CA Server Automation

管理ガイド

リリース 12.8

CA Technologies 製品リファレンス

このドキュメントは、以下の CA Technologies 製品およびコンポーネント、またはサードパーティ コンポーネントへの参照を含む場合があります。

- CA Configuration Automation （以前は CA Application Configuration Manager （CA ACM））
- CA eHealth®
- CA Embedded Entitlements Manager （CA EEM）
- CA IT Asset Manager （CA ITAM）
- CA ITCM （CA IT Client Manager）
- CA NSM （CA Network and Systems Management）
- CA Network Automation™
- CA Patch Manager
- CA Process Automation（以前は CA IT Process Automation Manager（CA IT PAM））
- CA Server Automation
- CA Service Desk Manager （CA SDM）
- Software Delivery （CA IT Client Manager のコンポーネント）
- CA Spectrum® Infrastructure Manager（CA Spectrum）
- CA SystemEDGE
- Racemi DynaCenter®

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

付録 C: トラブルシューティング 1231

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

関連ドキュメント

CA マニュアル選択メニューでは、以下の CA Server Automation マニュアルを提供します。

管理ガイド

管理者向けに製品アーキテクチャ、トラブルシューティング、概念、および設定タスクを説明します。

インストール ガイド

CA Server Automation のインストール前提条件、ベスト プラクティス、およびプロシージャを説明します。

リファレンス ガイド

AutoShell、CLI スクリプト コマンド、およびログ ファイルに関する詳細情報を提供します。

パフォーマンス メトリック参照

サポート対象プラットフォームのシステム パフォーマンスのモニタリングに利用可能なパフォーマンス メトリックについて説明します。

CA Process Automation コネクタ リファレンス ガイド

CA Process Automation コネクタおよびユース ケースに関する詳細情報を提供します。

オンライン ヘルプ

CA Server Automation ユーザ インターフェースを使用してタスクを完了するために役立つ情報を提供します。

予約マネージャ ヘルプ

ユーザと管理者が、予約マネージャ ユーザ インターフェースを使用してタスクを完了するために役立つ情報を提供します。

リリース ノート

新機能と変更された機能に関する情報、およびオペレーティング システムのサポート、システム要件、テクニカル サポートへの問い合わせ方法などの製品実装情報を提供します。

サービス レスポンス モニタリング ユーザ ガイド

SRM のインストールおよび設定の詳細が記載されています。

SystemEDGE ユーザ ガイド

SystemEDGE エージェントに関するエンドユーザ情報を提供します。

SystemEDGE リリース ノート

新機能と変更された機能に関する情報、およびオペレーティング システムのサポート、システム要件、テクニカル サポートへの問い合わせ方法などのエージェント実装情報を提供します。

さらに、CA マニュアル選択メニューでは以下の Rapid Server Imaging（RSI）サーバ ガイドを提供します。

- *RSI サーバ管理ガイド*
- *RSI サーバ インストール ガイド*
- *RSI サーバ リリース ノート*

PDF マニュアルを表示するには、Adobe の Web サイトから Adobe Reader をダウンロードしてインストールします（コンピュータにまだインストールされていない場合）。

規則

このガイドでは、以下の規則を使用します。

大文字と小文字の区別

このガイドで言及されるクラス、コマンド、ディレクティブ、環境パラメータ、関数、プロパティの名前はすべて大文字と小文字を区別します。また、記載されているとおりに正確に入力する必要があります。システム コマンドと環境変数名は、オペレーティング システムの要件に応じて、大文字と小文字が区別される*場合があり*ます。

相互参照

他のガイド、またはこのガイドの他のセクション内の情報への参照は、以下の形式で表示されます。

ガイド名

別のガイドの名前を示します。

「章名」

このガイドまたは別のガイドの章の名前を示します。

同義語

属性、オブジェクト、オブジェクト識別子（OID）などの用語は、このドキュメントでは「変数」と同義です。

SystemEDGE エージェント、CA SystemEDGE などの用語は、このドキュメントでは SystemEDGE と同義です。

構文

構文とユーザ入力では、以下の形式を使用します。

斜体

実際の値を指定する必要がある変数名またはプレースホルダを示します。

{a|b}

オペランド a または b を選択する必要があることを示します。

[ ] または [[ ]]

オプションのオペランドを示します。

構文例

以下の例は、上記の規則を使用しています。

`modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset -session ssh`

オペランド -min および -max は必須ですが、プロセッサ セット内の CPU の最小数または最大数のどちらを定義するかに応じて、いずれか 1 つのみを使用します。オペランド -m は、指定しなくてもこのコマンドは機能します。 コマンドのほかの部分は記載されているとおりに入力する必要があります。

デフォルト ディレクトリ

パス ステートメント内で使用する *CASYSEDGE* は、SystemEDGE がインストールされているディレクトリを示します。 **デフォルト：** C:¥Program Files¥CA¥SystemEDGE.

インストール パス

パス ステートメント内で使用する *Install_Path* は、CA Server Automation または CA Server Automation コンポーネントがインストールされているディレクトリを示します。

デフォルト

- Windows x86： C:¥Program Files¥CA
- Windows x64： C:¥CA、C:¥Program Files (x86)¥CA、または C:¥Program Files¥CA
- UNIX、Linux： /opt/CA

第 2 章: 概要

このセクションには、以下のトピックが含まれています。

アーキテクチャ

CA Server Automation はポリシーベースの製品であり、物理および仮想リソースのモニタ、再設定、プロビジョニングを行って、複雑なサービス指向のデータ センターの負荷要求に対応します。 CA Server Automation は、サービス指向アーキテクチャ (SOA) 上に構築されており、データ センターを継続的に分析して、サーバが必要なタスクを実行するために最適にプロビジョニングされるようにします。 Web -ベースの CA Server Automation ユーザ インターフェースを使用して、データ センターを管理したり、データ センター内の各管理対象システムに関する詳細情報を取得したりできます。

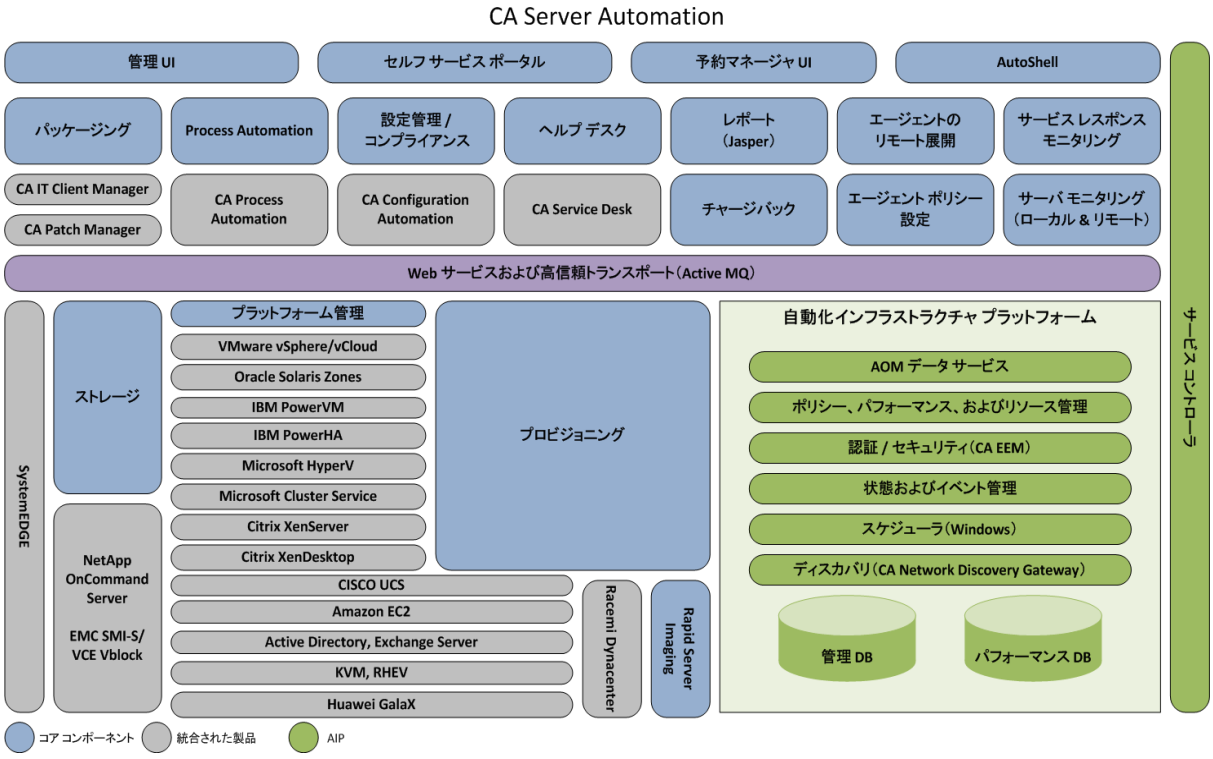
CA Server Automation を使用して、以下の CA 技術を活用できます。

- 要求のエスカレーションおよび解決に役立つ CA Service Desk Manager （CA SDM）
- セキュリティを高める CA Embedded Entitlements Manager （CA EEM）
- 軽量スタンドアロン ディスカバリ機能を備えた Network Discovery Gateway
- オペレーティング システムおよびアプリケーションの展開のための CA IT Client Manager （CA ITCM）
- パッチの保守および関連データ センター リソースへの配信を行う CA Patch Manager
- ディスカバリおよび変更管理を行う CA Configuration Automation
- データ センターのワークフロー プロセスを自動化する CA Process Automation

CA Server Automation は以下の外部テクノロジと統合されます。

- 異種混合のハードウェア プロビジョニングおよび仮想化を行う Cisco Unified Computing System （UCS）
- VMware vSphere/vCloud （仮想マシン（VM）と vApp のオペレーティング環境の管理）
- 仮想マシン オペレーティング環境管理およびプロビジョニング用 Microsoft System Center Virtual Machine Manager（SCVMM）との統合（オプション）を行う Microsoft Hyper-V Server
- Microsoft Cluster Service
- Amazon Cloud 内のリモート仮想化された Windows および Linux のプロビジョニングを行う Amazon Elastic Compute Cloud （EC2）
- サーバ仮想化およびオペレーティング環境管理のための Citrix XenServer
- Citrix XenDesktop
- AIX プロビジョニングを行う IBM Network Installation Manager （NIM）
- IBM PowerHA
- IBM PowerVM for AIX 仮想化管理
- クロスプラットフォームの異なるハードウェアのプロビジョニングを行う Racemi 提供の Rapid Server Imaging （RSI）
- Huawei GalaX
- Red Hat Enterprise Virtualization （RHEV）
- Oracle Solaris ゾーン仮想化管理

以下の図は、製品アーキテクチャを示しています。



コア コンポーネント：

サービス コントローラ

すべてのコンポーネントの場所およびステータスを識別するための一元化された場所を提供します。 必要な場合は、この一元化された場所から複数の管理サーバに CA Server Automation コンポーネントを分配できます。 状況によっては、コンポーネントが、統合する技術と同じサーバにインストールされている必要があります。 たとえば、関連付けられたコンポーネントは、Software Delivery サーバにインストールする必要があります。 適切に機能するためには、これらのコンポーネントを 1 つのメイン サービス コントローラに登録することも必要です。

プロビジョニング

CA ITCM、OS インストール管理技術（OSIM）、VMware vCenter、Microsoft Hyper-V、Amazon EC2、、および Rapid Server Imaging のための統一された統合ポイントを提供します。

パフォーマンス モニタ

システム メトリックを収集するエージェントを使用して、情報とパフォーマンス メトリックを集めます。サポートされるエージェントは、CA パフォーマンス エージェント、、および SystemEDGE エージェント（SNMP 経由）です。 管理対象サーバは、データ センター インフラストラクチャ内のコア サーバです。 管理 DB に管理対象サーバが入力された後に、パフォーマンス モニタはデータの収集を開始します。

リソース マネージャ

サービスや静的 IP プールなどのリソースを作成および変更する機能を提供し、さらに各システムの管理ステータスも設定します。

検証

CA Configuration Automation との統合により、設定および変更管理機能を提供します。

パッケージング

CA ITCM および CA Patch Manager との統合により、ソフトウェア パッケージとパッチを管理対象サーバに展開します。

開始

Microsoft タスク スケジューラと統合してジョブをスケジュールします。 長期間または繰り返し実行される保守タスクとアクションをジョブとしてスケジューリングできます。

CA Process Automation

CA Process Automation との統合により、スケジューリング、設定、モニタリング、および IT プロセスの自動化を行います。 任意の時点で、プロセス内での位置が正確にわかるようにプロセスを視覚化します。

管理 DB

すべての管理対象オブジェクトに関する情報を格納する共通のデータリポジトリを提供します。情報とは、サーバ情報、サービス関係、サービスしきい値、ルールとアクション、イベント、CA Configuration Automation や CA Software Delivery などの他のコンポーネント用の認証情報、データ センター レベルのポーリングと記録間隔、データ センター レベルのしきい値と遅延などです。

パフォーマンス DB

パフォーマンス モニタによって集められたメトリックをすべて格納するリポジトリを提供します。 また、どのサーバからどのメトリックが収集されたか、それらのメトリックの値（期間内に集計された）、サーバ レベルのポーリングと記録間隔、およびサーバ レベルのしきい値と遅延（全体的なサーバ使用率の）も格納します。

ポリシー

収集されたパフォーマンス データを分析して、どのユーザ定義のビジネス ルールに対する違反があったかを特定し、ターゲット サーバまたはサービスに対してアクションを実行します。 あらかじめ、特定の問題を解決するためのルールとアクションを定義しておくと、ポリシー コンポーネントが、指定されたパラメータを使用して知的な決定を下します。 サーバまたはサービスを識別した後に、状況を解決するためにさまざまなアクションを実行できます。 たとえば、CA Software Delivery にジョブをサブミットして、リモート ターゲット サーバにソフトウェア パッケージを配信したり、カスタム スクリプトを実行したり、新規システムをプロビジョニングしたり、さらに多くの修正アクションを完了したりできます。

ヘルプ デスク

CA SDM と統合して、ヘルプ デスク チケットのステータスのオープン、更新、モニタリングをサポートします。

レポート

管理およびパフォーマンス データベースに保存されたデータを使用して、レポート機能を提供します。

イベント管理

CA Server Automation コンポーネントが生成したすべてのイベントをキャプチャして、SNMP 転送を提供します。これを使用して、SNMP トラップを受信できる任意の CA またはサードパーティ製品にイベントを転送できます。

認証

CA EEM と統合して、すべての認証要求および許可を管理し、共通のアクセス ポリシーを提供します。

予約マネージャ

Web ベース インターフェースで、エンド ユーザのためのセルフ サービス リソース予約システムを提供します。ユーザは、管理者の操作を必要とせずに、迅速かつ安全に物理および仮想サーバの予約、設定、およびプロビジョニングを実行できます。

SNMP トラップ レシーバ

受信 SNMP トラップをリスンし、イベント（表示）に変換して、各種コンポーネントに配信します。

状態エンジン

エージェントが収集したヘルス状態情報を、CA Server Automation エンティティの階層の上位へとプロパゲートします。

ストレージ

NetApp Provisioning Manager との統合により、新規または追加ストレージを仮想および物理システムにプロビジョニングします。

プラットフォーム管理モジュール（PMM）

CA Server Automation が統合する以下の仮想化プラットフォームに対してモニタリングと管理のインターフェースを提供します。

- Active Directory、Exchange Server
- Cisco UCS
- Citrix XenServer
- Huawei GalaX
- Hyper-V
- IBM PowerVM 論理パーティション
- Microsoft Cluster Service
- Red Hat Enterprise Virtualization （RHEV）
- Solaris ゾーン
- VMware vSphere/vCloud

データベース

製品は、管理データベースとパフォーマンス データベースの両方を使用します。

管理 DB

管理 DB は、管理データの説明用モデルに基づく、すべての管理対象オブジェクトの共通データ リポジトリです。管理 DB には、サーバ、サービス、ルール、アクション、仮想プラットフォーム オブジェクト、イベント、アラート、およびこれらのオブジェクトの関係に関する情報が格納されます。

CA Server Automation は、管理 DB を使用して、以下の情報を格納します。

- サーバ情報
- サービス関係
- サービスしきい値

- ルールおよびアクション
- イベント
- 他のコンポーネントの認証情報

注: 管理データベースの設定の詳細については、「*リファレンス ガイド*」の「コマンド ライン ユーティリティ」の章を参照してください。

パフォーマンス DB

パフォーマンス DB は、データ センター内のサーバから収集されたメトリックをすべて格納するリポジトリです。

CA Server Automation は、パフォーマンス DB を使用して、以下の情報を格納します。

- 収集されるメトリックの種類と収集元サーバ
- これらのメトリックの値（期間内に集計された）
- サーバ レベルの記録間隔
- サーバ レベルのしきい値（全体的なサーバ使用率）
- データ センター レベルの記録間隔
- データ センター レベルのしきい値

このデータベースに保存されたデータは、さまざまな機能に使用されます。たとえば、この DB のデータを使用して、履歴レポートが作成されます。CA Server Automation はまた、このデータベースのデータと、ユーザが作成したルールを使用して、論理的なビジネスの意思決定を行います。

注: パフォーマンス データベースの設定の詳細については、セクション「dpmutil -perfdb コマンド - パフォーマンス データベースの設定」を参照してください

ユーザ インターフェース

CA Server Automation の Web ベースユーザ インターフェースを使用して、中央の場所でデータ センターを管理できます。 Web ベース インターフェースでは、個別にコンポーネント インターフェースを開かずに、CA Server Automation 内の埋め込みコンポーネントの機能を使用できます。

たとえば、CA Server Automation Web ベースユーザ インターフェースから、問題管理用の CA SDM、およびイメージおよびパッケージ展開用の CA Software Delivery を使用できます。また、CA EEM 機能を使用して、アクティブなディレクトリを利用したり、CA EEM を開かずにユーザ インターフェースからユーザおよび許可を管理したりできます。

オプションを選択すると、ユーザ インターフェースにアクセスしたり、製品を直接統合してさらに高度な機能を実行したりできます。 たとえば、ネイティブ セキュリティを使用するための CA EEM、パッケージ展開での問題のトラブルシューティングを行う CA Software Delivery、または高度な変更および設定管理機能を実行するための CA Configuration Automation を開くことができます。 統合された製品がインストールされたサーバにログインして、そのユーザ インターフェースにアクセスできます。または、CA Server Automation ユーザ インターフェースの［管理］-［設定］ページに移動して、コンポーネントを選択し、コンポーネントのホーム ページを起動できます。

ユーザ インターフェースへのアクセス

システムの検出およびプロビジョニング、ポリシーの作成、ジョブのスケジューリングなどを行うには、ユーザ インターフェースにアクセスします。 CA Server Automation の［スタート］メニューのショートカットは、CA Server Automation サーバでのみ利用できます。 ［スタート］メニューを使用して、ユーザ インターフェースや CLI コマンド ウィンドウなどの製品機能にアクセスします。 別のサーバからインターフェースにアクセスするには、Web ブラウザで URL を入力する必要があります。

ユーザ インターフェースにアクセスする方法

1. CA Server Automation サーバで、［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation の起動］を選択します。

   CA Server Automation ログイン ページが以下の URL に表示されます。

   `https://servername:port/UI`

   servername

   CA Server Automation サーバを指定します。

port

Apache Tomcat サーバのポートを指定します。

デフォルト： 8443

注: セキュリティ証明書リクエストを受信した場合は、それを無視して続行します。 このようなメッセージが表示されないようにするには、任意のベンダーから証明書を取得して、サーバにそれを適用します。セキュリティ証明書のインストールの詳細については、Apache Tomcat の Web サイトを参照してください。

2. ログイン認証情報を入力し、［ログイン］をクリックします。

   ダッシュボードが表示されます。

第 3 章: ユーザとユーザ グループの管理

このセクションには、以下のトピックが含まれています。

ユーザ アクセス制御

CA EEM で、CA Server Automation コンポーネント間のすべての通信が確保されます。 以下の設定のいずれかを選択できます。

- Active Directory
- ネイティブ セキュリティ

注: 外部ディレクトリの設定の詳細については、「CA EEM 導入ガイド」および*オンライン ヘルプ*を参照してください。 これらのドキュメントは、［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［ドキュメント］を選択して CA EEM のインストール場所で見つけるか、または CA サポート オンライン Web サイト（http://www.ca.com/jp/support）で見つけることができます。

Active Directory

既存の Active Directory 設定に接続したときは、事前定義済みのユーザおよびユーザ グループが、ユーザの中央レポジトリと一貫しています。 CA Technologies では、CA Server Automation または CA EEM を使用するのではなく、Active Directory 内でユーザを作成および変更することを推奨します。

CA Server Automation は、LDAP （Lightweight Directory Access Protocol）を使用して、Microsoft Active Directory サーバの読み取りおよび書き込みを行います。 デフォルトでは、LDAP トラフィックはセキュリティが保証されずに送信されます。 このため、サーバと Microsoft Active Directory の間の通信ではセキュリティが保証されません。Microsoft Active Directory のセキュリティを確保するために、SSL （セキュア ソケット レイヤ）を使用する LDAP（LDAPS）を使用してください。 この場合は、Microsoft の認証機関または別の認証機関のいずれかから、正しくフォーマットされた証明書をインストールします。

注: データを安全に送信するための Active Directory の設定の詳細については、Microsoft の Web サイトを参照してください。 ナレッジ ベース記事「サードパーティの証明機関が SSL 経由で LDAP を有効にする方法」を検索してください。LDAPS を使用するように Active Directory を設定した後は、データを安全に送信できます。

Active Directory でのセキュリティ上の考慮事項

Microsoft Active Directory サーバに対する読み取りと書き込みでは、Lightweight Directory Access Protocol （LDAP）が使用されます。 LDAP トラフィックはデフォルトで、セキュリティで保護されずに転送されます。このため、サーバと Microsoft Active Directory の間の通信ではセキュリティが保証されません。Microsoft Active Directory をセキュリティで保護するには、LDAP over Secure Sockets Layer （SSL） - LDAPS を使用します。 Microsoft または Microsoft 以外の認証局から発行された適切に書式設定された証明書をインストールする必要があります。

その要件は Microsoft サポート技術情報の記事で解説されています。

注: データを安全に転送するための Active Directory の設定方法の詳細については、Microsoft Web サイトにある Microsoft サポート技術情報の記事「サードパーティの証明機関が SSL 経由で LDAP を有効にする方法」を参照してください。Active Directory で LDAPS を使用するための設定を行ったら、データを安全に転送できます。

ネイティブ セキュリティ

［ネイティブ セキュリティ］を使用して、CA EEM 管理者は、特に CA Server Automation のためのユーザ、ユーザ グループ、およびポリシーを作成できます。これは、この情報がローカルのストアに存在するためです。［ネイティブ セキュリティ］では、独自のユーザとユーザ グループのセットを手動で定義する必要があります。これらのユーザとユーザ グループは、ディレクトリ サービスで現在定義されているものとは一致していない場合があります。

CA EEM が CA Server Automation で動作するしくみ

CA EEM には、以下のキー オブジェクトが含まれます。

- ID （ユーザおよびユーザ グループ）
- リソース
- ポリシー

CA EEM は、以下の機能を提供します。

認証

ユーザを認証します。 認証されたユーザは、その後の許可処理で使用できます。

許可

ユーザが特定のリソースにアクセスすることを可能にします。 リソースとは、任意の論理または物理エンティティです。 CA Server Automation の典型的なリソースは、ユーザ インターフェース コンポーネント（タブ、コマンド、ドロップダウン リストなど）です。 リソース クラスに関連付けられたポリシーのセットで、許可が制御されます。これらのポリシーは、CA Server Automation に CA EEM を統合する主な方法です。

CA EEM ユーザ インターフェースへのアクセス

ネイティブ セキュリティを使用するために、CA EEM ホーム ページにログインします。また、［スタート］メニューから CA EEM ドキュメントを利用できます。さらに、ログインした後は、ホーム ページでオンライン ヘルプを利用できます。

CA EEM ユーザ インターフェースにアクセスする方法

1. ［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［EEM ユーザ インターフェース］を選択します。

   CA EEM の［ログイン］ウィンドウが表示されます。

   注: セキュリティ証明書リクエストを受信した場合は、それを無視して続行します。このようなメッセージが表示されないようにするには、任意のベンダーから証明書を取得して、サーバにそれを適用します。セキュリティ証明書のインストールの詳細については、Apache Tomcat の Web サイトを参照してください。

2. アプリケーションのドロップダウン リストから［AIP］を選択します。

   ［ユーザ名］フィールドには「EiamAdmin」が入力されています。

3. ［パスワード］フィールドにパスワードを入力し、［ログイン］をクリックします。

   CA EEM ホーム ページの、デフォルトで表示されるホーム ページが表示されます。

CA EEM ユーザの作成

CA Server Automation へのアクセス権を付与するには、CA EEM ユーザを作成します。この手順では、CA Server Automation の CA EEM が使用する共通データ ストアに CA EEM ユーザを手動で追加する方法について説明します。 また、外部ディレクトリを参照してユーザを追加することもできます。

注: 外部ディレクトリへの参照によるユーザの追加の詳細については、「CA EEM 導入ガイド」および*オンライン ヘルプ*を参照してください。

CA EEM ユーザを作成する方法

1. CA EEM ホーム ページ上の［ID の管理］をクリックします。

   デフォルトで［ユーザ］ページが選択されています。

2. ［ユーザの検索］セクションにある［アプリケーション ユーザの詳細］オプションを選択します。

3. ［属性］ドロップダウン リストで［ユーザ名］を、［演算子］ドロップダウン リストで［LIKE］を選択されたままにし、［値］フィールドは空白のままにして、［実行］をクリックします。

   すべての CA Server Automation ユーザが［ユーザ］ペインの階層ツリーにリスト表示されます。

4. 左側のペインにある［新規ユーザ］アイコンをクリックします。

   ［新規ユーザ］ペインが右側に表示されます。

5. このユーザのユーザ ID をユーザ名フィールドに入力して、［ユーザの詳細］ペインの［アプリケーション ユーザの詳細の追加］をクリックします。

6. ［アプリケーション グループ メンバシップ］ペインの［利用可能なユーザ/ユーザ グループ］からアプリケーション グループを選択して右矢印をクリックします。

   アプリケーション グループが［選択したユーザ/ユーザ グループ］に追加されます。

   注: このユーザを、1 つ以上の動的グループまたはグローバル グループに追加することもできます。 詳細については、CA EEM のマニュアルを参照してください。

7. ［認証］ペインの［新しいパスワード］および［パスワードの確認］フィールドに、このユーザのパスワードを入力して［保存］をクリックします。

   ［ユーザ］ペインの下に確認メッセージが表示されます。

デフォルト ユーザ グループの作成

ユーザ グループを使用して、ビジネス上の役割ごとにユーザを論理的にグループ化できます。 ユーザ グループを作成して、複数のユーザに同じアクセス権限を付与することができます。この手順では、アプリケーション グループの作成についてのみ記述しますが、この後の手順で、そのアプリケーション グループのためのポリシーの作成について説明します。また、グローバル グループ、動的グループ、および個別のユーザのためのポリシーも作成できます。

ユーザ グループを作成する方法

1. CA EEM ホーム ページの［ホーム］タブ上の［ID の管理］をクリックします。

   デフォルトで［ユーザ］ページが選択されています。

2. ［グループ］をクリックし、［アプリケーション グループを表示］チェック ボックスをオンにして［実行］をクリックします。

   利用可能なアプリケーション グループがすべて、［ユーザ グループ］ペインの［アプリケーション グループ］の下にリスト表示されます。

3. 左側のペインの［新規アプリケーション グループ］をクリックします。

   ［新規アプリケーション ユーザ グループ］ページが右側のペインに表示されます。

4. 新しいアプリケーション グループの名前を入力し、［保存］をクリックします。

   新しいアプリケーション ユーザ グループが作成されます。

パスワード管理

ユーザ認証情報は、CA Server Automation コンポーネント間の通信にとって不可欠です。 CA Server Automation は、ユーザおよびパスワード情報を内部に格納します。 CA Server Automation が統合する外部コンポーネントまたはアプリケーションのパスワードを変更する場合は、整合性を保つために、これらのパスワードを CA Server Automation で変更します。 そうしないと、CA Server Automation が正しく動作しません。

以下の領域を考慮してください。

- Active Directory セキュリティ
- ネイティブ セキュリティ
- CA EEM 管理者
- データベース sa ユーザ（SQL 認証）

CA EEM 管理者パスワード（EiamAdmin）の変更

CA EEM 管理者パスワード（EiamAdmin）を変更する場合は、CA EEM でパスワードを変更し、さらに CA Server Automation でも変更します。

CA EEM で管理者パスワード（EiamAdmin）を変更する方法

1. ［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［EEM ユーザ インターフェース］に移動し、ユーザ インターフェースを開きます。

   ［ログイン］ダイアログ ボックスが表示されます。

2. 現在の EiamAdmin パスワードでログインします。

   ユーザ インターフェースが開きます。

3. ［設定］および［EEM サーバ］をクリックします。

   ［EEM サーバ］ペインが表示されます。

4. ［EiamAdmin のパスワード］をクリックします。

   ［新しいパスワード］および［パスワードの確認］フィールドが表示されます。

5. パスワードを入力し、［保存］をクリックします。

   これで、新しい EiamAdmin パスワードを使用して CA EEM にログインできます。

CA Server Automation で管理者パスワード（EiamAdmin）を変更する方法

1. ［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］に移動します。

   コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

   ```
   dpmutil -set -eiam
   ```

   dpmutil コマンドが、必要な認証情報の入力を要求します。

   情報を入力してコマンドを完了します。

3. CAAIPApache および CAIPTomcat サービスをリサイクルします。

   認証情報が一致し、CA Server Automation が予期したとおりに動作します。

注: いずれの場合も、*Install_path*¥Apache¥ logs¥error.log にある Apache のログ ファイルで、製品が適切に起動したことを確認できます。 最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。「-set -eiam」および「-set -sysuser」に使用した認証情報を、CA EEM UI へのログインに使用できることを確認します。 その後、有効な認証情報を使用して dpmutil コマンドを再度実行します。

データベース管理者(sa)パスワードの変更

Microsoft SQL 認証を使用しており、Microsoft SQL ユーザ (通常は「sa」ユーザ) のパスワードを変更する場合は、CA Server Automation パスワードも変更します。

Microsoft SQL Server のデータベース管理者(sa)パスワードを変更する方法

1. Microsoft SQL Server Management Studio を開いてログインします。
2. オブジェクト エクスプローラーで［セキュリティ］、［ログイン］を展開します。
3. sa を開き、右側のペインでパスワードを変更します。

注: 詳細については、Microsoft SQL Server のドキュメントを参照してください。

CA Server Automation のデータベース管理者(sa)パスワードを変更する方法

1. ［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］に移動します。

   コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

   ```
   dpmutil –set –mgmtdb
   ```

   dpmutil コマンドが、適切な認証情報の入力を要求します。

   情報を入力してコマンドを完了します。

3. パフォーマンス データベースが同じサーバおよびデータベース ユーザ（sa）を使用している場合は、以下のコマンドを入力します。

   ```
   dpmutil -set -perfdb
   ```

   dpmutil コマンドが、適切な認証情報の入力を要求します。

   情報を入力してコマンドを完了します。

4. CAAIPApache および CAIPTomcat サービスをリサイクルします。

   認証情報が一致し、CA Server Automation が予期したとおりに動作します。

ネイティブ セキュリティのシステム ユーザ パスワードの変更

CA Server Automation では、Apache サービスの開始または停止などのために、*sys_service* システム ユーザが正しく機能することが必要です。 ネイティブ セキュリティでのインストール中に、*sys_service* システム ユーザとそのパスワードを指定します。 インストール プログラムは、CA EEM および CA Server Automation 内に sys_service 認証情報を格納します。後から CA EEM 内の sys_service のパスワードを変更する場合は、すべての CA Server Automation サービスが引き続き実行されるように、CA Server Automation でもパスワードを変更します。

CA EEM で sys_service パスワードを変更する方法

1. ［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［EEM ユーザ インターフェース］に移動し、ユーザ インターフェースを開きます。

   ［ログイン］ダイアログ ボックスが表示されます。

2. 現在の EiamAdmin パスワードでログインします。

   ユーザ インターフェースが開きます。

3. ［ID の管理およびユーザの検索］をクリックします。

   ［ユーザ］ペインにユーザが表示されます。

4. sys_service ユーザをクリックします。

   右側のペインにユーザ プロパティが表示されます。

5. ［認証］セクションまでスクロールし、［パスワードのリセット］をクリックします。

   ［新しいパスワード］および［パスワードの確認］フィールドが表示されます。

6. パスワードを入力し、［保存］をクリックします。

   これで、新しいパスワードが CA EEM に格納されました。

CA Server Automation で sys_service ユーザ パスワードを変更する方法

1. ［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］に移動します。

   コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

   ```
   dpmutil –set –sysuser
   ```

   dpmutil コマンドが、必要な認証情報の入力を要求します。

   情報を入力してコマンドを完了します。

3. CAAIPApache および CAIPTomcat サービスをリサイクルします。

   認証情報が一致し、CA Server Automation が予期したとおりに動作します。

Active Directory セキュリティのシステム ユーザ パスワードの変更

CA Server Automation をインストールする際に Active Directory に接続するよう設定すると、CA Server Automation をインストールしたユーザは自動的に CA EEM に登録されます。 この登録によって、CA Server Automation が Active Directory ドメインからユーザを認証できるようになります。ユーザ パスワードが変更されると、CA EEM がユーザを認証できなくなるため、ユーザは CA Server Automation ユーザ インターフェースにログインできません。 以下のようにユーザ パスワードを変更します。

Active Directory のユーザ パスワードを変更する方法

1. ［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［EEM ユーザ インターフェース］に移動し、ユーザ インターフェースを開きます。

   ［ログイン］ダイアログ ボックスが表示されます。

2. 現在のパスワードでログインします。

   ユーザ インターフェースが開きます。

3. ［設定］および［EEM サーバ］をクリックします。

   ［EEM サーバ］ペインが表示されます。

4. 左側のペインの［グローバル ユーザ/グローバル グループ］をクリックして、デフォルト オプション［外部ディレクトリから参照］を選択されたままにします。

5. タイプをデフォルトの［Microsoft Active Directory］のままにし、［パスワード］および［パスワードの確認］フィールドに新しいパスワードを入力して［保存］をクリックします。

6. CA EEM を閉じます。

7. ［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］に移動します。

   コマンド プロンプトが表示されます。

8. 以下のコマンドを入力します。

   ```
   dpmutil –set –sysuser
   ```

   Sysuser は、CA Server Automation をインストールするユーザと同じユーザです。 dpmutil コマンドが、手順 5 で指定した、必要な認証情報の入力を要求します。

   情報を入力してコマンドを完了します。

9. CAAIPApache および CAIPTomcat サービスをリサイクルします。

   認証情報が一致し、CA Server Automation が予期したとおりに動作します。

注: いずれの場合も、*Install_path*¥Apache¥ logs¥error.log にある Apache のログ ファイルで、製品が適切に起動したことを確認できます。 最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。「-set -eiam」および「-set -sysuser」に使用した認証情報を、CA EEM UI へのログインに使用できることを確認します。 有効な認証情報を使用して dpmutil コマンドを再度実行します。

ユーザ グループ管理

［ユーザ グループ］ページでは、ユーザとユーザ グループの認証および製品機能へのユーザ アクセス制御にアクセスできます。

関連項目:

ユーザまたはユーザ グループの検索 (P. 45)
ユーザ グループの作成 (P. 46)
グループへのユーザの割り当て (P. 47)
外部ディレクトリ ユーザ グループのユーザ グループへの割り当て (P. 48)
ユーザ グループ権限の設定 (P. 49)
ユーザ グループ権限の設定 (P. 49)
サービスに対するユーザ グループ権限の設定 (P. 50)
コマンド スクリプトの実行権限の設定 (P. 51)
外部ディレクトリのインポート (P. 51)
ユーザ グループの削除 (P. 52)
ユーザ グループに対するサービスへのアクセス権の割り当て (P. 53)
ユーザ グループからのユーザまたはユーザ グループの削除 (P. 53)

ユーザまたはユーザ グループの検索

追加または削除するユーザまたはユーザ グループを検索できます。

ユーザまたはユーザ グループを検索する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。

   ユーザ グループのページが右ペインに表示されます。

4. ［メンバシップ］をクリックします。

   ［ユーザ/ユーザ グループ］ページが表示されます。

5. ［アイデンティティ］ドロップダウン リストで［ユーザ］または［ユーザ グループ］を選択します。検索する属性を［属性］ドロップダウン リストで選択し、LIKE 演算子を選択されたままにしておきます。［値］フィールドに値（またはワイルドカードを含む部分的な値）を入力して［検索］をクリックします。

   一致するユーザまたはユーザ グループ名のリストが［利用可能なユーザ/ユーザ グループ］リストに表示されます。

ユーザ グループの作成

ユーザ グループを使用すると、ビジネス上の役割に従ってユーザを論理的にグループ化できます。ユーザ グループを作成して、複数のユーザに同じアクセス権限を付与することができます。

ユーザ グループを作成する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. ユーザ グループの名前を入力します。ビジネス上の役割またはサービスに基づく名前を使用できます。
4. （オプション）説明を入力します。
5. ［保存］をクリックします。

   新規ユーザ グループが左側のペインに表示されます。

関連項目:

グループへのユーザの割り当て (P. 47)

グループへのユーザの割り当て

ユーザは、自身のユーザ グループに割り当てられたアクセス権限を継承します。 既存のユーザ グループに新規ユーザを追加して、そのユーザにユーザ グループのアクセス権限を付与することができます。 管理者ユーザ グループは事前定義済みグループで、デフォルトでリストに表示されます。

グループにユーザを割り当てる方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。

   サブメニューが表示されます。

4. ［メンバシップ］サブメニューを選択します。

   一連のメンバシップ ペインが表示されます。

5. 追加するユーザの名前を［値］テキスト ボックスに入力して、［検索］をクリックします。

   検索結果が［利用可能なユーザ/ユーザ グループ］ペインに表示されるか、一致するものが見つからなかったことを知らせるメッセージが表示されます。ユーザ名が確実でない場合は、ユーザまたはユーザ グループを検索 (P. 45)できます。

6. 追加するユーザを［利用可能なユーザ/ユーザ グループ］ペインで選択し、右矢印  をクリックします。

   ユーザ名が［選択したユーザ/ユーザ グループ］ペインに移動します。

7. ［保存］をクリックして、ユーザの追加を完了します。

   ユーザには、そのユーザ グループのアクセス権限が付与されます。

外部ディレクトリ ユーザ グループのユーザ グループへの割り当て

既存のアクセス権を付与するとき、外部ディレクトリから既存の CA Server Automation ユーザ グループにユーザ グループを追加できます。 管理者ユーザ グループは事前定義済みグループで、デフォルトでリストに表示されます。

外部ディレクトリ ユーザ グループをユーザ グループに割り当てる方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ノードが左側のペインに表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。

   ［ユーザ グループ］ページが右側のペインに表示されます。

4. ［メンバシップ］サブメニューを選択します。

   一連の［メンバシップ］ペインがタブの下に表示されます。

5. ［アイデンティティ］リストから［ユーザ グループ］を選択します。

   ユーザの検索条件が［属性］リストに表示されます。

6. 外部ディレクトリから追加するユーザ グループ名を［値］テキストボックスに入力し、［検索］をクリックします。

   ユーザが検索されるか、一致するものが見つからなかったことがメッセージで通知される場合、そのユーザ グループは［利用可能なユーザ/ユーザ グループ］ペインに表示されます。ユーザ グループ名は、［利用可能なユーザ/ユーザ グループ］リストの［グローバル グループ］で確認できます。

7. 追加するユーザ グループを［利用可能なユーザ/ユーザ グループ］ペインから選択し、右方向矢印  をクリックします。

   選択したユーザ グループが［選択したユーザ/ユーザ グループ］ペインに移動します。

8. ［保存］をクリックし、ユーザ グループの追加を完了します。

   ユーザには、関連付けられているユーザ グループに割り当てられたアクセス権限がただちに付与されます。

ユーザ グループ権限の設定

［管理］ページを使用して、サービスへのユーザ グループのアクセスを制御できます。 管理者権限が付与されたユーザは、すべてのサービスにアクセスできます。

注: ユーザに CA Server Automation へのアクセス権を付与する場合の詳細については、「管理ガイド」を参照してください。

ユーザ グループ権限を設定する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. 権限を設定するユーザ グループを選択し、［権限］タブをクリックします。

   ［権限］ページが表示されます。

4. アクセスを付与または制限するタブおよびアクションのチェック ボックスをオンにし、［保存］をクリックします。

   ユーザ グループ権限が更新されます。

   注: 特定のページからユーザ グループを制限する場合は、そのページ上のすべてのアクションからも、そのユーザ グループを制限します。

ユーザ グループ権限の設定

ユーザ インターフェースの機能領域および特定の機能へのユーザ グループのアクセス権を制御できます。AIPAdmins ユーザ グループにはデフォルトで、すべての機能領域および機能へのアクセス権があります。

ユーザ グループ権限を設定する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. 権限を設定するユーザ グループを選択して［権限］をクリックします。

   ［権限］ページが表示されます。

4. アクセスを付与または制限する機能領域または機能を選択して、［保存］をクリックします。

   ユーザ権限が更新されます。

サービスに対するユーザ グループ権限の設定

サービスへのユーザ グループのアクセスを制御できます。 管理者権限を持つユーザは、デフォルトですべてのサービスにアクセスできます。

ユーザ グループ権限を設定する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. 左側のペインでユーザ グループをクリックします。

4. ［サービス アクセス］をクリックします。

   右側のペインに、サービスが有効または無効にされているリソースが表示されます。

5. 必要に応じて、サービス アクセス権についてリソースを有効または無効にします。

6. ［保存］をクリックします。

   ［サービス アクセス］リストが更新されます。

コマンド スクリプトの実行権限の設定

管理者ユーザを使用することによって、個別のコマンド スクリプト アクションに対するアクセス権をユーザ グループに付与するか、個別のコマンド スクリプト アクションに対するユーザのアクセス権を有効にできます。 対象のコマンド スクリプト アクションは、［アクション & ルール］ページ（ポリシー）で作成済みの必要があります。

コマンド スクリプト アクションの実行権限を設定する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。

   タブが右側のペインに表示されます。

4. ［権限］タブを選択します。

   権限のリストと、権限を選択または選択解除するためのチェック ボックスが表示されます。

5. ［ポリシー］フォルダを展開し、［コマンド スクリプトの実行］を選択して、［保存］をクリックします。

   コマンド スクリプト権限が更新されます。

外部ディレクトリのインポート

ユーザ グループとしてユーザ名とパスワードの認証を提供する外部ディレクトリ サービスをインポートできます。

外部ディレクトリをインポートする方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。
4. ［メンバシップ］を選択します。

   ［ユーザ / ユーザ グループ］ページが表示されます。
5. ［アイデンティティ］ドロップダウン リストから［ユーザ グループ］を選択し、［値］テキスト ボックスに外部ディレクトリの名前または名前の一部を入力して、［検索］をクリックします。

   検索が失敗すると、確認メッセージが表示されます。見つかると、見つかったユーザ グループの情報が［利用可能なユーザ/ユーザ グループ］セクションに設定されます。 外部ディレクトリが CA Server Automation にインポートされました。

ユーザ グループの削除

不要になったユーザ グループは削除できます。

ユーザ グループを削除する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。
2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。
3. ［ユーザ グループ］を右クリックし、［ユーザ グループを削除します］を選択します。

   ユーザ グループが削除されます。

ユーザ グループに対するサービスへのアクセス権の割り当て

ユーザのグループが複数存在する環境では、通常、各グループで他のグループのリソースが表示されないようにする必要があります。 管理者は、ユーザのグループに特定のリソースを割り当てることができます。 管理者によっては、自分がメンバであるグループにのみ、リソースを割り当てることができます。 ただし、グループ *AIPAdmins* の管理者には、リソースを割り当てるための完全なアクセス権があります。

ユーザ グループにサービスへのアクセス権を割り当てる方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［ユーザ グループ］をクリックします。

   ［ユーザ グループ］ページが表示されます。

3. 左ペインで、権限を設定するユーザ グループを選択して［サービス アクセス］をクリックします。

   システムに定義されたサービスをリスト表示するツリーが表示されます。

4. アクセスを付与または制限するサービスを選択して［保存］をクリックします。

   ユーザ グループには、関連付けられたサービスに割り当てられたアクセス権限が付与されます。

ユーザ グループからのユーザまたはユーザ グループの削除

既存の CA Server Automation ユーザ グループからユーザとユーザ グループを削除できます。 管理者ユーザ グループは事前定義済みグループで、デフォルトでリストに表示されます。

ユーザ グループからユーザまたはユーザ グループを削除する方法

1. ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. ［ユーザ グループ］を選択します。

   ［ユーザ グループ］メニューが左側のペインに表示されます。

3. ［ユーザ グループ］を展開して、リストからユーザ グループを選択します。

   サブメニューが右側のペインに表示されます。

4. ［メンバシップ］サブメニューを選択します。

   一連のメンバシップ ペインが表示されます。

5. ［選択したユーザ/ユーザ グループ］ペインから削除するユーザまたはユーザ グループを選択して、左矢印  をクリックします。

   ユーザまたはユーザ グループが［利用可能なユーザ/ユーザ グループ］ペインに移動します。

6. ユーザとユーザ グループの削除が完了したら、［保存］をクリックします。

第 4 章: システム パフォーマンスの管理

このセクションには、以下のトピックが含まれています。

システム管理

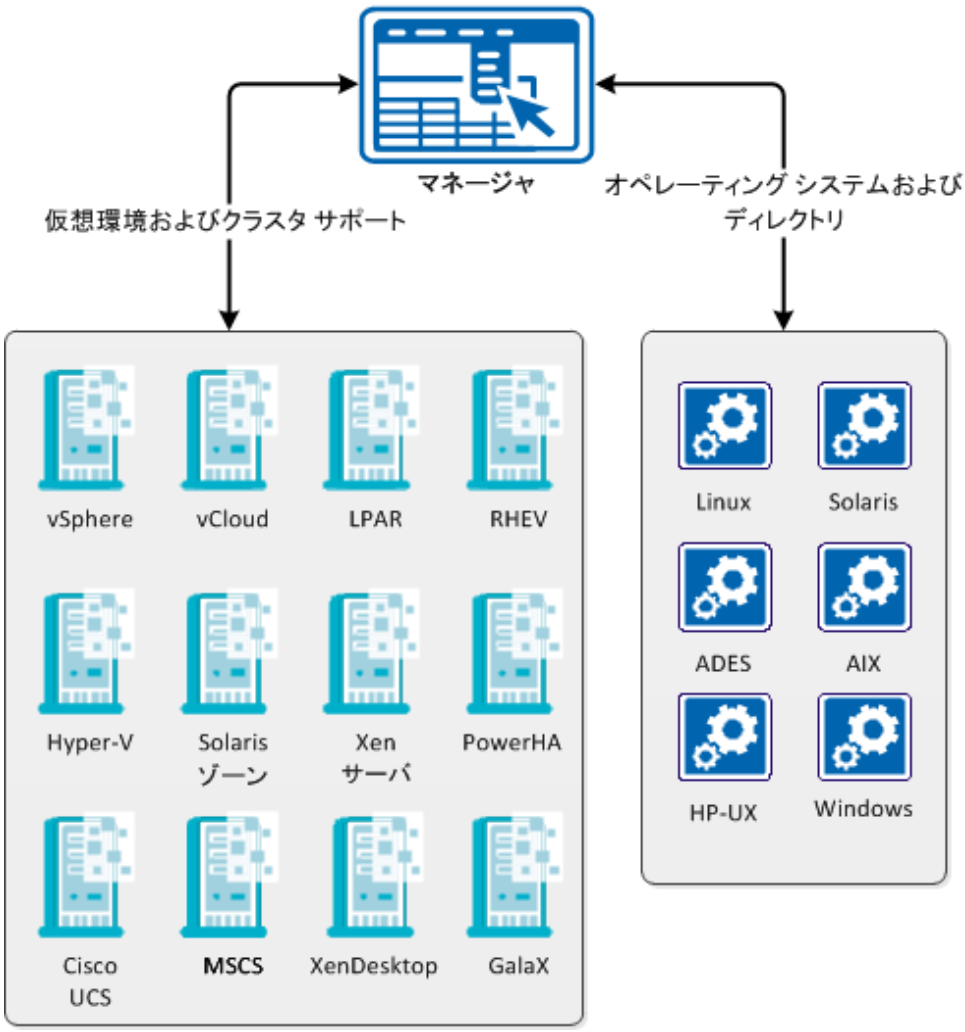
CA Server Automation は、仮想環境を管理するよう設計されていますが、システム（管理対象ノード）の検出や管理も行います。 CA Server Automation は、管理対象ノード上の以下のオペレーティング システムをサポートしています。

- AIX
- HP-UX
- Linux、zLinux
- Solaris （Intel、SPARC）
- Windows

管理対象ノードの利用可能な管理コンポーネントは、次のとおりです。

- SystemEDGE
- Advanced Encryption AIM
- リモート モニタリング AIM （Windows サーバのみ）
- サービス レスポンス モニタリング（SRM）AIM
- CA Systems Performance LiteAgent

サポートされている仮想環境およびオペレーティング システム



SystemEDGE は、CA Server Automation でのシステム管理の基礎であり、以下の利点を備えています。

- すべての管理対象システムへの、一元化されたリモート エージェント展開
- 一元化されたリモート エージェント設定
- エージェントのオブジェクト モデルからのステータス情報を含む、モニタされたすべてのメトリックの視覚化
- サービス レスポンス モニタ AIM のリモート展開および設定
- 強化されたエージェント セキュリティ オプション

注: SystemEDGE エージェント機能の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

関連項目

SystemEDGE 機能 (P. 72)
サービス レスポンス モニタリング (P. 87)
リモート モニタリング コンポーネント間のインタラクション (P. 780)
エージェントの設定 (P. 82)
エージェントの視覚化 (P. 90)
セキュリティおよび保守 (P. 85)

ディスカバリ

以前は管理対象外であったサーバまたは新たに追加されたサーバを含む、管理するサーバまたはサブネット全体を検出して追加できます。

注: CA Server Automation ディスカバリには、ホスト名解決が必要です。検出されたサーバの IP アドレスが変わった場合は、IP アドレスが CA Server Automation で自動的には解決されません。 その結果、ディスカバリ プロファイルで管理データベースが更新されません。 IP アドレスが変わった場合は、サーバを再検出してください。

システムの検出

検出、管理、あるいはサービスに割り当てるシステムを 1 つ指定できます。

システムを検出する方法

1. ［リソース］-［管理］-［システムの検出］を選択します。
2. ［システム名］フィールドに入力して、サーバの名前または IP アドレスを指定します。
3. （オプション）［次へ］をクリックします。

   ［拡張ディスカバリおよび SNMP 情報］ダイアログ ボックスが表示されます。
4. （オプション）［拡張ディスカバリ］を有効にして、SoftAgent 技術を使用した詳細な検出が実行されるようにします。
5. （オプション）［SNMP デフォルトを上書きする］を有効にして、SNMP 情報を使用した詳細なディスカバリが実行されるようにします。
6. ［終了］をクリックします。

   システムが検出されると、成功のメッセージが表示されます。 検出されたサーバは自動的に管理されますが、サブネット ディスカバリ内のサーバは管理されません。

システムの削除

検出済みのシステムを削除すると、そのシステムは CA Server Automation から削除されます。

システムを削除する方法

1. ［リソース］-［管理］-［システムの管理］を選択します。
2. 右ペインの上部のドロップダウン メニューから、以下のいずれかを選択します。
   - ベア メタル サーバ
   - 管理対象サーバ
   - 管理対象外サーバ

   検出されたシステムのリストが表示されます。
3. 削除する 1 台または複数のシステムを選択し、［アクション］ドロップダウン メニューで［削除］を選択します。

   注: また、［システム］ページで［すべて削除］を選択することにより、すべてのシステムを削除できます。

   確認のためのメッセージが表示されます。
4. ［はい］をクリックします。

   システムは［システム］ページから削除され、CA Server Automation 内で検出済みシステムのリストに表示されなくなります。

ネットワークの検出

検出対象となるネットワークのセグメントを指定できます。 ネットワーク ディスカバリ用の IP アドレスをユーザ インターフェースで指定するときは、CIDR （Classless Inter-Domain Routing）表記法を使用します。 この表記法は以下の例に示すとおり、アドレスと、サブネット プレフィックスとして使用するビットの数で構成されます。

172.24.143.0/24

ワイルドカードと範囲を使用することもできます。

172.24.143.*

172.24.143.{1-255}

ネットワークを検出する方法

1. ［リソース］-［管理］-［ネットワークの検出］をクリックします。
2. 以下のフィールドを指定します。

   ネットワーク名

   ネットワークの名前を指定します。

   ネットワーク アドレス

   ネットワーク IP アドレスを指定します。 このフィールドにカーソルを置くと、アドレスの例が表示されます。

   除外アドレス

   （オプション）ディスカバリから除外するネットワーク アドレスを指定します。

3. ［ディスカバリ方法］の以下のオプションから *1* つを選択して、対応するフィールドに入力します。

   Ping スイープ

   ネットワーク内の IP アドレスをすべて検出します。

   DNS

   ドメイン ネーム システム（DNS）サーバに登録されているホスト名を検出します。 ドメイン名と DNS サーバ名を各フィールドに入力します。

4. （オプション）［次へ］をクリックします。

   ［拡張ディスカバリおよび SNMP 情報］ダイアログ ボックスが表示されます。

5. （オプション）［拡張ディスカバリ］を有効にして、SoftAgent 技術を使用した詳細な検出が実行されるようにします。

6. （オプション）［SNMP デフォルトを上書きする］を有効にして、SNMP 情報を使用した詳細なディスカバリが実行されるようにします。

7. ［終了］をクリックします。

   ネットワークが検出されると、成功のメッセージが表示されます。 検出されたサーバは自動的に管理されますが、サブネット ディスカバリ内のサーバは管理されません。

拡張ディスカバリおよび SNMP 情報

認証情報および SNMP 情報を指定して、システムまたはネットワークを検出できます。

拡張情報を使用して検出する方法

1. ［リソース］-［管理］-［ネットワークの検出］または［システムの検出］を選択します。

   ［ディスカバリ タイプおよびターゲットの指定］セクションが表示されます。

   ［ディスカバリ タイプ］セクションおよび［ディスカバリ方法］セクションに必要な詳細情報を入力し、［次へ］をクリックします。 ［拡張ディスカバリおよび SNMP 情報］セクションが表示されます。

2. ［拡張ディスカバリ］セクションの以下のフィールドで選択および入力を行います。

   拡張ディスカバリ

   ディスカバリ用の拡張認証情報を指定するには、このオプションを選択します。

   ディスカバリ認証情報

   オプションの*いずれか*を選択して、認証情報を指定します。

   認証情報の指定

   ユーザ名およびパスワードなどの認証情報を指定するには、このオプションを選択します。

   保存された認証情報の選択

   ［利用可能］リストから既存の保存された認証情報を選択します。

3. ［SNMP 情報］セクションの以下のフィールドで選択および入力を行い、次に、［次へ］をクリックします。

   SNMP デフォルトを上書きする

   ディスカバリ用の SNMP デフォルトを上書きするには、このオプションを選択します。

   SNMP 設定

   オプションの*いずれか*を選択して、認証情報を指定します。

   認証情報の指定

   SNMP バージョンやコミュニティ文字列などの認証情報を指定するには、このオプションを選択します。

   保存された認証情報の選択

   ［利用可能］リストから既存の保存された認証情報を選択します。

4. ［終了］をクリックします。

システムまたはネットワークが検出されると、成功したことを示すメッセージが表示されます。検出されたサーバは自動的に管理されますが、サブネット ディスカバリ内のサーバは管理されません。

ネットワーク ディスカバリのキャンセル

進行中のネットワーク ディスカバリはキャンセルできます。

ネットワーク ディスカバリをキャンセルする方法

1. ［リソース］をクリックし、［管理］ペインを開きます。
2. ［管理］セクションで［検出されたネットワークの管理］をクリックします。
3. ディスカバリをキャンセルする進行中のネットワークを選択し、［ネットワーク リスト］ツールバーで［—］（キャンセル）をクリックします。

   選択したネットワークのディスカバリをキャンセルするかどうかを確認するメッセージが表示されます。

ネットワークの再検出

検出済みのネットワークにシステムが追加されるか、またはネットワークが最後のディスカバリ以降にほかの方法で変更されている場合、そのネットワークの再検出を行うことができます。

ネットワークを再検出する方法

1. ［リソース］-［管理］-［検出されたネットワークの管理］を選択します。

   検出されたネットワークのリストが、右ペイン内に表示されます。
2. 再検出するネットワークを選択し、［ネットワーク リスト］ツールバーで （再検出）をクリックします。

   ディスカバリがそのネットワーク上で開始されます。ディスカバリが完了すると、ネットワークに対するすべての変更（システムの追加または削除）が反映されます。

ネットワークの削除

検出済みのネットワークを削除できます。 ただし、すでに検出済みのシステムはそれらのステータスを保持します。

ネットワークを削除する方法

1. ［リソース］-［管理］-［検出されたネットワークの管理］を選択します。

   検出されたネットワークのリストが、右ペイン内に表示されます。

2. 削除するネットワークを選択し、［ネットワーク リスト］ツールバーで［-］（削除）をクリックします。

   確認のためのメッセージが表示されます。

3. ［OK］をクリックします。

   ネットワークはネットワーク リストから削除されます。

サービス

既存の管理対象サーバをサービスにグループ化し、そのグループをモニタできます。

関連項目:

サービスの作成 (P. 64)
サービスの編集 (P. 66)
サービスからのサーバの削除 (P. 68)
サービスの削除 (P. 68)

サービスの作成

モニタするサーバを、ビジネス ニーズでの必須リソースを反映する論理サービスにまとめることができます。

サービスを作成する方法

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。

2. ［データ センター］または［CA Server Automation サービス］などの親サービス ノードを選択します。
3. ［管理］を右クリックし、［新しいサービス］クリックします。

   ［サービス: 新規］ダイアログ ボックスが表示されます。
4. ［サービス名］フィールドに新規サービスの名前を入力し、［サービスの優先度］フィールドで優先度レベルを設定します。

   注: サービス名では以下の文字はサポートされていません： % " “ ” ‘ ' < > / ¥ : ` ~ ;

   サービスの優先度

   1 回のポーリング サイクルでアクションを実行する順序を指定します。

   例：

   ServiceA： 優先度 3

   ServiceB： 優先度 1

   ServiceC： 優先度 2

   それぞれのルールがすべて true として評価された場合、アクションは ServiceB、ServiceC、ServiceA の順序で実行されます。
5. 遅延回数を変更するか、または表示されるデフォルトを受け入れます。

   遅延

   アクションをトリガする前に、ルールが True と評価される必要がある頻度を定義します。
6. 下限しきい値と上限しきい値のパーセンテージを変更するか、またはデフォルトを受け入れます。

   下限および上限しきい値（%）

   サービス全体の下限および上限しきい値を指定します。

   制限： サービス レベルでは全体使用率メトリックのみを評価できます。

7. サービスを CCA サーバに割り当てることができます。サーバの同じリストを持つ CCA サービスが自動的に作成されます。

   注: CCA サーバが検出しないサーバは CCA サービスに追加されません。問題が発生していないかどうかをイベント テーブルで確認します。

   また、サービス内のすべてのサーバに適用される管理プロファイルも選択できます。

8. ［サーバ］セクションの［利用可能なサーバ］リストから新規サービスのサーバを選択し、右向き矢印をクリックします。

   注: 利用可能なサーバのリストが長い場合は、リストをフィルタしてサーバのセットを減らします。 これを行うには、［フィルタ］矢印をクリックし、フィルタ条件を入力して［検索］をクリックします。

   サーバが［選択済みサーバ］セクションに移動します。

9. ［アクション］ドロップダウン メニューの［保存］をクリックします。

   新しいサービスが保存され、［エクスプローラ］ペインに表示されます。

   サービス レベルで、スナップショットの作成、コンポーネントの表示、ディスカバリまたは変更の検出を実行できます。 サービスを右クリックし、関連するオプションを選択します。

サービスの編集

既存のサービスを編集して、名前の変更、設定の変更、またはグループに対するリソースの追加または削除を行うことができます。

サービスを変更する方法

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. サービスを選択し、［管理］を右クリックして、［サービスの編集］をクリックします。

   ［サービス: 編集］ダイアログ ボックスが表示されます。

3. 必要に応じて、［サービスの優先度］フィールドで優先度レベルを、または下限しきい値および上限しきい値のパーセンテージを変更します。

   サービスの優先度

   1 回のポーリング サイクルでアクションを実行する順序を指定します。

   例：

   ServiceA： 優先度 3

   ServiceB： 優先度 1

   ServiceC： 優先度 2

   それぞれのルールがすべて true として評価された場合、アクションは ServiceB、ServiceC、ServiceA の順序で実行されます。

4. 遅延の発生頻度を変更するか、またはデフォルトを受け入れます。

   遅延

   アクションをトリガする前に、ルールが True と評価される必要がある頻度を定義します。

   下限および上限しきい値（%）

   サービス全体の下限および上限しきい値を指定します。

   制限： サービス レベルでは全体使用率メトリックのみを評価できます。

5. サービスに追加するサーバを［サーバ］セクションの［利用可能なサーバ］リストから選択し、次に、右向き矢印をクリックします。

   注: 利用可能なサーバのリストが長い場合は、リストをフィルタしてサーバのセットを減らします。 これを行うには、［フィルタ］矢印をクリックし、フィルタ条件を入力して［検索］をクリックします。

   サーバが［選択済みサーバ］セクションに移動します。

6. サービスから削除するサーバを［サーバ］セクションの［選択済みサーバ］リストから選択し、次に、左向き矢印をクリックします。

   サーバは［選択済みサーバ］セクションから［利用可能なサーバ］セクションに移動します。

7. ［保存］をクリックします。

   ［サーバ］リストが更新されます。

サービスからのサーバの削除

サーバが特定のサービスに属さないようにすることが必要な場合があります。 サービスからサーバを削除できます。

サービスからサーバを削除する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインで［データ センター］フォルダおよび［CA Server Automation サービス］フォルダを展開します。

   データ センターによって検出され、管理されているリソースが表示されます。

3. サーバを右クリックし、［管理］-［サービスから削除］を選択します。

   サーバを削除するかどうかを確認するメッセージが表示されます。

4. ［OK］をクリックします。

   サーバはサービスから削除されます。

サービスの削除

サービスを削除すると、そのサーバ収集は削除されますが、サービス内のサーバは、CA Server Automation 内で管理対象のままとなります。

サービスを削除する方法

1. ［リソース］-［管理］-［サービスの管理］を選択します。

   サービスのリストが、右ペイン内に表示されます。

2. サービスを選択し、［サービス］ツールバーで［-］（削除）をクリックします。

   確認のためのメッセージが表示されます。

3. ［はい］をクリックします。

   サービスが削除されます。

管理対象リソースと管理対象外リソース

リソースをモニタするかどうかを指定するには、そのモニタ状態を変更します。 オブジェクト設定を管理対象外に変更すると、PMM は要求を処理し、AIM で値を管理対象外に設定します。 現在のモニタ設定は MIB 属性に保持され、子オブジェクトも管理対象外に変更されます。トラップは、親の設定変更と状態変更に関して生成されます。 その後のポーリングおよび記録サイクルで親オブジェクトとその子のトラップは生成されません。

オブジェクトを選択して、その設定を管理対象に変更すると、PMM は要求を処理し、AIM でその値を管理対象に設定します。現在のモニタ設定は MIB 属性に保持され、子オブジェクトも管理対象に変更されます。設定変更トラップは親に関して生成されます。 次のポーリングおよび記録サイクルで親オブジェクトとその子の状態が評価され、必要に応じて状態変更トラップが生成されます。

重要: リソースの管理対象または管理対象外のステータスは、SystemEDGE の管理対象または管理対象外モードとは異なります。 コンピュータ システムを管理対象外に設定すると、そのシステムに SystemEDGE がインストールされている場合は SystemEDGE の保守モードが有効になります。

関連項目:

管理対象リソースの管理の停止 (P. 70)
管理対象外リソースの管理 (P. 70)
管理対象リソースの削除 (P. 71)

管理対象リソースの管理の停止

現在管理対象のサーバの管理を停止できます。

次の手順に従ってください:

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインで［データ センター］フォルダおよび［CA Server Automation サービス］フォルダを展開します。

   データ センターによって検出され、管理されているリソースが表示されます。

3. サーバを右クリックし、［管理］-［管理対象外］を選択します。

   サーバを管理対象外にするかどうかを確認するメッセージが表示されます。

4. ［OK］をクリックします。

   管理対象外サーバは管理対象リソース リストに表示されません。管理対象外サーバを表示するには、［エクスプローラ］ペインで［管理対象外］フォルダを開きます。

管理対象外リソースの管理

検出済みのリソースは、管理対象リソースのリストに追加することにより、パフォーマンスをモニタできます。

リソースを管理する方法

1. ［リソース］をクリックし、［管理］ペインを開きます。
2. ［管理］セクションで［システムの管理］をクリックします。
3. ドロップダウン リストから［管理対象外サーバ］を選択します。

   管理対象外リソースのリストが表示されます。

4. 管理するリソースを選択し、［アクション］ドロップダウン メニューで［管理］をクリックします。

   リソースを管理対象にするかどうかを確認するメッセージが表示されます。

5. ［管理対象］フォルダを展開します。

   リソースが［管理対象］リスト内に表示されます。また、メトリック収集が次の記録サイクルで開始されます。

管理対象リソースの削除

管理が不要になったリソースは削除できます。

管理対象リソースを削除する方法

1. ［リソース］をクリックします。
2. ［リソース］ページが表示されます。
3. ［エクスプローラ］ペインで［データ センター］フォルダおよび［CA Server Automation サービス］フォルダを展開します。

   データ センターによって検出され、管理されているリソースが表示されます。

4. サーバを右クリックし、［管理］-［システムから削除］を選択します。

   削除するかどうかを確認するメッセージが表示されます。

5. ［OK］をクリックします。

   削除済みのサーバは、管理対象サーバ リストおよび管理対象外サーバ リストに表示されません。

SystemEDGE 機能

SystemEDGE は、物理および仮想システムの SNMP ベースのモニタリングを提供する軽量エージェントです。 このエージェントを使用して、システム設定、パフォーマンス、ユーザ、ファイル システムなどの重要なシステム情報にアクセスします。 指定したしきい値または条件に基づいて、この情報をモニタし、モニタに基づいたオブジェクトを作成して集計オブジェクト状態を維持します。

SystemEDGE は、以下の MIB からのモニタリング メトリックをサポートします。

- MIB-II （RFC 1213）
- Host Resources MIB（RFC 1514）
- システム管理 MIB （CA 固有）
- IF-MIB （一部） （RFC 2233）
- IP-MIB （一部） （RFC 4293）
- TCP-MIB （一部） （RFC 4022）
- UDP-MIB （一部） （RFC 4113）

システム管理 MIB のモニタリング テーブルを使用して、以下のタイプのインテリジェントなモニタリングを有効にすることができます。

セルフ モニタリング

エージェントがサポートする任意の整数ベース MIB オブジェクトのモニタリングを提供します。 セルフ モニタ テーブルにエントリを作成して、モニタするオブジェクト、比較演算子、しきい値、および重大度を指定します。 エージェントは、このエントリに従って自動的にオブジェクトをモニタします。エージェントはオブジェクトをモニタし、指定されたしきい値および重大度値に従って現在の状態を維持します。 しきい値に違反すると、エージェントが状態変更トラップを送信します。

プロセスとサービスのモニタリング

任意のプロセス、Windows サービス、またはアプリケーションのモニタリングを提供します。 プロセス モニタ テーブルにエントリを作成して、プロセスまたはサービスが実行されているかをモニタするか、指定されたしきい値に対してプロセス テーブル オブジェクトをモニタします。 エージェントはプロセスをモニタし、指定されたしきい値および重大度値に従って現在の状態を維持します。 しきい値に違反するか、プロセス（実行中または停止中）の状態が変わると、エージェントは状態変更トラップを送信します。

プロセス グループ モニタリング

プロセスのグループを定義し、そのグループの変更をモニタする機能を提供します。 プロセス グループ モニタ テーブルでエントリを作成してプロセス グループを定義します。このグループをエージェントがモニタします。プロセス グループが変更された場合は、エージェントがトラップを送信します。

ログ ファイルおよびディレクトリ モニタリング

正規表現として指定された文字列を検索して、任意の UTF-8 エンコーディング システムまたはアプリケーション ログ ファイルのモニタリングを提供します。 ログ モニタ テーブルのエントリを作成します。エージェントは、指定されたログ ファイルで、ユーザ定義の正規表現に一致する行をモニタします。 一致する行が見つかると、エージェントがトラップを送信します。 送信されたトラップに含まれる重大度をモニタに関連付けることができます。

Windows イベント モニタリング

イベント ソースなどのさまざまなフィルタを使用して、Windows イベント ログ エントリのモニタリングを提供します。 NT イベント モニタ テーブルのエントリを作成します。エージェントは、イベント ログで、ユーザ定義の正規表現に一致するイベントをモニタします。 一致する行が見つかると、エージェントがトラップを送信します。

履歴の収集

マネージャ側ベースライニングおよび傾向分析用の履歴データ収集を提供します。 履歴制御テーブルでエントリを作成します。エージェントは、時間が経つにつれてメトリックを収集します。 メトリックを使用して、特定の期間中の平均システム パフォーマンスの図を提供します。

モニタリング機能および SystemEDGE アーキテクチャの詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

関連項目

システム管理 MIB (P. 74)
状態管理モデル (P. 77)
オブジェクト集計の設定 (P. 274)
ステートレスなモニタリング (P. 79)
管理対象モードおよび管理対象外モード (P. 79)

システム管理 MIB

システム管理 MIB は、根本的なシステムおよびそのアプリケーションのヘルス状態およびパフォーマンスをモニタするためのオブジェクトを含むプライベート MIB です。

システム管理 MIB 内でモニタできる、オブジェクトを備えたグループおよびテーブルを以下に示します。

システム グループ（sysedgeSystem）

ホスト名、CPU タイプ、およびオペレーティング システムのバージョンなどの基本システム情報が含まれます。

マウントされたデバイス テーブル（devTable）

ホスト上でマウントされたデバイスとファイル システムに関する情報が含まれます。 ファイル システム スペースなどの値のモニタを作成できます。または、このテーブルに列値を設定して、マウントされたデバイスをマウント解除できます。

カーネル設定グループ（kernelConfig）

CPU の数、仮想メモリの量、およびクロック速度などのカーネル情報が含まれます。 このグループを使用して、カーネルの設定方法およびカーネルのバージョンをモニタできます。

ブート設定グループ（bootconf）

ルート ファイル システム、ダンプ ファイル システム、およびスワップ領域に関する情報が含まれます。 このテーブルをモニタして、ルート ファイル システム名、ファイル システム ブロック、およびファイル システム タイプなどの値を追跡します。

ストリーム グループ（streams）

ストリーム I/O サブシステムに関する情報が含まれます。 使用中のストリームの数、ストリーム割り当て失敗の数、およびキュー内のストリームの数など、このグループ内のオブジェクトをモニタして、サブシステムのヘルス状態をモニタできます。

ユーザ テーブル（userTable）

システム上のユーザ アカウントに関する情報が含まれます。

グループ テーブル（groupTable）

システム上のユーザ グループに関する情報が含まれます。

プロセス テーブル（processTable）

実行中のプロセスに関する情報が含まれます。 このテーブルをモニタして、現在実行されているプロセスを追跡できます。また、特定の属性を設定して、プロセスを制御することもできます。 たとえば、processkill 列の値を 9 に設定して、プロセスを強制終了できます。

Who テーブル（whoTable）

システムに現在ログオンしているユーザに関する情報が含まれます。 このテーブル内の属性をモニタして、任意の特定の時間にシステムを使用しているユーザを追跡できます。

リモート シェル グループ（remoteshell）

リモート システムでシェル スクリプトとプログラムを実行するための属性が含まれます。 このテーブルで属性を設定して、コマンド、その引数、および出力ファイルの名前を指定します。

カーネル パフォーマンス グループ（kernelperf）

ホスト オペレーティング システムのヘルス状態およびパフォーマンスに関する情報が含まれます。現在のプロセスおよび開いているファイルの数、アクティブなジョブの数、およびスケジューラ キュー内のジョブの数などの属性をモニタできます。

プロセス間通信テーブル（msgqueTable、shmemTable、semTable）

メッセージ キュー、共有メモリ、およびセマフォに関する情報が個別のテーブルに含まれます。 これらのテーブルをモニタして、プロセス間の通信を調整します。

メッセージ バッファ割り当てテーブル（mbufAllocTable）

システムがどのようにメッセージ バッファを使用しているかに関する情報が含まれます。このテーブルの属性をモニタして、バッファ リクエストが拒否された回数または遅れた回数などの情報を追跡します。

ストリーム バッファ割り当てテーブル（strbufAllocTable）

Streams サブシステムによって使用されるバッファのバッファ割り当ておよび使用状況の統計に関する情報が含まれます。

I/O バッファ キャッシュ グループ（ioBufferCache）

基本ディスク I/O の I/O バッファ割り当ておよび使用状況に関する情報が含まれます。 このテーブルをモニタして、I/O バッファ アクティビティのピーク時などの情報を追跡します。

ディレクトリ名のルックアップ キャッシュ グループ（dnlc）

ディレクトリおよびファイル名キャッシュのパフォーマンスに関する情報が含まれます。

AIX 論理パーティション グループ（logicalPartition）

IBM AIX 論理パーティション（LPAR）に関する情報が含まれます。 各パーティションの物理または論理 CPU などの属性、および各パーティションの CPU の数をモニタできます。

トラップ コミュニティ テーブル（trapCommunityTable）

設定済みコミュニティ、ユーザ、およびトラップ デスティネーションなどの SNMP 情報が含まれます。

NT システム グループ（ntSystem）

Windows システムに固有の情報が含まれます。 このグループには、システム、スレッド、レジストリ、サービス、システム パフォーマンス、キャッシュ パフォーマンス、メモリ パフォーマンス、ページ ファイル パフォーマンス、およびイベント モニタの各グループが含まれ、Windows システム上のこれらの領域の属性をモニタします。

RPC 統計グループ（rpc）

カーネル リモート プロシージャ コールに関する情報が含まれます。このテーブルをモニタして、RPC アクティビティのピーク時を検出するためのカウンタおよび統計などの属性を追跡します。

NFS 統計グループ（nfs）

カーネルの NFS 機能に関する情報を含みます。 このテーブルをモニタして、NFS アクティビティのピーク時を検出するための統計およびカウンタなどの属性を追跡します。

ディスク統計テーブル（diskStatsTable）

ディスク I/O に関する情報が含まれます。

CPU 統計テーブル（cpuStatsTable）

各 CPU のパフォーマンス統計が含まれます。 アイドル モードでの経過時間、および待機モードでの経過時間などの属性をモニタできます。

システム管理 MIB にはまた、モニタリング テーブルおよびオブジェクト集計をサポートするためのテーブルも含まれます。

状態管理モデル

SystemEDGE エージェントは、CA Server Automation 管理モデル全体に統合された、セルフ モニタおよびプロセス モニタ用の状態管理モデルをサポートします。 エージェントは、さまざまな重大度の複数のモニタを単一の管理対象オブジェクトに集計します。 このオブジェクトの状態は、最高の重大度の違反されたモニタに対応します。

エージェントは、割り当てられた重大度値に従って、個々のモニタ状態を計算します。 計算結果の状態は、以下のいずれかです。

- 不明（1）
- OK （2）
- 警告（3）
- マイナー（4）
- メジャー（5）
- 重大（6）
- 致命的（7）
- 稼働中（11）
- ダウン（12）

注: モニタの重大度が「なし」の場合は、状態が「稼働中」と「ダウン」のいずれかに切り替わります。

システム管理 MIB の集計テーブルは、オブジェクト クラス、インスタンス、および属性値を使用して、同じ値のモニタを 1 つのエントリに集計します。 このエントリは、モニタされたオブジェクトを表し、このオブジェクトに対して集計状態が維持されます。

注: オブジェクト クラス、インスタンス、および属性の値をモニタに入力しない場合は、エージェントが、意味のあるデフォルト情報を入力します。デフォルト セルフ モニタ値は、モニタされた OID をインスタンス、クラス、および属性値にマップする sysedge.oid ファイルを使用するモニタされた OID に基づいています。 デフォルト プロセス モニタ値は、プロセス正規表現とモニタされた属性に基づいています。

集計テーブルは、しきい値違反によってオブジェクトのすべてのモニタが最悪の状態になる場合にのみ、テーブル内の現在の状態を更新し、状態変更トラップを送信します。たとえば、3 つのモニタで CPU 使用率をモニタしており、その 1 つが 60 パーセント（割り当てられた重大度が「警告」）、もう 1 つが 80 パーセント（重大度が「重大」）、もう 1 つが 100 パーセント（重大度が「致命的」）で、エージェントが 82 パーセントの CPU 使用率を返したと仮定します。 この値は、60 パーセントおよび 80 パーセントのモニタでしきい値違反を引き起こします。ただし、エージェントは、80 パーセントのモニタに対する 1 つの状態変更トラップのみを送信し、集計状態を「重大」変更します。

ステートレスなモニタリング

ステートレスなモニタは、オブジェクト ステータス情報の取得も、オブジェクト モデルによる全体的オブジェクト状態の維持も行いません。 これらのモニタは重大度値を維持しますが、この重大度の目的は、個々のモニタの重要性の追跡であるため、オブジェクト状態の計算には使用されません。 以下のテーブルは、ステートレスなモニタリングをサポートします。

- プロセス グループ モニタ
- ログ ファイル モニタ
- NT イベント モニタ

これらのモニタは、CA Server Automation ユーザ インターフェースで設定できますが、その結果であるデータは表示できません。 定義されたモニタに基づいて、以下のいずれかが検出された場合は、エージェントが送信するトラップを調べる必要があります。

- プロセス グループの変更
- 指定した正規表現に一致するログ ファイル メッセージ
- ディレクトリしきい値違反
- 指定した基準に一致する Windows イベント ログ イベント

プロセス グループ、ログ ファイル、および Windows イベント モニタの作成の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

管理対象モードおよび管理対象外モード

SystemEDGE を展開（またはスタンドアロン方式でインストール）するときに、管理対象モードでエージェントを実行するように指定できます。管理対象モードでは、エージェントの展開元である CA Server Automation マネージャ ノード（またはスタンドアロン エージェント インストールで指定したマネージャ ノード）によってエージェントが管理されます。 管理対象モードでエージェントを実行すると、リモート設定および CA Server Automation ユーザ インターフェースからの高度な視覚化など、すべての CA Server Automation エージェント管理機能が有効になります。 また、管理対象モードでは、CA Server Automation が、エージェント設定のプライマリ ソースとして確立されます。 管理対象モードのエージェントが CA Server Automation の外部で変更された場合、CA Server Automation 管理者は、その変更をブロックまたは上書きすることができます。

また、SystemEDGE を、レガシー モードで、または設定を制御する CA Server Automation マネージャなしで実行することもできます。 レガシー モードで実行されるエージェントが使用できるのは、レガシー モニタ、または状態の維持と計算を行わないモニタだけではありません。

CA Server Automation からエージェントを展開するときは、パッケージ ラッパーの設定で［管理対象モードでの実行］チェック ボックスを使用して、管理対象モードで実行するかどうかを指定します。 エージェントを CA Server Automation とは別にインストールするときは、管理対象モードで実行するためにエージェントの CA Server Automation マネージャ ノードを使用します。

Application Insight Module（AIM）

Application Insight Module （AIM）は、アプリケーション固有のイベントとプロセスをモニタおよび管理する機能を追加します。 AIM は SystemEDGE の機能拡張です。

Cisco Unified Computing System（UCS）用の AIM

CA Server Automation は Cisco UCS と対話して、デバイスを照会し、統計情報を収集します。 Cisco UCS は、各種リソースを異種システムとして管理するのではなく、ネットワーク、ハードウェア、ストレージ、および仮想化の各リソースを 1 つの連携システムに統合します。

Citrix XenDesktop 用の AIM

Citrix XenDesktop 環境をモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。

Citrix XenServer 用の AIM

Citrix XenServer 環境をモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 AIM は、XML RPC を使用して XenServers と直接通信することにより、設定されているすべての XenServer とリソース プールの全体ビューを取得します。

Active Directory および Exchange Server 用の AIM

クラウドおよび社内運用の両方のインフラストラクチャ上の Active Directory および Exchange Server をモニタする機能を提供します。 AIM によって、ドメインおよび Exchange Server の管理、保守、およびアップグレードを実施できます。

Huawei GalaX 用の AIM

Huawei GalaX 環境をモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。

IBM PowerHA 用の AIM

IBM PowerHA （旧名称「High Availability Cluster Multiprocessing」システム）をモニタする機能を提供します。

IBM PowerVM 用の AIM（LPAR）

LPAR を含むシステム全体をモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 AIM は Secure Shell（SSH）接続を介して HMC/IVM と通信します。したがって、関連付けられた HMC/IVM システムを介して POWER システム上の LPAR と通信できます。 HMC/IVM システム、および AIM が実行されている Windows サーバで、SSH が有効になっていることを確認してください。

KVM 用の AIM

RHEV 環境をモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 AIM は RHEV マネージャと通信して、マネージャに登録されるすべての KVM サーバの全体ビューを取得します。

Microsoft Cluster Service 用の AIM

Microsoft のクラスタをモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 Microsoft Cluster Service と通信して、モニタ対象のクラスタ、ノード、サービス、およびアプリケーションの全体ビューを取得します。

Microsoft Hyper-V 用の AIM

Microsoft Hyper-V 環境をモニタする機能を提供します。Hyper-V サーバ用の SystemEDGE AIM は、Hyper-V サーバで実行されます。

リモート モニタリング用の AIM

リモートの Windows システムをモニタする機能を提供します。リモート モニタリングは、エージェントレス モニタリングとも呼ばれます。

サービス レスポンス モニタ用の AIM

Windows、UNIX、または Linux サーバで実行されているサービスの健全性と応答性をモニタする機能を提供します。

Solaris ゾーン用の AIM

ゾーンを実行するように設定された Solaris システムをモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 SSH 接続を介して、管理対象の Solaris ゾーン サーバと通信します。 管理対象の Solaris サーバ、および AIM が実行されている Windows サーバで、SSH が有効になっていることを確認してください。

VMware vCenter Server 用の AIM

VMware vCenter Server の管理下にあるシステムをモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。 AIM は vCenter Server ソフトウェアと通信して、関連付けのある VMware vCenter Server が管理するすべての ESX サーバの全体ビューを取得します。

VMware vCloud Director 用の AIM

VMware vCloud Director の管理下にある仮想システムをモニタする機能を提供します。 この AIM は、SystemEDGE がインストールされている任意の Windows システムで実行できます。

関連項目

NodeCfgUtil の概要 (P. 1220)

エージェントの設定

CA Server Automation ユーザ インターフェースでは、以下の 2 つの種類の SystemEDGE 設定が利用可能です。

ポイント設定

ポリシーを展開することなく、エージェントに単一の一時的な変更を加えることができます。たとえば、セルフ モニタしきい値を変更するか、一時プロセス モニタを追加するか、または SRM テストのセルフ モニタを作成することができます。 ポリシーを展開すると、ポイント設定が上書きされます。

ポリシー設定

1 つの操作で、管理対象マシンのセットに展開できるエージェント設定ポリシーを作成します。たとえば、共通モニタおよび SRM テストのセットを含むポリシーを定義し、企業内のすべてのシステムにそのポリシーを展開して、同一の重要なシステム メトリックが確実にモニタされるようにすることができます。

CA Server Automation ユーザ インターフェースからの管理対象モードのエージェントの設定は、その他のすべての設定形式より優先されます。sysedge.cf 設定ファイルまたは SNMP SET を介してユーザがローカル エージェントを手動で変更した場合は、ポリシーが適用された後に、これらの変更が CA Server Automation ポリシー設定で上書きされます。

関連項目

ポイント エージェント設定の実行 (P. 83)
設定の概要 (P. 198)

ポイント エージェント設定の実行

CA Server Automation を使用すると、ポリシーの作成も適用も行わずに、単一のエージェントへの単一またはポイント設定変更を実行することができます。 この機能は、単一のシステムのモニタリング設定を一時的に変更するためのものです。 以下のシナリオで、ポイント設定変更が有用または必要となる場合の例を説明します。

- 一時的に考慮される、個々のシステムに特有の変更すべて
- 一時的な異常に対処するための変更
- 一般的なモニタリング ポリシーにこれらをコミットする前の、さまざまなモニタリングの重大度としきい値を使用した実験用の変更

ポイント設定変更を行う場合、CA Server Automation は、すべての既存のポリシーまたはローカル設定に加えて、システムへの変更を適用します。ただし、次回にポリシーをシステムに適用するときは、ポイント設定変更がポリシーによって上書きされます。 ポイント設定変更は、ベース ポリシーにマージされるまで、またはポリシー アプリケーションによって上書きされるまで、ポリシー例外としてレポートされます。

ポイント設定は、セルフおよびプロセス モニタに対して実行できます。

ポイント エージェント設定を実行する方法

1. ［リソース］をクリックして、［エクスプローラ］ペインで設定するシステムを選択します。

   システム情報が右側のペインに表示されます。

2. 右側のペインの［設定］をクリックして、［セルフ モニタ］または［プロセス モニタ］を選択します。

   既存のセルフまたはプロセス モニタが表示されます。

3. ツールバーの［+］（新規）をクリックします。

   新しいセルフまたはプロセス モニタを作成するためのフィールドが表示されます。

4. 必要なフィールドに入力し、［保存］をクリックします。

   注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

   モニタが保存され、更新されたセルフまたはプロセス モニタのリストに表示されます。

また、既存のセルフまたはプロセス モニタの変更、削除、またはコピーも実行できます。

モニタリング ソフトウェアの設定

［モニタリング ソフトウェア］ページでは、個別のサーバ、サーバ グループ、またはサービス用の非ポリシー関連情報を設定できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. システムまたはサービスを選択します。

3. ［モニタリング ソフトウェア］をクリックします。

   ［マシンの詳細］ペインが表示されます。

4. 必要に応じて設定を変更し、［適用］をクリックします。

   System Description

   システムの説明を定義します。

   システム担当者

   システムの連絡先を定義します。

   システムの場所

   システムの場所を定義します。

   SystemEDGE **ログ レベル**

   SystemEDGE のログ レベルを指定します。

   設定が更新されます。

セキュリティおよび保守

CA Server Automation は、以下に示す、SystemEDGE エージェントのための強化されたセキュリティと保守のオプションを提供します。

- ユーザ インターフェースで設定可能な保守モード
- SystemEDGE エージェントの設定の単一ポイント
- CA Server Automation の外部で実行された変更をブロックする機能
- CA Server Automation の外部で実行された変更の通知、および不要な変更を無視または拒絶する機会

関連項目

保守モードの有効化 (P. 85)

保守モードの有効化

CA Server Automation で SystemEDGE 保守モードを有効にできます。このモードでは、エージェントが、すべてのモニタ エントリの処理およびトラップ送信を停止します。 保守モードは、エージェントのシステムが計画に従って停止中に、誤ったアラーム トラップを受信しないようにする場合に便利です。

保守モードでは、エージェントはメトリックの収集を続行し、SNMP 要求に応答しますが、すべてのモニタおよび履歴収集の処理を一時停止します。エージェントは、保守期間の初めにすべてのモニタの現在値を保存して、保守期間の最後の現在値と比較します。また、必要な場合は、現在値に応じてトラップを送信します。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［管理対象］を展開し、システムを選択します。
3. ［モニタリング ソフトウェア］をクリックします。

   ［マシンの詳細］ペインが表示されます。

4. ［保守モード］オプションを［有効］に設定し、［適用］をクリックします。

   エージェントがウォーム スタートを実行し、保守モードが有効になります。

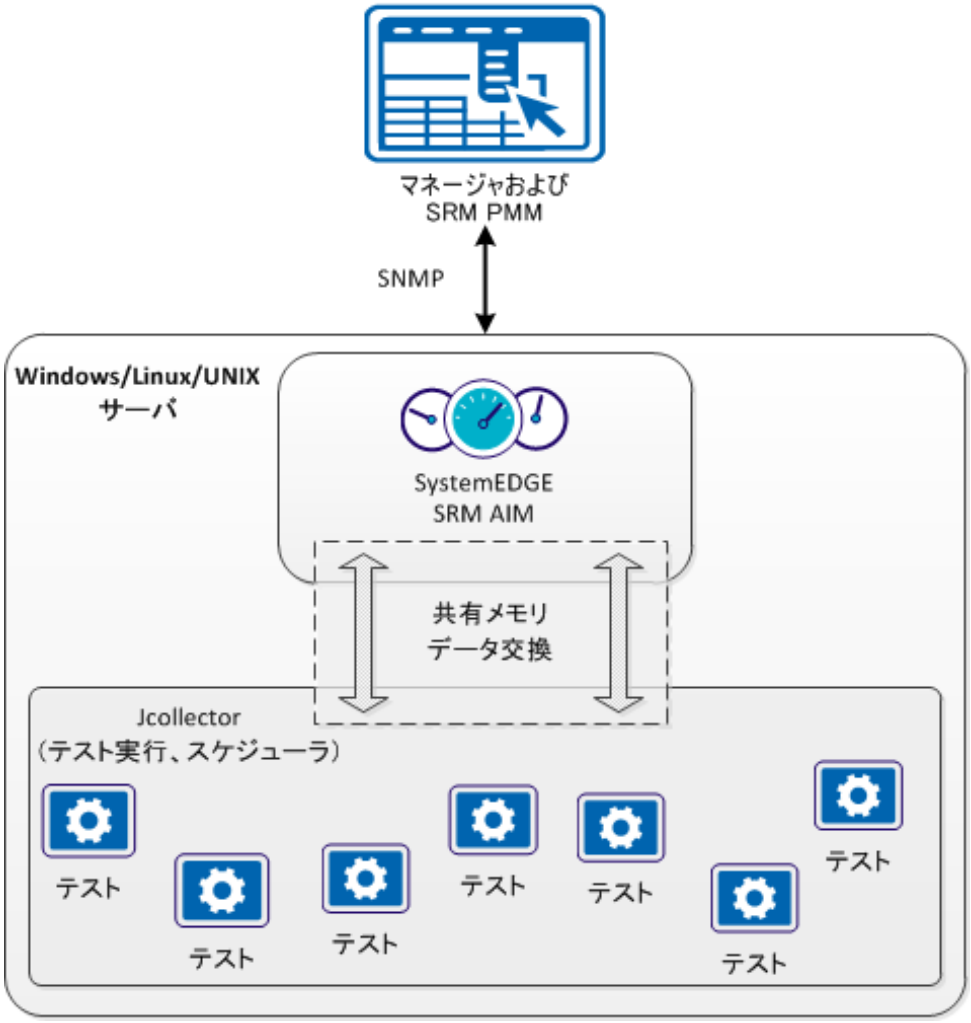
エージェントで保守モードを終了するには、［保守モード］を無効にして［適用］をクリックします。

サービス レスポンス モニタリング

サービス レスポンス モニタリング Application Insight Module （SRM AIM）は、SystemEDGE の拡張機能（プラグイン）です。 SRM は、ローカルまたはリモート システムで実行される論理または物理サービスの応答を取得します。 SRM は Java ベースのマルチスレッドで、複数のサーバにわたって複数のテスト設定を処理します。 SRM は、事前設定テストまたはカスタム テストを実行して、実行の経過時間とスループットを測定します。

以下の図は、これらの関係を示しています。

サービス レスポンス モニタリング コンポーネント間のインタラクション



svcrsp.cf 設定ファイルにはテストの仕様が含まれます。 SRM AIM は、この設定ファイルを読み取り、テストの仕様を共有メモリ セグメントで利用できるようにします。 SRM Jcollector コンポーネントは、共有メモリから各テスト設定を読み取ります。 Jcollector はテストを実行し、このタイミング プロセスの結果を収集して、それを SRM AIM にプロパゲートします。 SystemEDGE は、これらの結果および関連付けられたステータス情報を CA Server Automation に送信します。

サービス レスポンス モニタ（SRM）AIM は、DNS、DHCP、SQL などの重大なシステム サービスの可用性と応答時間を、定義済みしきい値に基づいてモニタします。SRM テストを作成して、この機能を有効にします。SRM テストを使用すると、以下を実行できます。

- システム サービスの可用性と応答時間のテスト
- ユーザが影響を受ける前の、複雑な多層インフラストラクチャ内での可視性の取得による問題の特定
- 遅延、停止、およびパフォーマンスの問題のリアルタイム通知の取得
- DNS や DHCP などのサービスがサービス レベル アグリーメントに準拠して実行されていることの確認
- キャパシティ計画、トラブルシューティング、または長期にわたる動作での傾向分析のための履歴データの保守

CA Server Automation は、SRM AIM の以下の機能を提供します。

- SystemEDGE エージェントによるリモート展開
- リモート テスト設定
- テストの視覚化

SRM AIM アーキテクチャの詳細については、「SRM ユーザ ガイド」を参照してください。

関連項目

SRM テスト (P. 89)

SRM テスト

SRM AIM は、以下の反応時間テストを提供します。

Active Directory

Windows Active Directory サービスが正しく動作して、共有ファイルとリソースを管理することを確認します。

カスタム

重要なカスタム サービスまたは他のタスクが効率よく動作することを確認します。

DHCP

DHCP （Dynamic Host Configuration Protocol）サーバが応答して、アドレス要求に応答することを確認します。

DNS

DNS （Domain Name System）サーバがホスト名を処理して、アドレス解決要求を処理することを確認します。

ファイル I/O

ファイル システム全体での読み取り、書き込み、および比較の作業を確認します。

FTP および TFTP

ユーザが、指定されたサーバにログインして、ファイルのアップロードとダウンロードを実行できることを確認します。

HTTP および HTTPS

ユーザがビジネス Web サーバに接続できることを確認し、また特定のテキストが Web ページ上に表示されるかどうかを確認します。

LDAP

LDAP サーバへの接続を確認して、ユーザ リクエストおよび LDAP クエリ用のアクセスを確認します。

NIS

NIS マップ リクエストが処理されていることを確認します。

NNTP

ユーザが Usenet ニュースグループ サーバおよび社内掲示板に接続できることを確認します。

PING

ネットワーク デバイスが存在し、ネットワークを介してアクセス可能であることを確認します。

電子メール

電子メール サーバが利用可能であり、電子メールを効率よく処理することを確認します。 SRM は、 IMAP、MAPI、POP3、SMTP、および SMTP サーバから発信される往復の電子メールのテストをサポートします。

SNMP

SNMP エージェントが SNMPv1 GET リクエストに応答することを確認します。

SQL クエリ

SQL データベース サーバが利用可能で、短いクエリを処理することを確認します。

TCP

システムが接続リクエストをリスンして、処理することを確認します。

仮想ユーザ

記録可能な（通常は WinTask で）実際のユーザ トランザクション（キーボード入力とマウスのクリック）の継続的な応答時間および可用性データを取得して、ビジネス タスクが正常に実行されていることを確認します。

エージェントの視覚化

CA Server Automation ユーザ インターフェースは、管理対象モードのエージェントを備えたシステムのモニタリング情報を表示します。 プラットフォーム管理モデル（PMM）は、エージェント情報を解釈して変換し、この情報が根本的な CA Server Automation AIP アーキテクチャに適合して、AOM データベースに表示されるようにします。 PMM は、ベース SystemEDGE エージェントおよび SRM AIM で利用可能です。

CA Server Automation ユーザ インターフェースで視覚化できるエージェント データには、以下が含まれます。

- 状態管理モデルを使用して作成された管理対象オブジェクト。
- すべての管理対象オブジェクトの状態
- 個々のモニタ
- SRM テスト

関連項目

管理対象オブジェクト状態の表示 (P. 92)
SystemEDGE モニタの表示 (P. 91)
サービス レスポンス テストの表示 (P. 93)

SystemEDGE モニタの表示

CA Server Automation ユーザ インターフェースには、管理対象モードで SystemEDGE を実行しているシステムの定義済みのセルフ モニタとプロセス モニタがすべて表示されます。 各モニタに関する詳細を表示し、モニタの追加、削除、変更、コピーなどのポイント設定を実行 (P. 83)できます。

SystemEDGE モニタを表示する方法

1. ［リソース］をクリックして［管理対象］を展開し、いずれかのシステムを選択します。

   システムの［サマリ］ページが右側のペインに表示されます。

2. ［設定］をクリックして、［セルフ モニタ］または［プロセス モニタ］をクリックします。

   ［セルフ モニタ］または［プロセス モニタ］ペインが表示されます。

［セルフ モニタ］および［プロセス モニタ］ペインには、以下のモニタ プロパティをリスト表示した表が含まれます。

- インデックス
- 状態
- ステータス

注: この状態は、モニタが関連付けられた管理対象オブジェクトの状態と同じではない場合があります。 管理対象オブジェクトの状態は、オブジェクトを構成するすべてのモニタの中で最悪の現在の状態です。

- オブジェクトのクラス、インスタンス、および属性

  注: これらの列の値が同じであるモニタは、同じ管理対象オブジェクトの一部です。

- 現在モニタされているオブジェクトの値、演算子、およびしきい値
- 重大度
- トラップ数
- 最後のトラップ

管理対象オブジェクト状態の表示

CA Server Automation ユーザ インターフェースには、管理対象システムの SystemEDGE 管理対象オブジェクトがすべて表示されます。

管理対象オブジェクト状態の表示方法

1. ［リソース］をクリックし、［エクスプローラ］ツリーの適切なフォルダを展開して、SystemEDGE が実行される管理対象システムを選択します。

   システムの［サマリ］ページが右側のペインに表示されます。

［システム ステータス情報］ペインには、管理対象オブジェクトの総数および最大のオブジェクト重大度が含まれます。

［管理対象オブジェクト］テーブルには、各管理対象オブジェクトに関する以下の情報が含まれます。

- ヘルス状態
- 稼働ステータス（アクティブ、保守中、破棄）
- オブジェクト クラス、インスタンス、および属性
- 現在モニタされている値、オペレータ、しきい値、およびモニタリング マシン名

このテーブルから、管理対象オブジェクトを選択して［アクション］-［定義に移動］をクリックし、管理対象オブジェクトを形成するモニタを表示できます。

サービス レスポンス テストの表示

CA Server Automation ユーザ インターフェースには、サービス レスポンス モニタ AIM を備えた管理対象モードで SystemEDGE を実行するシステムに対するサービス レスポンス テストが表示されます。

サービス レスポンス テストの表示方法

1. ［リソース］をクリックして［管理対象］を展開し、いずれかのシステムを選択します。

   システムの［サマリ］ページが右側のペインに表示されます。

2. ［詳細］をクリックして、［サービス レスポンス］をクリックします。

   ［サービス レスポンス テスト］ペインが表示されます。

［サービス レスポンス テスト］ペインには、以下のテスト プロパティをリスト表示する表が含まれます。

- インデックス番号
- オブジェクト クラス名
- テストの名前とタイプ
- テスト送信先
- 間隔
- ステータス
- 最終結果
- エラー総数

第 5 章: SystemEDGE および Application Insight Module（AIM）の管理

この章では、環境にモニタリング ソフトウェアを設定する方法について説明します。 また、適切なユーザ権限と、SystemEDGE を管理対象モードまたは管理対象外モードに変更する方法の詳細についても説明します。

このセクションには、以下のトピックが含まれています。

ユーザ権限およびアクセス要件のリファレンス

以下のセクションでは、CA Server Automation コンポーネントをインストールし、CA Server Automation を使用して環境をモニタするためのアクセス要件の概要を説明します。 各セクションでは、必要な通信ポートについても説明します。 マネージャの分散インストールがファイアウォールをまたぐ場合は、以下のリストを使用して、必要な通信ポートが開いていることを確認できます。

このドキュメントの対象読者は以下のとおりです。

- 仮想環境を管理するために CA Server Automation をインストール、設定、使用する管理者。
- 仮想環境をモニタするために CA Server Automation を使用するオペレータ。

関連項目:

Active Directory および Exchange Server（ADES）

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

（Exchange 2007）ドメイン管理者または Exchange 管理者の役割が必要です。

（Exchange 2010）Exchange Organization Management の役割が必要です。

通信ポート

PowerShell ポート： 80、443、5985、5986

ADSI ポート： 3268、389

Cisco UCS

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ブレードの電源操作、サービス プロファイルの操作、プール操作、ポリシー操作、インポート/エクスポート操作といった UCS 操作を実行するために十分な権限を持った UCS Manager のユーザ アカウントが必要です。

注: UCS ユーザ管理者権限を与えることを推奨します。

管理者権限を与えることができない場合は、UCS ユーザに以下の役割を割り当てます。

- Ext-lan-config
- Ext-san-config
- Service-profile-config
- Service-profile-config-policy
- Service-profile-ext-access
- Service-profile-network
- Service-profile-network-policy
- Service-profile-qos
- Service-profile-qos-policy
- Service-profile-security
- Service-profile-security-policy
- Service-profile-server
- Service-profile-server-oper
- Service-profile-server-policy
- Service-profile-storage

- Service-profile-storage-policy
- Operations
- Server-equipment

通信ポート

HTTP ポート： 80

HTTPS ポート： 443

Citrix XenDesktop

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

Citrix XenDesktop バージョン 5.6 では、XenDesktop で少なくとも読み取り専用の管理者の役割を持つ Active Directory アカウントが必要です。

通信ポート

WinRM ポート： 5985、5986

SNMP ポート： 161

WMI ポート： 135

Citrix XenServer

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

（XenServer 6.0 以降）読み取り専用の役割を持つルートまたは Active Directory のサブジェクトが必要です。

通信ポート

HTTPS ポート： 443

SNMP ポート： 161

Huawei GalaX

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

Huawei GalaX モニタリングでは、管理者のユーザ認証情報と、GalaX 環境から取得した対応する p12 ファイルが必要です。

通信ポート

HTTP ポート： 8773

Hyper-V

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ローカルの管理者アカウントが必要です。

SCVMM モニタリング

System Center Virtual Machine Monitoring （SCVMM）の管理者の役割が必要です。

通信ポート

Windows RPC エンドポイント マッパー ポート： 135

DCOM/WMI ポート： RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

IBM PowerHA

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

PowerHA の監視

以下の CLI コマンドを実行する権限を持つアカウントが必要です。

- clstat
- clRGinfo -s
- cldump
- cllsnw
- cltopinfo
- cllsif
- clshowsrv -v
- vmstat

通信ポート

Secure Shell TCP ポート： 22

IBM PowerVM

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

以下の要件は、CA Server Automation でモニタする既存の環境によって異なります。

ハードウェア管理コンソール（HMC）

hmcsuperadmin タスク役割アカウントが必要です。 リソース役割に管理する P-Server だけが含まれるユーザを定義することを推奨します。

注: HMC モニタリングには、HMC *および*VIOS 設定の *両方*が必要です。

仮想 IO サーバ（VIOS）のモニタリング

モニタする VIOS 上の padmin ユーザ アカウントが必要です。

Integrated Virtualization Manager（IVM）のモニタリング

モニタする IVM 上の padmin ユーザ アカウントが必要です。

注: IVM モニタリングには IVM 設定が必要です。

通信ポート

Secure Shell TCP ポート： 22

Microsoft Cluster Server

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

ドメイン管理者アカウントまたはクラスタ ノードのローカル アカウントが必要です。 ドメイン ユーザを使用する場合は、ドメイン管理者グループに属している必要があります。 クラスタ ノードのローカル アカウントを使用する場合は、ユーザが管理者グループのメンバである必要があります。

重要: すべてのノードに同じクラスタ ノード ローカル認証情報をセット アップしてください。 クラスタ サービスが別のノードに移動され、そのノードには別の認証情報がある場合、AIM が接続できなくなります。

通信ポート

Windows RPC エンドポイント マッパー ポート： 135

DCOM/WMI ポート： RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

Oracle Solaris ゾーン

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

root ユーザによるアクセスが必要です。

通信ポート

Secure Shell TCP ポート： 22

Red Hat Enterprise Virtualization

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

スーパーユーザ権限を持つ、対応する Red Hat Enterprise Administrator の役割が必要です。

注: Microsoft Active Directory （AD）ユーザまたは Red Hat Enterprise IPA ユーザを使用できます。

通信ポート

REST API ポート： 8443

リモート展開エージェント

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

Windows へのインストール

Windows のシステム管理者権限が必要です。

Linux へのインストール

root アクセス権、あるいは sudo または pfexec の使用が必要です。

クロスプラットフォーム リモート展開

インフラストラクチャ展開（ID）を使用します。

ID マネージャ コンポーネント

（Windows のターゲット）ターゲット マシンに Windows 共有 Admin$ のマッピングが必要です。

（UNIX または Linux のターゲット）マネージャとターゲットの間の SSH 接続が正しく行われていることが必要です。

リモート展開（Windows）

CIFS UDP ポート： 137 （受信/送信）

CIFS UDP ポート： 138 （受信/送信）

TCP ポート： 135

CIFS TCP ポート： 139 （受信/送信）

CIFS TCP ポート： 445 （受信/送信）

CAM UDP ポート： 4104 （受信/送信）

CAM TCP ポート： 4105 用の通信ポート

リモート展開（UNIX、Linux）

CAM UDP ポート： 4104 （受信/送信）

Secure Shell TCP ポート： 22 （受信）

TCP ポート： 135

CAM TCP ポート： 4105 用の通信ポート

リモート モニタリング

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

リモート モニタリング

Windows Management Instrumentation（WMI）へアクセスできる認証情報が必要です。

通信ポート

Windows RPC エンドポイント マッパー ポート： 135

DCOM/WMI ポート： RPC エンドポイントのネゴシエーション時に動的に割り当てられます。

ベスト プラクティスとして、リモート モニタリング システムは AD ドメインのメンバである必要があります。 このメンバシップによって、各 RM システムにローカルのユーザ アカウントを定義しなくても、ドメイン アカウントを使用することができます。 AD ドメインの Domain Admins グループのメンバである CARMuser ドメイン アカウントを作成します。

RM のインストール中にユーザ認証情報設定が要求されたときに、ドメイン アカウントとパスワードを指定します。 このドメインのシステム メンバには、追加の設定が不要です。

注: 必要に応じて、CARMuser アクセス権を制限し、ユーザが Domain Admins グループのメンバにならないようにすることができます。 この場合、WMI 名前空間アクセスおよび DCOM アクセスを設定する必要があります。 WMI 名前空間アクセスおよび DCOM アクセスの定義の詳細については、Microsoft の Web サイトを参照してください。

SystemEDGE と Advanced Encryption

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

Linux または UNIX へのインストール

root アクセス権または権限のないユーザ アカウント用の sudo 設定の使用が必要です。

モニタリング

cf ファイルを編集およびロードする権限、またはリモート設定を使用する権限。

通信ポート

UDP ポート： 161 （SNMP Get/Set 要求）、代替ポート： 1691

UDP トラップ ポート： 162 （送信）

管理対象モードの SystemEDGE は CAM を使用

CAM UDP ポート： 4104

CAM TCP ポート： 4105

VMware vCenter

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

（AIM に有効） AIM コンポーネント用の VC の読み取り専用ユーザ アクセスが必要です。

（PMM に有効）vSphere vCenter Server に対して指定される権限のセットが必要です。

重要: ユーザの役割は、実行する操作のタイプと一致する必要があります。そうでない場合は操作は実行できません。

通信ポート

HTTPS ポート： 443

VMware vCloud

このセクションでは、環境のインストールやモニタに必要なアクセス権限と、必要な通信ポートを一覧表示します。 一覧表示されている通信ポートが開いていることを確認してください。

AIM のインストール

AIM ホストに対する Windows システム管理者権限が必要です。

モニタリング

（AIM に有効） システム管理者の役割が必要です。

（VMware WS に有効）操作はユーザの役割に制限されています。

System Administrator@System

フル アクセスを許可します。

Organizational Access@org_name

組織レベルおよび役割の割り当ての操作に制限します。

通信ポート

REST API ポート： 8443

SNMP およびアクセス制御リストの設定方法

このセクションでは、グローバルとサーバ レベルの SNMP 設定の違い、アクセス制御リストを適用する方法、および SNMP を設定してシステムを正しく検出する方法について説明します。

関連項目:

SNMP の整合性 (P. 109)
グローバルおよびサーバ レベルの SNMP 設定 (P. 110)
SNMPv1/v2 設定およびアクセス制御リストの設定方法 (P. 112)
サーバ レベルの SNMP 設定を管理する方法 (P. 126)
SNMPv3 の設定方法 (P. 131)

SNMP の整合性

システムおよびネットワークを正しく検出するためには、SNMP 設定に整合性があることが必要です。 リモート システム上の SystemEDGE の SNMP 設定が CA Server Automation マネージャに存在しない場合は、CA Server Automation でそのシステム上の必要なリソースを検出できません。 CA Server Automation がシステムを検出するには、少なくとも有効な読み取り専用 SNMP 認証情報が必要です。

SystemEDGE エージェントをリモートに展開し、［ポリシー設定］によってエージェントを設定する場合は、マネージャと管理対象システムの間の SNMP の整合性に関する条件が自動的に満たされます。

リモート サーバ上で SNMP 設定をローカルに設定する場合は、SNMP 設定の整合性を確認します。 リモート サーバ上の SNMP 設定がマネージャ上で指定されていない場合は、CA Server Automation で不足している認証情報をグローバル SNMP オブジェクトとして指定し、リモート システムを検出します。

この章で説明する SNMP のシナリオおよび手順は、SystemEDGE エージェントが管理対象モードで実行されると仮定しています。 管理対象モードでは、SystemEDGE は CA Server Automation の［ポリシー設定］によって設定されます。

関連項目:

グローバルおよびサーバ レベルの SNMP 設定 (P. 110)

グローバルおよびサーバ レベルの SNMP 設定

サーバ レベルまたはグローバルの SNMP 設定のようなカテゴリは、CA Server Automation マネージャにのみ存在します。ポリシー設定では、これらの設定のコレクションをポリシーによって管理対象サーバに配布します。 これらの SNMP 設定は、最終的にそれぞれの管理対象のターゲット サーバの sysedge.cf 設定ファイルに反映されます。 SystemEDGE ではサーバ レベルまたはグローバルの SNMP 設定を区別しません。 この情報はマネージャにのみ格納されます。 マネージャは、ポリシーのどのバージョンがどの管理対象サーバに適用されたかを理解しています。

必要に応じて、CA Server Automation マネージャに独自のグローバルまたはサーバ レベルの SNMP 設定を追加できます。

ほとんどの場合、グローバル SNMP 設定のメカニズムにより、サーバの SNMP 設定を管理する柔軟性がもたらされます。特定のケースでは、サーバ レベルの SNMP 設定を使用することが必要な場合があります。 ポリシー設定により、ポリシー用に SNMP 設定のコレクションを作成するときの柔軟性が高まります。 必要に応じて、グローバルまたはサーバ レベルの SNMP 設定を選択できます。

グローバル SNMP 設定により、リモート展開用の SystemEDGE パッケージ ラッパーの以下のフィールドのドロップダウン リストが入力されます。

- ポート
- 読み取りコミュニティ
- 読み取り/書き込みコミュニティ

あるいは、フィールドをインラインで編集できます。

利用可能な SNMPv1 コミュニティ文字列はポート設定によって異なります。 ポート番号を初めて選択するときには、そのポート用のドロップダウン リストに有効なコミュニティ文字列が自動的に取得されます。 パッケージ ラッパーに認証情報が指定されていない場合は、インストーラはデフォルトでパブリックの読み取り専用文字列になります。 パッケージ ラッパーの認証情報は、SystemEDGE がインストールされた時点から、管理対象サーバがポリシー設定を登録して管理対象モードに入るときまで有効です。 SystemEDGE によってポリシーから設定がロードされます。

注: SystemEDGE は、インストールのために少なくとも 1 つの SNMPv1 コミュニティを必要とします。 CA Server Automation がサーバの SystemEDGE を検出した後、CA Server Automation はこれらの SNMPv1 設定をサーバ レベルの SNMP 設定として扱うことができます。

［管理］-［設定］-［展開 & 設定］の以下のオプションは、パッケージ ラッパーの SNMP 設定がサーバ レベルの SNMP 設定になるかどうかを制御します。

- SystemEDGE エージェントが登録されるときにサーバ固有の SNMP 設定を作成します。

このオプションが有効な場合、CA Server Automation はインストール用の SNMPv1 設定をサーバ レベルの SNMP 認証情報として使用します。

各リモート展開ジョブに対しては、展開プロセス中にターゲット システムに適用されるポリシーを指定できます。 特定のポリシーを指定しないと、CA Server Automation は SystemEDGE のデフォルト ポリシーを使用します。複数の SystemEDGE ポリシーを定義している場合は、SystemEDGE の［ポリシー］ペインのデフォルト ポリシーを既存のポリシーのリストから決定できます。

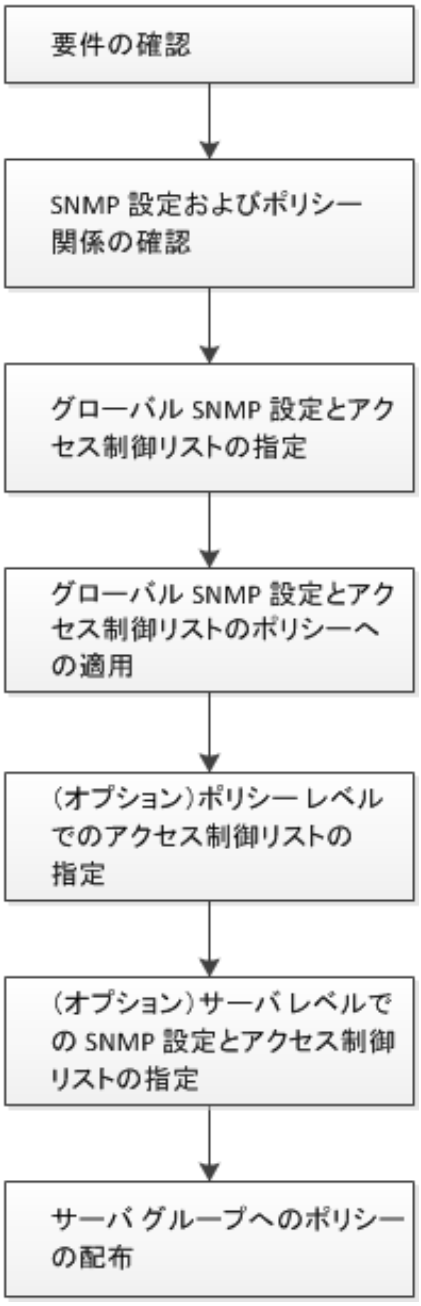
関連項目:

SNMPv1/v2 設定およびアクセス制御リストの設定方法 (P. 112)
サーバ レベルの SNMP 設定を管理する方法 (P. 126)
SNMPv3 の設定方法 (P. 131)

SNMPv1/v2 設定およびアクセス制御リストの設定方法

以下の図は、使用する環境に SNMP を設定するために必要なアクションの概要を示しています。 この図には、一般的および例外的なケースが含まれています。 例外的なケースはオプションとして図に表示されています。

SNMP 設定およびアクセス制御リストの設定方法



以下の手順に従います。

要件の確認（SNMPv1/2） (P. 114)
SNMP 設定およびポリシー関係の確認 (P. 115)
グローバル SNMP 設定とアクセス制御リストの指定 (P. 117)
グローバル SNMP 設定とアクセス制御リストのポリシーへの適用 (P. 118)
（オプション）ポリシー レベルでのアクセス制御リストの指定 (P. 120)
（オプション）サーバ レベルでの SNMP 設定とアクセス制御リストの指定 (P. 121)
サーバ グループへのポリシーの配布 (P. 122)
3 つのサーバ グループの例 (P. 123)

要件の確認（SNMPv1/2）

CA Server Automation の SNMP の設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、および Windows Server オペレーティング システムに精通している。
- CA SystemEDGE に関する基礎知識がある。
- モニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- 管理対象ノードでモニタリング エージェント（CASystemEDGE）にアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- CA Server Automation によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

関連項目:

SNMP 設定およびポリシー関係の確認 (P. 115)

SNMP 設定およびポリシー関係の確認

SNMPv1/v2 の SNMP 設定オブジェクトは、名前、コミュニティ文字列、操作のタイプ（読み取り専用または読み書き）、SNMP のバージョン、ポート、タイムアウト、再試行の制限、およびアクセス制御リスト（ACL）で構成されます。

ACL は、SystemEDGE が実行されている管理対象システムのグループのためのマネージャ システムのリストを指定します。 CA Server Automation マネージャは、ポリシー設定によって管理対象システムに SNMP 設定と ACL を配布します。 これらの管理対象システムは、ACL にリストされているマネージャ システムからのみ SNMP リクエストを許可します。ACL が指定されていない場合、管理対象システムはすべてのシステムから SNMP リクエストを許可します。

ACL が定義されている場合、CA Server Automation マネージャも ACL のリストに自動的に追加されます。 CA Server Automation マネージャには常に接続できます。

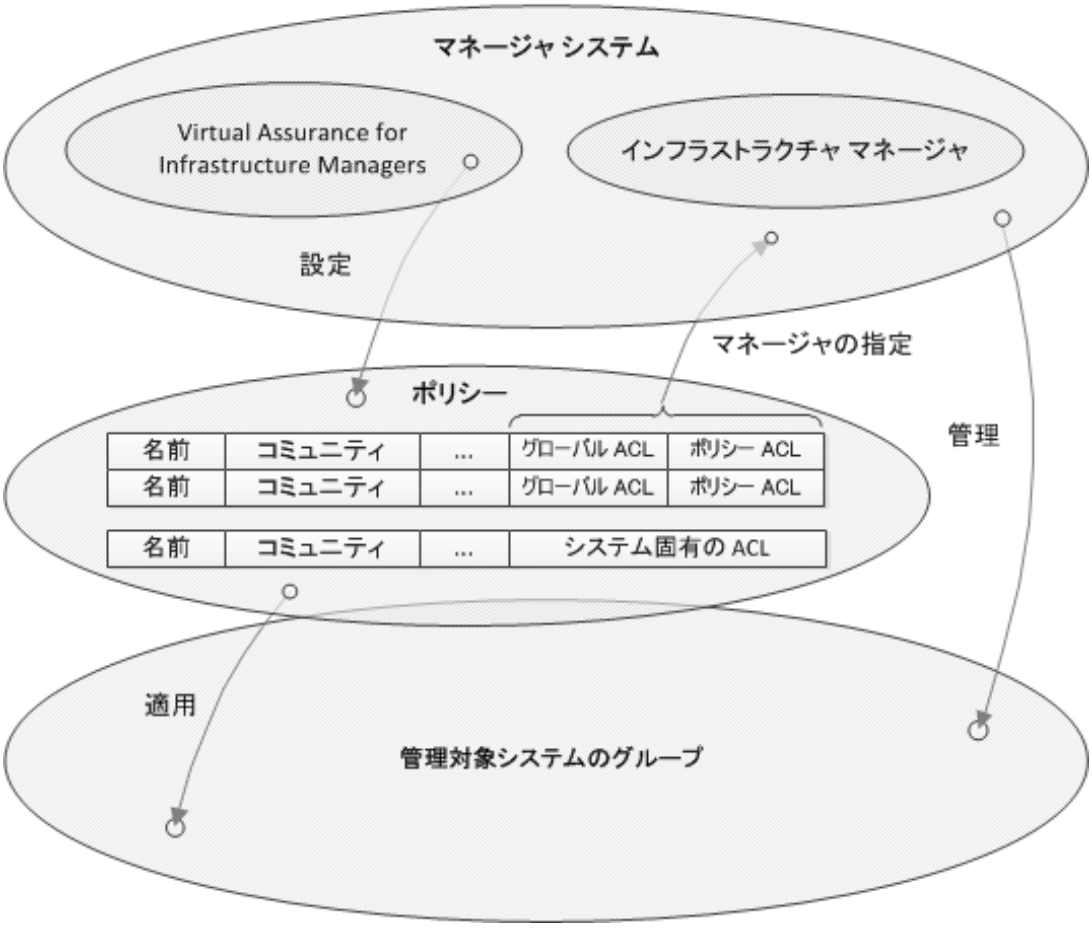
ほとんどの場合、多数またはすべてのシステムで同じ SNMP 認証情報が使用されます。 これらの認証情報を適切に管理し適用するために、グローバル レベルで SNMP 認証情報および ACL を指定できます。 システムを正しく検出し管理するには、マネージャ システムとエージェント システムで整合性のある SNMP 認証情報および ACL 設定が必要です。 グローバル SNMP 設定オブジェクトは、［管理］-［設定］-［SNMP］で指定します。

例外的なケースでは、ACL をポリシー レベルで追加、または SNMP 認証情報と ACL をシステム レベル全体で指定できます。 システム レベルで SNMP 設定を変更する場合は、影響を受ける各システムの設定を変更します。

これらの SNMP 設定だけがターゲット システムに適用され、ターゲット システムと同じポートを使用します。

以下の図は、ポリシーのアーキテクチャを示しています。

ポリシーのアーキテクチャ



SNMP 設定は、グローバル、ポリシー、またはシステム レベルで設定できます。また、これらの設定をポリシーに割り当てることができます（左上の矢印）。 ポリシーは CA Server Automation を使用して管理対象システムのグループに適用できます。 アクセス制御リスト（ACL）では、管理対象システムのグループを管理するマネージャ システムの名前を指定します。ACL に必要なマネージャ システムをすべて追加すると、管理対象システムはこれらのマネージャからの SNMP リクエストにのみ応答します。

関連項目:

グローバル SNMP 設定とアクセス制御リストの指定

SystemEDGE の SNMP 認証情報のためのアクセス制御リストは、グローバル、ポリシー、およびシステム レベルで設定できます。ACL をグローバルな SNMP オブジェクトに関連付けると、システムに固有の SNMP オブジェクトへの依存性を最小限に留めることができます。

ユーザ インターフェースの［管理］-［設定］-［SNMP］を使用して、ACL をグローバル レベルで編集します。

次の手順に従ってください:

1. ユーザ インターフェースで［管理］-［SNMP］に移動します。

   ［SNMP 設定］ページが表示されます。

2. （オプション） SNMP 設定オブジェクトを作成するには、［アクション］-［新規］をクリックします。

   ［新しい SNMP 設定］ダイアログ ボックスが表示されます。 SNMP 設定オブジェクトは、名前、コミュニティ文字列、操作のタイプ（読み取り専用または読み書き）、SNMP のバージョン、ポート、タイムアウト、再試行の制限、およびアクセス制御リスト（ACL）で構成されます。 SNMP 設定に適用する管理対象ノードに指定されたポート番号を使用します。

3. SNMP 設定オブジェクトの作成に必要なデータを指定して、［OK］をクリックします。

4. ACL に追加する SNMP 設定オブジェクトを選択し、［編集］アイコンをクリックします。

   ［SNMP 設定の編集］ダイアログ ボックスと ACL のパネルが表示されます。

5. ［ポリシー設定 SystemEDGE アクセス制御リスト］パネルでマネージャ システムの名前または IP アドレスを指定して、［OK］をクリックします。

   特定のグローバル SNMP 設定オブジェクトのための ACL が指定されます。

そのアクセス制御リストを使用してグローバル SNMP 設定オブジェクトをポリシーに適用できます。

関連項目:

グローバル SNMP 設定とアクセス制御リストのポリシーへの適用 (P. 118)
（オプション）ポリシー レベルでのアクセス制御リストの指定 (P. 120)
（オプション）サーバ レベルでの SNMP 設定とアクセス制御リストの指定 (P. 121)
サーバ グループへのポリシーの配布 (P. 122)

グローバル SNMP 設定とアクセス制御リストのポリシーへの適用

適切な ACL を使用してグローバル SNMP 設定を完了したら、ポリシーに SNMP 設定を適用します。

次の手順に従ってください:

1. ユーザ インターフェースで［リソース］-［設定］に移動します。

   ［ポリシー］ページが表示されます。

2. ナビゲーション ペインで［ポリシー］-［ポリシー］-［SystemEDGE］を展開します。

   ［SystemEDGE］ページが表示され、利用可能なポリシーが一覧表示されます。

3. （オプション） をクリックしてポリシーを作成します。

   ［新規 SystemEDGE ポリシー］ダイアログ ボックスが表示されます。

4. ポリシーの作成に必要なデータを指定して、［OK］をクリックします。

5. 1 つ以上の管理対象システムに適用するポリシーを開き、［トラップ & コミュニティ］をクリックします。

   ［コミュニティ］ページが表示され、SNMP 設定のテーブルと以下のオプションが表示されます。

   - ［サーバ コミュニティのみを含める］
   - ［サーバ コミュニティおよびすべてのデフォルト コミュニティを含める］（グローバル コミュニティ）
   - ［カスタム選択］

   注: 設定に含まれているテーブルの唯一のデフォルト（グローバル）SNMP 設定は、エージェント ポートに一致するポートを持つ設定です。

6. 3 つのオプションの 1 つを選択し、それぞれのターゲット システムに指定された適切なポートを持ったコミュニティが少なくとも 1 つあることを確認します。

   最初のオプション［*サーバ コミュニティのみを含める*］を選択する場合は、適切なサーバ レベルの SNMP 設定がターゲット システムに対して存在することを確認してください。選択できる利用可能なサーバ コミュニティは一般的に以下のものです。

   - サーバ読み取り
   - サーバ書き込み

   これらは既存のサーバ レベルの読み取りおよび書き込みの認証情報を表しています。

   2 番目のオプションを選択する場合は、テーブルのすべてのグローバル SNMP 設定とサーバ レベルの設定がターゲット システムに適用されます。

   3 番目のオプションを選択する場合は、テーブルから選択された SNMP 設定だけがターゲット システムに適用されます。このオプションでは、グローバル設定のみを選択できます。

7. ［ポリシーの保存］をクリックします。

必要に応じて、適切なサーバ グループにポリシーを配布したり、ポリシーまたはサーバ レベルで追加の ACL を指定したりできます。

関連項目:

（オプション）ポリシー レベルでのアクセス制御リストの指定 (P. 120)
（オプション）サーバ レベルでの SNMP 設定とアクセス制御リストの指定 (P. 121)
サーバ グループへのポリシーの配布 (P. 122)

（オプション）ポリシー レベルでのアクセス制御リストの指定

オプションのグローバル ACL を使用してグローバル SNMP 設定を指定した後、ポリシー レベルで ACL を定義できます。

次の手順に従ってください:

1. ［ポリシー］ページから、テーブルの 2 番目または 3 番目のオプションを選択して、グローバル SNMP 設定に適用します。
   - ［サーバ コミュニティおよびすべてのデフォルト コミュニティを含める］（グローバル コミュニティ）
   - カスタム選択
2. テーブルからグローバル SNMP 設定オブジェクトを選択して、［*表示*］または［*定義なし*］リンクをクリックします。

   ［ACL］ダイアログ ボックスが開きます。
3. ［*ポリシー固有の SNMP アクセス制御リスト*］フィールドにマネージャ システムの名前または IP アドレスを追加して、［OK］をクリックします。

   このポリシーを適用するサーバ グループのサーバは、これらのマネージャ システムからの SNMP リクエストを許可します。
4. ［ポリシーの保存］をクリックします。

必要に応じて、適切なサーバ グループにポリシーを配布したり、システム レベルで追加の ACL を指定したりできます。

関連項目:

（オプション）サーバ レベルでの SNMP 設定とアクセス制御リストの指定 (P. 121)
サーバ グループへのポリシーの配布 (P. 122)

（オプション）サーバ レベルでの SNMP 設定とアクセス制御リストの指定

例外的なケースでは、特定の管理対象システムに対して SNMP 設定およびアクセス制御リストを指定できます。

次の手順に従ってください:

1. ユーザ インターフェースで［リソース］-［エクスプローラ］に移動します。

   ［エクスプローラ］ペインが表示されます。

2. ［エクスプローラ］ツリーを展開し、SNMP 認証情報およびアクセス制御リストを指定するシステムを右クリックします。

3. ポップアップ メニューから、［ポリシー］-［SNMP の設定］を選択します。

   ［SNMP 設定］ダイアログ ボックスには、そのシステムに対して有効な SNMP 設定が一覧表示されます。

4. ［追加］をクリックします。

   ［新しい SNMP 設定］ダイアログ ボックスが表示されます。

5. 名前、ポート、コミュニティ文字列、操作のタイプ（読み取り専用または読み取り/書き込み）、SNMP のバージョン、タイムアウト、および再試行の限度を指定します。 サーバにインストールされている SystemEDGE のポート番号を使用します。 ［OK］をクリックします。

6. ダイアログ ボックスが閉じて、選択したシステムのページが表示されたら、［モニタリング ソフトウェア］-［SNMP アクセス制御］タブをクリックします。

   指定したシステムに固有の SNMP コミュニティ設定が一覧表示されます。

7. ［アクセス制御リスト］列から［編集］リンクをクリックします。

   システムに固有の［アクセス制御リスト］ダイアログ ボックスが表示されます。

8. ［SNMP アクセス制御リスト］フィールドにマネージャ システムの名前を入力し、［OK］をクリックします。

   管理対象システムは、ACL に一覧表示されたマネージャ システムからの SNMP リクエストを許可します。

9. ［保存］をクリックします。

適切なサーバ グループにポリシーを配布します。

関連項目:

サーバ グループへのポリシーの配布 (P. 122)

サーバ グループへのポリシーの配布

適切な ACL を使用して SNMP 設定を完了したら、ネットワーク内のシステムにポリシーを適用します。

次の手順に従ってください:

1. ユーザ インターフェースで［リソース］-［設定］に移動します。

   ［ポリシー］ページが表示されます。

2. ナビゲーション ペインで［ポリシー］-［ポリシー］-［SystemEDGE］を展開します。

   ［SystemEDGE］ページが表示され、利用可能なポリシーが一覧表示されます。

3. 以前に適切な SNMP 設定を使用して保存したポリシーを選択します。

   ［ポリシー］ページが表示されます。

   注: ［ポリシー設定］を使用して管理対象システムに既存のサーバ レベルの SNMP 設定および ACL を適用しない場合は、［サーバ コミュニティ］ペインの［サーバ読み取り］および［サーバ書き込み］エントリをクリアします。

4. ［アクション］-［適用］をクリックします。

   ［マシンを選択］ページが表示されます。

5. そのポリシーを設定するシステムをすべて選択し、［適用］をクリックします。

   配布ステータスを表示するか、または［ポリシー］ページに戻ることができます。

   新しい設定がターゲット システムに適用されます。

関連項目:

3 つのサーバ グループの例 (P. 123)

3 つのサーバ グループの例

以下の例では、3 つのサーバ グループ、グローバル SNMP 設定、およびグローバルおよびポリシー レベルで指定された ACL で構成される使用例について説明します。

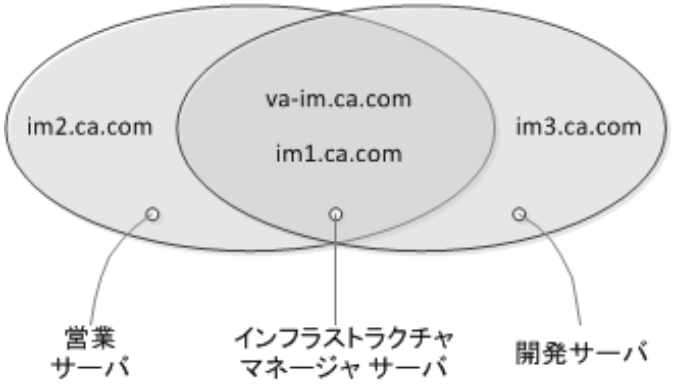
データセンターは以下のサーバ グループで構成されています。

- インフラストラクチャ マネージャ サーバ： CA Server Automation システム、SQL Server システム、CA EEM システム、1 台以上の配布サーバ、3 つのインフラストラクチャ マネージャ システム（im1.ca.com、im2.ca.com、im3.ca.com）。これらのシステムは va-im.ca.com、im1.ca.com によって管理されます。
- 営業サーバ: 営業部門に属し、va-im.ca.com、im1.ca.com、im2.ca.com によって管理されるすべてのサーバ。
- 開発サーバ: 開発部門に属し、va-im.ca.com、im1.ca.com、im3.ca.com によって管理されるすべてのサーバ。

サーバ グループ	グローバル コミュニティ設定	グローバル アクセス制御リスト	ポリシー レベルのアクセス制御リスト
インフラストラクチャ マネージャ サーバ	_public_	va-im.ca.com、im1.ca.com	-
	admin	va-im.ca.com、im1.ca.com	-
営業サーバ	_public_	va-im.ca.com、im1.ca.com	im2.ca.com
	admin	va-im.ca.com、im1.ca.com	im2.ca.com

開発サーバ	_public_	va-im.ca.com、im1.ca.com	im3.ca.com
	admin	va-im.ca.com、im1.ca.com	im3.ca.com

アクセス制御リストの関係



次の手順に従ってください:

1. ［管理］-［SNMP］で以下のグローバル SNMP オブジェクトを指定します。

   infrastructure-read: port 161, read-only access, community _public_, ACL: va-im.ca.com, im1.ca.com

   infrastructure-write: port 161, read-write access, community _admin_, ACL: va-im.ca.com, im1.ca.com

   sales-read: port 161, read-only access, community _public_, ACL: va-im.ca.com, im1.ca.com

   sales-write: port 161, read-write access, community _admin_, ACL: va-im.ca.com, im1.ca.com

   development-read: port 161, read-only access, community _public_, ACL: va-im.ca.com, im1.ca.com

   development-write: port 161, read-write access, community _admin_, ACL: va-im.ca.com, im1.ca.com

2. デフォルト ポリシーに基づいて、infrastructure、sales、および development の 3 つのポリシー（各サーバ グループごとに 1 つずつ）を作成します。
3. infrastructure ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
   - カスタム選択

4. グローバル SNMP オブジェクトの infrastructure-read および infrastructure-write を infrastructure ポリシーに追加します。
5. ポリシーを保存します。
6. sales ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
   - カスタム選択
7. グローバル SNMP オブジェクトの sales-read および sales-write を sales ポリシーに追加します。
8. sales-read および sales-write の［表示］リンクをクリックします。

   対応する［ACL］ダイアログ ボックスが開きます。
9. im2.ca.com を sales-read および sales-write オブジェクトに追加して（ポリシー固有の SNMP アクセス制御リスト）、［OK］をクリックします。
10. ポリシーを保存します。
11. development ポリシーのページに切り替え、テーブルからグローバル SNMP 設定を適用する 3 番目のオプションを選択します。
    - カスタム選択
12. グローバル SNMP オブジェクトの development-read および development-write を development ポリシーに追加します。
13. development-read および development-write の［表示］リンクをクリックします。

    対応する［ACL］ダイアログ ボックスが開きます。
14. im3.ca.com を development-read および development-write オブジェクトに追加して、［OK］をクリックします。
15. ポリシーを保存します。
16. 各ポリシー（infrastructure、sales、development）を、その関連するサーバ グループに適用します。

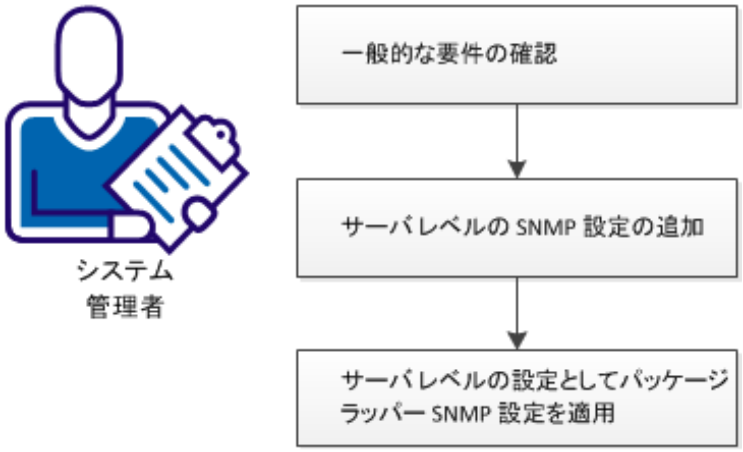
関連項目:

SNMP 設定およびポリシー関係の確認 (P. 115)

サーバ レベルの SNMP 設定を管理する方法

以下の図は、サーバ レベルの SNMP 設定を管理するために必要なアクションの概要を示しています。

サーバ レベルの SNMP 設定を管理する方法



以下の手順に従います。

要件の確認（サーバ レベル） (P. 126)
サーバ レベルの SNMP 設定の追加 (P. 127)
サーバ レベルの設定としてパッケージ ラッパー SNMP 設定を適用する (P. 129)

要件の確認（サーバ レベル）

CA Server Automation のサーバ レベルの SNMP 設定の管理を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、および Windows Server オペレーティング システムに精通している。
- CA SystemEDGE に関する基礎知識がある。
- 「SNMPv1/v2 設定およびアクセス制御リストの設定方法」のシナリオを確認した。
- モニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。

- 管理対象ノードでモニタリング エージェント（CASystemEDGE）にアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- CA Server Automation によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

サーバ レベルの SNMP 設定の追加

CA Server Automation は SNMP リクエストを使用して SystemEDGE からパフォーマンス メトリックを収集します。 個々のサーバの SNMP を設定できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［データ センター］フォルダ、サブフォルダの順に展開し、設定するサーバを選択します。
3. 右クリックし、［ポリシー］を選択します。

   ［ポリシー］サブメニューが表示されます。

4. ［SNMP の設定］をクリックします。

   ［SNMP の設定］ダイアログ ボックスが開き、サーバ レベルの設定が表示されます。

5. 以下のいずれかのオプションを実行します。
   - リストから既存のメトリック用のチェック ボックスをオンにし、ツール アイコン（編集）をクリックして既存のエントリを変更します。
   - ［追加］をクリックして、サーバ レベルで SNMP エントリを作成します。

   ［新しい SNMP 設定］ダイアログ ボックスが表示されます。

6. 以下のフィールドに入力して、［OK］をクリックします。

名前

定義する SNMP 認証情報を説明します。

ポート

これらの認証情報で管理するシステムで SystemEDGE 用に設定するポートを定義します。

SNMP バージョン

使用されている SNMP バージョンを指定します。 SNMP v3 トラップを選択した場合は、追加の設定パラメータ用のパネルが表示されます。

コミュニティ文字列（SNMP v1/v2 用）

SNMP コミュニティ文字列を指定します。

セキュリティ ユーザ（SNMP v3 用）

定義する SNMP 認証情報のための SNMP セキュリティ ユーザを指定します。

アクセス タイプ

アクセス タイプを指定します。 有効なオプションは、「読み取り専用」または「読み書き」です。

タイムアウト

通知配信の確認待機がタイムアウトするまでの時間を秒単位で指定します。

デフォルト： 10 秒

再試行の制限

タイムアウト後に通知の送信を再試行する回数を指定します。

認証（SNMP v3 用）

使用する認証プロトコルを指定します。［タイプ］ドロップダウン リストから［MD5］または［SHA］を選択し、パスワードを指定します。

プライバシー（SNMP v3 用）

使用するプライバシー プロトコルを指定します。［タイプ］ドロップダウン リストから［DES］、［AES］、または［3DES］を選択し、パスワードを指定します。

SNMP 設定が保存され、［サーバの設定］テーブルに表示されます。

サーバ レベルの設定としてパッケージ ラッパー SNMP 設定を適用する

SystemEDGE でポリシー設定を登録した後、サーバ レベルの SNMP 設定としてパッケージ ラッパー SNMP 設定を使用するように CA Server Automation に指定することができます。 これを行わないと、パッケージ ラッパー SNMP 設定は SystemEDGE がポリシー設定を登録するまでの間しか使用されません。

次の手順に従ってください:

1. ［管理］-［設定］-［展開 & 設定］に移動します。

   以下のオプションは、パッケージ ラッパーの SNMP 設定がサーバ レベルの SNMP 設定になるかどうかを制御します。

   - SystemEDGE エージェントが登録されるときにサーバ固有の SNMP 設定を作成します。

2. 要件に応じて、このオプションを有効または無効にします。

   このオプションを無効にすると、パッケージ ラッパー SNMP 設定はマネージャに保存されず、配布には使用できません。

   このオプションを有効にすると、パッケージ ラッパー SNMP 設定はサーバ レベルの SNMP 設定として CA Server Automation マネージャに保存されます。

3. ［リソース］-［設定］に移動して、管理対象ノードに適用する SystemEDGE ポリシーを開きます。

   ［ポリシー］ペインが表示されます。

4. ［トラップ & コミュニティ］-［サーバ コミュニティ］で適切なアイテムを選択します。

   ［サーバ読み取り］および［サーバ書き込み］は、このポリシーを適用する管理対象ノードに使用できるサーバ レベルの SNMP 設定を表します。

5. ［デフォルト コミュニティ］から適切な項目を選択します。

   ［デフォルト コミュニティ］はグローバル SNMP 設定を表します。

6. ［リソース］-［展開］-［パッケージ］に移動して、SystemEDGE パッケージ ラッパーを開きます。

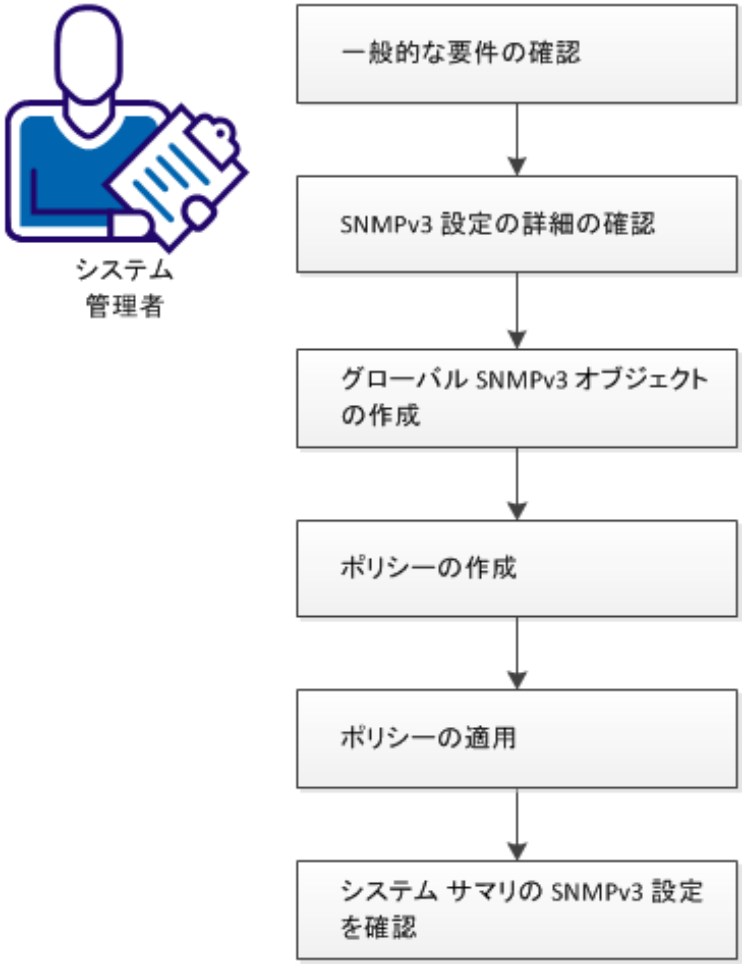
7. SNMP 認証情報を設定し、管理対象ノードへのインストール後に SystemEDGE エージェントに適用するポリシーを選択し、ラッパーを保存します。

8. ［展開ジョブ］を作成し、管理対象ノードにそのポリシーで SystemEDGE パッケージを展開します。

SNMPv3 の設定方法

以下の図は、使用する環境に SNMPv3 を設定するために必要なアクションの概要を示しています。 このユース ケースでは、CA Server Automation の SNMPv3 設定について説明します。

SNMPv3 の設定方法



以下の手順に従います。

一般的な要件の確認（SNMPv3）

CA Server Automation の SNMP の設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、および Windows Server オペレーティング システムに精通している。
- CA SystemEDGE に関する基礎知識がある。
- 「SNMPv1/v2 設定およびアクセス制御リストの設定方法」のシナリオを確認した。
- 「サーバ レベルの SNMP 設定を管理する方法」のシナリオを確認した。
- モニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- 管理対象ノードでモニタリング エージェント（CASystemEDGE）にアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- CA Server Automation によって関連するシステムがすべて検出されている。
- 設定するすべてのシステムで SystemEDGE が管理対象モードで実行されている。

SNMPv3 設定の詳細の確認

使用環境での CA Server Automation マネージャと管理対象ノードとの間の通信に SNMPv3 を使用することを検討している場合は、以下の詳細事項を考慮してください。

- SystemEDGE は、インストールのために少なくとも 1 つの SNMPv1 コミュニティを必要とする。CA Server Automation がサーバを検出した後、CA Server Automation はこれらの SNMPv1 設定をサーバ固有の SNMP 設定として扱う。
- 使用するインフラストラクチャ マネージャが SNMPv3 をサポートしていることを確認する。
- グローバル SNMPv3 認証情報を作成する。
- リモート サーバに SNMPv3 設定を適用するためのポリシーを作成する。
- 純粋な SNMPv3 設定が必要な場合は、ポリシー設定でサーバ固有の SNMPv1 設定を適用しないようにする。

グローバル SNMPv3 オブジェクトの作成

特定のサーバに有効なグローバル SNMP 設定またはサーバ固有の SNMP 設定を作成できます。グローバル設定は、ポリシーによってサーバ グループに適用できます。

次の手順に従ってください:

1. ユーザ インターフェースで［管理］-［SNMP］に移動します。

   グローバル オブジェクト用の［SNMP 設定］ページが表示されます。

2. SNMP 設定オブジェクトを作成するには、［アクション］-［新規］をクリックします。

   ［新しい SNMP 設定］ダイアログ ボックスが表示されます。

3. ［SNMP バージョン］を［SNMPv3］に設定します。

   SNMPv3 に関連するフィールドがダイアログ ボックスに表示されます。

4. 以下のフィールドに入力して、［OK］をクリックします。

   名前

   定義する SNMP 認証情報の名前を指定します。

   ポート

   これらの認証情報で管理するシステムで SystemEDGE 用に設定するポートを定義します。

   SNMP バージョン

   SNMPv3 を指定します（前の手順で設定済み）。

   セキュリティ ユーザ

   定義する SNMP 認証情報のための SNMP セキュリティ ユーザを指定します。

   アクセス タイプ

   アクセス タイプを指定します。 有効なオプションは、「読み取り専用」または「読み書き」です。

   タイムアウト

   通知配信の確認待機がタイムアウトするまでの時間を秒単位で指定します。

   デフォルト： 10 秒

   再試行の制限

タイムアウト後に通知の送信を再試行する回数を指定します。

認証

使用する認証プロトコルを指定します。［タイプ］ドロップダウン リストから［MD5］または［SHA］を選択し、パスワードを指定します。

プライバシー

使用するプライバシー プロトコルを指定します。［タイプ］ドロップダウン リストから［DES］、［AES］、または［3DES］を選択し、パスワードを指定します。

SNMP 設定が保存され、［サーバの設定］テーブルに表示されます。

ポリシーの作成

グローバル SNMPv3 設定が完了したら、ポリシーに SNMPv3 設定を適用します。

次の手順に従ってください:

1. ユーザ インターフェースで［リソース］-［設定］に移動します。

   ［ポリシー］ページが表示されます。

2. ナビゲーション ペインで［ポリシー］-［ポリシー］-［SystemEDGE］を展開します。

   ［SystemEDGE］ページが表示され、利用可能なポリシーが一覧表示されます。

3. をクリックしてポリシーを作成します。

   ［新規 SystemEDGE ポリシー］ダイアログ ボックスが表示されます。

4. ポリシーの作成に必要なデータを指定して、［OK］をクリックします。

5. 1 つ以上の管理対象システムに適用するポリシーを開き、［トラップ & コミュニティ］をクリックします。

   ［コミュニティ］ページが表示され、SNMP 設定のテーブルと以下のオプションが表示されます。

   - サーバ コミュニティのみを含める
   - サーバ コミュニティおよびすべてのデフォルト コミュニティを含める
   - カスタム選択

注: 設定に含まれているテーブルの唯一のデフォルト（グローバル）SNMP 設定は、エージェント ポートに一致するポートを持つ設定です。

6. ［カスタム選択］を選択します。

   このオプションでは、グローバル SNMPv3 オブジェクトのみを選択し、サーバ固有の SNMP 設定をすべてクリアします。

7. ターゲット システムごとに指定された適切なポートを持つ SNMPv3 設定オブジェクトを少なくとも 1 つ選択し、［ポリシーの保存］をクリックします。

   選択した SNMPv3 オブジェクトは、ポリシーと関連付けられます。

8. ［トラップ先］タブをクリックします。

   ［トラップ先］ページが表示されます。［SNMPv3 トラップ デスティネーション］を設定できます。

9. ［トラップ タイプ］フィールドから、［SNMPv3 トラップ情報］または［SNMPv3 通知情報］（INFORM 要求および確認済みトラップとも呼ばれる）を選択します。

   選択内容に応じて、以下のフィールドが表示されます。

   デスティネーション

   トラップの送信先となるホストを指定します。 ホスト名または IP アドレスを指定できます。

   ポート

   トラップの送信先となるデスティネーション ホスト上のポート番号を指定します。

   ユーザ名

   トラップの送信時に使用する SNMPv3 ユーザを指定します。

   エンコーディング

   トラップの送信時に使用するエンコーディングのタイプを指定します。

   デフォルト： 000

   このエンコーディングは SNMPv1 のトラップ エンコーディングの設定と同様です。「*SystemEDGE ユーザ ガイド*」、「SNMPv1 トラップ デスティネーションの設定」も参照してください。

コンテキスト

このフィールドの値としては、*（アスタリスク）のみがサポートされています。 この値は必須です。

タイムアウト

（通知のみ）通知の配信確認処理がタイムアウトするまでの待機時間を秒単位で指定します。

再試行回数

（通知のみ）タイムアウト後に通知の送信を再試行する回数を指定します。

10. これらのフィールドに入力し、［追加］をクリックします。

    新しいエントリが［トラップ先］テーブルに表示されます。

    最後の手順を繰り返すと、テーブルにさらにエントリを追加できます。

11. ［トラップ先］のいずれかを選択し、［ポリシーの保存］をクリックします。

    ポリシーが適切なトラップ先に保存されます。

適切なサーバ グループにポリシーを配布できます。

ポリシーの適用

SNMPv3 設定が完了したら、ネットワーク内のシステムにポリシーを適用できます。

次の手順に従ってください:

1. ユーザ インターフェースで［リソース］-［設定］に移動します。

   ［ポリシー］ページが表示されます。

2. ナビゲーション ペインで［ポリシー］-［ポリシー］-［SystemEDGE］を展開します。

   ［SystemEDGE］ページが表示され、利用可能なポリシーが一覧表示されます。

3. 以前に適切な SNMPv3 設定を使用して保存したポリシーを選択します。

   ［ポリシー］ページが表示されます。

4. ［アクション］-［適用］をクリックします。

   ［マシンを選択］ページが表示されます。

5. そのポリシーを設定するシステムをすべて選択し、［適用］をクリックします。

   配布ステータスを表示するか、または［ポリシー］ページに戻ることができます。

   新しい設定がターゲット システムに適用されます。

代替方法

リモート システムに SystemEDGE を展開し、SNMPv3 認証情報を使用する場合は、パッケージ ラッパーにポリシーを適用し、展開ジョブを実行できます。

システム サマリの SNMPv3 設定を確認します。

SNMPv3 設定がターゲット システムに正しく適用されたことを確認するには、CA Server Automation ユーザ インターフェースの［エクスプローラ］ペインに切り替えます。

次の手順に従ってください:

1. ［エクスプローラ］ペインのコンポーネント ツリーを展開します。
2. SNMPv3 設定を適用した管理対象システムを選択し、［サマリ］を開きます。

   ［マシン ステータス情報］が表示されます。
3. ［アクティブな SNMP 認証情報］フィールドに、SNMPv3 グローバル オブジェクトが表示されていることを確認します。

注: 管理対象サーバに純粋な SNMPv3 設定を適用しており、そのサーバで SystemEDGE のコントロール パネル（Windows のみ）を開いた場合は、コミュニティとトラップのフィールドは空です。 SystemEDGE のコントロール パネルには、これらのフィールドの SNMPv1 情報が表示されます。

SystemEDGE および AIM の展開方法

このセクションでは、モニタリング ソフトウェアを正しく展開するためのジョブを設定および管理する方法について説明します。

関連項目:

概要

CA Server Automation は、SystemEDGE および他のエージェントをすべての管理対象システムにリモートで展開するための包括的なソリューションを提供します。 カスタマイズされたインストール パラメータを含む付属パッケージに基づいて展開テンプレートを作成すると同時に、そのようなテンプレートを多数の管理対象システムに展開できます。 この自動展開ソリューションによって、1 つの場所から、企業全体にわたってエージェントを展開して設定することが可能となります。

リモート展開には、以下の機能があります。

展開設定

ターゲット システムへのソフトウェア パッケージの展開方法を定義する設定を作成、編集、および削除できます。これらの設定は、「パッケージ ラッパー」と呼ばれます。

展開ジョブ管理

展開ジョブの作成、開始、取り消し、およびフィルタリングが可能になり、複数の配布サーバを使用して複数のターゲットにパッケージを同時に展開できます。

展開ジョブ レポート

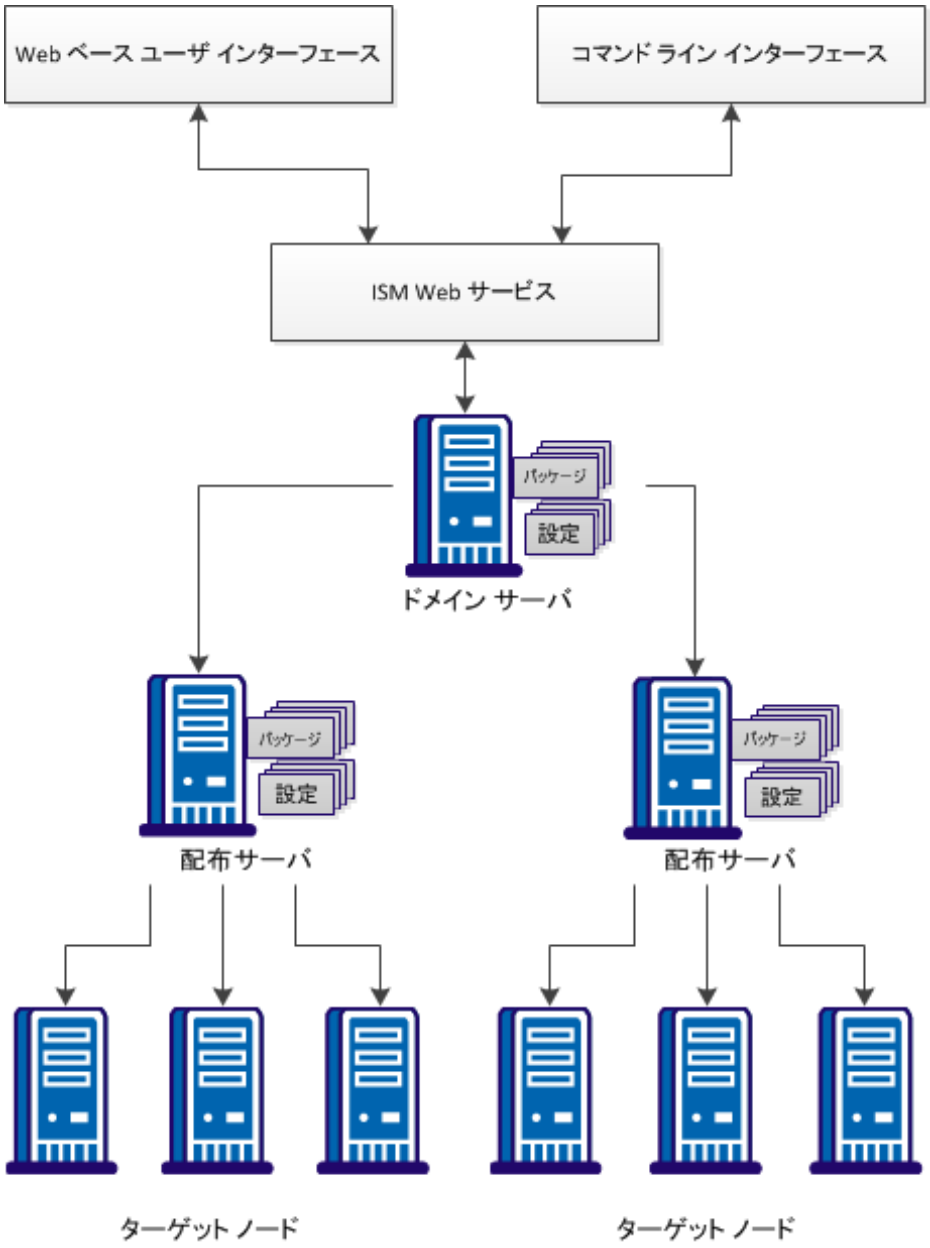
展開ジョブのステータスをクエリすることができます。

展開イベント

管理対象ノードの状態を追跡する展開関連イベントのソースを提供します。

リモート展開アーキテクチャ

展開ソリューションの全体的アーキテクチャは、ドメイン サーバおよび配布サーバ コンポーネントによって推進されます。 以下の図は、展開関連コンポーネントの概要を表しています。



パッケージについて

展開パッケージは、企業全体にわたるシステムにモニタリング ソフトウェアを展開するために必要なマテリアルを提供します。 展開パッケージは、プラットフォームに固有なパッケージ ラッパーに分かれています。パッケージ ラッパーは、エージェント ソフトウェアをインストールするのに必要なインストール パラメータをカプセル化します。また、展開をサポートするすべてのプラットフォームで使用できます。

注: デフォルトのパッケージ ラッパー名がローカライズされておらず、サポートされたすべての言語で「default」と表示されます。 カスタムのパッケージ ラッパー名はローカライズされています。

展開コンポーネント

このセクションでは、展開の主要コンポーネントのリストを示し、簡単に説明します。

ドメイン サーバ

ドメイン サーバは、すべての設定および制御データのリポジトリです。サーバは、展開操作に必要な設定およびソフトウェア パッケージ データの管理を担当し、すべての設定操作を管理しています。 詳細なイベント データが、展開プロセス中にドメインおよび配布サーバ間で渡されます。 単一のドメイン サーバにより、すべての配布サーバ ジョブのステータスが維持されます。

配布サーバ

配布サーバは、同じマシンに置かれている Infrastructure Deployment Manager （IDManager）サーバを制御します。 アーキテクチャでは、複数の配布サーバによって提供される展開サービスが考慮されています。

インフラストラクチャ展開

インフラストラクチャ展開によって展開ジョブが開始され、管理されます。 展開プロセス中に、Infrastructure Deployment Manager （IDManager）がリモート システムへのアクセスを提供し、Infrastructure Deployment Primer （IDPrimer）が、エージェント ソフトウェア パッケージをリモートでインストールするメカニズムを提供します。IDPrimer は、ターゲット コンピュータに展開パッケージ データを転送して、インストールを実行するために使用されます。 それ以降の同じターゲット コンピュータへの展開では常に、すでにインストールされた IDPrimer を使用できます。 IDManager は、すべての展開操作を制御し、ジョブ ステータスを処理します。

設定

このセクションでは、リモート展開のユーザ インターフェース設定と配布サーバの接続に関する詳細について説明します。

関連項目:

展開ダッシュボード ビュー (P. 143)
リモート展開の検索機能の強化 (P. 144)
ジョブステータス フィルタ (P. 145)
配布サーバが接続するドメイン サーバの変更 (P. 145)

展開ダッシュボード ビュー

ダッシュボードには、展開メトリックを追跡するための以下のビューがあります。

展開タスク サマリ

完了、アクティブ、保留中、および失敗の展開タスクの数を示す円グラフとリストを表示します。

未解決展開タスク

正常に完了しなかった展開のリストを表示します。ジョブ ID をクリックすると、タスクが未解決である理由に関する詳細を表示できます。

アクティブな展開タスク

現在アクティブな展開タスクのリストを表示します。 詳細には、関連付けられた展開ジョブ、ターゲット、パッケージ、および現在の状態が含まれます。タスク ID をクリックすると、現在のステータスの詳細を表示できます。

展開パッケージ サマリ

各展開パッケージ タイプの展開の数を示す棒グラフを表示します。

完了した展開ジョブ

正常に完了した展開のリストを表示します。ジョブ ID をクリックすると、ジョブに関する詳細を表示できます。

リモート展開の検索機能の強化

検索機能が強化されたことにより、リモート展開に関連するキーワードで検索を実行し、この結果からリモート展開操作に迅速にアクセスできるようになりました。 この機能の利点は以下のとおりです。

この機能の利点は以下のとおりです。

- リモート展開コンポーネントに迅速にアクセスできる。
- サーバとサービスにリモート展開ソフトウェア パッケージを展開できる。
- リモート展開ソフトウェア パッケージおよびテンプレートを管理できる。
- 展開ジョブを迅速に作成および管理し、利用可能なパッケージおよびラッパーにアクセスできる。

次の手順に従ってください:

1. ［値］フィールドにキーワード（またはワイルドカードを使用した部分的な値）を入力して、［検索］をクリックします。

   例:

   「展開」、「リモート」、または「リモート展開」などを指定します。

   ［リモート展開］リンクのリストが表示されます。

2. 適切なリモート展開操作を選択します。

   リモート展開操作を実行します。

ジョブステータス フィルタ

ジョブ ステータス データは各ジョブに関連する詳細のみを表示するためにフィルタされます。列を並べ替えてカスタマイズすることや、1 つ以上の列によってフィルタすることができます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］フォルダが表示されます。

2. ［ジョブ］をクリックします。

   右側のペインにジョブの詳細が表示されます。

3. （オプション）［ジョブ ステータス］列のチェック ボックスを選択/選択解除します。

   カスタマイズされた列が表示されます。

4. 列のフィルタを選択/選択解除します。

   フィルタの選択に基づいてジョブが表示されます。

配布サーバが接続するドメイン サーバの変更

ドメイン サーバ マシンのネットワーク アドレスが元のインストールの後に変更される場合は、新しいネットワーク アドレスに接続するように配布サーバを再設定する必要があります。

以下に示すように設定を変更する前に、新しいネットワーク アドレスが配布サーバから接続可能であることを確認することが重要です。 配布サーバが新しいアドレスでドメイン サーバに接続できない場合は、展開機能が正しく動作しません。

配布サーバが接続するドメイン サーバを変更する方法

1. ［スタート］メニューから、［管理ツール］-［サービス］を開きます。

   ［サービス］ユーザ インターフェースが表示され、インストールされたサービスのリストが表示されます。

2. ［CA SM Distribution Server］を右クリックし、［プロパティ］を選択します。

   ［プロパティ］ダイアログ ボックスが表示されます。

3. ［停止］をクリックして、サービスを停止します。
4. ［開始パラメータ］フィールドに、以下のパラメータを入力します。

   -m *domainserver*

   domainserver パラメータで、ドメイン サーバの IP アドレスまたは DNS 名を指定します。
5. ［開始］をクリックします。

   これで、配布サーバは、入力したドメイン サーバのアドレスに接続しようとします。

スケーラビリティ

展開システムは、複数の配布サーバをスケーラビリティ レイヤとして使用して、ある程度のスケーラビリティを提供します。 各配布サーバは、1 つの IDManager インスタンスと通信します。 IDManager は、複数のターゲット コンピュータへの複数のコンポーネント展開を管理できます。 CA Server Automation では、この連合モデルにより、多くの同時展開がサポートされます。

展開のサイジング キー ファクタ

インフラストラクチャのサイジングやシステム パフォーマンスには、以下のような、大きな影響を与える数多くのキー ファクタがあります。

- 配信するソフトウェア パッケージのサイズ。
- 配信するソフトウェア パッケージの数。
- ソフトウェア パッケージ配信の頻度。
- 展開コンポーネントとターゲット コンピュータの間のネットワーク遅延。
- ネットワーク帯域幅の管理。

注: ターゲットへの初期展開では、小規模のインストール エージェントである IDPrimer がインストールされます。 一度 IDPrimer がインストールされると、同じターゲットへの以降の展開にかかる時間が短縮されます。

展開の推奨事項：

- ターゲット サーバが通常は、ソフトウェアのリモート展開の要件を満たしていることを確認します。
- 追加の配布サーバは、ターゲットのローカルの場所にインストールします。
- 可能な場合は、ターゲットのローカルな配布サーバを使用して展開します。
- 可能な場合は、ネットワーク トラフィックが低い期間に展開を開始するようにスケジュールします。

注: CA Server Automation スケーラビリティの詳細については、「スケーラビリティのベスト プラクティス」を参照してください。

関連項目:

スケーラビリティのベスト プラクティス (P. 1195)

複数の配布サーバ

リモート展開ソリューションでは、すべての展開で単一の中央サーバ（マネージャ）を使用できますが、以下の要件のいずれかを満たす場合は、中央のドメイン サーバを指すリモート配布サーバをインストールすることを推奨します。

- 2 か所以上の地理的に離れた場所にエージェント ソフトウェアを展開する必要があるが、それらを単一のマネージャで一元管理する必要がある。

  この場合は、それぞれの場所に、中央のドメイン サーバに接続された配布サーバを少なくとも 1 つ配置することを推奨します。
- 場所は 1 つであるが、展開する必要のあるマシンが数百台ある。

  この場合は、複数のサブネットにわたって論理的に分離された多数の配布サーバをインストールできます。これらの配布サーバは、中央のドメイン サーバに接続されています。

展開パッケージ

展開パッケージは、企業全体にわたってモニタリング用ソフトウェアをシステムに展開するために必要な要素を提供します。 展開パッケージは、プラットフォーム固有のバージョンに分解でき、展開をサポートするすべてのプラットフォームでパッケージ ラッパーが利用可能です。

重要: AIM は SystemEDGE および Advanced Encryption パッケージに依存します。 これらのパッケージのいずれかを展開するには、SystemEDGE と Advanced Encryption がシステムにすでに存在するか、または展開ジョブに含まれている必要があります。

以下の展開パッケージが利用可能です。

CCA Agent

CCA エージェントを提供します。

Performance Agent（CA Systems Performance LiteAgent）

Windows、UNIX、または Linux のパフォーマンス メトリックをモニタおよび収集するための軽量なモニタリング エージェントを提供します。

SystemEDGE

コア SystemEDGE エージェントを提供します。

SystemEDGE ADES

Active Directory および Exchange Server 用の AIM を提供します。

SystemEDGE Advanced Encryption

SystemEDGE の FIPS 140 準拠暗号化パッケージを提供します。

SystemEDGE AIX LPAR

IBM PowerVM （LPAR）用の AIM を提供します。

SystemEDGE CXEN

Citrix XenServer 用の AIM を提供します。

SystemEDGE Citrix XenDesktop

Citrix XenDesktop 用の AIM を提供します。

SystemEDGE GalaX

Huawei GalaX8800 用の AIM を提供します。

SystemEDGE Hyper-V

Microsoft Hyper-V 用の AIM を提供します。

SystemEDGE IBM PowerHA

IBM PowerHA （旧名称「Availability Cluster Multi-Processing」）用の AIM を提供します。

SystemEDGE KVM

KVM テクノロジに基づき、RHEV （Red Hat Enterprise Virtualization）用の AIM を提供します。

SystemEDGE MSCS

Microsoft クラスタ サポート（MSCS）用の AIM を提供します。

SystemEDGE RM

リモート モニタリング AIM を提供します。

SystemEDGE Solaris Zone

Oracle Solaris ゾーン用の AIM を提供します。

SystemEDGE SRM

サービス レスポンス モニタ AIM を提供します。

SystemEDGE UCS

Cisco UCS 用の AIM を提供します。

SystemEDGE VC

VMware vCenter 用の AIM を提供します。

SystemEDGE VCLOUD

VMware vCloud Director 用の AIM を提供します。

デフォルト パッケージ ラッパー

デフォルトのパッケージ ラッパーが提供されており、リモート展開を使用して展開できるソフトウェア パッケージにすぐに使用できます。 これらのパッケージ ラッパーには、選択したソフトウェア パッケージ用に一連のデフォルト値が設定されたインストーラ パラメータが含まれます。パッケージが必須パラメータを必要とする場合は、これらのパラメータを指定し、パッケージを展開する前に設定を保存します。

パッケージのインストーラ パラメータ値を変更する必要がある場合を除き、パラメータを再度編集する必要はありません。 必須パラメータを指定せずにパッケージを展開しようとすると、展開プロセスは停止されます。このようなパッケージ ラッパーは展開可能な状態ではありません。

利用可能なパッケージ ラッパーには、以下のパラメータが含まれます。必須パラメータは、ユーザ インターフェースで以下のように示されます。

SystemEDGE

［管理］-［設定］-［SNMP］で指定されたグローバル SNMP 設定によって、SystemEDGE パッケージ ラッパーの以下のフィールドのドロップダウン リストが入力されます。

- ポート
- 読み取りコミュニティ
- 読み取り/書き込みコミュニティ

あるいは、フィールドをインラインで編集できます。

利用可能なコミュニティ文字列はポート設定によって異なります。ポート番号を初めて選択するときには、そのポート用のドロップダウン リストに有効なコミュニティ文字列が自動的に取得されます。

インストール パス

パッケージ用のルート インストール ディレクトリを定義します。

データ パス

パッケージ用のデータ ディレクトリを定義します。

共有パス

CA 共有コンポーネントに使用するルート インストール ディレクトリを定義します。

ポート

SystemEDGE ポート番号を定義します。

デフォルト： 161

説明

SNMP システムの説明を定義します。

Location

SNMP システムの場所を定義します。

連絡先

SNMP システムの連絡先を定義します。

読み取りコミュニティ

SNMP 読み取り専用コミュニティ文字列を定義します。

デフォルト： public

読み取り/書き込みコミュニティ

SNMP 読み取り/書き込みコミュニティ文字列を定義します。

トラップ コミュニティ

SNMP トラップ コミュニティ文字列を定義します。

トラップ先

SNMP トラップ先のホスト名を定義します。

トラップ ポート

SNMP トラップ ポートを定義します。

デフォルト： 162

権限分離ユーザ（UNIX/Linux）

SNMP 通信中にエージェントが使用して実行する認証情報のユーザ名を指定します。

このエントリは、別のユーザ アカウントで SNMP 通信を実行するようにエージェントに指示します。 また、このエージェントは、このユーザのデフォルト グループを有効なグループとして使用します。

デフォルト： エージェントは root アカウントを使用して動作します。

[エージェントの起動]チェック ボックス

インストールの最後に SystemEDGE を自動的に開始するかどうかを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

注: ［再起動の抑制］ チェック ボックスは Windows パッケージでのみ利用可能です。

[ネイティブ エージェントの無効化]チェック ボックス

ネイティブ SNMP エージェントを置換するかどうかを指定します。

[ネイティブ設定を使用]チェック ボックス

ネイティブ SNMP エージェント設定を使用するかどうかを指定します（ネイティブ SNMP エージェントを置換する場合）。

[管理対象モードでの実行]チェック ボックス

管理対象モードで SystemEDGE を実行するかどうかを指定します。

[管理対象ポリシー名]ドロップダウン リスト

利用可能な SystemEDGE ポリシーのリストを指定します。

注: バージョン 4.3 またはバージョン 4.2 パッチ レベル 3 から SystemEDGE をアップグレードする場合、インストーラは以下のパラメータのみを使用します。

CASE_PUBDATADIR
CASE_MANAGER_HOSTNAME
CASE_MANAGER_POLICY_NAME
CASE_START_AFTER_INSTALL
CASE_LEGACY_MODE
CASE_SNMP_PORT
CASE_INSTALL_DOCS
CASE_SNMP_TRAP_COMMUNITY (1)
CASE_SNMP_TRAP_DESTINATION (1)
CASE_SNMP_TRAP_PORT (1)
CASE_SNMP_READ_COMMUNITY (1)
CASE_SNMP_WRITE_COMMUNITY (1)
CASE_SNMP_READ_ALLOWED_MANAGERS (1)
CASE_SNMP_WRITE_ALLOWED_MANAGERS (1)

その他のパラメータは無視されます。

(1) これらのパラメータは特別です。 これらの設定は、既存の SystemEDGE 4.x 設定に追加され、これによって、SystemEDGE 4.x マネージャと SystemEDGE 5.x マネージャの両方が機能するようになります。

注: パラメータの詳細については、「*SystemEDGE ユーザ ガイド*」の「*インストールおよび展開*」の章を参照してください。

CA SystemEDGE ADES

Windows ドメイン

モニタする Windows ドメインを指定します。

ドメイン ユーザ

ドメイン サーバまたは Exchange Server に接続するためのドメイン管理者ユーザを指定します。

ドメイン ユーザ パスワード

ドメイン サーバまたは Exchange Server に接続するためのドメイン管理者ユーザのパスワードを指定します。

管理エンティティ

管理対象エンティティを指定します。

0

Active Directory をモニタリングの対象にします。

1

Exchange Server をモニタリングの対象にします。

2

Active Directory および Exchange Server の両方をモニタリングの対象にします。

管理モード

管理のオプションを指定します。

0

ドメイン全体をモニタリングの対象にします。

1

ドメインの特定のホストをモニタリングに対象にします。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

SystemEDGE Advanced Encryption

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE AIX LPAR

LPAR ホスト

IBM LPAR サーバへの接続に使用するホスト名を指定します。 このパッケージを展開するための IBM LPAR のホスト名を指定します。

ユーザ名

IBM LPAR サーバへの接続に使用するユーザ名を指定します。 このパッケージを展開するための IBM LPAR のユーザ名を指定します。

パスワード

IBM LPAR サーバへの接続に使用するパスワードを指定します。 このパッケージを展開するための IBM LPAR パスワードを指定します。

CA SystemEDGE CXEN

CXEN ホスト名

Citrix XenServer の統合に使用するホスト名を指定します。

CXEN ユーザ名

Citrix XenServer の統合に使用するユーザ名を指定します。

CXEN パスワード

Citrix XenServer の統合に使用するパスワードを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE CXenDesktop

ホスト名

Citrix XenDesktop 統合に使用するホスト名を指定します。

ユーザ名

Citrix XenDesktop 統合に使用するユーザ名を指定します。

パスワード

Citrix XenDesktop 統合に使用するパスワードを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE GalaX

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE PowerHA

ホスト名

IBM PowerHA への接続に使用するホスト名を指定します。 このパッケージを展開するための PowerHA ホスト名を指定します。

ユーザ名

IBM PowerHA への接続に使用するユーザ名を指定します。 このパッケージを展開するための PowerHA ユーザ名を指定します。

パスワード

IBM PowerHA への接続に使用するパスワードを指定します。 このパッケージを展開するための PowerHA パスワードを指定します。

ポート

PowerHA ポート番号を定義します。

デフォルト： 22

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE Hyper-V

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE KVM（RHEV）

KVM Hostname

RHEV（Red Hat Enterprise Virtualization）に接続するためのホスト名を指定します。

KVM Username

RHEV に接続するためのユーザ名を指定します。

KVM Password

RHEV に接続するためのパスワードを指定します。

KVM Port

RHEV に接続するためのポートを指定します。

デフォルト： 8443

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE MSCS

MSCS ホスト名

クラスタに接続するためのホスト名を指定します。

MSCS ユーザ名

クラスタに接続するためのユーザ名を指定します。

MSCS パスワード

クラスタに接続するためのパスワードを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE RM

デフォルト WMI ユーザ名

リモート マシンへの接続に使用するデフォルト ユーザ名を定義します。このパッケージを展開するためのユーザ名を指定します。

デフォルト WMI パスワード

リモート マシンへの接続に使用するデフォルト パスワードを定義します。 このパッケージを展開するためのパスワードを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE SRM

[スクリプトを許可]チェック ボックス

テストとしてのスクリプトの実行を許可するかどうかを指定します。

[ファイル I/O テストを許可]チェック ボックス

テストとしてのファイル I/O の実行を許可するかどうかを指定します。

[信頼できない SSL の許可]チェック ボックス

未検証の証明書による SSL サイトへのアクセスを許可するかどうかを指定します。

[ユーザ TOS の無効化]チェック ボックス(Windows)

アプリケーションが送信 IP パケットでサービス ビットのタイプを設定しないようにするかどうかを指定します。

[再起動の抑制]チェック ボックス(Windows)

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE Solaris ゾーン

ゾーン ホスト

Solaris ゾーン サーバへの接続に使用するホスト名を指定します。このパッケージを展開するための Solaris ゾーン ホスト名を指定します。

ユーザ名

Solaris ゾーン サーバへの接続に使用するユーザ名を指定します。このパッケージを展開するための Solaris ゾーン ユーザ名を指定します。

パスワード

Solaris ゾーン サーバへの接続に使用するパスワードを指定します。このパッケージを展開するための Solaris ゾーン パスワードを指定します。

CA SystemEDGE UCS

UCS ホスト名

UCS への接続に使用するホスト名を指定します。 このパッケージを展開するための UCS ホスト名を指定します。

UCS ユーザ名

UCS への接続に使用するユーザ名を指定します。 このパッケージを展開するための UCS ユーザ名を指定します。

UCS パスワード

UCS への接続に使用するパスワードを指定します。 このパッケージを展開するための UCS パスワードを指定します。

UCS プロトコル

HTTP と HTTPS のどちらのプロトコルを使用するかを指定します。

ポート

UCS ポート番号を定義します。

デフォルト： HTTP 用の 80 または HTTPS 用の 443。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE VC

ホスト名

vCenter への接続に使用するホスト名を指定します。このパッケージを展開するための vCenter ホスト名を指定します。

ユーザ名

vCenter への接続に使用するユーザ名を指定します。このパッケージを展開するための vCenter ユーザ名を指定します。

パスワード

vCenter への接続に使用するパスワードを指定します。 このパッケージを展開するための vCenter パスワードを指定します。

ポート

vCenter ポート番号を定義します。

デフォルト： 443

プロトコル

HTTP と HTTPS のどちらのプロトコルを使用するかを指定します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA SystemEDGE VCLOUD

VCLOUD ホスト名

vCloud への接続に使用するホスト名を指定します。

VCLOUD username

vCloud への接続に使用するユーザ名を指定します。

VCLOUD パスワード

vCloud への接続に使用するパスワードを指定します。

VCLOUD ポート

vCloud のポート番号を定義します。

デフォルト： 443

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

CA Systems Performance LiteAgent

共有パス

CA 共有コンポーネントに使用するルート インストール ディレクトリを定義します。

インストール パス

パッケージ用のルート インストール ディレクトリを定義します。

[再起動の抑制]チェック ボックス

インストールの終わりで自動的な再起動を抑制するかどうかを指定します。

関連項目

新規パッケージ ラッパーの作成 (P. 167)
パッケージ ラッパーの変更 (P. 168)

展開パッケージ ライブラリ

パッケージ ライブラリには、インストール可能なソフトウェア パッケージの設定可能なセットが含まれており、これを使用して、展開に使用できる製品、バージョン、およびプラットフォームを制御できます。 設定されたソフトウェア パッケージの無人インストールに必要なパラメータを定義する標準パッケージ設定を作成すると、これらの製品のインストール方法を制御できます。

各パッケージには、関連付けられたパッケージ設定ファイルが必要です。設定ファイルは、パッケージの詳細とパッケージ インストールの設定方法を説明する情報の両方を提供します。詳細については、「展開パッケージ設定ファイル」セクションを参照してください。

パッケージ ライブラリは、以下のディレクトリにあります。

%AllUsersProfile%¥CA¥SM¥domainserver¥Deployment¥Packages¥SM

ディレクトリ ツリーのレイアウトは、IDManager コンポーネントの要件によって定義されます。パッケージ ライブラリ自体は、2 つのサブディレクトリ、Public および Private が含まれるトップレベルのパッケージ ディレクトリから構成されます。 Public ディレクトリには、展開可能なすべてのソフトウェア パッケージが含まれます。

```
..
└──────SM
    ├──────CA_LiteAgent
    ├──────CA_ProcProbe_Utility
    ├──────CA_SystemEDGE_AdvancedEncryption
    ├──────CA_SystemEDGE_Core
    │    └──────5.8.0
    │        └──────ENU
    │            ├──────AIX_aix
    │            ├──────HPUX_hp
    │            ├──────HPUX_ia64
    │            ├──────Linux_ia64
    │            ├──────Linux_ppc
    │            ├──────Linux_x86
    │            ├──────Solaris_sparc
    │            ├──────Solaris_x86
    │            ├──────Windows_ia64
    │            ├──────Windows_x64
    │            └──────Windows_x86
    ├──────CA_SystemEDGE_CXEN
    ├──────CA_SystemEDGE_CXENDESKTOP
    ├──────CA_SystemEDGE_ESAD
    ├──────CA_SystemEDGE_GALAX
    ├──────CA_SystemEDGE_HACMP
    ├──────CA_SystemEDGE_HyperV
    ├──────CA_SystemEDGE_KVM
    ├──────CA_SystemEDGE_LPAR
    ├──────CA_SystemEDGE_MSCS
    ├──────CA_SystemEDGE_RM
    ├──────CA_SystemEDGE_SRM
    ├──────CA_SystemEDGE_UCS
    ├──────CA_SystemEDGE_VCLOUD
    ├──────CA_SystemEDGE_Zone
    └──────CA_VMVCAIM
```

トップ レベル Public ディレクトリには、5 つのサブディレクトリがあります。

コンポーネント名

IDManager インスタンス名である必要があります（CA Server Automation の場合は SM）。

ソフトウェア パッケージ

単一の展開可能なパッケージのすべてのバージョン、ローカリゼーション、およびアーキテクチャが含まれます（CA_SystemEDGE_Core、CA_SystemEDGE_SRM など）。

バージョン

内部に含まれるソフトウェア パッケージのバージョン。

言語

インストール パッケージ言語。

例： ENU

アーキテクチャ

アーキテクチャ固有のインストール要素（Windows_ia64、Solaris_x86 など）。

注: アーキテクチャ ディレクトリ名は、IDManager でサポートされるプラットフォームのいずれかである必要があります。

配布サーバ マシン内で実行される場合、IDManager コンポーネントは配布サーバの下のディレクトリを使用します。 これには、その内部使用のために暗号化されたパッケージの一時キャッシュが含まれます。 これらのパッケージは、ジョブの完了時に削除する必要があります。

プライベート IDPrimer インストール要素は、別のディレクトリ内に含まれています。 これらはデフォルトで、IDManager コンポーネント自体のインストール ディレクトリの下の以下のディレクトリに格納されています。

<CA Shared Components>/IDMgrApi/packages/private/idprimer

このディレクトリには、インフラストラクチャ展開コンポーネントでサポートされるすべてのプラットフォームの IDPrimer インストール要素が含まれます。

パッケージ フィルタ

サーバにアップグレードが適用されている場合は、数が増加するパッケージ バージョンをリモート展開で表示できます。 このリリースのデフォルト動作では、利用可能な最新のパッケージのみが表示されます。 その結果、［パッケージ］-［詳細］タブのデータもフィルタされ、各パッケージの最新バージョンのみが表示されます。 このパネルからラッパーを選択すると、選択されたラッパーの位置でツリーが展開されます。

すべてのパッケージを表示する場合は、［パッケージ］情報パネルの［最新パッケージのバージョンのみを表示します］チェック ボックスを使用してデフォルト フィルタ動作を上書きできます。 このチェック ボックスをオンにした場合（デフォルト）は、左側のツリーおよび［パッケージの詳細］タブで古いパッケージ バージョンがすべてフィルタされ、表示されなくなります。

フィルタリング動作を変更する方法

1. ［パッケージ情報］パネルにある［最新パッケージのバージョンのみ］チェック ボックスをオン/オフにします。
2. ユーザ インターフェースで［展開］ビューをリフレッシュします。

   最新のパッケージ バージョンが表示されます。

注: UI 内で、パッケージ バージョンが表示される他の場所がすべて影響されるとは限りません。

展開パッケージ設定ファイル

ソフトウェア パッケージ インストール要素のほか、展開可能な各パッケージは、追加のパッケージ設定ファイル pkginfo_PLATFORM.xml で参照されます。 パッケージ設定ファイルでは、インストール パッケージと設定プロセスについて説明されています。

この設定ファイルは以下を提供します。

- インストール パッケージのローカライズ可能な説明。

- マシンで読み取り可能な形式でパッケージ依存性をエンコードするメカニズム。
- 一般的にアクセス可能なインストール パラメータ タイプの文書化。
- 一定のレベルの検証を UI 内で実行するための、パラメータ タイプへの追加コンテキスト。
- パッケージ インストール プログラムでパラメータを表すのに使用される、パラメータ名とトークンの間のマッピング（プラットフォームに依存しない方式）。
- ターゲット マシンでのインストール要素の実行方法の指定。
- インストーラ終了コードと、展開システムが解釈したコードの間のマッピング

pkginfo.xml ファイルのローカライズ済み要素を、ロケール固有のファイルを並行使用して提供するか、または単一のファイルに埋め込むことができます。 pkginfo_PLATFORM.xml と一致する名前のファイルは、ローカライズされたメッセージ データを取得するためにロードされます。

展開システムがパッケージ設定ファイルを、パッケージング ツリー内のプラットフォーム固有のサブディレクトリと並行して見つける必要があります。 たとえば、以下のディレクトリを参照します。

%AllUsersProfile%¥CA¥SM¥domainserver¥Deployment¥Packages¥SM¥CA_SystemEDGE_Core¥5.7.1¥ENU

```
pkginfo_AIX.xml
pkginfo_HPUX.xml
pkginfo_Linux.xml
pkginfo_LinuxPPC.xml
pkginfo_Solaris_sparc.xml
pkginfo_Solaris_x86.xml
pkginfo_Windows.xml
```

リモート展開の使用

CA Server Automation ユーザ インターフェースから一元化されたリモート展開を使用して、1 回の操作で複数システムにモニタリング エージェントを展開できます。 CA Server Automation によるパッケージ展開は、セントラル インターフェースから企業全体にわたってインストールされたモニタリング ソフトウェアを設定することができる、安全で信頼できるソリューションです。

展開の制限

展開を実行する前に、以下の制限を考慮してください。

- CA Server Automation マネージャ システムにエージェントをインストールする場合は、手動のスタンドアロン エージェント インストールを実行します。 CA Server Automation マネージャ システムでのエージェントの展開はサポートされていません。
- 既存のホスト オペレーティング システム サービスを使用して、ターゲット システムへのリモート アクセスを獲得できるかどうかによって、展開プロセスが異なります。これらのサービスがターゲット ノードで利用可能でない場合は、IDPrimer クライアント パッケージおよび対応するキーをターゲット システムにインストールすることが必要になります。

  注: インストールの詳細については、「*インフラストラクチャ展開プライマ ソフトウェアの手動インストール*」を参照してください。
- 展開は、サポートされるエージェント プラットフォームの大部分（すべてではない）でサポートされています。

  注: 展開のサポートの詳細については、「CA Server Automation リリース ノート」を参照してください。

展開認証情報の制限

UI では、ユーザ名とパスワードのフィールドへのエントリはいずれも、64 文字に制限されています。

監査証跡

ジョブとタスクは、展開システムの 2 つの基本概念です。 *展開ジョブ*は、1 つ以上のターゲット システムで利用可能な 1 つ以上のパッケージを指定します。 *展開タスク*は、ターゲット システム上でのソフトウェア パッケージの個別の展開を表します。 展開ジョブ レポートにより、展開ジョブのステータスをクエリできます。

展開ジョブの状態を作成、制御、および照会することができます。 ジョブの開始後、その個々の展開タスクが、実際の展開を実行する利用可能な配布サーバに委任されます。 ジョブの進行につれ、進捗状況を追跡できるため、展開が確実に実行され、問題があれば識別して修正できます。

リモート展開は、以下の情報を提供できます。

- 現在、どの展開ジョブが：
  - 非アクティブである（まだ開始されていない）
  - アクティブ
  - 完了しているもののうち、どれが：
    - 成功
    - 部分的に成功
    - 失敗
- どの展開ジョブが：
  - 特定のターゲット マシンに関連付けられているか
  - 特定のパッケージ/パッケージ グループに関連付けられているか
- どのパッケージが特定のターゲット マシンに展開されたか
- どのユーザが特定のパッケージの展開を作成/開始したか
- どのマシンが特定の展開ジョブでターゲットになるか
- どのマシンがアクティブな展開ジョブのターゲットになるか

注: リモート展開は、noexec フラグでマウントされた /tmp ファイル システムを備えた UNIX/Linux システムへのソフトウェアの展開をサポートします。

新規パッケージ ラッパーの作成

パッケージ ラッパーは、特定のパッケージの展開時に使用する、展開メカニズムのプラットフォーム固有の手順を提供します。 各パッケージには、リモート展開をサポートする、すべてのプラットフォーム用のデフォルトのパッケージ ラッパーが含まれています。 デフォルトとは異なる設定が必要なシステムがある場合は、新しいパッケージ ラッパーを作成できます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］フォルダが表示されます。

2. ［パッケージ］を展開します。

   利用可能なパッケージのリストが ［展開］ペイン内に表示されます。

3. ［展開］ペイン内のパッケージ名を右クリックし、［新しいラッパーの作成］を選択します。 または、［利用可能なラッパー］ツールバーの［+］（新規）をクリックします。

   ［新規ラッパー］ダイアログ ボックスが表示されます。

4. ラッパーの名前および説明 (オプション) を入力し、ラッパーがサポートするプラットフォームを指定して、［OK］をクリックします。

   ラッパーが作成され、詳細が右側のペインに表示されます。

   注: SystemEDGE パッケージ ラッパーを作成する場合は、［トラップ ポート］、［トラップ先］、および［トラップ コミュニティ］フィールドの間の依存性を考慮してください。 これらのフィールドは、どれも設定しないか、すべてを設定するかのいずれかにする必要があります。 一部のフィールドを設定した場合は、インストーラがエラー メッセージを表示します。

パッケージ ラッパーの変更

パッケージ ラッパーは、インストール パス、ポート、トラップ コミュニティなど、展開パッケージのプラットフォーム固有のインストール設定セットを定義します。 ユーザが作成した、またはデフォルトのパッケージ ラッパーを編集して、このインストール設定のセットを変更することができます。 利用可能なプロパティは、パッケージのタイプによってさまざまです。

パッケージ ラッパーを変更する方法

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］フォルダが表示されます。

2. ［パッケージ］、パッケージの特定の種類、およびラッパー プラットフォームを展開し、変更するラッパーを選択します。

   右側のペインにラッパーの詳細が表示されます。

3. 必要に応じて、パッケージ プロパティを変更して［保存］をクリックします。 ［プロパティ］ペインに表示されるオプションは、選択したパッケージ タイプによって異なります。

パッケージ ラッパーのコピー

パッケージ ラッパーは、コピーし、必要に応じてそのプロパティを編集することができます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［パッケージ］、パッケージの特定の種類、およびプラットフォームを展開します。

3. ラッパーを選択します。

   右側のペインにラッパーの詳細が表示されます。

4. ラッパー名を右クリックします。［コピー］を選択します。［アクション］ドロップダウン メニューから［コピー］を選択することもできます。

   ［コピー］ダイアログ ボックスが表示されます。

5. パッケージ ラッパーの名前と任意の説明を入力し、［OK］をクリックします。

   新しいパッケージ ラッパーが［展開］ペインに表示されます。

6. 必要に応じてプロパティを編集し、［保存］をクリックします。

   新しいパッケージ ラッパーが左ペインに表示されます。

パッケージ ラッパーの削除

必要のなくなったパッケージ ラッパーは削除することができます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［パッケージ］、パッケージの特定の種類、およびプラットフォームを展開します。

3. ラッパーを選択します。

   右側のペインにラッパーの詳細が表示されます。

4. ラッパー名を右クリックします。［削除］を選択します。［アクション］ドロップダウン メニューから［削除］を選択することもできます。

   警告メッセージが表示されます。

5. ［はい］をクリックして削除を確定します。

   パッケージ ラッパーが削除されます。

パッケージ ラッパーの名前変更

パッケージ ラッパーの名前は変更することができます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［パッケージ］、パッケージの特定の種類、およびプラットフォームを展開します。

3. ラッパーを選択します。

   右側のペインにラッパーの詳細が表示されます。

4. ラッパー名を右クリックします。

5. ［名前の変更］を選択します。［アクション］ドロップダウン メニューから［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。

6. 新しい名前を入力し、［OK］をクリックします。

   パッケージ ラッパーの名前が変更されます。

展開ジョブの作成

システムにエージェントを展開するには、展開ジョブを作成します。 展開ジョブには、展開パッケージを適切なシステムに適切なタイミングで配信するために、CA Server Automation にとって必要な詳細が含まれます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［管理対象リソース］ペインで［ジョブ］フォルダを右クリックし、［新規ジョブの作成］を選択します。［ジョブ］フォルダを選択し、［ジョブ ステータス］ツールバーの［+］（新規）をクリックする方法もあります。

   ［ジョブ セットアップ］ページが表示されます。

3. ［ジョブ名］ペインで名前を入力し、オプションで、ベースにする既存のテンプレートを選択して、［次へ］をクリックします。

   ［パッケージ選択］ページが表示されます。

4. プラットフォームと、展開するパッケージを選択します。

5. （オプション）［詳細］タブをクリックします。

   ［パッケージ ラッパー詳細］ダイアログ ボックスが表示され、パッケージ プロパティをインラインで編集できます。パッケージ ラッパーが不完全または無効な状態であっても、フィールドがインライン編集によって修正できる場合。

   a. ［編集］をクリックし、パッケージ ラッパーのプロパティを変更します。

   b. ［保存］をクリックし、［OK］をクリックします。

      パッケージ ラッパーのプロパティが更新されます。

6. 下矢印をクリックしてパッケージ ラッパーをジョブに追加し、［次へ］をクリックします。

   ［マシン選択］ページが表示されます。

7. 展開先のシステムを選択し、［次へ］をクリックします。環境内に多数のサーバがある場合、すべてのサーバを一覧表示するには、一定数のエントリを含むページが複数必要になることがあります。ページでサーバを選択し、次のページにスクロールしても、前のページで行った選択内容は有効なままです。

   ［選択済みマシン］ページが表示されます。

8. ［認証情報の設定］をクリックし、接続を確立するために必要なシステム認証情報を設定して、［次へ］をクリックします。

   注: ドメイン認証情報を使って Windows ターゲット システムに展開する場合は、「DOMAIN¥ユーザ名」の形式を使用する必要があります。

   詳細設定ページが表示されます。

9. （オプション）展開を管理する配布サーバを設定します。設定しない場合は、自動的に選択されます。

10. ジョブのスケジュール オプションを選択します。

    即時配布

    新しい展開ジョブを作成した直後にジョブを開始します。 即時配布はデフォルト オプションです。

    時差配布

    特定の時間にパッケージを配布します。

    スケジュール済み配布

    将来の特定の時間に展開をスケジュールします。

11. （オプション）以前に同じ展開インフラストラクチャを使ってパッケージをシステムに正常に展開したことがある場合は、再度そのインフラストラクチャを強制的に実行することができます。

12. ［次へ］をクリックします。

    ［サマリ］ページが表示されます。

13. ジョブの詳細を確認し、［展開］をクリックします。

    展開ジョブが作成されます。

注: 作成したジョブはテンプレートとして保存できます。将来のジョブで簡単に再利用できるように、テンプレートにはパッケージとマシンの選択内容が保存されます。

展開前の読み取り/書き込みコミュニティの指定

SystemEDGE のモニタリング機能と管理機能をフルに活用するには、SystemEDGE エージェントのための有効な読み取り/書き込みコミュニティを指定する必要があります。 読み取り/書き込みコミュニティ文字列は、展開の前に、SystemEDGE のリモート展開パッケージ ラッパー内で設定できます。

展開前の読み取り/書き込みコミュニティの指定

1. ［リソース］-［展開］ を選択します。
2. ［展開］ペインを開きます。

   利用可能な展開グループが表示されます。
3. ［パッケージ］、パッケージの特定の種類、およびラッパー プラットフォームを展開し、変更するラッパーを選択します。

   右側のペインにラッパーの詳細が表示されます。
4. ［読み取り/書き込みコミュニティ］フィールドで読み取り/書き込みパラメータを指定し、［保存］をクリックします。

   注: ユーザ インターフェースでスペース文字またはセミコロン（;）を含むコミュニティ文字列を指定すると、エージェントは正しく機能しません。

関連項目:

サーバ レベルの SNMP 設定の追加 (P. 127)
マシンへのポリシーの適用 (P. 323)

インストール後の読み取り/書き込みコミュニティの指定

SystemEDGE のモニタリング機能と管理機能をフルに活用するには、SystemEDGE エージェントのための有効な読み取り/書き込みコミュニティを指定する必要があります。 SystemEDGE エージェントをすでに展開している場合、インストール後に読み取り/書き込みコミュニティ文字列を追加できます。 これは、複数システムのモニタおよび管理に使用できるグローバル SNMP エントリを作成することにより、またはサーバ固有 SNMP エントリを作成することにより、実行できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［トラップ & コミュニティ］タブをクリックします。

   ［コミュニティ］ページが表示されます。

4. ［サーバ固有 SNMP 設定のみを含める］を選択します。

5. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

グローバル SNMP エントリを作成する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［設定］をクリックします。

   ［設定］ページが表示されます。

3. ［SNMP］をクリックします。

4. リストで、編集する SNMP 設定のチェック ボックスをオンにし、ツール アイコン（編集）をクリックします。

   ［SNMP 設定の編集］ダイアログ ボックスが表示されます。

5. ［アクセス タイプ］ドロップダウン リストから［読み書き］を選択し、［コミュニティ文字列］フィールドにパラメータを指定して、［OK］をクリックします。

6. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

7. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

8. ［トラップ & コミュニティ］タブをクリックします。

   ［コミュニティ］ページが表示されます。

9. ［サーバ固有 SNMP 設定および選択されたデフォルト設定を含める］を選択します。

10. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

注: 詳細については、「マシンへのポリシーの適用」を参照してください。

関連項目:

サーバ レベルの SNMP 設定の追加 (P. 127)

展開ジョブのステータスの追跡

コンピュータのセットにエージェント パッケージのセットを展開するジョブが開始されたら、その進捗状況とステータスを追跡できます。［ジョブ］タブには、作成されたすべての展開ジョブの表が表示され、これには、ジョブ名、含まれるパッケージ、ジョブ ステータスなどのリストが含まれます。この表から、ジョブが失敗した理由を含む、特定のジョブに関する詳細を確認できます。

注:［ジョブ ステータス］ペインで、フィルタを選択して特定のジョブ タスクをフィルタできます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［ジョブ］フォルダをクリックします。

   ［ジョブ ステータス］ページが表示されます。

3. 表示するジョブをクリックします。

   ［ジョブ情報］ページが表示されます。

4. ［タスク ステータス］ペインで、利用可能なフィルタのいずれかを使用して特定のジョブ タスクをフィルタします。あるいは、ページングインターフェースを使用してタスクを特定します。

5. ［拡張ステータス］をクリックしてタスクの拡張情報を表示します。

   タスクに関する詳細を含む［拡張済みステータス情報］ダイアログボックスが表示されます。

   情報

   タスクに関する一般情報を表示します。

   メッセージ

   タスクに関するメッセージ（「パッケージの配信に失敗しました」など）を表示します。

   理由

   失敗の理由を表示します。

   例：

   - マシン可用性が不足
   - システム認証情報が無効
   - システム ホスト名を解決できない
   - パッケージ依存性を実現できない

   アクション

   問題を修正するために取るアクションを表示します。

展開ジョブの再サブミット

失敗した、または部分的に失敗した展開ジョブは、再サブミットすることができます。

次の手順に従ってください:

1. ［リソース］-［展開］ を選択します。

   ［展開］ペインに［パッケージ］、［テンプレート］、および［ジョブ］が表示されます。

2. ［ジョブ］フォルダをクリックします。

   ［ジョブ ステータス］ページが表示されます。

3. 再サブミットするジョブをクリックします。

   ［ジョブ情報］ページが表示されます。

4. ［アクション］をクリックし、［再サブミット］を選択します。

   ［パッケージ選択］画面に展開ウィザードが表示されます。

5. 展開する希望のパッケージ ラッパーを選択し、［次へ］をクリックします。

   ［選択済みマシン］ページが表示されます。

6. （オプション）展開したくないマシンを削除します。

   注: すべてのパッケージが以前正常に展開されたマシンは選択されません。

7. ［認証情報の設定］をクリックし、選択したすべてのマシンの認証情報を適宜変更します。オプションで、再起動ジョブからマシンを削除し、［次へ］をクリックします。

   詳細設定ページが表示されます。

8. （オプション）ジョブのスケジュール オプションを変更します。

   即時配布

   新しい展開ジョブを作成した直後にジョブを開始します。 即時配布はデフォルト オプションです。

   時差配布

   特定の時間にパッケージを配布します。

   スケジュール済み配布

   将来の特定の時間に展開をスケジュールします。

9. すべてのパッケージ（以前展開に成功したパッケージを含む）を強制的に展開するには、［以前展開されていたパッケージの再展開］を選択し、［次へ］をクリックします。

   ［サマリ］ページが表示されます。

10. ジョブの詳細を確認し、［展開］をクリックします。

    ジョブが再サブミットされます。

展開済みパッケージの表示

［モニタリング ソフトウェア］ページでは、単一のマシンまたは複数のマシンに展開したパッケージのリストを表示できます。

展開済みのパッケージを表示する方法

1. ［リソース］を選択します。

   ［エクスプローラ］ペインが表示されます。

2. システムまたはサービスを選択します。

   ［サマリ］ページが表示されます。

3. ［モニタリング ソフトウェア］-［展開］を選択します。

   ［展開履歴］ページが開き、マシンの全展開ジョブのリストが示されます。 テーブルには、選択したシステムの全展開ジョブの詳細が表示されます。

   - タスク ID
   - ジョブ ID

- ターゲット
- パッケージ
- プラットフォーム
- ラッパー
- ラッパー バージョン
- 開始者
- 開始時刻
- 終了時刻
- ステータス
- 拡張ステータス

展開履歴の表示

展開履歴情報は、以下の場所で利用可能です。

[展開]ペイン

完了、アクティブ、保留中、失敗の展開タスクの数、および成功した展開のサマリが表示されます。 このビューにアクセスするには、最上位の［展開］フォルダをクリックします。

[ジョブ]ペイン

ジョブ名、含まれるパッケージ、およびジョブ ステータスのリストを含む、作成したすべての展開ジョブの表が表示されます。この表から、ジョブが失敗した理由を含む、特定のジョブに関する詳細を確認できます。 展開失敗の共通の原因には、以下のものがあります。

- システム認証情報が無効
- システム ホスト名を解決できない
- パッケージ依存性を実現できない

注: このペインからジョブを再サブミットし、失敗の理由を修正して再展開できます。 このビューにアクセスするには、［ジョブ］フォルダをクリックします。

具体的なリモート展開の使用例

カスタム ポートを使用した SystemEDGE エージェントの展開/インストール

標準以外のポートに SystemEDGE エージェントを展開するには、多くの設定を実行する必要があります。 展開後にマネージャが確実にシステムを検出して管理できるようにするには、以下の手順に従います。

1. パッケージ ラッパーを更新します。
   - リモート展開ソリューションを使用している場合は、まず、包装係を設定して、使用するポートを指定する必要があります。 ユーザ インターフェースで［プロビジョニング］-［展開］に移動し、［ポート］フィールドを変更します。 書き込みコミュニティ文字列も、ここで更新できます。
2. CA Server Automation で SNMP コミュニティ文字列を更新します。
   - マネージャが標準以外のポートを使用して正常にマシンのモニタリングと管理を行うには、モニタリングと管理に使用する、適切なポート/書き込みコミュニティ文字列の組み合わせを認識している必要があります。 そのためには、複数のシステムのモニタリングと管理に使用できるグローバルな SNMP エントリを作成するか、サーバ固有の SNMP エントリを作成することができます。
     - グローバル SNMP 設定を更新する方法： ユーザ インターフェースで［管理］-［SNMP］に移動し、適切な SNMP コミュニティ文字列/ポートの組み合わせを含む新しいエントリを追加します。
     - サーバ固有の SNMP 設定を更新する方法： ［ポリシー］-［エクスプローラ］-［*Machine_Name*］-［メトリック］-［SNMP 設定］に移動し、必要なポート/書き込みコミュニティ文字列の新しいエントリを追加します。

これらの設定を更新した後は、通常の方法でエージェントを展開/インストールできます。 その後、SystemEDGE プラットフォーム管理モジュールがカスタムのポート/書き込みコミュニティ文字列の組み合わせを使用して、サーバを検出、モニタ、および管理を行います。

SystemEDGE エージェント用ポートの再設定

エージェントを再インストールすると、SystemEDGE エージェント用のポートを再設定できます。 エージェントを再インストールした後は、再設定するポートの詳細をプロビジョニングで編集しても、設定は変わりません。

SystemEDGE エージェント ポートの再設定

SystemEDGE エージェント ポートは、標準（デフォルト）ポート 161 から 1691 に再設定できます。たとえば、デフォルト ポート 161 上で MIB-II エージェントを実装する Microsoft SNMP サービスをインストールすることができます。 sysedge.cf ファイルを編集する方法は、エージェント ポートを再設定するためのサポートされている方法ではありません。 ポートの変更は、エージェントの再インストールによって実行する必要があります。これは、別のポートを指定するリモート展開を使用して、エージェントを再展開することにより実行できます。 Windows システムの場合、SystemEDGE コントロール パネル アプレットを使用して、エージェントを再設定することもできます。

コントロール パネルでの SystemEDGE エージェントの再設定

1. ［スタート］-［コントロール パネル］をクリックして、［プログラムの追加と削除］を選択します。さらに、リスト内の SystemEDGE Core を選択して、［変更］をクリックします。

   SystemEDGE セットアップ ウィザードが開きます。

2. ［次へ］をクリックします。

   ［再インストール タイプ］ページが表示されます。

3. ［再インストール］を選択し、［次へ］をクリックします。

   ［アプリケーション設定］ページが開き、インストール文書設定を変更できます。

4. ［次へ］をクリックします。

   ［SystemEDGE SNMP ポート番号］ページが開きます。

5. SystemEDGE ポート番号 1691 を指定し［次へ］をクリックします。
6. 設定を確認し、［再インストール］をクリックします。

   SystemEDGE エージェントはポート番号 1691 を使用するように再設定されます。

リモート展開/ポリシー設定を使用する SystemEDGE エージェント ポートの再設定

1. 「展開ジョブの作成 (P. 170)」の章にある手順に従ってください。ウィザードの手順 5 で、［以前展開されていたパッケージの再展開］を選択します。

   注: 再インストールでは、ポート番号以外のすべての指定されたインストール パラメータは無視されます。

   ポートを変更するためにエージェントを再インストールした後、正しいコミュニティ文字列でエージェントが設定されていることを確認するために、管理者はいくつかの手順を手動で実行する必要があります。

2. 以下のいずれかを実行します。

   サーバ用のサーバ固有 SNMP エントリを作成する。

   1. CA Server Automation UI で［リソース］タブをクリックし、［エクスプローラ］ペインを開き、Machine_Name を選択します。

      Machine_Name が選択されます。

   2. Machine_Name を右クリックし、［ポリシー］-［SNMP の設定］を選択します。

      ［SNMP 設定］ページが表示されます。

   3. ［追加］をクリックして、必要なポートに新しいエントリを作成します。

      ［新しい SNMP 設定］ページが表示されます。

   4. 必要な詳細を入力して、［OK］をクリックします。

      サーバ用に、サーバ固有の SNMP エントリが作成されます。

   グローバル SNMP 設定が存在し、ポリシーを更新することを確認する。

   CA Server Automation の UI で、［管理］-［SNMP］にナビゲートし、必要なポートの新しいエントリを追加します。設定が正しければ、［リソース］タブに移動して［設定］ペインを開き、ポリシーを選択してポリシーを編集します。 次に、［トラップ & コミュニティ］-［コミュニティ］をクリックし、中央のオプション［サーバ固有 SNMP 設定およびすべてのデフォルト設定を含める］を選択します。 ［ポリシーの保存］をクリックして、ポリシーを保存します。 この時点で、システムにポリシーを適用 (P. 323)する必要があります。 エージェント マシン上で SystemEDGE コントロール パネル アプレットを使用して、エージェントによって使用されるコミュニティ文字列を確認できます。

注: 詳細については、「Administration Guide」の「Deploying/Installing SystemEDGE Agents Using Custom Ports」を参照してください。

関連項目:

サーバ レベルの SNMP 設定の追加 (P. 127)

非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開

非特権ユーザ アカウントを使用する場合は、sudo 設定に関する以下の要件を考慮してください。

- sudo では、実行されたプログラムに有効な疑似端末が接続されていることを強制できません。 このような検証を特定のユーザ（グローバルに有効である場合）に対して無効にするには、/etc/sudoers ファイルに「Defaults: $username !requiretty」という行を追加します。 $username は、リモート展開に使用する実際のユーザ名に置換します。

  ファイルを編集する標準的な方法は、visudo コマンドの使用です。 visudo コマンドは $EDITOR を起動します。 編集が完了すると、ファイルの構文が確認されます。 結果が有効でない場合、visudo はファイルの保存をブロックします。

- sudo では、上位のプログラムを実行する前にユーザにパスワードを要求できません。 この動作を実行するには、ユーザに権限を与える行に NOPASSWD: キーワードが存在することが必要です。

- sudo では、必要なコマンドまたはすべての実行が可能である必要があります。 上記の要件を満たす設定エントリ（/etc/sudoers 内の行）の例は、次のとおりです。

  ```
  $username ALL=(ALL) NOPASSWD: ALL
  ```

  または

  ```
  $username ALL = NOPASSWD: /usr/bin/id,/bin/sh /tmp/idprimer/PifInst *
  ```

  注: $username は、リモート展開に使用する実際のユーザ名に置換します。 「id」および「sh」のパスが /usr/bin/id または /bin/sh とは異なる場合は、設定エントリのパスを適切に調整してください。

Solaris では、pfexec の以下の要件を考慮してください。

- すべてのローカル ユーザには、以下のコマンドで「プライマリ管理者」プロファイルを付与できます。

  ```
  usermod -P “Primary Administrator” {user}
  ```

- /etc/user_attr ファイル内のエントリを手動で追加することで、すべての非ローカル ユーザに「プライマリ管理者」プロファイルを付与できます。

  ```
  user::::type=normal;profiles=Primary Administrator
  ```

書き込みコミュニティを含まないエージェント設定

SystemEDGE パッケージ ラッパーに対する書き込みコミュニティの設定は必須ではありませんが、以下の情報を考慮してください。

- SystemEDGE エージェントに SNMP 読み取りコミュニティのみが設定されており、書き込みコミュニティが設定されていない場合でも、このエージェントは SystemEDGE PMM で検出可能です。ただし、SNMP 書き込みコミュニティが設定されたエージェントがない場合は、エージェントにポイント設定変更を実行できません。
- 完全な vCenter およびリモート モニタリング機能は、エージェントに書き込みコミュニティが設定されている場合にのみサポートされます。SNMP 書き込みコミュニティが設定されたエージェントがない場合は、CA Server Automation UI からの AIM 設定および管理を実行できません。
- 書き込みコミュニティのないエージェントは、CA Server Automation UI からポリシー設定を使用して、インストール後に設定できます。 ポリシー設定を使用すると、SNMP v1/2 より安全な SNMP v3 を使用するようにエージェントを設定することもできます。

ファイアウォール ソフトウェアを実行している Windows Vista™、Windows 2008、および Windows XP コンピュータへの展開

ファイアウォール ソフトウェアを実行しているコンピュータにエージェントを展開できるようにするには、以下を考慮します。

- Windows Vista™ または Windows 2008 オペレーティング システムが稼働するターゲット コンピュータのファイアウォールが *オフ*（無効）になっており、そのコンピュータへの展開に失敗する場合は、値が 0x1 の DWORD タイプとして、以下のレジストリ変数を作成または設定する必要があります。

  HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System¥LocalAccountTokenFilterPolicy

  これが必要である理由は、Windows Vista™ または Windows 2008 におけるユーザ アカウント管理（UAC）では、管理権限がローカル ユーザに自動的には付与されないためです。これは、ローカル ユーザが管理者グループのメンバであっても必要です。

  注: この値を設定すると、結果的に UAC アクセス トークンのフィルタリングが無効化されます。

  Windows Vista™ または Windows 2008 が稼働しているコンピュータに対してローカル管理者アカウントを持っている場合は、この値を設定する意味があります。ドメイン管理者は、これを変更しても影響を受けません。

- Windows Vista™または Windows 2008 が稼働しているターゲット コンピュータのファイアウォールが *オン*（有効）になっている場合は、そのコンピュータへの展開を有効にするために、ファイル共有ポートだけでなく、以下のポートも開いている必要があります。

  UDP ポート

  CAM： 4104

  ファイルとプリンタの共有など： 137、138

  TCP ポート

  IDManager： 135

  ファイルとプリンタの共有など： 139、445

- それでも展開が失敗する場合は、Windows Vista™ または Windows 2008 のファイアウォールの以下の「送信の規則」を完全に有効にする必要があります。
  - リモート アシスタンス
  - ネットワーク ディスカバリ
  - ファイルとプリンタの共有
  - コア ネットワーク
- ファイアウォール ソフトウェアを実行する Windows XP コンピュータへのエージェント展開を有効にするには、以下の手順を手動で実行する必要があります。
  1. セキュリティ ポリシー［ネットワーク アクセス：ローカル アカウントの共有とセキュリティ モデル］を［Guest のみ - ローカル ユーザが Guest として認証する］から［クラシック - ローカル ユーザがローカル ユーザとして認証する］に変更します。

     クラシック モデルでは、リソースへのアクセスを微調整でき、通常は指定されたリソースへの「読み取り専用」アクセスが可能な、ローカル アカウントを使用するネットワーク ログインがゲスト アカウントにマップされないようにすることができます。
  2. 以下のファイアウォール設定を行います。
     - ファイルおよびプリンタの共有を許可
     - UDP ポート 4104 のオープン
     - TCP ポート 135 のオープン

展開ジョブ

ターゲット システムにエージェントを展開するには、最初に展開ジョブを作成します。 展開ジョブには、展開パッケージを適切なシステムにスケジュールされた時間で配信するために、CA Server Automation にとって必要な詳細が含まれます。 いくつかの場所からアクセス可能なリモート展開ジョブ ウィザードを使用して、新規ジョブを作成できます。 以下のいずれかの方法を選択します。

- ダッシュボードの［クイック起動］パネルにある［ジョブの展開］リンクを使用する
- ［リソース］-［展開］タブの［ジョブ］パネルから［+］（新規）ボタンを使用する
- ［リソース］-［エクスプローラ］タブにある管理対象ノードのコンテキスト メニューを使用する
- ［リソース］-［エクスプローラ］タブにある現在選択されている管理対象ノードの［モニタリング ソフトウェア］-［展開］タブから［+］（新規）ボタンを使用する

展開ジョブを作成するときは、以下の情報を指定します。

ジョブ情報

ジョブ名および、既存のテンプレートに基づいたジョブを作成するかどうかが含まれます。

展開パッケージ

プラットフォーム、展開するパッケージ、および各パッケージ固有のラッパーが含まれます。

マシン情報

パッケージの展開先のシステムと、接続の確立に必要なシステム認証情報が含まれます。

IP Address

ジョブを展開するインターフェースの IP アドレスを指定します。システムに複数の IP アドレスがある場合は、管理プロパティを持つ IP アドレスをデフォルトとして設定します。

注: 管理プロパティが有効になっていない IP アドレスは選択できません。

展開時間

展開を、すぐに実行するか、特定の時間だけずらして実行するか、または将来の特定の時間にスケジュールして実行するかを指定します。

また、ジョブを作成した後に、テンプレートとして保存できます。 将来のジョブで簡単に再利用できるように、テンプレートにはパッケージとマシンの選択内容が保存されます。

インフラストラクチャ展開プロセス

展開を実行するときの展開プロセスの主要な手順は、以下のとおりです。

1. 管理者のコンピュータから、インフラストラクチャ展開クライアント コンポーネントが、1 つ以上のターゲット コンピュータのリストにエージェントをインストールする要求を IDManager マネージャに発行します。 展開マネージャは、クライアントに対してリモートのコンピュータ上で実行されている場合があります。 ターゲットのリストは、明示的なマシン名または IPv4 アドレスで構成されています。

   注: 検出されたリソースにのみ展開できます。

   各ターゲット コンピュータへの展開が成功するには、ターゲット名が明示的に入力されているかコンテナから取得されているかにかかわらず、展開マネージャ コンピュータで表示されているように、ターゲットのアドレスへの解決に適したターゲット名であることが重要です。 たとえば、ディレクトリから取得されるターゲットのリストが完全修飾名（ネットワーク ドメイン名を持つ）ではない場合、特定のネットワーク設定では展開を継続できないことがあります。

2. IDPrimer がターゲット コンピュータにインストール済みであるかどうかが確認されます。 インストールされていない場合は、最初にターゲット コンピュータに IDPrimer がインストールされます。 IDManager は、IDPrimer インストール パッケージを配信しようとします。 どのような方法を使用して配信されるかは、ターゲットの動作環境、およびその環境で有効になっているセキュリティによって異なります。 IDPrimer イメージがターゲット コンピュータにコピーされた後、インストールが開始されます。

   一部のオペレーティング システムには、IDPrimer インストールをリモート起動する方法がありません。 この場合は、IDPrimer インストールの手動での実行が必要になる場合があります。

3. IDPrimer インストーラによって、インストーラ自体および CA メッセージ（CAM）コンポーネントがターゲット コンピュータにインストールされます。 IDPrimer がインストールされ、IDManager がターゲット コンピュータから「インストール完了」シグナルを受信すると、パッケージ展開を開始することができます。 IDManager マネージャで以前に IDPrimer がインストールされており、それを使用して認証を行っている場合は、ユーザ名またはパスワードを再度提供しなくても、その IDManager マネージャでパッケージを展開できます。 その後の展開では、IDPrimer によって非対称の暗号化キーを使用して認証が行われ、すでにアクセスが取得された管理者へのアクセスが制限されます。

関連項目

CA Server Automation インフラストラクチャを自動展開するための前提条件 (P. 191)
IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項 (P. 194)
IDManager が使用する転送パッケージのプロトコル (P. 194)
インフラストラクチャ展開プライマ ソフトウェアの手動インストール (P. 195)
Windows での展開プライマ インストール (P. 195)
Linux または UNIX での展開プライマ インストール (P. 196)
展開管理証明書のプライマ インストールへの提供 (P. 196)
Windows 上の展開管理証明書 (P. 196)
Linux または UNIX 上の展開管理証明書 (P. 197)
Linux の Compatibility Library (P. 197)

CA Server Automation インフラストラクチャを自動展開するための前提条件

このインフラストラクチャ展開コンポーネントを使用して、ターゲット コンピュータにリモートでエージェント ソフトウェアをインストールできます。 このインストールは、ソースおよびターゲット コンピュータ上の基本オペレーティング システムの機能によってのみ実行できます。 このインストールは企業のネットワーク設定による制限の対象となります。

ソフトウェア展開時の最初のステップは、小規模のプライマ アプリケーションである IDPrimer をターゲット コンピュータにリモート インストールすることです。 *IDPrimer* ソフトウェアの役割は、その後にソフトウェア コンポーネントのインストール イメージを転送することと、そのインストールの起動を実行することです。ターゲット コンピュータに IDPrimer を配信する場合、展開マネージャは、ターゲットで有効なユーザ クレデンシャルを提供する必要があります。

IDPrimer は、以下のメカニズムのいずれかを使用して、ターゲット システムに転送されます。 ターゲット オペレーティング システムを展開マネージャが認識している場合は、適切な転送メカニズムが選択されます。ターゲットのオペレーティング システムを判別できない場合は、以下の各メカニズムが順に試行されます。

- ネットワーク共有を開く

  展開マネージャは、ターゲット システムにある Windows ネットワーク共有に接続します。 デフォルトでは、使用される共有名は ADMIN$ です。 IDManager 設定オプションはデフォルトの共有名を制御します。 このメカニズムは、Windows ベースの環境で実行している展開マネージャからのみ使用可能です。 Windows XP Home などの少し異なる Windows バージョンは、この展開のメカニズムをサポートしていません。

- SSH プロトコルを使用してターゲット コンピュータとのネットワーク接続を開き、SFTP を使用してプライマ インストール パッケージを転送する

  このメカニズムは、SSH サーバが稼働しているすべてのコンピュータに対して機能しますが、Linux や UNIX コンピュータがターゲットの場合にも役立ちます。

  注: Solaris システムに展開する場合は、SunSSH v1.1（またはそれ以降）または OpenSSH の最新バージョンを使用することをお勧めします。Solaris プラットフォームおよびバージョンに適用可能なパッチの詳細については、Web サイト、http://opensolaris.org/os/community/security/projects/SSH をご覧ください。

  ターゲット コンピュータ上でファイアウォールを実行している場合は、以下の条件が満たされることを確認します。

  - SSH ポート（22）は展開マネージャからの接続を許可するために有効にされます
  - また、ターゲット コンピュータ上の SSH サーバが、3DES 暗号を含む RSA キーによる暗号化、および HMAC-SHA1 メッセージ認証コード（MAC）を使用するように設定されています

  注: ほとんどの SSH サーバは、デフォルトでこの設定をサポートしますが、そうでない場合は、SSH サーバのドキュメントで詳細を調べてください。

  UNIX または Linux エージェントに展開するために、最近の SSH 実装の /etc/ssh/sshd_config 設定ファイルを以下のように設定する必要があります。

  - PasswordAuthentication を Yes に設定
  - PermitRootLogin を Yes に設定（または「非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開 (P. 184)」セクションの説明に従って sudo/pfexec を設定）
  - SFTP サブシステムが有効であることを確認

  リモート展開では、noexec フラグでマウントされた /tmp ファイル システムを含むシステムへのソフトウェア展開がサポートされます。

IPv4 および IPv6 スタックの両方を実行している IBM AIX システムへ、IPv6 アドレスを使用して展開する場合は、ターゲット コンピュータの SSH サーバが IPv4 向けのポート 22 を使用するように設定します。 SSH を設定するには、sshd_config 設定ファイルを編集し、ListenAddress を「::」に設定します。

注: 展開マネージャとターゲット コンピュータの間で FIPS 準拠の SSH 通信を行うには、展開マネージャでの FIPS 専用モードの設定とは別に、ターゲット上で稼働している SSH サーバも FIPS 準拠の暗号化モジュールを使用していることを確認します。

重要: 現在使用されているオペレーティング システムでは、ソフトウェアのリモート インストールが推奨されていません。また、明確に禁止されている場合もあります。 これらのシステムにソフトウェアを展開しようとすると、ステータスが「プライマ トランスポートがありません」になり、展開は失敗します。 このような場合は、DVD などの物理的な配布メディアを使用するなど、他の手段を使用してソフトウェア コンポーネントをインストールしてください。

あるいは、IDPrimer ソフトウェアを備えたマシンを事前インストールまたはプロビジョニングすることができます。こうすると、基本オペレーティング システムが提供している機能を必要とせずに、展開を実行できます。認証が行われていない場合は、許可された展開を実行する前に、有効な認証情報を入力します。

ご使用の環境で自動展開が可能かどうかを判別するには、以下のような標準オペレーティング システム操作を実行して確認します。

- Windows 共有を使用した IDPrimer イメージの配信の場合は、展開マネージャ ホスト コンピュータから各展開ターゲット コンピュータにマップします。 展開リクエストで提供されるターゲット ユーザ クレデンシャルを使用します。

  デフォルトの共有： ADMIN$

- SSH を使用した IDPrimer イメージの配信の場合、SSH を使用して、展開マネージャから展開ターゲット コンピュータへ接続できる必要があります。

関連項目

非特権ユーザ アカウントを使用した UNIX/Linux へのリモート展開 (P. 184)

IPv6 アドレスを使用したインフラストラクチャ展開に関する注意事項

IPV6 環境で CA Server Automation 展開サービスを使用する場合は、以下の前提条件を認識している必要があります。

1. マネージャ マシン（および各展開（配布）サーバ））で、以下のレジストリ キーを 1 に設定する必要があります。
   - HKLM¥System¥CurrentControlSet¥Services¥smb¥Parameters¥IPv6EnableOutboundGlobal (REG_DWORD)
2. Windows 2003 マネージャ マシンには、以下に示す 3 つのホットフィックス更新を適用する必要があります。
   - http://support.microsoft.com/kb/947369/en-us
   - http://support.microsoft.com/kb/950092/en-us
   - http://support.microsoft.com/kb/974927/en-us
3. ターゲット マシンのホスト名は、グローバル IPv6 アドレスに解決される必要があります。また、IPv6 アドレスの逆引きルックアップは、同じホスト名に解決される必要があります。
4. 各マネージャ マシンで、インフラストラクチャ展開設定ポリシー オプション usehostnames の値が 1 であることが必要です。このファイルは、デフォルトでは、以下のディレクトリにあります。

   C:¥Program Files¥CA¥SC¥IDMgrApi¥config¥SM¥idconfig.xml

IDManager が使用する転送パッケージのプロトコル

IDManager は、配布サーバを使用した展開時に、以下のプロトコルを使用してパッケージをターゲット コンピュータに転送します。

Windows ネットワーク共有

配布サーバとターゲット コンピュータが Windows 上にある場合は、このメカニズムを使用します。

SSH/SFTP

配布サーバかターゲット マシンのいずれかが Linux または UNIX 上にある場合は、このメカニズムを使用します。

これらの転送メカニズムの詳細については、「CA Server Automation インフラストラクチャを自動展開するための前提条件」を参照してください。

インフラストラクチャ展開プライマ ソフトウェアの手動インストール

何らかの理由でターゲット コンピュータへの自動展開が不可能な場合でも、プライマ ソフトウェアを手動でターゲット コンピュータにインストールしてソフトウェアを展開できます。 この展開は、物理的にプライマ パッケージをインストールするか、またはログイン スクリプトを使用してインストールを実行するかのいずれかによって可能です。

プライマ ソフトウェア自体のインストールだけでなく、セキュリティ キーもインストールする必要があります。このキーは、ターゲット コンピュータへの展開に使用する展開マネージャによって生成されます。

Windows での展開プライマ インストール

Windows を実行しているターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- CA Server Automation インストール メディア（DVD）をターゲット コンピュータで利用できるようにするか、プライマ設定ファイルをターゲット コンピュータに手動でコピーします。プライマ設定ファイルは、インストール メディアの以下のディレクトリに格納されています。

  32 ビット Windows で有効

  %PROGRAMFILES%¥CA¥SC¥IDMgrApi¥packages¥private¥idprimer¥Windows_x86

  64 ビット Windows で有効

  %PROGRAMFILES(X86)%¥CA¥SC¥IDMgrApi¥packages¥private¥idprimer¥Windows_x86

- ターゲット コンピュータ上で IDPrimer_Setup.exe を実行して、プライマをインストールします。

Linux または UNIX での展開プライマ インストール

Linux または UNIX ターゲット コンピュータでの展開プライマのインストールには、以下のアクションが必要です。

- CA Server Automation インストール メディア（DVD）をターゲット コンピュータで利用できるようにするか、プライマ インストール イメージをターゲット コンピュータに手動でコピーします。 プライマ インストール イメージは、インストール メディアの以下のディレクトリに格納されています。

  %PROGRAMFILES%¥SC¥IDMgrApi¥packages¥private¥idprimer¥Linux_x86

- ターゲット コンピュータ上のプライマ インストール イメージが含まれるディレクトリに移動して、以下のインストール コマンドを実行し、プライマをインストールします。

  ```
  # sh installidp
  ```

展開管理証明書のプライマ インストールへの提供

展開マネージャは、ターゲット コンピュータ上のプライマが展開パッケージを受け取る前にターゲット コンピュータに転送する必要がある証明書を生成します。 展開証明書ファイルの名前は dmkeydat.cer です。

証明書ファイルの場所は、インストール時に設定されます。 証明書ファイルをより安全なエリア、またはフェールオーバ ソリューションを提供する 2 つのマネージャが共有する場所へ格納する場合は、別のファイルの保存場所を設定します。 後者の場合、証明書を共有すると、展開マネージャがいずれかのマネージャから配信された IDPrimer コンポーネントと通信できるようになり、認証クレデンシャルを再度提供する必要もありません。

Windows 上の展開管理証明書

Windows では、展開証明書は以下のディレクトリにあります。

C:¥Program Files¥CA¥SC¥IDMgrApi¥config¥SM

証明書ファイル（MANAGER1 SM.PMR のように .PMR というサフィックスの）は、ターゲット コンピュータのプライマ インストール フォルダにコピーする必要があります。これは、デフォルトでは以下のフォルダです。

¥Program Files¥CA¥SC¥IDPrimer

Linux または UNIX 上の展開管理証明書

Linux と UNIX では、ターゲット コンピュータのプライマ インストール フォルダに展開証明書をコピーする必要があります。これは、デフォルトでは以下のフォルダです。

/opt/CA/SharedComponents/ID/primer/bin

Linux の Compatibility Library

IDPrimer インストーラは、特定の 32 ビット ライブラリ依存関係が存在することを前提としています。IDPrimer をインストールするには、これらの 32 ビット ライブラリが Linux ホスト上に存在している必要があります。

ほとんどの 32 ビットの Linux ディストリビューションでは、デフォルトですでにインストールされています。64 ビットの Linux の依存関係を満たすには、以下のコマンドを実行します。

- RedHat、CentOS、SuSE （32 ビットおよび 64 ビット OS）で有効：

  ```
  yum install libstdc++.i686
  ```

  このコマンドは、glibc、libstdc++、nss-softokn-freebl および libgcc の合計 4 つの RPM パッケージにインストールされます。

- Debian（64 ビット）で有効：

  ```
  apt-get install ia32-libs
  ```

  このコマンドは必須の 32 ビット ライブラリ （libc、libstd++、libgcc）をインストールします。

注: 必須の Compatibility Library および追加のシステム パッケージの詳細については、Linux サプライヤのサポート Web サイトを参照してください。

関連項目:

インフラストラクチャ展開プロセス (P. 189)

ポリシーとテンプレートを使用した SystemEDGE およびサービス レスポンス モニタの設定方法

このセクションでは、制御の中心点である CA Server Automation から、環境内のモニタリング ソフトウェアを管理する方法について説明します。

関連項目:

設定の概要 (P. 198)
ポリシーおよび階層型テンプレートをサーバに適用する方法 (P. 201)
自動ウォッチャーを作成してシステムに適用する方法 (P. 246)
ユーザ固有のメトリック（MIB 拡張）をモニタする方法 (P. 255)
特定の Windows パフォーマンス レジストリのメトリックをモニタする方法 (P. 258)
SRM ポリシーを作成する方法 (P. 262)
エージェントの検出 (P. 263)
ポリシー設定機能の一般的な使用法 (P. 263)

設定の概要

CA Server Automation ユーザ インターフェースから一元化された［ポリシー設定］を使用して、1 回の操作で管理対象エージェントを設定し、その設定を複数のシステムに適用できます。 ポリシー設定を使用すると、SystemEDGE と SRM AIM を一元化された場所で設定し、一貫性、信頼性、安全性のいずれにも優れた方法で企業全体にポリシーを配布できます。

CA Server Automation を使用したリモート ポリシー設定には、以下の利点があります。

- 複数のモニタリング プラットフォームにわたって使用する、プラットフォームに依存しないモニタリング ポリシーの作成
- 単一のサーバにもサーバのグループにも設定ポリシーを適用可能
- 1 つのポリシーに組み合わせることができるモニタリング テンプレートの作成

- 設定イベントおよびアクションの監査証跡
- イベントとレポートを通じた企業全体にわたるポリシー コンプライアンスの追跡
- 展開ソリューションとの統合、および、展開と同様、ターゲット システム上のフットプリントの最小化
- 数千の同時設定への拡張
- 複数のエージェント設定ソース（CA Server Automation、SystemEDGE など）に対するサポート、および CA Server Automation を通じた変更の受け入れまたは拒否
- SystemEDGE によってロードされた AIM のリモートからの制御
- 将来のポリシー設定するための既存の SystemEDGE 設定のインポート
- 個々に OID 番号を入力する必要がなくなる多数のモニタ定義設定時の選択リスト
- 手動でインデックスを定義する必要がなく、競合を回避できる自動モニタ インデックス割り当て

関連項目

SystemEDGE ポリシーを作成する方法 (P. 264)
SRM ポリシーを作成する方法 (P. 262)
マシンへのポリシーの適用 (P. 323)
ポリシー適用の進捗状況の確認 (P. 325)
適用されるポリシーの設定と表示 (P. 326)
エージェント ポリシーのダッシュボード ビュー (P. 200)
ユーザ固有のメトリック（MIB 拡張）をモニタする方法 (P. 255)
特定の Windows パフォーマンス レジストリのメトリックをモニタする方法 (P. 258)

エージェント ポリシーのダッシュボード ビュー

ダッシュボードで以下のビューを使用して、エージェント ポリシー割り当てを追跡できます。

ポリシー ステータス サマリ

ポリシーの数を示す円グラフとリストが表示されます。システムは次の 5 つの状態にいずれかになります。

未設定

SystemEDGE エージェントがインストールされていますが、ポリシーは設定されません。

インストール済みエージェント

SystemEDGE エージェントがインストールされています。

設定完了

SystemEDGE エージェントがインストールされ、ポリシーが設定されます。

構成エラー

SystemEDGE がインストールされ、ポリシーが設定されていますが、最終設定に失敗しました

インストール済みエージェント（未管理）

SystemEDGE がインストールされていますが、ポリシー設定で管理できないモードで実行されています。

ポリシー内訳

すべてのポリシーと各ポリシーに含まれるシステムの数を示す円グラフとリストが表示されます。

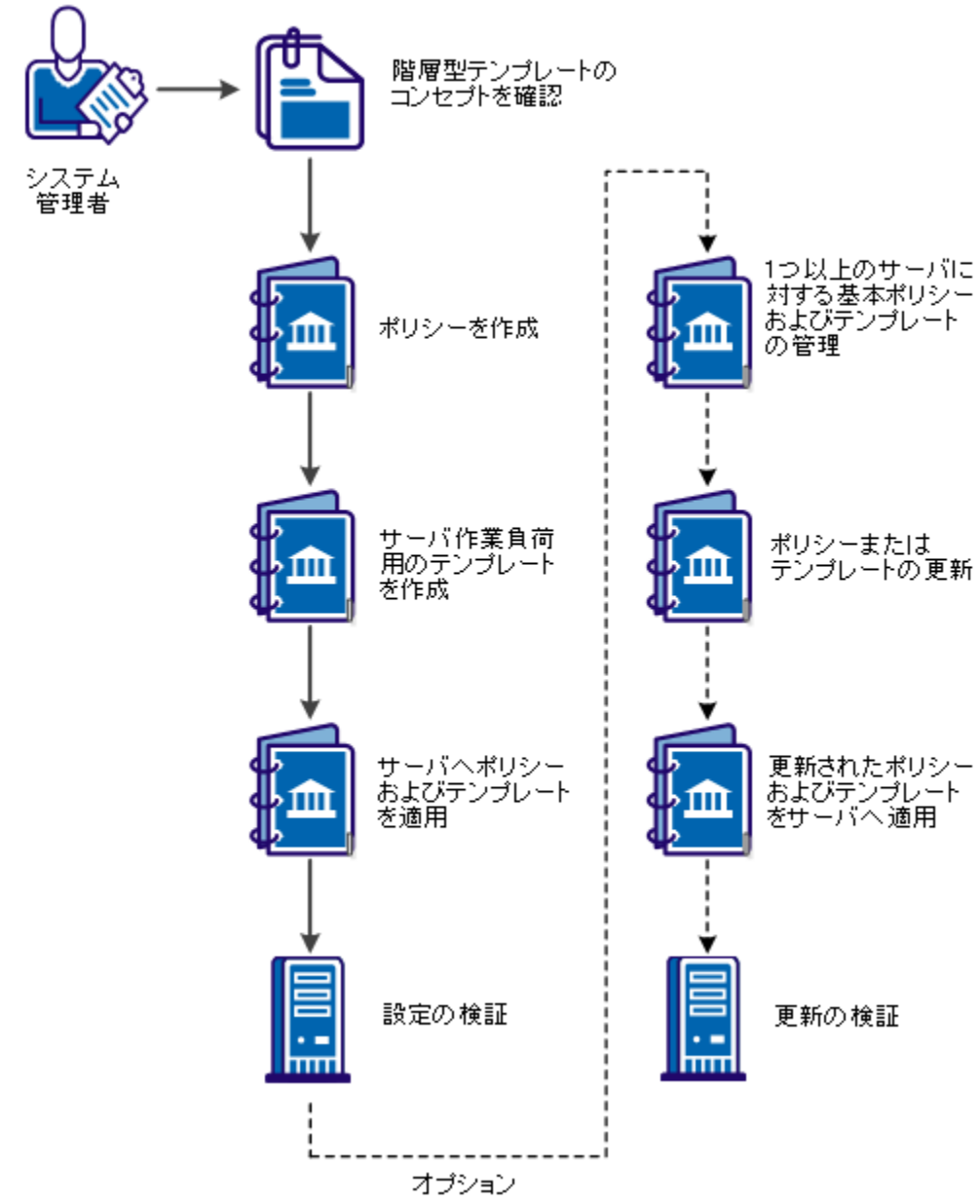
標準以外のポリシーを持つマシン

適用されたポリシーに対する標準以外の変更が含まれるシステムが表示されます。

ポリシーおよび階層型テンプレートをサーバに適用する方法

ベース ポリシーを作成し、そのポリシーにテンプレートを階層として追加することにより、CA Server Automation ユーザ インターフェースから SystemEDGE エージェント モニタリングを制御できます。 以下の図では、ベース ポリシーと階層型テンプレートの使用方法を示しています。

サーバへのポリシーおよび階層型テンプレートの適用



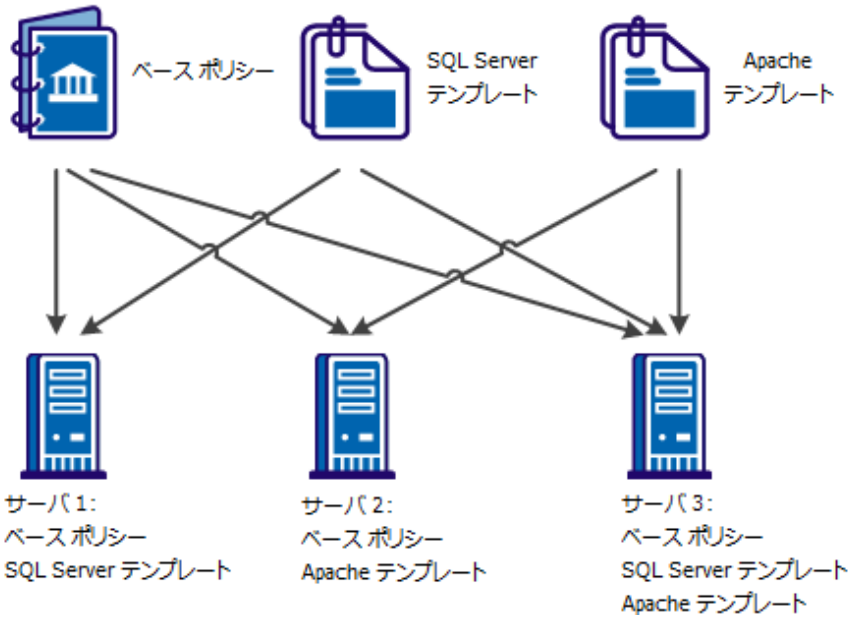
以下の手順に従います。

階層型テンプレートの概念 (P. 203)
ポリシーの作成 (P. 206)
サーバ ワークロード用のテンプレートの作成 (P. 220)
ポリシーとテンプレートのサーバへの適用と設定の確認 (P. 240)
（オプション）サーバのベース ポリシーおよびテンプレートの管理 (P. 242)
（オプション）ポリシーまたはテンプレートの更新 (P. 240)
（オプション）サーバへのポリシー/テンプレート更新の適用と更新の確認 (P. 244)

階層型テンプレートの概念

企業では、サーバまたはサーバ グループによって処理されるワークロードは異なります。 サーバまたはサーバ グループによって処理されるワークロードに固有の複数のポリシーを作成することができます。 ポリシーを容易に作成できるようにするために、テンプレートを使用してアプリケーション固有のモニタを作成します。 ベース ポリシーと階層型テンプレートが組み合わされて設定ファイルが形成され、モニタするサーバに適用されます。 階層型テンプレートは、追加または削除することができます。 テンプレート更新はサーバに直接適用できます。ベース ポリシーを変更したり、更新されたテンプレートをベース ポリシーに再インポートしたりする必要はありません。

例: ベース ポリシーおよびテンプレートをサーバに適用



階層型ポリシーは、以下のシナリオで使用できます。

異種アプリケーション

異なるセットのアプリケーションを実行するサーバごとにテンプレートのライブラリを作成します。各サーバにテンプレート更新を直接適用できます。

動的な環境

サーバの負荷は、動的な環境で頻繁に変化します。階層型テンプレートを使用して、モニタを論理グループに分離します。負荷の変化に基づいて、論理グループを直接システムに適用したり、システムから削除したりできます。

共有サーバ

企業セットアップでは、サーバは複数の部門間で共有されます。 各部門は共有サーバ上のアプリケーションを管理し、モニタします。 階層型テンプレートを使用することにより、テンプレートの個別の管理および各部門のシステムへの適用を行うことができます。

アプリケーションの保守

モニタリングは複数のテンプレートに分割できます。 サーバでは、使用していないアプリケーションのテンプレートを削除でき、システムの他の部分のモニタリングに影響することもありません。

すぐに使用できるテンプレート

すぐに使用できるテンプレートを管理対象ノードに適用できます。 管理対象ノードに対するテンプレート設定を使用してポリシーを設定します。テンプレートは以下のオペレーティング システムに利用可能です。

すべてのオペレーティング システム用:

- CPU Utilization - Autowatch
- Swap Capacity

Windows の場合:

- App Monitoring - CA eTrust Antivirus
- Process Crash
- System Errors
- System Processes
- User Activity
- Windows Services - Autowatch

UNIX（AIX、HPUnix、Linux、Solaris）:

- System Messages
- System Processes
- User Activity

ポリシーの作成

エージェントのモニタリングを制御するため、モニタ、MIB 拡張、トラップ & コミュニティ、および制御設定のセットを定義するベース ポリシーを作成します。

トラップ & コミュニティと制御設定の中の共通設定はポリシーのみに利用可能です。 階層型テンプレート を使用する場合、共通設定はベース ポリシー内に指定されます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規 SystemEDGE ポリシー］ダイアログ ボックスが表示されます。

3. ポリシーの名前と任意の説明、システム タイプ、および既存のポリシーをベースにするかどうかを入力し、［OK］をクリックします。

   ポリシーが作成され、右側のペインに設定画面が表示されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが作成および保存されます。

注: 必要に応じて、既存のデフォルト ポリシーをベース ポリシーとして使用することができます。

関連項目:

SystemEDGE ポリシーのコピー (P. 264)
SystemEDGE ポリシーの名前変更 (P. 265)
SystemEDGE ポリシーの削除 (P. 265)

SystemEDGE ポリシー制御設定の定義

SystemEDGE ポリシー コントロール設定を使用して、以下のエージェント動作を制御できます。

- セキュリティ設定
- SNMP の設定
- MIB テーブルへのデータのロード
- UNIX の設定
- パフォーマンス モニタリングの設定

これらの共通コントロール設定は、ベース ポリシーに追加することで特定のサーバ ワークロード設定から分離することができます。

ポリシーに定義されたコントロール設定は、この設定でモニタするすべてのシステムに適用することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［制御設定］をクリックします。

   ［コントロール］ページが表示されます。

4. （オプション）［デフォルトを使用］をクリックします。

   デフォルトの選択ペインが表示されます。デフォルトの設定を変更できます。

5. 以下の制御設定を行います。

SNMP

以下の基本的な SNMP プロパティを定義できます。

バインド アドレス

エージェントがバインドし、受信 SNMP リクエストをリスンするインターフェースを指定します。 有効なアドレスは IPv4 または IPv6 のアドレスです。

注: 対応するデフォルトのポートはインストール中に指定します。

バインド ポート

SNMP トラップを送信するために、エージェントがバインドするトラップ ポートを指定します。bind_address が指定されていない場合、エージェントは利用可能なすべての UDP アドレスにバインドします。

デフォルト： システムによって選択されたポート

IP ファミリ

エージェントの通信方法（IPv4 のみ、IPv6 のみ、またはその両方）を指定します。 デフォルトでは、エージェントは、IPv4、IPv6 の順に使用を試行します。

FIPS モード

FIPS 準拠の暗号化を使用するように、エージェントを指定します。 CA eTrust 公開鍵インフラストラクチャ ライブラリを有効にするには、［非 FIPS モード］を選択します。この方法が失敗する場合は、内部の最低限のセキュリティ ソリューションにフォールバックします。 FIPS 準拠の暗号化を有効にするには、［FIPS 共存モード］を選択します。この方法が失敗する場合は、CA eTrust 公開鍵インフラストラクチャ ライブラリにフォールバックします。これらが失敗した場合は、［FIPS のみのモード］を選択して、RSA BSAFE Crypto-C Micro Edition FIPS 準拠ライブラリを有効にし、暗号化を実行しません。

デフォルト： 非 FIPS モード

トラップ ソース

トラップを送信するために使用されるソース アドレスを指定します。 有効なアドレスは IPv4 アドレス、IPv6 アドレス、またはホスト名です。

デフォルト： エージェントのホスト名

セキュリティ設定

以下のセキュリティ基本設定を定義できます。

認証トラップ

エージェントが認識できないという、コミュニティ名を備えた SNMP メッセージをエージェントが受信した場合に、認証失敗トラップを送信します。

デフォルト： 無効

プロセス セット

プロセス テーブルおよび Running Software テーブルで、エージェント システム上で実行されているプロセスや他のソフトウェアにアクセスできます。これらのテーブルで SNMP セットを許可すると、セキュリティの問題が発生する場合があります。

リモート シェル グループ

管理システムは、リモート シェル グループを使用して、エージェント システム上でシェル スクリプトおよびプログラムを実行するようにエージェントに対してリモートから指示できます。 このタイプの情報が漏えいすると、潜在的なセキュリティ リスクが発生する可能性があります。

実行アクション

しきい値違反が発生したときに、モニタリング テーブルを使用したアクション コマンドの実行を有効にします。 アクション コマンドおよびスクリプトを実行する機能が原因で、セキュリティ上の問題が発生する可能性があります。

MIB テーブルへのデータのロード

システム管理 MIB の以下のテーブルに入力します。

- プロセス テーブル
- ユーザ グループ テーブル
- Who テーブル
- トラップ コミュニティ テーブル
- ミラー テーブルのモニタ
- ミラー テーブルを集計
- トップ プロセス テーブル

各テーブルには、MIB で公開可能な機密情報か、ディスク領域を節約するために無効にできる重要でない情報のいずれかが含まれています。 デフォルト設定では、プロセス テーブルを除くすべてのテーブルにデータをロードできます。

その他

以下のその他の設定を定義できます。

SNMP を使用してエージェントが更新されるのを許可

SNMP SET を使用したエージェントの更新を許可します（書き込みコミュニティの削除など）。 エージェント上で SNMP SET を許可すると、この方式でのあらゆる更新において、SNMP SET 変更の通知が送信されます。 また、これらの更新により、システムのポリシー詳細の表示時に例外が発生します。

マネージャに設定の更新を通知

エージェントが処理する SNMP 設定リクエストすべてについて、エージェントによるマネージャへの通知送信を可能にします。

ウォーム スタートのディスカバリ

ウォーム スタート設定が更新されるたびに、すべてのデバイスでエージェントが再検出されます。デバイスが多数あるシステムを管理している場合、ウォーム スタートのたびにディスカバリが実行されると、非常に多くの時間とリソースを消費する場合があります。

Perl 互換正規表現を使用

Perl 互換正規表現（PCRE）を使用すると、正規表現をサポートするモニタを定義するときに i18n 互換の正規表現を指定できます。 正規表現の例には、ログ ファイル、プロセス、プロセス グループ、Windows サービスおよび Windows イベントがあります。また、このオプションを使用して、より複雑な正規表現を作成できます。 このオプションは、SystemEDGE エージェント 5.1.0 以降のバージョンで提供されています。

インデックスの競合を自動的に解決する

インデックスの競合を解決できるようにします。すべてのシステムに階層型テンプレートを適用するとき、インデックスはテンプレート内に追加されたモニタに割り当てられます。割り当てられたインデックスがベース ポリシーまたは別のテンプレート内の既存のインデックスと競合する場合、このオプションは一意のインデックス値を再割り当てします。

注: ベース ポリシー内に含まれるインデックスは、配信された設定で常に維持されます。 このオプションが無効な場合、競合するインデックスを解決できません。ただし、システムに階層型テンプレートを適用するとき、競合するインデックスは、競合するインデックスが発生した階層型テンプレート上にエラーとして表示されます。

履歴パフォーマンス モニタリング

パフォーマンス キューブ AIM に対して以下の設定を定義できます。パフォーマンス キューブ AIM では、履歴パフォーマンスを管理するための履歴情報を Systems Performance キューブに収集します。

収集間隔

履歴テーブルからパフォーマンス キューブに情報を収集する頻度を指定します。

インデックス範囲の開始

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンス キューブ データを収集するための履歴コントロール エントリを作成します。 この予約済み範囲は、SRM （サービス レスポンス モニタリング) がパフォーマンス データを収集するよう設定されている場合などに使用されます。

インデックス範囲の終了

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンス キューブ データを収集するための履歴コントロール エントリを作成します。 この予約済み範囲は、SRM （サービス レスポンス モニタリング) がパフォーマンス データを収集するよう設定されている場合などに使用されます。

UNIX 制御設定

UNIX システム上で実行されるエージェントに対して、以下の設定を定義できます。

サブプログラム グループ

サブプログラムを実行するルート以外のグループ名を指定します。

サブプログラム ユーザ

サブプログラムを実行するルート以外のユーザ名を指定します。

Linux Freemem を含む

空きメモリの計算に、システム バッファ、ディスク キャッシュ メモリ、またはその両方を含めるかどうかを指定します。

システム デバイスのクエリ

以下のシステム デバイス メトリックのクエリを有効にできます。

- シリアル デバイス ステータス
- フロッピー ディスク ステータス
- ディスク サイズ、容量、説明、およびその他のプロパティ (ディスクのプローブ)
- NFS ファイル システム ステータス
- HP-UX グラフィックス ステータス

これらのメトリックに対してクエリを実行すると、潜在的なエージェント ブロックに関する問題が発生する可能性があります。 デフォルト設定では、シリアル デバイス ステータスおよび NFS ファイル システム ステータスに対するクエリのみが有効になっています。

6. ［プラグイン］をクリックします。

［プラグイン］ペインが表示されます。 このペインで、エージェントを使用してロードする AIM を指定します。

7. 以下のいずれかを実行します。
   - ［利用可能なすべてのプラグインをロードします］を選択して、エージェント システムで利用可能なすべての AIM をロードします。
   - ［テーブルで選択されたプラグインをロードします］を選択します。
   - ［外部プラグイン］ツールバーの［+］（新規）をクリックし、外部プラグイン テーブルに AIM を追加します。

注: 利用可能な AIM の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

AIM ロードが設定されます。

8. ［モニタを集計］をクリックします。

「オブジェクト集計の設定 (P. 214)」の説明に従って、モニタの集計を設定します。

制御設定が定義されます。

9. ［ポリシーの保存］をクリックします。

ポリシーが保存されます。

関連項目:

オブジェクト集計の設定 (P. 274)

オブジェクト集計の設定

デフォルトでは、SystemEDGE がモニタを集計し、オブジェクト クラス、インスタンス、および属性プロパティに同じ値を含む管理対象オブジェクトを生成します。 たとえば、SysHealth のクラス、CPU のインスタンス、および SysTime の属性を備えたすべてのモニタが組み合わせられ、集計管理対象オブジェクトとなります。

SystemEDGE ポリシーを定義するときに、より高いレベルでオブジェクトを集計するよう、エージェントを設定できます。 また、オブジェクト集計および状態管理モデルに関連するエージェント動作の他の側面も設定できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［制御設定］をクリックします。

   ［コントロール］ページが表示されます。

4. ［モニタを集計］をクリックします。

   ［モニタを集計］ページが表示されます。

5. 集計レベルを指定するチェック ボックスを 1 つ以上、オンにします。

   これらはデフォルトより高い集計レベルを表し、最も高いレベルでは 1 つの最上位エージェント オブジェクトにすべてのモニタを集計できます。 集計レベルを指定すると、指定したレベルまでステータスをプロパゲートする層構造のオブジェクト アーキテクチャを作成できます。

6. 以下の追加設定を設定して、［ポリシーの保存］をクリックします。

   すべての集計済みモニタのレガシートラップを送信します。

   管理対象オブジェクトを形成するすべてのモニタのレガシー トラップを送信するかどうかを指定します。 デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタの状態変更トラップを送信するのみです。

   すべての集計済みモニタのコマンドを実行します。

   管理対象オブジェクトを形成するすべてのモニタのアクション コマンドを実行するかどうかを指定します。 デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタのアクション コマンドを実行するのみです。

   集計設定が設定されます。 変更を有効にするには、ポリシーを適用または再適用します。

関連項目:

SystemEDGE ポリシー制御設定の定義 (P. 267)

トラップとコミュニティの定義

SNMP 設定では、エージェントが使用するコミュニティ、およびエージェントがトラップを送信する宛先を定義します。

次の手順に従ってください：

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［トラップ & コミュニティ］タブをクリックします。

   ［コミュニティ］ページが表示されます。

4. 以下のいずれかを選択して［アクション］をクリックし、［適用］を選択します。
   - サーバ固有 SNMP 設定のみを含める
   - サーバ固有 SNMP 設定およびすべてのデフォルト設定を含める
   - ［サーバ固有 SNMP 設定および選択されたデフォルト設定を含める］を選択します。

［SNMP 設定］が更新され、［コミュニティ］テーブル内のコミュニティ ページに以下が表示されます。

名前

コミュニティ文字列の名前を指定します。

ポート

SNMP のポートを指定します。

SNMP バージョン

コミュニティが使用する SNMP バージョンを指定します。

アクセス権

コミュニティが、読み書きまたは読み取り専用のいずれの権限を持つかを指定します。

注: 少なくとも 1 つの読み取り専用コミュニティと、1 つの読み書きコミュニティを追加してください。

コミュニティ/ユーザ

コミュニティ名を指定します。

認証プロトコル

SNMPv3 データを認証するプロトコルを指定します。

プライバシー プロトコル

SNMPv3 データを認証するプロトコルを指定します。

アクセス制御リスト

IP アドレスのスペース区切りリストを指定して、コミュニティの使用をこれらのアドレスのみに制限します。 リストを空にしておくと、エージェントは、関連付けられたコミュニティ名を使用するあらゆるシステムに対してアクセス権を付与します。 アクセス リストは、SNMPv1 を使用するコミュニティについてのみ有効です。

注: SNMPv2c および SNMPv3 のアクセス リストの定義の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

5. （オプション）必要に応じて、他のコミュニティを追加、更新、または削除します。
6. ［ポリシーの保存］をクリックします。

ポリシーが保存されます。

7. ［トラップ先］をクリックします。

   ［トラップ先］ページが表示されます。

8. 以下のコントロールを使用して、トラップ先を定義し、［追加］をクリックします。

   トラップ タイプ

   SNMP バージョンに応じて、送信するトラップのタイプを指定します。

   デスティネーション

   トラップを送信する IPv4 アドレスまたは IPv6 アドレスを指定します。

   ポート

   トラップを送信する UDP ポートを指定します。

   コミュニティ

   トラップで送信されるコミュニティ名を指定します。

エンコーディング

（オプション）トラップ内の［制御設定］ペインの［トラップ ソース］フィールドで定義したソース アドレスを含める方法を指定します。このパラメータはトラップ ソースが IPv6 アドレスに変換される場合に重要です。3 桁の XYZ の形式（先頭の未使用桁をゼロで埋める）でエンコーディング パラメータを入力します。

デフォルト： 000

X

4 バイトの IPv4 ソース アドレス フィールド（SNMPv1 トラップのみ）の拡張を制御します。 16 バイトの IPv6 アドレスを含めるのに、ソース アドレス フィールドを拡張しない場合は 0 を入力し、ソース アドレス フィールドを拡張する場合は 1 を入力します。

Y、Z

トラップの varbind （Y）または UDP パケット（Z、SNMPv1 トラップのみ）にソース情報を含めるかどうかを制御します。これらの桁に以下のいずれかを入力します。

0： トラップの varbind または外部 UDP パケットは変更されません。

1： varbind またはパケットに trap_source パラメータ（IPv4/IPv6 アドレスまたはホスト名）をそのまま含めます。

2： trap_source パラメータを、可能であれば IPv4 アドレスとして（続いて IPv6 アドレス、ホスト名の順に試行）含めます。

3： trap_source パラメータを、可能であれば IPv6 アドレスとして（続いて IPv4 アドレス、ホスト名の順に試行）含めます。

4：trap_source パラメータを、可能であればホスト名として（続いて IPv4、IPv6 の順に試行）含めます。

5： 2 の優先順位に従い、ホスト名を含めます。

6： 3 の優先順位に従い、ホスト名を含めます。

7： 1 の優先順位に従い、ホスト名を含めます（trap_source が IPv6 アドレスの場合）。

トラップ ソース

（オプション）トラップ ソースとして使用する IPv4 アドレス、IPv6 アドレス、またはホスト名を指定します。

デフォルト： グローバル トラップ

トラップ先が［定義済みトラップ先］テーブルに表示されます。

9. （オプション）必要に応じて、他のトラップ先を追加、更新、または削除します。
10. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

サーバ ワークロード用のテンプレートの作成

サーバのワークロードに固有のテンプレートを作成します。モニタと MIB 拡張を指定できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［テンプレート リスト］ページが表示されます。
2. ［テンプレート リスト］ツールバーの［+］（新規）をクリックします。

   ［新規 SystemEDGE モニタリング テンプレート］ダイアログ ボックスが表示されます。
3. テンプレートの名前と説明（説明はオプションです）、システム タイプ、および既存のテンプレートをベースにするかどうかを入力し、［OK］をクリックします。

   テンプレートが作成され、［サマリ］ページが表示されます。
4. テンプレートは、モニタおよび MIB 拡張のコレクションです。テンプレートにモニタを追加する方法については、「テンプレートまたはポリシーへのモニタの追加 (P. 221)」を参照してください。テンプレートに MIB 拡張を追加するには、「MIB 拡張の定義 (P. 235)」を参照してください。

5. ［テンプレートの保存］をクリックします。

   テンプレートが作成および保存されます。

テンプレートまたはポリシーへのモニタの追加

サーバまたはサーバ グループによって処理されるワークロードに固有のテンプレートに、モニタを追加します。 以下の手順は、ポリシーへのモニタの追加の場合と似ています。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］をクリックし、追加するモニタを選択します。

   モニタを作成するために、以下のモニタに対するしきい値と重大度の値を指定する設定を定義します。

   - しきい値モニタの作成 (P. 222)
   - プロセス モニタの作成 (P. 225)
   - ログ ファイル モニタの作成 (P. 227)
   - Windows イベント モニタの作成 (P. 229)
   - 履歴モニタの作成 (P. 231)
   - プロセス グループ モニタの作成 (P. 233)

4. （オプション）追加するモニタごとに同じ手順を繰り返します。
5. ［保存］をクリックします。

   モニタがポリシーまたはテンプレートにロードされます。

関連項目:

しきい値モニタの定義 (P. 286)
プロセス モニタの定義 (P. 289)
ログ ファイル モニタの定義 (P. 291)
Windows イベント モニタの定義 (P. 293)
履歴モニタの定義 (P. 295)
プロセス グループ モニタの定義 (P. 297)

しきい値モニタの作成

エージェントが、指定したしきい値に対して、サーバまたはサーバ グループをモニタすることを可能にするしきい値モニタを作成します。 しきい値違反が発生すると、エージェントがトラップを送信します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［しきい値］をクリックします。

   ［しきい値モニタ］ページが表示されます。

5. ［しきい値モニタ］ツールバーの［+］（新規）をクリックします。

   ［しきい値モニタの詳細: 新規］ペインが表示されます。

6. 以下のしきい値設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス

モニタするオブジェクト クラスを指定します。 値は利用可能な MIB テーブルを参照します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を定義します。 値は任意の文字列（たとえば FileSystems）です。

オブジェクト属性

モニタするオブジェクト属性を指定します。 値は、オブジェクト クラスとして選択されたテーブルの利用可能な属性を参照します。 属性（たとえば devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）は、このしきい値モニタでモニタする MIB オブジェクト（OID）の初期部分を指定します。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を定義します。 これは任意の文字列です（PercentUsed など）。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。 この値、たとえば、デバイス テーブル（devTable）内の 3 番目の行をモニタするための .3 は、このしきい値モニタでモニタする MIB オブジェクト（OID）のインデックス部分を指定します。 いくつかのオブジェクト クラスについては、インスタンス自体の名前を指定できます（たとえば .3 の代わりに C：、または UNIX マシンで /var）。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を定義します。 値は任意の文字列（たとえば SysVol_C）です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

［しきい値設定］ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. ［保存］をクリックします。

［しきい値モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

しきい値モニタがテンプレートにロードされます。

プロセス モニタの作成

エージェントが、指定したしきい値に対してプロセス、サービス、またはプロセス テーブル オブジェクトをモニタできるようにするプロセス モニタを作成します。 しきい値違反が発生するか、プロセスの状態（実行中または停止中）が変化すると、エージェントはトラップを送信します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. プロセスをクリックします。

   ［プロセス モニタ］ページが表示されます。

5. ［プロセス モニタ］ツールバーの［+］（新規）をクリックします。

   ［プロセス モニタの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を指定します。 値は任意の文字列（たとえば Process）です。

オブジェクト属性

モニタするオブジェクト属性を指定します。 値は、プロセス モニタリングで利用できる属性を定義します。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を定義します。 値は任意の文字列（たとえば MemUsedPercent）です。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。 これは、名前による一致処理、、または名前による Windows サービスの一致処理に使用される正規表現（オプションの設定に依存します）です。 パターンは一意に単一のプロセス（サービス）と一致する必要があります。 引数を含むことができます（オプション設定を参照してください）。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を指定します。 値は任意の文字列（たとえば ApacheServer）です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

［しきい値設定］ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. ［保存］をクリックします。

   ［プロセス モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

プロセス モニタがポリシーにロードされます。

ログ ファイル モニタの作成

エージェントがすべての UTF-8 エンコードされたシステムまたはアプリケーションのログ ファイルを、正規表現として指定されている文字列を検索することによってモニタできるようにする、ログ ファイル モニタを作成します。 一致する行が見つかると、エージェントがトラップを送信します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［ログ ファイル］をクリックします。

   ［ログ ファイル モニタ］ページが表示されます。

5. ［ログ ファイル モニタ］ツールバーの［+］（新規）をクリックします。

   ［ログ ファイルの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   モニタ タイプ

   使用するモニタ タイプを指定します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   ログ ファイル/ディレクトリ名

   モニタするファイルまたはディレクトリのパスを定義します。

   検索フィルタ

   検索フィルタを指定します。

   間隔

   モニタ評価間隔を分単位で定義します。

   重大度

   一致したときのモニタの重要度を指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時刻

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時刻

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. ［保存］をクリックします。

   ［ログ ファイル モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

ログ ファイル モニタがポリシーにロードされます。

Windows イベント モニタの作成

エージェントが別のフィルタ（イベント ソース）を使用して、Windows イベント ログ エントリをモニタできるようにする Windows イベント モニタを作成します。 一致する行が見つかると、エージェントがトラップを送信します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［Windows イベント］をクリックします。

   ［Windows イベント モニタ］ページが表示されます。

5. ［Windows イベント モニタ］ツールバーの［+］（新規）をクリックします。

   ［Windows イベントの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   イベント ログ

   読み取るイベント ログを指定します。

   イベント タイプ

   モニタするイベント タイプを指定します。

   ソース フィルタ

   使用するソース フィルタを定義します。

   説明フィルタ

   使用する説明フィルタを定義します。

   重大度

   一致したときのモニタの重要度を指定します。

［保守ウィンドウ］サブタブで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. ［保存］をクリックします。

   ［Windows イベント モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

Windows イベント モニタがポリシーにロードされます。

履歴モニタの作成

エージェントがマネージャ側ベースラインおよび傾向分析用の履歴データを収集できるようにする履歴モニタを作成します。 エージェントはメトリックを使用して、特定の期間中の平均システム パフォーマンスの図を提供します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［履歴］をクリックします。

   ［履歴モニタ］ページが表示されます。

5. ［履歴モニタ］ツールバーの［+］（新規）をクリックします。

   ［履歴詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   オブジェクト クラス

   モニタするオブジェクトを指定します。 値は利用可能な MIB テーブル値を参照します。

   オブジェクト属性

   モニタするオブジェクト属性を指定します。 値は、オブジェクト クラスとして選択されたテーブルの利用可能な属性を参照します。属性（たとえば devCapacity=1.3.6.1.4.1.546.1.1.1.7.1.14）は、この履歴エントリを使用してモニタするための MIB オブジェクト（OID）の初期部分を指定します。

   オブジェクト インスタンス

   モニタするオブジェクト インスタンスを定義します。 この値（たとえば、0.3 はデバイス テーブル（devTable）の 3 行目をモニタします）は、この履歴エントリでモニタする MIB オブジェクトのインデックス部分（OID）を指定します。

   間隔

   収集間隔を 30 秒の倍数で定義します。

   バケット

   収集するサンプル数を定義します。

   ［パフォーマンス キューブに追加］チェック ボックス

   このエントリのパフォーマンス キューブ データを収集するかどうかを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時刻

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時刻

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

7. ［保存］をクリックします。

   ［履歴モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

履歴モニタがポリシーにロードされます。

プロセス グループ モニタの作成

エージェントがプロセスのグループを定義し、そのグループの変更をモニタできるようにするプロセス グループ モニタを定義します。プロセス グループが変化すると、エージェントはトラップを送信します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］および適切なサブカテゴリを展開します。

   ［テンプレート リスト］ページが表示されます。

2. ［テンプレート リスト］内のテンプレートを選択します。

   テンプレートの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［プロセス グループ］をクリックします。

   ［履歴モニタ］ページが表示されます。

5. ［プロセス グループ モニタ］ツールバーの［+］（新規）をクリックします。

   ［プロセス グループ詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   プロセス名

   プロセス名を定義します。 これは、名前による一致処理、に使用される正規表現（オプションの設定に依存します）です。

   間隔

   モニタの評価間隔を 30 秒の倍数で定義します。

   ユーザ名

   任意のプロセス名正規表現に加えて、モニタするユーザ名を定義します。

   グループ名

   任意のプロセス名正規表現に加えて、モニタするグループ名を定義します。

   重大度

   グループ変更に関する、モニタの重要性を指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

7. ［保存］をクリックします。

   ［プロセス グループ モニタ］設定が保存されます。

8. ［テンプレートの保存］をクリックします。

プロセス グループ モニタがポリシーにロードされます。

MIB 拡張の定義

MIB 拡張を定義すると、ローカル ファイル操作では利用できない機能が利用できるようになります。 ポリシー設定機能により、フィールド名、および、オブジェクト タイプなどのキー プロパティのリストが提供されます。

ポリシーまたはモニタリング テンプレートを設定する場合に［MIB 拡張］タブをクリックすると、以下のオブジェクトが追加できます。

- MIB 拡張
- Windows パフォーマンス
- Windows レジストリ

注: テンプレートまたはポリシーに MIB 拡張を追加するには、「テンプレートまたはポリシーへの MIB 拡張の追加 (P. 236)」を参照します。 テンプレート内の MIB 拡張は、モニタされたシステムに MIB 拡張を直接適用することを目的としてサポートされています。 ポリシー内で使用するための MIB 拡張は、ポリシー内に直接作成する必要があります。

テンプレートまたはポリシーへの MIB 拡張の追加

ポリシー設定機能を使用して、テンプレートまたはポリシー用の MIB 拡張を定義します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］または［ポリシー］を展開します。
2. ［テンプレート リスト］または［利用可能ポリシー］ページから、テンプレートまたはポリシーの名前をクリックします。

   ［サマリ］ページが表示されます。
3. ［MIB 拡張］タブをクリックします。

   ［MIB 拡張］ページが表示されます。
4. 以下のコントロールを使用して、MIB 拡張属性を定義し、［追加］をクリックします。

   インデックス

   属性リーフ番号を定義します。

   タイプ

   属性タイプを指定します。

   拡張コマンド

   実行するスクリプトまたはバイナリのフル パスまたは名前（パラメータを含む）を定義します。

   アクセス権

   属性アクセス権限を指定します。
5. ［Windows パフォーマンス］タブをクリックします。

   ［Windows パフォーマンス］ペインが表示されます。
6. 以下のコントロールを使用して、Windows パフォーマンス属性を定義し、［追加］をクリックします。

   インデックス

   属性リーフ番号を定義します。

   タイプ

   属性タイプを指定します。

オブジェクト

パフォーマンス レジストリ オブジェクトを指定します。

カウンタ

パフォーマンス レジストリ カウンタを指定します。

インスタンス

パフォーマンス レジストリ インスタンスを定義します。

7. ［Windows レジストリ］タブをクリックします。

［Windows レジストリ］ペインが表示されます。

8. 以下のコントロールを使用して、Windows レジストリ属性を定義し、［追加］をクリックします。

インデックス

属性リーフ番号を定義します。

タイプ

属性タイプを指定します。

キー

HKEY_LOCAL_MACHINE にレジストリ キーを定義します。

値

属性値を定義します。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

9. ［テンプレートまたはポリシーの保存］または Policy をクリックします。

設定が保存されます。

(オプション)テンプレートまたはポリシーからのモニタのインデックス再作成

［しきい値］、［プロセス］、［ログ ファイル］、［Windows イベント］、［履歴］、および［プロセス グループ］タブのモニタには、インデックスを再作成することができます。 インデックスの再作成によって、既存のインデックスに連続する値が割り当てられます。

注: モニタにインデックスを再作成すると、将来のインデックスが次の論理的なベース インデックスから開始されるようになります。

モニタにインデックスを再作成するには、以下を考慮します。

- モニタが存在することを確認します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］または［ポリシー］を展開します。
2. ［テンプレート リスト］または［利用可能ポリシー］ページから、テンプレートまたはポリシーの名前をクリックします。

   ［サマリ］ページが表示されます。
3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、モニタのリストが表示されます。

4. 適切なモニタ タブをクリックし、［アクション］をクリックして、［再インデックス付け］を選択します。

   新しいベース インデックスのダイアログ ボックスが表示されます。

5. ベース インデックスとして数値を入力します。

   例： 1000

6. ［インデックスを連続させます］を選択します。

   ［インデックスを連続させます］

   ［インデックスを連続させます］オプションを選択して、既存のインデックスが連続するようにします。

   例： 1001、1002、1003、1004 など。

   注: このオプションを選択しないと、インデックス間の欠番は保持されます。

   例： 1001、1010、1020、1030 など。

7. ［OK］をクリックしてインデックスの再作成を確定します。

   モニタにインデックスが再作成されます。

テンプレートまたはポリシーからのモニタの削除

テンプレートまたはポリシーからモニタを削除することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］または［ポリシー］を展開します。
2. ［テンプレート リスト］または［利用可能ポリシー］ページから、テンプレートまたはポリシーの名前をクリックします。

   ［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. 適切なモニタ タブをクリックし、削除するモニタを 1 つまたは複数選択します。
5. ［アクション］をクリックし、［削除］を選択します。

   警告メッセージが表示されます。

6. ［OK］をクリックして削除を確定します。
7. （オプション）追加するモニタごとに同じ手順を繰り返します。
8. ［ポリシーの保存］をクリックします。

   モニタがポリシーから削除されます。

   注: サーバまたはサーバ グループによって使用されているテンプレート、またはテンプレートを持つポリシーは、削除できません。

（オプション）ポリシーまたはテンプレートの更新

必要に応じて、ポリシーやテンプレートに対してモニタを追加または削除し、ポリシーやテンプレートを更新することができます。 更新手順は作成プロセスに似ています。

次の手順に従ってください：

1. サーバ ワークロードに固有のモニタを追加するか削除します。テンプレートまたはポリシーにモニタを追加する方法については、「テンプレートまたはポリシーへのモニタの追加 (P. 221)」を参照してください。 ポリシーからモニタを削除するには、「テンプレートまたはポリシーからのモニタの削除 (P. 239)」を参照してください。
2. MIB 拡張を定義 (P. 235) します。
3. SystemEDGE ポリシー制御設定を定義 (P. 207) します。

   ポリシーまたはテンプレートが更新されます。

ポリシーとテンプレートのサーバへの適用と設定の確認

テンプレートを作成した後、企業全体のサーバまたはサーバ グループに、テンプレートを持つポリシーを直接適用できます。

次の手順に従ってください:

1. ［利用可能ポリシー］テーブル内のポリシーを選択するか、または［テンプレート リスト］からテンプレートを選択します。

   ポリシーまたはテンプレートの［サマリ］ページが表示されます。
2. ［管理対象マシン］タブを選択します。

   管理対象マシンのリストが表示されます。

3. ［アクション］をクリックし、［適用］を選択します。

   ポリシーを適用するシステムを選択するためのタブが表示されます。

   ［このポリシー/テンプレートを実行しているマシンを更新］

   すでにポリシーまたはテンプレートを実行しているシステムにポリシーを適用します。

   ［このポリシー/テンプレートを実行していないマシンに適用］

   システムにポリシーまたはテンプレートを適用します。

4. （ポリシーの場合のオプション）［このポリシーを実行しているマシンを更新］タブから、以下のいずれかを実行します。

   - 現在ポリシーを実行しているすべてのマシンにこのポリシーを展開するには、［このポリシーを使用してすべてのマシンを更新］を選択します。 このオプションは、グローバルに適用する設定ポリシーの変更を行った場合に便利です。
   - 以下の条件のいずれかを満たすマシンのみを更新するには、［選択したマシン グループを更新］を選択します。
     - ポリシーの期限切れバージョンを実行しているマシン
     - ポリシー例外が適用されているマシン
     - ポリシーの現在のバージョンを実行しているマシン
     - このポリシーに対して設定エラーがあるマシン

     ポリシー例外は、適用されるポリシー内で示されていないエージェントにユーザがポイント設定変更を適用すると発生します。
   - ［詳細（手動でマシンを選択）］を選択して、［マシンを選択］ペインにポリシーを再割り当てするマシンを手動で追加します。

5. （テンプレートの場合のオプション）［このテンプレートを実行しているマシンを更新］タブから、以下のいずれかを選択します。

   ［既存のマシン］で、以下のいずれかのオプションを選択します。

   - このテンプレートを適用してすべてのマシンを更新
   - このテンプレートの最新の変更が適用されていないマシンのみを更新
   - テンプレートが正常に適用されていないマシンのみを更新
   - 詳細（手動でマシンを選択）
   - マシンからこのテンプレートを削除

6. （オプション）［このポリシー/テンプレートを実行していないマシンに適用］タブから、ポリシーまたはテンプレートを適用するシステムを選択します。
7. ［ポリシーの適用］または［テンプレートの適用］をクリックします。

   適用が開始されます。
8. サーバが予期したように動作するかどうかを確認します。必要な場合、更新されたポリシーとテンプレートを更新および適用できます。

（オプション）サーバのベース ポリシーおよびテンプレートの管理

1 つまたは複数のサーバ用のテンプレートおよびベース ポリシーを管理します。現在のベース ポリシーの置換、テンプレートの追加、テンプレートの削除などを実行できます。

次の手順に従ってください:

1. ［リソース］タブをクリックし、［エクスプローラ］ペインを開き、ポリシー設定を変更するサーバを選択します。

   サーバの［リソース］ページが表示されます。
2. ［モニタリング ソフトウェア］-［ポリシー］を選択します。

   ポリシー、およびサーバに適用されているテンプレートのリストが表示されます。
3. このサーバの現在のベース ポリシーを別の使用可能なベース ポリシーで置き換えるには、  （ポリシーの変更）をクリックします。

   ［ポリシーの変更］ダイアログ ボックスが表示され、利用可能なベース ポリシーがすべて示されます。
4. 適切なポリシーを選択して［適用］をクリックします。

   選択されたサーバに新しいベース ポリシーが適用されました。 ポリシーのステータスは［配信が要求されました］から［配信］、［設定完了］に変更されます。

5. 選択されたサーバの設定に対してテンプレートを追加または削除するには、  （テンプレートの変更）をクリックします。

   ［テンプレートの変更］ダイアログ ボックスが表示され、利用可能なテンプレートが左ペインに、適用されているテンプレートが右ペインに示されます。

6. 追加または削除するテンプレートを選択し、矢印を使用して割り当てを行い、［適用］をクリックします。

   テンプレートの新しいセットが設定に適用されました。テンプレートのステータスは［配信が要求されました］から［配信］、［設定完了］に変更されます。

   新しい設定が適用されました。

複数のサーバをグループとして管理することもできます。

次の手順に従ってください:

1. サーバのグループを指定するサービスをデータセンター レベルで作成します。

   新しいサービスが［エクスプローラ］ペインに表示されます。

2. サービスを選択します。

   サービス ページが表示されます。

3. ［モニタリング ソフトウェア］-［ポリシー］を選択します。

   ポリシー、およびサーバに適用されているテンプレートのリストが表示されます。

   以降の手順は単一のサーバの場合と同じです。

4. 設定を完成します。

(オプション)ポリシーまたはテンプレートの更新

必要に応じて、ポリシーやテンプレートに対してモニタを追加または削除し、ポリシーやテンプレートを更新することができます。 更新手順は作成プロセスに似ています。

次の手順に従ってください：

1. サーバ ワークロードに固有のモニタを追加するか削除します。テンプレートまたはポリシーにモニタを追加する方法については、「テンプレートまたはポリシーへのモニタの追加 (P. 221)」を参照してください。 ポリシーからモニタを削除するには、「テンプレートまたはポリシーからのモニタの削除 (P. 239)」を参照してください。
2. MIB 拡張を定義 (P. 235) します。
3. SystemEDGE ポリシー制御設定を定義 (P. 207) します。

   ポリシーまたはテンプレートが更新されます。

(オプション)サーバへのポリシー/テンプレート更新の適用と更新の確認

テンプレートを更新した後、企業全体のサーバまたはサーバ グループにテンプレート更新を直接適用します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］を選択します。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。
2. テンプレート名を選択します。

   ［サマリ］ページが開き、テンプレート情報が示されます。
3. ［アクション］をクリックし、［適用］を選択します。

   モニタリング テンプレートを適用するマシンを選択するためのタブが表示されます。 ［このテンプレートを実行しているマシンを更新］タブでは、すでにテンプレートを使用しているマシンにモニタリング テンプレートを適用できます。 ［このテンプレートを実行していないマシンに適用］タブでは、テンプレートをまったく使用していないマシンにモニタリング テンプレートを適用できます。

4. （オプション）［既存のマシン］の下の［このテンプレートを実行しているマシンを更新］タブ オプションでマシンを選択します。
5. （オプション）［選択したマシン］の下で、テンプレートが再適用されるマシンを選択します。
6. （オプション）テンプレートを適用するマシンを［このテンプレートを実行していないマシンに適用］タブから選択します。
7. ［適用］をクリックします。

   テンプレート アプリケーションが起動され、［ステータスの表示］リンクが表示されます。
8. ［ステータスの表示］リンクをクリックして、SystemEDGE モニタリング テンプレート更新がサーバに適用されていることを確認します。

   SystemEDGE モニタリング テンプレート更新が適用されたサーバのリストを表示するページが開きます。

   階層型テンプレートの更新がサーバまたはサーバ グループに正常に適用されました。
9. サーバが予期したように動作するかどうかを確認します。 必要な場合、更新されたポリシーとテンプレートを再度更新および適用できます。

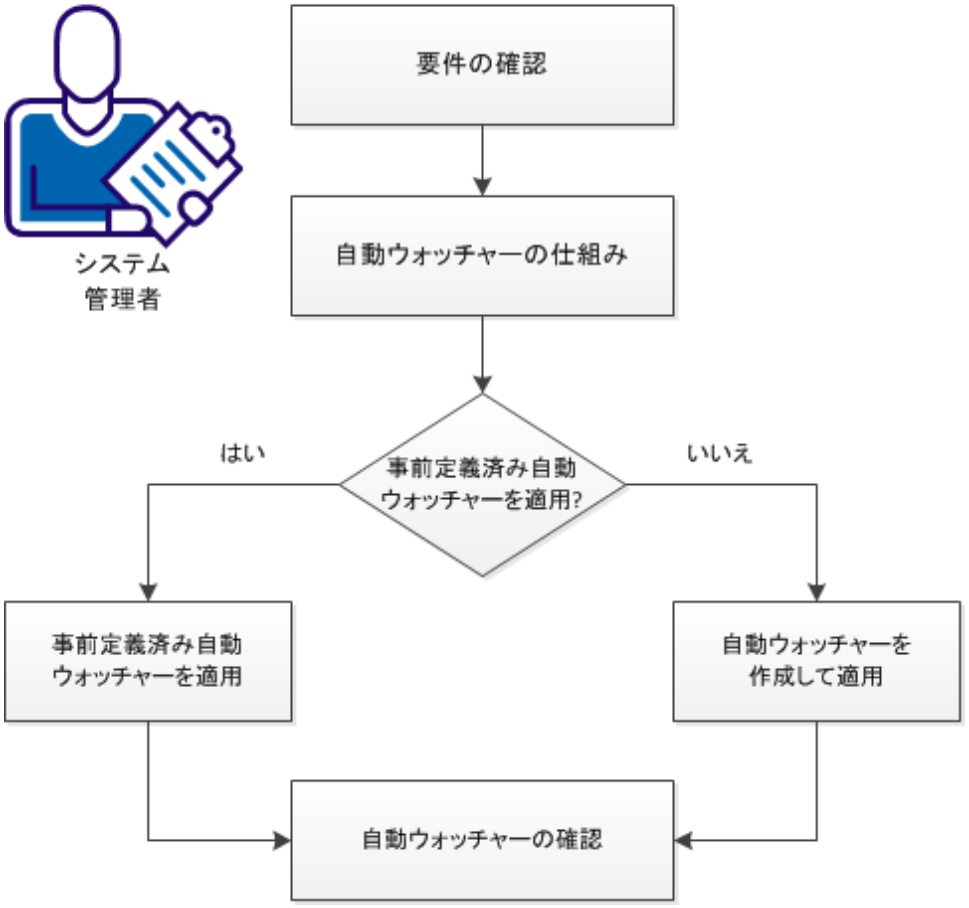
自動ウォッチャーを作成してシステムに適用する方法

このシナリオでは、システム管理者が自動ウォッチャーを使用して、管理対象システムのリソースを動的にモニタする方法について説明します。

管理対象システムに追加および削除されるリソースの検出に、自動ウォッチャーを使用できます。 リソースが追加される場合、自動ウォッチャーは対応するモニタを作成します。リソースが削除される場合、自動ウォッチャーは「消失アクション」を実行します。

以下の図は、管理対象システムに自動ウォッチャーを作成して適用する方法の概要を示しています。

自動ウォッチャーを作成してシステムに適用する方法



以下の手順に従います。

要件の確認

SystemEDGE 用の自動ウォッチャーを作成する前に、以下の要件を確認します。

- TCP/IP および SNMP に精通している。
- CA Server Automation および SystemEDGE に関する基礎知識がある。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 影響を受ける SystemEDGE エージェントが管理対象モードで実行されていることを確認する。

関連項目:

自動ウォッチャーの仕組み

自動ウォッチャーは、自動ウォッチャーがモニタを作成するリソースの名前に一致するパターンとして正規表現を使用して、定期的なディスカバリプロセスを実行します。 自動ウォッチャーを使用すると、新しいリソースがオンラインになるときに、これらに対するモニタを SystemEDGE で自動的に作成できます。 自動ウォッチャーは予約済みのインデックス範囲（1000000 ～ 1999999）でモニタを作成します。

リソースが非表示になるとき、SystemEDGE は CA Server Automation にトラップを送信し、自動ウォッチャーで設定した「消失アクション」を適用します。 モニタ対象のリソースが消失する場合には、「消失アクション」によってモニタを削除したり、リソースのステータスを以下の特定のステータスに設定したりすることができます。

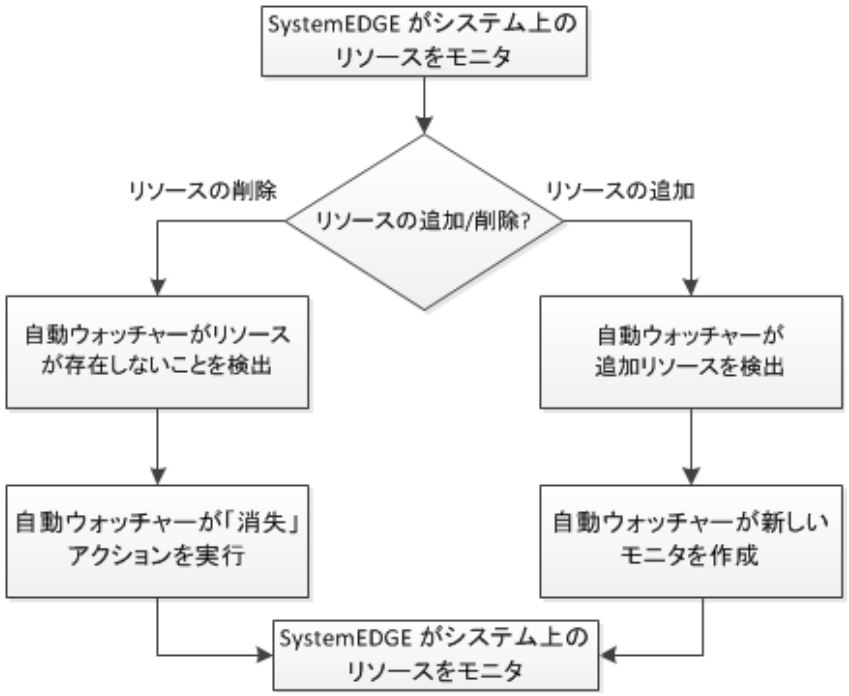
「OK」、「警告」、「マイナー」、「メジャー」、「重大」、「稼働中」、「ダウン」。

自動ウォッチャーを使用すると、管理対象システムに存在するリソースを知らなくても、柔軟にポリシーや階層型テンプレートを作成できます。リソースには、デバイス、サービス、管理対象システムで実行されるプロセスを指定できます。

使用できる自動ウォッチャーのタイプは以下のとおりです。

- 汎用自動ウォッチャー：デバイス、インターフェース、ファイルシステム、ファイルなど、管理対象システムのさまざまなリソース用のモニタを作成します。
- プロセスとサービスの自動ウォッチャー：管理対象システムで実行されるプロセスとサービス用のモニタを作成します。

自動ウォッチャーのプロセス ワークフロー



消失アクションを設定するときには、以下のガイドラインを使用できます。

- 消失するリソースがシステムの健全性に影響する場合は、対応するリソースのステータスを重大な状態に変更する消失アクションを設定できます。
- 消失するリソースがシステムの健全性に影響しない場合は、対応するモニタを削除する消失アクションを設定できます。

関連項目:

汎用自動ウォッチャー (P. 250)
プロセスとサービスの自動ウォッチャー (P. 250)

汎用自動ウォッチャー

汎用自動ウォッチャーでは、デバイス、インターフェース、ファイルシステム、ファイルなど、管理対象システムのさまざまなリソース用のモニタを作成できます。

汎用自動ウォッチャーの例としては、以下のものがあります。

- 検出されたすべてのデバイスの容量
- 検出されたすべてのディスクのディスク サービス時間
- すべての cmd プロセスの常駐セット サイズ
- すべてのトンネル ネットワーク インターフェースの稼働ステータス
- すべてのデバイスのデバイス ステータス

関連項目:

自動ウォッチャーの仕組み (P. 248)

プロセスとサービスの自動ウォッチャー

プロセスとサービスのモニタを動的に作成するには、プロセスとサービスの自動ウォッチャーを使用します。

サービス自動ウォッチャーは、自動ウォッチャーの条件（サービス名、開始タイプなど）にサービスが一致した場合に、プロセス テーブルに複数のサービス モニタを作成します。たとえば、インストールされている SQL サービスで開始タイプが「自動」であるものをすべてモニタできます。

プロセス自動ウォッチャーは、以下の 2 つの方法でプロセス モニタを作成します。

- プロセス名を使用（デフォルト） - プロセス名が 自動ウォッチャーの条件に一致する場合。

  たとえば、プロセス名が「sql」または「svchost」であるという条件にプロセスが一致するときに、プロセス モニタを作成します。 自動ウォッチャーによって作成されたプロセス モニタは、PID に関係なく、一致するプロセスで現在管理対象システムで実行されているものを追跡します。

  - 自動ウォッチャーによって作成されたプロセス モニタの定義は、手動で作成されたプロセス モニタと同じです。
  - 同じ名前で引数が異なるプロセスのセットを個別に管理できます。たとえば、「java.exe」などです。
  - 関連するプロセスのセットに対するモニタを作成できます。

- PID の使用 - PID が 自動ウォッチャーの条件に一致する場合。 自動ウォッチャーでは、ユーザ インターフェースで PID フラグを使用してモニタ プロセスを有効にするか、または sysedge.cf ファイルで監視フラグ 0x1000 を指定します。

  自動ウォッチャーによって作成された各モニタは、一致するプロセスのインスタンスをすべて追跡します。

  - プロセスの特定のインスタンス用のモニタを作成します。
  - ほかと区別するための引数を使用せず、複数のプロセスのインスタンスをモニタします。

関連項目:

自動ウォッチャーの仕組み (P. 248)

事前定義済み自動ウォッチャーの適用

ポリシー設定では、テンプレートで事前定義済みの自動ウォッチャーと以下の SystemEDGE のデフォルト ポリシーを提供します。

- CPU Utilization （OS 非依存テンプレート）
- CA ARCserve （Windows テンプレート）
- Windows Services （Windows テンプレート）
- Microsoft Exchange （Windows テンプレート）
- All Filesystems （SystemEDGE デフォルト ポリシー）
- All Disks （SystemEDGE デフォルト ポリシー）

事前定義済み自動ウォッチャーを使用できるかどうかを確認します。

次の手順に従ってください：

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］または［モニタリング テンプレート］を展開して、［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ペインまたは［テンプレート リスト］が開き、事前定義済みの自動ウォッチャーが表示されます。

2. ［利用可能ポリシー］ペインまたは［テンプレート リスト］で、事前定義済みの自動ウォッチャーをクリックします。

   自動ウォッチャーの［詳細］ペインが表示されます。

3. ［アクション］-［適用］をクリックします。

   ［マシン選択］ページが表示されます。

4. 適切なシステムを選択して、［適用］をクリックします。

   自動ウォッチャーが選択したシステムの SystemEDGE 設定に追加されます。

   SystemEDGE は、自動ウォッチャーの設定に基づいてモニタを自動的に作成します。

   注: 管理対象外モードの SystemEDGE の場合は、sysedge.cf ファイルで自動ウォッチャーを指定します。 SystemEDGE を管理対象モードに変更すると、SystemEDGE が CA Server Automation に登録する前に定義された自動ウォッチャーをポリシーへインポートできます。

関連項目:

自動ウォッチャーの作成とシステムへの適用 (P. 253)

自動ウォッチャーの作成とシステムへの適用

管理対象モードの SystemEDGE では、ポリシーまたはテンプレートで自動ウォッチャーを指定できます。 一元化された設定により、すべてのサーバにわたって一貫性のあるモニタリングを実行できます。 ポリシーまたはテンプレートで自動ウォッチャーを設定し、管理対象システム上のリソースをモニタするために自動ウォッチャーを適用します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］または［モニタリング テンプレート］を展開して、［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ペインまたは［テンプレート リスト］が表示されます。

2. ポリシーまたはテンプレートを開き、［自動ウォッチャー］をクリックします。

   ［汎用自動ウォッチャー］ペインが表示されます。

3. プロセスまたはサービスの自動ウォッチャーを追加する場合は、［プロセス/サービス］タブを選択します。

4. ツールバーの （追加）をクリックします。

   自動ウォッチャーの［詳細］ペインが表示されます。

5. 必要な値を指定して、［保存］をクリックします。

   自動ウォッチャーが保存されます。

6. ［アクション］-［適用］をクリックします。

   ［マシン選択］ページが表示されます。

7. 適切なシステムを選択して、［適用］をクリックします。

   自動ウォッチャーが選択したシステムの SystemEDGE 設定に追加されます。

   SystemEDGE は、自動ウォッチャーの設定に基づいてモニタを自動的に作成します。

   注: 管理対象外モードの SystemEDGE の場合は、sysedge.cf ファイルで自動ウォッチャーを指定します。 SystemEDGE を管理対象モードに変更すると、SystemEDGE が CA Server Automation に登録する前に定義された自動ウォッチャーをポリシーへインポートできます。

関連項目:

自動ウォッチャーの確認 (P. 254)

自動ウォッチャーの確認

CA Server Automation のユーザ インターフェースで、自動ウォッチャーによってリソースに対応するモニタが作成されたかどうかを確認できます。自動ウォッチャーは予約済みのインデックス範囲（1000000 ～ 1999999）でモニタを作成します。

次の手順に従ってください：

1. ［リソース］タブをクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインで［データ センター］フォルダおよび［CA Virtual Assurance サービス］フォルダを展開します。

   データ センターによって検出され、管理されているリソースが表示されます。

3. 対応するモニタを確認するリソースを選択します。

   選択したリソースの［クイック スタート］タスクが表示されます。

4. ［環境設定］タブをクリックします。

   ［セルフ モニタ］ページ表示され、予約済みのインデックス範囲で自動ウォッチャーが作成したモニタが表示されます。

関連項目:

自動ウォッチャーの仕組み (P. 248)

ユーザ固有のメトリック(MIB 拡張)をモニタする方法

次の例では、ユーザ固有のメトリックをモニタする方法を、手順を追って説明します。

ユーザ固有のメトリック(MIB 拡張)をモニタする方法

1. 必要なデータを返すプログラムを作成します。 たとえば、いくつかの固定データを返すシンプルな DOS バッチ スクリプトをエージェント システム上に作成します。

   ```
   @echo off
   echo 99
   ```

2. テキスト エディタを開き、C： ドライブ上の data.bat にこれらの 2 行を保存します。
3. このバッチ ファイルを参照する MIB 拡張を作成します。
   a. ユーザ インターフェースから、［*ポリシー*］をクリックし、［ナビゲーション］ペインで［*設定*］を開き、［ポリシー］ツリーを展開して、SystemEDGE ポリシーを開きます。

      ［ポリシー詳細］が右ペインに表示されます。

   b. ［MIB 拡張］タブをクリックします。

      ［MIB 拡張］ページが表示されます。

   c. フィールドに以下のデータを追加します。

      インデックス： 1 （これが 1 つ目の MIB 拡張である場合）

      タイプ： integer

      拡張コマンド： C:¥data.bat

      アクセス権： 読み取り専用

   d. ［*追加*］をクリックします。

      MIB 拡張がポリシーに追加されます。

   e. ［*ポリシーの保存*］をクリックします。

      ポリシーが保存されます。

4. 新しいモニタの値を確認するためのしきい値モニタを作成します。
   a. ［*モニタ*］をクリックし、［*しきい値*］をクリックします。
      ［しきい値モニタの詳細： 編集］ペインが表示されます。
   b. フィールドに以下のデータを追加します。
      インデックス： （自動的に追加されます）
      プラットフォーム： OS 非依存
      オブジェクト クラス： extensionGroup ［スカラ変数を新規追加して拡張された MIB］
      オブジェクト属性： 1
      オブジェクト インスタンス名： MyData
      間隔： 60
      重大度： メジャー アラーム
      演算子： 次の値以上
      値： 50
      スケール： 1
      サンプル タイプ： 絶対値
   c. ［*保存*］をクリックします。
      ポリシーが保存されます。 しきい値が「50」の「メジャー」アラームが追加されます。 上で作成したスクリプトは常に値「99」を返すため、すぐにこのしきい値に違反することになります。

d. ［*アクション*］をクリックし、［*適用*］をクリックしてポリシーをコンピュータに適用します。

   ［選択したマシン］ペインが表示されます。

e. 選択したマシンが正しいことを確認して、［*適用*］をクリックします。

   MIB 拡張が追加されたポリシーが、選択したコンピュータに適用されます。

   ［*ポリシーに戻る*］をクリックします。

   ［ポリシー詳細］ペインが表示されます。

エージェントが設定されたら、［リソース］タブでこのしきい値モニタの状態を表示できます。「メジャー」しきい値が違反されていることがわかります。

特定の Windows パフォーマンス レジストリのメトリックをモニタする方法

次の例では、ユーザ固有のメトリックをモニタする方法を、手順を追って説明します。 Windows パフォーマンス オブジェクトおよびカウンタで使用する名前は、perfmon.exe 内の名前と一致する必要があります。

ユーザ固有のメトリック（MIB 拡張）をモニタする方法

1. Windows パフォーマンス レジストリのメトリック用に MIB 拡張を作成します。
   a. ユーザ インターフェースから［リソース］タブをクリックし、［設定］ペインを開き、［ポリシー］ツリーを展開して、適切なサブカテゴリをクリックします。

      ［ポリシー詳細］が右ペインに表示されます。

   b. ［*MIB 拡張*］タブをクリックします。

      ［MIB 拡張］ページが表示されます。

   c. ［*Windows パフォーマンス*］をクリックします。

      ［Windows パフォーマンス定義済み拡張］ペインが表示されます。

   d. ［追加］フィールドに以下のデータを追加します。
      例：

      インデックス： 1 （この拡張が 1 つ目である場合）。

      タイプ： integer

      オブジェクト： システム

      カウンタ：プロセス数（実行中のプロセスの合計を指定します）。

      システム メトリックには「インスタンス」がないため、このフィールドは空白のままになります。

      注: ポリシーを作成する際に、オブジェクトとカウンタのカスタム エントリを指定できます。 同じメトリックは、別のポリシーを作成する際に将来使用するために保存されます。

   e. ［*追加*］をクリックします。

      MIB 拡張がポリシーに追加されます。

   f. ［*ポリシーの保存*］をクリックします。

      ポリシーが保存されます。

2. 新しいモニタの値を確認するためのしきい値モニタを作成します。
   a. ［*モニタ*］をクリックし、［*しきい値*］をクリックします。
      ［しきい値モニタの詳細： 編集］ペインが表示されます。
   b. ［+］（新規）をクリックして、モニタを作成します。
      ［しきい値モニタの詳細: 新規］ペインが表示されます。

c. 以下のしきい値設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス

モニタするオブジェクト クラスを指定します。 値は利用可能な MIB テーブルを参照します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を定義します。 値は任意の文字列（たとえば FileSystems）です。

オブジェクト属性

モニタするオブジェクト属性を指定します。 値は、オブジェクト クラスとして選択されたテーブルの利用可能な属性を参照します。属性（たとえば devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）は、このしきい値モニタでモニタする MIB オブジェクト（OID）の初期部分を指定します。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を任意の文字列で定義します（たとえば「PercentUsed」など）。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。 この値、たとえば、デバイス テーブル（devTable）内の 3 番目の行をモニタするための .3 は、このしきい値モニタでモニタする MIB オブジェクト（OID）のインデックス部分を指定します。 いくつかのオブジェクト クラスについては、インスタンス自体の名前を指定できます（たとえば .3 の代わりに C：、または UNIX マシンで /var）。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を定義します。 値は任意の文字列（たとえば SysVol_C）です。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

［しきい値設定］ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時刻

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時刻

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

d. ［*保存*］をクリックします。

モニタがポリシーに追加されます。

3. ［*アクション*］をクリックし、［*適用*］をクリックしてポリシーをコンピュータに適用します。

   ［選択したマシン］ペインが表示されます。

   a. 選択したマシンが正しいことを確認して、［*適用*］をクリックします。

      MIB 拡張が追加されたポリシーが、選択したコンピュータに適用されます。

   b. ［*ポリシーに戻る*］をクリックします。

      ［ポリシー詳細］ペインが表示されます。

エージェントが設定されたら、［エクスプローラ］-［サマリ］の下にある［リソース］タブでこのしきい値モニタの状態を表示できます。

SRM ポリシーを作成する方法

実行するテスト、モニタするしきい値、基本設定、その他エージェントの実行方法とモニタ対象を制御する設定を定義するには、SRM ポリシーを作成します。 作成したポリシーは、SRM AIM と共に管理対象モードで SystemEDGE エージェントを実行する任意の数のシステムに適用できます。ポリシーを使用すると、ローカルで手動によって設定できるすべての設定操作を実行できるうえに、統合されたインターフェース、選択リスト、およびリモート システムへの動的展開といった利点が得られます。

SRM ポリシーを作成するには、以下の手順に従います。

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［サービス レスポンス］ペインが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規サービス レスポンス モニタリング ポリシー］ダイアログ ボックスが表示されます。

3. ポリシーの名前と説明、および既存のポリシーをベースにするかどうかを入力し、［OK］をクリックします。

   ポリシーが作成され、右側のペインに設定画面が表示されます。

4. ポリシーに含めるテストを定義します。
5. テストのしきい値を定義します。
6. 制御設定を定義します (P. 312)。
7. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

エージェントの検出

エージェントに複数の NIC （ネットワーク インターフェース コントローラ）がある場合は、ポリシー設定によってそのエージェントの名前またはアドレスがすべて検出されます。 不要な名前やアドレスが検出されないようにするために、ポリシー設定ではジョブを展開する管理名またはアドレスでエージェントを検出する機能をサポートしています。

注: システムはエージェントのリストを 30 分ごとにリフレッシュします。

次の手順に従ってください:

1. CA Virtual Assurance アプリケーションにログインし、［リソース］タブをクリックします。
2. ［エクスプローラ］タブから、［ドメイン サーバ］を右クリックし、［ポリシー］-［SystemEDGE］-［エージェントの検出］を選択します。

   確認ダイアログ ボックスが表示されます。
3. ［OK］をクリックします。

   注: リストを表示するには、［モニタリング ソフトウェア］タブをクリックし、［ポリシー］タブをクリックします。 管理名またはアドレスを持つ利用可能なエージェントのリストが表示されます。

ポリシー設定機能の一般的な使用法

このセクションでは、一般的なポリシー設定機能について説明します。

SystemEDGE ポリシーを作成する方法

モニタのセット、ロードする AIM、基本設定、その他エージェントの実行方法とモニタ対象を制御する設定を定義するには、SystemEDGE ポリシーを作成します。 作成したポリシーは、管理対象モードで SystemEDGE エージェントを実行する任意の数のシステムに適用できます。 ポリシーを使用すると、ローカルで手動によって設定できるすべての設定操作を実行できるうえに、統合されたインターフェース、選択リスト、およびリモートシステムへの動的展開といった利点が得られます。

SystemEDGE ポリシーを作成するには、以下の手順に従います。

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［SystemEDGE］ペインが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規 SystemEDGE ポリシー］ダイアログ ボックスが表示されます。

3. ポリシーの名前と説明、および既存のポリシーをベースにするかどうかを入力し、［OK］をクリックします。

   ポリシーが作成され、右側のペインに設定画面が表示されます。

4. ポリシーに含めるモニタを定義します。
5. 制御設定を定義します (P. 267)。
6. SNMP 設定を定義します (P. 215)。
7. MIB 拡張を定義します。
8. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシーのコピー

既存の SystemEDGE ポリシーはコピーすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. コピーするポリシーを[利用可能ポリシー]テーブルから選択し、［アクション］をクリックして、［コピー］を選択します。［設定］ペインでポリシーを右クリックし、[コピー]を選択することもできます。

   ［コピー］ダイアログ ボックスが表示されます。

3. ポリシーの新しい名前を入力し、［OK］をクリックします。

   ポリシーがコピーされ、右側のペインに設定画面が表示されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシーの名前変更

既存の SystemEDGE ポリシーの名前は変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 名前を変更するポリシーを[利用可能ポリシー]テーブルから選択し、［アクション］をクリックして、［名前の変更］を選択します。［設定］ペインでポリシーを右クリックし、［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。

   注: ポリシーが使用中の場合は、ポリシー名を変更できないことを示すエラー メッセージが表示されます。

3. ポリシーの新しい名前を入力し、［OK］をクリックします。

   確認のメッセージが表示され、ポリシーの名前が変更されたことが通知されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシーの削除

既存の SystemEDGE ポリシーを削除できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルで削除するポリシーを選択し、［アクション］をクリックして、［削除］を選択します。［設定］ペインでポリシーを右クリックし、［削除］を選択することもできます。

   注: ポリシーが使用されている場合、ポリシーを削除できないことを示すエラー メッセージが表示されます。

   警告メッセージが表示されます。

3. ［OK］をクリックして削除を確定します。

   確認メッセージが表示されます。 ポリシーは削除されます。

ポリシーへの SystemEDGE 設定のインポート

SystemEDGE を最新バージョンにアップグレードした後、以前の SystemEDGE 設定をインポートし、SystemEDGE ポリシーに変換することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規 SystemEDGE ポリシー］ダイアログ ボックスが表示されます。

3. ［インポート］をクリックします。

   ［SystemEDGE エージェント マシン］ウィンドウが表示されます。

4. SystemEDGE 設定をインポートする元のコンピュータを選択し、［OK］をクリックします。

   注: マシン リストには、元の設定ファイルからアップグレードされたすべてのマシンと、定義されたモニタが表示されます。SystemEDGE 5.x が検出され、ポリシー設定に登録されると、コンピュータがリストに表示されます。 コンピュータがリストに表示されない場合は、SystemEDGE の以前のバージョン レベルでモニタが定義されているかどうか、および［ポリシー設定］で設定が行われているかどうかを確認します。

5. ［新規 SystemEDGE ポリシー］ダイアログ ボックスで名前および説明（任意）を入力し、［OK］をクリックしてインポート プロセスを完了します。

6. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシー制御設定の定義

SystemEDGE ポリシー コントロール設定を使用して、以下のエージェント動作を制御できます。

- セキュリティ設定
- SNMP の設定
- MIB テーブルへのデータのロード
- UNIX の設定
- パフォーマンス モニタリングの設定

ポリシーで定義された制御設定をすべてのマシンに適用できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［制御設定］をクリックします。

   ［コントロール］ページが表示されます。

4. （オプション）［デフォルトを使用］をクリックします。

   デフォルトの選択ペインが表示されます。デフォルトの設定を変更できます。

5. 以下の制御設定を行います。

   SNMP

   以下の基本的な SNMP プロパティを定義できます。

   バインド アドレス

   エージェントがバインドし、受信 SNMP リクエストをリスンするインターフェースを指定します。 有効なアドレスは IPv4 または IPv6 のアドレスです。

   注: 対応するデフォルトのポートはインストール中に指定します。

   バインド ポート

   SNMP トラップを送信するために、エージェントがバインドするトラップ ポートを指定します。bind_address が指定されていない場合、エージェントは利用可能なすべての UDP アドレスにバインドします。

   デフォルト： システムによって選択されたポート

   IP ファミリ

   エージェントの通信方法（IPv4 のみ、IPv6 のみ、またはその両方）を指定します。 デフォルトでは、エージェントは、IPv4、IPv6 の順に使用を試行します。

FIPS モード

FIPS 準拠の暗号化を使用するように、エージェントを指定します。 CA eTrust 公開鍵インフラストラクチャ ライブラリを有効にするには、［非 FIPS モード］を選択します。この方法が失敗する場合は、内部の最低限のセキュリティ ソリューションにフォールバックします。 FIPS 準拠の暗号化を有効にするには、［FIPS 共存モード］を選択します。この方法が失敗する場合は、CA eTrust 公開鍵インフラストラクチャ ライブラリにフォールバックします。RSA BSAFE Crypto-C Micro Edition FIPS を有効にするには、［FIPS のみのモード］を選択します。この方法が失敗する場合は、暗号化は実行されません。

デフォルト： 非 FIPS モード

トラップ ソース

トラップを送信するために使用されるソース アドレスを指定します。 有効なアドレスは IPv4 アドレス、IPv6 アドレス、またはホスト名です。

デフォルト： エージェントのホスト名

セキュリティ設定

以下のセキュリティ基本設定を定義できます。

認証トラップ

エージェントが認識できないという、コミュニティ名を備えた SNMP メッセージをエージェントが受信した場合に、認証失敗トラップを送信します。

デフォルト： 無効

プロセス セット

プロセス テーブルおよび Running Software テーブルで、エージェント システム上で実行されているプロセスや他のソフトウェアにアクセスできます。これらのテーブルで SNMP セットを許可すると、セキュリティの問題が発生する場合があります。

リモート シェル グループ

管理システムは、リモート シェル グループを使用して、エージェント システム上でシェル スクリプトおよびプログラムを実行するようにエージェントに対してリモートから指示できます。 このタイプの情報が漏えいすると、潜在的なセキュリティ リスクが発生する可能性があります。

実行アクション

しきい値違反が発生したときに、モニタリング テーブルを使用したアクション コマンドの実行を有効にします。 アクション コマンドおよびスクリプトを実行する機能が原因で、セキュリティ上の問題が発生する可能性があります。

MIB テーブルへのデータのロード

システム管理 MIB の以下のテーブルに入力します。

- プロセス テーブル
- ユーザ グループ テーブル
- Who テーブル
- トラップ コミュニティ テーブル
- ミラー テーブルのモニタ
- ミラー テーブルを集計
- トップ プロセス テーブル

各テーブルには、MIB で公開可能な機密情報か、ディスク領域を節約するために無効にできる重要でない情報のいずれかが含まれています。 デフォルト設定では、プロセス テーブルを除くすべてのテーブルにデータをロードできます。

その他

以下のその他の設定を定義できます。

SNMP を使用してエージェントが更新されるのを許可

SNMP SET を使用したエージェントの更新を許可します（書き込みコミュニティの削除など）。エージェントで SNMP セットを許可した場合、この方法で更新すると、SNMP セットの変更が通知され、システムのポリシー詳細を表示すると例外が発生します。

マネージャに設定の更新を通知

エージェントが処理する SNMP 設定リクエストすべてについて、エージェントによるマネージャへの通知送信を可能にします。

ウォーム スタートのディスカバリ

ウォーム スタート設定が更新されるたびに、すべてのデバイスでエージェントが再検出されます。デバイスが多数あるシステムを管理している場合、ウォーム スタートのたびにディスカバリが実行されると、非常に多くの時間とリソースを消費する場合があります。

Perl 互換正規表現を使用

Perl 互換正規表現（PCRE）を使用すると、正規表現をサポートするモニタを定義するときに i18n 互換の正規表現を指定できます。 正規表現の例には、ログ ファイル、プロセス、プロセス グループ、Windows サービスおよび Windows イベントがあります。また、このオプションを使用して、より複雑な正規表現を作成できます。 このオプションは、SystemEDGE エージェント 5.1.0 以降のバージョンで提供されています。

インデックスの競合を自動的に解決する

インデックスの競合を解決できるようにします。すべてのマシンに階層型テンプレートを適用するとき、インデックスはテンプレート内に追加されたモニタに割り当てられます。割り当てられたインデックスがベース ポリシーまたは別のテンプレート内の既存のインデックスと競合する場合、このオプションは一意のインデックス値を再割り当てします。

注: ベース ポリシー内に含まれるインデックスは、配信された設定で常に維持されます。このオプションが無効な場合、競合するインデックスを解決できません。ただし、マシンに階層型テンプレートを適用するとき、競合するインデックスは、競合するインデックスが発生した階層型テンプレート上にエラーとして表示されます。

履歴パフォーマンス モニタリング

パフォーマンス キューブ AIM に対して以下の設定を定義できます。パフォーマンス キューブ AIM では、履歴パフォーマンスを管理するための履歴情報を Systems Performance キューブに収集します。

収集間隔

履歴テーブルからパフォーマンス キューブに情報を収集する頻度を指定します。

インデックス範囲の開始

インデックスの予約済み範囲の開始を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンス キューブ データを収集するための履歴コントロール エントリを作成します。 この予約済み範囲は、SRM （サービス レスポンス モニタリング) がパフォーマンス データを収集するよう設定されている場合などに使用されます。

インデックス範囲の終了

インデックスの予約済み範囲の終了を指定します。デフォルトでは、エージェントはこの範囲でパフォーマンス キューブ データを収集するための履歴コントロール エントリを作成します。 この予約済み範囲は、SRM （サービス レスポンス モニタリング) がパフォーマンス データを収集するよう設定されている場合などに使用されます。

UNIX 制御設定

UNIX システム上で実行されるエージェントに対して、以下の設定を定義できます。

サブプログラム グループ

サブプログラムを実行するルート以外のグループ名を指定します。

サブプログラム ユーザ

サブプログラムを実行するルート以外のユーザ名を指定します。

Linux Freemem を含む

空きメモリの計算に、システム バッファ、ディスク キャッシュ メモリ、またはその両方を含めるかどうかを指定します。

システム デバイスのクエリ

以下のシステム デバイス メトリックのクエリを有効にできます。

- シリアル デバイス ステータス
- フロッピー ディスク ステータス
- ディスク サイズ、容量、説明、およびその他のプロパティ (ディスクのプローブ)
- NFS ファイル システム ステータス
- HP-UX グラフィックス ステータス

これらのメトリックに対してクエリを実行すると、潜在的なエージェント ブロックに関する問題が発生する可能性があります。 デフォルト設定では、シリアル デバイス ステータスおよび NFS ファイル システム ステータスに対するクエリのみが有効になっています。

6. ［プラグイン］をクリックします。

［プラグイン］ペインが表示されます。 このペインで、エージェントを使用してロードする AIM を指定します。

7. 以下のいずれかを実行します。
   - ［利用可能なすべてのプラグインをロードします］を選択して、エージェント システムで利用可能なすべての AIM をロードします。
   - ［テーブルで選択されたプラグインをロードします］を選択します。
   - ［外部プラグイン］ツールバーの［+］（新規）をクリックし、外部プラグイン テーブルに AIM を追加します。

注: 利用可能な AIM の詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

AIM ロードが設定されます。

8. ［モニタを集計］をクリックします。

「オブジェクト集計の設定 (P. 274)」の説明に従って、モニタの集計を設定します。

制御設定が定義されます。

9. ［ポリシーの保存］をクリックします。

ポリシーが保存されます。

関連項目:

オブジェクト集計の設定 (P. 274)

オブジェクト集計の設定

デフォルトでは、SystemEDGE がモニタを集計し、オブジェクト クラス、インスタンス、および属性プロパティに同じ値を含む管理対象オブジェクトを生成します。 たとえば、SysHealth のクラス、CPU のインスタンス、および SysTime の属性を備えたすべてのモニタが組み合わせられ、集計管理対象オブジェクトとなります。

SystemEDGE ポリシーを定義するときに、より高いレベルでオブジェクトを集計するよう、エージェントを設定できます。 また、オブジェクト集計および状態管理モデルに関連するエージェント動作の他の側面も設定できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［制御設定］をクリックします。

   ［コントロール］ページが表示されます。

4. ［モニタを集計］をクリックします。

   ［モニタを集計］ページが表示されます。

5. 集計レベルを指定するチェック ボックスを 1 つ以上、オンにします。

   これらはデフォルトより高い集計レベルを表し、最も高いレベルでは 1 つの最上位エージェント オブジェクトにすべてのモニタを集計できます。 集計レベルを指定すると、指定したレベルまでステータスをプロパゲートする層構造のオブジェクト アーキテクチャを作成できます。

6. 以下の追加設定を設定して、［ポリシーの保存］をクリックします。

   すべての集計済みモニタのレガシートラップを送信します。

   管理対象オブジェクトを形成するすべてのモニタのレガシー トラップを送信するかどうかを指定します。 デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタの状態変更トラップを送信するのみです。

   すべての集計済みモニタのコマンドを実行します。

   管理対象オブジェクトを形成するすべてのモニタのアクション コマンドを実行するかどうかを指定します。 デフォルトでは、オブジェクト内の他のモニタでしきい値違反が発生しても、エージェントは、最も重大度の高いモニタのアクション コマンドを実行するのみです。

   集計設定が設定されます。 変更を有効にするには、ポリシーを適用または再適用します。

関連項目:

SystemEDGE ポリシー制御設定の定義 (P. 267)

新しい SystemEDGE モニタリング テンプレートの定義

SystemEDGE はさまざまなポリシーを使って設定することができます。［モニタリング テンプレート］では、複数のポリシーを設定し、共有サーバ上の同じエージェントに配信できます。

［モニタリング テンプレート］ページでは、特定のサーバまたはサーバ グループに適用されたポリシーを表示および更新できます。 SystemEDGE モニタリング テンプレート（階層型テンプレート）を作成してポリシーにインポートできます。 これによって複数のポリシーでモニタを再利用できるようになり、モニタを何回もセットアップする必要がありません。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［SystemEDGE］ページが表示されます。

2. ［テンプレート リスト］ツールバーの［+］（新規）をクリックします。

   ［新規 SystemEDGE モニタリング テンプレート］ダイアログ ボックスが表示されます。

3. テンプレートの名前と任意の説明、システム タイプ、および既存のテンプレートをベースにするかどうかを入力し、［OK］をクリックします。

   テンプレートが作成され、［サマリ］ページが表示されます。テンプレートにモニタを追加する方法については、「SystemEDGE ポリシーへのモニタの追加 (P. 285)」を参照してください。

4. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

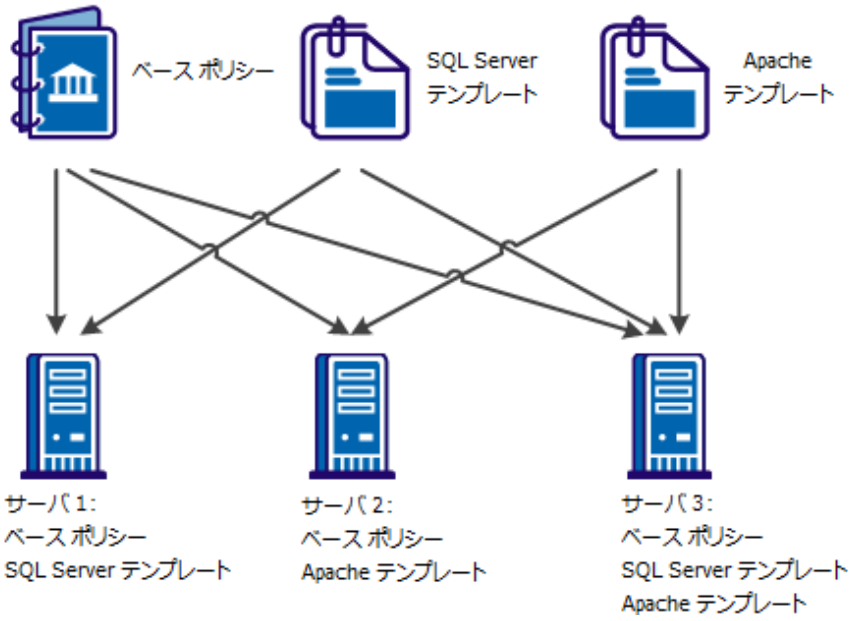
関連項目:

階層型テンプレート (P. 277)
SystemEDGE ポリシーへのモニタリング テンプレートのインポート (P. 280)
SystemEDGE モニタリング テンプレートのコピー (P. 281)
SystemEDGE モニタリング テンプレートの変更 (P. 281)
SystemEDGE モニタリング テンプレートの名前変更 (P. 282)
SystemEDGE モニタリング テンプレートの削除 (P. 282)
モニタリング テンプレート適用の進捗状況の確認 (P. 283)
マシンへのテンプレートの適用 (P. 283)
階層型テンプレート (P. 277)
SystemEDGE モニタリング テンプレートの変更 (P. 281)
SystemEDGE モニタリング テンプレートの名前変更 (P. 282)
モニタリング テンプレート適用の進捗状況の確認 (P. 283)
マシンへのテンプレートの適用 (P. 283)

階層型テンプレート

企業では、サーバまたはサーバ グループによって処理されるワークロードは異なります。 サーバまたはサーバ グループによって処理されるワークロードに固有の複数のポリシーを作成することができます。 ポリシーを容易に作成できるようにするために、テンプレートを使用してアプリケーション固有のモニタを作成します。 ベース ポリシーと階層型テンプレートが組み合わされて設定ファイルが形成され、モニタするサーバに適用されます。 階層型テンプレートは、追加または削除することができます。 テンプレート更新はサーバに直接適用できます。ベース ポリシーを変更したり、更新されたテンプレートをベース ポリシーに再インポートしたりする必要はありません。

例: ベース ポリシーおよびテンプレートをサーバに適用



階層型ポリシーは、以下のシナリオで使用できます。

異種アプリケーション

異なるセットのアプリケーションを実行するサーバごとにテンプレートのライブラリを作成します。各サーバにテンプレート更新を直接適用できます。

動的な環境

サーバの負荷は、動的な環境で頻繁に変化します。階層型テンプレートを使用して、モニタを論理グループに分離します。負荷の変化に基づいて、論理グループを直接システムに適用したり、システムから削除したりできます。

共有サーバ

企業セットアップでは、サーバは複数の部門間で共有されます。 各部門は共有サーバ上のアプリケーションを管理し、モニタします。 階層型テンプレートを使用することにより、テンプレートの個別の管理および各部門のシステムへの適用を行うことができます。

アプリケーションの保守

モニタリングは複数のテンプレートに分割できます。 サーバでは、使用していないアプリケーションのテンプレートを削除でき、システムの他の部分のモニタリングに影響することもありません。

すぐに使用できるテンプレート

すぐに使用できるテンプレートを管理対象ノードに適用できます。 管理対象ノードに対するテンプレート設定を使用してポリシーを設定します。テンプレートは以下のオペレーティング システムに利用可能です。

すべてのオペレーティング システム用:

- CPU Utilization - Autowatch
- Swap Capacity

Windows の場合:

- App Monitoring - CA eTrust Antivirus
- Process Crash
- System Errors
- System Processes
- User Activity
- Windows Services - Autowatch

UNIX（AIX、HPUnix、Linux、Solaris）:

- System Messages
- System Processes

User Activity

SystemEDGE ポリシーへのモニタリング テンプレートのインポート

SystemEDGE ポリシーへモニタリング テンプレートをインポートできます。これは、1 回の操作ですべてのシステムの既存のポリシーを一貫したポリシーに置換します。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［アクション］をクリックし、［インポート］を選択します。

   テンプレートのインポート ウィザードが表示されます。

5. ［システム タイプ］を選択し、インポートするモニタリング テンプレートをドロップダウン リストから選択します。

6. （オプション）インポートされたモニタごとに新しいベース インデックスを定義します。

7. ドロップダウン リストから［競合の解決オプション］を選択し、［次へ］をクリックします。

   ［競合の解決］ページが表示されます。

8. 任意のモニタ競合を調査し、インデックスを調整して、［次へ］をクリックします。

   ［サマリ］ページが表示されます。

9. インポートされるモニタを調査し、［終了］をクリックしてインポート プロセスを完了します。

10. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

SystemEDGE モニタリング テンプレートのコピー

既存の SystemEDGE モニタリング テンプレートはコピーすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。

2. コピーするモニタリング テンプレートを選択し、［アクション］をクリックして、［コピー］を選択します。［設定］ペインでモニタリング テンプレートを右クリックし、［コピー］を選択することもできます。

   ［コピー］ダイアログ ボックスが表示されます。

3. モニタリング テンプレートの新しい名前を入力し、［OK］をクリックします。

   モニタリング テンプレートがコピーされ、右側のペインに設定画面が表示されます。

SystemEDGE モニタリング テンプレートの変更

SystemEDGE モニタリング テンプレートは変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。

2. テンプレート名を選択します。

   ［サマリ］ページが開き、テンプレート情報が示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. 適切なモニタ タブをクリックし、変更するモニタを選択します。

   ［編集］ダイアログ ボックスが表示されます。

5. 必要に応じて設定を変更し、［保存］をクリックします。
6. （オプション）追加するモニタごとに同じ手順を繰り返します。
7. ［保存］をクリックします。

   モニタリング テンプレートが保存されます。

SystemEDGE モニタリング テンプレートの名前変更

既存の SystemEDGE モニタリング テンプレートの名前は変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。
2. 名前を変更するモニタリング テンプレートを選択し、［アクション］をクリックして、［名前の変更］を選択します。［設定］ペインでモニタリング テンプレートを右クリックし、［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。
3. モニタリング テンプレートの新しい名前を入力し、［OK］をクリックします。

   モニタリング テンプレートの名前が変更され、右側のペインに設定画面が表示されます。

SystemEDGE モニタリング テンプレートの削除

必要のなくなった既存の SystemEDGE モニタリング テンプレートは削除することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。

2. ［管理対象マシン］タブをクリックします。

   ［サマリ］ページが開き、テンプレートに適用された管理対象マシンのリストが示されます。

3. 削除するモニタリング テンプレートを選択し、［削除］アイコンをクリックします。

   確認メッセージが表示されます。

4. ［OK］をクリックして削除を確定します。

   モニタリング テンプレートが削除されます。

モニタリング テンプレート適用の進捗状況の確認

モニタリング テンプレート適用操作の進捗状況は、個々のテンプレートについて詳細なレベルで確認することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］を選択します。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。

2. テンプレート名を選択します。

   ［サマリ］ページが開き、テンプレート情報が示されます。

3. ［管理対象マシン］タブをクリックします。

   ［管理対象マシン］ページが開き、設定ステータスの表示が可能なモニタリング テンプレートを現在実行しているマシンのリストが示されます。

4. （オプション）［設定の表示］をクリックします。

   ［SystemEDGE 設定］ペインが開き、ポリシーとテンプレート、およびエージェントに対して配信された設定ファイルを表示できます。

マシンへのテンプレートの適用

モニタリング テンプレートを更新したら、企業全体でそれをマシンに適用できます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］を選択します。

   ［サマリ］ページには SystemEDGE モニタリング テンプレートのリストが表示されます。

2. テンプレート名を選択します。

   ［サマリ］ページが開き、テンプレート情報が示されます。

3. ［アクション］をクリックし、［適用］を選択します。

   モニタリング テンプレートを適用するマシンを選択するためのタブが表示されます。［このテンプレートを実行しているマシンを更新］タブでは、すでにテンプレートを使用しているマシンにモニタリング テンプレートを適用できます。［このテンプレートを実行していないマシンに適用］タブでは、テンプレートをまったく使用していないマシンにモニタリング テンプレートを適用できます。

4. （オプション）［既存のマシン］で、以下のいずれかのオプションを選択します。

   - このテンプレートを適用してすべてのマシンを更新
   - このテンプレートの最新の変更が適用されていないマシンのみを更新
   - テンプレートが正常に適用されていないマシンのみを更新
   - 詳細（手動でマシンを選択）
   - マシンからこのテンプレートを削除

5. （オプション）［選択したマシン］の下で、テンプレートが再適用されるマシンを選択します。

6. （オプション）テンプレートを適用するマシンを［このテンプレートを実行していないマシンに適用］タブから選択します。

7. ［適用］をクリックします。

   テンプレートの適用が開始されます。

テンプレートへの SystemEDGE 設定のインポート

SystemEDGE を最新バージョンにアップグレードした後、以前の SystemEDGE 設定をインポートし、SystemEDGE モニタリング テンプレートに変換することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［SystemEDGE］をクリックします。

   ［利用可能な SystemEDGE モニタリング テンプレート］ページが表示されます。

2. ［利用可能な SystemEDGE モニタリング テンプレート］ツールバーで［+］（新規）をクリックします。

   ［新規 SystemEDGE モニタリング テンプレート］ダイアログ ボックスが表示されます。

3. ［インポート］をクリックします。

   ［SystemEDGE エージェント マシン］ウィンドウが表示されます。

4. SystemEDGE 設定をインポートする元のコンピュータを選択し、［OK］をクリックします。

   注: マシン リストには、元の設定ファイルからアップグレードされたすべてのマシンと、定義されたモニタが表示されます。SystemEDGE 5.x が検出され、ポリシー設定に登録されると、コンピュータがリストに表示されます。 コンピュータがリストに表示されない場合は、SystemEDGE の以前のバージョン レベルでモニタが定義されているかどうか、および［ポリシー設定］で設定が行われているかどうかを確認します。

5. ［新規 SystemEDGE モニタリング テンプレート］ダイアログ ボックスで名前および説明（任意）を入力し、［OK］をクリックしてインポート プロセスを完了します。

6. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

SystemEDGE ポリシーへのモニタの追加

SystemEDGE ポリシーにはモニタを追加することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックし、追加するモニタを選択します。
   - しきい値モニタの定義 (P. 286)
   - プロセス モニタの定義 (P. 289)
   - ログ ファイル モニタの定義 (P. 291)
   - Windows イベント モニタの定義 (P. 293)
   - 履歴モニタの定義 (P. 295)
   - プロセス グループ モニタの定義 (P. 297)
4. （オプション）追加するモニタごとに同じ手順を繰り返します。
5. ［ポリシーの保存］をクリックします。

   モニタがポリシーにロードされ、ポリシーが保存されます。

注: モニタの詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

関連項目:

しきい値モニタの定義 (P. 286)
プロセス モニタの定義 (P. 289)
ログ ファイル モニタの定義 (P. 291)
Windows イベント モニタの定義 (P. 293)
履歴モニタの定義 (P. 295)
プロセス グループ モニタの定義 (P. 297)

しきい値モニタの定義

SystemEDGE ポリシーのしきい値設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。
2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［しきい値］をクリックします。

   ［しきい値モニタ］ページが表示されます。

5. ［しきい値モニタ］ツールバーの［+］（新規）をクリックします。

   ［しきい値モニタの詳細: 新規］ペインが表示されます。

6. 以下のしきい値設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   オブジェクト クラス

   モニタするオブジェクト クラスを指定します。ドロップダウン リストの値は、利用可能な MIB テーブルです。

   オブジェクト クラス名

   オブジェクト状態モデルに使用するオブジェクト クラス名を定義します。 これは任意の文字列です（FileSystems など）。

   オブジェクト属性

   モニタするオブジェクト属性を指定します。 ドロップダウン リストの値は、オブジェクト クラスとして選択されたテーブルの利用可能な属性です。 属性（たとえば devCapacity = 1.3.6.1.4.1.546.1.1.1.7.1.14）は、このしきい値モニタでモニタする MIB オブジェクト（OID）の初期部分を指定します。

   オブジェクト属性名

   オブジェクト状態モデルに使用するオブジェクト属性名を定義します。 これは任意の文字列です（PercentUsed など）。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。 この値、たとえば、デバイス テーブル（devTable）内の 3 番目の行をモニタするための .3 は、このしきい値モニタでモニタする MIB オブジェクト（OID）のインデックス部分を指定します。 いくつかのオブジェクト クラスについては、インスタンス自体の名前を指定できます（たとえば .3 の代わりに C：、または UNIX マシンで /var）。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を定義します。 これは任意の文字列です（SysVol_C など）。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

［しきい値設定］ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

   ［しきい値モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

しきい値モニタがポリシーにロードされます。

プロセス モニタの定義

SystemEDGE ポリシーのプロセス設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. プロセスをクリックします。

   ［プロセス モニタ］ページが表示されます。

5. ［プロセス モニタ］ツールバーの［+］（新規）をクリックします。

   ［プロセス モニタの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

インデックス

使用するテーブル インデックスを定義します。

プラットフォーム

プラットフォームを指定します。

説明

オプションの説明を定義します。

オブジェクト クラス名

オブジェクト状態モデルに使用するオブジェクト クラス名を指定します。 これは任意の文字列です（Process など）。

オブジェクト属性

モニタするオブジェクト属性を指定します。 ドロップダウン リストの値は、プロセス モニタリングに利用可能な属性です。

オブジェクト属性名

オブジェクト状態モデルに使用するオブジェクト属性名を定義します。 これは任意の文字列です（MemUsedPercent など）。

オブジェクト インスタンス

モニタするオブジェクト インスタンスを指定します。 これは、名前による一致処理、、または名前による Windows サービスの一致処理に使用される正規表現（オプションの設定に依存します）です。 パターンは一意に単一のプロセス（サービス）と一致する必要があります。 引数を含むことができます（オプション設定を参照してください）。

オブジェクト インスタンス名

オブジェクト状態モデルに使用するオブジェクト インスタンス名を指定します。 これは任意の文字列です（ApacheServer など）。

間隔

モニタの評価間隔を 30 秒の倍数で定義します。

［しきい値設定］ページで、以下の設定を定義できます。

重大度

オブジェクト状態モデルで使用する重大度を指定します。

演算子

使用する演算子を指定します。

値

使用する値を定義します。

サンプル タイプ

使用するサンプル タイプを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

［プロセス モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

プロセス モニタがポリシーにロードされます。

ログ ファイル モニタの定義

SystemEDGE ポリシーのログ ファイル設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［ログ ファイル］をクリックします。

   ［ログ ファイル モニタ］ページが表示されます。

5. ［ログ ファイル モニタ］ツールバーの［+］（新規）をクリックします。

   ［ログ ファイルの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   モニタ タイプ

   使用するモニタ タイプを指定します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   ログ ファイル/ディレクトリ名

   モニタするファイルまたはディレクトリのパスを定義します。

   検索フィルタ

   検索フィルタを指定します。

   間隔

   モニタ評価間隔を分単位で定義します。

   重大度

   一致したときのモニタの重要度を指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

   ［ログ ファイル モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

ログ ファイル モニタがポリシーにロードされます。

Windows イベント モニタの定義

SystemEDGE ポリシーの Windows イベント設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［Windows イベント］をクリックします。

   ［Windows イベント モニタ］ページが表示されます。

5. ［Windows イベント モニタ］ツールバーの［+］（新規）をクリックします。

   ［Windows イベントの詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   イベント ログ

   読み取るイベント ログを指定します。

   イベント タイプ

   モニタするイベント タイプを指定します。

   ソース フィルタ

   使用するソース フィルタを定義します。

   説明フィルタ

   使用する説明フィルタを定義します。

   重大度

   一致したときのモニタの重要度を指定します。

［保守ウィンドウ］サブタブで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］サブタブで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

   ［Windows イベント モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

Windows イベント モニタがポリシーにロードされます。

履歴モニタの定義

SystemEDGE ポリシーの履歴設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［履歴］をクリックします。

   ［履歴モニタ］ページが表示されます。

5. ［履歴モニタ］ツールバーの［+］（新規）をクリックします。

   ［履歴詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   オブジェクト クラス

   モニタするオブジェクトを指定します。 ドロップダウン リストの値は、利用可能な MIB テーブルです。

   オブジェクト属性

   モニタするオブジェクト属性を指定します。 ドロップダウン リストの値は、オブジェクト クラスとして選択されたテーブルの利用可能な属性です。 属性（たとえば devCapacity=1.3.6.1.4.1.546.1.1.1.7.1.14）は、この履歴エントリを使用してモニタするための MIB オブジェクト（OID）の初期部分を指定します。

   オブジェクト インスタンス

   モニタするオブジェクト インスタンスを定義します。 この値、たとえば、デバイス テーブル（devTable）内の 3 番目の行をモニタするための .3 は、この履歴値モニタでモニタする MIB オブジェクト（OID）のインデックス部分を指定します。

間隔

収集間隔を 30 秒の倍数で定義します。

バケット

収集するサンプル数を定義します。

[パフォーマンス キューブに追加]チェック ボックス

このエントリのパフォーマンス キューブ データを収集するかどうかを指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

   ［履歴モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

履歴モニタがポリシーにロードされます。

プロセス グループ モニタの定義

SystemEDGE ポリシーのプロセス グループ設定は定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］をクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［プロセス グループ］をクリックします。

   ［履歴モニタ］ページが表示されます。

5. ［プロセス グループ モニタ］ツールバーの［+］（新規）をクリックします。

   ［プロセス グループ詳細: 新規］ダイアログ ボックスが表示されます。

6. 以下のプロセス設定を行います。

   インデックス

   使用するテーブル インデックスを定義します。

   プラットフォーム

   プラットフォームを指定します。

   説明

   オプションの説明を定義します。

   プロセス名

   プロセス名を定義します。 これは、照合に使用する正規表現です（オプション設定から独立しています）。プロセスを名前で、、それぞれ照合します。

   間隔

   モニタの評価間隔を 30 秒の倍数で定義します。

   ユーザ名

   任意のプロセス名正規表現に加えて、モニタするユーザ名を定義します。

   グループ名

   任意のプロセス名正規表現に加えて、モニタするグループ名を定義します。

   重大度

   グループ変更に関する、モニタの重要性を指定します。

［保守ウィンドウ］ページで、以下の設定を定義できます。

状態

モニタ保守エントリがアクティブであるか、非アクティブであるかを指定します。

開始時間

モニタがオフになり、保守ウィンドウが開始する開始時刻を定義します。

停止時間

モニタが再びオンになり、保守ウィンドウが終了する停止時刻を定義します。

［オプション設定］ページで、さまざまなモニタ エントリまたは履歴制御エントリで使用可能な以下のフラグを定義できます。

注: 詳細については、「SystemEDGE ユーザ ガイド」を参照してください。

7. ［保存］をクリックします。

   ［プロセス グループ モニタ］設定が保存されます。

8. ［ポリシーの保存］をクリックします。

   プロセス グループ モニタがポリシーにロードされます。

SystemEDGE ポリシー内のモニタの表示

SystemEDGE ポリシーに含まれているモニタは表示することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。モニタリング クラスのサブタブをクリックすると、ポリシーに含まれている他のモニタを表示できます。

関連項目

SystemEDGE ポリシー内のモニタの変更 (P. 300)
SystemEDGE ポリシーからのモニタの削除 (P. 301)

SystemEDGE ポリシー内のモニタのコピー

SystemEDGE ポリシー内のモニタはコピーすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。
2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。
3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。
4. 適切なモニタ タブをクリックし、コピーするモニタを選択します。
5. ［アクション］をクリックし、［コピー］を選択します。

   ［編集］ダイアログ ボックスが表示されます。
6. 必要に応じて設定を変更し、［保存］をクリックします。
7. （オプション）追加するモニタごとに同じ手順を繰り返します。
8. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシー内のモニタの変更

SystemEDGE ポリシー内のモニタは変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. 適切なモニタ タブをクリックし、変更するモニタを選択します。
5. ［アクション］をクリックし、［変更］を選択します。

   ［編集］ダイアログ ボックスが表示されます。

6. 必要に応じて設定を変更し、［保存］をクリックします。
7. （オプション）追加するモニタごとに同じ手順を繰り返します。
8. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシーからのモニタの削除

SystemEDGE ポリシー内のモニタは削除することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. 適切なモニタ タブをクリックし、削除するモニタを選択します。
5. ［アクション］をクリックし、［削除］を選択します。

   警告メッセージが表示されます。

6. ［OK］をクリックして削除を確定します。
7. （オプション）追加するモニタごとに同じ手順を繰り返します。

8. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SystemEDGE ポリシー内の既存テンプレートの変更

既存のモニタリング テンプレートは、変更して SystemEDGE ポリシーにインポートすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［モニタ］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるモニタのリストが表示されます。

4. ［アクション］をクリックし、［インポート］を選択します。

   テンプレートのインポート ウィザードが表示されます。

5. 必要な情報を使ってモニタリング テンプレートを更新します。

6. ［システム タイプ］を選択し、インポートする更新済みのモニタリング テンプレートをドロップダウン リストから選択します。

7. （オプション）インポートされたモニタごとに新しいベース インデックスを定義します。

8. ［競合の解決オプション］で［既存のモニタをインポートされるエンティティに置換します］を選択し、［次へ］をクリックします。

   ［競合の解決］ページが表示されます。

9. 任意のモニタ競合を調査し、インデックスを調整して、［次へ］をクリックします。

   ［サマリ］ページが表示されます。

10. インポートされるモニタを調査し、［終了］をクリックしてインポート プロセスを完了します。

11. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

12. ［アクション］ドロップダウン リストから［適用］を選択します。

    保存したポリシーが希望のマシンに適用されます。

新しい SRM ポリシーの定義

SRM ポリシーを作成することで、実行するテスト、モニタするしきい値、基本設定、およびエージェントの実行方法とモニタ対象を制御する他の設定を定義することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規サービス レスポンス モニタリング ポリシー］ダイアログ ボックスが表示されます。

3. ポリシーの名前と任意の説明、システム タイプ、および既存のポリシーをベースにするかどうかを入力し、［OK］をクリックします。

   ポリシーが作成され、右側のペインに設定画面が表示されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

関連項目:

SRM ポリシーのコピー (P. 303)
SRM ポリシーの名前変更 (P. 304)
SRM ポリシーの削除 (P. 305)

SRM ポリシーのコピー

既存の SRM ポリシーはコピーすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. コピーするポリシーを［利用可能ポリシー］テーブルから選択し、［アクション］をクリックして、［コピー］を選択します。［設定］ペインでポリシーを右クリックし、［コピー］を選択することもできます。

   ［コピー］ダイアログ ボックスが表示されます。

3. ポリシーの新しい名前を入力し、［OK］をクリックします。

   ポリシーがコピーされ、右側のペインに設定画面が表示されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM ポリシーの名前変更

既存の SRM ポリシーの名前は変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 名前を変更するポリシーを［利用可能ポリシー］テーブルから選択し、［アクション］をクリックして、［名前の変更］を選択します。［設定］ペインでポリシーを右クリックし、［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。

   注: ポリシーが使用中の場合は、ポリシー名を変更できないことを示すエラー メッセージが表示されます。

3. ポリシーの新しい名前を入力し、［OK］をクリックします。

   確認のメッセージが表示され、ポリシーの名前が変更されたことが通知されます。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM ポリシーの削除

既存の SRM ポリシーは削除することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 削除するポリシーを［利用可能ポリシー］テーブルから選択し、［アクション］をクリックして、［コピー］を選択します。［設定］ペインでポリシーを右クリックし、［削除］を選択することもできます。

   注: ポリシーが使用中の場合は、ポリシーを削除できないことを示すエラー メッセージが表示されます。

3. 警告メッセージが表示されます。［OK］をクリックして削除を確定します。

4. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM ポリシーへのテストの追加

SRM ポリシーにはテストを追加することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［テスト］をクリックし、［テスト モニタ］ツールバーの［+］（新規）をクリックします。

   ［新規］ダイアログ ボックスが表示されます。

4. ［テスト名］フィールドに、テストの一意の名前を入力します。この名前は 64 文字以下にしてください。テスト名では大文字と小文字が区別されます。

5. （オプション）テストの説明を入力します。

6. （オプション）テスト クラスを定義します。
7. ［テスト タイプ］リストで、希望のテスト タイプをクリックします。

Active Directory

Windows Active Directory サービスが正しく動作して、共有ファイルとリソースを管理することを確認します。

カスタム

重要なカスタム サービスまたは他のタスクが効率よく動作することを確認します。

DHCP

DHCP （Dynamic Host Configuration Protocol）サーバが応答して、アドレス要求に応答することを確認します。

DNS

解決要求に対応するためにドメイン名システム サーバがホスト名を処理していることを確認します。

ファイル I/O

ファイル システム全体での読み取り、書き込み、および比較の作業を確認します。

FTP および TFTP

ユーザが、指定されたサーバにログインして、ファイルのアップロードとダウンロードを実行できることを確認します。

HTTP および HTTPS

ユーザがビジネス Web サーバに接続できることを確認し、また特定のテキストが Web ページ上に表示されるかどうかを確認します。

LDAP

LDAP サーバへの接続を確認して、ユーザ リクエストおよび LDAP クエリ用のアクセスを確認します。

NIS

NIS マップ リクエストが処理されていることを確認します。

NNTP

ユーザが Usenet ニュースグループ サーバおよび社内掲示板に接続できることを確認します。

PING

ネットワーク デバイスが存在し、ネットワークを介してアクセス可能であることを確認します。

電子メール

電子メール サーバが利用可能であり、電子メールを効率よく処理することを確認します。 SRM は、 IMAP、MAPI、POP3、SMTP、および SMTP サーバから発信される往復の電子メールのテストをサポートします。

SNMP

SNMP エージェントが SNMPv1 GET リクエストに応答することを確認します。

SQL クエリ

SQL データベース サーバが利用可能で、短いクエリを処理することを確認します。

TCP

システムが接続リクエストをリスンして、処理することを確認します。

仮想ユーザ

記録可能な（通常は WinTask で）実際のユーザ トランザクション（キーボード入力とマウスのクリック）の継続的な応答時間および可用性データを取得して、ビジネス タスクが正常に実行されていることを確認します。

注: 各テスト タイプの詳細と定義については、「SRM ユーザ ガイド」を参照してください。

8. ［テスト間隔］フィールドにテストの間隔（秒単位）を指定します。間隔は、30 秒の倍数にする必要があります。 このオプションは、テストのパフォーマンスを調整するために使用します。
9. ［テスト タイムアウト］フィールドにテストがタイムアウトする時間（秒単位）を指定します。 テスト間隔より短く、テストの実行にかかる時間より長い数値を選択してください。
10. ［ポーリング間隔］リストから以下のいずれかを選択して、ポーリング間隔を設定します。
    - 通常
    - オフ
    - 低速

    注: 詳細については、「SRM ユーザ ガイド」を参照してください。
11. （オプション）［履歴データの保持］チェック ボックスをオンにします。
12. ［保存］をクリックすると、ポリシーにテストが追加されます。

    テストが保存されます。
13. （オプション）追加するテストごとに同じ手順を繰り返します。
14. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

関連項目:

SRM テストの変更 (P. 308)
SRM ポリシーへのしきい値定義の追加 (P. 310)
SRM しきい値定義の変更 (P. 311)
SRM 制御設定の定義 (P. 312)

SRM テストの変更

既存の SRM テストは変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 変更するテストが含まれるポリシーを［利用可能ポリシー］テーブルから選択します。

   ［サマリ］ページが表示されます。

3. ［テスト］タブをクリックします。

   ［テスト モニタ］ページが表示されます。

4. 変更するテストを選択し、［アクション］をクリックして、［変更］を選択します。

   ［編集］ダイアログ ボックスが表示されます。

5. 必要に応じてテストを変更し、［保存］をクリックします。

   テストが更新されます。

6. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM テストのコピー

既存の SRM テストはコピーすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. コピーするテストが含まれるポリシーを［利用可能ポリシー］テーブルから選択します。

   ［サマリ］ページが表示されます。

3. ［テスト］タブをクリックします。

   ［テスト モニタ］ページが表示されます。

4. コピーするテストを選択し、［アクション］をクリックして、［コピー］を選択します。

   コピー ダイアログ ボックスが表示されます。

5. SRM テスト名を入力します。

   SRM テストがコピーされます。

SRM テストの削除

既存の SRM テストは削除することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 削除するテストが含まれるポリシーを［利用可能ポリシー］テーブルから選択します。

   ［サマリ］ページが表示されます。

3. ［テスト］タブをクリックします。

   ［テスト モニタ］ページが表示されます。

4. 削除するテストを選択し、［アクション］をクリックして、［削除］を選択します。

5. アクションを確認します。

   SRM テストが削除されます。

SRM ポリシーへのしきい値定義の追加

SRM ポリシーにはしきい値定義を追加することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックし、［しきい値モニタ］ツールバーの［+］（新規）をクリックします。

   ［しきい値モニタの詳細］ダイアログ ボックスが表示されます。

4. 以下のしきい値モニタ設定を行います。

   名前

   しきい値モニタ名を定義します。

   属性

   使用する属性を指定します。

   演算子

   使用する演算子を指定します。

   警告値

   使用する警告値を定義します。

   マイナー値

   使用するマイナー値を定義します。

   メジャー値

   使用するメジャー値を定義します。

   重大値

   使用する重大値を定義します。

   致命的値

   使用する致命的値を定義します。

5. ［保存］をクリックすると、ポリシーにしきい値定義が追加されます。

   しきい値定義が保存されます。

6. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM しきい値定義の変更

既存の SRM しきい値定義は変更することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. 変更するしきい値定義が含まれるポリシーを[利用可能ポリシー]テーブルから選択します。

   ［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックします。

   ［しきい値モニタ］ページが表示されます。

4. 変更するしきい値定義を選択し、［アクション］をクリックして、［変更］を選択します。

   ［編集］ダイアログ ボックスが表示されます。

5. 必要に応じてしきい値定義を変更し、［保存］をクリックします。

   しきい値定義が更新されます。

6. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM 制御設定の定義

SRM 制御設定では、通常は svcrsp.cf ファイルで制御する、以下のような AIM 動作のさまざまな要素を定義します。

- セキュリティ設定
- ログ レベル
- インデックス予約

SRM ポリシー内に定義されている制御設定は、ポリシーが適用されるすべてのマシンに適用されます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. 目的のポリシーのページで［制御設定］タブをクリックします。

   ［制御］ペインが表示されます。

4. 以下の制御設定を行います。

最大スレッド数

テストを実行する際に jcollector が使用するスレッドの数を指定します。

ログ レベル

SRM AIM のログ レベルを指定します。デフォルトは [警告] です。

外部スクリプトを許可する

外部スクリプトの実行を許可するかどうかを指定します。

ファイル I/O テストの実行を許可する

ファイル I/O テストの実行を許可するかどうかを指定します。

信頼できない SSL 証明書を許可する

信頼された SSL 証明書がないサイトでの SSL テストを許可するかどうかを指定します。

Java bin の場所

Java 実行可能ファイルの場所を定義します。

注: AIX 上の完全パスおよびバイナリを指定してください。

環境内の CLASSPATH の上書き

ロードする追加クラスを定義します。 定義されない場合、環境内の CLASSPATH を上書きします。

コレクタなし

SystemEDGE で jcollector を開始するかどうかを指定します。

JRE 内部キャッシュのバイパス

JRE 内部キャッシュをバイパスするかどうかを指定します。

IPv4 (HP-UX) 用の TOS なし

TOS を無効にするかどうかを指定します。

共有メモリ名

共有メモリの ID を定義します。

予約されたテスト インデックス

テスト インデックスの予約済み範囲を定義します。

制御設定が定義されます。

5. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

新しい SRM テスト定義テンプレートの定義

SRM テスト定義テンプレートは、作成してポリシーにインポートすることができます。 これによって複数のポリシーでテストを再利用できるようになり、テストを何回もセットアップする必要がありません。

新しい SRM テスト定義テンプレートを定義する方法

1. ［リソース］タブをクリックして［設定］ペインを開き、［モニタリング テンプレート］を展開して［サービス レスポンス］をクリックします。

   ［サービス レスポンス］ページが表示されます。

2. ［テスト テンプレート リスト］ツールバーの［+］（新規）をクリックします。

   ［新規サービス レスポンス テスト定義テンプレート］ダイアログ ボックスが表示されます。

3. テスト定義テンプレートの名前と任意の説明、および既存のテンプレートをベースにするかどうかを入力し、［OK］をクリックします。

   テスト定義テンプレートが作成され、［サマリ］ページが表示されます。テンプレートにテストを追加する方法については、「SRM (305P.) ポリシーへのテストの追加」を参照してください。

4. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

関連項目:

SRM ポリシーへのテスト定義テンプレートのインポート (P. 315)
SRM テスト定義テンプレートの変更 (P. 316)
SRM テスト定義テンプレートのコピー (P. 316)
SRM テスト定義テンプレートの名前変更 (P. 317)
SRM テスト定義テンプレートの削除 (P. 318)

SRM ポリシーへのテスト定義テンプレートのインポート

テスト定義テンプレートは SRM ポリシーにインポートすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［テスト］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるテスト モニタのリストが表示されます。

4. ［アクション］をクリックし、［インポート］を選択します。

   テンプレートのインポート ウィザードが表示されます。

5. インポートするテスト テンプレートをドロップダウン リストから選択します。

6. （オプション）インポートする各テスト定義の新しいベース インデックスを定義します。

7. ドロップダウン リストから［競合の解決オプション］を選択し、［次へ］をクリックします。

   ［競合の解決］ページが表示されます。

8. テスト定義の競合を確認し、インデックスの調整を行います。次に、インポートすべきでないテスト定義を選択解除し、［次へ］をクリックします。

   ［サマリ］ページが表示されます。

9. インポートするテスト定義を確認し、［終了］をクリックしてインポート プロセスを完了します。

10. ［ポリシーの保存］をクリックします。

    ポリシーが保存されます。

SRM テスト定義テンプレートの変更

SRM テスト定義テンプレートは変更することができます。

SRM テスト定義テンプレートを変更する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   テスト テンプレートを含むテスト テンプレート リストが表示されます。

2. 変更するサービス レスポンス テスト テンプレートを選択します。

   テスト テンプレートの［サマリ］ページが表示されます。

3. ［テスト］タブをクリックし、変更するテスト モニタを選択します。次に、［アクション］をクリックし、［変更］を選択します。

   ［編集］ダイアログ ボックスが表示されます。

4. 必要に応じて設定を変更し、［保存］をクリックします。

5. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

SRM テスト定義テンプレートのコピー

SRM テスト定義テンプレートはコピーすることができます。

SRM テスト定義テンプレートをコピーする方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   テスト テンプレートを含むテスト テンプレート リストが表示されます。

2. コピーするサービス レスポンス テスト テンプレートを選択します。

   テスト テンプレートの［サマリ］ページが表示されます。

3. ［テスト］タブをクリックし、コピーするテストを選択します。次に、［アクション］をクリックし、［コピー］を選択します。［設定］ペインでテスト テンプレートを右クリックし、［コピー］を選択する方法もあります。

   ［コピー］ダイアログ ボックスが表示されます。

4. テスト定義テンプレートの新しい名前を入力し、［OK］をクリックします。

   テスト定義テンプレートがコピーされ、テスト テンプレート リストに表示されます。

SRM テスト定義テンプレートの名前変更

SRM テスト定義テンプレートの名前は変更することができます。

SRM テスト定義テンプレートを名前変更する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   テスト テンプレートを含むテスト テンプレート リストが表示されます。

2. 名前を変更するサービス レスポンス テスト テンプレートを選択します。

   テスト テンプレートの［サマリ］ページが表示されます。

3. ［テスト］タブをクリックし、名前を変更するテストを選択します。次に、［アクション］をクリックし、［名前の変更］を選択します。［設定］ペインでテスト テンプレートを右クリックし、［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。

4. テスト定義テンプレートの新しい名前を入力し、［OK］をクリックします。

   確認のメッセージが表示され、テスト定義テンプレートの名前が変更されたことが通知されます。

SRM テスト定義テンプレートの削除

SRM テスト定義テンプレートは削除することができます。

SRM テスト定義テンプレートを削除する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   テスト テンプレートを含むテスト テンプレート リストが表示されます。

2. 削除するサービス レスポンス テスト テンプレートを選択します。

   テスト テンプレートの［サマリ］ページが表示されます。

3. ［テスト］タブをクリックし、削除するテストを選択します。次に、［アクション］をクリックし、［削除］を選択します。［設定］ペインでテスト テンプレートを右クリックし、［削除］を選択することもできます。

   警告メッセージが表示されます。

4. ［OK］をクリックして削除を確定します。

   確認メッセージが表示されます。これで、テスト テンプレートは削除されます。

新しい SRM しきい値定義テンプレートの定義

SRM しきい値定義テンプレートは、作成してポリシーにインポートすることができます。これによって複数のポリシーでしきい値を再利用できるようになり、しきい値を何回もセットアップする必要がありません。

新しい SRM しきい値定義テンプレートを定義する方法

1. ［設定］ペインを開き、［モニタリング テンプレート］を展開して、［サービス レスポンス］をクリックします。

   ［サービス レスポンス］ページが表示されます。

2. ［しきい値テンプレート リスト］ツールバーの［+］（新規）をクリックします。

   ［新規サービス レスポンスしきい値定義テンプレート］ダイアログ ボックスが表示されます。

3. しきい値定義テンプレートの名前と任意の説明、および既存のテンプレートをベースにするかどうかを入力し、［OK］をクリックします。

   しきい値定義テンプレートが作成され、［サマリ］ページが表示されます。 テンプレートにしきい値定義を追加する方法については、「SRM (310P.)ポリシーへのしきい値定義の追加」を参照してください。

4. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

関連項目:

SRM ポリシーへのしきい値定義テンプレートのインポート (P. 319)
SRM しきい値定義テンプレートの変更 (P. 320)
SRM しきい値定義テンプレートのコピー (P. 321)
SRM しきい値定義テンプレートの名前変更 (P. 321)
SRM しきい値定義テンプレートの削除 (P. 322)

SRM ポリシーへのしきい値定義テンプレートのインポート

しきい値定義テンプレートは SRM ポリシーにインポートすることができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［SystemEDGE］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックします。

   ［サマリ］ページが開き、ポリシーによって管理されるしきい値モニタのリストが表示されます。

4. ［アクション］をクリックし、［インポート］を選択します。

   テンプレートのインポート ウィザードが表示されます。

5. インポートするしきい値テンプレートをドロップダウン リストから選択します。
6. インデックス競合の処理方法を選択し、［次へ］をクリックします。

   ［競合の解決］ページが表示されます。
7. しきい値定義の競合を確認し、しきい値定義名の調整を行います。次に、インポートすべきでないしきい値定義を選択解除し、［次へ］をクリックします。

   ［サマリ］ページが表示されます。
8. インポートするしきい値定義を確認し、［終了］をクリックしてインポート プロセスを完了します。
9. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

SRM しきい値定義テンプレートの変更

SRM しきい値定義テンプレートは変更することができます。

SRM しきい値定義テンプレートを変更する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   しきい値テンプレートを含むしきい値テンプレート リストが表示されます。
2. 変更するサービス レスポンスしきい値テンプレートを選択します。

   テスト テンプレートの［サマリ］ページが表示されます。
3. ［しきい値］をクリックし、変更するしきい値モニタを選択します。次に、［アクション］をクリックし、［変更］を選択します。

   ［しきい値モニタの詳細］ダイアログ ボックスが表示されます。
4. 必要に応じて設定を変更し、［保存］をクリックします。
5. ［テンプレートの保存］をクリックします。

   テンプレートが保存されます。

SRM しきい値定義テンプレートのコピー

SRM しきい値定義テンプレートはコピーすることができます。

SRM しきい値定義テンプレートをコピーする方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   しきい値テンプレートを含むしきい値テンプレート リストが表示されます。

2. コピーするサービス レスポンスしきい値テンプレートを選択します。

   しきい値テンプレートの［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックし、コピーするしきい値モニタを選択します。次に、［アクション］をクリックし、［コピー］を選択します。［設定］ペインでモニタリング テンプレートを右クリックし、［コピー］を選択することもできます。

   ［コピー］ダイアログ ボックスが表示されます。

4. しきい値定義テンプレートの新しい名前を入力し、［OK］をクリックします。

   しきい値定義テンプレートがコピーされ、しきい値テンプレート リストに表示されます。

SRM しきい値定義テンプレートの名前変更

SRM しきい値定義テンプレートの名前は変更することができます。

SRM しきい値定義テンプレートの名前を変更する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   しきい値テンプレートを含むしきい値テンプレート リストが表示されます。

2. 名前を変更するサービス レスポンスしきい値テンプレートを選択します。

   しきい値テンプレートの［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックし、名前を変更するしきい値モニタを選択します。次に、［アクション］をクリックし、［名前の変更］を選択します。［設定］ペインでテスト テンプレートを右クリックし、［名前の変更］を選択することもできます。

   ［名前の変更］ダイアログ ボックスが表示されます。

4. しきい値定義テンプレートの新しい名前を入力し、［OK］をクリックします。

   確認のメッセージが表示され、しきい値定義テンプレートの名前が変更されたことが通知されます。

SRM しきい値定義テンプレートの削除

SRM しきい値定義テンプレートは削除することができます。

SRM しきい値定義テンプレートを削除する方法

1. ［設定］ペインを開いて［モニタリング テンプレート］を展開します。次に、［サービス レスポンス］をクリックし、［テスト定義テンプレート］を展開します。

   しきい値テンプレートを含むしきい値テンプレート リストが表示されます。

2. 削除するサービス レスポンスしきい値テンプレートを選択します。

   しきい値テンプレートの［サマリ］ページが表示されます。

3. ［しきい値］タブをクリックし、削除するしきい値モニタを選択します。次に、［アクション］をクリックし、［削除］を選択します。［設定］ペインでモニタリング テンプレートを右クリックし、［削除］を選択することもできます。

   警告メッセージが表示されます。

4. ［OK］をクリックして削除を確定します。

   確認メッセージが表示されます。しきい値テンプレートが削除されます。

既存の SRM 設定のインポート

既存の Service Availability （SA） 2.0 AIM を SRM 3.1.0 にアップグレードした後に、前の SA 2.0 設定をインポートし、それを SRM 3.1.0 ポリシーに変換することができます。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して［サービス レスポンス］をクリックします。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］ツールバーの［+］（新規）をクリックします。

   ［新規サービス レスポンス ポリシー］ダイアログ ボックスが表示されます。

3. ［インポート］をクリックし、ポリシーのインポート元のマシンをリストから選択して、［OK］をクリックします。
4. 名前と任意の説明を入力し、［OK］をクリックすると、インポート プロセスは完了します。
5. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

マシンへのポリシーの適用

設定ポリシーを作成したら、企業全体でマシンに適用する必要があります。設定ポリシーを適用すると、すべてのポリシー設定が含まれたコンパイル済み設定ファイルが、指定されたすべてのエージェント マシンに CA Server Automation によってプッシュされます。新規ポリシーは、自動エージェント ウォーム スタート後に実装されます。

以下のいずれかが該当する場合は、マシンにポリシーを再適用できます。

- ポリシーを更新した。
- エージェント マシン上の設定が変更されたことを知らせる通知を受信した。

次の手順に従ってください:

1. ［リソース］タブをクリックして［設定］ペインを開き、［ポリシー］を展開して、［SystemEDGE］または［サービス レスポンス］を選択します。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. 適用するポリシーを選択します。

   ［ポリシー詳細］が右ペインに表示されます。

4. ［アクション］をクリックし、［適用］を選択します。

   ポリシーを適用するマシンを選択するためのタブが表示されます。［このポリシーを実行しているマシンを更新］タブでは、すでにポリシーを実行しているマシンにポリシーを適用できます。［このポリシーを実行していないマシンに適用］タブでは、ポリシーのないマシンまたは別のポリシーを使用しているマシンにポリシーを適用できます。

5. （オプション）［このポリシーを実行しているマシンを更新］タブから、以下のいずれかを実行します。

   - 現在ポリシーを実行しているすべてのマシンにこのポリシーを展開するには、［このポリシーを使用してすべてのマシンを更新］を選択します。 このオプションは、グローバルに適用する設定ポリシーの変更を行った場合に便利です。
   - 以下の条件のいずれかを満たすマシンのみを更新するには、［選択したマシン グループを更新］を選択します。
     - ポリシーの期限切れバージョンを実行しているマシン
     - ポリシー例外が適用されているマシン
     - ポリシーの現在のバージョンを実行しているマシン
     - このポリシーに対して設定エラーがあるマシン

     これらのオプションのいずれかを選択します。 ポリシー例外は、適用されるポリシー内で示されていないエージェントにユーザがポイント設定変更を適用すると発生します。
   - ［詳細（手動でマシンを選択）］を選択して、［マシンを選択］ペインにポリシーを再割り当てするマシンを手動で追加します。

6. （オプション）［このポリシーを実行していないマシンに適用］タブから、ポリシーを適用するマシンを選択します。
7. ［ポリシーの適用］をクリックします。

   ポリシーの適用が開始されます。

ポリシー適用の進捗状況の確認

個々のポリシーに対して、ポリシー適用操作の進捗状況を詳細に確認できます。

次の手順に従ってください:

1. ［リソース］タブを選択して［設定］ペインを開き、［ポリシー］を展開して、［SystemEDGE］または［サービス レスポンス］を選択します。

   ［利用可能ポリシー］ページが表示されます。
2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。
3. ［管理対象マシン］タブをクリックします。

   ［管理対象マシン］ページに現在ポリシーを実行しているマシンのリストが表示され、ここで設定ステータスを表示できます。
4. （オプション）［例外の表示］をクリックします。

   ［ポリシー例外］ペインが表示され、ポリシーが最後に適用されてからシステムに適用された SNMP SET を参照できます。

   注: この画面は SystemEDGE ポリシーに対してのみ表示されます。
5. （オプション）［設定の表示］をクリックします。

   ［ポリシー設定］ペインが表示され、エージェントに配信された設定ファイルを参照できます。
6. （オプション）［エラーの表示］をクリックします。

   ［ポリシー エラー］ペインが表示されます。ポリシーを正常に適用できなかった場合、ポリシーが拒否されたときにエージェントによって返されたエラーのリストを参照できます。

適用されるポリシーの設定と表示

ポリシー機能では、個別のサーバ、サーバ グループ、またはサービスに適用されたポリシーおよびテンプレートを管理できます。 以下の操作を実行できます。

- ポリシーおよびテンプレートの更新
- 最後のポリシーまたはテンプレートの適用以降の例外を表示します。
- ポリシー設定の表示
- ポリシー エラーの表示
- ポリシーの一括更新
- テンプレートの削除

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. システムまたはサービスを選択します。［リソース］ページをクリックし、［モニタリング ソフトウェア］をクリックします。

   ［マシンの詳細］ページが表示されます。

3. ［ポリシー］をクリックします。

   ［ポリシー］ページに、SystemEDGE と SRM のポリシーおよび SystemEDGE テンプレートのリストが表示されます。

   注:［フィルタ］には、［保留］、［配信］（成功）、［設定完了］、および［失敗］のいずれかの状態である階層型テンプレートのリストが表示されます。

4. ポリシーおよびテンプレートを一括更新できます。［ポリシーとテンプレート］テーブルで、一括更新するポリシーまたはテンプレートを選択し、［アクション］をクリックして以下のいずれかのオプションを選択します。

   - SystemEDGE ポリシーの一括更新
   - サービス レスポンス ポリシーの一括更新
   - SystemEDGE テンプレートの一括更新
   - テンプレートの一括削除

   注: ポリシーが単一のサーバに適用されている場合は、ポリシー名を入力するためのプロンプトが表示されます。

   ポリシーの一括更新:

   選択したポリシーをサービス グループに適用する場合には、ポリシーを適用するマシンを選択するオプションがあります。

   テンプレートの一括更新:

   ［利用可能なテンプレート］からテンプレートを選択するオプションがダイアログ ボックスに表示されます。 テンプレートを選択した後に、以下のいずれかのオプションをクリックします。

   ［既存の設定を選択されたテンプレートで置換します］

   すべてのマシンに適用されている既存のテンプレートを削除し、選択したテンプレートをすべてのマシンに適用します。

   ［選択されたテンプレートを既存の設定に追加します］

   選択したテンプレートを追加します。選択したテンプレートのいずれかがマシン設定の一部としてすでに適用されている場合は、それらのテンプレートが再適用されます。

   テンプレートの一括削除

   マシンに適用されている既存のテンプレートを削除します。

5. ［ポリシーの適用］をクリックして、マシンにポリシーまたはテンプレートを適用します。

   ［ポリシー］ページで、ポリシーまたはテンプレートのマシンへの適用に関する進捗状況を確認できます。

6. （オプション）［設定の表示］アイコンをクリックします。

   ［ポリシー設定］ページが表示されます。テンプレートを含むマシンでは、ポリシー、テンプレート、および SystemEDGE 設定ファイルが表示されます。 サービス レスポンス モニタを含むマシンでは、さらにサービス レスポンス モニタの設定ファイルも表示されます。

7. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

ポリシーを以前のバージョンに戻す

ポリシーは以前のバージョンに戻すことができます。

次の手順に従ってください:

1. ［リソース］タブを選択して［設定］ペインを開き、［ポリシー］を展開して、［SystemEDGE］または［サービス レスポンス］を選択します。

   ［利用可能ポリシー］ページが表示されます。

2. ［利用可能ポリシー］テーブルでポリシーを選択します。

   ポリシーの［サマリ］ページが表示されます。

3. ［バージョン］タブをクリックします。

   ［バージョン］ページが表示されます。

4. リストアするバージョンをテーブルから選択し、［最新のバージョンにする］をクリックします。

   確認のメッセージが表示されます。 ［OK］をクリックします。 ポリシーの新しいバージョンが作成され、サマリ ページが表示されます。

5. （オプション）バージョンの新しいコピーを作成することができます。［利用可能ポリシー］テーブルからバージョンを選択し、［コピー］をクリックします。

   ［コピー］ダイアログ ボックスが表示されます。

6. ポリシーの新しい名前を入力し、［OK］をクリックします。

   ポリシーがコピーされ、［設定］ペインのポリシー ツリーに追加されます。 新しいコピーのサマリ ページが表示されます。

7. ［ポリシーの保存］をクリックします。

   ポリシーが保存されます。

新規インスタンスのデフォルト ポリシーの指定

検出されたすべての新しいインスタンスについて、単一のデフォルト ポリシーを設定することができます。SystemEDGE または SRM のインストール中または展開中にポリシーを指定しなかった場合、または指定したポリシーが利用可能でない場合、デフォルト ポリシーが配信されます。

デフォルト ポリシーを指定する方法

1. ［設定］ペインを開き、［ポリシー］を展開して、［SystemEDGE］または［サービス レスポンス］を選択します。

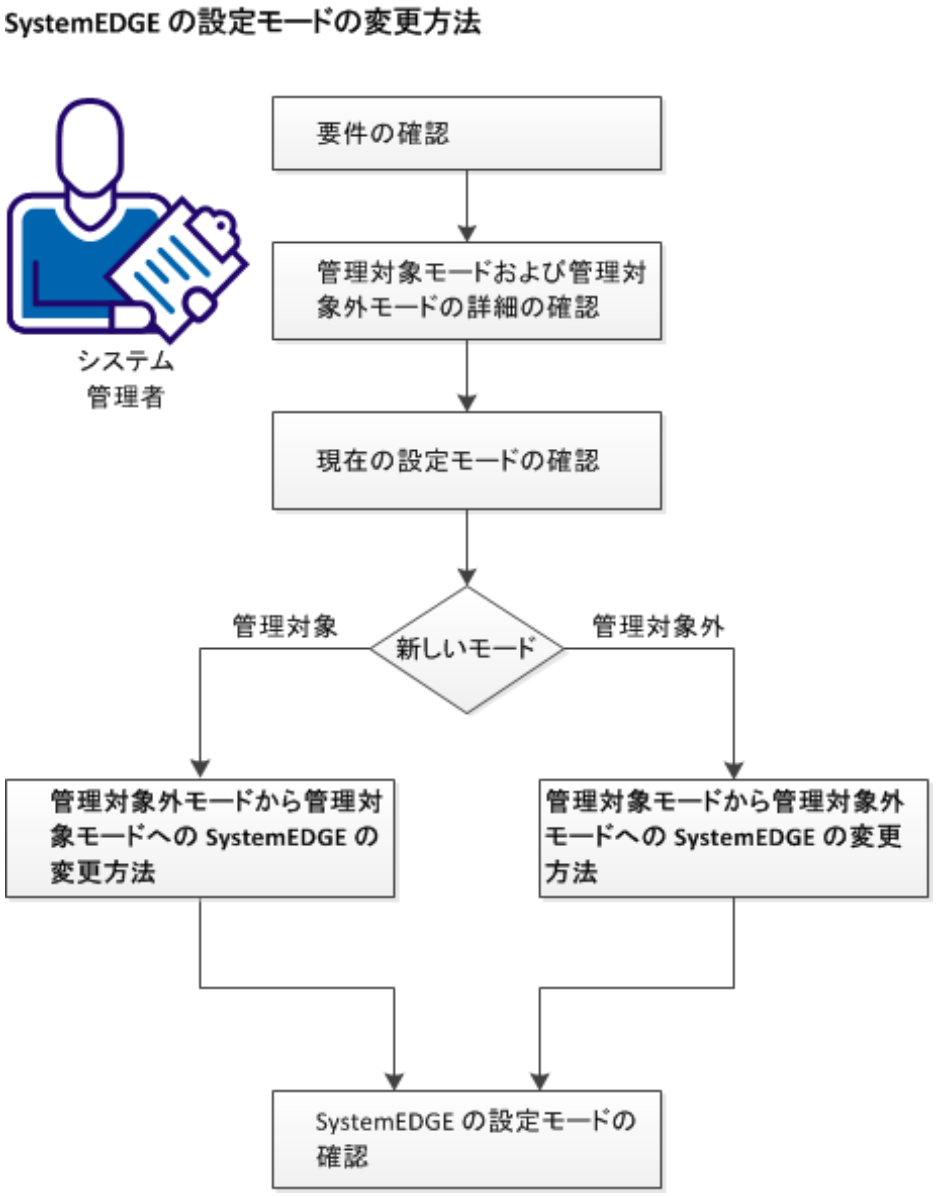
   ［利用可能ポリシー］ページが表示されます。

2. ［デフォルト ポリシー］セクションで、使用するポリシーを［デフォルト ポリシー］ドロップダウン リストから選択し、［適用］をクリックします。

   デフォルト ポリシーが適用されます。

SystemEDGE の設定モードの変更方法

SystemEDGE の設定モードの変更が必要になる場合があります。 以下の図は、設定モードを変更するために必要なアクションの概要を示しています。



以下の手順に従います。

要件の確認

SystemEDGE の設定モードを変更する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA SystemEDGE に関する基礎知識がある。
- モニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- 管理対象ノードでモニタリング エージェント（CASystemEDGE）にアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- CA Server Automation によって関連するシステムがすべて検出されている。

管理対象モードおよび管理対象外モードの詳細の確認

以下の用語を確認してください。このシナリオでは、管理対象外モードおよび管理対象モードという用語は、SystemEDGE の設定で使用しています。

管理対象外モード

特定のサーバの SystemEDGE 設定は CA Server Automation のポリシー設定によって管理されません。 sysedge.cf ファイルを編集して、設定を変更することができます。

管理モード

特定のサーバの SystemEDGE 設定は CA Server Automation のポリシー設定によって管理されます。CA Server Automation マネージャの［ポリシー設定］で SystemEDGE の設定を指定し、これをネットワーク内の適切なサーバに配布します。 sysedge.cf ファイルをローカルで編集すると、その変更は次回のポリシー配布の際に CA Server Automation によって上書きされます。

SystemEDGE の設定モードに影響する以下の場合を考慮します。

- 製品メディアから一般的な SystemEDGE インストールを実行する場合、SystemEDGE はインストール後に管理対象外モードで実行されるよう設定されます。
- 製品メディアからカスタマイズした SystemEDGE インストールを実行する場合、管理対象モードを使用するようマネージャ システムを設定できます。 マネージャ システムを指定して、CA Server Automation によってインストール後に SystemEDGE が検出された場合、SystemEDGE はポリシー設定に自動的に登録され、管理対象モードで実行されます。
- リモート展開を使用して SystemEDGE をリモート システムにインストールする場合、展開ジョブで SystemEDGE の設定モードを指定できます。 デフォルト値は管理対象モードです。

重要: ［エクスプローラ］ペインには、管理対象と管理対象外のフォルダが表示されます。ここには、CA Server Automation によってポーリングされるサーバ（管理対象）と、ポーリングされないサーバ（管理対象外）が一覧表示されます。 このプロパティは、SystemEDGE 設定の管理対象モードまたは管理対象外モードとは異なります。 ［エクスプローラ］ペインのサーバの管理対象または管理対象外のステータスは、SystemEDGE の設定モードには影響しません。 SystemEDGE 設定ファイルの特定のエントリは、SystemEDGE の設定モードを示します。

SystemEDGE の現在の設定モードの確認

以下の手順では、SystemEDGE の設定モードを確認する方法について説明します。

以下の用語がこれらのユース ケース全体で使用されます。

静的な sysedge.cf ファイル

インストーラによって導入されるファイルを示します。このファイルは *Installed_Dir*¥SystemEDGE¥config ディレクトリに置かれます。

デフォルト：

Windows： C:¥Program Files¥CA¥SystemEDGE¥config

UNIX/Linux： /opt/CA/SystemEDGE/config

動的な sysedge.cf ファイル

現行の SystemEDGE 設定ファイルを示します。このファイルは *Data_Dir*¥port<*number*> ディレクトリに置かれます。

デフォルト：

Windows： C:¥Users¥Public¥CA¥SystemEDGE¥port161

UNIX/Linux： /opt/CA/SystemEDGE/config/port161

次の手順に従ってください:

1. SystemEDGE の設定モードを確認するサーバにログインします。
2. SystemEDGE の「data」ディレクトリに移動して、port<*number*> ディレクトリを開きます。Windows の場合は、SystemEDGE のコントロール パネルから data ディレクトリの sysedge.cf ファイルを開くことができます。

   注:「data」ディレクトリにある動的な sysedge.cf ファイルは、「config」ディレクトリにある静的な sysedge.cf ファイルとは異なります。
3. port<*number*> ディレクトリにある動的な sysedge.cf ファイルを開きます。

   SystemEDGE が管理対象モードで実行される場合、最初の行には制御値（ctrl_value）を指定します。

例：

```
ctrl_value 0x9e30d00e

# Generated file - DO NOT EDIT
#
# Configuration file generated on 2012:03:27 05:37
#
# Generated from default.generic.0.prof
#
version 5.7
```

SystemEDGE が管理対象外モードで実行される場合、最初の行にはバージョンを指定します。

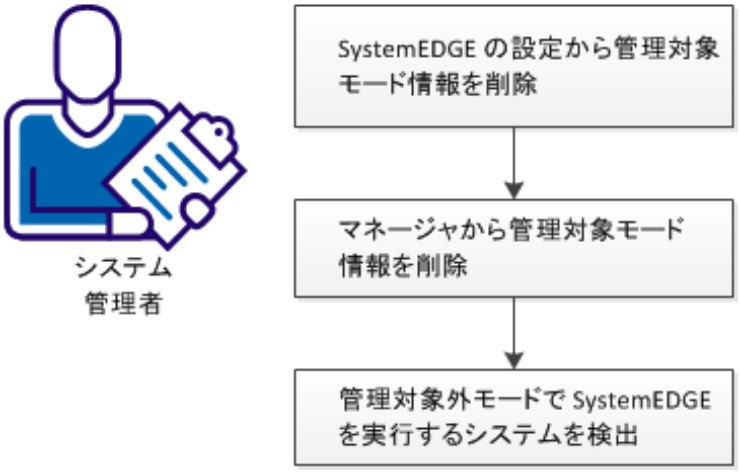
例：

```
version 5.7
```

管理対象モードから管理対象外モードへの SystemEDGE の変更方法

以下の図は、管理対象外モードに変更するために必要なアクションの概要を示しています。

管理対象モードから管理対象外モードへの SystemEDGE の変更方法



以下の手順に従います。

SystemEDGE の設定からの管理対象モードの情報の削除 (P. 335)
マネージャからの管理対象モードの情報の削除 (P. 336)
管理対象外モードで SystemEDGE を実行するシステムの検出 (P. 337)

SystemEDGE の設定からの管理対象モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. SystemEDGE の設定モードを変更するサーバにログインします。
2. 便利な場所に以下のバックアップ ディレクトリを作成します。

   ```
   data.backup
   config.backup
   ```

3. 通常の方法で SystemEDGE を停止します。
4. SystemEDGE の「data」ディレクトリに移動して、port<*number*> ディレクトリを開きます。 デフォルトのディレクトリは port161 です。

   ディレクトリの内容が一覧表示されます。

5. data.backup ディレクトリに以下のファイルを移動させて、port<*number*> ディレクトリに表示されないようにします。

   ```
   .sysedge.id
   sysedge.cf
   ```

6. SystemEDGE の「config」ディレクトリに移動します。

   ディレクトリの内容が一覧表示されます。

7. config.backup ディレクトリに以下のファイルをコピーします。

   ```
   sysedge.cf
   ```

8. 「config」ディレクトリに移動して、テキスト エディタで sysedge.cf ファイルを開き、ファイルの末尾までスクロールします。

9. 以下の行を削除します。

   manager_name *<hostname of the manager>*

10. ファイルを保存して、SystemEDGE を起動します。

    SystemEDGE によって「data」ディレクトリに管理対象モードの情報のない sysedge.cf ファイルが作成されます。

マネージャからの管理対象モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. CA Server Automation のユーザ インターフェースにログインし、［管理］に移動します。

   ［リソース］タブが開き、［エクスプローラ］ペインが表示されます。

2. SystemEDGE の設定を変更するサーバの名前を［検索］フィールドへ入力し、  （検索）をクリックします。

   ［検索］ウィンドウが開き、検索結果が表示されます。

3. 検索結果のいずれかをクリックします。

   該当サーバの［リソース］ページが開き、［クイック スタート］パネルが表示されます。

4. ［システムから削除］をクリックします。

   該当サーバが［エクスプローラ］ペインに表示されなくなります。 管理対象モードの情報を含めて、サーバに関連するすべてのオブジェクトがマネージャから削除されます。

管理対象外モードで SystemEDGE を実行するシステムの検出

以下の手順では、管理対象外モードで実行されているサーバを再検出する方法について説明します。

次の手順に従ってください:

1. CA Server Automation のユーザ インターフェースにログインし、［管理］に移動します。

   ［リソース］タブが開き、［エクスプローラ］ペインが表示されます。

2. ［データ センター］を右クリックして、［管理］-［検出］-［サーバ］を選択します。

   ［検出］ウィンドウが開きます。

3. 前の手順で削除したサーバの名前を入力し、［終了］クリックします。

   CA Server Automation によって、SystemEDGE が管理対象外モードで実行されているサーバが検出されます。

   CA Server Automation で検出が完了すると、検出されたサーバの SystemEDGE は［ポリシー設定］に登録されていないことが確認できます。 SystemEDGE は管理対象外モードで実行されています。

4. ［エクスプローラ］ペインのサーバ名をダブルクリックします。

   該当サーバの［リソース］ページが表示されます。

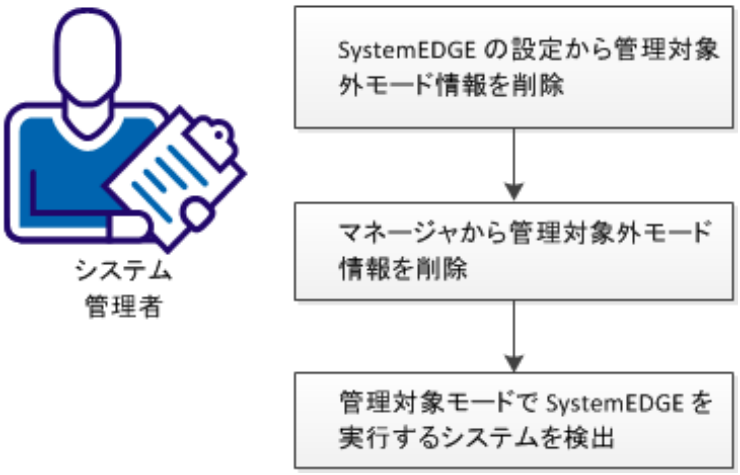
5. ［サマリ］タブに切り替えて、CA Server Automation よってサーバが正しく検出されたことを確認します。 必要に応じて、CA Server Automation がサーバのモニタリングに使用している別の SNMP コミュニティを選択できます。

   これで、sysedge.cf 設定ファイルを編集して該当サーバの SystemEDGE を設定できるようになります。

管理対象外モードから管理対象モードへの SystemEDGE の変更方法

以下の図は、管理対象モードに変更するために必要なアクションの概要を示しています。

管理対象外モードから管理対象モードへの SystemEDGE の変更方法



以下の手順に従います。

SystemEDGE の設定からの管理対象外モードの情報の削除 (P. 338)
マネージャからの管理対象外モードの情報の削除 (P. 339)
管理対象モードで SystemEDGE を実行するシステムの検出 (P. 340)

SystemEDGE の設定からの管理対象外モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象外モードの情報を削除して、サーバを管理対象モードに変更できるよう準備する方法について説明します。

次の手順に従ってください:

1. SystemEDGE の設定モードを変更するサーバにログインします。
2. 便利な場所に以下のバックアップ ディレクトリを作成します。

   ```
   data.backup
   config.backup
   ```

3. 通常の方法で SystemEDGE を停止します。

4. SystemEDGE の「data」ディレクトリに移動して、port<*number*> ディレクトリを開きます。 デフォルトのディレクトリは port161 です。

   ディレクトリの内容が一覧表示されます。

5. data.backup ディレクトリに以下のファイルを移動させて、port<*number*> ディレクトリに表示されないようにします。

   ```
   sysedge.cf
   ```

6. SystemEDGE の「config」ディレクトリに移動します。

   ディレクトリの内容が一覧表示されます。

7. config.backup ディレクトリに以下のファイルをコピーします。

   ```
   sysedge.cf
   ```

8. 「config」ディレクトリに移動して、テキスト エディタで sysedge.cf ファイルを開き、ファイルの末尾までスクロールします。

9. 以下の行を追加します。

   ```
   manager_name <hostname of the manager>
   ```

10. ファイルを保存して、SystemEDGE を起動します。

    SystemEDGE によって「data」ディレクトリに sysedge.cf ファイルが作成されます。

マネージャからの管理対象外モードの情報の削除

以下の手順では、特定のサーバの SystemEDGE の設定から管理対象外モードの情報を削除する方法について説明します。

次の手順に従ってください:

1. CA Server Automation のユーザ インターフェースにログインし、［管理］に移動します。

   ［リソース］タブが開き、［エクスプローラ］ペインが表示されます。

2. SystemEDGE の設定を変更するサーバの名前を［検索］フィールドへ入力し、（検索）をクリックします。

   ［検索］ウィンドウが開き、検索結果が表示されます。

3. 検索結果のいずれかをクリックします。

   該当サーバの［リソース］ページが開き、［クイック スタート］パネルが表示されます。

4. ［システムから削除］をクリックします。

   該当サーバが［エクスプローラ］ペインに表示されなくなります。サーバに関連するすべてのオブジェクトがマネージャから削除されます。

管理対象モードで SystemEDGE を実行するシステムの検出

以下の手順では、管理対象モードで SystemEDGE を実行するサーバを再検出する方法について説明します。

次の手順に従ってください:

1. CA Server Automation のユーザ インターフェースにログインし、［管理］に移動します。

   ［リソース］タブが開き、［エクスプローラ］ペインが表示されます。

2. ［データ センター］を右クリックして、［管理］-［検出］-［サーバ］を選択します。

   ［検出］ウィンドウが開きます。

3. 前の手順で削除したサーバの名前を入力し、［終了］クリックします。

   CA Server Automation によってサーバが検出されます。

   CA Server Automation で検出が完了すると、検出されたサーバの SystemEDGE が［ポリシー設定］に登録されていることが確認できます。SystemEDGE は管理対象モードで実行されています。

4. ［エクスプローラ］ペインのサーバ名をダブルクリックします。

   該当サーバの［リソース］ページが表示されます。

5. ［サマリ］タブに切り替えて、CA Server Automation よってサーバが正しく検出されたことを確認します。 必要に応じて、CA Server Automation がサーバのモニタリングに使用している別の SNMP コミュニティを選択できます。

SystemEDGE の設定モードの確認

基本的には、「現在の設定モードの確認 (P. 333)」の手順を繰り返すことができます。

SystemEDGE が管理対象外モードで実行される場合、「data」ディレクトリの動的な sysedge.cf ファイルの最初の行にはバージョンを指定します。

例

```
リリース 5.7.1
```

SystemEDGE が管理対象モードで実行される場合、最初の行には制御値（ctrl_value）を指定します。

例

```
ctrl_value 0x9e30d00e

# Generated file - DO NOT EDIT
#
# Configuration file generated on 2012:03:27 05:37
#
# Generated from default.generic.0.prof
#
リリース 5.7.1
```

ディスカバリ プロセス中に、動的な sysedge.cf ファイルの末尾にメタ情報が追加されています。

例

```
template data_directory <path>
data_directory "C:¥Users¥Public¥CA¥SystemEDGE¥"
template default_port CA Portal
default_port 161
template manager_name <name>
manager_name manager_server.mycompany.com
template manager_policy_name <policy>
manager_policy_name default.generic
template manager_policy_version <version>
manager_policy_version 1
```

関連項目:

SystemEDGE の現在の設定モードの確認 (P. 333)

第 6 章: 仮想環境の管理

このセクションには、以下のトピックが含まれています。

Cisco UCS

Cisco Unified Computing System （Cisco UCS）は Cisco のデータ センター ソリューションです。このソリューションでは、ペア ファブリック インターコネクト スイッチを 2 つまでのスイッチ、40 のシャーシおよび 320 のブレード サーバ（ブレード）と統合します。 スイッチ上で実行される Cisco UCS Manager は、ネットワーキング、ストレージおよびブレードの管理機能を提供し、仮想化もサポートします。 CA Server Automation は Cisco UCS と対話し、ハードウェア リソースや健全性とデバイスの統計などの UCS デバイス情報をクエリします。 CA Server Automation は UCS AIM および PMM を使用して、Cisco UCS をサポートします。Cisco UCS インターフェースおよびそれらの操作の詳細については、Cisco UCS のドキュメントを参照してください。

管理者は、管理ユーザ インターフェースまたは dpmutil CLI コマンドのいずれかを使用して、UCS Manager を登録できます。 dpmutil を使用する場合は、nodecfgutil.exe を実行して UCS AIM を設定します。

注: CLI コマンドの詳細については、「リファレンス ガイド」を参照してください。

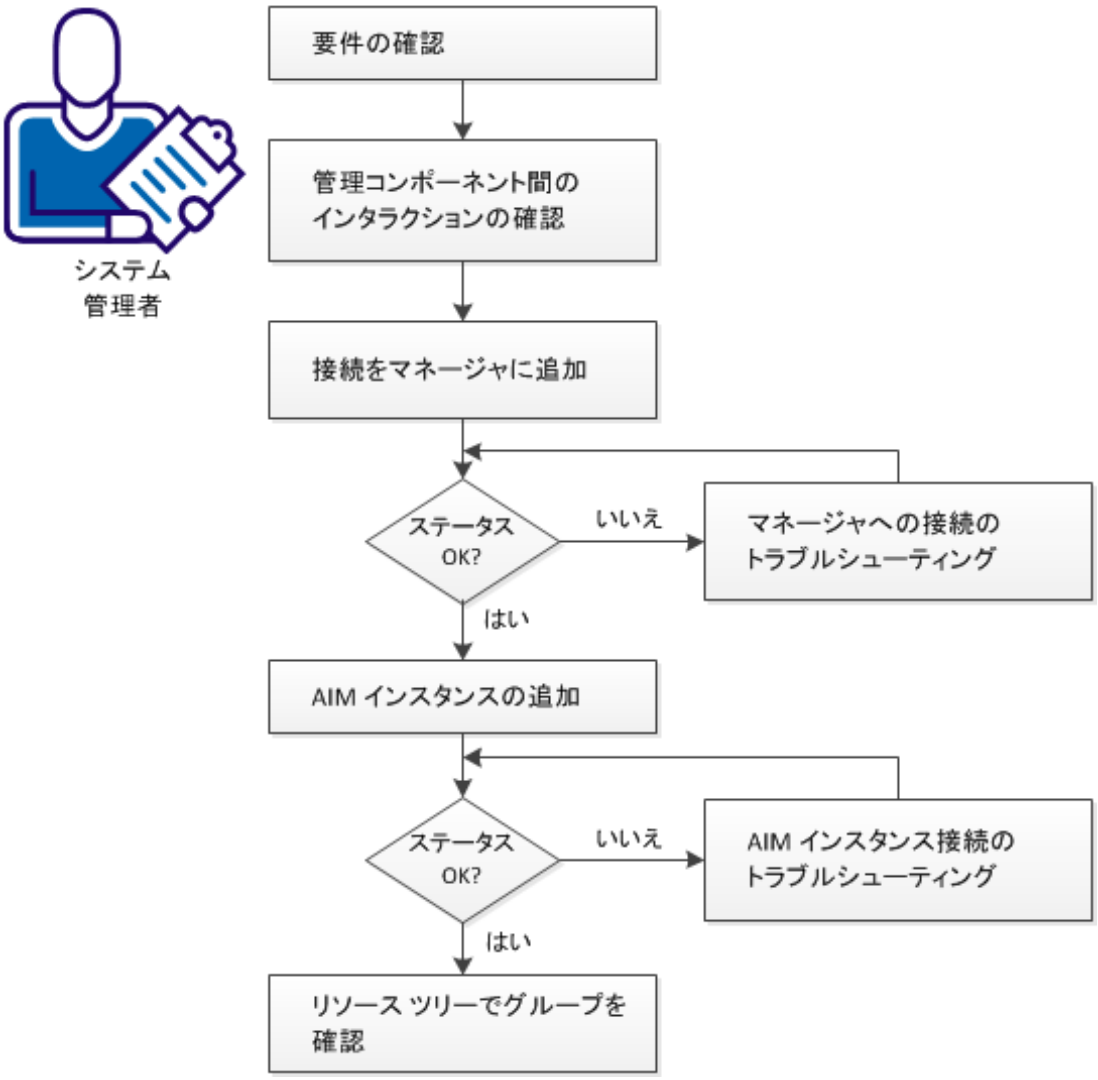
関連項目:

Cisco UCS 管理コンポーネントを設定する方法 (P. 345)
Cisco UCS の管理 (P. 359)

Cisco UCS 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



スイッチ上で実行される Cisco UCS Manager は、ネットワーキング、ストレージおよびブレードの管理機能を提供し、仮想化もサポートします。

CA Server Automation は Cisco UCS と対話し、ハードウェア リソースや健全性とデバイスの統計などの UCS デバイス情報をクエリします。 CA Server Automation は UCS AIM および PMM を使用して、Cisco UCS をサポートします。

以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443

- 使用する環境にあるサーバが正常に実行されていることを確認済みである。
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

関連項目:

Cisco UCS サーバ (P. 347)

Cisco UCS サーバ

Cisco UCS 管理に対する以下の条件を確認します。

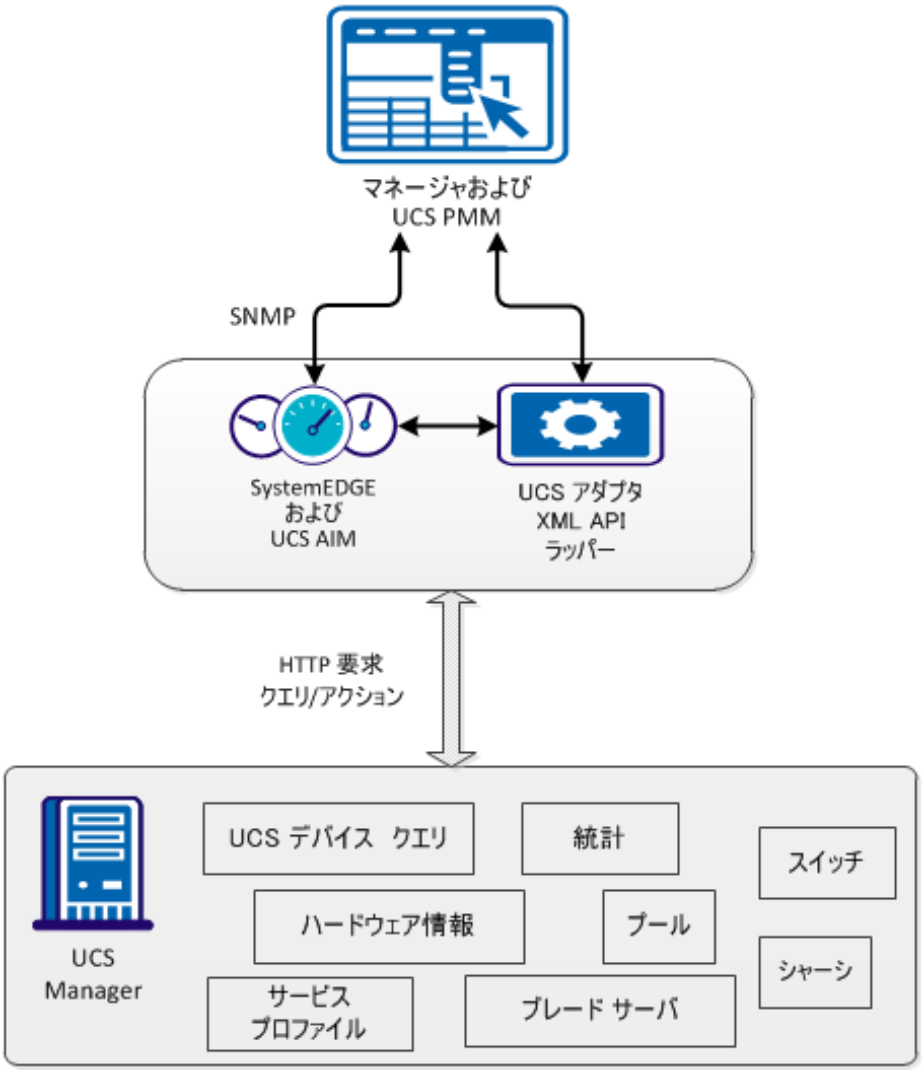
- Cisco Java ユーザ インターフェースを起動して Cisco UCS Manager が実行されていることを確認します。 Cisco Java ユーザ インターフェースを起動するリンクは http://<UCS_Manager_name> または https://<UCS_Manager_name> です。

Cisco UCS 管理コンポーネント間のインタラクション

Cisco UCS 統合では、UCS デバイスおよび統計データの取得やデバイスの設定を行うための SNMP get/set 要求を提供するため、SystemEDGE 用の UCS AIM が必要となります。 UCS プラットフォーム管理モジュール（PMM）からも、UCS デバイスや統計情報のクエリが行われ、管理 DB 内にデータが保存されます。 Cisco UCS Manager とのインタラクション用に、Cisco から XML API が提供されています。

API を使用すると、CA Server Automation でハードウェア、統計、プール（UUID、MAC、WWPN、WWNN）、および UCS Manager サービス プロファイル情報にアクセスできるようになります。

Cisco UCS 管理コンポーネント間のインタラクション



この図は、Cisco UCS の統合コンポーネントを示しています。 UCS アダプタと Cisco UCS Manager 間の通信プロトコルは、HTTP または HTTPS です。

XML API によって、特定のデバイス プロパティの設定や、プールおよびサービス プロファイルの管理を行う機能も提供されます。 プールおよびサービス プロファイルの管理は、プール範囲の競合を検出するために、CA Server Automation で複数の UCS Manager にわたって管理されるユースケースの 1 つです。

マネージャへの Cisco UCS の追加

ユーザ インターフェースの［管理］ページを使用して、Cisco UCS Manager サーバを追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Cisco UCS］を選択します。

3. ［Cisco UCS］ペインのツールバーで （追加）をクリックします。

   ［Cisco Unified Computing System サーバの追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、ポート）を入力し、優先 AIM を指定して、［管理ステータス］（チェック ボックス）をオンにします。

5. 必要なサーバ識別情報を入力して、［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

   注: 接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。 ［はい］をクリックすると、CA Server Automation によってサーバが赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の  （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバ システムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

UCS AIM サーバの登録

CA Server Automation マネージャに Cisco UCS コンポーネントを追加した後、Cisco UCS 環境を管理するために、ユーザ インターフェースの［管理］ページを使用して AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左側のペインの［プロビジョニング］セクションから［Cisco UCS］を選択します。
3. ［UCS AIM サーバ］ペイン ツールバーの (追加) をクリックします。

   ［Cisco Unified Computing System AIM サーバの追加］ダイアログ ボックスが表示されます。
4. ドロップダウン リストから［UCS AIM サーバ］を選択します。

   UCS AIM サーバのリストが表示されます。

5. ドロップダウン リストから［Cisco UCS サーバ］を選択します。

   ［Cisco UCS］ペインに一覧表示されたサーバが［Cisco UCS サーバ］ドロップダウン リストに入力されます。 管理できる UCS サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが登録されます。

   注: インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了したら、Cisco UCS 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの Cisco UCS の確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. Cisco UCS グループを展開します。

   管理対象の Cisco UCS リソースが表示されます。

CA Server Automation で、設定された Cisco UCS 環境を管理する準備が整いました。

Cisco UCS の管理

CA Server Automation と Cisco UCS の統合により、一元化されたユーザ インターフェースから UCS スイッチ、シャーシ、およびブレードを管理することができます。スイッチ上で実行される UCS Manager は、UCS リソースを表示し、クローン作成、スナップショット、電源操作などの管理操作を実行できる場所になります。

このセクションでは、［リソース］ページから Cisco UCS リソースに対して実行できるリソース管理操作について説明します。［リソース］ページには、以下の UCS オブジェクトに関する基本情報が表示されます。

- Cisco UCS サーバ
- UCS Manager サーバ
- シャーシ
- ブレード サーバ
- Fabric Interconnect
- 組織

［サマリ］ページでは、オブジェクトに関連付けられている情報を見ることができます（たとえば、シャーシ サマリではそのブレードを表示でき、ブレード サマリではそのストレージを表示できます）。また、リソースに関連付けられているイベントを見ることができます。

［詳細］ページを利用できる場合は、その他のリソース情報（システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど）を見ることができます。ここで自動化ソースを割り当てた後、デフォルトのアクセス プロファイルと管理プロファイルがシステムに対して自動的に作成され、ディスカバリが実行されます。

リソース管理タスクを実行するための、他のページを表示できる場合もあります。［エクスプローラ］ペイン内のオブジェクトを右クリックして表示されるメニューを使って UCS 管理タスクを実行することもできます。

関連項目:

一元化されたサービス プロファイルを使用する方法 (P. 360)
Cisco UCS リソースの表示 (P. 362)
サービス プロファイルとブレードの関連付け (P. 363)
UCS Manager 設定のバックアップ (P. 364)
vNIC テンプレート (P. 365)
UCS 組織 (P. 365)
UCS プール (P. 366)
ポート プロファイルを管理する方法 (P. 371)
UCS のアクション タイプ (P. 373)

一元化されたサービス プロファイルを使用する方法

CA Server Automation Management Database 内に存在するセントラル サービス プロファイルは、複数の UCS ドメインにわたって設定情報を管理する効率的な方法を提供します。 CA Server Automation ユーザ インターフェースを使用して、UCS Manager から Management Database にサービス プロファイルをインポートするか、Management Database 内にセントラル サービス プロファイルを作成します。

Management Database から、任意の UCS Manager にセントラル サービス プロファイルをエクスポートできます。

セントラル サービス プロファイルの管理

リソース ページからセントラル サービス プロファイルを管理できます。エクスプローラのペインで［Cisco UCS サーバ］を選択し、右側のペインの［セントラル サービス プロファイル］をクリックしてアクセスします。

UCS Manager からサービス プロファイルをインポートするには

1. 白の三角形（インポート）のアイコンをクリックします。
2. ［サービス プロファイルのインポート］ダイアログ ボックスを使用して、［UCS Manager］を選択します。［リフレッシュ］をクリックしてサービス プロファイル リストを取り込み、［すべてのサービス プロファイルのインポート］を選択するか、またはリストから 1 つ以上の値を選択します。インポート後に UCS Manager からインポートされたプロファイルを削除するには、［ソース サービス プロファイルの削除］を選択します。
3. ［OK］をクリックします。

   選択したサービス プロファイルは Management Database にインポートされます。

Management Database でセントラル サービス プロファイルを作成または更新する方法

1. ［+］（作成）アイコンをクリックするか、またはセントラル サービス プロファイルを選択してツール（編集）アイコンをクリックします。
2. ウィザード ページを使用して、セントラル サービス プロファイルを作成または更新します。

   注: Management Database 内にサービス プロファイルを作成する場合、プールおよびポリシーは指定できません。これらの情報は参照専用です。 これらの情報は、セントラル サービス プロファイルを UCS Manager にエクスポートした後に指定できます。
3. サービス プロファイルが作成または更新されたら、［終了］をクリックします。

UCS Manager にサービス プロファイルをエクスポートするには

1. 1 つ以上のセントラル サービス プロファイルを選択します。
2. 青の三角形（エクスポート）のアイコンをクリックします。

   ［サービス プロファイルのエクスポート］ダイアログ ボックスが表示されます。

3. ［利用可能な UCS Manager］リストで、1 つの UCS Manager を選択し、右方向矢印をクリックして、［選択された UCS Manager］リストに転送します。 すべてを転送するには、二重の右方向矢印をクリックします。
4. ［OK］をクリックします。

   注: プールとポリシーはエクスポートされないため、ターゲットの UCS Manager 上にすでに存在している必要があります。

Management Database からサービス プロファイルを削除するには

1. 削除するサービス プロファイルを選択します。
2. ［-］（削除）アイコンをクリックします。

Cisco UCS リソースの表示

［リソース］ページでは、UCS オブジェクト ツリーのすべてのレベルの UCS リソースを表示できます。たとえば、以下のオブジェクトを検査して情報を確認できます。

- Cisco UCS サーバ - カテゴリおよびブレード割り当てごとの UCS リソース、およびインポートされたサービス プロファイル
- 一元化されたサービス プロファイル - UCS Manager の割り当て、インポート、およびエクスポート
- UCS Manager - Fabric Interconnect、シャーシ、および組織
- シャーシ - マウントされているブレードの数、ファンの数（およびそれらのステータス）、および入力/出力モジュール
- ブレード サーバ - ブレードの数、電源がオンかオフか、サービス プロファイルに関連付けられているかどうか、および OS ホスト名

  注: OS ホストを参照するには［エクスプローラ］ツリーのブレードを展開します。 ブレードの OS ホスト名が表示されるのは、プロビジョニングとディスカバリが完了した後です。
- 個別のブレード - マザーボード、CPU、メモリ、およびストレージを含めて高いレベルのインベントリ
- Fabric Interconnect - 高いレベルのハードウェアおよびファン
- 組織 - プール、サービス プロファイル、およびサービス プロファイル テンプレート

Cisco UCS リソースを表示する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. Cisco UCS リソースを検索し選択します。

   右側のペインに、［リソース］ページが表示されます。

サービス プロファイルとブレードの関連付け

サービス プロファイルは、ブレードとの関連付けと関連付け解除、およびフェールオーバ時に適用する設定を行うことができます。

UCS サービス プロファイルを調整する方法

1. 右クリックし、［ポリシー］を選択します。

   ［ポリシー］サブメニューが表示されます。

2. 右クリックし、［ポリシー］-［アクション & ルール］を選択します。

   ［アクション & ルール］ページが表示されます。

3. ［アクション］をクリックします。

   ［アクション］ページが表示されます。

4. ［+］（新しいアクションの追加）をクリックします。

   ［アクションの定義: 新規］ページが表示されます。

5. ［タイプ］ドロップダウン リストでアクション タイプ［サービス プロファイルの設定］をクリックします。

   ［サービス プロファイルの設定］フォームが表示されます。

6. サービス プロファイルを適用する UCS リソースの詳細を指定します。プロファイル操作を選択します。

   注: ヘルプ デスクの承認が必要な場合は、必要に応じて情報を入力します。

7. ［アクション］ドロップダウンの［保存］をクリックします。

   サービス プロファイルの関係が変更されます。

UCS Manager 設定のバックアップ

CA Server Automation は、以下に示すタイプの UCS Manager 設定情報のバックアップをサポートします。

- すべての状態
- すべての設定
- システム設定
- 論理設定

エクスポート/インポート機能を使用すると、Cisco UCS 機能をエミュレートし、バックアップ ジョブを作成および再実行できるようになります。

UCS Manager の設定をエクスポートする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。
2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。
3. Cisco UCS Manager を選択します。

   右側のペインに UCS Manager ページが表示されます。
4. ［エクスポート/インポート］をクリックします。

   ［エクスポート/インポート］ページが表示されます。
5. ［エクスポート ジョブ］セクションで、［+］（作成）をクリックします。

   ［バックアップ操作の作成］ダイアログ ボックスが表示されます。
6. エクスポート情報を入力し、［OK］をクリックします。

   エクスポート ジョブが開始され、［エクスポート］リストに表示されます。

UCS Manager の設定をインポートする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。
2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. Cisco UCS Manager を選択します。

   右側のペインに UCS Manager ページが表示されます。

4. ［エクスポート/インポート］をクリックします。

   ［エクスポート/インポート］ページが表示されます。

5. ［インポート ジョブ］セクションで、［+］（作成）をクリックします。

   ［バックアップ操作の作成］ダイアログ ボックスが表示されます。

6. インポート情報を入力し、［OK］をクリックします。

   インポート ジョブが開始され、［インポート］リストに表示されます。

vNIC テンプレート

CA Server Automation は、vNIC テンプレートの作成および管理をサポートします。 サービス プロファイルまたは VM のいずれかとしてテンプレート ターゲットを指定できます。

vNIC テンプレートを作成するには、サービス プロファイル ウィザードで［vNIC Template を使用］を選択し、［vNIC テンプレートの作成］ダイアログ ボックスを開きます。 また、［エクスプローラ］ペインで UCS 組織を右クリックします。

UCS 組織

関連する UCS リソースを組織でグループ化して、プール、サービス プロファイル、およびサービス プロファイル テンプレートのネスト階層を作成することで、UCS リソース管理を行うことができます。組織とサブ組織は作成および削除できます。

関連項目:

サブ組織の作成 (P. 366)

サブ組織の作成

UCS ルート ツリー上には、組織またはサブ組織を作成できます。

組織を追加する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

   ルートに移動するか、ルートを開いてサブ組織をクリックします。

3. ルートまたはサブ組織を右クリックし、［管理］-［サブ組織の作成］を選択します。

4. 新しいサブ組織を作成するには、［サブ組織の作成］ダイアログ ボックスを使用します。

   サブ組織が作成されます。

UCS プール

CA Server Automation では、UCS リソースをさらに効率的に管理するためのプールを作成できます。

注: プール範囲の競合が発生した場合は、警告が表示されます。

利用可能なプールのタイプは、以下のとおりです。

- UUID プール
- MAC プール
- ワールド ワイド ノード名（WWNN）プール
- ワールド ワイド ポート名（WWPN）プール
- サーバ プール

WWNN プールと WWPN プールは、リモート ストレージ（SAN）を使用するためのブレードの設定に使用できます。

関連項目:

UCS プールの表示 (P. 367)
UCS プールの作成 (P. 368)
UCS プールの名前変更 (P. 369)
UCS プールの削除 (P. 370)

UCS プールの表示

［リソース］ページでは、UCS プールを表示できます。

UCS プールを表示する方法

1. ［リソース］をクリックします。
   ［リソース］ページが表示されます。
2. ［エクスプローラ］ペインを開きます。
   利用可能なグループ、サービス、およびシステムが表示されます。
3. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。
4. ［サマリ］をクリックします。
   ［サマリ］ページが表示されます。
5. ［コンポーネント］セクションのドロップダウン メニューでプール タイプをクリックします。
6. 表示するプールを選択し、ツール (表示) アイコンをクリックします。
7. プール リストに戻るには、［キャンセル］をクリックします。

UCS プールの作成

UCS リソースをさらに効率的に管理するため、［リソース］ページでは UCS プールを作成できます。

リソース プールを作成する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。

4. ［サマリ］をクリックします。

   ［サマリ］ページが表示されます。

5. ［コンポーネント］セクションのドロップダウン メニューでプール タイプをクリックします。

6. ［+］（新規プールの追加）ボタンをクリックします。

   ［プールの作成］ダイアログ ボックスが表示されます。

7. ダイアログ ボックスを使って定義を完成させます。

   プールがプール リストに追加されます。

注:［クイック スタート］メニューをカスタマイズして機能を提供できます。

UCS プールの名前変更

［リソース］ページでは、UCS プールの名前を変更できます。

UCS プールの名前を変更する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。

4. ［サマリ］をクリックします。

   ［サマリ］ページが表示されます。

5. ［コンポーネント］セクションのドロップダウン メニューでプール タイプをクリックします。

6. 名前を変更するプールを選択します。

7. 二重矢印アイコン（>>）をクリックします。

   ［プールの名前変更］ダイアログ ボックスが表示されます。

8. ダイアログ ボックスを使ってプールの名前を変更します。

   リスト内のプールの名前が変更されます。

UCS プールの削除

［リソース］ページでは、UCS プールを削除できます。

UCS プールを削除する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. UCS 組織ツリーの最上位にあるルートをクリックし、希望の組織に移動します。

4. ［サマリ］をクリックします。

   ［サマリ］ページが表示されます。

5. ［コンポーネント］セクションのドロップダウン メニューでプール タイプをクリックします。

6. 削除するプールを選択します。

7. ［-］（削除）アイコンをクリックします。

   削除の確認が表示されます。

8. ［はい］をクリックします。

   プールが削除されます。

ポート プロファイルを管理する方法

CA Server Automation を使用してポート プロファイルを管理するには、以下の手順に従います。

1. プラグインをエクスポートします。

   Cisco UCS Manager と vCenter 間の通信を確立するには、ターゲットの vCenter 内に拡張 XML ファイルを以下のとおり生成およびインストールします。

   - vCenter 4.0 の場合、複数の拡張ファイルが必要です。
   - vCenter 4.0 update 1 以上の場合、Cisco UCS Manager から 1 つの拡張ファイルをエクスポートします。

   必要なファイルがエクスポートされたら、vSphere Client を使用してそれらのファイルを新規プラグインとして vCenter にインポートします。これは、UCS Manager と vCenter の組み合わせごとに一度ずつ必要になります。Cisco UCS Manager では、別の UCS Manager からエクスポートされたファイルを使用することはできません。

2. .vib ファイルを ESX サーバにエクスポートします。

   ESX のバージョンに応じて、適切な .vib ファイル コンポーネントを Cisco Nexus 1000V Virtual Ethernet Module ソフトウェアからインストールすることによって、ESX サーバを設定します。このパッケージ（Cisco および VMware による共同設計）により、VMware 仮想インフラストラクチャと完全に統合される分散仮想スイッチ ソリューションが有効になります。

3. ポート プロファイル ネットワーク トポロジの作成（P. 373）
4. ポート プロファイルとポート プロファイル クライアントの作成（P. 373）

ポート プロファイル ネットワークトポロジの作成

ポート プロファイルを VMware にプッシュするには、Cisco UCS Manager に vCenter、データセンター、DVS フォルダ、DVS、およびプロファイル クライアント オブジェクトが定義されている必要があります。 これらのオブジェクトのトポロジは VMware のトポロジと一致する必要があります。 CA Server Automation では、必要なトポロジを作成できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. エクスプローラ ツリーで UCS Manager を右クリックし、［VMware］をクリックして、［vCenter のレイアウト］ダイアログ ボックスを開きます。
3. vCenter を展開し、vCenter、データセンター、DVS フォルダ、DVS、またはプロファイル クライアント オブジェクトを強調表示します。
4. ［アクション］ドロップダウン メニューで［新規作成］を選択します。
5. 必須情報を入力し、［終了］をクリックします。 DVS パネル上の［有効］を選択すると、関連付けられたポート プロファイルが vCenter に自動的にプッシュされます。

   vCenter、データセンター、DVS フォルダ、DVS、またはプロファイル クライアント オブジェクトが追加されます。

注: このダイアログ ボックスを使用してトポロジ オブジェクトを削除するには、［アクション］ドロップダウン リストの［削除］をクリックします。

ポート プロファイルとポート プロファイル クライアントの作成

CA Server Automation vCenter の［レイアウト］ダイアログ ボックスを使用して、ポート プロファイルおよびポート プロファイル クライアントを作成することができます。

次の手順に従ってください：

1. エクスプローラ ツリーで UCS Manager を右クリックし、［VMware］をクリックして、［vCenter のレイアウト］ダイアログ ボックスを開きます。
2. ポート プロファイルを作成する場合は［ポート プロファイル］をハイライトし、ポート プロファイル クライアントを作成する場合は既存のポート プロファイルをハイライトします。
3. ［アクション］ドロップダウン メニューで［新規作成］を選択します。
4. 必須情報を入力し、［OK］をクリックします。

   ポート プロファイルまたはポート プロファイル クライアントが作成されます。

注: この手順を使用して、ポート プロファイルおよびポート プロファイル クライアントを編集または削除することもできます。 既存のポート プロファイルまたはポート プロファイル クライアントをハイライトして、［アクション］ドロップダウン リストの［編集］または［削除］を選択します。

UCS のアクション タイプ

Cisco UCS リソースは、CA Server Automation のアクション タイプを使用して新しいアクションを作成することができます。これらのアクションは、割り当てられたルール条件が満たされた場合に、UCS の電源投入、リソースの割り当て、およびその他の操作を自動化します。 また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

Citrix XenServer

Citrix XenServer は、仮想化されたサーバおよびクライアント オペレーティング システムにベア メタルに近い仮想化パフォーマンスを提供する仮想化プラットフォームです。 XenServer は Xen ハイパーバイザを使用して、それがインストールされているサーバを仮想化し、各サーバが保証されたパフォーマンスで同時に複数の仮想マシン（VM）をホストできるようにします。 XenServer には、XenServer ホストの物理および仮想リソースを管理するための独自のオペレーティング システムがあるため、特定のオペレーティング システムを必要としません。 XenServer では、Linux と Windows のゲスト オペレーティング システムをサポートしています。

XenServer リソースは、以下の 3 つのレベルで管理できます。

ホスト管理

XenServer ホスト オブジェクトは、XenServer とその VM が実行される物理ホストを表します。 XenServer ホストはスタンドアロン ホストとすることも、XenServer プールと関連付けることもできます。保守モードでは、XenServer ホストで利用可能な仮想および物理リソースのモニタ、仮想ディスク イメージが含まれるストレージ リポジトリの管理、タスクの管理、または XenServer ホストの実行を行えます。

リソース プール管理

*リソース プール*は最大で 16 台の XenServer ホストを接続したグループです。 リソース プール内の XenServer ホストは、共有ストレージと動的に制御されるメモリ、CPU、およびネットワーク リソースを組み合わせて、VM が実行されるオペレーティング環境を提供します。プール内での XenServer ホストのメンバシップまたは役割を管理したり、高可用性を確保するために XenServer にプール メンバのヘルス状態をモニタさせたりすることができます。必要に応じて、プール ホスト間で VM のライブ マイグレーションを行って、ダウンタイムを回避できます。

仮想マシンの管理

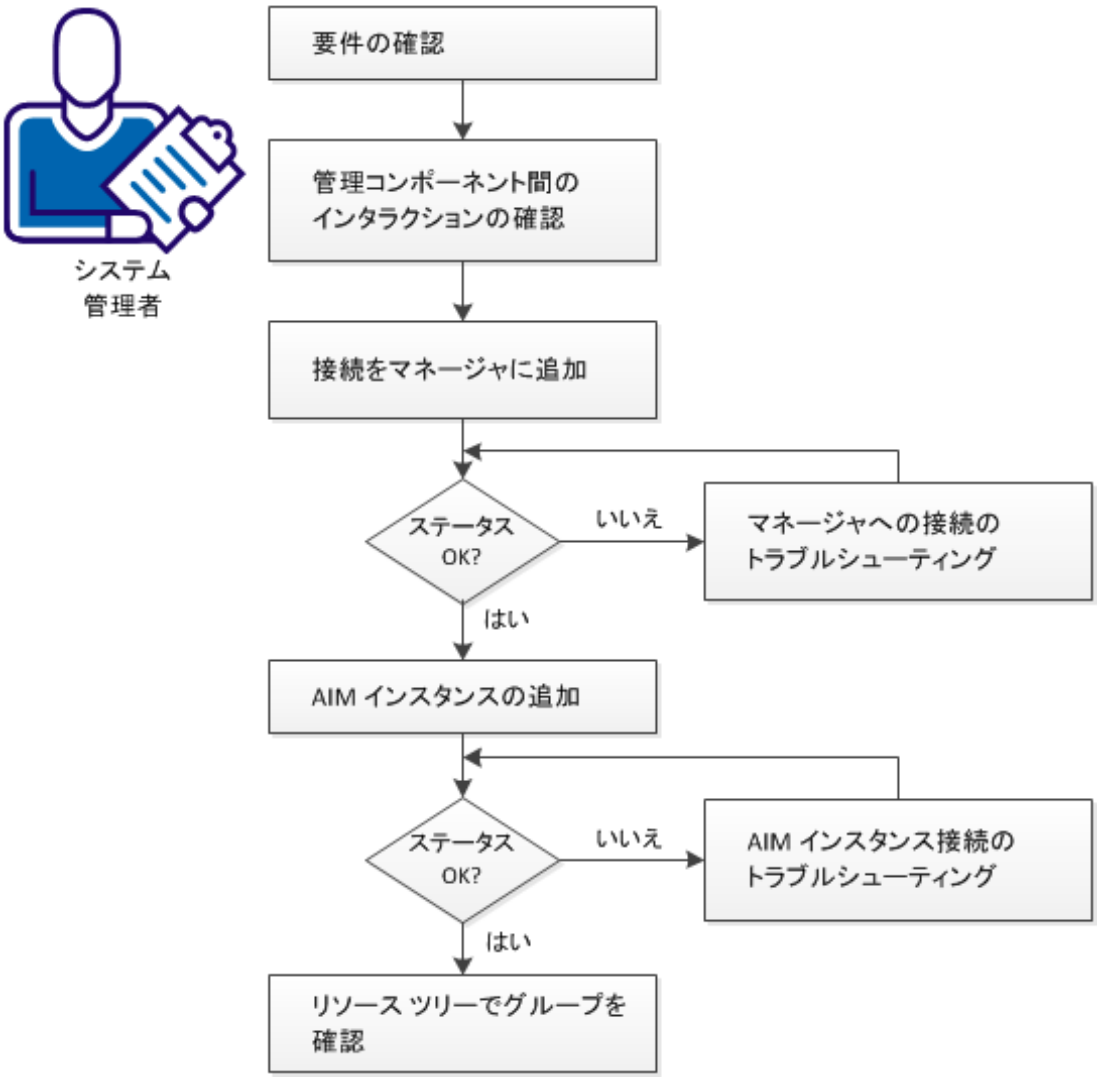
VM 管理レベルで、以下のタスクを実行できます。

- VM の制御（検出、開始、中断、シャットダウン、ディスクから削除）
- VM の管理（クローン）

XenServer 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

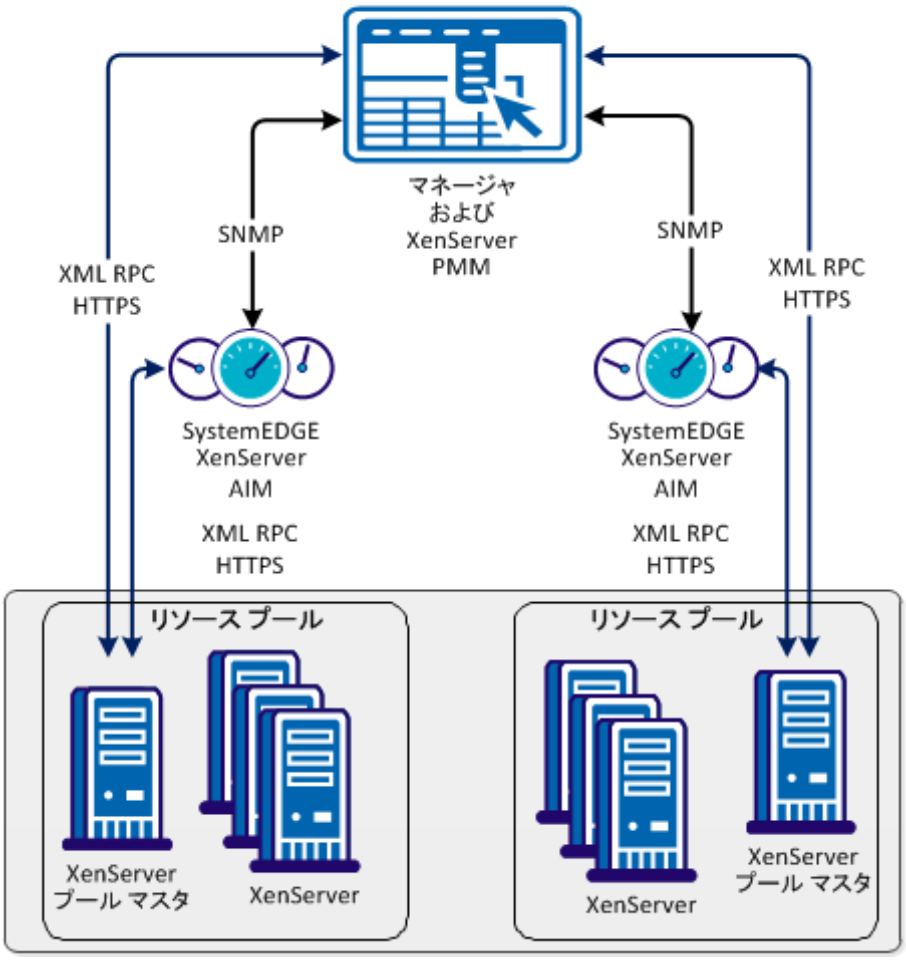
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

Citrix XenServer 管理コンポーネント間のインタラクション

Citrix XenServer AIM はマルチインスタンスのリモート AIM として実装されます。 CA Citrix XenServer AIM は、複数のスタンドアロン Citrix XenServer および Citrix XenServer リソース プールをリモートでモニタできます。 Citrix XenServer AIM は x86 および x64 モジュールとして実装されます。

Citrix XenServer 用の管理 API は XML RPC に基づいています。 Citrix XenServer のリソース プールの場合、すべての XML RPC 通信は AIM、PMM、およびプール マスタ間にのみ発生します。

XenServer 管理コンポーネント間のインタラクション



マネージャへの Citrix XenServer 接続の追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、Citrix XenServer 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Citrix XenServer］を選択します。

3. ［登録済み Citrix XenServer］ペイン ツールバーの （追加）をクリックします。

   ［Citrix XenServer の追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ名、パスワード、リソース プールの UUID）を入力し、優先 AIM を指定して、［管理ステータス］（チェック ボックス）を有効にします。

   重要: ［登録済み Citrix XenServer］へプール マスタが追加されていることを確認してください。

5. ［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。 CA Server Automation によって Citrix XenServer システムが自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

マネージャへのサーバ接続の失敗（Citrix XenServer）

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- サーバ システム上で管理サービスが正常に動作しているかどうかを確認します。

サーバの接続データを更新する方法

1. 失敗した接続に関連付けられた （追加）または （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されていることをコマンドの出力で確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバの名前を入力します。 例：

   ```
   192.168.50.50 myServer
   ```

4. 右上角の  （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。 サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システム上で管理サービスが正常に動作しているかどうかを確認する方法

1. サーバ システムにアクセスする方法を管理者に問い合わせます。
2. サーバ システムにログインし、xsconsole コマンドを実行します。

   サービス コントロール コンソールが起動します。
3. サービスのステータスを確認し、報告された問題を解決します。
4. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが現在も有効であることを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された Citrix XenServer AIM インスタンスの追加

CA Server Automation マネージャに Citrix XenServer 接続を追加した後、Citrix XenServer を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左側のペインの［プロビジョニング］セクションから［Citrix XenServer］を選択します。

3. ［検出された Citrix XenServer AIM インスタンス］ペイン ツールバーの （追加）をクリックします。

   ［Citrix XenServer AIM の追加］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［Citrix XenServer AIM サーバ］を選択します。

   検出された XenServer AIM サーバのリストが表示されます。 XenServer AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウン リストから［Citrix XenServer］を選択します。

   ［登録済み Citrix XenServer］ペインに一覧表示された XenServer が［XenServer］ドロップダウン リストに入力されます。 管理できる XenServer は、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了したら、Citrix XenServer 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの Citrix XenServer グループの確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. Citrix XenServer グループを展開します。

   管理対象の Citrix リソース プールが表示されます。
3. リソース プールのエントリを展開します。

   管理対象 Citrix XenServer が表示されます。

CA Server Automation で、設定された Citrix XenServer 環境を管理する準備が整いました。

XenServer のプロビジョニング用に Linux テンプレートを準備する方法

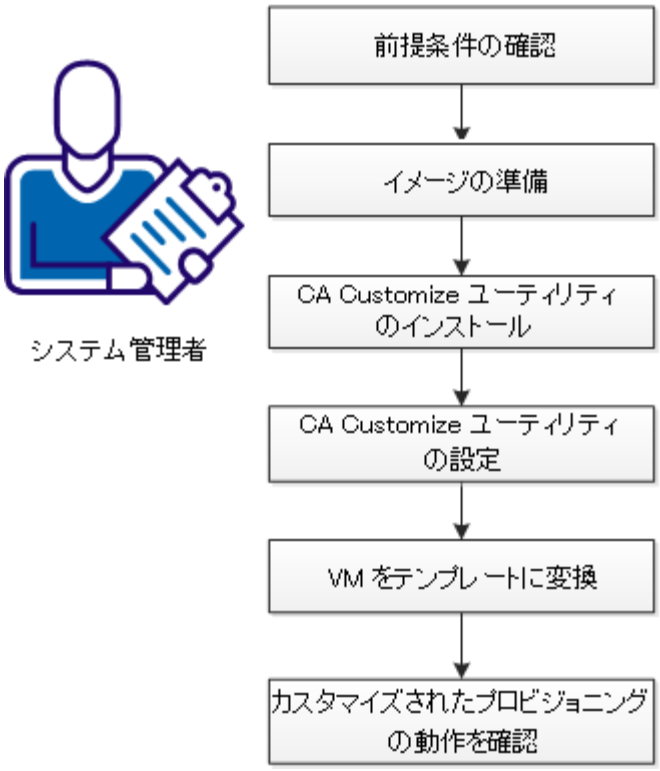
CA Server Automation は、以下のオペレーティング システムを実行する新しい仮想マシン（VM）のカスタマイズされたプロビジョニングをサポートします。

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

カスタマイズ オプションには、ホスト名、パスワード、ドメイン、またはネットワーク設定が含まれます。

以下の図は、システム管理者が VM のプロビジョニング用に Linux テンプレートを準備する方法を示しています。

VM のプロビジョニング用に Linux テンプレートを準備する方法



以下の手順に従います。

カスタマイズされた VM プロビジョニングの前提条件

Linux ゲストをカスタマイズするには、ファイル システムまたはコンソールへの直接アクセスが必要です。

XenServer 環境が以下の前提条件に適合することを確認します。

- リソース プール内の各 XenServer で、SSH または SFTP アクセスを有効にしておく必要があります。

Linux イメージの準備（XenServer）

Linux オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従ってイメージを準備します。 一部の手順は Linux ディストリビューションによって異なる場合があります。

次の手順に従ってください:

1. Linux オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. Citrix XenServer 用の XenTools を仮想マシンにインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに追加するカスタマイズを適用します。

この Linux イメージは、CA Customize ユーティリティを使用してさらにカスタマイズできます。

CA Customize ユーティリティのインストール

CA Customize ユーティリティを使用すると、CA Server Automation で仮想マシンの設定を外部から変更できます。 このゲスト ユーティリティは、OS の開始時に CD ドライブをモニタします。 特別な ISO が接続されると、以下のアクションが実行されます。

1. コマンド セットによってゲストがカスタマイズされます。
2. ゲスト システムはカスタマイズ済みとしてマークされます。
   この状態がリセットされるまで、システムはこれ以上変更できなくなります。
3. システムが停止し、カスタマイズが成功したことを示します。

ca-customize ゲスト ユーティリティを正しくインストールする方法

1. このユーティリティを以下で見つけます。
   - Red Hat Enterprise Server 6.0 の場合

     ```
     <InstallationRoot>¥Utilities¥linuxCustomization¥rh6
     ```
   - SUSE Linux Enterprise Server 11 の場合

     ```
     <InstallationRoot>¥Utilities¥linuxCustomization¥sles11
     ```
2. この実行可能ファイルを、準備する VM のハード ドライブの以下の場所に移動します。

   ```
   /usr/bin/ca-customize
   ```
3. （オプション）サポートされていない他のゲスト システムをサポートするには、ユーザ独自の ca-customize スクリプトを指定します。
4. ca-customize ユーティリティの実行可能ビットを有効にします。

   ```
   chmod 755 /usr/bin/ca-customize
   ```

CA Customize ユーティリティの設定

Linux プロビジョニング用のテンプレートをセットアップできます。 ゲストをカスタマイズするには、利用可能なスクリプトを使用します。また、ユーザ独自のスクリプトを使用して詳細なセットアップを行うこともできます。

次の手順に従ってください:

1. ネットワークがカスタマイズのプロセスに影響しないように、ネットワーク インターフェースを無効にします。

   注: ネットワークはカスタマイズ中に自動的に有効化されます。

2. 必要に応じて、*/etc/ca-customize.conf* ファイルを使用して、デフォルトの CDROM デバイス名を上書きします。

   CD_DEVICE=/dev/cdrom

   CD ドライブに使用するデバイス名を定義します。

   デフォルト： /dev/cdrom

3. ブート プロセスの最後に自動起動をセットアップします。

   - （SUSE Linux の場合）*/etc/init.d/after.local* ファイルを作成または変更します。

     ```
     #!/bin/bash
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

   - （Red Hat Linux の場合）以下の行を */etc/rc.local* ファイルに追加します。

     ```
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

4. システムをシャットダウンします。

VM をテンプレートに変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. VM をシャットダウンします。
2. 準備したイメージを XenServer テンプレートに変換するには、XenCenter を使用します。

テンプレートが CA Server Automation に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

カスタマイズされたプロビジョニングの動作

以下の手順は、カスタマイズされた VM プロビジョニングのワークフローを表します。

1. プラットフォーム管理サービスは新しい Linux VM をプロビジョニングします。
2. プラットフォーム管理サービスは、カスタマイズ パラメータを使用して新しい ISO を準備し、新しい VM に添付します。
3. プラットフォーム管理サービスは VM を開始します。
4. VM はカスタマイズ ISO が添付されていることを検出します。VM はカスタマイズ変更を適用します。
5. カスタマイズが成功すると、VM はシャットダウンします。PMM は VM の停止を検出します。 プラットフォーム管理サービスは再度 VM を開始し、プロビジョニングを完了します。
6. カスタマイズが失敗すると、VM は停止しません。 プラットフォーム管理サービスは以下のアクションを実行します。
   a. プロビジョニングの失敗を返します
   b. プロビジョニング ジョブを例外状態に設定します

カスタマイズ ログ

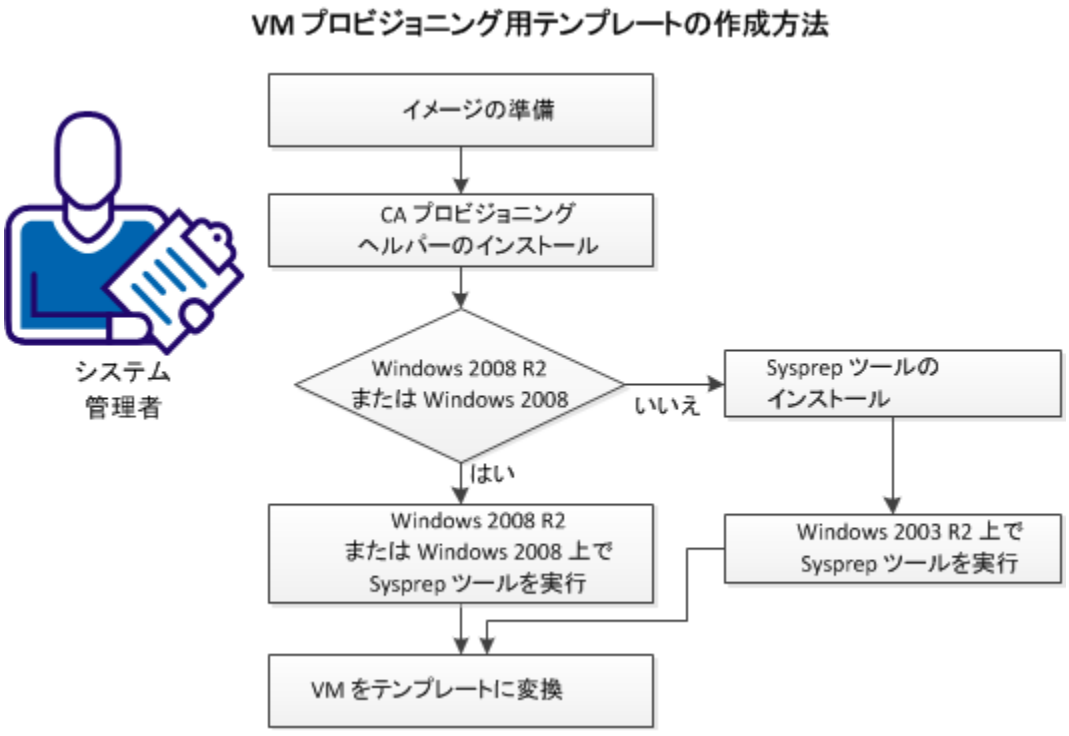
成功したカスタマイズは、*/etc/ca-customized* ファイルに格納されます。このファイルには、カスタマイズ変更のリストが含まれます。

カスタマイズに失敗すると、ログが */etc/ca-customized.tmp* ファイルに格納されます。

XenServer のプロビジョニング用に Windows テンプレートを準備する方法

CA Server Automation では、Windows 2003 R2 Server（32 ビット/64 ビット）、Windows 2008 （32 ビット/64 ビット）または Windows 2008 R2 Server （64 ビット）を実行する新しい仮想マシン（VM）でのプロビジョニングのカスタマイズをサポートしています。 カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が XenServer のプロビジョニング用に Windows テンプレートを準備する方法を示しています。



次の手順に従ってください:

1. Windows イメージを準備します (P. 394)。
2. CA プロビジョニング ヘルパーをインストールします。 (P. 395)
3. （Windows 2003 R2 で有効） Sysprep ツールをインストールします (P. 395)。
4. 使用するオペレーティング システムに応じて、以下のアクションの*いずれか*を選択します。
   - Windows 2003 R2 で Sysprep ツールを実行する。 (P. 395)
   - Windows 2008 または Windows 2008 R2 で Sysprep ツールを実行する。 (P. 396)
5. VM を XenCenter のテンプレートに変換します (P. 396)。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従って、イメージを準備します。 テンプレートをカスタマイズするには、CA Server Automation のプロビジョニング操作を有効にする手順に従ってください。 一部の手順は Windows のバージョンによって異なります。

次の手順に従ってください:

1. Windows オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. Citrix XenServer 用の XenTools を仮想マシンにインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。
4. （Windows 2003 で有効）組み込みの管理者アカウントのパスワードを空白にします。

   注: 管理者パスワードが空でないと、プロビジョニングの際に SysPrep で新しいパスワードを設定できず、既存のパスワードが残ります。

XenServer 環境の前提条件

XenServer 環境が以下の前提条件に適合することを確認します。

- リソース プール内の各 XenServer で、SSH または SFTP アクセスを有効にしておく必要があります。

CA プロビジョニング ヘルパーのインストール

CA プロビジョニング ヘルパーは、CA Server Automation で仮想マシンの設定を外部から変更できるようにするものです。

次の手順に従ってください:

1. <InstallationRoot>¥Utilities¥Sysprep¥CAProvisioningHelper.exe でこのユーティリティを見つけます。
2. 準備する VM のハード ドライブの任意の場所に、この実行可能ファイルを移動します。
3. コマンド ラインから CA プロビジョニング ヘルパーを 1 回実行します。

Sysprep ツール

Microsoft は、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンするための Sysprep ツールを提供しています。以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Sysprep ツールを Windows 2003 R2 にインストールして実行する

Windows 2003 では、Sysprep ツールはデフォルトではインストールされませんが、Windows インストール CD-ROM に収録されています。

Sysprep ツールのインストール

Windows インストール CD-ROM から Sysprep ツールをインストールします。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。

   ```
   ¥SUPPORT¥TOOLS¥DEPLOY.CAB
   ```

2. CAB ファイルに含まれるファイルをすべて選択し、%SystemDrive%¥Sysprep （通常は C:¥Sysprep）にコピーします。

   注: ディレクトリ名は変更しないでください。

3. Sysprep ディレクトリに移動して、以下を実行します。

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

Windows 2008 R2 での Sysprep ツールの実行

通常の Windows インストール プロセスでは、SysPrep プロセスを実行するためのすべてのファイルがインストールされます。 Windows インストールを設定した後、以下の手順を実行します。

1. Windows Server 2008 R2 用の Windows 自動インストール キット（WAIK）を使用して、有効な XML 応答ファイルを作成します。WAIK は Microsoft の Web サイトから入手できます。

   注: このプロビジョニングでは、ダミーの自動応答ファイルが必要で、これがないとシャットダウンできません。応答ファイルの内容はプロビジョニング プロセスによって置換されるため、どのようなものでもかまいません。ただし、ファイルは SysPrep に固有の XML スキーマに従う必要があります。

2. 作成された XML ファイルに「sysprep.xml」と名前を付け、これを以下の Sysprep ディレクトリに置きます。

   %SystemRoot%¥system32¥sysprep

3. 以下のコマンドを実行します。

   ```
   sysprep /generalize /oobe /shutdown /unattend:sysprep.xml
   ```

VM を XenCenter のテンプレートへ変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. 仮想マシンをシャットダウンします。
2. 準備したイメージを XenServer テンプレートに変換するには、XenCenter を使用します。

   テンプレートが CA Server Automation に表示され、プロビジョニングのカスタマイズに使用できるようになります。

VM ステータスの管理（XenServer）

仮想マシンのステータスを制御するには、以下のいずれかの操作を行います。

- 検出
  - サーバ
  - ネットワーク
- 開始
- 中断
- シャットダウン
- ディスクから削除

VM ステータスを制御する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. VM を右クリックし、［管理］を選択して、以下のいずれかのオプションを選択します。

   検出

   サーバまたはネットワークを検出します。

   開始

   指定された XenServer ホスト上の VM を開始します。

   中断

   指定された XenServer ホストで実行されている VM を中断して、その現在の状態を保存します。 VM を再開するまで、すべてのアクティビティが中断されます。

   シャットダウン

   指定された XenServer ホストで実行されている VM をシャットダウンします。

   ディスクから削除

   ディスクから VM を削除します。

   対応するウィザードが表示されます。

3. 必要な情報を入力して、次の手順に進みます。

4. サブミットします。

   ステータス操作が実行され、確認のメッセージが表示されます。 インターフェースをリフレッシュして、最新の VM ステータスを表示します。 操作の結果を確認するイベントが表示されます。

Citrix XenServer 仮想マシンのプロビジョニング

以下の手順を実行することで、仮想マシンをプロビジョニングできます。VM のプロビジョニング用の Windows テンプレートを準備してください。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. Citrix XenServer グループを右クリックし、［プロビジョニング］-［Citrix XenServer 仮想マシンのプロビジョニング］を選択します。

   プロビジョニング ウィザードが表示されます。

3. 必要な情報を入力します。

   VM 名

   新しい VM 名を定義します。

   テンプレート

   Windows プロビジョニング テンプレートを指定します。

   管理者パスワード

   新しい VM の管理者パスワードを定義します。

   製品のアクティベーション キー

   Windows 2003 のアクティベーション キーを定義します。

   フル ネーム

   VM のフル ネームを定義します。

4. （オプション）追加情報（ワークグループ、メモリ、CPU、VM ホスト、組織）を指定します。 静的 IP アドレスを使用する場合は、DHCP を無効にし、IP アドレス、マスク、およびデフォルト ゲートウェイを指定します。

   注: メモリと CPU の設定は、使用する Windows プロビジョニング テンプレートによって異なります。

5. サブミットします。

   確認メッセージが表示されます。

6. ［ジョブ］パネルをリフレッシュして、進捗状況を表示します。

   操作の結果を確認するイベントが表示されます。

Huawei GalaX

Huawei GalaX には以下のプラットフォームが含まれます。

仮想化インフラストラクチャ プラットフォーム

コンピューティング、ストレージ、ネットワークなどの物理リソースを、集中管理、柔軟なスケジュール設定、動的割り当てが可能な仮想リソースに仮想化します。 仮想化インフラストラクチャは、クラウドコンピューティング ベースのデータ センターを構築するために使用される重要なプラットフォームです。

クラウド コンピューティング インフラストラクチャ プラットフォーム

仮想化インフラストラクチャ プラットフォームによって提供された仮想リソースをカプセル化および管理します。 キャリアや企業がデータ センター OMM 機能を構築するのを支援します。 管理機能にはリソース管理、イメージ管理、課金管理、スケジュール管理、およびユーザ管理が含まれます。

操作および保守管理(OMM)プラットフォーム

OMM ユーザのための統合 OMM インターフェースを提供します。 OMM ユーザは、Web インターフェースによって SingleCLOUD OMM System にリモートからアクセスできます。 ユーザは、リソース管理、リソース モニタリング、およびリソース統計レポートなどの操作を実行できます。

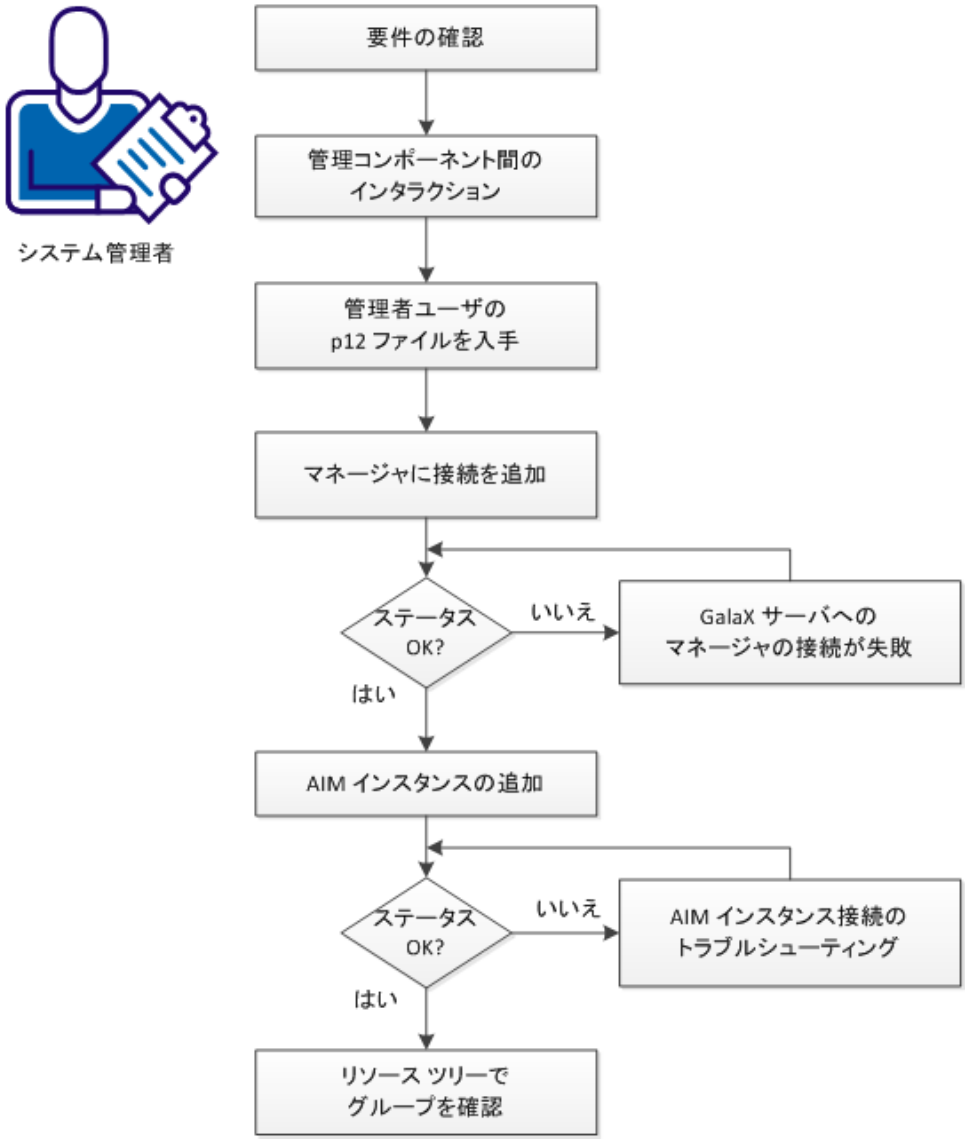
関連項目:

Huawei GalaX 管理コンポーネントを設定する方法 (P. 401)
Virtual Private Cloud VLAN を作成する方法 (P. 416)
Huawei SingleCLOUD 環境を管理する方法 (P. 428)
GalaX のプロビジョニング用に Windows テンプレートを準備する方法 (P. 439)

Huawei GalaX 管理コンポーネントを設定する方法

システム管理者として、ユーザの Huawei GalaX 環境に接続し、そのパフォーマンスをモニタするように CA Server Automation を設定できます。

GalaX 管理コンポーネントの設定方法



以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するポートを決定済みである。
  デフォルトの HTTP ポート： 8773。
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

Huawei GalaX 管理コンポーネント間のインタラクションの確認

システム管理者として、CA Server Automation を使って新しい Huawei GalaX 環境を管理するとします。CA Server Automation を使用すると、1 つ以上の GalaX 環境の物理リソースと仮想リソースを動的に管理できます。 Huawei GalaX は、1 つ以上の Computing Resource Managers（CRM）と通信する Elastic Service Controller（ESC）から構成されます。CRM は複数の Computing Node Agents （CNA）と通信します。

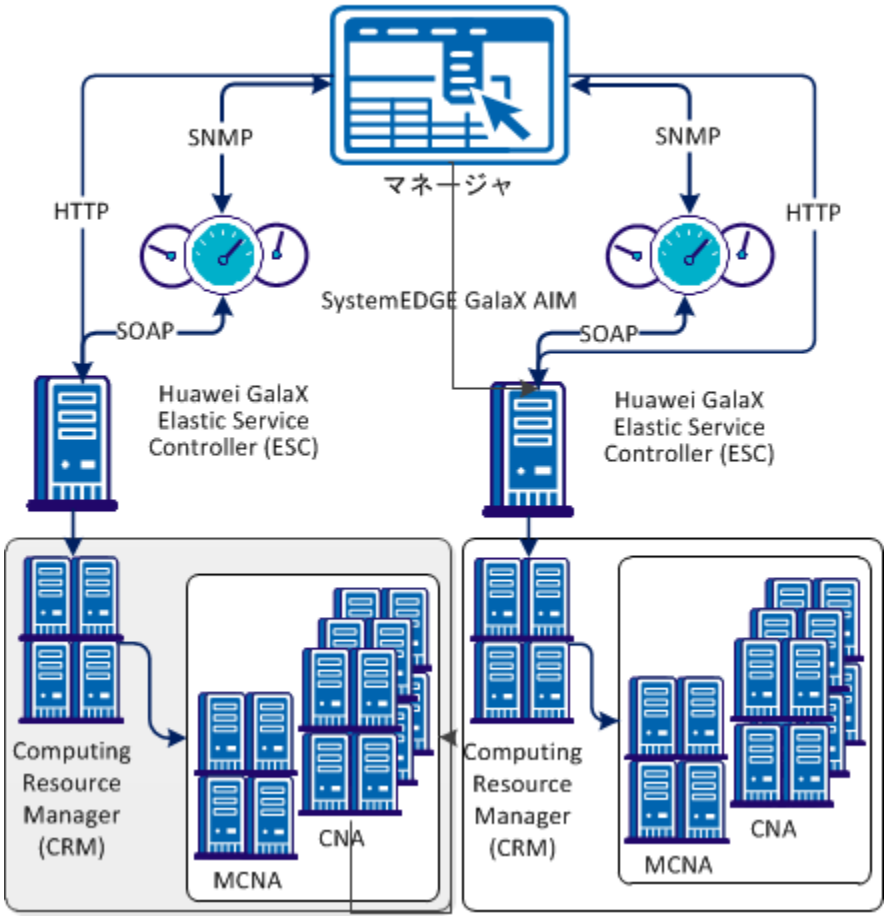
GalaX を管理するため、CA Server Automation は、その GalaX プラットフォーム管理モジュール（PMM）、GalaX Application Insight Module （AIM）、および Elastic Service Controller （ESC）の間にネットワーク接続を必要とします。 これらのネットワーク接続を確立するには、CA Server Automation GalaX 管理コンポーネント（つまり GalaX PMM と GalaX AIM）を設定します。

GalaX AIM は、SystemEDGE の機能範囲を拡張する SystemEDGE エージェントプラグインです。 GalaX AIM によって SystemEDGE は、複数の GalaX 環境のパフォーマンスをモニタでき、モニタ対象 GalaX リソースの状態を評価できます。 しきい値に基づき、SystemEDGE および AIM はモニタ対象リソースのステータスを判断し、その情報を SNMP を使用して CA Server Automation マネージャにプロパゲートします。

GalaX PMM は CA Server Automation マネージャのコンポーネントです。PMM には、SOAP を使用するすべての Huawei GalaX 操作のサポートと接続を提供する役割があります。 PMM は、Computing Resource Manager との接続を管理し、GalaX 関連の操作を実行します。また、AIM からデータを取得し、CA Server Automation 管理データベースに入力します。

以下の図は、2 つの GalaX ESC 環境例において、影響を受けるコンポーネントのインタラクションを示しています。 通常、GalaX PMM およびそのマルチインスタンス サポートを含む各 GalaX AIM は、複数の Elastic Service Controller に接続できます。 図中に示される接続では制限が指定されていません。 必要なネットワーク接続は、TCP/IP、SNMP、および SOAP に基づきます。

Huawei GalaX 管理コンポーネント間のインタラクション



管理者ユーザ p12 ファイルの取得

CA Server Automation UI で操作を実行するには、GalaX 環境から管理者ユーザ p12 ファイルを取得します。 p12 ファイルでは、GalaX 環境を設定、モニタ、および管理するための管理者権限が提供されます。

p12 証明書ファイルは、GalaX のインストール中に生成されます。 証明書ファイルはグローバルに一意であり、特定の Elastic Service Controller（ESC）API に対してのみ有効です。 特定の証明書ファイルを使用して異なる GalaX ESC サーバにアクセスすることはできません。

以下の手順を実行する前に、お使いの GalaX ESC サーバの IP アドレス、および、root ユーザのパスワードを確認してください。

次の手順に従ってください:

1. p12 ファイルの生成に使用するパスワードを指定します。

   このパスワードは、CA Server Automation マネージャと GalaX ESC サーバの間の接続を設定する際にも必要になります。

2. root を使用して GalaX ESC サーバにログインします。

3. ターミナル ウィンドウを開き、以下のコマンドを実行します。

   ```
   cd /opt/eucalyptus/.euca
   ```

   このディレクトリには証明書ファイルが含まれています。

4. デジタル署名された証明書ファイルおよび秘密鍵証明書ファイルの名前を取得するには、ls コマンドを実行します。

   ファイル名の形式は、以下のようになります。

   - デジタル署名された証明書ファイル： euca2-admin-*-cert.pem
   - 秘密鍵証明書ファイル： euca2-admin-*-pk.pem

5. 以下のコマンドを実行します。

   ```
   Openssl pcks12 –export –in <デジタル署名された証明書ファイル> -out admin.p12 –inkey <秘密鍵証明書ファイル>
   ```

   例：

   ```
   openssl pkcs12 -export -in euca2-admin-109f9d47-cert.pem -out admin.p12 -inkey euca2-admin-109f9d47-pk.pem
   ```

6. システムにプロンプトが表示されます： "Enter Export Password"
7. 手順 1 で指定したパスワードを入力します。

   システムによって、要求された admin.p12 証明書ファイルが /opt/eucalyptus/.euca ディレクトリに生成されます。
8. CA Server Automation マネージャが存在するサーバに admin.p12 ファイルをコピーします。 ディレクトリは、サーバ上の任意のディレクトリを使用できます。 admin.p12 ファイルを Windows システムにコピーするには、WinSCP などのツールを使用することができます。
9. これで、CA Server Automation マネージャと GalaX ESC サーバの間の接続を確立するために admin.p12 ファイルとパスワードを使用できるようになりました。

新しい GalaX 接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、GalaX 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Huawei SingleCLOUD］を選択します。

   右側のペインがリフレッシュされ、管理対象の GalaX サーバおよび関連する GalaX AIM サーバが表示されます。

3. ［GalaX サーバ］ペイン ツールバーの （追加）をクリックします。

   ［新しい GalaX サーバ］ ダイアログ ボックスが表示されます。

4. 必要な接続データ（ユーザ名、サーバ、ポート、P12 ファイル パス、およびパスワード）を入力し［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上の［GalaX Server］ペインに GalaX Server が緑のステータス アイコンを使って追加されます。 CA Server Automation によって GalaX サーバが自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によって GalaX サーバが赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。

GalaX サーバへのマネージャの接続が失敗する

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であることを確認します。
- CA Server Automation サーバと GalaX サーバ間の時間差が 5 分未満であることを確認します。
- 接続に必要なサービスがサーバ上で正しく実行されていることを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の  （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

CA Server Automation サーバと GalaX サーバ間の時間差が 5 分未満であるかどうかを確認する方法

1. GalaX サーバにアクセスするために、システム管理者に問い合わせます。
2. GalaX サーバのシステム時間を確認します。
3. CA Server Automation マネージャ システムのシステム時間を確認します。
4. システムの時間差が 5 分を超える場合は、時間設定を適切に更新します。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. GalaX サーバにログインします。
2. 接続に必要なサービスが正しく実行されていることを確認します。
3. 必要に応じて、サービスを開始または再起動します。
4. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

GalaX サーバの AIM インスタンスの追加

CA Server Automation マネージャに新しい GalaX 接続を追加した後、新しい GalaX サーバを管理するための GalaX AIM インスタンスを追加します。 その後、そのすべての物理および仮想コンポーネントを含む Huawei GalaX 環境全体が CA Server Automation によって検出されます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Huawei SingleCLOUD］を選択します。

   右側のペインがリフレッシュされ、管理対象の GalaX サーバおよび関連する GalaX AIM サーバが表示されます。

3. ［GalaX AIM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［新しい GalaX AIM サーバ］ダイアログ ボックスが表示されます。

4. ［GalaX AIM サーバ］ ドロップダウン リストを開きます。

   検出された GalaX AIM サーバのリストが表示されます。

5. ドロップダウン リストから［GalaX AIM サーバ］を選択します。

   ［GalaX サーバ］ペインに一覧表示された GalaX サーバが［GalaX サーバ］ドロップダウン リストに入力されます。 管理できる GalaX サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに常駐している場合、AIM サーバがドロップダウン リスト内に表示されるように、最初に CA Server Automation によってシステムが検出される必要があります。

6. 管理する GalaX サーバを選択し、［OK］をクリックします。

   選択した GalaX サーバの新しい AIM インスタンスが追加されます。 インスタンスがエラー状態または停止状態でない場合、CA Server Automation は関連付けられている Huawei GalaX 環境の検出を開始します。 ディスカバリ プロセスが完了したら、Huawei GalaX の仮想および物理リソースの管理を開始できます。

リソース ツリーでの Huawei GalaX の確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. Huawei SingleCLOUD グループを展開します。

   Huawei GalaX リソースが表示されます。

CA Server Automation で、設定された Huawei GalaX 環境を管理する準備が整いました。 リソースのステータスとプロパティをモニタできます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

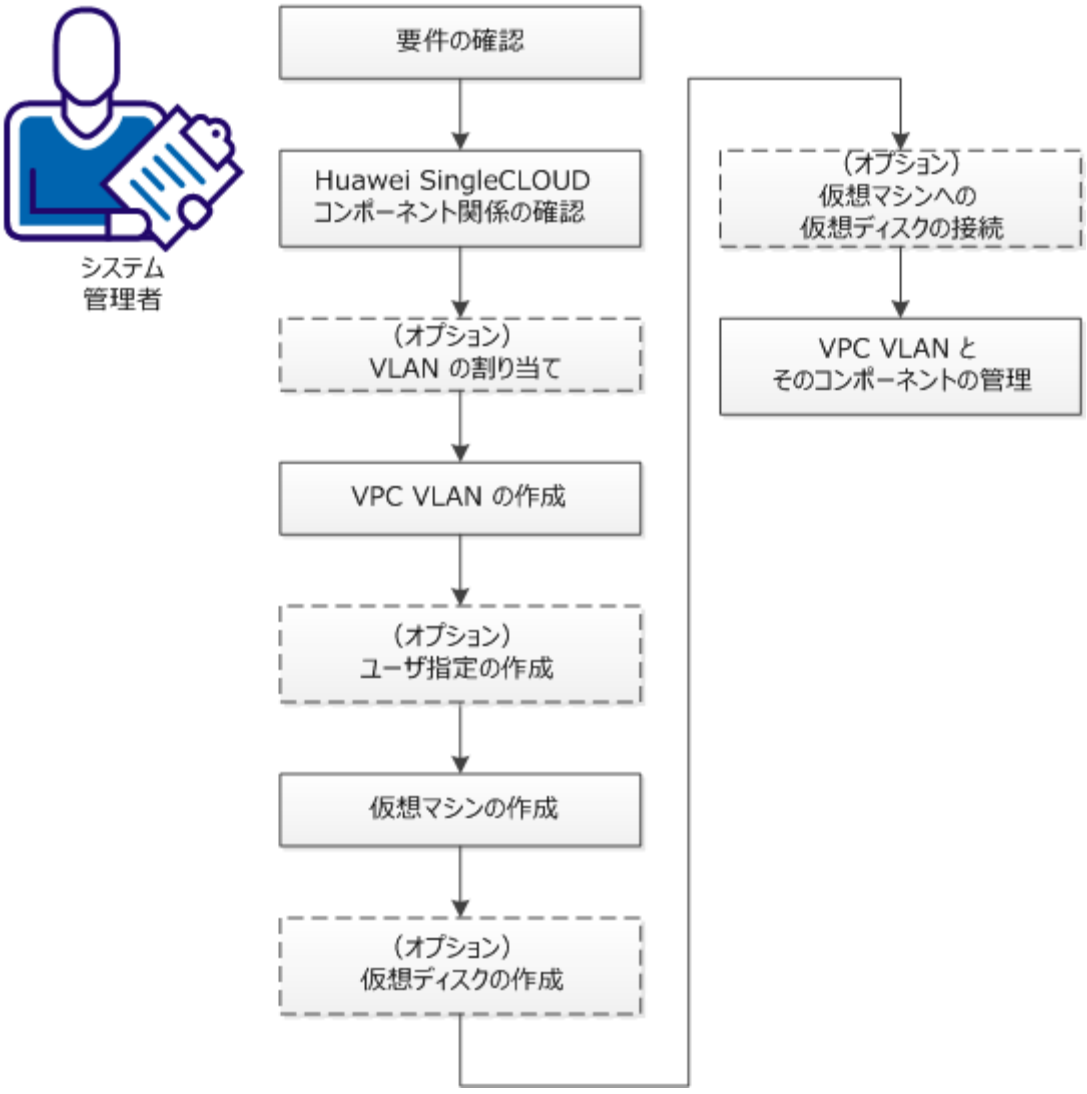
- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

Virtual Private Cloud VLAN を作成する方法

システム管理者として GalaX 環境の関連する仮想マシンと仮想ディスクで Virtual Private Cloud を作成するとします。 *Virtual Private Cloud （VPC）*は、複数の仮想マシンおよび関連する仮想ディスクを備えた Huawei SingleCLOUD ユーザのためのプライベート ローカル ネットワークです。CA Server Automation が GalaX 環境をすでに検出しているため（「要件の確認 (P. 419)」を参照）、CA Server Automation ユーザ インターフェースは必要な VPC VLAN リソースを作成するためのインフラストラクチャを提供します。

以下の図は、VPC VLAN の作成方法に関する必要な手順を示しています。

VPC VLAN の作成方法



以下の手順に従います。

要件の確認

CA Server Automation で Huawei SingleCLOUD インスタンスをセットアップする前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Server Automation ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- モニタリング ソフトウェア（SystemEDGE）の展開および設定に精通していること。
- CA Server Automation がインストールされており、CA Server Automation ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ（仮想マシン用）およびストレージ クラスタ（仮想ディスク用）が Huawei GalaX 環境で利用可能であること。
- 仮想マシンに適用するオペレーティング システムのイメージが Huawei GalaX 環境で利用可能であること。
- CA Server Automation と Huawei GalaX サーバの間の接続が確立されていること。
- GalaX AIM が Huawei GalaX サーバをモニタするように設定されていること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Server Automation が Huawei GalaX サーバとその関連リソース（クラスタ、ストレージ クラスタ、仮想マシンなど）を検出していること。
- 共有ディスクには Microsoft Cluster Service（MSCS）が必要です。

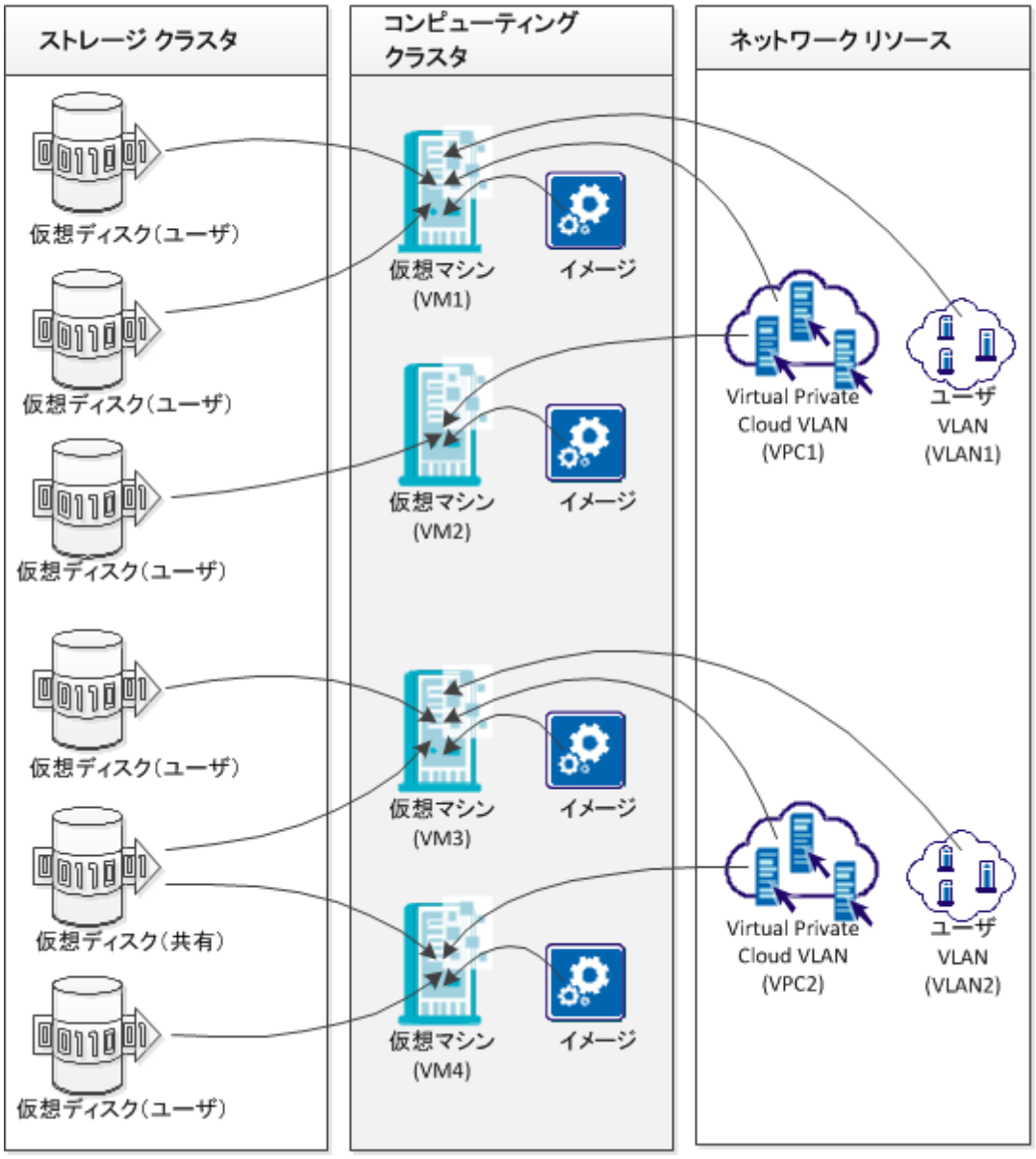
Huawei SingleCLOUD コンポーネント関係の確認

Huawei GalaX 環境は Huawei SingleCLOUD ソリューションの一部で、クラウド サービス プロバイダまたは企業顧客のクラウド コンピューティング データ センター向けに設計されています。

Huawei SingleCLOUD ソリューションは階層状のアーキテクチャから構成されます。 物理層およびネットワーク層のデバイスはソリューションへ統合されます。 クラスタ、分散ストレージ、NAS ストレージ、および仮想化の技術に基づいて、これらの統合されたデバイスはストレージ、コンピューティング、およびネットワーク サービスを上層のサービスに提供します。CA Server Automation 内の Huawei SingleCLOUD インスタンスには、お使いの Huawei GalaX 環境を管理、モニタするために必要なインフラストラクチャが含まれます。 Huawei GalaX 環境は、クラスタおよびそれらに関連するリソースから構成されます。

以下の図は、CA Server Automation によって管理できる SingleCLOUD ソリューションの GalaX コンポーネントおよびこれらのコンポーネント間の依存関係を示します。

Huawei SingleCLOUD GalaX コンポーネントおよびそれらの関係



最初に、クラウド内の仮想マシンとそのユーザへの VLAN アクセスを提供する VPC VLAN を作成します。 必要に応じて、ユーザ VLAN を仮想マシンに追加できます。 コンピューティング クラスタ内の仮想マシンには、適切なイメージ、および仮想マシンが属する VPC VLAN が必要です。 イメージには、この仮想マシン用のオペレーティング システムおよびアプリケーションが含まれます。

その後、ストレージ クラスタで仮想ディスクを作成し、これらのディスクを適切な仮想マシンに接続して、ユーザに固有のデータを格納することができます。 ユーザ ディスクと共有ディスクという 2 つのタイプの仮想ディスクがサポートされています。ユーザ ディスクには仮想マシンとの 1 対 1 の関係があります。また、共有ディスクには一対多数の関係がありえます。 共有ディスクには Microsoft Cluster Service（MSCS）サポートが必要です。

（オプション）VLAN の割り当て

Virtual Private Cloud オブジェクトが VLAN を必要とするため、最初に VLAN を割り当てます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切な SingleCLOUD サーバを選択します。

   右側のペインがリフレッシュされ、［リソース管理］および［ネットワーク管理］タブが表示されます。

3. ［ネットワーク管理］-［VLAN］をクリックします。

   既存の VLAN オブジェクトのリストが表示されます。

4. ［VLAN］ペインのツールバーで  （追加）をクリックします。

   ［VLAN の割り当て］ダイアログ ボックスが表示されます。

5. VLAN 名を指定し、ドロップダウン メニューからクラスタを選択し、方法（自動または手動入力）を指定して、［OK］をクリックします。

   VLAN が割り当てられます。

VPC VLAN の作成

VPC は、いくつかの仮想マシンおよび関連する仮想ディスクを備えたクラウド ユーザのためのプライベート ローカル ネットワークとして機能します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切な SingleCLOUD サーバを選択します。

   右側のペインがリフレッシュされ、［リソース管理］および［ネットワーク管理］タブが表示されます。

3. ［ネットワーク管理］-［VPC］をクリックします。

   既存の VPC インスタンスのリストが表示されます。

4. ［VPC］ペインのツールバーで （追加）をクリックします。

   ［VPC の作成］ダイアログ ボックスが表示されます。

5. VPC 名を指定し、ドロップダウン メニューからクラスタを選択し、（自動的にまたはリストから手動で）VLAN を割り当てて、［OK］をクリックします。

   VPC インスタンスが作成されます。

（オプション）ユーザ指定の作成

ユーザ指定は、仮想マシンを作成するために使用可能な CPU、メモリ、およびシステム ボリューム サイズに対する 1 セットの設定値です。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   エクスプローラのツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切な SingleCLOUD サーバを選択します。

   右側のペインがリフレッシュされ、［リソース管理］および［ネットワーク管理］タブが表示されます。

3. ［リソース管理］-［ユーザ指定］をクリックします。

   既存のユーザ指定のリストが表示されます。

4. ［ユーザ指定］ペインのツールバーで  （追加）をクリックします。

   ［ユーザ指定の作成］ダイアログ ボックスが表示されます。

5. CPU、メモリおよびシステム ボリューム サイズのユーザ指定の名前および値を指定します。 ［OK］をクリックします。

   ユーザ指定が作成されます。

仮想マシンの作成

仮想マシンには、システム ボリューム、CPU、メモリおよびディスク空き領域の設定用のイメージ、VPC および NIC 仕様が必要です。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切なコンピューティング クラスタを右クリックします。

   ポップアップ メニューが表示されます。

3. ［管理］-［テンプレートから VM を作成］を選択します。

   ［VM の作成］ダイアログ ボックスが開きます。

4. 以下のパラメータを指定して、［OK］をクリックします。

   - VM 数
   - VM Name
   - Image ID
   - ユーザ指定または CPU、メモリ、ディスク領域
   - VPC VLAN
   - （オプション）追加のネットワーク インターフェース コントローラ（NIC）

- サービス品質（QoS）の設定
  - メモリ予約
  - CPU 予約
  - CPU 制限
  - 高可用性
  - NIC 速度制限

CA Server Automation は指定された仮想マシンを作成します。仮想マシンは、割り当てられた VPC VLAN に属します。 仮想マシンのリストを取得するには、［コンピューティング クラスタ］パネルの［詳細］タブを開きます。

以下のダイアログ ボックスには追加の説明が必要です。

メモリ予約

仮想マシンに割り当てられる物理メモリの最小の割合を指定します。 予約はパーセント（%）で定義され、値は 0 ～ 100 % を割り当てることができます。

例： メモリを 2 GB に設定し、予約を 25 % に設定した場合、システムにより、仮想マシンに 512 MB 以上が確保されます。

CPU 予約

この仮想マシンに予約される物理 CPU パフォーマンスの割合の最小値を指定します。 予約はパーセント（%）で定義され、値は 0、50、または 100 % を割り当てることができます。

例： 予約を 50 % に設定した場合、システムにより、各 CPU コアの CPU 時間は 50 % 以上が確保されます。

CPU 制限

この仮想マシンが割り当てることができる CPU パフォーマンスの最大のパーセンテージを指定します。

注: 制限の値は、予約用にしていた値以上である必要があります。

（オプション）仮想ディスクの作成

仮想ディスクはユーザ固有のデータを格納するためのもので、仮想マシンに接続されています。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切なストレージ クラスタを右クリックします。

   ポップアップ メニューが表示されます。

3. ［管理］-［ディスクの作成］を選択します。

   ［ディスクの作成］ダイアログ ボックスが表示されます。

4. 以下のパラメータを指定して、［OK］をクリックします。

   - ディスク名
   - ディスク タイプ（ユーザ ディスクまたは共有ディスク）。ユーザ ディスクは 1 つの仮想マシンに接続できます。 共有ディスクは複数の仮想マシンに接続できます。
   - 動的な割り当て（通常またはシン プロビジョニング）

     シン プロビジョニングには IP SAN デバイス サポートが必要です。
   - ディスク サイズ（GB）
   - 仮想ディスクの説明

   CA Server Automation は仮想ディスクを作成します。仮想ディスクのリストを取得するには、［ストレージ クラスタ］パネルの［詳細］タブを開きます。

（オプション）仮想マシンへの仮想ディスクの接続

指定された仮想ディスク タイプに従って、1 つの仮想マシンにユーザ ディスクを、複数の仮想マシンに共有ディスクを接続することができます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開し、適切なストレージ クラスタを選択します。

   ［ストレージ クラスタ］パネルが表示され、指定された仮想ディスクがリスト表示されます。

3. 接続する仮想ディスクを選択し、接続アイコンをクリックします。

   利用可能な仮想ディスクのリストが表示されます。

4. 適切な仮想マシンを選択し、［OK］をクリックします。

   仮想ディスクが接続されます。

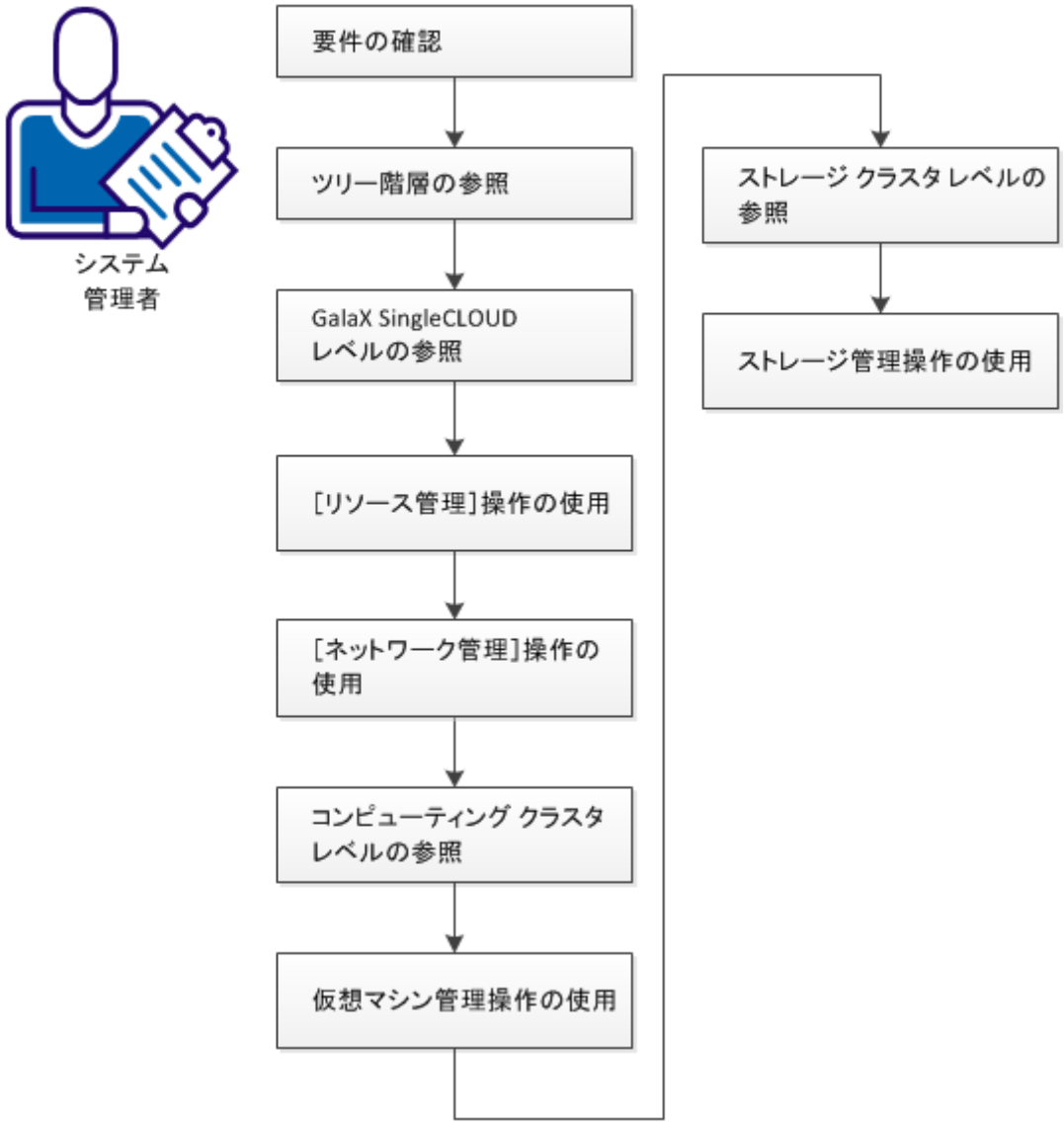
VPC VLAN とそのコンポーネントの管理

通信に VLAN を使用する仮想ディスクが接続された仮想マシンが指定されているとします。 これらのリソースは、CA Server Automation によって管理できる Virtual Private Cloud に属します。

Huawei SingleCLOUD 環境を管理する方法

ユーザ インターフェースの大部分が見たとおりの内容であるため、このシナリオは Huawei SingleCLOUD 環境のオブジェクト階層を検索し、関連する管理機能を参照するためのガイドラインです。

Huawei SingleCLOUD 環境を管理する方法



以下の手順に従います。

要件の確認

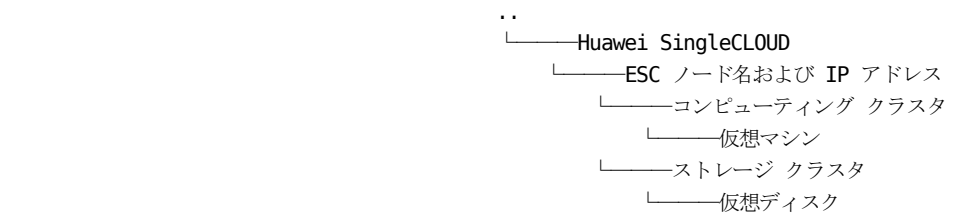
CA Server Automation 内の Huawei SingleCLOUD インスタンスを管理する前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Server Automation ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- モニタリング ソフトウェア（SystemEDGE）の展開および設定に精通していること。
- CA Server Automation がインストールされており、CA Server Automation ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ（仮想マシン用）およびストレージ クラスタ（仮想ディスク用）が Huawei GalaX 環境で利用可能であること。
- 仮想マシンに適用するオペレーティング システムのイメージが Huawei GalaX 環境で利用可能であること。
- CA Server Automation と Huawei GalaX サーバの間の接続が確立されていること。
- GalaX AIM が Huawei GalaX サーバをモニタするように設定されていること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Server Automation が Huawei GalaX サーバとその関連リソース（クラスタ、ストレージ クラスタ、仮想マシンなど）を検出していること。
- 仮想マシンを備えた Virtual Private Cloud が利用可能である。

ツリー階層の参照

SingleCLOUD vCloud フォルダは、最上位のサービス レベルを表します。SingleCLOUD サービスは 1 つ以上の Elastic Service Controller （ESC）から構成されます。 各 ESC は、仮想マシンと仮想ディスクを備えた複数のコンピューティング クラスタおよびストレージ クラスタを制御できます。

以下の図は、SingleCLOUD vCloud フォルダのオブジェクト階層を表しています。



次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   ［エクスプローラ］ツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開します。

   - Huawei SingleCLOUD イベントのリストを開くには、Huawei SingleCLOUD オブジェクトを選択します。
   - リソース管理とネットワーク管理にアクセスするには、ESC ノードを選択します。
   - 利用可能な仮想マシンのリストを取得するか、または仮想マシンを作成するには、コンピューティング クラスタを選択します。
   - 利用可能な仮想ディスクのリストを取得するか、または仮想ディスクを作成するには、ストレージ クラスタを選択します。

GalaX SingleCLOUD サーバ レベルの参照

GalaX SingleCLOUD は、ツリー階層内の 2 番目のレベルに存在します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   エクスプローラのツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開します。

   フォルダ階層が表示されます。

3. ESC ノードを選択します。

   ［リソース管理］および［ネットワーク管理］タブが表示されます。

   - スナップショット、イメージ、およびユーザ指定には［リソース管理］を使用します。
   - VPC VLAN およびユーザ VLAN には［ネットワーク管理］を使用します。

［リソース管理］操作の使用

ユーザ インターフェースは、［リソース管理］タブ下で以下の操作を提供します。

- スナップショットとそれらのプロパティの表示
- 仮想マシンへのスナップショットのリストア
- スナップショットの削除
- イメージとそれらのプロパティの表示
- ユーザ指定とそれらのプロパティの表示
- ユーザ指定の作成
- ユーザ指定の編集
- ユーザ指定の削除

使用方法とダイアログ ボックスから内容がわかるようになっています。必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

[ネットワーク管理]操作の使用

ユーザ インターフェースは、［リソース管理］タブ下で以下の操作を提供します。

- VPC VLAN の作成
- VPC VLAN およびそれらのプロパティの表示
- VPC VLAN の削除
- ユーザ VLAN の割り当て
- ユーザ VLAN の削除

使用方法とダイアログ ボックスから内容がわかるようになっています。必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

コンピューティング クラスタ レベルの参照

コンピューティング クラスタはツリー階層内の 3 番目のレベルに存在します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。［管理］-［リソース］をクリックします。

   エクスプローラのツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開します。

   フォルダ階層が表示されます。

3. コンピューティング クラスタを選択するか展開します。

   使用可能な仮想マシンのリストが表示されます。

4. コンピューティング クラスタを右クリックして、仮想マシンを作成します。

   システム ボリューム（リソース管理）用のディスクとオペレーティング システムを含むイメージ、VPC VLAN、ユーザ指定（オプション）、ユーザ VLAN （オプション）が必要です。

5. 仮想マシン管理操作を実行する仮想マシンを右クリックします。

   適用不可の操作は利用できなくなっています。

仮想マシン管理操作の使用

ユーザが仮想マシンを右クリックするときに、ユーザ インターフェースは、仮想マシン用の管理操作を提供します。 使用方法とダイアログ ボックスから内容がわかるようになっています。

- VM の削除
- VM の再起動
- VM の電源オン
- VM の電源オフ
- VM のセーフ再起動（オペレーティング システムのシャットダウン）
- VM のセーフ電源オフ（オペレーティング システムのシャットダウン）
- VM のハイバネート
- VM の始動
- VM 名の変更
- 初期パスワードの表示
- ブート順序の設定
- スナップショットのロールバック
- VM スナップショットの作成

以下の管理操作には、追加の説明が必要です。

- CPU 設定および QoS の変更
- メモリ設定および QoS の変更
- VNC ログイン
- ツールのマウント/マウント解除

CPU 設定および QoS の変更

以下の値を指定します。

CPU 数

仮想マシンに割り当てられる CPU コアの数を指定します。仮想マシンに割り当てることができる CPU コアの最大数は、8 です。

例： この数値を 5 に設定した場合、5 つの CPU コアが仮想マシンに対して利用可能になります。

予約

この仮想マシンに予約される物理 CPU パフォーマンスの割合の最小値を指定します。 予約はパーセント（%）で定義され、値は 0、50、または 100 % を割り当てることができます。

例： 予約を 50 % に設定した場合、システムにより、各 CPU コアの CPU 時間は 50 % 以上が確保されます。

制限

この仮想マシンが割り当てることができる CPU パフォーマンスの最大のパーセンテージを指定します。

注: 制限の値は、予約用にしていた値以上である必要があります。

メモリ設定および QoS の変更

以下の値を指定します。

メモリ

仮想マシンに割り当てるメモリの量を指定します。 メモリは、512 MB ～ 256 GB の範囲でメガバイト（MB）で定義されます。

例： メモリを 512 MB に設定した場合、仮想マシンに割り当てることができるメモリの最大値は 512 MB になります。

予約

仮想マシンに割り当てられる物理メモリの最小の割合を指定します。予約はパーセント（%）で定義され、値は 0 ～ 100 % を割り当てることができます。

例： メモリを 2 GB に設定し、予約を 25 % に設定した場合、システムにより、仮想マシンに 512 MB 以上が確保されます。

VNC ログイン

VNC を使用して VM にアクセスできるようにするには、VNC ログインでの初期設定が必要です。VncViewer.jar をダウンロードし、それを CA Server Automation マネージャ システムにインストールします。

次の手順に従ってください:

1. CA Server Automation マネージャ サーバにログインし、ユーザ インターフェースを開きます。エクスプローラ ツリーを展開し、Huawei SingleCloud VM を右クリックして、［管理］-［VNC ログイン］を選択します。

   手順を示すメッセージが表示されます。

2. CA Server Automation マネージャ サーバから ESC または OMM サーバに接続し、以下のディレクトリから VncViewer.jar をダウンロードします。

   ```
   /opt/omm/oms/webapps/oms/business/resourcemanage/virtualresources
   ```

3. 再度［VNC ログイン］をクリックします。

   メッセージ ダイアログ ボックスが開きます。

4. ダイアログ ボックスのメッセージをクリックします。

   ［ファイルのアップロード］ダイアログ ボックスが表示されます。

5. ［参照］をクリックし、ダウンロードされた VncViewer.jar ファイルに移動して、［開く］をクリックします。

   ［ファイル パス］がダイアログ ボックスに表示されます。

6. ［OK］をクリックします。

   CA Server Automation は、VncViewer.jar を以下にアップロードします。*Install_Path*¥*product*¥tomcat¥webapps¥UI directory.

   VNC ビューアが自動的に開き、VM に接続します。

この手順を完了すると、VNC ログインが利用可能になり、お使いの環境内の任意の Huawei SingleCloud VM にリモートでアクセスできるようになります。

ツールのマウント/マウント解除

機能を最大限に利用するには、SingleCloud ツールを VM にインストールします。

次の手順に従ってください:

1. CA Server Automation マネージャ サーバにログインし、ユーザ インターフェースを開きます。エクスプローラ ツリーを展開し、VM を右クリックして、［管理］-［ツールのマウント/マウント解除］を選択します。

   CA Server Automation のダイアログ ボックスに、現在の VM ステータスおよび SingleCloud ツールのステータスが表示されます。

2. SingleCloud ツール ステータスを変更してマウント/マウント解除するには、［OK］をクリックします。

3. SingleCLOUD ツールを VM に正常にマウントした後、PV ドライバをインストールします。VM が Linux OS 上で実行されている場合は、VM を再起動して、PV ドライバをインストールします。

リソース割り当てのベスト プラクティス

Huawei SingleCLOUD 環境で仮想マシンに適したリソース割り当て設定（予約および制限）を指定します。

以下のガイドラインは、仮想インフラストラクチャの最適なパフォーマンスを実現するうえで役立ちます。

- 使用したい量ではなく、許容できる*最小限の* CPU またはメモリの量を指定するために、予約を使用します。 ホストは、仮想マシンの予測される需要および制限に基づいて、利用可能な追加のリソースを割り当てます。 仮想マシンの追加または削除などの環境の変更を行う場合、予約によって指定した CPU またはメモリの量は変わりません。
- 仮想マシンの予約を指定するときに、すべてのリソースをコミットしないでください。 予約量がシステム容量の限界に近くなると、予約の変更が著しく困難になるため、未予約の部分が適宜残るようにしてください。

ストレージ クラスタ レベルの参照

ストレージ クラスタはツリー階層内の 3 番目のレベルに存在します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［リソース］をクリックします。

   エクスプローラのツリーが開きます。

2. Huawei SingleCLOUD フォルダを展開します。

   フォルダ階層が表示されます。

3. ストレージ クラスタを展開します。

   使用可能な仮想ディスクのリストが表示されます。

4. ストレージ クラスタを右クリックして、仮想ディスクを作成します。

   以下のダイアログ ボックスには追加の説明が必要です。

   ディスク タイプ: **ユーザ ディスク**

   1 つの仮想マシンに接続できます。

   ディスク タイプ: **共有ディスク**

   複数の仮想マシンに接続できます。

   動的な割り当て: **シン プロビジョニング**

   指定されたディスク領域を予約しますが、その領域にデータを格納する必要が生じるまでは、ディスクの予約領域全体を完全には確保しません。 シン プロビジョニングの仮想ディスクのサイズは、格納されるデータの量に応じて増加します。

   シン プロビジョニングによりデータストアの超過割り当てが可能になり、予約済みであっても使用されていないディスク領域を最小化することにより、格納に使用できる領域を増加させることができます。

5. ［エクスプローラ］ツリーで仮想ディスクを右クリックし、仮想ディスク管理操作を実行します。

   仮想ディスクの詳細を表示するか、または仮想ディスクを削除できます。

ストレージ管理操作の使用

ユーザが仮想マシンを右クリックするときに、ユーザ インターフェースは、仮想マシン用の管理操作を提供します。 使用方法とダイアログ ボックスから内容がわかるようになっています。

- 仮想ディスクの削除
- 仮想ディスクの詳細の表示
- 仮想ディスクのイベントを表示する仮想ディスクの選択

利用可能な仮想ディスクのリストを開くにはストレージ クラスタを選択します。 以下の操作を使用できます。

- 仮想ディスクの接続
- 仮想ディスクの接続解除
- 仮想ディスクの削除

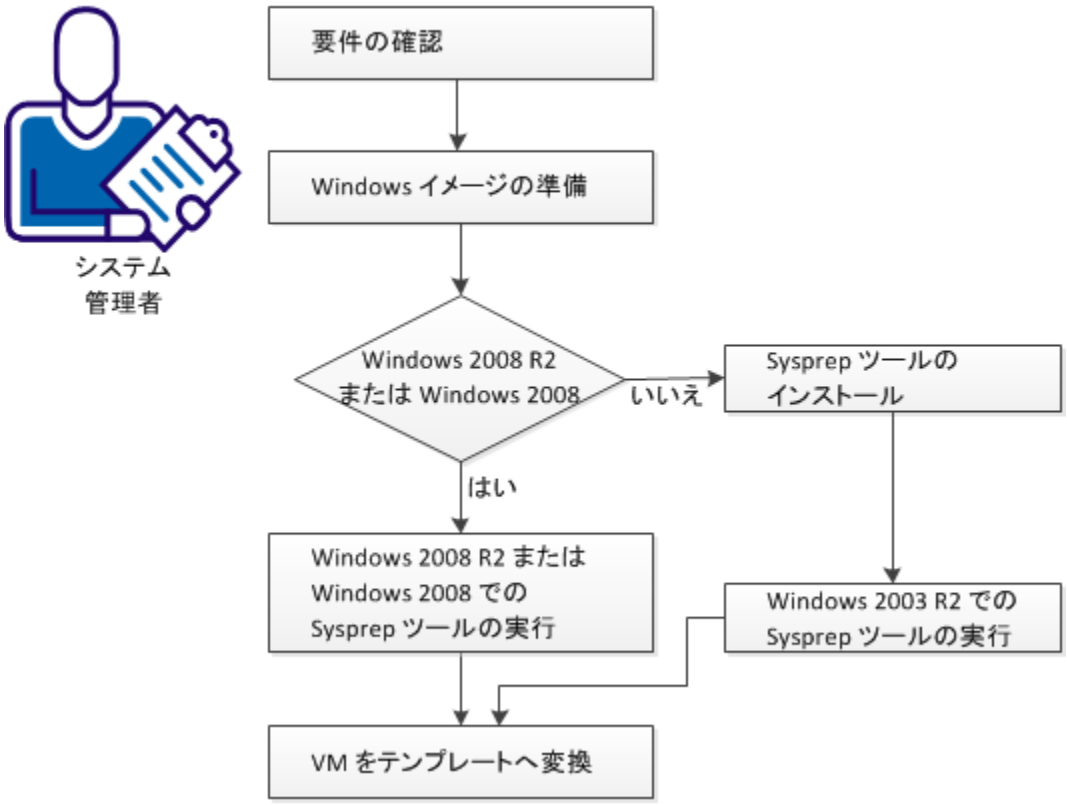
使用方法は意味がわかるようになっています。 必要な場合、ツールヒントを表示させるためにアイコン上にカーソルを移動することができます。

GalaX のプロビジョニング用に Windows テンプレートを準備する方法

CA Server Automation では、Windows 2003 R2 Server（32 ビット/64 ビット）、Windows 2008 （32 ビット/64 ビット）または Windows 2008 R2 Server （64 ビット）を実行する新しい仮想マシン（VM）でのプロビジョニングのカスタマイズをサポートしています。 カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が GalaX のプロビジョニング用に Windows テンプレートを準備する方法を示しています。

VM のプロビジョニング用にテンプレートを作成する方法



Microsoft sysprep ツールでは、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンが可能です。 以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Windows 2003 では、Sysprep ツールはデフォルトではインストールされませんが、Windows インストール CD-ROM に収録されています。

以下の手順に従います。

要件の確認

CA Server Automation での仮想マシン プロビジョニング用テンプレートを作成する前に、以下の前提条件を確認します。

- Huawei GalaX 環境に精通していること。
- CA Server Automation ユーザ インターフェース、およびリソースをプロビジョニングする方法に精通していること。
- CA Server Automation がインストールされており、CA Server Automation ユーザ インターフェースにアクセスできること。
- Huawei GalaX 環境が利用可能で、実行されていること。
- コンピューティング クラスタのサーバ（仮想マシン用）およびストレージ クラスタ（仮想ディスク用）が Huawei GalaX 環境で利用可能であること。
- ユーザ VLAN プールおよび VPC VLAN プール用のサーバが利用可能であること。
- CA Server Automation が Huawei GalaX サーバとその関連リソース（クラスタ、ストレージ クラスタ、仮想マシンなど）を検出していること。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従って、イメージを準備します。 テンプレートをカスタマイズするには、CA Server Automation のプロビジョニング操作を有効にする手順に従ってください。 一部の手順は Windows のバージョンによって異なります。

次の手順に従ってください:

1. Windows オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシンに SingleCloud ツールをインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。

   ¥SUPPORT¥TOOLS¥DEPLOY.CAB

2. CAB ファイルに含まれるファイルをすべて選択し、%SystemDrive%¥Sysprep （通常は C:¥Sysprep）にコピーします。

   注: ディレクトリ名は変更しないでください。

3. Sysprep ディレクトリに移動して、以下を実行します。

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

Windows 2008 R2 での Sysprep ツールの実行

通常の Windows セットアップでは、Sysprep プロセスを実行するためのすべてのファイルがインストールされます。 Windows インストールを設定した後、以下の手順を実行します。

1. 以下のディレクトリに移動します。

   C:¥Windows¥system32¥sysprep

2. 以下のコマンドを実行します。

   ```
   sysprep /generalize /shutdown
   ```

sysprep コマンドはインストール用イメージを準備し、仮想マシンをシャットダウンします。 generalize パラメータは、コンピュータ名、ログファイル、リストア ポイント、およびハードウェア固有情報などの一意のシステム情報をすべて削除します。

VM を GalaX のテンプレートへ変換

sysprep コマンドが仮想マシンをシャット ダウンした後、テンプレートを作成するために SingleCloud ユーザ インターフェースに移動します。

次の手順に従ってください:

1. SingleCloud ユーザ インターフェースにログインします。
2. ［VM］タブをクリックし、sysprep で準備した仮想マシンを選択します。
3. 仮想マシンを右クリックし、［イメージのエクスポート］を選択します。

   ［イメージのエクスポート］ダイアログ ボックスが表示されます。

4. ファイル名を指定し、［イメージ タイプ］を「ゴースト」に設定して［OK］をクリックします。

   仮想マシンはゴースト イメージとして保存されます。

5. SingleCloud ユーザ インターフェースでゴースト イメージを登録します。

   ゴースト イメージをプロビジョニング用のテンプレートとして使用できるようになりました。

プロビジョニングされた仮想マシンの使用

前のシナリオ (P. 439)に従って作成されたテンプレートを使用すると、プロビジョニングされた仮想マシンの動作が以下のようになります。

プロビジョニングされた仮想マシンを最初に起動する際、起動プロセスは、ロケール設定、製品キー、EULA などのユーザ入力を待機し、この特定のマシン用のホスト名の指定が可能になります。

仮想マシンにアクセスするには、VNC が利用可能であることを確認します。

IBM PowerVM（LPAR）

IBM PowerVM システムは、システムを論理パーティション（LPAR）に分割する機能を提供します。 論理パーティションはそれぞれ独立したシステムとして実行されます。また、パーティション間でリソースを分散することもできます。通常、各システムにはディスク リソースおよびネットワーク インターフェースを仮想化する仮想 I/O サーバ（VIOS）という専門のパーティションがあります。 システムを分割することにより、個別のコンピューティング ニーズを考慮しながら、仮想リソースを動的に共有できます。 PowerVM システムには、ハードウェア管理コンソール（HMC）または Integrated Virtualization Manager （IVM）のいずれかである仮想化マネージャ コンポーネントがあります。 HMC は、個別のシステム上で実行されるアプライアンスで、複数の PowerVM システムを管理するために使用されます。IVM は仮想 I/O サーバに対する拡張で、ローカル PowerVM システムのみを管理できます。

PowerVM AIM を使用して、SystemEDGE で LPAR のリソースをモニタリングできます。

LPAR プラットフォーム管理モジュール（PMM）は、すべての LPAR 操作に対する接続と運用上のサポートを提供します。 PMM は、接続管理、ハードウェア管理コンソール（HMC）または Integrated Virtualization Manager （IVM）からのデータ取得、さまざまな LPAR 関連操作の実行、データベースへの取り込み、およびすべての HMC/IVM インタラクションに対する Web サービス/SSH の提供を行います。

HMC/IVM から管理対象システムおよび LPAR のデータを取得し、以下の LPAR 関連操作を実行できます。

サーバ レベル

サーバ レベルで、以下のタスクを実行できます。

- LPAR のプロビジョニング
- LPAR の削除

電源操作レベル

電源操作レベルで、以下のタスクを実行できます。

- LPAR のアクティブ化
- LPAR のシャットダウン
- LPAR の再起動

リソース調整レベル

リソース調整レベルで、以下のタスクを実行できます。

- LPAR プロセッサおよびメモリ ユニットの追加
- LPAR プロセッサおよびメモリ ユニットの削除

IBM PowerVM サーバ管理の概要

CA Server Automation の CA IBM PowerVM コンポーネントでは、IBM PowerVM リソースをモニタおよび管理できます。 モニタおよび管理されるリソースには以下のタイプがあります。

- ハードウェア管理コンソール（HMC）
- Integrated Virtualization Manager （IVM）
- 仮想 IO サーバ（VIOS）
- 管理対象システム（POWER サーバ）
- 論理パーティション（LPAR）

*ハードウェア管理コンソール（HMC）*は、IBM PowerVM システム上で管理タスクを実行するために使用する外部アプライアンスです。 HMC は、リソースをパーティションに動的に割り当てるなど、論理パーティションを作成または変更するのに使用できます。HMC は POWER システムのサーバファームウェア層と通信し、大規模 PowerVM 環境での単一制御ポイントを提供します。

*Integrated Virtualization Manager （IVM）*は仮想 I/O サーバ（VIOS）の機能拡張で、単一の POWER システムを管理できます。 IVM では、LPAR を作成し管理できます。IVM では、VIOS 機能の管理を可能にし、Web ベースユーザ インターフェースを提供します。

*仮想 I/O サーバ（VIOS）*は、すべての物理 I/O リソースを所有するように設定された特別な論理パーティションで、その仮想化機能をほかの LPAR に提供します。LPAR は、仮想 I/O サーバを介して仮想デバイスとしてディスク、ネットワーク、および光学デバイスにアクセスします。 仮想化されたリソースを持つ PowerVM システムには、それぞれ仮想 I/O サーバがあります。

*論理パーティション（LPAR）*は、独立したシステムとして仮想化される、ハードウェア リソースのサブセットです。物理システムは複数の LPAR に分割でき、それぞれの LPAR が個別のオペレーティング システムとアプリケーションを提供します。 論理パーティションの数は、システムのハードウェア構成によって異なります。 LPAR はネットワーク内で別々のシステムとして通信します。

IBM PowerVM リソースを管理するには、HMC/IVM サーバと仮想 I/O サーバに SSH アクセス認証情報を提供します。

CA Server Automation の［管理］-［設定］-［プロビジョニング］-［IBM PowerVM］グループを使用して、PowerVM リソースを管理するよう CA Server Automation を設定できます。

以下のパネルを使用できます。

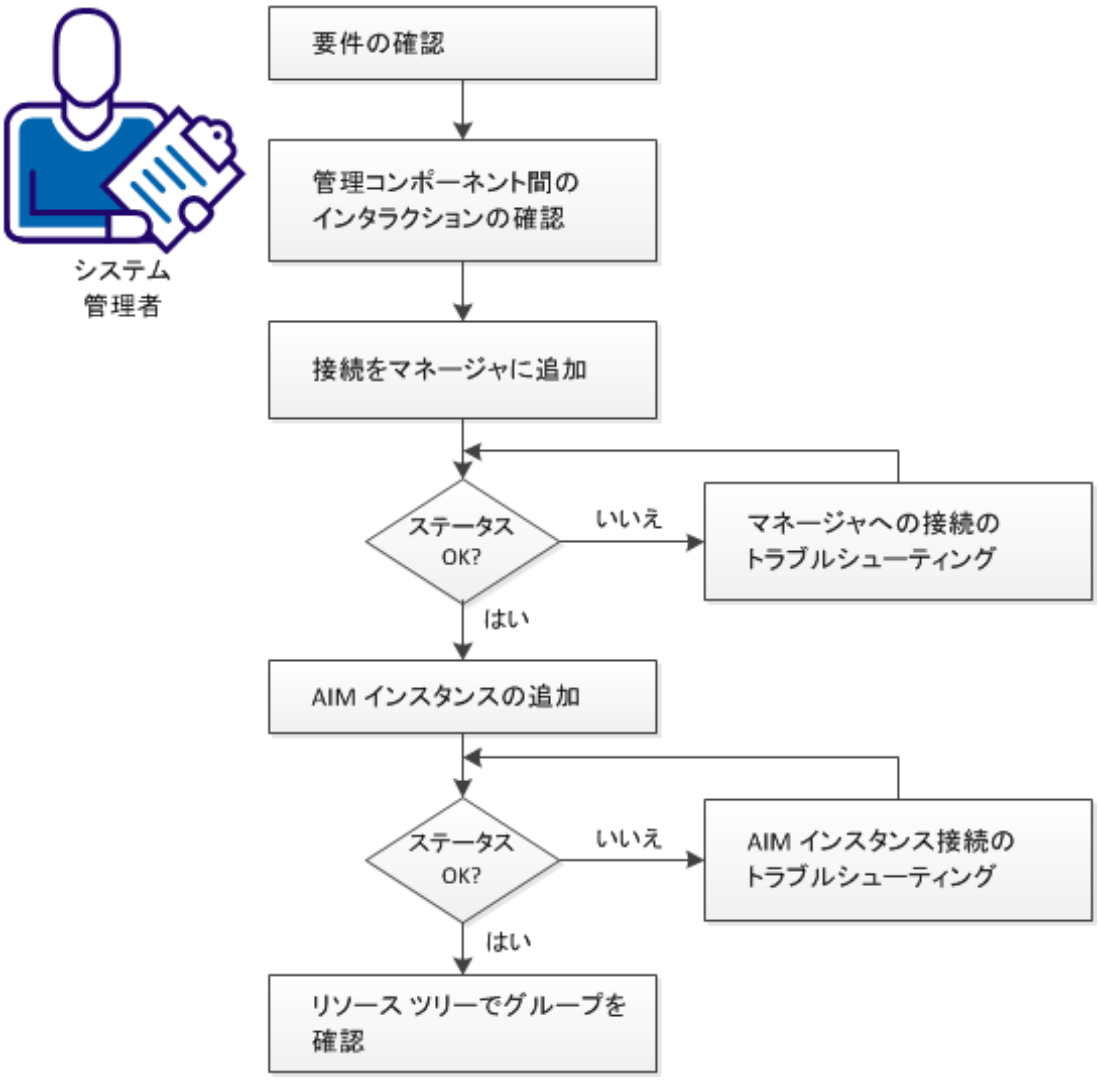
- HMC/IVM サーバ
- 仮想 I/O サーバ
- LPAR AIM サーバ

LPAR AIM サーバは、SystemEDGE および LPAR AIM が実行されるシステムです。 LPAR AIM は、ローカル CA Server Automation マネージャ システムまたはリモート Windows サーバ上で実行できます。 LPAR AIM はマルチインスタンス AIM で、複数の HMC または IVM に接続できます。 AIM が HMC または IVM サーバの管理を開始すると、この HMC または IVM サーバに接続されている P-Server が AIM によってすべて検出および管理されます。

PowerVM 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

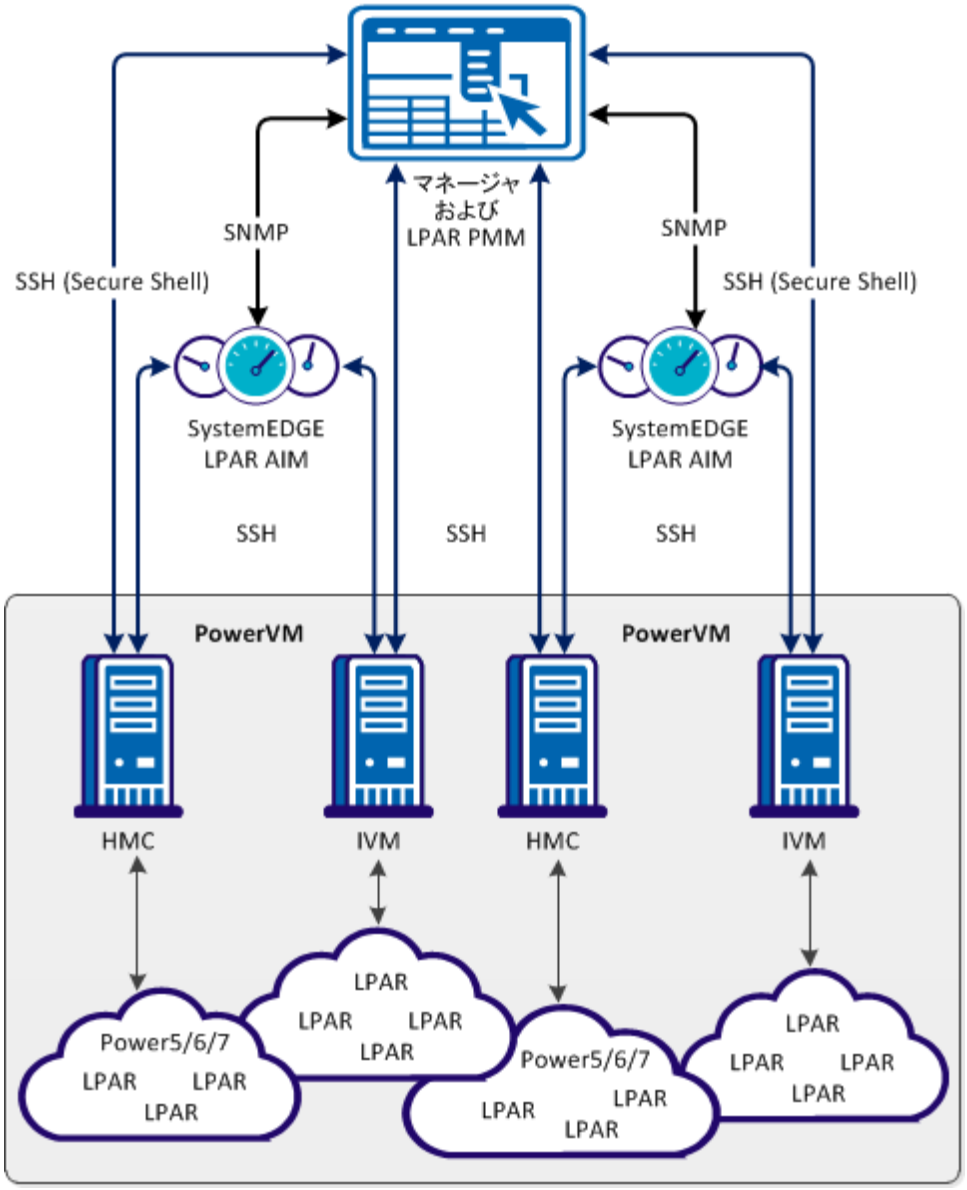
- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

AIX LPAR 管理コンポーネント間のインタラクション

以下の図は、IBM LPAR 管理に関与するコンポーネントがどのように対話するかを示しています。 AIM サーバとは、SystemEDGE および LPAR AIM が稼働する Windows サーバです。 AIM と HMC/IVM サーバの間の通信は SSH（Secure Shell）に基づいています。 CA Server Automation は複数の HMC サーバまたは IVM サーバ接続できるため、CA Server Automation ではお使いの LPAR 環境全体のビューが取得できます。

PowerVM 管理コンポーネント間のインタラクション



インストールの後、必要な HMC/IVM および仮想 I/O サーバに接続情報を追加して、環境を設定します。 以下の*いずれか*の方法を使用します。

- ユーザ インターフェースの［管理］タブ
- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

接続情報は管理対象ノード上の設定ファイルに書き込まれます。LPAR AIM は設定ファイルをポーリングし、HMC/IVM を通じて LPAR 環境のモニタリングを開始します。

IBM PowerVM 設定の使用例

以下の使用例では、［管理］タブにおける管理対象の PowerVM 環境の LPAR AIM インスタンス エントリの扱いについて説明します。

- HMC サーバおよび LPAR AIM インスタンスを追加します。

  AIM は以下を検出します。

  - HMC と関連付けられている Power システム。
  - Power システムと関連付けられている仮想 I/O サーバ。 HMC を追加するときに指定したデフォルトの VIOS 認証情報が適用されている AIM。

    重要: HMC サーバ用のデフォルトの VIOS 認証情報を指定しない場合は、［仮想 I/O サーバ］パネルで各 VIOS の VIOS 認証情報を指定して、検出された VIOS を設定します。 デフォルトの VIOS 認証情報が特定の VIOS に適用されない場合は、［仮想 I/O サーバ］パネルの認証情報を上書きできます。

- 優先 AIM

  2 つの AIM で 1 つの HMC を管理できます。2 番目の AIM が追加されると、これは冗長 AIM になります、最初に追加された AIM は優先 AIM になります。 冗長 AIM の下の HMC のステータスは中断になります。 このステータスは、HMC が優先 AIM によって管理されていることを反映しています。優先 AIM は［HMC/IVM サーバ］パネルで変更できます。

- デュアル HMC 機能は、1 台の Power システムを 2 台の HMC サーバと関連付ける設定をサポートしています。

  P-Server および関連付けられた HMC サーバは、1 まとまりの管理エンティティで、1 つの AIM によって管理する必要があります。 デュアル HMC の設定では、1 つの AIM のスコープでのみサポートされています。たとえば、ある Power システム（P1）を、2 台の HMC サーバ（HMC1 および HMC2）に接続します。 両方の HMC サーバは 1 つの AIM （AIM1）によって管理されます。

- デュアル HMC によるフェールオーバ

  優先 HMC に障害が発生した場合、冗長 HMC がシステムの管理を自動的に開始します。 冗長 HMC が現在の HMC になります。 ただし、優先 HMC が利用可能になっても、現在の HMC は変更されません。 優先 HMC によって再度システムを管理するには、［管理］-［設定］タブにある［LPAR AIM サーバ］パネルで現在の HMC を変更します。

  注: 優先 HMC に障害が発生すると、冗長 HMC によってシステムが管理されます。 フェールオーバ後、システムに対する現在の HMC は手動で変更できます。

- デフォルトの VIOS 認証情報に正しくない仮想 I/O サーバ認証情報は指定できません。

  ユーザ インターフェースに、操作の失敗を示すメッセージが表示されます。正しくない仮想 I/O サーバ認証情報を適用しようとすると()、仮想 I/O サーバの状態は「認証失敗」に変わります。 接続の問題により、管理対象システム インスタンスの状態は「VIOS 待ち」から「期限切れ」に変わります。

- 仮想 I/O サーバなしで管理対象システム インスタンスを追加します。

  管理対象システム インスタンスが「準備完了」の状態でインスタンス テーブルに表示されます。

- P-server を管理対象システムに追加します。

  新しい P-server および VIOS は自動的に検出されます。 VIOS 認証情報がデフォルトの VIOS 認証情報と同じである場合、設定は必要ありません。 VIOS 認証情報がデフォルト VIOS 認証情報と同じでない場合は、AIM インスタンスに VIOS 認証情報を設定します（）。

- 「設定が無効」状態の仮想 I/O サーバを管理対象システムから削除します。

  LPAR AIM は、対応するレコードをインスタンス テーブルから削除し、管理対象システムの状態は「準備完了」に変わります。

- 「準備完了」状態の仮想 I/O サーバを管理対象システムから削除します。

  LPAR AIM は、対応するレコードをインスタンス テーブルから削除します。

- 1 つまたは 2 つの仮想 I/O サーバを含む管理対象システム インスタンスを削除します。

  管理対象システム インスタンスおよび関連付けられた仮想 I/O サーバのエントリが、インスタンス テーブルに表示されなくなります。

- IBM PowerVM 管理ペインでは、ステータス情報がアイコンとツールヒントによって表示されます。

  詳細なツールヒントは、警告およびエラーのアイコンの上にカーソルを置くと表示されます。

  以下のアイコンが表示されます。

   ディスカバリが進行中

   ポーリングなし

   エラー

   警告

   無効

   不明

HMC または IVM サーバ接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、HMC または IVM サーバ接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［IBM PowerVM］を選択します。

   右側のペインがリフレッシュされ、管理対象の HMC サーバ、IVM サーバ、関連付けられている仮想 I/O サーバ、および LPAR AIM サーバが表示されます。

3. ［HMC/IVM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［新しい HMC/IVM サーバ］ ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード）を入力し、優先 AIM を指定して、［管理ステータス］（チェック ボックス）をオンにします。
   注: 指定された HMC または IVM サーバに対して複数の AIM インスタンスを指定した場合にのみ、優先 AIM フィールドがアクティブになります。

5. （オプション）仮想 I/O サーバのデフォルト認証情報を指定します。

   仮想 I/O サーバのデフォルト認証情報は、新しく検出された仮想 I/O サーバに適用されます。

   重要: HMC サーバ用のデフォルトの VIOS 認証情報を指定しない場合は、［仮想 I/O サーバ］パネルで各 VIOS の VIOS 認証情報を指定して、検出された VIOS を設定します。 デフォルトの VIOS 認証情報が特定の VIOS に適用されない場合は、［仮想 I/O サーバ］パネルの認証情報を上書きできます。

6. ［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上の［HMC/IVM サーバ］ペインにサーバが緑のステータス アイコンを使って追加されます。 CA Server Automation によって HMC/IVM サーバが自動的に検出されます。

接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

［管理］ - ［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の  （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバ システムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

LPAR AIM インスタンスの追加

CA Server Automation マネージャに HMC または IVM サーバ接続を追加した後、新しいサーバを管理するための AIM インスタンスを追加します。その後、CA Server Automation によって PowerVM 環境が検出されます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［IBM PowerVM］を選択します。

   右側のペインがリフレッシュされ、管理対象の HMC サーバ、IVM サーバ、関連付けられている仮想 I/O サーバ、および LPAR AIM サーバが表示されます。

3. ［LPAR AIM サーバ］ペイン ツールバーの  （追加）をクリックします。

   ［新しい LPAR AIM サーバ］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［LPAR AIM サーバ］を選択します。

   検出された LPAR AIM サーバのリストが表示されます。 LPAR AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウン リストから［HMC または IVM サーバ］を選択します。

   ［HMC/IVM サーバ］ペインに一覧表示された HMC または IVM サーバが［HMC/IVM サーバ］ドロップダウン リストに入力されます。 管理できる HMC または IVM サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている PowerVM 環境の検出を開始します。

   - 各 HMC サーバについては、AIM はすべての Power システムと仮想 I/O サーバを検出します。
   - 各 IVM サーバについては、AIM は IVM が管理する Power システムを検出します。

   ディスカバリ プロセスが完了したら、PowerVM 環境の管理を開始できます。

［管理］タブには、AIM が検出したすべての Power システムと VIO サーバの集計された状態が表示されます。 これらの個別の設定状態を表示するには、［管理対象システムを表示］（  ）アイコンをクリックします。

管理対象 Power システムの優先 HMC の変更

Power システムでデュアル HMC を使用する場合は、優先 HMC を変更できます。

重要: 1 つの LPAR AIM でプライマリと冗長用の HMC サーバの両方を管理していることを確認します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［IBM PowerVM］を選択します。

   右側のペインがリフレッシュされ、管理対象の HMC サーバ、IVM サーバ、関連付けられている仮想 I/O サーバ、および LPAR AIM サーバが表示されます。

3. HMC サーバと関連付けられている （管理対象/VIO サーバを設定）をクリックします。

   ［IBM PowerVM］ダイアログ ボックスに管理対象/VIO サーバが表示されます。

4. ［アクション］行の下にある （優先 HMC を切り替えます）をクリックして確認します。

   冗長 HMC が優先 HMC として設定されます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  （無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでグループを確認する

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. IBM PowerVM グループを展開します。

   管理対象の HMC および IVM サーバが表示されます。
3. ［HMC または IVM サーバ］エントリを展開します。

   管理対象システムが表示されます。

CA Server Automation で、追加された PowerVM 環境とその仮想インフラストラクチャを管理する準備が整いました。

calpara.xml ファイル

calpara.xml ファイルの主な目的は、永続データやデフォルト値などの LPAR AIM の設定データを格納することです。モニタリングの設定は、特定の環境に合わせて調整できます。

このドキュメントは、XML 形式に精通しているシステム管理者を対象としています。このファイルを変更するときには、十分に注意してください。calpara.xml ファイルを変更するには、SystemEDGE を終了し、ファイルを変更した後に SystemEDGE を再起動します。

重要: モニタリングのしきい値、遅延、または重大度の調整が必要な場合は、デフォルト値のみを変更します。 ポーリング グループと DisableOutOfDate の設定は、CA サポートから指示された場合にのみ変更してください。

calpara.xml ファイルは以下の場所にあります。

```
<SystemEDGE_InstallDir>¥plugins¥calpara¥calpara.xml
```

永続データ

永続データは AIM が次に開始するときに利用できます。 このデータは AIM の存続期間中に変更でき、SNMP の SET 要求を使用してユーザが設定することができます。

以下に永続データの例を示します。

- インスタンス
- システム
- パーティション
- スロット
- ポーリング グループ

インスタンス

インスタンス テーブル（lparAimInstanceTable）に設定されている各インスタンスについては、以下の例のようなセクションが格納されます。

```
<ManagedInstance>
    <InstIndex>7</InstIndex>
    <SerialNr>1010101</SerialNr>
    <ServerName>vios1.company.com</ServerName>
    <ServerType>vios</ServerType>
    <RowStatus>1</RowStatus>
</ManagedInstance>
```

ServerType

サーバ タイプとして、hmc、vios、または ivm のいずれかを指定します。

RowStatus

ステータスを active （1）または notInService （2）として指定します。

システム

システム テーブル（lparAimStatSysTable）に設定されている管理対象の Power システムについては、以下の例のようなセクションが関連する ManagedInstance セクション内に格納されます。

```
<System>
    <MonitorIndices>530091,530092,530093,530094,530095</MonitorIndices>
</System>
```

MonitorIndices

Power システムの動作ステータス、CPU、およびメモリの使用状況をモニタするために AIM が作成した SystemEDGE モニタのインデックスを格納します。

注: 今後 AIM で Power システムを管理しない場合は、対応するモニタが削除されます。

パーティション

パーティション テーブル（lparAimStatLPTable）内の管理対象の各論理パーティションについては、以下の例のような 4 つの対応するエントリが関連する ManagedInstance セクション内の Partitions セクションに格納されます。

```
<Partitions>
    ...
    <LparIndex>7</LparIndex>
    <LparId>7</LparId>
    <LparName>LPAR12345</LparName>
    <MonitorIndices>530141,530142,530143,530144,530145</MonitorIndices>
    ...
</Partitions>
```

注: 今後 AIM で Power システムを管理しない場合は、対応するモニタが削除されます。

スロット

スロット テーブル（lparAimStatSlotTable）内の各物理スロットについては、以下の例のような 4 つの対応するエントリが関連する ManagedInstance セクション内の Slots セクションに格納されます。

```
<Slots>
    ...
    <SlotIndex>3</SlotIndex>
    <DRCName>U787B.001.DNWFF77-P1-C3</DRCName>
    <DRCIndex>553713666</DRCIndex>
    <SlotName>C3</SlotName>
    ...
</Slots>
```

LPAR AIM では、このデータを使用して、スロットに関係する変更を起動直後に検出します。これによって対応する SNMP トラップが送信される可能性があります。

ポーリング グループ

ポーリング グループは、関連する一連のコマンドであり、すべて同じポーリング間隔で実行されます。 ポーリング テーブル（lparAimPollTable）内の各ポーリング グループについては、それぞれのポーリング グループ セクションに対応する 3 つのエントリが格納されます。 以下の例は、基本ポーリング グループを示しています。

```
<Basic>
    <PollDefault>5</PollDefault>
    <PollSpecific>30,30</PollSpecific>
    <PollInstances>4,6</PollInstances>
</Basic>
```

PollDefault

デフォルト ポーリング間隔（分単位）を格納し、すべてのインスタンスに適用します。ただし、PollInstances に一覧表示されるインスタンス（インスタンスのインデックスのリスト）は除きます。

PollSpecific

PollInstances に格納されたインスタンスのリストに 1 対 1 で対応させて適用するポーリング間隔（分単位）のリストを格納します。

注: PollSpecific と PollInstances は最初は空です。

デフォルト値

以下のセクションでは、calpara.xml ファイルに格納される遅延、しきい値、重大度を指定するデフォルト値について説明します。これらは、AIM によって SystemEDGE モニタを作成するときに使用されます。

重要: デフォルト値は AIM の存続期間中に変更できず、ユーザが設定することもできません。

```
<LowestPollInterval>5</LowestPollInterval>
<DisableOutOfDate>0</DisableOutOfDate>
<MonitorIndexStart>530001</MonitorIndexStart>
<SysAliveSev>fatal</SysAliveSev>
<CpuLagValue>3</CpuLagValue>
<CpuThresh1Val>95</CpuThresh1Val>
<CpuThresh1Sev>warning</CpuThresh1Sev>
<CpuThresh2Val>98</CpuThresh2Val>
<CpuThresh2Sev>critical</CpuThresh2Sev>
<MemLagValue>2</MemLagValue>
```

```
<MemThresh1Val>95</MemThresh1Val>
<MemThresh1Sev>warning</MemThresh1Sev>
<MemThresh2Val>98</MemThresh2Val>
<MemThresh2Sev>critical</MemThresh2Sev>
```

LowestPollInterval

許可されている最短のポーリング間隔（分単位）を格納します。

DisableOutOfDate

データ ステータス（lparAimInstDataStatus） outOfDate を除外するかどうかを指定します。

注: コマンド実行が失敗した場合に、outOfDate(7) になったデータ ステータスを無効にするには、この変数を 1 に設定します。

デフォルト： 0

MonitorIndexStart

AIM がスタートアップ後に作成する最初の SystemEDGE モニタのインデックスを指定します。

注: 新しいモニタを作成する場合、AIM は常に、等しいかより大きい、次に空いているインデックスを検索します。

SysAliveSev

Power システムまたは論理パーティションの動作ステータスをモニタするために AIM が作成する SystemEDGE モニタの重大度を指定します。

有効な値： ok、warning、minor、major、critical、fatal。

注: この値を変更しても、既存のモニタに影響はありません。

CpuThresh1Val と CpuThresh2Val

Power システムまたは論理パーティションの CPU 使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタのしきい値を指定します。

値の範囲： 0 ～ 100。

注: この値を変更しても、既存のモニタに影響はありません。

CpuThresh1Sev と CpuThresh2Sev

Power システムまたは論理パーティションの CPU 使用率のモニタするために AIM が作成する 2 つの SystemEDGE モニタの重大度を指定します。

有効な値： ok、warning、minor、major、critical、fatal。

注: この値を変更しても、既存のモニタに影響はありません。

MemThresh1Val と MemThresh2Val

Power システムまたは論理パーティションのメモリ使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタのしきい値を指定します。

値の範囲： 0 ～ 100。

注: この値を変更しても、既存のモニタに影響はありません。

MemThresh1Sev と MemThresh2Sev

Power システムまたは論理パーティションのメモリ使用率をモニタするために AIM が作成する 2 つの SystemEDGE モニタの重大度を指定します。

有効な値： ok、warning、minor、major、critical、fatal。

注: この値を変更しても、既存のモニタに影響はありません。

CpuLagValue と MemLagValue

Power システムまたは論理パーティションの CPU とメモリ使用率をモニタするために AIM が作成する SystemEDGE モニタの遅延値を指定します。 遅延値には、モニタがその数に到達するとステータスが変わる連続するポーリング間隔（基本ポーリング グループ）の数を指定します。

注: この値を変更しても、既存のモニタに影響はありません。

LPAR モニタリング

LPAR リソースをモニタするには、UI 機能を使用せず、sysedge.cf ファイル内に LPAR AIM MIB に基づく SystemEDGE モニタおよび SystemEDGE コンポーネント オブジェクト モデルを作成します。適切なオブジェクト クラスを使用し、LPAR リソースに応じてオブジェクト インスタンスを指定します。 作成されてモニタされた LPAR オブジェクトは、LPAR AIM がインストールされているコンピュータ システムにそれらの状態を伝達します。以下の例のように、monObjInstance 属性に HMC、POWER5/POWER6/POWER7 および LPAR システム情報を提供することをお勧めします。

例

sysedge.cf ファイル用の以下のモニタ定義は、*powersys* という名前の POWER5 または POWER6 のシステムの Alive ステータスを監視するように設定されています。 *lpar01* という名前の LPAR は、2 以上になるように設定されています。すなわち、警告 -3、マイナー -4 などです。

```
monitor oid monCurrState.53001 98 0x0 60 absolute > 2 'Lpar System status'  '' 'System'
'hmc/powersys/Total'        Alive critical
monitor oid monCurrState.53006 99 0x0 60 absolute > 2 'Lpar01 System status' ''
'System' 'hmc/powersys/lpar01/Total' Alive critical
```

注: モニタのインスタンス名は lpar:// から開始することはできません。

以下のテーブルでは、sysedge.cf ファイル用のモニタ定義例に一致するセルフ モニタ テーブルの例について説明します。

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530001	lparAimStatSys Status.1	System	lpar://System:Serial Number/Total	Alive	critical	ok
530002	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	warning	ok
530003	lparAimStatSys CPUUsage PerMil.1	CPU	lpar://System:Serial Number/Total	PercentUsed	minor	ok

mon Index	monOID	mon ObjClass	monObjInstance	mon ObjAttribute	mon Severity	mon CurrState
530004	lparAimStatSys MemoryUsage PerMil.1	Memory	lpar://System:Serial Number/Total	PercentUsed	warning	warning
530005	lparAimStatSys MemoryUsage PerMil.1	Memory	lpar://System:Serial Number/Total	PercentUsed	minor	minor
530006	lparAimStatLP Status.1.1	System	lpar://System:Serial Number/lpar01/Tota l	Alive	critical	critical
530007	lparAimStatLPCPU Usage.1.1	CPU	lpar://System:Serial Number/lpar01/Tota l	PercentUsed	warning	ok
530008	lparAimStatLPCPU Usage.1.1	CPU	lpar://System:Serial Number/lpar01/Tota l	PercentUsed	minor	ok
530009	lparAimStatLP MemoryUsage.1.1	Memory	lpar://System:Serial Number/lpar01/Tota l	PercentUsed	warning	ok
530010	lparAimStatLP MemoryUsage.1.1	Memory	lpar://System:Serial Number/lpar01/Tota l	PercentUsed	minor	ok
530011	lparAimStatLP Status.1.2	System	lpar://System:Serial Number/lpar02/Tota l	Alive	critical	critical
530012	lparAimStatLPCPU Usage.1.2	CPU	lpar://System:Serial Number/lpar02/Tota l	PercentUsed	warning	ok
530013	lparAimStatLPCPU Usage.1.2	CPU	lpar://System:Serial Number/lpar02/Tota l	PercentUsed	minor	ok
530014	lparAimStatLP Memory Usage.1.2	Memory	lpar://System:Serial Number/lpar02/Tota l	PercentUsed	warning	ok

IBM AIX コンピュータの論理パーティションの追加

プロビジョニング ウィザードを使用して、IBM AIX システム上の論理パーティションを管理できます。

IBM AIX コンピュータの論理パーティションを追加する方法

1. ［リソース］をクリックします。
2. ［エクスプローラ］ペインで［IBM PowerVM サーバ］を右クリックし、［プロビジョニング］-［LPAR のプロビジョニング］を選択します。

   プロビジョニング ウィザードが開き、［パーティションとメモリ］ページが表示されます。
3. HMC/IVM サーバおよび管理対象ステム名を選択します。パーティション名を指定し、HMC サーバを使用する場合はプロファイル名を指定します。 パーティション用の最小メモリ、希望メモリ、最大メモリを指定します。 ［次へ］をクリックします。

   ［プロセッサ］ページが表示されます。
4. プロセッサ ユニットの一部または専用のプロセッサ、および最小、希望、最大のプロセッサ ユニットを割り当てるかどうかを指定します。共有モードおよび仮想プロセッサの場合は、高度な設定を使用できます。 ［次へ］をクリックします。

   ［I/O コンポーネント］ページが表示されます。

5. パーティションに関連付ける I/O デバイスを選択し、［次へ］をクリックします。

   注: 各 I/O デバイスについて、その I/O デバイスが論理パーティションをアクティブにするために必要であるか、オプションであるかを指定できます。 I/O デバイスが必要である場合は、I/O デバイスが利用不可であるか、別の論理パーティションに使用されていると、パーティションをアクティブにすることができません。 I/O デバイスがオプションであり、パーティションがアクティブになったときに希望の I/O デバイスが利用可能な場合は、管理対象システムが I/O デバイスをパーティションに割り当てます。 オプションの I/O デバイスが利用可能でない場合は、管理対象システムが I/O デバイスをスキップします。

   ［I/O プール］ページが表示されます。

6. （オプション）新しい I/O プールを作成するには、［I/O プール］テーブルで［+］（追加）をクリックし、数値を入力して、［保存］をクリックします。

   注: パーティションに I/O デバイスを追加すると、I/O デバイスは I/O プールに属します。 このパーティションをアクティブにすると、管理対象システムは、パーティションに対して定義された I/O プールを自動的に論理パーティションに追加します。

7. ［次へ］をクリックします。

   HMC サーバが選択された場合、［仮想シリアル］ページが表示されます。

   IVM サーバが選択された場合、［仮想イーサネット］ページが表示されます。 手順 10 に進みます。

8. （オプション）パーティション用の最大仮想アダプタを指定します。 新しい仮想シリアル アダプタを作成するには、［+］（追加）をクリックし、アダプタ ID、リモート パーティション、およびリモート スロット番号を指定します。 仮想アダプタが割り当てられており、パーティション プロファイルに必要な仮想アダプタを実行するために十分なメモリが管理対象システムにあることを要求して、そうでない場合は、論理パーティションがアクティブにならないようにすることができます。

9. ［次へ］をクリックします。

   ［仮想イーサネット］ページが表示されます。

10. パーティション用の最大仮想アダプタを指定します。（オプション）新しい仮想イーサネット アダプタを追加するには、［+］（追加）をクリックし、アダプタ ID、仮想 LAN ID、アクセスする外部ネットワーク、トランク優先度、IEEE 802.1 Q 互換性、追加の仮想 LAN ID、およびイーサネット アダプタの必要性を選択します。

11. ［次へ］をクリックします。

    ［仮想ディスク］ページが表示されます。

12. パーティション用の仮想 SCSI デバイスまたは物理ファイバ チャネル ポートを指定します。（オプション）新しい仮想 SCSI アダプタを追加するには、［仮想 SCSI アダプタ］テーブル上の［+］（追加）をクリックします。

    アダプタ ID を選択し、SCSI アダプタが必要かどうかを指定して、［SCSI デバイス］テーブルでデバイス名を選択します。希望デバイスが［SCSI デバイス］リストにある場合は、［OK］をクリックし、［仮想 SCSI］パネルで［次へ］をクリックして、最後の手順までスキップします。新しい SCSI バッキング デバイスを追加するには、［SCSI デバイス］テーブル上の［+］（新規バッキング デバイス）をクリックします。

    注: 選択されたデバイスにスロット番号がある場合、それは仮想 I/O サーバ パーティションに定義された仮想 SCSI サーバ アダプタのスロット番号です。 選択されたデバイスにスロット番号がない場合は、仮想 SCSI サーバ アダプタにまだ関連付けられていません。 パーティションを作成するジョブが発生した場合、仮想 SCSI サーバ アダプタが作成され、デバイスに割り当てられます。

    注: NPIV をサポートする物理ファイバ チャネル ポートを選択すると、パーティションに対して仮想ファイバ チャネル サーバ アダプタと仮想ファイバ チャネル クライアント アダプタが作成されます。

13. ［次へ］をクリックします。

    新しいバッキング デバイスを追加する場合のみ、ストレージのプロビジョニング ウィザードが表示されます。 新しいバッキング デバイスを追加しない場合は、手順 21 に移ります。

14. プロビジョニング メソッドを選択します。 ストレージ プロビジョニングの詳細については、「管理ガイド」の「NetApp のストレージ プロビジョニング マネージャ」参照してください。

15. ［HMC サーバ］-［管理対象システム］を選択します。

16. ［仮想 I/O サーバ］を選択します。 新しい仮想 I/O サーバを追加するには、［新規］をクリックして仮想 I/O サーバを作成します。 仮想 I/O サーバのパーティション名、ユーザ名、およびパスワードを選択し、［保存］をクリックして、仮想 I/O サーバを検証し、かつ設定を追加します。
17. NetApp Data Fabric Manager、希望するストレージ サービス、およびその他の詳細オプションを選択します。
18. ［終了］をクリックして、要求を確認します。

    NetApp iSCSI ストレージが仮想 I/O サーバにアタッチされ、新しくプロビジョニングされたストレージが選択されます。

    ［新しい SCSI アダプタ］ダイアログ ボックスが表示されます。
19. このデバイスまたは別のデバイスを選択し、［OK］をクリックします。
20. ［次へ］をクリックします。

    ［NIM］ページが表示されます。［オペレーティング システムの展開］を切り替えることによって、NIM を使用して AIX をプロビジョニングするかどうかを選択できます。
21. 必要なビルド マシン、システム属性、Software Delivery 情報、およびテンプレートを指定して、［次へ］をクリックします。
22. ［サマリ］ページを確認し、［コンピュータの追加］をクリックします。

    論理パーティションが作成され、NIM プロビジョニングが開始します。

    物理ファイバ チャネル ポートが選択されており、NIM が有効な場合は、パーティションに割り当てられた WWPN がダイアログ ボックスに表示されます。 WWPN 用のストレージ LUN のゾーン設定や作成には、追加設定が必要です。 NIM プロビジョニングを続行またはキャンセルするオプションがあります。 追加設定が完了した後に続行を選択することができます。 また、設定が完了した後で別の NIM プロビジョニング操作をキャンセルおよび実行することを選択できます。

IBM PowerVM の管理

このセクションでは、［リソース］ページから実行できる IBM PowerVM の管理操作について説明します。

［リソース］ページでは、イベントを表示し LPAR に対して管理操作を実行できます。［エクスプローラ］ペインで［IBM PowerVM］グループを展開すると、以下のオブジェクトが一覧表示されます。

- HMC/IVM サーバ
- PowerVM システム
- 論理パーティション（LPAR）

リソース サマリおよびイベントの表示

CA Server Automation では、右側のペインに［サマリ］が表示されます。［サマリ］ページには、オブジェクト階層の以下のレベルのリソース プロパティが表示されます。

- PowerVM Server
- LPAR

［パフォーマンス チャート］ペインには、利用可能なメトリックおよびオプションで使用率が表示されます。 パフォーマンス チャートを適切に表示するには、フィルタ設定を使用します。

- CPU
- メモリ
- その他のメトリック

［一般情報］ペインには、以下のプロパティが含まれます。

- 名前、アイテム タイプ、タイプ（pSeries）
- CPU とメモリの数量特性
- LPAR および利用可能な処理装置の数
- シリアル番号

［概要］ペインには、以下の情報が表示されます。

- CPU 状態
- メモリ状態
- 稼働状態
- ヘルス状態
- プロパゲートされたヘルス状態
- 収集エンジンの状態

［サマリ］タブでは、オブジェクトに関連付けられた情報（メモリ合計、オペレーティング システム、CPU の数、IP アドレス、CPU とメモリの全体的な使用率、リソースに関連付けられたイベントなど）を表示できます。しきい値制限を設定するには、［使用方法］パネルの［設定］タブをクリックします。

論理パーティションの電源ステータスの制御

論理パーティションのステータスを制御するには、以下のいずれかの操作を行います。

- アクティブ化
- 再起動
- シャットダウン
- 削除

これらの操作はいずれも、1 つ以上の論理パーティションに対して同時に実行できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインでステータス処理を実行する管理対象マシンを選択します。
2. パーティションを右クリックし、［管理］を選択します。［クイックスタート］をクリックし、電源制御の関連するリンクをクリックする方法もあります。 以下の*いずれか*を選択します。

   アクティブ化

   現在電源オフまたは中断になっている、選択された論理パーティションをアクティブ化します。

   再起動

   ゲスト オペレーティング システムをシャットダウンし、再起動します。

   シャットダウン

   選択された論理パーティションをシャットダウンします。 現在電源がオンになっている論理パーティションのみ、シャットダウンすることができます。

   削除

   選択された論理パーティションを完全に削除します。 論理パーティションは、シャット ダウンされている場合のみ削除できます。

   確認ダイアログ ボックスが開きます。
3. ［OK］をクリックします。

   ステータス操作が実行され、確認のメッセージが表示されます。 インターフェースをリフレッシュすると、新しい論理パーティション ステータスが表示されます。 操作の結果を確認するイベントが表示されます。

論理パーティションのアクティブ化

論理パーティションをアクティブ化して、パーティションにリソースをコミットし、インストールされたオペレーティング システムを開始することができます。パーティションをアクティブ化できるのは、パーティションが実行されていないときのみです。

論理パーティションをアクティブ化する方法

1. ［エクスプローラ］ペイン上でパーティションを右クリックし、［管理］-［アクティブ化］を選択します。

   ［論理パーティションのアクティブ化］ダイアログ ボックスが表示されます。

2. 以下のフィールドに入力し、［OK］をクリックします。

   プロファイル

   パーティションのアクティブ化に使用するパーティション プロファイルを指定します。

   キー ロック

   キー ロック位置を指定します。キー ロックは、システムに許可される電源オン モードと電源オフ モードを設定します。 CA Server Automation は、以下の有効なキーロック モードをサポートします。

   上書きしない

   LPAR は、選択されたプロファイル内に指定されたキーロック モードを使用します。

   通常

   LPAR が通常の設定で起動されます。 日常的なタスクの実行には、ほぼ例外なく、このオプションを使用します。

   手動

   キー ロック位置を［手動］に設定する場合は、セキュリティへの影響を考慮してください。

   起動モード

起動モードを指定します。 選択されたプロファイル内に指定されたものとは異なる起動モードを使用する場合のみ、起動モードを選択し、［アクティブ化］チェック ボックスをオンにします。パーティション プロファイルをアクティブ化するときに、他の方法を指定しない限り、システムは、この起動モードを使用して、論理パーティション上でオペレーティング システムを開始します。 CA Server Automation は、以下の有効な起動モードをサポートします。

上書きしない

LPAR は、選択されたプロファイル内に指定された起動モードを使用します。

通常

LPAR が通常の設定で起動されます。 日常的なタスクの実行には、ほぼ例外なく、このオプションを使用します。

ファームウェアを開く

LPAR が起動されると、ファームウェア プロンプトが開かれます。このオプションは、デバッグ情報を追加で取得するために、サービスマンが使用します。

3. パーティションの［イベント］タブをクリックします。

   操作の結果を確認するイベントが表示されます。

論理パーティションの削除

不要になったパーティションを管理対象システムから削除できます。 論理パーティションを削除すると、すべてのハードウェア リソースはプライマリ パーティションに返されます。 電源がオフのパーティションのみを削除できます。

論理パーティションをアクティブ化する方法

1. ［エクスプローラ］ペインでパーティションを右クリックし、［管理］-［削除］を選択します。

   確認ダイアログ ボックスが開きます。

2. ［OK］をクリックします。

   要求がサブミットされたことを確認するメッセージが表示されます。

3. パーティションの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが表示されます。パーティションの電源がオフになっていないと、削除は失敗します。削除が成功した場合、インターフェースをリフレッシュすると、パーティションは［エクスプローラ］ペインに表示されなくなります。

論理パーティションの再起動

すでに実行されているパーティションを再起動できます。 パーティションを再起動すると、パーティションはシャットダウンされ、オペレーティング システムが再度開始されます。

注: 論理パーティションを再起動するには、論理パーティションが［実行中］または［ファームウェアを開く］状態である必要があります。

論理パーティションを再起動する方法

1. ［エクスプローラ］ペイン上でパーティションを右クリックし、［管理］-［再起動］を選択します。

   ［論理パーティションの再起動］ダイアログ ボックスが表示されます。

2. ［タイプ］ドロップダウン リストを使用して、以下のいずれかの再起動タイプを選択し、［OK］をクリックします。

   即時

   論理パーティションをすぐにシャットダウンします。 HMC/IVM はすべてのアクティブなジョブを即座に終了します。 アクティブなジョブ内で実行されていたプログラムでは、ジョブ クリーンアップを実行できません。 データが部分的に更新されていた場合、このオプションは望ましくない結果を引き起こすことがあります。 このオプションは、制御されたシャットダウンが成功しなかった場合のみ使用してください。

   OS のシャットダウン

   論理パーティションに対してシャットダウン コマンドを発行することにより、論理パーティションを通常どおりシャットダウンします。 この操作中に、論理パーティションは、必要なすべてのシャットダウン アクティビティを実行します。 このオプションは AIX 論理パーティションにのみ使用できます。

   OS のシャットダウン即時

   論理パーティションに対してシャットダウン -F コマンドを発行することにより、論理パーティションを即座にシャットダウンします。この操作中に、論理パーティションは、メッセージを他のユーザおよびシャットダウン アクティビティにバイパスします。 このオプションは AIX 論理パーティションにのみ使用できます。

3. パーティションの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが表示されます。

論理パーティションのシャットダウン

パーティションをシャットダウンすると、オペレーティング システムがシャットダウンされます。 パーティションをシャットダウンするには、パーティションが［実行中］または［ファームウェアを開く］状態である必要があります。

論理パーティションをシャットダウンする方法

1. ［エクスプローラ］ペイン上でパーティションを右クリックし、［管理］-［シャットダウン］を選択します。

   ［論理パーティションのシャットダウン］ページが表示されます。

2. ［タイプ］ドロップダウン リストを使用して、以下のいずれかのシャットダウン タイプを選択し、［OK］をクリックします。

   即時

   論理パーティションをすぐにシャットダウンします。 HMC/IVM はすべてのアクティブなジョブを即座に終了します。 アクティブなジョブ内で実行されていたプログラムでは、ジョブ クリーンアップを実行できません。 データが部分的に更新されていた場合、このオプションは望ましくない結果を引き起こすことがあります。 このオプションは、制御されたシャットダウンが成功しなかった場合のみ使用してください。

   OS のシャットダウン

   論理パーティションに対してシャットダウン コマンドを発行することにより、論理パーティションを通常どおりシャットダウンします。 この操作中に、論理パーティションは、必要なすべてのシャットダウン アクティビティを実行します。 このオプションは AIX 論理パーティションにのみ使用できます。

   OS のシャットダウン即時

   論理パーティションに対してシャットダウン -F コマンドを発行することにより、論理パーティションを即座にシャットダウンします。この操作中に、論理パーティションは、メッセージを他のユーザおよびシャットダウン アクティビティにバイパスします。 このオプションは AIX 論理パーティションにのみ使用できます。

3. パーティションの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが表示されます。

CPU とメモリの設定

仮想マシンに割り当てるメモリ共有を設定して、その割り当てリソースを調整することができます。 この操作が成功するためには、リソースを追加するときに、適切な量の未割り当てのメモリ共有または CPU 共有が利用可能である必要があります。 メモリ共有または CPU 共有で許可される最小または最大の値が存在する場合、リソース割り当てを変更するときは常にこの制限内にとどめる必要があります。 ［リソース］タブの［クイック スタート］リンクを使用すると、VM の CPU とメモリの割り当てを編集できます。特定の VM リソース割り当てアクションでは、作成およびスケジュール ポリシーを使用することもできます。

重要: CPU およびメモリの追加または削除などの動的 LPAR 操作の場合は、各 LPAR システムに AIX バージョン 5.2、5.3、または 6.0 以上をインストールします。 あるいは、LPAR システム上で AIX リソース制御デーモン IBM.DRM を実行します。

CPU の設定

VM の CPU 割り当てを設定する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを探して右クリックし、［設定］-［プロセッサの設定...］を選択します。

   ［プロセッサ リソース割り当ての設定］ダイアログ ボックスが表示されます。

3. 以下の調整タイプの中から *1* つ選択します。

   動的調整

   実行中の VM を更新します。

   プロファイルの更新

   アクティブなプロファイルを更新します。 プロファイルの変更を反映するには、VM を再起動する必要があります。

   動的調整およびプロファイル更新

   実行中の VM とアクティブなプロファイルの両方を更新します。

4. 対応するフィールドを編集し、［OK］をクリックします。

   確認メッセージが表示されます。

メモリの設定

VM のメモリ割り当てを設定する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを探して右クリックし、［設定］-［メモリの設定...］を選択します。

   ［メモリ リソース割り当ての設定］ダイアログ ボックスが表示されます。

3. 以下の調整タイプの中から 1 つ選択します。

   動的調整

   実行中の VM を更新します。

   プロファイルの更新

   アクティブなプロファイルを更新します。 プロファイルの変更を反映するには、VM を再起動する必要があります。

   動的調整およびプロファイル更新

   実行中の VM とアクティブなプロファイルの両方を更新します。

4. 対応するフィールドを編集し、［OK］をクリックします。

   確認メッセージが表示されます。

Microsoft Hyper-V Server

Windows Server 2008 R2 Hyper-V（ハイパーバイザベースのサーバ仮想化技術）が、Windows Server 2008 R2 の不可欠な機能として利用可能で、これにより、サーバ仮想化を実行できます。 Hyper-V Server 用 SystemEDGE AIM は、Hyper-V Server コンピュータ上で実行されます。

Hyper-V Server PMM は、接続と、すべての Hyper-V Server 操作の運用上のサポートを提供します。 PMM は、接続の管理、VM 関連の操作の実行、Hyper-V Server から取得したデータのデータベースへの入力を担当します。

Hyper-V Server 用 AIM は、以下のリソース タイプをモニタします。

Hyper-V Server

Hyper-V が実行されている物理サーバの計算機能とメモリ リソースをすべて表します。 Hyper-V AIM は、Hyper-V Server コンピュータのヘルス状態に関する情報を提供します。 たとえば、CPU とメモリ使用率に関するステータスおよびデータが提供されます。

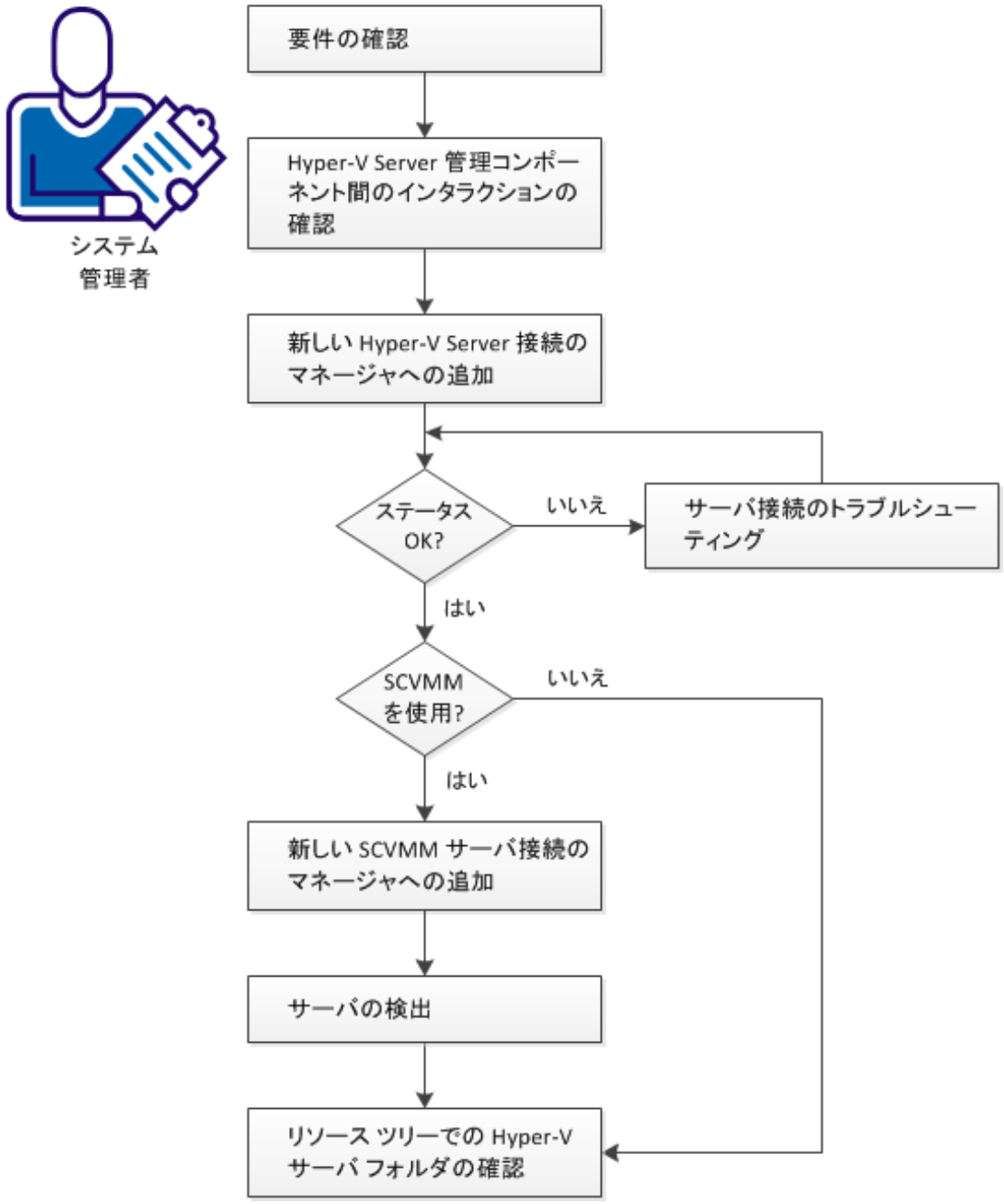
仮想マシン

ゲスト オペレーティング システムおよびアプリケーションが実行可能な仮想化された x86 環境を指定します。 仮想マシンを作成すると、特定のホスト、クラスタ、またはリソース プール、およびデータ ストアに割り当てられます。 仮想マシンは、物理デバイスがそのワークロードに応じてエネルギーを動的に使用するのと同様に、その物理ホスト上でリソースを動的に使用します。

Hyper-V 管理の設定方法

以下の図は、必要なアクションに関する概要を示しています。 図には、接続の問題のトラブルシューティング戦略が含まれます。

Hyper-V Server 管理コンポーネントを設定する方法



以下の手順に従います。

Hyper-V の要件の確認 (P. 489)
Microsoft Hyper-V を使用するために必要な設定の適用 (P. 490)
新しい Hyper-V Server 接続のマネージャへの追加 (P. 493)
（オプション）CA Server Automation マネージャへの SCVMM 管理インスタンスの追加 (P. 496)
サーバの検出 (P. 502)
リソース ツリーでの Hyper-V Server フォルダの確認 (P. 503)

Hyper-V の要件の確認

CA Server Automation の Hyper-V 管理コンポーネントの設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation、CA SystemEDGE、および Hyper-V Server に関する基礎知識がある。
- Hyper-V プラットフォーム管理モジュール（PMM）、Hyper-V Application Insight Module （AIM）、およびモニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- Hyper-V AIM が Hyper-V Server にインストールされていることを確認する。
- 管理対象となる Hyper-V Server にアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Hyper-V Server が正しく実行されることを確認済みである。
- CA Server Automation マネージャと Hyper-V Server の SNMP 設定に整合性があることを確認する。 読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用する Hyper-V Server が CA Server Automation マネージャによって検出されることを確認済みである。

関連項目:

Microsoft Hyper-V を使用するために必要な設定の適用 (P. 490)
Hyper-V Server 管理コンポーネント間のインタラクション (P. 491)
新しい Hyper-V Server 接続のマネージャへの追加 (P. 493)
（オプション）CA Server Automation マネージャへの SCVMM 管理インスタンスの追加 (P. 496)
サーバの検出 (P. 502)
リソース ツリーでの Hyper-V Server フォルダの確認 (P. 503)

Microsoft Hyper-V を使用するために必要な設定の適用

前提条件を確認し、Microsoft Hyper-V 管理用の以下の設定を適用します。

Microsoft Hyper-V を使用するために必要な設定を適用する方法

1. SystemEDGE、Advanced Encryption、および Hyper-V AIM が Hyper-V Server にインストールされていることを確認します。 各管理対象 Hyper-V Server に割り当てることのできる AIM は 1 つだけです。
2. Hyper-V Server 上でローカルのユーザ アクセス制御（UAC）を無効にします。
3. 以下のレジストリ値を設定してネットワーク UAC を無効にします。
   `HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥System¥LocalAccountTokenFilterPolicy,1 (REG_DWORD)`
4. コマンド プロンプトから以下のコマンドを実行して、リモート WMI ファイアウォール例外を有効にします。

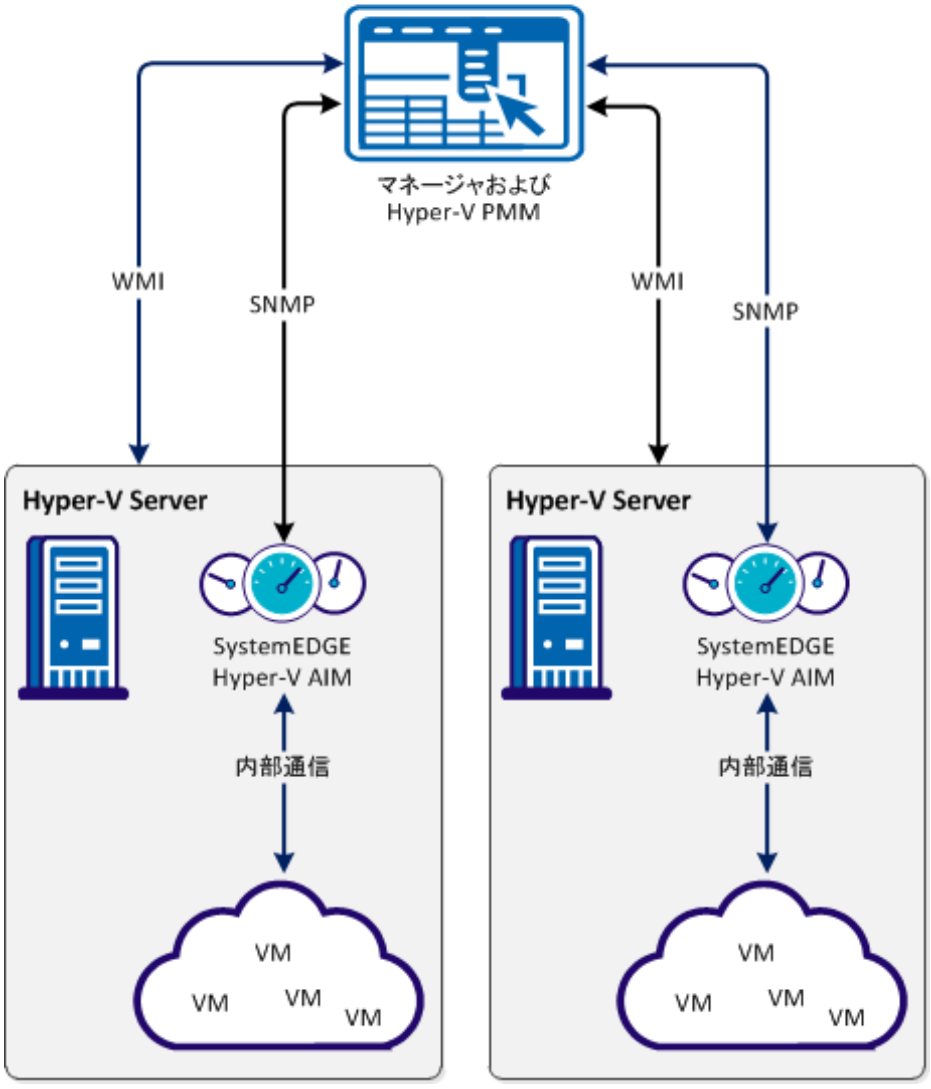
   ```
   netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes
   ```

5. サーバ アクセス用の管理コンポーネントで設定されたユーザが「Distributed COM Users」グループのメンバであることを確認します。

Hyper-V Server 管理コンポーネント間のインタラクション

以下の図は、Hyper-V 管理に関与するコンポーネントがどのように対話するかを示しています。 SystemEDGE および Hyper-V AIM は、Windows 2008（Hyper-V）サーバ上で実行され、仮想環境を管理します。 Hyper-V AIM はデータを収集し、Hyper-V Server と関連付けられた物理および仮想リソースをすべて表示します。

Hyper-V Server 管理コンポーネント間のインタラクション



接続情報を追加して、Hyper-V 管理を設定できます。 以下の*いずれか*の方法を使用します。

- ユーザ インターフェースの［管理］タブ
- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

関連項目:

新しい Hyper-V Server 接続のマネージャへの追加 (P. 493)
（オプション）CA Server Automation マネージャへの SCVMM 管理インスタンスの追加 (P. 496)
サーバの検出 (P. 502)
リソース ツリーでの Hyper-V Server フォルダの確認 (P. 503)

新しい Hyper-V Server 接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、Hyper-V 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Hyper-V Server］を選択します。

   右側のペインがリフレッシュされ、管理対象の Hyper-V Server が表示されます。

3. ［Hyper-V Server］ペイン ツールバーの（追加）をクリックします。

   ［新しい Hyper-V Server］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード）を入力し、［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上の［Hyper-V Server］ペインに Hyper-V Server が緑のステータス アイコンを使って追加されます。 CA Server Automation によって Hyper-V Server が自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によって Hyper-V Server が赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。 接続のトラブルシューティングについては、Hyper-V サーバ接続のトラブルシューティング (P. 494)を参照してください。

関連項目:

（オプション）CA Server Automation マネージャへの SCVMM 管理インスタンスの追加 (P. 496)
サーバの検出 (P. 502)
リソース ツリーでの Hyper-V Server フォルダの確認 (P. 503)
Hyper-V サーバ接続の失敗 (P. 494)

Hyper-V サーバ接続の失敗

症状:

［管理］-［設定］で新しい Hyper-V Server 接続を追加した後、Hyper-V Server への接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- Hyper-V Server の接続に使用したデータ（サーバ名、ユーザ、パスワード）が今でも有効かどうかを確認します。 必要な場合は、接続データを更新します。
- Hyper-V Server システムが実行されており、アクセス可能であるかどうかを確認します。

Hyper-V Server の接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。

   ［新しい Hyper-V Server］または［Hyper-V Server の編集］ダイアログボックスが表示されます。

2. 有効なサーバ名、ユーザ、およびパスワードを追加します。 ［管理ステータス］を有効にして［OK］をクリックします。

   接続データが更新されます。

3. 右上角の  （検証）をクリックして新しい設定を検証します。

   Hyper-V Server への接続を確立できない場合は、次の手順に進みます。

Hyper-V Server システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Hyper-V Server Name>
   ping <IP Address of Hyper-V Server>
   ```

2. Hyper-V Server に有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   Hyper-V Server が DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに Hyper-V Server を追加します。 手順 3 に進みます。

   Hyper-V Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Hyper-V Server Name>
   ```

   正しい IP アドレスと Hyper-V Server の名前を入力します。 例：

   ```
   192.168.50.50 myHyper-V
   ```

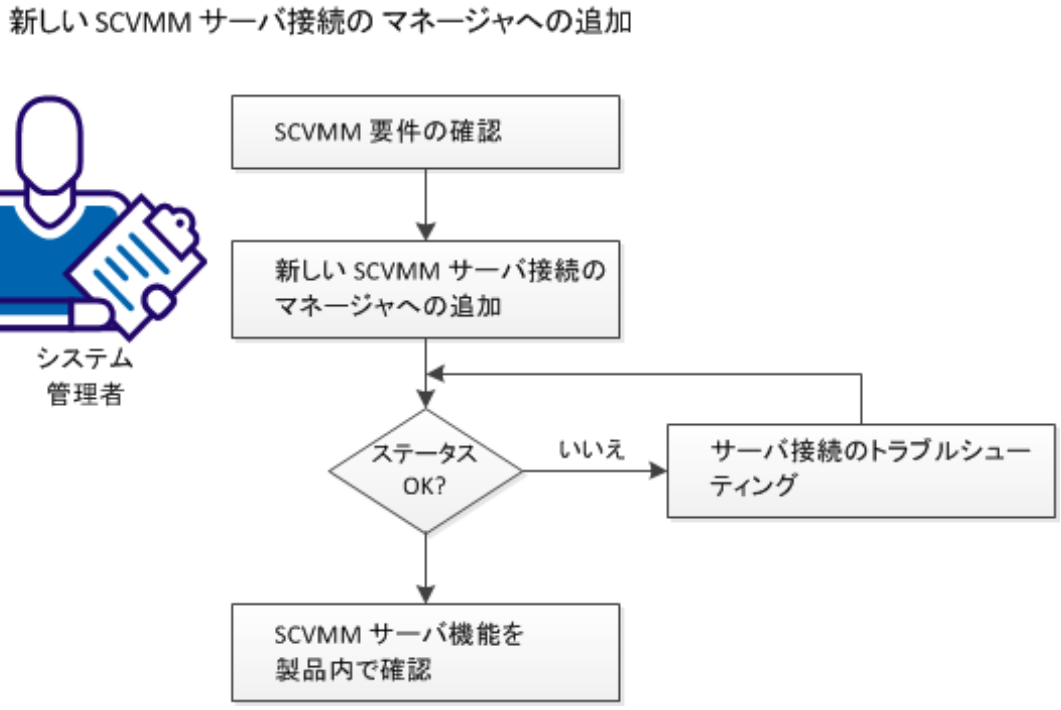
4. 右上角の  （検証）をクリックします。

   Hyper-V Server への接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

   Hyper-V の管理者または VMware のサポート担当者と協力して、Hyper-V Server の接続の問題を解決します。

（オプション）CA Server Automation マネージャへの SCVMM 管理インスタンスの追加

以下の図は、必要なアクションに関する概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。



以下の手順に従います。

Microsoft SCVMM を使用するために必要な設定の適用 (P. 497)
新しい SCVMM サーバ接続のマネージャへの追加 (P. 499)
SCVMM サーバ接続の失敗 (P. 500)

Microsoft SCVMM を使用するために必要な設定の適用

CA Server Automation はオプションで、Hyper-V のプロビジョニングのために Microsoft System Center Virtual Machine Manager （SCVMM）と統合できます。 Hyper-V のモニタリングと管理に SCVMM は必要ありません。 SCVMM の代わりに、VM プロビジョニング用のローカル テンプレート（Hyper-V Server にバインド）を使用することもできます。

オプションの SCVMM 統合を使用するときは、以下の前提条件を確認し、必要な設定を適用します。

Microsoft SCVMM を使用するために必要な設定を適用する方法

1. SCVMM サーバ、VM プロビジョニング用の Hyper-V ターゲット ホストの全候補、および Hyper-V PMM を実行している CA Server Automation マネージャが、同じ Active Directory ドメインのメンバであることを確認します。
2. CA Server Automation と SCVMM で、VM プロビジョニング用の Hyper-V ターゲット ホストが設定されていることを確認します。 CA Server Automation は SCVMM のディスカバリを行いません。
3. SCVMM で Windows Remote Management （WinRM）が設定されていることを確認します。
4. WinRM を設定するには、SCVMM サーバのコマンド ラインで以下のコマンドを実行します。

   ```
   winrm quickconfig
   ```

5. SCVMM サーバでの WinRM の基本設定に加えて、暗号化されない HTTP を許可するか、HTTPS を有効にします。

   暗号化されない HTTP トラフィックを許可するには、以下のコマンドを実行します。

   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

   HTTPS を有効にするには、SCVMM サーバ用の SSL 証明書を取得、インストールして、以下のコマンドを実行します。

   ```
   winrm quickconfig -transport:https
   ```

SCVMM サーバ上でリモート シェル用の割り当て管理のパラメータ設定が不適切であると、環境内での SCVMM サーバの予想使用率によっては、VM プロビジョニングに失敗する可能性があります。関係のあるパラメータは以下のとおりです。

MaxShellsPerUser

ユーザ当たりのシェルの最大数を指定します。

デフォルト： 5

MaxConcurrentUsers

シェルを開くことができる同時ユーザの最大数を指定します。

デフォルト： 5

一度に複数のプロビジョニング ジョブを見込んでいる場合、SCVMM サーバ上のパラメータ設定は以下のように増やすことができます。

```
winrm set winrm/config/winrs @{MaxShellsPerUser="数値"}
winrm set winrm/config/winrs @{MaxConcurrentUsers="数値"}
```

例

```
winrm set winrm/config/winrs @{MaxShellsPerUser="30"}
winrm set winrm/config/winrs @{MaxConcurrentUsers="10"}
```

Microsoft が提供している「Quota Management for Remote Shells」（英語）の記事も参照してください。

新しい SCVMM サーバ接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、SCVMM 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［SCVMM サーバ］を選択します。

   右側のペインがリフレッシュされ、管理対象の SCVMM サーバが表示されます。

3. ［SCVMM サーバ］ペイン ツールバーの（追加）をクリックします。

   ［新しい SCVMM サーバ］ ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード）を入力し、［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上の［SCVMM Server］ペインに SCVMM Server が緑のステータス アイコンを使って追加されます。 CA Server Automation によって SCVMM サーバが自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によって SCVMM サーバが赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。 接続のトラブルシューティングについては、SCVMM サーバ接続のトラブルシューティング (P. 500)を参照してください。

SCVMM サーバ接続の失敗

症状:

［管理］-［設定］で新しい SCVMM サーバ接続を追加した後、SCVMM サーバへの接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- SCVMM サーバの接続に使用したデータ（サーバ名、ユーザ、パスワード）が今でも有効かどうかを確認します。 必要な場合は、接続データを更新します。
- SCVMM サーバ システムが実行されており、アクセス可能であるかどうかを確認します。

SCVMM サーバの接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。

   ［新しい SCVMM サーバ］または［SCVMM サーバの編集］ダイアログボックスが表示されます。

2. 有効なサーバ名、ユーザ、およびパスワードを追加します。 ［管理ステータス］を有効にして［OK］をクリックします。

   接続データが更新されます。

3. 右上角の  （検証）をクリックして新しい設定を検証します。

   SCVMM サーバへの接続を確立できない場合は、次の手順に進みます。

SCVMM サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <SCVMM Server Name>
   ping <IP Address of SCVMM Server>
   ```

2. SCVMM サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   SCVMM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに SCVMM サーバを追加します。 手順 3 に進みます。

   SCVMM サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <SCVMM Server Name>
   ```

   正しい IP アドレスと SCVMM サーバの名前を入力します。 例：

   ```
   192.168.50.50 mySCVMM
   ```

4. 右上角の  （検証）をクリックします。

   SCVMM サーバへの接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

   SCVMM の管理者または Microsoft のサポート担当者と協力して、SCVMM サーバの接続の問題を解決します。

サーバの検出

CA Server Automation マネージャに新しい Hyper-V サーバ接続とオプションの SCVMM 接続を追加した後、Hyper-V Server と SCVMM サーバを検出します。その後、そのすべての仮想コンポーネントを含む Hyper-V 環境全体が CA Server Automation によって検出されます。

CA Server Automation マネージャと、Hyper-V Server および SCVMM サーバの SNMP 認証情報に整合性があることを確認します。必要な場合は、SNMP 設定をそれに応じて更新します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。［リソース］-［データ センター］をクリックします。

   ［データ センター］ページが表示されます。

2. 右側のペインにある［クイック スタート］から、［システムの検出］をクリックします。

   右側のペインがリフレッシュされ、［システムの検出］ウィザードが表示されます。

3. 必要なデータを入力し、［終了］をクリックします。

   CA Server Automation によってシステムが検出されます。

関連項目:

リソース ツリーでの Hyper-V Server フォルダの確認 (P. 503)

リソース ツリーでの Hyper-V Server フォルダの確認

新しい Hyper-v Server は、設定およびディスカバリに成功すると、［リソース］-［エクスプローラ］ペインの［Hyper-V Server］フォルダに表示されます。

次の手順に従ってください:

1. ［リソース］-［エクスプローラ］をクリックします。

   リソース ツリーが表示されます。

2. ［Hyper-V Server］を展開します。

   管理対象の Hyper-V Server が表示されます。

3. 新しい Hyper-V Server エントリを展開します。

   管理対象の Hyper-V インフラストラクチャが表示されます。

CA Server Automation で、追加された Hyper-V 環境とその仮想インフラストラクチャを管理する準備が整いました。

Hyper-V の管理

Hyper-V Server では、Hyper-V サーバおよび仮想マシンを管理できます。Hyper-V Server は、すべての仮想リソースを表示し、開始、停止、削除などの管理操作を実行できる一元的な場所です。

このセクションでは、［リソース］ページから Hyper-V Server リソースに対して実行できるリソース管理操作について説明します。［リソース］ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Hyper-V Server
- 仮想マシン

［リソース］をクリックし、［エクスプローラ］ペインを開きます。次に、いずれか 1 つの Hyper-V リソースを選択し、そのリソースの［サマリ］をクリックします。

［サマリ］ページでは、そのオブジェクトに関連付けられている情報（Hyper-V Server や、Hyper-V サーバ上の仮想マシン上の仮想マシンなど）、およびリソースに関連付けられているイベントを表示できます。

［詳細］ページでは、リソースの他の詳細情報（システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど）を見ることができます。

［エクスプローラ］ペインのメニューを右クリックすると、管理とポリシーのタスクを実行することができます。

関連項目

VM ステータスの管理（Hyper-V） (P. 507)
仮想マシンの削除 (P. 508)
仮想マシン名の変更 (P. 509)
アクションとルールの作成 (P. 509)
起動とシャットダウンのアクションの編集 (P. 510)
VM の CPU およびメモリの割り当ての編集 (P. 512)
Hyper-V 管理アクション (P. 513)

仮想マシン（Hyper-V Server）の追加

データ センターに VM を作成できます。 VM を作成するには、事前定義済みテンプレートを使用する必要があります。

注: Hyper-V の［ストレージの合計］の値には、テンプレートから VM を作成するのに必要な総容量が含まれます。 この値は、すべての仮想ディスク、VM の RAM サイズ、スナップショットおよびバッファが含まれた複数のファクタの組み合わせです。この情報を使用して、選択済みテンプレートに基づいた VM を作成するのに必要なストレージの最大容量の指針にします。

VM を作成する方法

1. ［リソース］-［エクスプローラ］ を選択します。

   ［エクスプローラ］ペインが表示されます。

2. Hyper-V リソースを右クリックし、［プロビジョニング］-［Hyper-V VM のプロビジョニング］を選択します。
3. 以下の詳細を指定して［次へ］をクリックします。
   - SCVMM サーバおよび Hyper-V サーバ。
   - VM を作成するために使用するテンプレート名。
   - VM を作成するデスティネーション パス。
   - 作成する VM の名前。
   - VM が作成された後で VM を開始するかどうかを指定します。

   ［仮想マシン メモリ］ページが表示されます。
4. VM メモリの詳細を指定し［次へ］をクリックします。

   ［ゲスト OS カスタマイズ］ページが表示されます。
5. ゲストのオペレーティング システムの詳細を指定し［次へ］をクリックします。

   ［ネットワーク管理］ページが表示されます。

6. VM のネットワークの詳細を指定し［次へ］をクリックします。

   注: カスタム仕様が DHCP の使用を指定している場合は、テーブル内のネットワーク接続セルのみを編集できます。カスタム仕様が静的 IP アドレスの使用を指定している場合は、NIC セル以外のセルをすべて編集できます。 CA Server Automation はカスタム仕様のネットワークが［ユーザに通知］を設定することをサポートしていません。この設定を使用するカスタム仕様はフィルタで除外され利用できません。

7. ［コンピュータの追加］をクリックします。

   確認メッセージがペインの一番上に表示されます。

   注: イメージングには時間がかかるため、オペレーティング システムのインストール中の遅延を予想しておく必要があります。 より効率的なディスカバリのために、検出再試行時間、または caimgconf.cfg ファイル（*install_path*¥CA¥*productname*¥conf にあります）内の間隔を調節できます。.

関連項目

マシンのプロビジョニング： Microsoft Hyper-V (P. 918)

VM ステータスの管理（Hyper-V）

以下のいずれかの VM 操作の実行により Hyper-V Server 仮想マシンのステータスを制御できます。

- 開始
- 停止
- 一時停止
- 再起動
- シャットダウン
- 保存

これらの操作は、複数の VM で同時に実行できます。

VM ステータスを制御する方法

1. ［エクスプローラ］ペインでステータス処理を実行する仮想マシンを選択します。
2. VM を右クリックし、［管理］を選択します。［クイック スタート］をクリックし、電源制御の関連するリンクをクリックする方法もあります。 以下の*いずれか*を選択します。

   開始

   仮想マシンを開始し、ゲスト オペレーティング システムを起動します。 現在電源がオフになっているか、中断されている仮想マシンのみ、電源をオンにすることができます。

   停止

   仮想マシンを電源オフします。 現在電源がオンになっているか、中断されている仮想マシンのみ、電源をオフにすることができます。

   一時停止

   仮想マシンを中断し、現在の状態を保存します。 マシンを再開するまで、すべてのアクティビティが中断されます。

   再起動

   ゲスト オペレーティング システムをシャットダウンし、再起動します。

   シャットダウン

ゲスト オペレーティング システムをシャットダウンします。現在電源がオンになっている仮想マシンのみ、シャットダウンすることができます。

保存

仮想マシンの現在のステータスを保存します。このオプションは、他のプラットフォームでの［中断］に似ています。

確認ダイアログ ボックスが開きます。

3. ［OK］をクリックします。

ステータス操作が実行され、確認のメッセージが表示されます。 インターフェースをリフレッシュして、最新の VM ステータスを表示します。 操作の結果を確認するイベントが表示されます。

仮想マシンの削除

Hyper-V Server から仮想マシンを削除すると、仮想マシンは仮想ディスクから削除されます。

仮想マシンを削除する方法

1. ［エクスプローラ］ペインを開きます。

利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［削除］を選択します。

［Hyper-V VM の削除］ダイアログ ボックスが、追加のコンポーネントを削除するオプションと共に表示されます。

3. ［OK］をクリックします。

要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

処理の結果を確認するイベントが表示されます。 成功すると、その仮想マシンが仮想ディスクから削除され、インターフェースをリフレッシュした後、［エクスプローラ］ペインに表示されなくなります。

注: 電源オフの状態にある VM のみを削除できます。その状態でないと、削除リンクは無効になります。

仮想マシン名の変更

Hyper-V Server から既存の仮想マシンの名前を変更できます。

仮想マシンの名前を変更する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［名前の変更］を選択します。

   ［VM の名前変更］ダイアログ ボックスが表示されます。

3. 新しい VM 名を入力して、［OK］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

アクションとルールの作成

仮想マシンなど、さまざまなタイプのリソースの既定のポリシーに基づいて、アクションおよびルールを作成できます。

仮想マシンのアクションおよびルールを作成する方法

1. ［リソース］-［エクスプローラ］-［データ センター］を選択します。
2. ［ポリシー］タブおよび［アクション］サブタブを開きます。
3. ［+］（追加）をクリックして、新しいアクションを作成します。
4. ドロップダウン メニューから適切な項目を選択し、ユーザ インターフェース内の手順に従ってアクションを作成します。
5. ［ルール］サブタブを選択し、［+］（追加）をクリックして新しいルールを作成します。

   ［ルール/テンプレートの特定および評価］ダイアログ ボックスが表示されます。

   ウィザードに従って、作成プロセスを進めます。利用可能なアクションのリストからアクションをこのルールに割り当てます。

   アクションとルールの詳細については、「アクションの作成 (P. 839)」および「ルールの作成」を参照してください。

起動とシャットダウンのアクションの編集

仮想マシンを起動およびシャットダウンするアクションを編集できます。

起動とシャットダウンのアクションを編集する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［設定］-［起動とシャットダウンのアクション］を選択します。

   ［起動とシャットダウンのアクション］ダイアログ ボックスが表示されます。

3. ［起動とシャットダウンのアクション］ダイアログ ボックスには以下のフィールドが含まれます。

   アクション開始

   Hyper-V Server の開始時に実行するアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

   - 常に

     Hyper-V Server の開始時に常に VM を開始します。

   - 自動

     VM が実行モードでシャットダウンした場合、Hyper-V Server が開始するときに、VM を自動的に開始します。

   - なし

     Hyper-V Server の開始時に VM を開始しません。

   開始遅延

   Hyper-V Server の開始後に VM を開始する遅延時間（数秒）を調整します。

   シャットダウン アクション

   仮想マシンのシャットダウン時に実行するアクションを指定します。ドロップダウン リストから、以下のいずれかを選択します。

   - オフ

     Hyper-V Server のシャット ダウン前に VM をオフにします。

   - 保存

Hyper-V Server のシャット ダウン前に VM を保存（中断）します。

- シャットダウン

  Hyper-V Server のシャット ダウン前に VM をシャットダウンします。

復旧アクション

Hyper-V Server で障害が発生したときに仮想マシンの以前の詳細を回復するためのアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- なし

  サーバ障害発生後の Hyper-V Server の開始時に特別なアクションを行いません。

- 再起動

  VM サーバが失敗した後に Hyper-V Server が開始するとき、VM を再起動します。

- 元に戻す

  サーバ障害発生後の Hyper-V Server の開始時に、最新のスナップショットを使って VM を元に戻します。

4. すべての詳細を編集した後、［OK］をクリックします。 確認メッセージが表示されます。

VM の CPU およびメモリの割り当ての編集

仮想マシンに割り当てられている CPU 数とメモリ共有を編集して、割り当てられているリソースを調整できます。 リソースを追加する場合、適切な量の割り当てられていないメモリと CPU 共有が利用できる必要があります。 メモリまたは CPU 共有で許可される最小値および最大値が存在する場合は、リソース割り当ての変更は、これらの制限内で行う必要があります。

特定の VM リソース割り当てアクションを使用して、ポリシーの作成およびスケジュールを行うこともできます。

VM の CPU およびメモリの割り当てを編集する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［設定］-［リソース割り当て］-［CPU およびメモリ］を選択します。

   ［CPU およびメモリ リソース割り当て］ダイアログ ボックスが表示されます。

3. CPU の数、予約済み CPU パーセンテージ、および CPU 制限のパーセンテージを調節します。

4. 仮想マシンに割り当てられているメモリ共有を調節し、すべての詳細を編集した後、［OK］をクリックします。

   確認メッセージが表示されます。

Hyper-V 管理アクション

以下のアクション タイプを Hyper-V Server で使用できます。

- マシンの削除 (P. 886)
- マシン状態の変更 (P. 851)
- 電源の設定 (P. 868)
- CPU/メモリの設定 (P. 857)

割り当てられたルール基準が満たされるときに、Hyper-V Server の起動オプションとシャットダウン オプションの設定、および他の操作を自動化する新規アクションを作成するためにこれらのアクション タイプを使用できます。 これらのアクションが特定の時刻に行われるようにスケジュールすることもできます。

自動化ポリシーを作成するアクションおよびルールの使用の詳細については、「ポリシー」の章を参照してください。

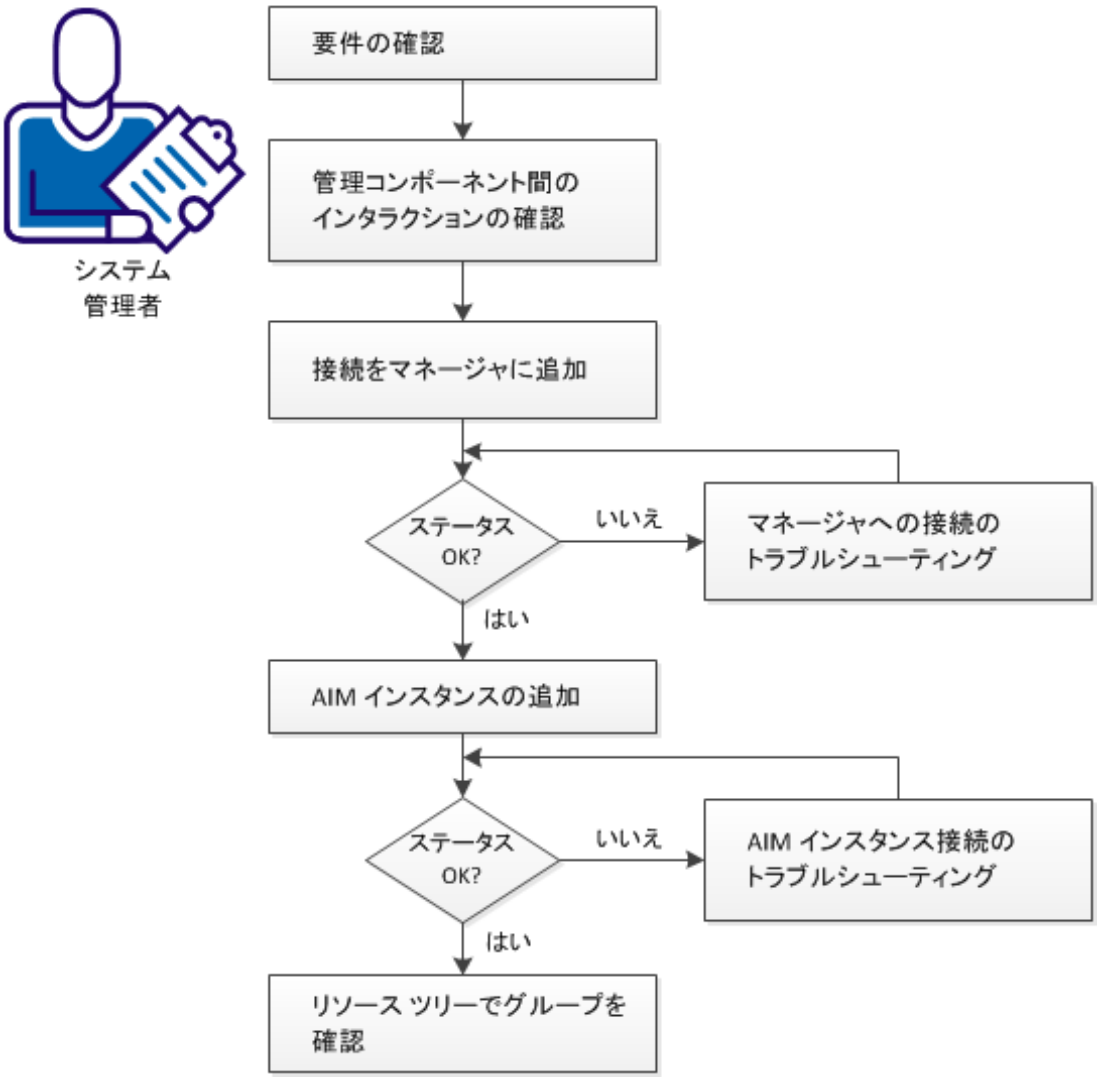
Red Hat Enterprise Virtualization

CA Server Automation では、カーネル ベースの仮想マシン サポートが導入されました。 *カーネル ベースの仮想マシン（KVM）*は Linux カーネル用のハードウェア支援型仮想化インフラストラクチャです。CA KVM AIM はマルチインスタンスのリモート AIM として実装されます。 CA KVM AIM は RHEV モニタリングを有効にします。 *Red Hat Enterprise Red Hat Enterprise Virtualization （RHEV）*は KVM ハイパーバイザに基づいたエンタープライズ仮想化製品です。

Red Hat Enterprise Virtualization 管理コンポーネントの設定方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

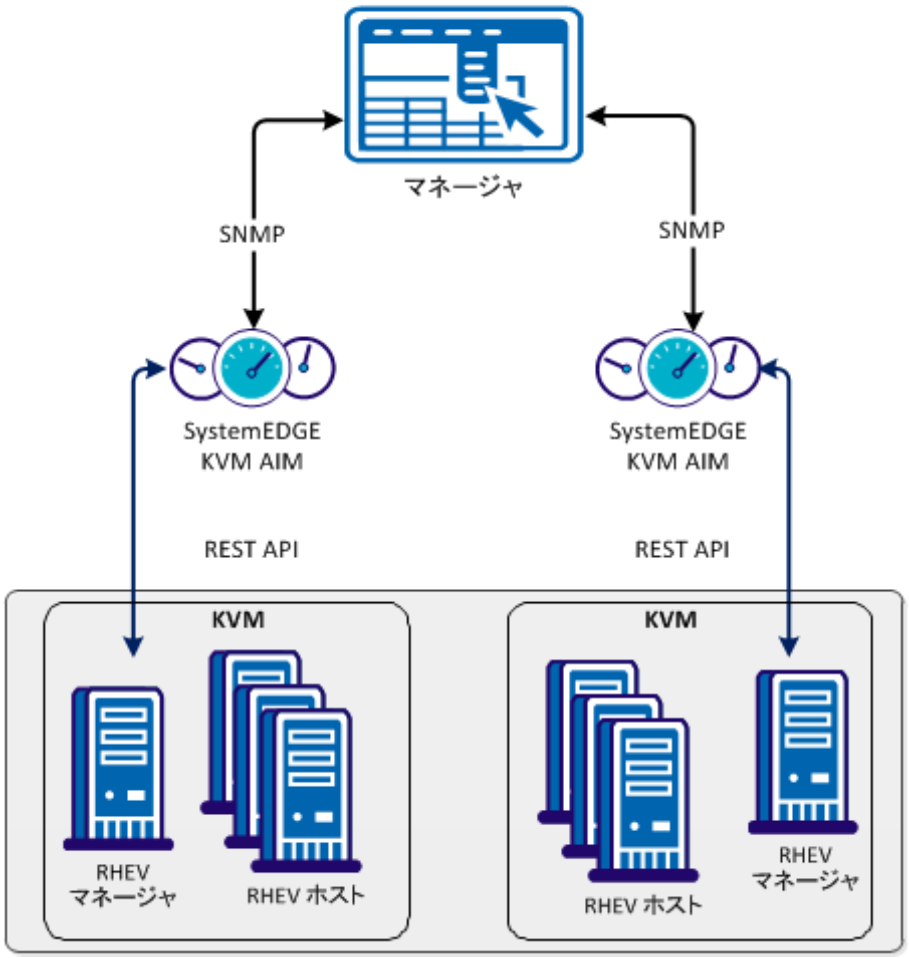
- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

RHEV 管理コンポーネント間のインタラクション

以下の図は、RHEV モニタリングに関与するコンポーネントがどのように対話するかを示しています。 SystemEDGE と KVM AIM は、同じ Windows Server 上で実行します。 AIM は REST API を使用して、1 つ以上の RHEV マネージャと通信します。

KVM 管理コンポーネント間のインタラクション



マネージャへの Red Hat Enterprise Virtualization 接続の追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、Red Hat Enterprise Virtualization 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左ペインの［プロビジョニング］セクションから Red Hat Enterprise Virtualization を選択します。

3. ［登録された Red Hat Enterprise Virtualization サーバ］ペイン ツールバー上の （追加）をクリックします。

   ［Red Hat Enterprise Virtualization サーバの追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、ISO ライブラリ認証情報、ポート）を入力し、優先の AIM を指定し、［管理ステータス］（チェック ボックス）を有効にします。

   注: ISO ライブラリには、プロビジョニング用の ISO イメージが含まれています。 ISO イメージがない場合、プロビジョニングは動作しません。

5. ［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた （追加）または （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバ システムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された Red Hat Enterprise Virtualization AIM インスタンスの追加

Red Hat Enterprise Virtualization 接続を CA Server Automation マネージャに追加した後、Red Hat Enterprise Virtualization 環境を管理するために AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左ペインの［プロビジョニング］セクションから Red Hat Enterprise Virtualization を選択します。

3. ［検出された Red Hat Enterprise Virtualization AIM インスタンス］ペイン ツールバー上の （追加）をクリックします。

   ［Red Hat Enterprise Virtualization AIM インスタンスの追加］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［RHEV AIM サーバ］を選択します。

   検出された RHEV AIM サーバのリストが表示されます。

5. ドロップダウン リストから［RHEV サーバ］を選択します。

   ［登録された Red Hat Enterprise Virtualization サーバ］ペインに一覧表示された RHEV サーバが［RHEV サーバ］ドロップダウン リストに入力されます。 管理できる RHEV サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了したら、Red Hat Enterprise Virtualization 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例 :

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの Red Hat Enterprise Virtualization グループの確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. Red Hat Enterprise Virtualization グループを展開します。

   管理対象の Red Hat Enterprise Virtualization リソースが表示されます。

これで、CA Server Automation は、設定された Red Hat Enterprise Virtualization 環境を管理できる状態になります。

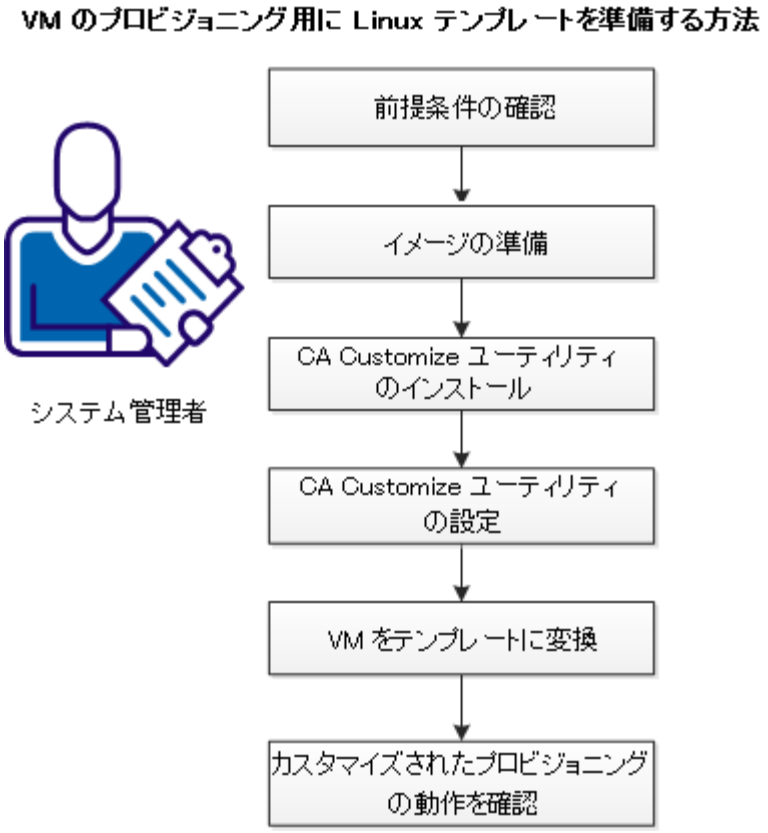
KVM のプロビジョニング用に Linux テンプレートを準備する方法

CA Server Automation は、以下のオペレーティング システムを実行する新しい仮想マシン（VM）のカスタマイズされたプロビジョニングをサポートします。

- Red Hat Enterprise Server 6.0
- SUSE Linux Enterprise Server 11

カスタマイズ オプションには、ホスト名、パスワード、ドメイン、またはネットワーク設定が含まれます。

以下の図は、システム管理者が VM のプロビジョニング用に Linux テンプレートを準備する方法を示しています。



以下の手順に従います。

カスタマイズされた VM プロビジョニングの前提条件 (P. 527)
Linux イメージの準備（KVM） (P. 527)
CA Customize ユーティリティのインストール (P. 528)
CA Customize ユーティリティの設定 (P. 529)
VM をテンプレートに変換 (P. 530)
カスタマイズされたプロビジョニングの動作 (P. 530)

カスタマイズされた VM プロビジョニングの前提条件

Linux ゲストをカスタマイズするには、ファイル システムまたはコンソールへの直接アクセスが必要です。

RHEV 環境が以下の前提条件に適合することを確認します。

- 各 RHEV データ センターが、RHEV マネージャ システム上でローカル ISO ライブラリを使用している。
- 各マシンで SFTP アクセスが有効になっている。
- RHEV マネージャで SSH アクセスが有効になっている。

Linux イメージの準備（KVM）

Linux オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従ってイメージを準備します。 一部の手順は Linux ディストリビューションによって異なる場合があります。

次の手順に従ってください:

1. Linux オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシン内で RHEV Guest Tools をインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに追加するカスタマイズを適用します。

この Linux イメージは、CA Customize ユーティリティを使用してさらにカスタマイズできます。

CA Customize ユーティリティのインストール

CA Customize ユーティリティを使用すると、CA Server Automation で仮想マシンの設定を外部から変更できます。 このゲスト ユーティリティは、OS の開始時に CD ドライブをモニタします。 特別な ISO が接続されると、以下のアクションが実行されます。

1. コマンド セットによってゲストがカスタマイズされます。
2. ゲスト システムはカスタマイズ済みとしてマークされます。
   この状態がリセットされるまで、システムはこれ以上変更できなくなります。
3. システムが停止し、カスタマイズが成功したことを示します。

ca-customize ゲスト ユーティリティを正しくインストールする方法

1. このユーティリティを以下で見つけます。
   - Red Hat Enterprise Server 6.0 の場合

     ```
     <InstallationRoot>¥Utilities¥linuxCustomization¥rh6
     ```

   - SUSE Linux Enterprise Server 11 の場合

     ```
     <InstallationRoot>¥Utilities¥linuxCustomization¥sles11
     ```

2. この実行可能ファイルを、準備する VM のハード ドライブの以下の場所に移動します。

   ```
   /usr/bin/ca-customize
   ```

3. （オプション）サポートされていない他のゲスト システムをサポートするには、ユーザ独自の ca-customize スクリプトを指定します。
4. ca-customize ユーティリティの実行可能ビットを有効にします。

   ```
   chmod 755 /usr/bin/ca-customize
   ```

CA Customize ユーティリティの設定

Linux プロビジョニング用のテンプレートをセットアップできます。 ゲストをカスタマイズするには、利用可能なスクリプトを使用します。また、ユーザ独自のスクリプトを使用して詳細なセットアップを行うこともできます。

次の手順に従ってください:

1. ネットワークがカスタマイズのプロセスに影響しないように、ネットワーク インターフェースを無効にします。

   注: ネットワークはカスタマイズ中に自動的に有効化されます。

2. 必要に応じて、*/etc/ca-customize.conf* ファイルを使用して、デフォルトの CDROM デバイス名を上書きします。

   CD_DEVICE=/dev/cdrom

   CD ドライブに使用するデバイス名を定義します。

   デフォルト： /dev/cdrom

3. ブート プロセスの最後に自動起動をセットアップします。

   - （SUSE Linux の場合）*/etc/init.d/after.local* ファイルを作成または変更します。

     ```
     #!/bin/bash
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

   - （Red Hat Linux の場合）以下の行を */etc/rc.local* ファイルに追加します。

     ```
     [ -e /etc/ca-customized ] || /usr/bin/ca-customize
     ```

4. システムをシャットダウンします。

VM をテンプレートに変換

テンプレートを使用すると、カスタマイズした仮想マシンをいくつでも作成できます。

次の手順に従ってください:

1. VM をシャットダウンします。
2. シャットダウンした仮想マシンを RHEV テンプレートに変換するには、RHEV Administration Portal を使用します。

テンプレートが CA Server Automation に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

カスタマイズされたプロビジョニングの動作

以下の手順は、カスタマイズされた VM プロビジョニングのワークフローを表します。

1. プラットフォーム管理サービスは新しい Linux VM をプロビジョニングします。
2. プラットフォーム管理サービスは、カスタマイズ パラメータを使用して新しい ISO を準備し、新しい VM に添付します。
3. プラットフォーム管理サービスは VM を開始します。
4. VM はカスタマイズ ISO が添付されていることを検出します。VM はカスタマイズ変更を適用します。
5. カスタマイズが成功すると、VM はシャットダウンします。PMM は VM の停止を検出します。 プラットフォーム管理サービスは再度 VM を開始し、プロビジョニングを完了します。
6. カスタマイズが失敗すると、VM は停止しません。 プラットフォーム管理サービスは以下のアクションを実行します。
   a. プロビジョニングの失敗を返します
   b. プロビジョニング ジョブを例外状態に設定します

カスタマイズ ログ

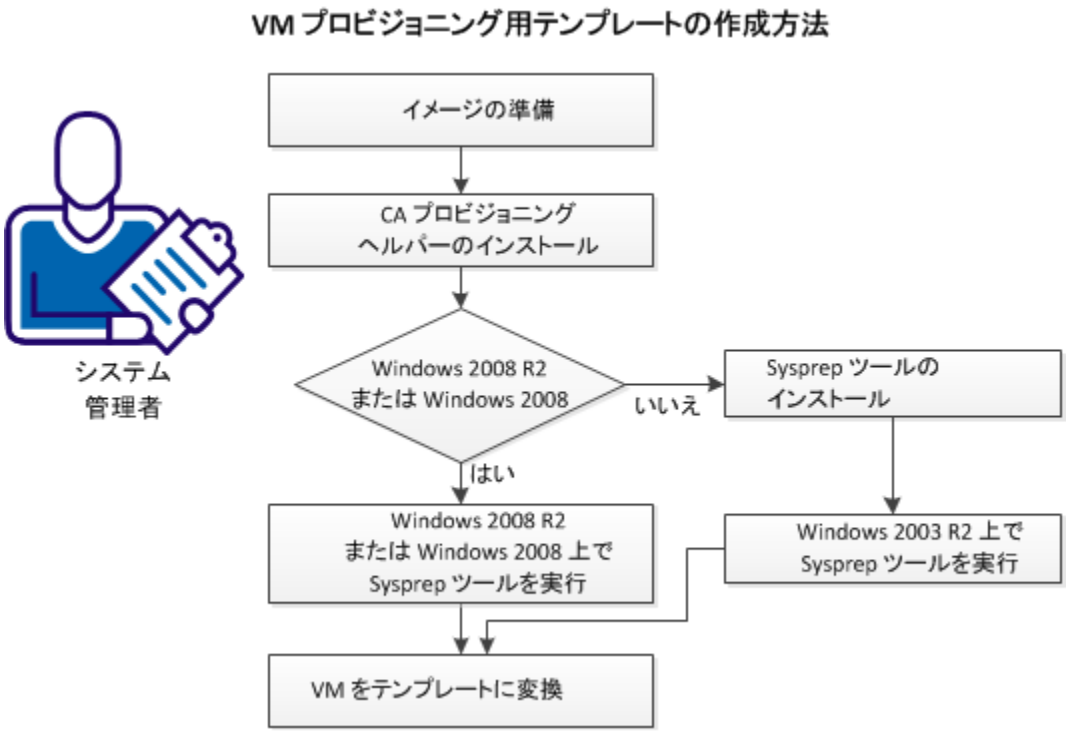
成功したカスタマイズは、*/etc/ca-customized* ファイルに格納されます。このファイルには、カスタマイズ変更のリストが含まれます。

カスタマイズに失敗すると、ログが */etc/ca-customized.tmp* ファイルに格納されます。

KVM のプロビジョニング用に Windows テンプレートを準備する方法

CA Server Automation では、Windows 2003 R2 Server（32 ビット/64 ビット）、Windows 2008 （32 ビット/64 ビット）または Windows 2008 R2 Server （64 ビット）を実行する新しい仮想マシン（VM）でのプロビジョニングのカスタマイズをサポートしています。 カスタマイズ オプションには多数の設定があります。たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

以下の図は、システム管理者が KVM のプロビジョニング用に Windows テンプレートを準備する方法を示しています。



次の手順に従ってください:

1. イメージを準備します。（P. 533）
2. CA プロビジョニング ヘルパーをインストールします。（P. 395）
3. （Windows 2003 R2 で有効） Sysprep ツールをインストールします（P. 395）。
4. 使用するオペレーティング システムに応じて、以下のアクションの*いずれか*を選択します。
   - Windows 2003 R2 で Sysprep ツールを実行する。 (P. 395)
   - Windows 2008 R2 上で Sysprep ツールを実行する。 (P. 396)
5. VM をテンプレートに変換します。（P. 535）

RHEV 環境の前提条件

RHEV 環境が以下の前提条件に適合することを確認します。

- 各 RHEV データ センターが、RHEV マネージャ システム上でローカル ISO ライブラリを使用している。
- 各マシンで SFTP アクセスが有効になっている。
- RHEV マネージャで SSH アクセスが有効になっている。

Windows イメージの準備

Windows オペレーティング システムが含まれるテンプレートを作成するときには、この手順に従って、イメージを準備します。 テンプレートをカスタマイズするには、CA Server Automation のプロビジョニング操作を有効にする手順に従ってください。 一部の手順は Windows のバージョンによって異なります。

次の手順に従ってください:

1. Windows オペレーティング システムを新しい仮想マシンにゼロからインストールします。
2. 仮想マシン内で RHEV Guest Tools をインストールします。
3. ユーザ アカウント、ポリシー、アプリケーション、ホット フィックスなど、新しい仮想マシンに適用したいカスタマイズを適用します。
4. （Windows 2003 で有効）組み込みの管理者アカウントのパスワードを空白にします。

   注: 管理者パスワードが空でないと、プロビジョニングの際に SysPrep で新しいパスワードを設定できず、既存のパスワードが残ります。

CA プロビジョニング ヘルパーのインストール

CA プロビジョニング ヘルパーは、CA Server Automation で仮想マシンの設定を外部から変更できるようにするものです。

次の手順に従ってください:

1. <InstallationRoot>¥Utilities¥Sysprep¥CAProvisioningHelper.exe でこのユーティリティを見つけます。
2. 準備する VM のハード ドライブの任意の場所に、この実行可能ファイルを移動します。
3. コマンド ラインから CA プロビジョニング ヘルパーを 1 回実行します。

Sysprep ツールのインストール

Windows インストール CD-ROM から Sysprep ツールをインストールします。

Sysprep ツール

Microsoft は、設定されている Windows インストールを一般化、フリーズ、およびシャットダウンするための Sysprep ツールを提供しています。以下のセクションでは、Windows 2003 R2 および Windows 2008 R2 用の Sysprep ツールを使用する方法の詳細について説明します。

Windows 2003 R2 での Sysprep ツールの実行

Sysprep ツールのインストールを設定した後、Sysprep ツールを実行します。

次の手順に従ってください:

1. 以下の CAB ファイルを探して開きます。

   ```
   ¥SUPPORT¥TOOLS¥DEPLOY.CAB
   ```

2. CAB ファイルに含まれるファイルをすべて選択し、%SystemDrive%¥Sysprep （通常は C:¥Sysprep）にコピーします。

   注: ディレクトリ名は変更しないでください。

3. Sysprep ディレクトリに移動して、以下を実行します。

   ```
   sysprep -quiet -reseal -mini -forceshutdown
   ```

Windows 2008 R2 での Sysprep ツールの実行

通常の Windows インストール プロセスでは、SysPrep プロセスを実行するためのすべてのファイルがインストールされます。 Windows インストールを設定した後、以下の手順を実行します。

1. Windows Server 2008 R2 用の Windows 自動インストール キット（WAIK）を使用して、有効な XML 応答ファイルを作成します。WAIK は Microsoft の Web サイトから入手できます。

   注: このプロビジョニングでは、ダミーの自動応答ファイルが必要で、これがないとシャットダウンできません。応答ファイルの内容はプロビジョニング プロセスによって置換されるため、どのようなものでもかまいません。ただし、ファイルは SysPrep に固有の XML スキーマに従う必要があります。

2. 作成された XML ファイルに「sysprep.xml」と名前を付け、これを以下の Sysprep ディレクトリに置きます。

   %SystemRoot%¥system32¥sysprep

3. 以下のコマンドを実行します。

   ```
   sysprep /generalize /oobe /shutdown /unattend:sysprep.xml
   ```

VM を RHEV のテンプレートへ変換

シャットダウンした仮想マシンを RHEV テンプレートに変換するには、RHEV Administration Portal を使用します。

テンプレートが CA Server Automation に表示され、プロビジョニングのカスタマイズに使用できるようになります。

これらの手順の実行後、新規テンプレートを使用して任意の数のカスタマイズされた仮想マシンを新しく作成することができます。

VM ステータスの管理（KVM）

仮想マシンのステータスを制御するには、以下のいずれかの操作を行います。

- 検出
  - サーバ
  - ネットワーク
- 開始
- 中断
- シャットダウン
- 破棄

VM ステータスを制御する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. VM を右クリックし、［管理］を選択して、以下のいずれかのオプションを選択します。

   検出

   サーバまたはネットワークを検出します。

   開始

   指定された RHEV ホスト上の VM を開始します。

   中断

   指定された RHEV ホストで実行されている VM を中断して、その現在の状態を保存します。VM を再開するまで、すべてのアクティビティが中断されます。

   シャットダウン

   指定された RHEV ホストで実行されている VM をシャットダウンします。

   破棄

   VM を削除します。

   対応するウィザードが表示されます。

3. 必要な情報を入力して、次の手順に進みます。

4. サブミットします。

   ステータス操作が実行され、確認のメッセージが表示されます。 インターフェースをリフレッシュして、最新の VM ステータスを表示します。 操作の結果を確認するイベントが表示されます。

RHEV 仮想マシンのプロビジョニング

以下の手順を実行することで、仮想マシンをプロビジョニングできます。VM のプロビジョニング用の Windows テンプレートを準備してください。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. Red Hat Enterprise Virtualization グループを右クリックし、［プロビジョニング］-［RHEV 仮想マシンのプロビジョニング］を選択します。

   プロビジョニング ウィザードが表示されます。

3. 必要な情報を入力します。

   VM 名

   新しい VM 名を定義します。

   テンプレート

   Windows プロビジョニング テンプレートを指定します。

   管理者パスワード

   新しい VM の管理者パスワードを定義します。

   製品のアクティベーション キー

   Windows 2003 のアクティベーション キーを定義します。

   フル ネーム

   VM のフル ネームを定義します。

4. （オプション）追加情報（ワークグループ、メモリ、CPU、VM ホスト、組織）を指定します。 静的 IP アドレスを使用する場合は、DHCP を無効にし、IP アドレス、マスク、およびデフォルト ゲートウェイを指定します。

   注: メモリと CPU の設定は、使用する Windows プロビジョニング テンプレートによって異なります。

5. サブミットします。

   確認メッセージが表示されます。

6. ［ジョブ］パネルをリフレッシュして、進捗状況を表示します。

   操作の結果を確認するイベントが表示されます。

Solaris ゾーン

Solaris ゾーンは、仮想化されたオペレーティング システムを定義します。これにより、分離された安全な環境が提供され、アプリケーションを実行できます。 この環境では、各アプリケーションおよびサービスにリソースを割り当てることができ、プロセスがほかのゾーンに影響しないようにします。 Solaris は、1 つのエンティティとして各ゾーンを管理します。 *コンテナ*は 1 つのゾーンで、オペレーティング システムのリソース管理も使用します。Solaris ゾーン PMM は、Solaris ゾーン環境のヘルス管理、管理、およびプロビジョニングを提供します。

Solaris ゾーン コンテナ リソースは、次の 3 レベルで管理できます。

Solaris ゾーン ゾーン管理

Solaris サーバは*ゾーン*を使用して、分離された環境でアプリケーションを実行します。これにより、アプリケーションが物理的に別のコンピュータ上で実行されているように見えます。 サーバ上の各ゾーンは、リソース プールからリソースを選択し、仮想ネットワーク インターフェース、ファイル システム、メモリ、および他の専用ユニットを追加します。

Solaris ゾーン プロジェクト管理

*プロジェクト*は、個別のワークロード エンティティに分割するアプリケーションまたはアプリケーションのセットです。 ゾーンは、ワークロードと設定に従って、ゾーン内の他のリソースまたはプロジェクトとは別に、プロジェクトにリソースを割り当てます。

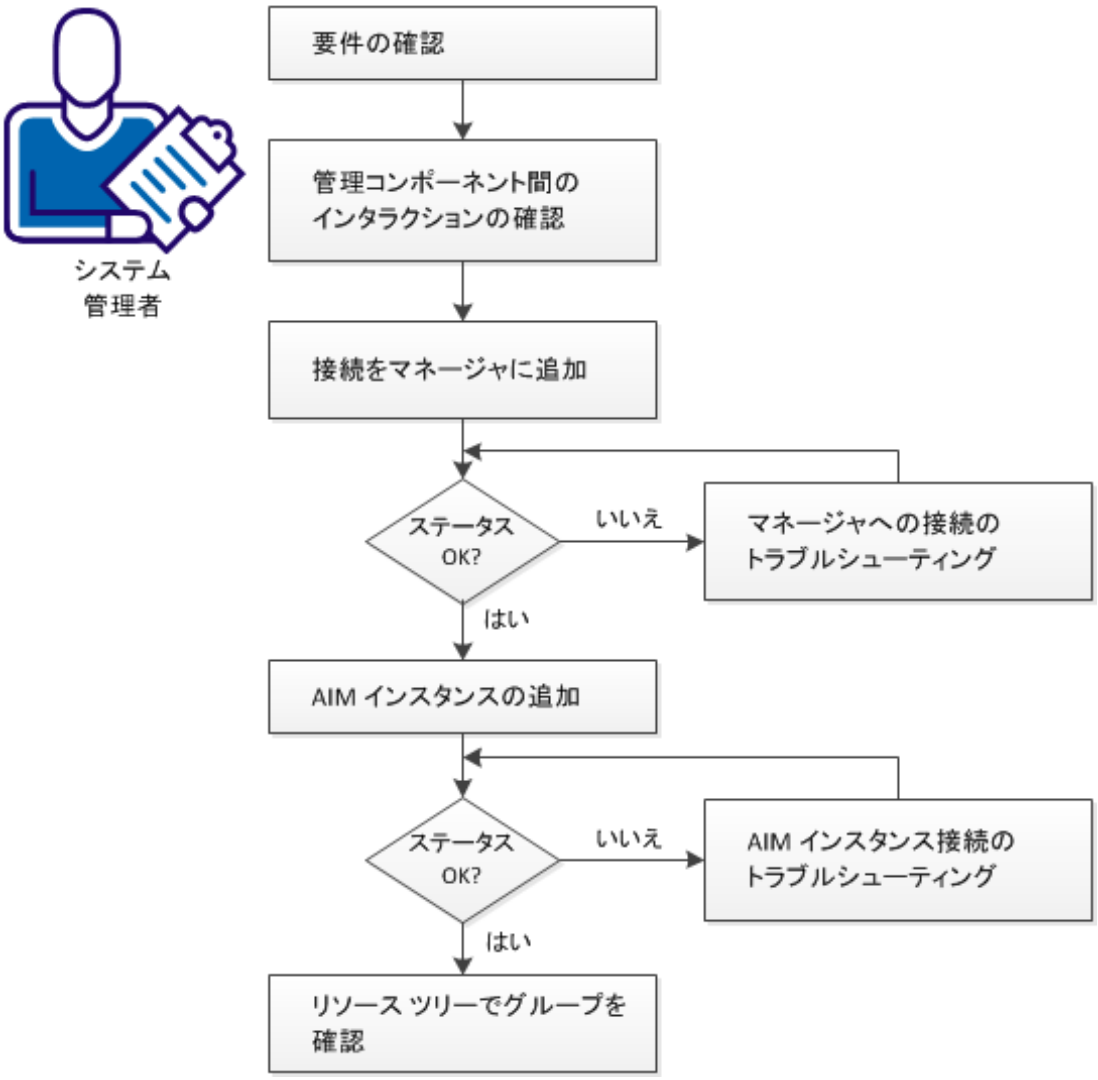
Solaris ゾーン リソース プール管理

*リソース プール*は、プロセッサ セット設定用の永続的な設定メカニズム、およびクラス割り当てのスケジューリングを提供します。 リソース プールは、ゾーン内のプロジェクトおよびタスクに、それらの設定に従って動的にリソースを割り当てることができます。

Solaris ゾーン管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



Solaris ゾーン PMM は、Solaris ゾーン環境のヘルス管理、管理、およびプロビジョニングを提供します。

以下の手順に従います。

要件の確認 (P. 541)
Solaris ゾーン管理コンポーネント間のインタラクション (P. 544)
マネージャへの Solaris ゾーン接続の追加 (P. 545)
サーバへのマネージャの接続が失敗する (P. 546)
ゾーン AIM サーバの追加 (P. 549)
AIM インスタンス接続のトラブルシューティング (P. 550)
リソース ツリーでの Solaris ゾーン グループの確認 (P. 553)

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

関連項目:

Solaris ゾーン管理の要件 (P. 543)

Solaris ゾーン管理の要件

Solaris ゾーンの管理のために CA Server Automation に必要なユーザ アカウントが、Solaris サーバ上の以下の設定と許可に適合するかどうかを確認します。

- Solaris サーバでのユーザのプロンプトは「#」（デフォルト）である必要があります。
- Solaris ユーザには、以下のコマンドを実行する権限が必要です。
  - zlogin
  - zoneadm
  - zonecfg
- ユーザには、グローバル ゾーンから zlogin で個別の Solaris ゾーンにログインし、以下のコマンドを実行する権限が必要です。
  - uname -a
  - sar
  - prstat
  - netstat

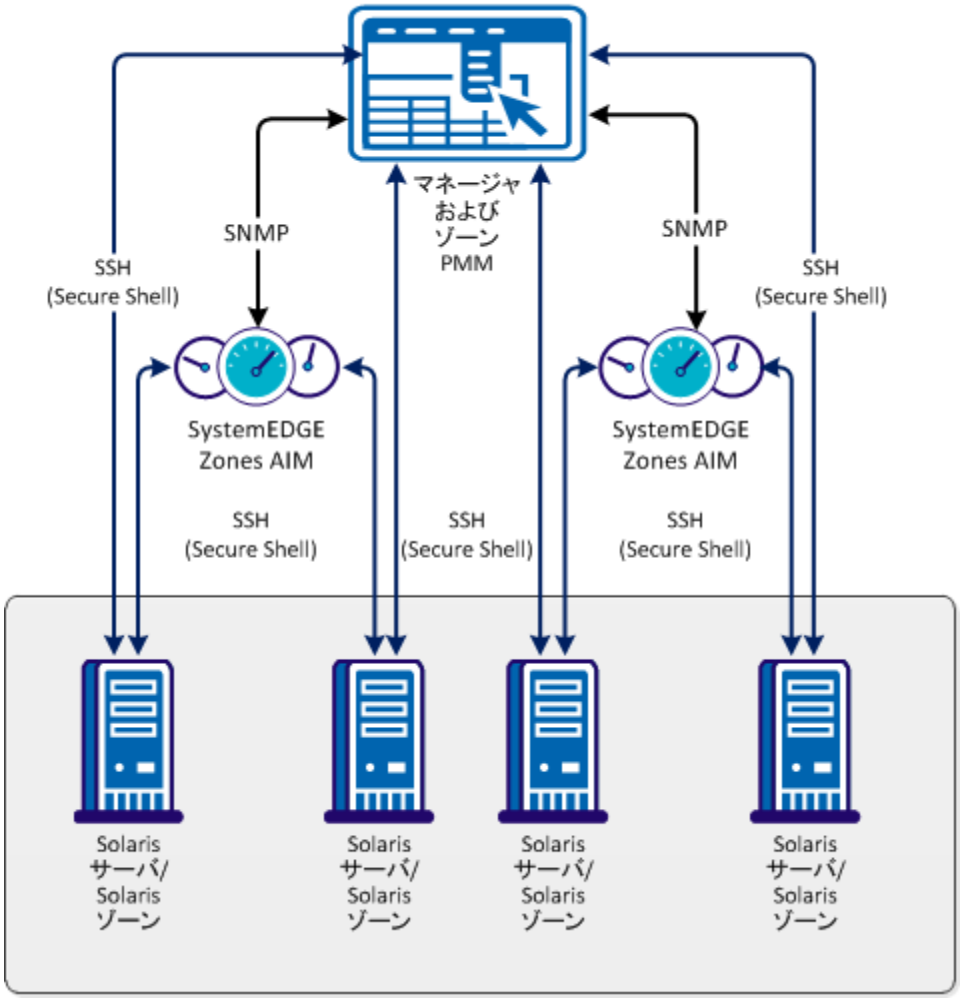
Solaris ゾーン AIM が存在する管理対象ノード上で、ユーザ インターフェースまたは NodeCfgUtil.exe ユーティリティを使用して、設定時に CA Server Automation に対するこのユーザ名および対応するパスワードを追加します。

［エクスプローラ］-［管理］-［リソース プールの作成］からリソース プールを作成して、Solaris ゾーン サーバ上のゾーン、プロジェクト、およびアプリケーションにリソースを割り当てます。 ゾーンにはゾーン作成中にリソースを割り当てます。

Solaris ゾーン管理コンポーネント間のインタラクション

以下の図に、Solaris ゾーン管理に関与するコンポーネントがどのように相互作用するのかを示します。管理対象ノードは、SystemEDGE および Solaris ゾーン AIM が実行される Windows サーバです。 AIM と Solaris ゾーン サーバの間の通信は SSH （Secure Shell）に基づいています。

Solaris ゾーン管理コンポーネント間のインタラクション



各 Solaris ゾーン サーバに必要な接続情報を追加するには、ユーザ インターフェースの［管理］タブまたは管理対象ノードで NodeCfgUtil.exe ユーティリティを使用します。 接続情報は管理対象ノード上の設定ファイルに書き込まれます。 AIM は設定ファイルをポーリングし、ユーザの Solaris ゾーン環境をモニタし始めます。

マネージャへの Solaris ゾーン接続の追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、Solaris ゾーン接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Solaris ゾーン］を選択します。

3. ［Solaris ゾーン サーバ］ペイン ツールバーの  （追加）をクリックします。

   ［Solaris ゾーン サーバ］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、ポート）を入力し、優先 AIM を指定して、［管理ステータス］（チェック ボックス）をオンにします。

5. ［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

   注: 接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。 ［はい］をクリックすると、CA Server Automation によってサーバが赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた （追加）または （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバ システムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

ゾーン AIM サーバの追加

CA Server Automation マネージャに Solaris ゾーン接続を追加した後、Solaris ゾーン環境を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Solaris ゾーン］を選択します。

3. ［ゾーン AIM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［新しいゾーン AIM サーバ］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［AIM サーバ］を選択します。

   ［ゾーン サーバ］ペインに一覧表示されたゾーン サーバが［インスタンス］ドロップダウン リストに入力されます。管理できるゾーン サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

5. ドロップダウン リストから［インスタンス］を選択し、［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。

   これで、AIM サーバ上の AIM は指定されたゾーン サーバからデータを収集するように設定されました。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。 ディスカバリ プロセスが完了したら、Solaris ゾーン環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの Solaris ゾーン グループの確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. Solaris ゾーン グループを展開します。

   管理対象の Solaris ゾーン リソースが表示されます。

CA Server Automation で、設定された Solaris ゾーン環境を管理する準備が整いました。

Solaris ゾーン管理

Solaris ゾーン サーバは、ゾーンによって隔離された環境でアプリケーションを実行することで、各アプリケーションが物理的に別々のコンピュータ上で実行されているように見せることができます。 サーバ上の各ゾーンは、リソース プールからリソースを選択し、仮想ネットワーク インターフェース、ファイル システム、メモリ、および他の専用ユニットを追加します。

このセクションでは、Solaris ゾーンのリソースに対して［リソース］ページから実行できる管理操作について説明します。 ［リソース］ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Solaris ゾーン サーバ
- Solaris ゾーン

［リソース］をクリックし、［エクスプローラ］ペインを開きます。次に、いずれか 1 つのリソースを選択し、そのリソースの［サマリ］をクリックします。［サマリ］ページでは、リソースに関連付けられている情報（Solaris ゾーン サーバ上のゾーン、リソース プール、ディスクや、ゾーン上のネットワーク インターフェースとプロジェクトなど）、またはリソースに関連付けられているイベントを見ることができます。

注: ［使用方法］パネルの［設定］ボタンを使ってアラートを［正常］として選択すると、CPU またはメモリが重大または警告の状態になった場合でも、ゾーンは正常状態（緑色）で表示されます。 同様に、アラートを［警告］として選択すると、ゾーンは常に警告状態で表示されます。

コンポーネント ツリーには、ゾーンによって使用されるリソース プールだけが表示されます。 非アクティブなリソース プールは、このパネルに一覧表示されません。

［詳細］ページでは、リソースの他の詳細情報（システム プロパティ、ソフトウェア、ハードウェア、パフォーマンスなど）を見ることができます。

リソース管理タスクを実行するための、他のページが表示される場合もあります。 ［エクスプローラ］ペインのメニューを右クリックすると、管理とポリシーのタスクを実行することもできます。

関連項目

リソース プールの作成 (P. 558)
ゾーン ステータスの制御 (P. 559)
ゾーンのクローン作成 (P. 561)
ゾーンの削除 (P. 562)
利用可能な Solaris ゾーン アクション (P. 562)

Solaris ゾーンの追加

Solaris ゾーン サーバは、ゾーンを使用してアプリケーションを独立した環境で実行し、それらが物理的に別のシステムで実行されているように表示します。サーバ上の各ゾーンは、リソース プールからリソースを選択し、仮想ネットワーク インターフェース、ファイル システム、メモリ、および他の専用ユニットを追加します。 ゾーンを作成する場合は、この情報をすべて指定する必要があります。 作成したゾーンは自動的にインストールされます。

Solaris ゾーンを追加する方法

1. ［リソース］タブを選択し、［エクスプローラ］ペインの［ゾーン ホスト］を右クリックして、［プロビジョニング］-［ゾーンのプロビジョニング］を選択します。

   ［Solaris ゾーン プロビジョニング］ウィザードが表示されます。

2. ［ゾーン ID およびタイプ］ページで以下のフィールドに入力し［次へ］をクリックします。

   ホスト

   ゾーンを作成するホストを定義します。

   名前

   ゾーンの名前を定義します。

   説明

   （オプション）ゾーンの説明を定義します。

   タイプ

   ゾーンが［ネイティブ］、［ルート全体］、［ブランド化］のどれであるかを定義します。 ブランド化ゾーンは既存のゾーン テンプレートに基づきます。

テンプレート名

（オプション）［タイプ］を［ブランド化］に設定した場合、ゾーンの作成元となるテンプレートを定義します。

インストール アーカイブ パス

ゾーン上のインストール アーカイブのディレクトリ パスを定義します。 このフィールドは、［タイプ］を［ブランド化］に設定した場合にのみ必要になります。

［CPU、メモリ、その他］ページが表示されます。

3. 以下のフィールドに入力し、［終了］をクリックします。

タイプ

スケジューラ タイプを定義します。 タスクに割り当てられた CPU 共有の数に基づいて CPU 割り当てを制御するためにフェア シェア スケジューリング クラスを使用するには、［FSS］を選択します。

容量

ゾーンに割り当てる物理メモリ容量をメガバイト単位で定義します。

スワップ メモリ

ゾーンに割り当てるスワップ メモリの量をメガバイト単位で定義します。 スワップ メモリは 50 MB 以上である必要があります。

ロック メモリ

ゾーンに割り当てるロック メモリの量をメガバイト単位で定義します。 ロック メモリ量は物理メモリ量より少なくなければいけません。

ゾーン パス

ゾーンのルート ディレクトリ パスを定義します。

NIC タイプ

（オプション）NIC タイプを定義します。 ドロップダウン リストからタイプを選択します。 NIC を選択しないと、ゾーンには NIC カードまたは IP アドレスが割り当てられません。

IP アドレス

（オプション）ゾーンの IP アドレスを定義します。

リソース プール

ゾーンと共に使用するリソース プールを定義します。 ドロップダウン リストからプールを選択します。 ゾーンと共に新しいリソース プールを使用したい場合は、プールを先に作成します。 プールを選択しない場合、デフォルトが使用されます。

自動再起動

グローバル ゾーンが再起動されるとき、ゾーンを自動的に再起動するかどうかを定義します。

リソース プールの作成

Solaris ゾーン サーバ上のゾーン、プロジェクト、およびアプリケーションにリソースを割り当てるときに使用するリソース プールは作成することができます。 作成したリソース プールは、ゾーン作成中にゾーンに割り当てることができます。

リソース プールを作成する方法

1. ［エクスプローラ］ペインで Solaris ゾーン サーバを右クリックし、［管理］、［リソース プールの作成］を選択します。

   ［リソース プールの作成］ダイアログ ボックスが表示されます。

2. 以下のフィールドに入力し、［OK］をクリックします。

   名前

   リソース プールの名前を指定します。

   最小 CPU 共有

   プールにとって常に必要な CPU 共有の最小数を指定します。

   最大 CPU 共有

   プールで利用できる CPU 共有の最大数を指定します。

   プロセッサ設定名

   プールのプロセッサ設定名を指定します。

   スケジューラ タイプ

   リソースの割り当て時に使用するスケジューリングのタイプを指定します。 作業負荷の重要度（プロジェクトまたはタスクについて指定された CPU 共有の数）に基づいてリソースを割り当てるためにフェア シェア スケジューリングを使用するには、［FSS - フェア シェア スケジュール］を選択します。

   プールが作成され、確認のメッセージが表示されます。

3. プールを作成したゾーン サーバの［サマリ］タブをクリックし、［表示］ドロップダウン リストから［リソース プール］を選択して、プールが作成されたことを確認します。

ゾーン ステータスの制御

ゾーンのステータスを制御するために、停止、再起動、開始、およびアンインストールの操作を実行することができます。これらの操作を、グローバル ゾーンまたはインストールされた状態のゾーンに対して実行することはできません。

ゾーン ステータスを制御する方法

1. ［エクスプローラ］ペインでゾーンを右クリックし、［管理］および以下のいずれかのオプションを選択します。

   開始

   ゾーンを開始し、実行状態に置きます。 インストールされた状態のゾーンのみ開始できます。

   停止

   インストールされた状態にリセットすることで、ゾーンを停止します。 ゾーンを停止すると、すべてのプロセスが停止し、ネットワーク インターフェースが削除されます。また、ゾーンの既存のアプリケーション環境と仮想プラットフォームを削除するための他の操作が実行されます。 ゾーンを停止した後は、同じゾーンを開始して環境を再初期化する必要があります。 現在実行されているゾーンのみ停止できます。

   再起動

   ゾーンを停止し、再起動します。 現在実行されているゾーンのみ再起動できます。 ゾーンを再起動すると、サーバによって新しいゾーン ID が割り当てられます。

   削除

   ゾーンを削除します。 詳細については、「ゾーンの削除」を参照してください。

   インストール

   ネイティブまたはブランド化のゾーンをインストールします。インストールが完了すると、ゾーンは設定された状態に入ります。ゾーンをインストールするときは、ブランド化ゾーンのアーカイブ パスを求めるダイアログ ボックスが開きます。ネイティブ ゾーンをインストールする場合は、このフィールドを空のままにします。ブランド化ゾーンの場合には、アーカイブ パスを入力します。

注: アーカイブ パス パラメータを入力しないでブランド化ゾーンをインストールしようとしたり、アーカイブ パス パラメータを入力してネイティブ ゾーンをインストールしようとしたりすると、エラー メッセージが表示されます。

アンインストール

ゾーンのルート ファイル システム下にあるファイルをすべてアンインストールします。 現在実行されていない（インストールされた状態）ゾーンのみアンインストールできます。 ゾーンを削除するには、事前にゾーンをアンインストールする必要があります。

クローン

ゾーンのクローンを作成します。 詳細については、「ゾーンのクローン作成」を参照してください。

確認ダイアログ ボックスが開きます。

2. ［OK］をクリックします。

   要求がサブミットされたことを確認するメッセージが表示されます。

3. ゾーン ホストの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが表示されます。

注: 現在の操作が進行中で、まだ完了していない場合、ゾーン ステータスは未完了と表示されます。

関連項目

ゾーンの削除 (P. 562)
ゾーンのクローン作成 (P. 561)

ゾーンのクローン作成

ゾーンのクローン作成では、既存のゾーンからデータをコピーすることで、新しいゾーンを設定およびインストールできます。 クローン作成の対象となるゾーンは、クローン操作を行えるように停止する必要があります。この操作を、グローバル ゾーンや、設定された状態または実行中の状態にあるゾーンに対して実行することはできません。

ゾーンのクローンを作成する方法

1. ［エクスプローラ］ペインでゾーンを右クリックし、［管理］-［クローン］を選択します。

   ［クローン作成］ペインが表示されます。

2. ［ターゲット］ペインの以下のフィールドに入力し、［クローン］をクリックします。

   名前

   クローン作成される情報のコピー先となるゾーンの名前を指定します。

   パス

   クローン作成される情報のコピー先となるゾーンのファイル パスを指定します。

   確認メッセージが表示されます。

3. ゾーン ホストの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが、ダッシュボードに表示されます。操作が完了すると、クローン作成されたゾーンは、その親ホストの［エクスプローラ］ペインに表示されます。

ゾーンの削除

グローバル ゾーン以外のゾーンは Solaris ゾーン サーバから削除できます。ゾーンを削除するには、事前にゾーンをシャット ダウンする必要があります。

インストールされた状態のゾーンに対して削除操作を実行すると、ゾーンは最初にアンインストールされてから削除されます。他の状態にある（実行中など）ゾーンに対して削除操作を実行すると、エラー メッセージが表示されます。

ゾーンを削除する方法

1. ［エクスプローラ］ペインでゾーンを右クリックし、［管理］、［削除］を選択します。

   確認ダイアログ ボックスが開きます。

2. ［OK］をクリックします。

   削除を確認するメッセージが表示されます。

3. ゾーン ホストの［サマリ］タブをクリックします。

   操作の結果を確認するイベントが表示されます。 操作が完了すると、削除したゾーンは[エクスプローラ]ペインに表示されなくなります。

利用可能な Solaris ゾーン アクション

Solaris ゾーンで利用できるアクション タイプを以下に示します。

- ゾーン マシンのクローン作成 (P. 853)
- ゾーン マシンの削除 (P. 888)
- ゾーン マシンのプロビジョニング (P. 922)

このようなアクション タイプを使用して、割り当てたルール条件が満たされたときにゾーン操作を自動化する新しいアクションを作成できます。また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

アクションとルールを使って自動化ポリシーを作成する方法の詳細については、「ポリシー」の章を参照してください。

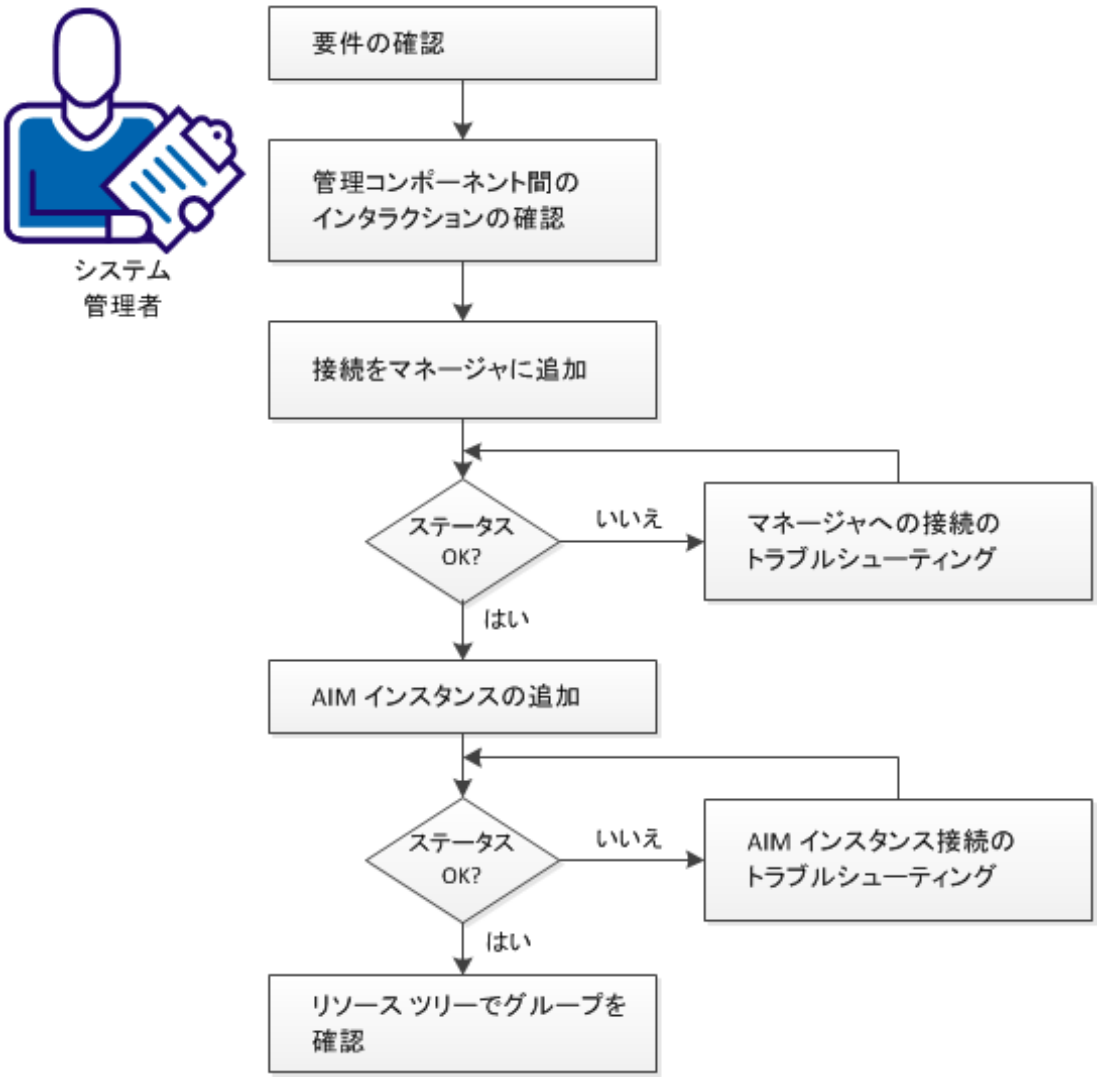
VCE Vblock Unified Infrastructure Manager サービス

CA Server Automation は、VCE Vblock Unified Infrastructure Manager サービスをサポートします。 Vblock システムは、管理、仮想化、計算、ネットワーク、およびストレージのコンポーネントで構成されるサービスをプロビジョニングするためのインフラストラクチャを提供します。

VCE Vblock 管理コンポーネントの設定方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



以下の手順に従います。

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティングシステムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。

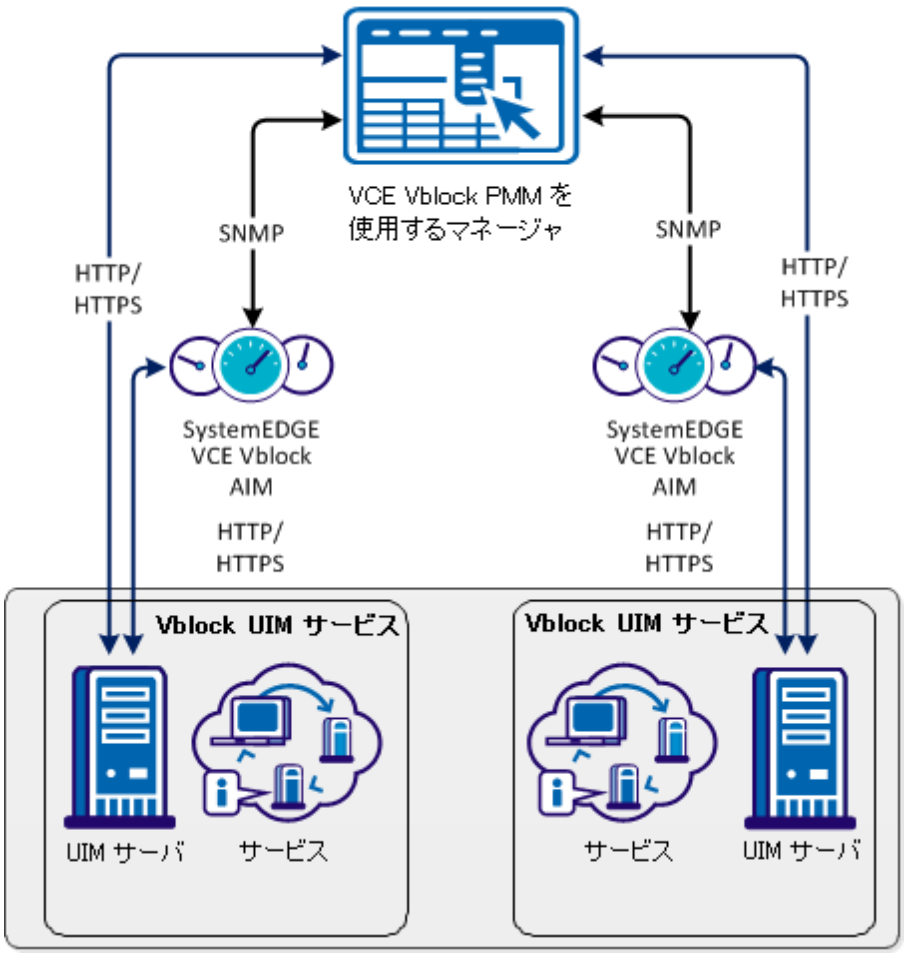
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

VCE Vblock 管理コンポーネント間のインタラクション

VCE Vblock AIM はマルチインスタンスのリモート AIM として実装されます。 AIM は、複数のスタンドアロン VCE Vblock UIM サーバとそのサービスリソースをリモートでモニタできます。 Citrix XenServer AIM は x86 および x64 モジュールとして実装されます。

VCE Vblock 用の管理 API は、Web サービスに基づいています。

VCE Vblock 管理コンポーネント間のインタラクション



マネージャへの VCE Vblock 接続の追加

ユーザ インターフェースの［管理］タブを使用して、VCE Vblock Unified Infrastructure Manager （UIM）サーバ接続を CA Server Automation マネージャに追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから、［VCE Vblock］を選択します。

3. ［UIM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［UIM サーバの追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ名、パスワード、ポート、およびプロトコル）を入力し、優先 AIM を指定して、［管理ステータス］（チェック ボックス）を有効にします。

5. ［OK］をクリックします。

   ネットワーク接続が正常に確立されると、右上のペインにサーバが追加され、緑のステータス アイコンが表示されます。 CA Server Automation によって VCE Vblock システムが自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

マネージャへのサーバ接続の失敗（VCE Vblock）

症状:

［管理］ -［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバ接続に使用したデータが有効かどうかを確認します。 必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスがサーバ システム上で正しく実行されているかどうかを確認します。

サーバの接続データを更新する方法

1. 失敗した接続に関連付けられた （追加）または （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルにサーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバの名前を入力します。 例：

   ```
   192.168.50.50 myServer
   ```

4. 右上角の  （検証）をクリックします。

   サーバの認証情報と接続データが正しく設定されており、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。 このような場合は、サーバに問題がある可能性があります。 サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システム上で管理サービスが正常に動作しているかどうかを確認する方法

1. VCE Vblock UIM サーバにアクセスするために、システム管理者に問い合わせます。
2. UIM サーバにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された VCE Vblock AIM インスタンスの追加

CA Server Automation マネージャに VCE Vblock UIM サーバ接続を追加した後に、UIM サーバを管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左側のペインの［プロビジョニング］セクションから、［VCE Vblock］を選択します。

3. ［UIM AIM サーバ］ペイン ツールバーの (追加) をクリックします。

   ［UIM AIM サーバの追加］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［UIM AIM サーバ］を選択します。

   検出された UIM AIM サーバのリストが表示されます。 UIM AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウン リストから、対応する UIM サーバを選択します。

   CA Server Automation は、［UIM サーバ］ペインにリスト表示された UIM サーバを、［UIM サーバ］ドロップダウン リストに追加します。管理できる UIM サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了したら、VCE Vblock 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

- ディスカバリが進行中
- ポーリングなし
- エラー
- 警告
- 無効
- 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの VCE Vblock の確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. ［VCE Vblock UIM サービス］グループを展開します。

   利用可能なサービス リソースが表示されます。

CA Server Automation で、検出された VCE Vblock 環境を管理する準備が整いました。 リソースのステータスとプロパティをモニタできます。

VMware vCloud

VMware vCloud Director では、仮想インフラストラクチャ リソースを仮想データ センターへプールして、ユーザにそれらを公開することにより、安全なマルチテナント クラウドを構築できます。 CA Server Automation では VMware vCloud Director の管理をサポートしています。
vCloud Director のリソースは、仮想マシンを実行するための CPU、メモリ、ストレージ、vNetwork 分散スイッチなどの vSphere リソースの基盤によって異なります。 これらの基盤となる vSphere リソースを使用して、vCloud で仮想マシンと vApp を作成できます。

*vCloud 組織*は、ユーザ、グループ、および計算リソースのコレクションを表す管理の 1 単位です。対応する仮想データセンターは必要な計算リソースを提供します。ユーザは組織レベルでの認証後、仮想マシンまたは vApp を作成、使用、管理できます。

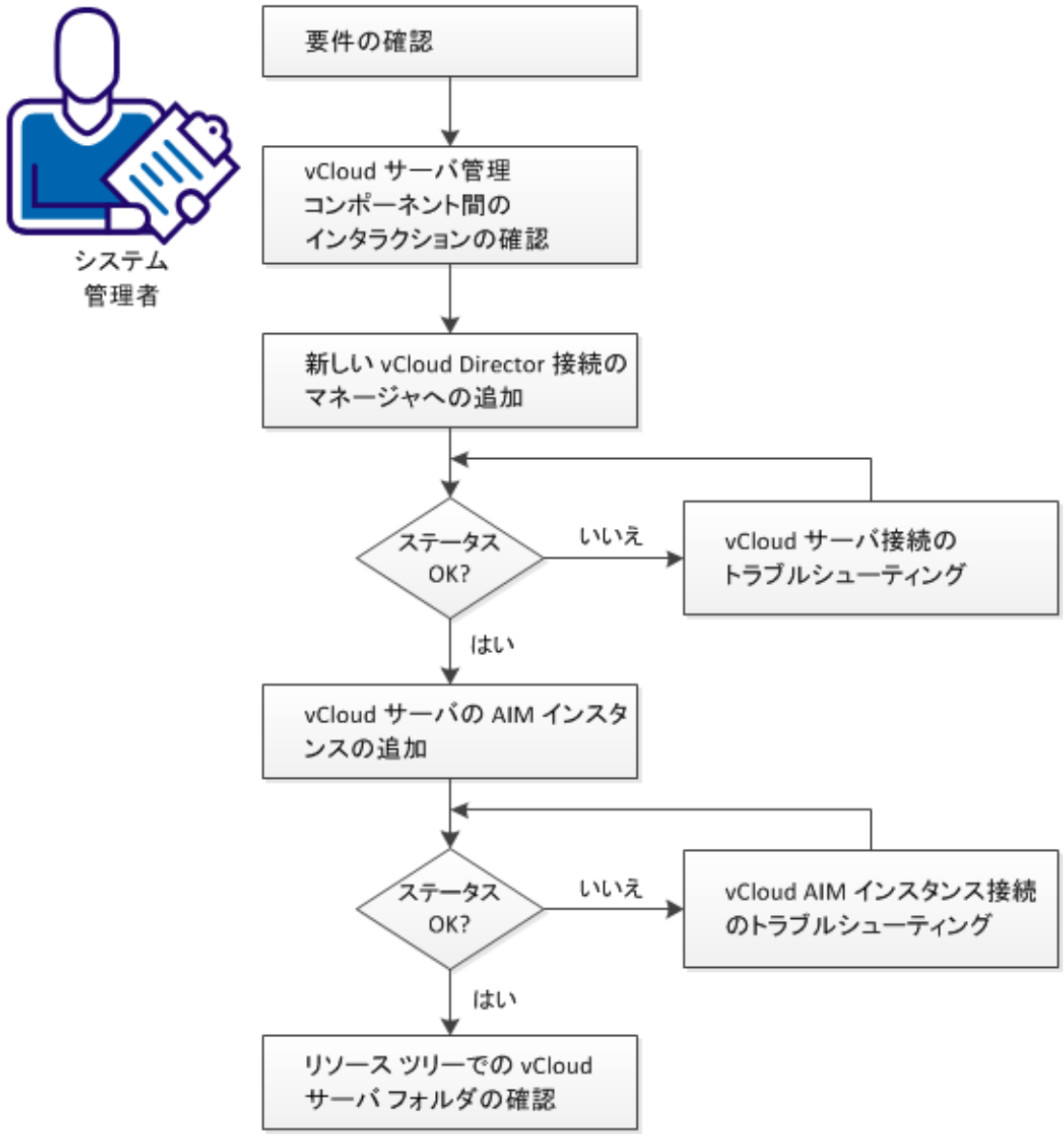
*仮想データセンター（vDC）*は、vCloud 組織に仮想計算リソースを提供します。 仮想システムのプロビジョニング、実行、および仮想データセンターへの格納を行えます。 vCloud 組織は複数の仮想データセンターを持つことができます。

組織は、vApp テンプレートおよびメディア ファイルを格納するために*カタログ*を提供します。 組織のメンバは、独自の vApp を作成するためにカタログで vApp テンプレートおよびメディア ファイルを使用できます。

vCloud Director 管理コンポーネントを設定する方法

以下の図は、必要なアクションに関する概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

vCloud サーバ管理コンポーネントを設定する方法



以下の手順に従います。

vCloud の要件の確認

CA Server Automation の vCloud Director 管理コンポーネントの設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティングシステムに精通している。
- CA Server Automation、CASystemEDGE、VMware vSphere、および VMware vCloud に関する基礎知識がある。
- VMware プラットフォーム管理モジュール（PMM）、vCloud Application Insight Module （AIM）、およびモニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる vCloud Director サーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して vCloud Director にアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- vSphere 環境とその vCloud Director が正しく実行されることを確認済みである。
- VMware PMM と vCloud AIM が別々のシステムにインストールされている場合、それらのシステムでの SNMP 設定に整合性があることを確認済みである。 読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するすべてのリモート vCloud AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

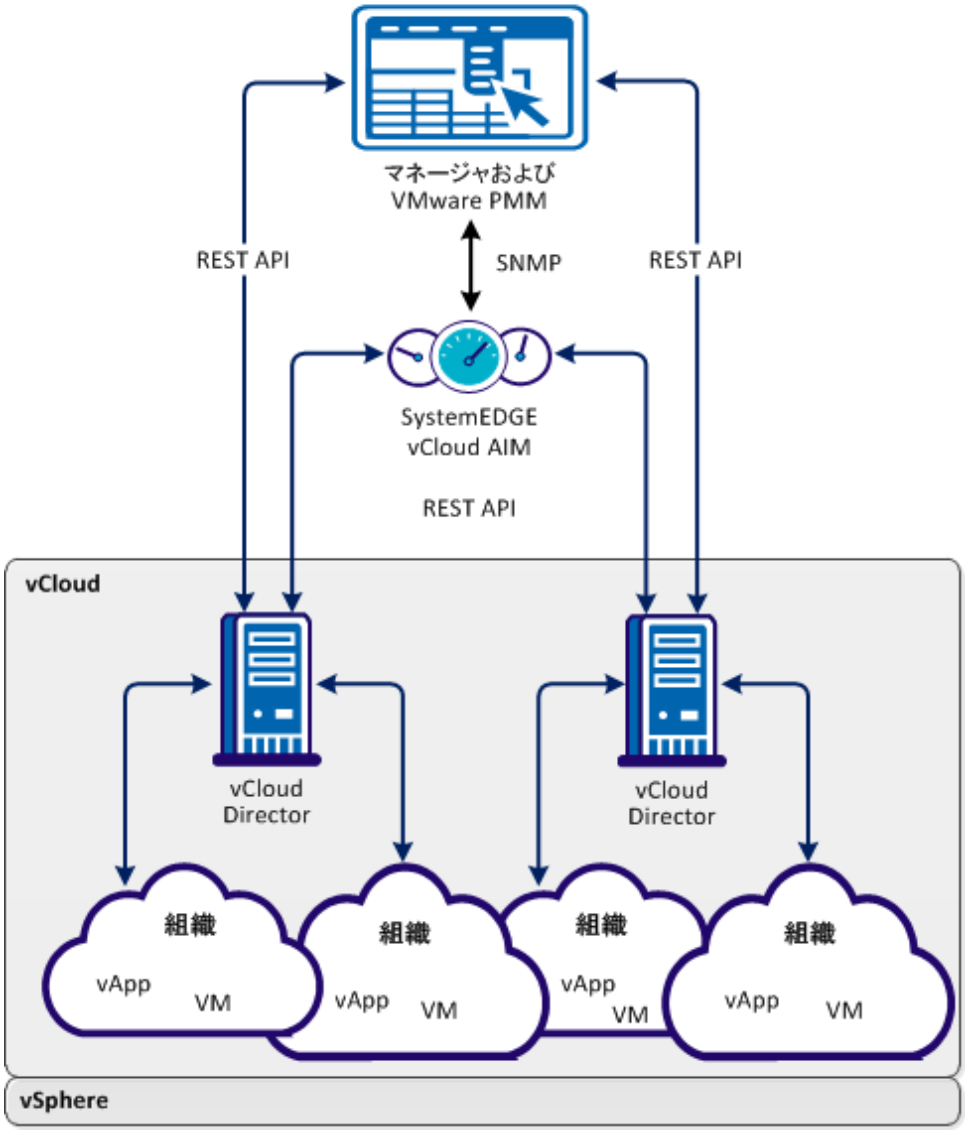
関連項目:

vCloud Director 接続のマネージャへの追加 (P. 582)
vCloud サーバの AIM インスタンスの追加 (P. 586)
リソース ツリーでの VMware vCloud フォルダの確認 (P. 593)

vCloud 管理コンポーネント間のインタラクション

以下の図は、vCloud Director 管理に関与するコンポーネントがどのように対話するかを示しています。 SystemEDGE と vCloud AIM は、同じ Windows サーバ上で実行します。 この AIM は、1 つ以上のリモート vCloud Director サーバと通信して、仮想環境を管理します。vCloud AIM はデータを収集し、vCloud Director と関連付けられている仮想リソースをすべて表示します。基盤となる vSphere 環境は、仮想マシンおよび vApp を実行するためのリソースを提供します。

vCloud Director 管理コンポーネント間のインタラクション



vCloud の管理は、ユーザ インターフェースの［管理］タブで設定できます。

注: VMware ツールは、VM の仮想化を最適化します。このツールを VMware 環境内の各 VM にインストールすることをお勧めします。VMware ツールがインストールされていない VM では、この製品の一部の機能が利用できないか、または正常に機能しません。 この理由により、VMware ツールがインストールされていない VM はサポートされていません。

vCloud Director 接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、vCloud Director 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［vCloud サーバ］を選択します。

   右側のペインがリフレッシュされ、管理対象の vCloud サーバ、関連付けられている vCloud AIM サーバ、および vCloud サーバ AIM インスタンスが表示されます。

3. ［vCloud サーバ］ペイン ツールバーの（追加）をクリックします。

   ［vCloud サーバの追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ名、パスワード、プロトコル、ポート）を入力し、優先 AIM を指定し、［管理ステータス］（チェック ボックス）をオンにして、［OK］をクリックします。

   ユーザ名を指定するときには、ユーザ役割およびアクセス レベルを考慮するために以下の構文を使用できます。

   - システム管理者（フル アクセス） : administrator@System
   - 組織レベルおよび役割の割り当ての操作に制限（組織によるアクセス） : *username@organization_name*

   ネットワーク接続が正常に確立されている場合、右上の［vCloud サーバ］ペインに vCloud サーバが緑のステータス アイコンを使って追加されます。 CA Server Automation によって vCloud サーバが自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によって vCloud サーバが赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。 接続のトラブルシューティングについては、「vCloud サーバ接続のトラブルシューティング (P. 583)」を参照してください。

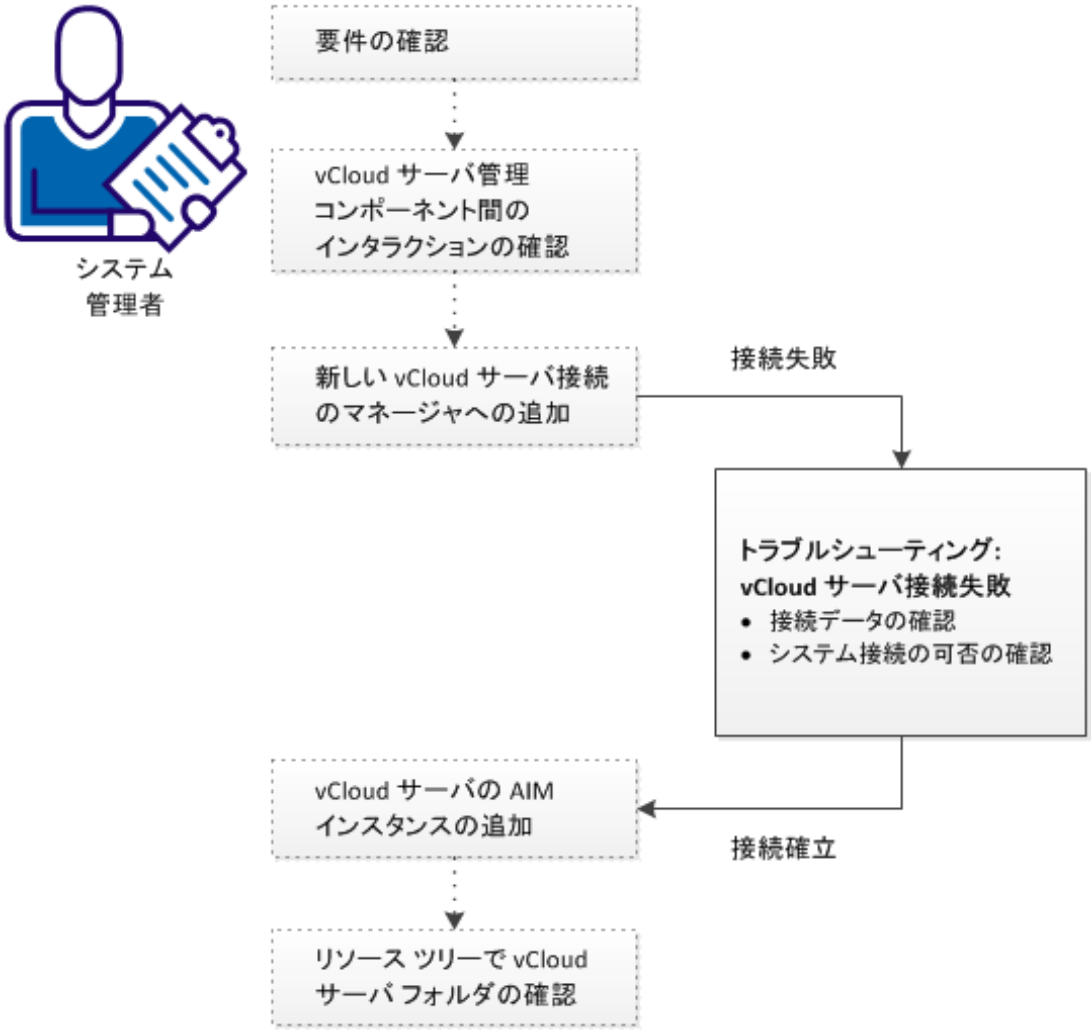
関連項目:

vCloud サーバの AIM インスタンスの追加 (P. 586)
リソース ツリーでの VMware vCloud フォルダの確認 (P. 593)
vCloud サーバ接続のトラブルシューティング (P. 583)

vCloud サーバ接続のトラブルシューティング

vCloud サーバ接続に失敗しました。 以下の図に示すトラブルシューティング情報に従ってください。

vCloud サーバ接続のトラブルシューティング方法



以下の手順に従います。

vCloud サーバ接続の失敗 (P. 584)
vCloud サーバの AIM インスタンスの追加 (P. 586)
リソース ツリーでの VMware vCloud フォルダの確認 (P. 593)

vCloud サーバ接続の失敗

症状:

［管理］-［設定］で新しい vCloud サーバ接続を追加した後、vCloud サーバへの接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCloud サーバの接続に使用したデータ（サーバ名、ユーザ、パスワード、プロトコル、ポート）が今でも有効かどうかを確認します。 必要な場合は、接続データを更新します。
- vCloud サーバシステムが実行されており、アクセス可能であるかどうかを確認します。

vCloud サーバの接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。

   ［vCloud サーバの追加］または［vCloud サーバの編集］ダイアログ ボックスが表示されます。

2. 有効なサーバ名、ユーザ、パスワード、プロトコル、およびポートを追加します。 優先 AIM を指定します。 ［管理ステータス］を有効にして［OK］をクリックします。

   接続データが更新されます。

3. 右上角の  （検証）をクリックして新しい設定を検証します。

   vCloud サーバへの接続を確立できない場合は、次の手順に進みます。

vCloud サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <vCloud Server Name>
   ping <IP Address of vCloud Server>
   ```

2. vCloud サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   vCloud サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに vCloud サーバを追加します。手順 3 に進みます。

   vCloud サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <vCloud Server Name>
   ```

   正しい IP アドレスと vCloud サーバの名前を入力します。 例：

   ```
   192.168.50.50 myvCloud
   ```

4. 右上角の  （検証）をクリックします。

   vCloud サーバへの接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

   vCloud の管理者または VMware のサポート担当者と協力して、vCloud サーバの接続の問題を解決します。

vCloud サーバの AIM インスタンスの追加

CA Server Automation マネージャに新しい vCloud サーバ接続を追加した後、新しい vCloud サーバを管理するための vCloud AIM インスタンスを追加します。 その後、組織、vApp、VM など、そのすべての仮想コンポーネントを含む vCloud 環境全体が CA Server Automation によって検出されます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［vCloud サーバ］を選択します。

   右側のペインがリフレッシュされ、管理対象の vCloud サーバ、関連付けられている vCloud AIM サーバ、および管理対象の vCloud サーバの AIM インスタンスが表示されます。

3. ［vCloud AIM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［vCloud AIM サーバの追加］ ダイアログ ボックスが表示されます。

4. ［vCloud AIM サーバ］ ドロップダウン リストを開きます。

   検出された vCloud AIM サーバのリストが表示されます。vCloud AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウン リストから vCloud AIM サーバを選択します。

   ［vCloud サーバ］ペインに一覧表示された vCloud サーバが［vCloud サーバ］ドロップダウン リストに入力されます。 つまり、管理できる vCloud サーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

6. 管理する vCloud サーバを選択し、［OK］をクリックします。

   選択した vCloud サーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている vCloud 環境の検出を開始します。ディスカバリ プロセスが完了したら、vCloud の仮想リソースの管理を開始できます。

関連項目:

リソース ツリーでの VMware vCloud フォルダの確認 (P. 593)
vCloud AIM インスタンス接続のトラブルシューティング (P. 588)

vCloud AIM インスタンス接続のトラブルシューティング

vCloud AIM 接続が準備未完了のステータスにあります。以下のいずれかのステータス アイコンが表示されます。

 ディスカバリ中 - プラットフォーム マネージャによってすべてのデータが同期されるまで待機します。

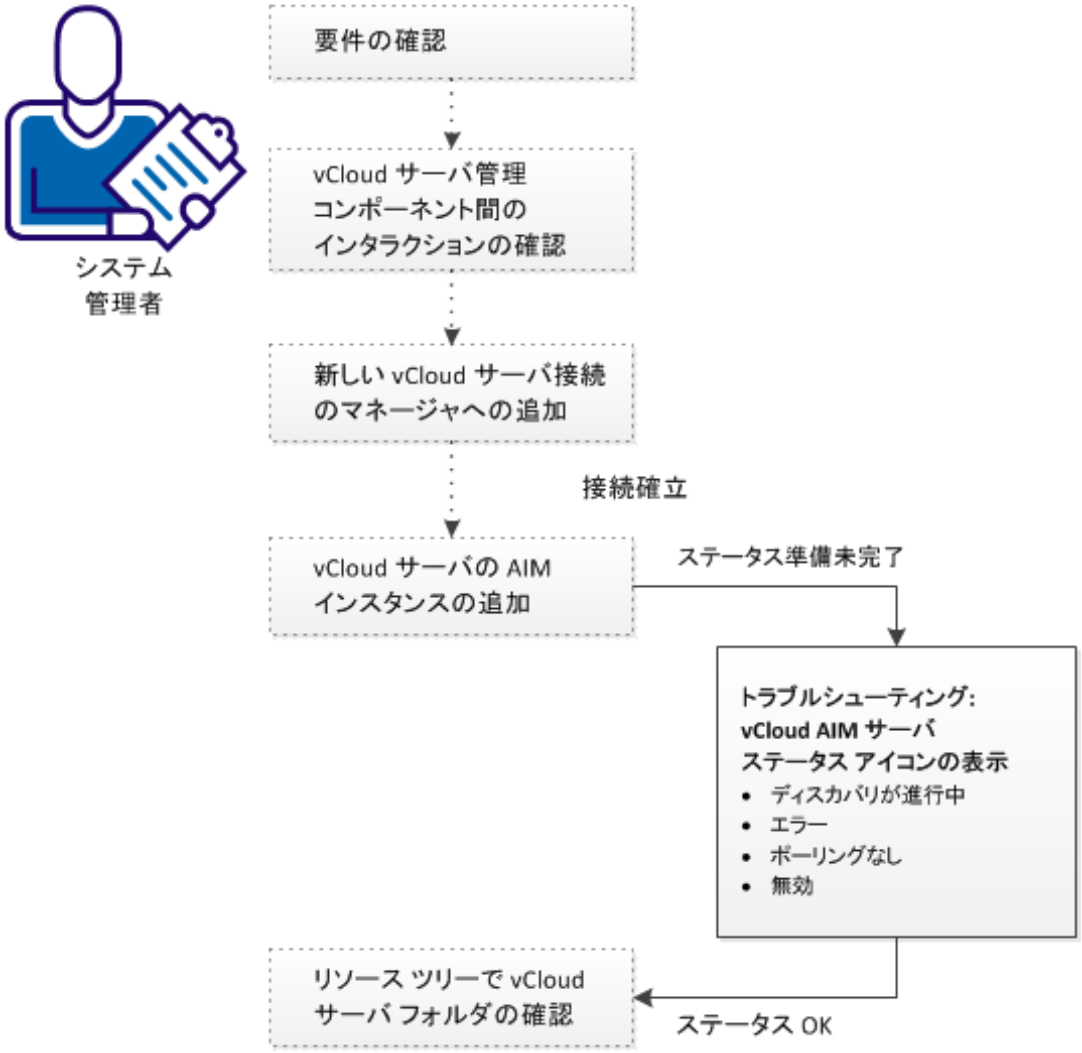
 エラー - AIM に接続できません。 ネットワーク接続を確認してください。

 ポーリングなし - CA Server Automation マネージャはこの AIM インスタンスをポーリングしません。

 無効 - このインスタンスは管理されていません。

以下の図に示すトラブルシューティング情報に従ってください。

vCloud AIM インスタンス接続のトラブルシューティング方法



関連項目:

vCloud AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される (P. 590)
vCloud AIM インスタンスのステータス アイコンに「エラー」が表示される (P. 590)
vCloud AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される (P. 592)
vCloud AIM インスタンスのステータス アイコンに「無効」が表示される (P. 592)

vCloud AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］で vCloud サーバに対して vCloud AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

vCloud 環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、vCloud 内の仮想リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを置くと、未処理のディスカバリ要求の数を示すツールヒントが表示されます。 ディスカバリ ジョブが完了すると、CA Server Automation は vCloud サーバ フォルダをリソース ツリーに追加します。 これで、vCloud とその仮想インフラストラクチャ全体の管理を開始できます。

vCloud AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で vCloud サーバに対して vCloud AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

vCloud AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- vCloud AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

vCloud AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. vCloud AIM サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   vCloud AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに vCloud AIM サーバを追加します。 手順 3 に進みます。

   vCloud サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと vCloud AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myvCloudAIM
   ```

4. ［vCloud AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. vCloud AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［vCloud AIM サーバ］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によって vCloud AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

vCloud AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で vCloud Director に対して vCloud AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定の vCloud Director を管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。 サーバ エントリの［編集］をクリックし、優先 AIM を選択します。 優先 AIM が現在の AIM になります。

vCloud AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の vCloud AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン  （無効）が表示されます。 この vCloud AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ vCloud AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが、管理対象外の状態である vCloud サーバ用に vCloud AIM が設定されている。
- ［vCloud サーバ］ペインで設定されていない vCloud サーバに AIM が接続されている。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下のいずれかを実行します。

- 欠落している vCloud サーバから CA Server Automation マネージャへの接続を追加します。
- 既存の vCloud サーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの VMware vCloud フォルダの確認

新しい vCloud サーバは、設定およびディスカバリに成功すると、［リソース］-［エクスプローラ］ペインの［VMware vCloud］フォルダに示されます。

次の手順に従ってください:

1. ［リソース］-［エクスプローラ］をクリックします。

   リソース ツリーが表示されます。

2. ［VMware vCloud］を展開します。

   管理対象の vCloud Director サーバが表示されます。

3. 新しい vCloud Director サーバ エントリを展開します。

   管理対象の vCloud インフラストラクチャが表示されます（組織、vApp、VM など）。

CA Server Automation で、追加された vCloud 環境とその仮想インフラストラクチャを管理する準備が整いました。

リモートおよびマルチインスタンスの vCloud Director のサポート

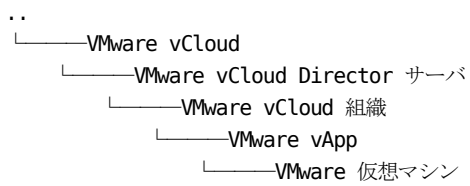
vCloud AIM は 1 つ以上のリモート vCloud Director インスタンスと通信します。 ただし、複数のリモート vCloud AIM を持つ CA Server Automation マネージャを使用して複数の vCloud Director 環境を管理する場合は、以下を考慮してください。

それぞれの vCloud Director は、設定時に指定した優先 vCloud AIM の 1 つと一意に関連付けられます。優先 AIM の設定は、複数の AIM で 1 つの vCloud Director を管理する場合に、どの AIM をポーリングに使用するかを示します。

vCloud のフォルダ構造

vCloud Director サーバへの接続が正しく設定されると、CA Server Automation によって、組織、vApp、および仮想マシンから構成される vCloud Director 環境が検出されます。ディスカバリが完了すると、VMware vCloud フォルダが [リソース] タブの [エクスプローラ] ペインに表示されます。フォルダを展開して、vCloud 環境を管理することができます。

以下の図は、VMware vCloud フォルダの下のオブジェクト階層を表しています。



VMware vCloud フォルダは、最上位のサービス レベルを表します。 vCloud サービスは、複数の VMware vCloud Director サーバで構成できます。 それぞれの vCloud Director には、通常は vApp と仮想マシンを持つ複数の組織があります。

組織レベルでは、カタログに保存されたテンプレートに基づいて vApp をプロビジョニングできます。

vCloud での vApp のサポート

vApp の概念は、vCloud 環境と vSphere 環境で類似しています。どちらも、単一のエンティティとして操作できるアプリケーション オブジェクトを表しています。 通常、vApp には複数の VM が含まれています。それぞれの VM には、エンドユーザに提供する vApp アプリケーションまたはサービスを実行するという独自の目的があります。vApp で実行される操作は、vApp のすべての VM でも実行されます。たとえばどちらのタイプも、vApp 内のすべての VM の起動および停止順序を定義し、vApp 内のすべての VM が使用できる CPU とメモリのリソース制限を定義します。

vCloud 内の vApp の目的は、アプリケーションまたはサービスをテンプレートとして 1 度定義して、組織カタログによってそれを複数の組織からアクセスできるようにすることです。 vCloud はデータを vCloud データベースに保存します。これは vCenter Server データベースとは異なります。

重要: vCloud で定義した VM を vCenter Server から直接操作しないでください。この操作によって、vCloud データベースが実際に定義された VM と同期できなくなる場合があります。 CA Server Automation は、データベースが非同期にならないように、vCloud および vCenter Server の下に表示される VM に対する操作を制限しています。

vCloud vApp と vSphere vApp の相違点

- vCloud vApp には、ネスト階層のための機能がありません。 vSphere vApp にはほかの vApp およびリソース プールを含めることができます。
- vCloud では、CPU とメモリのリソース制限は仮想データセンター(vDC)によって定義されます。また、vApp はこれらの仮想データセンターのいずれかにマップされます。

  vSphere では、vApp のリソース制限は vApp 自体によって定義されます。
- vCloud vApp には、さまざまな vCenter Server および ESX ホストで定義された VM を含めることができます。

  vSphere vApp の VM は、特定のデータセンターおよびクラスタの VM に制限されています。
- vCloud vApp はリース制限があります。 vApp のランタイムとストレージの制限を定義できます。 ランタイム制限に到達すると、vCloud vApp は使用できなくなります。ストレージ制限に到達すると、vApp は組織のリース ポリシーに応じて vCloud から削除されるか、期限切れ項目フォルダに移動されます。

  vSphere vApp は、ユーザが手動で削除するまで残ります。
- vCloud vApp は vApp テンプレートから作成されます。vApp テンプレートは、vCenter Server から VM をインポートするか、OVF パッケージをインポートすることで作成されます。vApp は、テンプレートを作成した組織のクラウドにテンプレートを展開することによって作成されます。 展開後、その他の VM は vApp へ移動させることができます。

  vSphere vApp は、CPU とメモリのリソースに必要な制限を加えて vApp を定義することで作成されます。その後、vApp が定義されたデータ センター用の VM は、vApp へ移動させることができます。

vCloud のリソース プール プロバイダとしての vCenter Server

vCenter Server の役割を設定して、vCloud のリソース プール プロバイダとして機能させることができます。この場合、vCenter Server は、vCloud が VM を作成するための計算リソースとメモリ リソースを提供します。 このリソース プールは、プロバイダ vDC として vCloud に表示されます。

この設定によって、このリソース プールの VM が、vCenter オブジェクト階層および vCloud オブジェクト階層の CA Server Automation ［エクスプローラ］ペインに表示されます。 そのような VM の［サマリ］パネルの vCloud の下には、vCenter Server の下に表示されるのと同じ情報が表示されます。

- パフォーマンス チャート
- 一般情報
- 概要（モニタ対象リソースのステータス情報）
- CPU とメモリの使用率（しきい値の設定は vCenter Server のみでサポートされます）
- ディスク使用率

これらの VM に適用できる操作セットは、vCloud および vCenter Server 環境の両方で制限されます。操作セットを制限することで、vCenter と vCloud が同期されない問題を回避できます。 たとえば、その VM の親 vApp が vCloud で実行中の場合、vCenter Server 下の VM の電源はオフにできません。そのような VM の電源をオフにするには、最初に vCloud 内の vApp の電源をオフにします。

有効な VM 操作を以下に示します。

- モニタリング ソフトウェアの展開
- 自動化ルールの管理
- サーバ メトリック収集の設定
- しきい値の設定

VM が作成された vCloud に vCenter Server への接続がない場合、［サマリ］ペインには以下の情報のみが表示されます。

- アイテム タイプ
- 名前
- 稼働ステータス

vCloud 組織

vCloud 組織は、ユーザ、グループ、および計算リソースのコレクションに対する管理の 1 単位です。組織は、vApp テンプレートおよびメディア ファイルを格納するためにカタログを提供します。 組織のメンバは、独自の vApp を作成するためにカタログで vApp テンプレートおよびメディア ファイルを使用できます。

仮想データセンター（vDC）は、vCloud 組織に仮想計算リソースを提供します。 仮想システムのプロビジョニング、実行、および仮想データセンターへの格納を行えます。 vCloud 組織は複数の仮想データセンターを持つことができます。

テンプレートからの vApp のプロビジョニング

vCloud 組織のレベルでは、カタログに保存されるテンプレートから vApp をプロビジョニングできます。

次の手順に従ってください:

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. VMware vCloud フォルダを展開します。

   vCloud フォルダの構造が表示されます。

4. 組織オブジェクトを右クリックします。

   ［プロビジョニング］ポップアップ メニューが表示されます。

5. ［テンプレートからの vApp のプロビジョニング］をクリックします。

   ［テンプレートからの新規 vApp のプロビジョニング］ダイアログ ボックスが表示されます。

6. ［名前］、［vApp テンプレート］、［展開リース］、および［ストレージ リース］を指定します。 ［OK］をクリックします。

   CA Server Automation によって組織内に vApp が作成されます。

vCloud の vApp に対する操作

vCloud 組織のレベルでは、カタログに保存されるテンプレートから vApp をプロビジョニングできます。

次の手順に従ってください:

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. VMware vCloud フォルダを展開します。

   vCloud フォルダの構造が表示されます。

4. vApp オブジェクトを右クリックします。

   ［管理］ポップアップ メニューが表示されます。

5. 以下のいずれかの操作を選択します。

   vApp の電源オン

   vCloud vApp の電源をオンにします。

   vApp の電源オフ

   vCloud vApp の電源をオフにします。

   vApp のリセット

   vCloud vApp をリセットします。

   vApp の中断

   vCloud vApp を中断します。

   vApp の再開

   vCloud vApp を再開します。

   vApp のクローン作成

   既存の vApp から vCloud vApp を作成します。

   vApp の移動

   vCloud vApp を別の仮想データセンターに移動します。

vApp の削除

vCloud vApp を削除します。

vApp リースの変更

展開およびストレージ リースを変更します。

必要なパラメータ値を指定して、［OK］をクリックします。

6. ［イベント］をクリックして、vApp の新規ステータスを確認します。

イベントのリストが表示されます。

VMware vSphere および vCenter Server

CA Server Automation は、VMware vSphere および vCenter Server の仮想環境を管理します。 vCenter Server は、vSphere 環境にアクセスするために CA Server Automation および vCenter AIM が使用する主要コンポーネントです。SystemEDGE と vCenter AIM は、CA Server Automation マネージャ サーバまたは任意の Windows サーバ上で実行されます。

CA Server Automation は、接続およびすべての VMware vCenter Server 操作の運用上のサポートを提供します。 マネージャは、接続の管理、VM 関連操作の実行、VMware vCenter Server から取得したデータのデータベースへの入力を行います。 プロビジョニング サービスは、クローニング、電源操作、リソースおよび共有の調整などの VMware vCenter Server 操作を実行します。

vCenter Server AIM は、Web サービスを使用して 1 つ以上のリモート vCenter Server インスタンスと通信します。 AIM は SNMP を使用してマネージャと通信します。vCenter Server の管理に複数の vCenter AIM を利用できる場合、設定時に任意の vCenter AIM を指定できます。または、マネージャに選択させることもできます。

注: eHealth、Spectrum Infrastructure Manager 環境で CA Server Automation マネージャを使用せずに vCenter AIM を実行した場合、AIM はシングル インスタンス モードのみをサポートします。

モニタ対象の vSphere および vCenter Server のリソース

vCenter AIM は、vSphere 環境のコンポーネント間の論理的および物理的関係を検出します。AIM は、仮想化された環境全体を視覚化し、以下のリソース タイプやプロパティを管理します。

データセンター

*データセンター*は、ホスト、仮想マシン、リソース プール、またはクラスタのコンテナとして機能します。仮想設定が特定の部門の要件を満たしていれば、データセンターは、地理的な地域や個別のビジネス機能などの組織構造を表すことができます。また、データセンターを使用して、テスト用の分離された仮想環境を構築したり、環境を組織したりすることができます。

データストア

*データストア*は、データセンター内の基本要素である物理ストレージ リソースの組み合わせを仮想的に表現したものです。これらの物理ストレージ リソースとして提供できるのは、サーバ上のローカル ディスクや SAN ディスク アレイなどです。

ESX ホスト

ESX サーバが実行される物理サーバの計算およびメモリ リソースをすべて表します。

ハードウェア センサ

CPU、メモリ、ファン、電圧、ストレージ、温度、および電源に関する物理情報を提供します。ハードウェア センサには、vCenter Server 経由で ESX サーバでアクセスできます。

物理 NIC

ESX サーバ上の物理イーサネット アダプタを指定します。

リソース プール

*リソース プール*は、単一ホストまたはクラスタの物理的なコンピューティング リソースとメモリ リソースのパーティションを定義します。任意のリソース プールを小さくパーティション分割することで、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。また、リソース プールを階層的に構成して、ネストすることもできます。

vApp

vApp は、VM の集合を 1 つの単位として扱う特殊なリソース プールです。 vApp は Open Virtualization Format を使用します。 Open Virtualization Format（OVF）は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービス レベルを規定し、カプセル化するための標準です。 CA Server Automation は vApp 上で操作を実行できます。 vApp 上での操作は vApp 内のすべての VM にプロパゲートされます。

vCenter Server

vCenter Server コンピュータのヘルス状態に関する情報を提供します。たとえば、CPU、データストア、およびメモリ使用率に関するステータスおよびデータが提供されます。

仮想ディスク

*仮想ディスク*は、仮想ゲスト オペレーティング システム内のディスク ドライブを定義します。 仮想ディスクは、ローカル ホストまたはリモート ファイル システム上にある特定のファイルまたはファイルのセットです。これは、オペレーティング システム内の物理ディスク ドライブと同じように動作します。

仮想マシン

ゲスト オペレーティング システムおよびアプリケーションが実行可能な仮想化された x86 環境を指定します。 仮想マシンを作成すると、特定のホスト、クラスタ、またはリソース プールに割り当てられ、さらにデータ ストアに割り当てられます。仮想マシンは、物理デバイスがそのワークロードに応じてエネルギーを動的に使用するのと同様に、その物理ホスト上でリソースを動的に使用します。

VMware クラスタ/高可用性/フォールト トレランス

VMware vSphere では、高可用性（HA）のために設定されたクラスタに定義された VM 上で *フォールト トレランス（FT）*を有効にすることができます。フォールト トレランスは、クラスタ内の別の ESX サーバ上でセカンダリ VM を作成します。 セカンダリ VM は、ワークロードを実行しているプライマリ VM とのロックステップ モードで作動します。 障害が発生した場合は、セカンダリ VM が、すぐに障害発生時点からワークロードの実行を引き継ぎます。 CA Server Automation は、クラスタ内のプライマリおよびセカンダリ VM を検出して管理します。

vNetwork Distributed Switch

ホストからデータセンター レベルまでの仮想スイッチの設定を抽象化します。 vNetwork Distributed Switch は、そのスイッチに関連付けられているデータセンター内のすべてのホストにおいて、単一の仮想スイッチとして動作します。 vNetwork Distributed Switch は、分散ポート グループから構成されます。これは、標準的なスイッチ上のポート グループと同様に設定されていますが、複数のホストにわたっています。これらのプロパティは複数のホスト間でマイグレートされるため、仮想マシンで一貫したネットワーク設定を維持できます。

vNetwork Standard Switch

物理スイッチと同様に動作します。各 ESX サーバには、ポート グループを通じて仮想マシンに接続する固有の仮想スイッチがあります。これらの仮想スイッチには、ESX サーバの物理イーサネット アダプタへのアップリンク接続もあります。仮想マシンは、仮想スイッチ アップリンクに接続された物理イーサネット アダプタを通じて外界と通信します。

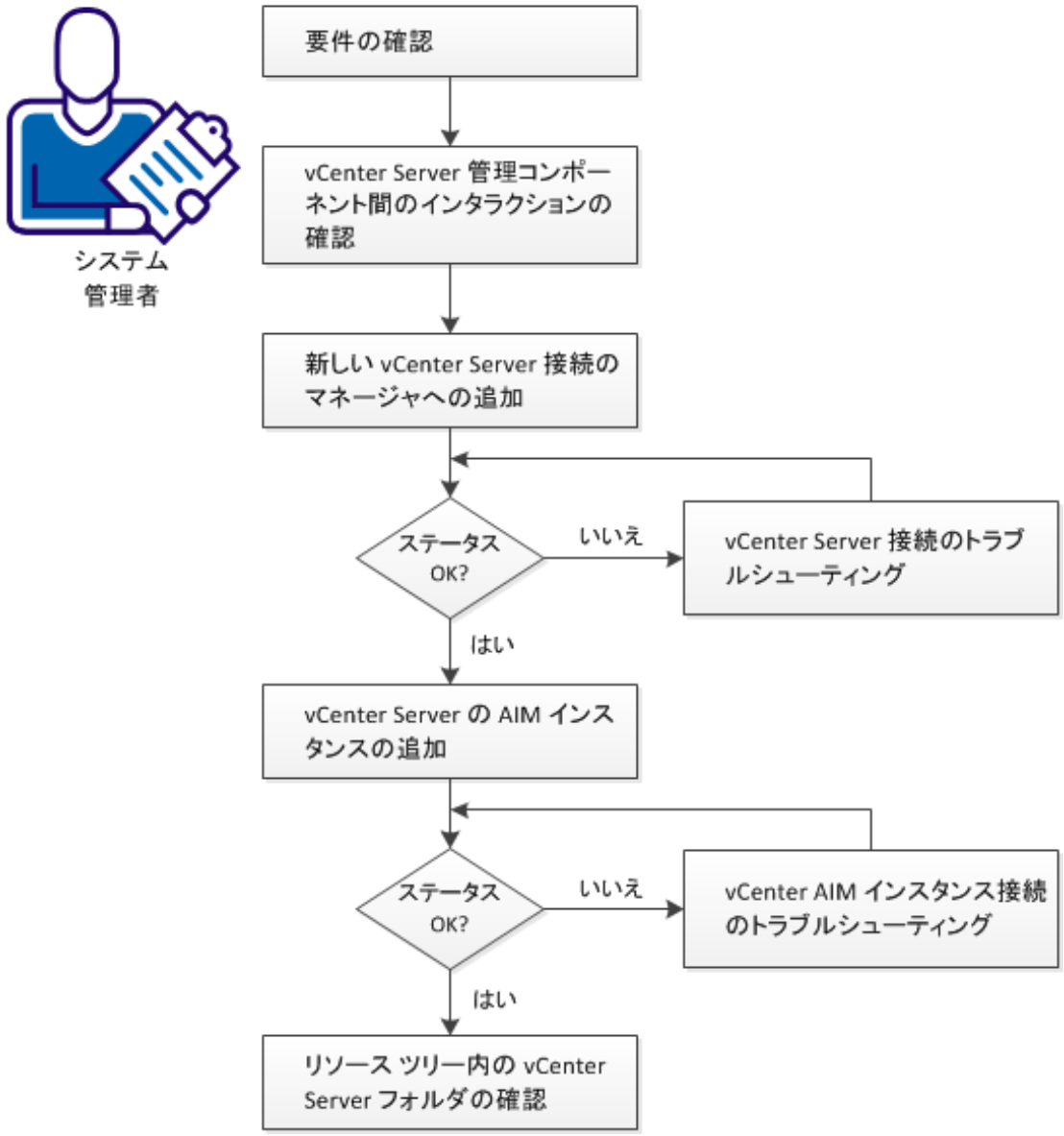
仮想 NIC

仮想マシン上の仮想イーサネット アダプタを指定します。 ゲスト オペレーティング システムは、仮想イーサネット アダプタが物理イーサネット アダプタであるかのように、デバイス ドライバを介して仮想イーサネット アダプタと通信します。 仮想イーサネット アダプタは固有の MAC アドレスと 1 つ以上の IP アドレスを持ち、標準的なイーサネット プロトコルに応答します。

vCenter Server 管理コンポーネントを設定する方法

以下の図は、必要なアクションに関する概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

vCenter Server 管理コンポーネントを設定する方法



以下の手順に従います。

要件の確認

CA Server Automation の vCenter Server 管理コンポーネントの設定を開始する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation、CASystemEDGE、および VMware vSphere に関する基礎知識を持っている。
- vCenter プラットフォーム管理モジュール（PMM）、vCenter Application Insight Module （AIM）、およびモニタリング エージェント（CA SystemEDGE）を含む CA Server Automation マネージャ インストールにアクセスできる。
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる新しい vSphere 環境の vCenter Server にアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。
- Web サービスを通して vSphere 環境の vCenter Server にアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 新しい vSphere 環境とその vCenter Server が正しく実行されることを確認済みである。
- VMware PMM と vCenter AIM が別々のシステムにインストールされている場合、それらのシステムでの SNMP 設定に整合性があることを確認済みである。 読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート vCenter AIM サーバが CA Server Automation マネージャによって検出されたことを確認済みである。

関連項目:

vCenter Server 管理コンポーネント間のインタラクションの確認 (P. 605)
新しい vCenter Server 接続のマネージャへの追加 (P. 609)
vCenter Server の AIM インスタンスの追加 (P. 614)
リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)

vCenter Server 管理コンポーネント間のインタラクションの確認

システム管理者として、CA Server Automation を使って新しい VMware vSphere 環境を管理するとします。 CA Server Automation を使用すると、1 つ以上の vSphere 環境の物理リソースと仮想リソースを動的に管理できます。

vSphere は、1 台の vCenter Server、物理 ESXi ホスト、および ESXi ホスト上で実行される仮想インフラストラクチャから構成されます。 vCenter Server は、仮想インフラストラクチャ全体を含む vSphere 環境を制御するための中心点です。 このインフラストラクチャの構成要素には、データセンター、クラスタ、リソース プール、vApps、VM、仮想デバイス、仮想スイッチなどがあります。 vSphere を管理するため、CA Server Automation は、その vCenter プラットフォーム管理モジュール（PMM）、vCenter Application Insight Module（AIM）、および VMware vCenter Server の間にネットワーク接続を必要とします。 これらのネットワーク接続を確立するには、CA Server Automation vCenter Server 管理コンポーネント（つまり vCenter PMM と vCenter AIM）を設定します。

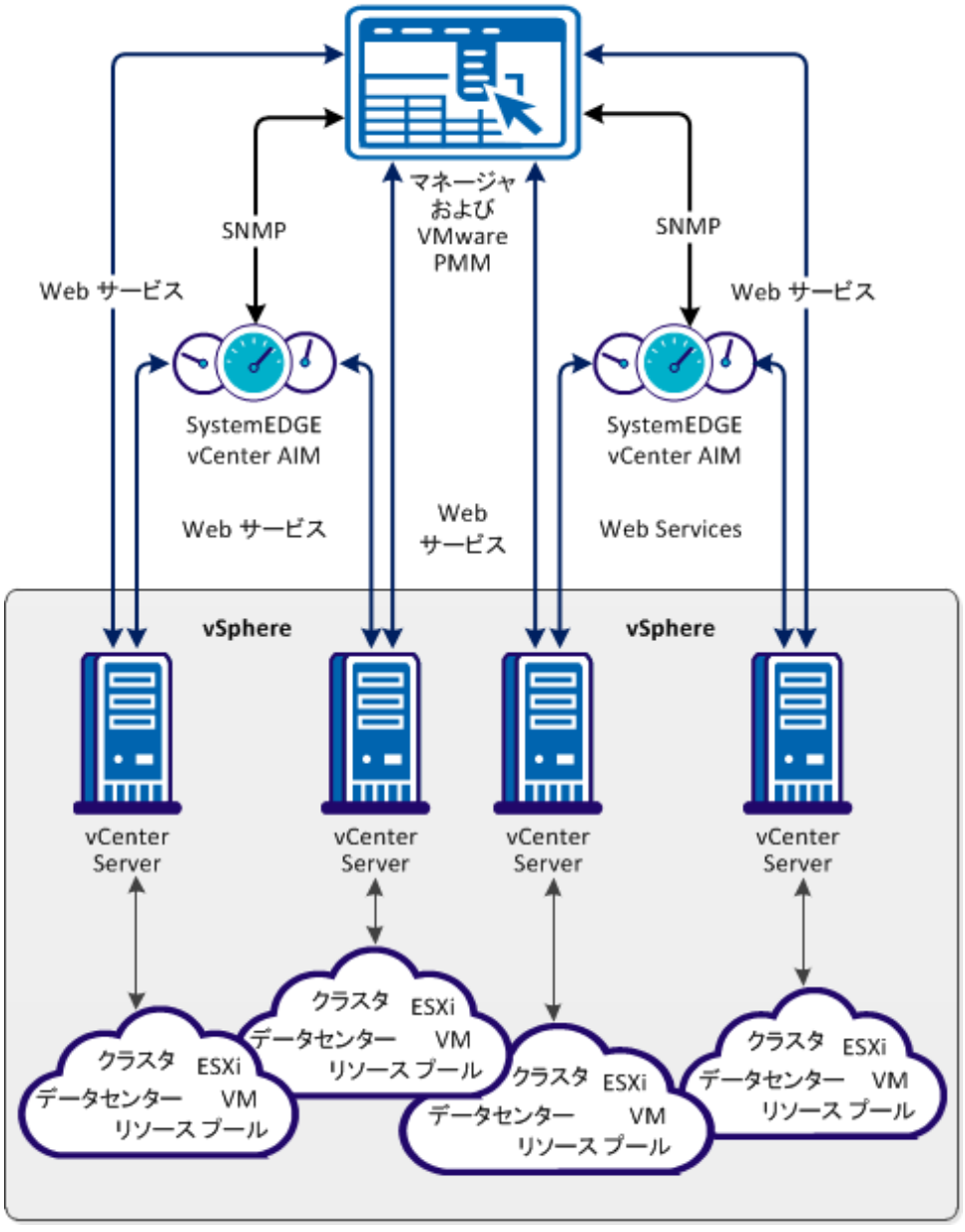
vCenter AIM は、SystemEDGE の機能範囲を拡張する SystemEDGE エージェント プラグインです。 vCenter AIM によって SystemEDGE は、複数の vSphere 環境のパフォーマンスをモニタでき、モニタ対象 vSphere リソースの状態を評価できます。 一般的なモニタ対象リソースは、仮想 CPU、仮想メモリ、仮想スイッチ、仮想ディスク、リソース プール、vApp、およびその他の仮想リソースです。 しきい値に基づき、SystemEDGE および vCenter AIM はモニタ対象リソースのステータスを判断し、その情報を SNMP を使用して CA Server Automation マネージャにプロパゲートします。

vCenter PMM は CA Server Automation マネージャのコンポーネントです。 PMM には、Web サービスを使用するすべての VMware vCenter 操作のサポートと接続を提供する役割があります。 PMM は、vCenter Server との接続を管理し、vSphere 関連の操作を実行します。また、vCenter AIM からデータを取得し、CA Server Automation 管理データベースに入力します。 典型的な操作には、VM の作成、開始、停止、クローン作成、CPU 共有の追加、削除、VM 実行時の VM へのメモリの追加があります。

vCenter PMM および AIM は相互に対話するので、CA Server Automation は動的に複数の vSphere 環境を管理できます。 CA Server Automation は、AIM によって収集されたしきい値、ステータス、および値に基づいて、自動的に操作を実行できます。 たとえば、CA Server Automation は、VM の負荷に応じて CPU 共有を動的に追加または削除できます。

以下の図は、4 台の vCenter Server によって表される 4 つの vSphere 環境例において、影響を受けるコンポーネントのインタラクションを示しています。 通常、vCenter PMM およびそのマルチインスタンス サポートを含む各 vCenter AIM は、複数の vCenter Server に接続できます。 図中に示される接続では制限が指定されていません。 必要なネットワーク接続は、TCP/IP、SNMP、および Web サービスに基づきます。

vCenter Server 管理コンポーネント間のインタラクション



CA Server Automation コンポーネントを正常に設定すると、CA Server Automation は新しい vSphere 環境を検出します。 検出に成功すると、vSphere 環境の vCenter Server およびその仮想インフラストラクチャが、CA Server Automation の［エクスプローラ］ペインのリソース ツリーに表示されます。 管理者は、新しい vSphere 環境を管理できます。

注: VMware ツールは、VM の仮想化を最適化します。このツールを VMware 環境内の各 VM にインストールすることをお勧めします。VMware ツールがインストールされていない VM では、この製品の一部の機能が利用できないか、または正常に機能しません。 この理由により、VMware ツールがインストールされていない VM はサポートされていません。

関連項目:

新しい vCenter Server 接続のマネージャへの追加 (P. 609)
vCenter Server の AIM インスタンスの追加 (P. 614)
リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)

新しい vCenter Server 接続のマネージャへの追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、vCenter Server 接続を追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［vCenter Server］を選択します。

   右側のペインがリフレッシュされ、管理対象の vCenter Server、関連付けられている vCenter AIM サーバ、および vCenter Server AIM インスタンスが表示されます。

3. ［vCenter Server］ペイン ツールバーの（追加）をクリックします。

   ［新しい vCenter Server］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、プロトコル、ポート）を入力し、優先 AIM を指定し、［管理ステータス］（チェック ボックス）をオンにして、［OK］をクリックします。

   ネットワーク接続が正常に確立されている場合、右上の［vCenter Server］ペインに vCenter Server が緑のステータス アイコンを使って追加されます。 CA Server Automation によって vCenter Server が自動的に検出されます。

   接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。［はい］をクリックすると、CA Server Automation によって vCenter Server が赤のステータス アイコンを使ってリストに追加されます。 ［いいえ］をクリックすると、何も追加されません。 接続のトラブルシューティングについては、「vCenter Server 接続のトラブルシューティング (P. 610)」を参照してください。

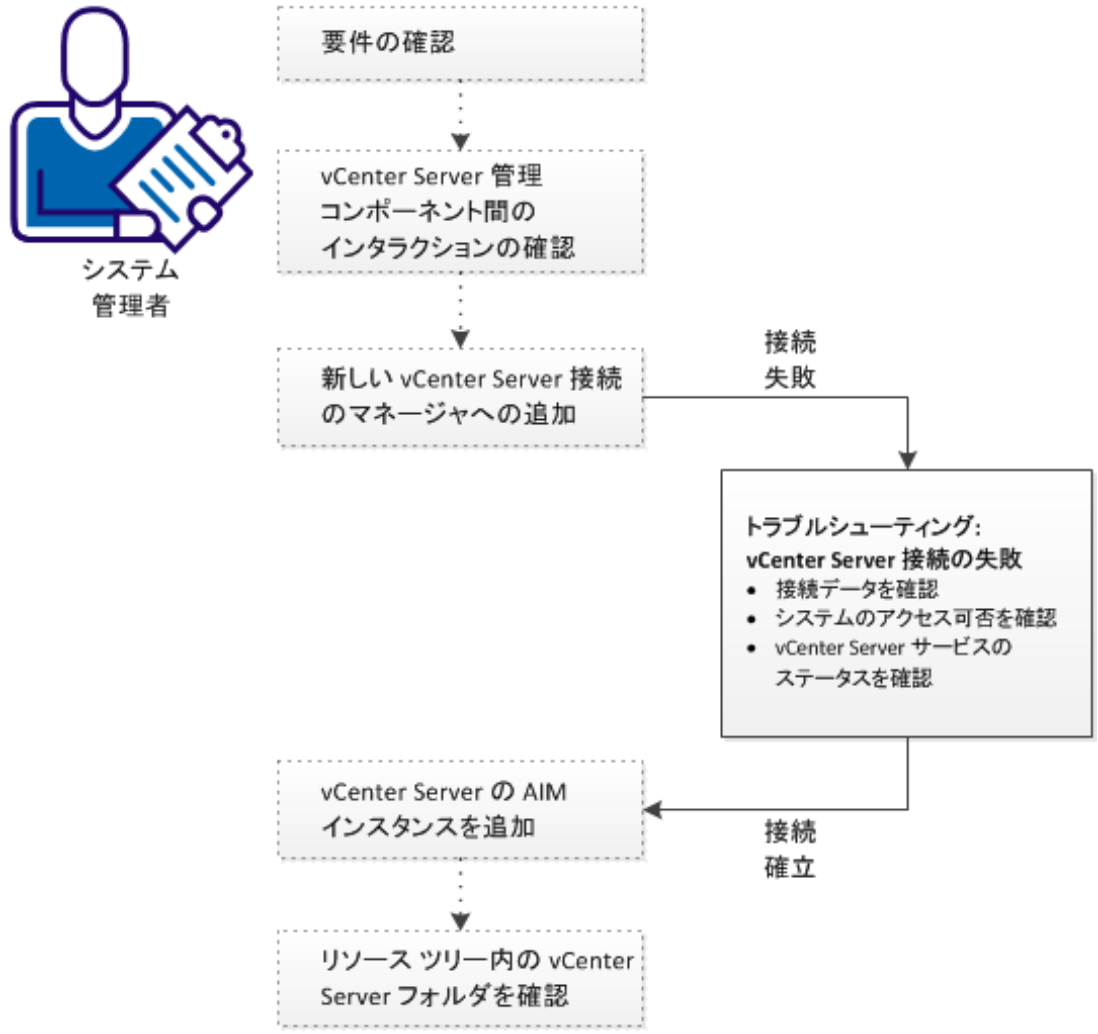
関連項目:

vCenter Server の AIM インスタンスの追加 (P. 614)
リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)
vCenter Server 接続のトラブルシューティング (P. 610)

vCenter Server 接続のトラブルシューティング

vCenter Server 接続に失敗しました。 以下の図に示すトラブルシューティング情報に従ってください。

vCenter Server 接続のトラブルシューティング方法



以下の手順に従います。

vCenter Server の接続に失敗した (P. 611)
vCenter Server の AIM インスタンスの追加 (P. 614)
リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)

vCenter Server の接続に失敗した

症状:

［管理］-［設定］で vCenter Server 接続を追加した後、vCenter Server への接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter Server の接続に使用されたデータ（サーバ名、ユーザ、パスワード、プロトコル、ポート）が今でも有効かどうかを確認します。 必要な場合は、接続データを更新します。
- vCenter Server システムが実行されており、アクセス可能であるかどうかを確認します。
- vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認します。

vCenter Server の接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。

   ［新しい vCenter Server］または［vCenter Server の編集］ダイアログボックスが表示されます。

2. 有効なサーバ名、ユーザ、パスワード、プロトコル、およびポートを追加します。［管理ステータス］を有効にして［OK］をクリックします。

   接続データが更新されます。

3. 右上角の  （検証）をクリックして新しい設定を検証します。

   vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <vCenter Server Name>
   ping <IP Address of vCenter Server>
   ```

2. vCenter Server に有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   vCenter Server が DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに vCenter Server を追加します。 手順 3 に進みます。

   vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <vCenter Server Name>
   ```

   正しい IP アドレスと vCenter Server の名前を入力します。 例：

   ```
   192.168.50.50 myvCenter
   ```

4. 右上角の  （検証）をクリックします。

   vCenter Server の認証情報と接続データが正しく、vCenter Server に対して ping を実行できる場合は、接続がまだ失敗する可能性があります。この場合は、vCenter Server に問題がある可能性があります。 vCenter Server への接続を確立できない場合は、次の手順に進みます。

vCenter Server システム上で VMware 管理サービスが正常に動作しているかどうかを確認する方法

1. vCenter Server システムにアクセスする方法を vSphere の管理者に問い合わせます。
2. vCenter Server システムにログインし、［スタート］メニューから［管理ツール］-［サービス］を開きます。

   ［サービス］ウィンドウが表示されます。
3. *VMware VirtualCenter Server* サービスを選択します。サービスを開始または再開します。
4. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［vCenter Server］ペインの右上角にある  （検証）をクリックします。

   CA Server Automation によって vCenter Server の接続が検証されます。

   vCenter Server への接続が失敗する場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

   vSphere の管理者または VMware のサポート担当者と協力して、vCenter Server の接続の問題を解決します。

vCenter Server の AIM インスタンスの追加

CA Server Automation マネージャに新しい vCenter Server 接続を追加した後、新しい vCenter Server を管理するための vCenter AIM インスタンスを追加します。 その後、vCenter Server、ESX サーバ、VM、その他の仮想コンポーネントなど、そのすべての物理および仮想コンポーネントを含む vSphere 環境全体が CA Server Automation によって検出されます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［vCenter Server］を選択します。

   右側のペインがリフレッシュされ、管理対象の vCenter Server、関連付けられている vCenter AIM サーバ、および管理対象 vCenter Server の AIM インスタンスが表示されます。

3. ［vCenter AIM サーバ］ペイン ツールバーの （追加）をクリックします。

   ［新しい vCenter AIM サーバ］ ダイアログ ボックスが表示されます。

4. ［vCenter AIM サーバ］ ドロップダウン リストを開きます。

   検出された vCenter AIM サーバのリストが表示されます。 vCenter AIM をローカル システムにインストールしている場合は、ローカル システムの名前もリストに表示されます。

5. ドロップダウン リストから vCenter AIM サーバを選択します。

   ［vCenter Server］ペインに一覧表示された vCenter Server が［vCenter Server］ドロップダウン リストに入力されます。 つまり、管理できる vCenter Server は、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

6. 管理する vCenter Server を選択し、［OK］をクリックします。

   選択した vCenter Server の新しい AIM インスタンスが追加されます。 インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている vSphere 環境の検出を開始します。 ディスカバリ プロセスが完了したら、vSphere の仮想および物理リソースの管理を開始できます。

関連項目:

リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)
vCenter AIM インスタンス接続のトラブルシューティング (P. 616)

vCenter AIM インスタンス接続のトラブルシューティング

vCenter AIM 接続が準備未完了のステータスにあります。 以下のいずれかのステータス アイコンが表示されます。

 ディスカバリ中 - プラットフォーム マネージャによってすべてのデータが同期されるまで待機します。

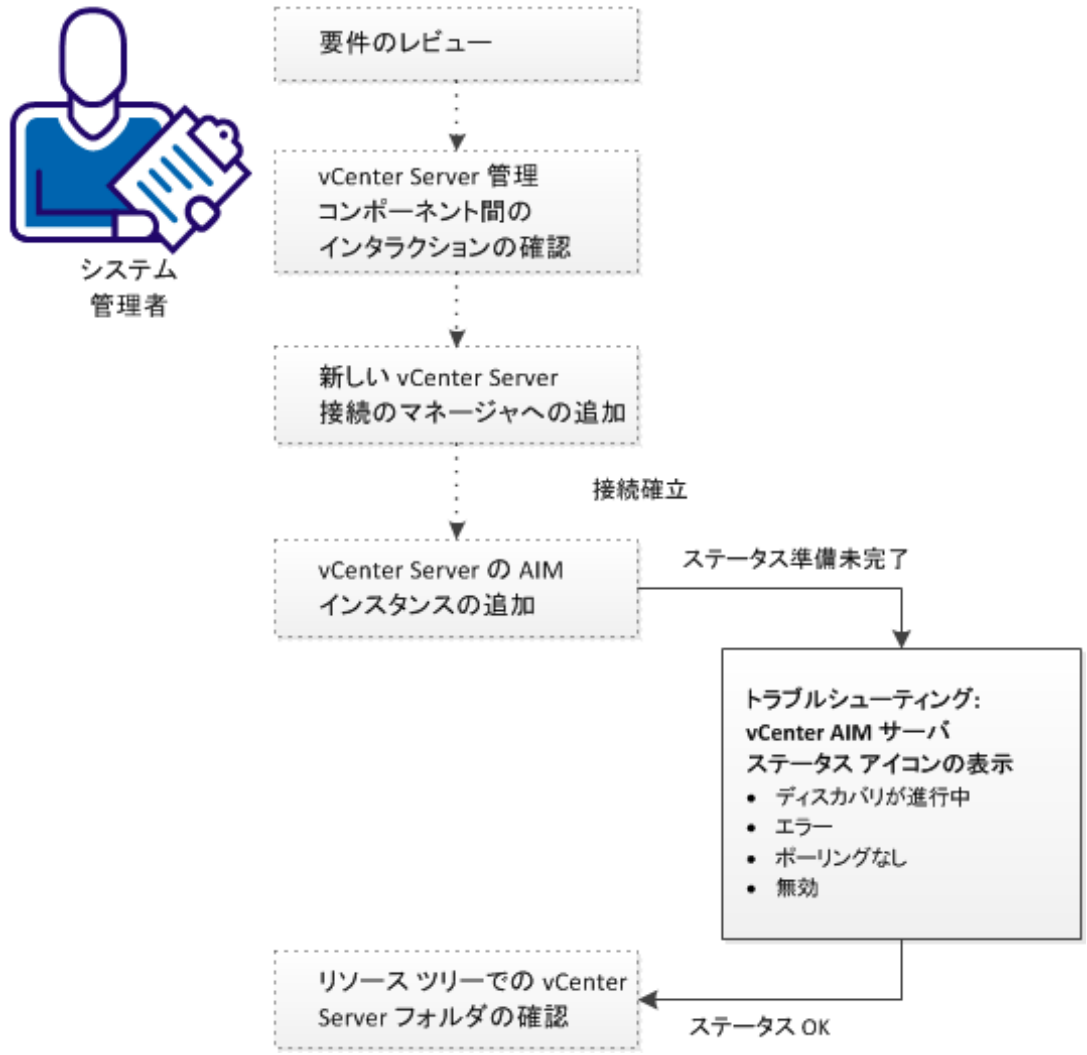
 エラー - AIM に接続できません。 ネットワーク接続を確認してください。

 ポーリングなし - CA Server Automation マネージャはこの AIM インスタンスをポーリングしません。

 無効 - このインスタンスは管理されていません。

以下の図に示すトラブルシューティング情報に従ってください。

vCenter AIM インスタンス接続のトラブルシューティング方法



関連項目:

vCenter AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される (P. 618)
vCenter AIM インスタンスのステータス アイコンに「エラー」が表示される (P. 618)
vCenter AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される (P. 620)
vCenter AIM インスタンスのステータス アイコンに「無効」が表示される (P. 621)

vCenter AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

vSphere 環境のディスカバリ プロセスが完了するまで待機します。ディスカバリにかかる時間は、vSphere 内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを置くと、未処理のディスカバリ要求の数を示すツールヒントが表示されます。 ディスカバリ ジョブが完了すると、CA Server Automation は vCenter Server フォルダをリソース ツリーに追加します。 これで、vSphere とその仮想インフラストラクチャ全体の管理を開始できます。

vCenter AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で vCenter Server に対して vCenter AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。AIM に接続できません。

解決方法:

vCenter AIM への接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- vCenter AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

vCenter AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. vCenter AIM サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   vCenter AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに vCenter AIM サーバを追加します。 手順 3 に進みます。

   vCenter Server が DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと vCenter AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myvCenterAIM
   ```

4. ［vCenter AIM サーバ］ペインの右上角の （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. vCenter AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［vCenter AIM サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によって vCenter AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、このシナリオの要件に従って集めたデータがまだ有効であることを確認してください。

vCenter AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で vCenter Server に対して vCenter AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定の vCenter Server を管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。 サーバ エントリの［編集］をクリックし、優先 AIM を選択します。 優先 AIM が現在の AIM になります。

vCenter AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の vCenter AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この vCenter AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ vCenter AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態である vCenter Server 用に vCenter AIM が設定されている。
- ［vCenter Server］ペインで設定されていない vCenter Server に AIM が接続されている。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落している vCenter Server から CA Server Automation マネージャへの接続を追加します。
- 既存の vCenter Server 接続を編集し、その管理ステータスを「有効」に変更します。

vCenter AIM インスタンスのステータス アイコンに「複数インスタンス」が表示される

症状:

［管理］-［設定］で vCenter Server に対して vCenter Server AIM インスタンスを追加した後、ステータス アイコンに  （複数の AIM がこのインスタンスを管理している）が表示されます。

解決方法:

CA Server Automation マネージャが 1 つの vCenter AIM インスタンスのみを使用して各 vCenter Server を管理していることを確認します。 CA Server Automation マネージャが複数の AIM インスタンスを使用して vCenter Server を管理している場合は、管理上の問題が発生します。 CA Server Automation は関連付けられた vCenter Server のモニタリングを停止します。

どの AIM インスタンスを使用して vCenter Server を管理するかを決定し、［vCenter AIM サーバ］ペインから他のインスタンスを削除してください。

次の手順に従ってください:

1. 削除する AIM インスタンスを選択し、 （削除）をクリックします。

   ［項目の削除］ダイアログ ボックスが表示されます。

2. ［はい］をクリックします。

   マネージャと AIM インスタンスの間で一意の関係が確立するまで、他の複数のインスタンスに対して上記の手順を繰り返します。

リソース ツリーでの vCenter Server フォルダの表示の確認

新しい vCenter Server は、設定およびディスカバリに成功すると、［リソース］-［エクスプローラ］ペインの［VMware vCenter Server］フォルダに示されます。

次の手順に従ってください:

1. ［リソース］-［エクスプローラ］をクリックします。

   リソース ツリーが表示されます。

2. ［VMware vCenter Server］を展開します。

   管理対象の vCenter Server が表示されます。

3. 新しい vCenter Server エントリを展開します。

   管理対象の vSphere インフラストラクチャが表示されます（VMware データセンター、ESX サーバ、リソース プール、VM など）。

CA Server Automation は、追加された vSphere 環境とその仮想インフラストラクチャを管理する準備が整いました。

VM のデバイス管理

デバイス管理には、以下が含まれます。

- vDisk の追加と削除
- vNIC の追加と削除

仮想ディスクの追加または削除

VM に対して仮想ディスクの動的な追加または削除を行うことができます。以下のディスクを追加できます。

- 同じまたは別のデータストアからの新しいディスク
- データストアからの既存ディスク
- 別のデータストアからの既存ディスクの追加

仮想ディスクを追加する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［新しいディスクの追加］を選択します。

   ［新しいディスクの追加］ダイアログ ボックスが表示されます。

4. 必要に応じて新しいディスクの詳細を入力します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   新しいディスクの追加を確認するメッセージが表示されます。

仮想ディスクを削除する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［ディスクの削除］を選択します。

   ［ディスクの削除］ダイアログ ボックスが表示されます。

4. ハード ドライブおよびデータを削除するかどうかを選択します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   ディスクの削除を確認するメッセージが表示されます。

仮想ネットワーク インターフェースの追加または削除

既存の VM に対して仮想ネットワーク インターフェースの動的な追加または削除を行うことができます。

仮想ネットワーク インターフェースを追加する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［新しい仮想ネットワーク インターフェースの追加］を選択します。

   ［新しい仮想ネットワーク インターフェースの追加］ダイアログ ボックスが表示されます。

4. 新しいネットワーク インターフェースの詳細を入力します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   新しいカードの追加を確認するメッセージが表示されます。

仮想ネットワーク インターフェースを削除する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［仮想ネットワーク インターフェースの削除］を選択します。

   ［仮想ネットワーク インターフェースの削除］ダイアログ ボックスが表示されます。

4. 削除する NIC を選択します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   ネットワーク インターフェースの削除を確認するメッセージが表示されます。

仮想マシンに対するフォールト トレランス

VMware vSphere では、高可用性（HA）のために設定されたクラスタに定義された VM 上で *フォールト トレランス（FT）* を有効にすることができます。 フォールト トレランスは、クラスタ内の別の ESX サーバ上でセカンダリ VM を作成します。セカンダリ VM は、ワークロードを実行しているプライマリ VM とのロックステップ モードで作動します。 障害が発生した場合は、セカンダリ VM が、すぐに障害発生時点からワークロードの実行を引き継ぎます。 CA Server Automation は、クラスタ内のプライマリおよびセカンダリ VM を検出して管理します。

VM 管理に関しては、CA Server Automation が、プライマリおよびセカンダリ VM を単一の VM として扱い、フォールト トレランスを有効にして、そのフォールト トレランス プロパティを表示します。 プライマリ VM が左側のペイン（最初のクラス オブジェクト）に表示され、その FT プロパティが右側のペインに表示されます。 セカンダリ VM のプロパティ（2 番目のクラス オブジェクト）は、右側のペインにのみリスト表示されます。 セカンダリ VM 上では、起動、停止、クローンなどの VM 操作を実行できません。

［一般情報］パネルに表示された VM の数は、実行中の非 FT VM とプライマリ FT VM の数に基づいています。 セカンダリ FT VM は、VM の全体の合計数には含まれていません。

CA Server Automation は、環境内のさまざまなレベルで FT VM データを収集します。

フォールトトレランスの要件

VM がフォールト トレラントである場合は、以下の操作が無効である必要があります。

- VM のクローン作成
- インベントリから削除します（登録解除）
- スナップショット
- テンプレートに変換します

仮想マシンのフォールトトレランス プロパティ

CA Server Automation では、各 VM について、以下が表示されます。

フォールトトレランス ステータス

VM フォールト トレランス ステータスを示します。

フォールトトレラントでない

VM がフォールト トレラントではないことを示します。

保護されている

VM がフォールト トレラントであり、保護されていることを示します。

保護されていない (起動中)

フォールト トレランスが起動中であり、VM が保護されていないことを示します。

保護されていない (セカンダリ VM が必要)

フォールト トレランスが有効であるが、セカンダリ VM を必要とすることを示します。

保護されていない (無効)

フォールト トレランスが無効であり、VM が保護されていないことを示します。

保護されていない (VM が実行されていない)

フォールト トレランスが有効であるが、VM が実行されていないことを示します。

セカンダリの場所

セカンダリ ホストの場所を識別します。

ESX ホストのフォールト トレランス属性

ESX ホストのフォールト トレランス属性は以下のとおりです。

フォールト トレランス

ホストでフォールト トレランスが有効になっているかどうかを識別します。

フォールト トレランス バージョン

ホスト上で実行中のフォールト トレランスのバージョンを識別します。

注: 相互の互換性があるのは、フォールト トレランスのバージョンが同じであるホストのみです。

プライマリ VM の合計（AIM で計算）

このホストに設定されたプライマリ VM の総数を示します。

セカンダリ VM の合計（AIM で計算）

このホストに設定されたセカンダリ VM の総数を示します。

電源オン プライマリ VM（AIM で計算）

このホスト上で実行中（電源がオン）のプライマリ VM の総数を示します。

電源オン セカンダリ VM（AIM で計算）

このホスト上で実行中（電源がオン）のセカンダリ VM の総数を示します。

フォールト トレランスのモニタ

VMware vSphere では、高可用性（HA）のために設定されたクラスタに定義された VM 上で *フォールト トレランス (FT)* を有効にすることができます。 フォールト トレランスは、クラスタ内の別の ESX サーバ上でセカンダリ VM を作成します。セカンダリ VM は、ワークロードを実行しているプライマリ VM とのロックステップ モードで作動します。 障害が発生した場合は、セカンダリ VM が、すぐに障害発生時点からワークロードの実行を引き継ぎます。 CA Server Automation は、クラスタ内のプライマリおよびセカンダリ VM を検出して管理します。

フォールト トレランスのプロパティをモニタする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［VMware vCenter Server］フォルダおよび ESX サーバ オブジェクトを展開します。

   VM のリストが表示されます。

4. （オプション）ESX ホストを選択します。

   ［サマリ］タブに以下の FT 属性が表示されます。

   フォールト トレランス

   ホストでフォールト トレランスが有効になっているかどうかを識別します。

   フォールト トレランス バージョン

   ホスト上で実行中のフォールト トレランスのバージョンを識別します。

   注: 相互の互換性があるのは、フォールト トレランスのバージョンが同じであるホストのみです。

   プライマリ VM の合計

   このホストに設定されたプライマリ VM の総数を示します。

   セカンダリ VM の合計

   このホストに設定されたセカンダリ VM の総数を示します。

電源オン プライマリ VM

このホスト上で実行中（電源がオン）のプライマリ VM の総数を示します。

電源オン セカンダリ VM

このホスト上で実行中（電源がオン）のセカンダリ VM の総数を示します。

5. （オプション）VM を選択します。

［サマリ］タブに以下の FT プロパティが表示されます。

フォールト トレランス ステータス

VM フォールト トレランス ステータスを示します。

フォールト トレラントでない

VM がフォールト トレラントではないことを示します。

保護されている

VM がフォールト トレラントであり、保護されていることを示します。

保護されていない (起動中)

フォールト トレランスが起動中であり、VM が保護されていないことを示します。

保護されていない (セカンダリ VM が必要)

フォールト トレランスが有効であるが、セカンダリ VM を必要とすることを示します。

保護されていない (無効)

フォールト トレランスが無効であり、VM が保護されていないことを示します。

保護されていない (VM が実行されていない)

フォールト トレランスが有効であるが、VM が実行されていないことを示します。

セカンダリの場所

セカンダリ ホストの場所を識別します。

フォールト トレランスの管理

VM のフォールト トレランス プロパティは制御することができます。

VM のフォールトトレランス プロパティを管理する方法

1. ［エクスプローラ］ペインで VM を選択します。

   右側に［一般情報］ペインが表示され、VM のフォールト トレランス ステータスが示されます。

2. VM を右クリックし、［管理］を選択して、ドロップダウン メニューからアクションを 1 つ選択します。フォールト トレランスの管理に利用できるアクションを以下に示します。

   - フォールト トレランスをオフ
   - フォールト トレランスの有効化
   - フォールト トレランスの無効化
   - セカンダリ VM のマイグレート

3. 選択したアクションについて、情報を入力し、内容を確認します。

   確認のメッセージが表示されます。

VM のホットプラグ サポート

CA Server Automation は、VM でホットプラグ オプションが有効かどうかを検出します。 CA Server Automation は、VM の電源がオンのときに、ホットプラグ対応 VM の以下の調整をサポートします。

- vCPU の追加
- vRAM の追加

注: ホットプラグ オプションを有効または無効にする方法については、「VMware vSphere 仮想マシン管理ガイド」を参照してください。

vCPU の動的な追加または削除

プロビジョニングされた VM に対して CPU の動的な追加または削除を行うことができます。ホット プラグが VM に有効な場合、実行時に vCPU を動的に追加できます。

CA Server Automation は以下の VM プロパティを検証します。

- ESX ライセンス（ESX レベル）
- サポートされる最大 vCPU 数（ESX レベル）
- ホット プラグが有効（VM レベル）

例

- ESX ライセンスが許可する CPU が 8 個（Enterprise Plus）、最大サポート vCPU が 8 個、およびホット プラグが無効な場合、1、2、4、8 個の CPU を追加できます。
- ESX ライセンスが許可する CPU が 8 個（Enterprise Plus）、最大サポート vCPU が 8 個、およびホット プラグが有効な場合、1、2、3、4、5、6、7、8 個の CPU を追加できます。

vCPU を追加する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［vCPU の追加/削除］を選択します。

   ［vCPU の変更］ダイアログ ボックスが表示されます。

4. 必要に応じて CPU の数を調節します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   変更を確認するメッセージが表示されます。

   注: vCPU を削除するには、仮想マシンをオフにする必要があります。

メモリの動的な追加または削除

プロビジョニングされた VM に対してメモリの動的な追加または削除を行うことができます。 ホット プラグが VM に有効な場合、実行時にメモリを動的に追加できます。

メモリを追加する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックするか、［クイック スタート］タブをクリックし、［メモリの追加/削除］を選択します。

   ［仮想メモリの変更］ダイアログ ボックスが表示されます。

4. 必要に応じてメモリの数を調節します。

   確認のためのメッセージが表示されます。

5. ［OK］をクリックします。

   変更を確認するメッセージが表示されます。

   注: メモリを削除するには、VM をオフにする必要があります。

仮想マシンの論理ボリューム

CA Server Automation は、仮想ディスクの論理ボリュームの管理をサポートします。 たとえば、VM で C: ドライブを管理できます。

リソース割り当て

利用可能なリソース容量では、リソース コンシューマの需要が満たされない場合、仮想マシン、vApp、およびリソース プールのリソースの量をカスタマイズします。

共有、予約、および制限の設定を使用して、仮想マシン、リソース プール、または vApp に提供される CPU およびメモリのリソース量を決定します。

リソース割り当ての共有

共有は、共有相手に対する仮想マシン、リソース プール、または vApp の相対的な優先度または重要性を指定します。 ある仮想マシンに、別の競合仮想マシンの 2 倍のリソース共有がある場合、2 倍のリソースを消費できます。

共有には、通常、自然数を指定します。 デフォルトを使用するか、または各仮想マシンに共有の特定の数値（相対値）を割り当てることができます。

共有の指定は、リソースを共有する仮想マシン、vApp、またはリソース プールに対してのみ影響します。 リソースを共有する仮想マシンまたはリソース プールは階層で同じ親を持ちます。 予約および制限によって制限される相対的な共有の値に従ってリソースを共有します。 仮想マシンに共有を割り当てるときには、オンになっている他の仮想マシンに相対する、その仮想マシンの優先度を常に指定します。

たとえば、競合が発生すると、2000 の共有を持つ仮想マシンには、1000 の共有を持つ仮想マシンよりも多くの CPU 時間が割り当てられます。 共有は他の共有に相対して設定されます。このため、共有の値ではなく相対的な大きさが意味を持ちます。 1000、2000、3000 の共有の値を持つ 3 台の仮想マシンは、1、2、3 の共有の値を持つ 3 台の仮想マシンと同じように動作します。 任意の数スキーム（1、2、3 や 1000、2000、3000 など）を使用できます。 数値間に余裕を残して設定する場合、将来、より容易にリソース プールにリソースを追加できます。

リソースで競合が発生していないとき、共有は仮想マシンの操作に影響しません。 共有の指定は、リソース プールまたは vApp のバランスを保つのに役立ちます。

リソース割り当ての予約

予約は、仮想マシン、リソース プール、または vApp に対する、保証された CPU またはメモリの最小割り当て量を指定します。 vSphere は、予約されていない十分なリソースが仮想マシンで利用できる場合に限り、仮想マシンをオンにすることを許可します。 サーバは、物理サーバの負荷が高いときにも、予約されたリソース量を保証します。 予約はメガヘルツまたはメガバイトの単位で定義します。

たとえば、2 GHz の CPU を利用できるとします。 VM1 に 1000 MHz および VM2 に 1000 MHz の予約を指定します。 現在、仮想マシンはそれぞれ必要な場合に 1 GHz を取得することが保証されています。 ただし、VM1 が 500 MHz しか使用していない場合、VM2 は 1.5 GHz を使用できます。

予約のデフォルトは 0 です。 最低限必要な CPU またはメモリの量を、仮想マシンで常に利用できることを保証するために、予約を指定できます。

リソース割り当ての制限

制限は、仮想マシン、リソース プール、または vApp の CPU またはメモリの最大割り当て量を制限します。 サーバは仮想マシンに予約された量より多く割り当てることができますが、制限を超えて割り当てることはできません。 システム上で利用されていない場合でも、制限を超えて、CPU またはメモリを割り当てることはできません。 制限はメガヘルツまたはメガバイトの単位で定義します。

デフォルトでは、CPU とメモリの制限は、無制限に設定されています。 メモリ制限が無制限に設定されていると、vSphere は、仮想マシンを作成するときに、有効にメモリの量を決定します。 通常、制限を指定する必要はありません。

リソース割り当てのベスト プラクティス

ESX/ESXi 環境に適したリソース割り当て設定（共有、予約、および制限）を指定します。

以下のガイドラインは、仮想インフラストラクチャの最適なパフォーマンスを実現するうえで役立ちます。

- 利用可能なリソースの総数を頻繁に変更する可能性がある場合、共有を使用して、複数の仮想マシンにわたってリソースを割り当てます。共有を使用しているときに、ホストをアップグレードする場合、共有の数値は変更されません。 たとえば、各共有がより多くのメモリまたは CPU を表すようになったとしても、仮想マシンはそれぞれ同じ優先度のままになります。
- 使用したい量ではなく、許容できる*最小限の* CPU またはメモリの量を指定するために、予約を使用します。 ホストは、仮想マシンの共有の数、予測される需要、および制限に基づいて、利用可能な追加のリソースを割り当てます。 仮想マシンの追加または削除など、環境を変更しても、予約によって指定されたリソースの量は変更されません。
- 仮想マシンの予約を指定するときに、すべてのリソースをコミットしないでください。 予約する量がすべてのシステム容量の限界に近づくと、予約やリソース プールの階層を変更することが困難になるため、予約しない部分が適切に残るように計画してください。
- 詳細については、www.vmware.com にある vSphere 関連のドキュメントを参照してください。

VM の CPU およびメモリの割り当ての編集

仮想マシンに割り当てられている CPU 数とメモリ共有を編集して、割り当てられているリソースを調整できます。 リソースを追加する場合、適切な量の割り当てられていないメモリと CPU 共有が利用できる必要があります。 メモリまたは CPU 共有で許可される最小値および最大値が存在する場合は、リソース割り当ての変更は、これらの制限内で行う必要があります。

特定の VM リソース割り当てアクションを使用して、ポリシーの作成およびスケジュールを行うこともできます。

VM の CPU およびメモリの割り当てを編集する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［設定］-［リソース割り当て］を選択します。

   ［リソース割り当て］セクションが表示されます。

3. 仮想マシンに割り当てられている CPU の数とメモリ共有を調節し、編集した各値の［保存］をクリックします。

   確認メッセージが表示されます。

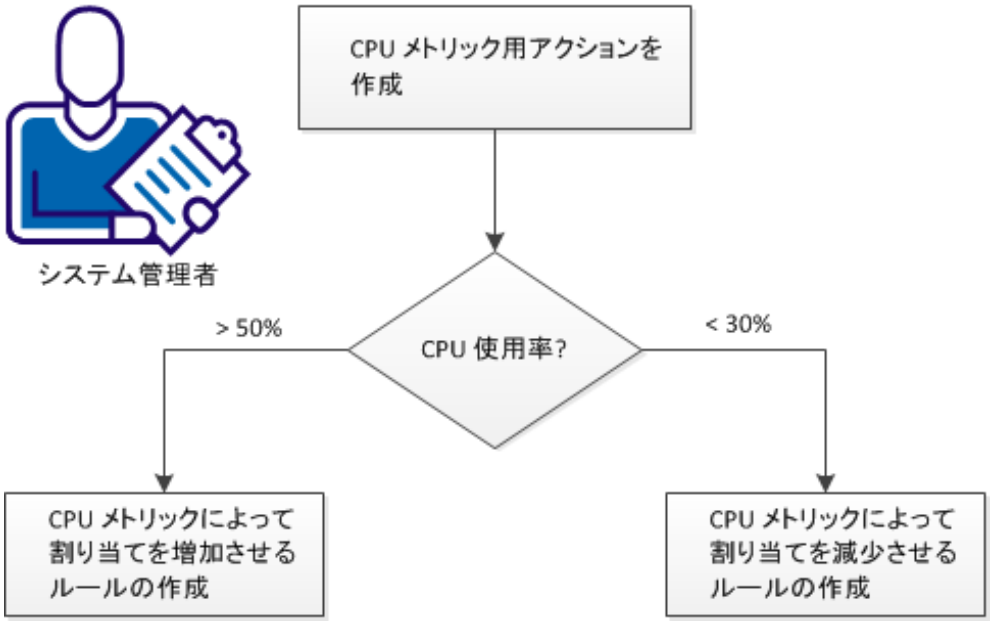
ポリシー アクションを使ってパフォーマンスの問題を特定する方法

このシナリオでは、システム管理者がパフォーマンスの問題を特定し、動的に対処する方法について説明します。 この情報は、管理対象 vCenter 環境のリソース共有の割り当てを最適化するシステム管理者を対象にしています。

ポリシー アクションによって、VM リソースが特定され、CPU 割り当てが動的に調整されます。 *共有*は、複数の VM 間でリソース競合が発生した場合に、どの VM がリソースを取得するかを決定します。 共有を使用することによって、CPU リソースの動的な割り当てが可能になります。 各 VM には、指定された数の共有が割り当てられます。 割り当ては、ESX サーバホスト上の CPU リソースの現在の使用率に基づいて、動的に変化します。

VM の CPU 使用率が 50 パーセントを超える場合、CPU 共有の割り当ては動的に増加されます。 CPU 使用率が 30 パーセント未満の場合、CPU 共有の割り当ては動的に減少されます。 ポリシー コンポーネントは、問題のある仮想マシンを特定するだけでなく、ビジネスの継続性を維持する動的アクションを実行できるようにします。 ポリシー アクションは、リソースを必要とする仮想マシンにリソースを割り当て、リソースの必要がなくなったときに割り当てを解除します。

パフォーマンスの問題を特定するためのポリシー アクションの使用方法



ポリシー アクションを使ってパフォーマンスの問題を特定して対処するには、以下の手順に従います。

1. CPU メトリックのアクションを作成します。 (P. 641)
2. CPU 使用率が 50 パーセントを超える場合は、CPU メトリックによって割り当てを増加させるルールを作成 (P. 642) します。
3. CPU 使用率が 30 パーセント未満の場合は、CPU メトリックによって割り当てを減少させるルールを作成 (P. 642) します。

CPU メトリックのアクションの作成

システム管理を自動化するためのポリシーの作成に使用できるルールおよびアクションの作成は、ポリシーによって提供されます。デフォルト ライブラリに含まれないアクションに対してはカスタム アクションを作成できます。

次の手順に従ってください:

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［ポリシー］をクリックし、次に、［アクション］をクリックします。

   ［アクション］ページが表示されます。

4. アクションを追加するには、右上のバーの［+］をクリックします。
5. アクションの名前を入力します。
6. ［カテゴリ］ドロップダウン リストから［リソース設定］を選択します。
7. ［タイプ］ドロップダウン リストから［共有の設定］を選択します。
8. 任意の VC サーバ上の任意の VM にこのアクションを適用するには、［VC サーバ］ フィールドでエントリを「%VCServer%」のままにします。
9. ［VC データ センター］フィールドで、エントリを「%DATACENTER%」のままにします。
10. ［ターゲット VM マシン］フィールドで、エントリを「%VMNAME%」のままにします。
11. ［操作］ドロップダウン リストから［CPU の設定］を選択し、［値］に「10000」を入力します。

    数は任意です。また、共有値は標準値に設定されます。

    注: 使用する値を大きくまたは小さくすると、それに応じて共有の割り当ても増減します。

12. 変更の承認が必要な場合は、［ヘルプ デスク承認］を有効にします。

    アクションが作成されると、イベント コンソールにメッセージが表示されます。

CAAP4521 ポリシー： アクション <アクション名> が作成されました。

CPU メトリックによって割り当てを増加させるルールの作成

CPU メトリックによって CPU 割り当てを増加させるルールを作成すると、使用率がしきい値を超えたときに動的なリソース割り当てが実行されます。

次の手順に従ってください:

1. ［リソース］タブをクリックし、［ポリシー］-［ルール］をクリックします。
2. ルールを追加するには、右上のバーの［+］をクリックします。
3. ルールの名前を入力し、［次へ］をクリックします。
4. ルールの［アクションの選択］リストからアクションを選択し、［次へ］をクリックします。
5. CPU 使用率が 50 パーセントを超えた場合に VM の CPU 共有を増加させる、メトリックベースのルールを入力します。

CPU メトリックによって割り当てを減少させるルールの作成

CPU メトリックによって割り当てを減少させるルールを作成します。 CPU 使用率が 30 パーセント未満の場合、CPU 共有の割り当ては動的に減少されます。

次の手順に従ってください:

1. ［リソース］タブをクリックし、［ポリシー］-［ルール］をクリックします。
2. ルールを追加するには、右上のバーの［+］をクリックします。
3. ルールの名前を入力し、［次へ］をクリックします。
4. ルールの［アクションの選択］リストからアクションを選択し、［次へ］をクリックします。
5. CPU 使用率が 30 パーセント未満の場合に VM の CPU 共有を減少させる、メトリックベースのルールを入力します。

vApp のサポート

vApp は、VM の集合を 1 つの単位として扱う特殊なリソース プールです。vApp は Open Virtualization Format を使用します。 Open Virtualization Format （OVF）は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービス レベルを規定し、カプセル化するための標準です。 CA Server Automation は vApp 上で操作を実行できます。vApp 上での操作は vApp 内のすべての VM にプロパゲートされます。

任意の vApp を小さくパーティション分割することで、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。VM、リソース プール、または vApps のようなリソースを既存の vApp に追加できます。 また、vApp を階層的に構成して、ネストすることもできます。

vApp は、ホストおよびクラスタ レベルに表示されます。

CA Server Automation vApp レベルで以下の管理操作をサポートします。

- 検出
  - サーバ
  - ネットワーク
  - vCenter Server
- サービスのキャプチャ
- リソースの追加
- vApp のクローン作成
- vApp の電源オン
- vApp の電源オフ
- vApp の中断
- VMware vCenter からの削除
- VMware vCenter からの登録解除
- 並べ替え順序の編集

CA Server Automation は、vApp に対する以下のプロビジョニング操作をサポートします。

- VMware VM のプロビジョニング
- VMware vApp のプロビジョニング

VMware vApp のプロビジョニング

vApp は、ESX ホストまたはクラスタ レベルに、または既存のリソース プールまたは vApp の一部として直接作成できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインのホストまたはクラスタ レベルから、ESX ホストまたはクラスタを右クリックします。

   ポップアップ メニューが表示されます。

2. ［プロビジョニング］-［VMware vApp のプロビジョニング］を選択します。

   ［vApp の新規作成］ダイアログ ボックスが表示されます。

3. 以下のフィールドで値を指定して、［OK］をクリックします。

   名前

   vApp を識別します。

   CPU 共有

   親ホスト、リソース プール、または vApp の合計 CPU リソースに関して、この vApp 用の CPU 共有を指定します。 親が同じ vApp は、予約と制限によって制約される相対的な共有の値に従ってリソースを共有します。 適切な相対値を表す共有の数を指定します。

   たとえば、ホスト上に vApp1 と vApp2 があり、各々に 1000 CPU 共有が割り当てられていると仮定します。相対値が等しいので、vApp はそれぞれ、親ホストの 50 パーセントの CPU 時間を使用できます。vApp1 に 2000 CPU 共有、vApp2 に 1000 CPU 共有が割り当てられている場合、相対値が等しくありません。共有の総数は 3000 で、1000 の共有は 33.3 パーセントを表し、2000 の共有は 66.6 パーセントを表します。 したがって、vApp2 は CPU の 66.6 パーセントを、vApp2 は 33.3 パーセントを使用できます。

   CPU 予約

   この vApp に保証される CPU 割り当てを指定します。

   CPU 無制限

   ［CPU 制限］の設定を無効にします。 実際の制限は、利用可能な物理リソースに設定されるようになります。

   CPU 制限

この vApp に割り当てる CPU の上限を指定します。通常、デフォルトを受け入れることができます。

メモリ共有

親リソース プールまたは vApp のメモリ合計リソースに関して、この vApp 用のメモリ共有を指定します。 親が同じ vApp は、予約と制限によって制約される相対的な共有の値に従ってリソースを共有します。 適切な相対値を表す共有の数を指定します。

たとえば、ホスト上に vApp1 と vApp2 があり、各々に 1000 メモリ共有が割り当てられていると仮定します。 相対値が等しいので、vApp はそれぞれ、親ホストの 50 パーセントのメモリを使用できます。 vApp1 に 2000 メモリ共有、vApp2 に 1000 メモリ共有が割り当てられている場合、相対値が等しくありません。 共有の総数は 3000 で、1000 の共有は 33.3 パーセントを表し、2000 の共有は 66.6 パーセントを表します。 したがって、vApp2 はメモリの 66.6 パーセントを、vApp2 は 33.3 パーセントを使用できます。

メモリ予約

この vApp に保証されるメモリ割り当てを指定します。

メモリ無制限

［メモリ制限］の設定を無効にします。 実際の制限は、利用可能な物理リソースに設定されるようになります。

メモリ制限

この vApp に割り当てるメモリの上限を指定します。通常、デフォルトを受け入れることができます。

新しい vApp が［エクスプローラ］ペインに表示されます。

vApp のクローン作成

仮想マシンのクローンを作成する方法に類似した方法で vApp のクローンを作成できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインのホストまたはクラスタ レベルで、クローンの作成元となる vApp を選択します。
2. vApp を右クリックします。

   ポップアップ メニューが表示されます。
3. ［管理］-［vApp のクローン作成］を選択します。

   ［vApp のクローン作成］ダイアログ ボックスが表示されます。
4. 以下のフィールドで値を指定して、［OK］をクリックします。

   名前

   新規にクローン作成される vApp を識別します。

   場所

   適切な場所を指定します。 ポップアップ メニュー上に表示されるオブジェクトを展開し、場所を選択します。

   データストア

   ドロップダウン メニューからの適切なデータストアを指定します。

   新規にクローン作成された vApp が、［エクスプローラ］ペインに表示されます。

その他の vApp 操作

CA Server Automation は、vApp に関する以下の操作をサポートします。

- 電源オン
- 電源オフ
- 中断
- VMware vCenter からの削除
- VMware vCenter からの登録解除

次の手順に従ってください:

1. ［エクスプローラ］ペインでホストまたはクラスタ レベルから、適切な vApp を選択します。
2. vApp を右クリックします。

   ポップアップ メニューが表示されます。
3. ［管理］を選択し、実行する操作をクリックします。

   確認ダイアログ ボックスが開きます。
4. ［OK］をクリックします。

   CA Server Automation によって、選択された操作が実行されます。

イベントによる vApp のモニタリング

以下のイベントで vApp をモニタできます。

- vApp の追加：

  vApp *MyvApp* が親リソース プールのリソースに追加されました。
  vSphere *vcserver.mycomp.com*
- vApp の削除：

  vApp *MyvApp* が親リソース プールのリソースから削除されました。
  vSphere, vcserver.mycomp.com

以下のトラップを使用できます。

- ResPoolvAppAddedTrap： vApp をリソース プールまたは vApp に追加します。
- ResPoolvAppRemovedTrap： vApp をリソース プールまたは vApp から削除します。
- ResPoolvAppVCConfigChangeTrap： vApp 内の vApp エンティティの設定データが変更されました。
- VMAddedTovAppTrap： VM が vApp に追加されました。
- VMRemovedFromvAppTrap： VM が vApp から削除されました。
- VMvAppVCConfigChangeTrap： vApp 内の VM エンティティの設定データが変更されました。

イベントで vApps をモニタする方法

1. ［ダッシュボード］タブをクリックし、［イベント］パネルまでスクロールして、［テーブル フィルタを表示］アイコンをクリックします。

   ［フィルタ］パネルが表示されます。

2. モニタする vApp イベント用の適切なフィルタを指定して、［適用］をクリックします。

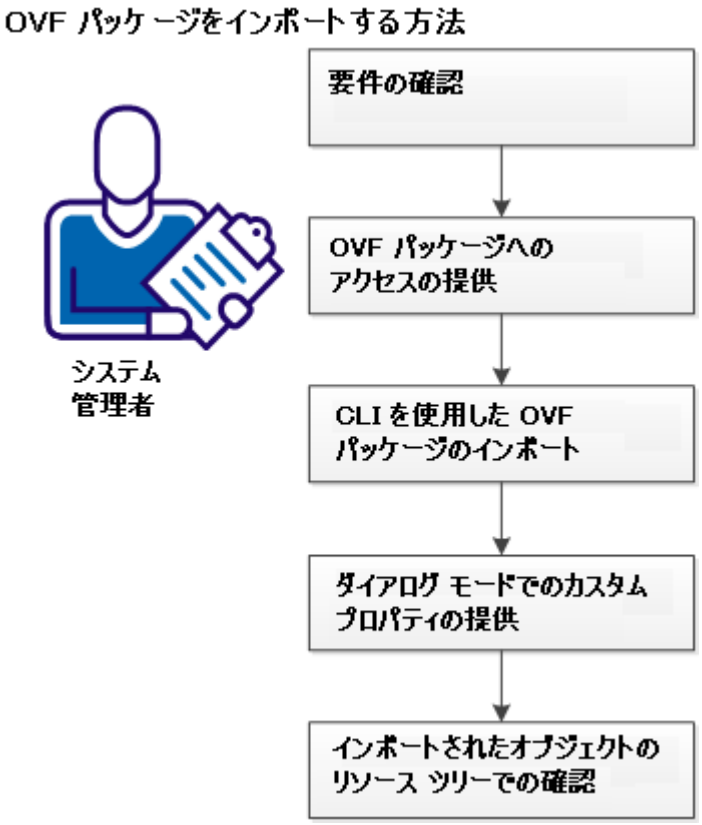
   ［イベント］パネルに、フィルタされたイベントのリストが表示されます。

CA Server Automation を使用した OVF パッケージのインポート方法

このシナリオは、CA Server Automation を使用した OVF パッケージのインポートに関する情報を提供します。 この情報は、システム管理者が OVF パッケージをインポートし、これらの OVF パッケージで指定される vApps を展開するのを支援するために提供されます。

Open Virtualization Format （OVF）は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービス レベルを規定し、カプセル化するための標準です。

以下の図は、OVF パッケージをインポートする手順を説明します。



以下の手順に従います。

要件の確認 (P. 651)
OVF パッケージへのアクセスの提供 (P. 651)
dpmovf import コマンド -- OVF パッケージのインポート (P. 652)
ダイアログ モードでのカスタム プロパティの提供 (P. 654)
インポートされたオブジェクトのリソース ツリーでの確認 (P. 655)

要件の確認

また、以下の要件も確認してください。

- CA Server Automation ユーザ インターフェースにアクセスできる。
- ターゲット vSphere 環境とその vCenter Server が正しく実行されることを確認済みである。
- 管理者として CMD ウィンドウを開始できること、および、dpmovf.exe ファイルがコンピュータにインストールされていることを確認済みである。

関連項目:

vCenter Server 管理コンポーネント間のインタラクションの確認 (P. 605)
新しい vCenter Server 接続のマネージャへの追加 (P. 609)
vCenter Server の AIM インスタンスの追加 (P. 614)
リソース ツリーでの vCenter Server フォルダの表示の確認 (P. 623)

OVF パッケージへのアクセスの提供

CA Server Automation から OVF パッケージにアクセスできるようにするには、以下のいずれかのタスクを実行します。

- マネージャ上で、OVF パッケージがある場所にドライブをマップします。
- OVF パッケージをマネージャ上にコピーします。

dpmovf import コマンド -- OVF パッケージのインポート

dpmovf import コマンドは OVF パッケージをインポートし、VM または vApps を作成します。 -properties 属性を使用すると、カスタム プロパティ ファイルを提供できます。 カスタム プロパティ ファイルを使用すると、OVF パッケージで定義されているカスタム プロパティを指定できます。 カスタム プロパティ ファイルには、プロパティ キーおよび対応するプロパティ値のリストが含まれます。

注: カスタム プロパティ ファイルがない場合は、properties.txt ファイルが作業ディレクトリに作成されます。 デフォルト ディレクトリは CA¥*ProductName*¥bin です。

このコマンドの形式は、以下のとおりです。

```
dpmovf import
-host vCenter_server
-user user_name
-password user_password
-name VM_VApp_name
-path OVF_file_path
-datacenter data_center
-datastore data_store
-resourcepool resource_pool
[-locale iso639value]
[-properties properties_file]
```

-host *vCenter_server*

vCenter Server ホストの名前を指定します。

-user *user_name*

ログインするユーザ名を指定します。

-password *user_passsword*

ログインするユーザのパスワードを指定します。

-name *VM_VApp_name*

VM または vApp の名前を指定します。

-path *OVF_file_path*

OVF ファイル パスを指定します。

-datacenter *data_center*

データ センター名を指定します。

-datastore *data_store*

データ ストアを指定します。

-resourcepool *resource_pool*

リソース プールを指定します。

-locale *iso639value*

（オプション）デフォルトの英語出力より優先させるロケールを、ISO 639_3166 の組み合わせ（たとえばフランス語の場合は fr_FR）で指定します。コマンド プロンプトのロケールを使用する場合は「native」を指定します。

-properties *properties_file*

（オプション）カスタム プロパティ ファイル パスを指定します。

例: CA Server Automation を使用した、CA プラットフォーム用の OVF ファイルのインポート

この例では、CA プラットフォーム OVF パッケージをインポートし、vApp および VM を作成します。 CA プラットフォーム OVF ファイルは *CA Platform_v1_0_0_92c.ovf*、ファイルの場所は *D:¥OVF¥CA_Platform* です。ユーザ名は *user123* です。vApp の以下の属性が指定されています : *my_datastore*、*my_datacenter*、および *my_resourcepool*。 カスタム プロパティは *custom_properties.txt* ファイルで提供されます。

```
dpmovf import -path "D:¥OVF¥CA_Platform¥CA Platform_v1_0_0_92c.ovf" -name
"My_CA_Platform" -host my_host.company.com -user user123 -locale en-US -datastore
"my_datastore" -datacenter "my_datacenter" -resourcepool "my_resourcepool"
-properties "custom_properties.txt"
```

ダイアログ モードでのカスタム プロパティの提供

OVF ファイルにカスタム プロパティが含まれる場合、ダイアログ モードでカスタム プロパティを編集できます。カスタム プロパティ ファイルを指定すると、ダイアログ モードでカスタム プロパティ ファイルを上書きできます。

注: カスタム プロパティ ファイルがない場合は、properties.txt ファイルが作業ディレクトリに作成されます。 デフォルト ディレクトリは CA¥*ProductName*¥bin です。

次の手順に従ってください:

1. 編集するカスタム プロパティのカスタム プロパティ番号を入力します。
2. カスタム プロパティの値を入力します。
3. 提供または編集するすべてのカスタム プロパティに対して、手順 1 ～ 2 を繰り返します。
4. 以下のいずれかのオプションを入力します。

   r

   プロパティ ファイルを読み取ります。

   w

   プロパティ ファイル内のプロパティすべてを上書きします。

   c

   インポート コマンドを実行します。

   注: 提供されたプロパティの一部は、条件が満たされているか、あるいは提供された値が有効かどうかを確認するために検証されます。

CA Server Automation は vCenter に OVF を展開し、OVF ファイルで指定される vApps および VM が参照可能です。

インポートされたオブジェクトのリソース ツリーでの確認

vApps と VM をインポートした後、追加されたインスタンスは［VMware vCenter Server］フォルダのリソース エクスプローラ ペインに一覧表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. ［VMware vCenter Server］を展開します。

   インポートされたオブジェクトが表示されます。

OVF ファイルで指定された vApps が vCenter 環境にインポートされています。CA Server Automation では、vSphere 環境に追加された vApps および VM を管理する準備ができています。

クラスタ内の vCenter Server

vCenter Server がクラスタ内に存在する場合、vCenter Server AIM はこのクラスタの外部で実行される必要があります。 クラスタ ホストを指すように vCenter Server AIM を設定します。 vCenter Server が正常に起動すると、AIM がフェールオーバを検出でき、その内部キャッシュに再度読み込みを行います。

vNetwork パネル内の仮想標準スイッチおよび分散仮想スイッチ

vNetwork パネルは、VMware データセンター レベルおよび ESX ホスト レベルのユーザ インターフェースで利用できます。VMware データセンター レベルでは、vNetwork は、そのデータセンターの分散仮想スイッチを示します。 ESX ホスト レベルでは、vNetwork は、関連付けられた分散仮想スイッチおよび仮想標準スイッチを示します。

関連項目:

vNetwork 標準スイッチ（vSwitch） (P. 656)
分散仮想スイッチ (P. 656)
プロパティ (P. 658)
アクション (P. 662)
イベントによる分散仮想スイッチのモニタリング (P. 664)

vNetwork 標準スイッチ（vSwitch）

CA Server Automation は、抽出されたネットワーク デバイスである標準 vSwitch のポリシーおよびプロパティをモニタします。 vSwitch で、VM 間のトラフィックを内部的にルーティングして、外部ネットワークにリンクできます。 vSwitch では、複数のネットワーク アダプタの帯域幅を組み合わせて、通信トラフィックを分散します。vSwitch は物理 NIC フェールオーバを処理することができます。

vSwitch で、物理イーサネット スイッチがモデル化されます。 デフォルトの vSwitch 用論理ポート番号は 120 です。 VM の 1 つのネットワーク アダプタを各ポートに接続できます。 vSwitch と関連付けられた各アップリンク アダプタは、1 つのポートを使用します。vSwitch 上の各論理ポートは、単一のポート グループのメンバです。 各 vSwitch には、1 つ以上のポート グループを割り当てることもできます。 2 つ以上の VM を同じ vSwitch に接続すると、それらの間のネットワーク トラフィックはローカルにルーティングされます。アップリンク アダプタが vSwitch に付けられている場合は、アダプタが接続された外部ネットワークに各 VM がアクセスできます。

仮想標準スイッチ オブジェクトを展開すると、関連付けられたポートおよびポート グループを参照できます。

- ポート グループには、そのポート グループを使用する関連 VM が含まれます。

分散仮想スイッチ

CA Server Automation は、vSphere 環境で、以下の分散仮想スイッチをサポートします。

- VMware vNetwork 分散スイッチ（vDS、vSphere コンポーネント）
- Cisco Nexus 1000V スイッチ（vSphere と統合）

CA Server Automation は、vSphere 環境の分散仮想スイッチを検出し、イベントを介して、そのポリシーとプロパティをモニタします。 CA Server Automation VM プロビジョニングでは、vNetwork 分散スイッチおよび Cisco Nexus 1000V スイッチがサポートされます。

分散仮想スイッチは、それに関連付けられているすべてのホストにわたる 1 つの仮想スイッチとして動作します。 分散仮想スイッチは、これらのホストに対して同じスイッチ（同じ名前、同じネットワーク ポリシー）とポート グループを表します。 これらのプロパティは複数のホスト間でマイグレートされるため、VM は一貫したネットワーク設定を維持できます。

各分散仮想スイッチは、vNetwork Standard Switch と同様、VM が使用できるネットワーク ハブです。分散仮想スイッチは、VM 間のトラフィックを内部的に転送したり、物理 NIC（アップリンク アダプタ）に接続することで外部ネットワークにリンクしたりすることができます。

分散仮想ポート グループ（dvPort グループ）は、分散仮想スイッチと関連付けられたポート グループであり、各メンバ ポートのポート設定オプションを指定します。dvPort グループは、分散仮想スイッチを介してネットワークに接続する方法を定義します。

分散仮想アップリンク（dvUpLinks）は、ESX または ESXi のホスト上で、物理 NIC （vmnics）のある程度の抽象化を提供します。 各物理 NIC は 1 つの dvUplink にマップされます。dvPort グループから dvUplink へのマッピングは、分散仮想スイッチによるネットワークへのアクセスに、VM が ESX または ESXi ホスト上のどの物理 NIC を使用するかを定義します。

Cisco Nexus 1000V スイッチは、仮想イーサネット モジュール（VEM）および仮想スーパーバイザ モジュール（VSM）から構成されます。 Cisco Nexus 1000V スイッチに関連付けられた各 ESX または ESXi ホストでは、VEM が VMware vSwitch の代わりにハイパーバイザ カーネル内でモジュールとして実行されます。 VSM は、1 つの論理的なスイッチとして複数の VEM を制御し、ESX または ESXi のホスト上の VM 内で動作します。

詳細については、http://pubs.vmware.com にある VMware vNetwork 分散スイッチのマニュアルまたは http://www.cisco.com/go/1000vdocs にある Cisco Nexus 1000V スイッチのマニュアルを参照してください。

注: Cisco Nexus 1000V スイッチを使用する場合は、VSM VM が、CA Server Automation ユーザ インターフェースに特殊な VM として表示されません。VSM VM に適用するルールおよびアクションが Cisco Nexus 1000V スイッチに影響しないことを確認してください。

分散仮想スイッチ オブジェクトを展開すると、関連付けられたポート グループおよびアップリンク グループを参照できます。

- ポート グループには、そのポート グループを使用する関連付けられた VM が含まれます。
- ［アップリンク グループ］には、物理アップリンク アダプタがリスト表示されます。

プロパティ

［プロパティ］ペインには、仮想標準スイッチまたは分散仮想スイッチのプロパティが表示されます。

ポリシー

以下のリストに、仮想標準スイッチまたは分散仮想スイッチ用のデフォルト ポリシー（有効化されているポリシー）を示します。

プロミスキャス モード

ポート上ですべてのトラフィックを見られるかどうかを示します。

MAC アドレス変更

MAC （Media Access Control）アドレスを変更できるかどうかを示します。

偽造された送信

MAC アドレスが仮想ネットワーク アダプタの MAC アドレスと異なるかどうかを示します。

トラフィック シェイピング

ポート上でトラフィック シェイパが有効かどうかを示します。

平均帯域幅

ポートでシェイピングが有効な場合、平均帯域幅をビット/秒で示します。

ピーク帯域幅

ポートでトラフィック シェイピングが有効な場合、バースト時のピーク帯域幅をビット/秒で示します。

バースト サイズ

ポートでシェイピングが有効な場合、許可される最大バースト サイズをバイト単位で示します。

ネットワーク障害検出

ネットワーク障害検出が有効かどうかを示します。 有効な値は以下のとおりです。

- false (1)
- true (2)

スイッチの通知

リンクが失敗した場合に、物理スイッチに通知するかどうかを指定します。

フォールバック

フォールバックが有効かどうかを示します。

ポリシー受信フレーム

受信フレームにチーミング ポリシーが適用されるかどうかを示します。

アクティブなアダプタ

負荷分散に使用されるアクティブなネットワーク アダプタのリストを表示します。

スタンバイ アダプタ

フェールオーバに使用されるスタンバイ ネットワーク アダプタのリストを表示します。

vSwitch のプロパティ

以下の vSwitch プロパティから、ポート番号の特性がわかります。

ポート数

分散仮想スイッチまたは仮想標準スイッチの現在のポート数を示します。

ポートの最大数

分散仮想スイッチのポートの最大数を示します。

注: 分散仮想スイッチの場合、この情報は VMware データセンター レベルでのみ利用できます。 ESX ホスト レベルでは利用できません。

ポート グループのプロパティ

以下のポート グループ プロパティが VLAN ID を示します。

VLAN ID

ポート グループの VLAN ID を示します。

ポートのプロパティ

以下のプロパティがポート特性を指定します。

VLAN ID

ポートの VLAN ID を示します。

タイプ

ポートのタイプ (VMkernel ポート、サービス ポートなど) を示します。

ネットワークのプロパティ

以下のプロパティが、仮想スイッチのネットワーク特性を指定します。

- IPv4 アドレス
- IPv6 アドレス
- MAC アドレス

仮想マシン数

以下の値は、ポート グループと関連付けられた VM に関する統計情報を提供します。

- 電源オン
- 電源オフ
- 中断
- 不明

アクション

仮想標準スイッチと分散仮想スイッチの管理に適切なアクションを使用します。 以下のアクションを使用できます。

- vSwitch の追加
- vSwitch の更新
- vSwitch の削除
- ポート グループの追加
- ポート グループの更新
- ポート グループの削除
- ポート グループの名前変更

これらのアクションを適用しようとすると、ダイアログ ボックスが表示され、必要な情報の入力を求められます。表示される可能性のあるフィールドは、以下のとおりです。

スイッチ名

操作を実行するスイッチの名前を指定します。

NIC

（オプション）ESX ホスト メンバと関連付けられた物理 NIC のリストを指定します。

アップリンク ポート名

（オプション）使用するアップリンク ポート名のリストを指定します。

ポートの最大数

（オプション）分散仮想スイッチのポートの最大数を指定します。

バインド タイプ

（オプション）ポート グループのバインド タイプを指定します。 有効な値は以下のとおりです。

earlyBinding

VM がポートグループにバインドする際にポートを割り当てます。このバインディング タイプは、接続性の常時確保に有効ですが、ポートが永続的に予約されます。 デフォルトはこのバインディング タイプです。

lateBinding

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。 このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。 LateBinding は vCenter で設定できます。

ephemeral

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。 このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。 ephemeral バインディングは、ESX ホストと vCenter で設定できます。

ポート数

（オプション）ポート グループのポートの数を指定します。

ポート グループ名

ポート グループ名を指定します。

新しいポートグループ名

新しいポート グループ名を指定します。

LAN ID *vlanid*

（オプション）仮想ポート グループの操作に使用する整数値（*vlanid*）を指定します。

イベントによる分散仮想スイッチのモニタリング

以下のイベントで分散仮想スイッチをモニタできます。

- スイッチの追加：

  分散仮想スイッチ VM-dvSwitch がデータセンター MyDC に追加されました。 vSphere： vcserver.mycomp.com

- スイッチの削除：

  分散仮想スイッチ VM-dvSwitch がデータセンター MyDC から削除されました。 vSphere： vcserver.mycomp.com

- ポート グループの追加：

  分散仮想ポート グループ VM dvPortGroup が仮想分散スイッチ VM-dvSwitch に追加されました。 データセンター： MyDC、vSphere: vcserver.mycomp.com

- ポート グループの削除：

  分散仮想ポート グループ VM dvPortGroup が仮想分散スイッチ VM-dvSwitch から削除されました。 データセンター： MyDC、vSphere: vcserver.mycomp.com

- アップリンクの追加：

  分散仮想アップリンク VM DVUplink が分散仮想スイッチ VM-dvSwitch に追加されました。 データセンター： MyDC、vSphere: vcserver.mycomp.com

- アップリンクの削除：

  分散仮想アップリンク VM DVUplink が分散仮想スイッチ VM-dvSwitch から削除されました。 データセンター： MyDC、vSphere: vcserver.mycomp.com

イベントで分散仮想スイッチをモニタする方法

1. ［ダッシュボード］タブをクリックし、［イベント］パネルまでスクロールして、［テーブル フィルタを表示］アイコンをクリックします。

   ［フィルタ］パネルが表示されます。

2. モニタする分散仮想スイッチ イベント用の適切なフィルタを指定して、［適用］をクリックします。

   ［イベント］パネルに、フィルタされたイベントのリストが表示されます。

VMware vCenter のプロビジョニングと一般的なユース ケース

このセクションでは、仮想リソースをプロビジョニングする方法と一般的なユース ケースについて説明します。

仮想マシン（vCenter Server）の追加

VM を追加する場合は、以下の 2 つの方法のいずれかを使用できます。

- 事前定義済みテンプレートのクローンを作成する
- 既存の VM およびカスタマイズ仕様のクローンを作成する （カスタマイズ仕様でゲスト OS の特性を定義する）

VM プロビジョニングは標準スイッチと分散仮想スイッチをサポートします。 分散仮想スイッチに接続している VM にプロビジョニングする場合、ユーザ インターフェース内の適切な検出済み dvPort グループを指定できます。 dvPort グループは、分散仮想スイッチを介してネットワークに接続が行われる方法を定義します。

VM を追加する方法

1. ［エクスプローラ］ペインで［VMware vCenter サーバ］を右クリックし、［プロビジョニング］-［VMware VM のプロビジョニング］を選択します。

   ［VMware vCenter プロビジョニング］ダイアログ ボックスが表示されます。

2. ドロップダウン リストからオプションを選択して設定を指定します。

   注: クローン作成用にリスト表示される仮想マシンは、CA Server Automation によってモニタされている仮想マシンに制限されます。 VM へのアクセスはセキュリティを確保するために制限されます。 利用できないシステムのクローンを作成する場合は、他のシステムと同じようにそのシステムを検出し、それをドロップダウン リストで利用可能にします。

3. 使用するユーザ名、パスワードおよびホスト名を入力します。 入力しない場合、仕様で指定された名前がデフォルトで使用されます。

   注: Windows および Linux のユーザ名およびパスワードが、カスタマイズ仕様ファイルで定義されたものと一致する必要があります。

4. 以下のいずれかのオプションを選択し、［次へ］をクリックします。
   - VC 仮想マシンは既存の VM を使用する
   - VC テンプレートはテンプレートを使用して新しい VM を作成する
   - VC 仕様は利用可能なリストからカスタマイズ仕様を選択する

   ［仮想マシン メモリ］ページが表示されます。
5. （オプション）VM 用のメモリを調節し［次へ］をクリックします。

   メモリ

   VM テンプレートまたは VM に定義されたメモリ値をフィールドに入力します。

   デフォルト： 最低 4 MB および最大 16 GB

   注: caimgconf.cfg ファイル内のこれらの値を設定します。

   ［仮想マシン CPU］ページが表示されます。
6. （オプション）VM 用の CPU を調節し［次へ］をクリックします。

   仮想プロセッサ

   VM テンプレートまたは VM に定義された仮想プロセッサの数をフィールドに入力します。

   デフォルト： 最低 1 CPU および最大 4 CPU

   注: caimgconf.cfg ファイル内のこれらの値を設定します。

   ［ディスク］ページが、選択済み VM または選択したテンプレートからのデフォルト値が入力されたフィールドと共に表示されます。
7. （オプション）ドライブ サイズを設定し、［ドライブの追加］をクリックしてドライブを追加し、ハード ディスクに関連付けるデータ ストアおよび使用する SCSI コントローラをドロップダウン リストから設定し、［次へ］をクリックします。

   データストア

   VM が作成される、VMware ESX ホストのデータ ストア名を識別します。

ドライブ サイズ

ドライブ サイズを指定して VM により多くのハード ディスクを追加することができます。

制限： 最小のドライブ サイズは 1 MB ですが、選択したデータ ストア用のドライブ サイズを超過することはできません。

SCSI コントローラ

仮想アダプタとして使用する SCSI コントローラを指定します。

［ネットワーク］ページが表示され、テーブルに選択されたテンプレートからのデフォルト値が入力されます。

8. （オプション）［ネットワーク管理］テーブルのセルの内部をクリックすると、ドロップダウン リストがアクティブになり、任意の設定を変更できます。

   カスタム仕様が DHCP の使用を指定している場合は、テーブル内のネットワーク接続セルのみを編集できます。 ネットワーク接続は、現在標準および分散仮想スイッチの両方のネットワークをサポートしています。 以下の命名規則に基づいて、標準スイッチと分散仮想スイッチの名前を区別できます。

   - 標準スイッチの名前はネットワーク名です。
   - 分散仮想スイッチの名前は、dvPort グループ名の後に、丸かっこで囲まれた分散仮想スイッチ名を連結したもの（dvPortGroupName (dvSwitchName)）です。

   カスタム仕様が静的 IP アドレスの使用を指定している場合は、NIC セル以外のセルをすべて編集できます。CA Server Automation はカスタム仕様のネットワークが［ユーザに通知］を設定することをサポートしていません。この設定を使用するカスタム仕様はフィルタで除外され利用できません。

   ［次へ］をクリックします。

9. ［コンピュータの追加］をクリックします。

   確認メッセージがペインの一番上に表示されます。

   注: イメージングには時間がかかるため、オペレーティング システムのインストール中の遅延を予想しておく必要があります。 より効率的なディスカバリのために、検出再試行時間、または caimgconf.cfg ファイル（*install_path*¥CA¥*productname*¥conf にあります）内の間隔を調節できます。

10. ［リフレッシュ］をクリックすると新しい VM が左ペインに表示されます。

    データ センターに新しいクローン作成された VM があります。 ダッシュボードにイメージング プロセスのイベントを表示できます。また、イメージング ジョブ レポートを生成できます。

仮想マシンのクローン作成

仮想マシンのクローンを作成することによって、同じ仮想マシン ファームのいかなる場所にも配置できる仮想マシンのコピーを作成できます。また、クローンを作成するときに、ゲスト オペレーティング システムをカスタマイズできます。 仮想マシンが電源オフの状態にあるときのみ、仮想マシンのクローンを作成できます。

仮想マシンのクローンを作成する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインでクローン作成する仮想マシンを見つけて右クリックし、［管理］-［クローン作成］を選択します。

   ［クローン作成］ペインが表示されます。

3. 以下のフィールドに入力し、［クローン］をクリックします。

   名前

   VM クローン名を指定します。

   データストア

   クローン作成された VM を格納するデータストアを指定します。データストアはソース VM と同じファーム内にある必要があります。

   カスタム仕様

   使用するゲスト オペレーティング システム仕様を指定します。デフォルトまたはカスタマイズを選択できます。

   デスティネーション リソース プール

   クローン作成された VM がリソースを取得するプールを指定します。

   要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。処理が完了すると、クローンが［エクスプローラ］ペインに表示されます。

VM ステータスの管理（VMware）

以下のいずれかの VM 操作の実行により vCenter Server 仮想マシンのステータスを制御できます。

- 電源オン
- 電源オフ
- 中断
- リセット
- シャットダウン

これらの操作は、複数の VM で同時に実行できます。

VM ステータスを制御する方法

1. ［エクスプローラ］ペインでステータス処理を実行する仮想マシンを選択します。
2. VM を右クリックし、［管理］を選択します。［クイック スタート］をクリックし、電源制御の関連するリンクをクリックする方法もあります。 以下の*いずれか*を選択します。

   電源オン

   仮想マシンを開始し、ゲスト オペレーティング システムを起動します。 現在電源がオフになっているか、中断されている仮想マシンのみ、電源をオンにすることができます。

   電源オフ

   仮想マシンを電源オフします。 現在電源がオンになっているか、中断されている仮想マシンのみ、電源をオフにすることができます。

   中断

   仮想マシンを中断し、現在の状態を保存します。 マシンを再開するまで、すべてのアクティビティが中断されます。

   リセット

   ゲスト オペレーティング システムをシャットダウンし、再起動します。

   シャットダウン

ゲスト オペレーティング システムをシャットダウンします。現在電源がオンになっている仮想マシンのみ、シャットダウンすることができます。

確認ダイアログ ボックスが開きます。

3. ［OK］をクリックします。

ステータス操作が実行され、確認のメッセージが表示されます。インターフェースをリフレッシュして、最新の VM ステータスを表示します。 操作の結果を確認するイベントが表示されます。

次のアイコンが VM ステータスを示します。

VM が重大な状態であることを示します。

VM が警告の状態であることを示します。

VM が正常な状態であることを示します。

VM が不明な状態であることを示します。

テンプレートの仮想マシンへの変換

仮想マシン テンプレートを仮想マシンに変換できます。 テンプレートから変換された VM は、そのテンプレートの名前と設定を使用します。

テンプレートを仮想マシンに変換する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［VM に変換］を選択します。

   ［変換］ページが表示されます。

3. 仮想マシンの ESX サーバおよびリソース プールを選択し、［変換］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシン テンプレートの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。 処理が完了した後、インターフェースをリフレッシュすると、テンプレートが［エクスプローラ］ペインに仮想マシンとして表示されます。

仮想マシンをテンプレートに変換します

電源オフした仮想マシンをテンプレートに変換して、他の仮想マシンのベースとしてその仮想マシンの設定を使用できます。

仮想マシンをテンプレートに変換する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［テンプレートに変換］を選択します。

   確認ダイアログ ボックスが開きます。

3. ［OK］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。処理が完了した後、インターフェースをリフレッシュすると、仮想マシンが［エクスプローラ］ペインにテンプレートとして表示されます。

スナップショットの作成

後で同じ状態に戻ることができるように、スナップショットを作成して、仮想マシンの現在の状態を保存します。 スナップショットは、メモリ内容、設定、および仮想ディスク状態を含め、仮想マシン全体の状態を保存します。 電源オン、電源オフ、または中断されている仮想マシンのスナップショットを作成できます。

スナップショットを作成する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［スナップショット］を選択します。

   ［スナップショット］ペインが表示されます。

3. ［アクション］ドロップダウン メニューから［新規］を選択します。

   ［新しいスナップショットの作成］ダイアログ ボックスが表示されます。

4. スナップショット名および説明を入力して、メモリのキャプチャを有効にするべきかどうかを指定し、［OK］をクリックします。

   確認メッセージが表示されます。

5. 仮想マシンの［サマリ］をクリックします。

6. 処理を確認するイベントが表示されることを確認します。

   処理が完了すると、スナップショットが［スナップショット］ペインに表示されます。

スナップショットの削除

必要がなくなったスナップショットを削除できます。

スナップショットを削除する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［スナップショット］を選択します。

   ［スナップショット］ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。

3. スナップショットを選択し、［アクション］ドロップダウン メニューから［削除］を選択します。

   確認ダイアログ ボックスが開きます。

4. ［OK］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

5. 仮想マシンの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。処理が完了した後、スナップショットが［スナップショット］ペインに表示されなくなります。

すべてのスナップショットの削除

1 回の操作で、1 つの仮想マシンの既存のスナップショットをすべて削除できます。

すべてのスナップショットを削除する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［スナップショット］を選択します。

   ［スナップショット］ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。

3. ［アクション］ドロップダウン メニューから［すべて削除］を選択します。

   確認ダイアログ ボックスが開きます。

4. ［OK］をクリックします。

   確認メッセージが表示されます。

5. 仮想マシンの［サマリ］をクリックします。

   処理を確認するイベントが表示されることを確認します。処理が完了した後、すべてのスナップショットが［スナップショット］ペインに表示されなくなります。

仮想マシンの削除

VMware vCenter Server から仮想マシンを削除すると、仮想マシンは仮想ディスクから削除されます。

仮想マシンを削除する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［vCenter Server から削除］を選択します。

   確認ダイアログ ボックスが開きます。

3. ［OK］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

   処理の結果を確認するイベントが表示されます。 成功すると、その仮想マシンが仮想ディスクから削除され、インターフェースをリフレッシュした後、［エクスプローラ］ペインに表示されなくなります。

仮想マシンのテンプレートからの展開

テンプレートの設定を使用して、テンプレートから新しい仮想マシンを作成および展開できます。

テンプレートから仮想マシンを展開する方法

1. ［エクスプローラ］ペインで［VMware vCenter サーバ］を右クリックし、［プロビジョニング］-［VMware VM のプロビジョニング］を選択します。

   ［VMware vCenter プロビジョニング］ダイアログ ボックスが表示されます。

2. すべての必須フィールドを指定し、適切な VC テンプレートを選択します。

   ［次へ］をクリックします。

3. 残りの手順を実行して、仮想マシン用の仮想ハードウェアを指定します。［終了］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

4. 処理を確認するイベントが表示されることを確認します。

   処理が完了した後、インターフェースをリフレッシュすると、新しい仮想マシンが［エクスプローラ］ペインに表示されます。

クラスタ サービスの管理

VMware vCenter クラスタ上の以下のサービスのステータスを制御できます。

HA

ホストで障害が発生したときの、自動マイグレーションおよび VM の再起動を可能にします。

DRS

リソースのコレクションとしてホストを管理できます。必要に応じて、DRS のサービスは、VM をホストに、リソースを VM にマイグレートします。

Cluster Services を管理する方法

1. ［エクスプローラ］ペイン上の VMware vCenter クラスタを選択します。

   ［概要］ペインが右側に表示され、HA サービスおよび DRS サービスのステータスを表示します。

2. ドロップダウン メニューから［有効］または［無効］を選択します。

   サービスのステータスが変更されます。

仮想マシンのマイグレート

仮想マシンをマイグレートして、別の ESX ホストにその仮想マシンを移動できます。 電源オフのマシンをマイグレートできます。または、VMotion を備えたマシン上では電源オンのマシンをマイグレートできます。 中断されている仮想マシンはマイグレートできません。

仮想マシンをマイグレートする方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインでマイグレートする仮想マシンを見つけて右クリックし、［管理］-［マイグレート］を選択します。

   ［マイグレート］ペインが表示されます。

3. 仮想マシンのデスティネーション ESX サーバおよびリソース プールを入力し、［マイグレート］をクリックします。

   注: VM データストア/ディスクが 2 つの ESX ホスト間で共有される場合のみ、ESX ホスト間の VM マイグレーションがサポートされます。

   確認メッセージが表示されます。

4. 仮想マシンの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。 処理が完了した後、仮想マシンが［エクスプローラ］ペインのマイグレートされた場所に表示されます。

仮想マシンのモニタ

VM のステータスとプロパティは詳細にモニタすることができます。

仮想マシンをモニタする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［VMware vCenter Server］フォルダおよび ESX サーバ オブジェクトを展開します。

   VM リストが表示されます。

4. ［サマリ］タブをクリックします。

   右側のペインに、一般情報、FT プロパティ、概要、CPU とメモリの使用率、ディスク使用率（論理ボリューム）、およびイベントが表示されます。

   ［概要］パネルに示されるディスク状態は、仮想ディスクの仮想ハードウェア状態を表しています。この状態は SystemEDGE によって計算され、vCenter AIM 内に設定されたモニタに基づいています。この情報は、1 秒あたりの読み取り数/書き込み数という観点から見た、仮想ディスクの真のパフォーマンス データに基づいています。

   ［ディスク使用率］パネルに示されるディスク状態は、ゲスト オペレーティング システムの観点から見た論理ボリュームの使用率を表しています。 この状態は SystemEDGE によって計算され、vCenter AIM 内に設定されたモニタに基づいています。 VM とゲスト オペレーティング システムが動作している場合のみ、この情報が有効になります。

   ［一般情報］パネルには、VM の接続状態に関する詳細が示されます。接続状態の有効な値は以下のとおりです。

   - 未接続
   - 接続済み
   - 孤立

   孤立の接続状態は、クラスタがフェールオーバーしている状況で発生する場合があります。仮想マシンが孤立状態であるとマークされているとき、［概要］セクションに反映される状態は、孤立状態になる前に収集されたデータに基づいています。

ESX サーバのモニタ

ESX サーバのステータスとプロパティは詳細にモニタすることができます。

ESX サーバをモニタする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［VMware vCenter Server］フォルダを展開し、ESX サーバを選択します。
4. ［サマリ］タブをクリックします。

   右側のペインに、一般情報、FT 属性、概要、CPU とメモリの使用率、使用状況、およびイベントが表示されます。

5. ［vNetwork］タブをクリックします。

   右側のペインに、関連付けられている仮想標準スイッチ（vSwitch）および分散仮想スイッチ（vDS）のリストが表示されます。

6. リストから仮想スイッチを選択します。

   右側のペインに、仮想スイッチのプロパティが表示されます。

スナップショットに戻す

スナップショットに戻すと、スナップショットを作成したときの正確な状態に仮想マシンが戻されます。

スナップショットに戻す方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［スナップショット］を選択します。

   ［スナップショット］ペインが表示され、その仮想マシンの既存のすべてのスナップショットが表示されます。

3. スナップショットを選択し、［アクション］ドロップダウン メニューから［元に戻す］を選択します。

   確認ダイアログ ボックスが開きます。

4. ［OK］をクリックします。

   確認メッセージが表示されます。

5. 仮想マシンの［サマリ］タブをクリックします。

   処理を確認するイベントが表示されることを確認します。

仮想マシンの登録解除

vCenter Server から仮想マシンを登録解除すると、仮想マシンはそのまま存在しますが、VMware vCenter Server インベントリからは削除されます。

仮想マシンを登録解除する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［エクスプローラ］ペインで仮想マシンを見つけて右クリックし、［管理］-［vCenter Server からの登録解除］を選択します。

   確認ダイアログ ボックスが開きます。

4. ［OK］をクリックします。

   要求のサブミットを確認するメッセージが表示されます。

5. 仮想マシンの［サマリ］タブをクリックします。

   処理の結果を確認するイベントが表示されます。 成功すると、仮想マシンは vCenter インベントリから削除されます。

vCenter の自動化とポリシー アクション

以下のアクション タイプを VMware vCenter Server で使用できます。

- ディスクの追加 (P. 845)
- ネットワーク インターフェースの追加 (P. 847)
- 共有の設定 (P. 875)
- CPU/メモリの設定 (P. 859)
- 電源の設定 (P. 871)
- テンプレートの仮想マシンへの変換 (P. 877)
- 仮想マシンのテンプレートへの変換 (P. 879)
- マシンの削除 (P. 890)
- VM スナップショットの管理 (P. 899)
- CPU の変更 (P. 909)
- メモリの変更 (P. 911)
- マシンのプロビジョニング (P. 926)
- ディスクの削除 (P. 929)
- ネットワーク インターフェースの削除 (P. 931)
- マシンをマイグレート (P. 907)

割り当てられたルール基準が満たされるときに、vCenter の電源、リソース割り当て、および他の操作を自動化する新規アクションを作成するためにこれらのアクション タイプを使用できます。 また、これらのアクションが特定の時間に実行されるようにスケジュールすることもできます。

自動化ポリシーを作成するアクションおよびルールの使用の詳細については、「ポリシー」を参照してください。

カスタム仕様の表示

カスタム仕様は、仮想マシン上で使用しているゲスト オペレーティング システムのカスタム バージョンです。 現在のカスタム仕様、最後の更新の日付、および現在のバージョン番号をすべて表示できます。

カスタム仕様を表示する方法

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. VMware vCenter Server を検索して選択します。

   右側のペインに［サーバ］ページが表示されます。

3. ［設定］タブをクリックし、［カスタマイズの仕様］サブメニューを選択します。

   ［カスタマイズの仕様］セクションが表示されて、既存のカスタマイズ仕様が表示されます。

一般情報の表示

CA Server Automation は、右側のペイン内で［一般情報］を表示し、オブジェクト階層内の以下のレベルでリソース プロパティを提供します。

- vCenter Server
- ESX Server
- リソース プール
- VM

リソース プロパティには、以下のカテゴリに関する情報が含まれます。

- 名前、アイテム タイプ、バージョン
- CPU とメモリの数量特性
- VM 数とリソース プール数
- リソースの現在のモード

さらに、CA Server Automation には接続状態、電源状態、および VM レベルについてのフォールト トレランス情報が表示されます。

有効なフォールト トレランス ステータスの値は以下のとおりです。

- フォールト トレラントでない
- 保護されている
- 保護されていない (起動中)
- 保護されていない (セカンダリ VM が必要)
- 保護されていない (無効)
- 保護されていない (VM が実行されていない)

セカンダリの場所の値は以下のとおりです。

- 利用不可
- セカンダリ CPU 合計使用率
- セカンダリ メモリ合計

［一般情報］パネルには、フォールト トレランスが設定されているかどうか、バージョン、およびサポートされている FT VM のさまざまな数量に関する詳細が表示されます。 その数量には、以下が含まれます。

- プライマリ VM の合計
- セカンダリ VM の合計
- 電源オン プライマリ VM
- 電源オン セカンダリ VM

［一般情報］パネルに表示された VM の数は、実行中の非 FT VM とプライマリ FT VM の数に基づいています。 セカンダリ FT VM は、VM の全体の合計数には含まれていません。

関連項目

ESX サーバのモニタ (P. 682)
仮想マシンのモニタ (P. 681)

第 7 章: リソースの設定

実装に応じて、CA Server Automation をインストールした後にこれらのセクションの 1 つ以上で説明されていたタスクを実行します。

このセクションには、以下のトピックが含まれています。

プロキシ サーバの追加

インストール時に、統合されたコンポーネントによって使用されるプロキシ サーバをセットアップできます。 ［管理］タブを使用して複数のプロキシ サーバを追加できます。

次の手順に従ってください:

1. ［管理］タブを表示し、［設定］メニューから［プロキシ サーバ］を選択します。

   ［プロキシ サーバ］ページが開き、現在設定されているプロキシが表示されます。

2. ［プロキシ サーバ］ツールバーの［+］（追加）をクリックします。

   ［プロキシ サーバ設定］パネルが表示されます。

3. サーバ接続パラメータと認証情報を入力し、［OK］をクリックします。

   統合されたコンポーネントによって使用される利用可能なプロキシのリストにサーバが追加されます。

Cisco UCS サーバ

Cisco UCS 管理に対する以下の条件を確認します。

- Cisco Java ユーザ インターフェースを起動して Cisco UCS Manager が実行されていることを確認します。 Cisco Java ユーザ インターフェースを起動するリンクは http://<UCS_Manager_name> または https://<UCS_Manager_name> です。

関連項目:

コマンド ラインからの Cisco UCS AIM の設定 (P. 691)

コマンド ラインからの Cisco UCS AIM の設定

一般的な AIM 設定ユーティリティを使用して AIM が UCS Manager と通信するのに必要な接続パラメータを指定できます。SystemEDGE および Cisco UCS AIM がインストールされているすべてのサーバでユーティリティを実行できます。 ユーティリティは、CA Server Automation マネージャがインストールされていない AIM を保有するリモート サーバで必要です。

注: CA Server Automation ユーザ インターフェースを使用して、UCS Manager AIM を登録することもできます。 UCS AIM を登録するには、［管理］をクリックし、［Cisco UCS サーバ］をクリックし、［UCS AIM サーバ］ツールバーで「+」（追加）をクリックします。

AIM 設定ユーティリティを使用することによって、以下のアプリケーション シナリオが可能です。

- Cisco UCS Manager で Cisco UCS ユーザ認証情報を変更します。次に、Cisco UCS Manager 接続パラメータを更新します。
- Cisco UCS AIM インストール中に、設定手順がスキップされます。その後、接続パラメータを指定します。

一般的な AIM 設定ユーティリティ（nodecfgutil.exe）は、Install_Path¥SystemEDGE¥plugins¥AIPCommon ディレクトリにあるコマンド ライン ユーティリティです。

コマンド ラインから UCS AIM を設定する方法

1. コマンド プロンプトを開き、*Install_Path*¥SystemEDGE¥plugins¥AIMCommon ディレクトリに移動し、以下のコマンドを入力します。

   ```
   nodecfgutil.exe
   ```

   ユーティリティは使用方法に関する情報を表示します。

2. メニューの説明に従って、Cisco UCS Manager のアクセス情報を追加、更新、または削除します。 アクセス情報は暗号化されて、*Install_Path*¥SystemEDGE¥plugins¥AIPCommon¥ucs.cfg ファイルに格納されます。

3. Cisco UCS AIM は自動的に変更を取得し、SystemEDGE エージェントを再利用することなく、新しい Cisco UCS Manager インスタンスをモニタするかまたは既存の Cisco UCS Manager インスタンスのモニタリングを削除します。

AIX NIM イメージングの設定方法

AIX NIM イメージをプロビジョニングするには、以下のプロセスを使用します。

1. AIX NIM サーバに NIM アダプタをインストールします。
2. ca_post_install.sh スクリプト ファイルを編集します。
3. NIM Master サーバを設定します。設定は［Administration, Configuration］ページを使用して、CA Server Automation のインストール中に、またはインストールの後に実行できます。

AIX NIM サーバへの NIM アダプタのインストール

グラフィカル インターフェースまたはコマンド ライン テキスト コンソールを使用して、NIM アダプタをインストールできます。

NIM アダプタをインストールする方法

1. コンピュータにインストール メディアを挿入し、DVD2¥Installers¥AIX_aix¥NIM ディレクトリに移動し、AIX NIM サーバに ca-nim-adapter.AIX をコピーします。
2. AIX NIM サーバに以下のコマンドを入力します。

   ```
   ./ca-nim-adapter.AIX
   ```

   XWindows および DISPLAY が AIX UNIX 端末が開いているコンピュータに設定されている場合、グラフィカル インターフェース インストーラが起動します。それ以外の場合は、コマンドライン インターフェース インストーラが起動します。
3. ［次へ］をクリックします。

   ［使用許諾契約］ページが表示されます。
4. 使用許諾契約を読み、［同意します］をクリックします。

   ［インストール ディレクトリ］ オプションが表示されます。

5. インストールするディレクトリを指定し、[次へ]をクリックします。
6. インストール パスを確認し、［製品をインストール］をクリックします。

   インストール後の手順が表示されます。
7. ［OK］をクリックして、インストーラを終了します。

注: NIM で動作するように CA Server Automation を設定するには、スクリプト ファイル *install_path*/imaging/etc/ca_post_install.sh を更新する必要があります。ハッシュ パスワードは、ターゲット AIX コンピュータのハッシュ パスワードと一致する必要があります。 ca_post_install.sh スクリプトの内容を確認して更新します。このスクリプトには、適切なオプションを設定するための指示が含まれています。

ca_post_install.sh スクリプト ファイルの編集

ca_post_install.sh スクリプト ファイルを編集してハッシュされたパスワードを設定し、/tmp および /opt ファイルシステムのサイズを増やすことができます。

ハッシュされたパスワード変数の更新

NIM クライアントがイメージされた後、IBM AIX インストーラは空のルート パスワードを残します。 ルート パスワードを指定するには、ca_post_install.sh スクリプト ファイルを使用する前に更新します。 ハッシュされたパスワード（DES 形式）を設定し、NIM クライアント用の HASH_PASSWORD 変数を更新して使用します。

注: ca_post_install.sh スクリプト ファイルには、**管理者**のプレーン テキストの値に変換するデフォルトのハッシュ パスワードが含まれています。

HASH_PASSWORD 変数を更新する方法

1. NIM クライアントを設定するパスワードで設定されているシステムにアクセスします。
2. /etc/security ディレクトリに移動し、passwd ファイルを開きます。

   passwd ファイル内のハッシュされたルート パスワード エントリは以下のようになります。

   ```
   root:
       password = YmB7AkapuLf8/s
   ```

3. ハッシュされたルート パスワードをコピーし、*install_path*/imaging/etc ディレクトリに移動して、ca_post_install.sh スクリプト ファイルを開きます。
4. ca_post_install.sh スクリプト ファイル内の HASH_PASSWORD 変数にパスワードを貼り付けます。
5. ファイルを保存して、終了します。

/tmp および /opt ファイルシステムのサイズを増やします。

/tmp または/opt ファイルシステムのスペースが十分にない場合は、NIM クライアントへのエージェントの展開が失敗する場合があります。 選択されたデフォルトは、インストールするエージェントには小さすぎます。したがって、少なくとも /tmp は 400 MB に、/opt は 700 MB に増やしてください。 ファイルシステムのサイズを増やす NIM スクリプトがない場合は、ca_post_install.sh スクリプトの chfs コマンドのコメントを外します。これらの行のコメントを外すと、NIM クライアントがイメージングされた後で NIM スクリプト リソースとしてこのスクリプトを使用することにより、NIM アダプタはファイル システムのサイズを増やすことができます。

注: スクリプトがまだこれらの行を有効にしていないという確信がない限り、これらの行を有効にしないでください。

/tmp および /opt ファイルシステムのサイズを増やす方法

1. *install_path*/imaging/etc ディレクトリに移動して ca_post_install.sh スクリプト ファイルを開きます。

2. 先頭の # 文字を削除することによりスクリプト内の両方の chfs コマンドのコメントを外します。

   コメントされた行は以下の例のように表示されます。

   ```
   #chfs -a size=$OPTFSSIZE /opt
   ```

   コメントを外された行は以下の例のように表示されます。

   ```
   chfs -a size=$OPTFSSIZE /opt
   ```

   注: オプションで、OPTFSSIZE および TMPFSSIZE の変数をデフォルトよりも大きい値に変更できますが、小さい値には設定しないでください。

3. ファイルを保存して、終了します。

NIM アダプタ デーモンの開始または停止

NIM アダプタ デーモンは、インストール後またはシステムのブート時に自動的に開始されます。

NIM アダプタ デーモンを手動で開始するには、以下のコマンドを実行します。

```
install-path/imaging/bin/canimstart.sh start
```

NIM アダプタ デーモンを手動で停止するには、以下のコマンドを実行します。

```
install-path/imaging/bin/canimstart.sh stop
```

NIM Master サーバの設定

CA Server Automation インストールの後に NIM Master サーバを設定できます。

NIM Master サーバを設定する方法

1. NIM Master サーバに NIM アダプタを設定します。
2. CA Server Automation ユーザ インターフェースにログインします。
3. ［管理］をクリックします。

   ［管理］ページが表示されます。
4. ［設定］をクリックします。

   ［設定］ページが表示されます。
5. 左ペインで、［NIM マスタ サーバ］をクリックします。

   ［NIM マスタ サーバ］ページが表示されます。
6. 「+」（追加）をクリックします。

   ［NIM マスタ アクセス認証情報の追加］ダイアログ ボックスが表示されます。
7. 認証情報を追加し［OK］をクリックします。
8. ［検証］をクリックして接続ステータスを確認します。

NIM Master サーバの同期

NIM Master サーバのリソースとプロパティの同期は *install_path*¥conf¥caimgconf.cfg 内の CONFIG_KEY_IMG_IMAGELIST_SYNC_INTERVAL キーに基づきます。デフォルトの設定は 12 時間です。また、オンデマンドで同期することもできます。

注: caimgconf.cfg 変更には、CAAIPApache サービスの再起動が必要です。

NIM Master サーバをオンデマンドで同期する方法

1. CA Server Automation ユーザ インターフェースにログインします。
2. ［管理］をクリックします。

   ［管理］ページが表示されます。
3. ［設定］をクリックします。

   ［設定］ページが表示されます。
4. 左ペインで、［NIM マスタ サーバ］をクリックします。

   ［NIM マスタ サーバ］ページが表示されます。
5. 1 つ以上の NIM サーバを選択します。
6. 「>>」（NIM サーバのプロパティをリフレッシュします）をクリックします。

動的な NIM マシン リソースのサポート

CA Server Automation では、NIM 環境で NIM マシン リソースを動的に作成するために Web サービス メソッドを提供します。 IP アドレスがメソッドに提供され、それをサポートするためにどの NIM マスタに NIM ネットワーク リソースがあるかを決定します。 そのアドレスに存在しない場合のみ NIM マシン リソースが作成されます。

リソースは以下の規則を使用して作成されます。

ca_UUID

UUID はランダムに生成された UUID です。 NIM マシン リソースを削除する Ｗｅｂ サービス メソッドは、CA Server Automation によって作成された NIM マシンのみを削除します。 NIM マスタが CA Server Automation 設定から削除され、後で再び追加された場合、設定変更の前に Web サービスによって作成されたすべての NIM マシンは、削除対象として考慮されなくなります。 NIM マスタが設定から削除されると、CA Server Automation 作成レコードがすべて削除されます。

Imaging サービスは Web サービスを公開しますが、それらの使用方法を決定するのは外部コンシューマ（予約マネージャなど）のみです。

ＮＩＭマシンの作成には、特定の必須プロパティおよび任意のプロパティが使用されます。 CA Server Automation では、caimgconf.cfg ファイルの ＮＩＭマシン グループに定義されたデフォルトのプロパティを使用します。プロパティはグローバルで、すべての NIM マスタに適用されます。これらの値は、環境に応じて調整できます。

Web サービスの環境要件には以下が含まれます。

- NIM ネットワーク リソースは、NIM 環境内にすでに定義されている必要があります。
- NIM ネットワーク リソースでは、ネットワーク アドレス範囲が重複することは許可されません。これには、同じ ＮＩＭマスタで定義されたネットワーク リソース、および複数の ＮＩＭマスタ サーバにわたって定義されたリソースが含まれます。
- IP アドレスは DNS 解決可能である必要があります。
- NIM マシンは CPUID なしで作成されます。

Solaris JumpStart プロビジョニング

JumpStart アダプタは CA Server Automation と統合されているため、イメージを含む Solaris システムをプロビジョニングすることができます。JumpStart アダプタはシステムを探索して情報を検出し、どのイメージがサーバで利用可能かを決定します。 利用可能なイメージの 1 つを選択し、特定のターゲット コンピュータに対してイメージング ジョブをサブミットできます。

CA Server Automation ドキュメントでは、読者が JumpStart ソリューションに精通していることを前提としています。 Oracle によって JumpStart サーバ技術に課されている要件および制限はすべて、CA Server Automation でも有効です。

概要

このセクションでは、JumpStart が使用できるインストール イメージを作成するための手順、およびオペレーティング システムがインストールされた後でシステムを設定するのに必要な手順について説明します。

*JumpStart サーバ*は、環境で利用可能なオペレーティング システム イメージを格納するサーバを指します。 *JumpStart クライアント*は、JumpStart サーバに格納されたオペレーティング システム イメージのうちの 1 つとプロビジョニングできるシステムを指します。

複数のインストールとブート サーバを設定できます。

IPMI 準拠のサービス プロセッサを使用する Solaris 10 x86 クライアントは、正しく設定されている Solaris DHCP サーバが存在するのであれば、プロビジョニングできます。

複数の JumpStart アダプタ環境にサポートを提供するためには、1 つの JumpStart アダプタが各 JumpStart ブート サーバにインストールされ設定されている必要があります。

JumpStart の前提条件

JumpStart ソリューションを使用するための前提条件には、以下が含まれます。

- サーバが、Solaris 10 SPARC または Solaris 10 x86 で実行されている必要があります。
- JumpStart ブート サーバは、イメージングされる各 SPARC クライアントの同じサブネットに存在する必要があります。
- クライアント アーキテクチャにかかわらず、ホスト名はすべて、DNS サーバで静的な名前として設定されている必要があります。
- 設定に使用したプロトコルは、ファイアウォールでブロックできません。
- JumpStart ソリューションには、SPARC システム用の RARP/BOOTP/TFTP プロトコルが必要です。
- JumpStart ソリューションには、Solaris 10 x86 ベースのシステム用の PXE/DHCP/TFTP が必要です。
- SPARC および Solaris 10 x86 システムは、Network File System（NFS）を使用してリモート JumpStart インストール イメージにアクセスします。
- サーバのインストールには、完全な Solaris 10 メディアが必要です。
- 初期インストールのみがサポートされていますが、Solaris イメージのアップグレードはサポートされていません。
- サポートされた Solaris バージョンごとに 1 つの JumpStart 設定ディレクトリおよび 1 つのプロファイル/ルール ディレクトリのみが許可されます。
- SPARC クライアント コンピュータが、すでに Solaris を実行しており、動的に使用できるよう再イメージングされている必要があります。
- 再起動できるように、SSH（セキュア ソケット シェル）の root アクセス権のために SPARC クライアント コンピュータが事前設定されている必要があります。
- Solaris 10 X86 クライアント コンピュータには、IPMI（Intelligent Platform Management Interface）1.5 または 2.0 互換のサービス プロセッサが必要です。
- 各サービス プロセッサには、静的な IP アドレスが設定されている必要があります。

- サービス プロセッサの IPMI 機能が有効であり、BIOS で設定されている必要があります。
- 各サービス プロセッサは、パブリック ネットワークから到達できるように事前設定されている必要があります。
- DHCP サーバが SSH アクセス用に設定されており、JumpStart x86 プロビジョニング リクエスト中に CA Server Automation JumpStart アダプタと通信可能である必要があります。

JumpStart アダプタのインストール

以下のいずれかの方法を使用して、JumpStart アダプタをインストールします。

- コマンド ラインから
- 応答ファイルから

コマンド ラインからの JumpStart アダプタのインストール

JumpStart アダプタをインストールするには、ca-jumpstart-adapter.Solaris（または x86 インストールでは ca-jumpstart-adapter.SolarisIntel）を実行します。 インストール プロンプトに従い、デフォルトの場所（/opt/CA/*productname*）または別の場所のいずれかを選択します。

レスポンス ファイルを使用した JumpStart アダプタのインストール

レスポンス ファイルを作成するには、対話型インストール プロセスを実行してレスポンス ファイルを生成します。

応答ファイルを作成するには、以下の手順に従います。

```
./ca-jumpstart-adapter.Solaris -a ca-jumpstart-adapter.Solaris.@pif -r resp.txt
```

サイレント インストールを実行するために応答ファイルを使用する方法

```
./ca-jumpstart-adapter.Solaris -r resp.txt
```

テキスト端末コンソールを使用した JumpStart サーバへのイメージングのインストール

テキスト端末コンソールを使用して、アダプタを対話形式でインストールできます。

テキスト端末コンソールを使用して、アダプタをインストールする方法

1. インストール メディアをコンピュータに挿入し、DVD2¥Installers¥Solaris_sparc¥JumpStart または DVD2¥Installers¥Solaris_x86¥JumpStart に移動し、それぞれ ca-jumpstart-adapter.Solaris または ca-jumpstart-adapter.SolarisIntel を JumpStart サーバにコピーします。FTP クライアントを使用する場合は、ファイルをバイナリ形式でコピーし、ファイルに実行権限も設定します。
2. JumpStart サーバに以下のコマンドを入力します。

   ```
   ca-jumpstart-adapter.Solaris or ca-jumpstart-adapter.SolarisIntel
   ```

   コンソールが表示されてインストールの準備をします。
3. Enter キーを押します。

   ［使用許諾契約］ページが表示されます。
4. ［使用許諾契約］の下部にスクロールします。
5. Tab キーで［同意します］に移動して Enter キーを押します。

   インストール フォルダ オプションが表示されます。
6. デフォルトの場所を受け入れる場合は、Tab キーで［次へ］に移動します。 受け入れない場合は、インストール場所を指定し、 Tab キーで［次へ］に移動し、Enter キーを押します。
7. 選択内容を受け入れてインストールを開始するには、Tab キーで［製品をインストール］に移動します。前の画面に移動するには、Tab キーで［前へ］に移動します。インストールをキャンセルするには、Tab キーで［キャンセル］に移動して Enter キーを押します。

JumpStart アダプタのアンインストール

JumpStart アダプタ アンインストーラは *install_path*/Uninstall ディレクトリに配置されています。 デフォルトのインストール場所が選択されている場合、アンインストーラは /opt/CA/*productname*/Uninstall に配置されています。

サイレント アンインストールを実行する方法（レスポンス ファイルは必要ありません）

```
./uninstall.ca-jumpstart-adapter -s
```

対話型アンインストールを実行する方法

```
./uninstall.ca-jumpstart-adapter
```

Solaris 用の JumpStart

JumpStart を使用して Solaris イメージを展開するには、最初に CA Server Automation JumpStart アダプタを Solaris JumpStart サーバにインストールします。 インストール手順は「JumpStart アダプタのインストール」セクションに説明があります。 アダプタをインストールした後で、cajmpst.cf ファイルを手動で編集します。

dpmutil ユーティリティを使用した Solaris DHCP サーバの設定

Solaris JumpStart サーバをインストールした後、dpmutil コマンド ライン ユーティリティを実行し、Solaris Dynamic Host Configuration Protocol（DHCP）サーバを設定して Solaris x86 コンピュータのプロビジョニングを有効にします。 dpmutil を実行するには管理者権限を持つユーザ名が必要です。

dpmutil コマンドで DHCP サーバを追加する方法

1. 管理者ユーザ名およびパスワードを使用して、CA Server Automation サーバにログインします。
2. コマンド プロンプトで以下のコマンドを入力し、Enter キーを押します。

   ```
   dpmutil -set -–dhcp-u
   ```

   ユーティリティは、CA Server Automation ユーザ名およびパスワードを要求するプロンプトを表示します。

3. ユーザ名とパスワードを入力し Enter キーを押します。

   ユーティリティは DHCP ホスト サーバの名前を要求するプロンプトを表示します。

   注: DHCP サーバは、JumpStart x86 のプロビジョニング要求中に CA Server Automation JumpStart アダプタがそれと通信できるように SSH アクセスが設定されている必要があります。

4. ホスト名を入力して Enter キーを押します。

   ユーティリティは DHCP サーバのユーザ名およびパスワードを要求するプロンプトを表示します。

5. ユーザ名とパスワードを入力し Enter キーを押します。

   DHCP サーバは CA Server Automation が x86 コンピュータをプロビジョニングできるように設定されます。

cajmpst.cf ファイルの編集

cajmpst.cf ファイルを編集して JumpStart 設定サーバおよび JumpStart プロファイル サーバの場所を指定することができます。

cajmpst.cf ファイル（デフォルトのインストール場所）を編集する方法

1. /opt/CA/*productname*/imaging/etc ディレクトリに移動してテキスト エディタで cajmpst.cf ファイルを開きます。

   ファイルが開きます。

   注: /opt/CA/CAM/imaging/etc はデフォルトのパスです。 別のパスにインストールするように選択した場合は、それに応じて移動します。

2. ファイル内の以下の行へ移動します。

```
# Solaris 10 用の rules ファイル パス（JumpStart プロファイル サーバ）。
#Solaris_10_Profile_Server = /jumpstart/ca/profile/Solaris_10

# Solaris 10 用の sysidcfg ファイル パス（JumpStart 設定サーバ）。
#Solaris_10_Config_Server = /jumpstart/ca/profile/Solaris_10
```

   注: トップレベルのファイル パスに sysidcfg ファイルを含める必要があります。 また、追加のターゲット固有の sysidcfg ファイルを配置するサブディレクトリを作成することもできます。サブディレクトリ名には、ターゲット サーバを識別するために MAC アドレス（コロンのない小文字）またはユーザ定義のホスト名を使用することができます。

```
# Solaris 9 用の rules ファイル パス（JumpStart プロファイル サーバ）
#Solaris_9_Profile_Server = /qa/jumpstart/Solaris_9

# Solaris 9 用の sysidcfg ファイル パス（JumpStart 設定サーバ）
#Solaris_9_Config_Server = /qa/jumpstart/Solaris_9

# Solaris 8 用の rules ファイル パス（JumpStart プロファイル サーバ）
#Solaris_8_Profile_Server = /qa/jumpstart/Solaris_8

# Solaris 8 用の sysidcfg ファイル パス（JumpStart 設定サーバ）
#Solaris_8_Config_Server = /qa/jumpstart/Solaris_8
```

3. Solaris のバージョンに関係するパス情報が含まれた 2 つの変数の前の # 文字を削除し、JumpStart サーバの場所を更新します。 たとえば、Solaris 9 を実行している場合は、以下の変数を編集します。

   ```
   Solaris_9_Profile_Server = <path>
   Solaris_9_Config_Server = <path>
   ```

   ファイルの更新されたセクションは以下のように表示されます。

   ```
   # Solaris 10 用の JS プロファイル サーバの場所
   #Solaris_10_Profile_Server = /qa/jumpstart/Solaris_10

   # Solaris 10 用の JS 設定サーバの場所
   #Solaris_10_Config_Server = /qa/jumpstart/Solaris_10
   # Solaris 9 用の JS プロファイル サーバの場所
   Solaris_9_Profile_Server = <path>

   # Solaris 9 用の JS 設定サーバの場所
   Solaris_9_Config_Server = <path>
   ```

   注: Solaris の両方のバージョンを実行している場合は、パス情報が含まれる 4 つの変数をすべて編集します。Solaris 8 変数は、Solaris 8 を使用してプロビジョニングする予定がないのであれば、無視することができます。

4. ファイルを保存して、終了します。

   これで編集は完了です。

post_install.sh ファイルのコピー

CA Technologies では、必要な post_install.sh 終了スクリプトを提供します。元のコンテンツは削除しないでください。 コンテンツを追加し、識別された固有のパラメータを変更できます。

このファイルを使用するには、/opt/CA/*productname*/imaging/etc ディレクトリ（またはユーザが選択したインストール パス）に移動し、post_install.sh ファイルを Solaris 8、9 または 10 用の JumpStart ルール ファイルに指定されたディレクトリへコピーします。

Solaris 8 イメージを作成する方法

Solaris 8 イメージの作成には、CD からインストール可能なイメージを抽出し、クライアントを CA Server Automation と統合するのに必要なパッケージを追加し、これらのパッケージに必要なパッチを追加して設定ファイルを変更することが含まれます。

関連項目:

ディレクトリの準備 (P. 707)
メディアからのインストール可能なイメージの抽出 (P. 708)
パッケージをイメージに追加する (P. 709)
パッチをイメージに追加する (P. 710)
設定ファイルを変更する方法 (P. 711)
JumpStart での SSH の設定 (P. 718)

ディレクトリの準備

JumpStart イメージング用のディレクトリを設定します。 image 親ディレクトリには、JumpStart クライアント コンピュータにインストールされるオペレーティング システム イメージが含められます。 config 親ディレクトリには、JumpStart がオペレーティング システムをインストールして JumpStart クライアントを設定するのに使用する設定ファイルが含められます。 サイトに固有のディレクトリ値を編集し、親ディレクトリを作成し、次に、それらを共有します。

ディレクトリを準備する方法

1. サイトに固有の値が含まれる、以下のコードおよびコマンドの例を編集します。 これは包括的なリストではありません。

   image_hostname

   JumpStart サーバのホスト名を指定します。

   client_hostname

   JumpStart サーバのホスト名を指定します。

   image_parent

   オペレーティング システム イメージ ディレクトリが含まれる JumpStart サーバ上のディレクトリのパスを指定します。

   例： /jsimages

   config_parent

   JumpStart 設定ファイルが含まれる JumpStart サーバ上のディレクトリのパスを指定します。

   例： /jumpstart

   sol_8 is

   （オプション）置換または削除できるサブディレクトリを指定します。

   サイト固有の設定が設定されます。

2. インストール ディレクトリを作成し、必要に応じて以下のように設定ディレクトリを作成します。

   ```
   mkdir –m 755 /image_parent/sol_8

   mkdir –m 755 /config_parent

   mkdir –m 755 /config_parent/bin
   ```

3. /etc/dfs/dfstab ファイルに移動し、以下の行を追加します。

   ```
   share –F nfs –o ro,anon=0 /image_parent/sol_8
   ```

   ```
   share –F nfs –o ro,anon=0 /config_parent
   ```

   ディレクトリが共有されます。

4. 以下のコマンドを入力します。

   ```
   shareall
   ```

   共有ディレクトリがアクティブになります。

メディアからのインストール可能なイメージの抽出

Solaris メディアからインストール可能なイメージを抽出します。

メディアからインストール可能なイメージを抽出する方法

1. Solaris 8 Software 1 CD を CD-ROM ドライブに挿入し、自動的にマウントされない場合は CD をマウントし、［コマンド プロンプト］ウィンドウに次の行を入力します。

   ```
   cd /cd_drive/cdrom0/s0/Solaris_8/Tools
   ```

   ```
   ./add_to_install_server /image_parent/sol8
   ```

   ファイルはソフトウェア CD 1 から抽出されます。

2. Solaris 8 Software 2 CD を CD-ROM ドライブに挿入し、自動的にマウントされない場合は CD をマウントし、［コマンド プロンプト］ウィンドウに次の行を入力します。

   ```
   cd /cd_drive/cdrom0/s0/Solaris_8/Tools
   ```

   ```
   ./add_to_install_server /image_parent/sol_8
   ```

   ファイルはソフトウェア CD 2 から抽出されます。イメージが作成された後、JumpStart クライアントが CA Server Automation と統合できるように、パッケージをイメージに追加する必要があります。

パッケージをイメージに追加する

パッケージは JumpStart クライアントを CA Server Automation と統合するために必要です。www.sunfreeware.com Web サイトから必須パッケージおよびオプションのパッケージをダウンロードし、それらをイメージに追加します。

パッケージをイメージに追加する方法

1. 作業ディレクトリに libgcc-3.4.6 をダウンロードし、パッケージを解凍します。

   ```
   cd /working_directory

   gunzip libgcc-3.4.6-sol8-sparc-local.gz
   ```

2. 以下のコマンドを入力します。

   ```
   pkgtrans libgcc-3.4.6-sol8-sparc-local . all

   cp –r SMClgcc /image_parent/sol_8/Solaris_8/Product
   ```

   パッケージが変換されて、libgcc パッケージがイメージに追加されます。

3. 作業ディレクトリに openssh-5.0p1 をダウンロードし、パッケージを解凍します。

   ```
   cd /working_directory

   gunzip openssh-5.0p1-sol8-sparc-local.gz
   ```

4. 以下のコマンドを入力します。

   ```
   pkgtrans openssh-5.0p1-sol8-sparc-local . all

   cp –r SMCosh501 /image_parent/sol_8/Solaris_8/Product
   ```

   パッケージが変換されて、SSH パッケージがイメージに追加されます。

5. 作業ディレクトリに openssl-0.9.8h をダウンロードし、パッケージを解凍します。

   ```
   cd /working_directory

   gunzip openssl-0.9.8h-sol8-sparc-local.gz
   ```

6. 以下のコマンドを入力します。

   ```
   pkgtrans openssl-0.9.8h-sol8-sparc-local . all

   cp –r SMCossl /image_parent/sol_8/Solaris_8/Product
   ```

   パッケージが変換されて、SSL パッケージがイメージに追加されます。

7. 作業ディレクトリに zlib-1.2.3 をダウンロードし、パッケージを解凍します。

   ```
   cd /working_directory
   ```

   ```
   gunzip zlib-1.2.3-sol8-sparc-local.gz
   ```

8. 以下のコマンドを入力します。

   ```
   pkgtrans zlib-1.2.3-sol8-sparc-local . all
   ```

   ```
   cp –r SMCzlib /image_parent/sol_8/Solaris_8/Product
   ```

   パッケージが変換されて、zlib パッケージがイメージに追加されます。パッケージをイメージに追加し終えたら、これらのパッケージに必要なパッチをイメージに追加します。

パッチをイメージに追加する

イメージに追加したパッケージに必要なパッチ、および任意のオプションのパッチを追加します。JumpStart クライアントを CA Server Automation に統合するのに必要なパッチも 2 つあります。 www.sun.com Web サイトからパッチをダウンロードし、それらをイメージに追加します。

注: パッチをダウンロードするには Sun オンライン アカウントが必要です。 Sun の Web サイトの自己登録ページでログインするか登録します。

パッチをイメージに追加する方法

1. パッチ 108434-22 を Sun Web サイトの libc パッチ ページから作業ディレクトリへダウンロードします。

   ```
   cd /working_directory
   ```

2. 以下のコマンドを入力します。

   ```
   jarunzip -x–xf 108434-22.jar.zip
   ```

   ファイルが解凍されます。

3. 以下のコマンドを入力します。

   ```
   cp –r 1084340-22 /image_parent/sol_8/Solaris_8/Patches
   ```

   libc パッチはイメージにコピーされます。

4. パッチ 112438-03 を Sun Web サイトの random パッチ ページから作業ディレクトリへダウンロードします。

   ```
   cd /working_directory
   ```

5. 以下のコマンドを入力します。

   jjar –xxf 112438-03.jarzip を解凍します。

   ファイルが解凍されます。

6. 以下のコマンドを入力します。

   cp –r 112438-03 /image_parent/sol_8/Solaris_8/Patches

   random パッチはイメージにコピーされます。

設定ファイルを変更する方法

イメージを作成した後、設定ファイルを作成または変更します。これによって、JumpStart クライアントがプロビジョニングされるときに、パッケージがインストールされ、パッチが適用されて、必要なその他の設定が実行されるようにします。

関連項目:

［Order］ファイルの編集 (P. 711)
［Package Table of Contents］ファイルの編集 (P. 712)
［プロファイル］ファイルの編集 (P. 713)
［ルール］ファイルの編集 (P. 714)
設定ファイルの編集 (P. 715)
［終了］ファイルの編集 (P. 716)

［Order］ファイルの編集

［Order］ファイルは、イメージを使用してインストールされるパッケージ、およびそれらがインストールされる順序を示します。

［Order］ファイルを編集する方法

1. image 親ディレクトリに移動し、［Order］ファイルを編集します。

   /image_parent/sol_8/Solaris_8/Product/.order

2. 新しいパッケージをパッケージ リストの最後に以下のように追加します。

   SMClgcc

   libgcc パッケージを定義し、任意の順序でリスト表示できます。

   SMCossl

   SSL パッケージを定義し、任意の順序でリスト表示できます。

   SMCzlib

   zlib パッケージを定義し、任意の順序でリスト表示できます。

   SMCosh501

   SSH パッケージを定義し、他のパッケージ（SSL、libgcc および zlib）の後にリスト表示される必要があります。

   オプションのパッケージをインストールしている場合、それらを順番に追加する必要があります。

3. ファイルを保存します。

[Package Table of Contents]ファイルの編集

［Package Table of Contents］ファイルには、インストールされているパッケージに関する情報が含まれます。 パッケージにはそれぞれ［Package Table of Contents］ファイルに必要な情報が含まれている情報ファイルがあります。

[Package Table of Contents]ファイルを編集する方法

1. image 親ディレクトリに移動し、［Package Table of Contents］ファイルを編集します。

   ```
   /image_parent/sol_8/Solaris_8/.packagetoc
   ```

2. 各パッケージの情報ファイルを検索し、任意のテキスト エディタを使用して開いて、［Package Table of Contents］ファイルに必要な情報を抽出します。 たとえば、Open SSL 情報は以下のディレクトリに配置されています。

   ```
   /image_parent/sol_8/Solaris_8/Product/SMCossl/pkginfo
   ```

3. すべての必須パッケージおよびオプションのパッケージの情報を使用して［Package Table of Contents］ファイルを編集します。 情報によっては必須のものと、サイズ値のようにオプションのものとがあります。
4. ファイルを保存します。

［プロファイル］ファイルの編集

イメージに追加されたパッケージの名前で［プロファイル］ファイルを更新します。 ファイルは既存の JumpStart イメージまたは新しく作成された Solaris 8 イメージからコピーできます。 上級ユーザは一意の情報で複数のプロファイル ファイルを作成する必要がある場合があります。 特定のプロファイルは［ルール］ファイルでイメージおよび 1 つ以上のコンピュータと関連付けられます。

［プロファイル］ファイルを編集する方法

1. configuration 親ディレクトリに移動して［プロファイル］ファイルをコピーします。

   ```
   cd /config_parent/ca/profile/Solaris_8
   cp /image_parent/sol_8/Solaris_8/Misc/jumpstart_sample/ any_machine profile
   cp –r /image_parent/sol_8/Solaris_8/Misc/jumpstart_sample/*
   ```

2. テキスト エディタで［プロファイル］ファイルを開き、新しいパッケージをパッケージ リストの最後、および filesys エントリの前に追加します。

   ```
   package SMClgcc add
   package SMCossl add
   package SMCzlib add
   package SMCosh501 add
   ```

3. ファイルを保存します。

[ルール]ファイルの編集

[ルール] ファイルには、イメージの [プロファイル] ファイルおよび [終了] ファイルの名前が含まれます。[ルール] ファイルは既存の JumpStart イメージまたは新しく作成された Solaris 8 イメージからコピーできます。上級ユーザは、インストールできるイメージを制御するルールを書き込むだけでなく、特定の JumpStart クライアント上で実行されているスクリプトを開始または終了するルールも書き込む必要がある場合があります。また、サイト固有の終了スクリプトも要求できます。これらのスクリプトは、bin/post_install.sh への呼び出しが含まれている場合は受け入れられます。

[ルール]ファイルを編集する方法

1. configuration 親ディレクトリに移動し、テキスト エディタで [ルール] ファイルを開きます。

   ```
   /config_parent/config_dir/Solaris_8/rules
   ```

2. 以下の形式でルールを書き込みます。 ルールは自由形式です。

   ```
   rule value  begin_file  profile_file finish_file
   ```

3. 既存のルール ファイルの名前を変更するか削除し、最小 [ルール] ファイルに以下のルールを使用して 1 つのルールを作成します。

   ```
   any  profile  bin/post_install.sh
   ```

4. ファイルを保存します。

5. check シェル スクリプトを実行して [ルール] ファイルへの変更を検証します。

   ```
   ./check
   ```

   JumpStart は、check シェル スクリプトによって作成される rules.ok ファイルを使用します。

設定ファイルの編集

設定ファイルには、JumpStart がサイレント（無人）インストールを実行できるようにするのに必要な情報が含まれます。 設定ファイルの構文およびキーワードの詳細については Sun の Web サイト上の Solaris 8 sysidcfg ドキュメントを参照してください。

設定ファイルを編集する方法

1. configuration 親ディレクトリに移動し、テキスト エディタで設定ファイルを開きます。

   ```
   /config_parent/ca/profile/Solaris_8/sysidcfg
   ```

2. ファイルを編集し、保存します。

設定ファイルの例

設定ファイルの例を以下に示します。

```
system_locale=en_US

timezone=US/Pacific

timeserver=localhost

terminal=sun-cmd

name_service=DNS {domain_name=domain.com name_server=ip_address}

security_policy=none

network_interface=PRIMARY {default_route=ip_address netmask=255.255.255.0
protocol_ipv6=no}
```

[終了]ファイルの編集

[終了] ファイルはオペレーティング システム イメージが JumpStart クライアントにインストールされた後で実行されます。 このスクリプトには、インストールを完了し、JumpStart クライアントを完全に操作可能にする設定手順が含まれます。

[終了]ファイルを編集する方法

1. configuration 親ディレクトリに移動し、post_install.sh ファイルをコピーします。

   ```
   /config_parent/config_dir/Solaris_8/bin/post_install.sh
   ```

   ```
   cp $CA_DCA_MANAGER/imaging/etc/post_install.sh
   config_parent/config_dir/Solaris_8/bin/
   ```

   CA Server Automation JumpStart アダプタに提供された post_install.sh ファイルがコピーされます。

2. 任意のテキスト エディタを使用して［終了］ファイルを開き、以下の変数の値を置換します。

   PASSWD

   パスワードを設定します。

   例： PASSWD=pZWXCvV5eAkJU

   PATCH_LOCATION

   パッチへのパスを指定します。

   例：
   PATCH_LOCATION=server_hostname:/image_parent/sol_8/Solaris_8/Patches

IPC の調整可能なパラメータ

調整可能な Solaris パラメータを指定します。 設定を有効にするにはシステムの再起動が必要です。

例：

SHMMAXv8_HEX=0x400000

SHMSEGv8_HEX=0x100

SEMMNIv8_HEX=0x100

SEMMNSv8_HEX=0x12c

SEMUMEv8_HEX=0x20

SEMMNUv8_HEX=0x100

オプションのパッチ

インストール イメージに追加されたすべての追加のパッチを指定します。 プロビジョニング中にこれらのパッチを追加するには、このセクションで patchadd ステートメントを追加します。

```
if [ "$OSVER" = "5.8" ] ; then
        echo "${ID}Install SUN patches"
        echo "${ID}mount -f nfs ${PATCH_LOCATION} ${A_ROOT}/mnt"
        mount -f nfs ${PATCH_LOCATION} ${A_ROOT}/mnt

        echo "${ID}patchadd -R ${A_ROOT} ${A_ROOT}/mnt/112438-03"
        patchadd -R ${A_ROOT} ${A_ROOT}/mnt/112438-03

        echo "${ID}patchadd -R ${A_ROOT} ${A_ROOT}/mnt/108434-22"
        patchadd -R ${A_ROOT} ${A_ROOT}/mnt/108434-22

        echo "${ID}umount ${A_ROOT}/mnt"
        umount ${A_ROOT}/mnt
```

パスワード、パッチの場所、CA IPC の調整可能なパラメータおよびオプションのパッチは、［終了］ファイルに設定されています。

JumpStart での SSH の設定

CA Server Automation JumpStart は、SSH サービスを使用して JumpStart クライアントと通信します。 このサービスが機能しないと、CA Server Automation は JumpStart クライアントをモニタしたり、制御することができません。 このサービスが JumpStart クライアント上で機能していない場合は、次のいずれかの方法でそれをインストールできます。JumpStart クライアント上で JumpStart を手動で実行するか、または JumpStart クライアント上でサービスをインストールして設定します。 JumpStart を使用して SSH をインストールして設定するには、JumpStart サーバがクライアントについて認識しており、JumpStart プロセスが JumpStart クライアント上で開始される必要があります。

手動の JumpStart プロビジョニングにクライアントを設定する方法

1. 以下のコマンドで sol_10/Solaris_10 を最上位リリースのオペレーティング システムのイメージへのパスで置換します。

   ```
   /image_parent/sol_10/Solaris_10/Tools/add_install_client ¥
   -s server_hostname:/image_parent/sol_8 ¥
   -p server_hostname:/config_parent/config_dir/Solaris_8 ¥
   -c server_hostname:/config_parent/config_dir/Solaris_8 ¥
   -e ethernet_address client_hostname client_class
   ```

   add_install_client シェル スクリプトは、パス名、イーサネットまたは MAC アドレス、ホスト名およびハードウェア クラスなどの JumpStart クライアントに関する情報を使用して /etc/bootparams を更新します。

2. 以下のコマンドを入力してイーサネット（MAC）アドレスを取得します。

   ```
   ifconfig –a
   ```

   注: このコマンドの出力は、先頭の 0 （複数可）が省略された MAC アドレスを表示します。 add_install_client スクリプトには、先頭の 0（複数可）が省略されていない MAC アドレスが必要です。 この MAC アドレスは、JumpStart サーバ上の /etc/ethers ファイルのエントリとも一致する必要があります。

3. 以下のコマンドを入力してノード名を取得します。 ホスト名はドメイン情報が含まれたノード名です。

   ```
   uname –n
   ```

4. 以下のコマンドを入力してコンピュータのハードウェア名（クラス）を取得します。

   ```
   uname –m
   ```

   JumpStart クライアントが追加されます。

5. ルートとしてログインし、以下のコマンドを入力します。

   ```
   reboot “net – install"
   ```

   JumpStart プロセスがクライアント上で開始されます。

注: SSH を手動で設定するための詳細については、www.sunfreeware.com の Solaris 8 セクションを参照してください。

CA Network Automation の設定

CA Network Automation では、企業内の Cisco Internetwork Operating System（Cisco IOS）を実行する Cisco ルータおよびスイッチを検出および管理できます。 また、検出されたネットワーク デバイスの追加、削除、および更新も可能です。 CA Network Automation は、管理対象のネットワーク デバイスへの追加の変更を実行するスクリプトを提供します。

CA Server Automation では、CA Network Automation スクリプトが *install-directory*¥nma_scripts フォルダ内に用意されています。

注: CA Network Automation スクリプトは、 スイッチおよびスイッチ-ルータ デバイス上（例： Cisco 5000 スイッチ ファミリ）で実行されることが想定されています。

この統合を使用するには、CA Network Automation があらかじめ設定され、スクリプトが NetMRI システムにインポートされている必要があります。これらのスクリプトを NetMRI システムにインポートするには、［設定管理］-［ジョブ管理］ページに移動して［インポート］をクリックします。

CA Network Automation サーバの設定

CA Server Automation から Network Automation スクリプトを実行するには、CA Server Automation と共に使用する CA Network Automation サーバを 1 つ設定します。

次の手順に従ってください：

1. CA Server Automation ユーザ インターフェースを開きます。
2. ［管理］モードで、［管理］-［設定］をクリックします。
3. ［ネットワーク/ストレージ］セクションで［Network Automation サーバ］をクリックします。
4. ［+］（追加）をクリックし、以下の情報を入力します。

   サーバ名

   CA Network Automation サーバの名前または IP アドレスを指定します。

   ユーザ名

   CA Network Automation サーバのユーザ名を指定します。

   パスワード

   CA Network Automation サーバ ユーザのパスワードを指定します。

   プロトコル

   CA Network Automation サーバにアクセスするために使用するプロトコルを指定します。

   デフォルト： HTTP

   ポート

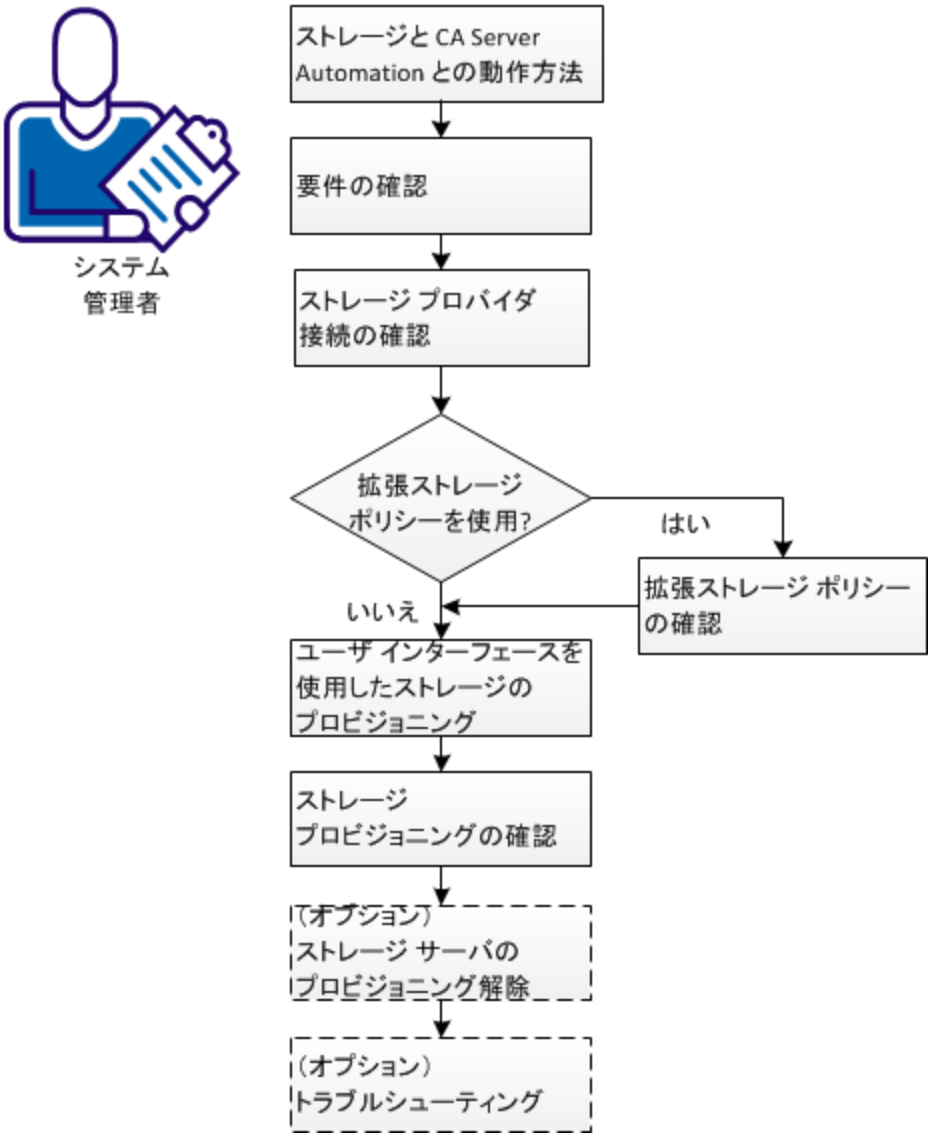
   CA Network Automation サーバによって使用されるポート番号を指定します。
5. ［OK］をクリックします。

CA Network Automation サーバが設定されます。

ストレージをプロビジョニングする方法

システム管理者のジョブには、仮想サーバおよび物理サーバについての CA Server Automation 内のストレージのプロビジョニングが含まれます。以下の図は、ストレージ デバイスのプロビジョニングに必要な手順を示します。

ストレージをプロビジョニングする方法

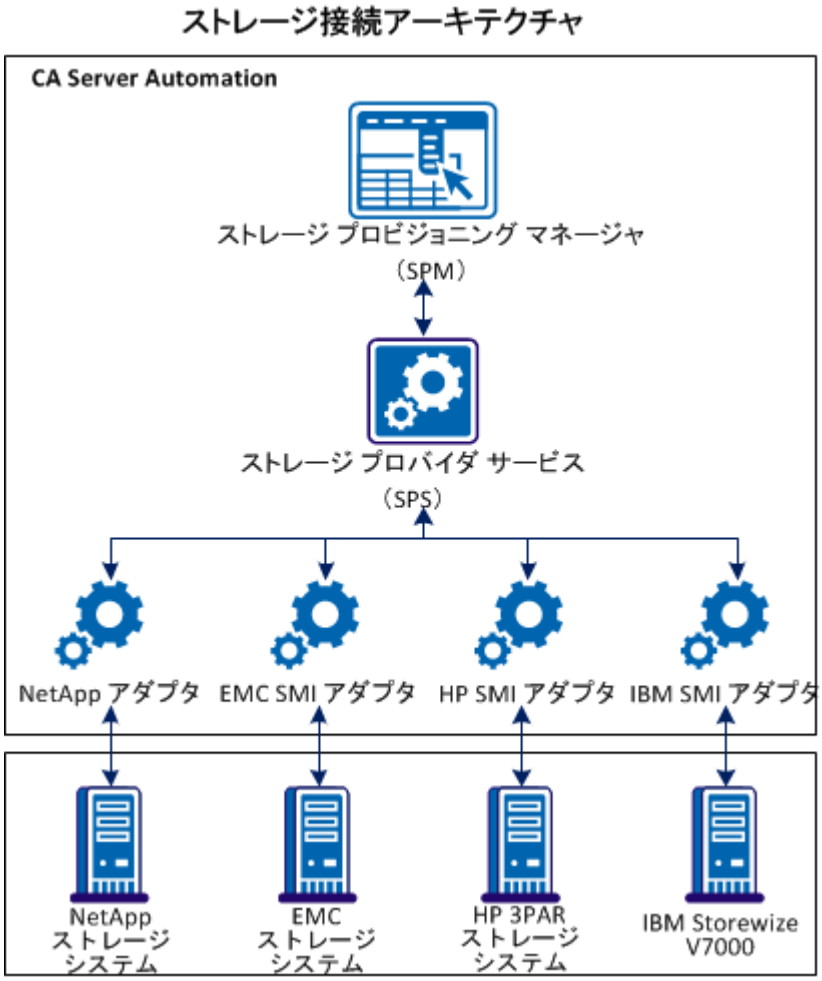


ストレージをプロビジョニングするには、以下の手順に従います。

1. ストレージと CA Server Automation との動作方法 (P. 723)
2. 要件の確認 (P. 726)
3. ストレージ プロバイダ接続の確認 (P. 727)
   a. ストレージ プロバイダ サーバ リストの表示 (P. 728)
   b. ストレージ プロバイダ サーバの追加 (P. 729)
   c. ストレージ プロバイダ接続の確認 (P. 729)
4. 拡張ストレージ ポリシーの確認 (P. 730)
   a. 拡張ストレージ ポリシー リストの表示 (P. 731)
   b. 拡張ストレージ ポリシーの追加 (P. 732)
5. ユーザ インターフェースを使用したストレージのプロビジョニング (P. 733)
6. ストレージ プロビジョニングの確認 (P. 734)
7. （オプション） ストレージのプロビジョニング解除 (P. 735)
8. （オプション） トラブルシューティング (P. 737)

ストレージと CA Server Automation との動作方法

以下の図は、CA Server Automation のストレージ アーキテクチャを示します。



以下プロセスは、ストレージが CA Server Automation と共にどのように作動するかについて説明します。

1. ストレージ プロビジョニング マネージャ（SPM）は、ストレージ プロバイダ サービス（SPS）とインタラクションを行って以下タスクを実行します。
   - ストレージ デバイスの接続
   - サーバ設定の検索
   - ストレージ ポリシーの管理
   - ストレージ ジョブの追跡
   - ポリシー データの提供
2. SPS は、ストレージ プロビジョニング要求を SPM から受信します。SPS は、NetApp アダプタや EMC SMI アダプタなど、対応するアダプタにこれらの要求を送信します。

   以下のストレージ デバイスが CA Server Automation でサポートされています。

   NetApp OnCommand

   以下のプロトコルがサポートされています。
   - SAN ベースの iSCSI
   - SAN ベースの FCP
   - NAS ベースの CIFS
   - NAS ベースの NFS

   以下のプロビジョニング メソッドが CA Server Automation マネージャでサポートされています。
   - ストレージ サービス（NetApp Provisioning Manager）
   - プロビジョニング ポリシー（NetApp Provisioning Manager）

   EMC SMI-S

   以下のプロトコルがサポートされています。
   - SAN ベースの iSCSI
   - SAN ベースの FCP

   以下のプロビジョニング メソッドが CA Server Automation マネージャでサポートされています。
   - EMC SMI-S

HP 3PAR

以下のプロトコルがサポートされています。

- SAN ベースの iSCSI
- SAN ベースの FCP

以下のプロビジョニング メソッドが CA Server Automation マネージャでサポートされています。

- HP SMI-S

IBM Storewize V7000

以下のプロトコルがサポートされています。

- SAN ベースの iSCSI
- SAN ベースの FCP

以下のプロビジョニング メソッドが CA Server Automation マネージャでサポートされています。

- IBM SMI-S

3. 論理ユニット番号（LUN）およびマネージャが作成され、イニシエータがアダプタを使用して登録されます。
4. SPM はホストにログインし、作成されたストレージに接続します。

要件の確認

ストレージ接続を設定する前に、以下の要件を確認します。

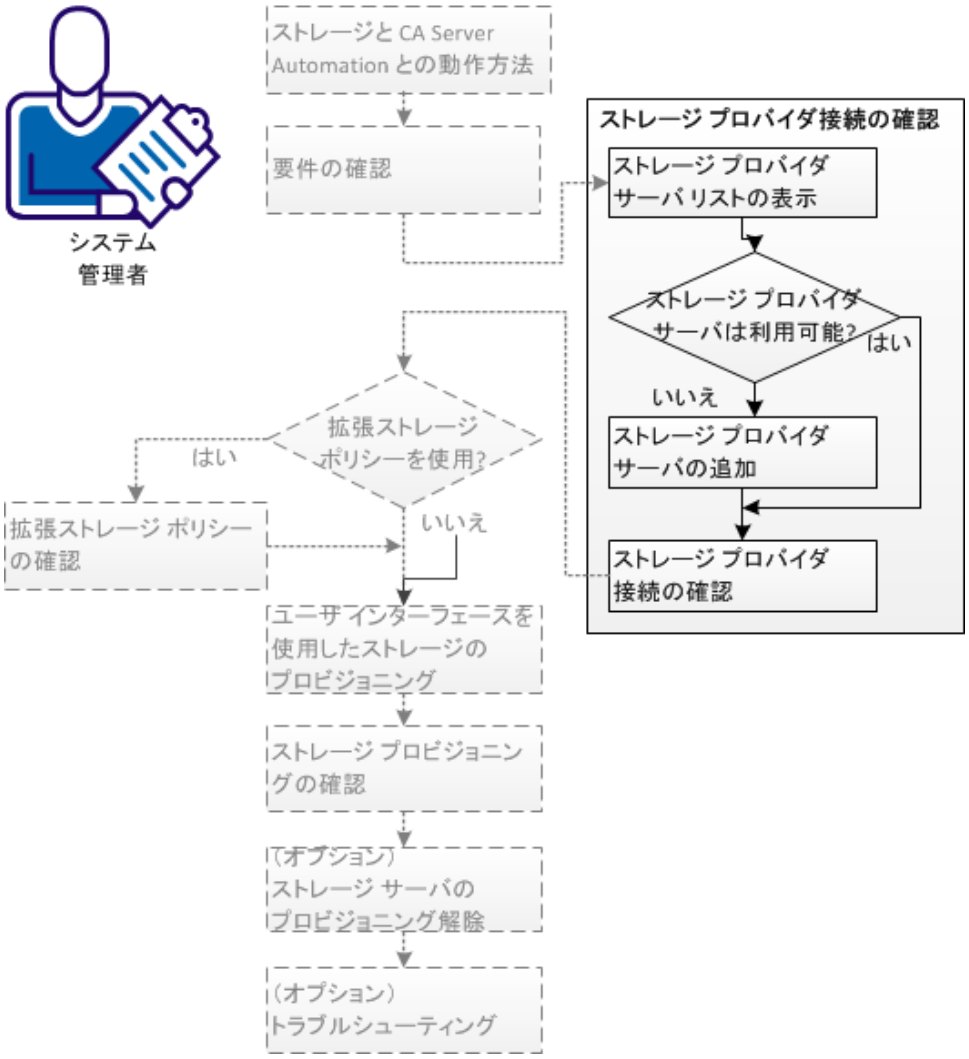
- 最新の CA Server Automation リリース ノートで、サポートされるストレージ アレイおよびストレージ サーバのバージョンを確認します。
- CA Server Automation およびプロビジョニング リソースに精通している必要があります。
- サポートされているストレージ サーバに対するマルチパスがイニシエータ上で設定されていることを確認します。
- iSCSI または ファイバ チャネル（FC）プロトコルがイニシエータ上で設定されていることを確認します。

  注: CA Server Automation は、Windows、AIX、HP-UX、および Solaris について iSCSI プロトコルをサポートします。 CA Server Automation は、VMware ESX、Red Hat Enterprise Linux、および SUSE Linux Enterprise Server について、iSCSI および FC プロトコルをサポートします。
- iSCSI および FC サービスがイニシエータ上で実行されていることを確認します。

ストレージ プロバイダ接続の確認

システム管理者は、必要なストレージ プロバイダ サーバがプロビジョニング用に利用可能かどうかを確認できます。 プロバイダが利用可能でない場合、プロバイダの接続ステータスを追加して確認できます。 以下の図は、ストレージ プロバイダ接続を確認する手順を示します。

ストレージをプロビジョニングする方法



ストレージ プロバイダ接続を確認するには、以下の手順に従います。

1. ストレージ プロバイダ サーバ リストの表示 (P. 728)
2. ストレージ プロバイダ サーバの追加 (P. 729)
3. ストレージ プロバイダ接続の確認 (P. 729)

ストレージ プロバイダ サーバ リストの表示

ストレージ プロバイダ サーバ リストを表示させて、プロビジョニングに利用可能なストレージ サーバを確認することができます。

次の手順に従ってください：

1. CA Server Automation アプリケーションにログインし、管理ビューを開きます。
2. ［管理］タブ、［設定］タブを選択し、［ストレージ プロバイダ］をクリックします。

   ［ストレージ設定］ページに、利用可能なストレージ プロバイダ リストが表示されます。

   注: プロバイダがリストにない場合は、リストにプロバイダを追加します。 詳細については、「ストレージ プロバイダ サーバの追加 (P. 729)」を参照してください。

ストレージ プロバイダ サーバの追加

ストレージ プロバイダ サーバをユーザ インターフェースに追加して、利用可能なストレージ プロバイダのリストにストレージ プロバイダの名前を表示させます。

次の手順に従ってください：

1. ［ストレージ プロバイダ］ペイン ツールバー上のアイコン をクリックします。

   新規ストレージ プロバイダの追加用ダイアログ ボックスが開きます。

2. プロバイダ、サーバ名、ユーザ名、およびパスワードなどの必要な情報を入力します。

   注:

   - ユーザには、ストレージ サーバに対する管理者権限が必要です。
   - IBM SMI-S は HTTPS プロトコルのみをサポートします。

3. ［OK］をクリックします。

   新しいストレージ プロバイダ サーバがストレージ プロバイダのリストに追加されます。

ストレージ プロバイダ接続の確認

ストレージ プロバイダ接続を確認し、ストレージ サーバにプロビジョニングの準備ができているかを確認します。

次の手順に従ってください：

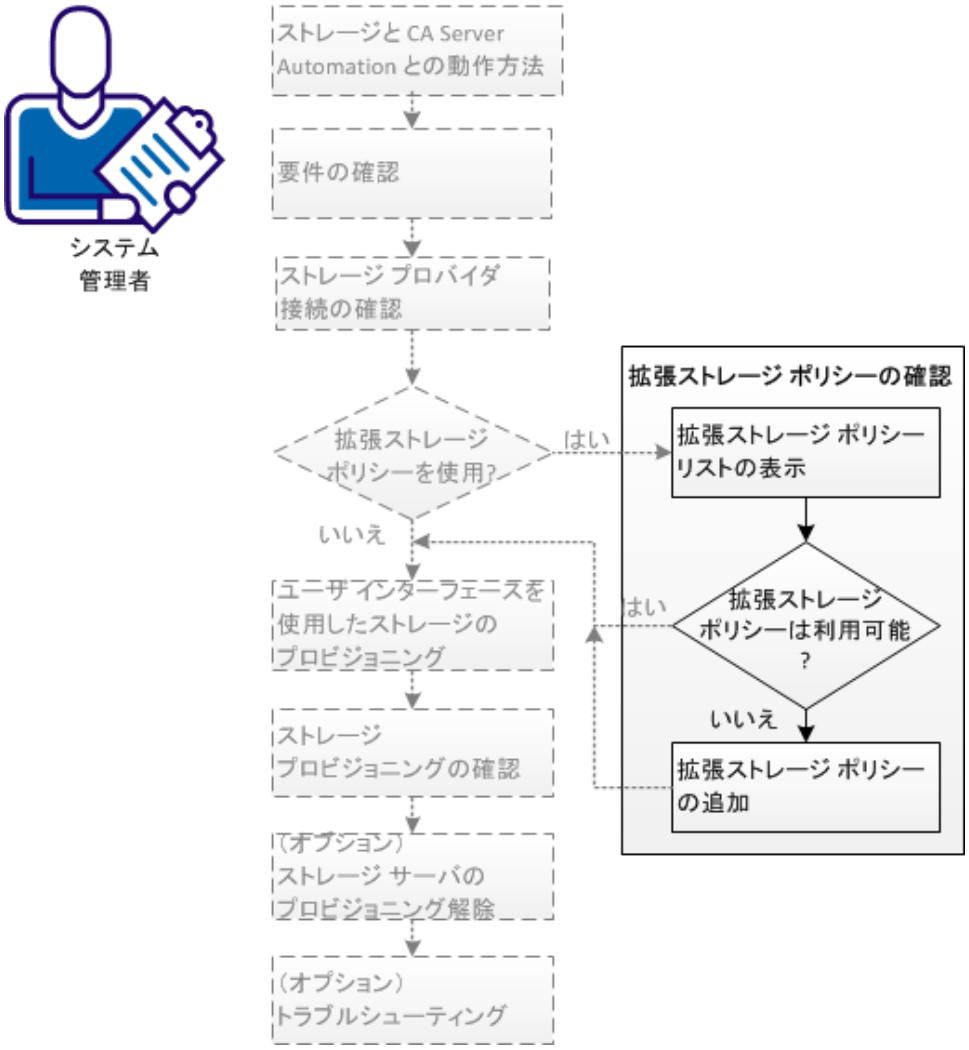
1. ［ストレージ プロバイダ］ペインの［ステータス］列を表示します。
2. 以下のステータスを確認します。

   - ストレージ プロバイダ サーバに対して アイコンが［ステータス］列に表示される場合は、マネージャとの接続が確立されています。
   - ストレージ プロバイダ サーバに対して アイコンが［ステータス］列に表示される場合は、マネージャとの接続が確立されていません。 アイコンの上にポインタを置いてエラー メッセージを表示させ、エラーの解決に必要なアクションを実行吸います。

拡張ストレージ ポリシーの確認

システム管理者は、仮想サーバまたは物理サーバに対するストレージのプロビジョニングのために拡張ストレージ ポリシーを作成できます。 拡張ストレージ ポリシーには、ストレージをプロビジョニングするための、プロビジョニング メソッドなどの事前定義済みメソッド、ストレージ プロバイダ サーバ タイプ、プロトコル タイプ、およびポリシー属性などが含まれます。 以下の図は、拡張ストレージ ポリシーを確認する方法を示します。

ストレージをプロビジョニングする方法



拡張ストレージ ポリシーを確認するには、以下の手順に従います。

1. 拡張ストレージ ポリシー リストの表示 (P. 731)
2. 拡張ストレージ ポリシーの追加 (P. 732)

拡張ストレージ ポリシー リストの表示

ポリシーの可用性を確認するために、拡張ストレージ ポリシーを表示させることができます。 ポリシーが存在しない場合は、ストレージをプロビジョニングするポリシーを作成できます。

次の手順に従ってください：

1. CA Server Automation マネージャにログインし、管理ビューを開きます。
2. ［リソース］タブをクリックし、［エクスプローラ］ペインから［データ センター］を選択します。

   ［データ センター クイック ビュー］ページが表示されます。
3. ［ポリシー］タブをクリックし、次に、［ストレージ］タブをクリックします。

   利用可能な拡張ストレージ ポリシーのリストが表示されます。
4. （オプション）拡張ストレージ ポリシーを編集するには、その拡張ストレージ ポリシーに対応する［アクション］列の アイコンをクリックします。

   注: サーバ固有の拡張ストレージ ポリシーを表示するには、左ペインのツリーでサーバを選択します。 右ペインから［ポリシー］タブをクリックし、次に［ストレージ］タブを選択します。

拡張ストレージ ポリシーの追加

必要な要件を備えたストレージのプロビジョニング用に、拡張ストレージ ポリシーを追加できます。

次の手順に従ってください：

1. CA Server Automation マネージャにログインし、管理ビューを開きます。
2. ［リソース］タブをクリックし、［エクスプローラ］ペインから［データ センター］を選択します。

   ［データ センター］クイック ビュー ページが表示されます。
3. ［ポリシー］タブをクリックし、次に、［ストレージ］タブをクリックします。

   利用可能な拡張ストレージ ポリシーのリストが表示されます。
4. ［拡張ストレージ ポリシー］ペイン ツールバー上の アイコンをクリックします。

   ［新しい拡張ストレージ ポリシーの作成］ウィザードが開きます。
5. ウィザードに従って、拡張ストレージ ポリシーを作成します。

   注: サーバ固有の拡張ストレージ ポリシーを追加するには、左ペインのツリーでサーバを選択します。右ペインから［ポリシー］タブ、［ストレージ］タブをクリックします。

ユーザ インターフェースを使用したストレージのプロビジョニング

仮想サーバおよび物理サーバにストレージを割り当てるユーザ インターフェースを使用して、ストレージをプロビジョニングできます。

次の手順に従ってください：

1. CA Server Automation マネージャにログインし、管理ビューを開きます。
2. ［リソース］タブをクリックし、エクスプローラ ペインから［データセンター］-［CA Server Automation サービス］を選択します。

   利用可能な仮想サーバと物理サーバのリストが表示されます。
3. セットアップするサーバを右クリックし、［プロビジョニング］-［ストレージ プロビジョニング］を選択します。

   ストレージのプロビジョニング ウィザードが表示されます。
4. ウィザードに従って、ストレージ プロビジョニングを実行します。

   ストレージは、割り当てられた仮想サーバまたは物理サーバにプロビジョニングされます。

   注: ストレージ接続が確立されていない場合は、エラー メッセージを確認し、適切なアクションを実行します。

ストレージ プロビジョニングの確認

プロビジョニングされたストレージが動作しており、使用準備ができているかどうかを確認するために、ストレージ プロビジョニングを確認することができます。

Windows プラットフォームでストレージ プロビジョニングを確認する方法

a. プロビジョニングされたコンピュータにログインし、マイ コンピュータを開きます。

b. 新しいハード ディスク ドライバが作成されており、ハード ディスク ドライバのリストに表示されていることを確認します。

注: 新しいディスクを利用可能にするには、それをフォーマットします。

Linux/UNIX プラットフォームでストレージ プロビジョニングを確認する方法

a. プロビジョニングされたコンピュータにログインし、mount コマンドを実行します。

b. コマンドの出力に、マウントされたデバイスがマウント ポイントと共に一覧表示されることを確認します。

c. マウント ポイント フォルダに移動し、マウント ポイントに lost+found フォルダが表示されることを確認します。

（オプション）ストレージのプロビジョニング解除

cadpmspm deprovision コマンドを使用して、イニシエータ用の既存のプロビジョニングされたストレージをプロビジョニング解除します。 プロビジョニング解除すると、ストレージ サーバで作成された LUN が削除されます。

注: ディスカバリ、サイズ変更、接続など、他のストレージ タスクを実行するには、cadpmspm CLI コマンドを使用します。

次の手順に従ってください：

1. ［スタート］-［すべてのプログラム］-［CA］-［CA Server Automation］をクリックし、CA Server Automation コマンド プロンプトを開きます。
2. cadpmspm deprovision コマンドを実行して、LUN を削除します。

cadpmspm コマンドの形式は、以下のとおりです。

```
cadpmspm –deprovision
-dataset=DatasetName
[-stsrv=StorageServer -stplat=StoragePlatform]
[-ws_user=username -ws_password=password]
[-locale iso639value]
```

-dataset=*DatasetName*

イニシエータに接続されたデータ セットの名前（LUN）を指定します。データ セットの名前を取得するには、以下のいずれかの手順を実行します。

- ユーザ インターフェースを開き、［管理］ -［リソース］に移動します。 エクスプローラ ツリーの［データ センター］をクリックし、［ユーザ リソース］を開き、［ストレージ］を選択します。データ セット名は［名前］列に一覧表示されます。
- 管理者権限で CA Server Automation サーバにログインし、［スタート］メニューから CA Server Automation コマンド プロンプトを起動します。 以下のコマンドを実行します。

  ```
  cadpmspm.exe -discover -detail=0 -sttype=9 -stplat=StoragePlatform
  ```

  利用可能な値について、stplat パラメータの説明を参照します。

-stsrv=*StorageServer*

（オプション）ストレージ プロバイダ サーバ名を指定します。

-stplat=*StoragePlatform*

（オプション）ストレージ プラットフォームを指定します。設定可能な値は以下のとおりです。

1

ストレージ プラットフォームとして NetApp を指定します。

2

ストレージ プラットフォームとして EMC を指定します。

3

ストレージ プラットフォームとして HP を指定します。

4

ストレージ プラットフォームとして IBM を指定します。

デフォルト： 1

-ws_user *username* -ws_password *password*

（オプション）Web サービスのセキュリティ チェックで使用する認証情報を指定します。 認証情報が含まれていない場合、入力が求められます。 caaipsecurity を使用して独自のセッションをセット アップすることにより、認証情報のプロンプトを回避します。

-ws_user *username* -ws_password *password*

（オプション）Web サービスのセキュリティ チェックで使用する認証情報を指定します。 認証情報が含まれていない場合、入力が求められます。 caaipsecurity を使用して独自のセッションをセット アップすることにより、認証情報のプロンプトを回避します。

-locale *iso639value*

（オプション）デフォルトの英語出力より優先させるロケールを、ISO 639_3166 の組み合わせ（たとえばフランス語の場合は fr_FR）で指定します。コマンド プロンプトのロケールを使用する場合は「native」を指定します。

例:

以下の例では、IBM SMI-S ストレージをプロビジョニング解除する方法を示します。

```
cadpmspm -deprovision -dataset=vm4953720121121020542
-stplat=4 -stsrv=192.168.178.142 -ws_user=admin -ws_password=admin
```

(オプション)トラブルシューティング

関連項目:

HP ストレージの正確なディスク空き領域を取得できない (P. 737)
vCenter ストレージのプロビジョニング時に、エクスポートされた LUN を検出できない (P. 737)
プロビジョン ウィザードでストレージ プロバイダ接続が失敗する (P. 738)
新しい iSCSI ディスクの検出に失敗する (P. 738)

HP ストレージの正確なディスク空き領域を取得できない

症状

CA Server Automation マネージャから HP ストレージ プールで利用可能な正確なディスク空き領域を検出できません。

解決策

CA Server Automation で、HP ストレージで作成された共通プロビジョニング グループに対して増加制限が設定されているかどうかを確認します。デフォルト値は 1024T です。

vCenter ストレージのプロビジョニング時に、エクスポートされた LUN を検出できない

症状

vCenter プラットフォームのストレージのプロビジョニング時、エクスポートされた LUN の検出に失敗したというエラーが表示されます。

解決策

vCenter プラットフォームのストレージをプロビジョニングする際に、ターゲット ポータルを手動で追加します。HP および IBM のストレージ デバイスのターゲット ポータルが vCenter 環境に追加されていることを確認します。

プロビジョン ウィザードでストレージ プロバイダ接続が失敗する

症状

ストレージのプロビジョニング中、［プロビジョニング メソッドの選択］ダイアログ ボックスでストレージ プロバイダ接続が失敗したというエラーが表示されます。［ストレージ システム］フィールドに「利用可能なデータがありません」と表示されます。

解決策

ストレージ セキュリティ ポリシーに従い、CA Server Automation ログイン認証情報を使用してストレージ プロバイダを設定しているかどうかを確認します。

新しい iSCSI ディスクの検出に失敗する

症状

ストレージのプロビジョニング中、新しい iSCSI ディスクの検出に失敗したというエラーが表示されます。

解決策

ネットワークまたはコンピュータ環境が遅いとき、このエラーが発生します。

次の手順に従ってください：

1. *Install_path*¥ServerAutomation¥conf フォルダに移動し、caspmconf.cfg ファイルを編集用に開きます。
2. 以下のパラメータに新しい値を設定します。
   - CONNECTOR_MAX_RETRY_TIMES
   - CONNECTOR_ACTION_POLLING_INTERVAL

   ファイルを保存して閉じます。
3. 再度ストレージをプロビジョニングします。

Software Delivery を設定する方法

Software Delivery サービスを使用すると、CA Server Automation 内の管理対象システムにソフトウェアを展開したり、パッチを適用したりすることができます。

1. SDAdapter サービスが実行されていることを確認します（［管理］-［設定］ページ、［サービス］リスト）。

   SDAdapter サービスが実行されていない場合は、Software Delivery サーバを設定します。SDAdapter サービスが自動的に起動されます。

2. 各 CA ITCM インスタンスが 1 つの CA Server Automation インスタンスによる管理用に設定されていることを確認します。設定されていない場合、プロビジョニングが失敗する場合があります。

3. Active Directory を使用している場合は、認証の前に外部ディレクトリとして使用するように Software Delivery サーバを設定します。

注: Windows ドメイン アカウントを使用する場合、ユーザは管理者グループ（利用できるすべてのセキュリティ オブジェクト クラスへのフル コントロール アクセス クラスの権限を持つ）のメンバであるローカル ユーザ、またはローカル管理者グループのメンバでもあるドメイン アカウントのいずれかになります。

CA Process Automation でのプロセスの自動化

CA Process Automation はルーチン管理タスクを自動化し、操作の効率およびインシデント対応処理を改善すると共に、ベスト プラクティスおよび規制管理コンプライアンスを保証します。CA Process Automation は以下に示すような多数のプロセスを自動化して管理できます。

- アプリケーションのモニタリングと再起動
- 惨事復旧
- 仮想インフラストラクチャ管理
- 情報技術インフラストラクチャ ライブラリ（ITIL）コンプライアンス
- セキュリティ
- ディスカバリ
- 変更の検出
- プロビジョニング
- パフォーマンス モニタリング
- ストレージ プロビジョニング

CA Process Automation の CA Server Automation との統合は、CA Server Automation がアクティブにしたプロセスをシステム管理者に設定させて管理させるグラフィカル ユーザ インターフェースを提供することによって、ルールとアクションの処理を向上させます。CA Process Automation は、これらのプロセスを使用して操作上のプロセスを自動的に実行します。CA Process Automation は、さらにオペレータやその他のユーザが自動プロセスのスケジュール、開始、およびモニタリングできるようにするクライアント アプリケーションもサポートします。

一般的な使用シナリオを以下に示します。

- 管理者は、指定の日時またはサーバ上で特定のメトリックが到達した場合に 1 つまたは複数の仮想マシンのプロビジョニングが必要なルールを設定します。
- このルールは、CA Server Automation の CA Process Automation との連結をアクティブにし、そのサーバ上ですでに設定されているプロセスをトリガします。
- プロセスが終了すると、イベントは CA Server Automation に送信され、利用可能な場合は、Service Desk チケットが作成されます。

CA Process Automation の前提条件

CA Process Automation を使用する前に、以下の要件が満たされていることを確認します。

- CA Server Automation、CA Process Automation、CA EEM の最新版および JRE の公開版がインストールされている。
- CA Process Automation サーバが設定されている。
- CA Process Automation はシングル サインオンに設定されている（P. 741）。
- CA Process Automation Web サービスへのアクセスが有効になっている。

注: コンポーネントのインストールをスキップした場合は、dpmutil コマンド ライン ユーティリティまたは［管理］、［設定］ページを使用して、後でコンポーネントを設定できます。dpmutil の詳細については、「*リファレンス ガイド*」を参照してください。

シングル サインオン用の CA Process Automation の設定

CA Process Automation サーバに対するシングル サインオン用の CA Server Automation サーバを指定します。 シングル サインオンを使用するには、CA EEM を使用して CA Process Automation を設定する必要があります。

シングル サインオン用に CA Process Automation および CA EEM を設定するには

1. CA Process Automation サーバで CA EEM UI にログインします (P. 36)。
2. CA EEM UI の［ID の管理］-［グループ］で、必要なグループとユーザが使用可能であることを確認します。
3. ユーザのパスワードを希望するパスワードにリセットします。
4. インストールされた CA Process Automation 上でドロップダウン リストから EEM を選択し、以下のフィールドを指定します。

   EEM サーバ

   CA EEM サーバのホスト名を示します。

   例： itpamserver.itpam.ca.local

   EEM アプリケーション名

   CA EEM アプリケーションのインスタンス名を示します。

   例： ITPAM

   EEM 証明書ファイル

   証明書ファイルのフル パスを示します。

   例： C:¥Program Files¥CA¥PAM¥server¥c2o¥.c2orepository¥public¥certification¥PAM.p12

   EEM 証明書パスワード

   証明書ファイルのパスワードを示します。

   例： itpamcertpass

   CA EEM のセキュリティ設定が完了しました。

CA Process Automation ユーザ インターフェースへのアクセス

すべての CA Process Automation 機能（設計、展開、モニタ、制御、および監査）が、単一のブラウザベース UI から使用できます。ログイン後、ホーム ページで CA Process Automation のドキュメントを参照することもできます。［スタート］メニュー ショートカットは CA Process Automation サーバでのみ利用可能です。 個別のサーバからインターフェースにアクセスするユーザは、Web ブラウザで URL を入力する必要があります。 また、CA Server Automation UI から CA Process Automation クライアントのユーザ インターフェースにアクセスすることもできます。

次の手順に従ってください:

1. CA Process Automation サーバで、［スタート］-［プログラム］-［CA］-［CA Process Automation ドメイン］-［CA Process Automation を開始］の順に選択します。

   CA Process Automation ページが以下の URL で表示されます。

   `https://servername:port/itpam`

   servername

   CA Process Automation ユーザ インターフェースがインストールされているサーバの名前を示します。

   port

   サーバのリスニング ポートを指定します。

   デフォルト： 8080

2. 管理者ログイン認証情報を入力し、［ログイン］をクリックします。

   CA Process Automation のホーム ページが表示されます。このインターフェースを使用してプロセスを設定します。

CA Process Automation プロセスの設定

CA Process Automation プロセスはアクションの視覚的な説明を提供します。プロセスのどこにいるかが正確に分かります。また、複数のアクションのインスタンスを表示できます。CA Process Automation プロセスを設定する前に、アクション (P. 839)とルールを最初に作成します。ルールはマッピングされ、プロセスをトリガします。 ルールとアクションを作成し、CA Server Automation UI からプロセスを設定します。

CA Process Automation プロセスを設定する方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［データ センター］ノードを選択します。
4. ［ポリシー］をクリックし、次に、［アクション］をクリックします。

   ［アクション］ページが表示されます。

5. ツールバーの［+］（新規）をクリックします。

   ［アクションの定義: 新規］ページが表示されます。

6. ［アクション名］テキスト ボックスに意味のあるアクションの名前を入力し、ドロップダウン リストから［Run CA Process Automation Process］を選択します。

   ［詳細］セクションが表示されます。

7. ［アクションの開始］ドロップダウン リストで以下の設定のいずれか *1* つを選択します。

   遅延なし

   そのアクションを使用するルールが再度トリガされた場合に同じアクションをすぐに再実行できるように指定します。

   遅延時間

   そのアクションを使用するルールが再度トリガされた場合に同じアクションを再実行するまでに経過させる必要のある時間の量を指定します。

   制限： 秒

   注: スケジュール済みジョブがアクションを実行する場合は、［アクションの開始］設定に効力はありません。

8. ［アクションの完了］ドロップダウン リストで以下の設定のいずれか 1 つを選択します。

   待機なし

   アクション シーケンスで次のアクションが実行される前に完了するアクションに対して待機しないように指定します。

   最大待機時間

   アクション シーケンスで次のアクションが実行される前に完了するアクションに対して最大待機時間を指定します。

   完了まで待機

   アクション シーケンスで次のアクションが実行される前に完了するアクションに対して完了まで待機するように指定します。

   注: ［アクションの完了］ドロップダウン リストは、長期に実行されるアクションにのみ表示されます。

9. ドロップダウン リストからプールを選択します。フォームでインターフェースを作成できるため、ユーザは起動時にプロセスを開始して、そのプロセスに適切な入力を行うことができます。

   必須入力フィールドは、選択したフォームによって異なります。

10. すべての入力フィールドに入力します。

    注: 接続パラメータは CA Process Automation に設定されています。 CA Server Automation URL はサービス コントローラを識別します。これは［管理］ページの下部の［設定］リストに表示されます。

11. （オプション）［CA Process Automation クライアントのプロセスを開く］をクリックして CA Process Automation にログインし、プロセス定義を表示します。
12. チケットがサードパーティによる承認が必要な場合は、［ヘルプ デスク承認］チェック ボックスをオンにします。

    注: CA SDM を正しく設定してこのオプションを使用します。

    ［チケット タイプ］および［テンプレート］フィールドが有効になります。
13. チケットが承認された後でそれを自動的に閉じる場合は、［承認または拒否時にチケットを自動的にクローズ］チェック ボックスをオンにします。
14. ［チケット タイプ］ドロップダウン リストからチケット タイプを選択します。 以下のタイプが有効なオプションですが、設定によって異なります。

    - インシデント
    - 問題
    - 要求

    ［テンプレート］ドロップダウン リストは選択したチケット タイプに関連付けられたテンプレートで更新されます。
15. ［テンプレート］ドロップダウン リストからテンプレートを選択します。

    使用しているチケット モデルに応じて事前定義された値が各フィールドに入力されます。
16. ［アクション］ドロップダウン リストから［保存］を選択します。

    確認メッセージにより、正常に保存されたことが通知されます。

    注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。 スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

関連項目:

アクション タイプ (P. 842)

イベント転送

このセクションでは、SNMP（簡易ネットワーク管理プロトコル）管理サーバまたはサード-パーティ SNMP 管理サーバにイベントを転送するように CA Server Automation を設定する方法について説明します。

SNMP 用の Windows の設定

SNMP サービスおよび SNMP トラップ サービスは Windows と共にインストールされますが、典型的なセットアップの一部ではありません。 SNMP サービスおよびトラップ サービスが実行されていることを確認してください。

SNMP 用に Windows を設定する方法

1. ［スタート］-［コントロール パネル］-［管理ツール］-［サービス］をクリックします。

   ［サービス］ダイアログ ボックスが表示されます。

2. 以下のうち、*1* つを指定します。

   - SNMP サービスと SNMP トラップ サービスがリストに含まれる場合は、［イベント転送］設定を続行します。
   - SNMP サービスと SNMP トラップ サービスがリストに*含まれない*場合は、手順 3 から続行します。

3. ［スタート］-［コントロール パネル］-［プログラムの追加と削除］-［Windows コンポーネントの追加と削除］をクリックします。

   ［Windows コンポーネント ウィザード］ダイアログ ボックスが表示されます。

4. リストを下へスクロールし、［管理とモニタ ツール］を選択して［次へ］をクリックします。

   Windows インストール メディアを使用するよう求められます。

5. 画面上の指示に従って、インストールを実行します。

6. 手順 1 を繰り返して、SNMP サービスと SNMP トラップ サービスが実行されていることを確認します。

sysedge.cf ファイルの編集による SNMPv1 トラップの設定

SystemEDGE¥data¥port<n> ディレクトリにある sysedge.cf ファイルには、SNMPv1 トラップ コミュニティの定義が含まれており、これが、SNMPv1 トラップ メッセージの送信先を SystemEDGE に指示します。 SystemEDGE のインストール中に、または sysedge.cf ファイルの編集によって、トラップ送信先および SNMPv1 コミュニティを設定できます。任意の数の管理システムにトラップを送信するようにエージェントを設定できます。

重要: モニタ対象サーバ上の sysedge.cf ファイルを編集する前に、SystemEDGE が管理対象外モードで実行されている、つまり、サーバが［ポリシー設定］で登録されていないことを確認してください。SystemEDGE が管理対象モードで実行されている場合は、CA Server Automation の［ポリシー設定］で変更を上書きできます。

sysedge.cf を編集して SNMPv1 トラップを設定する方法

1. *SE_Install_Dir*¥data¥port<*num*> ディレクトリ（Windows）または *SE_Install_Dir*/config/port<*num*> ディレクトリ（UNIX、Linux）に移動して、sysedge.cf ファイルのバックアップ コピーを作成します。
2. テキスト エディタで sysedge.cf を開き、ファイルの上部でトラップ送信先セクションを見つけます。

   トラップ送信先セクションには、トラップ送信先およびコミュニティの簡単な説明が含まれます。
3. SNMPv1 トラップを送信する管理システムごとに、トラップ送信先セクションの最後に行を追加します。 構文は以下のとおりです。

   `trap_community` *`community-name`* `[IP-`*`address`*` | `*`hostname`*`] [`*`port-number`*`]`

   community-name

   SNMP コミュニティを指定します（public や admin など）。

   IP-address

   （オプション）ターゲット システムの IP アドレスを指定します。

   デフォルト： 127.0.0.1

hostname

（オプション）ターゲット システムの名前を指定します。

デフォルト： localhost

port-number

（オプション）トラップの送信先のポートを指定します。

デフォルト： 162

4. ファイルを保存して閉じます。
5. 以下のいずれかのオプションを実行します。
   - Windows サービス コントロールから SystemEDGE サービスを再起動して SystemEDGE を再起動し、変更をアクティブにします。
   - Windows コマンド プロンプトから以下のコマンドを実行して SystemEDGE を再起動し、変更をアクティブにします。

     ```
     net stop sysedge
     net start sysedge
     ```

   - UNIX または Linux 端末のウィンドウから以下のコマンドを実行して SystemEDGE を再起動し、変更をアクティブにします。

     ```
     /etc/init.d/sysedge restart （Linux、Solaris）
     /etc/init.d/sysedge restart （HP-UX）
     /etc/rc.d/sysedge restart （AIX）
     ```

例

sysedge.cf に以下の行を追加して、mycommunity というコミュニティ名のトラップを 2 つのシステムに送信します。 最初のシステムの IP アドレスは 192.168.5.26 です。 2 番目のシステムはホスト atlanta-noc で、ポート番号 1692 でリスンします。

```
trap_community mycommunity 192.168.5.26
trap_community mycommunity atlanta-noc 1692
```

注: sysedge.cf が定義するのは SNMPv1 トラップ コミュニティのみです。SNMPv2c または SNMPv3 トラップの設定については、*SE_Install_Dir*¥doc ディレクトリ（Windows）または /opt/EMPsysedge/doc ディレクトリ（UNIX、Linux）にインストールされた「*SystemEDGE ユーザ ガイド*」を参照してください。

イベント転送のための CA Server Automation の設定

CA またはサードパーティ SNMP Event Manager にイベントを転送するように製品を設定します。 この処理は、次の 2 つの部分で構成されます。

1. CA Server Automation のトラップまたはイベントを受信するためにイベント マネージャを設定します。
2. イベントを転送するために CA Server Automation を設定します。

以下の手順では、イベントを受信するためにイベント マネージャのコンソールを設定したと想定しています。

次の手順に従ってください:

1. CA Server Automation ユーザ インターフェースを開きます。
2. ［管理］をクリックします。

   ［管理］ページが表示されます。
3. ［設定］をクリックします。

   ［設定］ページが表示されます。
4. 左側のペインで［イベント］をクリックします。

   ［イベント］ペインが表示されます。
5. + （追加する）をクリックします。

   ［転送］および［タイプ］フィールドが自動的に入力されています。

   注: これらのフィールドが入力されていない場合は、Apache Tomcat を再起動してください。
6. ［サーバ］フィールドに管理サーバの名前を入力します。
7. SNMP 用の別のポート番号を入力するか、デフォルト ポート 162 （自動的に入力されている）のままにします。
8. ［OK］をクリックします。

   確認メッセージが表示されます。
9. ［保存］をクリックして、更新されたイベント転送レコードを保存します。

   設定が更新されて、設定情報が表示されます。 これで、CA Server Automation が、イベントを転送するように設定されました。

SNMP V3 エンジン ID

SNMPv3 標準では、各エンジン（トラップ送信者）に ID が必要です。 各管理プラットフォーム（ターゲット アプリケーション）は、エンジン ID を異なる方法で認識します。 CA Server Automation など、一部の管理プラットフォームでは、実際の 16 進数のエンジン ID が正しく設定されている必要があります。

CA Server Automation の場合は、16 進数のエンジン ID が、コンピュータ名と文字列 DCAMTrap の組み合わせをシードとして使用して構築されます。 たとえば、コンピュータ名が COMP999 の場合、エンジン ID のシードは COMP999-DCAMTrap です。 CA Server Automation は、アルゴリズムでシードを使用してエンジン ID を計算します。 コンピュータ名は、一意性を確保するために使用されます。 16 進数値は、CA Server Automation インストール ディレクトリの下の出力ファイルに書き込まれます。 このファイルの名前は dem_snmp3_engine_id.dat です。 このファイルは、別の管理サーバにイベントを転送するように CA Server Automation を設定した後に作成されます。

SNMP 管理サーバの設定

管理サーバを設定して SNMP トラップを受信します。

CA Spectrum IM

SNMP トラップを受信するように CA Spectrum を設定する方法については、「*CA Spectrum SNMPv3 ユーザ ガイド*」を参照してください。

第 8 章: クラスタおよび仮想デスクトップのモニタリング

このセクションには、以下のトピックが含まれています。

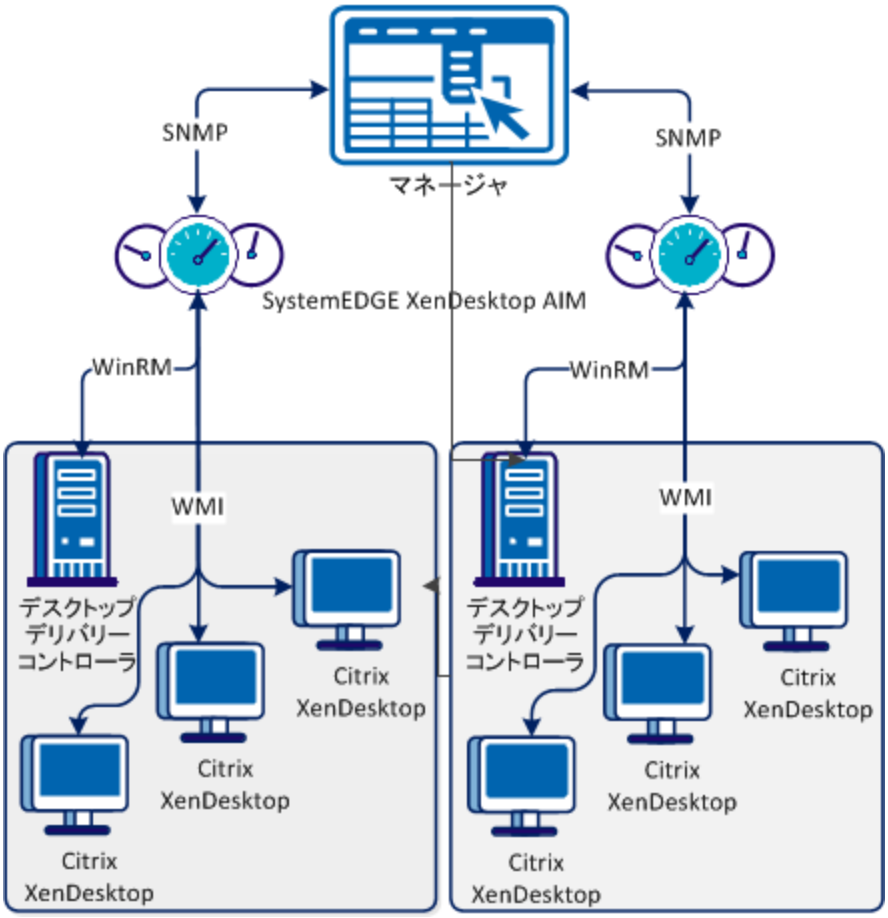
Citrix XenDesktop 環境

CA Server Automation は Citrix XenDesktop 環境をリモートでモニタします。Citrix XenDesktop AIM は統計データを提供し、Citrix XenDesktop 環境内の問題の検出を容易にします。

Citrix XenDesktop 管理コンポーネント間のインタラクション

以下の図は、Citrix XenDesktop 管理に関与するコンポーネントがどのように対話するかを示しています。 AIM サーバとは、SystemEDGE および XenDesktop AIM が稼働する Windows サーバです。 XenDesktop AIM と Citrix XenDesktop コントローラの間の通信には、Windows リモート管理（WinRM）を使用します。XenDesktop AIM とユーザの環境内の Citrix XenDesktop の間の通信には、WMI を使用します。 CA Server Automation は複数の Citrix XenDesktop コントローラに接続でき、Citrix XenDesktop 環境全体を把握することができます。

Citrix XenDesktop 管理コンポーネント間のインタラクション



Citrix XenDesktop コントローラの必要な接続情報を追加するには、以下の方法を使用します。

- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

接続情報は管理対象ノード上の設定ファイルに書き込まれます。XenDesktop AIM は設定ファイルをポーリングし、Citrix XenDesktop コントローラを介して、あるいは Citrix XenDesktop から直接、Citrix XenDesktop 環境のモニタリングを開始します。

Citrix XenDesktop の前提条件

- XenDesktop AIM のインストールには、以下の一覧表示された前提条件が必要です。

  注: Windows Management Framework の詳細については、Microsoft サポート技術情報の記事 968929 を参照してください。

信頼済みホスト リストへのマシン名の追加

Citrix XenDesktop が別のドメイン内にある場合は、AIM マシン上の WinRM サービス用に、マシン名を信頼済みホスト設定に追加します。

以下のコマンドを使用します。

```
set-Item wsman:¥localhost¥client¥trustedhosts machine_dnsname
```

machine_dnsname

XenDesktop AIM が接続するコンピュータの完全な DNS 名のリストを指定します。

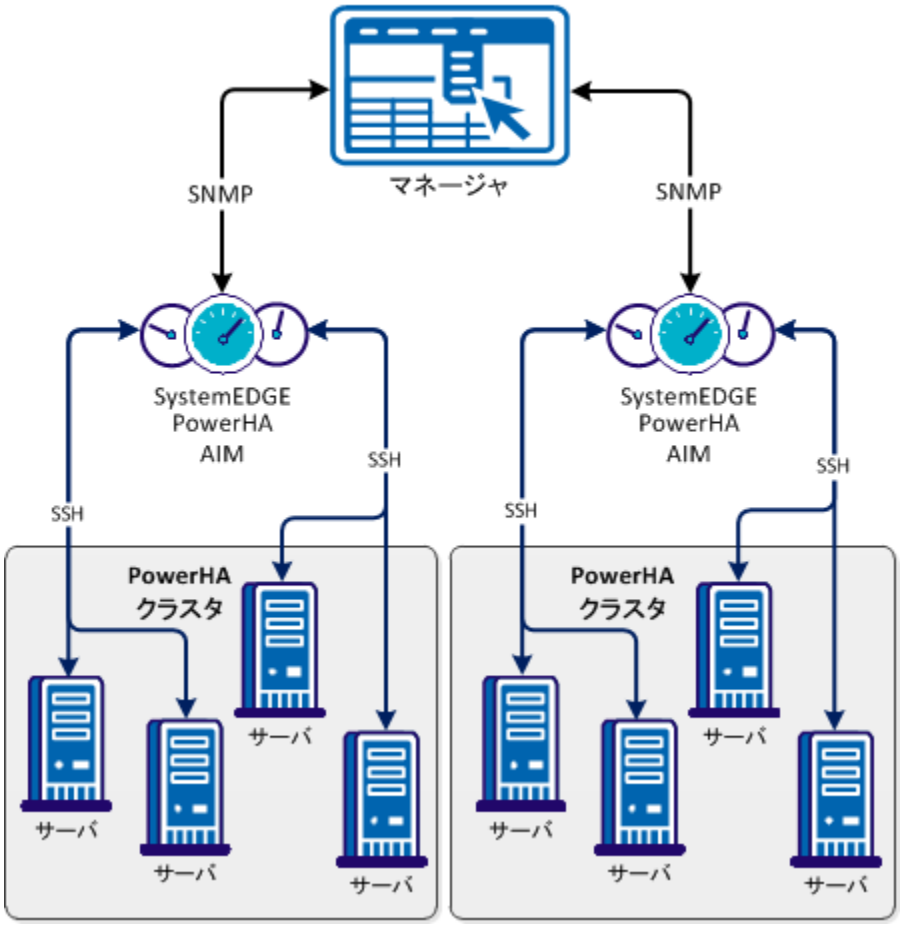
IBM PowerHA

CA Server Automation は、IBM PowerHA （旧名称「High Availability Cluster Multiprocessing （HACMP）」）をモニタします。 CA Server Automation はクラスタをリモートでモニタし、障害を検出して、クラスタ内のアラートやその他の環境の問題に関する詳細を提供します。

IBM PowerHA 管理コンポーネント間のインタラクション

以下の図は、IBM PowerHA に関与する管理コンポーネントがどのように対話するかを示しています。 AIM サーバとは、SystemEDGE および PowerHA AIM が稼働する Windows サーバです。 AIM と PowerHA クラスタの間の通信では、SSH （Secure Shell）が使用されます。 CA Server Automation は複数のクラスタに接続できるため、CA Server Automation では IBM PowerHA 環境全体のビューが取得できます。

PowerHA 管理コンポーネント間のインタラクション



必要な各 IBM PowerHA クラスタに要求される接続情報を追加するには、以下の方法を使用します。

- AIM サーバ上の NodeCfgUtil.exe ユーティリティ

接続情報は管理対象ノード上の設定ファイルに書き込まれます。PowerHA AIM は設定ファイルをポーリングし、マスタ ノードを通じて IBM PowerHA 環境のモニタリングを開始します。

SSH の設定

クラスタ ノードをモニタするには、リモート アクセス用の SSH を設定します。

次の手順に従ってください:

1. クラスタ (ノード) 上に SSH デーモンをインストールして実行します。
2. SSH 接続を許可するようにローカル ファイアウォールを設定します。

ダイアログ モードの NodeCfgUtil による PowerHA AIM の設定

NodeCfgUtil.exe は、AIM 設定を変更するために使用できるユーティリティです。このユーティリティをダイアログ モードで使用すると、適切な AIM が管理するノードを設定できます。

次の手順に従ってください:

1. AIM がインストールされているコンピュータで管理者としてログインし、Windows エクスプローラを開きます。
2. *SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリに変更し、NodeCfgUtil.exe を起動します。

   NodeCfgUtil によって、インストールされた AIM が検出され、その後に表示されるダイアログ ボックスに一覧表示されます。
3. *1* を入力して、新しい管理対象ノードを追加します。

4. 画面上の指示に従って、設定を完了します。 各ノードには、認証用の有効なユーザ名とパスワードが必要です。
5. 設定が完了したら、0 を入力して前のメニューに戻るか、またはユーティリティを終了します。

NodeCfgUtil は、PowerHA の設定ファイル（hacmp.cfg）を *SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリに書き込みます。また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。

例

以下の例は、PowerHA AIM の設定に正常に追加された *mycluster* に関する［管理対象ノードのインストール］ダイアログ ボックスを示します。PowerHA AIM はマルチインスタンス AIM です。 この手順を繰り返し、この AIM で管理するエンティティをさらに追加できます。

```
**** 管理対象ノードの選択 ****
1. Microsoft クラスタ
2. IBM PowerHA
0. 前のメニューに戻る
*******************************
選択項目を入力してください: 2
IBM PowerHA ノードの以下の情報を入力します...
（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）。
1. クラスタ名： mycluster
2. ユーザ名： administrator
3. パスワード： ************
4. ポート［デフォルトは 22］：
CAAC1016 認証しています。お待ちください...
CAAC1019 認証に成功しました。
CAAC1023 ノードが正常に追加されました。
キーをどれか押してください...
```

コマンド モードの NodeCfgUtil による PowerHA AIM の設定

NodeCfgUtil.exe は、AIM 設定を変更するために使用できるユーティリティです。 このユーティリティをコマンド モードで使用する場合、AIM 設定に追加できるのは管理対象ノードのみです。

注: NodeCfgUtil.exe は Windows 管理者として実行してください。

このコマンドの形式は、以下のとおりです。

```
(1) nodecfgutil -help
(2) nodecfgutil powerha -u user -p password -h cluster_name [-t port]
```

-help

コンソールに関する使用情報が表示されます。

powerha

仮想環境または物理環境を指定します。

-u *user|usercertificate*

管理者ユーザの名前またはユーザ証明書をそれぞれ指定します。

-p *password*

そのユーザのパスワードを指定します

- h *cluster_name*

クラスタの名前を指定します。

-t *port*

（オプション）ポート番号を指定します。

デフォルト： 22

次の手順に従ってください:

1. AIM がインストールされているシステムでコマンド プロンプトを開きます。

   コマンド プロンプトが表示されます。

2. 以下のコマンドの*いずれか*を入力します。

   ```
   (1) nodecfgutil -help
   (2) nodecfgutil powerha -u user -p password -h cluster_name [-t port]
   ```

   (1) コンソールに関する使用情報が表示されます。

   (2) IBM PowerHA に対して認証を実行し、正しい認証情報を格納します。

   このユーティリティは、IBM PowerHA の設定ファイル（hacmp.cfg）を *SystemEDGE_InstallLpath¥plugins¥AIPCommon* ディレクトリに書き込みます。

CA IBM SystemEDGE PowerHA AIM トラップ

CA SystemEDGE PowerHA AIM トラップ タイプ

CA SystemEDGE PowerHA AIM トラップ タイプのリストを以下に示します。varbind の詳細については、MIB ファイルを参照してください。

hacmpAimInstanceAddedTrap

新しいインスタンスまたはサーバが追加されるとトラップを送信します。

トラップ ID： 165800

hacmpAimInstanceRemovedTrap

インスタンスまたはサーバが削除されるとトラップを送信します。

トラップ ID： 165801

hacmpAimInstanceDataStatusChanged

インスタンスまたはサーバ データ ステータスが変更されるとトラップを送信します。

トラップ ID： 165802

hacmpAimNodeAddedTrap

ノードが追加されるとトラップを送信します。

トラップ ID： 165803

hacmpAimNodeRemovedTrap

ノードが削除されるとトラップを送信します。

トラップ ID： 165804

hacmpAimResourceGroupAddedTrap

リソース グループが追加されるとトラップを送信します。

トラップ ID： 165805

hacmpAimResourceGroupRemovedTrap

リソース グループが削除されるとトラップを送信します。

トラップ ID： 165806

hacmpAimResourceGroupMigration

リソース グループがマイグレートされるとトラップを送信します。

トラップ ID： 165807

hacmpAimResourceAddedTrap

インスタンスまたはサーバ リソースが追加されるとトラップを送信します。

トラップ ID： 165808

hacmpAimResourceRemovedTrap

リソースが削除されるとトラップを送信します。

トラップ ID： 165809

Microsoft Cluster Service

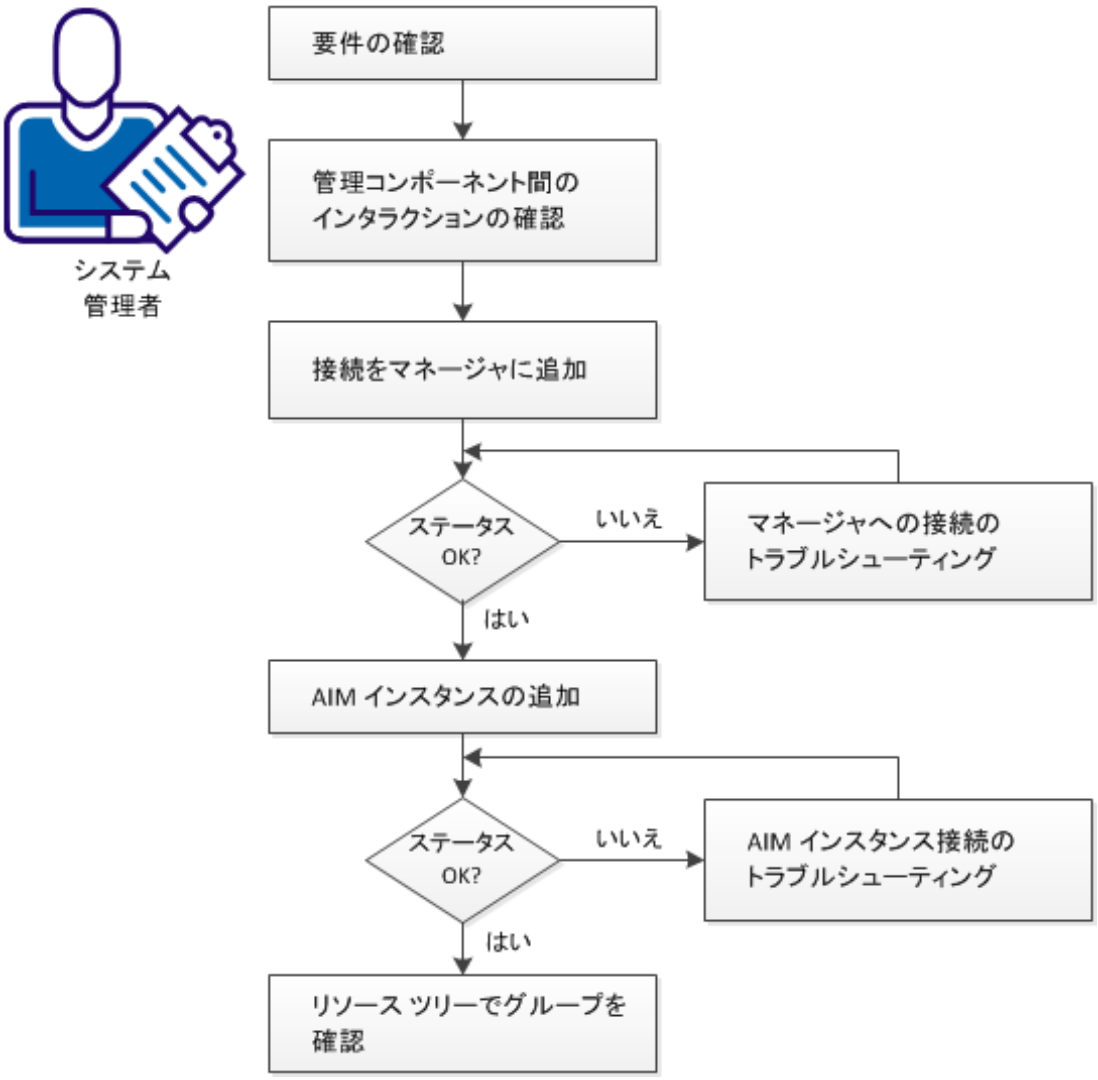
Microsoft Cluster Service （MSCS）は 2 つ以上のサーバを一緒に接続し、それらが単一のコンピュータとしてクライアントに表示されるようにします。 クラスタ化によって、フェイルセーフ アプリケーションを保有することができます。 Microsoft SQL Server のようなクラスタ対応アプリケーションは一度にノード上で実行されます。 そのノードがダウンした場合、別のノードがサービスを引き継ぎます。クラスタ化によって、アプリケーションが絶えず稼働されていることを確認することができます。

パフォーマンス モニタリングでは、CPU やメモリ使用などのメトリック収集用のクラスタおよび個別のクラスタ ノードへのリモート アクセスが必要です。 クラスタ固有の情報は各ノードで利用できます。 MSCS AIM は、WMI （ポート 135）を使用してクラスタと通信します。

Microsoft Cluster Service 管理コンポーネントを設定する方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

管理コンポーネントの設定方法



Microsoft Cluster Service （MSCS）は 2 つ以上のサーバを一緒に接続し、それらを単一のコンピュータとしてクライアントに表示します。 クラスタ化によって、フェイルセーフ アプリケーションを保有することができます。Microsoft SQL Server のようなクラスタ対応アプリケーションは一度に 1 つのノード上で実行されます。 そのノードがダウンした場合、別のノードがサービスを引き継ぎます。 クラスタ化によって、アプリケーションを常に稼働させることができます。

Microsoft クラスタ コンポーネントが CA Server Automation にインストールされている場合、管理者は［管理］タブを使用して、クラスタを登録し管理できます。

以下の手順に従います。

要件の確認 (P. 761)
MSCS 管理コンポーネント間のインタラクション (P. 763)
マネージャへの Microsoft Cluster Service の追加 (P. 765)
サーバへのマネージャの接続が失敗する (P. 766)
検出された MSCS AIM インスタンスの追加 (P. 768)
AIM インスタンス接続のトラブルシューティング (P. 769)
リソース ツリーでの Microsoft Cluster Service の確認 (P. 773)

要件の確認

CA Server Automation の管理コンポーネントを設定する前に、以下の要件を確認します。

- TCP/IP、SNMP、Web サービスおよび Windows Server オペレーティング システムに精通している。
- CA Server Automation および SystemEDGE に精通している。
- 以下を含む CA Server Automation マネージャ インストールにアクセスできる。
  - プラットフォーム管理モジュール（PMM）
  - Application Insight Module （AIM）
  - モニタリング エージェント（SystemEDGE）
- CA Server Automation ユーザ インターフェースにアクセスできる。
- 管理対象となる環境のサーバにアクセスするための有効な認証情報を入手できる（ユーザ名とパスワード）。

- Web サービスを通して使用する環境のサーバにアクセスするために使用するプロトコル（HTTP または HTTPS）およびポートを決定済みである。 デフォルト： HTTPS、ポート 443
- 使用する環境にあるサーバが正常に実行されていることを確認済みである。
- PMM と AIM が別々のシステムにインストールされている場合、PMM と AIM のシステムでの SNMP 設定に整合性があることを確認済みである。読み取り/書き込みコミュニティ文字列および SNMP ポート番号が同一である。
- 使用するリモート AIM サーバが CA Server Automation マネージャによって検出されることを確認済みである。

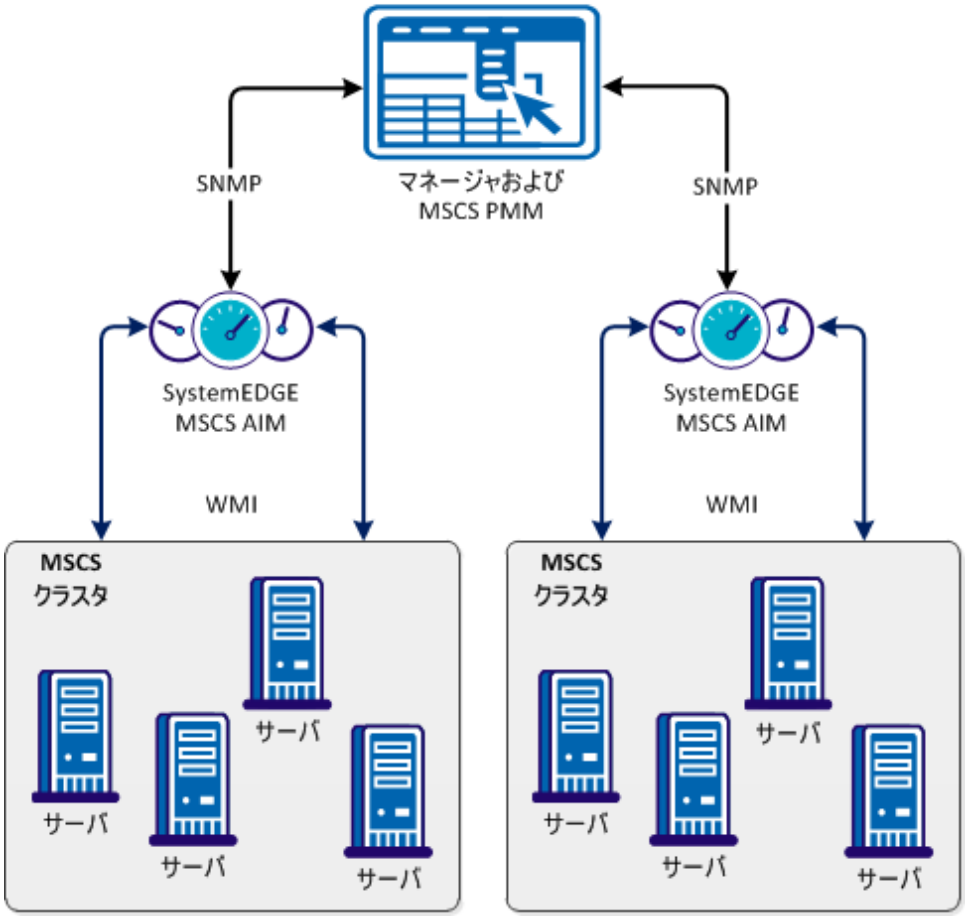
MSCS 管理コンポーネント間のインタラクション

以下の図は、MSCS モニタリングに関与するコンポーネントがどのように対話するかを示しています。 SystemEDGE と MSCS AIM は、同じ Windows Server 上で実行します。

Microsoft Cluster Service （MSCS）は 2 つ以上のサーバを一緒に接続し、それらが単一のコンピュータとしてクライアントに表示されるようにします。 クラスタ化によって、フェイルセーフ アプリケーションを保有することができます。 Microsoft SQL Server のようなクラスタ対応アプリケーションは一度にノード上で実行されます。 そのノードがダウンした場合、別のノードがサービスを引き継ぎます。クラスタ化によって、アプリケーションが絶えず稼働されていることを確認することができます。

パフォーマンス モニタリングでは、CPU やメモリ使用などのメトリック収集用のクラスタおよび個別のクラスタ ノードへのリモート アクセスが必要です。 クラスタ固有の情報は各ノードで利用できます。 MSCS AIM は、WMI （ポート 135）を使用してクラスタと通信します。

MSCS 管理コンポーネント間のインタラクション



マネージャへの Microsoft Cluster Service の追加

CA Server Automation ユーザ インターフェースの［管理］タブを使用して、Microsoft クラスタを追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左側のペインの［プロビジョニング］セクションから［Microsoft Cluster Services］を選択します。

3. ［Microsoft Cluster Service］ペイン ツールバーの （追加）をクリックします。

   ［新規クラスタの登録］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、ポート）を入力し、優先 AIM を指定して、［管理ステータス］を有効にします。

5. ［OK］をクリックします。

   Microsoft クラスタが登録されます。

   ネットワーク接続が正常に確立されている場合、右上のペインにサーバ追加され、緑のステータス アイコンが表示されます。

   注: 接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。 ［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

サーバへのマネージャの接続が失敗する

症状:

［管理］ - ［設定］でサーバ接続を追加した後に、サーバ接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバへの接続に使用したデータが現在も有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- 接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認します。

サーバ接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の  （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスが設定されているかどうかを調べるには、これらのコマンドの出力を確認します。

   サーバが DNS で見つからない場合は、CA Server Automation マネージャ システム上にある Windows の hosts ファイルにサーバを追加します。手順 3 に進みます。

   サーバが DNS で見つかった場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバ名を入力してファイルを保存します。例：

   ```
   192.168.50.50 myServer
   ```

4. CA Server Automation ユーザ インターフェースで、［管理］タブの［設定］に移動して、［サーバ］ペインの右上角にある （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合でも、接続に失敗することがあります。このような場合は、サーバに問題がある可能性があります。サーバへの接続を確立できない場合は、次の手順に進みます。

接続に必要なすべてのサービスが、サーバ システム上で正しく実行されているかどうかを確認する方法

1. サーバにアクセスするために、システム管理者に問い合わせます。
2. サーバ システムにログインします。
3. 接続に必要なすべてのサービスが正しく実行されているかどうかを確認します。
4. 必要に応じて、サービスを開始または再起動します。
5. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある （検証）をクリックします。

   CA Server Automation によってサーバ接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って収集したデータが正しいことを確認してください。

   管理者またはサポート担当者と協力して、サーバ接続の問題を解決します。

検出された MSCS AIM インスタンスの追加

CA Server Automation マネージャに Microsoft Cluster Service 接続を追加した後、Microsoft Cluster Service 環境を管理するための AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左側のペインの［プロビジョニング］セクションから［Microsoft Cluster Service］を選択します。

3. ［検出された Microsoft クラスタ AIM インスタンス］ペイン ツール バーの  （追加）をクリックします。

   ［クラスタ AIM インスタンスの追加］が表示されます。

4. ドロップダウン リストから［AIM ホスト］を選択します。

   検出された AIM ホストのリストが表示されます。

5. ドロップダウン リストから［登録済みクラスタ］を選択します。

   CA Server Automation は、［登録済み Microsoft クラスタ］ペインに一覧表示されたクラスタ名が が［登録済みクラスタ］ドロップダウン リストに入力されます。管理できるクラスタは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したクラスタの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了したら、Microsoft Cluster Service 環境の管理を開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

リソース ツリーでの Microsoft Cluster Service の確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. MSCS グループを展開します。

   MSCS リソースが表示されます。

CA Server Automation で、設定された MSCS 環境を管理する準備が整いました。 MSCS リソースのステータスとプロパティをモニタできます。

クラスタの登録

ユーザ インターフェースの［管理］ページを使用して、Microsoft クラスタを登録できます。

ユーザ インターフェースから Microsoft クラスタを登録する方法

1. ［管理］をクリックします。

   ［管理］ページが表示されます。
2. ［設定］ペインの［プロビジョニング］セクションで、［Microsoft Cluster Services］をクリックします。

   ［Microsoft Cluster Services］セクションが右側に表示されます。
3. ［登録済み Microsoft クラスタ］ツールバー上で「+」（追加）をクリックします。

   ［新規クラスタの登録］ダイアログ ボックスが表示されます。
4. 必要なクラスタ名およびアクセス識別情報を入力し［OK］をクリックします。

   Microsoft クラスタが登録されます。

注: クラスタを登録する場合は、クラスタ ホスト名を使用します。

クラスタの削除

ユーザ インターフェースの［管理］ページを使用して、Microsoft クラスタを削除できます。

次の手順に従ってください:

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［設定]ペインの[プロビジョニング]セクションで、［Microsoft Cluster Services］をクリックします。

   ［Microsoft Cluster Services］ページが表示されます。

3. ［登録済み Microsoft クラスタ］セクションで、削除するクラスタを選択します。

4. ［登録済み Microsoft クラスタ］ツールバー上で「-」（削除）をクリックします。

5. ［OK］をクリックします。

   クラスタが削除されます。

クラスタ プロパティの変更

ユーザ インターフェースの［管理］ページを使用して、Microsoft クラスタ プロパティを変更できます。

クラスタ プロパティを変更するには、以下の手順に従います。

1. ［管理］をクリックします。

   ［管理］ページが表示されます。

2. ［設定］ペインの［プロビジョニング］セクションで、［Microsoft Cluster Services］をクリックします。

   ［Microsoft Cluster Services］セクションが右側に表示されます。

3. 編集するクラスタを選択します。

4. ［登録済み Microsoft クラスタ］ツールバー上の［編集］アイコンをクリックします。

   ［クラスタ プロパティの変更］ダイアログ ボックスが表示されます。

5. 必須プロパティを編集し、［OK］をクリックします。

   クラスタ プロパティが変更されます。

Microsoft Cluster Service の管理

Microsoft Cluster Service の管理では、Microsoft のクラスタ、サービスとアプリケーション、およびノードを管理できます。Microsoft Cluster Service は、すべてのクラスタを表示して管理操作を実行するための一元的な場所です。

このセクションでは、［リソース］ページから Microsoft クラスタ リソースに対して実行できる管理操作について説明します。 ［リソース］ページでは、以下のオブジェクトに関する基本情報と詳細情報を表示できます。

- Microsoft クラスタ
- サービスとアプリケーション
- ノード

［リソース］をクリックし、［エクスプローラ］ペインを開きます。次に、いずれか 1 つのクラスタ リソースを選択し、そのリソースの［サマリ］をクリックします。

［サマリ］ページでは、オブジェクトに関連付けられている情報と、リソースに関連付けられているイベントを見ることができます。

Microsoft Cluster Service のモニタ

MS クラスタ リソースのステータスとプロパティは詳細にモニタすることができます。

クラスタ リソースをモニタする方法

1. ［リソース］をクリックします。

   ［リソース］ページが表示されます。

2. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

3. ［Microsoft Cluster Service］フォルダを展開し、クラスタ オブジェクトをクリックします。

   クラスタ ノードおよびサービス オブジェクトのリストが表示されます。

4. ［サービスとアプリケーション］オブジェクトをクリックします。

   サービスのリストが表示されます。

5. サービス オブジェクトをクリックします。

   右側のペインに、一般情報、リソース、およびイベントが表示されます。

   ［一般情報］パネルには、サービス名、ステータス、および所属先クラスタの名前が表示されます。

   ［リソース］パネルの［概要］タブには、リソース名、タイプ、ステータスなどのリソース詳細が表示されます。 ［リソース］パネルの［プライベート プロパティ］タブには、各リソースのプライベート プロパティが表示されます。

   ［イベント］パネルには、最新のイベントが表示されます。

第 9 章: エージェントレス モニタリング

CA Server Automation は、サポートされた仮想環境（Hyper-V を除く）および Windows システム（リモート モニタリング）のエージェントレス モニタリングを提供します。

このセクションには、以下のトピックが含まれています。

リモート モニタリング

リモート モニタリング （RM）を使用すると、エージェントレス システムのヘルス状態をモニタできます。 RM により、リモート システムにモニタリング エージェント（SystemEDGE など）をインストールしなくても、柔軟性の高いモニタリング システムを実現できます。

RM では、リモート システムのモニタリングに、RM AIM という中間マネージャを採用しています。 RM AIM は、リモートの Windows システム上で WMI クエリを使用してメトリック情報を収集します。

関連項目:

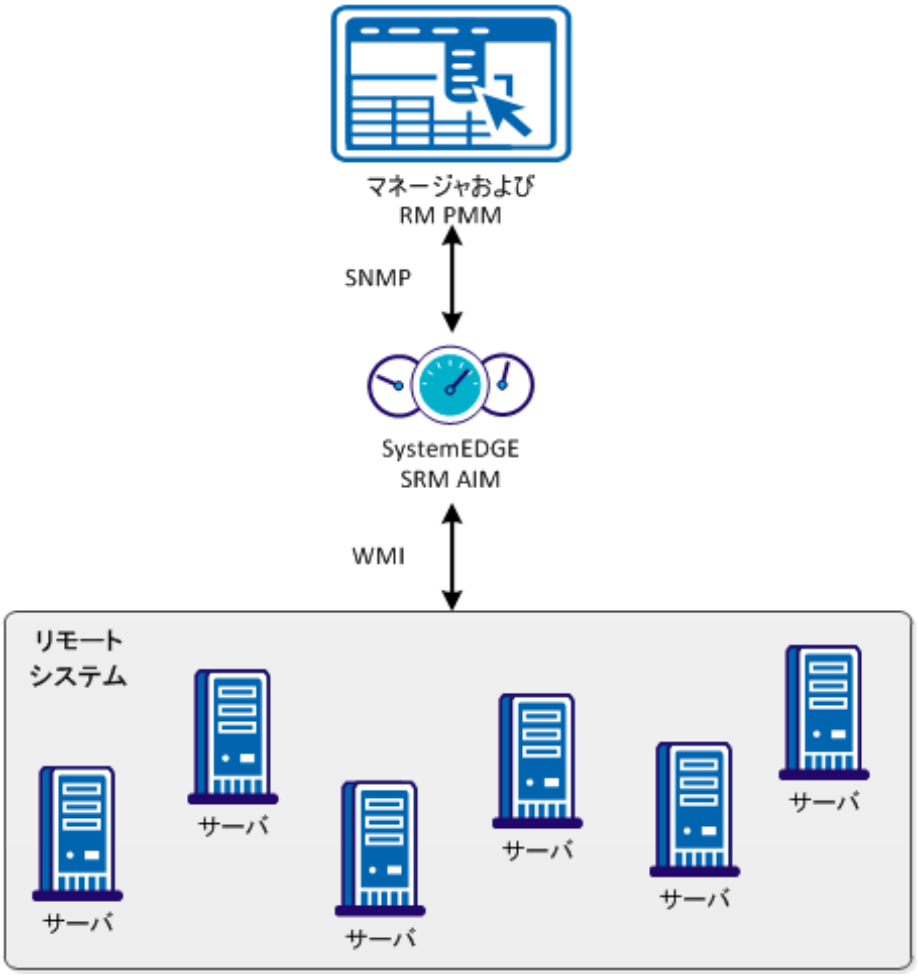
リモート モニタリング コンポーネント間のインタラクション

リモート モニタリング AIM は、DCOM を使用する root¥CIMV2 ネームスペースへの WMI 接続を通じて、RM システムにアクセスします。DCOM には、ローカル システム管理者のユーザおよびパスワード認証情報が必要です。 Windows コンピュータをモニタする場合は、RM AIM がファイルに格納しているこれらの認証情報を提供する必要があります。 パスワードは暗号化されます。

リモート モニタリングは、モニタされた RM システム上で WMI クエリ（ポート 135）を実行することにより、Windows システム情報を収集して提供します。 WMI ではポート 135 を使用します（デフォルト）。

以下の図は、これらの関係を示しています。

リモート モニタリング コンポーネント間のインタラクション



リモート モニタリングの利点

リモート モニタリングには、エージェント ベースのテクノロジではなく、エージェントレス テクノロジが含まれているため、どちらの戦略に対しても利点があります。 RM または展開したエージェントのどちらを使用するかを判断する際には、以下の情報を使用してください。

RM には以下の利点があります。

- セットアップ、設定、および展開にかかるコストを抑えられる。
- ソフトウェア アップグレードとメンテナンスが簡略化される。
- 展開に要する時間が短く、モニタ対象の環境への影響も少ない。
- 管理対象サーバのリソースの使用量が少ない。

展開したエージェントには以下の利点があります。

- モニタ対象サーバおよびアプリケーションについて、より詳細なデータとよりレベルの高い機能を利用できる。
- 動作に必要なネットワーク帯域幅が小さい。
- 拡張性が高く、数千のサーバにも拡張できる。
- ネットワーク接続が使用不可になっても（エージェントは自律的に動作できるため）、継続してサーバのヘルス状態をモニタし、データ収集を実行できる。
- 管理対象サーバに対するコマンドと制御の機能が強力になる。

機能と利点

リモート モニタリングを使用すると、エンド ユーザの観点からのモニタリングが *シームレスに*統合されます（すなわち、エージェントと RM のどちらであっても、モニタ対象システムの管理インターフェースの外観と操作性が同じになります）。

RM には、ヘルス状態と重要業績評価指標（KPI）メトリックのモニタリングを通じてシステムを管理できる機能が含まれています。 また、RM を通じて、システム ステータスと使用率メトリックに関するレポートを取得できます。 RM には、回復力、スケーラビリティ、統合、オートメーションなどの利点が含まれています。 以降のセクションで、主要な機能と利点について説明します。

エージェントレスのモニタ対象システム

リモート モニタリングでは、エージェント ベース テクノロジとエージェントレス テクノロジを使用して管理されるシステムに対し、シームレスなヘルス モニタリングを実行できます。

RM マネージャ コンポーネント（RM PMM）によって、RM システムとそのヘルス状態を表す CIM システム オブジェクトが作成されます。

この情報は［ダッシュボード］および［リソース］パネルに示されます。

次の手順に従ってください:

1. ［リソース］-［エクスプローラ］を開き、［リモート モニタリング］フォルダを展開します。

   検出されたシステムが、コンポーネント ツリー内に表示されます。

2. システムを選択します。

   システムのページが右ペイン内に表示されます。

3. ［リモート モニタリング］タブを開きます。

   エージェントレスの収集済みデータが表示されます。

重要業績評価指標メトリック

リモート モニタリングでは、モニタ対象の RM システムで WMI クエリを実行することにより、Windows メトリック情報が収集されて提供されます。豊富な情報が、さまざまな Win32 CIM クラスで利用可能になり、RM AIM を通じて提供されます。

視覚化

RM UI では、以下の情報を設定できます。

- リモートでのモニタ対象のシステム
- それらのシステムで収集されるメトリック
- それらのメトリックをモニタするかどうか、およびモニタリングの方法（重大度としきい値を含む）

設定

リモート モニタリングは、モニタリングの対象としてリモート システムが選択されると、モニタリングの設定を行わなくても、そのリモート システムの KPI がすぐにモニタされます。標準設定のモニタリングしきい値は、ニーズに合わせて調節できます。

また、設定を定義して設定セットに格納し、設定セットを 1 つ以上の RM システムに割り当てることができます。

アクセス制御

ユーザが管理者または非管理者ユーザとして UI にログインすると、セキュリティ メカニズムによって認証と許可の機能が提供されます。 リモート モニタリングによって、ユーザが管理者であるか非管理者ユーザであるかに基づいて特定のアクション（RM システムの設定など）が許可または禁止されます。

RM AIM は、root¥CIMV2 ネームスペースへの WMI 接続を通じて（DCOM を使用して）RM システムにアクセスします。アクセスには、ローカルの RM システム管理者ユーザおよびパスワード認証情報が必要です。 これらの認証情報（RM システムがモニタされる際にユーザが提供する）は、パスワード暗号化を使用して、ファイルに格納されます。

回復力

RM AIM は、SystemEDGE とは別のプロセスです。RM AIM のエラーが原因で SystemEDGE がクラッシュすることはありません。 RM AIM がクラッシュしたり、SystemEDGE のリクエストに応答しなくなると、SystemEDGE 内の *RM AIM アライブチェック*によって RM AIM が再起動されます。

スケーラビリティ

1 つの SystemEDGE に対して 1 つの RM AIM があり、各 RM AIM はおよそ 200 の RM システムをモニタできます。 1 人のマネージャに対して 1 つの RM PMM があり、各 RM PMM はおよそ 20 の RM AIM を管理できます。 デフォルト設定セットには、10 のモニタ対象メトリックと、各メトリックにモニタが 2 つずつ含まれています。

SystemEDGE のスケーラビリティの観点から見れば、これは以下のとおりになります。

- 10 * 2 * 200 = 4000 個の monitorTable エントリ
- 10 *200 = 2000 個の aggregateTable エントリ

統合

RM モニタ情報は、SNMP MIB に公開され、eHealth、および Spectrum のマネージャから容易にアクセスできます。

自動化

RM AIM にはコマンド ライン ユーティリティ（rmonwatch）が含まれます。これにより、スクリプトを使用して、RM システムとその認証情報をリモートで設定できます。

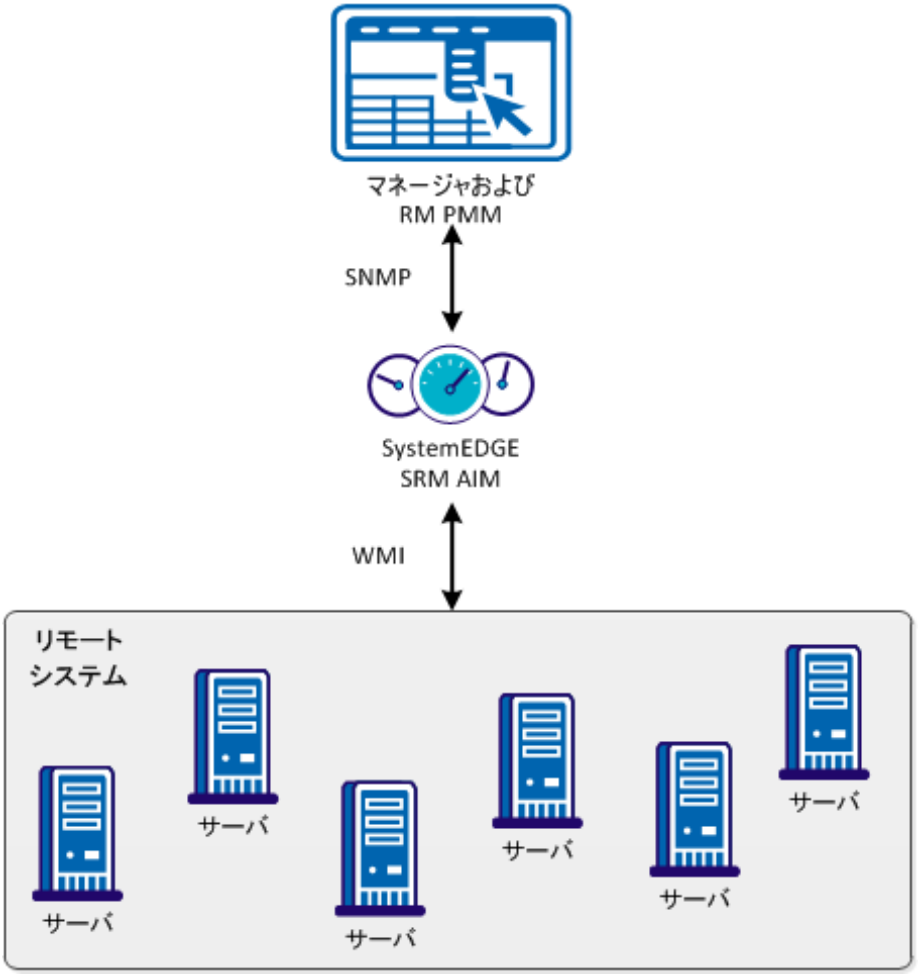
アーキテクチャ

以下の図は、メイン RM コンポーネントの概要を示しています。

1 つ以上の RM AIM が、DCOM/RPC 上で WMI を通じて Windows サーバのモニタリングを実行します。特定のサイトまたはサブネット内では、AIM からモニタ対象 Windows サーバに直接 TCP 接続する必要があります。 AIM は展開コンポーネントを通じて展開されます。

プラットフォーム管理モジュール（RM PMM）は、マネージャ インフラストラクチャへのインターフェースを提供し、CIM オブジェクト モデルに管理対象オブジェクトを作成します。PMM は、SNMP を使用して、RM AIM と通信します。

リモート モニタリング コンポーネント間のインタラクション

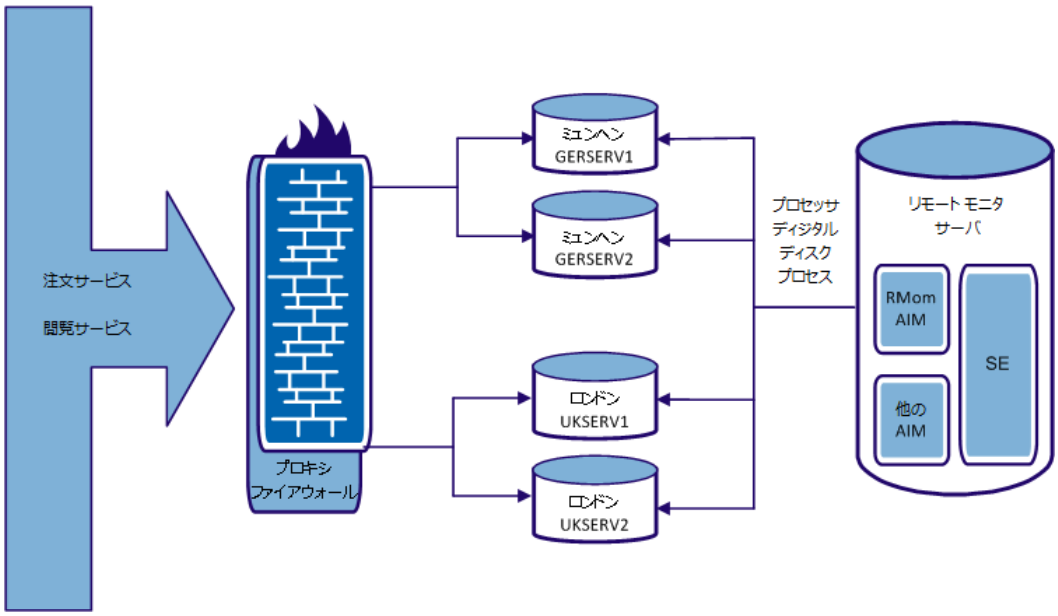


ユース ケース シナリオ

リモート モニタリングの以下のようなユース ケースについて考えてみます。 ある企業が、書籍の注文サービスと書籍の閲覧サービスから構成される Web ブック ストアを提供しています。

- 注文サービスは、ミュンヘンの 2 つのサーバとロンドンの 1 つのサーバから提供されています。
- 閲覧サービスは、ロンドンの 2 つのサーバとミュンヘンの 1 つのサーバから提供されています。

ミュンヘンのサーバは GERSERV1 および GERSERV2、ロンドンのサーバは UKSERV1 および UKSERV2 です。 いずれも、負荷分散とフェールオーバが設定されています。



サービスのモニタリングは、注文サービスと閲覧サービスとで異なります。この例では、2 つの設定セット（各サービス タイプに 1 つずつ）が定義されています。 これらの設定セットには、以下の情報のクエリとモニタが含まれています。

- CPU

  CPU アイドル時間合計の割合。

- FSys

  それぞれのサービス タイプにとって重要な論理ディスクの空き領域（注文サービスの場合は C:、閲覧サービスの場合は D:）。

- Proc

  注文プロセスの作業セットのサイズ（単一のプロセス order.exe）または閲覧プロセスのすべての作業セットのサイズ合計（プロセス browse のグループ）。

各モニタ対象システムに対して、サービスの役割（注文、閲覧、または両方）に応じて、以下の設定セットが割り当てられます。

システム名	設定セット
GERSERV1	order browse
GERSERV2	order
UKSERV1	order browse
UKSERV2	browse

設定の前提条件

リモート エージェントを設定する前に、以下の前提条件が満たされていることを確認してください。

- RM システムのファイアウォールとポートの要件

  RM AIM システムは、WMI 接続を通じて RM システムにアクセスします。 WMI では、エンドポイント マッパー（EPMAP）によって動的に指定される EPMAP ポート TCP （135）と DCOM TCP ポートを使用する DCOM 通信が使用されます。

  設定を単純にするために、RM AIM は RM システムと同じファイアウォール境界内に配置する必要があります。

  注: 固定ポートの使用方法の詳細については、Microsoft MSDN Web サイトの記事「Setting Up a Fixed Port for WMI」（英語のみ）を検索してください。

- マネージャ システムのファイアウォールとポートの要件

  RM AIM では、SystemEDGE によって提供される SNMP インフラストラクチャを利用します。ここでは、追加のポートが必要ありません。

  RM 設定は SNMP を使用して実行されます。 設定データにはパスワードが含まれるため、RM ではパスワード暗号化を使用します。

- SystemEDGE ポートと SNMP

  マネージャ システムは SNMP を通じて SystemEDGE システムにアクセスします。SNMP ポート（UDP 161 受信）が SystemEDGE システム上で開いている必要があります。 SystemEDGE システムによって SNMP トラップ（UDP 162 送信）が送信されます。

- SystemEDGE ポートとポリシーベース設定

  マネージャ システムは CAM を通じて SystemEDGE システムにアクセスします。UDP（4104）ポートまたは TCP（4105）ポートが SystemEDGE AIM システム上で開いている必要があります。SystemEDGE AIM システムでは、CAM を使用してマネージャ システムにメッセージを送信します。

- WMI アクセスのベスト プラクティス

  RM AIM は、WMI を使用して RM システムズに接続し、認証情報を要求します。 ベスト プラクティスとして、RM システムは AD ドメイン（RIVER など）のメンバにする必要があります。 このメンバシップによって、各 RM システムにローカルのユーザ アカウントを定義しなくても、ドメイン アカウントを使用することができます。 AD ドメインの Domain Admins グループのメンバである CARMuser ドメイン アカウントを作成します。

  RM のインストール中にユーザ認証情報設定が要求されたときに、ドメイン アカウント（RIVER¥CARMuser など）にパスワードを指定します。 このドメインのシステム メンバには、追加の設定が不要です。

  注: 必要に応じて、CARMuser アクセス権を制限し、ユーザが Domain Admins グループのメンバにならないようにすることができます。この場合、WMI 名前空間アクセスおよび DCOM アクセスを設定する必要があります。WMI 名前空間アクセスおよび DCOM アクセスの定義の詳細については、Microsoft の Web サイトを参照してください。

リモート モニタ システムの設定

設定セットは、RM システムに割り当てられたエンティティです。これにより、収集されるメトリック（WQL クエリ）とメトリックのモニタ方法が定義されます。

設定セットは複数の設定項目で構成されます。 設定項目はメトリック定義（WQL クエリ）とモニタリング定義（しきい値、重大度など）で構成されます。

RM には、以下のような、すぐに使えるメトリック定義とモニタリング定義の設定セットが用意されています。

- デフォルト
- extended
- metricDisk
- metricFS
- metricNet

1 つの RM システムに対して複数のしきい値と重大度の設定を使用して複数のメトリックをモニタする必要がある場合は、標準設定セットのクローンを作成し、システム固有のモニタリングのニーズに合わせてクローンのセットを調整します。

以下の表は RM メトリックとそれらが属する設定セットの一覧です。

メトリック	設定セット
CPU_PercentIdle	デフォルト
Disk_PercentIdle	デフォルト
Event_SystemErrors	デフォルト
FSys_FreeMB	デフォルト
FSys_FreeMBDecrease	デフォルト
Mem_PercentUsed	デフォルト
Net_MACAddress	デフォルト
Net_MACIndex	デフォルト
Net_QueueLength	デフォルト
Proc_PercentCPU	デフォルト
Proc_PercentMemory	デフォルト
Srvc_StoppedAuto	デフォルト
Sys_LastBootTime	デフォルト
Sys_LastLocalTime	デフォルト
Sys_OSInfo	デフォルト
Sys_PhysMemKB	デフォルト
Disk_ReadPerSec	extended
Disk_WritePerSec	extended
Disk_QueueLength	extended
Mem_FreeMB	extended
Mem_FreePages	extended
Mem_NonPagedMB_3GB	extended

メトリック	設定セット
Mem_PagedMB	extended
Mem_PagedMB_3GB	extended
Mem_PagingPerSec	extended
Mem_NonPagedMB	extended
Net_PercentBusy	extended
Sys_Is64bit	extended
Sys_Has3GBSwitch	extended
Sys_OSType	extended
BIOS_Version	extended
BIOS_SerialNumber	extended
Disk_AvgDiskBytesPerRead	metricDisk
Disk_AvgDiskBytesPerWrite	metricDisk
Disk_AvgDiskReadQueueLength	metricDisk
Disk_AvgDiskWriteQueueLength	metricDisk
Disk_DiskWritesPersec	metricDisk
Disk_PercentDiskReadTime	metricDisk
Disk_PercentDiskWriteTime	metricDisk
Disk_SplitIOPerSec	metricDisk
Net_PacketsOutboundErrors	metricNet
Net_PacketsReceivedErrors	metricNet
Net_PacketsReceivedDiscarded	metricNet
Net_PacketsReceivedNonUnicastPersec	metricNet
Net_PacketsReceivedUnicastPersec	metricNet
Net_PacketsSentNonUnicastPersec	metricNet
Net_PacketsSentUnicastPersec	metricNet
FSys_PercentFreeSpace	metricFS

注: RM メトリックの詳細については、「Performance Metrics Reference」を参照してください。

設定セットの作成

リモート モニタリングには、変更すべきでない、すぐに使用できる設定セットが複数用意されています。 自分のニーズに合ったカスタム設定セットを作成するには、［設定セット］ページを使用します。

設定セットを作成する方法

1. ［+］（新規作成）をクリックします。

   ［個別設定セットの詳細］ペインが表示されます。

2. 新しい設定セットの名前と説明を入力し、新しいセットに含める設定セットを強調表示します（複数のエントリを強調表示するには、Ctrl キーを押しながら選択します）。

3. ［保存］をクリックします。

   新しい設定セットが［設定セット］リストに追加されます。

注: ［アクション］ドロップダウン リストを使用すると、カスタム設定セットのクローン作成および削除もできます。

リモート モニタリング メトリックのサポート

CA Server Automation はメトリックを収集し、デフォルト設定セット内の RM メトリックの固定セットに基づいてレポートを生成します。

このため、レポートを使用するすべてのシステムには、デフォルト設定セット（または、それらのメトリックが含まれる設定セットか設定セット グループ）を割り当てる必要があります。

サポートされるデフォルト設定セットのメトリックは以下のとおりです。

- CPU_PercentIdle
- Disk_PercentIdle
- Event_SystemErrors
- Mem_PercentUsed
- FSys_FreeMB
- Fsys_FreeMBDecrease
- Net_QueueLength
- Proc_PercentCPU
- Proc_PercentMemory
- Srvc_StoppedAuto

リモート モニタリングを使用したシステムの管理

システムを管理するのに必要な RM 情報と設定にアクセスするには、［リソース］ペインで管理対象リソースを選択し、［リモート モニタリング］をクリックします。［リモート モニタリング］ページでは、以下のアクションを実行できます。

- モニタリング対象のリモート システムの追加
- クエリの管理
- 認証情報設定の管理
- 設定セットの作成
- 設定エントリの管理

ダッシュボードでは、以下の RM モジュールを使用できます。

- CA SystemEDGE マシン ステータス
- CA SystemEDGE オブジェクト ステータス

モニタリング対象のリモート システムの追加

リモートでモニタするシステムのシステム情報を入力するには、［システム］ページを使用します。

システムを追加する方法

1. ［+］（新規作成）をクリックします。

   ［新規作成］ペインが表示されます。

2. リモートでモニタするシステムの名前を［RM システム名］フィールドに入力し、以下の設定を編集します（必要に応じて）。

   RM システム名

   RM システムの名前を指定します。 ユーザ インターフェースを使用して、FQDN 表記法でのみ RM システム名を入力する必要があります（「vm1234.ca.com」など）。 「rmonwatch」ユーティリティを使用すると、RM システムをショート ネームまたは IP アドレスで指定することもできます。

   ステータス

   システムがアクティブまたは保守中のどちらであるかを指定します。

   プロトコル

   プロトコルが DCOM または SOAP のどちらかであるかを指定します。

   最大インスタンス

   システムに対する任意のクエリによってインスタンス テーブル内に作成されるインスタンスの最大数を指定します。

   認証情報

   リモート システムのユーザ認証情報を指定します。

   設定セット

   リモート システムで収集される設定セット（またはメトリックのグループ）を指定します。

3. ［保存］をクリックします。

リモートでモニタするシステムのリストにシステムが追加されます。

クエリ結果の表示

RM システムに関連付けられたクエリ結果を表示するには、［クエリ］ページを使用します。

［クエリ］ページでは、以下のアクションを実行できます。

- クエリの結果と設定の詳細を表示する（クエリ テーブルでクエリを強調表示し、［結果］または［設定］を選択します）。
- システム、ステータス、設定セット、または特定のクエリに基づいてクエリ結果をフィルタする（双眼鏡のアイコンでクエリ フィルタの表示/非表示を切り替えます）。
- クエリ テーブルに表示される情報を管理する（列見出しをクリックすると、列を昇順または降順で並べ替えたり、列を追加または削除したりできます）。

認証情報設定の管理

RM システムに関連付けられた個々の認証情報設定を管理するには、［認証情報］ページを使用します。

［認証情報］ページでは、以下のアクションを実行できます。

- 認証情報を追加する（［+］（新規作成）アイコンを使用し、［個別認証情報の詳細］ペインで設定を入力して、［保存］をクリックします）。
- 認証情報を削除する（既存の認証情報を強調表示し、［-］アイコンをクリックします）。
- 認証情報を編集する（既存の認証情報を強調表示し、［個別認証情報の詳細］ペインで設定を更新して、［保存］をクリックします）。

設定エントリの管理

クエリに関連付けられた設定を表示および管理するには、［設定エントリ］ページを使用します。

設定を表示または管理する方法

1. ［設定エントリ］テーブル内のクエリを強調表示します。フィルタの表示/非表示アイコン（双眼鏡）を使用すると、設定セット、重大度、クエリ クラス、およびエスカレーション重大度のエントリにフィルタを適用できます。

   ［個別設定エントリの詳細］ペインが表示されます。

2. 以下の値を表示または更新し、［保存］をクリックします。

インデックス

設定セット内の設定エントリに対して一意のインデックスを指定します。

クエリ名

クエリの名前を指定します（「.」記号は使用できません）。

同じクエリ名を別の設定セット内に使用することもできます。ただし、システムに複数の設定セットを適用するときは、すべてのクエリ名が一意であることを確認してください。 修飾子を固定エントリに設定した場合、クエリ名を変更することはできません。

説明

設定エントリの説明を指定します。

間隔

連続して行われるクエリ実行とモニタ評価の間隔を秒単位で指定します（値は 30 秒の倍数である必要があります）。

クエリ クラス

設定エントリのクエリ クラスを指定します。

クエリ スコープ

クエリに適用するスコープを指定します。

クエリ プロパティ

クエリ クラスのプロパティを指定します。

設定セット

設定セットの名前を指定します（「,」を使用しないでください）。

クエリ依存

あるクエリ（Q2）が別のクエリ（Q1）に依存することを指定します。つまり、Q2 は Q1 の結果に基づいてのみ作成されます。

修飾子

設定済みのクエリとモニタに関連する追加情報を指定します。

可能な値は、以下のとおりです。

- エントリは削除できず、クエリ名は変更できません（固定エントリ）
- クエリは 1 回のみ実行されます（少なくとも 1 回成功）
- クエリは、失敗するとそれ以上実行されません
- クエリ テーブルにクエリが表示されません
- 結果はインスタンスごとに表示されます
- 結果は現在の値の代わりに以前の値を示します
- 結果は増加デルタ値を示します
- 結果は減少デルタ値を示します
- 同じオブジェクト データと重大度を持つモニタを AND 関係として集計

クエリ合計

合計参照として適用するクエリ クラスのプロパティを指定します。

クエリ スケール

プロパティ値に適用するスケールを指定します（*100、/1024、/1024*100 など）。このスケールは、クエリ テーブルでのクエリ スケールのデフォルトとして使用されます。 クエリ プロパティの値は、結果属性に保存される前に、スケールによって乗算または除算されます。

クエリ インスタンス

インスタンス テーブルでインスタンスの名前付けに使用するクエリ クラスのプロパティを指定します。

条件

結果属性値を、しきい値およびエスカレーションしきい値と比較するための条件を指定します。

しきい値

結果属性値と比較するしきい値を指定します。

重大度

しきい値条件が満たされる場合に、SysEDGE オブジェクト状態モデルに使用する重大度を指定します。

オブジェクト クラス

SysEDGE オブジェクト状態モデルに使用するクラス名を指定します（「*」を使用しないでください）。

オブジェクト インスタンス

SysEDGE オブジェクト状態モデルに使用するインスタンス名を指定します（「*」を使用しないでください）。

オブジェクト 属性

SysEDGE オブジェクト状態モデルに使用する属性名を指定します（「*」を使用しないでください）。

遅延

SysEDGE オブジェクト状態モデルの状態変化が起きるために、しきい値（エスカレーション）条件が満たされる必要のある回数を指定します。

エスカレーション デルタ

エスカレーション条件を示すのに必要なしきい値との差分を指定します。

エスカレーション 重大度

エスカレーション条件が満たされる場合に、SysEDGE オブジェクト状態モデルに使用する重大度を指定します。

結果

SysEDGE モニタを使ってモニタするクエリ テーブルまたはインスタンス テーブル内のクエリの結果属性を指定します。

すべての変更が反映されるように、設定は更新されます。

第 10 章: Active Directory および Exchange Server 用の AIM のインストールおよび設定

このセクションには、以下のトピックが含まれています。

はじめに

Active Directory および Exchange Server（ADES）AIM では、Active Directory および Exchange Server 環境のヘルス状態およびキー パフォーマンス インジケータ（KPI）メトリックをモニタできます。 ADES AIM には、以下の機能があります。

- メールボックス サーバのメッセージ レコード マネージャ、論理ディスクの使用率、論理ディスクの読み取り/書き込みをモニタします。
- ハブ トランスポート サーバのネットワーク遅延、キュー、メール配信メトリック、論理ディスク使用率、および論理ディスク読み取り/書き込みをモニタします。
- アクティブ ディレクトリのパフォーマンス、レプリケーション、論理ディスク使用率、および論理ディスク読み取り/書き込みをモニタします。

ADES AIM は、モニタリングのために以下のデータを収集します。

- Active Directory と Exchange Server の設定データ
- Active Directory と Exchange Server のパフォーマンス データ

ADES AIM のスケーラビリティ

ADES AIM の展開を計画する場合、インフラストラクチャのサイジングおよびシステム パフォーマンスに影響を及ぼす以下のキー ファクタを考慮します。

- オペレーティング システムおよびその他のアプリケーションが使用するメモリを除き、ADES AIM が利用可能なメモリ
  - 1 GB の空きメモリがあるホストは 20 のホスト（2 台の Active Directory ホストと 18 台の Exchange ホスト）をモニタできます。
  - 2 GB の空きメモリがあるホストは 40 のホスト（6 台の Active Directory ホストと 34 台の Exchange ホスト）をモニタできます。
  - 3 GB の空きメモリがあるホストは 60 のホスト（10 台の Active Directory ホストと 50 台の Exchange ホスト）をモニタできます。
- 環境の地理的分布
  - ADES AIM が地理的に近い場所にある場合、環境の検出とポーリングにかかる時間が短縮されます。
  - 大きな遅延や多量のパケット損失は、AIM が必要なすべてのデータを取得できない原因となります。

注: サイジング情報は展開要件の概算であり、最終的なものではありません。 サイジング情報はモニタリング環境によって異なります。

ADES AIM のインストール

ADES AIM をインストールするために以下のタスクを完了します。

1. CA SystemEDGE リリース 5.8 エージェントおよび CA Advanced Encryption リリース 5.8 をインストールします。
2. 以下のいずれかの方法を使用して、ADES AIM をインストールします。
   - CA Server Automation リモート展開によって展開します。
   - コマンド モードによって手動でインストールします。
3. 以下の内容をモニタするドメインを指定して、ADES AIM を設定します。

注:

- ADES Manager と CA Spectrum を併用する場合は、ADES AIM ホストを管理するホストに SpectroSERVER をインストールしないでください。 また、ADES AIM は SystemEDGE ホストにインストールされている唯一の AIM である必要があります。
- 他のドメインと信頼関係を持つドメインのいずれかのメンバ サーバである Windows ホスト上に SystemEDGE および ADES AIM をインストールします。
- SystemEDGE エージェントおよび ADES AIM ホストには、Active Directory や Exchange Server の役割は設定できません。

リモート展開を使用した ADES AIM の展開

CA Server Automation リモート展開を使用して、ADES AIM をホストにインストールするソフトウェア ジョブを作成します。

次の手順に従ってください：

1. CA Server Automation アプリケーションにログインし、管理ビューに移動します。
2. ［リソース］タブで、ADES AIM を展開するホストを検索します。
3. ジョブを作成し、プラットフォーム タイプとして Windows を選択します。利用可能なラッパー パッケージが表示されます。

   ジョブの作成時に、ラッパー パッケージで以下のパラメータを指定します。

   ユーザ

   完全修飾ドメイン名（FQDN）なしのドメイン管理者の名前を定義します。 たとえば、adminuser と指定します。

   パスワード

   ユーザのパスワードを指定します。

   ドメイン名

   ADES AIM を介してモニタするドメインの名前を定義します。FQDN を入力します。

   管理エンティティ

   テクノロジに基づき、管理するホストを指定します。

   0

   Active Directory ホストのみをモニタします。

   1

   Exchange Server ホストのみをモニタします。

   2

   Active Directory ホストと Exchange Server ホストの両方をモニタします。

管理モード

管理するホストを指定します。

0

管理エンティティで定義されるドメイン内のすべてのホストを自動的に検出してモニタします（ドメイン ベースの管理）。

注: 子ドメインのホストは自動的にモニタされません。

1

ドメイン内のホストをすべて検出しますが、マネージャによって設定されているホストのみをモニタします(ホスト ベースの管理）。

4. 必要なパッケージを選択し、ホストに展開します。

［ジョブ］パネルでジョブ ステータスを確認します。ジョブが失敗した場合は、再度パッケージを展開します。

注: 詳細については、「SystemEDGE および AIM の展開方法 (P. 138)」を参照してください。

コマンド モードでの ADES AIM のインストール

コマンド モードでのインストールでは、リモート展開を使用せずに、ホストに ADES AIM をインストールします。

注: ADES AIM をインストールする前に、CASystemEDGE リリース 5.8 および CA Advanced Encryption リリース 5.8 がホストにインストールされるていることを確認してください。

次の手順に従ってください：

1. *DVD1*¥Installers¥Windows¥Data¥SysMan に移動して、以下の ZIP ファイルをローカル ディスクにコピーします。
   - CA_SystemEDGE_ESAD-Windows.zip
   - CA_SystemEDGE_ESAD-Windows-metadata.zip
2. コピーした ZIP ファイルをローカル ディスクに解凍します。 解凍した場所で、以下のファイルが利用可能になります。
   - caesadaimx64.msi
   - ca-setup.exe
   - ca-setup.dat
3. コマンド プロンプト ウィンドウを開き、*Extracted_Path*¥CA_SystemEDGE_ESAD¥5.8.0¥ENU¥Windows_x64 に移動します。
4. ca-setup.exe を実行して、ADES AIM をインストールします。 コマンドのフォーマットは、以下のとおりです。

   ```
   ca-setup EULA_ACCEPTED="[yes|no]"
   CASE_ESAD_DOMAIN_NAME="domain_name"
   CASE_ESAD_DOMAIN_USER_NAME="username@fqdn"
   CASE_ESAD_DOMAIN_PWD="password"
   CASE_ESAD_MANAGEMENT_ENTITY="[0|1|2]"
   CASE_ESAD_MANAGEMENT_MODE="[0|1]"
   ```

   EULA_ACCEPTED="[*yes*|*no*]"

   ライセンスが許可されるかどうかを指定します。

   CASE_ESAD_DOMAIN_NAME="*fully_qualified_domain_name*"

   ADES AIM を介してモニタするドメインの完全修飾名を指定します。

   CASE_ESAD_DOMAIN_USER_NAME="*username@fqdn*"

ドメイン管理者権限および Exchange Organization Administrator 権限、または Organization Management 権限を持つユーザの名前を指定します。

CASE_ESAD_DOMAIN_PWD="*password*"

ユーザのパスワードを指定します。

CASE_ESAD_MANAGEMENT_ENTITY="[*0*|*1*|*2*]"

テクノロジに基づき、管理するホストを指定します。

0

Active Directory ホストのみをモニタします。

1

Exchange Server ホストのみをモニタします。

2

Active Directory ホストと Exchange Server ホストの両方をモニタします。

CASE_ESAD_MANAGEMENT_MODE="[*0*|*1*]"

管理するホストを指定します。

0

管理エンティティで定義されるドメイン内のすべてのホストを自動的に検出してモニタします（ドメイン ベースの管理）。

注: 子ドメインのホストは自動的にモニタされません。

1

ドメイン内のホストをすべて検出しますが、マネージャによって設定されているホストのみをモニタします（ホスト ベースの管理）。

5. SystemEDGE サービスを再起動して、ADES AIM を実行します。

例

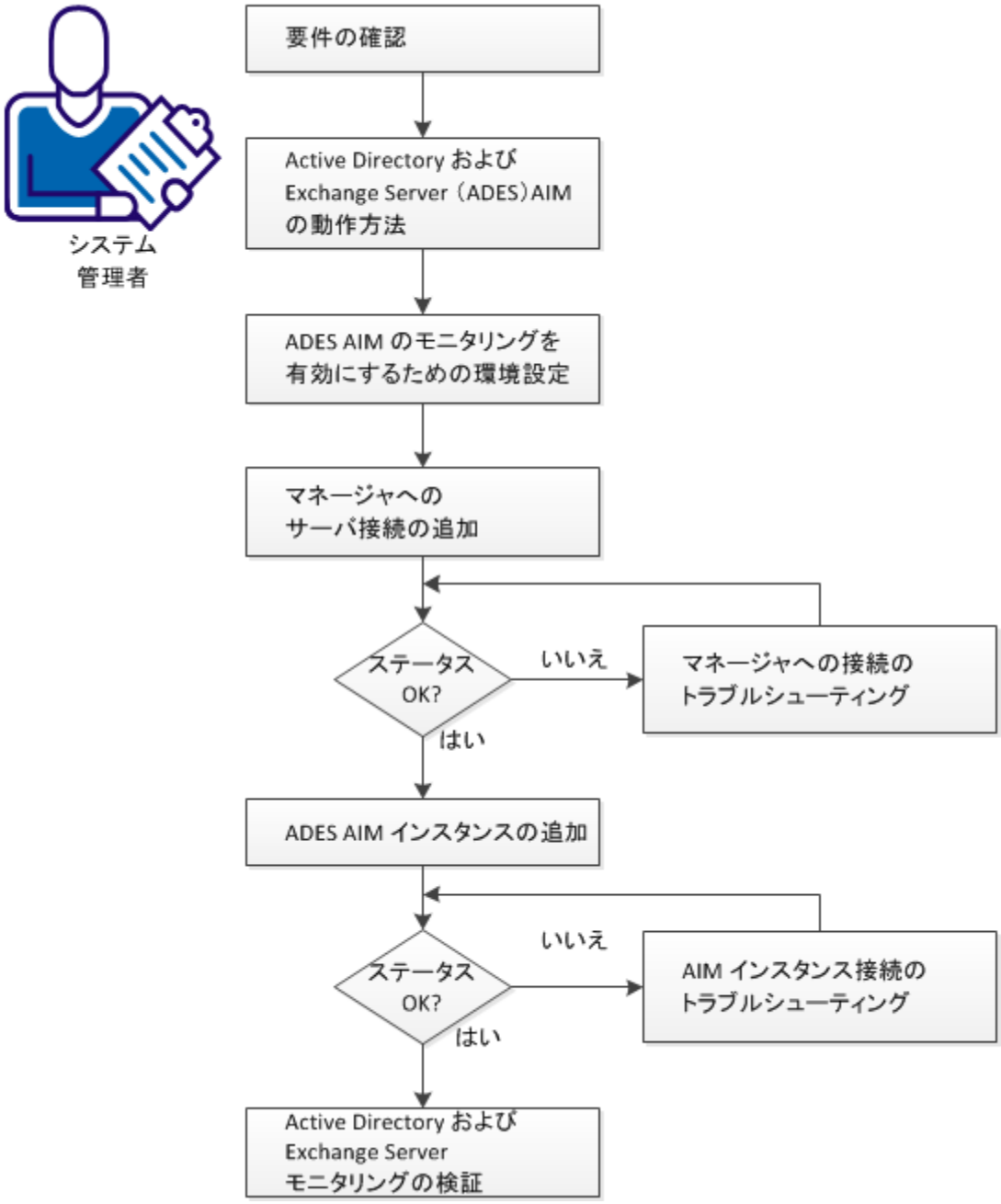
以下の例は、ADES AIM をホストにインストールし、ドメイン mydomain.com をモニタする方法を示しています。

```
ca-setup EULA_ACCEPTED="yes"
CASE_ESAD_DOMAIN_NAME="mydomain.com"
CASE_ESAD_DOMAIN_USER_NAME="adminuser@mydomain.com"
CASE_ESAD_DOMAIN_PWD="domainpass123" CASE_ESAD_MANAGEMENT_ENTITY="2"
CASE_ESAD_MANAGEMENT_MODE="0"
```

Active Directory および Exchange Server のモニタリングの設定方法

以下の図は、管理コンポーネントを設定するために必要なアクションの概要を示しています。 接続の問題が発生した場合のトラブルシューティング戦略も含まれます。

Active Directory および Exchange Server のモニタリングの設定方法



以下の手順に従います。

要件

以下の前提条件が ADES AIM をインストールおよび設定するのに必要です。

一般的な要件

- CA Server Automation を使用してサーバを検出し、パッケージを展開するための知識。
- 必要な権限
  - リモート展開用の権限を持つユーザ アカウント。
  - 手動インストール用のホスト上のローカル管理者権限を持つユーザ アカウント。
  - ドメインをモニタリングするためのドメイン管理者権限と Exchange Organization Administrator 権限、または Exchange Organization Management 権限。

    注: ドメイン管理者権限と Exchange Organization Administrator 権限が同じユーザに割り当てられていることを確認します。

ソフトウェア要件

- ADES AIM ホストがサポートされているオペレーティング環境
  - Windows Server 2008 SP2
  - Windows 2008 R2 SP2 x64
- サポートされているドメイン コントローラの動作環境：
  - Windows 2008
  - Windows 2008 R2
- サポートされている Exchange Server バージョン：
  - Exchange 2007 SP3
  - Exchange 2010 SP2

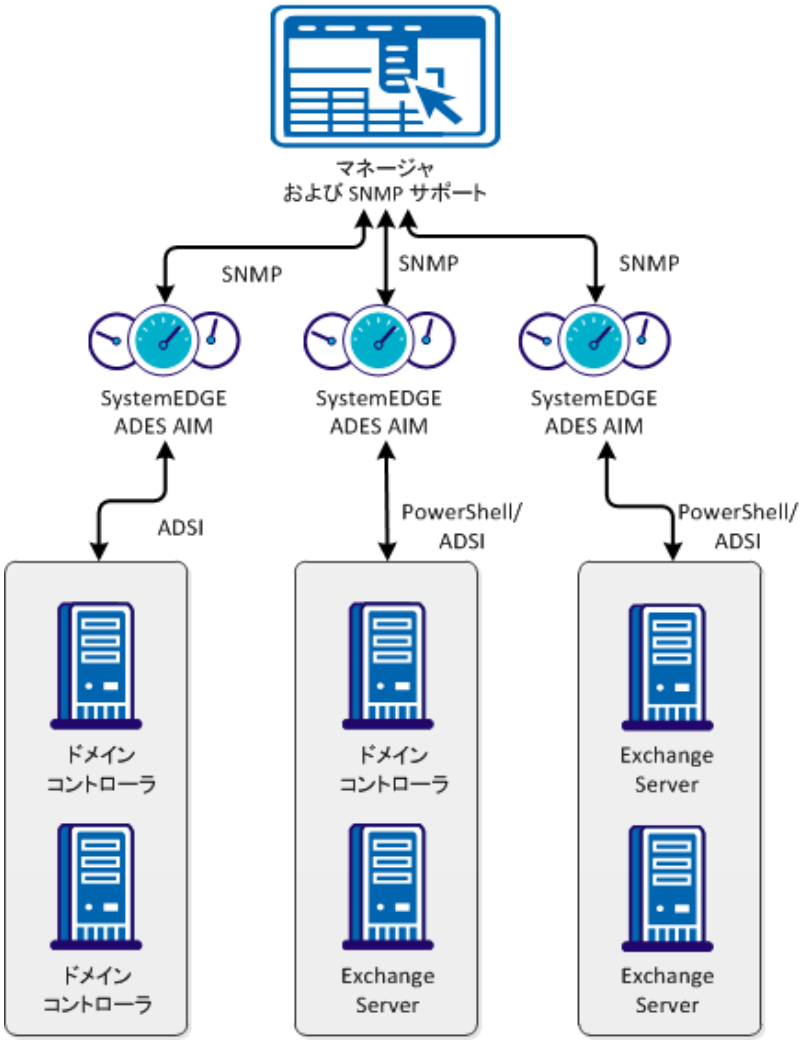
  注:
  - Exchange 2003 ホストのモニタリングはサポートされていません。
  - フォレスト間での Exchange 2007 ホストのモニタリングはサポートされていません。
- 必要なアプリケーション

- .Net 3.5 以降のバージョン
- Windows PowerShell 2.0
- Exchange 2007 ホストをモニタリングするための Exchange 2007 Management Tools SP3
- CA SystemEDGE リリース リリース 5.8 および CA Advanced Encryption リリース 5.8

Active Directory および Exchange Server AIM の動作方法

以下の図は、ADES AIM のアーキテクチャを示しています。

Active Directory および Exchange Server の管理コンポーネント間のインタラクション



以下のプロセスでは、ADES AIM の仕組みについて説明します。

1. ADES AIM はドメイン コントローラを検索してホストを検出します。ADES AIM は、以下に関する情報を収集します。
   - ドメイン コントローラやグローバル カタログなどの Active Directory サーバの役割。
   - ハブ トランスポート、メールボックス、およびクライアント アクセス サーバなどの Exchange Server の役割。

   注: ユニファイド メッセージングおよびエッジ トランスポートの役割は、モニタリングに対してはサポートされていません。
2. ホストが検出されると、AIM は以下からデータを収集するメッセージを送信します。
   - ドメイン コントローラ（ADSI コールを使用）
   - Exchange Server （PowerShell コマンドを使用）
3. AIM はデータを受信し、SystemEDGE エージェントについて MIB テーブルを更新します。
4. CA eHealth や CA Spectrum などのマネージャは、SystemEDGE ホストにポーリングして、表示するデータを収集します。
5. AIM は管理対象ホスト（モニタリング用に設定されている Active Directory と Exchange Server ホスト）に継続的にポーリングして、その MIB テーブルを更新します。

ADES AIM のモニタリングを有効にするための環境設定

Exchange ホスト上で PowerShell 設定を適用して、ADES AIM がドメインをモニタできるようにします。

注: モニタリングを開始する前に、すべての Exchange Server を設定します。

次の手順に従ってください：

1. ［スタート］-［プログラム］-［アクセサリ］-［Windows PowerShell］-［Windows PowerShell (x86)］を選択します。

   Windws PowerShell コマンドプロンプトが表示されます。

2. 以下のコマンドを実行して、WinRM サービスを介してホストをリモートで管理できるようにします。

   ```
   Enable-PSRemoting
   ```

   WinRM セットアップにより、リモート管理が開始され、WS-Man リクエストを受信するための WinRM リスナが作成されます。

3. 以下のコマンドを実行して、信頼されたホストのリストにホストを追加します。

   ```
   Set-Item WSMan:Localhost¥Client¥TrustedHosts -Value * -Force
   ```

4. 以下のコマンドを実行して、WinRM サービスを再開します。

   ```
   Restart-Service WinRM
   ```

   TrustedHosts 設定が更新され、Exchange Server のモニタリングが利用可能になります。

ドメイン サーバまたは Exchange Server のマネージャへの追加

ユーザ インターフェースを使用して、Microsoft Active Directory ドメイン コントローラまたは Exchange Server の接続をマネージャに追加できます。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。 ［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。

2. 左ペインの［プロビジョニング］セクションから［Microsoft Active Directory および Exchange Server］を選択します。

3. ［サーバ］ペイン ツールバーの （追加）をクリックします。

   ［サーバの追加］ダイアログ ボックスが表示されます。

4. 必要な接続データ（サーバ名、ユーザ、パスワード、モード、テクノロジ）を入力し、優先 AIM を指定して、［管理ステータス］を有効にします。

5. ［OK］をクリックします。

   CA Server Automation はサブミットされた接続データを検証し、サーバへの接続を確立しようとします。

   ネットワーク接続が正常に確立されている場合は、右上のペインにサーバが緑のステータス アイコンを使って追加されます。

   注: 接続に失敗した場合、［検証が失敗しました］ダイアログ ボックスが表示されます。 ［はい］をクリックすると、CA Server Automation によってサーバがリストに追加され、接続の失敗を示す赤のステータス アイコンが表示されます。 ［いいえ］をクリックすると、何も追加されません。

マネージャへのサーバ接続の失敗

症状:

［管理］-［設定］でサーバ接続を追加した後、サーバへの接続の検証に失敗しました。

解決方法:

接続に失敗する原因となる可能性がある最も一般的な問題を以下の手順で解決します。

- サーバの接続に使用したデータが今でも有効かどうかを確認します。必要な場合は、接続データを更新します。
- サーバ システムが実行されており、アクセス可能であるかどうかを確認します。
- サーバ システム上で管理サービスが正常に動作しているかどうかを確認します。

サーバの接続データを更新する方法

1. 失敗した接続に関連付けられた  （追加）または  （編集）をクリックします。
2. 接続の詳細を追加し、［管理ステータス］を有効にし、［OK］をクリックします。

   接続データが更新されます。
3. 右上角の  （検証）をクリックして新しい設定を検証します。

   サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システムが実行されており、アクセス可能であるかどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   nslookup <Server Name>
   ping <IP Address of Server>
   ```

2. サーバに有効な DNS エントリおよび IP アドレスがあることをコマンドの出力で確認します。

   サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルにサーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress <Server Name>
   ```

   正しい IP アドレスとサーバの名前を入力します。 例：

   ```
   192.168.50.50 myServer
   ```

4. 右上角の  （検証）をクリックします。

   サーバの認証情報と接続データが正しく、サーバに対して ping を実行できる場合は、接続がまだ失敗する可能性があります。 この場合は、サーバに問題がある可能性があります。 サーバへの接続を確立できない場合は、次の手順に進みます。

サーバ システム上で管理サービスが正常に動作しているかどうかを確認する方法

1. サーバ システムにアクセスする方法を管理者に問い合わせます。
2. サーバ システムにログインし、［スタート］メニューから［管理ツール］-［サービス］を開きます。

   ［サービス］ウィンドウが表示されます。
3. サービスを選択し、そのサービスを開始または再開します。
4. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によってサーバの接続が検証されます。

   サーバへの接続が失敗する場合は、このシナリオの要件に従って集めたデータが有効であることを確認してください。

   管理者またはサポート担当者と協力して、サーバの接続の問題を解決します。

ADES AIM インスタンスの追加

Active Directory および Exchange Server の接続を CA Server Automation マネージャに追加した後、環境を管理するために AIM インスタンスを追加します。

次の手順に従ってください:

1. ［スタート］メニューから CA Server Automation ユーザ インターフェースを開きます。［管理］-［設定］をクリックします。

   ［設定］ページが表示されます。
2. 左ペインの［プロビジョニング］セクションから［Microsoft Active Directory および Exchange Server］を選択します。

3. ［AIM サーバ］ペイン ツールバーの  （追加）をクリックします。

   ［AIM サーバの追加］ダイアログ ボックスが表示されます。

4. ドロップダウン リストから［AIM ホスト］を選択します。

   検出された AIM ホストのリストが表示されます。

5. ドロップダウン リストからサーバを選択します。

   CA Server Automation によって、［サーバ］ペインに一覧表示されたサーバ名がサーバ ドロップダウン リストに入力されます。 管理できるサーバは、CA Server Automation マネージャで有効な接続が確立されているものに限られます。

   注: AIM がリモート システムに存在している場合、CA Server Automation でこのシステムを最初に検出する必要があります。検出後、AIM サーバがドロップダウン リストに表示されます。

6. ［OK］をクリックします。

   選択したサーバの新しい AIM インスタンスが追加されます。インスタンスがエラー状態または停止状態にない場合、CA Server Automation は関連付けられている環境の検出を開始します。ディスカバリ プロセスが完了すると、Active Directory および Exchange Server の環境のモニタリングを開始できます。

AIM インスタンス接続のトラブルシューティング

AIM 接続が準備未完了のステータスにある場合は、以下のステータス アイコンのいずれかが表示されます。

 ディスカバリが進行中

 ポーリングなし

 エラー

 警告

 無効

 不明

AIM インスタンス ステータスの詳細については、ツールヒントを参照してください。 以下のトラブルシューティングのセクションでは、問題を解決するための詳細情報と手順について説明します。

AIM インスタンスのステータス アイコンに「ディスカバリが進行中」が表示される

症状:

［管理］-［設定］でサーバに対して AIM インスタンスを追加した後、ステータス アイコンに  （ディスカバリが進行中）が表示されます。

解決方法:

環境のディスカバリ プロセスが完了するまで待機します。 ディスカバリにかかる時間は、環境内の仮想および物理リソースに関連する管理対象オブジェクトの数によって異なります。 アイコンの上にカーソルを移動すると、未処理のディスカバリ要求の数を示すツールヒントが表示されます。ディスカバリ ジョブが完了すると、CA Server Automation はサーバ フォルダをリソース ツリーに追加します。その後、環境の管理を開始できます。

AIM インスタンスのステータス アイコンに「ポーリングなし」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （ポーリングなし）が表示されます。

解決方法:

関連付けられたインスタンスに、特定の必要なアクションはありません。このアイコンは、CA Server Automation マネージャがこの AIM をポーリングしないこと表します。 この AIM は優先 AIM ではありません。

特定のサーバを管理するために複数の AIM が設定されている場合、PMM は現在の AIM として AIM の 1 つを選択します。 別の AIM を使用したい場合は、［管理］-［設定］-［プロビジョニング］で優先 AIM を設定できます。サーバ エントリの［編集］をクリックし、優先 AIM を選択します。優先 AIM が現在の AIM になります。

AIM インスタンスのステータス アイコンに「エラー」が表示される

症状:

［管理］-［設定］で AIM インスタンスを追加した後、ステータス アイコンに  （エラー）が表示されます。 AIM に接続できません。

解決方法:

AIM への接続に失敗する原因となる可能性がある最も一般的な問題を、以下の手順で解決します。

- AIM サーバがアクセス可能であるかどうかを確認します。
- SystemEDGE が実行されているかどうかを確認します。 必要な場合は、SystemEDGE を開始または再開します。

AIM サーバ システムがアクセス可能かどうかを確認する方法

1. CA Server Automation マネージャ システムでコマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   ping servername
   ```

2. コマンドの出力に、AIM サーバの有効な DNS エントリおよび IP アドレスが含まれていることを確認します。

   AIM サーバが DNS 内にない場合は、CA Server Automation マネージャ システムの Windows ホスト ファイルに AIM サーバを追加します。 手順 3 に進みます。

   サーバが DNS 内にある場合は、手順 4 に進みます。

3. ASCII エディタで %windir%¥system32¥drivers¥etc ディレクトリの hosts ファイルを開き、以下の行を追加します。

   ```
   ipaddress servername
   ```

   正しい IP アドレスと AIM サーバの名前を入力します。 例：

   ```
   192.168.50.51 myAIM
   ```

4. ［AIM サーバ］ペインの右上角の  （検証）をクリックします。

   エラー ステータスが変わらない場合は、次の手順に進みます。

SystemEDGE が実行されているかどうかを確認する方法

1. AIM サーバにログインし、%windir%¥Program Files¥CA¥SystemEdge¥bin ディレクトリから sysedge.cpl を実行します。

   SystemEDGE コントロール パネルが開き、SystemEDGE の実行状態が表示されます。

2. SystemEDGE を開始または再開します。

   SystemEDGE が実行されていることが SystemEDGE コントロール パネルに表示されるまで待機します。

3. CA Server Automation ユーザ インターフェースに移動し、マネージャ システムの［AIM サーバ］ペインの右上角にある（検証）をクリックします。

   CA Server Automation によって AIM サーバの接続が検証されます。

   エラー ステータスが変わらない場合は、収集したデータがこのシナリオの要件に従っていることを確認してください。

AIM インスタンスのステータス アイコンに「無効」が表示される

症状:

CA Server Automation がネットワーク内の AIM インスタンスを検出した後、いくつかのインスタンスについてステータス アイコン（無効）が表示されます。 この AIM インスタンスは管理されていません。

このステータスは、CA Server Automation が以下の関係を持つ AIM を検出した場合に表示されます。

- CA Server Automation マネージャへの接続が有効であるが管理対象外の状態であるサーバ用に AIM が設定されている。
- AIM は、まだ設定されていないサーバに接続されます。

解決方法:

AIM インスタンスのステータスを「準備完了」に変更するには、以下の*いずれか*を実行します。

- 欠落しているサーバから CA Server Automation マネージャへの接続を追加します。
- 既存のサーバ接続を編集し、その管理ステータスを「有効」に変更します。

Active Directory および Exchange Server モニタリングの検証

設定が正常に実行された後、CA Server Automation は Active Directory および Exchange Server のモニタリングを開始します。 Active Directory および Exchange Server のイベントをユーザ インターフェースでモニタします。

（オプション）ノード設定ユーティリティを使用した ADES AIM の設定

ユーザ インターフェースの代わりに NodeCfgUtil を使用して ADES AIM を設定する方法もあります。 ADES AIM を設定することで、ADES AIM で管理する 1 つ以上のドメインを追加、変更、または削除できます。 NodeCfgUtil は、ADES AIM の設定ファイル（esad.cfg）を作成します。このファイルは、*SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリにあります。

次の手順に従ってください：

1. Windows エクスプローラを開き、*SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリに移動します。
2. NodeCfgUtil.exe を起動します。
3. 選択に応じてオプションを入力します。 ドメインの追加、変更、または削除ができます。 たとえば、「1」を入力して新しい管理対象ノードを追加します。
4. ［管理対象ノードの選択］画面内の ADES AIM に対応する数を入力します。 たとえば、「1」を入力して ADES AIM を選択します。
5. 画面上の指示に従って、設定を完了します。 各ドメインには、認証用の有効なユーザ名とパスワード、および適切な管理エンティティと管理モードが必要です。
6. 設定が完了したら、「0」を入力して設定を保存し、ユーティリティを終了します。
7. SystemEDGE サービスを再起動して、変更を適用します。

例

以下の例は、ADES AIM の設定に正常に追加された mydomain.net に関する［管理対象ノードのインストール］ダイアログ ボックスを示しています。管理エンティティは Active Directory に設定されます。管理モードはドメイン ベースで設定されます。

**** 管理対象ノードの選択 ****

1. Microsoft Active Directory および Exchange Server

0. 前のメニューに戻る

****

選択項目を入力してください: 1

Microsoft Active Directory および Exchange Server ノードの

以下の情報を入力します...

（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）

1. ドメイン名（FQDN） : mydomain.com

2. ユーザ名（例： adminuser@domain.com） : administrator@mydomain.com

3. パスワード： **********

4. 管理エンティティ（0： AD のみ、1： Exchange のみ、2： AD と Exchange の両方） : 0

5. 管理モード： （0： ドメイン ベース/自動、1： ホスト ベース/手動） : 0

CAAC1016 認証しています。お待ちください...

CAAC1019 認証に成功しました。

CAAC1023 ノードが正常に追加されました。

キーをどれか押してください。 . .

ADES AIM のアンインストール

エージェントをアンインストールすると、エージェントおよびその関連する設定データがホストから削除されます。

次の手順に従ってください：

1. SystemEDGE コントロール パネルを使用して、SystemEDGE プロセスを停止します。
2. ［スタート］-［コントロール パネル］-［プログラム］-［プログラムと機能］を選択します。

   ［プログラムのアンインストールまたは変更］ウィンドウが開きます。
3. Exchange Server および Active Directory コンポーネント用の CA AIM を右クリックし、［アンインストール］を選択します。

   確認メッセージが表示されます。
4. ［はい］をクリックします。

   ADES AIM コンポーネントが削除されます。 ADES AIM コンポーネントが［追加/削除］コントロール パネルに表示されていないことを確認します。

トラブルシューティング

関連項目:

AIM が非アクティブで、データを収集していない (P. 827)
1 つ以上のドメインがモニタされない (P. 828)
一部のカウンタがモニタされない (P. 828)
一部のホストがモニタされない (P. 829)

AIM が非アクティブで、データを収集していない

症状

AIM が非アクティブになっていて、データを収集できません。

解決策

以下を確認してください。

- caesadaim.exe プロセスが実行中である。
- 設定済みのすべてのドメインに対して、AIM ディレクトリ内にドメインのログ ファイルが作成されている。

プロセスが実行中でないか、ログ ファイルが作成されていない場合は、SystemEDGE サービスを再起動します。

SystemEDGE サービスを再起動しても AIM が実行されない場合は、以下の要件を確認して適切な処置を行います。

- AIM ホストに .NET 3.5 SP1 Framework がインストールされている。
- AIM と同じホストに Exchange Management Tools 2007 SP3 がインストールされている（ドメインに Exchange 2007 Server が 1 台以上含まれている場合）。

1 つ以上のドメインがモニタされない

症状

ADES AIM が 1 つ以上のドメインをモニタしません。

解決策

- ADES AIM フォルダに、モニタ対象の各ドメインのログ ファイルが domain_AIM.log という名前で作成されていることを確認します。 ログ ファイルが作成されていない場合は、nodecfgutil.exe を使用したモニタリングの対象としてドメインが設定されていることを確認します。
- ドメインのログ ファイルが作成されている場合は、ログ ファイルを開き、以下のエラー メッセージを探します。

  ```
  The specified domain does not exist or cannot be contacted.
  ```

  このメッセージがログ ファイルに含まれている場合は、ADES AIM ホストとドメイン コントローラ間の通信がブロックされていないことを確認します。 ドメイン コントローラが ADES AIM ホストからアクセス可能な場合は、CA Spectrum で AIM のディスカバリを開始します。

一部のカウンタがモニタされない

症状

一部のパフォーマンス カウンタがモニタされません。

解決策

ADES AIM で検出を再度開始して、カウンタが存在しないホスト上にカウンタを作成します。

注: 特定の設定に対して表示されるパフォーマンス カウンタは、必要な設定またはインスタンスがホストで利用可能な場合にのみモニタされます。

一部のホストがモニタされない

症状

ドメイン内の Active Directory ホストおよび Exchange Server ホストでモニタされていないものがあります。

解決策

以下の設定を確認してください。

- AIM がドメイン モードまたはホスト モードで設定されている。

  注: ホスト モードでは、ユニバーサル ホスト テーブルにあるホストごとに、CA Spectrum または MIB ブラウザを使用して管理ステータスを変更します。

- AIM が Active Directory ホストのみ、または Exchange Server ホストのみをモニタするように管理エンティティで設定されている。ADES AIM が両方のテクノロジをモニタするように、NodeCfgUtil を使用して、ドメインの［管理エンティティ］オプションの値を 2 に変更します。

第 11 章: ルールとアクションの使用

このセクションには、以下のトピックが含まれています。

ルールとアクション

ルールとアクションを設定するには、まずルールとアクションについて理解し、それらが相互にまたは他のコンポーネントと対話する方法について理解する必要があります。 これらのインタラクションを理解することによって、ルールとアクションをセットアップしてデータ センターを効率的に管理する最適な方法を決定することができます。

CA Server Automation はメトリックを収集して分析し、リソースを分配する方法に関する分析に基づいて最適な決定を行います。 たとえば、CA Server Automation がサーバまたはサービスを高稼働率または低稼働率であると判断した場合は、新しいコンピュータをプロビジョニングできます。

使用状況はサーバ レベルおよびサービス レベルでモニタされます。 サーバ レベル モニタリングでは、特定のサーバの診断問題に関与するため、重要なパフォーマンス インジケータのみが使用されます。 サービス レベル モニタリングでは全体としてサービスに関する問題を診断し、全体の使用率がパフォーマンス インジケータとして使用されます。

ルールはサーバ レベルまたはサービス レベルで作成できます。 ルールを作成してパフォーマンス メトリックおよび生成されたイベントを評価します。 ルールは、個別の条件または条件の組み合わせで構成されます。 アクションが実行されるようにするには、全体を true の状態に評価する必要があります。 ルールは独自のルールを作成するか、またはルール テンプレートのセットを選択し、自動化ポリシーを使用して生成することもできます。

注: パフォーマンス メトリックおよび説明のリストについては、「Performance Metrics Reference」を参照してください。

デフォルトでは、ルールはデータ センター レベルで収集設定に定義されている記録間隔（デフォルト = 300 秒）で評価されるか、モニタされたメトリック値が原因でイベントが発生した場合に評価されます。 データ センターとは異なる間隔を設定する場合は、特定のサーバを設定してデフォルトのデータ センターの記録間隔を上書きすることができます。 サーバ レベル ルールは設定されたサーバ レベルの記録間隔で評価されます。 サービス レベル ルールは、そのサービス内のすべてのサーバの中で最も短い記録間隔で評価されます。 記録間隔を変更する場合は、ポリシー マネージャ サービスを停止して再起動し、ルールを評価するために更新された間隔を取得して使用します。

メトリックは評価データのソースです。 メトリック ルールが true に評価すると、アクションはトリガされます。 ルールが true に評価するには遅延が超過している必要があります。 あるシナリオでは、ルールの一度だけの違反でアクションがトリガされるようにするために遅延を 1 に設定しますが、他のインスタンスでは、一度だけのイベントでのルールのトリガを望まない場合があります。

たとえば、CA Server Automation が、呼び出しを管理したり、問題の解決策を追跡したり、企業ナレッジを共有したり、IT 資産を管理するカスタマ サポート アプリケーションの CA SDM に統合されるとします。アクションがトリガされた場合に自動的にチケットがオープンされるようにするには、アクションが CA SDM と対話するよう設定します。 これはサードパーティの承認が必要なアクションに役立ちます。 サードパーティが CA SDM でユーザのチケットを承認した後で、アクションは自動的に実行されます。

また、開始コンポーネントを使用して、指定された時刻にアクションが実行されるようにスケジュールすることもできます。 ジョブを作成するときに、アクションの最新のパラメータが保存されます。ジョブがサブミットされた後でアクションの詳細を変更しても、すでに実行されるようにスケジュールされていたジョブには影響を及ぼしません。 すでにスケジュールされているジョブのアクションの詳細を変更する必要がある場合は、アクションを使用するジョブを開いて再度それを保存し、それを新しいアクションの詳細で更新します。

CA SDM の設定

バージョン 12.5 以前の CA SDM リリースについては、適切なチケット ステータス コードで CA SDM を正しく設定することにより、必要に応じて問題が自動的に開くようにアクションを設定できます。

注: CA Server Automation および CA SDM のリリース番号は、2 つの製品がデータベースを共有しない限り、同じである必要はありません。

CA SDM 設定する方法

1. Web ブラウザに以下の情報を入力することにより CA SDM サーバにログインします。

   http://*servicedesk_servername*:8080

   CA SDM のスプラッシュ画面が表示されます。

2. ユーザ名とパスワードを入力して、［ログイン］をクリックします。

   CA SDM のメイン ページが表示されます。

3. ［管理］をクリックし、左側のペインに Service Desk ツリー ノードを展開します。

4. ［要求/インシデント/問題］を選択して［ステータス］を選択します。

   ［要求/インシデント/ステータス リスト］が表示されます。

5. ［新規作成］をクリックします。

   ［新しい要求ステータスの作成］ウィンドウが表示されます。

6. ［シンボル］テキスト ボックスに［**承認済み**］を入力し、［レコード ステータス］ドロップ ダウン リストから［アクティブ］を選択し、［コード］テキスト ボックスに［**APP**］を入力し、［保存］をクリックします。

   リストに新しい要求ステータスが表示されます。

7. ［シンボル］テキスト ボックスに［**拒否**］を入力し、［レコード ステータス］ドロップ ダウン リストから［アクティブ］を選択し、［コード］テキスト ボックスに［**REJ**］を入力し、［保存］をクリックします。

   リストに新しい要求ステータスが表示されます。

   CA SDM のセットアップが完了し、アクションがトリガされると、自動的に要求を開始できます。

CA SDM チケット ステータス設定の構成

CA SDM の 12.5 以前のバージョンではヘルプ デスク チケットに APP （承認済み）および REJ （拒否）のデフォルトのステータス コードの設定が使用されていました。 CA Server Automation では、ヘルプ デスク チケットの承認時に開始される操作を実行するためにこれらの承認コードを使用し検索します。 これらの操作には限定されていませんが、アクションの実行、システムの予約などが含まれます。 CA SDM のバージョン 12.5 を使用している場合は、新規チケット ステータス コードがサポートされています。 PRBAPP （承認済み）および PRBREJ （拒否）は CA Server Automation の既存の承認コードに関連付ける必要があります。 新しいコードをサポートし、製品を正しく動作するには、以下の手順に従って設定ファイルを更新します。

チケット ステータス設定を変更する方法

1. テキスト エディタを使用して CA Server Automation *Install_Path*¥conf ディレクトリにある caaipconf.cfg ファイルを開いて［ヘルプ デスク］セクションにスクロールします。
2. 以下のようにして特殊なステータス コードのプロパティを検索します。

```
<property name="SPECIAL_STATUS_CODE">
    <!-- APP_CODE=PRBAPP;REJ_CODE=PRBREJ;(each code must be terminated by a
    semicolon) -->
    <value/>
    <displayName>SD R12.5 以降に追加されたコードのタイプ</displayName>
</property>
```

3. 以下のようにしてコードを非コメント化して変更します。

```
<property name="SPECIAL_STATUS_CODE">
    <value>APP_CODE=PRBAPP;REJ_CODE=PRBREJ;</value>
    <displayName>SD R12.5 以降に追加されたコードのタイプ</displayName>
</property>
```

   CA Server Automation は CA SDM 12.5 のステータス コードを使用できるように設定されました。

4. ファイルを保存して閉じ、設定の変更を有効にします。

ルールの設計

ルールとアクションをセットアップする場合は、以下の点について考慮します。

- 分析する VM、サーバ、およびサービス
- CA Server Automation が違反を検出したときに実行するアクション
- 汎用にするルールと特殊にするルール スクリプトまたはバッチ ファイルが含まれる汎用ルールを計画する場合は環境への影響を慎重に考慮します。
- 評価の対象として興味のあるメトリック
- アクションがトリガされるまでに、ルールに違反する回数 アクションを過度に実行すると、環境でパフォーマンスに負の影響を与えることを考慮します。

  注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。 スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

ルールの作成

ルールは、ルール条件が True と評価された場合にアクションを実行するトリガとして機能します。

注: 元の作成者または管理者のみがルールを編集または削除できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーのサーバまたはサービスを選択します。
2. ［ポリシー］タブをクリックし、次に、［ルール］タブをクリックします。

   ［ルール］ページが表示されます。
3. ［+］（新しいルールの追加）をクリックします。

   ［ルール/テンプレート］ウィザードが表示されます。

4. ［識別］セクションでルールに意味のある名前を入力し、次に、［ルール］を選択してルールを作成します。

   注: 複数のルール定義で使用できるルール テンプレートを作成するには［テンプレート］を選択します。

5. ［有効］を選択してルールをアクティブにします。
6. ［許可される実行回数］として［無制限］を選択するか、［最大］を選択して最大再試行回数を入力します。

   注: ルールが実行される回数に制限を設定することで、再試行が過度に発生してシステムの応答時間が遅くなる事態を防ぐことができます。

7. ［次へ］をクリックします。

   ［テンプレートのモデル化およびアクションの選択］セクションが表示されます。

8. テンプレートにルールをモデル化するかどうか定義します。既存のテンプレートを選択するか、または新規テンプレートの名前を入力し、［有効］を選択してテンプレートへのすべての変更を継承します。
9. リストからルールのアクションを選択します。［次へ］をクリックします。

   ［ルールの定義式］セクションが表示されます。

10. ［ルールの評価式］セクションで以下のフィールドを入力することにより、ルールの条件式を作成します。

    ソース

    ルールが評価するデータのソースを指定します。ソースは［全体使用率］、［イベント］、または特定のサーバ メトリックにすることができます。

演算子

［値］フィールドに入力する値に対しソース データを評価する方法を指定します。 有効な演算子はソースによって異なります。 たとえば、［全体使用率］を選択した場合、以下の演算子が有効です。

"=" "!=" "<" "<=" ">" ">="

［イベント］を選択した場合、値は以下のとおりです。

contains

文字列またはサブ文字列と完全に一致します。 ［値］フィールドにワイルドカードは使用できません。

RegEx（正規表現）

指定された正規表現に一致する文字列が検索された場合は true の値を返します。 指定された正規表現に一致する文字列が検索されなかった場合は false の値を返します。

NotRegEx

指定された正規表現に一致する文字列が検索されなかった場合は true の値を返します。 指定された正規表現に一致する文字列が検索された場合は false の値を返します。

重要: ルールとアクション名に一致させる文字列が含まれていないことを確認します。 このベストプラクティスにより、イベントが次のルール評価サイクルで一致した場合に、アクションの追加の実行を回避することができます。

例： ［値］フィールドに一致する文字列として *しきい値* が含まれる場合、以下のイベントが一致します。

イベント A： メモリの *しきい値* が超えました。

イベント B： しきい値

値

選択された演算子がソース データを評価するための、数値または英数文字列を指定します。

遅延

アクションをトリガする前に、ルールが True と評価される必要がある頻度を定義します。 定義するアクションによっては 1 回発生した後でトリガされる場合があります。 その他のアクションでは多数の発生が永続的な問題を示した後でのみ、トリガされる必要があります。 **注**: ソースが［イベント］に設定された場合、［遅延］はデフォルトでは無効になります。

論理演算子

論理演算子 AND または OR を使用することによって、複数の数式を定義します。 ［新規］をクリックして各定義を完成し、定義された数式のリストに数式を追加します。 定義する最後の数式はデフォルトでは［NOOP］に設定されます。

条件式は、ルールが true と評価されたときに、アクションをトリガするために使用されます。 ［設定の確認］セクションが表示されます。

11. ルールの詳細を確認し、ページの一番上で［次へ］をクリックします。
12. ［終了］をクリックして更新をコミットします。

    ルールまたはテンプレートがルール リストに追加されます。
13. ［ルール リストに戻る］リンクをクリックしてルールが追加されたことを確認します。

例: サーバ レベル ルールの設定

この例では、サーバが CPU とメモリのしきい値を 3 回以上越えた場合、またはサーバが検出されたことを示すイベントが発生した場合のルールを設定します。

ルールの式:

1. CPU 使用率 % > 80 （遅延 3） AND
2. メモリ使用率 % > 50 （遅延 3） OR
3. 検出されたイベント RegEx .*
4. NOOP が検出されたイベント RegEx .*

アクション: 200 の CPU 共有を追加する（最大 8000）

事前定義済みアクション タイプの使用

ルールには、事前定義済みアクション タイプを選択できます。 ルールの条件が true に評価された場合、定義したアクションが実行されます。

次の手順に従ってください:

1. ［ポリシー］タブをクリックし、次に、［アクション & ルール］タブをクリックします。

   ［アクション & ルール］ページが表示されます。

2. ［アクション］タブをクリックします。

   ［アクション］ページが表示されます。

3. ［+］（新しいアクションの追加）をクリックします。

   ［アクションの定義: 新規］ページが表示されます。

4. ［名前］テキスト ボックスでアクションに意味のある名前を入力し、以下のメニューを使用して、事前定義済みアクション タイプを選択します。

   - ［カテゴリ］ - 製品の機能領域フィルタ。 すべてのアクション タイプをリスト表示するには、［すべてのカテゴリ］を選択します。
   - ［タイプ］ - 利用可能なアクション タイプ
   - ［環境］ - 適用可能なプラットフォーム（たとえば VMware vCenter または Microsoft Hyper-V）

   ［詳細］セクションが表示されます。 セクション内に表示されるオプションは、選択したアクション タイプによって異なります。

5. ［アクションの開始］ドロップダウン メニューで、以下の設定のいずれか 1 つを選択します。

   遅延なし

   そのアクションを使用するルールが再度トリガされた場合に同じアクションをすぐに再実行できるように指定します。

   遅延時間

   アクションを使用するルールが再度トリガされた場合に、同じアクションを再実行できるまでに待機する必要がある時間を秒数で指定します。

   注: アクションがスケジュール済みジョブによって実行される場合は、［アクションの開始］設定は効力がありません。

6. ［アクションの完了］ドロップダウン リストで以下の設定のいずれか 1 つを選択します。

   待機なし

   アクションが完了するまで待機せずにアクション シーケンスの次のアクションを実行するように指定します。

   最大待機時間

   アクション シーケンスで次のアクションが実行される前に完了するアクションに対して最大待機時間を分数で指定します。

   完了まで待機

   アクションが完了するのを待機するように指定します。 アクション シーケンスの次のアクションは、このアクションが完了した後に限って実行されます。

   注: ［アクションの完了］ドロップダウン リストは、長期に実行されるアクションにのみ表示されます。

7. 要求された情報をフィールドに入力します。

8. チケットがサードパーティによる承認が必要な場合は、［ヘルプ デスク承認］チェック ボックスをオンにします。

   注: このオプションを使用するには、CA SDM を設定する必要があります。

   ［チケット タイプ］および［テンプレート］フィールドが有効になります。

   注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。 スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

9. チケットを承認後に自動的にクローズする場合は、［承認または拒否時にチケットを自動的にクローズ］を選択します。

10. ［チケット タイプ］ドロップダウン リストからチケット タイプを選択します。以下のタイプは有効なオプションですが、設定によって異なります。

    - デフォルト
    - インシデント
    - 問題
    - 要求

    ［テンプレート］ドロップダウン リストは選択したチケット タイプに関連付けられたテンプレートで更新されます。

11. ［テンプレート］ドロップダウン リストからテンプレートを選択します。

    使用しているチケット モデルに応じて事前定義された値が各フィールドに入力されます。

12. ［保存］をクリックします。

    確認メッセージにより、正常に保存されたことが通知されます。

    テストのために[アクション]ページからアクションを実行するには、アクションを選択して［アクションの実行］アイコンをクリックします。

アクション タイプ

利用可能なアクション タイプにはいくつかのカテゴリがあります。

注: 任意の操作で特殊文字または予約文字を使用する場合、オペレーティング システムおよびシェル動作を考慮する必要があります。 動作には、オペレーティング システム シェルによって実行されるカスタム スクリプトの呼び出しが含まれています。シェル動作、および特殊文字をエスケープする方法の詳細については、Microsoft TechNet の Web サイト http://technet.microsoft.com/en-us/library/cc723564.aspx を参照してください。

事前定義済みアクション タイプ

事前定義済みアクション タイプは、ルールにアクションを作成する場合に使用できる一般的に用いられるアクションです。アクション タイプは呼び出しコマンド ライン ユーティリティです。 すべてのアクション タイプは、ユーザ インターフェースの [ポリシー] ページの [アクション & ルール] ページにリスト表示されています。

注: アクション タイプの詳細な説明については、「*オンライン ヘルプ*」を参照してください。

カスタム アクション タイプ

完全なコマンド ラインを入力する代わりに、代替文字列を使用して、カスタム アクション タイプを作成できます。 カスタム アクション タイプは事前定義済みアクション タイプのドロップダウン リストに追加されます。ユーザ インターフェースの [管理] ページで、一般的に、カスタム アクションへのユーザ アクセスを制御したり、個別のカスタム アクションへのアクセスを制御できます。

[コマンド スクリプトの実行] アクション タイプでは、サーバ上で複数のアクションを実行できる文字列代替を提供します。 文字列代替によって、より柔軟なルールを提供し、カスタム スクリプトの必要性を削減します。 以下の文字列代替が利用可能です。

- %ACTIONNAME%
- %EVENTMESSAGE%
- %EVENTSOURCE%
- %RULENAME%
- %SERVER%
- %SERVICE%

以下の文字列代替はアクション シーケンスで実行されるアクションにのみ有効です。

- %STDOUT% - 標準出力
- %STDERR% - 標準エラー
- %EXITCODE% - アクション終了コード

アクション シーケンス

アクション シーケンスはアクション タイプとして処理され、［ポリシー］ページで他のアクション タイプと共にドロップダウン リストに表示されます。アクション シーケンスでは、指定されたシーケンスでルールに複数のアクションを定義し、単一のアクションとしてそれらを実行することができます。名前で指定したアクションのシーケンスを保存できます。また、そのシーケンスは繰り返して使用できるように管理データベースに保存されます。ユーザ インターフェースの［ポリシー］-［アクション & ルール］ページを使用して、ジョブとしてアクション シーケンスをスケジュールできます。 アクション シーケンスに対する CA SDM サポートは、他のアクション タイプに対する処理とは異なります。 シーケンスで実行される個々のアクションにヘルプデスク承認を設定できますが、ヘルプ デスク承認をアクション シーケンス全体に設定することはできません。

アクション シーケンスを使用する場合は以下の重要な点を考慮します。

- 無限ループを作成するシーケンスは設定しないでください。 アクション シーケンスは同期的に実行されますが、いくつかのアクションは非同期的に実行されます。 そのため、特定のアクションに対して返される時にタスクが完了していることを期待する場合は、注意して使用してください。 一般的に長期間実行している同期的なアクションには -wait パラメータがあり、戻る前、または指定されたタイムアウトの後で、タスクが完了するまで待機させます。
- アクション シーケンスに関連付けられているアクションを削除しようとすると、製品によって、そのアクションが削除されないように阻止されます。
- アクション シーケンスが異常終了した場合は、ポリシー マネージャが再起動するときに、最新の既知のシーケンスで再起動します。 進行中のアクション シーケンスは、手動でユーザ インターフェースまたは Web サービスから取り消すことができます。

- アクション シーケンスで実行しているカスタム アクションに %STDOUT% （標準出力）、%STDERR% （標準エラー）、または %EXITCODE% （アクション リターン コード）の代替文字列アクションを指定する場合、前のアクションの標準出力/標準エラー/終了コードは、現在のアクションにパイプ処理することができます。 パイプ処理では、次のアクションの入力に最初のアクションの出力を使用します。 アクションの出力をリダイレクトすると、それを次のアクションにパイプ処理することはできません。 たとえば、カスタム アクション *ipconfig* が ipconfig_output.txt という名前のテキスト ファイルにリダイレクトされた場合、次のアクションのパイプ処理にその出力を使用することはできません。

事前定義済みアクション タイプのリスト

このセクションでは、ポリシー ルールのアクションを作成するのに利用できる、以下の事前定義済みアクション タイプについて説明します。

ディスクの追加: VMware vCenter

ディスクの追加アクション タイプでは、仮想マシンにディスクを追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

ディスクの追加先となる仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

データストア

選択した VM の ESX サーバに関連付けられているデータストアの名前を指定します。 ドロップダウン リストから 1 つ選択します。

ドライブ サイズ

追加ディスクのサイズを指定します。値を入力し、ドロップダウン リストから［MB］または［GB］を選択します。

SCSI コントローラ

追加ディスクの作成に使用する SCSI コントローラを指定します。 ドロップダウン リストから 1 つ選択します。

[シン プロビジョニング]チェック ボックス

シン プロビジョニングを有効にするかどうかを指定します。

ディスク モード

ディスク モードを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- 永続
- 独立永続
- 独立非永続

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

ネットワーク インターフェースの追加: VMware vCenter

ネットワーク インターフェースの追加アクション タイプを使用すると、仮想マシンに仮想 NIC を追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

仮想 NIC の追加先となる仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

デバイス タイプ

デバイス タイプを指定します。 ドロップダウン リストから 1 つ選択します。

ネットワーク

選択した VM の ESX サーバに関連付けられているネットワークを指定します。 ドロップダウン リストから 1 つ選択します。

以下の命名規則に基づいて、標準スイッチと分散仮想スイッチの名前を区別できます。

- 標準スイッチの名前はネットワーク名です。
- 分散仮想スイッチの名前は、dvPort グループ名の後に、丸かっこで囲まれた分散仮想スイッチ名を連結したもの（dvPortGroupName (dvSwitchName)）です。

MAC アドレス

（オプション）MAC アドレスを指定します。 MAC アドレスが自動生成されるようにしたい場合は、フィールドを空白のままにします。

[ウェイク オン ラン]チェック ボックス

仮想 NIC の LAN 上でのウェイクアップを設定するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

サーバをサービスに追加

サーバをサービスに追加アクション タイプでは、既存のサービスにサーバを追加できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス名

サービスの名前を指定します。

サーバ リスト(カンマで区切られたリスト)

サービスに追加するサーバのリストを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシン状態の変更: Microsoft Hyper-V

マシン状態の変更アクション タイプでは、Hyper-V 環境内の仮想マシンの状態変更を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

状態

仮想マシンの希望する状態を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- 電源オフ
- シャットダウン
- 保存
- 中断
- 開始

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンのクローン作成: Solaris ゾーン

Solaris ゾーン マシンのクローン作成アクション タイプでは、既存のゾーンからデータをコピーすることにより、新しいゾーンを設定およびインストールします。 この操作を、グローバル ゾーンまたはインストールされた状態のゾーンに対して実行することはできません。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ゾーン ホスト

クローン作成するゾーンが含まれる Solaris ゾーン ホストを定義します。

ゾーン

クローン作成するゾーンを定義します。イベント メッセージから抽出されたテキストを使用できます。

名前

新しいゾーンの名前を定義します。 自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

パス

新しいゾーンのインストール パスを定義します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

CPU/メモリの設定: IBM LPAR

CPU/メモリの設定アクション タイプでは、IBM LPAR 環境内の仮想マシンに割り当てる CPU リソースとメモリ リソースに対して制限を設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

パーティション名

パーティションの一意の名前を表示します。

プロファイル名

選択した LPAR の既存のプロファイル名を指定します。

オペレーション

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- メモリ ユニットの追加
- メモリ ユニットの削除
- プロセッサの追加
- プロセッサの削除

プロセッサ

追加または削除するプロセッサの数を指定します。

調整タイプ

調整タイプを指定します。 オプションを 1 つ選択します。

- 動的調整のみ
- 動的調整およびプロファイル更新

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

CPU/メモリの設定: Microsoft Hyper-V

CPU/メモリの設定アクション タイプでは、Hyper-V 環境内の仮想マシンに割り当てる CPU 共有とメモリ共有の数を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

CPU 割り当て

仮想マシンの CPU 割り当てを指定します。 ドロップダウン リストから、以下のいずれかを調整します。

- CPU 数
- CPU 予約 %
- CPU の重み
- CPU 制限 %
- 現在の CPUID

メモリ割り当て

仮想マシンに割り当てるメモリ共有を指定します（メガバイト）。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

CPU/メモリの設定: VMware vCenter

CPU/メモリの設定アクション タイプでは、CPU リソースとメモリ リソースに対して制限を設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

ターゲット VM マシン

リソース調整の対象となる仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

操作

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- CPU 制限の設定
- メモリ制限の設定
- CPU 予約の設定
- メモリ予約の設定

MHz、MB

選択した操作について適切な値を入力します。

[無制限]チェック ボックス

選択した操作においてリソースを無制限に使用することを許可します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

電源の設定: Cisco UCS

このアクション タイプでは、UCS ブレード サーバ用の電源管理アクションを設定できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

UCS Manager

UCS Manager の名前を指定します。

UCS シャーシ

UCS シャーシの名前を指定します

UCS ブレード

UCS ブレードの名前を指定します

電源操作

ドロップダウン リストから操作を選択します。

サイクル即時

ただちにブレードの電源をオンにしてオフにします。

サイクル待機

グレードの電源を入れ直し、すべてのアプリケーションにシャットダウンを通知します。

ハード リセット即時

ブレードの電源を入れ直します（ブレードの電源プラグを抜くのと似た作用です）。

ハード リセット待機

ブレードの電源をオフにします。 電源をオフにする前に、ブレードによってすべてのアプリケーションにシャットダウンが通知されます。

ソフト シャットダウン

ブレードをシャットダウンします。 シャットダウンする前に、ブレードによってすべてのアプリケーションにシャットダウンが通知されます。

シャットダウン

ブレードをただちにシャットダウンします。

起動

ブレードを起動します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

電源の設定: IBM LPAR

LPAR 電源の設定アクション タイプでは、LPAR の電源設定を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

パーティション名

制御するパーティション名を指定します。

操作

実行する電源操作を指定します。[アクティブ化]を選択する場合は、［操作オプション］セクション内の以下のフィールドに入力します。

パーティション プロファイル

電源設定のアクティブ化に使用するパーティション プロファイルを指定します。

キー ロック

パーティション プロファイル内のキー ロック モードを指定します。 キー ロックによって、システムで許可される電源オンと電源オフのモードが確立されます。キー ロックは、manual または normal のいずれかです。 セキュリティ上の理由により、キー ロック位置を manual に設定することは推奨されません。

起動モード

パーティション プロファイル内の起動モードを指定します。 パーティション プロファイルをアクティブ化するときに別の方法を指定する場合を除き、この起動モードを使って論理パーティション上のオペレーティング システムが起動されます。 CA Server Automation は以下の有効な起動モードをサポートしています。

normal

論理パーティションを normal として開始します。 （多くの日常的なタスクを実行するには、このオプションを使用します）。

open_firmware

論理パーティションを起動して Open Firmware のプロンプトを表示します。サービス担当者は、このオプションを使って追加のデバッグ情報を取得します。

［シャットダウン］を選択する場合は、［操作オプション］セクション内の以下のフィールドに入力します。

遅延

遅延のあるシャットダウン シーケンスを使用して、論理パーティションをシャットダウンします。 このシーケンスでは、ジョブを終了し、ディスクにデータを書き込むための論理パーティション時間が考慮されます。 論理パーティションは、事前定義された時間内にシャットダウンできない場合、異常終了します。 次回の再起動は通常より時間がかかる場合があります。

即時

論理パーティションをただちにシャットダウンします。 HMC はアクティブなすべてのジョブをただちに終了します。 そのようなジョブで実行されているプログラムは、いかなるジョブのクリーンアップも許可されません。 データが部分的に更新されている場合、このオプションを使用すると好ましくない結果になる可能性があります。 このオプションを使用するのは、制御されたシャットダウン試行が失敗した後だけにしてください。

OS のシャットダウン

論理パーティションに対して shutdown コマンドを発行することによって、論理パーティションを通常どおりにシャットダウンします。 この操作中、論理パーティションは必要なシャットダウン アクティビティをすべて実行します。 このオプションは AIX 論理パーティションでのみ利用できます。

OS のシャットダウン即時

論理パーティションに対して shutdown -F コマンドを発行することによって、論理パーティションをただちにシャットダウンします。 この操作中、論理パーティションは他のユーザおよび他のシャットダウン アクティビティへのメッセージをバイパスします。 このオプションは AIX 論理パーティションでのみ利用できます。

［再起動］を選択する場合は、［操作オプション］セクションから *1* つのオプションを選択します。

パーティション プロファイル

パーティションの再起動に使用するパーティション プロファイルを指定します。

即時

論理パーティションをただちにシャットダウンします。 HMC はアクティブなすべてのジョブをただちに終了します。 そのようなジョブで実行されているプログラムは、いかなるジョブのクリーンアップも許可されません。 データが部分的に更新されている場合、このオプションを使用すると好ましくない結果になります。このオプションを使用するのは、制御されたシャットダウン試行が失敗した後だけにしてください。

OS のシャットダウン

論理パーティションに対して shutdown コマンドを発行することによって、論理パーティションを通常どおりにシャットダウンします。 この操作中、論理パーティションは必要なシャットダウン アクティビティをすべて実行します。 このオプションは AIX 論理パーティションでのみ利用できます。

OS のシャットダウン即時

論理パーティションに対して shutdown -F コマンドを発行することによって、論理パーティションをただちにシャットダウンします。 この操作中、論理パーティションは他のユーザおよび他のシャットダウン アクティビティへのメッセージをバイパスします。 このオプションは AIX 論理パーティションでのみ利用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

電源の設定: Microsoft Hyper-V

電源の設定アクション タイプでは、Hyper-V 環境内にある仮想マシンの起動とシャットダウンを制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

状態を変更する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

アクション開始

Hyper-V Server の開始時に実行するアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- 常に

  Hyper-V Server の開始時に常に VM を開始します。

- 自動

  Hyper-V Server の開始時に自動的に VM を開始します。

- なし

  Hyper-V Server の開始時に VM を開始しません。

開始遅延

Hyper-V Server の開始後に VM を開始する遅延時間（数秒）を調整します。 ドロップダウン リストから 1 つ選択します。

シャットダウン アクション

仮想マシンのシャットダウン時に実行するアクションを指定します。ドロップダウン リストから、以下のいずれかを選択します。

- オフ

  Hyper-V Server のシャット ダウン前に VM をオフにします。

- 保存

  Hyper-V Server のシャット ダウン前に VM を保存（中断）します。

- シャットダウン

Hyper-V Server のシャット ダウン前に VM をシャットダウンします。

復旧アクション

Hyper-V Server で障害が発生したときに仮想マシンの以前の詳細を回復するためのアクションを指定します。 ドロップダウン リストから、以下のいずれかを選択します。

- なし

  サーバ障害発生後の Hyper-V Server の開始時に特別なアクションを行いません。

- 再起動

  サーバ障害発生後の Hyper-V Server の開始時に VM を再起動します。

- 元に戻す

  サーバ障害発生後の Hyper-V Server の開始時に、最新のスナップショットを使って VM を元に戻します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

電源の設定: VMware vCenter/vApp 電源の調整

電源の設定アクション タイプは、VMware vCenter 環境内の仮想マシンおよび vApp の電源設定を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VM/vAPP

ターゲット タイプ（VM または vApp）を指定するラジオ ボタン。

ターゲット

電源調整の対象となる仮想マシンまたは vApp の名前を指定します。ドロップダウン リストから 1 つ選択します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

電源操作

実行する電源操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- VC 電源オン
- VC 電源オフ
- VC 電源リセット
- VC 電源中断
- VC 電源シャットダウン
- vApp の電源オン
- vApp の電源オフ
- vApp の中断

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

サービス プロファイルの設定: Cisco UCS

［サービス プロファイルの設定］アクション タイプでは、サービス プロファイルの UCS ブレード サーバへの関連付け、関連付け解除、またはフェールオーバを実行できます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

UCS マネージャ

UCS Manager の名前を指定します。

UCS Chassis

Cisco UCS シャーシの名前を指定します。

UCS ブレード

Cisco UCS ブレードの名前を指定します。

サービス プロファイル

サービス プロファイルの名前を指定します。

プロファイル操作

ドロップダウン リストからプロファイルを選択します。

関連付け

サービス プロファイルをブレードに関連付けます。

関連付け解除

ブレードからサービス プロファイルを関連付け解除します。

フェールオーバ

このオプションを使用すると、サービス プロファイルに対してチェック ボックスが表示されます。このチェックボックスをオンにすると、サービス プロファイルは次に利用可能なブレードに自動的にフェールオーバされるようになります。 デフォルトでは、チェック ボックスはオンになっています。また、シャーシおよびブレードのドロップダウンは両方とも無効になっています。

特定のサービス プロファイルのフェールオーバ用にシャーシとブレードを指定したい場合は、チェック ボックスをオフにします。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

共有の設定: VMware vCenter

共有の設定アクション タイプでは、VMware vCenter 環境内にある仮想マシンの CPU 共有とメモリ共有を制御します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

ターゲット VM マシン

共有調整の対象となる仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

操作

実行する操作を指定します。ドロップダウン リストから、以下のいずれかを選択します。

- CPU の設定
- CPU の追加
- CPU の削除
- メモリの設定
- メモリの追加
- メモリの削除

値

選択した操作について適切な値を入力します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレートを VM に変換: VMware vCenter

［テンプレートを VM に変換］アクション タイプを使用すると、テンプレートを仮想マシンに変換できます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

VM が配置されているデータ センターを指定します。 ドロップダウン リストから 1 つ選択します。

VC 計算リソース

VM が作成されるクラスタまたは VMware ESX ホストを指定します。ドロップダウン リストから 1 つ選択します。

VC ESX サーバ

VM が常駐する VMware ESX サーバを指定します。 ドロップダウン リストから 1 つ選択します。

VC リソース プール

クローン作成用の VM の選択元となるリソース プールの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC テンプレート

変換対象のテンプレートの名前を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

VM をテンプレートに変換: VMware vCenter

VM をテンプレートに変換アクション タイプでは、電源がオフの仮想マシンをテンプレートに変換できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC 仮想マシン

変換対象の仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択するか、イベント メッセージから抽出されるテキストを使用します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

イベントの作成

イベントの作成アクション タイプでは、システム ディスカバリ、システム削除、複数システムのディスカバリ、システム管理ステータスの変更などのイベントを作成できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

イベント ステータス

イベントのステータスを指定します。

イベント コンポーネント

イベントに関係のあるコンポーネント名を指定します。

イベント メッセージ

イベントが生成されたというメッセージを指定します。

イベント ソース

イベントのソースを指定します。

イベント ターゲット

イベントのターゲットを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

レポートの作成

［レポートの作成］アクション タイプを使用すると、自動的にレポートを作成できます。 このアクションをスケジュールして、レポートが定期的に作成されるようにすることができます。このアクション タイプも［レポート］タブから作成できます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

レポート タイプ

作成されるレポートのタイプを指定します。利用可能なレポート タイプおよび関連する作成オプションの説明については、「レポート」を参照してください。

生成されたレポートは、［スケジュール済みレポート］フォルダの［レポート］タブで表示できます。

サービスの作成

サービスの作成アクション タイプでは、モニタ対象のサーバを構成して、ビジネス ニーズで要求されるリソースが反映された論理サービスへと変えることができます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス名

サービスの名前を指定します。

サーバ リスト(カンマで区切られたリスト)

利用可能なサーバのリストを指定します。

下限しきい値

サービス全体の下限しきい値を指定します。

上限しきい値

サービス全体の上限しきい値を指定します。

遅延

アクションをトリガする前に、ルールが True と評価される必要がある頻度を定義します。 条件が 1 回満たされたときにトリガすべきアクションもあれば、条件が何回も満たされて永続的な問題の可能性が示されて初めてトリガすべきアクションもあります。

優先度

1 回のポーリング サイクルでアクションを実行する順序を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンの削除: IBM LPAR

LPAR マシンの削除アクション タイプでは、指定した LPAR を削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

パーティション名

削除するパーティション名を定義します。

注: このアクションの場合、削除するパーティションの電源をオフにする必要があります。 このアクションによって、論理パーティションと、パーティション プロファイルに格納された設定データが消去されます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンの削除: Microsoft Hyper-V

Hyper-V VM の削除アクション タイプでは、Hyper-V Server 環境から仮想マシンを削除します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Hyper-V ホスト

Hyper-V Server が常駐するホストの名前を指定します。 ドロップダウン リストから 1 つ選択します。

Hyper-V VM 名

削除する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

付属のリソース

削除する仮想マシンに付属するリソースを指定します。 削除するリソースを選択します。

- ハード ドライブ
- フロッピー ドライブ
- DVD/ISO イメージ

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンの削除: Solaris ゾーン

Solaris ゾーン マシンの削除アクション タイプでは、Solaris ゾーン ホストからゾーンを削除します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ゾーン ホスト

削除するゾーンが含まれる Solaris ゾーン ホストを定義します。

ゾーン

削除するゾーンを定義します。 自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンの削除: VMware vCenter

vCenter VM の削除アクション タイプでは、VMware vCenter Server 環境から仮想マシンを削除します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

VC データ センター

仮想マシンが常駐するデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。 選択したデータ センターは、そのデータ センターに関連付けられた VM の名前と共に、［ターゲット VM マシン］ドロップダウン リストに入力されます。

ターゲット VM マシン

削除する仮想マシンの名前を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

名前でホストを検出

名前でホストを検出アクション タイプでは、指定のホスト名を使ってホストを検出できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ホスト名

ホスト名を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

ネットワークの検出

ネットワークの検出アクション タイプでは、ドメイン内で利用できるネットワークを検出できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

ネットワーク ID

検出するネットワーク ID を指定します。

ネットワーク名

検出するネットワーク名を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

分散スイッチの管理: VMware vCenter

分散仮想スイッチを管理するには、このアクション タイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

以下のいずれか 1 つの操作を選択します。

- ポート グループの追加
- ポート グループの削除
- ポート グループの更新

Virtual Center

vCenter Server を指定します。 ドロップダウン リストから 1 つ選択します。

仮想スイッチ

管理する仮想スイッチを指定します。ドロップダウン リストから 1 つ選択します。

ポート グループ

ポート グループ名を指定します。 ドロップダウン リストから 1 つ選択します。

バインド タイプ(オプション)

以下のバインド タイプのいずれかを選択します。

earlyBinding

VM がポートグループにバインドする際にポートを割り当てます。このバインディング タイプは、接続性の常時確保に有効ですが、ポートが永続的に予約されます。 デフォルトはこのバインディング タイプです。

lateBinding

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。 このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。LateBinding は vCenter で設定できます。

ephemeral

VM の電源がオンで NIC の状態が接続済みの場合、VM にポートを割り当てます。 このバインディング タイプは、VM の電源がオフになるか、NIC が切断されると、ポートを割り当て直します。 ephemeral バインディングは、ESX ホストと vCenter で設定できます。

VLAN ID（**オプション**）

仮想ポート グループの操作に使用される整数値を指定します。

ポート数（オプション）

ポート グループのポートの数を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

フォールト トレランスの管理: VMware vCenter

フォールト トレランスを管理するには、このアクション タイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

指定した VM について以下のいずれかの操作を選択します。

- 電源オン
- 電源オフ
- 有効
- 無効
- セカンダリ VM のマイグレート

Virtual Center

vCenter Server のホスト名を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

VM が属するデータセンターを指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

フォールト トレラント VM を指定します。ドロップダウン リストから 1 つ選択します。

セカンダリ ホスト

セカンダリ VM が常駐する ESX サーバを指定します。 ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

VM スナップショットの管理: VMware vCenter

VM スナップショットの管理アクション タイプでは、指定したターゲット システム上の仮想マシン スナップショットを作成する、元に戻す、または削除することができます。

注: ESXi ホストを vCenter から削除した後に再度追加したために VM スナップショットの管理アクションが失敗する場合は、対応するスナップショットを再度選択し、アクションを保存してください。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Operation

以下のいずれかのアクションを指定します。

- スナップショットの作成
- スナップショットに戻す
- スナップショットの削除

［スナップショットの作成］を選択する場合は、以下のフィールドに入力します。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。 ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを作成する仮想マシンの名前を指定します。 ドロップダウン リストから仮想マシンを選択します。 あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

名前

作成する仮想マシン スナップショットの名前を定義します。 自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

説明

（オプション）仮想マシン スナップショットについて説明します。

[メモリのキャプチャ]チェック ボックス

（オプション）スナップショットの一部としてのシステム実行メモリを使ってスナップショットを作成するかどうかを指定します。

［スナップショットに戻す］を選択する場合は、以下のフィールドに入力します。

VC サーバ

vCenter が常駐するサーバの名前を指定します。ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する vCenter 内のデータ センターの名前を指定します。ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを元に戻す仮想マシンの名前を指定します。 ドロップダウン リストから仮想マシンを選択します。

名前

元に戻す仮想マシン スナップショットの名前を定義します。

名前を入力するか、双眼鏡のアイコンをクリックし、表示されるダイアログ ボックスで元に戻すスナップショットを選択します。

ID

元に戻す仮想マシン スナップショットの ID を定義します。

注: スナップショットを元に戻すには名前または ID のいずれかを使用します。両方は必要ありません。 1 つの仮想マシンについて同じ名前のスナップショットが複数ある場合は、ID が必要です。

［スナップショットの削除］を選択する場合は、以下のフィールドに入力します。

VC サーバ

vCenter が常駐するサーバの名前を指定します。ドロップダウン リストからサーバを選択します。

データ センター

仮想マシンが常駐する vCenter 内のデータ センターの名前を指定します。ドロップダウン リストからデータ センターを選択します。

仮想マシン

スナップショットを削除する仮想マシンの名前を指定します。 ドロップダウン リストから仮想マシンを選択します。

名前

削除する仮想マシン スナップショット名を定義します。

名前を入力するか、双眼鏡のアイコンをクリックし、表示されるダイアログ ボックスで削除するスナップショットを選択します。

ID

削除する仮想マシン スナップショットの ID を定義します。

注: スナップショットを削除するには名前または ID のいずれかを使用します。両方は必要ありません。 1 つの仮想マシンについて同じ名前のスナップショットが複数ある場合は、ID が必要です。

[子の削除]チェック ボックス

（オプション）スナップショットのすべての子を削除するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

仮想スイッチの管理: VMware vCenter

仮想スイッチを管理するには、このアクション タイプを使用します。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

操作

以下のいずれか 1 つの操作を選択します。

- ポート グループの追加
- ポート グループの削除
- ポート グループの更新

Virtual Center

vCenter Server を指定します。 ドロップダウン リストから 1 つ選択します。

データセンター

データセンターを指定します。ドロップダウン リストから 1 つ選択します。

ESX **サーバ**

仮想スイッチが属する ESX サーバを指定します。ドロップダウン リストから 1 つ選択します。

仮想スイッチ

管理する仮想スイッチを指定します。ドロップダウン リストから 1 つ選択します。

ポート グループ

ポート グループ名を指定します。 ドロップダウン リストから 1 つ選択します。

VLAN ID (**オプション**)

仮想ポート グループの操作に使用される整数値を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

Windows サービスの管理

Windows サービスの管理アクション タイプは、AutoShell コマンド ラインおよびスクリプト環境を使用して Windows サービスを制御します。

アクションの定義の［詳細］セクションには、以下のフィールドが含まれます。

操作オプション

サービスで実行される操作を指定します。

注: クエリ サービス操作が返す Windows サービス ステータスは %STDOUT% パラメータからのみ取得できます。イベント テーブルからは利用できません。このパラメータはアクション シーケンスで実行されるアクションでのみ有効です。

注: 以下の動作は Windows で直接実行されたサービス管理と異なります。

- サービスが「停止済み」のステータスであっても、［サービスの再起動］操作を実行できます。サービス ステータスは「開始済み」に変更されます。
- サービスが「開始済み」のステータスのときに［サービスの無効化］操作を実行すると、サービスは無効になります。また、そのステータスは「停止済み」に変わります。

ホスト名

サービスが実行されるコンピュータの名前を定義します。

ユーザ名

ユーザ名を定義します。

パスワード

パスワードを定義します。 確認のためパスワードを再入力します。

サービス名

操作の対象となるサービスの名前を定義します。 名前を入力するか、イベント メッセージから抽出されるテキストを使用します。

注: Windows でサービスの［プロパティ］ダイアログ ボックスを開いて、サービス名を確認します。 ［コンピュータの管理］ウィンドウに表示される表示名と混同しないでください。

［サービス スタートアップ タイプの変更］を選択した場合は、以下のフィールドに入力します。

スタートアップ タイプ

サービスに設定されるスタートアップ タイプを指定します。オプションには［自動］、［手動］、［無効］があります。［起動］オプションは、デバイス ドライバがブート ローダによってロードされることを意味します。［システム］オプションは、デバイス ドライバがカーネル初期化中に開始されることを意味します。

［サービス依存関係の変更］を選択した場合は、以下のフィールドに入力します。

依存関係

サービスを開始できる前に実行されている必要がある依存関係（他のサービス、システム ドライバ、またはロード オーダー グループ）を定義します。 複数の依存関係を定義する場合は、スラッシュでそれらを区切ります。

［サービス アカウントの変更］を選択した場合は、以下のフィールドに入力します。

ローカル システム アカウント/このアカウント

サービスがログインするアカウントを指定します。LocalSystem アカウントを使用するか、またはここでアカウントを定義します。

マシンをマイグレート: VMware vCenter

vCenter VMotion のマイグレーション アクション タイプでは、VMware VMotion を使用して仮想マシンをマイグレートします。この操作を行うには VMware ESX サーバを正しく設定する必要があります。また、ターゲット コンピュータ上には VMotion ライセンスが配置されている必要があります。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

VC サーバ

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

ソース データ センター

ソース仮想マシンが常駐するデータ センターの名前を指定します。ドロップダウン リストから 1 つ選択します。

ソース仮想マシン

ソース VM として使用するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

[デスティネーション ESX サーバ]

マイグレーションのターゲットとなる ESX サーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

注: ESX ホスト間で VM のマイグレーションがサポートされるのは、2 つの ESX ホスト間で VM データストア/ディスクが共有される場合のみです。

デスティネーション リソース プール

使用するリソース プールの名前を指定します。 ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

CPU の変更: VMware vCenter

CPU の変更アクション タイプでは、仮想マシンに割り当てる CPU の数を変更できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

CPU 変更の対象となる仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

CPU

VM に割り当てる CPU の数を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

メモリの変更: VMware vCenter

メモリの変更アクション タイプでは、仮想マシンのメモリ割り当てを変更できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが常駐する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

CPU 変更の対象となる仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

メモリ

VM に割り当てるメモリの量を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

ヘルプデスク チケットのオープン

ヘルプデスク チケットのオープン アクション タイプでは、ヘルプデスク チケットを開くのに使用するプロパティを定義できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サマリ

チケットの詳細を端的に示します。

説明

チケットについて説明します。

エンティティ

(オプション) ヘルプ デスク システムで既知の設定項目とチケットとを一致させるために使用するサーバまたはサービスの名前を定義します。 設定項目のホスト名とエンティティ名が同じである場合、チケットはその設定項目と関連付けられます。

タイプ

チケットのタイプを指定します。

テンプレート

チケットのテンプレートを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

マシンのプロビジョニング : IBM LPAR

このアクション タイプは LPAR をプロビジョニングします。

［ビルド パーティション］セクションには、以下のフィールドが含まれます。

HMC/IVM 名

選択したパーティションが存在する管理対象サーバに関連付けられた HMC/IVM を指定します。

システム名

仮想マシンが存在する IBM LPAR のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

パーティション名

イメージ作成用のパーティションの名前を定義します。

プロファイル名

選択した LPAR の既存プロファイルの名前を定義します。

［メモリ設定］セクションには、以下のフィールドが含まれます。

インストール済みメモリ

インストール済みのメモリが識別されます。

利用可能なメモリ

インストール済みのメモリが識別されます。

最小

最小メモリ量を指定します。

希望

希望するメモリ量を指定します。

最大

最大メモリ量を指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

［プロセッサ］セクションには、以下のフィールドがあります。

処理モード

処理モードを指定します。

以下のオプションから選択します。

- 部分的プロセッサ ユニット（共有）
- 全プロセッサ（専用）

利用可能なユニット

利用可能なプロセッサ ユニットが識別されます。

最小

最小プロセッサ ユニットを指定します。

希望

希望するプロセッサ ユニットを指定します。

最大

最大プロセッサ ユニットを指定します。

I/O コンポーネント

LPAR に関連付ける I/O コンポーネントを指定します。

I/O プール

I/O プールを追加、削除、および変更できます。

最大仮想アダプタ

仮想アダプタの最大数を定義します。

仮想アダプタ

仮想アダプタの数が識別されます。

仮想シリアル アダプタ

仮想シリアル アダプタを追加、削除、および変更できます。

仮想イーサネット アダプタ

仮想イーサネット アダプタを追加、削除、および変更します。

仮想 SCSI アダプタ

仮想 SCSI アダプタを追加、削除、および変更できます。

プロビジョニング プロセスはクライアント コンピュータ上で開始され、ジョブが正常に完了すると確認のメッセージによって通知されます。

マシンのプロビジョニング : Microsoft Hyper-V

Hyper-V VM のプロビジョニング アクション タイプでは、VM を作成およびインストールします。 以下のパラメータを指定します。

アクション定義の［詳細］セクションの先頭ページには、以下のフィールドがあります。

SCVMM サーバ

Microsoft System Center Virtual Machine Manager （SCVMM）ライブラリ サーバを指定します。 ドロップダウン リストから 1 つ選択します。

Hyper-V Server

Hyper-V サーバを指定します。 ドロップダウン リストから 1 つ選択します。

テンプレート

テンプレートを指定します。ドロップダウン リストから 1 つ選択します。

デスティネーション パス

作成する VM のデスティネーション パスを指定します（テンプレートを格納）。 ドロップダウン リストから 1 つ選択します。

VM 名

VM の名前を指定します。

VM の開始

作成した VM を自動的に開始します。 デフォルトでは、新しい VM は電源オフの状態です。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

［次へ］をクリックして表示される 5 番目のページの［詳細］セクションには以下のフィールドがあります。

ハードウェア プロファイル

Microsoft System Center Virtual Machine Manager （SCVMM）ライブラリ サーバによって定義されるハードウェア プロファイルの名前を指定します。

仮想プロセッサ

VM に割り当てる仮想プロセッサの数を指定します。

デフォルト： 1

メモリ

作成する VM の RAM メモリをメガバイト（MB）単位で指定します。

デフォルト： 1024

［次へ］をクリックして表示される 3 番目のページの［詳細］セクションには以下のフィールドがあります。

ゲスト OS プロファイル

（オプション）Microsoft System Center Virtual Machine Manager（SCVMM）ライブラリ サーバによって定義されるゲスト オペレーティング システム プロファイルの名前を指定します。 このパラメータは、SCVMM ライブラリ サーバに格納されているオペレーティング システム構成設定を上書きします。 SCVMM 統合を使って VM のプロビジョニングを行う場合、このパラメータが有効になります。

製品キー

（オプション）VM 用の Windows 製品アクティベーション キーを指定します。 このパラメータをサポートするには、Sysprep ツールを使って作成した Windows イメージが必要です。このオプションはコマンドの非同期実行では無効になります。

フル ネーム

新しい VM にインストールする Windows イメージ（Sysprep ツールを使って作成）のユーザ名を指定します。

組織

（オプション）新しい VM にインストールする Windows イメージ（Sysprep ツールを使って作成）の組織名を指定します。このパラメータをサポートするには、Sysprep ツールを使って作成した Windows イメージが必要です。 このオプションはコマンドの非同期実行では無効になります。

管理者パスワード

（オプション）このオプションは VM 用のデフォルト管理者アカウント パスワードを設定するのに使用します。このパラメータをサポートするには、Sysprep ツールを使って作成した Windows イメージが必要です。 このパラメータは非同期実行では無視されます。

注: このオプションを正常に設定するには、Sysprep ツールを使って作成する Windows Server 管理者パスワードを空に設定します。

ワークグループに参加

VM について作成したいワーク グループを指定します。 ドメインとワーク グループの指定は相互に排他的です。

ドメインに参加

VM のドメイン名を指定します。 ドメインとワークグループの指定は相互に排他的です。

ドメイン ユーザ

デフォルトの Administrators グループの一員として作成するドメイン ユーザ名を指定します。

ドメイン ユーザ パスワード

デフォルトの Administrators グループの一員として作成するドメイン ユーザ アカウントのパスワードを指定します。

［次へ］をクリックして表示される 4 番目のページの［詳細］セクションには以下のフィールドがあります。

DHCP の使用

VM のネットワーク インターフェースで DHCP を有効にするオプションを指定します。 テンプレート イメージに複数のネットワーク アダプタがある場合、DHCP は最初のインターフェースでオンになります。有効にした場合、他のネットワーク パラメータにはアクセスできなくなります。

IP アドレス

VM に割り当てる静的な IPv4 アドレスを指定します。

ネットワーク マスク

VM に割り当てるサブネット マスクを指定します。

デフォルト ゲートウェイ

VM のデフォルト ゲートウェイを指定します。

DNS Server

VM に対して設定する DNS サーバを指定します。

IP メトリック

（オプション）VM に対して設定するインターフェース メトリックを指定します。このオプションは、-ip4ddr オプションと共に使用します。インターフェース名を -ip4addr オプションに指定する場合、このオプションにも同じインターフェース名を使用する必要があります。 このパラメータをサポートするには、Sysprep ツールを使って作成した Windows イメージが必要です。 このオプションはコマンドの非同期実行では無効になります。

デフォルト： 1

マシンのプロビジョニング : Solaris ゾーン

Solaris ゾーン マシンのプロビジョニング アクション タイプでは、ゾーンを作成およびインストールします。Solaris ゾーン ホスト、ゾーン名、ゾーン タイプ、および他のゾーン プロパティを指定します。 作成したゾーンは自動的にインストールされます。

アクション定義の［詳細］セクションの先頭ページには、以下のフィールドがあります。

ホスト

ゾーンを作成する Solaris ゾーン ホストを定義します。

名前

ゾーン名を定義します。 自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

説明

（オプション）ゾーンの説明を定義します。

タイプ

ゾーンが［ネイティブ］、［ルート全体］、［ブランド化］のどれであるかを定義します。ブランド化ゾーンは既存のゾーン テンプレートに基づきます。

テンプレート

（オプション）［タイプ］を［ブランド化］に設定した場合、ゾーンの作成元となるテンプレートを定義します。

インストール アーカイブ パス

ゾーン上のインストール アーカイブのディレクトリ パスを定義します。 このフィールドは、［タイプ］を［ブランド化］に設定した場合にのみ必要になります。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

［次へ］をクリックして表示される 5 番目のページの［詳細］セクションには以下のフィールドがあります。

タイプ

スケジューラ タイプを定義します。 タスクに割り当てられた CPU 共有の数に基づいて CPU 割り当てを制御するためにフェア シェア スケジューリング クラスを使用するには、［FSS］を選択します。

容量

ゾーンに割り当てる物理メモリ容量をメガバイト単位で定義します。

スワップ メモリ

ゾーンに割り当てるスワップ メモリの量をメガバイト単位で定義します。 スワップ メモリは 50 MB 以上である必要があります。

ロック メモリ

ゾーンに割り当てるロック メモリの量をメガバイト単位で定義します。 ロック メモリ量は物理メモリ量より少なくなければいけません。

ゾーン パス

ゾーンのルート ディレクトリ パスを定義します。

NIC タイプ

NIC タイプを定義します。 ドロップダウン リストからタイプを選択します。 NIC を選択しないと、ゾーンには NIC カードまたは IP アドレスが割り当てられません。

IP アドレス

ゾーンの IP アドレスを定義します。

リソース プール

ゾーンと共に使用するリソース プールを定義します。ドロップダウン リストからプールを選択します。ゾーンと共に新しいリソース プールを使用したい場合は、プールを先に作成します。 プールを選択しない場合、デフォルトが使用されます。

自動再起動

グローバル ゾーンが再起動されるとき、ゾーンを自動的に再起動するかどうかを定義します。

マシンのプロビジョニング : VMware vCenter

vCenter マシンのプロビジョニング アクション タイプでは、仮想マシン（VM）をプロビジョニングできます。 テンプレート、およびテンプレートと連携するターゲット vCenter 仕様が必要です。 VM のプロビジョニングに関するサービス ルールが存在する場合、新しい VM は、ルールの作成対象となったサービス内に配置されます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

VC サーバ

vCenter が常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC データ センター

マシンをプロビジョニングするデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC 計算リソース

計算リソースが常駐するサーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC ESX サーバ

プロビジョニングされた VM のターゲットとなる VMware ESX サーバの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC データ ストア

使用するデータ ストアの名前を指定します。 ドロップダウン リストから 1 つ選択します。

VC ターゲットの場所

VC ターゲットの場所を指定します。 ドロップダウン リストから 1 つ選択します。

ホスト名/VM 名

使用する名前または VC 名を仕様内から選びます。 ドロップダウン リストから 1 つ選択します。 あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

ユーザ名

仕様にアクセスするユーザ名認証情報を指定します。

パスワード

仕様にアクセスするためのパスワードを指定します。

VC 仮想マシン

利用可能な VC 仮想マシンのうち、どれを使用するかを指定します。選択した場合は、ドロップダウン リストから 1 つをクリックします。

VC テンプレート

利用可能な VC テンプレートのうち、どれを使用するかを指定します。クリックした場合は、事前に作成済みのソフトウェア パッケージ グループのうちの 1 つをドロップダウン リストから選択します。

NIC（VC テンプレート）

VC テンプレートによって使用されるネットワーク インターフェース カードの数を指定します。

VC 仕様

使用する VC 仕様の名前を指定します。 ドロップダウン リストから 1 つ選択します。

NIC（VC 仕様）

VC 仕様によって使用されるネットワーク インターフェース カードの数を指定します。

OS システム タイプ

プロビジョニングされた VM のオペレーティング システムのタイプを表示します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

メモリ

VM に割り当てるメモリの量をメガバイト単位で指定します。

仮想プロセッサ

VM に割り当てる仮想プロセッサの数を指定します。

データストア

（オプション）ハード ディスクを追加作成するストレージ データストアを指定します。

ドライブ サイズ

（オプション）追加のハード ドライブのサイズを指定します。

SCSI コントローラ

（オプション）ハード ドライブの追加作成に使用する SCSI コントローラを指定します。

ネットワーク管理

ネットワーク接続設定を変更できます。

グローバル NIC 設定

DNS 検索サフィックスを追加できます。

ディスクの削除: VMware vCenter

ディスクの削除アクション タイプでは、仮想マシンからディスクを削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が存在するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが存在する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

ディスクを追加する仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

ハードドライブ

削除するディスクを指定します。ドロップダウン リストから 1 つ選択します。

[ディスク ファイルの削除]チェック ボックス

ディスク データを削除するかどうかを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

ネットワーク インターフェースの削除: VMware vCenter

ネットワーク インターフェースの削除アクション タイプでは、仮想マシンから仮想 NIC を削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

Virtual Center

VMware vCenter が存在するサーバの名前を指定します。ドロップダウン リストから 1 つ選択します。

データセンター

仮想マシンが存在する VMware vCenter 内のデータ センターの名前を指定します。 ドロップダウン リストから 1 つ選択します。

仮想マシン

仮想 NIC を削除する仮想マシンの名前を指定します。 ドロップダウン リストから 1 つ選択します。

ネットワーク インターフェース

削除する仮想 NIC を指定します。ドロップダウン リストから 1 つ選択します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

サーバをサービスから削除

サーバをサービスから削除アクション タイプでは、既存のサービスからサーバを削除できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

サービス

サービスの名前を指定します。

サーバ リスト(カンマで区切られたリスト)

サービスから削除するサーバのリストを指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

アクションの実行

アクションの実行アクション タイプでは、アクションを実行できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

アクション名

アクションを指定します。

イベント ソース

アクションのソースを指定します。

イベント メッセージ

イベント メッセージを指定します。

ルール名

アクションのルールを指定します。

サーバ名

アクションのサーバを指定します。

サービス名

アクションのサービスを指定します。

プロパゲート

-service_name オプションで指定されたサービス内のすべてのサーバに対して、アクションを実行するように指定します。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

アクション シーケンスの実行

アクション シーケンスの実行アクション タイプでは、1 つのルールに複数のアクションを選択し、定義したシーケンスでそれらのアクションを実行できます。

アクション定義の[詳細]セクションには、以下のフィールドがあります。

中断の場合再起動

アクション シーケンスが中断された場合、そのアクション シーケンスを再起動します。アクションは中断されたポイントからは再開されません。シーケンスが先頭に戻って開始されます。

アクション シーケンス

アクションと条件を 1 行、または複数行選択できます。 [アクション シーケンス]を選択すると、ドロップダウン リストが有効になります。ドロップダウン リストを選択しない場合、テキストがテーブル セルに表示されます。

シーケンス

アクションのシーケンスを指定します。

注: 条件が満たされずにアクション シーケンスが終了した場合、デフォルトではリターン コード -1 が返されます。

アクション

アクション名を指定します。ドロップダウン リスト内の利用可能なアクションからアクションを選択できます。

条件名

次に実行されるアクションを決定する条件を指定します。独自のカスタム条件を作成するか、または以下のいずれかの事前定義済み条件を使用できます。

- 失敗時
- 成功時

注: 条件は作成された順序で評価されます。

次の手順

条件の結果に基づいて実行する次のアクションを指定します。

続行

条件が true と評価された場合に、続行して次のアクションへ進みます。

終了（RC=0）

条件が true と評価された場合に、シーケンスを終了し、ログにコード 0 を返します。

RC を返して終了（RC= アクション RC）

条件が true と評価された場合に、アクション シーケンスを終了し、アクションのリターン コードを返します。

アボート（RC=-1）

条件が true と評価された場合に、アクション シーケンスを停止し、ログにコード -1 を返します。

移動

条件が true と評価された場合に、指定されたアクション シーケンス番号に進みます。

アクションの追加

テーブルに新しいアクションを追加し、新しいシーケンス番号を自動的に生成します。

条件の追加

アクションに新しい条件を追加します。

削除

選択された行を削除し、シーケンス番号を更新します。 行には、アクションまたは条件を含めることができます。 この機能により、アクション全体を削除せずに、アクションの条件を削除できます。

保存

アクション シーケンスを保存します。

注: シーケンスの最後のアクションで［次の手順］が［*続行*］に設定されている場合、設定は［Exit w/RC］（RC= アクション RC）に自動的に変更されます。また、シーケンスの最後のアクションの［次の手順］が変更されたことが、情報メッセージによって通知されます。

コマンド スクリプトの実行

コマンド スクリプトの実行アクション タイプでは、スクリプトを使用して、コマンドを処理したサーバから外部コマンドを実行できます。 たとえば、［開始］ページからコマンドが実行される場合、コマンドを実行する Windows スケジューラと同じサーバ上にターゲット コマンドが存在する必要があります。 ルール評価の結果としてコマンドが実行される場合、ジョブの実行後、アクションが Windows スケジューラ サーバをホストしているコンピュータ上で実行されます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

コマンド ライン

実行するコマンドまたは代替文字列を指定します。 あるいは、自動生成されるテキストや、イベント メッセージから抽出されるテキストを使用できます。

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

ヘルス状態の設定

ルール ヘルス状態の設定アクション タイプは、ルールのヘルス状態を［警告］、［マイナー］、［メジャー］、［重大］のいずれかに設定できます。

アクション定義の［詳細］セクションには、以下のフィールドがあります。

ヘルス状態

以下のいずれかのアクションを指定します。

- 警告
- マイナー
- メジャー
- 重大

承認が必要

チケットがサードパーティによる承認が必要であると指定する場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

承認または拒否時にチケットを自動的にクローズ

チケットが承認または拒否された後でそれを閉じる場合に選択します。

注: このオプションを使用するには、CA SDM を設定する必要があります。

チケット タイプ

ドロップダウン リストから有効なチケット タイプを選択します。 設定に応じて、有効なタイプには次のものが含まれます。

- デフォルト
- インシデント
- 問題
- 要求

注: このオプションを使用するには、CA SDM を設定する必要があります。

テンプレート

チケットを作成するために使用するテンプレートを指定します。 ドロップダウン リストからテンプレートを選択します。 選択されたチケット タイプに応じて、フォームは対応する値で入力されます。

注: このオプションを使用するには、CA SDM を設定する必要があります。

カスタム アクションの作成

代替パラメータを定義することによりカスタマイズされたアクション タイプを作成できます。 カスタム アクション タイプは、事前定義済みアクション タイプと共に［アクション タイプ］ドロップダウン リストに追加されます。

次の手順に従ってください:

1. ［エクスプローラ］ペインで［データ センター］ノードを選択します。
2. ［リソース］-［ポリシー］をクリックし、次に、［カスタム アクション タイプ］タブをクリックします。

   ［カスタム アクション タイプ］ページが表示されます。
3. ＋（追加する）をクリックします。

   ［カスタム アクション タイプ： 新規追加］セクションが表示されます。

4. 以下のフィールドに入力して新しいアクション タイプと代替パラメータを定義し、次に、［保存］をクリックします。

アクション タイプ名

新しいアクション タイプの名前を定義します。

コマンド

アクション タイプのコマンド ライン構造を定義します。コマンドの一部として置換する場合に、%SERVER%、$MYKEY$ などの代替パラメータを定義できます。代替キーは、1 つのコマンドあたり 1 回のみ使用できます。 たとえば、%SERVER% 代替キーは、コマンド内で 1 回のみ使用できます。

代替キー

代替キーに一意の文字列を定義します。 代替キー名はコマンドに定義されている名前と一致する必要があります。 複数の代用キーを定義する場合は、それぞれの代替キーを個別に定義する必要があります。

プロンプト

アクションを作成するときに入力する代替パラメータに関連付けられた引数名を定義します。

デフォルト値

デフォルト代替キー値を定義します。

新しいパラメータが代替パラメータ リストに表示されます。

5. ［アクション］ドロップダウン リストから［保存］を選択します。

カスタム アクション タイプが保存されます。

アクション シーケンスの定義

ルールには、アクション シーケンスを定義できます。ルールの条件が true に評価された場合、定義したアクション シーケンスが実行されます。 また、カスタム条件を作成し、シーケンスにそれらを構築することもできます。

注: アクション シーケンスは、ジョブとしてスケジュールしたり、dpmpolicy runaction CLI コマンドを使用して実行することもできます。

次の手順に従ってください:

1. ［エクスプローラ］ペインで［データ センター］ノードを選択します。
2. ［リソース］ - ［ポリシー］をクリックし、次に、［アクション］タブをクリックします。

   ［アクション］ページが表示されます。
3. ［+］（新しいアクションの追加）をクリックします。

   ［アクションの定義: 新規］セクションが表示されます。
4. アクション シーケンスに分かりやすい名前を入力し、［タイプ］ドロップダウン メニューから［アクション シーケンスの実行］を選択します。

   ［条件ロジック］セクションが表示されます。
5. 異常終了後にシーケンスを再起動するには、［中断の場合再起動］チェック ボックスをオンのままの状態にします。 シーケンスは、実行された前回のアクションを再起動して続行します。 異常終了の後にシーケンスを続行しない場合は、このチェック ボックスをオフにします。
6. アクション シーケンスにアクションを追加するには、［アクション シーケンス］ペインで［+］（アクションの追加）をクリックします。［アクションの追加］は、アクション シーケンスの最後に新しいアクションを追加します。 シーケンスの途中にアクションを挿入する場合は、挿入位置の後のアクションをすべて削除します。 新しいアクションを挿入した後、削除したアクションを再定義します。
7. アクション シーケンスの条件ロジックを構築する条件を選択します。新しい条件ロジックは、条件ロジック シーケンスの最後にのみ追加できます。 シーケンスの途中に新しい条件ロジックを挿入する場合は、挿入位置の後の条件ロジックをすべて削除します。 新しい条件ロジックを挿入した後、削除した条件ロジックを再定義します。

8. 追加の条件ロジック シーケンスにそれぞれ条件ロジック評価のタイプを選択します。 出力タイプには、以下のものがあります。

   ReturnCode

   アクション リターン コードを評価します。

   注: リターン コードの評価用の有効な比較演算子は、==、!=、>、<、>=、<= です。

   STDOUT

   特定の文字列の標準出力を検索します。

   STDERR

   特定の文字列の標準エラーを検索します。

   注: STDOUT と STDERR の有効な比較演算子は「指定の語句を含む」および「次を含まない」です。

   注: ［論理演算子］フィールド（AND/OR）を使用して条件をリンクできます。 ［論理演算子］は、最終条件では NOOP に自動的に設定されます。

   新しい条件ロジックはシーケンスに追加されます。

9. 条件の入力が完了したら、［条件の保存］をクリックします。

   条件が保存されます。

10. ［アクション シーケンス］ペインで［保存］をクリックします。

    アクションが保存されます。

    テストのために[アクション]ページからアクションを実行するには、アクションを選択して［アクションの実行］アイコンをクリックします。

スケジュールの定義

事前定義された時刻にアクションが実行されるようにスケジュールできます。 たとえば、デフォルトの Windows スケジューラを使用して毎日実行される必要があるアクションをスケジュールしたり、保守タスクのように定期的に実行されるアクションをスケジュールできます。

次の手順に従ってください:

1. ［エクスプローラ］ペインで［データ センター］ノードを選択します。

2. ［リソース］-［ポリシー］をクリックし、次に、［スケジュール済みアクション］タブをクリックします。

   ［スケジュール済みアクション］ページが表示されます。

3. 以下のフィールドを指定します。

   名前

   スケジュール済みアクションの名前を定義します。

   事前通知

   スケジュールされたアクションが実行される前にイベントを生成するかどうかを指定します。 イベントがダッシュボードに表示されます。

   事後通知

   スケジュールされたアクションが実行された後でイベントを生成するかどうかを指定します。 イベントがダッシュボードに表示されます。

   頻度

   スケジュール済みアクションが実行される頻度を指定します： 一度のみ、日単位、週単位、月単位（日）または月単位（曜日）。

   日付

   スケジュール済みアクションを開始する日付を定義します。

   時間

   スケジュール済みアクションを実行する時間を定義します。

   注: ジョブのスケジュールには使用されないため、秒を入力する必要はありません。

   タイプ

   スケジュールしているアクションに使用されたアクション タイプを指定します。

   注: スケジューラでは、代替パラメータを含むアクションがサポートされていません（唯一の例外は %AutoIncrement(0)% と %AutoDecrement(0)% です）。 代替パラメータが含まれるアクションは、ポリシー ルール評価を介してのみ実行できます。

アクション

各アクション タイプにすでに作成されたアクションをリスト表示します。

注: リストには、ヘルプ デスクの承認要件を指定するアクションは含まれていません。

4. ドロップダウン リストから［保存］を選択します。

アクションがスケジュールされることを確認するメッセージが表示されます。 スケジュールされたアクションが、［スケジュール済みアクション］リストのスケジュール済みのジョブのリストに表示されます。

注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。 スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

自動化ポリシーの作成

［自動化ポリシーの作成］ウィザードを使用して、2 つの事前定義済みポリシー タイプに基づいた自動化ルールを作成することができます。

- 仮想マシン動的リソース ブローカ - CPU とメモリの割り当てが、定義済みの使用率しきい値に基づいて動的に変更されます。
- 全体使用率メトリックのしきい値モニタリング - ヘルス状態は全体的な使用率に従って設定されます。

次の手順に従ってください:

1. ［管理］ペインを開き、［自動化ポリシーの作成］をクリックします。

［自動化ポリシーの作成］ウィザードが表示されます。

2. ［ポリシー タイプ］を選択し、［次へ］をクリックして、ターゲット リソースを選択し、ルールの条件を設定します。

［ポリシー サマリ］に結果が表示されます。

3. ［終了］をクリックします。

ポリシーが確認され、対応するルールが作成されます。

ポリシーのユース ケース

以下のシナリオでは、ポリシーを実装するためのいくつかのユース ケースについて説明します。

関連項目:

ユース ケース： サーバをサービスに追加する (P. 948)
ユース ケース： 新規ルールをサービスに追加する (P. 949)
ユース ケース： アクションを定義する (P. 949)

ユース ケース: サーバをサービスに追加する

このユース ケースでは、サーバを事前に作成されたサービスに追加するプロセスについて示します。

1. サーバをサービスに追加するための前提条件を確認します。
   - サービスが存在している。
   - サーバが存在している。
   - サービスにはすでに優先度が割り当て済みである。
   - ユーザにはサービスを変更するアクセス権がある。
2. サーバをサービスに追加します。
3. サーバをサービスに追加した結果を確認します。
   - このサーバは現在サービスのメンバである。
   - このサーバは現在サービスの使用率に含まれている。
   - このサービスを含めたことで、使用率に対するすべてのサービス ルールに影響する。

ユース ケース: 新規ルールをサービスに追加する

このユース ケースでは、新規ルールをサービスに追加するプロセスを説明します。

1. ルールをサービスに追加するための前提条件を確認します。
   - サービスが存在している。
   - ユーザにルールを作成するアクセス権がある。
   - サーバがサービス内にある。
2. このサービスに対するルールの定義を作成します。
3. ルールをサービスに追加した結果を確認します。
   - 新規ルールが作成されている。
   - 新規ルールがルールの条件に有効なすべてのサービスについて評価している。

ユース ケース: アクションを定義する

このユース ケースでは、スケジューリング ジョブまたはポリシー ルールで使用するアクションを定義するプロセスについて示します。

1. アクションを定義するための前提条件を確認します。
   - ユーザにアクションを定義するアクセス権がある。
   - 目的のアクション定義に必要なリソースが検出されている。
2. CA Server Automation ユーザ インターフェースでアクションの属性およびアクションの名前を定義します。
3. サーバをサービスに追加した結果を確認します。
   - アクションはユーザによって提供された説明で作成されている。
   - アクションは現在ルールで利用できる。
   - アクションは現在ジョブスケジューリングで利用できる。

   注: ヘルプ デスク承認要件を指定するアクションは、アクションのスケジュールには使用できません。 スケジュール済みアクションに同じアクションを必要とする場合は、ヘルプ デスク承認要件が含まれない、2 つ目のアクションを作成します。

データ収集の設定

データ センターでの以下のようなデータ収集の方法を制御できます。

- メトリック収集の時間間隔
- メトリックを収集するシステム（フィルタリング）
- 各サーバで収集するメトリック
- データの経過期間とデータの有効期限（データを保持する期間）

関連項目:

メトリック収集に関する重要な点 (P. 950)
データ センター用のデータ収集の設定 (P. 953)
サーバ用のデータ収集の設定 (P. 955)
仮想リソース用のデータ収集の設定 (P. 957)
パフォーマンスしきい値の設定 (P. 961)
メトリック フィルタの設定 (P. 962)

メトリック収集に関する重要な点

メトリックを選択する場合に、十分な情報を得たうえでの決定を行うために、以下の点について確認し、CA Server Automation のパフォーマンスおよびアプリケーション メトリック収集について理解します。

- CA Server Automation はどのようにしてメトリック データを収集するのですか。 CA Server Automation は、リモート コンピュータ上で CA Systems Performance LiteAgent または SystemEDGE エージェントと通信して、指定されたシステム メトリックを収集します。

  基本システム メトリックを収集する任意のサーバに CA Systems Performance LiteAgent または SystemEDGE エージェントをインストールします。 SystemEDGE エージェントが存在する場合、CA Systems Performance LiteAgent は必要ありません。 必要な場合は、製品のユーザ インターフェースを使用して SystemEDGE エージェントをインストールできます。すべてのパフォーマンス メトリックはパフォーマンス DB 内に格納されます。

- どのようにして全体使用率が計算されますか。 全体使用率とは、CA Server Automation によって管理されたサーバに関して現在収集されているすべてのメトリックの集計です。 この計算は、メトリックの値および通常操作のパラメータを定義するユーザ定義のしきい値に基づいています。

  注: 全体使用率の計算に新しいメトリックを含めるには、ユーザ インターフェースの［ポリシー］、［メトリック］、［しきい値］セクションで［全体使用率計算に含める］を選択します。 このメトリックを含めると、CA Server Automation は、サーバの状態を評価するときに最新の結果を表示します。

- メトリック評価によって全体使用率にどのような影響がありますか。 テーブルに示されたメトリックの詳細は、CA Server Automation が異なるメトリックを評価する方法を理解するのに役立ちます。 各メトリックのメソッドのプロパティには*厳密*または*補足*のいずれかが設定されています。 厳密値が高いと、全体的な使用率の増加を示すため、低い厳密値よりも悪いシナリオになります。 補足値が高いと、全体的な使用率の減少を示すため、肯定的なシナリオになります。 一般的に、厳密値が高いと全体的な使用率にマイナスに影響し、厳密値が低いと全体的な使用率にプラスに影響します。 対照的に、補足値が高いと全体的な使用率にプラスに影響し、補足値が低いと全体的な使用率にマイナスに影響します。 たとえば、［メモリ：コミットされた使用中のバイト数の割合］の値が増加すると、システムの全体的な使用率は増加します。 ［メモリ：利用可能（MB）］の値が増加すると、全体的な使用率は減少します。

デフォルト メトリックとは何ですか。 デフォルト メトリック定義は、すべてのサポートされているプラットフォームの［フィルタ］セクションのメトリック リストにあります。デフォルト メトリック インジケータはメトリック リストにあり、［デフォルト］列で［はい］の値を使用して検索できます。 サーバが追加されると、CA Server Automation はこのリストを使用してメトリックの定義を取得します。プラットフォーム、タイプ、サブタイプ、インスタンスおよび［フィルタ］セクションで収集するデータのタイプを設定できます。 各サーバのメトリック フィルタおよび定義はパフォーマンス DB に格納されます。

- 現在システムでパフォーマンス データを利用できますか。デフォルトでは、データを収集できなくても、CA Server Automation がサーバの状態に悪影響を与えることはありません。 データの欠如は、サーバの重大度に反映されません。イベント リストを確認するか、または特定のシステムを選択することによって、メトリック データが収集されているかどうかを判定できます。ただし、収集されたデータが使用可能かどうかをより迅速に判定するための手段が必要な場合や、パフォーマンス データが重大である場合があります。 この場合は、パフォーマンス データを収集できない場合にシステムの状態を自動的に［警告］または［重大］に変更するように CA Server Automation を設定します。パフォーマンス データが使用できないシステムを容易に識別できるようにするには、CA Server Automation *install_path*¥conf ディレクトリにある caaipconf.cfg ファイルを変更します。このファイルをテキスト エディタで開き、以下のようにヘルス状態のプロパティの場所を見つけます。

```
<プロパティ名="CONFIG_KEY_DEFAULT_HEALTH_STATE">
            <!-- 有効な値： 0 （不明）、5 （OK）、10 （警告）、15 （マイナーな障害）、20 （メジャーな障害）、25 （重大な障害） -->
            <!-- CA_ComputerSystem に関連付けられた CA_CollectionState オブジェクトの HealthState の値を変更します -->
            <!-- 30 に設定された場合、CE は HealthState を設定しません。 -->
            <value>5</value>
            <displayName>メトリックまたはデータ収集で問題が発生した場合はデフォルトのノードのヘルス状態</displayName>
        </property
```

CA Server Automation は、XML 要素の値で囲まれた値を 5 または 10（それぞれ、［OK］または［警告］を示します）などのサポートされているほかの値のいずれかに変更します。 これらの変更には、パフォーマンス データを収集できない場合の目的の状態が反映されます。 例：

```
<プロパティ名="CONFIG_KEY_DEFAULT_HEALTH_STATE">
            <!-- 有効な値： 0 （不明）、5 （OK）、10 （警告）、15 （マイナーな障害）、20 （メジャーな障害）、25 （重大な障害） -->
```

```
            <!-- CA_ComputerSystem に関連付けられた CA_CollectionState オブジェクトの
HealthState の値を変更します -->
            <!-- 30 に設定された場合、CE は HealthState を設定しません。 -->
            <value>10</value>
            <displayName>メトリックまたはデータ収集で問題が発生した場合はデフォルトのノード
のヘルス状態</displayName>
        </property
```

<value> が「10」に変更されたため、パフォーマンス データが利用可能でないシステムは、CA Server Automation ユーザ インターフェースに警告の状態で表示されます。

注: パフォーマンス メトリックおよび説明のリストについては、「Performance Metrics Reference」を参照してください。

データ センター用のデータ収集の設定

データ センター レベルでデータ収集を設定できます。データ センター レベル ポリシーはすぐに有効になります。

次の手順に従ってください:

1. ［リソース］をクリックして、［エクスプローラ］ペインで［データ センター］フォルダを選択します。
2. 右クリックし、［ポリシー］-［収集の設定］を選択します。

   ［設定］ダイアログ ボックスが表示されます。

3. ［収集設定］セクションで以下のフィールドに入力します。

［データ記録間隔 (秒)］

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト： 300 秒

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

［ポーリングされたデータの保持 (日数)］

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。 この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。 保存されたポーリング済みデータ オブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。 パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト： 10 日

日単位ロールアップ データの保持（日数）

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

最大： 365

デフォルト： 365

4. ［しきい値］セクションにしきい値の制限を入力し、［保存］をクリックします。

これで、設定が保存されました。

サーバ用のデータ収集の設定

個々のサーバにデータ収集を設定できます。 このプロシージャを使用してデータ センターのデータを収集する特定のサーバを設定します。また、モニタするメトリックを選択し、個々のメトリックにしきい値を設定し、全体的な使用率にメトリックを含めることができます。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［データ センター］フォルダを開き、サーバが属するサービスを選択します。
3. 右クリックし、［ポリシー］を選択します。

   ［ポリシー］サブメニューが表示されます。

4. ［メトリック］をクリックします。

   メトリック ウィザードが表示されます。

5. データ収集を設定するサーバを選択します。
6. ［間隔の設定］ダイアログ ボックスで以下のフィールドに入力します。

   デフォルトを使用

   オンにした場合はデフォルトとしてデータ センター レベルを指定します。 チェック ボックスをオフのままにする場合は、指定した値が代わりに使用されます。

［データ記録間隔 (秒)］

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト： 300 秒

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

日単位ロールアップ データの保持（日数）

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

最大： 365

デフォルト： 365

［ポーリングされたデータの保持 (日数)］

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。 この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。 保存されたポーリング済みデータ オブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。 パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト： 10 日

7. ［利用可能なメトリック］セクションからモニタするメトリックを選択し、下向き矢印をクリックします。

   選択されたメトリックは、［収集対象として選択されたメトリック］セクションに移動します。

   注: デフォルト メトリック（CPU とメモリ）を無効にし、他のメトリックを有効にする場合、新しく選択したメトリックのしきい値を変更するまで、全体的な使用率は表示されません。

8. 各サーバでモニタするパフォーマンス メトリックを設定し、各メトリックのしきい値境界を設定できます。 しきい値を設定するメトリックを選択し、以下のフィールドに入力します。

   上限しきい値

   選択したメトリック グループの使用率の上限を定義します。

   デフォルト： 80%

   下限しきい値

選択したメトリック グループの使用率の下限を定義します。

デフォルト： 20%

全体使用率計算に含める

選択したメトリックを全体使用率の計算用に含めて CA Server Automation によって評価されるように指定します。

9. ［終了］をクリックして設定を保存します。

仮想リソース用のデータ収集の設定

仮想プラットフォームおよびこれらのプラットフォームで作成されて管理された仮想リソース用のデータ収集を設定できます。 特定の仮想マシンまたは他のリソースを設定し、データ センターのデフォルトとは異なる間隔でデータを収集する場合は、このプロシージャを使用します。 また、モニタするメトリックを選択し、個々のメトリックにしきい値を設定し、全体的な使用率にメトリックを含めることもできます。

以下の仮想プラットフォーム オブジェクト用のデータ収集を設定できます。

- vCenter Server
- vCenter データ センター
- vCenter ESX Server
- vCenter 仮想マシン
- Hyper-V
- Microsoft クラスタ

- Microsoft クラスタ ノード
- IBM PowerVM Server
- IBM 論理パーティション
- Solaris ゾーン サーバ
- Solaris ゾーン

仮想リソース用のデータ収集の設定

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. ［データ センター］または［Microsoft Cluster Service］フォルダを展開し、次に任意のサブフォルダを展開し、設定するオブジェクトを選択します。

   そのオブジェクトのサブタブが右側のペインに表示されます。

   注: トップ レベル フォルダ（VMware vCenter Server など）を選択した場合、またはデータが収集されないオブジェクト（vCenter クラスタなど）を選択した場合は、そのフォルダまたはオブジェクトに含まれている特定のオブジェクトを選択してデータ収集を設定する必要があります。

   注: トップ レベル フォルダとして MS Cluster Service を選択すると、クラスタとそれらのノードが表示されます。

3. 右クリックし、［ポリシー］-［サーバ メトリック収集の設定］を選択します。

   注: トップ レベル フォルダとして Solaris ゾーンを選択すると、［システム］セクションの［ハードウェア クラス］列には値［その他］が常に表示されます。

4. ［利用可能なメトリック］セクションからモニタするメトリックを選択し、次に、下方向キーをクリックします。

   選択したメトリックは、［収集対象として選択されたメトリック］セクションに移動します。

   注: デフォルト メトリック（CPU とメモリ）を無効にし、他のメトリックを有効にする場合、新しく選択したメトリックのしきい値を変更するまで、全体的な使用率は表示されません。

5. ［保存］をクリックして選択したメトリックを適用します。
6. リソースを右クリックし、［ポリシー］-［収集の設定］を選択します。
7. ［収集設定］セクションで以下のフィールドに入力します。

   デフォルトを使用

   オンにした場合はデフォルトとしてデータ センター レベルを指定します。 チェック ボックスをオフのままにする場合は、指定した値が代わりに使用されます。

[データ記録間隔 (秒)]

パフォーマンス DB にデータが収集されて保存される頻度を定義します。

デフォルト： 300 秒

注: モニタ対象環境の 1000 台のマシンごとに、データ記録間隔を 300 秒増加させることを推奨します。

日単位ロールアップ データの保持（日数）

パフォーマンス DB に日単位データの平均を保存する期間を定義します。

最大： 365

デフォルト： 365

[ポーリングされたデータの保持 (日数)]

パフォーマンス DB にポーリングされたデータを保存する期間を定義します。 この数を定義する場合は、収集された管理対象システム、サービスおよびメトリックの数を考慮します。 保存されたポーリング済みデータ オブジェクトが徐々に蓄積されて、パフォーマンスに影響を与える場合があります。 パフォーマンスの問題が発生する場合は、保存日数の数を減らします。

デフォルト： 10 日

8. ［保存］をクリックして、設定を保存します。

注: デフォルトのしきい値が使用されます。 しきい値を変更する場合は、これらを別々に実行する必要があります。

パフォーマンスしきい値の設定

各サーバでモニタするパフォーマンス メトリックを設定し、各メトリックのしきい値境界を設定できます。

次の手順に従ってください:

1. ［エクスプローラ］ペインを開きます。

   利用可能なグループ、サービス、およびシステムが表示されます。

2. ［データ センター］フォルダおよび任意のサブフォルダを展開し、設定するサーバを選択します。仮想サーバに移動して仮想マシンまたは論理パーティションなどの特定の仮想リソースを選択します。

3. 右クリックし、［ポリシー］を選択します。

   ［ポリシー］サブメニューが表示されます。

4. ［しきい値の設定］をクリックします。

   ［しきい値の設定］が表示されます。

5. しきい値を設定するメトリックを選択し、以下のフィールドに入力します。

   上限しきい値 (%)

   選択したメトリック グループの使用率の上限を定義します。

   デフォルト： 80%

   下限しきい値 (%)

   選択したメトリック グループの使用率の下限を定義します。

   デフォルト： 20%

   ［全体使用率の計算用に含める］

   選択したメトリックを全体使用率の計算用に含めて CA Server Automation によって評価されるように指定します。

6. ［変更］をクリックして設定を保存します。

メトリック フィルタの設定

モニタするパフォーマンス メトリックに応じてメトリックをデータ センターのメトリック フィルタに追加したり、メトリック フィルタから削除したりすることができます。

メトリック フィルタを設定する方法

1. ［エクスプローラ］ペインで［データ センター］フォルダを選択します。
2. 右クリックし、［ポリシー］-［収集条件の設定］を選択します。

   ［収集条件］ダイアログ ボックスが表示されます。
3. 以下の*いずれか*を実行します。
   - 既存のメトリックのチェック ボックスをオンにして既存のエントリを変更します。 選択されたメトリックの情報は、［詳細］セクションのフィールドに入力されます。 任意の変更を加えて、［更新］をクリックします。
   - OS を選択し、［詳細］セクションのフィールドに入力して新しいメトリックを追加して、［追加］をクリックします。

   メトリックが保存されます。

   ［詳細］セクションには以下のフィールドがあります。

   OS

   モニタされているメトリックのオペレーティング システムを定義します。

   タイプ

   モニタされているメトリックのタイプを定義します。

   例：

   ［タイプ］ : CA ディスク グループ

   ［サブタイプ］ : 毎秒（平均）書き込みます

   サブタイプ

   メトリックのどの側面がモニタされているか定義します。

   例：

   ［タイプ］ : CA ディスク グループ

   ［サブタイプ］ : 毎秒（平均）読み取ります

インスタンス

MIB 階層の管理対象オブジェクトのインスタンスを定義します。

例：

タイプ： vmvcaim.StatClusterEffectiveCPU

サブタイプ： 1.3.6.1.4.1.546.16.52.2.7.2.1.14

インスタンス： %3 [%2]

%<n> の <n> は、[インスタンス]の下にリスト表示される数値で、それぞれの AIM MIB テーブル内の n 番目の列に対応する任意の値に一致します。 たとえば、すべての行エントリ（同じ管理対象オブジェクトのインスタンス）には vmvcAimStatClusterTable。これは、メトリックがユーザ入力なしで利用可能な場合、すべてのインスタンスの管理対象オブジェクトのメトリックを瞬時に収集するのに役立ちます。

上限しきい値 (%)

選択したメトリック グループの使用率の上限を定義します。

デフォルト： 80%

下限しきい値 (%)

選択したメトリック グループの使用率の下限を定義します。

デフォルト： 20%

遅延

しきい値イベントが生成されるまでに発生したしきい値違反の連続回数を定義します。 このオプションを設定し、しきい値を評価するためのイベントがいっぱいになるのを防ぎます。 アクションを定義して、しきい値違反イベントをログ記録し、しきい値モニタリングのルールをセットアップすることができます。

方法

収集方法が補足的であるか、補足的なデルタであるか、厳密であるか、または厳密なデルタであるかを指定します。補足的なメソッドには、セットのサブセット内にまだ含まれていないメトリックが含まれます。 厳密なメソッドは、指定された厳密なメトリックを収集します。

カテゴリ

モニタされたメトリックがシステム、アプリケーションまたは SNMP メトリックかどうか指定します。

選択されたメトリックをデフォルトで収集

CA Server Automation がフィルタによってデフォルトで指定されたメトリックを収集するかどうかを指定します。 メトリック フィルタがデフォルトとして設定されていない場合、CA Server Automation は指定されたメトリックを自動的に収集しません。

［全体使用率の計算用に含める］

選択したメトリックを全体使用率の計算用に含めて CA Server Automation によって評価されるように指定します。

［収集用にアクティブ化］

収集に利用可能なメトリックを評価する場合にメトリック フィルタの使用が有効であると指定します。

4. 削除する任意のメトリックのチェック ボックスをオンにし、次に、［削除］をクリックします。

選択したエントリが削除されます。

第 12 章: リソースのプロビジョニング

このセクションには、以下のトピックが含まれています。

イメージング サービス

CA Server Automation では、新しい物理および仮想コンピュータにプロビジョニングを行うことができ、既存のリソースを再イメージングすることもできます。物理コンピュータ イメージングは、Windows および Linux オペレーティング システムを使用するサーバで利用できます。 プロビジョニング機能を使用すると、VM のプロパティのクローン作成、マイグレーション、設定、および変更を実行できます。

イメージング サービスは、以下の技術を統合および使用して、プロビジョニング操作を実行します。

- VM のプロビジョニングのための VMware vCenter Server 統合。
- 設定なしですぐに使用できる Hyper-V サーバ上のローカル テンプレートに基づいた、VM のプロビジョニングのための Hyper-V 統合。
  - 既存の SCVMM イメージ ライブラリを再利用するための Microsoft System Center Virtual Machine Manager （SCVMM） との統合。
- ゾーンのプロビジョニングのための Solaris ゾーンの統合。
- VM のプロビジョニングのための Citrix XenServer の統合。
- VM のプロビジョニングのための VMware vCloud Director の統合。
- KVM プロビジョニングのための Red Hat Enterprise Virtualization の統合。

- NIM による IBM AIX プロビジョニング
- クラウドでのイメージ プロビジョニングのための Amazon Elastic Cloud（EC2）
- Windows および Linux サーバのイメージングのための CA Software Delivery OSIM
- Solaris サーバ イメージングのための JumpStart サーバ
- 異なるハードウェアのイメージングのための Rapid Server Imaging（RSI）

以下のイメージング サービス アクションのためにイベントが生成されます。

- イメージング サーバへのイメージング ジョブのサブミット
- イメージング ジョブ ステータスへの変更
- イメージング ジョブ完了後のターゲット コンピュータの検出

サービス プロビジョニング

このセクションには、以下のトピックが含まれます。

サービスをプロビジョニングする方法

*サービス管理者*は、CA Server Automation を使用して、物理および仮想サーバ環境内のサービスを管理およびプロビジョニングします。 *サービス消費者*が必要なアプリケーションを必要なホスト マシン上で実行できるよう、簡単にプロビジョニングする方法を提供する必要があります。

サービス管理者にとって、サービス プロビジョニングは、アプリケーションとサービス テンプレートの定義で構成されます。 サービス テンプレートは、定義された順序で展開されたアプリケーションのセット（アプリケーション アクションのセットを含む）と、サービスを展開する方法および場所を決定するマシン テンプレートで構成されます。

サービス テンプレートは、サービス消費者にワンクリック サービス プロビジョニングを提供します。消費者は、プロビジョニング用のサービス テンプレートを選択し、テンプレートを実行中のサービスとして展開するために必要なすべての追加情報を入力します。

CA Server Automation は、サービスのインスタンスを、サービス テンプレートの要件に一致するプロビジョニングされたリソースに展開します。

たとえば、2 層の Web アプリケーションおよびデータベース サービスの場合は、以下のようになります。

サービス管理者

1. Web アプリケーションとデータベース アプリケーションを定義し、それらをインストールして実行するために必要な実行アクションとリソースを指定します。
2. Web およびデータベース アプリケーションを使用してサービス テンプレートを作成し、それらをホストするために必要なリソースを設定します。

サービス消費者

1. サービス テンプレートのインスタンスをプロビジョニングします。

   CA Server Automation は、アプリケーションを利用可能なサーバ リソースに展開し、サービス消費者に Web サービスを指定された場所で使用する準備ができたことを通知します。

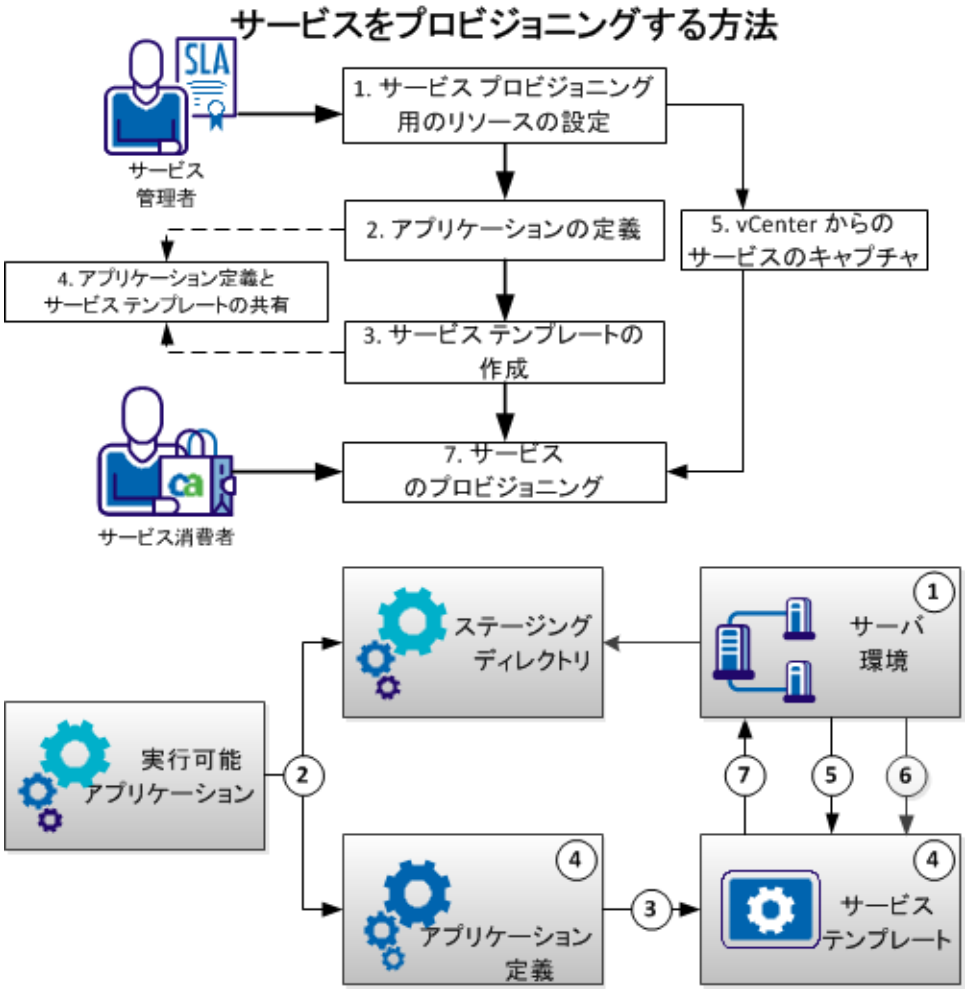
CA Server Automation には、一連のすぐに使用可能なアプリケーション定義やサービス テンプレートが用意されています。これには、以下のサービスが含まれます。

- Windows 用の Apache HTTP サーバ

CA Server Automation は、以下の環境へのサービス プロビジョニングをサポートします。

- VMware vCenter Server
- Amazon EC2 インスタンス

以下のプロセスは、サービス管理者がアプリケーションを組み合わせて、サービス消費者によるワンクリック サービス プロビジョニングを可能にするサービス テンプレートを作成する方法の概要を示しています。



1. サービス プロビジョニング用のリソースの設定（P. 970）

   プロビジョニングされたサービスをホストするために利用可能な環境とサーバ リソースを指定します。

   - （オプション）サービス プロビジョニング用のマシン テンプレートの設定 (P. 971)

     サービス テンプレートで使用するデフォルトのマシン設定を指定します。

   - （オプション）vCenter 用の動的仕様の設定 (P. 972)

     サービス テンプレート内の仮想マシンに適用するカスタム ライセンスとドメイン設定を指定および作成します。

2. アプリケーションの定義（P. 973）

   アプリケーション、前提条件と制限事項、およびアプリケーションに対するリソースとオペレーティング システムの要件を指定します。

   アプリケーションの実行を指定するには、以下のいずれかのタイプのアクションを定義します。

   - アプリケーション インストールの実行 (P. 976)

     ステージング ディレクトリのアプリケーション ファイルと、それを展開するために必要なすべての実行アクション オプションを指定します。

   - コマンドの実行 (P. 979)

     アプリケーションの正常な展開を可能にするために必要な追加のコマンドがある場合は指定します。

   - ファイルの作成および更新 (P. 981)

     アプリケーションの正常な展開に必要な設定またはプロパティ ファイルを作成または変更します。 たとえば、サイレント インストールの応答ファイルなどです。

   - CA ITCM ソフトウェア パッケージまたはグループの展開 (P. 985)

     CA ITCM ソフトウェア パッケージを、スタンドアロンのアプリケーション定義として、または別のアプリケーションの展開の一部として展開します。

   - CA Process Automation プロセスの実行 (P. 986)

     CA Process Automation で定義されたプロセス ワークフローを、スタンドアロンのアプリケーション定義として、または別のアプリケーションの展開の一部として実行します。

3. サービス テンプレートの作成（P. 988）

   アプリケーションのセットおよびその他のサービス テンプレートとそれらをホストするために必要なマシンを、展開可能なサービス テンプレートとして指定します。

4. （オプション）アプリケーション定義とサービス テンプレートの共有（P. 993）

   アプリケーション定義とサービス テンプレートをファイルにエクスポートした後、それらを CA Server Automation の別のインスタンスにインポートします。

5. vCenter からのサービスのキャプチャ（P. 994）

   VMware vCenter 内で実行されているサービス インスタンスからサービス テンプレートとアプリケーション定義を作成します。

6. サービスのプロビジョニング（P. 995）

   サービスのインスタンスをサーバ環境に展開します。

サービス プロビジョニング用のリソースの設定

CA Server Automation がサービスをプロビジョニングできるようにするには、サービスをホストするために利用可能な環境リソースを指定します。

CA Server Automation は、以下の環境へのサービス プロビジョニングをサポートします。

- VMware vCenter Server
- Amazon EC2 インスタンス

注: CA Server Automation は、サービス プロビジョニングにデフォルトのオンデマンド リソース プールを使用します。これらのリソース プールを設定したり、サービス プロビジョニングにほかのリソース プールを指定したりするには、予約マネージャ の管理機能を使用します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を選択します。
2. ［オンデマンド サービス］ツールバーで、［+］（VMware vCenter Server の追加）をクリックします。

3. 使用する vCenter Server または を選択して［OK］をクリックします。

   ダイアログ ボックスによって、vCenter または とそれに対応する ESX ホスト サーバまたは が、サービス プロビジョニングに利用可能な環境リソースのリストに追加されます。

4. （オプション） ESX ホスト サーバまたは を選択し、［-］（削除）をクリックして、それらをサービス プロビジョニングに使用できないようにします。

5. ［アクション］-［保存］をクリックします。

   CA Server Automation は、サービス プロビジョニングに利用可能なリソースを更新します。

関連項目:

vCenter Server 管理コンポーネントを設定する方法 (P. 603)

サービス プロビジョニング用のマシン テンプレートの設定

CA Server Automation を使用すると、指定したオペレーティング システム用の VM テンプレートを選択できます。 サービス テンプレートはこれらのテンプレートを使用して、サービス プロビジョニング中に必要なマシンのプロビジョニングを自動化できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を選択します。

2. ［オンデマンド サービス］ページで、使用するテンプレートが含まれた vCenter Server のツール アイコンをクリックします。

   ［マシン テンプレート設定］パネルが表示されます。

3. リストからオペレーティング システムを選択し、利用可能な VM テンプレートのリストからテンプレートを選択して、［デフォルトとして設定］をクリックします。 VM テンプレートが必要なオペレーティング システムごとに、この手順を繰り返します。

   CA Server Automation は、選択された VM テンプレートを指定されたオペレーティング システムと関連付けます。

4. （オプション）OS ファミリ用のすべての VM テンプレート設定のリストを表示および管理するには、そのオペレーティング システム グループ フォルダをクリックします。
5. ［OK］をクリックして［マシン テンプレート設定］を終了します。

vCenter 用の動的仕様の設定

VMware vCenter は、カスタム仕様を使用して、仮想マシンに適用するライセンスとドメイン情報の設定を格納します。 CA Server Automation を使用すると、既存のカスタム仕様を指定したり、サービス テンプレートで使用されるマシンに適用するための新しい仕様を作成したりすることができます。

次の手順に従ってください:

1. ［管理］をクリックし、［設定］-［プロビジョニング］メニューで［サービス プロビジョニング］を選択します。
2. ［動的カスタム仕様］ツールバーの［+］（新規）をクリックします。
3. ［名前］と適用される［オペレーティング システム］を指定し、この仕様をデフォルト仕様にするかどうかを指定します。
4. 既存の VMware 仕様を使用するか、または VMware 仕様を作成するには、以下のいずれかのアクションを実行します。
   - ドロップダウン リストから既存の［VMware カスタマイズ仕様］を選択し、［終了］をクリックします。
   - ［次へ］をクリックし、新しい仕様の所有者、ライセンス、ドメイン、その他の詳細を指定して、［終了］をクリックします。

   この仕様は、サービス テンプレート内のマシンに適用するために利用可能な仕様のリストに追加されます。

アプリケーションの定義

サービス プロビジョニングにおける最初の手順では、サービス テンプレートを構成するために利用可能なアプリケーションのセットと、それらを実行するために必要なアクションを定義します。

注: CA Server Automation は、そのインストール フォルダ内のデフォルトのステージング ディレクトリを使用して、サービス プロビジョニング用の実行可能ファイルを格納します。

次の手順に従ってください:

1. 必要なすべてのアプリケーション ファイルをステージング ディレクトリ内の新しいフォルダにコピーします。

   重要: ライセンスの制限により、CA Technologies は、ライセンスされたアプリケーション ファイルの提供が禁止されています。所有しているライセンスされたバージョンを使用してください。

   注: CA ITCM パッケージの展開などの一部のユース ケースでは、アプリケーション ファイルは必要ありません。

2. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

3. アプリケーションの［名前］、［説明］、［バージョン］、および［ベンダー］を指定します。

4. （オプション）アプリケーションを［エクスプローラ］ツリー内のユーザ定義グループに整理できるようにするには、セミコロンで区切られたタグのリストを指定します。

5. アプリケーションの実行可能ファイルを含むステージング ディレクトリ内のフォルダを［ファイルの場所］に指定します。

6. （オプション）このアプリケーションの正常な展開を可能にするために実行する必要のある前提条件のアプリケーションがある場合は指定します。

   注: 前提条件のアプリケーションは、この手順を使用して定義してください。

7. （オプション）アプリケーションに対する制限がある場合は指定します。 たとえば、サーバあたり 1 つのインスタンス、またはサービスあたり 1 つのインスタンスなどです。
8. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。
9. アプリケーションに対するリソース要件、サポートされるオペレーティング システムを指定し、［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。

10. （オプション）プロビジョニング中にアプリケーション サービスを展開するために必要なアクションを定義するには、［+］をクリックします。

［アクションの定義］ウィザードが表示されます。

［アクション］入力を使用し、参考手順を参照して、以下のいずれかのアクションを指定します。

アプリケーション インストールの実行 (P. 976)

ステージング ディレクトリのアプリケーション ファイルと、それを展開するために必要なすべての実行アクション オプションを指定します。

注: 以下のユース ケースでは、アプリケーション ファイルの指定が必要ない場合があります。

- CA ITCM ソフトウェア パッケージを展開する場合。
- アプリケーションは、プリインストールされたアプリケーションがすでに含まれている、キャプチャされた VM テンプレートである。

コマンドの実行 (P. 979)

アプリケーションの正常な展開を可能にするために必要な追加のコマンドがある場合は指定します。

ファイルの作成および更新 (P. 981)

アプリケーションの正常な展開に必要な設定またはプロパティ ファイルを作成または変更します。

CA ITCM ソフトウェア パッケージまたはグループの展開 (P. 985)

CA ITCM ソフトウェア パッケージを、スタンドアロンのアプリケーション定義として、または別のアプリケーションの展開の一部として展開します。

CA Process Automation プロセスの実行 (P. 986)

CA Process Automation で定義されたプロセス ワークフローを、スタンドアロンのアプリケーション定義として、または別のアプリケーションの展開の一部として実行します。

注: プロビジョニング中に実行されるのは、定義されたアクションがあるアプリケーションだけです。 参考手順では、アプリケーション定義中にアクションの設定を省略し、後で定義を変更することを前提にしています。

11. （オプション） CA Server Automation が CA Configuration Automation と統合されている場合は、［次へ］をクリックし、このアプリケーションに関連付けるブループリントをすべて指定します。ブループリントは、現在の展開と比較するためのベンチマークのソフトウェア展開を提供します。

    注: ブループリントの詳細については、CA Configuration Automation のドキュメントを参照してください。

12. ［終了］をクリックします。

    ウィザードは、このアプリケーションを［アプリケーション］ペイン内のリストに追加します。このアプリケーションは、サービス テンプレートの作成で使用できるようになりました。

アプリケーション インストールの実行

サービス プロビジョニング中にアプリケーションを実行するには、実行するアプリケーション ファイルを指定し、アプリケーションの実行方法を定義するためのアクション オプションを指定します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］を選択します。［アプリケーション］ペインで、編集するアプリケーションのツール アイコンをクリックします。
2. ［インストール アクションの設定］タブを選択します。
3. + （追加する）をクリックします。

   ［インストール アクションの選択］パネルに［アクションの定義］ウィザードが表示されます。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、この手順から開始してください。

4. ［アクション］ドロップダウン リストから［プログラムの実行］を選択します。
5. ドロップダウン リストから、実行する［プログラム名］を選択します。アプリケーションに対して指定された［ファイルの場所］によって、使用可能な実行可能ファイルが決定されます。

   注: ［プログラム名］フィールドには、アプリケーション ファイルを実行するために必要なコマンドとオプションを直接入力できます。ただし、このオプションでは、アプリケーション オプションを変更できません。

6. （オプション）アクションを実行するときに使用するユーザ認証情報を指定するには、［ユーザ名］をクリックします。

   注: このオプションにより、サービス プロビジョニング中にユーザによって制限されたアクションが可能になります。主なユース ケースとして、ドメイン ユーザの認証情報を使用してクラスタ化されたアプリケーションの展開を可能にする場合があります。

7. 説明を追加し、指定された実行可能アプリケーションに対してサポートされるオペレーティング システムを必要に応じて変更して、［次へ］をクリックします。

   ［インストール アクション オプションの定義］パネルが表示され、［アクション プレビュー］に、サービス プロビジョニング中にアプリケーションが展開されているときに実行するアプリケーション コマンドが表示されます。

   注: アクションやアプリケーションに対してサポートされるオペレーティング システムを指定すると、OS 固有の個別のアクションを定義できます。 アクションは、アプリケーションが、そのアクションに対して指定されたオペレーティング システムに展開された場合にのみ実行されます。 たとえば、Windows と Linux をサポートするアプリケーションを定義し、Windows と Linux に対してそれぞれ .bat と .sh の個別のアクションを指定します。

8. （オプション）［追加］アイコンをクリックします。

   a. アプリケーションの実行を変更するために使用する［アクション パラメータ］を指定します。

   b. アクション パラメータの［説明］、［データ タイプ］、および［デフォルト値］を指定します。

   c. （オプション）エンド ユーザがアプリケーションの実行中にアクション パラメータの値を入力できるよう指定するには、［ユーザ編集可能］を選択します。 入力が必要なときにエンド ユーザが受け取るプロンプトとして［ラベル］を指定します。

   d. （オプション）ユーザ入力が必要なことを指定するには、［必須］を選択します。

   e. ［終了］をクリックします。

   ウィザードは、アクション オプションを［インストール アクション オプションの定義］パネル内の［オプション］リストに追加し、［アクション プレビュー］を更新します。

   注: 実行可能コマンド全体（そのすべてのオプションを含む）を入力するには、［解析］アイコンをクリックします。 ウィザードはコマンドを解析し、それぞれ個別のアクション オプションを作成します。 続行する前に、各アクション オプションを個別に編集します。

9. ［終了］をクリックします。

   ウィザードは、このアクションを［インストール アクションの設定］パネル内の［アクション］リストに追加します。

10. （オプション）アプリケーション実行中に適用するその他のアクションを追加するには、手順 3 ～ 9 を繰り返します。 アクションを実行する順序を指定するには、上矢印と下矢印を使用します。

11. ［OK］をクリックします。

    注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、［終了］をクリックします。

    CA Server Automation は、サービス プロビジョニング中に展開されているときに定義されたアクションを実行するよう、アプリケーション定義を変更します。

コマンドの実行

場合によっては、サービス プロビジョニング中のアプリケーションの正常な展開のために追加のアクションが必要になることがあります。 たとえば、アプリケーションを展開するには、その前に別のサービスを停止し、展開の後に再起動が必要になる場合があります。 アプリケーション定義では、これらの追加のアクションを実行するためにコマンドライン入力を直接指定できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］を選択します。 ［アプリケーション］ペインで、編集するアプリケーションのツール アイコンをクリックします。
2. ［インストール アクションの設定］タブを選択します。
3. + （追加する）をクリックします。

   ［インストール アクションの選択］パネルに［アクションの定義］ウィザードが表示されます。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、この手順から開始してください。
4. ［アクション］ドロップダウン リストから［プログラムの実行］を選択します。
5. ［プログラム名］フィールドに実行可能コマンドを入力します。

   注: ユーザ定義可能な入力や設定可能なオプションが必要な場合は、基本コマンドのみを入力します。
6. （オプション）アクションを実行するときに使用するユーザ認証情報を指定するには、［ユーザ名］をクリックします。

   注: このオプションにより、サービス プロビジョニング中にユーザによって制限されたアクションが可能になります。主なユース ケースとして、ドメイン ユーザの認証情報を使用してクラスタ化されたアプリケーションの展開を可能にする場合があります。

7. 説明を追加し、指定された実行可能コマンドに対してサポートされるオペレーティング システムを必要に応じて変更して、［次へ］をクリックします。

   ［インストール アクション オプションの定義］パネルが表示され、［アクション プレビュー］に、サービス プロビジョニング中にアプリケーションが展開されているときに実行するコマンドが表示されます。

   注: アクションやアプリケーションに対してサポートされるオペレーティング システムを指定すると、OS 固有の個別のアクションを定義できます。 アクションは、アプリケーションが、そのアクションに対して指定されたオペレーティング システムに展開された場合にのみ実行されます。 たとえば、Windows と Linux をサポートするアプリケーションを定義し、Windows と Linux に対してそれぞれ .bat と .sh の個別のアクションを指定します。

8. （オプション）［追加］アイコンをクリックします。

   a. コマンドの実行を変更するために使用する［アクション パラメータ］を指定します。

   b. アクション パラメータの［説明］、［データ タイプ］、および［デフォルト値］を指定します。

   c. （オプション）エンド ユーザがコマンドの実行中にアクション パラメータの値を入力できるよう指定するには、［ユーザ編集可能］を選択します。 入力が必要なときにエンド ユーザが受け取るプロンプトとして［ラベル］を指定します。

   d. （オプション）ユーザ入力が必要なことを指定するには、［必須］を選択します。

   e. ［終了］をクリックします。

   ウィザードは、アクション オプションを［インストール アクション オプションの定義］パネル内の［オプション］リストに追加し、［アクション プレビュー］を更新します。

   注: 実行可能コマンド全体（そのすべてのオプションを含む）を入力するには、［解析］アイコンをクリックします。 ウィザードはコマンドを解析し、それぞれ個別のアクション オプションを作成します。 続行する前に、各アクション オプションを個別に編集します。

9. ［終了］をクリックします。

   ウィザードは、このアクションを［インストール アクションの設定］パネル内の［アクション］リストに追加します。

10. （オプション）アプリケーション実行中に適用するその他のアクションを追加するには、手順 3 ～ 9 を繰り返します。 アクションを実行する順序を指定するには、上矢印と下矢印を使用します。

11. ［OK］をクリックします。

    注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、［終了］をクリックします。

    CA Server Automation は、サービス プロビジョニング中に展開されているときに定義されたアクションを実行するよう、アプリケーション定義を変更します。

ファイルの作成および更新

多くのアプリケーションは、実行されるときに設定ファイルを参照します。アプリケーション定義では、定義の一部としてファイルを作成および更新することができます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］を選択します。 ［アプリケーション］ペインで、編集するアプリケーションのツール アイコンをクリックします。
2. ［インストール アクションの設定］タブを選択します。
3. + （追加する）をクリックします。

   ［インストール アクションの選択］パネルに［アクションの定義］ウィザードが表示されます。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、この手順から開始してください。
4. ［アクション］ドロップダウン リストから［ファイルの作成］または［ファイルの更新］を選択します。
5. ファイル名を入力し、［ファイルの作成］オプションの場合は［ファイル フォーマット］を指定します。

6. （オプション）アクションを実行するときに使用するユーザ認証情報を指定するには、［ユーザ名］をクリックします。

   注: このオプションにより、サービス プロビジョニング中にユーザによって制限されたアクションが可能になります。主なユース ケースとして、ドメイン ユーザの認証情報を使用してクラスタ化されたアプリケーションの展開を可能にする場合があります。

7. 説明を追加し、指定されたファイルに対してサポートされるオペレーティング システムを必要に応じて変更して、［次へ］をクリックします。

   ［インストール アクション オプションの定義］パネルが表示されます。

   注: アクションやアプリケーションに対してサポートされるオペレーティング システムを指定すると、OS 固有の個別のアクションを定義できます。 アクションは、アプリケーションが、そのアクションに対して指定されたオペレーティング システムに展開された場合にのみ実行されます。 たとえば、Windows と Linux をサポートするアプリケーションを定義し、Windows と Linux に対してそれぞれ .bat と .sh の個別のアクションを指定します。

8. ファイルの作成アクション用のファイルにパラメータを追加するには、［追加］アイコンをクリックします。

   a. ファイルに追加する［アクション パラメータ］を指定します。

   b. アクション パラメータの［デフォルト値］を指定します。

      注: パラメータの値セットを保持するには、［値リスト］を使用します。

   c. （オプション）エンド ユーザがコマンドの実行中にアクション パラメータの値を入力できるよう指定するには、［ユーザ編集可能］を選択します。 入力が必要なときにエンド ユーザが受け取るプロンプトとして［ラベル］を指定します。

   d. （オプション）ユーザ入力が必要なことを指定するには、［必須］を選択します。

   e. ［終了］をクリックします。

   ウィザードは、パラメータと値をプロパティ ファイルに追加します。ファイル内の行ごとに、この手順を繰り返します。

   例: **キーと値のプロパティ ファイルに編集可能なパスワードを追加する方法**

   - ［アクション パラメータ］に「*password*」を指定します。
   - ［デフォルト値］に「*changeit*」を指定します。
   - ［ユーザ編集可能］を選択し、［ラベル］に「*パスワードの入力*」を指定します。

   CA Server Automation は、*password=changeit* をプロパティ ファイルに追加します。 ユーザがサービスをプロビジョニングすると、CA Server Automation はユーザにパスワードの入力を求めます。

9. ファイルの更新アクション用のファイル内のパラメータを編集するには、［追加］アイコンをクリックします。

   a. ［アクション パラメータ］に、置換するテキストを指定します。

   b. ［デフォルト値］に、新しいテキストを指定します。

      注: パラメータの値セットを保持するには、［値リスト］を使用します。

   c. （オプション）エンド ユーザがコマンドの実行中にアクション パラメータの値を入力できるよう指定するには、［ユーザ編集可能］を選択します。 入力が必要なときにエンド ユーザが受け取るプロンプトとして［ラベル］を指定します。

   d. （オプション）ユーザ入力が必要なことを指定するには、［必須］を選択します。

   e. ［終了］をクリックします。

   ウィザードは、ファイル内の指定されたテキストを新しい値で置換します。 置換するテキスト文字列ごとに、この手順を繰り返します。

   例: **一般的な** Wiki **プロパティ ファイル内の** Wiki **の名前を指定する方法**

   - ［アクション パラメータ］に「###WIKINAME###」を指定します。
   - ［デフォルト値］として Wiki サイトの名前を指定します。

   CA Server Automation は、プロパティ ファイル内の ###WIKINAME### のインスタンスを Wiki サイトの名前で置換します。

10. ［終了］をクリックします。

    ウィザードは、このアクションを［インストール アクションの設定］パネル内の［アクション］リストに追加します。

11. （オプション）アプリケーション実行中に適用するその他のアクションを追加するには、手順 3 ～ 10 を繰り返します。 アクションを実行する順序を指定するには、上矢印と下矢印を使用します。

12. ［OK］をクリックします。

    注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、［終了］をクリックします。

    CA Server Automation は、サービス プロビジョニング中に展開されているときに定義されたアクションを実行するよう、アプリケーション定義を変更します。

CA ITCM ソフトウェア パッケージまたはグループの展開

CA Server Automation は、CA ITCM と統合することにより、サービス プロビジョニング中にソフトウェア パッケージやパッケージ グループを展開することができます。 ソフトウェア パッケージを展開するようにアプリケーションを定義するか、または別のアプリケーションの定義の一部として適用する追加のアクションとしてソフトウェア パッケージの展開を追加することができます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］を選択します。 ［アプリケーション］ペインで、編集するアプリケーションのツール アイコンをクリックします。
2. ［インストール アクションの設定］タブを選択します。
3. + （追加する）をクリックします。

   ［インストール アクションの選択］パネルに［アクションの定義］ウィザードが表示されます。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、この手順から開始してください。
4. ［アクション］ドロップダウン リストから［ITCM パッケージ］または［ITCM パッケージ グループ］を選択します。
5. パッケージの場合は、パッケージを展開するために使用する［ITCM サーバ］、［パッケージ］、および［プロシージャ］を指定します。

   パッケージ グループの場合は、使用する［パッケージ グループ］を指定します。

   注: 選択できるのは、CA Server Automation で使用するようにセットアップされた選択されたパッケージおよびパッケージ グループのみです。

6. 説明を追加し、指定されたパッケージまたはグループに対してサポートされるオペレーティング システムを必要に応じて変更して、［終了］をクリックします。

   ウィザードは、このアクションを［インストール アクションの設定］パネル内の［アクション］リストに追加します。

   注: アクションやアプリケーションに対してサポートされるオペレーティング システムを指定すると、OS 固有の個別のアクションを定義できます。 アクションは、アプリケーションが、そのアクションに対して指定されたオペレーティング システムに展開された場合にのみ実行されます。 たとえば、Windows と Linux をサポートするアプリケーションを定義し、Windows と Linux に対してそれぞれ .bat と .sh の個別のアクションを指定します。

7. （オプション）アプリケーション実行中に適用するその他のアクションを追加するには、手順 3 ～ 6 を繰り返します。 アクションを実行する順序を指定するには、上矢印と下矢印を使用します。

8. ［OK］をクリックします。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、［終了］をクリックします。

   CA Server Automation は、サービス プロビジョニング中に展開されているときに定義されたアクションを実行するよう、アプリケーション定義を変更します。

CA Process Automation プロセスの実行

CA Process Automation では、一連の並列操作を複雑なワークフローに結合できます。 CA Server Automation と CA Process Automation との統合を使用すると、アプリケーション定義の一部としてプロセス ワークフローを指定できます。

注: プロセス ワークフローの詳細については、CA Process Automation のドキュメントを参照してください。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］を選択します。 ［アプリケーション］ペインで、編集するアプリケーションのツール アイコンをクリックします。

2. ［インストール アクションの設定］タブを選択します。

3. + （追加する）をクリックします。

   ［インストール アクションの選択］パネルに［アクションの定義］ウィザードが表示されます。

   注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、この手順から開始してください。

4. ［アクション］ドロップダウン リストから［Process Automation プロセス］を選択します。

5. 使用可能なプロセスのドロップダウン リストから、プロセスの［要求開始フォーム］を指定します。

   注: CA Process Automation でプロセス ワークフローを表示および編集するには、［プロセスを開く］をクリックします。

6. 説明を追加し、指定されたプロセスに対してサポートされるオペレーティング システムを必要に応じて変更して、［次へ］をクリックします。

   ［インストール アクション オプションの定義］パネルが表示され、アクション オプションとして定義されたプロセス内の各手順が表示されます。

   注: アクションやアプリケーションに対してサポートされるオペレーティング システムを指定すると、OS 固有の個別のアクションを定義できます。 アクションは、アプリケーションが、そのアクションに対して指定されたオペレーティング システムに展開された場合にのみ実行されます。 たとえば、Windows と Linux をサポートするアプリケーションを定義し、Windows と Linux に対してそれぞれ .bat と .sh の個別のアクションを指定します。

7. （オプション）アクションを編集するにはツール アイコンをクリックし、それらの実行順序を変更するには上矢印と下矢印を使用します。

8. ［終了］をクリックします。

   ウィザードは、このアクションを［インストール アクションの設定］パネル内の［アクション］リストに追加します。

9. （オプション）アプリケーション実行中に適用するその他のアクションを追加するには、手順 3 ～ 8 を繰り返します。 アクションを実行する順序を指定するには、上矢印と下矢印を使用します。

10. ［OK］をクリックします。

    注: アプリケーションの定義 (P. 973)中にアクションを追加する場合は、［終了］をクリックします。

    CA Server Automation は、サービス プロビジョニング中に展開されているときに定義されたアクションを実行するよう、アプリケーション定義を変更します。

サービス テンプレートの作成

サービス プロビジョニングは、サービス テンプレートに基づいたサービスの作業インスタンスの作成です。サービス テンプレートは、アプリケーションのセット（関連付けられたアクションを含む）と、サービスをホストするために必要なマシン定義です。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規サービス テンプレート］を選択します。

   ［サービス テンプレートの作成］パネルが表示されます。

2. サービス テンプレートの名前と説明を入力し、サービスをホストするために必要なマシンの数を選択します。

3. （オプション）サービス テンプレートにエンドポイント テンプレート ファイルを添付するには、［サービス情報ファイル］を指定します。

   ［サービス情報ファイル］は、サービスが正常にプロビジョニングされたときにユーザに表示されるパネルです。HTML 形式のファイルは、サービスにアクセスするために必要な接続の詳細や、サービスを使用するために必要なその他の任意の情報を指定します。

   注: サービス情報ファイルの例については、CA Server Automation に付属のサービス テンプレートを確認してください。

4. （オプション）サービス テンプレートを［エクスプローラ］ツリー内のユーザ定義グループに整理できるようにするには、セミコロンで区切られたタグのリストを指定します。

5. （オプション）追加のアプリケーションを許可して、サービスをプロビジョニングするときにエンドユーザが依存アプリケーションを追加できるようにします。

   注: このオプションは、エンドユーザが後で特定の依存アプリケーションを追加することによってベースにすることができる基本テンプレートを作成するために使用します。 たとえば、サポートしているインフラストラクチャを使用してアプリケーション サーバをプロビジョニングし、エンドユーザが任意の依存アプリケーションを追加で指定できるようするためのテンプレートを作成します。

6. （オプション）サービスをプロビジョニングするために必要なマシンの設定と要件を編集します。

   注: デフォルトでは、サービス テンプレートは、サービス プロビジョニングに必要なすべてのマシンに VM テンプレートを自動的に適用します。指定されたオペレーティング システムのために使用する任意のデフォルトの VM テンプレートを指定するには、サービス プロビジョニング用のマシン テンプレートを設定します (P. 971)。 デフォルトのテンプレートが存在せず、どのテンプレートも選択されない場合、CA Server Automation は vCenter VMware サーバに適切なテンプレートを要求します。

   a. ［詳細］をクリックします。

      ［ターゲット マシン詳細］パネルが表示され、マシンごとのデフォルト設定が表示されます。

   b. 単一のマシンの設定を編集するには、ツール アイコンをクリックします。

      注: 複数のマシンの設定を編集するには、複数のマシンを選択し、右矢印をクリックします。

      ［マシン］パネルが表示され、そのマシンの設定とリソース設定が表示されます。

   c. （オプション）使用する VMware vCenter テンプレートを指定します。

   d. マシンに必要な CPU およびメモリ リソースと、そのマシンがマシンのクラスタであるかどうかを指定します。

      注: クラスタの場合、マシンの設定はクラスタ内の各マシンに適用されます。

   e. （オプション） VMware vCenter プロビジョニングに使用する動的仕様を指定または作成します。

   f. ［ディスク］タブをクリックし、マシンのビューを表示して、ディスク ストレージ設定を変更します。

      注: 複数のマシンを変更する場合は、ディスクを追加すると、選択されたマシンの共有ストレージが作成されます。

   g. マシンのネットワーク設定を表示および変更するには、［NIC］タブをクリックします。

   h. ［OK］をクリックします。

i. 必要に応じてマシンごとに手順 b ～ h を繰り返し、［閉じる］をクリックして［サービス テンプレート］パネルに戻ります。

7. （オプション）複数のアプリケーションに同じパラメータが必要な場合は、個別のアプリケーションでパラメータを設定する代わりに、グローバル代替変数を使用できます。 複数のアプリケーションに同じデータベース接続と認証情報が必要な場合、デフォルト値を指定する代替変数を作成できます。 その後、個々のアプリケーションでそれらの代替変数を指定することができます。

   ［オプション］タブで、［追加］アイコンをクリックしてグローバル代替変数を追加します。

   a. ［アクション パラメータ］に代替変数を入力します。 変数の開始と終了には # を使用します。

      例： #DB_URL#

   b. 変数の［説明］、［ラベル］、および［データ タイプ］を入力します。

   c. 変数の［デフォルト値］を入力します。

      注: 変数の値セットを保持するには、［値リスト］をクリックします。

   d. （オプション）エンド ユーザがアプリケーションの実行中にアクション パラメータの値を入力できるよう指定するには、［ユーザ編集可能］を選択します。 入力が必要なときにエンド ユーザが受け取るプロンプトとして［ラベル］を指定します。

   e. （オプション）ユーザ入力が必要なことを指定するには、［必須］を選択します。

   f. ［OK］をクリックします。

      CA Server Automation は、この変数をサービス テンプレートの［オプション］のリストに追加します。

   g. 必要に応じてサービス テンプレート内のアプリケーション アクション オプションを編集し、アクション パラメータの［デフォルト値］を代替変数に置換します。

8. サービス テンプレートにアプリケーションを追加するには、以下の手順に従います。

   a. ［利用可能なアプリケーションおよびサービス テンプレート］パネルの［アプリケーション リスト］タブを選択します。

   b. 選択するアプリケーションをダブルクリックします。

      アプリケーションは［選択されたアプリケーションおよびサービス テンプレート］パネルにリスト表示されます。

   c. アプリケーションをホストするシステムを指定します。

   d. （オプション）サービス テンプレート アプリケーションを設定するための編集アイコンをクリックします。

   ［選択されたアプリケーションおよびサービス テンプレート］パネルはアプリケーションの詳細で更新されます。

9. このサービス テンプレートの一部としてその他のサービス テンプレートをプロビジョニングするには、以下の手順に従います。

   a. ［利用可能なアプリケーションおよびサービス テンプレート］パネル内の［サービス テンプレート リスト］タブを選択します。

   b. 選択するサービス テンプレートをダブルクリックします。

      テンプレートは［選択されたアプリケーションおよびサービス テンプレート］パネルでリスト表示されます。

   ［選択されたアプリケーションおよびサービス テンプレート］パネルが、サービス テンプレートの詳細で更新されます。

10. （オプション）その他のアプリケーションとサービス テンプレートを追加するには、手順 8 と 9 を繰り返します。 実行する順序を指定するには、上矢印と下矢印を使用します。

    注: アプリケーションの複数のインスタンスを同じマシンまたは異なるマシンに展開するには、マシンごとにアプリケーションの追加を繰り返します。

11. ［OK］をクリックします。

    CA Server Automation は、このテンプレートを［エクスプローラ］ツリー内のサービス テンプレートのリストに追加します。 サービス テンプレートが、プロビジョニング用に準備できました。

    注: CA Server Automation は、予約マネージャ で使用する予約テンプレートをサービス テンプレートに基づいて自動的に作成します。

アプリケーション定義とサービス テンプレートの共有

CA Server Automation を使用すると、CA Server Automation の各インスタンスにわたってアプリケーション定義とサービス テンプレートを共有できます。

アプリケーション定義またはサービス テンプレートをエクスポートするには、以下の手順に従います。

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］または［サービス テンプレート］を選択します。
2. エクスポートするアプリケーションまたはテンプレートを選択し、［エクスポート］アイコンをクリックします。
3. ［保存］をクリックし、エクスポート ファイルのファイル名と場所を指定して、［保存］をクリックします。

   CA Server Automation は、アプリケーション定義またはサービス テンプレートが含まれた XML ファイルを作成します。

アプリケーション定義またはサービス テンプレートをインポートするには、以下の手順に従います。

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［アプリケーション］または［サービス テンプレート］を右クリックして［インポート］を選択します。
2. アプリケーション定義またはサービス テンプレートが含まれた XML ファイルを指定し、［インポート］をクリックします。

   CA Server Automation は、ファイルで指定されたアプリケーション定義およびサービス テンプレートを作成します。
3. 新しいアプリケーション定義のための適切な実行可能ファイルをステージング ディレクトリに追加します。
4. 必要に応じてアプリケーション定義とサービス テンプレートを編集することにより、環境への適切なプロビジョニングを可能にします。

   新しいアプリケーション定義とサービス テンプレートがサービス プロビジョニングに使用できるようになりました。

vCenter からのサービスのキャプチャ

CA Server Automation を使用すると、VMware vCenter 上で実行されている既存のサービスをキャプチャし、サービス テンプレートおよびそのサービス テンプレートを構成するアプリケーションを作成することができます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［データ センター］の下のサービス ノードを右クリックして［管理］-［サービスのキャプチャ］を選択します。

   ［サービスをサービス テンプレートにキャプチャ］パネルが表示されます。

2. サービス テンプレートの名前と説明を入力します。
3. テンプレート内のアプリケーションを実行する順序を指定するには、上矢印と下矢印を使用します。
4. 各テンプレートで使用するアプリケーション名やテンプレート名を変更するには、［変更］をクリックします。
5. ［OK］をクリックします。

   CA Server Automation はマシンを停止してそれらをアプリケーションとしてキャプチャし、サービスに基づいたサービス テンプレートを作成します。

   キャプチャされた各アプリケーションは、マシンと、そのマシンに含まれるソフトウェアの VM テンプレートで構成されます。 必要に応じてアプリケーションとサービス テンプレートを変更することにより、それらの別のマシンへの展開を可能にします。

   注: CA Server Automation は、予約マネージャ で使用する予約テンプレートをサービス テンプレートに基づいて自動的に作成します。

サービスのプロビジョニング

サービス テンプレートを作成すると、*サービス消費者*によるワンクリック サービス プロビジョニングが可能になります。

注: この手順では、サービスが直ちにプロビジョニングされます。指定した時間にサービスをプロビジョニングしたい場合は、予約マネージャ を使用し、サービス用の予約テンプレートを使用して予約を作成します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］-［サービス テンプレート］を選択します。 ［サービス テンプレート］ペインで、プロビジョニングするサービスの［サービスのプロビジョニング］アイコンをクリックします。
2. プロビジョニングするサービス インスタンスの名前を入力します。
3. （オプション）［詳細］をクリックし、利用可能なアプリケーションから選択してサービス テンプレートで展開します。

   注: その他のアプリケーションは、それぞれのアプリケーション定義に従って展開および実行されます。 選択できるのは、すでにサービス テンプレート内に存在するアプリケーションに依存しているアプリケーションのみです。
4. （オプション）サービス テンプレート内のアプリケーション定義で指定されている追加の入力をすべて指定します。
5. ［OK］をクリックします。

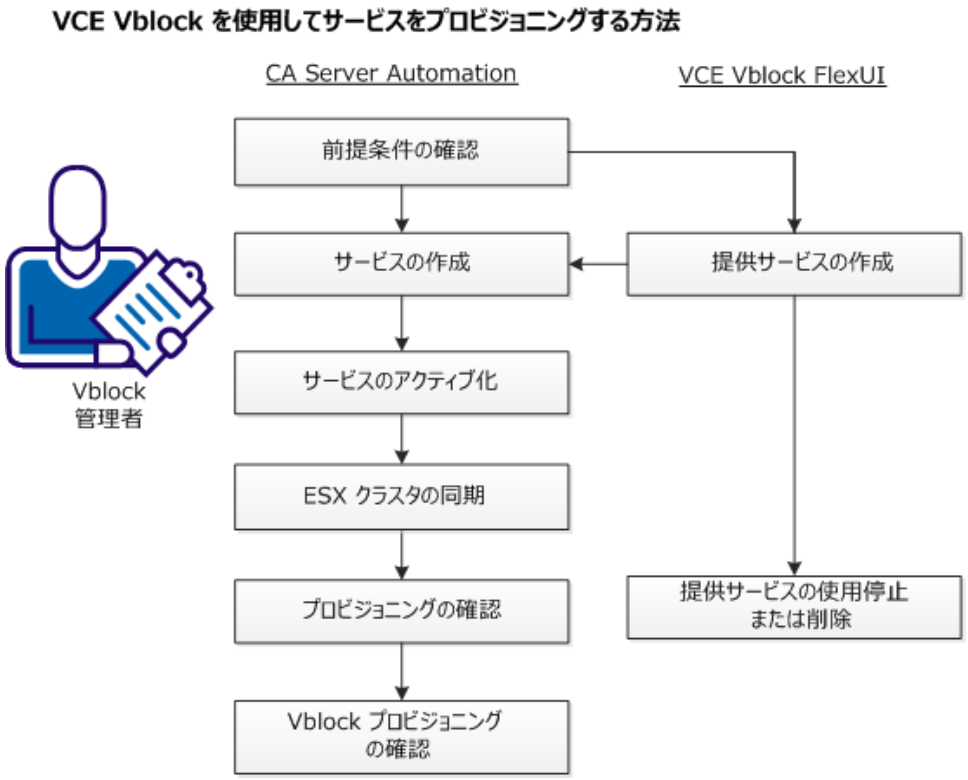
CA Server Automation は要求されたサービス インスタンスをプロビジョニングし、それを［エクスプローラ］ツリーの［オンデマンド リソース］の下のリソースのリストに追加します。 ［ジョブ］ペインでプロビジョニングのステータスを追跡します。

VCE Vblock を使用してサービスをプロビジョニングする方法

CA Server Automation では統合をサポートしており、EMC Ionix Unified Infrastructure Manager （UIM）用の UIM 3.0 API を使用して、1 つ以上の Vblock サーバを管理することができます。 Vblock 管理者は CA Server Automation を使用して VCenter プロビジョニング プロセスを大幅に加速し、実稼働までの時間を短縮することができます。また、Vblock 統合では、VCPMM やサービス プロビジョニングなどの他の CA Server Automation コンポーネントに、VM、アプリケーションおよび他の論理 Vblock コンポーネントを管理およびプロビジョニングさせることができます。

重要：CA Server Automation Vblock の統合には、EMC ®Ionix ™ Unified Infrastructure Manager （UIM/P）を使用します。 VCE では、UIM 以外の製品を使用する Vblock コンポーネントのプロビジョニングはお勧めしません。 たとえば、UCS Manager を直接使用するか、 CA Server Automation UCS PMM を使用して、Cisco UCS ブレード（Vblock UCS）を管理およびプロビジョニングすることはお勧めしません。

Vblock サービスは提供サービスという名前の定義済みテンプレートから作成されます。このテンプレートでは、デフォルトのセットと、サービスが消費できるサーバ数とストレージ容量を制限する制約が提供されます。提供サービスを予め用意することにより、UIM サービスは最小限の入力で管理されます。



前提条件の確認 (P. 998)

（オプション） Vblock 提供サービスの作成 (P. 999)

Vblock サービス インスタンスの作成 (P. 1001)

Vblock サービスのアクティブ化 (P. 1002)

ESX クラスタの同期 (P. 1002)

Vblock プロビジョニングの確認 (P. 1002)

Vblock プロビジョニングのトラブルシューティング (P. 1003)

前提条件の確認

CA Server Automation を使用して Vblock サービスを展開する前に、以下の情報を認識していることを確認してください。

- Vblock 統合は CA Server Automation で設定します。 設定情報については、「VCE Vblock 管理コンポーネントの設定方法 (P. 564)」を参照してください。 また Vblock 設定プロセスは、CA Server Automation の［ファースト ステップ ダッシュボード］からも開始できます。
- Web ベース FlexUI ユーザ インターフェースを含む、VCE Vblock の動作環境に精通している必要があります。 UIM 提供サービスは、FlexUI の管理ページを使用して作成する必要があります。
- CA Server Automation ユーザ インターフェースとリソースのプロビジョニング方法の概要について理解している必要があります。

（オプション）Vblock 提供サービスの作成

CA Server Automation で Vblock サービスをプロビジョニングするには、提供サービスが UIM 環境に存在する必要があります。

FlexUI を使用した提供サービスの作成/変更方法

1. FlexUI の［管理］ページで、［追加］をクリックします。
2. ［編集］をクリックして名前と説明を指定し、オペレーティング システムを選択します。 変更を保存します。
3. ［サーバ］タブを選択します。
4. ［追加］をクリックし、ブレードを追加します。
5. サーバのグレード、説明、最小値、最大値、およびデフォルトのブレードを選択します。 変更を保存します。
6. ［ストレージ］タブを選択します。
7. ［制約］の下にある［追加］をクリックし、グレード、説明、最小 LUN サイズ（GB）および最大合計（GB）を設定します。変更を保存します。
8. ［起動］の下にある［追加］をクリックし、起動、グレード、説明、およびサイズ（GB）を設定します。 変更を保存します。
9. ［ネットワーク］タブを選択し、［追加］をクリックします。
10. Vblock、サービス品質、PIN グループ、および仮想ネットワークを設定します。 変更を保存します。
11. ［閉じる］をクリックします。

    提供サービスが作成または更新されます。 FlexUI の［管理］ページの［提供サービス］ページに表示されることを確認します。

リソース ツリーでの VCE Vblock の確認

設定および検出に成功すると、新たに検出されたリソースが［リソース］-［エクスプローラ］ペインの対応するグループに表示されます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. ［VCE Vblock UIM サービス］グループを展開します。

   利用可能なサービス リソースが表示されます。

CA Server Automation で、検出された VCE Vblock 環境を管理する準備が整いました。 リソースのステータスとプロパティをモニタできます。

Vblock サービスの作成

VCE Vblock 提供サービスを使用すると、オペレーティング システムと追加ソフトウェアの両方を 1 回の操作でプロビジョニングできます。このプロビジョニング方法はデフォルトのランタイム処理よりも高速で効率的ですが、あらかじめ FlexUI ユーザ インターフェースを使用して Vblock 提供サービスを用意しておく必要があります。

Vblock サービスを作成する方法

1. ［リソース］タブをクリックし、［エクスプローラ］ペインの Vblock ツリー階層に移動します。

   Vblock リソース、提供サービス、および既存のサービスを参照します。既存の提供サービスから新しいサービスを作成し、必要に応じて、Vcenter 同期までの全プロセスを 1 つの操作で行えるように効率化できます。 CA Server Automation は計画されたサービスを作成するだけでなく、プロビジョニング、有効化および Vcenter 同期プロセスを含めることができます。

2. 使用したい提供サービスを右クリックし、［作成］を選択します。

   ［Vblock サービスの作成］ダイアログ ボックスが表示されます。

3. 必要なサービスと詳細情報を指定します。

4. ［OK］をクリックします。

   Vblock サービス インスタンスが作成されます。 以下のサービス アクションを実行できます。

   - サービスのアクティブ化
   - アクティブなサービスの非アクティブ化
   - 既存のサービスの削除
   - プロビジョニングされたサービスのブレードの解放

Vblock サービスのアクティブ化

サービスをプロビジョニング（予約）するには、サービスを右クリックして［アクティブ化］を選択します。 サービスのサーバ、ネットワークおよびストレージ リソースが予約されます。 サービスによって使用されるインフラストラクチャは、使用中としてタグ付けされ、他のサービスでは利用できなくなります。 このサービスがアクティブにされるのが初めての場合、オペレーティング システムがインストールされます。 サーバはオペレーティング システムの電源をオンにし、起動します。

ESX クラスタの同期

既存の vCenter で Vblock サービスをアクティブにするには、サービスの ESX クラスタが vCenter とそのデータセンターに関連付けられている必要があります。

Vblock サービスを vCenter と同期する方法

1. Vblock サービスを選択し、［アクション］メニューから［同期］を選択します。

   注: 同期オプションは、［vSync ステータス］が［同期可能］または［成功］の場合にのみ有効です。

Vblock プロビジョニングの確認

Vblock サービス アクションは［ジョブ］ペインに表示されます。UIM タスクをモニタしています。 ［ジョブ］ペインにはまた、進捗状況、親子プロセスおよびジョブ結果も表示されます。

Vblock プロビジョニングのトラブルシューティング

例: サービス インスタンスの作成で遅延が発生する

症状：

既存の提供サービスの詳細情報のロードに長時間かかる場合がある。

解決方法：

これは、vCenter クラスタ情報をロードする際の UIM/P のパフォーマンスの問題です。

例: 2 番目のサービス アクションがエラーをスローする。

症状：

2 番目のサービス アクションを選択すると、エラーが返される。

解決方法：

これは Vblock サーバの制限事項です。Vblock では、完全に独立したアクションでも、2 つのアクションを並行して実行することはできません。1 番目のアクションが完了するまで 2 番目のアクションは待機させます。

例: Vblock サービスを削除できない。

症状：

CA Server Automation で Vblock サービスを削除しようとしたが、できなかった。

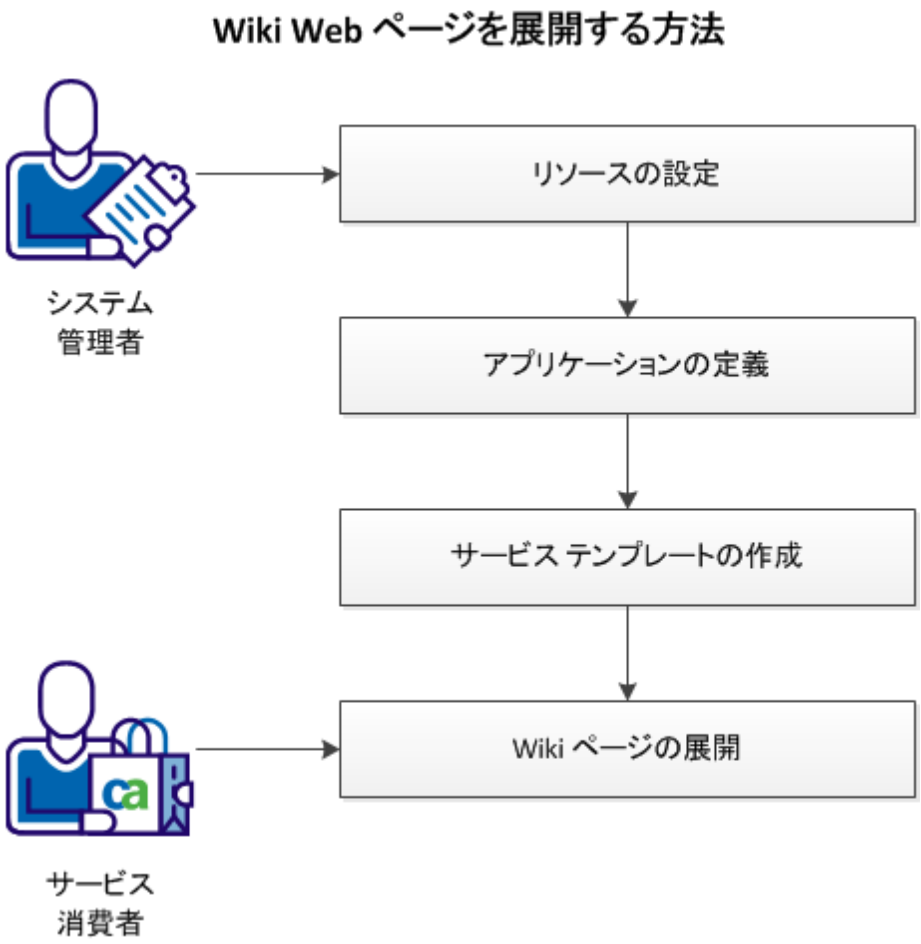
解決方法：

削除できるサービスは、計画および使用停止サービスのみです。UIM/P では、サービスの使用停止 API は提供されていません。サービスを削除するには、FlexUI ユーザ インターフェースを使用して、使用停止する必要があります。

Wiki Web ページを展開する方法

この例では、エンド ユーザが MediaWiki Web ページを展開できるようにするためのテンプレートを準備する方法を示します。まず、アプリケーション実行可能ファイルとそれらの実行アクションを定義します。次に、サービス テンプレート内でこれらのアプリケーションを組み合わせて、それらの実行順序と、それらをホストするために必要なマシンを定義します。

以下のプロセスは、システム管理者がアプリケーションを組み合わせて、サービス消費者によるワンクリック サービス プロビジョニングを可能にするサービス テンプレートを作成する方法の概要を示しています。



1. Wiki 用のマシン テンプレートの設定（P. 1005）

   サービス テンプレートで使用するデフォルトのマシン設定を指定します。

2. Wiki 用のアプリケーションの定義（P. 1006）

   実行可能アプリケーション、前提条件、およびアプリケーションに対するリソースとオペレーティング システムの要件を指定します。

3. Wiki サービス テンプレートの作成（P. 1019）

   アプリケーションのセットと、それらをホストするために必要なマシンを展開可能なサービス テンプレートとして指定します。

4. Wiki の展開（P. 1020）

   サービスのインスタンスをサーバ環境に展開します。

Wiki 用のマシン テンプレートの設定

CA Server Automation を使用すると、指定したオペレーティング システム用の VM テンプレートを指定できます。これらのテンプレートは、サービス プロビジョニング中に必要なマシンに自動的に適用できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を選択します。
2. 右側のパネルで、使用するテンプレートが含まれた vCenter Server のツール アイコンをクリックします。

   ［マシン テンプレート設定］パネルが表示されます。

3. リストからオペレーティング システムを選択し、利用可能な VM テンプレートのリストからテンプレートを選択して、［デフォルトとして設定］をクリックします。

   CA Server Automation は、選択された VM テンプレートを指定されたオペレーティング システムと関連付けます。

4. （オプション）OS ファミリ用のすべての VM テンプレート設定のリストを表示および管理するには、そのオペレーティング システム グループ フォルダをクリックします。
5. ［OK］をクリックして［マシン テンプレート設定］を終了します。

Wiki 用のアプリケーションの定義

サービス プロビジョニングにおける最初の手順では、サービス テンプレートを構成するために使用可能なアプリケーションのセットと、それらを実行するために必要なアクションを定義します。

次の手順に従ってください:

1. CA Server Automation インストール ディレクトリ内のステージング ディレクトリに、以下の各アプリケーション用のフォルダを作成します。
   - Apache HTTP サーバ
   - PHP
   - MySQL
   - Wiki データベース
   - MediaWiki コンテンツ
2. すべてのアプリケーション ファイルを対応するフォルダにコピーします。
3. CA Server Automation で新しいアプリケーションを定義します。詳細については、以下の章を参照してください。

Apache HTTP サーバの定義

Apache HTTP サーバは、Wiki が実行されるホストです。この Web サーバは、サービスとしてインストールします。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

2. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
3. アプリケーション ファイルの場所を指定します。
4. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。

5. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Microsoft Windows Server バージョン
6. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「Windows ファイアウォールの無効化」、「Windows 2003 での Windows ファイアウォールの無効化」、「Apache サーバのインストール」、「再起動」の 4 つのインストール アクションを定義します。

7. ［+］をクリックして「Windows ファイアウォールの無効化」アクションを定義します。
   a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

      ```
      netsh advfirewall set currentprofile state off
      ```

   b. ［次へ］をクリックします。

c. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

8. ［+］をクリックして「Windows 2003 での Windows ファイアウォールの無効化」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
netsh advfirewall set opmode disable & if "%errorlevel%"=="1" exit /b 0
```

b. ［次へ］をクリックします。

c. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

9. ［+］をクリックして「Apache サーバのインストール」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
cmd.exe /c start /w msiexec.exe
```

b. ［次へ］をクリックします。

c. ［インストール アクション オプションの定義］パネルで、以下の 4 つのオプションを追加します。

```
/i %CD%¥httpd-2.2.22-win32-x86-openssl-0.9.8t.msi
INSTALLDIR=C:¥Apache
SERVERADMIN=admin@localhost.com
SERVERNAME=%LOCALHOST%
AgreeToLicense=1
ALLUSERS=1
RebootYESNo=No
```

d. アクションのプレビューを確認し、［終了］をクリックします。

アクションが保存されます。

10. ［+］をクリックして「再起動」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
cmd.exe /c shutdown -r -t 20 & exit /b 1641
```

b. ［次へ］をクリックします。

c. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

11. ［次へ］をクリックしてから［終了］をクリックします。

Apache HTTP サーバ アプリケーションが保存されます。

PHP の定義

PHP は、Wiki などの動的な Web ページの作成に使用されるスクリプト言語です。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

2. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
3. アプリケーション ファイルの場所（絶対パスまたはステージング フォルダを基準にした相対パス）を指定します。
4. このアプリケーションの前提条件として Apache HTTP サーバを指定します。
5. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。

6. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Microsoft Windows Server バージョン
7. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「PHP のインストール」、「Apache の停止」、「Apache の起動」の 3 つのインストール アクションを定義します。

8. ［+］をクリックして「PHP のインストール」アクションを定義します。
   a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

      ```
      cmd.exe /c start /w msiexec.exe
      ```

   b. アクションの説明を入力します。

c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下の 5 つのオプションを追加します。

```
/i %CD%¥php-5.3.13-Win32-VC9-x86.msi

APACHEDIR=C:¥Apache¥conf

/qn

AgreeToLicense=YES

ADDLOCAL=ext_php_mysql,ext_php_mysqli,apache22
```

e. ［終了］をクリックします。

アクションが保存されます。

9. ［+］をクリックして「Apache の停止」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
net stop apache2.2
```

b. ［次へ］をクリックします。

c. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

10. ［+］をクリックして「Apache の起動」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
net start apache2.2
```

b. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

11. ［次へ］をクリックしてから［終了］をクリックします。

PHP アプリケーションが保存されます。

MySQL の定義

MySQL は、Wiki データベースが実行されるサーバです。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

2. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
3. アプリケーション ファイルの場所（絶対パスまたはステージング フォルダを基準にした相対パス）を指定します。
4. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。

5. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Microsoft Windows Server バージョン
6. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「MySQL のインストール」、「MySQL の設定」、「ルートへの権限の付与」の 3 つのインストール アクションを定義します。

7. ［+］をクリックして「MySQL のインストール」アクションを定義します。
   a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

      ```
      msiexec
      ```

   b. アクションの説明を入力します。
   c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下の 3 つのオプションを追加します。

```
/i %CD%¥mysql-5.5.25-winx64.msi
```

```
/passive
```

```
INSTALLDIR=C:¥MySQL
```

e. INSTALLDIR オプションをユーザ編集可能にします。

f. ［終了］をクリックします。

アクションが保存されます。

8. ［+］をクリックして「MySQL の設定」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
cmd
```

b. アクションの説明を入力します。

c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下のオプションを追加します。

```
/C C:¥MySQL¥bin¥MySQLInstanceConfig.exe -i -q "-lC:¥mysql_install_log.txt"
"-nMySQL Server 5.5" "-pC:¥MySQL" -v5.5 "-tC:¥MySQL¥my-template.ini"
"-cC:¥mytest.ini" ServerType=DEVELOPMENT DatabaseType=MIXED
ConnectionUsage=DSS Port=3306 ServiceName="MySqlD"
```

```
RootPassword=pass
```

e. RootPassword オプションをユーザ編集可能にします。

f. ［終了］をクリックします。

アクションが保存されます。

9. ［+］をクリックして「ルートへの権限の付与」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
cmd
```

b. アクションの説明を入力します。

c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下のオプションを追加します。

```
/C C:¥MySQL¥bin¥mysql -u root -e "GRANT ALL PRIVILEGES ON *.* TO
'Root'@'localhost' IDENTIFIED BY 'pass';"

--password=pass
```

e. password オプションをユーザ編集可能にします。

f. ［終了］をクリックします。

アクションが保存されます。

10. ［次へ］をクリックしてから［終了］をクリックします。

MySQL アプリケーションが保存されます。

MediaWiki データベースの定義

MediaWiki データベースは、Wiki Web ページのコンテンツが格納される場所です。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

2. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
3. アプリケーション ファイルの場所（絶対パスまたはステージング フォルダを基準にした相対パス）を指定します。
4. このアプリケーションの前提条件として MySQL を指定します。
5. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。

6. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Windows オプション
7. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「データベースのインストール」、「MySQL の停止」、「MySQL の起動」の 3 つのインストール アクションを定義します。

8. ［+］をクリックして「データベースのインストール」アクションを定義します。
   a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

      ```
      cmd /C "C:¥MySQL¥bin¥mysql
      ```

   b. アクションの説明を入力します。
   c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下のオプションを追加します。

```
--user=root

--password=pass

< %CD%¥wiki_db.txt > %CD%¥output.txt"
```

e. password オプションをユーザ編集可能にします。

f. ［終了］をクリックします。

アクションが保存されます。

9. ［+］をクリックして「MySQL の停止」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
net stop MySqlD
```

b. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

10. ［+］をクリックして「MySQL の起動」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

```
net start MySqlD
```

b. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

11. ［次へ］をクリックしてから［終了］をクリックします。

MediaWiki データベース アプリケーションが保存されます。

MediaWiki コンテンツの定義

これらのファイルは、Wiki の実行に必要なアプリケーション ファイルです。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。

2. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
3. アプリケーション ファイルの場所（絶対パスまたはステージング フォルダを基準にした相対パス）を指定します。
4. このアプリケーションの前提条件として PHP と MediaWiki データベースを指定します。
5. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。

6. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Windows オプション
7. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「ファイルのコピー」と「DB サーバの更新」の 2 つのインストール アクションを定義します。

8. ［+］をクリックして「ファイルのコピー」アクションを定義します。
   a. ［インストール アクションの選択］パネルで、［アクション］フィールドに実行するコマンドを入力します。

      xcopy

   b. アクションの説明を入力します。
   c. ［次へ］をクリックします。

d. ［インストール アクション オプションの定義］パネルで、以下の 2 つのオプションを追加します。

```
%CD%¥* C:¥Apache¥htdocs
```

```
/S
```

e. ［終了］をクリックします。

アクションが保存されます。

9. ［+］をクリックして「DB サーバの更新」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］ドロップダウン リストから［ファイルの更新］を選択します。

b. アクションの説明を入力します。

c. ［ファイル名］フィールドに、設定ファイルへのパス「C:¥Apache¥htdocs¥LocalSettings.php」を入力します。

d. ［次へ］をクリックします。

e. ［インストール アクション オプションの定義］パネルで、以下の 5 つのオプションを追加します。

```
CONFIG_FILE_ACTION=FILEUPDATE
```

```
CONFIG_FILE_NAME=C:¥Apache¥htdocs¥LocalSettings.php
```

```
#DB_SERVER#=%DEPENDINGHOST%
```

```
#BLOG_TITLE#=<Wiki Title>
```

```
#DBPASSWORD#=pass
```

f. #DB_SERVER#、BLOG_TITLE、および #DBPASSWORD# オプションをユーザ編集可能にします。

g. ［終了］をクリックします。

アクションが保存されます。

10. ［次へ］をクリックしてから［終了］をクリックします。

MediaWiki コンテンツ アプリケーションが保存されます。

Wiki サービス テンプレートの作成

サービス プロビジョニングは、サービス テンプレートに基づいたサービスの作業インスタンスの作成です。 この手順では、すでに定義したアプリケーションと、サービスをホストするために必要なマシンの数で構成された、Wiki 展開用のサービス テンプレートを作成します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規サービス テンプレート］を選択します。

   ［サービス テンプレートの作成］パネルが表示されます。

2. サービス テンプレートの名前と説明を入力し、サービスをホストするために必要なマシンの数を選択します。 マシンの数は、Wiki Web ページの予測される負荷や、このページに格納しようとしているコンテンツの量によって異なります。 この例では、すべてのアプリケーションを 1 つのサーバにインストールします。

3. ［詳細］をクリックして、マシンの設定を表示します。 すべての値を［自動］に設定されたままにします。 この設定では、プロビジョニング中にテンプレート内のすべてのアプリケーションのサポートされる OS タイプがチェックされ、最も便利な VMware テンプレートが自動的に選択されます。

4. ［サービス情報ファイル］を指定します。 この HTML ファイルは、プロビジョニング プロセスの最後にエンド ユーザに表示され、サービスへのアクセス方法を通知します。

5. ［+］（新規）をクリックして、MediaWiki コンテンツ アプリケーションをサービス テンプレートに追加します。

   ［アプリケーションの選択］パネルに［サービス テンプレート アプリケーションの設定］ウィザードが表示されます。

6. 利用可能な定義済みのアプリケーションのリストから MediaWiki コンテンツを選択し、［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。ここでは何も変更しないでください。

7. ［次へ］をクリックします。

   ［アプリケーション設定の確認］パネルが表示されます。

8. ［終了］をクリックします。

［サービス テンプレートの作成］パネルが、アプリケーションとそれをホストするマシンの詳細で更新されます。

9. 手順 5 ～ 8 を繰り返して MediaWiki データベース アプリケーションを追加します。 アプリケーションの前提条件により、プロビジョニング中に Apache HTTP サーバ、PHP、および MySQL が自動的に追加されます。
10. ［OK］をクリックします。

    CA Server Automation は、このテンプレートを［エクスプローラ］ツリー内のサービス テンプレートのリストに追加します。 サービス テンプレートが、プロビジョニング用に準備できました。

Wiki の展開

サービス テンプレートを作成すると、エンド ユーザによるワンクリック サービス プロビジョニングが可能になります。

次の手順に従ってください:

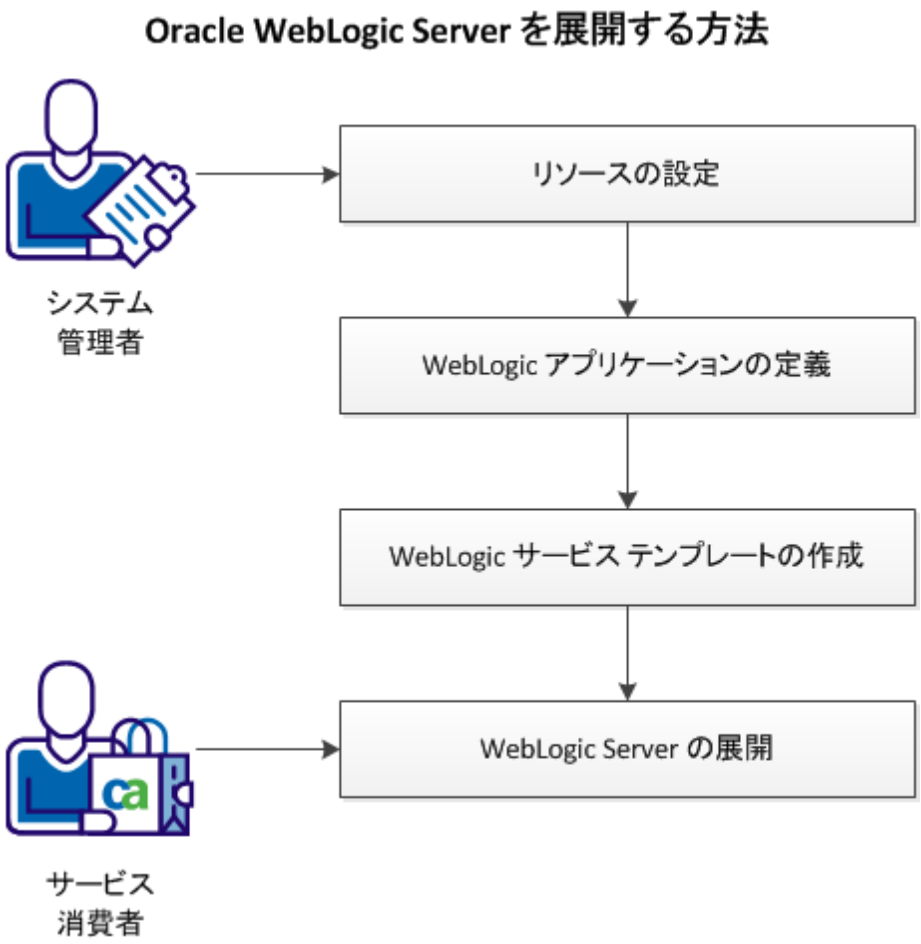
1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］の下にある［サービス テンプレート］を選択します。
2. ［サマリ］タブで、作成された Wiki サービス テンプレートを選択し、［サービスのプロビジョニング］アイコンをクリックします。
3. プロビジョニングするサービス インスタンスの名前を入力します。
4. Wiki Web ページのタイトルを指定します。 このユーザ入力は、MediaWiki コンテンツ アプリケーションの定義で指定されています。
5. ［OK］をクリックします。

    CA Server Automation は要求されたサービス インスタンスをプロビジョニングし、それを［エクスプローラ］ツリーの［オンデマンド リソース］の下のリソースのリストに追加します。 ［ジョブ］ペインでプロビジョニングのステータスを追跡します。
6. プロビジョニングが完了した後、Wiki Web ページへのリンクを含むページが表示されます。プロビジョニングが成功したことを確認するには、このリンクをクリックします。

Oracle WebLogic Server を展開する方法

この例では、エンド ユーザが Oracle WebLogic アプリケーション サーバのインスタンスを展開できるようにするためのテンプレートを準備する方法を示します。 まず、アプリケーション実行可能ファイルとそれらの実行アクションを定義し、次に、このアプリケーションが含まれたサービス テンプレートを作成します。

以下のプロセスは、システム管理者が、サービス消費者によるワンクリック サービス プロビジョニングを可能にするサービス テンプレートを作成する方法の概要を示しています。



1. WebLogic 用のマシン テンプレートの設定（P. 1022）

   サービス テンプレートで使用するデフォルトのマシン設定を指定します。

2. WebLogic アプリケーションの定義（P. 1023）

   WebLogic アプリケーションと、アプリケーションに対するリソースとオペレーティング システムの要件を指定します。

3. WebLogic サービス テンプレートの作成（P. 1026）

   アプリケーションをホストし、展開可能なサービス テンプレートをセットアップするために必要なマシンを指定します。

4. WebLogic Server の展開（P. 1027）

   サービスのインスタンスをサーバ環境に展開します。

WebLogic 用のマシン テンプレートの設定

CA Server Automation を使用すると、指定したオペレーティング システム用の VM テンプレートを指定できます。これらのテンプレートは、サービス プロビジョニング中に必要なマシンに自動的に適用できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を選択します。
2. 右側のパネルで、使用するテンプレートが含まれた vCenter Server のツール アイコンをクリックします。

   ［マシン テンプレート設定］パネルが表示されます。

3. リストからオペレーティング システムを選択し、利用可能な VM テンプレートのリストからテンプレートを選択して、［デフォルトとして設定］をクリックします。

   CA Server Automation は、選択された VM テンプレートを指定されたオペレーティング システムと関連付けます。

4. （オプション）OS ファミリ用のすべての VM テンプレート設定のリストを表示および管理するには、そのオペレーティング システム グループ フォルダをクリックします。

［OK］をクリックして［マシン テンプレート設定］を終了します。

WebLogic アプリケーションの定義

最初の手順では、サービス テンプレートで使用する WebLogic アプリケーションと、そのアプリケーションを実行するために必要なアクションを定義します。

次の手順に従ってください:

1. CA Server Automation インストール ディレクトリ内のステージング ディレクトリに、WebLogic アプリケーション用のフォルダを作成します。
2. すべてのアプリケーション ファイルをこのフォルダにコピーします。
3. CA Server Automation ユーザ インターフェースで、［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規アプリケーション］を選択します。

   ［アプリケーションの詳細］パネルに［アプリケーションの定義］ウィザードが表示されます。
4. アプリケーションの［名前］、［バージョン］、および［ベンダー］を指定します。
5. アプリケーション ファイルの場所（絶対パスまたはステージング フォルダを基準にした相対パス）を指定します。
6. ［次へ］をクリックします。

   ［システム要件］パネルが表示されます。
7. 以下の推奨される値を設定します。
   - CPU の数 - 1
   - メモリ - 512 MB
   - ディスク領域 - 5 GB
   - オペレーティング システム - すべての Microsoft Windows Server バージョン。
8. ［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。「WebLogic のインストール」、「ドメイン用のファイルの作成」、「ドメインの作成」、「WebLogic サービスの開始」の 4 つのインストール アクションを定義します。
9. ［+］をクリックして「WebLogic のインストール」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］ドロップダウン リストから［プログラムの実行］を選択します。

b. アクションの説明を入力します。

c. ［プログラム名］フィールドで、以下の実行可能ファイルを選択します。

```
server103_win32.exe
```

d. ［次へ］をクリックします。

e. ［インストール アクション オプションの定義］パネルで、以下の 3 つのオプションを追加します。

```
-mode=silent

-silent_xml=C:¥SA¥Weblogic-10.3¥silent.xml

-log=C:¥CA_SA_Weblogic_silent.log
```

f. ［終了］をクリックします。

アクションが保存されます。

10. ［+］をクリックして「ドメイン用のファイルの作成」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］ドロップダウン リストから［プログラムの実行］を選択します。

b. アクションの説明を入力します。

c. ［プログラム名］フィールドに、実行するバッチ ファイルを入力します。

```
C:¥SA¥Weblogic-10.3¥CreateWeblogicFile.bat
```

d. ［次へ］をクリックします。

e. ［インストール アクション オプションの定義］パネルで、以下のオプションを追加します。

```
-domianname CA_SA_Weblogic
```

このオプションをエンド ユーザで編集可能にします。

f. ［終了］をクリックします。

アクションが保存されます。

11. ［+］をクリックして「ドメインの作成」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］ドロップダウン リストから［プログラムの実行］を選択します。

b. アクションの説明を入力します。

c. ［プログラム名］に、実行するバッチ ファイルを入力します。

```
C:¥bea¥WLS_WLI_WLP_103_silent¥wlserver_10.3¥common¥bin¥wlst.cmd
```

d. ［次へ］をクリックします。

e. ［インストール アクション オプションの定義］パネルで、以下のオプションを追加します。

```
C:¥SA¥Weblogic-10.3¥CreateDomain.py
```

f. ［終了］をクリックします。

アクションが保存されます。

12. ［+］をクリックして「WebLogic サービスの開始」アクションを定義します。

a. ［インストール アクションの選択］パネルで、［アクション］ドロップダウン リストから［プログラムの実行］を選択します。

b. アクションの説明を入力します。

c. ［プログラム名］フィールドに、実行するバッチ ファイルを入力します。

```
C:¥SA¥Weblogic-10.3¥InstallStartWeblogicSvc.bat
```

d. ［次へ］をクリックします。

e. ［インストール アクション オプションの定義］パネルで、プレビューの確認のみを行い、［終了］をクリックします。

アクションが保存されます。

13. ［次へ］をクリックしてから［終了］をクリックします。

WebLogic アプリケーションが保存されます。

WebLogic サービス テンプレートの作成

サービス プロビジョニングは、サービス テンプレートに基づいたサービスの作業インスタンスの作成です。 この手順では、すでに定義したアプリケーションと、サービスをホストするために必要なマシンの数で構成された、WebLogic Server 展開用のサービス テンプレートを作成します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］を右クリックして［新規サービス テンプレート］を選択します。

   ［サービス テンプレートの作成］パネルが表示されます。

2. サービス テンプレートの名前と説明を入力し、サービスをホストするために必要なマシンの数を選択します。 マシンの数は、サーバの予測される負荷によって異なります。

3. ［詳細］をクリックして、マシンの設定を表示します。 すべての値を［自動］に設定されたままにします。 この設定では、プロビジョニング中にテンプレート内のすべてのアプリケーションのサポートされる OS タイプがチェックされ、最も便利な VMware テンプレートが自動的に選択されます。

4. ［サービス情報ファイル］を指定します。 この HTML ファイルは、プロビジョニング プロセスの最後にエンド ユーザに表示され、サービスへのアクセス方法を通知します。

5. ［その他のアプリケーション］チェック ボックスをオンにします。これにより、サービス プロビジョニング中に WebLogic Server にアプリケーションを追加できます。

6. ［+］（新規）をクリックして、WebLogic アプリケーションをサービス テンプレートに追加します。

   ［アプリケーションの選択］パネルに［サービス テンプレート アプリケーションの設定］ウィザードが表示されます。

7. 利用可能な定義済みのアプリケーションのリストから WebLogic を選択し、［次へ］をクリックします。

   ［インストール アクションの設定］パネルが表示されます。ここでは何も変更しないでください。

8. ［次へ］をクリックします。

   ［アプリケーション設定の確認］パネルが表示されます。

9. ［終了］をクリックします。

   ［サービス テンプレートの作成］パネルが、アプリケーションとそれをホストするマシンの詳細で更新されます。

10. ［OK］をクリックします。

    CA Server Automation は、このテンプレートを［エクスプローラ］ツリー内のサービス テンプレートのリストに追加します。 サービス テンプレートが、プロビジョニング用に準備できました。

WebLogic Server の展開

サービス テンプレートを作成すると、エンド ユーザによるワンクリック サービス プロビジョニングが可能になります。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで［オンデマンド サービス］の下にある［サービス テンプレート］を選択します。
2. ［サマリ］タブで、作成された WebLogic サービス テンプレートを選択し、［サービスのプロビジョニング］アイコンをクリックします。
3. プロビジョニングするサービス インスタンスの名前を入力します。
4. WebLogic ドメイン名を指定します。 このユーザ入力は、WebLogic アプリケーションの定義で指定されています。
5. ［その他のアプリケーション］をクリックし、利用可能なアプリケーションから選択してサービス テンプレートで展開します。

   注: 選択できるのは、すでにサービス テンプレート内に存在するアプリケーション（この場合は、WebLogic）に依存しているアプリケーションだけです。 プロビジョニング中に利用可能にするすべてのアプリケーションの前提条件として WebLogic を設定します。

6. ［OK］をクリックします。

   CA Server Automation は要求されたサービス インスタンスをプロビジョニングし、それを［エクスプローラ］ツリーの［オンデマンド リソース］の下のリソースのリストに追加します。 ［ジョブ］ペインでプロビジョニングのステータスを追跡します。

7. プロビジョニングが完了した後、WebLogic Server 管理コンソールへのリンクを含むページが表示されます。プロビジョニングが成功したことを確認するには、このリンクをクリックします。

CA Software Delivery

Software Delivery サービスは、Windows および Linux のオペレーティング システム イメージング、およびアプリケーション パッケージの、UNIX、Linux、Windows 環境への配信の通信を管理します。 Software Delivery サービスは、イメージング サービスからのすべての受信オペレーティング システム リクエストを処理します。

イメージング サービスは、CA Software Delivery サービス（OSIM）を使用して、リモート Windows または Linux サーバ上のイメージング プロセスを開始します。リクエストはその後、イメージングのために Software Delivery サービスに送信され、このサービスによって CA Software Delivery のターゲット サーバでのプロセスが開始されます。

Software Delivery サービスは、OSIM との統合を提供します。このサービスは、サーバで利用可能なイメージに関する OS イメージ情報を CA Software Delivery から取得します。 これらのイメージは、Windows または Linux オペレーティング システムのいずれかです。 Windows イメージは、ゴースト イメージである場合もあります。 その後、表示されたこれらのイメージから選択して、定義したクライアント コンピュータでイメージング ジョブをサブミットできます。

このドキュメントでは、読者が CA Software Delivery（OSIM）ソリューションに精通していることを前提としています。 ソリューションによって課されている要件および制限はすべて、CA Server Automation に有効です。

パッケージングについて

CA Software Delivery サーバに登録されるパッケージは、数百件に上ります。CA Server Automation では、パッケージのサブセットを選択できるため、データ センターに適用されるパッケージを管理できます。 その後、CA Server Automation ユーザ インターフェースからリモート コンピュータにこれらのパッケージを展開したり、ジョブとして展開するスケジュールを立てたりすることができます。

スケジュール立てて複数のパッケージを展開すると、CA Software Delivery ではジョブが 1 つずつ展開されます。 ジョブは両方とも、CA Server Automation ユーザ インターフェースで作成します。 最初のジョブは CA ITCM のインターフェースに送信され、もう一方のジョブはキューに入れられます。 CA ITCM のインターフェースでジョブを表示した場合は、1 つのジョブが表示されます。最初のジョブが完了すると、その後に次のジョブが表示されます。 CA Server Automation インターフェースでジョブを表示する場合は、スケジュールされた複数のジョブを同時に表示できます。

CA Patch Manager

CA Patch Manager は、異種混合環境でソフトウェア パッチを管理します。 CA ITCM と共に CA Patch Manager をインストールすると、CA Server Automation の管理対象サーバにパッチを配信できます。 パッチは、パッチ配信の前提条件に適合していると識別されたコンピュータに配信できます。

CA Server Automation はパッチのステータスをチェックして、そのパッチが承認されているかどうかを確認します。 CA Server Automation でのパッケージ配信のセットアップ時には、パッチが CA ITCM で利用可能かどうかにかかわらず、承認されたパッチのみが、利用可能なパッケージのリストに表示されます。

サーバにパッチを配信するには、サーバに CA IT Asset Manager エージェントがインストールされている必要があります。 このエージェントによって、以下のグループのいずれかにサーバが分類されます。

- パッチが必要なサーバ
- パッチが必要でないサーバ
- パッチ配信の前提条件に適合しないサーバ

CA Patch Manager はこれらのグループを自動的に作成し、更新します。したがって、CA Server Automation では、どのサーバがパッチ展開に利用可能かがわかっています。 エージェントがインストールされていない場合にパッチを提供しようとすると、CA Server Automation はエラー メッセージを返します。 このメッセージは、サーバの状態が不明であり、パッチが提供できないことを通知します。

汎用グループおよびテンプレートの使用

新しいシステムを検出またはプロビジョニングする場合、次の手順は通常、特定のメトリックのモニタし、ルールを適用して、ソフトウェア パッケージを展開することです。 これらの操作は、システムごとに個別に実行するのが普通です。 手順は以下のとおりです。

- 各ソフトウェア パッケージは、1 つずつ展開します。 展開するパッケージがどれか、および各パッケージのインストールの順序を正確に認識します。
- ［メトリック］ページに移動して、モニタするメトリックを選択します。 選択するメトリックはどれかを正確に認識します。
- サーバに適用する正確なルール、ステートメント、およびアクションを手動で定義します。 ルールを作成する方法、どのステートメントをどのように作成するか、および講じる処置を認識します。

特に複数のシステムを設定している場合に、このプロセスは非効率的になることがあります。 CA Server Automation では、汎用的な方法で、ソフトウェア パッケージを 1 つのグループにまとめることができます。 これらのグループを使用すると、サーバまたはサービスにすぐにグループを適用できます。 さらに、異なるエンティティをリンクしてテンプレートを形成することができるため、他のシステムに同じ Software Delivery パッケージを適用できます。

ソフトウェア パッケージをまとめるときは、必ず同じオペレーティング システムのソフトウェア パッケージを使用して、パッケージ グループを作成します。 パッケージ グループは、異なるオペレーティング システム タイプのパッケージを 1 つのパッケージ グループで展開する機能をサポートしていません。 たとえば、1 つのパッケージ グループを作成して Windows XP に展開し、別のパッケージ グループを作成して Linux に展開します。

注: 汎用グループおよびテンプレートの作成については、*オンライン ヘルプ*を参照してください。

Software Delivery 設定ファイル

casdaconf.cfg ファイルは、*Install_Path*¥CA¥*productname*¥conf ディレクトリにあります。 このファイルを編集するには、テキスト エディタを使用します。

設定パラメータには以下が含まれます。

CONFIG_KEY_SDA_LoggerCategory=sdadapter

Software Delivery アダプタのロガー カテゴリを定義します。

CONFIG_KEY_SDA_HTTP_Protocol

Software Delivery アダプタ ホストのプロトコルを定義します。

デフォルト： https

CONFIG_KEY_SDA_Port

Software Delivery アダプタ ホストのリスニング ポートを定義します。

デフォルト： 443

CONFIG_KEY_SDA_PackageList_Sync_Interval

Software Delivery サーバからのパッケージ リストを同期する Software Delivery アダプタの時間間隔を指定します。 Software Delivery アダプタは、Software Delivery サーバ パッケージまたはプロシージャ グループ カタログをポーリングし、このリストを CA Server Automation によってメンテナンスされるリストと同期します。 この属性は、2 つのリストが同期される頻度を設定します。

デフォルト： 43200000

制限： ミリ秒

CONFIG_KEY_SDA_ImageList_Sync_Interval

Software Delivery サーバからの OS イメージ リストを同期する Software Delivery アダプタの時間間隔を指定します。

デフォルト： 600000

制限： ミリ秒

CONFIG_KEY_SDA_Imaging_job_Sync_Interval

Software Delivery サーバからの OSIM イメージング ジョブ ステータスを同期する Software Delivery アダプタの時間間隔を指定します。

デフォルト： 360000

制限： ミリ秒

CONFIG_KEY_SDA_Packaging_job_Sync_Interval

Software Delivery サーバからのソフトウェア パッケージ ジョブ ステータスを同期する Software Delivery アダプタの時間間隔を指定します。

デフォルト： 30000

制限： ミリ秒

CONFIG_KEY_SDA_Sync_Interval

WS タイムアウトを防ぐための時間間隔を指定します。

デフォルト： 300000

制限： ミリ秒

CONFIG_KEY_SDA_CCM_Run_System_Discovery_Profile_Initial_Delay

Software Delivery アダプタによってサブミットされたパッケージ ジョブによって CCA エージェントが正常にインストールされると、ディスカバリ プロファイルが実行されます。 この属性は、CCA エージェントが正常にインストールされたことを Software Delivery アダプタが検出した後、ディスカバリ プロファイルが実行されるまでに経過する秒数を設定します。

デフォルト： 2000

制限： ミリ秒

CONFIG_KEY_SDA_CCM_Run_System_Discovery_Profile_Max_Retry_Times

CA Configuration Automation Web サービスに連絡してエラーが検出されたときに、ディスカバリ プロファイルを実行する再試行の数を指定します。

デフォルト： 5

CONFIG_KEY_SDA_CCM_Run_System_Discovery_Profile_Retry_Time_Interval

試行が失敗したときに処理する実行システム ディスカバリ プロファイルを実行する試行間の間隔を指定します。

デフォルト： 60000

制限： ミリ秒

CONFIG_KEY_SDA_Stage_SD_Agent_Time_Out

スケーラビリティ サーバへの Software Delivery エージェントのステージングのタイムアウト期間を指定します。

デフォルト： 360000

制限： ミリ秒

CONFIG_KEY_SDA_New_Package_Entry_State

Software Delivery アダプタが新しいソフトウェア パッケージの存在を検出した後に CA Server Automation に追加されるそれらのパッケージのデフォルト エントリ状態を指定します。有効な値は、unmanaged または managed です。

デフォルト： unmanaged

CONFIG_KEY_SDA_Agent_Check_Retry_Count

Software Delivery エージェントがインストールされているかどうかを確認するために Common Application Framework（CAF）を使用しているときの再試行の回数を指定します。

デフォルト： 3

CONFIG_KEY_SDA_DSM_URL

パッケージング コンポーネントが CA ITCM Web サービスに接続するために使用する URL を定義します。

例： DSM_URL=http://localhost/UDSM_R11_WebService/mod_gsoap.dll

CONFIG_KEY_SDA_Max_Img_Jobs

同時に実行できるイメージング ジョブ数の最大値を指定します。

デフォルト： 20

CONFIG_KEY_SDA_Img_Job_Rrtry_Delay

イメージング ジョブの再試行時の遅延時間を指定します。

デフォルト： 600000

制限： ミリ秒

CONFIG_KEY_SDA_Img_Job_Max_Retry_Count

失敗したイメージング ジョブを再試行する回数の最大値を指定します。

デフォルト： 3

CONFIG_KEY_SDA_Img_Job_Queue_Sync_Interval

Software Delivery アダプタがイメージング ジョブ キューを更新する時間間隔を指定します。

デフォルト： 120000

制限： ミリ秒

CONFIG_KEY_SDA_CLI_TIMEOUT

dpmsd CLI のデフォルト タイムアウト値を指定します。

デフォルト： 60

制限： 分

CONFIG_KEY_SDA_PROVISIONING_TIMEOUT

OSIM ジョブのデフォルト タイムアウト値を指定します。

デフォルト： 120

制限： 分

CONFIG_KEY_SDA_SCREG_RETRY_MAX_COUNT

CA Server Automation サービス コントローラに Software Delivery サービスを登録する試行の最大数を指定します。

デフォルト： 360

CONFIG_KEY_SDA_Img_Job_Pending_Timeout_Value

OSIM が保留状態であるときのデフォルト タイムアウト値を指定します。

デフォルト： 60

制限： 分

CONFIG_KEY_SDA_Img_Job_Pending_Timeout_Retry_Count

OSIM が保留状態であるときの試行の最大数を指定します。

デフォルト： 3

CONFIG_KEY_SDA_Img_Job_Pending_Timeout_Failout={Yes|No}

OSIM の保留タイムアウト時間が経過した後に OSIM ジョブを停止することを指定します。

デフォルト： No

CONFIG_KEY_SDA_Img_Job_Progress_Timeout_Value

OSIM の進捗状態のデフォルト タイムアウト値（分単位）を指定します。

デフォルト： 120

CONFIG_KEY_SDA_Img_Job_Progress_Timeout_Retry_Count

OSIM が進行中でタイムアウトになった場合の再試行の最大数を指定します。

デフォルト： 2

CONFIG_KEY_SDA_Img_Job_Progress_Timeout_Failout={Yes|No}

OSIM の進捗タイムアウト時間が経過した後に OSIM ジョブが停止するかどうかを指定します。

デフォルト： はい

CONFIG_KEY_SDA_Img_Cancel_Job_In_Progress={Yes|No}

すでに進行中である OSIM ジョブを取り消すことができるかどうかを指定します。

デフォルト： はい

CONFIG_KEY_SDA_ITCM_SESSIONPOOL_SIZE

各 CA ITCM サーバに対する CA ITCM セッション プール内のセッションの最大数。

デフォルト： 10

CONFIG_KEY_SDA_ITCM_RENEW_SESSIONPOOL_INTERVAL

CA ITCM セッション プールの更新間隔（ミリ秒）

デフォルト： 600000

エージェント バージョンの変更

環境内で使用しているエージェントのバージョンは、使用している CA IT Client Manager のバージョンに依存するため、提供されたデフォルトとは異なる場合があります。この状況が発生した場合は、追加の管理エージェントの展開時にエージェントのバージョンを変更します。 このプロセスで、casdaconf.cfg ファイルでリスト表示されたエージェントのバージョンを変更する手順が提供されます。

ファイルを変更して保存した後は、変更を有効にするために Apache HTTP Server を再起動します。

casdaconf.cfg ファイルには、特定のオペレーティング環境のためにインストールするべきパッケージを指示する属性が含まれます。 これらの属性は、追加の管理エージェントを展開するために使用され、その形式は以下のとおりです。

```
AutoDeploy:<platform>:<SD packageinfo>[index]
```

展開する追加の管理エージェントのパッケージ情報を取得する casdaconf.cfg ファイル エントリについての説明が記載されています。

platform

有効な値は、以下の CA IT Client Manager プラットフォームです。

AUTODEPLOY: WINDOWS_X86

AUTODEPLOY: LINUX_X86

AUTODEPLOY: HPUX_HP

AUTODEPLOY: AIX_AIX

AUTODEPLOY: SOLARIS_SPARC

AUTODEPLOY: SOLARIS x86

SD packageinfo

実行するパッケージを識別します。 パッケージを展開すると、以下のエントリがパッケージの説明に使用されます。

SDA_PKG_NAME

パッケージの名前を定義します。

SDA_PKG_VERSION

パッケージのバージョンを定義します。

SDA_PKG_PROCEDURE

インストール パッケージを実行するプロシージャを定義します。

index

最初にインストールするパッケージを決定し、パッケージとプロシージャの情報をグループ化して、インストールするものを識別します。

casdaconf.cfg ファイルで提供されるエージェントのデフォルト エントリです。 環境内で使用されるパッケージのバージョンで動作するように、これらのエントリを変更します。 すべてのエントリのインデックスが正しい場合は、エントリの追加および削除が可能です。インデックスは 1 から開始し、追加のエントリは連続する数字である必要があります。1 を使用した後に 3 を使用することはできません。

例: 自動展開プロファイルを定義して CCA エージェントおよびパフォーマンス エージェントを連続して展開する

この例では、Windows システム上で CCA エージェントを最初に展開して、次にパフォーマンス エージェントを展開する自動展開プロファイルを定義する方法を示します。

- AUTODEPLOY: WINDOWS_X86:SD_PKG_NAME1=CCA Agent Win32
- AUTODEPLOY: WINDOWS_X86:SD_PKG_VERSION1= r5.0
- AUTODEPLOY: WINDOWS_X86:SD_PKG_PROC1= CA_ACM_Windows_Agent_Install_VM
- AUTODEPLOY: WINDOWS_X86:SD_PKG_VERSION2= 12.0
- AUTODEPLOY: WINDOWS_X86:SD_PKG_PROC2=Install

Amazon EC2 プロビジョニング

CA Server Automation を使用して、パブリックまたはプライベート クラウド内で Amazon Elastic Compute Cloud（EC2）インスタンスをプロビジョニングおよび管理できます。

関連項目:

サポートされている機能 (P. 1038)
前提条件 (P. 1039)
Amazon EC2 リソースを設定およびプロビジョニングする方法 (P. 1040)

サポートされている機能

CA Server Automation は、Amazon EC2 オペレーティング環境で以下の機能をサポートします。

完全サポート

- オンデマンド インスタンス
- Amazon Virtual Private Cloud
- 複数の Amazon Web サービス（AWS）アカウント
- 複数の場所（可用性ゾーンおよび地域）

  Amazon のすべての地域がサポートされます。Amazon サイトに新しい地域が追加されると、CA Server Automation ユーザ インターフェースによってそれらが動的にダウンロードされます。 Amazon Machine Image（AMI）とインスタンスをプロビジョニングし、設定された各地域に対して操作を実行できます。

部分的なサポート

- Amazon Elastic Block Storage （EBS）

  EBS インスタンスを停止または再開できます。 EBS インスタンスを停止すると、データと状態が保存され、チャージが回避されます。EBS インスタンスを開始すると、前の状態とデータが回復されます。 実行中または停止中の EBS インスタンスから AMI を作成できます。

- Amazon EC2 インスタンスのタイプ
  - t1.micro
  - m1.small
  - c1.medium
  - m1.large
  - m1.medium
  - m1.xlarge
  - c1.xlarge
  - m2.xlarge
  - m2.2xlarge
  - m2.4xlarge
  - cc1.4xlarge

前提条件

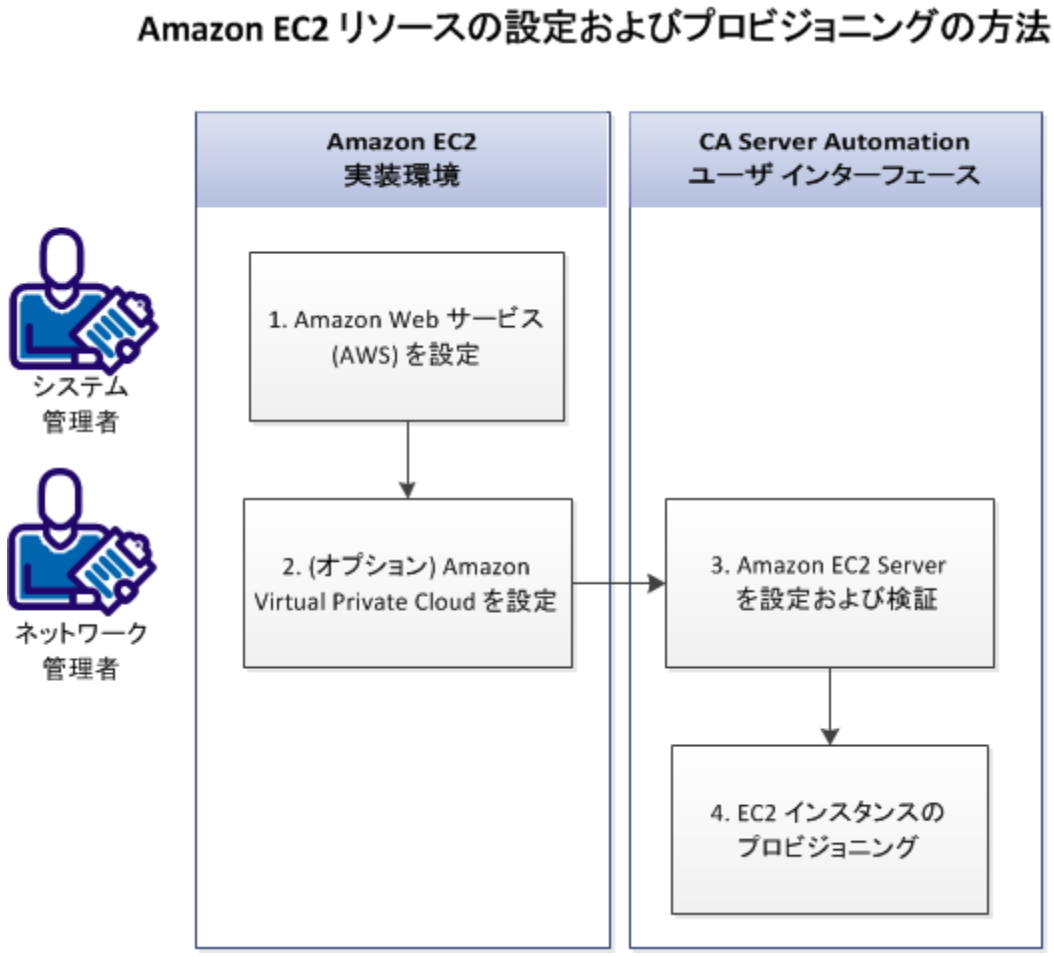
Amazon EC2 を CA Server Automation 用に設定する前に、以下の前提条件を確認してください。

- Amazon EC2 オペレーティング環境に精通していること
- CA Server Automation Amazon EC2 アダプタがインストールされており、CA Server Automation ユーザ インターフェースにアクセスできること
- CA Server Automation ユーザ インターフェースとリソースのプロビジョニング方法の基本を理解していること

Amazon EC2 リソースを設定およびプロビジョニングする方法

システム管理者は、CA Server Automation を使用して Amazon EC2 オペレーティング環境から AMI をプロビジョニングできます。 また、システム管理者は、ネットワーク管理者の支援を受けながら、ユーザに接続して Amazon Virtual Private Cloud （VPC）からのリソースを計算できます。

以下の図は、CA Server Automation で Amazon EC2 リソースを設定及びプロビジョニングするプロセスを示しています。



1. Amazon Web サービス（AWS）の設定（P. 1041）
2. Amazon Virtual Private Cloud の設定（P. 1043）
3. Amazon EC2 サーバの設定と検証（P. 1044）
4. EC2 インスタンスのプロビジョニング（P. 1046）

Amazon Web サービス（AWS）を設定する方法

以下のワークシートを使用して、Amazon EC2 オペレーティング環境の設定を確認します。

Amazon オペレーティング環境でのタスク	特記事項	CA Server Automation ユーザ インターフェースのフィールド
Amazon Web サービス（AWS）アカウントの作成	複数のアカウントがサポートされています。	AWS アカウント ID：
Amazon EC2 サービスへの登録	このサービスには、Amazon Simple Storage Service （パブリック クラウド）および Amazon Virtual Private Cloud（VPC）が含まれています。	
X.509 証明書と秘密鍵の作成	証明書と秘密鍵は、CA Server Automation で Amazon EC2 サーバを設定するときに必要な認証情報です。 この情報は安全な場所に保管し、紛失した場合は新しい証明書を生成してください。	X.509 証明書ファイル フル パス： 秘密鍵ファイル フル パス：
（オプション）プロキシ サーバ情報の収集	プロキシ サーバを使用して、ネットワーク内の Amazon EC2 インスタンスをモニタできます。このサーバはオプションですが、多くの場合、セキュリティを向上させます。	プロキシ サーバ名： ホスト名： ポート： ユーザ名： パスワード：

Amazon Machine Image（AMI）の作成、起動、バンドル、アップロード、および登録	AMI 識別子は、CA Server Automation 内のイメージと同等です。 **セキュリティ グループの作成** セキュリティ グループは、プロビジョニング中に CA Server Automation インターフェースに表示されます。 **キー ペアの作成** CA Server Automation で Amazon AMI を起動するには、指定されたキー ペアが必要です。キー ペアの名前は、インスタンスを起動する Web サービス コールで指定されます。 SSH は、秘密鍵を使用して認証を行います。 キー ペアを作成するには、AWS コンソールまたは ElasticFox Firefox プラグインを使用します。返された秘密鍵は、ファイルシステム上の安全な場所に保存します。 **EBS ボリュームの作成** EBS ボリュームは、同じ可用性ゾーン内の任意のインスタンスに接続できます。 CA Server Automation ユーザ インターフェースでは、EBS ボリュームが 1 つのデバイス タイプとして表示されます。	AMI ID： OS タイプ： キー ペア名： （SSH キー ペア） マニフェスト： インスタンス タイプ： セキュリティ グループ： パブリック 可用性ゾーン： デバイス タイプ： EBS
	地域の決定 地域（米国東部、北ヴァージニアなど）は、個別の地理的な領域に分散して位置します。 CA Server Automation では、動的な更新を使用して Amazon のすべての地域がサポートされます。 可用性ゾーンは、障害を分離するための地域を備えた特定の場所です。インスタンス用のゾーンを指定しない場合は、Amazon が 1 つを選択します。	地域の選択

Amazon Virtual Private Cloud を設定する方法

CA Server Automation では、Amazon Virtual Private Cloud（VPC）にアクセスするために VPN 接続が必要です。 サブネット内に AMI を作成してネットワークを分離できます。

CA Server Automation 用に VPC を実装する場合、ネットワーク管理者は以下のタスクを完了する必要があります。

Amazon オペレーティング環境でのタスク	メモ	CA Server Automation ユーザ インターフェースのフィールド
サブネットおよび IP アドレス範囲の作成	「*Amazon Virtual Private Cloud Network Administration Guide*」を参照してください。	サブネット： サブネット IP アドレス： ドメイン名：
VPN 接続の作成	「*Amazon Virtual Private Cloud Network Administration Guide*」を参照してください。	プライベート： 可用性ゾーン：
CA Server Automation でのゲートウェイ/ルータの設定	AWS サブネットにアクセスするため、CA Server Automation マネージャにゲートウェイ/ルータを設定します。	

Amazon EC2 サーバの設定と検証

Amazon EC2 サーバを CA Server Automation で設定し、利用可能にする必要があります。また、インスタンスをプロビジョニングする前に、CA Server Automation から Amazon のパブリックおよびプライベート クラウドへの接続を検証する必要があります。

以下の手順に従います。

1. 証明書と秘密鍵を CA Server Automation マネージャにコピーします。
2. Amazon EC2 アダプタ サービスがインストールされているサーバで、CA Server Automation ユーザ インターフェースを起動します。
3. ［管理］タブをクリックします。
4. ［設定］パネルの［プロビジョニング］で［EC2 サーバ］を選択します。

5. 実装に必要な以下の情報を入力します。

   - **AWS アカウント ID：** AWS アカウント ID。
     例： 538614568157
   - **X.509 証明書フル パス：** Amazon X.509 証明書ファイル（.pem）。

     例：C:¥ec2_account¥cert-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.pem
   - **秘密鍵ファイル フル パス：** Amazon 秘密鍵ファイル（.pem）。

     例： C:¥ec2_account¥pk-YYYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY.pem
   - **地域の設定：** この EC2 サーバ用に設定した地域。

     例： us-east-1
   - **デフォルトの地域**： プロビジョニングのデフォルトとして表示する地域。

     例： ap-northeast-1
   - **デフォルト アカウント**： アカウントがデフォルトで有効になっているかどうか。

     例： 有効
   - **プロキシ サーバ**： サービス要求の仲介者の役割を果たすサーバ。

     例： yourproxy.com
   - **キー ペアの設定：** ［キー ペアの設定］ダイアログ ボックスを開きます。設定する地域を選択します。ダイアログ ボックス リストに、該当する地域に対するすべての設定済みキー ペアが表示されます。キー ペア情報を格納するには、［OK］をクリックします。

6. CA Server Automation マネージャで、システム クロック アプリケーションにアクセスし、時間をネットワーク タイム プロトコル（NTP）サーバと同期させます。

   注: Amazon EC2 サーバは、セキュリティ上の理由から、外部サーバの時間が自身の時間と一致しない場合、外部サーバによる接続の試行を無効にします。CA Server Automation マネージャの時間を同期させると、次の手順で発生する可能性がある検証エラーを回避できます。

7. ［アクション］メニューで［検証］を選択します。

   CA Server Automation と Amazon パブリックまたはプライベート クラウドの間の接続が検証されます。［接続ステータス］が緑である場合は、EC2 インスタンスのプロビジョニングを開始できます。 検証が失敗した場合は、検証アクションを再試行する前に以下を確認します。

   - AWS アカウント ID が正しいこと
   - 証明書と秘密鍵ファイルが利用可能で、正しい場所にあること
   - CA Server Automation マネージャ サーバのシステム時間が同期していること
   - プロキシ認証情報が正しいこと（ファイアウォール内部で CA Server Automation を実行する場合にのみ適用）

EC2 インスタンスをプロビジョニングする方法

Amazon EC2 インスタンスをプロビジョニングする前に、このインスタンスに対するパスワードの取得に使用するキー ペアが設定済みであることを確認します。 「Amazon EC2 サーバの設定と検証 (P. 1044)」も参照してください。 インスタンスがビルトイン パスワードを使用する場合は、パスワードが「ServerAuto123」に設定されていることを確認します。

次の手順に従ってください:

1. エクスプローラ ツリーで［データ センター］または［Amazon EC2 インスタンス］を右クリックし、［プロビジョニング］-［Amazon EC2 インスタンスのプロビジョニング］を選択します。

   ［Amazon EC2 インスタンスのプロビジョニング］ウィザードが開きます。

2. ウィザードの手順に従って、Amazon EC2 インスタンスをプロビジョニングします。

以下の表に追加情報を示します。

ユーザ インターフェース	問題	解決策
インスタンス タイプ	**SOAP エラー**： 「The requested instance type's architecture (i386) does not match the architecture in the manifest for <*ami_name*> (x86_64).」 小さなインスタンス タイプで 64 ビット イメージを使用しました。	64 ビット イメージ用の大きなインスタンス タイプを作成してください。
	SOAP エラー： 「AMIs with an instance-store root device are not supported for the instance type 't1.micro'.」 非 EBS AMI で t1.micro インスタンス タイプを使用しました。 Amazon では、この設定はサポートされません。	EBS AMI で t1.micro インスタンスを作成してください。

Cisco UCS ブレードへのベア メタル プロビジョニング

Cisco UCS ブレードへのベア メタル プロビジョニングには、CA Server Automation ユーザ インターフェースで以下のいずれかの方法を使用できます。

- Cisco UCS プロビジョニング ウィザード
- Rapid Server Imaging （RSI）プロビジョニング
- CA ITCM

また、以下のコマンドライン プロビジョニング メソッドのいずれかを使用することもできます。

- dpmucs コマンド
- dpmrsi コマンド

以下の情報を考慮して、どの方法を使用するかを決定してください。

- Cisco UCS ブレードのプロビジョニングでは、ブレードの電源サイクルや、ブレードを特定のサービス プロファイルに関連付けるために必要な時間のために、かなりの時間がかかる場合があります。
- RSI または ITCM のプロビジョニング メソッドを使用している場合は、操作を実行する*前に*、ブレードにサービス プロファイルがすでに関連付けられていることを確認する必要があります。
- ITCM 展開の場合は、PXE ブートに使用されるサービス プロファイルから MAC アドレスを取得する必要があります。 プロビジョニング ジョブが CA ITCM にサブミットされた後、CA Server Automation ユーザ インターフェースからブレードの電源サイクル操作を実行する必要があります。
- 物理システムで RSI ベア メタル プロビジョニングを実行する場合は、展開中にターゲット システムをブートする手動操作を回避するために、ネットワークおよびターゲット システムの両方が Wake-On-LAN 用に設定されている必要があります。ネットワーク ルータがサブネット全体にわたって、指示されたブロードキャストを許可するよう設定されていない限り、Wake-On-LAN は、CA Server Automation インスタンスと同じサブネット内にあるシステムに対してのみ動作します。

  注: Cisco UCS プロビジョニングでは、Cisco UCS Manager が電源制御に使用されるため、Wake-On-LAN は必要ありません。

IBM AIX の LPAR プロビジョニング

LPAR プロビジョニングは、IBM PowerVM システム上の論理パーティションを管理するためにイメージング サービスを使用します。Imaging サービスは、LPAR PMM に要求を送信し、PMM は HMC または IVM サーバに接続して、要求されたアクションを実行するためのコマンドを発行します。

CA Server Automation ユーザ インターフェースは、LPAR アダプタがモニタする IBM AIX プロビジョニング ジョブのステータスを表示します。 LPAR を設定して、ステータスをモニタし、イメージを展開します。

このドキュメントでは、読者が LPAR 要件に精通していることを前提としています。NIM によって IBM AIX に課されている要件および制限はすべて、CA Server Automation で有効です。

注: NIM および IBM AIX の詳細については、IBM の Web サイト（http://www.redbooks.ibm.com/）にある IBM Redbooks を参照してください。 IBM Redbooks Web サイトにある「*NIM From A to Z in AIX 5L*」は、役に立つリソースです。

NIM による IBM AIX プロビジョニング

NIM プロビジョニングでは、Network Installation Manager（NIM）を使用して、IBM PowerPC ベースの論理パーティションおよび物理コンピュータに AIX OS イメージング サービスを提供します。 NIM アダプタは NIM マスタ上に存在しており、そこで NIM 環境をセットアップし、メンテナンスします。 NIM マスタ上で実行される OS バージョンは同じ OS バージョン、または NIM クライアントに展開するバージョンより後のバージョンである必要があります。

プロビジョニングできるのは、NIM 環境ですでに定義され、AIX で設定されている IBM システムのみです。OS がインストールされていない物理（ベア メタル）コンピュータはプロビジョニングできません。

CA Server Automation ユーザ インターフェースは、NIM アダプタがモニタする IBM AIX プロビジョニング ジョブのステータスを表示します。NIM を設定して、ステータスをモニタし、イメージを展開します。

このドキュメントでは、読者が NIM に精通していることを前提としています。 NIM によって IBM AIX に課されている要件および制限はすべて、CA Server Automation でも有効です。

注: NIM および IBM AIX の詳細については、IBM の Web サイト（http://www.redbooks.ibm.com/）にある IBM Redbooks を参照してください。 IBM Redbooks Web サイトにある「*NIM From A to Z in AIX 5L*」は、役に立つリソースです。

前提条件

以下のリストには、NIM の環境要件および制限が含まれます。

- 各 NIM マスタ サーバには、NIM アダプタがインストールされている必要があります。
- 代替 NIM マスタはサポートされていません。
- NIM マスタ サーバは、ssh を使用してログオン可能である必要があります。
- NIM クライアントは、1 つの NIM マスタにのみ登録できます。
- NIM クライアントは NIM マスタに登録する必要があります。
- NIM クライアントは TCP/IP で設定する必要があります。
- NIM クライアントは最初に、NIM マスタとの rsh （非セキュア）または nimsh （セキュア）コミュニケーションが許可されるように設定する必要があります。
- NIM マシン リソースが nimsh プロトコルを定義する場合、nimsh クライアントがクライアント コンピュータ上で実行されている必要があります。
- イメージング ジョブはすべて、オプション「Remain NIM client after install」セットで実行されます。これにより、NIM クライアントは、追加の設定なしで再イメージングできます。
- NIM クライアントは、TFTP ネットワーク制限により、NIM マスタと同じサブネット上にある必要があります。
- NIM クライアントは、NIM マスタが NIM コマンド ライン インターフェースを使用してイメージング可能である必要があります。
- NIM マスタは、その NIM クライアントのホスト名すべてを修飾できるように設定する必要があります。

- 新しい LPAR または選択された LPAR をプロビジョニングするときに、NIM アダプタは、NIM システム MAC アドレスを LPAR 仮想イーサネット アダプタ MAC アドレスに更新します。

リソース グループを使用した IBM AIX クライアント システムの追加

CA Server Automation は NIM と統合されているため、リソース グループを使用して、IBM AIX オペレーティング システムを備えたクライアント コンピュータをイメージングできます。

リソース グループを使用して AIX クライアント システムを追加する方法

1. IBM PowerVM リソースを右クリックし、［プロビジョニング］-［NIM のプロビジョニング］を選択します。

   ［NIM で AIX をプロビジョニング］ダイアログ ボックスが表示されます。

2. 以下のフィールドを指定します。

   NIM マスタ

   NIM 環境をセットアップしてメンテナンスするコンピュータを定義します。NIM 環境は、コンピュータの論理的なグループです。複数の NIM 環境が同じ TCP/IP ネットワーク上にある場合がありますが、アクティブな NIM マスタは環境ごとに 1 つのみです。

   マシン リソース名

   NIM インストールおよび更新操作のターゲット コンピュータの名前を定義します。

3. ［リソース タイプ］メニューで［リソース グループ］を選択し、ドロップダウン リストからリソース グループを選択します。

   注: ［リソース グループ］を選択した場合は、個別の［リソース］フィールドが表示されません。

4. 残りのフィールドに入力し、［コンピュータの追加］をクリックします。

   リソース グループ

   NIM クライアントへのリソースを、個々に関連付けるより迅速に割り当てるために使用するリソースの論理グループを定義します。

ユーザ名

エージェント展開に使用されるルート ユーザを定義します。

パスワード

エージェント展開に使用されるルート ユーザのパスワードを定義します。

論理パーティションを使用

選択すると、物理システムではなく、イメージするシステムとして IBM LPAR を指定します。 このシステムでは、イメージング時にオペレーティング システムが実行中である必要はありません。

HMC/IVM 名

1 つ以上の管理対象サーバを管理する HMC または IVM を定義します。

システム名

HMC または IVM サーバで割り当てられた管理対象システムの名前。このシステムは、LPAR をホストしており、SCSI およびイーサネット アダプタなどのリソースを LPAR が使用できるように仮想化された物理ハードウェアを含んでいます。

パーティション名

イメージするターゲット システムとして使用される既存の LPAR を定義します。

プロファイル名

（HMS のみ）選択した LPAR を初期化する方法に関する情報を含む既存のパーティション プロファイルを定義します。

テンプレート

すでに作成済みでテンプレートとして使用可能なソフトウェア パッケージ グループのリストを表示します。

ドメイン マネージャ

操作が実行されるドメイン マネージャの名前を定義します。 この名前は、Software Delivery アダプタまたは CA ITCM ドメイン マネージャが 1 つしか設定されていない場合はオプションです。 このパラメータは、CA Server Automation に対してのみ有効です。

スケーラビリティ サーバ

エージェントのプライマリ インターフェースとして機能し、複数のホストに CA ITCM の負荷を分散します。 CA Software Delivery は、ソフトウェア配信用の複数のスケーラビリティ サーバをサポートします。

イメージング プロセスがクライアント コンピュータ上で開始され、イメージング ジョブが正常に完了すると、確認メッセージによって通知されます。イメージング プロセスが完了すると、コンピュータは正しく検出、分類されます。

個別リソースを使用した IBM AIX システムの追加

CA Server Automation は NIM と統合されているため、個別リソースを使用して、IBM AIX オペレーティング システムを備えたクライアント コンピュータをイメージングできます。

個別のリソースを使用して AIX クライアント コンピュータを作成する方法

1. IBM PowerVM リソースを右クリックし、［プロビジョニング］-［NIM のプロビジョニング］を選択します。
2. 以下のフィールドを指定します。

   NIM マスタ

   NIM 環境をセットアップしてメンテナンスするコンピュータを定義します。NIM 環境は、コンピュータの論理的なグループです。複数の NIM 環境が同じ TCP/IP ネットワーク上にある場合がありますが、アクティブな NIM マスタは環境ごとに 1 つのみです。

   マシン リソース名

   NIM インストールおよび更新操作のターゲット コンピュータの名前を定義します。

3. ［リソース タイプ］メニューで［個別リソース］を選択し、残りのフィールドに入力して、［コンピュータの追加］をクリックします。

   MKSYSB イメージ

   （MKSYSB インストール タイプに必須）クローン作成用の MYSYSB イメージを指定します。

ベース オペレーティング システム インスタンス

ベース オペレーティング システム（BOS）のインストール用の情報を含むファイルを指定します。

ライセンス プログラム製品

イメージング リクエストに使用するライセンス プログラム製品ファイルを定義します。

共有製品オブジェクト ツリー

イメージング リクエストに使用する共有製品オブジェクト ツリーを定義します。

解決設定

（オプション）ローカル解決ルーチン用のドメイン名プロトコル名前サーバ情報を定義する有効な */etc/resolv.conf* エントリを含むファイルを定義します。

初回ブート スクリプト

（オプション）BOS インストール処理の完了後の初回の NIM クライアント起動時に、デバイスの設定に使用するファイルの名前を定義します。

インストール後のスクリプト

（オプション）インストール後に実行するスクリプトのリストを定義します。

ユーザ名

エージェント展開に使用されるルート ユーザを定義します。

パスワード

エージェント展開に使用されるルート ユーザのパスワードを定義します。

論理パーティションを使用

選択すると、物理システムではなく、イメージするシステムとして IBM LPAR を指定します。 このシステムでは、イメージング時にオペレーティング システムが実行中である必要はありません。

HMC/IVM 名

1 つ以上の管理対象サーバを管理する HMC または IVM を定義します。

システム名

HMC または IVM サーバで割り当てられた管理対象システムの名前。このシステムは、LPAR をホストしており、SCSI およびイーサネット アダプタなどのリソースを LPAR が使用できるように仮想化された物理ハードウェアを含んでいます。

パーティション名

イメージするターゲット システムとして使用される既存の LPAR を定義します。

プロファイル名

（HMS のみ）選択した LPAR を初期化する方法に関する情報を含む既存のパーティション プロファイルを定義します。

テンプレート

すでに作成済みでテンプレートとして使用可能なソフトウェア パッケージ グループのリストを表示します。

ドメイン マネージャ

操作が実行される CA ITCM ドメイン マネージャの名前を定義します。 これは、SD アダプタまたは CA ITCM ドメイン マネージャが 1 つしか設定されていない場合はオプションです。 このパラメータは、CA Server Automation に対してのみ有効です。

スケーラビリティ サーバ

エージェントのプライマリ インターフェースとして機能し、複数のホストに CA ITCM の負荷を分散します。 CA Software Delivery は、ソフトウェア配信用の複数のスケーラビリティ サーバをサポートします。

クライアント コンピュータでイメージング プロセスが開始され、イメージング ジョブが正常に完了すると、それを通知する確認メッセージが表示されます。イメージング プロセスが完了すると、コンピュータが検出されて分類されます。

MKSYSB ユーティリティの使用

関連項目:

前提条件に関する知識 (P. 1056)
MKSYSB を使用して IBM AIX イメージをプロビジョニングする方法 (P. 1056)

前提条件に関する知識

CA Server Automation を使用して MKSYSB イメージを展開する前に、以下の情報を認識していることを確認してください。

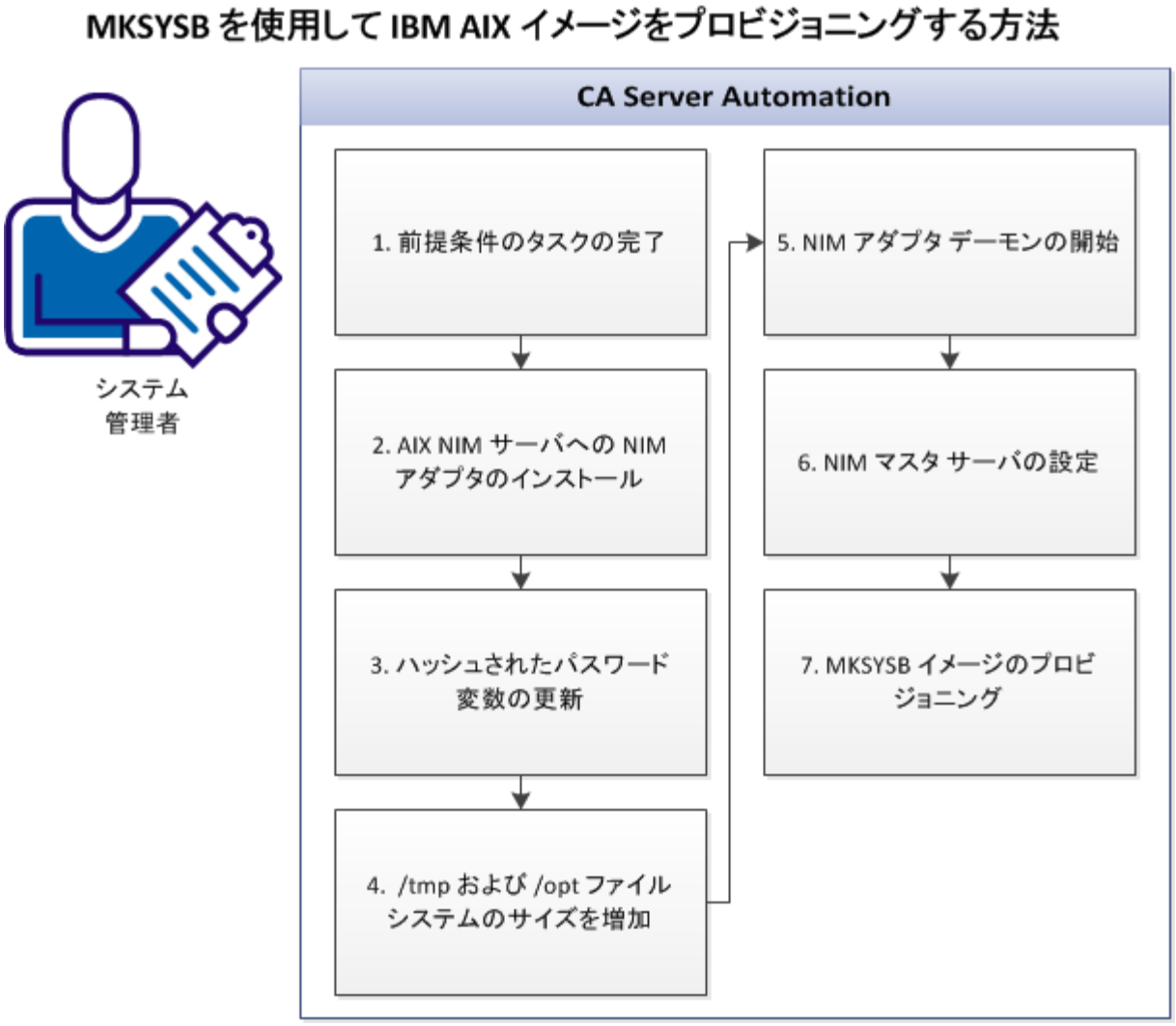
- IBM PowerVM および LPAR オペレーティング環境（NIM MKSYSB ユーティリティを含む）に精通していること。
- CA Server Automation ユーザ インターフェースとリソースのプロビジョニング方法の基本を理解していること。

MKSYSB を使用して IBM AIX イメージをプロビジョニングする方法

システム管理者は、MKSYSB ユーティリティを使用して、CA Server Automation で IBM AIX システム イメージをプロビジョニングします。

IBM AIX イメージは、仮想マシン（LPAR）、またはすでに AIX オペレーティング システムを実行している物理 IBM コンピュータにプロビジョニングできます。 IBM NIM MKSYSB ユーティリティを使用すると、オペレーティング システムと追加ソフトウェアの両方を含む IBM AIX イメージを 1 回の操作でプロビジョニングできます。 このプロビジョニング方法は、デフォルトの実行時の処理より高速で効率的ですが、MKSYSB イメージまたはリソースを使用可能な状態に準備しておく必要があります。

以下のフローチャートは、IBM AIX システム イメージを展開するために必要な一連の手順を示しています。



MKSYSB を使用して IBM AIX イメージをプロビジョニングするには、以下のタスクを実行します。

1. 前提条件のタスクの完了 (P. 1058)
2. AIX NIM サーバへの NIM アダプタのインストール (P. 1059)
3. ハッシュされたパスワード変数の更新 (P. 1059)
4. /tmp および /opt ファイルシステムのサイズを増やします。 (P. 1060)
5. NIM アダプタ デーモンの開始 (P. 1061)
6. NIM Master サーバの設定 (P. 1062)
7. MKSYSB イメージのプロビジョニング (P. 1062)

前提条件のタスクの完了

CA Server Automation を使用して MKSYSB イメージを展開する前に、以下の前提条件を確認してください。

- 準備された MKSYSB イメージまたは NIM MKSYSB リソースを取得していること。
- イメージングにどのリソースと IBM サーバを使用するかを決定していること。
- CA Server Automation と IBM PowerVM および NIM サーバに対する管理者の認証情報を持っていること。
- CA Server Automation ユーザ インターフェースにアクセスできる。

AIX NIM サーバへの NIM アダプタのインストール

NIM アダプタは、グラフィカル インターフェースまたはコマンドライン テキスト コンソールを使用してインストールできます。

次の手順に従ってください:

1. コンピュータにインストール メディアを挿入し、DVD2¥Installers¥AIX_aix¥NIM ディレクトリに移動し、AIX NIM サーバに ca-nim-adapter.AIX をコピーします。
2. AIX NIM サーバに以下のコマンドを入力します。

   ```
   ./ca-nim-adapter.AIX
   ```

   XWindows および DISPLAY が AIX UNIX 端末が開いているコンピュータに設定されている場合、グラフィカル インターフェース インストーラが起動します。それ以外の場合は、コマンドライン インターフェース インストーラが起動します。
3. ［次へ］をクリックします。

   ［使用許諾契約］ページが表示されます。
4. 使用許諾契約を読み、［同意します］をクリックします。

   ［インストール ディレクトリ］ オプションが表示されます。
5. インストールするディレクトリを指定し、[次へ]をクリックします。
6. インストール パスを確認し、［製品をインストール］をクリックします。

   インストールが完了し、［サマリ］ページが表示されます。
7. ［OK］をクリックして、インストーラを終了します。

ハッシュされたパスワード変数の更新

NIM クライアントがイメージングされると、IBM AIX インストーラは空の root パスワードを作成します。 root パスワードを指定するには、ca_post_install.sh スクリプト ファイルを更新します。ハッシュ されたパスワード（DES 形式）を設定し、NIM クライアントが使用する HASH_PASSWORD 変数を更新します。

注: ca_post_install.sh スクリプト ファイルには、**管理者**のプレーン テキストの値に変換するデフォルトのハッシュ パスワードが含まれています。

次の手順に従ってください:

1. NIM クライアントを設定するパスワードで設定されているシステムにアクセスします。
2. /etc/security ディレクトリに移動し、passwd ファイルを開きます。

   passwd ファイル内のハッシュされたルート パスワード エントリは以下のようになります。

   ```
   root:
       password = YmB7AkapuLf8/s
   ```

3. ハッシュされたルート パスワードをコピーし、*install_path*/imaging/etc ディレクトリに移動して、ca_post_install.sh スクリプト ファイルを開きます。
4. ca_post_install.sh スクリプト ファイル内の HASH_PASSWORD 変数にパスワードを貼り付けます。
5. ファイルを保存して、終了します。

/tmp および /opt ファイル システムのサイズを増やします。

デフォルトのファイル システム サイズは、必ずしも IBM イメージ プロビジョニング用に十分な大きさがあるとは限りません。 /tmp または /opt ファイル システム内のスペースが不足していると、NIM クライアントへのエージェントの展開が失敗する場合があります。 選択されたデフォルト値が、インストールするエージェントに対して小さすぎる場合は、少なくとも 400 MB （/tmp の場合）および 700 MB （/opt の場合）に増やしてください。 ファイル システムのサイズを増やす NIM スクリプトがない場合は、ca_post_install.sh スクリプトの chfs コマンドのコメントを外します。 chfs コマンドを使用すると、NIM クライアントのイメージングの後にこのスクリプトを NIM スクリプト リソースとして使用することにより、NIM アダプタがファイル システム サイズを増やすことができます。

注: これらの行は、スクリプトでまだ使用されていない場合にのみ有効にしてください。

次の手順に従ってください:

1. *install_path*/imaging/etc ディレクトリに移動し、ca_post_install.sh スクリプト ファイルを開きます。

2. 先頭の # 文字を削除することによりスクリプト内の両方の chfs コマンドのコメントを外します。

   コメントされた行は以下の例のように表示されます。

   ```
   #chfs -a size=$OPTFSSIZE /opt
   ```

   コメントを外された行は以下の例のように表示されます。

   ```
   chfs -a size=$OPTFSSIZE /opt
   ```

   注: オプションで、OPTFSSIZE 変数と TMPFSSIZE 変数をデフォルトより大きい値に変更してください。デフォルトより小さい値には設定しないでください。

3. ファイルを保存して、終了します。

NIM アダプタ デーモンの開始または停止

NIM アダプタ デーモンは、インストール後またはシステムのブート時に自動的に開始されます。

NIM アダプタ デーモンを手動で開始するには、以下のコマンドを実行します。

```
install-path/imaging/bin/canimstart.sh start
```

NIM アダプタ デーモンを手動で停止するには、以下のコマンドを実行します。

```
install-path/imaging/bin/canimstart.sh stop
```

NIM Master サーバの設定

CA Server Automation のインストール後に NIM マスタ サーバを設定できます。 NIM マスタ サーバは、MKSYSB リソースを提供します。

次の手順に従ってください:

1. CA Server Automation ユーザ インターフェースにログインし、［管理］をクリックします。
2. ［設定］をクリックし、［設定］ページの左ペインで［NIM マスタ］をクリックします。

   ［NIM マスタ］ページが表示されます。
3. +（追加する）をクリックします。
4. NIM 管理者の認証情報を入力して［OK］をクリックします。
5. ［検証］をクリックして接続ステータスを確認します。

IBM AIX イメージのプロビジョニング

IBM NIM 環境を MKSYSB リソースを使用して設定するときは、IBM AIX イメージをプロビジョニングするために CA Server Automation ユーザ インターフェースを使用します。

次の手順に従ってください:

注: CA Server Automation ユーザ インターフェースに管理者としてログインしていることを確認します。

1. ［リソース］をクリックし、［エクスプローラ］ペインを開きます。
2. IBM PowerVM リソースを右クリックし、［プロビジョニング］-［NIM のプロビジョニング］を選択します。

   ［NIM で AIX をプロビジョニング］ダイアログ ボックスが表示されます。

3. 以下のフィールドを指定します。

   NIM マスタ

   NIM 環境を設定するコンピュータを指定します。 環境内に配置できるアクティブな NIM マスタ サーバは 1 つのみです。

   マシン リソース名

   NIM のインストールおよび更新操作のターゲット コンピュータを指定します。

4. ［インストール タイプ］ドロップダウンで、［mksysb］を選択します。
5. ［リソース タイプ］ドロップダウンで、［リソース グループ］を選択します。
6. MKSYSB リソース グループを選択します。
7. ［システム属性］ペインで、ホスト NIM システムにログインするために管理者の認証情報を提供します。

   注: 管理者のユーザ ID とパスワードは、IBM AIX イメージング設定時に *install_path*/imaging/etc/ca_post_install.sh スクリプトで指定したものと一致する必要があります。

8. ［コンピュータの追加］をクリックします。

新規 IBM AIX システム イメージが作成され、使用する準備ができています。MKSYSB リソース グループをすでに利用可能にしておくことで、プロビジョニングで複数ステップのビルド プロセスを実施する必要はなくなりました。

Rapid Server Imaging

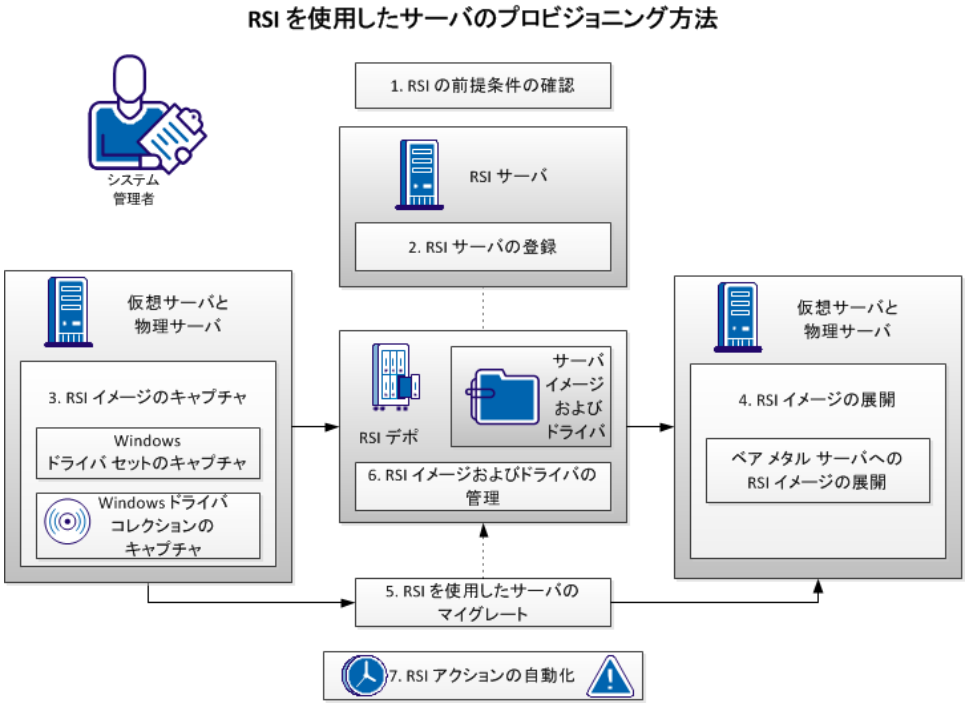
*システム管理者*は、CA Server Automation を使用して、物理および仮想サーバ環境を管理およびプロビジョニングします。 サーバ環境にまたがるプロビジョニング、バックアップ、惨事復旧、およびマイグレーションのためのサーバ イメージを提供するには、信頼性に優れたイメージング メカニズムが必要です。

Rapid Server Imaging（RSI）は、クロスプラットフォームおよび異種混合のハードウェア プロビジョニング、物理および仮想サーバ マイグレーション、惨事復旧、およびイメージのキャプチャと展開を実行するために使用します。 ハードウェアが同じプロセッサ ファミリに属している場合は、複数の動作環境を備えた異なるハードウェアにわたってイメージを展開できます。

管理対象のサーバでイメージをキャプチャして、別の管理対象サーバまたはベア メタル システムに、キャプチャしたイメージを展開できます。 物理から物理、物理から仮想、仮想から物理、仮想から仮想の各システム間でイメージをキャプチャして展開したり、直接マイグレートしたりすることができます。 ベア メタル プロビジョニングの場合を除き、CA Server Automation 管理対象サーバでは RSI エージェントを実行する必要があります。

注: RSI のインストールおよび設定の詳細については、CA Server Automation マニュアル選択メニューにある RSI ドキュメントを参照してください。

以下の図は、CA Server Automation の RSI 機能の概要を示しています。



1. RSI の前提条件 (P. 1066) の確認
   - Hyper-V に対する RSI の前提条件 (P. 1068)
2. RSI サーバの登録 (P. 1068)
3. RSI イメージのキャプチャ (P. 1069)
   - Windows ドライバ セットのキャプチャ (P. 1070)
   - Windows ドライバ コレクションのキャプチャ (P. 1071)
4. RSI イメージの展開 (P. 1072)
   - ベア メタル サーバへの RSI イメージの展開 (P. 1073)
5. RSI を使用したサーバのマイグレート (P. 1074)
6. RSI イメージおよびドライバの管理 (P. 1077)
7. RSI アクションの自動化 (P. 1077)

以下の特定のビジネス目標をサポートするには、RSI 機能をその他の CA Server Automation 機能と組み合わせます。

- ITCM を使用して RSI を展開する方法 (P. 1078)
- RSI を使用してバックアップおよびリストアする方法 (P. 1087)
- RSI を使用して惨事復旧を実行する方法 (P. 1089)

RSI の前提条件

CA Server Automation に RSI サーバを登録して RSI 機能を使用できるようにするには、その前に RSI 環境を設定します。

次の手順に従ってください:

1. RSI サーバをインストールします。

   注: RSI サーバのインストールの詳細については、「*RSI サーバ インストール ガイド*」を参照してください。

2. RSI サーバを設定します。

   注: RSI サーバの設定の詳細については、「*RSI サーバ管理ガイド*」を参照してください。

3. ハイパーバイザを設定します。

   注: ハイパーバイザの設定の詳細については、「*RSI サーバ管理ガイド*」を参照してください。

4. （オプション）RSI ネットワーク環境の外部で追加のサーバを管理する場合は、外部ネットワークを設定します。

   注: 外部ネットワークの設定の詳細については、「*RSI サーバ管理ガイド*」を参照してください。

   注: どんな外部ネットワークも RSI 環境で利用可能にすることができます。

   a. RSI エージェント リモート接続に対して RSI サーバ上でポートを開きます。

      例： 4105

   b. 必要な場合は、ファイアウォール ルールを更新して新しいポート上のトラフィックを許可し、NAT ルールを更新して RSI サーバへのリダイレクトを許可します。

      例： https://RSIserver:443

   c. ターゲット サーバに RSI エージェントをインストールします。

   d. 適切な RSI URL でターゲット サーバ上の dpad.ini ファイルを編集します。

      例： https://RSIserver:4105

   e. RSI エージェントを再起動します。

注: CA Server Automation は、代替の RSI 展開方法をサポートします。 詳細については、「ITCM を使用して RSI を展開する方法 (P. 1078)」を参照してください。

Hyper-V に対する RSI の前提条件

サポートされている任意のオペレーティング システム上で、Microsoft Hyper-V/RSI 環境内の仮想マシンを使用する場合は、以下の前提条件を確認します。

- 各 VM には、DynaCenter ブート ネットワークの 1 つに接続された、少なくとも 1 つのレガシー ネットワーク アダプタが必要です。 レガシー ネットワーク アダプタは、1 つのみ使用することを推奨します。複数のアダプタを使用する場合は、最初のアダプタが DynaCenter ブート ネットワークに接続されていることを確認します。
- Hyper-V ツールは、Windows Server 2003 の 64 ビット エディション上のレガシー ネットワーク アダプタをサポートしていないため、DynaCenter は、このオペレーティング システムをサポートしていません。

  注: サポートされるオペレーティング システムの完全なリストについては、「*RSI サーバ インストール ガイド*」のサポート マトリックスを参照してください。
- 各 VM には、1 つ以上の準仮想化されたネットワーク アダプタ（VM への展開時に OS によって使用される）が存在する必要があります。

RSI サーバの登録

CA Server Automation によって管理された環境にまたがって RSI 機能を有効にするには、RSI サーバとオプションの環境設定を登録します。

次の手順に従ってください:

1. ［管理］をクリックし、左の［設定］パネルで［プロビジョニング］を見つけて［Rapid Server Imaging］をクリックします。
2. ［RSI サーバ］パネルで、［+］（追加）アイコンをクリックし、RSI サーバを追加して、接続ステータスが緑色であることを確認します。
3. （オプション）仮想マシンを使用する場合は、［Rapid Server Imaging 登録済みハイパーバイザ］パネルで［+］（追加）アイコンをクリックし、ハイパーバイザを追加します。

   注: ハイパーバイザの認証情報が検証されます。

4. （オプション）デフォルトの RSI ネットワークを使用しない場合は、［Rapid Server Imaging 登録済みネットワーク］パネルで［+］（追加）をクリックしてブートおよび外部ネットワークを追加します。

   注: ネットワークは検証されません。

5. （オプション）デフォルトの RSI デポを使用しない場合は、［RSI デポ］パネルで［+］（追加）をクリックして、キャプチャされたイメージを保存するためのデポを追加します。

CA Server Automation が RSI サーバに接続し、サーバ環境にまたがって RSI 機能を有効にします。

RSI イメージのキャプチャ

CA Server Automation が RSI サーバに統合されている場合は、後で展開するために物理および仮想サーバの RSI イメージをキャプチャできます。新しい物理または仮想サーバをプロビジョニングするために格納されたイメージを、サーバのリストアまたは惨事復旧のためのバックアップ イメージとして使用します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリー内でキャプチャするマシンを右クリックて、［プロビジョニング］-［イメージのキャプチャ］を選択します。
2. 使用する［RSI サーバ］および［デポ］を選択し、［イメージ名］を設定します。
3. キャプチャするマシンの［ターゲット MAC］と［OS タイプ］を指定します。
4. （オプション）イメージの［説明］と、キャプチャ パラメータを含む外部ファイルの［プロファイル URL］を設定します。
5. （オプション）イメージから除外する［ファイル システム］を指定します。
6. （オプション）実行中のサーバのオンライン キャプチャを実行するには、［ライブ キャプチャ］を選択します。まずサーバをシャットダウンし、再起動の後にイメージをキャプチャするには、［ライブ キャプチャ］を無効にします。

7. （オプション）複数のネットワークが登録され、［ライブ キャプチャ］が無効になっている場合は、キャプチャに使用するネットワークを選択します。
8. ［OK］をクリックします。

   パネルは、ターゲット マシンからイメージをキャプチャし、それを選択されたデポに格納する要求をサブミットします。展開の進行状況を［ジョブ］ペインで追跡します。

重要: Windows イメージの場合は、そのイメージの正常な展開に必要なドライバをキャプチャするようにしてください。

Windows ドライバ セットのキャプチャ

Windows 上で RSI イメージを正常に展開するには、多くの場合、そのイメージ内のソフトウェアに関連付けられたドライバを展開することが必要です。RSI が正常にインストールおよび設定された後、RSI イメージを使用した展開のために、CA Server Automation を使用してターゲット サーバからドライバ セットをキャプチャします。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーの［データ センター］を右クリックして、［管理］-［RSI リソース］を選択します。

   ［RSI リソース］ パネルが表示されます。
2. ［ドライバ セット］タブを選択します。

   ［ドライバ セット］リストは、現在キャプチャされているドライバ セットを表示します。
3. ツールバーで［+］（［ドライバ セットのキャプチャ］）をクリックします。
4. キャプチャ元の［ターゲット サーバ］と［ドライバ セット名］を入力します。
5. キャプチャ元のマシンの［ターゲット MAC］と使用する［RSI サーバ］を指定します。
6. （オプション）ドライバ セットの［説明］を指定します。
7. （オプション）複数のネットワークが登録されている場合は、キャプチャに使用するネットワークを選択します。

8. ［OK］をクリックします。

   ダイアログ ボックスから、ターゲット サーバからドライバ セットをキャプチャする要求がサブミットされます。 キャプチャの進行状況を［ジョブ］ペインで追跡します。

Windows ドライバ コレクションのキャプチャ

Windows 上で RSI イメージを正常に展開するには、多くの場合、そのイメージ内のソフトウェアに関連付けられたドライバを展開することが必要です。RSI が正常にインストールおよび設定された後、RSI イメージを使用した展開のために、CA Server Automation を使用してドライバ メディアから直接ドライバ コレクションをキャプチャします。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーの［データ センター］を右クリックして、［管理］-［RSI リソース］を選択します。

   ［RSI リソース］ パネルが表示されます。

2. ［ドライバ コレクション］タブを選択します。

   ［ドライバ コレクション］リストに、現在の一連のキャプチャされたドライバ コレクションが表示されます。

3. ツールバーの［+］（［ドライバ インポートの収集］）をクリックします。

   ［ドライバ インポートの収集］ダイアログ ボックスが開きます。

4. キャプチャ元のメディア、ドライバ コレクションの説明、ソースおよびベンダー ID を入力して［OK］をクリックします。

   ダイアログ ボックスから、ターゲット メディアからドライバ コレクションをキャプチャする要求がサブミットされます。 キャプチャの進行状況を［ジョブ］ペインで追跡します。

RSI イメージの展開

RSI がインストールおよび設定された後、以前にキャプチャされた RSI イメージを物理サーバおよび仮想マシンに展開できます。

注: この手順は、オペレーティング システムと RSI エージェントがすでにセットアップされているサーバまたは仮想マシンへの基本的な RSI イメージ展開です。 より複雑なイメージ展開については、「ベア メタル サーバへの RSI イメージの展開 (P. 1073)」を参照してください。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリー内で展開先のマシンを右クリックて、［プロビジョニング］-［イメージの展開］を選択します。

   ［イメージの展開］ウィザードが開きます。

2. 使用する［RSI サーバ］と［デポ］を選択し、展開する［イメージ］を選択します。

3. （オプション）複数のネットワークが登録されている場合は、展開に使用するネットワークを選択します。

4. イメージをホストするマシンの［ターゲット MAC］を入力します。

5. （オプション）データを含むイメージの一部のみを展開するには［スケール］を選択し、展開パラメータを含む外部ファイルの［プロファイル URL］を設定します。

6. （Windows のみ）展開する［ドライバ セット］を選択します。

   注: Windows イメージが正常に展開された後、Windows は chkdsk を実行します。 ターゲット システムは自動的に再起動し、Windows は PnP（プラグアンドプレイ）を実行してドライバをインストールします。

7. （オプション）イメージをホストしているマシンに適用する［ホスト名］を指定し、使用する［ネットワーク インターフェース］を選択します。

   注: ホスト名の設定は、イメージまたはプロファイル内のホスト名より優先されます。

8. ［OK］をクリックします。

   ウィザードから、ターゲット マシンにイメージを展開する要求がサブミットされます。 展開の進行状況を［ジョブ］ペインで追跡します。

ベア メタル サーバへの RSI イメージの展開

RSI を使用すると、オペレーティング システムと RSI エージェントを含む完全なイメージを、現在ソフトウェアが含まれていない物理サーバまたは仮想マシンに展開できます。 ベア メタル展開を使用すると、環境に物理サーバ（UCS ブレードなど）を追加するか、または新しい仮想マシンを追加した後、それをすべてのソフトウェア要件を含む完全なイメージでプロビジョニングできます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーで展開先のマシンまたは環境を右クリックして、［プロビジョニング］-［新しい Windows/Linux システム (RSI) の追加］を選択します。

   ［ベア メタルの追加］ウィザードが表示されます。

2. 使用する［RSI サーバ］と［デポ］を選択し、展開する［イメージ］を選択します。
3. （オプション）複数のネットワークが登録されている場合は、展開に使用するネットワークを選択します。
4. ［マシン タイプ］を指定します。
   - ［物理マシン］の［ターゲット MAC］を指定します。
   - ［仮想マシン］の［ハイパーバイザ］と［ターゲット サーバ ID］を指定します。
5. （オプション）データを含むイメージの一部のみを展開するには［スケール］を選択し、展開パラメータを含む外部ファイルの［プロファイル URL］を設定します。
6. （Windows のみ）展開する［ドライバ セット］を選択します。

   注: Windows イメージが正常に展開された後、Windows は chkdsk を実行します。 ターゲット システムは自動的に再起動し、Windows は PnP（プラグアンドプレイ）を実行してドライバをインストールします。

7. （オプション）イメージをホストしているマシンに適用する［ホスト名］を指定し、使用する［ネットワーク インターフェース］を選択します。

   注: ホスト名の設定は、イメージまたはプロファイル内のホスト名より優先されます。

8. ［OK］をクリックします。

   ウィザードから、ターゲット マシンにイメージを展開する要求がサブミットされます。 展開の進行状況を［ジョブ］ペインで追跡します。

RSI を使用したサーバのマイグレート

CA Server Automation が RSI サーバに統合されている場合、サーバ イメージを物理または仮想マシンから別の物理または仮想マシンに直接マイグレートできます。 オプションで、サーバをベア メタル サーバまたは仮想マシンの新しいインスタンスにマイグレートできます。

重要: Windows イメージをマイグレートする前に、そのイメージの正常な展開に必要なドライバをキャプチャするようにしてください。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーでキャプチャするマシンを右クリックして、［プロビジョニング］-［RSI マイグレーション］を選択します。

   ［マイグレート元］パネルに［マイグレーションの実行］ウィザードが表示されます。

2. 使用する［RSI サーバ］および［デポ］を選択し、オプションで［イメージ名］を編集します。

3. キャプチャするマシンの［ターゲット MAC］と［OS タイプ］を指定します。

4. （オプション）イメージの［説明］と、キャプチャ パラメータを含む外部ファイルの［プロファイル URL］を設定します。

5. （オプション）イメージから除外する［ファイル システム］を指定します。

6. （オプション）実行中のサーバのオンライン キャプチャを実行するには、［ライブ キャプチャ］を選択します。 まずサーバをシャットダウンし、再起動の後にイメージをキャプチャするには、［ライブ キャプチャ］を無効にします。

7. （オプション）複数のネットワークが登録され、［ライブ キャプチャ］が無効になっている場合は、キャプチャに使用するネットワークを選択します。

8. （オプション）マイグレートが完了した後にデポからイメージを削除するには、［イメージの削除］を選択します。
9. ［次へ］をクリックします。

   ［マイグレート デスティネーション］パネルが表示されます。
10. ［プロビジョニング タイプ］を選択します。
    - 既存のマシンに展開するには、［デフォルト］を選択します。
    - 現在 RSI エージェントが展開されていない、またはオペレーティング システムがインストールされていない新しいサーバまたは仮想マシンにプロビジョニングするには、［ベア メタル］を選択します。
    - 仮想マシンの新しいインスタンスを、マイグレートされたサーバイメージをホストするようにプロビジョニングするには、［新しい VM］を選択します。

      ［VMware vCenter プロビジョニング］ウィザードが表示されます。「仮想マシン（vCenter Server）の追加 (P. 665)」で説明されている手順に従います（手順 2 から開始します）。 ウィザードが完了すると、［マイグレート デスティネーション］パネルに戻ります。

      注: 新しい VM のプロビジョニングでは、VM テンプレートは使用されません。 ディスクとネットワークの設定手順は、オプションではありません。

      重要: すべてのディスクに対して同じデータストアを指定してください。 データストアが異なる複数のディスクを作成すると、新しい VM のプロビジョニングが失敗します。
11. 展開に使用する RSI サーバを選択します。

    注: キャプチャと展開用の RSI サーバが異なる場合、これらのサーバは同じデポにアクセスする必要があります。
12. ［マシン タイプ］を指定します。
    - ［物理マシン］の［ターゲット MAC］を指定します。
    - ［仮想マシン］の［ハイパーバイザ］と［ターゲット サーバ ID］を指定します。
13. （オプション）データを含むイメージの一部のみを展開するには［スケール］を選択し、展開パラメータを含む外部ファイルの［プロファイル URL］を設定します。

14. （Windows のみ）展開する［ドライバ セット］を選択します。

    注: Windows イメージが正常に展開された後、Windows は chkdsk を実行します。 ターゲット システムは自動的に再起動し、Windows は PnP（プラグアンドプレイ）を実行してドライバをインストールします。

15. （オプション）イメージをホストしているマシンに適用する［ホスト名］を指定し、使用する［ネットワーク インターフェース］を選択します。

    注: ホスト名の設定は、イメージまたはプロファイル内のホスト名より優先されます。

16. ［終了］をクリックします。

    ウィザードから、イメージをターゲット マシンにマイグレートする要求がサブミットされます。 マイグレートの進行状況を［ジョブ］ペインで追跡します。

    注: CA Server Automation から WakeOnLan を使用してネットワーク ブートできない物理ベア メタル サーバへのマイグレーションの場合は、マイグレート中にサーバを再起動するために手動操作が必要になることがあります。

RSI イメージおよびドライバの管理

CA Server Automation を使用すると、キャプチャされたイメージ、ドライバ セット、およびコレクションを管理できます。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーの［データ センター］を右クリックして、［管理］-［RSI リソース］を選択します。

   ［RSI リソース］ パネルが表示されます。

2. ［イメージ］、［ドライバ セット］、または［ドライバ コレクション］タブを選択します。

3. ドライバ セットおよびコレクションを追加するには［+］をクリックし、選択したイメージ、ドライバ セット、およびコレクションを削除するには［-］をクリックします。

注: 削除されたイメージおよびドライバはデポからも削除されるため、RSI サーバからの展開には使用できなくなります。

RSI アクションの自動化

CA Server Automation を使用すると、ポリシー管理機能を使用して RSI アクションを自動化できます。 各アクションでは、対応する手動の機能が複製され、さらに承認などのポリシー管理入力が追加されます。

ポリシー管理を使用した自動化には、以下の RSI アクションが使用できます。

- イメージのキャプチャは、RSI イメージのキャプチャ (P. 1069)になります。
- イメージの展開は、RSI イメージの展開 (P. 1072)になります。

ポリシー管理では、定期的なスケジュールに基づいて、またはイベント モニタリングに応じてアクションを自動化できます。 詳細については、「ルールとアクションの使用 (P. 831)」を参照してください。

CA ITCM を使用して Rapid Server Imaging を展開する方法

システム管理者は、CA Server Automation を使用して、物理サーバ リソースと仮想サーバ リソースにまたがるソフトウェア イメージの最適なポリシー主導型プロビジョニングを管理します。

Rapid Server Imaging （RSI）は、クロスプラットフォームおよび異種混合のハードウェア プロビジョニング、物理および仮想サーバ マイグレーション、惨事復旧、およびイメージのキャプチャと展開を実行するために使用します。 ハードウェアが同じプロセッサ ファミリに属している場合は、複数の動作環境を備えた異なるハードウェアにわたってイメージを展開できます。

オプションの統合製品 CA ITCM（CA Software Delivery を含む）を使用して、RSI サーバおよび RSI エージェント用に事前設定されたパッケージを配信します。

前提条件:

1. CA ITCM をインストールし、RSI を展開する環境を管理できるように設定します。

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

2. CA Server Automation の設定時に、ドメイン マネージャとスケーラビリティ サーバの設定を CA ITCM の展開に合わせて設定します。

3. 以下の CA Server Automation サービスがインストールされ、CA ITCM を使用した RSI 展開をサポートするように設定されていることを確認します。

   - プロビジョニング マネージャ
   - 展開および設定配布（スケーラビリティ）サーバ
   - SDAdapter
   - Rapid Server Imaging （RSI）への CA 統合

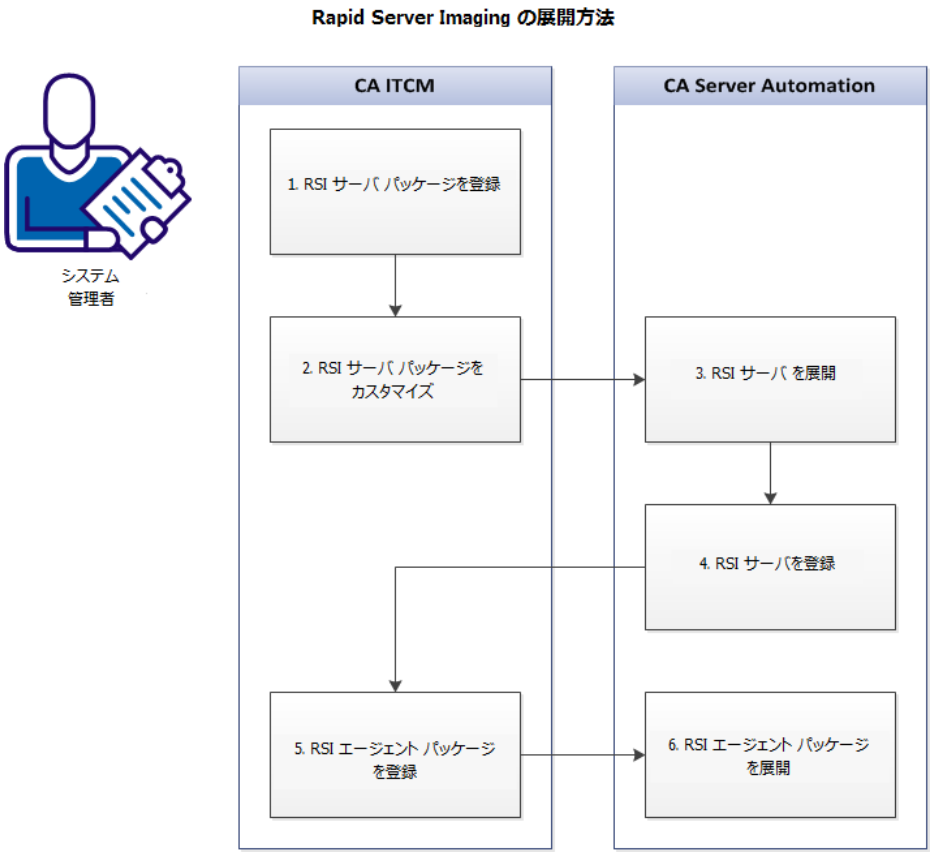
   注: 詳細については、「CA Server Automation インストール ガイド」を参照してください。

重要: 提供されている RSI サーバ MWS パッケージは、Red Hat Linux サーバにのみ展開できます。

このプロセスを実行するには、以下のアクセス権があることを確認してください。

- RSI パッケージが含まれている CA Server Automation インストール メディアの DVD3 へのアクセス。
- CA Server Automation および CA ITCM の管理者権限
- RSI サーバおよびエージェントを展開するのに必要な、すべてのターゲット サーバの管理者認証情報
- （オプション）仮想マシンを制御するハイパーバイザの認証情報

以下のプロセスは、CA Server Automation および CA ITCM を使用して RSI をインストールおよび展開する方法の概要を示しています。



1. RSI サーバ パッケージの登録 (P. 1081)
2. RSI サーバ パッケージのカスタマイズ (P. 1082)
3. RSI サーバの展開 (P. 1084)
4. RSI サーバの登録 (P. 1068)
5. RSI エージェント パッケージの登録 (P. 1085)
6. RSI エージェント パッケージの展開 (P. 1086)

RSI サーバ パッケージの登録

CA Server Automation のイメージング機能とソフトウェア配信機能を使用して RSI サーバを展開するには、CA ITCM に RSI サーバ パッケージを登録します。

次の手順に従ってください:

1. linux フォルダを CA Server Automation インストール メディアの以下の場所から CA ITCM サーバの一時フォルダにコピーします。

   DVD3¥Racemi¥SoftDeliveryPackages¥MWS

   注: フォルダには少なくとも 3.5 GB の空き領域が必要です。

2. 以下の場所から全コンテンツをコピーします。

   DVD3¥Racemi¥DynaCenter_*version*.

3. 以下の場所に内容を配置します。

   local_drive:¥*temporary_folder*¥linux¥1.vol¥DynaCenter_*version*

   注: 長さ 0 のファイル「COPY CONTENTS HERE」を使用して正しい場所を識別します。

4. CA ITCM サーバ上で、［スタート］-［すべてのプログラム］-［CA］-［IT Client Manager］-［DSM エクスプローラ］をクリックします。

5. DSM エクスプローラ ツリーで、［ソフトウェア］-［ソフトウェア パッケージ ライブラリ］-［すべてのソフトウェア］を展開します。

6. ［すべてのソフトウェア］を右クリックし、ショートカット メニューから［インポート］-［ソフトウェア パッケージ］を選択します。

   ［ソフトウェア パッケージの登録］ダイアログ ボックスが表示されます。

7. 以下のパスを入力して［OK］をクリックします。

   local_drive:¥*temporary_folder*¥linux

   ソフトウェア パッケージが CA ITCM にインポートされ、DSM エクスプローラに「Racemi DynaCenter MWS *バージョン*」として一覧表示されます。

RSI サーバ パッケージのカスタマイズ

CA Server Automation インストール メディアで提供されている RSI サーバ パッケージは、RSI の展開環境に合わせてカスタマイズする必要があります。

設定ファイルには、以下の環境パラメータが指定されています。

- RSI サーバのネットワーク設定
- RSI サーバがアクセスできるネットワーク
- ターゲット サーバのイメージングに関してサポートされているオペレーティング システム
- イメージ保存デポの場所

次の手順に従ってください:

1. CA ITCM で DSM エクスプローラ ツリーを開き、［ソフトウェア］-［ソフトウェア パッケージ ライブラリ］-［すべてのソフトウェア］に移動します。

   ［Racemi DynaCenter MWS］パッケージを右クリックし、［封印解除］をクリックします。

2. 左ペインで［Racemi DynaCenter MWS］-［ソース］を展開し、［パッケージ］をクリックします。

   右ペインにパッケージのフォルダ構造が表示されます。

3. config.ini ファイルを編集します。

   # で始まるすべての行のコメントを外し、環境に応じてパラメータ値を適宜入力します。

   たとえば、下記の設定ファイルのパラメータによって以下の項目が定義されます。

   - ループ バック アドレス 127.0.0.1 を使用する単一の RSI サーバ
   - サポートされるすべてのオペレーティング システム（デフォルトでは Windows と Red Hat Linux が指定される）を実行しているターゲット サーバのイメージングのサポート
   - ネットワーク アドレス 10.130.64.0 ～ 255 を使用したターゲット サーバへのアクセス
   - 10.130.64.162 でアクセス可能なプライマリ ネットワーク インターフェース eth0
   - 10.130.64.162 で以下のストレージ パスを使用してアクセス可能な保存デポ
     - パス /repo/R にあるコンポーネント [default] 用のデフォルト ストレージ
     - エージェントのイメージおよびイメージ メタデータ [instance] 用のパス /repo/I
     - キャプチャされたイメージ [image] 用のパス /repo/images

```
[general]
oem_configuration = True
agent_addressing = dhcp
os_support = Solaris-sun4u, Solaris-i86pc
mws_address = 127.0.0.1
database_address = 127.0.0.1
[client_networks]
[[10.130.64.0/24]]
gateway = 10.130.64.1
addresses = 10.130.64.0-10.130.64.255
mws_interface = eth0
mws_ip = 10.130.64.162
[storage]
[[default]]
path = /repo/R
server_address = 10.130.64.162
type = component
[[instance]]
path = /repo/I
```

```
server_address = 10.130.64.162
type = image_metadata
[[image]]
path = /repo/images
server_address = 10.130.64.162
type = captured_image
```

注: config.ini ファイルのパラメータの詳細については、「*RSI サーバ インストール ガイド*」の「サイレント インストール」を参照してください。

4. 左ペインで、［Racemi DynaCenter MWS］を右クリックし、［封印］を選択し、［OK］をクリックします。

   これで、RSI サーバ パッケージを展開する準備ができました。

RSI サーバの展開

CA Server Automation を使用して、CA ITCM に登録されたカスタマイズ済みの RSI サーバ パッケージを展開します。

1. ［リソース］をクリックし、［エクスプローラ］ツリーの［データ センター］を右クリックして、［パッケージング］-［パッケージの管理］を選択します。

   ［パッケージ］-［パッケージ］タブが表示されます。

2. RSI サーバ パッケージが登録されたドメイン サーバを選択します。
3. ［利用可能なパッケージ］セクションから Racemi DynaCenter MWS パッケージを選択し、下矢印をクリックしてそれを［選択されたパッケージ］セクションに移動します。
4. ［保存］をクリックします。

   ［管理対象パッケージ］リストが更新されたことを示す確認メッセージが表示されます。 RSI サーバ パッケージを展開できる状態です。

5. ［エクスプローラ］ツリーの［データ センター］を右クリックし、パッケージング］-［ソフトウェアの展開］を選択します。

   ［管理対象リソース］セクションが表示されます。

6. ［RSI サーバ］パッケージ展開用の管理対象サーバを選択します。
7. Racemi DynaCenter MWS パッケージを選択し、手順「インストール」、および使用するドメイン サーバを選択します。

8. ［OK］をクリックします。

   注: CA Software Delivery エージェントがターゲット サーバにインストールされていない場合は、エージェントをインストールするように求めるダイアログ ボックスが表示されます。

9. ターゲット サーバ用の有効な認証情報、スケーラビリティ サーバ名、オペレーティング システム タイプを入力して［OK］をクリックします。

   パネルは、選択されたサーバに RSI サーバ パッケージをインストールする要求をサブミットします。

RSI エージェント パッケージの登録

CA Server Automation のプロビジョニング機能を有効にして RSI エージェントのソフトウェア配信パッケージを展開するには、CA ITCM にパッケージを登録します。 各エージェント パッケージは特定のオペレーティング システムをサポートし、RSI サーバが、そのオペレーティング システムを使用してサーバ上でイメージをキャプチャして展開できるようにします。

注: 各オペレーティング システムのパッケージを個別にインポートしてください。

次の手順に従ってください:

1. CA ITCM サーバ上で、［スタート］-［すべてのプログラム］-［CA］-［IT Client Manager］-［DSM エクスプローラ］をクリックします。
2. DSM エクスプローラ ツリーで、［ソフトウェア］-［ソフトウェア パッケージ ライブラリ］-［すべてのソフトウェア］を展開します。
3. ［すべてのソフトウェア］を右クリックし、ショートカット メニューから［インポート］-［ソフトウェア パッケージ］を選択します。

   ［ソフトウェア パッケージの登録］ダイアログ ボックスが表示されます。

4. 以下のタスクのいずれか *1* つを実行します。

   - パスを入力します。

     たとえば、Windows の場合は以下のパスを入力します。

     DVD_drive:¥DVD3¥Racemi¥SoftDeliveryPackages¥DPADAgent¥win

   - CA Server Automation インストール メディアの DVD3 上の SoftDeliveryPackages フォルダでターゲット オペレーティング システムの適切なフォルダに移動します。［選択］をクリックしてフォルダのパスを選択し、［OK］をクリックします。

   RSI エージェント ソフトウェア パッケージが CA ITCM にインポートされ、DSM エクスプローラにリスト表示されます。

RSI エージェント パッケージの展開

CA Server Automation を使用して、CA ITCM に登録された RSI エージェント パッケージをターゲット サーバに展開します。

次の手順に従ってください:

1. ［リソース］をクリックし、［エクスプローラ］ツリーの［データ センター］を右クリックして、［パッケージング］-［パッケージの管理］を選択します。

   ［パッケージ］-［パッケージ］タブが表示されます。

2. RSI エージェント パッケージが登録されたドメイン サーバを選択します。

3. ［利用可能なパッケージ］セクションから RSI エージェント パッケージを選択し、下向き矢印をクリックしてそれを［選択されたパッケージ］セクションに移動します。

4. ［保存］をクリックします。

   ［管理対象パッケージ］リストが更新されたことを示す確認メッセージが表示されます。 RSI Agent パッケージは、展開できる状態です。

5. ［エクスプローラ］ツリーの［データ センター］を右クリックし、パッケージング］-［ソフトウェアの展開］を選択します。

   ［ソフトウェア展開］パネルが表示されます。

6. RSI エージェント パッケージ展開用の管理対象サーバを選択します。
7. 各サーバについて、展開する RSI エージェント パッケージ、手順「インストール」、および使用するドメイン サーバを選択します。

   注: 各管理対象サーバ上のオペレーティング システム用の適切な RSI エージェントを選択します。
8. ［OK］をクリックします。

   注: CA Software Delivery エージェントがターゲット サーバにインストールされていない場合は、エージェントをインストールするように求めるダイアログ ボックスが表示されます。
9. ターゲット サーバ用の有効な認証情報、スケーラビリティ サーバ名、オペレーティング システム タイプを入力して［OK］をクリックします。

   パネルは、選択された各サーバに 選択された RSI エージェント パッケージをインストールする要求をサブミットします。

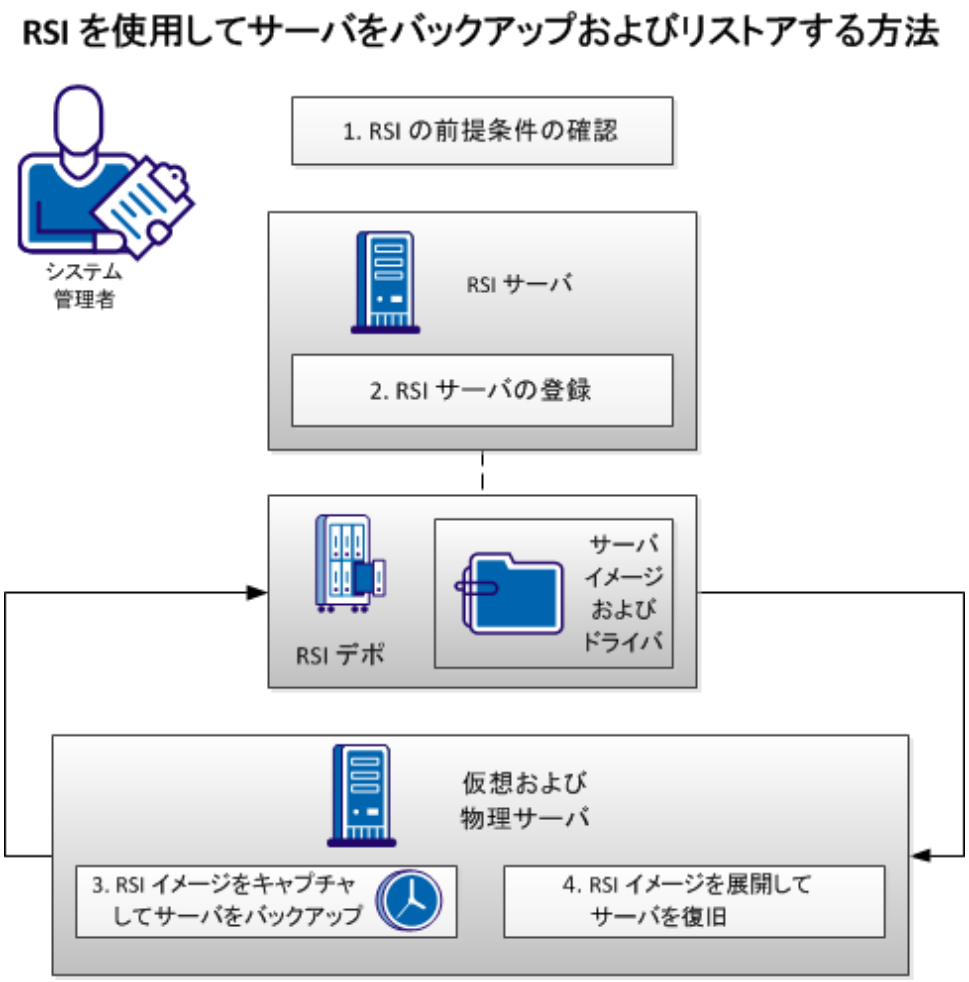
   エージェント パッケージの展開が完了すると、RSI イメージのキャプチャを使用してターゲット サーバに CA Server Automation の機能を展開できます。

RSI を使用してバックアップおよびリストアする方法

*システム管理者*は、CA Server Automation を使用して、物理および仮想サーバ環境を管理およびプロビジョニングします。 バックアップとリストアのための信頼性に優れたメカニズムが必要です。

Rapid Server Imaging（RSI）は、クロスプラットフォームおよび異種混合のハードウェア プロビジョニング、物理および仮想サーバ マイグレーション、惨事復旧、およびイメージのキャプチャと展開を実行するために使用します。 ハードウェアが同じプロセッサ ファミリに属している場合は、複数の動作環境を備えた異なるハードウェアにわたってイメージを展開できます。

以下のプロセスは、RSI を使用して管理対象サーバをバックアップおよびリストアする方法の概要を示しています。



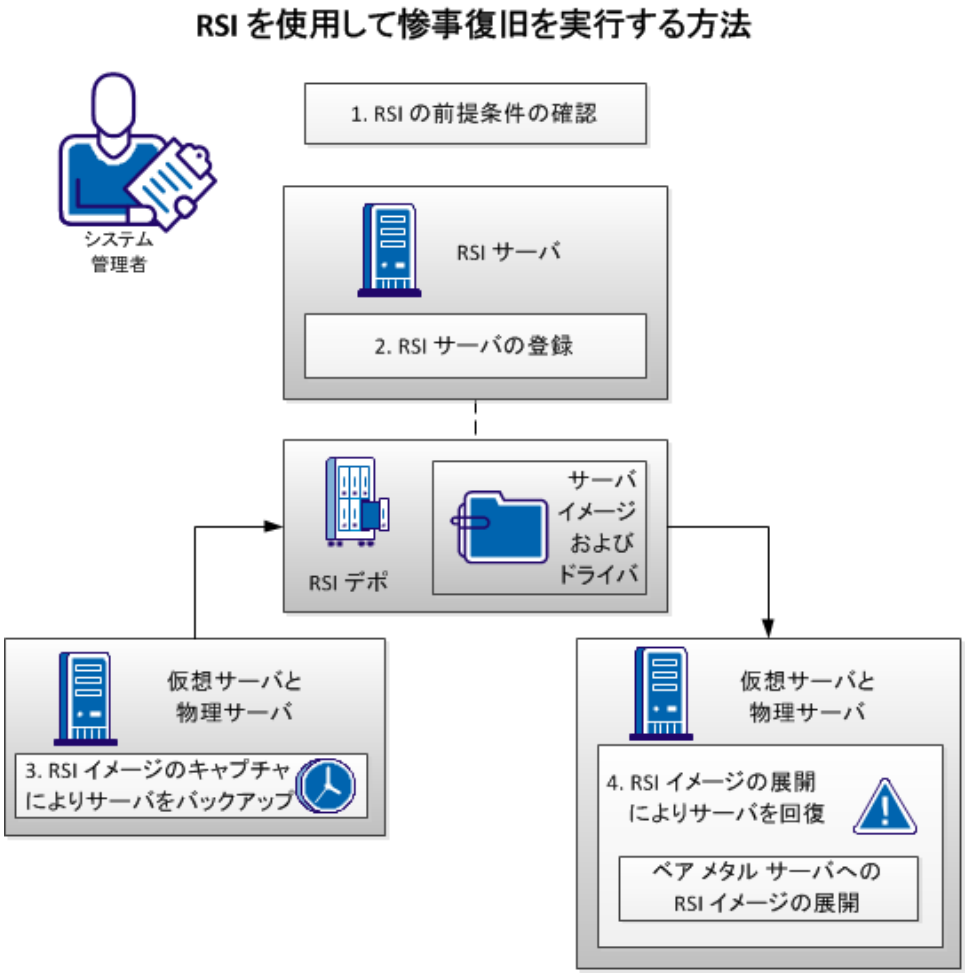
1. RSI の前提条件 (P. 1066) を確認します。
   - Hyper-V に対する RSI の前提条件 (P. 1068)
2. RSI サーバを登録します (P. 1068)。
3. RSI イメージをキャプチャ (P. 1069) し、それらを RSI デポ内に格納することによって、サーバをバックアップします。
   - （Windows のみ）Windows ドライバ セットをキャプチャします (P. 1070)。
   - （オプション）RSI アクションを自動化します (P. 1077)。 定期的に RSI イメージをキャプチャするためのスケジュールを定義します (P. 945)。
4. RSI デポから RSI イメージを展開する (P. 1072) ことによって、サーバをリストアします。

RSI を使用して惨事復旧を実行する方法

*システム管理者*は、CA Server Automation を使用して、物理および仮想サーバ環境を管理およびプロビジョニングします。 惨事復旧のための信頼性に優れたメカニズムが必要です。

Rapid Server Imaging（RSI）は、クロスプラットフォームおよび異種混合のハードウェア プロビジョニング、物理および仮想サーバ マイグレーション、惨事復旧、およびイメージのキャプチャと展開を実行するために使用します。 ハードウェアが同じプロセッサ ファミリに属している場合は、複数の動作環境を備えた異なるハードウェアにわたってイメージを展開できます。

以下のプロセスは、RSI を使用して管理対象サーバの惨事復旧を実行する方法の概要を示しています。



1. RSI の前提条件 (P. 1066) の確認
   - Hyper-V に対する RSI の前提条件 (P. 1068)
2. RSI サーバを登録します (P. 1068)。
3. RSI イメージのキャプチャ (P. 1069) によってサーバをバックアップし、それらのイメージを RSI デポ内に格納します。
   - (Windows のみ) Windows ドライバ セットをキャプチャします (P. 1070)。
   - (オプション) RSI アクションを自動化します (P. 1077)。定期的に RSI イメージをキャプチャするためのスケジュールを定義します (P. 945)。
4. RSI デポから RSI イメージを展開する (P. 1072) ことによって、サーバ イメージを新しいサーバに回復します。
   - (オプション) RSI アクションを自動化します (P. 1077)。モニタ対象サーバのイベントに基づいて自動的にイメージを展開するためのルールを作成します (P. 835)。
   - RSI イメージをベア メタル サーバに展開 (P. 1073) して、システム イメージ (新しいオペレーティング システムを含む) を空のサーバに回復します。

UCS 向けの Rapid Server Imaging サポート

Cisco UCS ブレードを物理サーバ リソースの基礎タイプまたは VM ホストとして使用して、サポート対象 RSI イメージ移行 (物理から物理、物理から仮想、仮想から物理、または仮想から仮想) を指定できます。

例: x86 システムから Cisco UCS ブレードへのアプリケーションの移動

レガシー x86 システムから Cisco UCS システムに Windows アプリケーションをマイグレートするには、両方のシステムを CA Server Automation の制御下に配置します。 RSI 機能を使用して、レガシー x86 システムでアプリケーション イメージをキャプチャし、Cisco UCS システム上の適切なサービス プロファイルと関連付けられたブレードにイメージを転送します。

第 13 章: 予約マネージャ のセットアップ

予約マネージャ は、物理マシンおよび仮想マシンの予約、予約テンプレートの作成、インベントリの表示、および予約の管理を行う機能を提供します。

予約マネージャ のインストールの後、以下のアクティビティを完了してエンドユーザ用に準備します。

- 組織単位をセットアップしてシステムおよびシステム イメージへのユーザ アクセスを制御します。
- 1 つ以上のリソース プールを定義し、アクセス ポリシーを指定します。
- ユーザが利用できるシステムをインベントリに追加し、それらを分類し、1 つ以上のリソース プールに関連付けます。
- ユーザが利用できるオペレーティング システム イメージ (および仮想システム テンプレート) を識別し、アクセス ポリシーを指定します。
- ユーザが利用できるソフトウェア パッケージを識別し、アクセス ポリシーを指定します。

これらのアクティビティを完了するのに必要な特定の順序はありません。

この章では、エンドユーザ用に 予約マネージャ をセットアップするためのインストール後のタスクについて説明します。

注: 予約マネージャ オンライン ヘルプではベストプラクティス、および予約マネージャ を使用する方法を説明します。 インストール処理の詳細は「インストール ガイド」にあります。

このセクションには、以下のトピックが含まれています。

予約マネージャ の前提条件

エンドユーザ向けに 予約マネージャ のセットアップを開始する前に、以下のタスクを実行します。

- 予約マネージャ が正しく登録されていることを確認します。これを行うには、CA Server Automation の［管理］ - ［設定］ページで、予約マネージャ のステータスを確認します。
- 予約マネージャ 用に環境を準備します。
- 予約マネージャ 用に CA Server Automation を準備します。
- すべての必要なコンポーネントとサーバが正しくインストールされていることを確認します。

関連項目:

予約マネージャ 用の環境の準備 (P. 1094)
予約マネージャ のための CA Server Automation の準備 (P. 1097)

予約マネージャ 用の環境の準備

予約マネージャ をセットアップする前に、以下の情報を収集して環境を準備します。

1. 予約要求を処理するために 予約マネージャ インベントリに含めるシステムを識別します。 必要なシステム情報には以下が含まれます。
   - Windows、AIX、Solaris または Linux 用のデフォルト パスワード
   - ネットワーク インターフェース コントローラ モデル
2. ユーザが利用できるように、必要なネットワーク インターフェース コントローラのデバイス ドライバが 1 つ以上の OS イメージで利用可能であることを確認します。
3. 展開するオペレーティング システムとバージョンを識別します。

4. 各 Windows および Linux オペレーティング環境に対する CA ITCM サポートを確認します。
5. サポートする仮想プラットフォームを識別し、対応するサーバ サポートを確認します。 以下に、検討すべきサーバおよびプラットフォームの例を示します。

   Amazon Elastic Compute Cloud（EC2）

   Amazon Elastic Compute Cloud （EC2）に Windows および Linux プロビジョニングのイメージング機能を提供します。

   CA ITCM サーバ - OSIM イメージング

   Software Delivery が含まれた CA ITCM OS インストール技術（OSIM）を使用して、Windows または Linux オペレーティング システムを実行するコンピュータをプロビジョニングします。

   Citrix XenServer

   Citrix XenServer は、あらかじめ設定したシステム情報を使用して仮想マシンを展開する機能を提供する、管理対象サーバ仮想化プラットフォームです。

   Huawei GalaX

   Huawei GalaX 環境は Huawei SingleCLOUD ソリューションの一部で、クラウド サービス プロバイダまたは企業顧客のクラウド コンピューティング データ センター向けに設計されています。Huawei GalaX 環境は、Elastic Service Controller （ESC）および下位のコンピューティング/ストレージ クラスタから構成されます。

   Huawei SingleCLOUD ソリューションは抽象階層アーキテクチャから構成されます。 物理層およびネットワーク層のデバイスはソリューションへ統合されます。クラスタ、分散ストレージ、NAS ストレージ、および仮想化の技術に基づいて、これらの統合されたデバイスはストレージ、コンピューティング、およびネットワーク サービスを上層のサービスに提供します。 CA Server Automation 内の検出された Huawei SingleCLOUD インスタンスでは、お使いの Huawei GalaX 環境を管理、モニタするために必要なインフラストラクチャが提供されます。

Hyper-V SCVMM

System Center Virtual Machine Manager（SCVMM）では、ハードウェアおよびオペレーティング システム オプションでテンプレートおよびカスタマイズ プロファイルを使用してシステムを展開するための機能を提供します。ほとんどのサイトには Microsoft Hyper-V または VMware vCenter のいずれかがありますが、両方ではありません。

注: 予約マネージャ は、Windows Server 2003 および Windows Server 2008 オペレーティング システムの Hyper-V プロビジョニングをサポートします。 Windows 7 および Windows Vista はサポートされていません。

IBM PowerVM（HMC/IVM）

AIX オペレーティング システムで IBM PowerVM 論理パーティションに対する管理機能と仮想化機能を提供します。

NIM **マスタ サーバ**

IBM AIX オペレーティング システムを実行するコンピュータにイメージング機能を提供します。 このコンポーネントは、IBM AIX オペレーティング システムをプロビジョニングする場合にのみ必要です。 複数の NIM Master サーバがサポートされています。 NIM Master サーバが設定されていて、システム リソースおよびリソース グループが NIM Master サーバ上で作成されて設定されている必要があります。NIM Master サーバは CA Server Automation に登録されている必要があります。

Red Hat Enterprise Virtualization（RHEV）

Red Hat Enterprise Virtualization は、あらかじめ設定されたシステム情報を使用して、仮想マシンを展開する機能を提供する仮想化管理ソリューションです。

Software Delivery **アダプタ**

パッケージング コンポーネントは予約要求を処理するために割り当てられたサーバに、要求されたソフトウェアをインストールします。Software Delivery ではソフトウェアを既存のサーバに追加する必要があります。

Solaris JumpStart サーバ

Solaris オペレーティング システムを実行するコンピュータにイメージング機能を提供します。 このコンポーネントは、Solaris オペレーティング システムをプロビジョニングする場合にのみ必要です。

VMware vCenter Server

カスタム テンプレートおよびカスタム仕様を使用して、仮想マシンを展開するための機能を提供します。

6. 予約マネージャ へのアクセスを付与するすべてのにユーザを識別します。 以下を確認します。
   - 予約マネージャ 管理者ユーザ
   - 予約マネージャ エンド ユーザ
7. ネイティブ CA EEM セキュリティを使用している場合は、すべてのユーザが CA EEM データベースに定義されていることを確認します。

予約マネージャ のための CA Server Automation の準備

CA Server Automation を設定して、インベントリの作成と予約要求の処理で 予約マネージャ が使用する環境を準備します。 予約マネージャ のセットアップ用に CA Server Automation を準備するには、以下の手順に従います。

1. ソフトウェア パッケージを選択して展開に利用できるようにします。
2. CA ITCM Operating System Installation Management （OSIM）イメージングをテストするすべてのシステムを検出します。 ［リソース］タブを選択し、［エクスプローラ］ペイン内のシステムを右クリックして［プロビジョニング］を選択し、イメージを 予約マネージャ インベントリ用のシステムにプロビジョニングします。
3. （オプション）前の手順で検出されたすべてのシステムに CCA エージェントを展開します。 エージェントが、MAC アドレス、CPU の数、利用可能なメモリおよびディスク領域などのシステムの詳細情報を収集したことを確認します。

4. 適切な管理レベルを提供するのに必要な数のサービスを作成します。予約マネージャ に対して利用可能にするシステムをこれらのサービスに追加します。

   予約マネージャ は、これらのサービスをインポートしてユーザが予約できるシステムのリソース プールを作成します。 予約マネージャ は、サービスおよびリソース プール レベル、およびその他の使用ポリシーでシステムへのアクセスを制御します。

   サービスの設定には、CA Server Automation で提供される Automation Management Framework をインストールする必要があります。Automation Management Framework は、予約のセットアップまたは取り消し処理中に CA Server Automation アクションをオプションで実行します。

セットアップおよび設定

このセクションでは、予約マネージャ のセットアップと設定について説明します。

サービス プロビジョニング用の事前定義済みのコンテンツおよび設定

CA Server Automation で実行されたサービス プロビジョニング機能のいくつかは、予約マネージャ でも有効です。 サービス テンプレートは CA Server Automation 管理ユーザ インターフェースで事前定義されています。予約マネージャ の予約テンプレートは、サービス テンプレートに基づいて作成されます。 予約マネージャ ユーザ インターフェースまたは CA Server Automation ポータル インターフェースから、サービスの予約を作成できます。

事前定義済みのサービス プロビジョニングを提供するために、以下のアクションが実行されます。

- ［オンデマンド リソース］はデフォルトのリソース プールの名前で、設定済みで利用可能な VMware vCenter データ ストアがデフォルトですべて含まれます。 CA Server Automation ポータルで vCenter Server が設定されると、オンデマンド リソース プールに ESX サーバ リソースが追加されます。
- オンデマンド リソース プールにアクセスするために、サービス管理者の組織単位が追加および設定されます。

- Citrix XenServer、Red Hat Enterprise Virtualization （KVM ベース）、および Huawei GalaX では、現在サービス プロビジョニングをサポートしていません。これらのプラットフォーム用のリソース プールを作成するには、以下の手順に従います。
  - XenServer については、管理者は 1 つ以上のプールを作成し、各プールに対するデータ ストアを手動で選択する必要があります。
  - KVM については、管理者は 1 つ以上のプールを作成し、クラスタを手動で選択する必要があります。 クラスタに属するハイパーバイザはすべて自動的に追加され、分離することはできません。
  - GalaX については、管理者は 1 つ以上のプールを作成し、プールが使用する可用性ゾーンを手動で選択する必要があります。 可用性ゾーンのストレージ ユニットがすべて含まれています。
- CA Server Automation で事前に定義されているすべてのサービス テンプレートから予約テンプレートが自動的に作成されます。

  注: 事前定義済みの予約テンプレートの詳細を表示するには、［予約テンプレート］に移動してウィザードを使用します。

仮想マシンを利用可能にする

以下のプロセスを使用して仮想マシンを予約できるようにします。

1. VM が作成された場合、それらが追加される仮想リソース プールを識別します。
2. VM を作成するのにユーザが使用できる VM テンプレートを定義します。
3. リソース プールおよび VM テンプレート用の両方のアクセス ポリシーをセットアップします。

以下のセクションでは、VM 予約をサポートする 予約マネージャ をセットアップする方法について説明します。

注: ユーザ権限は特定プラットフォームの製品にセット アップされている必要があります。

仮想マシンの予約をサポートするための前提条件

予約マネージャ が使用する仮想マシンを展開する前に、リソース プールのプラットフォーム リソースを以下のように特定します。

- Citrix XenServer： XenServer 内のデータ ストア
- Huawei GalaX： 可用性ゾーンの内のストレージ ユニット（GalaX サーバ）
- Red Hat Enterprise Virtualization （KVM） ： データセンター内のクラスタ内のハイパーバイザ（Red Hat 管理サーバ）
- VMware： 1 つ以上の VMware ESX サーバまたは VMware ESX サーバのクラスタ

次に、各サーバまたはクラスタ上で仮想マシンを作成する対象となるリソース プールを定義します。 サーバまたはクラスタが仮想マシンを作成できるかどうか決定するために、予約マネージャ はサーバ上の新しい仮想マシンで利用可能なメモリの量を計算します。

サーバまたはクラスタ上のリソース プールにメモリ制限が定義されている場合、予約マネージャ では将来のリソース可用性を判断するために対象のリソース プールへの排他的アクセスを必要とします。

リソース プール レベルのメモリ制限がない場合、予約マネージャ のその計算は全面的にサーバ レベルで仮想マシンで利用可能なメモリの量に基づきます。 予約マネージャ では、将来のリソース可用性を正確に判断するために仮想マシンの作成に使用されるサーバの排他的使用を必要とします。

注: リソース プールおよび VM テンプレートの追加は、データ センターおよびフォルダが追加されたときに定義されたコンテキストに応じて実行されます。データ センターまたはフォルダの名前が変更されたり、VM テンプレートが別のフォルダに移動された場合、事前に 予約マネージャ に追加されたリソース プールおよびテンプレートは使用できなくなります。したがって、これらのアイテムを追加する前にプラットフォームの構造を安定させることが重要です。

仮想マシンのリソース プールの作成

以下の手順では、予約マネージャ 用の仮想リソース プールを作成する方法について説明します。

注: リソース プールの追加は、それらが追加された時点のプラットフォームのコンテキストで実行されます。 たとえば、VMware データセンターの名前が変更された場合、予約マネージャ 内に定義されたリソース プールは使用できなくなります。 したがって、リソース プールを追加する前にプラットフォームの構造を安定させることが重要です。

仮想リソース プールを作成する方法

1. 予約マネージャ の管理者として、[予約マネージャを管理] の [リソース プールを管理] をクリックします。

   [リソース プール] リストが表示されます。

2. [リソース プール] リストの右上角の [アクション] メニューから適切なプラットフォーム プールを選択し、ウィザードの指示に従います。

例: XenServer

データストアのリストを取得するために [Xen リソース プール] および [Xen サーバ] を選択します (サーバはサブオプションです)。 データストアを個別に選択してリソース プールの一部とすることができます。

例: KVM

[RedHat Management Server]、[データセンター] および [クラスタ/ホスト名] を選択します。 クラスタに属するハイパーバイザはすべてリソース プールに含まれています。サブセットは選択できません。

例: Huawei GalaX

[Galax サーバ] および [可用性ゾーン] を選択します。 すべての可用性ゾーンがリソース プールに追加されるため、ストレージ ユニット テーブルは参照用です。

予約承認のためのヘルプ デスクの使用

予約マネージャ は、予約承認プロセスを管理するためのヘルプ デスク システムを使用するオプションを提供します。

予約承認のためのヘルプ デスク システムを使用する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［承認］領域を開き、以下の値を変更して［OK］をクリックします。
   - ヘルプ デスク チケットのオープン
   - ヘルプ デスク チケットのタイプ
   - ヘルプ デスク チケット テンプレート
   - 承認時にヘルプ デスク チケットを自動的にクローズ

   設定変更は、次に予約が作成されるときに有効になります。

VMware リソース プール内のスナップショットの管理

管理者は、ユーザに VMware 仮想マシンのスナップショットを作成する権限を付与することができます。 また、許可されるスナップショットの数を指定したり、ファイル システムを静止するかどうかを指定したりすることができます。

注: スナップショットは VMware についてのみサポートされています。

VMware リソース プールでスナップショットを管理する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. リソース プールをクリックします。

   ［リソース プールの詳細］ペインが開き、［プロパティ］タブが表示されます。

3. Tab キーの右側で、以下の手順を実行します。
   - ［VM スナップショットの作成を許可する］を選択します。
   - ［スナップショットの最大数］の数を選択します。

- （オプション）［ファイル システムの静止 （VMware ツールのインストールが必要）］を選択します。

  このオプションを使用すると、VMware ツールはスナップショットが作成されたときに電源がオンになっている仮想マシンのファイル システムを静止することができます。 静止によって、コンピュータのディスク上のデータをバックアップに適した状態にします。 この処理には、オペレーティング システムのメモリ内キャッシュからの使用済みバッファのディスクへのフラッシュや、その他の上位レベルのアプリケーション固有のタスクなどの操作が含まれる場合があります。

スナップショットの許可は、このリソース プールを使用する新しい予約に対して有効になります。

リソース プールからプロビジョニングされないように VM を停止する

管理者は、特定のリソース プールからプロビジョニングされないように VMware 仮想マシンを停止することができます。

注: プロビジョニングの停止は VMware についてのみサポートされています。

特定のリソース プールからの VM のプロビジョニングを停止する方法

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。

   ［ホーム］ページが開きます。

2. ［予約マネージャを管理］をクリックします。

   ［管理］ページが表示されます。

3. ［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示されます。

4. リソース プールをダブルクリックします。

   ［リソース プールの詳細］ペインが表示されます。

5. ［リソース プールの詳細］タブをクリックし、［稼働ステータス］列のドロップダウン リストから選択します。

   稼働ステータス

   ステータスを［*サービス中*］または［*利用不可*］に設定します。

   デフォルト：［サービス中］

   ［利用不可］に設定された場合、VM の作成中にリソースの可用性をチェックするときにプールは考慮されません。 プロビジョニング時に、予約がこのプールから割り当てられた場合、スケジューラはそれを別のプールに移動させようとします。 他のプールが要求を対応できない場合、予約は失敗します。

VMware リソース プール用のストレージのプロビジョニング

管理者は、新規データストアをプロビジョニングし、それを 予約マネージャ 内の VMware リソース プールに追加された VMware ホストに接続できます。

EMC CLARiiON ストレージと NetApp ストレージは、VMware に対してのみサポートされています。 ストレージは 1 回の操作で、EMC CLARiiON ストレージ システム上にプロビジョニングし、ESX サーバに自動的に接続して、リソース プールに追加することができます。 この機能を使用する前に、NetApp 用のストレージ プロビジョニング マネージャを設定する必要があります。

ストレージをプロビジョニングしてリソース プールのホストに接続する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. リソース プールを選択します。

   ［リソース プールの詳細］ペインが表示されます。

3. ［リソース プールの詳細］をクリックします。

   データセンターのリストが表示されます。

4. データセンターを選択します。

   選択したデータセンターが強調表示されます。

5. ［アクション］ドロップダウン リストをクリックし、［編集］を選択します。

   ［データ ストアの編集］ページが表示されます。

6. ［アクション］ドロップダウン リストをクリックし、［データストアのプロビジョニング］を選択します。

7. ドロップダウンから［拡張ストレージ ポリシー］を選択します。 希望するストレージの量およびデータストアに接続する名前を指定します。

8. ［OK］をクリックします。

   データストアは、ストレージ プロビジョニング ジョブが開始されたリソース プールに追加されます。

ストレージ プロビジョニング ジョブのステータスを追跡するには、次のセクションを参照してください。

VMware リソース プール用ジョブのプロビジョニング

管理者は、予約マネージャ からのストレージ プロビジョニング ジョブを表示できます。

ストレージ プロビジョニング ジョブを表示する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. ［アクション］ドロップダウン リストをクリックし、［ストレージ ジョブの表示］を選択します。

   予約マネージャ から開始されたストレージ ジョブをリスト表示するページが表示されます。

VMware 仮想マシン用のテンプレートの作成

管理者は、1 つ以上のテンプレートを作成してユーザが予約を作成できるようにします。

注: VM テンプレートの追加は、vSphere データセンターおよびフォルダが追加されたときに定義されたコンテキストに応じて実行されます。VMware データセンターまたはフォルダの名前が変更されるか、VM テンプレートが別のフォルダに移動した場合、予約マネージャ に定義されたテンプレートは、使用できなくなります。 したがって、テンプレートを追加する前に vSphere の構造を安定させることが重要です。

VMware 仮想マシン用のテンプレートを作成する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［予約テンプレートを管理］をクリックします。

   ［リソース プール］ページが表示されます。

2. 右上角の［アクション］メニューから［作成］を選択し、ウィザードの指示に従います。

テンプレートの代替変数

Hyper-V、KVM、XenServer、または VMware 仮想マシンの名前またはプレフィックス、あるいは 予約マネージャ 仮想リソース プール内のフォルダの名前またはプレフィックスの代わりに（またはこれらと組み合わせて）以下の代替変数を使用することができます。 VM 名には 10 文字の文字制限がありますが、代替変数を使用する場合は、文字列長の制限はありません。 これらの代替変数は、［予約テンプレートの作成］ウィザードの［要件の指定］ページで使用されます。

%DATACENTER%

VM が作成されるデータ センター名を識別します。

%HOSTSYSTEM%

VM が作成されるサーバ名を識別します。

%ORGUNIT%

予約をサブミットするユーザの組織単位名を識別します。

%PROJECTID%

ユーザが予約をサブミットするときに入力するプロジェクト ID を識別します。

%RESERVATIONID%

ユーザが予約をサブミットするときに割り当てられる数値の予約 ID を識別します。

%RESERVATIONNOTES%

予約に関連した注意事項を識別します。

%RESOURCEPOOL%

予約マネージャ リソース プールの名前を指定します。

%TENANT%

予約をサブミットするテナントの名前を識別します。

%TENANTID%

［テナント ID］設定の値が含まれます。 仮想マシン名での使用に適した、テナントの短縮または省略された名前として機能します。ユーザがテナントのメンバである場合はテナント固有の設定が使用され、それ以外の場合はグローバル設定が使用されます。

%USERNAME%

予約マネージャ にログインしたユーザの名前を識別します。

%VCSERVERNAME%

予約済みシステムが存在する VC サーバの名前を識別します。

プレフィックスが使用されている場合は、予約マネージャ で一意の仮想マシン名になるように、数値のサフィックスが名前に追加されます。 一意の名前を生成するのに他の方法を使用することもできます。たとえば、予約 ID をユーザ名と組み合わせて使用するなどです。

注: 名前またはプレフィックスのいずれで構成される場合でも、NetBIOS 制限のため、VM 識別子は 15 文字以内とする必要があります。予約マネージャ が予約 ID またはマシン番号を追加する場合でも、15 文字の長さ制限が適用されます。

例:

%USERNAME%-%RESERVATIONID%　userkey01-62

%HOSTSYSTEM%-ServerA　ESX1-ServerA

仮想マシンの予約

セットアップしたリソース プールから仮想システムを予約するように 予約マネージャ が設定されていることを確認するには、［ホーム］ブレッドクラムをクリックしてホーム ページに戻ります。

仮想マシン用の予約要請を作成できます。 使用する仮想マシン テンプレート、ソフトウェアおよび作成するマシンの数などの要件を指定します。予約マネージャ は、これらの設定を使用して仮想マシンを作成し、それを予約してプロビジョニングすることによって要求を処理します。

仮想マシンの作成でサポートされている唯一の方法は、テンプレートによる展開です。 仮想マシンに使用するテンプレートを選択します。 次のオプションは、選択されたテンプレートと互換性のある仮想マシンに制限されています。

仮想マシンの予約を作成するには、管理者として、予約マネージャ の［ホーム］ページで［仮想マシンの作成］オプションをクリックし、ウィザードの手順を完了します。

仮想マシン名への VMware プレフィックスの指定

リソース プール レベルで仮想マシンにプレフィックスを指定できます。プレフィックスは一貫した命名規則を提供します。

注: 名前またはプレフィックスのいずれで構成される場合でも、NetBIOS 制限のため、VM 識別子は 15 文字以内とする必要があります。予約マネージャ が予約 ID またはマシン番号を追加する場合でも、15 文字の長さ制限が適用されます。

注: この手順は、Amazon EC2 および IBM PowerVM 仮想マシンには該当しません。

仮想マシン名にプレフィックスを指定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示されます。

2. リソース プールをダブルクリックします。

   ［リソース プールの詳細］ページが開き、［プロパティ］タブが表示されます。

3. 以下のフィールドに値を選択します。

   VM 名の生成

   名前/プレフィックス

   注: KVM は 1 つの VM 名プレフィックスを使用します。

4. ［OK］をクリックします。

   VM 名に、指定されたプレフィックスが含まれます。

Hyper-V 仮想マシンの予約の有効化

管理者は、予約マネージャ からリソース プールとテンプレートをセットアップして、ユーザが Hyper-V システムを予約できるように設定できます。

- 予約マネージャ の［リソース プールを管理］オプションで、［アクション］ ドロップダウン メニューから ［Hyper-V プールの追加］ を選択します。 ウィザードに従って、プールをセットアップするプロセスを進めます。
- 予約マネージャ の ［予約テンプレートを管理］ オプションで、［アクション］ドロップダウン メニューから［作成］ を選択します。ウィザードに従って、テンプレートをセットアップするプロセスを進めます。

Amazon Machine Image を EC2 から利用可能にする

以下のシナリオでは、Amazon Elastic Compute Cloud （EC2） から Amazon Machine Images （AMI） を予約する方法を説明します。

前提条件

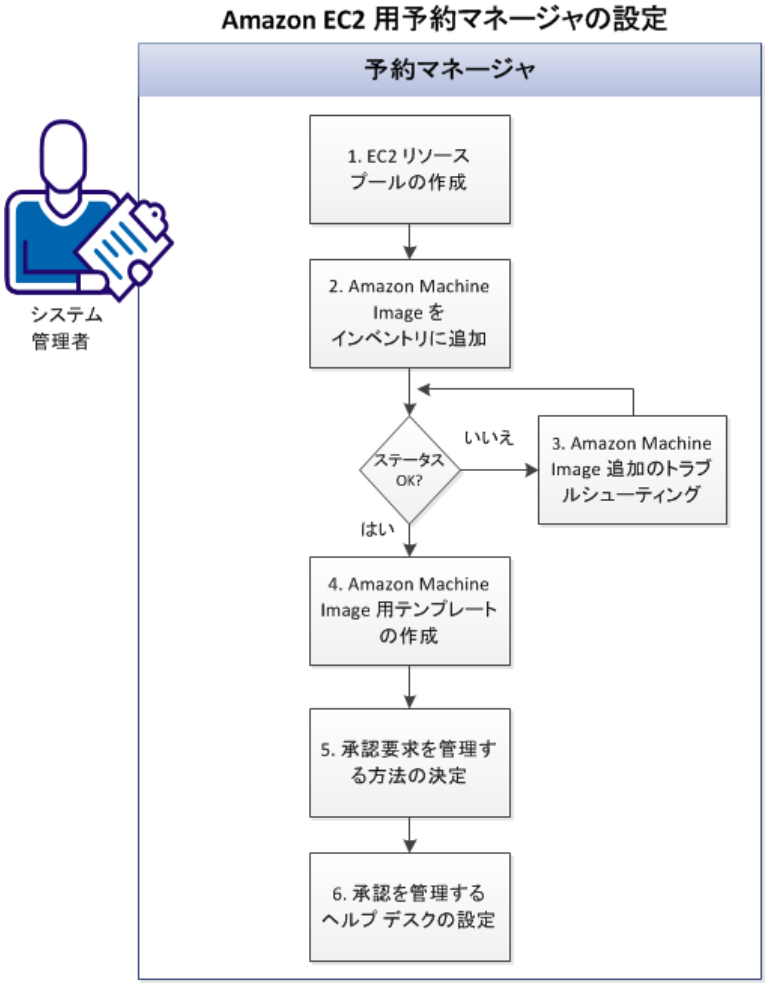
Amazon Machine Image （AMI） を予約用に設定する前に、以下の前提条件を確認してください。

- 予約マネージャ を使用して CA Server Automation が設定されている
- 予約マネージャ の管理ユーザ インターフェースにアクセスできる
- CA Server Automation 管理者の認証情報を持っている
- CA Server Automation で Amazon Elastic Compute Cloud （EC2） 仮想コンピューティング環境が設定されている
- EC2 環境と AMI の一般的な知識がある

Amazon EC2 用の 予約マネージャ の設定

システム管理者は、エンド ユーザが Amazon Elastic Compute Cloud （EC2）から Amazon Machine Image（AMI）を予約できるように 予約マネージャ を設定できます。 このプロセスでは、予約マネージャ の管理者ユーザ インターフェースにすでにログインしていることを前提としています。

以下の図は、AMI を予約に使用できるようにするプロセスを示しています。



次の手順に従ってください:

1. EC2 リソース プールの作成 (P. 1111)
2. Amazon Machine Image をインベントリに追加する (P. 1112)
3. Amazon Machine Image の追加に関するトラブルシューティング（必要な場合） (P. 1113)
4. Amazon Machine Image 用のテンプレートの作成 (P. 1114)
5. ヘルプ デスクの要求を管理する方法の決定 (P. 1115)
6. 承認を管理するためのヘルプ デスクの設定 (P. 1115)

EC2 リソース プールの作成

AMI 予約用の EC2 リソース プールを作成します。

次の手順に従ってください:

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。
2. ［予約マネージャを管理］-［リソース プールを管理］を選択します。
3. ［アクション］をクリックし、ドロップダウン メニューから［EC2 プールの追加］を選択します。
4. プール名と（オプションで）プールの説明を入力し、［次へ］をクリックします。
5. ［リソース プールの作成］ウィザードを使用してプールをセットアップします。

   ［キー ペア名］

   AMI インスタンスへのアクセスに使用されるキー ペア名を定義します。 ドロップダウン リストから 1 つ選択します。

   注: 選択されたキー ペアに関連付けられた秘密鍵ファイルを Linux AMI インスタンスを予約しているユーザに提供してください。 インスタンスが実行されたら、ユーザは秘密鍵ファイルへのパスを指定して実行しているインスタンスへの SSH 接続を開始する必要があります。

[ネットワーク選択]領域:

パブリック

インスタンスが Amazon のパブリック クラウドに展開されることを示します。 オプションで、可用性ゾーンを選択します。 EC2 のベスト プラクティスでは特定のゾーンを選択**しません**が、必要に応じてリストからゾーンを選択できます。

プライベート

クラウド内のプライベート領域である Virtual Private Cloud （VPC）を示します。 サブネットを選択します。

6. 予約をサブミットするときにユーザが要求できる AMI の期間と数に関する制限を指定します。

   最大日数

   予約の長さを指定された日数に制限します。 予約の長さに制限を設定しない場合は、［無制限］を選択します。

   最大システム数

   このプールの中から 1 人のユーザが一度に予約できるインスタンスの数を制限します。

7. 選択された EC2 プールのコンテキストで AMI を開始することを許可されているメンバが属する組織単位を選択し、［終了］をクリックします。

   注:（オプション）このプールから予約をテストできるように、ユーザにアクセス権を付与する前に自分自身にアクセス権を付与してください。 後でアクセス権を付与する場合は、この手順を省略してください。

Amazon Machine Image をインベントリに追加する

ユーザが EC2 から AMI を予約できるように、システム イメージ インベントリに AMI を追加します。

次の手順に従ってください:

1. CA Server Automation 管理者の認証情報を使用して 予約マネージャ ユーザ インターフェースにログインします。
2. ［予約マネージャを管理］-［システム イメージ インベントリを管理 ］を選択します。

3. ［アクション］ドロップダウン メニューから［AMI イメージの追加］を選択し、以下の選択を行います。
   - AMI 用のオペレーティング環境、未分類のイメージを表示する場合は［不明］
   - 選択したオペレーティング環境に基づいたフィルタされたリストからのイメージ
   - （オペレーティング環境に［不明］を指定した場合）不明なイメージを分類するためのオペレーティング環境（［OS の更新］から選択）
   - この AMI のインスタンスを開始するときに使用するデフォルトの［層］名（インスタンス タイプ）
   - 予約をサブミットするときにユーザにデフォルト インスタンス タイプを変更できるようにする場合は、［ユーザ上書きモード］チェック ボックスをオンにします。
   - この AMI が開始されたときに利用可能にする任意のユーザ データ
4. この AMI のインスタンスへのアクセスを設定するために使用されるセキュリティ グループを［選択されたセキュリティ グループ］領域に移動します。 予約をサブミットするときにユーザがデフォルトのセキュリティ グループ設定を変更できるようにするには、［ユーザ上書きモード］チェック ボックスをオンにします。
5. このイメージのインストールを許可されている組織単位を［選択された組織単位］に移動し、［終了］をクリックします。

Amazon Machine Image の追加に関するトラブルシューティング

症状:

［AMI イメージの追加］ウィザードを起動したときに、EC2 サーバが接続されているにもかかわらず、選択できる AMI が存在しません。

解決方法:

デフォルトでは、AMI は、EC2 サーバ接続で指定された所有者のみが使用できます。 パブリック AMI （Amazon で提供されるパブリック AMI など）をユーザが使用できるように、デフォルトを変更できます。 予約マネージャのサーバ上でコマンド プロンプトから dpmutil を実行し、発行されたパブリック AMI をインベントリに追加して EC2 を再構成します。

Amazon Machine Image 用のテンプレートの作成

ユーザが Amazon Elastic Compute Cloud（EC2）で予約を作成できるように、AMI 用の 1 つ以上の予約テンプレートを作成します。

次の手順に従ってください:

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。
2. ［予約マネージャを管理］-［予約テンプレートを管理］を選択します。
3. ［アクション］メニューから［作成］を選択します。
4. ［予約テンプレートの作成］ウィザードを使用して AMI テンプレートを作成します。

   ［名前の指定］ページ

   名前と説明（オプション）を指定します。

   ［システム イメージの指定］ページ

   新しいシステムを展開するために使用できるシステム イメージを一覧表示します。［システム イメージ］リストから AMI イメージを選択します。

   ［要件の指定］ページ

   システム要件を指定します。 作成するインスタンスの数を指定します。（オプション）必要に応じてセキュリティ グループを変更し、別のインスタンス タイプ（サービスの層）を選択します。

   ［アクションの指定］ページ

   （オプション）システムをプロビジョニングする前に、またはプロビジョニングが完了または期限切れになった後で実行するアクションを選択します。

   ［アクセス ポリシーの指定］ページ

   テンプレートへのアクセス権を付与されているメンバが属する組織単位を選択します。

承認要求を管理する方法の決定

予約要求は自動的に承認するか、または手動による承認のために管理者に送信することができます。 要求を自動的に承認するように 予約マネージャ を設定した場合は、リソースが利用可能であれば、予約が直ちに承認されます。 電子メールは送信されません。 予約要求を自動的に承認しないように 予約マネージャ を設定した場合は、ユーザが新しい要求をサブミットすると、電子メール通知が送信されます。それらの要求のステータスは[承認待ち]で、要求を手動で承認または拒否する必要があります。

要求の自動承認は、リソース プールごとに有効になります。特定のリソース プールに対する要求の自動承認を設定するには、［リソース プールの詳細］ページの［アクセス ポリシー］タブで［予約要求を自動承認する］オプションを設定します。

承認を管理するためのヘルプ デスクの設定

オプションで、予約承認を管理するようにヘルプ デスク システムを設定します。

注: この手順は、すべてのプラットフォームに適用されます。

次の手順に従ってください:

1. CA Server Automation 管理者のユーザ認証情報を使用して、予約マネージャ にログインします。
2. ［予約マネージャを管理］-［構成設定を管理］を選択します。
3. ［承認］領域で以下の設定を行います。

   承認時にヘルプ デスク チケットを自動的にクローズ

   予約が承認または拒否されたときにヘルプ デスク チケットを直ちに閉じるかどうかを指定します。

   デフォルト： false（チケットはクローズされません）

   ヘルプ デスク チケット テンプレート

   チケットを開くときに使用されるオプションのチケット テンプレートを指定します。 テンプレートを使用すると、優先度などのチケット属性のデフォルト値を定義できます。

   デフォルト： なし

ヘルプ デスク チケットのタイプ

開かれるチケットのタイプを指定します。

制限： 要求|インシデント|問題

デフォルト： 要求

ヘルプ デスク チケットのオープン

承認が必要な予約要求がサブミットされる場合に、ヘルプ デスク チケットを開くかどうか制御します。 true に設定された場合は、チケットが開かれます。

デフォルト： オフ

電子メール通知のパラメータの設定

管理者は、アプリケーションの展開が成功した時点で、設定されたパラメータ値を含む通知を予約の要求者に送信します。 アプリケーション テンプレートが作成された場合の電子メール通知用にパラメータを選択できます。 予約テンプレートを作成するときに、［電子メール通知に含める］を選択してください。

論理パーティション

IBM PowerVM を使用することによって、管理者はユーザが予約できる論理パーティションを作成できます。 管理者は、論理パーティション用のリソース プールおよびパブリック テンプレートを作成して編集することもできます。

論理パーティションはより大きなシステムの小さなセグメントです。 論理パーティションには独自のオペレーティング システムおよびアプリケーションがあり、相互に独立しています。

関連項目:

IBM PowerVM 論理パーティション用のリソース プールの作成 (P. 1117)
IBM PowerVM 論理パーティション用のリソース プールの編集 (P. 1118)
IBM PowerVM 論理パーティション用のテンプレートの作成 (P. 1119)
IBM PowerVM 論理パーティション用の静的 IP アドレス (P. 1120)
ネットワーク アドレス プールの定義 (P. 1132)
IBM PowerVM 論理パーティションの層単位によるチャージバックの設定 (P. 1166)
IBM PowerVM 論理パーティション用のチャージバック層の選択 (P. 1167)

IBM PowerVM 論理パーティション用のリソース プールの作成

以下の手順では、予約マネージャ 内に IBM PowerVM 論理パーティション用のリソース プールを作成する方法について説明します。

論理パーティション用のリソース プールを作成する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示されます。

2. ［リソース プール］リストの右上角の［アクション］メニューから［IBM PowerVM プールの追加］を選択します。

   ［プールの指定］ページにリソース プールを作成するためのウィザードが表示されます。

3. プロンプトが表示されたら、以下を使用してウィザードの手順を完了します。

   ［論理パーティション リソースの指定］ページ

   このリソース プールに関連付ける IBM PowerVM サーバ（HMC/IVM）を選択します。

   次に［アクション］メニューから［追加］を選択することにより、管理対象システムおよびストレージを追加できます。 層がすべてのサイトで有効になるというわけではないことに注意してください。

予約マネージャ はリソース プールを作成します。

IBM PowerVM 論理パーティション用のリソース プールの編集

以下の手順では、予約マネージャ 内の IBM PowerVM 論理パーティション用のリソース プールで編集できる内容について説明します。

次の手順に従ってください:

1. 管理者として、予約マネージャ の［ホーム］ページで［リソース プールを管理］をクリックします。

   ［リソース プール］ページが開き、テーブルに既存のリソース プールが表示されます。

2. 編集するプールを選択し、［アクション］メニューから［詳細］を選択します。

   ［リソース プールの詳細］ペインが開き、［プロパティ］タブが表示されます。 説明に従って以下のタブに情報を入力するか更新します。

   [プロパティ]タブ

   - 最大システム数
   - 最大日数
   - ドメイン マネージャ
   - スケーラビリティ サーバ
   - 予約要求を自動承認する
   - 論理パーティションの電源状態の管理を許可する

   [リソース プールの詳細]タブ

   IBM PowerVM サーバ（HMC/IVM）、管理対象システム、VIO サーバ、およびこのリソース プールと関連付けられたストレージを追加、編集、または削除します。［アクション］メニューを使用します。

   注: 層がすべてのサイトで有効になるとは限りません。

   [アクセス ポリシー]タブ

   リソース プール内のシステムへのアクセス権が付与されたメンバの組織単位を選択するか削除します。

ユーザに IBM PowerVM 論理パーティションの電源ステータスを管理させる

管理者は、ユーザに IBM 論理パーティションでいくつかの管理タスクを実行する権限を付与することができます。 ユーザは、管理者に連絡することなく論理パーティションの電源ステータスを管理できます。

次の手順に従ってください:

1. CA Server Automation 管理者のユーザ認証情報を使用して、予約マネージャ にログインします。

   ホーム ページが開きます。

2. ［予約マネージャを管理］をクリックします。

   ［管理］ページが開きます。

3. ［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示され、既存のプールがリスト表示されます。

4. リソース プールをダブルクリックします。

   ［リソース プールの詳細］ページが開き、［プロパティ］タブが表示されます。

5. 以下のフィールドの選択をオンまたはオフにします。

   論理パーティションの電源状態の管理を許可する

6. ［OK］をクリックします。

   権限が付与されます。

IBM PowerVM 論理パーティション用のテンプレートの作成

管理者は、一般的に使用されるシステム設定を定義するパブリック テンプレートを作成できます。 新しい IBM PowerVM 論理パーティション用のパブリック テンプレートを定義できます。

IBM PowerVM 論理パーティション用のエンド ユーザのためのパブリック テンプレートを作成する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［予約テンプレートを管理］をクリックします。

   ［予約テンプレート］ページが表示されます。 このページでは、システムを予約するときにユーザが選択できるパブリック テンプレートをリスト表示します。このページから、新しいパブリック テンプレートを作成できます。

2. ［アクション］メニューから［作成］を選択し、ウィザードを完了します。

IBM PowerVM 論理パーティション用の静的 IP アドレス

IBM PowerVM 論理パーティションには静的 IP アドレスが必要です。 これらの IP アドレスは、DNS 解決可能で NIM マスタ上の NIM マシン リソース設定に一致する必要があります。 このリリースでは、動的 NIM マシン リソースの導入により、以下が可能になっています。

- 予約プロビジョニング プロセスの一部として、NIM マシン リソース設定を自動的に作成
- 予約の期限切れまたは取り消し時に削除

管理者は、NIM マスタ上で設定をあらかじめ定義する必要はありません。

注: 既存の NIM マシン リソース設定は引き続き使用され、予約の期限切れまたは取り消し時に削除されません。

重要: ネットワーク アドレス プールは IBM PowerVM に対して一意である必要があります。 IBM PowerVM と同じネットワーク アドレス プールにある仮想マシンに IP アドレス範囲を追加しないでください。

ユーザが予約を作成すると、IP アドレスは管理者が定義した IP アドレスの範囲から割り当てられます。 予約が処理されるかキャンセルされると、IP アドレスはリリースされ、別の予約で利用できるようになります。

関連項目:

ネットワーク アドレス プールの定義 (P. 1132)

IBM PowerVM 論理パーティションの設定

論理パーティション、ディスク サイズ、開始スロット番号、およびその他にデフォルトおよび最大メモリを設定できます。

IBM PowerVM 論理パーティションを設定する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［IBM PowerVM］領域で設定を編集します。

物理システムを利用可能にする

以下のプロセスを使用して物理システムを予約できるようにします。

1. 共有する物理システムが含まれる CA Server Automation サービスを識別します。
2. サービスをインポートして 予約マネージャ リソース プールを作成します。
3. ユーザが利用可能なシステムにインストールできるオペレーティング システム イメージを定義します。
4. リソース プールおよびシステム イメージの両方にアクセス ポリシーをセットアップします。

以下のセクションでは、予約マネージャ を準備して物理システムの予約をサポートする方法について説明します。

物理システムの予約をサポートするための前提条件

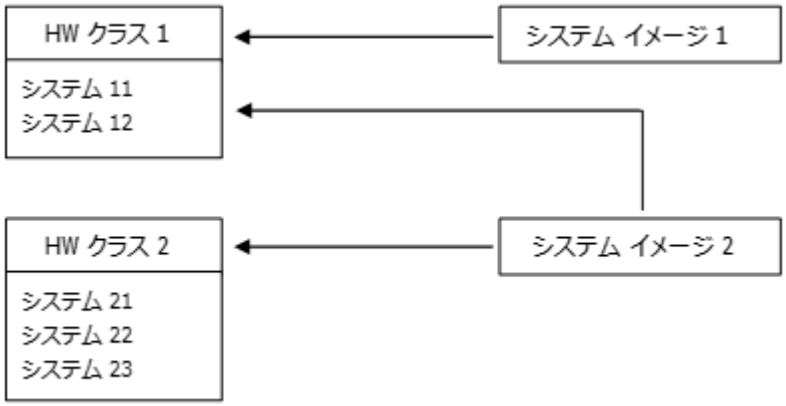
初めて 予約マネージャ にアクセスする前に、CA Server Automation の［リソースの追加］機能を使用し、予約マネージャ インベントリに追加される各システムの 1 回限りのイメージ インストールを実行します。 すべてのシステムが登録された後で、CA Server Automation を使用してサービスを作成し、システムを新しいサービスに追加します。

注:［リソースの追加］機能は、これらのシステムを正常に再イメージ化するために 予約マネージャ が必要とする情報と共に CA Server Automation を設定します。

予約マネージャ が必要なシステム設定の情報を収集するために、インベントリ内のすべてのサーバに 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。 特に、予約マネージャ では、各システムの CPU の数、メモリの量およびディスク領域の量についての情報が必要です。

ハードウェア クラス

ハードウェア クラスの関係では、システムにインストールできるオペレーティング システムを指定します。 これらの関係は、インベントリにシステムおよびシステム イメージを追加する間に作成します。 システムをインベントリに追加したら、そのシステムを 1 つのハードウェア クラスに関連付けます。 ただし、システム イメージをインベントリに追加する場合は、システムを 1 つ以上のハードウェア クラスに関連付けることができます。 以下の例ではそれらの関係を図示します。



システム イメージ 1 は HW クラス 1 に関連付けられているため、システム イメージ 1 はシステム 11 およびシステム 12 に適用できます。

システム イメージ 2 は HW クラス 1 および HW クラス 2 に関連付けられているため、システム イメージ 2 はシステム 11、システム 12、システム 21、システム 22 およびシステム 23 に適用できます。

インベントリのインポートによるリソース プールの作成

リソース プールを CA Server Automation サービスにリンクすることにより、リソース プールを迅速にセットアップできます。

インベントリのインポートによってリソース プールを作成する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示されます。

2. ［リソース プール］リストの右上角の［アクション］ドロップダウンメニューから［インベントリのインポート］を選択します。

   ［インベントリのインポート］ウィザードが表示されます。 ウィザードを使用して、作成した CA Server Automation サービスのメンバである物理システムを 予約マネージャ インベントリに追加します。

3. ［サービスの選択］ウィザード ページに入力し、［次へ］をクリックします。

   予約マネージャ は、CA Server Automation サービスと同じ名前のリソース プールを作成し、CA Server Automation サービス内のすべてのシステムをインベントリにインポートします。 プロセスが正常に完了すると、確認メッセージが表示されます。 ウィザードが終了し、［サービスのインポート］ページが表示され［リソース プール］リストを表示します。

予約マネージャ インベントリのシステムの表示

以下の手順では、予約マネージャ インベントリのシステムを表示する方法について説明します。

予約マネージャ インベントリのシステムを表示する方法

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。

   ［ホーム］ページが開きます。

2. ［予約マネージャを管理］をクリックします。

   ［管理］ページが表示されます。

3. ［システム インベントリを管理］リンクをクリックします。

   ［システム インベントリ］ページが表示されます。予約マネージャ インベントリの各システムに対して、［システム インベントリ］ページにシステム名、ハードウェア クラス、モデル、プロセッサ、CPU の数、メモリの量、場所および各システムのディスク領域の量がリスト表示されます。

   注: CA Configuration Automation エージェントがこれらのシステムにインストールされている場合、CPU、メモリ（メガバイト単位）およびディスク領域（メガバイト単位）の値は、すでに設定されています。CA Configuration Automation エージェントのないシステムでは、ユーザがシステムを予約できるようになる前に、これらの属性を設定します。

4. （オプション）システムについての詳細が必要な場合は、［名前］列のシステム名をクリックします。

   選択されたシステムに対して［システムの詳細］ページが表示され、システムのプロパティおよび関連付けられたリソース プールを表示します。［プロパティ］タブは、場所、シリアル番号、IP アドレスおよび MAC アドレスなどの追加情報を提供します。

システムの属性値の変更

ユーザがシステムの予約を開始する前に、予約マネージャ インベントリ内のシステムの属性値を設定します。

注: これらのシステムに CA Configuration Automation エージェントがインストールされている場合、関連する多数の属性値がすでに設定されている場合があります。

システムの属性値を変更する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［システム インベントリを管理］をクリックします。

   ［システム インベントリ］ページが表示されます。予約マネージャ インベントリの各システムに対して、［システム インベントリ］ページにシステム名、ハードウェア クラス、モデル、プロセッサ、CPU 数、メモリ容量、場所、およびシステムのディスク領域の容量がリスト表示されます。

2. 属性値を変更するシステム名の隣にあるチェック ボックスをオンにし、次に、［アクション］メニューから［詳細］を選択します。

   選択したシステムの［システムの詳細］ページが開き、以下のタブが表示されます。

   - プロパティ
   - リソース プール

3. ［プロパティ］をクリックし、必要に応じて設定を変更します。
4. ［リソース プール］タブをクリックし、必要に応じてそのシステムで選択されたリソース プールのリストを変更します。
5. ［OK］をクリックします。

   予約マネージャ は変更を保存して［システムの詳細］ページを閉じます。［システム インベントリ］ページが開き、選択したシステムに設定された属性が表示されます。

関連項目:

ハードウェア クラス (P. 1122)
物理システムの予約をサポートするための前提条件 (P. 1121)

JumpStart ブート サーバの定義

ユーザが Solaris システム イメージのインストール要求を許可される場合、管理者は必要な JumpStart ブート サーバを識別できるように 予約マネージャ を設定する必要があります。

予約マネージャ は、ユーザ用にセットアップされたサーバで Solaris オペレーティング システムのインストールを開始するのに Solaris JumpStart ブート サーバ技術を使用します。 予約マネージャ は複数の JumpStart ブート サーバおよびインストール サーバを保有する環境をサポートするため、ユーザに割り当てることができるシステムをサポートするには、すべての JumpStart ブート サーバを識別する必要があります。

JumpStart ブート サーバを定義する方法

1. 予約マネージャ［ホーム］ページ上の管理者として、［JumpStart ブート サーバを管理］をクリックします。

   ［JumpStart ブート サーバ］ページが表示されます。 JumpStart ブート サーバが定義されるまで、このページには最初は空のテーブルが表示されます。JumpStart ブート サーバがすでに追加されている場合、ページには利用可能な JumpStart ブート サーバおよび関連付けられた IP マスク、説明および場所がリスト表示されます。

2. ［アクション］メニューから［追加］を選択し、ウィザードの指示に従います。

オペレーティング システム イメージのユーザへの提供

1 つ以上のオペレーティング システム イメージをユーザが選択できるようにする必要があります。

オペレーティング システム イメージを利用可能にする方法

1. 管理者として、予約マネージャ の［ホーム］ページで［システム イメージ インベントリを管理］をクリックします。

   ［システム イメージ］ページが表示されます。 このページでは、システムの予約時にユーザが選択できるオペレーティング システム イメージおよび仮想マシン テンプレートのインベントリがリスト表示されます。 このページから、ユーザが利用できるように提供するオペレーティング システム イメージまたは仮想マシン テンプレートを定義できます。

2. ［アクション］ドロップダウン メニューから［イメージの追加］を選択し、ウィザードの指示に従います。

   ［システム イメージ］ページが表示されて、インベントリに正常に追加されたオペレーティング システム イメージをリスト表示します。

KVM および Xen イメージ（Windows のみ）：

システム イメージ用のカスタム仕様ファイルでは、システム設定が必要です。 システム イメージを作成する際、このシステム イメージに以下のシステム設定情報を指定します。

名前

システム設定データの名前を指定します。

製品キー

VM オペレーティング システムの製品キーを指定します。

組織

組織情報を指定します。

ネットワーク グループまたはドメイン:

ネットワーク グループに参加するには、［ネットワーク グループ］の名前を指定します。

ドメインに参加するには、［ドメイン名］、［ドメイン ユーザ］、［ドメイン パスワード］、および［ドメイン パスワードの確認］を指定します。

1 回実行コマンド

仮想マシンで実行するコマンド ラインを指定します。

関連項目:

ハードウェア クラス (P. 1122)

システムを予約

特定の日付に使用できるように割り当てられたリソース プールから物理システムを予約できます。 オペレーティング システム、ソフトウェアおよびハードウェアなどのシステム要件を定義します。 予約マネージャは、十分なリソースが存在することを確認し、リソースの可用性およびプロビジョニングをスケジュールします。

システムを予約するには、［予約マネージャ］ユーザ インターフェースのホーム ページから［システムを予約］をクリックし、ウィザードの手順を完了します。

サービスをユーザから利用可能にする

以下のプロセスを使用して、サービスをユーザが予約に利用できるようにします。

1. リソース プールへのユーザ アクセスを識別および確立します。
2. サービス テンプレートへのユーザ アクセスを識別および確立します。

以下のセクションでは、予約マネージャ を使用してサービスの予約をサポートする方法について説明します。

サービス リソース プールの設定

予約マネージャ は、サービスをプロビジョニングするときにリソース プールを使用します。

CA Server Automation インターフェースからサービスをプロビジョニングする場合は、以下のデフォルトのオンデマンド リソース プールが使用されます。

オンデマンド リソース

仮想リソースが含まれたリソース プール。 CA Server Automation での使用のために Virtual Center が設定されると、このプールにリソースが自動的に追加されます。

オンデマンド EC2 リソース

EC2 リソースが含まれたリソース プール。CA Server Automation での使用のために EC2 が設定されると、このプールにリソースが自動的に追加されます。

デフォルトでは、サービス管理者の組織単位にはこれらのプールへのアクセス権があります。 管理者は、必要に応じてこれらのプールからリソースを削除したり、アクセス ポリシーを変更したりすることができます。

デフォルトのリソース プールは、予約マネージャ で自動的に利用可能になります。予約マネージャ では、必要に応じて、カスタマイズされたサービスやユーザ アクセスを備えた追加のリソース プールを作成できます。

エンド ユーザがサービスの予約を作成するには、少なくとも 1 つのリソース プールへのアクセス権が必要です。組織単位のメンバシップによって、リソース プールへのユーザ アクセスが決定されます。

サービス用のテンプレートの作成

サービスの予約は、予約テンプレートによってのみ作成されます。 サービス パラメータは、サービス テンプレートが作成された時点で定義されます。 管理者は、予約マネージャ で予約を作成するときに、これらのパラメータ値を上書きできます。 これらのパラメータは、システムが割り当てられるときにサービスを正しく設定するために使用されます。

CA Server Automation インターフェースでサービス テンプレートが作成されると、予約マネージャ 用のサービス テンプレートが自動的に作成されます。 また、予約マネージャ インターフェースを使用してサービス テンプレートを作成または変更することもできます。

注: サービス用のシステム イメージを作成する必要はありません。

予約マネージャ でサービス テンプレートを作成する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［予約テンプレートを管理］をクリックします。
2. ［アクション］ドロップダウン メニューから［サービスの作成］を選択します。

   ［サービスの作成］ウィザードが表示されます。 ウィザードの指示に従います。

エンド ユーザ用のパブリック テンプレート

管理者は、システムを割り当てる方法を決定するエンド ユーザ用のパブリック テンプレートを作成できます。 テンプレートは予約要求を処理する新しい仮想マシンを作成するために使用されます。

予約マネージャ は、テンプレートを作成するためのウィザードを提供します。

関連項目:

イメージ タイプ用のテンプレートの作成 (P. 1130)
VMware 仮想マシン用のテンプレートの作成 (P. 1106)
IBM PowerVM 論理パーティション用のテンプレートの作成 (P. 1119)

イメージ タイプ用のテンプレートの作成

管理者は、1 つ以上のテンプレートを作成してユーザが予約を作成できるようにします。 システム イメージが Amazon EC2、Citrix XenServer、KVM、Microsoft Hyper-V、または VMware 以外のイメージ タイプである場合は、テンプレートを作成できます。

システム イメージ タイプのテンプレートを作成するには、予約マネージャ の［予約テンプレートを管理］オプションの右上角にある［アクション］メニューから［作成］をクリックし、

ウィザードを完了します。

グループ テンプレートの作成

管理者は、個々の予約テンプレートを包括してシステムの完全なアプリケーションの設定を作成することができます。 仮想リソースを使用する場合、管理者は特定の仮想リソース プールをターゲットにして、すべての仮想マシンが同じリソース プールで作成されるかどうか決定できます。

注: 管理者は、仮想マシンの作成時にユーザが管理パスワードを設定することを許可できます(「ユーザによる管理タスクの実行 (P. 1137)」を参照)。グループ テンプレートを使用して予約が行われた場合、ユーザはパスワードを指定することを許可されません。

グループ テンプレートを作成するには、予約マネージャの［予約テンプレートを管理］オプションの［アクション］メニューで［グループの作成］ウィザードを完了します。

静的 IP アドレスの使用

予約マネージャ では、静的 IP アドレスを使用して、仮想マシンへのプロビジョニングやその他のネットワーク タスクを実行できます。 デフォルトでは、予約マネージャ は Dynamic Host Configuration Protocol （DHCP）を使用しますが、管理者は静的 IP アドレスを使用するよう製品を設定できます。

ユーザが予約を作成すると、IP アドレスは管理者が定義した IP アドレスの範囲から割り当てられます。 予約が処理されるかキャンセルされると、IP アドレスはリリースされ、別の予約で利用できるようになります。

静的 IP アドレスを使用するように 予約マネージャ を設定するには、以下の手順に従います。

ネットワーク アドレス プールの定義 (P. 1132)

VMware カスタマイズの仕様を作成します。 (P. 1133)

静的 IP アドレスの有効化 (P. 1134)

ネットワーク アドレス プールの定義

サイトで静的 IP アドレスを有効にするための最初の手順は、製品のメイン ユーザ インターフェースでネットワーク アドレス プールを定義することです。ネットワーク アドレス プールは IP アドレスの範囲で構成されます。

注: 予約マネージャ では、予約に使用されているネットワーク アドレス プールを編集または削除することはできません。 IP アドレス範囲などを変更する必要がある場合は、新しいネットワーク アドレス プールを作成します。 また、VM または論理パーティションと関連付けられたネットワークを削除することはできません。

ネットワーク アドレス プールを定義する方法

1. Web ブラウザで以下の URL を入力し、管理者の認証情報を使用してログインします。

   `https://server:port`

   注: デフォルト ポートは 8443 です。

   製品のメイン インターフェースが表示されます。

2. ［リソース］をクリックします。
3. 左ペイン内のデータ センターをクリックし、［管理］-［ネットワーク アドレス プールの管理］を選択します。

   ［ネットワーク アドレス プール］ダイアログ ボックスが表示されます。

4. ［+］（新規）をクリックし、必須フィールド（［ネットワーク アドレス プール名］、［IP アドレス］、［サブネット マスク］、および［VLAN ID］）に情報を入力します。 ［次へ］をクリックします。

   ネットワーク情報の入力用に新しいページが表示されます。

5. 必須フィールド（［デフォルト ゲートウェイ］、［優先 DNS サーバ］、および［ドメイン名］）に情報を入力します。 必須でないフィールドは省略可能です。 ［次へ］をクリックします。

   IP アドレス範囲用のダイアログ ボックスが表示されます。

6. 必須フィールド（［開始 IP アドレス］、［終了 IP アドレス］、および［タイプ］（［静的］を選択））に情報を入力します。 ［追加］をクリックします。

   注: ネットワーク アドレス プールを定義する際、静的 IP アドレス範囲が別のタイプのデータ センターに割り当てられていないことを確認してください。

   ［仮想ホスト］ペインが表示されます。

7. 1 つ以上の仮想ホストを選択し、［追加］をクリックして、［終了］をクリックします。

   注: 仮想ホスト上に作成された VM に IP アドレスを割り当てるには、事前に各仮想ホストをネットワークと関連付けておく必要があります。

   注: この手順は、プールの作成時には省略可能です。 ただし、予約を作成する前に実行する必要があります。

   ネットワーク アドレス プールが作成されます。

   注: ユーザに明示的にアクセスを許可するまで、ネットワーク アドレス プールにはアクセスできません。 手順については、「VLAN スコーピング (P. 1151)」を参照してください。

VMware カスタマイズの仕様およびテンプレートの作成

VMware vCenter または vSphere では、静的 IP アドレスを有効にするカスタマイズの仕様およびテンプレートを作成します。 静的 IP アドレスで予約を作成する際には、これらの仕様とテンプレートを使用する必要があります。

注: VMware カスタマイズの仕様およびテンプレートを作成する方法の詳細については、VMware ドキュメントを参照してください。

これらのアイテムを作成する際には、以下の情報を考慮してください。

- **カスタマイズの仕様** -- ネットワーク インターフェース（NIC）のカスタマイズでは、IP アドレスを指定する必要があります。 カスタマイズの仕様では、任意の IP アドレスの値を指定できます。 仮想マシンは、この仮想マシン用に選択されたネットワーク IP アドレス プールの中から、使用されていない IP アドレスで設定されます。 NIC のカスタマイズでは、NIC に［DHCP を使用］を指定しないでください。

静的 IP アドレスの有効化

［ネットワーク選択を許可］フィールドの値を［true］に設定することによって、静的 IP アドレスを有効にします。［予約マネージャを管理］-［構成設定を管理］に移動し、［予約］領域を開いて［ネットワーク選択を許可］フィールドを見つけます。

リソース プールとテンプレートに関する考慮事項

仮想マシンの 予約マネージャ でリソース プールおよびテンプレートを作成する際、必ず静的 IP アドレスの情報を入力します。

リソース プール

作成したネットワーク アドレス プールに接続された ESX サーバを指定します。

テンプレート

静的 IP の設定が含まれた VMware カスタマイズの仕様を指定します。

関連項目:

ネットワーク アドレス プールの定義 (P. 1132)
VMware カスタマイズの仕様およびテンプレートの作成 (P. 1133)

電子メール通知の設定

予約マネージャ は、エンド ユーザおよび管理者に重要なイベントの電子メール通知を送信できます。 管理者に電子メール通知を送信する例としては、新しい仮想マシンのための十分なスペースがデータ ストアにない場合などです。

インストール後の構成を実行して電子メール サポートをアクティブ化します。CA EEM が外部ディレクトリを使用するように設定されている場合、CA EEM は自動的にユーザの電子メール アドレスを取得します。 外部ディレクトリのサポートなしで CA EEM を使用している場合、CA EEM 管理者はユーザの電子メール アドレスを指定する必要があります。

電子メール通知を設定するには、予約マネージャの［構成設定を管理］オプションの［通知］領域で設定を行います。

ユーザに予約準備完了を通知する電子メールのカスタマイズ

予約に関連付けられたシステムが完全に設定されて準備が完了した場合、予約マネージャ はエンド ユーザに電子メール通知を送信できます。また、予約済みシステムの管理者またはルート パスワードをこの電子メール通知で送信するかどうか指定することもできます。 電子メールのテキストはカスタム メッセージを表示できます。 たとえば、予約済みシステムにログインするためには認証情報が必要であることを示すようにこのメッセージを設定できます。

ユーザに予約準備完了を通知する電子メールをカスタマイズするには、予約マネージャの［構成設定を管理］オプションの［通知］領域で以下の設定を行います。

- 予約準備完了テキスト
- 予約準備完了メールにパスワードを明記

ユーザへの終了通知の期間の指定

予約の終了時刻が接近している場合、予約マネージャ はユーザに 1 つの電子メール通知を送信するか、または複数の時間間隔で繰り返し通知を送信することができます。 終了時間に比例して通知が送信されるように設定できます。 デフォルトでは、通知は予約終了時刻の 24 時間前に送信されます。

ユーザへの終了通知の期間を指定するには、予約マネージャで［構成設定を管理］に移動し、［予約期限切れ警告時刻］設定を設定します。

ジョブが失敗した場合にユーザに通知する電子メールの設定

予約に関連付けられたプロビジョニング ジョブが失敗した場合、予約マネージャ はエンド ユーザに電子メール通知を送信できます。 デフォルトでは管理者のみがプロビジョニングの失敗について通知を受け取ります。

ジョブが失敗した場合にユーザに通知する電子メールを設定する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［通知］領域で以下のリンクをクリックし、値を変更して［OK］をクリックします。

   ジョブ エラーをエンド ユーザに通知

   設定変更は、次に予約が作成されるときに有効になります。

停滞したタスク アラートを送信する時間の指定

タスクが予想以上に時間がかかっているとき、予約マネージャ は管理者に電子メール アラートを送信できます。 タスクの最後のステータス更新からの経過時間が受信され、現在の時間が定義された時間間隔を超える場合、アラートが送信されます。

この時間間隔は設定できます。デフォルトでは 2 時間です。 この設定は、オペレーティング システム イメージング、ソフトウェア インストールなどを含む、すべてのタスクのタイプに適用されます。 そのため、通常のタスクがすべて完了するように時間間隔を十分に長く設定します。

停滞したタスク アラートを送信する時間を指定する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［通知］領域で以下のリンクをクリックし、値を指定して［OK］をクリックします。

   タスク ステータス更新タイムアウト

   設定変更は、次に予約が作成されるときに有効になります。

アナウンスメントの設定

予約マネージャ はエンド ユーザ ホーム ページ上にオプションの［アナウンスメント］ペインを表示できます。 アナウンスメントを使用して、計画された停止や計画されていない停止、新しいシステムやイメージのサポートなど、重要な操作上の情報やニュースをユーザに通信します。

アナウンスメントを設定する方法

1. 管理者として、予約マネージャ の［ホーム］ページで［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［一般］領域で以下のリンクをクリックします。

   Announcements

3. Announcements.html が配置されているディレクトリを開き、テキストを変更します。

   重要: アナウンスメント ファイルを編集する場合は、UTF-8 エンコーディングで保存してください。英語以外のオペレーティング システムでは、マルチバイト文字は UTF-8 エンコーディングで保存される必要があります。 Windows のメモ帳を使用して UTF-8 エンコーディングで保存できます。

4. ファイルを保存して閉じます。

   アナウンスメントの変更は、ブラウザを再起動するときに行われます。

ユーザによる管理タスクの実行

管理者は、ユーザに VMware 仮想マシンでいくつかの管理タスクを実行する権限を付与することができます。 その後、ユーザは管理者に連絡することなく以下の手順を実行できます。

- 仮想マシンの作成時に管理パスワードを変更する。
- 仮想マシンの電源ステータスを制御する。 管理者は、ユーザに割り当てられている仮想マシンの電源オン、電源オフまたは中断をユーザが実行するように設定できます。
- 仮想マシンのスナップショットを作成します。 *スナップショット*は、ある時点における仮想マシンの記録です。
- 元のプロビジョニングの後に仮想マシンの設定を変更します。

ユーザが一部の管理タスクを実行できるようにするには、予約マネージャの［リソース プールを管理］オプションで目的の設定を選択します。 目的のリソース プールをダブルクリックし、各フィールドの選択をオンまたはオフにします。

予約済みシステムへのユーザ アクセス

予約マネージャ を使用してシステムを予約するユーザは、予約済みシステムにアクセスするためのユーザ名とパスワードを知っている必要があります。 デフォルトでは、予約マネージャ は予約通知電子メールにユーザ名とパスワードが含まれます。 予約マネージャ はこの電子メールに含めるユーザ名とパスワードを決定する必要があります。

予約マネージャ は、システムにソフトウェアを展開するためのユーザ名とパスワードも知っている必要があります。 ソフトウェアの展開に使用される管理者アカウント名は、スーパーユーザとして 予約マネージャ に定義されている権限のあるユーザです。 スーパーユーザ アカウント名およびパスワードは dpmutil -set -superuser コマンドを使用して、インストール中に、またはインストール後に定義できます。 スーパーユーザ アカウント名は各オペレーティング システムに定義される必要があります。 ただし、単一のオペレーティング システム環境（たとえば Windows）に定義できるのは 1 つのスーパーユーザ アカウント名のみです。 この単一のアカウント名は、ソフトウェアを展開するために新しくイメージされたシステムにアクセスする場合に使用されます。 任意のオペレーティング環境で、システムが異なる管理者アカウント名で設定されている場合、予約マネージャ に既知の定義されたスーパーユーザ アカウント名で設定されていないシステムにソフトウェアを展開しようとすると、失敗します。展開の問題を回避するためには、アカウントをセットアップして、そのオペレーティング システム環境のスーパーユーザとして定義されたアカウント名をサポートするようにすることを推奨します。 あるいは、そのシステム イメージの選択時にエンド ユーザにソフトウェアのインストールを許可しないようにします。

以下のセクションでは、予約マネージャ が有効な認証情報を確定する方法について説明します。

JumpStart プロビジョニング パスワードの設定

Solaris オペレーティング システムのベア メタル プロビジョニングは Solaris JumpStart 技術を使用して実装されます。 ターゲット Solaris コンピュータに設定されているルート パスワードは JumpStart sysidcfg 設定ファイルでハッシュされたパスワードとして定義されます。 予約マネージャ が使用するすべての Solaris OS イメージは同じルート パスワードを使用するように設定される必要があります。

Hyper-V Windows プロビジョニング パスワードの設定

Hyper-V 環境では、すべてのユーザに同じ認証情報を付与して Windows システムにアクセスできるようにしたり、予約要求をサブミットする場合にユーザが固有のパスワードを選択できるようにセットアップすることができます。 リソース プール レベルで使用するポリシーを指定します。

ユーザに固有のパスワードの選択を許可しない場合は、*dpmutil set superuser* コマンドを発行します。 このコマンドは後で取得できるようにデータベース内に Windows 管理者パスワードを保存します。 例：

```
dpmutil -set -superuser
```

コマンドは管理者権限のある認証情報を要求するプロンプトを表示します。

予約マネージャ は、ユーザにシステムの準備完了を通知する電子メールを送信するときにパスワードを取得します。 指定するパスワードは、Windows システムのプロビジョニングで使用するために Hyper-V OS プロファイルで指定した任意のパスワードを上書きします。

［*管理者パスワードの指定を許可する*］オプションがリソース プールに設定されている場合、予約を作成するユーザは VM に設定されている管理者パスワードを入力できます。

Hyper-V OS プロファイルで指定されたすべてのパスワードが上書きされます。

OSIM プロビジョニング パスワードの設定

Linux と Windows オペレーティング システムのベア メタル プロビジョニングは、CA IT Client Manager OS Installation Management 技術（OSIM）によって実装されます。 OS イメージを OSIM ライブラリに追加する場合、定義する必要があるパラメータのうちの 1 つはターゲット システムのルート パスワードまたは管理者パスワードです。 すべての Windows OS イメージは同じ管理者パスワードを使用するように設定される必要があり、すべての Linux OS イメージは同じ root パスワードを使用するように設定される必要があります。

NIM プロビジョニング パスワードの設定

AIX オペレーティング システムのベア メタル プロビジョニングは IBM Network Installation Management 技術（NIM）を使用して実装されます。ターゲット AIX マシンの設定に使用されるルート パスワードは、CA Server Automation NIM アダプタと共にインストールされる ca_post_install.sh スクリプトでハッシュされたパスワードとして定義されます。 すべての AIX OS イメージは同じ root パスワードが使用されるように設定する必要があります。

VMware Windows プロビジョニング パスワードの設定

VMware 環境では、すべてのユーザに同じ認証情報を付与して Windows システムにアクセスできるようにしたり、予約要求をサブミットする場合にユーザが固有のパスワードを選択できるようにセットアップすることができます。 リソース プール レベルで使用するポリシーを指定します。

ユーザが固有のパスワードを選択するように許可されていない場合は、dpmutil set superuser コマンドを発行して後で取得できるように Windows 管理者パスワードをデータベースに保存します。 例：

```
dpmutil -set -superuser
```

コマンドは管理者権限のある認証情報を要求するプロンプトを表示します。

予約マネージャ は、ユーザにシステムの準備完了を通知する電子メールを送信するときにパスワードを取得します。 指定するパスワードは、Windows システムのプロビジョニングに使用するために VMware カスタマイズの仕様で指定されたパスワードと一致する必要があります。

カスタマイズの仕様は VMware Infrastructure Client を使用して定義されます。 この方法を使用する場合は、テンプレートを作成するときに使用される仮想マシン用の管理者パスワードは、空白か空の値に設定される必要があります。 空白に設定された場合、カスタマイズの仕様で定義されたパスワードは仮想マシンのプロビジョニング中に設定されます。

仮想マシン テンプレートを 予約マネージャ インベントリに追加する場合は、保存されたカスタマイズの仕様を各テンプレートに関連付けます。すべての Windows カスタマイズの仕様が同じ管理者パスワードを使用するように設定する必要があります。

ユーザが固有のパスワードを選択するように許可されている場合、Windows 管理者アカウントはユーザが入力したパスワードで設定されます。パスワードは暗号化され、他の予約データと共に保存されます。ユーザ指定のパスワードは、カスタマイズの仕様で定義されたパスワードを上書きします。空白の管理者パスワードを使用する VM テンプレートをセットアップするための要件でも、エンド ユーザに固有のパスワードを指定させる必要があります。

VMware Linux プロビジョニング パスワードの設定

Linux VM 用のルート パスワードは、テンプレートに変換される前に、仮想マシンに定義されたパスワードです。すべての Linux 仮想マシン テンプレートが同じルート パスワードを使用するように設定する必要があります。

以下のコマンドを発行し、後で取得できるようにデータベースに Linux ルート パスワードを格納します。 コマンドは情報を入力するようにプロンプトを表示します。

```
dpmutil -set -superuser
```

予約マネージャ は、ユーザにシステムの準備完了を通知する電子メールを送信するときにパスワードを取得します。

EC2 Windows プロビジョニング パスワードの設定

AMI の起動時に Windows インスタンス用の管理者パスワードが生成されます。各 Windows インスタンスに一意のパスワードが割り当てられます。インスタンスを開始するときに使用される秘密鍵は、管理者パスワードを取得して解読するために必要です。

この要件をサポートするために、予約マネージャ では、秘密鍵が dpmutil set ec2-private-keypair コマンドを使用して設定される必要があります。 予約マネージャ は、Windows インスタンスが実行されていることを検出した場合、保存された秘密鍵を使用してパスワードを取得するアクションを開始します。 Windows 管理者パスワードは、システムを要求したエンドユーザに送信される電子メール通知に含まれています。

インスタンスを開始するときに使用される秘密鍵は、新規インスタンスが関連付けられる EC2 リソース プールによって決定されます。

注: dpmutil set superuser コマンドで定義された Windows 管理者パスワードは、Windows インスタンスへのアクセスには使用されません。

EC2 Linux プロビジョニング パスワードの設定

Linux OS を実行している AMI インスタンスは SSH を使用してアクセスされます。 ssh コマンドを発行したり、PuTTY のような SSH ツールを使用する場合は、ユーザは、インスタンスを開始するために使用された秘密鍵でインスタンスにログインする必要があります。 エンド ユーザに対して秘密鍵を利用可能にするのは 予約マネージャ ではありません。 管理者がエンド ユーザに秘密鍵を提供する責任を担います。EC2 リソース プールは、インスタンスを開始するために使用される秘密鍵を決定します。したがって、1 つのサイトで複数の秘密鍵を使用できます。別の EC2 リソース プールを作成し、それらに異なる秘密鍵を割り当ててアクセスを制限します。各グループのメンバにアクセス権がある EC2 リソース プールに割り当てられた秘密鍵ファイルを提供します。

注: dpmutil set superuser コマンドで定義された Linux ルート パスワードは、Linux インスタンスへのアクセスには使用されません。

ユーザ管理

ユーザの制限と権限を設定および指定する必要があります。 このセクションには、ユーザ設定のための手順が含まれています。

組織単位

組織単位 (org unit) はユーザのグループです。組織単位は、リソース プール、ソフトウェア グループ、システム イメージおよびテンプレートのようなオブジェクトにユーザ アクセス権を付与することにより、セキュリティを提供します。

組織単位については、以下の情報を考慮します。

- ユーザは複数の組織単位に所属できます。ユーザは、予約マネージャ ウィンドウの左上で［*所属先*］リンクをクリックすることにより、別の組織単位に切り替えることができます。
- リソースへのアクセスは各組織単位に応じて調整できます。
- 組織単位のメンバシップは、CA EEM ユーザの以下のプロパティに基づいて設定することができます。 予約マネージャ 管理者は CA EEM セットアップを複製する必要はありません。
  - ユーザが属するグローバル グループ
  - ユーザが属する CA アプリケーション グループ
  - 部門、会社、オフィス、市区町村、都道府県または国などの属性。したがって、北米のセールス サポートのすべてのユーザは「セールス」という名前の組織単位のメンバにすることができます。
- 管理者が組織単位からユーザを削除する場合、そのユーザは組織単位内で以下のいずれかの状況が発生するまで作業を続行できます。
  - ユーザはログアウトして再度ログインします。
  - ユーザは、［*所属先*］リンクをクリックして組織単位を変更します。
- CA EEM はネイティブ、Active Directory および LDAP をサポートします。
- デフォルトでは、すべてのユーザがパブリック組織単位のメンバです。明示的にユーザをパブリック組織単位に追加しないでください。 すべての CA EEM グローバル ユーザが予約要求を行えるようにするには、リソース アクセスをパブリック組織単位に追加します。パブリック組織単位の権限が、特定の組織単位の権限に追加されます。

  重要: デフォルトのパブリック組織単位を無効にすることができます。パブリック組織単位を無効にする場合は、組織単位ごとの予約権限を明示的に指定する必要があります。
- ユーザがそれらを容易に識別できるように、組織単位に説明的な名前を使用します。

組織単位の作成

組織単位は、リソース プールおよびテンプレートのような 予約マネージャ 機能にユーザ アクセス権を与えます。

組織単位を作成する方法

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。

   ［ホーム］ページが開きます。

2. ［予約マネージャを管理］リンクをクリックします。

   ［管理］ページが表示されます。

3. ［組織単位を管理］をクリックします。

   ［組織単位］ページが表示されます。

4. リストの右上隅にある［アクション］メニューから［追加］を選択します。

組織単位へのユーザの追加

CA EEM ユーザを既存の組織単位に追加できます。

組織単位にユーザを追加する方法

1. CA Server Automation 管理者のユーザ認証情報を使用して、予約マネージャ にログインします。

   ［ホーム］ページが開きます。

2. ［予約マネージャを管理］リンクをクリックします。

   ［管理］ページが表示されます。

3. ［組織単位を管理］をクリックします。

   ［組織単位］ページが表示されます。

4. 組織単位を選択し、次に、リストの右上角の［アクション］メニューから［詳細］を選択します。

   ［組織単位の詳細］ページが表示されます。 このページには、組織単位設定を変更できるいくつかのタブが含まれています。

5. ［メンバ］をクリックします。

6. 検索するプロパティのタイプ（ユーザまたはユーザ属性）、検索する属性および演算子を選択します。 値を入力し、［検索］をクリックします。

   予約マネージャ から CA EEM に対して、検索条件に一致するすべてのユーザまたは属性を求めるクエリが実行され、［利用可能なユーザ/属性］リストに結果が表示されます。

   注: LIKE 演算子には、暗黙的なワイルドカード検索が含まれます。 完全一致を取得するには、EQUAL 演算子を使用してください。

7. ユーザまたは属性を選択して、右方向キー をクリックして名前を［ユーザの選択］リストへ移動し、［OK］をクリックします。

   予約マネージャ は、選択したユーザまたは属性を組織単位に追加し、確認メッセージを表示します。

マルチテナント環境

テナントは、ユーザとリソースのコレクションです。テナント ユーザは、すべての CA EEM グローバル ユーザのサブセットです。 テナント リソースは、CA Server Automation によって検出され、管理されるすべてのリソースのサブセットです。

テナントのある環境では、管理者には以下の 2 つのタイプがあります。

- スーパー管理者
- テナント管理者

スーパー管理者は、予約マネージャ の管理タスクをすべて実行できます。スーパー管理者は、テナントに含まれるユーザを指定したり、各テナントの管理に 1 人以上のテナント管理者を指定したりします。このため、大規模な環境では、スーパー管理者が日常業務の一部をテナント管理者に委任することができます。

テナント管理者は、テナントに属するリソースのみを管理できます。 これらの管理者は、テナント内のユーザを代表して管理タスクのサブセットを実行します。

テナントに属するエンド ユーザは 予約マネージャ のユーザのみです。これらのユーザは 予約マネージャ にログインして、予約要求を行います。

スーパー管理者

スーパー管理者は、ユーザ グループ AIPAdmins のメンバであるため、CA Server Automation と 予約マネージャ の両方の管理タスクをすべて実行できます。

スーパー管理者は、テナント ユーザ、リソース、および管理者を定義するオブジェクトと設定の作成を担当します。 スーパー管理者が新しいテナントを定義するには、以下の手順に従います。

- CA Server Automation でテナント用のサービスを 1 つ以上作成します。テナント物理コンピュータ システムをこれらのサービスに追加します。
- CA Server Automation からテナント サービスをインポートすることで、予約マネージャ 内にテナント用の物理リソース プールを 1 つ以上作成します。
- 予約マネージャ 内にテナント用の仮想リソース プールを 1 つ以上作成します。

  注: このタイプのプールを作成すると、予約マネージャ によって CA Server Automation 内に同じ名前のサービスが自動的に作成されます。その後、エンド ユーザが仮想リソース プールに仮想マシンを作成すると、予約マネージャ によって対応するサービスに VM が自動的に追加されます。

- 予約マネージャ 内にテナントを作成し、リソース プールへのアクセスを指定し、管理者とユーザを指定します。
- 予約マネージャ 内にテナント用のシステム イメージ、ソフトウェア グループ、および予約テンプレートを作成します。 これらのオブジェクトは、テナントによって所有されるリソース、またはテナントのメンバが利用できるリソースを参照する必要があります。テナントのメンバが予約要求を行う際に、これらのリソースが使用されます。

  注: テナント管理者も予約テンプレートを作成できます。 スーパー管理者が作成したテンプレートは、1 つ以上のテナントに割り当てることができます。 テナント管理者が作成したテンプレートは、そのテナントのメンバのみが使用します。
- テナント管理者がこれらのオブジェクトへのアクセス権をテナント ユーザに付与できるように、予約マネージャ 内のテナントにこれらのオブジェクトへのアクセス権を付与します。
- 各テナントで利用できるネットワーク定義を指定します。
- テナントを表示または非表示したり、テナント名で表示をフィルタしたりします。

テナントの保守は、テナント ユーザとリソースの変更に対して、以下のように、それまでの設定を適合させることで行います。

- テナント管理者を保持します。
- 必要に応じて、サービスを変更し、CA Server Automation 内にテナント用のサービスを新規作成します。
- 必要に応じて、予約マネージャ 内にテナント用のシステム イメージ、ソフトウェア グループ、および予約テンプレートを変更または作成します。
- 必要に応じて、リソースへのテナント アクセスを変更します。
- 必要に応じて、テナント内のメンバシップを変更します。

注: スーパー管理者は、テナント用の組織単位を作成できません。テナント管理者のみが、テナント メンバ用の組織単位の作成を担当します。 ただし、スーパー管理者がテナントを作成すると、予約マネージャ はそのテナント用の 1 つの組織単位を自動的に作成します。この新しいデフォルトの組織単位には、そのテナントと同じ名前が付けられます。 テナント作成時にそのテナントに割り当てられたリソースはすべて、デフォルトの組織単位に割り当てられます。

テナントの追加

スーパー管理者は、テナントの新規作成、テナント管理者とエンド ユーザの追加、およびリソース プールやその他のリソースへのアクセス権の付与を実行できます。

テナントを追加するには、［テナントを管理］オプションの［アクション］メニューの［追加］オプションでウィザードを完了します。

テナントの編集

スーパー管理者は、テナントのプロパティ、管理者とエンド ユーザ、およびリソース プールへのアクセス権を編集できます。

テナントを編集するには、予約マネージャ の［テナントを管理］オプションでテナントをクリックし、表示されるタブ内の情報を更新します。

テナント管理者

*テナント管理者*には、限られた（つまり、範囲が決められた）役割が与えられており、アクセスできる範囲は、ある 1 つのテナントに所属するユーザとリソースに限られています。

スーパー管理者はテナントを定義し、テナントのメンバシップ、テナントがアクセスできるリソース、およびテナントを管理するユーザを指定します。

テナント管理者の役割は、次のとおりです。

- スーパー管理者によって作成され、テナントに割り当てられた物理および仮想リソース プールを表示し、変更します。 テナント管理者は、リソース プールに対して、次のアクションを実行できます。
  - ユーザが予約できるシステムの数を制限する
  - ユーザがマシンを予約できる時間を制限する
  - VM の命名規則を指定する
  - 予約に手動の承認が必要かどうかを指定する
  - ユーザが Windows 管理者パスワードを設定できるかどうかを指定する
  - ユーザが VM の電源操作を発行できるかどうかを指定する

- ユーザが VMware 仮想マシンのスナップショットを作成できるかどうかを指定する
- VM の解放時に、VM が削除されるかどうか指定する
- メモリの超過割り当てのレベルを指定する

注: 複数のテナントでリソース プールを共有している場合、テナント管理者はプールの設定を変更できません。 テナント管理者は、プールとその設定を表示し、プールをテナントの組織単位に割り当てることができます。

リソース プールがテナント専用として割り当てられている場合、テナント管理者は一部のプール設定を変更できません。 テナント管理者は、CA ITCM （ITCM ドメイン マネージャとスケーラビリティ サーバ）、vCenter（フォルダ配置）、および Amazon クラウド（キー ペア名とネットワーク選択）を変更できません。 ただし、テナント管理者はこれらの設定を表示できます。

テナント管理者は、リソース プールを作成または削除することはできません。

- 組織単位を作成して管理します。組織単位は、テナント メンバの 予約マネージャ リソースへのアクセス権を定義するのに使用します。 リソースのタイプには予約テンプレート、システム イメージ、リソース プール、ソフトウェア グループなどがあります。テナントがアクセスできるリソースは、テナントの組織単位に割り当てることができます。

  テナント管理者は、組織単位にテナント メンバおよびネットワーク定義を追加できます。

- 予約テンプレートを作成して、管理します。 テナント管理者は、テナント メンバが予約時に使用するテンプレートの作成、変更、削除を行えます。 組織単位は、テンプレートへのメンバのアクセス権を制御します。

- 指定されたサービス内のリソースに基づく予約に対して、操作を実行します。テナント管理者は、予約に対して次のアクションを実行できます。
  - 予約要求を承認または拒否する
  - 予約を延長する
  - 予約をキャンセルして、リソースを解放する
  - 予約のステータスを確認する
  - 予約タスクを再起動またはスキップする
- システム インベントリを表示し、指定されたサービスから取得されたリソース プールに属するシステムの可用性を確認する

テナント管理者がホーム ページ上で［予約マネージャを管理］をクリックすると、次のリンクが表示されます。テナント管理者は、これらのリンクを使用して、前述のすべてのタスクを実行できます。

- すべての予約を表示
- システム インベントリを管理
- リソース プールを管理
- 予約テンプレートを管理
- 組織単位を管理

テナントのエンド ユーザ

予約マネージャ のテナント ユーザは、テナントに属さないユーザとまったく同じようにシステムを利用できます。組織単位内のメンバシップによって、テナント ユーザが予約をするときに使用できる予約テンプレート、システム イメージ、ソフトウェア グループ、および物理システムが決まります。

VLAN スコーピング

予約マネージャ 管理者は、エンド ユーザの選択対象としてアクセス可能な VLAN をスコープする必要があります。 これは、各組織単位のメンバにアクセス可能なネットワーク アドレス プールを指定することにより実行されます。

VLAN へのアクセス権を付与する方法

1. ［管理］-［組織単位を管理］を選択します。
2. 新しい組織単位を追加するか、または既存の組織単位を開きます。
3. ［ネットワーク アクセス］タブに移動し、1 つ以上の VLAN を選択します。

管理

環境を設定、管理、およびカスタマイズするためのいくつかの操作を実行できます。 このセクションの手順では、サイトに 予約マネージャ の設定を合わせる方法について説明します。

ほとんどの設定はユーザ インターフェースの［構成設定］ページにあります。 このページでは、「承認」や「通知」などの名前を持つグループへの設定を編成します。 各グループには、設定の詳細な説明が含まれていて、値を変更できるダイアログ ボックスへのリンクがあります。グループを展開するか折り畳むことができます。

予約マネージャ ユーザ インターフェースへのアクセス

予約マネージャ ユーザ インターフェースにアクセスして組織単位、ユーザ アクセス、システムおよび仮想マシン可用性を設定し、また、予約で使用されるサポートされたソフトウェア、イメージおよびテンプレートを設定します。

ユーザ インターフェースにアクセスする方法

1. 予約マネージャ サーバ上で［スタート］-［プログラム］-［CA］-［CA Server Automation］-［CA Server Automation 予約マネージャ の起動］を選択します。

   予約マネージャ ログイン ページが以下の URL で表示されます。

   `https://servername:port/ssrm/`

   servername

   予約マネージャ サーバの名前を指定します。

   port

   サーバがリスンしているポートを指定します。

   デフォルト： 8443

2. 管理者ログイン認証情報を入力し、［ログイン］をクリックします。

   ［ホーム］ページが表示されます。

3. ［予約マネージャ を管理］をクリックします。このリンクは管理者のみに利用可能です。

   ［管理］ページが表示されます。このページからすべての管理タスクを実行します。

［スタート］メニューのショートカットは 予約マネージャ サーバでのみ利用できます。個別のサーバからインターフェースにアクセスするユーザは、Web ブラウザで URL を入力する必要があります。

フィルタで表示されるデータ

ユーザ インターフェースに表形式でデータが表示される場合、テーブルの各列のフィルタ条件を定義できます。その後、テーブルは必要な量のデータのみを表示します。

表示されたデータをフィルタする方法

1. ［フィルタ］ペインで［コンテンツを表示］をクリックします。

   フィルタ ペインが展開され、表示されたデータをフィルタするのに使用できるパラメータ フィールドが表示されます。

2. 適切なフィルタ条件を指定し、［フィルタの適用］をクリックします。

   テーブルはフィルタ条件に応じてデータを表示します。

予約要求の承認または拒否

予約要求を自動的に承認しないように 予約マネージャ を設定している場合、ユーザが新規要求をサブミットした後に 予約マネージャ から電子メール通知を受信します。その要求のステータスは［承認待ち］となり、要求を手動で承認または拒否する必要があります。

要求を自動的に承認するように 予約マネージャ を設定している場合、予約マネージャ は電子メールを送信しません。要求されたリソースが利用可能な場合、予約はすぐに承認されます。

予約要求を手動で承認または拒否する方法

1. CA Server Automation 管理者のユーザ認証情報を使用して、予約マネージャ にログインします。

   ［ホーム］ページが開きます。

2. ［予約マネージャを管理］をクリックします。

   ［管理］ページが表示されます。

3. ［すべての予約を表示］をクリックします。

   ［予約の表示］ページが表示されます。

4. ［承認待ち］ステータスが表示されている要求を選択し、［アクション］メニューから［詳細］を選択します。

   ［予約の詳細］ページが表示されます。 CA SDM の統合がセットアップされている場合、ヘルプ デスク チケットへのハイパーリンクはこのページに含まれています。 ヘルプ デスク チケットを承認または拒否するには、CA SDM、または 予約マネージャ の［アクション］メニューのいずれかを使用します。

5. 予約要求を確認し、［アクション］をクリックして、要求を承認または拒否します。

   予約マネージャ は［予約の表示］ページに戻り、更新されたステータスが表示されます。

関連項目:

承認待ち要求通知を送信する時間の指定 (P. 1191)
未承認予約の自動取り消しの設定 (P. 1192)

予約の延長

予約の終了日より前に予約を延長する必要があります。そうしないと、リソースはリソース プールに返却されます。

予約を延長するには、予約の詳細の［アクション］メニューから［延長...］を選択します。

要求したリソースが使用できない場合や、許可される最大のシステム数に達した場合は、要求が拒否されます。 管理者は、延長の拒否を無効にして、延長を許可することができます。

可用性の確認により、終了日を超えて予約を延長するための十分なリソースがないと判定された場合は、管理者に通知されます。 管理者は、予約を延長して可用性の確認の警告を無効にしても安全かどうかを判断します。

リソース割り当ておよび予測チャート

リソース割り当ておよび予測チャートを使用すると、予約マネージャ 管理者は、分析のためにリソース割り当てを表示できます。

- 割り当てチャートには、リソースの現在の使用状況が表示されます。
- 予測チャートには、指定した期間内のスケジュールされた予約に基づいて予測された使用状況が表示されます。

注: 予約マネージャ は、Amazon EC2、Citrix XenServer、Huawei GalaX、または KVM についてはリソース数が無制限とみなし、リソース割り当ておよびリソース割り当て予測の機能を提供しません。

リソース割り当てを表示する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. リソース プールのチェック ボックスをオンにして、［アクション］ドロップダウン メニューから［リソース割り当て］をクリックします。

   リソース割り当てチャートが表示されます。

   注: テーブル ヘッダにある［チャートの表示］または［テーブルの表示］ボタンをクリックすると、チャートまたはテーブルが表示されます。

3. チャートを表示し、［現在のチャート ビュー］ドロップダウン オプションから目的の条件を選択します。

4. チャートにカーソルを合わせるか、またはチャート内のバーをクリックします

   ホスト情報が表示されます。

   注: テーブル ビューでは、同じ情報のホストにカーソルを合わせるか、または選択します。

予測に関して、管理者は開始時刻と終了時刻のほか、データを時間単位、日単位、月単位のいずれで表示するかを指定できます。 データを日単位または月単位で表示する場合、その期間のピークの予約済みリソースが表示されます。

割り当て予測を表示する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. リソース プールのチェック ボックスをオンにして、［アクション］ドロップダウン メニューから［割り当て予測］をクリックします。

   リソース割り当て予測チャートが表示されます。

3. ドロップダウン リストから以下のフィールド用のデータを選択します。

   表示基準

   時間、日または月に基づいたデータを提供します。

   開始時刻

   開始日と時間を指定します。

   終了時刻

   終了日と時間を指定します。

4. ［チャートのリフレッシュ］をクリックします。

   チャートに、選択した値に基づいたリソース割り当てが表示されます。

頻繁に使用されるレポートの実行

メイン インターフェースからすべての利用可能なレポートを実行できますが、頻繁に使用されるレポートは 予約マネージャ 管理者インターフェースから実行することもできます。 管理インターフェースからレポートを実行すると、予約マネージャ リソース プールのコンテキストでレポートを起動することができます。

頻繁に使用されるレポートを実行する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］リストが表示されます。

2. 1 つのリソース プールを選択し、［アクション］をクリックして［レポート］を選択します。

   注: 複数のリソース プールを選択する場合は、［レポート］オプションが利用できません。

   ［レポートの作成］ダイアログ ボックスが表示されます。

3. フィールドに入力し、［OK］をクリックします。

   レポートが別のウィンドウに表示されます。

タスク スケジューリングの中断と再開

予約マネージャ には、システム保守中にジョブが実行されないようにするため、スケジュールされた予約タスクの開始を管理者が中断できるスケジューラ機能があります。 保守が完了したら、管理者はスケジューラ操作を再開して、中断したタスクの処理を開始できます。

スケジューラが一時停止すると、まだ開始されていないすべての OS プロビジョニング、ソフトウェア展開、および終了処理のタスクが中断されます。 さらに、予約セットアップ ワークフローまたは期限切れ処理ワークフローの一部として実行される予定の、予約テンプレート内で指定されているプレアクション、ポストアクション、および有効期限アクションもすべて中断されます。

スケジューラを中断する時点で進行中であった予約タスクは停止されません。 進行中のタスクの完了後に実行するようにスケジュールされた予約タスクは、スケジューラが再開されると開始されます。 たとえば、スケジューラが中断されたときに仮想マシンが展開されていると、スケジューラが中断されている間はそれ以降のタスク（ポストアクションやソフトウェア展開タスクなど）が開始されません。

スケジューラの中断後に実行される保守アクティビティに 予約マネージャ または CA Server Automation サービスの停止が含まれる場合は、進行中のすべての予約タスクがサービス停止の前に完了するように時間を計算することをお勧めします。 これによって、進行中のタスクの成功または失敗を 予約マネージャ でモニタできることが保証されます。

以下の操作はスケジューラの中断による影響を受けません。

- 仮想マシンの電源状態を変更する、スナップショットを作成または元に戻す、および仮想マシンの再設定を行うユーザ要求
- スケジューラが中断している間でも、新しい予約は受け入れられますが、プロビジョニングの新しい予約はリリースされません

計画的に停止する場合は、停止期間中に期限切れになる予約を延長するための時間を与えるため、ユーザに事前に通知してください。 停止中は予約を延長できない場合があります。 計画された停止期間より長く予約を延長することをお勧めします。 スケジューラが中断している間に期限切れになる予約は、スケジューラが再開されるとすぐに処理されます。

すべてのプロビジョニング タスクを中断して再開する方法

1. CA Server Automation 管理者の認証情報を使用して、予約マネージャ にログインします。

   注: 予約マネージャ が保守のためにオフラインであるというメッセージが表示される場合があります。 ディスプレイ最下部の［管理者ログイン］をクリックします。

   ［ホーム］ページが開きます。

2. ［*予約マネージャ を管理する*］リンクをクリックします。

   ［管理］ページが表示されます。

3. ディスプレイ右上の［保守］リンクをクリックします。

   ダイアログ ボックスが開き、以下のオプションが示されます。 1 つまたは両方を選択または選択解除します。

   保留中の予約タスクを中断

   Web アクセスをブロック（保守モード）

4. 保守が完了したら、［OK］をクリックします。

   注: 保守が 1 日以上続く場合は、保守が完了するまで、これらの手順を繰り返します。

個別タスクの中断および再起動

予約マネージャ は、プロビジョニング タスクが現在の状況下で失敗する可能性があることを検出すると、自動的にタスクを中断します。 このような場合、管理者は問題が存在し、解決する必要があることを示す電子メール通知を受信します。 たとえば、予約マネージャ は仮想マシンをプロビジョニングする前に十分なディスク領域が利用可能かどうかを確認します。 ディスク領域が不十分な場合は、展開タスクが自動的に中断されます。 管理者は、中断されたタスクを再起動する前にディスク領域の問題を解決する必要があります。

システムが中断した*個別*のプロビジョニング タスクを再起動する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［すべての予約を表示］をクリックします。

   ［予約の表示］ページが表示されます。［ジョブ ステータス］列にジョブが中断されていることが表示されます。

2. 再起動する予約の隣のチェック ボックスをオンにし、［アクション］メニューをクリックして［詳細］をクリックします。

3. ［ジョブ ステータス］列のリンクをクリックしてジョブを再開します。

4. 中断されたジョブを選択し、［アクション］メニューをクリックし、［選択されたタスクから再起動］を選択します。

   ジョブが再起動されます。

チャージバック

CA Server Automation は、Amazon EC2、IBM PowerVM （LPAR）、Microsoft Hyper-V および VMware vCenter のチャージバックをサポートします。 チャージバック機能は、仮想マシンの使用を時間レートでチャージする方法を提供します。 CA Server Automation は、2 種類の価格設定の方式をサポートします。 物理システムおよび仮想マシン用のチャージバック方式では、個々の CPU、メモリ、および予約済みディスク リソースに対するチャージ設定が可能です。 サポートされている各プラットフォームには、これらのメソッドの 1 つに基づく固有の価格設定モデルがあります。 Amazon EC2 インスタンスおよび IBM PowerVM 論理パーティションのチャージバック方法は、*層ベースの価格設定*を使用します。 すべてのチャージバック モデルのデフォルトは 0（時間単位でのチャージなし）ですが、管理者は値を変更できます。 また、使用量チャージを示すレポートも利用できます。

注: チャージバック レコードは一日の最後（午前零時以降）に作成されます。 オプション［過去 24 時間］では前日からのコストを取得します。

予約を作成すると、コストが表示されます。 予約要件を変更する場合、予約要求をサブミットする前に金額を再計算できます。

注: チャージバックの使用の有無、一日あたりのコストを計算する頻度、計算データを保持する日数および使用する通貨を制御できます。「チャージバックの設定 (P. 1162)」を参照してください。

リソース単位のチャージバック

物理システムおよび仮想マシン（Hyper-V および VMware）用のチャージバック ポリシーは、予約されているリソースに基づきます。 これは定額の時間レートにすることができますが、以下の状況（組み合わせは任意）に対して追加料金を適用することもできます。

- CPU の数または基本のしきい値を超える CPU
- メモリの各 GB またはしきい値を超えるメモリの GB
- ディスク領域の各 GB またはしきい値を超えるディスク領域の GB

チャージバック ポリシーの例として、時間レートが 25 セントで、複数の CPU、2 GB のメモリおよび 10 GB の領域を使用する場合は追加料金がかかります。

注: ストレージ層が許可される場合は、ディスク領域に対して追加料金を使用することができません。 代わりに、時間レートが各層に割り当てられます。 したがって、チャージバックはストレージ層単位または追加料金のいずれか一方になります。層の詳細については、「ユーザにストレージ層の選択を許可 (P. 1192)」を参照してください。

Amazon EC2 用の層単位のチャージバック

Amazon EC2 については、チャージバック ポリシーは利用可能な追加料金のない、時間あたりの定額料金で、以下のインスタンス タイプに基づきます。

- c1.medium
- c1.xlarge
- cc1.4xlarge
- m1.small
- m1.large
- m1.xlarge
- m2.xlarge
- m2.2xlarge
- m2.4xlarge
- t1.micro

IBM PowerVM 論理パーティション用の層単位のチャージバック

IBM PowerVM 論理パーティションについては、チャージバック ポリシーは利用可能な追加料金のない、時間あたりの定額料金です。 CA Server Automation には以下の層があります。

- lpar.Large
- lpar.Medium
- lpar.Small

管理者は必要に応じてテンプレートの作成または編集時に追加することができます。

関連項目:

リソース単位のチャージバックの設定 (P. 1162)
ストレージ層のチャージバックの設定 (P. 1164)
Amazon EC2 の層単位によるチャージバックの設定 (P. 1165)
IBM PowerVM 論理パーティションの層単位によるチャージバックの設定 (P. 1166)
IBM PowerVM 論理パーティション用のチャージバック層の選択 (P. 1167)

チャージバックの設定

チャージバックが使用されるかどうか、コストがどれくらいの頻度で計算されるか、および使用する通貨を制御できます。

チャージバックを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［チャージバック］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   チャージバック計算の通貨

   チャージバック計算の頻度

   チャージバックの保持

   チャージバックは有効です

ログアウトして再度ログインしたときに、設定の変更は有効になります。

リソース単位のチャージバックの設定

リソース単位のチャージバックは、物理システムおよび仮想マシン（Hyper-V および VMware）で予約されたリソースへの請求に使用される方法です。

チャージバック レートを割り当てる場合、予約期間の間、チャージは 1 日 24 時間週 7 日間課せられることに留意してください。 エネルギー コストやハードウェア維持費などの要素に基づいて現実的な時間レートおよび追加料金を入力します。 レートは、1 時間あたり 10 セントから 50 セントになる場合が多数です。

注: チャージバックはオプションです。 デフォルトのレートは 0（チャージバックなし）です。

リソース単位のチャージバックを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の下にある［チャージバック モデルを管理］をクリックし、モデルを選択して［アクション］メニューから［詳細］を選択します。

   リソース チャージバックのペインが表示されます。

2. 以下のフィールドに値を入力します。

   - ［**基本時間レート**］（例： $0.15）
   - ［**基本メモリ (GB)**］（例： 1）
   - ［**基本ディスク (GB)**］（例： 10）
   - ［**基本 CPU**］（例： 1）

   注: ストレージ層が許可されている場合は、［基本ディスク (GB)］および［追加ディスク］は後に続く手順で利用できません。 代わりに時間レートがストレージ層に入力されます。 「ストレージ層のチャージバックの設定 (P. 1164)」を参照してください。

3. （オプション）以下の追加料金を任意の組み合わせで入力します。 前の手順で入力した基本のしきい値を超過すると、追加料金が課されます。 チェック ボックスを使用して追加料金をアクティブにします。

   - ［**追加メモリ**］（例： $0.01）
   - ［**追加ディスク**］（例： $0.01）
   - ［**追加 CPU**］（例： $0.05）

     注: ストレージ層が許可されている場合、追加料金は利用できません。 代わりに、時間レートが各層に割り当てられます。 したがって、チャージバックはストレージ層単位または追加料金のいずれか一方になります。 層の詳細については、「ユーザにストレージ層の選択を許可 (P. 1192)」を参照してください。

4. ［OK］をクリックします。

ストレージ層のチャージバックの設定

ストレージ層のチャージバックでは、物理システムおよび仮想マシン（Hyper-V および VMware）上の各層に異なるレートを課すことができます。

ストレージ層は各ディスクに関連付けられたデータ ストアの分類です。層は、通常、VM とそのハード ドライブが作成されるデータストアの各種レベルのパフォーマンスを示しています。 管理者はストレージ層を有効または無効にできます。

管理者がストレージ層を有効にすると、ユーザは仮想マシンの予約時にそれらを選択できます。「ユーザにストレージ層の選択を許可 (P. 1192)」を参照してください。

チャージバック レートを割り当てる場合、予約期間の間、チャージは 1 日 24 時間週 7 日間課せられることに留意してください。 エネルギー コストやハードウェア維持費などの要素に基づいて現実的な時間レートおよび追加料金を入力します。 レートは、1 時間あたり 10 セントから 50 セントになる場合が多数です。

注: チャージバックはオプションです。 デフォルトのレートは 0（チャージバックなし）です。

ストレージ層のチャージバックを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の下にある［チャージバック モデルを管理］をクリックし、モデルを選択して［アクション］メニューから［詳細］を選択します。

   リソース チャージバックのペインが表示されます。

2. 以下のフィールドに値を入力します。
   - ［**基本時間レート**］（例： $0.15）
   - ［**基本メモリ (GB)**］（例： 1）
   - ［**基本 CPU**］（例： 1）

3. （オプション）以下の時間単位の追加料金を任意の組み合わせで入力します。 前の手順で入力した基本のしきい値を超過すると、追加料金が課されます。チェック ボックスを使用して追加料金をアクティブにします。
   - ［**追加メモリ**］（例： $0.01）
   - ［**追加 CPU**］（例： $0.05）
4. ストレージ層のディスク領域の時間レートを入力します。
5. ［OK］をクリックします。

関連項目:

ユーザにストレージ層の選択を許可 (P. 1192)

Amazon EC2 の層単位によるチャージバックの設定

層単位のチャージバックは、Amazon Cloud インスタンスの予約に対する請求に使用される方法です。

チャージバック レートを割り当てる場合、予約期間の間、チャージは 1 日 24 時間週 7 日間課せられることに留意してください。 エネルギー コストやハードウェア維持費などの要素に基づいて現実的な時間レートを入力します。 レートは、1 時間あたり 10 セントから 50 セントになる場合が多数です。

注: チャージバックはオプションです。 デフォルトのレートは 0（チャージバックなし）です。

Amazon EC2 用の層単位のチャージバックを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の下にある［チャージバック モデルを管理］をクリックし、［Amazon Cloud インスタンス］をクリックします。

   層チャージバックのペインが表示されます。

2. チャージバック用のインスタンス タイプを選択し、時間レートを入力します。 インスタンス タイプを以下に示します。
   - c1.medium
   - c1.xlarge
   - m1.large
   - m1.small
   - m1.xlarge
   - m2.xlarge
   - m2.2xlarge
   - m2.4xlarge
   - t1.micro
3. ［OK］をクリックします。

IBM PowerVM 論理パーティションの層単位によるチャージバックの設定

層単位のチャージバックは、IBM PowerVM 論理パーティションの予約に対する請求に使用される方法です。

チャージバック レートを割り当てる場合、予約期間の間、チャージは 1 日 24 時間週 7 日間課せられることに留意してください。 エネルギー コストやハードウェア維持費などの要素に基づいて現実的な時間レートを入力します。 レートは、1 時間あたり 10 セントから 50 セントになる場合が多数です。

注: チャージバックはオプションです。 デフォルトのレートは 0（チャージバックなし）です。

IBM PowerVM 論理パーティション用の層単位のチャージバックを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の下にある［チャージバック モデルを管理］をクリックし、［IBM 論理パーティション］をクリックします。

   層チャージバック用のフィールドを備えたペインが表示されます。

2. チャージバック用の層を選択し、時間レートを入力します。デフォルトの層は以下に示すとおりですが、管理者がテンプレートの作成または編集時にこれよりも多くの層を定義している場合があります。
   - lpar.Large
   - lpar.Medium
   - lpar.Small
3. ［OK］をクリックします。

IBM PowerVM 論理パーティション用のチャージバック層の選択

チャージバックがサイトで使用されている場合は、IBM PowerVM 論理パーティション用のテンプレートを開いて、チャージバック層を選択できます。

IBM PowerVM 論理パーティション用のチャージバック層を選択する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［予約テンプレートを管理］をクリックします。

   ［予約テンプレート］ページが表示されます。このページでは、システムを予約するときにユーザが選択できるパブリック テンプレートをリスト表示します。

2. 論理パーティション用のテンプレートをダブルクリックします。

   ［予約テンプレートの詳細］ページが表示されます。

3. ［割り当てポリシー］タブをクリックし、［チャージバック層名］ドロップダウン リストから層を選択します。

   注: 新しい名前を入力することにより、新しいチャージバック層を作成することもできます。新しいすべての層に時間レートを必ず設定してください。「IBM PowerVM 論理パーティション用の層単位のチャージバックの設定 (P. 1166)」を参照してください。

チャージバックの表示の設定

チャージバック機能は、仮想マシンの使用を時間単位でチャージできる方法を提供します。 製品には VMware および Amazon Cloud の価格モデルが付属しています。 デフォルトは 0（時間ごとのチャージなし）で、管理者は値を変更できます。

チャージバックを使用しない場合、管理者は時間レートと合計コストの表示を隠してエンド ユーザに表示されないようにすることができます。

チャージバックの時間レートと合計コストの表示を隠す方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［予約］領域で以下のリンクをクリックします。

   チャージバック コスト情報の表示

3. 値を入力し、［OK］をクリックします。

   ブラウザを再起動するときに、変更は有効になります。

カスタマイズ

標準の設定とセットアップに加えて、予約マネージャ をカスタマイズすることができます。 このセクションには、サービスやリソースをカスタマイズする方法に関する手順が含まれています。

連絡先ハイパーリンクの設定

各 予約マネージャ Web ページの右上角にハイパーリンクを設定できます。これにより、管理上のサポートまたはテクニカル サポートを要求できます。 リンクのラベルと URL が設定されている場合のみ、リンクが表示されます。 デフォルトでは、連絡先ハイパーリンクは表示されません。

連絡先ハイパーリンクを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［一般］領域で以下のリンクをクリックします。表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   管理者連絡先名

   管理者連絡先 URL

ブラウザを再起動すると、設定の変更は有効になります。

予約マネージャ モバイル アプリケーションの使用

CA 予約マネージャ モバイル アプリケーションを使用すると、モバイル デバイスから予約タスクを実行できます。

モバイル アプリケーションを iPhone または iPad にダウンロードできます。

Apple の App Store で「CA Mobile 予約マネージャ」を検索し、この無料のアプリケーションをダウンロードします。

モバイル アプリケーションは、以下の機能を提供します。

My Systems

現在および将来予約しているシステムを一覧表示します。

Recents

過去の予約を表示し、新しい予約を作成できます。

Announcements

予約マネージャ のホーム アナウンスメント画面情報を表示します。

Settings

モバイル アプリケーションの設定。

次の手順に従ってください：

1. モバイル アプリケーションを起動します。
2. ［Settings］オプションで以下の情報を指定します。
   - 予約マネージャ のサーバ名
   - ポート番号。 デフォルトは 443 です。
   - 予約マネージャ のユーザ ID とパスワード。
   - 使用している電子メール アドレス。

3. ［Test Connection］をタップして情報を確認します。
4. 複数の組織単位のメンバである場合は、使用する組織単位をタップして選択します。

オンライン ヘルプの設定

予約マネージャ では、ホーム ページの一番上に、オンライン ヘルプを開く［ヘルプ］リンクが表示されます。 デフォルトでは、［ヘルプ］リンクは 予約マネージャ ヘルプに移動します。 管理者は、URL のカスタマイズまたはエントリの削除ができます。

オンライン ヘルプの設定方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。
2. ［一般］領域で以下のリンクをクリックします。

   エンド ユーザ ヘルプ
3. 値を入力し、［OK］をクリックします。

   ブラウザを再起動するときに、変更は有効になります。

ホーム ページのカスタマイズ

デフォルトでは、エンド ユーザは、予約マネージャ ホーム ページ上で以下のリンクへのアクセス権があります。

- システムを予約
- 仮想マシンを作成
- Amazon Cloud に新しい仮想マシンを作成
- 予約テンプレートを表示
- システム インベントリを表示
- 予約を表示

管理者は、これらのいずれかのリンクへのアクセスを削除することにより、このページでユーザに表示されるオプションをカスタマイズできます。たとえば、定義されたパブリック テンプレートに基づいた予約要求のみをユーザが作成するように希望するとします。 この場合は、［システムを予約］、［仮想マシンを作成］、および［システム インベントリを表示］リンクをホーム ページから削除します。

注:［予約マネージャ を管理する］リンクはエンド ユーザに対して利用可能にすることはできません。 このリンクは管理者ユーザにのみ表示されます。

ホーム ページをカスタマイズする方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［クイック スタート］領域で以下のリンクをクリックします。各々に値を変更できるダイアログ ボックスが表示され、［OK］をクリックします。これらのオプションのうちのいずれかを false に設定すると、対応するリンクがエンド ユーザ ホーム ページから削除されます。

   マシン アクセスの予約

   VM アクセスの予約

   AMI アクセスの作成

   テンプレート アクセスの表示

   予約アクセスの表示

   マシン アクセスの表示

ブラウザを再起動すると、設定の変更は有効になります。

ホーム ページでの短い説明の設定

管理者は、ホーム ページのタスクの説明を短くする（一文）かどうか設定できます。

ホーム ページに短い説明を設定する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［クイック スタート］領域で以下のリンクをクリックします。

   短い説明の使用

3. 値を変更して、［OK］をクリックします。

ブラウザを再起動すると、設定の変更は有効になります。

電子メールのカスタマイズ

予約マネージャ には、HTML 通知電子メール用のテンプレートがあります。これらのテンプレートを使用することで、管理者は、電子メールのテキストをカスタマイズし、代替変数を使用して、サーバ名、現在の時刻などの動的な情報を含めることができます。

ジョブが成功したことを通知する電子メールは、青色のバーで色分けされているため、ジョブが実行されたことがひとめでわかります。 ジョブが失敗したことを通知する電子メールは、オレンジ色のバーで色分けされます。

関連項目:

ディレクトリ構造 (P. 1172)
テンプレートと電子メールのタイプ (P. 1173)
代替変数 (P. 1174)
電子メールのタイプとカテゴリ (P. 1177)
条件付きの代替変数 (P. 1179)
電子メール通知のパラメータの設定 (P. 1116)

ディレクトリ構造

テンプレートは、ディレクトリ %INSTALL_ROOT%/MailTemplates に置かれ、その後に（ISO-639-1 標準に基づく）2 文字の言語コード、テンプレートのファイル名が続きます。 たとえば、英語のテンプレートのパスは次のとおりです。

%INSTALL_ROOT%/MailTemplates/en/*template_name*.html

テンプレートと電子メールのタイプ

テンプレートのファイル名は、電子メールのタイプに基づきます。 電子メールのタイプとは、電子メールが自動生成される状況のことです。 たとえば、次のような状況があります。

RESERVED_SYSTEM_READY

RESERVED_SYSTEM_TERMINATION_WARNING

RESERVATION_READY

RESERVATION_ABOUT_TO_EXPIRE

RESERVATION_EXPIRED

RESERVED_SYSTEM_READY という電子メールのタイプに対応するテンプレートは、RESERVED_SYSTEM_READY.html です。

テンプレート ファイルは、XHTML を使用して記述されます。 すべてのテンプレートに共通の CSS ファイルが 1 つあり、この CSS ファイルが（外部スタイル シートとしてではなく、直接） HTML 電子メール メッセージに埋め込まれます。1 つの CSS ファイル（styles.css）を編集すれば済むため、効率的にカスタマイズできます。

注: styles.css を削除しないでください。

重要: テンプレート ファイルを編集する場合は、UTF-8 エンコーディングで保存してください。 英語以外のオペレーティング システムで、マルチバイト文字を使用している場合は、UTF-8 エンコーディングで保存する必要があります。 Windows のメモ帳では、UTF-8 エンコーディングで保存できます。

代替変数

テンプレート ファイルには、以下のように、代替変数を含めることができます。

システム名: %SYSTEM_NAME%

注: 代替変数のすべての値はグローバル レベルで設定でき、一部の値はテナント レベルで設定できます。 値がテナント レベルで指定された場合、グローバル値は無視されます。

代替変数は、電子メール メッセージのカテゴリと関連付けられています。カテゴリは次のとおりです。

- 予約
- システム
- タスク
- 詳細メッセージ
- その他

予約

次の変数は、予約メッセージと関連付けられています。

%IMAGENAMES%	予約に使用されたイメージ名（カンマ区切り文字列）
%NUMSYSTEMS%	予約されたシステムの数
%ORGUNIT%	要求者の組織単位
%PROJECTID%	予約に関連付けられたプロジェクト ID
%READYSYSTEMLIST%	準備ができている予約済みシステムのシステム名または IP アドレスのリスト（HTML リスト）
%READYSYSTEMTABLE%	準備ができている予約済みシステムのシステム名または IP アドレスのテーブル（HTML テーブル）
%REQUESTEDSOFTWARE%	要求されたソフトウェアのリスト（HTML リスト）
%RESERVATIONENDTIME%	予約の終了時間
%RESERVATIONID%	予約 ID
%RESERVATIONNOTES%	予約に関して入力されたメモ

%RESERVATIONREADYTEXT%	予約の準備完了を通知するすべての電子メールに含められる、ユーザ入力テキスト
%RESERVATIONSTARTTIME%	予約の開始時間
%TENANT%	テナントの名前。
%TENANTID%	代替のテナント ID （短縮または省略形）
%TEMPLATENAME%	この予約に使用されたテンプレート
%TICKETID%	この予約に関連付けられたチケット ID
%TICKETURL%	この予約に関連付けられたチケット URL
%USEREMAILADDRESS%	要求者の電子メール アドレス
%USERNAME%	予約要求者のユーザ名
%VCSERVERNAME%	予約済みシステムをホストしている VC サーバの名前。
%VMNAMES%	予約済みシステムのリスト（HTML リスト）

システム

次の変数は、システム メッセージと関連付けられています。

%DATACENTER%	データ センターの名前
%HOSTSYSTEM%	VM ホスト システムの名前
%IMAGENAME%	VM の作成に使用されたシステム イメージの名前
%IPADDRESSES%	システムに関連付けられた IP アドレスのリスト（カンマ区切り文字列）
%RESOURCEPOOL%	リソース プールの名前
%SERVER%	ユーザ用に予約されているサーバの名前。 新しい VM が作成されている場合、この名前は VM 名と同じです。
%SYSTEMPASSWORD%	システム パスワード（「ReservedSystemReadyNotificationContainsPassword」が true の場合のみ含まれます）。 Amazon EC2 システムの場合、この変数は常に含まれます。
%SYSTEMUPDATEDTIME%	システムのステータスが最後に更新された時間

%SYSTEMUSERNAME%	%SYSTEMPASSWORD% に関連付けられたユーザ名（「ReservedSystemReadyNotificationContainsPassword」が true の場合のみ含まれます）
%VMCONSOLEURL%	VM コンソールの URL
%VMNAME%	仮想マシンの名前

タスク

次の変数は、タスク メッセージと関連付けられています。

%TASKID%	タスク ID
%TASKDESCRIPTION%	タスクの概要です。
%TASKTYPE%	タスク タイプ
%TASKTYPESHORT%	タスク タイプの短縮版

詳細メッセージ

次の変数は、詳細メッセージと関連付けられています。

%DETAILEDMESSAGE%	詳細なメッセージ

その他

次の変数は、*「承認が必要です」*メッセージとのみ関連付けられています。

%AUTOCANCEL%	予約が時間内に承認されていない場合（true または false）、このメッセージには、予約が自動的にキャンセルされるかどうかが表示されます。
%AUTOCANCELMESSAGE%	%AUTOCANCEL% が true の場合、このメッセージには予約が自動的にキャンセルされることが示されます。 それ以外の場合、値は表示されません。
%APPROVALDEADLINE%	%AUTOCANCEL% が true の場合、このメッセージには、予約が未承認の場合にキャンセルされる時刻が表示されます。

次の変数は、すべてのメッセージと関連付けられています。

%CURRENTTIME%	現在の時刻

関連項目:

条件付きの代替変数 (P. 1179)

電子メールのタイプとカテゴリ

以下の表は、電子メール通知のタイプと、それらに関連付けられたメッセージ カテゴリを示しています。 メッセージ カテゴリと関連付けの詳細については、「代替変数 (P. 1174)」セクションを参照してください。

以下の表の「はい」は、電子メール通知のタイプがメッセージ カテゴリに関連付けられていることを示します。

電子メール通知のタイプ	予約	システム	タスク	詳細メッセージ
APPROVAL_REQUIRED	はい	はい*	いいえ	いいえ
HELPDESK_TICKET_OPENED_FOR_RESERVATION	はい	はい	いいえ	いいえ
NOT_ENOUGH_SPACE_FOR_SNAPSHOT	いいえ	はい	いいえ	はい
RESERVATION_ABOUT_TO_EXPIRE	はい	はい	いいえ	いいえ
RESERVATION_APPROVED	はい	はい	いいえ	いいえ
RESERVATION_CANCELED	はい	はい*	いいえ	いいえ
RESERVATION_EXPIRED	はい	はい	いいえ	いいえ
RESERVATION_EXTENDED	はい	いいえ	いいえ	いいえ

RESERVATION_NOT_APPROVED_IN_TIME	はい	はい	いいえ	いいえ
RESERVATION_PROCESSING_RESUMED	はい	はい	いいえ	はい
RESERVATION_PROCESSING_SUSPENDED	はい	はい	いいえ	はい
RESERVATION_READY	はい	はい*	いいえ	いいえ
RESERVATION_REJECTED	はい	はい	いいえ	いいえ
RESERVATION_TASK_FAILED	はい	はい	はい	はい
RESERVATION_TASK_TAKES_TOO_LONG	はい	はい	はい	はい
RESERVED_SYSTEM_READY	はい	はい	いいえ	いいえ
RESERVED_SYSTEM_TERMINATION_WARNING	はい	はい	いいえ	いいえ
REVERT_TO_SNAPSHOT_FOR_RESERVED_SYSTEM_COMPLETED	はい	はい	いいえ	いいえ
SCHEDULER_PROCESSING_RESUMED	いいえ	いいえ	いいえ	はい
SCHEDULER_PROCESSING_SUSPENDED	いいえ	いいえ	いいえ	はい
SNAPSHOT_FOR_RESERVED_SYSTEM_CREATED	はい	はい	いいえ	いいえ
TERMINATION_TASK_FAILED	はい	はい	はい	はい
TEXT_SUPPLIED	はい	はい	いいえ	いいえ
VM_POWER_OPERATION_FAILED	はい	はい	いいえ	はい

「はい*」は、システムを 1 つ予約する場合のみに該当します。

条件付きの代替変数

代替変数がすべての状況に該当しないこともあります。 たとえば、%VMCONSOLEURL% は、VMware ベースのシステムのみに該当します。予約マネージャ が Hyper-V システムについての電子メールを送信する場合でも、電子メールには VM コンソール URL のフィールドが表示されますが、値は空白になります。電子メールに空白のフィールドが含まれると、混乱を招く恐れがあり、見た目もよくありません。

テンプレート内で変数をアンパサンド (@) で囲むと (以下の例を参照)、空白のフィールドを削除できます。

@%VMCONSOLEURL%@

以下の例は、テンプレート内でのコーディング方法を示しています。

```
<table border=1>
<td>System Name</td> <td>%SERVER%</td>
<td>IP Address</td> <td>%IPADDRESSES%</td>
<td>VM Console URL</td> <td>@%VMCONSOLEURL%@</td>
</table>
```

注: 変数は、変数に関連付けられたテキストと同じ行内にある必要があります。 以下の例では、空白フィールドは削除されません。

```
<td>VM Console URL</td>
<td>@%VMCONSOLEURL%@</td>
```

パブリック組織単位からのリソースの継承の有効化または無効化

管理者は、パブリック組織単位に割り当てられたリソースをすべてのユーザから利用できるようにするかどうかを指定できます。

この設定の値が true の場合は、すべての組織単位に、パブリック組織単位がアクセスできるすべてのリソースへのアクセス権が自動的に付与されることを示します。

パブリック組織単位オプションを設定する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［一般］領域で以下のリンクをクリックします。

   ［組織単位は、パブリックリソースへのアクセスが付与されています］

3. ［値］フィールドの設定を必要に応じて変更して［OK］をクリックします。

設定の変更は、ブラウザを再起動するときに行われます。

ホーム ページのようこそテキストの入力

管理者は、［タスク］と［アナウンスメント］の上の、ホーム ページの一番上に表示される、ようこそテキストを指定できます。

ホーム ページのようこそテキストを入力する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［一般］領域で以下のリンクをクリックします。

   ホームのようこそテキスト

3. ［値］フィールドの設定を変更し［OK］をクリックします。

設定の変更は、ブラウザを再起動するときに行われます。

タイムアウト値の入力

予約マネージャ では管理者がタイムアウト値を指定します。タイムアウト値は、データ要求が有効になるまでに待機する分数を示します。

タイムアウト値を入力する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［一般］領域で以下のリンクをクリックします。

   データのタイムアウト

3. 値を入力し、［OK］をクリックします。

ブラウザを再起動するときに、変更は有効になります。

仮想マシン リソースでの制限の設定

管理者は、仮想マシンの予約時にユーザが要求できる同時に展開する VM の数、CPU の数、メモリの量およびディスクの数に制限を設定することができます。

仮想マシン リソースに制限を設定する方法

1. 予約マネージャの管理者として、［予約マネージャを管理］の下にある［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［仮想マシン］領域で以下のリンクをクリックします。 各々に値を変更できるダイアログ ボックスが表示され、［OK］をクリックします。

   ［Virtual Center 最大作業負荷］

   ［仮想 CPU の制限］

   ［仮想メモリの制限］

   ［仮想ディスクの制限］

   ［仮想ディスク領域の制限］

次の予約が行われるときに、設定の変更は有効になります。

ESX サーバまたはクラスタにおけるメモリのオーバーコミットメントの設定

実際のメモリ使用率が許容される場合、VMware サーバまたはクラスタ上で使用されるメモリの量を増加させることができます。 これを行うことにより、より多くの仮想マシンを展開することができます。

オーバーコミットメントは、パーセントで指定します。たとえば、ESX サーバにホストする VM で利用可能な 30 GB の物理メモリがある場合、50 パーセントのオーバーコミットメントにより、メモリは 45 GB に増加します。

ESX サーバまたはクラスタにメモリのオーバーコミットメントを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［リソース プールを管理］をクリックします。

   ［リソース プール］ページが表示され、既存のプールがリスト表示されます。

2. ESX サーバまたはクラスタをダブルクリックします。

   ［リソース プールの詳細］ページが開き、［プロパティ］タブが表示されます。

3. 以下のフィールドを選択し、パーセンテージを入力します。

   ［メモリの超過割り当てを許可する］パーセント:

4. ［OK］をクリックします。

   メモリはオーバーコミットメントされます。

VMware 仮想マシン用のフォルダの指定

新しく作成された VMware 仮想マシン用のフォルダを指定できます。フォルダによって、vSphere Client などの管理ツールを使用する場合に多数の VM をより簡単に管理することができます。

vCenter のフォルダに関して以下の情報に注意してください。

- フォルダは、vCenter の［Virtual Machines & Templates］ビューから作成する必要があります。というのも、［Hosts and Clusters］ビューで作成されたフォルダとは別のタイプのフォルダであるためです。
- このリソース プールを使用して予約を作成する前に、フォルダが vCenter に存在している必要があります。

新しく作成された VMware 仮想マシン用のフォルダを指定する方法

1. 予約マネージャ の管理者として、[予約マネージャを管理] の [リソース プールを管理] をクリックします。

   [リソース プール] ページが表示され、既存のプールがリスト表示されます。

2. VMware リソース プールをダブルクリックします。

   [リソース プールの詳細] ページが開き、[プロパティ] タブが表示されます。

3. [フォルダ] フィールドに、名前を入力します。

   注: フォルダ名は 80 文字未満の空でない文字列である必要があります。 スラッシュ（/）、円記号（¥）およびパーセント（%）は URL 表記（例： %2F）を使用してエスケープされます。 同じ階層内のフォルダに同じ名前を付けることはできません。 フォルダ/フォルダを指定できます。

4. [OK] をクリックします。

   新しい VM が指定されたフォルダに配置されます。

仮想マシンあたりの NIC の最大数の指定

管理者は、仮想マシン用に要求できるネットワーク アダプタ（*ネットワーク インターフェース カード*または NIC とも呼ばれる）の最大数を指定できます。 デフォルト（および最大値）： 10

注: Huawei GalaX は複数の NIC をサポートしていません。

1 つの仮想マシンあたりのネットワーク アダプタの最大数を指定する方法

1. 予約マネージャ の管理者として、[予約マネージャを管理] の [構成設定を管理] をクリックします。

   [構成設定] ページが表示されます。

2. [仮想マシン] 領域で以下のリンクをクリックし、値を設定して [OK] をクリックします。

   [仮想ネットワーク インターフェースの制限]

サービスへの新規仮想マシンの追加

予約マネージャ によって、管理者は新しい仮想マシンが CA Server Automation サービスに自動的に追加されるかどうかを指定できます。 この機能により、サイトで簡単に予約されている仮想マシンのパフォーマンスと使用状況をモニタすることができます。サイトでは、VMware ESX サーバをクラスタに追加するなど、パフォーマンスを改善するために追加のリソースを利用可能にする必要があるかどうかを評価することもできます。サイトでは、仮想マシンが使用中であるかどうか、また返却された場合の候補であるかどうかも確認することができます。 このオプションが有効な場合、新しい仮想マシンはリソース プールとして同じ名前のサービスに追加されます。指定したサービスが存在しない場合は、作成されます。

サービスに新規仮想マシンを追加する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［仮想マシン］領域で以下のリンクをクリックし、値を設定して［OK］をクリックします。

   VC 仮想マシンをサービスに追加

設定変更は、次に予約が作成されるときに有効になります。

予約の設定

予約マネージャ では、管理者は予約に対して以下の機能を設定できます。

- 予約のデフォルト期間を指定します。 この値は、ユーザが予約をするときに、ユーザに表示される最初の終了日を計算するために使用されます。
- 予約要求時にプロジェクト ID を必須にします。このオプションが true に設定されている場合、ユーザは予約要求をサブミットする前に、プロジェクト ID フィールドに値を入力する必要があります。プロジェクト ID を使用すると、コストをプロジェクトにチャージバックしたり、プロジェクトごとの使用状況をレポートしたりするためにプロジェクト情報を使用できます。
- ユーザがテンプレートの最小ハードウェア要件を上書きできるようにします。
- ユーザがネットワークを選択できるようにします。

予約を設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［予約］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   デフォルトの予約期間

   ネットワーク選択を許可

   プロジェクト ID が必要

   要件の指定を許可

次の予約が行われるときに、設定の変更は有効になります。

関連項目:

別の選択対象を許可 (P. 1186)
チャージバックの表示の設定 (P. 1168)
自動選択対象の上書き (P. 1187)
メモリと CPU の選択対象の指定 (P. 1187)

別の選択対象を許可

［マシンを予約します］ウィザードの［システムの選択］ページを設定して、選択されたシステム イメージをサポートし、要求された日付に利用可能であるが、以下の 1 つ以上の条件を満たさないシステムのリストを表示します。

- CPU 数
- 最小メモリ
- 最小ディスク領域

これは、特定のシステムの要求を処理できない場合に役立ちます。

許容できる代替システムがリスト表示されると、ユーザは表示されたリストからシステムを選択できます。

ユーザが複数のシステムを要求した場合、また、要求が部分的にだけ処理された場合は、リストは自動的に選択されたシステムを一番上に表示します。 ユーザはリストから追加のシステムを選択して予約をサブミットするか、または日付指定ページに戻って再度試行することができます。

ユーザは、［要件の指定］ページで要求されたシステム数を選択したり、テンプレートが作成された日付を選択するのに制限されていません。 システムの数がリソース プール ポリシーに基づいてユーザが許可された最大数を超えない限り、選択されたシステムは予約されます。

別の選択対象を許可する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［予約］領域で以下のリンクをクリックします。

   代替システム要件の指定を許可

3. 値を入力し、［OK］をクリックします。

次の予約が行われたときに、設定の変更は有効になります。

自動選択対象の上書き

［マシンを予約します］ウィザードの［システムの選択］ページを設定して、要求に一致するすべてのシステムのリストを表示できます。 チェック マークは、予約を処理するために自動的に選択されたシステムを示します。 必要に応じて、エンド ユーザはリストから他のシステムを選択することにより、この事前選択を上書きできます。

ユーザは、［要件の指定］ページで要求されたシステム数を選択したり、テンプレートが作成された日付を選択するのに制限されていません。 システムの数がリソース プール ポリシーに基づいてユーザが許可された最大数を超えない限り、選択されたシステムは予約されます。

自動選択対象を上書きする方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［予約］領域で以下のリンクをクリックします。

   ［マシン選択を許可］

3. 値を入力し、［OK］をクリックします。

次の予約が行われたときに、設定の変更は有効になります。

メモリと CPU の選択対象の指定

管理者は、ユーザが予約をするときに選択できるメモリの量および CPU の数を制御できます。

メモリと CPU の選択対象を指定する

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［予約］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   ［予約メモリ選択］

   ［予約 CPU 選択］

次の予約が行われるときに、変更は有効になります。

サービスの設定

予約マネージャ では、管理者はサービスに対して以下の機能を設定できます。

- 下限しきい値と上限しきい値を指定する。
- 遅延を指定する。
- 優先度を入力する。

サービスを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［仮想マシン］領域で以下のリンクをクリックします。表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   ［サービス下限しきい値］

   ［サービス上限しきい値］

   ［サービス遅延］

   ［サービスの優先度］

次のサービスが行われるときに、設定の変更は有効になります。

スナップショットの設定

予約マネージャ では、管理者はサービスに対して以下の機能を設定できます。

- スナップショットを作成する前に空き容量をチェックする。
- 拡張の割合を指定する。
- 管理するスナップショットに予約済みスペースの割合を指定する。

注: 予約マネージャ は、一度に 1 つのスナップショットを許可します。新しいスナップショットを作成する場合、新しいスナップショットに十分なスペースを確保するために、以前のスナップショットはすべて削除されます。 これには、vCenter または vSphere から直接作成された任意のスナップショットが含まれます。

スナップショットを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［仮想マシン］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   スナップショット用の空き領域のチェック

   スナップショット用のファイルシステム許容増加率

   スナップショット予約の管理

次のスナップショットが作成されるときに、設定の変更は有効になります。

ソフトウェア展開の無効化

管理者は、ユーザが仮想マシンにソフトウェアを展開できないように、予約マネージャ を設定できます。 設定では、ユーザ インターフェース内のすべてのソフトウェア展開機能を非表示にできます。

ソフトウェア展開機能を無効にする方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［CA ITCM 統合］領域で［ソフトウェア展開の有効化］リンクをクリックし、［OK］をクリックします。

予約マネージャ の再起動時に、変更は有効になります。

物理システムの割り当てポリシーの変更

予約マネージャ が予約要求を満たすことができると決定した後、要求の条件に合う各システムの合計コストを計算します。 caaipconf.cfg ファイルの各プロパティに対する重みの値を変更して、環境に応じたシステム割り当てポリシーをカスタマイズすることができます。

物理システムの割り当てポリシーを変更する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［物理プロビジョニング］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   CPU 数予約の重み付け

   ディスク領域予約の重み付け

   メモリ予約の重み付け

設定変更は、次に予約が作成されるときに有効になります。

関連項目:

低価格アルゴリズムの動作方法 (P. 1191)

低価格アルゴリズムの動作方法

加重アルゴリズムは、優先プール ポリシーと共に使用されます。 管理者は、ユーザ要求に一致するリソースを検索するためのリソース プールの順序を定義します。 システムがプライマリ プールで利用可能な場合、加重アルゴリズムが適用されて最適なシステムを決定します。 セカンダリ リソース プールでは、プライマリ プールで一致するシステムを検索できなかった場合にのみ検索されるため、セカンダリ プールで加重アルゴリズムに基づいたより最適なシステムがあったとしても、検索されません。

加重アルゴリズムは、ユーザ要件に最も一致する物理システムを選択します。 このアルゴリズムはデフォルトでは以下のシステム プロパティに重みを加えます。

- ［CPU の数］ : 各 CPU に 500 で重みを加えます。
- ［利用可能なメモリ］ : メモリの利用可能な各ギガバイトに 50 で重みを加えます。
- ［ハード ディスク領域］: ハード ディスク領域の各ギガバイトに 2 で重みを加えます。

したがって、1 つの CPU はデフォルト ポリシーを使用する 10 GB の RAM および 250 GB のハード ディスク領域とほぼ同じだけかかります。

承認待ち要求通知を送信する時間の指定

予約の開始時刻が接近していて、予約がまだ承認されていない場合、予約マネージャ は管理者に電子メールアラートを送信できます。 開始時刻の何時間前にこの通知を送信するのかを設定できます。 デフォルトでは、通知は予約開始時刻の 2 時間前に送信されます。

注: このオプションは、予約マネージャ が手動での承認に設定されている場合にのみ、適用されます。

承認待ち要求通知を送信する時間を指定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［承認］領域の［要承認の通知時刻］をクリックします。
3. ［値］フィールドの設定を変更し、［OK］をクリックします。

設定変更は、次に予約が作成されるときに有効になります。

未承認予約の自動取り消しの設定

予約マネージャ は、明示的に承認されない予約を自動的に取り消すことができます。 自動取り消しが有効な場合、予約の開始時刻から予約を取り消すまでに待機する時間を指定することもできます。 デフォルトでは、このオプションは無効になっています。

未承認予約の自動取り消しを設定する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［承認］領域で以下のリンクをクリックします。 表示されるダイアログ ボックスで、必要に応じて値を変更し、［OK］をクリックします。

   未承認予約の自動キャンセル

   未承認予約の自動キャンセル遅延時間

設定変更は、次に予約が作成されるときに有効になります。

ユーザにストレージ層の選択を許可

ストレージ層は各ディスクに関連付けられたデータ ストアの分類です。 層は、通常、VM とそのハード ドライブが作成されるデータストアの各種レベルのパフォーマンスを示しています。 管理者はストレージ層を有効または無効にできます。

ストレージ層が有効な場合、ユーザは仮想マシンの予約時にそれらを選択できます。

ユーザにストレージ層の選択を許可する方法

1. 予約マネージャ の管理者として、［予約マネージャを管理］の［構成設定を管理］をクリックします。

   ［構成設定］ページが表示されます。

2. ［仮想マシン］領域の［データ ストア層の選択を許可］をクリックします。

3. 値を入力し、［OK］をクリックします。

ブラウザを再起動すると、設定の変更は有効になります。

関連項目

ストレージ層のチャージバックの設定 (P. 1164)

第 14 章: スケーラビリティのベスト プラクティス

このセクションには、以下のトピックが含まれています。

スケーラビリティの概要

このセクションでは、CA Server Automation の展開に関するベスト プラクティスおよび推奨事項について説明します。 このドキュメントの目的は、実稼働環境内に CA Server Automation をロールアウトする場合に必要となる作業、特に次の項目を計画する作業を支援することです。

- VMware 環境のモニタリングおよび CA Server Automation 管理
- IBM LPAR 環境のモニタリング
- Oracle Solaris ゾーン環境のモニタリング
- SystemEDGE およびほかのモニタリング ソフトウェアの展開
- SystemEDGE の初期および継続的な設定

以下のセクションが含まれています。

1. リモート展開およびポリシー設定の概要 (P. 1198)
2. ハードウェアの仕様 (P. 1196)
3. データベースに関する考慮事項 (P. 1197)
4. ネットワークに関する考慮事項 (P. 1198)
5. スケーラビリティに関する推奨事項および制限事項 (P. 1201)
6. スケーラビリティに関する使用事例 (P. 1210)

ハードウェアの仕様

このセクションでは、CA Server Automation の大規模実装のためのハードウェア最小仕様をリスト表示します。 より大規模な実装においては、管理サーバの仕様の拡張を考慮してください。

- ドメイン サーバ： 2.6 GHz の Dual-Core プロセッサ、4 GB の RAM、100 GB のディスク。
- 配布サーバ: 1 GHz のシングル コア/プロセッサ/仮想プロセッサ、2 GB の RAM、100 GB のディスク、100 Mb/秒イーサネット。
- VC AIM モニタリング サーバ: 2.6 GHz の Dual Core プロセッサ、4 GB の RAM、100 GB のディスク。
- LPAR AIM モニタリング サーバ： 2.6 GHz の Dual Core プロセッサ、4 GB の RAM、100 GB のディスク。
- Solaris ゾーン AIM モニタリング サーバ： 2.6 GHz の Dual Core プロセッサ、4 GB の RAM、100 GB のディスク。
- ターゲット システム： 1 GHz のシングル コア/プロセッサ/仮想プロセッサ、512 MB の RAM、2 GB のディスク、100 Mb/秒イーサネット x 1

注: CPU とメモリの使用率は、最大 50 パーセントに抑える必要があります。

注: さらに、パフォーマンス チャートのデータ収集では、モニタされているマシンとメトリックの数に応じて、マネージャ上で最大 3.5 GB のディスク領域と 2 GB の RAM が必要になる場合があります。

ADES AIM のスケーラビリティ

ADES AIM の展開を計画する場合、インフラストラクチャのサイジングおよびシステム パフォーマンスに影響を及ぼす以下のキー ファクタを考慮します。

- オペレーティング システムおよびその他のアプリケーションが使用するメモリを除き、ADES AIM が利用可能なメモリ
  - 1 GB の空きメモリがあるホストは 20 のホスト（2 台の Active Directory ホストと 18 台の Exchange ホスト）をモニタできます。
  - 2 GB の空きメモリがあるホストは 40 のホスト（6 台の Active Directory ホストと 34 台の Exchange ホスト）をモニタできます。
  - 3 GB の空きメモリがあるホストは 60 のホスト（10 台の Active Directory ホストと 50 台の Exchange ホスト）をモニタできます。
- 環境の地理的分布
  - ADES AIM が地理的に近い場所にある場合、環境の検出とポーリングにかかる時間が短縮されます。
  - 大きな遅延や多量のパケット損失は、AIM が必要なすべてのデータを取得できない原因となります。

注: サイジング情報は展開要件の概算であり、最終的なものではありません。 サイジング情報はモニタリング環境によって異なります。

データベースに関する考慮事項

管理対象の環境が拡大するほど、発生するデータベース アクティビティも増えることが予想されます。 製品用のデータベースのサイズは、製品の使用状況に応じて大きくなります。保守の実施状況によりますが、30 GB 以上を消費する可能性があります。データ保持については、一般的なルールに従うことをお勧めします。つまり、モニタ対象環境内のマシン 1000 台ごとにデータ記録間隔を 300 秒増やします。

注: データベース専用のスタンドアロン システムを使用すると、パフォーマンスを改善できます。 データベースをネットワーク上の他の CA Server Automation コンポーネントの近くに配置すれば（同一サブネット上など）、応答時間は向上します。

関連項目:

データ収集の設定 (P. 950)

ネットワークに関する考慮事項

CA Server Automation のロール アウトを計画する場合には、ネットワーク接続の品質を検討して、管理コンポーネントを配置する場所を決定します。以下の項目が、ソリューションのスケーラビリティおよび効率に影響を及ぼします。

- ネットワーク品質： 品質が低いと、データの損失が発生し、結果としてレスポンスの遅延、または接続障害を引き起こします。
- ネットワーク帯域幅： 帯域幅が低いと、コンポーネント間でのデータ転送速度が制限されます。
- ネットワーク遅延： ネットワーク遅延が大きいと、帯域幅が低い場合と同様に、データ転送率が制限されます。
- DNS： 適切に設定されていない DNS では、モニタリング エージェントの展開および継続的な設定作業に支障が発生します。

特に、リモート DB を使用している場合は、管理コンポーネント間に少なくとも 100 Mb/秒のネットワーク リンクを使用することを推奨します。ネットワーク速度が 100 Mb/秒未満の場合は、別の配布サーバをターゲット システムと連結して導入することを検討してください。

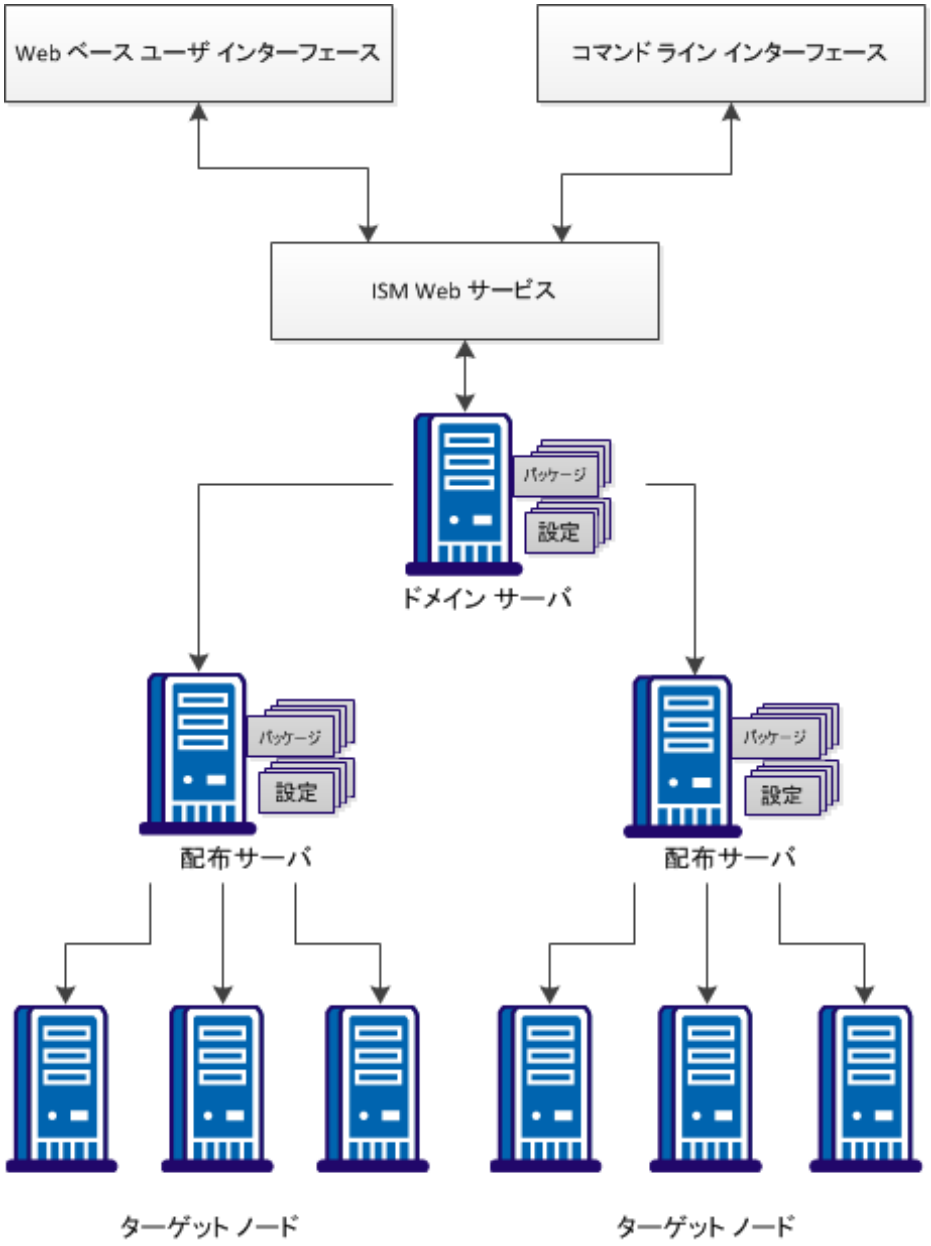
リモート展開およびポリシー設定の概要

CA Server Automation は、SystemEDGE エージェントをすべての管理対象システムにリモート展開するための包括的なソリューションを提供します。カスタマイズされたインストール パラメータを含むパッケージに基づいた展開テンプレートを作成すると同時に、これらのテンプレートを多数の管理対象システムに展開することができます。

さらに CA Server Automation は、すべての管理対象システム上で実行されている SystemEDGE エージェントの設定を継続的に行うための包括的なソリューションを提供します。 ポリシー設定は、ポリシーのライブラリを作成する機能を提供します。これらのポリシーは、SystemEDGE および SRM AIM を実行する 1 つ以上のシステムに適用されます。ポリシー設定によって管理されたエージェントがインストールされると、そのエージェントは自動的にポリシーを要求します。 このため、エージェントは、制御され、一貫したセットのポリシーを実行します。その後、エージェントは、エージェントが実行しているポリシー、またはエージェントがメンバであるサービスに基づいて、個別に更新できます。

リモート展開およびポリシー設定は、ドメイン サーバおよび配布サーバの技術を共有します。 この技術は、スケーラビリティが高く、複数のデータ センターにわたって配布することを可能にするソリューションを提供します。

以下の図は、リモート展開およびポリシー設定のコンポーネントの基本的なアーキテクチャを示しています。



スケーラビリティに関する推奨事項

このセクションでは、スケーラビリティに関する推奨事項および制限事項について説明します。

以下の情報について検討します。

- VMware 環境のモニタリング（P. 1201）
- VMware 環境の CA Server Automation 管理（P. 1203）
- リモート展開およびポリシー設定に関する推奨事項（P. 1207）
- ドメイン サーバに関する推奨事項（P. 1209）
- 配布サーバに関する推奨事項（P. 1210）
- スケーラビリティに関する使用事例（P. 1210）

vCenter AIM モニタリングの推奨事項

SystemEDGE エージェントには、初期化時にオプションの *Application Insight Module （AIM）*をロードできるプラグイン アーキテクチャが備わっています。AIM は SystemEDGE エージェントの機能拡張です。たとえば、vCenter AIM により、SystemEDGE は VMware vCenter Server を介して vSphere 環境を管理できます。

vCenter AIM （Application Insight Module）は、SystemEDGE フレームワーク内にインプリメントされたプラガブル コンポーネントです。 そのため、これによって発行されるデータは複数の SNMP マネージャから利用可能です。 CA Server Automation マネージャ、eHealth、および Spectrum IM などの製品はこのデータをレバレッジできます。

このコンポーネントが CA Server Automation マネージャの外部で使用される可能性があるため、スケーラビリティ推奨事項はそれぞれ別に指定されます。スケーラビリティ推奨事項については、主として 2 つの考慮事項があります。

vCenter AIM モニタリングに対する一般的な推奨事項

vCenter AIM モニタリングにおけるスケーラビリティ制限について、一般的な推奨事項を以下に示します。

- VM の最大数（概算）： 240,000 / (x + 6)
- オブジェクトの最大数（概算）： 2,000,000 / (x + 6)

  x は AIM に対する SNMP ポーリングの 1 時間あたりの回数です。

モニタ対象オブジェクトに関するスケーラビリティ制限

一般的に、スケーラビリティの制限においては CPU 使用率が主な考慮事項となります。 vCenter AIM モニタリングについては、CPU 使用率に影響を及ぼす 3 つの主な要因を考慮します。

- モニタ対象である vCenter Server が動的であること。

  vCenter Server のアクティビティのレベルは CPU 消費に影響を及ぼします。 以下のスケーラビリティ推奨事項では、モニタ対象である vCenter Server の平均的なアクティビティ レベルを想定しています。
- SNMP マネージャの数、およびそれらの SNMP マネージャのポーリング間隔。

  vCenter AIM のポーリングを行う SNMP マネージャの数が多い場合、あるいはポーリング間隔が短い場合、CPU 消費は増加します。
- VM 数に関するオブジェクト数の比率。

  オブジェクトは、vCenter AIM によってモニタされる vSphere の任意の要素です。 たとえば、vCenter AIM は、データストア、仮想ディスク、物理ネットワーク インターフェース コントローラ、仮想スイッチ、SCSI コントローラ、ESX ホスト ハードウェア センサなどをモニタします。オブジェクトの数は CPU の使用率に直接影響があります。vCenter AIM キャッシュを維持する必要があり、さらにこのデータのパブリッシュに追加のオーバーヘッドが必要となるためです。 現実のシステムでは、通常、指定された vCenter 内の仮想マシンより 6 ～ 11 倍も多くのオブジェクトがあります。

これらの要因に基づくと、vCenter AIM をモニタする単一の SNMP マネージャでポーリング間隔が 10 分の場合、VM 数の制限は約 20,000 になります。

モニタ対象サーバに関するスケーラビリティ制限

vCenter AIM は複数の vCenter Server 環境で機能します。 vCenter AIM のフレームワークでは、vCenter Server あたりの VM 数が少なくなると CPU 使用率がわずかに低下します。 たとえば、それぞれ 2,000 の VM を持つ 3 つの vCenter Server の CPU 使用率は、6,000 の VM を持つ 1 つの vCenter Server の CPU 使用率より低くなります。

vCenter AIM の応答性がスケーラビリティの制限になる場合があります。一般的に、vCenter AIM は最大 10 の vCenter Server をモニタできます。

CA Server Automation vCenter 管理の推奨事項

CA Server Automation マネージャには、vCenter データのモニタや発行だけでなく、多くの機能があります。 マネージャは、履歴データの格納と管理、vCenter に対するアクティブな操作の実行、自動化ポリシーの実行、レポートなどを行います。 そのため、vCenter AIM より多くのリソースが必要となることが多く、主なデータ収集メカニズムとして使用されます。

仮想マシンに関する vCenter 管理の制限

CA Server Automation マネージャの大部分は単一のプロセス空間内に存在するため、多くの場合、オペレーティング システムの制限がスケーラビリティにおける主な問題となります。 以下の制限要因を考慮してください。

- 利用可能なメモリ： 管理対象オブジェクトの数が増加すると、データのキャッシュやメッセージングの処理に必要なメモリの量が急激に増加します。マネージャのメモリを 8GB 以上に増加させることを推奨します。
- 利用可能な CPU： CA Server Automation マネージャは、特に急速な環境変化または初期起動において、大量の CPU リソースを必要とします。自動プロセスの応答性を向上させるために、ある程度大規模な管理対象環境については、追加の CPU （3.2 GHz 以上）を準備することを推奨します。
- オペレーティング システムの制限： CA Server Automation マネージャの大部分は単一のプロセス空間内に存在します。その結果、32 ビット オペレーティング システムのメモリ アドレス空間は、システム メモリの空き容量がまだ残っている場合にも使い尽くされる可能性があります。 この問題を回避するために、ある程度大規模な管理対象環境については、64 ビットのプロセッサとオペレーティング システムを使用することを推奨します。

例:

以下の例は、CA Server Automation マネージャの要件およびスケーラビリティ制限の推奨事項を提供します。

- 最小要件（32 ビット、2.6GHz の CPU、4GB の RAM、100GB のディスク）

  スケーラビリティ制限： 2,500 のコンピュータ システム（VM および ESX ホスト）。
- 推奨されるシステム（64 ビット プロセッサおよびオペレーティング システム、3.2GHz CPU、8GB の RAM、100GB ディスク）

  スケーラビリティ制限： 8,000 のコンピュータ システム（VM および ESX ホスト）。

初期ディスカバリでのパフォーマンスの考慮事項

管理対象とする vCenter 環境の初期ディスカバリおよびデータベース ロードの実行には、時間がかかる場合があります。 このプロセス中に、以下のアクションが実行されます。

1. vCenter AIM が vCenter 環境全体を解析し、マネージャに結果を発行します。
2. CA Server Automation マネージャは vCenter AIM から発行されたデータを取得し、処理用に内部キャッシュを作成します。
3. 内部キャッシュは現在の CA Server Automation マネージャ データベースの内容と同期され、現在データベース内にないコンピュータ システムについての検出が実行されます。

vCenter サーバの初期管理中、データベースにはコンピュータ システムがないため、これらのオブジェクトはすべて検出され、作成されます。 初期ディスカバリの完了に必要な予測時間を考慮してください。 ベースライン テストに基づく平均スループット： 毎分 8 ～ 9 のコンピュータ システム

例:

以下の例は、環境のサイズ、および、初期ディスカバリの完了に必要と予想される時間を提供します。

- 2,500 のコンピュータ システム - 約 5 時間
- 8,000 のコンピュータ システム - 約 15 時間

この初期取り込み中は、CPU 使用率が高い状態が長く続きます。

注: 初期ディスカバリプロセスには多大な時間がかかります。 ただし、初期ディスカバリは製品の使用において 1 度だけ実行されます。 vCenter AIM および CA Server Automation 内部キャッシュのプロセスは、非常に短時間で完了します。たとえば、vCenter AIM によって通常 2,500 コンピュータ システムが発行され、CA Server Automation マネージャによって約 5 分でキャッシュされます。

LPAR AIM モニタリングの推奨事項

LPAR AIM （Application Insight Module）は、SystemEDGE フレームワーク内に実装されたプラガブル コンポーネントです。 そのため、これによって発行されるデータは複数の SNMP マネージャから利用可能です。CA Server Automation、eHealth、Spectrum IM などの製品は、このデータを活用できます。

以下のセクションでは、LPAR AIM モニタリングに関するスケーラビリティの推奨事項を指定します。

LPAR AIM モニタリングに関するスケーラビリティの推奨事項

1 つの LPAR AIM は、以下の範囲の Power システム環境設定を処理できます。

- HMC サーバの数： 1 ～ 4
- HMC サーバあたりの Power システムの数： 2 ～ 10
- Power システムあたりの仮想 I/O サーバの数： 1 ～ 2
- Power システムあたりの LPAR の数： 10 ～ 100

LPAR AIM モニタリングに関する一般的な推奨事項では、LPAR 環境の標準的な設定は以下のとおりです。

- モニタ対象の Power システム数： 最大 20
- モニタ対象の VIO サーバ数： 最大 30
- モニタ対象の LPAR 数： 最大 300

AIM は、おおよそ LPAR の数に比例して、CPU とメモリを消費します。 最大 300 の LPAR では、sysedge プロセスの CPU 消費は 10 パーセント未満になります。

注: 示された CPU 消費は、ほかの AIM を実行していない専用の SystemEDGE エージェントに対して有効です。

LPAR AIM に 300 の LPAR が追加されると、sysedge プロセスのメモリ消費は約 8 MB 増えます。

Solaris ゾーン AIM モニタリングの推奨事項

Solaris ゾーン AIM （Application Insight Module）は、SystemEDGE フレームワーク内に実装されたプラガブル コンポーネントです。 そのため、これによって発行されるデータは複数の SNMP マネージャから利用可能です。CA Server Automation、eHealth、Spectrum IM などの製品は、このデータを活用できます。

以下のセクションでは、Solaris ゾーン AIM モニタリングに関するスケーラビリティの推奨事項を指定します。

Solaris ゾーン AIM モニタリングに関するスケーラビリティの推奨事項

一般的な推奨事項として、1 つのゾーン AIM で以下の構成をモニタします。

- モニタ対象のゾーン サーバ数： 最大 20
- モニタ対象のゾーン数： 最大 1000

AIM は、ゾーンの数に比例して CPU とメモリを消費します。 ただし、最初の数個のゾーンに対する初期のメモリ消費は高く、より多くのゾーンが追加されるに従って減っていきます。

1000 のゾーンでは、sysedge プロセスの CPU 消費は 5 パーセント未満になります。

注: 示された CPU 消費は、ほかの AIM を実行していない専用の SystemEDGE エージェントに対して有効です。

ゾーン AIM に 1000 のゾーンが追加されると、sysedge プロセスのメモリ消費は約 20 MB 増えます。

リモート展開およびポリシー設定に関する推奨事項

リモート展開およびポリシー設定の作業を効率化するために、以下の観点および推奨事項を検討します。

- ターゲット マシンの数

  最適なパフォーマンスのためには、1 つのバッチでの展開ジョブ サイズを 500 のターゲット マシンに制限します。

- 配布サーバの数

  複数の配布サーバを使用すると、展開のスループットが向上します。

- 展開パッケージ サイズ

  展開ソフトウェア パッケージのサイズが小さいほど、スループットが良くなります。 推奨される数は、すべての管理対象サーバに SystemEDGE および Advanced Encryption が必要であると想定したものです。

  注: 典型的なパッケージ サイズは 10MB ～ 20MB です。

- ネットワークの品質および速度

  配布サーバとターゲット マシンの間で、低い帯域幅のネットワークが使用されており、多量のパケット損失および大きな遅延が発生している場合は、展開と設定の作業の効率と信頼性が低下します。

- ターゲット システムにモニタリング ソフトウェアをロールアウトする時間スケール

  連結した展開サーバを使用して、モニタリング ソフトウェアの展開を時間的にずらして実行します。こうすることで、ネットワーク インフラストラクチャの負荷が軽減されます。 負荷の軽減は、複数のジョブの作成、またはソリューションに組み込まれている時差配布の機能を使用して達成できます。

  モニタリング ソフトウェアを短時間で展開する必要がある場合は、環境内に追加の配布サーバを展開することを推奨します。

- （ポリシー設定による）エージェント再設定の頻度

  典型的なネットワーク環境での SystemEDGE エージェントの再設定には、約 30 秒に加え、1 エージェントにつき 2 ～ 10 秒かかることが予想されます。 エージェントを頻繁に再設定する必要がある場合、環境内により多くの配布サーバを展開することを推奨します。

- 複数のサイトに存在するターゲット システムの地理的分布

  ターゲット システムが複数のサイトに分散されている場合、各サイトに配布サーバを展開することを推奨します。 これは、リモート データ センターで低速なリンク（100 Mb/秒未満）または信頼性の低いリンクが使用されている場合、特に推奨されます。 ローカル配布サーバを展開することにより、展開および設定の要求がすべてオンサイトの配布サーバを介して送信できます。 このアクションにより、中央とリモート サイトの間のトラフィックが軽減されます。

- 通信ポート

  リモート展開およびポリシー設定では、ドメイン サーバから配布サーバへの通信と、配布サーバからエージェントへの通信に、CA-Messaging による通信を使用します。 CA-Messaging はポート 4104（UDP）および 4105（TCP）を使用して通信します。 ファイアウォールで保護されているリモートサイトの場合、サイトに配布サーバを配置することにより、すべての CA-Messaging 通信をポイント ツー ポイントとしてセットアップできます。

  注: エージェント ディスカバリおよび継続的なモニタリングについては、SNMP 通信（通常ポート 161）が使用されます。 管理対象システムからマネージャへの直通通信用にこのポートを開きます。

- ポリシー設定のポリシーおよびテンプレートの管理

  環境内のさまざまなワークロードに基づいて、モニタリング要件をテンプレートにまとめることを推奨します。ポリシーまたはテンプレートあたり最大 1000 のモニタを使用してください。 システムに適用するテンプレートの数は任意ですが、テンプレートの数を 1 システムにつき 100 に制限することを推奨します。

- サービス メンバシップ

  設定操作を容易にするために、1 サービスにつき約 500 サーバを上限としてサーバをサービスにまとめることを推奨します。 1 つのサーバを複数のサービスのメンバとすることが可能であるため、異なるワークロードごとに複数のサービスを作成することを推奨します。 こうすると、テンプレートをサービスに直接適用できます。

- テスト展開

ドメイン サーバに関する推奨事項

展開および設定ドメイン サーバ（ドメイン サーバ）は、展開とポリシー設定の全操作を管理および制御します。

ターゲット システムの数が 10,000 を超える場合、CA Server Automation の複数のインスタンスを実行することを推奨します。

配布サーバに関する推奨事項

*展開および設定配布（スケーラビリティ）サーバ*によって、展開とポリシー設定の操作が効率的かつタイムリーに実行されることが保証されます。

CA Server Automation マネージャをインストールしたら、リモート展開およびポリシー設定をロールアウトするための次の手順は、配布サーバの数を検討することです。

展開操作では、標準的な 100 Mb/秒のネットワーク環境の場合、2,000 のターゲット システムごとに 1 台の配布サーバを使用することを推奨します。

注: ポリシー設定を使用し、リモート展開を使用しない場合、各配布サーバは最大 3,000 サーバに拡張できます。

重要: 大規模な展開操作を行う前に、各配布サーバにつき少なくとも 1 つのシステムへのテスト展開を実行することを推奨します。 より大規模な展開で失敗が発生しないことを確認するために、配布サーバを使用して、あらゆるパッケージを展開することを推奨します。

スケーラビリティに関する使用事例

このセクションでは、典型的な実稼働環境を表す使用事例を提供します。これらの事例をお使いの環境と比較し、環境に最も適合する推奨事項に従うことをお勧めします。

部門のデータ センター

この使用事例では、1,000 のシステムをモニタリングする必要があります。すべてのシステムが 1 つのデータ センター内に配置されています。 すべてのシステムが、ファイアウォール内の 1 つの場所にあります。また、コンピュータ間の通信には、高速のリンクが使用されています。

この環境の推奨事項は以下のとおりです。

- コンポーネントのインストール

  すべての CA Server Automation マネージャ コンポーネントは、同じシステムにインストールできます。

- 初期展開

  すべてのターゲット ノードにモニタリング ソフトウェアを展開するために 2 つのジョブを作成します。 ネットワークの負荷にもよりますが、SystemEDGE（および必要な場合 Advanced Encryption）の初期展開を完了するのに、8 ～ 12 時間を必要とします。

  リモート システムへの展開が完了すると、CA Server Automation マネージャ は SystemEDGE を検出します。 ポリシー設定は各エージェントに初期ポリシーを配信します。 初期ポリシーの配信は、ジョブ完了の約 8 時間後に完了することが予想されます。

- サービス メンバシップ

  保守を容易にするために、管理対象のサーバを、1 サービス当たり 200 サーバを目安として、サービスにまとめます。 サービスは、ビジネス機能、ネットワーク トポロジ、または他の要件に応じてまとめることができます。

- ポリシーの適用

  必要な場合は、1 回の操作で、すべてのモニタ対象システムにポリシーを適用できます。

複数のデータ センター

この使用事例では、複数のデータ センターに配置された 10,000 のシステムが管理されています。各データ センターのシステム数は 500 ～ 2,500 の範囲でさまざまです。 データ センターは、複数の場所に地理的に分散しています。 データ センター間は、100 Mb/秒未満の専用線でリンクされています。 システムはさまざまなワークロードを実行し、多くの異なる部門（アプリケーション所有者）によって管理されています。

この環境の推奨事項は以下のとおりです。

- コンポーネントのインストール

  専用サーバに CA Server Automation マネージャ コンポーネントをインストールします。 このサーバはその最小サポート要件を満たす必要があります。しかし、少なくとも 8 GB の RAM を備えた Quad-Core サーバが推奨されます。

  上位の仕様（Quad-Core プロセッサと 8 GB の RAM）を備えた個別の専用サーバにデータベースをインストールすることを推奨します。

  リモート データ センターをサポートするために、各データ センター内に 1 つの配布サーバをインストールすることを推奨します。 2,000 を超えるサーバが含まれているデータ センターについては、2 番目の配布サーバをインストールすることを推奨します。

  注: ポリシー設定を使用し、リモート展開を使用しない場合、各配布サーバは最大 3,000 サーバに拡張できます。

- 初期展開

  複数の配布サーバを使用した展開を計画する場合に考慮すべき関連要因を以下に示します。

  - 可能な場合は、単一の展開ジョブ サイズを最大 500 のターゲット システムに制限します。
  - 最も近い配布サーバが展開操作のために選択されることを確認します。
  - 同時展開は単一の配布サーバ内でサポートされていますが、複数の配布サーバが使用される場合に限定することを推奨します。 4 台の配布サーバを用意することにより、各配布サーバで展開するマシンを 500 台にすることができます。
  - 同じ配布サーバを使用して同時展開を実行する場合は、ジョブごとに異なるターゲット マシンが展開されることを確認します。

- 複数のパッケージが多くのシステムに配信される場合、パッケージ配信を複数のジョブに分割することを考慮します。 たとえば、SystemEDGE および Advanced Encryption を先に展開します。
- 大規模な展開中に失敗が発生する場合は、すべての前提条件を確認してから［ジョブの再サブミット］を使用して展開を再試行します。
- 将来の操作に備えて、展開をテンプレートとして保存することを推奨します。

- サービス メンバシップ

  保守を容易にするために、管理対象のサーバを、1 サービス当たり最大 500 サーバを目安として、サービスにまとめます。 リモート データ センターについては、データ センターのサイズに応じて、それぞれに 1 つ以上のサービスを作成することを推奨します。

  複数の部門が特定のシステムを使用している場合、各部門による管理を容易にするために、それらのシステムを複数のサービスに追加できます。

- ポリシーの適用

  この使用事例では、サーバはさまざまなワークロードを実行します。 そのため、ベース ポリシーには制御設定のみが含まれるようにすることを推奨します。 モニタリング要件に基づいて複数のテンプレートを作成し、個別のモニタリング設定を保持します。 その後、これらのテンプレートは、手動でシステムを選択することにより、またはサービスにテンプレートを適用することにより、必要なシステムに適用できます。

  モニタリング要件を複数のテンプレートに分割すると、必要なシステムに必要なテンプレートを個別に適用できます。 システムを手動で選択するか、またはサービスにテンプレートを適用します。 テンプレートの適用は、2,000 ～ 2,500 のシステムに分けて行うことを推奨します。

  ベース ポリシーを変更する必要がある場合、2,000 ～ 2,500 のシステムに分けてポリシーを適用することを推奨します。

  注: テンプレートを使用する場合、テンプレートまたはポリシーの各配信において、すべての割り当て済みテンプレートがベース ポリシーにマージされます。 次の手順は、結果の設定のエージェントへの配信です。 そのため、複数のテンプレートがシステムに適用される場合、配信時間がわずかに長くなることがあります。

大規模な環境

この事例では、約 21,000 のエージェントが管理されています。 これらのエージェントは 3 つのデータ センターに配置されており、各データ センターには 2,000 ～ 10,000 のターゲットが存在します。 データ センターは分散されていますが、高速のリンクで接続されています。 管理対象システムは大部分が仮想化されており、さまざまなワークロードを実行し、必要に応じて再プロビジョニングされます。

この環境の推奨事項を以下に示します。

- コンポーネントのインストール

  各データ センターで CA Server Automation のインスタンスを実行し、各インスタンスが最大 10,000 のシステムを管理することを強く推奨します。

  各データ センターでは、専用サーバに CA Server Automation マネージャ コンポーネントをインストールすることを推奨します。このサーバはその最小サポート要件を満たす必要があります。さらに、RAM を 8 GB に増強することを推奨します。

  8 GB の RAM を備えた個別の専用サーバにデータベースをインストールすることを推奨します。

  CA Server Automation を単一のインスタンスで運用する必要がある場合は、Quad-Core プロセッサと 16 GB の RAM を備えたマネージャ サーバとデータベース サーバを使用することを推奨します。

  リモート展開およびポリシー設定の操作をサポートするために、各データ センターに 1 つの配布サーバをインストールすることを推奨します。3 つの配布サーバの内の 1 つはマネージャ システムにインストールします。

- 初期展開

  この使用事例では、データセンターに 1 つの配布サーバが追加されています。 セットアップ時の 1 つの相違を除いて、前のシナリオで強調されたすべての要因が、このシナリオにも等しく適用されます。

- サービス メンバシップ

  保守を容易にするために、管理対象のサーバを、1 サービス当たり 500 サーバを目安として、複数のサービスに分割することを推奨します。

- ポリシーの適用

  ベース ポリシーを、制御設定と「ベース OS」モニタに制限することを推奨します。 異なる複数のイメージが仮想マシンのベースとして使用されている場合、ベース ポリシーを各 OS イメージについて作成することができます。 登録時にこのポリシーを要求するように SystemEDGE が設定されていることを確認してください。

  アプリケーション固有のモニタについては、個別のモニタリング要件に基づいてテンプレートを作成します。 テンプレート間のインデックス競合を回避するために、各アプリケーションに「インデックス範囲」を事前に定義することを推奨します。 あるいは、ベース ポリシーを、「制御設定」セクションで「インデックスの競合を自動的に解決する」に設定できます。

  モニタリング要件を複数のテンプレートに分割すると、必要なシステムに必要なテンプレートを個別に適用できます。 手動でシステムを選択するか、またはサービスにテンプレートを適用することによって、個別に適用できます。 テンプレートの適用は、2,000 ～ 2,500 のシステムに分けて行うことを推奨します。

  ベース ポリシーを変更する必要がある場合、2,000 ～ 2,500 のシステムに分けてポリシーを適用することを推奨します。

  注: テンプレートを使用する場合、テンプレートまたはポリシーの各配信において、すべての割り当て済みテンプレートがベース ポリシーにマージされます。 次の手順は、結果の設定のエージェントへの配信です。 そのため、複数のテンプレートがシステムに適用される場合、配信時間がわずかに長くなることがあります。

  重要: CA Server Automation の複数のインスタンスが展開されており、作成されたポリシーを異なるインスタンス間で共有したい場合は、CA サポートにお問い合わせください。 CA サポートは、CA Server Automation インスタンス間でのポリシーおよびテンプレートのエクスポートおよびインポートに関して支援できます。

付録 A: FIPS 140-2 の暗号化

このセクションには、以下のトピックが含まれています。

FIPS の概要

連邦情報処理標準（FIPS） 140-2 は、製品が暗号化に使用すべき暗号のライブラリおよびアルゴリズムのセキュリティ標準です。 FIPS 140-2 の暗号化は、CA 製品のコンポーネント間、および CA 製品とサードパーティ製品間におけるすべての機密データの通信に影響を与えます。 FIPS 140-2 は、取り扱い注意ではあるが機密扱いではないデータを保護するセキュリティ システムの中で暗号アルゴリズムを使用するための要件を規定しています。

CA Server Automation では、米国政府が採用している高度暗号化標準（AES）を使用します。CA Server Automation には、RSA Crypto-J v3.5 および Crypto-C ME v2.0 暗号ライブラリが組み込まれています。これらは、FIPS 140-2 の暗号モジュール セキュリティ要件を満たしていることが確認されています。

付録 B: ツール

このセクションには、以下のトピックが含まれています。

NodeCfgUtil による AIM の設定

Node Config Utility を使用すると、CA Server Automation ユーザ インターフェースを使用せずに、SystemEDGE AIM を設定できます。

このセクションでは、このユーティリティのダイアログ モードおよびコマンド モードについて説明します。

関連項目:

NodeCfgUtil の概要

AIM を設定して仮想環境を検出するには、以下の*いずれか*のアクションを実行します。

- ユーザ インターフェースから［管理］タブを開いて［設定］-［プロビジョニング］に移動し、認証情報を追加して AIM を設定する適切なサーバ タイプを選択します。 CA Server Automation は自動的に物理コンポーネントおよび仮想コンポーネントを検出し、管理データベース取り込みます。
- Windows AIM サーバ上で NodeCfgUtil.exe ユーティリティを使用して、仮想環境管理に必要なデータを追加します。 ユーティリティは *SystemEDGE_install_path*¥plugins¥AIPCommon ディレクトリにあります。次に、CA Server Automation マネージャから AIM サーバを再検出します。このオプションでは、必要な手順を手動で実行できます。

以下のガイドラインを考慮してください。

- 仮想環境またはクラスタへのアクセス用に指定されたユーザには、リモート アクセスを許可する権限が必要です。
- Hyper-V Server を管理するには、Hyper-V Server に SystemEDGE および Hyper-V AIM をインストールします。 SystemEDGE と Hyper-V AIM は、同じ Hyper-V Server 上で実行する必要があります。 次に、AIM を設定し、Hyper-V Server を検出します。
- Citrix XenServer AIM は、プール マスタまたはスタンドアロンの Citrix XenServer にのみ接続できます。 そうしないと、AIM が動作しません。
- VMware vSphere を管理するには、対応する vCenter Server の認証情報を入力します。
- VM の仮想化を最適化するには、対応するシステム ツールを VM にインストールします。 多くの機能は、これらのツールがインストールされている場合にのみ使用できます。 ユーザの環境に応じて、以下のシステム ツールを使用します。
  - （VMware の場合） VMware ツール
  - （XenServer の場合） XenTools
  - （RHEV の場合） RHEV Guest Tools

  注: 対応するシステム ツールの詳細については、サードパーティのドキュメントを参照してください。

AIM サーバからサポートされる環境を検出する方法

1. CA Server Automation マネージャ サーバ上で実行されない SystemEDGE および AIM が、これらに関連付けられた CA Server Automation マネージャと同じ SNMP 設定を使用することを確認します。
2. Windows AIM サーバで NodeCfgUtil.exe ユーティリティを実行して、対応する AIM の設定データを更新します。

   NodeCfgUtil.exe ユーティリティは、ファイル（zone.cfg、vc.cfg など）内の AIM ごとにデータを格納します。
3. マネージャ サーバでユーザ インターフェースを開き、［リソース］、ナビゲーション ペインの［データ センター］の順にクリックします。
4. 右クリックし、［管理］-［検出］を選択します。

   ディスカバリ オプションが表示されます。
5. 以下のいずれかのアクションを選択します。
   - システムの検出
   - ネットワークの検出

   対応するダイアログ ボックスが開きます。
6. 管理するサーバのシステム名を入力します。 あるいは、ディスカバリ プロセス用のネットワーク プロパティを入力できます。 ［OK］をクリックします。

   CA Server Automation がディスカバリ プロセスを開始します。

   検出されたリソースが［エクスプローラ］ペインに表示されます。

関連項目

vCenter Server 管理コンポーネントを設定する方法 (P. 603)

ダイアログ モードの NodeCfgUtil による AIMs の設定

NodeCfgUtil.exe を使用して、IBM PowerVM、IBM PowerHA、Solaris ゾーン、VMware vCenter、VMware vCloud、Microsoft クラスタ、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory および Exchange Server（ADES）、および Huawei GalaX 用の AIM 設定を変更できます。 このユーティリティは、対応する AIM の設定ファイルを *sysedge_InstallLpath¥plugins¥AIPCommon* ディレクトリに書き込みます。また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。

このユーティリティをダイアログ モードで使用すると、適切な AIM が管理するノードを設定できます。

注: NodeCfgUtil.exe は Windows 管理者として実行してください。

次の手順に従ってください:

1. AIM がインストールされているコンピュータで管理者としてログインし、Windows エクスプローラを開きます。
2. *SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリに変更し、NodeCfgUtil.exe を起動します。

   NodeCfgUtil によって、インストールされた AIM が検出され、その後に表示されるダイアログ ボックスに一覧表示されます。
3. *1* を入力して、新しい管理対象ノードを追加します。
4. 画面上の指示に従って、設定を完了します。 各ノードには、認証用の有効なユーザ名とパスワードが必要です。

   設定が完了したら、0 を入力して前のメニューに戻るか、またはユーティリティを終了します。

NodeCfgUtil は、*SystemEDGE_InstallPath*¥plugins¥AIPCommon ディレクトリに、Solaris ゾーン（zone.cfg）、vCenter Server （vc.cfg）、vCloud Director（vcloud.cfg）、Microsoft クラスタ（mscs.cfg）、Citrix XenServer（cxen.cfg）、UCS（ucs.cfg）、PowerVM（lpar.cfg）、PowerHA（hacmp.cfg）、RHEV（kvm.cfg）、Huawei GalaX（galaxa.cfg）、Citrix XenDesktop（xendesktop.cfg）、または ADES（esad.cfg）用の設定ファイルを書き込みます。

注: また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。 対応するダイアログ ボックスには、目的に応じた名前が付けられています。

例

以下の例は、vCenter AIM の設定に正常に追加された myvc5 サーバに関する[管理対象ノードのインストール]ダイアログを示します。AIM は現在、vCenter Server サーバを管理できる状態です。 vCenter AIM はマルチインスタンス AIM です。 したがって、この手順を繰り返し、この AIM で管理する vCenter Server をさらに追加できます。

```
***** メイン メニュー *****
1. 管理対象ノードのインストール
2. 管理対象ノードの変更

3. 管理対象ノードの削除

0. 終了

**********************

選択項目を入力してください:

**** 管理対象ノードの選択 ****
1. IBM PowerVM
2. Oracle Solaris ゾーン
3. Citrix XenServer
4. VMware vCenter
5. Cisco UCS
6. Microsoft Cluster Service
7. Microsoft Active Directory および Exchange Server
8. IBM PowerHA
9. VMware vCloud Director
10. Red Hat Enterprise Virtualization
11. Huawei GalaX
12. Citrix XenDesktop
0.  前のメニューに戻る
******************************
選択項目を入力してください: 4
```

```
VMware vCenter ノードの以下の情報を入力します...

（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）。

1. サーバ名： myvc5
2. ユーザ名： administrator
3. パスワード： *********
4. ポート [デフォルト=443]:
5. プロトコル [デフォルト=https]:

CAAC1016 認証しています。お待ちください...
CAAC1019 認証に成功しました。
CAAC1023 ノードが正常に追加されました。

キーをどれか押してください...
```

以下の例は、ADES AIM の設定に正常に追加された mydomain に関する［管理対象ノードのインストール］ダイアログ ボックスを示します。 管理エンティティは Active Directory に設定されます。管理モードはドメイン全体に設定されます。 詳細については、NodeCfgUtil コマンド モードを参照してください。 ADES AIM はマルチインスタンス AIM です。 したがって、この手順を繰り返し、この AIM で管理するエンティティをさらに追加できます。

```
**** 管理対象ノードの選択 ****
1. Microsoft Cluster Service
2. Microsoft Active Directory および Exchange Server
0. 前のメニューに戻る ********************************
選択項目を入力してください: 2
Microsoft Active Directory および Exchange Server ノードの以下の情報を入力します...

（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）。

1. ドメイン名： mydomain
2. ユーザ名： administrator
3. パスワード： ************
4. 管理エンティティ： 0
5. 管理モード： 0

CAAC1016 認証しています。お待ちください...
CAAC1018 認証に成功しました。

キーをどれか押してください...
```

以下の例は、LPAR AIM の設定に正常に追加された HMC1 サーバ用の［管理対象システム］ダイアログ ボックスを示します。 AIM が HMC サーバに関連したすべての仮想 I/O サーバを検出した後、それらのサーバは NodeCfgUtil に表示されるため、各サーバを変更してその認証情報を指定できます。 AIM は、完全に設定された最初の VIO サーバの認証情報を、まだ設定されていないすべての VIO サーバのデフォルト認証情報として使用します。そのため、すべての VIO サーバが認証情報を共有している場合は、1 つの VIO サーバのみの認証情報を指定すれば十分です。そうでない場合は、各 VIO サーバに異なる認証情報を設定する必要があります。 AIM は現在、HMC サーバを管理できる状態です。

```
**** 管理対象ノードの選択 ****
1. IBM PowerVM
0. 前のメニューに戻る
******************************
選択項目を入力してください: 1
既存のエントリのリスト...
1. hmc: HMC1.company.com
2. vio: ibm101.company.com
変更するエントリを選択します（前のメニューに戻るには 0 を選択します）: 2
IBM LPAR ノードの以下の情報を入力します...
（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）。
1. サーバ名: ibm101
2. ユーザ名: admin
3. パスワード： *********

CAAC1016 認証しています。お待ちください...
CAAC1019 認証に成功しました。
CAAC1024 ノードが正常に変更されました。

キーをどれか押してください...
```

以下の例は、GalaX AIM の設定に正常に追加された *mycluster* に関する［管理対象ノードのインストール］ダイアログ ボックスを示します。 詳細については、NodeCfgUtil コマンド モードを参照してください。GalaX AIM はマルチインスタンス AIM です。 したがって、この手順を繰り返し、この AIM で管理するエンティティをさらに追加できます。

注: Huawei Galax8800 コンポーネントを設定するには、証明書ファイル名を指定する必要があります。

```
**** 管理対象ノードの選択 ****
1. Huawei GalaX
0. 前のメニューに戻る
******************************
選択項目を入力してください: 1
```

```
GalaX HACMP ノードの以下の情報を入力します。

（いずれかの時点で前のメニューに戻るには、Ctrl + Q キーを入力します）。

1. サーバ名： myserver
2. 証明書ファイル名： certificatename123.p12
3. パスワード： ************
4. ポート [default =8773]:
5. プロトコル [default =http]:

CAAC1016 認証しています。お待ちください...
CAAC1018 認証に成功しました。

キーをどれか押してください...
```

コマンド モードの NodeCfgUtil による AIM の設定

NodeCfgUtil.exe を使用して、IBM PowerVM、IBM PowerHA、Solaris ゾーン、VMware vCenter、VMware vCloud、Microsoft クラスタ、Cisco UCS、Citrix XenServer、Citrix XenDesktop、RHEV、Active Directory および Exchange Server（ADES）、および Huawei GalaX 用の AIM 設定を変更できます。 このユーティリティは、対応する AIM の設定ファイルを *sysedge_InstallLpath¥plugins¥AIPCommon* ディレクトリに書き込みます。 また、NodeCfgUtil ユーティリティを使用して、既存のエントリの編集または削除を実行できます。

このユーティリティをコマンド モードで使用する場合、AIM 設定に追加できるのは管理対象ノードのみです。

注: NodeCfgUtil.exe は Windows 管理者として実行してください。

このコマンドの形式は、以下のとおりです。

```
(1) nodecfgutil -help
(2) nodecfgutil {lpar|zone|mscs} -u user -p password -h
{pvmname|hostname|cluster_name}
(3) nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol
(4) nodecfgutil ades -u user -p passwd -d domainname -e entity -o option
(5) nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname
(6) nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name|hostname} [-t port]
(7) nodecfgutil galax -u usercertificate -p password -h hostname [-t port] [-c
protocol]
```

-help

コンソールに関する使用情報が表示されます。

lpar|ucs|vc|zone|mscs|ades|xen|vcloud|powerha|kvm|galax|xendesktop

仮想環境または物理環境を指定します。

-u *user|usercertificate*

管理者ユーザの名前またはユーザ証明書をそれぞれ指定します。

-p *password*

そのユーザのパスワードを指定します

-h *hostname*

対応する AIM で管理されるサーバの名前を指定します。

-d *domainname*

ADES AIM でモニタするドメインの名前を指定します。

-h *pvmname*

LPAR AIM で管理する IBM PowerVM サーバ（HMC または IVM）の名前を指定します。

- h *cluster_name*

クラスタの名前を指定します。

-t *port*

（オプション）ポート番号を指定します。

-c *protocol*

（vCenter および UCS のみ）プロトコル（HTTP、https）を指定します。

リターン コード： 0 は成功、-1 は失敗

-e *entity*

管理対象エンティティを指定します。

0

Active Directory をモニタリングの対象にします。

1

Exchange Server をモニタリングの対象にします。

2

Active Directory および Exchange Server の両方をモニタリングの対象にします。

-o *option*

管理のオプションを指定します。

0

ドメイン全体をモニタリングの対象にします。

1

ドメインの特定のホストをモニタリングに対象にします。

次の手順に従ってください:

1. AIM がインストールされているシステムでコマンド プロンプトを開きます。

   コマンド プロンプトが表示されます。

2. 以下のコマンドの*いずれか*を入力します。

```
(1) nodecfgutil -help
(2) nodecfgutil {lpar|zone|mscs} -u user -p password -h
{pvmname|hostname|cluster_name}
(3) nodecfgutil {vc|ucs} -u user -p password -h hostname -t port -c protocol
(4) nodecfgutil ades -u user -p passwd -d domainname -e entity -o option
(5) nodecfgutil {xen|vcloud|xenserver} -u user -p passwd -h hostname
(6) nodecfgutil {powerha|kvm} -u user -p password -h {cluster_name|hostname} [-t
port]
(7) nodecfgutil galax -u usercertificate -p password -h hostname [-t port] [-c
protocol]
```

(1) コンソールに関する使用情報が表示されます。

(2) Solaris ゾーン、IBM PowerVM、または MSCS に対して渡された認証情報を認証および格納します。

(3) vCenter または Cisco UCS に対して認証を実行し、正しい認証情報を格納します。

(4) Active Directory および Exchange Server （ADES）に対して認証を実行し、正しい認証情報を格納します。

(5) Citrix XenServer、Citrix XenDesktop、または VMware vCloud に対して認証を実行し、正しい認証情報を格納します。

(6) IBM PowerHA または Red Hat Enterprise Virtualization （KVM）に対して認証を実行し、正しい認証情報を格納します。

(7) HUAWEI Galax に対して認証を実行し、正しい認証情報とユーザ証明書を格納します。

サポート エージェント

サポート エージェントは診断情報を収集します。 サポート エージェントにアクセスするには、以下のアドレスを使用します。

http://<Manager Server>:8556

ユーザ インターフェースは説明がなくてもわかりやすく、以下の情報を提供します。

- システムの重要な部分のパフォーマンス メトリック
- 詳細な Web サービス使用率統計
- ログ ファイル モニタリング
- 長時間の SQL クエリ

付録 C: トラブルシューティング

このセクションには、以下のトピックが含まれています。

CA Server Automation トラブルシューティング

このセクションには、CA Server Automation のトラブルシューティング トピックが含まれます。

注: セキュリティ証明書リクエストを受信した場合は、それを無視して続行します。 このようなメッセージが表示されないようにするには、任意のベンダーから証明書を取得して、サーバにそれを適用します。 セキュリティ証明書のインストールの詳細については、Apache Tomcat の Web サイトを参照してください。

関連項目:

Solaris ゾーン環境でのポーリング間隔設定の調整

症状:

Solaris ゾーン環境でポーリング間隔の設定を調整する方法がわかりません。

解決方法:

システムとゾーンの数が増加する場合は、Solaris ゾーン AIM のポーリング間隔を増加させます。たとえば、ホストとゾーンの数が 100 を超える場合は、デフォルト ポーリング間隔を 240 に設定します。

属性にゼロの値が表示される

症状:

属性にゼロの値が表示される

解決方法:

値が 1 よりも小さい場合、SystemEDGE は値を切り捨ててゼロにします。

注: zoneAimStatHostDiskSvc MIB 属性には、常にゼロの値が表示されます。

ブラウザにイベントの連続するスペースが表示されない

症状:

ブラウザにイベント説明の複数の連続するスペース文字が表示されません。

解決方法:

追加のスペースは HTML 仕様に応じて切り詰められるので、ブラウザには複数の連続するスペースが表示されません。 ブラウザからイベントを切り取ってルールに貼り付ける場合はイベント説明が異なる場合があるため、注意を要します。

Cisco UCS フォルダが UI 内に表示されない

症状:

Cisco UCS サービスの製品インストールを設定した後で、Cisco UCS フォルダがユーザ インターフェースに表示されません。

解決方法:

UCS AIM が設定されているサーバで［サービス］を開いて SystemEDGE が実行されていることを確認します。SystemEDGE サービスが停止している場合は、それを再起動します。 nodecfgtutil.exe を開始して UCS Manager ノードのアクセス情報を確認します。 MIB ブラウザを使用して UCS Manager からのデータ ポーリングを確認します。UCS アクセス情報が入力されていない場合は、追加情報を sysedge ログで確認します。

DB トランザクション ログ サイズが予期せずに増加する

症状:

多数の管理対象オブジェクト、設定変更およびメトリック データ収集アクティビティがあるデータ センターでは、管理データベースおよびパフォーマンス データベースのログが予期せずに増加する場合があります。この問題は制限のあるリソースを使用する環境ではディスク領域を低下させる原因となる場合があります。

解決方法:

この問題を解決するには、Microsoft サポートの Web サイトにある、完全なトランザクション ログのトラブルシューティングについての KB 記事を参照してください。

トランザクション ログ ファイル、aom2.ldf および dpm.ldf は、デフォルト Microsoft SQL Server インストールのディレクトリ C:¥Program Files¥Microsoft SQL Server¥...¥MSSQL¥Data にあります。

注: データベース ログ ファイルのサイズが縮小される場合は、Apache のサービスを再起動してパフォーマンスを改善してください。

廃止された Solaris ゾーン AIM 属性で常に N/A またはゼロが表示される

症状:

Solaris ゾーン AIM MIB のいくつかの値に常に N/A またはゼロが表示されます。

解決方法:

Solaris ゾーン AIM のこれらの MIB 属性は廃止され、下位互換性のために残されています。 廃止された MIB 属性は以下のとおりです。

- zoneAimStatHostDiskMode
- zoneAimStatProcessorSetContainerList
- zoneAimStatProcessorSetResourcepoolId
- zoneAimStatProcessorSetResourcePoolIdList
- zoneAimStatProcessorSetResourcepoolName
- zoneAimStatProjectFSSEnabled
- zoneAimStatResourcePoolContainerList

ドメイン サーバが使用できない

症状：

ドメイン サーバが使用できないか、停止されたか、機能していないか、または要求を処理しておらず、サービス コントローラ (SC) はこのコンポーネントが稼働中であることを示しています。

解決方法：

この動作は、データベース接続の失敗または AIM パスワードの期限切れのために発生し、ポリシー設定およびリモート展開コンポーネントの動作に影響を与える可能性があります。 サポート サービスの Web サービス（ISM）をモニタすると、ドメイン サーバの機能が定期的にモニタされます。 ISM によって予期しない動作が識別されると、ユーザには「*CA SM ドメイン サービスはダウンしているか応答していません*」というメッセージでステータスの変更が通知されます。

このステータスは、以下のコマンドでモニタできます。

```
Caaipscutil /status /id=ISM /user=<ユーザ> /password=<パスワード>
```

インフラストラクチャの状態および機能を確認するために、［管理］パネルにはドメイン サーバのステータスが示されます。

dpmvc virtualswitch コマンドでの空のタスク ID

症状:

dpmvc virtualswitch コマンドを実行すると、空のタスク ID が表示されます。

解決方法:

この操作は非同期で実行されず、結果はただちに返されます。 ただし、PMM はこの操作をタスク化された操作として扱います。 そのため、応答にはタスク ID が含まれますが、それは常に空の文字列（""）です。

たとえば CLI から以下のコマンドを実行すると、空のタスク ID が表示されます。

```
dpmvc virtualswitch -vs_add -vc_server MYVC5 -switch_name XYZ
-esx_host_name MYESX -ws_user admin -ws_password ca_admin
```

CLI の出力

```
...
SC URL: https://VASManager/aip/sc
VC URL: https://VASManager:443/aip/vc
Task ID:
Command execution successful
```

dpmvc faulttolerance や dpmvc distributedswitch などのほかのコマンドは非同期に実行され、タスク ID が表示されます。

ローカル モニタとリモート モニタに同じ値が表示されない

症状:

ローカル モニタとリモート モニタで、同じ属性に同じ値が表示されません。

解決方法:

シームレスなローカルおよびリモート モニタリングでは、同一のモニタ対象オブジェクト名を選択できます。 ただし、異なる API では異なる値を返す場合があります。

リモート マシン上の SystemEDGE は、サーバ上で RM AIM から独立して実行され、それらのポーリング スケジューラの開始ポイントは同期できません。 モニタ対象メトリックは非常に変化しやすいため、サンプルが異なる可能性があります。

AIX システム上での SystemEDGE インストーラのナビゲーションの問題

症状:

AIX 6.1 および 7.1 に SystemEDGE をインストールすると、lsm （UNIX インストーラ）テキスト ユーザ インターフェースのナビゲーションが動作しません。 この問題は、Advanced Encryption および SRM AIM でも発生します。

解決方法:

他の UNIX オペレーティング システムおよび古い AIX バージョン上での場合と異なり、TERM が（通常の）xterm の値に設定されていると、AIX 6.1 および 7.1 上では lsm テキスト ユーザ インターフェースのナビゲーションが機能しません。Java ベースのグラフィカル lsm UI を使用すると、この問題は発生しません。

回避策としては、インストールを開始する前に TERM を別の値（たとえば vt100）に設定し、［+］および［-］キーを使用してナビゲートするか、または、（PuTTY の場合のみ）アプリケーション カーソル キー モードを無効にするよう設定します。

NodeCfgUtil は XenDesktop コントローラへの接続を検証できない

症状:

NodeCfgUtil は、XenDesktop コントローラへの接続を検証できません。

解決方法:

XenDesktop AIM がインストールされているマシンに以下のコンポーネントがインストールされていることを確認します。

- Microsoft .NET Framework 4.0
- Windows Management Framework Core （Windows PowerShell 2.0、Windows Remote Management （WinRM） 2.0）

Solaris Lists SPARC および x86 システムへのリモートでの展開

症状:

Deployment UI にリスト表示されたコンピュータは、通常展開している選択済みオペレーティング環境にフィルタされます。 ただし、以下の状況の場合は、リストされている選択済みオペレーティング環境以外のコンピュータを表示できます。

- Solaris x86 または Solaris SPARC サーバのいずれかに展開した場合、リスト表示されたサーバは、ターゲット オペレーティング環境として Solaris x86 または Solaris SPARC を選択したかどうかにかかわらず、すべての Solaris アーキテクチャ向けです。
- 分類されていない任意のコンピュータに展開した場合。

解決方法:

展開が正常に行われるように、ターゲット コンピュータが選択済みのエージェント アーキテクチャと一致することを確認します。 リスト表示されたすべてのコンピュータを選択して続行すると、展開は一致するアーキテクチャでは成功し、一致しないアーキテクチャでは失敗します。

vCenter Server を削除すると、別の管理対象 vCenter Server のオブジェクトが非表示になる

症状:

vCenter Server を管理から削除すると、別の管理対象 vCenter Server のオブジェクトが予期せず非表示になります。

解決方法:

製品管理の問題を回避するには、別の vCenter Server を管理している VM に vCenter AIM をインストールしないでください。 その VM に関連付けられている vCenter のモニタリングと管理を CA Server Automation から削除すると、AIM を実行している VM システムを含め、vCenter に関連付けられているオブジェクトが削除されます。

vCenter Server のパスワードを変更するとデータ収集に失敗する

症状:

VMware vCenter Server と通信するために CA Server Automation が使用しているユーザの VMware vCenter Server パスワードをリセットした後で、データ収集が機能しません。

解決方法:

新しいパスワードで vCenter AIM 設定を更新します。 パスワードは、ユーザ インターフェースの［管理］タブ、または vCenter AIM が実行されているサーバの NodeCfgUtil から更新できます。

モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされる

症状:

モニタされたシステムがダウンしている場合は Solaris ゾーン AIM がリセットされます。

解決方法:

モニタされたシステムのうちの 1 つがダウンしている間に、AIM をリセットした場合、AIM は各ポーリング間隔でそのシステムをポーリングします。 AIM はシステムが再度稼働するまで、プロパティを更新しません。

コンポーネントのステータス アイコンが[設定されていません]を示している

症状:

CA Server Automation によってコンポーネントがインストールされた後、このコンポーネントのステータス アイコンが⚠（[設定されていません]）を示しています。 このステータスは、CA Server Automation が、未設定のサーバに接続されているコンポーネントを登録した場合に表示されます。

解決方法:

このコンポーネントのステータスを「準備完了」に変更するには、不足しているサーバ接続の設定および検証を追加します。

Microsoft SQL サーバに接続できない

症状:

Microsoft SQL Server （評価版）への認証情報を認証する試行が、製品のインストール中に失敗します。 エラー メッセージ［MSSQL への接続を確立できませんでした］が表示されます。

解決方法:

この問題は、TCP/IP が評価版ではデフォルトで無効になるために発生します。 TCP/IP を有効にします。

SystemEDGE のアップグレード

症状:

SystemEDGE を リリース 5.8 にアップグレードすると、以前の CA Server Automation リリースの AIM が実行されません。

解決方法:

Advanced Encryption およびすべての AIM を CA Server Automation リリース 12.8 にアップグレードします。 SystemEDGE リリース 5.8 は、以前の CA Server Automation リリースの AIM をロードしません。

製品のアップグレードがユーザ インターフェースに反映されない

症状:

CA Server Automation を新バージョンにアップグレードしたのに、ユーザ インターフェースに反映されない。

解決方法:

アップグレード後、アップグレード前と同じブラウザ インスタンスを使用している場合、ユーザ インターフェースに新しいバージョンが反映されない可能性があります。 ブラウザ セッションを閉じて新たに開き、ブラウザのキャッシュをクリアして、ユーザ インターフェースにログインします。

ユーザ インターフェースが動作しない

症状:

Windows 認証を使用してリモートの SQL Server を使用すると、ユーザ インターフェースが正常に動作しません。

解決方法:

インストール中に、適切なドメイン ユーザを追加し、「サービスとしてログオン」権限を付与するように指示されます。 このドメイン ユーザ アカウントに対して、CAAIPTOMCAT、CAAIAPACHE、および CA SM Domain Server サービスが設定されていることを確認します。サービスを再設定しなかった場合、CA Server Automation ユーザ インターフェースは機能しません（ダッシュボードが空であるか、機能が動作しない）。

これらの条件は SQL Server 認証では必要ありません。

次の手順に従ってください:

1. ［コントロール パネル］の［管理ツール］から［サービス］ダイアログ ボックスを開きます。

   使用可能なサービスのリストが表示されます。

2. CA SM ドメイン サーバ、CAAIAPACHE サービス、および CAAIPTOMCAT サービスの［プロパティ］ダイアログ ボックスを開きます。
3. 各ダイアログ ボックスの［ログイン］タブに移動し、［以下のアカウント］を選択します。次に、参照できる有効な認証情報（ドメイン ユーザ アカウント）を入力します。
4. このドメイン ユーザ アカウントを両方のシステム（マネージャ サーバとデータベース サーバ）のローカル Administrators グループに追加します。
5. このドメイン ユーザ アカウントを SQL Server の sysadmin （または dbcreator 以上）のサーバ役割に追加します。

プロビジョニング画面およびポリシー画面でユーザ インターフェースが応答しない

症状:

プロビジョニング ページまたはポリシー ページを表示しているときにデータベース サーバが再起動すると、ユーザ インターフェースは空白になるかまたは反応がありません。

解決方法:

CA Server Automation ユーザ インターフェースからログアウトして再度ログインします。

vCenter Server AIM 属性にゼロが表示される

症状:

vCenter Server 属性にゼロが表示されます。

解決方法:

以下のオブジェクト値は、vCenter Server AIM がローカル vCenter Server インスタンスにインストールされている場合にのみ取得できます。AIM がリモートである場合は、これらのパラメータにゼロ（0）が表示されます。

- vmvcAimStatServerCPUUsage [1.3.6.1.4.1.546.16.52.2.2.12.0]
- vmvcAimStatServerMemUsage [1.3.6.1.4.1.546.16.52.2.2.17.0]
- vmvcAimStatServerTotalPhysMem [1.3.6.1.4.1.546.16.52.2.2.18.0]
- vmvcAimStatServerUsedPhysMem [1.3.6.1.4.1.546.16.52.2.2.19.0]

VM 使用率の値が電源オフ後にすぐに更新されない

症状:

VM 使用率の値が電源オフ後にすぐに更新されません。

解決方法:

VM の電源が切られた後で、使用率の値は次の正常なポーリングまで 0 にドロップしません。ポーリングには最大 5 分かかります。これはデフォルトのデータ収集および記録間隔です。

アップグレード後の空白の[クエリ結果]タブ

症状:

アップグレード後、リモート モニタリング クエリ結果に空白の値が表示されます。

解決方法:

システムの追加時、RM PMM には、FQDN （Fully Qualified Domain Name、完全修飾ドメイン名）表記法に準拠しているリモート システム名が必要です。 ただし、RM AIM では既存のシステムが FQDN でない名前のまま残されます。 この名前の不一致が原因となって、空白のクエリ結果が表示されます。 この名前の不一致は、以下のように修正できます。

アップグレード前の変換

- リフレッシュ UI にログインし、リモート モニタリングから FQDN でないシステムをすべて削除します。

  関連付けられたシステム、クエリ、インスタンス、およびモニタが、両方のマネージャ（データベース）、および RM AIM プラグインを持つ SystemEDGE エージェントからすべて削除されます。
- FQDN 表記法を使用してこれらのシステムを再度追加し、同じ設定セットを指定して、関連付けられたクエリ、インスタンス、およびモニタを再作成します。
- アップグレードを実行します。

アップグレード後の変換

- SystemEDGE エージェント マシンにログインし、Refresh RM AIM プラグインを実行します。
- 現在のリモート モニタリング設定が含まれる rmonwbem.cf ファイルをデータ ディレクトリ パスで検索し、このファイルのコピーを作成します。 たとえば、rmonwbem-upgrade.cf として保存します。
- リフレッシュ UI にログインし、リモート モニタリングから FQDN でないシステムをすべて削除します。

  関連付けられたシステム、クエリ、インスタンス、およびモニタが、両方のマネージャ（データベース）、および RM AIM エージェント マシンからすべて削除されます。

- ここでアップグレードを実行します。 エージェント マシンで、rmonwbem-upgrade.cf を入力ファイルとして指定して *rmonwatch add* コマンドを実行します。 この処理により、すべてのシステムおよび関連付けられたクエリ、インスタンス、およびモニタが FQDN 表記法で再度追加されます。

  注: アップグレード後の変換方法には、システムを自動的に再度追加し、UI からシステムを設定できる長所があります。

アップグレード変換の後には、クエリ結果に値が表示されます。

設定の後、CA Process Automation サーバへのアクセスに認証情報が要求される

症状:

dpmutil -set -itpam-cfg-eem コマンドを使用して CA Process Automation EEM ユーザ名とパスワードを設定しても、CA Server Automation から CA Process Automation サーバにアクセスすると、認証情報の入力を要求されます。この問題は、JDK 6 環境の Java Cryptography Extension ポリシーに影響を及ぼす輸出規制に起因します。

解決方法:

この問題を解決するには、Oracle Sun Developer Network （SDN）から jce_policy-6.zip をダウンロードしてインストールに以下の JAR ファイルを適用します。

- local_policy.jar
- US_export_policy.jar

CA Server Automation によってインストールされたファイルをダウンロードしたファイルで置き換えます。

サポートされない CA DSM の機能がある

症状:

CA Server Automation で使用できない CA ITCM の機能がある

解決方法:

サポートされていない機能は以下のとおりです。

- ImageX の GETIMAGE
- Microsoft Automated Deployment Services （ADS）
- クラスタのフェールオーバ
- ソフトウェア ジョブの優先順位付け
- プラットフォーム仮想化
- Windows Embedded for Point of Service （WEPOS）
- モデル コンピュータのバックアップとリストア
- ソフトウェア配信ジョブ完了時のコンピュータのシャットダウン
- カスタムの管理者メッセージ

CA Network Automation スクリプトが Cisco 5000 スイッチ デバイス上で失敗する

症状:

Cisco 5000 スイッチ ファミリ デバイス上で CA Network Automation スクリプトを実行すると、ジョブが終了するかスキップされます。

解決方法:

NetMRI がデバイスを正しく検出していません。 ネットワーク管理者によって、デバイスがスイッチまたはスイッチ-ルータとして設定されていることを確認してください。

注: CA Network Automation スクリプトは、 スイッチおよびスイッチ-ルータ デバイス上（例： Cisco 5000 スイッチ ファミリ）で実行されることが想定されています。

CA Configuration Automation エージェントがインストール中に停止する

症状:

CA Configuration Automation エージェントをインストールすると、インストールが停止します。

解決方法:

いくつかのシステムで、Windows DEP オプションが javaw.exe の実行を妨げます。 CA Configuration Automation エージェント インストールに javaw.exe を使用するために、インストールが停止します。 この問題を解決するには、以下の手順に従います。

1. Windows の［コントロール パネル］を開き、［システム］をダブルクリックします。

   ［システムのプロパティ］ダイアログ ボックスが表示されます。

2. ［詳細設定］をクリックし、次に、［パフォーマンス］セクションで［設定］をクリックします。

   ［パフォーマンス オプション］ダイアログ ボックスが表示されます。

3. ［データ実行防止］タブをクリックします。

4. ［重要な Windows プログラムおよびサービスについてのみ有効にする］を選択し、［OK］をクリックします。

CA ITCM から削除された OS イメージが CA Server Automation から削除されない

症状:

CA ITCM からすべての OS イメージを削除した後で、それらは CA ITCM には表示されなくなりましたが、CA Server Automation にはまだ表示されます。

解決方法:

この問題を解決するには、OS イメージを CA ITCM だけでなく、ソフトウェア パッケージ ライブラリからも削除します。

大規模ネットワークのディスカバリ

症状：

ディスカバリでは、1024 を超えるノードが含まれるネットワーク（たとえば 255.255.0.0 のサブネット マスクを使用する Class B ネットワーク）を検出できません。

解決方法：

ネットワーク ディスカバリをより小さなサブネット（たとえば 255.255.255.0 のサブネット マスクを使用する Class C ネットワーク）で実行します。 大規模ネットワーク上でディスカバリに失敗する場合は、以下のプロシージャに従ってディスカバリ データベースをクリーンアップします。

1. Network Discovery Gateway がインストールされているサーバの Windows サービス コントロールで以下のサービスを停止します。
   - Network Discovery Gateway
   - CA Server Automation Windows サービス
   - Network Discovery Gateway エージェント
   - Network Discovery Gateway サーバ
   - Apache 2.2
2. Network Discovery Gateway がインストールされているフォルダを開きます。 ファイルは以下のパスにあります。

   ```
   [CA Server Automation_installation_drive]:¥Program Files¥CA¥SC¥Network Discovery Gateway
   ```
3. *.sq3 ファイルを削除します。
4. 以下の順序で Network Discovery Gateway および CA Server Automation Windows サービスを開始します。
   1. Network Discovery Gateway エージェント
   2. Network Discovery Gateway サーバ
   3. Apache 2.2

ディスカバリでオペレーティング システムが識別されない

症状:

検出されたシステムおよびオペレーティング システムは、Windows の代わりに*その他*として分類されます。

解決方法:

ファイアウォールが有効な場合、インターネット トラフィックがブロックされるため、オペレーティング システムは識別されません。Windows としてオペレーティング システムを分類するには、ファイアウォールをオフにします。

管理対象フォルダに重複したゾーン エントリがある

症状:

CA Server Automation が複数の Solaris ゾーン ホストを検出しました。 エクスプローラの［管理対象］フォルダに同じ名前のゾーンが表示されます。

解決方法:

同じ名前のゾーンが異なる Solaris ゾーンに属する場合は、「重複した」エントリが表示されます。 ［管理対象］フォルダでリスト表示されたゾーンは同じ名前を持つ別のオブジェクトです。［Solaris ゾーン］フォルダでは、これらのゾーンはホストの下に表示されて、一意に識別できます。

Solaris ゾーン フォルダ

```
ZoneHost1
|-- ZoneA
ZoneHost2
|-- ZoneA
```

管理対象フォルダ

```
管理対象
|-- ...
|-- ZoneA
|-- ZoneA
|-- ...
```

CA DSM エージェントと Asset Management プラグインをインストールするとエラーが発生する

症状:

Windows サーバ上に CA DSM エージェント と Asset Management プラグインをインストールしようとすると、以下のエラーが発生します。
1619: このインストール パッケージを開くことができませんでした。

解決方法:

この問題は CA ITCM の既知の制限です。 回避策については、CA Software Delivery のドキュメントにある「MSI パッケージのネットワーク インストールが失敗します」を参照してください。Windows オペレーティング システムでの制限については、Microsoft サポート技術情報の記事（http://support.microsoft.com/kb/2022222/） で詳細に説明されています。

ESX ジョブステータスは最新だが OS のインストールが完了していない

症状:

CA ITCM を使用していて、ユーザ インターフェースは ESX/ESXi4.1 プロビジョニング ジョブステータスを「最新」として表示します。ブート イメージはターゲット システムに展開されましたが、OS イメージのインストールが開始されません。

解決方法:

OS イメージのインストールが終了するまで待機します。そうすれば、OS は使用できる状態になります。

ESX/ESXi マシンを検出できない

症状:

CA ITCM OSIM を使用してプロビジョニングされた ESX および ESXi マシンの検出に失敗し、以下のエラーが表示されます。
<machinename> の検出に失敗しました。

解決方法:

この問題は、ESX または ESXi マシンが DHCP 設定で割り当てられたホスト名を取得することを許可しない VMware の制限です。回復するには、以下の手順に従います。

1. VI クライアントまたはコンソールを使用して、ESX/ESXi マシンのホスト名を、ESX/ESXi マシンがプロビジョニングされたときに CA Server Automation で指定された名前に変更します。
2. ホストを再起動します。
3. ホストを再検出します。

IE8 を使用する同じコンピュータに別のユーザ認証情報でログインする

症状:

同じコンピュータの 2 つの異なるウィンドウに 2 つの異なるユーザ アカウントでログインすると、1 つのユーザ アカウントのログイン情報がもう一つのユーザ アカウントを上書きします。 製品は、いずれかのユーザのセキュリティ属性により正しく動作しません。 この不一致は、UI がログイン情報を Internet Explorer 8 ブラウザのコンテキストに保存し、ブラウザがデフォルトでは他のブラウザ インスタンスとコンテキストを共有するために発生します。

注: Internet Explorer の以前のバージョンではこの問題がありません。

解決方法:

このように共有の結果発生する問題を回避するには、以下のいずれかのアクションを実行します。

- 異なるユーザ ログインには別のコンピュータを使用します。
- オプション *-nomerge* を使用して Internet Explorer 8 を開始します。 以下のコマンドを Windows コマンド ラインに入力するか、またはショートカットを作成または変更します。
  `C:¥Program Files¥Internet Explorer¥iexplore.exe" -nomerge`

  このオプションは、各ウィンドウで個別のコンテキストを使用するように Internet Explorer 8 に指示します。同じ Internet Explorer 8 ウィンドウ内の個別のタブは常にコンテキストを共有します。

エクスプローラ ペインに Cisco UCS Manager が表示されない

症状:

Cisco UCS PMM および AIM が設定されていて、ユーザ インターフェースに取り込む時間がありました。 しかしながら、Cisco UCS サーバが CA Server Automation エクスプローラ ペインにシャーシ、ブレード、内部接続、および組織情報と共に表示されません。

解決方法:

UCS Manager 名を確認する方法

1. Cisco ユーザ インターフェースを開きます。
2. ［Cisco 管理］ページで、Cisco Java UI システム名を検索し、その名前が DNS で解決可能かどうか確認します。名前が解決可能でない場合は、<drive>:¥WINDOWS¥system32¥drivers¥etc¥hosts ファイルを UCS Manager の正確な名前および IP アドレスで更新します。
3. 正しい UCS Manager システム名で UCS AIM を再設定します。
4. UCS Manager を登録します。
5. UCS AIM を登録します。
6. Cisco UCS Manager がエクスプローラ ペインに表示されることを確認します。

新しいシステム名が表示されない

症状:

システムの名前を変更し、そのシステムのディスカバリを実行してシステムを CCA サーバに割り当てても、システムが古い名前のまま表示されます。

解決方法:

新しい名前を表示するには、DNS サーバが、IP アドレスをシステム名にマップするテーブルをリフレッシュする必要があります。 DNS サーバがテーブルをリフレッシュするまで待機し、再度ディスカバリを実行してください。

OpenSSL ソフトウェア互換性の問題

症状:

OpenSSL を使用するソフトウェアを CA Server Automation と同じシステムにインストールすると、互換性の問題が発生します（特にソフトウェアが System32 ディレクトリにライブラリ ファイルをインストールする場合）。

解決方法:

非互換性の OpenSSL バージョンを削除します。

注: OpenSSL バージョンを削除する前に、他のアプリケーションがそれらを使用していないことを確認してください。

パスワードを変更すると認証エラーが発生する場合がある

Active Directory、CA EEM、Microsoft SQL 、およびシステム ユーザのパスワードを変更すると、CA Server Automation に問題が発生する場合があります。

Active Directory パスワードの有効期限により、ログインの問題が発生する

症状:

CA Server Automation ユーザ インターフェースを表示できません。

解決方法:

CA Server Automation をインストールする際に Active Directory に接続するよう設定すると、CA Server Automation をインストールしたユーザは自動的に CA EEM に登録されます。 このユーザ登録によって、CA Server Automation は Active Directory ドメインからユーザを認証できます。 このユーザのパスワードを変更すると、CA EEM はユーザを認証できなくなるため、ユーザは CA Server Automation ユーザ インターフェースにログインできなくなります。

この問題を解決するには、本製品をインストールしたユーザのパスワードを変更します。

ユーザ パスワードを変更する方法

1. ［スタート］-［プログラム］-［CA］-［Embedded Entitlements Manager］-［EEM ユーザ インターフェース］をクリックし、CA EEM ユーザ インターフェースにログインします。
2. ［アプリケーション］ドロップダウン リストから［管理者］を選択し、［ユーザ名］を「EiamAdmin」のままにして、パスワードを入力し、［ログイン］をクリックします。
3. ［設定］をクリックし、［EEM サーバ］をクリックします。
4. 左ペインで［グローバル ユーザ/グローバル グループ］をクリックし、［外部ディレクトリから参照］オプションを選択したままにします。

5. ［タイプ］を「Microsoft Active Directory」のままにし、［パスワード］フィールドと［パスワードの確認］フィールドに新しいパスワードを入力し、［保存］をクリックします。
6. ［スタート］-［すべてのプログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］をクリックします。 CA Server Automation コマンド プロンプトから以下のコマンドを実行します。

   ```
   dpmutil -set -sysuser
   ```

   CA EEM ユーザ名およびパスワードの入力を求められます。

注: *Install_path*¥Apache¥logs¥error.log にある Apache HTTP Server ログ ファイルで、適切な製品スタートアップを確認できます。 最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。 dpmutil コマンドと共に使用される認証情報が CA EEM ユーザ インターフェースへのログインに使用できることを確認します。 有効な認証情報を使用して、dpmutil コマンドを再試行します。

CA EEM パスワードを変更すると認証失敗が発生する

症状：

CA EEM パスワードを変更した後 CA Server Automation を開始すると、サービスが実行されません。

解決方法：

CA EEM 管理者パスワード（EiamAdmin）を変更すると、CA Server Automation は正常に開始しません。 すべてのサービスがダウンしているように見えます。 本製品には CA EEM 認証情報が保存されているため、以下のいずれかの手順を実行して、CA Server Automation 内の認証情報を変更します。

CA Server Automation がネイティブ セキュリティを使用している場合

1. dpmutil -set -eiam を実行し、新しい認証情報を指定します。
2. CA EEM でシステム（sys_service）認証情報を確認します。 変更されていれば、dpmutil -set -sysuser を実行します。
3. CAAIPApache および CAIPTomcat サービスをリサイクルします。

CA Server Automation が Active Directory を使用している場合

1. 手順 1 と同じ認証情報か CA EEM 管理者権限を持つ別の AD ユーザのいずれかで dpmutil -set -sysuser を実行します。
2. CAAIPApache および CAIPTomcat サービスをリサイクルします。

注: *Install_path*¥Apache¥logs¥error.log にある Apache HTTP Server ログ ファイルで、適切な製品スタートアップを確認できます。 最後のエントリが「Validating EEM is available」である場合は、認証情報にまだ問題があります。 dpmutil コマンドと共に使用される認証情報が CA EEM ユーザ インターフェースへのログインに使用できることを確認します。 有効な認証情報を使用して、dpmutil コマンドを再試行します。

SQL ユーザ パスワードを変更すると UI が空白になる

症状：

Microsoft SQL ユーザ パスワードを変更した後、CA Server Automation ユーザ インターフェースを表示できません。

解決方法：

Microsoft SQL 認証を使用していて、Microsoft SQL ユーザのパスワード（通常 *sa* パスワード）を変更すると、CA Server Automation UI が空白になるか、Microsoft SQL エラー メッセージが表示されます。 本製品には Microsoft SQL ユーザ認証情報が保存されているため、以下の手順を実行して、認証情報を変更します。

SQL ユーザ認証情報を変更する方法

1. ［スタート］-［すべてのプログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］をクリックします。 CA Server Automation コマンド プロンプトから以下のコマンドを実行します。

   ```
   dpmutil -set –mgmtdb
   ```

   本製品の主要なテーブルにアクセスするために使用するデータベース サーバ、バージョン、ポート、および認証情報の入力を求められます。

2. パフォーマンス データベースが管理データベースと同じデータベース サーバおよび SQL ユーザを使用する場合は、以下のコマンドを実行します。

   ```
   dpmutil -set -perfdb
   ```

   サーバ名、管理者ユーザ名とパスワード、データベース タイプ、データベース インスタンス、およびデータベース ポートの入力を求められます。

3. CAAIPApache および CAIPTomcat サービスをリサイクルします。

システム ユーザ パスワードを変更すると UI が空白になる

症状：

システム ユーザ パスワードを変更した後、CA Server Automation ユーザ インターフェースを表示できません。

解決方法：

ユーザ sys_service は、ネイティブ セキュリティのインストール時に作成されます。このユーザのパスワードを変更すると、CA Server Automation では UI が空白で表示さ、すべてのサービスは実行されません。 本製品には sys_service 認証情報が保存されているため、以下の手順を実行して、認証情報を変更する必要があります。

システム ユーザ認証情報を変更する方法

1. ［スタート］-［すべてのプログラム］-［CA］-［CA Server Automation］-［CA Server Automation コマンド プロンプト］をクリックします。 CA Server Automation コマンド プロンプトから以下のコマンドを実行します。

   ```
   dpmutil -set -sysuser
   ```

   ユーザ名とパスワードの入力を求められます。

2. CAAIPApache および CAIPTomcat サービスをリサイクルします。

Rapid Server Imaging（RSI）トラブルシューティング

このセクションには、Rapid Server Imaging のトラブルシューティング トピックが含まれます。

RSI サーバ エラー

症状:

仮想ハードウェアにプロビジョニングする場合、RSI サーバは以下のエラーをレポートします。

```
Failure - Could not communicate with server at xxx.xxx.xxx.193/8011: [Errno 104]
Connection reset by peer

Event watcher timer (45 seconds) expired waiting for ['FTShutdownHeartbeat']
```

解決方法:

これらはハイパーバイザ パフォーマンスの問題です。 パフォーマンスを最大化するためにハイパーバイザ設定を確認します。 その後、VM のプロビジョニングを再試行します。

RSI サーバと ITCM サーバ

症状:

CA Software Delivery サーバと Rapid Server Imaging（RSI）サーバの両方がインストールされている場合、プロビジョニング タスク（オフライン キャプチャ、ドライバ セットのキャプチャ、展開など）が以下のエラーで失敗することがあります。

ブート構成エラーがないかサーバを確認します。 （ネットワーク ブートは有効になっていますか。）

これは、RSI サーバが PXE ブート要求に応答する必要がある場合に、CA-Unicenter ManagedPC ブート サーバが代わりに応答する場合に発生します。

解決方法:

PXE ブート要求を無視するように CA-Unicenter ManagedPC ブート サーバを設定するには、以下の手順に従います。

1. CA ITCM ユーザ インターフェースにログインします。
2. エクスプローラから、［コントロール パネル］-［設定］-［設定ポリシー］に移動します。
3. ［デフォルト コンピュータ ポリシー］を右クリックし、［封印解除］を選択します。
4. ［DSM エクスプローラ］-［スケーラビリティ サーバ］-［OSIM］-［ManagedPC］-［サーバ］に移動します。
5. 右側のパネルで、［ユーザ応答制御リスト］を選択し、その値を 2 に変更します。
6. ［デフォルト コンピュータ ポリシー］に再度移動し、［封印］を選択します。

エラーのキャプチャまたは展開

症状:

新しく登録されたネットワークを使用すると、オフライン キャプチャまた展開中にエラーが表示されます。

ネットワークに到達できません

解決方法:

RSI サーバで、デポを登録して新しく登録されたネットワーク（ブートまたは外部）に関連付けます。 「*RSI サーバ管理ガイド*」を参照してください。

RSI: イメージはタイムアウトのため展開されません

症状:

タイムアウトが RSI イメージの展開中に発生し、展開は失敗します。

解決方法:

イメージを再度展開させます。

Linux イメージをプロビジョニングする場合の無効な X の設定

症状:

あるサーバから別のサーバに Linux イメージを移動させると、X の設定は無効にされ、再設定が必要です。イメージを展開した後、および Linux サーバを再起動している間に、X の設定が正しくないとのメッセージが表示され、再試行するように要求されます。 SUSE Linux Enterprise Server Linux の配布については、X の再設定が完了するまで、ブート プロセスは遅延になります。 イメージをキャプチャまたは展開するときに、この遅延はタイムアウト エラーとなります。

解決方法:

この問題を解決するには、プロンプトで［はい］と応答して X の設定を再設定します。

サイズ変更オプションを使用すると、Linux と UNIX のプロビジョニングに失敗する

症状:

dpmrsi deploy image コマンドの *-scale* オプションでは、ターゲット サーバのディスクに合わせてソース イメージのファイル システム サイズを拡大または縮小させます。RSI サーバは、ソース ディスクの各ファイル システム内の使用済みスペースを使用することによって、ファイル システムのターゲット サイズを計算し、新規ファイル システムのサイズを均等に設定します。 この方法では、ファイル システムによっては新しいディスクに作成されたスペースが不十分である場合があります。 UNIX および Linux システムでは、この方法によって小さな /tmp ファイル システムが作成されます。 /tmp が小さすぎる場合、プロビジョニングは失敗します。

解決方法:

この問題を解決するには、*-scale* オプションを使用せずにプロビジョニング操作を再起動し、プロビジョニングが完了した後で、手動でファイル システムのサイズを変更します。 ［UI Actions］ドロップダウン メニューからイメージを展開させるときにスケール イメージ オプションをオフにすることができます。

OS タイプ、デポ、またはネットワークを一覧表示しても結果が返されない

症状:

RSI のインストールの後、OS タイプ、デポ、またはネットワークを一覧表示しても、結果が返されません。

解決方法:

RSI サーバ上で portmap および nfs サービスが実行されていることを確認します。 実行されていない場合は、これらのサービスを起動し、各サービスがシステムのブート時に自動的に起動するように設定されていることを確認します。 RSI をアンインストールし、再度インストールを実行します。

登録済みサーバが失敗する

症状:

サーバが Racemi® DynaCenter® にすでに登録されている場合、ハイパーバイザの登録が以下のエラーで失敗します。

CAAM2228 RSI タスク RegisterHypervisor-73bef2acde は失敗しました。エラー スロット *server_id* は使用中です *RSI_server_name*

解決方法:

この問題を解決するには、使用中の server_id を登録解除し、次に、ハイパーバイザを登録します。

RSI: リモート サーバのディスカバリに失敗する

症状:

時々、Rapid Server Deployment 要求が成功した後で、ターゲット サーバの自動ディスカバリが失敗します。 以下のイベントがイメージング サマリ タブに表示されます。

CAAM0515 ディスカバリ操作のステータスが更新されました： ターゲット マシン= 、ステータス=処理中、試行 nn

解決方法:

ターゲット サーバで実行している RSI エージェントは、ディスカバリのための IP アドレスの通信に失敗しました。 この問題を解決するには、ターゲット サーバで RSI エージェントをリサイクルし、手動でターゲット サーバ用のコマンドを検出します。

イメージのキャプチャまたは展開時の RSI エージェント エラー

症状:

イメージ キャプチャまたは展開の要求をサブミットするとき、以下のエラーが CA Server Automation UI で発生します。

エラー： イメージの展開に失敗しました： RSI エージェントに接続するときにエラーが発生しました。エージェントが動作していることを確認してください。

解決方法:

この問題を解決するには、ターゲット サーバで RSI エージェントを再起動します。

Solaris SPARC プロビジョニングは DVD の検出で失敗する

症状:

Solaris SPARC エージェント イメージは、誤って DVD をストレージとして検出します。 DVD ドライブに DVD が挿入されていると、プロビジョニング操作に失敗します。

解決方法:

ドライブから DVD を取り出し、プロビジョニング操作を再起動します。

SSL エラーで RSI イメージングに失敗する

症状:

RSI イメージング タスク（キャプチャ、展開、ドライバ コレクション、およびドライバ セットのキャプチャ）は、SSL エラーで失敗します。

解決方法:

このエラーにはいくつかの考えられる原因がありますが、問題を修正するために以下のアクションを試行します。

1. CA Server Automation プログラム ファイルに移動します。

   C:¥Program Files¥CA¥*productname*¥conf

2. caimgconf.cfg ファイルを開きます
3. 再試行回数パラメータの値を 3 から 6 に増やします。

   CONFIG_KEY_IMG_SSL_SOAP_ERROR_MAX_RETRY_COUNT

4. Apache サービスを再起動します。

ターゲット サーバはイメージ キャプチャまたは展開の後の再起動中に応答を停止する

症状:

エージェント イメージを実行するターゲット サーバはイメージ キャプチャまたは展開の後で、再起動中に応答を停止します。

解決方法:

RSI サーバは、タイミングの問題により、サーバがシャットダウンを完了する前に、割り当てられたエージェント イメージをリリースします。 この問題を回避するには、イメージ キャプチャおよび展開を開始する前に各ターゲット サーバの OS タイプに個別のエージェント イメージを割り当てます。

1. 以下のコマンドを実行して、すべてのサポートされている OS タイプのエージェント イメージを作成します。

   ```
   # . /opt/race/share/conf/buildout.conf;
   /opt/race/share/conf/provisionmgr.sh
   ```

   サンプル出力：

   ```
   Sourcing confData

   Server class ProvisionMgr-Linux2.6 exists

   Server class ProvisionMgr-CentOS4-x86_64 exists

   Server class ProvisionMgr-CentOS5-i686 exists

   Server class ProvisionMgr-CentOS5-x86_64 exists

   Server class ProvisionMgr-Solaris10-sun4u exists

   Server class ProvisionMgr-Solaris9-sun4u exists

   Server class ProvisionMgr-Solaris8-sun4u exists

   Server class ProvisionMgr-Solaris10-i86pc exists
   ```

2. RSI サーバで以下のコマンドを実行して各ターゲット サーバにエージェント イメージを割り当てます。

   ```
   # dccmd assign agent <server_id> <ostype>
   ```

IBM サーバでの Windows ドライバ コレクション問題

症状:

IBM Server Guide から収集したドライバを使用して、IBM サーバへの Windows イメージをプロビジョニングする場合、Windows デバイス マネージャのいくつかのクリティカルでないデバイスに感嘆符または疑問符が表示されます。 Windows デバイス マネージャにアクセスするには、［スタート］-［すべてのプログラム］-［管理ツール］-［コンピュータの管理］-［デバイス マネージャ］をクリックします。 また、Windows ドライバ コレクションでは、期待する結果が得られません。

解決方法:

この問題を解決するには、サーバから IBM ドライバを直接収集します。

Windows プロビジョニングが失敗する

症状:

ターゲット サーバに十分な量のディスク領域があっても、Windows プロビジョニングが失敗します。 以下のエラーが表示されます。

```
Could not populate from ntfsclone image _.ntfsclone.gz
```

解決方法:

展開操作を行う場合、ターゲット サーバのディスク領域に、ソース サーバのディスク領域と同等以上の容量が必要です。 この問題を解決するには、［アクション］ドロップダウン メニューから UI にイメージを展開する際に、スケール イメージ オプションを有効にします。 また、*-scale* オプションを指定して *dpmrsi deploy image* コマンドを使用し、プロビジョニング操作を再度実行することもできます。**注**: dpmrsi コマンドの詳細については、「リファレンス ガイド」の「Rapid Server Imaging のコマンド」セクションを参照してください。

Rapid Server Imaging を使用したインストールがエラーになる

症状:

既存の RSI サーバをアップグレードすると、問題が表示されずに失敗します。

解決方法:

Rapid Server Imaging（RSI）コンポーネントのインストール中にインストールが失敗する場合は、以下の手順に従います。

1. 有効な Racemi DynaCenter ライセンスがあることを確認します。

   ライセンスを確認するには、RSI サーバ上で「rshowlicense」を実行します。

2. RSI サーバ上で Apache HTTP サーバ サービスが実行されていることを確認します。

予約マネージャトラブルシューティング

このセクションには、予約マネージャ のトラブルシューティング トピックが含まれます。

関連項目:

Amazon マシン イメージが選択対象として利用できない (P. 1268)
チャージバック計算が予約金額よりも少ないまたは多い (P. 1268)
インストール ターゲットを解決できない (P. 1269)
VM を要求するときに利用可能なリソースがありませんというメッセージが表示される (P. 1270)
パスワードの変更によって表示されるエラー メッセージ (P. 1270)
VMware データストアでの層ラベルの変更 (P. 1271)
パーソナリティの自動展開用のパッケージ エントリを検索できません (P. 1271)
vCenter からの情報を取得できない (P. 1272)
VM リソースが要求された日付では利用できない (P. 1273)
CPU の制限による VM 予約の失敗 (P. 1274)
クラスタ化された環境での VM 予約の失敗 (P. 1274)

Amazon マシン イメージが選択対象として利用できない

症状:

管理者が［AMI イメージの追加］ウィザードを開始する場合、選択対象として利用可能な AMI インスタンスがありません。 EC2 サーバへの接続ステータスは正常です。

解決方法:

デフォルトでは、EC2 サーバ接続情報で指定された所有者によって所有される AMI のみが、インベントリに追加できます。 デフォルトを変更すると、Amazon または他のユーザによって発行されたパブリック AMI が使用できるようになります。 パブリック AMI がインベントリに追加されるようにするには、dpmutil を実行して Amazon EC2 を再設定します。

チャージバック計算が予約金額よりも少ないまたは多い

症状:

ユーザが既存の予約にリソースを追加する場合は、全期間に相当する 24 時間に対してリソースの全額が請求されます。 ユーザが既存の予約にリソースを追加し、それらのリソースをその日の終わりまでに返した場合、追加料金はかかりません。

解決方法:

デフォルトでは、チャージバック コストは、毎日 1 回真夜中に計算されます。1 日未満の使用に対して請求するには、［チャージバック計算の頻度］設定の値を増やします。 詳細については、「チャージバックの設定 (P. 1162)」を参照してください。

インストール ターゲットを解決できない

症状:

ソフトウェア インストール タスクが失敗し、［予約イベント］テーブル内のイベントは、「SD エージェント インストール ジョブ」が失敗したことを示します。 リスト表示される理由は「ターゲットを解決できません」です。

このメッセージは、CA Software Delivery アプリケーションが、付与された名前を使用して、ターゲット システムにアクセスできなかったことを示します。この問題は、DNS が新しくプロビジョニングされた仮想マシンの名前で更新されていない場合に発生する場合があります。

解決方法:

この問題が DNS の更新の遅延により発生した場合は、ソフトウェア インストール タスクを［予約タスク］ページから再起動します。

タスクが再度失敗する場合は、CA ITCM サーバにログインし、名前を使用してターゲット システムに ping を実行します。 到達できない場合は、Software Delivery サーバ DNS がターゲット VM の名前で更新されない理由を調査します。

VM を要求するときに利用可能なリソースがありませんというメッセージが表示される

症状:

仮想マシン テンプレートを選択した後、「組織単位 org_unit は、選択した仮想テンプレートのプロビジョニングに使用するリソース プールにアクセスできる権限が付与されていません。」という警告メッセージがユーザに表示されます。ユーザは予約ウィザードの次の手順に進むことができません。このメッセージは一般的に、エンド ユーザに仮想マシン テンプレートへのアクセス権はあるけれども、ESX サーバに仮想マシンを作成する権限またはテンプレートと同じデータ センターでクラスタ化する権限が付与されていないときに表示されます。

解決方法:

この問題を解決するには、以下の手順に従います。

1. 選択された仮想テンプレートが存在するデータ センターを識別します。 このデータ センターは［システム イメージ］テーブルの［場所］列に表示されます。
2. このユーザが属する組織単位を識別します。
3. 選択された仮想マシン テンプレートと同じデータ センターに定義されている仮想リソース プールを識別します。ユーザが属する組織単位へのアクセス権を提供します。
4. あるいは、同じデータ センターにある 1 つ以上の ESX サーバまたはクラスタが含まれた新しい仮想リソース プールを作成します。組織単位へのアクセス権を提供します。

パスワードの変更によって表示されるエラー メッセージ

症状:

パスワードを変更した後で、CA Server Automation に以下のメッセージが表示されます。

セキュリティ トークンは認証されなかったか許可されませんでした。

症状:

パスワードを変更する前に CA Server Automation にログインした場合は、このメッセージが表示される場合があります。 ログアウトしてから再度ログインします。

VMware データストアでの層ラベルの変更

症状:

データストアに層ラベルを割り当てると、層ラベルは同じ名前の他のデータストアに変更されます。

解決方法:

予約マネージャ で VMware データストアを設定する際、各データストアに層ラベルを割り当てることができます。 同じ名前の異なるデータストアがある場合、層ラベルがすべてに適用され変更することはできません。唯一の回避策はデータストアの名前を一意の名前に変更することです。

パーソナリティの自動展開用のパッケージ エントリを検索できません

症状:

ソフトウェア インストール タスクは、「パーソナリティの自動展開用のパッケージ エントリを検索できません」というエラーで失敗します。

このメッセージは、プロビジョニングされているシステムに自動的に展開されるソフトウェアの定義に問題があることを示します。 自動的に展開されるソフトウェアのリストは、パッケージング コンポーネントがインストールされたサーバにある casdaconf.cfg (P. 1031) ファイルに定義されています。

解決方法:

各オペレーティング環境に対して少なくとも 1 つのソフトウェア パッケージがインストールされるように設定されていて、そのオペレーティング環境用の AUTODEPLOY 定義が連続的に番号付けされていることを確認します。

関連項目:

Software Delivery 設定ファイル (P. 1031)

vCenter からの情報を取得できない

症状:

「選択できるリソースは現在ありません」という警告メッセージがエンドユーザに表示されます。 メッセージには「*template_name* 用の Virtual Center から情報を取得できません」という情報も含まれます。

このメッセージは、選択された仮想マシン テンプレートへのアクセス権がユーザに付与されているのに、VMware vCenter 内のテンプレートが利用可能でない場合に表示されます。 テンプレートが削除されているかまたは 予約マネージャ インベントリに追加したときから孤立している場合に、この状況が発生する場合があります。

解決方法:

この問題を解決するには、以下の手順のいずれか *1* つに従います。

1. テンプレートが VMware vCenter Server から削除されている場合は、このテンプレートに関連付けられた 予約マネージャ インベントリ アイテムへのすべてのアクセス権を削除します。
2. テンプレートが孤立している場合は、VMware Infrastructure Client を使用してこの問題を修正します。
3. テンプレートの名前が変更された場合は、元の名前に変更するか、または 予約マネージャ インベントリ アイテムへのアクセス権をすべて削除します。

これらの手順のいずれでも問題が解決しない場合は、vCenter Server への CA Server Automation 接続がダウンしているかどうか確認します。 CA Server Automation ユーザ インターフェースにログイン (P. 31)し、［管理］ページの［設定］タブに表示される vCenter Server 接続ステータスを確認します。

VM リソースが要求された日付では利用できない

症状:

「要求を処理できません： 仮想マシン リソースは要求された日付に利用できません」という警告メッセージがエンド ユーザに表示されます。 エンド ユーザは予約ウィザードの次の手順に進むことができません。

このメッセージは以下の理由で表示される場合があります。

- ユーザは指定された期間内に予約できる仮想マシンの最大数をすでに要求している。
- 予約マネージャ は、このユーザに利用可能な ESX サーバまたはクラスタのいずれにも予約期間の要求に対応できる空き容量がないと判断した。

解決方法:

次のいずれかの解決策を使用します。

1. ユーザは、リソースが利用可能な時間に予約期間を変更できます。
2. 予約できる VM 数が制限されたことによってユーザが新しい仮想マシンを予約できない場合は、ユーザにアクセス権がある 1 つ以上の仮想リソース プールに定義されている［最大システム数］の設定を変更することにより、制限を増やします。
3. ESX サーバの容量制限が低すぎるためにユーザが新しい VM を予約できない場合は、関連付けられたリソース プールを変更します。［プロパティ］タブで［メモリの超過割り当てを許可する］を選択し、割合を入力します。 詳細については、「ESX サーバまたはクラスタにおけるメモリのオーバーコミットメントの設定 (P. 1182)」を参照してください。

CPU の制限による VM 予約の失敗

症状:

VMware が選択された ESX サーバに許可している仮想 CPU よりも多い仮想 CPU が要求された場合に、予約は失敗します。 以下のようなメッセージが表示されます。

仮想マシンでは、*X* CPU が機能している必要がありますが、ホスト ハードウェアは *X* のみを提供します。

この仮想マシンにはサポートされていない仮想 CPU の数が設定されています。

解決方法:

設定を変更することにより、環境内の ESX サーバ用の仮想 CPU の数を減らすことができます。 トピック「仮想マシン リソースでの制限の設定 (P. 1181)」の［*仮想 CPU の制限*］フィールドを参照してください。

クラスタ化された環境での VM 予約の失敗

症状:

クラスタ化された環境での予約に失敗します。 以下のようなメッセージが表示されます。

理由： データストアが仮想リソース プール*名*に正しく設定されません。
解決策： ESX サーバ *Server_name* への展開に使用できるデータストアが指定されていることを確認してください。

詳細： 例外： 使用できるデータストアがないため、仮想マシンを *Server_name* に展開する試行は実行できません。
仮想リソース プール*名*を編集し、*Server_name* に仮想マシンを展開するときに使用できるデータストアを指定してください。

解決方法:

次のいずれかの解決策を使用します。

- 新しい仮想マシンを作成する場合、各 ESX サーバは使用できるデータストアを定義する必要があります。 リスト表示された ESX サーバをデータストアに関連付けるためにリソース プールを更新します。
- VMware vCenter クラスタ名にスラッシュ（/）文字が含まれていないことを確認します。

スケジュールされたジョブが実行されない

症状:

スケジュールされたジョブが実行されません。 スケジュールされたジョブが実行される場合、ジョブが確実に実行されるようにするには、サービス コントローラおよび開始コンポーネントがアクティブで、ジョブを実行しているサーバからアクセス可能である必要があります。 この問題には以下のような症状が含まれます。

- ダッシュボード メッセージが表示されません。
- スケジュールされたジョブ リストでは、ジョブステータスを［利用不可］として表示します。
- ジョブが実行されません。

解決方法:

ジョブを実行しているコマンド ライン プログラムのログ ファイルを確認して、以下のエントリを検索します：「ジョブ ID を取得できませんでした」。ログ ファイルの例として dpmpolicycli.log、dpmccmcli.log などがあります。

注: ログ ファイルの詳細については、「リファレンス ガイド」を参照してください。

CA SDM 例外エラー

症状:

CA SDM がダウンしている場合、管理の接続ステータスの［設定］ページに CA SDM に接続できないことを示す以下のメッセージが表示されます。

「ServiceDeskClientAdapter validateSDUser() exception: ; nested exception is: java.net.ConnectException: Connection refused: connect」。

解決方法:

この問題を解決するには、CA SDM を再起動します。

Software Delivery アダプタのエラー

症状:

ユーザ インターフェースでリソースを追加すると、以下のエラーが表示されます。
`Software Delivery アダプタ サービスは ITCM サーバ名用に登録されていません`

解決方法:

CA Software Delivery と SQL サーバが（マネージャ システム上ではなく）リモートにインストールされている場合は、Apache サービスの認証情報を管理者に設定します。この問題を解決するには、以下の手順に従います。

1. Apache サービスの認証情報を管理者に変更します。
2. Apache サービスを再起動します。

症状:

Software Delivery サーバをプロビジョニングすると、以下のエラーが表示されます。
`コンピュータ <name> の追加に失敗しました。 エラー: SDAdapter_addComputer (失敗)。 DSM へのコンピュータの追加に失敗しました。`

解決方法:

最も一般的な原因は、各 CA ITCM インスタンスを 1 つの CA Server Automation インスタンスによる管理用に設定していないことです。 別の原因として、CA ITCM でサポートされている接続の最大数を超えていることが考えられます。 この問題を解決するには、以下の手順に従います。

1. ［管理］タブの Software Delivery サーバに移動します。
2. ほかの CA Server Automation インスタンスのすべてのエントリを削除します。
3. IIS と CA ITCM をリセットします。
4. CA ITCM サーバ上の caf サービスを再起動します。
5. Apache サービスを再起動します。
6. サーバを再プロビジョニングします。

   問題が解決されない場合は、テクニカル サポートにお問い合わせください。

SSP - ホームの内容が Internet Explorer 9 に表示されない

症状：

セルフ サービス ポータルのホームの内容が Internet Explorer 9 に表示されません。

解決方法：

Internet Explorer セキュリティ強化の構成を無効にします。 サーバ マネージャを開き、［セキュリティ情報］ペインの［IE ESC の構成］をクリックします。

vCenter Server フォルダが UI に表示されない

症状:

製品をインストールした後で、ユーザ インターフェースに vCenter Server フォルダが表示されません。

解決方法:

- マネージャ システムで Apache のサービスが実行されているかどうか確認します。 停止している場合は、Apache のサービスを開始します。
- SystemEDGE vCenter AIM システムで SystemEDGE サービスが実行されているかどうか確認します。 停止している場合は、サービスを開始します。
- vCenter AIM が正しく設定されることを確認します。設定は、ユーザ インターフェースの［管理］タブ、または vCenter AIM システムの NodeCfgUtil から確認できます。
- CA Server Automation マネージャから vCenter AIM を実行しているサーバを検出します。

ユーザ インターフェースからサーバを検出する方法

1. ［リソース］タブを選択し、次に、［管理］タブを選択します。［ディスカバリ］サブタブが選択され、［ディスカバリ タイプ］はデフォルトでは［システム］に設定されます。
2. ［システム名］フィールドに AIM システム名の完全修飾ドメイン名または IP アドレス用を入力します。
3. ［OK］をクリックします。

   しばらくすると、指定されたシステムに関係のあるイベントが［ダッシュボード］タブの［イベント］ウィンドウに表示されます。

VM 予約エラー: Software Delivery のコンピュータ UID が見つからない

症状:

VM をプロビジョニングした後で Software Delivery エージェントを展開すると、エージェントは一意のコンピュータ UID を使用して Software Delivery サーバに再度登録しません。コンピュータ UID はコンピュータ システムを識別するために必要です。 以下のようなイベント メッセージが UI ダッシュボードに表示されます。

予約タスクは失敗しました。 予約 ID： n、システム名： host_name タスク： 2 ソフトウェア インストール、理由： "システムの準備ジョブのステータスが更新されました： ターゲット コンピュータ = host_name、説明 = DCRM 要求、以前のジョブステータス = スケジュール済み、現在のジョブステータス = 失敗、host_name で展開された SD エージェントのコンピュータ UID が見つかりません"。

解決方法:

この失敗には 2 つの考えられる原因があります。

1. Software Delivery エージェントの展開が通常より長くかかった場合。この問題を解決するには、タスクに失敗するまでに、Software Delivery サービスが待機する時間の長さを増やします。操作に失敗するまでにコンピュータ UID 検索を試行する回数を増やすことによって、時間の長さを増やします。

   a. Software Delivery サービスがインストールされている CA ITCM ドメイン マネージャ上にある casdaconf.cfg ファイルを開きます。

   b. 以下の設定ファイルの設定を参照し、値を増やして、ファイルを保存します。

      ```
      SD_DSM_Find_Computer_Retry_Count =3
      ```

   c. Software Delivery サービスがインストールされているシステムで Apache を再起動して変更を有効にし、次に、予約操作を再試行します。

2. Common Application Framework （CAF）における問題。 この問題を解決するには、以下の手順を使用して、CAF を再起動します。

   a. コマンド プロンプトを開いて「caf stop」を入力します。

   b. CAF サービスが停止した後で、「caf start」を入力します。

   c. CAF サービスが再起動されたら、予約操作を再試行します。

VM が検出されない

症状:

VMware vCenter VM が検出されません。

解決方法:

VMware ツールが VMware 環境の VM にインストールされることを確認します。

用語集

AIM

「Application Insight Module」を参照してください。

AIP

「オートメーション統合プラットフォーム」を参照してください。

Amazon Elastic Compute Cloud （EC2）

*Amazon Elastic Compute Cloud （EC2）*では、Amazon.com から開発者にデータ センター サービスが提供されます。 詳細については、http://docs.amazonwebservices.com にアクセスしてください。

AOM

「オートメーション オブジェクト モデル（AOM）」を参照してください。

Application Insight Module、AIM

SystemEDGE エージェントには、初期化時にオプションの *Application Insight Module （AIM）*をロードできるプラグイン アーキテクチャが備わっています。AIM は SystemEDGE エージェントの機能拡張です。たとえば、vCenter AIM により、SystemEDGE は VMware vCenter Server を介して vSphere 環境を管理できます。

AutoShell

AutoShell を使用すると、複雑な反復タスクや管理タスクを自動化できる、コマンド ラインとスクリプトの環境が得られます。 AutoShell は、プログラミング言語ではなく、スクリプト言語とコマンド ライン シェルを組み合わせたものです。

AutoShell は、標準化されたスクリプト言語 ECMA-Script（JavaScript）をベースにしています。 JavaScript は一般に Web ページで使用されるスクリプト言語として知られていますが、必ずしもブラウザで実行される必要はありません。 このスタンドアロンのスクリプト言語を使用して、オブジェクト指向、XML、および正規表現処理に対するサポートを実装できます。

AutoShell では、Mozilla Spidermonkey JavaScript インタープリタの事前定義済みバージョンを使用します。 これにより、Mozilla Firefox Web ブラウザにも JavaScript 機能が提供されます。

Autoshell Loadable Module、ALM

*Autoshell Loadable Module（ALM）*は AutoShell コアの拡張です。インストール時に選択された CA Server Automation のコンポーネントに応じて、必要な ALM が自動的にインストールされます。たとえば、ALM により、LPAR、Solaris ゾーン、vCenter Server などのプラットフォームを AutoShell を通じて管理できます。

CIM

「Common Information Model （CIM）」を参照してください。

Cisco Nexus 1000V スイッチ

*Cisco Nexus 1000V スイッチ*は、VMware vSphere 環境で実行できる分散仮想スイッチです。Cisco Nexus 1000V スイッチは、仮想イーサネット モジュール（VEM）および仮想スーパーバイザ モジュール（VSM）から構成されます。 VEM は、Cisco Nexus 1000V スイッチに関連付けられた各 ESX ホストまたは ESXi ホスト上で、VMware vSwitch に置き換わるもので、ハイパーバイザ カーネル内のモジュールとして実行されます。 VSM は、複数の VEM を 1 つの論理スイッチとして制御し、ESX ホストまたは ESXi ホスト上の VM 内で実行されます。 詳細については、http://www.cisco.com/go/1000vdocs で Cisco Nexus 1000V スイッチのドキュメントを参照してください。
CA Server Automation VM プロビジョニングでは、VMware vNetwork Distributed Switch および Cisco Nexus 1000V スイッチをサポートしています。

Cisco Unified Computing System （UCS）

*Cisco Unified Computing System （UCS）*は、データ センター ハードウェアと仮想化サービスを提供します。

cmdlet

cmdlet はコマンドの一種ですが、行の先頭が余白以外の文字で始まる必要があります。 この制限のため、スタンドアロンでしか使用できず、より幅広く使用される JavaScript 式には含めることができません。特に、rvalue（代入演算子の右端のオペランド）として使用することはできません。
? は、AutoShell cmdlet の一例です。

Common Information Model （CIM）

*Common Information Model （CIM）*は、システム、ネットワーク、デバイスなどに関する情報を格納するデータベースのスキーマを提供します。CIM の実装により、さまざまな管理アプリケーションがさまざまなソースからデータを収集できます。

CPU 共有（VMware）

共有は自然数として指定され、各仮想マシン間の相対値を示します。

共有の指定は、階層で同じ親を持つ仮想マシン、vApp、またはリソースプールに関してのみ意味をなします。 仮想マシンに共有を割り当てるときには、オンになっている他の仮想マシンに相対する、その仮想マシンの優先度を常に指定します。

たとえば、競合が発生すると、2000 の共有を持つ仮想マシンには、1000 の共有を持つ仮想マシンよりも多くの CPU 時間が割り当てられます。 共有は他の共有に相対して設定されます。このため、共有の値ではなく相対的な大きさが意味を持ちます。 1000、2000、3000 の共有の値を持つ 3 台の仮想マシンは、1、2、3 の共有の値を持つ 3 台の仮想マシンと同じように動作します。 任意の数スキーム（1、2、3 や 1000、2000、3000 など）を使用できます。

dvPort グループ（VMware）

各 VMware vNetwork Distributed Switch には、1 つ以上の *dvPort グループ*が割り当てられています。dvPort グループは、共通の設定で複数のポートをグループ化し、ラベル付きネットワークに接続する VM に安定したポイントを提供します。 一意のネットワーク ラベルによって、各 dvPort グループが識別されます。 ネットワーク ラベルは現在のデータセンターで一意です。
dvPort グループによって、vNetwork Distributed Switch の各メンバ ポート用にポート設定オプションが指定されます。また、dvPort グループによって、ネットワークへの接続方法が定義されます。

dvUplink ポート（VMware）

*分散仮想アップリンク（dvUplinks）*は、ESX ホストの物理 NIC （vmnics）の抽象化レベルを提供します。各物理 NIC は 1 つの dvUplink にマップされます。 VMware vNetwork Distributed Switch に関連付けられた各ホストでは、各物理 NIC （アップリンク）が 1 つのアップリンク ポートを介して vNetwork Distributed Switch に割り当てられます。

EC2

「Amazon Elastic Compute Cloud （EC2）」を参照してください。

Elastic Service Controller （ESC）

*Elastic Service Controller （ESC）*は、仮想リソース、コンピューティング、ストレージ、および他のサービスの集中管理を提供する Huawei コントローラです。

ESX/ESXi ホスト（VMware）

*ESX または ESXi ホスト*は、ESX または ESXi サーバ仮想化ソフトウェアを使用して仮想マシンを実行する物理コンピュータです。 ホストによって、仮想マシンが使用する CPU とメモリのリソースが提供され、仮想マシンはストレージとネットワーク接続へのアクセスが可能になります。

funclet

funclet は、オプションの句、文字列化などが含まれた構文のような、冗長なコマンドを管理します。 funclet は、通常、cmdlet のように、1 行内に単独で使用されます。 funclet は、より広範囲な式の一部として処理できる値を返すことができます。

Huawei SingleCLOUD

Huawei SingleCLOUD はクラウド コンピューティング データ センター用のクラウド サービス ソリューションです。

IBM High Availability Cluster Multiprocessing （HACMP）

*IBM High Availability Cluster Multiprocessing （HACMP）*は、IBM System p プラットフォームの AIX UNIX および Linux 上に高可用性クラスタを構築するためのソリューションです。

Integrated Virtualization Manager（IVM、LPAR）

*Integrated Virtualization Manager （IVM）*は仮想 I/O サーバ（VIOS）の機能拡張で、単一の POWER システムを管理できます。 IVM では、LPAR を作成し管理できます。IVM では、VIOS 機能の管理を可能にし、Web ベースユーザ インターフェースを提供します。

internet Small Computer Systems Interface、iSCSI

iSCSI は、イントラネット上のデータ転送を円滑化し、長距離にまたがるストレージを管理するのに使用されます。 iSCSI は SCSI コマンドを IP パケット内にカプセル化します。この IP パケットが他の IP パケットと同様にネットワーク上でルーティングされます。 IP パケットがデスティネーションに到達すると、iSCSI デバイスはパケットのカプセル化を解除し、SCSI コマンドを解釈します。

MIB オブジェクト、MIB 属性

*MIB オブジェクト*は、1 つ以上のリソース オブジェクトまたはデータ項目を表す MIB に定義されたエンティティです。MIB オブジェクトにはグループ、テーブルおよび個別の属性が含まれます。また、それらは管理情報の構造（SMI）に従って定義される必要があります。

Multiple Shared-Processor Pools （MSPP）

*Multiple Shared-Processor Pools （MSPP）*は、Power6 以降のサーバでサポートされている機能です。 この機能により、複数のプロセッサ プールの作成が可能になり、CPU リソースの割り当てがより柔軟になります。

Network Installation Manager（NIM）（LPAR）

*Network Installation Manager （NIM）*は、LPAR および個々のサーバで AIX イメージをインストール、保守するための集中管理ポイントです。 NIM によって、そのようなインスタンスのインストールも容易になります。インストール元が、同じマスタ イメージ、異なるイメージ、インストール メディア、または該当インスタンスの以前の mksysb であれ、すべて同じです。 インスタンスは、それ自体が LPAR であるか、物理サーバ上にあるかに関係なく、OS イメージを参照します。

Open Virtualization Format （OVF）

Open Virtualization Format （OVF）は、多層アプリケーションのすべてのコンポーネントと、アプリケーションに関連付けられた運用ポリシーおよびサービス レベルを規定し、カプセル化するための標準です。

P12 ファイル

*P12 ファイル*は、秘密鍵をその証明書と共に格納するアーカイブ ファイルです。 P12 ファイルは、Huawei GalaX 環境で使用されます。

POWER プロセッサ（LPAR）

RISC ベースの *POWER プロセッサ*は、IBM サーバ、ミニコンピュータ、ワークステーション、およびスーパー コンピュータの多くで CPU として採用されています。

Red Hat Enterprise Virtualization

*Red Hat Enterprise Virtualization （RHEV）*は KVM ハイパーバイザに基づいたエンタープライズ仮想化製品です。

SNMPv3

SNMPv3 は以下の 3 つの通信のレベルがあるプロトコルです。
noAuthNoPriv： メッセージにユーザ名が伴うという点で SNMPv1 と SNMPv2 をミラーリングします。送信者と受信者の間に一貫性がある必要があります。
AuthNoPriv： 一貫したユーザ名およびパスワードを使用します。
AuthPriv： メッセージの本体を暗号化するユーザ名、パスワードおよび暗号化キーを使用します。

SOA

「サービス指向アーキテクチャ」を参照してください。

UCS

「Cisco Unified Computing System （UCS）」を参照してください。

UCS マネージャ

UCS ハードウェア（スイッチ、シャーシ、およびブレード）を管理するソフトウェア モジュール

vCenter Server （VMware）

VMware *vCenter Server* は、仮想 vSphere 環境の設定、プロビジョニング、および管理を集中管理する場所を提供します。vCenter Server は、Microsoft Windows サーバおよび Linux サーバ上でサービスとして実行されます。

vCenter Server エージェント（VMware）

VMware *vCenter Server* エージェントは、ESX サーバを vCenter Server と接続します。

vCenter Server データベース（VMware）

VMware *vCenter Server* データベースには、VirtualCenter によって管理される物理サーバ、リソース プール、データセンター、および仮想マシンに関する永続的な情報が格納されます。

Virtual Private Cloud （VPC）

*Virtual Private Cloud （VPC）*は、複数の仮想マシンおよび関連する仮想ディスクを備えた Huawei SingleCLOUD ユーザのためのプライベート ローカル ネットワークです。

vNetwork Distributed Switch、vDS （VMware）

VMware vNetwork Distributed Switch は、ホストからデータセンター レベルに仮想スイッチの設定を抽象化します。vNetwork Distributed Switch は、そのスイッチに関連付けられているデータセンター内のすべてのホストにおいて、単一の仮想スイッチとして動作します。 vNetwork Distributed Switch は、分散ポート グループから構成されます。これは、標準的なスイッチ上のポート グループと同様に設定されていますが、複数のホストにわたっています。 これらのプロパティは複数のホスト間でマイグレートされるため、仮想マシンで一貫したネットワーク設定を維持できます。
各 vNetwork Distributed Switch は、vNetwork Standard Switch と同様、VM が使用できるネットワーク ハブです。 vNetwork Distributed Switch は、VM 間のトラフィックを内部的に転送したり、物理 NIC（アップリンク アダプタ）に接続することで外部ネットワークにリンクしたりすることができます。
詳細については、http://pubs.vmware.com で vNetwork Distributed Switch のドキュメントを参照してください。

CA Server Automation VM プロビジョニングでは、VMware vNetwork 分散スイッチおよび Cisco Nexus 1000V スイッチがサポートされます。 vNetwork パネル、AutoShell、または CLI コマンドを介して分散仮想スイッチを管理できます。

vNetwork Standard Switch、vSwitch （VMware）

CA Server Automation では、抽象化されたネットワーク デバイスである Standard vSwitch のポリシーとプロパティを管理します。VMware vNetwork Standard Switch （vSwitch）は、単一のホスト、およびそのホスト上の仮想マシンで動作し、標準スイッチに接続させることができます。
vSwitch で、VM 間のトラフィックを内部的にルーティングして、外部ネットワークにリンクできます。 vSwitch では、複数のネットワーク アダプタの帯域幅を組み合わせて、通信トラフィックを分散します。 vSwitch は物理 NIC フェールオーバを処理することができます。

VSA-- マルチパス

マルチパスによって、ストレージ サーバへの複数のルートをセットアップできます。1 つのルートが失敗した場合、次の利用可能なルートがストレージ サーバに設定されます。

XML-RPC

異なるオペレーティング システムまたは異なる環境で実行されるソフトウェアが、インターネットを経由してプロシージャ コールを実行できます。 *XML-RPC* では、転送プロトコルとして HTTP を使用し、エンコーディングに XML を使用します。

アクセス制御リスト

アクセス制御リスト（ACL）は、IP アドレスのスペース区切りリストを指定して、コミュニティの使用をこれらのアドレスのみに制限します。 リストを空にしておくと、エージェントは、関連付けられたコミュニティ名を使用するあらゆるシステムに対してアクセス権を付与します。

オートメーション オブジェクト モデル（AOM）

*オートメーション オブジェクト モデル*は、管理対象エンティティが格納されるデータベースです。 これは、管理データを記述するためのモデルである CIM スキーマに基づいています。 「Common Information Model （CIM）」も参照してください。

オートメーション統合プラットフォーム（AIP）

*オートメーション統合プラットフォーム*は、Web サービスと ActiveMQ をベースとした管理プラットフォームです。

カーネル ベースの仮想マシン（KVM）

*カーネル ベースの仮想マシン（KVM）*は Linux カーネル用のハードウェア支援型仮想化インフラストラクチャです。

仮想 I/O サーバ、VIOS （LPAR）

*仮想 I/O サーバ（VIOS）*は、すべての物理 I/O リソースを所有するように設定された特別な論理パーティションで、その仮想化機能をほかの LPAR に提供します。LPAR は、仮想 I/O サーバを介して仮想デバイスとしてディスク、ネットワーク、および光学デバイスにアクセスします。 仮想化された入出力デバイスを備えた各 PowerVM システムには、1 つ以上の仮想 I/O サーバがあります。

仮想 LAN （VLAN）

「*仮想ローカル エリア ネットワーク*」を参照してください。

仮想 NIC （VMware）

仮想 NIC は、仮想マシンの仮想イーサネット アダプタです。 ゲスト オペレーティング システムは、仮想イーサネット アダプタが物理イーサネット アダプタであるかのように、デバイス ドライバを介して仮想イーサネット アダプタと通信します。仮想イーサネット アダプタは固有の MAC アドレスと 1 つ以上の IP アドレスを持ち、物理 NIC のように標準的なイーサネット プロトコルに応答します。

仮想スイッチ（VMware）

*仮想スイッチ*は、物理スイッチと同じように動作します。各 ESX サーバには、ポート グループを通じて仮想マシンに接続する固有の仮想スイッチがあります。 これらの仮想スイッチには、ESX サーバの物理イーサネット アダプタへのアップリンク接続もあります。 仮想マシンは、仮想スイッチ アップリンクに接続された物理イーサネット アダプタを通じて外界と通信します。

仮想ディスク（VMware）

*仮想ディスク*は、仮想ゲスト オペレーティング システム内のディスク ドライブを定義します。 仮想ディスクは、ローカル ホストまたはリモート ファイル システム上にある特定のファイルまたはファイルのセットです。これは、オペレーティング システム内の物理ディスク ドライブと同じように動作します。

仮想マシン、VM （VMware）

*仮想マシン（VM）*は、物理コンピュータと同じように、オペレーティング システムおよびアプリケーションを実行するソフトウェア ベースのコンピュータです。 物理ホストのリソースが仮想マシンによって、作業負荷に応じて動的に消費されます。 仮想マシンは柔軟性の高いコンピューティング ユニットであるため、展開には、データ センター、クラスタ、クラウド コンピューティング、テスト環境、デスクトップ、ノート PC など、さまざまな環境が含まれます。 一番の強みは、データ センターにあります。仮想マシンはデータセンターでサーバ統合、作業負荷の最適化、およびエネルギー効率の向上のために使用されます。

仮想ローカル エリア ネットワーク

同じ物理的な場所になくても、同じブロードキャスト ドメインに接続されたホストのように通信する一群のホスト。 同じネットワーク スイッチ上にあるかどうかにかかわらず仮想ローカル エリア ネットワーク（VLAN）上の端末ステーションをグループ化できます。 物理的にデバイスを再配置する代わりに、ソフトウェアを使用して VLAN 接続を設定できます。

簡易ネットワーク管理プロトコル（SNMP： Simple Network Management Protocol）

*簡易ネットワーク管理プロトコル（SNMP）*はインターネットの標準的な管理プロトコルです。SNMP 管理アプリケーションおよびエージェントは、get 要求、set 要求、get-next 要求、get レスポンス、およびトラップ PDU を使用して互いと通信します。 MIB は、ネットワークとシステムのリソースおよびアプリケーションの履歴を管理し、それらが交換するデータを定義します。

管理情報ベース（MIB）

*管理情報ベース（MIB）*はリソースのプロパティを説明するデータ ストアです。 MIB には ASN.1 で書き込まれます。これは管理基準によって指定された言語で、SNMP MIB を定義するために OSI の管理情報の構造（SMI）基準に準拠しています。

共有メモリ（Solaris）

*共有メモリ*は、プロジェクト内で実行されるプロセスで使用可能なメモリの合計量を定義します。

クラスタ

*クラスタ*とは、2 台以上の独立したコンピュータ システムが連携して 1 つのエンティティとして機能するものです。 並列処理、負荷分散、およびフォールト トレランスではクラスタ化を行います。

グローバル ゾーン（Solaris）

*グローバル ゾーン*は、すべての Solaris システムに含まれているゾーンです。 非グローバル ゾーンがシステムに存在する場合、システムおよびシステムの全体管理のデフォルト ゾーンはグローバル ゾーンになります。

軽量プロセス、LWP （Solaris）

*軽量プロセス（LWP）*は、Solaris 10 カーネル スレッド モデルに属します。 LWP によって、カーネル スレッドとユーザ スレッドが関連付けられ、ユーザ スレッドの実行コンテキストが形成されます。Solaris 10 カーネルでは、カーネル サービスとカーネル タスクがカーネル スレッドとして実行されます。 ユーザ スレッドが作成されると、関連付けられた LWP とカーネル スレッドも作成され、ユーザ スレッドにリンクされます。 リソース管理によって、LWP の境界を設定できます。

コンテナ（Solaris）

Solaris *コンテナ*は、アプリケーションの完全なランタイム環境を提供します。 リソース管理と Solaris ゾーンはコンテナの一部です。

サービス指向アーキテクチャ（SOA）

*サービス指向アーキテクチャ（SOA）*は、さまざまなビジネス機能向けに大規模なアプリケーションではなく小規模なサービスを作成するプログラミング手法です。 これらのサービスは、複数の部門で共通機能を共有できるため、高い柔軟性と再利用性を実現できます。

シャーシ（UCS）

Cisco UCS スイッチおよびブレードを格納するハードウェア フレーム

上限のある論理パーティション（LPAR）

*上限のある論理パーティション*は、割り当てられたプロセッサ ユニットを超えるプロセッサ能力を使用できない論理パーティションです。 上限のあるパーティションには最大容量が割り当てられていて、容量が超過しないように、また物理システム全体の動作に影響を与えないようになっています。

ストレージ エリア ネットワーク、SAN

*ストレージエリアネットワーク（SAN）*は、リモート コンピュータ ストレージ デバイスをサーバに接続するためのアーキテクチャです。リモート デバイスがオペレーティング システムにローカルに接続されているように表示されます。

ストレージ層

「層」を参照してください。

スナップショット

*スナップショット*は、ある時点における仮想マシンの記録です。 スナップショットを使用すると、予約マネージャ ユーザは管理者に問い合わせなくても、VM を以前の状態にリストアできます。 スナップショットは開発環境やテスト環境で役立ちます。 スナップショットの作成を許可するかどうかを管理者が制御できるため、すべてのサイトでスナップショットを利用できるとは限りません。

正規表現

*正規表現*とは、照合に使用するテキスト パターンです。 プレーン テキストと特殊文字の組み合わせを含む文字列を使って、必要とされる種類の一致を指定します。

セキュリティ グループ（Amazon EC2）

*セキュリティ グループ*は、実行中のインスタンスに対する IP フィルタリングを説明するために Amazon が使用する用語です。 詳細については、http://docs.amazonwebservices.com にアクセスしてください。

層

予約マネージャ において、*ストレージ層*は各ディスクに関連付けられたデータストアの分類です。層は、通常、VM とそのハード ドライブが作成されるデータストアの各種レベルのパフォーマンスを示しています。

組織単位

*組織単位*は、ユーザのグループの 1 つです。組織単位は、ユーザにリソース プール、システム イメージ、テンプレートなどのオブジェクトへのアクセス権を付与することで、セキュリティを確保します。

タイムシェア スケジューラ、TS （Solaris）

*タイムシェア スケジューラ（TS）*は、すべてのプロセスに対して、利用可能な CPU の均等なアクセスを提供するスケジューラ クラスを指定します。これによって、優先度に基づいて CPU 時間が割り当てられます。

タスク（Solaris）

*タスク*は、一定期間における 1 セットの作業を表します。個々のタスクは 1 つのプロジェクトに関連付けられます。

データストア（VMware）

*データストア*は、データセンター内の基本要素である物理ストレージ リソースの組み合わせを仮想的に表現したものです。 これらの物理ストレージ リソースとして提供できるのは、サーバ上のローカル ディスクや SAN ディスク アレイなどです。

データセンター（VMware）

*データセンター*は、ホスト、仮想マシン、リソース プール、またはクラスタのコンテナとして機能します。 仮想設定が特定の部門の要件を満たしていれば、データセンターは、地理的な地域や個別のビジネス機能などの組織構造を表すことができます。 また、データセンターを使用して、テスト用の分離された仮想環境を構築したり、環境を組織したりすることができます。

デュアル HMC （LPAR）

デュアル HMC は、高可用性を提供する冗長なハードウェア管理コンソール（HMC）管理システムです。

動的再構成コネクタ インデックス、DRC インデックス（LPAR）

物理システム ユニットの各スロットには、*DRC インデックス*が割り当てられています。 展開プロセスで LPAR を実際に作成するには、この番号が必要になります。 管理コンソール（HMC）およびシステムは、このインデックスを使用してシステム上の各スロットを一意に識別します。 ユニットに電源を投入するまで、DRC インデックスはスロットに割り当てられません。

トラップ

*トラップ*は、エージェントとリソースのイベントの管理アプリケーションに通知するために、1 つ以上の管理者へ SNMP エージェントが送信できる非請求メッセージです。 SNMP トラップは一般的（SNMP エージェントのすべてのタイプに共通）であるか、または企業に固有（それを送信するエージェントに一意）です。

ハードウェア管理コンソール、HMC （LPAR）

*ハードウェア管理コンソール（HMC）*は、IBM PowerVM システム上で管理タスクを実行するために使用する外部アプライアンスです。 HMC は、リソースをパーティションに動的に割り当てるなど、論理パーティションを作成または変更するのに使用できます。HMC は POWER システムのサーバファームウェア層と通信し、大規模 PowerVM 環境での単一制御ポイントを提供します。

非グローバル ゾーン（Solaris）

*非グローバル ゾーン*は、Solaris オペレーティング システムの単一インスタンスに、仮想化されたオペレーティング システム環境を提供します。 Solaris ゾーン ソフトウェア パーティション テクノロジによって、オペレーティング システム サービスが仮想化されます。

ファイバ チャネル、FC

*ファイバ チャネル*は、コンピュータ デバイス間でデータを転送するための、標準化されたギガビット速度テクノロジです。ファイバ チャネルは、コンピュータ サーバを共有ストレージ デバイスに接続したり、ストレージ コントローラとストレージ ドライブを相互接続したりするのに特に適しています。

フェア シェア スケジューラ、FSS （Solaris）

*フェア シェア スケジューラ（FSS）*は、共有に基づいて CPU 時間を割り当てるスケジューラ クラスを指定します。 共有では、プロジェクトに割り当てられるシステムの CPU リソースの割合が定義されます。

複数の仮想 I/O サーバ

*複数の仮想 I/O サーバ*を使用すると、クライアント パーティションのダウンタイムのない仮想 I/O サーバ メンテナンスを可能にすることによってアプリケーションの可用性を向上させる機能が提供されます。

プラットフォーム管理モジュール（PMM）

*プラットフォーム管理モジュール（PMM）*は、対応する環境用の接続および運用上のサポートを提供する Web サービスです。 サポートされる環境には、たとえば、VMware vSphere、Microsoft Hyper-V、IBM PowerVM、Solaris ゾーン、Cisco UCS、Microsoft Cluster Service などがあります。PMM は、これらの環境のサーバとの接続を管理し、環境関連の操作を実行し、対応する AIM からデータを取得し、CA Server Automation 管理データベースに格納します。

ブレード（UCS）

Cisco UCS シャーシに接続されているサーバ

プロジェクト（Solaris）

*プロジェクト*は、ホストに関連付けられたコンテナを定義します。 プロジェクトは抽象化レイヤの 1 つで、物理システム リソースの収集の構成と管理に役立ちます。

プロジェクトはタスクの集合であり、タスクはプロセスの集合です。login、cron、newtask、setproject、または su コマンドによって新しいセッションが開かれると、プロジェクト内で新しいタスクが開始されます。 各プロセスは 1 つのタスクのみに属し、各タスクは 1 つのプロジェクトのみに属します。

プロジェクトとタスクは、Solaris 10 オペレーティング システム内の作業負荷を識別するのに使用される基本エンティティです。プロジェクトは 1 セットのユーザおよび 1 セットのグループに関連付けられます。ユーザとグループは、自身がメンバであるプロジェクトのコンテキストでプロセスを実行でき、複数のプロジェクトのメンバになることもできます。 プロジェクトは、リソースの使用を制限できる基本エンティティです。 タスクは、プロセスが関連付けられるエンティティで、プロジェクトは 1 セットのタスクに関連付けられます。

プロセッサ セット、pset （Solaris）

*プロセッサ セット*は、CPU の非結合グループを定義します。 各プロセッサ セットに、ゼロ個以上のプロセッサを含めることができます。プロセッサ セットは、リソース プール設定内のリソース要素の 1 つです。

プロセッサ プール（LPAR）

*プロセッサ プール*は異なる論理パーティション間で共有することができる物理プロセッサのセットです。

プロビジョニング

ディスカバリの後、*プロビジョニング*によって、物理マシンまたは仮想マシンを検索し、オペレーティング システムとイメージを追加して、利用できるようにすることができます。 特定のマシン特性が必要な場合、本製品によって、そのニーズを満たすようにマシンをプロビジョニングできます。

ポーリング間隔

*ポーリング間隔*とは、リソース グループに対して連続的に行うポーリングの間隔時間です。

ポリシーベースの設定

*ポリシーベースの設定*を使用すると、1 回の操作で、管理対象のマシンのセットに展開できるエージェント設定ポリシーを作成できます。

文字列化

*文字列化*とは、一連の文字を取得して、適切な JavaScript リテラル文字列に変換することを指します。

リソース管理（Solaris）

Solaris ゾーンの *リソース管理*は、作業負荷に対して特定リソースの消費に制限を定義することで、直接セットアップすることができます。 作業負荷は、アプリケーションまたはアプリケーションのグループのすべてのプロセスを集約したものです。

リソース管理は、zonecfg（1M）に記述された zonecfg コマンドによって、/etc/project ファイルまたはゾーンの設定に格納されます。

リソース プール（Solaris）

*リソース プール*は、システム リソースをパーティション分割するための設定メカニズムを定義します。 リソース プールとは、パーティション分割できるリソース グループ間の関連付けです。

リソース プール（VMware）

*リソース プール*は、単一ホストまたはクラスタの物理的なコンピューティング リソースとメモリ リソースのパーティションを定義します。 任意のリソース プールを小さくパーティション分割することで、特定のグループや特定の目的のためにリソースを分割して割り当てることができます。 また、リソース プールを階層的に構成して、ネストすることもできます。

リモート展開

*リモート展開*は、1 回の操作で企業全体の複数のシステムにモニタリング エージェントを展開して設定する機能を提供します。

論理パーティション、LPAR

*論理パーティション（LPAR）*は、独立したシステムとして仮想化される、ハードウェア リソースのサブセットです。物理システムは複数の LPAR に分割でき、それぞれの LPAR が個別のオペレーティング システムとアプリケーションを提供します。 論理パーティションの数は、システムのハードウェア構成によって異なります。 LPAR は通常、データベースや Web サーバなどの異なる環境で使用されます。 LPAR は、ネットワーク内で独立したシステムとして通信を行います。

論理メモリ ブロック、LMB （LPAR）

*論理メモリ ブロック（LMB）*は、LPAR に割り当てられる物理メモリと論理メモリの粒度を指定します（256 MB など）。

割り当てプール容量（LPAR）

共有プロセッサ プールの*割り当てプール容量*は、プロセッサ プールのパーティション グループが使用できる保証プロセッサ容量を定義します。

索引

C

D

E

F

G

H

I

J

R

S

U

V

W

X

あ

か

さ

た

な

は

ま

や

ら

わ