CA Virtual Assurance for Infrastructure Managers

リリース ノート

リリース 12.7.1

CA Technologies 製品リファレンス

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

- CA eHealth®
- CA Embedded Entitlements Manager （CA EEM）
- CA IT Asset Manager （CA ITAM）
- CA ITCM （CA IT Client Manager）
- CA NSM （CA Network and Systems Management）
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager （CA SDM）
- CA Spectrum®
- CA SystemEDGE
- インフラストラクチャ マネージャ用の CA システム性能
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

CA への連絡先

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

目次

第 1 章: はじめに

「CA Virtual Assurance リリース ノート」では、本リリースでの新機能と拡張機能、製品インストールの前提条件、およびサードパーティ ツールとの統合について詳しく説明します。

最新の「CA Virtual Assurance リリース ノート」については、CA サポート オンラインでマニュアル選択メニューを参照してください。

CA Virtual Assurance をインストールする方法の詳細については、「インストール ガイド」を参照してください。 全ドキュメント セットの簡単な説明については、このガイドの「関連ドキュメント」の章参照してください。

第 2 章: システム要件

CA Virtual Assurance を正常にインストールして動作させるには、システムがこのセクションの要件を満たすか、上回っている必要があります。

この製品は、TCP/IP、SNMP、DNS（Domain Name Service、ドメイン名サービス）などのネットワーキング テクノロジを使用しています。 これらのテクノロジが利用できない、パフォーマンスが低下している、またはテクノロジに不正確な情報や期限切れの情報が含まれる場合、テクノロジ障害を含む製品機能に悪影響が及ぶ可能性があります。

このセクションには、以下のトピックが含まれています。

マネージャ要件

このセクションでは、CA Virtual Assurance リリース 12.7.1 のマネージャをインストールするためのハードウェアとソフトウェアの要件について詳しく説明します。

ハードウェア要件

CA Virtual Assurance コンポーネントの分散実装または非分散実装には、以下のハードウェアが必要です。

- CPU : Intel Xeon 51xx 2.6 GHz または相当プロセッサ、あるいは Intel Core 2 Duo 2.6 GHz または相当プロセッサ

  注: CPU 要件は、CA Virtual Assurance の Web ブラウザベースの UI を実行する、クライアント デスクトップ/ワークステーションにも該当します。

- RAM :
  - 1,000 以下のシステムを管理する展開 : 4GB
  - 5,000 以下のシステムを管理する展開（64 ビット オペレーティング システム上） : 8GB
  - 5,000 以上のシステムを管理する展開（64 ビット オペレーティング システム上） : 16GB
- ネットワーク インターフェース コントローラ（NIC） : 100 Mbps 以上
- メインのインストール ドライブのディスク空き領域 : 30 GB
- データベースをインストールするドライブのディスク空き領域 : 30 GB

  注: Virtual Assurance のデータベースを格納するように Microsoft SQL Server を設定した場合は、データベースを保持するドライブにディスク領域が必要です。 ドライブの場所は任意です。製品のインストールに使用したのと同じドライブにすることもできれば、別のドライブ、または別のシステム上のドライブを選ぶこともできます。 製品をインストールしたのと同じドライブにする場合、必要なディスクの空き領域は 2 つの値の合計です。 製品用のデータベースのサイズは、製品の使用状況に応じて大きくなります。保守の実施状況によりますが、30 GB 以上を消費する可能性があります。

重要: トランザクション ログが無制限に拡張されないようにするには、Microsoft のサポート情報記事 873235 に説明されている、Microsoft SQL Server の設定方法を参照してください。

重要: 継続して最適なパフォーマンスを確保するために、データベースの断片化を検出し、解決する方法について、Microsoft サポート技術情報の記事 189858 を参照してください。

重要: CA Virtual Assurance をその他の CA 製品と一緒にインストールする場合は、組み合わせによる影響を考慮し、それに応じてハードウェアの仕様を調整してください。たとえば、1 つのサーバに CA Virtual Assurance（4 GB の RAM）および CA Service Desk Manager （3 GB の RAM）をインストールする場合、最低 7 GB の RAM を備えたサーバを使用します。 CA サポート オンラインの Web サイト（http://supportconnect.ca.com）で、統合製品のリリース ノートを確認してください。

注:CPU 要件は、CA Virtual Assurance の Web ブラウザベースの UI を実行するクライアント デスクトップ/ワークステーションにも適用されます。

ソフトウェア要件

このセクションでは、分散コンポーネントおよび非分散コンポーネントの実装に必要なソフトウェアに関する情報を提供します。

Windows 上のマネージャ

CA Virtual Assurance マネージャは、以下のオペレーティング システムをサポートし、これらのオペレーティング システムで動作が保証されています。

- Windows Server 2008 Standard、Enterprise、および Datacenter Edition（x86、x64）、SP2 オプション
- Windows Server 2008 R2 Standard、Enterprise、および Datacenter Edition（x86、x64）、SP1 オプション

CA Virtual Assurance では、新規に SystemEDGE をインストールする場合、または CA Virtual Assurance マネージャをリリース 12.6 または 12.7 からアップグレードする場合にのみ、以下の Windows バージョンがサポートされます。

- Windows Server 2003 SP2 および 2003 R2 SP2 Standard、Enterprise、および Datacenter Edition （x86、x64）

CA サポート オンラインの Web サイトにある互換性マトリックスには、サポートされているオペレーティング環境の最新のリストが掲載されています。

注: 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。

注: CA Virtual Assurance マネージャまたは <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。

データベース要件

CA Virtual Assurance はデータベースとして Microsoft SQL Server を使用します。 CA Virtual Assurance は他の CA 製品と統合されるため、統合される製品のデータベース要件を確認してください。

このリリースでは、以下のバージョンをサポートしており、動作が保証されています。

- 2008 SP2 （32 ビット、64 ビット）、Standard Edition および Enterprise Edition、SP3 オプション
- 2008 R2 （32 ビット、64 ビット）、Standard Edition および Enterprise Edition、SP1 オプション
- 2008 R2 Express （32 ビット、64 ビット）、Database with Management Tools Edition および Database with Advanced Services Edition、SP1 オプション
- 2012（32 ビット、64 ビット）、Standard Edition および Enterprise Edition
- 2012 Express（32 ビット、64 ビット）、Database with Management Tools Edition および Database with Advanced Services Edition

ローカルまたはリモートの SQL Server データベースに接続するには、マネージャ システムに SQL Server Tools （OSQL.EXE）が必要です。

重要: SQL Server 2005 を使用する既存の 12.6 または 12.7 のインストールをアップグレードする場合、最初に SQL Server をサポートされているバージョンにアップグレードし、12.6 または 12.7 の製品が動作することを確認してから、CA Virtual Assurance リリース 12.7.1 へアップグレードしてください。

以下の点に注意してください。

- 本製品を便利にお使いいただくために、SQL Server 2008 R2 Express Edition （32 ビット）が、CA Virtual Assurance インストール メディア上の以下の場所で利用可能です：
  DVD1¥Installers¥Windows¥External¥MSSQLExpress¥setup.exe。
- 名前付きインスタンスおよび SQL Server クラスタはサポートされます。TCP/IP を有効にし、各インスタンスに静的ポートを割り当てます。 動的ポートはサポートされていません。
- マネージャ コンポーネントがインストールされたシステムには、SQL クライアント（サーバ ツール）もインストールされている必要があります。
- SQL Server Tools をインストールした後、この場所（デフォルト インストール パスを使用する場合）に OSQL.EXE が正しくインストールされていることを確認します。
  - MS SQL 2008： C:¥Program Files¥Microsoft SQL Server¥100¥Tools¥Binn

重要: 継続して最適なパフォーマンスを確保するために、データベースの断片化を検出し、解決する方法について、Microsoft サポート技術情報の記事 189858 を参照してください。

リモート データベース

リモート データベースを使用している場合、一致する適切なバージョンの SQL Server Native Client がローカル システムで必要です。

例

- リモートの 2008 SP2、R2、または R2 Express データベースには、ローカルの 2008 SP2、2008 R2、または Native Client のいずれかが必要です。リモートの 2012 データベースには、ローカル 2012 Native Client が必要です。

SQL Server Native Client は、Microsoft ダウンロード センターで「Microsoft SQL Server 用 Feature Pack」を検索することで利用可能です。お使いの *リモート*データベースとオペレーティング環境に基づいて、以下の手順を実行します。

1. 最新の適切なバージョンを選択します。
2. オペレーティング環境用の適切なモジュールをダウンロードして、*ローカル* システムにインストールします。

   例： ENU¥<*x86 または x64*>¥sqlncli.msi

ブラウザの要件

CA Virtual Assurance は、ユーザ インターフェース用に以下のブラウザをサポートしています。 これらの Web ブラウザは、（製造元によって決定される）その Web ブラウザのライフサイクルの間、または CA Technologies がサポートを終了するまでサポートされます。

- Microsoft Internet Explorer 8.0、9.0

  注: 「このページのスクリプトが、Internet Explorer の実行速度を遅くしています。」というメッセージが表示された場合は、Microsoft サポート技術情報の記事 175500 を確認してください。

- Mozilla Firefox 16.0 （すべてのマイナー バージョンを含む）

CA Virtual Assurance で図やチャートを表示するには、Adobe Flash Player プラグインを備えたサポート対象ブラウザが必要です。 以下のバージョンがサポートされています。

- Adobe Flash Player バージョン 10.0、11.1、11.4

  注: CA Virtual Assurance では Adobe Flash Player のメジャー バージョンをサポートしています。マイナー バージョンも実行できますが、それらのバージョンは認定されていません。

その他の CA ソフトウェア

CA Virtual Assurance には、インストール メディアに含まれている以下のソフトウェアが必要です。

CA Embedded Entitlements Manager（CA EEM）

CA Virtual Assurance は CA EEM バージョン 8.4 SP4 CR14 （8.4.414）を配布およびサポートし、連携して動作することが確認されています。

また、CA Virtual Assurance は以下をサポートしています。

- すべての「CA EEM 8.4」のサブバージョン（CA EEM 8.4 SP4（8.4.244）から現在配布しているバージョンまで、また新しい「CA EEM8.4」SP まで）。
- この製品のリリース後に出荷される CR のサブバージョン。

インストール時に CA EEM の不十分なバージョンが検出された場合、サポートされているバージョンにアップグレードできるように、インストール プログラムによって最小要件が表示されます。

サポートを要求する、この製品と CA EEM の別バージョンとの動作を確認する場合は、CA 担当者にお問い合わせください。

注: サイトに CA Server Automation または CA Virtual Assurance のインスタンスが複数ある場合、CA EEM サーバは共有できません。

注: この製品によって CA EEM がインストールされる場合、［TLS を使用］オプションは、デフォルトでは有効になりません。 セキュリティを高めるためには、CA EEM インターフェースへログインし、［設定］タブで TLS オプションを選択します。

CA Network Discovery Gateway

このソフトウェアは、システムおよびネットワークのディスカバリに必要です。

SystemEDGE

リリース 5.x.y は CA Virtual Assurance リリース 12.x.y に対応します。
例： **SystemEDGE 5.7.1 は CA Virtual Assurance 12.7.1 に対応します。**

注: 最新バージョンの SystemEDGE がシステムにインストールされていない場合、インストール プログラムによって SystemEDGE がインストールされます。 SystemEDGE は CA Virtual Assurance AIM に必要です。 AIM は SystemEDGE エージェントの機能拡張です。

環境内のリモート サーバの管理には、SystemEDGE リリース 4.3.4、4.3.5、4.3.6、5.1.0、5.6.0、5.7.0 を使用できます。

CA Virtual Assurance 用のオプションの CA ソフトウェア

以下に示すオプションの CA ソフトウェアをインストールし、CA Virtual Assurance を適切に設定することで、特定の統合機能を有効にすることができます。

CA Service Desk Manager

ヘルプ デスクのチケットをオープンするには、バージョン 12.5 以降が必要です。

国際化（i18n）

CA Virtual Assurance は、UTF-8 文字エンコーディングを使用して言語固有の文字を表示する、国際化製品（i18n）です。 たとえば、入出力データ内のドイツ語の ü （ウムラウト）、フランス語の è （抑音アクセント）、日本語の文字を表示できます。

UTF-8 による文字のエンコーディングは、以下の領域などでサポートされています。

- オブジェクトやリソースの説明文
- メッセージ
- 管理可能なリソースに接続するためのユーザ名およびパスワード
- 正規表現（SystemEDGE）

この製品のインストールは、サポートされた Microsoft Windows オペレーティング システムの英語版、フランス語版、ドイツ語版および日本語版にてサポートされています。 また、Windows については、オペレーティング システムでサポートされているバージョンの SQL Server（英語または該当するローカライズ バージョン）を使用できます。

重要: UTF-8 エンコーディングを使用する製品ファイルを編集した場合は、必ず UTF-8 エンコーディングで保存するよう注意してください。英語以外のオペレーティング システムで、マルチバイト文字を使用している場合は、UTF-8 エンコーディングで保存する必要があります。 Windows のメモ帳では、UTF-8 エンコーディングで保存できます。

一般的な制限

CA Virtual Assurance は他の CA 製品と統合可能のため、統合製品用の国際サポート声明を確認してください。

CA Virtual Assurance は、文字 'a - z'、'A - Z'、'0 - 9'、および '-' から構成されるホスト名またはクラスタ名のみをサポートします。 ホスト名またはクラスタ名は、先頭文字をハイフン（「-」）にすることや、すべて数値にすることはできません。 Windows システムの NetBIOS 名は、その DNS ホスト名と一致している必要があります。

CA Virtual Assurance は、次の場合、ASCII 文字のみをサポートします。

- SQL Server のホスト名（ホスト名の制約を受ける）、インスタンス名、ユーザ名、およびパスワード
- CA EEM/Security のホスト名（ホスト名の制約を受ける）、ユーザ名、およびパスワード
- ポリシー名を除く、すべての CA SystemEDGE パラメータ
- SystemEDGE 権限分離ユーザ（UNIX および Linux のみ）
- SNMP の読み取り、読み取り/書き込み、およびトラップのコミュニティ文字列
- %TEMP% 環境変数
- すべての CA Virtual Assurance コンポーネントのインストール先パス

コンソール ディスプレイのカスタマイズ

言語固有の文字を含むコンソール データを表示する場合は、CLI コマンドの以下の前提条件を確認します。

- 使用しているオペレーティング システムで、適切な言語サポートが利用可能であることを確認します。
- コマンドまたは NodeCfgUtil ユーティリティの実行に使用する Windows コマンド プロンプト内で、Lucida Console フォントを有効にします。
- コマンドの実行に使用する UNIX または Linux コンソール内で、UTF-8 文字エンコーディングを有効にします。端末コンソール内で以下のコマンドを入力して、現在の言語設定を表示します。

  ```
  echo $LANG
  ```

  UTF-8 が無効な場合、コンソール ウィンドウで、たとえば以下のコマンドを入力します（適切な文字エンコーディングを使用してください: en_US.UTF-8、ja_JP.UTF-8、fr_BE.UTF-8、de_DE.UTF-8 など）。

  ```
  LANG=en_US.UTF-8; export LANG
  ```

AutoShell および CA Virtual Assurance CLI Autoshell コマンド

AutoShell および CA Virtual Assurance CLI コマンドでは、ISO 639_3166 の組み合わせ（例： フランス語では fr_FR）に基づいたロケール指定が可能な -locale スイッチがサポートされています。「リファレンス ガイド」の「AutoShell の呼び出し」および「CLI コマンド」を参照してください。

Solaris ゾーン稼働時間

Solaris ゾーンの稼働時間（Uptime） MIB 属性（zoneAimStatZoneUpTime）は、ASCII 文字のみをサポートする DisplayString として指定されます。ユーザ インターフェース内の対応するフィールドでは UTF8 文字が表示されません。

デフォルトのパッケージ ラッパー名

デフォルトのパッケージ ラッパー名はローカライズされておらず、すべてのサポート対象言語で「デフォルト」が読み込まれます。カスタム パッケージ ラッパー名では UTF-8 文字がサポートされています。

サービス レスポンス モニタリング AIM 設定ファイル

言語固有の文字を追加するために svcrsp.cf 設定ファイルを変更する場合は、ご使用のテキスト エディタが保存形式として UTF-8 をサポートしていることを確認します。 ファイルの保存時に、テキスト エディタによって UTF-8 バイト オーダー マークが挿入されると、SystemEDGE は、設定ファイルを読み取るときにバイト オーダー マークを無視します。

SRM CLI コマンド

svcwatch CLI は、出力とコンソールのヘルプ情報のローカライズをサポートしています。

オプションの -L スイッチを使用すると、ユーティリティは、コンソールの現在のロケールと、利用可能な場合は言語カタログを検出します。 言語カタログが見つからない場合、ユーティリティはデフォルト言語である英語に戻ります。

Cisco UCS の制限

Cisco Unified Computing System （Cisco UCS）は、英語の文字のみをサポートします。 UCS Manager では英語以外の文字が無効として扱われるため、CA Virtual Assurance では、サービス プロファイルやプールなどの UCS フィールド内のサポートされていない文字は許可されません。

Business Objects レポート

Business Objects レポートを使用するには、英語または日本語版の Microsoft SQL Server が必要です。他の言語はサポートされていません。

インストール時の制限

パラメータ -L *ロケール*（Install.exe -L fr など）を使用することにより、サイレント インストール用の言語を指定できます。 サポートされているロケールは、en （英語）、ja （日本語）、de （ドイツ語）、および fr （フランス語）です。 ロケールを指定しないと、インストーラは、最も適切なもの（システム ロケールまたは英語（en））を選択します。

中国語のシステムでない限り、指定する DVD インストール パスに漢字を含めることはできません。 中国語のシステム以外で漢字を指定すると、インストーラは以下のメッセージを表示し、失敗します。

```
Unable to extract the compressed file. Please get another copy of the installer and try again.
```

CA Virtual Assurance AIM サーバおよび管理対象ノードの要件

このセクションでは、AIM サーバまたは管理対象ノードによってサポートされるハードウェア要件およびオペレーティング システムについて詳しく説明します。

管理対象ノードおよび AIM サーバのハードウェア要件

SystemEDGE および AIM のハードウェア要件は以下のとおりです。

最小要件

CPU： OS ベンダーと同じ

RAM： OS ベンダーと同じ

空きディスク領域： 50 MB（管理対象ノード、SystemEDGE のみ*）
空きディスク領域： 250 MB（CA Virtual Assurance AIM をすべてインストールした AIM サーバ）

ネットワーク インターフェース コントローラ（NIC）： 100 Mbps

推奨

CPU： OS ベンダーと同じ

RAM： OS ベンダーと同じ

空きディスク領域： 150 MB 以上（管理対象ノード、SystemEDGE のみ）**
空きディスク領域： 500 MB（CA Virtual Assurance AIM をすべてインストールした AIM サーバ）

ネットワーク インターフェース コントローラ（NIC）： 100 Mbps 以上

（*）ディスク領域要件は、UNIX プラットフォームと Windows プラットフォームでは異なります。Windows をインストールする場合、MSI インストーラは、SystemEDGE をインストールするディスク領域を必要とします。

（**）診断トレースが有効である場合、ランタイム ファイルのディスク領域の要件は大きくなります。 デフォルトでは、診断トレースのサイズは 10 MB に制限されています。

SystemEDGE のオペレーティング システム サポート

SystemEDGE リリース 5.7.1 を実行するシステムには、以下のいずれかのオペレーティング システムが必要です。

Windows

- Windows Server 2003 SP2 Standard、Enterprise、Data Center、および Small Business Server Edition （32 ビット、x86）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （32 ビット、x86）
- Windows Server 2003 SP2 Standard、Enterprise、および Data Center （64 ビット、x64）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）
- Windows Server 2003 SP2 x64 Edition （64 ビット）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（32 ビット、x86）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（64 ビット、x64）
- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）
- Windows XP Professional SP3 （32 ビット、x86）
- Windows Vista SP1 Business、Enterprise、および Ultimate Edition（32 ビット、x86）
- Windows Vista SP1 Business、Enterprise、および Ultimate Edition（64 ビット、x64）
- Windows 7 Professional、Ultimate Edition（32 ビット、x86）
- Windows 7 Professional、Ultimate Edition（64 ビット、x64）

HP

- HP-UX 11.11 PA-RISC （64 ビット）
- HP-UX 11.23 PA-RISC （64 ビット）
- HP-UX 11.23 ia64 （64 ビット）
- HP-UX 11.31 PA-RISC （64 ビット）
- HP-UX 11.31 ia64 （64 ビット）

IBM AIX

- IBM AIX Version 6.1 （64 ビット）
- IBM AIX Version 7.1 （64 ビット）

Linux

- Red Hat Linux Web Server、Advanced Server、および Enterprise Server 5.0 （32 ビット、x86）
- Red Hat Linux Web Server、Advanced Server、および Enterprise Server 5.0 （64 ビット、x64）
- Red Hat Enterprise Linux 6.0 （32 ビット、x86）
- Red Hat Enterprise Linux 6.0 （64 ビット、x64）
- SUSE Linux Enterprise Server 10.0 （32 ビット、x86）
- SUSE Linux Enterprise Server 10.0 （64 ビット、x64）
- SUSE Linux Enterprise Server 10.0 （64 ビット、ia_64）
- SUSE Linux Enterprise Server 11 （32 ビット、x86）
- SUSE Linux Enterprise Server 11 （64 ビット、x64）
- Debian Linux Version 5.0 （Lenny） （32 ビット、x86）
- Debian Linux Version 5.0 （Lenny） （64 ビット、x64） - レガシー モードのみ
- Debian Linux Version 5.0 （Lenny） （64 ビット、ia_64） - レガシー モードのみ

zLinux

- SUSE Linux Enterprise Server 10 （zSeries） - レガシー モードのみ
- SUSE Linux Enterprise Server 11 （zSeries） - レガシー モードのみ
- Red Hat Enterprise Server 5.0 （zSeries） - レガシー モードのみ

Linux on pSeries

- Red Hat Enterprise Server 5.0
- Red Hat Enterprise Server 6.0

Solaris

注: SystemEDGE では、Solaris 10 オペレーティング システムのすべての Solaris ゾーンの設定をサポートします。

- Solaris UltraSPARC 9 （64 ビット）
- Solaris UltraSPARC 10 （64 ビット）
- Solaris 9 （32 ビット、x86）
- Solaris 10 （32 ビット、x86）
- Solaris 10 （64 ビット、x64）

注: 展開や設定などの CA Virtual Assurance に固有の機能は、すべてのプラットフォームでサポートされていない場合があります。

CA Virtual Assurance AIM のオペレーティング システム サポート

CA Virtual Assurance に付属の SystemEDGE AIM と Advanced Encryption は、以下のオペレーティング システムで実行できます。

Windows： Advanced Encryption

- Windows XP Professional SP3 （32 ビット、x86）
- Windows Vista SP1 Business、Enterprise、および Ultimate Edition（32 ビット、x86）
- Windows Vista SP1 Business、Enterprise、および Ultimate Edition（64 ビット、x64）
- Windows 7 Professional、Ultimate Edition（32 ビット、x86）
- Windows 7 Professional、Ultimate Edition（64 ビット、x64）

- Windows Server 2003 SP2 Standard、Enterprise、Data Center、および Small Business Server Edition （32 ビット、x86）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （32 ビット、x86）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）
- Windows Server 2003 SP2 x64 Edition （64 ビット）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（32 ビット、x86）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（64 ビット、x64）
- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）

Windows： サービス レスポンス モニタリング AIM

- Windows Server 2003 SP2 Standard、Enterprise、Data Center、および Small Business Server Edition （32 ビット、x86）
- Windows Server 2003 SP2 x64 Edition （64 ビット）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （32 ビット、x86）
- Windows Server 2003 R2 SP2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（32 ビット、x86）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（64 ビット、x64）
- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition （64 ビット、x64）

Windows： LPAR AIM、UCS AIM、VC AIM、ゾーン AIM、XenServer AIM、レスポンス モニタリング AIM

- Windows Server 2008 Standard、Enterprise、および Data Center Edition（32 ビット、x86）
- Windows Server 2008 Standard、Enterprise、および Data Center Edition（64 ビット、x64）
- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition（64 ビット、x64）

Windows： Hyper-V AIM

- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition（64 ビット、x64）

HP： Advanced Encryption、サービス レスポンス モニタリング AIM

- HP-UX 11.11 PA-RISC （64 ビット）
- HP-UX 11.23 PA-RISC （64 ビット）
- HP-UX 11.23 ia64 （64 ビット）
- HP-UX 11.31 PA-RISC （64 ビット）
- HP-UX 11.31 ia64 （64 ビット）

IBM AIX： Advanced Encryption、サービス レスポンス モニタリング AIM

- IBM AIX Version 6.1 （64 ビット）
- IBM AIX Version 7.1 （64 ビット）

注: JRE は AIX 用 SRM AIM に付属しています。

Linux： Advanced Encryption、サービス レスポンス モニタリング AIM

- Red Hat Linux Web Server、Advanced Server、および Enterprise Server 5.0（32 ビット、x86）
- Red Hat Linux Web Server、Advanced Server、および Enterprise Server 5.0（64 ビット、x64）
- Red Hat Enterprise Linux 6.0 （32 ビット、x86）
- Red Hat Enterprise Linux 6.0 （64 ビット、x64）

- SUSE Linux Enterprise Server 10.0 （32 ビット、x86）
- SUSE Linux Enterprise Server 10.0 （64 ビット、x64）
- SUSE Linux Enterprise Server 10.0 （64 ビット、ia_64）
- SUSE Linux Enterprise Server 11 （32 ビット、x86）
- SUSE Linux Enterprise Server 11 （64 ビット、x64）
- Debian Linux Version 5.0 （Lenny） （32 ビット、x86）
- Debian Linux Version 5.0 （Lenny） （64 ビット、x64） - レガシー モードのみ
- Debian Linux Version 5.0 （Lenny） （64 ビット、ia_64） - レガシー モードのみ

  注: サービス レスポンス モニタリング AIM では、Debian Linux 5.0 （64 ビット、ia_64）はサポートされていません。

Solaris： Advanced Encryption、サービス レスポンス モニタリング AIM

注: SystemEDGE では、Solaris 10 オペレーティング システムのすべての Solaris ゾーンの設定をサポートします。

- Solaris UltraSPARC 9 （64 ビット）
- Solaris UltraSPARC 10 （64 ビット）
- Solaris 9 （32 ビット、x86）
- Solaris 10 （32 ビット、x86）
- Solaris 10 （64 ビット、x64）

zLinux： Advanced Encryption

- SUSE Linux Enterprise Server 10 （zSeries） - レガシー モードのみ
- SUSE Linux Enterprise Server 11 （zSeries） - レガシー モードのみ
- Red Hat Enterprise Server 5.0 （zSeries） - レガシー モードのみ

Linux on pSeries： Advanced Encryption

- Red Hat Enterprise Server 5.0
- Red Hat Enterprise Server 6.0

CA Systems Performance LiteAgent のオペレーティング システム サポート

CA Systems Performance LiteAgent を実行するコンピュータは、以下のいずれかのオペレーティング システムが必要です。

Windows

注: CA Virtual Assurance 12.6 からアップグレードする場合にのみ、以下の Windows 2003 オペレーティング システムがサポートされています。

- Windows Server 2008 （32 ビット、x86）
- Windows Server 2008 （64 ビット、x64）
- Windows Server 2008 R2 （64 ビット、x64）
- Windows Server 2003 Standard、Enterprise、Data Center、および Small Business Server Edition （32 ビット、x86）
- Windows Server 2003 （64 ビット、x64）
- Windows Server 2003 R2 Standard、Enterprise、および Data Center Edition （32 ビット、x86）
- Windows Server 2003 R2 （64 ビット、x64）
- Windows XP Professional SP3 以降（32 ビット、x86）
- Windows XP Professional SP2 以降（64 ビット、x64）
- Windows Vista Business、Enterprise、Ultimate （32 ビット、x86）
- Windows Vista Business、Enterprise、Ultimate （64 ビット、x64）

Linux

- Red Hat Linux Enterprise Server 5.0 （32 ビット、x86）
- Red Hat Linux Enterprise Server 5.0 （64 ビット、x64）
- SUSE Linux Enterprise Server 10.0 （32 ビット、x86）
- SUSE Linux Enterprise Server 10.0 （64 ビット、x64）

Solaris

注: 展開や設定などの CA Virtual Assurance に固有の機能は、すべてのプラットフォームでサポートされていない場合があります。

- Solaris UltraSPARC 9 （32 ビット）
- Solaris UltraSPARC 9 （64 ビット）
- Solaris UltraSPARC 10 （64 ビット）
- Solaris 10 （32 ビット、x86）
- Solaris 10 （64 ビット、x64）

HP

- HP-UX 11.23 PA-RISC （64 ビット）
- HP-UX 11.23 IA64 （64 ビット）
- HP-UX 11.31 PA-RISC （64 ビット）
- HP-UX 11.31 IA64 （64 ビット）

注: HP-UX 11 については、PHNE 27063 s700 800 11 ARPA Transport の累積パッチ以降を推奨します。 このパッチは、HP-UX ライブラリのメモリの問題を解決します。

IBM AIX

- IBM AIX Version 5.3 （32 ビット、64 ビット）
- IBM AIX Version 6.1 （64 ビット）
- IBM AIX Version 7.1 （64 ビット）
- IBM AIX Version 7 （64 ビット）

サポートされる統合プラットフォーム

CA Virtual Assurance はユーザの環境で、仮想プラットフォームおよび物理プラットフォームと統合します。 これらのプラットフォームを管理するには、適切な SystemEDGE AIM を CA Virtual Assurance マネージャ サーバまたは個別の AIM サーバにインストールおよび設定します。

注: Microsoft Hyper-V については、管理する各物理 Microsoft Hyper-V Server に SystemEDGE および Microsoft Hyper-V AIM をインストールします。

サポートされるプラットフォーム

Active Directory および Exchange Server

Active Directory および Exchange Server のモニタリングを有効にするには、使用環境に以下の製品がインストールされていることを確認してください。

- .Net 3.5 以降のバージョン
- Power shell v2.0
- AIM ホスト上に Exchange Management Tools SP3 （Exchange Server 2007 のモニタリング用）

注: Exchange Management Tools SP3 は、Exchange Server 2010 のモニタリングには必要ありません。

Cisco Unified Computing System（UCS）

Cisco UCS の管理を有効にするには、環境内に以下の製品がインストールされていることを確認します。

- Cisco UCS 1.3、1.4、2.0

Citrix XenServer

Citrix XenServer の仮想管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

- Citrix XenServer バージョン 6.0

Huawei GalaX

Huawei GalaX のモニタリングおよび管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

- Huawei GalaX8800 バージョン 1.0

AIX 用 IBM HACMP

AIX 用 IBM HACMP のモニタリングを有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

IBM HACMP 6.1

AIX バージョン 6.1 プラットフォーム用の IBM HACMP により、クラスタ、ノード、およびネットワーク インターフェース ステータスをモニタできます。

IBM Power VM（論理パーティション、LPAR）

IBM LPAR の仮想管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

IBM AIX LPAR

IBM LPAR POWER5、POWER6、または POWER7 プラットフォームでは、AIX 上およびその管理対象システム上の論理パーティションを管理できます。

IBM Hardware Management Console（HMC）

IBM POWER5、POWER6、または POWER7 プラットフォームの論理パーティションを管理するには、HMC V7R3.5、V7R7.1、V7R7.2 をインストールします。

注: HMC V7R7.1 は POWER7 によってサポートされる最低レベルです。

IBM Integrated Virtualization Manager（IVM）

論理パーティションを管理するために HMC の代わりに使用します。仮想 I/O サーバ（VIOS）上で実行されます。

IBM Virtual I/O Server（VIOS）

IBM Virtual I/O Server（VIOS）を使用すると、IBM AIX POWER5、POWER6、および POWER7 の論理パーティションを設定できます。

注: VIOS バージョン 1.5、2.1、および 2.2 がサポートされています。

Microsoft Cluster（MSCS）

Microsoft クラスタの管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

- Windows Server 2003 と Windows Server 2008 をベースにした Microsoft クラスタ

Microsoft Hyper-V Server

Microsoft Hyper-V Server の仮想管理を有効にするには、環境内に以下のいずれかの製品が少なくとも 1 つインストールされていることを確認してください。

- Hyper-V Server 2008 R2 （64 ビット、x64）

注: 予約マネージャは、Windows Server 2003 および Windows Server 2008 オペレーティング システムの Hyper-V プロビジョニングをサポートします。

Oracle Solaris ゾーン

Oracle Solaris ゾーン サーバの仮想管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

- Solaris ゾーンを管理するゾーン互換性を備えた Solaris 10 。

Red Hat Enterprise Virtualization

Red Hat Enterprise Virtualization の仮想管理を有効にするには、使用環境に以下のコンポーネントがインストールされていることを確認してください。

- RHEV 3.0

VMware vCenter Server

VMware vCenter Server の仮想管理を有効にするには、以下のいずれかのコンポーネントが環境内にインストールされていることを確認してください。

VMware ESX サーバ/VMware ESXi サーバ

VM セッションを作成するには、バージョン 4.0、4.1、5.0、または 5.1 が必要です。

注: ESX サーバおよび ESXi サーバをサポートするには、vCenter Server が ESX サーバまたは ESXi サーバを管理するように設定されている必要があります。

VMware vCenter Server

仮想マシンのクローン作成とマイグレート、および VMware vSphere の管理には、VMware vCenter Server version 4.0、4.1、5.0、または 5.1 が必要です。

注: VMware ツールによって VM が最適化されるので、VMware 環境内の各 VM に VMware ツールをインストールすることを強くお勧めします。 VMware ツールがインストールされていない VM では、この製品の一部の機能が利用できないか、正しく動作しません。 この理由により、VMware ツールがインストールされていない VM はサポートされていません。

VMware vCloud

VMware vCloud の仮想管理を有効にするには、環境内に以下のコンポーネントがインストールされていることを確認してください。

- VMware vCloud Director バージョン 1.5 および 5.1

第 3 章: 新しい機能および拡張機能

このセクションには、以下のトピックが含まれています。

Huawei GalaX

このリリースでは、以下の新機能または変更が利用可能です。

Huawei GalaX のモニタリング

CA Virtual Assurance は Huawei GalaX 環境をモニタします。

Huawei GalaX の管理

CA Virtual Assurance は Huawei GalaX 環境を管理します。

マルチインスタンス

SystemEDGE GalaX AIM は複数の Huawei GalaX 環境を管理できます。

リモート展開

このリリースの CA Virtual Assurance では、以下の RSI 機能がサポートされます。

AIM 展開のサポート

Huawei GalaX AIM の展開を可能にするデフォルトのパッケージ ラッパーを提供します。

ユーザ インターフェース

このリリースでは、以下の新機能または変更が利用可能です。

ローカライズされたユーザ インターフェース

ユーザ インターフェースは英語と日本語で利用可能です。

製品バナー

ユーザ インターフェースの上部のセクションには以下の変更が含まれます。

- 検索はサービス テンプレートおよびアプリケーションを検索するために使用できます。
- ［ヘルプ］ドロップダウン リストでは、［満足度の取得］リンクに代わって CA サポート チャネルへのリンクが提供されます。

ドキュメント

このリリースのドキュメントには、製品詳細、サポート資料、および研修サービスなどの、シナリオおよび補足情報へのリンクがあるエンドツーエンドのマニュアル選択メニューが含まれています。

マニュアル選択メニューは、［スタート］メニューから直接開くか、またはオンライン ヘルプやローカル ヘルプのナビゲーション ペインで［マニュアル選択メニューへ戻る］をクリックして開くことができます。

以下のシナリオとユース ケースがドキュメントに追加され、マニュアル選択メニューから直接アクセスできます。

- Huawei GalaX 管理コンポーネントを設定する方法
- Virtual Private Cloud を作成する方法
- Huawei SingleCLOUD 環境を管理する方法
- SQL Server ユーザ権限を必要最小限に調整する方法

第 4 章: 前リリース(12.7)の新機能および拡張機能

このセクションには、以下のトピックが含まれています。

Exchange Server および Active Directory 用の AIM

このリリースには以下が含まれます。

Exchange Server および Active Directory 用の AIM

Active Directory および Exchange Server 用の AIM を使用すると、クラウドおよび社内運用の両方のインフラストラクチャ上の Active Directory 環境と Exchange Server 環境をモニタできます。このリリースでは、以下がサポートされます。

- Microsoft Exchange Server 2007
- Microsoft Exchange Server 2010
- Microsoft Active Directory 2008

サポートされるオペレーティング システム

- Windows Server 2008 Standard、Enterprise、および Data Center Edition
- Windows Server 2008 R2 Standard、Enterprise、および Data Center Edition

注: このリリースの Active Directory および Exchange Server 用の AIM では、国際化はサポートされていません。

Citrix XenServer

このリリースでは、以下の新機能または変更が利用可能です。

Citrix XenServer の管理とモニタリング

CA Virtual Assurance は Citrix XenServer 6.0 環境をモニタおよび管理します。

マルチインスタンス

XenServer AIM は複数の XenServer を管理できます。

XenServer プロビジョニングのカスタマイズ

CA Virtual Assurance では、Windows 2003 R2 Server （32 ビット/64 ビット）、Windows 2008 （32 ビット/64 ビット）または Windows 2008 R2 Server （64 ビット）を実行する新しい仮想マシン（VM）でのプロビジョニングのカスタマイズをサポートしています。カスタマイズ オプションには多数の設定があります。 たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

ドキュメント

このリリースのドキュメントには、製品詳細、サポート資料、および研修サービスなどの、シナリオおよび補足情報へのリンクがあるエンドツーエンドのマニュアル選択メニューが含まれています。

マニュアル選択メニューは、［スタート］メニューから直接開くか、またはオンライン ヘルプやローカル ヘルプのナビゲーション ペインで［マニュアル選択メニューへ戻る］をクリックして開くことができます。

以下のシナリオとユース ケースはドキュメントに含まれており、マニュアル選択メニューから直接アクセスできます。

- ポリシーおよび階層型テンプレートをサーバに適用する方法
- マネージャ サーバのバックアップ方法
- SystemEDGE の設定モードの変更方法（管理対象モード、管理対象外モード）

- 管理対象外モードから管理対象モードへの SystemEDGE の変更方法
- Active Directory および Exchange Server 用の AIM の設定方法
- サポートされている各仮想環境（vCenter、vCloud、PowerVM、Cisco UCS、Hyper-V、Red Hat Enterprise Virtualization、Solaris ゾーン、XenServer）の管理コンポーネントの設定方法
- Microsoft Cluster Service 管理の設定方法
- SNMPv1/v2 設定およびアクセス制御リストの設定方法
- SNMPv3 の設定方法
- Active Directory および Exchange Server 用の AIM の設定方法
- リソースを動的にモニタする自動ウォッチャーの作成および適用方法
- eHealth との統合方法
- CA Spectrum IM との統合方法
- KVM のプロビジョニング用に Windows テンプレートを準備する方法
- XenServer のプロビジョニング用に Windows テンプレートを準備する方法
- サーバ レベルの SNMP 設定を管理する方法
- CA Virtual Assurance の更新方法
- CA Virtual Assurance のアップグレード方法
- ポリシー アクションを使ってパフォーマンスの問題を特定する方法
- スケーラビリティのベスト プラクティス
- ユーザ権限およびアクセス要件のベスト プラクティス

IBM HACMP

このリリースでは、以下の新機能または変更が利用可能です。

HACMP **モニタリング**

HACMP AIM は、HACMP モニタリング用に、パフォーマンス メトリックを提供します。

IBM LPAR

このリリースでは、以下の新機能または変更が利用可能です。

統合管理パネル

IBM PowerVM の設定は、**VC** やゾーンなど、ほかのプラットフォームと統合されています。 設定される **HMC** によって管理される **Power** サーバはすべて自動的に管理されます。 **CA Virtual Assurance** では、**HMC** に後で追加される新しい **Power** サーバを自動的に検出します。

複数の共有プロセッサ プール

複数のプロセッサ プールを作成し、リソースの柔軟な割り当てが可能になります。 選択された管理対象 **Power** システムの［サマリ］タブに［プロセッサ プール］ペインが追加されました。

デュアル HMC

CA Virtual Assurance はデュアル **HMC** をサポートします。 *デュアル **HMC*** は、高可用性を提供する冗長なハードウェア管理コンソール（**HMC**）管理システムです。**2** つの **HMC** により **1** つのシステムを管理する場合、それらはピアになります。 各 **HMC** は管理対象システムの制御に使用できます。**1** つの **HMC** で複数の管理対象システムを管理できます。また、各管理対象システムは **2** つの **HMC** を持つことができます。

優先 AIM

ユーザ インターフェースの［管理］タブにある［**HMC/IVM** サーバ］設定が機能拡張され、優先 **AIM** を指定できるようになりました。

管理ステータス

［**HMC/IVM** サーバ］設定により、**HMC/IVM** サーバの管理を有効または無効にすることができます。

仮想 I/O サーバ（VIOS）のデフォルトの認証情報

VIOS のデフォルト認証情報は、特定の **HMC** サーバに対して検出された **VIOS** に適用されます。

複数の仮想 I/O サーバ

CA Virtual Assurance では、複数の仮想 **I/O** サーバ（**VIOS**）をサポートします。 *複数の仮想 I/O サーバ*を使用すると、クライアント パーティションのダウンタイムのない仮想 **I/O** サーバ メンテナンスを可能にすることによってアプリケーションの可用性を向上させる機能が提供されます。**CA Virtual Assurance** では、**Power** サーバに付属している **VIOS** をすべて検出し、**VIOS** アクセス認証情報を設定することができます。

未設定コンポーネントの遅延ロード

この機能では、未設定の登録済みコンポーネントの警告ステータス  （*設定されていません*）を提供します。

ファイバ チャネルのサポート

CA Virtual Assurance は、ファイバ チャネル仮想化およびワールド ワイド ポート名（**WWPN**）の可用性のステータスに関する重要な情報を提供します。 *ファイバ チャネル*は、コンピュータ デバイス間でデータを転送するための、標準化されたギガビット速度テクノロジです。ファイバ チャネルは、コンピュータ サーバを共有ストレージ デバイスに接続したり、ストレージ コントローラとストレージ ドライブを相互接続したりするのに特に適しています。

Oracle Solaris ゾーン

このリリースでは、以下の新機能が利用可能です。

完全ルート ゾーン プロビジョニング

ゾーンを作成するときに「完全ルート ゾーン」タイプを指定することができます。完全ルート ゾーンは、パッケージを継承しない自己完結型のゾーンで、グローバル ゾーン **OS** から独立しています。

ポリシー設定

このリリースでは、以下の新機能または変更が利用可能です。

強化されたマシンの検索結果

CA Virtual Assurance ユーザ インターフェースの検索結果のポリシー設定情報を提供します。

複数のモニタの削除

単一のアクションでポリシーまたはテンプレートから複数のモニタを削除することができるため、設定のモニタリングが容易になります。

グローバル SNMP オブジェクトと ACL の関連付け

ポリシーを介してシステムに適用されるグローバル **SNMP** オブジェクトで、アクセス制御リストをサポートします。

サーバに固有の SNMP 設定

サーバ レベルで、アクセス制御リストおよび **SNMP** 設定をサポートします。ポリシーを介してシステムにこれらの設定を適用するかどうかを決定できます。

自動ウォッチャー

汎用、サービス、およびプロセスの自動ウォッチャーにより、動的なリソース モニタリングをサポートします。

エージェントの検出

ポリシー設定では、利用可能な名前およびアドレスをすべて使用して、ポリシー設定にまだ登録されないエージェントを検出することができます。

モニタおよび自動ウォッチャーのインデックス再作成

モニタおよび自動ウォッチャーのインデックスを **1** 回の操作で再割り当てすることができます。

ポリシーまたはテンプレートのインポートとエクスポート

ポリシーとテンプレートを **CA Virtual Assurance** インスタンスからエクスポートしたり、別の **CA Virtual Assurance** インスタンスへインポートしたりすることができます。

マネージャの変更のサポート

既存のマネージャでリモート **SystemEDGE** エージェントを再設定し、別のマネージャで登録することができます。

このリリースでは、CA Virtual Assurance により以下のポリシー設定レポートが提供されます。

エージェント リスト(配布サーバ別)レポート

配布サーバ別に管理された **SystemEDGE** エージェントを表示し、設定が最新かどうかを示します。

エージェント リスト(ポリシー別)レポート

ポリシー別に管理された **SystemEDGE** エージェントを表示し、設定が最新かどうかを示します。

システムによる設定例外レポート

ポリシーまたはテンプレートが最後に適用された後に、**SNMP** を介して設定が変更されたシステムのレポートを表示します。

管理対象エージェント リスト レポート

管理対象モードの **SystemEDGE** エージェントを一覧表示します。

ポリシー/テンプレート別期限切れ設定レポート

エージェントで現在期限切れのポリシーおよびテンプレートをポリシー別およびテンプレート別に表示します。

システム別期限切れ設定レポート

エージェントで現在期限切れのポリシーおよびテンプレートをマシン別に表示します。

ポリシーとポリシー テンプレートの詳細レポート

選択したポリシーまたはテンプレートのレポートを表示します。

システム設定の詳細レポート

選択したシステムに適用された設定のレポートを表示します。

未設定システムのレポート

ポリシー設定で登録されていないシステムを表示します。

Red Hat Enterprise Virtualization

このリリースでは、以下の新機能または変更が利用可能です。

Red Hat Enterprise Virtualization のモニタリング

CA Virtual Assurance は RHEV 3.0 環境をモニタします。

RHEV プロビジョニングのカスタマイズ

CA Virtual Assurance では、Windows 2003 R2 Server （32 ビット/64 ビット）、Windows 2008 （32 ビット/64 ビット）または Windows 2008 R2 Server （64 ビット）を実行する新しい仮想マシン（VM）でのプロビジョニングのカスタマイズをサポートしています。カスタマイズ オプションには多数の設定があります。 たとえば、組み込みの管理者アカウントのパスワード、コンピュータ名、およびネットワーク設定を変更できます。

リモート展開

このリリースの CA Virtual Assurance では、以下の RSI 機能がサポートされます。

新しいプラットフォームのサポート

SystemEDGE は、リモート展開を使用する IBM Power PC 上の RedHat Linux をサポートします。

展開レポート

指定の配布サーバの一定期間における展開ジョブ ステータスを取得するための新規レポートを提供します。［レポート コンポーネントの選択］および［ジョブの選択］では、さまざまなレポート生成オプションを提供します。

コンテキスト メニューを使用した管理対象ノードへの展開

リモート展開ジョブ ウィザードを開くことができます。 ジョブ ウィザードはターゲットとして選択したノードにのみ展開します。

［ジョブ］パネルの更新

ページング、フィルタリング、ソート、およびその他のジョブ詳細のカスタマイズをサポートします。

AIM 展開のサポート

以下の **AIM** の展開を可能にするデフォルトのパッケージ ラッパーを提供します。

- High Availability Cluster Multiprocessing （HACMP） 用の AIM
- Citrix XenServer （XEN） 用の AIM
- VMware vCloud （VCLOUD） 用の AIM
- Active Directory および Exchange Server （ADES）用の AIM
- Red Hat Enterprise Virtualization （KVM）用の AIM

共通ジョブ トラッキング ポートレット

リモート展開ジョブの強化されたジョブ トラッキングを提供します。

強化された検索結果

検索結果のリモート展開操作への迅速なアクセスを提供します。

展開ジョブ ウィザードの更新

ジョブ ウィザードで **EULA** を削除します。

SystemEDGE パッケージ ラッパーの更新

ラッパーで **SNMP** コミュニティ文字列を更新して検証します。

ユーティリティの更新

このリリースでは、以下の新機能または変更が利用可能です。

CA Virtual Assurance の更新

［スタート］メニューから **CA Virtual Assurance** 更新ユーティリティを実行して、**CA Virtual Assurance** の利用可能な **PTF** （**Program Temporary Fix**）を選択してダウンロードできます。 製品の **bin** ディレクトリにある **dpminstapplyptfs.exe** からパッチをインストールできます。

ユーザ インターフェース

このリリースでは、以下の新機能または変更が利用可能です。

製品バナー

ユーザ インターフェースの上部のセクションには以下の新しいコントロールが含まれます。

- ［セルフ サービス ポータル］リンクでは、Liferay ベースのポータル インターフェースにアクセスします。
- ［管理/ダッシュボード］リンクは、ダッシュボードと操作ページを切り替えます。
- ［ヘルプ］ドロップダウン メニューには、以下の項目が含まれます。
  - オンライン ヘルプ（support.ca.com の最新ドキュメント）
  - ローカル ヘルプ（Web アクセスを行わないシステム用）
  - CA サポート（support.ca.com - 登録済みのログインが必要）
  - 満足度の取得（オンライン フィードバック ディスカッション）
  - バージョン情報（製品情報）

ダッシュボード

このリリースでは、ダッシュボードはより大きく、合理化されており、以下の機能が提供されます。

- インタビュー形式で操作を選択できる［ファースト ステップ］ダッシュボード。
- サービス プロビジョニング機能にアクセスする［サービス］ダッシュボード。
- 動作環境に基づいた計算を保存する［見積もり削減状況］ダッシュボード。
- グループ化および根本原因と関連する［ジョブ］/［イベント］/［アラーム］コンソール。

右下角の［設定］メニューでは、以下の項目にアクセスします。

- ダッシュボード（ダッシュボードとポートレットのプロパティおよびライブラリ）
- ユーザ設定（リフレッシュとイベントの設定）

管理

追加された機能は以下のとおりです。

- 下部パネルの［ジョブ］テーブル
- ドラッグ アンド ドロップ： サーバをサービスへ、サービス プロファイルを UCS ブレードへ

VMware vCloud

このリリースでは、以下の新機能または変更が利用可能です。

VMware vCloud の管理とモニタリング

CA Virtual Assurance は VMware vCloud Director 1.0、1.0.1、または 1.5 環境をモニタおよび管理します。

マルチインスタンス

vCloud AIM では、複数の VMware vCloud Director サーバを管理できます。

第 5 章: パッチおよび発行済みの修正プログラム

このバージョンの製品で、パッチおよび発行済みの修正プログラムが利用可能な場合があります。 CA サポート オンライン Web サイト（http://supportconnect.ca.com）にアクセスして、製品のインストールまたはアップグレードを進める前に、パッチをダウンロードするか、発行済みの修正プログラムを参照してください。 パッチおよび発行済み修正プログラムは、Download Center の［Published Solutions］ペインから入手可能です。

このセクションには、以下のトピックが含まれています。

SNMPv3 トラップの転送の問題

CA Virtual Assurance の SNMPv3 トラップを正常に受信するには、CA NSM イベント マネージャを特定の方法で設定する必要があります。CA NSM イベント マネージャが適切に設定されていない場合、処理中のトラップが終了します。

重要: CA NSM 11.1 の場合： CA の修正プログラム QO99777 および Microsoft の修正プログラム 931565 を適用する必要があります。

CA NSM の問題の詳細については、CA サポート オンライン（http://www.ca.com/jp/support/）で修正プログラム番号 QO99777 を参照してください。 ［Technical Support］、［Download Center］の順にクリックし、［Quick Search］フィールドに修正プログラム番号 QO99777 を入力して、製品情報に関する報告を検索します。

また、Microsoft のサポート Web サイトでサポート技術情報の記事 931565 を検索する必要があります。この記事では、Windows Server 2003 ベースのコンピュータ上でサードパーティ製のセキュリティ スキャン ソフトウェアを実行したときに、WinSNMP アプリケーションが停止する状況について説明されています。

第 6 章: マニュアル

このセクションには、以下のトピックが含まれています。

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が記載されています。

SystemEDGE ユーザ ガイド

SystemEDGE のインストールおよび設定の詳細について説明します。

SystemEDGE リリース ノート

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

第 7 章: 既知の問題

CA サポート オンライン上の *CA Virtual Assurance リリース ノート*には、発行後に検出された問題およびその他の情報が記載されています。

最新バージョンのリリース ノートについては、
http://www.ca.com/jp/support にアクセスしてください。

1. CA サポート オンラインにログインします。
2. ［Enterprise/Small and Medium Business］を選択します。
3. ［Documentation］を選択します。
4. ［Bookshelf］ドロップダウン リストから［CA Virtual Assurance Bookshelf］を選択して、［実行］をクリックします。
5. ［Bookshelf］ウィンドウからリリース ノートを開きます。

このセクションには、以下のトピックが含まれています。

ローカライズされた Service Desk テンプレート名が切り捨てられる

症状:

CA Virtual Assurance が CA Service Desk（CA Service Desk Manager）と統合されていて、Service Desk テンプレート名がローカライズされる場合、テンプレート名は切り捨てられることがあります。 CA Service Desk Manager は、最大長を超えるテンプレート名を処理できません。 テンプレート名の最大長は 30 文字の半角文字または 15 文字の全角文字です。

解決方法:

テクニカル サポート問題を解決し、テスト修正パッチをリクエストします。 問題番号 USRD 2248 をレポートします。

ログイン プロセスが遅い

症状:

ユーザ管理が Active Directory に接続する場合、ログイン プロセスに時間がかかる場合がある。

解決方法:

CA EEM は、デフォルトの LDAP ポート 389 を使用して、Active Directory をバインドできます。 ログインに時間がかかる場合は、グローバル カタログ ポート 3268 に変更します。

次の手順に従ってください:

1. CA EEM を開始します。

   ログイン ページが表示されます。

2. アプリケーションとして「AIP」、ユーザとして「EiamAdmin」を選択し、ログインします。

   ユーザ インターフェースが表示されます。

3. ［設定］ - ［EEM サーバ］を選択します。

   ［EEM サーバ］ペインが表示されます。

4. ［グローバル ユーザ］ / ［グローバル グループ］を選択します。

   ユーザ インターフェースに［グローバル ユーザ］/［グローバル グループ］のプロパティが表示されます。

5. ［ポート番号］を「3268」に変更し、［保存］をクリックします。

   変更は直ちに有効になります。 この変更後、いずれかのサービスをリサイクルする必要はありません。

Mozilla Firefox の自動アップグレード

症状:

Mozilla Firefox ブラウザのアップグレード後に、CA Server Automation Web アプリケーションを使用すると、ページ レンダリングの問題が発生する場合があります。

解決方法:

Mozilla Firefox が自動的にアップグレードされる場合があります。 ページ レンダリングの問題が発生した場合は、ブラウザがアップグレードされたかどうかを確認し、ブラウザのキャッシュをクリアします。

付録 A: 使用条件

この付録には、CA Virtual Assurance で使用されるサードパーティ製ソフトウェアの著作権および使用許諾契約情報が含まれます。

このセクションには、以下のトピックが含まれています。

サードパーティ製ソフトウェアの使用条件 (P. 57)

サードパーティ製ソフトウェアの使用条件

このセクションでは、サードパーティ製ソフトウェアの使用条件に関する情報が提供されます。 サードパーティ使用許諾契約は、CA マニュアル選択メニュー内の ¥Bookshelf Files¥TXT フォルダで利用可能です。

- Adobe Flex SDK
- AIX JRE
- Apache Axis2 1.5.2
- Apache HTTP Web Server 2.2.23
- Apache Software Foundation
- Apache Solr 1.4.1
- Apache Tomcat 6.0.35
- base64 0.00.00B
- Boost 1.42
- bzip2 1.0.2
- Castor 0.9.5.4
- concurrent utilities 1.3.4
- curl 7.25.0
- Eclipse BIRT Runtime v. 2.3.2.2
- Expat 2.0.1
- Hibernate 3.2.2
- HP-UX JRE 6.0.14 PA-RISC

- HSQLDB 1.8
- ICU4C 3.4
- ipmitool 1.8.10
- JAXB 2.1
- JAXP 1.4.2
- JGoodies Looks 2.2.0
- JRE v1.6
- JSMin
- json-lib 2.4
- JSW v.3.2.3
- JXTA 2.3.6
- libarchive 3.0.2
- libcurl 7.21.0 and libcurl 7.21.1
- libssh2 1.2.6
- libtorrent 0.15.7
- Libxml2 2.7.7、Libxml2 2.7.8、Libxml2 2.8.0、および Libxml2 2.9.0
- Libxslt 1.1.24（../../TXT/Libxslt1.1.24.txt）
- MIT Kerberos v5 release 1.4
- Mod_gsoap 0.7
- NetApp NMSDK 4.0
- Netscape Portable Runtime 4.7.1
- netx 0.5
- node.js 0.4.12
- NUNIT 2.2.8
- OpenFire 3.7.1
- OpenLDAP 2.1
- openSSH for Windows CE 0.0.2 Alpha
- OpenSSL 0.9.8g, 0.9.8h, 0.9.8j, and 0.9.8o
- OpenSSL 0.9.8r and OpenSSL 0.9.8u

- OpenSSL 0.9.8x
- openwsman 2.0
- Oracle JDBC Driver 10G Release 2
- Oracle JDK 1.6.0_32（../../TXT/OracleJDK1.6.0_32.txt）
- PCRE 8.1 and PCRE Library 8.12
- Pegasus 2.7
- Perl 5.12.2
- PHP 5.3.13（../../TXT/PHP5.3.13.txt）
- POCO 1.3.2
- PuTTY 0.60
- py2exe for Python 2.6.x 0.6.9
- Python 2.6
- Rhino 1.6R4
- Sun JDK 1.6.0
- Sun JRE v.1.6
- swfobject 2.1
- Ubuntu 10.04
- VIX API
- Windows Installer XML (WiX)
- Zlib 1.2.3 and Zlib 1.2.5