CA Virtual Assurance for Infrastructure Managers

インストール ガイド

リリース 12.8

CA Technologies 製品リファレンス

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

- CA 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 Patch Manager
- CA Server Automation
- CA Service Desk Manager （CA SDM）
- CA Spectrum®
- CA SystemEDGE
- CA Systems Performance for Infrastructure Managers
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

CA への連絡先

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

目次

第 1 章: はじめに

CA Virtual Assurance は、仮想データ センター インフラストラクチャのパフォーマンスを管理する、ポリシーベースの製品です。

サービス指向アーキテクチャ上に構築された CA Virtual Assurance は、このようなインフラストラクチャを継続的に分析し、必要なタスクを実行するための UNIX、Linux、および Windows サーバの確実なプロビジョニングと、変更の自動検出を可能にします。

CA Virtual Assurance は、仮想環境と動的環境のパフォーマンスを高め、作業負荷を減らすことで、運用効率およびエンドツーエンドのデータ センター自動化を向上させます。

このセクションには、以下のトピックが含まれています。

スコープ

このガイドでは、CA Virtual Assurance をインストールし、実装する方法、およびこの製品の使用を開始する方法について説明します。 製品のアーキテクチャ、コンポーネント、および要件の概要も示します。

また、CA Virtual Assurance をさまざまなモードでインストールする手順を段階別に説明し、インストール後のタスクについて詳しく解説します。

用語集では、仮想化テクノロジで使用される特定の用語について説明します。

対象読者

このガイドは、CA Virtual Assurance をインストールおよび設定して、仮想環境を管理するために使用する管理者を対象としています。 読者が、お使いの環境で使用されるオペレーティング システム、仮想化技術、および SNMP に精通していることを前提とします。

関連ドキュメント

CA Virtual Assurance のマニュアルは、次のマニュアルで構成されています。

管理ガイド

ユーザの環境の仮想リソースを管理するために、CA Virtual Assurance を管理および使用する方法を調査します。

インストール ガイド

簡単なアーキテクチャ情報、さまざまなインストール方法、インストール後の設定情報、および導入時の手順が含まれます。

オンライン ヘルプ

CA Virtual Assurance ユーザ インターフェースを使用するためのウィンドウの詳細、および手順の説明を提供します。

リファレンス ガイド

AutoShell、CLI コマンド、および MIB 属性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。

リリース ノート

オペレーティング システムのサポート、システム要件、発行済みの修正プログラム、各国語のサポート、既知の問題、およびドキュメント ロードマップに関する情報を提供します。

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 のインストールおよび設定の詳細について説明します。

SystemEDGE リリース ノート

オペレーティング システムのサポート、システム要件、および機能に関する情報を提供します。

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 Virtual Assurance または CA Virtual Assurance 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: CA Virtual Assurance のインストール

このセクションには、以下のトピックが含まれています。

インストールの要件および考慮事項

このセクションでは、CA Virtual Assurance をインストールするための要件と考慮事項について説明します。

SQL Server Express のインストールおよび設定

SQL Server をインストールしていない場合は、代わりに、DVD1 から SQL Server Express をインストールします。

次の手順に従ってください:

1. DVD1 の Installers¥Windows¥External¥MSSQLExpress ディレクトリに移動し、セットアップを実行します。
2. インストール後、SQL Server 構成マネージャを使って TCP/IP を有効にします。
3. SQL Server 構成マネージャから、静的な TCP ポート番号を特定します（［ネットワーク構成］/［プロトコル］/［TCP/IP のプロパティ］/［IP アドレス］）。
4. CA Virtual Assurance インストール時のポート番号とインスタンス名（デフォルトでは SQLEXPRESS）を適用して、SQL Server Express に接続します。

リモート SQL Server にアクセスする予定の場合

- SQL Server クライアントを CA Virtual Assurance マネージャ コンピュータにインストールします。
- リモート SQL Server 上のリモート接続を有効にします。

関連項目

SQL Server を使用するための要件の確認 (P. 15)

SQL Server を使用するための要件の確認

CA Virtual Assurance には、管理データベースとパフォーマンス データベース用の SQL Server が必要です。 CA Virtual Assurance は以下の SQL Server サポートを提供します。

- ローカルまたはリモートの SQL Server
- デフォルトの SQL Server インスタンスまたは指定のインスタンス
- SQL Server 用の静的な TCP/IP ポート
- Windows 認証と SQL Server 認証

次の手順に従ってください:

1. SQL Server 要件の確認
   - TCP/IP が有効であることを確認します。
   - 使用を計画しているインスタンスについて、静的な TCP/IP ポートが指定されていることを確認します。 動的ポートはサポートされていません。
   - ローカル データベースのサーバ名として使用されている IP アドレスがないことを確認します。
   - リモート コンピュータから接続する場合、リモート接続が有効になっていることを確認します。
   - 必要な認証モードが指定されていることを確認します（混合モードまたは Windows 認証）。
   - 新しい標準インストールまたはカスタム インストールで使用を計画しているインスタンスに、AOM2 または DPM という名前のデータベースが含まれていないことを確認します。CA Virtual Assurance はこれらのデータベースをインストール中に作成します。
2. SQL Server クライアント要件の確認

   ローカルの CA Virtual Assurance マネージャ システムに SQL Server クライアントがインストールされていることを確認します。 CA Virtual Assurance マネージャは、ローカルまたはリモートの SQL Server に接続するために、SQL Server クライアントを必要とします。 CA Virtual Assurance マネージャ インストール プログラムは、利用可能なシステム パス エントリを使用して SQL Server クライアント プログラムにアクセスします。

セキュリティに関する考慮事項

CA Virtual Assurance は CA Embedded Entitlements Manager （CA EEM）を使用してセキュリティ保護されています。CA Virtual Assurance のインストール時、以下のいずれかの認証方法を選択できます。

ネイティブ セキュリティ

CA EEM 管理者は、CA Virtual Assurance 専用に独自のユーザ、ユーザ グループ、およびポリシーを作成することができます。これらすべての情報がローカル ストアに保持されるためです。ただし、そのためには、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。その定義は、ディレクトリ サービスに現在登録されているユーザまたはユーザ グループと一致しない可能性があります。

Active Directory

既存の Active Directory 設定と統合する場合、ユーザおよびユーザ グループはすべて事前に定義されているので、ユーザの中央リポジトリと一貫性が保たれます。 ただし、新規ユーザの作成または既存ユーザの変更を行うには、Active Directory を使用します。CA Virtual Assurance または CA EEM は使用できません。

要件を評価し、最適な設定を選択します。

Windows メモリ管理の最適化

CA Virtual Assurance マネージャまたは CA Virtual AssuranceAIM サーバ上で Windows メモリ管理のパフォーマンスを最適化するには、Microsoft サポート技術情報の記事（http://support.microsoft.com/kb/315407/ja）で解説されている設定を適用できます。

SystemEDGE と CA Systems Performance LiteAgent の比較

CA Virtual Assurance には、SystemEDGE と CA Systems Performance LiteAgent の 2 つのモニタリング エージェントが付属しています。

SystemEDGE は、業界標準の MIB を使用してモニタ対象要素へのアクセスを提供する、SNMP 準拠エージェントです。 また、SystemEDGE は拡張可能プラグイン（AIM）インターフェースも提供するため、vCenter Server、Solaris ゾーン、サービス レスポンスのモニタリングなど、追加のモニタリングが可能です。 SystemEDGE はステータスとパフォーマンスのデータを CA Virtual Assurance マネージャに提供します。 仮想環境と仮想サーバを管理するためには、SystemEDGE は必須です。

CA Systems Performance LiteAgent は、Windows、UNIX、および Linux 上の多くのパフォーマンス メトリックへのアクセスを提供する、軽量なモニタリング エージェントです。 Windows の場合、パフォーマンス レジストリに含まれるほぼすべてのメトリックをモニタする機能が含まれます。 モニタリングはマネージャ コンポーネントからの要求に基づいて、オンデマンドで実行されます。 CA Systems Performance LiteAgent はパフォーマンス データを CA Virtual Assurance マネージャに提供します。

SystemEDGE と CA Systems Performance LiteAgent の違いに関する詳細については、以下の表を参照してください。

機能	SystemEDGE Agent	CA Systems Performance LiteAgent
SNMP-compliant エージェント	Y	N
SNMP-based トラップ	Y	N
Zero Configuration エージェント	N	Y
SNMP v1/v2 通信	Y	N
SNMP v3 通信	Y	N
コンピュータ名/アドレスによるモニタリング制限	Y	N
CAM ベースの通信	設定操作のみ	Y
複数のマネージャ インスタンスのサポート	Y	Y
Spectrum IM のサポート	Y	N

機能	SystemEDGE Agent	CA Systems Performance LiteAgent
eHealth のサポート	Y	N
NSM のサポート	Y	Y
サードパーティ マネージャのサポート	Y	N
UI の［リソース］タブのサポート	Y	N
UI の［ポリシー］タブのサポート	Y	Y
パフォーマンス DB へのデータ保存	Y	Y
ファイルベースの設定	Y	n/a
マネージャ UI ベースの設定	Y	n/a
階層オブジェクト モデル	Y	N
エージェント ベースのしきい値モニタリング	Y	N
ホスト リソース MIB のサポート	Y	N
Windows のパフォーマンス メトリック	部分的 [1]	Y
拡張可能なパフォーマンス モニタリング	N	Y [2]
広範な UNIX/Linux モニタリング	Y	Y
真の平均的なパフォーマンス モニタリング	Y	N
vCenter Server 管理のサポート	Y （AIM）	N
Hyper-V 管理のサポート	Y （AIM）	N
Solaris ゾーン管理のサポート	Y （AIM）	N
LPAR モニタリングのサポート	Y （AIM）	Y
UCS 管理のサポート	Y （AIM）	N
Active Directory および Exchange Server のサポート	Y （AIM）	N
IBM PowerHA AIM のサポート	Y （AIM）	N
VMware vCloud 用の AIM のサポート	Y （AIM）	N
Citrix XenServer 用の AIM のサポート	Y （AIM）	N
Citrix XenDesktop 用の AIM のサポート	Y （AIM）	N
KVM 用の AIM のサポート	Y （AIM）	N

機能	SystemEDGE Agent	CA Systems Performance LiteAgent
Huawei GalaX 用の AIM のサポート	Y （AIM）	N

（1） SystemEDGE は限定された一連のパフォーマンス メトリックをサポートします。 「SystemEDGE ユーザ ガイド」を参照してください。

（2） CA Systems Performance LiteAgent は Windows パフォーマンス メトリックを動的にモニタできます。

CA Virtual Assurance のインストール

このセクションでは、Windows オペレーティング環境に CA Virtual Assurance をインストールするためのコンポーネント、インストール オプション、および手順について詳しく説明します。

インストールの準備

インストールでは、インストールするコンポーネントを選択したり、認証情報を指定したりできます。 インストール中、ウィザードには選択したコンポーネントをインストールするために必要なダイアログ ボックスのみ表示されます。 選択内容に応じて、以下の環境関連のデータが要求されます（かっこ内はデフォルト値）。

コンポーネント	サーバ	ユーザ	パスワード	プロトコル	ポート
管理 DB （1）	X	X （sa）	X	-	X （1443）
パフォーマンス DB （1）	X	X （sa）	X	-	X （1443）
CA EEM 認証（2）	X	EiamAdmin	X	-	-
サービス ユーザとしての Apache ログオン（3）	-	X	X	-	-
サービス ユーザとしての Tomcat ログオン（4）	-	X	X	-	-
ネイティブ セキュリティ ユーザ（5）	-	X	X	-	-

コンポーネント	サーバ	ユーザ	パスワード	プロトコル	ポート
Active Directory セキュリティ (5, 6)	X	X	X	-	-
システム ユーザ	-	sys_service	X	-	-
Network Discovery Gateway	-	-	-	-	X （8082）
Apache HTTP サーバ	-	-	-	-	X （443）
Apache Tomcat サーバ	-	-	-	-	X （8443）
Apache Tomcat シャットダウン	-	-	-	-	X （8005）
ActiveMQ	-	-	-	-	X （61616）

（1） Windows 認証（デフォルト）または SQL 認証を選択します。 SQL 認証を選択した場合は、データベース管理者（sa）の名前とパスワードを入力します。 管理データベースの適切な初期サイズを選択します。

初期サイズ	システム数	空きディスク領域
小	1,000	1 GB - コア コンポーネント 500 MB - ログ ファイル
中	5,000	5 GB - コア コンポーネント 1 GB - ログ ファイル
大	10,000	10 GB - コア コンポーネント 5 GB - ログ ファイル

SQL Server データベースはデフォルトでは完全復旧モデルに設定されるため、トランザクション ログはバックアップされるまで増加します。 データベース バックアップは定期的にスケジュールしてください。

パフォーマンス データベースのデフォルト値は 500 MB で、必要に応じて自動的に増加します。

（2）CA EEM がサポートする AIP インスタンスは 1 つだけです。指定された EEM インストール内に AIP インスタンスが存在する場合は、以下のいずれかのオプションを実行します。

- AIP インスタンスのない CA EEM インストールを指定します。
- 不要になった AIP インスタンスを削除します。 CA EEM ユーザ インターフェースを開き、［設定］タブを開いて AIP を選択し、［登録解除］をクリックします。
- CA Virtual Assurance によって CA EEM をローカル システムにインストールさせます。

注: CA EEM 12.0 を使用する場合は、CA Virtual Assurance のインストールを開始する前に、CA EEM で ［EEM アプリケーション ユーザ］および［EEM システム ユーザ］を指定します。たとえば、管理者および sys_service ユーザを CA EEM に追加できます。

（3）ユーザ名とパスワードを入力して、Apache での「サービスとしてログオン」権限を Windows の管理ドメイン ユーザに付与します。 リモート SQL Server に Windows 認証を使用する場合は、このユーザが必要です。この章の「複数のサーバへのインストール (P. 29)」も参照してください。

（4）ユーザ名とパスワードを入力して、Tomcat での「サービスとしてログオン」権限を Windows の管理ドメイン ユーザに付与します。 リモート SQL Server に Windows 認証を使用する場合は、このユーザが必要です。 Tomcat と Apache に対して同じユーザを指定できます。 この章の「複数のサーバへのインストール (P. 29)」も参照してください。

（5）Active Directory セキュリティまたはネイティブ セキュリティ（デフォルト）を選択します。

（6） Active Directory セキュリティを選択し、外部ディレクトリのホスト名、ユーザ、およびパスワードを入力します。

注: インストールで、配布サーバと同じシステムに SystemEDGE をインストールする場合、SystemEDGE の構成マネージャ ホスト名は localhost に設定されます。

関連項目

CA Virtual Assurance マネージャ インストーラによる SystemEDGE のインストール (P. 57)

インストールの実行

すべての前提条件を満たしていると判断したら、以下の手順に従います。

次の手順に従ってください:

1. DVD ドライブにインストール メディアを挿入します。

   自動再生が有効の場合、インストール ウィザードが自動的に開始されます。インストール ウィザードが開始されない場合は、setup.hta をダブルクリックするか、インストール メディア上の *DVD ドライブ*¥Installers¥Windows ディレクトリに移動し、install.exe をダブルクリックします。

   ［インストール前の確認］ダイアログ ボックスが表示されます。

2. ［インストール前の確認］の項目に問題がないことを確認します。

   問題のある項目が存在する場合は、要件を修正し、インストールを再開します。

3. ［続行］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。

4. 内容を読み、契約の下部にスクロールすると、［*使用許諾契約書に同意します*］オプションがアクティブになります。 このオプションを選択し、［次へ］をクリックします。

   ［インストールする機能を選択］ダイアログ ボックスが表示されます。

5. インストールする CA Virtual Assurance コンポーネントを選択して、［次へ］をクリックします。

   ［必須の設定］ダイアログ ボックスが表示されます。

6. 緑のチェック マークが付いている項目と赤い x アイコンが付いている項目を確認します。

   - インストール パス

     注: 次の文字はデスティネーション パスでサポートされていません： 感嘆符「!」、左角かっこ「［」、右角かっこ「］」、左丸かっこ「(」、右丸かっこ「）」、およびセミコロン「;」。

   - データベース

     管理データベースとパフォーマンス データベースの設定を確認し、必要に応じて、データベース サーバ名、インスタンス、認証タイプ、またはポート番号（1433）を変更します。 ［OK］をクリックします。

     デフォルト： Windows 認証

     SQL 認証を選択する場合は、データベース管理者（sa）の名前とパスワードを入力します。

     注: データベース ログイン認証情報、サーバ名、またはポートが有効でない場合は、エラー メッセージが表示されるので、正しい情報を入力します。 エラーを解決できない場合、インストール プログラムは終了し、コンピュータに変更は行われません。 詳細については、「SQL Server を使用するための要件の確認 (P. 15)」を参照してください。

- CA EEM

  既存の CA EEM インストールを参照しない場合、CA Virtual Assurance はローカル システムに CA EEM をインストールします。CA Virtual Assurance はインストール中に CA EEM 内に AIP インスタンスを作成します。 CA EEM がサポートする AIP インスタンスは 1 つだけです。

  既存の CA EEM インストールを参照する場合、インストール プログラムは CA EEM で登録済みの AIP インスタンスを確認します。インストール プログラムが AIP インスタンスを検出した場合、インストール プロセスは停止します。 その AIP インスタンスが使用されていない場合は、登録解除できます。 CA EEM から AIP インスタンスを削除するには、CA EEM ユーザ インターフェースを開き、［設定］タブを開いて［AIP］を選択し、［登録解除］をクリックします。

  注: CA EEM 12.0 を使用する場合は、インストール ウィザードで CA EEM を設定する前に［EEM アプリケーション ユーザ］および［EEM システム ユーザ］を指定していることを確認してください。 インストール ウィザードの［CA EEM 設定ユーティリティ］ダイアログ ボックスで、［既存のセキュリティを使用］を有効にします。 CA EEM で指定した EEM アプリケーション ユーザ、EEM システム ユーザおよびパスワードを追加します。

- ネットワーク ポート

  一覧表示されているコンポーネントのネットワーク ポートを指定するか、または以下のデフォルト値を使用することができます。

  - ネットワーク ディスカバリ ゲートウェイ ポート： 8082
  - Apache ポート： 443
  - Tomcat サーバ ポート： 8443
  - Tomcat シャットダウン ポート： 8005
  - Apache ActiveMQ メッセージ ブローカ ポート： 61616

- 追加の実行時ロケール

  必要に応じて、アクティブにする追加のロケールを *1* つ指定して、［OK］をクリックします。

  デフォルト： 英語（米国）

- SNMP 管理

  デフォルト コミュニティの public と admin、それらの関連する SNMP ポート 161、1691、および 6665 に加えて、独自の読み取り専用と読み取り/書き込みのコミュニティおよびポートを指定できます。

  デフォルト： public、snmp_admin

  インストール中に指定されるコミュニティはすべて、インストールされた製品のグローバル（デフォルト）SNMP 設定として使用されます。必要に応じて、CA Virtual Assurance ユーザ インターフェースで SNMP 設定をさらに指定できます。「*管理ガイド*」の「SNMP およびアクセス制御リストの設定方法」を参照してください。

7. 必要な情報を入力し、［次へ］をクリックします。

   ［インストール前のサマリ］ダイアログ ボックスが開き、インストールするコンポーネントのリストが表示されます。

8. ［インストール］をクリックして、インストールを開始します。

   ［インストールの進捗状況］ダイアログ ボックスが表示されます。

   注: インストールが成功すると、インストールしたコンポーネントごとに *Install_Path*¥*productname*¥log¥install ディレクトリにログ ファイルが作成されます。

9. ［完了］をクリックします。

   ［製品ステータスの確認］ダイアログ ボックスが表示されます。

10. ［製品ステータスの確認］の項目に問題がないことを確認します。

    問題のある項目が存在する場合は、実行するアクションを確認します。たとえば、利用可能なパッチをインストールします。

    注:

    - CA Virtual Assurance の更新をインストールする場合は、「CA Virtual Assurance の更新方法 (P. 48)」を参照してください。
    - インストールが失敗した場合、インストールがエラーと共に完了したことを示すダイアログ ボックスが表示されます。 詳細については、インストール ログ（Install_Path¥*productname*¥log¥install¥install.log）およびエラー リスト（Install_Path¥*productname*¥log¥install¥install_error_detected.log）を参照してください。

11. ［スタート］-［プログラム］-［CA］-［CA Virtual Assurance］に移動し、CA Virtual Assurance を起動して、インストール時に指定した認証情報を使用してログインします。

関連項目

インストールの準備 (P. 19)
SQL Server を使用するための要件の確認 (P. 15)

インストールのキャンセル

CA Virtual Assurance インストール プログラムを実行すると、システム上の一時ディレクトリに製品ファイルが展開されている間、プログレス バーが表示されます。 インストール中の最初のダイアログ ボックスが表示される前にインストール処理をキャンセルすると、プログレス バーは消え、製品はインストールされません。 ただし、展開処理を中断することはできないので、ファイルの展開が完了するまでインストール プログラムは続行されます。 次に一時ディレクトリが削除され、システムは未変更のままになります。 ファイルの展開および一時ディレクトリの削除によって、CPU のパフォーマンスが一時的に低下する場合があります。

初期インストール後のコンポーネント インストール

初期インストール時にすべてのコンポーネントをインストールしなかった場合は、インストール プログラムを再実行して不足しているコンポーネントをインストールできます。

マネージャのサイレント インストール

このセクションでは、マネージャのサイレント インストールを実行する方法について説明します。各セクションの 1 つ以上の手順を完了してください。

注: サイレント インストールを開始する前に、ターゲット コンピュータが「*リリース ノート*」に記載されている前提条件を満たしていることを確認してください。

関連項目

インストール メディアからのサイレント インストール ファイルのコピー (P. 27)
マネージャのサイレント インストールの実行 (P. 29)

インストール メディアからのサイレント インストール ファイルのコピー

レスポンス ファイルを編集し、実際のインストール プログラムを実行する前に、インストール メディアに含まれるこれらのファイルとその他のサポート ファイルを、マネージャまたはエージェントが存在するサポート対象サーバにコピーします。

DVD1 は、Windows へのマネージャの完全インストール（SystemEDGE と SystemEDGE AIM を含む）に必要です。

DVD2 は、AIX、HP-UX、Linux、または Solaris （SPARC、x86）での CA Virtual Assurance 管理対象ノードのインストールに必要です。

次の手順に従ってください:

1. DVD1 の Installers ディレクトリをターゲット コンピュータにコピーします。
2. ダウンロードしたインストール メディアのルート ディレクトリに移動し、*ResponseFileTemplates* ディレクトリに移動します。

   silent.properties ファイルがリスト内に表示されます。
3. silent.properties ファイルをターゲット コンピュータ上の ¥Installers¥Windows ディレクトリにコピーします。

   要件ごとにホスト サーバ上の silent.properties ファイルを編集できます。

silent.properties ファイルの編集

サイレント インストール プログラムは silent.properties ファイルを使用して、サポート対象の Windows コンピュータにマネージャ コンポーネントをインストールするための基本設定に関する情報を取得します。 サイレント インストールを実行するには、このファイルを編集します。

重要: silent.property ファイルでは、UTF-8 の文字エンコーディングのみがサポートされています。 UTF-8 文字のサポートおよび国際化の詳細については、リリース ノートを参照してください。

次の手順に従ってください:

1. ターゲット コンピュータ上の ¥Installers¥Windows ディレクトリに移動し、テキスト エディタで silent.properties ファイルを開きます。

   ファイルの内容が表示されます。
2. ファイル内の指示に従って、コメント内のインストール オプションのセクションを指定します。 例：

   `USER_INSTALL_DIR=C:¥¥Program Files¥¥CA¥¥productname`

   パスを定義するには、2 つの円記号（¥¥）を使用します。

   注: 必要なセクションを更新します。ファイル内のセクションは使用されなくても削除しないでください。
3. ファイルを保存して閉じます。

サイレント インストール プログラムを実行すると、自分の設定に基づいて指定のマネージャ コンポーネントがインストールされます。

マネージャのサイレント インストールの実行

Windows システム上でマネージャのサイレント インストールを実行するには、DVD1 のファイルを使用します。

次の手順に従ってください:

1. ターゲット 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 ウィンドウが表示されます。

2. ¥Installers¥Windows¥ ディレクトリに移動し、以下のコマンドを入力します。

   `install.exe -i silent -f silent.properties ファイルのパス¥silent.properties`

   インストールが開始され、マネージャがシステムにインストールされます。

3. インストールが完了したら、*Install_Path*¥*productname*¥log¥install ディレクトリ内のファイルにエラーや警告がないかどうかを確認します。

   注: 分散サイレント インストールでは、まずサービス コントローラを実行してから、他のコンポーネントをインストールする必要があります。これは、他のコンポーネントを検証できるようにするためです。

関連項目

インストール メディアからのサイレント インストール ファイルのコピー (P. 27)
silent.properties ファイルの編集 (P. 28)

複数のサーバへのインストール

デフォルト設定に基づいたインストールは、一元化されたインストールになります。CA Virtual Assurance マネージャ コンポーネント、データベース、SystemEDGE および全 AIM は、すべて単一の Windows サーバ上で実行されます。ただし、必要なすべての CA Virtual Assurance コンポーネントを個別のサーバにインストールできます。

このセクションでは、複数のサーバが関係するインストールのシナリオについて説明します。

関連項目

複数のサーバへインストールする場合のガイドライン (P. 30)
エージェントの個別インストール (P. 55)

複数のサーバへインストールする場合のガイドライン

CA Virtual Assurance コンポーネントを異なるサーバにインストールするには、各サーバでインストールを実行する必要があります。 インストール時にコンポーネント ツリーで必要なコンポーネントをそれぞれ選択します。 コンポーネント間に依存性があるため、以下のガイドラインを考慮します。

- インストール先がファイアウォールをまたがって存在する場合は、影響を受けるコンポーネント間の対応する通信ポートを開きます。
- タイムゾーンをシームレスに操作するには、ご使用の分散コンピューティング環境が共通のタイム ソース（NTP サーバ、GPS など）に同期されていることを確認します。
- Automation Management Framework が実行されるサーバで SQL 管理ツール（OSQL、BCP）が利用できることを確認します。 SQL 管理ツール（OSQL、BCP）は SQL Server インストールに含まれており、ローカルまたはリモート SQL Server へのアクセスに必要です。 Automation Management Framework と、管理データベースおよびパフォーマンス データベースにアクセスする全 CA Virtual Assurance マネージャ コンポーネントは、1 台のサーバ上に存在している必要があります。
- SQL Server で TCP が有効になっており、静的なポート（デフォルト：1433）が設定されていることを確認します。 リモート SQL Server に接続する場合は、SQL Server でリモート アクセスを許可します。 CA Virtual Assurance では、Windows 認証または SQL Server 認証時に管理データベースとパフォーマンス データベースにアクセスすることができます。

- リモート SQL Server に対して Windows 認証を使用する場合は、次の要件を確認します： CA SM ドメイン サーバ、Apache HTTP サーバ、および Apache Tomcat サービスは、ローカル以外のシステム アカウントで実行される必要があります。ローカル以外のシステム アカウント（ドメイン ユーザ アカウント）は、マネージャ サーバとデータベース サーバに対するアクセス権限が必要です。 リモート SQL Server に Windows 認証を使用する場合は、自動的にそのユーザの入力を求められます。

  これらの条件は SQL Server 認証では必要ありません。

- 配布サーバをリモート システムにインストールする場合、関連する CA SM ドメイン サーバに接続するように配布サーバを設定します。

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 配布サーバの［プロパティ］ダイアログ ボックスを開きます。
3. 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追加します。

   -m *<CA SM ドメイン サーバ サービスが実行されているシステムの名前>*

5. サービスを開始し、［OK］をクリックします。

シナリオ: 最大限の分散インストール

このシナリオでは、個別のサーバにインストールできる CA Virtual Assurance コンポーネントをすべて一覧表示します。

サーバ 1

CA Virtual Assurance マネージャ コンポーネント
SQL Server 管理ツール（OSQL、BCP）

サーバ 2

CA EEM

サーバ 3

管理データベース

サーバ 4

パフォーマンス データベース

サーバ 5

配布サーバ

サーバ 6

SystemEDGE および AIM

実際の実装によっては、サーバ数はより少なくても十分です。

例

1 台のサーバ上のリモート データベース、リモート配布サーバ、ローカル CA EEM、SystemEDGE、および AIM：

サーバ 1

CA Virtual Assurance マネージャ コンポーネント
SQL Server 管理ツール（OSQL、BCP）
CA EEM
SystemEDGE および AIM

サーバ 2

管理データベース
パフォーマンス データベース

サーバ 3

配布サーバ

関連項目

通信ポート (P. 33)

通信ポート

CA Virtual Assurance では、複数のポートが開いていて、正常に機能する必要があります。 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。

Active Directory および Exchange Server（ADES）

PowerShell ポート： 80、443、5985、5986

ADSI ポート： 3268、389

Apache サーバ

HTTPS ポート： 443

CA EEM サーバ

iGateway ポート： 5250

SystemEDGE

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

CA Systems Performance LiteAgent

CAM UDP ポート： 4104

CAM TCP ポート： 4105

Cisco UCS

HTTP ポート： 80

HTTPS ポート： 443

Citrix XenDesktop

WinRM ポート： 5985、5986

SNMP ポート： 161

WMI ポート： 135

Citrix XenServer

HTTPS ポート： 443

SNMP ポート： 161

Huawei GalaX

HTTP ポート： 8773

Hyper-V および SCVMM

WMI ポート： 135

IBM PowerHA

Secure Shell TCP ポート： 22

IBM PowerVM

Secure Shell TCP ポート： 22

カーネル ベースの仮想マシン（KVM）

REST API ポート： 8443

キー パフォーマンス データベース（KPDB）

デフォルトの HTTP ポート： 8555

Microsoft SQL Server

管理 DB TCP ポート： 1433

パフォーマンス DB TCP ポート： 1433

MSCS AIM

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

Secure Shell TCP ポート： 22

ポリシー設定

CAM UDP ポート： 4104 （受信/送信）

CAM TCP ポート： 4105 （受信）

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

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

リモート モニタリング AIM

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。

SNMP **スタック**

UDP ポート： 161、1691、162 （トラップ、受信）

サポート エージェント

デフォルトの HTTP ポート： 8556

Tomcat（**ユーザ インターフェース**）

HTTPS ポート： 8443

シャットダウン ポート： 8005

VMware vCenter

HTTPS ポート： 443

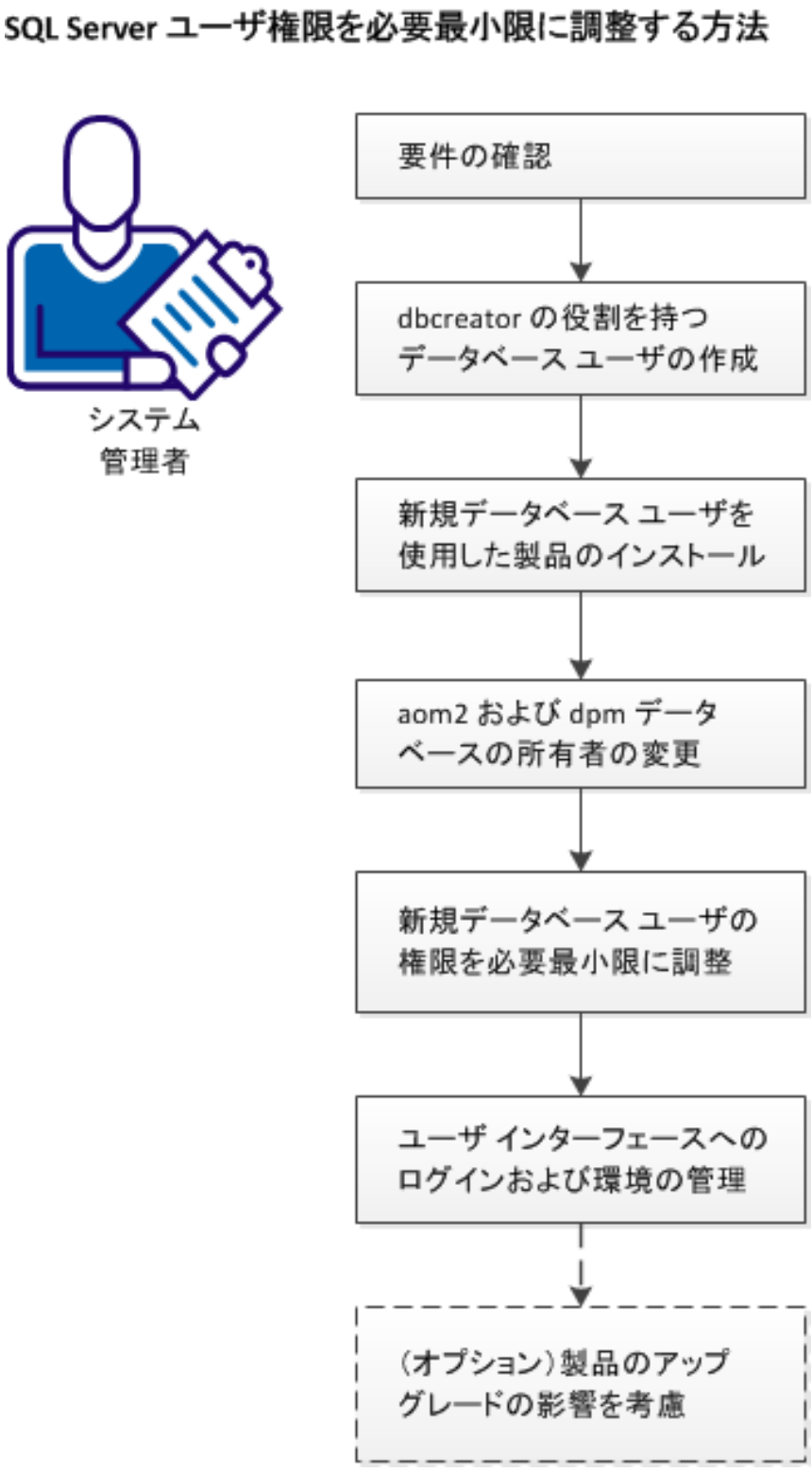
VMware vCloud

REST API ポート： 8443

SQL Server ユーザ権限を必要最小限に調整する方法

システム管理者として CA Virtual Assurance に必要な権限を最小化して SQL Server データベースにアクセスするとします。

以下の図は、権限を調整するために必要な手順を示しています。


SQL Server ユーザ権限を必要最小限に調整する方法
システム
管理者
要件の確認
dbcreator の役割を持つ
データベース ユーザの作成
新規データベース ユーザを
使用した製品のインストール
aom2 および dpm データ
ベースの所有者の変更
新規データベース ユーザの
権限を必要最小限に調整
ユーザ インターフェースへの
ログインおよび環境の管理
(オプション)製品のアップ
グレードの影響を考慮

以下の手順に従います。

要件の確認

CA Virtual Assurance データベース ユーザのユーザ権限の変更を開始する前に、以下の要件を確認します。

- ユーザは Windows Server および SQL Server の管理をよく理解しています。
- CA Virtual Assurance をインストールするシステムが、リリース ノートで指定されたマネージャ要件を満たしています。
- SQL Server が「インストール ガイド」および「リリース ノート」に指定された要件に従ってインストールされています。
- SQL Server 認証または Windows 認証が使用できます。
- CA Virtual Assurance をインストールするための以下のいずれかのアカウント タイプが使用できます。
  - ドメイン ユーザ（domain¥domainuser）
  - ローカル ユーザ（system¥localuser）
  - ローカル管理者（system¥administrator）

  インストールに使用するアカウントは管理グループのメンバである必要があります。
- シナリオ内の例では、CA Virtual Assurance のインストールに my_domain¥my_account アカウントを使用し、またこのアカウントは管理者グループのメンバーでもあります。

dbcreator の役割を持つデータベース ユーザの作成

製品インストール中に使用する CA Virtual Assurance 用のデータベース ユーザを作成し、このユーザに役割 dbcreator を適用します。 インストール後、CA Virtual Assurance は同じユーザをユーザ マッピング設定に使用できます。

Windows 認証

次の手順に従ってください:

1. my_domain¥my_account を使用するか、ローカル システム管理者としてシステムにログインします。
2. 管理者（sa）権限で、またはローカル システム管理者として SQL Server にログインします。
3. ナビゲーション ツリーのセキュリティ フォルダを展開します。
4. ログイン フォルダを右クリックしてから、［新しいログイン］を選択します。

   ［新しいログイン］ダイアログ ボックスが表示されます。
5. ［全般］セクションの下で、以下の設定を指定します。
   - ［Windows 認証］を選択します。
   - ［検索］をクリックし、ログイン名（たとえば my_account）を入力し、［名前の確認］をクリックします。
   - ダイアログ ボックスで、解決されたアカウント my_domain¥my_account を確認します。
6. ［サーバー ロール］セクションに移動し、dbcreator の役割を追加し、［OK］をクリックします。

   新しいデータベース ユーザは、製品をインストールするために十分な権限があります。

SQL Server 認証

次の手順に従ってください:

1. my_domain¥my_account を使用するか、ローカル システム管理者としてシステムにログインします。
2. 管理者（sa）権限を使用して SQL Server にログインします。
3. ナビゲーション ツリーのセキュリティ フォルダを展開します。
4. ログイン フォルダを右クリックしてから、［新しいログイン］を選択します。

   ［新しいログイン］ダイアログ ボックスが表示されます。
5. ［全般］セクションの下で、以下の設定を指定します。
   - ログイン名を入力します（例： causer）。
   - SQL Server 認証を選択し、このユーザのパスワードを入力します。
   - ［ユーザーは次回ログイン時にパスワードを変更する］チェック ボックスをオフにします。
6. ［サーバー ロール］セクションに移動し、dbcreator の役割を追加し、［OK］をクリックします。

   新しいデータベース ユーザは、製品をインストールするために十分な権限があります。

新規データベース ユーザを使用した製品のインストール

新規データベース ユーザを使用して、製品をインストールできます。

Windows 認証

次の手順に従ってください:

1. my_domain¥my_account を使用して、システムにログインします。
2. Windows エクスプローラを開き、DVD¥Windows¥Installers ディレクトリに移動し、install.exe を右クリックして［管理者として実行］を選択し、CA Virtual Assurance インストール ウィザードを開始します。
3. ［必須の設定］ダイアログ ボックスでデータベース エントリをクリックします。

   データベースの設定ダイアログ ボックスが開きます。
4. ［Windows 認証］を選択します（デフォルト）。
5. 必要な場合はデータベース インスタンスを指定します。
6. ［Windows 認証 - Apache］セクションで［ローカル システム アカウントを使用］をオフにします。
7. 新規ユーザ名（my_domain¥my_account）およびパスワードを入力します。
8. 「サービスとしてログオンする権限の付与」にチェックを入れて［OK］をクリックします。
9. インストール ウィザードの指示に従って、インストールを開始します。
10. インストールが完了したら、Windows では［スタート］-［管理ツール］-［サービス］をクリックします。

    ［サービス］ウィンドウが表示されます。
11. CAAIPApache と CAAIPTomcat までスクロールし、サービスを停止します。

SQL Server 認証

次の手順に従ってください:

1. my_domain¥my_account を使用するか、ローカル システム管理者としてシステムにログインします。
2. CA Virtual Assurance の製品インストーラを起動し、インストール ウィザードを開始します。

   ローカル システム管理者でないユーザの場合は、Windows エクスプローラを開いて、DVD¥Windows¥Installers ディレクトリに移動します。install.exe を右クリックし、［管理者として実行］を選択して、インストール ウィザードを開始します。
3. ［必須の設定］ダイアログ ボックスでデータベース エントリをクリックします。

   データベースの設定ダイアログ ボックスが開きます。
4. ［SQL 認証］を選択します。
5. 必要な場合はデータベース インスタンスを指定します。
6. 新しいユーザ名（causer）とパスワードを入力し、［OK］をクリックします。
7. インストール ウィザードの指示に従って、インストールを開始します。
8. インストールが完了したら、Windows では［スタート］-［管理ツール］-［サービス］をクリックします。

   ［サービス］ウィンドウが表示されます。
9. CAAIPApache と CAAIPTomcat までスクロールし、サービスを停止します。

aom2 および dpm データベースの所有者の変更

CA Virtual Assurance のインストールでは、2 つのデータベースが作成されます： dpm および aom2。 これらのデータベースの所有権を sa ユーザまたはローカル管理者に変更します。

Windows 認証

次の手順に従ってください:

1. 管理者（sa）権限で、またはローカル システム管理者として SQL Server にログインします。
2. ［新しいクエリ］をクリックします。

   SQL コンソールが開きます。
3. 以下の SQL コマンドを入力します。

```
use dpm
exec sp_changedbowner 'system¥administrator', 'true'
use aom2
exec sp_changedbowner 'system¥administrator', 'true'
```

4. ［実行］をクリックします。

   ローカル システム管理者は aom2 および dpm データベースを所有します。

SQL Server 認証

次の手順に従ってください:

1. 管理者（sa）権限を使用して SQL Server にログインします。
2. ［新しいクエリ］をクリックします。

   SQL コンソールが開きます。
3. 以下の SQL コマンドを入力します。

```
use dpm
exec sp_changedbowner 'sa', 'true'
use aom2
exec sp_changedbowner 'sa', 'true'
```

4. ［実行］をクリックします。

   sa ユーザは aom2 および dpm データベースを所有します。

新規データベース ユーザの権限を必要最小限に調整する

CA Virtual Assurance では、データベース ユーザが aom2 と dpm データベースを使用するための十分な権限を持っている必要があります。 この手順では、これらの権限を最小限に調整する方法について説明します。

Windows 認証

次の手順に従ってください:

1. 管理者（sa）権限で、またはローカル システム管理者として SQL Server にログインします。
2. SQL Server Management Studio のオブジェクト 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. 新規ユーザ（たとえば my_domain¥my_account）を右クリックし、［プロパティ］、［ユーザー マッピング］を開きます。

   ［ユーザー マッピング］ダイアログ ボックスが表示されます。
4. ダイアログ ボックスで aom2 データベースを選択し、db_datareader および db_datawriter の役割メンバシップを割り当てます。
5. ダイアログ ボックスで dpm データベースを選択し、db_datareader および db_datawriter の役割メンバシップを割り当てます。 ［OK］をクリックします。
6. ［新しいクエリ］をクリックします。

   SQL コンソールが開きます。
7. 新しいデータベース ユーザ（my_domain¥my_account）がストアド プロシージャを実行できるようにするには、以下の SQL コマンドを入力します。

```
use dpm
GRANT EXECUTE TO "my_domain¥my_account"
use aom2
GRANT EXECUTE TO "my_domain¥my_account"
```

8. ［実行］をクリックします。
9. オブジェクト エクスプローラーで新規ユーザ（my_domain¥my_account）を右クリックし、［プロパティ］、［サーバー ロール］を開きます。

   ［サーバー ロール］ダイアログ ボックスが表示されます。
10. dbcreator の役割を削除し［OK］をクリックします。

    新規データベース ユーザは aom2 および dpm データベースを使用するための十分な権限を CA Virtual Assurance に提供します。

SQL Server 認証

次の手順に従ってください:

1. 管理者（sa）権限を使用して SQL Server にログインします。
2. SQL Server Management Studio のオブジェクト 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. 新規ユーザ（たとえば causer）を右クリックし、［プロパティ］、［ユーザー マッピング］を開きます。

   ［ユーザー マッピング］ダイアログ ボックスが表示されます。
4. ダイアログ ボックスで aom2 および dpm データベースを選択し、両方のデータベースに db_datareader および db_datawriter ロール メンバシップを割り当てます。 ［OK］をクリックします。
5. ［新しいクエリ］をクリックします。

   SQL コンソールが開きます。
6. 新しいデータベース ユーザ（causer）がストアド プロシージャを実行できるようにするには、以下の SQL コマンドを入力します。

```
use dpm
GRANT EXECUTE TO causer
use aom2
GRANT EXECUTE TO causer
```

7. ［実行］をクリックします。
8. オブジェクト エクスプローラーで新規ユーザ（causer）を右クリックし、［プロパティ］、［サーバー ロール］を開きます。

   ［サーバー ロール］ダイアログ ボックスが表示されます。
9. dbcreator の役割を削除し［OK］をクリックします。

   新規データベース ユーザは aom2 および dpm データベースを使用するための十分な権限を CA Virtual Assurance に提供します。

ユーザ インターフェースへのログインおよび環境の管理

CA Virtual Assurance ユーザ インターフェースを使用する前に、CAAIPApache および CAAIPTomcat サービスを開始します。

次の手順に従ってください:

1. Windows で、［スタート］-［管理ツール］-［サービス］をクリックします。

   ［サービス］ウィンドウが表示されます。
2. CAAIPApache および CAAIPTomcat までスクロールし、サービスを開始します。

   サービスが正常に開始した後、CA Virtual Assurance は、使用可能な状態になります。
3. CA Virtual Assurance ユーザ インターフェースを開始し、環境を管理します。

（オプション）製品のアップグレード時に SQL Server ユーザ権限を考慮

上述の SQL Server ユーザ権限には、CA Virtual Assurance のアップグレードをサポートするために db_owner の役割メンバシップが含まれる必要があります。

system¥administrator または sa データベース ユーザに以下の権限があることを確認してください。

- aom2 および dpm データベースに対する db_owner 役割メンバシップ

CA Virtual Assurance の SQL Server ユーザはインストール ウィザードで指定され、SQL Server 認証か Windows 認証かの選択に依存します。アップグレードをサポートするには、SQL Server ユーザには少なくとも aom2 データベースおよび dpm データベースに対する以下の権限が必要です。

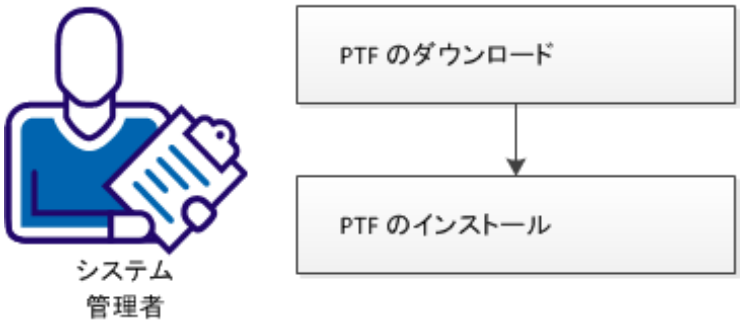
- db_datareader 役割メンバシップ
- db_datawriter 役割メンバシップ
- EXECUTE 権限
- db_owner 役割メンバシップ

アップグレードが正常に実行された後は、db_owner 役割メンバシップをデータベース ユーザから削除できます。通常の操作にはこれが必要ないためです。

CA Virtual Assurance の更新方法

システム管理者の仕事には、マネージャ システムでの CA Virtual Assurance の PTF （Program Temporary Fix）の適用が含まれます。 PTF の適用には、1 つのアプリケーションで処理できる PTF のダウンロードおよびインストールが含まれます。

PTF の適用方法



次の手順に従ってください:

1. 更新を確認します (P. 49)。
2. 更新（PTF）をダウンロードして適用します (P. 49)。

更新の確認

更新をダウンロードして適用する前に、このリリースの適切な更新が入手可能かどうかを確認します。

次の手順に従ってください:

1. システム トレイの アイコンを右クリックし、［更新の確認］をクリックします。

   ツールヒントに結果が表示されます。

また、更新を自動的に確認するタイミングの設定を指定できます。

次の手順に従ってください:

1. システム トレイの アイコンを右クリックし、［設定］をクリックします。

   ［設定］ダイアログ ボックスが表示されます。

2. ダイアログ ボックスのフィールドに入力して、［OK］をクリックします。

   ［更新の確認］スケジュールが設定されます。

更新(PTF)のダウンロードおよび適用

マネージャ システム上の CA Virtual Assurance を最新にしておくために PTF をダウンロードして適用します。

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 Virtual Assurance］に移動し、［CA Virtual Assurance の更新］をクリックします。

   ［更新： CA Virtual Assurance］ウィンドウが表示されます。

2. ［適用可能］ページを開きます。

   このリリースに適用可能な PTF が一覧表示されます。

3. 必要な PTF を選択し、［選択した更新をダウンロード］をクリックして［ダウンロードした更新をすべて適用］をクリックします。

   更新ユーティリティによって、%INSTALL_PATH%¥*productname*¥CAPTFS ディレクトリに PTF がダウンロードされ、適用プロセスが開始されます。適用の進捗状況ダイアログ ボックスにステータスが表示されます。

4. PTF が正常に適用されたら、適用の進捗状況ダイアログ ボックスを終了します。

   適用した PTF は、［更新： CA Virtual Assurance］ウィンドウの［適用済み］ページに一覧表示されます。

5. ［終了］をクリックします。

エージェントの展開

CA Virtual Assurance 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。

CA Virtual Assurance には、以下のベース展開パッケージが用意されています。

- SystemEDGE Agent Core
- SystemEDGE Advanced Encryption
- CA Citrix XenServer AIM
- SystemEDGE リモート モニタリング AIM
- SystemEDGE サービス レスポンス モニタ AIM
- CA Systems Performance LiteAgent
- CA IBM LPAR AIM
- CA IBM High Availability Cluster Multiprocessing AIM
- CA KVM AIM （CA Server Automation には適用できません）
- CA Cisco UCS AIM
- CA Microsoft Hyper-V AIM
- CA Microsoft Cluster Service Support AIM
- CA Solaris Zones AIM
- CA VMware vCenter Server AIM
- CA VMware vCloud AIM
- CA Exchange Server および Active Directory 用 AIM

CA Virtual Assurance は、以下の SystemEDGE 展開シナリオをサポートします。

- SystemEDGE エージェントがまだ存在しないシステムに SystemEDGE リリース 5.7.1 エージェントを展開できます。
- SystemEDGE 4.3 エージェントが存在するシステムに SystemEDGE リリース 5.7.1 エージェントを展開できます。 展開すると、既存のエージェントがリリース 5.7.1 に自動的にアップグレードされます。
- 個々のシステムに対する設定変更または設定テンプレートによる設定変更を行うことができます。 後者のオプションでは、変更を既存の管理対象 SystemEDGE エージェントまたは管理対象 SystemEDGE エージェントのグループに展開できます。

注: 展開機能の詳細については、*CA Virtual Assurance のオンライン ヘルプ* および「管理ガイド」を参照してください。

CA Virtual Assurance は、以下の SystemEDGE 展開シナリオをサポート*しません*。

- SystemEDGE 5.0.0 より古いバージョンのエージェントは展開できません。
- SystemEDGE エージェントを CA Virtual Assurance マネージャ システム上に展開することはできません。 エージェントは CA Virtual Assurance マネージャによって自動的にインストールされます。

注: 展開のサポートの詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

展開ジョブの作成

リモート展開を通じて CA Virtual Assurance マネージャからサポートする AIX、HP-UX、Linux、Solaris、または Windows の各システムには、SystemEDGE および AIM をインストールできます。

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 Virtual Assurance 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。

リモート展開の詳細については、「CA Virtual Assurance 管理ガイド」を参照してください。

エージェントの個別インストール

このセクションでは、CA Virtual Assurance エージェントを管理対象ノードにインストールするためのコンポーネントと手順について詳しく説明します。

SystemEDGE コンポーネントの依存関係

CA Virtual Assurance は、SystemEDGE と適切な Application Insight Module（AIM）を組み合わせて使用することで、物理環境と仮想環境を管理します。 AIM は、このエージェントの機能範囲を拡張する SystemEDGE プラグインです。

使用できる AIM は以下のとおりです。

- Active Directory および Exchange Server 用の AIM （Windows）
- Cisco UCS 用の AIM （Windows）
- Citrix XenDesktop 用の AIM （Windows）
- Citrix XenServer 用の AIM （Windows）
- Huawei GalaX 用の AIM （Windows）
- IBM LPAR 用の AIM （Windows）
- IBM PowerHA 用の AIM （Windows）
- KVM 用の AIM （Windows、Linux）
- Microsoft Hyper-V 用の AIM （Windows）
- Microsoft Cluster Service サポート用の AIM （Windows）
- リモート モニタリング用の AIM （Windows）
- サービス レスポンス モニタリング用の AIM （Windows、UNIX、Linux）
- Oracle Solaris ゾーン用の AIM （Windows）
- VMware Infrastructure または vSphere を管理するための VMware vCenter Server 用の AIM （Windows）
- VMware vCloud 用の AIM （Windows）

注: プラットフォームの詳細については、「リリース ノート」を参照してください。

これらの AIM は、SystemEDGE および Advanced Encryption がインストールされているシステムでのみ使用します。 CA Virtual Assurance はそのようなシステムを検出し、インストール済みコンポーネントの機能範囲に基づいてそれらを管理します。

SystemEDGE は、以下のオペレーティング システムで実行されます。

- AIX
- HP-UX
- Linux
- Solaris x86
- Solaris SPARC
- Windows

注: グラフィカル ユーザ インターフェースからエージェントをインストールするときに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した場合、エージェントが正しく機能しません。

CA Virtual Assurance マネージャ インストーラによる SystemEDGE のインストール

CA Virtual Assurance マネージャ インストーラを使用すると、SystemEDGE セットアップ プログラムを個別に実行しなくても SystemEDGE をインストールできます。 SystemEDGE に対して CA Virtual Assurance マネージャ インストーラを使用する場合は、構成マネージャ ホスト名に関する以下のデフォルト動作を考慮する必要があります。

- 標準インストールでは、SystemEDGE の構成マネージャ ホスト名が localhost に設定されます。
- カスタム インストールで、配布サーバと同じシステムに SystemEDGE をインストールする場合、SystemEDGE の構成マネージャ ホスト名は localhost に設定されます。
- カスタム インストールで、配布サーバのないシステムに SystemEDGE をインストールする場合、SystemEDGE の構成マネージャ ホスト名はアスタリスク（*）に設定されます。 アスタリスクは、このシステムを検出する最初の CA Virtual Assurance マネージャが SystemEDGE の構成マネージャ ホストであることを指定します。

SystemEDGE および AIM を含むリモート サーバのセットアップおよび管理を行う場合は、リモート展開とポリシー設定を使用することをお勧めします。 リモート展開では、展開パッケージの作成プロセスを示します。パッケージが展開されるスケジュール、展開先サーバ（Windows、Linux、UNIX）のリストを指定できます。 ポリシー設定では、構成マネージャ ホスト名の設定に基づいて、ネットワーク内の SystemEDGE エージェントの設定を管理できます。 詳細については、「管理ガイド」およびオンライン ヘルプを参照してください。

以下の状況では、推奨される CA Virtual Assurance リモート展開方法を使用せずに、エージェントを手動でインストールする必要があります。

- リモート展開をサポートしないシステムにエージェントをインストールする。
- レガシー モードでエージェントをインストールする。
- 構成マネージャ ホスト名やその他すべての設定をセットアップ中に手動で指定する。

サポートされているバージョンのリストについては、「リリース ノート」を参照してください。

関連項目

レガシー モードでのエージェントのインストール (P. 93)

Windows システムでのインストール

このセクションでは、Windows システムに SystemEDGE を手動でインストールする方法について説明します。 対話型ウィザードを使用してインストールできます。またコマンド ラインを使用して無人でインストールすることもできます。 サポートされているすべてのハードウェア アーキテクチャごとにパッケージが用意されています。 インストーラはハードウェア アーキテクチャを検出し、適切なインストール パッケージを実行します。

以下の状況では、推奨される CA Virtual Assurance 展開方法を使用せずに、エージェントを手動でインストールする必要があります。

- リモート展開をサポートしないシステムにエージェントをインストールする。
- レガシー モードでエージェントをインストールする。

このガイド全体を通じて、*Windows* とは、サポートされているバージョンの Windows を指します。 サポートされているバージョンのリストについては、「SystemEDGE リリース ノート」を参照してください。

Windows でのエージェントのインストール

対話型ウィザードを使用して、Windows 用 SystemEDGE エージェントを手動でインストールできます。

次の手順に従ってください:

1. Administrator として Windows システムにログオンし、以下のいずれかを実行します。
   - CA Virtual Assurance インストール イメージの DVD1 で setup.hta をダブルクリックし、［CA Virtual Assurance］ダイアログ ボックスで［SystemEDGE エージェントのインストール］をクリックします。
   - DVD1¥Installers¥Windows¥Agent¥SysMan¥CA_SystemEDGE_Core フォルダを開き、ca-setup.exe をダブルクリックします。

   注: Windows Vista 以降を実行するシステムでは、非管理者としてインストールできます。オペレーティング システムによって、管理者の認証情報を使用してインストールを認可するように要求されます。

   インストール ウィザードが起動します。 インストーラがシステムのハードウェア アーキテクチャを検出し、適切なバージョンのインストール パッケージを実行します。

2. ［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。

3. 使用許諾契約を読み、下部までスクロールします。［使用許諾契約書に同意します］を選択し、［次へ］をクリックします。

   ［インストール タイプ］ページが表示されます。

4. ［標準］または［カスタム］を選択し、［次へ］をクリックします。

   注: 以下のプロシージャではカスタム インストールについて説明します。［標準］を選択して［次へ］をクリックすると、［設定の確認］ページが表示されます。

   ［デスティネーション場所］ダイアログ ボックスが表示されます。

5. インストール場所およびデータ ディレクトリとしてデフォルトを受け入れるか、参照して選択し、［次へ］をクリックします。手順 9 に進みます。別の場所を指定する場合は、［詳細］をクリックし、手順 8 に進みます。

   デスティネーション場所

   エージェントをインストールする場所を指定します。デフォルトでは、インストール ディレクトリは *Install_Path*¥SystemEDGE です。また、ランタイム プログラム データは config サブディレクトリに保存されます。その他のパラメータを指定するには、［詳細］をクリックします。

   注: 以前のバージョンのエージェントがすでにインストールされているシステムにエージェントをインストールする場合、インストーラは既存のエージェントのインストール ディレクトリを選択します。

   ［詳細］ダイアログ ボックスを省略すると、［構成マネージャ設定］ダイアログ ボックスが表示されます。

6. ［詳細なデスティネーション場所］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

   SystemEDGE バイナリ パス

   プログラム バイナリおよびドキュメント用のディレクトリを指定します。

   SystemEDGE データ パス

   ランタイム プログラム データ用のディレクトリを指定します。

   CA 共有コンポーネント パス

   CA 共有コンポーネント用のディレクトリを指定します。いずれかの CA ソフトウェアによって設定されると、このディレクトリは変更できません。また、ユーザ インターフェース内の対応するフィールドは無効になります。

   ［構成マネージャ設定］ダイアログ ボックスが表示されます。

7. 次のフィールドの入力を完了し、［次へ］をクリックします。

   構成マネージャ ホスト名

   このエージェントを管理する構成マネージャのホスト名を指定します。CA Virtual Assurance が実行されるシステムからこのエージェントを設定できるようにするために、このパラメータの値を入力します。 アスタリスク（*）を入力すると、エージェント システムを最初に検出したマネージャが、このパラメータに設定されます。

   デフォルトの設定ポリシー名

   エージェントが使用する、CA Virtual Assurance マネージャによって保持される設定ポリシー ファイルの名前を指定します。 このパラメータの値を入力して、マネージャからの既存の設定ファイルに従って SystemEDGE を設定します。

   システム上でネイティブ Microsoft SNMP エージェントが実行されていることをインストーラが検知すると、以下の［ネイティブ SNMP エージェント オプション］ダイアログ ボックスが表示されます。

8. SNMP（Simple Network Management Protocol）がシステムにインストールされている場合は、以下のいずれかのオプションを選択して、［次へ］をクリックします。

   既存の SNMP エージェントのデフォルト

   ネイティブ SNMP エージェントから継承されるデフォルトの設定を使用するかどうかを指定します。 ネイティブ SNMP エージェントとは異なるコミュニティ文字列およびトラップ先を使用する場合は、このチェック ボックスをオフにしておきます。

   ネイティブ SNMP エージェントの無効化

   ネイティブ SNMP エージェントを停止して無効にするかどうかを指定します。 ネイティブ SNMP エージェントを有効にしておく場合は、別のポート上で SystemEDGE を実行します。

9. 次のフィールドの入力を完了し、［次へ］をクリックします。

   SNMP のポート番号

   SystemEDGE エージェントを実行するポートを指定します。

   デフォルト： 161

   重要: このポート番号は、SystemEDGE エージェント専用にします。 ほかのアプリケーションがこのポート番号を使用している場合、インストールは失敗します。 ネイティブ SNMP エージェントがすでにデフォルト ポートを使用している場合は、たとえば 1691 や 6665 など、別のポートを指定します。

   ［SNMP システム情報］ダイアログ ボックスが表示されます。

10. 次のフィールドの入力を完了し、［次へ］をクリックします。

    システムの説明

    システムに関する情報（システム名など）を指定します。この情報は、sysDescr MIB-II オブジェクトに入力されます。

    システムの場所

    システムの場所を指定します。この値は、sysLocation MIB-II オブジェクトに入力されます。

    システム担当者

    システム担当者の情報を指定します。この情報は、sysContact MIB-II オブジェクトに入力されます。

    ［SNMP コミュニティ設定］ダイアログ ボックスが表示されます。

11. 以下のフィールドに入力し、［次へ］をクリックします。手順 13 に進みます。 複数のコミュニティ文字列を指定する場合は、［詳細］をクリックして、手順 12 に進みます。

    読み取り専用コミュニティ

    SNMP 読み取り専用コミュニティ文字列を指定します。

    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指定します。

    ［詳細］ダイアログ ボックスを省略すると、［SNMP トラップ設定］ダイアログ ボックスが表示されます。

12. ［SNMP コミュニティ設定 - 詳細］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

    読み取り専用コミュニティ

    SNMP 読み取り専用コミュニティ文字列を指定します。 複数のコミュニティを指定する場合は、セミコロンで区切ります（たとえば、public1; public2）。また、アクセスを制限するために、各コミュニティに対して IP アドレスのリストを含めることができます（たとえば、public 1.2.3.4）。

    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指定します。 複数のコミュニティを指定する場合は、セミコロンで区切ります（たとえば、rwcomm1; rwcomm2）。 また、アクセスを制限するために、各コミュニティに対してスペースで区切られた IP アドレスのリストを含めることができます（たとえば、rwcomm1 1.2.3.4）。読み取り/書き込みコミュニティは、いくつかの AIM（たとえば、RM）の正しい操作、およびいくつかのリモート用途（たとえば、モニタの作成）を行うために必要です。

    ［SNMP トラップ設定］ダイアログ ボックスが表示されます。

13. 以下のフィールドに入力し、［次へ］をクリックします。手順 15 に進みます。 複数のトラップ先を指定する場合は、［詳細］をクリックして、手順 14 に進みます。

    トラップ コミュニティ文字列

    送信されたトラップ メッセージ内のエンコードされた SNMP コミュニティを指定します。

    デフォルト： public

    デスティネーション ホスト

    トラップ メッセージのデスティネーションを指定します。

    デフォルト： ［構成マネージャ設定］ダイアログ ボックスで設定される *構成マネージャ ホスト名*。

    ポート番号

    トラップ メッセージが送信されるポートを指定します。

    デフォルト： 162

    ［詳細］ダイアログ ボックスを省略すると、［その他の設定］ダイアログ ボックスが表示されます。

14. ［SNMP トラップ設定 - 詳細］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

    トラップ設定

    1 つ以上のトラップ先を指定します。 複数のエントリをセミコロンで区切って指定できます（たとえば、public server1; public server2 1162）。

    ［その他の設定］ダイアログ ボックスが表示されます。

15. 以下のフィールドに入力し、［次へ］をクリックします。

    インストール後に開始

    エージェントがインストールの最後に開始されるかどうかを指定します。

    インストール ドキュメント

    ドキュメントをインストールするかどうかを指定します。

    ［設定の確認］ページが表示されます。

16. インストール設定を確認し、［インストール］をクリックします。

    インストールが終了すると、［インストールが完了しました］ページが表示されます。

17. ［終了］をクリックします。

    インストールは終了です。

コマンド ラインを使用した Windows へのエージェントのインストール

コマンド ライン バージョンのインストーラを使用して、SystemEDGE Windows パッケージをインストールできます。 コマンド ラインからインストールするときは、パラメータを使用して各種のインストール プロパティを設定します。 コマンド ラインから以下を行うことができます。

- インストール パラメータを事前に入力して（または入力せずに）インストール ウィザードを開始する
- インストール パラメータを指定して、対話式ウィザードなしでインストーラを実行する

以下の手順では、この 2 番目のシナリオ（コマンド ラインからの無人インストールの実行）について説明します。

次の手順に従ってください:

1. Windows システムに管理者としてログインします。

   注: Windows Vista 以降を実行しているシステムでは、管理者以外の権限でもインストールできます。その場合、管理者の認証情報でインストールを許可するようにオペレーティング システムから促されます。

2. コマンド プロンプトを開き、DVD1¥Installers¥Windows¥Agent¥SysMan¥CA_SystemEDGE_Core フォルダに移動して、以下の必須パラメータを入力します（手順 3 を完了するまで、コマンドを実行**しないで**ください）。

   ```
   ca-setup CA_SETUP_MODE=UNATTENDED EULA_ACCEPTED="YES" [parameter]
   ```

   注: インストール パラメータのヘルプを参照するには、ca-setup -? をコマンド プロンプトで入力してください。

   CA_SETUP_MODE

   インストール モードを指定します。 サイレント モードでインストールを実行するには、このパラメータを UNATTENDED に設定します。 このパラメータを省略すると、コマンド実行後に、インストール ウィザードはあらかじめ指定されたパラメータ値を使用して開始されます。

   EULA_ACCEPTED

   使用許諾契約を読み取り、使用許諾契約に同意するかどうかを指定します。インストール モードを UNATTENDED に設定している場合に、このパラメータを省略するか、**YES** 以外に設定すると、インストールは失敗します。 このパラメータは、対話式インストールでは不要です。

3. 必要に応じてオプションのパラメータを追加し、コマンドを実行します。

   注: 以下のオプションのパラメータを省略する場合は、値は必要ありません。

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   インストール メッセージをログ記録する場所およびファイル名を指定します。

   CA_SETUP_VERBOSE

   「yes」に設定すると、インストーラが詳細モードになります。 詳細モードでは、インストール ログ ファイルにより詳細な情報がログ記録されます。

CASE_INSTALLDIR

SystemEDGE のインストール ディレクトリを指定します。このディレクトリには、AIM、Advanced Encryption など、SystemEDGE 関連のものすべてが含まれており、コア インストーラによって設定された後は、変更されることはありません。

注: デフォルト以外のインストール ディレクトリを定義すると、インストーラは、SystemEDGE サブフォルダを作成せずに、指定されたディレクトリにエージェント ファイルを直接インストールします。

デフォルト： C:¥Program Files¥CA¥SystemEDGE

CASE_PUBDATADIR

SystemEDGE データ ディレクトリを指定します。すべての設定は、このディレクトリで実行され、動的なデータが保存されます（このドキュメント内では、SystemEDGE データ ディレクトリを変数 CASYSEDGE_DATA と呼んでいます）。 エージェントの設定ファイルは、SNMP_PORT パラメータの値に基づいて、ポートに固有のサブディレクトリ内に配置されます。

デフォルト： C:¥Documents and Settings¥All Users¥Application Data¥CA¥SystemEDGE （Windows XP および 2003）、C:¥Users¥Public¥CA¥SystemEDGE （Windows Vista および 2008）

CASE_SNMP_PORT

SystemEDGE によって使用されるポートを指定します。 この値は、CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承することもできます。CASE_SNMP_PORT パラメータを使用してポートを指定すると、継承された値が上書きされます。 このポートは一意である必要があります。一意でないと、インストールは失敗します。 デフォルトポートである 161 がネイティブ SNMP エージェントによってすでに使用されている場合（そして、このエージェントを無効にする計画がない場合）、たとえば 1691 や 6665 など、別の一意のポートを指定する必要があります。

デフォルト： 161

CASE_SNMP_SYS_DESC

sysDescr MIB-II オブジェクトに入力されるシステムについての情報（システム名など）を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。CASE_SNMP_SYS_DESC パラメータを使用して説明を指定した場合は、継承された値が上書きされます。

CASE_SNMP_SYS_LOC

sysLocation MIB-II オブジェクトに入力されるシステムの場所を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。CASE_SNMP_SYS_LOC パラメータを使用して場所を指定した場合は、継承された値が上書きされます。

CASE_SNMP_SYS_CONTACT

sysContact MIB-II オブジェクトに入力されるシステム担当者情報を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。CASE_SNMP_SYS_CONTACT パラメータを使用して担当者を指定した場合は、継承された値が上書きされます。

CASE_SNMP_READ_COMMUNITY

エージェントへ GET 要求を送信できる SNMP 読み取りコミュニティの名前を指定します。 セミコロンで区切ることにより、複数のコミュニティを指定できます（たとえば public1; public2）。また、コミュニティごとにスペースで区切った IP アドレス リストを含めて、アクセスを制限できます（たとえば public 1.2.3.4）。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。
CASE_SNMP_READ_COMMUNITY パラメータを使用して読み取りコミュニティを指定した場合は、継承された値が上書きされます。

デフォルト： snmp_public （新規インストールで（アップグレードは除く）、読み取り/書き込みコミュニティが指定されていない場合のみ有効）

CASE_SNMP_READ_ALLOWED_MANAGERS

SNMP_READ_COMMUNITY を持つエージェントにクエリすることを許された SNMP マネージャの IP アドレスまたはホスト名をスペースで区切って指定します。 リストを指定する場合、SNMP_READ_COMMUNITY には、1 つの語（SNMP コミュニティ）のみが含まれる必要があります。

CASE_SNMP_WRITE_COMMUNITY

エージェントへ GET 要求と SET 要求を送信できる SNMP 書き込みコミュニティの名前を指定します。 セミコロンで区切ることにより、複数のコミュニティを指定できます（たとえば rwcomm1;rwcomm2）。また、コミュニティごとにスペースで区切った IP アドレス リストを含めて、アクセスを制限できます（たとえば rwcomm1 1.2.3.4）。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。
CASE_SNMP_WRITE_COMMUNITY パラメータを使用して書き込みコミュニティを指定した場合は、継承された値が上書きされます。

CASE_SNMP_WRITE_ALLOWED_MANAGERS

SNMP_WRITE_COMMUNITY を持つエージェントにクエリすることを許された SNMP マネージャの IP アドレスまたはホスト名をスペースで区切って指定します。 リストを指定する場合、SNMP_WRITE_COMMUNITY には、1 つの語（SNMP コミュニティ）のみが含まれる必要があります。

CASE_SNMP_TRAP_COMMUNITY

SNMP トラップ コミュニティおよびトラップ先アドレスを指定します。セミコロン（;）で区切ることにより複数のトラップ コミュニティ設定を指定できます。 このパラメータの値は、CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承することもできます。CASE_SNMP_TRAP_COMMUNITY パラメータを使用してトラップ コミュニティを指定すると、継承された値が上書きされます。 以下の値がこのパラメータに必要です。

- コミュニティ名
- トラップの送信先のデスティネーション アドレス

以下の値は、このパラメータのオプションです。

- トラップの送信先のポート番号
- トラップ ソースのエンコーディング オプション
- トラップ ソースのホスト名

トラップ コミュニティ設定の構文：

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

例：

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

CASE_SNMP_TRAP_DESTINATION

トラップの送信先のホスト名または IP アドレスを指定します。 指定する場合、SNMP_TRAP_COMMUNITY には、1 つの語（SNMP コミュニティ）のみが含まれる必要があり、また SNMP_TRAP_PORT を指定する必要があります。

CASE_SNMP_TRAP_PORT

トラップの送信先のデスティネーション ポート番号を指定します。指定する場合、SNMP_TRAP_COMMUNITY には、1 つの語（SNMP コミュニティ）のみが含まれる必要があり、また SNMP_TRAP_DESTINATION を指定する必要があります。

CASE_DISABLE_NATIVE_SNMP

ネイティブ SNMP エージェントを停止して無効にするかどうかを指定します。

デフォルト： no

CASE_DEFAULT_FROM_NATIVE_SNMP

ネイティブ SNMP エージェントのデフォルトの SNMP 設定を使用するかどうかを指定します。

デフォルト： no

CASE_MANAGER_HOSTNAME

このエージェントを管理する構成マネージャのホスト名を指定します。 このパラメータに値を入力すると、指定したマネージャからこのエージェントを設定できます。 アスタリスク（*）を入力すると、エージェント システムを最初に検出したマネージャが受け入れられます。 このマネージャは、エージェントの設定をフル コントロールできるようになります。 デフォルトでは、マネージャ ホストは入力（使用）されず、エージェントは管理対象外モードで実行されます。

CASE_MANAGER_POLICY_NAME

エージェントで使用する必要がある、構成マネージャのポリシー ファイルの名前を指定します。このパラメータに値を入力すると、マネージャの既存の設定ファイルに従って SystemEDGE が設定されます。 デフォルトでは、エージェントはインストール済みのポリシー ファイルを使用します。

CASE_START_AFTER_INSTALL

インストールの完了後にエージェントを自動的に開始するかどうかを指定します。

デフォルト： yes

CASE_INSTALL_DOCS

SystemEDGE のドキュメントをエージェントと同時にインストールするかどうかを指定します。

デフォルト： yes

CASE_LEGACY_MODE

エージェントをレガシー モードでインストールするかどうかを指定します。 レガシー モードでは、ベース エージェントのみがインストールされ、CA Virtual Assurance でのエージェントの使用を円滑にする要素は、まったくインストールされません。 CA Virtual Assurance でエージェントを使用しない場合は、レガシー モードを使用してインストールしてください。

エージェントを管理対象モードに変更するには、エージェントを再インストールまたはアップグレードし、CASE_LEGACY_MODE=no と指定します。

デフォルト： no

コマンド ラインで、コマンドおよびすべての必須パラメータおよび値を入力します。 Enter キーを押してインストールを開始します。 インストーラは、オペレーティング システムのハードウェア アーキテクチャを検出し、インストーラの適切なバージョンを実行します。

注: ユーザがインストールに関する使用許諾に同意しない場合、インストールは失敗します。

インストールを確認するには、［Windows サービス］ダイアログ ボックスに CA SystemEDGE サービスがあるかどうかを確認します。または、インストール ディレクトリ内に SystemEDGE ファイル、あるいは［プログラムの追加と削除］ダイアログ ボックス内に CA SystemEDGE コアがあるかどうかを確認します。インストール ログ ファイルを指定した場合は、そのファイルをチェックしてインストールの成功を確認することもできます。

注: Windows Vista 以降を実行するシステムにインストールする場合は、SystemEDGE インストーラが「Microsoft Visual C++ 2005 再頒布可能パッケージ」を自動的にインストールします。 このパッケージがインストールされていないと、SystemEDGE は機能しません。「Microsoft Visual C++ 2005 再頒布可能パッケージ」をインストールするには、表示された使用許諾契約に同意する必要があります。 「Microsoft Visual C++ 2005 再頒布可能パッケージ」の使用許諾契約は、対話式の SystemEDGE インストーラには表示されません。

UNIX および Linux システムでのインストール

ここでは、UNIX および LINUX のシステム上で SystemEDGE エージェントを手動でインストールする方法について説明します。 対話型ウィザードを使用してインストールできます。またコマンド ラインを使用して無人でインストールすることもできます。 対話型ウィザードはテキスト モードでコンソール上に表示されます。Xserver が利用でき、DISPLAY 環境が正しく設定されている場合は、グラフィカルなアプリケーションとして表示されます。

以下の状況では、推奨される CA Virtual Assurance 展開方法を使用せずに、エージェントを手動でインストールする必要があります。

- リモート展開をサポートしないシステムにエージェントをインストールする。
- レガシー モードでエージェントをインストールする。

サポートされる UNIX および LINUX のプラットフォームおよびバージョンの詳細については、「*SystemEDGE リリース ノート*」を参照してください。

関連項目

レガシー モードでのエージェントのインストール (P. 93)

UNIX システムおよび LINUX システムでのエージェントのインストール

対話式ウィザードを使用して、UNIX および Linux に手動で SystemEDGE エージェントをインストールできます。

注:

- このドキュメントでは、インストール ディレクトリを CASYSEDGE と表し、データ ディレクトリを CASYSEDGE_DATA と表します。
- インストール プログラムは、/etc/profile 内のシステム環境設定を変更しません。

次の手順に従ってください:

1. root ユーザとしてシステムにログインし、DVD2 をマウントします。
2. 端末コンソールを開き、Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core ディレクトリに移動します（使用中のオペレーティング システムに対応する *platform* ディレクトリを選択します）。
3. このディレクトリから、以下のようにインストーラを実行します。

   ```
   sh ca-setup.sh
   ```

   インストーラの［はじめに］ページが表示されます。
4. ［次へ］をクリックします。

   ［使用許諾契約書］ページが表示されます。
5. 使用許諾契約を読み、［使用許諾契約書に同意します］を選択します。［次へ］をクリックします。

   ［インストール タイプ］ページが表示されます。
6. ［標準］または［カスタム］を選択し、［次へ］をクリックします。

   注: 以下の手順では、カスタム インストールについて説明します。［標準］を選択した場合は、［次へ］をクリックすると［設定の確認］ページが表示されます。

   ［デスティネーション場所］ダイアログ ボックスが表示されます。

7. インストール場所およびデータ ディレクトリとしてデフォルトを受け入れるか、参照して選択し、［次へ］をクリックします。手順 9 に進みます。 別の場所を指定する場合は、［詳細］をクリックして手順 8 に進みます。

   デスティネーション場所

   エージェントをインストールする場所を指定します。 デフォルトでは、インストール ディレクトリは /opt/CA/SystemEDGE であり、ランタイム プログラム データは config サブディレクトリに保存されます。 その他のパラメータを指定するには、［詳細］をクリックします。

   注: 旧バージョンのエージェントがすでにインストールされているシステムにエージェントをインストールする場合は、インストーラが既存のエージェントのインストール ディレクトリを自動的に選択します。

   ［詳細］ダイアログ ボックスを省略すると、［構成マネージャ設定］ダイアログ ボックスが表示されます。

8. ［詳細なデスティネーション場所］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

   SystemEDGE バイナリ パス

   プログラム バイナリおよびドキュメント用のディレクトリを指定します。

   SystemEDGE データ パス

   ランタイム プログラム データ用のディレクトリを指定します。

   CA 共有コンポーネント パス

   CA 共有コンポーネント用のディレクトリを指定します。 いずれかの CA ソフトウェアによって設定されると、このディレクトリは変更できません。また、ユーザ インターフェース内の対応するフィールドは無効になります。

   ［構成マネージャ設定］ダイアログ ボックスが表示されます。

9. 次のフィールドの入力を完了し、［次へ］をクリックします。

構成マネージャ ホスト名

このエージェントを管理する構成マネージャのホスト名を指定します。CA Virtual Assurance が実行されるシステムからこのエージェントを設定できるようにするために、このパラメータの値を入力します。 アスタリスク（*）を入力すると、エージェント システムを最初に検出したマネージャが、このパラメータに設定されます。

デフォルトの設定ポリシー名

エージェントが使用するポリシー ファイル（CA Virtual Assurance マネージャによって管理されるファイル）の名前を指定します。 このパラメータの値を入力して、マネージャからの既存の設定ファイルに従って SystemEDGE を設定します。

インストーラがシステム上で実行されているネイティブ SNMP エージェントを検出すると、［ネイティブ SNMP エージェント オプション］ダイアログ ボックスが表示されます。

10. 次のフィールドの入力を完了し、［次へ］をクリックします。

既存の SNMP エージェントのデフォルト

ネイティブ SNMP エージェントから継承されるデフォルトの設定を使用するかどうかを指定します。 ネイティブ SNMP エージェントとは異なるコミュニティ文字列およびトラップ先を使用する場合は、このチェック ボックスをオフにしておきます。

ネイティブ SNMP エージェントの無効化

ネイティブ SNMP エージェントを停止して無効にするかどうかを指定します。 ネイティブ SNMP エージェントを有効にしておく場合は、別のポート上で SystemEDGE を実行します。

11. 次のフィールドの入力を完了し、［次へ］をクリックします。

    SNMP のポート番号

    SystemEDGE エージェントを実行するポートを指定します。他のアプリケーションが使用していないポートを指定してください。他のアプリケーションがこのポートを使用していると、インストールは失敗します。 ネイティブ SNMP エージェントがすでにデフォルト ポートを使用している場合は、たとえば 1691 や 6665 など、別のポートを指定します。

    デフォルト： 161

    ［SNMP システム情報］ダイアログ ボックスが表示されます。

12. 次のフィールドの入力を完了し、［次へ］をクリックします。

    システムの説明

    システムに関する情報（システム名など）を指定します。この情報は、sysDescr MIB-II オブジェクトに入力されます。

    システムの場所

    システムの場所を指定します。この値は、sysLocation MIB-II オブジェクトに入力されます。

    システム担当者

    システム担当者の情報を指定します。この情報は、sysContact MIB-II オブジェクトに入力されます。

    ［SNMP コミュニティ設定］ダイアログ ボックスが表示されます。

13. 以下のフィールドに入力し、［次へ］をクリックします。手順 15 に進みます。 複数のコミュニティ文字列を指定する場合は、［詳細］をクリックして手順 14 に進みます。

    読み取り専用コミュニティ

    SNMP 読み取り専用コミュニティ文字列を指定します。

    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指定します。

    ［詳細］ダイアログ ボックスを省略すると、［SNMP トラップ設定］ダイアログ ボックスが表示されます。

14. ［SNMP コミュニティ設定 - 詳細］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

読み取り専用コミュニティ

SNMP 読み取り専用コミュニティ文字列を指定します。 個々のコミュニティをセミコロンで区切ることによって、複数のコミュニティを指定できます（たとえば、public1;public2）。 また、アクセスを制限するために、各コミュニティに対して IP アドレスのリストを含めることができます（たとえば、public 1.2.3.4）。

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指定します。 個々のコミュニティをセミコロンで区切ることによって、複数のコミュニティを指定できます（たとえば、rwcomm1;rwcomm2）。 また、アクセスを制限するために、各コミュニティに対してスペースで区切られた IP アドレスのリストを含めることができます（たとえば、rwcomm1 1.2.3.4）。 読み取り/書き込みコミュニティは、いくつかの AIM （たとえば、RM）の正しい操作、およびいくつかのリモート用途（たとえば、モニタの作成）を行うために必要です。

［SNMP トラップ設定］ダイアログ ボックスが表示されます。

15. 以下のフィールドに入力し、［次へ］をクリックして手順 17 に進みます。 複数のトラップ デスティネーションを指定する場合は、［詳細］をクリックして手順 16 に進みます。

    トラップ コミュニティ文字列

    送信されたトラップ メッセージ内のエンコードされた SNMP コミュニティを指定します。

    デフォルト： public

    デスティネーション ホスト

    トラップ メッセージのデスティネーションを指定します。

    デフォルト： ［構成マネージャ設定］ダイアログ ボックスで設定される *構成マネージャ ホスト名*。

    ポート番号

    トラップ メッセージが送信されるポートを指定します。

    デフォルト： 162

    ［詳細］ダイアログ ボックスをスキップすると、［権限分離ユーザ］ダイアログ ボックスが表示されます。

16. ［SNMP トラップ設定 - 詳細］ダイアログ ボックスで以下のフィールドに入力し、［次へ］をクリックします。

    トラップ設定

    1 つ以上のトラップ先を指定します。 複数のエントリをセミコロンで区切って指定できます（たとえば、public server1;public server2 1162）。

    ［権限分離ユーザ］ダイアログ ボックスが表示されます。

17. 以下のフィールドに入力して、［次へ］をクリックします。

    ユーザ名

    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（UNIX のみ）。 このエージェントはまた、有効なグループとして、このユーザのデフォルト グループを使用します。

    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。

    ［その他の設定］ダイアログ ボックスが表示されます。

18. 以下のフィールドに入力し、［次へ］をクリックします。

    インストール後に開始

    エージェントがインストールの最後に開始されるかどうかを指定します。

    インストール ドキュメント

    ドキュメントをインストールするかどうかを指定します。

    ［設定の確認］ページが表示されます。

19. インストール設定を確認し、［インストール］をクリックします。

    インストールが終了すると、［インストールが完了しました］ページが表示されます。

20. ［終了］をクリックします。

    インストールは終了です。

64 ビット版 Linux のリリースでの SystemEDGE インストールが失敗する

症状:

64 ビット版 Linux のリリースに SystemEDGE をインストールすると、インストールが失敗します。

解決方法:

64 ビット版 Linux のリリースに SystemEDGE を実行しインストールするには、必要な 32 ビット ライブラリをインストールします。

- Red Hat または SuSE のディストリビューション上で有効：

  ```
  yum install glibc.i686
  ```

- Debian ディストリビューション上で有効：

  ```
  apt-get install ia32-libs
  ```

コマンド ラインを使用した UNIX へのエージェントのインストール

インストーラのコマンド ライン バージョンを使用して SystemEDGE UNIX パッケージをインストールできます。 コマンド ラインからインストールするときは、パラメータを使用して各種のインストール プロパティを設定します。 コマンド ラインから以下を行うことができます。

- インストール パラメータを事前に入力して（または入力せずに）インストール ウィザードを開始する
- インストール パラメータを指定して、対話式ウィザードなしでインストーラを実行する

注:

- UNIX では、応答ファイルの自動作成によるサイレント インストールの実行はサポートされません。 ただし、応答ファイルを手動で作成して無人インストールに使用することはできます。
- インストール プログラムは、/etc/profile 内のシステム環境設定を変更しません。

以下の手順では、この 2 番目のシナリオ（コマンド ラインからの無人インストールの実行）について説明します。

次の手順に従ってください:

1. root としてシステムにログインします。
2. DVD2/Installers/*platform*/Agent/SysMan/CA_SystemEDGE_Core ディレクトリに移動します（使用中のオペレーティング システムに対応する platform ディレクトリを選択します）。次に、以下の必須パラメータを入力します（手順 3 を完了するまでコマンドを**実行しないでください**）。

   ```
   sh ca-setup.sh CA_SETUP_MODE="UNATTENDED" EULA_ACCEPTED="yes" [parameter]
   ```

   注: インストール パラメータのヘルプを参照するには、ca-setup -? をコマンド プロンプトで入力してください。

   CA_SETUP_MODE

   インストール モードを指定します。インストール ウィザードを表示せずにインストールを実行するには、このパラメータを UNATTENDED に設定します。 このパラメータを省略すると、コマンド実行後に、インストール ウィザードはあらかじめ指定されたパラメータ値を使用して開始されます。

   EULA_ACCEPTED

   使用許諾契約を読み取り、使用許諾契約に同意するかどうかを指定します。インストール モードを UNATTENDED に設定している場合に、このパラメータを省略するか、**YES** 以外に設定すると、インストールは失敗します。 このパラメータは、対話式インストールでは不要です。

3. 必要に応じてオプションのパラメータを追加し、コマンドを実行します。

   注: 以下のオプションのパラメータを省略する場合は、値は必要ありません。

   CA_SETUP_LOG_FILE
   CA_SETUP_VERBOSE
   CASE_INSTALLDIR
   CASE_PUBDATADIR
   CASE_SNMP_PORT
   CASE_SNMP_SYS_DESC
   CASE_SNMP_SYS_LOC
   CASE_SNMP_SYS_CONTACT
   CASE_SNMP_READ_COMMUNITY
   CASE_SNMP_READ_ALLOWED_MANAGERS
   CASE_SNMP_WRITE_COMMUNITY
   CASE_SNMP_WRITE_ALLOWED_MANAGERS
   CASE_SNMP_TRAP_COMMUNITY
   CASE_SNMP_TRAP_DESTINATION
   CASE_SNMP_TRAP_PORT
   CASE_DISABLE_NATIVE_SNMP
   CASE_DEFAULT_FROM_NATIVE_SNMP
   CASE_MANAGER_HOSTNAME
   CASE_MANAGER_POLICY_NAME
   CASE_PRIVSEP_USER
   CASE_START_AFTER_INSTALL
   CASE_INSTALL_DOCS
   CASE_LEGACY_MODE

   CA_SETUP_LOG_FILE

   インストール メッセージをログ記録する場所およびファイル名を指定します。 デフォルトでは、/opt/CA/installer/log/*CA_SETUP_PACKAGE_NAME*.log にメッセージが記録されます。

   CA_SETUP_VERBOSE

   「yes」に設定すると、インストーラが詳細モードになります。 詳細モードでは、インストール ログ ファイルにより詳細な情報がログ記録されます。

CASE_INSTALLDIR

SystemEDGE のインストール ディレクトリを指定します。このディレクトリには、AIM、Advanced Encryption など、SystemEDGE 関連のものすべてが含まれており、コア インストーラによって設定された後は、変更されることはありません。

注: デフォルト以外のインストール ディレクトリを定義すると、インストーラは、SystemEDGE サブフォルダを作成せずに、指定されたディレクトリにエージェント ファイルを直接インストールします。

デフォルト： /opt/CA/SystemEDGE

CASE_PUBDATADIR

SystemEDGE データ ディレクトリを指定します。すべての設定は、このディレクトリで実行され、動的なデータが保存されます（このドキュメント内では、SystemEDGE データ ディレクトリを変数 CASYSEDGE_DATA と呼んでいます）。 エージェントの設定ファイルは、SNMP_PORT パラメータの値に基づいて、ポートに固有のサブディレクトリ内に配置されます。

デフォルト： /opt/CA/SystemEDGE/config

CASE_SNMP_PORT

SystemEDGE によって使用されるポートを指定します。 この値は、CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承することもできます。CASE_SNMP_PORT パラメータを使用してポートを指定すると、継承された値が上書きされます。 このポートは一意である必要があります。一意でないと、インストールは失敗します。 デフォルトポートである 161 がネイティブ SNMP エージェントによってすでに使用されている場合（そして、このエージェントを無効にする計画がない場合）、たとえば 1691 や 6665 など、別の一意のポートを指定する必要があります。

デフォルト： 161

CASE_SNMP_SYS_DESC

sysDescr MIB-II オブジェクトに入力されるシステムについての情報（システム名など）を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。
CASE_SNMP_SYS_DESC パラメータを使用して説明を指定した場合は、継承された値が上書きされます。

CASE_SNMP_SYS_LOC

sysLocation MIB-II オブジェクトに入力されるシステムの場所を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。
CASE_SNMP_SYS_LOC パラメータを使用して場所を指定した場合は、継承された値が上書きされます。

CASE_SNMP_SYS_CONTACT

sysContact MIB-II オブジェクトに入力されるシステム担当者情報を指定します。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。CASE_SNMP_SYS_CONTACT パラメータを使用して担当者を指定した場合は、継承された値が上書きされます。

CASE_SNMP_READ_COMMUNITY

エージェントへ GET 要求を送信できる SNMP 読み取りコミュニティの名前を指定します。 セミコロンで区切ることにより、複数のコミュニティを指定できます（たとえば public1; public2）。また、コミュニティごとにスペースで区切った IP アドレス リストを含めて、アクセスを制限できます（たとえば public 1.2.3.4）。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。
CASE_SNMP_READ_COMMUNITY パラメータを使用して読み取りコミュニティを指定した場合は、継承された値が上書きされます。

デフォルト： snmp_public （新規インストールで（アップグレードは除く）、読み取り/書き込みコミュニティが指定されていない場合のみ有効）

CASE_SNMP_READ_ALLOWED_MANAGERS

CASE_SNMP_READ_COMMUNITY でエージェントへの照会を許可された SNMP マネージャの IP アドレス/ホスト名のスペース区切りリストを指定します。 これを指定する場合は、CASE_SNMP_READ_COMMUNITY に 1 つの語（SNMP コミュニティ）のみを含める必要があります。

CASE_SNMP_WRITE_COMMUNITY

エージェントへ GET 要求と SET 要求を送信できる SNMP 書き込みコミュニティの名前を指定します。 セミコロンで区切ることにより、複数のコミュニティを指定できます（たとえば rwcomm1;rwcomm2）。また、コミュニティごとにスペースで区切った IP アドレス リストを含めて、アクセスを制限できます（たとえば rwcomm1 1.2.3.4）。 この値も CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承できます。CASE_SNMP_WRITE_COMMUNITY パラメータを使用して書き込みコミュニティを指定した場合は、継承された値が上書きされます。

CASE_SNMP_WRITE_ALLOWED_MANAGERS

CASE_SNMP_WRITE_COMMUNITY でエージェントへの照会を許可された SNMP マネージャの IP アドレス/ホスト名のスペース区切りリストを指定します。 これを指定する場合は、CASE_SNMP_WRITE_COMMUNITY に 1 つの語（SNMP コミュニティ）のみを含める必要があります。

CASE_SNMP_TRAP_COMMUNITY

SNMP トラップ コミュニティおよびトラップ先アドレスを指定します。セミコロン（;）で区切ることにより複数のトラップ コミュニティ設定を指定できます。 このパラメータの値は、CASE_DEFAULT_FROM_NATIVE_SNMP パラメータを使用して、ネイティブ SNMP エージェントから継承することもできます。CASE_SNMP_TRAP_COMMUNITY パラメータを使用してトラップ コミュニティを指定すると、継承された値が上書きされます。 以下の値がこのパラメータに必要です。

- コミュニティ名
- トラップの送信先のデスティネーション アドレス

以下の値は、このパラメータのオプションです。

- トラップの送信先のポート番号
- トラップ ソースのエンコーディング オプション
- トラップ ソースのホスト名

トラップ コミュニティ設定の構文：

community-string {*ip-address*|*hostname*} [*port* [*encoding* [*source*]]]

例：

public 1.2.3.4;public 2.3.4.5 1162;trapcom 3.4.5.6 1162 100 4.5.6.7

CASE_SNMP_TRAP_DESTINATION

トラップの送信先のホスト名または IP アドレスを指定します。 これを指定する場合は、CASE_SNMP_TRAP_COMMUNITY に 1 つの語（SNMP コミュニティ）のみを含めると共に、CASE_SNMP_TRAP_PORT も指定する必要があります。

CASE_SNMP_TRAP_PORT

トラップの送信先のデスティネーション ポート番号を指定します。これを指定する場合は、CASE_SNMP_TRAP_COMMUNITY に 1 つの語（SNMP コミュニティ）のみを含めると共に、CASE_SNMP_TRAP_DESTINATION も指定する必要があります。

CASE_DISABLE_NATIVE_SNMP

ネイティブ SNMP エージェントを停止して無効にするかどうかを指定します。

デフォルト： no

CASE_DEFAULT_FROM_NATIVE_SNMP

ネイティブ SNMP エージェントのデフォルトの SNMP 設定を使用するかどうかを指定します。

デフォルト： no

CASE_MANAGER_HOSTNAME

このエージェントを管理する構成マネージャのホスト名を指定します。 このパラメータに値を入力すると、指定したマネージャからこのエージェントを設定できます。 アスタリスク（*）を入力すると、エージェント システムを最初に検出したマネージャが受け入れられます。 このマネージャは、エージェントの設定をフル コントロールできるようになります。 デフォルトでは、マネージャ ホストは入力（使用）されず、エージェントは管理対象外モードで実行されます。

CASE_MANAGER_POLICY_NAME

エージェントで使用する必要がある、構成マネージャのポリシー ファイルの名前を指定します。このパラメータに値を入力すると、マネージャの既存の設定ファイルに従って SystemEDGE が設定されます。 デフォルトでは、エージェントはインストール済みのポリシー ファイルを使用します。

CASE_START_AFTER_INSTALL

インストールが完了した後に、エージェントを自動的に開始するかどうかを指定します。 有効な値は Yes、No、PRESERVE です。 PRESERVE を使用すると、アップグレード時に、インストールを開始した時点でエージェントが実行されていた場合にのみエージェントを起動できます。

デフォルト： PRESERVE

CASE_PRIVSEP_USER

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（UNIX のみ）。 このエージェントはまた、有効なグループとして、このユーザのデフォルト グループを使用します。

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。

CASE_INSTALL_DOCS

SystemEDGE のドキュメントをエージェントと同時にインストールするかどうかを指定します。

デフォルト： yes

CASE_LEGACY_MODE

エージェントをレガシー モードでインストールするかどうかを指定します。レガシー モードでは、ベース エージェントのみがインストールされ、CA Virtual Assurance でのエージェントの使用を円滑にする要素は、まったくインストールされません。 CA Virtual Assurance でエージェントを使用しない場合は、レガシー モードを使用してインストールしてください。

エージェントを管理対象モードに変更するには、エージェントを再インストールまたはアップグレードし、CASE_LEGACY_MODE=no と指定します。

デフォルト： no

インストールが始まります。 使用許諾契約に同意しなかった場合、インストールは失敗します。

lsm のインストーラ ログ ファイルは常に /opt/CA/installer/log/$CA_SETUP_PACKAGE_NAME.log にあります。このファイルを使用して、インストールが成功したかどうかを確認できます。

インストールを確認する場合は、インストール ディレクトリに SystemEDGE のファイルがあるかどうかを確認します。

$CASYSEDGE 変数のレガシー サポート

Linux/UNIX 上のインストール プログラムは、/etc/profile 内のシステム環境設定を変更しません。 その結果、$CASYSEDGE 変数は使用できなくなりました。

使用環境で $CASYSEDGE をサポートする必要がある場合は、以下のいずれかのオプションを実行します。

- シェルで $CASYSEDGE を作成する。

  sh、ksh、または bash シェルで以下のコマンドを実行します。

  ```
  ./etc/profile.CA
  ```

  csh を使用する場合は、以下のコマンドを実行します。

  ```
  source /etc/csh_login.CA
  ```

- インストール プログラムが /etc/profile を変更し、$CASYSEDGE を作成するようにします。

  シェルを開き、以下のコマンドを入力します。

  ```
  Update_Profile=1;export Update_Profile
  sh ca-setup.sh
  ```

  csh を使用する場合は、以下のコマンドを実行します。

  ```
  setenv Update_Profile 1
  sh ca-setup.sh
  ```

  インストール プログラムは SystemEDGE をインストールし、環境内に $CASYSEDGE を作成します。

リリース 5.7.1 へのアップグレード中に、SystemEDGE インストール プログラムは既存の環境を変更しません。以前に作成された $CASYSEDGE 変数は環境内に残ります。

応答ファイルの設定と使用

ユーザ操作のないサイレント インストールを実行するための応答ファイルを作成できます。 応答ファイルの使用は、コマンド ラインに CA_SETUP_MODE=UNATTENDED を指定するのと同じ効果があります。応答ファイルを使用すると、インストールはサイレント（無人）モードになります。

インストーラは、応答ファイル内のプロパティを使用して、ユーザ入力を要求せずにエージェントをインストールします。

次の手順に従ってください:

1. 管理者または root としてコンピュータ システムにログインします。
2. 「コマンド ラインを使用した～へのエージェントのインストール」セクションで指定したパラメータに基づいて応答ファイルを作成します。応答ファイルは、以下のようなパラメータ設定で構成されるテキスト ファイルです。

   ```
   parameter1=value1
   parameter2=value2
   ...
   ```

3. *DVDdrive*¥Installers¥*OperatingSystem*¥Agent¥SysMan¥CA_SystemEDGE_Core directory ディレクトリに移動し、使用中のオペレーティング システムに従って以下のいずれかのコマンドを入力します。

   ```
   ca-setup CA_SETUP_RESPONSE_FILE="<name of the response file>"  (Windows)
   ```

   ```
   sh ca-setup.sh CA_SETUP_RESPONSE_FILE="<name of the response file>" (UNIX、Linux)
   ```

   CA_SETUP_RESPONSE_FILE

   応答ファイルのパスと名前を指定します。

   応答ファイルの設定を使用して、サイレント モードでインストールが実行されます。

レガシー モードでのエージェントのインストール

レガシー モードで SystemEDGE をインストールすると、ベース エージェントのすべての機能が得られますが、CA Virtual Assurance と組み合わせて使用するときに役立つ以下のコンポーネントは除外されます。

- CA Virtual Assurance からのリモート設定を可能にする CAM
- CA Virtual Assurance からのリモート展開を可能にする IDPrimer

CA Virtual Assurance または同様の管理アプリケーションで SystemEDGE を管理することを予定してしない場合にのみ、SystemEDGE をレガシー モードでインストールしてください。 レガシー モードでエージェントをインストールした後、CA Virtual Assurance を使用してエージェントを管理したい場合は、エージェントをアップグレードできます。

注: SystemEDGE の旧バージョンをアップグレードするときは、特に指定しない限り、完全なエージェントに自動的にアップグレードされます。

次の手順に従ってください:

1. CA_SystemEDGE_Core ディレクトリをインストール メディアからハード ディスクにコピーします。
2. CA_SystemEDGE_Core ディレクトリに移動し、ASCII エディタで ca-setup.dat を開きます。
3. ca-setup.dat を編集して、CASE_LEGACY_MODE=yes を設定します。
4. ca-setup.dat を保存します。
5. 「エージェントの Windows へのインストール (P. 59)」または「エージェントの UNIX および Linux システムへのインストール (P. 74)」の説明に従ってインストールを実行します。
6. インストールを完了します。

コマンド ラインからレガシー モードでエージェントをインストールするには、ca-setup コマンドに以下のパラメータを追加します。

```
CASE_LEGACY_MODE="yes"
```

AIM のインストール

AIM を SystemEDGE 上にインストールする場合は、以下のガイドラインを考慮してください。

- SRM AIM、RM AIM、MSCS AIM、または仮想環境管理用の AIM は、Advanced Encryption および SystemEDGE に依存します。
- Advanced Encryption は SystemEDGE に依存します。

このような依存関係に基づくインストール順序は以下のとおりです。

1. SystemEDGE コア
2. Advanced Encryption
3. SRM AIM、RM AIM、MSCS AIM、または仮想環境管理用の AIM

上記以外の順序はインストーラで許可されません。 たとえば、Advanced Encryption の前に SRM をインストールしようとすると、エラー メッセージが表示され、インストールは開始されません。

ca-setup.exe を使用して Windows に AIM をインストールする方法

1. 以下のサブディレクトリが含まれる DVD1¥Installers¥Windows¥Agent¥SysMan ディレクトリに移動します。
   - CA_SystemEDGE_CXEN
   - CA_SystemEDGE_GALAX
   - CA_SystemEDGE_HACMP
   - CA_SystemEDGE_HYPERV
   - CA_SystemEDGE_KVM
   - CA_SystemEDGE_LPAR
   - CA_SystemEDGE_MSCS
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_SOLZONES
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_UCS
   - CA_SystemEDGE_VC
   - CA_SystemEDGE_VCLOUD
2. SRM または RM AIM の場合、適切なディレクトリに移動し、以下のコマンドを実行します。

   ```
   ca-setup
   ```

   画面上の指示に従って、インストールを完了します。
3. Hyper-V、LPAR、MSCS、ゾーン、UCS、vCenter、HACMP、vCloud、CXEN、または KVM AIM の場合、コマンド プロンプトを開き、適切なディレクトリに移動して、以下のコマンドを実行します。

   ```
   ca-setup EULA_ACCEPTED="YES"
   ```

   ca-setup プログラムによってインストールが警告なしで実行されます。

注: CA Virtual Assurance マネージャのカスタム インストールを使用して、Windows サーバに SystemEDGE コンポーネントをインストールすることもできます。

ca-setup.sh を使用して UNIX に AIM をインストールする方法

1. 端末コンソールを開き、以下のサブディレクトリを含む DVD2/Installers/*プラットフォーム*/Agent/SysMan ディレクトリに移動します。
   - CA_SystemEDGE_SRM
2. 適切なディレクトリに移動し、以下のコマンドを実行します。

   ```
   sh ca-setup.sh
   ```

   画面上の指示に従って、インストールを完了します。

SRM のインストール中、以下のパラメータを指定できます。

スクリプト実行の許可

カスタム スクリプトの実行を許可するかどうかを指定します。このようなスクリプトはスーパーユーザ権限で実行します。

デフォルト： いいえ （標準インストール）

ファイル入出力テストの許可

ファイル入出力テストの実行を許可します。テストはスーパーユーザ権限で実行されるので、このパラメータが有効な場合、スーパーユーザはシステム上のすべてのファイルにアクセスできます。

デフォルト： いいえ （標準インストール）

信頼できない SSL 証明書を許可する

HTTPS テストで、証明書が無効なサイト（信頼できないサイトや、Web サイトと証明書内の名前とが一致しないサイト）へのアクセスを許可します。

デフォルト： いいえ （標準インストール）

その他

SRM ドキュメント コンポーネントをインストールします。

デフォルト： はい

CA Systems Performance LiteAgent のインストール

CA Systems Performance LiteAgent は、Windows、UNIX、または Linux システムにインストールできます。

注: CA Systems Performance LiteAgent は 32 ビットおよび 64 ビットのオペレーティング システム上で実行されます。

Windows システムに CA Systems Performance LiteAgent をインストールする方法

DVD1 からカスタム インストールを実行して CA Systems Performance LiteAgent をインストールします。

AIX、HP-UX、Linux、Solaris SPARC、Solaris x86 システムに CA Systems Performance LiteAgent をインストールする方法

UNIX または Linux に CA Systems Performance LiteAgent をインストールするには、リモート展開を使用します。

注: リモート展開の詳細については、「管理ガイド」を参照してください。

第 3 章: CA Virtual Assurance のアップグレード

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 Virtual Assurance のアップグレード方法

以下の CA Virtual Assurance リリースを リリース 12.8 にアップグレードできます。

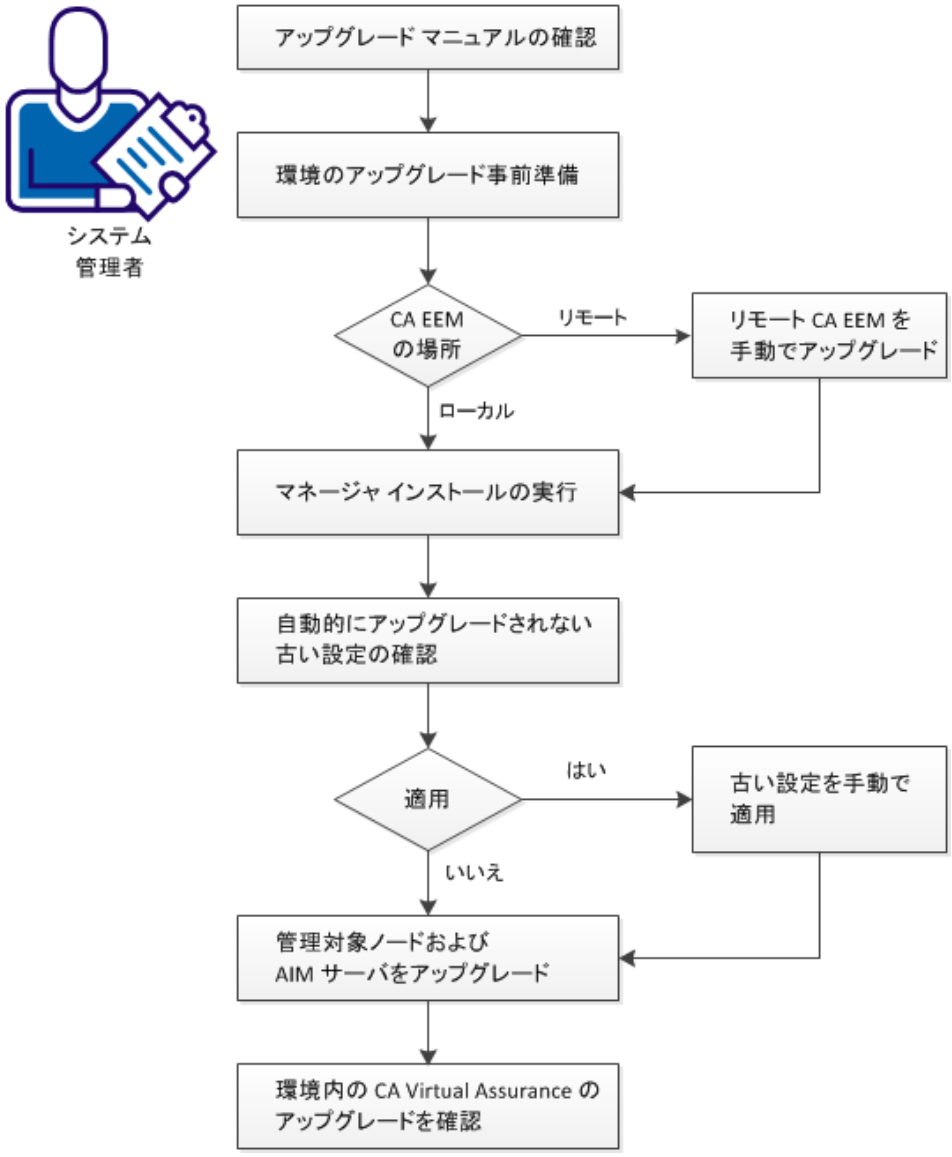
- CA Virtual Assurance Release 12.6、12.7、または 12.7.1。

注: アップグレード中は、旧バージョンで使用されたロケールのみがサポートされます。 アップグレード中に新しいロケール サポートを追加することはできません。

注: アップグレードを行う前に、CA サポート オンライン上の最新の「リリース ノート」および「Solutions and Patches」で重要なパッチを参照してください。

以下の図は、アップグレード処理の概要を示しています。

CA Virtual Assurance for Infrastructure Managers のアップグレード方法



以下の手順に従います。

アップグレード ドキュメントの確認

CA Virtual Assurance のアップグレード処理を開始する前に、この章のアップグレード情報を読みます。 この章には、アップグレードの準備および実行に必要な手順に関する重要な情報が含まれています。

この章に加え、リリース ノートにあるハードウェアおよびソフトウェアの要件を確認し、このガイドの「カスタム インストールの準備 (P. 19)」を読みます。

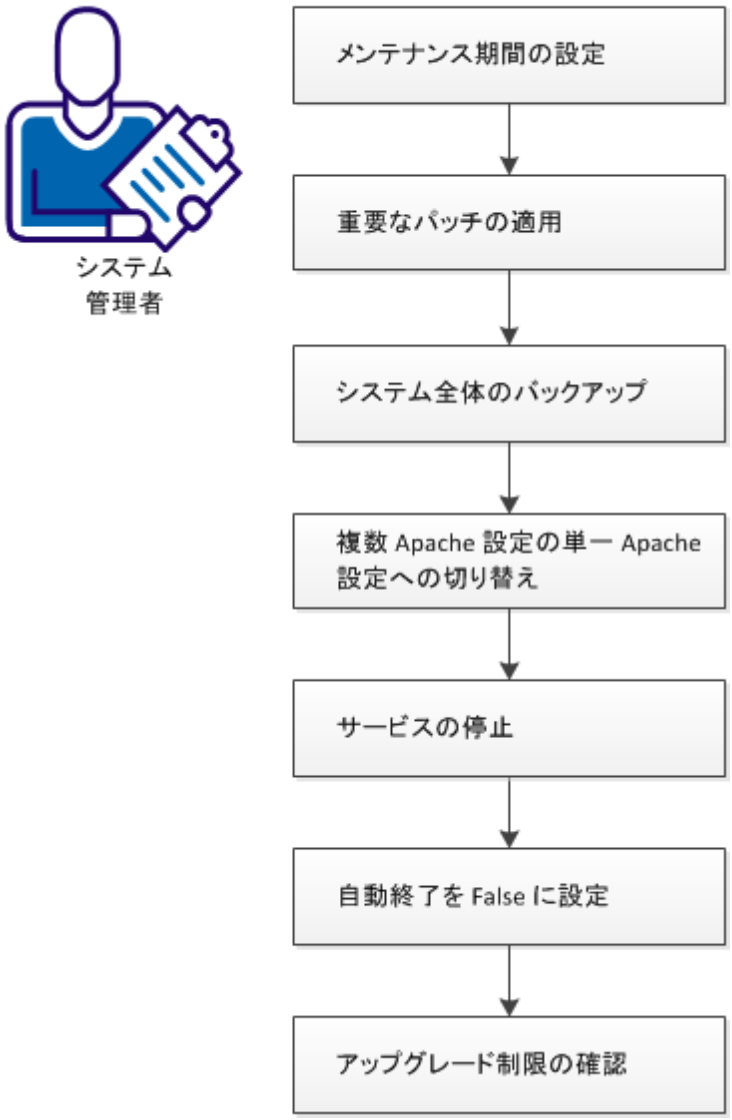
認証にリモート CA EEM インストールを使用している場合は、CA EEM ドキュメントのアップグレード手順を読みます。

ご使用のネットワークにある管理対象ノードまたは AIM サーバのアップグレードにリモート展開を使用する場合の詳細については、「管理ガイド」およびオンライン ヘルプを参照してください。

アップグレード対象環境の準備

このセクションでは、アップグレード処理の開始前における環境の準備方法について説明します。

環境のアップグレードの準備方法



以下の手順に従います。

メンテナンス期間の設定

影響を受けるユーザとメンテナンス期間についてあらかじめ同意しておきます。 メンテナンス期間中に操作を行う管理者ユーザがいないことを確認します。

重要なパッチの適用

CA サポート オンライン上の最新の「リリース ノート」および「Solutions and Patches」で更新を参照してください。

リリース 12.6 から リリース 12.8 にアップグレードする場合は、リリース 12.6 に以下のいずれかのパッチを適用します。

- RO48212 (LPARAIM - 32 BIT - CUMULATIVE FIX 12162)
- RO48213 (LPARAIM - 64 BIT - CUMULATIVE FIX 12162)

システム全体のバックアップ

マネージャ ノードに対してシステム全体（フル）のバックアップを実行します。 マネージャ ノードは以下のコンポーネントが含まれるすべてのサーバです。

- ドメイン サーバ
- 配布サーバ
- データベース
- EEM サーバ

マネージャ ノードは業界標準ツールを使用してバックアップします（たとえば物理サーバ用に ARCserve、または仮想マシン用にスナップショットを使用）。 複数のマネージャ ノードがある場合は、バックアップがすべてのサーバ上で同時に実行されることを確認します。

バックアップは、ユーザ アクティビティのないときにオフラインで実行することをお勧めします。 バックアップを開始する前に、リモート展開用のアクティブなジョブがすべて完了していることを確認します。

注: ディザスタ リカバリはシステム全体に関係するため、システム上にソフトウェアがある他の製品の所有者にも相談してください。

次の手順に従ってください:

1. ［リソース］-［展開］-［ジョブ］を選択し、すべてのジョブが 100 パーセント完了していることを確認します。
2. 以下のいずれかのオプションを使用して、各サービスを停止します。
   - コマンド ライン インターフェース：
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ
3. 以下の*いずれか*を実行します。
   - マネージャ システム全体のスナップショットを取得します。
   - マネージャ システム全体のゴースト イメージを取得します。
4. 以下のいずれかのオプションを使用して、停止されたサービスを再度開始します。
   - コマンド ライン インターフェース：
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ

注: バックアップがドメイン サーバに接続したマネージャ ノード上で実行されない場合は、配布サービスのみを停止および開始します。

複数 Apache 設定の単一 Apache 設定への切り替え

複数の Apache 設定で実行されるようにご使用のインストールが設定されている場合は、アップグレードの実行前に単一の Apache 設定に変更します。 アップグレード後には複数の Apache 設定に戻すことができます。

複数の Apache に関するドキュメント、および設定を元に戻す手順については、CA サポート にお問い合わせ (P. 3)ください。

サービスの停止

アップグレードの開始前に以下のサービスを停止します。

次の手順に従ってください:

1. CA Virtual Assurance ユーザ インターフェースからログアウトします。
2. 以下の Windows サービスを停止します。
   a. CAAIPApache
   b. CA Message Queuing Server (ActiveMQ)
   c. CAAIPTomcat

      重要: CAAIPTomcat サービスを停止できない場合は、タスク マネージャから関連する java.exe プロセスを終了します。 java.exe プロセスを特定するには、タスク マネージャを開き、［表示］-［列の選択］をクリックして、［イメージ パス名］を選択します。 終了する必要がある java.exe プロセスは、次のパス名を持ちます。
      Install_Path¥*ProductName*¥jre¥bin¥java.exe

自動終了を False に設定

CA Virtual Assurance アップグレード インストールでは、aom2 および dpm データベースに対する自動終了の有効化をサポートしていません。

次の手順に従ってください:

1. 管理者（sa）権限で、またはローカル システム管理者として SQL Server にログインします。
2. SQL Server Management Studio のオブジェクト エクスプローラーで［データベース］を展開します。
3. aom2 を右クリックし、［プロパティ］を選択します。

   ［プロパティ］ウィンドウが開きます。
4. ［オプション］を開きます。

   パラメータのリストが表示されます。
5. 自動終了の値を False に設定します。
6. ［OK］をクリックします。
7. dpm データベースについて、これらの手順を繰り返します。

アップグレード制限の確認

いくつかのコンポーネント ディレクトリは、製品のアップグレード時に以下のように名前が変更されます。

<製品ルート>¥component は <製品ルート>¥component-old に変更

これらの「古い」ディレクトリは、アップグレードの完了後も参照用に残されます。 アップグレード前にこれらのディレクトリ ツリーに対して何らかの変更または追加が行われている場合、それらは「古い」ディレクトリ内に含まれています。 それらの変更は、<製品ルート>¥component を引き継ぐ新しい稼働製品には自動的にはマージされません。 これらの変更が新しい製品でも有効になるようにするには、カスタマイズされた設定を手動で再適用します。

上述の制限が適用されるコンポーネントとそのディレクトリ名のリストを以下に示します。

- Apache HTTP Server: <製品ルート>¥apache
- Apache ActiveMQ: <製品ルート>¥activeMQ
- Apache Tomcat: <製品ルート>¥tomcat、¥tomcat¥UI を含む

  注: Tomcat 自身にこの制限がある一方で、Tomcat 下の設定データの中にはアップグレード時に自動的に引き継がれるものもあります。

リモート CA EEM の手動アップグレード

CA EEM を CA Virtual Assurance マネージャと同じサーバ上で実行する場合、このセクションはスキップできます。CA Virtual Assurance のアップグレードでは、ローカルにインストールされた CA EEM が自動的にアップグレードされます。

独立したサーバ上で CA EEM を実行する場合は、サポートされている CA EEM バージョンについてリリース ノートを参照してください。CA EEM をアップグレードする必要がある場合、以下の手順に従います。

次の手順に従ってください:

1. CA EEM サーバの Windows ［スタート］メニューから、CA EEM マニュアル選択メニューを開きます。
2. 「導入ガイド」のアップグレード セクションを読みます。
3. CA Virtual Assurance のインストール メディア（DVD1）を DVD ドライブに挿入します。
4. Windows エクスプローラを開き、¥Installers¥Windows¥External¥CAEEMServer にディレクトリを変更します。
5. EEMServer_win32.exe を起動して CA EEM をアップグレードし、CA EEM アップグレード ドキュメントの手順に従います。

マネージャ インストールの実行

すでにインストール済みのコンポーネントはすべてアップグレードされます。 すでにインストール済みのコンポーネントのアップグレードは必須で、既存の設定はすべて保持されます。 また、アップグレードでインストールする新しいコンポーネントを選択することができます。 新しく選択したコンポーネントは、インストール中に設定できます。

すべての前提条件を満たしていると判断したら、以下の手順に従います。インストール中にコンポーネントの設定を省略する場合、インストール後にグラフィカル ユーザ インターフェースの［管理］タブを使用してコンポーネントを設定できます。

注: コンポーネントの設定の詳細については、「管理ガイド」を参照してください。

次の手順に従ってください:

1. DVD ドライブにインストール メディアを挿入します。

   自動再生が有効の場合、インストール ウィザードが自動的に開始されます。インストール ウィザードが開始されない場合は、setup.hta をダブルクリックするか、インストール メディア上の *DVD ドライブ*:¥Installers¥Windows ディレクトリに移動し、install.exe をダブルクリックします。

   ［検出されたアップグレード］ダイアログ ボックスが表示されます。

2. ［継続］をクリックします。

   ［はじめに］ダイアログ ボックスが表示されます。

3. ［次へ］をクリックします。

   使用許諾契約のダイアログ ボックスが表示されます。

4. 内容を読み、契約の下部にスクロールすると、［*使用許諾契約書に同意します*］オプションがアクティブになります。 このオプションを選択し、［次へ］をクリックします。

   ［インストールする機能を選択］ダイアログ ボックスが表示されます。インストール済みのコンポーネントはすべてアップグレードされます。

5. （オプション）インストールする追加コンポーネントを選択して、［次へ］をクリックします。
6. アップグレードでは、CA EEM、ネットワーク ディスカバリ ゲートウェイ、および追加コンポーネントのための認証情報またはその他の追加情報が求められます。

   インストール ウィザードでは最後にインストール サマリのダイアログ ボックスが表示され、インストールするコンポーネントが一覧表示されます。
7. ［インストール］をクリックして、アップグレードを開始します。

   インストールが成功すると、インストールしたコンポーネントごとに以下のディレクトリにログ ファイルが作成されます。

   Install_Path¥log¥install

   インストール完了を示すダイアログ ボックスが表示されます。
8. インストーラを終了する前に、ダイアログ ボックス内の情報を読みます。
9. ［スタート］、［プログラム］、［CA］、［CA Virtual Assurance］、［CA Virtual Assurance の起動］に移動し、ユーザ インターフェースにログインします。
10. アップグレードが失敗した場合の詳細については、インストール ログ（*インストール パス*¥log¥install¥install.log）およびエラー リスト（*インストール パス*¥log¥install¥install_error_detected.log）を参照してください。

    ［インストールがエラーで終了しました］ダイアログ ボックスが表示されます。アップグレード失敗の問題を解決するには、CA サポート にお問い合わせください。

自動的にアップグレードされなかった古い設定の確認

以下のディレクトリを使用して、旧リリースからの設定の引き継ぎが必要かどうかを確認できます。

- Apache HTTP Server: <製品ルート>¥apache-old
- Apache ActiveMQ: <製品ルート>¥activeMQ-old
- Apache Tomcat: <製品ルート>¥tomcat-old、¥tomcat¥UI を含む

  注: Tomcat 下の設定データの中にはアップグレード時に自動的に引き継がれるものもあります。

古い設定の手動適用

アップグレードした CA Virtual Assurance インストールで使用する、引き継がれていない設定データがある場合、以下のガイドラインを使用します。

次の手順に従ってください:

1. Apache、Tomcat、または ActiveMQ の設定ドキュメントを読みます。
2. CA Virtual Assurance からログアウトします。
3. 必要な Apache、Tomcat、または ActiveMQ 設定ファイルを変更します。
4. 設定ファイルを変更したサービスを再起動します。
5. CA Virtual Assurance にログインします。

管理対象ノードおよび AIM サーバのアップグレード

管理対象ノードおよび AIM サーバをアップグレードする推奨の方法は、リモート展開を使用することです。リモート展開を使用すると、SystemEDGE、Advanced Encryption、および AIM をアップグレードできます。

ご使用のシステムで SystemEDGE の管理対象モードがサポートされていない場合、リモート展開は使用できません。 以下のいずれかのオプションを使用することをお勧めします。

- インストール メディアからの手動インストール
- たとえば SSH などを使用した、SystemEDGE、Advanced Encryption、および SRM AIM のリモート インストール

以下の手順に従います。

エージェントと AIM のアップグレード (P. 112)
ポリシーへの SystemEDGE モニタのインポート (P. 116)

エージェントと AIM のアップグレード

SystemEDGE r11.6 へは、SystemEDGE の以下のアップグレード可能なリリースからアップグレードできます。

- 4.3.4 以降（4.3.x）
- 5.1.0 以降（5.1.x）
- 5.6.0 以降（5.6.x）
- 5.7.0 以降（5.7.x）

インストーラは元のインストール パスのルートにアップグレードされたディレクトリを作成し、前のリリースからそのディレクトリに設定ファイルをコピーします。 エージェントは、初めて起動したときに設定データを新しく作成されたデータ ディレクトリにマイグレートします。 SystemEDGE を r11.6 にアップグレードする場合は、Advanced Encryption および対応する AIM をすべて最新バージョンにアップグレードしてください。

注: SystemEDGE r11.6 は、前の CA Virtual Assurance リリースの AIM をロードしません。

以下のいずれかの方法で SystemEDGE をアップグレードできます。

- アップグレード可能なエージェントがインストールされたシステムに対する CA Virtual Assurance によるリモート展開

  注: SystemEDGE、Advanced Encryption、および AIM をアップグレードする場合は、アップグレード用の単一のリモート展開ジョブを使用します。SystemEDGE、Advanced Encryption、およびすべての必要な AIM を［リモート展開］タブに追加します。 SystemEDGE は、r11.6 レベルの AIM または iddmod のようなレガシー AIM のみをロードします。 したがって、5.7.x レベル以下の AIM は隔離されます。

  リモート展開の詳細については、「*管理ガイド*」の「リモート展開」の章を参照してください。

- Windows でのカスタム マネージャ インストール。 このオプションはインストール済みコンポーネントをすべてアップグレードします。インストールする他のエージェントおよび AIM をすべて選択します。
- アップグレード可能なエージェントがインストールされたシステムに対する手動インストール

  アップグレードを実行するには、「Windows へのエージェントのインストール (P. 59)」または「UNIX へのエージェントのインストール (P. 74)」の説明に従ってエージェントをインストールします。

アップグレードがサポートされていない古いリリースの場合は、以下の手順に従います。

- 以前のリリースの SystemEDGE の場合は、エージェントをアンインストールしてから SystemEDGE r11.6 をインストールします。 アンインストールの前にすべての設定データを保存し、そのデータを SystemEDGE r11.6 に適用します。

関連項目:

SystemEDGE 4.3.4 からのエージェント アップグレード (P. 113)

SystemEDGE 4.3.4 からのエージェント アップグレード

インストーラは、設定ファイルを以前の 4.3.4 リリースからアップグレードするときに以下を実行します。

- インストーラは、以下のファイルの旧バージョンを検出して、CASYSEDGE¥upgraded ディレクトリにコピーします。
  - system32¥sysedge.cf （Windows）および /etc/syedge.cf （UNIX）
  - CASYSEDGE¥config¥sysedgeV3.cf （Windows および UNIX）
  - system32¥sysedge.mon（Windows）および /etc/sysedge.mon（UNIX）
  - system32¥sysedge.lic （Windows）および /etc/sysedge.lic （UNIX）
  - CASYSEDGE¥plugins¥monwin¥monwin.cf （Windows および UNIX）
- エージェントを初めて起動すると、以下のファイルが CASYSEDGE_DATADIR ディレクトリに直接コピーされます。
  - CASYSEDGE¥config¥sysedge.cf （Windows および UNIX）
  - CASYSEDGE¥config¥sysedgeV3.cf （Windows および UNIX）

- エージェントは、sysedge.cf のコピー操作の一部として、アップグレードされるディレクトリに含まれる sysedge.cf、sysedge.mon、および monwin.cf ファイル内の設定データをデータ ディレクトリ内の新しい sysedge.cf ファイルにマイグレートします。
- エージェントは、sysedgeV3.cf のコピー操作の一部として、アップグレードされるディレクトリに含まれる sysedgeV3.cf ファイル内の設定データをデータ ディレクトリ内の新しい sysedgeV3.cf ファイルにマイグレートします。

注: データ ディレクトリには、実行時の設定変更に使用される sysedge.cf ファイルのバージョンを格納します。

エージェントは、以前のリリースからアップグレードするときに、設定ファイルの設定に対して自動的に以下の変更を加えます。

- procAlive プロセス モニタの構文は、threshold プロセス モニタの構文に合わせて変更されます。エージェントは、既存の procAlive エントリを自動的に新しい形式に変換します。

  注: procAlive エントリの構文の詳細については、「プロセスとサービスのモニタリング」の章を参照してください。

- no_process_sets および no_remoteshell_group パラメータを無効にすると、SNMP 書き込みコミュニティのみを使用してエージェント システムへのクリティカルなアクセスが可能になります。 このため、エージェントはこれらのパラメータの古い設定をマイグレートせず、これらのパラメータを常に有効にします。
- sysedge_memory パラメータは廃止され、アップグレードされた sysedge.cf ファイルから削除されます。 未処理のアラームは、sysedge.mon ファイルにモニタの現在の状態を格納することによって処理されるようになりました。 既存のエントリは、新しいアラーム処理設定にマイグレートされます。
- tc_publish パラメータの名前は（真偽が逆の） no_trapcommunity_table に変更され、デフォルトで有効になります。
- リモート展開を使用して SystemEDGE リリース 4.3.4 から SystemEDGE r11.6 にアップグレードすると、マイグレートされたモニタは sysedge.cf.bak ファイルに格納されます。

- 展開の戦略によっては、［ポリシー設定］を使用してマイグレートされたモニタを環境に適用できます。

  注: 詳細については、CA Virtual Assurance のマニュアル選択メニューを参照してください。

- ローカル システム上の SystemEDGE リリース 4.3.4 を SystemEDGE r11.6 にアップグレードすると、インストール プログラムはモニタをマイグレートし、それを新しい設定に反映します。

以前の構文はすべて新バージョンのエージェントと互換性がありますが、エージェントの機能を強化する多くのオプションが新たに追加されています。 古いモニタ エントリを調べ、構文を編集して追加のオプションを組み込むことをお勧めします。

注: SystemEDGE をリリース 4.3.4 以降（4.3.x）から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。

ポリシーへの SystemEDGE モニタのインポート

エージェントをアップグレードする前に、SystemEDGE エージェントで使用される SNMP コミュニティ文字列が［管理］タブの［SNMP］で指定されていることを確認します。 コミュニティ文字列はコンピュータごとに指定することもできます（［ポリシー］ - *コンピュータ* - ［メトリック］ - ［SNMP］）。 SystemEDGE インストーラは SystemEDGE ファイルを「アップグレード後の」ディレクトリに移動します。アップグレード後、エージェントはこれらのファイルを読み取ります。OID は保持されます。ポリシー設定では既存の sysedge.cf ファイルのエントリが読み取られるだけです。sysedge.mon ファイルはインポートされません。

リモート展開では、モニタの Raw OID がインスタンス内にインポートされます。

次の手順に従ってください:

1. SystemEDGE エージェントのコミュニティ文字列が、［管理］タブで、エージェントのポートの SNMP に含まれていることを確認します。
2. SystemEDGE を r11.6 にアップグレードします。
3. SystemEDGE r11.6 が正しく検出されることと（［リソース］タブ）、このリリースにポリシーがあることを確認します。
4. ［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。
5. ［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。
6. ポリシーの名前を入力し、［インポート］をクリックします。

   ［SystemEDGE エージェント マシン］ダイアログ ボックスが表示されます。

7. アップグレードされたサーバを選択し、［OK］をクリックします。

   ［SystemEDGE エージェント マシン］ダイアログ ボックスが閉じます。

8. ［新規 SystemEDGE］ダイアログ ボックスの［OK］をクリックします。

   インポートしたモニタを含むポリシーが CA Virtual Assurance によって作成されます。

モニタは編集または更新できます。SystemEDGE r11.6 状態モデルを使用することもできます。

使用環境での CA Virtual Assurance アップグレードの確認

CA Virtual Assurance コンポーネントが正常にアップグレードされたら、全体的に CA Virtual Assurance が予期したように動作するかどうかを確認します。

パフォーマンス データのアップグレード

CA Virtual Assurance を リリース 12.8 にアップグレードしたら、パフォーマンス データをアップグレードします。 使用履歴を保持するには、dpmkpdb.exe CLI ユーティリティを使用して、パフォーマンス データをエクスポートおよびインポートします。

注: dpmkpdb.exe ユーティリティの詳細については、「リファレンス ガイド」を参照してください。

次の手順に従ってください:

1. 収集エンジンからのパフォーマンス データのエクスポート：

   dpmkpdb.exe export_ce -ws_user *username* -ws_password *password* -output *export.txt*

2. KPDB へのデータのインポート：

   dpmkpdb.exe import -ws_user *username* -ws_password *password* -input *export.txt*

第 4 章: ユーザ インターフェースの使い方

この章では、CA Virtual Assurance のグラフィカル ユーザ インターフェース、AutoShell、およびマニュアル選択メニューを簡単に紹介します。これらのコンポーネントは、標準インストールの完了後、Windows の［スタート］メニュー、［CA］、［CA Virtual Assurance］を選択してマネージャを起動すると利用できます。

仮想環境を管理するための考え方、詳細、および具体的なタスクについては、「管理ガイド」、*オンライン ヘルプ*、または「リファレンス ガイド」を参照してください。

このセクションには、以下のトピックが含まれています。

CA Virtual Assurance の起動

インストールおよびインストール後の設定が完了したら、CA Virtual Assurance を起動できます。

次の手順に従ってください:

1. ［CA］、［CA Virtual Assurance］を選択し、CA Virtual Assurance を起動します。

   CA Virtual Assurance のログイン ページが表示されます。

   注: CA Virtual Assurance ユーザ インターフェースを初めて起動するとき、ブラウザには SSL 証明書の警告が表示されます。署名済みの SSL 証明書が設定されていない、セキュリティで保護されたサイトにブラウザで接続すると、この警告が表示されます。 SSL 証明書は特定のサーバおよび認証局について作成する必要があり、自動的に生成、インストールすることはできません。 警告が表示されたら、［OK］をクリックして続行します。

2. 製品のインストール中に定義したユーザ名とパスワードを入力し、［ログイン］をクリックします。

   製品のダッシュボードが表示されます。

Web ブラウザに Flash プラグインがインストールされている場合、CA Virtual Assurance では図またはグラフだけ表示できます。 Flash プラグインを利用できない場合、プラグインのダウンロード リンクが図やグラフの代わりに表示されます。 ダッシュボードにはデフォルトで、システム ステータス、使用率履歴、サービス、CA Virtual Assurance ステータス、およびイベントが表示されます。 ダッシュボードを設定するには、左側のペインから右側のペインにモジュールをドラッグします。

機能の概要

CA Virtual Assurance グラフィカル ユーザ インターフェースは、左側のナビゲーション ペインと右側のデータ ペインから構成されます。 ペイン上部にあるタブを使用して、以下の機能領域間を切り替えます。

ダッシュボード

仮想環境および関連付けのある物理リソースの現在のステータスに関する概要ビューを示します。 ダッシュボードを設定するには、ナビゲーション ペインからデータ ペインにモジュールをドラッグします。

リソース

環境内で検出されたリソースに関する詳細を示します。モニタ対象のリソースに関する詳細情報を表示するには、ナビゲーション ツリー内でリソースをクリックします。 新しいリソースを検出するには、ナビゲーション ツリーから［データ センター］を選択し、［クイック スタート］タブを開きます。

［リソース］タブから以下の機能を使用できます。

- モニタリングと管理機能の設定。
- VM および Solaris ゾーンのプロビジョニング。
- SystemEDGE および AIM のリモート展開。
- SystemEDGE および AIM 設定の作成と管理。
- アクションおよびアクションの実行をトリガするルールの管理。

レポート

環境の特定の状況または特徴に関するレポートを作成できます。 事前定義済みまたはカスタムのレポートを左側のペインから選択できます。

環境管理

CA Virtual Assurance コンポーネント設定、ユーザ グループの管理、または管理へのアクセスが可能です。

注: 詳細については、「管理ガイド」または*オンライン ヘルプ*を参照してください。

AutoShell の開始

AutoShell は、複雑な反復タスクと管理タスクを自動化する、コマンド ラインおよびスクリプト環境です。 スクリプト言語（JavaScript）とコマンド ライン シェルを組み合わせたものです。 JavaScript 構文と AutoShell のコマンド、関数、およびクラスを、AutoShell 内で直接組み合わせて使用したり、.js ファイルのスクリプトを実行したりできます。

注: AutoShell 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。

次の手順に従ってください:

1. Windows エクスプローラを開き、以下のディレクトリに移動します。
   C:¥Program Files¥CA¥SC¥AutoShellManager
2. caaipaomautoshell.exe をダブルクリックします。

   AutoShell ログイン ダイアログ ボックスが表示されます。
3. インストール中に定義したユーザ名とパスワードを入力します。

   AutoShell コマンド プロンプトが表示されます。

   ```
   CA AutoShell v1.5.0.1
   Based on Mozilla SpiderMonkey 1.7
   User name: ca
   Password : *********
   VASU::->
   ```
4. AutoShell の式またはコマンドを適宜入力します。
5. AutoShell を終了するには「**exit**」と入力します。

例

Hello World! の表示

```
? "Hello World!"
Hello World
```

1 から 10 までの数を表示

```
for(i=1;i<11;i++)qout(i);
1
2
3
4
5
6
7
8
9
10
```

現在の日付と時刻の表示

```
? "Today is", new Date
Today is Tue Jun 02 2009 14:17:05 GMT-0400 (Eastern Daylight Time)
```

関連項目

有効な AutoShell ユーザ (P. 123)

有効な AutoShell ユーザ

CA Virtual Assurance のインストール時に、インストール ウィザードのネイティブ セキュリティ ユーザ情報画面で CA Embedded Entitlements Manager（CA EEM）のユーザ ID とパスワードを定義します。 認証情報は CA EEM データベースに格納されます。ユーザは CA Virtual Assurance 管理者グループに割り当てられ、CA Virtual Assurance ユーザ インターフェースおよび AutoShell マネージャへのログインに使用できます。

CA EEM を使用する CA Virtual Assurance コンポーネントが、ローカルまたはリモート システムにインストールされている場合、AutoShell マネージャは常に CA EEM データに対するログイン認証情報を検証します。 そうでない場合、AutoShell マネージャは、Windows 認証に対するログイン認証情報を検証します。

CA Virtual Assurance コマンド プロンプトの起動

「リファレンス ガイド」で解説されている CLI コマンドを使用する場合は、CA Virtual Assurance コマンド プロンプトを起動します。

次の手順に従ってください:

1. ［CA］、［CA Virtual Assurance］、［CA Virtual Assurance コマンド プロンプト］を選択します。

   ［CA Virtual Assurance コマンド プロンプト］ダイアログ ボックスが表示され、*Install_Path/productname*¥bin ディレクトリが開きます。

2. CLI コマンドを入力します。

マニュアル選択メニューとオンライン ヘルプの起動

マニュアル選択メニューには CA Virtual Assurance のドキュメント セット全体が含まれます。 すべてのガイドは HTML 形式と PDF 形式で用意され、オンライン ヘルプと Readme は HTML 形式で用意されています。マニュアル選択メニューでは、すべてのドキュメントにまたがって全文検索が可能です。 オンライン ヘルプ システムは、ユーザ インターフェース内の上位レベル タブ別にトピックが構成されています。

オンライン ヘルプを起動する方法

1. CA Virtual Assurance ユーザ インターフェースを開き、ウィンドウの右上角の［ヘルプ］をクリックします。

   タブ関連のトピックが表示されます。

2. 必要に応じて、［目次］、［索引］、［検索］を含むナビゲーション ペインを使用します。

オンライン ヘルプからマニュアル選択メニューを開く方法

1. CA Virtual Assurance ユーザ インターフェースを開き、ウィンドウの右上角の［ヘルプ］をクリックします。

   タブ関連のトピックが表示されます。

2. ナビゲーション ペインの目次への移動

3. 最上位までスクロールし、［マニュアル選択メニューへ戻る］をクリックします。

   マニュアル選択メニューが表示されます。

[スタート]メニューからマニュアル選択メニューを起動する方法

1. Windows の［スタート］メニューから、［CA］、［CA Virtual Assurance］、［マニュアル選択メニュー］を選択します。

   ［マニュアル選択メニュー］ウィンドウが表示されます。

2. 以下のいずれかを実行します。

   - ［マニュアル選択メニュー］ウィンドウに示された適切なリンクをクリックして、ドキュメントまたはオンライン ヘルプ システムを開きます。
   - ［マニュアル選択メニュー］ウィンドウの右上角のフィールドに語句を入力し、［Search］をクリックすると、すべてのドキュメントにまたがって全文検索が実行されます。

第 5 章: CA Virtual Assurance のアンインストール

このセクションには、以下のトピックが含まれています。

アンインストール オプション

CA Virtual Assurance には以下のアンインストール オプションがあります。

- 完全アンインストール
- 特定機能のアンインストール（マネージャのみ）
- サイレント モードでのアンインストール

マネージャのアンインストール

［完全アンインストール］オプションは、CA Virtual Assurance のコンポーネントと機能をすべて削除し、以下の組み込みコンポーネントを削除するオプションを提供します。

- CA EEM
- Apache
- Tomcat
- 管理データベース
- パフォーマンス データベース

アンインストール ウィザードでは、CA Virtual Assurance インストール処理中に初期インストールされた組み込みコンポーネントに限り削除できます。 この製品のインストール前からシステムに存在していた共有コンポーネントは、製品をアンインストールしても削除されません。

注: アンインストールの対象として Apache サービスと Tomcat サービスを選択していなくても、アンインストール処理によってこれらのサービスが停止される場合があります。

関連項目

完全アンインストールの実行 (P. 128)
コマンド プロンプトからのマネージャのアンインストール (P. 129)
サイレント モードでのマネージャのアンインストール (P. 130)

完全アンインストールの実行

CA Virtual Assurance の機能とコンポーネントをすべて削除するときは、［完全アンインストール］オプションを使用します。 このオプションを使用すると、組み込みコンポーネントを保持するか削除するかを選択できます。

次の手順に従ってください:

1. Windows の［スタート］メニューから、［スタート］、［設定］、［コントロール パネル］、［プログラムの追加と削除］をクリックします。

   ［アプリケーションの追加と削除］ウィンドウが表示されます。

2. CA Virtual Assurance を選択し、［変更と削除］をクリックします。

   ［CA Virtual Assurance のアンインストール］ダイアログ ボックスが表示されます。

3. ［次へ］をクリックします。

   ［アンインストール オプション］ダイアログ ボックスが表示されます。

4. 管理データベースを保持するかどうかを選択し、［次へ］をクリックします。

   アンインストールが開始されます。 CA Virtual Assurance および選択したすべてのコンポーネントがシステムから削除されます。

   注: CA Virtual Assurance のインストール時にインストールされていない組み込みコンポーネントはアンインストールされません。

コマンド プロンプトからのマネージャのアンインストール

Windows コマンド プロンプトから CA Virtual Assurance をアンインストールするには、以下の手順に従います。

次の手順に従ってください:

注: この手順で示すコマンド構文内の引用符は必須です。コマンド名にはスペースが含まれるためです。

1. 管理者としてログインし、コマンド プロンプトを開きます。

   コマンド プロンプト ウィンドウが表示されます。

2. *Install_Path*¥*productname*¥Uninstall ディレクトリに移動し、以下のコマンドを入力します。

   ```
   Uninstall.exe
   ```

   アンインストールが開始されます。

3. 以下のいずれか 1 つのオプションを選択し、画面上の指示に従ってアンインストールを完了します。

   - 完全アンインストール
   - 選択した機能のアンインストール

関連項目

サイレント モードでのマネージャのアンインストール (P. 130)

サイレント モードでのマネージャのアンインストール

Windows サーバからマネージャを警告なしで削除するには、以下の手順に従います。

次の手順に従ってください:

1. 管理者としてログインし、コマンド プロンプトを開きます。

   コマンド プロンプト ウィンドウが表示されます。

2. *Install_Path*¥*productname*¥Uninstall ディレクトリに移動し、以下のコマンドを入力してマネージャをアンインストールします。

   ```
   Uninstall.exe -i silent
   ```

   アンインストールが開始されます。 CA Virtual Assurance がシステムから削除されます。

関連項目

コマンド プロンプトからのマネージャのアンインストール (P. 129)

SystemEDGE のアンインストール

このセクションでは、SystemEDGE エージェントに関連付けられたファイルとサブディレクトリを削除する方法について説明します。

Windows 上の SystemEDGE および AIM のアンインストール

アンインストーラは、システムから SystemEDGE を削除します。ユーザは、データ ディレクトリからコンフィギュレーション データを削除するどうかを指定できます。 Windows の［プログラムの追加と削除］ウィンドウまたはコマンド ラインを使用してエージェントと AIM をアンインストールできます。

アンインストールするときは、以下の依存関係を考慮してください。

- 仮想環境用の AIM、RM AIM、および SRM AIM は Advanced Encryption と SystemEDGE に依存します。
- Advanced Encryption は SystemEDGE に依存します。

これらの依存関係に基づいて、アンインストールの順序は以下のようになります。

1. RM AIM、SRM AIM、または仮想環境用の AIM
2. Advanced Encryption
3. SystemEDGE コア

これ以外の順序ではアンインストールできません。 リモート展開でインストールされたコンポーネントを削除する場合は、Idprimer と CAM はアンインストールされません。

SystemEDGE または AIM を Windows の［プログラムの追加と削除］ウィンドウでアンインストールする方法

1. ［スタート］-［設定］-［コントロール パネル］-［プログラムの追加と削除］を選択します。

   ［プログラムの追加と削除］ウィンドウが表示され、以下のコンポーネントが一覧表示されます。

   - 仮想環境用の AIM
   - CA SystemEDGE Core
   - CA SystemEDGE AdvancedEncryption
   - CA SystemEDGE RM
   - CA SystemEDGE SRM

2. アンインストールの順序に従って適切なコンポーネントを右クリックし、［アンインストール］を選択します。

   SystemEDGE の場合は、設定ファイルを保持するかどうかを指定するダイアログ ボックスが表示されます。

3. ［はい］または［いいえ］をクリックします。

   アンインストール プロセスのチャートを示すダイアログ ボックスが表示されます。アンインストールが完了すると、ダイアログ ボックスが閉じます。

コマンド ラインを使用して SystemEDGE または AIM をアンインストールする方法

1. コマンド プロンプトを開き、DVD1¥Installers¥Windows¥Agent¥SysMan ディレクトリに移動します。以下のサブディレクトリが含まれています。

   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_RM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core

2. 以下のコマンドを実行します。

   ```
   ca-setup -x
   ```

   SystemEDGE の場合は、設定ファイルを保持するかどうかを指定するダイアログ ボックスが表示されます。

3. ［はい］または［いいえ］をクリックします。

   アンインストール プロセスのチャートを示すダイアログ ボックスが表示されます。アンインストールが完了すると、ダイアログ ボックスが閉じます。

SystemEDGE または AIM のサイレント アンインストールを実行する方法

- SystemEDGE をアンインストールするには、以下の手順に従います。

  a. コマンド プロンプト ウィンドウを開き、以下のディレクトリ パスに移動します。

     DVD1¥Installers¥Windows¥Agent¥SysMan¥CA_SystemEDGE_Core

b. 以下のコマンドを実行します。

```
ca-setup.exe CA_SETUP_MODE=UNINSTALL CASE_KEEP_DATA=[YES|NO]
```

SystemEDGE がコンピュータからアンインストールされます。

注: 確認するには、コントロール パネルに移動し、SystemEDGE がコントロール パネルの項目から削除されていることを確認します。

- AIM を削除するには、以下の手順に従います。

a. コマンド プロンプト ウィンドウを開き、以下の適切な AIM ディレクトリ パスに移動します。

DVD1¥Installers¥Windows¥Agent¥SysMan¥*AIM*

b. 以下のコマンドを実行します。

```
ca-setup.exe CA_SETUP_MODE=UNINSTALL
```

AIM がコンピュータからアンインストールされます。

注: ［Program Files］-［CA］-［SystemEDGE］-［plugins］に移動し、AIM フォルダが削除されていることを確認してください。

UNIX システム上の SystemEDGE および AIM のアンインストール

アンインストーラは、システムから SystemEDGE または AIM を削除します。SystemEDGE については、データ ディレクトリから設定データを削除するかどうかを指定できます。

アンインストールするときは、以下の依存関係を考慮してください。

- SRM AIM は Advanced Encryption および SystemEDGE に依存します。
- Advanced Encryption は SystemEDGE に依存します。

これらの依存関係に基づいて、アンインストールの順序は以下のようになります。

1. SRM AIM
2. Advanced Encryption
3. SystemEDGE コア

これ以外の順序ではアンインストールできません。 リモート展開でインストールされたコンポーネントを削除する場合は、Idprimer と CAM はアンインストールされません。

ca-setup.sh を使用してエージェントまたは AIM をアンインストールする方法

1. 端末コンソールを開き、root としてログイン（su）します。
2. DVD2/Installers/<*Platform*>/Agent/SysMan ディレクトリに移動します。以下のサブディレクトリが含まれています。
   - CA_SystemEDGE_SRM
   - CA_SystemEDGE_AdvancedEncryption
   - CA_SystemEDGE_Core
3. 適切なディレクトリに移動し、以下のコマンドを実行します。

   ```
   sh ca-setup.sh -x
   ```

   設定ファイルを保持するかどうかを指定するダイアログ ボックスが表示されます。
4. ［はい］または［いいえ］をクリックします。

   アンインストール プロセスのチャートを示すダイアログ ボックスが表示されます。アンインストールが完了すると、ダイアログ ボックスが閉じます。

lsm を使用してエージェントまたは AIM をアンインストールする方法

1. 端末コンソールを開き、root としてログイン（su）します。
2. 以下のリストから適切なコマンドを選んで実行します。

   ```
   lsm -e CA_SystemEDGE_SRM
   lsm -e CA_SystemEDGE_AdvancedEncryption
   lsm -e CA_SystemEDGE_Core
   ```

   SystemEDGE の場合は、設定ファイルを保持するかどうかを指定するように求められます。
3. ［はい］または［いいえ］をクリックします。

   アンインストールが完了します。

エージェントまたは AIM のサイレント アンインストールを実行する方法

- エージェントをアンインストールするには、以下の手順に従います。
  a. 端末コンソールを開き、root としてログイン（su）します。 以下のディレクトリ パスに移動します。

     DVD2/Installers/*Platform*/Agent/SysMan/CA_SystemEDGE_Core

b. 以下のコマンドを実行します。

```
sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL CASE_KEEP_DATA=[YES|NO]
```

エージェントがコンピュータからアンインストールされます。

- AIM をアンインストールするには、以下の手順に従います。

a. 端末コンソールを開き、root としてログイン（su）します。 以下の適切な AIM ディレクトリ パスに移動します。

DVD2/Installers/*Platform*/Agent/SysMan/*AIM*

b. 以下のコマンドを実行します。

```
sh ca-setup.sh CA_SETUP_MODE=UNATTENDED_UNINSTALL
```

AIM がコンピュータからアンインストールされます。

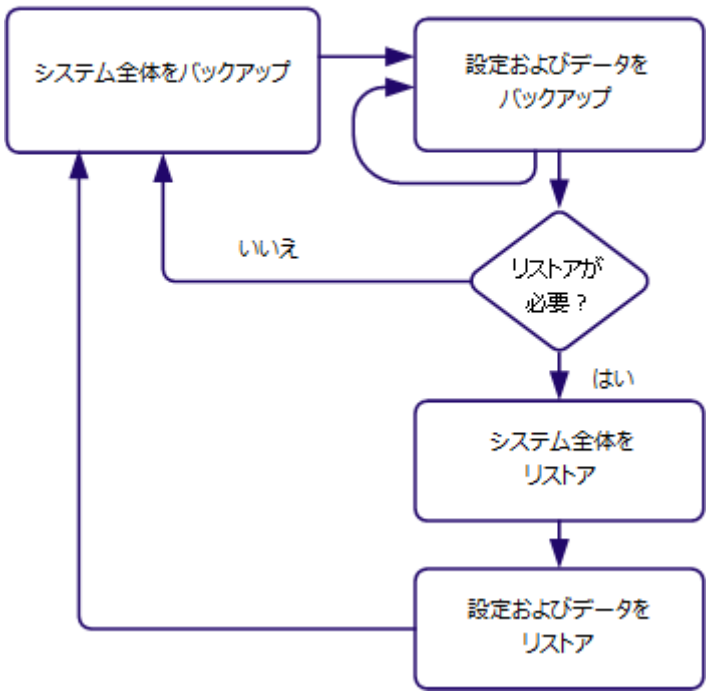
第 6 章: バックアップとリストア

このセクションには、以下のトピックが含まれています。

バックアップおよびリストアの概要

以下のセクションでは、バックアップの 2 つのモードと、対応するリストア プロセスについて説明します。 以下の図は、環境をリストアするために必要な手順の例を示しています。

バックアップおよびリストア プロセス



システムをバックアップするおよび復旧するには、以下の手順に従います。

1. 必要に応じて、システム全体をバックアップ (P. 138) します。
2. 設定とデータをバックアップします。 (P. 140)
3. システムをリストアする場合：
   a. システム全体をリストアします。 (P. 145)
   b. 設定とデータをリストアします。 (P. 146)

システム全体のバックアップ

マネージャ ノードに対して少なくとも週に 1 回はシステム全体のバックアップ（フル）を実行することをお勧めします。 マネージャ ノードは以下のコンポーネントが含まれるすべてのサーバです。

- ドメイン サーバ
- 配布サーバ
- データベース
- EEM サーバ

マネージャ ノードは業界標準ツールを使用してバックアップします（たとえば物理サーバ用に ARCserve、または仮想マシン用にスナップショットを使用）。 複数のマネージャ ノードがある場合は、バックアップがすべてのサーバ上で同時に実行されることを確認します。

バックアップは、ユーザ アクティビティのないときにオフラインで実行することをお勧めします。 バックアップを開始する前に、リモート展開用のアクティブなジョブがすべて完了していることを確認します。

注: ディザスタ リカバリはシステム全体に関係するため、システム上にソフトウェアがある他の製品の所有者にも相談してください。

次の手順に従ってください:

1. ［リソース］-［展開］-［ジョブ］を選択し、すべてのジョブが 100 パーセント完了していることを確認します。
2. 以下のいずれかのオプションを使用して、各サービスを停止します。
   - コマンド ライン インターフェース：
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ
3. 以下の*いずれか*を実行します。
   - マネージャ システム全体のスナップショットを取得します。
   - マネージャ システム全体のゴースト イメージを取得します。
4. 以下のいずれかのオプションを使用して、停止されたサービスを再度開始します。
   - コマンド ライン インターフェース：
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ

注: バックアップがドメイン サーバに接続したマネージャ ノード上で実行されない場合は、配布サービスのみを停止および開始します。

設定とデータのバックアップ

このセクションでは、データベース、キー設定ファイル、およびその他のデータに対する増分バックアップについて推奨される事項を説明します。差分バックアップを少なくとも 1 日に 1 回、使用率が低いとき、またはシステムをオフラインにできるときに実行することをお勧めします。

このセクションでは、以下の手順について説明します。

- データベースのバックアップ (P. 140)
- ディレクトリとデータのバックアップ (P. 141)

データベースのバックアップ

SQL Management Studio を使用すると、管理データベースとパフォーマンス データベースをバックアップできます。

次の手順に従ってください:

1. SQL Server Management Studio を起動します。
2. AOM2 と DPM のデータベースが存在する登録済み SQL Server を展開します。
3. データベースを展開します。
4. データベースを右クリックし、［タスク］-［バックアップ］をクリックします。
5. バックアップ タイプが「フル」に設定され、バックアップの格納場所のパスが指定されていることを確認します。
6. ［OK］をクリックします。

以下の表は、パフォーマンスおよび管理データベースに関する推奨事項を表しています。

データベース	説明	推奨事項
AOM2	管理データベース	増分バックアップ

データベース	説明	推奨事項
DPM	パフォーマンス データベース	パフォーマンス データベースには、エージェントによって収集されたパフォーマンス メトリックが含まれます。 このデータが履歴の観点から不可欠である場合を除き、このデータベースをバックアップすることは推奨されません。

ディレクトリとデータのバックアップ

リモート展開および設定データは、毎日、または会社のバックアップ ポリシーに従ってバックアップすることをお勧めします。

以下の表は、主なディレクトリ、その場所、対応する省略形を示しています。

ディレクトリ	場所の特定方法	省略形
製品インストール ディレクトリ * （32 ビット システムに有効）	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥DynamicProvisioningManager" /v InstallDirectory	<INSTALLDIR>
製品インストール ディレクトリ * （64 ビット システムに有効）	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥ComputerAssociates¥DynamicProvisioningManager"/v InstallDirectory	<INSTALLDIR>
展開および設定のプライベート データ ディレクトリ	Findstr /i "CAISM_PRIVATE_DATA" "<INSTALLDIR>¥bin¥smglobals.ini"	<PRIVATEDATADIR>
展開および設定のパブリック データ ディレクトリ	Findstr /i "CAISM_PUBLIC_DATA" "<InstallDir>¥bin¥smglobals.ini"	<PUBLICDATADIR>

ディレクトリ	場所の特定方法	省略形
IDManager インストール ディレクトリ *（32 ビット システムに有効）	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥InfrastructureDeployment"/v MgrApiPath	<IDDIR>
IDManager インストール ディレクトリ *（64 ビット システムに有効）	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥ComputerAssociates¥InfrastructureDeployment"/v MgrApiPath	<IDDIR>

(*) 注: 64 ビット システム上で 32 ビット コマンド プロンプトを使用

以下の表は、バックアップの推奨事項を示しています。

説明	ディレクトリ	推奨事項
インストーラ設定ファイル	<INSTALLDIR>¥bin¥ smglobals.ini	このファイルは CA Virtual Assurance ディレクトリ設定を定義します。 増分バックアップ セットに推奨されます。
ドメイン サーバ データ	<PRIVATEDATADIR>¥ domainserver	増分バックアップに必要なディレクトリ下で、以下の場所にある展開パッケージを除きます。 <PRIVATEDATADIR>¥domainserver¥Deployment¥Packages¥SM
展開パッケージ	<PRIVATEDATADIR>¥ domainserver¥ Deployment¥ Packages¥SM	バックアップの必要はありません。 インストール メディアから取得できます。
配布サーバ データ	<PRIVATEDATADIR>¥ distributionserver¥	ドメイン サーバと配布サービスが停止されているときにバックアップが実行された場合、バックアップの必要はありません。

説明	ディレクトリ	推奨事項
配布サーバ上の IDManager 設定	<IDDIR>¥config¥SM	増分バックアップに必要です。 リモート配布サーバ上でこの情報をバックアップできず、配布サーバが再インストールされた場合、次の展開時にこの配布サーバを使用して認証情報を再入力します。
Web サービス データ	<PRIVATEDATADIR>¥ caismwebservice	バックアップの必要はありません。 ドメイン サーバから継承されます。
CA Virtual Assurance ログ ファイル	<PUBLICDATADIR>¥log	参照用に必要な場合はバックアップします。
ID ログ ファイル	<IDDIR>¥logs	参照用に必要な場合はバックアップします。

次の手順に従ってください:

1. すべてのアクティブなリモート展開ジョブが完了していることを確認します。
2. 以下のいずれかのオプションを使用して、各サービスを停止します。
   - コマンド ライン インターフェース：
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ
3. 推奨されたディレクトリをバックアップします。
4. 以下のいずれかのオプションを使用して、停止されたサービスを再度開始します。
   - コマンド ライン インターフェース：
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ

システム全体のリストア

次の手順に従ってください:

1. 以下のいずれかのオプションを使用して、各サービスを停止します。
   - コマンド ライン インターフェース：
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ
2. バックアップされたのと同じマシン上で同じバックアップ ツールを使用してリストアを実行します。

   重要: 複数のマネージャ ノードをリストアした場合、データの不整合を回避するため、すべてのシステムを同じバックアップ レベルにリストアします。 ドメイン サーバを含むマネージャ ノードを最後にリストアします。
3. 以下のいずれかのオプションを使用して、停止されたサービスを再度開始します。
   - コマンド ライン インターフェース：
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ

注: バックアップがドメイン サーバに接続したマネージャ ノード上で実行されない場合は、配布サービスのみを停止および開始します。

関連項目

設定とデータのリストア (P. 146)

設定とデータのリストア

システム全体のリストアを実行した後に、差分バックアップ データをリストアします。

このセクションでは、以下の手順について説明します。

- データベースのリストア（P. 146）
- ディレクトリとデータのリストア（P. 147）

関連項目

システム全体のリストア (P. 145)

データベースのリストア

データベースをリストアする場合は、SQL Management Studio を使用します。

次の手順に従ってください:

1. 次のサービスをシャットダウンします： CAAIPApache、CAAIPTomcat、CA SM Distribution Server、CA SM Domain Server
2. SQL Server Management Studio を起動します。
3. データベースが存在する登録済み SQL Server を展開します。
4. データベースを展開します。
5. データベースを右クリックし、［タスク］-［データベースのリストア］をクリックします。
6. データベースを選択します。
7. リストアが作成されるデバイス パスを特定します。
8. ［OK］をクリックします。
9. サービスを再起動します： CAAIPApache、CAAIPTomcat、CA SM Distribution Server、CA SM Domain Server

ディレクトリとデータのリストア

設定とデータのファイルは、バックアップされたマシンと同じマシン上で同じバックアップ メディアからリストアします。

次の手順に従ってください:

1. ［リソース］-［展開］-［ジョブ］を選択し、アクティブな展開ジョブが進行中でないことを確認します。
2. 以下のいずれかのオプションを使用して、各サービスを停止します。
   - コマンド ライン インターフェース：
     ```
     net stop CASMDmnSrvr
     net stop CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ
3. 同じバックアップ メディアから設定およびデータのファイルをリストアします。

   注: リストア処理は、最後にバックアップされたときと同じ状態に情報を戻します。最後のバックアップ以降に行なわれた変更はすべて失われます。
4. 複数のマネージャ ノードがバックアップされた場合は、他のマネージャ ノードのリストアを続行します。
5. 以下のいずれかのオプションを使用して、停止されたサービスを再度開始します。
   - コマンド ライン インターフェース：
     ```
     net start CASMDmnSrvr
     net start CASMDstrbnSrvr
     ```
   - Windows サービス コントロール マネージャ：
     - CA SM ドメイン サーバ
     - CA SM 配布サーバ

注: バックアップがドメイン サーバに接続したマネージャ ノード上で実行されない場合は、配布サービスのみを停止および開始します。

第 7 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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. 152)
2. ハードウェアの仕様 (P. 150)
3. データベースに関する考慮事項 (P. 151)
4. ネットワークに関する考慮事項 (P. 152)
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. 154)
6. スケーラビリティに関する使用事例 (P. 163)

ハードウェアの仕様

このセクションでは、CA Virtual Assurance 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 Virtual Assurance 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。

ネットワークに関する考慮事項

CA Virtual Assurance 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。

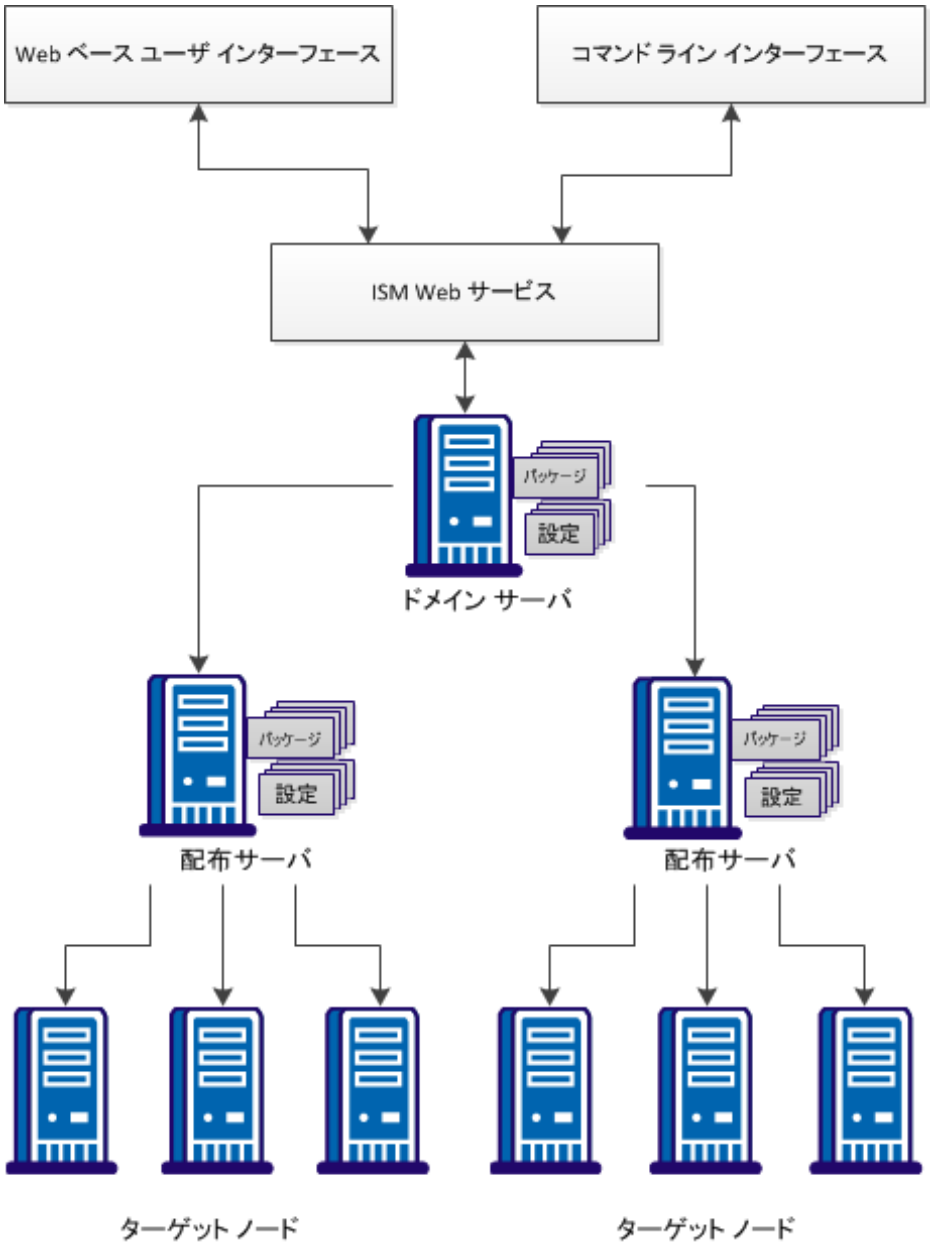
リモート展開およびポリシー設定の概要

CA Virtual Assurance 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 Virtual Assurance 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. 154）
- VMware 環境の CA Virtual Assurance 管理（P. 156）
- リモート展開およびポリシー設定に関する推奨事項（P. 160）
- ドメイン サーバに関する推奨事項（P. 162）
- 配布サーバに関する推奨事項（P. 163）
- スケーラビリティに関する使用事例（P. 163）

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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance vCenter 管理の推奨事項

CA Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance、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 Virtual Assurance、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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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 Virtual Assurance 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。

用語集

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。

Hyper-V

Hyper-V は、Windows Server 2008 R2 用の Microsoft ハイパーバイザベースのサーバ仮想化テクノロジです。複数の独立した仮想マシン（VM）が 1 台の物理サーバ上で実行され、Windows や Linux などの複数の異なるオペレーティング システムを実行できます。

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。

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。

VA--ADES AIM

Active Directory および Exchange Server 用の AIM を使用すると、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 環境と Exchange Server 環境をモニタできます。 この AIM は、AD 環境と ES 環境の設定、およびキー パフォーマンス インジケータのモニタリングを可能にします。

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。

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。

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。

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 Virtual Assurance 管理データベースに格納します。

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。

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。

索引

V

W

あ

か

さ

た

な

は

ま

や

ら