

CA Application Performance Management

CA Infrastructure Management 統合ガイド

リリース 9.5



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、複製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せん。

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 © 2013 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

このドキュメントは、以下の CA Technologies 製品および機能に関するものです。

- CA Application Performance Management (CA APM)
- CA Application Performance Management ChangeDetector (CA APM ChangeDetector)
- CA Application Performance Management ErrorDetector (CA APM ErrorDetector)
- CA Application Performance Management for CA Database Performance (CA APM for CA Database Performance)
- CA Application Performance Management for CA SiteMinder® (CA APM for CA SiteMinder®)
- CA Application Performance Management for CA SiteMinder® Application Server Agents (CA APM for CA SiteMinder® ASA)
- CA Application Performance Management for IBM CICS Transaction Gateway (CA APM for IBM CICS Transaction Gateway)
- CA Application Performance Management for IBM WebSphere Application Server (CA APM for IBM WebSphere Application Server)
- CA Application Performance Management for IBM WebSphere Distributed Environments (CA APM for IBM WebSphere Distributed Environments)
- CA Application Performance Management for IBM WebSphere MQ (CA APM for IBM WebSphere MQ)
- CA Application Performance Management for IBM WebSphere Portal (CA APM for IBM WebSphere Portal)
- CA Application Performance Management for IBM WebSphere Process Server (CA APM for IBM WebSphere Process Server)
- CA Application Performance Management for IBM z/OS® (CA APM for IBM z/OS®)
- CA Application Performance Management for Microsoft SharePoint (CA APM for Microsoft SharePoint)
- CA Application Performance Management for Oracle Databases (CA APM for Oracle Databases)

- CA Application Performance Management for Oracle Service Bus (CA APM for Oracle Service Bus)
- CA Application Performance Management for Oracle WebLogic Portal (CA APM for Oracle WebLogic Portal)
- CA Application Performance Management for Oracle WebLogic Server (CA APM for Oracle WebLogic Server)
- CA Application Performance Management for SOA (CA APM for SOA)
- CA Application Performance Management for TIBCO BusinessWorks (CA APM for TIBCO BusinessWorks)
- CA Application Performance Management for TIBCO Enterprise Message Service (CA APM for TIBCO Enterprise Message Service)
- CA Application Performance Management for Web Servers (CA APM for Web Servers)
- CA Application Performance Management for webMethods Broker (CA APM for webMethods Broker)
- CA Application Performance Management for webMethods Integration Server (CA APM for webMethods Integration Server)
- CA Application Performance Management Integration for CA CMDB (CA APM Integration for CA CMDB)
- CA Application Performance Management Integration for CA NSM (CA APM Integration for CA NSM)
- CA Application Performance Management LeakHunter (CA APM LeakHunter)
- CA Application Performance Management Transaction Generator (CA APM TG)
- CA Cross-Enterprise Application Performance Management
- CA Customer Experience Manager (CA CEM)
- CA Embedded Entitlements Manager (CA EEM)
- CA eHealth® Performance Manager (CA eHealth)
- CA Insight™ Database Performance Monitor for DB2 for z/OS®
- CA Introscope®
- CA SiteMinder®
- CA Spectrum® Infrastructure Manager (CA Spectrum)

- CA SYSVIEW® Performance Management (CA SYSVIEW)

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	11
統合エンド ユーザ エクスペリエンス 監視	12
ソリューション アーキテクチャ	12
デプロイ時の考慮事項	15
ポートの考慮事項	17
Single Sign-On	18
CA SiteMinder サポート	19
詳細	19
第 2 章: コンポーネントの概要	23
Multi-Port Monitor	23
統合アプライアンス内のデータ フロー	25
Application Delivery Analysis マネージャ	25
NetQoS Performance Center/CA Performance Center	26
TIM	27
Enterprise Manager	28
APM データベース	29
CEM コンソール	30
Workstation	30
WebView	31
Java Agent	32
.NET Agent	32
第 3 章: 統合シナリオ	35
CA APM を Multi-Port Monitor に接続する方法	35
前提条件	38
Multi-Port Monitor 上の TIM	39
スタンドアロン TIM オプション	40
Multi-Port Monitor に TIM をインストールする	41
ハードウェア フィルタの構成	42
論理ポートに TIM 監視を構成する	46
マルチプロセス モードでの TIM	48
TIM のマルチプロセス モードの設定	50
TIM を Enterprise Manager に関連付ける	52

(オプション) Web サーバフィルタの構成.....	54
監視の同期.....	55
接続の確認.....	56
CA APM を Application Delivery Analysis に接続する方法.....	56
前提条件.....	57
インストーラ プログラムの実行.....	58
ADA-APM サービスの開始.....	62
時間の同期.....	62
接続の確認.....	63
CA APM を CA Performance Center に接続する方法.....	64
前提条件.....	66
インストーラ プログラムの実行.....	67
APM-CAPC サービスの開始.....	68
APM WebView でのアラートの設定.....	69
NetQoS Performance Center への APM ビューのインポート.....	71
APM をデータ ソースとして登録.....	71
[アプリケーションヘルス] への APM メニュー項目の追加.....	73
HTTPS サポートの有効化 (オプション).....	74
接続の確認.....	75
CA APM を NetQoS Performance Center に接続する方法.....	76
前提条件.....	78
インストーラ プログラムの実行.....	79
APM-CAPC サービスの開始.....	80
APM WebView でのアラートの設定.....	81
NetQoS Performance Center データベースの更新.....	82
CA APM をデータ ソースとして登録.....	83
HTTPS サポートの有効化 (オプション).....	85
接続の確認.....	86

第 4 章: シナリオの問題切り分け 87

CEM コンソールからアプリケーションおよびインフラストラクチャの問題を切り分ける方法.....	87
問題切り分けオプションの決定.....	88
Multi-Port Monitor からの問題切り分けの続行.....	93
APM WebView からの問題切り分けの続行.....	94
APM WebView からアプリケーションおよびインフラストラクチャの問題を切り分ける方法.....	94
問題切り分けオプションの決定.....	95
APM WebView からの問題切り分けの続行.....	103
NPC/CAPC からの問題切り分けの続行.....	104
ネットワーク データの遅延.....	104

ヒント データ	105
ADA がネットワークおよびサーバの稼働状況を計算する方法	106
NPC からアプリケーションの問題を切り分ける方法.....	107
問題切り分けオプションの決定.....	108
APM WebView からの問題切り分けの続行.....	121
NPC/CAPC からの問題切り分けの続行	121

付録 A: トラブルシューティング 123

CA APM アプリケーションデータが NPC 上で利用できない.....	123
CA APM アプリケーションデータが CAPC 上で利用できない.....	124
TIM の動作停止.....	125
インフラストラクチャ データが CEM コンソールで利用できない	128
Workstation 上の [詳細情報] ボタンが機能しない	128

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

[統合エンドユーザエクスペリエンス監視](#) (P. 12)

[ソリューションアーキテクチャ](#) (P. 12)

[デプロイ時の考慮事項](#) (P. 15)

[ポートの考慮事項](#) (P. 17)

[Single Sign-On](#) (P. 18)

[CA SiteMinder サポート](#) (P. 19)

[詳細](#) (P. 19)

統合エンド ユーザ エクスペリエンス監視

統合エンド ユーザ エクスペリエンス監視は、CA APM と CA Infrastructure Management 間の統合です。この統合により、エンドユーザのアプリケーション使用状況に関連するアプリケーション レベルのデータが可視化されます。統合のために選択したコンポーネントにより、さまざまなコンソールおよびユーザ インターフェイスで使用可能な情報が決まります。

統合オプションは以下のとおりです。

CA APM と Multi-Port Monitor

この統合では、CEM コンソールで高度なネットワーク パフォーマンス情報を表示できます。詳細については、「[CA APM を Multi-Port Monitor に接続する方法 \(P. 35\)](#)」を参照してください。

CA APM と NetQoS Performance Center/CA Performance Center

この統合では、NetQoS Performance Center で CA APM アプリケーションデータを表示できます。詳細については、「[CA APM を NetQoS Performance Center に接続する方法 \(P. 76\)](#)」または「[CA APM を CA Performance Center に接続する方法 \(P. 64\)](#)」を参照してください。

CA APM と CA Application Delivery Analysis

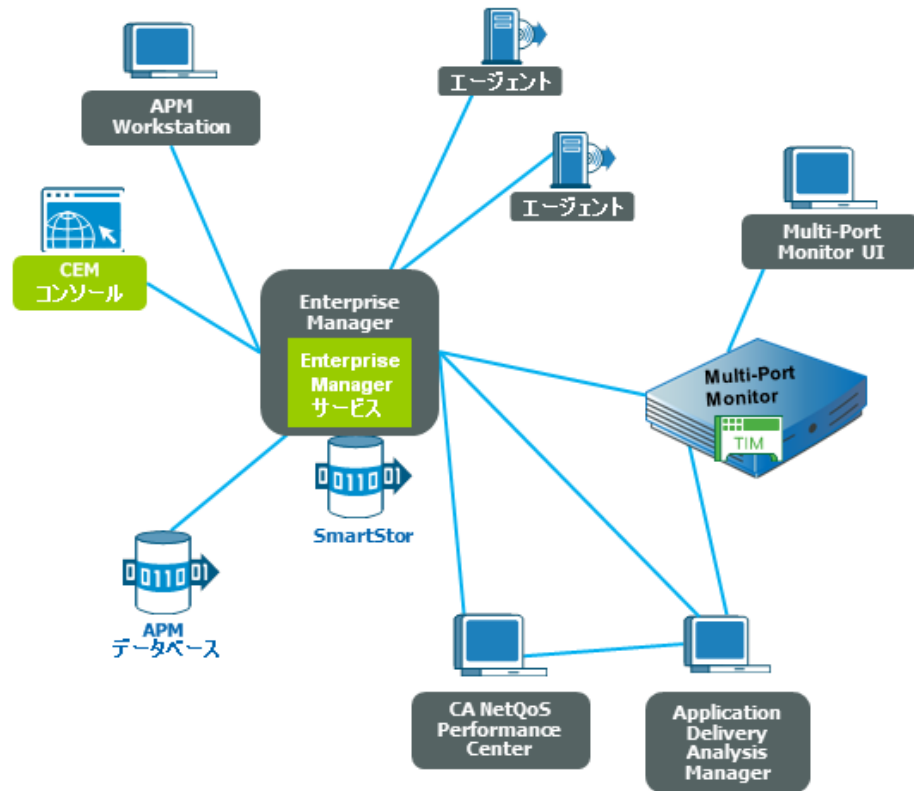
この統合では、APM WebView でインフラストラクチャ データを表示できます。詳細については、「[CA APM を CA Application Delivery Analysis に接続する方法 \(P. 56\)](#)」を参照してください。

ソリューション アーキテクチャ

統合エンド ユーザ エクスペリエンス監視ソリューションには、ネットワークのサイズおよび複雑さに応じて利用できる、多くの展開オプションが用意されています。このセクションでは、考えられる 2 つのシナリオの概要について説明します。

単一の Multi-Port Monitor で十分な小規模な環境では、展開アーキテクチャは以下の図のようになります。

図1: 単一のマルチポート監視を備えた展開アーキテクチャ。

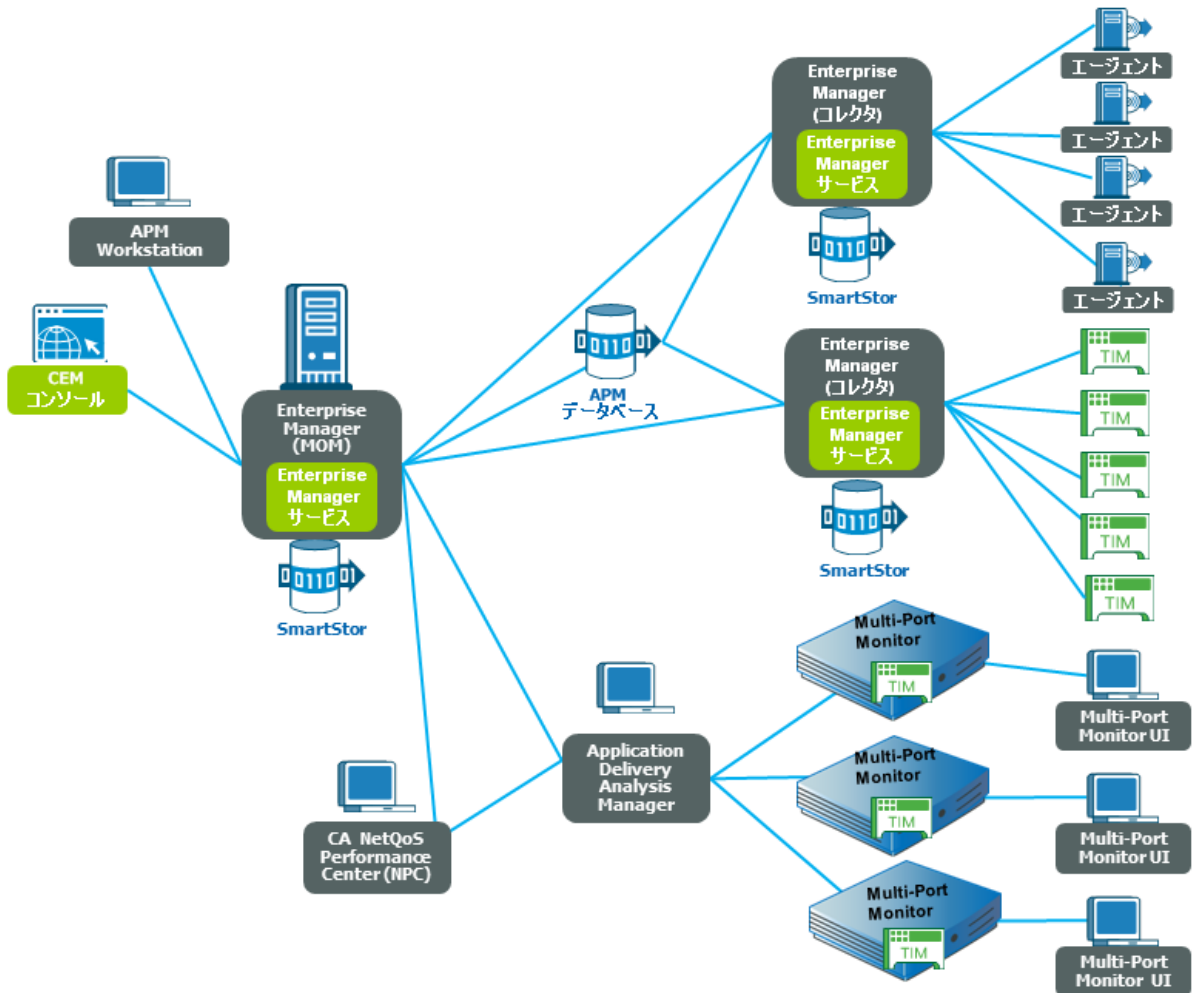


複数の Multi-Port Monitor が必要な、より複雑な環境では、以下の構成に拡張できます。

- 10 の Enterprise Manager コレクタ
- 5 つの Multi-Port Monitor
- 5 つのスタンドアロン TIM
- 3 つの ADA マネージャ、200 の Java エージェントまたは .Net エージェント

さらに複雑な環境では、通常、複数のクラスタ化された CA APM 環境と複数の Multi-Port Monitor が必要になります。クラスタ化された CA APM 環境では、複数の Enterprise Manager (クラスタ化されたときにはコレクタと呼ばれます) がすべてのエージェントメトリックを収集します。すべての Enterprise Manager コレクタおよび MOM (Manager of Managers) の Enterprise Manager からのメトリックをサブスクライブできます。さらに、MOM はクラスタ機能を管理します。たとえば、MOM はデータに対するすべての Workstation 要求を処理し、それらの要求をコレクタから収集します。大規模な環境では、以下のような展開アーキテクチャも考えられます。

図2: クラスタ化された展開アーキテクチャ。



デプロイ時の考慮事項

インストールまたはアップグレードを行う前に、デプロイ方法を注意深く計画してください。以下のリストでは、考慮する必要のあるいくつかの重要な手順の概要について説明します。

- 既存の環境を評価し、必要なコンポーネントをどこに、どのようにデプロイするかを決定します。
- 監視対象の環境の特性を確認します。
- 統合アプライアンスの **SPAN** またはミラー ポート オプションを理解し考慮します。 **Multi-Port Monitor** は、アプリケーショントラフィックをネットワークに転送する主要なスイッチに、**SPAN** またはミラーポート経由で接続する必要があります。

注: 統合アプライアンスに関するミラー ポートの詳細については、「**CA Multi-Port Monitor ユーザガイド**」を参照してください。

- スタンドアロンの **TIM** 用のミラー ポート オプションを理解し考慮します。スタンドアロンの **TIM** はミラーポートまたはネットワークタップに接続する必要があります。この構成により、**TIM** がデータ伝送に影響を与えることなく、ネットワークトラフィックを監視できるようになります。

注: スタンドアロンの **TIM** に関するミラーポートおよびネットワークタップの詳細については、「**CA APM 設定および管理ガイド**」を参照してください。

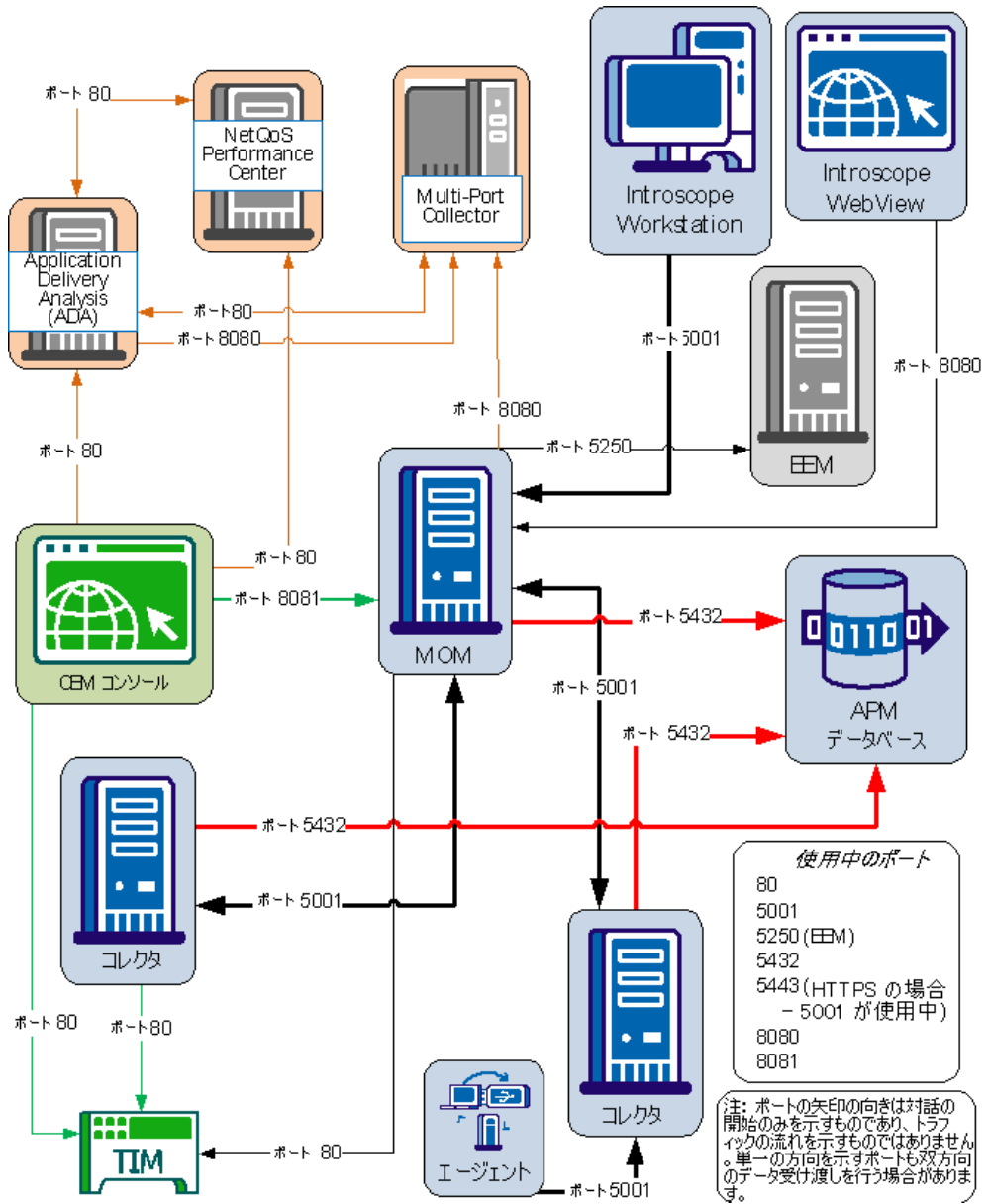
- サーバの **IP** アドレスおよびアプリケーションのポート番号の情報を収集します。エンタープライズネットワークで監視する **IP** アドレスおよびアプリケーションのポートの情報は、スイッチ **SPAN** またはミラーセッションを構成するために必要です。
- コレクタアプライアンスと **ADA** マネージャとの間の通信に影響を及ぼす可能性があるファイアウォールについて考慮します。

注: **Multi-Port Monitor** によって使用されるポートとプロトコルについては、「**CA Multi-Port Monitor ユーザガイド**」を参照してください。

- 以下の CA APM コンポーネントの要件を「CA APM インストールおよびアップグレードガイド」で確認します。
 - APM データベース
 - Enterprise Manager
 - CEM コンソール
 - Workstation
 - スタンドアロン TIM
- .NET エージェントのインストール要件を、「CA APM .NET エージェント実装ガイド」で確認します。
- Java エージェントのインストール要件を、「CA APM Java エージェント実装ガイド」で確認します。

ポートの考慮事項

CA APM および CA Infrastructure Management コンポーネントでは、通信の実行に使用される特定のポートが必要です。以下の図は、これらのコンポーネントとポートを示しています。



注: TIM は Multi-Port Monitor にインストールされると、ポート 80 上の Multi-Port Monitor を介して MOM Enterprise Manager と通信します。ポート 8080 は、Multi-Port Monitor と通信するために MOM Enterprise Manager によって使用されます。

Single Sign-On

シングルサインオンは、NetQoS Performance Center (NPC) /CA Performance Center (CAPC) およびすべてのサポートされるデータ ソースで使用される認証スキームです。ユーザは NPC/CAPC に認証されると、再びサインインする必要なく、コンソールや登録されているデータ ソース間を移動できます。

個別の製品インターフェース間の移動が可能になるので、オペレータはシームレスにドリルダウン操作を行うことができます。たとえば、CEM コンソールから TIM に初めて移動するときには、ADA または NPC/CAPC (ADA が NPC/CAPC にバインドされる場合) で構成されているクレデンシャルを使用して、サインオンする必要があります。最初のサインオンが認証されると、2 つのコンポーネント間で移動するときに再びログオンすることは要求されません。

注: シングルサインオンは、CA APM Workstation または WebView ではサポートされていません。CA APM Workstation/WebView に移動するごとに、そのクレデンシャルを使用してサインオンする必要があります。

NPC/CAPC は分散アーキテクチャを使用します。シングルサインオン Web サイトのインスタンスが、サポートされるデータ ソースまたは NPC/CAPC がインストールされているすべてのサーバに自動的にインストールされます。2 つのデータ ソース製品が同じサーバにインストールされている場合、それらはシングルサインオン Web サイトの同じインスタンスを使用します。分散アーキテクチャによって、個別の CA データ ソース製品へのログインは、これらが実行しているサーバへのログインによって可能になります。

注: シングルサインオンの詳細については、「*CA Performance Center 管理者およびユーザガイド*」を参照してください。

CA SiteMinder サポート

アプリケーション サーバに SiteMinder がインストールされている場合は、トランザクションを監視できるように TIM を設定します。TIM が適切に構成されていないと、それらのアプリケーション サーバから発生したトランザクションがすべて無視されます。

注: SiteMinder を使用してトランザクションを監視できるように TIM を設定する方法の詳細については、「*CA APM 設定および管理ガイド*」を参照してください。

詳細

以下のドキュメントおよびリソースを参照してください。

- *CA APM インストールおよびアップグレードガイド*

展開チームおよびシステム管理者を対象としています。このガイドでは、以下のコンポーネントのインストールおよびアップグレードについて説明します。

- APM データベース
- Enterprise Manager/MOM
- Workstation
- スタンドアロン TIM

- *CA APM 設定および管理ガイド*

システム管理者を対象としています。このガイドでは、以下のコンポーネントの構成および管理情報（アプリケーション トランザクション コンテンツの定義に関する情報を除く）について説明します。

- APM データベース
- Enterprise Manager/MOM
- Workstation
- スタンドアロン TIM

- **CA APM トランザクション定義ガイド**
システム管理者を対象としています。このガイドでは、ビジネスアプリケーション、**BusinessService**、およびトランザクションの各定義の確立および維持に関連する情報について説明します。
- **CA APM Java エージェント実装ガイド**
システム管理者を対象としています。このガイドでは、**Java** エージェントのインストールおよび構成に関する情報について説明します。
- **CA APM .NET Agent ユーザガイド**
システム管理者を対象としています。このガイドでは、**.NET** エージェントのインストールおよび構成に関する情報について説明します。
- **CA APM Workstation ユーザガイド**
システム管理者およびシステムアナリストを対象としています。このガイドでは、**Workstation** を使用して、アプリケーションの問題を切り分ける作業に関する情報について説明します。
- **CA APM WebView シナリオ**
システム管理者およびシステムアナリストを対象とするタスク中心のシナリオです。これらのシナリオでは、**WebView** を使用してアプリケーションの問題を切り分ける作業に関する情報について説明します。
- **CA APM サイジングおよびパフォーマンスガイド**
システム管理者を対象としています。このガイドでは、サイジング要件に基づいたハードウェアサイジングおよびシステムパフォーマンスに関する情報について説明します。
- **CA Multi-Port Monitor インストールガイド**
システム管理者を対象としています。このガイドでは、**Multi-Port Monitor** ソフトウェアのインストールに関する情報について説明します。
- **CA Multi-Port Monitor アップグレードガイド**
システム管理者を対象としています。このガイドでは **Multi-Port Monitor** ソフトウェアのアップグレードに関する情報について説明します。
- **CA Multi-Port Monitor ユーザガイド**
システム管理者およびシステムアナリストを対象としています。このガイドでは、**Multi-Port Monitor** の構成、管理、および使用に関する情報について説明します。

- **CA CA Performance Center インストールガイド**
システム管理者を対象としています。このガイドでは、NPC/CAPC ソフトウェアのインストールに関連する情報について説明します。
- **CA CA Performance Center 管理者およびユーザガイド**
システム管理者およびシステムアナリストを対象としています。このガイドでは、NPC/CAPC の管理および使用に関連する情報について説明します。
- **CA Application Delivery Analysis インストールガイド**
システム管理者を対象としています。このガイドでは、CA Application Delivery Analysis ソフトウェアのインストールに関連する情報について説明します。
- **CA Application Delivery Analysis 管理者ガイド**
システム管理者を対象としています。このガイドでは、CA Application Delivery Analysis の構成および管理に関連する情報について説明します。
- **CA Application Delivery Analysis ユーザガイド**
アナリストを対象としています。このガイドでは、CA Application Delivery Analysis ユーザ インターフェースの使用に関連する情報について説明します。

第 2 章: コンポーネントの概要

このセクションには、以下のトピックが含まれています。

[Multi-Port Monitor](#) (P. 23)

[Application Delivery Analysis マネージャ](#) (P. 25)

[NetQoS Performance Center/CA Performance Center](#) (P. 26)

[TIM](#) (P. 27)

[Enterprise Manager](#) (P. 28)

[APM データベース](#) (P. 29)

[CEM コンソール](#) (P. 30)

[Workstation](#) (P. 30)

[WebView](#) (P. 31)

[Java Agent](#) (P. 32)

[.NET Agent](#) (P. 32)

Multi-Port Monitor

Multi-Port Monitor は、以下を搭載するハードウェア アプライアンスです。

- 高パフォーマンスのキャプチャカード
- システムおよびデータベースに使用される 4 ディスクの RAID アレイ
- パケットを格納するために使用される 12 ディスクの RAID アレイ

Multi-Port Monitor は、複数のパケット コレクションを 1 つのアプライアンスにグループ化する高キャパシティ コレクタです。Multi-Port Monitor にはハードウェアとソフトウェアの両方のコンポーネントがあります。ハードウェア コンポーネントは、スイッチで送受信されるトラフィックをキャプチャおよび処理する 16 ディスクのサーバです。ソフトウェア コンポーネントは、メンテナンス タスクの実行、デバイス上のコレクションのステータスのチェック、およびカスタム ビューの作成の機能を提供する管理 Web インターフェースです。

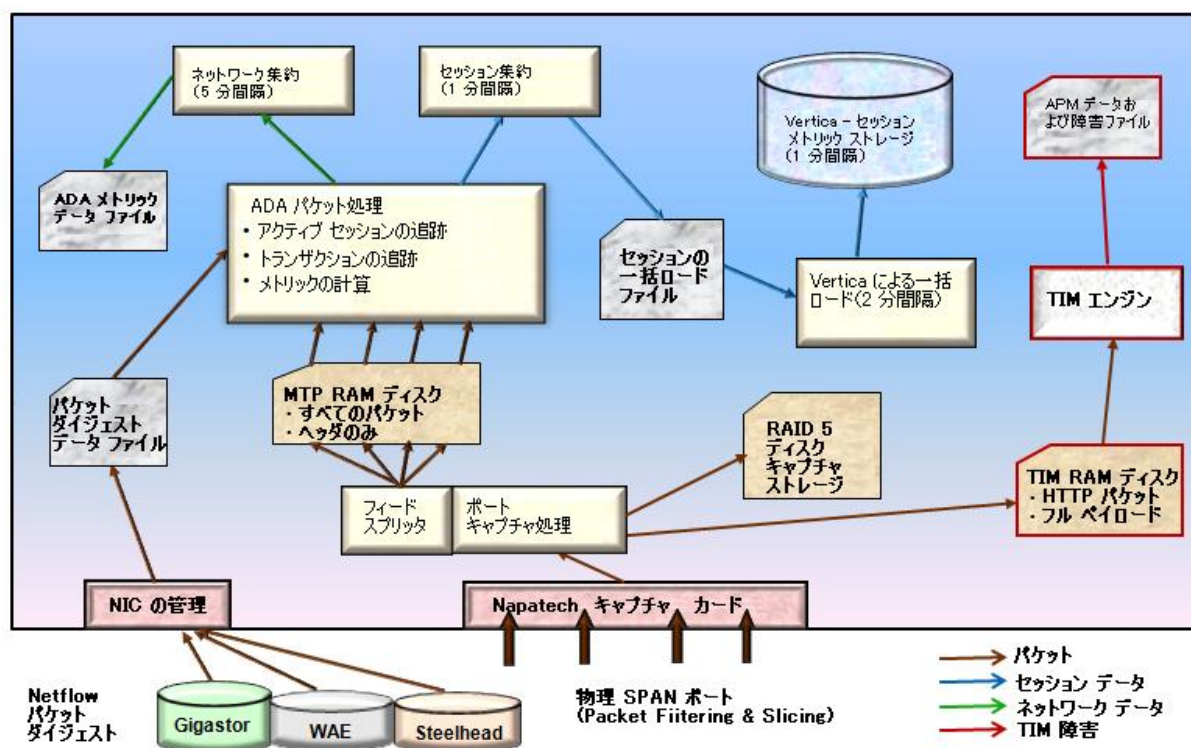
TIM が Multi-Port Monitor 上で実行されているとき、アプライアンスは、TIM が実行されていない Multi-Port Monitor と区別するために、統合アプライアンスと呼ばれることがあります。統合アプライアンスは、ネットワーク、サーバ、およびアプリケーションに対する非侵入性のパッシブ監視を実行するために、ADA および TIM の両方をサポートします。統合アプライアンスは、CA APM および ADA の両方のためのコレクタ アプライアンスとなっています。統合アプライアンスはスイッチに接続し、SPAN トラフィックを収集して、TIM および ADA にその情報を送信します。その後、これらの 2 つのエンジンは、それぞれのコンソールである CEM コンソールおよび ADA マネージャに情報を送信します。

重要: Multi-Port Monitor (TIM がインストールされていない) では、ネットワーク上の異なるポイントから、Multi-Port Monitor 上のそれぞれ独自の論理ポートにスパンすることができます。統合アプライアンスでは、1 つの論理ポートを TIM に対して選択し、WAN からの Web トラフィックをスパンする必要があります。このトラフィックは、ADA と同様に TIM のために処理されます。ほかのスパンのために、理想的にはサーバに最も近いアクセス層スイッチからのほかの論理ポートを使用します。TIM 以外の論理ポートは、ADA のみのために処理されます。

注: アプライアンスの詳細については、「Multi-Port Monitor ユーザガイド」および「Multi-Port Monitor インストールガイド」を参照してください。

統合アプライアンス内のデータフロー

次の図は、Multi-Port Monitor 統合アプライアンス内のパケット、セッションデータ、ネットワークデータ、およびTIM 障害のフローを示します。統合アプライアンスには、2つのRAM ディスクがあることに注意してください。1つ目のディスクは、ADA 処理用に TCP パケットを格納するためだけに使用されます。2つ目のディスクは、TIM 処理用に HTTP データを格納するためだけに使用されます。



Application Delivery Analysis マネージャ

ADA は、物理サーバおよび ADA マネージャと呼ばれる Web ベースのユーザインターフェースを備えたパッシブ パケット コレクタです。ADA は、以下の機能を実行します。

- セッション レベルのネットワーク レベルメトリックに重点を置いて TCP データを監視する
- 収集ファイルを収集デバイスからデータベースにインポートする
- しきい値に対して評価することによって、データを正常、低下、超過に分類し、結果を格納する

- インシデントリストおよび監視数を維持する
- 5分間隔でのパフォーマンスメトリックを計算し、ADAマネージャに送信する
- サーバ、ネットワーク、およびアプリケーションを定義および関連付けて、構成情報を収集デバイスにプッシュする
- 収集および処理されたデータをレポートページおよびビューに表示する

NetQoS Performance Center/CA Performance Center

CA NetQoS Performance Center (NPC) /CA Performance Center (CAPC) は、Web ベースのレポートインターフェースで、CA Performance Center スイートの製品、CA APM、およびサポートされるサードパーティ製品からのパフォーマンスデータを表示します。NPC/CAPC レポートは、パフォーマンスデータおよびデバイスデータをさまざまな形式で表示するので、ネットワーク、アプリケーション、およびデバイスを効率的に管理するのに役立ちます。

CA APM と NPC/CAPC を統合すると、以下のアプリケーション関連の情報が NPC/CAPC で使用可能になります。

- CA APM により監視される Application、BusinessService、および BusinessTransaction のリスト、および選択した時間範囲内のそれらの稼働状況ステータス
- すべてのアプリケーション、ビジネス トランザクション コンポーネント (BTC) のメトリックの傾向、および選択した時間範囲のカスタマエクスペリエンスメトリック (CA APM ユーザーインターフェース上に RTTM として表示されます)
- 選択した BusinessTransaction のインシデント/障害の詳細
- インフラストラクチャに関する詳細分析に役立つ、障害に関連する特定のクライアント サブネットおよびサーバへのリンク

TIM

TIM は、SPAN ポート上の HTTP パケットおよび HTTPS パケットを監視して、ユーザ ログインおよびそれに関連するトランザクションを識別し、障害およびほかの統計を監視およびレポートします。TIM はこれらのすべてのメトリックを計算し、CEM コンソールに送信します。

TIM は、スタンドアロンの TIM および Multi-Port Monitor にインストールされた TIM の 2 つのインスタンスで利用できます。両方のインスタンスとも、SPAN データを監視し、Web ベースのトランザクションのメトリックを収集します。TIM が Multi-Port Monitor にインストールされると、統合アプライアンスはアプリケーションおよびインフラストラクチャデータレベルでアプリケーションの使用状況をレポートします。以下の表は、2 つの TIM の間の主な違いについて、概要を示します。

Multi-Port Monitor 上の TIM	スタンドアロン TIM
64 ビットの CentOS Linux 5.5 上で実行	64 ビットの Red Hat Linux 5.5 上で実行
スループットを向上させるためにマルチプロセス モードで実行	シングルプロセス モードで実行
Multi-Port Monitor キャプチャ層によって書き込まれたファイルからパケットを読み取り	NIC からパケットを直接読み取り
時間はパケットのタイムスタンプから取得。パケットが Multi-Port Monitor に入ると、Napatech カードが (Napatech クロックを使用して) パケットにタイムスタンプを付けます。	時間はシステム時間 (ホストの時計) から取得
Multi-Port Monitor には専用の Napatech カードがあるため、Napatech カードまたはネットワーク カードは不要。	Napatech カードまたはネットワーク カードの購入が必要。
以下のデフォルト ログオン クレデンシャルを使用 ユーザ名 : nqadmin パスワード : nq	以下のデフォルト ログオン クレデンシャルを使用 ユーザー名 : cemadmin パスワード : quality

Enterprise Manager

Enterprise Manager は、複数のコレクタに分散配置されるサービスを実行します。これらのサービスには、TIM コレクション、統計集約、およびデータベースクリーンアップがあります。単一の Enterprise Manager と共に展開されている場合は、スタンドアロン環境と呼ばれます。複数の Enterprise Manager と共に展開されている場合は、クラスタ化された環境と呼ばれ、1 つの Enterprise Manager が MOM になります。Enterprise Manager のクラスタ化された環境では、MOM がほかの Enterprise Manager を管理します。各管理対象 Enterprise Manager はコレクタと呼ばれ、エージェントメトリックを収集して、MOM に中継します。

Enterprise Manager は、エンタープライズシステムのサイズや複雑さに応じてさまざまな方法でデプロイできます。特定の Enterprise Manager のロールは、それらがスタンドアロン環境またはクラスタ化された環境でどのように展開されたかによって異なります。

Enterprise Manager/MOM は CEM コンソールおよびテキストファイルを使用して構成されます。Enterprise Manager/MOM によって処理されたデータの一部は、CEM コンソールを使用して表示できます。また、ほかのデータは CA APM Workstation/WebView を使用して表示できます。

CEM コンソールの詳細については、次を参照してください

[CEM コンソール](#) (P. 30)

CA APM Workstation の詳細については、次を参照してください

[Workstation](#) (P. 30)

APM データベース

APM データベースのプラットフォームとして、PostgreSQL または Oracle のいずれかを選択できます。いくつかの要因はユーザのデータベースプラットフォーム選択に影響を及ぼす場合があります。たとえば、PostgreSQL データベースは簡単にインストールでき、構成および稼働中の管理が最小限で済みます。PostgreSQL データベースも、Enterprise Manager インストーラから自動的にインストールできます。このデータベースでは、データベースのインストール、データの整合性の維持、およびユーザアクセスの制御を行うための個別のデータベース管理者は通常必要ではありません。ただし、PostgreSQL データベースには、いくつかの制限があり、そのため、一部のデプロイシナリオや組織に適さない場合があります。

一般的に、PostgreSQL または Oracle のいずれかをデータベースプラットフォームとして使用するかを判断する場合には、以下の要因を考慮します。これらの要因は、APM データベースを PostgreSQL から Oracle に移行することを計画する場合にも影響を及ぼすことがあります。

- インストール済みのデータベース インスタンスがない場合、Enterprise Manager インストーラを使用して、PostgreSQL を事前構成なしでインストールできます。
- データベース メンテナンスを最小限にし、環境を可能な限り単純な構成で維持する場合、PostgreSQL データベースを使用する方が、Oracle のデータベースを使用するより容易です。
- データベース管理者グループのサポートなしで APM データベースを管理する場合、PostgreSQL データベースに必要とされる管理オーバーヘッド、専門知識およびデータベースに特有のスキルは、より少なく済みます。
- 組織で使用するデータベースが特定のベンダーのデータベースに統一されている場合は、そのデータベースプラットフォームを使用する必要がある場合があります。
- 特定のデータベースプラットフォームに対して既存のデータベース管理者リソースおよび手順がある場合、そのデータベースプラットフォームを使用することで、それらのリソースを最も活用できる可能性があります。
- 既存のデータベース管理者がいない場合、Oracle のインストール、構成、および管理は、PostgreSQL データベースより難しい場合があります。

- 組織のデータベース構成要件が複雑な場合、PostgreSQL で提供されるものより、さらに高度な構成および管理オプションを必要とする可能性があります。
- 大容量の実運用環境を監視する場合、PostgreSQL で提供されるものより、さらに堅牢でかつ拡張性のあるデータベースを必要とする可能性があります。

注: APM データベースの詳細については、「CA APM インストールおよびアップグレードガイド」を参照してください。

CEM コンソール

CEM コンソールは、以下の機能を提供するユーザインターフェースです。

- **BusinessTransaction** を記録および定義する (この情報はトランザクション定義を作成するために使用されます)
- **BusinessTransaction** 関連のレポートを作成および表示する
- 障害データおよびトランザクション定義の表示、サービスへのトランザクションのグループ化、および Enterprise Manager データへの CA APM ユーザアクセスの管理を行う

統合エンドユーザエクスペリエンス監視ソリューション内での CEM コンソールの役割および機能は、以下の例外を除いて、ほとんど同じです。

- ネットワーク稼働状況データが [障害詳細] ページで利用できる
- 障害およびネットワークの情報を使用して、潜在的なパフォーマンス問題を識別し、Multi-Port Monitor に直接移動できる

CEM コンソールは Enterprise Manager インストールの一環としてインストールされます。

Workstation

Workstation では、さまざまな形式でメトリック データを表示できます。承認されたユーザは、管理および設定機能を実行できます。Workstation では、以下のウィンドウにデータが表示されます。

コンソール

Data Viewer が配置されているダッシュボードにデータが表示されません。

Investigator

エージェント、アプリケーション、リソースおよびメトリックのツリービューおよびマップビューを示します。

管理モジュールエディタ

管理モジュールとエレメントのツリービューを表示して、管理モジュールの作成および編集を可能にします。

Dashboard Editor

ドメイン（またはスーパードメイン）に対して書き込みアクセス権を持つユーザは、このエディタで、**Data Viewer** やその他のダッシュボードオブジェクト（インポート画像、図形、線、テキストなど）の作成と編集を行うことができます。

Data Viewer

タイプに基づいたデータの表示。

CA APM と CA Application Delivery Analysis を統合すると、インフラストラクチャ稼働状況データを Workstation の Investigator およびコンソールで使用できます。さらに、[ネットワークステータス情報] ダッシュボードから NetQoS Performance Center に直接アクセスできます。

注: Workstation の詳細については、「CA APM Workstation ユーザガイド」を参照してください。

WebView

APM WebView は Workstation の代替として使用できますが、管理機能がありません。APM WebView を使用して、さまざまな形式でメトリックデータを表示します。APM WebView では、以下のウィンドウにデータが表示されます。

コンソール

Data Viewer が配置されているダッシュボードにデータが表示されます。

Investigator

エージェント、アプリケーション、リソースおよびメトリックのツリービューおよびマップビューを示します。

管理

管理モジュールとエレメントのツリービューを表示して、管理モジュールの作成および編集を可能にします。

CA APM と CA Application Delivery Analysis を統合すると、インフラストラクチャ稼働状況データを Investigator およびコンソールで使用できます。また、[ネットワークステータス情報] ダッシュボードから NPC/CAPC に直接アクセスできます。

Java Agent

Java エージェントは、Java 仮想マシン (JVM) およびアプリケーションサーバ上で実行されるアプリケーションからパフォーマンスデータを収集します。Java エージェントは、周辺のコМПユーティング環境からパフォーマンスおよび可用性データも収集します。Java エージェントはアプリケーションバイトコードのプロブを使用してデータを収集し、Enterprise Manager に送信します。ProbeBuilder ディレクティブ (PBD) ファイルは、プロブがどのデータを監視するか制御します。お使いの環境の監視ニーズに応じて、PBD ファイルを変更できます。標準的な PBD は、お使いのアプリケーションサーバに固有の PBD と同じように、Java エージェントのインストール時にインストールされます。PBD ファイルでトレーサおよびディレクティブを細かく調整すると、環境に合った目的のメトリック情報が配信されます。

Enterprise Manager は、Java エージェントから受信したデータを処理し、分析します。この情報は、CA APM Workstation からアクセスできます。Workstation を使用すると、情報を監視し、受信したデータに基づいてアクションおよびアラートを設定できます。

注: 詳細については、「CA APM Java Agent 実装ガイド」を参照してください。

.NET Agent

.NET エージェントは、コンポーネントレベルの情報を提供する、管理対象エンタープライズ .NET アプリケーション用のアプリケーション管理ソリューションです。.NET エージェントは、Microsoft Common Language Runtime (CLR) 環境で実行されるミッションクリティカルな .NET アプリケーションを監視します。

エージェントは、アプリケーションおよび環境のメトリックを収集し、Enterprise Manager に中継します。Introscope エージェントにメトリックをレポートするアプリケーションは、インストールされたアプリケーションと呼ばれます。システムに .NET エージェントをインストールして構成すると、そのシステムで実行されるアプリケーションは起動時に自動的にインストールされます。

デフォルトでは、システムでアクティブな IIS の ASP.NET アプリケーションのみがインストールされます。IIS の ASP .NET アプリケーションのほかに、スタンドアロンの .NET 実行可能ファイルなど、どのような .NET アプリケーションもインストールできます。また、アプリケーションのサブセットまたは特定のアプリケーションをインストールすることもできます。

インストールのプロセスは ProbeBuilding テクノロジを使用して実行されます。このテクノロジでは、ProbeBuilder ディレクティブ (PBD) ファイルで定義されたトレーサを使用して、実行時にエージェントがアプリケーションと CLR から収集したメトリックが識別されます。その後、.NET エージェントから Enterprise Manager にこのメトリック情報が送信されます。

注: 詳細については、「CA APM .NET Agent 実装ガイド」を参照してください。

第 3 章: 統合シナリオ

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 APM を Multi-Port Monitor に接続する方法 \(P. 35\)](#)

[CA APM を Application Delivery Analysis に接続する方法 \(P. 56\)](#)

[CA APM を CA Performance Center に接続する方法 \(P. 64\)](#)

[CA APM を NetQoS Performance Center に接続する方法 \(P. 76\)](#)

CA APM を Multi-Port Monitor に接続する方法

CA APM を Multi-Port Monitor に接続すると、監視対象のアプリケーションに関連する高度なネットワーク パフォーマンス情報を表示できます。表示している障害について、ネットワーク データが Multi-Port Monitor データベースから CEM コンソールにインポートされ、APM データベースに保存されます。このデータは TIM によって生成された障害と共に CEM の [障害詳細] ページに表示されます。障害およびネットワークの情報を使用して、潜在的なパフォーマンス問題を識別し、Multi-Port Monitor に直接移動できます。

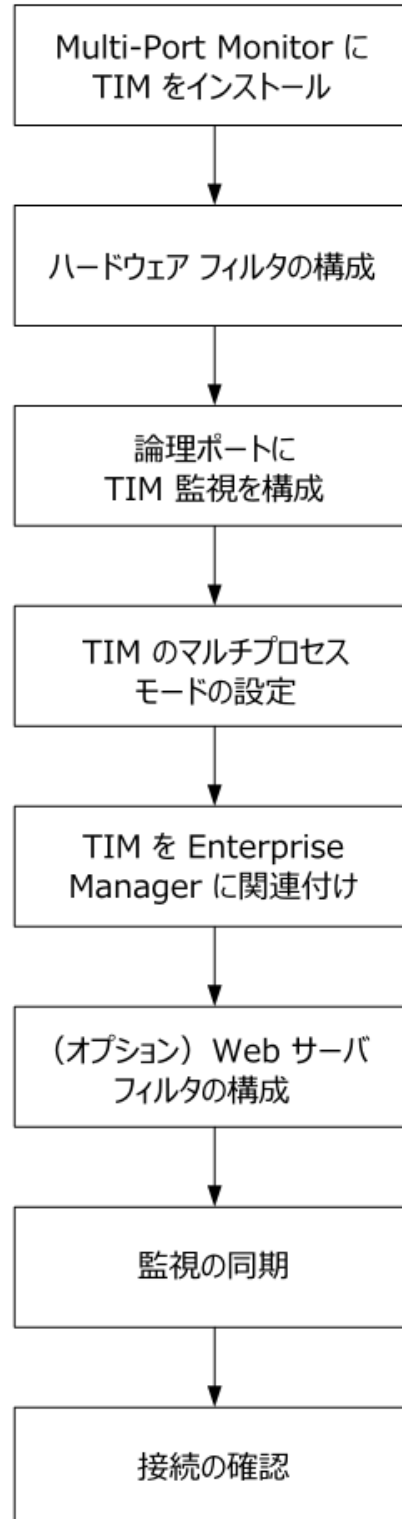
注: 障害が生成されてから、ネットワーク データが CEM の [障害詳細] ページに表示されるまでには、短い遅延 (約 4 ~ 5 分) が発生することがあります。たとえば、障害が 2 分前に生成され、ネットワーク稼働状況情報が CEM の [障害詳細] ページに表示されない場合は、数分待つてから、ビューをリフレッシュします。遅延は、ネットワーク データを Multi-Port Monitor メトリック データベースにロードする処理が定期的に行われることによって発生します。

以下の図に、管理者として CA APM を Multi-Port Monitor に接続する方法を示します。

CA APM を Multi-Port Monitor に 接続する方法



管理者



管理者として、以下の手順を実行します。

1. [Multi-Port Monitor に TIM をインストールします](#) (P. 41)。
2. [ハードウェア フィルタを構成します](#) (P. 42)。
3. [論理ポートに TIM 監視を構成します](#) (P. 46)。
4. [TIM をマルチプロセス モードに設定します](#) (P. 50)。
5. [TIM を Enterprise Manager に関連付けます](#) (P. 52)。
6. [\(オプション\) Web サーバフィルタを構成します](#) (P. 54)。
7. [監視を同期します](#) (P. 55)。
8. [接続を確認します](#) (P. 56)。

前提条件

開始する前に、以下のものがインストールおよび設定されていることを確認します。

- Multi-Port Monitor 2.2
- APM データベース 9.1 以降
- Enterprise Manager 9.1 以降
- CA APM Workstation 9.1 以降
- CA APM WebView (オプション)
- 以下のいずれかが必要です。
 - CA APM .NET エージェント 9.0 以降
 - CA APM Java エージェント 9.0 以降

Multi-Port Monitor 上の TIM

TIM を使用すると、システム管理者は、Multi-Port Monitor アプライアンスを統合アプライアンスとして機能するように構成できます。統合アプライアンスでは、TCP および HTTP のデータを収集し、これらのパケットを TIM および CA Application Delivery Analysis へ渡すことができます（使用している環境にこの製品がある場合）。Multi-Port Monitor 統合アプライアンスは、エンドユーザによるアプリケーション使用状況に関連するアプリケーションおよびインフラストラクチャの両方のパフォーマンスメトリックを検証する機能を提供します。

重要: Multi-Port Monitor（TIM がインストールされていない）では、ネットワーク上の異なるポイントから、Multi-Port Monitor 上のそれぞれ独自の論理ポートにスパンすることができます。統合アプライアンスでは、1 つの論理ポートを TIM に対して選択し、WAN からの Web トラフィックをスパンする必要があります。このトラフィックは、ADA と同様に TIM のために処理されます。ほかのスパンのために、理想的にはサーバに最も近いアクセス層スイッチからのほかの論理ポートを使用します。TIM 以外の論理ポートは、ADA のみのために処理されます。

以下の表は、Multi-Port Monitor にインストールされた TIM とスタンドアロンの TIM の違いを示します。

Multi-Port Monitor 上の TIM	スタンドアロン TIM
64 ビットの CentOS Linux 5.5 上で実行	64 ビットの Red Hat Linux 5.5 上で実行
スループットを向上させるためにマルチプロセスモードで実行	シングルプロセスモードで実行
Multi-Port Monitor キャプチャ層によって書き込まれたファイルからパケットを読み取り	NIC からパケットを直接読み取り
時間はパケットのタイムスタンプから取得。パケットが Multi-Port Monitor に入ると、Napatech カードが（Napatech クロックを使用して）パケットにタイムスタンプを付けます。	時間はシステム時間（ホストの時計）から取得
Multi-Port Monitor には専用の Napatech カードがあるため、Napatech カードまたはネットワークカードは不要。	Napatech カードまたはネットワークカードの購入が必要。

Multi-Port Monitor 上の TIM	スタンドアロン TIM
以下のデフォルト ログオン クレデンシャル を使用 ユーザ名 : nqadmin パスワード : nq	以下のデフォルト ログオン クレデンシャルを 使用 ユーザー名 : cemadmin パスワード : quality

スタンドアロン TIM オプション

既存のスタンドアロン TIM に対しては、以下のオプションが利用できます。

1. スタンドアロン TIM の維持、バージョン 9.1 以降へのアップグレード、各 TIM (Multi-Port Monitor 上の新しい TIM を含む) の再構成を行って、特定のネットワーク トラフィックを監視し、TIM 間のトラフィックを負荷分散します。

注: スタンドアロン TIM は、ほとんどの場合において ADA と統合できません。スタンドアロン TIM および Multi-Port Monitor 上の TIM の両方によって収集されたデータは、CEM コンソールに表示される障害を生成します。ただし、Multi-Port Monitor 上の TIM によって生成された障害からのセッション分析データのみリンクできます。Multi-Port Monitor は、統合を有効にするために、CA APM および ADA の両方用の SPAN データを処理する必要があります。

2. スタンドアロン TIM を削除し、Multi-Port Monitor 上の新しい TIM にそれら用の SPAN を移動します。「CA Multi-Port Monitor ユーザガイド」を参照してください。

TIM 監視および負荷分散を構成する方法の詳細については、次を参照してください

[\(オプション\) Web サーバフィルタの構成 \(P. 54\)](#)

Multi-Port Monitor に TIM をインストールする

TIM を Multi-Port Monitor にインストールして有効にし、TCP と HTTP のデータを収集します。以下の 2 つのインストール ファイルは、Multi-Port Monitor に必要な CentOS 固有のイメージであり、以下の順にインストールする必要があります。

1. サードパーティ イメージ : APMCOSTRDPRTxxxx.img
2. TIM イメージ : APM_COSTIMCMxxxx.img

[CA サポート](#) の CA APM ソフトウェア ダウンロード セクション、または TIM ソフトウェア DVD バンドルからこれら 2 つのファイルにアクセスします。

インストールを開始する前に、Multi-Port Monitor が構成されており、ネットワークに接続されていることを確認します。

次の手順に従ってください:

1. 管理者 クレデンシャルか、デフォルトを変更していない場合は以下のクレデンシャルを使用して、Multi-Port Monitor にログオンします。
ユーザ名 = nqadmin
パスワード = nq
2. [System Setup] タブをクリックします。
3. [Install Software] タブをクリックします。
[Install Software] ページが表示されます。
4. サードパーティ ソフトウェアをインストールします。
 - a. [Browse] をクリックして、TIM インストール ファイルを見つけます。
 - b. APMCOSTRDPRTxxxx.img ファイルを選択します。
 - c. [Upload and Install] をクリックします。
 - d. ライセンス使用条件の内容を確認してから同意します。
続行するには、EULA に同意します。
 - e. ソフトウェア インストール ログが表示されます。エラーが発生する場合は、CA サポートに問い合わせてください。
サードパーティ ソフトウェアがインストールされます。

5. TIM ソフトウェアをインストールします。
 - a. [Install Software] タブをクリックします。
 - b. [Browse] をクリックして、TIM インストール ファイルを見つけます。
 - c. APM_COSTIMCMxxxx.img ファイルを選択します。
 - d. [Upload and Install] をクリックします。
 - e. ライセンス使用条件の内容を確認してから同意します。
続行するには、EULA に同意します。
 - f. ソフトウェア インストール ログが表示されます。エラーが発生する場合は、CA サポートに問い合わせてください。

TIM ソフトウェアがインストールされます。
6. (オプション) [System Setup] タブをクリックしてインストールされたパッケージのリストを表示するか、[Administration] タブをクリックして Multi-Port Monitor 論理ポート上で TIM 監視を有効にします。
7. Multi-Port Monitor を再起動します。

ハードウェア フィルタの構成

CA APM と Multi-Port Monitor の統合の場合、TIM によって監視される Web トラフィックは完全なパケットを含む必要があります。完全なパケット キャプチャを、Multi-Port Monitor Web UI から「HTTP 全体パケット」と呼ばれるデフォルトのフィルタを編集することによって定義します。

事前定義済みフィルタおよびユーザ作成フィルタを作成、有効化、無効化、および変更できます。

次の手順に従ってください:

1. Web インターフェイスで [Administration] - [Logical Ports] をクリックします。

[Logical Ports] ページが表示されます。
2. フィルタする論理ポートの [Edit Filters] 列の [Filters] リンクをクリックします。

[Logical Ports: Hardware Filters] ページが表示されます。

3. フィルタを作成するには、[New] をクリックします。[Logical Ports: New Hardware Filter] ページが表示されます。

a. 以下のフィールドに入力します。

- **Filter Enabled**。名前が指定されている論理ポートにフィルタを適用します。選択した場合、nqcapd プロセスを再起動した後、フィルタが適用されます。
- **Filter Name**。作成または編集するフィルタの名前。フィルタ名は、それが適用される論理ポート用の [Hardware Filters] ページに表示されます。
- **Filter Priority**。優先度は、フィルタ条件が重複する場合に優先するフィルタを決定します。2 つ以上の重複するフィルタの優先度が同じ場合、その優先順位は未定義になります。値は 0 (最高の優先度) から 62 (最低の優先度) の範囲です。デフォルトの優先度は 10 です。

フィルタ優先度設定はパケット スライシングと一緒に使用できます。たとえば、各 HTTP パケットのより多くのバイトを保持したいとします。スライシングを「TCP ヘッダ + 50 バイト」に設定し、優先度を 1 に設定して、TCP およびポート 80 のフィルタを指定します。その後、スライシングを「TCP ヘッダ + 1 バイト」に設定し、優先度を 10 に設定して、TCP の別のフィルタを指定します。このシナリオでは、ほかの TCP トラフィックよりも HTTP トラフィックに対してより多くのペイロードバイトが保持されます。

- **Packet Slicing Mode**。各パケットの選択した部分のみをキャプチャするためのオプション。ハードウェアフィルタでは、TCP/IP 以外のプロトコルのパケットをキャプチャできます。ただし、Multi-Port Monitor は、TCP トラフィックに関してのみパフォーマンス メトリックを収集します。ボリューム メトリックはすべてのトラフィック タイプに対して収集されます。

Capture full packet : フィルタを通過する各パケットからすべての情報がキャプチャされます。

Capture fixed size : すべてのパケットから数バイトがキャプチャされます。[Packet Slicing Size] フィールドで、キャプチャするバイト数を指定します。

Capture headers plus size : すべてのレイヤ 2、レイヤ 3、およびレイヤ 4 ヘッダ、および [Packet Slicing Size] フィールドのペイロードバイトの固定数がキャプチャされます。レイヤ 2 ヘッダには Ether II、LLC、SNAP、Raw ヘッダ、および VLAN、ISL、MPLS タグが含まれます。レイヤ 3 ヘッダには IPv4 (IPv4 オプションを含む)、IPv6、および IPX ヘッダが含まれます。レイヤ 4 ヘッダには TCP、UDP、および ICMP ヘッダが含まれます。

- **Include only Protocols**。キャプチャして処理するプロトコルを制限します。選択したプロトコルのみが監視に含まれます。チェックボックスがオンになっていない場合、すべてのプロトコルが含まれます。

Transport Control Protocol (TCP) は CA Application Delivery Analysis が監視する主なプロトコルです。

User Datagram Protocol (UDP) は、リアルタイムまたはストリーミングアプリケーションが送信するデータの転送に使用されます。

Internet Control Message Protocol (ICMP) は、サーバ間のエラーメッセージングおよび CA Application Delivery Analysis traceroute 調査に使用されます。キャプチャして処理するプロトコルを制限します。選択したプロトコルのみが監視に含まれます。チェックボックスがオンになっていない場合、すべてのプロトコルが含まれます。

- **VLANs**。監視するまたは監視から除外する仮想ローカルエリアネットワーク (VLAN) の識別子。トラフィックが指定された論理ポートを通過する VLAN の識別子をリストします。複数の VLAN はカンマを使用し、スペースなしで区切ります。リストした VLAN からのトラフィックを破棄するには、[Exclude] を選択します。
- **Subnets**。監視するまたは監視から除外するサブネット。有効な IPv4 アドレスおよびサブネットマスク、または有効な IPv6 アドレスおよびプレフィックスビットを指定します。リストで IPv4 と IPv6 のアドレスを組み合わせないでください。リストしたサブネットからのトラフィックを破棄するには、[Exclude] を選択します。

IPv4 アドレスには $x.x.x.x/n$ の形式を使用します。 $x.x.x.x$ はドット付き表記の IPv4 サブネットアドレスで、 n はマスクに使用するビットの数です。

IPv6 アドレスには $x:x:x:x/n$ の形式を使用します。 $x:x:x:x$ はコロン区切りの IPv6 サブネットアドレスで、 n はプレフィックスビットの数です。標準の IPv6 アドレスの短縮形を使用できます。たとえば、 $2001:ba0:1a0::/48$ などです。

ヒント： IPv4 および IPv6 のサブネットをフィルタするには、IPv4 サブネット用にハードウェアフィルタを 1 つ作成し、IPv6 サブネット用に別のハードウェアフィルタを作成します。

- **IP Addresses**。監視するまたは監視から除外する個別のホストの IPv4 または IPv6 のアドレス、またはアドレスの範囲。複数のアドレスはカンマを使用し、スペースなしで区切ります。範囲は、ハイフンを使用し、スペースなしで区切ります。リストで単一のアドレスと範囲を組み合わせないでください。アドレスの同じリストまたは範囲で IPv4 と IPv6 のアドレスを組み合わせないでください。リストしたアドレスからのトラフィックを破棄するには、[Exclude] を選択します。

IPv4 アドレスにはドット付き表記を使用します。たとえば、 $10.9.7.7$ 、または $10.9.8.5-10.9.8.7$ などです。

コロン区切りの IPv6 アドレスを使用します。標準の IPv6 アドレスの短縮形を使用できます。たとえば、 $2001:f0d0:1002:51::4$ などです。

ヒント： IPv4 および IPv6 のアドレスをフィルタするには、IPv4 アドレス用にハードウェアフィルタを 1 つ作成し、IPv6 アドレス用に別のハードウェアフィルタを作成します。

Ports。 監視するまたは監視から除外する TCP ポートまたはポート範囲。複数のポート番号はカンマを使用し、スペースなしで区切ります。ポートの範囲については、**2483-2484** のような形式を使用します。リストしたポートからのトラフィックを破棄するには、**[Exclude]** を選択します。

- b. (オプション) **[Advanced]** をクリックし、正規表現を使用してより詳細なフィルタを作成します。詳細については、「**Use Regular Expressions for Precise Filtering**」を参照してください。
 - c. **[Save]** をクリックします。新しいフィルタが **[Logical Ports: Hardware Filters]** ページに表示されます。
4. フィルタを変更または有効にするには、**[Edit]** をクリックします。**[Logical Ports: Edit Hardware Filter]** ページが表示されます。
 - a. 手順 3a の説明に従ってフィールドに入力します。
 - b. (オプション) **[Show Details]** をクリックして、正規表現として選択内容を表示します。
 - c. **[Save]** をクリックします。フィルタが **[Logical Ports: Hardware Filters]** ページに表示されます。
 5. フィルタを有効にした場合は、**nqcapd** プロセスを再起動します。

論理ポートに TIM 監視を構成する

TIM は、1 つの論理ポートからのミラーポートを監視します。複数の物理ポートを 1 つの論理ポートにマップするには、WAN からの Web トラフィックを論理ポートにミラーリングします。このトラフィックは TIM および **CA Application Delivery Analysis** のために処理されます (環境にこの製品がある場合)。ほかのポートミラーリングのために、理想的にはサーバに最も近いアクセス層スイッチからのほかの論理ポートを使用します。**Multi-Port Monitor** 上の TIM 以外の論理ポートは、**CA Application Delivery Analysis** のみのために処理されます。

次の手順に従ってください:

1. ブラウザ ウィンドウを開き、**Multi-Port Monitor Web** インターフェースにログインします。

Multi-Port Monitor Web インターフェースが開きます。

2. **[Administration]** タブをクリックします。

[Logical Ports] ページが表示されます。利用可能なポートのデフォルト設定が表示されます。

1. **[Edit Filters]** 列の **[Filters]** リンクをクリックして、ハードウェアフィルタをポートに適用します。
2. 以下の情報を入力します。

名前

TIM が監視する論理ポートの名前を指定します。

名前は、監視しているトラフィックのソースを識別するのに役立ちます。たとえば、監視しているスイッチの名前または場所を使用します。

有効

監視用のポートを有効にします。

[Enabled] チェック ボックスがオンになっていることを確認します。

Save Packets to Disk

(オプション) キャプチャされたデータ パケットを **Multi-Port Monitor** ハードディスク ドライブに保存します。このオプションを有効にすると、データは **[Analysis]** ページで PCAP にエクスポートできるようになります。デフォルトでは、**Multi-Port Monitor** は、パケットを 6 時間保持します。

TIM Monitor

構成している論理ポートに関連付けます。

構成している論理ポートに関連付けられているチェック ボックスをオンにします。

Physical Ports

1 つ以上の利用可能な物理ポートを論理ポートに割り当てます。

利用可能なポートは、CA Technologies から購入したキャプチャカード構成によって異なります。

論理ポートの番号は、0 から始まります。キャプチャ層が、物理ポートから論理ポートへのマッピングを実行します。マッピング処理は、TIM に対して透過的に行われます。

3. [保存] をクリックします。
4. nqcapd プロセスを再起動します。
このタスクを Multi-Port Monitor の [プロセス] ページで実行します。
5. (オプション) [System Status] ページで [Capture Card Logical Port Status] テーブルを表示して、論理ポートのステータスを確認します。
ポートに関連付けられたハードウェア フィルタ内の構文エラーなど論理ポートの開始に関する問題がある場合は、[Status] 列にエラー ステータスが表示されます。

マルチプロセス モードでの TIM

TIM を Multi-Port Monitor にインストールすると、TIM は複数プロセス間のトラフィックの負荷を複数の CPU 間で分散させることができます。マルチプロセス モードで実行すると、TIM のスループットが著しく増加します。正確なスループット値は、監視するトラフィックやトランザクションの定義方法など多くの要因によって異なります。

マルチプロセス モードでは、TIM は、ワーカ プロセスと呼ばれる複数のプロセス間にネットワーク トラフィックを分散します。マルチプロセス モードの TIM を効率的に動作させるには、以下の手順に従います。

- 監視対象トラフィックをワーカ プロセス間でできるだけ均等に分配します。
- 同じワーカ プロセスが同じビジネス トランザクション インスタンスに属するすべてのパケットを監視することを確認します。

異なるネットワーク構成では、これらのガイドラインは別の手段によって達成できます。CA Technologies では、ワーカ プロセス間のトラフィックを分配するために、いくつかの柔軟な方法を用意しています。以下のオプションがあります。

クライアント IP アドレス

ネットワーク トラフィックは、クライアント IP アドレスに基づいてワーカ プロセスに割り当てられます。これがデフォルトで、CA Technologies の推奨値です。お使いのネットワーク環境でこのオプションが有用でない場合は、ほかのオプションを考慮します。たとえば、TIM がプロキシ サーバの後ろに配置されている場合など、すべてのトラフィックが同じクライアント IP アドレスから送信されているように見える場合などは、その他の設定オプションを検討します。この例のデフォルト設定は `shared=client` です。このネットワーク環境では、クライアント IP アドレスを使用して TIM 上で負荷分散することはできません。このため、サーバ IP アドレス オプションを使用することを考慮します。

サーバ IP アドレス

ネットワーク トラフィックは、サーバ IP アドレスに基づいてワーカ プロセスに割り当てられます (`shared=server` など)。このオプションでは、1つのサーバが1つのビジネス トランザクションのすべてのトランザクションを処理する必要があります。

混在

トラフィックは、クライアントとサーバの IP アドレスの組み合わせに基づいてワーカ プロセスに割り当てることができます。サーバルールとクライアント ルールの間には不一致がある場合は、サーバルールが優先されます。

ロード バランサ構成ファイルを使用して、TIM がクライアントまたはサーバをどのように負荷分散するかを定義します。

注: スタンドアロンの TIM はシングルプロセス モードで実行されます。

構成ファイルを編集する方法については、次を参照してください

[ロード バランサ構成ファイルを編集する](#) (P. 50)

例: マルチプロセス モードで実行するための設定オプション

以下の例では、TIM をマルチプロセス モードでセットアップするための設定オプションを示します。設定の変更は、`/etc/wily/cem/tim/config/` 内にあるバランサ構成ファイル (`balancer.cnf`) で行います。設定の変更を有効にするには、TIM を再起動します。

例 1

138.42.123.* /24 サブネットに属する、HTTP トランザクションが発生するクライアントの場合、次の設定を使って、このサブネットにワーカ プロセス 0 を割り当てます: `client=138.42.123.* /24 worker=0`。

例 2

138.42 サブネット内にサーバがある場合は、次の設定を使って、このサブネットにワーカ プロセス 0 を割り当てます: `server=138.42.0.0/16 worker=0`。

TIM のマルチプロセス モードの設定

TIM をマルチプロセス モードに設定すると、TIM は複数プロセス間のトラフィックの負荷を複数の CPU 間で分散させることができます。この設定には、2 段階の処理があります。

1. [ロードバランサ構成ファイルを編集する](#) (P. 50)。
2. [マルチプロセス モードを有効にする](#) (P. 52)。

ロードバランサ構成ファイルを編集する

ロードバランサ構成ファイルを編集して、TIM がクライアントまたはサーバをどのように負荷分散するかを定義します。ロードバランサ構成ファイルはプレーンテキストファイルのため、変更を加える場合はテキストエディタを使用する必要があります。

次の手順に従ってください：

1. 接続されているキーボードとモニタを使用して、統合アプライアンス（TIM を実行する Multi-Port Monitor）に直接ログインします。また、Windows 上で実行される PuTTY などのセキュア シェル（SSH）クライアントを使用して、リモート システムからログインすることもできます。
 1. 接続されているキーボードとモニタを使用している場合は、最初の画面で **Alt+F2** を押します。

Linux ログイン画面が表示されます。
 2. 以下のクレデンシャルでログインします。
 - ユーザ名：netqos
 - パスワード：Multi-Port Monitor ソフトウェアをインストールした際に作成したパスワード。

「netqos」のユーザ名とパスワードは、スーパーユーザ アクセスを提供します。

Linux コマンドライン インターフェイスが開きます。
2. テキスト エディタを使用して **balancer.cnf** ファイルを開きます。

このファイルは **/etc/wily/cem/tim/config/balancer.cnf** にあります。

ワープロなどのような、書式情報を付加するプログラムを使用しないでください。
3. コマンドの先頭に「**sudo**」を付加して、ファイルの編集を行います。設定ファイルは、スーパーユーザ アクセスおよび「**sudo**」を先頭に付加した場合にのみ編集できます。

たとえば、vi エディタを使用している場合は、以下のコマンドを使用します。

```
$ sudo vi /etc/wily/cem/tim/config/balancer.cnf
```
4. ファイルを保存します。
5. TIM を再起動します。

編集を適用するために TIM を再起動する必要があります。

マルチプロセス モードの有効化/無効化

TIM 設定ウィンドウから、マルチプロセス モードを有効/無効にします。このモードはデフォルトで有効になっています。

次の手順に従ってください：

1. Multi-Port Monitor UI にログオンし、[System Setup] を選択します。
2. Tim x.x.x.x build xx を選択します。
TIM 設定ページが表示されます。
3. [Configure TIM Settings] を選択します。
[TIM Settings] ページが表示されます。
4. [Parallel/UseWorkers] を選択します。
5. [New Value] フィールドを必要に応じて変更します。
1 はマルチプロセス モードが有効であることを意味します。
0 はマルチプロセス モードが無効であることを意味します。
6. TIM を再起動します。
この変更を有効にするには、TIM を再起動する必要があります。

TIM を Enterprise Manager に関連付ける

このタスクは、Multi-Port Monitor 上の TIM とスタンドアロンの TIM の両方に関連します（該当する場合）。

TIM がトランザクションを監視できるように、TIM を有効にします。TIM 監視が無効であると Enterprise Manager にデータが送信されません。Enterprise Manager をクラスタ化している場合は、MOM Enterprise Manager から TIM を有効化します。

TIM を有効にする場合の例を以下に示します。

- TIM を設定して Enterprise Manager に関連付ける場合
- TIM または Enterprise Manager、あるいはその両方をアップグレードした後
- 構成をインポートした後

次の手順に従ってください:

1. Web ブラウザを開き、Enterprise Manager をホストするサーバのアドレスを入力します。クラスタ化された環境を使用している場合は、MOM のアドレスを指定します。

`http://<IP_Address>:8081`

<IP_Address> は、MOM またはスタンドアロン Enterprise Manager の IP アドレスまたは DNS 名です。例:

`http://192.168.1.54:8081`

`http://cem.company.com:8081`

DNS 名を使用するには、DNS 管理者によって DNS 名が設定されている必要があります。

注: デフォルトのポートは 8081 です。これは *IntroscopeEnterpriseManager.properties* ファイル内で *introscope.enterprisemanager.webserver.port=8081* のように定義されており、変更することができます。

2. ユーザ名とパスワードを入力します。
CEM コンソールが表示されます。
3. [設定] - [監視] を選択します。
4. TIM がリストに表示されない場合
 - a. [新規] をクリックします。
 - b. TIM の名前と IP アドレスを入力します。
 - c. TIM が Multi-Port Monitor ポート上でリスンする場合は、[Multi-Port Monitor 有効] チェック ボックスをオンにします。
この操作は Multi-Port Monitor をデプロイしている場合にのみ行います。
 - d. [保存] をクリックします。
5. 必要な TIM ごとに、隣にあるチェック ボックスをオンにし、[有効化] をクリックします。

これで、Enterprise Manager と TIM 間の通信が有効になります。追加のタブが、CA CEM コンソールに表示されます。

(オプション) Web サーバフィルタの構成

このタスクはオプションです。ハードウェアフィルタを構成した後でも大量のネットワークトラフィックが存在する場合は、このタスクを実行します。この場合、Web サーバフィルタを構成することによって、TIM が監視するトラフィックを特定のサーバにさらに制限する必要があります。TIM が過負荷になると、記録が機能しない場合があります。

Multi-Port Monitor は、アプライアンス上で実行する TIM 用に構成された Web サーバフィルタを使用して、TIM に転送するデータを定義します。

次の手順に従ってください：

1. CEM にログオンします。
2. [設定] の [Web サーバフィルタ] を選択します。
3. [新規] をクリックします。
4. TIM 監視の対象となるネットワークの箇所を説明する名前を入力します。たとえば、*WebFarmCorp1* となります。

5. [監視] リストで、ネットワークのこの箇所を監視する TIM を選択します。

各 TIM はデフォルトで IP アドレス範囲を監視します。特定の MAC アドレスで監視する場合は、手順 6 に進んでください。

- a. [開始 IP アドレス] フィールドに入力します。

範囲内でアドレス値が最も低い Web サーバの IP アドレスを入力します。監視対象サーバが 1 台のみの場合は、特定の IP アドレスを入力します。

- b. [終了 IP アドレス] フィールドに入力します。

範囲内でアドレス値が最も高い Web サーバの IP アドレスを入力します。監視対象サーバが 1 台のみの場合は、特定の IP アドレスを入力します。

- c. [ポート] フィールドに入力します。
 - TIM が特定のポートでのみトランザクションを監視する場合は、ポート番号を入力します。
 - TIM がすべてのポートですべてのトランザクションを監視する場合は、0 (デフォルト) を入力します。
 - d. ほとんどの場合、TIM は、サーバが重複しないように、ネットワーク内の特定のサーバを監視することをお勧めします。ただし、特殊な状況では、IP アドレスの重複を許可することもできます。

1 つの IP アドレスまたは範囲に対して複数の監視を構成する場合は、[IP アドレスの重複を確認せずに保存] チェック ボックスをオンにします。
6. IP アドレス範囲の代わりに特定の MAC アドレスを監視する場合：
 - a. [アドレスタイプ] で [MAC アドレス] をクリックします。
 - b. 監視するデバイスの MAC アドレスを入力します。例：
12:eb:a0:32:51:4c
 7. [保存] をクリックすると、TIM 監視が指定どおりに構成されます。

監視の同期

監視を同期して、現在のドメイン構成ファイルをすべての有効な TIM およびエージェントに送信します。

次の手順に従ってください：

1. CEM コンソールにログオンします。
2. [設定] - [監視] を選択します。
3. 必要な監視が無効になっている場合は、それらを有効にします
4. [すべての監視を同期] をクリックします。

有効な監視がすべて同期され、関連するアイコンが右上に表示されます。このタスクを実行することにより、更新されたトランザクション定義が、ネットワーク上のすべての有効な TIM に送信されます。TIM は、定義されているトランザクションの監視をただちに開始します。すべての監視を同期すると、CEM コンソールはトランザクションおよび追跡情報も Enterprise Manager に送信します。

接続の確認

表示している障害について、ネットワーク データが **Multi-Port Monitor** データベースから **CEM** コンソールにインポートされます。このデータは **TIM** によって生成された障害と共に **CEM** の [障害詳細] ページに表示されます。

CEM の [障害詳細] ページでネットワーク データを探し、**Multi-Port Monitor** への **CA APM** 接続を確認します。

次の手順に従ってください：

1. **CEM** コンソールにログオンします。
2. [CEM] - [インシデント管理] - [障害] を選択します。
3. 以下のいずれかの操作を行います。
 1. リストから障害を選択します。
 2. 特定の障害を検索します。
4. 選択した障害に関連付けられたネットワークの稼働状況メトリックを確認します。

[CT 計測値]、[DTT]、[ENRTT]、[TCP 対話分析] などのネットワーク メトリックを使用できます。[TCP 対話分析] フィールドで、**Multi-Port Monitor** へのリンクを使用できます。

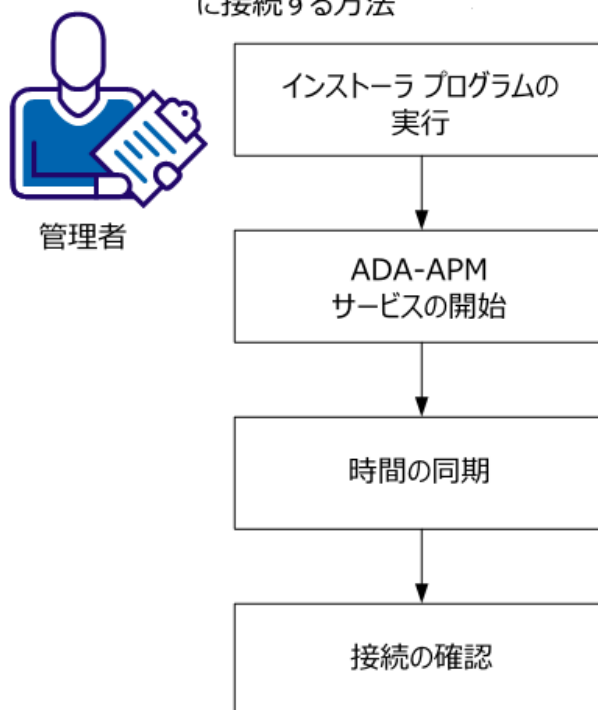
これらのメトリックの詳細については、「**CEM** コンソールから開始するアプリケーションおよびインフラストラクチャの問題を切り分ける方法」を参照してください。

CA APM を Application Delivery Analysis に接続する方法

CA APM を **CA Application Delivery Analysis (ADA)** に接続することにより、**APM WebView** でインフラストラクチャ データを表示できます。**Enterprise Manager** は定期的に **ADA** マネージャ上の **Web** サービスを呼び出してこれらのメトリックを取得し、**APM WebView** 上に表示します。また、**Enterprise Manager** は、履歴レポートで使用するために、これらのメトリックを **SmartStor** に格納します。

以下の図に、管理者として CA APM を CA Application Delivery Analysis に接続する方法を示します。

CA APM を Application Delivery Analysis に接続する方法



管理者として、以下の手順を実行します。

1. [インストーラプログラムを実行します](#) (P. 58)。
2. [ADA-APM サービスを開始します](#) (P. 62)。
3. [時間を同期します](#) (P. 62)。
4. [接続を確認します](#) (P. 63)。

前提条件

開始する前に、以下のものがインストールおよび設定されていることを確認します。

- CA Application Delivery Analysis 9.1 以降
- NetQoS Performance Center 6.1/CA Performance Center 2.0
- APM データベース 9.1 以降

- Enterprise Manager 9.1 以降
- CA APM Workstation 9.1 以降
- CA APM WebView (オプション)
- 以下のいずれかが必要です。
 - CA APM .NET エージェント 9.0 以降
 - CA APM Java エージェント 9.0 以降

インストーラプログラムの実行

CA APM Integration for CA Application Delivery Analysis インストーラ プログラムには、CAPC Integration Pack と CA Application Delivery Analysis Extension for APM の 2 つのインストール可能コンポーネントが含まれています。このセクションの操作手順では、CA Application Delivery Analysis Extension for APM のインストール方法を示します。このインストール可能コンポーネントは、CA Application Delivery Analysis と CA APM 間の通信を可能にします。

インストール可能コンポーネントを Enterprise Manager または MOM (クラスタ化された CA APM 環境の場合) にインストールします。

インストールを完了するには、以下の情報が必要です。

- Enterprise Manager のホスト名
- Enterprise Manager のポート番号
- CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントが接続するサーバのホスト名または IP アドレス

次の手順に従ってください:

1. [CA サポート](#) の CA APM ソフトウェア ダウンロード セクションから、CA APM Integration for CA Application Delivery Analysis インストーラ プログラムをダウンロードします。
2. Integration Pack インストーラ プログラムのローカルバージョンを見つけて、ダブルクリックします。
インストーラが開始します。
3. 初期画面で [次へ] をクリックします。

4. エンドユーザ ライセンス使用条件の内容を確認します。
続行するには、使用条件に同意します。
5. 統合パック ファイルのインストール先を指定し、[次へ] をクリックします。
6. CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントを選択します。
7. [次へ] をクリックします。
8. このインストール可能コンポーネントの接続先の Enterprise Manager のホスト名およびポートを指定し、[次へ] をクリックします。
9. このインストール可能コンポーネントの接続先のすべての CA Application Delivery Analysis コンソールのホスト名または IP アドレスを指定し、[次へ] をクリックします。
10. CA Application Delivery Analysis Extension for APM を Windows サービスとして設定するかどうかを指定し、[次へ] をクリックします。

Windows OS 環境では、CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントは、ADA-APM サービスをインストールします。
11. 設定を確認し、[インストール] をクリックします。

CA Application Delivery Analysis プロパティ ファイル

CA Application Delivery Analysis Extension for APM のインストールが完了すると、ADAExtensionForAPM フォルダに ADACConnector ファイルが作成されています。これらのファイルを使用して、構成を確認します。また、必要に応じてデフォルト設定を更新します。

以下に、CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントによって設定される構成の一部を示します。これらのプロパティを使用して、構成を確認し、必要に応じて更新します。

Enterprise Manager のホスト名

com.wily.apm.adaconnector.em.host=<EM ホスト名>

Enterprise Manager のポート番号

com.wily.apm.adaconnector.em.port=<EM ポート>

ホスト名または IP アドレス

この情報は、CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントが接続されるすべての ADA マネージャの値を反映します。

```
com.wily.apm.adaconnector.adawsssoap_address_source1=<アドレス>  
com.wily.apm.adaconnector.ada_hostName1=<ホスト名>
```

インストーラプログラムの名前

```
com.wily.apm.adaconnector.ada_processName1=<ADAExtensionforAPM>
```

ADAExtensionforAPM 値は、Workstation で見られるようなプロセス名を表します。

ADAConector ファイルでは、以下の構成を設定できます。

機能拡張されたメトリック

これらのインフラストラクチャメトリックに対するクエリは、デフォルトでは無効です。以下のインフラストラクチャメトリックを Workstation で利用できるようにするには、クエリを有効にします。

- データ転送時間
- ネットワーク ラウンドトリップ時間
- 再送遅延
- サーバ応答時間

サンプルプロパティ

```
com.wily.apm.adaconnector.ada_enhancedmetrics_enabled2=<true|false>
```

<enabled2> は、ADA マネージャのインデックスです。最初の ADA マネージャは <enabled1> に相当し、2 番目の管理コンソールは <enabled2> に相当します。以降同様です。

CA Application Delivery Analysis Web サービス クエリ

ADA データ時間枠と Web サービス クエリとの間の待機時間です。デフォルトの待機時間は 5 分です。ADA マネージャは、Multi-Port Monitor やシングルポート ADA コレクタなどさまざまなコレクタに接続できます。収集されたデータを集約できるようにするために、ADA 時間枠は、5 分間の長さで、7:00、7:05 のように 5 分の境界で終了します。ADA マネージャは、データベースを 5 分ごとに更新します。このプロパティの待機時間値は、クエリの対象となる時間枠を、指定したタイムフレームだけ移動させます。たとえば、待機時間を 2 分として定義すると、ADA 時間枠は、7:02、7:07 のように 2 分遅れて始まるようになります。

CA サポート から指示された場合を除き、デフォルト値を変更しないことをお勧めします。

注: このプロパティを更新しても Web サービス呼び出しの頻度は変更されません。この頻度は 5 分間隔に固定されています。

サンプルプロパティ (ミリ秒単位)

```
com.wily.apm.adaconnector.adawebservice.wait=120000
```

SmartStor データフィード間隔

ADA から Enterprise Manager へのデータフィード間隔。

デフォルトの間隔は 15 秒です。CA サポート から指示された場合を除き、デフォルト値を変更しないことをお勧めします。

サンプルプロパティ (ミリ秒単位)

```
com.wily.apm.adaconnector.smartstorfeed.interval=15000
```

SmartStor データフィード待機時間

CA Application Delivery Analysis Web サービスのクエリと、Enterprise Manager がデータフィードを開始するまでの間の待機時間。

デフォルトの待機時間は 10 秒です。CA サポート から指示された場合を除き、デフォルト値を変更しないことをお勧めします。

サンプルプロパティ (ミリ秒単位)

```
com.wily.apm.adaconnector.smartstorfeed.wait=10000
```

ADA-APM サービスの開始

CA Application Delivery Analysis Extension for APM のインストール可能コンポーネントをインストールした後、ADA-APM サービスを開始します。

Windows OS

Windows サービスで ADA-APM サービスを開始します。

このサービスは自動的に開始しません。インストール後、手動で開始します。

Linux/UNIX OS

以下のコマンドを使用して、CA Application Delivery Analysis Extension for APM を開始します。

```
<INSTALL_HOME>%ADAExtensionForAPM$./ADACconnector
```

時間の同期

以下のマシン間のクロックを共通時間ソースに同期させます。

- CA Application Delivery Analysis
- Enterprise Manager または MOM

クロックを同期させることにより、NetQoS Performance Center/CA Performance Center 上の CA APM アプリケーション データと APM WebView 上のインフラストラクチャ データの整合性が確保されます。このタスクが実行されない場合、コンポーネント間で時間の誤差が発生し、不正確なデータまたはデータの損失が発生することがあります。

CA Technologies は、ネットワーク全体を NTP (Network Time Protocol) 時間ソースまたは時間サーバに同期させることを推奨します。これができない場合は、少なくとも、上記のマシンを同期させる必要があります。

接続の確認

組み込みのダッシュボードと特定のネットワーク メトリックを探し、CA APM と CA Application Delivery Analysis の接続を確認します。

次の手順に従ってください：

1. APM WebView または Introscope Workstation のいずれかにログオンします。
2. コンソールで [ネットワーク ステータス情報] ダッシュボードを探します。
3. Investigator の [メトリック ブラウザ] タブで、各クライアント サブネット およびサーバの以下の情報を探します。
 - ネットワークの稼働状況ステータス
 - サーバの稼働状況ステータス
 - データ転送時間
 - ネットワーク ラウンドトリップ時間
 - 再送遅延
 - サーバ応答時間

デフォルトでは、以下のメトリックは無効です。

- データ転送時間
- ネットワーク ラウンドトリップ時間
- 再送遅延
- サーバ応答時間

これらのメトリックを有効にするには、ADA プロパティ ファイルで `com.wily.apm.adaconnector.ada_enhancedmetrics_enabled1=<true|false>` プロパティを使用します。このプロパティ ファイルの詳細については、「CA APM を Application Delivery Analysis に接続する方法」のシナリオを参照してください。

[ネットワーク ステータス情報] ダッシュボードから、NetQoS Performance Center/CA Performance Center に直接移動できます。組み込みのダッシュボードに加えて、インフラストラクチャ メトリックを使用してカスタム ダッシュボードも作成できます。

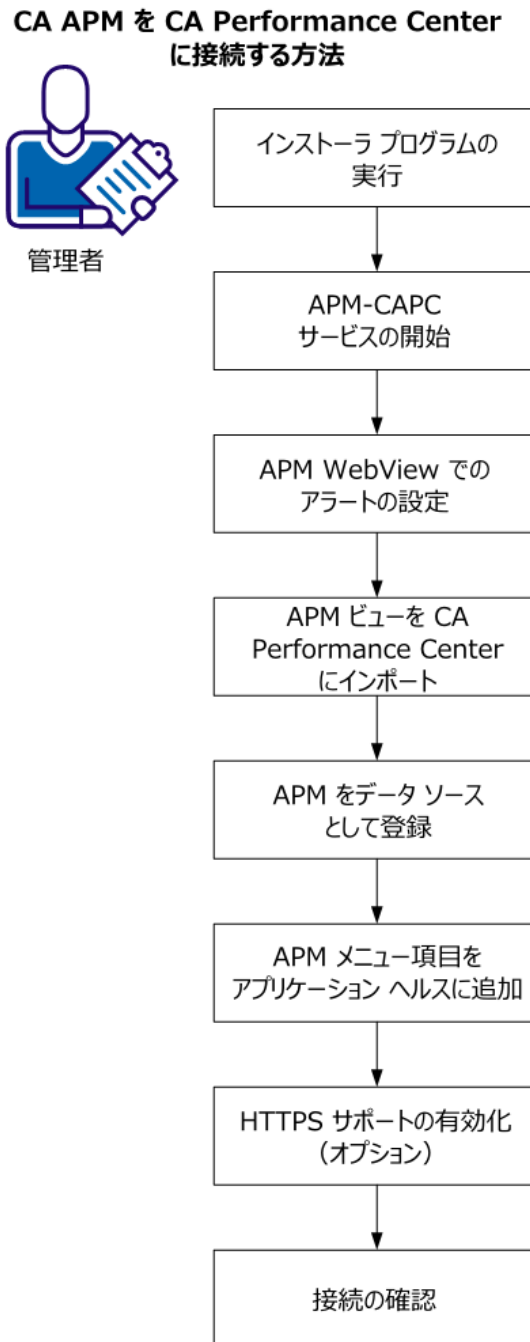
注: ダッシュボードの作成の詳細については、「*CA APM Workstation ユーザガイド*」を参照してください。

CA APM を CA Performance Center に接続する方法

CA APM を CA Performance Center に接続することにより、CA Performance Center で CA APM アプリケーション データを表示できます。アプリケーション データは、Enterprise Manager から CA Performance Center に流れます。

CA APM は、CAPC Integration Pack のインストール可能コンポーネントを使用して CA Performance Center に接続されます。このインストール可能コンポーネントは、APM-CAPC サービスをインストールし、CA Performance Center が認識および表示できる形式で CA APM データを提供します。

以下の図に、管理者として CA APM を CA Performance Center に接続する方法を示します。



管理者として、以下の手順を実行します。

1. [インストーラプログラムを実行します](#) (P. 67)。
2. [APM-CAPC サービスを開始します](#) (P. 68)。
3. [APM WebView でアラートを設定します](#) (P. 69)。
4. [APM ビューを CA Performance Center にインポートします](#) (P. 71)。
5. [APM をデータ ソースとして登録します](#) (P. 71)。
6. [APM メニュー項目をアプリケーションヘルスに追加します](#) (P. 73)。
7. [HTTP サポートを有効にします \(オプション\)](#) (P. 74)。
8. [接続を確認します](#) (P. 75)。

前提条件

開始する前に、以下のものがインストールおよび設定されていることを確認します。

- CA Performance Center 2.0.00
- APM データベース 9.1 以降
- Enterprise Manager 9.1 以降
- CA APM Workstation 9.1 以降
- CA APM WebView (オプション)
- 以下のいずれかが必要です。
 - CA APM .NET エージェント 9.0 以降
 - CA APM Java エージェント 9.0 以降
- APM WebView または Workstation アプリケーション問題切り分けマップエレメントのアラート
- ビジネストラザクション、ビジネス サービス、およびビジネスコンポーネントを監視するためのエージェント

インストーラプログラムの実行

CA APM Integration for CA Application Delivery Analysis インストーラ プログラムには、CA Performance Center Integration Pack と CA CA Application Delivery Analysis Extension for APM の 2 つのインストール可能コンポーネントが含まれています。このセクションでは、CA Performance Center Integration Pack のインストール方法を示します。このインストール可能コンポーネントは、CA Performance Center と CA APM 間の通信を可能にします。

インストール可能コンポーネントを Enterprise Manager または MOM（クラスタ化された CA APM 環境の場合）にインストールします。

インストールを完了するには、以下の情報が必要です。

- Enterprise Manager のホスト名
- Enterprise Manager Web サーバのポート番号
- CA APM Workstation ユーザ名
- CA APM Workstation パスワード
- Enterprise Manager サービス ユーザ名およびパスワード
- CA Performance Center Integration Pack のインストール可能コンポーネントが使用する Web サーバ ポート

次の手順に従ってください:

1. [CA サポート](#) の CA APM ソフトウェア ダウンロード セクションから、CA APM Integration for CA Application Delivery Analysis インストーラ プログラムをダウンロードします。
2. Integration Pack インストーラ プログラムのローカルバージョンを見つけ、ダブルクリックします。
インストーラが開始します。
3. 初期画面で [次へ] をクリックします。
4. エンドユーザ ライセンス使用条件の内容を確認します。
続行するには、使用条件に同意します。
5. 統合パック ファイルのインストール先を指定し、[次へ] をクリックします。

6. CA Performance Center Integration Pack のインストール可能コンポーネントを選択します。
7. [次へ] をクリックします。
8. Enterprise Manager ホスト名および Web サーバ ポートを指定し、[次へ] をクリックします。
9. Enterprise Manager の CA Introscope® および TESS アカウントを指定し、[次へ] をクリックします。
10. CA Performance Center Integration Pack を Windows サービスとして設定するかどうかを指定し、[次へ] をクリックします。

Windows OS 環境では、CA Performance Center Integration Pack のインストール可能コンポーネントは APM-CAPC サービスをインストールします。

11. CA Performance Center Integration Pack で使用する Web サーバ ポートを指定し、[次へ] をクリックします。
12. 設定を確認し、[インストール] をクリックします。

CA Performance Center Integration Pack のインストール可能コンポーネントのインストール後、手順 5 で指定したディレクトリに CAPCIntegrationPack フォルダが表示されます。このフォルダには、抽出された Jetty Web サーバおよび apm-capc-integration フォルダを含む webapps フォルダがあります。

APM-CAPC サービスの開始

CA Performance Center Integration Pack をインストール後、APM-CAPC サービスを開始します。

Windows OS

Windows サービスで APM-CAPC サービスを開始します。

このサービスは自動的に開始しません。インストール後、手動で開始します。

Linux/UNIX OS

以下のコマンドを使用して、CA Performance Center Integration Pack を開始します。

```
<INSTALL_HOME>%CAPCIntegrationPack%bin$. /jetty.sh start
```

APM WebView でのアラートの設定

APM WebView のアラートでは、メトリックでしきい値を設定し、メトリックがしきい値を越えた際にアクションを実行できます。アプリケーション問題切り分けマップ内のオブジェクトの多くは、アラートを表示できます。これらのアラートには、オブジェクトのベースラインメトリックのワースト ケースのステータスが反映されます。

アラートを作成して、アプリケーション、ビジネス サービス、およびビジネス トランザクションの稼働状況ステータス インジケータを CA Performance Center で使用できるようにします。

次の手順に従ってください:

1. WebView で、 [Investigator] - [問題切り分けマップ] をクリックします。
2. ツリーで、以下のように編集するアラートに移動します。
By Frontend|Application_Name|Backend Calls|file%customer-records
3. コンポーネントを右クリックし、コンテキストメニューから [名前のアラートを編集] を選択します。
[名前のアラートの編集] ダイアログ ボックスが表示されます。
4. 左側のペインで、アラート ステータスに影響するメトリックを選択します。

5. [問題] ドロップダウン リストからアラートをトリガする問題のタイプを選択します。

高すぎる値

メトリック値がしきい値を超えたときにアラートをトリガします。

低すぎる値

メトリック値がしきい値を下回ったときにアラートをトリガします。

特定の不正な値

メトリック値がしきい値と等しいときにアラートをトリガします。その後、そのしきい値はしきい値ではなく不正な値として扱われます。

予期しない値

メトリック値がしきい値と等しくないときにアラートをトリガします。その後、その値はしきい値ではなく予期しない値として扱われます。

6. [サマリ メトリック] タブをクリックします。危険アラートおよび警告アラートのしきい値と感度レベルを設定して、[適用] をクリックします。

危険

メトリック値がしきい値を超えたときにアラートをトリガします。アラートは赤色で表示されます。

警告

メトリック値がしきい値に近づいたときにアラートをトリガします。アラートは黄色で表示されます。

7. [適用] をクリックします。
8. メトリックごとに手順 4 ~ 7 を繰り返します。
9. [OK] をクリックします。

NetQoS Performance Center への APM ビューのインポート

統合 XML ファイルをコピーし、APM ビュー定義を CA Performance Center データベースにインポートします。

次の手順に従ってください:

1. 以下の場所へ移動します。
`<CAPC Integration Pack Home>%CAPCIntegrationPack%CAPC_2_0`
2. 以下の場所の `plugins` フォルダに、`CAPC_2_0` フォルダから `apm` ディレクトリをコピーします。
`<CAPC-HOME>/PerformanceCenter/SQL/plugins`
3. コマンドプロンプトから以下のコマンドを実行して、ビューを CA Performance Center データベースにインポートします。
`<CAPC-HOME>/PerformanceCenter/Tools/bin/npcshell.sh dbmigrate -package com.ca.im.plugin.apm -path <CAPC-HOME>/PerformanceCenter/SQL/plugins/apm`

APM をデータソースとして登録

CA Performance Center は、登録されているデータソースからの情報のみを受信できます。

次の手順に従ってください:

1. 管理者権限を持つユーザとして CA Performance Center にログインします。
2. [管理] - [設定] を選択し、[データソース] をクリックします。
[データソースリスト] ページが表示されます。
3. [追加] をクリックします。
[データソースの追加] ページが表示されます。

4. [ソースタイプ] リストから [Application Performance Management] を選択します。

注: [ソースタイプ] リストには、CA Performance Center データソースとして登録できるすべての CA Technologies 製品が表示されます。製品には、お使いの環境にインストールされていないものや、サードパーティ製品と統合されているものも含まれます。ほかの企業から提供されている、サポート対象のデータソースは、必要な構成を完了した後に表示されます。Application Performance Management データソースでは、単一の有効なデータソースの定義がサポートされます。別のデータソースを追加する場合は、既存のデータソースを削除します。

5. データソースのホスト名を入力します。

ホスト名は、このデータソースのデータベースがインストールされているサーバの IP アドレスまたは DNS ホスト名です。CA APM データソースについては、CA Performance Center Integration Pack のインストーラプログラムがインストールされているホストの IP アドレスを入力します。

6. データソースに接続するために使用するプロトコルを選択します。CA APM データソースのデフォルトプロトコルは HTTP です。

ネットワークで通信に SSL が使用されている場合は、https を選択します。システムが正しく構成されていることを確認してから、https オプションを選択します。

注: CA Performance Center とデータソース製品との間の通信に SSL を使用することを計画している場合は、「CA Single Sign-on Guide」を参照してください。CA APM データソースに特有の条件として、ここで https オプションを選択した場合、Enterprise Manager と統合 Web サービスとの間で SSL 通信を有効にします。

7. データソースに接続するときに使用するポートを入力します。ポートは、前の手順で選択したプロトコルによって異なります。Application Performance Manager データソースのデフォルトポートは 8082 です。

注: CA Performance Center とデータソース製品との間の通信に SSL を使用する方法の詳細については、「Single-Sign-On Guide」を参照してください。

8. データソース用の表示名を入力します。デフォルトでは、データソースのタイプとホスト名を組み合わせ、データソースの名前が作成されます。

例: <データソース名>@<ホスト名>

注: Web コンソールのアドレスは CA APM には適用できません。

9. データソースの登録が完了したら、[保存] をクリックします。

登録したデータソースが、CA Performance Center のデータソースリストに表示されます。

[アプリケーションヘルス]への APM メニュー項目の追加

CA Performance Center で、以下の CA APM ダッシュボードメニュー項目を [アプリケーションヘルス] メニューに追加します。

- APM - アプリケーションステータス
- APM - ビジネス サービス ステータス

メニュー項目は、デフォルトのテナントまたは既存の任意のテナントに追加できます。既存のテナントにメニューが設定された後は、新しいテナントは以下の手順を実行せずに、自動的にメニューにアクセスできます。

次の手順に従ってください:

1. デフォルトのテナントまたは別のテナント管理者アカウントを持つ管理者としてログインします。
2. [管理] - [ユーザ設定] を選択し、[メニュー] をクリックします。
[メニューの管理] ページには、メニューの現在のリストが表示されます。
3. [アプリケーションヘルス] を選択し、[編集] をクリックします。
4. [利用可能] リストで、[APM - アプリケーション サマリ] ダッシュボードおよび/または [APM - ビジネス サービス サマリ] ダッシュボードを選択します。複数のダッシュボードを選択するには、Shift キーを押しながらクリックします。
5. 右矢印をクリックします。
6. ダッシュボードが [選択] リストに移動します。
7. [保存] をクリックします。
メニュー項目が設定されます。

HTTPS サポートの有効化(オプション)

SSL (Secure Sockets Layer) を使用して、セキュリティが強化された HTTPS プロトコルを有効にできます。この設定では、以下のような CA APM と CA Performance Center との間の通信が可能になります。

- サーバ証明書を取得します。一部の管理者は、セキュリティをさらに強化するために、クライアント証明書を使用することもできます。SSL、サーバ証明書、およびクライアント証明書を使用するために IIS の Web サイトを構成する手順は、このドキュメントの対象外です。ただし、以下の Microsoft の記事は、これらの IIS Web サイトのセキュリティ機能の使用方法について詳細に説明しています。

SSL and Certificates (IIS 6.0) :

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true>

- CA Performance Center と CAPC Integration Pack との間の HTTPS 通信を有効にするために、HTTPS 対応の [CA APM データ ソースを構成します](#) (P. 71)。
- [apm-capc-integration.properties ファイルを編集して](#) (P. 74)、Enterprise Manager と CAPC Integration Pack のインストール可能コンポーネントとの間の HTTPS 通信を有効にします。

apm-capc-integration.properties ファイルの編集

apm-capc-integration.properties ファイルを編集することにより、Enterprise Manager と CAPC Integration Pack のインストール可能コンポーネントとの間で HTTPS 通信を有効にできます。

次の手順に従ってください:

1. 以下の場所にある apm-capc-integration.properties ファイルをテキストエディタで開きます。
<INSTALLATION_HOME>%CAPCIntegrationPack%resources
2. プロパティ com.apm.npc.em.transport.protocol を探し、値 <https> を指定します。
3. プロパティ javax.net.ssl.keyStore を探し、値 <KEYSTORE LOCATION FOR SSL CONNECTION> を指定します。

4. プロパティ `javax.net.ssl.keyStorePassword` を探し、値 `<KEYSTORE PASSWORD FOR SSL CONNECTION>` を指定します。
5. プロパティ `javax.net.ssl.trustStore` を探し、値 `<TRUSTSTORE LOCATION>` を指定します。
6. プロパティ `javax.net.ssl.trustStorePassword` を探し、値 `<TRUSTSTORE PASSWORD>` を指定します。
プロパティが設定されます。

接続の確認

CA Performance Center では、選択した期間に対してドリルダウン方式でアプリケーションヘルスおよびパフォーマンス ステータス データが表示されます。CA APM を CA Performance Center にデータ ソースとして登録すると、[アプリケーション サマリ] レポートまたは [ビジネス サービス サマリ] レポートからアプリケーションデータにアクセスできます。これらのレポートから、インシデントおよび障害までドリルダウンできます。

事前設定済みのレポートのデータを探し、CA APM と CA Performance Center の接続を確認します。

次の手順に従ってください：

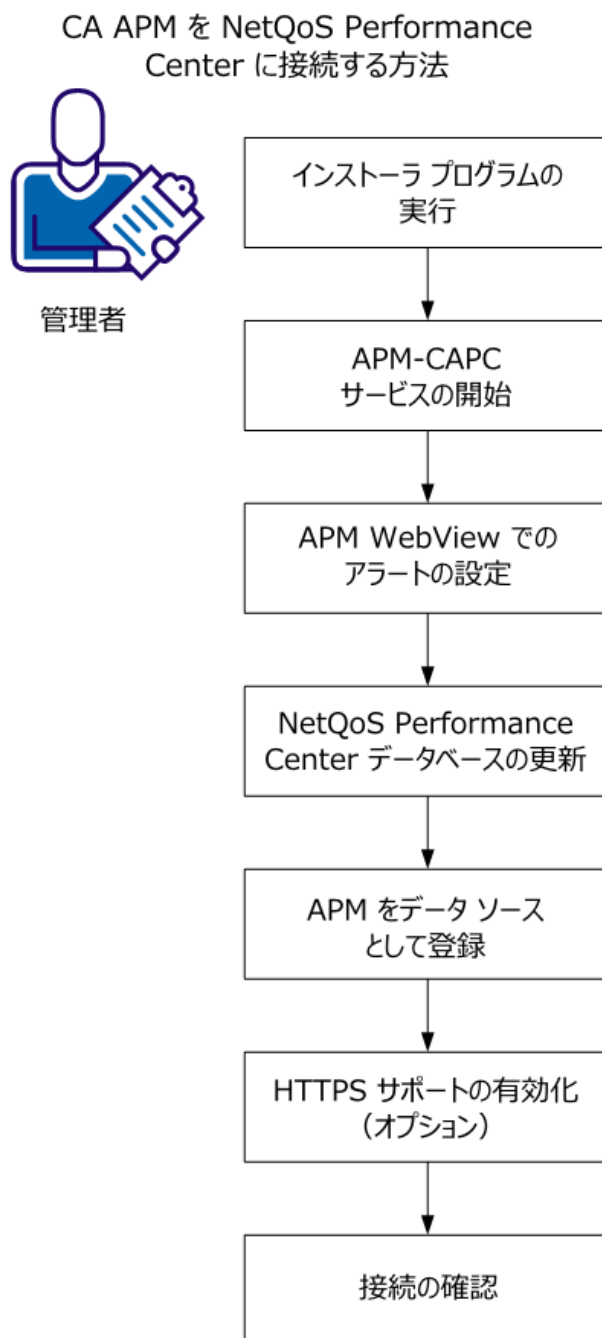
1. CA Performance Center にログオンします。
2. CA Performance Center の [レポート] メニューから、以下の CA APM 関連のレポートが表示されることを確認します。
 - APM-- アプリケーション サマリ
 - APM-- ビジネス サービス サマリ
3. [アプリケーション サマリ] レポートでビジネス アプリケーションの稼働状況ステータスが表示されます。
4. [ビジネス サービス サマリ] レポートで選択したアプリケーションのビジネス サービスの稼働状況ステータスが表示されます。

CA APM を NetQoS Performance Center に接続する方法

CA APM を NetQoS Performance Center (NPC) に接続することにより、NPC で CA APM アプリケーションデータを表示できます。

CA APM は、CAPC Integration Pack のインストール可能コンポーネントを使用して NPC に接続されます。このインストール可能コンポーネントは、APM-CAPC サービスをインストールし、NPC が認識および表示できる形式で CA APM データを提供します。

以下の図に、管理者として CA APM を NPC に接続する方法を示します。



管理者として、以下の手順を実行します。

1. [インストーラプログラムを実行します](#) (P. 79)。
2. [APM-CAPC サービスを開始します](#) (P. 68)。
3. [APM WebView でアラートを設定します](#) (P. 81)。
4. [NetQoS Performance Center データベースを更新します](#) (P. 82)。
5. [APM をデータ ソースとして登録します](#) (P. 83)。
6. [HTTP サポートを有効にします \(オプション\)](#) (P. 85)。
7. [接続を確認します](#) (P. 86)。

前提条件

開始する前に、以下のものがインストールおよび設定されていることを確認します。

- NetQoS Performance Center 6.1 以降
- APM データベース 9.1 以降
- Enterprise Manager 9.1 以降
- CA APM Workstation 9.1 以降
- CA APM WebView (オプション)
- 以下のいずれかが必要です。
 - CA APM .NET エージェント 9.0 以降
 - CA APM Java エージェント 9.0 以降
- APM WebView または Workstation アプリケーション問題切り分けマップ エレメントのアラート
- ビジネストランザクション、ビジネス サービス、およびビジネス コンポーネントを監視するためのエージェント

インストーラプログラムの実行

CA APM Integration for CA Application Delivery Analysis インストーラ プログラムには、CA Performance Center Integration Pack と CA Application Delivery Analysis Extension for APM の 2 つのインストール可能コンポーネントが含まれています。このセクションでは、CA Performance Center Integration Pack のインストール方法を示します。このインストール可能コンポーネントは、NetQoS Performance Center と CA APM 間の通信を可能にします。

インストール可能コンポーネントを Enterprise Manager または MOM（クラスタ化された CA APM 環境の場合）にインストールします。

インストールを完了するには、以下の情報が必要です。

- Enterprise Manager のホスト名
- Enterprise Manager Web サーバのポート番号
- CA APM WebView または Workstation ユーザ名
- CA APM WebView または Workstation パスワード
- Enterprise Manager サービス ユーザ名およびパスワード
- CAPC Integration Pack のインストール可能コンポーネントが使用する Web サーバ ポート

次の手順に従ってください:

1. [CA サポート](#) の CA APM ソフトウェア ダウンロード セクションから、CA APM Integration for CA Application Delivery Analysis インストーラ プログラムをダウンロードします。
2. Integration Pack インストーラ プログラムのローカルバージョンを見つけて、ダブルクリックします。
インストーラが開始します。
3. 初期画面で [次へ] をクリックします。
4. エンドユーザ ライセンス使用条件の内容を確認します。
続行するには、使用条件に同意します。
5. 統合パック ファイルのインストール先を指定し、[次へ] をクリックします。
6. CA Performance Center Integration Pack のインストール可能コンポーネントを選択します。

7. [次へ] をクリックします。
8. Enterprise Manager ホスト名および Web サーバ ポートを指定し、[次へ] をクリックします。
9. Enterprise Manager の CA Introscope® および TESS アカウントを指定し、[次へ] をクリックします。
10. CA Performance Center Integration Pack を Windows サービスとして設定するかどうかを指定し、[次へ] をクリックします。

Windows OS 環境では、CA Performance Center Integration Pack のインストール可能コンポーネントは APM-CAPC サービスをインストールします。

11. CA Performance Center Integration Pack で使用する Web サーバ ポートを指定し、[次へ] をクリックします。
12. 設定を確認し、[インストール] をクリックします。

CA Performance Center Integration Pack のインストール可能コンポーネントのインストール後、手順 5 で指定したディレクトリに CAPCIntegrationPack フォルダが表示されます。このフォルダには、抽出された Jetty Web サーバおよび apm-capc-integration フォルダを含む webapps フォルダがあります。

APM-CAPC サービスの開始

CA Performance Center Integration Pack をインストール後、APM-CAPC サービスを開始します。

Windows OS

Windows サービスで APM-CAPC サービスを開始します。

このサービスは自動的に開始しません。インストール後、手動で開始します。

Linux/UNIX OS

以下のコマンドを使用して、CA Performance Center Integration Pack を開始します。

```
<INSTALL_HOME>%CAPCIntegrationPack%bin$. /jetty.sh start
```


APM WebView でのアラートの設定

Workstation のアラートでは、メトリックでしきい値を設定し、メトリックがしきい値を越えた際にアクションを実行できます。アプリケーション問題切り分けマップ内のオブジェクトの多くは、アラートを表示できます。これらのアラートには、オブジェクトのベースラインメトリックのワーストケースのステータスが反映されます。

アラートを作成して、アプリケーション、ビジネス サービス、およびビジネス トランザクションの稼働状況ステータス インジケータを NetQoS Performance Center で使用できるようにします。

次の手順に従ってください:

1. WebView で、[Investigator] - [問題切り分けマップ] をクリックします。
2. ツリーで、以下のように編集するアラートに移動します。

By Frontend|*Application_Name*|Backend Calls|file%customer-records

3. コンポーネントを右クリックし、コンテキストメニューから [名前のアラートを編集] を選択します。

[名前のアラートの編集] ダイアログ ボックスが表示されます。

4. 左側のペインで、アラート ステータスに影響するメトリックを選択します。
5. [問題] ドロップダウン リストからアラートをトリガする問題のタイプを選択します。

高すぎる値

メトリック値がしきい値を超えたときにアラートをトリガします。

低すぎる値

メトリック値がしきい値を下回ったときにアラートをトリガします。

特定の不正な値

メトリック値がしきい値と等しいときにアラートをトリガします。その後、そのしきい値はしきい値ではなく不正な値として扱われます。

予期しない値

メトリック値がしきい値と等しくないときにアラートをトリガします。その後、その値はしきい値ではなく予期しない値として扱われます。

6. [サマリ メトリック] タブをクリックします。危険アラートおよび警告アラートのしきい値と感度レベルを設定して、[適用] をクリックします。

危険

メトリック値がしきい値を超えたときにアラートをトリガします。アラートは赤色で表示されます。

警告

メトリック値がしきい値に近づいたときにアラートをトリガします。アラートは黄色で表示されます。

7. [適用] をクリックします。
8. メトリックごとに手順 4～7 を繰り返します。
9. [OK] をクリックします。

NetQoS Performance Center データベースの更新

このタスクでは、`apm_integration.sql` スクリプトを使用して NetQoS Performance Center データベースを更新します。このスクリプトは、利用可能なデータソースのリストに CA APM データソースを追加します。NetQoS Performance Center でアプリケーションデータを表示するために必要な、そのほかの CA APM 固有の情報をデータベースに追加します。

SQL スクリプトを実行する方法

1. CAPCIntegrationPack フォルダから NetQoS Performance Center マシンに `apm_integration.sql` ファイルをコピーします。

このフォルダは、CA APM Integration Pack for CA Application Delivery Analysis インストーラをインストールすると作成されます。

2. Windows のコマンドプロンプトを開きます。
3. `cd <location of the apm_integration.sql>` を実行します。
4. `mysql` を実行します。

5. `source <path>%apm_integration.sql` を実行します。
NetQoS Performance Center データベースが更新されます。

CA APM をデータソースとして登録

NetQoS Performance Center は、登録されているデータソースからのみデータを受信できます。

注: データソースを管理する方法、および単一の NetQoS Performance Center インスタンスでサポートされるデータソースの数の詳細については、「*CA Performance Center 管理者およびユーザガイド*」を参照してください。

次の手順に従ってください:

1. 管理者権限を持つユーザとして NetQoS Performance Center にログインします。
2. [管理] - [設定] を選択し、[データソース] をクリックします。
[データソースリスト] ページが開きます。
3. [新規] をクリックします。
[データソースの追加] ページが開きます。
4. 追加するデータソースのタイプを [ソースタイプ] リストから選択します。

注: [ソースタイプ] リストには、NetQoS Performance Center データソースとして登録できるすべての CA Technologies 製品が表示されます。これらには、お使いの環境にインストールされていないものや、サードパーティ製品と統合されているものも含まれます。ほかの企業から提供されている、サポート対象のデータソースは、必要な構成を完了した後に表示されます。データソースタイプがリストに表示されない場合は、そのタイプで許容されるデータソースの最大数がすでに登録されていないかどうかを確認します。

5. データソースのホスト名を入力します。

ホスト名は、このデータソースのデータベースがインストールされているサーバの IP アドレスまたは DNS ホスト名です。CA APM データソースについては、CAPC Integration Pack のインストール可能コンポーネントがインストールされているホストの IP アドレスを入力します。

6. データ ソースに接続するために使用するプロトコルを選択します。CA APM データ ソースのデフォルト プロトコルは HTTP です。

ネットワークで通信に SSL が使用されている場合は、https を選択します。システムが正しく構成されていることを確認してから、https オプションを選択します。

注: NetQoS Performance Center とデータ ソース製品との間の通信に SSL を使用することを計画している場合は、「*CA Single Sign-on Guide*」を参照してください。CA APM データ ソースに特有の条件として、https オプションを選択した場合、Enterprise Manager と統合 Web サービスとの間で [SSL 通信を有効にする](#) (P. 85) 必要があります。

7. データ ソースに接続するときに使用するポートを入力します。ポート番号は、前の手順で選択したプロトコルによって異なります。デフォルトの CA APM ポートは 8082 です。

NetQoS Performance Center とデータ ソース製品との間の通信に SSL を使用する方法の詳細については、「*CA Single Sign-on Guide*」を参照してください。

8. Web コンソールのアドレスを確認します。ホスト名と異なっている場合は、[上記と同じ] チェック ボックスをオフにして、Web コンソール情報を入力します。

9. (オプション) データ ソース用の表示名を入力します。

デフォルトでは、データ ソースのタイプとホスト名を組み合わせ、データ ソースの名前が作成されます。ここで別の名前を入力することができます。

たとえば、*APM@xxx.x.x.xx* の代わりに、データ ソースを *APM_SantaFe* と命名できます。

10. データ ソースの登録が完了したら、[保存] をクリックします。

登録したデータ ソースが、NetQoS Performance Center の [データ ソースリスト] に表示されます。

HTTPS サポートの有効化(オプション)

SSL (Secure Sockets Layer) を使用して、セキュリティが強化された HTTPS プロトコルを有効にできます。SSL を CA APM と NetQoS Performance Center との間の通信に使用するには、以下の手順に従います。

- サーバ証明書を取得します。一部の管理者は、セキュリティをさらに強化するために、クライアント証明書を使用します。SSL、サーバ証明書、およびクライアント証明書を使用するために IIS の Web サイトを構成する手順は、このドキュメントの対象外です。ただし、以下の Microsoft の記事は、これらの IIS Web サイトのセキュリティ機能の使用方法について詳細に説明しています。

SSL and Certificates (IIS 6.0) :

<http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx?mfr=true>

- NetQoS Performance Center と NetQoS Performance Center Integration Pack のインストール可能コンポーネントとの間の HTTPS 通信を有効にするために、HTTPS 対応の CA APM [データ ソース](#) (P. 83) を構成します。
- [apm-capc-integration.properties](#) [ファイルを編集して](#) (P. 74)、Enterprise Manager と CAPC Integration Pack のインストール可能コンポーネントとの間の HTTPS 通信を有効にします。

apm-capc-integration.properties ファイルの編集

apm-capc-integration.properties ファイルを編集することにより、Enterprise Manager と CAPC Integration Pack のインストール可能コンポーネントとの間で HTTPS 通信を有効にできます。

次の手順に従ってください:

1. 以下の場所にある apm-capc-integration.properties ファイルをテキストエディタで開きます。
<INSTALLATION_HOME>%CAPCIntegrationPack%resources
2. プロパティ com.apm.npc.em.transport.protocol を探し、値 <https> を指定します。
3. プロパティ javax.net.ssl.keyStore を探し、値 <KEYSTORE LOCATION FOR SSL CONNECTION> を指定します。

4. プロパティ `javax.net.ssl.keyStorePassword` を探し、値 `<KEYSTORE PASSWORD FOR SSL CONNECTION>` を指定します。
5. プロパティ `javax.net.ssl.trustStore` を探し、値 `<TRUSTSTORE LOCATION>` を指定します。
6. プロパティ `javax.net.ssl.trustStorePassword` を探し、値 `<TRUSTSTORE PASSWORD>` を指定します。
プロパティが設定されます。

接続の確認

NetQoS Performance Center では、選択した期間に対してドリルダウン方法でアプリケーションヘルスおよびパフォーマンスステータスデータが表示されます。CA APM を NetQoS Performance Center にデータソースとして登録すると、[アプリケーションサマリ] レポートまたは [ビジネスサービスサマリ] レポートからアプリケーションデータにアクセスできます。これらのレポートから、インシデントおよび障害までドリルダウンできます。

事前設定済みのレポートのデータを探し、CA APM と NetQoS Performance Center の接続を確認します。

次の手順に従ってください：

1. NetQoS Performance Center にログオンします。
2. NetQoS Performance Center の [レポート] メニューから、以下の CA APM 関連のレポートが表示されることを確認します。
 - APM-- アプリケーションサマリ
 - APM-- ビジネスサービスサマリ
3. [アプリケーションサマリ] レポートでビジネスアプリケーションの稼働状況ステータスが表示されます。
4. [ビジネスサービスサマリ] レポートで選択したアプリケーションのビジネスサービスの稼働状況ステータスが表示されます。

第 4 章: シナリオの問題切り分け

このセクションには、以下のトピックが含まれています。

[CEM コンソールからアプリケーションおよびインフラストラクチャの問題を切り分ける方法 \(P. 87\)](#)

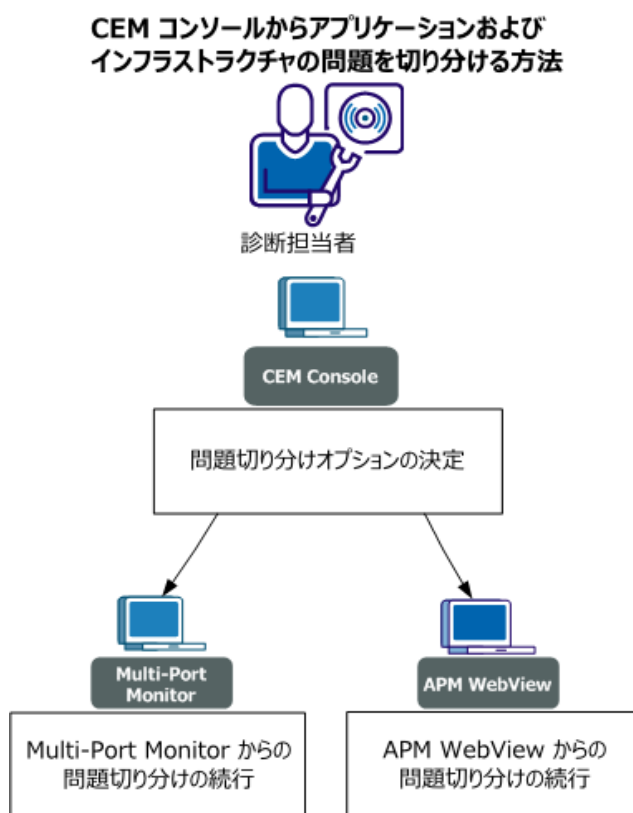
[APM WebView からアプリケーションおよびインフラストラクチャの問題を切り分ける方法 \(P. 94\)](#)

[NPC からアプリケーションの問題を切り分ける方法 \(P. 107\)](#)

CEM コンソールからアプリケーションおよびインフラストラクチャの問題を切り分ける方法

CEM コンソール上のネットワーク データは、監視対象のアプリケーションに関連する高度なネットワーク パフォーマンス情報を診断担当者に提供します。その情報を基に、切り分け対象の問題にネットワークの問題が関係しているかどうかを判断し、**Multi-Port Monitor** でセッションレベルのデータを掘り下げることができます。ネットワークが問題ではないことをメトリックが示している場合、**APM WebView** に接続してアプリケーションの調査および問題切り分けを行います。

以下の図は、考えられる問題切り分けシナリオを示しています。



診断担当者として、以下の手順を実行します。

1. [問題切り分けオプションを決定します \(P. 88\)](#)。
2. [Multi-Port Monitor から問題切り分けを続行します \(P. 93\)](#)。
3. [APM WebView から問題切り分けを続行します \(P. 94\)](#)。

問題切り分けオプションの決定

アプリケーションに関連するインフラストラクチャの問題が表示される場合は、いくつかの問題切り分けオプションを決定し、次の手順のガイドとして役立てます。

次の手順に従ってください：

1. CEM コンソールにログオンします。
2. [CEM] - [インシデント管理] - [障害] を選択します。

3. 以下のいずれかの操作を行います。
 1. リストから障害を選択します。
 2. 特定の障害を検索します。
4. 選択した障害に関連付けられたネットワークの稼働状況メトリックを確認します。

たとえば、高いネットワーク往復時間またはパケット損失が表示される場合は、**Multi-Port Monitor** に接続することを選択する方法があります。そこから、ネットワーク インフラストラクチャの詳細に調査できます。

ネットワーク稼働状況メトリックの詳細については、「[\[障害詳細\] ページ上のネットワーク メトリック \(P. 89\)](#)」を参照してください。

[障害詳細] ページ上のネットワーク メトリック

CEM が障害を識別すると、セッションレベルの TCP 情報について **Multi-Port Monitor** にクエリし、障害の詳細の一部として保存します。障害にドリルダウンすると、CEM コンソールでこの TCP 情報が利用可能になります。

各フィールドには、障害発生時間までの 15 分間における、Web サーバとクライアント IP との間でのアプリケーションのためのすべての TCP セッションの平均値が表示されます。[TCP 対話分析] フィールドのリンクを使用すると、個別の TCP セッションのメトリックを確認できます。

以下のネットワーク情報が [障害詳細] ページに表示されます。

NCT 計測値

接続時間の計測値。選択した時間間隔に発生した監視対象 TCP 接続の数。メトリックの測定値と使用率レベルを適切に示します。たとえば、計測値が大きい場合は、イベントがユーザに影響を及ぼしている可能性があります。

DTT

データ転送時間。サーバが応答を開始してからデータを送信し終えるまでの間の経過時間。応答のサイズ、使用可能な帯域幅、アプリケーションとネットワーク間のインタラクションなど、いくつかの要因がこの値に影響します。TCP ウィンドウに収まるデータよりも多い送信データがある場合、初期サーバ応答時間を除外し、NRTT のみを含みます。この値は、すべてのデータを配信するのに必要なネットワーク ラウンドトリップの数およびラウンドトリップあたりの遅延に関連しています。

ENRTT

有効なネットワーク ラウンドトリップ時間。NRTT および再送遅延(再送信がトランザクションに対して引き起こす遅延)を含んでいます。ユーザが実際に経験する遅延を反映しており、再送信が引き起こすパフォーマンス低下のインジケータとして機能します。

NCT

ネットワーク接続時間。クライアントがサーバ接続応答を確認するまでにかかった時間。一般的に、ネットワーク遅延は、接続時間の遅延を引き起こします。NCT は、キャリア遅延のベースラインおよび NRTT 値との比較対象として機能します。

NRTT

ネットワーク ラウンドトリップ時間。パケットがネットワーク上のサーバとクライアント間を移動するのにかかった時間(再送信による遅延を除く)。アプリケーションおよびサーバの処理時間はこの値から除外されます。この値は、NCT の値と比較すると役立ちます。

NRTT 計測値

ネットワーク往復時間計測値。選択した時間間隔中のネットワーク上のサーバとクライアントとの間の往復の数。メトリックの測定値と同様に、使用率レベルを適切に示します。たとえば、大きい値が計測されると、イベントが多くのユーザに影響を及ぼしている可能性があります。

再送

再送遅延。再送信が原因の **NRTT** の追加の遅延。再送信はデータの損失後に再送信されるパケットです。データは、各トランザクションの実際の再送信時間ではなく、すべての計測の平均として表されます。再送遅延によりクライアントの確認応答に遅延が生じると、**NRTT** の値は増加します。このメトリックでは、**TCP** 輻輳のため、損失が **DTT** に与える影響が明らかになりません。このメトリックは、クライアントからサーバにではなく、サーバからクライアントへのデータの損失のみを反映します。

SCT

サーバ接続時間。サーバがクライアントから **SYN** パケットを受信してからサーバが最初の **SYN/ACK** を送信するまでの時間。

TCP 接続を開くときには、3つのパケット (**SYN**、**SYN/ACK**、および **ACK**) が交換されます。**TCP** ヘッダには **SYN** (同期) および **ACK** (確認応答) ビットがあります。最初のパケットは **SYN** ビットセットを持っています。2番目のパケットは両方のビットセットを持っています。3番目のパケットは **ACK** ビットセットのみを持っています。この交換は、接続の初期シーケンス番号を確立します。

SCT および **NCT** は **Connection Setup Time** メトリックを含みます。詳細については、「**ADA Sessions reports**」を参照してください。

SRT

サーバ応答時間。サーバがクライアント要求に回答するのにかかった時間。サーバ速度、アプリケーション設計、および要求の量が **SRT** に影響します。

TCP バイト

バイト単位での **TCP** データ ボリューム。選択したホストまたはホストのペアによって選択した期間中に送受信された **TCP** バイトの総数。

TCP 受信バイト

バイト単位での **TCP** データ ボリューム。選択した期間中に選択したサーバがクライアントとの間で送受信したアプリケーションレイヤバイトの総数。

TCP バイト損失率

送受信された **TCP** バイトの割合として表されるデータの損失。

TCP バイト率

バイト単位での TCP データ ボリューム。選択した期間内のバイト/秒単位のデータ レート。

TCP 受信バイト率

ビット単位の TCP スループット。選択した期間中の選択したサーバおよびクライアントの間のデータ レート（ビット/秒（バイト/秒 x 8）単位）。

TCP 再送バイト率

データ合計に対する再送信されたデータの比率、監視対象ネットワークで失われたデータの割合、およびビット/秒での損失率。

TCP 対話分析

[Analysis] タブにある、Multi-Port Monitor の [TCP Conversation] レポートへのリンク。Multi-Port Monitor 上のクライアント ネットワーク情報は、CEM コンソールによって要求されたセッションのクライアント ネットワーク ID に対応します。[TCP Conversation] レポートの初期ビューは、トランザクション時間によって並べられます。このレポートから、[Server/Client Pair] ビューにアクセスして、指定したサーバと対話しているクライアント IP アドレスと同じサブネットに属するすべてのクライアントを確認できます。

パケット損失率

送受信された TCP パケットの割合として表されるデータの損失。

TCP パケット率

パケット単位の TCP スループット。選択した期間内のパケット/秒単位のデータ レート。ADA レポートは「データ レート」という用語を使用します。

TCP 受信パケット率

パケット単位の TCP スループット。選択した期間中の選択したサーバおよびクライアントの間のデータ レート（パケット/秒単位）。

TCP 再送パケット率

データ合計に対する再送信されたデータの比率、監視対象ネットワークで失われたデータの割合、およびパケット/秒での損失率。

TCP パケット

パケット単位での TCP データ ボリューム。選択したホスト（またはホストのペア）が選択した期間中に送受信した TCP パケットの総数。

TCP 再送バイト

データの損失が原因で再送信された TCP バイトの数。

TCP 再送パケット

データの損失が原因で再送信された TCP パケットの数。

トランザクション時間

クライアントが要求（パケット レベルまたはトランザクション レベル）を送信した時点からクライアントが応答で最後のパケットを受信した時点までの時間。

トランザクション計測時間

トランザクション計測時間。選択した間隔中に発生した、監視対象 TCP トランザクションの数。メトリックの測定値と使用率レベルを適切に示します。たとえば、計測値が大きい場合は、イベントが多くユーザに影響を及ぼしている可能性があります。

Multi-Port Monitor からの問題切り分けの続行

障害のネットワーク メトリックがネットワーク/サーバのパフォーマンス低下（高いネットワーク往復時間またはパケット損失など）を示している場合、1つのオプションとして、[TCP 対話分析] リンクを介して Multi-Port Monitor に接続する方法があります。Multi-Port Monitor から、インフラストラクチャをより詳細に調査できます。以下のいずれかを実行して Multi-Port Monitor にアクセスします。

次の手順に従ってください：

1. CEM の [障害詳細] ページから、[TCP 対話分析] フィールドに関連付けられたリンクを選択します。

このリンクを選択すると、Multi-Port Monitor の [TCP Conversation] レポートが表示されます。[TCP Conversation] レポートの初期ビューは、トランザクション時間によって並べられます。このレポートから、[Server/Client Pair] ビューにアクセスして、指定したサーバと対話しているクライアント IP アドレスと同じサブネットに属するすべてのクライアントを確認できます。

詳細については、「*Multi-Port Monitor ユーザガイド*」を参照してください。

次の手順に従ってください：

1. Multi-Port Monitor にログオンします。
2. [Analysis] タブを選択します。
3. 関連する [TCP Conversation] レポートに移動します。

詳細については、「*Multi-Port Monitor ユーザガイド*」を参照してください。

APM WebView からの問題切り分けの続行

障害のネットワーク メトリックがビジネスで想定される範囲内にある場合、1つのオプションとして、APM WebView からアプリケーションの問題切り分けを続行する方法があります。

次の手順に従ってください：

1. APM WebView にログオンします。
2. コンソールまたは Investigator を使用して問題を切り分けます。

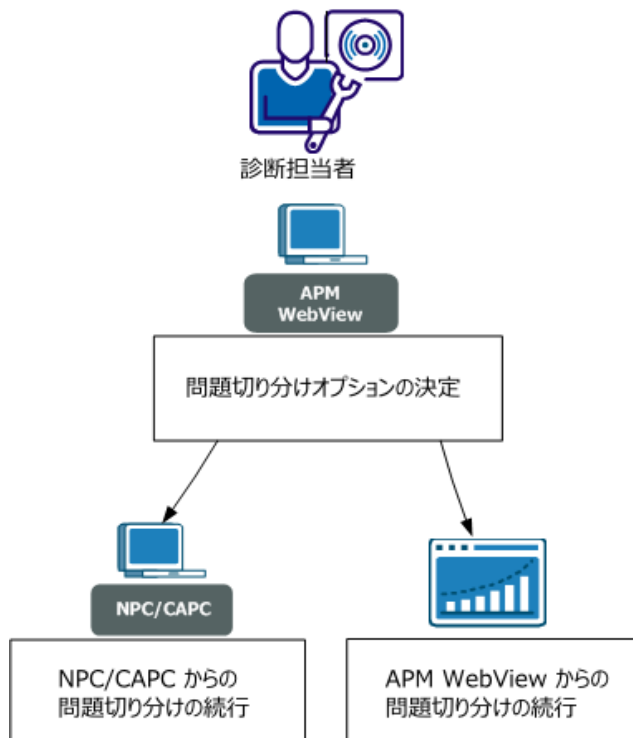
APM WebView からアプリケーションおよびインフラストラクチャの問題を切り分ける方法

APM WebView 上のインフラストラクチャ データを使用することによって、サポート エンジニアは以下を行うことができます。

- クライアント ネットワークおよびサーバの稼働状況を高レベルで確認し、インフラストラクチャの詳細な調査をすぐに行う必要があるかどうかを判断します。
- 必要がある場合は、NetQoS Performance Center (NPC) /CA Performance Center (CAPC) に直接接続して、特定のクライアント ネットワークまたはサーバを調査できます。
- インフラストラクチャ データではパフォーマンスが許容範囲にあることを示している場合、アプリケーションでパフォーマンスの低下が引き続き見られる場合、APM WebView を使用して、アプリケーションをより詳しく調査できます。

以下の図は、考えられる問題切り分けシナリオを示しています。

APM WebView からアプリケーションおよびインフラストラクチャの問題を切り分ける方法



診断担当者として、以下の手順を実行します。

1. [問題切り分けオプションを決定します \(P. 95\)](#)。
2. [NPC/CAPC から問題切り分けを続行します \(P. 104\)](#)。
3. [APM WebView から問題切り分けを続行します \(P. 103\)](#)。

問題切り分けオプションの決定

アプリケーションに関連するインフラストラクチャの問題が表示される場合は、いくつかの問題切り分けオプションを決定し、次の手順のガイドとして役立てます。

次の手順に従ってください：

1. APM WebView にログオンします。

2. 以下のいずれかのダッシュボードまたは概要ページに移動します。

1. [コンソール] の [ダッシュボード] ドロップダウンリストから、[ネットワーク ステータス情報] ダッシュボードを選択します。

クライアントサブネットおよびサーバの稼働状況ステータスを使用して、次の手順を決定します。たとえば、クリティカルなクライアントネットワークまたはサーバのパフォーマンスが正常で場合は、関連付けられている [詳細情報] ボタンを選択し、NetQoS Performance Center (NPC) /CA Performance Center (CAPC) のクライアントサブネット/サーバの概要レポートにアクセスします。

[詳細情報] ボタンは 1 回だけ構成する必要があります。APM Workstation からボタンを設定します。「[\[ネットワーク ステータス情報\] ダッシュボードで \[詳細情報\] を構成する \(P. 98\)](#)」を参照してください。

このダッシュボードの詳細については、「[\[ネットワーク ステータス情報\] ダッシュボード \(P. 97\)](#)」を参照してください。

2. Investigator、[メトリック ブラウザ] タブ、[Networks] ノードまたは [Server] ノード、[概要] タブから、監視対象のすべてのネットワーク/サーバの概要データに移動します。

各クライアントサブネット/サーバの稼働状況ステータスを使用して、次の手順を決定します。たとえば、クリティカルなクライアントサブネットまたはサーバに 2 の稼働状況ステータス (低下) がある場合、NPC/CAPC にログオンして、詳細情報を取得することができます。

稼働状況ステータスの詳細については、「[概要 - すべてのネットワーク/サーバ \(P. 100\)](#)」を参照してください。

- Investigator、[メトリック ブラウザ] タブ、[Networks] ノードまたは[Server]ノード、クライアントサブネットまたは特定のサーバ、[概要] タブから、監視対象の特定のクライアントサブネット/サーバの概要データに移動します。

稼働状況ステータス情報またはその他のメトリックを使用して、クライアントサブネットまたはサーバが追加の調査を必要とするかどうかを判断します。たとえば、問題があるアプリケーションをホストしているサーバが想定どおりに実行されていることをデータが示す場合、APM WebView を使用して、アプリケーションをより詳細に調査することができます。

デフォルトでは、以下のメトリックは無効です。

- データ転送時間
- ネットワーク ラウンドトリップ時間
- 再送遅延
- サーバ応答時間

これらのメトリックを有効にするには、ADA プロパティ ファイルで `com.wily.apm.adaconnector.ada_enhancedmetrics_enabled1=<true|false>` プロパティを使用します。このプロパティ ファイルの詳細については、「CA APM を Application Delivery Analysis に接続する方法」のシナリオを参照してください。

この概要データの詳細については、[「概要 - 各ネットワーク/サーバ \(P. 101\)」](#) を参照してください。

[ネットワーク ステータス情報]ダッシュボード

[ネットワーク ステータス情報] ダッシュボードは WebView コンソールから利用できます。このダッシュボードには、パフォーマンスが最も低い 10 のクライアントおよびサーバ、および関連する稼働状況ステータスが表示されます。クリティカルなクライアントネットワークまたはサーバのパフォーマンスが正常かどうかをひと目で確認できます。また、詳細情報を表示する NetQoS Performance Center (NPC) /CA Performance Center (CAPC) へのリンクも提供されています。APM Workstation から [詳細情報] ボタンを構成して、ダブルクリックすると、NPC/CAPC のクライアントサブネット/サーバ概要レポートが表示されます。各ボタンはそれぞれ 1 回だけ構成する必要があります。

Y 軸は、以下を表します。

CA Application Delivery Analysis によって計算された指定したタイム フレーム（デフォルト ビューはライブ データ用）の各クライアント サブネット/サーバの稼働状況ステータス。Enterprise Manager/MOM は CA Application Delivery Analysis 稼働状況ステータス データを取得し、Workstation 内の対応する数値を表示します。2 つのシステム間のデータ マッピングについては、以下のテーブルを参照してください。

CA Application Delivery Analysis ステータス	WebView ステータス値
利用不可	4
超過	3
低下	2
正常	1
未評価	0
なし	-1（対応するクライアント サブ ネット/サーバは Enterprise Manager にレポートしていません）

[詳細情報] ボタンを構成する方法の詳細については、次を参照してください

[\[ネットワーク ステータス情報\] ダッシュボードで \[詳細情報\] を構成する \(P. 98\)](#)

Application Delivery Analysis がネットワークおよびサーバの稼働状況を計算する方法の詳細については、次を参照してください

[ADA がネットワークおよびサーバの稼働状況を計算する方法 \(P. 106\)](#)

[ネットワーク ステータス情報] ダッシュボードで [詳細情報] を構成する

[詳細情報] ボタンをクリックすると、NetQoS Performance Center (NPC) /CA Performance Center (CAPC)（具体的には、[ネットワーク概要] と [サーバ概要] のレポート）に移動します。これらのレポートへのリンクについては、ボタンごとに 1 回限りの構成を行う必要があります。APM Workstation でボタンを設定します。

次の手順に従ってください:

1. APM Workstation にログオンします
2. Workstation の [Console] ウィンドウで、[ダッシュボード] - [ダッシュボードを編集] を選択します。
[ネットワーク ステータス情報] ダッシュボードの [エディタ] ビューが表示されます。
3. [詳細情報] ボタンを右クリックし、[グループ化解除] を選択します。
4. [詳細情報] テキストを右クリックし、[オブジェクトリンク...] を選択します。
[オブジェクトリンク] ウィンドウが表示されます。
5. [編集] をクリックします。
[オブジェクトリンクを編集] ウィンドウが表示されます。
6. [Web リンク] ラジオ ボタンが選択されていることを確認します。
7. [URL] テキストボックスで、<hostname> を NPC/CAPC サーバの名前に置換します。

注: URL はデフォルトで NPC にアクセスします。CAPC にアクセスするには、デフォルトを変更して、CAPC ポート番号 (通常は 8181) および新しいアドレスを含めます。

CAPC の追加のネットワーク情報にアクセスするには、以下を置換します。

`http://<hostname>/npc/default.aspx?pg=6001&mn=6001`

以下のテキストで置換します。

`http://<hostname>:CA Portal/pc/desktop/?pg=2000009&mn=3`

CAPC の追加のサーバ情報にアクセスするには、以下を置換します。

`http://<hostname>/npc/default.aspx?pg=7006&mn=6003`

以下のテキストで置換します。

`http://<hostname>:CA Portal/pc/desktop/?pg=2000010&mn=3`

8. [オブジェクトリンクを編集] ウィンドウおよび [オブジェクトリンク] ウィンドウの両方で [OK] をクリックします。
9. レポートの [エディタ] ビューで、[ファイル] - [保存] を選択します。

10. [エディタ] ビューを閉じます。

これ以降に [ネットワーク ステータス情報] ダッシュボードを使用すると、いずれのユーザの場合でも、NPC/CAPC の関連する概要レポートに直接アクセスできます。

概要 - すべてのネットワーク/サーバ

監視対象のすべてのネットワーク/サーバと関連付けられている概要データは、APM WebView、Investigator、[メトリック ブラウザ] タブ、[Networks] ノードまたは [Server] ノード、[概要] タブからアクセスできます。[概要] ページでは、以下の情報が、デフォルトではステータス メトリック値の降順に並べ替えられて表示されます。

ネットワーク/サーバ名

ツリー階層で表示されるネットワーク/サーバの名前。

ステータス

CA Application Delivery Analysis によって計算された指定したタイム フレーム (デフォルト ビューはライブ データ用) の各クライアントサブネット/サーバの稼働状況ステータス。Enterprise Manager/MOM は CA Application Delivery Analysis 稼働状況ステータス データを取得し、Workstation 内の対応する数値を表示します。2つのシステム間のデータ マッピングについては、以下のテーブルを参照してください。

CA Application Delivery Analysis ステータス	WebView ステータス値
利用不可	4
超過	3
低下	2
正常	1
未評価	0
なし	-1 (対応するクライアントサブネット/サーバは Enterprise Manager にレポートしていません)

デフォルトのしきい値が、2つのステータス メトリック値のために定義されます。警告は2のステータス値に相当します。危険は3のステータス値に相当します。メトリック値が警告しきい値を超えると、[ステータス] セルの背景色は黄色になります。危険しきい値を超えると、[ステータス] セルの背景色は赤色になります。これらのしきい値は、ADAExtensionforAPM.tv.xml ファイルを編集することによってカスタマイズできます。このファイルは、CA Application Delivery Analysis Extension for APM のインストーラプログラムの <EM_HOME>\ext\xmltv フォルダにあります。

Application Delivery Analysis がネットワークおよびサーバの稼働状況を計算する方法の詳細については、次を参照してください

[ADA がネットワークおよびサーバの稼働状況を計算する方法 \(P. 106\)](#)

概要 - 各ネットワーク/サーバ

[概要] ページには、クライアント サブネットまたは特定のサーバに関連するデータが表示されます。この情報には、APM WebView、Investigator、[メトリック ブラウザ] タブ、[Networks] ノードまたは [Server] ノード、クライアント サブネットまたは特定のサーバ、[概要] タブからアクセスできます。

デフォルトでは、以下のメトリックは無効です。

- データ転送時間
- ネットワーク ラウンドトリップ時間
- 再送遅延
- サーバ応答時間

これらのメトリックを有効にするには、ADA プロパティ ファイルで `com.wily.apm.adaconnector.ada_enhancedmetrics_enabled1=<true|false>` プロパティを使用します。このプロパティ ファイルの詳細については、「CA APM を Application Delivery Analysis に接続する方法」のシナリオを参照してください。

[概要] ページには、以下の情報が表示されます。

ステータス

CA Application Delivery Analysis によって計算された指定したタイムフレーム（デフォルト ビューはライブ データ用）の各クライアントサブネット/サーバの稼働状況ステータス。Enterprise Manager/MOM は CA Application Delivery Analysis 稼働状況ステータス データを取得し、Workstation 内の対応する数値を表示します。2つのシステム間のデータ マッピングについては、以下のテーブルを参照してください。

CA Application Delivery Analysis ステータス	WebView ステータス値
利用不可	4
超過	3
低下	2
正常	1
未評価	0
なし	-1（対応するクライアントサブネット/サーバは Enterprise Manager にレポートしていません）

データ転送時間 (ミリ秒)

データ転送時間は、最初の応答（サーバ応答時間の終了）からその要求で送信された最後のパケットまでに測定された、完全なアプリケーション応答を転送するのにかかった時間を測定します。応答時間は、アプリケーションの設計、サーバのパフォーマンス、またはネットワークによって影響を受けることがあります。TCP ウィンドウに収まるデータよりも多い送信データがある場合、初期サーバ応答時間を除外し、ネットワーク ラウンドトリップ時間のみを含みます。

ネットワーク往復時間 (ミリ秒)

ネットワーク ラウンドトリップ時間は、パケットがネットワーク上のサーバとクライアント間を移動するのにかかった時間を測定します（損失は除く）。アプリケーション、サーバ、およびクライアントの処理時間は除外されます。

再送遅延 (ミリ秒)

再送遅延は、元のパケット送信から最後の重複したパケット送信までの経過時間を測定します。再送遅延は、再送パケットだけではなく、計測値全体の平均としてレポートされます。10 個のパケットで構成される 1 セットのうちの 1 つのパケットが 300 ミリ秒の再送信時間を必要とする場合、再送遅延は 30 ミリ秒 (300 ミリ秒/10 個のパケット) としてレポートされます。

サーバ応答時間 (ミリ秒)

サーバ応答時間は、サーバが初期応答をクライアント要求に対して送信するのにかかった時間または初期のサーバ「待ち時間」を測定します。サーバ応答時間の増加は通常、CPU、メモリ、ディスク、I/O などのサーバリソースの不足、アプリケーションの不具合、または多層アプリケーション内の層のパフォーマンスの不足を示します。

Application Delivery Analysis がネットワークおよびサーバの稼働状況を計算する方法の詳細については、次を参照してください

[ADA がネットワークおよびサーバの稼働状況を計算する方法 \(P. 106\)](#)

APM WebView からの問題切り分けの続行

ステータスまたはメトリックのデータではネットワーク/サーバが正常であることを示していても、関連するアプリケーションでパフォーマンスの低下が引き続き見られる場合、1 つのオプションとして、APM WebView からアプリケーションの問題切り分けを続行する方法があります。

次の手順に従ってください：

1. APM WebView にログオンします。
コンソールまたは Investigator を使用して問題を切り分けます。

NPC/CAPC からの問題切り分けの続行

稼働状況ステータスまたはメトリックのデータがネットワーク/サーバのパフォーマンス低下を示している場合、1つのオプションとして、NetQoS Performance Center (NPC) /CA Performance Center (CAPC) を使用してインフラストラクチャの問題を調査する方法があります。以下のいずれかの手順を使用して NPC/CAPC にアクセスします。

次の手順に従ってください：

1. [ネットワーク ステータス情報] ダッシュボードから、関連する [詳細情報] ボタンを選択して NPC/CAPC のクライアントサブネット/サーバ概括レポートにアクセスします。
2. NPC/CAPC にログオンし、検索機能を使用してネットワーク/サーバの詳細情報を取得します。

NPC/CAPC の使用方法については、「*CA Performance Center 管理者およびユーザガイド*」を参照してください。

ネットワーク データの遅延

APM WebView 上のネットワーク データおよびサーバデータは、CA Application Delivery Analysis 管理コンソールのデータから約 5 分遅延しています。管理コンソールは、Multi-Port Monitor やシングルポート CA Application Delivery Analysis コレクタなどさまざまなコレクタに接続できます。収集されたデータを集約できるようにするために、CA Application Delivery Analysis 時間枠は、5 分間の長さで、7:00、7:05 のように 5 分の境界で終了します。CA Application Delivery Analysis 管理コンソールは、データベースを 5 分ごとに更新します。このため、CA Application Delivery Analysis 管理コンソールと CA APM との間の Web サービスブリッジは、5 分の時間範囲内で最大 5 分遅れてネットワーク稼働状況データを取得します。たとえば、現在の時刻が午後 6 時 22 分の場合、データ要求の対象は、午後 6 時 15 分から午後 6 時 20 分までの範囲になります。これらの 2 つの時刻の間の APM WebView 上のデータポイントでは、同じ結果が表示されます。

Web サービスからのサンプル ログ メッセージを以下に示します。

```
11/06/15 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADACConnector] Calling ADA
web service...
11/06/15 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADACConnector]
utcStartTime: 2011-06-15T18:15:00.000+0530
11/06/15 06:22:00.175 PM IST [INFO] [pool-1-thread-2] [ADACConnector] utcEndTime:
2011-06-15T18:20:00.000+0530
```

ヒント データ

[ネットワーク ステータス情報] ダッシュボードや [概要] ページなどの APM WebView グラフでは、ヒントが利用できます。グラフ上のデータポイントの上にマウスカーソルを置くと、より詳細な情報がヒントによって表示されます。以下のヒントフィールド値は、選択したタイムスライスの Y 軸で示される稼働状況ステータスのデータ値に対応します。

- メトリックの値
- メトリックの最小値と最大値

CA Application Delivery Analysis はデータを 5 分間隔で収集します。ただし、CA Application Delivery Analysis と CA APM との間の統合ブリッジは、15 秒の間隔で 1 つのデータポイントのみを送信します。そのため、Workstation は、CA Application Delivery Analysis から新しいデータを取得するまで、同じデータ値を表示します。さらに、選択したタイムスライスでレポートされたデータポイントの数が、常に 1 と表示されます。CA APM エージェントがデータを送信する場合、15 秒の間隔で複数のデータポイントを送信します。複数のデータが送信されることで、APM WebView は、これらのデータから平均値を算出し、アプリケーションメトリックの [値]、[最小値]、および [最大値] との差を表示することができます。

ADA がネットワークおよびサーバの稼働状況を計算する方法

CA Application Delivery Analysis は、TCP トランザクションを観測し、以下の計算を行って、ネットワーク/サーバの稼働状況を評価します。

- アプリケーションと通信する各クライアント ネットワークのネットワーク メトリック。ネットワーク メトリックの 5 分間平均がしきい値を超え、かつ CA Application Delivery Analysis がメトリックを最小回数のみ観測した場合、CA Application Delivery Analysis は、クライアント ネットワークの対応する 5 分間隔を「低下」または「超過」と評価し、ネットワーク インシデントを作成します。
- アプリケーションをホストする各サーバのサーバ メトリック。サーバ メトリックの 5 分間平均がしきい値を超え、かつ CA Application Delivery Analysis がメトリックを最小回数のみ観測した場合、CA Application Delivery Analysis は、サーバの対応する 5 分間隔を「低下」または「超過」と評価し、サーバ インシデントを作成します。

パフォーマンス データを評価するために、CA Application Delivery Analysis 管理コンソールは、2 営業日全体のデータを収集する必要があります。GMT の午前零時から次の午前零時までを 1 営業日として数えます。たとえば、CA Application Delivery Analysis 管理コンソールがサーバ ポートとクライアント ネットワークとの間の TCP セッションのデータ収集を米国標準時の月曜日午後 3 時 30 分に開始した場合、米国標準時の水曜日午後 7 時 (GMT の午前零時) まで、CA Application Delivery Analysis はそのネットワークのアプリケーションのパフォーマンスを評価できません。CA Application Delivery Analysis 管理コンソールが 2 営業日全体のデータを収集していない場合、CA Application Delivery Analysis はサーバ ポートとクライアント ネットワークとの間の TCP セッションを「未評価」と分類します。

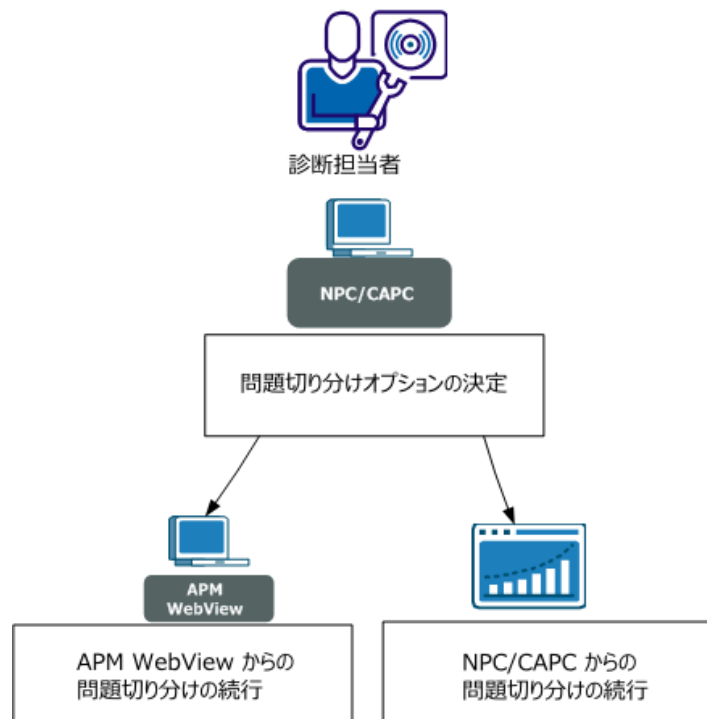
NPC からアプリケーションの問題を切り分ける方法

NetQoS Performance Center (NPC) /CA Performance Center (CAPC) 上のアプリケーションデータを使用することによって、診断担当者は NPC/CAPC UI から以下を行うことができます。

- アプリケーションおよびビジネス サービスの稼働状況ステータスを確認する。
- 障害およびより詳細なメトリックにドリルダウンする。
- アプリケーションメトリックがビジネスの想定されるパフォーマンスを示している場合は、障害に関連する Web サーバまたはクライアントを確認する。

以下の図では、診断担当者として NPC/CAPC からアプリケーションの問題を切り分ける方法のいくつかのオプションについて説明します。

NPC/CAPC からアプリケーションの問題を切り分ける方法



診断担当者として、以下の手順を実行します（手順 2 および手順 3 は、アプリケーションおよび問題切り分けを決定するメトリックに依存します）。

1. [問題切り分けオプションを決定します](#) (P. 108)。
2. [APM WebView から問題切り分けを続行します](#) (P. 121)。
3. [NPC/CAPC から問題切り分けを続行します](#) (P. 121)。

問題切り分けオプションの決定

NPC/CAPC UI でアプリケーションパフォーマンスの問題が表示される場合は、いくつかの問題切り分けオプションを決定し、次の手順のガイドとして役立てます。

次の手順に従ってください：

1. NPC/CAPC にログオンします。
2. [アプリケーションヘルス] メニューから、[APM - アプリケーションサマリ]または[APM - ビジネス サービス サマリ]のいずれかのダッシュボードを開きます。

[ステータス] フィールドの稼働状況ステータス情報を使用して、詳細に調査する必要があるアプリケーションまたはビジネス サービスを決定します。

このダッシュボードの詳細については、「[\[APM - アプリケーションサマリ\] ダッシュボード](#) (P. 111)」を参照してください。

このダッシュボードの詳細については、「[\[APM - ビジネス サービス サマリ\] ダッシュボード](#) (P. 112)」を参照してください。

3. [APM - アプリケーションサマリ] ダッシュボードおよび [APM - ビジネス サービス サマリ] ダッシュボードからドリルダウンして、[APM - ビジネス トランザクションサマリ] レポートを表示します。

[ビジネス トランザクションサマリ] レポートには、選択したビジネス サービスのビジネス トランザクションの稼働状況ステータスが表示されます。 [ステータス] フィールドの稼働状況ステータス情報を使用して、詳細に調査する必要があるビジネス トランザクションを決定します。

このレポートの詳細については、「[\[APM - ビジネス トランザクションサマリ\] レポート](#) (P. 113)」を参照してください。

4. [APM - ビジネストランザクションサマリ] レポートからドリルダウンして、[APM - メトリックおよびインシデントサマリ] レポートを表示します。

[APM - メトリックおよびインシデントサマリ] レポートには、選択したビジネストランザクションのビジネストランザクションコンポーネント (BTC) メトリックおよびカスタマエクスペリエンスメトリック (UI 上に RTTM として表示) が表示されます。

ビジネストランザクションメトリックコンポーネントおよびカスタマエクスペリエンスメトリック (RTTM) を使用して、続行する方法を決定します。たとえば、RTTM と BTC のメトリックが高い平均応答時間、間隔ごとのエラー数、およびストール数、またはそれらのいずれかを示している場合、Workstation にログオンしてアプリケーションを詳細に調査する方法があります。RTTM と BTC のメトリックがビジネスの想定される範囲内にある場合、障害に関連付けられているクライアント IP アドレスまたは Web サーバアドレスを選択する方法があります。このオプションでは、障害に関連するネットワークの問題を調査できます。

このレポートの詳細については、「[\[APM - メトリックおよびインシデントサマリ\] レポート \(P. 114\)](#)」を参照してください。

5. [APM - メトリックおよびインシデントサマリ] レポートからドリルダウンして、[APM - 障害サマリ] レポートを表示します。

[APM - 障害サマリ] レポートには、選択したインシデントの最後の 10 件のインシデントおよび関連する詳細情報が表示されます。

このレポートの詳細については、「[障害サマリ レポート \(P. 118\)](#)」を参照してください。

NPC/CAPC のアプリケーション データ表示方法

NetQoS Performance Center (NPC) /CA Performance Center (CAPC) 上のアプリケーションデータは、CA APM によって収集されたアプリケーションの稼働状況データを表します。Web サービス統合ブリッジを使用することによって、データが NPC/CAPC で利用できるようになります。CA APM は種々のアプリケーション コンポーネントで実行される個々のメソッドのパフォーマンスを測定することにより、アプリケーションの稼働状況を監視します。アプリケーション コンポーネントのバイト コードに挿入されたプローブは、エージェントにデータをレポートします。エージェントはその後、データを Enterprise Manager にレポートします。JMX および PMI のようなそのほかのサブシステムもまた、エージェントにより収集されるデータをレポートします。Enterprise Manager は、これらのデータを、アプリケーション サブシステムの多くのポイントで測定されたアプリケーション パフォーマンスを表すメトリックに、コンパイルします。CA APM は、アプリケーションに関連する観測されたトランザクションに基づいて、アプリケーション、ビジネス サービス、および ビジネス トランザクションを関連付けます。

NPC/CAPC では、選択した期間に対してドリルダウン方式でアプリケーション稼働状況およびパフォーマンス ステータス データが表示されます。CA APM を NPC/CAPC にデータ ソースとして登録すると、[アプリケーション サマリ] レポートまたは [ビジネス サービス サマリ] レポートからアプリケーションデータにアクセスできます。これらのレポートから、障害までドリルダウンできます。

アプリケーションの稼働状況およびパフォーマンスのステータス データは、以下のカテゴリに分類されます。

アプリケーション

CA APM によって監視されるアプリケーションの稼働状況ステータスが示されます。アプリケーションを選択すると、監視されているビジネス サービスが表示されます。

ビジネス サービス

選択したアプリケーションのビジネス サービスの稼働状況ステータスが示されます。ビジネス サービスを選択すると、CA APM によって監視されているビジネス トランザクションが表示されます。

ビジネストランザクション

選択したビジネス サービスのビジネス トランザクションの稼働状況ステータスが示されます。 **BusinessTransaction** を選択すると、カスタマエクスペリエンス メトリック (UI 上に RTTM として表示されます)、および **BusinessTransaction** コンポーネント (BTC) のメトリックおよびインシデントが表示されます。

インシデント

トランザクション タイプおよび障害タイプに基づいて関連付けされる障害のグループが示されます。 インシデントを選択すると、最新の N 個 (N の最大値 = 10) の障害が表示されます。

障害

各障害に固有の情報が表示されます。 各障害に関連する Web サーバ IP アドレスまたはクライアント IP アドレスを選択すると、それぞれのサーバアドレスまたはクライアント アドレスの検索結果ページが表示されます。

注: NetQoS Performance Center/CA Performance Center およびその UI コンポーネントについては、「*CA CA Performance Center 管理者およびユーザガイド*」を参照してください。

[APM - アプリケーション サマリ]ダッシュボード

[APM - アプリケーション サマリ] ダッシュボード ページには、ビジネス アプリケーションの稼働状況ステータスが表示されます。 このダッシュボードには、[アプリケーションヘルス] メニューからアクセスします。

CA APM は、Java、J2EE、および .NET のアプリケーションのパフォーマンスおよび稼働状況を監視します。 フロントエンドは、アプリケーションとして参照されます。

ビジネス アプリケーションは、ビジネス サービスを自動化するソフトウェアプログラムです。 CA APM は、Web アプリケーションによって生成される Web トランザクションを監視します。 ビジネス アプリケーションはトランザクション階層の一部です。

このダッシュボードの [アプリケーション ステータス] ビューには、以下の情報が表示されます。

アプリケーション

CA APM の監視対象アプリケーションが表示されます。このレポートには、定義済みのビジネス トランザクション コンポーネントを持つアプリケーションのみが表示されます。アプリケーションを選択すると、関連付けられているビジネス サービスを確認できます。

ステータス

指定した時間範囲でのアプリケーションの稼働状況が表示されます。この情報を使用することによって、詳細に調査する必要があるアプリケーションを決定できます。色の意味は、以下のとおりです。

- 白 - Enterprise Manager が応答していないため、データはありません (メトリック値はありません)
- 灰色 - データはありません (メトリック値 : 0)
- 緑 - 適正 (メトリック値 : 1)
- 黄 - 警告 (メトリック値 : 2)
- 赤 - 危険 (メトリック値 : 3)

APM - ビジネス サービス サマリ

[APM - ビジネス サービス サマリ] ダッシュボード ページには、選択したアプリケーションのビジネス サービスの稼働状況ステータスが表示されます。このダッシュボードにアクセスするには、アプリケーションからドリルダウンするか、[アプリケーションヘルス] メニューから直接移動します。

CA APM のビジネス サービスは、ビジネス トランザクションのグループです。測定は、トランザクション階層内のこのレベルに集約されます。

このダッシュボードの [ビジネス サービス ステータス] ビューには、以下の情報が表示されます。

ビジネス サービス

選択したアプリケーションのビジネス サービスがリスト表示されます。ビジネス サービスを選択すると、関連するビジネス トランザクションを確認できます。

ステータス

指定した時間範囲でのビジネス サービスの稼働状況が表示されます。この情報を使用することによって、詳細に調査する必要があるビジネス サービスを決定できます。色の意味は、以下のとおりです。

- 白 - Enterprise Manager が応答していないため、データはありません (メトリック値はありません)
- 灰色 - データはありません (メトリック値: 0)
- 緑 - 適正 (メトリック値: 1)
- 黄 - 警告 (メトリック値: 2)
- 赤 - 危険 (メトリック値: 3)

APM - ビジネストランザクション サマリ

[ビジネス トランザクション サマリ] レポートには、選択したビジネス サービスのビジネストランザクションの稼働状況ステータスが表示されます。このレポートを表示するには、[APM - アプリケーション サマリ] または [APM - ビジネス サービス サマリ] からドリルダウンします。

ビジネストランザクションという用語は、バックトゥバックの順序でコンピュータによって生成されたトランザクションを示します。トランザクションに異なるクライアント動作 (待ち時間) を追加できるユーザが生成したトランザクションを含めることはできません。ビジネストランザクションは、1つの識別トランザクションと任意の順序で実行される関連する他の複数のトランザクションから構成されます。トランザクションは、「含める」または「キャッシュ可能」、またはその両方として指定することができます。ビジネストランザクションは CEM コンソールで定義されています。

注: ビジネストランザクションを定義および作成する方法の詳細については、「CA APM トランザクション定義ガイド」を参照してください。

このレポートの [ビジネス トランザクション ステータス] ビューには、以下の情報が表示されます。

ビジネス トランザクション

選択したサービスのビジネス トランザクションがリスト表示されます。ビジネス トランザクションを選択すると、関連するカスタマ エクスペリエンス メトリック (UI 上に RTTM として表示されます) およびビジネス トランザクション コンポーネント (BTC) のメトリックおよびインシデントが表示されます。

ステータス

指定した時間範囲でのビジネス トランザクションの稼働状況が表示されます。この情報を使用することによって、詳細に調査する必要があるビジネス トランザクションを決定できます。色の意味は、以下のとおりです。

- 白 - Enterprise Manager が応答していないため、データはありません (メトリック値はありません)
- 灰色 - データはありません (メトリック値 : 0)
- 緑 - 適正 (メトリック値 : 1)
- 黄 - 警告 (メトリック値 : 2)
- 赤 - 危険 (メトリック値 : 3)

APM - メトリックおよびインシデント サマリ

[APM - メトリックおよびインシデント サマリ] レポートには、選択したビジネス トランザクションのビジネス トランザクション コンポーネントメトリックおよびカスタマ エクスペリエンス メトリック (UI 上に RTTM として表示) が表示されます。CA APM エージェントは、ビジネス トランザクションごとにビジネス トランザクション コンポーネントメトリックをレポートします。これらのメトリックは Blame メトリックと呼ばれることがあります。TIM は、ビジネス トランザクションごとにカスタマ エクスペリエンス メトリックを収集して、Enterprise Manager に送信します。

詳細については、「[ビジネス トランザクション コンポーネントメトリック \(P. 115\)](#)」を参照してください。

詳細については、「[カスタマ エクスペリエンス メトリック \(P. 117\)](#)」を参照してください。

ビジネストランザクション コンポーネント メトリック

CA APM エージェントは、ビジネストランザクションごとに 5 つのビジネストランザクション コンポーネント メトリックをレポートします。これら 5 つのメトリックは、**BLAME** メトリックと呼ばれることがあります。BTC ビューには、以下のメトリックが表示されます。

Average Response Time (ms)

応答時間は要求が完了するまでの時間です。この時間は、アプリケーション応答速度の基本的な測定値を示します。そのため、

- 応答時間が短いことは理想的です。
- 応答時間が長いと問題があることを示唆します。

Average Response Time（平均応答時間）メトリックは、間隔中に完了するすべての要求の応答時間の平均を示します。

注: **Average Response Time** のカウントは、**Responses Per Interval** の値と同じです。

Responses Per Interval

Responses Per Interval（間隔ごとの応答数）メトリックには、その間隔中に完了した呼び出しの数が反映されます。データ処理量の測定値であるため、アプリケーションのパフォーマンスを示します。一般的に、

- 数字が大きい方が理想的で、
- 数字が小さい方が望ましくありません。
- 応答の予測されなかった急上昇は、外部システムの過剰使用を示します。Web サイトへのサービス妨害攻撃などです。

Concurrent Invocations

呼び出しは、アプリケーションおよびそのさまざまな部分によって処理される要求です。**Concurrent Invocations**（同時進行中の呼び出し）は、一定の時間に処理される要求の数です。

CA APM は、特定の間隔の終了時にまだ処理中であった要求の数を数えて、**Concurrent Invocations** メトリックを計算します。

- **Concurrent Invocations** 値は低い方が理想的です。
- 同時進行中の呼び出し値が高い場合は、問題があることを示唆しています。

Errors Per Interval

エラー数は、JVM および HTTP エラー コードでレポートされる例外の数です。エラーの例には、以下のものが挙げられます。

- HTTP サーバによりレポートされた **404 Page Not Found** ステータス
- SQL 例外
- Java 例外

エラー数は少ない方が理想的です。

Stall Count

ストールした要求とは、指定した時間しきい値内に完了しなかった要求です。要求がストールとしてカウントされる場合、要求がハングしたり、完了しないことを意味するものではなく、その実行がストールしきい値を超えたことを示します。

- カウントが小さい方が理想的です。
- カウントが高い方が望ましくありません。

デフォルトのストールしきい値は、**30 秒**です。

ストールイベントの情報は、トランザクション イベント データベースに格納されます。

カスタマ エクスペリエンス メトリック

TIM は、ビジネス トランザクションごとにカスタマ エクスペリエンス メトリック (UI 上に RTTM として表示されます) を収集して、Enterprise Manager に送信します。複数の TIM が同じビジネス トランザクションを監視している場合、これらのメトリックは Enterprise Manager 上で集約されます。

カスタマ エクスペリエンスには以下のメトリックが含まれます。

Average Response Time (ms)

各間隔について、ビジネス トランザクションの実行に要した平均時間 (ミリ秒) です。

Total Defects Per Interval

TIM 全体から集約されたビジネス トランザクションのすべての障害タイプの障害数です。

Total Transactions Per Interval

TIM 全体から集約されたビジネス トランザクションの間隔ごとの合計 トランザクション数です。

障害タイプ

カスタマ エクスペリエンス メトリックは (製品 UI で RTTM と表示されることもあります)、いくつかの障害タイプに分類されます。このメトリックは、これらのタイプのいずれかの下に表示されます。これらはユーザがカスタマイズする前のデフォルトの障害名です。

障害メトリックはビジネス トランザクションと関連付けられた各障害タイプについて収集されます。これには、例えば「<BT 名> の低速トランザクション」というようなユーザが命名したトランザクションが含まれます。

各障害タイプのデフォルト値を以下に示します。s は秒を表しています。

低速

トランザクション時間 > 5.000s

高速

トランザクション時間 < 0.005s

高スループット

スループット > 100.0KB/s

低スループット

スループット < 1.0KB/s

大サイズ

トランザクション サイズ > 100.0KB

小サイズ

トランザクション サイズ < .0.1KB

トランザクションなし

コンポーネント タイムアウト = 10.000s

カスタマ エクスペリエンス メトリックの計算方法

カスタマ エクスペリエンス トランザクション メトリックは、Enterprise Manager 上の Javascript 計算機を使用して計算されます。

注: 集約メトリックは、実行中の TIM コレクション サービスおよび BTstats プロセッサがあるコレクタ Enterprise Manager 上でのみ計算されます。これらの計算は MOM Enterprise Manager 上では実行されません。

障害サマリ レポート

[APM - 障害サマリ] レポートには、選択したインシデントの最後の 10 件のインシデントおよび関連する詳細情報が表示されます。

障害とは、トランザクションが顧客の期待を満たせなかった場合や、トランザクションの規格に適合できなかった場合を表します。障害は、動作障害と応答障害に分類されます。トランザクションが複数の規格に適合しない場合、複数の障害が生成されます（「低速トランザクション」および「コンポーネントなし」など）。

[障害サマリ] レポートには、以下の情報が表示されます。

障害 ID

各障害を識別する番号

障害名

障害に関連付けられている名前

ビジネス サービス

障害に関連付けられているビジネス サービス

ビジネストランザクション

障害に関連付けられているビジネス トランザクション

日付と時刻

障害が発生した日時

値

ベースライン値。この値以上の場合、CA APM はトランザクションを障害と見なします。以下の CEM コンソールページから、障害をトリガするこのベースラインスループット値を設定します。

[管理]、[ビジネス サービス]、(ビジネス サービス)、(ビジネストランザクション)、[ビジネストランザクション規格]

ビジネス インパクト

ビジネス インパクトは、障害またはインシデントがビジネスにもたらす影響を測定したものです。

CEM コンソールは、ビジネストランザクション、障害タイプ、およびユーザと関連付けられた障害に基づいて、受信する各障害にビジネスインパクトを割り当てます。

障害のビジネス インパクトは以下のように計算されます。

ビジネストランザクションのウェイト * 障害タイプのウェイト * ユーザのウェイト

たとえば、以下のインパクト レベルが各値に割り当てられている場合

ビジネストランザクションの加重 = 4

障害タイプの加重 = 4

ユーザの加重 = 4

$4 * 4 * 4 = 64$

ビジネス インパクトは 64 です。

インパクトレベル	割り当てられるウェイト
最小	1
最低	2

インパクトレベル	割り当てられるウェイト
低	3
中	4
高	5
クリティカル	6
すぐにトリガ	7

ログイン名

障害に関連付けられているエンド ユーザのログイン名

ユーザ グループ

障害の影響を受けたユーザ グループの名前

CA APM では、ユーザ グループにより、（監視対象）ユーザのコレクション用の設定を行うことができます。個別のユーザごとに設定を行う必要はありません。ユーザ グループは、問題が発生している可能性がある（監視対象）ユーザのグループを簡単に識別できるように定義できます。ユーザは1つのユーザ グループのみに属します。

クライアント IP アドレス

障害によって影響を受けたエンド ユーザのクライアント IP アドレス

クライアントのより詳細な情報にアクセスするにはクリックします。このクライアント IP アドレスに関する、NPC/CAPC の検索結果ページが表示されます。

Web サーバ IP アドレス

障害に関連する、要求元 Web サーバの IP アドレス

Web サーバに関するより多くの詳細情報にアクセスするにはクリックします。この Web サーバ IP アドレスに関する、NPC/CAPC の検索結果ページが表示されます。

Web サーバ MAC アドレス

障害に関連する、サーバ用のネットワーク カードのハードウェア アドレス

APM WebView からの問題切り分けの続行

NPC/CAPC の RTTM と BTC のメトリックが高い平均応答時間、間隔ごとのエラー数、またはストール数をビジネスに対して示している場合、1つのオプションとして、APM WebView からの問題切り分けを続行する方法があります。APM WebView を使用して、アプリケーションに関する詳細を取得します。

次の手順に従ってください：

1. APM WebView にログオンします。
コンソールまたは Investigator を使用して問題を切り分けます。

NPC/CAPC からの問題切り分けの続行

NetQoS Performance Center (NPC) /CA Performance Center (CAPC) の RTTM と BTC のメトリックがビジネスの想定される範囲内にある場合（しかし、[アプリケーション] ダッシュボードまたは [ビジネス サービス] ダッシュボードにパフォーマンスの問題が引き続き示されている場合）、1つのオプションとして、障害に関連するネットワークの問題を調査する方法があります。NPC/CAPC を使用してこの調査を実行できます。

次の手順に従ってください：

1. [APM - 障害サマリ] レポートから、以下のいずれかを実行します。
 1. [クライアント IP アドレス] リンクを選択して NPC/CAPC に接続し、クライアントに関する詳細情報を取得します。
 2. [Web サーバ IP アドレス] リンクを選択して NPC/CAPC に接続し、Web サーバに関する詳細情報を取得します。
2. 詳細なクライアント情報または Web サーバ情報を使用して、アプリケーションに関連するネットワークの問題を切り分けます。

ネットワーク メトリックの詳細については、「*CA Performance Center 管理者およびユーザガイド*」を参照してください。

付録 A: トラブルシューティング

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 APM アプリケーション データが NPC 上で利用できない \(P. 123\)](#)

[CA APM アプリケーション データが CAPC 上で利用できない \(P. 124\)](#)

[TIM の動作停止 \(P. 125\)](#)

[インフラストラクチャ データが CEM コンソールで利用できない \(P. 128\)](#)

[Workstation 上の \[詳細情報\] ボタンが機能しない \(P. 128\)](#)

CA APM アプリケーション データが NPC 上で利用できない

症状:

アプリケーション関連のレポート（[ビジネス サービス サマリ] または [アプリケーション サマリ]）を選択しましたが、NetQoS Performance Center に CA APM データが表示されません。

解決方法:

以下を確認してください。

- [CA Performance Center Integration Pack \(P. 79\)](#) が Enterprise Manager または MOM にインストールされている。
- [APM-CAPC サービスを開始 \(P. 68\)](#) している。
- [NetQoS Performance Center データベースが更新 \(P. 82\)](#) されている。
- NetQoS Performance Center に [データ ソースとして APM を登録 \(P. 83\)](#) している。
- [アプリケーション問題切り分けマップアラートを作成 \(P. 81\)](#) している。

データソースを登録する手順の詳細については、次を参照してください

[CA APM をデータ ソースとして登録](#) (P. 83)

アプリケーション マップ アラートを構成する方法の詳細については、次を参照してください

[APM WebView でのアラートの設定](#) (P. 81)

CA APM アプリケーション データが CAPC 上で利用できない

症状:

アプリケーション関連のレポート（[ビジネス サービス サマリ] または [アプリケーション サマリ]）を選択しましたが、CA Performance Center に CA APM データが表示されません。

解決方法:

以下を確認してください。

- [CA Performance Center Integration Pack](#) (P. 67) が Enterprise Manager または MOM にインストールされている。
- [APM-CAPC サービスを開始](#) (P. 68) している。
- CA Performance Center に [APM ビューをインポート](#) (P. 71) している。
- CA Performance Center に [データ ソースとして APM を登録](#) (P. 71) している。
- CA Performance Center の [アプリケーションヘルス] メニューに [APM ダッシュボードを追加](#) (P. 73) している。
- [アプリケーション問題切り分けマップアラートを作成](#) (P. 69) している。

データソースを登録する手順の詳細については、次を参照してください

[CA APM をデータ ソースとして登録 \(P. 83\)](#)

アプリケーション マップ アラートを構成する方法の詳細については、次を参照してください

[APM WebView でのアラートの設定 \(P. 81\)](#)

TIM の動作停止

症状:

Multi-Port Monitor にインストールされた TIM が正しく機能しなくなりました。たとえば、統計の記録および生成を停止しています。さらに、TIM ログに「skip old packets」というメッセージが表示されています。

解決方法:

TIM を Multi-Port Monitor にインストールすると、Multi-Port Monitor の NapaTech カードは、そのカードの時間を使用して、パケットの到着時間をマークします。Multi-Port Monitor 上のシステム時間と NapaTech カードの時間が大幅に異なる場合、TIM は正常に動作を停止できます。

以下の 2 つの使用例があります。どちらの使用例を状況に適用するかを決定します。

1. TIM 処理は、Multi-Port Monitor によって生成されるパケット ファイルより遅れることがあります。たとえば、TIM が停止して再起動された場合、または TIM が処理できるよりも速いタイミングで Multi-Port Monitor がパケット ファイルを生成している場合です。以下の手順に従うことで、TIM の遅延時間を確認します。
 - a. NapaTech カードの時間が、Multi-Port Monitor 上のユーザのシステム時間と同期することを確認します。
 - b. Multi-Port Monitor のシステム ステータス ページを確認し、警告メッセージが表示されていないことを確認します。

この 2 つのシナリオを確認済みの場合、TIM には問題はありません。TIM は、15 分（このデフォルト値は変更可能）を越える時間を経過したプロセス パケット ファイルを処理しません。これらの古いパケット ファイルをスキップした後、TIM は通常の処理を再開します。TIM には、Multi-Port Monitor の生成ファイルに追いつく時間が必要なだけです。

2. NapaTech カードの時間を、Multi-Port Monitor 上のシステム時間と比較します。NapaTech カードの時間を参照するには、端末から以下のコマンドを使用します。

```
/opt/napatech/bin/TimeConfig -cmd time_get
```

Multi-Port Monitor のシステム時間を確認するには、端末から以下のコマンドを使用します。

```
date
```

2 つの時間が異なっていて、Multi-Port Monitor のシステム ステータス ページに警告メッセージが表示されている場合は、NapaTech カードと NTP（Network Time Protocol）サーバの時間を確認します。

以下の Web サイトでタイムゾーンを選択して、NTP 時間を取得します。
<http://www.time.gov/>

以下のシナリオを検討し、状況へ適用するものを決定します。

シナリオ 1

状況

- NapaTech カードの時間が、NTP 時間と大幅に異なります（15 分以上の差）。
- Multi-Port Monitor 上のシステム時間が、NTP 時間とほとんど変わりません（5 秒未満の差）。

アクション

- 以下コマンドを実行することで、NapaTech の時間をシステム クロックと同期させます。

```
/opt/NetQoS/scripts/syncNapatechClock
```
- NapaTech の時間と Multi-Port Monitor 上のシステム時間との差が 5 分未満の場合は、NapaTech ドライバと OS と同期を取ることで、徐々に NapaTech クロックが調節されます。NapaTech の時間と Multi-Port Monitor 上のシステム時間との差が 5 分以上の場合は、NapaTech の時間はすぐに Multi-Port Monitor 上のシステム時間と同期を取ろうとします。

シナリオ 2

状況

- NapaTech カードの時間が、NTP 時間とほとんど変わりません。
- Multi-Port Monitor 上のシステム時間および CEM コンソール時間が、NTP 時間と大幅に異なります。

アクション

- CEM コンソール時間を NTP 時間と同期するように調節します。
- 待機して、Multi-Port Monitor 上のシステム時間が CEM によって設定され、NTP 時間とも同期していることを確認します。
- Multi-Port Monitor 上の ntpd プロセスが実行されていることを確認します。実行されていない場合は開始します。

Multi-Port Monitor 上のシステム時間と NTP 時間との差が 1000 秒を越えているとき、ntpd プロセスは自動的に停止できます。

シナリオ 3

状況

- NapaTech カードの時間が、NTP 時間と大幅に異なります。
- Multi-Port Monitor 上のシステム時間および CEM コンソール時間も、NTP 時間と大幅に異なります。

アクション

- CEM コンソール時間を NTP 時間と同期するように調節します。
- 待機して、Multi-Port Monitor 上のシステム時間が CEM によって設定され、NTP 時間とも同期していることを確認します。
- Multi-Port Monitor 上の ntpd プロセスが実行されていることを確認します。実行されていない場合は開始します。
- 以下コマンドを実行することで、NapaTech の時間をシステムクロックと同期させます。

```
/opt/NetQoS/scripts/syncNapatechClock
```

インフラストラクチャ データが CEM コンソールで利用できない

症状:

障害の詳細を調査していますが、存在することが想定される関連するネットワーク インフラストラクチャ情報が表示されません。

解決方法:

以下の構成が正しく行われていることを確認してください。

- TCP データに対する Multi-Port Monitor への Web サービス呼び出しを開始するために、CEM コンソール UI（[監視] - [Multi-Port Monitor マシン]）で [Multi-Port Monitor 有効] チェック ボックスがオンになっている。
- 障害が 5 分以上前に生成されている。ネットワーク稼働状況データが Multi-Port Monitor データベースで利用可能になるまで最大 5 分の遅延が出る場合があります。障害が 5 分以内に生成されている場合は、数分待ってからブラウザ ページを更新します。

Workstation 上の [詳細情報] ボタンが機能しない

症状:

CA APM Workstation/WebView の [ネットワーク ステータス情報] ダッシュボードから NetQoS Performance Center (NPC) /CA Performance Center (CAPC) に直接接続できません。このダッシュボード上の [詳細情報] ボタンが機能しません。

解決方法:

[詳細情報] ボタンをクリックすると、NPC/CAPC（具体的には、[ネットワーク概要] と [サーバ概要] のレポート）に移動します。これらのレポートへのリンクについては、ボタンごとに 1 回限りの構成を行う必要があります。「[\[ネットワーク ステータス情報\] ダッシュボードで \[詳細情報\] を構成する \(P. 98\)](#)」を参照してください。

[詳細情報] ボタンを構成する手順については、次を参照してください

[\[ネットワーク ステータス情報\] ダッシュボードで \[詳細情報\] を構成する \(P. 98\)](#)