

アップグレード ガイド

CA Application Delivery Analysis
バージョン 10.1



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」）により隨時、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写、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 © 2014 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: 製品のアップグレード	7
アップグレードパス	8
アップグレードに関する考慮事項	9
前提条件	10
データベースのバックアップ	11
Windows Server 2008 R2 へのマイグレート	11
CA ADA 監視デバイスのマイグレート	12
CA ADA マネージャのマイグレート	14
ソフトウェアのアップグレード	16
トラブルシューティング	17
CA Single Sign-On ポート変更	18
前のインストールの一部を削除できない	18
データベース ヘルス チェックの失敗	19

第1章：製品のアップグレード

アップグレードプロセスでは、以下のアップグレードが可能です。

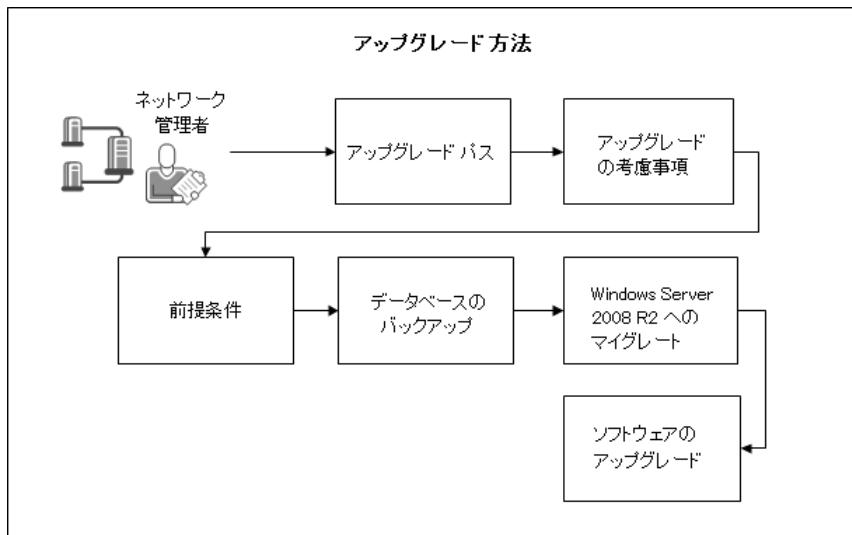
スタンドアロン展開

管理コンソールおよび CA Standard Monitor が同じサーバにインストールされています。

分散展開

管理コンソールおよび CA Standard Monitor が異なるサーバにインストールされています。

以下の図はアップグレードプロセスを示しています。



以下のトピックで、アップグレードプロセスを説明します。

1. [アップグレードパス \(P. 8\)](#)
2. [アップグレードに関する考慮事項 \(P. 9\)](#)
3. [前提条件 \(P. 10\)](#)
4. [データベースのバックアップ \(P. 11\)](#)
5. [Windows Server 2008 R2へのマイグレート \(P. 11\)](#)
6. [ソフトウェアのアップグレード \(P. 16\)](#)

アップグレード パス

CA Application Delivery Analysis をバージョン 9.2 または 9.3 から 10.1 にアップグレードします。必要に応じて、バージョン 9.2 または 9.3 にアップグレードしてから、10.1 にアップグレードします。

重要: CA ADA 10.1 は、Multi-Port Monitor バージョン 9.2 と互換性がありません。CA ADA マネージャを 10.1 にアップグレードする場合、データ収集を再開するにはバージョン 9.2 Multi-Port Monitor をバージョン 10.0 以降にアップグレードする必要があります。

環境別の手順 :

Windows Server 2008 R2 Standard

CA Application Delivery Analysis を現在のバージョンにアップグレードします。

Windows Server 2003

Windows Server 2003 から Windows Server 2008 R2 Standard に CA ADA をマイグレートすることをお勧めします。

CA Application Delivery Analysis が NetQoS Performance Center にデータ ソースとして登録されており、両方の製品が同じコンピュータにインストールされている場合は、アップグレードしないでください。CA Application Delivery Analysis で提供される CA Single Sign-On アプリケーションは、CA NetQoS Performance Center で提供される CA Single Sign-On とは互換性がありません。代わりに、CA NetQoS SuperAgent を Windows Server 2008 にマイグレートします。

アップグレードに関する考慮事項

CA Application Delivery Analysis 10.1 は以下に対するデータ ソースです。

- CA NetQoS Performance Center 6.1 以降
- CA Performance Center 2.3

アップグレードの前に、以下の内容について考慮します。

- リリース ノートを参照して、アップグレードに関する既知の問題など、このリリースに関する重要な情報を確認します。
- スタンドアロン展開をアップグレードする場合、アップグレードプロセスは管理コンソールを分散管理コンソールに変換します。アップグレード後、管理コンソールはその監視ポート上の SPAN 監視サポートを引き続き提供します。CA では、スタンドアロン管理コンソールを提供しなくなりました。
- CA ADA 9.2 または 9.3 からアップグレードする場合、Standard Monitor および ADA マネージャが正しく動作するためには、両方を 10.1 にアップグレードする必要があります。ADA マネージャと Standard Monitor のバージョンが異なる場合、監視デバイスによって収集されるデータをレポートに使用することはできません。
- アップグレード処理の過程で、CA Application Delivery Analysis のアップグレードに加え、以下の製品がインストールされている場合は、以下にリストされているサポート対象バージョンにアップグレードすることを検討してください。
 - CA Multi-Port Monitor Version 10.0 以降
 - CA GigaStor と CA Observer バージョン 16 および更新された CA GigaStor コネクタ (CA Application Delivery Analysis 10.1 で提供されています)。

前提条件

CA Application Delivery Analysis ソフトウェアをアップグレードする前に、以下のタスクを実行します。

- CA ADA マネージャをアップグレードする場合：
 - データベースをバックアップします。 詳細については、[「データベースのバックアップ」\(P. 11\)](#)を参照してください。
 - 十分なディスク空き容量があることを確認します。 C: および D: ドライブパーティション上の利用可能なディスク容量は、<インストールパス>\mysql51\data\super 内の最大ファイルより大きくする必要があります。
- アプリケーションサーバの役割（Microsoft .NET Framework 3.5.1 を含む）がインストールされていることを確認します。アップグレードプログラムでは、Microsoft .NET Framework 3.5.1 がインストールされていることを必要とします。
- すべてのサーバおよび仮想マシン上で、以下の種類のサードパーティソフトウェアを無効にします。
 - アンチウイルス
 - アンチスパイウェア
 - サーバ監視およびメンテナンスツール (SMS、SUS、または MoM など)
- カスタマイズした設定ファイルをすべてバックアップします。たとえば、CA Application Delivery Analysis Standard Monitor 上のパケットキャプチャ調査を無効にするために InspectorAgent.exe.config ファイルを編集した場合、アップグレード後にこの変更をリストアする必要があります。
- 利用可能なオペレーティングシステムパッチが確実に適用されるようにするため、サーバをすべて再起動します。

- セットアッププログラム (ADASetup10.1.xxx.exe) を [CA テクニカルサポート](#) から取得し、ソフトウェアをインストールするサーバまたは仮想マシンにプログラムをコピーします。
- セットアッププログラムの実行が許可されていることを確認します。
 - a. セットアッププログラムを右クリックし、[プロパティ] を選択します。
 - b. [禁止の解除] をクリックします。
 - c. [OK] をクリックします。

データベースのバックアップ[®]

CA ADA ソフトウェアをアップグレードする前に CA ADA マネージャ データベースをバックアップします。

以下の手順に従います。

1. CA ADA マネージャ サーバにログインします。
2. サービスマネージャを開きます。
3. NetQoS MySQL51 を含め、CA および NetQoS のサービスをすべて停止します。
4. CA ADA インストールディレクトリを参照し、¥mysql51¥data フォルダとその中身をリモートのバックアップ場所にコピーします。

Windows Server 2008 R2 へのマイグレート

CA ADA コンポーネントを Windows Server 2003 から Windows Server 2008 R2 Standard にマイグレートすることをお勧めします。これには以下が含まれます。

- CA Standard Monitor
- CA Virtual Systems Monitor
- CA ADA マネージャ

CA ADA マネージャをマイグレートする前に、CA ADA 監視デバイスをマイグレートします。CA ADA を Windows Server 2008 R2 Standard にインストールする詳細については、「インストールガイド」を参照してください。

CA ADA 監視デバイスのマイグレート

CA ADA 監視デバイスを Windows Server 2003 から Windows Server 2008 R2 にマイグレートします。これには以下が含まれます。

- CA Standard Monitor
- CA Virtual Systems Monitor

Windows オペレーティング システムの標準アップグレードを実行しないでください。代わりに、以下で新しいサーバをプロビジョニングします。

- Windows Server 2008 R2 Standard

重要: CA ADA 監視デバイスの既存の IP アドレスを新しいサーバにマイグレートすることを計画してください。同じ管理および監視の IP アドレスが必要です。

- CA ADA 10.1

注: CA ADA インストール パスを保持する必要はありません。

注: CA ADA のインストールの詳細については、「インストール ガイド」を参照してください。

次の手順に従ってください:

1. CA ADA 監視デバイスをホストする Windows Server 2003 で以下を実行します:
 - a. 管理および監視の IP アドレスを書き留めます。
 - b. CA ADA 監視デバイスをネットワークから削除します。
2. CA ADA 10.1 監視デバイスをホストする予定の Windows Server 2008 で以下を実行します:
 - a. Windows 2003 サーバに一致するよう管理および監視の IP アドレスを変更します。
 - b. CA ADA 監視デバイスをインストールします。
 - c. サーバを再起動します。
 - d. ミラーリングされたスイッチ ポートを監視 NIC に接続します。
 - e. サービスマネージャで、CA ADA Monitor サービスが実行中であることを確認します。
3. 管理者として CA ADA 管理 コンソールにログインし、以下のタスクを実行します。

- a. [環境管理] ページをクリックします。
- b. 歯車型アイコンをクリックし、[監視デバイスを同期] をクリックします。
- c. 管理コンソールがその監視デバイスからデータを受信することを確認するまで 10 分間待機します。

CA ADA マネージャのマイグレート

CA ADA マネージャを Windows Server 2003 から Windows Server 2008 R2 Standard にマイグレートします。

Windows オペレーティング システムの標準アップグレードを実行しないでください。代わりに、以下で新しいサーバをプロビジョニングします。

- Windows Server 2008 R2 Standard

重要: CA ADA マネージャの既存の IP アドレスを新しいサーバにマイグレートするよう計画してください。同じ管理 IP アドレスが必要です。

- CA ADA 10.1

重要: CA ADA 10.1 を同じディスクおよびフォルダ場所にインストールするよう計画してください。同じ CA ADA インストールパスが必要です。たとえば、CA ADA マネージャが Windows Server 2003 上の C:\NetQoS にインストールされる場合、Windows Server 2008 上でも C:\NetQoS にインストールされる必要があります。デフォルトでは、CA ADA 10.1 は C:\CA にインストールされます。

次の手順に従ってください:

1. CA ADA マネージャをホストする Windows Server 2003 で以下を実行します:
 - a. ホスト IP アドレスおよび CA ADA インストールパスを書き留めます (ディスクおよびフォルダを含む)。
 - b. サービスマネージャで、NetQoS MySQL51 サービスを停止します。
 - c. `drive:\netqos\mysql51\data\super` フォルダとその中身を共有フォルダにコピーします。
 - d. CA ADA マネージャをネットワークから削除します。
2. CA ADA マネージャ 10.1 をホストする予定の Windows Server 2008 で以下を実行します:
 - a. Windows Server 2003 に一致するようホスト IP アドレスを変更します。
 - b. Windows Server 2003 サーバにインストールされたのと同じディスクおよびフォルダ場所に CA ADA マネージャをインストールします。
 - c. サーバを再起動します。
 - d. サービスマネージャで、NetQoS MySQL51 サービスを停止します。

- e. Windows エクスプローラで、CA ADA インストールディレクトリを参照し、¥mysql51¥data¥super フォルダとその中身を削除します。
 - f. ¥super フォルダとその中身を共有フォルダから¥mysql51¥data¥ フォルダにコピーします。
 - g. コピーが完了したら、サーバを再起動します。
 - h. サービスマネージャで、CA ADA Monitor サービスが実行中であることを確認します。必要に応じて、サービスのスタートアップの種類を【自動】に設定し、データ収集を再開するためにサービスを開始します。
3. 管理者として CA ADA 管理コンソールにログインし、以下のタスクを実行します。
 - a. 【環境管理】ページをクリックします。
 - b. 歯車型アイコンをクリックし、【監視デバイスを同期】をクリックします。
 - c. 管理コンソールがその監視デバイスからデータを受信することを確認するまで 10 分間待機します。

ソフトウェアのアップグレード

スタンドアロン展開または分散展開においてソフトウェアをアップグレードします。種類別の手順

分散展開

管理コンソールをアップグレードする前に、CA Standard Monitor デバイスをアップグレードします。

スタンドアロン展開

管理コンソールおよび Standard Monitor は自動的にアップグレードされます。

セットアッププログラムは、ステータスを *drive:\CA\ADA_Uninstaller\Logs* に記録します。

アップグレード後、カスタマイズした設定ファイルをすべてリストアします。たとえば、CA Standard Monitor 上のパケットキャプチャ調査を無効にするために InspectorAgent.exe.config ファイルを編集した場合、アップグレード後にこの変更をリストアします。

以下の手順に従います。

1. サーバまたは仮想マシンに管理者としてログインします。
2. [サービス] で、CA ADA Inspector サービスを停止します。
3. ADASetup10.1.xxx.exe ファイルをダブルクリックします。
[ようこそ] ダイアログ ボックスが表示されます。
4. [次へ] をクリックします。
使用許諾契約 ウィンドウが表示されます。
5. 使用許諾契約の内容を確認して同意し、[次へ]をクリックします。
[既存の製品バージョンの検出] ウィンドウが表示されます。
6. [次へ] をクリックします。
[アップグレード サマリ] ウィンドウが表示され、インストール フォルダが識別されます。インストール フォルダは変更できません。

7. [インストール] をクリックします。
アップグレード処理が開始します。メッセージにアップグレードの進捗状況が表示されます。
8. CA ADA マネージャをアップグレードする場合、[データベース ヘルス チェック] ウィンドウが表示されます。[はい] をクリックしてチェックを実行します。
アップグレードが完了すると、[インストール完了] ウィンドウが表示されます。
9. システムを再起動するオプションを選択し、[完了] をクリックします。
30 分以内に新しいデータが管理コンソールのレポートに表示されると、アップグレードは成功です。
10. (オプション、ただし推奨) インストール ドライブでディスク デフラグを実行します。
 - a. CA および NetQoS 関連のサービスをすべて停止します。
 - b. システム ツール ウィンドウからディスク デフラグ ツールを実行します。

詳細:

[データベース ヘルス チェックの失敗 \(P. 19\)](#)

トラブルシューティング

詳細については、以下のセクションを参照してください。

CA Single Sign-On ポート変更

CA Application Delivery Analysis バージョン 9.1 からアップグレードした場合、CA Application Delivery Analysis 上の CA Single Sign-On 設定は、ユーザを認証するために別のポート (TCP 8381) を使用します。CA Multi-Port Monitor へのサインイン時には、CA Application Delivery Analysis マネージャの TCP 8381 上で実行される CA Single Sign-On アプリケーションにリダイレクトされます。ファイアウォール設定でこれが許可されていることを確認します。

アップグレード後、必要な場合は CA Application Delivery Analysis 上の CA Single Sign-On 設定を更新して、別の TCP ポート使用できます。詳細については、CA テクニカルサポートにお問い合わせください。

前のインストールの一部を削除できない

アップグレード実行可能ファイルが完了せず、前のインストール部分の削除に失敗したことを示すメッセージが表示される場合は、以下の手順に従います。

1. [キャンセル] ボタンを使用して、アップグレードスクリプトを中断します。
2. アップグレードスクリプトのインスタンスがすべて終了したら、アップグレード対象サーバを再起動します。
3. 再度アップグレードスクリプトを起動します。

データベース ヘルス チェックの失敗

アップグレード プログラムが完了せず、データベース ヘルス チェックに失敗したことを示すメッセージが表示される場合は、以下の手順に従います。

1. 問題の迅速な解決に役立てるため、エラーのスクリーン ショットを取得し、問題の原因となったテーブルにマークを付けます。
2. CA Support Online にログインし、“MySQL database corruption” を検索します。表示される解決策記事の手順に従い、スクリーン ショットでマーク付けされたテーブルを修復します。
3. アップグレード プログラムを再度実行します。