インストール ガイド

CA Application Delivery Analysis

10.1

ca technologies

CA への連絡先

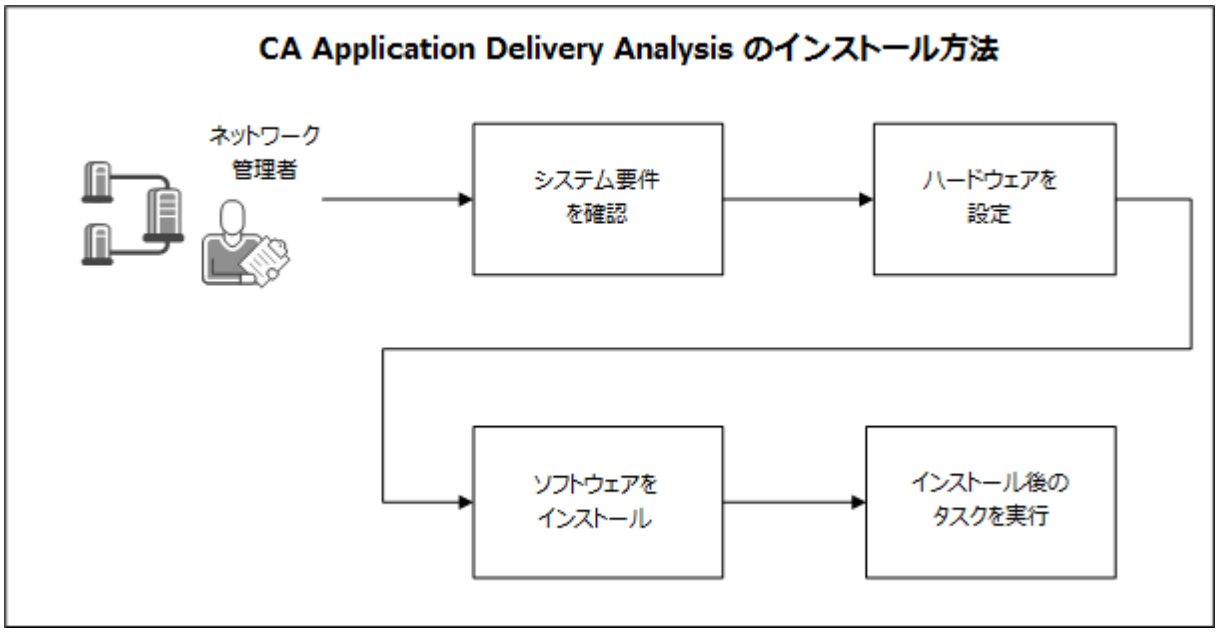
テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに

CA Application Delivery Analysis（CA ADA）は、レポート ページおよびビューでエンドツーエンドのパフォーマンス監視を提供します。 CA ADA は、トラブルシューティング情報を収集し、アプリケーション、ネットワーク、またはサーバのパフォーマンス問題の原因を特定するのに役立ちます。

以下の図は、CA ADA をインストールするプロセスを示します。



詳細:

システム要件 (P. 9)
インストール後の設定 (P. 35)
ソフトウェアのインストール (P. 29)
ハードウェアの設定 (P. 23)

第 2 章: システム要件

CA Technologies からハードウェアを購入した場合、すべてのコンポーネントはオペレーティング システムとセキュリティがすでに設定された状態で配布されます。 このセクションの手順を使用して、組織のニーズに合うように設定の検証や更新を行ってください。

ソフトウェアのみを購入した場合は、このセクションの内容に従って、オペレーティング システムを設定および保護します。

サーバ管理者は CA Application Delivery Analysis をインストールする必要があります。

開始する前に、必要なすべてのファイルを、インストール サーバにコピーしてください。 オペレーティング システムが保護された後は、ファイルが含まれている共有フォルダにアクセスできない可能性があります。

このセクションには、以下のトピックが含まれています。

サポートされているオペレーティング システム

CA Application Delivery Analysis コンポーネントは、Microsoft Windows 2008 R2 （Standard Edition）および以下を必要とします。

- 最新のサービス パックおよび重要な更新。
- Microsoft .NET Framework 3.5.1。
- Java Runtime Environment （JRE）。

  注: CA ADA セットアップ プログラムは JRE をインストールします。JRE を別途インストールすることはお勧めしません。
- 英語、中国語（簡体字）、または日本語。

  注: ［地域の設定］では、小数値を示すためにピリオド（.）を使用する必要があります。 たとえば、ポルトガル語（ブラジル）の地域設定は、小数値を示すためにデフォルトではカンマ記号を使用します。 地域設定をカスタマイズして、小数の記号をピリオドに変更します。
- 1024x768 （XGA）以上のディスプレイ解像度。
- ASP.NET 2.0 （COM+ ネットワーク アクセス、IIS、ASP を含む）
- このドキュメントで説明されているとおりに設定されたオペレーティング システム。
- SNMP および SMTP のサービスを有効にします。
- （推奨）管理者によるリモート アクセスを可能にするため、リモート デスクトップ接続を有効にします。
- IPv4 ホスト アドレス。 現時点では、IPv6 アドレスを持つサーバへのインストールはサポートされていません。

サポートされている Web ブラウザ

管理コンソールへのアクセスは、以下のブラウザでサポートされています。

- Microsoft Internet Explorer 7 または 8

  Internet Explorer 8 を使用して管理コンソールにアクセスすると、ページ上部のフォーマットが正しく表示されません。この問題を回避するには、Internet Explorer で F12 キーを押して、次に［ブラウザ モード］を［Internet Explorer 8］、［ドキュメント モード］を［Quirks モード］に設定します。

- Mozilla Firefox 11.x

他のブラウザやバージョンでも CA Application Delivery Analysis が動作する可能性がありますが、テストされているわけではありません。

ハードウェア要件

管理コンソールおよび Standard Monitor は別々のサーバにインストールしてください。管理コンソールは 1 つの管理 NIC で設定し、CA Standard Monitor などの監視デバイスからレスポンス時間メトリックを受信するようにします。

管理コンソール

CA は、管理コンソールを以下の仕様のサーバ上でテストしました。サーバが少なくとも以下の仕様を満たしている場合、どのベンダーのサーバでも管理コンソールがサポートされます。

- 2 つの Intel® E5520 Xeon クアド コア 2.66 GHz、1333 MHz FSB プロセッサ
- 24GB RAM
- 6 つの 146 GB SAS ハード ドライブ（RAID 5 構成）
- 最大 8 つの SAS ポート用バッテリ バックアップ キャッシュ付き RAID コントローラ
- 10/100/1000 Mbps イーサネット RJ-45 ポート
- Intel 82576 Gigabit Ethernet Controller

Standard Monitor

CA は、CA Standard Monitor を以下の仕様のサーバ上でテストしました。サーバが少なくとも以下の仕様を満たしている場合、どのベンダーのサーバでも Standard Monitor がサポートされます。

- Intel® E5520 Xeon クアドコア 2.66 GHz、1333 MHz FSB プロセッサ
- 3GB RAM
- 3 つの 146 GB SAS ハード ドライブ（RAID 5 構成）
- 最大 8 つの SAS ポート用バッテリ バックアップ キャッシュ付き RAID コントローラ
- 2 つの 10/100/1000 Mbps イーサネット RJ-45 ポート

  （オプション）2 つの監視 NIC 上の TCP トラフィックを監視するには、追加のイーサネット RJ-45 ポートをプロビジョニングします。
- Intel 82576 Gigabit Ethernet Controller

仮想マシン要件

CA Application Delivery Analysis は、VMware ESX® および VMware ESXi® 3.5、4.0、5.0 上で管理コンソールおよび CA Standard Monitor をサポートします。

物理サーバにストレスがかかる環境で同等のパフォーマンスを達成するには、物理サーバにあるよりも多くのメモリが VMware で必要になります。物理サーバは、ディスク I/O の領域では仮想マシンよりも優れています。CA Application Delivery Analysis サーバでは大きいディスク I/O 負荷が想定されます。 VMware マシン上で、同等以下のパフォーマンスになることが予期されます。

VMware 上に展開された CA Standard Monitor は、CA GigaStor Connector や WAN 最適化デバイス（Cisco WAE など）からのデータを受信できます。

重要: CA Application Delivery Analysis をホストする仮想マシンに VMware Tools をインストールします。 仮想マシン設定から CD/DVD ドライブを削除します。

Standard Monitor

CA は、Standard Monitor を以下の仕様の仮想マシン上でテストしました。お使いの仮想マシンが少なくとも以下の仕様に一致していることをお勧めします。

- 1 つの仮想プロセッサ
- 4GB RAM
- 300 GB の空きディスク領域
- 2 つの仮想ネットワーク アダプタ（最小 1 ギガビット） アップリンク ポート（ESX ホストから発信する物理ポート）は、仮想ネットワーク アダプタの 1 つで必要となります。

  （オプション）2 つの監視 NIC 上の TCP トラフィックを監視するには、追加のイーサネット RJ-45 ポートをプロビジョニングします。

管理コンソール

CA は、管理コンソールを以下の仕様の仮想マシン上でテストしました。お使いの仮想マシンが少なくとも以下の仕様に一致していることをお勧めします。

- 1 つの仮想プロセッサ
- 30 GB RAM
- 700 GB の空きディスク領域
- 1 つの仮想ネットワーク アダプタ（最小 1 ギガビット） アップリンク ポート（ESX Host から出る物理ポート）は、ネットワーク アダプタ上で必要です。

ファイアウォール要件

以下は、CA ADA コンポーネント間の通信を可能にするために開いておく必要のあるファイアウォール ポートをまとめたものです。

管理コンソールから

- CA Standard または Virtual Monitor に対して：TCP 1000、1001、3308、8080
- CA ADA Multi-Port Monitor に対して： TCP 80 および 8080

Standard Monitor または Virtual Monitor から

- 管理コンソールに対して： TCP 3308

CA ADA Multi-Port Monitor から

- 管理コンソールに対して： TCP 80、TCP 3308、TCP 8381

  CA Application Delivery Analysis 上の CA Single Sign-On 設定では、ユーザの認証に別のポート（TCP 8381）が使用されます。CA Multi-Port Monitor にサインインすると、CA ADA 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。

  必要に応じて、インストール後に CA ADA 上の CA Single Sign-On 設定を更新して、別の TCP ポート使用するようにできます。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。

Cisco NAM 上のメトリック エンジンから

- 管理コンソールに対して： TCP 9996

Cisco WAE 上の FlowAgent から

- CA Standard Monitor または Multi-Port Monitor に対して： TCP 7878
- 管理コンソールに対して： TCP 7878

CA GigaStor コネクタから

- CA Standard Monitor または Multi-Port Monitor に対して： UDP 9995
- 管理コンソールに対して： TCP 1001

Adobe アプリケーション

レポート、グラフ、製品ドキュメントを表示するには、Adobe® Acrobat Reader および Flash Player が必要です。

- Acrobat Reader の最新バージョンは http://get.adobe.com/reader/ からダウンロードしてインストールします。
- Flash Player の最新バージョンは http://get.adobe.com/flashplayer/からダウンロードしてインストールします。

サーバ役割および役割サービスのインストール

必要な Windows サーバの役割および役割サービスをインストールします。

次の手順に従ってください:

1. サーバに管理者としてログインします。
2. ［スタート］、［管理ツール］、［サーバ マネージャ］を選択します。

   ［サーバ マネージャ］ウィンドウが開きます。
3. 左側のコンソール ツリーで［役割］をクリックします。
4. ［役割の追加］をクリックします。

   ［役割の追加］ウィザードが表示されます。
5. ［次へ］をクリックします。
6. ［サーバーの役割の選択］リストから［アプリケーション サーバー］を選択します。

   アプリケーション サーバの役割には .NET Framework 3.5.1 が含まれます。
7. ［次へ］をクリックします。
8. ［次へ］をクリックします。

   アプリケーション サーバ用の［役割サービスの選択］ページが表示されます。
9. ［Web サーバー（IIS）サポート］役割サービスを追加します。
   a. ［Web サーバー（IIS）サポート］チェック ボックスを選択します。

      確認メッセージが表示されます。
   b. 確認メッセージ内の［必要な役割サービスを追加］をクリックします。

      ［役割サービスの選択］ページで、［Web サーバー（IIS）サポート］オプションが強調表示されます。
10. COM+ 役割サービスを追加します。
    a. ［COM+ ネットワーク アクセス］チェック ボックスを選択します。
    b. ［次へ］をクリックします。

11. IIS 6 管理互換を有効にします。
    a. 再度［次へ］をクリックします。

       Web サーバ（IIS）用の［役割サービスの選択］ページが表示されます。

    b. リストの［管理ツール］セクションの［IIS 6 管理互換］チェックボックスを選択し、［次へ］をクリックします。

       ［インストール オプションの確認］ページには、アプリケーション サーバの役割、Web サーバ（IIS）の役割、および .NET Framework 3.5.1 機能の設定について概要が表示されます。

12. IIS および COM+ の役割サービスと、選択したオプションをインストールします。
    a. ［インストール］をクリックします。

       ［進行状況］ページが表示されます。インストールが完了すると、［結果］ページが開きます。

    b. （オプション）［インストール レポートの印刷、電子メール送信、または保存］をクリックし、情報を確認してページを閉じます。

       ［インストール レポート］ページには、変更のサマリ、それらの変更に関する情報、インストールの完全なログの場所が表示されます。

    c. ［閉じる］をクリックします。

       ［役割の追加］ウィザードが閉じます。

13. ASP 役割サービスを追加およびインストールします。
    a. 左側のコンソール ツリーで、［役割］の下の Web サーバ（IIS）リンクをクリックします。

       ［Web サーバ（IIS）］ビューが右ペインに開きます。

    b. ［役割サービス］セクションの［役割サービスの追加］リンクをクリックします。

       ［役割サービスの追加］ウィザードで［役割サービスの選択］ページが開きます。

c. リストで［アプリケーション開発］の下の ASP チェック ボックスをオンにして［次へ］をクリックします。

［インストール オプションの確認］ページに、これまでの操作の概要と、関連するメッセージが表示されます。

d. ［インストール］をクリックします。

インストールが完了するまで進捗状況を示すページが表示され、その後［結果］ページが表示されます。

e. （オプション）［インストール レポートの印刷、電子メール送信、または保存］をクリックし、情報を確認してページを閉じます。

［インストール レポート］ページには、変更のサマリ、それらの変更に関する情報、インストールの完全なログの場所が表示されます。

f. ［閉じる］をクリックします。

［インストールの結果］ページが閉じます。

14. サーバ マネージャ ウィンドウを終了します。

SNMP サービスと SMTP サーバのインストール

SNMP サービスと SMTP サーバをインストールします。

簡易ネットワーク管理プロトコル（SNMP）は、CA ADA Watchdog サービスによって必要とされます。 簡易メール転送プロトコル（SMTP）サービスは、送信電子メール メッセージを配信するために使用される IIS コンポーネントです。

次の手順に従ってください:

1. サーバに管理者としてログインします。
2. ［管理ツール］、［サーバ マネージャ］に移動します。

［サーバ マネージャ］ウィンドウが開きます。

3. 左側のコンソール ツリーで［機能］をクリックします。

［サーバ マネージャ］ウィンドウに、サーバにインストールされている機能のリストが表示されます。

4. ［機能の概要］の下の［機能の追加］をクリックします。

   ［機能の選択］ページに、［機能の追加］ウィザードで利用可能なインストール済み機能のリストが表示されます。

5. 機能リストで Desktop SNMP Service を選択します。

   確認メッセージが表示されます。

6. ［必要な機能を追加］をクリックします。

   サービスのインストールの確認ページで、インストールされる機能を確認します。 このページには、インストールに関する重要なメッセージも表示されます。

7. ［インストール］をクリックします。

   ［インストールの進行状況］ページには、インストールの進捗状況が示されます。インストールが完了すると、［インストールの結果］ページに新しい機能が表示され、サーバを再起動する必要があることが示されます。

8. ［閉じる］をクリックします。

   今すぐサーバを再起動するかどうかを尋ねるメッセージが表示されます。

9. ［いいえ］をクリックします。

10. SMTP サーバに対して手順 5 から 8 を繰り返します。

    今すぐサーバを再起動するかどうかを尋ねるメッセージが表示されます。

11. ［はい］をクリックします。

    サーバの再起動の後、サーバ マネージャ ウィンドウの［機能］ビューには新しくインストールされた機能が表示されます。

ごみ箱の設定

必要に応じてごみ箱を設定し、削除されたファイルがサーバからすぐに削除されるようにできます。デフォルトの動作では、ごみ箱に削除済みファイルのコピーが保存されるため、より多くの容量を使用します。

以下の手順に従います。

1. CA Network Flow Analysis の管理者権限を持つユーザとしてログインします。
2. デスクトップ上で［ごみ箱］アイコンを右クリックします。
3. メニューから［プロパティ］を選択します。

   ［ごみ箱のプロパティ］ダイアログ ボックスが表示されます。
4. ［全般］タブで［ローカル ディスク（C:）を選択します。
5. オプション［ごみ箱にファイルを移動しないで、削除と同時にファイルを消去する］を選択します。
6. ［適用］をクリックします。
7. 設定する各追加ドライブに対してこの手順を繰り返します。
8. ［OK］をクリックします。

不要な Windows サービスの無効化

CA ADA で不要となったサービスを無効にすることができます。 不要なサービスを削除するとサーバの保護を強化できますが、これは必須ではありません。 以下のサービスが別の理由で必要である場合は、これらを無効にしないでください。

以下の手順に従います。

1. サーバの管理者権限を持つユーザとしてログインします。
2. ［サービス］ウィンドウを開き、［スタート］、［管理ツール］、［サービス］の順にクリックします。

   ［サービス］ウィンドウが表示されます。
3. 以下のサービスを右クリックし、［手動］または［無効］を選択します。

   ［停止］は選択しないでください。選択すると、サーバが再起動されるたびにサービスが再度開始されます。

無効にできる Windows サーバ サービス

- Application Layer Gateway Service
- Application Management
- Certificate Propagation
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- DNS Client
- Function Discovery Resource Publication
- Human Interface Device Access
- IP Helper
- Link-Layer Topology Discovery Manager
- Microsoft Iscsi Initiator Service
- Multimedia Class Scheduler
- Netlogon
- Network List Service
- Network Location Awareness
- Portable Device Enumerator Service
- Print Spooler
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Registry
- Resultant Set of Policy Provider
- Secondary Logon
- Smart Card
- Smart Card Removal Policy

無効にできる Windows サーバ サービス

- Special Administration Console Helper
- SSDP Discovery
- Tablet PC Input Service
- Telephony
- Volume Shadow Copy
- Windows Audio
- Windows Audio Endpoint Builder
- Windows CardSpace
- Windows Color System
- WinHTTP Web Proxy Auto-Discovery Service
- WMI Performance Adapter

TrapConfiguration キーの作成

SNMP サービスが誤検出されたイベントをログ記録するのを防ぐため、空の TrapConfiguration キーを Windows レジストリに作成することをお勧めします。

以下の手順に従います。

1. サーバの管理者権限を持つユーザとしてログインします。
2. コマンド プロンプト ウィンドウを開きます。
3. 以下のコマンドを実行します。

   ```
   reg add
   HKLM¥SYSTEM¥CurrentControlSet¥Services¥SNMP¥Parameters¥TrapConf
   iguration
   ```

   コマンドが正常に実行された場合、「操作は正常に完了しました」という値が戻されます。

   空の TrapConfiguration レジストリ キーが次の場所に作成されます：HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥SNMP¥Parameters。

第 3 章: ハードウェアの設定

ハードウェアを設定するには、以下のタイプのケーブルが必要です。

電源ケーブル

サーバを 2 つの電源に接続します。できれば UPS デバイスも 2 つに分けます。バックアップ電源用に 2 本目のケーブルも必要です。

管理 NIC ケーブル

銅線 1Gb ケーブル

スイッチに差し込まれた場合、管理 NIC は CA ADA サーバへのネットワーク アクセスを提供します。

また管理 NIC は、Cisco WAE と NAM デバイス、および CA GigaStor からパフォーマンス データを受信します。

監視 NIC ケーブル

銅線 1Gb ケーブル

スイッチ上のミラーリングされたポートからネットワーク トラフィックを収集します。

このセクションには、以下のトピックが含まれています。

管理コンソール サーバの設定

ここでは、管理コンソールをホストするサーバを設定する手順について説明します。

以下の手順に従います。

1. 電源ケーブルの一端をサーバのコンセントに接続します。
2. 電源ケーブルのもう一端を 2 つの別々の電源と接続します。
3. 管理ケーブルの一端をサーバ上の NIC と接続します。

4. 管理コンソールへのネットワーク アクセスを可能にするスイッチに、管理ケーブルのもう一端を接続します。
5. サーバの電源を入れます。
6. CA からのアプライアンスを設定する場合、以下の認証情報でアプライアンスにログインします。
   - ユーザ名： netqos
   - パスワード： Changepassword1

   デフォルトのパスワードはすぐに変更することをお勧めします。
7. NIC 用のネットワーク接続 (P. 25)を設定します。
8. NIC にIP アドレス (P. 26)を割り当てます。

Standard Monitor サーバの設定

Standard Monitor をホストするサーバを設定する手順について説明します。

以下の手順に従います。

1. 電源ケーブルの一端をサーバのコンセントに接続します。
2. 電源ケーブルのもう一端を 2 つの別々の電源と接続します。
3. モニタと管理ケーブルの一端をサーバ上の NIC と接続します。
4. ミラーリングされたスイッチ ポートに監視ケーブルのもう一端を接続します。
5. 管理コンソール サーバに管理ケーブルのもう一端を接続します。
6. サーバの電源を入れます。
7. CA からのアプライアンスを設定する場合、以下の認証情報でアプライアンスにログインします。
   - ユーザ名： netqos
   - パスワード： Changepassword1

   デフォルトのパスワードはすぐに変更することをお勧めします。
8. NIC 用のネットワーク接続 (P. 25)を設定します。
9. NIC にIP アドレス (P. 26)を割り当てます。

NIC 用ネットワーク接続の設定

管理コンソールまたは CA Standard Monitor をインストール予定の各サーバで、ネットワーク インターフェース カード（NIC）を設定します。

- CA Standard Monitor 用に、管理 NIC と監視 NIC のネットワーク接続をセットアップします。 トラフィックを受信するために最大 2 つまでの監視 NIC を設定できることに注意してください。
- 管理コンソール用に、管理 NIC の優先度を設定します。

以下の手順に従います。

1. ［コントロール パネル］で、［ネットワーク接続］をクリックします。

   ［ネットワーク接続］ウィンドウが表示されます。

2. LAN または高速インターネット接続の名前を確認します。 必要であれば、以下のリストに示すような、インターフェースに対応させるデフォルト名を変更します。

   銅線 Ethernet アダプタ

   デフォルト名： Local Area Connection 2

   割り当てる新しい名前： Management

   銅線 Ethernet アダプタ

   デフォルト名： Local Area Connection 3

   割り当てる新しい名前： Monitor

   Gigabit Fiber ポート

   デフォルト名： Local Area Connection

   割り当てる新しい名前： Fiber Monitor

   ヒント： デバイスの背面からケーブルを抜いたときに、［ネットワーク接続］ダイアログ ボックスでどのインターフェース ステータスが「切断」に変わるかどうかを確認することにより、デバイスを特定できます。

3. 管理コンソールまたは CA Standard Monitor 上の未使用の監視 NIC を無効にします。

   a. NIC を右クリックします。

   b. ［無効］を選択します。

4. ［詳細設定］、［詳細設定］、［アダプタとバインド］をクリックします。
5. 上向き矢印を使用して、管理 NIC を［接続］ペイン内の先頭に移動させます。この操作は優先度を設定し、CA ADA が正しく動作できるようにします。
6. すべての NIC について、以下のインターネット プロトコル（TCP/IP）チェック ボックスをオフにします。
   - Microsoft ネットワーク用に共有するファイルとプリンタ
   - Microsoft ネットワーク用のクライアント
7. ［OK］をクリックします。

管理 NIC への IP アドレスの割り当て

管理コンソールまたは CA Standard Monitor 上の管理 NIC に、静的 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを割り当てます。

注: 管理 NIC は、ネットワークにデータを転送する唯一の NIC です。 監視 NIC などの他の NIC に割り当てられた IP アドレスは、接続されるネットワークで有効である必要がなく、デフォルトのゲートウェイ割り当ても不要です。

以下の手順に従います。

1. ［コントロール パネル］を開いて、［ネットワーク接続］を選択します。
2. 管理ネットワーク接続を右クリックし、［プロパティ］を選択します。
3. ［全般］タブで［プロパティ］をクリックします。
4. インターネットプロトコル Version 4 （TCP/IPv4）*以外の*すべてのネットワーク コンポーネントのチェック ボックスをオフにします。
5. インターネットプロトコル Version 4 （TCP/IPv4）を選択し、［プロパティ］をクリックします。
6. ［次の IP アドレスを使用する］を選択し、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。

7. ［OK］をクリックします。
8. 以下の推奨値を使用して、監視 NIC に対して手順 5 から 7 を繰り返します。

   監視 NIC

   IP アドレス： 1.1.0.2

   サブネット マスク： 255.0.0.0

   ファイバ監視 NIC

   IP アドレス： 1.1.0.1

   サブネット マスク： 255.0.0.0

第 4 章: ソフトウェアのインストール

このセクションには、以下のトピックが含まれています。

前提条件

CA ADA ソフトウェアをインストールする前に、以下のタスクを実行します。

- 最新の CA ADA セットアップ ファイル（ADASetup10.1.xxx.exe）を CA サポートからダウンロードします。
- CA からの CA ADA アプライアンスがある場合、現在インストールされているソフトウェア バージョンを確認することをお勧めします。必要な場合は最新のバージョンにアップグレードします。 ソフトウェア バージョンを確認するには、CA ADA コンソールにログインし、［バージョン情報］リンクをクリックします。CA ADA のアップグレードに関する詳細については、「*アップグレード ガイド*」を参照してください。
- CA ADA は、NetQoS Performance Center 6.1 と同じコンピュータ上にインストールしないでください。 CA ADA と共に提供される CA Single Sign-On アプリケーションは、CA NetQoS Performance Center と共に提供される CA Single Sign-On とは互換性がありません。 必要に応じて、CA ADA を別のコンピュータにインストールしてください。
- 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、セットアップ ファイルを抽出またはコピーします。
- 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。

管理コンソールのインストール

ここでは、物理サーバまたは仮想マシンに管理コンソールをインストールするための手順について説明します。CA Standard Monitor もインストールされますが、監視デバイスとして自動的に追加されません。 インストール後に、レスポンス時間データのソースとして手動で監視デバイスを追加 (P. 35)します。

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。

以下の手順に従います。

1. サーバに管理者としてログインします。
2. 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。
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. 使用許諾契約を確認して同意し、［次へ］をクリックします。

   ［インストール設定の選択］ダイアログ ボックスが表示されます。
5. ［分散マネージャ］を選択し、［次へ］をクリックします。

   ［情報］ダイアログ ボックスでは、CA ADA を CA SOLVE:Access または CA Performance Center のデータ ソースとして登録するよう促します。
6. ［続行］をクリックします。

   ［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ます。
7. （*オプション*）別の場所を選択する場合は、［選択］をクリックします。 デフォルトの場所は C:¥CA です。
8. ［次へ］をクリックします。

   ［インストール前のサマリ］ダイアログ ボックスに、インストール パラメータがまとめて表示されます。

9. ［インストール］をクリックします。

   インストール プロセスが開始されます。インストールの進捗状況が表示されます。 インストールが完了すると、［インストール完了］ウィンドウが開きます。

10. ［はい］を選択してシステムを再起動します。

11. ［完了］をクリックします。

    サーバを再起動した後、CA Standard Monitor などの監視デバイスを管理コンソールに追加できます。

詳細:

インストール後の設定 (P. 35)

Standard Monitor のインストール

以下の手順を使用して、監視デバイスをインストールします。

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。

以下の手順に従います。

1. サーバに管理者としてログインします。
2. 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。

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. 使用許諾契約を確認して同意し、［次へ］をクリックします。

   ［インストール設定の選択］ダイアログ ボックスが表示されます。

5. Single-Port Monitor を選択し、［次へ］をクリックします。

   ［情報］ダイアログ ボックスでは、CA ADA を CA SOLVE:Access または CA Performance Center のデータ ソースとして登録するよう促します。

6. ［続行］をクリックします。

   ［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ます。

7. （*オプション*）別の場所を選択する場合は、［選択］をクリックします。 デフォルトの場所は C:¥CA です。
8. ［次へ］をクリックします。

   ［インストール前のサマリ］ダイアログ ボックスに、インストール パラメータがまとめて表示されます。
9. ［インストール］をクリックします。

   インストール プロセスが開始されます。インストールの進捗状況が表示されます。 インストールが完了すると、［インストール完了］ウィンドウが開きます。
10. ［はい］を選択してシステムを再起動します。
11. ［完了］をクリックします。

    サーバを再起動したら、インストール後の設定 (P. 35)を行うことができます。

Virtual Monitor のインストール

以下の手順を使用して、CA Virtual Monitor をインストールします。

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。

以下の手順に従います。

1. 仮想マシンに管理者としてログインします。
2. 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。
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. 使用許諾契約を確認して同意し、［次へ］をクリックします。

   ［インストール設定の選択］ダイアログ ボックスが表示されます。
5. Virtual Monitor を選択し、［次へ］をクリックします。

   ［情報］ダイアログ ボックスでは、CA ADA を CA SOLVE:Access または CA Performance Center のデータ ソースとして登録するよう促します。

6. ［続行］をクリックします。

   ［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ます。

7. （*オプション*）別の場所を選択する場合は、［選択］をクリックします。 デフォルトの場所は D:¥CA です。

8. ［次へ］をクリックします。

   ［インストール前のサマリ］ダイアログ ボックスに、インストール パラメータがまとめて表示されます。

9. ［インストール］をクリックします。

   インストール プロセスが開始されます。インストールの進捗状況が表示されます。 インストールが完了すると、［インストール完了］ウィンドウが開きます。

10. ［はい］を選択してシステムを再起動します。

11. ［完了］をクリックします。

    仮想マシンを再起動したら、インストール後の設定 (P. 35)を行うことができます。

第 5 章: インストール後の設定

このセクションには、以下のトピックが含まれています。

CA Application Delivery Analysis の更新のインストール

CA サポートから入手可能なすべての更新をインストールします。

アンチウイルス スキャンからディレクトリを除外

アンチウイルス ソフトウェアをインストールする必要がある場合は、以下のディレクトリをウイルス スキャンから除外します。

- C:¥Windows¥Temp
- CA ADA のインストール ディレクトリおよびそのサブディレクトリ。デフォルトでは、CA ADA は C:¥CA にインストールされます。

システム時刻とタイム ゾーンの同期

次の手順に従ってください:

1. サーバに管理者権限を持つユーザとしてログインします。
2. タスクバーの右端にある日付または時間を右クリックし、［日付と時刻の調整］を選択します。

   ［日付と時刻］ダイアログ ボックスが表示されます。
3. ［インターネット時刻］タブをクリックします。
4. ［設定の変更］をクリックします。

   ［インターネット時刻設定］ダイアログ ボックスが表示されます。

5. ［インターネット時刻サーバーと同期する］チェックボックスを選択します。
6. 同期する NTP タイム サーバを選択します。 デフォルトの選択は time.windows.com です。
7. ［今すぐ更新］をクリックします。

   システム時刻が選択されたサーバと同期されます。
8. ［インターネット時刻設定］ダイアログ ボックスで［OK］をクリックします。
9. ［日付と時刻］ダイアログ ボックスで［OK］をクリックします。

注: CA Standard Monitor が別のタイム ゾーンにある場合は、各監視デバイスをそのローカル タイム ゾーンに設定します。 NTP サーバを使用して、時刻が正確であることを確認できます。 時間はグリニッジ標準時（GMT）に変換されます。

管理コンソールから設定タスクを実行

管理コンソールを使用して以下のタスクを実行します。

- CA Standard Monitor を監視デバイスとして追加します。
- 監視するサーバ サブネットおよびクライアント ネットワークを定義します。

注: 詳細については、CA Application Delivery Analysis オンライン ヘルプまたは「CA Application Delivery Analysis 管理者ガイド」を参照してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. 監視デバイスを追加します。
   a. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
   b. ［表示項目］メニューの下の［ADA 監視の追加］をクリックします。

      ［Standard Monitor のプロパティ］が表示されます。
   c. ［Standard Monitor のプロパティ］のフィールドの入力が完了したら、［OK］をクリックします。

      「ネットワーク インターフェース カードの設定 (P. 25)」で設定した管理および監視用 NIC の IP アドレスを提示します。 詳細については、［ヘルプ］をクリックしてください。
3. 対象のサーバ サブネットを定義します。
   a. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
   b. ［サーバ サブネット リスト］までスクロールし、［サーバ サブネットの追加］をクリックします。
   c. ［サーバ サブネットの追加］が表示されます。
   d. ［サーバ サブネット］内のフィールドに入力し、［OK］をクリックします。

      サーバ サブネット プロパティの設定の詳細については、［ヘルプ］を参照してください。
4. 対象のクライアント ネットワークを定義します。

a. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

b. ［表示項目］メニュー下の［ネットワークの追加］をクリックします。

c. ［ネットワークのプロパティ］が表示されます。

d. ［ネットワークのプロパティ］の各フィールドに入力してから、［OK］をクリックします。

e. ネットワーク プロパティの詳細については、［ヘルプ］をクリックしてください。

5. 監視デバイスを同期するためのリンクをクリックし、現在のサーバ サブネットおよびクライアント ネットワークの定義に基づいてデータ収集を開始します。

付録 A: ベストプラクティスの展開

このセクションでは、関連するすべてのトラフィックを監視するのに役立つサーバ設定と配置について助言します。

サーバ配置の決定方法

CA ADA サーバは、監視するトラフィックを処理する各ネットワーク スイッチ上で SPAN またはミラー ポートとの接続を必要とします。接続は通常、アクセス層で実行されます。 接続する監視デバイスのすぐ近くに CA ADA 管理コンソールをインストールします。

サーバは、できるだけ多くの関連ネットワーク トラフィックを観測できる必要があります。 以下の事柄を検討します。

- どのアプリケーションを監視しますか。
- どのサーバがこれらのアプリケーションをホストしますか。
- これらのサーバはどのスイッチに接続されていますか。
- ユーザはどのサブネットから監視対象アプリケーションにアクセスしますか。

一方向ストリームの監視方法

一方向ストリームはインライン ファイバ タップで観測できます。 タップの中には、入口が 1 つで出口が 2 つのネットワーク カードで設計されているものがあります。一方は送信用、もう一方は受信用です。 この場合、CA ADA がトラフィックを正確に測定するには、CA ADA Multi-Port Monitor などのマルチ NIC 監視が必要です。

非対称のルーティング環境で、1 つのコア スイッチはデータをデータ センターにルーティングします。 別のコア スイッチは、データ センターを出るトラフィックをルーティングします。 サーバ ファームの送受信トラフィックをキャプチャするには、同じ監視に対して 2 つのポート ミラーが必要です。

CA Standard Monitor は一方向または非対称のトラフィックを監視できません。

スイッチ ポートのミラーリング方法

ネットワーク スイッチでは、*ポート ミラーリング*機能により、ネットワーク パケットのコピーを分析のためにあるポートから別のスイッチまたはポートに送信します。

ポートのミラーリングは、トラフィックを CA ADA 監視デバイスにミラーリングする安全で効果的な方法です。

一部のスイッチでは、これらのシナリオで必要となる多様な TCP パケット ミラーリング機能が提供されません。

トラフィックを最適にミラーリングできない場合は、ファイバ タップなどの代替手段を使用してください。

注: Cisco スイッチ上のポート ミラーリング機能は、Switched Port Analyzer（SPAN）と呼ばれます。

トラフィックが監視対象のサーバとの間で送信されているスイッチ ポートを、CA ADA サーバ上の監視 NIC、または CA ADA 監視デバイスが接続されているポートにミラーリングします。 ミラー ポートが正しく設定されている場合、CA ADA は、デスクトップまたはサーバ エージェントを使用することなく、クライアントとサーバ間のアプリケーション トラフィックのフローを監視します。

詳細については、「*Data Acquisition Best Practices Guide*」を参照してください。