

CA Virtual Assurance for Infrastructure Managers

インストール ガイド

リリース 12.6



このドキュメント(組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」)は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社(以下「CA」)により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

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

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

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

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

本ドキュメントの制作者は CA です。

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

Copyright © 2011 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

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 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 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	9
スコープ	9
対象読者	9
関連ドキュメント	10
規則	11
 第 2 章: インストールの準備	 13
前提条件	13
製品コンポーネント.....	13
マネージャ コンポーネント.....	14
エージェント コンポーネント.....	15
CA Virtual Assurance コンポーネント間の依存関係	17
CA Virtual Assurance と外部コンポーネントの間の依存関係.....	18
 第 3 章: CA Virtual Assurance のインストール	 19
インストールの要件および考慮事項	19
SQL Server を使用するための要件の確認.....	20
Microsoft Hyper-V を使用するために必要な設定の適用	22
SystemEDGE と CA Performance LiteAgent の比較	23
セキュリティに関する考慮事項	25
Windows メモリ管理の最適化	25
標準インストールとカスタム インストール	25
インストール オプション	26
標準インストールの準備	27
カスタム インストールの準備	28
インストールの実行	31
インストールのキャンセル	34
初期インストール後のコンポーネント インストール	34
ログイン パスワードの変更.....	35
Embedded Entitlements Manager 管理者パスワード (EiamAdmin) の変更.....	36
マネージャのサイレント インストール	37

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	37
silent.properties ファイルの編集	38
マネージャのサイレント インストールの実行	39
複数のサーバへのカスタム インストール	40
複数のサーバへインストールする場合のガイドライン	40
通信ポート	43
エージェントの展開	46
展開ジョブの作成	47
エージェントの個別インストール	49
SystemEDGE コンポーネントの依存関係	49
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	50
Windows システムでのインストール	52
UNIX システムでのインストール	67
応答ファイルの設定と使用	81
レガシー モードでのエージェントのインストール	82
AIM のインストール	83
CA Performance LiteAgent のインストール	85

第 4 章: CA Virtual Assurance のアップグレード 87

サポートされているアップグレード	87
CA Virtual Assurance のアップグレード方法	88
アップグレードドキュメントの確認	89
アップグレード対象環境の準備	90
メンテナンス期間の設定	91
重要なパッチの適用	91
システム全体のバックアップ	92
複数 Apache 設定の単一 Apache 設定への切り替え	93
サービスの停止	93
アップグレード制限の確認	94
リモート Embedded Entitlements Manager の手動アップグレード	95
マネージャ インストールの実行	96
自動的にアップグレードされなかった古い設定の確認	97
古い設定の手動適用	98
管理対象ノードおよび AIM サーバのアップグレード	98
エージェントと AIM のアップグレード	99
ポリシーへの SystemEDGE モニタのインポート	103

使用環境での CA Virtual Assurance アップグレードの確認.....	104
---	-----

第 5 章: ユーザ インターフェースの使い方 105

CA Virtual Assurance の起動	105
機能の概要	106
AutoShell の開始	107
有効な AutoShell ユーザ	109
CA Virtual Assurance コマンド プロンプトの起動.....	109
マニュアル選択メニューとオンライン ヘルプの起動	110

第 6 章: CA Virtual Assurance のアンインストール 111

アンインストール オプション	111
マネージャのアンインストール	112
完全アンインストールの実行.....	112
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.....	113
サイレント モードでのマネージャのアンインストール.....	114
SystemEDGE のアンインストール	114
Windows 上の SystemEDGE および AIM のアンインストール.....	114
UNIX システム上の SystemEDGE および AIM のアンインストール	116

第 7 章: バックアップとリストア 119

バックアップおよびリストアの概要.....	119
システム全体のバックアップ	120
設定とデータのバックアップ	122
データベースのバックアップ	122
ディレクトリとデータのバックアップ	123
システム全体のリストア	126
設定とデータのリストア	127
データベースのリストア	127
ディレクトリとデータのリストア	128

用語集	129
索引	135

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ます。分析により、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、変更の自動検出を支援します。

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](#) (P. 9)

[対象読者](#) (P. 9)

[関連ドキュメント](#) (P. 10)

[規則](#) (P. 11)

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、仮想化テクノロジー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、MIB 属性、およびパフォーマンス メトリックに関する詳細情報を提供します。

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について説明します。

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

ほかのガイド、またはこのガイドのほかのセクション内の情報へ参照は、以下の形式で記述されます。

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に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 *sysedge_home* 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：インストールの準備

この章では、CA Virtual Assurance のインストールを成功させるための前提条件およびコンポーネントの依存関係について説明します。

このセクションには、以下のトピックが含まれています。

[前提条件](#) (P. 13)

[製品コンポーネント](#) (P. 13)

[CA Virtual Assurance コンポーネント間の依存関係](#) (P. 17)

[CA Virtual Assurance と外部コンポーネントの間の依存関係](#) (P. 18)

前提条件

CA Virtual Assurance のインストールを開始する前に、以下の前提条件を確認してください。

- CA Virtual Assurance を適切にインストールするための、DVD または ISO イメージへの完全なアクセス
- Windows 環境に CA Virtual Assurance をインストールするための管理者権限
- Linux または UNIX の環境に CA Virtual Assurance コンポーネントをインストールするためのスーパーユーザ (su)、root、または sudo 権限

製品コンポーネント

このセクションでは、CA Virtual Assurance コンポーネントを一覧表示し、それぞれについて簡単に説明します。

マネージャ コンポーネント

インストールした CA Virtual Assurance マネージャ、以下のコンポーネントグループで構成されます。

グラフィカル ユーザ インターフェース

CA Virtual Assurance および他の統合される CA 製品を一元的にモニタリング、管理するための Web ベース ユーザ インターフェースです。

Automation Management Framework

CA Virtual Assurance のビジネス主導オートメーションのフレームワークコンポーネントを提供します。主要コンポーネントは CA Virtual Assurance の全コンポーネントの中央レジストリです。このコンポーネントは、通信の管理および方向づけを行い、サービスの受信/送信要求を処理します。他のコンポーネントには、システム エージェントからシステム メトリックを収集する中央エンジン、エンタープライズリソース管理などがあります。

パフォーマンス管理とモニタリング

システムとサービスのパフォーマンスをモニタおよび管理する機能を提供します。

- システム パフォーマンス管理 (SystemEDGE)
- リモート モニタリング
- サービスレスポンス モニタリング
- CA Performance LiteAgent

仮想システム管理とモニタリング

仮想環境を管理するためのコンポーネントを提供します。

- Microsoft Hyper-V Server
- AIX の論理パーティション
- Microsoft Cluster Server モニタリング
- VMware vCenter Server および関連付けのある VMware ESX Server ベース仮想インフラストラクチャ
- Solaris ゾーン サーバ
- Cisco Unified Computing System (UCS)

プロビジョニング マネージャ

VMware vCenter Server とシームレスに連携して OS イメージングおよび基本的なシステム管理を実現するのに使用されるイメージング コンポーネントを提供します。

モニタリング、展開、ポリシー設定

リモート展開およびポリシーベースの設定を行うためのコンポーネントを提供します。

統合とツール

ヘルプ デスク マネージャおよびすべての AutoShell コンポーネントとの統合機能を提供します。

AutoShell および CLI

高度なスクリプティング機能を提供します。

ヘルプ

製品ドキュメントおよび状況依存オンライン ヘルプ (マニュアル選択メニュー) を提供します。

エージェント コンポーネント

CA Virtual Assurance には以下のエージェント コンポーネントがあります。

SystemEDGE

業界標準の SNMP インターフェースを介して強力なシステム管理を実現します。

Cisco UCS AIM

Cisco Unified Computing System を管理およびモニタする機能を提供します。

LPAR AIM (AIX PowerVM)

LPAR を含むシステム全体を管理およびモニタする機能が備わっています。

Microsoft クラスタ サーバ AIM

リモートシステムから **Microsoft** クラスタをモニタします。**MSCS** をモニタするには、**CPU** およびメモリ使用率などのメトリック収集用のクラスタおよび個々のクラスタ ノードへのリモートアクセスが必要です。

Microsoft Hyper-V AIM

Hyper-V Server を管理およびモニタする機能が備わっています。

Solaris ゾーン AIM

コンテナとゾーンを実行するように設定された **Solaris 10** システムを管理およびモニタする機能が備わっています。

VMware vCenter AIM

VMware vCenter Server の管理下にあるシステムを管理およびモニタする機能を提供します。

リモート モニタリング AIM

エージェントなしでシステムを管理およびモニタする機能を提供します。

サービス レスポンス モニタリング AIM

サービスの可用性をモニタするためのテストを提供します。

CA Performance LiteAgent

軽量なモニタリング エージェントである **CA Performance LiteAgent** を使用すると、**Windows** および **UNIX/Linux** 上の大量のパフォーマンス メトリックにアクセスできます。

Exchange Server および Active Directory 用 AIM

Exchange Server および **Active Directory** 用 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における **Exchange Server** 環境と **Active Directory** 環境をモニタできます。この AIM は、**Exchange Server** 環境と **Active Directory** 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。

CA Virtual Assurance コンポーネント間の依存関係

関連付けられている条件が満たされていると、以下のコンポーネントがインストールされます。**Embedded Entitlements Manager** の既存バージョンがインストールされている場合は、それを使用することもできます。詳細については、「リリースノート」を参照してください。

注: 追加コンポーネントのサポート対象バージョンについては、「リリースノート」を参照してください。

Apache Tomcat

以下のコンポーネントをインストール対象に選択すると、**Tomcat** がインストールされます (あるいは、現在のバージョンがすでにインストールされている場合は、**CA Virtual Assurance** 用に設定されます)。

- グラフィカル ユーザ インターフェース フレームワーク

Apache HTTP サーバ

以下の 1 つ以上のコンポーネントをインストール対象に選択すると、**Apache** がインストールされます。

- AIP フレームワーク
- プロビジョニング マネージャ

管理データベース

以下の 1 つ以上のコンポーネントをインストール対象に選択すると、管理データベース情報が要求またはインストールされます。

- AIP フレームワーク
- グラフィカル ユーザ インターフェース フレームワーク

パフォーマンス データベース

以下の 1 つ以上のコンポーネントをインストール対象に選択すると、パフォーマンス データベースがインストールされます。

- AIP フレームワーク
- グラフィカル ユーザ インターフェース フレームワーク

CA Embedded Entitlements Manager (Embedded Entitlements Manager)

以下の 1 つ以上のコンポーネントをインストール対象に選択すると、**Embedded Entitlements Manager** がインストールされます。

- AIP フレームワーク
- グラフィカル ユーザ インターフェース フレームワーク

注: 1 台の **Embedded Entitlements Manager** サーバがサポートする **CA Virtual Assurance** マネージャ インストールは 1 つです。

CA Virtual Assurance と外部コンポーネントの間の依存関係

CA Virtual Assurance の全機能を使用するには、特定の外部コンポーネントについて、このセクションに示す依存関係を考慮してください。これらのコンポーネントは、**CA Virtual Assurance** のインストールに含まれず、独自のインストールプログラムがあります。

注: コンポーネントの詳細については、「管理ガイド」を参照してください。

ヘルプ デスク マネージャ

CA Service Desk との統合を実現し、ヘルプ デスク チケットのステータスのオープン、更新、およびモニタリングをサポートします。コンポーネントのインストール中またはインストール後に、**CA Virtual Assurance** について **CA Service Desk** アクセスを指定できます。

System Center Virtual Machine Manager (Microsoft SCVMM 仮想化)

CA Virtual Assurance は **Microsoft SCVMM** と統合することで、**SCVMM** のモニタリング、管理、およびプロビジョニング サービスを実現します。

第 3 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](#) (P. 19)

[標準インストールとカスタム インストール](#) (P. 25)

[マネージャのサイレント インストール](#) (P. 37)

[複数のサーバへのカスタム インストール](#) (P. 40)

[エージェントの展開](#) (P. 46)

[エージェントの個別インストール](#) (P. 49)

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 のインストール計画にとって重要な情報を提供します。

SQL Server を使用するための要件の確認

CA Virtual Assurance は、その管理データベースとパフォーマンス データベースに SQL Server を必要とします。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。
- 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。

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、代替方法として DVD1 から SQL Server Express をインストールすることもできます。

CA Virtual Assurance ローカル アクセスのために SQL Server Express をインストールおよび設定するには、以下のタスクを実行します。

- 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。
- 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。
- 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])。
- 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。

リモートの SQL Server にアクセスする予定の場合は、CA Virtual Assurance マネージャ コンピュータに SQL Server クライアントをインストールします。リモート SQL Server 上でリモート接続が有効にされている必要があります。

関連項目

[SQL Server を使用するための要件の確認](#) (P. 20)

Microsoft Hyper-V を使用するために必要な設定の適用

前提条件を確認し、Microsoft Hyper-V 管理用の以下の設定を適用します。

Microsoft Hyper-V を使用するために必要な設定を適用する方法

1. SystemEDGE、Advanced Encryption、および Hyper-V AIM が Hyper-V Server にインストールされていることを確認します。各管理対象 Hyper-V Server に割り当てることのできる AIM は 1 つだけです。
2. Hyper-V Server 上でローカルのユーザ アクセス制御 (UAC) を無効にします。
3. 以下のレジストリ値を設定してネットワーク UAC を無効にします。
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy,1 (REG_DWORD)`
4. コマンドプロンプトから以下のコマンドを実行して、リモート WMI ファイアウォール例外を有効にします。

`netsh advfirewall firewall set rule group="Windows Management Instrumentation (WMI)" new enable=yes`
5. サーバ アクセス用の管理コンポーネントで設定されたユーザが「Distributed COM Users」グループのメンバであることを確認します。

SystemEDGE と CA Performance LiteAgent の比較

CA Virtual Assurance には、SystemEDGE と CA 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 Performance LiteAgent は、Windows、UNIX、および Linux 上の大量のパフォーマンス 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、これには、パフォーマンスレジストリに含まれるほとんどすべてのメトリックをモニタする機能も含まれます。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 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 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 エージェント	CA Performance LiteAgent
SNMP 準拠のエージェント	Y	N
SNMP ベースのトラップ	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の制限	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
eHealth のサポート	Y	N

機能	SystemEDGE エージェント	CA Performance LiteAgent
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
Host Resource 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
UNIX または Linux の広範囲のモニタリング	Y	Y
真の平均パフォーマンス 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
Exchange Server および Active Directory に対するサポート	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 Performance LiteAgent は、あらゆる Windows パフォーマンス メトリックを動的にモニタする機能を備えています。

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 Assurance AIM 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。

標準インストールとカスタム 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 オプション

Windows オペレーティング環境での CA Virtual Assurance のインストール オプションは以下のとおりです。

標準インストール

すべての前提条件が満たされているマネージャ コンポーネントとクライアント コンポーネントをすべてインストールします。このオプションは、環境とシステム設定に関して以下の事項を前提とすることにより、インストール処理を効率化します。

- 管理データベースとパフォーマンス データベースは同じコンピュータ上にインストールされます。データベースはローカル システムまたはリモートシステムに常駐できます。
- Embedded Entitlements Manager は CA Virtual Assurance マネージャシステムにインストールされます。Embedded Entitlements Manager がすでにインストールされている場合は、インストール プログラムによってカスタム インストールが自動的に起動されます。
- Apache サーバは SSL に対応しており、ポート 443 でリスンします。
- Apache Tomcat は SSL に対応しており、ポート 8443 でリスンします。シャットダウン ポートとコネクタ ポートはデフォルトのポート 8005 が使用されます。
- AIM と統合はインストール後に設定できます。
- カスタム インストール中に指定できるアカウントおよびパスワードはすべて、ca_admin に設定されます。

注: インストール後は Embedded Entitlements Manager 内でデフォルトパスワードを変更してください。

このオプションを選択するのは、以下の状況の場合です。

- CA Virtual Assurance アーキテクチャに関する深い知識がない。
- 同じコンピュータにすべての管理コンポーネントをインストールしても、負荷の共有は問題にならない。

カスタム インストール

CA Virtual Assurance を柔軟にインストールできます。インストール、管理、または統合するコンポーネントを指定できます。

このオプションを選択するのは、以下の状況の場合です。

- インストール中に、アカウント、パスワード、またはポートを指定したい。
- 分散インストールを実装したい。たとえば、管理データベース、パフォーマンス データベース、Embedded Entitlements Manager、または配布サーバを別個のシステムにインストールする場合です。
- 必要な機能だけインストールしたい。たとえば SystemEDGE と CA Virtual Assurance の AIM だけをインストールする場合です。
- インストール中に AIM および統合を設定したい。

関連項目

[標準インストールの準備 \(P. 27\)](#)

[複数のサーバへインストールする場合のガイドライン \(P. 40\)](#)

[エージェントの個別インストール \(P. 49\)](#)

標準インストールの準備

マネージャ コンポーネントとクライアント コンポーネントのすべてを 1 台のシステムにインストールする場合は、標準インストール オプションを使用します。インストール ウィザードでは、以下の環境関連のデータが要求されます (カッコ内はデフォルト値)。

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)
vCenter Server	X	X	X	X (HTTPS)	X (443)
SystemEDGE (2)	-	-	-	-	X (161、162)

(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: 1 GB (小)、5 GB (中)、または 10 GB (大)

(2) コミュニティ文字列(public/snmp_admin)。

注: 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。

関連項目

[ログインパスワードの変更](#) (P. 35)

[Embedded Entitlements Manager 管理者パスワード\(EiamAdmin\)の変更](#) (P. 36)

カスタム インストールの準備

カスタム インストール オプションでは、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。カスタム インストール中、インストールウィザードには、選択したコンポーネントをインストールするのに必要なダイアログ ボックスだけが表示されます。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(カッコ内はデフォルト値)。

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	-	-
Active Directory セキュリティ (5、6)	X	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
システム ユーザ	-	sys_service	X	-	-
Network Discovery Gateway	-	-	-	-	X (8082)
ネットワーク ディスカバリ (7) ゲートウェイ サービス アカウ ント	-	X	X	-	-
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	-	-	-	X (61616)
ヘルプ デスク (Service Desk 統合)	X	X	X	X (HTTP)	X (8080)
HMC/IVM サーバ (LPAR)	X	X	X	-	-
Solaris ズーン サーバ	X	X	X	-	-
vCenter Server	X	X	X	X (HTTPS)	X (443)
SCVMM	X	X	X	-	-
Hyper-V Server	X	X	X	-	-
Cisco Unified Computing System (8)	X	X	X	X (HTTP)	X (80)
配布サーバ (9)	X	-	-	-	-
SystemEDGE (10)	-	-	-	-	X (161、162)
リモート モニタリング	-	X	X	-	-
Microsoft Cluster Server	X	X	X	-	-

(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: 1 GB (小)、5 GB (中)、または 10 GB (大)

(2) **Embedded Entitlements Manager** 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** インスタンスがすでに存在する場合は、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 **Embedded Entitlements Manager** 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。 <EMM> ユーザ インターフェースを開き、[設定] タブを開いて、[登録解除] をクリックします。
- **CA Virtual Assurance** によって **Embedded Entitlements Manager** をローカルシステムにインストールさせます。

(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。

(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。

(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。

(7) 以下のいずれかのオプションを選択します。

- ローカル システム アカウント(デフォルト)。
- ユーザ名とパスワードを入力して、「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。

(8) **AIM** ホスト名、**SNMP** バージョン、および **SNMP** ポートも必要です。

(9) リモート サーバへの配布サーバのインストール中、またはインストール後にシステム管理ドメイン用のホスト名を指定します。

(10) コミュニティ文字列がデフォルトで使用されます (読み取り専用、読み取り/書き込み): `public`、`snmp_admin`

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。以下のインストール手順では、完全カスタム インストールについて説明します。

インストール中にコンポーネントの設定を省略した場合、グラフィカル ユーザ インターフェースの[管理]タブからコンポーネントを設定できます。ローカル システム上の AIM もインストール後に `NodeCfgUtil` を使用して設定できます。

`NodeCfgUtil` プログラムは、<インストールパス

>`¥SystemEDGE¥plugins¥AIPCommon` ディレクトリにあります。詳細については、「[管理ガイド](#)」を参照してください。

注: 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。

関連項目

[ログイン パスワードの変更](#) (P. 35)

[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. 50)

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。インストール時にコンポーネントをスキップした場合、インストール後にそのコンポーネントを設定できます。グラフィカル ユーザ インターフェースの[管理]タブ、または `dpmutil` ユーティリティを使用します。詳細については、「[管理ガイド](#)」を参照してください。

インストールを実行する方法

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。

[はじめに]ダイアログ ボックスが表示されます。

2. [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。

3. 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 タイプを選択するダイアログ ボックスが表示されます。

4. 標準またはカスタムのインストールを選択し、[次へ]をクリックします。

CA eHealth または CA eHealth TrapEXPLODER がインストールされている場合は、メッセージが表示され、インストール処理は終了します。別のコンピュータに CA Virtual Assurance をインストールするか、他の CA プログラムを削除して CA Virtual Assurance のインストールを再開します。

CA eHealth も CA eHealth TrapEXPLODER もインストールされていない場合は、[インストール フォルダの選択]ダイアログ ボックスが表示され、デフォルトのインストール場所が示されます。

5. 以下のいずれかを実行します。

- [次へ]をクリックしてデフォルトの場所にインストールします。

- [選択]をクリックして新規フォルダ場所を参照し、[OK]をクリックします。

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「;」。

[ランタイム ロケール]ダイアログ ボックスが表示されます。

6. アクティブにする追加のロケールを 1 つ指定し、[次へ]をクリックします。

デフォルト: 英語(米国)

管理データベース接続情報のダイアログ ボックスが表示されます。

7. SQL Server 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、SQL 管理者ユーザ名、パスワード、またはポート番号(1433)を変更します。[次へ]をクリックします。

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 \(P. 20\)](#)」を参照してください。

8. インストール ウィザードの指示に従い、インストールを完了するために必要とされる値、名前、およびパスワードを入力します。インストール ウィザードで要求されるデータについては、「[標準インストールの準備 \(P. 27\)](#)」および「[カスタム インストールの準備 \(P. 28\)](#)」で詳しく説明しています。

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。

9. [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。

インストールパス¥VirtualAssurance¥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。標準インストールの場合、デフォルト ユーザ名とパスワードも示されます。

ユーザ名: admin

パスワード: ca_admin

10. 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。
11. [スタート]、[プログラム]、[CA]、[CA Virtual Assurance]、[CA Virtual Assurance の起動]に移動し、デフォルトの認証情報 admin/ca_admin を使用してユーザ インターフェースにログインします。

重要: 標準インストールでは、インストールした CA Virtual Assurance コンポーネントのログイン ユーザ名とすべてのパスワードが admin/ca_admin に設定されます。セキュリティ上の理由により、初回ログイン後はこれらのパスワードを変更することを強くお勧めします。

12. 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 (インストール パス `¥VirtualAssurance¥log¥install¥install.log`) およびエラー リスト (インストール パス `¥VirtualAssurance¥log¥install¥install_error_detected.log`) を参照してください。

関連項目

[ログイン パスワードの変更](#) (P. 35)

[Embedded Entitlements Manager 管理者パスワード \(EiamAdmin\) の変更](#) (P. 36)

[標準インストールの準備](#) (P. 27)

[カスタム インストールの準備](#) (P. 28)

[SQL Server を使用するための要件の確認](#) (P. 20)

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

初期インストール後、インストール プログラムを実行して、同じ製品内の新しいコンポーネントをインストールします。初期インストール後にインストール プログラムを実行しても、既存のコンポーネントは再インストールされません。また、既存のコンポーネントを新しいデータで修復または再設定されることもありません。

ログイン パスワードの変更

CA Virtual Assurance ユーザおよび管理者にとって安全で適切なログイン認証情報を指定することは重要です。特に標準インストールの完了後は、デフォルトのログイン情報 `admin/ca_admin` を変更する必要があります。そのためには、CA Virtual Assurance と共にインストールされる CA Embedded Entitlements Manager を使用します。

ログイン パスワードを変更する方法

1. [スタート]、[プログラム]、[CA]、[Embedded Entitlements Manager]、[EEM UI]に移動し、ユーザ インターフェースを開きます。
ログイン ダイアログ ボックスが表示されます。
2. デフォルト パスワード (`ca_admin`) でログインします。
ユーザ インターフェースが開きます。
3. [ID の管理およびユーザの検索]をクリックします。
[ユーザ] ペインにユーザが表示されます。
4. 管理者ユーザをクリックします。
右側のペインにユーザのプロパティが表示されます。
5. [認証] セクションまでスクロールし、[パスワードのリセット] をクリックします。
[新しいパスワード] フィールドと [パスワードの確認] フィールドが表示されます。
6. パスワードを入力し、[保存] をクリックします。
これで、新しいパスワードで CA Virtual Assurance にログインできます。

CA Virtual Assurance にユーザを追加して管理するには、CA EEM を使用します。CA EEM のユーザドキュメントまたはオンライン ヘルプ システムを参照してください。

重要: EiamAdmin ユーザのデフォルト パスワード (`ca_admin`) も変更します。

関連項目

[Embedded Entitlements Manager 管理者パスワード \(EiamAdmin\) の変更](#) (P. 36)

Embedded Entitlements Manager 管理者パスワード(EiamAdmin)の変更

Embedded Entitlements Manager 管理者パスワード(EiamAdmin)を変更する場合は、Embedded Entitlements Manager でパスワードを変更し、さらに CA Virtual Assurance でも変更します。

Embedded Entitlements Manager で管理者パスワード(EiamAdmin)を変更する方法

1. [スタート]-[プログラム]-[CA]-[Embedded Entitlements Manager]-[EEM UI]に移動し、ユーザ インターフェースを開きます。
[ログイン]ダイアログ ボックスが表示されます。
2. 現在の EiamAdmin パスワードでログインします。
ユーザ インターフェースが開きます。
3. [設定]および[EEM サーバ]をクリックします。
[EEM サーバ]ペインが表示されます。
4. [EiamAdmin パスワード]をクリックします。
[新しいパスワード]および[パスワードの確認]フィールドが表示されます。
5. パスワードを入力し、[保存]をクリックします。
これで、新しい EiamAdmin パスワードを使用して Embedded Entitlements Manager にログインできます。

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

1. [スタート]-[プログラム]-[CA]-[CA Virtual Assurance]-[CA Virtual Assurance コマンド プロンプト]に移動します。
コマンド プロンプトが表示されます。

2. 以下のコマンドを入力します。

```
dpmutil -set -eiam
```

dpmutil コマンドが、必要な認証情報の入力を要求します。

情報を入力してコマンドを完了します。

3. CAAIPApache および CAIPTomcat サービスを再利用します。

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

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

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する必要があります。

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 Windows x64 システムではないことと、「リリース ノート」に記載された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 \(P. 37\)](#)
[マネージャのサイレント インストールの実行 \(P. 39\)](#)

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をホストするサポート対象サーバにコピーする必要があります。

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、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。

インストール メディアからサイレント インストール ファイルをコピーする方法

1. DVD1 の Installers ディレクトリを、ディレクトリ構造を維持したままターゲットコンピュータにコピーします。
2. DVD または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。

ホストサーバ上の `silent.properties` ファイルは、次のセクションで説明するとおりに編集できます。

レスポンス ファイルを編集したら、次のセクションで説明するサイレント インストールの手順を開始できます。

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。

silent.properties ファイルを編集する方法

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¥¥VirtualAssurance`

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。

マネージャのサイレント インストールを実行する方法

1. 管理者としてログインし、DVD1 の全ファイルを、ディレクトリ構造を維持したままターゲット システムにコピーします。
2. *silent.properties* ファイルを編集して保存し、必要なコンポーネントをインストールします。

注: レスポンス ファイルには、編集のための詳しい指示が記述されています。

3. 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。

4. ¥¥Installers¥¥Windows¥¥ ディレクトリに移動し、次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。

5. インストールが完了したら、インストール パス¥¥VirtualAssurance¥¥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. 37)

[silent.properties ファイルの編集](#) (P. 38)

複数のサーバへのカスタム インストール

デフォルト設定に基づいた標準インストールまたはカスタム 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、カスタム インストールでは、必要な CA Virtual Assurance コンポーネントをすべて別のサーバにインストールできるようにする高度な柔軟性が提供されています。

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. 40)

[エージェントの個別インストール](#) (P. 49)

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 コンポーネントを別のサーバにインストールするには、各サーバ上でカスタム インストールを実行します。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。製品のインストール後、CA SM ドメイン サーバ、CAAIPACHE サービス、および CAAIPTOMCAT サービスが、このドメイン ユーザ アカウントに対して設定されていることを確認します。サービスを再設定しなかった場合、CA Virtual Assurance ユーザ インターフェースは機能しません (ダッシュボードが空であるか、機能が動作しない)。
- これらの条件は SQL Server 認証では必要ありません。

Windows 認証用に SQL Server リモート アクセスを設定する方法

1. [コントロール パネル] の [管理ツール] から [サービス] ダイアログ ボックスを開きます。
使用可能なサービスのリストが表示されます。
2. CA SM ドメイン サーバ、CAAIPACHE サービス、および CAAIPTOMCAT サービスの [プロパティ] ダイアログ ボックスを開きます。
3. 各ダイアログ ボックスの [ログオン] タブに移動し、[次のアカウント] を選択します。次に、参照できる有効な認証情報 (ドメイン ユーザ アカウント) を入力します。
4. このドメイン ユーザ アカウントを両方のシステム (マネージャ サーバとデータベース サーバ) のローカル Administrators グループに追加します。
5. このドメイン ユーザ アカウントを SQL Server の sysadmin (または dbcreator 以上) のサーバ役割に追加します。

注: コンポーネント間の依存関係の詳細については、このガイドの「CA Virtual Assurance コンポーネント間の依存関係」を参照してください。

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

[CA Virtual Assurance コンポーネント間の依存関係](#) (P. 17)

[CA Virtual Assurance と外部コンポーネントの間の依存関係](#) (P. 18)

[通信ポート](#) (P. 43)

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。

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

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

WMI ポート: 135

CA Performance LiteAgent

CAM UDP ポート: 4104

CAM TCP ポート: 4105

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

WMI ポート: 135

SNMP スタック

UDP ポート: 161、1691、162 (トラップ、受信)

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

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。カスタマイズ済みのインストール パラメータを含む提供パッケージに基づいて展開テンプレートを作成し、これらのテンプレートを多数の管理対象システムに同時に展開できます。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
- 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 Performance LiteAgent
- CA IBM LPAR AIM
- 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 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 5.6 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 5.6 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バージョン 5.6 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。

展開ジョブを作成する方法

1. [リソース]-[展開] を選択します。
[展開] ペインに [パッケージ]、[テンプレート]、および [ジョブ] フォルダが表示されます。
2. [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 ウィザードが表示されます。
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]リンクをクリックします。[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は「不完全」または「無効」な状態であってもかまわず、インライン編集によって修正できます。[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。次に、[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場合があります。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. 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。すぐに実行するか、特定の時間だけずらして実行するか、または将来の特定の時間にスケジュールして実行します。

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. エンド ユーザ使用許諾契約 (EULA) を読み、[すべてのパッケージについて EULA に同意する]チェックボックスをオンにします。ジョブの作成に同意して続行します。

14. ジョブの詳細を確認し、[展開]をクリックします。

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。

- 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)
- IBM LPAR 用の AIM (Windows)
- Microsoft Hyper-V 用の AIM (Windows)
- Microsoft Cluster Service サポート用の AIM (Windows)
- Solaris ゾーン用の AIM (Windows)
- Cisco UCS 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)
- Exchange Server および Active Directory 用 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 を使用できるのは、SystemEDGE および Advanced Encryption がインストールされているシステムだけです。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 (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)。

- 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が必要な場合、リモート展開とポリシー設定を使用する方法をお勧めします。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. 82)

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。

Windows にエージェントをインストールする方法

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、下にスクロールして[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。

コマンドラインからの Windows へのエージェント 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場合は、パラメータを使用してさまざまなインストール 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 ウィザードを開始します。インストール パラメータをあらかじめ入力しておくことも、パラメータなしで開始することも可能です。
- インストール パラメータを指定し、対話型ウィザードを使用せずにインストーラを実行します。

この手順では 2 番目のシナリオである、コマンドラインから無人インストールを実行する方法について説明します。

コマンドラインから Windows にエージェントをインストールする方法

1. Windows システムに管理者としてログオンします。

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表示するには、「ca-setup -?」とコマンド 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。インストールをサイレント モードで実行するには、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、コマンドを実行した後に、指定したパラメータ値があらかじめ入力された状態でインストール ウィザードが開かれます。

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は、省略した場合、値を指定する必要はありません。

```
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、詳細なインストール モードがオンになります。詳細モードでは、より多くの情報がインストール ログ ファイルにログ記録されます。

CASE_INSTALLDIR

SystemEDGE インストール ディレクトリを指定します(このドキュメント内では、SystemEDGE インストール ディレクトリを、変数 **CASYSEDGE** と呼んでいます)。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 を使用してエージェントをクエリすることを許可された **SNMP** マネージャの (スペースで区切られた) **IP** アドレス/ホスト名リストを指定します。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 を使用してエージェントをクエリすることを許可された **SNMP** マネージャの (スペースで区切られた) **IP** アドレス/ホスト名リストを指定します。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(;)で区切ることで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_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した場合は、継承された値が上書きされます。このパラメータでは、以下の値を必ず指定する必要があります。

- コミュニティ名
- トラップを送信するデスティネーション アドレス

このパラメータでは、以下の値を任意に指定できます。

- トラップの送信先ポート番号
- 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 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
```

エンコーディング オプションの設定の詳細については、「SNMPv1トラップ デスティネーションの設定」を参照してください。

CASE_SNMP_TRAP_DESTINATION

トラップの送信先ホスト名または 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す、また SNMP_TRAP_PORT を指定する必要があります。

CASE_SNMP_TRAP_PORT

トラップを送信する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す、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

コマンドライン内に、コマンドと、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、適切なバージョンのインストーラを実行します。

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 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。

エージェントの UNIX および Linux システムへのインストール

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 CASYSEEDGE と表し、データ ディレクトリを CASYSEEDGE_DATA と表します。

エージェントを UNIX および Linux システムにインストールする方法

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]をクリックします。手順 17 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 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。

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。

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。

コマンドラインを使用して UNIX にエージェントをインストールする方法

1. システムに root としてログオンします。
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してコマンドを実行すると、指定したパラメータ値が事前に入力された状態でインストール ウィザードが開きます。

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。

- 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記録する場所と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、詳細インストールモードがオンになります。詳細モードでは、インストールログファイルにより多くの情報が記録されます。

CASE_INSTALLDIR

SystemEDGE インストール ディレクトリを指定します(このドキュメント内では、SystemEDGE インストール ディレクトリを、変数 **CASYSEEDGE** と呼んでいます)。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 **CASYSEEDGE_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。セミコロンの区切りにより、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_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した場合は、継承された値が上書きされます。このパラメータでは、以下の値を必ず指定する必要があります。

- コミュニティ名
- トラップを送信するデスティネーション アドレス

このパラメータでは、以下の値を任意に指定できます。

- トラップの送信先ポート番号
- 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 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
```

エンコーディング オプションの設定の詳細については、「SNMPv1 トラップ デスティネーションの設定」を参照してください。

CASE_SNMP_TRAP_DESTINATION

トラップの送信先となるホスト名または 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

トラップを送信する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

インストールの完了後にエージェントを自動起動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

エージェントが **SNMP** 通信の実行時に使用する認証情報のユーザ名を指定します。

このエントリを使用して、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(**UNIX** のみ)に指示します。また、エージェントはこのユーザのデフォルトグループを有効なグループとして使用します。

デフォルト: エージェントは **root** アカウントを使用して動作します。

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。

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。

応答ファイルを設定して使用する方法

1. 管理者または **root** としてコンピュータシステムにログオンします。
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は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いない場合にのみ、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。

レガシー モードでエージェントをインストールする方法

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 \(P. 52\)](#)」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 \(P. 67\)](#)」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

SystemEDGE 上に AIM をインストールするときは、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 Core
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によって許可されません。たとえば、Advanced Encryption がインストールされていない状態で 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_HYPERV
 - CA_SystemEDGE_LPAR
 - CA_SystemEDGE_MSCS
 - CA_SystemEDGE_RM
 - CA_SystemEDGE_SOLZONES
 - CA_SystemEDGE_SRM
 - CA_SystemEDGE_UCS
 - CA_SystemEDGE_VC
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、または vCenter 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 AIM 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、このオプションが有効なとき、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 Performance LiteAgent のインストール

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

注: CA Performance Lite Agent 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 Performance Lite Agent 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 Performance Lite Agent をインストールします。

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

UNIX または Linux に CA Performance Lite Agent をインストールするには、リモート展開を使用します。オンライン ヘルプに記載されている手順に従います。

第 4 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。

[サポートされているアップグレード \(P. 87\)](#)

[CA Virtual Assurance のアップグレード方法 \(P. 88\)](#)

[アップグレードドキュメントの確認 \(P. 89\)](#)

[アップグレード対象環境の準備 \(P. 90\)](#)

[リモート Embedded Entitlements Manager の手動アップグレード \(P. 95\)](#)

[マネージャインストールの実行 \(P. 96\)](#)

[自動的にアップグレードされなかった古い設定の確認 \(P. 97\)](#)

[古い設定の手動適用 \(P. 98\)](#)

[管理対象ノードおよび AIM サーバのアップグレード \(P. 98\)](#)

[使用環境での CA Virtual Assurance アップグレードの確認 \(P. 104\)](#)

サポートされているアップグレード

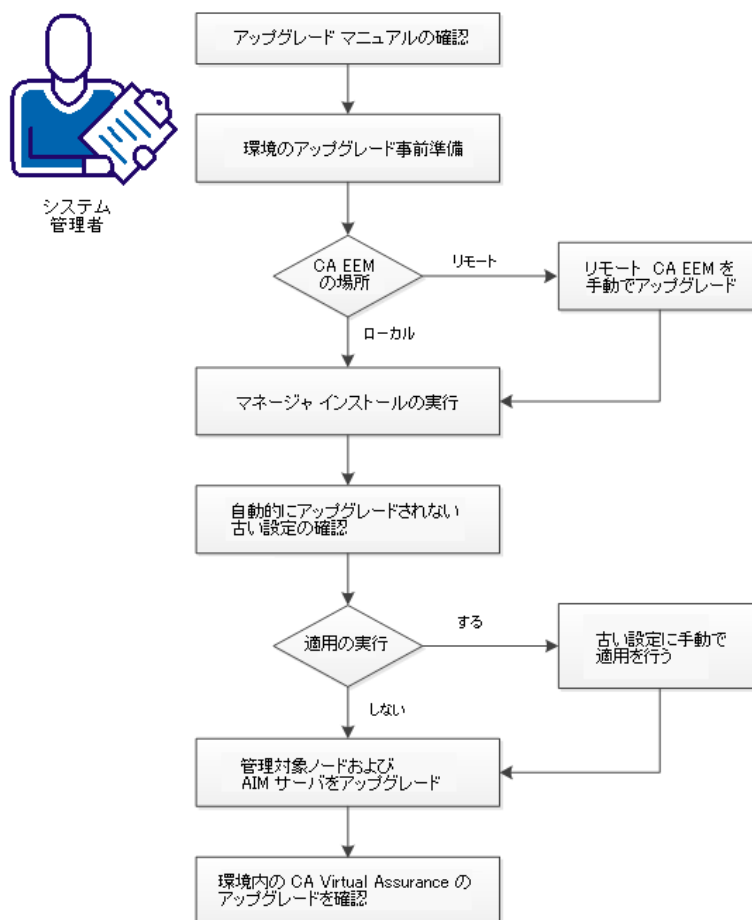
以下の CA Virtual Assurance リリースを リリース 12.6 にアップグレードできます。

- CA Virtual Assurance リリース 12.0.2 (SP2)
- CA Virtual Assurance リリース 12.5

CA Virtual Assurance のアップグレード方法

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をアップグレードする方法



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](#) (P. 89)

[アップグレード対象環境の準備](#) (P. 90)

[リモート Embedded Entitlements Manager の手動アップグレード](#) (P. 95)

[マネージャ インストールの実行](#) (P. 96)

[自動的にアップグレードされなかった古い設定の確認](#) (P. 97)

[古い設定の手動適用](#) (P. 98)

[管理対象ノードおよび AIM サーバのアップグレード](#) (P. 98)

[使用環境での CA Virtual Assurance アップグレードの確認](#) (P. 104)

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 \(P. 28\)](#)」を読みます。

認証にリモート Embedded Entitlements Manager インストールを使用している場合は、Embedded Entitlements Manager 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。

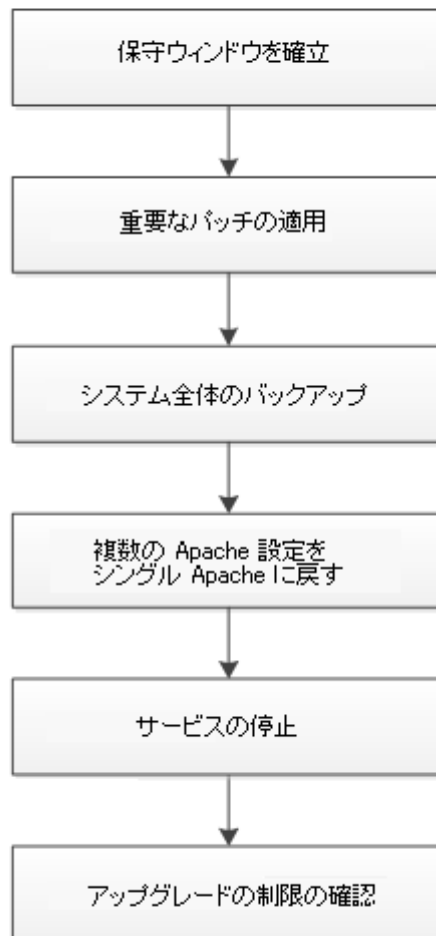
アップグレード対象環境の準備

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。

環境をアップグレード用に事前準備する方法



システム
管理者



以下の手順に従います。

[メンテナンス期間の設定](#) (P. 91)

[重要なパッチの適用](#) (P. 91)

[システム全体のバックアップ](#) (P. 120)

[複数 Apache 設定の単一 Apache 設定への切り替え](#) (P. 93)

[サービスの停止](#) (P. 93)

[アップグレード制限の確認](#) (P. 94)

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 Virtual Assurance リリース 12.0.2 (SP2) がインストールされている場合は、以下の順番で修正を適用します。

- TF91826 (VDEPIN - アップグレード展開)

- T283929 (VPMCE-11019 CUMUL FIX)

パフォーマンス データベース内にサイズが大きいパフォーマンス データがある場合は、アップグレード前にこのパッチを適用します。このパッチを適用しなくてもアップグレード処理は実行できますが、アップグレードに非常に長い時間がかかる場合があります。

- RO31482 SYSEEDGE および AIM Upgrade 修正 - 32 ビット/64 ビット Windows のいずれも対象

CA Virtual Assurance リリース 12.0.2 (SP2) をリリース 12.5 にアップグレードした場合は、リリース 12.6 にアップグレードする前に、ドメイン サーバ マネージャ 12.5 に以下の修正を適用します。

- TF91826 (VDEPIN - アップグレード展開)

注: TF91826 および T283929 のパッチを適用する場合は、CA サポート にお問い合わせください。これらのパッチは公開されていません。

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、すべてのサーバ上で同時にバックアップが実行されるようにします。

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。
 - CAAIPTomcat
 - CAAIPApache
 - CA Message Queuing Server (ActiveMQ)

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 Embedded Entitlements Manager の手動アップグレード

Embedded Entitlements Manager 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 Embedded Entitlements Manager 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 Embedded Entitlements Manager を実行する場合は、サポートされている Embedded Entitlements Manager 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。Embedded Entitlements Manager 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. Embedded Entitlements Manager サーバの Windows [スタート]メニューから、Embedded Entitlements Manager 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 Embedded Entitlements Manager をアップグレードし、Embedded Entitlements Manager 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、**Embedded Entitlements Manager**、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. 99)

[ポリシーへの SystemEDGE モニタのインポート](#) (P. 103)

エージェントと AIM のアップグレード

SystemEDGE バージョン 5.6 へは、SystemEDGE の以下のアップグレード可能バージョンからアップグレードできます。

- 4.3
- 5.0.0
- 5.0.1
- 5.0.2
- 5.1.0

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 をバージョン 5.6 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 バージョン 5.6 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 および AIM をアップグレードする場合は、SystemEDGE、Advanced Encryption、必要なすべての AIM が含まれる単一のリモート展開ジョブを使用します。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」セクション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 \(P. 52\)](#)」または「[UNIX へのエージェントのインストール \(P. 67\)](#)」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バージョンの場合は、以下の手順に従います。

- 以前のバージョンの **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** バージョン 5.6 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** バージョン 5.6 に適用します。

SystemEDGE 4.3 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 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/sysedge.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** バージョン 4.3 から **SystemEDGE** バージョン 5.6 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 マシン上の **SystemEDGE** バージョン 4.3 を **SystemEDGE** バージョン 5.6 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 をバージョン 4.3 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。

ポリシーに SystemEDGE モニタをインポートする方法

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 をバージョン 5.6.0 にアップグレードします。
3. SystemEDGE 5.6.0 が正しく検出されることと([リソース]タブ)、このバージョンにポリシーがあること([ポリシー]タブ)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 5.6.0 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。

第 5 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](#) (P. 105)

[AutoShell の開始](#) (P. 107)

[CA Virtual Assurance コマンド プロンプトの起動](#) (P. 109)

[マニュアル選択メニューとオンライン ヘルプの起動](#) (P. 110)

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。

CA Virtual Assurance を起動する方法

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。これは、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。

AutoShell を起動するには

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

```
? "今日の日付: ", 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. 109)

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 (Embedded Entitlements Manager) のユーザ ID とパスワードを定義します。認証情報は Embedded Entitlements Manager 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。

Embedded Entitlements Manager 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 Embedded Entitlements Manager 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。

CA Virtual Assurance のコマンド プロンプトを起動する方法

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、インストールパス/VirtualAssurance/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、ウィンドウの右上隅の [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、ウィンドウの右上隅の [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] ウィンドウの右上隅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 6 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](#) (P. 111)

[マネージャのアンインストール](#) (P. 112)

[SystemEDGE のアンインストール](#) (P. 114)

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 \(P. 112\)](#)

[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 \(P. 113\)](#)

[サイレント モードでのマネージャのアンインストール \(P. 114\)](#)

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。

マネージャの完全アンインストールを実行する方法

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

コマンド プロンプトからマネージャをアンインストールする方法

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. インストールパス¥VirtualAssurance¥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 \(P. 114\)](#)

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。

コマンドラインからサイレントモードでマネージャをアンインストールする方法

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. インストールパス¥VirtualAssurance¥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 \(P. 113\)](#)

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

アンインストールは、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 データを削除するか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 Core

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。

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 Core

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 UNIX 上の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 UNIX 上の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。

第 7 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](#) (P. 119)

[システム全体のバックアップ](#) (P. 120)

[設定とデータのバックアップ](#) (P. 122)

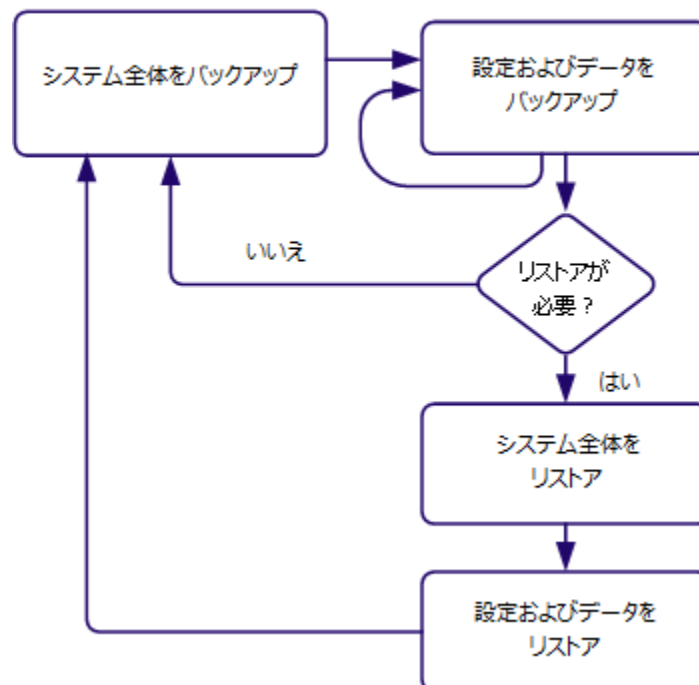
[システム全体のリストア](#) (P. 126)

[設定とデータのリストア](#) (P. 127)

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. 120)します。
2. [設定とデータをバックアップします。](#) (P. 122)
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. 126)
 - b. [設定とデータをリストアします。](#) (P. 127)

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、すべてのサーバ上で同時にバックアップが実行されるようにします。

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、使用率が低く、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. 122)
- [ディレクトリとデータのバックアップ](#) (P. 123)

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 *	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥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>
IDManager インストール ディレクトリ *	REG QUERY "HKEY_LOCAL_MACHINE¥SOFTWARE¥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 <CAVPM> 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、次の場所にある展開パッケージを除く： <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>% distributions erver%	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。
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、この配布サーバを使用して次に展開を実行するときに認証情報を再入力する必要があります。
Web サービス データ	<PRIVATEDATADIR>% caismwebser vice	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	参照用に必要とされない限り、バックアップの必要はありません。
ID ログ ファイル	<IDDIR>%logs	参照用に必要とされない限り、バックアップの必要はありません。

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. 127)

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. 127)
- [ディレクトリとデータのリストア](#) (P. 128)

関連項目

[システム全体のリストア](#) (P. 126)

データベースのリストア

データベースをリストアするには、SQL Management Studio を以下の手順で使用します。

1. 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。

用語集

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ーです。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。

Application Insight Module、AIM

SystemEDGE エージェントには、初期化時にオプションの *Application Insight Module (AIM)* をロードできるプラグインアーキテクチャが備わっています。AIM は SystemEDGE エージェントの機能拡張です。たとえば、vCenter AIM により、SystemEDGE は VMware vCenter Server を介して vSphere 環境を管理できます。

AutoShell

AutoShell を使用すると、複雑な反復タスクや管理タスクを自動化できる、コマンドラインとスクリプトの環境が得られます。*AutoShell* は、プログラミング言語ではなく、スクリプト言語とコマンドラインシェルを組み合わせたものです。

AutoShell は、標準化されたスクリプト言語 ECMA-Script (JavaScript) をベースにしています。JavaScript は一般に Web ページで使われるスクリプト言語として知られていますが、必ずしもブラウザで実行される必要はありません。このスタンドアロンのスクリプト言語を使用して、オブジェクト指向、XML、および正規表現処理に対するサポートを実装できます。*AutoShell* では、Mozilla Spidermonkey JavaScript インタープリタの事前定義済みバージョンを使用します。これにより、Mozilla Firefox Web ブラウザにも JavaScript 機能が提供されます。

Autoshell Loadable Module、ALM

Autoshell Loadable Module (ALM) は *AutoShell* コアの拡張です。インストール時に選択された CA Virtual Assurance のコンポーネントに応じて、必要な ALM が自動的にインストールされます。たとえば、ALM により、LPAR、Solaris ズーン、vCenter Server などのプラットフォームを *AutoShell* を通じて管理できます。

Cisco Unified Computing System (UCS)

Cisco Unified Computing System (UCS) は、データセンターハードウェアと仮想化サービスを提供します。

ESAD AIM

Exchange Server および Active Directory 用 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における Exchange Server 環境と Active Directory 環境をモニタできます。この AIM は、ES 環境と AD 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。

ESX/ESXi ホスト (VMware)

ESX または ESXi ホストは、ESX または ESXi サーバ仮想化ソフトウェアを使用して仮想マシンを実行する物理コンピュータです。ホストによって、仮想マシンが使用する CPU とメモリのリソースが提供され、仮想マシンはストレージとネットワーク接続へのアクセスが可能になります。

Integrated Virtualization Manager (IVM、LPAR)

Integrated Virtualization Manager (IVM) は仮想 I/O サーバ (VIOS) の機能拡張で、単一の POWER Server を管理できます。IVM では、LPAR を作成し管理できます。IVM では、VIOS 機能の管理を可能にし、Web ベースユーザ インターフェースを提供します。

Internet Small Computer Systems Interface、iSCSI

iSCSI は、イントラネット上のデータ転送を円滑化し、長距離にまたがるストレージを管理するのに使用されます。iSCSI は SCSI コマンドを IP パケット内にカプセル化します。この IP パケットが他の IP パケットと同様にネットワーク上でルーティングされます。IP パケットがデスティネーションに到達すると、iSCSI デバイスはパケットのカプセル化を解除し、SCSI コマンドを解釈します。

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。

SNMPv3

SNMPv3 は以下の 3 つの通信のレベルがあるプロトコルです。

noAuthNoPriv: メッセージにユーザ名が伴うという点で SNMPv1 と SNMPv2 をミラーリングします。送信者と受信者の間に一貫性がある必要があります。

AuthNoPriv: 一貫したユーザ名およびパスワードを使用します。

AuthPriv: メッセージの本体を暗号化するユーザ名、パスワードおよび暗号化キーを使用します。

UCS

「Cisco Unified Computing System (UCS)」を参照してください。

UCS マネージャ

UCS ハードウェア (スイッチ、シャーシ、およびブレード) を管理するソフトウェア モジュール

vCenter Server (VMware)

VMware *vCenter Server* は、仮想 vSphere 環境の設定、プロビジョニング、および管理を集中管理する場所を提供します。vCenter Server は、Microsoft Windows サーバおよび Linux サーバ上でサービスとして実行されます。

vCenter Server エージェント (VMware)

VMware *vCenter Server* エージェントは、ESX サーバを vCenter Server と接続します。

vNetwork Standard Switch、vSwitch (VMware)

CA Virtual Assurance では、抽象化されたネットワーク デバイスである Standard vSwitch のポリシーとプロパティを管理します。VMware vNetwork Standard Switch (vSwitch) は、単一のホスト、およびそのホスト上の仮想マシンで動作し、標準スイッチに接続させることができます。

vSwitch で、VM 間のトラフィックを内部的にルーティングして、外部ネットワークにリンクできます。vSwitch では、複数のネットワーク アダプタの帯域幅を組み合わせ、通信トラフィックを分散します。vSwitch は物理 NIC フェールオーバーを処理することができます。

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、その仮想化機能を他の LPAR に提供します。LPAR は、仮想 I/O サーバを介して仮想デバイスとしてディスク、ネットワーク、および光学デバイスにアクセスします。仮想化されたリソースを持つ PowerVM システムには、それぞれ仮想 I/O サーバがあります。

仮想スイッチ (VMware)

仮想スイッチは、物理スイッチと同じように動作します。各 ESX サーバには、ポート グループを通じて仮想マシンに接続する固有の仮想スイッチがあります。これらの仮想スイッチには、ESX サーバの物理イーサネット アダプタへのアップリンク接続もあります。仮想マシンは、仮想スイッチ アップリンクに接続された物理イーサネット アダプタを通じて外界と通信します。

仮想マシン、VM (VMware)

仮想マシン (VM) は、物理コンピュータと同じように、オペレーティングシステムおよびアプリケーションを実行するソフトウェア ベースのコンピュータです。物理ホストのリソースが仮想マシンによって、作業負荷に応じて動的に消費されます。仮想マシンは柔軟性の高いコンピューティング ユニットであるため、展開には、データ センター、クラスタ、クラウド コンピューティング、テスト環境、デスクトップ、ノート PC など、さまざまな環境が含まれます。一番の強みは、データ センターにあります。仮想マシンはデータセンターでサーバ統合、作業負荷の最適化、およびエネルギー効率の向上のために使用されます。

簡易ネットワーク管理プロトコル (SNMP: Simple Network Management Protocol)

簡易ネットワーク管理プロトコル (SNMP) はインターネットの標準的な管理プロトコルです。SNMP 管理アプリケーションおよびエージェントは、get 要求、set 要求、get-next 要求、get レスポンス、およびトラップ PDU を使用して互いと通信します。MIB は、ネットワークとシステムのリソースおよびアプリケーションの履歴を管理し、それらが交換するデータを定義します。

管理情報ベース (MIB)

管理情報ベース (MIB) はリソースのプロパティを説明するデータストアです。MIB には ASN.1 で書き込まれます。これは管理基準によって指定された言語で、SNMP MIB を定義するために OSI の管理情報の構造 (SMI) 基準に準拠しています。

グローバルゾーン (Solaris)

グローバルゾーンは、すべての Solaris システムに含まれているゾーンです。非グローバルゾーンがシステムに存在する場合、システムおよびシステムの全体管理のデフォルトゾーンはグローバルゾーンになります。

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。

ゾーン (Solaris)

Solaris ゾーンは、Solaris 10 システムでセットアップできる、仮想化されたオペレーティングシステム環境を定義します。ゾーンはオペレーティングシステムサービスを仮想化し、隔離され、セキュリティで保護された環境をアプリケーションに提供します。各 Solaris システムには、システムのデフォルトゾーンであるグローバルゾーンが含まれます。たとえば、グローバル以外のゾーンは、作成、削除、変更、停止、または再起動が可能です。

トラップ

トラップは、エージェントとリソースのイベントの管理アプリケーションに通知するために、1 つ以上の管理者へ **SNMP** エージェントが送信できる非請求メッセージです。**SNMP** トラップは一般的 (**SNMP** エージェントのすべてのタイプに共通) であるか、または企業に固有 (それを送信するエージェントに一意) です。

ハードウェア管理コンソール、HMC (LPAR)

ハードウェア管理コンソール (HMC) は、IBM POWER Server 上で管理タスクを実行するために使用される外部アプライアンスです。HMC は、リソースをパーティションに動的に割り当てるなど、論理パーティションを作成または変更するのに使用できます。HMC は POWER Server のサーバファームウェア層と通信し、大規模 PowerVM 環境での単一制御ポイントを提供します。

非グローバルゾーン (Solaris)

非グローバルゾーンは、Solaris オペレーティング システムの単一インスタンスに、仮想化されたオペレーティング システム環境を提供します。Solaris ゾーンソフトウェア パーティション テクノロジーによって、オペレーティング システム サービスが仮想化されます。

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

A

AIM のインストール - 83
Application Insight Module、AIM - 129
AutoShell - 129
Autoshell Loadable Module、ALM - 129
AutoShell の開始 - 107

C

CA Performance LiteAgent のインストール - 85
CA Technologies 製品リファレンス - 3
CA Virtual Assurance コマンド プロンプトの起動
- 109
CA Virtual Assurance コンポーネント間の依存関
係 - 17
CA Virtual Assurance と外部コンポーネントの間
の依存関係 - 18
CA Virtual Assurance のアップグレード - 87
CA Virtual Assurance のアップグレード方法 - 88
CA Virtual Assurance のアンインストール - 111
CA Virtual Assurance のインストール - 19
CA Virtual Assurance の起動 - 105
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 - 50
CA への連絡先 - 3
Cisco Unified Computing System (UCS) - 129

E

Embedded Entitlements Manager 管理者パス
ワード (EiamAdmin) の変更 - 36
ESAD AIM - 130
ESX/ESXi ホスト (VMware) - 130

I

Integrated Virtualization Manager (IVM、LPAR)
- 130
internet Small Computer Systems Interface、
iSCSI - 130

M

Microsoft Hyper-V を使用するために必要な設
定の適用 - 22

P

POWER プロセッサ (LPAR) - 130

S

silent.properties ファイルの編集 - 38
SNMPv3 - 130
SQL Server Express のインストールおよび設定 -
21
SQL Server を使用するための要件の確認 - 20
SystemEDGE 4.3 からのエージェント アップグ
レード - 100
SystemEDGE コンポーネントの依存関係 - 49
SystemEDGE と CA Performance LiteAgent の比
較 - 23
SystemEDGE のアンインストール - 114

U

UCS - 130
UCS マネージャ - 131
UNIX システム上の SystemEDGE および AIM の
アンインストール - 116
UNIX システムでのインストール - 67

V

vCenter Server (VMware) - 131
vCenter Server エージェント (VMware) - 131
vNetwork Standard Switch、vSwitch (VMware)
- 131

W

Windows 上の SystemEDGE および AIM のアン
インストール - 114
Windows システムでのインストール - 52

Windows でのエージェントのインストール - 52
Windows メモリ管理の最適化 - 25

あ

アップグレード制限の確認 - 94
アップグレード対象環境の準備 - 90
アップグレードドキュメントの確認 - 89
アンインストール オプション - 111
インストール オプション - 26
インストールのキャンセル - 34
インストールの実行 - 31
インストールの準備 - 13
インストールの要件および考慮事項 - 19
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 - 37
エージェント コンポーネント - 15
エージェントと AIM のアップグレード - 99
エージェントの UNIX および Linux システムへのインストール - 67
エージェントの個別インストール - 49
エージェントの展開 - 46
応答ファイルの設定と使用 - 81

か

カスタム インストールの準備 - 28
仮想 I/O サーバ、VIOS (LPAR) - 131
仮想スイッチ (VMware) - 131
仮想マシン、VM (VMware) - 132
簡易ネットワーク管理プロトコル (SNMP: Simple Network Management Protocol) - 132
完全アンインストールの実行 - 112
管理情報ベース (MIB) - 132
管理対象ノードおよび AIM サーバのアップグレード - 98
関連ドキュメント - 10
規則 - 11
機能の概要 - 106
グローバル ゾーン (Solaris) - 132
コマンドラインからの Windows へのエージェントインストール - 59

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 - 113
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 - 73

さ

サービスの停止 - 93
サイレント モードでのマネージャのアンインストール - 114
サポートされているアップグレード - 87
システム全体のバックアップ - 92, 120
システム全体のリストア - 126
自動的にアップグレードされなかった古い設定の確認 - 97
重要なパッチの適用 - 91
初期インストール後のコンポーネント インストール - 34
スコープ - 9
正規表現 - 132
製品コンポーネント - 13
セキュリティに関する考慮事項 - 25
設定とデータのバックアップ - 122
設定とデータのリストア - 127
前提条件 - 13
ゾーン (Solaris) - 132

た

対象読者 - 9
通信ポート - 43
ディレクトリとデータのバックアップ - 123
ディレクトリとデータのリストア - 128
データベースのバックアップ - 122
データベースのリストア - 127
展開ジョブの作成 - 47
トラップ - 133

は

ハードウェア管理コンソール、HMC (LPAR) - 133
はじめに - 9
バックアップおよびリストアの概要 - 119

バックアップとリストア - 119
非グローバルゾーン(Solaris) - 133
標準インストールとカスタム インストール - 25
標準インストールの準備 - 27
複数 Apache 設定の単一 Apache 設定への切り
 替え - 93
複数のサーバへインストールする場合のガイド
 ライン - 40
複数のサーバへのカスタム インストール - 40
古い設定の手動適用 - 98
ポーリング間隔 - 133
ポリシーへの SystemEDGE モニタのインポート -
 103

ま

マニュアル選択メニューとオンライン ヘルプの
 起動 - 110
マネージャ インストールの実行 - 96
マネージャ コンポーネント - 14
マネージャのアンインストール - 112
マネージャのサイレント インストール - 37
マネージャのサイレント インストールの実行 - 39
メンテナンス期間の設定 - 91

や

有効な AutoShell ユーザ - 109
ユーザ インターフェースの使い方 - 105

ら

リモート Embedded Entitlements Manager の手
 動アップグレード - 95
レガシー モードでのエージェントのインストール
 - 82
ログイン パスワードの変更 - 35
論理パーティション、LPAR - 133

漢字

使用環境での CA Virtual Assurance アップグ
 レードの確認 - 104