のワークフロープロバイダを使用し、独自の全体ワークフローおよび Data Importer プロセスを作成することもできます。

CA Process Automation Data Importer プロセスのセットアップ方法

Data Importer プロセスをセットアップするには、以下の手順に従います。

1. CA APM と CA Process Automation をインストールします。
2. CA APM をインストールしたアプリケーションサーバにログインします。
3. ストレージマネージャサービスがインストールされている CA APM アプリケーションサーバの以下のフォルダにアクセスします。
[ITAM Root Path]¥Storage¥Common Store¥Import
4. Import_Automation_Workflow.xml ファイルを見つけます。
5. CA Process Automation で、Import_Automation_Workflow.xml ファイルをインポートします。

6. CA Process Automation で、Import_Automation_Workflow.xml をプロセス全体ワークフローに統合します。
7. CA Process Automation で、Data Importer プロセス パラメータの設定を変更します。
 - a. 必要な設定と一致するようにデフォルトのインポート サービス URL を変更します。
 - b. デフォルトの CA APM ユーザ ID およびパスワードを自分の設定に変更します。
 - c. 対象データ インポートと一致するようにデフォルトのデータ インポート名を変更します。
 - d. 対象データ インポートに対応するデータ ファイル名を指定します。

注: CA Process Automation の使用については、CA Process Automation のドキュメントを参照してください。

CA Process Automation ワークフロー プロセス パラメータの変更

CA APM と CA Process Automation をインストールし、Import_Automation_Workflow.xml ファイルを CA Process Automation にインポートすると、デフォルトのワークフロー プロセス パラメータが CA Process Automation 内に定義されます。必要な設定を含めるために、デフォルトのプロセス パラメータを変更できます。プロセス パラメータの実際の（ハードコードされた）値を入力します。入力した値が有効であることを確認する必要があります。

プロセス パラメータは、メインデータ セット内または個々のプロセス開始リクエスト フォーム内で変更できます。個々のプロセスについて指定するパラメータは、そのプロセスのメインデータ セット内のパラメータよりも優先されます。

次の手順に従ってください:

重要: CA APM および CA Process Automation では、パラメータに入力した情報は検証されません。入力が有効で、正しいフォーマットでデータを入力したことを確認してください。

1. CA Process Automation にログインし、CA Process Automation クライアントに移動します。

2. Data Importer パラメータの情報を入力します。以下のフィールドについて説明します。

ITAMImportServiceURL

インポート サービスが実行されている場所の完全 URL パスを指定します。

例 :

`http://server/ImportService/ImportService.svc`

username

CA APM ユーザ ID を指定します。

password

CA APM ユーザ パスワードを指定します。

Importname

実行するデータ インポートの名前を指定します。

FilePath

データインポートに関連付けられたデータ ファイルの完全パスおよび名前を指定します。

例 :

`C:\YYCAITAMCostcenter.csv`

3. CA Process Automation の変更を保存します。

注: CA Process Automation でプロセスをセットアップする詳細については、CA Process Automation のドキュメントを参照してください。

CA Service Catalog インテグレーション

CA Service Catalog を CA APM に統合すると、サービスリクエストのリクエストアイテムを、CA APM アセットに関連付けることができます。リクエストのフルフィルメント時に、CA APM アセットを、CA Service Catalog からリクエストされたアイテムに関連付けることができます。リクエストに割り当て済みのアセットは表示することができ、必要に応じてリクエストから削除することもできます。また、アセットに対するリクエストのフルフィルメントを拒否することもできます。

重要: CA APM と CA Service Catalog の統合が正常に機能するためには、同じ CA MDB および同じ CA EEM を共有する必要があります。

注: 在庫からのリクエストのフルフィルメントの詳細については、「ユーザガイド」を参照してください。CA Service Catalog 内でのリクエストの作成および管理の詳細については、「CA Service Catalog 統合ガイド」を参照してください。

第 7 章: CA APM への CA SAM の実装

このセクションには、以下のトピックが含まれています。

[概要 \(P. 137\)](#)

[CA APM および CA SAM データ同期 \(P. 138\)](#)

[CA APM で CA SAM を実装する方法 \(P. 144\)](#)

[データ管理の推奨事項 \(P. 159\)](#)

[CA Software Compliance Manager をアンインストールする方法 \(P. 164\)](#)

概要

CA APM は CA SAM と連携して、ソフトウェアアセット管理機能の実行を可能にします。CA SAM は、CA Software Compliance Manager (CA SCM) に取って代わるソフトウェアアセットおよびコンプライアンス管理の進化形です。CA Software Compliance Manager の計画の詳細については、CA サポートオンライン上の製品サポートサイトを参照してください。

重要: CA APM でのソフトウェアアセットの管理は推奨されていません。CA APM リリース 12.9 が提供する拡張機能を活用するため、ソフトウェアアセットとライセンスの管理に CA SAM を使用することをお勧めします。

CA SAM には以下の利点があります。

- 利用可能ライセンスの数を使用されたライセンスの数と比較することで、ソフトウェアライセンス準拠の位置を判断するプロセスをサポートします。
- CA SAM ユーザインターフェースにソフトウェアライセンスインポート機能を統合します。
- ライセンスに関する詳細な商用情報を含むソフトウェアライセンスカタログの作成およびメンテナンスを簡素化します。
- ソフトウェアライセンスカタログ内の定義された製品にインストールと使用状況のデータを割り当てます。
- ソフトウェア製品認識を実行します。
- 製品価格、ライセンスコスト、および契約支払いの財務分析を許可します（この機能は追加モジュールで利用可能です）。

CA APM および CA SAM の両方を実装すると、組織内のハードウェアおよびソフトウェアアセットの両方の管理を調整できます。CA APM はハードウェアアセットデータのメンテナンスを、CA SAM はソフトウェアアセットとライセンスのデータのメンテナンスを実行します。CA APM および CA SAM の両方が必要とする共通のデータは共有されます。

CA APM および CA SAM データ同期

CA SAM と CA APM を実装するとき、CA APM および CA SAM はハードウェアおよびソフトウェアアセット管理に必要なデータを共有します。データおよびアセット管理プロセスの統合性を維持するため、データを CA APM と CA SAM で同期する必要があります。データ同期は、CA APM と CA SAM の両方の中にある同じオブジェクトに同じデータ値が含まれることを確認します。このデータ同期は以下の方法で実行されます。

- 自動 - CA APM 内で (ユーザインターフェース、Web サービス、または Data Importer を通して) 以下のオブジェクトを作成、更新、または削除する場合、オブジェクトは CA SAM で自動的に同期されます。CA APM のみで以下のオブジェクトを作成、更新、または削除します。
 - 会社
 - ロケーション
 - コストセンター
 - ディビジョン
 - 連絡先

重要: CA SAM 管理者は、権限のない変更を防ぎ、データの正しい同期を確実にするためにこれらのオブジェクトを CA SAM 内で読み取り専用とする必要があります。この要件の詳細については、「データ管理の推奨事項」を参照してください。オブジェクトを CA SAM で読み取り専用として指定する詳細については、CA SAM ドキュメントを参照してください。

注: [連絡先] 以外のこれらのオブジェクトは CA APM および CA SAM で同じラベルを使用します。CA SAM で、[連絡先] オブジェクトは「ユーザ」とラベル付けされます。

[連絡先]、[会社]、および [ロケーション] に対して、自動同期は特定のデータタイプに対して以下の表で示されているとおりにのみ発生します。

オブジェクト	タイプが以下のときに自動的に同期する
連絡先	ユーザ
会社	内部

オブジェクト	タイプが以下のときに自動的に同期する
ロケーション	NULL
	<ul style="list-style-type: none"> ■ 手動 - CA APM または CA SAM に以下のオブジェクトを作成または更新する場合、オブジェクトを手動で同期します。CA APM または CA SAM に以下のオブジェクトを作成するか更新します。 <ul style="list-style-type: none"> - 国 - 地域 たとえば、CA SAM に国オブジェクトを作成する場合は、同じオブジェクトを CA APM に手動で作成します。CA APM 内の地域オブジェクトを更新する場合は、CA SAM 内のそのオブジェクトを手動で更新します。 ■ データのロード - 以前の CA APM リリース 12.6 インストールから CA APM リリース 12.9 にアップグレードする場合、会社、場所、コストセンター、部門および連絡先に関する既存の CA APM データを CA SAM にロードできます。データ ロードの詳細については、「CA SAM への CA APM データのロード (P. 158)」を参照してください。 <p>注: 手動によるデータ同期の詳細については、「データ管理の推奨事項」を参照してください。</p> <p>注: CA APM を CA SAM の既存のインスタンスを使用して実装している場合は、まだ同期されていない既存の CA SAM データがあります。自動同期プロセスを開始する前に、既存の CA SAM データを CA APM データに同期します。詳細については、CA サポートの CA SAM 製品ページ にある推奨記事、「How to Synchronize CA APM Data with an existing CA SAM Instance」を参照してください。</p>

データ同期の設定方法

特定のビジネスニーズに合わせて、CA APM および CA SAM データの自動データ同期を設定できます。同期されるオブジェクトのタイプおよび属性を設定できます。また、同期の対象となるデータ行を選択するために使用する基準を設定できます。データ同期を設定するには、設定ファイル SAMDataSynchConfig.xml を編集します。

重要: 製品インストールは、データ属性および基準のデフォルト設定を使用してデータ同期設定ファイル SAMDataSynchConfig.xml を保存します。このファイルは、デフォルト設定をカスタマイズする場合にのみ変更します。

データ同期設定ファイルは、以下の [イベント サービス] および [アプリケーション サーバ] フォルダにあります。

```
<InstallFolder>¥CA¥ITAM¥EventService¥SAMDataSynchConfig.xml  
<InstallFolder>¥CA¥ITAM¥Application Server¥SAMDataSynchConfig.xml
```

注: フォルダの 1 つで設定ファイルを変更する場合は、その他のフォルダの設定ファイルにも同じ変更を加えます。

例: SAMDataSynchConfig.xml 設定ファイルの構造

以下の例では、デフォルトの属性および基準に対して以下の変更を加えた設定ファイルのセクションを示します。

- APMCriteria ステートメント (強調表示) – CA APM 連絡先属性 (contacttype.value) の基準として Analyst が追加されました。User はデフォルト基準です。
- SamField ステートメント (強調表示) – CA APM 連絡先 (contactid) は CA SAM ユーザ (import_user_id) にマップされました。デフォルトステートメント (例ではコメントアウト) は CA SAM ユーザ (import_user_id) に CA APM アセット所有者 (resourceownerid) をマップしました。

```
<SamTable apmsyncclass="contact" samsynctable="users" >  
  <SamField apmattribute="individualid" samattribute="import_id" />  
  <SamField apmattribute="emailid" samattribute="login" />  
  <SamField apmattribute="costcenterkey" samattribute="import_level_2_id" />  
  <SamField apmattribute="lastname" samattribute="last_name" />  
  <SamField apmattribute="firstname" samattribute="first_name" />  
  <SamField apmattribute="emailid" samattribute="email" />  
  <APMCriteria>  
    <Criteria apmattribute="contacttype.value" value="User" />  
    <Criteria apmattribute="contacttype.value" value="Analyst" />  
  </APMCriteria>  
  
</SamTable>  
  
<SamTable apmsyncclass="asset" samsynctable="devices" >  
  <SamField apmattribute="costcenterkey" samattribute="import_org_level_2_id" />  
  <SamField apmattribute="locationid" samattribute="import_location_id" />  
  <!--<SamField apmattribute="resourceownerid" samattribute="import_user_id" />-->  
  <SamField apmattribute="contactid" samattribute="import_user_id" />  
  
</SamTable>
```

例における以下の用語には説明が必要です。

SamTable

CA APM および CA SAM データ オブジェクトまたはテーブルのマッピングを表す XML ノードを指定します。

Apmsyncclass

CA APM のデータ同期オブジェクトの名前を指定します。

Samsynctable

CA SAM で CA APM オブジェクトのマップ先となるデータベーステーブルの名前を指定します。

SamField

CA APM および CA SAM 属性のマッピングを表す XML ノードを指定します。

Apmattribute

データ同期オブジェクトの CA APM 属性を指定します。属性の名前を生成するには、データベース クライアント ツールを使用して CA APM データベースにログインし、以下のクエリを実行します。

```
select attribute_name, class_name, table_name, field_name from arg_attribute_def
where class_name='object_name';
```

設定 XML で、attribute_name 列の値を Apmattribute XML 属性の値として使用します。

Samattribute

CA SAM で CA APM 属性のマップ先となるデータベース テーブルのフィールド名前を指定します。CA SAM オブジェクトおよび属性のリストについては、「*CA Software Asset Manager Administration Manual*」を参照します。

APMCriteria

1 つまたは複数の子基準ノードを保持する XML ノードを指定します。

基準

CA APM データベース テーブル内で OR コネクタを使用して適用される基準を表す XML ノードを指定します。

データ同期設定の制限

データ同期設定ファイルに加えることができる変更には以下の制限が適用されます。

- 属性のマッピングを変更できるのは、データ オブジェクト内に限られます。オブジェクト レベルではマッピングを変更できません。たとえば、CA SAM User を持つ CA APM Location はマップできません。CA APM Location は CA SAM Location にのみマップできます。
- 列は基準の下に追加できます。たとえば、Contact オブジェクトにはデフォルトの Contact タイプとして User があります。その結果、データ同期には Contact タイプが User である Contact オブジェクト内のすべてのデータ行が選択されます。その他の基準を追加できます。以下のステートメントでは、基準の追加方法のサンプルを示します。

```
<APMCriteria>
  <Criteria apmattribute="contacttype.value" value="User" />
  <Criteria apmattribute="contacttype.value" value="Analyst" />
  <Criteria apmattribute="costcenter.value" value="NewCostCenter" />
</APMCriteria>
```

これらのステートメントは、データ同期のために以下の選択基準を指定します。

- 連絡先タイプが User または Analyst に等しいすべての連絡先
- コスト センターが New Cost Center に等しいすべての連絡先
- 基準 XML ノードはそれぞれ 1 つの値のみを持つことができます。たとえば、連絡先タイプのデフォルト基準値は User です。その他の値（たとえば「Analyst」または「Employee」）を追加（または削除）することができます。ただし、基準値として「Analyst, Employee」のように指定することはできません。それぞれの一意の値に対して 1 つの基準 XML ノードを作成します。

属性の追加

データ同期設定ファイルに属性を追加することができます。また、既存のステートメントの編集によりファイル内の既存の属性を変更できます。

次の手順に従ってください:

1. 既存の SamField ノードに以下のステートメントを追加して SamField ノードを作成します。

```
<SamField apmattribute="attribute_name" samattribute="attribute_name" />
```

注: このステートメントに必要な値を識別するには、以下の手順に従います。

- データベース クライアント ツールを使用して、CA APM データベース上で以下のクエリを実行します。

```
select class_name, attribute_name, table_name, field_name
from arg_attribute_def where class_name='object_name';
```

- クエリ結果で、前の手順で生成された attribute_name 値をコピーします。この値を apmattribute 値として新しい SamField ノードステートメントに貼り付けます。

- 「*CA Software Asset Manager Administration Manual*」の「Data Imports」の章を参照し、「Formats」セクションのフィールド表を見つけます。
- 適切なフィールド名をコピーし、samattribute 値として新しい SamField ノードステートメントに貼り付けます。

注: 適切な CA SAM フィールドの選択方法については、CA サービスにお問い合わせください。

基準の追加

データ同期設定ファイルに基準を追加して、データ同期に選択されるデータ値を拡張できます。

次の手順に従ってください:

- 既存の基準ノードに以下のステートメントを追加して基準ノードを作成します。

```
<Criteria apmattribute="value" value="value" />
```

注: このステートメントに必要な値を識別するには、以下の手順に従います。

- データベース クライアント ツールを使用して、CA APM データベース上で以下のクエリを実行します。

```
select class_name, attribute_name, table_name, field_name
from arg_attribute_def where class_name='object_name';
```

- クエリ結果で、前の手順で生成された attribute_name 値をコピーします。この値を apmattribute 値として新しい基準ノードステートメントに貼り付けます。

- 以下の手順を実行して基準値を指定します。

- 以下のクエリを実行します。

```
Select field_name, table_name from arg_attribute_def where class_name =
'<apmsyncclass 値>' および attribute_name = <apmattribute 値>.
```

- b. クエリ結果で、table_name から field_name を選択します。
- c. フィールド値をコピーし、手順 1 の `value="value"` パラメータに貼り付けます。

注: 同期する一意の値ごとに別々の基準ノードを作成します。

CA APM で CA SAM を実装する方法

CA APM で CA SAM を実装するには、以下の手順に従います。

1. [前提条件を確認します](#) (P. 144)。
2. [Internet Information Services のインストールを検証します](#) (P. 145)。
3. [CA SAM インポートおよびエクスポートサービスをインストールします](#) (P. 29)。
4. [CA SAM インポートおよびエクスポートサービスを設定します](#) (P. 147)。
5. [CA SAM の CA APM イベントサービスを設定します](#) (P. 149)
6. [SAM インポート ドライバを設定します](#) (P. 152)。
7. [ハードウェアインポートの Windows タスクをスケジュールします](#) (P. 153)。
8. [CA APM イベントサービスを開始します](#) (P. 153)。
9. [ソフトウェアアセット管理機能を有効にします](#) (P. 154)。
10. [CA APM データを CA SAM にロードします](#) (P. 158)。

注: CA SAM を実装するには、CA Support Online から CA SAM カタログの最新のバージョンをダウンロードし、CA SAM にそのカタログを適用する必要があります。カタログのダウンロードは CA APM で CA SAM を実装する前と後のどちらでも実行できます。CA SAM カタログの詳細については、CA SAM のドキュメントを参照してください。

前提条件の確認

正常に CA APM で CA SAM を実装するために、以下の前提条件を確認します。

- CA APM がインストール済みである。

重要: CA APM ワークフロー プロバイダの URL がアクセス可能で、対応するログイン認証情報が有効であることを確認します。

注: CA APM 環境が CA Service Desk Manager (CA SDM) と統合する場合は、CA SDM 監査履歴を有効にしたことを確認します。

- CA SAM インストール メディアから CA SAM がインストール済みである。CA SAM のインストールに関する詳細については、CA SAM のドキュメントを参照してください。

重要: CA SAM サーバに Microsoft .NET Framework 4.0 をインストールする必要があります。

注: CA SAM を使用して 250,000 を超えるハードウェア アセット用のソフトウェア アセットを管理する場合は、システムのパフォーマンスを改善するために以下のインストール構成をお勧めします。

- ディスカバリ データのみを処理する CA SAM ステージング サーバをインストールする。ステージング サーバを MySQL データベースに実装することでパフォーマンスとスケーラビリティを改善します。
- CA SAM 実稼働サーバを SQL Server または Oracle データベースのいずれかにインストールする。
- 処理がステージング サーバで完了した後、CA SAM 実稼働サーバにディスカバリ データを転送する。

Internet Information Services がインストールされているかどうかの確認

CA SAM の実装に必要な新しい CA APM コンポーネントをインストールするとき、CA SAM インポートおよびエクスポート サービスがインストールされます。CA SAM インポートおよびエクスポート サービスのインストールは、有効な ASP.NET および WCF Activation 機能を持ったインターネット インフォメーション サービス (IIS) 7.5 を必要とします。CA SAM インポートおよびエクスポート サービスのインストールを開始する前に、IIS がインストールされており、CA SAM がインストールされているサーバで必須機能が有効であることを確認します。

インターネット インフォメーション サービス(IIS)がインストールされているか確認する方法

1. 個々のアプリケーション サーバおよび Web サーバにログインします。
2. コントロール パネル（[管理ツール] - [サービス]）を開きます。
3. IIS 管理サービスがサーバにインストールされていることを確認します。

IIS バージョン 7.5 を Windows Server 2008 R2 にインストールする方法

1. [サーバーマネージャ] から、[役割] を選択します。
2. [役割の概要] 領域で、[役割の追加] をクリックして [次へ] をクリックします。
[サーバーの役割の選択] ダイアログ ボックスが表示されます。
3. [役割] リストから [アプリケーションサーバ] を選択し、[次へ] を2回クリックします。
アプリケーションサーバ役割用の [役割サービスの選択] ダイアログ ボックスが表示されます。
4. [Web サーバー (IIS) サポート] - [Windows プロセス アクティブ化サービスサポート] - [HTTP アクティブ化] を選択します。
5. より多くの役割サービスおよび機能をインストールするように促される場合は、[必要な役割サービスを追加] をクリックし、[次へ] を2回クリックします。
6. 選択内容のサマリが正しいことを確認し、[インストール] をクリックします。
7. インストールが完了した後、[閉じる] をクリックします。

CA SAM インポートおよびエクスポート サービスをインストールする。

CA APM および CA SAM を実装する場合は、CA SAM インポートおよびエクスポート サービス コンポーネントを CA SAM サーバにインストールします。

注: ソフトウェア アセット管理システムとして CA SAM を実装しない場合、CA SAM インポートおよびエクスポート サービスをインストールする必要はありません。

重要: CA SAM インポートおよびエクスポート サービスをインストールする前に、Microsoft .NET Framework 4.0 を CA SAM サーバにインストールする必要があります。

次の手順に従ってください:

1. CA SAM サーバにログインします。
2. CA APM インストールメディア上の SAMImportExportSetup フォルダに移動します。そのフォルダとすべての内容を CA SAM サーバ上のローカルフォルダにコピーします。
3. CA SAM サーバ上の SAMImportExportSetup フォルダで、CAITAMSAMImportExportServiceInstaller.msi をダブルクリックします。
インストール ルート パス用のプロンプトが表示されます。
4. CA SAM インポートおよびエクスポートサービスコンポーネントのインストール先 ITAM ルート パスを入力します。
以下の例は、推奨のパスを示しています。

例 :

C:\Program Files\CA\ITAM

CA SAM インポートおよびエクスポートサービスのインストールが完了しました。

CA SAM インポートおよびエクスポート サービスの設定

CA SAM インポートおよびエクスポート サービスは、検出されたハードウェア データを CA APM へエクスポートします。このサービスは、CA APM から所有権 データ エクスポートを受信し、CA SAM 内のアセット情報を更新します。このサービスはまた、CA APM から自動データ同期エクスポート（会社、場所、コスト センター、部門、および連絡先）を受信し、CA SAM 内の情報を更新します。

次の手順に従ってください:

1. CA SAM サーバにログインします。
2. 以下の場所に移動します。
[ITAM Root Path]\ITAM\SAMImportExportService
3. テキスト エディタで、web.config ファイルを開きます。

4. 以下の手順に従って、インポート フォルダ パスを編集します。

- a. 以下のステートメントを探します。

```
<add key="ImportFolderPath" value="[import folder path]"/>
```

- b. [import folder path] をデータ交換フォルダ下の external フォルダのパスに置き換えます。データ交換フォルダは、CA SAM インストール フォルダにあります。

例：

```
C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external
```

5. 以下の手順に従って、エクスポート フォルダ パスを編集します。

- a. 以下のステートメントを探します。

```
<add key="ExportFolderPath" value="[export folder path]"/>
```

- b. [export folder path] を external フォルダ下の in フォルダのパスに置き換えます。external フォルダは、CA SAM インストール フォルダ下のデータ交換 フォルダの下にあります。

例：

```
C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external\in
```

6. web.config ファイルを保存します。

7. 以下の場所に移動します。

```
[ITAM Root Path]\ITAM\SAM\ImportExportService\data_exchange
```

8. エクスポート フォルダ パスに以下のいずれかのファイルをコピーすることにより、デバイス エクスポートを設定します。

- CA_SAM_Device_Export_SQL.xml (SQL Server データベース用)
- CA_SAM_Device_Export_ORA.xml (Oracle データベース用)

例：

```
C:\Program Files (x86)\ca_sam\app\uploads\prod\data_exchange\external\in
```

9. external フォルダを使用する cron ジョブを作成するには、以下の手順に従います。

- a. 管理者として CA SAM にログインします。

- b. [管理者]、[設定]、[Cron ジョブ] をクリックします。

- c. Cron ジョブ ツールバー内の新規レコードアイコン (*) をクリックします。

- d. 以下の情報を指定します。

関数名

`data_exchange_external` を選択します。

説明

次の説明を入力します : CA Data Coordination Service Tasks。

間隔(分)

インポートおよびエクスポートの時間間隔の値 (たとえば 5) を入力します。

- e. [保存] をクリックします。

ダイアログ ボックスが閉じます。

10. cron ジョブの XML ファイルを選択します。

- [交換] - [データ交換] - [交換ディレクトリ] を選択します。
- [交換ディレクトリ] フィールドで `external` を選択します。
- [表示] フィールドで XML ファイルを選択します。
- [参照] をクリックし、以下のいずれかの XML ファイルを検索して選択します。
 - CA_SAM_Device Export_SQL.xml (SQL Server データベースの場合)
 - CA_SAM_Device Export_ORA.xml (Oracle データベースの場合)
- [ファイルのアップロード] をクリックします。
- `data_exchange cron` ジョブ用の開始アイコンをクリックします。
- [cron ジョブの開始] ダイアログ ボックスが表示されます。
- [cron ジョブの開始] をクリックします。
- ダイアログ ボックスが閉じます。

CA SAM インポートおよびエクスポート サービスの設定は完了しました。

CA SAM の CA APM イベント サービスを設定します。

CA APM の [管理] タブのパラメータを検証または編集することにより、CA APM イベント サービスを設定します。

次の手順に従ってください:

1. 管理者として Web サーバ上の CA APM にログインします。
2. [管理] - [システム構成] - [イベントサービス] ページに移動します。
3. [詳細オプションを表示] をクリックします。
CA SAM に適用されるパラメータが表示されます。
4. 以下のパラメータの値を検証または編集します。

イベント発生のチェック間隔(ミリ秒)

定義済みのイベントに関するフィールドの変更をデータベースがチェックする間に CA APM が待機する時間 (ミリ秒)。

SAM 機能が有効な場合、このパラメータが 30000 に設定されることを検証します。SAM 機能が有効でない場合、この値が [イベントサービス] 設定ファイルの設定に一致することを確認します。

デフォルト (CA SAM 実装なし) : 3600000 (1 時間)

デフォルト (CA SAM 実装あり) : 30000 (30 秒)

イベントトリガのチェック間隔(ミリ秒)

ワークフロー プロバイダに送信する必要があるトリガされたイベントのデータベースによるチェック間に CA APM が待機する時間 (ミリ秒)。

SAM 機能が有効な場合、このパラメータが 60000 に設定されることを検証します。SAM 機能が有効でない場合、この値が [イベントサービス] 設定ファイルの設定に一致することを確認します。

デフォルト (CA SAM 実装なし) : 3600000 (1 時間)

デフォルト (CA SAM 実装あり) : 60000 (60 秒)

トリガされたイベントステータスの更新間隔(ミリ秒)

ワークフロー プロバイダに送信された、トリガされたイベントのステータスの更新間に CA APM が待機する時間(ミリ秒)。

SAM 機能が有効な場合、このパラメータが 60000 に設定されることを検証します。SAM 機能が有効でない場合、この値が [イベントサービス] 設定ファイルの設定に一致することを確認します。

デフォルト (CA SAM 実装なし) : 3600000 (1 時間)

デフォルト (CA SAM 実装あり) : 60000 (60 秒)

アセット連絡先の更新間隔(ミリ秒)

CA CMDB のアセット連絡先の更新間に CA APM が待機する時間(ミリ秒)。

デフォルト : 43200000 (12 時間)

CA SAM ステータス更新頻度

MDB 内の CA SAM インポートジョブのステータスを更新する頻度(ミリ秒)。

デフォルト : 120000 (120 秒)

オンデマンド最大スレッド数

CA APM と CA SAM の間のデータ同期を処理するためのスレッドの最大数。デフォルト(ゼロ)は、システムがシステムハードウェア設定に応じて必要な数のスレッドを作成することを示します。デフォルト値以外の値はすべて、システム環境設定に関係なく同じ数のスレッドを使用します。

デフォルト : 0

CA SAM イベント通知電子メール

CA SAM データ同期に関する通知を受信するための CA APM 管理者電子メール アドレス。

認証トークン

CA APM イベントサービスと CA SAM インポートおよびエクスポートサービスの間の通信を確立するトークン。この値は CA SAM インポートおよびエクスポートサービス設定に一致する必要があります。

注: この値を変更する場合、CA SAM サーバ上の CA SAM インポートおよびエクスポートサービスに対する認証トークンの値を、この値に一致するように更新する必要があります。

上位のクエリ

一度に処理されるトリガされたイベントの数。

例：この値が 1000 に設定され、1500 のイベントがトリガされる
とします。最初の処理パスで最初の 1000 レコードが処理され、次
の処理パスで残りの 500 レコードが処理されます。

デフォルト：1000

SAM インポート ドライバの設定

CA APM の [管理] タブのパラメータを検証または編集することにより、SAM インポート ドライバを設定します。

次の手順に従ってください：

1. 管理者として Web サーバ上の CA APM にログインします。
2. [管理]、[システム構成]、[SAM インポート ドライバ] ページに移動します。
3. 以下のパラメータの値を検証または編集します。

サーバ

CA SAM ドライバのインポートコンポーネントがインストールさ
れているサーバの名前。

ユーザ名

Data Importer でレコードを追加、変更、または削除するためには必
要なユーザ名。

ITAM ルートパス

製品がインストールされているルートへのパス。

ファイル パス

CA SAM エクスポート ファイルがインポートされるルートへのパ
ス。

例：[ITAM Root Path]¥ITAM¥Import Driver¥Input

プロセッサ実行可能パスのインポート

Data Importer プロセッサ実行可能ファイル (ImportProcessor.exe)
へのパス。

例：[ITAM ルート パス]¥ITAM¥Import Processor¥ImportProcessor.exe

ハードウェア インポート用 Windows タスクのスケジュール

Windows タスク スケジューラを使用して、CA SAM から検出されたハードウェアデータを CA APM へインポートするようにタスクをスケジュールします。以下の手順では、インポートを毎日 1 回実行するようにスケジュールします。

注: この手順は Windows タスク スケジューラの使用について説明していますが、別のタスク スケジューラまたはプロセス オーケストレーション ツールを使用することもできます。

Windows Server 2008 の場合は、以下の手順に従います。

1. CA APM アプリケーション サーバ上の [スタート] メニューから、Windows タスク スケジューラを開きます。
たとえば Windows Server 2008 で、[コントロール パネル] - [システムとセキュリティ] - [管理ツール] - [タスクのスケジュール] に移動します。
 2. [タスクの作成] をクリックします。
 3. [全般] タブで、タスクの名前を指定します。
 4. [ユーザーがログオンしているかどうかにかかわらず実行する] のチェック ボックスをオンにします。
 5. [操作] タブに移動し、[新規] をクリックします。
 6. [操作] フィールドで、[プログラムの開始] を選択します。
 7. [プログラム/スクリプト] フィールドで Import Driver Program フォルダを参照して探し、ImportDriver.exe ファイルを選択して [OK] をクリックします。
 8. [トリガー] タブに移動し、[新規] をクリックします。
 9. [設定] フィールドで、[毎日] を選択します。
 10. [開始] フィールドで、[午前 12:00:00] を選択します。
 11. [間隔] で [1] 日を選択して [OK] をクリックします。
 12. [タスクの作成] ダイアログ ボックスで、[OK] をクリックします。
- 検出されたハードウェア データをインポートする Windows タスクのスケジューリングが完了しました。

CA APM イベント サービスの開始

旧 CA APM リリースからアップグレードする場合、CA APM および CA SAM の実装を完了するには CA APM イベント サービスを開始します。

次の手順に従ってください:

1. CA APM アプリケーションサーバ上で [スタート] - [コントロール パネル] - [管理ツール] - [サービス] を選択します。
2. CA Asset Portfolio Management – Event Service のエントリを見つけます。
3. サービスを右クリックし、[開始] を選択します。

サービスが開始されます。

ソフトウェア アセット管理機能の有効化

CA APM コンポーネントをすべてインストールして設定した後、ソフトウェア アセット管理機能を有効にします。

現在 CA APM と CA Software Compliance Manager (CA SCM) を統合している場合は、CA SCM をアンインストールしてからソフトウェア アセット管理機能を有効にしてください。CA SCM をアンインストールする詳細については、「[CA Software Compliance Manager をアンインストールする方法 \(P. 164\)](#)」を参照してください。CA SCM をアンインストールする方法および時期の詳細については、CA サービスの担当者に問い合わせてください。

注: 旧リリースでソフトウェア アセット管理機能を有効にしており、これからアップグレードを実行する場合、以下の手順はスキップしてください。ただし、共通ホーム ページの CA SAM セクションを参照するには、CA APM Web サーバ上の web.config 設定ファイルを更新してください。以下のステートメントを更新します。

```
<add key="CASAMWebClientUrl" value="http://CA_SAM_server_name/prod" />
```

例 :

```
<add key="CASAMWebClientUrl" value="http://itamsam/prod" />
```

次の手順に従ってください:

1. 管理者として Web サーバ上の CA APM にログインします。
2. [管理] - [システム構成] - [ソフトウェア アセット管理] に移動します。

- 必要な情報を入力します。以下のフィールドについて説明します。

CA SAM Web クライアント URL

CA SAM ホーム ページの URL を指定します。

注: ログインした後、CA SAM ホーム ページから Web クライアントの URL をコピーできます。

CA SAM インポート エクスポート Web サービス URL

CA SAM Web サービスの URL を指定します。以下の形式を使用します。

`http://[CA SAM System Name]:[Port Number]/SAMImportExportService/Service.svc`

- [CA SAM System Name] を CA SAM サーバの名前に置換します。
- [Port Number] を CA SAM インポートおよびエクスポート サービスがホストされるポートの番号に置換します。

SAM 機能の有効化

ソフトウェア アセット管理機能が有効であることを指定します。以前の CA APM ユーザ インターフェースに CA SCM フィールドがあった場合は、このチェック ボックスをオンにした後で削除されます。

CA SAM Web サービス WSDL の URL

CA SAM Web Service Definition Language (WSDL) の URL。この URL は CA SAM Web サービスにアクセスするために使用されます。以下の形式を使用します。

`http://[CA SAM システム名] : [ポート番号] /prod/SOAP/dyn_server.php`

- [CA SAM System Name] を CA SAM サーバの名前に置換します。
- [ポート番号] を CA SAM Web サービスがホストされるポートの番号に置換します。

CA SAM Web サービス ログイン

CA SAM Web サービスのログイン名。

注: このログイン名と [CA SAM Web サービス パスワード] が config_soap.inc ファイル内のログイン名とパスワードに一致することを確認してください。このファイルは、以下の CA SAM インストール フォルダ パスにあります。

app¥includes¥prod¥st¥config_soap.inc

重要: config_soap.inc ファイルのデフォルトの内容は、コメント化されています。コメント記号 (*/* */*) を削除して、ログイン名とパスワードを設定してください。

CA SAM Web サービス パスワード

CA SAM Web サービスのログイン パスワード。

CA SAM SSO の暗号化アルゴリズム

CA IT Asset Manager の共通 ホーム ページから CA SAM へのシングル サインオン アクセスに使用される暗号化アルゴリズムを指定します。

このエントリは、CA SAM システム構成内の security_auth_token_cipher フィールドのエントリと一致する必要があります。

注: CA SAM シングル サインオンの詳細については、『CA Software Asset Manager Administration Manual』のシングル サインオンの説明を参照してください。

CA SAM SSO の認証メカニズム

CA SAM へのログインに使用されるメカニズムを指定します。

このエントリは、CA SAM システム構成内の security_auth_method フィールドのエントリと一致する必要があります。

注: このメカニズムには、auth_token_password を選択することを推奨します。auth_token メカニズムは、ほかの CA SAM ユーザのログインを無効にします。

ユーザ認証のための CA SAM SSO フィールド

ユーザを認証するために使用される一意の識別子（インポート ID または電子メールアドレス）のタイプを指定します。

このエントリは、CA SAM システム構成内の `security_auth_token_user_identifier` フィールドのエントリと一致する必要があります。

CA SAM SSO 密钥キー

CA APM と CA SAM が共有し、ユーザ認証を暗号化および復号化するために使用されるキーを指定します。このキーによって、適切に認証されていない CA APM ユーザは CA SAM にアクセスできないようになります。

このエントリは、CA SAM システム構成内の `security_auth_token_key` フィールドのエントリと一致する必要があります。

4. [保存] をクリックします。
5. Apache Tomcat Common Asset Viewer サービスを再起動します。
注: 後で以下のいずれかのフィールドのエントリを変更する場合も、Apache Tomcat Common Asset Viewer サービスを再起動します。
 - CA SAM Web サービス WSDL URL
 - CA SAM Web サービス ログイン
 - CA SAM Web サービス パスワード
6. CA APM Web サーバおよびアプリケーションサーバで `iisreset` コマンドを実行してインターネットインフォメーションサービス (IIS) を再起動します。
ソフトウェアアセット管理機能が有効になります。また、CA SCM フィールドは CA APM ユーザインターフェースから削除されます。

CA APM データが存在する場合（たとえば CA APM12.6 がインストール済みで、アップグレードしている場合）、[データのロード] ボタンは有効になります。その後、選択したオブジェクトの既存の CA APM データを CA SAM にロードできます。データのロードの詳細については、「[CA SAM への CA APM データのロード \(P. 158\)](#)」を参照してください。CA APM の新規インストールを実行している場合、このボタンは有効になりません。新規インストールに既存のデータがありません。

共通ホーム ページのシングル サインオン

CA SAM の実装が完了すると、CA IT Asset Manager の共通ホーム ページに、ハードウェアおよびソフトウェアアセット管理ダッシュボードが表示されます。これらのダッシュボードには、CA APM および CA SAM 内のページを開くリンクが含まれます。CA APM にログインし、共通ホーム ページを開いた後、CA SAM にログインせずに、CA SAM ページにアクセスできます。

シングル サインオンを実装するには、以下の手順が完了していることを確認します。

- CA APM のユーザ ID は CA SAM のユーザ ID としても存在します。
- CA SAM のユーザの電子メールアドレスおよびインポート ID は、CA APM のユーザの電子メールアドレスおよび連絡先 ID と一致します。
- CA SAM ユーザは CA SAM の機能を実行する権限が与えられています。
 - a. CA SAM ユーザ詳細ページにアクセスするには、[組織] - [ユーザ] を選択し、次に既存のユーザ レコードを編集するかユーザ レコードを作成します。
 - b. CA Software Asset Manager 認証のチェック ボックスをオンにします。

CA SAM への CA APM データのロード

CA APM 内のソフトウェアアセット管理機能を有効にした後、選択済みオブジェクトの既存の CA APM データを CA SAM にロードできます。このデータのロードにより、CA APM と CA SAM で一致するオブジェクトが同じデータ値を持つように、データを同期できます。ロードできる CA APM データには以下のオブジェクトが含まれます。

- ロケーション
- ディビジョン
- 会社
- コストセンター
- 連絡先

CA APM を以前にインストールしている場合は、これらのオブジェクトの既存の CA APM データがあります。CA APM を新規にインストールしている場合は、既存のデータがありません。

注: CA SAM に CA APM データをロードする前に、CA APM データが CA SAM 要件を満たすことを確認してください。これらの要件は「自動データ同期のフィールド要件」で定義されています。

次の手順に従ってください:

1. [管理] - [システム構成] - [ソフトウェアアセット管理] ページで、[データのロード] ボタンが有効であることを確認します。

注: CA APM データが存在する場合 (たとえば CA APM12.6 がインストール済みで、アップグレードしている場合)、[データのロード] ボタンは有効になります。

2. [データのロード] をクリックします。

データのロードにより、場所、部門、会社、コストセンター、および連絡先の各オブジェクト値が CA SAM にコピーされます。ステータステーブルは、データのロードの進捗状況を表示します。

オブジェクトの一部が CA SAM との同期に失敗した場合、エラー レコードがログファイルに書き込まれます。[エラー レコードを取得] ボタンをクリックすると、このログファイルを表示できます。[エラー レコードを取得] ボタンは SAM 機能を有効にした場合にのみ、利用可能になります。

3. [エラー レコードを取得] をクリックして、データ同期エラーが発生したかどうかを確認します。

CSV ファイルを開くか保存するように促されます。エラーが CSV ファイルに存在する場合、エラーは以下の順にオブジェクトごとにグループ化されます。

- ロケーション
- ディビジョン
- 会社
- コストセンター
- 連絡先

4. CSV ファイルのエラーおよび説明を確認し、CA APM オブジェクトデータを修正します。

修正したオブジェクトは、次のデータ同期中に CA SAM と同期されます。

データ管理の推奨事項

このセクションの推奨事項は、CA APM が CA SAM で実装されるときのデータ管理に役立ちます。

手動データ同期

データおよびアセット管理プロセスとの整合性を維持するために CA APM と CA SAM の間でデータを同期する必要があります。データ同期は、CA APM と CA SAM の両方の中にある同じオブジェクトに同じデータ値が含まれることを確認します。

CA APM または CA SAM で国と地域のオブジェクトを作成または更新した場合、オブジェクトを手動で同期します。たとえば、CA SAM に国オブジェクトを作成する場合は、同じオブジェクトを CA APM に手動で作成します。CA APM 内の地域オブジェクトを更新する場合は、CA SAM 内のそのオブジェクトを手動で更新します。

手動データ同期のルール

データが正しく同期されることを確認するには、国と地域のオブジェクトを作成または更新するときに、以下のルールを使用します。

- 国 - 国の CA APM 省略形は同じ国の CA SAM レコードインポート ID と一致する必要があります。
- 地域 - 地域の CA APM 名は同じ地域の CA SAM レコードインポート ID と一致する必要があります。

コストセンターのデータ管理

CA APM と CA SAM の間のデータ同期は、データおよびアセット管理プロセスの整合性を保証します。この同期は、以下のオブジェクトに対して自動的に行われます。

- 会社
- ロケーション
- コストセンター
- ディビジョン
- 連絡先

注: [連絡先] 以外のこれらのオブジェクトは CA APM および CA SAM で同じラベルを使用します。CA SAM で、[連絡先] オブジェクトは「ユーザ」とラベル付けされます。

CA APM 内の連絡先、会社、場所、部門の各オブジェクトを作成、更新、または削除すると、オブジェクトは CA SAM で自動的に同期されます。CA SAM の管理者は、連絡先、会社、場所、および部門を CA SAM で読み取り専用として指定する必要があります。このアクションは、CA SAM ユーザがこれらのオブジェクトを変更するのを防ぎます。次にデータ同期が行われるときに、それが上書きされます。ただし、管理者はコストセンター オブジェクトを CA SAM で読み取り専用として指定できません。階層をレポートするコストセンターは CA SAM で管理する必要があるためです。

コストセンターのデータ管理に関する推奨ガイドライン

コストセンターのデータ管理を促進するため、以下のガイドラインを使用することを推奨します。

- CA SAM における管理者役割に、コストセンター オブジェクトを管理する権限を追加する。他のユーザ役割ではコストセンター オブジェクトにアクセスできません。
- 以下のアクションを実行するとき、CA APM を使用する。
 - コストセンターを挿入または削除する。
 - コストセンターの名前または説明を更新する。
- 重要: CA SAM 内のコストセンターの名前または説明を変更すると、変更内容は次のデータ同期の後に上書きされます。
- 以下のアクションを実行するとき、CA SAM を使用する。
 - 階層をレポートするコストセンターを管理する。
 - コストセンターを国に割り当てる。

在庫の測定単位

CA SAM は、ハードウェア アセット管理に役立つハードウェアのディスカバリデータを CA APM に送信します。CA APM には CA SAM から送信される以下のハードウェアの在庫項目用の特定の測定単位が必要です。

- 合計ディスク容量：ギガバイト (GB)
- 合計メモリ：メガバイト (MB)
- プロセッサ (CPU) 速度：メガヘルツ (MHz)

CA SAM 内のこれらの項目に関するハードウェアの在庫データをロードして管理するときは、CA SAM データがこれらの測定単位を使用することを確認します。

自動データ同期のフィールド要件

自動データ同期は、会社、場所、コストセンター、部門、および連絡先の各オブジェクトに関する CA APM データを CA SAM 内の対応するオブジェクトにコピーします。同期を正常に行うために、以下のサブセクションにある各オブジェクト用のフィールド要件ガイドラインに従います。

連絡先

連絡先オブジェクト用のフィールドの一部は CA APM ではオプションですが、CA SAM では必須です。そのフィールドについて、以下の表にまとめます。CA SAM で必須のすべてのフィールドが CA APM でデータを含んでいることを確認します。

CA APM フィールド	CA APM で必須?	CA SAM で必須?
ユーザ ID/ユーザ名	いいえ	はい
コストセンター	いいえ	はい
姓	はい	はい
名	いいえ	はい

会社

CA SAM では、階層グループ分け（部門、会社、コストセンター）に関するコンプライアンスをレポートできます。部門についてレポートする場合、CA SAM には、会社オブジェクトの部門の詳細が必要です。データ同期を正常に行うため、CA APM の会社オブジェクトに部門の詳細があることを確認します。

注: 会社の部門の詳細を CA APM に入力するには、まずディレクトリ、リスト管理、会社リスト、部門の中に部門を作成します。次に、[会社詳細] ページで会社を作成または更新するとき、[会社タイプ] で [内部] を選択します。[ディビジョン] テキスト ボックスが表示され、会社の部門を選択できます。

コストセンター

CA SAM では、階層グループ分け（ディビジョン、会社、コストセンター）に関するコンプライアンスをレポートできます。会社についてレポートする場合、CA SAM には、コストセンター オブジェクトの会社情報が必要です。データ同期を正常に行うため、CA APM のコストセンター オブジェクトに会社詳細があることを確認します。

未定義オペレーティング システムを持つアセット

CA APM が受信するディスカバリ データに、CA APM で定義されていないオペレーティング システム名が含まれることがあります。この状況が発生すると、CA APM はオペレーティング システム値として「未定義」を対応するアセットに割り当てます。CA APM は[アセットの詳細] ページの[オペレーティング システム] フィールドに「未定義」という値を表示します。

未定義オペレーティング システムの元の検出された名前を表示して、それらの名前を CA APM オペレーティング システム名に追加できます。また、新しい名前を含めるように、未定義オペレーティング システムを持つアセットを更新できます。

注: CA APM は、任意の検出ソース (CA SAM を含む) から未定義オペレーティング システムを持つデータを受信できます。

未定義オペレーティング システムの元の名前を表示するには、以下の手順に従います。

1. 管理者として CA APM にログインします。
2. [管理] - [照合管理] - [照合メッセージ検索] に移動します。
照合メッセージのリストが表示されます。
3. 含まれていないオペレーティング システムを特定するメッセージを探します。

注: このページ上で「含まれていないオペレーティング システム」というメッセージテキストを検索できます。

メッセージには元の検出された名前が含まれます。

未定義オペレーティング システムを持つアセットを更新するには、以下の手順に従います。

1. [ディレクトリ] - [リスト管理] - [オペレーティング システム] に移動し、含まれていないオペレーティング システム名を CA APM 名に追加します。
2. 以下の手順に従って、未定義のオペレーティング システムを持った個々のアセットを更新します:
 - a. 未定義オペレーティング システムを持ったアセットの[アセットの詳細] ページに移動します。
 - b. [オペレーティング システム] フィールドで [新規に選択] アイコンをクリックし、新規の名前を選択します。

3. 以下の手順に従って、未定義オペレーティング システムを持った複数のアセットを更新します。
 - a. [管理] - [照合管理] に移動します。
 - b. 照合ルール名をクリックします。
選択したルールに関する [照合ルールの詳細] ページが表示されます。
 - c. [アセット更新の監視] が選択されていることを確認します。
 - d. [更新オプション] 領域で、[オペレーティング システム] と [最終実行日] を選択します。
 - e. [保存] をクリックします。

CA APM が未定義オペレーティング システムを持ったアセットに関する新しいディスカバリ データを受信すると、CA APM は入力された新しい名前でオペレーティング システムを更新します。

CA Software Compliance Manager をアンインストールする方法

CA APM が CA Software Compliance Manager (CA SCM) に統合されるときに SAM 機能を有効にするには、CA SCM をアンインストールします。

注: すべてのユーザが CA SCM からログアウトしたことを確認します。アンインストールの開始前に製品からログアウトしていないユーザには、タスクの完了時にエラーが表示されます。

CA SCM 12.0 をアンインストールするには、以下の手順に従います。

1. CA SCM 12.0 がインストールされているコンピュータにログインします。
2. [コントロールパネル]-[プログラムの追加と削除] で、CA SCM リリース 12.0 累積パッチをアンインストールします (存在する場合)。
3. CA APM リリース 12.9 をインストールした CA APM アプリケーション サーバにログインします。
4. CA APM リリース 12.9 をインストールしたフォルダに移動します。
5. CA SCM 12.0 をインストールした各コンピュータ (データベース サーバ以外) 上の一時的な場所に SWCM12.0Uninstall フォルダとそのすべての内容をコピーします。

一時的な場所の例 :

C:\Windows\Temp

6. CA SCM 12.0 コンピュータ上の一時的な場所内の Uninstall フォルダに移動します。
7. SWCM_Uninstall.bat ファイルをダブルクリックして、アンインストールを開始します。
8. 画面の指示に従って、アンインストールプロセスを実行します。

アンインストールが実行され、CA Business Intelligence BusinessObjects Enterprise、CA EEM、CA MDB およびコンテンツインポートクライアントを除くすべてのインストール済みの CA SCM 12.0 コンポーネントが正常に削除されます。

CA SCM 12.6 をアンインストールするには、以下の手順に従います。

注: CA SCM 12.6 をインストールした各コンピュータ (データベース サーバを除く) 上で以下の手順を実行します。

1. CA SCM 12.6 がインストールされているコンピュータにログインします。
2. [コントロールパネル]-[プログラムの追加と削除] で、CA SCM リリース 12.6 累積パッチをアンインストールします (存在する場合)。
3. CA SCM 12.6 がインストールされている Uninstall フォルダに移動します。

例 :

C:\Program Files\CA\SWCM\Uninstall

4. SWCM_Uninstall.bat ファイルをダブルクリックして、アンインストールを開始します。
5. 画面の指示に従って、アンインストールプロセスを実行します。

アンインストールが実行され、CA Business Intelligence BusinessObjects Enterprise、CA EEM、CA MDB およびコンテンツインポートクライアントを除くすべてのインストール済みの CA SCM 12.6 コンポーネントが正常に削除されます。

第 8 章: トラブルシューティング

このセクションには、以下のトピックが含まれています。

[「インストールが開始されない」または「サーバが見つからない」というエラーが表示される \(P. 167\)](#)

[テナント管理ページを表示できないというブラウザ エラーが表示される \(P. 168\)](#)

[テナント管理ページが表示されない \(P. 168\)](#)

[Web サーバ名にアンダースコア文字が使われている \(P. 168\)](#)

[拡張文字が含まれるユーザ名を使うとログインに失敗する \(P. 169\)](#)

[IIS 7 が Windows 2008 にインストールされると WCF サービスが失敗する \(P. 169\)](#)

[「含まれていないオペレーティング システム」というメッセージがメッセージ キューに表示される \(P. 170\)](#)

「インストールが開始されない」または「サーバが見つからない」というエラーが表示される

サポートされているすべてのオペレーティング環境に該当します。

問題の状況:

CA APM のインストールを開始するとき、「インストールが開始されない」または「サーバが見つからない」というエラーが表示されます。

解決方法:

UtilDev Web Server Pro という Windows サービスを再起動します。

テナント管理ページを表示できないというブラウザ エラーが表示される

問題の状況:

[管理] - [テナント管理] をクリックすると、以下のようなブラウザ エラーメッセージが表示されます。

ページを表示できません。

解決方法:

CA CASM サービスが開始されていることを確認します。

テナント管理ページが表示されない

問題の状況:

[管理] タブをクリックしても、[テナント管理] のオプションが表示されません。

解決方法:

テナント管理アクセスが有効な役割が、CA APM 管理者によって割り当てられていません。[テナント管理] へのアクセスが必要な場合は、CA APM 管理者に問い合わせてください。

Web サーバ名にアンダースコア文字が使われている

サポートされているすべてのオペレーティング環境に該当します。

問題の状況:

Web サーバのホスト名にアンダースコア文字を使用すると、製品にログインするときや、ユーザ設定で CA EEM を使用するときに、問題が発生する場合があります。

解決方法:

仮想システムまたはゴーストシステムを使用している場合は、アンダースコア文字を含まない別のイメージを作成して、新しいホスト名を設定します。実稼働システムの場合は、別の URL で製品にアクセスできるように、内部ドメインネームシステム (DNS) に新しいホスト名を追加します。

拡張文字が含まれるユーザ名を使うとログインに失敗する

問題の状況:

CA EEM で単一 DB ログイン認証を使用しているとき、CA APM Web インターフェースにログインすることができません。

解決方法:

拡張文字（日本語またはドイツ語の文字）が含まれないユーザ名を選択します。

IIS 7 が Windows 2008 にインストールされると WCF サービスが失敗する

Windows 2008 オペレーティング環境で有効です。

問題の状況:

Windows 2008 に Microsoft インターネット インフォメーション サービス (IIS) 7 がインストールされると、WCF サービスが動作しません。CA APM では、WCF サービスを使用して Web サービス機能を実装します。

解決方法:

サービス ファイル タイプが正確にマップされていないか、IIS 7 などの Windows コンポーネントが正しい順序でインストールされていない場合に、この問題が発生します。この問題を修正するには、IIS 設定を確認し、（必要に応じて）変更します。Microsoft から、この問題に関する情報と解決策が提供されています。

この問題を解決するには、以下の手順を実行します。

1. Web ブラウザで、Microsoft の Web サイト (<http://www.microsoft.com>) を開き、「IIS ホスト サービスのエラー」を検索します。
2. 記事の指示に従います。

「含まれていないオペレーティング システム」というメッセージ キューに表示される

問題の状況:

照合エンジンによる正規化ルールの処理中に、メッセージ キューに以下のいずれかのエラー メッセージが表示されます。

- 以下の検出されたオペレーティング システムが、パブリック オペレーティング システム リストにありません:
 含まれていないオペレーティング システム: オペレーティング システム名
- 以下の検出されたオペレーティング システムは、オペレーティング システム リストに含まれていないため、パブリック オペレーティング システム リストまたはテナント用リストに追加する必要があります: テナント名
 含まれていないオペレーティング システム: オペレーティング システム名

注: 照合エンジンによって、データベース内のメッセージ キューにメッセージが書き込まれます。これらのエラー メッセージがメッセージ キューに表示されるには、ハードウェア照合エンジンの構成設定で [エンジンのデバッグ レベル] を [致命的] (またはそれより高い詳細レベル) に設定します。メッセージ キューと構成設定の詳細については、「CA APM 管理ガイド」を参照してください。

解決方法:

正規化ルールは、すべてのテナントと公開データに適用され、複数のテナントにわたって使用される場合があります。正規化リストを通じて割り当てられたオペレーティング システム値がテナントに存在しない場合、照合エンジンによってエラー メッセージが生成され、オペレーティング システムをそのテナント用または公開データとして追加する必要があることが通知されます。

注: 正規化ルールの詳細については、「CA APM 管理ガイド」を参照してください。

含まれていないオペレーティング システムが 1 つか 2 つの場合は、正規化ルールにオペレーティング システムを手動で追加することによって問題を解決できます。オペレーティング システムの正規化ルールを定義する方法の詳細については、「CA APM 管理ガイド」を参照してください。

含まれていないオペレーティング システムが多数の場合、この問題を解決するには、以下の手順を実行します。

1. CA APM にログインし、[管理] - [照合管理] をクリックします。
2. 左側の [照合メッセージ検索] をクリックします。

[検索結果] に、メッセージ キューの照合ログ メッセージが表示されます。

3. 含まれていないオペレーティング システムの正規化ルールに関するエラー メッセージを検索します。
メッセージ キューに、含まれていないオペレーティング システムの正規化 ルールに関するエラー メッセージがすべて表示されます。
4. 製品に登録されたシステム管理者の電子メール アドレスが正しいことを確 認し、 [CSV へのエクスポート] をクリックします。
含まれていないオペレーティング システムが CSV ファイルにエクスポート されます。システム管理者が、CSV ファイルへのリンクが記載された電子メー ル メッセージを受信します。
5. CSV ファイルのコンテンツを編集して、Data Importer 用のファイルを準備 します。たとえば、重複したオペレーティング システムや不要な語句をファイ ルから削除できます。
注: Data Importer の使用方法の詳細については、「管理ガイド」を参照して ください。
6. CA APM にログインし、 [管理] - [Data Importer] をクリックして、オペレ ティング システムが含まれていないテナントまたは公開データを選択しま す。
7. CSV ファイルをインポートします。
含まれていないオペレーティング システムが CA MDB にインポートされ、照 合エンジンの正規化処理中に使用できるようになります。