CA Configuration Automation®

管理者ガイド

r12.8

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA® Embedded Entitlements Manager（CA EEM）
- CA Spectrum®® Automation Manager
- CA® SiteMinder® Web Access Manager（CA SiteMinder）

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: CA Configuration Automation の概要

CA Configuration Automation は標準ベースのソフトウェア製品であり、 企業の分散したハードウェアおよびソフトウェアのコンポーネントを、一元化されたブラウザ ベースのウィンドウで管理できます。 CA Configuration Automation を使用することにより、以下のことができます。

- ユーザの企業内のサーバを検出
- それらのサーバにインストールされているオペレーティング システム、データベースおよびソフトウェア アプリケーション コンポーネントを特定
- 複雑なデータ、情報および構成の設定に、コンポーネント内からアクセス
- ユーザの企業内のサーバ間の関係および依存関係を特定
- サーバおよびサービス設定の変更および相違を検出
- ユーザのサービスのスナップショット（あるタイミングにおけるコピー）を作成および保持
- ソフトウェア コンポーネントおよび設定ポリシーの、企業標準およびベストプラクティスへの準拠を保証
- サービス内のソフトウェア コンポーネントの複数の属性に対する変更を実行
- ユーザのサーバとサービスの修復に要する平均時間について、トラブルシュートおよび改善を実行

以下のセクションでは、CA Configuration Automation ソフトウェア コンポーネントについて説明し、重要な概念についての概要を示します。

CA Configuration Automation の概念

このセクションでは、ユーザになじみのない可能性がある CA Configuration Automation 用語および概念について説明します。 このドキュメントには、これらの用語およびその他の用語が簡潔に定義された用語集が含まれています。

CA Configuration Automation は、ユーザの企業の分散したソフトウェア コンポーネントを管理するための、2 つの異なる方法をサポートします。

- *サーバ中心*の管理は、ユーザの企業のインフラストラクチャを管理するニーズを満たします
- *サービス中心*の管理は、ユーザの企業全体にわたる複雑に階層化されたアプリケーションやマルチ コンポーネント アプリケーションを管理する上でのニーズを満たします

CA Configuration Automation は、どちらの方法でもディスカバリ、スナップショット、リフレッシュ、変更の検出、比較、およびルール コンプライアンス操作を提供します。

ディスカバリ

サーバとソフトウェアを検索するためにディスカバリ操作を実行するネットワーク セグメントを識別できます。 各ネットワーク セグメントに一意の名前を割り当てて、サーバをスキャンできます。 さらに、実行するスキャンのタイプおよび頻度を指定する管理プロファイルを定義することができます。その後、この管理プロファイルを 1 つ以上のネットワーク セグメントに割り当てて、企業全体にわたってディスカバリ操作を自動化することができます。

CA Configuration Automation は、組織のネットワーク全体にわたるサーバおよびソフトウェア コンポーネントの、総合的で最新のインベントリを確立することにより、ユーザの企業のアプリケーション管理を開始します。コンポーネントを検出すると、ディレクトリ、ファイル、レジストリ、データベース テーブル、および構成パラメータを含む、アプリケーションの完全なクロスプラットフォームのインベントリを詳細に取得できます。アプリケーション ベースのディスカバリの基準はブループリントです。これは、CA Configuration Automation エージェントがサーバ上でアプリケーションを検索できるようにするために、そのアプリケーションの基本的な構造をまとめたものです。 ブループリントについては、このセクションで詳しく説明します

第 2 章: ブループリントの概要

ブループリントはソフトウェア コンポーネントの概念的な定義またはメタデータです。このメタデータは、以下の処理を行うためのディレクティブおよびメカニズムを定義します。

- 指定されたコンピュータ上のソフトウェア コンポーネントを検出します
- コンポーネントのファイル システムおよびデータベース エレメントをキャプチャします
- コンポーネント内およびコンポーネント間の関係および依存関係を表現および表示します
- 構成情報を検索、分析、および管理します
- 診断マクロを定義、実行、および解析します
- これらのすべてのエレメントに、推奨されるベスト プラクティス値を定義します

CA Configuration Automation は、構成および管理タスクを簡略化する標準化された形式でブループリントを表示します。 CA は、共通で使用されているソフトウェア コンポーネントの、事前定義済みブループリントのライブラリを提供します。 既存のブループリントを編集したり、カスタム ブループリントを作成することもできます。

サービス

CA Configuration Automation では、サービスは、1 つ以上の管理対象サーバで実行されているソフトウェア コンポーネントのコレクションとして定義されます。 ユーザは、検出する必要があるサーバ、サーバ グループ、および関連するコンポーネント ブループリントを指定することで、サービスを定義できます。通常、企業内の一意のビジネス機能に対して 1 つのサービスが充当されますが、企業内では 1 つのサービスのインスタンスを複数稼働されることもできます。

CA Configuration Automation では、構成詳細、依存関係と制約ルール、ファイル システム エレメント、ランタイム ログ、診断、ユーティリティ、およびコンポーネントのインベントリを含む、すべてのサービスの標準化された注釈付きのビューが表示されます。

［プロファイル］

プロファイルを使用すると、ユーザは以下のプロファイルを使用する CA Configuration Automation ディスカバリおよび管理操作を自動化することができます。

- アクセス プロファイルはサーバと関連付けられ、サーバ アクセスおよびエージェント インストールのルールを提供します。
- ネットワーク プロファイルは、サーバを検出するための操作ルールを提供します。
- 管理プロファイルはネットワークおよびサーバ レベルで作成して割り当てると、ディスカバリ、ブループリント、およびソフトウェア管理タスクを管理することができます。
- 通知プロファイルには、ある操作が実行されるときに送信される電子メール メッセージを作成するための通知詳細が格納されます。

スナップショット

CA Configuration Automation は、スナップショットを使用して企業をモニタすることで、コンポーネントまたはサーバ内の変更を検出できます。 スナップショットは、サーバまたはサービスのソフトウェア構成のある時点のコピーです。 ユーザは自動的にアプリケーションのインベントリを再キャプチャして構成データを十分な詳細のスナップショットにアーカイブし、それをトラブルシューティング、レコード保持、またはリリース管理、およびマイグレーション計画に使用することができます。

また、スナップショットを［ゴールド基準］として指定し、監査および変更の検出のベースラインとして、スナップショット内のアプリケーションの状態に使用することができます。

ルール コンプライアンス

CA Configuration Automation が収集する詳細情報の使用およびルール コンプライアンス操作の実行により、複雑なアプリケーションの、内部および規定のコンプライアンスとの適合が保証されます。 CA Configuration Automation は、アプリケーションの制御を支援して柔軟で綿密なポリシー定義を備えたベスト プラクティスを確立し、さらにユーザ定義のルールの適用を自動化します。 企業のパフォーマンス構成、セキュリティの設定、および従属変数の監査はアプリケーションのインフラストラクチャを強固にし、エラーの出やすい手動のレビューから組織を解放します。

CA Configuration Automation コンポーネント

CA Configuration Automation ソフトウェアには、以下のコンポーネントが含まれます。

- CA Configuration Automation サーバ
- CA Configuration Automation データベース
- CA Configuration Automation エージェント
- CCA グリッド ノード
- CA Network Discovery Gateway
- CA EEM
- BusinessObjects レポート サーバ

これらのコンポーネントについては、以降のセクションで説明します。

CA Configuration Automation サーバ

CA Configuration Automation サーバ では、一貫したストレージ管理、データ アクセス制御、および CA Configuration Automation エージェントとの通信管理を行う中央レジストリとして動作する、ブラウザ ベースのユーザ インターフェースが提供されます。 CA Configuration Automation サーバ により、ディスカバリ、構成、調整、および分析機能を含めた製品の操作のすべての局面が制御されます。 CA Configuration Automation サーバ は、すべての Windows サーバからサポートされているブラウザでアクセスすることができます。

CA Configuration Automation データベース

CA Configuration Automation データベース には、収集された CA Configuration Automation データおよび構成情報がすべて格納され、これには以下のものがあります。

- サーバ構成（ハードウェア、ソフトウェア、システム情報）
- サービス構成とコンポーネント
- サーバおよびサービスのスナップショット
- ジョブ スケジューラ情報
- カスタム レポート定義
- カスタム ブループリント

CA Configuration Automation サーバ のインスタンスはそれぞれ対応するデータベース インスタンスを必要とします。 複数の CA Configuration Automation サーバ は、同じデータベース サーバ上の同じデータベースを共有できますが、各サーバは、データベース インスタンス内にデータを格納するための専用のテーブルスペースおよびテーブルのセットを保持している必要があります。

CCA エージェント

CA Configuration Automation エージェントは軽量の実行可能ファイルで、ユーザの企業の CCA 管理対象サーバ上で実行されているサービス ブループリント ベース コンポーネントの、サーバを対象にする操作を検査し、実装します。 CCA エージェントは、サーバとソフトウェアの両方の構成に関して詳細な構成管理を実行できます。

CA Configuration Automation エージェントは、UNIX ベースのサーバ上にデーモンとして、または Windows ベースのサーバ上にサービスとしてインストールされます。

CA Configuration Automation でサーバおよびサービスを詳しく管理するには、CA Configuration Automation エージェントを企業内のすべての管理対象サーバにインストールする必要があります。 また、CA Configuration Automation サーバ コンポーネントの検出および管理を行うには、各 CA Configuration Automation サーバ マシンに CA Configuration Automation エージェントをインストールすることをお勧めします。

注: CA Configuration Automation は、対象のシステムに関して、SSH を使用したエージェント不要の安全な問い合わせおよび監視機能も提供します。このオプションは、エージェントのインストールを実行できない場合、またはプラットフォームで CA Configuration Automation エージェントがサポートされていない場合の代替として実行できます。

CCA グリッド ノード

グリッド処理は、複数のグリッド ノードに処理の負荷を分散させてパフォーマンスを向上させるために使用されます。1 台のサーバで複数のスレッドを使用して、複数の CCA グリッド ノードをサポートすることができます。 CA Configuration Automation の処理は*グリッドに対応しており*、処理を独立した実行可能エンティティに分割することができます。 これらの実行可能エンティティは、グリッド サーバ、グリッド ノード、およびスレッドに分散して実行されます。

CCA グリッド ノードは Linux、UNIX および Windows のプラットフォームでサポートされており、各プラットフォーム専用のインストール プログラムがあります。 CCA グリッド ノードをインストールし、CA Configuration Automation サーバ にそれを登録した後は、CA Configuration Automation ユーザにとってグリッド処理は不可視になります。

CA ネットワーク ディスカバリ ゲートウェイ

NDG サーバは、企業内のサーバおよびサービスの場所を特定し監視する CA Configuration Automation のディスカバリ処理を行います。 CA Configuration Automation サーバ をインストールする前に、サポートされている Windows プラットフォームに NDG サーバをインストールする必要があります。CA Configuration Automation インストール プログラムによって、NDG サーバの名前、およびディスカバリ処理に使用するポートの入力が求められます。

CA EEM

CA Embedded Entitlements Manager（CA EEM）は、CA Configuration Automation ユーザ インターフェースに対してユーザやグループの管理およびロールベースの認証サービスを提供します。

Business Objects

Business Objects は CA Configuration Automation に付属するサードパーティ製のビジネス インテリジェンス プラットフォームであり、対話型のレポート機能を提供します。 事前定義済みの CA Configuration Automation レポートが Business Objects サーバ上でホストされます。

第 3 章: CA Configuration Automation ユーザ インターフェースの使用

この章では CA Configuration Automation ブラウザ ベースのユーザ インターフェースを紹介します。 コマンド ライン インターフェース（CLI）の詳細については、「コマンド ライン インターフェースの使用」を参照してください。

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 Configuration Automation へのログイン

ユーザ インターフェースにアクセスするには、CA Configuration Automation にログインします。 初めてログインする場合は、正しい URL を入力し、デフォルトまたはユーザ定義の CCA 管理者ユーザとしてログインします。UI にアクセスすると、パスワードを変更できます。

次の手順に従ってください:

1. サポートされている Web ブラウザを開き、アドレス フィールドに以下のような適切な URL を入力します。

   `http://<server>:port/CCAUI.html`

   `http://<server>:port/CCAUI.jsp`

   <server>

   インストール中に入力した CA Configuration Automation サーバ名を定義します。

   port

   インストール中に入力したポート番号を定義します。

   デフォルト： 8080

   CA Configuration Automation のログイン ページが表示されます。

2. （オプション）ブラウザ ツールバーの［お気に入り］をクリックし、メニューから［お気に入りに追加］を選択して、ログイン ページをお気に入りの Web ページに追加します。

3. ログイン ページで、以下のいずれかのアクションを完了し、［ログイン］をクリックします。

   - CA Configuration Automation サーバ のインストール中にデフォルトの CCA 管理者を使用した場合、［ユーザ名］および［パスワード］フィールドに「ccaadmin」を入力します。
   - CA Configuration Automation サーバ のインストール中にデフォルトの CCA 管理者を使用しなかった場合、CCA 管理者に指定した名前およびパスワードを入力します。

   ［タスク］パネルが表示され、ログインしている管理者ユーザが表示されます。ユーザが関連するパスワードを変更できるリンクも表示されます。

CA Configuration Automation UI の概要

CA Configuration Automation にログインすると、［タスク］パネルがデフォルトで表示されます。

右上のリンクから以下の主な UI パネルにアクセスできます。

- 管理
- ダッシュボード
- 環境管理
- タスク

各パネルには、オンライン ヘルプ システムへのリンクが存在します。 以下のセクションでは、各パネルについて簡単に説明します。

管理パネル

日々のほとんどの構成管理操作は［管理］パネルで完了します。

関連するタイプのオブジェクトを作成、表示、管理するには、［管理］パネルで以下のタブを使用します。

- サービス
- サーバ
- ソフトウェア
- ネットワーク
- ブループリント
- コンプライアンス
- 修復
- ジョブ
- ログ
- レポート

管理タブ ページにはそれぞれ、そのページで定義されるオブジェクトをリスト表示するテーブルが含まれます。 オブジェクトはテーブルに手動で、またはディスカバリ操作の結果として追加できます。別のアプリケーションからオブジェクトをインポートできます。または、CA Configuration Automation インストール プログラムにより、事前定義済みデータとして別のアプリケーションのオブジェクトをインストールできます。

［レポート］タブを除いて、すべての管理タブに［フィルタ］ペインが含まれています。このペインでフィルタし、選択したオブジェクトのみを表示します。 フィルタの作成に関する詳細については、「テーブル ビューでのフィルタリング (P. 28)」を参照してください。

ほとんどの管理タブにはまた、管理アクションを選択できる以下のドロップダウン リストが含まれます。

アクションの選択

オブジェクトおよび操作を実行、管理、エクスポート、削除するためのオプションが含まれています。

テーブル ビュー

デフォルト テーブル ビューまたは自分で作成するカスタム ビューを表示するためのオプションが含まれています。

テーブル アクション

オブジェクト（サーバやサービスなど）を作成またはインポートするためのオプションと以下の共通タスクが含まれています。

- Excel にエクスポート
- 印刷
- テーブル ビューの構成

すべてのタブ ページにある［テーブル アクション］ドロップダウン リストに共通タスクがリスト表示されます。 共通タスクの詳細については、「共通のテーブル アクション」を参照してください。

［管理］パネルの詳細については、関連するタブに対応するセクションを参照してください。

ダッシュボード パネル

ダッシュボード パネルには、［グラフ］および［ビジュアル］の 2 つのタブが含まれます。

[グラフ]タブ

［グラフ］タブでは、［ダッシュボード］および［グラフ］の 2 つのフォルダが含まれる［ダッシュボード］ペインを使用できます。 ［ダッシュボード］フォルダには、CA Configuration Automation で管理するオブジェクトのグラフィカルなサマリを表示する、以下の事前定義済みダッシュボードが含まれます。

- VM ホスティング サーバ
- VM ゲスト ソフトウェア コンポーネント
- VM ゲスト サーバ
- 仮想化
- ソフトウェア コンポーネント
- サービス
- サーバ（管理対象外）
- サーバ（管理対象）
- サーバ
- コンプライアンス
- 通信関係
- 変更履歴

［グラフ］フォルダには、関連するグラフが含まれる以下のサブフォルダが含まれます。

- すべてのグラフ
- サーバ
- 関係
- 仮想環境
- アプリケーション
- ソフトウェア コンポーネント

- サービス
- ルール コンプライアンス
- 変更の検出
- グリッド情報

ダッシュボード、およびそれに対応するグラフには、それらを表示、構成、削除、およびリフレッシュするためのオプション、また情報をどのように表示するかを変更するためのオプションが含まれています。 さらに、新しいダッシュボードやカスタム ダッシュボードを作成することができ、他の CA Configuration Automation 実装との、ダッシュボードのインポートやエクスポートも可能です。

［ダッシュボード］パネルの詳細については、「ダッシュボード」を参照してください。

[ビジュアル]タブ

［ビジュアル］タブでは、［グラフ］および［テンプレート］の 2 つのフォルダが含まれる［ビジュアル］ペインを使用できます。 ［グラフ］フォルダおよび［テンプレート］フォルダには両方とも、以下のサブフォルダが含まれます。

- アプリケーション
- サーバ
- サービス
- ソフトウェア コンポーネント

［グラフ］サブフォルダ内の事前定義済みビューを表示したり、［テンプレート］サブフォルダ内のビューを表示、変更、および保存してカスタム グラフを作成したりできます。

［ビジュアル］パネルの詳細については、「ビジュアル」を参照してください。

環境管理パネル

以下の［環境管理］パネル タブでは、CA Configuration Automation ユーザの定義と管理、CA Configuration Automation サーバ設定の表示と構成、ポート ベースの通信マッピングの管理を行います。

構成

以下のページが含まれています。

プロパティ

CA Configuration Automation の外観と動作を表示し、編集するための設定が含まれています。

セキュリティ証明書

CA Configuration Automation サーバ および CA Configuration Automation エージェントを作成および管理するための設定が含まれています。

通信マッピング

製品がポートを介して一般的に使用するポート番号および通信タイプをリスト表示します。 このページで、通信タイプの設定を編集できます。

アプリケーション マッピング

関連するアプリケーションの標準インストール ディレクトリを識別するアプリケーションおよび正規表現をリスト表示します。 このページで、マッピングを追加、編集、管理できます。

詳細については、「構成の設定 (P. 37)」を参照してください。

アクセス管理

CA EEM 統合機能を提供する以下のアクセス管理ページにリンクしています。

ユーザ

ユーザを作成および管理するための機能を提供します。

ポリシー

特定の CA Configuration Automation 機能へのユーザ アクセスを管理するための機能を提供します。

構成

ユーザおよびユーザ グループ情報の格納場所およびアクセス元を指定します。

詳細については、「アクセス管理の構成 (P. 90)」を参照してください。

ネットワーク

Network Discovery Gateway がインストールされているサーバを表示する［Network Discovery Gateway］テーブルが含まれています。このページから NDG サーバの作成、管理、および削除ができます。

Catalyst 統合

事前定義済みおよびカスタム Catalyst 属性プロファイルを表示する［Catalyst 属性プロファイル］テーブルが含まれています。 このページから［Catalyst 属性プロファイル］を作成、インポート、エクスポート、編集、削除、およびコピーすることができます。

プロファイル

事前定義済みおよびカスタムの Catalyst 属性プロファイルを定義します。CA Catalyst サーバにエクスポートする CI を決定できます。

ジョブ

CA Configuration Automation から Catalyst サーバに発行される情報（サーバ、サービス、ストレージ システム、またはブループリント）を指定します。

ログ

プロファイルおよびジョブに関連する操作をログ記録します。

診断

以下の診断ページにリンクしています。

CCA 情報

UI に関する構成詳細および CA Configuration Automation 統合を表示します。

データベース情報

CA Configuration Automation データベース およびデータベース スキーマに関する構成の詳細を表示します。

グリッド情報

すべてのグリッド ノードの詳細を表示します。 このタブにはまた、テーブル ビューまたはツリー ビューで CA Configuration Automation サーバ グリッド ジョブが表示されます。

分散ロック情報

グリッドの間でサービスの割り当てを調整するために、グリッドの間で共有されるロックを指定します。 ロックはスケジュールされたジョブが実行される場所のサーバ詳細を提供します。 サービスが割り当てられ、エラーが発生した場合、再度割り当てられます。

診断の収集

CA Technologies Support が CA Configuration Automation サーバ または CA Configuration Automation サーバ グリッド ノードの問題をトラブルシューティングするためにリクエストする情報を収集します。

ログ アーカイブ

ログが最大のストレージ サイズ制限を超えるときにアーカイブされるログを指定します。

データ移行

CA Cohesion CCA からデータを移行するための以下のオプションを提供します。

- Cohesion データベースから CA Configuration Automation 12.6 へ
- Cohesion データベースから JAR ファイルへ
- JAR ファイルから CA Configuration Automation データベースへ
- CA Cohesion ACM から CA Configuration Automation r12.6 にセキュリティ証明書をインポートします。

CA Cohesion ACM から CA Configuration Automation にデータを移行する方法の詳細については、「CA Cohesion ACM からのデータの移行 (P. 125)」を参照してください。

タスク パネル

［タスク］パネルを使用して、以下の一般的なタスクを完了します。

- ネットワークの検出
- アクセス プロファイルおよびエージェント展開
- サービスの検出
- コンプライアンス ジョブの実行
- エージェントの検索およびアップグレード

タスクをクリックすると、そのタスクの詳細な説明、およびそのタスクを完了するのに必要なサブタスクにリンクするナビゲーション ボタンが含まれるウィザードが開きます。

テーブル ビューでのフィルタリング

各［CA Configuration Automation 管理］タブ ページ（サービス、サーバ、ネットワーク、ブループリント、コンプライアンス、修復、ジョブ、ログ、レポート）には、対応するオブジェクトの詳細を表示するテーブルが含まれています。これらのテーブルは、非常に大きくなる場合があります。大量のテーブル データを簡単に扱うには、重要なオブジェクトのみを表示するフィルタを作成します。

テーブル データをフィルタする方法

1. 9 つのタブ ページのうちのいずれかを開きます。

   ページに対応するテーブルが表示されます。たとえば、ユーザが［サーバ］タブを選択すれば、ページには［サーバ］テーブルが表示されます。

2. ドロップダウン リストからオプションを選択するか、または以下のフィールドに入力してフィルタを作成します。

   列

   フィルタするテーブル内の列を指定します。 ドロップダウン リストには、フィルタできるテーブル内の各列のオプションが含まれています。

   値

   フィルタの対象となる、選択した列内の値を指定します。 ドロップダウン リストによっては、［列］フィールドで選択された列の値のオプションが含まれます。 利用可能なオプションがない場合は、フィールドにテキスト文字列を入力する必要があります。

   注:

   - ［値］フィールドは、大文字と小文字を区別しません。
   - 文字列は正確に一致する必要があり、部分的に一致する場合は結果が返されません。たとえば、［ブループリント］テーブルにすべての「Apache ブループリント」を表示する場合、「Apache」と入力しても、ブループリントは返されません。
   - ワイルドカードがサポートされています。ワイルドカードとしてアスタリスク（*）またはパーセント記号（%）を使用できます。たとえば「Apache*」は、Apache（Apache Tomcat Servlet Engine、Apache HTTP サーバなど）で始まるすべてのブループリントを返します。

3. （オプション）より複雑なフィルタを作成するには、さらにフィルタ基準を追加します。

   a. 以下のいずれかのオプションを選択します。

      - And - ［列］および［値］フィールドの両方のエントリに一致するオブジェクトをテーブルに表示するように指定します。
      - Or - ［列］および［値］フィールドのどちらかのエントリと一致するオブジェクトをテーブルに表示するように指定します。

   b. 2 番目の［列］のドロップダウン リストからオプションを選択します。

   c. 2 番目の値列内に値を入力するか、または選択します。

      たとえば、［ブループリント］ページで最初の［列］フィールドをブループリント名に設定し、最初の［値］フィールドを「Apache*」に設定、2 番目のフィールド ペアを「ブループリント バージョン」および「1.0.0」にし、［And］オプションを選択してフィルタを作成すると、バージョン 1.0.0 の Apache ブループリントが表示されます。 ユーザが［Or］オプションを選択した場合は、テーブルには Apache で始まるブループリント（バージョンにかかわらない）およびバージョン 1.0.0 のブループリント（名前にかかわらない）がすべて表示されます。

4. ［リフレッシュ］ボタンをクリックします。

   テーブルは、フィルタ条件と一致するオブジェクトの行を表示します。

フィルタをクリアし、すべてのテーブル データを表示する方法

1. 8 つのタブ ページのうちのいずれかを開きます。

   ページに対応するテーブルが表示されます。

2. 以下のいずれかを実行します。

   - フィルタのフィールドをクリアするには、［リセット］をクリックします。
   - 両方の［列］のドロップダウン リストから空白のエントリを選択します（空白オプションは、メニューの最初のエントリです。最初のテキスト オプションの上に表示されます）。

3. ［リフレッシュ］ボタンをクリックします。

   フィルタがクリアされ、テーブルには、テーブル データの最初の 50 行が表示されます（51 行から先は別ページに表示されます。1 ページに 50 行です）。

共通のテーブル アクション

各［CA Configuration Automation 管理］タブ ページ（［サービス］、［サーバ］、［ネットワーク］、［プロファイル］、［ジョブ］、［ブループリント］、［レポート］、［修復］）には、対応するオブジェクトの詳細を表示するテーブルが含まれています。各テーブルには［テーブル アクション］ドロップダウン リストがあり、ページに固有のテーブル アクションおよびすべてのテーブルに共通な以下の 3 つのオプションが含まれています。

- Excel にエクスポート
- 印刷
- テーブル ビューの構成

これらについては、次のセクションで説明します。

テーブル データを Excel にエクスポートする

テーブル データと列ヘッダを Microsoft Excel スプレッドシートにエクスポートして、CA Configuration Automation ユーザとして設定されていない人達と CA Configuration Automation データを共有することができます。

テーブル データを Excel にエクスポートする方法

1. エクスポートするテーブルがあるタブ ページを開きます。
2. ［テーブル アクション］ドロップダウン リストから［Excel にエクスポート］を選択します。

   ［ファイルをダウンロード］ウィンドウが表示され、ファイルを開くか保存するように指示されます。
3. 以下のいずれかを実行します。
   - ［保存］をクリックして、ファイルの名前と場所を入力し、［保存］をクリックします。

     指定した場所にファイルが保存されます。
   - ［開く］をクリックします。

     テーブル データが Excel に表示されます。 エクスポートしたデータをファイルとして保存するには、［名前を付けて保存］を選択します。

テーブル データの印刷

紙の写しが必要な場合は、テーブル データを印刷できます。

次の手順に従ってください:

1. 印刷するテーブルがあるタブ ページを開きます。
2. ［テーブル アクション］ドロップダウン リストから［印刷］を選択します。

   テーブル データがプリンタに送信されます。

テーブル ビューの作成

テーブル（たとえば［サーバ］テーブル）が含まれるタブ ページには、［テーブル アクション］ドロップダウン リストに［テーブル ビューの作成］オプションも含まれています。 このオプションを使用して、ユーザの個人的な好みに合わせてテーブルの内容を表示するカスタム テーブル ビューを定義します。

テーブル ビューを作成する方法

1. ［管理］リンクをクリックし、次にエレメント テーブル（たとえば［サーバ］タブ）が含まれるタブ ページが表示される任意のタブをクリックします。

   タブのページが表示されます。この例では、タブ ページに［サーバ］テーブルが含まれます。

2. ［テーブル アクション］ドロップダウン リストから［テーブル ビューの作成］を選択します。

   ［テーブル ビューの作成］ウィザードの［詳細］ページが表示されます。

3. 対応するフィールドに以下の情報を入力し、［次へ］をクリックします。

   名前

   テーブル ビューの名前を指定します。

   リフレッシュ間隔

   テーブルが自動的にリフレッシュされるレート（秒）を指定します。

   ページ サイズ

   1 ページ当たりのテーブルの行の最大数を指定します。

   並べ替え列

   並べ替え順序を決定するために使用する列を指定します。 たとえば、［サーバ名］列を選択した場合、サーバ名がアルファベット順に並べ替えられます。 ［作成日付/時刻］列を選択すると、サーバ名が時系列で並べ替えられます。

並べ替え順

［昇順］または［降順］を指定します。 たとえば、列がアルファベット順に並べ替えられ、並べ替え順序が［昇順］に設定されると、A から Z の順序になります。

共有ビュー

このビューをすべてのユーザに利用可能にするか、またはテーブル ビューの作成者にのみ利用可能にするかどうかを指定します。

［列］ページが、すべての利用できる列を表示した［選択された列］フィールドと共に表示されます（つまり、デフォルトでは、テーブルは利用可能な列をすべて表示します）。

4. このカスタム ビューから削除する［選択された列］フィールド内の 1 つ以上の列をダブルクリックします。

   選択した列は［使用可能な列］フィールドに移動されます。

5. ［次へ］をクリックします。

   ［フィルタ］ページが表示されます。

6. ドロップダウン リストからオプションを選択するか、または以下のフィールドに入力してフィルタを作成します。

列

フィルタするテーブル内の列を指定します。 ドロップダウン リストには、フィルタできるテーブル内の各列のオプションが含まれています。

値

フィルタの対象となる、選択した列内の値を指定します。 ドロップダウン リストによっては、［列］フィールドで選択された列の値のオプションが含まれます。 利用可能なオプションがない場合は、フィールドにテキスト文字列を入力する必要があります。

注:

- ［値］フィールドは、大文字と小文字を区別しません。
- 文字列は正確に一致する必要があり、部分的に一致する場合は結果が返されません。 たとえば、［ブループリント］テーブルにすべての「Apache ブループリント」を表示する場合、「Apache」と入力しても、ブループリントは返されません。
- ワイルドカードがサポートされています。ワイルドカードとしてアスタリスク（*）を使用できます。たとえば「Apache*」は、Apache（Apache Tomcat Servlet Engine、Apache HTTP サーバなど）で始まるすべてのブループリントを返します。

7. （オプション）より複雑なフィルタを作成するには、さらにフィルタ基準を追加します。

   a. 以下のいずれかのオプションを選択します。

      - And - ［列］および［値］フィールドの両方のエントリに一致するオブジェクトをテーブルに表示するように指定します。
      - Or - ［列］および［値］フィールドのどちらかのエントリと一致するオブジェクトをテーブルに表示するように指定します。

   b. 2 番目の［列］ドロップダウン リストからオプションを選択します。

   c. 2 番目の値列内に値を入力するか、または選択します。

   たとえば、［ブループリント］ページで最初の［列］フィールドをブループリント名に設定し、最初の［値］フィールドを「Apache*」に設定、2 番目のフィールド ペアを「ブループリント バージョン」および「1.0.0」にし、［And］オプションを選択してフィルタを作成すると、バージョン 1.0.0 の Apache ブループリントが表示されます。ユーザが［Or］オプションを選択した場合は、テーブルには Apache で始まるブループリント（バージョンにかかわらない）およびバージョン 1.0.0 のブループリント（名前にかかわらない）がすべて表示されます。

8. ［完了］をクリックします。

   カスタム テーブル ビューが作成され、［テーブル ビュー］テーブルに表示されます。

第 4 章: CA Configuration Automation の管理

このセクションには、以下のトピックが含まれています。

構成の設定

CA Configuration Automation によってインストールおよび参照される多くの構成ファイルがありますが、［プロパティ］ページにある使いやすい単一の UI を使用して多くの CA Configuration Automation 構成の設定を表示および編集することができます。［プロパティ］ページにアクセスするには、［環境管理］リンクをクリックして［構成］タブをクリックします。

［プロパティ］ページの構成の設定に加えて、［構成］タブ ページから以下のページにある設定にもアクセスでき、それらの設定を表示および管理することができます。

- セキュリティ証明書
- 通信マッピング

CA Configuration Automation プロパティの表示および編集

CA Configuration Automation 構成設定は、さまざまな構成ファイルに含まれていますが、UI の［プロパティ］ページで表示または編集できます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブの［プロパティ］リンクをクリックします。

   ［プロパティ］ページが開き、現在のプロパティが、グループ別にアルファベット順に表示されます（たとえば cca、discovery、eem、grid）。各プロパティについては、以下のセクションで説明します。

2. （オプション）編集するプロパティの横の［サーバ名］列をクリックし、CA Configuration Automation サーバ名または IP アドレスを入力します。

   CA Configuration Automation サーバ名または IP アドレスを指定しない場合、製品は CA Configuration Automation サーバ インスタンスをすべて編集します。

3. Enter キーを押して変更を保存します。

4. 編集するプロパティの横にある［値］列をクリックします。

   選択したフィールドが読み取り専用から読み取り/書き込みに変更されます。

5. 選択された［値］フィールドを編集し、Enter キーを押します。

   新しいプロパティが適切な構成ファイルに保存されます。

agent プロパティ グループ

agent プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

port

CA Configuration Automation エージェントのリスニング ポートを指定します。

デフォルト： 8063

agentless プロパティ グループ

agentless プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

probes.connectBurstSize

バースト サイズ。

デフォルト： 60

probes.connectTimeout

プローブ接続がタイムアウトするまでの秒数を指定します。

デフォルト： 5000

probes.connectTimeoutWin

Windows サーバに対するプローブのソケット接続タイムアウトを指定します。

デフォルト： 5000

probes.hostBatchSize

プローブが同時に開始されるサーバの数を指定します。

デフォルト： 4

probes.maxProbesInProgress

同時に実行できるプローブの最大数を指定します。

デフォルト： 60

probes.readTimeout

プローブが応答の読み取りに失敗するまでのミリ秒数を指定します。

デフォルト： 1000

probes.selectTimeout

ノンブロッキング IO 操作のタイムアウトを指定します。

デフォルト： 250

probes.threadCount

プローブによって使用されるスレッド数を指定します。

デフォルト： 0（無制限）

bo プロパティ グループ

bo （BusinessObjects）プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

admin.password

BusinessObjects 管理者ユーザ パスワードを定義します。

デフォルト： **********

admin.user

BusinessObjects 管理者ユーザ ID を定義します。

デフォルト： Administrator

mail.server.attachment.size

最大の電子メール添付ファイル サイズを定義します。

デフォルト： 25 MB

rptInstance.maxViewCount

［レポート インスタンス］タブに表示するレポート インスタンスの最大数を定義します。

デフォルト： 999

schedule.rpt.wait.time

レポートを完了するため、BusinessObjects に対する CCA の待ち時間（秒単位）を定義します。

デフォルト： 7200

server

BusinessObjects XI サーバ名を定義します。

server.auth

BusinessObjects レポート サーバにアクセスするために使用する認証タイプを定義します。

デフォルト： secEnterprise

server.port

BusinessObjects XI サーバのポートを定義します。

デフォルト： 6400

user.group

CCA の BusinessObjects レポート グループを定義します。

デフォルト： CCA Users

user.prefix

^$+userID 識別子に追加する BusinessObjects ユーザ名のプレフィックスを定義します。

デフォルト： cca

webserver.name

BusinessObjects サーバの名前または IP アドレスを定義します。

webserver.port

BusinessObjects のサーバのリスニング ポートを定義します。

デフォルト： 8080

webserver.protocol

BusinessObjects サーバが使用する通信プロトコルを定義します。

デフォルト： HTTP

catalyst プロパティ グループ

catalyst プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

catalyst.checksum.delete

［Catalyst 統合］の［ジョブ］ページで、［アクション］ドロップダウン リストに［再発行のためのクリア］項目を表示するか表示しないかを指定します。

デフォルト： false （メニュー項目は表示されません）

catalyst.events.enabled

Catalyst アラート イベントをトリガするかどうかを指定します。

デフォルト： false （Catalyst アラート イベントがトリガされます）

catalyst.server.httpport

Catalyst サーバのリスニング ポートを定義します。

catalyst.server.name

Catalyst サーバの名前または IP アドレスを定義します。

cca プロパティ グループ

cca （CA Configuration Automation）プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

add.server.simulation

CA Technologies 内部使用専用。

デフォルト： false

agent.cmd.retries

ディスカバリ中にサーバがエージェントと通信するために実行する再試行数を定義します。

デフォルト： 5

agent.cmd.retry.wait.sec

ディスカバリ中にサーバが次の再試行を行うまで待機状態となる間隔（秒単位）を定義します。

デフォルト： 5

agent.cmd.timeout.sec

エージェント コマンド応答を待つ間隔（秒単位）を定義します。

デフォルト： 600

agent.keystore

CA Configuration Automation サーバ キーストア名を定義します。

agent.keystorePassword

CA Configuration Automation サーバ キーストアのパスワードを定義します。

デフォルト： **********

agent.simulator

CA Technologies 内部使用専用。

agent.soap.connect.timeout

サーバとエージェントが SSL 経由で通信している場合、SOAP 接続タイムアウトが発生するまでの間隔（ミリ秒単位）を定義します。

デフォルト： 5000

agent.ssl.enabled

SSL が CA Configuration Automation サーバ で有効化かどうかを指定します。

デフォルト： false

agent.truststore

エージェント通信の truststore の場所を定義します。

agent.truststorePassword

truststore の パスワードを定義します。

デフォルト： **********

archive.cleanup.limit.minutes

バックログを削除するためにクリーンアップ ジョブが使用できる間隔（分単位）を定義します。 特定のサーバまたはサービスに対して管理プロファイルを実行していない場合、手動の比較操作またはスナップショット操作用のバックログが作成されます。

デフォルト： 60

archive.management.profile.limit.minutes

初めて CCA にアップグレードした場合、管理プロファイルのアーカイブが使用できる間隔 (分単位) を定義します。アップグレード中、アーカイブされていないスナップショットの中には、アーカイブに時間がかかるものがあります。

デフォルト： 1

archive.purge.eligibility.minutes

最近追加されたか、アーカイブから回復したか、表示されたスナップショットが、アーカイブの対象となるのが適切でない間隔（分単位）を定義します。

重要: CA テクニカル サポートから指示された場合のみ、archive.cleanup.limit.minutes、archive.management.profile.limit.minutes および archive.purge.eligibility.minutes プロパティ グループを編集してください。

auto.refresh.limit

自動フィルタ テーブル UI リフレッシュの許容最大数を定義します。

デフォルト： 50

cleanup.execution.interval

使用されていないオブジェクトの自動データベース クリーンアップが実行される間隔を時間数で定義します。

デフォルト： 24

db.batch.chunk.size

CA Configuration Automation サーバ がストレージまたは処理目的で CA Configuration Automation データベース に送信するデータ量を定義します。

デフォルト： 500

db.garbage.collection.interval

Java 関連のガベージ コレクション間の分数を定義します。

デフォルト： 30

discover.lock.timeout

［自動データベース ロック］のタイムアウトを定義します。

デフォルト： 30000

discovery.debug.enabled

ディスカバリのデバッグを有効にするかどうかを指定します。

デフォルト： false

discovery.extensive.log

拡張されたサーバおよびテスト ディスカバリ ログを指定します。 このログは、インジケータ検索、実際に使われているコンポーネント ルート、およびディスカバリからブループリントが除外された理由に関する情報を提供します。 拡張されたログにより、エラーを解決するための行動計画が提供されます。

デフォルト： いいえ

installation.port

CA Configuration Automation サーバ リスニング ポートを定義します。

デフォルト： 8080

installation.protocol

CA Configuration Automation サーバ が使用する UI アクセス プロトコルを定義します。

デフォルト： HTTP

installation.server

CA Configuration Automation サーバ ホスト コンピュータの名前を定義します。

job.archive.minimum.records

ジョブ履歴アーカイブを完了するために必要なレコードの最小数を定義します。

デフォルト： 200

job.archive.skip.records

残りのレコードをアーカイブする前にスキップされるレコードの数を定義します。

デフォルト： 200

job.archive.threshold

ジョブ履歴アーカイブに含めることができるレコードの最大数を定義します。

デフォルト： 500

locale

ロケールを定義します。

デフォルト： ja

log.archive.directory

ログ ファイル アーカイブの場所を定義します。

log.archive.minimum.records

ログ アーカイブを作成するために必要とされるレコードの最小数を定義します。

デフォルト： 1000

log.archive.skip.records

残りのレコードをアーカイブする前にスキップされるレコードの数を定義します。

デフォルト： 1000

log.archive.threshold

ログ アーカイブに含めることができるレコードの最大数を指定します。

デフォルト： 5000

log.viewer.threshold

各データベース操作で取得されるログ テーブル レコードの最大数を定義します。

デフォルト： 10000

mail.from

管理用の電子メールの送信先のアドレスを定義します。

デフォルト： ccaserver@noreply.*CCA_Server_name*

mail.server

管理用の電子メールを送信元の電子メール サーバは定義します。

max.treeview.items

グリッド ジョブおよびクラスタ UI で表示できるツリー ビュー項目の最大数を定義します。

デフォルト： 500

maximum.jobThreads

CA Configuration Automation サーバ またはグリッド サーバ当たりのジョブ スレッドの最大数を定義します。

デフォルト： 32

server.ssl.enabled

UI にアクセスするために CA Configuration Automation サーバ が HTTPS を使用するかどうかを指定します。

デフォルト： false

service.profiler.debug.enabled

サービス プロファイラ UI 内の［サービス プロファイル］ペインに、［クエリの表示］ボタンが含まれるかどうかを指定します。 関連するデバッグ機能により、サービスをグラフ表示するために使用されるクエリが表示されます。

重要: このプロパティは、CA テクニカル サポートから指示があった場合のみ編集してください。

set.session.timeout.interval.minutes

ユーザが CA Configuration Automation から自動ログ アウトするまでの間隔（分単位）を定義します。

デフォルト： -1 ユーザが自動的にログアウトになることはありません。

single.thread.metalink

CA Technologies 内部使用専用。

デフォルト： true

ssh.discovery.jTDS.driver.available

jTDS JDBC ドライバを Microsoft SQL Server との接続に使用するかどうかを指定します。

デフォルト： false （jTDS JDBC ドライバを使用しない）

ssh.file.based

SSH ファイルベースのディスカバリを使用するかどうかを指定します。このオプションを false に設定すると、キャッシュに SSH Discovery 結果が格納されます。巨大ファイル システムを対応したサーバが検出された場合、メモリは大容量データを格納できません。 その結果、メモリ不足例外が発生します。このフラグを true に設定すると、ディスカバリ結果は一時ファイルにリダイレクトされます。 結果を解析した後、ファイルは削除されます。

デフォルト： false （SSH のファイル ベースのディスカバリを使用しない）

ssh.file.chunk.size

ssh.file.based プロパティを true に設定した場合、一時ファイルへの書き込みが行われる前に、キャッシュ結果から読み取りが行われる最大バイト数を定義します。

デフォルト： 8192 （8 MB）

ssh.rexec.timeout.sec

SSH Server コマンドが失敗するまでの間隔（秒単位）を定義します。

デフォルト： 90

ssh.socket.timeout.sec

SSH Server 接続が終了するまでの間隔（秒単位）を定義します。

デフォルト： 300

telnet.connection.retries

ディスカバリ中に何らかの理由で Telnet 接続が切断された場合、再接続の試行回数を定義します。

デフォルト： 3 ディスカバリ中に Telnet で接続がドロップする場合は、この値を 6 に増やします。

telnet.read.add_cr_byos

指定されたオペレーティング システムの Telnet コマンドにキャリッジ リターンを追加するかどうかを指定します。デフォルトでは、Telnet コマンドがキャリッジ リターンを必要としないため、オペレーティング システムの指定は不要です。

telnet.read.byte_to_byte_delay_secs

結果を読み取り中、次のバイトを待機する最大時間（秒単位）を定義します。アクセス プロファイル内の[プロンプトの表示方法]オプションをオフにした場合のみ、本製品はこの値を使用します。

デフォルト： 2. ディスカバリ中に Telnet で接続をドロップする場合は、この値を 4 に増やします。

telnet.read.timeout_secs

コマンドを発行した後に、結果を収集するまで待機する最大間隔（秒単位）を定義します。

デフォルト： 900 。ディスカバリ中に Telnet で接続をドロップする場合は、この値を 1500 に増やします。

timezone

CA Configuration Automation サーバが使用するタイム ゾーンを定義します。

wmi.file.based.discovery

WMI ベースのディスカバリに対してファイル ベースの操作を使用するかどうかを指定します。 このプロパティを true に設定すると、パフォーマンスを向上させるため、WMI ディスカバリでファイル ベースの操作を使用します。

wmi.process.output.charset

適切な文字セットが設定されていない環境の日本語システムを修正します。 CA Configuration Automation サーバ UI で「ジャンク テキスト」メッセージを回避するには、このような環境でこの値を SJIS に設定します。

wmi.script.exec.timeout.sec

WMI ベースのディスカバリまたはリフレッシュ操作が応答する必要がある間隔を定義します。

デフォルト： 900

discovery プロパティ グループ

discovery プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

default.maximum.files

ディスカバリ プロセス中にインジケータを求めて検索されるファイルの最大数を指定します。 このプロパティを使用して、大きなファイル システムのコンピュータでディスカバリ速度を向上させることができます。

デフォルト： 50,000

default.maximum.registry

ディスカバリ プロセス中にインジケータを求めて検索されるレジストリ エントリの最大数を指定します。このプロパティを使用して、大量のレジストリ データがあるコンピュータでディスカバリ速度を向上させることができます。

デフォルト： 50,000

directive.netprobe.timeout.msec

ネットワーク プローブを使用して、エージェントレス ディスカバリの実行に使用可能な最大時間を指定します。

デフォルト： 2000

directive.rexec.timeout.sec

スクリプト出力の待機状態が無期限にならないようにするため、ブループリントのスクリプトのリモート実行を許可する最大時間を指定します。

デフォルト： 300

fileget.encodeing.detector.retries

構成ファイルにローカライズされたコンテンツが含まれる場合、ファイル コンテンツのエンコーディング検出の精度を向上させます。

構成ファイルにローカライズされたコンテンツが含まれる場合のファイル コンテンツのエンコーディング検出の精度が向上しました。

デフォルト： 3

manage.files.by.disc.option

Follow Symbolic からのコンポーネントの管理対象ファイルと、［ネットワーク ドライブを含める］管理プロファイルの検出を指定します。

デフォルト： true。

注: プロパティ値を false に設定すると、シンボリック リンクからの管理対象ファイルおよび［ネットワーク ドライブを含める］が検出されます。

parsing_error_log_size

パーサー エラー メッセージ テキストの長さを指定します。

デフォルト： 10000

platform.exclude.files.unix

UNIX および Linux サーバのディスカバリ中に無視するファイルのカンマ区切りリストを指定します。

platform.exclude.files.win32

Windows サーバのディスカバリ中に無視するファイルのカンマ区切りリストを指定します。

platform.exclude.unix

UNIX および Linux サーバのディスカバリ中に無視するディレクトリのカンマ区切りリストを指定します。

デフォルト：/cdrom、/boot、/dev、/proc、/tmp、/lost+found、/mnt、/devices./sys

platform.exclude.win32

Windows サーバのディスカバリ中に無視するディレクトリのカンマ区切りリストを指定します。

デフォルト : A:、?:/RECYCLER、?:/$Recycle.Bin、C:/Documents and Settings、C:/Users、 C:/ProgramData

server.reconcile

検出されたサーバの IP アドレスを調整するかどうかを指定します。

デフォルト： false

use.registry.cache

エージェントレス ディスカバリ（すなわち WMI、SSH、および Telnet）がキャッシュ内にレジストリ データを格納するかどうかを指定します。 ターゲット グリッド ノードまたは CCA サーバがインストールされているコンピュータの RAM のサイズが 2GB 以下の場合は、このプロパティを false に設定してください。

db プロパティ グループ

db プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

batch.update.timeout.retries

バッチ モードでタイムアウトが発生した場合、再試行回数を定義します。

デフォルト： 5 （最小値は 0）

batch.update.timeout.seconds

バッチモードでのデータの挿入、更新、または削除を続行する前に待機する時間（秒単位）を定義します。

デフォルト： 300 （最小値： 30、最大値 10800）

deadlock.retry.delay.ms

トランザクションを再試行する前に待機する時間（ミリ秒単位）を定義します。

デフォルト： 10000 （最小値： 1000、最大値： 300000）

jdbc.trace.level

データベース操作に関連する JDBC ログ記録を定義します。 有効な値は以下のとおりです。

Severe

深刻な障害を意味する、最も高いログ記録レベルです。 JDBC ドライバは、エラーおよび例外をレポートするためにこのレベルを使用します。

Warning

潜在的な問題を示します。

Info

情報メッセージを提供します。

Config

設定メッセージを提供します。 JDBC ドライバはこのレベルをグローバル設定に使用します。

Fine

基本的なトレース情報を提供します。 JDBC ドライバはこのレベルを、ほとんどのログ メッセージに使用します。

Finer

より詳細なトレース情報を提供します。

Finest

非常に詳細なトレース情報を提供します。Finest は最低のログ記録レベルです。

Off

ログ記録をオフにします。

All

すべてのメッセージのログ記録を有効にします。

max.batch.size

データベース操作中に各バッチで処理される行数を定義します。

デフォルト： 1000 （最小値： 100、最大値： 10000）

query.timeout.seconds

クエリ選択試行を続行するための間隔（秒単位）を定義します。

デフォルト： 300 （最小値： 30、最大値： 3600）

update.timeout.seconds

挿入、更新または削除の各試行を続行するための間隔（秒単位）を定義します。

デフォルト： 3600 （最小値： 30、最大値： 10800）

distributed lock プロパティ グループ

distributed lock プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

distributedlock.heartbeatExpirationInterval

CA サポートの指示があった場合にのみ変更してください。

デフォルト： 600

distributedlock.heartbeatRefreshInterval

CA サポートの指示があった場合にのみ変更してください。

デフォルト： 300000

distributedlock.retryInterval

CA サポートの指示があった場合にのみ変更してください。

デフォルト： 5000

distributedlock.garbageCollectionInterval

以下の操作実行中、プロセスが獲得する分散型ロックの最大クリーンアップ時間を指定します。

- ディスカバリ
- 変更の検出
- 比較
- ルール コンプライアンス操作

デフォルト： 300000

eem プロパティ グループ

eem プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

applicationInstance.name

CA EEM の内の CA Configuration Automation を識別します。

デフォルト： CCA

auth.enabled

CA EEM でユーザ認証が行われるかどうかを指定します。 このプロパティが false に設定された場合は、［ユーザ名］および［パスワード］フィールドに入力されたエントリはすべて有効です。

デフォルト： true

cca.admin.user

CA Configuration Automation 管理者ユーザを識別します。

デフォルト： ccaadminuser

client.auth.enabled

X.509 クライアント証明書認証が有効かどうかを指定します。

デフォルト： false

eventdeliveryhost

イベントの送信元ホストを指定します。

host

EEM サーバのホスト名。

grid プロパティ グループ

grid プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

ftp.account

FTP サーバへの接続で使われるユーザ名を定義します。 Telnet ディスカバリ操作に対して、FTP プロパティが使われます。 グリッド サーバごとに FTP アカウントを構成して、アカウントがホスト名だけでサーバを識別できるようにします。 ドメイン（darkstar.ca.com など）または IP アドレスを伴うホスト名を使用しないでください。

ftp.password

ftp.account ユーザに関連付けるパスワードを定義します。

ftp.port

FTP サーバ リスニング ポートを定義します。

デフォルト： 21

ftp.root

FTP サーバのルート ディレクトリ（つまり、FTP ホーム ディレクトリ）を定義します。

heartbeat.expiration.interval

グリッド ノードのハートビートが有効と見なされる間隔（秒単位）を定義します。グリッド ノードがデータベース内のハートビートを更新した場合、ハートビートの有効期間も、現在の時刻に heartbeat.expiration.interval の値を加算した値に更新されます。 グリッド ノードが有効期限までにハートビートを更新しなかった場合、グリッド ノードは使用不可状態か停止状態と見なされます。

デフォルト： 300

heartbeat.refresh.interval

他のグリッド サーバからデータを取得するまでの間隔（分単位）を定義します。各グリッド ノードは、データベース内のハートビート行を一定の間隔で更新します。 一定のハートビート更新は、このノードが実行されていることを他のグリッド ノードに示します。たとえば、コンピュータの電源をオフにすると、最終的にハートビートは期限切れになります。ハートビートが期限切れになると、他のグリッド ノードは、期限切れになったグリッド ノードが動作しなくなったと想定します。

デフォルト： 60

history.retention.days

データベース内のグリッド サーバに関するイベント情報とジョブ情報を、レポート目的で維持する期間（日単位）を定義します。

デフォルト： 14

job.resubmit.delay.ms

ジョブを再サブミットする前に、未処理のグリッド ジョブを遅らせる間隔（ミリ秒単位）を定義します。

デフォルト： 5000

max.jobs.master

マスタ グリッド サーバが同時に実行できるジョブの最大数を定義します。他の UI アクティビティ用にリソースを保存するため、デフォルトではこの値に対し、グリッド ノードに対する値よりも小さい値が設定されています。

デフォルト： 10

max.jobs.slaves

スレーブ グリッド サーバが同時に実行できるジョブの最大数を定義します。 この値が小さくしすぎると、スケール効率が低下します。この値を大きくしすぎると、リソースを使い果たしてしまい、メモリ不足例外が発生する可能性があります。

デフォルト： 20

rpc.connect.timeout.seconds

CA Technologies 内部使用専用。

デフォルト： 15

rpc.reply.timeout.seconds

CA Technologies 内部使用専用。

デフォルト： 0

stess.multiplier

CA Technologies 内部使用専用。

デフォルト： 3

system.wide.max.jobs

すべてのグリッド サーバが同時に実行できるジョブの総数を指定します。この値を高く設定しすぎると、サポート可能な最大接続数など、データベース リソースを消耗する可能性があります。

デフォルト： 100

tcp.base.port

グリッド間の通信の初期ポートを定義します。 単一のコンピュータに、単一の UI サーバと任意の数のグリッド ノードをインストールできます。 これらの各サーバは起動時、グリッド間通信用ソケットを作成します。

デフォルト： 8065

tcp.port.range

グリッド間通信に使用できる、tcp.base.port から始まる連続ポートの範囲を定義します。 tcp.base.port から tcp.base.port および tcp.port.range までのすべてのポートは、ファイアウォールに対してオープンにする必要があります。

デフォルト： 15

ndg プロパティ グループ

ndg プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

chunk.enabled

NDG がデータ チャンクを定期的にインポートするか、またはスキャンによるデータ インポートの完了まで待機するかを指定します。

デフォルト： true

chunk.interval

データ チャンクをインポートする前に待機する秒数を指定します。

デフォルト： 30

comm.attributes.prune.interval

パケット分析スキャンによって収集された古い通信関係の属性を削除する前に待機する日数を指定します。

デフォルト： 30

comm.relationships.prune.interval

以下の操作によって収集された古い通信関係を廃棄する前に待機する日数を指定します。

- Softagent ネットワーク接続処理
- パケット分析スキャン
- Netflow スキャン
- パケット分析スキャンおよび Netflow スキャンのトラフィック サマリ データ

デフォルト： 92

default.port

NDG Web サービスの呼び出しに使用するポート指定します。

デフォルト： 8081

ignore_server_with_duplicate_ip

この値が true に設定されていると、CCA データベース内にすでに存在するサーバと競合する IP を持つサーバが検出された場合に、ネットワーク ディスカバリによって新しいサーバ エントリが作成されないように指定されます。

デフォルト： false

注: 重複した IP を検出した場合には、ネットワーク ディスカバリ処理が警告メッセージをログに記録します。

reconcile_ip.use_tcp_connect_scan

［TCP 接続スキャン」を［IP の調整］操作を実行するかどうかを指定します。 このプロパティが false に設定された場合、［ping スイープ］が使用されます。

デフォルト： false

scheduler プロパティ グループ

scheduler プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

InstanceId

ジョブ インスタンス ID 番号を指定します。

デフォルト： AUTO

instanceName

ジョブ インスタンス名を指定します。

デフォルト： ACMScheduler

scheduler.rmi プロパティ グループ

scheduler.rmi プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

registryPort

Remote Method Invocation（RMI）ポートを指定します。

デフォルト： 1099

scheduler.threadPool プロパティ グループ

scheduler.threadPool プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

threadcount

スケジュールされたジョブ当たりのスレッド数を指定します。

デフォルト： 100

threadPriority

スレッドの優先度を指定します。

デフォルト： 4

sdk プロパティ グループ

sdk プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

sdk.enabled

SDK クライアントが CA Configuration Automation サーバ にアクセスできるかどうかを指定します。

デフォルト： true

sdk.session.cache.idle.time

SDK リクエストが完了した後に SDK 認証キャッシュ エントリが削除されるまでの間隔を分数で指定します。

デフォルト： 10

sdk.session.cache.size

SDK 認証キャッシュ内のエントリの最大数を指定します。

デフォルト： 100

snmp プロパティ グループ

snmp プロパティ グループには、［プロパティ］テーブルから編集できる以下のプロパティが含まれます。

default.communitystring

SNMP コミュニティ文字列を指定します。

デフォルト： public

default.retries

SNMP 再試行回数を指定します。

デフォルト： 3

default.timeout

SNMP 送信タイムアウトを指定します。

デフォルト： 5000

ping.timeout

SNMP ping タイムアウトを指定します。

100

プロパティのインポート

別の CA Configuration Automation インスタンスから Java Archive（JAR）ファイルとして設定プロパティをインポートできます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブをクリックします。
2. ［構成］タブで、［プロパティ］リンクをクリックします。
3. ［プロパティ］ページで、［テーブル アクション］をクリックし、［プロパティのインポート］を選択します。

4. ［プロパティのインポート］ダイアログ ボックスで、以下のフィールドに入力します。

   インポートする JAR ファイル

   インポートするプロパティが含まれている JAR ファイルの名前を定義します。［参照］をクリックしてファイルを選択できます。

   既存のプロパティを上書き

   同じ名前のファイルに上書きするかどうかを指定します。別の CA Configuration Automation インスタンスにプロファイルを保持するには、このオプションを選択します。

5. 以下のいずれかのボタンをクリックします。

   すべてをインポート

   JAR ファイル内のすべてのプロパティをインポートします。

   選択内容をインポート

   JAR ファイルからインポートするプロパティを選択するためのダイアログ ボックスが表示されます。

   ファイルがインポートされ、［プロパティ］テーブルにプロパティが表示されます。

セキュリティ証明書の作成および管理

セキュリティ証明書を使用して、CA Configuration Automation サーバ と CA Configuration Automation エージェント間での通信用の SSL ベースのセキュリティを実装し、CA Configuration Automation ユーザ インターフェースのアクセスを保護します。

CA Configuration Automation サーバ から CCA エージェントへの通信の保護

CA Configuration Automation サーバ と CA Configuration Automation エージェントの間には、以下の 2 つの通信チャネルがあります。

- CA Configuration Automation エージェントから開始された通信
- CA Configuration Automation サーバ から開始された通信

エージェントから開始され通信のみが、CA Configuration Automation サーバにエージェントを自動登録できる通信であり、基本的なエージェント構成およびサーバ情報をサーバに定期的に送信する通信です。 この機能はオプションであり、CA Configuration Automation の正常な操作に必須ではありません。 セキュア モードは、エージェントからサーバへの通信には提供されません。セキュリティが求められる環境では、[サーバ ping]オプションを無効にすることができます。

サーバとエージェントの間の他のすべての通信（ディスカバリ操作およびリフレッシュ操作を含む）は、サーバから開始されます。 これらの通信を保護することで、管理対象サーバと CA Configuration Automation サーバの間で交換されるデータが暗号化によって保護され、エージェントへの不正アクセスが認証によって防止されます。 セキュリティ暗号化スイートは、RSA キー交換、128 ビット キーの RC4 ストリーム暗号、および TLS v1 での MD5 ダイジェストを使用します。

CA Configuration Automation UI アクセスの保護

CA Configuration Automation Web ベース UI は、HTTP 経由で提供されます。HTTPS を使用して UI アクセスを保護することができます。HTTPS は、HTTP クライアントと HTTP サーバの間の Secure Socket Layer（SSL）暗号化および認証を提供します。

CA Configuration Automation サーバ UI へのアクセスを保護した後、ユーザは HTTP ではなく HTTPS を使用して CA Configuration Automation サーバ にログインする必要があります（たとえば、https://*<CCA_Server_Name>:<port_number>*/cca/CCAUI.html）。

SSL セキュリティ用に CA Configuration Automation を設定する方法

このセクションでは、SSL セキュリティを使用するように CA Configuration Automation を設定する方法について説明します。 以下プロセスでは、完了する必要のあるステップをすべてリスト表示します。

1. 認証局の作成 (P. 64)
2. サーバ証明書の作成 (P. 64)
3. HTTPS の有効化 (P. 68)
4. CA Configuration Automation エージェントの保護

認証局、サーバ証明書、および HTTPS 証明書の作成

CA Configuration Automation の認証局は、CA Configuration Automation サーバ および CA Configuration Automation エージェントの証明書を作成するために使用されます。 パスワードは、認証局を保護し、認証局を設定した場合および新しい証明書が署名された場合に必要とされます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブで［セキュリティ証明書］をクリックします。

   ［セキュリティのサマリ］ページが開き、以下のセキュリティ コンポーネントのステータスが表示されます。

   認証局

   認証局がすでに作成されているかどうかを指定します。

   HTTPS サポート

   CA Configuration Automation サーバ UI に対して HTTPS が有効かどうかを指定します。

エージェント セキュリティ

CA Configuration Automation エージェントに対して SSL セキュリティが有効かどうかを指定します。

クライアント認証

CCA サーバに対してクライアント認証を有効にするかどうかを指定します。

2. ［テーブル アクション］ドロップダウン リストから［認証局の作成］を選択します。

［認証局の作成］ダイアログ ボックスが表示されます。

3. ［認証局の作成］ダイアログ ボックスで、以下のフィールドに入力し、［OK］をクリックします。

認証局パスワード

証明書のパスワードを定義します。 このパスワードはシステム セキュリティの鍵です。 セキュリティのベスト プラクティスに従ってパスワードを選択します。同じパスワードを HTTPS 証明書などの他の証明書には使用しないでください。

パスワードの確認

この値に一致させることにより、認証局のパスワードが正しく入力されたことを確認します。

サーバ証明書パスワード

サーバ証明書パスワードを指定します。

パスワードの確認

この値に一致させることにより、サーバ証明書のパスワードが正しく入力されたことを確認します。

HTTPS のセットアップ

CA Configuration Automation UI へのアクセスに対して HTTPS が有効かどうかを指定します。 X.509 証明書の認証では、HTTPS が有効である必要があります。

HTTPS 証明書パスワード

HTTPS 証明書パスワードを指定します。

パスワードの確認

この値に一致させることにより、HTTPS 証明書のパスワードが正しく入力されたことを確認します。

アプリケーションは以下のアクションを実行します。

- 自己署名付きのプライベート認証局およびパブリック認証局の証明書の作成
- CA Configuration Automation サーバ 証明書の作成および署名
- セキュリティ関連のすべてのディレクトリおよびファイルのセットアップ
- CA Configuration Automation サーバ のキー ストアおよび信頼ストアの作成
- ［HTTPS のセットアップ］チェック ボックスが選択された場合、HTTPS 証明書が作成され、以下のアクションが実行される必要があります。
  - CA Configuration Automation UI へのアクセスの保護
  - X.509 証明書認証の有効化
- 必要に応じて server.xml ファイル内のコネクタ エントリの変更

以下のディレクトリには、CA Configuration Automation 認証局の証明書、発行された証明書のデータベース、および発行されたすべての鍵と証明書のコピーが含まれます。

- **UNIX および Linux**： /opt/CA/CCAServer/security
- **Windows**： ¥Program Files¥CA¥CCA Server¥security

4. CA Configuration Automation サーバ を停止し、再起動します。
5. （オプション）CA Configuration Automation エージェントのセキュリティ証明書を作成および有効化します（「エージェントの保護」に従って必要とされる場合）。

   それぞれの CCA エージェントで、個別の証明書がサーバごとに発行される必要があります。［サーバ］ページで選択した個別のサーバごとに、［エージェントの保護］オプションを使用して CA Configuration Automation エージェントのセキュリティ証明書を作成します。

セキュリティ証明書の作成

CA Configuration Automation を使用すると、x509 セキュリティ証明書を作成できます。x509 セキュリティ証明書を使用すると、以下の間の通信を保護できます。

- CA Configuration Automation サーバ および CA Configuration Automation エージェント
- クライアント（ブラウザ）と CCA サーバ

セキュリティ証明書を作成する方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

   注: ［証明書］テーブルにエントリがない場合、サーバ証明書を作成することはできません。

2. ［テーブル アクション］ドロップダウン リストから［証明書の作成］を選択します。

   ［証明書の作成］ダイアログ ボックスが表示されます。

3. 対応するフィールドに以下の情報を入力し、［OK］をクリックします。

   サーバ

   保護される CA Configuration Automation サーバ を指定します。

   証明書の目的

   以下のいずれかの通信タイプを保護するために使用されている証明書を指定します。

   - CA Configuration Automation エージェント -- CA Configuration Automation エージェントで開始される通信を保護します。
   - CA Configuration Automation サーバ -- CA Configuration Automation サーバ で開始される通信を保護します。
   - クライアント認証 -- クライアント（ユーザのブラウザ）と CA Configuration Automation サーバ の間の通信を保護します。X.509 証明書認証にはこのオプションを使用します。

- HTTPS -- HTTPS 対応の CA Configuration Automation サーバ で開始される通信を保護します。
- Network Discovery Gateway -- グリッド ノードと NDG 間の通信を保護します。

有効期限 (日数)

この証明書が有効な期間を日数で指定します。

証明書パスワード

このセキュリティ証明書に関連付けられたパスワードを指定します。

パスワードの確認

パスワードを正しく入力したことを確認します。入力したパスワードは、このエントリと一致する必要があります。

認証局パスワード

認証局を作成したときに入力されたパスワードを指定します。

証明書が作成され、［証明書］テーブルに表示されます。

HTTPS の有効化

認証局を作成した後に HTTPS を有効にしなかった場合、手動で HTTPS を有効にして、HTTPS 証明書を作成し、CA Configuration Automation ユーザ インターフェースへのアクセスを保護することができます。

HTTPS を有効にする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［セキュリティのサマリ］パネルを調べて、［認証局］フィールドが［作成済み］、［HTTPS サポート］フィールドが［無効］になっていることを確認します。

3. ［テーブル アクション］ドロップダウン リストから［HTTPS の有効化］を選択します。

   HTTPS 証明書の作成を求めるプロンプトが表示されます。

4. ［OK］をクリックします。

   以下のフィールドが入力された状態で、［HTTPS 証明書の作成］ダイアログ ボックスが表示されます。

   サーバ

   CA Configuration Automation サーバ ホストを指定します。

   証明書の目的

   HTTPS を指定します。

5. 対応するフィールドに以下の情報を入力し、［OK］をクリックします。

   有効期限 (日数)

   HTTPS 証明書の有効期間を指定します。
   デフォルト： 3650

   証明書パスワード

   HTTPS 証明書のパスワードを指定します。

   パスワードの確認

   パスワードを正しく入力したことを確認します。入力したパスワードは、このエントリと一致する必要があります。

   認証局パスワード

   認証局パスワードを指定します。

   HTTPS 証明書が［証明書］テーブルに追加されます。

6. HTTPS 証明書の横にあるチェック ボックスをオンにし、［テーブル アクション］ドロップダウン リストから［HTTPS の有効化］を選択します。

   ［HTTPS の有効化］ダイアログ ボックスが表示されます。

7. 認証局パスワードを入力し、［OK］をクリックします。

   ［HTTPS サポート］フィールド（［セキュリティのサマリ］パネル）が［有効化されました (サーバの再起動が必要)］と表示されます。

8. CA Configuration Automation サーバ を停止し、再起動します。

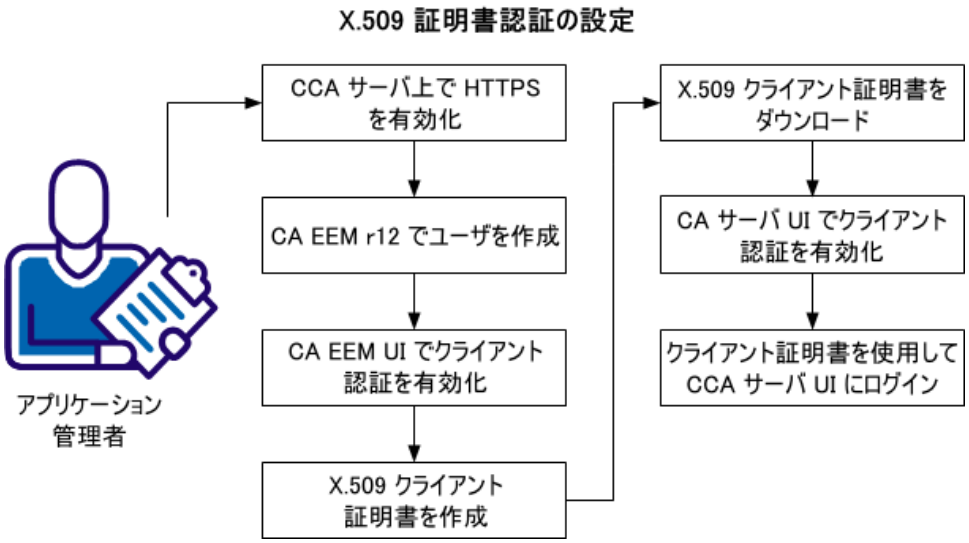
   HTTPS が有効な状態で、HTTP ではなく HTTPS を使用して CA Configuration Automation にログインする必要があります。たとえば、以下のように HTTPS を使用します。

   `https://<CCA_Server_Name>:<port_number>`

X.509 証明書認証の設定

アプリケーション管理者は、X.509 クライアント証明書を持ったユーザのみが CA Configuration Automation サーバ UI にログインできるように CA Configuration Automation を設定することができます。

以下は、X.509 証明書認証の設定に関係するタスクを示しています。



アプリケーション管理者は、X.509 証明書認証を設定するために以下のタスクを実行できます。

1. CA Configuration Automation サーバ 上で HTTPS を有効 (P. 64)にします。
2. CA EEM r12 にユーザを作成 (P. 71) します。
3. CA EEM UI でクライアント認証を有効 (P. 74)にします。
4. X.509 クライアント証明書を作成 (P. 67) します。
5. X.509 クライアント証明書をダウンロード (P. 76) します。
6. CA Configuration Automation サーバ UI でクライアント認証を有効 (P. 75)にします。
7. クライアント証明書を使用して CA Configuration Automation にログイン (P. 77) します。

CA EEM の CA Configuration Automation ユーザの作成

CA EEM をインストールおよび統合したら、既存の CA EEM ユーザを CA Configuration Automation に読み込むか、または新規ユーザを作成できます。

ユーザを追加する前に CA Configuration Automation で定義されている唯一のユーザは、CA Configuration Automation のインストール中に作成されたスーパーユーザです。 このスーパーユーザは、すべての CA Configuration Automation 機能に対する権限を持っています。スーパーユーザは、CA EEM への接続性が失われた場合に、ユーザ アクセスを設定して製品にアクセスするための初回ログイン用に設計されています。少なくとも 1 人のユーザがすべての機能にアクセス権があることを確認します。 このユーザの権限を制限するには、製品を管理するための別の管理者ユーザを作成して使用する必要があります。

ユーザを作成して内部データベースに格納したり、外部ディレクトリ（Active Directory など）からユーザをインポートしたりすることもできます。

注: CA Configuration Automation と CA EEM の統合では、CA Configuration Automation の［環境管理］パネルから CA EEM UI を開始できます。ただし、CA EEM にアクセスするためにユーザ アカウントおよびパスワードが必要となります。

次の手順に従ってください:

1. CA Configuration Automation を開き、［環境管理］リンクをクリックし、［アクセス管理］タブをクリックします。
2. ［ユーザ］ページで、［ユーザ］領域（左下）の cca_users フォルダ アイコンのすぐ左にある［新規ユーザ］アイコンをクリックします。

   CA EEM の［新規ユーザ］ページが CA Configuration Automation のコンテキストで表示されます。

3. ［名前］フィールドに名前を入力します。

   制限： 100 英数文字

4. ［アプリケーション ユーザの詳細の追加］をクリックし、以下の情報を入力します。

   アプリケーション インスタンス名

   このユーザ アカウントがアクセスできる CA Configuration Automation インスタンスを定義します。

   アプリケーション グループ メンバシップ

   このユーザがメンバとして所属するアプリケーション固有のグループ（複数可）を定義します。

5. ユーザに関する適切な詳細を［全般］領域に入力します。

6. ［使用可能なグローバル ユーザ グループ］列のグループをダブルクリックして、既存のグローバル ユーザ グループ（複数可）にユーザを追加します。

   ［選択されたグローバル ユーザ グループ］列に選択したグループが表示されます。

   注: 特定のユーザ グループを見つけるには、必要に応じて［属性］、［演算子］、［値］フィールドに入力し、［検索］をクリックします。

7. ［認証］領域の以下のフィールドに入力します。

   不正なログイン カウント

   ユーザが試行したログインが連続して失敗した回数を示します。この値は、ログインに成功するとゼロにリセットされます。

   再開日

   ユーザ アカウントを有効にする日付を定義します。 日時を選択するには、カレンダ アイコンをクリックします。ユーザは［再開日］の前、または［停止日］の後にログインすることはできません。

   停止日

   ユーザ アカウントが無効になった日付を定義します。 日時を選択するには、カレンダ アイコンをクリックします。 有効期限を指定しない場合は、このフィールドを空白のままにします。 ユーザは［再開日］の前、または［停止日］の後にログインすることはできません。

パスワード ポリシーを上書き

パスワード ポリシーに適合しないパスワードを持つことをユーザに許可するかどうかを指定します。

次のログイン時にパスワードを変更

管理者によって割り当てられたパスワードで初めてログインした後に、ユーザがパスワードを変更する必要があるかどうかを指定します。

一時停止

ユーザ アカウントを手動で非アクティブにするかどうかを指定します。

新しいパスワード

管理者によって割り当てられたユーザのパスワードを定義します。［次のログイン時にパスワードを変更］オプションを選択した場合、ユーザが CA Configuration Automation に最初にログインした後、このパスワードを変更するよう要求されます。

パスワードの確認

エントリが一致することを要求することにより、パスワードに間違いが含まれていないことを確認します。

8. ［保存］をクリックします。

次のメッセージが表示されます。

確認： グローバル ユーザが正常に作成されました。

手順 4 でアプリケーション固有の詳細を指定した場合、メッセージに以下の行も含まれます。

（グローバル ユーザの詳細が正常に作成されました。アプリケーション ユーザの詳細が正常に作成されました。）」という確認メッセージが表示されます。

9. ユーザごとに、この手順を繰り返します。

CA EEM でのクライアント認証の有効化

CA Configuration Automation のクライアント認証では、CA EEM でクライアント認証（証明書の検証）を有効にする必要があります。

次の手順に従ってください:

1. お使いの CCA サーバから %CCA _installation%¥lib¥“tomcat.keystore” を以下の EEM サーバの場所にコピーします。

   ```
   %EmbeddedEntitlementsManager%¥ca
   ```

2. CA EEM にログインし、［設定］タブ、［EEM サーバ］リンクをクリックし、左ペインで［証明書の検証］リンクをクリックします。

   右側のペインに［証明書の検証］ページが表示されます。

3. ［証明書検証の有効化］オプションを選択し、以下のフィールドに入力します。

   キーストア ファイルの場所

   EEM サーバ上のキーストア ファイルの場所を定義します。

   Keystore Password

   認証局を作成する場合に使用するパスワードを定義します。

4. ［ユーザ マッピング フィールド］ドロップダウン リストから［件名］を選択します。

5. 証明書からユーザ名を取得するには、[ユーザ名抽出パターン]フィールドに以下のパターンを指定します。

   ```
   CN=([^,]*)
   ```

6. 各クライアント証明書に一致するユーザを作成します。 ユーザ名は、クライアント証明書を作成したときに使用されたユーザ名と同じである必要があります。

7. EEM サーバを停止して、再起動します。

   クライアント認証が EEM サーバで有効になりました。

CA Configuration Automation でのクライアント認証の有効化

クライアント認証を有効にして、クライアント（ブラウザ）と CA Configuration Automation サーバの間の通信を保護できます。

注: クライアント認証を有効にしたら、ユーザはクライアント証明書を使用してのみログインできます。 ユーザ名とパスワードを使用してログインすることはできなくなります。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブで［セキュリティ証明書］をクリックします。
2. ［セキュリティ証明書］ページで、［セキュリティのサマリ］パネルを確認します。

   ［認証局］の値が［作成済み］、［HTTPS サポート］の値が［有効］である必要があります。
3. ［テーブル アクション］ドロップダウン リストから、［クライアント認証の有効化］を選択します。
4. ［OK］をクリックし、クライアント証明書のみがログインに使用できるという通知を閉じます。
5. ［クライアント認証の有効化］ダイアログ ボックスで、以下のフィールドに入力し、［OK］をクリックします。

   EEM 管理者ユーザ名

   CA EEM 管理者のユーザ名を定義します。

   EEM 管理者パスワード

   指定した CA EEM 管理者に関連付けるパスワードを定義します。

   認証局パスワード

   認証局を作成するために使用されるパスワードを定義します。

   ［セキュリティのサマリ］パネルの［クライアント認証サポート］フィールドに［有効］が表示されます（サーバの再起動が必要）。
6. クライアント証明書をダウンロードし、CCA サーバを停止して再起動します。

   クライアント認証が有効化されました。

クライアント証明書のダウンロード

クライアント(ユーザのブラウザ)と CA Configuration Automation サーバ の間の通信に使用するクライアント証明書ファイルをダウンロードできます。

次の手順に従ってください:

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. 証明書のなかで、［目的］列に［クライアント認証］が設定されているもののチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［クライアント証明書のダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。証明書ファイルは次の形式を使用して名前が割り当てられます：<certificateName>.cer。 この名前は以下の手順で編集できます。

3. ［保存］をクリックしてから、証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所にクライアント証明書ファイルがコピーされます。

クライアント証明書を使用した CA Configuration Automation へのログイン

設定手順が完了したら、ユーザはクライアント証明書を使用した場合のみ CA Configuration Automation にログインできます。

次の手順に従ってください:

1. クライアント証明書を Internet Explorer にインポートします。
   a. ［ツール］-［インターネット オプション］の順に選択します。
   b. ［インターネット オプション］ダイアログ ボックスで、［コンテンツ］タブをクリックし、［証明書］をクリックします。

      ［証明書］ダイアログ ボックスが開きます。
   c. ［インポート］をクリックします。
   d. ［証明書のインポート ウィザード］での指示に従います。

      インポートが完了したら、［証明書］ダイアログ ボックスの［個人］タブに証明書が含まれます。
2. CA Configuration Automation にログインするには、以下の URL を入力します。

   `https://<CCA_Server_Name>:<port_number>/cca/CCAUI.html`

   ブラウザに複数の証明書が存在する場合、［デジタル証明書の選択］ダイアログ ボックスが表示されます。
3. ユーザの［発行者］列にリスト表示された CCA クライアント証明書を選択し、［OK］をクリックします。

   CA Configuration Automation サーバ UI が開きます。

CA Configuration Automation 証明書認証用の CA EEM 構成オプション

このセクションでは、CA Configuration Automation 証明書認証で使用できる CA EEM 構成オプションについて説明します。

証明書の無効化

CA EEM で証明書を無効にすると、その証明書を使用するユーザは CA Configuration Automation サーバにログインできなくなります。 無効にするメカニズムの設定については、CA EEM のドキュメントを参照してください。

CA EEM SDK クライアントでのデバッグ ログの有効化

デフォルトでは、eiam.javasdk.log ファイルは %CCAServer_INSTALLED_DIR%¥logs ディレクトリにインストールされます。 デフォルト ログ ファイル レベルは「エラー」に設定されています。このログ レベルを「デバッグ」に設定できます。

次の手順に従ってください:

1. ¥%CCAServer_ INSTALLED _DIR%¥tomcat¥conf ディレクトリにある eiam.log4j.config ログ設定ファイルをテキスト エディタで開きます。
2. ログ レベルを debug に設定します。

```
<root>
    <priority value="debug" />
    <appender-ref ref="SDK" />
    <!-- <appender-ref ref="Console" /> -->
</root>
```

3. CCA サーバを停止して、再起動します。

CA EEM での証明書検証デバッグ ログの有効化

デフォルトでは、certvalidation.log ファイルは、%SC%¥EmbeddedEntitlementsManager¥logs ディレクトリにインストールされます。 デフォルト ログ ファイル レベルは「情報」に設定されています。 このログ レベルを「デバッグ」に設定できます。

次の手順に従ってください:

1. %SC% ¥EmbeddedEntitlementsManager¥config¥logger ディレクトリにある Server.java ログ設定ファイルをテキスト エディタで開きます。
2. ログ レベルを debug に設定します。

```
<logger name="com.ca.eiam.server.certvalidation" additivity="false">

    <level value="debug"/>

    <appender-ref ref="certvalidation"/>

</logger>
```

3. EEM サーバを停止して、再起動します。

CA Configuration Automation セキュリティ設定および証明書の表示

［セキュリティのサマリ］テーブルおよび［証明書］テーブルでは、既存のセキュリティ構成を表示し、必要に応じて既存のセキュリティ証明書を編集できます。

セキュリティの設定および証明書を表示する方法

［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

［セキュリティ証明書］ページが開き、［セキュリティのサマリ］テーブルに以下のセキュリティの設定が表示されます。

認証局

認証局がすでに作成されているかどうかを指定します。

HTTPS サポート

CA Configuration Automation サーバ に対して HTTPS が有効かどうかを指定します。 このエントリは、CA Configuration Automation サーバ を再起動する必要があるかどうかも示します。

エージェント セキュリティ

エージェント セキュリティが有効かどうかを指定します。このエントリは、CA Configuration Automation サーバ および各グリッド ノードを再起動する必要があるかどうかも示します。

既存の証明書が［証明書］テーブルに表示されます。

証明書の削除

不要になった証明書を CA Configuration Automation データベース から削除できます。

セキュリティ証明書を削除する方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. 証明書 (複数可) の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［証明書の削除］を選択します。

   ［証明書の削除］ダイアログ ボックスで証明書パスワードの入力を求められます。

3. パスワードを入力し、［OK］をクリックします。

   証明書が削除されます。

認証局の破棄

HTTPS モードでサーバを使用しなくなった場合、CA Configuration Automation サーバ を保護している認証局を破棄できます。

認証局を削除する方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルの上にある［セキュリティのサマリ］に［認証局: 作成済み］と表示されます。

2. モードを変更するサーバの認証局の横にあるチェック ボックスをオンにし、［テーブル アクション］ドロップダウン リストから［認証局の破棄］を選択します。

   認証局が破棄されます。

3. CA Configuration Automation サーバ を停止し、再起動します。

   サーバは HTTPS モードで作動しなくなります。

エージェント キーのダウンロード

CA Configuration Automation エージェントを保護する証明書ファイルをダウンロードできます。

エージェント キーをダウンロードする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［目的］列が CA Configuration Automation エージェントに設定されている証明書の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［エージェント キーのダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. 証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所にファイルがコピーされます。デフォルトでは、ファイル名は以下の形式になります。

   *<server_name.domain_name>*_agent.cer

サーバ証明書のダウンロード

CA Configuration Automation サーバ を保護する証明書ファイルをダウンロードできます。

サーバ証明書をダウンロードする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［目的］列が CA Configuration Automation エージェントに設定されている証明書の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［サーバ証明書のダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. 証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所に ccaca.cer ファイルがコピーされます。

サーバ Keystore のダウンロード

サーバ Keystore 証明書ファイルをダウンロードできます。

サーバ Keystore をダウンロードする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［目的］列が CA Configuration Automation サーバ に設定されているする証明書の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［サーバ Keystore のダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. 証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所にサーバ Keystore ファイルがコピーされます。

サーバ Truststore のダウンロード

サーバ Truststore 証明書ファイルをダウンロードできます。

サーバ Truststore をダウンロードする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［目的］列が CA Configuration Automation サーバ に設定されているする証明書の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［サーバ Truststore のダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. 証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所にサーバ Truststore ファイルがコピーされます。

HTTPS Keystore のダウンロード

HTTPS Keystore ファイルをダウンロードできます。

HTTPS Keystore をダウンロードする方法

1. ［環境管理］-［構成］-［セキュリティ証明書］をクリックします。

   ［セキュリティ証明書］ページが開き、［証明書］テーブルに既存の証明書が表示されます。

2. ［目的］列が HTTPS に設定されているする証明書の横にあるチェックボックスをオンにし、［アクションの選択］ドロップダウン リストから［HTTPS Keystore のダウンロード］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. 証明書ファイルを保存する場所にナビゲートし、［保存］をクリックします。

   指定した場所に HTTPS Keystore ファイルがコピーされます。

通信マッピングの操作

［通信マッピング］ページには、環境内のポートとアプリケーションのマッピングを示すテーブルが含まれます。 これらのマッピングは、「関係詳細の表示」に記載のとおり、［サーバ詳細］の［関係］ページで使用されます。

以下の手順は、 CA Configuration Automation が 2 つのポート（サーバ 1 のポートと（サーバ 2 のポート）間のマッピングに従って、使用するポートを決定する方法を示しています。

- ［通信マッピング］テーブルにデスティネーション ポート（サーバ 2）に対応するエントリがある場合、そのエントリによって通信が識別されます。
- そのエントリがないときは、［通信マッピング］テーブルにソース ポート（サーバ 1）に対応するエントリがある場合、そのエントリによって通信が識別されます。
- ［通信マッピング］テーブルにどちらのポートにも対応するエントリがない場合、通信は［関係の表示］ページで［不明］としてラベル付けされます。

通信マッピングの表示および編集

［通信マッピング］ページを使用して、現在のポート割り当てを表示または編集することができます。

CA Configuration Automation マッピングを表示および編集する方法

1. ［環境管理］-［構成］-［通信マッピング］をクリックします。

   ［通信マッピング］ページが開き、現在のマッピングがポート番号の数字順でテーブルに表示されます。

2. 編集する［通信タイプ］列の値をクリックします。

   編集可能なテキスト フィールドが表示されます。

3. 値を編集し、Enter キーを押します。

   新しいプロパティ値が適切な構成ファイルに保存されます。

通信マッピングの作成

新しいマッピングを作成し、それらのマッピングを［通信マッピング］ページから管理できます。

新しいマッピングを作成する方法

1. ［環境管理］-［構成］-［通信マッピング］をクリックします。

   ［通信マッピング］ページが開き、現在のマッピングがポート番号の数字順でテーブルに表示されます。

2. ［テーブル アクション］ドロップダウン リストから［通信マッピングの作成］を選択します。

   ［通信マッピングの作成］ページが表示されます。

3. 以下のフィールドに適切な情報を入力し、［保存］をクリックします。

   ポート

   CA Configuration Automation が通信しているポート番号を指定します。

   プロトコル

   プロトコル タイプ（TCP または UDP のいずれか）を指定します。

   通信名

   通信用のポートを使用するプログラムまたはコンポーネントを表します。

   マッピングが正常に作成されたことを確認するメッセージが表示され、マッピングが［通信マッピング］テーブルに表示されます。

通信マッピングの削除

不要になったマッピングを削除できます。

通信マッピングを削除する方法

1. ［環境管理］-［構成］-［通信マッピング］をクリックします。

   ［通信マッピング］ページが開き、現在のマッピングがポート番号の数字順でテーブルに表示されます。

2. 削除するマッピングの横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［通信マッピングの削除］を選択します。

   選択したマッピングの削除の確認を求めるプロンプトが表示されます。

3. ［OK］をクリックします。

   選択したマッピングが削除されたことを示す確認メッセージが表示されます。

アプリケーション マッピングの操作

［アプリケーション マッピング］ページには、事前定義済みおよびユーザ定義のアプリケーション マッピングをリスト表示するテーブルが含まれます。

［アプリケーション マッピング］は、アプリケーション名、およびアプリケーションのインストール場所を示す正規表現パスで構成されます。その後、これらのマッピングは、実行可能ファイルのインストール パスが（たとえば Netstat 関係などで）利用可能な場合、通信関係およびビジュアル グラフでアプリケーション名を照会および解決するために使用されます。関係の詳細については、「関係詳細の表示」を参照してください。

アプリケーション マッピングの表示および編集

［アプリケーション マッピング］ページを使用して、関連付けられたアプリケーションの場所を定義する正規表現値を表示および編集することができます。

アプリケーション マッピングを表示および編集する方法

1. ［環境管理］-［構成］-［アプリケーション マッピング］をクリックします。

   ［アプリケーション マッピング］ページが開き、現在のマッピングがアプリケーションのベンダーまたは発行元のアルファベット順でテーブルに表示されます。

2. 編集する［アプリケーション パス］列の値をクリックします。

   編集可能なテキスト フィールドが表示されます。

3. 新しい値を編集し、Enter キーを押します。

   テーブルが新しい値で更新されます。

アプリケーション マッピングの作成

CA Configuration Automation で事前定義されていないアプリケーションの新しいマッピングを作成できます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブで［アプリケーション マッピング］リンクをクリックします。

   ［アプリケーション マッピング］ページが開き、現在のマッピングがアプリケーションのベンダーまたは発行元のアルファベット順で表示されます。

2. ［テーブル アクション］ドロップダウン リストから、［アプリケーション マッピンの作成］を選択します。

3. ［アプリケーション マッピンの作成］ダイアログ ボックスの以下のフィールドに入力し、［保存］をクリックします。

   アプリケーション名

   アプリケーションの名前を定義します。

   デフォルトでは、事前定義済みマッピングの形式は <*アプリケーション ベンダー*> <*アプリケーション名*> になります（たとえば Microsoft Internet Explorer）。

   アプリケーション パス

   アプリケーションおよびサポート ファイルがインストールされているディレクトリを表す正規表現を定義します。

   テスト値

   値を入力し、正規表現でアプリケーション ファイルを特定できるかどうかをテストすることができます。

   たとえば、C:¥Program Files¥Internet Explorer¥ExtExport.exe を入力し、値「:¥¥.*Progra.*¥¥Internet Explorer¥¥.*」に対して［テスト］をクリックします。 アプリケーションは、ファイルを検索するために正規表現値を使用します。 ファイルが見つかった場合、確認メッセージが表示されます。

   メッセージによってマッピングが正常に作成されたことを確認します。［アプリケーション マッピング］テーブルにマッピングが表示されます。

アプリケーション マッピングのインポート

アプリケーション マッピングは、別の CA Configuration Automation インスタンスから Java Archive （JAR）ファイルとしてインポートできます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［構成］タブをクリックします。
2. ［構成］タブで、［アプリケーション マッピング］リンクをクリックします。
3. ［アプリケーション マッピング］ページで、［テーブル アクション］をクリックし、次に、［アプリケーション マッピングのインポート］を選択します。
4. ［アプリケーション マッピングのインポート］ダイアログ ボックスの以下のフィールドに入力します。

   インポートする JAR ファイル

   インポートするアプリケーション マッピングが含まれている JAR ファイルの名前を指定します。 ［参照］をクリックしてファイルを選択できます。

   既存のアプリケーション マッピングを上書き

   同じ名前のファイルに上書きするかどうかを指定します。別の CA Configuration Automation インスタンスにプロファイルを保持するには、このオプションを選択します。

5. 以下のいずれかのボタンをクリックします。

   すべてをインポート

   JAR ファイル内のすべてのアプリケーション マッピングをインポートします。

   選択してインポート

   JAR ファイルからインポートする特定のアプリケーション マッピングを選択するためのダイアログ ボックスが表示されます。

   ファイルがインポートされ、［アプリケーション マッピング］テーブルにマッピングが表示されます。

アプリケーション マッピングの削除

不要になったアプリケーション マッピングを削除できます。

アプリケーション マッピングを削除する方法

1. ［環境管理］-［構成］-［アプリケーション マッピング］をクリックします。

   ［アプリケーション マッピング］ページが開き、現在のマッピングがアプリケーションのベンダーまたは発行元のアルファベット順でテーブルに表示されます。

2. 削除するマッピングの横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［アプリケーション マッピングの削除］を選択します。

   選択したマッピングの削除の確認を求めるプロンプトが表示されます。

3. ［OK］をクリックします。

   選択したマッピングが削除されたことを示す確認メッセージが表示されます。

ユーザおよびロールベース セキュリティの設定

このセクションでは、ユーザ、ユーザ グループ、ポリシー、セキュリティ権限を設定および管理する方法について説明します。 これらのタスクは、［環境管理］パネルの［アクセス管理］タブ、および Embedded Entitlements Manager （CA EEM）で実行します。 CA EEM を統合し、CA Configuration Automation のコンテキストで開始することができます。

CA EEM は、ユーザ管理およびリソース アクセス制御を提供します。 CA Configuration Automation は、CA EEM に定義されたユーザを、設定可能な権限およびアクセス レベルを持つ製品固有のユーザ グループに追加します。

アクセス権限は、ユーザがアクセスできるデータ、データが表示される方法、ユーザが実行できるアクションを決定します。

注: CA EEM をインストールして CA Configuration Automation と統合する方法の詳細については、「*実装ガイド*」を参照してください。 CA EEM 機能の詳細については、CA EEM のドキュメントおよびオンライン ヘルプを参照してください。

CA EEM セキュリティ証明書のインストールおよび EEM Host プロパティの設定

セキュリティ証明書は、CA Configuration Automation のコンテキストに応じて CA EEM を表示するために必要になります。 CA EEM インストール プログラムは、修飾されていないホスト名を使用して、必要なセキュリティ証明書を作成します。

CA Configuration Automation サーバ インストール プログラムでは、［CA Embedded Entitlements Manager 設定］画面で EEM サーバ名の入力が要求されます。 デフォルトでは、インストール プログラムは［EEM サーバ名］フィールドに、CA Configuration Automation サーバ がインストールされているローカル ホストの非修飾名を入力します。 CA Configuration Automation サーバ は、このデフォルトの名前（またはユーザが入力した名前）を［構成］ページの［プロパティ］テーブルに格納します。 ［アクセス管理］タブを表示しようとしてエントリがセキュリティ証明書に一致しない場合、以下のエラーが表示されます。

コンテンツは、有効なセキュリティ証明書によって署名されていないため、ブロックされました。

このエラーを回避するには、セキュリティ証明書をインストールし、証明書と一致するように EEM ホスト プロパティを設定します。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、［アクセス管理］タブをクリックします。

   エラー メッセージが CA Configuration Automation UI に表示されます。 Internet Explorer では、ブロックされたコンテンツに関する同様のメッセージが黄色いバーでブラウザの上部に表示します。

2. 黄色いバーをクリックし、［ブロックされたコンテンツの表示］を選択します。

3. CA Configuration Automation ログイン ページで、ユーザ名およびパスワードを入力し、［ログイン］をクリックします。

   ［アクセス管理］タブ ページが開き、コンテキストに応じて CA EEM UI が表示されます。

4. CA EEM フレーム内の任意の場所で右クリックし、［プロパティ］を選択します。
5. ［プロパティ］ダイアログ ボックスで、［証明書］をクリックします。

   ［証明書］ダイアログ ボックスが表示されます。

   重要: ［全般］タブの［発行先］フィールドのサーバ名に注意してください。 ここに表示される値を、手順 9 内の［プロパティ］テーブルに正確に入力します。
6. ［証明書のインストール］をクリックします。
7. ［証明書ストアの選択］ダイアログ ボックスで、［信頼されたルート証明機関］証明書ストアを選択し、［OK］をクリックします。
8. ［構成］タブの［プロパティ］リンクをクリックします。
9. ［プロパティ］テーブルで、既存の［値］フィールドの値を、手順 5 の［全般］タブの［発行先］フィールドの値に変更します。
10. Enter キーを押します。

    新しい値が保存され、ユーザおよびユーザ グループを管理するために CA Configuration Automation で CA EEM を使用することができます。

CA EEM の CA Configuration Automation ユーザの作成

CA EEM をインストールおよび統合したら、既存の CA EEM ユーザを CA Configuration Automation に読み込むか、または新規ユーザを作成できます。

ユーザを追加する前に CA Configuration Automation で定義されている唯一のユーザは、CA Configuration Automation のインストール中に作成されたスーパーユーザです。 このスーパーユーザは、すべての CA Configuration Automation 機能に対する権限を持っています。スーパーユーザは、CA EEM への接続性が失われた場合に、ユーザ アクセスを設定して製品にアクセスするための初回ログイン用に設計されています。少なくとも 1 人のユーザがすべての機能にアクセス権があることを確認します。 このユーザの権限を制限するには、製品を管理するための別の管理者ユーザを作成して使用する必要があります。

ユーザを作成して内部データベースに格納したり、外部ディレクトリ（Active Directory など）からユーザをインポートしたりすることもできます。

注: CA Configuration Automation と CA EEM の統合では、CA Configuration Automation の［環境管理］パネルから CA EEM UI を開始できます。ただし、CA EEM にアクセスするためにユーザ アカウントおよびパスワードが必要となります。

次の手順に従ってください:

1. CA Configuration Automation を開き、［環境管理］リンクをクリックし、［アクセス管理］タブをクリックします。
2. ［ユーザ］ページで、［ユーザ］領域（左下）の cca_users フォルダ アイコンのすぐ左にある［新規ユーザ］アイコンをクリックします。

   CA EEM の［新規ユーザ］ページが CA Configuration Automation のコンテキストで表示されます。
3. ［名前］フィールドに名前を入力します。

   制限： 100 英数文字
4. ［アプリケーション ユーザの詳細の追加］をクリックし、以下の情報を入力します。

   アプリケーション インスタンス名

   このユーザ アカウントがアクセスできる CA Configuration Automation インスタンスを定義します。

   アプリケーション グループ メンバシップ

   このユーザがメンバとして所属するアプリケーション固有のグループ（複数可）を定義します。
5. ユーザに関する適切な詳細を［全般］領域に入力します。
6. ［使用可能なグローバル ユーザ グループ］列のグループをダブルクリックして、既存のグローバル ユーザ グループ（複数可）にユーザを追加します。

   ［選択されたグローバル ユーザ グループ］列に選択したグループが表示されます。

   注: 特定のユーザ グループを見つけるには、必要に応じて［属性］、［演算子］、［値］フィールドに入力し、［検索］をクリックします。

7. ［認証］領域の以下のフィールドに入力します。

不正なログイン カウント

ユーザが試行したログインが連続して失敗した回数を示します。この値は、ログインに成功するとゼロにリセットされます。

再開日

ユーザ アカウントを有効にする日付を定義します。 日時を選択するには、カレンダ アイコンをクリックします。ユーザは［再開日］の前、または［停止日］の後にログインすることはできません。

停止日

ユーザ アカウントが無効になった日付を定義します。 日時を選択するには、カレンダ アイコンをクリックします。 有効期限を指定しない場合は、このフィールドを空白のままにします。 ユーザは［再開日］の前、または［停止日］の後にログインすることはできません。

パスワード ポリシーを上書き

パスワード ポリシーに適合しないパスワードを持つことをユーザに許可するかどうかを指定します。

次のログイン時にパスワードを変更

管理者によって割り当てられたパスワードで初めてログインした後に、ユーザがパスワードを変更する必要があるかどうかを指定します。

一時停止

ユーザ アカウントを手動で非アクティブにするかどうかを指定します。

新しいパスワード

管理者によって割り当てられたユーザのパスワードを定義します。［次のログイン時にパスワードを変更］オプションを選択した場合、ユーザが CA Configuration Automation に最初にログインした後、このパスワードを変更するよう要求されます。

パスワードの確認

エントリが一致することを要求することにより、パスワードに間違いが含まれていないことを確認します。

8. ［保存］をクリックします。

次のメッセージが表示されます。

確認： グローバル ユーザが正常に作成されました。

手順 4 でアプリケーション固有の詳細を指定した場合、メッセージに以下の行も含まれます。

（グローバル ユーザの詳細が正常に作成されました。アプリケーション ユーザの詳細が正常に作成されました。）」という確認メッセージが表示されます。

9. ユーザごとに、この手順を繰り返します。

ユーザの検索

［ユーザの検索］ページには、以下のフィールドが表示されます。

グローバル ユーザ

すべてのアプリケーションに割り当てられるすべてのユーザを含めます。

アプリケーション ユーザの詳細

特定のアプリケーションに割り当てられるすべてのユーザを含めます。

属性

検索する属性を指定します。 ［グローバル ユーザ］属性は事前定義済みです。［アプリケーション ユーザの詳細］属性はアプリケーションごとに定義されます。

オペレータ

検索に使用する演算子を指定します。

値

検索する値を指定します。ワイルドカードとしてアスタリスク (*) を使用できます。ただし、先頭または末尾の文字としてのみ使用できます。

［値］フィールドを空白にしておくと、* に設定したのと同じ意味になり、すべての値と一致します。

空フォルダの表示

空のフォルダまたはユーザが含まれていないフォルダを検索します。

実行

指定した基準に基づいてユーザを検索します。 ［ユーザ］パネルの下にユーザが表示されます。

アクセス ポリシーの作成

アクセス ポリシーは、CA EEM に作成されたルールで、CA Configuration Automation 機能に対するアクセス権限を定義するために CA Configuration Automation ユーザおよびユーザ グループに関連付けられます。CA EEM は、ポリシーがユーザに適用されるかどうか判断するためにアイデンティティおよびリソース クラスを照合します。

［アクセス管理］タブ ページには、［ポリシー］ページへのリンクが含まれます。 ［ポリシー］ページでは、アクセス ポリシーを検索、参照、作成、編集することができます。

ポリシーは、ポリシー タイプによってツリー形式で並べられ、以下のタブに表示されます。

明示的な許可

ポリシーに適合した場合に、指定したリソースに対する指定したアクセス権をアイデンティティに*許可*します。

明示的な否認

ポリシーに適合した場合に、指定したリソースに対する指定したアクセス権をアイデンティティに*許可しません*。

アプリケーションに固有のアクセス ポリシーに加えて、以下のポリシー タイプが含まれています。

委任ポリシー

ユーザが自分の権限を他のユーザに委任することを可能にします。

動的ユーザ グループ ポリシー

ルールを使用してアプリケーションに固有のグループとメンバシップを定義するポリシーを指定します。

イベント ポリシー

配信されるイベント、およびサマリに結合されるだけのイベントを決定します。イベント ポリシーを使用することによって、詳細にレポートされるイベントを設定できます。

責任ポリシー

認証の確認後に、必要なアクションをアプリケーションに戻します。責任ポリシーはアプリケーションに固有です。責任の名前および属性が 1 つ以上含まれます。 責任ポリシーを使用して、アクセス権が許可または拒否されたときに実行する必要のあるアクションを制御できます。 たとえば、イベントを送信したり、ワークフロー プロセスを開始したり、電子メールを送信したりすることができます。

スコープ ポリシー

CA EEM のオブジェクト（ポリシー、カレンダなど）に対する管理者アクセス権を制限します。

次の手順に従ってください:

1. CA Configuration Automation を開き、［環境管理］リンクをクリックし、［アクセス管理］タブをクリックします。

   CA EEM の［ホーム］タブ ページが CA Configuration Automation のコンテキストに応じて表示されます。

   注:

   - CA EEM ログイン ページが表示された場合は、EEM 管理者ユーザの認証情報を入力し、［アプリケーション］ドロップダウン リストを CCA に設定して［ログイン］をクリックします。
   - CA EEM ログイン ページ上の［アプリケーション］ドロップダウン リストに CCA が含まれていない場合、CA Configuration Automation が CA EEM に正常に登録されていません。 CA Configuration Automation を使用してアクセスを管理することはできません。

2. ［ID の管理］をクリックし、［ポリシー］リンクをクリックします。

3. ［ポリシー］ページで、［明示的な許可］または［明示的な否認］タブをクリックし、［アクセス ポリシー］フォルダに対して［新規アクセス ポリシー］アイコンをクリックします。

4. ［新しいアクセス プロファイル］ページで、以下のフィールドに入力して［保存］をクリックします。

名前

ポリシー名を定義します。 表示上の問題を防ぐため、英数字のみを使用してください。

説明

ポリシーの説明を入力します。 たとえば、ポリシーの目的を指定できます。

カレンダ

ポリシー評価照合プロセスで使用するカレンダを指定します。 カレンダを指定しない場合、すべての日付と時刻が対象になります。

リソース クラス名

ポリシーが定義されるリソース クラスの名前を指定します。 たとえば、すべての委任ポリシーに対してリソースクラス名を safeDelegation に設定し、すべての責任ポリシーのリソース クラス名を safeObligation に設定できます。新しいリソース クラスは［アプリケーション インスタンス］ページで定義します。

明示的な否認

ポリシーによって指定され、［明示的な否認］タブに表示されるアクセス権をポリシーが明示的に否認するかどうかを指定します。

無効

ポリシーが無効になり、照合フェーズで考慮されないかどうかを指定します。

導入前

ポリシーが非アクティブとして認識されるかどうかを指定します。［導入前］チェック ボックスをオンにした場合、アプリケーションは許可を確認するためにポリシーを使用しません。

タイプ

以下のフィールドがアクセス ポリシーの設定を制御します。

アクセス ポリシー

リスト表示されたすべてのリソースにアクションおよびフィルタを適用します。

アクセス制御リスト

リスト表示されたリソースごとに特定のアクションがあるか、フィルタがあるかどうかを指定します。

ID アクセス制御リスト

アプリケーションがアクションを特定のアイデンティティに適用することを指定します。リストに含まれていないすべてのアイデンティティに適用されるデフォルト ルールを作成します。また、アイデンティティ タイプ（ユーザ、アプリケーション グループ、グローバル グループ、動的グループ）をアイコンでマークします。

注: アプリケーションでは、リソース用にシンプルなリストを管理し、このタイプのポリシー用のフィルタはありません。

ID パネル

ポリシー評価の照合フェーズで使用するアイデンティティ（ユーザ、ユーザ グループ、グローバル ユーザ グループ）のリストを定義します。 このリストが空の場合、すべての ID が一致します。

タイプ

アイデンティティのタイプ（ユーザ、アプリケーション グループ、グローバル グループ、または動的グループ）を指定します。

タイプを選択したら、検索条件（属性、演算子、値など）を指定して［検索］をクリックすると、一致するアイデンティティが表示されます。

アイデンティティ

指定されたタイプに一致するアイデンティティを表示します。

選択した ID

ポリシーが適用されるアイデンティティを表示します。 選択済みアイデンティティ フィールドにアイデンティティを移動させるには、右矢印をクリックします。

アクセス ポリシー構成パネル

選択されたタイプが［アクセス ポリシー］である場合、［アクセス ポリシーの設定］パネルには以下のフィールドが表示されます。

リソースの追加

ポリシー評価の照合フェーズで使用するリソースを定義します。 ワイルドカード文字を指定するには、リソース名の先頭または末尾にアスタリスク（*）を使用します。 リソース クラス名の先頭と末尾以外の場所にあるアスタリスクはリテラルとして処理されます。

アクション

ポリシー評価の照合フェーズで使用するアクション（作成、更新、削除、エクスポート、またはインポートのうち 1 つ以上）を指定します。 アクションを選択しない場合、すべてのアクションが対象になります。

フィルタ

ポリシー評価フェーズで使用するフィルタを定義します。フィルタを定義するには、［フィルタの追加］をクリックします。

アクセス制御リストの設定パネル

選択されたタイプが［アクセス制御リスト］である場合、［アクセス制御リストの設定］パネルには以下のフィールドが表示されます。

リソースの追加

ポリシー評価フェーズで使用するリソースを定義します。 リソース名を入力し、［追加］アイコン（+）をクリックします。

アクション

関連付けられたリソースに使用するアクション（作成、更新、削除、エクスポート、インポートのうち 1 つ以上）を指定します。

リソース名を正規表現として扱う

リソース名を正規表現と見なすべきかどうかを指定します。たとえば、正規表現として保存されたリソース J* へのアクセス権を持つアイデンティティは、J で始まるあらゆるリソースにアクセスできます。

フィルタ

関連するリソース名に適用されるフィルタを定義します。フィルタを定義するには、鉛筆アイコンをクリックします。

ID アクセス制御リストの設定パネル

選択されたタイプが［ID アクセス制御リスト］である場合、［ID アクセス制御リストの設定］パネルには以下のフィールドが表示されます。

タイプ

アイデンティティのタイプ（ユーザ、アプリケーション グループ、グローバル グループ、または動的グループ）を指定します。

タイプを選択したら、検索条件（属性、演算子、値など）を指定して［検索］をクリックすると、一致するアイデンティティが表示されます。

アイデンティティ

指定されたタイプに一致するアイデンティティを表示します。

選択した ID

ポリシーが適用されるアイデンティティを表示します。

リソース

ポリシー評価フェーズで使用するリソースを定義します。このリソースには、特定のアクションおよびフィルタが関連付られています。

リソースの追加

ポリシー評価の照合フェーズで使用するリソースを定義します。ワイルドカード文字を指定するには、リソース名の先頭または末尾にアスタリスク（*）を使用します。 リソース クラス名の先頭と末尾以外の場所にあるアスタリスクはリテラルとして処理されます。

リソース名を正規表現として扱う

リソース名を正規表現と見なすべきかどうかを指定します。たとえば、正規表現として保存されたリソース J* へのアクセス権を持つアイデンティティは、J で始まるあらゆるリソースにアクセスできます。

アプリケーションはアクセス プロファイルを作成します。

グローバル ユーザおよびグローバル グループの記憶域の設定

グローバル ユーザとユーザ グループが格納される場所を指定できます。記憶域のオプションは以下のとおりです。

- 内部データストアに格納
- Reference from an external directory
- CA SiteMinder から参照

グローバル ユーザおよびグローバル グループの記憶域を設定する方法

1. CA Configuration Automation を開き、［環境管理］-［アクセス管理］-［構成］をクリックします。

   ［EEM サーバ構成］ページが表示されます。

2. 以下のいずれかのオプションを選択し、表示されるフィールドにエントリを指定して、［保存］をクリックします。

   内部データストアに格納

   グローバル ユーザおよびグローバル グループを内部に格納します。

   Reference from an external directory

   グローバル ユーザおよびグローバル グループを外部ディレクトリに格納します。 これを選択した場合、グローバル ユーザおよびグローバル グループは読み取り専用と見なされます。 このオプションを選択すると、以下のフィールドが表示されます。

   タイプ

   外部ディレクトリのタイプを指定します。現在サポートされているタイプには、CA Identity Manager、Microsoft Active Directory、Novell eDirectory、Novell eDirectory-CN、Sun One Directory、および Custom Mapped Directory が含まれます。

   ホスト

   外部ディレクトリのホストを指定します。 ホスト名は、外部ディレクトリがインストールおよび実行されているコンピュータの IP 名または IP アドレスです。 IP 名または IP アドレスは、Internet Packet version 4（IPv4）または version 6（IPv6）の形式になります。

   ポート

   外部ディレクトリ ホストで接続するポートを指定します。 これは LDAP ポートです。

   ベース DN

   ベースとして使用される LDAP DN を指定します。この DN の下で検出されたグローバル ユーザおよびグローバル グループのみが eIAM にマップされます。

   注: ベース DN にスペースを含めることはできません。

ユーザ DN

外部ディレクトリ ホストに接続するために使用する DN を指定します。

注: ユーザ DN の cn にカンマを含めることはできません。たとえば、ユーザ DN が cn=firstname,middlename,dc=foo,dc=com の場合、カンマの前に円記号（¥）を使用します。たとえば、ユーザ DN は cn=firstname¥,middlename,dc=foo,dc=com になります。

パスワードおよびパスワードの確認

外部ディレクトリ ホストに接続するために使用するユーザ DN のパスワードを指定します。

トランスポート レイヤ セキュリティ

外部ディレクトリへの LDAP 接続を行うときに TLS を使用するかどうかを指定します。

マップされていない属性を含める

マップされていない外部属性を指定します。

注: マップされていない属性は検索に使用できます。また、フィルタとしても使用できます。

グローバル ユーザをキャッシュ

これを選択した場合、eIAM サーバはグローバル ユーザをメモリにキャッシュします。これにより、スケーラビリティが失われる代わりにルックアップが速くなります。

注: グローバル ユーザ グループは常にキャッシュされます。

キャッシュ更新時間

キャッシュにされたグループ（オプションでユーザ）を更新する時間（分単位）を指定します。

Exchange グループをグローバル ユーザ グループとして取得

Exchange グループも有効なグローバル ユーザ グループとして使用されるように指定します。これにより、配信リストのメンバに対するポリシーを書き込むことができます。 タイプ Microsoft Active Directory にのみ利用可能です。

ステータス

外部ディレクトリ バインドのステータス、および外部ディレクトリ データがロードされるかどうかを指定します。

 成功を意味します。また、外部ディレクトリ バインドが成功するか、またはデータがロードされた場合に表示されます。

 警告を意味します。外部ディレクトリ データがまだロードしている場合に表示されます。

 エラーを意味します。外部ディレクトリ バインドが失敗した場合に表示されます。

注: 変更を保存せずに、ステータスをリフレッシュするには、［ステータスのリフレッシュ］をクリックします。

CA SiteMinder から参照

グローバル ユーザおよびグローバル グループを CA SiteMinder データ ストアに格納します。 これを選択した場合、ユーザおよびグループは読み取り専用と見なされます。 このオプションを選択すると、以下のフィールドが表示されます。

ホスト

SiteMinder が実行されているホスト システムの名前を定義します。 ホスト名は、SiteMinder がインストールおよび実行されているコンピュータの IP 名または IP アドレスです。 IP 名または IP アドレスは、Internet Packet version 4（IPv4）または version 6（IPv6）の形式になります。

管理者名

システムとドメインのオブジェクトをメンテナンスする権限がある SiteMinder スーパーユーザを定義します。

管理者パスワードおよびパスワードの確認

SiteMinder 管理者のパスワードを定義します。

エージェント名

エージェントの名前を定義します。 この名前は、［ポリシー サーバ］に提供されるエージェント名と一致する必要があります。

注: エージェント名は大文字と小文字が区別されません。

エージェント秘密および秘密確認

SiteMinder ユーザ インターフェースに定義されている共有秘密を定義します。

注: エージェント秘密は大文字と小文字が区別されます。

グローバル ユーザをキャッシュ

eIAM サーバがグローバル ユーザをメモリにキャッシュするように指定します。これにより、スケーラビリティが失われる代わりにルックアップが速くなります。

注: グローバル ユーザ グループは常にキャッシュされます。

キャッシュ更新時間

キャッシュにされたグループ（オプションでユーザ）を更新する時間（分単位）を指定します。

マップされていない属性を含める

マップされていない外部属性を指定します。

注: これらも検索に使用できます。または、フィルタとして使用できます。

認可ストア タイプ

SiteMinder によって認可に使用されるストアのタイプを指定します。現在サポートされているタイプには、CA Identity Manager、Custom Mapped Directory、Microsoft Active Directory、Novell eDirectory、Novell eDirectory-CN、および Sun One Directory が含まれます。

認可ストア名

ユーザ情報が認可される認可ストアを指定します。

認証ストア名

ユーザ情報が認証される認証ストアを指定します。

Exchange グループをグローバル ユーザ グループとして取得

Microsoft Exchange グループが有効なグローバル ユーザ グループになるように指定します。

検索タイムアウト

SiteMinder がユーザの検索時に外部ディレクトリからの応答を待機する最大時間を指定します。 指定した時間が経過すると、SiteMinder は外部ディレクトリとの接続をタイムアウトします。

デフォルト： 60 秒

ストアのリフレッシュ

接続パラメータに基づいてストア情報（［認可ストア名］および［認証ストア名］）を取得します。

ステータス

外部ディレクトリ バインドのステータス、および外部ディレクトリ データがロードされるかどうかを指定します。

 成功を意味します。また、外部ディレクトリ バインドが成功するか、またはデータがロードされた場合に表示されます。

 警告を意味します。外部ディレクトリ データがまだロードしている場合に表示されます。

 エラーを意味します。外部ディレクトリ バインドが失敗した場合に表示されます。

選択した保存方法が、グローバル ユーザとグローバル グループに実装されます。

CA EEM シングル サインオン シナリオ

CA Configuration Automation は、以下の状況において、既存の CA EEM ブラウザ Cookie を使用し、シングル サインオンをサポートします。

- 起動する製品の CA EEM ユーザが、起動する製品の CA EEM インターフェースを使用して CA EEM にログインしました。 CA Configuration Automation および起動する製品が CA EEM サーバを共有しています。
- 起動する製品が、CA EEM サーバに自動で認証するために CA EEM API を使用しており、起動する製品が CA EEM からのトークンを CA Configuration Automation のコンテキスト内起動 URL パラメータ（EEM=[token]）に渡します。

CA EEM が以前に認証されなかった場合、CA Configuration Automation ログオン画面が表示されます。 CA EEM は CA EEM ブラウザ Cookie を作成および使用し、CA Configuration Automation はシングル サインオンをサポートしません。

ネットワーク ディスカバリ ゲートウェイの管理

［環境管理］パネルの［ネットワーク］タブには、ネットワーク ディスカバリ ゲートウェイ (NDG) サーバを作成、表示、編集、テスト、および保護するための機能が含まれています。 NDG サーバは、企業内のサーバおよびサービスを特定および監視する CA Configuration Automation ディスカバリ操作を担当します。

Network Discovery Gateway の表示および編集

ネットワークにインストールされた NDG サーバはすべて表示できます。特定の NDG サーバに関する詳細を表示して編集することもできます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、次に［ネットワーク］タブをクリックします。

   ［Network Discovery Gateway］ページが開き、CA Configuration Automation のインストールの前提条件としてインストールした NDG サーバが表示されます。他の NDG サーバをインストールした場合、それらも表示されます。

2. ［サーバ名］列のリンクをクリックします。

   選択した NDG サーバの［詳細］ページが表示されます。

3. （オプション）サーバがディスカバリ操作に使用するポート番号を編集し、［保存］をクリックします。

   ［Network Discovery Gateway］ページに更新された情報が表示されます。

Network Discovery Gateway の作成

CA Configuration Automation をインストールする際、CA Configuration Automation サーバ が使用する NDG サーバの名前およびポート番号の入力がユーザに要求されます。 他の NDG サーバをインストールした場合、それらを CA Configuration Automation で追加および管理することができます。

次の手順に従ってください:

1. ［環境管理］リンクをクリックし、次に［ネットワーク］タブをクリックします。
2. ［Network Discovery Gateway］ページで、［テーブル アクション］ドロップダウン リストから［Network Discovery Gateway の作成］を選択します。
3. ［Network Discovery Gateway の作成］ページで、Network Discovery Gateway がディスカバリ操作に使用するサーバ名とポート番号を入力します。
4. ［保存］をクリックします。

   アプリケーションはサーバ接続をテストします。接続が確認された場合、［Network Discovery Gateway］ページ上で NDG サーバがテーブルに追加されます。

ネットワーク ディスカバリ ゲートウェイのテスト

CA Configuration Automation によって管理されている NDG サーバへの接続をテストできます。

NDG サーバをテストする方法

1. ［環境管理］ リンクをクリックし、次に、［ネットワーク］タブをクリックします。

   ［ネットワーク ディスカバリ ゲートウェイ］ページが開き、既存の NDG サーバが表示されます。
2. NDG サーバ（複数可）の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［ネットワーク ディスカバリ ゲートウェイのテスト］を選択します。

   ［サーバ テスト結果］ウィンドウが開き、選択したサーバごとに［応答中］または［失敗］のいずれかが表示されます。

ネットワーク ディスカバリ ゲートウェイの保護

セキュリティ証明書を使用して、NDG サーバと CA Configuration Automation サーバ の間の通信を保護できます。 証明書を作成する方法の詳細については、「セキュリティ証明書の作成および管理 (P. 62)」を参照してください。

NDG サーバを保護する方法

1. ［環境管理］リンクをクリックし、次に［ネットワーク］タブをクリックします。

   ［ネットワーク ディスカバリ ゲートウェイ］ページが開き、既存の NDG サーバが表示されます。

2. 保護するサーバ（複数可）の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［ネットワーク ディスカバリ ゲートウェイの保護］を選択します。

   ［ネットワーク ディスカバリ ゲートウェイの保護］ダイアログ ボックスが表示されます。

3. 対応するフィールドに以下の情報を入力し、［OK］をクリックします。

   エージェントの証明書パスワード

   エージェント証明書の作成時に関連付けられたパスワードを指定します。

   パスワードの確認

   証明書パスワードを正しく入力したことを確認します。入力したパスワードは、このエントリと一致する必要があります。

   認証局

   認証局の作成時に関連付けられたパスワードを指定します。

   接続が保護され、［ネットワーク ディスカバリ ゲートウェイ］テーブルの［保護されている］列にチェック マークが表示されます。

ネットワーク ディスカバリ ゲートウェイの削除

管理する必要がなくなった NDG サーバを CA Configuration Automation から削除できます。

NDG サーバを削除する方法

1. ［環境管理］リンクをクリックし、次に［ネットワーク］タブをクリックします。

   ［ネットワーク ディスカバリ ゲートウェイ］ページが開き、既存の NDG サーバが表示されます。

2. 削除するサーバ（複数可）の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［ネットワーク ディスカバリ ゲートウェイの削除］を選択します。

   削除の確認を求めるプロンプトが表示されます。

3. ［OK］をクリックします。

   選択した NDG サーバが［ネットワーク ディスカバリ ゲートウェイ］テーブルから削除されます。

Catalyst 属性プロファイルおよびジョブの管理

Catalyst 属性プロファイルの作成

Catalyst 属性プロファイルを作成して、CA Configuration Automation から CA Catalyst に送信され、その他のコンシューミング製品（CA CMDB など）に送信されるデータのタイプを指定します。

Catalyst 属性プロファイル プロファイルを作成する方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst 属性プロファイル］タブ ページが表示されます。

2. ［テーブル アクション］をクリックし、次に［Catalyst 属性プロファイルの作成］を選択します。

   ［Catalyst 属性プロファイルの作成］ウィザードの［プロファイル］ページが表示されます。

3. 対応するフィールドに以下の情報を入力し、［次へ］をクリックします。

   名前

   プロファイルの名前を指定します。

   説明

   プロファイルを説明します。

   動的

   CA Catalyst、CCA コネクタ、およびコンシュームする製品が、CA Configuration Automation 内の以下のイベントについて動的に通知を受けるかどうか指定します。

   - サーバ、サービス、またはコンポーネントが追加されるか削除されます。
   - サーバはサービスに追加されるか、またはサービスから削除されます。

   デフォルト

   このプロファイルが、スケジュール設定された Catalyst 属性プロファイル ジョブに対するデフォルトのプロファイルであることを指定します。

   ［属性］ページが表示されます。

4. ［属性］ペイン内の、以下の属性タイプの隣にあるプラス記号をクリックします（複数可）。

   - サーバ
   - コンポーネント
   - 関係
   - ストレージ

   選択したノードが展開され、その属性タイプで利用可能な属性が表示されます。

5. プロファイルに含める属性の隣にあるチェック ボックスをオンにします（複数可）。 選択された属性は、CA Catalyst および CCA コネクタによって消費する製品で利用可能になります。

   選択された属性詳細が右ペイン内に表示されます。

6. ［完了］をクリックします。

   新しいプロファイルが作成され、［Catalyst 属性プロファイル］テーブルに表示されます。

Catalyst 属性プロファイルの表示および編集

既存の Catalyst 属性プロファイルを表示および編集できます。

Catalyst 属性プロファイルを表示および編集する方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst 属性プロファイル］タブ ページが開き、［Catalyst 属性プロファイル］テーブルが表示されます。

2. ［プロファイル名］列のリンクをクリックします。
   選択したプロファイルの［詳細］ページが表示されます。

3. （オプション）［プロファイル］ページまたは［属性］ページでエントリを編集してから、［保存］をクリックします。

   フィールドの説明は、「Catalyst 属性プロファイルの作成 (P. 113)」にあります。

   プロファイルが更新されます。

Catalyst 属性プロファイルの削除

実行またはスケジュールする必要がなくなったプロファイルを削除できます。

Catalyst 属性プロファイルを削除する方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst 属性プロファイル］タブ ページが表示されます。

2. 削除するプロファイル（複数可）の横にあるチェック ボックスをオンにし、［アクションの選択］ドロップダウン リストから［プロファイルの削除］を選択します。

   削除の確認を求めるプロンプトが表示されます。

3. ［OK］をクリックして、プロファイルの削除を確定します。

   選択したプロファイルは削除され、［Catalyst 属性プロファイルの作成］テーブルから除去されます。

Catalyst 属性プロファイルのインポート

Catalyst 属性プロファイルを、CA Configuration Automation の別のインスタンスから Java Archive（JAR）ファイルとしてインポートできます。

Catalyst 属性プロファイルをインポートする方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst 属性プロファイル］タブ ページが表示されます。

2. ［テーブル アクション］をクリックし、次に［Catalyst 属性プロファイルのインポート］を選択します。

   ［Catalyst 属性プロファイルのインポート］ダイアログ ボックスが表示されます。

3. 対応するフィールドに、以下の情報を入力するか、または選択します。

   インポートする JAR ファイル

   インポートするプロファイルが含まれている JAR ファイルの名前を指定します。［参照］をクリックしてファイルにナビゲートできます。

   既存の Catalyst 属性プロファイルを上書きします

   インポート中のファイルが、同じ名前のファイルを上書きするかどうかを指定します。 CA Configuration Automation の別のインスタンスのプロファイルに加えられた変更を保持する場合は、このオプションを選択します。

4. 以下のいずれかのボタンをクリックします。

   すべてをインポート

   JAR ファイル内のすべてのプロファイルをインポートします。

   選択内容をインポート

   ダイアログ ボックスが表示され、ここで、インポートする JAR ファイル内のプロファイルを選択することができます。

   ファイルはインポートされ、［Catalyst 属性プロファイル］テーブルにプロファイルが表示されます。

Catalyst 属性プロファイルのエクスポート

Catalyst 属性プロファイルを JAR ファイルとしてエクスポートし、CA Configuration Automation の別のインスタンスで使用することができます。

Catalyst 属性プロファイルをエクスポートする方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst］タブ ページが表示されます。

2. エクスポートするプロファイル（複数可）の隣にあるチェック ボックスをオンにし、［アクションの選択］をクリックして、［Catalyst 属性プロファイルのエクスポート］を選択します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。

3. ［保存］をクリックします。

   ［名前を付けて保存］ダイアログ ボックスが表示され、エクスポート JAR ファイルは以下の形式でデフォルトの名前を割り当てられます。

   CatalystAttributesProfile_Export_<*タイムスタンプ*>.jar

   例： CatalystAttributesProfile_Export_2011_08_01_10_03_13.jar

4. 必要に応じてファイル名を編集し、ファイルを保存する場所を選択して［保存］をクリックします。

   プロファイルは、選択した場所へエクスポートされます。

Catalyst 属性プロファイルをデフォルトとして設定

1 つの Catalyst 属性プロファイルを*デフォルト*として指定することができます。スケジュール済み Catalyst 属性プロファイル ジョブは、デフォルト プロファイルを使って、どの属性が CA Catalyst および CCA コネクタを使用している消費する製品で利用可能になったかを決定します。

Catalyst 属性プロファイルをデフォルトのプロファイルとして設定する方法

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［プロファイル］リンクをクリックします。

   ［Catalyst 属性プロファイル］タブ ページが表示されます。

2. デフォルトのプロファイルにする Catalyst 属性プロファイルの隣にあるチェック ボックスをオンにして、［アクションの選択］をクリックし、［デフォルトとして設定］を選択します。

   ［デフォルト］列で、選択したプロファイルの隣にチェック マークが表示されます。

Catalyst ジョブの作成

プロファイル内の属性をコンシューミング製品にエクスポートする Catalyst 属性プロファイル ジョブを作成およびスケジュールします。

次の手順に従ってください:

1. ［環境管理］リンクをクリックして［Catalyst］タブをクリックし、次に［ジョブ］リンクをクリックします。
2. ［テーブル アクション］ドロップダウン リストをクリックし、［Catalyst ジョブの作成］を選択します。
3. ［Catalyst ジョブの作成］ページ上でフィールドに入力し、［次へ］をクリックします。

   名前

   ジョブを指定します。

   説明

   ジョブの目的を説明します。

   属性プロファイル

   ジョブに使用するプロファイル定義します。

   値:

   - デフォルトを使用
   - すべての Catalyst 属性
   - ユーザが作成したカスタム プロファイル
4. ［サービス］ページで、Catalyst ジョブに含めるサービス（複数可）を［利用可能なサービス］列でダブルクリックします。

   選択したサービスは、［選択されたサービス］列に移動します。
5. ［次へ］をクリックします。
6. ［サーバ グループ］ページで、Catalyst ジョブに含めるサーバ グループ（複数可）を［利用可能なサーバ グループ］列でダブルクリックします。

   選択したグループは、［選択されたサーバ グループ］列に移動します。
7. ［次へ］をクリックします。

8. ［サーバ］ページで、Catalyst ジョブに含めるサーバ（複数可）を［利用可能なサーバ］列でダブルクリックします。

   選択したサーバは、［選択されたサーバ］列に移動します。

9. ［次へ］をクリックします。

10. ［ストレージ システム］ページで、Catalyst ジョブに含めるストレージ システム（複数可）を［利用可能なストレージ システム］列でダブルクリックします。

11. ［次へ］をクリックします。

12. ［ブループリント グループ］ページで、Catalyst ジョブに含めるグループ（複数可）を［利用可能なブループリント グループ］列でダブルクリックします。

    選択したグループは、［選択されたブループリント グループ］列に移動します。

13. ［次へ］をクリックして、［ブループリント］ページを開きます。

14. ［ブループリント］ページで、Catalyst ジョブに含めるブループリント（複数可）を［利用可能なブループリント］列でダブルクリックします。

    選択したブループリントは、［選択されたブループリント］列に移動します。

15. ［次へ］をクリックします。

16. ［スケジュール］ページで、［頻度］ドロップダウンリストから、このプロファイルがエクスポート ジョブの実行に使用する値として以下のいずれかを選択します。

    スケジュールなし

    ジョブと関連付けられたプロファイルが自動的に実行されないように指定します。 ジョブは手動で実行することも、後で実行するようにスケジュール設定することもできます。

    1 回

    ジョブと関連付けられたプロファイルが 1 回実行されることを指定します。 このオプションを選択した場合は、［時刻］フィールドを設定します。

分単位

ジョブと関連付けられたプロファイルが分単位の特定の間隔で実行されることを指定します。 このオプションを選択した場合は、以下の値を定義します。

開始時刻

プロファイルの実行が開始される時間を定義します。［開始時刻］には必ず正時を指定します（例：10:00:00PM、8:00:00AM など）。

開始日

プロファイルが初めて実行される日付を定義します。

終了日

プロファイルが最後に実行される日付を定義します。

反復間隔 # 分毎

プロファイルが実行される間隔（分単位）を定義します。

たとえば、プロファイルを午後 11:00 から 10 分間隔で実行する場合、［開始時刻］に 11:00:00PM を指定し、［反復間隔 10 分］を指定します。 プロファイルは午後 11:00、11:10、11:20、11:30、と実行され、その時間の終わり（この場合は午前 0 時）まで繰り返されます。 現在のプロファイルが次の間隔が発生する時間までに完了しない場合、その実行が完了してから次の実行が開始されます。

時間単位

ジョブと関連付けられたプロファイルが時間単位の特定の間隔で実行されることを指定します。このオプションを選択した場合は、以下の値を定義します。

開始時刻

プロファイルの実行が開始される時間を定義します。［開始時刻］には必ず正時を指定します（例：10:00:00PM、8:00:00AM など）。

開始日

プロファイルが初めて実行される日付を定義します。

終了日

プロファイルが最後に実行される日付を定義します。

反復間隔 # 時間毎

プロファイルが実行される間隔（時間単位）を定義します。

たとえば、プロファイルを午後 11:00 から 4 時間ごとに実行する場合、［開始時刻］に 11:00:00PM を指定し、［反復間隔 4 時間］を指定します。 プロファイルは、午後 11:00、午前 3:00、午前 7:00、午前 11:00、午後 3:00、午後 7:00 に実行されます。現在のプロファイルが次の間隔が発生する時間までに完了しない場合、その実行が完了してから次の実行が開始されます。

注: 現在の日の開始時刻がすでに経過している場合、プロファイルはすぐに実行され、指定された反復スケジュールが再開されます。

日単位

ジョブと関連付けられたプロファイルが日単位の特定の間隔で実行されることを指定します。 このオプションを選択した場合は、以下の値を定義します。

開始時刻

プロファイルの実行が開始される時間を定義します。［開始時刻］には必ず正時を指定します（例： 10:00:00PM、8:00:00AM など）。

開始日

プロファイルが初めて実行される日付を定義します。

終了日

プロファイルが最後に実行される日付を定義します。

反復間隔 # 日毎

プロファイルが実行される間隔（日単位）を定義します。

週単位

ジョブと関連付けられたプロファイルが週単位の特定の間隔で実行されることを指定します。 このオプションを選択した場合は、以下の値を定義します。

開始時刻

プロファイルの実行が開始される時間を定義します。［開始時刻］には必ず正時を指定します（例： 10:00:00PM、8:00:00AM など）。

開始日

プロファイルが初めて実行される日付を定義します。

終了日

プロファイルが最後に実行される日付を定義します。

反復間隔 # 週

プロファイルが実行される間隔（週単位）を定義します。

月単位

ジョブと関連付けられたプロファイルが月単位の特定の間隔で実行されることを指定します。 このオプションを選択した場合は、以下の値を定義します。

開始時刻

プロファイルの実行が開始される時間を定義します。［開始時刻］には必ず正時を指定します（例：10:00:00PM、8:00:00AM など）。

開始日

プロファイルが初めて実行される日付を定義します。

終了日

プロファイルが最後に実行される日付を定義します。

反復間隔 # 月

プロファイルが実行される間隔（月単位）を定義します。

17. ジョブと関連付けられたプロファイルが実行されたときにアプリケーションが送信する通知を定義します。

通知プロファイル

このプロファイルを使用したディスカバリ操作がスケジュールどおりに実行された場合に使用される通知プロファイルを定義します。 詳細については、「通知プロファイルの作成」を参照してください。

件名

選択した通知プロファイルによって送信される電子メール メッセージの件名行を定義します。

18. ［完了］をクリックします。

［Catalyst ジョブ］テーブルに新しいジョブのリストが表示されます。

CA Configuration Automation 診断

［診断］タブ ページには、以下の読み取り専用情報ページへのリンクが含まれます。

- CCA 情報
- データベース情報
- グリッド情報
- 配布されたロック情報

さらに、［診断］タブ ページには、［診断の収集］ページへのリンクが含まれます。このリンクを使用して、お使いの CA Configuration Automation サーバ または CA Configuration Automation サーバ のいずれかおよびグリッド ノードのヒープ ダンプを生成できます。 ヒープ ダンプとは、Java 仮想マシン(JVM) ヒープ内のすべてのオブジェクトの Point-in-Time レコードです。 この情報は、CA サポートによってリクエストされた場合のみ生成される必要があります。

CA Cohesion ACM からのデータの移行

CA Configuration Automation には、以下の CA Cohesion リリースから CCA データベースにデータを移行し、CA Configuration Automation サーバ UI で管理するための機能があります。

- CA Cohesion r4.5.3
- CA Cohesion ACM r5.0
- CA Cohesion ACM r5.0 SP1

注: この章では、以下、これらのリリースを CA Cohesion ACM と総称します。

以下の CA Cohesion ACM オブジェクトは CA Configuration Automation に移行できます。

- サーバ
- サーバ管理プロファイル
- サーバ ディスカバリ プロファイル
- サーバ アクセス プロファイル

- サーバ グループ
- サーバ スナップショット
- サービス
- サービス管理プロファイル
- サービス ディスカバリ プロファイル
- サービス スナップショット
- ブループリント
- ファイル構造クラスおよびパーサ
- グローバル変数
- セキュリティ証明書

移行の前提条件および制限事項

CA Cohesion ACM からデータを移行する前に、以下の前提条件を満たしていることを確認します。

- CA Configuration Automation r12.6 サーバをインストールし、ライセンス契約している。
- Cohesion データベースおよび CA Configuration Automation データベース の両方に対してデータベース アクセス権を持っている。

- CA Cohesion ACM の実装が Sybase データベースを使用した場合は、以下の手順を実行している。
  - Sybase ドライバ sybase-jdbc4.2.jar（4.2 はドライバ バージョンだが、異なる可能性もある）のコピー（以下がコピー元）
    <Cohesion_home>¥Server¥server¥webapps¥cohesion¥WEB-INF¥lib¥
    （以下がコピー先）
    <CCA_r12.6_home>¥tomcat¥webapps¥cca¥WEB-INF¥lib¥
  - r12.6 CA Configuration Automation サーバ の再起動
- セキュリティ証明書をインポートする場合は、以下を考慮します。
  - 認証局が CA Configuration Automation r12.6 に作成されていることを確認します。
  - サーバ証明書パスワードを知っている必要があります。
  - CA Cohesion ACM の KeyStore ファイルおよび TrustStore ファイルが必要です。

データを移行する前に、以下の制限事項を考慮します。

- CA Configuration Automation データベース 内にすでに存在する同様のデータは上書きされません。
- 特定のスナップショット情報を含む CA Cohesion ACM 管理プロファイルの変更検出および比較のオプションは移行されません。
- 定期的なスケジューリング オプションのみが管理プロファイルと共に移行されます。
- 管理プロファイル内のスケジュールされた操作の開始時刻は、スケジュール区間の開始時刻に設定されます。
- CA Cohesion ACM アクセス プロファイル内のプロキシ オプションは移行されません。
- スナップショットを移行する際に、パラメータ ディレクティブおよび構成ファイルがブループリント内に存在しない場合、それらの値は無視され、スナップショットの値の移行が続行します。

マイグレーション オプション

CA Configuration Automation には、CA Cohesion CCA からのデータの移行について以下のオプションがあります。

- Cohesion データベースから CA Configuration Automation データベースへの移行 (P. 128)
- Cohesion データベースからアーカイブ ファイルへの移行 (P. 131)
- アーカイブ ファイルから CA Configuration Automation データベース への移行 (P. 133)
- セキュリティ証明書のインポート (P. 134)

これらのオプションに関連付けられている手順については、以下のセクションで説明します。

Cohesion データベースから CCA データベースへのデータの移行

移行の前提条件を満たすことを確認した後に、Cohesion CA Configuration Automation データベース から CA Configuration Automation データベースにデータを移行できます。

Cohesion データベースから CA Configuration Automation データベース にデータを移行する方法

1. ［環境管理］リンクをクリックし、次に［データ移行］リンクをクリックします。

   ［データ移行］ページが開き、以下のパネルが表示されます。

   - Cohesion データベースから
   - アーカイヴ ファイルから
   - セキュリティ証明書

2. ［Cohesion データベースから］パネルの［CA Configuration Automation データベースへ］リンクをクリックします。

   ［Cohesion データベース詳細］ページが表示されます。

3. 対応するフィールドに以下の情報を入力し、[接続のテスト]をクリックします。

   データベース タイプ

   次のいずれかのデータベースを指定します。SQL サーバ または Oracle。

   サーバ名

   Cohesion データベースをホストするサーバを指定します。

   ポート番号

   Cohesion データベースが通信に使用するポート番号を指定します。

   データベース名

   （SQL サーバ データベースのみ）SQL サーバ データベース インスタンスを指定します。

   Oracle SID

   （Oracle データベースのみ）Oracle データベース インスタンスを一意に識別するシステム ID（SID）を指定します。

   データベース ユーザ

   Cohesion データベースにアクセスできる管理者ユーザのユーザ名を指定します。

   データベース パスワード

   データベース ユーザのパスワードを指定します。

   CA Configuration Automation は、指定された情報を使用して Cohesion データベースに接続できるようにし、接続を確認します。

4. ［次へ］をクリックします。

   ［共有オブジェクト］ページが表示されます。

5. 以下のいずれかの移行対象のオブジェクト タイプをクリックします。

   - サーバ
   - サービス
   - ブループリント

6. （ブループリントのみ）以下のチェック ボックスのうち、移行しないオブジェクト タイプのチェック ボックスをオフにします。
   - ブループリントの移行
   - グローバル変数

   デフォルトでは、両方のオブジェクト タイプが移行されます。
7. （オプション）特定のオブジェクトのみを CA Configuration Automation r12.6 に移行する場合は、フィルタを作成します。
   a. ［フィルタ］タブをクリックします。
   b. ［利用可能］列のオブジェクトを選択します（Ctrl+ クリックまたは Shift+ クリックを使用して、複数のオブジェクトを選択できます）。
   c. 右方向の一重矢印をクリックして、選択したオブジェクトを［選択済み］列に移動します。
   d. ［OK］をクリックします。
8. （オプション）他のオブジェクト タイプを含めるには、ステップ 5 ～ 7 を繰り返します。
9. ［終了］をクリックします。

   移行が開始され、完了時に移行が成功したかどうかが確認されます。

Cohesion データベースからアーカイブ ファイルへのデータの移行

移行の前提条件を満たすことを確認した後に、Cohesion データベースから JAR ファイルにデータを移行できます。

Cohesion CA Configuration Automation データベース から CA Configuration Automation データベース にデータを移行する方法

1. ［環境管理］リンクをクリックし、次に［データ移行］リンクをクリックします。

   ［データ移行］ページが開き、以下のパネルが表示されます。

   - Cohesion データベースから
   - アーカイヴ ファイルから
   - セキュリティ証明書

2. ［Cohesion データベースから］パネルの［アーカイブ ファイルへ］リンクをクリックします。

   ［Cohesion データベース詳細］ページが表示されます。

3. ［Cohesion データベース詳細］パネルの対応するフィールドに以下の情報を入力し、［接続のテスト］をクリックします。

   データベース タイプ

   次のいずれかのデータベースを指定します。SQL サーバ または Oracle。

   サーバ名

   Cohesion データベースをホストするサーバを指定します。

   ポート番号

   Cohesion データベースが通信に使用するポート番号を指定します。

   データベース名

   （SQL サーバ データベースのみ）SQL サーバ データベース インスタンスを指定します。

   Oracle SID

   （Oracle データベースのみ）Oracle データベース インスタンスを一意に識別するシステム ID（SID）を指定します。

データベース ユーザ

Cohesion データベースにアクセスできる管理者ユーザのユーザ名を指定します。

データベース パスワード

データベース ユーザのパスワードを指定します。

CA Configuration Automation は、指定された情報を使用して Cohesion データベースに接続できるようにし、接続を確認します。

4. ［アーカイブ詳細］パネルの対応するフィールドに以下の情報を入力します。

   ファイル パス

   JAR ファイルを保存する場所を指定します。

   ファイル名

   JAR ファイルの名前を指定します（このエントリに .jar が自動的に付加されます）。

5. ［次へ］をクリックします。

   ［共有オブジェクト］ページが表示されます。

6. 以下のいずれかの移行対象のオブジェクト タイプをクリックします。
   - サーバ
   - サービス
   - ブループリント

7. （ブループリントのみ）以下のチェック ボックスのうち、移行しないオブジェクト タイプのチェック ボックスをオフにします。
   - ブループリントの移行
   - グローバル変数

   デフォルトでは、両方のオブジェクト タイプが移行されます。

8. （オプション）特定のオブジェクトのみをアーカイブ ファイルに移行する場合は、フィルタを作成します。
   a. ［フィルタ］タブをクリックします。
   b. ［利用可能］列のオブジェクトを選択します（Ctrl+ クリックまたは Shift+ クリックを使用して、複数のオブジェクトを選択できます）。

c. 右方向の一重矢印をクリックして、選択したオブジェクトを［選択済み］列に移動します。

d. ［OK］をクリックします。

9. （オプション）他のオブジェクト タイプを含めるには、ステップ 5 ～ 8 を繰り返します。

10. ［完了］をクリックします。

移行が開始され、アーカイブ ファイルが正常に作成されたかどうかが確認されます。

アーカイブ ファイルから CCA データベースへのデータの移行

「Cohesion データベースからアーカイブ ファイルへのデータの移行 (P. 131)」に記載の手順で作成した JAR ファイルから CA Configuration Automation r12.6 データベースにデータを移行できます。

注: 移行ツールによって作成された JAR ファイルのみが CA Configuration Automation にインポートできます。

アーカイブ ファイルから CA Configuration Automation データベース にデータを移行する方法

1. ［環境管理］リンクをクリックし、次に［データ移行］リンクをクリックします。

［データ移行］ページが開き、以下のパネルが表示されます。

- Cohesion データベースから
- アーカイヴ ファイルから
- セキュリティ証明書

2. ［アーカイブ ファイルから］パネルの［CA Configuration Automation データベースへ］リンクをクリックします。

［アーカイブ ファイルからのデータ移行］ダイアログ ボックスが表示されます。

3. ［参照］をクリックし、Cohesion CCA アーカイブ ファイルにナビゲートします。

選択したファイルが［アーカイブ ファイル詳細］フィールドに表示されます。

4. ［OK］をクリックします。

   移行が開始され、完了時に［データ移行結果］ダイアログ ボックスが表示されます。

5. 以下のいずれかのボタンをクリックします。

   ログ ファイルの表示

   移行ログ ファイルを表示します。

   ログ ファイルの保存

   ダウンロード イアログ ボックスを表示します。このダイアログ ボックスでは、移行ログ ファイルを保存する場所を指定できます。

   クローズ

   ［データ移行結果］ダイアログ ボックスを閉じます。

   アーカイブ ファイルのコンテンツが CA Configuration Automation にインポートされます。

セキュリティ証明書の移行

移行の前提条件を満たすことを確認した後に、Cohesion ACM に作成されたセキュリティ証明書を CA Configuration Automation r12.6 に移行できます。

Cohesion データベースから CA Configuration Automation データベース にセキュリティ証明書を移行する方法

1. ［環境管理］リンクをクリックし、次に［データ移行］リンクをクリックします。

   ［データ移行］ページが開き、以下のパネルが表示されます。

   - Cohesion データベースから
   - アーカイヴ ファイルから
   - セキュリティ証明書

2. ［セキュリティ証明書］パネルの［証明書のインポート］リンクをクリックします。

   ［証明書のインポート］ダイアログ ボックスが表示されます。

3. 対応するフィールドに以下の情報を入力し、[接続のテスト]をクリックします。

   Cohesion サーバ名

   証明書が作成された Cohesion サーバを指定します。

   Cohesion サーバ証明書パスワード

   サーバ証明書の作成時に関連付けられたパスワードを指定します。

   CA Configuration Automation サーバ 証明書パスワード

   CA Configuration Automation サーバ に作成された認証局に関連付けられたパスワードを指定します。

   Cohesion KeyStore ファイル

   Cohesion サーバの *<cohesion_home>*¥server¥lib フォルダにある Keystore ファイルの名前を指定します。

   Cohesion TrustStore ファイル

   Cohesion サーバの *<cohesion_home>*¥server¥lib フォルダにある Truststore ファイルの名前を指定します。

4. ［OK］をクリックします。

   証明書の移行が開始され、完了時に移行が成功したかどうかが確認されます。

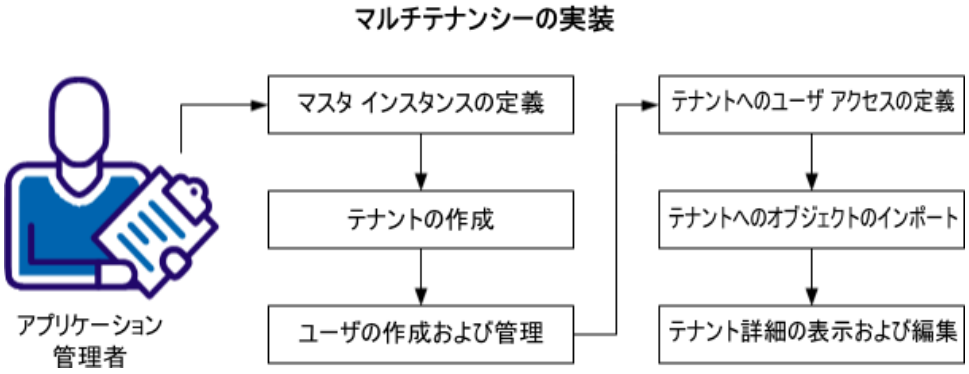
マルチテナンシーの実装

アプリケーション管理者は、マルチテナンシーを実装できます。

マルチテナンシー機能を使用すると、複数の CA Configuration Automation サーバ インスタンス間でマスタ/テナントの関係を確立できます。 マスタ サーバには、必要な数だけテナントを存在させることができます。 これにより、大規模な CA Configuration Automation 実装環境において、1 つのマスタ CA Configuration Automation サーバ が、他のテナント CA Configuration Automation サーバ を管理するポータルとして機能することが可能になります。 たとえば、大陸ごとに 1 つのテナントを持つなど、テナントを地理的に分類できる場合があります。 また、サービス プロバイダが、マスタ サーバ上で管理機能を実行している間に、各クライアントにテナント CA Configuration Automation インスタンスを提供するためにマルチテナンシーを使用することもできます。

マルチテナンシー管理機能によって、CA Configuration Automation コンポーネント（カスタムのブループリント、ネットワーク プロファイル、管理プロファイルを含む）をマスタからテナントに容易に展開できるようになります。

以下は、マルチテナンシーの実装に関係するタスクを示しています。



アプリケーション管理者は、マルチテナンシーを実装するために以下のタスクを実行できます。

1. マスタ インスタンスを定義 (P. 137) します。
2. テナントを作成 (P. 137) します。
3. ユーザを作成および管理 (P. 139) します。
4. テナントへのユーザ アクセスを定義 (P. 141) します。

5. テナントにオブジェクトをインポート (P. 141) します。
6. テナント詳細を表示および編集 (P. 143) します。

マスタ インスタンスの定義

マスタ インスタンスは、CA Configuration Automation サーバ のインストール中に定義されます。

［サーバ タイプ］画面で［テナント マスタ］オプションを選択します。このオプションは、CA Configuration Automation サーバ のマスタ インスタンスをインストールするように指定します。 マスタ インスタンスは、マスタ テナントや他のテナント上でデータにアクセスまたは管理できない複数のテナント インスタンスをホストできます。

テナントの作成

マスタ/テナントの関係は以下の 2 とおりの方法で定義できます。

- ［サーバ タイプ］画面で、CA Configuration Automation サーバ のインストール中に、［テナント］オプションを選択し、マスタ サーバ認証情報を指定します。この情報は、テナント管理 UI に渡され、［テナント］タブ ページのテーブルに表示されます。
- テナント管理 UI で、［テナント］タブ ページの［テナントの作成］オプションを選択します。［テナントの作成］機能を使用して、以前にインストールされた CA Configuration Automation サーバ インスタンスをテナントとして定義することができます。

  注: 以前のリリースからの CA Configuration Automation サーバ インスタンスを使用してテナントを作成することはできません。

次の手順に従ってください:

1. マスタ CA Configuration Automation サーバ 上のテナント管理 UI にログインし、［テナント］タブをクリックします。

   ［テナント］テーブルが表示され、テナントの作成機能を使用してこのマスタ サーバに対して作成されたテナントが示されます。

2. ［テーブル アクション］ドロップダウン リストから［テナントの作成］を選択します。

   ［テナントの作成］ページが表示されます。

3. 対応するフィールドに以下の情報を入力し、［完了］をクリックします。

   名前

   テナント名を指定します。

   説明

   テナントに関する詳細を指定します。

   サーバ名

   CA Configuration Automation サーバ テナント インスタンスを指定します。 これは、サーバ名または IP アドレス（IPv4 または IPv6）のいずれかになります。

   ポート

   テナント CA Configuration Automation サーバ のリスニング ポートを指定します。

   SSL 有効

   テナントとマスタ サーバの間の通信を保護するために SSL を使用するかどうかを指定します。

   閲覧ユーザ

   マスタ インスタンス上のテナント管理 UI からテナントを表示および管理できるユーザを指定します。 ［利用可能な閲覧ユーザ］列でユーザをダブルクリックすると、［選択された閲覧ユーザ］列に移動します。

   テナントが作成され、［テナント］テーブルに表示されます。［テナント］ペインでは、テナントの参照が許可されたユーザに対して表示されます。

ユーザの作成および管理

CA Configuration Automation ユーザは、CA Configuration Automation サーバ UI または CA EEM UI のいずれかを使用して定義します。 いずれの場合も、［管理環境］パネルをクリックし、［アクセス管理］タブの［ユーザ］リンクをクリックします。機能は 2 つの場所のどちらでもまったく同じです。

テナント UI のユーザを以下の事前定義済みユーザ グループのいずれかまたは両方に追加できます。

テナント管理者

メンバは、アクセス権限を持つテナント インスタンス上のテナント管理 UI で管理機能にアクセスできます。［テナント］ペインには、管理者 UI を開くための［環境管理］リンクが含まれています。このペインには、選択されたテナント上で CA Configuration Automation サーバ UI を開くためのリンクも含まれます。

テナント閲覧ユーザ

メンバは、［テナント］ペインに表示されるテナント インスタンス上で CCA サーバ UI にアクセスできます。

注: テナント閲覧ユーザ権限は、［テナント］ペインでテナントを表示するために必要です。

次の手順に従ってください:

1. マスタ CA Configuration Automation サーバ でテナント管理 UI にログインし、［テナント］タブをクリックします。

   ［テナント］ペインおよびテナント テーブルが表示されます。このマスタ サーバに対して設定されたテナントが表示されます。

2. ［テナント］ペインで、ユーザを追加または変更する対象のテナント名をクリックします。

   選択したテナントに対して CA Configuration Automation サーバ UI が表示されます。

3. ［環境管理］リンクをクリックし、［アクセス管理］タブの［ユーザ］リンクをクリックします。

   ［ユーザの検索］および［ユーザ］ペインが表示されます。

4. 以下のいずれかのタスクを実行します。
   - CA Configuration Automation 製品ガイドの説明に従ってユーザを追加します。 以下の点に注意してください。
     - ［アプリケーション ユーザの詳細の追加］をクリックし、AppInstanceName フィールドに「**CCA**」と入力します。
     - ［CCA テナント管理者］または［CCA テナント閲覧ユーザ］グループにユーザを追加します。
     - ［保存］をクリックします。
   - ユーザの変更
     - ［ユーザの検索］ペインの［値］フィールドにユーザ名を入力し、［実行］をクリックします。
     - ［ユーザ］ペインのツリーでユーザ名をクリックします。右の［ユーザ］ペインに、選択したユーザの詳細が表示されます。
     - ［CCA テナント管理者］または［CCA テナント閲覧ユーザ］グループにユーザを追加します。
     - ［保存］をクリックします。
5. ［テナント］ペインで［環境管理］リンクをクリックします。
6. テナント管理 UI で、［ユーザ］タブをクリックします。

   ［選択された管理者］または［選択された閲覧ユーザ］列に、手順 4 で作成したユーザが表示されます。

テナントへのユーザ アクセスの定義

CCA テナント閲覧ユーザ グループのメンバとしてユーザを定義したら、各テナントにアクセス可能なユーザを指定できます。

1. マスタ CA Configuration Automation サーバ でテナント管理 UI にログインし、［テナント］タブをクリックします。
2. 右ペインの［名前］列で、テナント名をクリックします。

   選択したテナントに対して［テナント プロパティ］ページが表示されます。
3. ［利用可能なテナント］列で、このテナントにアクセスできる各閲覧ユーザをダブルクリックします。

   選択した閲覧ユーザが［選択された閲覧ユーザ］列に移動し、テナントへのアクセス権限が付与されます。［選択された閲覧ユーザ］列のユーザがテナント ポータルにログインすると、選択したテナントが［テナント］ペインに表示されます。

   注: 選択したテナントがテナント グループのメンバである場合、このユーザはテナント グループ内のすべてのメンバにアクセスできます。

テナントへのオブジェクトのインポート

以下のオブジェクトを 1 つ以上のテナントにインポートできます。

- 管理プロファイル
- ブループリント
- ファイル構造クラス
- ネットワーク スキャン ポリシー
- 通知プロファイル
- ルール グループ
- 修復プロファイル
- ダッシュボード
- グラフ
- ブループリント グループ
- テーブル ビュー

- アプリケーション マッピング
- Catalyst プロファイル
- プロパティ

注: テナント インスタンスをにオブジェクトをインポートする前に、CA Configuration Automation サーバ インスタンスから Java Archive（JAR）としてオブジェクトをエクスポートします。 オブジェクトのエクスポートに関する詳細については、「製品ガイド」または CA Configuration Automation サーバ オンライン ヘルプを参照してください。

次の手順に従ってください:

1. マスタ CA Configuration Automation サーバ 上のテナント管理 UI にログインし、［インポート］タブをクリックします。
2. ［タイプ］ドロップダウン リストで、インポートするオブジェクト タイプを選択します。
3. ［参照］をクリックし、エクスポートされた JAR ファイルにアクセスして［開く］をクリックします。

   ［インポートする JAR ファイル］フィールドに、選択したファイルが表示されます。
4. （オプション）［既存のオブジェクトを上書き］チェック ボックスをオンにすると、インポートしているファイルと同じ名前のファイルが存在する場合に上書きします。
5. ［利用可能なテナント］列で、オブジェクトをインポートする対象のテナントを 1 つ以上ダブルクリックします。
6. ［インポート］をクリックします。

   選択したテナントにオブジェクトがインポートされます。

テナント詳細の表示および編集

テナントを作成したときに指定したテナント詳細は表示および編集できます。

次の手順に従ってください:

1. マスタ CA Configuration Automation サーバ でテナント管理 UI にログインし、［テナント］タブをクリックします。
2. 右ペインの［名前］列で、テナント名をクリックします。

   選択したテナントに対して［テナント プロパティ］ページが表示されます。
3. 必要に応じてフィールドを編集し、［保存］をクリックします。

   フィールドの詳細については、「テナントの作成 (P. 137)」を参照してください。

第 5 章: ルールの概要および作成

制約ルールは、特定のタイプの CA Configuration Automation のエレメントに対して値制約を設定するために使用されます。具体的には、以下のような制約ルールがあります。

- ［インジケータ］-［検証ルール］フォルダ内のルール（［コンポーネント ブループリント］のみ）
- ［パラメータ］フォルダ内のパラメータ（［サービス］のみ）
- ［管理対象］-［ファイル システム オーバレイ］内のファイルおよびディレクトリ
- ［管理対象］-［レジストリ オーバーレイ］フォルダ内のレジストリ キーおよび値
- ［パラメータ］-［ルール］フォルダ内のパラメータ
- ［構成］-［構造クラス］フォルダ内のパラメータ
- ［構成］フォルダ内のファイル

制約ルールは必ずエレメントと 1 対 1 で関連付けられています。また、下層の［コンポーネント ブループリント］に作成され、そこから継承できます。あるいは、サービス インスタンス内に作成され、そのインスタンスに直接適用することもできます。 作成する*明示的な*制約ルールに加えて、CA Configuration Automation の*暗黙的な*組み込みルールがあります。たとえば、エレメントに対して特定の値またはデータ タイプを指定した場合、CA Configuration Automation は組み込みの［デフォルトの確認］ルールまたは［データ タイプの検証］ルールを自動的に作成します。

注: 可能な場合は、［コンポーネント ブループリント］内の制約ルールを作成することを検討してください。 一度作成したルールは、下層の［コンポーネント ブループリント］を使用するサービスによって自動的に継承されます。

制約ルールの開始、表示、および編集は、選択した［コンポーネント ブループリント］の［ルール］フィールドから行われます。

定義された制約ルールの数または［なし］が、［ルール］の右側にある角かっこに表示されます。 ドロップダウン リストから、特定の制約ルールの表示、すべての制約ルールの表示、または制約ルールの追加が可能です。

- ［すべてのルールを表示...］を選択すると、新しいページが開き、すべての制約ルールのリストが表形式で表示されます。 テーブルの並べ替え順序を変更するには、テーブルのいずれかの見出しをクリックします。
- ［新しいルール...］を選択すると、［ルール］属性シートが表示されます。
- 特定の制約ルールを選択すると、名前が［ルール］フィールドに表示され、その制約ルールの属性シートが表示されます。 属性シートからほとんどのルールを編集または削除することができます。 ただし、CA Configuration Automation の組み込みまたは*暗黙*のルール（［デフォルトの確認］または［データ タイプの検証］など）を編集または削除することはできません。 これらの組み込みルールは表示のみ可能です。

［コンポーネント ブループリント］にデフォルト値が指定されている場合、組み込みの［デフォルトの確認］ルールが自動的に作成されます。 これらのデフォルト ルールは情報であり（［ルール コンプライアンス］にアイコンで［情報］として表示されます）、推奨されるデフォルト値から逸脱する値がある場合、それを認識できます。

明示的に定義された制約ルールは、それらの値をエレメント自体から、またはエレメントのいずれかの属性から取得します。 利用可能な属性および値タイプは CA Configuration Automation 内のエレメントごとに異なります。 したがって、制約ルールはエレメント タイプによって大幅に異なります。 例：

エレメント タイプ	正当な制約ルール
ファイル	■ ファイル サイズ ■ ファイル変更時刻 ■ ファイル所有者 ■ ファイル アクセス権 ■ ファイル バージョン ■ 製品バージョン

エレメント タイプ	正当な制約ルール
ディレクトリ	■ ディレクトリ数 ■ ファイル数 ■ バイト数 ■ 階層数 ■ ディレクトリ変更時刻 ■ ディレクトリ所有者 ■ ディレクトリ アクセス権 ■ ディレクトリが存在する必要がある ■ ファイルが存在している必要がある
ルール、パラメータ、グループ、レジストリ キー、および値	■ 値

第 6 章: ディレクティブの概要および作成

ディレクティブは、サービス内で管理されるエレメントから値を抽出するため、または CA Configuration Automation エージェントを使用して管理対象サーバから値を取得するために使用されます。4 つのディレクティブ タイプを以下に示します。

- 検証ディレクティブ - インストールが不完全なコンポーネント、間違ったバージョンのコンポーネント、または特定のサービスに関係のないコンポーネントを最初に検出して除外します。
- パラメータ ディレクティブ - ファイル システムやレジストリのルート、コンポーネント バージョン、ベンダー、データベース接続情報など、コンポーネントを特定および識別するために不可欠なパラメータを定義します。
- 実行可能ディレクティブ - サーバから構成情報を抽出および解釈するためのディレクティブを定義します。
- マクロ ステップ ディレクティブ - コンポーネント ブループリントによって管理されているデータが含まれるサーバに固有の問題に関する診断を支援し、システム情報、メモリ統計、またはディスク ボリューム統計の表示など、サーバまたはサービスに関する追加情報を提供します。

以下の各セクションで、これらのディレクティブについて詳しく説明します。

検証ディレクティブ

検証に関連する値のディレクティブを［コンポーネント ブループリント］で開始するには、［インジケータ］の検証ディレクティブ エレメントを 選択し、［ディレクティブの追加］をクリックします。 既存の検証ディレクティブは、検証ディレクティブ エレメントを選択するとき表示される検証ディレクティブ ツリーから表示および編集します。

表示されるフィールドは、選択するディレクティブ タイプによって変わります。

例:

- Oracle 8i Database（UNIX）v8.* コンポーネント ブループリントは、［リモート実行］検証ディレクティブを定義します。これは、SQL Plus を使用してバージョンを取得し、検出されたコンポーネントがバージョン 8 であることを確認します。
- Apache HTTP Server（UNIX）v1.3.* コンポーネント ブループリントは、［定数］検証ディレクティブを定義します。これは、バージョン情報を取得し、検出されたコンポーネントがバージョン 1.3.* であることを確認します。

  注: 一致させる正規表現の例ではワイルドカード（*）を使用しています。 ディスカバリでは、1.3 で始まるバージョンがすべて検索されます。

パラメータ ディレクティブ

パラメータに関連する値のディレクティブを［コンポーネント ブループリント］で開始するには、［パラメータ］のディレクティブ エレメントを選択し、［ディレクティブの追加］をクリックします。既存のパラメータ ディレクティブは、パラメータ ディレクティブ エレメントを選択するとき表示されるパラメータ ツリーから表示および編集されます。

表示されるフィールドは、選択したディレクティブ タイプによって異なります。

例：

- WIN32 v*.* コンポーネント ブループリントは、サービス内で検出された Windows オペレーティング システム コンポーネントのパラメータで製品名および関連するサービス パック バージョンを表示する［定数］パラメータ ディレクティブを定義します。
- 同様の WIN32 v*.* コンポーネント ブループリントは、サービス内で検出された Windows オペレーティング システム コンポーネントのパラメータでベンダーを表示する［定数］パラメータ ディレクティブを定義します。

構成実行可能ディレクティブ

構成実行ファイルに関連する値のディレクティブを［コンポーネント ブループリント］で開始するには、［構成］の実行可能エレメントを選択し、［ディレクティブの追加］をクリックします。 既存の実行可能ディレクティブは、構成実行可能ディレクティブ エレメントを選択するとき表示される実行可能ディレクティブ ツリーから表示および編集されます。

表示されるフィールドは、選択したディレクティブ タイプによって異なります。

例：

- Active Directory Service v*.* コンポーネント ブループリントは、FSMO 役割を取得する LDAP の取得構成実行可能ディレクティブを定義します。
- BIG-IP Load Balancer v*.* コンポーネント ブループリントは、指定された MIB アドレスにある値を取得する SNMP の取得構成実行可能ディレクティブを定義します。

マクロ ステップ ディレクティブ

マクロ ステップに関連する値のディレクティブを［コンポーネント ブループリント］で開始するには、［診断］、［マクロまたはユーティリティ］、［マクロ］の下にあるマクロ エレメントを選択し、［ステップの追加］をクリックします。 既存のマクロ ステップは、マクロ ステップ エレメントを選択するとき表示されるマクロ ステップ ツリーから表示および編集されます。

表示されるフィールドは、選択したディレクティブ タイプによって異なります。

例

- IBM WebSphere 6 Server Instance (UNIX) v6.* コンポーネント ブループリントは、ヘルプ オプションで WebSphere Server を開始するリモート実行マクロ ステップ ディレクティブを定義します。
- BIG-IP Load Balancer v*.* コンポーネント ブループリントは、指定された MIB アドレスにある総稼働時間の値を取得する SNMP の取得マクロ ステップ ディレクティブを定義します。

付録 A: UNIX および Linux Softagent ディスカバリの sudo の設定

NDG Softagent を使用して UNIX および Linux サーバを検出する場合、NDG は認証情報ボールトで提供される認証情報のセットを使用して、UNIX および Linux ホストへの SSH 接続の確立を試行します。 UNIX/Linux セキュリティの設定方法によっては、NDG Softagent によって発行される一部のコマンドに関して非 root ユーザには権限がないため、サーバのデータ検出数が少なくなる可能性があります。

非 root ユーザがディスカバリ関連コマンドを発行できないようにするために、以下のオプションがあります。

- 認証情報ボールトで root ユーザ認証情報を提供することによって、すべてのディスカバリ関連コマンドが root として発行されるようにします。 これにより、コマンドの権限が保証されます。
- sudo コマンドを使用して、非 root ユーザが root の認証情報を提供する必要なしに、root の権限でディスカバリ関連コマンドを発行できるようにします。

また、sudo ユーザに関連付けられたユーザ ID のパスも定義する必要があります。このパスには、NDG ディスカバリが使用する以下コマンドおよびユーティリティの場所がすべて含まれます。

- /bin
- /sbin
- /usr/sbin
- /opt/xensource/bin

sudo を使用して非 root ユーザに権限を与えるように /etc/sudoers ファイルを設定する方法

1. visudoers コマンドを使用して、/etc/sudoers ファイルを編集します。
2. ユーザ ndguser が root の認証情報を求められずに、sudo を使用してすべての NDG Softagent コマンドを発行できるように、以下のエントリを作成します。

```
# simple entry for ndg discovery if client does not need granularity
# ndguser ALL=NOPASSWD: ALL
# detailed entry for ndg discovery permitting only those commands used by discovery

ndguser ALL = NOPASSWD: /bin/uname, /bin/echo, /bin/cat, ¥
                        /bin/domainname, /bin/hostname, ¥
                        /bin/netstat, /bin/df, /bin/ps, /bin/rpm, ¥
                        /bin/ls, /sbin/ifconfig, /sbin/ip, ¥
                        /sbin/mii-tool, /sbin/chkconfig, ¥
                        /sbin/sfdisk, /usr/sbin/dmidecode, ¥
                        /usr/bin/cdrecord, ¥
                        /opt/xensource/bin/xe, /bin/lshmc
```

   注: ndguser を作成する代わりに、このエントリを変更して既存ユーザに権限を与えることもできます。パスワードを求められずにすべてのコマンドを発行できるように /etc/sudoers ファイルにユーザがすで設定されている場合、またはすべてのコマンドを含む詳細なリストがすでに提示されている場合、そのユーザを認証情報ボールトに追加することにより、そのユーザを変更することなくそのまま使用できます。

3. sudoers ファイルを保存して閉じます。
4. 「ネットワーク スキャン ポリシーの作成」に記載のとおり、［ネットワーク スキャン ポリシー］ページの［sudo 使用の有効化］チェックボックスをオンにします。

sudo ユーザのパスを定義する方法

1. UNIX または Linux システムのシェルのシェル構成ファイル（通常はユーザの $HOME ディレクトリ内の .bashrc）を編集し、以下の行をユーザの PATH 定義に追加します。

```
PATH=$PATH:/bin:/sbin:/usr/sbin:/opt/xensource/bin
export PATH
```

2. ファイルを保存して閉じます。

付録 B: CA Configuration Automation タスクと CA EEM 権限のマッピング

この付録では、CA Configuration Automation UI タスクと、そのタスクの実行に必要な CA EEM 権限をマップします。CA Configuration Automation タスク別に UI 上の場所を示し、［テーブル アクション］ドロップダウンの［アクションの選択］ドロップダウン リストからどのタスクを選択するかを説明します。

CA EEM 権限については、ポリシーおよび対応するアクションとの関係で説明します。

注:

- すべてのユーザが CA Configuration Automation UI 全体に対して表示権限を持っています。
- 操作の権限付与に失敗した場合、エラー メッセージが表示されます。
- CA EEM はポリシー評価を実行します
- ポリシーはユーザに直接割り当てるか、ユーザ グループに割り当てることができます

このセクションには、以下のトピックが含まれています。

サービス オプション

サービス オプション	CA EEM ポリシーおよびアクション
サービスの削除	サービス管理、削除
スナップショットの作成	サービス管理、作成
変更検出の実行	サービス管理、run_change_detection
比較の実行	サービス管理、run_compare
ルール コンプライアンスの実行	サービス管理、run_rule_compliance
サービスのリフレッシュ	サービス管理、リフレッシュ
ディスカバリの実行	サービス管理、run_discovery
ディスカバリの停止	サービス管理、stop_discovery
管理プロファイルの実行	サービス管理、run_management_profile

管理プロファイルの割り当て	サービス管理、更新
サービスのエクスポート	サービス管理、エクスポート
すべてのサービスの表示	すべてのユーザにビュー権限を付与
サービスの作成	サービス管理、作成
サービスの更新	サービス管理、更新
サービスのインポート	サービス管理、インポート

サービス スナップショット オプション

サービス スナップショット オプション	CA EEM ポリシーおよびアクション
すべてのスナップショットの表示	すべてのユーザにビュー権限を付与
スナップショットの削除	サービス管理、削除
ゴールド基準として設定	サービス管理、更新
シルバー基準として設定	サービス管理、更新
ブロンズ基準として設定	サービス管理、更新
ベースラインとして設定	サービス管理、更新
ゴールド基準の削除	サービス管理、更新
シルバー基準の削除	サービス管理、更新
ブロンズ基準の削除	サービス管理、更新
ベースライン指定の削除	サービス管理、更新
スナップショットのエクスポート	サービス管理、エクスポート

サービス コンポーネント オプション

サービス コンポーネント オプション	CA EEM ポリシーおよびアクション
コンポーネントの削除	サーバ管理、削除
コンポーネントのリフレッシュ	サーバ管理、更新

コンポーネントの表示	すべてのユーザにビュー権限を付与

サーバ オプション

サーバ オプション	CA EEM ポリシーおよびアクション
サーバの削除	サーバ管理、削除
サーバの管理	サーバ管理、更新
サーバの拒否	サーバ管理、更新
サーバのテスト	サーバ管理、test_servers
スナップショットの作成	サーバ管理、作成
変更検出の実行	サーバ管理、run_change_detection
比較の実行	サーバ管理、run_compare
ルール コンプライアンスの実行	サーバ管理、run_rule_compliance
サーバのリフレッシュ	サーバ管理、リフレッシュ
ディスカバリの実行	サーバ管理、run_discovery
ディスカバリの停止	サーバ管理、stop_discovery
管理プロファイルの実行	サーバ管理、run_management_profile
プロファイルの割り当て	サーバ管理、更新
保護エージェント	CCA 管理者アクセス、更新、および サーバ管理、install_uninstall_agent
エージェントのインストール	サーバ管理、install_uninstall_agent
エージェントのアンインストール	サーバ管理、install_uninstall_agent
すべてのサーバの表示	すべてのユーザにビュー権限を付与
サーバの作成	サーバ管理、作成
ファイルからサーバを追加	サーバ管理、作成
サーバの更新	サーバ管理、更新
サーバのインポート	サーバ管理、作成

サーバ スナップショット オプション

サーバ スナップショット オプション	CA EEM ポリシーおよびアクション
スナップショットの削除	サーバ管理、削除
ゴールド基準として設定	サーバ管理、更新
シルバー基準として設定	サーバ管理、更新
ブロンズ基準として設定	サーバ管理、更新
ベースラインとして設定	サーバ管理、更新
ゴールド基準の削除	サーバ管理、更新
シルバー基準の削除	サーバ管理、更新
ブロンズ基準の削除	サーバ管理、更新
ベースライン指定の削除	サーバ管理、更新
スナップショットのエクスポート	サーバ管理、エクスポート
スナップショットのインポート	サーバ管理、インポート
すべてのスナップショットの表示	すべてのユーザにビュー権限を付与

サーバ コンポーネント オプション

サーバ コンポーネント オプション	CA EEM ポリシーおよびアクション
コンポーネントの削除	サーバ管理、更新
コンポーネントのリフレッシュ	サーバ管理、更新
コンポーネントの表示	すべてのユーザにビュー権限を付与

サーバ グループ オプション

サーバ グループ オプション	CA EEM ポリシーおよびアクション
サーバ グループの作成	サーバ管理、作成

サーバ グループの更新	サーバ管理、更新
サーバ グループの表示	すべてのユーザにビュー権限を付与

管理プロファイル オプション

管理プロファイル オプション	CA EEM ポリシーおよびアクション
デフォルト プロファイルとして設定	管理プロファイル管理、更新
プロファイルの有効化	管理プロファイル管理、更新
プロファイルの無効化	管理プロファイル管理、更新
プロファイルの削除	管理プロファイル管理、削除
プロファイルの作成*	管理プロファイル管理、作成
プロファイルの更新	管理プロファイル管理、更新
プロファイルのエクスポート	管理プロファイル管理、エクスポート
プロファイルのインポート	管理プロファイル管理、インポート
プロファイルの実行	サーバ管理、run_management_profile および サービス管理、run_management_profile
プロファイルの表示	すべてのユーザにビュー権限を付与

ネットワーク プロファイル オプション

ネットワーク プロファイル オプション	CA EEM ポリシーおよびアクション
デフォルト プロファイルとして設定	ネットワーク管理、更新
プロファイルの有効化	ネットワーク管理、更新
プロファイルの無効化	ネットワーク管理、更新
プロファイルの削除	ネットワーク管理、削除

プロファイルの作成	ネットワーク管理、作成
プロファイルの更新	ネットワーク管理、更新
プロファイルの表示	すべてのユーザにビュー権限を付与

ネットワーク スキャン ポリシー オプション

ネットワーク スキャン ポリシー オプション	CA EEM ポリシーおよびアクション
ネットワーク スキャン ポリシーの削除	ネットワーク管理、削除
ネットワーク スキャン ポリシーの作成	ネットワーク管理、作成
ネットワーク スキャン ポリシーのインポート	ネットワーク管理、インポート
ネットワーク スキャン ポリシーのエクスポート	ネットワーク管理、エクスポート
ネットワーク スキャン ポリシーの更新	ネットワーク管理、更新
ネットワーク スキャン ポリシーの表示	すべてのユーザにビュー権限を付与

アクセス プロファイル オプション

アクセス プロファイル オプション	CA EEM ポリシーおよびアクション
アクセス プロファイルの削除	アクセス プロファイル管理、削除
アクセス プロファイルの作成	アクセス プロファイル管理、作成
アクセス プロファイルのインポート	アクセス プロファイル管理、インポート
アクセス プロファイルのエクスポート	アクセス プロファイル管理、エクスポート
アクセス プロファイルの更新	アクセス プロファイル管理、更新
アクセス プロファイルの表示	すべてのユーザにビュー権限を付与

認証情報ボールト プロファイル オプション

認証情報ボールト プロファイル オプション	CA EEM ポリシーおよびアクション
デフォルト プロファイルとして設定	ネットワーク管理、更新
認証情報ボールト プロファイルの削除	ネットワーク管理、削除
認証情報ボールト プロファイルの作成	ネットワーク管理、作成
認証情報ボールト プロファイルの更新	ネットワーク管理、更新
認証情報ボールト プロファイルの表示	すべてのユーザにビュー権限を付与

通知プロファイル オプション

通知プロファイル オプション	CA EEM ポリシーおよびアクション
デフォルト プロファイルとして設定	通知プロファイル管理、更新
通知プロファイルの削除	通知プロファイル管理、削除
通知プロファイルの作成	通知プロファイル管理、作成
通知プロファイルの更新	通知プロファイル管理、更新
通知プロファイルの表示	すべてのユーザにビュー権限を付与

ブループリント オプション

ブループリント オプション	CA EEM ポリシーおよびアクション
ブループリントのコピー	ブループリント管理、コピー

ブループリントの削除	ブループリント管理、削除
ディスカバリの有効化	ブループリント管理、更新
ディスカバリの無効化	ブループリント管理、更新
ブループリントのエクスポート	ブループリント管理、エクスポート
ブループリントのインポート	ブループリント管理、インポート
ブループリントの作成	ブループリント管理、作成
ブループリントの更新	ブループリント管理、更新
ブループリントの表示	すべてのユーザにビュー権限を付与

構造クラス オプション

構造クラス オプション	CA EEM ポリシーおよびアクション
構造クラスのコピー	ブループリント管理、作成
構造クラスの削除	ブループリント管理、削除
構造クラスの作成	ブループリント管理、作成
構造クラスのインポート	ブループリント管理、インポート
構造クラスのエクスポート	ブループリント管理、エクスポート
構造クラスの更新	ブループリント管理、更新
構造クラスの表示	すべてのユーザにビュー権限を付与

グローバル変数オプション

グローバル変数オプション	CA EEM ポリシーおよびアクション
グローバル変数の削除	ブループリント管理、削除
グローバル変数の作成	ブループリント管理、作成
グローバル変数のインポート	ブループリント管理、インポート
CSV にエクスポート	ブループリント管理、エクスポート

グローバル変数の更新	ブループリント管理、更新
グローバル変数の表示	すべてのユーザにビュー権限を付与

コンプライアンス管理オプション

コンプライアンス管理オプション	CA EEM ポリシーおよびアクション
コンプライアンス プロファイルの作成	コンプライアンス管理、作成
コンプライアンス プロファイルの削除	コンプライアンス管理、削除
コンプライアンス プロファイルの更新	コンプライアンス管理、更新
ジョブの実行	コンプライアンス管理、run_job

ダッシュボード オプション

ダッシュボード オプション	CA EEM ポリシーおよびアクション
ダッシュボードの作成	ダッシュボード管理、作成
ダッシュボードのインポート	ダッシュボード管理、インポート
ダッシュボードのエクスポート	ダッシュボード管理、エクスポート
ダッシュボードの更新	ダッシュボード管理、更新
ダッシュボードの削除	ダッシュボード管理、削除
ダッシュボードの表示	すべてのユーザにビュー権限を付与

修復オプション

修復オプション	CA EEM ポリシーおよびアクション
修復を許可	修復管理、許可

レポート オプション

レポート オプション	CA EEM ポリシーおよびアクション
レポートの実行	レポート管理、実行
レポートの保存	レポート管理、作成
レポートの更新	レポート管理、更新
レポートの削除	レポート管理、削除
レポートのスケジュール	レポート管理、実行
保存済みレポートの表示 レポート テンプレートの表示	すべてのユーザにビュー権限を付与

環境管理オプション

管理オプション	CA EEM ポリシーおよびアクション
アクセス管理	CCA 管理者アクセス、更新
構成、セキュリティ証明書	CCA 管理者アクセス、更新