

CA Application Performance Management

設定および管理ガイド

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

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

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

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: 「CA APM 設定および管理ガイド」の概要 | 25 |
| APM の概要 | 25 |
| 第 2 章: Enterprise Manager の起動と停止 | 27 |
| Windows での Enterprise Manager の起動 | 27 |
| Enterprise Manager の Windows サービスとしての実行 | 28 |
| Windows での Enterprise Manager の手動による起動 | 30 |
| UNIX での Enterprise Manager の起動 | 31 |
| UNIX での Enterprise Manager の手動による起動 | 31 |
| UNIX での Enterprise Manager コントロールスクリプトの実行 | 31 |
| UNIX での nohup モードでの Enterprise Manager の実行 | 32 |
| 別の JVM を使用するための Enterprise Manager の設定 | 33 |
| Enterprise Manager ログファイルについて | 34 |
| 日付またはサイズによる Enterprise Manager ログのロール | 34 |
| Enterprise Manager config ディレクトリの構成 | 36 |
| Enterprise Manager の停止 | 38 |
| ターミナル ウィンドウからの Enterprise Manager の停止 | 38 |
| Workstation からの Enterprise Manager の停止 | 38 |
| Enterprise Manager の自動シャットダウン | 38 |
| 予期しないシャットダウン後の再起動 | 39 |
| Enterprise Manager のシェルおよびターミナル ウィンドウのコマンド | 41 |
| 第 3 章: Enterprise Manager の通信の構成 | 43 |
| デフォルトの Enterprise Manager の通信チャンネル | 43 |
| 使用中のポートへの通信チャンネルの再バインド | 44 |
| SSL の構成 | 45 |
| ファイアウォールを越えた Enterprise Manager との接続 | 48 |
| Enterprise Manager Web サーバの HTTPS 用の設定 | 48 |
| HTTPS の動作の仕組みの理解 | 49 |
| デフォルトの Jetty 構成ファイル | 49 |
| 第 4 章: Enterprise Manager データベースの構成 | 55 |
| APM データベースの管理 | 55 |

| | |
|--|----|
| データベースのバックアップまたはリストア | 56 |
| データベース構成のエクスポートまたはインポート | 63 |
| 別のオペレーティング システムへの APM データベースの移動 | 71 |
| PostgreSQL データベースから Oracle データベースへのデータの移動 | 72 |
| データベースのトラブルシューティング | 74 |
| SmartStor によるデータ保存の設定 | 75 |
| SmartStor 層の動作の詳細 | 76 |
| メタデータの自動削除 | 77 |
| SmartStor のシステム要件の判断 | 77 |
| SmartStor のデータ層の値の指定 | 78 |
| トランザクション イベント データベースの場所および保存期間 | 79 |
| ベースライン ストレージの場所の設定 | 79 |
| SmartStor、ベースライン、およびトランザクション イベント データのバックアップ | 80 |
| クエリ専用の複製クラスタの作成 | 81 |
| SmartStor ツールを使用した SmartStor データのチューニング | 82 |
| SmartStor ツール コマンド | 83 |
| merge | 84 |
| remove_metrics | 84 |
| remove_agents | 86 |
| keep_agents | 87 |
| prune | 87 |
| test_regex | 89 |
| list_agents | 90 |
| SmartStor メタデータの廃棄 | 90 |
| SmartStor データおよびメタデータの削除 | 92 |
| 例：test_regex コマンドを使用した SmartStor データ問題の検出 | 95 |
| 8.x データから 9.x へのアップグレード | 97 |
| アップグレード コマンドを使用した 8.x データのアップグレード | 97 |

第 5 章: 仮想エージェントを使用したメトリックの集約 99

| | |
|-------------------|-----|
| 仮想エージェントの理解 | 99 |
| 仮想エージェントの要件 | 100 |
| 仮想エージェントの設定 | 101 |

第 6 章: Enterprise Manager とクラスタの設定 105

| | |
|--------------------------------------|-----|
| スタンドアロン Enterprise Manager の設定 | 105 |
| Enterprise Manager クラスタの理解 | 105 |
| Enterprise Manager をクラスタ化すべき状況 | 106 |
| MOM がコレクタを管理する方法の理解 | 107 |

| | |
|--|-----|
| クラスタ化および Enterprise Manager クロック同期 | 108 |
| クラスタとエージェントの名前付け | 109 |
| クラスタ化および管理モジュール | 109 |
| Enterprise Manager フェールオーバーの使用 | 110 |
| Enterprise Manager フェールオーバーのルール | 112 |
| Enterprise Manager フェールオーバーを単一ホストで動作させるための構成 | 114 |
| MOM フェールオーバーおよび CA CEM TIM について | 114 |
| Enterprise Manager のクラスタの設定 | 116 |
| MOM の設定 | 117 |
| コレクタの設定 | 118 |
| CDV の概要 | 119 |
| CDV の設定 | 121 |

第 7 章: MOM エージェント負荷分散の設定 123

| | |
|--|-----|
| エージェント負荷分散の概要 | 123 |
| MOM がコレクタにエージェントを割り当てる方法 | 124 |
| MOM がクラスタのバランスを再調整する方法 | 125 |
| エージェント負荷分散のメトリック重み係数の設定 | 126 |
| エージェント負荷分散のメトリックしきい値の設定 | 127 |
| エージェント負荷分散の間隔プロパティの設定 | 128 |
| エージェント負荷分散の使用シナリオ | 129 |
| 新しいコレクタがクラスタに追加されたときのエージェント負荷分散 | 129 |
| コレクタがエージェント付きで追加されたときのエージェント負荷分散 | 130 |
| コレクタ障害時のエージェント負荷分散 | 130 |
| コレクタ再起動時のエージェント負荷分散 | 130 |
| 重みによるエージェント負荷分散 | 131 |
| コレクタへのエージェントの割り当ての構成 | 131 |
| エージェントの負荷分散の設定例 | 136 |

第 8 章: Enterprise Manager ネットワークトポロジエージェントの設定 143

| | |
|--|-----|
| エージェントと Enterprise Manager 間のネットワーク トポロジの概要 | 144 |
| CA Introscope 間でのエージェント接続情報の継承方法 | 146 |
| 設定がエージェントから Enterprise Manager への接続に及ぼす影響 | 148 |
| エージェントが Enterprise Manager からの切断されたときの動作 | 149 |
| エージェントの接続要求が拒否されたときの動作 | 150 |
| Enterprise Manager ネットワーク トポロジエージェントの設定プロセス | 151 |
| Enterprise Manager ネットワーク トポロジエージェントの計画 | 152 |
| loadbalancing.xml ルールがないときに新しいエージェント接続を許可するかどうかの設定 | 154 |

| | |
|--|-----|
| エージェントの再接続待機時間の設定 | 155 |
| 禁止されたエージェント接続のクランプ限界値の設定 | 156 |
| 許可済み Enterprise Manager へのエージェントの連続的な再接続の設定 | 157 |
| Enterprise Manager によって許可および禁止されるエージェントに関する loadbalancing.xml の設定 | 159 |
| エージェントと Enterprise Manager 間のネットワーク トポロジの設定 | 159 |
| Enterprise Manager が拒否されたエージェントを処理する方法 | 159 |
| コレクタが introscope.apm.agentcontrol.agent.allowed プロパティを使用する場合 | 160 |
| エージェントが loadbalancing.xml で許可または禁止の正規表現に一致しない場合 | 161 |
| エージェントに割り当てられたコレクタが利用不可能で、他のコレクタが利用可能な場合 | 161 |
| コレクタが禁止されたエージェントを直接接続で処理する方法 | 162 |
| introscope.apm.agentcontrol.agent.allowed プロパティがない場合のエージェント接続のデフォルト値 | 162 |
| MOM が利用不可能な場合に CA Introscope がエージェントの接続先を決定する方法 | 162 |

第 9 章: コマンドライン Workstation の使用 163

| | |
|--------------------------------------|-----|
| コマンドライン Workstation (CLW) について | 163 |
| CLW の実行 | 164 |
| JVM の要件 | 164 |
| CLW コマンドを実行する場所 | 164 |
| CLW インタラクティブ モードの使用 | 165 |
| CLW の呼び出し | 165 |
| CLW での大文字と小文字の区別 | 166 |
| CLW コマンドの出力結果 | 166 |
| CLW および正規表現 | 166 |
| CLW コマンド内の円記号および引用符 | 167 |
| さまざまな環境での CLW の使用 | 167 |
| コマンドライン Workstation ログの設定 | 167 |
| CLW コマンドリファレンス | 168 |
| Enterprise Manager コマンド | 168 |
| Introscope エージェント コマンド | 170 |
| APM ステータス コンソール コマンド | 174 |
| 管理モジュール コマンド | 179 |
| アクション コマンド | 182 |
| アラート コマンド | 185 |
| アラートダウンタイム スケジュール コマンド | 187 |
| 計算機コマンド | 189 |
| ダッシュボード コマンド | 191 |
| メトリック コマンドおよびメトリック グループ コマンド | 193 |
| レポートテンプレート コマンド | 195 |

| | |
|------------------------------------|-----|
| SNMP コレクション コマンド | 200 |
| トランザクション追跡オプションの設定 | 202 |
| トランザクション追跡セッションの開始 | 202 |
| アプリケーション問題切り分けマップのコマンド | 211 |
| Loadbalancing.xml コマンド | 218 |
| サンプル スクリプト | 221 |
| トランザクション追跡セッション | 221 |
| アラートによって開始されるトランザクション追跡セッション | 225 |

第 10 章: WatchDog コマンドライン ツールの使用 227

| | |
|--|-----|
| WatchDog の概要 | 227 |
| WatchDog の実行 | 228 |
| SAP での WatchDog の実行 | 229 |
| WatchDog コマンド | 230 |
| WatchDog start コマンド | 231 |
| WatchDog stop コマンド | 232 |
| WatchDog status コマンド | 233 |
| WatchDog コマンド オプション | 234 |
| WatchDog -watch コマンド オプション | 235 |
| WatchDog -port コマンド オプション | 236 |
| WatchDog -startcmd コマンド オプション | 236 |
| WatchDog -interval コマンド オプション | 237 |
| WatchDog -startuptime コマンド オプション | 238 |
| WatchDog -jre コマンド オプション | 238 |
| WatchDog -emport コマンド オプション | 239 |
| WatchDog -emuser コマンド オプション | 239 |
| WatchDog -empwd コマンド オプション | 240 |
| WatchDog ログ ファイルの表示 | 240 |
| サンプル スクリプト | 240 |

第 11 章: WebView オプションの設定 241

| | |
|--------------------------------------|-----|
| WebView アプリケーション コンテキスト パスの設定 | 241 |
| APM WebView のパフォーマンスの設定および監視方法 | 242 |
| 前提条件の確認 | 245 |
| APM UI Performance Monitor の設定 | 246 |
| 設定の確認 | 247 |
| WebView UI のパフォーマンスの監視 | 248 |
| WebView メトリック グループの設定 | 251 |

| | |
|--|------------|
| ダッシュボードデータの表示および解釈 | 252 |
| 第 12 章: Workstation の構成 | 257 |
| 冗長モードでの Workstation の実行 | 257 |
| Workstation の出力のファイルへのリダイレクト | 258 |
| ログイン値を指定するための Workstation の設定 | 258 |
| アジア系言語レポート向けの Workstation の設定 | 259 |
| 第 13 章: システム設定 | 261 |
| クロック スキュー許容度の設定 | 261 |
| 最大データ ポイント取得プロパティの設定 | 262 |
| クエリによって返されるデータ ポイントの制限 | 264 |
| 返されるクエリ結果数の増加 | 265 |
| APM ステータス コンソールのクランプおよび重要イベントの設定 | 265 |
| 第 14 章: アプリケーション問題切り分けマップの構成 | 269 |
| アプリケーション問題切り分けマップ | 269 |
| トランザクション サンプリング | 270 |
| マップ エlement エイジングの設定 | 271 |
| アプリケーション問題切り分けマップ データのクランプ | 276 |
| アプリケーション問題切り分けマップ データの廃棄の設定 | 276 |
| アプリケーション問題切り分けマップ オブジェクトの廃止時間の設定 | 280 |
| アプリケーション問題切り分けマップの時間エイジング プロパティ | 281 |
| アプリケーション問題切り分けマップの時間エイジング プロパティの設定 | 282 |
| 第 15 章: Catalyst データをロードするための APM の設定 | 285 |
| CA Catalyst データをロードするための CA APM の設定 | 286 |
| CatalystPolicy.xml ファイルの設定 | 287 |
| 第 16 章: CA CEM の概要 | 289 |
| CEM コンソールおよびセットアップ ページへのアクセス | 289 |
| CEM コンソールへのアクセス | 289 |
| CA CEM へのログインのトラブルシューティング | 291 |
| [TIM System Setup] ページへのアクセス | 291 |
| CEM コンソールから TIM へのアクセス | 292 |
| CA CEM 管理者の責任 | 292 |

| | |
|-----------------|-----|
| 日単位のタスク | 292 |
| 週単位のタスク | 293 |
| 月単位のタスク | 294 |
| 四半期単位のタスク | 294 |

第 17 章: CA CEM のネットワーク オプション 297

| | |
|---|-----|
| CA CEM のネットワーク オプションの概要 | 297 |
| ネットワーク トラフィックの監視の概要 | 298 |
| ネットワーク タップの使用 | 298 |
| ミラー ポートの使用 | 299 |
| CA CEM の挿入場所の概要 | 300 |
| インターネットとインターネットルータの間 | 301 |
| インターネット ルータとファイアウォールの間 | 302 |
| ファイアウォールと集約スイッチの間 | 303 |
| 集約スイッチとネットワーク ロード バランサの間 | 303 |
| ネットワーク ロード バランサと Web サーバの間 | 304 |
| ブラウザから Enterprise Manager への接続 | 305 |
| IPv6 と CA CEM | 305 |
| IPv6 の概要 | 305 |
| CA CEM での IPv6 | 306 |
| IPv6 ネットワーク トラフィックの監視 | 306 |
| デュアルスタック (IPv6 および IPv4) ホストでの CA CEM の実行 | 306 |
| IPv6 の有効なアドレス形式 | 309 |

第 18 章: CA CEM の管理 311

| | |
|---|-----|
| CA CEM 管理のプロセス | 311 |
| Enterprise Manager サービスの配置 | 312 |
| Enterprise Manager サービスの標準的な配置 | 314 |
| クラスタ化された環境での Enterprise Manager サービスの配置 | 316 |
| リアルタイム トランザクション メトリックのための TIM の選択 | 317 |
| 自動 トランザクション 検出のための TIM の選択 | 317 |
| Enterprise Manager 構成の変更 | 318 |
| Enterprise Manager の削除 | 320 |
| Enterprise Manager サービスのトラブルシューティング | 320 |
| CA CEM ドメインの定義 | 323 |
| インシデント コストとビジネス インパクトとの対比 | 329 |
| インシデント 関連設定の定義 | 331 |
| インシデント 管理設定の構成 | 334 |

| | |
|--------------------------------------|-----|
| インシデント生成ルールの設定..... | 334 |
| ビジネスインパクトの設定およびインシデントエビデンスの収集..... | 335 |
| エビデンスコレクションスクリプトで使用する引数..... | 338 |
| インシデントエイジアウトルールの設定..... | 339 |
| インシデントのオープン時または重大度の変更時の電子メールの送信..... | 340 |
| SMTPサーバ設定の構成..... | 341 |
| 新規ビジネスサービスのセキュリティグループの設定..... | 344 |
| 監視の有効化..... | 348 |
| 監視の同期..... | 348 |
| 前回の同期以降の構成変更の表示..... | 349 |

第 19 章: CA CEM 上のユーザおよびグループの管理 353

| | |
|---------------------------------|-----|
| ユーザグループの概要..... | 354 |
| ユーザグループの最大数..... | 355 |
| 要求属性別の新規ユーザの自動割り当て..... | 356 |
| サブネットユーザグループへの新規ユーザの自動割り当て..... | 357 |
| 新規ユーザのサブネットユーザグループの作成..... | 357 |
| プロキシサーバを使用するユーザの識別..... | 359 |
| 新規ユーザグループの管理..... | 361 |
| ユーザグループへの新規ユーザの手動割り当て..... | 361 |
| ユーザグループの設定..... | 362 |
| 一括編集によるユーザ設定の構成..... | 364 |
| 関連 SLA の設定..... | 365 |
| 関連 SLA の表示..... | 366 |
| 関連 SLA の追加..... | 367 |
| 既存の関連 SLA の更新..... | 369 |
| 関連 SLA の削除..... | 369 |
| ユーザグループの削除..... | 370 |
| ユーザの非アクティブ化または削除..... | 370 |
| ユーザの再アクティブ化..... | 371 |

第 20 章: CA CEM でのシステムオペレーションの管理 373

| | |
|-------------------------|-----|
| CA CEM イベントの概要..... | 373 |
| 重大度レベル..... | 373 |
| 発生する可能性のあるイベントのリスト..... | 374 |
| CA CEM イベントの表示..... | 377 |
| CA CEM イベントの管理..... | 377 |
| イベントの電子メール通知の受信..... | 377 |

| | |
|---------------------------------|-----|
| TIM マシン稼働状況の確認..... | 379 |
| [Appliance Health] ページ参照表 | 380 |
| CA CEM 監査証拠の確認..... | 381 |

第 21 章: CA CEM のレポート機能 383

| | |
|-----------------------------------|-----|
| CA CEM レポートのキャプチャ | 383 |
| CA CEM レポート集約の概要 | 383 |
| レポート配信..... | 384 |
| レポートデータのセキュリティ保護..... | 385 |
| レポート形式..... | 385 |
| レポートタイムフレーム | 386 |
| レポートの概要..... | 387 |
| PDF レポート | 388 |
| 電子メール レポート | 389 |
| 保存済みまたはスケジュール済みレポート | 389 |
| レポートのスケジュール..... | 390 |
| [マイ レポート] の使用によるレポートのスケジュール | 390 |
| レポートの生成およびスケジュール..... | 394 |
| CA CEM データのエクスポート | 395 |
| データのエクスポート..... | 395 |
| レポートの保存またはスケジュール | 397 |
| CSV ヘッダ | 398 |

第 22 章: CA CEM によるセキュアな Web アプリケーションの監視 399

| | |
|---|-----|
| SSL 秘密鍵のインポートおよび管理..... | 399 |
| Apache または OpenSSL ベースの Web サーバ秘密鍵の保存..... | 400 |
| Microsoft インターネット インフォメーション サービス (IIS) 秘密鍵のエクスポート | 400 |
| SunONE、iPlanet、Netscape Enterprise Server | 401 |
| SSL 対応の CA CEM の設定..... | 405 |
| HTTPS サーバの複数の鍵..... | 406 |
| SSL 使用時の CA CEM 機能の検証..... | 406 |

第 23 章: CA CEM での Napatech アダプタの使用 407

| | |
|---|-----|
| CA CEM での Napatech アダプタの使用について | 407 |
| Napatech アダプタおよびソフトウェアの入手..... | 408 |
| Napatech アダプタおよび Napatech ソフトウェアのインストール | 408 |
| Napatech アダプタおよび監視の有効化..... | 410 |
| (オプション) Napatech フィルタの作成および有効化..... | 411 |

| | |
|--------------------------------------|-----|
| 高度なフィルタの作成..... | 413 |
| その他の Napatech アダプタ タスク | 414 |
| Napatech アダプタのトラブルシューティング | 416 |
| Napatech アダプタがトラフィックを受信しない..... | 417 |
| Ethernet ポートとしての Napatech アダプタ | 417 |
| 目的のトラフィックが見当たらない..... | 418 |
| シリアル番号および他の Napatech アダプタの詳細..... | 418 |

第 24 章: CA CEM で CA Introscope を使用する設定 421

| | |
|---|-----|
| CA APM の開始..... | 422 |
| CA APM カスタマ エクスペリエンス メトリックの概要 | 422 |
| CA APM 問題解決の切り分けの概要..... | 423 |
| CA CEM 設定のためのチェックリスト | 425 |
| 必要な統合機能の決定..... | 425 |
| Introscope の設定 | 426 |
| カスタマ エクスペリエンス メトリック統合の設定 | 430 |
| CA CEM 設定の確認..... | 439 |
| Introscope 設定のためのチェックリスト..... | 439 |
| 必要な統合機能の決定..... | 440 |
| Enterprise Manager の設定..... | 440 |
| Java エージェントとの統合 | 442 |
| .NET エージェントとの統合 | 446 |
| Introscope 設定の確認 | 449 |
| CA Introscope および CA CEM 間の統合のトラブルシューティング | 449 |
| CA CEM 上での CA Introscope 統合の確認..... | 449 |
| 症状と解決策..... | 450 |
| アップグレードに関する考慮事項..... | 452 |
| ビジネス アプリケーションのセットアップ | 453 |

第 25 章: CA SiteMinder と CA CEM の統合 455

| | |
|--|-----|
| CA SiteMinder のチェックリスト..... | 456 |
| CA CEM での CA SiteMinder の設定 | 456 |
| カスタム CA SiteMinder エージェントの作成..... | 458 |
| CA SiteMinder での CA CEM のカスタム エージェント タイプの作成..... | 458 |
| CA CEM でのポリシー サーバの定義 | 459 |
| CA CEM でのエージェントの定義 | 460 |
| TIM SiteMinder ホスト設定の表示..... | 461 |
| CA SiteMinder の有効化..... | 461 |

| | |
|---|-----|
| CA SiteMinder および CA CEM 間の統合のトラブルシューティング | 462 |
|---|-----|

第 26 章: CA Service Desk と CA CEM の統合 463

| | |
|---|-----|
| CA Service Desk と CA CEM について | 463 |
| CA Service Desk 統合の概要 | 463 |
| CA CEM との統合用の CA Service Desk の設定 | 464 |
| CA Service Desk プラグインの設定 | 464 |
| CA Service Desk 要求領域の設定 | 468 |
| CA Service Desk と CA CEM の併用 | 468 |
| CA Service Desk および CA CEM 間の統合のトラブルシューティング | 469 |
| 症状と解決策 | 470 |
| CA Service Desk と CA CEM との統合で使用される用語 | 471 |
| CA Service Desk の用語 | 472 |
| CA Service Desk と CA CEM の用語の対応 | 472 |

第 27 章: CA APM Cloud Monitor の CA APM への統合 475

| | |
|---|-----|
| CA APM 導入環境に CA APM Cloud Monitor を統合する方法 | 476 |
| CA APM Cloud Monitor エージェントのダウンロードおよびインストール | 476 |
| CA APM Cloud Monitor エージェント接続の検証 | 477 |
| データを制限する方法 | 479 |

付録 A: プロパティファイル リファレンス 481

| | |
|--|-----|
| IntroscopeEnterpriseManager.properties | 482 |
| 利用可能なプロセッサ | 483 |
| アラート動作 | 484 |
| 通信 | 484 |
| Workstation Login Parameters Auto Fill セクション | 490 |
| EM Web サーバの設定 | 490 |
| ホット設定サービス | 492 |
| アプリケーション ヒューリスティック | 492 |
| ログ | 493 |
| 永続コレクション - データベースへのデータの記録 | 495 |
| フラット ファイルのプロパティ | 497 |
| トランザクション イベント データベース | 497 |
| トランザクション 追跡 サンプルング | 498 |
| Enterprise Manager のメトリック クランプ | 499 |
| SmartStor | 502 |
| ベースライン データの保存 | 508 |

| | |
|---|-----|
| SNMP コレクション | 508 |
| WebView | 508 |
| CA APM ChangeDetector | 509 |
| 管理モジュールのブートストラップ | 509 |
| 管理モジュールのデプロイ | 510 |
| クラスタ化の設定 | 510 |
| エージェントの相互作用 | 515 |
| Enterprise Manager フェールオーバー | 520 |
| 設定ディレクトリ | 521 |
| アプリケーション問題切り分けマップ データ | 522 |
| ロケーションマップ データ | 528 |
| Web サービス | 528 |
| 送信メッセージ キュー | 529 |
| スレッド ダンプ | 531 |
| Web サービスがパフォーマンスを処理するためのスレッド プロパティ | 534 |
| SNMP 問題切り分けマップ アラート アクション | 535 |
| アプリケーションマップ オブジェクト | 536 |
| APMEnterpriseManager.properties | 537 |
| c3p0 プロパティ | 537 |
| Hibernate 固有のプロパティ | 539 |
| apm-events-thresholds-config.xml | 541 |
| Introscope クランプ プロパティ | 542 |
| introscope.clw.max.users | 542 |
| introscope.enterprisemanager.agent.connection.limit | 543 |
| introscope.enterprisemanager.agent.error.limit | 545 |
| introscope.enterprisemanager.agent.metrics.limit | 545 |
| introscope.enterprisemanager.agent.trace.limit | 546 |
| introscope.cdv.max.users | 547 |
| introscope.enterprisemanager.disconnected.historical.agent.limit | 547 |
| introscope.enterprisemanager.events.limit | 550 |
| introscope.enterprisemanager.metrics.historical.limit | 550 |
| introscope.enterprisemanager.metrics.live.limit | 551 |
| introscope.enterprisemanager.transactionevents.storage.max.disk.usage | 551 |
| introscope.workstation.max.users | 552 |
| カスタマ エクスペリエンス クランプ プロパティ | 553 |
| 重要イベントのしきい値の設定 | 556 |
| ResourceMetricMap.properties | 559 |
| CPU Utilization | 561 |
| Time Spent in GC | 562 |
| Threads in Use | 562 |
| JDBC Connections in Use | 562 |

| | |
|---|-----|
| Catalyst.properties | 562 |
| catalyst.host | 563 |
| catalyst.protocol | 564 |
| catalyst.port | 564 |
| catalyst.login | 564 |
| catalyst.password | 564 |
| catalyst.rest.entrypoint | 565 |
| catalyst.rest.alerts.pollingperiodsec | 565 |
| catalyst.rest.virtualhosts.pollingperiodsec | 565 |
| catalyst.product.url | 566 |
| catalyst.alert.filter.total | 566 |
| catalyst.alert.filter.time | 566 |
| catalyst.alert.filter.products | 567 |
| catalyst.alert.filter.types | 567 |
| catalyst.alert.filter.severities | 568 |
| catalyst.rest.maxFailures | 568 |
| catalyst.rest.maxAlertsPerPage | 569 |
| catalyst.rest.alerts.threads | 569 |
| catalyst.rest.virtualhosts.threads | 569 |
| catalyst.entity.cache.size | 570 |
| catalyst.entity.cache.expirationsec | 570 |
| catalyst.database.alerts.enabled | 570 |
| catalyst.database.map.name | 571 |
| EMservice.conf | 571 |
| wrapper.java.command | 572 |
| wrapper.java.mainclass | 572 |
| wrapper.java.classpath.x | 572 |
| wrapper.java.library.path.1 | 572 |
| wrapper.java.additional.x= | 573 |
| wrapper.java.initmemory | 573 |
| wrapper.java.maxmemory | 573 |
| wrapper.app.parameter.x | 574 |
| wrapper.startup.timeout | 574 |
| wrapper.console.format | 574 |
| wrapper.console.loglevel | 575 |
| wrapper.logfile | 575 |
| wrapper.logfile.format | 575 |
| wrapper.logfile.loglevel | 575 |
| wrapper.logfile.maxsize | 576 |
| wrapper.logfile.maxfiles | 576 |
| wrapper.syslog.loglevel | 576 |
| wrapper.ntservice.name | 577 |

| | |
|--|-----|
| wrapper.ntservice.displayname | 577 |
| wrapper.ntservice.description | 577 |
| wrapper.ntservice.dependency.x..... | 577 |
| wrapper.ntservice.starttype | 577 |
| wrapper.ntservice.interactive | 578 |
| Introscope Enterprise Manager.lax | 578 |
| lax.application.name | 578 |
| lax.class.path | 578 |
| lax.command.line.args | 579 |
| lax.dir..... | 579 |
| lax.main.class | 579 |
| lax.main.method | 579 |
| lax.nl.current.vm | 580 |
| lax.nl.java.launcher.main.class..... | 580 |
| lax.nl.java.launcher.main.method | 580 |
| lax.nl.java.option.additional..... | 581 |
| lax.nl.message.vm.not.loaded | 582 |
| lax.nl.valid.vm.list..... | 582 |
| lax.nl.win32.microsoftvm.min.version..... | 582 |
| lax.root.install.dir | 583 |
| lax.stderr.redirect | 583 |
| lax.stdin.redirect | 584 |
| lax.stdout.redirect..... | 584 |
| lax.user.dir..... | 585 |
| lax.version | 585 |
| IntroscopeWorkstation.properties..... | 585 |
| log4j.logger.Workstation | 586 |
| log4j.appender.logfile.File..... | 586 |
| introscope.workstation.graph.antialiased | 586 |
| transport.http.proxy.host | 587 |
| transport.http.proxy.port | 587 |
| transport.http.proxy.username | 587 |
| transport.http.proxy.password | 588 |
| transport.tcp.truststore | 588 |
| transport.tcp.trustpassword | 588 |
| transport.tcp.truststore | 589 |
| transport.tcp.keystore | 589 |
| transport.tcp.keypassword | 589 |
| transport.tcp.ciphersuites..... | 590 |
| Introscope Workstation.lax | 590 |
| lax.application.name | 590 |
| lax.class.path..... | 591 |

| | |
|--|-----|
| lax.command.line.args | 591 |
| lax.dir | 591 |
| lax.main.class | 591 |
| lax.main.method | 592 |
| lax.nl.current.vm | 592 |
| lax.nl.java.launcher.main.class..... | 592 |
| lax.nl.java.launcher.main.method | 592 |
| lax.nl.java.option.additional..... | 593 |
| lax.nl.message.vm.not.loaded | 593 |
| lax.nl.valid.vm.list..... | 593 |
| lax.nl.win32.microsoftvm.min.version..... | 594 |
| lax.root.install.dir | 594 |
| lax.stderr.redirect | 594 |
| lax.stdin.redirect | 595 |
| lax.stdout.redirect..... | 595 |
| lax.user.dir..... | 595 |
| lax.version | 596 |
| IntroscopeWebView.properties | 596 |
| introscope.webview.jetty.configurationFile | 596 |
| introscope.webview.tcp.ipaddress | 596 |
| introscope.webview.tcp.port..... | 597 |
| introscope.webview.context.path | 597 |
| introscope.webview.enterprisemanager.tcp.host..... | 597 |
| introscope.enterprisemanager.webview.disableLogin..... | 598 |
| introscope.webview.enterprisemanager.tcp.port..... | 598 |
| log4j.logger.WebView | 598 |
| log4j.logger.WebServer..... | 599 |
| log4j.logger | 599 |
| log4j.logger.com.wily | 600 |
| log4j.logger.org.apache.myfaces | 600 |
| log4j.logger.org.apache.jasper..... | 600 |
| log4j.logger.org.apache.struts | 601 |
| log4j.logger.org.mortbay | 601 |
| ログ記録設定プロパティ | 602 |
| log4j.appender.console..... | 602 |
| log4j.appender.logfile | 603 |
| log4j.appender.logfile.File..... | 603 |
| Introscope WebView.lax | 603 |
| 実行可能ファイルの名前..... | 603 |
| lax.class.path..... | 603 |
| lax.command.line.args | 604 |
| lax.dir..... | 604 |

| | |
|---|------------|
| lax.main.class | 604 |
| lax.main.method | 604 |
| lax.nl.current.vm | 605 |
| lax.nl.java.launcher.main.class..... | 605 |
| lax.nl.java.launcher.main.method | 605 |
| lax.nl.java.option.additional..... | 605 |
| lax.nl.message.vm.not.loaded | 606 |
| lax.nl.valid.vm.list..... | 606 |
| lax.nl.win32.microsoftvm.min.version..... | 606 |
| lax.root.installation.dir..... | 606 |
| lax.stderr.redirect | 607 |
| lax.stdin.redirect | 607 |
| lax.stdout.redirect..... | 607 |
| lax.user.dir..... | 608 |
| lax.version | 608 |
| APMCloudMonitor.properties | 608 |
| apmcm.folders.include | 609 |
| apmcm.monitors.include | 609 |
| apmcm.checkpoints.include | 610 |
| apmcm.include.inactive.monitors | 610 |
| apmcm.folder.metrics.include | 611 |
| apmcm.monitor.psp.metrics.include..... | 611 |
| apmcm.monitor.checkpoint.metrics.include..... | 612 |
| apmcm.force.global.update..... | 612 |
| apmcm.log.adjustment | 613 |
| | |
| 付録 B: JDBC API | 615 |
| JDBC API の設定..... | 615 |
| JDBC API の使用..... | 615 |
| メトリック クエリ | 616 |
| トランザクション追跡クエリ | 617 |
| | |
| 付録 C: Introscope 拡張機能の構成 | 619 |
| SNMP アダプタの構成 | 619 |
| SNMP アダプタの制限事項 | 619 |
| SNMP アダプタのコンポーネント | 619 |
| アラート..... | 621 |
| 通知とアラートの設定..... | 621 |
| SNMP 機能の構成..... | 623 |
| HP LoadRunner へのアップロード | 625 |

| | |
|--|-----|
| HP OpenView へのアップロード..... | 627 |
| Introscope メトリックから SNMP メトリックへの変換..... | 629 |
| Introscope アラート Web サービス拡張機能の構成..... | 630 |

付録 D: デフォルトの tess-default.properties ファイル 633

| | |
|---|-----|
| tess-default.properties プロパティ デフォルト ファイルの変更..... | 633 |
| エビデンス コレクションの Perl パスまたは Python パスの設定..... | 634 |
| perl.path..... | 635 |
| python.path..... | 635 |
| [その他障害情報] リンクのディレクトリ パスの設定..... | 636 |
| additionalDefectDetailFileLocation..... | 637 |
| 障害処理のパフォーマンスの向上..... | 638 |
| defects.affectedUserGroupUpdateInterval_Secs..... | 639 |
| defects.affectedUserGroupAgeoutInterval_Mins..... | 640 |
| 不正なファイルのディレクトリの場所の変更..... | 640 |
| collectors.badDataDirectory..... | 641 |
| その他の CA CEM デフォルト プロパティ..... | 642 |
| baseline.durationInDays..... | 642 |
| BTStatsMetricName.backwardCompatible..... | 643 |
| email.defaultFromAddress..... | 643 |
| invalid.importexport.filename.chars..... | 644 |
| timTessCommunication.useSsl..... | 644 |

第 1 章: 「CA APM 設定および管理ガイド」 の概要

本書を使用するには、Web サーバ、ブラウザ、サポートされているプラットフォーム、およびネットワーク環境の実務的な知識が必要です。CA CEM で監視するアプリケーションをよく理解していることも必要です。また、CA CEM と統合するその他の製品についても把握している必要があります。

本書の前提条件を以下に示します。

- CA APM は、「CA APM インストールおよびアップグレードガイド」の情報に従ってインストールされていること。
- 「CA APM 概要ガイド」に記載されている CA Introscope、CA APM および CA CEM の基本的な知識があること。

このセクションには、以下のトピックが含まれています。

[APM の概要 \(P. 25\)](#)

APM の概要

CA Introscope と CA CEM は、CA APM ソリューションの主力製品です。

CA APM は、エンドユーザエクスペリエンスを理解し、サービス レベル アグリーメント (SLA) を測定することを可能にする、効率の高い包括的なアプリケーションパフォーマンス管理戦略を提供します。すべてのトランザクションをエンドツーエンドのインフラストラクチャにマップし、完全に統合されたソリューションを使用してインシデントの問題切り分けと根本原因診断を行うことを可能にします。

CA APM を使用して、以下を行うことができます。

- 実際のユーザエクスペリエンスを理解する。
- ビジネス サービス上で SLA を設定し管理する。
- 100 パーセントのトランザクション可視性を獲得する。
- 問題の原因を迅速に決定する。
- 問題切り分けを行い、重要事項を識別し、根本原因解析を実行する。

- 実際のビジネス インパクトに基づいて、インシデントに優先順位を割り当てる。
- プロアクティブかつ予測型のアプリケーション監視を実現する。
- レポート回数を増やし、改善を継続的に行う。

第 2 章: Enterprise Manager の起動と停止

この章では、Enterprise Manager (EM) の起動と停止、およびサポートされている環境での起動の自動化の手順について説明します。

注: プロパティの詳細については、「[プロパティファイルリファレンス \(P. 481\)](#)」を参照してください。

このセクションには、以下のトピックが含まれています。

[Windows での Enterprise Manager の起動 \(P. 27\)](#)

[UNIX での Enterprise Manager の起動 \(P. 31\)](#)

[別の JVM を使用するための Enterprise Manager の設定 \(P. 33\)](#)

[Enterprise Manager ログファイルについて \(P. 34\)](#)

[日付またはサイズによる Enterprise Manager ログのロール \(P. 34\)](#)

[Enterprise Manager config ディレクトリの構成 \(P. 36\)](#)

[Enterprise Manager の停止 \(P. 38\)](#)

[予期しないシャットダウン後の再起動 \(P. 39\)](#)

[Enterprise Manager のシェルおよびターミナルウィンドウのコマンド \(P. 41\)](#)

Windows での Enterprise Manager の起動

Windows 環境で Enterprise Manager を実行する場合は、Enterprise Manager を手動で起動するか、または Windows サービスとして実行できます。

Enterprise Manager の Windows サービスとしての実行

Enterprise Manager を Windows サービスとしてインストールすると、コンポーネントを常に利用可能な状態にしておくことができます。Enterprise Manager を Windows サービスとして構成すると、マシン起動時にサービスが自動的に起動します。また、マシンと同時にシャットダウンします。

注: Introscope は、Tanuki Software (<http://wrapper.tanukisoftware.org>) が提供するパブリック ドメインの Java Service Wrapper を使用して、Enterprise Manager を Windows サービスとして実行できるようにします。Tanuki Wrapper の詳細については、「[Configuration Property Overview](http://wrapper.tanukisoftware.org)」(<http://wrapper.tanukisoftware.org>) を参照してください。

以下の説明は、読者がアプリケーションを Windows サービスで設定する作業に慣れており、かつ Windows の [サービス] コンソールの使用方法を理解していることを前提としています。

Enterprise Manager を Windows サービスとして実行するための前提条件

Enterprise Manager を Windows のサービスとして実行する場合は、Enterprise Manager がすでにインストールされており、コンソール モードで正常に動作することを確認しておく必要があります。

Enterprise Manager の Windows サービスとしての構成

このセクションでは、Windows マシン上で Introscope のデフォルト JVM システム パラメータに基づいて実行されている Enterprise Manager の 1 つをサービスとして登録する方法を説明します。

1. Enterprise Manager を停止します（「[Enterprise Manager の停止 \(P. 38\)](#)」を参照）。
2. *IntroscopeEnterpriseManager.lax* ファイル (<EM_Home>/ディレクトリにあります) で、*lax.stdin.redirect* プロパティの設定を空白にして、ファイルを保存します。
3. *IntroscopeEnterpriseManager.properties* ファイル (<EM_Home>/config ディレクトリにあります) で、*introscope.enterprisemanager.disableInteractiveMode* プロパティを *true* に設定し、ファイルを保存します。

4. Enterprise Manager サービスに一意の名前を割り当てます。デフォルトでは、サービス名は *EMService.conf* 内で割り当てられます。これは、*<EM_Home>/bin* ディレクトリにあります。マシン上でほかのサービスを設定しない場合は、デフォルトのサービス名をそのまま使用できます。それ以外の場合は、*EMService.conf* で、以下のプロパティを使用して、サービスの一意の名前および表示名を指定します。
 - *wrapper.ntservice.name=<一意の Enterprise Manager 名>*
 - *wrapper.ntservice.displayname=<Enterprise Manager 表示名>*
5. 変更をファイルに保存します。
6. サービスとして Enterprise Manager インスタンスを登録するには、*<EM_Home>/bin/EMCtrl32.bat register* スクリプトを実行します。

Windows の [サービス] コンソールに、Enterprise Manager が Windows サービスとして構成されていることが表示されます。

サービスとして実行する Enterprise Manager ごとに、これらの手順を繰り返します。

Windows サービスのプロパティの変更

EMService.conf ファイル内の構成プロパティを変更する必要がある場合は、この後のセクションの説明に従って、先にサービスの登録を解除してください。変更を有効にするには、サービスを変更して再登録します。

Enterprise Manager Windows サービスの登録解除

以下の場合に Enterprise Manager サービスの登録を解除します。

- *EMService.conf* プロパティ ファイルに変更を加えるとき
- Enterprise Manager のインスタンスの制御方法をコンソール制御に戻すとき
- Enterprise Manager のインスタンスをアンインストールするとき

Enterprise Manager のサービスの登録を解除する方法

1. Enterprise Manager サービスを停止し、Windows の [サービス] 管理 GUI をシャットダウンします。
2. `<EM_Home>/bin/EMCtrl32.bat unregister` スクリプトを実行します。

注: サービスに削除対象のマークが付けられるのは、Enterprise Manager サービスまたは Windows の [サービス] 管理 GUI のいずれかがアクティブな場合のみです。これは Windows サービスに対して定められている標準の動作です。この動作は、サービスが削除されないように Windows レジストリがロックされているために生じます。マシンを再起動すると、サービスは削除されます。

Enterprise Manager Windows サービスの停止と再起動

Windows サービスとして実行している Enterprise Manager を起動、停止、再起動するには、Windows の [サービス] 管理 GUI の標準コントロールを使用します。

Windows での Enterprise Manager の手動による起動

Enterprise Manager は、以下のいずれかの方法で手動で起動できます。

- [スタート] - [プログラム] - [CA APM] - [管理] - [CA APM] - [Enterprise Manager] を選択します。
- `<EM_Home>` ディレクトリにある *IntroscopeEnterpriseManager.exe* を実行します。

Enterprise Manager は、`<EM_Home>/Introscope Enterprise Manager.lax` (「Introscope Enterprise Manager.lax」を参照) のプロパティ設定に従って起動されます。

UNIX での Enterprise Manager の起動

UNIX 環境で Enterprise Manager を実行する場合は、Enterprise Manager を手動で起動するか、または *nohup* モードで実行します。

UNIX での Enterprise Manager の手動による起動

UNIX で Enterprise Manager を手動で起動する方法

- UNIX で Enterprise Manager を起動するには、コマンドプロンプトで以下のように入力して、`Introscope_Enterprise_Manager` を実行します。

```
「./Introscope Enterprise Manager」
```

Enterprise Manager は、`<EM_Home>`（「[プロパティファイルリファレンス \(P. 481\)](#)」を参照）のプロパティ設定に従って起動されます。

Enterprise Manager の出力は、UNIX のシェルに表示されます。シェルは、以下のセクションで説明する *nohup* モードで Enterprise Manager を起動しない限り、ユーザ入力を受け付けません。

UNIX での Enterprise Manager コントロール スクリプトの実行

サーバアプリケーションの起動、停止、およびステータス確認が可能なコントロールスクリプトを実行して、Enterprise Manager を管理できます。`EMCtrl.sh startup` スクリプトを使用すると、「./Introscope Enterprise Manager」コマンドを直接実行しなくても、Enterprise Manager を起動および停止することができます。

UNIX で Enterprise Manager コントロール スクリプトを実行する方法

`bin` ディレクトリで以下のコマンドを実行します。

- `./EMCtrl.sh start` - Enterprise Manager を起動します。
- `./EMCtrl.sh stop` - Enterprise Manager を停止します。
- `./EMCtrl.sh status` - Enterprise Manager のステータスを表示します。
- `./EMCtrl.sh help` - スクリプトでサポートされているオプションが表示されます。

UNIX での nohup モードでの Enterprise Manager の実行

UNIX の *nohup* は、*HUP*（ハングアップ）シグナルを無視してコマンドを実行することで、コマンドを送出したユーザがログアウトした後も、そのコマンドの実行を継続することが可能になります。この場合、通常はターミナルに表示される出力が、*nohup.out* という名前のファイルに保存されるようになります。

UNIX で Enterprise Manager を nohup モードで実行する方法

1. *IntroscopeEnterpriseManager.lax* ファイル（<EM_Home>/ディレクトリにあります）で、*lax.stdin.redirect* プロパティの設定を空白にして、ファイルを保存します。
2. *IntroscopeEnterpriseManager.properties* ファイル（<EM_Home>/config ディレクトリにあります）で、*introscope.enterprisemanager.disableInteractiveMode* プロパティを *true* に設定し、ファイルを保存します。
3. 以下のコマンドを使用して Enterprise Manager を起動します。

```
nohup Introscope_Enterprise_Manager&
```

注： Enterprise Manager を *nohup* モードで起動する場合は、必ずここで説明した構成をまず行ってください。構成せずに実行した場合、Enterprise Manager が起動しないか、起動できてもシステムリソースの消費量が極端に大きくなる可能性があります。

別の JVM を使用するための Enterprise Manager の設定

デフォルトでは、Introscope コンポーネントはバンドルされている JVM を使用します。このセクションでは、別の JVM を使用するように Enterprise Manager を設定する方法について説明します。

- Enterprise Manager を *Introscope Enterprise Manager.exe* で起動する場合には、*lax.nl.current.vm* プロパティ (*Introscope Enterprise Manager.lax* 内) を、目的の JVM 実行可能ファイルをポイントするように編集します。
 - 実行可能ファイルの絶対パスまたは相対パスを使用できます。
 - Windows では円記号はエスケープします。また、JVM 実行可能ファイルは、「*java*」ではなく「*java.exe*」のように拡張子を含めて指定してください。
- Enterprise Manager を Windows サービスとして実行する場合には、*wrapper.java.command* プロパティ (*EMService.conf* 内) を、希望する JVM 実行可能ファイルをポイントするように編集します。
 - 絶対パスを使用することができます。円記号はエスケープする必要があります。
 - 相対パスを使用することもできます。CA Technologies では、UNIX のスラッシュを使用して、*./* で開始することをお勧めします。
 - 実行可能ファイルは *java* です。 *java.exe* ではありません。
- AS/400 上で、Enterprise Manager を *runem.sh* スクリプトで起動する場合には、*JAVA_HOME* 変数 (*runem.sh* 内) を、希望する JVM のルートディレクトリをポイントするように編集します。
 - 実行可能ファイルへのパスは相対パスではなく絶対パスを使用してください。

Enterprise Manager ログ ファイルについて

Enterprise Manager のログ ファイル、*IntroscopeEnterpriseManager.log* (<EM_Home>/logs ディレクトリ内にあります) には、Introscope、CA CEM、および APM データベースの実行状況およびエラー状態が記録されます。たとえば、起動とシャットダウンに関するメッセージ、特定のタイプの過剰なオーバーヘッド、サードパーティのライブラリ、CA CEM と Enterprise Manager の通信、Introscope と CA CEM の各プロパティに関するデータなどです。

Enterprise Manager ログのプロパティを設定することができます。詳細については、「[ログ](#) (P. 493)」を参照してください。

日付またはサイズによる Enterprise Manager ログのロール

日付またはサイズに基づいて Enterprise Manager ログをロールして、指定した日数の情報を保持し、残りをパージできます。

Enterprise Manager ログ ファイルをロールする方法

1. <EM_Home>%config ディレクトリの *IntroscopeEnterpriseManager.properties* ファイルを開きます。
2. 「Logging Configuration」セクションを見つけます。
3. 必要なログ ロールが実行されるようプロパティを変更します。手順の詳細は以下のとおりです。
4. *IntroscopeEnterpriseManager.properties* ファイルを保存して閉じます。必要なログ ロール動作に応じて、以下のプロパティを設定します。

日付を指定して、または毎日、ログ ファイルをロールする方法

- 以下のとおりにプロパティを変更します。
 - `log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender`
 - `log4j.appender.logfile.DatePattern`

2つのプロパティが連携し、日付に基づいて Enterprise Manager ログ ファイルがロールされます。`log4j.appender.logfile.DatePattern` によって、`log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender` プロパティが実行されるログ ロール期間が定義されます。

たとえば、以下の構成では、ログ ファイルは毎日ロールされます。`log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender`
`log4j.appender.logfile.DatePattern='yyyy-MM-dd`

時間間隔によってログ ファイルをロールする方法

- プロパティ `log4j.appender.logfile.DatePattern` を変更します。この Enterprise Manager プロパティは、時刻に基づいて Enterprise Manager ログ ファイルをロールするタイミングを決定します。

以下に2つの例を示します。

- 以下の構成では、ログ ファイルが毎時間ロールされます。
`log4j.appender.logfile.DatePattern='.'yyyy-MM-dd-hh`
- 以下の構成では、ログ ファイルが毎日午前0時にロールされます。
`log4j.appender.logfile=com.wily.org.apache.log4j.DailyRollingFileAppender`
`log4j.appender.logfile.DatePattern='.'yyyy-MM-dd`

ログのサイズや数によってログ ファイルをロールする方法

- 以下のとおりにプロパティを変更します。
 - *log4j.appender.logfile.MaxBackupIndex*
このプロパティによって、Enterprise Manager で保持されるバックアップ ログ ファイルの数が決定します。
 - *log4j.appender.logfile.MaxFileSize*.
このプロパティによって、ログ ファイルの最大サイズが決定します。

たとえば、以下の構成では、最大 3 つのバックアップ/ロールされた Enterprise Manager ログが保持され、各ログのサイズが最大 2 キロバイトになります。

```
log4j.appender.logfile.MaxBackupIndex=3  
log4j.appender.logfile.MaxFileSize=2KB
```

Enterprise Manager config ディレクトリの構成

複数の Enterprise Manager があり、単一の Introscope インスタンスを使用してこれらを実行する場合、Enterprise Manager ごとに個別の構成ディレクトリを作成することができます。Enterprise Manager ごとに、*config*、*logs*、*data*、*traces* の各ディレクトリのコピーを作成します。config ディレクトリの各コピー内で、*IntroscopeEnterpriseManager.properties* ファイルの対応するプロパティが、*config*、*logs*、*data*、*traces* ディレクトリのコピーを指すように設定します。

個別の構成ディレクトリを作成することで、単一の Introscope インスタンス内にすべてのディレクトリを保持したまま、Enterprise Manager 別に config、logs、data、および traces ディレクトリを管理することができます。

Enterprise Manager に個別の構成ディレクトリを指定する方法

1. *IntroscopeEnterpriseManager.properties* ファイルを開き、以下のプロパティを変更します。

```
introscope.enterprisemanager.directory.config=config
```

デフォルトのディレクトリは *config* で、初めて Introscope をインストールしたときに作成される構成ディレクトリです。絶対パス（例：*C:¥¥Introscope¥em1¥¥config*）、または Introscope インストールディレクトリを基準にした相対パス（例：*config2*）のいずれかを使用して、このディレクトリの場所を変更します。例：

```
introscope.enterprisemanager.directory.config=  
C:¥¥Introscope¥¥em1¥¥config
```

注：Windows 環境でパスを有効にするには、円記号を二重にしてエスケープする必要があります。

2. 変更した *IntroscopeEnterpriseManager.properties* ファイルを保存します。
3. *Introscope Enterprise Manager.lax* ファイルを開き、以下のプロパティを変更します。

```
lax.nl.java.option.additional
```

このプロパティによって、Java のコマンドラインが変更され、複数のプロパティを持てるようになります。手順 1 で選択した *config* ファイルの場所を使用します。例：

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m -Djava.awt.headless=false  
-Dcom.wily.introscope.em.properties=C:¥¥Introscope¥em1¥¥config
```

注：このプロパティでは、Enterprise Manager プロパティ ファイルのあるディレクトリ、または *IntroscopeEnterpriseManager.properties* ファイルを直接指定することができます。例：

```
-Dcom.wily.introscope.em.properties=C:¥¥Introscope¥em1¥¥config
```

または

```
-Dcom.wily.introscope.em.properties=  
C:¥¥Introscope¥em1¥¥config¥IntroscopeEnterpriseManager.properties
```

4. *Introscope Enterprise Manager.lax* ファイルに加えた変更を保存します。
5. Enterprise Manager を再起動します。

Enterprise Manager の停止

Enterprise Manager を停止すると、以下の状態になります。

- エージェントはデータのレポートイングを停止します。
- SmartStor はデータを保存しなくなります。
- ユーザは Workstation からログアウトします。
- Enterprise Manager に接続していたユーザ全員の接続が切断されます。

ターミナル ウィンドウからの Enterprise Manager の停止

Enterprise Manager のターミナル ウィンドウで、以下のコマンドを入力します。

```
iscopeshutdown
```

注: このコマンドを使用するには、インタラクティブ モードを有効にしておく必要があります。Enterprise Manager プロパティ ファイルで、*introscope.enterprisemanager.disableInteractiveMode* を *false* に設定します。詳細については、「[プロパティ ファイル リファレンス \(P. 481\)](#)」を参照してください。

Workstation からの Enterprise Manager の停止

Enterprise Manager に対してシャットダウン権限を持っている場合は、管理モジュール エディタ ウィンドウの Workstation から [マネージャ] - [Enterprise Manager をシャットダウン] を選択して、Enterprise Manager を停止できます。

Enterprise Manager の自動シャットダウン

ディスク領域の不足によるディスク書き込みエラーを検出すると、Enterprise Manager は自動的にシャットダウンします。フェールオーバが設定されていれば、エージェントによるほかの Enterprise Manager へのフェールオーバが可能です。詳細については、「[CA APM Java Agent 実装ガイド](#)」または「[CA APM .NET Agent 実装ガイド](#)」を参照してください。

予期しないシャットダウン後の再起動

重要: このトピックは CA APM のみに適用されます。スタンドアロンの CA Introscope (TIM なし) を使用している場合は、このトピックをスキップしてください。

ほとんどの状況では、Enterprise Manager を再起動するのは、起動するのと同じです。ただし、計画されたシャットダウンではなく、エラー状態で Enterprise Manager が停止した場合は、再起動前にいくつかのファイルの削除が必要になることがあります。

過負荷やファイル処理エラーが原因で Enterprise Manager がシャットダウン (クラッシュ) した場合、未処理のファイルが、`<EM_Home>/cem/tess/badfiles` ディレクトリに残っていることがあります。これらのファイルが残っている状態で Enterprise Manager を再起動すると、再起動時にファイルが処理されます。これらのファイルのエラーか、これらのファイルによって生じる負荷が原因でシャットダウンした場合、Enterprise Manager は再起動時に再びこれらのファイルを処理するため、再起動後すぐにもう一度クラッシュが発生する可能性があります。

これを解決するには、Enterprise Manager を再起動する前に、ディレクトリからファイルを削除します。

クラッシュ後に Enterprise Manager を再起動する方法

重要: この手順の説明に従ってファイルを削除すると、一部のデータが失われます。失われる可能性があるのは、最新の障害詳細、カスタマエクスペリエンスメトリック、および統計です。

1. TIM コレクションサービスが実行されている Enterprise Manager 上で、`<EM_Home>/cem/tess/badfiles` ディレクトリ内のファイルを削除します。
削除対象のファイルは XML ファイルで、`btstats-2010-01-05-23_26_13-172.16.252.20.xml` や `defect-12627339680000057712-172.16.252.20.xml` などの名前が付いています。
TIM コレクションサービスなどの Enterprise Manager サービスについては、「[Enterprise Manager サービスの配置 \(P. 312\)](#)」を参照してください。
2. 以下のトピックのいずれかに記載されている方法で Enterprise Manager を起動します。
 - [Windows での Enterprise Manager の起動 \(P. 27\)](#)
 - [UNIX での Enterprise Manager の起動 \(P. 31\)](#)

Enterprise Manager 上の複数のクラッシュのトラブルシューティング

症状:

TIM コレクションサービスが実行されている Enterprise Manager がクラッシュし、再起動すると再度クラッシュします。

考えられる原因としては、TIM 関連のデータファイルによって Enterprise Manager に大きい負荷がかかっているか、これらのファイルにエラーが含まれています。

解決方法:

「[予期しないシャットダウン後の再起動 \(P. 39\)](#)」に記載されている手順に従って、これらのファイルを削除します。

Enterprise Manager のシェルおよびターミナル ウィンドウのコマンド

Enterprise Manager が実行されていて、*lax.stdin.redirect*（「プロパティ ファイルリファレンス」で定義されています）が *console* に設定されている場合、Enterprise Manager のターミナル ウィンドウまたはシェルで、以下のコマンドを入力することができます。

| コマンド | 結果 |
|---|---------------------------------|
| <code>iscopedebugpolling [true false] [遅延時間 (秒単位)]</code> | 定期的にデバッグ情報のレポートをログに記録します |
| <code>iscopehelp</code> | ヘルプ画面を表示します |
| <code>iscopeshutdown</code> | Enterprise Manager をシャットダウンします。 |

注: これらのコマンドを使用するには、インタラクティブ モードを有効にしておく必要があります。Enterprise Manager プロパティ ファイルで、*introscope.enterprisemanager.disableInteractiveMode* を *false* に設定します。詳細については、「[プロパティ ファイルリファレンス \(P. 481\)](#)」を参照してください。

第 3 章: Enterprise Manager の通信の構成

この章では、Enterprise Manager と Introscope 環境内のほかのコンポーネントとの通信、デフォルトの通信動作、および Enterprise Manager の通信の構成オプションについて説明します。

このセクションには、以下のトピックが含まれています。

[デフォルトの Enterprise Manager の通信チャンネル \(P. 43\)](#)

[ファイアウォールを越えた Enterprise Manager との接続 \(P. 48\)](#)

[Enterprise Manager Web サーバの HTTPS 用の設定 \(P. 48\)](#)

デフォルトの Enterprise Manager の通信チャンネル

デフォルトでは、Enterprise Manager は、エージェント、Workstation、WebView、および

Enterprise Manager のクラスタとの通信に、ポート 5001 を使用します。

Enterprise Manager へのソケット通信はすべて難読化され、パスワードは暗号化されます。

Enterprise Manager プロパティ ファイル内で、通信チャンネルとその使用について定義するプロパティを以下に示します。

- `introscope.enterprisemanager.serversocketfactory.<ChannelName>`
- `introscope.enterprisemanager.port.<ChannelName>`
- `introscope.enterprisemanager.serversockets.reuseaddr`
- `introscope.enterprisemanager.enabled.channels`

Enterprise Manager と通信する各エージェントには、同様のプロパティがあります。これらには、前に挙げたプロパティと一致する値を指定する必要があります。

同様に、WebView プロパティ ファイル内で、`introscope.webview.enterprisemanager.tcp.port` プロパティに Enterprise Manager ポートを指定します。

注: .NET エージェントは、Enterprise Manager への直接の SSL 接続をサポートしていません。エージェントプロパティの詳細については、お使いの環境に合わせて「[CA APM Java Agent 実装ガイド](#)」または「[CA APM .NET Agent 実装ガイド](#)」を参照してください。

詳細:

[Enterprise Manager クラスタの理解](#) (P. 105)

使用中のポートへの通信チャンネルの再バインド

実際にはソケットを使用しているものが何もないのに、メモリが使用中になっているために、ソケットが使用できなくなっているような状態があります。この状態の例としては、`FIN_WAIT` および `TIME_WAIT` などが挙げられます。

`introscope.enterprisemanager.serversockets.reuseaddr (487P.)` のプロパティを使用すると、Enterprise Manager の通信チャンネルを使用中のローカルポートに再バインドできるようになります。Enterprise Manager のソケットが使用不可の状態になっているが、Enterprise Manager を開始したい場合に、この機能を使用します。

注: このプロパティは、デフォルトでは有効化せずに、ソケットが使用不可の状態になっている場合のみに使用してください。Enterprise Manager が開始した後は、ポートが使用されているのには正当な理由（同じマシン上のコレクタがポートにバインドされている場合など）があるので、このプロパティを無効化します。

SSL の構成

Enterprise Manager を SSL を使うように設定するには、セキュアな通信チャネルを有効にするように、*IntroscopeEnterpriseManager.properties* を設定します。これはデフォルトのセキュアでないチャネルに加えて設定できます。

以下は、セキュアな通信チャネルとセキュアでない通信チャネルの両方を有効にする例です。ポート **5001** にデフォルトのセキュアでないリスナ、およびポート **5443** にセキュアなリスナを設定します。

```
# The enabled communication channels.
introscope.enterprisemanager.enabled.channels=channel1, channel2

# The default communication channel.
introscope.enterprisemanager.serversocketfactory.channel1=com.wily.isengard.p
ostofficehub.link.net.server.DefaultServerSocketFactory
introscope.enterprisemanager.port.channel1=5001

# The secure communication channel.
introscope.enterprisemanager.serversocketfactory.channel2=com.wily.isengard.p
ostofficehub.link.net.server.SSLServerSocketFactory
introscope.enterprisemanager.port.channel2=5443

# Location of a keystore containing certificates for authenticating the Enterprise
Manager to clients.
# Either an absolute path or a path relative to the config directory.
# On Windows, backslashes must be escaped. For example:
#
introscope.enterprisemanager.keystore.channel1=C:\¥¥Introscope¥¥config¥¥intern
al¥¥server¥¥keystore
introscope.enterprisemanager.keystore.channel2=internal/server/keystore
# The password for the keystore.
# Set this property to true to enable encryption of
introscope.enterprisemanager.keypassword.channel2
# Once introscope.enterprisemanager.keypassword.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the existing
encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
introscope.enterprisemanager.keypassword.channel2.plaintextpassword=true
introscope.enterprisemanager.keypassword.channel2=password
# Location of a truststore containing trusted client certificates.
```

```
# Either an absolute path or a path relative to the config directory.
# On Windows, backslashes must be escaped. For example:
#
introscope.enterprisemanager.truststore.channel1=C:\¥¥Introscope¥¥config¥¥inte
rnal¥¥server¥¥keystore
# A truststore is only needed if client authentication is required.
# Set this property to true to enable encryption of
introscope.enterprisemanager.trustpassword.channel2
# Once introscope.enterprisemanager.trustpassword.channel2 is encrypted,
# this property is automatically set to false.
#
# To change the existing password, enter the new password and set this property
to true.
# Note: If this property is set to true and the password is not changed, the existing
encrypted password will be encrypted again.
# If password field for a new channel is configured, add the corresponding
# plaintextpassword field and set it to true to enable encryption.
# introscope.enterprisemanager.trustpassword.channel2.plaintextpassword=false
# The password for the truststore
#introscope.enterprisemanager.trustpassword.channel2=password
# If no truststore is specified, the Enterprise Manager trusts all client
certificates.
```

SSL プロパティルール

SSL サーバ ソケットを使用するように Enterprise Manager を設定するには、デフォルトのチャンネルに加えてセキュアな通信チャンネルを有効にするように、*IntroscopeEnterpriseManager.properties* に設定します。

SSL プロパティを設定する場合、以下のルールに従います。

- キーストア プロパティはキーストアの場所です。これには、自身をクライアントに対して認証するために Enterprise Manager が使用する証明書が含まれている必要があります。Enterprise Manager のデフォルトのキーストアには、本質的に信頼されない自己署名証明書が含まれています。Workstation とエージェントはデフォルトでサーバ証明書を検証しないので、これは問題ではありません。

- キーストア プロパティは、絶対パスまたは *config* ディレクトリを基準にした相対パスのどちらかです。
- *needclientauth* プロパティが *true* に設定されている場合、Enterprise Manager はクライアントに認証するよう要求します。
 - Enterprise Manager はトラストストアで構成する必要があります。
 - エージェントと Workstation は、Enterprise Manager によって信頼された証明書を含むキーストアを使用して構成する必要があります。
 - *needclientauth = true* の場合にトラストストアが設定されていないと、Enterprise Manager は起動しません。
 - 起動するには、トラストストア プロパティの設定が必要です。
- トラストストア プロパティはトラストストアの場所です。ここには信頼されるクライアントの証明書が含まれます。これが必要なのは、クライアントが認証を要求された場合のみです。
 - トラストストアを指定しないと、すべてのクライアントが信頼されます。
- *ciphersuites* プロパティを使用して、有効な暗号スイートを設定します。
 - これは、匿名認証を有効にしたり、データ暗号化を回避したりする場合に使用できます。たとえば、匿名認証のために、暗号スイートを *SSL_DH_anon_WITH_RC4_128_MD5* に設定します。例：
`introscope.enterprisemanager.ciphersuites.channel2=SSL_DH_anon_WITH_RC4_128_MD5`
 - 特定の JSSE 実装には、匿名認証を使用できるいくつかの暗号スイート（すべて「*anon*」が含まれています）があります。ただし、暗号スイートはクライアントとサーバで共通であり、両方で有効です。
 - データを暗号化しない暗号スイートを指定します。例：
`introscope.enterprisemanager.ciphersuites.channel2=SSL_RSA_WITH_NULL_SHA`

ファイアウォールを越えた Enterprise Manager との接続

HTTP トンネリングはデフォルトで有効になっています。トンネリングにより、あるネットワークのデータをほかのネットワーク接続経路で送信できるようになります。

Workstation でトンネリング転送を使用するには、Enterprise Manager の組み込み Web サーバのポートに接続します。デフォルトでは、ポートは 8081 です。これは、Enterprise Manager のプロパティ ファイル内の、`introscope.enterprisemanager.webserver.port` プロパティを使用して設定できます。詳細については、「[introscope.enterprisemanager.webserver.port \(P. 487\)](#)」を参照してください。

Enterprise Manager にトンネリングを使用することに加えて、トンネル技術を使用して情報を送信するようにエージェントを構成できます。この機能を使用すると、エージェントは Enterprise Manager へリモートで接続できます。エージェントの HTTP トンネリングの詳細については、「[CA APM Java Agent 実装ガイド](#)」を参照してください。

Enterprise Manager Web サーバの HTTPS 用の設定

Enterprise Manger Web サーバを HTTPS 用に設定するには、Jetty 設定ファイルを使用します。Jetty ファイルは詳細な構成のために提供されており、`<EM_Home>/config` ディレクトリにあります。

このファイルをアクティブにするには、`IntroscopeEnterpriseManager.properties` ファイルの `introscope.enterprisemanager.webserver.jetty.configurationFile` プロパティのコメント化を解除します。

構成の詳細については、以下のトピックを参照してください。

- 「[デフォルトの Jetty 構成ファイル \(P. 49\)](#)」および「[Jetty-config.xml ファイルの変更 \(P. 50\)](#)」
- 詳細については、Jetty の Web サイト (<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL>) を参照してください。

HTTPS の動作の仕組みの理解

Enterprise Manager Web サーバは、SSL の HTTP トンネリングをサポートしています。このセキュリティ対策を実装するには、Enterprise Manager に組み込まれている Jetty Web サーバ用にオプションの Jetty XML 設定ファイルを導入します。

起動時に、Enterprise Manager は Jetty 設定ファイルをロードします。このファイルは、ポート 8444 にセキュアなリスナを設定します。このセキュアなリスナによって、Workstation とエージェントが Enterprise Manager Web サーバ経由で HTTPS トンネルを使用して Enterprise Manager にアクセスできます。デフォルトの Jetty 設定ファイルは `em-jetty-config.xml` です。

Jetty 設定ファイルの名前および場所は、`IntroscopeEnterpriseManager.properties` ファイルの [introscope.enterprisemanager.webserver.jetty.configurationFile](#) (P. 490) プロパティを使用して設定できます。

`introscope.enterprisemanager.webserver.port` プロパティは、`IntroscopeEnterpriseManager.properties` ファイルにある `introscope.enterprisemanager.webserver.port` プロパティと共に動作します。Enterprise Manager は、Enterprise Manager が Jetty 設定ファイルをロードしたときに、`introscope.enterprisemanager.webserver.port` プロパティで定義されているセキュアでないリスナを作成しません。ただし、Jetty 設定ファイルにはセキュアでないリスナを設定できます。

警告： `em-jetty-config.xml` ファイル内の `introscope.enterprisemanager.webserver.jetty.configurationFile` プロパティおよびセキュアでないリスナ ポートの両方のコメント化を解除すると、CA APM のセキュリティに問題が発生することがあります。これらの設定を一緒に行う前に、組織のアプリケーションセキュリティ担当者に通知してください。

デフォルトの Jetty 構成ファイル

デフォルトの `em-jetty-config.xml` ファイルは `<EM_Home>/config` ディレクトリにあります。

em-jetty-config.xml ファイルの変更

em-Jetty-config.xml ファイル内の SSL の多くのコンポーネントを変更できます。

Jetty の詳細については、

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL> を参照してください。

- HTTPS ポートをデフォルトの 8444 から変更するには、以下の例のように、*port* 属性の値を変更します。

```
<Set name="port">8444</Set>
```

- `introscope.config` システム プロパティは、`config` ディレクトリの場所を指定します。この場所は設定可能です。Enterprise Manager Web サーバは、起動時に `introscope.config` システム プロパティを設定します。

- デフォルトで、SSL リスナは、`/internal/server/keystore` にあるキーストアを使用するように設定されます。これは `config` ディレクトリを基準にした相対パスです。このキーストアには、信頼されない自己署名証明書が入っています。キーストアを、承認された認証局 (CA) が署名した証明書が含まれるキーストアと置き換えます。

- デフォルトのキーストアパスワードは `password` です。

`em-jetty-config.xml` および `webview-jetty-config.xml` 内のクリア テキストパスワードはデフォルトでは難読化されます。難読化されたパスワードは、`OBF:` で始まります。`OBF:` を取り除くことで、プレーンテキストパスワードになります。詳細については、

<http://docs.codehaus.org/display/JETTY/How+to+configure+SSL> を参照してください。

- デフォルトでは、SSL は自己署名証明書を受け入れるように設定されます。SSL は、クライアントの URL 内のホスト名がデジタル証明書のホスト名に一致することを検証しません。これは SSL が、何も設定しなくても、デフォルトのキーストアの信頼されない証明書を使って動作するようにするためです。安全性の高い認証を必要とする場合は、信頼できる証明書を含むキーストアを作成します。その後、XML 内の以下の属性を設定し、デフォルトのキーストアを独自のキーストアに置き換えます。

```
<Set name="validateCertificates">true</Set>
<Set name="verifyHostnames">true</Set>
<Set name="keystore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="password">password</Set>
```

- さらに、クライアント認証を要求する場合は、クライアント証明書を含むトラストストアを作成し、これらの属性を XML に設定し、デフォルトのトラストストアを独自のトラストストアに置き換えます。

```
<Set name="needClientAuth">true</Set>
<Set name="truststore"><SystemProperty name="introscope.config"
default="./config" />/internal/server/keystore</Set>
<Set name="trustPassword">password</Set>
```

- クライアント認証が必要な場合、エージェントと Workstation は、Enterprise Manager Web サーバによって信頼された証明書を含むキーストアを使って構成する必要があります。

有効な暗号スイートを設定するには、*cipherSuites* 属性を暗号スイートのリストに設定します。

```
<Set name="cipherSuites">
  <Array type="java.lang.String">
    <Item>SSL_DH_anon_WITH_RC4_128_MD5</Item>
  </Array>
</Set>
```

SSLを使用するには、エージェントと Workstation の暗号スイートが有効で、Enterprise Manager と共通のものである必要があります。以下のアクションに対して、有効な暗号スイートを制限することができます。

- 弱い暗号スイートの脆弱性の防止
- 匿名接続の許可
- データの非暗号化
- Enterprise Manager は maxThreads プロパティを使用して、Enterprise Manager が処理できる HTTPS エージェント接続の数を制限します。十分なスレッドがない場合、Enterprise Manager は、接続されたエージェントやエージェントからのプロセスメトリックを認識しません。

HTTPS を使用する場合、Enterprise Manager は `maxThreads` プロパティで設定されたエージェント数のみを処理します。許可されているエージェント接続の数は、`apm-events-thresholds-config.xml` ファイルの [introscope.enterprisemanager.agent.connection.limit](#) プロパティ (P. 543) で設定されます。 `maxThreads` の値が

`introscope.enterprisemanager.agent.connection.limit` の値以上であることを確認します。エージェントが HTTPS を介して接続するように設定されている場合、スレッドが不足すると、一部の HTTPS エージェントがクライアントに表示されないか、メトリックをレポートしない可能性があります。

注: `maxThreads` プロパティで Enterprise Manager が処理するエージェントの数を制限している場合、Enterprise Manager およびエージェントログには処理対象外のエージェントに関するエラー、警告、またはメッセージは含まれません。

デフォルト ヘッダ サイズをリセットするための `em-jetty-config.xml` の変更

CEM コンソールへのアクセス時に空白のページが表示されることがあるような場合は、要求ヘッダ サイズ制限のデフォルト値 (4 KB) をリセットすることができます。ヘッダ サイズ制限のリセットは、`em-jetty-config.xml` ファイルで行います。

以下の手順に従います。

1. MOM 上の `em-jetty-config.xml` ファイルの場所に移動し、テキストエディタで開きます。
2. 以下の行を含むセクションを見つけます。

```
<New class="com.wily.webserver.NoNPESocketConnector">
```
3. "NoNPESocketConnector" を以下の値に変更します。

```
<set name="headerBufferSize">8192</Set>"  
<Set name="RequestBufferSize">16384</Set>"
```

変更後のセクションは、以下のコード スニペットのようになります。

```
<Call name="addConnector">
  <Arg>
    <New class="com.wily.webserver.NoNPESocketConnector">
      <Set name="port">8081</Set>
      <set name="headerBufferSize">8192</Set>
      <Set name="RequestBufferSize">16384</Set>
      <Set name="ThreadPool">
        <New class="org.mortbay.thread.BoundedThreadPool">
          <Set name="minThreads">10</Set>
          <Set name="maxThreads">100</Set>
          <Set name="maxIdleTimeMs">60000</Set>
        </New>
      </Set>
    </New>
  </Arg>
</Call>
```

4. ファイルを保存して閉じます。
5. 各 MOM およびコレクタ上の IntroscopeEnterpriseManager.properties ファイルの場所に移動します。
6. 以下の行のコメント化を解除します。
introscope.enterprisemanager.webserver.jetty.configurationFile=
em-jetty-config.xml
7. IntroscopeEnterpriseManager.properties ファイルを保存して閉じます。

第 4 章: Enterprise Manager データベースの構成

この章では、CA Introscope の内部データベース用の設定オプションについて説明します。

APM データベースの詳細については、「[APM データベースの管理 \(P. 55\)](#)」を参照してください。

このセクションには、以下のトピックが含まれています。

[APM データベースの管理 \(P. 55\)](#)

[SmartStor によるデータ保存の設定 \(P. 75\)](#)

[トランザクションイベント データベースの場所および保存期間 \(P. 79\)](#)

[ベースラインストレージの場所の設定 \(P. 79\)](#)

[SmartStor、ベースライン、およびトランザクション イベント データのバックアップ \(P. 80\)](#)

[SmartStor ツールを使用した SmartStor データのチューニング \(P. 82\)](#)

[SmartStor メタデータの廃棄 \(P. 90\)](#)

[SmartStor データおよびメタデータの削除 \(P. 92\)](#)

[8.x データから 9.x へのアップグレード \(P. 97\)](#)

APM データベースの管理

この章には、APM データベースとの間のデータのエクスポートおよびインポートに関連する情報が含まれています。データベース全体または構成データのみをどちらかをインポートおよびエクスポートできます。

その他の CA Introscope データベース (SmartStor およびトランザクション イベント データベース) については、「[Enterprise Manager データベースの構成 \(P. 55\)](#)」を参照してください。

データベースのバックアップまたはリストア

バックアップおよびリストア機能には、APM データベースおよび構成情報をバックアップする機能が含まれています。

たとえば、データを保護するためにデータベースのコピーを別個のコンピュータに保持できます。このためには、まずデータベースをバックアップしてから、データベース バックアップ ファイルを別のコンピュータにコピーします。

APM データベースのバックアップおよびリストアのプロセス

CA CEM データ保護に関連する主なタスクを以下に示します。

1. [前提条件を理解する](#) (P. 56)。
2. [データベースを定期的にバックアップする](#) (P. 57)。
3. [必要に応じてデータベースをリストアする](#) (P. 59)。

PostgreSQL データベースのバックアップおよびリストアの各ユーティリティは、コマンドラインから実行できるバッチ ファイル(またはシェルスクリプト) の形式で提供されます。

注: APM データベースには、CA CEM 構成の設定、ユーザとグループ、ビジネス サービスとトランザクションの定義、およびアプリケーション問題切り分けマップ データが含まれています。

バックアップまたはリストアの前条件

警告: 指定された名前で作成する前にその指定されたデータベースがすでに存在すると、リストア機能はそのデータベースを破棄します。

バックアップおよびリストアの両方に必要な条件は、以下のとおりです。

- PostgreSQL データベースのバックアップまたはリストアのデータベース スクリプトを実行するマシンには、PostgreSQL がインストールされている必要があります。リモートマシンにも PostgreSQL がインストールされている場合は、必要に応じてそのリモートマシンでスクリプトを実行できます。

以下のいずれかのプラットフォームで APM データベースのリストアを実行する前に :

- OS/400 (IBM)
- Solaris x86

dbrestore スクリプトを実行するマシンに JAVA_HOME 環境変数が設定されていることを確認します。

JRE 1.6 で有効 : JAVA_HOME 環境変数を設定し、その変数が JRE ルートフォルダを指すようにします。JRE 1.6 またはそれ以降が必要です。パスにスペースを入れることはできません。たとえば、JRE が `c:\program files\java\jre1.6.0` にインストールされている場合は、JAVA_HOME を `c:\progra~1\java\jre1.6.0` のような短縮バージョンのパスに設定します。

データベースのバックアップ

バックアップユーティリティは、APM データベースの `.backup` ファイルを作成します。バックアップファイル名はカスタマイズできます。ファイル名を指定しない場合は、スクリプトにより、データベース名とファイル名サフィックス `.backup` から成る名前のバックアップファイルが作成されます。

APM データベースをバックアップする方法

1. ご使用のオペレーティングシステムで `database-scripts` ディレクトリに移動します。
 - Linux : `<EM_Home>/install/database-scripts/unix/`
 - Windows : `<EM_Home>\install\database-scripts\windows\`
2. コマンドラインを開き、ご使用のオペレーティングシステムに合わせて以下のスクリプトを実行します。
 - Windows : `dbbackup-postgres.bat`
 - Linux : `dbbackup-postgres.sh`

以下の構文および引数を使用します。

```
[dbbackup-postgres.bat | sh dbbackup-postgres.sh][dbserverhostip]
[dbinstalldir] [dbname] [dbuser] [dbpassword] [dbport] [outputfile]
```

引数は以下のとおりです。

dbserverhostIP

データベースをホストするマシンの IP アドレス。マシン上で直接実行している場合は、`localhost` を指定できます。

dbinstalldir

APM データベースのディレクトリの場所。

Linux では、パスにスペースが含まれている場合は、エスケープするか、または引用符で囲んでパスを指定する必要があります。Linux では、たとえば、ディレクトリ `/root/Introscope Enterprise Manager` は、`/root/Introscope¥ Enterprise¥ Manager` と表すことができます。

デフォルトを変更しなかった場合、ディレクトリの場所は以下のようになります。

Linux : `opt/database`

Windows : `<EM_Home>¥database`

database_name

データベース インスタンス名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を `cemdb` に設定する必要があります。Oracle を使用する場合、この引数を Oracle システム識別子 (SID) に設定する必要があります。

dbuser

APM データベースと関連付けるデータベース ユーザのユーザ名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を `admin` に設定する必要があります。Oracle を使用する場合、この引数を APM データベース スキーマ所有者に設定する必要があります。

注: これは、PostgreSQL データベース管理者のユーザ名ではありません。

password

APM データベースと関連付けるデータベース ユーザのパスワードを指定します。

port_number

データベースが Enterprise Manager およびその他のコンポーネントと通信するときのポート番号を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を `5432` に設定する必要があります。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を `1521` に設定する必要があります。

dbbackupdir

データベース バックアップ ファイルを保存する既存のディレクトリの場所。Linux では、パスにスペースが含まれている場合は、エスケープ処理したパスを指定する必要があります。Linux では、たとえば、ディレクトリ */root/Introscope Enterprise Manager* は、*/root/Introscope¥ Enterprise¥ Manager* と表すことができます。

ディレクトリを引用符で囲むことはできません。また、末尾をスラッシュにすることはできません。

outputfile

(オプション) データベース バックアップ ファイルの名前。このパラメータを指定しない場合は、スクリプトにより、指定されたデータベース名を含む、*dbname.backup* という名前のファイルが生成されます。バックアップ ファイル名のサフィックスは、標準規則では *.backup* ですが、これは必要条件ではありません。

以下は、*/opt/database/backups* ディレクトリに *cemdb.backup* ファイルを生成する例です。

```
sh dbbackup-postgres.sh 127.0.0.1 /opt/database cemdb admin quality
5432 ./backups
```

- バックアッププロセスが完了すると、確認メッセージが表示されます。スクリプトでエラーが発生した場合は、一般的に以下の原因が考えられます。
 - データベース名が正しくありません。
 - PostgreSQL がインストールされていません。
 - APM データベースの場所が正しくありません。

データベースのリストア

リストアユーティリティでは、事前にバックアップ済みの APM データベース バックアップ ファイルを現在のシステムにリストアすることができます。たとえば、システムクラッシュやハードディスク障害後にデータベースをリストアしてリカバリーすることができます。

警告： 指定された名前でデータベースを作成する前にその指定されたデータベースがすでに存在すると、リストア機能はそのデータベースを破棄します。

注: データベースが UNIX マシン上にある場合は、リストアプロセスによりデータベースのアップグレードも実行されます。

注: データベースのリストアに要する時間は、データベースのサイズに直接関連します。データベースが大きいほどリストアに要する時間は長くなります。また、リストア時間はマシンのキャパシティとメモリによっても異なります。たとえば、1 GB のデータベースのリストアは、マシンリソースに応じて、1～2 時間かかることがあります。

APM データベースをリストアする方法

1. データベースに接続しているユーザがないことを確認します。データベースに接続しているユーザがいる場合、データベースをリストアできません。
2. ご使用のオペレーティングシステムで `database-scripts` ディレクトリに移動します。
 - Linux : `<EM_Home>/install/database-scripts/unix/`
 - Windows : `<EM_Home>%install%database-scripts%windows%`

3. コマンドラインを開き、ご使用のオペレーティング システムに合わせて以下のスクリプトを実行します。

- Windows : *dbrestore-postgres.bat*

- Linux : *dbrestore-postgres.sh*

以下の構文および引数を使用します。

```
[dbrestore-postgres.bat | sh dbrestore-postgres.sh][dbserverhostip]
[dbinstalldir] [dbserviceuser] [dbservicepassword] [dbname] [dbuser]
[dbpassword] [dbport] [backupfile]
```

引数は以下のとおりです。

dbserverhostIP

データベースをホストするマシンの IP アドレス。マシン上で直接実行している場合は、*localhost* を指定できます。

dbinstalldir

APM データベースのディレクトリの場所。

Linux では、パスにスペースが含まれている場合は、エスケープするか、または引用符で囲んでパスを指定する必要があります。Linux では、たとえば、ディレクトリ */root/Introscope Enterprise Manager* は、*/root/Introscope¥ Enterprise¥ Manager* と表すことができます。

デフォルトを変更しなかった場合、ディレクトリの場所は以下のようになります。

Linux : *opt/database*

Windows : *<EM_Home>¥database*

dbserviceuser

PostgreSQL 管理者のユーザ名。デフォルトでは、これは *postgres* です。

dbservicepassword

dbserviceuser に関連付けられたパスワード (PostgreSQL 管理者のパスワード)。

database_name

データベース インスタンス名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を *cemdb* に設定する必要があります。Oracle を使用する場合、この引数を Oracle システム識別子 (SID) に設定する必要があります。

dbuser

APM データベースと関連付けるデータベース ユーザのユーザ名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を *admin* に設定する必要があります。Oracle を使用する場合、この引数を APM データベース スキーマ所有者に設定する必要があります。

注: これは、PostgreSQL データベース管理者のユーザ名ではありません。

password

APM データベースと関連付けるデータベース ユーザのパスワードを指定します。

port_number

データベースが Enterprise Manager およびその他のコンポーネントと通信するときのポート番号を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を 5432 に設定する必要があります。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を 1521 に設定する必要があります。

backupfile

データベース バックアップ ファイルのディレクトリの場所および名前。

/opt/database/backups ディレクトリから *cemdb.backup* ファイルをリストアする例を以下に示します。

```
sh dbrestore-postgres.sh 127.0.0.1 /opt/database postgres C@wilyapm90 cemdb
admin quality 5432 ./backups/cemdb.backup
```

4. リストア プロセスが完了すると、確認メッセージが表示されます。

エラーが発生した場合

- よくあるエラーの原因は、ユーザがデータベースにまだ接続していることです。PostgreSQL サーバを再起動することで、エラーが発生した接続を切断できます。
- データベースが存在しないというエラーが表示された場合は、問題ありません。これは、プロセスでデータベースを作成するためにスクリプトが使用されていることを意味します。

データベース構成のエクスポートまたはインポート

初めてインストールするときに CA CEM システムを実運用環境に配置できない場合があります。たとえば、すべての新しいハードウェアおよびソフトウェアを実運用ネットワークに入れる前にテストラボにインストールする、という企業方針があることがあります。

QA 環境またはテスト環境で CA CEM 構成を設定してテストし終えたら、その実証された構成を、CA CEM のエクスポートおよびインポートによって実運用環境に移動します。

構成情報には、ユーザ、ユーザグループ、ビジネス サービス、およびトランザクションが含まれます。

データベース構成のエクスポートおよびインポートのプロセス

CA CEM 構成のエクスポートに関連する主なタスクを以下に示します。

1. [前提条件を理解する](#) (P. 64)。
2. CA CEM [構成をエクスポートする](#) (P. 65)。
3. CA CEM [構成をインポートする](#) (P. 66)。

エクスポートおよびインポートの各ユーティリティは、コマンドラインから実行できるバッチファイル（またはシェルスクリプト）の形式で提供されます。

ビジネス トランザクション定義のインポートおよびエクスポートについては、「[CA APM トランザクション定義ガイド](#)」を参照してください。

APM データベース内の（構成情報だけでなく）すべての情報のバックアップおよびリストアについては、「[データベースのバックアップまたはリストア](#) (P. 56)」を参照してください。

データベース構成データをエクスポートまたはインポートする場合の前提条件

警告： 警告：2つのユーティリティを実行する場合は事前に APM データベースをバックアップしておくことを強くお勧めします（特にインポートでは、再構築する前に既存の構成が破棄されます）。インポートスクリプトによりデータベースが破壊され、最終的にデータベースには古いデータベースの構成データのみが含まれます。詳細については、「[データベースのバックアップまたはリストア \(P. 56\)](#)」を参照してください。

エクスポートおよびインポートの両方に必要な条件は、以下のとおりです。

- APM データベースがインストールされているマシンでスクリプトを実行します。
- Enterprise Manager インストーラによって配置された場所でスクリプトを実行します。スクリプトがこの場所から相対パスでファイルを参照するためです。
- これらのスクリプトを実行する前に、APM データベースへの接続をすべて切断します。Enterprise Manager をシャットダウンし、データベース管理ツール（pgAdmin など）を閉じて、すべてのユーザがログオフしていること、または CEM コンソールを閉じていることを確認します。TIM を無効にする必要はありませんが、インポート後に再度有効にする必要があることに注意してください。
- JRE 1.6 以降で有効：JAVA_HOME 環境変数を設定し、その変数が JRE ルートフォルダを指すようにします。JRE 1.6 またはそれ以降が必要です。パスにスペースを入れることはできません。たとえば、JRE が `c:\program files\java\jre1.6.0` にインストールされている場合は、JAVA_HOME を `c:\progra~1\java\jre1.6.0` のような短縮バージョンのパスに設定します。
- CA CEM の以前のバージョンから構成をインポートする場合は、Linux では以前の任意のバージョンをインポートできますが、Windows でインポートできるバージョンは 5.0 バージョン以降のみであることに注意してください。インポートユーティリティにより、データベーススキーマは古いリリースから現在のリリースに自動的にアップグレードされます。

APM データベース構成のエクスポート

configexport.bat または *configexport.sh* スクリプトは、CA CEM 構成情報をすべて含む XML ファイルを作成します。構成情報には、ユーザ、ユーザグループ、ビジネス サービス、およびトランザクションが含まれます。実稼働システム用のベースとして、構成情報をエクスポートしてテストまたはラボシステムからデータを移動することができます。

APM データベース構成をエクスポートする方法

1. \$JAVA_HOME 環境変数を設定します。
2. ご使用のオペレーティングシステムで
<EM_Home>/install/database-scripts ディレクトリに移動します。例：
cd /home/Introscope9.0.5.0/install/database-scripts/unix
3. コマンドまたはターミナル ウィンドウを開き、以下の引数を使用して、Windows では *configexport.bat*、その他のプラットフォームでは *configexport.sh* を実行します。
ConfigExport <dbhostIP> <database_name> <dbuser> <password> <port_number>
<databasetype> <export-file>

dbhostIP

データベースをホストするコンピュータの IP アドレスを指定します。このコマンドに localhost を使用することはできません。

database_name

データベース インスタンス名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を **cemdb** に設定します。Oracle を使用する場合、この引数を Oracle システム識別子 (SID) に設定します。

dbuser

APM データベースと関連付けるデータベース ユーザのユーザ名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を **admin** に設定します。Oracle を使用する場合、この引数を APM データベース スキーマ所有者に設定します。

注: これは、PostgreSQL データベース管理者のユーザ名ではありません。

password

APM データベースと関連付けるデータベース ユーザのパスワードを指定します。

port_number

データベースが Enterprise Manager およびその他のコンポーネントと通信するときのポート番号を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を 5432 に設定する必要があります。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を 1521 に設定する必要があります。

databasetype

使用しているデータベースのタイプを指定します。この引数を postgres または oracle に設定します。

export-file

エクスポートされたデータを含む XML ファイルの絶対パスおよびファイル名を指定します。

たとえば、Linux で *configexport* プログラムを実行するには、以下のようなコマンドラインを使用します。

```
./configexport.sh 197.168.144.10 arcade apmdba mypwd 1521 oracle  
/home/apmdba/export_oracle.xml
```

4. 構成のエクスポートプロセスが完了すると、確認メッセージが表示されます。

APM データベース構成のインポート

APM データベース間で構成設定をインポートできます。たとえば、*configimport.bat* または *configimport.sh* プログラムを使用して、QA システムから実運用システム上にデータベース構成をインポートできます。インポートされる構成設定にはユーザおよびユーザグループ、ビジネスサービスおよびトランザクションが含まれます。

APM データベース構成のインポートプロセスでは、以下の処理が実行されます。

- 以前のデータベース構成情報（オペレータ、ユーザ、グループ、ビジネスサービスプロセス、およびトランザクション定義に関する情報）が削除され、インポートされた構成データに置き換えられます。
- 障害、レポート、および統計データが削除されます。これらのデータは置き換えられません。

注: 構成は、以前のバージョンの CA CEM からインポートできます。たとえば、CA CEM 4.1 から構成をダウンロードしてエクスポートし、CA CEM 4.2 にアップロードしてインポートできます (Linux のみ)。

以下の手順に従います。

1. ご使用のオペレーティング システムで
<EM_Home>/install/database-scripts ディレクトリに移動します。例：
cd /home/Introscope9.0.5.0/install/database-scripts/unix
2. コマンドまたはターミナル ウィンドウを開き、以下の引数を使用して、
Windows では *configimport.bat*、その他のプラットフォームでは
configimport.sh を実行します。

```
ConfigImport -dbhost <ホスト名> -dbname <データベース名> -dbport <ポート番号>  
-databasetype <データベース タイプ> -dbuser <データベース ユーザ> -dbpassword <パス  
ワード> -dbscriptsdir <ディレクトリ> -importfile <インポート ファイル名>  
-targetRelease <ターゲット リリース> -dbserviceuser <データベース サービス ユーザ>  
-dbservicepwd <データベース サービス パスワード> [-postgresinstalldir <postgres イ  
ンストール ディレクトリ>] [-nolog] [-jdbcbatchsize <jdbc バッチ サイズ>]  
[-promptbeforeimport true|false] [-is64Bit true|false]
```

dbhost

データベースをホストするコンピュータのホスト名または IP アドレスを指定します。このコマンドに *localhost* を使用することはできません。

dbname

データベース インスタンス名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を *cemdb* に設定します。Oracle を使用する場合、この引数を Oracle システム識別子 (SID) に設定します。

dbport

データベースが Enterprise Manager およびその他のコンポーネントと通信するときのポートを指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を 5432 に設定します。Oracle を使用しており、デフォルトリスナポートを変更しなかった場合、この引数を 1521 に設定します。

databasetype

使用しているデータベースのタイプを指定します。引数を *postgres* または *oracle* に設定します。

dbuser

APM データベースと関連付けるデータベース ユーザのユーザ名を指定します。PostgreSQL を使用しており、デフォルトを変更しなかった場合、この引数を *admin* に設定します。Oracle を使用する場合、この引数を APM データベース スキーマ所有者に設定します。

dbpassword

APM データベースと関連付けるデータベース ユーザのパスワードを指定します。

dbscriptsdir

データベース固有の SQL スクリプトのディレクトリを指定します。たとえば、Oracle データベース スキーマを使用する場合は `<EM_Home>/install/oracle/database-scripts`、PostgreSQL データベースを使用する場合は `<EM_Home>/install/database-scripts` を使用します。

importfile

インポートするデータを含む XML ファイルの絶対パスおよびファイル名を指定します。

dbserviceuser

PostgreSQL 管理サービス ユーザ アカウントを指定します。デフォルトの管理サービス アカウントは *postgres* です。この引数は Oracle では使用できません。

dbservicepwd

PostgreSQL 管理サービス ユーザ アカウントのパスワードを指定します。

postgresinstalldir

(オプション) PostgreSQL を使用する場合、APM データベースのディレクトリの場所を指定します。Linux または Solaris では、パスにスペースが含まれる場合、パスは引用符で囲むか、またはエスケープシーケンスを含める必要があります。たとえば、ディレクトリが `/root/Introscope Enterprise Manager` である場合、
「`/root/Introscope Enterprise Manager`」または
「`/root/Introscope¥ Enterprise¥ Manager`」として場所を指定できます。

デフォルトを変更しなかった場合、場所は、32 ビット Linux または Solaris の場合は `opt/databas`、64 ビット Linux または Solaris の場合は `opt/database/postgres/8.3-community`、または Windows の場合は `<EM_Home>¥database` です。

この引数は Oracle では使用できません。

targetRelease

インポートするターゲットリリースを指定します。たとえば、9.0.5.1 設定ファイルをインポートできますが、DB を 9.1.0.0 にアップグレードしたい場合があります。

nolog

(オプション) 標準出力 (StdOut) へのログ記録をオフにすることを指定します。

jdbcbatchsize

(オプション) JDBC (Java DataBase Connectivity) を通じて一度に転送するデータ パケットの最大サイズを指定します。デフォルト値は 2500 です。

promptbeforeimport

(オプション) *configimport* プログラムでデータのインポートを開始する前に、プロンプトを表示するかどうかを指定します。プロンプトを表示する場合は、このパラメータを *true* に設定します。デフォルト値は *false* です。

is64Bit

(オプション) PostgreSQL データベースが 32 ビットか 64 ビットかを指定します。64 ビット PostgreSQL データベースへデータをインポートする場合、このパラメータを *true* に設定します。この引数は Oracle データベースでは使用できません。

たとえば、Linux の PostgreSQL データベース上で *configimport* プログラムを実行するには、以下のようなコマンドラインを使用します。

```
./configimport.sh -dbhost sfqa07 -dbname cemdb -dbport 5432 -databasetype postgres -dbuser admin -dbpassword mypassword -dbscriptsdir /apps/Introscope/install/database-scripts -importfile /tmp/apm_data.xml -dbserviceuser postgres -dbservicepwd %pas5w0rd -postgresinstalldir /opt/database -promptbeforeimport true
```

インポート スクリプトは、初期検証チェックを実行して、XML の形式が正しいことを確認します。

インポート スクリプトには、XML コンテンツを正常に処理できるように XML をさらに徹底的に検証するオプションも用意されています。「Y」を入力すると検証が実行されます。「N」を入力すると、XML コンテンツを検証せずにインポートが続行されます。

注: この 2 番目の検証は、XML ファイルのサイズに応じて、時間がかかることがあります。XML データを正常にインポートできることを確認することが重要です。正常にインポートできないと、エラーが発生します。

スクリプトでは、進捗状況メッセージが表示されます。検証が完了してインポートが開始したとき、およびインポートが完了したときに、メッセージが表示されます。

どちらかの検証チェックが失敗すると、エラーメッセージが表示され、構成のインポートは停止します。両方の検証チェックが成功すると、スクリプトによって、指定されたデータベース構成データがインポートされます。

重要: 設定のインポートでは、既存の HTTP アナライザプラグインの設定はインポートされません。プラグインを手動でインストールするには、CEM コンソールを使用します。

別のオペレーティングシステムへの APM データベースの移動

アップグレードプロセスの一部としてあるコンピュータから別のコンピュータ、またはあるプラットフォームから別のプラットフォームに APM データベースを移動する場合があります。たとえば、Windows または Linux 上の PostgreSQL から Solaris 上の PostgreSQL に APM データベースを移動する場合があります。あるプラットフォームから別のプラットフォームにデータベースを移動するには、ソースデータベースからビジネストランザクションおよび構成データをエクスポートして、次にそのビジネストランザクションと構成データを新しいプラットフォーム上のターゲットデータベースへインポートします。あるいは、*dbbackup-postgres* および *dbrestore-postgres* ユーティリティを使用して、既存の PostgreSQL データベースの完全なバックアップを作成し、新しいコンピュータ上のデータベースへリストアすることができます。

PostgreSQL データベースからのデータのエクスポートおよびインポート、または *dbbackup-postgres* および *dbrestore-postgres* ユーティリティの使用の詳細については、「CA APM 設定および管理ガイド」を参照してください。[PostgreSQL データベースから Oracle データベースへのデータの移動 \(P. 72\)](#)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。

PostgreSQL データベースから Oracle データベースへのデータの移動

データベースをアップグレードして PostgreSQL から Oracle データベースにデータを移行する場合は、最初にアップグレードを実行します。たとえば、組織で使用するデータベース プラットフォームが Oracle に統一されている場合、実運用レベルで監視できるようにするには、APM データベースを Oracle へ移行します。PostgreSQL にあるソース データベースから Oracle にあるターゲット データベースに既存のデータを移動する場合、CA APM 移行ユーティリティを使用してソースおよびターゲット データベースを指定できます。

PostgreSQL データベースから Oracle データベースへ移行する方法

1. アップグレード シナリオおよびアップグレード パスを確認して、アップグレードのための計画および準備をします。
2. すべてのコンポーネントのバックアップ コピーを作成します。
3. 対話型あるいはサイレント Enterprise Manager インストーラを使用して、Enterprise Manager および APM データベースをアップグレードします。
4. `<EM_Home>/install/migration` ディレクトリに移動します。
5. 運用環境に応じ、以下の引数を使用して `migration.bat` または `migration.sh` スクリプトを実行します。

```
migration -srcDatabaseName <データベース名> -srcDatabaseType <データベース タイプ>
-srcHost <ホスト名> -srcPort <ポート番号> -srcUser <ユーザ名> -srcPassword <パスワード> -tgtDatabaseName <ターゲット データベース名> -tgtDatabaseType <データベース タイプ> -tgtHost <ホスト名> -tgtPort <ポート番号> -tgtUser <ユーザ名> -tgtPassword <パスワード>
```

srcDatabaseName

ソース データベースの名前を指定します。デフォルト設定を使用した場合、データベース名は `cemdb` です。

srcDatabaseType

ソース データベース タイプを指定します。このリリースでは、唯一の有効な値は `postgres` です。

srcHost

ソース データベースのデータベース サーバのホスト名または IP アドレスを指定します。

srcPort

ソース データベースへの接続用のポート番号を指定します。デフォルト設定を使用した場合、ポートは **5432** です。

srcUser

ソース データベースのデータベース ユーザ名を指定します。デフォルト設定を使用した場合、データベース ユーザ名は **admin** です。

srcPassword

ソース データベースのデータベース ユーザのパスワードを指定します。

tgtDatabaseName

ターゲット データベースの名前またはサービス アカウント識別子を指定します。Oracle データベースの場合、ターゲット データベースの名前は一意のシステム識別子 (SID) です。

tgtDatabaseType

ターゲット データベース タイプを指定します。このリリースでは、有効な値は **oracle** のみです。

tgtHost

ターゲット データベースのデータベース サーバのホスト名または IP アドレスを指定します。

tgtPort

ターゲット データベースへの接続用のポート番号を指定します。デフォルト設定を使用した場合、ポートは **1521** です。

tgtUser

ターゲット データベースのデータベース ユーザ名を指定します。

tgtPassword

ターゲット データベースのデータベース ユーザのパスワードを指定します。

注: すべての引数は移行ツールを実行するのに必須であり、大文字と小文字が区別されます。

たとえば、PostgreSQL データベース *cemdb* から、SID が *orcl* でスキーマ所有者が *apmdb* である Linux コンピュータ上の Oracle データベースにデータを移動するには、以下のようなコマンドラインになります。

```
./migration.sh -srcDatabaseName cemdb -srcDatabaseType postgres -srcHost nyc16  
-srcPort 5432 -srcUser admin -srcPassword quality -tgtDatabaseName orcl  
-tgtDatabaseType oracle -tgtHost nyc23 -tgtPort 1521 -tgtUser apmdb -tgtPassword  
cent3R
```

6. スキーマが適切に移行されたことを確認するか、または移行に関する問題をトラブルシューティングするには、*logs* ディレクトリにある *migration.log* ファイルを確認します。たとえば、
<EM_Home>/install/migration/logs ディレクトリに移動します。

注: <EM_Home>/install/migration/log4j-migration.properties ファイル内の *log4j.appender.logfile.File* プロパティを変更することで、*migration.log* ファイルの場所を変更できます。移行およびログファイルプロパティのカスタマイズの詳細については、「移行プロパティのカスタマイズ」を参照してください。

データベースのトラブルシューティング

このトピックでは、データベースのトラブルシューティングに役立つヒントを示します。

症状:

APM データベースを実行しているマシン上に多くのデータベース (PostgreSQL または Oracle) プロセスがあります。これは正常ですか?

解決方法:

データベース プロセス (PostgreSQL または Oracle) は APM データベースへの各クライアント接続に対して作成されます。そのため、多くの異なるデータベース プロセスが同時に実行されるのは正常です。

SmartStor によるデータ保存の設定

SmartStor は、実運用環境で稼働している間、すべてのアプリケーションのパフォーマンス データ (Introscope メトリック) を外部データベースを使用せずに常時記録します。外部データベースを使わずに、履歴データを分析してアプリケーション ダウンタイムの根本原因を特定したり、キャパシティの分析を行ったりすることができます。SmartStor は Introscope のインストール時にデフォルトで有効に設定されます。

1 時間に 1 回、正時に、SmartStor は、クエリ処理を最適化するために .spool ファイルを .data ファイルに変換します。

1 日に 1 回、午前 0 時に、SmartStor は Enterprise Manager 層設定に基づいて履歴メトリック データを再フォーマットし、エイジアウトしたメトリックおよびメタデータを削除します。

以下は、IntroscopeEnterpriseManager.properties ファイル内のデフォルトの層設定です。

```
introscope.enterprisemanager.smartstor.tier1.frequency=15
```

```
introscope.enterprisemanager.smartstor.tier1.age=7
```

```
introscope.enterprisemanager.smartstor.tier2.frequency=60
```

```
introscope.enterprisemanager.smartstor.tier2.age=30
```

```
introscope.enterprisemanager.smartstor.tier3.frequency=900
```

```
introscope.enterprisemanager.smartstor.tier3.age=365
```

SmartStor では、最近使用されたデータが最も頻繁にアクセスされるデータであり、精度が最も高いと仮定したストレージ階層が使用されます。以下は、上記のデフォルト プロパティ設定に基づいたデータ精度です。

15 秒のチャンクで 1 週間分のデータを保存 (非圧縮)

1 分 (60 秒) のチャンクで 30 日分のデータを保存 (圧縮)

15 分 (900 秒) のチャンクで 1 年分のデータを保存 (圧縮)

重要: 専用のディスクに書き込むように SmartStor を設定して、Enterprise Manager のパフォーマンスおよび応答性に重大な影響を与えないようにします。Enterprise Manager のほかのアクティビティや、ホストで実行中のほかのプロセスとのディスク競合は、パフォーマンスの低下を引き起こす可能性があります。

SmartStor データ専用のディスクをセットアップする場合、このプロパティを true に設定します。Enterprise Manager インストーラは、デフォルトではこのプロパティを false に設定します。

「[introscope.enterprisemanager.smartstor.dedicatedcontroller](#) (P. 503)」を参照してください。

以下のセクションでは、SmartStor の計画および設定について説明します。

- [SmartStor のシステム要件の判断](#) (P. 77)
- [SmartStor のデータ層の値の指定](#) (P. 78)

SmartStor 層の動作の詳細

SmartStor 内の層は、メトリックデータの保存期間を定義します。最大で 3 つの層を持つことができ、各層の保存間隔は同じか増加します。第 1 層は最小の保存期間です。これは保存間隔 (秒単位) および保存期間 (日単位) で構成されます。第 1 層の保存期間の設定に基づいて第 2 層を設定します。第 2 層は第 1 層の「サマリ」であり、第 3 層は第 2 層の「サマリ」になると解釈してください。

例 :

| | 頻度 (15 秒の倍数) | 保存期間 (日数) |
|-------|-----------------|--------------|
| 第 1 層 | 15 | 7 |
| 第 2 層 | 15 | 14 |
| 第 3 層 | 30 | 10 |

SmartStor は一晩ごとに再時間区分され、メトリック データのアーカイブ ファイル (A1 と呼びます) が収集されます。新しいアーカイブ (A1) は第 1 層「バケット」に入り、7 日間そこにとどまります。8 日目に、A1 は第 2 層にプロモートされます。保存間隔に変更はありません。保存間隔はメトリック レポートの精度を表します。A1 はさらに 14 日間第 2 層に保存されます。15 日目に、A1 は第 3 層にプロモートされます。データの保存間隔が 30 秒に変更されます。メトリック データを表示した場合、それは 15 秒単位ではなく 30 秒単位で表示されます。A1 は第 3 層に 10 日間保存され、その後は SmartStor から削除されます。合計で、A1 は 31 日間 SmartStor に保存されていました。

メタデータの自動削除

SmartStor の再時間区分中に、Enterprise Manager は、関連するメトリック データ ポイントがないメタデータ (メトリック およびエージェントの説明) を自動的に削除します。このプロセスは、SmartStor の階層化時に、再利用できるようにディスクおよびメモリ容量を解放します。SmartStor 層の期間は `IntroscopeEnterpriseManager.properties` ファイルで設定されず。

Enterprise Manager は、SmartStor 内にメトリック データを持たないエージェントなど、Workstation に手動でマウントされた履歴エージェントを削除しません。

SmartStor のシステム要件の判断

SmartStor のシステム要件を確定するために SmartStorSizing スプレッドシートを使用できます。[このスプレッドシートは CA サポート サイトからダウンロード](#)できます。

メトリック数、および各データ層の保存間隔と保存期間を示す値を、さまざまに変更して試してみることができます。結果は GB 単位の使用量として表示されます。

SmartStor の性能は、使用するオペレーティング システム、JVM、およびファイル システムによって変化します。

各データ層の適切な保存間隔と保存期間が決まったら、SmartStor の適切なプロパティにそれらの値を指定してください。

SmartStor のデータ層の値の指定

SmartStor によるデータ保存を設定するために 3 つのデータ層を指定します。各層には、以下の 1 対のプロパティがあります。

- データ保存間隔（秒単位）
- データ保存期間（日単位）

保存間隔と保存期間の値には、以下の規則が適用されます。

- 保存間隔は、15 秒の倍数にする必要があります。
- 保存間隔は、1800 秒（30 分）を超える値にすることはできません。
- 各層の保存間隔は、前の層の保存間隔の偶数倍にする必要があります。この倍数は 1 にも設定できるので、すべての層の保存間隔を同じにすることも可能です。
- 保存期間を 0 にすることはできません。
- 3 つの層のすべてを定義する必要があります（3 つを超える数の層を定義することはできません）。

以下の手順に従います。

1. `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. `introscope.enterprisemanager.smartstor.tier1.frequency` プロパティに、適切な値を入力します。
3. `introscope.enterprisemanager.smartstor.tier1.age` プロパティに、適切な値を入力します。
4. 残り 2 つのデータ層についても、それぞれ同様に 1 対のプロパティを設定します。
5. Enterprise Manager を再起動します。

注: データ層の設定を変更して Enterprise Manager を再起動すると、SmartStor は、新しい設定に応じてデータを調整しようとします。SmartStor は、最大で 1 日分のデータを失う可能性があります。

トランザクション イベント データベースの場所および保存期間

Enterprise Manager では、トランザクション追跡データおよびほかのイベントデータをトランザクション イベント データベースに保存します。

トランザクション イベント データベースの場所は、Enterprise Manager のインストール時に設定されます。インストール時に別の場所を指定しない限り、データベースは <EM_Home>/traces ディレクトリに作成されます。インストール後は、*IntroscopeEnterpriseManager.properties* の *introscope.enterprisemanager.transactionevents.storage.dir* プロパティを使用して、別の場所を選択できます。

Introscope がトランザクション イベント データを保持する日数は、Enterprise Manager のインストール時に設定されます。デフォルト値は 14 ですが、*introscope.enterprisemanager.transactionevents.storage.max.data.age* プロパティを使用して変更できます。

注: Introscope がイベント データを保存する期間を長くすると、システムオーバーヘッドおよびディスクの保存要件が増大します。

ベースライン ストレージの場所の設定

デフォルトでは、Introscope は、メトリックのベースライン情報を Enterprise Manager マシンの <EM_Home>/data/baselines.db に保存します。

Enterprise Manager インストーラには、ベースライン ストレージの場所として別の場所を選択するオプションはありません。ただし、Enterprise Manager プロパティ ファイルの *introscope.enterprisemanager.dbfile* プロパティで、*baselines.db* に別の場所を定義できます。

Introscope がメトリックのベースライン情報を使用してアプリケーションの稼働状況を示す高レベルのインジケータを有効にする方法については、「CA APM Workstation ユーザ ガイド」を参照してください。

SmartStor、ベースライン、およびトランザクション イベント データのバックアップ

Enterprise Manager を停止した後で、Enterprise Manager SmartStor、ベースライン、およびトランザクション イベントのデータ ファイルをバックアップしてから、それらで作業することができます。

デフォルトでは、SmartStor およびベースライン データはすべて Enterprise Manager によって <EM_Home>/data ディレクトリに保存されます。

SmartStor 用の Enterprise Manager データ ファイルは以下のとおりです。

- *metrics.metadata* ファイル。エージェントがレポートした各種メトリックに関する情報を追跡します（最も重要なことは、*metrics.metadata* は、メトリックの名前を追跡するということです）。
- *.spool* で終わるファイル（*1251226800000.spool* など）のうち、Enterprise Manager によるスプールからクエリへの最後の変換以降に SmartStor に送信された 15 秒のメトリック値を保持するファイル。*.spool* ファイルでは、1 時間分を超えるデータは保持されません。
- *.data* で終わるファイル（*1251183600000.data* など）のうち、SmartStor の読み取り専用クエリに最適化された形式でメトリック値が保持されているファイル。これらのファイルには、15 秒、1 分、および 1 時間のデータ ポイント値が保持されます。

ベースライン データ用の Enterprise Manager データ ファイルは以下のとおりです。

- *baselines.db*

デフォルトでは、Enterprise Manager によって、すべてのトランザクション追跡およびイベント データが <EM_Home>/traces ディレクトリに格納されます。トランザクション イベント データ用の Enterprise Manager データ ファイルは以下のとおりです。

- *traces_YYYYMMDD.db*。例：*traces_20090923.db*

Enterprise Manager は実行中、*metrics.metadata*、*.spool*、*.data* の各ファイルをエラーなく作成し、書き込みを行える必要があります。そのため、CA Technologies は、Enterprise Manager データの移動、コピー、およびその他の作業を行う前に、Enterprise Manager を停止することを強くお勧めします。

警告： Enterprise Manager の実行中に Enterprise Manager データ ファイルをコピーまたは編集すると、データが失われます。

Enterprise Manager がシャットダウンされていれば、Enterprise Manager データのバックアップおよび作業として、以下のすべてが実行可能です。

- バックアップ メディアへのデータの保存
- Smartstor ツールを使用した SmartStor データの編集
SmartStor ツールの詳細については、「[SmartStor ツールを使用した SmartStor データのチューニング \(P. 82\)](#)」を参照してください。
- データの圧縮
- データのリストア
- 別の Enterprise Manager でオフラインで表示するためのデータのコピー

クエリ専用の複製クラスタの作成

SmartStor データ ファイルを複製クラスタ マシンにコピーし、履歴（非ライブ）データのクエリ専用ソースとして使用できます。

注： CA Technologies は、実運用環境内において、クラスタが実行されているハードウェアのキャパシティをサービス要求が大幅に超えている場合にのみ、複製クラスタを作成することをお勧めします。

以下の手順に従います。

1. 実運用クラスタまたはテスト クラスタのまったく同じ複製を作成します。
マシンを、MOM 用に 1 台、クラスタ内のコレクタごとに 1 台使用します。
2. 実運用クラスタをシャットダウンします。
3. SmartStor、ベースライン、およびトランザクション イベントの各データ ファイルを、実運用またはテストの MOM から複製 MOM へ、および実運用またはテストの各コレクタから複製コレクタへコピーします。
4. 実運用クラスタとクエリ専用複製クラスタの両方を起動します。
5. クエリ専用複製クラスタで必要なクエリを実行します。
6. クエリ専用複製クラスタ上のデータを最新に保つために、必要な手順を 1 日 1 回繰り返します。

SmartStor ツールを使用した SmartStor データのチューニング

Introscope では、以下を実行できる SmartStor コマンドラインツールを提供しています。

- メトリック リークおよびメトリック急増からのクリーンアップ
メトリック リークおよびメトリック急増については、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。
- 単一 Enterprise Manager の複数 Enterprise Manager への分割
- 複数 Enterprise Manager の単一 Enterprise Manager へのマージ

SmartStor ツール起動スクリプトは <EM_Home>/tools/ ディレクトリ内にあります。Windows 環境内では、*SmartStorTools.bat* 起動スクリプトを使用して SmartStor ツールを実行します。UNIX 環境では、*SmartStorTools.sh* 起動スクリプトを使用して SmartStor ツールを実行します。

有効な引数を使用して <EM_Home> コマンドラインから SmartStor ツール コマンドを実行すると、要求したコマンドがツールによって実行されます。無効な引数を使用して SmartStor ツール コマンドを実行した場合、スクリプトによってヘルプメッセージが表示されます。

警告： SmartStor ツールを使用する際には、必ずソース Enterprise Manager をシャットダウンしてください。CA Technologies は、SmartStor ツールを実行する際、ソース Enterprise Manager および対象 Enterprise Manager をシャットダウンすることをお勧めします。SmartStor ツールを使用する際に Enterprise Manager が実行されていると、SmartStor が破損するおそれがあります。これは、SmartStor ツールによって SmartStor データに変更が加えられ、Enterprise Manager によっても SmartStor にデータが書き込まれる場合に発生します。

以下の形式を使用して、下記の SmartStor ツール コマンドを実行します。

<SmartStorTools 起動スクリプト><コマンド><引数>

- merge
- remove_metrics
- remove_agents
- keep_agents
- prune
- list-agents
- test_regex

警告： prune ツールを使用する際は、十分な注意が必要です。このツールではデータの削除が実行されるため、誤って重要なデータを削除しないように注意してください。

SmartStor ツール コマンド

SmartStor ツール コマンドを使用すると、SmartStor データベース上でいくつかのメンテナンス タスクと管理タスクを実行できます。

重要： これらのコマンドでエージェント名およびメトリック名を指定する際、特殊文字は円記号を使用してエスケープする必要があります。特殊文字は、(`[{¥^-$|}]`)?`*+`です。たとえば、メトリック名 `SuperDomain/machineName/WebLogic/WebLogic` は、`SuperDomain¥/machineName¥/WebLogic¥/WebLogic` のように指定します。

merge

指定された SmartStor ソース ディレクトリを別の対象ディレクトリにマージします。

引数

- <対象 SmartStor ディレクトリ>
- `-help` ヘルプメッセージを表示します。
- <ソース SmartStor ディレクトリ>

例：

Windows

```
SmartStorTools.bat merge <ソース ディレクトリ> <対象ディレクトリ>
```

例：

```
SmartStorTools.bat merge <EM_Home>%data C:%data
```

コマンドが正常に実行されると、ソース ディレクトリ内にあるすべての SmartStor データが、対象ディレクトリ内のデータとマージされます。

UNIX

```
SmartStorTools.sh merge <ソース ディレクトリ> <対象ディレクトリ>
```

remove_metrics

指定された正規表現と一致するメトリックが削除されます。メトリック リークおよびメトリック急増をクリーンアップする際に、このツールを使用します。

警告： `remove_metrics` ツールを使用する際は、十分な注意が必要です。このツールではデータの削除が実行されるため、誤って重要なデータを削除しないように注意してください。

引数

- `-dest` - 対象 SmartStor ディレクトリ。
- `-help` - ヘルプメッセージを表示します。
- `-metrics` - 削除するメトリック用の正規表現。
- `-src` - ソース SmartStor ディレクトリ。

例：

Windows

```
SmartStorTools.bat remove_metrics -dest <対象ディレクトリ> -metrics <削除するメトリック> -src <ソース ディレクトリ>
```

例：

```
<EM_Home>%tools%SmartStorTools.bat remove_metrics -dest C:%SWDump%destination  
-metrics ".*Socket.*" -src <EM_Home>%data
```

コマンドが正常に実行されると、ソケットメトリックが削除され、それ以外のメトリックはすべて対象ディレクトリ内に残り、ソースディレクトリはすべてのメトリックがそのまま残ります。

UNIX

```
SmartStorTools.sh remove_metrics -dest <対象ディレクトリ> -metrics <削除するメトリック>  
-src <ソース ディレクトリ>
```

remove_agents

指定された正規表現と一致するエージェントが削除されます。

警告： `remove_agent` ツールを使用する際は、十分な注意が必要です。このツールではデータの削除が実行されるため、誤って重要なデータを削除しないように注意してください。

引数

- `-agents` - 削除するエージェント用の正規表現。
- `-dest` - 対象 SmartStor ディレクトリ。
- `-help` - ヘルプ メッセージを表示します。
- `-src` - ソース SmartStor ディレクトリ。

例：

Windows

```
SmartStorTools.bat remove_agents -agents <エージェント名> -dest <対象ディレクトリ> -src  
<ソース ディレクトリ>
```

例：

```
<EM_Home>%tools>SmartStorTools.bat remove_agents -agents ".*WebSphere.*" -dest  
C:%SWDump%destination -src <EM_Home>%data
```

コマンドが正常に実行されると、WebSphere エージェントに関連するすべてのメトリックが対象ディレクトリから削除され、ソース ディレクトリ内のメトリックはすべてそのまま残ります。

UNIX

```
SmartStorTools.sh remove_agents -agents ".*WebSphere.*" -dest <対象ディレクトリ> -src  
<ソース ディレクトリ>
```

keep_agents

指定された正規表現と一致するエージェントが維持されます。

引数

- `-agents` - 維持するエージェント用の正規表現
- `-dest` - 対象 SmartStor ディレクトリ
- `-help` - ヘルプ メッセージを表示します。
- `-src` - ソース SmartStor ディレクトリ

例 :

Windows

```
SmartStorTools.bat keep_agents -agents <エージェント名> -dest <対象ディレクトリ> -src  
<ソース ディレクトリ>
```

例 :

```
<EM_Home>%tools>SmartStorTools.bat keep_agents -agents ".*Websphere.*" -dest  
C:%SWDump%destination%keepagents -src data
```

コマンドが正常に実行されると、Websphere エージェントに関連するすべてのメトリックが対象ディレクトリ内に残り、ソースディレクトリ内の内容はそのまま残ります。

UNIX

```
SmartStorTools.sh keep_agents -agents <エージェント名> -dest <対象ディレクトリ> -src <  
ソース ディレクトリ>
```

prune

SmartStor 内に履歴データがないエージェントを見つけて、関連するメトリック メタデータをすべて削除します。メトリック リークおよびメトリック急増をクリーンアップする際に、このツールを使用します。

警告 : `prune` ツールを使用する際は、十分な注意が必要です。このツールではデータの削除が実行されるため、誤って重要なデータを削除しないように注意してください。

`prune` ツールの使用には、複数の手順が必要です。「[SmartStor メタデータの廃棄 \(P. 90\)](#)」を参照してください。

引数

- **-dest** -- ソースの変更前の *.data ファイルと一緒に切り取られたメタデータ ファイルを格納するディレクトリです。
- **-help** -- ヘルプ メッセージを表示します。
- **-silent** -- サイレント モード
- **-src** -- ソース SmartStor ディレクトリ

例

Windows

```
SmartStorTools.bat Prune -dest <保存先ディレクトリ> -src <ソース ディレクトリ>
```

例 :

```
<EM_Home>%tools>SmartStorTools.bat Prune -dest C:%SWDump%destination%backup -src data
```

コマンドが正常に実行されると、メタデータ ファイルは **dest** で指定したディレクトリに **metrics.metadata** という名前でバックアップされます。

UNIX

```
SmartStorTools.sh prune -dest <保存先ディレクトリ> -src <ソース ディレクトリ>
```


test_regex

指定された正規表現と一致するメトリックまたはエージェントを、Windows または UNIX コンソールに表示します。

引数

- `-help` - ヘルプ メッセージを表示します。
- `-src` - ソース SmartStor ディレクトリ
- `-agents` - 一致させるエージェント用の正規表現
- `-metrics` - 一致させるメトリック用の正規表現

例 :

Windows

```
SmartStorTools.bat test_regex -agents <エージェント名> -src <ソース ディレクトリ>
```

例 :

```
<EM_Home>%tools>SmartStorTools.bat test_regex -agents ".*Websphere.*" -src  
<EM_Home>%data
```

コマンドが正常に実行されると、WebSphere エージェントのメトリックがすべて表示されます。

UNIX

```
SmartStorTools.sh test_regex -agents <エージェント名> -src <ソース ディレクトリ>
```

list_agents

指定された正規表現と一致するエージェントを一覧表示します。

SmartStor ツールの `list_agents` ツールは、指定された正規表現と一致するエージェントを一覧表示します。

引数

- `-agents` - 一致させるエージェント用の正規表現
- `-src` - ソース SmartStor ディレクトリ
- `-help` - ヘルプ メッセージを表示します。

例 :

Windows

```
SmartStorTools.bat list_agents -agents <エージェント名> -src <ソース ディレクトリ>
```

例 :

```
<EM_Home>%tools>SmartStorTools.bat list_agents -agents ".*WebSphere.*" -src  
<EM_Home>%data
```

コマンドが正常に実行されると、正規表現（この例では、`".*WebSphere.*"`）に一致するすべてのエージェント名が、最後のレポート日とともに一覧表示されます。

UNIX

```
SmartStorTools.sh list_agents -agents <エージェント名> -src <ソース ディレクトリ>
```

SmartStor メタデータの廃棄

SmartStor 内に履歴データがないエージェントを検索したり、メトリックリークおよびメトリック急増をクリーンアップするには、*prune* SmartStor ツールを使用してから、関連するメトリック メタデータをすべて削除します。

重要: Enterprise Manager は実行時に SmartStor データを作成するため、SmartStor ツールを実行するときには Enterprise Manager をシャットダウンすることをお勧めします。Enterprise Manager の実行中に SmartStor ツールを使用すると、予測不能の結果が生じます。

以下の手順に従います。

1. Enterprise Manager をシャットダウンします。
2. コマンドプロンプトから、*prune* コマンドを実行します。

例：

Windows の場合：<EM_Home>%tools>SmartStorTools.bat prune -src <データディレクトリへのパス> -dest <バックアップディレクトリへのパス>

UNIX の場合：<EM_Home>%tools>SmartStorTools.sh prune -src <データディレクトリへのパス> -dest <バックアップディレクトリへのパス>

コマンドが正常に実行されると以下のようになります。

- メタデータ ファイルは *dest* で指定したディレクトリに *metrics.metadata* という名前でバックアップされます。
- Windows または UNIX コンソールに、*prune* オペレーション中に廃棄されたメトリックが表示されます。
- *.data ファイルは *src* で指定したディレクトリから、*dest* で指定したディレクトリに変更されずにコピーされます。

Windows または UNIX コンソールの廃棄済みメトリック リストをテキストファイルにリダイレクトするには、コマンド内に >> 引数を含めます。
例：<EM_Home>%tools>SmartStorTools.bat prune -src <データディレクトリへのパス> -dest D:%backup >>D:%console.txt

1. <EM_Home>/data ディレクトリ内にある *metrics.metadata* ファイルの名前を変更します。例：*noprunemetrics.metadata*
2. <EM_Home>/data ディレクトリで *test_regex* コマンドを実行します。

コマンドに含めた正規表現と一致するすべてのメトリックを表示したコマンド出力が、Windows または UNIX のコンソールに表示されます。廃棄されたメトリックは存在していませんので注意してください。

この *test_regex* コマンドは、大量のソケットメトリックを廃棄した場合などに実行します。

Windows の場合：

<EM_Home>%tools>SmartStorTools.bat test_regex -metrics ".*Socket.*" -src <データディレクトリへのパス>

UNIX の場合：

<EM_Home>/tools>SmartStorTools.sh test_regex -metrics ".*Socket.*" -src <データディレクトリへのパス>

3. Enterprise Manager を再起動します。

SmartStor データおよびメタデータの削除

余分な SmartStor データおよびメタデータを削除するには、SmartStor ツールを使用します。

重要: SmartStor ツールを実行する場合は、Enterprise Manager をシャットダウンします。Enterprise Manager は実行中に SmartStor データを作成するため、ユーザが SmartStor ツールを使用すると、予測できない結果になる場合があります。

SmartStor データの問題を特定する方法の例については、「[例: test_regex コマンドを使用した SmartStor データ問題の検出 \(P. 95\)](#)」を参照してください。また、「[CA APM Java Agent 実装ガイド](#)」または「[.NET Agent 実装ガイド](#)」でメトリック急増に関するトピックを参照してください。

以下の手順に従います。

1. Enterprise Manager をシャットダウンします。
2. コマンドプロンプトから、`test_regex` コマンドを実行し、現在のメトリック リストを表示します。

たとえば、Introscope が `<EM_Home>` ディレクトリ内にインストールされていて、SmartStor が `<EM_Home>\data` ディレクトリにデータを保存するよう構成されている場合は、以下のコマンドを実行します。

```
SmartStorTools.sh test_regex -metrics <エージェントの正規表現>
-src ../data
```

例: `SmartStorTools.sh test_regex -metrics ".*" -src ../data`

この結果、ホスト名、エージェント名、メトリック名、およびメトリック ID が含まれた完全修飾メトリック名のリストが表示されます。行の総数からメトリックの総数を判断できます。ただし、行数は、Investigator のサポータビリティメトリックから取得するメトリック数ほど正確ではありません。

エージェント名やメトリック名と一致する具体的な正規表現を使用し、その結果の行数を数えることで、スペースの大部分を占めているメトリックの種類を把握できます。これは、不要なメトリックや削除対象のメトリックを特定する際にも役立ちます。

3. メトリックのリストから、特定のエージェント内にある削除対象のメトリックを選択します。

4. SmartStor ツール `remove_metrics` コマンドを実行し、余分なメトリックのセットを削除します。

たとえば、SQL メトリック数が多い場合は、以下のコマンドを使用して、SQL メトリックをすべて削除します。

```
<EM_Home>%tools>SmartStorTools.bat remove_metrics  
-dest c:%sql_metrics_removed -metrics ".*SQL.*" -src <EM_Home>%data
```

コマンドが正常に実行されると、対象ディレクトリ内の SQL メトリックが削除され、それ以外のメトリックはすべて残り、ソースディレクトリにはすべてのメトリックがそのまま残ります。

注: このコマンドを実行するには、元のデータ (-src オプションによって指定されたデータ) が占めているスペースとほぼ同じ容量 (数 GB 縮小します) のターゲットスペースが必要です。上記の例では、SQL メトリックのない新しいデータ (-dest オプションによって指定されたデータ) は、`c:%sql_metrics_removed` ディレクトリにあります。

このコマンドは実行時間の長いオペレーションで、数時間かかる場合もあります。

5. 必要に応じて、余分なメトリックの別のセットに対して `remove_metrics` コマンドを繰り返してください。

ソケットも、メトリック リークの一般的な発生源です。

`remove_metrics` コマンドを実行した後は、以下のコマンドを使用して、ソケットメトリックを削除してください。

```
<EM_Home>%tools>SmartStorTools.bat remove_metrics  
-dest c:%sql_and_sockets__metrics_removed -metrics ".*Sockets.*"  
-src c:%sql_metrics_removed
```

このコマンドでは、ソースデータとして、SQL メトリックを削除した最初のコマンドによって取得されたデータ (`c:%sql_metrics_removed` ディレクトリ内のデータ) を使用します。その後、SQL メトリックおよびソケットメトリックの両方が削除されたデータは、-dest オプション: `c:%sql_and_sockets__metrics_removed` によって指定された場所に保存されます。この場合も、このコマンドを実行するには、元のデータとほぼ同じ容量の予備スペースが必要です。

6. メトリックの数を減らした後に、任意のバックアップメタデータファイルを `<EM_Home>%data` ディレクトリからバックアップディレクトリに移動します。

Enterprise Manager は自動的に最大のメタデータファイルを使用します。これは定義されたメトリックが最も多いファイルです。メトリックを減らすと、バックアップメタデータファイルが現在のデータファイルよりも大きくなる可能性があります。

7. クリーンになったメトリックデータおよびメタデータのメトリックデータ値を確認します。
 - a. `<EM_Home>%config` ディレクトリの `apm-events-thresholds-config.xml` ファイルを開きます。
 - b. 現在のプロパティ設定をメモに書きとめてから、プロパティ `introscope.enterprisemanager.metrics.historical.limit=500000` を設定します。
 - c. ファイルを保存して閉じます。
 - d. `<EM_Home>%config` ディレクトリの `IntroscopeEnterpriseManager.properties` ファイルを開きます。
 - e. 現在の設定をメモに書きとめてから、プロパティ `introscope.enterprisemanager.smartstor.directory=` がメトリック削除の対象場所を指すよう設定します。

たとえば、対象場所を `c:%sql_and_sockets__metrics_removed` と仮定します。この場合、プロパティ設定は `introscope.enterprisemanager.smartstor.directory=c:%sql_and_sockets__metrics_removed` になります。
 - f. ファイルを保存して閉じます。
 - g. Enterprise Manager を再起動します。
 - h. 以下のメトリックの値を確認します。

Enterprise Manager | Data Store | SmartStor | Metadata | Metrics with Data

値は、元の値よりもかなり小さくなっているはずです。そうでない場合は、不要なエージェント名またはメトリック名に対して適切な SmartStor ツールコマンドを使用して、削除手順を繰り返してください。履歴メトリック数が 300 K 未満になれば、Enterprise Manager は効率よく実行されます。

8. 必要に応じて、変更したプロパティ値を元の設定にリセットします。
 - a. `<EM_Home>%config` ディレクトリの `apm-events-thresholds-config.xml` ファイルを開きます。
 - b. `introscope.enterprisemanager.metrics.historical.limit` プロパティを元の設定にリセットします。
 - c. ファイルを保存して閉じます。
 - d. Enterprise Manager をシャットダウンします。
 - e. `<EM_Home>%config` ディレクトリの `IntroscopeEnterpriseManager.properties` ファイルを開きます。
 - f. `introscope.enterprisemanager.smartstor.directory` プロパティを元の設定にリセットします。
 - g. ファイルを保存して閉じます。
 - h. Enterprise Manager を再起動します。

例: test_regex コマンドを使用した SmartStor データ問題の検出

この例では、`test_regex` コマンドを使用して、JMX メトリックデータの急増を検出します。

以下の手順に従います。

1. `test_regex` コマンドを実行し、`metrics.metadata` の読み取り可能なバージョンを作成します。

たとえば、以下のようになります。

```
<EM_Home>%tools>SmartStorTools.bat test_regex  
-metrics -src <EM_Home>%data
```

この結果、メタデータ メトリックのリストが表示されます。

2. メタデータ メトリック リストを確認し、メトリック リークまたはメトリック急増の原因として考えられるソースを判別します。

たとえば、JMX メトリックのメトリック メタデータ エントリが大量にあることが検出される場合があります。

3. (オプション)スクリプトを実行して、メトリックの並べ替えやグループ化を行います。

たとえば、JMX メトリックがメトリック急増のソースであることを確認するには、以下のスクリプトを実行できます。

```
grep '|.* | awk -F'|' '{print $1}' | sort | uniq -c
```

UNIX システムを使用している場合は、並べ替えスクリプトを含む完全な `test_regex` コマンドとして、次のように指定します。

```
SmartStorTools.sh test_regex -metrics <エージェントの正規表現>
```

```
-src ../data | grep '|.* | awk -F'|' '{print $1}' | sort | uniq -c
```

```
例: SmartStorTools.sh test_regex -metrics ".*" -src ../data | grep '|.* | awk -F'|' '{print $1}' | sort | uniq -c
```

4. 並べ替えの結果を確認します。

たとえば、以下のようなメトリックの数とタイプに関するリストが表示されます。

1054327 JMX

1564 JSP

1051 OlamWebApp

889 EJB

569 CEF

496 Struts

173 Edocs

167 Servlets

36 CPU

29 Sockets

この例では、SmartStor に 100 万以上のメトリックが保存されており、その大部分は JMX メトリックです。これは、JMX メトリックの急増があったことを示しており、SmartStor ツールによるクリーンアップが可能です。メトリック急増の詳細については、「[CA APM Java Agent 実装ガイド](#)」または「[.NET Agent 実装ガイド](#)」を参照してください。

8.x データから 9.x へのアップグレード

SmartStor ツール コマンドを使用して、SmartStor データを 8.x エージェントから 9.x に更新できます。

このツールは、8.x フロントエンドおよびバックエンドメトリック ID を 9.x フロントエンドおよびバックエンドメトリック ID で更新します。これにより、アプリケーション問題切り分けマップに重複したメトリックが表示されなくなります。

Enterprise Manager とエージェントを 9.x にアップグレードしてから、アップグレード コマンドを使用します。

アップグレード コマンドを使用した 8.x データのアップグレード

以下の手順に従います。

1. Enterprise Manager をシャットダウンします。
2. コマンドプロンプトから、<EM_Home>/tools ディレクトリを参照します。
3. SmartStor データ ディレクトリをバックアップします。
4. ソースとデスティネーションのディレクトリ パスを指定して、*upgrade* コマンドを実行します。

以下の構文および引数を使用します。

構文:

```
upgrade <sourceDir> <destDir>
```

引数

- *sourceDir* - SmartStor 8.x メトリックが含まれる既存のディレクトリへのパス
- *destDir* - 新しいディレクトリへのパス

注: 新しいディレクトリはユーティリティによって処理中に作成されます。あらかじめ作成しないでください。

例:

```
C:¥Program Files¥CA
APM¥Introscope<new_version(9.X)>¥tools>SmartStorTools.bat
upgrade C:¥Program Files¥CA APM¥Introscope<新しいバージョン (9.X)
>¥data C:¥Program Files¥CA APM¥Introscope<新しいバージョン (9.X)
>¥upgradeddata
```

5. IntroscopeEnterpriseManager.properties ファイルを編集して、SmartStor ディレクトリをデスティネーションディレクトリのそれに設定します。
 - a. 編集するために
<EM_Home>/config/IntroscopeEnterpriseManager.properties を開き、「SmartStor Settings」セクションを見つけます。
 - b. *introscope.enterprisemanager.smartstor.directory* の値をデスティネーションディレクトリに設定します。
デフォルト値は *data* です。これは、<EM_Home>/data/ を表します。
6. Enterprise Manager を再起動します。

第 5 章: 仮想エージェントを使用したメトリックの集約

このセクションでは、仮想エージェントの設定方法および使用方法について説明します。

このセクションには、以下のトピックが含まれています。

[仮想エージェントの理解](#) (P. 99)

[仮想エージェントの要件](#) (P. 100)

[仮想エージェントの設定](#) (P. 101)

仮想エージェントの理解

複数の物理エージェントを 1 つの仮想エージェントに設定できます。仮想エージェントでは、複数の **Java Agent** によってレポートされたメトリックを集計した論理ビューを表示できます。

仮想エージェントは、クラスタ化されたアプリケーションを **Introscope** で管理する場合に便利です。

仮想エージェントは、同じクラスタ化アプリケーションのさまざまなインスタンスの監視を行うエージェントで構成され、**Introscope Workstation** に単一のエージェントとして表示されます。これによって、クラスタ化アプリケーションの複数のインスタンスのメトリックを、各アプリケーションインスタンスごとではなく、論理的なアプリケーションレベルで表示できます。

単一エージェントに関するビューおよび相互作用に限定すると、特定のアプリケーションインスタンスの性能および可用性のデータを表示できます。

仮想エージェントの要件

複数のスタンドアロン Enterprise Manager がある場合、同じ Enterprise Manager にレポートするエージェントだけを仮想エージェントに含めることができます。

Enterprise Manager クラスタでは、単一クラスタ内の Enterprise Manager にレポートするエージェントは、それらのレポート先のコレクタ Enterprise Manager に関係なく、同じ仮想エージェントに属することができます。

仮想エージェントを設定するには、以下の条件を考慮してください。

- エージェントは、複数の仮想エージェントに割り当てることができます。
- 複数の仮想エージェントを定義する場合、カスタム メトリック エージェントを含むクラスタ内のすべてのエージェントは、一意の名前を持つ必要があります。
- SuperDomain の下に存在する仮想メトリックはほかのカスタム ドメインに発行できます。例：

```
<agent-cluster name="Custom Metric Host" domain="SuperDomain"
tgtDomain="Production">
    <agent-specifier>(.*)*|(.*)*|Custom Metric Agent
*(Virtual*)(.*)</agent-specifier>

<metric-specifier>Agents*(.*) :ConnectionStatus</metric-specifier>
</agent-cluster>
```

この設定により、仮想メトリックである `ConnectionStatus` が、`superdomain.custom metric host (Collector):agent` リスト内のすべてのエージェントから取得され、`Production` ドメインに再発行されます。

仮想エージェントの設定

仮想エージェントを設定するには、エージェントがレポートする Enterprise Manager の `<EM_Home>/config` ディレクトリにある `agentclusters.xml` ファイルを使用します。クラスタ化された Enterprise Manager を実行する場合は、MOM `<EM_Home>/config` ディレクトリにある `agentclusters.xml` ファイルを使用して仮想エージェントを設定します。サンプル `agentclusters.xml` は、`EM_Home>/config` ディレクトリにあります。

以下のサンプル `agentclusters.xml` は、Introscope スーパードメインに `BuyNowAppCluster` という名前の仮想エージェントを定義します。仮想エージェントには、任意のホストで、名前が `BuyNow` で始まるすべてのエージェントが含まれます。

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain" >
    <agent-specifier>.*%|. *%|BuyNow.*</agent-specifier>
    <metric-specifier>Frontends%|. *</metric-specifier>
  </agent-cluster>
</agent-clusters>
```

ルートエレメント `<agent-clusters>` が必要です。 `<agent-cluster>` エレメントは、仮想エージェントを定義します。また、以下の 2 つの必須属性があります。

- **name** - 複数の仮想エージェントを定義する場合、それぞれが一意の名前を持つ必要があります。
- **domain** - 仮想エージェントを Introscope ドメインに割り当てます。
エージェントクラスタ定義でドメインが定義されていない場合 (`domain=""`)、仮想エージェントはデフォルトでスーパードメインを使用します。

複数の仮想エージェントを定義する場合は、それぞれに対して `<agent-cluster>` エレメントを定義します。 `<agent-cluster>` エレメントには、2 つの子エレメントが必要です。

- `<agent-specifier>` - 標準の完全修飾エージェント名を使用して、仮想エージェント内のエージェントを指定する正規表現を含みます。
`<host> | <process> | <agentName>`

- `<metric-specifier>` - 仮想エージェント内のエージェントから収集するメトリックを、リソースタイプ、またはリソースタイプのインスタンスのサブセットを使用して指定するプレフィックスを含みます。推奨されるプレフィックスは以下のとおりです。
 - Frontends
 - CPU
 - JMX
 - WebSpherePMI

注: 以上が推奨されるプレフィックスですが、任意のリソースをメトリック指定子として使用することもできます。

`<agent-cluster>` エlementには、複数の `<metric-specifier>` スタンザを含めることができます。

注: 一致するメトリックの量が多いほど、Enterprise Manager でのオーバーヘッドが大きくなり、最終的に Enterprise Manager の容量に大きな影響を与えることに注意してください。

重要: 正規表現、および「.*」や「(.*)」などのワイルドカードメトリック指定子を使用できますが、使用するには注意が必要です。ワイルドカードを使用すると、メトリックの量が多くなり、性能に影響を与える可能性があります。

特定のブラウザツリードメインノードの下に仮想エージェントを表示するには、`tgtDomain` 属性を定義します。

- `tgtDomain` - ドメイン属性で定義された仮想エージェントメトリックをブラウザツリーで表示するためにコピーするターゲットドメインを定義します。
 - `tgtDomain` が定義されない場合、ドメインの名前は `tgtDomain` となります。
 - `tgtDomain` 値が `domains.xml` で定義された有効なドメインでない場合、Introscope はターゲットドメインのブラウザツリーノードを作成できません。
 - `tgtDomain` 属性を使用して定義したドメインを表示するには、`domains.xml` で定義された権限が必要です。`domains.xml` の権限については、「CA APM セキュリティガイド」を参照してください。

このサンプル *agentclusters.xml* は、*BuyNowAppCluster* という名前の仮想エージェントを定義します。これは Introscope スーパードメイン ノードに定義され、*MyDomain* ノードに表示されます。

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<agent-clusters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="agentclusters0.1.xsd" version="0.1" >
  <agent-cluster name="BuyNowAppCluster" domain="SuperDomain"
tgtDomain="MyDomain"
    <agent-specifier>.*%|. *%|BuyNow.*</agent-specifier>
    <metric-specifier>Frontends%|. *</metric-specifier>
  </agent-cluster>
</agent-clusters>
```

この場合、*MyDomain* ドメインのみを表示する権限を持つ CA APM ユーザは、以下のブラウザ ツリーを参照できます。

```
Custom Metric Host (仮想)
  Custom Metric Process (仮想)
    BuyNowAppCluster
```


第 6 章: Enterprise Manager とクラスタの設定

このセクションでは、Enterprise Manager のクラスタ機能と、Enterprise Manager のロールおよびクラスタ機能の構成方法について説明します。

このセクションには、以下のトピックが含まれています。

[スタンドアロン Enterprise Manager の設定](#) (P. 105)

[Enterprise Manager クラスタの理解](#) (P. 105)

[Enterprise Manager フェールオーバーの使用](#) (P. 110)

[Enterprise Manager のクラスタの設定](#) (P. 116)

スタンドアロン Enterprise Manager の設定

`introscope.enterprisemanager.clustering.mode` プロパティを設定して、Enterprise Manager をスタンドアロンの Enterprise Manager として指定します。

以下の手順に従います。

1. スタンドアロンの Enterprise Manager の `<EM_Home>\config` ディレクトリにある `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. 「`introscope.enterprisemanager.clustering.mode=Standalone`」と設定します。
3. ファイルを保存して閉じます。
4. Enterprise Manager を再起動して、この設定を有効にします。

Enterprise Manager クラスタの理解

クラスタ環境では、Enterprise Manager は複数の *Manager* を管理する *Manager* (MOM : Manager of Managers) として機能し、クラスタ内のほかの Enterprise Manager を管理します。管理される Enterprise Manager は、コレクタと呼ばれます。

MOM にログインした Workstation ユーザは、以下の操作を実行できます。

- エージェントがレポートしたデータにアクセスして表示できます。
エージェントは、MOM の管理下にある各コレクタにレポートします。
- 通常の Workstation 機能のすべてをこれらのコレクタに対して実行できます。

オプションの Enterprise Manager はクロス クラスタ データ ビューア (CDV) として機能し、複数クラスタのコレクタに接続できます。

CDV にログインした Workstation ユーザは、以下の操作を実行できます。

- ダッシュボード、およびメトリック ブラウザ ツリーのエージェントおよびカスタマ エクスペリエンス メトリック データを参照しアクセスします。このデータは、CDV の接続先の各コレクタにレポートされます。
- これらのコレクタに対し、以下の機能を含む通常の Workstation 機能の一部を実行します。
 - 管理モジュール エディタを使用した、ダッシュボードの作成。
 - トランザクション追跡の実行
 - 動的インスツルメンテーションの使用。
 - [Enterprise Manager のクラスタを設定](#) (P. 116) できます。

Enterprise Manager をクラスタ化すべき状況

クラスタ化は、複数の Enterprise Manager と多数のエージェントで構成された大規模な Introscope 環境で有効です。クラスタ構成によって、複数の Enterprise Manager 環境の管理の複雑さとコストが軽減されます。

MOM がコレクタを管理する方法の理解

「[Enterprise Manager のクラスタの設定 \(P. 116\)](#)」の説明に従って構成された MOM を起動すると、MOM は、管理する各コレクタに接続しようとします。

Investigator 内のすべてのエージェントには、Enterprise Manager ホストと呼ばれるメトリックが自動的に含まれています。このメトリックは、クラスタ実行時に、エージェントが接続しているコレクタ Enterprise Manager を判別するのに役立ちます。

MOM は、コレクタとの接続に、設定済みの組み込みユーザアカウントを使用します。パスワードは、公開/秘密鍵による暗号化を使用して保護されます。詳細については、「[CA APM セキュリティガイド](#)」を参照してください。

MOM が管理下のいずれかのコレクタに初めて接続するときに、認証エラー、不明なホスト名の例外、または `java.rmi.ConnectIOException` などの回復不可能なエラーが発生した場合、そのコレクタはクラスタから削除されます。次回 MOM を再起動するまで、MOM はそのコレクタとの接続を停止します。

接続中断などの回復可能なエラー、または `java.rmi.ConnectionException` の場合、MOM は 10 秒ごとに接続試行を繰り返します。

接続ステータスのログは、以下のように記録されます。

- ログレベルが **DEBUG** の場合、接続失敗のスタックトレースがログに書き込まれます。
- ログレベルが **VERBOSE** の場合は、最初から 10 回目まで再試行が連続して失敗したときに、メッセージがログに書き込まれます。失敗が 10 回続くと、失敗した接続試行をそれ以上ログに記録しないことを通知するメッセージがログに書き込まれます。
- メッセージは、MOM がコレクタに接続または再接続するたびにログに書き込まれます。

MOM は、実行されている限り、管理対象のコレクタをポーリングします。

クラスタ化および Enterprise Manager クロック同期

Enterprise Manager クラスタでは、コレクタ システム クロックと、MOM のクロック設定の差が 3 秒以内である必要があります。起動時に、コレクタのクロックが MOM のクロックと同期していない場合、コレクタはクラスタに参加できません。操作中に、以前同期したコレクタのクロックとの差が 3 秒を超えると、MOM は、そのコレクタからのデータの受け取りを拒否します。

MOM とコレクタ Enterprise Manager 間のクロック同期は自動的には行われません。

MOM とコレクタ Enterprise Manager のクロックの同期を維持するためには、すべての Enterprise Manager がそれらのクロックを定期的に NTP サーバと同期するように設定することをお勧めします。コレクタのクロックと MOM のクロックの差が 3 秒を超えると、MOM のログ内のエラーメッセージに、MOM がそのコレクタからデータを受信しなくなっていることが記録されます。この場合は、NTP サーバと同期する間隔を短くします。クロック同期の後に Enterprise Manager を再起動する必要はありません。MOM は、クロックが同期されていることを検出すると、自動的にコレクタに再接続します。

注: クラスタ内のすべてのマシンのクロックを一定間隔で同期する、タイムサーバソフトウェアを実行する必要があります。

クラスタとエージェントの名前付け

Enterprise Manager クラスタでは、コレクタ Enterprise Manager にレポートするエージェントの名前は一意である必要があります。

MOM は、クラスタ全体で一意のエージェント名を要求します。各 Enterprise Manager では、接続しているエージェントの名前が必ず一意になっています（「CA APM Java Agent 実装ガイド」または「CA APM .NET Agent 実装ガイド」の「エージェント名前付けの競合の解決方法」を参照）。ただし、クラスタ全体のコレクタ間でエージェントが一意の名前を持っているかどうかは、ユーザが確認する必要があります。クラスタ内の複数のエージェントが同じ名前の場合、Workstation のビューに表示されるのは、MOM が最後に検出したエージェントのみです。エージェントがアプリケーションサーバから名前を取得するように構成するのも、一意のエージェント名を割り当てる 1 つの方法です。詳細については、お使いの環境に応じて、「CA APM Java Agent 実装ガイド」または「CA APM .NET Agent 実装ガイド」で、アプリケーションサーバからのエージェント名の取得に関する説明を参照してください。

コレクタは、カスタム メトリック エージェントの名前を自動的に変更し、エージェントのコレクタを識別する一意の識別子をエージェント名に追加します。デフォルト識別子の形式は *host@port* で、*host* はコレクタのホスト名、*port* はコレクタの接続ポートです（プロパティ `introscope.enterprisemanager.port.<チャンネル名>` で定義されています）。また、`introscope.enterprisemanager.clustering.collector.identifierr` プロパティを使用して識別子を設定することもできます。識別子は一意です。

たとえば、ポート 5001 で接続をリスニングする *myhost* のコレクタのスーパードメイン内のカスタム メトリック エージェント名は、以下のようになります。

```
Custom Metric Agent (myhost@5001) (*SuperDomain*)
```

クラスタ化および管理モジュール

Enterprise Manager クラスタでは、MOM にインストールされた管理モジュールのみが使用されます。パフォーマンス上の理由から、コレクタ Enterprise Manager には管理モジュールを配置しないことをお勧めします。

クラスタ環境での拡張ファイルのデプロイ

CA APM のデプロイで拡張機能をアクティブにした場合は、クラスタ化された環境に拡張ファイルをデプロイする際、特定の方法で管理する必要があります。

以下の手順に従います。

1. `<EM_Home>/examples/<Extension_Home>` 内で、拡張機能がインストールされている拡張フォルダを見つけます。`<Extension_Home>` は拡張機能の名前です。
2. このフォルダの内容すべてを MOM 上の `<EM_Home>/` にコピーします。
3. このフォルダの内容の、ディレクトリ `<EM_Home>/examples/<Extension_Home>/config` を除くすべてを、各コレクタ Enterprise Manager 上の `<EM_Home>/` にコピーします。

管理モジュール `.jar` ファイルは MOM 上のみに存在する必要があるため、`<EM_Home>/examples/<Extension_Home>/config` ディレクトリはコピーされません。

Enterprise Manager フェールオーバーの使用

Enterprise Manager フェールオーバーは、以下のように Enterprise Manager を指定することにより機能します。

- 一方の Enterprise Manager をプライマリ コンピュータとして指定し、他方をセカンダリまたはバックアップとして指定。
- 両方の Enterprise Manager をプライマリ コンピュータとして指定。

セカンダリの役割は、プライマリに障害が発生した場合に制御を引き継ぎ、プライマリが復帰したら制御を中止することです。このときプライマリは、セカンダリから制御を引き継ぐこととなります。

1 組の Enterprise Manager が単一の Introscope インストールを共有する場合、Enterprise Manager フェールオーバーを構成できます。通常、この 2 つの Enterprise Manager は別々のコンピュータ上にあります。Introscope システムは、ネットワーク ファイルシステム上に存在する必要があります。理由は、両方の Enterprise Manager が Introscope システムへの読み取りアクセスを必要とするためです。ただし、書き込みアクセスを同時に必要とするのは、1 つの Enterprise Manager のみです。たとえば、Introscope システムを、以下のようなネットワーク接続ストレージ (NAS) プロトコルを使用して共有することができます。

- ネットワーク ファイルシステム (NFS)
- サーバメッセージブロック (SMB)

クラスタの安定性を実現するために、CA Technologies は、MOM Enterprise Manager にフェールオーバーを構成することをお勧めします。また、クラスタ内の 1 つ以上のコレクタおよび CDV、またはスタンドアロン Enterprise Manager のフェールオーバーを設定できます。クラスタ内の MOM、コレクタ、および CDV のフェールオーバーを設定する場合は、各 Enterprise Manager を個別に設定します。

Enterprise Manager フェールオーバーは、デフォルトでは有効になっていません。

以下の手順に従います。

1. <EM_Home>\config ディレクトリに移動し、
IntroscopeEnterpriseManager.properties ファイルを開きます。
2. 「Hot Failover」セクションを見つけます。
3. [フェールオーバープロパティ](#) (P. 520) を設定します。

エージェント、TIM、および Workstation は Enterprise Manager への接続を試行する際、ホスト名の IP アドレスをすべて試します。プライマリ Enterprise Manager とセカンダリ Enterprise Manager の IP アドレスを持つ論理ホストを DNS に定義していると、エージェント、TIM、および Workstation はこれを Enterprise Manager ホスト名として使用し、どちらか稼働している方の Enterprise Manager に接続することができます。

- セカンダリ Enterprise Manager コンピュータのユーザに、プライマリ Enterprise Manager の SmartStor データ ディレクトリへの書き込み権限があることを確認します。

フェールオーバー時に、この権限により、セカンダリ Enterprise Manager がプライマリ Enterprise Manager の SmartStor データベースにデータを書き込むことができます。

注: フェールオーバー環境では、*EMCtrl* スクリプトを使用して、プライマリ Enterprise Manager を起動できます。セカンダリ Enterprise Manager は、この制御スクリプトを使用できません。たとえば、UNIX プラットフォームでは、制御スクリプト *EMCtrl.sh start* を使用してプライマリを起動します。セカンダリを起動するには、*./Introscope Enterprise Manager* コマンドを使用します。

Enterprise Manager フェールオーバーのルール

Enterprise Manager フェールオーバーには以下のルールが適用されます。

- フェールオーバーを設定した Enterprise Manager を起動するときは、各 Enterprise Manager を 1 つずつ起動します。プライマリ/セカンダリ構成の場合は、プライマリを最初に起動する必要があります。
- 両方の Enterprise Manager がプライマリの場合は、2 番目のプライマリは 1 番目のプライマリに障害が発生するまで待機し、1 番目のプライマリが復旧しても制御を中止しません。
- フェールオーバーでは通常、プライマリ、セカンダリ、およびインストールの各ディレクトリは、異なるホスト上にあります。ただし、Introscope インストール (Introscope が最初にインストールされた場所) と Enterprise Manager は同じホスト上に存在する場合があります。詳細については、「[Enterprise Manager フェールオーバーを単一ホストで動作させるための構成 \(P. 114\)](#)」を参照してください。
- Enterprise Manager のホストがプライマリ ホストのいずれかと一致する場合、Enterprise Manager はプライマリの役割を引き継ぎます。
- Enterprise Manager のホストがセカンダリ ホストのいずれかと一致する場合、Enterprise Manager はセカンダリの役割を引き継ぎます。
- Enterprise Manager のホストがプライマリ ホストまたはセカンダリ ホストと一致しない場合、Enterprise Manager は通常どおり起動します。ただし、警告メッセージがログに記録されます。

- セカンダリ Enterprise Manager は、プライマリ Enterprise Manager が起動を待機しているかどうかを 2 分ごと（構成可能）に調べます。待機している場合、セカンダリはプライマリに処理を渡して、シャットダウンします。
[introscope.enterprisemanager.failover.interval](#) (P. 521) プロパティは、プライマリ Enterprise Manager が起動を待機しているかどうかを実行中のセカンダリ Enterprise Manager がチェックする頻度を制御します。
- プライマリ Enterprise Manager は、セカンダリ Enterprise Manager や別のプライマリ Enterprise Manager には処理を渡しません。
- 起動とシャットダウンの順序：フェールオーバーペアを起動するときは、最初にプライマリ Enterprise Manager を起動してから次にセカンダリ Enterprise Manager を起動します。フェールオーバーペアをシャットダウンする場合は、最初にセカンダリを停止してからプライマリを停止します。

プライマリに処理を渡した後のセカンダリ Enterprise Manager の再起動

セカンダリ Enterprise Manager はプライマリに処理を渡すと、JVM を終了します。セカンダリ Enterprise Manager を再起動するかどうかはユーザの判断になります。再起動を実行するには、スクリプトを使用するか、セカンダリ Enterprise Manager を Windows サービスとして実行します。セカンダリは、プライマリに処理を渡すためにシャットダウンする場合、ステータスコード 23 (`org.eclipse.equinox.app.IApplication.EXIT_RESTART`) で終了します。コマンドライン割り込みや Workstation が原因で通常どおりシャットダウンする場合は、セカンダリはステータスコード 0 で終了します。

Windows を使用している場合は、以下のようなコマンドを使用できます。

```
:RESTART  
"Introscope Enterprise Manager"  
IF ERRORLEVEL 23 GOTO RESTART
```

Enterprise Manager フェールオーバーを単一ホストで動作させるための構成

Enterprise Manager フェールオーバーを、共有ファイル システムではなく単一ホスト上で動作するように構成できます。単一ホスト上に Enterprise Manager フェールオーバーをセットアップして、最初の Enterprise Manager に障害が発生したときに 2 番目の Enterprise Manager が引き継ぐようにすることができます。以下のアクティビティを実行しない場合、単一ホストでフェールオーバーをセットアップします。

- Windows サービスとしての Enterprise Manager の実行
- シェル スクリプトを使用した Enterprise Manager の再起動

重要: 同じホスト上に両方のフェールオーバー Enterprise Manager を設定すると、重大な停止を招くハードウェア プラットフォーム障害が発生する可能性がある単一障害点が作成されます。

以下の手順に従います。

1. *IntroscopeEnterpriseManager.properties* ファイル内の Enterprise Manager プロパティを以下のように設定します。
 - *introscope.enterprisemanager.failover.enable=true*
 - *introscope.enterprisemanager.failover.primary=localhost*
2. 最初のプライマリ Enterprise Manager を、Introscope Enterprise Manager.exe をクリックして起動します。
3. 2 番目のプライマリ Enterprise Manager を、Introscope Enterprise Manager.exe をクリックして起動します。

2 番目のプライマリ Enterprise Manager が正常に起動したら、コマンド プロンプト (コンソール) に、「*acquiring primary lock (プライマリ ロックを取得中)*」というメッセージが表示されます。このメッセージが表示されない場合は、フェールオーバーが正しく設定されていないか、またはプライマリ Enterprise Manager が実行されていません。

MOM フェールオーバーおよび CA CEM TIM について

CA APM 環境に CA CEM をデプロイしている場合、各 TIM と接続するよう MOM を構成します。TIM を有効にすると、MOM によって TIM に 2 つの IP アドレスが与えられます。MOM IP アドレスと、TIM コレクション サービスを実行するコレクタの IP アドレスです。このコレクタは TIM に接続して、TIM データを収集します。

MOM フェールオーバーを設定していて、TIM が実行され、有効になっている場合、プライマリ MOM によって TIM に以下の情報が提供されます。

- プライマリ MOM の IP アドレス
- 設定されている場合は、IntroscopeEnterpriseManager.properties ファイルに定義されたセカンダリ MOM の IP アドレス。

これらの IP アドレスは TIM に格納されます。 [Wily System Setup] - [TIM] - [TIM Settings] ページで確認できます。

フェールオーバー MOM が TIM に接続するには、以下の条件を満たす必要があります。

- TIM が実行され、有効になっている。
- IntroscopeEnterpriseManager.properties ファイルのプロパティが正しく設定されている。
 - IntroscopeEnterpriseManager.failover.enable プロパティが true に設定されている。
 - 1つ以上のプライマリ MOM の IP アドレスが introscope.enterprisemanager.failover.primary プロパティに定義されている

注: プライマリ MOM の IP アドレスを複数定義する場合は、セカンダリの IP アドレスを定義する必要はありません。

- プライマリ MOM の IP アドレスを 1 つのみ定義する場合、IntroscopeEnterpriseManager.properties ファイル内の introscope.enterprisemanager.failover.secondary プロパティに 1 つ以上のセカンダリ MOM の IP アドレスを定義します。

注: 必要に応じて、複数のセカンダリ MOM を定義できます。

- フェールオーバー MOM のアドレスを変更する場合は、すべての TIM を無効にしてから有効にします。TIM を有効にすると、TIM が新しいフェールオーバー MOM の IP アドレスを取得できます。CEM コンソールでフェールオーバー MOM の IP アドレスを確認できます。[TIM Settings] ページの [TessIpAddr] フィールドを確認します。

これらの条件を満たしている場合、プライマリ MOM に障害が発生すると、フェールオーバー MOM は自動的に TIM に接続します。フェールオーバーは、別のプライマリ MOM、またはセカンダリ MOM に対して設定できます。

これらの条件を満たしていない場合、MOM に障害が発生すると以下のアクションが発生します。

| 条件 | MOM の失敗時 |
|---|--|
| TIM が実行されておらず、有効になっていない。 | MOM の失敗前、または失敗後に、TIM に接続されません。TIM が MOM に認識され、MOM 接続を受信するには、実行され、有効になっている必要があります。 |
| IntroscopeEnterpriseManager.failover.enable プロパティが <i>false</i> に設定されている。 | コレクタは引き続き TIM からデータを取得しますが、別のプライマリまたはセカンダリ MOM は TIM への接続を試行しません。 代替のプライマリまたはセカンダリ MOM はコレクタに接続します。 |
| MOM の追加のプライマリまたはセカンダリ IP アドレスが定義されていない。 | コレクタは引き続き TIM からデータを取得しますが、別のプライマリまたはセカンダリ MOM は TIM への接続を試行しません。MOM 構成の変更は TIM に送信されません。 |

Enterprise Manager のクラスタの設定

Enterprise Manager のクラスタを設定するには、プロパティファイルで Enterprise Manager の役割およびクラスタ関連のプロパティを定義します。

重要: CA APM のクラスタ内およびクラスタ全体で、MOM、コレクタ、および CDV 用に別々の *domains.xml* ファイルを用意しないでください。

MOM は、ライブ エージェント（クラスタに現在データを送信しているエージェント）についてクラスタ内で異なるドメインを処理できます。しかし、MOM とコレクタとで履歴エージェント用の異なるドメインを持つことにより、履歴データの MOM ビューにおいて一貫性が保たれなくなる可能性があります。このような混合ドメインを持つクラスタでは、コレクタ上の履歴エージェントは追跡されません。したがってこれらのデータは、履歴エージェントを明示的にマウントしない限り、MOM によって作成された Workstation グラフには表示されません。この状況を回避するために、CA Technologies では、クラスタ内の MOM およびすべてのコレクタ上に同一の domains.xml ファイルを配置することを強く推奨します。こうすることで、特定のコレクタに関連する Workstation 上の履歴データを表示するために履歴エージェントをマウントしなくても、ライブエージェントおよび履歴エージェントのデータが常に MOM Workstation から参照できるようになります。

クロスクラスタデータビューア（CDV）をデプロイする場合、CDV の domains.xml ファイルには以下のドメインが含まれている必要があります。

- CDV の接続先となる全コレクタの全ドメイン。
- CDV のデータ収集元となるコレクタが含まれる全クラスタにまたがる全ドメイン。

あるドメインがコレクタの domains.xml ファイル内に存在し、CDV の domains.xml ファイル内に存在しない場合、以下のことが起こります。

- CDV は、存在しないコレクタ ドメインのデータを収集しません。
- CDV Workstation は、存在しないコレクタ ドメインのデータを表示しません。

注: domains.xml の操作の詳細については、「CA APM セキュリティガイド」を参照してください。

MOM の設定

introscope.enterprisemanager.clustering.mode プロパティを設定し、Enterprise Manager をコレクタセットに対する MOM として指定します。

以下の手順に従います。

1. MOM の <EM_Home>\%config ディレクトリにある IntroscopeEnterpriseManager.properties ファイルを開きます。

2. 「introscope.enterprisemanager.clustering.mode=MOM」と設定します。
3. MOM が管理する各コレクタの接続プロパティを定義します。各コレクタにつき、MOM プロパティ ファイル内でこれらのプロパティを定義します。各接続プロパティの <emName> は、コレクタ Enterprise Manager の任意の同じ識別子です。
 - introscope.enterprisemanager.clustering.login.<emName>.host - コレクタのホスト名または IP アドレスを指定します。
 - introscope.enterprisemanager.clustering.login.<emName>.port - コレクタのリスナーポートを指定します。
 - introscope.enterprisemanager.clustering.login.<emName>.publickey - このプロパティのコメント化を解除して、以下のデフォルト値に設定します。

config/internal/server/EM.public

接続プロパティを個別に設定した場合、これらはホット設定サービスを使用して有効になります。

4. ファイルを保存して閉じます。
5. Enterprise Manager を再起動して、これらのプロパティ設定を有効にします。

introscope.enterprisemanager.clustering.mode プロパティには、Enterprise Manager の再起動が必要です。

コレクタの設定

プロパティを設定して、Enterprise Manager をコレクタとして指定し、コレクタに接続できる CDV の最大数を設定します。

以下の手順に従います。

1. コレクタの <EM_Home>%config ディレクトリにある IntroscopeEnterpriseManager.properties ファイルを開きます。
2. 「introscope.enterprisemanager.clustering.mode=Collector」と設定します。
3. (オプション) このコレクタに特別な識別子を指定する場合は、プロパティ introscope.enterprisemanager.clustering.collector.identifier を設定します。

コレクタに特別な識別子を指定しない場合は、デフォルトの `host@port` が使用されます。ホストは Enterprise Manager のホスト名で、ポートは Enterprise Manager の接続ポートです。

4. ファイルを保存して閉じます。
5. Enterprise Manager を再起動して、これらのプロパティ設定を有効にします。
6. (オプション) コレクタへ接続できる CDV の最大数を設定します。

重要: コレクタおよび CDV 9.1 で有効: すべてのコレクタおよび CDV は、バージョン 9.1 以降の同じバージョンである必要があります。CDV は、異なるバージョンの CDV またはコレクタが混在しているクラスタ内のコレクタには接続できません。

このコレクタに接続する CDV を 1 つ以上設定する場合は、このプロパティを環境に応じて設定します。

- a. コレクタの `<EM_Home>%config` ディレクトリ内の `apm-events-thresholds-config.xml` ファイルを開きます。
- b. `introscope.enterprisemanager.collector.cdv.max` プロパティを設定します。
- c. `apm-events-thresholds-config.xml` ファイルを保存します。

これらの設定は、Enterprise Manager がホットデプロイ中にプロパティ ファイルを調べるとき (約 60 秒ごとに行われます) に適用されます。

CDV の概要

クロス クラスタ データ ビューア (CDV) は、複数のクラスタ内の複数のコレクタからエージェントおよびカスタマ エクスペリエンスのメトリック データを収集することに特化した Enterprise Manager です。CDV Workstation を使用すると、コレクタによって提供されるエージェ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の統合ビューを表示するためのダッシュボードを作成して表示できます。コレクタは組織のさまざまなデータセンターに配置できます。各コレクタは、複数の CDV に接続可能であるため、異なる CA APM クラスタにレポートしているアプリケーションを柔軟に監視および表示できます。

それぞれに独自のクラスタを持つ複数の CA APM を大規模にデプロイしている場合、CDV Workstation を使用することによって各クラスタ内のアプリケーションを監視できるようになります。この機能により、アプリケーションの問題が発生しているクラスタを特定できます。

注: エージェントは CDV に接続しません。

CDV に接続されているコレクタの図を参照する場合、CDV Workstation APM ステータス コンソール内の Enterprise Manager マップを表示できます。

注: APM ステータス コンソールの使用方法の詳細については、「CA Introscope Workstation ユーザ ガイド」を参照してください。

重要: コレクタおよび CDV 9.1 で有効: すべてのコレクタおよび CDV は、バージョン 9.1 以降の同じバージョンである必要があります。CDV は、異なるバージョンの CDV またはコレクタが混在しているクラスタ内のコレクタには接続できません。

コレクタはそれぞれ、`introscope.enterprisemanager.collector.cdv.max` プロパティで設定されたさまざまな数の CDV に接続できます。これにより、CA APM 管理者または triager (切り分け担当) が、複数アプリケーションの監視ビューを提供するダッシュボードを作成できます。たとえば、CA APM 環境は以下のクラスタおよび Enterprise Manager から構成されます。

- 3つのクラスタ: A、B および C
- 3つの CDV: 1、2 および 3
- 5つのコレクタ: 4、5、6、7 および 8
 - コレクタ 4 および 5 はクラスタ A 内にあります。
 - コレクタ 6 および 7 はクラスタ B 内にあります。
 - コレクタ 8 はクラスタ C 内にあります。

CA APM 管理者は以下のように 3 つの CDV を設定します。

- CDV 1 は、クラスタ A および B 内にある、コレクタ 4 および 6 に接続します。
- CDV 2 は、クラスタ A および C 内にある、コレクタ 4 および 8 に接続します。
- CDV 3 は、クラスタ A および C 内にある、コレクタ 5 および 8 に接続します。

CDV の設定

コレクタセットの1つを監視するように、CDV を設定できます。コレクタが別のクラスタ内にあってもかまいません。

以下の手順に従います。

1. CDV の `<EM_Home>%config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. 「`introscope.enterprisemanager.clustering.mode=CDV`」と設定します。
3. CDV が接続するコレクタのそれぞれに接続プロパティを定義します。

重要: コレクタおよび CDV 9.1 で有効: すべてのコレクタおよび CDV は、バージョン 9.1 以降の同じバージョンである必要があります。CDV は、異なるバージョンの CDV またはコレクタが混在しているクラスタ内のコレクタには接続できません。

コレクタごとに、以下のプロパティを定義します。各プロパティの `<emName>` は、コレクタの同じ任意の識別子です。

- `introscope.enterprisemanager.clustering.login.<emName>.host` - コレクタのホスト名または IP アドレスを指定します。
- `introscope.enterprisemanager.clustering.login.<emName>.port` - コレクタのリスナポートを指定します。
- `introscope.enterprisemanager.clustering.login.<emName>.publickey` 公開鍵 -- このプロパティのコメント化を解除して、デフォルト値 `config/internal/server/EM.public` に設定します。

接続プロパティを個別に設定した場合、これらはホット設定サービスを使用して有効になります。

4. `IntroscopeEnterpriseManager.properties` ファイルを保存します。
5. Enterprise Manager を再起動して、これらのプロパティ設定を有効にします。

`introscope.enterprisemanager.clustering.mode` プロパティには、Enterprise Manager の再起動が必要です。

CA APM 管理者および triager (切り分け担当) は、CDV Workstation ダッシュボードおよび Investigator メトリック ブラウザ ツリー内に設定されたコレクタのすべてからエージェント メトリック データを表示できます。

第 7 章: MOM エージェント負荷分散の設定

CA APM のクラスタ環境では、エージェント負荷分散がサポートされます。MOM はメトリックの負荷および CA Introscope 設定に基づいて、エージェント接続を分散させます。エージェントは利用可能なコレクタに接続します。

このセクションには、以下のトピックが含まれています。

[エージェント負荷分散の概要 \(P. 123\)](#)

[MOM がコレクタにエージェントを割り当てる方法 \(P. 124\)](#)

[MOM がクラスタのバランスを再調整する方法 \(P. 125\)](#)

[エージェント負荷分散のメトリック重み係数の設定 \(P. 126\)](#)

[エージェント負荷分散のメトリックしきい値の設定 \(P. 127\)](#)

[エージェント負荷分散の間隔プロパティの設定 \(P. 128\)](#)

[エージェント負荷分散の使用シナリオ \(P. 129\)](#)

[コレクタへのエージェントの割り当ての構成 \(P. 131\)](#)

エージェント負荷分散の概要

MOM は、関与しているエージェントを過負荷のコレクタから切断することにより、コレクタ間のメトリック数を均等にします。接続解除されたエージェントは MOM に再接続し、負荷の小さいコレクタにリダイレクトされます。負荷分散は、エージェントメトリックの負荷のみが対象となります。CA CEM データは負荷分散の対象とはなりません。

8.0 より前のエージェントに有効: 8.0 より前のエージェントは MOM に接続できません。代わりにコレクタの 1 つに直接接続する必要があります。8.0 より前のエージェントが MOM に接続しようとする、以下が発生します。

- MOM が接続を拒否する。
- CA Introscope が MOM ログとエージェント ログの両方に警告メッセージを書き込む。

注: 過負荷状態にあるコレクタの負荷分散を実行する場合、バージョン 9.1 より前の CA APM では、MOM は、コレクタに直接接続するように設定されたエージェントを対象にしていませんでした。CA APM バージョン 9.1 から、MOM は 9.1 以前および 9.1 以降のエージェントを対象にして切断できるようになりました。バージョン 9.1 以前およびそれ以降のエージェントの特定のコレクタへの接続を保持して、負荷分散を行わないようにするには、loadbalancing.xml に agent-Collector エlement を追加します。

注: クラスタがエージェントと TIM を含む全負荷を処理している場合は、Enterprise Manager サービスを実行しているコレクタに対して [重み係数](#) (P. 126) を使用します。Enterprise Manager サービスでは、リソースの増加が必要になる場合があります。重み係数を使用すると、メトリック キャパシティが減少しても対処できます。

MOM がコレクタにエージェントを割り当てる方法

MOM がコレクタにエージェントを割り当てる方法は、いくつかの要因で決まります。

- コレクタとエージェントとの接続履歴がない

エージェントが初めて起動したか再起動した場合、コレクタとの接続履歴はありません。この場合、MOM は負荷分散設定に基づいて、許可された利用可能なコレクタへエージェントを割り当てます。

- 接続タイプ

エージェントは、MOM への接続に使用する接続タイプと同じ接続タイプをサポートするコレクタにのみ割り当てられます。たとえば、エージェントが HTTP を使用して MOM に接続する場合、コレクタでも HTTP 接続を有効にする必要があります。接続タイプの詳細については、「CA APM Java Agent 実装ガイド」または「CA APM NET Agent 実装ガイド」を参照してください。

- loadbalancing.xml ファイルで行った設定

loadbalancing.xml ファイルで以下の設定をします。

- <include> ステートメントを設定すると、エージェントが特定のコレクタセットに接続することを許可します。
- <exclude> ステートメントを設定すると、エージェントが特定のコレクタセットに接続することを拒否します。

- ラッチ済みのプロパティを `true` に設定すると、許可された 1 つのコレクタセットの特定の優先コレクタへエージェントを接続します。
- 特定のコレクタとエージェントとの接続履歴

CA Introscope には、エージェントがあるコレクタからクラスタ内の別のコレクタへ転送される際に、SmartStor データが急増するのを防ぐ機能が含まれます。1 つのエージェントがすでにコレクタに接続されている場合、MOM は以降の接続でもそのコレクタを優先的に使用しますが、以下の要因がある場合は除きます。

 - コレクタが、`loadbalancing.xml` で許可されないように設定されている。
 - 低負荷の代替コレクタが利用可能である。
 - 優先コレクタが過負荷状態にある。
- `IntroscopeEnterpriseManager.properties` ファイルで行った設定

`IntroscopeEnterpriseManager.properties` ファイルで以下の設定をします。

 - エージェント負荷分散のメトリック重み係数を設定する。
 - エージェント負荷分散のメトリックしきい値を設定する。
 - [きめの細かいエージェント接続設定 \(P. 143\)](#) については、`introscope.apm.agentcontrol.agent.allowed` プロパティを設定します。これにより、コレクタが `loadbalancing.xml` で定義されていないエージェントを許可または拒否する手順が提供されます。

MOM がクラスタのバランスを再調整する方法

MOM は、クラスタ メトリックの負荷がアンバランスになったことを検知すると、エージェントをコレクタから切断して、他のコレクタに転送できます。クラスタがアンバランス状態になるのは、任意のコレクタ メトリックの負荷と重み調整されたクラスタの平均値の差が、設定された許容度しきい値を超えた場合です。

クラスタがアンバランス状態になるには、以下の例で示すように、いくつかの理由があります。

- コレクタ プロセスが停止されたか、エージェントが切断された。
- 新しいコレクタがクラスタに追加された。

- 1つのコレクタに多数のエージェントが直接接続されている。

MOM は、クラスタがアンバランスかどうかを一定の間隔でチェックします。クラスタがアンバランスの場合、MOM はメトリックの負荷が比較的高いコレクタからエージェントを切断することで、バランスの再調整を試みます。切断されたエージェントは MOM に再接続し、比較的負荷の低いコレクタに転送されます。この目的は、重み調整後のメトリック負荷をクラスタ全体で均一にするようにエージェントを割り当てるためです。エージェントが同じコレクタに再割り当てされると MOM が判断した場合、MOM はエージェントを切断しません。

エージェント負荷分散のメトリック重み係数の設定

エージェント負荷分散を設定する場合、MOM は重み調整された負荷に基づいてエージェントをコレクタに割り当てます。クラスタ内の個々のコレクタの重み係数を調整することができます。クラスタ内でのコレクタの相対的な優先度は、コレクタが処理できるメトリックの数によって決まります。コレクタが処理できるメトリックの数は、以下を含めた多数の要因の影響を受けます。

- 利用可能な CPU のキャパシティ
- メモリ
- Smartstor ディスク IO のパフォーマンス
- CA CEM データ負荷を処理する、任意の割り当てられた Enterprise Manager サービスをコレクタが実行するかどうか

エージェント負荷分散を設定するとき、MOM によってより少ないメトリックがより容量の少ないコレクタへ割り当てられるように、重み係数を設定できます。より負荷の高いメトリックはより優先度の高いコレクタが処理できるようにメトリックの重み負荷を設定することで、クラスタのパフォーマンスに関する問題を防ぐことができます。

`introscope.enterprisemanager.clustering.login.<emID>.weight` プロパティの値は整数で、コレクタの相対的な負荷を制御します。特定のコレクタの重みの値をクラスタのすべての重みの値の合計で割った値が、そのコレクタに割り当てられるメトリック負荷の割合（パーセンテージ）です。[MOM がコレクタにエージェントを割り当てる方法 \(P. 124\)](#)を決定する要因によって、この動作は変更されます。

注: `introscope.enterprisemanager.clustering.login.<emID>.weight` プロパティ名の `<emID>` は任意の識別子です。コレクタにはそれぞれ固有の識別子があります。使用している環境に適した識別子を指定します。

それ以降、コレクタへのエージェントの割り当ておよびエージェントメトリック負荷の再分散の際には、MOM は重み調整されたメトリック数を使用します。

たとえば MOM が、現在 0 個のメトリックしか報告されていない 3 つのコレクタすべてに接続したとします。

3 つのコレクタには、以下の重み設定があります。

- コレクタ A の重みは 150 です。
- コレクタ B の重みは 100 です。
- コレクタ C の重みは 50 です。

MOM は、メトリックをコレクタ A、B、および C におよそ 3:2:1 の割合で割り当てます。

以下の手順に従います。

1. `<EM_Home>/config` ディレクトリにある `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. コレクタへの重み負荷係数を割り当てるには、次のプロパティを設定します。
`introscope.enterprisemanager.clustering.login.<emID>.weight`
3. `IntroscopeEnterpriseManager.properties` ファイルを保存して閉じます。

エージェント負荷分散のメトリックしきい値の設定

`introscope.enterprisemanager.loadbalancing.threshold` プロパティでは、メトリックの不均衡に対するクラスタの耐性（すなわちしきい値）を設定します。

`introscope.enterprisemanager.loadbalancing.threshold` プロパティのデフォルト設定は 20,000 メトリックです。つまり、MOM がエージェントを再分散する前に、コレクタのメトリックの 20,000 個が不均衡になっている必要があります。重み調整されたクラスタの平均値（しきい値以上）より低い場合、またはそれより高い場合、コレクタは不均衡になります。例については、「[エージェント負荷分散の使用シナリオ \(P. 129\)](#)」を参照してください。

負荷分散のしきい値は、再分散を頻繁に行う必要がないように設定してください。エージェントメトリック負荷は、かなり安定している傾向があります。しきい値の設定が低すぎる場合、問題調査中に生成された一時的なメトリックが再分散を発生させることがあります。

以下の手順に従います。

1. `<EM_Home>/config` ディレクトリにある `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. メトリックの不均衡に対するクラスタの耐性を設定するには、次のプロパティを設定します。
`introscope.enterprisemanager.loadbalancing.threshold`
3. `IntroscopeEnterpriseManager.properties` ファイルを保存して閉じます。

エージェント負荷分散の間隔プロパティの設定

`introscope.enterprisemanager.loadbalancing.interval` プロパティは、クラスタで再分散の可能性があるかどうかを確認する間隔を MOM に伝えます。デフォルト間隔は 600 秒（10 分）で、最小間隔は 120 秒（2 分）です。

エージェントの再割り当て後にクラスタが再調整を行うための時間（数分間）が必要です。負荷分散の間隔が短すぎると、クラスタが直前の負荷分散に対する調整を完了する前に再分散が再開される恐れがあります。アプリケーション問題切り分けマップを使用すると、リスクはより大きくなります。この場合は、エージェントの再割り当て時に、エージェントがアプリケーション問題切り分けマップデータを新しいコレクタに再送信する必要があり、時間がかかることがあります。以下のアクションを実行した場合は、再分散を頻繁に実行しすぎると起こる不安定な状態の兆候に注意してください。

- **CA Introscope8.x で有効**：CA Introscope8.x の負荷分散のデプロイ
- 負荷分散の間隔をデフォルト未満に設定

以下の手順に従います。

1. `<EM_Home>/config` ディレクトリにある `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. クラスタの負荷分散を MOM が確認する頻度を設定するには、次のプロパティを設定します。
`introscope.enterprisemanager.loadbalancing.interval`
3. `IntroscopeEnterpriseManager.properties` ファイルを保存して閉じます。

エージェント負荷分散の使用シナリオ

ここでは、クラスタ環境におけるエージェント負荷分散の動作を理解するために役立つシナリオをいくつか説明します。

新しいコレクタがクラスタに追加されたときのエージェント負荷分散

コレクタ A、B、および C のクラスタが過負荷状態であると判断しました。

MOM 上の `IntroscopeEnterpriseManager.properties` ファイルに接続プロパティのセットを追加することにより、コレクタ D を動的に追加します。さらに、このクラスタ内のすべてのコレクタの再分散のしきい値を 10,000 メトリックに設定します。`IntroscopeEnterpriseManager.properties` ファイル内の `introscope.enterprisemanager.loadbalancing.threshold` プロパティを設定することで、この設定をしていました。

コレクタ D に報告されるメトリックは 0 ですが、コレクタ A、B、および C にそれぞれ報告される平均のメトリック負荷は 30,000 メトリックです。以下の要因により、MOM はクラスタを再分散します。

- 30,000 メトリックと 0 メトリックという平均負荷の差が、しきい値の 10,000 メトリックを上回っている。

MOM はコレクタ A、B、および C からそれぞれ 7,000 のメトリックを再分散し、その合計 21,000 のメトリックをコレクタ D に報告するようにすべて転送します。再分散後に、23,000 のメトリックがコレクタ A、B、および C それぞれに報告し、21,000 のメトリックがコレクタ D に報告します。

コレクタがエージェント付きで追加されたときのエージェント負荷分散

MOM がコレクタ A および B へ接続します。36,000 のメトリックがコレクタ A に報告し、30,000 のメトリックがコレクタ B に報告しています。IntroscopeEnterpriseManager.properties ファイル内の introscope.enterprisemanager.loadbalancing.threshold プロパティを使用して、メトリックしきい値を 10,000 メトリックに設定します。24,000 メトリックからの報告を受けるコレクタ C がクラスタに追加されます。

MOM は、以下の理由によりメトリックの負荷を再分散しません。

- 平均値が、コレクタ当たり 30,000 メトリックである。(36,000 + 30,000 + 24,000) = 90,000 メトリック / 3 コレクタ)
- いずれのコレクタも、平均値の 30,000 との差がしきい値の 10,000 メトリック以内である。

コレクタ障害時のエージェント負荷分散

MOM がコレクタ A、B、および C に接続します。36,000 メトリックがコレクタ A に報告し、30,000 メトリックがコレクタ B に報告し、24,000 メトリックがコレクタ C に報告しています。コレクタ A に障害が発生し、コレクタ A に報告していたエージェントが MOM に再接続します。MOM は約 15,000 メトリックをコレクタ B へ、約 21,000 メトリックをコレクタ C へそれぞれ転送します。これで、コレクタ B および C の両方にそれぞれ 45,000 メトリックが報告されます。

コレクタ再起動時のエージェント負荷分散

コレクタ A が障害から回復すると、クラスタが不均衡になります。平均のメトリック負荷は 30,000 メトリック ([0 + 45,000 + 45,000] / 3) です。ただし、コレクタ B および C にはそれぞれに報告している 45,000 のメトリックがあり、その 45,000 のメトリックは以下のような状態です。

- 平均を 15,000 メトリック上回っている
- しきい値の 10,000 メトリックを超えている

そのため、MOM はコレクタ B および C からそれぞれ合計 15,000 メトリックのエージェントを切断し、30,000 メトリックをすべてコレクタ A へ転送します。これにより、コレクタ A、B、および C へそれぞれ 30,000 メトリックが報告されるようになります。

重みによるエージェント負荷分散

MOM がコレクタ A、B、および C に接続します。しきい値は 10,000 に設定されています。24,000 メトリックがコレクタ A に報告し、30,000 メトリックがコレクタ B に報告し、36,000 メトリックがコレクタ C に報告して、合計は 90,000 メトリックです。クラスタのコレクタの平均メトリックは 30,000 です。コレクタ A の重みを 150、コレクタ B の重みを 100、コレクタ C の重みを 50 に設定します。重みの平均は 100 になります（重みの合計 $150 + 100 + 50$ をコレクタの数 3 で割った数）。

理想的には、各コレクタのメトリックの負荷はその相対的重みに比例します。コレクタ A の重みは 150 のため、理想的なメトリックは 45,000 です。この重みは平均より 50% 多いため、理想的なメトリックの負荷は平均値の 30,000 メトリックよりも 50% 多いものになります。コレクタ B の重みは平均値であるため、理想的なメトリックの負荷は平均値、つまり 30,000 メトリックになります。コレクタ C の重みは平均値の 50% であるため、理想的なメトリックの負荷は平均値の 50%、つまり 15,000 メトリックになります。

これらの相対的重みやメトリックの平均値に基づく、クラスタは不均衡になっています。コレクタ A は、重み調整された平均値よりも（しきい値以上）低いため（ $24,000 - 45,000 = -21,000$ ）、低負荷状態です。コレクタ B は 30,000 メトリックのため完全にバランスが取れています。このメトリックの負荷は、重み調整された平均値と同じです。コレクタ C は、重み調整された平均値（10,000 メトリックしきい値以上）を超えているため（ $36,000 - 15,000 = 21,000$ ）、過負荷状態です。MOM はコレクタ C から 21,000 メトリックを持つエージェントを外し、それらをコレクタ A へ転送することで、クラスタを再分散します。

コレクタへのエージェントの割り当ての構成

MOM loadbalancing.xml を使用して、MOM のロードバランサが接続元エージェントをどのようにコレクタに割り当てるかを制御するエージェントエレメントを構成できます。include エレメントおよび exclude エレメントを構成して、特定の Enterprise Manager へのエージェント接続を許可または禁止できます。

注: 過負荷状態にあるコレクタの負荷分散を実行する場合、バージョン 9.1 より前の CA APM では、MOM は、コレクタに直接接続するように設定されたエージェントを対象にしていませんでした。CA APM バージョン 9.1 から、MOM は 9.1 以前および 9.1 以降のエージェントを対象にして切断できるようになりました。バージョン 9.1 以前およびそれ以降のエージェントの特定のコレクタへの接続を保持して、負荷分散を行わないようにするには、loadbalancing.xml に agent-Collector エlement を追加します。

以下の手順に従います。

1. MOM 上の <EM_Home>/config ディレクトリに移動します。
2. loadbalancing.xml を開きます。
3. 環境の要件に応じて、プロパティを定義します。

これらのプロパティを定義するとき、以下のガイドラインおよび[エージェントの負荷分散の設定例](#) (P. 136)を使用します。

- <agent-collector name> 属性はオプションです。
- MOM ロード バランサは <agent-collector> Element を順番に評価します。

接続元エージェントが <agent-specifier> 正規表現に一致すると、<include> リストに含まれるコレクタの 1 つに割り当てられます。loadbalancing.xml 内で最初に一致した <agent-specifier> が優先されます。<include> リストがない場合、エージェントは <exclude> リストに含まれないコレクタに割り当てられます。これらの制限を満たす利用可能なコレクタがない場合、エージェントのコレクタ接続要求は拒否されます。

- <agent-collector> Element ごとに、エージェントのセットに一致する <agent-specifier> Element を 1 つまたは複数定義します。
- <agent-specifier> のテキストの内容が *¥|. *¥|EPAgent1</agent-specifier> などの Perl5 正規表現であることを確認します。

注: エージェント指定子の正規表現には、エージェントパス名の3つのエレメント <host machine name>|<custom process name>|<agent name> が含まれる必要があります。たとえば、EPAgent で始まる名前を持つエージェントすべてを含めるように、次のコンテンツを使用します。

```
<agent-specifier>.*%|..*%|EPAgent.*</agent-specifier>
```

- <agent-collector> エレメントでは、include リストが空の場合があります。include リストには、エージェントが接続を許可されたコレクタを含めることもできます。

- include リストが空の場合、エージェントはコレクタへ接続することを許可されません。

```
<include>  
</include>
```

- <include> エレメントおよび </include> エレメントに、エージェントが接続できるコレクタを追加できます。

この例では、エージェントは localhost@5002 という名前のコレクタ上でのみ許可されます。

```
<include>  
  <collector host="localhost" port="5002"/>  
</include>
```

- <agent-collector> エレメントでは、exclude リストが空の場合があります。exclude リストには、エージェントが接続を許可されていないコレクタを含めることもできます。

- exclude リストが空の場合、エージェントはすべてのコレクタへの接続を許可されます。

```
<exclude>  
</exclude>
```

- <exclude> エレメントおよび </exclude> エレメントに、エージェントが接続を許可されていないコレクタを追加できます。

この例では、エージェントは localhost@5002 という名前のコレクタ上でのみ許可されていません。

```
<exclude>  
  <collector host="localhost" port="5002"/>  
</exclude>
```

- `latched` プロパティを `true` に設定して、特定のコレクタが利用可能なときはいつも、そのコレクタへの接続を優先することを示します。このコレクタはラッチ済みコレクタと呼ばれます。

この例では、エージェントはポート 6001 上の `newCollector-ip` という名前のコレクタにラッチされます。`newCollector-ip` が利用不可のときは、MOM はエージェントを `Collector1-ip` へ割り当てることができます。

```
<include>
  <Collector host="newCollector-ip" port="6001" latched="true" />
  <Collector host="Collector1-ip" port="6001" />
</include>
</agent-Collector>
```

`include` リストへ 1 つのコレクタのみを追加する場合、ラッチ済みプロパティの設定は必要ありません。

複数のコレクタが「`latched=true`」に設定されている場合、接続設定はすべてのラッチ済みコレクタに適用されます。

ラッチ済みプロパティが `true` に設定され、コレクタが過負荷状態になっているとき、MOM はコレクタからエージェントを切断しません。ラッチ済みコレクタがダウンすると、切断されたエージェントは別に許可された利用可能なラッチ済みコレクタに接続します。

利用可能なラッチ済みコレクタがない場合、エージェントは許可されたコレクタに接続します。利用可能な許可されたコレクタがない場合、[エージェントの動作はエージェントのバージョンで決まります \(P. 150\)](#)。

たとえば、環境に 10 個のコレクタがある場合、エージェントを 1 つ以上のコレクタにラッチするよう設定できます。ラッチ済みコレクタがすべて利用不可になる場合、MOM はもう一方の利用可能なラッチされていないコレクタへエージェントを転送できます。

ラッチ済みプロパティがコレクタに設定されないとき、エージェントはそのコレクタに接続しますが、これはラッチ済みコレクタがすべて利用不可の場合のみに起こります。

ラッチ済みプロパティのデフォルト値は `false` です。

- クロス クラスタ データ ビューアを 1 つ以上デプロイ済みであり、負荷分散を使用している場合は、CDV が接続するコレクタへのみ目的のエージェントを接続します。そうでない場合、MOM は、ほかのコレクタへの CDV 接続を使用して、コレクタからエージェントを負荷分散できます。この状況では、以下のイベントが発生します。
 - CDV は、移動されたエージェントに関するメトリック データを収集できません。
 - CDV Workstation ユーザは、移動されたエージェントに関するデータを表示できません。
- 同じクラスタ内でホストされているコレクタにエージェントを負荷分散するには、デフォルトの通信チャンネルと関連付けられているポート番号を指定します。デフォルト ポートは 5001 です。

エージェントから Enterprise Manager への以下の通信プロトコルに対して、正しいポート番号を指定します。

 - 直接ソケット接続
 - HTTP トンネル接続またはプロキシ サーバ経由の HTTP トンネル
 - HTTPS 接続
 - SSL 接続
- 異なるクラスタでホストされているコレクタにエージェントを負荷分散するには、特定のセキュアな通信チャンネルと関連付けられているポート番号を指定します。1 つのクラスタ内の MOM は、別のクラスタ内のコレクタのプロパティを参照できません。

エージェントから Enterprise Manager への以下の通信プロトコルに対して、特定のセキュアな通信チャンネルの正しいポート番号を指定します。

 - 直接ソケット接続。デフォルトの通信チャンネルのポート（デフォルトではポート 5001）を指定します。
 - HTTP トンネル接続またはプロキシ サーバ経由の HTTP トンネル。HTTP ポート（デフォルトでは 8081）を指定します。
 - HTTPS 接続。HTTPS ポート（デフォルトでは 8444）を指定します。
 - SSL 接続。SSL ポート（デフォルトでは 5443）を指定します。

4. loadbalancing.xml を保存して閉じます。

新しい値は、Enterprise Manager がホット デプロイ中にプロパティ ファイルをチェックするとき自動的に有効になります。ホット デプロイは、約 60 秒ごとに実行されます。MOM は、次の負荷分散の間隔で、クラスタの負荷を分散させます。

エージェントの負荷分散の設定例

MOM エージェント負荷分散プロパティを、さまざまな方法で設定できます。以下の設定例にはコード サンプルが用意されています。

- [特定のコレクタまたはコレクタのセットへのエージェントの割り当て \(P. 136\)](#)
- [特定のコレクタまたはコレクタのセットからのエージェントの除外 \(P. 138\)](#)
- [複数のコレクタへの複数のエージェントの割り当て \(P. 138\)](#)
- [同じクラスタ内の特定のコレクタへのエージェントの割り当て \(P. 139\)](#)
- [別のクラスタ内の特定のコレクタへのエージェントの割り当て \(P. 140\)](#)

特定のコレクタまたはコレクタのセットへのエージェントの割り当て

以下の例は、MyAgent という名前のエージェントを、ポート 5001 上の「myhost」という名前のコレクタに割り当てる設定方法を示しています。

```
<agent-collector name="Assign MyAgent to One Collector Example">
  <agent-specifier>.*%|. *%|MyAgent</agent-specifier>
  <include>
    <collector host="myhost" port="5001"/>
  </include>
</agent-collector>
```

以下の例は、ラッチ済みプロパティを設定する方法を示しています。各値は以下のとおりです。

- エージェントはポート 6001 上の「newCollector-ip」という名前のコレクタに接続するように割り当てられます。
- newCollector-ip が利用不可のとき、MOM は、名前に「EPAgent」を含むすべてのエージェントを、Collector1-ip または Collector2-ip のいずれかへ割り当てることができます。


```
<agent-Collector name="Latch when Collector Unavailable Example">
  <agent-specifier>.*%|.*/EPAgent.*</agent-specifier>
  <include>
    <Collector host="newCollector-ip" port="6001" latched="true" />
    <Collector host="Collector1-ip" port="6001" />
    <Collector host="Collector2-ip" port="6001" />
  </include>
</agent-Collector>
```

以下の例は、エージェントを割り当てる方法を示しています。各値は以下のとおりです。

- コレクタは、ポート 5001 および 5002 で「localhost」という名前です。
- コレクタ localhost:5001 は localhost:5002 よりも優先されます。

```
<agent-collector name="Allow EPAgents on Two Collectors and One is Preferred Example">
  <agent-specifier>.*%|.*/EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
  </include>
</agent-collector>
```

以下の例は、エージェントを割り当てる方法を示しています。各値は以下のとおりです。

- コレクタは、ポート 5001、5002、5003 および 5004 の「localhost」という名前です
- コレクタ localhost:5001 および localhost:5003 は、localhost:5002 および localhost:5004 よりも優先されます。

```
<agent-collector name="Allow EPAgents on Four Collectors and Two are Preferred Example">
  <agent-specifier>.*%|.*/EPAgent.*</agent-specifier>
  <include>
    <collector host="localhost" port="5001" latched="true"/>
    <collector host="localhost" port="5002"/>
    <collector host="localhost" port="5003" latched="true"/>
    <collector host="localhost" port="5004"/>
  </include>
</agent-collector>
```

特定のコレクタまたはコレクタのセットからのエージェントの除外

以下の例は、**MyAgent** という名前のエージェントを **MyHost** という名前のコレクタから除外する方法を示しています。

```
<agent-collector name="Exclude MyAgent from a Collector Example">
  <agent-specifier>.*%|.*/MyAgent</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
  </exclude>
</agent-collector>
```

以下の例は、複数のエージェントを複数のコレクタから除外する方法を示しています。

```
<agent-collector name="Exclude Two Agents Assigned from Two Collectors Example">
  <agent-specifier>.*%|.*/MyAgent.*</agent-specifier>
  <agent-specifier>.*%|.*/MyOtherAgent.*</agent-specifier>
  <exclude>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </exclude>
</agent-collector>
```

複数のコレクタへの複数のエージェントの割り当て

以下の例は、複数のエージェントを複数のコレクタに割り当てる方法を示しています。

```
<agent-collector name="Two Agents Assigned to Two Collectors Example">
  <agent-specifier>.*%|.*/MyAgent.*</agent-specifier>
  <agent-specifier>.*%|.*/MyOtherAgent.*</agent-specifier>
  <include>
    <collector host="MyHost" port="5001"/>
    <collector host="MyOtherHost" port="5001"/>
  </include>
</agent-collector>
```

同じクラスタ内の特定のコレクタへのエージェントの割り当て

以下の例は、EPAgent という名前のエージェントをクラスタ内のコレクタに割り当てる方法を示します。条件は以下のとおりです。

- 「host1」と「host2」という名前のコレクタは、両方とも同じクラスタ内にあります。
- host1 または host2 に接続する EPAgent が、以下の接続のいずれかを使用できる。
 - 直接ソケット
 - HTTP
 - HTTPS
 - SSL
- コレクタ host1 および host2 は両方ともポート 5001 をデフォルトの通信チャンネルポートとして使用します。
- host1 が利用不可のとき、MOM は名前に「EPAgent」を含むすべてのエージェントを host2 に割り当てることができます。

host1 と host2 にエージェントを割り当てるには、MOM がデフォルトの通信チャンネルポートを使用し、loadbalancing.xml がそのポートを必要とすることに注意してください。

```
<agent-collector name="Allow EPAgents on Two Collectors in the Same Cluster Example">
```

```
  <agent-specifier>.*%|.*/.*|EPAgent.*</agent-specifier>
```

```
  <include>
```

```
    <collector host="host01" port="5001"/>
```

```
    <collector host="host02" port="5001"/>
```

```
  </include>
```

```
</agent-collector>
```

別のクラスタ内の特定のコレクタへのエージェントの割り当て

以下の例は、EPAgent という名前のエージェントを別のクラスタ内のコレクタに割り当てる方法を示します。条件は以下のとおりです。

- 「host1」と「host2」という名前のコレクタは、別のクラスタ内にあります。
- host1 または host2 に接続する EPAgent が、以下の接続のいずれかを使用できる。
 - 直接ソケット
 - HTTP
 - HTTPS
 - SSL
- host1 が利用不可のとき、MOM は名前に「EPAgent」を含むすべてのエージェントを host2 の特定の通信ポートに割り当てることができます。

host1 と host2 にエージェントを割り当てるには、MOM が EPAgent から Enterprise Manager への特定の通信チャンネルポートを使用し、loadbalancing.xml がそのポートを必要とすることに注意してください。

以下の例は、直接ソケット接続を使用してエージェントがコレクタに接続するとき、別のクラスタ内のコレクタに EPAgent を割り当てる方法を示します。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters - Direct Socket Connection Example">
  <agent-specifier>.*%|.*/EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5001"/>
    <collector host="host02" port="5001"/>
  </include>
</agent-collector>
```

以下の例は、HTTP を使用してエージェントがコレクタに接続するとき、別のクラスタ内のコレクタに EPAgent を割り当てる方法を示します。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters - HTTP Example">
  <agent-specifier>.*%|.*/EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8081"/>
    <collector host="host02" port="8081"/>
  </include>
</agent-collector>
```

以下の例は、HTTPS を使用してエージェントがコレクタに接続するとき、別のクラスタ内のコレクタに EPAgent を割り当てる方法を示します。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters - HTTPS Example">
  <agent-specifier>.*¥|.¥|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="8444"/>
    <collector host="host02" port="8444"/>
  </include>
</agent-collector>
```

以下の例は、SSL を使用してエージェントがコレクタに接続するとき、別のクラスタ内のコレクタに EPAgent を割り当てる方法を示します。

```
<agent-collector name="Allow EPAgents on Two Collectors in Different Clusters - SSL Example">
  <agent-specifier>.*¥|.¥|EPAgent.*</agent-specifier>
  <include>
    <collector host="host01" port="5443"/>
    <collector host="host02" port="5443"/>
  </include>
</agent-collector>
```


第 8 章: Enterprise Manager ネットワークトポロジ エージェントの設定

この機能を使用して、これらのコンピュータにどの特定のエージェントまたはエージェント グループを接続するかを計画して設定できます。

- 特定のスタンドアロン Enterprise Managers
- コレクタ
- コレクタのグループ

CA APM ではこのプロセスを、CA APM Enterprise Manager ネットワークトポロジ (または構造) エージェントの計画および設定として挙げています。

このセクションには、以下のトピックが含まれています。

[エージェントと Enterprise Manager 間のネットワークトポロジの概要](#) (P. 144)

[CA Introscope 間でのエージェント接続情報の継承方法](#) (P. 146)

[設定がエージェントから Enterprise Manager への接続に及ぼす影響](#) (P. 148)

[エージェントが Enterprise Manager からの切断されたときの動作](#) (P. 149)

[エージェントの接続要求が拒否されたときの動作](#) (P. 150)

[Enterprise Manager ネットワークトポロジエージェントの設定プロセス](#) (P. 151)

[Enterprise Manager ネットワークトポロジエージェントの計画](#) (P. 152)

[loadbalancing.xml ルールがないときに新しいエージェント接続を許可するかどうかの設定](#) (P. 154)

[エージェントの再接続待機時間の設定](#) (P. 155)

[禁止されたエージェント接続のクランプ限界値の設定](#) (P. 156)

[許可済み Enterprise Manager へのエージェントの連続的な再接続の設定](#) (P. 157)

[Enterprise Manager によって許可および禁止されるエージェントに関する loadbalancing.xml の設定](#) (P. 159)

[エージェントと Enterprise Manager 間のネットワークトポロジの設定](#) (P. 159)

エージェントと Enterprise Manager 間のネットワークポロジの概要

Enterprise Manager ネットワーク トポロジ エージェントの計画および設定では、CA APM のパフォーマンス問題を回避または削減することが目標になります。以下に回避すべき状況の例を示します。

- 新しいエージェントがランダムに起動されることにより、特定のコレクタが接続であふれる
- テスト環境のエージェントが実運用環境に接続する

以下のファイルおよびプロパティを使用して、エージェントが特定のスタンドアロン Enterprise Manager またはコレクタに接続する方法と時期を制御できます。

- loadbalancing.xml ファイル
- EnterpriseManager.properties ファイル内の introscope.apm.agentcontrol.agent.allowed プロパティ
- IntroscopeAgent.profile ファイル内の introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds プロパティ

[loadbalancing.xml で MOM エージェント負荷分散を設定 \(P. 131\)](#) する際は、以下の要素を考慮して、エージェントの移動先を MOM に指示します。

- コレクタ キャパシティ
- 生成されているエージェント メトリックの数
- コレクタ キャパシティの重み係数

例

環境が 1 つの MOM と 5 つのコレクタで構成されています。エージェント 1 およびエージェント 2 がコレクタ 1 および コレクタ 2 に負荷分散されるようにします。エージェントと Enterprise Manager をこのように接続させる場合は、loadbalancing.xml を以下のように設定します。

- エージェント 1 とエージェント 2 からコレクタ 1 と 2 への接続を許可する。
- これらのエージェントからコレクタ 3、4、5 への接続を許可しない。

過負荷になっている場合、MOM は以下のようにエージェントを処理します。

- 実行時のクラスタ負荷に応じて、エージェント 1 とエージェント 2 をコレクタ 1 とコレクタ 2 に割り当てる。
- これらのエージェントからコレクタ 3、4、5 への接続を許可しない。

また、`loadbalancing.xml` を使用して、エージェントと Enterprise Manager の接続をきめ細かく設定できます。その後、MOM はクラスタ全体でその設定を実行します。この章では、Enterprise Manager とエージェントをきめ細かく接続する方法について説明します。

MOM は、`loadbalancing.xml` に設定された、エージェント接続の許可/拒否ルールを各コレクタに送信します。送信は、起動時、およびその後 10 分間隔で行われます。コレクタは、これらのルールを使用して、エージェントが接続を要求したときにどのエージェントを許可および拒否するかを判断します。以下のアクションが発生したときにエージェントが接続可能なコレクタを認識できるように、コレクタはこれらのルールを各エージェントに送信します。

- MOM がダウンした。
- 拒否構成設定に基づいて、コレクタがエージェントの接続要求を拒否した。

[エージェントが Enterprise Manager への接続を拒否された \(P. 150\)](#) 場合、APM ステータス コンソールの拒否エージェント リストにエントリが表示されます。エージェントが Enterprise Manager にパッシブに接続され、データを送信していない場合にも、APM ステータス コンソールの拒否エージェント リストにエントリが表示されます。

APM ステータス コンソールの拒否エージェント リストを使用して、繰り返し拒否される、または、パッシブ接続である特定エージェントまたはエージェントグループを監視できます。それにより、拒否された、またはパッシブなエージェントが別のコレクタに接続できるように `loadbalancing.xml` を設定できます。

CA Introscope 間でのエージェント接続情報の継承方法

CA Introscope は、エージェントの管理機能を備え、Enterprise Manager 接続情報にこれを提供しており、MOM 上で定義できます。MOM によって、任意の関連付けられた設定が、クラスタ内のコレクタとエージェント間で実行できます。

MOM は、すべてのコレクタに `loadbalancing.xml` を定期的を送信し、クラスタ全体で `loadbalancing.xml` の同期をとります。CA Introscope は、コレクタまたは CDV の `loadbalancing.xml` の設定はすべて無視します。

コレクタが `loadbalancing.xml` を受信した後で MOM がダウンした場合、コレクタは `loadbalancing.xml` を使用して、MOM から受信した設定を許可または拒否します。コレクタが MOM に接続したことがない場合、コレクタは `IntroscopeEnterprismanager.properties` ファイル内の `introscope.apm.agentcontrol.agent.allowed` プロパティを使用して、エージェント接続を許可します。MOM が初めてコレクタに接続するとき、MOM は `introscope.apm.agentcontrol.agent.allowed` プロパティ値をコレクタに転送します。MOM の値はコレクタの値より優先されます。

コレクタはまた、`introscope.apm.agentcontrol.agent.allowed` プロパティを使用して、`loadbalancing.xml` で定義されていないエージェントに対する指示を許可または拒否できるようにします。

MOM はまた、エージェントが接続を許可され、かつエージェントが利用可能である Enterprise Manager のリストを、エージェントに提供します。このリストは Allowed Enterprise Manager リストと呼ばれます。Allowed Enterprise Manager リストは Enterprise Manager の IP アドレスに基づくため、別のクラスタ内の Enterprise Manager を含む可能性があります。

Allowed Enterprise Manager リストは、以下のコンピュータのいずれかが停止したときに、どの Enterprise Manager に接続するかをエージェントに伝えます。

- MOM
- スタンドアロン Enterprise Manager
- エージェントが接続される初期コレクタ

以下の要因の両方が発生すると、Enterprise Manager は loadbalancing.xml の手順に基づいて Allowed Enterprise Manager リストを準備します。

- スタンドアロン Enterprise Manager がダウンした。
- 環境にスタンドアロン Enterprise Manager とクラスタの両方が含まれている。

Allowed Enterprise Manager リストは、別のスタンドアロン Enterprise Manager またはコレクタへと、エージェントを向かわせます。

エージェントが再起動すると、IntroscopeAgent.profile ファイル内の introscope.agent.enterprisemanager.connectionorder プロパティから初期コレクタ接続情報を取得します。許可されたコレクタが、定義された値に加えて、このプロパティに自動的に提供されます。許可された利用可能なコレクタまたはスタンドアロン Enterprise Manager のリストが、エージェントが再起動するまでエージェントのメモリに残ります。再起動後、許可された利用可能な Enterprise Manager のリストはコレクタからエージェントへ送信されます。

設定がエージェントから Enterprise Manager への接続に及ぼす影響

エージェントが Enterprise Manager 上で許可または拒否されるように設定されている場合、エージェントが接続を要求すると Enterprise Manager はさまざまなアクションを実行できます。Enterprise Manager は接続を受理するか、拒否することができます。Enterprise Manager が接続要求を受理すると、エージェントは以下の 2 つの方法のうちのいずれかで接続できます。

- アクティブに接続し、メトリック データを Enterprise Manager に送信します。
- パッシブに接続し、データを送信しません。

[Enterprise Manager が接続要求を拒否する \(P. 150\)](#)と、エージェントの動作はバージョンによって異なります。

エージェントのバージョン、および許可と拒否の設定の両方に基づいて、Enterprise Manager は 3 つのアクションを実行できます。これらのアクションの結果、4 とおりのエージェント接続状態が生じます。このうちの 2 つの状態では、APM ステータス コンソールの拒否エージェント リストにエージェントが表示されます。

以下の表は、許可と拒否の設定されたエージェントが Enterprise Manager に接続を要求したとき、Enterprise Manager、エージェントおよび APM ステータス コンソールがどのような動作をするかを示しています。

| エージェントバージョン | Allowed/Disallowed Configuration | 接続要求に対する Enterprise Manager のアクション | 結果として生じるエージェントの接続状態 | APM ステータス コンソールの拒否エージェント リストの表示 |
|-------------|----------------------------------|------------------------------------|--------------------------|---------------------------------|
| 9.1 | 許可 | アクティブな接続の受理 | 接続されたエージェントがアクティブにデータを送信 | × |
| 9.1 より前 | 許可 | アクティブな接続の受理 | 接続されたエージェントがアクティブにデータを送信 | × |
| 9.1 | 拒否 | 接続の拒否 | 切断 | ○ |

| エージェントバージョン | Allowed/Disallowed Configuration | 接続要求に対する Enterprise Manager のアクション | 結果として生じるエージェントの接続状態 | APM ステータスコンソールの拒否エージェントリストの表示 |
|-------------|----------------------------------|------------------------------------|-----------------------------|-------------------------------|
| 9.1 | 拒否 | パッシブな接続の受理 | 接続されたエージェントがパッシブで、データを送信しない | ○ |
| 9.1 より前 | 拒否 | 接続の拒否 | 切断されたエージェントの接続の再試行 | ○ |

エージェントが Enterprise Manager からの切断されたときの動作

エージェントは、たとえば負荷分散されたか、Enterprise Manager がダウンしたときに、Enterprise Manager から切断されます。また、設定が変更されて Enterprise Manager が以前は接続を許可されていたエージェントを拒否するように指示された特定の状況でも、エージェントは切断されます。Enterprise Manager は、拒否するように新たに設定された、接続済みのエージェントを切断することで、この指示に応答します。

9.1 より前のエージェントで有効： 以下のアクションが発生すると、エージェントは Enterprise Manager から切断されます。

- プロパティまたは `loadbalancing.xml` の設定により、コレクタへのエージェント接続は許可から拒否に変更されます。
- エージェントが接続されている Enterprise Manager は、接続可能でなくなります。

9.1 エージェントで有効： 設定が許可から拒否に変更されて、`introscope.enterprisemanager.agent.disallowed.connection.limit` クランプ値に到達したときに、9.1 のエージェントは Enterprise Manager から切断されます。

エージェントの接続要求が拒否されたときの動作

loadbalancing.xml および introscope.apm.agentcontrol.agent.allowed プロパティの設定に基づいて、エージェントは特定の Enterprise Manager への接続を許可または拒否されます。エージェントが Enterprise Manager への接続を要求すると、Enterprise Manager は接続要求を受理または拒否できません。

以下のいずれかが生じると、エージェントの接続は拒否されます。

- introscope.apm.agentcontrol.agent.allowed プロパティが true に設定され、loadbalancing.xml がエージェントを拒否する
- introscope.apm.agentcontrol.agent.allowed プロパティが false に設定され、loadbalancing.xml が明示的にエージェントを許可しない
- 以下のクランプ値のいずれかに到達または超過した場合
 - introscope.enterprisemanager.agent.disallowed.connection.limit
 - introscope.enterprisemanager.agent.connection.limit

Enterprise Manager がエージェントの接続要求を拒否すると、以下のアクションが発生する可能性があります。

- Enterprise Manager に接続されたエージェントが切断する。
- 切断されたエージェントが、接続を許可されている他の Enterprise Manger へ接続を試行する。

エージェントは接続できるまでか、以下の条件の Enterprise Manager すべてに対する試行を終えるまで、接続を試行し続けます。

- エージェントが接続を許可されている Enterprise Manager
- 接続可能な Enterprise Manager

エージェントがすべての Enterprise Manager から拒否された場合、エージェントがどのように動作するかは、`introscope.agent.profile` ファイルの `introscope.agent.enterprisemanager.failbackRetryIntervallInSecondsproperty` 設定によって異なります。プロパティの設定によって、以下のようになります。

- コメント化が解除されていて継続時間が設定されていると、エージェントは設定された継続時間に基づいて、許可された Enterprise Manager への接続を定期的に試行し続けます。
- 設定されていない（コメント化されている）場合、エージェントは CA APM エージェントのバージョンに基づいて以下のように動作します。
 - **9.1 より前のエージェントで有効**：Enterprise Manager から切断され、再接続を試行し続けます。
 - **9.1 エージェントで有効**：Allowed Enterprise Manager リストの最後の許可された Enterprise Manager にパッシブに接続されます。エージェントは Enterprise Manager にメトリック データを送信しません。Enterprise Manager の構成情報がエージェントを許可状態に変更するのを待って、エージェントは休止します。

Enterprise Manager ネットワークトポロジ エージェントの設定プロセス

Enterprise Manager ネットワーク トポロジ エージェントの設定には、以下の高度な手順が必要です。

1. [Enterprise Manager またはコレクタ トポロジ エージェントを計画します](#) (P. 152)。
2. 組織のデプロイ環境に応じて、`introscope.enterprisemanager.properties` ファイルを設定します。

- a. (オプション) [loadbalancing.xml 内のいずれの正規表現にも一致しないエージェントからの、MOM または特定の Enterprise Manager への接続を許可または拒否に設定します](#) (P. 154)。

`introscope.apm.agentcontrol.agent.allowed` プロパティを設定します。

- b. (オプション) [Enterprise Manager へのエージェントの再接続試行用にランダムな継続時間を設定します](#) (P. 155)。

`introscope.apm.agentcontrol.agent.reconnect.wait` プロパティを設定します。

- c. (オプション) [Enterprise Manager にパッシブに接続できて、データを送信できない 9.1 のエージェントの数を設定します \(P. 156\)](#)。

`introscope.enterprisemanager.agent.disallowed.connection.limit` を設定します。

- 3. 組織のデプロイ環境に応じて、`IntroscopeAgent.profile` ファイルを設定します。

- (オプション) [Enterprise Manager から切断されたエージェントから、許可された任意の Enterprise Manager への再接続を継続的に試行するかどうか設定します \(P. 157\)](#)。

`introscope.agent.enterprisemanager.failbackRetryIntervalInSeconds` プロパティを設定します。

- 4. [loadbalancing.xml を設定します \(P. 159\)](#)。

- a. (オプション) 特定のエージェントが、特定の Enterprise Manager に常に接続するように、ラッチ済みプロパティを設定します。

- b. (オプション) `include` および `exclude` エlement を、特定の Enterprise Manager へのエージェント接続を許可および拒否するために設定します。

- c. `loadbalancing.xml` を保存します。

この新しい値は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを確認するとき (約 60 秒ごとに行われます) に有効になります。MOM は更新された `loadbalancing.xml` を、クラスタ内のコレクタにその次の負荷分散の間隔で送信します。

- 5. システムの監視を実行し、必要に応じて再設定します。

- a. 必要に応じて任意のプロパティを再設定します。

- b. `loadbalancing.xml` を更新します。

Enterprise Manager ネットワークトポロジ エージェントの計画

エージェント接続割り当てを設定する前に、Enterprise Manager またはコレクタ トポロジのエージェントを計画します。これらの割り当てでは、特定の個別またはグループのコレクタに対して、どのエージェントの接続を許可する、または許可しないかを設定します。

ビジネス慣行で必要とする場合は、エージェントをサブクラスタへセットアップします。エージェントを特定のコレクタセットに割り当て、次に `loadbalancing.xml` を設定して、MOM がそのコレクタセットのみ負荷分散するようにします。たとえば、特定のビジネスユニット用のアプリケーションを監視するエージェントを、10 のクラスタ内の 3 つのコレクタに接続させることができます。

計画中に、以下のような質問のやりとりをします。

- エージェントのクラスかグループ、または特定のエージェントが、クラスタ内または特定のコレクタ上で、許可または拒否されていますか?
- いずれのコレクタも、過負荷に対して特別に保護されていますか?

たとえば、不正に設定されたエージェントからの直接接続を防ぐことが必要なコレクタはありますか? すべてのエージェントが同一のエージェントプロファイルを持っていて接続を試行する場合、単一の IP アドレスに大量のデータが送信される場合があります。コレクタに接続されたエージェントが多すぎると、コレクタがクラッシュする場合があります。

以下の手順に従います。

1. エージェントのグループまたはクラスのそれぞれにつき、以下のコレクタセットのいずれを選択するか決定します。
 - a. アクセス許可
 - b. アクセス拒否

2. `loadbalancing.xml` に一致するものがないエージェントの、デフォルトの接続アクティビティを決定します。

特定の Enterprise Manager 上の `loadbalancing.xml` に一致するものがないすべてのエージェントを許可または拒否しますか?

3. 負荷分散されるエージェントはありますか? その場合のエージェントは、移動される先のすべてのコレクタで許可されますか。

エージェントの接続制限は MOM 用の負荷分散オプションを制限するため、接続制限の影響を注意深く検討してください。エージェントが低負荷のコレクタへ接続することを許可されないとき、負荷分散を実行する MOM は過負荷のコレクタからエージェントを削除できません。この場合、MOM は他のエージェントを過負荷のコレクタから低負荷のコレクタへと、負荷分散する必要があります。

4. Enterprise Manager から切断されたエージェントがどのように動作するか決定します。

エージェントに、許可された任意の Enterprise Manager への継続的な再接続を試行させるようにしますか?

または、エージェント CA APM バージョンに基づいて、以下のようにする方がよろしいですか?

- **9.1 より前のエージェントで有効**： Enterprise Manager から切断し、再接続の試行を続けさせますか?
- **9.1 エージェントで有効**： Allowed Enterprise Manager リストの最後の Enterprise Manager へのパッシブな接続を継続しますか?
パッシブに接続されたエージェントには、以下の特徴があります。
 - Enterprise Manager にメトリック データを送信しない
 - 利用可能になった他の Enterprise Manager への再接続を試行しない

5. CA APM 環境では、エージェントが以下の CA APM コンポーネントにわたって接続することが許可されますか?

- クラスタでは?
- コレクタおよびスタンドアロン Enterprise Manager では?
- クラスタ、コレクタおよびスタンドアロン Enterprise Manager の任意の組み合わせでは?

loadbalancing.xml ルールがないときに新しいエージェント接続を許可するかどうかの設定

エージェントが loadbalancing.xml 内の正規表現に一致しないとき、すべての新しいエージェント接続を許可するか拒否するか決定します。以下のコンピュータ用に決定をします。

- MOM
- 各コレクタ
- 任意のスタンドアロン Enterprise Manager

`introscope.apm.agentcontrol.agent.allowed` プロパティを、パフォーマンスの尺度として設定できます。

注: MOM のプロパティ値はコレクタの値より常に優先されます MOM がコレクタに接続するまでの間のみ、コレクタの値が使用されます。その間、MOM のプロパティ値がコレクタに転送されて使用されます。

また、`loadbalancing.xml` 内のこのプロパティ設定と設定を使用して、環境内の Enterprise Manager へのエージェント接続を微調整できます。

以下の手順に従います。

1. `<EM_Home>%config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. 「`introscope.apm.agentcontrol.agent.allowed= true`」と設定します。
3. `IntroscopeEnterpriseManager.properties` ファイルを保存します。
この設定は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

エージェントの再接続待機時間の設定

[切断されたエージェント \(P. 149\)](#) がスタンドアロンの Enterprise Manager またはコレクタへの再接続を試行する前に待機する必要がある時間（秒）を変更することができます。さまざまな待機時間を設定することで、多数のエージェントが同時に Enterprise Manager への再接続を試行するときに発生するパフォーマンスの問題を CA APM が回避できるようになります。待機時間を変更するには、`introscope.apm.agentcontrol.agent.reconnect.wait` プロパティを設定します。

以下の手順に従います。

1. `<EM_Home>%config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. `introscope.apm.agentcontrol.agent.reconnect.wait` プロパティを設定します。
3. `IntroscopeEnterpriseManager.properties` ファイルを保存します。

この設定は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

エージェントは Enterprise Manager から切断されると、Enterprise Manager によって生成された再接続時間に基づいて、再接続を試行します。接続時間は、ランダムに選択された正または負の値をデフォルト値に追加して算出されます。

禁止されたエージェント接続のクランプ限界値の設定

9.1 エージェントで有効： 禁止対象として設定されていてもスタンドアロン Enterprise Manager またはコレクタにパッシブに接続できる 9.1 エージェントの数を制限できます。パッシブに接続されたエージェントには、以下の特徴があります。

- Enterprise Manager にメトリック データを送信しない
- 利用可能になった他の Enterprise Manager への再接続を試行しない

このクランプ限界値の設定は、Enterprise Manager への接続数を制限するため、パフォーマンスの尺度になります。接続のたびに一定程度のリソースが必要になるため、接続数が多すぎると Enterprise Manager のパフォーマンスが低下する可能性があります。

以下の手順に従います。

1. `<EM_Home>\config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. `introscope.enterprisemanager.agent.disallowed.connection.limit` プロパティを設定します。
3. `IntroscopeEnterpriseManager.properties` ファイルを保存します。

この設定は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

このクランプ値に到達し、禁止対象として設定されたエージェントが Enterprise Manager に接続を試みると、Enterprise Manager は以下のアクションを実行します。

- このイベントをログに記録します。
- 新しい接続を拒否します。

許可済み Enterprise Manager へのエージェントの連続的な再接続の設定

すべての Enterprise Manager で接続を拒否されたエージェントが Allowed Enterprise Manager リストに記載された順に連続して再接続を試行するかどうかを設定できます。以下が Allowed Enterprise Manager です。

- エージェントプロファイルの `introscope.agent.enterprisemanager.connectionorder` プロパティ値で設定された Enterprise Manager。
- `loadbalancing.xml` の設定に基づいて許可されたすべての Enterprise Manager

拒否されたエージェントは、Enterprise Manager に接続できない場合に以下の方法で接続を処理します。

- Allowed Enterprise Manager リストに記載された次の許可済み Enterprise Manager に接続しようとします。
- そのエージェントが禁止対象として設定されている Enterprise Manager には接続しません。

拒否されたエージェントが接続を試行し続けるように設定することには、以下の特徴があります。

- 以下の CA Introscope コンポーネントにまたがってエージェントを接続できる環境に有効です。
 - クラスタ
 - コレクタおよびスタンドアロン Enterprise Manager
 - クラスタ、コレクタ、およびスタンドアロン Enterprise Manager の任意の組み合わせ
- 切断されたエージェントが以下の条件で強制的に許可済み Enterprise Manager への接続を試行し続けるようになります。
 - Enterprise Manager が接続できるようになるまで接続を試行します。
 - Enterprise Manager が別のクラスタ内にあっても接続を試行します。

上記の条件を満たさない場合、エージェントは以下の方法で接続を処理します。

- パッシブに Enterprise Manager に接続し、メトリック データを送信しません。
- 許可済み Enterprise Manager に接続しようとしません。これには、利用不可能になった後で利用可能になったものも含まれます。

以下の手順に従います。

1. IntroscopeAgent.profile ファイルを開きます。
2. introscope.agent.enterprisemanager.failbackRetryIntervallInSeconds プロパティを設定します。
3. IntroscopeEnterpriseManager.properties ファイルを保存します。
4. 管理対象アプリケーションを再起動します。

以下の状況が発生する場合があります。

- エージェントが Enterprise Manager への接続を拒否される。
- Enterprise Manager がダウンしている。

上記のような場合、エージェントは Allowed Enterprise Manager リスト上の次の許可済み Enterprise Manager にすぐに接続しようとします。

どの許可済み Enterprise Manager にも接続できない場合、エージェントは以下のアクションを実行します。

- introscope.agent.enterprisemanager.failbackRetryIntervallInSeconds プロパティで設定された期間だけ待機します。
- Allowed Enterprise Manager リストの最初の Enterprise Manager に戻って、許可済み Enterprise Manager への接続を再試行します。

このサイクルは、エージェントが能動的にデータを送信できる Enterprise Manager に接続するまで繰り返されます。

Enterprise Manager によって許可および禁止されるエージェントに関する loadbalancing.xml の設定

特定の Enterprise Manager に対するエージェントの接続を許可および禁止するには、MOM またはスタンドアロン Enterprise Manager 上で [loadbalancing.xml を設定](#) (P. 131) します。

MOM は loadbalancing.xml 内のエージェント接続情報を 10 分ごとにコレクタに送信し、コレクタは許可済み Enterprise Manager の情報をエージェントに送信します。MOM は、最新の loadbalancing.xml ファイルに基づいて、特定の Enterprise Manager に対するエージェントの接続を許可および禁止します。

MOM によって負荷分散したくないエージェントがある場合は、loadbalancing.xml を設定することもできます。以下の例では、MOM は EPAgent という名前のエージェントの負荷を Collector1-ip という名前のコレクタから他のコレクタに分散しません。

```
<agent-Collector name="EPAgent connects to only Collector1-ip">
<agent-specifier>.*%|..*%|EPAgent</agent-specifier>
  <include>
    <Collector host="Collector1-ip" port="6001"/>
  </include>
</agent-Collector>
```

エージェントと Enterprise Manager 間のネットワークトポロジの設定

Enterprise Manager が拒否されたエージェントを処理する方法

MOM は、10 分ごとにクラスタ内のすべてのコレクタに loadbalancing.xml を送信します。Enterprise Manager は、loadbalancing.xml および introscope.apm.agentcontrol.agent.allowed プロパティによって、どのエージェントに自身への接続が許可および禁止されているかを判定します。Enterprise Manager は、接続の許可と禁止の設定に基づいて、エージェントの接続要求を受け入れるか、または拒否できます。

Enterprise Manager がエージェントの接続を拒否するとき行われる操作を以下に示します。

9.1 より前のエージェントで有効

エージェントが接続されると、Enterprise Manager は 9.1 より前のエージェントを切断します。エージェントは、それぞれの許可済み Enterprise Manager リストを使用して、利用可能な別の許可済み Enterprise Manager に接続しようとします。すべての Enterprise Manager への接続が拒否された場合、エージェントは引き続き以下の条件を満たす最後の Enterprise Manager に接続しようとします。

- 利用可能である
- そのエージェントへの接続が許可されている

9.1 エージェントで有効

Enterprise Manager は 9.1 エージェントを切断し、切断されたエージェントは利用可能な別の Enterprise Manager に接続しようとします。すべての Enterprise Manager への接続が拒否された場合、エージェントは以前に接続していた最後の Enterprise Manager に接続します。エージェントは Enterprise Manager に接続されたままになりますが、データを送信しません。

コレクタが `introscope.apm.agentcontrol.agent.allowed` プロパティを使用する場合

MOM は、コレクタに接続すると、`introscope.apm.agentcontrol.agent.allowed` プロパティと `loadbalancing.xml` をコレクタに提供します。MOM がダウンした場合、コレクタは MOM から提供された以下の情報を使用して、どのエージェント接続を許可および禁止すべきかを決定します。

- `IntroscopeEnterpriseManager.properties` ファイルに含まれる現在の `introscope.apm.agentcontrol.agent.allowed` プロパティの設定。
- `loadbalancing.xml`。

MOM がコレクタに一度も接続していない場合は、MOM からコレクタに `introscope.apm.agentcontrol.agent.allowed` プロパティと `loadbalancing.xml` が転送されていません。そのため、コレクタはそれ自身の `introscope.apm.agentcontrol.agent.allowed` プロパティを使用して、特定のエージェント接続を許可するか禁止するかを決定します。

エージェントが loadbalancing.xml で許可または禁止の正規表現に一致しない場合

IntroscopeEnterpriseManager.properties ファイル内の introscope.apm.agentcontrol.agent.allowed プロパティの値は、loadbalancing.xml で正規表現に一致しないエージェントがコレクタに接続できるかどうかを決定します。

このプロパティ値が **true** である場合、loadbalancing.xml でどの正規表現にも一致しないエージェントはコレクタへの接続を許可されます。

このプロパティ値が **false** である場合、loadbalancing.xml でどの正規表現にも一致しないエージェントはコレクタへの接続を拒否されます。

エージェントに割り当てられたコレクタが利用不可能で、他のコレクタが利用可能な場合

9.1 より前のエージェント

コレクタはエージェントを切断し、切断されたエージェントは **MOM** に接続しようとしています。エージェントに接続を許可しているコレクタがない場合、**MOM** はすべてのエージェント接続の試行を拒否します。エージェントは、そのエージェントに対して許可されたコレクタが利用可能になるまで、**MOM** への接続を試行し続けます。許可されたコレクタが利用可能になると、**MOM** はそのコレクタにエージェントを転送します。

9.1 エージェント

コレクタはエージェントを切断し、切断されたエージェントは **MOM** に接続しますが、データを送信しません。許可されたコレクタが利用可能になると、**MOM** はそのコレクタにエージェントを転送します。

コレクタが禁止されたエージェントを直接接続で処理する方法

MOM は、定期的にクラスタ内のすべてのコレクタに `loadbalancing.xml` を送信します。各コレクタは、`loadbalancing.xml` ファイルによって、自身に接続することを許可されたエージェントを認識します。以下のアクション実行される場合があります。

- `loadbalancing.xml` ファイルが更新され、エージェントが特定のコレクタで禁止される。
- エージェントがそのコレクタに接続しようとする。

この結果、以下のアクションが実行されます。

9.1 より前のエージェント

コレクタはエージェントの接続を否定し、エージェントは接続を試行し続けます。

9.1 エージェント

コレクタはエージェントに最新の **Allowed Enterprise Manager** リストを提供します。禁止の設定に基づいて、エージェントはこのコレクタで許可されません。MOM が利用可能である場合、MOM はエージェントを利用可能な許可されたコレクタに転送します。MOM が利用可能でない場合、エージェントは自身の **Allowed Enterprise Manager** リストを使用して、利用可能な許可されたコレクタへの接続を順に試行します。

introscope.apm.agentcontrol.agent.allowed プロパティがない場合のエージェント接続のデフォルト値

`introscope.apm.agentcontrol.agent.allowed` プロパティのデフォルト値は許可です。

MOM が利用不可能な場合に CA Introscope がエージェントの接続先を決定する方法

エージェントが接続しようとしているコレクタは、接続を許可するか拒否するかを決定します。コレクタの決定は、自身の `loadbalancing.xml` ファイルに含まれる現在の許可と禁止の設定に基づいて行われます。

第 9 章: コマンドライン Workstation の使用

この章では、Enterprise Manager のコマンドラインインターフェースである Introscope コマンドライン Workstation (CLW) について説明します。

このセクションには、以下のトピックが含まれています。

[コマンドライン Workstation \(CLW\) について \(P. 163\)](#)

[CLW の実行 \(P. 164\)](#)

[CLW コマンドリファレンス \(P. 168\)](#)

[サンプルスクリプト \(P. 221\)](#)

コマンドライン Workstation (CLW) について

Introscope コマンドライン Workstation (CLW) を使用して、Introscope Workstation の機能の一部を実行できます。

CLW は、Introscope の処理タスクの自動化またはスケジューリングに役立ちます。たとえば、CLW を使用して、多くの管理モジュール内で複数のアラートを無効化するといった、繰り返しが必要なタスクを、Workstation インターフェースを使用するよりも短時間で実行できます。同様に、CLW は、自動的または定期的に行う必要があるスケジューリングタスクでも役立ちます。

CLW コマンドを使用すると、以下を実行できます。

- **管理モジュールおよびエレメントの管理** - 管理モジュールおよびエレメントの一覧表示、コピー、名前の変更、削除、アクティブかどうかのチェック、および現在の状態の変更を行えます。

CLW の `copy` コマンドおよび `rename` コマンドを使用して、既存の管理モジュールおよびエレメントから新しい管理モジュールおよびエレメントを作成できます。ただし、CLW を使用して、管理モジュールおよびエレメントを一から作成したり、それらの詳細を変更したりすることはできません。

- **エージェントの制御** - エージェントのレポートをリモートで開始、停止、および再開できます。また、設定ファイルをリモートのエージェントにコピーできます。

- **トランザクション追跡セッションの開始** - スクリプトを記述して、アラート状態の結果を受けてトランザクション追跡セッションを自動的に開始できます。
- **Enterprise Manager のシャットダウン** - スクリプトを記述して、スケジュールに従って Enterprise Manager をシャットダウンできます。たとえば Workstation を使用するのに不都合な営業時間外などに Enterprise Manager を定期的にシャットダウンすることができます。
- **CLW の終了時** - 何も問題がない場合、CLW は 0 のステータス コードで終了します。以下のうちいずれかの問題が発生している場合、負のステータス コードで終了します。
 - Enterprise Manager 認証の失敗
 - ネットワーク接続の切断、あるいは無効なホスト名などの、Enterprise Manager との接続問題
 - 無効な WS および Enterprise Manager がある。

CLW の実行

このセクションでは、CLW の実行方法の概要について説明します。各コマンドの詳細については、「[CLW コマンドリファレンス \(P. 168\)](#)」を参照してください。

JVM の要件

CLW では、JVM 1.6 以降が必要です。

CLW コマンドを実行する場所

CLW コマンドは、スクリプトまたはバッチ ファイルに含めるか、またはコマンドラインで入力できます。CLW .jar ファイルは、<EM_Home>/lib ディレクトリにインストールされます。このディレクトリから CLW コマンドを実行するか、このディレクトリへのパスをコマンドに含めます。

CLW インタラクティブ モードの使用

デフォルトのモードからインタラクティブ モードに変更するには、以下の例のように `-i` フラグを使用します。CLW のスクリプトを記述する場合は、スクリプトが中断されるため、このモードを使用することはできません。

```
java -Xmx128M <EM_logon> <TT_properties> -jar CLWorkstation.jar > usage | -i  
| <command>
```

インタラクティブ モードでは、コマンドのコマンドライン引数を読み取り、実行してから終了します。ただし、`-DHost=` など JVM オプション以外のコマンドライン引数が渡されなかった場合は、標準入力の 1 行を読み取って実行し、ファイルの最後に到達するか、システムを終了するまでこれを続行します。引数が渡されず、入力もない場合は、エラーが出力され、システムが終了します。# 記号で始まる行はすべて無視されます。

CLW の呼び出し

CLW コマンドでは、以下の構文を使用します。

```
java -Xmx128M <EM_logon> -jar CLWorkstation.jar <コマンド>
```

各項目の説明：

- `-Xmx128M` は、Java ヒープ サイズを設定します。これは、`java.lang.OutOfMemoryError` エラーが発生しないようにするためです。
- `<EM_logon>` は、以下の Enterprise Manager ログオン情報です。
 - `-Duser=<ユーザー名>`
 - `-Dpassword=<パスワード>`
 - `-Dhost=<Enterprise Manager のホスト/IP アドレス>`
 - `-Dport=<Enterprise Manager のポート番号>`
- `<コマンド>` は、「[CLW コマンドリファレンス \(P. 168\)](#)」で説明されているコマンドのいずれかです。

例 :

```
java -Xmx128M -Duser=jdoe -Dpassword=mypassword -Dhost=jdoeDT  
-Dport=5001 -jar CLWorkstation.jar <command>
```

ログオン情報を入力しないで CLW を呼び出した場合は、Enterprise Manager にアクセスするためのデフォルトのログオン値が使用されます。

```
java -Xmx128M -jar CLWorkstation.jar <command>
```

コマンドラインまたはスクリプトに入力する各 CLW コマンドは、以下の CLW 呼び出しで開始する必要があります。

```
java -Xmx128M -jar CLWorkstation.jar
```

注: *java.lang.OutOfMemoryError* が発生しないようにするには、Java のヒープサイズを設定します。

CLW での大文字と小文字の区別

CLW コマンドは、Introscope デプロイ環境内にあるエージェント、管理モジュール、および指定したその他の項目を指定する引数を受け付けます。CLW では大文字と小文字が区別されます。したがって、Introscope オブジェクトの名前は、正確に入力する必要があります。たとえば、エージェントの名前が *WebLogic1* である場合、*weblogic1* を参照する CLW コマンドは、このエージェントに対して実行されません。

CLW コマンドの出力結果

CLW コマンドは、コマンドウィンドウに出力結果を返します。必要に応じて、コマンドの出力結果をファイルに出力できます。

CLW および正規表現

CLW コマンドを使用すると、エージェント、管理モジュール、ダッシュボード、アクション、およびアラートなど、Introscope 環境の要素を操作できます。ターゲットの種類に応じて、コピー、一覧表示、名前の変更、アクティブ化、および非アクティブ化などの操作を実行できます。

CLW コマンドのターゲットは、正確なテキスト文字列、または Perl の正規表現を使用して指定します。たとえば、次の CLW コマンドは、Enterprise Manager に接続されているすべてのエージェントを一覧表示します。

```
list agents matching (.*)
```

以下のコマンドは、文字列 *weblogic* が名前に含まれるエージェントのみを一覧表示します。

```
list Agents matching .*weblogic.*
```

CLW コマンド内の円記号および引用符

スペースを含む CLW コマンド引数を指定するときは、引数を引用符 (") で囲み、シェルが引用符を解釈しないように各引用符の前には円記号を付けます。例：

```
¥"2005/01/01 12:20:37¥"
```

さまざまな環境での CLW の使用

正規表現の構文は、オペレーティング システムおよびコマンド シェルによって異なります。また、場合によっては、コマンドラインとスクリプトのどちらに正規表現を入力するかによっても異なります。この章のサンプル コマンドは、Windows 環境用に記述されており、バッチ ファイル内で正規表現を使用する場合に必要な構文を表しています。

コマンドライン Workstation ログの設定

CA APM を設定して、コマンドライン Workstation (CLW) コマンドを、Enterprise Manager コンソール、および *<EM_Home>/logs* ディレクトリ内の *IntroscopeEnterpriseManager.log* ファイルへログ記録するようにできます。

コマンドライン Workstation ログを設定する方法

1. *<EM_Home>¥config* ディレクトリの *IntroscopeEnterpriseManager.properties* ファイルを開きます。
2. *IntroscopeEnterpriseManager.properties* ファイル内で以下のプロパティを設定し、CLW コマンドのログ ファイルおよび Enterprise Manager コンソール上でのログ記録を有効にするためにします。
 - a. *log4j.additivity.Manager.CLW=true* を設定

注: このプロパティのデフォルト値は「false」です。

b. `log4j.logger.Manager.CLW=DEBUG` を設定

このプロパティのデフォルト値は、「INFO」です。

CLW コマンド リファレンス

このセクションでは、CLW コマンドに関する詳細を説明します。

注: 各コマンドに示されている構文には、コマンドの呼び出し部分は含まれていません。「[CLW の呼び出し \(P. 165\)](#)」の説明にあるように、各 CLW コマンドは、`java -jar CLWorkstation.jar` で開始する必要があります。

Enterprise Manager コマンド

Enterprise Manager は、アプリケーション パフォーマンス データをエージェントから集約し、要求された演算を実行し、パフォーマンス データを承認されたクライアントが利用できるようにし、データを保存します。

Enterprise Manager のシャットダウン

このコマンドは、Enterprise Manager をシャットダウンします。これを実行するには、「shutdown」アクセス権または「full」アクセス権が必要です。Enterprise Manager をシャットダウンすると、Enterprise Manager に接続している Workstation ユーザはすべてログオフされます。

構文

```
shutdown
```

例

```
shutdown
```

出力

なし。

SmartStor からの永続データの抽出(時間範囲内)

このコマンドは、指定した期間の履歴データを SmartStor から抽出します。エージェントを指定する正規表現、メトリックグループを指定する正規表現、および期間の開始日時と終了日時を指定します。日付と時刻の文字列の *hh:mm:ss* 部分はオプションです。指定しない場合は、デフォルトの *00:00:00* つまり午前 0 時になります。

構文

```
get historical data from agents matching [正規表現] and metrics matching [正規表現] between [完全一致] and [完全一致] with frequency of [完全一致] (second|seconds|sec|secs|s)
```

例

```
get historical data from agents matching (.weblogic.*) and metrics matching (Servlets:Responses Per Interval) between ¥"2011-10-12 00:00:00¥" and ¥"2011-10-12 00:10:00¥" with frequency of 60 seconds
```

このコマンドは、名前に文字列 **weblogic** を含むすべてのエージェントの **Servlets:Responses Per Interval** メトリックグループの永続データを抽出します。2011 年 10 月 12 日午前 0 時から 2011 年 10 月 12 日午前 0 時 10 分までの期間のデータが 60 秒の頻度で抽出されます。

出力

SmartStor のデータは、カンマ区切り値 (CSV) 形式で返されます。

SmartStor からの永続データの抽出(直前の N 分間)

このコマンドは、コマンド実行前の **N** 分間を指定して、その間の履歴データを抽出します。抽出されたデータは、特定の頻度 (秒単位) で表示されます。コマンドには、エージェントを指定する正規表現、メトリックグループを指定する正規表現、抽出される履歴の期間 (分単位)、およびデータ抽出の頻度 (秒単位) を指定します。

構文

```
get historical data from agents matching [正規表現] and metrics matching [正規表現] for past [完全一致] (minute|minutes) with frequency of [完全一致] (second|seconds|sec|secs|s)
```

例

get historical data from agents matching (.weblogic.) and metrics matching (Servlets:Responses Per Interval) for past 1 minute with frequency of 60 seconds*

このコマンドは、名前に文字列 `weblogic` を含むすべてのエージェントの `Servlets:Responses Per Interval` メトリック グループの永続データを抽出します。過去 1 分間のデータが 60 秒の頻度で抽出されます。

出力

SmartStor のデータは、カンマ区切り値 (CSV) 形式で返されます。

認証のためのパス名の指定

Enterprise Manager に接続したときに、ユーザ名/パスワード認証の代わりに使用する公開鍵ファイルのフルパス名を指定します。公開鍵は、Managers of Manager/コレクタの認証に使用するものと同じです。

公開鍵の構成の詳細については、「CA APM セキュリティ ガイド」を参照してください。

Introscope エージェント コマンド

エージェントは、Java アプリケーション マシンでマネージドアプリケーションの一部として動作し、プローブから報告されたデータを集めて要約し、Enterprise Manager に送信します。

List Agents

List Agents コマンドは、Enterprise Manager に接続されている 1 つまたは複数のエージェントを一覧表示します。一覧表示するエージェントを指定する正規表現を入力します。

構文

list agents matching <正規表現>

例

```
list agents matching (.*)
```

このコマンドは、Enterprise Manager に接続されているすべてのエージェントを一覧表示します。

出力

各エージェントが一覧表示されます。名前の前にはホストおよびプロセスが付きます。仮想エージェントも一覧に含まれます。例：

```
jdoe-dt|Weblogic|WebLogicAgent
```

```
Custom Metric Host (Virtual)|Custom Metric Process (Virtual)|Custom Metric Agent (Virtual)
```

List Historical Agents

List Historical Agents コマンドは、マウント解除され、Enterprise Manager にデータを送信していない、SmartStor 内のデータを持ったすべてのエージェントを一覧表示します。

構文

```
list historical agents
```

例

```
list historical agents
```

出力

マウント解除された履歴エージェントはそれぞれ、個別の行に表示され、その前にはホスト名とプロセスが示されます。例：

```
jdoe-dt|Weblogic|WebLogicAgent
```

List Historical Agents (時間範囲内)

このコマンドは、指定された時間範囲内の SmartStor 内に履歴データを持っている、マウント解除されたすべてのエージェントを一覧表示します。データを送信しているエージェントは自動的にマウントされます。したがって、リストには表示されません。

期間の開始および終了を指定します。日付と時刻の文字列の hh:mm:ss 部分はオプションです。指定しない場合は、デフォルトの 00:00:00 つまり午前 0 時になります。

構文

```
list historical agents between [時間] and [時間]
```

例

```
list historical agents between ¥"2013-04-22 00:00:00¥" and ¥"2013-04-23 00:10:00¥"
```

このコマンドは、2013 年 3 月 22 日の午前 0 時から 2013 年 3 月 23 日の午前 0 時 10 分の期間にデータを送信した、マウント解除されたすべてのエージェントを一覧表示します。

出力

指定された時間範囲内にデータを送信した、マウント解除された履歴エージェントはそれぞれ、個別の行に表示されます。エージェント名の前には、そのホスト名とプロセスが表示されます。例：

```
jdoh-dt|Weblogic|WebLogicAgent
```

Turn on Agents

このコマンドは、1 つまたは複数のエージェントのメトリック レポートを開始または再開します。ターゲットエージェントを指定する正規表現を入力します。

構文

```
turn on agents matching <正規表現>
```

例

turn on agents matching (.)*

このコマンドは、すべてのエージェントをオンにします。

出力

なし。

Turn off Agents

このコマンドは、1つまたは複数のエージェントのメトリック レポートを停止します。ターゲット エージェントを指定する正規表現を入力します。

Send Configuration file

このコマンドは、指定したファイルを1つまたは複数のエージェントに送信します。ファイルの名前、ターゲット エージェントを指定する正規表現、送信元ディレクトリ、および送信先ディレクトリを入力します。

ターゲット エージェントは、

introscope.agent.remoteagentconfiguration.enabled プロパティで、リモートで書き込みができるように構成する必要があります。場所およびそのデフォルト値は異なります。詳細については、「CA APM Java Agent 実装ガイド」または「CA APM .NET Agent 実装ガイド」を参照してください。

コピーできるのは、エージェントの

introscope.agent.remoteagentconfiguration.allowedfiles プロパティで明示的に指定されているファイルのみです。

このプロパティのデフォルト値は *domainconfig.xml* です。これは、Introscope が CA CEM のトランザクションを認識するのに必要なすべての情報が含まれるファイルです。

APM ステータス コンソール コマンド

このセクションでは APM ステータス コンソールに関連する CLW コマンドについて説明します。

注: APM ステータス コンソールの使用方法については、「CA APM Workstation ユーザ ガイド」を参照してください。

APM ステータス コンソールの CLW コマンドを実行するには、`apm_status_console_control` 権限が必要です。

注: この権限の詳細については、「CA APM セキュリティ ガイド」を参照してください。

この CLW カテゴリには以下のコマンドが含まれます。

[Get Cluster Configuration](#) (P. 174)

[List Active Clamps](#) (P. 175)

[List Important Events](#) (P. 178)

Get Cluster Configuration

このコマンドは、以下の情報を表示します。

- MOM およびクラスタ内のすべての CDV およびコレクタのホスト名とポート。
- スタンドアロン Enterprise Manager のホストとポート。

構文

```
get cluster configuration
```

例

```
get cluster configuration
```

このコマンドは、MOM およびクラスタ内のすべてのコレクタのホスト名とポートを一覧表示します。

出力

MOM およびクラスタ内のすべてのコレクタのホスト名とポートが一覧表示されます。最初に MOM が表示され、次にコレクタが表示されます。

```
MOM:
USERID04-W7@5001

Collectors:
localhost@3001
USERID04-@xyz_company.com@6001
```

スタンドアロン Enterprise Manager の場合は、Enterprise Manager のホストとポートが一覧表示されます。

```
StandAlone:
USERID05-W8@5001
```

List Active Clamps

このコマンドは、`apm-events-thresholds-config.xml` 内のクランププロパティのうち、現在の値がそのしきい値に到達したか、またはそれを超過したものを一覧表示します。これらはアクティブクランプと呼ばれます。このコマンドは、以下のアクティブクランプのリストを出力します。

- MOM およびクラスタ内のすべてのコレクタ上のアクティブクランプ。
- CDV および CDV に接続されたすべてのコレクタ上のアクティブクランプ。
- スタンドアロン Enterprise Manager 上のアクティブクランプ。

`apm-events-thresholds-config.xml` のクランプ値がそのしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータスコンソールにそれを通知します。

構文

```
list active clamps
```

例

list active clamps

このコマンドは、ユーザの環境に応じて以下の CA APM コンポーネント上にあるすべてのアクティブ クランプを一覧表示します。

- MOM およびクラスタ内のすべてのコレクタ。
- CDV、CDV に接続されたコレクタ、およびスタンドアロン Enterprise Manager。
- スタンドアロン Enterprise Manager

出力

ユーザの環境に応じて、以下の CA APM コンポーネントに含まれるすべてのアクティブ クランプが一覧表示されます。

- MOM およびクラスタ全体のコレクタ。
- CDV、接続されたコレクタ、およびスタンドアロン Enterprise Manager。
- スタンドアロン Enterprise Manager

各クランプに関して以下の情報が表示されます。

Enterprise Manager 名、クランプ名、クランプの説明、クランプのしきい値、クランプ値、クランプ時間

例 :

```
USERID04-w7@6001, introscope.enterprisemanager.metrics.live.limit, Per EM limit.
Takes into account only live metrics (i.e. currently reporting from Agents), 0,
40, 22:10:00 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit, Limits # of
Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per EM limit.
Takes into account only live metrics (i.e. currently reporting from Agents), 0,
219, 22:09:30 10/07/11
```

コマンド オプション

このセクションでは、*list active clamps* コマンド オプションについて説明します。

個別および複数のコレクタ上にあるアクティブ クランプの一覧表示

list active clamps コマンドには、以下の 2 つの引数を追加できます。

- of EM - 特定の MOM、コレクタ、CDV、またはスタンドアロン Enterprise Manager 上のアクティブ クランプのリストを返すには、この引数を使用します。

- 構文

```
list active clamps of EM <enterprise-manager-host@port>
```

- 例

```
list active clamps of EM localhost@3001
```

- 出力

Enterprise Manager 名、クランプ名、クランプの説明、クランプのしきい値、クランプ値、クランプ時間

```
localhost@3001, introscope.enterprise.agent.error.limit, Limits # of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
```

```
localhost@3001, introscope.enterprise.metrics.live.limit, Per EM limit. Takes into account only live metrics (i.e. currently reporting from Agents), 0, 219, 22:09:30 10/07/11
```

注: 不正な Enterprise Manager 名を入力すると、コンソールにエラーメッセージが表示され、アクティブ クランプがあるコレクタが一覧表示されます。正しい Enterprise Manager のアクティブ クランプのリストを取得するには、エラーメッセージに示された Enterprise Manager 名を使用してコマンドを再試行します。

- of EM EnterpriseManagerName1@port,EnterpriseManagerName2,@port EnterpriseManagerNameX@port - 指定した複数の Enterprise Manager 上のアクティブ クランプのリストを返すには、この引数を使用します。

- 構文

```
list active clamps of EM <EnterpriseManagerName1@port>, <EnterpriseManagerName2@port>
```

- 例

```
list active clamps of EM localhost@3001,USERID04-w7@5001
```

- 出力

指定したすべての Enterprise Manager の Enterprise Manager 名、クランプ名、クランプの説明、クランプのしきい値、クランプ値、クランプ時間

```
localhost@3001, introscope.enterprisemanager.agent.error.limit, Limits # of
Error Events Per Interval, 1, 1, 22:09:30 10/07/11
localhost@3001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.agent.error.limit, Limits #
of Error Events Per Interval, 1, 1, 22:09:30 10/07/11
USERID04-w7@3001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 0, 219, 22:09:30 10/07/11
USERID04-w7@5001, introscope.enterprisemanager.metrics.live.limit, Per EM
limit. Takes into account only live metrics (i.e. currently reporting from
Agents), 200, 390, 22:22:55 10/07/11
```

注: 不正な Enterprise Manager 名を入力すると、コンソールにエラーメッセージが表示され、アクティブクランプがあるコレクタが一覧表示されます。正しい Enterprise Manager のアクティブクランプのリストを取得するには、エラーメッセージに示された Enterprise Manager 名を使用してコマンドを再試行します。

List Important Events

このコマンドは、`apm-events-thresholds-config.xml` 内の重要イベントプロパティのうち、現在の値がそのしきい値に到達したか、またはそれを超過したものを一覧表示します。このコマンドは、クラスタ内のすべての CDV とコレクタ、またはスタンドアロン Enterprise Manager に関するリストを出力します。

`apm-events-thresholds-config.xml` のプロパティ値がそのしきい値に到達するか、または超過すると、Enterprise Manager は APM ステータス コンソールにそれを通知します。

構文

```
list important events
```

例

```
list important events
```

このコマンドは、クラスタ内、またはスタンドアロン Enterprise Manager 上のすべての重要イベントを一覧表示します。

出力

クラスタ内、またはスタンドアロン Enterprise Manager 上のすべての重要イベントに関するデータが一覧表示されます。

各イベントに関して以下の情報が表示されます。

Enterprise Manager 名、イベント重大度、イベント説明、イベント時間

例 :

```
USERID04-w7@6001, Warning Event, The Smartstor duration on EM USERID04-w7@6001 is more than configured threshold [Actual Value : 1,780/ Threshold : 5]. The most likely cause would be slow disk., 22:10:02 10/07/11
```

```
USERID04-w7@3001, Warning Event, The harvest duration of EM USERID04-w7@3001 is more than configured threshold [Actual Value : 169/ Threshold : 5], 22:09:30 10/07/11
```

```
USERID04-w7@3001, Warning Event, The Smartstor duration on EM USERID04-w7@3001 is more than configured threshold [Actual Value : 1,255/ Threshold : 5]. The most likely cause would be slow disk., 22:09:31 10/07/11
```

```
USERID04-w7@5001, Warning Event, The Smartstor duration on EM USERID04-w7@5001 is more than configured threshold [Actual Value : 95/ Threshold : 50]. The most likely cause would be slow disk., 22:32:40 10/07/11
```

管理モジュールコマンド

管理モジュールは、Workstation 内のエレメントを整理して、検索および操作を容易にします。管理モジュール用の CLW コマンドを使用すると、Enterprise Manager 間で管理モジュールおよびそれに含まれるエレメントを容易に移動できるようになります。

List Management Modules

List Management Modules コマンドは、1つまたは複数の管理モジュールを一覧表示します。管理モジュールを指定する正規表現を入力します。

構文

```
list management modules matching <正規表現>
```

例

```
list management modules matching (.*)
```

このコマンドは、すべての管理モジュールを一覧表示します。

出力

各管理モジュールの名前が一覧表示されます。

```
Sample  
Sample13  
Sample11
```

Query Management Module

Query Management Module コマンドは、管理モジュールおよびその現在の状態（アクティブまたは非アクティブ）を一覧表示します。ターゲット管理モジュールを指定する正規表現を入力します。

構文

```
query state of management modules matching <正規表現>
```

例

```
query state of management modules matching (.*)
```

このコマンドは、すべての管理モジュールの名前と状態を返します。

出力

各管理モジュールの名前および状態が一覧表示されます。

```
Sample1:Active  
Sample2:Active
```

Activate Management Module

Activate Management Module コマンドは、1つまたは複数の管理モジュールをアクティブにします。ターゲット管理モジュールを指定する正規表現を入力します。

注: **Activate Management Module** コマンドは、問題切り分けマップ構成管理モジュールをアクティブにできません。

Deactivate Management Module

Deactivate Management Module コマンドは、1つまたは複数の管理モジュールを非アクティブにします。ターゲット管理モジュールを指定する正規表現を入力します。

注: **Deactivate Management Module** コマンドは、問題切り分けマップ構成管理モジュールを非アクティブにできません。

Copy Management Module

Copy Management Module コマンドは、`<EM_Home>/config/modules` ディレクトリに管理モジュールのコピーを作成します。

このコマンドを使用すると、既存の管理モジュールに基づく1つまたは複数の新しい管理モジュールを効率的に作成できます。たとえば、メトリックグループを除き、既存の管理モジュールと同一の新しい管理モジュールを作成するには、**CLW** を使用して既存の管理モジュールをコピーし、**GUI Workstation** で新しい管理モジュールのメトリックグループを変更します。

Copy Management Module コマンドでは、コピーする管理モジュール、新しい管理モジュールの名前、および新しい管理モジュールの `.jar` ファイルの名前（ファイル拡張子を除く）を指定します。

注: **Deactivate Management Module** コマンドは、問題切り分けマップ構成管理モジュールを非アクティブにできません。

Delete Management Module

Delete Management Module コマンドは、管理モジュールを削除します。削除する管理モジュールの名前を正確に指定します。

読み取り専用管理モジュール

このコマンドは、指定された正規表現に一致する管理モジュールを読み取り専用にします。

警告： CA Technologies は、編集可能な管理モジュールのコピーを安全な場所へ保管し、後で使用できるようにしておくことをお勧めします。これは、いったん管理モジュールが読み取り専用を設定されると、編集可能な状態には戻せないためです。

以下の手順に従います。

1. `readonly management modules matching` <正規表現> を設定します。
2. Workstation にログインし、管理モジュールエディタを開きます。正規表現に一致する管理モジュールの横に鍵のアイコンがあることが確認できます。
3. 許可されなくなった管理モジュールの隣の [編集可能] チェック ボックスをオフにします。

注： この機能は、CA Technologies のパートナーが使用するためのものです。ユーザ環境でこの機能を使用する場合には、CA サポート にお問い合わせください。

アクション コマンド

アクションは、アラートによって生成される通知などの動作です。

List Actions

List Actions コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアクションを一覧表示します。アクションを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

```
list actions matching <正規表現> in management modules matching <正規表現>
```

例

list actions matching (.) in management modules matching (.*)*

このコマンドは、すべての管理モジュールのすべてのアクションを一覧表示します。

出力

各アクションが一覧表示されます。名前の前にはそれを含む管理モジュールが付けられます。

Sample.SMTP Email Action

Sample10.Workstation Notification

Sample2.Workstation Notification

Activate Actions

Activate Actions コマンドは、1つまたは複数の管理モジュールの1つまたは複数のアクションをアクティブにします。アクティブにするアクションを指定する表現、および対象アクションを含む管理モジュールを指定する表現の2つの正規表現を入力します。

構文

activate actions matching <正規表現> in management modules matching <正規表現>

例

activate actions matching (SMTP.) in management modules matching (.*)*

このコマンドは、すべての管理モジュール内の、文字列 *SMTP* で始まるアクションをアクティブにします。

出力

コマンドによってアクティブにされた各アクションが一覧表示されます。名前の前にはそれを含む管理モジュール、名前の後にはアクティブ状態が付けられます。

```
Sample.SMTP Email Action:Active  
Sample10.Workstation Notification:Active  
Sample2.Workstation Notification:Active
```

Deactivate Actions

Deactivate Actions コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアクションを非アクティブにします。非アクティブにするアクションを指定する表現、および対象アクションを含む管理モジュールを指定する表現の 2 つの正規表現を入力します。

Query Actions

Query Actions コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアクションの状態（アクティブまたは非アクティブ）を一覧表示します。アクションを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

Rename Action

Rename Action コマンドは、アクションの名前を変更します。アクションの名前、それを含む管理モジュール、およびアクションの新しい名前を指定します。

Delete Action

Delete Action コマンドは、1 つまたは複数の管理モジュールから 1 つまたは複数のアクションを削除します。アクションを指定する表現、および削除元の管理モジュールを指定する表現の 2 つの正規表現を入力します。

注: たとえば、アラートにリンクされているアクションなど、別のエレメントによって使用または参照されているアクションは削除できません。

アラートコマンド

アラートは、メトリック値をユーザ定義しきい値と比較することによって、マネージド Java アプリケーションで問題が発生している可能性があることを指摘します。

List Alerts

List Alerts コマンドは、1つまたは複数の管理モジュールの1つまたは複数のアラートを一覧表示します。アラートを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
list alerts matching <正規表現> in management modules matching <正規表現>
```

例

```
list alerts matching (.*) in management modules matching Sample
```

このコマンドは、*Sample* という名前の管理モジュール内のアラートを一覧表示します。

出力

各アラートが一覧表示されます。名前の前にはそれを含む管理モジュールが付けられます。

```
Sample.Console Summary Alert  
Sample.All Servlet Response Time  
Sample.All EJB Response Times
```

Activate Alerts

Activate Alerts コマンドは、1つまたは複数の管理モジュールの1つまたは複数のアラートをアクティブにします。アクティブにするアラートを指定する表現、および対象アラートを含む管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
activate alerts matching <正規表現> in management modules matching <正規表現>
```

例

activate alerts matching (.) in management modules matching Same2*

このコマンドは、**Sample2** という名前の管理モジュール内のアラートをすべてアクティブにします。

出力

コマンドによってアクティブにされた各アラートが一覧表示されます。名前の前にはそれを含む管理モジュール、名前の後にはアラートの状態が付けられます。

```
Sample2.Application Summary Alert:Active  
Sample2.SQL Average Processing Time #2 (ms):Active  
Sample2.CPUApp1:Active
```

Deactivate Alerts

Deactivate Alerts コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアラートを非アクティブにします。非アクティブにするアラートを指定する表現、および対象アラートを含む管理モジュールを指定する表現の 2 つの正規表現を入力します。

Query Alerts

Query Alerts コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアラートの状態 (アクティブまたは非アクティブ) を一覧表示します。アラートを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

Rename Alert

Rename Alert コマンドは、アラートの名前を変更します。アラートの名前、それを含む管理モジュール、およびアラートの新しい名前を指定します。

Delete Alerts

Delete Alerts コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアラートを削除します。アラートを指定する表現、および削除元の管理モジュールを指定する表現の 2 つの正規表現を入力します。

注: たとえば、ダッシュボードで使用されているアラートなど、別のエレメントによって使用または参照されているアラートは削除できません。

アラートダウンタイム スケジュール コマンド

アラート ダウンタイム スケジュールを使用すると、Workstation 管理モジュール エディタからダウンタイムを管理できます。

List Alert Downtime Schedules

List Alert Downtime Schedules コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアラート ダウンタイム スケジュールを一覧表示します。アラート ダウンタイム スケジュールを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

```
list alert downtime schedules matching [正規表現] in management modules matching [正規表現]
```

例

```
List alert downtime schedules matching (.*) in management modules matching Sample
```

出力

```
Sample.Example Alert Downtime Schedule  
Sample.Another Alert Downtime Schedule
```

Activate Alert Downtime Schedules

Activate Alert Downtime Schedules コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のアラート ダウンタイム スケジュールをアクティブにします。アクティブにするアラート ダウンタイム スケジュールを指定する表現、および対象のアラート ダウンタイム スケジュールをアクティブにする管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

```
activate alert downtime schedules matching [正規表現] in management modules matching [正規表現]
```

例

activate alert downtime schedules matching (.) in management modules matching Sample*

出力

Sample.Example Alert Downtime Schedule:Active

Sample.Another Alert Downtime Schedule:Active

Deactivate Alert Downtime Schedules

Deactivate Alert Downtime Schedules コマンドは、1つまたは複数の管理モジュールの1つまたは複数のアラート ダウンタイム スケジュールを非アクティブにします。非アクティブにするアラート ダウンタイム スケジュールを指定する表現、および対象のアラート ダウンタイム スケジュールを非アクティブにする管理モジュールを指定する表現の2つの正規表現を入力します。

Query Alert Downtime Schedules

Query Alert Downtime Schedules コマンドは、1つまたは複数の管理モジュールにおける、1つまたは複数のアラート ダウンタイム スケジュール状態（アクティブまたは非アクティブ）を一覧表示します。アラート ダウンタイム スケジュールを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

Rename Alert Downtime Schedules

Rename Alert Downtime Schedules コマンドは、アラート ダウンタイム スケジュールの名前を変更します。アラート ダウンタイム スケジュールの名前と、それを含む管理モジュール、およびアラート ダウンタイム スケジュールの新しい名前を指定します。

Delete Alert Downtime Schedules

Delete Alert Downtime Schedules コマンドは、1つまたは複数のアラート ダウンタイム スケジュールを、1つまたは複数の管理モジュールから削除します。アラート ダウンタイム スケジュールを指定する表現、および削除元の管理モジュールを指定する表現の2つの正規表現を入力します。

計算機コマンド

計算機は、メトリックデータを合計または平均することによってカスタムメトリックを作成します。

List Calculators

List Calculators コマンドは、1つまたは複数の管理モジュールの1つまたは複数の計算機を一覧表示します。計算機を指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

構文

list calculators matching <正規表現> in management modules matching <正規表現>

例

list calculators matching (.) in management modules matching (.*)*

このコマンドは、すべての管理モジュールのすべての計算機を一覧表示します。

出力

各計算機が一覧表示されます。名前の前にはそれを含む管理モジュールが付けられます。

Sample.Average Servlet Response Time

Activate Calculators

Activate Calculators コマンドは、1つまたは複数の管理モジュールの1つまたは複数の計算機をアクティブにします。アクティブにする計算機を指定する表現、および対象の計算機を含む管理モジュールを指定する表現の2つの正規表現を入力します。

構文

activate calculators matching <正規表現> in management modules matching <正規表現>

例

activate calculators matching (.) in management modules matching Sample2*

このコマンドは、**Sample2** という名前の管理モジュール内のすべての計算機をアクティブにします。

出力

コマンドによってアクティブにされた各計算機が一覧表示されます。名前の前にはそれを含む管理モジュール、名前の後にはその状態が付けられます。

Sample2.Average Servlet Response Time:Active

Deactivate Calculators

Deactivate Calculators コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数の計算機を非アクティブにします。非アクティブにする計算機を指定する表現、および対象計算機を含む管理モジュールを指定する表現の 2 つの正規表現を入力します。

Query Calculators

Query Calculators コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数の計算機の状態（アクティブまたは非アクティブ）を一覧表示します。計算機を指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

Rename Calculator

Rename Calculator コマンドは、計算機の名前を変更します。計算機の名前、それを含む管理モジュール、および計算機の新しい名前を指定します。

Delete Calculators

Delete Calculators コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数の計算機を削除します。計算機を指定する表現、および削除元の管理モジュールを指定する表現の 2 つの正規表現を入力します。

注: たとえば、ダッシュボードで使用されている計算機など、別のエレメントによって使用または参照されている計算機は削除できません。

ダッシュボード コマンド

ダッシュボードは、Workstation に表示されるページであり、グラフ、棒グラフ、およびアラート ステータス インジケータなどの Data Viewer オブジェクトとグラフ オブジェクトおよびテキスト オブジェクトで構成されます。

List Dashboards

List Dashboards コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のダッシュボードを一覧表示します。ダッシュボードを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

```
list dashboards matching <正規表現> in management modules matching <正規表現>
```

例

```
list dashboards matching (. *Triage) in management modules matching (. *)
```

このコマンドは、すべての管理モジュール内の、名前が文字列 *Triage* で終わるダッシュボードを一覧表示します。

出力

各ダッシュボードが一覧表示されます。名前の前にはそれを含む管理モジュールが付けられます。

```
Sample10.3. Triage
```

```
Sample2.3. Triage
```

```
Sample.3. Triage
```

Activate Dashboards

Activate Dashboards コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数のダッシュボードをアクティブにします。アクティブにするダッシュボードを指定する表現、および対象のダッシュボードを含む管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

activate dashboards matching <正規表現> in management modules matching <正規表現>

例

activate dashboards matching (.) in management modules matching Sample2*

このコマンドは、*Sample2* という名前の管理モジュール内のすべてのダッシュボードをアクティブにします。

出力

コマンドによってアクティブにされた各ダッシュボードが一覧表示されます。名前の前にはそれを含む管理モジュール、名名の後にはその状態が付けられます。

Sample2.4b. Database Detail:Active

Sample2.1. Introscope Console:Active

Sample2.2. Detection:Active

Deactivate Dashboards

Deactivate Dashboards コマンドは、1つまたは複数の管理モジュールの1つまたは複数のダッシュボードを非アクティブにします。非アクティブにするダッシュボードを指定する表現、および対象のダッシュボードを含む管理モジュールを指定する表現の2つの正規表現を入力します。

Query Dashboards

Query Dashboards コマンドは、1つまたは複数の管理モジュールの1つまたは複数のダッシュボードの状態（アクティブまたは非アクティブ）を一覧表示します。ダッシュボードを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

Rename Dashboard

Rename Dashboard コマンドは、ダッシュボードの名前を変更します。ダッシュボードの名前、それを含む管理モジュール、およびダッシュボードの新しい名前を指定します。

Delete Dashboards

Delete Dashboards コマンドは、1つまたは複数の管理モジュールの1つまたは複数のダッシュボードを削除します。ダッシュボードを指定する表現、および削除元の管理モジュールを指定する表現の2つの正規表現を入力します。

注: 別のエレメントによって使用または参照されているダッシュボードは削除できません。たとえば、別のダッシュボード上の **Data Viewer** へのハイパーリンクがあるダッシュボードは削除できません。

メトリック コマンドおよびメトリック グループ コマンド

メトリック グループは、コマンドの実行対象となるメトリックを指定します。これは、アラートおよび計算機などのエレメントの構成単位として使用されます。

List Metric Groups

List Metric Groups コマンドは、1つまたは複数の管理モジュールの1つまたは複数のメトリック グループを一覧表示します。メトリック グループを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
list metric groups matching <正規表現> in management modules matching <正規表現>
```

例

```
list metric groups matching (. *Response. *) in management modules matching Sample
```

このコマンドは、*Sample* という名前の管理モジュール内の、名前に文字列 *Response* を含むメトリック グループを一覧表示します。

出力

メトリック グループは以下の形式で一覧表示されます。

```
<管理モジュール>.<メトリック グループ>[Agent: "<エージェント記述子>"  
Attribute: "<メトリック記述子>"]
```

例 :

```
Sample.Servlet Average Response Time (ms) [Agent: "(.*)¥/(.*)¥/(.*)"  
Attribute:¥"Servlets:Average Response Time ¥(ms¥)"]
```

このサンプルは、メトリック グループについての以下の情報を提供します。

管理モジュール : *Sample*

メトリック グループ名 : *Servlet Average Response Time (ms)*

エージェント記述子 : *(.*)¥/(.*)¥/(.*)*

メトリック記述子 : *Servlets:Average Response Time (ms)*

Turn On Exact Metric

このコマンドは、エージェントが特定のメトリックをオンにすることを要求します。

構文

```
turn on exact metric <メトリック名>
```

例

```
turn on exact metric  
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:A  
verage Response Time (ms)
```

エージェントは

```
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:  
Average Response Time (ms) メトリックをオンにし、データの送信を開始し  
ます。
```

出力

なし

Turn Off Exact Metric

このコマンドは、エージェントが特定のメトリックをオフにすることを要求します。

構文

```
turn off exact metric <メトリック名>
```

例

```
turn off exact metric  
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:Average Response Time (ms)
```

エージェントは
jdoe-dt|Weblogic|WebLogicAgent|Servlets|Servlet21|Servlet21_1u2oj1_Impl:Average Response Time (ms) メトリックをオフにして、データの送信を停止します。

出力

なし

レポートテンプレートコマンド

このセクションでは、レポートの管理と生成を行う CLW コマンドについて定義しています。Introscope のレポート機能の詳細については、「CA APM Workstation ユーザガイド」の「レポート機能」の章を参照してください。

List Report Templates

List Report Templates コマンドは、1つまたは複数の管理モジュールの1つまたは複数のレポートテンプレートを一覧表示します。レポートテンプレートを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
list report templates matching <正規表現> in management modules matching <正規表現>
```

例

```
list report templates matching (.*) in management modules matching Sample
```

このコマンドは、*Sample* という名前の管理モジュール内のすべてのレポートテンプレートを一覧表示します。

出力

各レポートテンプレートの名前の前にはそれを含む管理モジュールが付けられます。

```
Sample.QA/Test Application Performance  
Sample.System Availability  
Sample.Application Capacity Planning
```

Activate Report Templates

Activate Report Templates コマンドは、1つまたは複数の管理モジュールの1つまたは複数のレポートテンプレートをアクティブにします。アクティブにするレポートテンプレートを指定する表現、および対象のレポートテンプレートを含む管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
activate report templates matching <正規表現> in management modules matching <正規表現>
```

例

activate report templates matching (.) in management modules matching Sample2*

このコマンドは、Sample2 という名前の管理モジュール内のすべてのレポートテンプレートをアクティブにします。

出力

コマンドによってアクティブにされた各レポートテンプレートが一覧表示されます。名前の前にはそれを含む管理モジュール、名名の後にはその状態が付けられます。

Sample2.Application Capacity Planning:Active

Sample2.Production Application Health:Active

Sample2.System Availability:Active

Deactivate Report Templates

Deactivate Report Templates コマンドは、1つまたは複数の管理モジュールの1つまたは複数のレポートテンプレートを非アクティブにします。非アクティブにするレポートテンプレートを指定する表現、および対象のレポートテンプレートを含む管理モジュールを指定する表現の2つの正規表現を入力します。

Query Report Templates

Query Report Templates コマンドは、1つまたは複数の管理モジュールの1つまたは複数のレポートテンプレートの状態（アクティブまたは非アクティブ）を一覧表示します。レポートテンプレートを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

Rename Report Template

Rename Report Template コマンドは、レポートテンプレートの名前を変更します。レポートテンプレートの名前、それを含む管理モジュール、およびレポートテンプレートの新しい名前を指定します。

Delete Report Templates

Delete Report Templates コマンドは、1 つまたは複数の管理モジュールから 1 つまたは複数のレポート テンプレートを削除します。 レポート テンプレートを指定する表現、および削除元の管理モジュールを指定する表現の 2 つの正規表現を入力します。

Generate Report

Generate Report コマンドはレポートを実行します。 以下の引数を設定します。

- レポート名
- 開始時刻
- 終了時刻
- 管理モジュール名
- ファイル名 - パスが指定されていない場合、このファイルは現在の作業ディレクトリに書き込まれます。 このファイルは、ファイル拡張子に関連付けられた形式で書き込まれます。 拡張子は、HTML、PDF、XLS、TEXT、XML、CSV のいずれかである必要があります。

コマンド

Generate Report コマンドには、基本、拡張、およびエージェント オーバーライド コマンドの 3 種類があります。

基本コマンド:

```
generate report named [完全一致] in management module named [完全一致] to [完全一致]
```

拡張コマンド:

```
generate report named [完全一致] in management module named [完全一致] starting at [完全一致] ending at [完全一致] to [完全一致]
```

オプション パラメータ

上記の基本コマンドおよび拡張コマンドの両方でオプションパラメータを使用できます。

```
{in agents matching [正規表現パターン]} {starting at [完全一致] ending at [完全一致]}
```

オプションパラメータの構文は以下のとおりです。

```
generate report named [完全一致] in management module named 完全一致  
{in agents matching [正規表現パターン]} {starting at [完全一致] ending at [完全一致]} to [完全一致]
```

レポートタイムスタンプの形式

レポートタイムスタンプはさまざまな形式で表されます。以下の表に、可能な各種形式を示します。

| タイムスタンプの形式 | 例 |
|-------------------------------------|----------------------------------|
| <i>M/d/yy h:mm a</i> | 11/17/08 3:00 PM |
| <i>M/d/yy h:mm:ss a</i> | 11/17/08 3:00:06 PM |
| <i>M/d/yy h:mm:ss a z</i> | 11/17/08 3:00:06 PM PST |
| <i>M/d/yy</i> | 11/17/08 |
| <i>MMM d, yyyy h:mm a</i> | Nov 17, 2008 3:00 PM |
| <i>MMM d, yyyy h:mm:ss a</i> | Nov 17, 2008 3:00:06 PM |
| <i>MMM d, yyyy h:mm:ss a z</i> | Nov 17, 2008 3:00:06 PM PST |
| <i>MMM d, yyyy</i> | Nov 17, 2008 |
| <i>MMMM d, yyyy h:mm a</i> | November 17, 2008 3:00 PM |
| <i>MMMM d, yyyy h:mm:ss a</i> | November 17, 2008 3:00:06 PM |
| <i>MMMM d, yyyy h:mm:ss a z</i> | November 17, 2008 3:00:06 PM PST |
| <i>MMMM d, yyyy</i> | November 17, 2008 |
| <i>EEE MMM dd HH:mm:ss zzz yyyy</i> | Mon Nov 17 15:00:06 PST 2008 |
| <i>MM/dd/yy HH:mm:ss</i> | 11/17/08 15:00:06 |
| <i>yyyy-MM-dd HH:mm:ss</i> | 2008-11-17 15:00:06 |
| <i>yyyy-MM-dd HH:mm:ss.SSSS</i> | 2008-11-17 15:00:06.0840 |

| | |
|------------------------------------|------------------------|
| <code>yyyy-MM-dd HH:mm</code> | 2008-11-17 15:00 |
| <code>yyyy-MM-dd hh:mm:ss a</code> | 2008-11-17 03:00:06 PM |
| <code>yyyy-MM-dd hh:mm a</code> | 2008-11-17 03:00 PM |
| <code>yyyy/MM/dd hh:mm:ss a</code> | 2008/11/17 03:00:06 PM |
| <code>yyyy/MM/dd hh:mm a</code> | 2008/11/17 03:00 PM |
| <code>yyyy/MM/dd HH:mm:ss</code> | 2008/11/17 15:00:06 |
| <code>yyyy/MM/dd HH:mm</code> | 2008/11/17 15:00 |

SNMP コレクション コマンド

以下のコマンドは、収集したメトリックのうち、公開される MIB に含めるメトリックを定義します。

List SNMP Collections

List SNMP Collections コマンドは、1 つまたは複数の管理モジュールの 1 つまたは複数の SNMP コレクションを一覧表示します。SNMP コレクションを指定する表現、および管理モジュールを指定する表現の 2 つの正規表現を入力します。

構文

```
list snmp collections matching <正規表現> in management modules matching <正規表現>
```

例

```
list snmp collections matching (.*) in management modules matching (.*)
```

このコマンドは、すべての管理モジュールのすべての SNMP コレクションを一覧表示します。

出力

各 SNMP コレクションの名前の前にはそれを含む管理モジュールが付けられます。例：

```
Sample2.JDBC QueryUpdate
```


Activate SNMP Collections

Activate SNMP Collections コマンドは、1つまたは複数の管理モジュールの1つまたは複数の SNMP コレクションをアクティブにします。アクティブにする SNMP コレクションを指定する表現、および対象の SNMP コレクションを含む管理モジュールを指定する表現の2つの正規表現を入力します。

構文

```
activate snmp collections matching <正規表現> in management modules  
matching <正規表現>
```

例

```
activate snmp collections matching (.*) in management modules matching  
Sample2
```

このコマンドは、**Sample2** という名前の管理モジュール内のすべての SNMP コレクションをアクティブにします。

出力

コマンドによってアクティブにされた各 SNMP コレクションが一覧表示されます。名前の前にはそれを含む管理モジュール、名名の後にはその状態が付けられます。

```
Sample2.JDBC QueryUpdate:Active
```

Deactivate SNMP Collections

Deactivate SNMP Collections コマンドは、1つまたは複数の管理モジュールの1つまたは複数の SNMP コレクションを非アクティブにします。非アクティブにする SNMP コレクションを指定する表現、および対象の SNMP コレクションを含む管理モジュールを指定する表現の2つの正規表現を入力します。

Query SNMP Collections

Query SNMP Collections コマンドは、1つまたは複数の管理モジュールの1つまたは複数の SNMP コレクションの状態（アクティブまたは非アクティブ）を一覧表示します。SNMP コレクションを指定する表現、および管理モジュールを指定する表現の2つの正規表現を入力します。

Rename SNMP Collection

Rename SNMP Collection コマンドは、SNMP コレクションの名前を変更します。SNMP コレクションの名前、それを含む管理モジュール、および SNMP コレクションの新しい名前を指定します。

Delete SNMP Collections

Delete SNMP Collections コマンドは、1つまたは複数の管理モジュールから1つまたは複数の SNMP コレクションを削除します。SNMP コレクションを指定する表現、および削除元の管理モジュールを指定する表現の2つの正規表現を入力します。

トランザクション追跡オプションの設定

CLW には、これらのシステム プロパティを使用してさまざまなトランザクション追跡オプションを設定するオプションが用意されています。

- - *Dintroscope.clw.tt.console* - true に設定すると、トランザクション追跡はコンソールに出力されます。
- - *Dintroscope.clw.tt.dirname* - トランザクション追跡の XML ファイルを保存するローカル ディレクトリ。
- - *Dintroscope.clw.tt.filename* - トランザクション追跡の保存に使用するファイル名。ここにディレクトリ名を含めることはできません。
- - *Dintroscope.clw.tt.encoding* - XML ファイルをディスクに書き込む際に使用するエンコード。このプロパティの設定には、デフォルトのオプションである *ISO-8859-1* と、*UTF-8*、*UTF-16*、および *Windows-1252* が含まれます。

トランザクション追跡セッションの開始

Transaction Tracer は、単一 JVM の境界を通過する個別のトランザクションのアクティビティを追跡します。

トランザクション追跡は、トランザクション イベント データベースに自動的に保存され、デフォルトで 1 つ以上の XML ファイル内にも取得されます。このファイルを、CA Introscope Workstation のトランザクション追跡ビューアで開いて分析できます。CA Introscope Transaction Tracer 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。

コマンド構文

CLW コマンドでは、トランザクション追跡セッションに関してさまざまな要素を指定できます。以下はその例です。

- 実行しきい値 - 追跡するトランザクションの最小実行時間。追跡は、しきい値よりも実行時間が長いトランザクションに対して実行されます。しきい値は、秒単位で指定できます。
- 追跡するエージェント - トランザクションを追跡するエージェントを指定する Perl 正規表現。
- セッションの存続期間 - トランザクション追跡セッションの存続期間 (秒単位)。

しきい値を秒で指定してトランザクション追跡セッションを開始する構文を以下に示します。

```
trace transactions exceeding <完全一致> (second/seconds/sec/secs/s) in  
agents matching <正規表現> for <完全一致> <second/seconds/sec/secs/s>
```

その他の CLW コマンドオプションの詳細は、[後述の「コマンドオプション」](#) (P. 204) で説明されています。トランザクション追跡 CLW コマンドの例については、「[トランザクション追跡コマンドの例](#) (P. 206)」を参照してください。

トランザクション追跡の出力ファイルの指定

トランザクション追跡の出力ファイルの名前を指定できます。

構文

```
Dintroscope.clw.tt.filename=<ファイル名>
```

例

トランザクション追跡の出力ファイルのファイル名 (完全パスではない) を指定します。出力ディレクトリを指定するプロパティと組み合わせて使用します。

出力

トランザクション追跡の結果が、指定したファイルに出力されます。

コマンド オプション

このセクションでは、トランザクション追跡コマンドのオプションについて説明します。

追跡モード

CLW は、トランザクション追跡セッションの結果を、以下の 2 つのモードでキャプチャすることをサポートしています。

- 同期モード - デフォルトで、CLW はセッションの最後に、トランザクションイベント データベース、および *TransactionTraceData-yyyyMMddhhmmss.xml* という名前の単一の XML ファイルに、追跡結果を書き込みます。ファイル名の日付と時刻の文字列はセッションの開始日時を反映しています。
- 非同期モード - このモードでは、CLW は、各トランザクションの追跡結果を、レポート後すぐにトランザクションイベント データベース、およびそのトランザクション固有の XML ファイルに書き込みます。このファイルは、*nnnn(sec)-TransactionTraceDatayyyyMMddhhmmss-<sequence number>.xml* という名前で、*nnnn* は秒単位のトランザクションの存続期間、および日付と時刻の文字列はトランザクションの開始日時を反映しています。自分でファイル名を付ける場合は、最後の「.」の前にシーケンス番号を追加します。付けたファイル名に「.」が含まれない場合は、ファイル名の最後にシーケンス番号が付けられます。

同期モードで記録された結果は、すべてのデータが 1 つのファイルに含まれているので、簡単に表示できます。ただし、セッションが終了するまでデータを表示することはできません。さらに、大量のトランザクション、または複雑なトランザクションの場合、同期キャプチャでは、多くのメモリを消費する可能性があります。

トランザクションデータを非同期で記録すると、メモリの消費量が少なくなり、また、トランザクション追跡セッションが終了する前にトランザクションデータを表示できます。

`-Dintroscope.clw.tt.mode=(Synch|Asynch)`

トランザクション イベント データベースのみへの出力

このオプションは、トランザクション追跡を実行し、その出力結果をトランザクション イベント データベースのみに保存する（XML ファイルには出力しない）場合に使用します。このコマンドは、Introscope アラートがトリガされたときに、そのアラートによって自動的に追跡トランザクションを開始する場合に便利です。

以下のように、コマンドの最初に「*quietly*」を付けます。

```
quietly trace transactions exceeding 2 seconds in agents matching "(.*)" for 60 seconds
```

ヘッダ データのみの返還

場合によっては、CLW を使用して大量のトランザクション追跡データを抽出する際に、*traces.db* ファイルが際限なく大きくなる可能性があり、その結果、CLW が結果を返すのにかなりの時間がかかってしまうことがあります。このプロパティを **false** に設定すると、Enterprise Manager が返すデータの量が減少するため、問題が解決します。

CLW は追跡データのヘッダ部分のみ返します。デフォルトまたはこのプロパティを **true** に設定すると、CLW によって取得されるトランザクション追跡データには、ヘッダと本文両方が含まれます。

```
-Dwily.ps.workstation.clws.gettracebody
```

Transaction Tracer クランプ

デフォルトの設定では、個別のトランザクション追跡で抽出される追跡コンポーネントの数は **5000** までです。そのサイズを超えるトランザクション追跡は、エージェントによって破棄され、以下のような警告メッセージがエージェント ログ ファイルに記録されます。

```
07/02/23 17:33:18 PST [WARN] [IntroscopeAgent] Transaction trace component limit of 5000 reached, recording will cease for this transaction.
```

トランザクション追跡で使用できるコンポーネントの最大数を変更するには、エージェント プロパティ

```
introscope.agent.transactiontrace.componentCountClamp=max_TT_components (デフォルトは 5000) を変更します。
```

たとえば、エージェントのプロファイルに以下の行があるとします。

```
introscope.agent.transactiontrace.componentCountClamp=30000
```

この行は、トランザクション追跡で使用できるコンポーネントの最大数を **30,000** に変更します。

警告： このクランプのサイズを大きくすると、トランザクション追跡に必要なメモリも増えるため、**JVM** の最大ヒープ サイズを適切に調整する必要があります。調整しないと、**Enterprise Manager** のメモリが不足する可能性があります。

トランザクション追跡コマンドの例

このセクションでは、トランザクション追跡セッションを開始する **CLW** コマンドの例を示します。以下の例の各コマンドは、**600** 秒間のセッションを開始します。すべてのエージェントからの **5** 秒を超えるトランザクションが追跡されます。

注: 例のコマンドはすべて、デフォルトのログイン設定を使用して **Enterprise Manager** に接続します。

トランザクション追跡セッションを実行するスクリプトの例については、「[サンプル スクリプト \(P. 221\)](#)」を参照してください。

デフォルトのオプション値を使用したトランザクション追跡

以下の CLW コマンドは、以下のデフォルト設定を使用してトランザクション追跡セッションを開始します。

- 追跡モード - トランザクション追跡データは同期的にキャプチャされます。したがって、すべての結果は 1 つの XML ファイルに書き込まれます。
- ディレクトリの場所 - *Dintroscope.clw.tt.dirname* が指定されていない場合、追跡結果は現在の作業ディレクトリに書き込まれます。

```
java -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

非同期キャプチャを使用したトランザクション追跡

以下の CLW コマンドは、セッションの出力にデフォルトディレクトリの場所を使用するトランザクション追跡セッションを開始します。

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

データは非同期でキャプチャされます。したがって、各トランザクションに対して個別の XML ファイルが作成されます。

ユーザ定義ディレクトリに書き込まれるトランザクション追跡結果

以下の CLW コマンドは、追跡モードのデフォルト設定（トランザクション追跡データを同期的にキャプチャする）を使用して、トランザクション追跡セッションを開始します。したがって、すべての結果は 1 つの XML ファイルに書き込まれます。

```
java -Dintroscope.clw.tt.dirname=C:\mytraces -jar CLWorkstation.jar trace transactions exceeding 5 seconds in agents matching "(.*)" for 600 seconds
```

このコマンドでは、XML ファイルにデフォルト以外のディレクトリ *C:\mytraces* を指定しています。

パラメータとエラー フィルタを使用するトランザクション追跡

ユーザは、実行する秒数を指定し、**Workstation** で利用可能なものと同じフィルタを使用するトランザクション追跡セッションを開始することができます。それらのフィルタには、ユーザ ID、URL、URL クエリ、セッション ID、リクエスト ヘッダ、リクエスト パラメータ、セッション属性、およびエラーなどがあります。

ユーザ ID、URL、URL クエリ、またはセッション ID に基づくフィルタリング

```
trace transactions where (userid|url|url query|sessionid) (equals|not equals|contains|not contains|starts with|ends with) [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
trace transactions where (userid|url|url query|sessionid) (exists|not exists) in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (userid|url|url query|sessionid) (equals|not equals|contains|not contains|starts with|ends with) [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (userid|url|url query|sessionid) (exists|not exists) in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

リクエスト ヘッダ、リクエスト パラメータ、またはセッション属性に基づくフィルタリング

```
trace transactions where (request header|request parameter|session attribute) [完全一致] (equals|not equals|contains|not contains|starts with|ends with) [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
trace transactions where (request header|request parameter|session attribute) [完全一致] (exists|not exists) in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (request header|request parameter|session attribute) [完全一致] (equals|not equals|contains|not contains|starts with|ends with) [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
quietly trace transactions where (request header|request parameter|session attribute) [完全一致] (exists|not exists) in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

エラーに基づくフィルタリング

```
trace transactions with errors containing [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```

```
quietly trace transactions with errors containing [完全一致] in agents matching [正規表現] for [完全一致] (second|seconds|sec|secs|s)
```


トランザクション イベント データベース内のトランザクション追跡結果のクエリ

トランザクション追跡結果は、自動的にトランザクションイベントデータベースに保存されます。そのデータは、ここで説明する CLW コマンドで取得できます。

Get Historical Events Matching <値>

このコマンドは、トランザクションイベントデータベースからフルイベント XML 出力ファイルを取得します。フルイベント（以下のサマリイベントに対して）は、トランザクションイベントビューアの下部 3 分の 2 で利用できるフルデータです。

```
java -Dintroscope.clw.tt.mode=Asynch -jar CLWorkstation.jar trace transactions get historical events matching "localhost"
```

出力例を以下に示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00" StartDate="2005-06-20T17:40:24.068-08:00"
User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddlemann-dt2" AgentName="Tomcat" StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<CalledComponents>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
<CalledComponent RelativeTimestamp="0" Duration="62" ComponentType="Servlets"
ComponentName="HelloWorldExample" MetricPath="Servlets|HelloWorldExample">
<CalledComponents>
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
```

```
<CalledComponent RelativeTimestamp="0" Duration="0" ComponentType="JNDI"
ComponentName="ProxyDirContext" MetricPath="JNDI|Context|ProxyDirContext">
<Parameters>
<Parameter Value="lookup" Name="Method"/>
</Parameters>
</CalledComponent>
</CalledComponents>
</TransactionTrace>
</TransactionTracerSession>
```

Get Summaries Matching <VALUE>

このコマンドは、トランザクションイベントデータベースからイベントサマリ XML のみを取得して、XML ファイルを出力します。イベントサマリは、トランザクションイベントビューアの上部ペインで利用できる情報です。このコマンドは、たとえば、トランザクションイベントデータベースからデータをエクスポートして、システムでその日に発生したエラー数についてのレポートを生成する場合に便利です。

get historical event summaries matching [正規表現]

出力例を以下に示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TransactionTracerSession Duration="78" Version="0.1"
EndDate="2005-06-20T17:40:24.146-08:00" StartDate="2005-06-20T17:40:24.068-08:00"
User="Admin">
<TransactionTrace Domain="SuperDomain" Duration="78" Process="UnknownProcess"
Host="maddlemann-dt2" AgentName="Tomcat" StartDate="2005-06-20T17:40:24.068-08:00"
EndDate="2005-06-20T17:40:24.146-08:00">
<CalledComponent RelativeTimestamp="0" Duration="78" ComponentType="Browser"
ComponentName="Browser" MetricPath="Browser">
<Parameters>
<Parameter Value="" Name="URL"/>
<Parameter Value="Normal" Name="Trace Type"/>
<Parameter Value="¥20050620¥17¥1119314425302" Name="Trace ID"/>
<Parameter Value="" Name="User ID"/>
</Parameters>
</CalledComponent>
</TransactionTrace>
</TransactionTracerSession>
```

アプリケーション問題切り分けマップのコマンド

問題切り分けマップアラートは、アプリケーションマップおよびアプリケーションマップエンティティに関連付けられた特別なアラートです。問題切り分けマップアラートの格納場所は、*TriageMapConfigurationsManagementModule.jar* ファイルの問題切り分けマップ構成管理モジュール内です。

以下のコマンドは、この管理モジュールで利用できます。

[List Management Modules](#) (P. 211)

[Query State of Management Modules](#) (P. 212)

[List Triage Map Alerts](#) (P. 212)

[Query State of Management Modules](#) (P. 214)

[List Triage Map Entity Metric Groups](#) (P. 216)

[Query the State of Triage Map Entity Metric Groups](#) (P. 217)

List Management Modules

このコマンドは、問題切り分けマップ管理モジュールの名前を一覧表示します。

構文

```
list management modules matching <正規表現>
```

例

```
list management modules matching (Triage Map.*)
```

このコマンドは、名前が *Triage Map* で始まる管理モジュールを一覧表示します。

出力

各管理モジュールの名前および状態が一覧表示されます。この場合、問題切り分けマップ構成管理モジュールは正規表現に一致し、以下のように一覧表示されます。

```
Triage Map Configurations
```

Query State of Management Modules

このコマンドは、問題切り分けマップ管理モジュールのステータスを一覧表示します。

構文

query state of management modules matching [正規表現]

例

query state of management modules matching (.)*

このコマンドは、すべての管理モジュールの名前と状態を返します。

出力

お使いのシステムについて設定された各管理モジュールの名前と状態を一覧表示します。例：

```
Supportability:Active  
Trade Application Definitions:Active  
Triage Map Configurations:Active  
Browser Response Time Adapter:Active  
Sample:Active  
MOM Infrastructure Monitoring:Active  
Reports Unit Tests:Active  
Collector - 1:Active  
ChangeDetector:Active  
CEM BT Stats:Active
```

List Triage Map Alerts

このコマンドは、問題切り分けマップアラートを一覧表示します。

構文

list triage map alerts matching [正規表現] in management modules matching [正規表現]

例

list triage map alerts matching (.) in management modules matching (Triage Map.*)*

このコマンドは、名前が *Triage Map* で始まる管理モジュール内のすべての問題切り分けマップアラートを一覧表示しようとします。

出力

システムで設定されたすべての問題切り分けマップアラートの名前を一覧表示します。例：

```
Triage Map Configurations.By Frontend|TradeService|Health:Average Response Time
(ms)_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|loginAdmin.action|loginAdmin.action:Errors Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend|ReportingService|Backend
Calls|WebServices:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Average Response Time (ms)_Location_MetricAlert
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Backend
Calls|localhost%9082/medrec(POINTBASE DB):Alert
Triage Map Configurations.By Frontend|ReportingEngine|Backend
Calls|jdbc%hsqldb%file%report-records:Stall Count_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Stall Count_Location_MetricAlert
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|home.action:Alert
Triage Map Configurations.By Frontend|/medrec|Health:Errors Per
Interval_Location_MetricAlert
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|View Orders:Total Defects Per Interval_Summary_MetricAlert
Triage Map Configurations.By Frontend|AuthenticationService|Health:Errors Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Concurrent Invocations_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Stall Count_Location_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Concurrent
Invocations_Summary_MetricAlert
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|viewPatients.action:Total Defects Per
Interval_Summary_MetricAlert
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Average Response Time
(ms)_Summary_MetricAlert
```

Query State of Management Modules

このコマンドは、問題切り分けマップアラートのステータスを一覧表示します。

構文

```
query state of triage map alerts matching [正規表現] in management modules
matching [正規表現]
```

例

```
query state of triage map alerts matching (.*) in management modules
matching (Triage Map.*)
```

このコマンドは、名前が *Triage Map* で始まる管理モジュール内のすべての問題切り分けマップアラートとその状態を一覧表示します。

出力

システムで設定されたすべての問題切り分けマップアラートの名前と状態を一覧表示します。例：

```
Triage Map Configurations.By Frontend|TradeService|Health:Average Response Time
(ms)_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|loginAdmin.action|loginAdmin.action:Errors Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|ReportingService|Backend
Calls|WebServices:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Average Response Time (ms)_Location_MetricAlert:Active
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Backend
Calls|//localhost%9082/medrec(POINTBASE DB):Alert:Active
Triage Map Configurations.By Frontend|ReportingEngine|Backend
Calls|jdbc%hsqldb%file%report-records:Stall Count_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|viewNewlyRegisteredPatien
ts.action:Stall Count_Location_MetricAlert:Active
Triage Map Configurations.Business Service|MedRecBS|Business
Transactions|home.action:Alert:Active
Triage Map Configurations.By Frontend|/medrec|Health:Errors Per
Interval_Location_MetricAlert:Active
Triage Map Configurations.Business Service|Trading Service|Business
Transactions|View Orders:Total Defects Per Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Errors Per
Interval_Summary_MetricAlert:Active
Triage Map Configurations.By Business Service|Trading Service|Options
Trading|Check Options:Concurrent Invocations_Summary_MetricAlert:Active
Triage Map Configurations.By Business
Service|MedRecBS|index.action|index.action:Stall
Count_Location_MetricAlert:Active
```

List Triage Map Entity Metric Groups

このコマンドは、問題切り分けマップ エンティティ メトリック グループの名前を一覧表示します。

構文

```
list triage map entity metric groups matching [正規表現] in management modules matching [正規表現]
```

例

```
list triage map entity metric groups matching (.*) in management modules matching (Triage Map.*)
```

このコマンドは、名前が **Triage Map** で始まる管理モジュール内のすべての問題切り分けマップ エンティティ グループを一覧表示します。

出力

システムで設定されたすべての問題切り分けマップ エンティティ グループの名前と状態を一覧表示します。 例：

```
Triage Map Configurations.By Frontend|/medrec|Health:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Health:Average Response Time (ms)_Summary
Triage Map Configurations.Business Service|MedRecBS|Business Transactions|index.action:Total Defects Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|View Orders|View my order:Concurrent Invocations_Location
Triage Map Configurations.By Frontend|PatientFacadeServiceWebApp|Health:Errors Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Transaction Summary|Request Transaction Summary:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|ReportingEngine|Health:Errors Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options Trading|Check Options:Errors Per Interval_Summary
Triage Map Configurations.By Frontend|AuthenticationEngine|Backend Calls|jdbc%hsqldb%file%customer-records:Average Response Time (ms)_Summary
Triage Map Configurations.By Frontend|OrderEngine|Health:Average Response Time (ms)_Location
Triage Map Configurations.Business Service|MedRecBS|Business Transactions|viewPatients.action:Total Transactions Per Interval_Summary
Triage Map Configurations.By Business Service|Trading Service|Options Trading|Check Options:Stall Count_Summary
```


Query the State of Triage Map Entity Metric Groups

このコマンドは、問題切り分けマップ エンティティ メトリック グループのステータスを一覧表示します。

構文

```
query state of triage map entities matching [正規表現] in management modules  
matching [正規表現]
```

例

```
query state of triage map entities matching (.*) in management modules  
matching (Triage Map .*)
```

このコマンドは、名前が **Triage Map** で始まる管理モジュール内のすべての問題切り分けマップ エンティティとその状態を一覧表示しようとします。

出力

システムで設定されたすべての問題切り分けマップ エンティティの名前を一覧表示します。例：

```
Triage Map Configurations.By Frontend|OrderEngine|Backend Calls:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action|kmuernxjnsdfgdfhjwerhgiusadfoiuoherg:Active
Triage Map Configurations.By Frontend|/medrec|Backend Calls|System localhost on port 9082:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewPatient.action|viewPatient.action:Active
Triage Map Configurations.By Frontend|Apache-Axis:Active
Triage Map Configurations.By Business Service|Trading Service:Active
Triage Map Configurations.By Business Service|Trading Service|Balances:Active
Triage Map Configurations.By Frontend|AuthenticationEngine:Active
Triage Map Configurations.By Frontend|AuthenticationService|Backend Calls|WebServices:Active
Triage Map Configurations.By Frontend|AuthenticationService|Health:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewRecordSummary.action:Active
Triage Map Configurations.By Business
Service|MedRecBS|viewNewlyRegisteredPatients.action|kmuernxjnsdfgdfhjwerhgiusadfoiuoherg:Active
Triage Map Configurations.By Business Service|Trading Service|Place Order:Active
Triage Map Configurations.Business Service|Trading Service|Business Transactions|Login:Active
Triage Map Configurations.Business Service|MedRecBS|Business Transactions|index.action:Active
```

Loadbalancing.xml コマンド

MOM は loadbalancing.xml ファイルを使用して、クラスタ全体でエージェントの負荷分散を行い、エージェントが特定のコレクタに接続できるようにします。これらのコマンドは loadbalancing.xml ファイルを更新します。

Autoprepare Loadbalancing.xml

このコマンドはアップグレード時に MOM で実行できます。このコマンドは、8.x および 9.0.x エージェントに IntroscopeAgent.profile で定義されたエージェントからコレクタへの接続があるときに使用します。

MOM は、コレクタに直接接続されているすべての 8.x および 9.0.x エージェントに関するランタイム情報を収集します。MOM は loadbalancing.xml の末尾に接続情報を挿入します。

重要: このコマンドは、MOM およびすべてのコレクタを 9.1.2 以降にアップグレードした後、エージェントをアップグレードする前に実行します。エージェントがアップグレードされた後にコマンドを実行すると、MOM は以前のエージェントからコレクタへの接続情報を収集できません。

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。

構文

```
autoprep prepare loadbalancing.xml
```

例

```
autoprep prepare loadbalancing.xml
```

エージェント A、B、C、D、E、F はすべてバージョン 8.x ~ 9.0.x です。以下の表に示すように、コレクタ 1、2、3 に接続するためにエージェントをその IntroscopeAgent.profile ファイルで設定します。

| エージェント名 | コレクタ名 |
|----------|---------|
| エージェント A | コレクタ 01 |
| エージェント B | コレクタ 01 |
| エージェント C | コレクタ 02 |
| エージェント D | コレクタ 02 |
| エージェント E | コレクタ 03 |
| エージェント F | コレクタ 03 |

この組織は、EPAgent2 という名前のエージェントを負荷分散するために loadbalancing.xml を使用します。

バージョン 8.x および 9.0.x のエージェントがすべて起動および動作している状態で、管理者は autoprep prepare loadbalancing.xml CLW コマンドを実行します。loadbalancing.xml ファイルには以下の例に太字で表示されているエントリが入力されます。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<loadbalancing xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="loadbalancing0.1.xsd">
  <agent-collector name="Example 1">
    <agent-specifier>.*¥|.¥|EPAgent2</agent-specifier>
    <exclude>
      <collector latched="false" port="5001" host="Collector02"/>
    </exclude>
  </agent-collector>
  <agent-collector name="Collector01@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentA</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentB</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector01"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector02@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentC</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentD</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector02"/>
    </include>
  </agent-collector>
  <agent-collector name="Collector03@5001 auto-generated configuration">
    <agent-specifier>HostName|ProcessName|AgentE</agent-specifier>
    <agent-specifier>HostName|ProcessName|AgentF</agent-specifier>
    <include>
      <collector latched="false" port="5001" host="Collector03"/>
    </include>
  </agent-collector>
</loadbalancing>
```

Example 1 は、管理者がコマンドを実行する前の、loadbalancing.xml のエンタリでした。MOM によって Example 1 の後に自動生成されたエンタリが追加されます。

出力

Loadbalancing.xml は、エージェントからコレクタへの接続エンタリで更新されます。

サンプル スクリプト

このセクションでは、CLW コマンドを使用するサンプル スクリプトを示します。

- [トランザクション追跡セッション](#) (P. 221)
- [アラートによって開始されるトランザクション追跡セッション](#) (P. 225)

これらのスクリプトはほかのスクリプト (`setlscEnv.cmd` および `configureWily.cmd`) を使用します。これらのスクリプトは、<http://wilycommunity.ca.com/entry.jspa@externalID=2103&categoryID=492.html> から入手できます。これらのスクリプトは、CLW の起動、シャットダウン、再起動、および使用を支援する *Useful Introscope Scripts* という、Community Developed Tool の一部です。適切な ZIP ファイルをダウンロードし、説明に従ってスクリプトをインストールします。

1. `scriptsBin.unix.zip` または `scriptsBin.win.zip` のいずれか適切なファイルをインストールされている Enterprise Manager に抽出します。このパッケージによって、`bin` というサブディレクトリが作成されます。
2. `bin` サブディレクトリに移動し、以下のいずれかを実行します。

```
.$configureScriptsEnv.cmd
```

または

```
./configureScriptsEnv.sh
```

3. これによって、`setlscEnv.cmd` または `setlscEnv.sh` というファイルが作成されます。このファイルには、ほかのスクリプトの読み込み元になる、関連する Introscope フォルダ ロケーションがすべて含まれています。

トランザクション追跡セッション

このスクリプトは、すべてのエージェントのトランザクション追跡セッションを開始します。実行時には、以下の 2 つの引数を指定します。

- 実行しきい値 - 追跡されるトランザクションの最小実行時間 (秒単位)。
- セッションの存続期間 - トランザクション追跡セッションの存続期間 (秒単位)。

スクリプトは、日付別に整理されたディレクトリ構造で結果を保存します。

名前

clwTxnTracer

構文

clwTxnTracer <しきい値> <期間>

各値は以下のとおりです。

*しきい値*はトランザクション実行時間のしきい値で、秒単位で指定します。

*期間*はセッションの存続期間で、秒単位で指定します。

例

clwTxnTracer 1 600

1 秒より長く実行されたすべてのトランザクションに対して、600 秒間のトランザクション追跡セッションが実行されます。

結果

トランザクション追跡データは、以下のように、現在の日付に対応するディレクトリ内の 1 つのファイルに書き込まれます。

```
<EM_Home>/traces¥<年>¥<月>¥<日>¥<エージェント>_<しきい値>secs_for<
継続時間>secs.<開始時刻>.xml
```

例 :

```
C:¥introscope¥traces¥2004¥11¥11¥AllAgents_1secs_for600secs.
14091705.xml
```

```
@ECHO OFFSETLOCAL
TITLE Introscope -- Transaction Tracer Session
```

```
REM ****
REM Sets the current working directory with quotes around it
REM This enables this file to execute correctly if it is
REM invoked somewhere other than its location.
REM ****
FOR /f "tokens=1 delims=" %%a in ('cd') DO SET PWD=%%a
```

```
REM ****
REM Set the command directory to the command argument itself,
REM namely the full path of this file or the relative path
REM to where the file was invoked.
SET CMD_DIR=%0
REM Now simply strip out the name of this file to get dir
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM      Use current filename
SET CMD_DIR=%CMD_DIR:clwTxnTracer.cmd=%
REM !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
REM Strip the quotes
REM add quotes if they're not there
SET CMD_DIR="%CMD_DIR%"
REM if not add quotes, then this statement chokes
SET CMD_DIR=%CMD_DIR:="=%
REM if the current dir wasn't determined, just set it to working dir
IF NOT EXIST "%CMD_DIR%" SET CMD_DIR=.
IF "%CMD_DIR%" == %0 SET CMD_DIR=.
IF "%CMD_DIR%" == "%0" SET CMD_DIR=.

REM ****
REM Now set the home directory for Introscope, and others
IF NOT EXIST "%CMD_DIR%\setIscEnv.cmd" goto noSetEnvFile
call "%CMD_DIR%\setIscEnv.cmd"

SET TT_THRESHOLD_IN_SECS=%1
SET TT_DURATION_IN_SECS=%2
IF "X%TT_THRESHOLD_IN_SECS%" == "X" SET TT_THRESHOLD_IN_SECS=10000
IF "X%TT_DURATION_IN_SECS%" == "X" SET TT_DURATION_IN_SECS=600
IF %TT_THRESHOLD_IN_SECS% LEQ 0 GOTO badArg
IF %TT_DURATION_IN_SECS% LEQ 0 GOTO badArg
SET TT_AGENTS=(.*)

REM Java Settings (e.g. increase Max heap size )
SET JAVA_OPTS=-Xms64m -Xmx512m
SET
JAVA_OPTS=%JAVA_OPTS% %CLW_USER_OPT% %CLW_PASSWORD_OPT% %CLW_EM_HOST_OPT% %CLW_EM
_PORT_OPT%
```

```
SET COMMAND=trace transactions exceeding %TT_THRESHOLD_IN_SECS% seconds in agents
matching ¥"%TT_AGENTS%¥" for %TT_DURATION_IN_SECS% seconds
```

```
SET AGENT_STR=%TT_AGENTS%
REM Remove the spaces, parentheses
SET AGENT_STR=%AGENT_STR:(=%
SET AGENT_STR=%AGENT_STR:)=%
SET AGENT_STR=%AGENT_STR:=%
if "X%TT_AGENTS%" == "X(.*)" SET AGENT_STR=AllAgents
FOR /f "tokens=1-4 delims=:" %a in ("%time%") DO SET SECS_STR=%a%b%c%d
FOR /f "tokens=1-4 delims=/ " %a in ("%date%") DO SET
TRACES_DIR=%ISC_TRACES%¥%d¥%b¥%c
```

```
REM Create the traces dir, if not exist
IF NOT EXIST "%TRACES_DIR%" MKDIR "%TRACES_DIR%"
SET
TT_FILE=%TRACES_DIR%¥%AGENT_STR%_%TT_THRESHOLD_IN_SECS%secs_for%TT_DURATION_IN_SE
CS%secs.%SECS_STR%.xml
```

```
TITLE Introscope -- Transaction Tracer for %TT_DURATION_IN_SECS% secs with
threshold %TT_THRESHOLD_IN_SECS% secs
REM send stderr to null b/c there are meaningless disconnect excepts that might be
*scary-looking*
ECHO Saving session output to %TT_FILE%
"%ISC_JAVA_HOME%¥bin¥java" %JAVA_OPTS% -jar "%CLW_JAR%" %COMMAND% > "%TT_FILE%"
2>NUL
goto finish
```

```
:badArg
ECHO Arguments should be greater than zero.
ECHO Syntax: $0 "threshold in secs" "duration in secs"
goto finish
```

```
:noSetEnvFile
ECHO There is no environment setup file: setIscEnv.cmd
ECHO Please re-run configureWily.cmd in installation directory!
goto finish
```

```
:finish
ENDLOCAL
```


アラートによって開始されるトランザクション追跡セッション

このスクリプトは、生成されているアラートの結果として、トランザクション追跡セッションを開始します。呼び出しには、シェルコマンドアクションを使用します。このとき、アラートメッセージテキストを引数として渡します。

スクリプトは、アラートメッセージテキストを解析して、アラートを生成したデータをレポートしたエージェント、および上回った危険レベルの値を検出します。これらをトランザクション追跡セッションのエージェントおよびしきい値として使用します。セッションの結果は、日付別に整理されたディレクトリ構造で保存されます。

名前

alert2TxnTracer

構文

シェルコマンドアクション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。

結果

トランザクション追跡データは、以下のように、現在の日付に対応するディレクトリ内の1つのファイルに書き込まれます。

```
<EM_Home>/traces¥<年>¥<月>¥<日>¥<エージェント>_<しきい値>secs_for<継続時間>secs.<開始時刻>.xml
```

例：

```
C:¥introscope¥¥traces¥2004¥11¥11¥AllAgents_1secs_for600secs.14091705.xml
```


第 10 章: WatchDog コマンドライン ツールの使用

信頼性とセキュリティのため、Enterprise Manager サーバを個別の WatchDog プロセスによって開始し、監視することができます。クロスプラットフォームの WatchDog コマンドラインツールを使用して、失敗した Enterprise Manager サーバの開始、停止、管理、および再起動を実行できます。

このセクションには、以下のトピックが含まれています。

[WatchDog の概要](#) (P. 227)

[WatchDog の実行](#) (P. 228)

[WatchDog コマンド](#) (P. 230)

[WatchDog コマンドオプション](#) (P. 234)

[WatchDog ログファイルの表示](#) (P. 240)

[サンプルスクリプト](#) (P. 240)

WatchDog の概要

WatchDog は、Enterprise Manager プロセスの開始、停止、および管理を行うクロスプラットフォーム コマンドラインツールです。また、このツールでは、既存の Enterprise Manager フェールオーバー機能をサポートするために、失敗した Enterprise Manager を再起動できます。

WatchDog コマンドラインツールは `<EM_Home>/bin` ディレクトリ内にあります。以下のいずれかの方法でコマンドを呼び出すことができます。

- `WatchDog.bat` または `WatchDog.sh` ヘルパーの使用
- `WatchDog.jar` から Java アプリケーションを直接実行する。この方法のほうが多くのオプションを指定できますが、複雑さも増します。たとえば、WatchDog プロセスを `watch` モードに設定して Enterprise Manager を起動するには、bin ディレクトリから「`WatchDog watch`」と入力します。

注: WatchDog を使用するには、JRE 1.6 が必要です。

すべての WatchDog コマンドは、結果コードと共にコマンドウィンドウまたはシェルに制御を返します。WatchDog は実際には 2 つのプログラムで構成されています。

- **WatchDog マネージャ**

コマンドラインからラインを受け取り、さまざまなアクションを実行して、結果を返します。

- **WatchDog サーバプロセス**

Enterprise Manager の稼働状況を監視し、停止した Enterprise Manager を自動的に再起動します。

注: WatchDog 以外のメカニズムでも Enterprise Manager を起動できるため、*start* コマンドは Enterprise Manager が起動中であるかどうかを常に認識できるわけではありません。このため、Enterprise Manager が WatchDog に認識されずに起動した直後に WatchDog を呼び出すと、2 つ目の Enterprise Manager インスタンスの起動が試行されます。Enterprise Manager の 2 回目の起動試行は失敗しますが、エラー結果は返されません。これは、発行されたコマンドが *start* のみであるためです。エラーは、`<EM_Home>/logs` 内にある Enterprise Manager ログ ファイルに記録されます。

結果的には、最初の WatchDog *start* コマンドの試行が成功し、WatchDog によって *running* コマンドが返されます。

WatchDog の実行

WatchDog の結果コードを表示するには、Windows コマンドプロンプトまたは UNIX シェルを使用します。

WatchDog.bat または WatchDog.sh を使用して WatchDog を実行する方法

1. Windows コマンドプロンプトまたは UNIX シェルを開きます。
2. Windows で `<EM_Home>%bin` に、または UNIX で `<EM_Home>/bin` に移動します。
3. `WatchDog<コマンド>` と入力します。<コマンド> は、*start*、*watch*、*stop*、*status*、*help* のいずれかです。コマンドの詳細については、「[WatchDog コマンド \(P. 168\)](#)」を参照してください。

WatchDog.jar を直接呼び出して WatchDog を実行する方法

1. Windows コマンドプロンプトまたは UNIX シェルを開きます。
 2. Windows で `<EM_Home>%bin` に、または UNIX で `<EM_Home>/bin` に移動します。
 3. オペレーティング システムに応じて、以下のコマンドを入力します。
 - Windows
`..%jre%bin%java -jar WatchDog.jar コマンド[-オプション]`
 - UNIX
`../jre/bin/java -jar WatchDog.jar コマンド[-オプション]`
- コマンドの詳細については、「[WatchDog コマンド \(P. 168\)](#)」を参照してください。

SAP での WatchDog の実行

SAP 環境で実行されている Enterprise Manager 上で WatchDog を使用する場合、WatchDog を使用できるようになるために、管理者クレデンシャルの入力を求められます。

SAP 環境内の Enterprise Manager で WatchDog コマンドを実行する方法

- Enterprise Manager 管理者ユーザ ID およびパスワードを入力し、次に進みます。

WatchDog コマンド

WatchDog コマンドは、4つの基本機能に対応しています。

- Enterprise Manager プロセスの開始および再起動 - 「[WatchDog start コマンド](#) (P. 231)」を参照してください。
- Enterprise Manager プロセスの停止 - 「[WatchDog stop コマンド](#) (P. 232)」を参照してください。
- Enterprise Manager のステータスの確認 - 「[WatchDog status コマンド](#) (P. 233)」を参照してください。

コマンドを入力する際、2つの構文のいずれかを使用します。

- 基本：Windows では *WatchDog.bat* ヘルパスクリプトを、UNIX では *WatchDog.sh* ヘルパスクリプトを使用することで、簡略化されています。
- 完全： *WatchDog.jar* Java アプリケーションを直接呼び出し、すべての WatchDog オプションが使用可能になります。

WatchDog は、コマンドライン上で、`java -jar WatchDog.jar コマンド [-オプション]` を使用して制御されます。

すべてのコマンドは、2つの結果コードを返します。

- 1つは Enterprise Manager 用です。
- もう1つは WatchDog の自動再起動機能用です。

WatchDog 結果コードは先頭に *wd* が付いています。

WatchDog start コマンド

`start` コマンドは、Enterprise Manager プロセスを開始しますが、Enterprise Manager プロセスを起動する既存のコマンドに依存します。

Enterprise Manager を起動するには、WatchDog 機能の自動再起動を指定して WatchDog を使用するか、基本構文を使用します。基本構文を使用する場合、Windows では *Introscope Enterprise Manager.exe*、UNIX では *Introscope_Enterprise_Manager* がデフォルトで指定されているので、`start` コマンドを指定する必要はありません。`watch` コマンドを使用すると、WatchDog サーバが `watch` モードになります。これによって、WatchDog サーバは Enterprise Manager が実行を停止しているかどうかを定期的に確認し、必要に応じて Enterprise Manager を再起動します。

完全な構文を使用して、`start` コマンドを `-watch` コマンドオプションと組み合わせて入力すると、WatchDog が `watch` モードになります。

注: WatchDog は同期プロセスである (何も待たずに結果を返す) ため、`start` または `stop` コマンドを入力した後に得られる可能性のある結果は、`startcommandissued` および `stopcommandissued` のみです。これらの結果は、単にコマンドが発行されたことを意味し、実際に Enterprise Manager が開始または停止したことを示していません。Enterprise Manager ログを確認するか、オペレーティングシステムのプロセスを確認するのが確実です。

start コマンド構文

このセクションでは、WatchDog `start` コマンド用の構文について説明します。

基本構文

WatchDog の開始

WatchDog `watch`

完全な構文

```
..%jre%bin%java -jar WatchDog.jar start -startcmd <コマンド>
```

```
..%jre%bin%java -jar WatchDog.jar start -watch -startcmd <コマンド>
```

Enterprise Manager の戻り値

startcommandissued - Enterprise Manager は実行されていません。

alreadyrunning - Enterprise Manager はすでに実行されています。

starting - Enterprise Manager は起動中です。

starterror - Enterprise Manager の起動の試行中にエラーが発生しました。

WatchDog の戻り値

wdstartedwatching - WatchDog は監視モードになっています。

wdalreadywatching - WatchDog はすでに実行中です。

wdstartedsleeping - WatchDog サーバプロセスは実行されていますが、監視モードではありません。

wdalreadysleeping - WatchDog はすでにスリープモードです。

WatchDog stop コマンド

WatchDog stop コマンドは、Enterprise Manager および WatchDog のサーバプロセスに対して *stop* コマンドを発行します。WatchDog は *watch* モードで実行されている可能性があるため、Enterprise Manager を確実に停止し、停止状態を維持するには、このコマンドが最善の方法です。

stop コマンド構文

このセクションでは、WatchDog stop コマンド用の構文について説明します。

基本構文

```
WatchDog stop
```

完全な構文

```
..¥jre¥bin¥java -jar WatchDog.jar stop
```


Enterprise Manager の戻り値

stopcommandissued - Enterprise Manager は実行されています。

alreadystopped - Enterprise Manager は実行されていません。

stoperror - Enterprise Manager の停止の試行中にエラーが発生しました。

WatchDog の戻り値

wdstopped - WatchDog は停止しました。

wdstopcommandissued - WatchDog は実行されています。

WatchDog status コマンド

status コマンドは、Enterprise Manager および WatchDog ステータスをレポートします。

status コマンド構文

このセクションでは、WatchDog status コマンド用の構文について説明します。

基本構文

WatchDog ステータス

完全な構文

```
..¥jre¥bin¥java -jar WatchDog.jar status
```

Enterprise Manager の戻り値

running - Enterprise Manager は実行されています。

stopped - Enterprise Manager は実行されていません。

starting - Enterprise Manager は起動中です。

statusunknown - Enterprise Manager のステータスは不明です。

WatchDog の戻り値

wdwatching - WatchDog は実行されています。

wdsleeping - WatchDog サーバ プロセスは実行されています (WatchDog によって Enterprise Manager が起動される場合と同様) が、監視モードではありません。

wdstopped - WatchDog は実行されていません。

WatchDog コマンド オプション

WatchDog では、基本構文では利用できない高度なオプションを用意しています。基本構文を使用している場合は、これらのオプションはそれぞれのデフォルト値が使用されます。

コマンド オプションは *start* コマンドのみに適用されます。ただし、*-port* コマンド オプションはすべてのコマンドで使用できます。

コマンド オプションは、以下のとおりです。

- [WatchDog -watch コマンド オプション](#) (P. 235)
- [WatchDog -port コマンド オプション](#) (P. 236)
- [WatchDog -startcmd コマンド オプション](#) (P. 236)
- [WatchDog -interval コマンド オプション](#) (P. 237)
- [WatchDog -startuptime コマンド オプション](#) (P. 238)
- [WatchDog -jre コマンド オプション](#) (P. 238)

WatchDog -watch コマンド オプション

-*watch* コマンド オプションは *start* コマンドと一緒にしか使用できません（「[WatchDog start コマンド \(P. 231\)](#)」を参照）。このオプションは、Enterprise Manager の自動再起動機能を有効にする唯一の方法です。

Enterprise Manager の起動後、*watch* 機能をオンまたはオフにすることができます。たとえば、WatchDog が *watch* モードになっていない状態で Enterprise Manager を実行している場合、-*watch* オプションと共に *start* コマンドを使用することで、WatchDog サーバを *watch* モードにすることができます。同様に、Enterprise Manager がすでに実行されていても、-*watch* オプションを付けずに *start* コマンドを使用すると、WatchDog の *watch* モードを解除できます。

-*watch* オプションと共に *start* コマンドを使用したときの戻り値は以下のとおりです。

- *startedwatching* - コマンドが入力されるまで、WatchDog は監視していませんでした。現在は監視中です。
- *alreadywatching* - コマンドが入力されるまで、WatchDog はすでに監視していました。現在も監視を継続しています。

-*watch* オプションを指定せずに *start* コマンドを使用したときの戻り値は以下のとおりです。

- *startedsleeping* - コマンドが入力されるまで、WatchDog はスリープ状態ではありませんでした。現在は監視を停止しています。
- *alreadysleeping* - コマンドが入力されるまで、WatchDog はすでにスリープ状態でした。現在は引き続き監視を停止しています。

-*watch* コマンド オプションの例:

```
<EM_Home>%bin>..%jre%bin%java -jar WatchDog.jar start -watch -startcmd  
"..%Introscope Enterprise Manager.exe"  
WatchMgr: iPort = 4321; watch = true; startcmd = ..%Introscope Enterprise Manager.exe;  
startcommandissued & wdstartedwatching
```

WatchDog -port コマンド オプション

`-port` オプションは、WatchDog のサーバ ポートの値を指定する際に使用します。値を入力しない場合は、デフォルト値 **4321** が使用されます。

最初の WatchDog `start` コマンドで `-port` 値を指定すると、以後のコマンドですべて同じ値が使用されます。

注: 別の方法として、`WatchDog.bat` ファイルを変更するか、新しいバッチファイルを作成することで、デフォルト以外のポートで WatchDog サーバを実行できます。これによって、すべてのコマンドで適切なポートが確実に WatchDog マネージャに渡されます。

`-port` コマンド オプションの例:

```
<EM_Home>%bin>..%jre%bin%java -jar WatchDog.jar
start -port 5555 -startcmd "..%Introscope Enterprise Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..%Introscope Enterprise
Manager.exe;
alreadyrunning & wdaalreadysleeping
```

WatchDog -startcmd コマンド オプション

このオプションは、Enterprise Manager を起動するコマンドを指定する際に使用します。

注: このコマンド オプションは `start` コマンドのみに適用されます。詳細については、「[WatchDog start コマンド \(P. 231\)](#)」を参照してください。

WatchDog -interval コマンド オプション

interval オプションを使用して、Enterprise Manager が停止しているかどうかを確認するための Enterprise Manager ステータス確認を実行する間隔を秒単位で指定します。このオプションが指定されない場合に使用されるデフォルト値は 10 秒です。

このオプションは、WatchDog のステータスが *watching* の場合に適用されます。

注: このコマンド オプションは *start* コマンドのみに適用されます。詳細については、「[WatchDog start コマンド \(P. 231\)](#)」を参照してください。

-interval コマンド オプションの例:

```
C:\Program Files\CA\Wily\Introscope9.0d140\bin>..%jre%\bin\java -jar WatchDog.jar
start -watch -interval 300 -startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 4321; watch = true; startcmd = ..\Introscope Enterprise Manager.exe;
startcommandissued & wdstartedwatching
```

WatchDog -startuptime コマンド オプション

このオプションを使用して、WatchDog に Enterprise Manager の起動を許可する時間を秒単位で指定します。WatchDog が Enterprise Manager を起動した後、このオプションに指定された時間が経過すると、Enterprise Manager のステータスが *starting* に変わります。これにより、Enterprise Manager ステータスを判別するよう構成されたメカニズムが、正常に機能します。

Enterprise Manager ステータス確認は Enterprise Manager の起動直後に実行されるため、*running* ステータスが返されません。そこで代替として、WatchDog が Enterprise Manager を起動した後の数秒間は、WatchDog の *status* コマンドに対して、*starting* ステータスが返されます。この機能によって、意図せず WatchDog が 2 つの Enterprise Manager インスタンスを起動することを防げます。

-startuptime オプションは、この遅延をデフォルト値 (30 秒) 以外の値に設定する際に使用します。

注: このコマンド オプションは *start* コマンドのみに適用されます。詳細については、「[WatchDog start コマンド \(P. 231\)](#)」を参照してください。

-startuptime コマンド オプションの例:

```
<EM_Home>%bin>..%jre%bin%java -jar WatchDog.jar start -watch -startuptime 60
-startcmd ".%Introscope Enterprise Manager.exe"
WatchMgr: iPort = 4321; watch = true; startcmd = ..%Introscope Enterprise Manager.exe;
startcommandissued & wdstartedwatching
```

WatchDog -jre コマンド オプション

このオプションを使用して、JRE がデフォルト ディレクトリの *jre/bin/java* 内がない場合に JRE パスを指定します。

-jre コマンド オプションの例:

```
C:%Program Files%Java%jre1.6.0_07%bin%java" -jar WatchDog.jar start -watch -jre
"C:%Program Files%Java%jre1.6.0_07%bin%java" -startcmd ".%Introscope Enterprise
Manager.exe"
startcommandissued & wdstartedwatching
```

WatchDog -emport コマンド オプション

`-emport` オプションを使用して、Enterprise Manager がデフォルト ポート 5001 以外のポート番号で実行されている場合に Enterprise Manager のサーバ ポートの値を指定します。Enterprise Manager がデフォルト ポート 5001 以外のポート番号で実行されている場合、このコマンドは必須です。

`-emport` コマンド オプションの例:

```
C:\Program Files\CA\Wily\Introscope9.0\bin>..%jre%bin%java -jar WatchDog.jar
start -emport 5003 -startcmd "..\Introscope Enterprise Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

WatchDog -emuser コマンド オプション

`-emuser` オプションは、Enterprise Manager がデフォルトの *Admin* 以外のユーザ名で構成されている場合に使用します。Enterprise Manager がデフォルトの *Admin* 以外のユーザ名で構成されている場合、このコマンドは必須です。

また、`-emuser` オプションは、`-empwd` オプションと共に使用してください。

`-emuser` コマンド オプションの例:

```
<EM_Home>%bin>..%jre%bin%java -jar WatchDog.jar
start -emuser EMUserName -empwd EMPasswd -startcmd "..\Introscope Enterprise
Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..\Introscope Enterprise
Manager.exe;
alreadyrunning & wdalreadysleeping
```

WatchDog -empwd コマンド オプション

-empwd オプションは、Enterprise Manager がデフォルトの "" 以外のパスワードで構成されている場合に使用します。

Enterprise Manager がデフォルトの "" 以外のパスワードで構成されている場合、このコマンドは必須です。

また、-empwd オプションは、-emuser オプションと共に使用してください。

-empwd コマンド オプションの例:

```
<EM_Home>%bin>..%jre%bin%java -jar WatchDog.jar
start -emuser EMUserName -empwd EMPassWord -startcmd "..%Introscope Enterprise
Manager.exe"
WatchMgr: iPort = 5555; watch = false; startcmd = ..%Introscope Enterprise
Manager.exe;
alreadyrunning & wdaIreadySleeping
```

WatchDog ログ ファイルの表示

WatchDogServer プロセス ログ ファイルは WatchDog.log ファイルに書き込まれます。

WatchDog ログ ファイルを表示する方法

1. <EM_Home>/logs に移動します。
2. WatchDog.log ファイルを開きます。

サンプル スクリプト

WatchDog.bat と WatchDog.sh では、Windows および UNIX プラットフォームの基本的な構文が採用されています。これらのスクリプトは、WatchDog の完全な構文を簡略化するカスタム スクリプト開発の出発点としても有用です。WatchDog.bat と WatchDog.sh は、Windows および UNIX のインストールの <EM_Home>/bin ディレクトリ内にあります。

第 11 章: WebView オプションの設定

このセクションには、以下のトピックが含まれています。

[WebView アプリケーション コンテキストパスの設定 \(P. 241\)](#)

[APM WebView のパフォーマンスの設定および監視方法 \(P. 242\)](#)

WebView アプリケーション コンテキストパスの設定

オプションで、WebView インストールのアプリケーション コンテキストパスを構成できます。このパスは、WebView のホストの完全修飾名およびポート番号の最後に追加され、WebView にアクセスするための URL を形成します。この機能を使用して、ユーザが WebView のアプリケーション名を定義できます。

コンテキストパスを使用せずに WebView にアクセスする方法

- 以下の URL を使用します。

`http://<サーバ名>:<ポート番号>`

コンテキストパスが構成されている場合に、WebView にアクセスする方法

- 以下の URL を使用します。

`http://<サーバ名>:<ポート番号>/<コンテキストパス>/`

たとえば、コンテキストパスが `webview` に定義されていて、`introscope.webview.tcp.port` プロパティがデフォルト値の `8080` に設定されている場合は、以下の URL で WebView にアクセスします。

`http://<サーバ名>:8080/webview/`

WebView のコンテキストパスは、WebView プロパティファイルの `introscope.webview.context.path` プロパティを使用して構成します。詳細については、「[introscope.webview.context.path \(P. 597\)](#)」を参照してください。コンテキストパスプロパティの定義後、WebView を再起動します。

APM WebView のパフォーマンスの設定および監視方法

注: SAP WebView ユーザは、APM UI Performance Monitor を利用できません。

APM UI Performance Monitor は、WebView アプリケーションのパフォーマンスメトリックを収集およびレポートします。管理者はこの情報を使用して、ユーザに影響が及ぶ前に潜在的な WebView のパフォーマンス問題を検出して分離します。たとえば、パフォーマンスの問題は、ハードウェアリソースが不足している場合やあまりに多くのセッションが同時に使用されている場合（特に大規模なデータビューと共に使用されている場合）に発生する可能性があります。

WebView サーバのインストールでは Java エージェントが展開されます。有効になっている場合、組み込みの Java エージェントはサーバコンポーネントとハードウェアリソースを監視します。また、収集されたメトリックは、Enterprise Manager にレポートされます。Enterprise Manager はデータを受け取ると、リアルタイムおよび履歴レポートのためにデータを処理して保存します。収集されたデータは、WebView の以下のサンプルダッシュボードに表示されます。

- [WebView - 概要](#) (P. 249)
- [WebView - マップおよびウィジェット](#) (P. 250)
- [WebView - リソース](#) (P. 251)

以下の図に、管理者として APM UI Performance Monitor を設定および使用する方法を示します。

APM UI のパフォーマンスの設定および監視方法



管理者

前提条件の確認

APM UI Performance Monitor の設定

WebView UI の
パフォーマンスの監視

設定の確認

- 前提条件の確認
- [APM UI Performance Monitor を設定します](#) (P. 246)。
- [設定を確認します](#) (P. 247)。
- [WebView UI のパフォーマンスを監視します](#) (P. 248)。
- (オプション) [WebView メトリック グループを設定します](#) (P. 251)。
- (オプション) [ダッシュボードデータを表示および解釈します](#) (P. 252)。

前提条件の確認

前提条件は以下のとおりです。

1. 以下のコンポーネントとそのディレクトリ（およびファイル）が構成に存在することを確認します。
 - Java エージェント。
`<WEBVIEW_HOME>/products/webview/agent`
 - エージェントのオペレーション、メトリックデータの収集、およびインスツルメンテーション処理を制御するための `WebView Probebuilder` ディレクティブ ファイル (`WebView.pbd`)。
`<WEBVIEW_HOME>/products/webview/agent/wily/core/config`
2. Java エージェントの `IntroscopeAgent.profile` ファイルを以下の手順で設定します。
 - a. `<INSTALL_HOME>/product/webview/agent/wily/core/config` に移動し、テキストエディタで `IntroscopeAgent.profile` を開きます。
 - b. `introscope.autoprobe.directivesFile` を検索し、`WebView.pbd` がプロパティ値の最後に追加されていることを確認します。
 - c. `introscope.agent.defaultProcessName` を検索し、プロパティ値が `APM WebView` であることを確認します。この値を変更または削除しないでください。
 - d. `introscope.agent.agentName` を検索し、プロパティ値が `APM.WebView` であることを確認します。

設定が完了しました。

APM UI Performance Monitor の設定

Java エージェントに APM UI Performance Monitor コンポーネントを設定します。2 つあるインストール オプションのいずれかを使用します。

- Enterprise Manager : `<EM_HOME>/product/webview`
- WebView サーバ スタンドアロン : `<WEBVIEW_HOME>/product/webview`

以下の手順は両方のインストールに適用されます。

以下の手順に従います。

1. `<INSTALL_HOME>` ディレクトリから、テキスト エディタで `Introscope_WebView.lax` ファイルを開きます。

2. 以下のプロパティを検索します。

```
lax.nl.java.option.additional
```

このプロパティのコメント行は、以下の例のようになります。

```
# Introscope Java Agent Arguments for WebView Monitor
# -XX:PermSize=128m -XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily
-Djetty.home=.
```

3. "#" を除く引数を行からコピーして、`lax.nl.java.option.additional` プロパティ値に追加します。

結果は以下の例のようになります。

```
lax.nl.java.option.additional=-Xms256m -Xmx1024m
-Djava.awt.headless=false
-Dorg.owasp.esapi.resources=./config/esapi
-Dsun.java2d.noddraw=true
-Dintroscope.webview.testpanel.enable=false
-Dintroscope.webview.saas.enable=false
-XX:PermSize=128m
-XX:MaxPermSize=256m
-javaagent:./product/webview/agent/wily/Agent.jar
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily
-Djetty.home=.
```

注: ファイル内の値はこの例とは異なる場合があります。

変更を保存します。

4. **WebView.jar** ファイルをコピーして、**WebView Monitor** 管理モジュールを展開します。コピー元の *modules* フォルダ :

```
<EM_HOME>/examples/WebViewMonitor/config/modules
```

コピー先の *deploy* フォルダ :

```
<INSTALL_HOME>/deploy
```

WebView サーバを再起動して設定を完了します。

5. (オプション) **Windows** のみ : **WebView** アプリケーションを開始するために **Windows** サービスを作成した場合、サービスの開始時に開始する **APM UI Performance Monitor** を以下のように設定できます。

- a. `<INSTALL_HOME>/bin` ディレクトリに移動し、テキスト エディタで `WVService.conf` ファイルを開きます。

- b. `# Java Additional Parameters` の下の以下のセクションを見つけます。

```
#wrapper.java.additional.4=-XX:PermSize=128m -XX:MaxPermSize=256m
```

```
-javaagent:./product/webview/agent/wily/Agent.jar
```

```
-Dcom.wily.introscope.agentProfile=./product/webview/agent/wily/core/config/IntroscopeAgent.profile
```

```
-Dcom.wily.introscope.wilyForWilyPrefix=com.wily -Djetty.home=.
```

- c. この文字列の先頭にある、これらのパラメータをコメント化するための「#」を削除します。

変更を保存します。

Windows サービスを再起動して設定を完了します。

設定の確認

設定が正しいことを確認します。

以下の手順に従います。

1. **WebView** で、**[Investigator]** - **[メトリック ブラウザ]** をクリックします。
2. 以下のように、**APM.WebView** に移動します。
`<DomainName>|<WebViewHostName>|APM Introscope WebView|APM.WebView`
3. 標準メトリックを表示し、**Enterprise Manager** にデータをレポートしていることを確認します。

4. [コンソール] タブをクリックし、以下のサンプル ダッシュボードが [ダッシュボード] ドロップダウン リストに表示されることを確認します。
 - [WebView - 概要](#)
 - [WebView - マップおよびウィジェット](#)
 - [WebView - リソース](#)
 5. [WebView - 概要] サンプル ダッシュボードを開き、以下のタスクを実行します。
 - データ ビューアのグラフを右クリックします。 [リンク] ドロップダウンリストから、 [管理モジュール] 内の対応するメトリックに移動します。
 - グラフからヒントを開き、リンクをクリックして、メトリック ブラウザ ツリーの対応するメトリックに移動します。
- 設定が確認されました。

WebView UI のパフォーマンスの監視

APM UI Performance Monitor のサンプル ダッシュボードには、WebView アプリケーションの状態監視および問題解決機能があります。パフォーマンスの問題を視覚的に通知できます。たとえば、ダッシュボードには、以下の情報を持つ棒グラフが表示されます。

- 3000 ミリ秒の警告しきい値を示す黄色のライン
- 4000 ミリ秒の危険しきい値を示す赤色のライン

以下の手順に従います。

1. [WebView](#) の [コンソール] タブで、ドロップダウン リストから [WebView](#) 監視のサンプル ダッシュボードを選択します。
 - [WebView - 概要](#) (P. 249)
 - [WebView - マップおよびウィジェット](#) (P. 250)
 - [WebView - リソース](#) (P. 251)
- ダッシュボードが開き、現在のパフォーマンス ステータスが表示されます。棒グラフには、現在のデータ値が水平方向の棒で表示されます。
2. [標準メトリック](#) (P. 254) を分析します。

3. ダッシュボードに示されたデータに関してより詳細な情報を必要とする場合は、以下のショートカットを使用します。
 - ハイパーリンクを持つダッシュボードオブジェクトの上にマウスカーソルを合わせます。すると、ポインタが手の形に変わります。オブジェクトのデフォルト ターゲットへのリンクに移動するには、オブジェクトをクリックします。
 - データ ビューア内のダッシュボードオブジェクトを右クリックします。すると、ポインタが手の形に変わります。 [リンク] ドロップダウンリストから、管理モジュール内の対応するオブジェクトに移動します。データ ビューアが、基となるメトリックグループに自動的にリンクされます。
 - エレメントの上にマウスカーソルを合わせて、ヒントを表示します。ヒントは、 [問題切り分けマップ] タブと [メトリックブラウザ] タブの両方に存在する階層ツリーおよび [ビューア] ペイン内のメトリックパスおよび値を識別します。 ツリー内のメトリックを表示するには、ヒント内のハイパーリンクをクリックします。
4. 時間範囲を選択して、[さまざまな時点のデータを表示します](#) (P. 253)。
5. [Average Response Time](#) (P. 255) をほかのメトリックの変化と組み合わせて、傾向を分析し、問題を識別および診断します。

注: WebView コンソールのダッシュボードでは、すべての情報が表示されますが、編集はできません。ダッシュボードを作成して編集するには、Workstation を使用します。

[WebView - 概要]ダッシュボード

[WebView - 概要] ダッシュボードは、管理者が環境全体にわたって WebView アプリケーションのパフォーマンスを監視するために設計されています。

グラフには、WebView アプリケーションおよびクライアントとサーバ間の相互動作に関する高度な情報が表示されます。

このダッシュボードには以下のグラフがあります。

WebView フロントエンド

WebView の監視対象アプリケーションのフロントエンドの稼働状況メトリックが表示されます。Average Response Time をほかのメトリックの変化と組み合わせて、傾向を分析することで、パフォーマンスの問題を識別し、診断します。

アクティブ ブラウザ

サーバに接続しているブラウザが表示されます。

アクティブ サービス

サブスクリプションマネージャに接続しているサービスが表示されます。

間隔ごとのクライアント要求数(15 秒)

間隔ごとのクライアントからの要求数が表示されます。

[WebView - マップおよびウィジェット]ダッシュボード

[WebView - マップおよびウィジェット] ダッシュボードは、管理者が問題切り分けマップと SOA 依存マップのパフォーマンス、および WebView の稼働状況メトリックを監視するために設計されています。

グラフには、これらのマップとウィジェットの全般的な稼働状況およびパフォーマンスが表示されます。

注: [Investigator] - [問題切り分けマップ] 内のビジネス サービスおよびフロントエンドに移動するまで、データは [問題切り分けマップ] グラフに表示されません。

このダッシュボードには以下のグラフがあります。

問題切り分けマップおよび SOA 依存マップの稼働状況

ビジネス サービスおよびフロントエンドの稼働状況メトリックは、APM Introscope WebView エージェントの [JSP] ノードの下に表示されます。

アクティブ ウィジェット数

アクティブなウィジェット数が表示されます。

間隔ごとのアクティブ ウィジェット数

間隔ごとのアクティブなウィジェット数が表示されます。

問題切り分けマップ ロード時間(ミリ秒)

問題切り分けマップのロード時間 (ミリ秒) が表示されます。

[WebView - リソース]ダッシュボード

[WebView - リソース]ダッシュボードは、管理者がフロントエンド I/O およびホスト リソースを監視するために設計されています。

グラフには、WebView リソースの全般的な稼働状況およびパフォーマンスが表示されます。

このダッシュボードには以下のグラフがあります。

フロントエンド I/O

フロントエンドソケット I/O の入出力帯域幅 (バイト/秒) およびフロントエンドソケット I/O の同時性が表示されます。

ホストリソース

プロセス CPU とホスト CPU の使用率の対比、サーバメモリの使用量と割り当て量の対比が表示されます。

WebView メトリック グループの設定

[WebView - リソース]ダッシュボードでは、WebView メトリック グループは、以下の情報を保存する管理モジュールオブジェクトです。

- エージェント一致パターン -- エージェント名の一部またはすべてを含むデータを指定することにより、メトリックへの入力をフィルタする Perl 5 の正規表現。
- メトリック一致パターン -- リソース (メトリックに至るまでの一連のフォルダ) およびメトリックを指定する Perl 5 の正規表現。

エージェント一致パターンのデフォルト エージェント プロセス名またはデフォルト エージェント名を変更する場合は、いくつかの追加手順を実行する必要があります。

以下の手順に従います。

1. **WebView** で [管理] タブをクリックし、[WebView 監視] メトリックグループを見つけます。
2. 更新する [WebView - リソース] ダッシュボードメトリックグループを見つけます。たとえば、[フロントエンド I/O]、[プロセスおよびホスト CPU]、[フロントエンド I/O 同時実行]、[ヒープサイズ]、および [割り当て] などです。
3. エージェント一致パターンのプロセス名の値 (APM Introscope **WebView**) またはエージェント名の値 (APM.**WebView**) を編集します。
4. 変更を保存します。
5. Java エージェントの *IntroscopeAgent.profile* をテキストエディタで開きます。
6. *introscope.agent.defaultProcessName* プロパティまたは *introscope.agent.agentName* プロパティを検索します。
7. 手順 3 で指定したものと同名前の値を入力します。
8. 変更を保存します。
設定が完了しました。

ダッシュボードデータの表示および解釈

ダッシュボードデータは、さまざまな方法で表示および解釈できます。

- [さまざまな時点のデータの表示](#) (P. 253)。
- [標準メトリックの表示](#) (P. 254)。
- [Average Response Time の傾向の解釈](#) (P. 255)。

さまざまな時点のデータの表示

ライブ データを表示できます。また、時間範囲を選択して、さまざまな時点のデータを表示できます。データのデフォルトのビューは [ライブ] です。

ブラウザの上部にある [時間ウィンドウ] を確認することで、WebView がライブ モードであるかどうかを確認できます。

ダッシュボードでさまざまな時点を表示するには、以下のタスクを実行します。

- [履歴データの表示](#) (P. 253)。
- [カスタム時間範囲の定義](#) (P. 254)。

履歴データの表示

アプリケーションを監視する場合、ライブ データ ビューが変化し、常に最新のデータが表示されます。ライブ データはデフォルト ビューです。時間範囲を選択すると、履歴データを表示できます。履歴データでは、問題が発生した時刻を特定できます。

以下の手順に従います。

1. WebView の [コンソール] タブで、[ダッシュボード] ドロップダウンリストから履歴データを表示するダッシュボードを選択します。
2. [時間ウィンドウ] ドロップダウンリストから、履歴ビュー用の時間範囲（[24 時間] など）を選択します。
選択した時間範囲（[24 時間] など）を使用して、その範囲のダッシュボードのデータが表示されます。終了時刻は現在の時刻に設定されます。
3. 開始時刻を変更する場合は、[時間ウィンドウ] の横にある進む矢印および戻る矢印をクリックします。
4. 範囲の終了時刻を現在時刻にリセットするには、[今すぐ終了] をクリックします。

カスタム時間範囲の定義

コンソール内のデータを表示するカスタム時間範囲を定義できます。

以下の手順に従います。

1. 履歴データを表示する対象となるメトリックまたはダッシュボードを選択します。
2. [時間ウィンドウ] ドロップダウンリストから [カスタムの範囲] を選択します。
3. [カスタムの範囲] ウィンドウが開き、現在の日付 (今日) がシルエットで強調された状態で表示されます。
4. カレンダー コントロールを使用して開始日と終了日を選択します。
5. [OK] をクリックします。

カスタム範囲のデータが設定されます。

標準メトリック

WebView は、エージェントがメトリックとしてリモートおよびローカルシステムから収集するアプリケーションパフォーマンス データを表示します。監視対象のフロントエンドおよびバックエンドのアプリケーション コンポーネント、およびその他の多くのアプリケーション コンポーネントについては、以下の標準メトリックが表示されます。

- **Average Response Time (ms)** (平均応答時間 (ミリ秒)) : 基準となるアプリケーション応答速度。
- **Concurrent Invocations** (同時進行中の呼び出し) : 一定の時間に処理される要求の数。
- **Errors Per Interval** (間隔ごとのエラー数) : 指定したタイム スライス内に発生するエラーの数。
- **Responses Per Interval** (間隔ごとの応答数) : 指定したタイム スライス内に完了する要求の数。
- **Stall Count** (ストール数) : ストールの数。ストールは、指定した時間しきい値内に完了しなかった要求です。

Average Response Time の傾向

Average Response Time をほかのメトリックの変化と組み合わせて、傾向を分析することで、問題を識別し、診断できます。詳細については以下の表を参照してください。

| Average Response Time の傾向 | 定義 |
|---------------------------|--|
| 一貫した問題 | <p>Available Thread Count の値が低く、Average Response Time の値が一貫して高い場合は、以下の問題を示している可能性があります。</p> <ul style="list-style-type: none">■ 非効率なコード■ 外部システムの過剰使用■ バックエンドが遅い■ レイヤが多すぎる <p>一貫した問題が常に存在し、改善することも悪化することはありません。</p> |
| 定期的な問題 | <p>Average Response Time が定期的 to 高くなり、定期的 to 急増した後、通常に戻るといようなグラフで示されます。</p> <p>Available Thread Count の値が低く、Average Response Time の値が定期的 to 高くなる場合は、以下の問題を示している可能性があります。</p> <ul style="list-style-type: none">■ GC リークが頻繁に発生■ 負荷に関連するバックエンドのボトルネック <p>CPU Utilization の値が低く、Average Response Time の値が定期的 to 高くなる場合は、以下の問題を示している可能性があります。</p> <ul style="list-style-type: none">■ 内部問題 <p>定期的な問題が発生し、一定の間隔で収まります。</p> |
| 段階的な問題 | <p>Average Response Time が長期にわたって着実に増加しており、Responses Per Interval の値が低い場合は、以下の問題を示している可能性があります。</p> <ul style="list-style-type: none">■ メモリ リーク <p>段階的な問題は時間と共に減少します。</p> |

第 12 章: Workstation の構成

この章では、Introscope Workstation のオプションの動作を設定する方法について説明します。

このセクションには、以下のトピックが含まれています。

[冗長モードでの Workstation の実行 \(P. 257\)](#)

[Workstation の出力のファイルへのリダイレクト \(P. 258\)](#)

[ログイン値を指定するための Workstation の設定 \(P. 258\)](#)

[アジア系言語レポート向けの Workstation の設定 \(P. 259\)](#)

冗長モードでの Workstation の実行

Workstation を冗長モードで実行すると、ログに詳細な情報が記録されます。これはデバッグまたはトラブルシューティングを行う際に有効です。

Workstation を冗長モードで実行する方法

1. `<EM_Home>/config` にあるファイル `IntroscopeWorkstation.properties` を開きます。
2. プロパティ `log4j.logger.Workstation` の「`INFO`」を、以下の文字列で置き換えます。

```
VERBOSE#com.wily.util.feedback.Log4JSeverityLevel
```

3. 変更を保存します。

Workstation の出力のファイルへのリダイレクト

Workstation の出力をファイルにリダイレクトする方法

1. `<EM_Home>/config` にあるファイル `IntroscopeWorkstation.properties` を開きます。
2. `log4j.logger.Workstation` プロパティ内で、「`console`」を「`logfile`」に置き換えます。たとえば、以下の設定により Workstation は、冗長メッセージをログ ファイルに記録します。
`log4j.logger.Workstation=VERBOSE#com.wily.util.feedback.Log4JSeverityLevel,logfile`
3. `log4j.appender.logfile.File` プロパティを使用して、Workstation のログ ファイルの名前および場所を変更できます。

ログイン値を指定するための Workstation の設定

`Introscope Workstation.lax` ファイルを変更して、ログインに必要な値の指定と、ログイン画面の表示の省略を行うことができます。

Workstation のログイン画面の表示が省略されるようにコマンドライン引数を設定する方法

1. ファイル `<EM_Home>/Introscope Workstation.lax` を開きます。
2. プロパティ `lax.command.line.args` で、値を指定する必要がある各ログイン コマンドに `-login` で始まるコマンドを追加します。たとえば、ローカル認証を使用している場合、このプロパティは以下のようになります。
`lax.command.line.args=$CMD_LINE_ARGUMENTS$ -loginimmediate
-loginhost foos -loginport 4503 -loginresponse sanderson,45tst87`

注: この設定項目からデフォルト値の `$CMD_LINE_ARGUMENTS$` を削除しないでください。

ログインが成功すると（正しい構文で使用されたコマンドによって正しい情報が指定された場合）、Workstation にログインした状態になり、コンソールが表示されます。

ログインに失敗すると、Workstation は起動しません。また、エラーメッセージがログに記録されます。

アジア系言語レポート向けの Workstation の設定

中国語や日本語などのマルチバイト文字セットを使用する言語で Introscope レポートを生成する場合は、以下の説明に従って Workstation にコンポーネントを追加します。

アジア系の言語で RTF または HTML 形式のレポートを生成する方法

- 「Windows のアジア系言語に対する追加言語サポート」をインストールします。
<http://www.microsoft.com/globaldev/handson/user/xpintl1supp.msp> を参照してください。

アジア系の言語で PDF 形式のレポートを生成する方法

- Acrobat Reader のアジア フォント パックを
<http://www.adobe.com/products/acrobat/acrrasianfontpack.html> からダウンロードして、インストールします。

第 13 章：システム設定

このセクションでは、CA APM の全体的なシステム設定について説明します。

このセクションには、以下のトピックが含まれています。

[クロック スキュー許容度の設定 \(P. 261\)](#)

[最大データ ポイント取得プロパティの設定 \(P. 262\)](#)

[クエリによって返されるデータ ポイントの制限 \(P. 264\)](#)

[返されるクエリ結果数の増加 \(P. 265\)](#)

[APM ステータス コンソールのクランプおよび重要イベントの設定 \(P. 265\)](#)

クロック スキュー許容度の設定

クロック スキュー許容度とは、時刻調整の変動量であり、通常はその値を微増させることで設定します。たとえば、わずかに進みの速いコンピュータのクロックを数秒間戻すと、ログにわずかな変更が加えられることとなります。遅らせることで生じた時刻の変動により、同じメトリックに対して異なる時刻にタイムスタンプが押されることになり、システムは重複している期間内に 2 つのメトリック値を取得することとなります。

時間を戻す処理は、オペレータによって明示的に行われる場合と、自動クロック同期によって非明示的に行われる場合があります。後者の方法は大規模なシステムでよく使用されます。

Enterprise Manager では、以下の 2 つのいずれかの方法でクロック スキュー許容度を解決します。

- 時刻の調整幅が大きい場合には、システムはエラーを発行して終了します。
- 小さな調整幅で時刻を戻した場合には、警告が発行され、タイムスタンプが調整前の時刻と同一になるまで、収集サイクルを停止します。

このしきい値の値はデフォルトの 60 秒に設定されていますが、変更可能です。指定秒数未満で時刻を戻した場合、警告が発行されて収集が一時的に中断されますが、それより大きい場合はシステムが終了します。

システムクロックが戻されたことを Enterprise Manager が検知すると、クロックが調整前の時間になるまで、収集サイクルを遅延させます。これは、時刻の進みが早い CPU で、ネットワーク タイム サービスによって時刻が再設定される場合などによく発生します。遅延の際には、警告メッセージが表示されます。警告メッセージを表示させない場合は、オプションの `introscope.enterprisemanager.clock.skewsuppresswarn` プロパティで設定できます。このプロパティの値は、メトリック ハーベストを遅らせるミリ秒数です。この値を超えると、遅延は重大であるとみなされてログに記録されます。

クロックスキュー許容度しきい値を設定するには、以下の手順に従います。

1. Enterprise Manager を停止します。
2. `<EM_Home>%config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
3. `introscope.enterprisemanager.clock.skewtoleranceseconds=<XXX>` プロパティを追加します。`<XXX>` は秒数です。
4. オプション: `introscope.enterprisemanager.clock.skewsuppresswarn` プロパティを設定します。デフォルト値 (ミリ秒) は `0` です。

注: この値を `introscope.enterprisemanager.clock.skewtoleranceseconds` プロパティより大きく設定することはできません。設定すると、警告が完全に表示されなくなり、システムが終了します。

5. Enterprise Manager を起動します。新しい設定が適用されます。

最大データポイント取得プロパティの設定

最大データポイント取得プロパティを、JDBC、CLW および Top N (CLW と Workstation の両方) クエリのパフォーマンスの尺度として設定できます。データポイントは、1つの期間に対する1つのメトリックの値です。

この Enterprise Manager クランププロパティによって、Enterprise Manager が任意の単一クエリで SmartStor から取得するメトリック データポイントの最大数が制限されます。ただし、Enterprise Manager は常に、少なくとも1つのメトリックのデータをすべて返します。このプロパティは、クラスタ化されたコレクタまたはスタンドアロンの Enterprise Manager のいずれかに適用されます。

このプロパティが設定されない場合、以下が発生する場合があります。

- Enterprise Manager が過負荷になり、CA APM システムのパフォーマンスが低下し、場合によってはメモリ不足エラーが発生します。
- このプロパティによって、コマンドライン Workstation や Workstation によって抽出されるデータが多くなりすぎる場合があります。これらのアクションによって、Enterprise Manager が応答を停止することがあります。

以下の手順に従います。

1. <EM_Home>\%config ディレクトリに移動し、
IntroscopeEnterpriseManager.properties ファイルを開きます。

2. 以下のプロパティを追加します。

introscope.enterprisemanager.query.datapointlimit=100000

100000 は、クエリごとに SmartStor から返されるデータポイントの数を約 100,000 に制限します。数値を入力しない場合、制限はありません。

3. *IntroscopeEnterpriseManager.properties* ファイルを保存します。

この設定は、Enterprise Manager がホットデプロイ中にプロパティファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

クエリによって返されるデータポイントの制限

`introscope.enterprisemanager.query.returneddatapointlimit` プロパティを、JDBC、CLW および Top N（CLW と Workstation の両方）クエリのパフォーマンスの尺度として設定できます。この Enterprise Manager クランププロパティによって、クエリによって返されるデータポイントの数が制限されます。データポイントは、1つの期間に対する1つのメトリックの値です。

クエリによって返されるデータポイントの数は、以下の要因によって変わります。

- 一致するメトリックの数
- 要求している時間範囲
- SmartStor データの精度（SmartStor データ層の構成に依存する）

たとえば、単一メトリックの1時間分のデータを1分の精度でクエリしていると仮定します。SmartStor 内にデータが15秒の精度で存在する場合、クエリは240のデータポイントと一致します。ただし、1分の精度でクエリしているため、15秒のデータポイントは1分のデータポイントに集約されます。そのため、クエリでは60のデータポイントのみが返されます。

メトリックが指定された場合、クエリは、要求されたデータのフルセットを返すか、何も返しません。メトリック用の一部のデータを表示することはできず、すべてのデータが表示されるか、何も表示されないかのいずれかです。クランプの効用は、データが返されるメトリックの数を減らせる点です。

メモリが乏しい環境で、このプロパティが設定されていないと、大きなデータクエリによって Enterprise Manager にメモリ不足状態が生じる可能性があります。

以下の手順に従います。

1. `<EM_Home>%config` ディレクトリに移動し、`IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. 以下のプロパティを追加します。

```
introscope.enterprisemanager.query.returneddatapointlimit= 100000
```

100000 は、クエリごとに SmartStor から返されるデータポイントの数を約 100,000 に制限します。数値を入力しない場合、制限はありません。

3. *IntroscopeEnterpriseManager.properties* ファイルを保存します。

この設定は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

返されるクエリ結果数の増加

RangeQuery クエリ、*PrefixQuery* クエリ、*WildcardQuery* クエリ、または *FuzzyQuery* クエリを実行すると、これらのクエリは検索実行前に展開されます。たとえば、インデックス付き文書に「car」と「cars」という用語が含まれている場合、クエリ「ca*」は検索実行前に「car OR cars」に展開されます。このため、この数が、この用語のしきい値のデフォルト値である 2048 を超えると、システム エラーが発生する可能性があります。この場合、*TooManyClauses* 例外が返されます。

返されるクエリ結果数を増やすには、以下の手順に従います。

1. <EM_Home>%config ディレクトリに移動し、*IntroscopeEnterpriseManager.properties* ファイルを開きます。
2. 以下のプロパティを追加し、デフォルト値の 2048 より大きな値を指定します。
introscope.enterprisemanager.lucene.search.BooleanQuery.SetMaxClauseCount

この設定は、Enterprise Manager がホット デプロイ中にプロパティ ファイルを調べるとき（約 60 秒ごとに行われます）に適用されます。

APM ステータス コンソールのクランプおよび重要イベントの設定

apm-events-thresholds-config.xml ファイル内の CA Introscope クランプ プロパティ、CA CEM クランプ プロパティ、および重要イベント プロパティのしきい値を設定できます。これらのプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールにそれを通知します。クランプの情報は [アクティブ クランプ] タブに表示されます。重要イベントの情報は [重要イベント] テーブルビューに表示されます。

以下の手順に従います。

1. <EM_Home>/config ディレクトリに移動し、
apm-events-thresholds-config.xml ファイルをバックアップします。
重要: ファイルのバックアップを無視しないでください。設定した
ファイルが破損すると、プロパティ値がデフォルトに戻り、ユーザの
設定はすべて失われます。
2. 環境に合わせてプロパティを設定します。
注: *threshold value* フィールドの値のみを設定してください。他の
clamp ID、importantEvent ID、description などのフィールドは、CA
Introscope がシステムの監視時に使用するフィールドなので、変更しな
いでください。
 - a. apm-events-thresholds-config.xml ファイルを開きます。
 - b. クランプおよび重要イベントのしきい値を変更します。
たとえば、<threshold value="500000"/> (500000 は変更後の値) な
どとします。
3. apm-events-thresholds-config.xml ファイルを保存して閉じます。
Enterprise Manager は、60 秒ごとにおよそ 1 回発生するホット デプロ
イ中にユーザの設定を適用します。
apm-events-thresholds-config.xml ファイルに構文エラーが見つかった
場合、Enterprise Manager は以下のアクションを実行します。
 - APM ステータス コンソールに通知して、[重要イベント] テーブル
ビューに apm.events.thresholds.config.error 重要イベントを表示
します。
 - すべてのクランプ プロパティおよび重要イベント プロパティの
値をデフォルト値に戻します。
4. 必要な場合は、apm-events-thresholds-config.xml ファイルのトラブル
シューティングを行います。
 - a. apm-events-thresholds-config.xml ファイルを開きます。
 - b. ファイルに構文エラーがないかどうかを確認し、必要に応じて修
正を行います。
 - c. ファイルを保存して閉じます。

- d. `apm-events-thresholds-config.xml` ファイルのエラーを検出または修正できない場合は、破損した `apm-events-thresholds-config.xml` ファイルを手順 1 で保存したバックアップ ファイルに置き換えます。
 - e. 手順 2 ~ 3 を繰り返します。
5. クラスタ全体の **Enterprise Manager** を設定する場合は、すべてのコレクタ、MOM、および CDV（デプロイされている場合）上で手順 1 ~ 4 を実行します。

CA Introscope と CA CEM のクランプ プロパティおよび重要イベント プロパティによってすべての **Enterprise Manager** が設定されます。

`apm-events-thresholds-config.xml` ファイルがデプロイされ、プロパティがしきい値のレベルに到達したか、またはそれを超過したときにクランプと重要イベントのクランプがアクティブになります。

第 14 章: アプリケーション問題切り分けマップの構成

この章では、アプリケーション問題切り分けマップのオプションの動作を構成する方法について説明します。

このセクションには、以下のトピックが含まれています。

[アプリケーション問題切り分けマップ](#) (P. 269)

[アプリケーション問題切り分けマップデータのクランプ](#) (P. 276)

[アプリケーション問題切り分けマップデータの廃棄の設定](#) (P. 276)

[アプリケーション問題切り分けマップオブジェクトの廃止時間の設定](#) (P. 280)

アプリケーション問題切り分けマップ

アプリケーション問題切り分けマップは、アプリケーションを構成するコンポーネントをグラフィカルに表示したもので、アプリケーションの稼働状況とエラーを表示します。このマップは、Introscope メトリック、エラーおよびイベントのパフォーマンスと分析から自動的に生成されます。定義に従い、ビジネスセントリックな観点からアプリケーションを表現します。アプリケーション問題切り分けマップを使用すれば、ユーザの環境内の各アプリケーションの構造やアプリケーション間の関係を視覚的にすぐ把握でき、現在の問題や潜在的な問題を特定し、切り分ける助けとなります。

アプリケーション問題切り分けマップの外観と使用法の詳細については、「CA APM Workstation ユーザガイド」を参照してください。

Introscope エージェントはビジネス トランザクションとエージェントを検出し、両者の依存関係を検出します。その後、エージェントはこの情報を Enterprise Manager にデータとしてレポートします。Enterprise Manager は、APM データベース内にデータを格納し、Workstation にデータを送信します。Workstation は、このデータを [マップ] タブにアプリケーション問題切り分けマップとして表示します。

以下を構成できます。

- エージェントによってアプリケーション問題切り分けマップデータを収集するかどうか。
- マップを描画するために、Introscope によってフロントエンドまたはビジネス サービスのデータをサンプリングする割合。「[トランザクション サンプリング \(P. 270\)](#)」を参照してください。
- アプリケーション問題切り分けマップデータを APM データベース内に保存する期間。「[マップ エlement エイジング \(P. 271\)](#)」を参照してください。
- アプリケーション問題切り分けマップデータを APM データベースから廃棄するかどうか、およびその頻度。「[アプリケーション問題切り分けマップデータの廃棄 \(P. 276\)](#)」を参照してください。

トランザクション サンプリング

Introscope では、トランザクション サンプリングと呼ばれる、アプリケーション問題切り分けマップ表示用データの供給方法を使用します。エージェントの開始後、Introscope は、(デフォルトで) 最初の 100 個のトランザクションを取得し、フロントエンドまたはビジネス トランザクションとその依存関係の初期マップを描画します。その後、10 個のうちの 1 個のトランザクションのみがマップへのデータ サポートを継続するレベルになるまで、サンプリングするトランザクション数を徐々に減らします。トランザクションが 1 万個になるたびに、このパターンが繰り返されます。

サンプリングレートは、*IntroscopeAgent.profile* 内の以下のプロパティを編集して調整できます。

- `introscope.agent.tracer.sampling.maxrate`
- `introscope.agent.tracer.sampling.initial.period`
- `introscope.agent.tracer.sampling.reset.period`

IntroscopeAgent.profile 内のプロパティの編集については、「[CA APM Java Agent 実装ガイド](#)」または「[CA APM .NET Agent 実装ガイド](#)」(お使いの環境に応じて) を参照してください。

これらのプロパティを調整して、マップ表示をサポートするトランザクションの数を増やすと、オーバーヘッドに影響を与える可能性があるため、注意してください。

マップ エlement エイジングの設定

接続用データがエイジアウトするか、APM データベースから廃棄されると、エージェントはフロントエンドとビジネス サービスおよびその依存関係を再検出します。Workstation はアプリケーション問題切り分けマップにこのデータを表示します。

エージェントによってアプリケーション問題切り分けマップ データを収集できるように指定した後で、エージェントによるデータ収集の頻度を構成できます。たとえば、以下の頻度でアプリケーション問題切り分けマップ データを収集するようにエージェントを構成できます。

- 環境に頻繁に変更が加えられる場合、24 時間ごとに 1 回。
- 環境への変更の頻度が少ない場合、1 週間に 1 回。

また、Enterprise Manager がマップにデータを配信する期間を構成できます。たとえば、エージェントによって検出されたデータを 1 週間または 1 か月間表示できます。この期間は 2 つのマップ時間範囲プロパティ「エイジング時間」と「ウィンドウ時間」に基づきます。

エイジングは、アプリケーション問題切り分けマップ エlement の特性です。CA Introscope がフロントエンドまたはビジネス トランザクションのデータを受信しなくなったとき、そのマップ エlement の状態をエイジングと呼びます。エイジング時間は、Workstation がアプリケーション問題切り分けマップ内のエlement の表示を継続する時間です。この時間が期限切れになったとき、エlement はエージェント キャッシュから削除され、アプリケーション問題切り分けマップに aged と表示されます。エイジング時間は `introscope.apm.data.agingTime` プロパティで設定します。デフォルト値は 1 日です。

時間ウィンドウは、エイジング エlement がマップから表示されなくなるまで Workstation がエlement を表示する時間です。このオプションは `introscope.apm.data.timeWindow` プロパティで設定します。デフォルト値は 3 日です。

たとえば、以下のようなデフォルト設定を仮定します。

アプリケーション A はアプリケーション問題切り分けマップのフロントエンドで、アプリケーション B と依存関係にあります。エージェントによってアプリケーション B のデータが継続的にレポートされ、アプリケーション B はマップ内に正常に表示されます。データがアプリケーション B からレポートされなくなると、エイジング時間とウィンドウ時間の計測が開始されます。1 日後、アプリケーション B のマップ ノードが **aged** と表示されます。3 日後、アプリケーション B のマップ ノードはマップに表示されなくなります。

考慮事項：

- **timeWindow** には、**agingTime** の期間が含まれます。
- **timeWindow** と **agingTime** を同じ期間に設定すると、マップ エlement を **aged** と表示できません。**timeWindow** の期間が終了すると、これらは表示されなくなります。
- **timeWindow** を **agingTime** よりも大きな値に設定した場合は、**aged** のマップ エlement は **agingTime** の期間の経過後に表示されなくなります。
- **agingTime** と **timeWindow** については、組織がアプリケーションに対して追加や変更を行う頻度に基づいて値を選択します。この値によって、エージェントと **Enterprise Manager** のオーバーヘッドが増減する可能性があります。設定する値が低いほど、マップに表示されるアプリケーションの依存関係はリアルタイムなものになります。高い値を設定すると、マップに現在のアプリケーションの依存関係が表示されます。

重要: クラスタ環境では、**agingTime** または **timeWindow** のデフォルトプロパティ値への変更は、**MOM** およびすべてのコレクタに適用される必要があります。

以下の手順に従います。

1. <EM_Home>/config ディレクトリにある IntroscopeEnterpriseManager.properties ファイルを開きます。
2. introscope.apm.data.agingTime の値を変更する場合
 - a. エージェントを停止します。
 - b. Enterprise Manager をシャットダウンします。

重要: introscope.apm.data.agingTime プロパティの値を変更する場合は、[「アプリケーション問題切り分けマップのエイジング時間設定を小さくする場合の影響 \(P. 274\)」](#)を参照してください。
3. introscope.apm.data.agingTime プロパティを設定します。デフォルト値は 1 日です。値は 1 分より小さくすることはできません。
4. introscope.apm.data.timeWindow プロパティを設定します。デフォルト値は 3 日です。値は 1 分より小さくすることはできません。
5. IntroscopeEnterpriseManager.properties ファイルを保存して閉じます。
6. introscope.apm.data.agingTime プロパティを変更した場合は、エージェントを再起動します。
7. Enterprise Manager を再起動します。
8. <EM_Home>/logs ディレクトリ内のマップデータ エイジング プロパティに関する Enterprise Manager ログ ファイル メッセージを確認します。例：

```
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :  
introscope.apm.data.agingTime set to value : [ PropertyWithTimeUnit : 1 Min]]
```

アプリケーション問題切り分けマップのエイジング時間設定を小さくする場合の影響

IntroscopeEnterpriseManager.properties ファイル内のプロパティ *introscope.apm.data.agingTime* の値を小さくする場合、CA Technologies では、履歴データへの予期しない影響を回避するために、アプリケーション問題切り分けマップデータをクリーンアップすることをお勧めします。エイジング時間を小さくすると、マップ表示に示されるデータサンプルも少なくなります。その結果、エージェントによる Enterprise Manager へのデータレポートが原因で、APM データベース内のデータに基づく誤った表示が行われる可能性があります。データベースからデータをクリーンアップすることで、この問題を回避できます。

データをクリーンアップするには、PostgreSQL クライアントを使用する必要があります。このクライアントは PostgreSQL サイト (<http://www.pgadmin.org>) からダウンロードできます。

PostgreSQL クライアントを使用してデータベースをクリーンアップする方法

- 以下の SQL ステートメントを実行します。

```
truncate apm_edge;
```

プロパティ *introscope.apm.data.agingTime* の値を増やす場合は、このような予期しない影響はありません。データベースのクリーンアップが必要になるのは、プロパティの値を減らす場合のみです。

エイジング関連のプロパティが履歴ビューに与える影響

アプリケーション問題切り分けマップで履歴データを表示する際、以下の概念に注意してください。

- 履歴期間の開始点と終点の設定にかかわらず、アプリケーション問題切り分けマップに表示されるデータは常に、最低でも *introscope.apm.data.timeWindow* プロパティに設定された期間を含みます。例：
 - 履歴期間の開始日と終了日の間を 10 日に設定し、*introscope.apm.data.timeWindow* を 3 日に設定した場合、マップには 10 日間全体のデータが表示されます。
 - 履歴期間の開始日と終了日の間を 2 日に設定し、*introscope.apm.data.timeWindow* を 3 日に設定した場合、マップには 3 日分のデータが表示されます。これは、2 日間の終了日と同じ日を最後とする 3 日分です。手動で設定された履歴期間のほうが小さい場合でも、*introscope.apm.data.timeWindow* プロパティに設定されている期間が、マップに表示される最小期間になります。
- マップエレメントのエイジングは、エイジング時間が履歴ウィンドウ後に発生したかのように、*introscope.apm.data.agingTime* プロパティに設定された期間を経過します。例：
 - *introscope.apm.data.agingTime* が 1 日に設定され、履歴期間が 10 日に設定されている場合、エージェントによって期間の最終日 (1 日) の間このエレメントがレポートされないと、マップエレメントが **aged** と表示されます。

アプリケーション問題切り分けマップ データのクランプ

アプリケーション問題切り分けマップへのデータフローを制御し、良好なパフォーマンスを確保するために、Introscope では、`introscope.apm.query.max.results` プロパティ

(`APMEnterpriseManager.properties` 内にあります) によって設定されたしきい値を使用し、Workstation がマップへの表示を試行するデータ量をクランプします。ツリーノードを選択するか、このしきい値を超えるマップエレメントのアンロールを試みると、「マップが大きすぎるため表示できません。」というメッセージが表示されます。プロパティの値を調整することで、このしきい値を調整できます。

注: `introscope.apm.query.max.results` プロパティの値を調整すると、Workstation パフォーマンスに影響を与える場合があります。

このプロパティの詳細については、「[introscope.apm.query.max.results \(P. 541\)](#)」を参照してください。

アプリケーション問題切り分けマップ表示のしきい値を編集する方法

1. `<EM_Home>/config` ディレクトリの `APMEnterpriseManager.properties` ファイルを開きます。
2. Enterprise Manager をシャットダウンします。
3. `introscope.apm.query.max.results` プロパティを見つけて、値を調整します。
4. `APMEnterpriseManager.properties` ファイルを保存して閉じます。
5. Enterprise Manager を再起動します。

アプリケーション問題切り分けマップ データの廃棄の設定

APM データベース内のアプリケーション問題切り分けマップ データは、時間の経過と共に増大する場合があります。APM データベース内の過剰なデータは、Enterprise Manager によるアプリケーション問題切り分けマップデータの取得だけでなく、Workstation と Enterprise Manager のパフォーマンスにも影響を与える可能性があります。アプリケーション問題切り分けマップデータを廃棄することで、APM データベース内の過剰なマップデータが収集されないようにすることができます。

重要: APM データベース上でのアプリケーション問題切り分けマップデータの廃棄を有効にする場合、この設定はクラスタ内の 1 つの **Enterprise Manager** でのみ行ってください。ただし、アプリケーション問題切り分けマップデータの廃棄は、**MOM** 上で有効にすることをお勧めします。

マップデータが廃棄されるまでデータベース内に保持される期間と、廃棄の実行スケジュールの頻度を構成することはできます。マップデータの廃棄はスケジューラを使用して制御します。データの廃棄を、日単位、週単位、月単位で実行するよう構成できます。

重要: アプリケーション問題切り分けマップデータの廃棄用のコレクタを設定することはできません。コレクタに対して `introscope.apm.pruning.enabled` プロパティを `true` に設定した場合、エラーが返されます。

マップの表示中にアプリケーション問題切り分けマップデータが廃棄された場合、ユーザがマップ時間範囲を変更するまで、廃棄されたデータはマップ上に残ります。時間範囲を変更すると、マップの再描画がトリガされます。

複数の **Enterprise Manager** でデータベースの廃棄を有効にした場合、複数の廃棄プロセスによるデータベースアクセスが競合し、データベースのデッドロックが発生します。

以下の手順に従います。

1. `<EM_Home>/config` ディレクトリの `IntroscopeEnterpriseManager.properties` ファイルを開きます。
2. **Enterprise Manager** をシャットダウンします。
3. `introscope.apm.pruning.enabled` プロパティが `true` に設定されていることを確認します。

このプロパティによって、エージェントによるアプリケーション問題切り分けマップデータの廃棄が可能になります。

`introscope.apm.pruning.enabled` を `false` から `true` にリセットした場合は、このプロパティを有効にするために **Enterprise Manager** を再起動してください。

4. (オプション) 以下のプロパティを設定します。

注: 環境内のアプリケーション問題切り分けマップ データの量を管理するために `introscope.apm.data.preserving.time` プロパティの値を低く設定します。そうしないと、例外が表示される場合があります。例外を防ぐには、APM SOI コネクタをインストールする前に、使用中の環境がアプリケーションの使用状況に従って調整されていることを確認します。まだ例外が表示される場合は、

`APMEnterpriseManager.properties` ファイル内の `introscope.apm.query.max.results` プロパティの値を増加させます。

- `introscope.apm.data.preserving.time`
- `introscope.apm.pruning.cron.trigger.expression`

- a. `introscope.apm.data.preserving.time` プロパティを設定します。このプロパティは、アプリケーション問題切り分けマップ データを APM データベース内に保存する期間を制御します。保存期間の値より古いマップ データは、エイジアウトしているとみなされ、廃棄することができます。デフォルト値は 365 日です。

廃棄中、`introscope.apm.data.preserving.time` と `Introscope.apm.data.agingTime` の値の合計値より古いマップ データが削除されます。たとえば、`introscope.apm.data.preserving.time` の値が 30 日で、`introscope.apm.data.agingTime` の値が 1 日である場合は、 $30 + 1 = 31$ 日より古いマップ データが削除されます。

組織がアプリケーションに対して追加や変更を行う頻度に基づいて値を更新してください。この追加や変更によって、アプリケーション問題切り分けマップ データが APM データベースに追加されます。詳細については、「[introscope.apm.data.preserving.time \(P. 526\)](#)」を参照してください。デフォルト値は 365 日です。

- b. `introscope.apm.pruning.cron.trigger.expression` プロパティを設定します。このプロパティは、エイジアウトしたアプリケーション問題切り分けマップ データを APM データベースから廃棄する頻度をスケジュールします。デフォルト値は毎日午前 6:00 です。

組織がアプリケーションに対して追加や変更を行う頻度に基づいて値を更新してください。この追加や変更によって、アプリケーション問題切り分けマップ データが APM データベースに追加されます。詳細については、

「[introscope.apm.pruning.cron.trigger.expression \(P. 527\)](#)」を参照してください。

5. *IntroscopeEnterpriseManager.properties* ファイルを保存して閉じます。
6. Enterprise Manager を再起動します。

Enterprise Manager が起動したら、<EM_Home>/logs に移動して、マップデータ廃棄プロパティに関連する Enterprise Manager ログファイルメッセージを確認できます。例：

```
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :  
introscope.apm.pruning.enabled set to value : true]  
11/23/09 12:02:13 PM PST [INFO] [Manager] [ The APM Data property :  
introscope.apm.pruning.cron.trigger.expression set to value : 0 0 6 * * ?]
```

アプリケーション問題切り分けマップ オブジェクトの廃止時間の設定

CA APM では、アプリケーション問題切り分けマップ オブジェクトおよびそれらの関係を、*Edge* と *Vertex* という用語を使用して表します。APM データベースは、これらのオブジェクトに関するデータを格納します。

時間が経過して、Enterprise Manager と監視対象アプリケーションの間の接続が失われると、Edge オブジェクトは、以下の 2 つの要因に従って「エイジアウト」します。

- `introscope.apm.data.obsolete.time` プロパティの値
- 以下の表で説明しているルール

Edge オブジェクトがエイジアウトすると、すべての関連オブジェクトは、ほかのアクティブな Edge オブジェクトで使用されていない場合「廃止」に分類されます。アプリケーション問題切り分けマップは、これらの廃止されたオブジェクトに関連付けられたエレメントをグレー表示して、それらのエレメントが古いデータで、最新のデータではないことを示します。

これらの古いオブジェクトは、APM データベースに残り、自動的に削除されません。廃棄に設定されたプロパティに基づいてアプリケーション問題切り分けマップ廃棄プロセスが実行される場合にのみ、オブジェクトは削除されます。廃棄のストアドプロシージャは、廃止ルールとは異なる廃棄ルールに基づいてオブジェクトを物理的に削除します。廃棄の詳細については、「[SmartStor メタデータの廃棄 \(P. 90\)](#)」を参照してください。

アプリケーション問題切り分けマップ オブジェクトのエイジングのルール

| オブジェクト | 条件 |
|---|--|
| Edge (データベース テーブル <code>apm_edge</code>) | Edge は、その更新日付が <code>introscope.apm.data.obsolete.time</code> プロパティの値より古い場合、廃止と見なされます。 |
| Vertex (データベース テーブル <code>apm_vertex</code>) | Vertex は、廃止された Edge によってのみ参照され、アプリケーション問題切り分けマップ内のほかの Edge によって参照されていない場合、廃止と見なされます。 |

| オブジェクト | 条件 |
|-----------------------------------|--|
| 所有者 (データベース テーブル apm_owner) | 所有者は、廃止された Edge によってのみ参照され、アプリケーション問題切り分けマップ内のほかの Edge によって参照されていない場合、廃止と見なされます。 |
| エージェント (データベース テーブル apm_agent) | エージェントは、アプリケーション問題切り分けマップ内の廃止された Vertex によってのみ参照されている場合、廃止と見なされます。 |

アプリケーション問題切り分けマップの時間エイジング プロパティ

アプリケーション問題切り分けマップの時間エイジング プロパティを設定すると、データベースから廃止されたオブジェクトに対する要求を返すことができます。時間が設定されていない場合、期間内の時点 (introscope.apm.data.preserving.time + introscope.apm.data.agingTime - introscope.apm.data.obsolete.time) を指している要求では、オブジェクトを廃止として指定できます。

デフォルト値は以下のとおりです。

- introscope.apm.data.preserving.time
デフォルト : 365 日
- introscope.apm.data.agingTime
デフォルト : 1 日
- introscope.apm.data.obsolete.time
デフォルト : 300 日

重要: クラスタ環境では、agingTime または timeWindow のデフォルト プロパティ値への変更は、MOM およびすべてのコレクタに適用される必要があります。

例

廃止されたオブジェクトについての情報を取得するには、11月1日 8:00 および 15:00、および 11月2日 10:00 に対してクエリ Web サービス API を実行します。このクエリは、各要求に対して以下の結果を返します。

Get obsolete objects at November 1 8:00

11月1日 8:00 で 300 日より古い廃止されたオブジェクトを識別します。 `introscope.apm.data.preserving.time` と `introscope.apm.data.agingTime` の合計値より古いオブジェクトは返されません。

Get obsolete objects from November 1 8:00 to November 1 15:00

11月1日 8:00 および 11月1日 15:00 から `introscope.apm.data.obsolete.time` 値の 300 日を減算して、11月1日 8:00 から 11月1日 15:00 の間の廃止されたオブジェクトを識別します。 `introscope.apm.data.preserving.time` と `introscope.apm.data.agingTime` の合計値より古いオブジェクトは返されません。

Get obsolete objects from November 1 15:00 to November 2 10:00

11月1日 15:00 および 11月2日 10:00 から `introscope.apm.data.obsolete.time` 値の 300 日を減算して、11月1日 15:00 から 11月2日 10:00 の間の廃止されたオブジェクトを識別します。 `introscope.apm.data.preserving.time` と `introscope.apm.data.agingTime` の合計値より古いオブジェクトは返されません。

アプリケーション問題切り分けマップの時間エイジング プロパティの設定

アプリケーション問題切り分けマップ オブジェクトは `introscope.apm.data.obsolete.time` プロパティに基づいて廃止とマークされます。 `introscope.apm.data.obsolete.time` でデフォルト値の 300 日が使用されると、300 日を経過したオブジェクトは廃止されます。

以下の手順に従います。

1. CA Enterprise Manager をシャットダウンします。
2. `<EM_Home>%config` ディレクトリの `IntroscopeEnterpriseManager.properties` ファイルを開きます。

3. `introscope.apm.data.obsolete.time` プロパティのコメント化が解除され、値がデフォルト値の 300 日以外に設定されていることを確認します。
時間数または日数を指定します。最小値は 24 時間または 1 日です。
4. `IntroscopeEnterpriseManager.properties` ファイルを保存して閉じます。
5. Enterprise Manager を再起動します。
廃止時間プロパティが設定されます。
6. `<EM_Home>/logs` ディレクトリ内のメッセージログを確認します。例：
10/19/12 12:02:13 PM EST [INFO] [Manager] [The APM Data property:
`introscope.apm.data.obsolete.timeset` to value : 2 DAYS]

注: 設定した値よりも古いオブジェクトは、APM データベースから物理的に削除されるので、レポートできません。

第 15 章: Catalyst データをロードするための APM の設定

この章では、CA Catalyst からデータをロードできるように CA APM を設定する方法について説明します。

このセクションには、以下のトピックが含まれています。

[CA Catalyst データをロードするための CA APM の設定 \(P. 286\)](#)

[CatalystPolicy.xml ファイルの設定 \(P. 287\)](#)

CA Catalyst データをロードするための CA APM の設定

Catalyst.properties ファイルを設定すると、CA Catalyst のデータを CA APM にロードし、処理して、Workstation 内で表示することができます。

以下の手順に従います。

1. `<EM_Home>/config` ディレクトリの *Catalyst.properties* ファイルを開きます。
2. Enterprise Manager をシャットダウンします。
3. 以下の必要なプロパティを編集します。

- *catalyst.host* = `<CA Catalyst RESTful API の場所を入力します>`
- *catalyst.protocol* = `<HTTP または HTTPS 接続を入力します>`
- *catalyst.port* = `<CA Catalyst のポート番号を入力します>`
- *catalyst.login* = `<CA Catalyst ユーザ名を入力します>`
- *catalyst.password* = `<CA Catalyst パスワードを入力します>`

注: *catalyst.login* および *catalyst.password* プロパティを設定すると、Enterprise Manager から CA Catalyst にログインすることが可能になります。再起動後（この手順の最終ステップを参照）、Enterprise Manager は、MD5 および Data Encryption Standard（DES）アルゴリズムによるパスワードベースの暗号化（PBE）を使用して、Catalyst パスワードを暗号化します。

- *catalyst.rest.entrypoint* = `/ssaweb/search`
4. （オプション）CA Catalyst アラートフィルタリングプロパティを設定します。
 5. *Catalyst.properties* ファイルを保存して閉じます。
 6. （オプション）`<EM_Home>/config` ディレクトリ内の *Catalyst.Policy.xml* ファイルを開き、エンティティアラート関連付けのためのルールを設定します。
 7. *Catalyst.Policy.xml* ファイルを保存して閉じます。
 8. Enterprise Manager を再起動します。

詳細:

[CatalystPolicy.xml ファイルの設定 \(P. 287\)](#)

[Catalyst.properties \(P. 562\)](#)

CatalystPolicy.xml ファイルの設定

CatalystPolicy.xml ファイルは、コネクタを使用したポリシーベースの設定で最大の柔軟性に提供するオプションの設定です。 *CatalystPolicy.xml* ファイルを使用すると、**USM** エンティティ、関連付けのあるエンティティのリスト、および関連付けのある関係のリストなどルールを定義できます。この設定により、定義されたルールに基づいて行う、指定された任意のエンティティ上のアラートの検索が絞り込まれます。

XML ファイル構造の例を以下に示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<policy xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="0.1"
xsi:noNamespaceSchemaLocation="policy0.1.xsd">
  <entity name="ComputerSystem" alertable="true">
    <include_entities>Processor Memory File Port</include_entities>
    <include_relations>IsComposedOf HasMember</include_relations>
  </entity>
  <entity name="Database" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="DatabaseInstance" alertable="true">
    <include_entities>Tablespace</include_entities>
    <include_relations>IsManagerFor</include_relations>
  </entity>
  <entity name="Group" alertable="false">
    <include_entities>ComputerSystem VirtualSystem</include_entities>
    <include_relations>HasMember</include_relations>
  </entity>
</policy>
```

詳細:

[CA Catalyst データをロードするための CA APM の設定 \(P. 286\)](#)

[Catalyst.properties \(P. 562\)](#)

第 16 章: CA CEM の概要

CA CEM は、ユーザのトランザクションを監視し、データセンターで問題の原因を隔離します。CA CEM は、トランザクションのパフォーマンスおよび品質を計測して、障害や不一致を特定し、ユーザおよびビジネスへの影響を数値化します。CA CEM によって、トランザクション応答時間が長くなる傾向を未然に検出し、さまざまな実用的なレポートを作成することで、問題が発生したり、サービス レベル アグリーメント (SLA) に準拠しなくなる前に、措置を講じることができます。

このセクションには、以下のトピックが含まれています。

[CEM コンソールおよびセットアップ ページへのアクセス](#) (P. 289)

[CA CEM 管理者の責任](#) (P. 292)

CEM コンソールおよびセットアップ ページへのアクセス

CA CEM は、Web ブラウザがインストールされている任意のコンピュータから設定および管理できます。

このトピックでは、CA CEM のインターフェース、およびそれらのインターフェースにアクセスする方法について説明します。

- [CEM コンソールへのアクセス](#) (P. 289)
- [TIM の Wily システム設定ページへのアクセス](#) (P. 291)
- [CEM コンソールから TIM へのアクセス](#) (P. 292)

CEM コンソールへのアクセス

ビジネス アプリケーション、ビジネス サービス、およびトランザクション定義の設定および処理は、Web ブラウザを搭載した任意のコンピュータから実行できます。

CEM コンソールは、CA CEM のメイン ユーザ インターフェースです。管理者は、このコンソールを使用して CA CEM の構成 (トランザクションの記録、トランザクション定義の作成など) を行います。アナリストは、このコンソールを使用してレポートを生成および表示します。

ユーザが管理者である場合、CEM コンソールには追加のメニュー オプションがあります。また、TIM が有効になっていない場合は、特定の CA CEM のリンクは表示されません。

(TIM が有効になっていない場合は、ツールと CA CEM のリンクは表示されません。)

特に明記する場合を除き、このガイドではユーザが管理者として CEM コンソールを使用していることを前提としています。

クラスタ化環境では、CEM コンソールはマネージャ オブ マネージャ (MOM) の上に存在します。

以下の手順に従います。

1. Web ブラウザを開き、以下のアドレスを入力します。

`http://<IP_Address>:8081/wily`

<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/wily`

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

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` ファイルに `introscope.enterprisemanager.webserver.port=8081` として定義されていますが、この番号は変更できます。

2. ユーザ名とパスワードを入力します。

CA CEM 管理者のデフォルトのユーザ名は、*cemadmin* です。

CEM コンソールが表示されます。

セキュリティとログインの詳細については、「CA APM セキュリティ ガイド」を参照してください。

CA CEM へのログインのトラブルシューティング

症状:

CA CEM にログインできない場合は、ブラウザでアクティブ スクリプトが有効であることを確認します。

アクティブ スクリプトが無効である場合は、CA CEM のログイン ページで [ログイン] をクリックすると、[CEM コンソール] / [戻る] ページにリダイレクトされます。これは、ユーザのユーザ名とパスワードが正しく入力されていても発生します。

解決方法:

アクティブ スクリプトを有効にするには、使用しているブラウザのユーザ ドキュメントを参照してください。たとえば Internet Explorer 8 では、[インターネット オプション] > [セキュリティ] > [レベルのカスタマイズ] > [スクリプト] > [アクティブ スクリプト] からこの設定にアクセスできます。

[TIM System Setup] ページへのアクセス

[TIM System Setup] ページから、さまざまな設定ページおよびステータス ページにアクセスできます。管理者は通常これらのページを使用してステータス情報の確認やトラブル シューティングを行います。

以下の手順に従います。

1. ウェブブラウザを開き、アドレスを入力します。<IP_Address> は TIM IP アドレスまたは DNS 名です。

`http://<IP_Address>/cgi-bin/wily/system/index`

例:

`http://192.168.1.54/cgi-bin/wily/system/index`

`http://cem.company.com/cgi-bin/wily/system/index`

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。

2. ユーザ名とパスワードを入力します。

[System Setup] ページのデフォルトのユーザ名は *admin* です。

[System Setup] ページが表示されます。

CEM コンソールから TIM へのアクセス

TIM の IP アドレスおよびパスを把握している場合は、[System Setup] ページから TIM 設定ページにアクセスできます。ただし、CEM コンソールが開いている場合は、そのコンソールから TIM 設定ページにアクセスできません。

以下の手順に従います。

1. 管理者のコンソールで、[設定] の [監視] を選択します。
2. TIM の IP アドレスをクリックします（右端の列）。
3. [System Setup] ページのユーザ名 *admin* とパスワードを入力します。
TIM 設定ページが表示されます。

CA CEM 管理者の責任

CA CEM 管理者の役割は、環境の複雑さ、統合のタイプ、ユーザの数、サポート リソース、および CA CEM 監視対象アプリケーションの増加の程度に応じて、サイトごとに異なります。

- [日単位のタスク](#) (P. 292)
- [週単位のタスク](#) (P. 293)
- [月単位のタスク](#) (P. 294)
- [四半期単位のタスク](#) (P. 294)

日単位のタスク

CA CEM 管理者の標準的な日単位のタスクを以下に示します。

- 日単位のバックアップを実行して確認する。
- インシデント、および必要に応じて障害を確認する。Introscope を使用して問題を解決する。
- 検出されたすべての CA CEM 問題を適切なグループに報告する。
- TIM および IntroscopeEnterpriseManager の各ログを確認する。

- システム イベントをオンラインで、または電子メール通知の受信後に確認する。たとえば、障害がドロップされているかどうか、などです（「[CA CEM イベントの表示 \(P. 377\)](#)」および「[イベントの電子メール通知の受信 \(P. 377\)](#)」を参照してください）。
- TIM の稼働状況を確認する（「[TIM マシン稼働状況の確認 \(P. 379\)](#)」を参照してください）。
- Introscope Workstation を使用して、Enterprise Manager 上での CA CEM の稼働状況を確認する。

週単位のタスク

CA CEM 管理者の標準的な週単位のタスクを以下に示します。

- バックアップおよびリストアの手順をテストする。
- CA SiteMinder、CA NSM、CA Service Desk などとの統合が期待どおりに機能していることをテストする。たとえば、シングルサインオンが SiteMinder Web エージェントで機能しているかどうかをテストします。
- CA CEM 構成ファイルおよびバックアップ ファイルのコピーをオフ サイトに保存する。
- Embedded Entitlements Manager の CA CEM 管理者リストに不要な管理者が含まれていないことを確認する。
- CA CEM 監査ログで、予期しない変更や無許可の変更が発生していないことを確認する。
- CA CEM の CPU、ディスク、およびシステムの各使用状況を確認する（「[TIM マシン稼働状況の確認 \(P. 379\)](#)」を参照してください）。
- 解決済みのインシデントや古いインシデントを必要に応じてクローズする。
- レポートで正確性および傾向を確認する。
- 電子メール レポートが期待どおりに作成および配布されていることを確認する。
- Introscope でリアルタイム ビジネス トランザクション メトリックおよびカスタム ダッシュボードを確認する。

- CA Service Desk や CA SiteMinder のログなど、統合ログを確認する
- エビデンス コレクションのログを確認する（「[ビジネスインパクトの設定およびインシデントエビデンスの収集 \(P. 335\)](#)」を参照してください）。

月単位のタスク

CA CEM 管理者の標準的な月単位のタスクを以下に示します。

- フェールオーバー手順を確認する（導入されている場合）。
- 古い/不要なユーザおよびユーザ グループをクリーンアップする。
- 新しいビジネス サービス/トランザクションなどを定義する必要があるかどうかを確認する。
- トランザクションの指定を変更する必要があるかどうかを確認する。
- ベースラインまたは SLA の設定を調整する必要があるかどうかを確認する。
- 月単位のレポートで正確性および傾向を確認する。
- 有効なトランザクションおよびビジネス トランザクション統計を確認し、監視する必要がなくなったトランザクションの定義を無効にする（トランザクション定義の管理については、「[CA APM トランザクション定義ガイド](#)」を参照してください）。
- HTTP アナライザ プラグインが有効な場合は、その動作を確認する。プラグインが期待どおりのニーズを満たしているかどうか、プラグインが満たす必要がある追加要件があるかどうか、前回の JAR ファイル更新以降にパフォーマンスの低下が発生したかどうかなどを確認します（「[CA APM トランザクション定義ガイド](#)」を参照してください）。

四半期単位のタスク

CA CEM 管理者の標準的な四半期単位のタスクを以下に示します。

- CA CEM アーキテクチャのパフォーマンス、スケーラビリティ、フェールオーバー、地理的な分散、およびその他の要因を確認する。
- CA CEM プロフェッショナル サービスが CA CEM のカスタマイズまたは統合に必要なかどうかを判断する。

- 起こりうる問題や新しい機能について (必要に応じて) 次の CA CEM リリースをベータテストする。
- ユーザグループ定義を確認する (たとえば、IP サブネット ユーザグループのルールに変更が必要かどうかを確認します)。

第 17 章: CA CEM のネットワーク オプション

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 CEM のネットワーク オプションの概要 \(P. 297\)](#)

[ネットワークトラフィックの監視の概要 \(P. 298\)](#)

[CA CEM の挿入場所の概要 \(P. 300\)](#)

[ブラウザから Enterprise Manager への接続 \(P. 305\)](#)

[IPv6 と CA CEM \(P. 305\)](#)

CA CEM のネットワーク オプションの概要

ネットワークには CA CEM を配置できる場所が複数あります。また、システムをネットワークに接続する方法にも選択肢があります。この章では、ネットワーク オプションについて説明します。

TIM と Enterprise Manager は別々のハードウェア上にあります。最初に検討することは、Enterprise Manager (コレクタおよび MOM (Manager of Managers)) に報告する TIM との接続です。

TIM を配置する場所には複数のオプションがあります。これらについては、「[CA CEM の挿入場所の概要 \(P. 300\)](#)」で説明します。TIM の場所によって、収集できる情報が決まります。

TIM の推奨挿入ポイントは、論理的にはネットワーク ロードバランサと Web サーバ集約スイッチの間、または集約スイッチが使用されていない場合はロードバランサと Web サーバの間です。詳細については、「[集約スイッチとネットワーク ロードバランサの間 \(P. 303\)](#)」を参照してください。

目的の場所に TIM をインストールするときに、ネットワークに TIM を接続する方法も選択する必要があります。

ネットワークトラフィックの監視の概要

TIM は、監視インターフェースを介してネットワークからのトラフィックを読み取ります。監視インターフェースは、ミラーポートまたはネットワークトラップに接続できます。

以下のセクションでは、TIM へのパケットの転送にミラーポートを使用する場合とネットワークタップを使用する場合を比較し、それぞれの長所と短所について説明します。

- [ネットワークタップの使用](#) (P. 298)
- [ミラーポートの使用](#) (P. 299)

ネットワークタップの使用

ネットワークタップは、インフラストラクチャの配線を直接利用するハードウェアデバイスで、パケットのコピーを作成して1つ以上の宛先に転送します。タップは、物理層でインフラストラクチャに接続し、ルータやスイッチ上のリソースを使用しません。タップの場合は、タップを挿入するために接続を一時的に停止する必要があります。

タップはネットワーク遅延に影響しません。多くのタップは、送信トラフィックと受信トラフィックを2つの物理インターフェースで別々に転送するので、TIM には物理インターフェースが2つ必要になります。これらのデータストリームはTIM によってマージする必要があります。ストリームのこのマージにより、TIM のパフォーマンスは少し低下します。タップには全二重のものもあります。この場合は、TIM に追加インターフェースもマージも必要ありません。

タップは送信専用デバイスなので、ミラーポートよりもセキュリティ性が高くなる可能性があります。タップのもう1つの長所は、設定が比較的単純であることです。タップはインラインデバイスなので、障害によって、ネットワークの操作が中断したり、障害のあるタップを置換するために（パッシブタップでない限り）停止が必要になる可能性があります。タップテクノロジーの発展により、障害が発生する可能性は大幅に軽減されています。

ミラーポートの使用

ミラーポート（Cisco 用語では SPAN ポート）は、ネットワーク ルータおよびスイッチのソフトウェア機能です。Cisco の 6500 シリーズのスイッチなど、最新のスイッチでは、SPAN ポートを有効にしてもスイッチのパフォーマンスには影響しません。一般に、ミラーポートは、プロトコルアナライザなどのネットワークトラブルシューティングデバイスを接続する場合に使用されます。スイッチがサポートするミラーポートの数には制限があるため、ネットワークエンジニアは、これらのメンテナンスポートへのデバイスの永久的な接続に消極的な場合があります。

ミラーポートはルータまたはスイッチのソフトウェア機能であるため、インフラストラクチャの変更は必要なく、有効にするための中断はタップよりも短くなります。追加の支出が必要となるタップとは異なり、すでにデプロイ済みであるスイッチであれば、通常は余分な支出をせずにミラーポートをサポートできます。

ミラーポートはネットワーク遅延に影響しません。一般に、ミラーポートは、転送前に送信トラフィックと受信トラフィックを組み合わせるので、TIM に必要なインターフェースの数は減ります。TIM は、複数のインターフェースからのデータストリームをマージする必要がないため、この構成ではパフォーマンスが若干向上します。

ほとんどの場合、ミラーポートは送信専用ポートですが、構成変更が間違っていると、ミラーポートは双方向スイッチポートとして設定される可能性があります。このため、ミラーポートは、タップよりもセキュリティ性が低いとみなされることがあります。TIM ソフトウェアは、監視ポート上で送信しないように設計されているため、TIM によってセキュリティリスクを招くことはありません。

注: アプリケーションのエンドユーザトラフィックが 2 つの異なるスイッチから入ってきている場合は、両スイッチのトラフィックを同一の TIM に対してミラー化することができます。これを行うには、ネットワークカード（複数ポートの NIC）を調達してデプロイする必要があります。ネットワークカードのサポートについては、「CA APM Compatibility Guide」を参照してください。

CA CEM の挿入場所の概要

インフラストラクチャにおける TIM の挿入場所は、収集する情報に影響します。

TIM は、監視インターフェースを介してネットワークからトラフィックを読み取ります。前述のセクションで説明したように、監視インターフェースは、ミラーポートまたはネットワークタップに接続できます。どちらの場合も、TIM は、対象となるパケットのコピーを受信し、分析してから、破棄します。TIM は監視ポート上では送信しません。トラフィックは TIM への一方方向です。TIM は監視ポートからのパケットの受信のみを行うように設定されています。

大企業の標準的なネットワーク インフラストラクチャでは、TIM 監視ポートを挿入する場所がたくさんあります。さまざまな挿入場所を図に示します。

注: ほとんどの環境では、冗長なインフラストラクチャが使用されていますが、簡潔にするため、この図では 1 つのパスのみを示します。



図の左から右方向に、パケットはインターネット ルータを介して社内に入ります。挿入場所 A は、ルータの外部に位置し、インターネットとルータの間です。

通常、このルータは、トラフィックをファイアウォールに転送します。挿入場所 B は、ルータとこのファイアウォールの間です。ファイアウォールは、インバウンドトラフィックおよびアウトバウンドトラフィックを検査し、社内のセキュリティポリシーによってトラフィックをブロックするか受け入れます。また、ファイアウォールは、ネットワークアドレス変換 (NAT) を実行して、社内のネットワーク接続デバイスをインターネットへの直接接続から保護することもできます。

注: 集約スイッチとネットワーク ロード バランサが同じデバイスに収められている場合もあります。

挿入場所 C は、ファイアウォールと集約スイッチ/ネットワーク ロード バランサの間です。受け入れ可能なトラフィックは、ファイアウォールから集約スイッチ/ネットワーク ロード バランサへ転送されます。多くの場合、集約スイッチ/ネットワーク ロード バランサは、SSL セッションを終了できるだけでなく、接続先クライアントの仮想 IP アドレス (VIP) をインスタンス化することもできます。多くの集約スイッチ/ネットワーク ロード バランサは、プロキシとして動作して、クライアントからの接続を終了し、クライアントに代わって Web サーバへの接続を確立します。集約スイッチ/ネットワーク ロード バランサの中には、Web サーバに対する負荷を軽減するために Web サーバへの永続接続を確立して使用するものもあります。

ほとんどの場合、集約スイッチはネットワーク ロード バランサにパケットを転送します。挿入場所 D は、集約スイッチとネットワーク ロード バランサの間です。

最終的に、Web サーバは、集約スイッチに接続されるか、ネットワーク ロード バランサに直接接続されます。挿入場所 E は、Web サーバの直前に位置し、集約スイッチと Web サーバの間、またはネットワーク ロード バランサと Web サーバの間のどちらかです。

パケットは、逆のパスで社内を出て、逆の順序でそれぞれの挿入場所を通過します (また、パケットが入るときに取るパスと出るときに取るパスが異なる (つまり、三角形になる) 可能性もあります)。または、Web サーバを出て、インターネットに直接入ることもあります。

インターネットとインターネット ルータの間

挿入場所 A は、インターネットとインターネット ルータの間です。この場合は、クライアント IP アドレスを必ず認識できます。



挿入場所 A では、サーバの IP アドレスまたはサーバの MAC アドレスをほとんど認識できません。CA CEM は、その除外ベースのリレーションシップ検出メカニズムで Web サーバの IP アドレスまたは MAC アドレスを使用して、収集するエビデンスセットを制限することで、トラブルシューティングの時間を短縮します。この情報がなくてもエビデンスコレクションの処理は続行されますが、エビデンスセットは削減されないため、技術担当者が分析する必要がある情報量は、除外ベースの検出を使用しない場合よりも多くなります。

TIM はユーザの識別にクライアント IP アドレスを使用しないため、挿入場所 A の使用にはメリットがほとんどなく、デメリットが多くなります。

インターネット ルータとファイアウォールの間

挿入場所 B は、インターネット ルータとファイアウォールの間で、ほとんどの場合クライアント IP アドレスを認識できます。

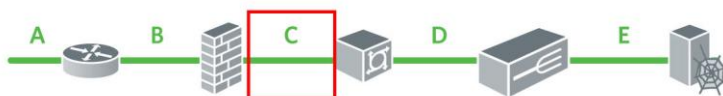


挿入場所 B では、サーバの IP アドレスまたはサーバの MAC アドレスをほとんど認識できません。CA CEM は、その除外ベースのリレーションシップ検出メカニズムで Web サーバの IP アドレスまたは MAC アドレスを使用して、収集するエビデンスセットを制限することで、トラブルシューティングの時間を短縮します。この情報がなくてもエビデンスコレクションの処理は続行されますが、エビデンスセットは削減されないため、技術担当者が分析する必要がある情報量は、除外ベースの検出を使用しない場合よりも多くなります。

TIM はユーザの識別にクライアント IP アドレスを使用しないため、挿入場所 B の使用にはメリットがほとんどなく、デメリットが多くなります。

ファイアウォールと集約スイッチの間

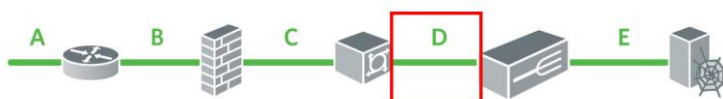
挿入場所Cは、ファイアウォールと集約スイッチの間で、ほとんどの場合クライアント IP アドレスを認識できます。挿入場所Cでは、サーバの IP アドレスをほとんど認識できません。



TIM はユーザの識別にクライアント IP アドレスを使用しないため、挿入場所Cの使用にはメリットがほとんどなく、デメリットが多くなります。環境により、挿入場所Cは、挿入場所AおよびB よりもわずかにメリットがある場合もあります。

集約スイッチとネットワークロード バランサの間

挿入場所Dは、集約スイッチとネットワークロード バランサの間で、通常はクライアント IP アドレスを認識できます。このため、ネットワークロード バランサがプロキシとして動作している場合は、ネットワークロード バランサで「ソースアドレスの保持」を有効にする必要があります。挿入場所Dでは、ほとんどの場合サーバの IP アドレスを認識できません。



ネットワークロード バランサが永続接続を使用している場合、TIM をここに配置すると TIM に対する負荷が軽減されます。負荷の軽減にはオープン接続を削減するという働きがあるので、重要になる可能性があります。ネットワークロード バランサがクライアントに代わって SSL を終了する場合に、トラフィックを再暗号化しなければ、TIM に対する負荷はほとんどのケースでさらに大幅に軽減されます。

Resonate など、一部の負荷分散環境では、サーバを MAC アドレスで識別できる可能性もあります。ただし、多くの環境では、返されるサーバ IP アドレスおよびサーバ MAC アドレスは、ネットワークロード バランサの仮想 IP アドレス (VIP) のものです。

TIM はエビデンス コレクションにサーバの IP アドレスを使用するため、挿入場所 D の使用には大きなメリットがあり、デメリットは実質的にありません。挿入場所 D は TIM の推奨挿入場所です。

ネットワーク ロード バランサと Web サーバの間

挿入場所 E は、ネットワーク ロード バランサと 1 つ以上の Web サーバの間で、通常はクライアント IP アドレスを認識できます。このため、ネットワーク ロード バランサがプロキシとして動作している場合は、ネットワーク ロード バランサで「ソースアドレスの保持」を有効にする必要があります。挿入場所 E では、ほとんどの場合サーバの IP アドレスを認識できます。



ネットワーク ロード バランサが永続接続を使用している場合、TIM をここに配置すると TIM に対する負荷が軽減されます。負荷の軽減にはオープン接続を削減するという働きがあるので、重要になる可能性があります。ネットワーク ロード バランサがクライアントに代わって SSL を終了する場合に、トラフィックを再暗号化しなければ、TIM に対する負荷はほとんどのケースでさらに大幅に軽減されます。

TIM はエビデンス コレクションにサーバの IP アドレスを使用するため、挿入場所 E の使用には大きなメリットがあります。ただし、挿入場所 E には挿入場所 D にはないデメリットがいくつかあります。Web サーバの数が多いと、挿入場所の数も多くなります。このため、挿入場所 E でのタップの使用は事実上不可能になる可能性があります。

ポート ミラーリングが使用されている場合は、挿入場所 D と挿入場所 E は機能的に同等です。多くの場合、挿入場所 E を使用するために必要なことは、仮想 LAN (VLAN) の展開のみです。挿入場所 D の場合は、単純なポート ミラーリングを使用できる可能性があります。

ブラウザから Enterprise Manager への接続

デフォルトでは、HTTP 接続がブラウザと Enterprise Manager の間で許可されます。

ただし、SSL 接続のみを許可するように Enterprise Manager へのアクセスを制限することができます。「CA APM セキュリティ ガイド」を参照してください。

IPv6 と CA CEM

このセクションでは、インターネットプロトコルバージョン 6 (IPv6)、IPv6 ネットワーク上の CA CEM 向けのマシン設定ページ、および CA CEM での IPv6 のアドレス形式について簡単に説明します。

- [IPv6 の概要](#) (P. 305)
- [CA CEM での IPv6](#) (P. 306)
- [IPv6 ネットワーク トラフィックの監視](#) (P. 306)
- [デュアルスタック \(IPv6 および IPv4\) ホストでの CA CEM の実行](#) (P. 306)
- [IPv6 の有効なアドレス形式](#) (P. 309)

IPv6 の概要

インターネットプロトコルバージョン 4 (IPv4) のアドレスは、今後数年以内に使い尽くされる見込みです。IPv6 により、利用可能なインターネットアドレスの数は増加します。

IPv6 アドレスは 128 ビット (16 バイト) です。通常は、基数 16 (16 進数) で作成され、各 16 ビットグループはコロン (:) で区切られます。たとえば、2001:0db8:30d2:55c9:06ff:e579:5aa4 となります。

対照的に、IPv4 アドレスは 32 ビット (4 バイト) です。通常は、基数 10 で作成され、各バイトはドット (.) で区切られます。たとえば、172.24.131.197 です。

CA CEM での IPv6

CA CEM での IPv6 サポートには 2 つの面があります。

- IPv6 ネットワーク トラフィックの監視
- IPv6 ネットワークでの CA CEM の設定

これらの 2 つの面は相互に依存しません。たとえば、IPv4 ネットワークに CA CEM マシンを配置して、IPv6 ネットワーク トラフィック および IPv4 ネットワーク トラフィックを監視することができます。同様に、IPv6 (またはデュアルスタック) ネットワークに CA CEM マシンを配置して、IPv6 ネットワーク トラフィック および IPv4 ネットワーク トラフィックを監視することができます。

IPv6 ネットワーク トラフィックの監視

CA CEM は、IPv4 アドレスと IPv6 アドレスの両方をサポートします。フィールドに IP アドレスまたはサブネット マスクを入力する場合は、IPv4 アドレスまたは IPv6 アドレスのどちらかを入力できます。

IPv6 ネットワーク トラフィックを監視する方法

- IPv4 トラフィックを監視する場合と同じ方法で CA CEM を設定します。必要に応じて、IPv4 アドレス (およびホスト名) の代わりに IPv6 アドレス (およびホスト名) を入力します。

「[IPv6 の有効なアドレス形式 \(P. 309\)](#)」を参照してください。

デュアルスタック (IPv6 および IPv4) ホストでの CA CEM の実行

CA CEM を設定してインストールする場合は、SE またはサポート担当者からの指示、または「CA APM インストールおよびアップグレードガイド」に記載されている手順に従ってください。デュアルスタックのホストとして、IPv4 アドレス および IPv6 のアドレスが Enterprise Manager および TIM の各マシンに割り当てられます。

重要: TIM に IPv6 アドレスを割り当てる場合は、TIM コレクション サービスを実行する Enterprise Manager にも IPv6 アドレスを割り当てる必要があります。同様に、TIM に IPv4 アドレスを割り当てる場合は、TIM コレクション サービスを実行する Enterprise Manager にも IPv4 アドレスが必要です。

この重要な制約は、たとえば、CA CEM コンソールでは以下のように適用されます。

- 有効な TIM が IPv6 アドレスの場合、IPv4 アドレスの Enterprise Manager で TIM コレクション サービスを実行することはできません（その逆の場合も同様です）。
- 有効な TIM が IPv6 アドレスの場合、IPv4 アドレスの TIM を有効にすることはできません（その逆の場合も同様です）。
- TIM コレクション サービスを実行している Enterprise Manager の IP アドレスの変更が原因で Enterprise Manager と有効な TIM の間でアドレスタイプの不一致が生じる場合は、IP アドレスを変更することはできません。
- 別の Enterprise Manager への TIM コレクション サービスの移動が原因で Enterprise Manager と有効な TIM の間でアドレスタイプの不一致が生じる場合は、移動することはできません。

構成の確認、変更、またはトラブルシューティングを行う必要がある場合は、以下の手順に従います。

TIM 上の CA CEM の IPv6 設定を確認または変更する方法

1. TIM の [Wily System Setup] ページにアクセスします（「[TIM の \[Wily System Setup\] ページへのアクセス](#) (P. 291)」）。
2. [Wily System Setup] ページで、[Machine Settings] の [Configure IPv6] を選択します。IPv6 アドレスが正しく割り当てられていること、および IPv6 が有効であることを確認します。

[IPv6 Setup] ページについての注意点を以下に示します。

- グローバル スコープの IPv6 アドレスは IPv4 アドレスに類似しています。
- RADV および DHCPv6 は、マシンに複数のグローバル IPv6 アドレスを割り当てることができます。しかし、手動で割り当てることができるアドレスは 1 つのみです。

- IPv6 アドレスを手動で割り当てる場合、ネットワークプレフィックスの長さを示すためにスラッシュを使用して表記します（これは、IPv4 ネットワークのサブネットマスクの指定に似ています）。
 - [Click to disable] ボタンは、トラブルシューティング用です。たとえば、IPv6 ネットワーク上の CA CEM マシンと通信できない場合は、IPv6 がシステム全体、およびマネジメントネットワークに接続されているインターフェース (ethn) の両方で有効であることを確認します。
3. IPv4 の設定が正しく割り当てられることを確認します。 [Machine Settings] に戻り、 [Network Setup] を選択します。

デュアルスタック Enterprise Manager の IP アドレスを変更する方法

- 「[Enterprise Manager の IP アドレスの編集 \(P. 318\)](#)」を参照してください。

CA CEM コンソールを参照するようにブラウザを設定する方法

- コンソールの URL でリテラル IP アドレスを使用している場合は、角かっこ ([]) を使用して IPv6 アドレスを表記します。
パスの例については、「[IPv6 の有効なアドレス形式 \(P. 309\)](#)」を参照してください。

IPv6 の有効なアドレス形式

IPv6 アドレスに使用する表記は、CEM コンソールを使用しているか、または [Wily System Setup] ページを使用しているかによって異なります。

- CEM コンソール - CEM コンソールに IPv6 アドレスを入力する場合は、以下の指定を除き、圧縮表記を使用することはできません。
 - サブネットマスク（この場合は、圧縮表記およびスラッシュを使用した表記を一緒に使用できます）。
 - [管理] - [記録セッション] ページの [クライアント IP アドレス]（この場合は、圧縮表記および混在表記の両方を使用できます）。

UI で所定の例に従っていることを確認します。

- [Wily System Setup] ページ - [Wily System Setup] ページ ([IPv6 Setup] ページなど) では、圧縮表記だけでなく、より長い表記を使用して IPv6 アドレスを指定できません。

[IPv6 Setup] ページでは、サブネットマスクではなくプレフィックスの長さを使用する必要があります（アドレスとの間をスラッシュで区切ります）。

以下の表に、CA CEM で IPv6 アドレスに使用できる表記の例を示します。

| IPv6 アドレスの例 | 表記および注意事項 |
|--|---|
| <code>3fff:ffff:0ed5:0000:0000:0000:2448:78eb</code> | 標準表記 CA CEM 内のどこでも使用できます。 |
| <code>3fff:ffff:ed5:0:0:0:2448:78eb</code> | 16 ビットグループ内で先頭の 0 を省略 CA CEM 内のどこでも使用できます。 |
| <code>3fff:ffff:fed5::2448:78eb</code> | 圧縮表記 CEM コンソールの UI（サブネットマスクでスラッシュを使用して表記する場合を除く）、および [管理] の [記録セッション] ページでは使用しないでください。 |

| IPv6 アドレスの例 | 表記および注意事項 |
|---|---|
| <code>3fff:ffff:fed5:0::/64</code> | スラッシュを使用した表記 サブネットマスク（[設定] - [ドメイン] - [サブネットマスク] および [管理] - [ユーザグループ]）および手動による IPv6 アドレス（[Wily System Setup] - [Machine Settings] - [Configure IPv6]）に使用します。 |
| <code>ffff:ffff:ffff:ffff:0:0:0:0</code> | サブネットマスク サブネットマスク（[設定] - [ドメイン] - [サブネットマスク] および [管理] - [ユーザグループ]）に使用します。 |
| <code>2001:0db8:85a3:08d3:0:0:172.31.124.132</code> | IPv4 と IPv6 の混在表記 [管理] の [記録セッション] ページを除き、CA CEM では使用しないでください。 |

以下の表に、CA CEM で IPv6 パスに使用できる表記の例を示します。

| IPv6 パスの例 | 表記および注意事項 |
|--|---|
| <code>http://cemhost_ipv6:8081/wily</code> | CEM コンソールへのパスの例（ここで、cemhost_ipv6 はホスト名として定義されます）。 |
| <code>http://[2001:db8:85a3:8d3:0:0:370:7348]:8081/wily</code> | CEM コンソールへのパスの例（ここで、Enterprise Manager の IP アドレスは IPv6 です）。 |

第 18 章: CA CEM の管理

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 CEM 管理のプロセス \(P. 311\)](#)
- [Enterprise Manager サービスの配置 \(P. 312\)](#)
- [CA CEM ドメインの定義 \(P. 323\)](#)
- [インシデントコストとビジネス インパクトとの対比 \(P. 329\)](#)
- [インシデント関連設定の定義 \(P. 331\)](#)
- [SMTP サーバ設定の構成 \(P. 341\)](#)
- [新規ビジネス サービスのセキュリティ グループの設定 \(P. 344\)](#)
- [監視の有効化 \(P. 348\)](#)
- [監視の同期 \(P. 348\)](#)
- [前回の同期以降の構成変更の表示 \(P. 349\)](#)

CA CEM 管理のプロセス

CA CEM の管理に関連する主なタスクを以下に示します。

1. 複数の Enterprise Manager 間に Enterprise Manager サービスを配置する。
「[Enterprise Manager サービスの配置 \(P. 312\)](#)」を参照してください。
2. ユーザの認識、ユーザ グループ、トランザクション、およびデータ保持の設定を含め、ドメインを定義する。「[CA CEM ドメインの定義 \(P. 323\)](#)」を参照してください。
3. インシデントの生成、ビジネス インパクトとエビデンス コレクション、インシデントエイジャウトルール、およびインシデント発生時の電子メールについてのインシデント設定を指定する。「[インシデント関連設定の定義 \(P. 331\)](#)」を参照してください。
4. レポートおよびイベント通知についての電子メール設定を定義する。
「[SMTP サーバ設定の構成 \(P. 341\)](#)」を参照してください。
5. 新規ビジネス サービスのデフォルトのセキュリティ グループを設定する。「[新規ビジネス サービスのセキュリティ グループの設定 \(P. 344\)](#)」を参照してください。
6. TIM を有効化する。このタスクは、設定時、および TIM が無効になっている場合に必要です。これにより、コレクタと TIM の間の通信が有効になります。「[監視の有効化 \(P. 348\)](#)」を参照してください。

7. 監視を同期する。このタスクは、TIM にトランザクションおよび障害構成情報を送信し、TIM に最新の構成で監視を開始させる場合に必要です。

また、ビジネス サービスおよびトランザクションに関連する構成変更を Introscope エージェントに送信する場合にも必要です。「[監視の同期 \(P. 348\)](#)」を参照してください。

Enterprise Manager サービスの配置

複数の Enterprise Manager (EM)、つまりコレクタと MOM がある場合は、複数の Enterprise Manager 間に Enterprise Manager サービスを配置することができます。サービスを配置しないと、Enterprise Manager サービスはすべて 1 つの Enterprise Manager 上で実行されるため、パフォーマンスが低下する場合があります。

注: システムに Enterprise Manager が 1 つのみ(スタンドアロン)の場合は、このトピックを省略できます。Enterprise Manager がスタンドアロンの場合は、すべての Enterprise Manager サービスを 1 つの Enterprise Manager 上で実行する必要があります。

複数の Enterprise Manager がある環境で CA APM を起動すると、Enterprise Manager サービスはすべて最初のコレクタで開始されます。すべてのコレクタが起動した後で、適切な Enterprise Manager に Enterprise Manager サービスを割り当てることができます。

以下の表に、Enterprise Manager サービスのタスクを実行する場合を示します。

注: Tess サービスは MOM ではなくコレクタで実行されます。

| 処理 | 実行するタスク |
|--|--|
| 初めて CA APM を設定する場合 | Enterprise Manager サービスの配置 (P. 312) Enterprise Manager 構成の変更 (P. 318) |
| 環境に Enterprise Manager を追加する場合 | Enterprise Manager サービスの配置 (P. 312) Enterprise Manager 構成の変更 (P. 318) |
| 環境内の Enterprise Manager の IP アドレスを変更する場合 | Enterprise Manager 構成の変更 (P. 318) |

環境から Enterprise Manager を削除する
場合

[Enterprise Manager サービスの配置](#) (P. 312) (Enterprise Manager をシャットダウンする前に Enterprise Manager から Enterprise Manager サービスを移動する)
[Enterprise Manager の削除](#) (P. 320)

以下の Enterprise Manager サービスを配布できます。

注: クラスタ内では各サービスの 1 つのインスタンス (のみ) を実行することができます。たとえば、TIM コレクションサービスを同時に 2 つの Enterprise Manager 上で実行することはできません。

DB クリーンアップ サービス

データベースから古いデータを削除します。

統計集約サービス

1 日 1 回データベースに統計を集約します。デフォルトでは、集約は深夜に実行されます。詳細については、「[CA CEM レポート集約の概要](#) (P. 383)」を参照してください。

TIM コレクション サービス

TIM がない場合 (つまり、CA APM ではなく Introscope を実行している場合)、このサービスの場所は重要ではありません。

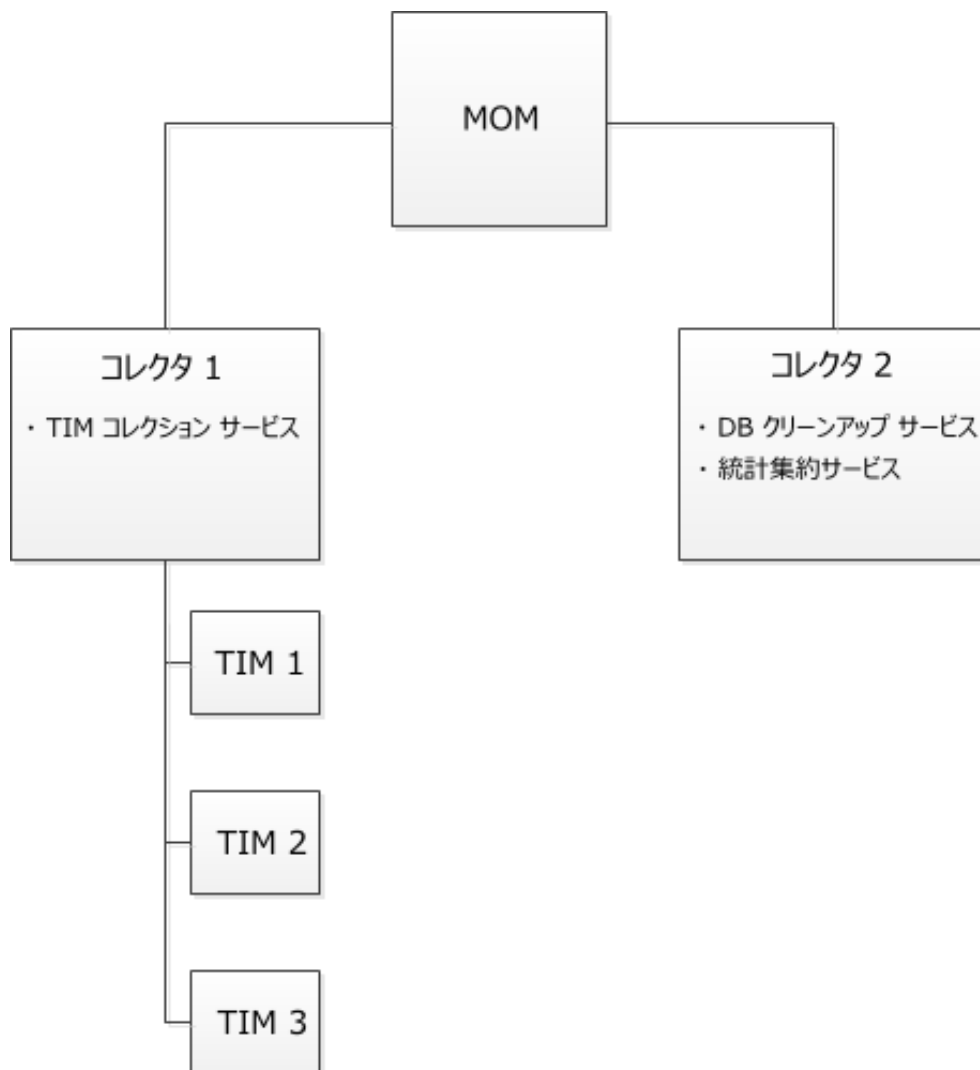
このサービスは、TIM によって収集されたデータを処理するために使用するサービスのグループで構成されます。ログイン、障害、記録、CA CEM イベント、時間単位の統計、カスタマエクスペリエンスメトリック、およびトランザクション検出の各処理についてのサービスが含まれます。

注: TIM コレクションサービスは、Enterprise Manager サービスの中で最も演算的に負荷の高いサービスです。

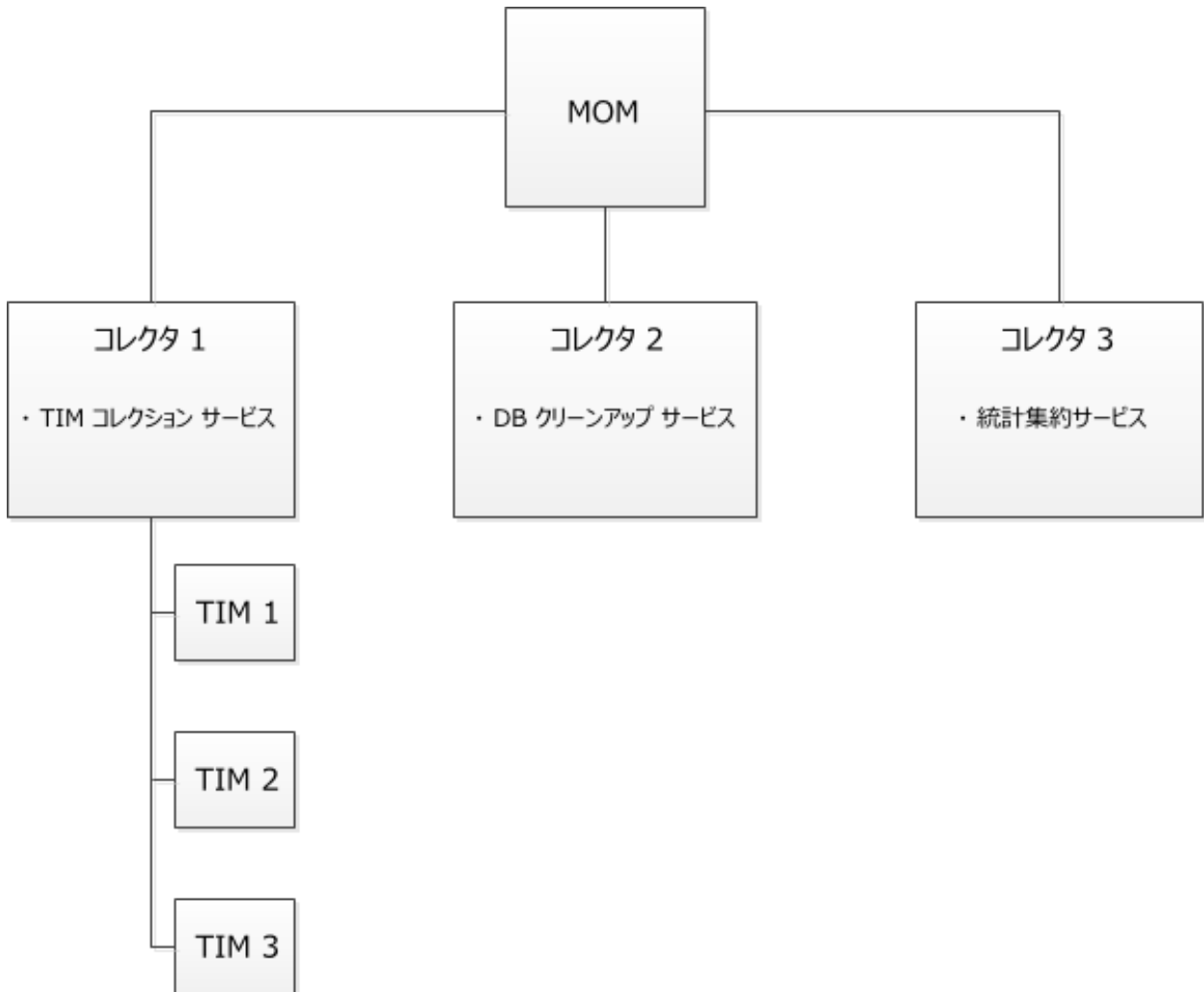
ほかの Enterprise Manager サービスはすべての Enterprise Manager に割り当てられます。これらのサービスは配置できないため、[サービス] ページには表示されません。

Enterprise Manager サービスの標準的な配置

以下の図に、2 コレクタ環境での Enterprise Manager サービスの標準的な配置を示します。



以下の図に、3 コレクタ環境での Enterprise Manager サービスの標準的な配置を示します。



クラスタ化された環境での Enterprise Manager サービスの配置

複数の Enterprise Manager 間で Enterprise Manager サービスを再分散する手順を以下に示します。たとえば、初めて CA APM を起動する場合や、システムとの間で Enterprise Manager を追加または削除する場合に、この手順を実行してください。

重要: Enterprise Manager から Enterprise Manager サービスを削除してから、Enterprise Manager をシャットダウンしてください。

この手順の目的は、複数の Enterprise Manager 間で作業負荷を分散することです。

注: TIM コレクション サービスを別の Enterprise Manager に移動した場合、元の Enterprise Manager に残っている未処理のデータ ファイルは（サービスを元の Enterprise Manager に戻さない限り）処理されません。詳細については、「[不正なファイルのディレクトリの場所の変更 \(P. 640\)](#)」を参照してください。

CA Technologies では、Enterprise Manager サービスの再分散にはピーク時以外の時間を選ぶことをお勧めします。ピーク時にシャットダウンしたりサービスを移動したりすると、処理の遅延が発生することがあります。

クラスタ化された環境で Enterprise Manager サービスを配置する方法

1. [設定] - [サービス] - [サービス構成] を選択します。
[サービス構成] ページに、各サービスを現在実行している Enterprise Manager の概要が表示されます。
2. DB クリーンアップ サービスなど、別の Enterprise Manager に割り当てるサービスをクリックします。
3. Enterprise Manager のリストからサービスの割り当て先の Enterprise Manager を選択し、[保存] をクリックします。

クラスタ内のすべての Enterprise Manager がリストに表示されます。Enterprise Manager が稼働しているかどうかを判別することができます。

注: MOM がリストに表示されない場合

CA Technologies では、TIM コレクション サービスを実行している Enterprise Manager でアンチウイルス ソフトウェアを実行しないことをお勧めします。アンチウイルス ソフトウェアを実行すると、サービスの速度が著しく低下することがあります。

4. 各 Enterprise Manager サービスが目的の Enterprise Manager 上で実行するまで、手順 2 および 3 を繰り返します。
5. [保存] をクリックします。

リアルタイムトランザクション メトリックのための TIM の選択

デフォルトでは、リアルタイム トランザクション メトリック データはすべての TIM から収集されます。ただし、環境内の一部の TIM のみが参加することを指定することもできます。これは、テストやトラブルシューティングの場合に必要なになります。

以下の手順に従います。

1. [設定] - [サービス] を選択します。
2. [TIM コレクション サービス] をクリックします。
3. [TIM コレクション サービス] メニューで、[RTTM コレクション サービス] を選択します（まだ選択されていない場合）。

リアルタイム トランザクション メトリックに参加している TIM には、TIM リストで有効のマークが設定されます。

4. 必要に応じて、リストから TIM を選択またはクリアします。
5. [保存] をクリックします。

自動トランザクション検出のための TIM の選択

自動トランザクション検出を実行している場合、デフォルトでは、すべての TIM からの HTTP トラフィックがスキャンされます。ただし、環境内で自動トランザクション検出に参加する一部の TIM のみを指定することができます。

これは、対象となるトランザクションが特定の TIM のみからアクセスされていることがわかっている場合に必要になります。トランザクション検出をこの TIM に制限すると、検出に関連するオーバーヘッドが他の TIM にかかりません。

自動トランザクション検出に参加する TIM を表示または指定する方法

1. [設定] の [サービス] を選択します。
2. [TIM コレクション サービス] をクリックします。

3. [TIM コレクションサービス] メニューで、[トランザクション検出コレクションサービス] を選択します。

トランザクション検出に参加している TIM には、TIM リストで有効のマークが設定されます。

4. 必要に応じて、リストから TIM を選択またはクリアします。
5. [保存] をクリックします。

Enterprise Manager 構成の変更

Enterprise Manager の説明または IP アドレスを変更する場合は、以下の手順に従います。

説明の編集

デフォルトでは、説明は、Enterprise Manager のホスト名およびポート番号を含むように設定されます。

たとえば、この説明を編集して、マシンのアセット ラベルまたは場所 ID を追加し、マシンの識別に役立てることができます。

Enterprise Manager の説明を変更する方法

1. [設定] - [サービス] - [EM 構成] を選択します。
2. Enterprise Manager を選択します。
3. 説明を編集し、[保存] をクリックします。

Enterprise Manager の IP アドレスの編集

通常は、[EM IP アドレス] フィールドに Enterprise Manager の正しい IP アドレスが自動的に入力されます。

Enterprise Manager の IP アドレスを編集する必要がある場合の例を以下に示します。

- 2つのネットワーク上にあるため、Enterprise Manager コンピュータに2つの IP アドレスがある。[EM 構成] ページに一方の IP アドレスが表示され、[TIM Settings] ページに TessCollectorIpAddr 値または TessIpAddr 値に対するもう一方のアドレスが表示されます。[TIM Setting] ページを表示するには、オプションの手順 6 を参照してください。

- Enterprise Manager が、IPv6 アドレスと IPv4 アドレスの両方を持つデュアルスタック ホストである。有効な TIM が IPv6 アドレスの場合は、TIM コレクションサービスを実行する Enterprise Manager も [EM IP アドレス] フィールドに IPv6 アドレスが表示されている必要があります。

Enterprise Manager の IP アドレスを変更する方法

1. [設定] - [サービス] - [EM 構成] を選択します。
2. Enterprise Manager を選択します。
3. もう一方の Enterprise Manager IP アドレスを選択し、[保存] をクリックします。

このアドレスを編集した後で、IP アドレスを再度変更した場合は、手動で更新する必要があります (Enterprise Manager の再起動時にフィールドが自動的に更新されなくなりました)。

4. [設定] - [監視] を選択します。
5. すべての TIM を無効にしてから有効にします。
 - a. TIM を選択します。
 - b. [無効化] をクリックします。
 - c. [有効化] をクリックします。
6. (オプション) Enterprise Manager が TIM コレクションサービスを実行している場合は、有効な TIM が更新後の IP アドレスを受け取ったことを確認します。
 - a. TIM の IP アドレスをクリックします。

[TIM System Setup] ページが表示されます。
 - b. [Configure TIM Settings] をクリックします。
 - c. TessCollectorIpAddr および TessIpAddr の各設定が正しいことを確認します。これらの設定を直接編集しないでください。

Enterprise Manager の削除

次に、[サービス] ページから Enterprise Manager を削除する方法について説明します。

Enterprise Manager は、起動すると自動的に [サービス] ページに表示されます。ただし、Enterprise Manager の名前は、[サービス] ページから自動的に削除されません。この手順の目的は、使用されなくなった Enterprise Manager の名前を [サービス] ページから削除することです。

Enterprise Manager を削除する方法

1. 削除する Enterprise Manager で Enterprise Manager サービスが実行されている場合は、別の Enterprise Manager にそれらのサービスを移動します。「[Enterprise Manager サービスの配置](#) (P. 312)」を参照してください。
2. Enterprise Manager をシャットダウンします。「*CA APM 設定および管理ガイド*」の「Enterprise Manager の停止」を参照してください。
3. [設定] - [サービス] - [EM 構成] を選択します。
4. Enterprise Manager を選択します。
5. [削除] をクリックします。

削除した Enterprise Manager は [サービス] ページに表示されなくなります。

後でこの Enterprise Manager を再起動すると、[サービス] ページに再び表示されます。

Enterprise Manager サービスのトラブルシューティング

Enterprise Manager サービス問題のトラブルシューティングに役立つと思われるヒントを以下に示します。

症状:

[イベント] ページに、サービスに関連する CA CEM イベントが表示されます。

- TIM コレクション サービスが停止しました
- 統計集約サービスが停止しました
- データベース クリーンアップ サービスが停止しました

解決方法:

Enterprise Manager サービスのいずれかが停止しているので、できる限り早く再起動する必要があります。

そのサービスを実行している Enterprise Manager を再起動してください。

症状:

日単位の統計が集約されていないようです。

レポートに日単位のデータが表示されません。

解決方法:

統計集約サービスが正常に実行されていない可能性があります。

統計集約サービスを実行している Enterprise Manager にある IntroscopeEnterpriseManager ログ ファイルを確認してください。

症状:

Enterprise Manager が TIM から速やかにデータを受信していないようです。

解決方法:

TIM コレクション サービスが正常に実行されていない可能性があります。

TIM コレクション サービスを実行している Enterprise Manager にある IntroscopeEnterpriseManager ログ ファイルを確認してください。

症状:

コレクタが TIM から情報を受け取っていません。

たとえば、TIM ログに以下のようなエラーメッセージがあります。

```
ERROR There is no collector service for this TIM
```

解決方法:

コレクタまたは MOM の IP アドレスが変更された可能性があります、[EM 構成] ページにその変更が反映されていません。

Enterprise Manager を再起動してください。または、「CA APM 設定および管理ガイド」の「[Enterprise Manager の IP アドレスの編集 \(P. 318\)](#)」に記載された手順に従ってください。

症状:

上と同じです (コレクタが TIM から情報を受け取っていません)。
たとえば、TIM ログに以下のようなエラーメッセージがあります。

```
ERROR There is no collector service for this TIM
```

解決方法:

コレクタまたは MOM に IP アドレスが 2 つある可能性があります。この場合、一方の IP アドレスは [EM 構成] ページに表示され、もう一方の IP アドレスは [TIM Settings] ページに表示されます。

[EM 構成] ページおよび [TIM Settings] ページでアドレスの不一致が発生しているかどうかを確認してください。

アドレスが同じではない場合は、「CA APM 設定および管理ガイド」の「[Enterprise Manager の IP アドレスの編集 \(P. 318\)](#)」に記載された手順に従ってください。

症状:

コレクタが稼働しているにもかかわらず、[サービス構成] ページでコレクタの実行状態が [停止中] と表示されています。

解決方法:

MOM とコレクタの間で時間の同期が取れていません。

MOM とコレクタの間で時間を同期します。

詳細については、「CA APM 設定および管理ガイド」の [Enterprise Manager のクロック同期 \(P. 108\)](#)に関するセクションを参照してください。

症状:

コレクタの実行状態が [不明] として表示されています。

解決方法:

コレクタのホスト名と IP アドレスが正しいことを確認します。正しくない場合は、<EM_Home>\config ディレクトリの *IntroscopeEnterpriseManager.properties* ファイルにある *introscope.enterprisemanager.clustering.login.em1.host* プロパティを編集します。IP アドレスが解決可能であることを確認します。localhost は使用しないでください。

CA CEM ドメインの定義

CA CEM ドメインでは、管理者は必要なトランザクション動作、ユーザおよびビジネス インパクト、CA CEM 全体のデータ保持について、CA CEM 全体のデフォルト値および設定を構成できます。

社内に CA CEM 用に定義された 1 つのドメインが必要です。ビジネス サービス、ビジネス トランザクション、およびビジネス アプリケーションは、ドメイン レベルの下に作成されます。デフォルトのドメイン名は [ローカルドメイン] です。

ユーザ グループ、ビジネス サービス、およびトランザクションを作成する場合は、CA CEM ドメインのデフォルト値を継承するか、または特定の値 (たとえば、ユーザに合わせた SLA 設定) を作成するかを選択できます。

CA CEM ドメインを定義する方法

1. [設定] - [ドメイン] を選択します。
2. [ドメイン設定] を定義します。

ドメイン名

CA CEM ドメインに、意味のある名前を付けます。ドメイン名は、大文字と小文字が区別されません。

包括的な障害詳細をキャプチャ

これを選択した場合は、[CEM] - [インシデント管理] - [障害詳細] ページに、クエリおよびポストの各パラメータに関する詳細データと要求および応答の各本文を表示することができます。詳細については、「CA APM セキュリティ ガイド」を参照してください。

[IP サブネット別に障害のトラブルシューティングを行う]

これを選択した場合は、インシデント トラブルシューティング グラフの [ネットワーク層] に、障害の分布がサブネット別に表示されます (ユーザは IP アドレス別に再グループ化されません)。

サブネット マスク

サブネットを定義するには、[IP サブネット別に障害のトラブルシューティングを行う] と一緒にこの機能を使用します。

通常、マスクは 255.255.255.0 に設定されます。ただし、大規模ネットワークでは、255.255.0.0 の方が適切な場合もあります。

3. [ユーザ グループ設定] を定義します。

IP サブネット別にユーザ グループを作成

この機能を使用すると、新しいユーザ グループが、新しいユーザのクライアント IP サブネット別に自動的に作成されます。

重要: インストール環境が大規模な電子商取引サイト（ユーザ数が数十万人または数百万人のサイト）の場合は、この機能を使用しないでください。作成されるユーザ グループの数が、処理できないほど膨大になる可能性があります。詳細については、「[ユーザおよびグループの管理 \(P. 353\)](#)」を参照してください。

サブネット マスク

ユーザ グループを作成するサブネットを定義するには、[IP サブネット別にユーザ グループを作成] と一緒にこの機能を使用します。

通常、マスクは 255.255.255.0 に設定されます。ただし、大規模ネットワークでは、255.255.0.0 の方が適切です。ユーザ グループは、特定の IP アドレスおよびより限定的なサブネット マスクに基づいて作成することにより、さらに絞り込むことができます。「[新規ユーザ グループの管理 \(P. 361\)](#)」を参照してください。

4. [識別設定] を定義します。

[ユーザ認識中にアプリケーションを無視]

このオプションを選択しないと、ユーザはそれぞれのビジネスアプリケーションで一意的になり、ユーザ ID ごとに（ビジネスアプリケーション+ログイン名）統計履歴がカウントされます。例：

- ApplicationOne_MyLoginName = ユーザ ID
- ApplicationTwo_MyLoginName = 別のユーザ ID

- ApplicationThree_MyLoginName= 3 番目のユーザ ID
- eCommApplication_MyLoginName = 4 番目のユーザ ID。ただし、これは電子商取引ビジネス アプリケーションであるため、障害は保持されます。統計は未指定ユーザの履歴に入ります。

ユーザが [ユーザ認識中にアプリケーションを無視] オプションを選択した場合は、ユーザが複数のビジネス アプリケーションにログインしている場合でもユーザは一度のみカウントされます。

重要: 最初のシナリオ (つまり、複数のユーザ ID 収集統計を持つ 1 人のユーザ) であるときに、このオプションを選択してビジネス アプリケーションを無視する場合は、別のユーザ ID を作成します。

- MyLoginName = ユーザ ID (ビジネス アプリケーションにかかわらず、このユーザによる今後のすべてのログインに適用されます)。

この例では、5 つのバケットに保持された、1 人のユーザの統計履歴があります。統計履歴は、データ保持ルールでの設定に従ってデータベースに残ります。

[パス パラメータ デリミタ]

パス パラメータを使用して、ユーザ、セッション、ユーザ グループ、またはトランザクションを識別する場合は、ここでデリミタを指定します。パス パラメータの詳細については、「CA APM トランザクション定義ガイド」を参照してください。

5. [デフォルト トランザクション設定] を定義します。
 - a. [インパクト レベル] を定義します。これによって、トランザクションの障害タイプのビジネス優先度が決まります。

通常は、デフォルト値の [中] で十分です。この値は、デフォルトでは CA CEM ドメインのビジネス サービスに継承されますが、トランザクション レベルで編集できます。

- b. トランザクション サービス レベル アグリーメント (SLA) レベルを定義します。

これらの値は、デフォルトでは CA CEM ドメインのビジネス サービスに継承されますが、トランザクション レベルで編集できます。CA CEM ドメイン レベル SLA のオプションを以下に示します。

成功率 SLA

パーセンテージとして表される成功率サービス レベル アグリーメント。デフォルトは 95 パーセント障害なしのトランザクションです。

シグマ SLA

数値として表されるシグマ サービス レベル アグリーメント。シグマ スコアは、100 万機会あたりの障害数 (DPMO) から計算される測定値です。デフォルトは 4.00 で、ほぼパーフェクトは 6.00、およびパーフェクト (トランザクション障害数ゼロ) は無限大です。

トランザクション時間 SLA

秒数で表されるトランザクション時間サービス レベル アグリーメント。デフォルトは 8 秒 (合計経過時間) です。

ヒント : CA CEM の時間は、1/1000 (0.001) 秒単位で指定できます。これより小さい値 (たとえば、0.0001) を指定すると、CA CEM は値を 0.000 に設定します。

6. [デフォルトユーザ設定] を定義します。
 - a. [インパクトレベル] を定義します。これによって、障害タイプのビジネス優先度が決まります。

通常は、デフォルト値の [中] で十分です。この値は、デフォルトでは CA CEM ドメインのビジネス サービスに継承されますが、ユーザ グループ レベルで編集できます。
 - b. デフォルトのユーザ サービス レベル アグリーメント (SLA) レベルを定義します。

これらの値は、デフォルトでは CA CEM ドメインのビジネス サービスに継承されますが、ユーザ グループ レベルで編集できます。

7. [値の設定] を定義します。

パフォーマンス レポート ([ビジネス サービス] ページおよび [ビジネス トランザクション] ページ) には、[IT 価値] 列を表示する (または表示しない) ことができます。IT 価値は、以下のように計算されます。

IT 価値 = (ビジネス トランザクションあたりの IT 価値) * (ビジネス トランザクション数)

たとえば、正常なビジネス トランザクションあたり 2.00 ドルが計測された場合、これは、成功したトランザクションごとにビジネスに 2.00 ドルの価値があることを意味します。

- a. IT 価値を表示するには、[IT 価値を計算] チェック ボックスをオンにし、[ビジネス トランザクションあたりの IT 価値] に金額を入力します。

このチェック ボックスがオフの場合、[IT 価値] 列はパフォーマンス レポートに表示されません。
 - b. [インシデント コストを計算] チェック ボックスの設定の詳細については、「[インシデントコストとビジネスインパクトとの対比 \(P. 329\)](#)」を参照してください。
8. [データ保持設定] を定義します。

ユーザを非アクティブにするまでの期間

ユーザは、ネットワーク上でトランザクションを生成している限りアクティブです。デフォルトでは、過去 730 日間トランザクションが計測されないと、ユーザは自動的に非アクティブになります。

ヒント：休暇または休職期間とその終了のような要因を検討してください。これらは、適切な日数を判断するのに役立ちます。

統計集約

統計は、1時間ごとにユーザ単位、ユーザグループ単位、およびすべてのユーザに対して集約されます。ユーザ統計およびユーザグループ統計を保持する期間を選択できます。

時間単位でユーザ統計を取る期間

デフォルトでは、時間単位のユーザ統計は3日間保持されます。3日を超えると、日単位または週単位のユーザ統計は参照できますが、3日前より古い時間単位の統計は参照できなくなります。

日単位でユーザ統計を取る期間

デフォルトでは、日単位のユーザ統計は15日間保持されます。15日を超えると、週単位のユーザ統計は参照できますが、15日前より古い日単位の統計は参照できなくなります。

週単位でユーザ統計を取る期間

デフォルトでは、週単位のユーザ統計は27週間保持されます。保持期間が6か月を超える週単位のユーザ統計は破棄されます。

時間単位でユーザグループ統計を取る期間

デフォルトでは、時間単位のユーザグループ統計は3日間保持されます。3日を超えると、日単位または週単位のユーザグループ統計は参照できますが、3日前より古い時間単位の統計は参照できなくなります。

日単位でユーザグループ統計を取る期間

デフォルトでは、日単位のユーザグループ統計は15日間保持されます。15日を超えると、週単位のユーザグループ統計は参照できますが、15日前より古い日単位の統計は参照できなくなります。

週単位でユーザグループ統計を取る期間

デフォルトでは、週単位のユーザグループ統計は27週間保持されます。保持期間が6か月を超えるユーザグループ統計は破棄されます。

警告： データ保持設定の値を大きくしすぎると、日単位の集約に遅れが生じる場合があります。 **IntroscopeEnterpriseManager** ログファイルに、**Enterprise Manager** が昨日の統計レコードではなく数日前の統計レコードを処理していることが示されている場合は、日単位の集約が遅延しています。

9. [保存] をクリックし、すべての設定を保持します。

インシデントコストとビジネスインパクトとの対比

次に、[ドメイン] ページ（[設定] - [ドメイン]）の [インシデントコストを計算] チェックボックスをオンにした場合の影響について説明します。

[インシデント管理] の [インシデント] レポートには、[インシデントコスト] 列または [ビジネスインパクト] 列のどちらかを表示できます。CA CEM はインシデントコストを以下のように定義します。

$$\text{インシデントコスト} = (\text{1 ユーザ 1 分あたりのコスト}) * (\text{ユーザ数}) * (\text{分数})$$

- ここで、分数は、分単位のインシデント継続期間で、ユーザ数は、未指定ユーザとして分類されるユーザを除く、一意のユーザの数です。

注： ユーザがログインする前に発生したエンタープライズトランザクション、およびすべての電子商取引トランザクションは、未指定ユーザグループによるものです。CA CEM トランザクションが未指定ユーザのみによって実行されている場合、CA CEM では [ユーザ] 列に記号が表示され、インシデントコストは 0.00 ドル (1 ユーザ 1 分あたりのコスト * 0 * 分数) になります。

インシデントコストを表示する方法

1. [インシデントコストを計算] チェックボックスをオンにします。

このチェックボックスをオンにすると、インシデントレポートに [ビジネスインパクト] 列は表示されず、代わりに [インシデントコスト] 列が表示されます。

2. [1 ユーザ 1 分あたりのインシデントコスト] に金額を入力します。

たとえば 0.50 ドルと入力した場合に、ビジネスインシデントが 5 人のユーザに対して 10 分間オープン状態であると、ビジネスに対するコストは 25.00 ドルになります。

ビジネスインパクトを表示する方法

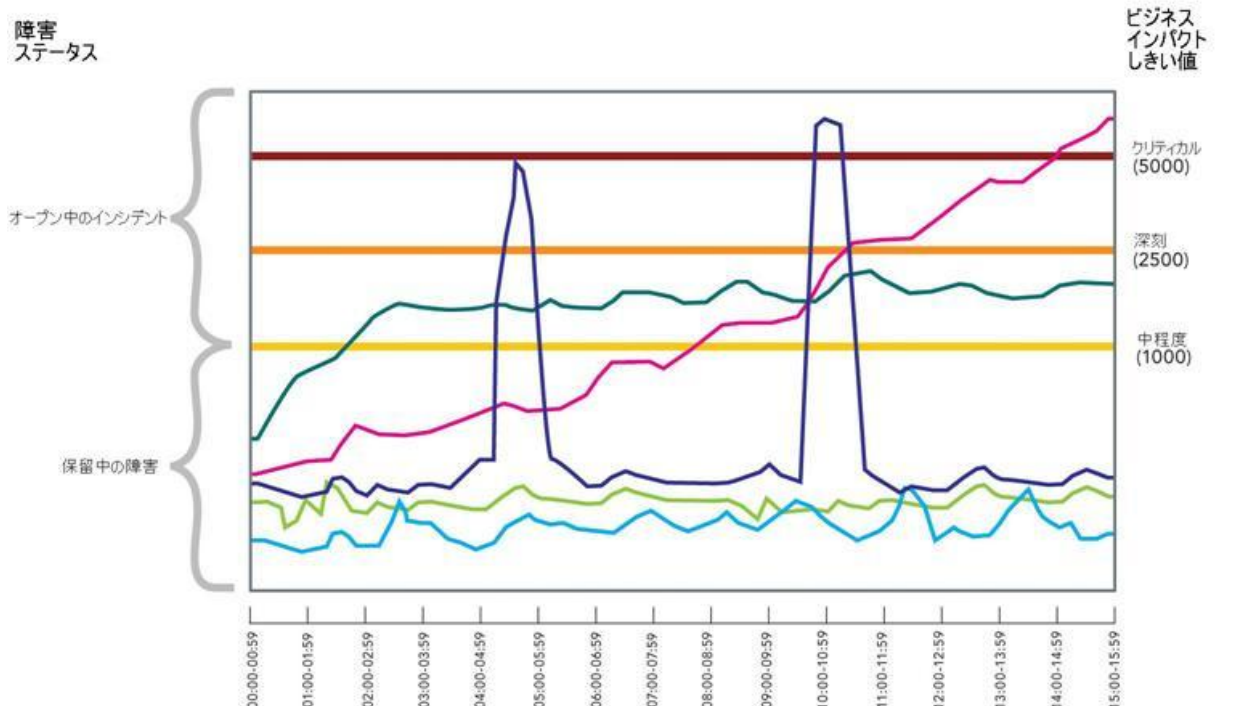
- [インシデントコストを計算] チェックボックスをオフにします。
 - [設定] の [ドメイン] ページで [インシデントコストを計算] チェックボックスをオンにした場合、インシデントレポートには [ビジネスインパクト] ではなく [インシデントコスト] が表示されます。
 - このチェックボックスをオフにすると、インシデントレポートに [インシデントコスト] 列は表示されず、代わりに [ビジネスインパクト] 列が表示されます。
 - [1 ユーザ 1 分あたりのインシデントコスト] テキストボックスに金額を入力する必要はありません。

注: ビジネスインパクトの制限については、「[インシデント関連設定の定義 \(P. 331\)](#)」を参照してください。

インシデント関連設定の定義

多くの環境では、多少の障害があるのは普通のことです。ただし、標準から乖離した変化が見られる場合は把握する必要があります。

標準からの偏差



標準からの偏差がある場合は、インシデント管理設定、インシデント生成ルール、およびインパクト設定を使用して、インシデントを生成することができます。

障害のビジネスインパクト

CA CEM は、障害が発生しているビジネス トランザクション、障害タイプ、およびユーザに基づいて、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

インパクト レベルは、以下のそれぞれに割り当てられます。

- ビジネストランザクション
- 障害タイプ
- ユーザ

| 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 |
| 低 | 3 |
| 中 | 4 |
| 高 | 5 |
| クリティカル | 6 |
| すぐにトリガ | 7 |

インシデントのビジネス インパクト

CA CEM は、受信する障害をインシデントに集約します。インシデントは、ビジネストランザクションおよび障害タイプ別に集約されます。インシデントのビジネス インパクトは、そのインシデントに集約されたすべての障害のビジネス インパクトの合計値と定義されます。このビジネス インパクトはインシデント管理レポートに表示されます。

ビジネストランザクション、障害タイプ、およびユーザの各インパクトがすべて中 (4) の場合は、 $4 * 4 * 4 = 64$ が障害のインパクトです。これがデフォルトで、[インシデント レポート \(P. 329\)](#)のグラフに表示されます。これらのデフォルトのビジネス インパクトを使用する場合は、以下のようになります。

- [中程度] が 1000 に設定されている場合は、16 個の障害で中程度のインシデントが 1 つオープンされます。
- [深刻] が 2500 に設定されている場合は、40 個の障害で深刻インシデントが 1 つエスカレートされます。
- [クリティカル] が 5000 に設定されている場合は、79 個の障害でクリティカルなインシデントが 1 つエスカレートされます。

インシデントの生成方法

インシデントを作成する方法は、2つあります。

- ビジネスインパクトのしきい値に達したときに作成する（これが、デフォルトの方法です）

有効なインシデント生成ルールを作成することによってトリガとする

主要インパクト要因レポート

主要インパクト要因レポートは、ビジネス サービス、ビジネス トランザクション、ユーザ/グループ、およびインシデントを含む、上位5つのインパクトの概要について報告します。

障害レポート

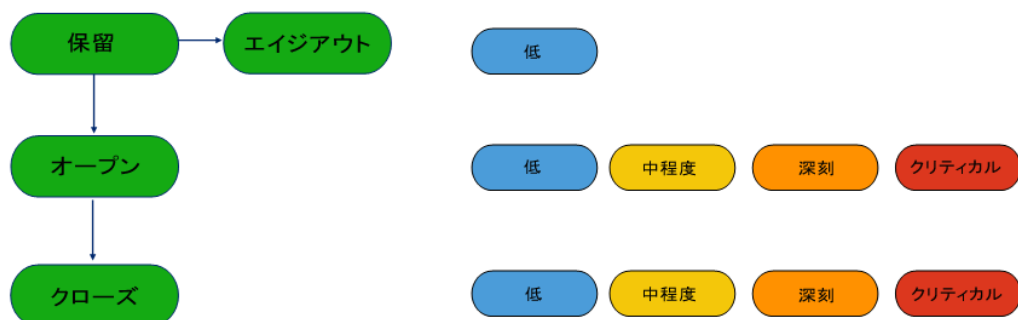
障害レポートには、各障害のビジネスインパクトが示されます。

インシデントのステータスとビジネスインパクトの重大度との対比

インシデントは、そのビジネスインパクトの値に応じて、複数の状態を取ることができます。任意の CA CEM ユーザがインシデントをクローズできます。それぞれの状態の境界は、[設定]の[インシデント設定]ページで、中程度、深刻、およびクリティカルの重大度の設定を使用して定義できます。

以下の図は、インシデントのステータスとビジネスインパクトの重大度を比較したものです。

インシデントのステータス ビジネスインパクトの重大度



インシデント管理設定の構成

インシデント管理の構成は、インシデント生成ルールおよびエイジアウトルールとその論理に直接影響します。

インシデント管理設定を構成する方法

1. [設定] の [インシデント設定] を選択します。
2. [評価間隔 (分)] に分数を入力します。デフォルト値は5分です。
この値がインシデント生成ルールおよびエイジアウトルールで使用されます。たとえば、5分に設定した場合は、5分おきに、アクティブな（有効な）それぞれのルールに従って、インシデントを生成する必要があるかどうか、または保留中のインシデントをエイジアウトする必要があるかどうかを確認されます。
3. [障害を削除するまでの期間] に日数を入力します。デフォルトでは、7日後に障害を削除します。
4. [保存] をクリックし、すべての設定を保持します。

インシデント生成ルールの設定

ビジネスに影響があるときにインシデントを生成するように、カスタマイズしたルールを設定することができます。

CA CEM では、[インパクト設定] で設定された重大度のしきい値に達したときもインシデントが生成されます。「[ビジネスインパクトの設定およびインシデントエビデンスの収集 \(P. 335\)](#)」を参照してください。

インシデント生成ルールを設定する方法

1. [設定] の [インシデント設定] を選択します。
2. 1つのインシデントを生成する必要がある障害の数を入力します。この数値は、短期間における障害数の急増を意味します。
たとえば、5分（評価期間の例）以内の障害数を1000個とするルールを設定することができます。これは、その期間内の障害数がビジネスに大きな影響を与えるためです。
3. インシデントを生成する必要がある障害の増加率（パーセンテージ）を入力します。この値は、短期間における障害率の急増を意味します。

4. 結合ルールを入力します。
 - インシデントを生成する必要がある障害の数。
 - 評価間隔の数（たとえば、前述の場合は 2（/3））。
 - 評価間隔のもう一方の数（たとえば、前述の場合は（2/） 3）。

この例では、3 回の評価間隔の最後の 2 回（または、評価間隔が 5 分の場合は、10/15 分）における障害数を 500 個とするルールを設定できます。
5. アクティブ化するそれぞれルールの隣にある [有効化] チェック ボックスをオンにします。

CA CEM は、評価間隔に基づいて（たとえば、5 分おきに）すべての有効なルールを確認します。

注: インシデント生成ルールでは AND 論理が使用されます。つまり、CA CEM がインシデントを生成するまで、すべての有効なルールが満たされている必要があります。
6. [保存] をクリックし、すべての設定を保持します。

ビジネス インパクトの設定およびインシデント エビデンスの収集

インパクトの設定では、インシデントを生成すると同時に、インシデント重大度レベルを決定するしきい値を設定できます。エビデンス コレクションの設定では、高度なエビデンス コレクション スクリプトをデプロイできます。

CA CEM は、インシデントの重大度を変更されるたびにエビデンス コレクション スクリプトを実行するように設定できます。

| スクリプト | 実行される場合 |
|-------------------------|-------------------------------|
| オープン時にエビデンスを収集する | インシデントがオープンした場合 |
| 重大度中程度の場合にエビデンスを収集する | インシデントの重大度が低から中程度に変更された場合 |
| 重大度深刻の場合にエビデンスを収集する | インシデントの重大度が中程度から深刻に変更された場合 |
| 重大度クリティカルの場合にエビデンスを収集する | インシデントの重大度が深刻からクリティカルに変更された場合 |

CA CEM でエビデンスを収集する前に、システムに Python または Perl をインストールしてください。次に、CA CEM プロパティの `python.path` または `perl.path` を変更して、Python または Perl のインストール場所を指定してください。

注: このトピックでは、インシデントのエビデンスの収集について説明します。CA Technologies プロフェッショナルサービスでは、個別の障害のエビデンスを収集し表示することができます。詳細については、「[\[その他障害情報\] リンクのディレクトリパスの設定 \(P. 636\)](#)」を参照してください。

以下の手順に従います。

1. TIM コレクションサービスを実行する Enterprise Manager に Python または Perl をインストールします。
2. `tess-customer.properties` ファイルを編集し、`python.path` プロパティまたは `perl.path` プロパティを変更します。

たとえば、`python.path=/usr/bin/python` または `perl.path=C:¥¥perl¥¥bin¥¥perl.exe` のようになります。

Windows プラットフォームで円記号を使用する場合、1つの円記号 (¥) はエスケープシーケンスとして解釈されるため、二重の円記号 (¥¥) にする必要があります。

注: `tess-customer.properties` ファイルがまだない場合は、作成してください。

詳細については、「[CA CEM のデフォルトプロパティ \(P. 633\)](#)」を参照してください。

Python または Perl を設定し終わったら、インシデントがオープンしたときまたはインシデントのステータスが変更されたときに実行するエビデンスコレクションスクリプトを作成して有効にすることができます。

インシデントのビジネスインパクトレベルを定義し、エビデンスコレクションスクリプトを設定する方法

1. [設定] の [インシデント設定] を選択します。

デフォルトの設定が表示されます。

2. 中程度、深刻、またはクリティカルなインシデントのインパクト設定を指定します。

これらの設定によって、インシデントが作成される時、およびインシデントの重大度が変更される時の両方が決まります。

デフォルトは、中程度の場合は 1000、深刻の場合は 2500、クリティカルの場合は 5000 です。「[インシデント関連設定の定義 \(P. 331\)](#)」を参照してください。

3. エビデンスコレクション設定を指定します。インシデントのオープン時、または中程度、深刻、またはクリティカルのインシデント時に、エビデンスを収集する場合は、チェックボックスをオンにします。たとえば、中程度のインシデントが検出されたときに以下のスクリプトを実行できます。

`%PYTHON%`

```
C:¥Introscope¥cem¥customer¥evidencecollectors¥evidence.py %ACTION% %SEVERITY%  
%DEFECTID% %TRANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
```

`%PERL%`

```
cem/customer/evidencecollectors/evidence.pl %ACTION% %SEVERITY% %DEFECTID% %T  
RANID% %TRANDEFID% %SERVER% %CLIENTIP% %OUTPUT%
```

これらの引数については、「[エビデンスコレクションスクリプトで使用する引数 \(P. 338\)](#)」を参照してください。

`python.path` プロパティに指定する場所（前述の「スクリプトに使用する Python または Perl を設定する方法」の手順 2）が、`%PYTHON%` に代入されます。Perl をインストールした場合は、コマンドラインで `%PYTHON%` の代わりに `%PERL%` を使用します。

4. [保存] をクリックし、インパクトレベルおよびエビデンスコレクション設定の変更を保存します。

エビデンス コレクション スクリプトで使用する引数

これらはエビデンス コレクション スクリプトで使用できる引数です。例については、前述の「スクリプトに使用する Python または Perl を設定する方法」の手順 3 を参照してください。

ACTION

OPEN または CLOSE (インシデントがオープンしているか、クローズしているかによって異なる)。

SEVERITY

ビジネスインパクト (低、中程度、深刻、またはクリティカル)。

DEFECTID

インシデントのデータベース ID。

TRANID

ビジネス トランザクションのデータベース ID。

TRANDEFID

ビジネス サービスのデータベース ID。

SERVER

最新の障害が検出されたサーバの IP アドレス (障害は複数のサーバで発生していることもあります)。ただし、この引数に取り込まれるのは、最新のサーバの IP アドレスのみです。

CLIENTIP

最新の障害が検出されたクライアント (ユーザの PC) の IP アドレス (障害は複数のクライアントで発生していることもあります)。ただし、この引数に取り込まれるのは、最新のクライアントの IP アドレスのみです。

OUTPUT

エビデンス コレクション スクリプトの出力を入れる場所。

エビデンス コレクションのサンプルスクリプト ファイルは、製品と一緒に `cem/customer/evidencecollectors/evidence-example.py` にインストールされています。
このスクリプトでは、引数の使用法が示されています。

インシデントエイジアウト ルールの設定

インシデントエイジアウトルールでは、下位の保留中のインシデントを取り除くことができます。

保留中のインシデントをいつエイジアウトするかを決定するカスタマイズしたルールを設定できます。

保留中のインシデントとは、発生したが、インパクトのしきい値に達していないために CA CEM ではまだインシデントとして報告されていない障害イベントです。たとえば、ビジネスインパクトのしきい値が 1000 で、999 のみのビジネスインパクトが計測された場合、そのインシデントは保留中です。

保留中のインシデントのエイジアウトルールを設定する方法

1. [設定] の [インシデント設定] を選択します。
2. 保留中のインシデントがエイジアウトするまでの期間 (分数) を入力します。この間に関連する障害が発生しなければ、エイジアウトが行われます。たとえば、1 日の場合は、1440 分 (60 分 * 24 時間 = 1440) と入力します。
3. 保留中のインシデントがエイジアウトするまで期間 (分数) を入力します。この間、インシデントが保留中の状態が継続すれば、エイジアウトが行われます。
4. 結合ルールを入力します。
 - 保留中のインシデント内の超えてはならない障害の数。
 - 評価間隔の数 (たとえば、9 (/10))。
 - 評価間隔のもう一方の数 (たとえば、(9/) 10) 。

この例では、10 回の評価間隔の最後の 9 回 (または、評価間隔が 5 分の場合は、45/50 分) における障害数を 500 個とするルールを設定できます。

5. アクティブ化するそれぞれルールの際にある [有効化] チェック ボックスをオンにします。

CA CEM は、評価間隔に基づいて（たとえば、5 分おきに）すべての有効なルールを確認します。

注: インシデント エイジャウト ルールでは OR 論理が使用されます。つまり、任意の有効なルールがあれば、CA CEM はインシデントをエイジャウトすることができます。

6. [保存] をクリックし、すべての設定を保持します。

インシデントのオープン時または重大度の変更時の電子メールの送信

インシデントがオープンしたときまたはインシデントの重大度を変更されたときに電子メールを送信するように CA CEM を設定することができます。たとえば、インシデントがクリティカルになるたびにインシデント アナリストに電子メールを送信するように CA CEM を設定できます。

注: 電子メールは重大度低のオープン インシデントに対しては生成されません。

以下の手順に従います。

1. [設定] - [インシデント設定] を選択します。
2. [インシデント電子メール設定] セクションで、必要に応じてフィールドを編集します。

電子メールを複数のアドレスに送信するには、カンマ (,) を使用して電子メールアドレスを区切ります。

3. [保存] をクリックし、すべての設定を保持します。
4. 電子メールを送信するように CA CEM が設定されていることを確認します。「[SMTP サーバ設定の構成 \(P. 341\)](#)」を参照してください。

CA CEM は以下の情報を含む電子メール通知を CEM 管理者に送信します。

- インシデント ID
- 影響を受けているビジネス アプリケーション
- 影響を受けているビジネス サービス
- 影響を受けているビジネス トランザクション
- 影響を受けたユーザ グループ数
- 影響を受けたユーザ数
- 障害数
- 障害名
- 初回発生障害
- 最終発生障害

SMTP サーバ設定の構成

CA CEM が電子メールでレポートを送信できるように、SMTP サーバの名前およびポート番号を指定する必要があります。また、添付レポートを付ける電子メールの件名およびメッセージテキストも設定できます。レポートについては、「[CA CEM のレポート機能 \(P. 383\)](#)」を参照してください。

これらの SMTP 設定は、CA CEM のイベントおよびインシデントの電子メール通知にも使用されます（「[イベントの電子メール通知の受信 \(P. 377\)](#)」および「[インシデントのオープン時または重大度の変更時の電子メールの送信 \(P. 340\)](#)」を参照してください）。

保存する前に電子メール接続をテストする必要があります。

以下の手順に従います。

1. [システム] の [電子メール設定] を選択します。
2. [SMTP サーバ設定] を定義します。

ホスト名

SMTP サーバのホスト名を入力します。

ポート

SMTP サーバのポート番号を入力します。

差出人アドレス

これは、テスト接続電子メールに差出人として表示されるアドレスです。

宛先

これは、テスト接続電子メールの送信先アドレスです。デフォルトでは、このアドレスと差出人アドレスは、**Embedded Entitlements Manager** の **CA CEM** ユーザ (オペレータ) の詳細から取得されます。このアドレスがない場合は、**tess-default.properties** ファイルの **email.defaultFromAddress** プロパティが使用されます。このデフォルトを変更するには、「[email.defaultFromAddress \(P. 643\)](#)」を参照してください。

必須の認証

SMTP サーバがユーザ名とパスワードを必要とする場合は、このチェックボックスをオンにします。

ユーザ名

認証が必須の場合に、ユーザ名を入力します。

パスワード

認証が必須の場合に、パスワードを入力します。

3. [電子メール設定] を定義します。

件名

電子メールでレポートを送信する場合の標準件名行を入力します。

メッセージ

電子メールでレポートを送信する場合の標準メッセージを入力します。

フッタ テキスト

電子メールで送信するレポートの一番下に表示する標準テキストを入力します。

4. [接続をテスト] をクリックします。以下の 3 つのいずれかが発生します。
 - 確認メッセージが表示され、テストが成功したことを示す電子メールを受信した場合、SMTP 設定および宛先アドレスの両方が適正です。
 - 確認メッセージは表示されたが、電子メールを受信しなかった場合は SMTP 設定は適正ですが、宛先アドレスが正しくありません。
 - エラーメッセージが表示された場合は、SMTP 設定が正しくありません (SMTP サーバがタイムアウトになるまで待つ必要がある場合は、メッセージが表示されるまで時間がかかることがあります)。
5. [保存] をクリックします。

注: レポート用の電子メールを設定していないと、CA CEM ユーザがレポートを作成しようとしたときにエラーメッセージが送信されます。

レポートのタイプ、およびレポートの設定およびスケジュールを行う場合の CA CEM ユーザ オプションの詳細については、「[CA CEM のレポート機能 \(P. 383\)](#)」を参照してください。

新規ビジネス サービスのセキュリティグループの設定

組織で **Embedded Entitlements Manager** をデプロイ済みの場合は、アクセスポリシーを使用して、ビジネス サービスおよびその関連データへのアクセス権限を持つセキュリティグループを制御することができます。

セキュリティグループは **Embedded Entitlements Manager APM** アプリケーション向けに作成されたユーザのグループです。 **Embedded Entitlements Manager** では、セキュリティグループはアプリケーショングループと呼ばれます。

管理者が、新たに作成されたすべてのビジネス サービスへのアクセス権限を自動的に取得するセキュリティグループを設定します。

デフォルトでは、以下の4つのアクセスポリシーが設定されています。

ビジネス サービス - すべての権限

CEM システム管理者グループには、すべてのビジネス サービスに対するすべての権限が付与されます。

ビジネス サービス - 読み取り/書き込み

CEM 構成管理者グループには、すべてのビジネス サービスに対する読み取りおよび書き込みの権限が付与されます。

ビジネス サービス - 機密データの読み取り

CEM インシデントアナリストグループには、すべてのビジネス サービスに対する機密データの読み取り権限が付与されます。

ビジネス サービス - 読み取り

CEM アナリストおよび CEM インシデントアナリストグループには、すべてのビジネス サービスに対する読み取り権限が付与されます。

標準のセキュリティグループ（CEM システム管理者、CEM 構成管理者、CEM インシデントアナリスト、CEM アナリスト）を使用している場合は、これらのアクセスポリシーで十分です。しかし、追加のセキュリティグループを作成し、それらのグループのメンバにすべてのビジネス サービスのアクセス権限を付与する場合は、それらのグループを含むようにアクセスポリシーを作成または変更する必要があります。

注: このトピックの手順では、すべてのビジネス サービスに対するアクセス ポリシーを変更または作成する方法について説明します。特定のビジネス サービスに対するアクセス ポリシーを変更または作成する場合は、「CA APM トランザクション定義ガイド」を参照してください。

すべてのビジネス サービスに対する既存のアクセス ポリシーを表示または編集する方法

1. [セキュリティ] の [アクセス ポリシー] を選択します。
CA CEM のインストール後にアクセス ポリシーを追加していない場合は、以下に示すアクセス ポリシーが表示されます。
2. 表示または編集するポリシーの名前をクリックします。
[更新アクセス ポリシー] ページが表示されます。
3. [更新アクセス ポリシー] ページのフィールドを変更し、[保存] をクリックします。

以下に、そのフィールドについて説明します。

[ビジネス サービス] で [すべて] を選択していることを確認します。これは、選択されたセキュリティグループが、これ以降に作成されるすべてのビジネス サービスに関連付けられ、既存のすべてのビジネス サービスに適用されることを意味します。

すべてのビジネス サービスに対する新規アクセス ポリシーを作成する方法

1. [セキュリティ] の [アクセス ポリシー] を選択します。
2. [新規] をクリックします。
3. [新規アクセス ポリシー] ページのフィールドに入力し、[保存] をクリックします。

以下に、そのフィールドについて説明します。

注: [ビジネス サービス] で [すべて] を選択し、[セキュリティグループ] で [選択] を選択していることを確認します。これは、選択されたセキュリティグループがすべての（既存およびこれ以降の）ビジネス サービスに関連付けられることを意味します。

次に、[新規アクセス ポリシー] ページのフィールドについて説明します。

アクセス ポリシー名

ポリシーに意味のある名前を付けます。

説明

説明的なコメントを追加します。

ポリシー オプション

ビジネス サービスに対するアクションを明示的に許可または拒否するポリシーを作成する場合に選択します。

許可と拒否の間で競合が発生した場合は、拒否ポリシーが優先されます。

有効

ポリシーを適用する場合は、ポリシーを有効にします。

現在は使用する必要がないが、将来的に使用する可能性がある場合は、ポリシーを無効にします。二度と使用しないポリシーは削除します。

書き込み

セキュリティグループのメンバが、[ビジネス サービス] タブから、ビジネス サービスおよびそのすべての子オブジェクト(ビジネス トランザクション、トランザクション、コンポーネントなど)を表示、編集、および削除できるようにするには、このチェック ボックスをオンにします。

アクセス権限を持っていないビジネス サービスが1つでもあると、そのユーザに [ビジネス サービス] タブは表示されません。

読み取り

セキュリティグループのメンバが、[CEM] タブでそのビジネス サービスに関連付けられたグラフおよびレポートを表示できるようにするには、このチェック ボックスをオンにします。

注: Embedded Entitlements Manager が、構成されている唯一の領域である必要があります。ローカル領域が (Embedded Entitlements Manager 領域のほかに) 構成されている場合は、すべてのユーザが、スケジュール済みレポート内のすべてのデータにアクセスできます。領域の詳細については、「CA APM セキュリティガイド」を参照してください。

機密データの読み取り

セキュリティグループのメンバが、障害に関連するホスト、URLパス、TCPポート、Cookie、およびHTTPヘッダを参照できるようにするには、このチェックボックスをオンにします。これらの情報は、[CEM] - [インシデント管理] - [障害詳細] ページに表示されます。

[包括的な障害詳細をキャプチャ] チェックボックス ([設定] の [ドメイン] ページ) がオンの場合、障害についてのクエリおよびポストの各パラメータと要求および応答の本文情報も [障害詳細] ページに表示されます。詳細については、「CA APM セキュリティガイド」の CA CEM の章を参照してください。

このオプションは [読み取り] チェックボックスと一緒に使用してください。 [障害詳細] ページを表示するには読み取りアクションが必要です。

ビジネス サービス

[すべて] を選択します。これを選択した場合、アクセスポリシーはすべてのビジネス サービス、および新規ビジネス サービスが作成された場合はすべての新規ビジネス サービスに適用されます。

注: 特定のビジネス サービスのアクセスポリシーを変更するには、詳細について「CA APM トランザクション定義ガイド」を参照してください。たとえば、1つの特定のビジネス サービスに対するアナリストのアクセス権限を拒否する場合は、CEM アナリストおよび CEM インシデントアナリストの各セキュリティグループのそのビジネス サービスに対して明示的拒否を設定します。

セキュリティグループ

[選択] を選択し、ポリシーのセキュリティグループを [選択] 列に移動します。

ここに表示されるセキュリティグループは、Embedded Entitlements Manager の APM アプリケーション固有のユーザグループに対応します。Embedded Entitlements Manager グローバルユーザグループは、CA CEM では選択できません。

セキュリティグループを表示または変更するには、Embedded Entitlements Manager を使用します。Embedded Entitlements Manager の使用方法の詳細については、「CA APM セキュリティガイド」を参照してください。セキュリティグループは CEM コンソールからは管理できません。

監視の有効化

トランザクションを監視できるように TIM が有効になっていることを確認する必要があります。TIM 監視が無効であると Enterprise Manager にデータが送信されません。

TIM を有効にする必要があ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（「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）。
- 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（「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）。
- 構成をインポートした後（「[APM データベース構成のインポート](#) (P. 66)」を参照してください）。

Enterprise Manager と TIM との通信を有効にする方法

1. [設定] - [監視] を選択します。
2. 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。

監視の同期

監視を同期することで、現在のドメイン構成ファイルを有効なすべての TIM およびエージェントに送信します。ドメイン構成ファイルには、トランザクション定義、障害規格、および Introscope トランザクション追跡パラメータが含まれます。

監視を同期する必要がある場合の例を以下に示します。

- CA CEM でビジネス サービスを作成または更新した後。CA CEM でのビジネス サービスおよびトランザクションの変更は、監視が同期されて、変更されたビジネス サービスのいくつかのメトリックが生成されるまで、Workstation にも WebView Investigator ツリーにも表示されません。
- TIM を設定して Enterprise Manager に関連付ける場合（「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）。

- 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（「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）。
- トランザクション定義の作成または変更後に、更新された定義をエージェントまたは有効な TIM に送信する場合（「CA APM トランザクション定義ガイド」を参照してください）。
- 構成ファイルのインポート後に、インポートされた定義をエージェントまたは有効な TIM に送信する場合（「[APM データベース構成のインポート](#) (P. 66)」を参照してください）。

ネットワーク上で監視を同期する方法

1. [設定] - [監視] を選択します。
2. 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（「[監視の有効化](#) (P. 348)」を参照してください）。
3. 前回の同期以降に構成に加えられた変更を確認する場合は、「[前回の同期以降の構成変更の表示](#) (P. 349)」を参照してください。
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。これで、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、CA CEM 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。

前回の同期以降の構成変更の表示

同期する前に、構成に加えられた変更をリストすることができます。これにより、同期前に変更を確認することができます。

これらのプロパティに(前回の同期以降に)加えられたすべての変更が[ドメイン構成変更履歴] テーブルに表示されます。

- ビジネスアプリケーション定義
- ビジネス サービス定義
- 障害定義
- ビジネス トランザクション定義

- 障害重大度定義
- トランザクション定義
- 障害インパクトレベル
- ユーザ識別パラメータ
- トランザクションパラメータ定義
- セッション識別パラメータ
- 中間セッション識別パラメータ
- トランザクション重要性定義
- ユーザグループ識別パラメータ
- トランザクションコンポーネント定義
- プライベートパラメータ

プライベートパラメータなど、特定のタイプのパラメータを削除すると、オブジェクト名が空白となり、プロパティ変更は「表示するものがありません」と表示されます。これは、オブジェクト名および変更がデータベースから削除されたためです。

前回の同期以降に加えられた構成変更を表示する方法

1. 監視が同期されていないことを確認します。
2. [設定] - [監視] を選択します。
3. [前回の同期以降の変更を表示] をクリックします。
変更履歴テーブルが表示されます。

注: 変更履歴テーブルには、前回の同期以降に加えられた構成変更がリストされます。これは、前回の同期と現在の構成との差異のリストと同じではありません。たとえば、値を5から2に変更した後で5に戻した場合、テーブルに行が生成されないのではなく、2つの行が生成されます。

デフォルトでは、[ドメイン構成変更履歴] テーブルの最大行数は 1,000 行に設定されています。この値を変更するには、「[前回の同期以降の変更のリストアップ数制限 \(P. 553\)](#)」を参照してください。

リストされたすべてのプロパティ値が意味のあるものとは限りません。たとえば、パラメータが作成されたときに表示される、[構成マネージャ] の値には、オブジェクトの内部クラス名が示されます。

第 19 章: CA CEM 上のユーザおよびグループの管理

ユーザおよびグループの管理に関連する主なタスクを以下に示します。

1. CA CEM で使用可能なユーザ グループのタイプの認識
2. トランザクション内の情報によるユーザ グループの自動的な作成
3. IP サブネット別のユーザ グループの自動的な作成
4. 新規ユーザ グループから他のグループへのメンバの割り当て
5. ユーザ グループおよび SLA (サービス レベル アグリーメント) の各設定の構成
6. 一括編集によるユーザおよびユーザ グループの管理
7. ユーザ グループ SLA とビジネス トランザクションとの相関
8. [ユーザ グループの削除 \(P. 370\)](#) または [個々のユーザの非アクティブ化または削除 \(P. 370\)](#)

注: この章の説明における「ユーザ」は、*監視対象アプリケーション*のユーザを指しています。たとえば、*バンキングアプリケーション*の場合、ユーザは、サインインしてアカウントの表示と管理を実行する、銀行のクライアントです。これらのユーザは、アカウントタイプによってグループ化されている場合があります。

CA CEM ユーザが CEM コンソールから利用できるタブやメニュー項目、ビジネス サービスを構成するなどの目的で、CA CEM ユーザをセキュリティ ユーザグループにグループ化する場合の詳細については、「CA APM セキュリティ ガイド」を参照してください。

ユーザグループの概要

ユーザグループとは、個々の各ユーザの設定を個別に構成する代わりに、ユーザの集合の設定を構成できる便利な方法です。ユーザグループは、問題が発生している可能性があるユーザ集団を簡単に識別できるように定義することができます。

新しいユーザグループを手動で作成できるだけでなく、ユーザをユーザグループに手動で移動することもできます。CA CEMには、ユーザグループを自動的に作成する方法も用意されています。ユーザは1つのCA CEMユーザグループのみに属します。

ユーザグループには複数のタイプがあります。

要求属性ユーザグループ

要求内のコンテンツによってグループ化されたユーザ群。

サブネットユーザグループ

ユーザサブネット別に新規ユーザの自動的な割り当てが行われるグループ。

手動作成のユーザグループ

新しいユーザグループ（または別のユーザグループ）からこのタイプのユーザグループへのユーザの移動は手動で行う必要があります。

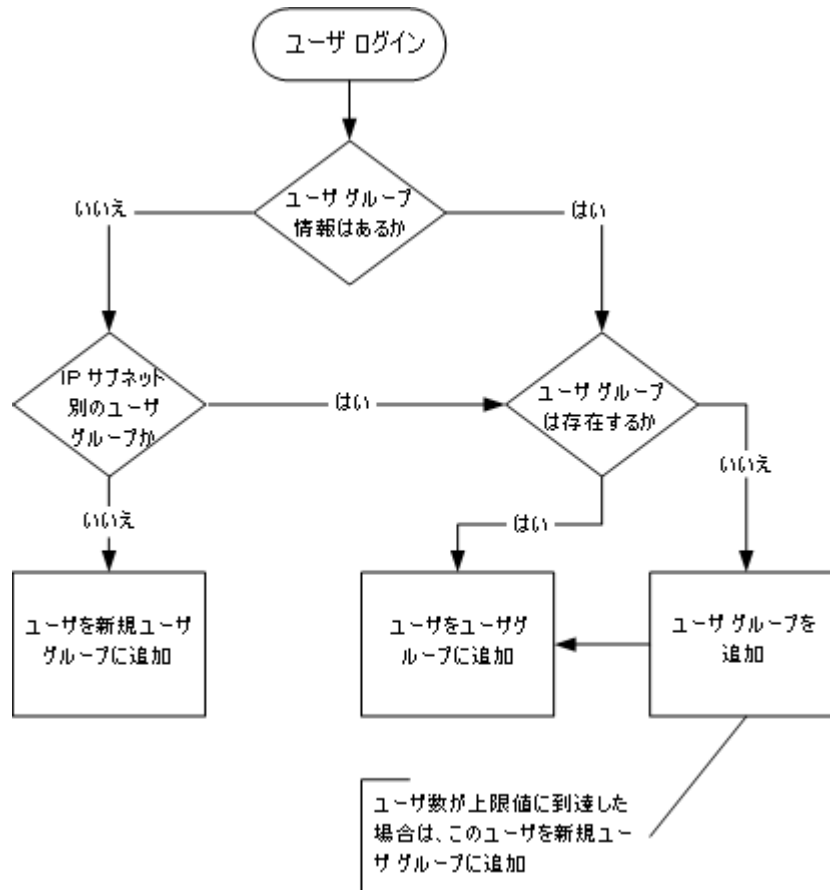
新規ユーザ

自動ユーザグループ生成方法が選択されていない場合、すべての新規ユーザログインは新しいユーザグループに割り当てられます。

未指定ユーザ

電子商取引トランザクションはすべて未指定ユーザグループに割り当てられます。また、ユーザがログインする前に発生したエンタープライズトランザクションも未指定ユーザグループに割り当てられます。

自動的なユーザグループ作成および割り当ての元になっている論理を以下のフローに示します。



ユーザグループの最大数

CA CEM では、自動的に作成されるユーザグループの数を制御できます。この制御は、CEM 管理者が気が付かないうちにグループ数が大幅に増加する可能性がある予期しない状況で役立ちます。

デフォルトでは、自動的に作成されるユーザグループの最大数は 5000 です。デフォルト値を調整するには、[apm-events-thresholds-config.xml](#) (P. 541) ファイルの [introscope.enterprisemanager.max.transaction.user.groups](#) (P. 554) プロパティを設定します。

要求属性別の新規ユーザの自動割り当て

作成している要求内の内容別にユーザをグループ化することができます。よくあるケースを以下に示します。

- URL 文字列 - たとえば、クエリ文字列内のプロパティ コードまたはカスタマ コード
- HTTP ヘッダ - たとえば、各種電話タイプまたは各種ゲートウェイのユーザ
- CA APM TG ヘッダ - たとえば、CA APM TG (x-wtg-info) ヘッダを使用している合成ユーザ

この方法を使用して、CA CEM は、ユーザの場所別または会社別にパフォーマンス情報を報告できます。たとえば、これによって、影響を受ける集団別に機能停止を管理することができます。電子商取引アプリケーションではユーザ グループ統計を使用することができます。

注: ユーザ グループ パラメータ別のグループ化は、サブネット別の自動ユーザ グループ分類に優先します。

重要: インストール環境が大規模な電子商取引サイト（ユーザ数が数十万人または数百万人のサイト）の場合は、注意してこの機能を使用してください。作成されるユーザ グループの数が、処理できないほど膨大になる可能性があります。

重要: ユーザ名ではなく、クライアント IP アドレスによってユーザを識別している場合は、要求属性別にユーザを割り当てないでください。クライアント IP アドレスの使用によるユーザの識別については、「CA APM トランザクション定義ガイド」を参照してください。

要求属性別に新規ユーザを割り当てる方法

1. [管理] の [ビジネス アプリケーション] を選択します。
2. 要求属性によってユーザを識別するビジネス アプリケーションを選択します。
3. [ユーザ グループ識別] を選択します。
既存のすべてのユーザ グループ パラメータのリストが表示されます。
4. [新規] をクリックして、新しいユーザ グループ パラメータを作成します。

5. 適切なパラメータ タイプを選択します。
6. パラメータ名を入力します。
7. [保存] をクリックします。

たとえば、**x-wtg-info** タイプは、**Synthetic** と呼ばれるグループに **CA APM TG** ユーザをグループ化します。これは、実際のトラフィックと **CA APM TG** トラフィックを区別する場合に役立ちます。

サブネット ユーザ グループへの新規ユーザの自動割り当て

ユーザの IP サブネットによってユーザをグループ化することができます。**CA CEM** は、新しいユーザの IP アドレスを既存のユーザ グループのサブネットと自動的に比較します。最も限定的なサブネット マスクが最初に調べられます。たとえば、以下のユーザ グループが定義されているとします。

```
SubGroup - 255.255.255.0 mask / 192.168.2.0 IP start
BigGroup - 255.255.0.0 mask / 192.168.0.0 IP start
```

SubGroup のサブネット マスクの方が限定的であるため、受信 IP トラフィックは最初に **SubGroup** ユーザ グループと比較されます。たとえば、IP アドレス **192.168.2.4** は **SubGroup** グループに割り当てられ、IP アドレス **192.168.9.9** は **BigGroup** グループに割り当てられます。

SubGroup グループにも **BigGroup** グループにも含まれない IP アドレスが検出された場合、そのユーザは構成オプションに従って割り当てられます。たとえば、IP アドレス **192.1.9.9** のサブネット マスクは **255.255.255.0** ですが、これは、どちらのグループの IP アドレス範囲にも当てはまりません。

注: ユーザ グループ パラメータ別のグループ化は、サブネット別の自動ユーザ グループ分類に優先します。詳細については、「[要求属性別の新規ユーザの自動割り当て \(P. 356\)](#)」を参照してください。

新規ユーザのサブネット ユーザ グループの作成

サブネット ユーザ グループは、[設定] の [ドメイン] タブにある [IP サブネット別にユーザ グループを作成] オプションによって決まります。

[設定] の [ドメイン] ページにある [IP サブネット別にユーザ グループを作成] オプションを選択した場合、新しい IP アドレスが検出されると、[新規ユーザ] というグループに割り当てられるのではなく、新しいユーザ グループの作成がトリガされます。

重要: インストール環境が大規模な電子商取引サイト（ユーザ数が数十万人または数百万人のサイト）の場合は、この機能を使用しないでください。作成されるユーザ グループの数が、処理できないほど膨大になる可能性があります。

デフォルトでは、自動的に作成されるユーザ グループの最大数は 5000 です。デフォルト値を調整したい場合は「[デフォルトの tess-default.properties ファイル \(P. 633\)](#)」を参照してください。

新しいユーザ グループの名前は、検出された IP アドレスの先頭の数字になります。この例では、新しいユーザ グループの名前は以下のようになります。

Usergroup-192.1.9.0 - 255.255.255.0 mask/192.1.9.0 address

新たに作成されたユーザ グループを表示する方法

1. [管理] の [ユーザ グループ] を選択します。
2. [Usergroup-192.1.9.0] をクリックして、リストされる新しいユーザを確認します。

注: ある IP アドレスを使用してサブネット ユーザ グループに割り当てられたユーザは、後でその IP アドレスが変更されても、そのユーザ グループに残ります。必要に応じて、元のユーザ項目を手動で移動することができます。

プロキシ サーバを使用するユーザの識別

「[サブネット ユーザ グループへの新規ユーザの自動割り当て \(P. 357\)](#)」で説明したシナリオでは、プロキシサーバを使用するユーザは、クライアント マシンのサブネットではなく、そのプロキシサーバのサブネットに従ってグループ化されます。ビジネス ニーズによっては、これは目的の処理と異なる可能性があります。クライアント サブネットに従ってユーザグループを作成する必要がある場合もあります。

同様に、障害リスト（[インシデント管理] の [障害] ページ）では、クライアント IP アドレスに、プロキシサーバの IP アドレスではなく、親マシンの IP アドレスを表示したい場合もあります。

要求トラフィックに、クライアント IP アドレスを含む HTTP ヘッダがある場合は、ログインおよび障害で接続 IP アドレスではなくクライアント IP アドレスが報告されるように CA CEM を設定できます。X-Forwarded-For、Forwarded-For、および iv-remote-address は、クライアント IP アドレスの識別に使用されるヘッダの例です。ドットで区切られた 10 進数表記の IP アドレス（または標準表記の IPv6 アドレス）が含まれているその他のヘッダも使用できます。例：

```
X-Forwarded-For: 172.24.192.4
```

ProxyForwardHeader という TIM 設定を使用して、ヘッダの名前を指定します。

注: ヘッダがない場合や値が IP アドレスの形式ではない場合は、接続 IP アドレスが使用されます。つまり、動作はデフォルトと同じで、ProxyForwardHeader の設定は指定されません。

TIM ごとに、ProxyForwardHeader の値を、クライアントの IP アドレスを含むヘッダに設定します。

ヘッダの値に基づいて、プロキシ サーバを使用するクライアントを識別する方法

1. TIM システム設定ページにアクセスします。（「[CEM コンソールから TIM へのアクセス \(P. 292\)](#)」）。
2. [Configure TIM Settings] をクリックします。
[TIM Settings] ページが表示されます。
3. [ProxyForwardHeader] をクリックします。

4. [New value] フィールドに、ヘッダ名（コロンなし）を入力し、[Change] をクリックします。

このフィールドでは、大文字小文字が区別されません。

5. 複数の TIM がある場合は、各 TIM について上記の手順を繰り返します。この設定は、その設定が定義されている各 TIM で監視されるすべてのサーバおよびアプリケーションに影響します。

ヘッダの値に基づいて、ユーザ グループを作成する方法

1. 前述の「ヘッダの値に基づいて、プロキシサーバを使用するクライアントを識別する方法」の説明に従って、ProxyForwardHeader を設定します。
2. CEM コンソールで、[IP サブネット別にユーザ グループを作成] オプションが選択されていることを確認します。
 - a. [設定] - [ドメイン] を選択します。
 - b. [IP サブネット別にユーザ グループを作成] を選択します。

これで、接続サブネットではなく、ヘッダに指定されているクライアントサブネットに基づいて、新しいユーザグループが作成されます。また、障害は、送信元が接続 IP アドレスではなく、クライアント IP アドレスとして報告されます。

3. (オプション) プロキシサーバを使用するクライアントの障害を作成して、構成をテストします。障害に関連付けられた IP アドレスがプロキシサーバではなくクライアントの IP アドレスの場合は、構成は適正です。

新規ユーザグループの管理

自動的なユーザグループ作成および割り当て方法のいずれかを設定しなかった場合は、既存のサブネットユーザグループに当てはまらない新しいユーザはすべて「新規ユーザ」グループに自動的に割り当てられます。

新規ユーザを表示する方法

1. 「管理」の「ユーザグループ」を選択します。
2. 「新規ユーザ」グループをクリックして、リストされる新しいユーザを確認します。

検出されているが、まだユーザグループに割り当てられていない新しいユーザが表示されます。

注: トランザクションの監視を開始するまで、新しいユーザは検出されません。

ユーザグループへの新規ユーザの手動割り当て

新しいユーザは、サブネットユーザグループまたは「新規ユーザ」グループに自動的に割り当てられます。

現在のグループからユーザを移動する方法

1. 「管理」の「ユーザグループ」を選択します。
2. 「新規」をクリックして、新しいユーザグループを定義します。
 - a. ユーザグループに意味のある名前（たとえば、ロンドン）を付けます。ユーザグループ名は、大文字と小文字が区別されません。
 - b. グループの説明を入力します。
 - c. 現時点では、その他のパラメータはそのままにしておきます。詳細については、「[ユーザグループの設定 \(P. 362\)](#)」を参照してください。
 - d. 「保存」をクリックし、新しいグループを保存します。
3. 作成したユーザグループをクリックします。トランザクションの監視を開始するまで、またはユーザをグループに移動するまで、新しいユーザは検出されません。
4. 「ユーザグループ」ページに戻り、「新規ユーザ」グループをクリックします。

5. 1人以上のユーザを新規ユーザグループに移動するには、[ログイン名]の左側のチェックボックスをオンにします。
6. [移動先] リストから新しいユーザグループ（たとえば、ロンドン）を選択します。
7. 新しいユーザグループにユーザを移動するには、[移動] をクリックします。
8. 現在のユーザグループから、リスト内の選択されたユーザグループにすべてのユーザを移動する場合は、[すべて移動] をクリックします（各 [ログイン名] の左側のチェックボックスをオンにする必要はありません）。
9. [ユーザグループ] ページに戻ったら、新しいユーザグループ（たとえば、ロンドン）をクリックして、移動されたユーザを確認します。

ユーザグループの設定

ネットワーク上のユーザグループを編集してSLAを定義する方法

1. [管理] の [ユーザグループ] を選択します。
現在のユーザグループが表示されます。
2. ユーザグループの名前をクリックして、グループの設定を変更します。
3. [全般] タブをクリックします。
4. 必要に応じて、ユーザグループ名を変更します。ユーザグループ名は、大文字と小文字が区別されません。
5. グループの説明を入力または変更します。
6. インパクトレベルを選択します。これによって、グループのトランザクションの障害タイプのビジネス優先度が決まります。通常は、デフォルト値の [中] で十分です。

デフォルトでは、CA CEM ドメインからインパクトレベルが継承されます。この値を変更する場合は、チェックボックスをオフにし、リストからインパクトレベルを選択します。

注: CA CEM ドメインのデフォルト値を変更するには、「[CA CEM ドメインの定義 \(P. 323\)](#)」に説明されているように、[設定] - [ドメイン] を選択します。

7. ビジネス サービス レベルで SLA を定義するサービス レベル アグリーメント (SLA) 値を選択します。

デフォルトでは、CA CEM ドメインから SLA 値が継承されます。値を変更する場合は、チェック ボックスをオフにし、リストから新しい値を選択します。

これらの値は、ビジネス サービス内でユーザグループのトランザクションが継承できるデフォルトの SLA 値を定義する場合にも使用されます。

成功率 SLA

パーセンテージとして表される成功率サービス レベル アグリーメント。デフォルトは 95 パーセントです。

シグマ SLA

数値として表されるシグマサービス レベル アグリーメント。シグマスコアは、100 万機会あたりの障害数 (DPMO) から計算される測定値です。デフォルトは 4.00 で、ほぼパーフェクトは 6.00、およびパーフェクト (トランザクション障害数ゼロ) は無限大です。

トランザクション時間 SLA

秒数で表されるトランザクション時間サービス レベル アグリーメント。デフォルトの値はありません。

8. ログイン ID で検出された新しいユーザを、サブネット名で識別される新しいユーザグループに自動的に追加する場合は、[IP サブネット別に新規ユーザをグループ化] チェック ボックスをオンにします。
 - a. ユーザグループの IP アドレス (たとえば、192.168.1.0) を入力します。
 - b. デフォルトのサブネットマスク (たとえば、255.255.255.0) を入力します。

この例では、192.168.1.1 から 192.168.1.254 までの IP アドレスを使用してログインするすべての新規ユーザは、[新規ユーザ] グループではなく、このユーザグループに自動的に割り当てられます。

ヒント: グループへのユーザの割り当てに IP アドレス方法を使用する場合は、グループ名に IP 情報を含めることをお勧めします。

9. [保存] をクリックして、新しいユーザグループを保存します。[ユーザグループ] リストに表示されます。

一括編集によるユーザ設定の構成

ユーザ設定に対して広範囲の変更を加えることが必要になる場合があります。たとえば、ユーザグループ全体ではなく、複数のユーザを探して、[シグマ SLA] の設定を 4.00 から 5.00 に変更したい場合があります。

一括編集を使用すれば、以下について広範囲の変更を加えることができます。

- ビジネス サービスおよびトランザクションの設定
- トランザクションおよびコンポーネントの障害状況
- ユーザ設定

トランザクション関連の設定を大規模に変更する場合は、「CA APM トランザクション定義ガイド」を参照してください。

[ユーザ検索] ページでは、ユーザ設定を大規模に変更することができます。

一括編集によってユーザ設定を構成する方法

1. [管理] - [ユーザグループ] - [ユーザ検索] を選択します。
検索オプションが表示されます。
2. ユーザグループの名前（たとえば、[Corporate]）を選択します。
3. インパクト レベル（たとえば、[すべて]）を選択します。
4. 特定のユーザを検索している場合は、必要に応じてログイン名、名、または姓を入力できます。
5. [検索] をクリックします。
検索の結果が表示されます。
6. 変更するユーザの左側にあるチェック ボックスをオンにします。または、リスト全体を変更する場合は、一番上のチェック ボックスをオンにします。
7. [次の値の設定] リストから項目を選択します。
 - シグマ SLA を継承
 - シグマ SLA
 - 成功率 SLA を継承

- 成功率 SLA
- トランザクション時間 SLA を継承
- トランザクション時間 SLA

選択したオプションに応じて、[値] テキストボックスまたは [はい | いいえ] リストが表示されます。

8. 値を入力するか、または [はい] または [いいえ] を選択して、[設定] をクリックします。

相関 SLA の設定

ユーザグループ全体に対して 1 つの SLA または (ユーザグループに依存せずに) トランザクションの SLA を使用するのではなく、ビジネス サービス別またはビジネス トランザクション別にユーザグループの SLA を設定することが必要になる場合があります。

トランザクションおよびユーザの場所に基づいて、許容可能な応答時間が異なる例を以下に示します。

| ユーザグループ/ビジネス トランザクションの許容可能な応答時間 | ローカル | リモート | 海外 |
|---------------------------------|------|------|------|
| ログイン | 3 秒 | 6 秒 | 9 秒 |
| 購入 | 5 秒 | 7 秒 | 10 秒 |

相関 SLA では、ユーザ グループ別、ビジネス サービス別、およびビジネス トランザクションの組み合わせ別に SLA を設定できます。ビジネス トランザクションまたはユーザ グループに関する一元的な SLA に代わり、相関 SLA ではそれらを多元的に表示します。

注: 相関 SLA は、ドメイン、ビジネス トランザクション、またはユーザ グループの SLA に代わるものではありません。相関 SLA はこれらの SLA のいずれからも継承されません。CEM 管理者が具体的に相関 SLA を設定する必要があります。

相関 SLA を設定するための手順を以下に示します。

- [相関 SLA の表示](#) (P. 366)
- [相関 SLA の追加](#) (P. 367)
- [既存の相関 SLA の更新](#) (P. 369)
- [相関 SLA の削除](#) (P. 369)

相関 SLA の表示

すでに作成されている相関 SLA を確認する場合や、削除対象の SLA を探して選択する場合は、以下の手順に従います。

1 つのテーブルにすべての相関 SLA を表示することはできません。これは、通常の実運用システムでは、すべてのユーザ グループ、ビジネス サービス、およびビジネス トランザクションのマトリックスが非常に大きいためです。ただし、所定のビジネス サービスまたは所定のユーザ グループの相関 SLA は表示できます。

ユーザ グループ別およびビジネス トランザクション別に相関 SLA を表示する方法

1. [管理] - [相関 SLA] を選択します。
2. [表示] フィールドで、[ユーザ グループ別] または [ビジネス サービス別] を選択します。
3. 2 番目のフィールドで、グループまたはサービスを選択します。

4. 3 番目のフィールドで、[すべて] を選択するか、グループまたはサービスを選択します。
5. [リフレッシュ] をクリックします。
指定されたユーザ グループまたはビジネス サービスの相関 SLA が表示されます。

相関 SLA の追加

この手順では、ユーザ グループ/ビジネス サービス/ビジネス トランザクションセットの新しい相関 SLA を作成する方法について説明します。

相関 SLA を追加する方法

1. [管理] - [相関 SLA] を選択します。
2. 作成する相関 SLA がまだ存在しないことを確認します。目的の相関 SLA があり、それを変更する場合は、「[既存の相関 SLA の更新 \(P. 369\)](#)」を参照してください。
3. [新規] をクリックします。
4. ユーザ グループ/ビジネス サービス/ビジネス トランザクションごとに相関の設定を定義します。
 - a. [ユーザ グループ] - ユーザ グループの名前を選択するか、または [すべて] を選択します。
 - b. [エリア] を選択します。
 - c. [ビジネス サービス] - ビジネス サービスの名前を選択するか、または [すべて] を選択します。

- d. [ビジネス トランザクション] - ビジネス トランザクションの名前を選択するか、または [すべて] を選択します。
- e. SLA の値を設定します。

成功率 SLA

パーセンテージとして表される成功率サービス レベル アグリーメント。デフォルトの値はありません。

シグマ SLA

数値として表されるシグマ サービス レベル アグリーメント。シグマ スコアは、100 万機会あたりの障害数 (DPMO) から計算される測定値です。許容可能なシグマ スコアは 4.00 です。ほぼパーフェクトは 6.00、およびパーフェクト (トランザクション障害数ゼロ) は無限大です。デフォルトの値はありません。

トランザクション時間 SLA

秒数で表されるトランザクション時間サービス レベル アグリーメント。デフォルトの値はありません。

5. [保存] をクリックします。

リストに新しい相関 SLA が表示されます。

注: 新しい相関 SLA が作成されても、既存の相関 SLA は変更されません。たとえば、ユーザ グループ A (UG-A)、ビジネス サービス X (BP-x)、およびビジネス トランザクション 3 (BT-3) に関する相関 SLA がすでにある場合に、UG-A、PB-x、およびすべてのビジネス トランザクションに関する新しい相関 SLA を作成しても、すでに定義済みの SLA (UG-A/BT-x/BT-3) は変更されません。

注: ビジネス サービス内のすべてのビジネス トランザクションに関する相関 SLA を作成し、後で別のビジネス トランザクションを追加する場合は、その追加されたビジネス トランザクションの新しい SLA を作成することを忘れないでください (このビジネス トランザクションの SLA は自動的に追加されません)。

既存の相関 SLA の更新

既存の相関 SLA を変更するには、[更新] ボタンを使用します。

既存の相関 SLA を変更する方法

1. [管理] - [相関 SLA] を選択します。
2. 変更する相関 SLA を選択します（変更する相関 SLA を表示するには、[表示] - [ビジネス サービス] - [ユーザ グループ] リストで [リフレッシュ] を使用します）。
3. [更新] をクリックします。
4. フィールドを設定して、変更する相関 SLA を指定します。
5. SLA の値を設定します。
6. [更新] をクリックします。

更新された相関 SLA がリストに表示されます。

相関 SLA の削除

相関 SLA が不要になった場合は削除できます。

SLA を削除する方法

警告： [削除] をクリックすると、SLA はすぐに削除されます。この削除に関連する「確認」ダイアログはありません。

1. [管理] - [相関 SLA] を選択します。
2. 削除する相関 SLA を選択します。
3. [削除] をクリックします。

ユーザグループの削除

ユーザグループおよび関連するすべてのトランザクション統計を削除できます。これを実行する必要があるのは、以下の場合です。

- オフィスを閉じるので、そのグループのトランザクション情報が不要になった場合
- グループをマージする（あるグループから別のグループにユーザを移動し、空になったグループを削除する）場合
- ユーザグループの自動作成によって、必要以上のユーザグループが作成された場合

重要: ユーザが含まれていないユーザグループを含め、不要なユーザグループを削除します。ユーザグループの数が多すぎると、パフォーマンスに悪影響が生じることがあります。

ユーザグループを削除する方法

1. [管理] の [ユーザグループ] を選択します。
2. [ユーザグループ] タブで、削除するユーザグループのチェックボックスをオンにします。
3. [削除] をクリックします。

ユーザの非アクティブ化または削除

CA CEM によって監視されない期間が長期に及ぶことがわかっているユーザが存在する場合は、そのユーザを一時的に非アクティブ化することができます。この場合、トランザクション履歴およびユーザレコードは保持されます。CA CEM で、任意の非アクティブ化ユーザからの新しいトランザクションを検出されると、そのユーザは自動的に再アクティブ化されません。

ユーザを削除した場合は、ユーザのトランザクション履歴のみが保持されます。削除されたユーザは管理ページには表示されません。ユーザの履歴はレポートでグレー表示されます。CA CEM で、任意の削除済みユーザからの新しいトランザクションを検出されると、新しいユーザが作成されます。ユーザの削除は、監視しているアプリケーションをそのユーザが二度と使用しないという確信がある場合のみ行ってください。

ユーザを非アクティブ化または削除する方法

1. [管理] の [ユーザグループ] を選択します。
2. [ユーザ検索] をクリックして、非アクティブ化または削除する必要がある特定のユーザを検索します。
3. 非アクティブ化または削除するユーザのチェックボックスをオンにします。
4. [非アクティブ化] または [削除] をクリックします。

ユーザの再アクティブ化

過去に非アクティブ化したユーザを再アクティブ化することができます。

ユーザをアクティブ化する方法

1. [管理] の [ユーザグループ] を選択します。
2. [ユーザ検索] をクリックして、アクティブ化する必要がある特定のユーザを検索します。
3. アクティブ化するユーザのチェックボックスをオンにします。
4. [アクティブ化] をクリックします。

第 20 章: CA CEM でのシステムオペレーションの管理

この章では、管理者が、CA CEM が正常に実行していることを確認するために実行するタスク（エラー レポートの確認、ディスク空き容量およびメモリの確認など）について説明します。

CA CEM 監視イベントについて、および CA CEM の監査証跡の表示について必要な情報を以下に示します。

1. [CA CEM イベントの概要](#) (P. 373)。
2. [CA CEM イベントの確認](#) (P. 377)。
3. [必須の CA CEM イベントの保持](#) (P. 377)。
4. [エラーや警告などの電子メール通知イベントを送信するための CA CEM の設定](#) (P. 377)。
5. [TIM マシンのメモリ使用量やディスク空き容量などの情報の確認](#) (P. 379)。
6. [CA CEM 監査証跡の確認](#) (P. 381)。

CA CEM イベントの概要

CA CEM はイベントをキャプチャしてログに記録するので、管理者はシステムの操作やパフォーマンスに影響する可能性があるイベントの情報を入手することができます。 イベント ログは定期的に確認することをお勧めします。

重大度レベル

イベントには 3 つの重大度レベルがあります。

- 情報
- 警告
- エラー

発生する可能性のあるイベントのリスト

CA CEM はこれらのシステム イベントをキャプチャしてログに記録します。

| イベント | 重大度 | カテゴリ | 詳細 |
|-------------------------------------|-----|-----------|--|
| ビジネス アプリケーション名が無効です | エラー | CA APM TG | CA APM TG スクリプト内のビジネス アプリケーション名で、「<」または「>」などの無効な文字が使用されています。CA APM TG で、CA CEM アプリケーション名を修正し、スクリプトを再度マイグレートします。 |
| データベース クリーンアップ サービスが開始しました | 情報 | 処理 | データベース クリーンアップ サービスが開始しました。サービスを実行している Enterprise Manager の IP アドレスがイベント リストに提供されます。 |
| データベース クリーンアップ サービスが停止しました | 情報 | 処理 | データベース クリーンアップ サービスが停止しました。サービスを実行していた Enterprise Manager の IP アドレスがイベント リストに提供されます。 |
| 障害がドロップされました | 警告 | 処理 | キャパシティ処理の過負荷により 1 つ以上の障害がドロップされたことが、インシデントによって報告されました。 |
| 重複するセッション ID が検出されました | 警告 | 監視 | 考えられる原因は、以下のとおりです。 2 つ以上の TIM が同じトラフィックを監視しています。 複数のログインのセッション ID が同じです（セッション識別に使用するパラメータの問題を示している可能性があります）。 |
| Enterprise Manager が TIM にアクセスできません | エラー | 通信 | Enterprise Manager が、データを取得するために TIM にアクセスできませんでした。 |
| Enterprise Manager が再起動しました | 情報 | 管理 | Enterprise Manager の再起動日時。 |

| イベント | 重大度 | カテゴリ | 詳細 |
|-----------------------|-----|------|---|
| HTTP アナライザプラグインエラー | エラー | 処理 | HTTP アナライザプラグインで障害が発生しました。 |
| 新規コンポーネントの追加で上限を超えました | 警告 | 処理 | このイベントは、[新規の非識別コンポーネントの検出]が選択されている場合にのみ発生する可能性があります。非識別コンポーネントの最大数を超えると、新しいコンポーネントが最も古いコンポーネントと置き換わります。これが発生するたびに、[新規コンポーネントの追加で上限を超えました]イベントがログに記録されます。 コンポーネントの自動検出の詳細については、「CA APM トランザクション定義ガイド」を参照してください。 |
| ログインがドロップされました | 警告 | 処理 | キャパシティ処理の過負荷により 1つ以上のログインがドロップされました。 |
| ネットワークデータがありません | 警告 | 通信 | TIM は、一定の期間、ネットワークを介してデータを受信していません。たとえば、ケーブルが移動された、ネットワークスイッチが正しく構成されていない、ネットワークトポロジが変更されたために CA CEM 構成と一致しなくなった、などの原因が考えられます。 |
| 統計集約サービスが開始しました | 情報 | 処理 | 統計集約サービスが開始しました。サービスを実行している Enterprise Manager の IP アドレスがイベントリストに提供されます。 |
| 統計集約サービスが停止しました | 情報 | 処理 | 統計集約サービスが停止しました。サービスを実行していた Enterprise Manager の IP アドレスがイベントリストに提供されます。 |
| TIM コレクションサービスが開始しました | 情報 | 処理 | TIM コレクションサービスが開始しました。サービスを実行している Enterprise Manager の IP アドレスがイベントリストに提供されます。 |

| イベント | 重大度 | カテゴリ | 詳細 |
|---|-----|-----------|--|
| TIM コレクション サービスが停止しました | 情報 | 処理 | TIM コレクション サービスが停止しました。 サービスを実行していた Enterprise Manager の IP アドレスがイベントリストに提供されます。 |
| ディスクの空き容量が少なくなったため、TIM は自身のデータ ファイルの一部を削除しました | 情報 | 管理 | ディスク空き容量を保護するために TIM は自身のデータ ファイルの一部を削除しました。 デフォルトでは、ディスクがキャパシティの 75% に達すると、ファイルが削除されます。 この動作は、[TIM Settings] ページの DiskSpace/MinFreeDataSpaceInPercent によって決まります。 |
| TIM は再起動しました | 情報 | 管理 | TIM の再起動日時。 |
| トランザクション定義がドロップされました | 情報 | 処理 | このイベントは、自動トランザクション検出がオンの場合にのみ発生する可能性があります。 このイベントは、キャパシティ処理の過負荷により、一部の自動的に検出されたトランザクションの定義がドロップされたことを意味します。 このイベントが表示された場合は、自動トランザクション検出をオフにして、後で実行することを検討してください。 |
| ユーザ グループの制限に達しました | 警告 | 処理 | IP サブネット別に自動的に作成されるユーザ グループの最大数に到達したことが、ユーザ グループによって報告されました。 |
| CA APM TG エージェントはダウンしています | 警告 | CA APM TG | CA APM TG エージェントが利用不能です。 |
| CA APM TG エージェントは稼働中です | 情報 | CA APM TG | CA APM TG エージェントが利用可能です。 |

CA CEM イベントの表示

CA CEM イベントを定期的に監視して、ネットワーク問題、システムまたはバックアップ障害、および HTTP アラナイザ プラグイン エラーの各兆候を探ることができます。

以下の手順に従います。

1. [システム] の [イベント] を選択します。
CA CEM イベントのリストが表示されます。
2. 詳細情報を表示するには、イベントの名前をクリックします。
イベントの詳細ページが表示されます。
3. [システム] の [イベント] を選択すると、イベントのリストに戻ります。

CA CEM イベントの管理

イベントを保持する日数を指定できます。

以下の手順に従います。

1. [システム] の [イベント] を選択し、[Event Manager] タブをクリックします。
CA CEM イベントの現在の設定が表示されます。
2. イベントの設定を定義します。
イベントを削除するまでの期間
CA CEM イベントがイベント ログから削除されるまでの日数。
3. [保存] をクリックします。

イベントの電子メール通知の受信

イベントが発生したときに電子メール通知を送信するように CA CEM を設定できます。

少なくとも、CA CEM 管理者がエラー イベントの電子メール通知を受信するようにイベント電子メール通知を設定する必要があります。

以下の項目を設定できます。

- 通知の送信先の電子メールアドレス。
- 通知するイベント。
- メッセージの件名および本文のテキスト。

イベントの電子メール通知を送信するように CA CEM を構成する方法

1. [システム] の [イベント] を選択し、[Event Manager] タブをクリックします。

CA CEM イベントの現在の設定が表示されます。

2. [イベント電子メール通知] チェック ボックスをオンにします。

[イベント通知設定] が表示されます。

3. 電子メール通知を有効にする（または無効にする）各イベントの隣にあるチェック ボックスをオンにします。

チェック ボックスはトグル オプションです。ステータスが現在 [無効] の場合に、チェック ボックスをオンにして [保存] をクリックすると、そのイベントの電子メール通知が開始します（ステータスは [有効] になります）。ステータスが現在 [有効] の場合に、チェック ボックスをオフにして [保存] を選択すると、そのイベントの電子メール通知が停止します（ステータスは [無効] になります）。

注: [ステータス] フィールドは、イベントの電子メール通知が有効か無効かを示します。電子メール通知のステータスにかかわらず、[イベント] ページにはすべてのイベントが表示されます。

4. (オプション) Enterprise Manager と TIM のサブセットのみから電子メール通知を受信する場合は、IP アドレスの範囲を指定します。

たとえば、Enterprise Manager に関する電子メール通知は表示するが、TIM に関する電子メール通知は表示しない場合は、Enterprise Manager アドレスを含み、TIM アドレスを除外した IP アドレス範囲を指定します。

5. 必要に応じて、電子メールの宛先アドレスおよび差出人アドレスを編集します。

6. (オプション) [メッセージ] フィールドを編集します。変数を使用して、カスタマイズした説明を作成します。

- <id>
- <name>

- <severity>
- <category>
- <source>
- <ipaddress>
- <desc>
- <time>

変数を並べ替えて、独自のメッセージを作成できます。電子メール通知の送信時に、各変数は実際のイベント値に置き換えられます。

ヒント： [例] 領域から [メッセージ] フィールドに変数およびテキストをコピーして貼り付けることができます。

7. [保存] をクリックします。
8. SMTP サーバの設定が正しいことを確認します。「[SMTP サーバ設定の構成](#) (P. 341)」を参照してください。

TIM マシン稼働状況の確認

ルーチンの保守およびトラブルシューティングの際に、TIM マシンの稼働状況を確認する必要があります。これには、ディスクおよびメモリ使用量やマシン上で実行されているプロセスの確認が含まれます。

注: これらの稼働状況レポートを表示するには、[Wily System Setup] ページにアクセスする必要があります。

TIM マシンの稼働状況のスナップショットを表示する方法

1. [設定] - [監視] を選択します。
2. [レポートを取得] をクリックします (右端の [TIM 稼働状況] 列にあります)。
3. ログインダイアログボックスが表示された場合は、[Wily System Setup] ページのユーザ名およびパスワードを使用してログインします。この場合のデフォルトのユーザ名は **admin** です。
[Appliance Health] ページが表示されます。

4. [\[Complete Appliance Health\]](#) リンクをクリックします。
 または、その他のリンクのいずれかをクリックして、稼働状況レポートの1つのセクションを表示します。
 各リンクについては、「[\[Appliance Health\] ページ参照表 \(P. 380\)](#)」を参照してください。
5. TIM マシンごとに前述の手順を繰り返します。

[Appliance Health] ページ参照表

この表では、[\[Appliance Health\]](#) ページ上の各リンクで表示される情報を説明します。

| リンク | 情報 | 同等の Linux コマンド |
|--------------------|---|----------------|
| Disk Information | <p>ファイルシステムのディスク使用量が MB 単位で表示されます。</p> <p>ディスク使用率が非常に高く、80% を超える場合は、TIM ログ ファイルを削除することでディスク使用量を削減してください。</p> | df -m |
| Memory Information | <p>システム内の空きメモリおよび使用済みメモリの容量が MB 単位で表示されます。</p> <p>空きメモリの容量が少ない場合は、過度なメモリスワッピング (スラッシング) に注意する必要があります。</p> <p>TIM で、最も多いスラッシング原因はプラグインです。メモリの使用を改善するためにプラグインコードを変更することが必要になる場合があります。</p> | free -m |
| Logged in Users | <p>マシンそのものにログインしているすべてのユーザが表示されます。通常は、ユーザを参照する必要はありませんが、たとえば、セキュアシェル (ssh) を介してマシンにログインしているルートユーザを参照することができます。</p> <p>認識していないユーザが表示された場合は、ただちに調べてください。</p> | who |

| | | |
|-----------------------------|--|------|
| Currently Running Processes | <p>実行中のすべてのプロセスが表示されます（標準構文を使用して表示されます。また、プロセスパスを示す場合は [CMD] 列で ASCII art を使用して表示されます）。</p> <p>このリストで、非常に高い CPU 使用量や、および <code>ps -efl --forest</code> 予期しないプロセスを探します。</p> | |
| Complete Appliance Health | <p>前述のすべての情報が表示されます。</p> | 上記参照 |

CA CEM 監査証跡の確認

CEM 管理者は、CA CEM アクティビティの監査証跡を表示することができます。

CA CEM アクティビティは、管理詳細ページに表示できます。監査情報はリスト ページでは入手できません。

監査証跡を表示する方法

1. 監査する管理ページのいずれかを選択します。
 - [管理] - [ビジネス サービス]
 - [設定] - [ドメイン]
 - [システム] - [電子メール設定]
2. アドレスで、URL の末尾に `&showHistory=true` または `?showHistory=true` を追加します（アンパサンド (&) または疑問符 (?) のどちらかを使用します)。
 - URL の末尾が `.html?pid=600001` のような場合は、アンパサンドを使用します。

```
http://<IP_Address>:8081/wily/ceM/tess/app/admin/tranDefGroupList.html?pid=1&showHistory=true
```

```
http://<IP_Address>:8081/wily/ceM/tess/app/admin/domainDetail.html?pid=1&showHistory=true
```

- URL の末尾が `.html` の場合は、疑問符を使用します。

```
http://<IP_Address>:8081/wily/ceM/tess/app/system/emailSettings.html?showHistory=true
```

3. [実行] をクリックするか、または **Enter** キーを押して監査証跡を表示します。

監査証跡はページの最下部に表示されます。

4. ページをスクロールダウンして、Wily CEM 監査情報を表示します。最新の 200 個の変更が表示されます。
5. 200 個のレコード表示のデフォルトを無視する場合は、クエリ文字列の末尾に `&maxResults=nnn` を追加できます。

例：

```
http://<IP_Address>:8081/wily/cem/tess/app/system/emailSettings.html?showHistory=true&maxResults=500
```

第 21 章: CA CEM のレポート機能

CA CEM のレポート機能について必要な情報を以下に示します。

1. [CA CEM レポートの概要、およびシステムをナビゲートしてレポートをキャプチャする方法 \(P. 383\)](#)。
2. [必要な CA CEM レポートの定期的なスケジュール設定 \(P. 390\)](#)。

CA CEM レポートのキャプチャ

CA CEM データは、複数の方法で分析できます。CA CEM のメニューをナビゲートして、ビジネス サービス、ビジネス トランザクション、ユーザ グループに基づき、インシデント別および障害別にクエリを実行できます。

レポート オプションは、選択するレポート タイプによって異なります。たとえば、傾向レポートを選択した場合は、傾向分析で比較するプライマリ タイム フレームとセカンダリ タイム フレームを指定する必要があります。

その他のレポート出力については、「[レポート配信 \(P. 384\)](#)」を参照してください。

利用可能なレポートについては、「[レポート形式 \(P. 385\)](#)」を参照してください。

CA CEM システム データ保持オプションおよび統計集約スケジュールが、レポート出力に影響することがあります。詳細については、「[レポートタイムフレーム \(P. 386\)](#)」を参照してください。

CA CEM レポート集約の概要

CA CEM 集約は、レポートに表示されるデータに影響します。CA CEM が日単位、週単位、月単位、および年単位で統計をどのように集約するかを理解します。

CA CEM レポートは、ビジネス トランザクションの集約統計に基づいています。1 時間に 1 回、CA CEM は、時間単位の集約を含む統計処理を実行します。

1日に1回、深夜に、時間単位の統計集約プロセスが終了した後で、CA CEMは以下を実行します。

- 日単位の集約プロセス
- 週単位の集約プロセス
- 月単位の集約プロセス

パフォーマンス上の理由から、1日1回の集約をお勧めしますが、レポートへの影響に注意する必要があります。例：

- 今日の午後5時に週単位または月単位のレポートを実行した場合、レポート統計には深夜時点のデータが含まれます。レポートに今日の統計は含まれません。
- 統計集約サービスを実行する Enterprise Manager が深夜に稼働していない場合、集約プロセスは（Enterprise Manager が次に深夜に実行するまで）実行されません。そのため、昨日の統計を探している場合、日単位（[昨日]のタイムフレーム）、週単位、月単位、または年単位のレポートに昨日の統計は含まれていません。
- [今日]のタイムフレームからのレポート統計に要する時間は、日単位の集約データよりも少し長くなります。
- 年単位のレポートは月単位の集約データに基づきます。

レポート配信

CA CEM では、さまざまな方法で CA CEM レポートのキャプチャおよび管理を行うことができます。

- CA CEM データのクエリを実行する際にレポートをオンラインで表示する
- [マイ レポート] リストから定義済みのレポートを表示する
- 保存または印刷できる PDF ファイルを作成する
- PDF ファイルをユーザまたはユーザのグループに電子メールで送信する
- 後で実行したり表示したりできるようにレポートを保存する
- 日単位、週単位、または月単位で実行して電子メールで配信するようにレポートをスケジュールする

レポートデータのセキュリティ保護

CA CEM ユーザのアクセスをビジネス サービスおよび関連するデータに制限するセキュリティ グループがある場合は、**Embedded Entitlements Manager** セキュリティ領域のみを持つようになっているか確認してください。

複数の領域（1つのローカル領域と1つの **Embedded Entitlements Manager** 領域など）がある場合、CA CEM ユーザがアクセス権を持っていないスケジュール済みレポートのデータが同ユーザによって参照される可能性があります。

領域の設定については、「**CA APM セキュリティ ガイド**」を参照してください。

レポート形式

[CEM] タブの以下のページにナビゲートして、CA CEM レポートをキャプチャすることができます。

- サービス レベル管理
 - トランザクション SLA - パフォーマンスおよび品質
 - ユーザ SLA - パフォーマンスおよび品質
 - 関連 SLAs
 - トランザクション傾向 - パフォーマンスおよび品質
 - ユーザ傾向 - パフォーマンスおよび品質
 - ビジネス価値
- インシデント管理
 - インシデント
 - 主要インパクト要因
 - 障害
 - トランザクション追跡セッション
- パフォーマンス レポート
 - ビジネス サービス
 - ユーザ グループ

- 品質レポート
 - ビジネス サービス
 - ユーザ グループ
- 分析グラフ
 - 成功率
 - 時間
 - スループット
 - サイズ
 - ボリューム
 - 数
 - 収率
 - 障害 - 頻度
 - セッション使用状況

レポートタイム フレーム

CA CEM では、さまざまな方法でレポート ビューのタイム フレームを指定することができます。

| タイム フレーム | 現在 | 過去 | カスタム |
|----------|-----|------|---------|
| 時間 | N/A | 前の時間 | カスタムの時間 |
| 日 | 今日 | 昨日 | カスタムの日 |
| 週 | 今週 | 前の週 | カスタムの週 |
| 月 | 今月 | 前の月 | カスタムの月 |
| 年 | 今年 | 前の年 | N/A |

注: レポートのタイム フレームを選択する場合、およびスケジュール済みレポートを指定する場合は、CA CEM システムの集約およびデータ保持設定を検討することが重要です。統計がまだ集約されていない場合、データがパージされた場合、またはインシデント設定が変更された場合は、レポートは期待どおりに作成されません。

CA CEM 管理者は、レポート目的に必要なデータを保持するようにシステムを設定していますが、最適なシステムパフォーマンスを得るためには、CA CEM 統計を定期的にパージする必要があります。データ保持設定の詳細については、「[CA CEM ドメインの定義 \(P. 323\)](#)」を参照してください。

CA CEM システムは、時間単位、日単位、週単位、および月単位の統計を保持するようにデータを集約します。また、集約は、パフォーマンスとスケーラビリティのために使用される手段でもあります。CA CEM 集約の詳細については、「[CA CEM レポート集約の概要 \(P. 383\)](#)」を参照してください。

レポートの概要

レポートが利用できる CEM ページには、さまざまなオプションが用意されています。

PDF

[PDF] リンクでは、レポートが PDF 形式で表示されます。ファイルにレポートを保存するか、または PDF を印刷することができます。

PDF を電子メールで送信

[PDF を電子メールで送信] リンクをクリックすると、新しいページが開き、そこから PDF レポートが添付された電子メールを送信できます。

レポートの保存/スケジュール設定

[レポートの保存/スケジュール設定] リンクをクリックすると、[マイレポート] に移動し、ここでレポートを保存またはスケジュールすることができます。

これらのレポート オプションのいずれかをクリックするときは、事前にクエリを実行して、有効なデータでレポート ページをリフレッシュしておく必要があります。

注: 2 番目の CEM レポート ページを開いた後で (たとえば、ブラウザの [新しいウィンドウで開く] オプションを使用した場合など) CEM レポート ページで [PDF] リンクをクリックすると、エラーになります。最初の CEM レポート ページに戻り、[リフレッシュ] をクリックし、再度 PDF リンクをクリックしてください。

PDF レポート

[PDF] リンクをクリックすると、レポートが Adobe Acrobat PDF 形式で開き、ファイルを保存したり印刷したりできます。

レポートを印刷する方法

1. Internet Explorer で PDF 形式のレポートを印刷するには、[ファイル] の [印刷] をクリックします。
2. [戻る] ボタンをクリックすると、前のページに戻ります。

ファイルにレポートを保存する方法

1. Internet Explorer で、[ファイル] の [名前を付けて保存] をクリックします。
2. レポートを保存する場所を探索します。レポートに適したファイル名を入力します。[保存] をクリックすると、レポートがファイルに保存されます。

注: 名前を変更しない場合、名前は *WilyCEMReport.pdf* になります。

3. [戻る] ボタンをクリックすると、前のページに戻ります。

PDF レポートでユーザ独自のロゴを使用する方法

- APM データベースの `ts_settings` テーブルにある `reports.userImage` を置き換えます。

注: 電子メールで送信するレポートにはロゴを使用できません。

電子メールレポート

[電子メール]リンクでは、PDF形式のレポートを送信できます。電子メールフォームと一緒に新しいウィンドウが開きます。

レポートを電子メールで送信する方法

1. 電子メールフォームに入力します。

差出人

これは、ログインユーザの電子メールアドレスです。電子メールアドレスを指定しない場合は、`tess-default.properties` ファイルの `email.defaultFromAddress` からアドレスが自動的に入力されます（「[デフォルトの tess-default.properties ファイル \(P. 643\)](#)」）。

宛先

電子メールアドレスまたは配布リストのカンマ区切りリストを入力します。

注: 電子メールアドレスの区切りにセミコロンを使用しないでください。

件名

添付レポートに対する意味のある件名行を入力します。

メッセージ

標準メッセージに、レポートに適した情報を追加します。

2. [送信] をクリックします。

注: 電子メールでレポートを送信する場合、CEM システム管理者はメール SMTP サーバを設定する必要があります。

保存済みまたはスケジュール済みレポート

[レポートの保存/スケジュール設定] 機能および [マイ レポート] 機能では、レポートを定期的に（日単位、週単位、または月単位で）実行するように設定できます。CA CEM システムは、レポートを生成し、指定された時間に電子メールで送信します。

詳細については、「[レポートのスケジュール \(P. 390\)](#)」を参照してください。

レポートのスケジュール

CA CEM にはレポートをスケジュールする方法が 2 つあります。

- [\[マイ レポート\] でレポートを定義してスケジュールする \(P. 390\)](#)。
- [目的のレポートを生成してからそのレポートをスケジュールする \(P. 394\)](#)。

[マイレポート]の使用によるレポートのスケジュール

このセクションでは、[マイ レポート] を使用して、レポートを手動でスケジュールする方法について説明します。

以下の手順に従います。

1. [CEM] の [マイ レポート] を選択し、[新規] をクリックします。
2. リストからレポート形式を選択します。各レポート形式に必要な追加情報は、選択するオプションによって異なります。

詳細については、「[レポート形式 \(P. 385\)](#)」を参照してください。

ビジネス価値レポートに必要な情報を以下に示します。

ビジネス アプリケーション

特定のビジネス アプリケーションまたは [すべて] を選択します。

ビジネス サービス

特定のビジネス サービスまたは [すべて] を選択します。

タイムフレーム

時間、日、週、月、または年を指定します。

電子メールで配信するこのレポートの PDF バージョンをスケジュールする

必要に応じて、電子メールで配信するこのレポートをスケジュールするオプションを選択できます。

詳細については、「[レポート タイム フレーム \(P. 386\)](#)」を参照してください。

ユーザ傾向品質レポートに必要な情報を以下に示します。

ビジネス アプリケーション

特定のビジネス アプリケーションまたは [すべて] を選択します。

ビジネス サービス

特定のビジネス サービスまたは [すべて] を選択します。

ビジネス トランザクション

オプションは、選択したビジネス サービスによって異なります。
特定のビジネス トランザクションまたは [すべて] を選択します。

ユーザ グループ

特定のユーザ グループまたは [すべて] を選択します。

プライマリ タイム フレーム

時間、日、週、月、または年を指定します。通常、これは現在のタイム フレーム (たとえば、今週) です。

セカンダリタイムフレーム

時間、日、週、月、または年を指定します。通常、これは過去のタイムフレームです。たとえば、今日と昨日や、今週と先週、先月、または昨年を比較できます。

電子メールで配信するこのレポートの PDF バージョンをスケジュールする

必要に応じて、電子メールで配信するこのレポートをスケジュールするオプションを選択できます。

3. レポートを実行する頻度を指定します。

日単位

レポートを実行する時間を選択します。

週単位

レポートを実行する時間および曜日を選択します。

月単位

レポートを実行する時間および日付を選択します。

重要: 所定の月に存在しない日付を選択した場合、その月にはレポートが送信されません。たとえば、31日を選択した場合、31日がない月にはそのレポートは送信されません。

4. レポートを実行する時間を指定します。繰り返し時間を設定します。

ヒント: レポートに過去1時間のデータを含める場合は、1時間後にレポートをスケジュールすることをお勧めします。こうすることで、統計プロセスを完了する時間を取ることができます。

CA CEM 集約の詳細については、「[CA CEM レポート集約の概要 \(P. 383\)](#)」を参照してください。

5. 電子メール設定を定義します。

ヒント： 件名行およびメッセージを使用して、レポートの受信者がレポートのタイプ、レポートの実行頻度、および質問がある場合の連絡先名を把握できるようにすることをお勧めします。

差出人アドレス

レポートの送信元の電子メールアドレスを入力します。たとえば、レポートの受信者が別の電子メールアドレスに返信するように設定したい場合は、このアドレスを変更できます。

差出人名

電子メールアドレスに関連付けられた名前を入力します。通常、これは差出人の名前、または担当する CA CEM ユーザの名前です。

宛先

電子メールアドレスまたは配布リストのカンマ区切りリストを入力します。

件名

このレポートに対する意味のある件名行を入力します。

メッセージ

このレポートに役立つメッセージを入力します。

6. [保存] をクリックします。新しいレポートがレポートのリストに表示されます。

すべての CA CEM ユーザは、自分が作成したレポートを表示できます。ほかの CA CEM ユーザが作成したレポートは、CA CEM システム管理者のみが表示できます。

ヒント： すべてのレポートに一貫した方法で名前を付ければ、必要なレポートを見つけやすくなります。たとえば、すべてのレポート名に以下を含めます。

- 含まれるビジネス アプリケーション、サービス、およびトランザクション
- 含まれるユーザグループ
- 頻度

レポートの生成およびスケジュール

このセクションでは、必要なオプションを使用してレポートを生成した後でそのレポートをスケジュールする方法の例を紹介します。

レポートを生成してスケジュールする方法

1. 目的のページに移動し、目的どおりにレポート ビューを生成します。
例：
 - a. [CEM] - [サービス レベル管理] - [ユーザ傾向] を選択します。
 - b. レポートに表示するユーザ グループ、ビジネス 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選択します。
 - c. プライマリ タイム フレームおよびセカンダリ タイム フレームを選択します。
 - d. ユーザ グループに関する品質レポートを表示するには、[品質] をクリックします。
 - e. [リフレッシュ] をクリックして、ページを品質レポートに更新します。
 - f. [レポートの保存/スケジュール設定] をクリックします。
[マイ レポート] ページが表示されます。[レポート設定] のすべてに、先ほど表示したユーザ傾向品質レポートの値が事前に入力されています。
2. 必要に応じて、事前に入力されているレポート設定を変更します。
3. [電子メールで配信するこのレポートの PDF バージョンをスケジュールする] チェック ボックスをオンにします。
[繰り返し] オプションおよび [電子メール設定] オプションが表示されます。
4. 必要に応じて、繰り返しの設定を定義します。
5. 必要に応じて、電子メールの設定を定義します。
6. [保存] をクリックして、このレポートをスケジュールします。
レポート スケジュール オプションの詳細については、「[\[マイ レポート\] の使用によるレポートのスケジュール \(P. 390\)](#)」を参照してください。

CA CEM データのエクスポート

[データ エクスポート] タブから CA CEM データをエクスポートできます。このタブでは、ビジネス統計、障害、およびインシデントのデータを取得できます。

以下の CA CEM データをエクスポートできます。

- 指定した時間範囲の集約および非集約ビジネス統計
- 指定した時間範囲の障害、過去 N 件の障害、または過去 X 分間の障害
- 指定した時間範囲のインシデント

注: 電子商取引モードでは、統計データ内のユーザ情報をエクスポートできません。

データのエクスポート

このセクションでは、CA CEM データのエクスポート方法の例を示します。

以下の手順に従います。

1. [CEM] - [データ エクスポート] - [統計データ] をクリックします。
[統計データ] ビューが表示されます。
2. 以下のオプションの組み合わせを指定します。
 - a. データに表示するレポートタイプ、ビジネス 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選択します。

- b. ユーザグループまたはユーザを選択します。

注: 非集約レポートタイプを選択する場合は、ユーザグループのみ選択できます。

- c. [開始日] と [終了日] を指定します。

注: デフォルトでは、現在のシステム日時が表示されます。

- d. 非集約レポートタイプの間隔を選択します（時間単位、日単位、週単位、月単位など）。

- e. （オプション）トランザクションのスループット、サイズ、時間のパーセント値を指定します。

[スループット]、[サイズ]、および[時間]の各フィールドは、トランザクションのパーセンタイル値を表します。複数のパーセンタイル値を区切るには、セミコロンを使用します。たとえば、「スループット = 25;50;75」となります。また、これらのフィールドで「すべて」を指定すると、5～95までのパーセンタイル値（増分単位は5）を含めることができます。

注: デフォルトでは、トランザクションのスループット、サイズ、および時間は50パーセントです。

- f. [CSVで保存] をクリックします。

[ファイルのダウンロード] ダイアログボックスから、統計データを含むCSVファイルが表示されます。

3. [CEM] - [データ エクスポート] - [障害データ] をクリックします。

[障害データ] ビューが表示されます。

4. 以下のオプションの組み合わせを指定します。

- a. エクスポートしたデータに表示するビジネス 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選択します。

- b. ユーザグループと障害タイプを選択します。

[コンテンツ エラー] 障害タイプを選択すると、障害データにエクスポートするコンテンツ文字列値を指定できます。

- c. [開始日] と [終了日] を指定するか、あるいは [過去 N 障害] (0 ~ 1000) または [過去 X 分間] (0 ~ 1440) を指定します。
- d. (オプション) 障害の一部として取得するメタ キーを指定します。
メタ キーは、障害の [HTTP 応答] および [要求ヘッダ] で指定された値です。

注: 複数のメタ キーを区切るには、セミコロンを使用します。メタ キーでは大文字と小文字が区別されます。

- e. (オプション) 障害が発生しているビジネストラランザクションのコンポーネント タイミング情報を含めるには、[はい] を選択します。
- f. [CSV で保存] をクリックします。

[ファイルのダウンロード] ダイアログ ボックスから、障害データを含む CSV ファイルが表示されます。

5. [CEM] - [データ エクスポート] - [インシデント データ] をクリックします。

[インシデント データ] ビューが表示されます。

6. [開始日] と [終了日] を指定します。
7. [CSV で保存] をクリックします。

[ファイルのダウンロード] ダイアログ ボックスから、インシデントデータを含む CSV ファイルが表示されます。

レポートの保存またはスケジュール

[マイ レポート] タブで [障害データ]、[インシデント データ]、または [統計データ] のレポート形式を選択し、CA CEM データをレポート用に保存したり、レポートをスケジュールすることができます。

注: CA CEM データのスケジュール済みレポートは、.zip 添付ファイルとして電子メールで送信されます。800 KB を超えるサイズの CSV レポートは均等に分割され、電子メールの .zip 添付ファイルとして送信されます。

レポート スケジュール オプションの詳細については、「[\[マイ レポート\]の使用によるレポートのスケジュール \(P. 390\)](#)」を参照してください。

CSV ヘッダ

以下のセクションでは、CSV ヘッダの一部について説明します。

- **TransactionThroughputPercentile(Bytes/s) の数 - <パーセンタイル要求>**
列は、パーセンタイル要求の数に基づいています。たとえば、「スループット = 25; 40; 75」により、指定された各パーセンタイル要求に対して 3 つの列が作成されます。パーセンタイル要求が指定されていない場合、デフォルトで、列 **TransactionThroughputPercentile - 50** パーセントとなります。
- **DefectValue** は特定のトランザクションに対して障害を生成するために満たす必要がある条件です。
- **MissingID** および **MissingName** は障害タイプ 9 に対してのみ生成されます。**MissingID** および **MissingName** は、不明なトランザクションコンポーネントまたはトランザクションユニットの ID および名前を示します。
- **Cause** は、インシデントが閉じられるときに提供される理由を示します。インシデントが閉じられると、たとえばビジネス トランザクションが削除されるときの理由は「ビジネス トランザクションが削除されました」になります。
- **CloseBy** は、インシデントを閉じるユーザのユーザ名を示します。
- **Evidence1**、**Evidence2**、および **Evidence3** は、インパクトしきい値がそれぞれ中程度、深刻、クリティカルのときに生成されるエビデンスコレクションファイルの名前を示します。
- **Status** 列では、1 はクローズ、2 はオープン、3 は保留、4 はエイジアウトを示します。
- **TriggerDate** は、インシデントの作成日を示します。
- **DefectType** の詳細については、「[CA APM API リファレンスガイド](#)」の「[障害のコマンド パラメータと構文](#)」を参照してください。
- **UserImportance**、**DefectImportance**、および **TransactionImportance** の詳細については、「[インシデント関連設定の定義](#) (P. 331)」を参照してください。

第 22 章: CA CEM によるセキュアな Web アプリケーションの監視

SSL ベースのセキュリティを使用する Web アプリケーションを監視するための CA CEM の設定に関連する主なタスクを以下に示します。

1. [Web サーバの SSL 秘密鍵を取得する](#) (P. 399)。
2. [SSL 秘密鍵が PEM ファイルにあることを確認する](#) (P. 399)。
必要な場合は、秘密鍵を変換します。
3. [CA CEM for SSL を設定して、PEM ファイルを CA CEM にアップロードする](#) (P. 405)。
4. [SSL 対応の CA CEM を確認する](#) (P. 406)。

SSL 秘密鍵のインポートおよび管理

CA CEM は複数の秘密鍵をサポートしているため、各種の秘密鍵を使用してさまざまな HTTPS サーバの SSL トラフィックを分析することができます。CA CEM は、Apache サーバおよび OpenSSL ベースのサーバで使用される PEM 秘密鍵の形式をサポートしています。Microsoft IIS、SunONE、iPlanet、および Netscape は秘密鍵方式を使用していますが、これらの鍵を、CA CEM で使用するために PEM ファイルに変換することができます。CA CEM は、キャプチャしたデータの復号化に必要な鍵を自動的に識別します。

変換を実行するシステムで、OpenSSL が利用できる必要があります。OpenSSL は <http://www.openssl.org> から入手できます。

サポートされている Web サーバの SSL 秘密鍵を取得する方法の詳細については、以下を参照してください。

- [Apache または OpenSSL ベースの Web サーバ](#) (P. 400)。
- [Microsoft インターネット インフォメーション サービス \(IIS\)](#) (P. 400)。
- [SunONE、iPlanet、または Netscape エンタープライズ サーバ](#) (P. 401)。

Apache または OpenSSL ベースの Web サーバ秘密鍵の保存

CA CEM で使用できるように、Apache または OpenSSL ベースの Web サーバ秘密鍵ファイルを保存することができます。

以下の手順に従います。

1. サーバ構成ファイルを見つけます。例：

```
/etc/httpd/conf.d/ssl.conf
```

2. 秘密鍵ファイルを参照している SSL 証明書キー ファイルを探します。

例：

```
SSLCertificateKeyFile=/etc/httpd/conf/ssl.key/server.key
```

3. `output.pem` にそのファイルをコピーして名前を変更します。

詳細については、<http://httpd.apache.org/> および <http://www.openssl.org/> を参照してください。

Microsoft インターネット インフォメーション サービス (IIS) 秘密鍵のエクスポート

Microsoft インターネット インフォメーション サービス (IIS) の秘密鍵は、CA CEM が読み取れる形式にエクスポートする必要があります。このフォーマットは PFX です。変換を実行するシステムで、OpenSSL が利用できる必要があります。OpenSSL は <http://www.openssl.org/> から入手できます。

まず、IIS サーバから秘密鍵をエクスポートしてから、出力ファイルを PEM 形式に変換します。

PFX 形式で鍵をエクスポートする方法

1. IIS が実行されている Windows ベースのシステムで、[スタート] の [ファイル名を指定して実行] をクリックします。
2. 「MMC.exe」と入力し、[OK] をクリックします。
3. [コンソール] メニューの [スナップインの追加と削除] をクリックします。
4. [追加] をクリックします。[証明書] スナップインを選択し、[追加] をクリックします。
5. [コンピュータ アカウント] を選択し、[次へ] をクリックします。

6. [ローカル コンピュータ] を選択し、[完了] をクリックします。
7. [閉じる] をクリックした後、[OK] をクリックします。
8. [証明書] のメニューを展開し、[個人] フォルダをクリックします。エクスポートする証明書を右クリックし、[すべてのタスク] - [エクスポート] を選択します。
ウィザードが表示されます。
9. チェックボックスを選択し、秘密鍵を含めて、PFX ファイルの作成が完了するまでウィザードの処理が続行します。

PFX ファイルを PEM 鍵ファイルに変換する方法

1. OpenSSL ソフトウェアを実行しているシステム上で以下のコマンドを入力します。

```
openssl pkcs12 -in filename.pfx -nocerts -out output.pem
```

2. filename.pfx を、作成したファイルの名前に置換します。
3. output.pem を、作成中の出力ファイルの名前に置換します。
4. コマンドを実行します。

この PEM ファイルの作成時に指定するパスワードは、このファイルを TIM にアップロードする際に使用するパスワードです。

SunONE、iPlanet、Netscape Enterprise Server

Sun、SunONE、iPlanet、および Netscape の Web サーバはすべて同じコアテクノロジーをベースとしています。これらの秘密鍵は、CA CEM が読み取れる形式にエクスポートする必要があります。

変換の実行に使用するシステムには、以下のユーティリティが必要です。

- OpenSSL
- ネットワーク セキュリティ サービス (NSS)
- Netscape ポータブル ランタイム (NSPR)

以下の手順では、変換に Windows システムを使用するものと想定しています。

秘密鍵ファイルを作成する方法

1. 鍵管理ユーティリティをダウンロードして解凍します。
 - OpenSSL - <http://www.openssl.org/> から入手できます。
 - ネットワーク セキュリティ サービス (NSS) - <http://www.mozilla.org/projects/security/pki/nss/> から入手できます。
 - Netscape ポータブル ランタイム (NSPR) - <http://www.mozilla.org/projects/nspr/> から入手できます。
2. ファイルを解凍します。
 - zip ファイルを一時ディレクトリに解凍します。
 - nss-3.9.zip を c:¥ に解凍します。
 - nspr-4.4.1 を c:¥ に解凍します。
3. **Win32-OpenSSL-v0.9.7c** で有効 : Win32-OpenSSL-v0.9.7c を実行して C:¥OpenSSL ディレクトリにインストールします。
4. 以下の行が含まれるように、PATH 変数を変更します。
`c:¥nss-3.9¥lib;c:¥nspr-4.4.1¥lib`
SunONE/iPlanet/Netscape の証明書および鍵は .db 拡張子のファイルに保管されます。
5. *.db ファイルを書き込み可能なディレクトリ (この例では c:¥dbfiles) にコピーします。

6. コマンドプロンプトを開き、以下のコマンドを入力します。

```
cd c:\nss-3.9\bin
```

デフォルトでは、NSS ツールは `key3.db` および `cert7.db` という名前のファイルを検索します。データベースファイルの名前が `key3.db` および `cert7.db` 以外の名前の場合、ファイルの名前を変更しないでください。代わりに、`certutil` および `pk12util` を使用して通常とは異なる名前のファイルを見つけられるように、`-P` (プレフィックス) スイッチを指定します。

たとえば、ファイルの名前が `prodSite-cert.db` および `prodSite-key.db` の場合は、`certutil` コマンドを使用して、`prodSite-cert7.db` および `prodSite-key3.db` というファイルを作成します。このコマンドの出力には、含まれる証明書の名前が表示されます。

```
certutil -P prodSite- -K -d C:\dbfiles\
```

7. NSS 証明書 DB 用のパスワードまたは PIN を入力します (データベースパスワードを入力します)。

ファイル `prodSite-cert7.db` および `prodSite-key3.db` が作成されます。

エクスポートおよび変換を実行する方法

1. プロンプトで、以下のように入力します。

```
pk12util -P prodSite- -d C:\dbfiles\ -o C:\dbfiles\output.p12 -n Server-Cert
```

2. NSS 証明書 DB 用のパスワードまたは PIN を入力します (データベースパスワードを入力します)。

3. PKCS12 ファイル用のパスワードを入力します (出力パスワードを入力します)。

4. パスワードを再入力します (出力パスワードを再入力します)。

これで、`C:\dbfiles` ディレクトリに `output.p12` という名前のファイルが作成されます。

出力パスワードは、このファイルを Enterprise Manager にアップロードする場合に必要なパスフレーズです。

5. `OpenSSL\bin` ディレクトリから、以下のコマンドを実行します。

```
openssl pkcs12 -in C:\dbfiles\output.p12 -nodes -out C:\dbfiles\pkcs12out.txt
```

このコマンドは、`pkcs12` 構造を `MAC` および `バッグ` 情報を含むテキストファイルに変換します。また、秘密鍵および証明書の `PEM` ファイルも作成します。

`pkcs12out.txt` ファイルの内容は、以下の例のようになります。

```
Enter Import Password:
MAC verified OK
Bag Attributes
localKeyID: 01 00 00 00
1.3.6.1.4.1.311.17.1: Microsoft Enhanced Cryptographic Provider v1.0
friendlyName: 98849c683ad0e90810a77235bd728b12_668b93c6-0795-
4ba7-9da8-78737a299d3f
Key Attributes
X509v3 Key Usage: 10
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ+Mc6msuRWBUDHeIH2eV1
yiL7ID/0vkUN6qGnnqVuMQ3kuy7mnN/qSPz37/FKTbwF10QOP2LCZVuhU6SI/90Q
1rTINqQEPi1hyPV10LDv8Fjev80jMD1gvjaCmP84FzcrifyDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2WcgXsbYhaX0KI3fRdFFASI4XN0
ZdpolP7oY/cdF6w5EFsVc64t7dIpD+AineQpGeYJ4WhmBstyVlBSHb9drcCQDFg
vvcyfm13tTl3MfecV3WhENU6889iGogbgLMMQvqmtOCFDPY7fPM3I38FbEw03Yu+
gWEZ/f7DLdDSt7GDKf0CQQDSaQxwTMabqGB6bWxqy6M5lpWBW8YAQAXpKhLILRqb
C/Jx fd63KTN90pegkhE0Bn50dqtqfS4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----
Bag Attributes
localKeyID: 01 00 00 00
subject=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
issuer=/C=US/ST=Utah/L=SLC/O=MooseCo./OU=Moose
Land/CN=www.megamoose.com
-----BEGIN CERTIFICATE-----
MIICgDCCAemgAwIBAgIDBJ3zMA0GCSqGSIb3DQEBAUAMIGSMQswCQYDVQQGEwJa
QTEVMBMGA1UECBMMV2VzdGVybiBDYXBlMRIwEAYDVQQHEwLDYXBlIFRvd24xDzAN
BgNVBAoTB1RoYXd0ZTEdMBsGA1UECXMUQ2VydGlmawNhdGUgU2VydmljZXMxKDAm
BgNVBAMTH1BlcnNvbmsIEZyZWVtYWlsIFJTSQAyMDAwLjguMzAwHhcNMDEwNDE3
MDAzNzU5WhcNMDEwNDE3MDAzNzU5WjBFMR8wHQYDVQQDEwZUaGF3dGUgRnJlZW1h
aWwgTWVtYmV5MSIwIAYJKoZIhvcNAQkBFhNqbGV2eUBzb25pY3dhbGwuY29tMIGf
MA0GCSqGSIb3DQEBAQUAA4Ger3DBiQKBBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ
Y29tMAwGA1UdEwEB/wQCMAAwDQYJKoZIhvcNAQEEBQADgYEAChF7eiQDoCQ08snA
izV22+7FWiEKSR0PLc0FTyty0UJoQ0RLt7SPqKPJ2NswyC0A2nHgn0FL7ImFGiAi
5Xg9LEAtscgC7ceo0C3GBKorPE8hiqGCuVcCLYLws7yGRWRPTzQp7TemCoAM0cv
i0/6K6qicSzUpEj7eYqCbogmEYU=
-----END CERTIFICATE-----
```

- この例で示すように、EM 拡張子を付けた別のファイル（たとえば `output.pem`）に鍵のストラクチャをコピーアンドペーストします。

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDLIwhdY7ngYk/AlomX9rqnaZfb8PdJ+Mc6msuRwBUDHeIH2eV1
yiL7ID/0vkUN6qGnnqVuMQ3kuy7mnN/qSPz37/FKTbwF10QOP2LCZVuhU6SI/90Q
1rTINqQEPi1hyPV10LDv8Fjevvhv80jMD1gvjaCmP84Fzc rifyDgHonh4nQIDAQAB
AoGAUXaJIjjeDjge15MHNuQBUqXr+o4V/ZpA+2WcgXsbYhaX0KI3fRdFFASI4XN0
ZdpolP7oY/cdF6w5EFsVc64t7dIpD+AineQpGeYJ4WhmBstyVlBShNb9drcCQDFg
vvcyfm i3tTL3MfecV3WhENU6889iGogbgLMMQvqmt0CFDPY7fPM3I38FbEw03Yu+
gWEZ/f7DLDDsT7GDKf0CQQDSaQxwTMabqGB6bWxqy6M5lpwBW8YAQAXpKhlLILRqb
C/Jx fD63KTN90pegkhE0Bn50dqtqfS4kodv45bHeHYxn
-----END RSA PRIVATE KEY-----
```

SSL 対応の CA CEM の設定

以下の手順に従います。

- [設定] の [HTTPS 設定] を選択します。
- アドレスタイプを選択します。
- ユーザが選択するアドレスタイプに応じて、イーサネットまたは Web サーバ IP を指定します。

Web サーバ IP の場合は、単一のアドレスまたはアドレス範囲のいずれかを入力します。

範囲の例: 172.16.10.2-172.16.10.15

2つのアドレスを、スペースを入れずに単一のハイフンで区切ります。

- Web サーバ ポート番号を指定します。
- `output.pem` ファイルの場所 (クライアント コンピュータ上) を探索し、そのファイルを選択します。

秘密鍵ファイルを PEM 形式に変換する方法については、「[SSL 秘密鍵のインポートおよび管理 \(P. 399\)](#)」を参照してください。

- PEM ファイルを作成するのに使用したパスワードを [鍵ファイルパスワード] フィールドに入力します。

PEM ファイルの作成にパスワードを使用していない場合は、このフィールドを空白のままにします。

- [保存] をクリックして PEM ファイルをアップロードします。

Web サーバごとに異なる `output.pem` ファイルがある場合は、Web サーバごとにこの手順を繰り返します。

HTTPS サーバの複数の鍵

鍵ごとにポートまたはアドレスが異なる場合には、HTTPS サーバまたは一連の HTTPS サーバは複数の秘密鍵をサポートすることができます。たとえば、内部ユーザ用に 1 つのキーがあり、外部ユーザ用に別のキーがある HTTPS サーバが 1 つあるとします。この場合、一方のポートを内部鍵用に使用し、他方のポートを外部鍵用に使用できます。

同一のアドレス（またはアドレス範囲）/ポートのペアに 2 番目の鍵を入力すると、最初の鍵は上書きされます。アドレス範囲が重複している場合、鍵は別々に保持されます。ただし、TIM はどちらか一方の鍵のみ、つまり実際の IP アドレスとポートを含む最初に検出した鍵を使用します。

SSL 使用時の CA CEM 機能の検証

以下の手順に従います。

1. [CEM コンソールから](#) (P. 292) [TIM System Setup] ページにアクセスします。
2. [View TIM Transaction Inspection] をクリックします。
3. TIM が監視するコンピュータの IP アドレスを入力します。
4. [Start] をクリックし、SSL として定義されたトランザクションの監視を開始します。
5. 単純な（前述で定義した）HTTPS トランザクションを実行します。
数秒後にトランザクション検査データがページに表示されます。
6. トランザクション検査が完了したら、[Stop] をクリックします。

注: [Stop] をクリックしないと、検査データは収集され続けます。

第 23 章: CA CEM での Napatech アダプタの使用

Napatech アダプタをインストールすると、一部の高トラフィック環境で TIM パフォーマンスが改善される場合があります。

このセクションには、以下のトピックが含まれています。

[CA CEM での Napatech アダプタの使用について](#) (P. 407)

[Napatech アダプタおよびソフトウェアの入手](#) (P. 408)

[Napatech アダプタおよび Napatech ソフトウェアのインストール](#) (P. 408)

[Napatech アダプタおよび監視の有効化](#) (P. 410)

[\(オプション\) Napatech フィルタの作成および有効化](#) (P. 411)

[その他の Napatech アダプタ タスク](#) (P. 414)

[Napatech アダプタのトラブルシューティング](#) (P. 416)

CA CEM での Napatech アダプタの使用について

TIM マシンにアダプタをインストールすることで、TIM でのパケットドロップを防止できる場合があります。これは以下の方法で実行されます。

- TIM がパケットを処理するまで、アダプタ バッファにパケットが保存されます。
- アダプタでトラフィックがフィルタされるため、TIM で分析するトラフィックがより少なくなります。
- CPU での Napatech アダプタからのデータの読み込みは、その他の大部分の Ethernet アダプタより少ない時間で済み、TIM 用により多くの CPU 時間が残されます。

アダプタで重複したパケットを削除できます -- SPAN ポートで同じパケットが 2 回以上現れる場合に役立ちます。

TIM での Napatech アダプタ使用のプロセス

1. [適切なアダプタおよびソフトウェアの入手](#) (P. 408)
2. [アダプタおよびソフトウェアのインストール](#) (P. 408)

3. [アダプタを使用するよう TIM を構成 \(P. 410\)](#)
4. [\(オプション\) アダプタのフィルタの作成および有効化 \(P. 411\)](#)

Napatech アダプタおよびソフトウェアの入手

4つの電気的ギガビットインターフェースを備えた Napatech NT4E-4T PCIe アダプタは、TIM 用にサポートされている唯一のアダプタです。このアダプタはファイバケーブルと一緒に使用できません。

Network Allies, LLC は、必要な適正アダプタおよび Napatech ソフトウェアを両方とも提供できる唯一の再販業者です。この Napatech ソフトウェアは NT4E-4T PCIe アダプタ専用設計されています。

注: Multi-Port Monitor アプライアンスで実行される TIM は、さまざまな Napatech アダプタをサポートしています。サポートされているアダプタの詳細については、「*CA APM Compatibility Guide*」(CA サポートから入手可能)を参照してください。

Napatech アダプタおよび Napatech ソフトウェアを入手する方法

- Network Allies から NT4E-4T PCIe アダプタ (部品番号 801-0075-0800CA) を購入します。
パッケージには、ソフトウェアおよびインストール手順を含む DVD および USB フラッシュドライブの両方が含まれています。

Napatech アダプタおよび Napatech ソフトウェアのインストール

DVD および USB フラッシュドライブには、以下のものが含まれます。

- Napatech ハードウェア インストール手順
- TIM にインストールするソフトウェア イメージ
- サンプル フィルタ ファイル

アダプタをインストールする方法

1. DVD および USB フラッシュドライブで提供される NT4E-4T ハードウェア インストール ガイドの手順に従います。TIM マシンの PCI Express スロットへアダプタをインストールします。
2. トラフィック監視ケーブルを監視ポート（通常は eth1）からアダプタ内の任意のポートに移動させます。

注: また、「[Napatech アダプタおよび監視の有効化 \(P. 410\)](#)」の後に、この手順を実行することができます。後で実行すると、損失データが少なく済みます。ただし、この段階で実行すると、サーバへの変更手順が 1 つ少なく済みます。

ソフトウェアをインストールする方法

1. Napatech ソフトウェア イメージ (napatech-<バージョン>.image) をネットワークで利用可能にします。
2. napatech-<バージョン>.image を [TIM Wily System Setup] ページからインストールします。TIM ソフトウェアのインストールに関する一般情報については、「[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。

3. (オプション) 「Wily System Setup」ページに移動して、Napatech ソフトウェアがインストールされていることを確認します。

ソフトウェアがインストールされている場合、ページの行頭文字が付いた行に「Napatech<インストール タイム スタンプ>」が表示されます。(リンクではありません。)

4. (オプション) Napatech ドライバ ログを確認します。
 - a. TIM システム設定ページで、[Configure Napatech] をクリックします。
 - b. [View the Napatech Driver Log] をクリックします。

c. ログを確認します。

たとえば、このページのログに以下のような行が表示されるとします。

```
4B85587F.00030BC4 | #WARN | NOTE: The adapter will have limited throughput.  
(注: アダプタではスループットが制限されます。)
```

```
4B85587F.00030D15 | #WARN | Link negotiated to 4 lanes. Adapter supports 8  
lanes. (リンクは 4 つのレーンにネゴシエートされました。アダプタでは 8 つのレーン  
がサポートされます。)
```

その後、8 レーンスロットの代わりに 4 レーンスロットに Napatech アダプタをインストールしたとします。これは、Napatech ボードのパフォーマンスに影響する可能性があります、動作は停止されません。

Napatech アダプタおよび監視の有効化

Napatech アダプタおよび Napatech ソフトウェアのインストール後、以下の手順に従って、Napatech アダプタを有効にし、ntxc0 : 0 ポートを監視するように TIM を構成します。

アダプタを有効化する方法

1. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
2. [Enable Napatech] をクリックし、TIM を再起動します。

TIM が実行されていない場合は、[Enable Napatech] をクリックします。TIM を開始して、監視を始めます。

アダプタを使用するために TIM ネットワーク監視インターフェースを設定する方法

1. [TIM System Setup] ページで、[Configure Napatech] をクリックします。

TIM ネットワーク監視インターフェースの構成に関する一般情報については、「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。

2. ntxc0 : 0 インターフェースを選択し、[Set] をクリックします。

トラフィック監視対象ケーブルを別のインターフェースから ntxc0 : 0 へ移動済み、または移動する予定の場合、使用していないインターフェース用のチェックボックスをオフにします。TIM は ntxc0 : 0 インターフェースおよび eth1 などの別のインターフェースから、または ntxc0 : 0 インターフェースのみから監視することができます。

3. アダプタポートの 1 つへトラフィック監視対象ケーブルをまだ接続していない場合は、ここで接続してください。トラフィック監視ケーブルを監視ポート（通常は eth1）からアダプタ内の任意のポートに移動させます。

(オプション) Napatech フィルタの作成および有効化

Napatech アダプタは、ハードウェアでのパケットフィルタリングの手段を提供します。

フィルタは、NTPL (Napatech programming language) で記述してから TIM にアップロードします。サンプルフィルタファイルを使用してください。サンプルフィルタファイルは USB フラッシュドライブに含まれています。

TIM は、Web サーバ IP アドレスによってトラフィックをフィルタできます（この方法での TIM 監視の設定については、「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）。ただし、Napatech アダプタのみを使用してフィルタする方法をお勧めします。ハードウェアフィルタリングの方が処理が高速です。

TIM および Napatech フィルタの両方で Web サーバフィルタを設定した場合、これらのフィルタは AND 演算子を使用して解釈されます。つまり、フィルタの論理積になります。

Napatech アダプタフィルタを作成し有効にする方法

1. サンプルのフィルタ ファイル (sample_filter.ntpl) を DVD または USB フラッシュ ドライブからコピーし、環境に合わせて編集します (Notepad または vi のような通常のテキスト エディタを使用してください)。
注: ファイルの先頭に DeleteFilter= all コマンドがあることを確認してください。
2. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
3. [Upload a Napatech Hardware Filter Configuration] をクリックします。
[TIM Napatech Hardware Filter Configuration] ページが表示されます。
4. ファイルの場所を指定し、アップロードおよびインストールを行います。
5. (オプション) フィルタがインストールされていると確認します。
 - a. TIM システム設定ページで、[Configure Napatech] をクリックします。
 - b. [View the Napatech Hardware Filter Configuration File] をクリックします (TIM Napatech Configuration ページ)。または、[View the Napatech Hardware Filter Configuration Log] をクリックして詳細情報を参照してください。

重要: 新規ファイルをアップロードすると、古いファイルの情報は Napatech ハードウェア フィルタ構成ログまたはファイルページ上では表示されなくなります。ただし、古いフィルタ自体が削除されるのは、新規フィルタ ファイルの先頭に DeleteFilter = all コマンドがある場合のみです。

高度なフィルタの作成

このセクションの例に基づいて高度なフィルタを作成できます。

IP アドレスの範囲でフィルタする方法

以下の例では、10.11.28.23 ~ 10.11.28.32 の範囲の IP アドレスを使用してフィルタする方法を示します。

```
{[10.11.28.23]..[10.11.28.32]}.
```

注: 1 バイトしか変わらないとき、この範囲は最適に動作します。変化が 1 バイトを上回る場合、リソースを使い果たす可能性があります。

サブネット マスクを使用してフィルタする方法

- 以下の例では、サブネット マスクを使用してフィルタする方法を示します。たとえば、192.168.1.x アドレス (x の値は重要ではありません) をフィルタする場合は、以下のフィルタを使用します。

```
mIPv4SrcAddr=={[FF.FF.FF.00]:[192.168.1.0]}
```

- 以下の例は、マスクで 1 であるビットのみを比較します。たとえば、サブネットが 10.20.30.0 ~ 10.20.33.255 だった場合は、以下のフィルタを使用します。

```
{[FF:FF:FA:00]:[10.20.30.0]}
```

最後のバイトは、前のバイトの 2 ビットと同様にマスクされます。

複数のポートでフィルタする方法

以下の例では、2 つのポートでフィルタする方法を示します。

```
mTcpSrcPort == 43,80
```

注: 1 バイトのみが変わっている限り、最大 8 つの項目を指定できます。また、それは 1 つのフィルタ リソースのみを使用します。

フレームのデデュプリケーション

重複が互いの 8 つのフレーム内であり、タイムアウト基準（以下のミリ秒コマンドで指定された値まで）を満たす限り、Napatech アダプタは重複したフレームを削除します。

```
Deduplication [Timeout = 100] = Channel == 0,1,2,3
```

デデュプリケーションは、4 つのポートすべてからのトラフィックをマージし、重複したフレームの検出に対して 100 ミリ秒のウィンドウを適用します。高度なデデュプリケーションは、フレームの部分を除外し、フレームの IP の部分のみを確認できます。IP ヘッダおよび 16 バイトの追加の固定オフセットを除外します。

```
Deduplication [DynOffset = Layer2And3HeaderSize; Offset = 16; Timeout = 10] = Channel == 0,1,2,3
```

その他の Napatech アダプタ タスク

以下に示す追加の Napatech アダプタ タスクを実行する必要がある場合があります。

- Napatech アダプタからのフィルタの削除
- Napatech アダプタの取り外し
- Napatech アダプタ固有のログの表示

Napatech アダプタからのフィルタの削除

トラブルシューティングの際や、トラフィックのフィルタが必要なくなった場合には、Napatech アダプタからフィルタを削除することができます。

Napatech アダプタからのフィルタの削除方法

1. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
2. [Upload a Napatech Hardware Filter Configuration] をクリックします。
[TIM Napatech Hardware Filter Configuration] ページが表示されます。

3. [Delete all Napatech hardware filters] をクリックします。
削除により、Napatech アダプタのフィルタ設定にすべてをキャプチャする設定が適用され、トラフィックはすべて TIM に送信されます。
4. (オプション) フィルタが削除されたことを確認します。
 - a. TIM システム設定ページで、[Configure Napatech] をクリックします。
 - b. [View the Napatech Hardware Filter Configuration File] をクリックします (TIM Napatech Configuration ページ)。
ページで以下のように表示されていることを確認します。
Capture=All

Napatech アダプタの取り外し

別の TIM マシン上のアダプタを試す場合などに、TIM から Napatech アダプタを取り外す必要がある場合があります。

Napatech アダプタの取り外し方法

1. [ntxc0:0 interface] チェック ボックスをオフにします ([アダプタを使用するために TIM ネットワーク監視インターフェースを設定する方法 \(P. 410\)](#))。
2. Napatech アダプタを無効にします。
 - a. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
 - b. [Disable Napatech] をクリックし、TIM を再起動します。または、TIM が実行されていない場合は、[Disable Napatech] をクリックします。
3. TIM マシンから Napatech アダプタ ハードウェアを取り外します。

Napatech アダプタ固有のログの表示

Napatech アダプタ固有のログ ファイルは 2 つあります。

- 「TIM Napatech hardware filter configuration log」は、フィルタが適用または削除されたときに更新されます。
- 「Napatech driver log」は、Napatech ドライバがロードされる度に更新されます (ドライバは TIM が再起動すると必ずロードされます)。

TIM Napatech hardware filter configuration log を表示する方法

1. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
2. [View the Napatech Hardware Filter Configuration Log] をクリックします。

TIM Napatech hardware filter configuration log が表示されます。

Napatech driver log を表示する方法

1. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
2. [View the Napatech Driver Log] をクリックします。

Napatech driver log が表示されます。

Napatech アダプタのトラブルシューティング

Napatech アダプタおよび TIM ログについて

TIM ログでは、ネットワーク インターフェースに関連するメッセージにはすべて、先頭に AdapterManager が付けられます。たとえば、Napatech アダプタに関連するメッセージは ntxc0 : 0 インターフェースを参照します。
例 :

```
AdapterManager: "ntxc0:0": thread starting
```

トラブルシューティングのトピック

このページには、以下のトラブルシューティングのトピックがあります。

- [Napatech アダプタがトラフィックを受信しない](#) (P. 417)
- [Ethernet ポートとしての Napatech アダプタ](#) (P. 417)
- [目的のトラフィックが見当たらない](#) (P. 418)
- [シリアル番号および他の Napatech アダプタの詳細](#) (P. 418)

Napatech アダプタがトラフィックを受信しない

症状:

TIM がパケットを受信しません。TIM Packet Statistics ページを確認すると、パケットがキャプチャされていません。

表示されているトラフィックがあることを確認してください。ケーブルを ntxc0 : 0 ポートから eth1 ポートに移動させ、eth1 ポートを有効にします。これでパケットが表示されるようであれば、アダプタに問題があります。

解決方法:

インターフェースが有効であることを確認します（「[アダプタを使用するために TIM ネットワーク監視インターフェースを設定する方法 \(P. 410\)](#)」を参照してください）。

ソフトウェアが構成されていることを確認します。[ソフトウェアのインストール方法 \(P. 408\)](#)を参照してください。

ログを確認します。「[Napatech アダプタ固有のログの表示 \(P. 414\)](#)」を参照してください。

ログから問題を探します。「[Napatech アダプタ固有のログの表示 \(P. 414\)](#)」および「[Napatech アダプタおよび TIM ログについて \(P. 416\)](#)」を参照してください。

フィルタを削除します。「[Napatech アダプタからのフィルタの削除 \(P. 414\)](#)」を参照してください。

Napatech アダプタ自体に問題があると考えられる場合は、Network Allies にお問い合わせください。それ以外の場合は CA サポート にお問い合わせください。

Ethernet ポートとしての Napatech アダプタ

症状:

TIM 上の Linux プロンプトで ifconfig コマンドを入力しても、ntxc0 : 0 ポートが表示されません。オペレーティングシステムが Napatech アダプタを Ethernet ポートとして認識しません。

解決方法:

対処は不要です。Napatech アダプタは、このアプリケーションで正常に動作しています。

目的のトラフィックが見当たらない

症状:

トラフィックが表示されてはいますが、目的のトラフィックではありません。

症状:

監視対象として複数のインターフェースを有効にしている場合は、ntxc0:0 インターフェースからトラフィックを取得していることを確認するために、他のインターフェースをオフにします。ntxc0:0 インターフェースからトラフィックを取得していない場合は、「[Napatech アダプタがトラフィックを受信しない \(P. 417\)](#)」を参照してください。

フィルタを確認します。フィルタを削除します。目的のトラフィックが表示されましたか。表示される場合は、フィルタの内容を確認して編集し、再度適用します。ファイルの先頭に `DeleteFilter= all` コマンドがあることを確認してください。

シリアル番号および他の Napatech アダプタの詳細

症状:

使用している Napatech アダプタのシリアル番号が必要です

(Network Allies サポートへの問い合わせを行う際などに、シリアル番号が必要になる場合があります)。

解決方法:

Napatech status ページで Napatech アダプタに関する情報を参照することができます。

Napatech status ページを開く方法

1. TIM システム設定ページで、[Configure Napatech] をクリックします。
[TIM Napatech Configuration] ページが表示されます。
2. Napatech status を表示します。
Napatech AdapterInfo プログラムが実行され、出力が表示されます。

第 24 章: CA CEM で CA Introscope を使用する設定

CA CEM は 2 人の異なるユーザのニーズを満たします。Web ビジネスを担当するユーザはトレンド、サービス レベル、および成功率のレポートを取得でき、インシデントへの応答を担当するユーザはトランザクション障害の詳細をリアルタイムに把握できます。Introscope は、アプリケーションサーバレベルでの問題特定について、業界をリードするソリューションを提供します。CA CEM と CA Introscope とを統合すると、稼働中の Web アプリケーションをエンドツーエンドで完全に把握することができます。このソリューションが CA APM です。

エンドツーエンドのカスタマ エクスペリエンスをリアルタイムに把握することにより、新たな洞察を得ることができます。それにより、提供するサービスや顧客のロイヤルティを向上させ、さらに、顧客のオンライン エクスペリエンスを改善することが可能です。CA APM レポートで入手できるトランザクション問題切り分け情報は、IT とビジネスの両方の関係者のニーズを共に満たす共通言語を提供します。

CA CEM は、ビジネス マネジメントのパートナーとして IT の役割を向上させ、高品質なオンラインサービスの提供を可能にします。

この章では、CA CEM との統合用に Introscope をインストールおよび設定する方法について説明します。製品の併用の詳細については、「CA CEM と Introscope の併用」を参照してください。Introscope エージェント記録機能については、「CA APM トランザクション定義ガイド」を参照してください。

このセクションには、以下のトピックが含まれています。

[CA APM の開始 \(P. 422\)](#)

[CA APM カスタマ エクスペリエンス メトリックの概要 \(P. 422\)](#)

[CA APM 問題解決の切り分けの概要 \(P. 423\)](#)

[CA CEM 設定のためのチェックリスト \(P. 425\)](#)

[Introscope 設定のためのチェックリスト \(P. 439\)](#)

[CA Introscope および CA CEM 間の統合のトラブルシューティング \(P. 449\)](#)

[アップグレードに関する考慮事項 \(P. 452\)](#)

[ビジネスアプリケーションのセットアップ \(P. 453\)](#)

CA APM の開始

CA APM では、CA Introscope と CA CEM を統合する必要があります。

CA APM の開始方法を以下に示します。

1. CA CEM と CA Introscope を組み合わせて、企業が必要とするカスタマエクスペリエンス情報を入手する方法を理解します。「[CA APM カスタマエクスペリエンスメトリックの概要 \(P. 422\)](#)」を参照してください。
2. CA CEM と CA Introscope を組み合わせて、IT 問題の切り分けと解決に役立てる方法を理解します。「[CA APM 問題解決の切り分けの概要 \(P. 423\)](#)」を参照してください。
3. CA CEM 側の統合を設定します。「[CA CEM 設定のためのチェックリスト \(P. 425\)](#)」を参照してください。
4. CA Introscope 側の統合を設定します。「[CA Introscope 設定のためのチェックリスト \(P. 439\)](#)」を参照してください。
5. 統合機能が動作することを確認します。「[CA Introscope および CA CEM 間の統合のトラブルシューティング \(P. 449\)](#)」を参照してください。
6. CA CEM / CA Introscope 環境を CA APM にアップグレードする場合は、アップグレードに関する考慮事項を確認してください。「[アップグレードに関する考慮事項 \(P. 452\)](#)」を参照してください。

CA APM カスタマ エクスペリエンス メトリックの概要

CA CEM と CA Introscope のカスタマエクスペリエンスメトリック統合は、Enterprise Manager および各 TIM 上の設定パラメータによって制御されます。

1. TIM は、すべてのカスタマエクスペリエンスメトリックを、7秒ごと、または定義された間隔で、XML ファイルに書き込みます。書き込みは、メトリックが削除されるまで、またはエイジアウト期間に達するか期間を超えるまで続きます。
2. Enterprise Manager TIM コレクションサービスは、カスタマエクスペリエンスメトリックファイルを取得した後、TIM に対してそれらのファイルを削除するよう指示します。

3. また、Enterprise Manager TIM コレクションサービスは、カスタマエクスペリエンスメトリックデータを解析しますが、データを APM データベースに格納したり、データに対して何らかの集約操作を実行したりすることはありません。
4. カスタマエクスペリエンスメトリックは収集元の TIM ごとにグループ化されます。Enterprise Manager は、カスタマエクスペリエンスメトリックデータを SmartStor データベースに格納します。
5. CA Introscope Workstation は、集約と障害のパーセンテージを提供するための TypeView と計算機を使用して、デフォルトのビジネスダッシュボードを表示します。
6. 必要に応じて、同じカスタマエクスペリエンスメトリックデータを使用して、独自のカスタムビジネスダッシュボードを作成できます。「CA CEM と CA Introscope の併用」を参照してください。

TIM コレクションサービスの詳細については、「[Enterprise Manager サービスの配置](#) (P. 312)」を参照してください。

CA APM 問題解決の切り分けの概要

問題解決の切り分けのための CA CEM と CA Introscope の統合は、CA Introscope 構成設定によって制御されます。構成情報はドメイン構成情報に含まれており、ドメイン構成情報にはトランザクション定義、障害規格、およびトランザクション追跡パラメータが含まれます。

1. [設定] - [監視] - [すべての監視を同期] をクリックすると、CA CEM はドメイン構成情報への変更を CA Introscope に通知します（[すべての監視を同期] をクリックすると、CA CEM は TIM に対してもドメイン構成情報を送信します）。
2. CA Introscope エージェントはドメイン構成情報への更新をリスニングします（9.0 より前のエージェントで有効：CEMDefinitionHandler が解析済みドメイン構成情報を登録済みのすべてのエージェントに送信します）。
3. 続いて、登録済みの各エージェントは後でトランザクション追跡を有効にするルールセットを作成します。ルールセットは、CA CEM トランザクションを識別するパラメータ名/値の正規表現パターンで構成されます。

4. ServletHeaderDecorator がインストールされている Java エージェントは、各 HTTP 応答ヘッダに追加情報を付加します。ヘッダ情報には GUID が含まれます。GUID は、CA Introscope トランザクション追跡と CA CEM 障害を互いに関係付けるために後で使用されます。.NET エージェントに同じ機能を実装するには HTTPHeaderDecorator のインストールが必要です。
5. CA CEM TIM は HTTP 応答ヘッダを解析し、レポートされた障害に情報を含めます。この情報は Enterprise Manager に送信されます。
6. CA CEM は、障害および GUID の情報を APM データベースに保存します。
7. CA CEM は低速トランザクションインシデントを生成し、トランザクション追跡セッション開始要求を Enterprise Manager に送信します (CA CEM は、[設定] - [インシデント設定] に基づいて、低速トランザクションインシデントを生成し、インシデントステータスを保留中からオープンに変更します)。

トランザクション追跡セッション開始要求には、ビジネス トランザクション名およびトランザクション追跡時間しきい値が含まれます。このしきい値は低速トランザクション障害規格の割合です。トランザクション追跡は、インシデントがクローズするか、または設定されたトランザクション追跡セッション継続時間に達するまで実行されます。

8. BizTrxHttpTracer がインストールされているエージェントは、エージェントのルールセットに指定されたビジネス トランザクション名でトランザクション定義を探します。エージェントはパラメータ照合を使用して、CA CEM トランザクションを識別します
9. エージェントがトランザクションを識別し、そのトランザクション時間がトランザクション追跡時間しきい値を超えている場合、エージェントはトランザクション追跡を Enterprise Manager に送信します。
10. CA CEM はトランザクション追跡を受信し、APM データベースに格納された GUID と照合します。一致する GUID が見つかった場合、CA CEM はトランザクション追跡情報を APM データベースに保存します。

Enterprise Manager トランザクション追跡情報およびその他の CA CEM 障害情報は、インシデントを解決のために適切なチームにディスパッチする場合に有用です。「CA CEM と CA Introscope の併用」を参照してください。

CA CEM 設定のためのチェックリスト

CA Introscope と統合するための CA CEM の設定について知っておく必要のあることを以下に示します。

CA Introscope と共に CA CEM を設定する方法

1. 使用する統合機能を決定します。「[必要な統合機能の決定 \(P. 440\)](#)」を参照してください。
2. CA Introscope Workstation を設定します。「[CA Introscope Workstation の設定 \(P. 426\)](#)」を参照してください。
3. CA Introscope トランザクション追跡を設定します。「[トランザクション追跡の設定 \(P. 427\)](#)」を参照してください。
4. リアルタイム トランザクション メトリックを設定します。「[リアルタイム トランザクション メトリック統合の設定 \(P. 430\)](#)」を参照してください。
5. 統合機能が動作することを確認します。「[CA CEM 設定の確認 \(P. 439\)](#)」を参照してください。

必要な統合機能の決定

CA APM には 2 つのタイプの統合があります。

- 問題解決の切り分け - 関連する トランザクション 情報を利用することで、問題の根本原因の分析が可能になります。
- カスタマ エクスペリエンス メトリック - ビジネス トランザクション のボリューム、エラー、および平均応答時間を定期的に更新します。

問題解決の切り分けを希望する場合は、Introscope 設定を構成する必要があります。この構成により、Workstation および トランザクション 追跡の設定が可能になります。

カスタマ エクスペリエンス メトリックを希望する場合は、TIM コレクション サービスを構成する必要があります。この構成により、コレクタの設定と、各 TIM 上でのメトリック収集が可能になります。

ビジネス環境において何が必要かに応じて、両方の統合機能を使用するか、どちらか1つだけを使用することを選択できます。

注: CA Introscope エージェント記録機能を使用する場合は、「CA APM トランザクション定義ガイド」を参照してください。

詳細:

[Introscope の設定 \(P. 426\)](#)

[カスタマエクスペリエンスメトリック統合の設定 \(P. 430\)](#)

[CA CEM 設定の確認 \(P. 439\)](#)

Introscope の設定

CA APM 統合を有効にするには、CA Introscope をセットアップするための基本情報を収集する必要があります。

このセクションには、以下のトピックが含まれます。

[CA Introscope Workstation の設定 \(P. 426\)](#)

[トランザクション追跡の設定 \(P. 427\)](#)

[トランザクション追跡セッション情報の表示 \(P. 430\)](#)

CA Introscope Workstation の設定

Workstation Web Start アプリケーションと WebView アプリケーションの接続パラメータを設定する必要があります。

CA Introscope Workstation と通信するために CA CEM を設定する方法

1. [設定] - [Introscope 設定] を選択します。
[Introscope 設定] ページが表示されます。
2. Workstation Web Start リンクの有効化 - CA CEM からインシデントページと障害ページに Workstation Web Start リンクを表示できるようにする場合は、このチェックボックスをオンにします。このチェックボックスをオンにしない場合、インシデントページと障害ページにリンクは表示されません。

3. Introscope WebView 情報を入力します。
 - a. **WebView リンクの有効化** - CA CEM からインシデント ページと障害ページに **WebView** リンクを表示できるようにする場合は、このチェック ボックスをオンにします。このチェック ボックスをオンにしない場合、インシデント ページと障害ページにリンクは表示されません。
 - b. **ホスト名** - CA CEM 用の **WebView** をホストする CA Introscope システムのホスト名または IP アドレスを入力します。
 - c. **ポート** - Enterprise Manager が **WebView** への接続をリスニングするポートを入力します。**WebView** のデフォルトポート番号は 8080 です。
 - d. **コンテキストパス** - `introscope.webview.context.path` プロパティ値を入力します。この値は、CA Introscope のアプリケーション コンテキストパスを指定します。

注: `introscope.webview.context.path` のデフォルト値は "/" です (テキストボックス内では引用符不要)。このプロパティは、Enterprise Manager をホストするコンピュータの `<EM_Home>%config%` ディレクトリにある `IntroscopeWebView.properties` ファイルで定義されています。
4. [設定の保存] をクリックします。

CA CEM によって Introscope Workstation 設定情報が保存されます。
5. 「[トランザクション追跡の設定](#) (P. 427)」に進みます。

トランザクション追跡の設定

インシデントが生成され、以下のルールに基づく場合、CA APM 統合はトランザクション追跡を開始します。また、CEM でインシデントの [概要] ページから、トランザクション追跡を手動で開始することもできます。

注: CA CEM の障害に関するトランザクション追跡情報は、アプリケーションサーバ時間のしきい値が 15 ミリ秒以上の場合にのみ CA CEM の [障害詳細] ページに表示されます。

トランザクション追跡を設定するか、またはデフォルトの設定値をそのまま使用できます。

重要: トランザクション追跡を実行すると、インストゥルメントされたアプリケーションのパフォーマンスが低下する場合があります（関連する低速トランザクション障害の規格が低すぎる場合は、インストゥルメントされたアプリケーションが停止する可能性もあります）。これらの設定はビジネス トランザクションごとではなく、グローバルであることに注意してください。

CA Introscope トランザクション追跡を設定する方法

1. トランザクション追跡セッションの最大継続時間(分)を入力します。
デフォルトでは、トランザクション追跡は 30 分後に停止します。

CA CEM は、ビジネス トランザクションに開いているインシデントがあるときに限り、CA Introscope によるトランザクション追跡セッションを開始します。CA CEM では、ビジネス トランザクション別、かつ時間しきい値別に追跡が行われ、それぞれに対して特別のトランザクション追跡メソッドが使用されます。たとえば、Update Profile Web 要求については、1000 ミリ秒 (1 秒) より長くかかるものをすべて追跡します。

こうすることで、要求が Update Profile でないことが一度識別されれば、追加処理が必要なくなるため、エージェントのパフォーマンスを最適化できます。いくつかのトランザクション追跡セッションが実行されている可能性もありますが、オーバーヘッドは最小限に抑えられます。

2. 低速トランザクション障害規格のトランザクション追跡時間しきい値 (%) を入力します。

デフォルトは 50 パーセントです。

トランザクション追跡時間しきい値は、トランザクションの実行時間制限です。トランザクション追跡が実行されている場合、しきい値の時間内に完了しないトランザクションがすべて追跡されます。

トランザクション追跡時間しきい値は、低速トランザクション障害規格に対する割合 (%) で設定します。たとえば、低速トランザクション障害規格が 5.00 秒に設定され、トランザクション追跡時間しきい値が 50 パーセントに設定されている場合、CA Introscope 内 (アプリケーションサーバ上) で完了するまでに 2.50 秒より長くかかるトランザクションがすべて追跡されます。

デフォルト値の 30 分および 50 パーセントを使用する上の例では、以下のステートメントがすべて true である場合に、トランザクションが追跡されます。

- ビジネス トランザクションに開いているインシデントがある。
- そのトランザクションが完了するには 2.50 秒より長くかかる。
- トランザクション追跡が実行されている時間が 30 分未満である。

重要: 場合によっては、CA CEM の低速トランザクション障害規格を 1 ミリ秒 (1/1000 秒) などの非常に短い時間に設定する必要があることがあります。たとえば、エラーの場合にのみ発生するトランザクションに対して、このような短い時間を設定する場合があります。ただし、この同じトランザクションが CA Introscope トランザクション追跡に 関与している場合、1 ミリ秒の設定は Enterprise Manager MOM、Enterprise Manager Collectors、およびエージェントでパフォーマンスの問題を引き起こす場合があります。

3. バックエンド コンポーネントを入力します。CA Introscope では、特定のパターンに一致するあらゆるコンポーネントがバックエンド コンポーネントと見なされます。

アスタリスク (「*」) はワイルドカードで、常にパターンの最後に使用されます。

例: *Backends/**, *JDBC/**

各パターンは、1 つのカンマで区切られます。したがって、上記の例には

*Backends/** と *JDBC/** の 2 つのパターンがあります。

トランザクション追跡内のコンポーネントが *Backends/** または *JDBC/** で始まる場合、それはバックエンド コンポーネントとして認識されます。

4. [設定の保存] をクリックします。

CA CEM にトランザクション追跡の設定情報が保存されます。

注: トランザクション追跡セッションの監視の詳細については、「トランザクション追跡セッション情報の表示」を参照してください。

トランザクション追跡セッション情報の表示

現在実行されているトランザクション追跡セッションのリストを表示できます。特定のインシデントを選択して、その詳細情報を取得することもできます。

実行中のトランザクション追跡をすべて表示する方法

1. [CEM] - [インシデント管理] を選択します。
[インシデント] ページが表示されます。
2. [トランザクション追跡セッション] リンクを選択します。
現在実行中のトランザクション追跡のリストが表示されます。
3. インシデント番号をクリックすると、そのインシデントの [CEM] - [インシデントの概要] ページに直接移動します。

カスタマ エクスペリエンス メトリック統合の設定

このセクションでは、カスタマ エクスペリエンス メトリックを使ったアップグレード、サービスの開始/停止方法、およびオプションのトラブルシューティングについて説明します。

このセクションには、以下のトピックが含まれます。

- [カスタマ エクスペリエンス メトリックを使ったアップグレード \(P. 431\)](#)
- [カスタマ エクスペリエンス メトリック コレクション サービスの開始 \(P. 431\)](#)
- [RTTM コレクション サービスの停止 \(P. 432\)](#)
- [TIM 上でのカスタマ エクスペリエンス メトリックのトラブルシューティング \(P. 433\)](#)
- [カスタマ エクスペリエンス メトリック用の TIM 設定 \(P. 435\)](#)

カスタマ エクスペリエンス メトリックを使ったアップグレード

注: CA CEM の以前のリリースでカスタマ エクスペリエンス メトリックを使用していた場合は、「ビジネス プロセス」から「ビジネス サービス」へと用語が変更されたため、影響が生じる可能性があります。

アップグレード後に何もしない場合は、新しい用語の「ビジネス サービス」がダッシュボードメトリックに表示されます。

CA CEM 4.5 で有効: メトリックで「ビジネス プロセス」のメトリック名を維持するには、*tess-customer.properties* を設定し、CA CEM 4.5 Javascript 計算機を引き続き使用します。

カスタマ エクスペリエンス メトリックで「ビジネス プロセス」メトリック名を維持する方法

1. *tess-customer.properties* を設定して、プロパティ *BTStatsMetricName.backwardCompatible* を変更します。
tess-customer プロパティ ファイルの編集方法については、「[「tess-customer.properties」プロパティ ファイルの変更 \(P. 633\)](#)」を参照してください。
2. Enterprise Manager 上の Javascript 計算機を CA CEM 4.5 の計算機に置き換えます。*CEM-AggregatedTree.js* と *CEM-DefectPercent.js* を置き換えます。
 - a. *CEM_BT_Stats_package.zip* ファイルを取得します。
 - b. *CEM-AggregatedTree.js* を *<EM_Home>%scripts* ディレクトリへ抽出します。
 - c. *CEM-DefectPercent.js* を *<EM_Home>%scripts* ディレクトリへ抽出します。
 - d. Javascript 計算機を再ロードするために、Enterprise Manager を再起動します。

カスタマ エクスペリエンス メトリック コレクション サービスの開始

TIM コレクションサービスによってカスタマ エクスペリエンス メトリック収集が可能になります。通常、元のインストールおよび設定の一環として、TIM コレクションサービスを含む Enterprise Manager サービスを配置することになります。

Enterprise Manager サービスの詳細については、「[Enterprise Manager サービスの配置 \(P. 312\)](#)」を参照してください。

カスタマエクスペリエンスメトリックデータが表示されるためには、事前にTIMコレクションサービスを構成し、RTTMコレクションサービスを開始する必要があります。

カスタマエクスペリエンスメトリックコレクションサービスを開始する方法

1. [設定] - [サービス] - [サービス構成] を選択します。
2. [TIMコレクションサービス] を選択します。
3. [TIMコレクションサービス] リストで、[RTTMコレクションサービス] を選択します（まだ選択されていない場合）。
4. [開始] をクリックして、カスタマエクスペリエンスメトリックコレクションサービスを開始します。
5. [サービスステータス] が [停止] から [実行中] に変わることを確認します。

RTTMコレクションサービスの停止

場合によっては、カスタマエクスペリエンスメトリックコレクションサービスを停止することがあります。

RTTMコレクションサービスを停止する方法

1. [設定] - [サービス] - [サービス構成] を選択します。
2. [TIMコレクションサービス] を選択します。
3. [TIMコレクションサービス] リストで、[RTTMコレクションサービス] を選択します（まだ選択されていない場合）。
4. [停止] をクリックして、カスタマエクスペリエンスメトリックコレクションサービスを停止します。
5. [サービスステータス] が [実行中] から [停止] に変わることを確認します。

TIM 上でのカスタマ エクスペリエンス メトリックのトラブルシューティング

注: TIM 用のオプションの設定手順を以下に示します。TIM コレクションサービスの構成は、ほとんどの場合、[設定] - [サービス] - [サービス構成] から行う必要があります。TIM コレクションサービスの詳細については、「[Enterprise Manager サービスの配置 \(P. 312\)](#)」を参照してください。

TIM 上でのカスタマ エクスペリエンス メトリック収集は、一時的または永久に無効にすることができます。収集の頻度とファイルのエイジングを変更したり、環境内でトラブルシューティングするためのほかの設定を変更したりできます。

TIM 上のカスタマ エクスペリエンス メトリックを一時的に無効にする方法

1. [Wily System Setup] ページで、[TIM] - [Configure TIM Settings] を選択します（[Wily System Setup] ページへのアクセス方法については、「[TIM の \[System Setup\] ページへのアクセス \(P. 291\)](#)」を参照してください）。

[TIM Settings] ページが表示されます。

2. [Define a New Value] をクリックします。
3. 名前を入力します: *BtStats/Enabled*
4. 新しい値を入力します: *0*
5. [Change] をクリックします。

これで、この TIM 上でのカスタマ エクスペリエンス メトリック収集が一時的に無効になります。次回 Enterprise Manager を再起動するとき、収集は再開されます。

注: 上記の手順は、カスタマ エクスペリエンス メトリック収集が事前に有効にされていることを前提としています。

TIM 上のカスタマ エクスペリエンス メトリックを永久に無効にする方法

1. [Wily System Setup] ページで、[TIM] - [Configure TIM Settings] を選択します

[TIM Settings] ページが表示されます。

2. [Define a New Value] をクリックします。
3. 名前を入力します: *BtStats/ForceDisabled*

4. 新しい値を入力します： 1

これで、この TIM 上のカスタマエクスペリエンス メトリックを CA CEM から制御することができなくなります。

5. [Change] をクリックします。

これで、この TIM 上でのカスタマエクスペリエンス メトリック収集が無効になります。次回 Enterprise Manager を再起動しても、この TIM 上でカスタマエクスペリエンス メトリック収集は再開されません。

注: この TIM 上でのカスタマエクスペリエンス メトリック収集を CA CEM から再度制御できるようにするには、値をデフォルト値 0 に戻します。

多くの TIM 設定は、環境内で任意に変更することができ、カスタマエクスペリエンス メトリック用の TIM 設定で定義されます。このような TIM 設定が [TIM Settings] ページに表示されない場合は、デフォルト値に設定されています。

TIM 上のカスタマ エクスペリエンス メトリック処理を変更する方法

1. [Wily System Setup] ページで、[TIM] - [Configure TIM Settings] を選択します

[TIM Settings] ページが表示されます。

2. TIM 設定がすでに存在する場合は、以下の手順に従います。

- a. 名前をクリックします。
- b. 新しい値を入力します。
- c. [Change] をクリックします。

3. TIM 設定が存在しない場合は、以下の手順に従います。

- a. [Define a New Value] をクリックします。
- b. 新しい名前を入力します。
- c. 新しい値を入力します。
- d. [追加] をクリックします。

カスタマ エクスペリエンス メトリック用の TIM 設定

以下に示す TIM 設定は、カスタマ エクスペリエンス メトリックのトラブルシューティングに役立ちます。

このセクションには、以下のトピックが含まれます。

[BtStats/ForceDisabled](#) (P. 435)

[BtStats/Enabled](#) (P. 436)

[BtStats/IntervalInSeconds](#) (P. 436)

[BtStats/LogLevel](#) (P. 437)

[BtStats/WriteEmptyFiles](#) (P. 437)

[BtStats/MaxFileAgeInSeconds](#) (P. 438)

BtStats/ForceDisabled

この設定を使用すると、該当の TIM 上のカスタマ エクスペリエンス メトリック機能を制御することができます。また、CA CEM による制御をオーバーライドすることもできます。

設定

数値

- 0 (この TIM 上の機能を CA CEM から制御可能にします)
- 1 (この TIM 上の機能を強制的にオフにします)

デフォルト

0

例

BtStats/ForceDisabled = 0

注

- カスタマ エクスペリエンス メトリック機能は TIM 上で無効にすることができます。
- 1 = *BtStats/Enabled* TIM 設定 (次へ) を無視します。
- 0 = カスタマ エクスペリエンス メトリック機能を CA CEM によって制御し、*BtStats/Enabled* TIM 設定 (次へ) を使用します。

BtStats/Enabled

この設定を使用すると、該当の TIM 上のカスタマ エクスペリエンス メトリック機能を制御することができます。

設定

数値

- 0 (デフォルトで無効)
- 1 (有効)

デフォルト

0

例

BtStats/Enabled = 0

注

- Enterprise Manager を起動すると、TIM 上のこの設定が CA CEM によって制御されます。ただし、*BtStats/ForceDisabled* TIM 設定 (前へ) はこの設定をオーバーライドできます。
- また、TIM 上でのカスタマ エクスペリエンス メトリック収集を一時的に無効にするために、TIM 上のこの設定を変更することもできます。ただし、Enterprise Manager の次回の再起動で、その設定を変更できます。
- 「[TIM 上でのカスタマ エクスペリエンス メトリックのトラブルシューティング \(P. 433\)](#)」を参照してください。

BtStats/IntervalInSeconds

この設定では、TIM がリアルタイム トランザクション統計ファイルを書き込む頻度を制御できます。

設定

数値 (正の整数である必要があります)

デフォルト

7

例

BtStats/IntervalInSeconds = 7

注

リアルタイム トランザクション統計ファイルはディレクトリ `/etc/wily/cem/tim/data/out/btstats` の TIM に格納されます。

BtStats/LogLevel

この設定を使用すると、カスタマエクスペリエンス メトリックの TIM ログファイルエントリを制御することができます。

設定

数値

- 0
- 1
- 2

デフォルト

0

例

`BtStats/LogLevel = 0`

注

- 0 = メッセージなし (デフォルト)
- 1 = BtStats ファイルの書き込みが行われるとき、TIM ログにメッセージが書き込まれます。
- 2 = メッセージと同じ。詳細モード

BtStats/WriteEmptyFiles

この設定では、TIM が空のリアルタイム トランザクション統計ファイルを書き込むかどうかを制御できます。

設定

数値

- 0
- 1

デフォルト

0

例

BtStats/WriteEmptyFiles = 0

注

- 0 = 空のファイルは書き込まれない（デフォルト）
- 1 = 空のファイル（空の BTlist を含む）が書き込まれる
- これはトラブルシューティングに役立つ場合があります。たとえば、TIM の間隔の間にトランザクションが検出されない場合でも、空のファイルが空の BTlist（つまり、トランザクションの検出なし）と共に書き込まれます。これは、Enterprise Manager が実行されている状態、または実行されていない状態で、TIM が BtStats ファイルを作成しているかどうかをテストするために使用できます。
- リアルタイム トランザクション統計ファイルはディレクトリ `/etc/wily/cem/tim/data/out/btstats` の TIM に格納されます。

BtStats/MaxFileAgeInSeconds

この設定では、リアルタイム トランザクション統計ファイルが (CA CEM によって取得されない場合に) 保持される期間を定義できます。TIM はこの値より古いファイルを削除します。

設定

数値（正の整数である必要があります）

デフォルト

3600

例

BtStats/MaxFileAgeInSeconds = 3600

注

- 3600 = 1 時間（デフォルト）
- BtStats ファイルが保持される期間を定義します。TIM はこの値より古いファイルを削除します。

- この設定が高すぎると、TIM がディスク領域を使い果たしてしまう場合があります。
- この設定が低すぎると、ファイルが CA CEM によって取得される前に削除されてしまう場合があります。
- リアルタイム トランザクション統計ファイルはディレクトリ `/etc/wily/cem/tim/data/out/btstats` の TIM に格納されます。

CA CEM 設定の確認

CA APM 用に CA Introscope をまだ設定していない場合は、「[CA CEM 設定のためのチェックリスト \(P. 439\)](#)」に進んでください。

設定の確認とトラブルシューティングについては、「[CA Introscope および CA CEM 間の統合のトラブルシューティング \(P. 449\)](#)」を参照してください。

Introscope 設定のためのチェックリスト

このリストでは、CA CEM との統合用に CA Introscope を設定するために必要な事項を示します。

CA Introscope を CA CEM と統合する方法

1. 使用する統合機能を決定します。「[必要な統合機能の決定 \(P. 440\)](#)」を参照してください。
2. 問題解決の切り分けのために Enterprise Manager を設定します。「[Enterprise Manager の設定 \(P. 440\)](#)」を参照してください。
3. 問題解決の切り分けのために各 Java エージェントを統合します。「[Java エージェントとの統合 \(P. 442\)](#)」を参照してください。
4. 問題解決の切り分けのために各 .NET エージェントを統合します。「[.NET エージェントとの統合 \(P. 446\)](#)」を参照してください。
5. 統合機能が動作することを確認します。「[CA CEM 設定の確認 \(P. 449\)](#)」を参照してください。

必要な統合機能の決定

CA APM には 2 つのタイプの統合があります。

- 問題解決の切り分け - 関連するトランザクション情報を利用することで、問題の根本原因の分析が可能になります。
- カスタマエクスペリエンス メトリック - ビジネス トランザクションのボリューム、エラー、および平均応答時間を定期的に更新します。

問題解決の切り分けを希望する場合は、低速インシデントに関する問題解決の切り分け情報を表示するために、Enterprise Manager および影響のあるすべてのエージェントを設定する必要があります。

注: 問題解決の切り分けのための CA CEM 統合がサポートされるのは、AutoProbe でインストール済みの Java および .NET エージェントアプリケーションのみです。

カスタマエクスペリエンス メトリックを希望する場合は、収集されたメトリックを表示するために、Enterprise Manager ダッシュボードを設定する必要があります。「独自の CA CEM カスタマエクスペリエンス ダッシュボードの作成」を参照してください。

ビジネス環境において何が必要かに応じて、両方の統合機能を使用するか、どちらか 1 つだけを使用することを選択できます。

注: CA Introscope エージェント記録機能を使用する場合は、「CA APM トランザクション定義ガイド」を参照してください。

詳細:

[Introscope の設定](#) (P. 426)

[カスタマエクスペリエンス メトリック統合の設定](#) (P. 430)

[CA CEM 設定の確認](#) (P. 439)

Enterprise Manager の設定

CA CEM と CA Introscope との統合を有効にするように Enterprise Manager を設定する必要があります。

9.0 より前のエージェントで有効：4.5 の Enterprise Manager 拡張機能を以下のように再デプロイする必要があります。

- Enterprise Manager 拡張機能をダウンロードし、MOM および各 Enterprise Manager コレクタにインストールします。
- Enterprise Manager 拡張機能を再ロードするために、各 Enterprise Manager (JVM) を再起動します。

仮想エージェントとしての CA CEM の確立

CA CEM は Enterprise Manager の仮想エージェントとして設定する必要があります。以下の手順を実行すると、エージェント間でメトリックを集約できます。また、[Introscope Workstation Web Start に移動] リンクから、CA Introscope コンソールだけにリンクするのではなく、Investigator ツリーに直接リンクすることも可能になります。

CA CEM を仮想エージェントとして設定する方法

1. `<EM_Home>%config%agentclusters.xml` ファイルを見つけます。

重要: CA CEM は、1つの Enterprise Manager に接続するか、MOM Enterprise Manager に接続するように設定できます。CA Introscope 環境内に複数の Enterprise Managers がある場合は、MOM の `agentclusters.xml` ファイルのみを変更する必要があります。

2. `agentclusters.xml` ファイル内の関連するエージェント行のコメントを外します。

```
<agent-cluster name="CEM Agent" domain="SuperDomain">
  <agent-specifier>.*%|.*/agent-specifier>
  <metric-specifier>Customer Experience%|.*/metric-specifier>
  <metric-specifier>Business Segment%|.*/metric-specifier>
</agent-cluster>
```

重要: 名前またはドメイン属性を変更しないでください。変更すると、統合が正しく機能しなくなります。

3. `agentclusters.xml` ファイルへの変更を保存します。

この変更を有効にするために Enterprise Manager を再起動する必要はありません。

9.0 より前のエージェント用の Enterprise Manager 拡張機能のデプロイ

9.0 より前のエージェントで有効: この CA CEM 4.5 拡張機能をデプロイする必要があるのは、5.0 より前のエージェントが Enterprise Manager に接続されている場合です。

CA CEM と CA Introscope との統合を可能にするため、9.0 より前のエージェントに接続する各 Enterprise Manager には CA CEM 4.5 CEMDefinitionHandler Enterprise Manager 拡張機能をインストールする必要があります。

以下の手順に従います。

1. 必要なファイルを入手するには、CA サポート にお問い合わせください。
2. CA CEM 4.5 CEMIntroscopeIntegrationKit を入手するには、CA CEM ソフトウェア リンクを使用します。
3. Enterprise Manager 上の `<EM_Home>\ext` ディレクトリに `CEMDefinitionHandler.jar` をダウンロードします。
4. 「[Enterprise Manager の再起動](#) (P. 442)」に進みます。

Enterprise Manager の再ロード

Enterprise Manager 統合を完了して問題解決の切り分けを行うために、Enterprise Manager を再起動する必要があります。

JVM を再起動すると、Enterprise Manager 拡張機能が有効になります。

Enterprise Manager を再ロードする方法

1. Enterprise Manager 拡張機能を再ロードするために、Enterprise Manager を再起動します。
2. 「[9.0 より前のエージェント用の Enterprise Manager 拡張機能のデプロイ](#) (P. 442)」に戻り、9.0 より前のエージェントに接続する Enterprise Manager ごとに手順を繰り返します。

Java エージェントとの統合

CA CEM と Introscope の統合環境で使用する Java エージェントごとに以下の手順を実行する必要があります。

1. CA CEM トランザクションに關与するアプリケーションを Introscope 対応にするように AutoProbe 追跡を設定します。
2. AutoProbe および ServletHeaderDecorator のエージェント プロパティを確認します。
3. エージェント構成プロパティを再ロードするために、エージェント (JVM) を再起動します。

.NET エージェントと統合する必要がある場合は、「[.NET エージェントとの統合 \(P. 446\)](#)」を参照してください。

Java 環境での AutoProbe 追跡の設定

Introscope Investigator ツリー内の詳細は、エージェントフォルダ内の PBL ファイルでアクティブにされている BizTrxHttpTracer と ServletHeaderDecorator に基づいています。これらの PBD が有効である場合、CA Introscope では各ビジネス トランザクションのメトリックを表示できます。

いったん統合が完了すれば、CA CEM 内に表示されるのと同じトランザクション名を使用して、ビジネス トランザクションがツリー内に表示されます。

AutoProbe の詳細については、「[CA APM Java Agent 実装ガイド](#)」を参照してください。

Java エージェント上で AutoProbe 追跡を設定する方法

1. <Agent_Home>%wily%core%config ディレクトリ内の *IntroscopeAgent.profile* を開きます。
2. たとえば *introscope.autoprobe.directivesFile* プロパティを見つけます。
introscope.autoprobe.directivesFile=
default-typical.pbl
3. プロパティ内で指定された PBL ファイルを見つけます。
上記の例で言うと、*default-typical.pbl* です。
4. 指定された PBL ファイルをテキスト エディタで開きます。
5. PBL ファイルで、ServletHeaderDecorator.pbd 行のコメントを外します。

```
#####  
# Servlet Header Decorator  
#  
# Enable this PBD for CEM integration. It appends additional  
# information to the HTTP response that is then captured by CEM.  
# =====  
ServletHeaderDecorator.pbd
```

6. PBL ファイルへの変更を保存します。
7. 「[デフォルトのエージェントプロパティの Java 環境での検証](#) (P. 444)」に進みます。

CA Introscope 9.0 で有効: *biz-trx-http.pbd* はデフォルトで有効になっています。

9.0 より前のエージェントで有効: *CEMTracer.pbd* のコメント化も解除する必要があります。

デフォルトのエージェントプロパティの Java 環境での検証

エージェントプロファイルプロパティファイルを使用して、AutoProbe および ServletHeaderDecorator のデフォルトのエージェントプロパティを変更できます。

CA CEM に関連するすべてのプロパティは、CA Introscope と CA CEM の統合に対応するように事前設定されています。デフォルト値がインストール環境に適合するかどうかを確認する必要があります。

重要: 少なくともセキュリティ関連のプロパティを確認してください。たとえば、*introscope.agent.decorator.security* プロパティはデフォルトでは **clear** に設定されています。これは初期のテスト用には適切ですが、ファイアウォールの外部に知られたくないトランザクションヘッダ内の情報が開示される可能性があります。このプロパティを **encrypted** に設定することにより、実稼働環境のセキュリティを強化できます。

CA CEM 関連のエージェントプロパティの詳細については、「CA Introscope エージェントプロファイルプロパティ」を参照してください。

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。

エージェントプロファイルプロパティを確認する方法

1. <Agent_Home>\wily\core\config ディレクトリ内の *IntroscopeAgent.profile* を開きます。

2. エージェントプロファイルに含まれるプロパティを「CA Introscope エージェントプロファイルプロパティ」のプロパティの説明と比較します。たとえば、以下のプロパティをデフォルト設定から変更できます。
 - *introscope.agent.decorator.enabled* - Java エージェントのデフォルト設定を `false` から `true` に変更します。これにより、問題解決切り分け機能が有効になります。
 - *introscope.agent.decorator.security* - デフォルト設定を `clear` から `encrypted` に変更します。これにより、トランザクションヘッダ内の機密情報が保護されます。
3. デフォルト値を変更する必要がある場合は、*IntroscopeAgent.profile* ファイルにそのプロパティを追加してから設定しなければならないことがあります。
4. *IntroscopeAgent.profile* ファイルへの変更を保存します。
5. 「[Java 環境へのエージェントプロパティの再ロード \(P. 445\)](#)」に進みます。

ヒント：プロパティがまったく表示されないとわかりづらいため、デフォルト値をそのまま使用する場合でも、明示的にプロパティを追加することをお勧めします。

Java 環境へのエージェントプロパティの再ロード

統合を完了するためには管理対象アプリケーション用のエージェントを再起動する必要があります。

JVM を再起動すると、エージェントプロパティが再ロードされ、AutoProbe および ServletHeaderDecorator が有効になります。

Java エージェントのエージェントプロファイル プロパティを再ロードする方法

1. エージェントプロパティを再ロードするためにエージェントを再起動します。
2. 「[Java エージェントとの統合 \(P. 442\)](#)」に戻り、エージェントごとに手順を繰り返します。

.NET エージェントとの統合

CA Introscope と CA CEM の統合環境で使用する .NET エージェントごとに以下の手順を実行します。

1. CA CEM トランザクションに参与するアプリケーションを CA Introscope 対応にするように AutoProbe 追跡を設定します。
2. AutoProbe および HTTPHeaderDecorator のエージェント プロパティを確認します。
3. エージェント構成プロパティを再ロードするために、エージェント (CLR) を再起動します。

Java エージェントと統合する場合は、「[Java エージェントとの統合 \(P. 442\)](#)」を参照してください。

.NET 環境での AutoProbe 追跡の設定

Introscope Investigator ツリー内の詳細は、エージェント フォルダ内の PBL ファイルでアクティブにされている BizTrxHttpTracer と HTTPHeaderDecorator に基づいています。BizTrxHttpTracer が有効である場合、CA Introscope では各ビジネス トランザクションのメトリックを表示できます。

いったん統合が完了すれば、CA CEM 内に表示されるのと同じトランザクション名を使用して、ビジネス トランザクションがツリー内に表示されます。

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

.NET エージェント上で AutoProbe 追跡を設定する方法

1. <Agent_Home> ディレクトリ内の *IntroscopeAgent.profile* を開きます。
2. たとえば *introscope.autoprobe.directivesFile* プロパティを見つけます。
introscope.autoprobe.directivesFile=
default-typical.pbl
3. プロパティ内で指定された PBL ファイルを見つけます。
上記の例で言うと、*default-typical.pbl* です。

4. 指定された PBL ファイルをテキスト エディタで開きます。
5. PBL ファイルで、`httpheaderdecorator.pbd` 行のコメントを外します。

```
#####  
# HTTP Header Decorator  
#  
# Enable this PBD for CEM integration.  
# It appends additional information to the  
# HTTP response that is then captured by CEM.  
# =====  
httpheaderdecorator.pbd
```

6. PBL ファイルへの変更を保存します。
7. 「[V デフォルトのエージェントプロパティの .NET 環境での検証](#) (P. 447)」に進みます。

CA Introscope 9.0 で有効: `biz-trx-http.pbd` はデフォルトで有効になっています。

9.0 より前のエージェントで有効: `CEMTracer.pbd` のコメント化も解除する必要があります。

.NET 環境でのデフォルトのエージェント プロパティの検証

エージェント プロファイル プロパティ ファイルを使用して、`AutoProbe` および `HTTPHeaderDecorator` のデフォルトのエージェント プロパティを変更できます。

CA CEM に関連するすべてのプロパティは、CA Introscope と CA CEM の統合に対応するように事前設定されています。デフォルト値がインストール環境に適合するかどうかを確認する必要があります。

重要: 少なくともセキュリティ関連のプロパティを確認してください。たとえば、`introscope.agent.decorator.security` プロパティはデフォルトでは `clear` に設定されています。これは初期のテスト用には適切ですが、ファイアウォールの外部に知られたくないトランザクションヘッダ内の情報が開示される可能性があります。このプロパティを `encrypted` に設定することにより、実稼働環境のセキュリティを強化できます。

CA CEM に関連するエージェント プロパティの詳細については、「[CA APM .NET Agent 実装ガイド](#)」を参照してください。

エージェント プロファイル プロパティを確認する方法

1. <Agent_Home> ディレクトリの *IntroscopeAgent.profile* を開きます。
2. エージェント プロファイルに含まれるプロパティを「CA Introscope エージェント プロファイル プロパティ」のプロパティの説明と比較します。たとえば、以下のプロパティをデフォルト設定から変更できます。
 - *introscope.agent.decorator.enabled* - .NET エージェントのデフォルト設定は **true** です。これにより、問題解決切り分け機能が有効になります。
 - *introscope.agent.decorator.security* - デフォルト設定を **clear** から **encrypted** に変更します。これにより、トランザクションヘッダ内の機密情報が保護されます。
3. デフォルト値を変更する必要がある場合は、*IntroscopeAgent.profile* ファイルにそのプロパティを追加してから設定しなければならないことがあります。
4. *IntroscopeAgent.profile* ファイルへの変更を保存します。
5. 「[.NET 環境へのエージェント プロパティの再ロード](#) (P. 448)」に進みます。

ヒント：プロパティがまったく表示されないとわかりづらいため、デフォルト値をそのまま使用する場合でも、明示的にプロパティを追加することをお勧めします。

.NET 環境へのエージェント プロパティの再ロード

統合を完了するためには管理対象アプリケーション用のエージェントを再起動する必要があります。

CLR を再起動すると、エージェント プロパティが再ロードされ、AutoProbe および HTTPHeaderDecorator が有効になります。

.NET エージェントのエージェント プロファイル プロパティを再ロードする方法

1. エージェント プロパティを再ロードするためにエージェントを再起動します。
2. 「[.NET エージェントとの統合](#) (P. 446)」に戻り、エージェントごとに手順を繰り返します。

Introscope 設定の確認

CA APM 用に CA CEM をまだ設定していない場合は、「[CA CEM 設定のためのチェックリスト \(P. 425\)](#)」に進んでください。

設定の確認とトラブルシューティングについては、「[Introscope および CA CEM 間の統合のトラブルシューティング \(P. 449\)](#)」を参照してください。

CA Introscope および CA CEM 間の統合のトラブルシューティング

CA CEM と CA Introscope との統合に関するトラブルシューティングが必要になる場合があります。このセクションでは、統合の確認手順の概要およびトラブルシューティングの方法を示します。

このセクションには、以下のトピックが含まれます。

[CA CEM 上での CA Introscope 統合の確認 \(P. 449\)](#)
[症状と解決策 \(P. 450\)](#)

CA CEM 上での CA Introscope 統合の確認

CA CEM 上で統合を確認するには、いくつかの方法があります。

CA CEM 上で CA Introscope 機能を確認する方法

1. Enterprise Manager が正しく設定されていることを確認します。
「[CA Introscope 設定の構成 \(P. 426\)](#)」を参照してください。
2. Enterprise Manager との通信を確認します。
 - a. [システム] の [イベント] を選択します。
 - b. Enterprise Manager とエージェントの間に未解決の通信エラーがないことを確認します。
 - c. Enterprise Manager と TIM の間に未解決の通信エラーがないことを確認します。
 - d. 「[CA CEM イベントの表示 \(P. 377\)](#)」を参照してください。

3. 最新のドメイン設定情報（トランザクション定義、障害規格、トランザクション追跡パラメータなど）をエージェントに送信するため、すべての監視を同期します（すべての有効な TIM 監視にも送信されません）。
 - a. [設定] - [監視] を選択します。
 - b. [すべての監視を同期] をクリックします。
 - c. Enterprise Manager - エージェント間の通信がアクティブであることを確認します。エージェント ログ ファイルを参照します。
4. Enterprise Manager ログに関連のエラーメッセージがないかどうかを確認します。CA CEM 関連のメッセージを探します。たとえば、ログメッセージ内で「tess」または「Biz」の語を検索します。
5. トランザクション追跡セッションが適切なタイミングで実行されていることを確認します。「トランザクション追跡セッション情報の表示」を参照してください。
6. リアルタイム トランザクションメトリック機能が TIM コレクションサービスによって有効にされることを確認します。「[カスタマエクスペリエンスメトリックのための TIM の選択 \(P. 317\)](#)」を参照してください。
7. リアルタイム トランザクションメトリック機能が各 TIM 上で有効であることを確認します。
[「TIM 上でのカスタマエクスペリエンスメトリックのトラブルシューティング \(P. 433\)」](#)を参照してください。

症状と解決策

以下のトピックでは、CA CEM と CA Introscope の統合に関するトラブルシューティングに役立ついくつかのヒントを示します。

カテゴリ

[.NET \(P. 451\)](#)

[イベントとログ \(P. 452\)](#)

.NET

症状

.NET のトランザクションが、IP アドレスのホスト名に基づいて照合するように定義されている場合には認識されません（同じ条件で Java エージェントによって監視されるトランザクションは認識され、Investigator ツリーに適切に表示されます）。

考えられる解決策

IP アドレスの代わりに大文字のホスト名で照合されるようホスト名を変更します（ [ビジネス サービス] - [ビジネス トランザクション] - [トランザクション] - [コンポーネント] - [識別] ）。

症状

.NET wily.Agent アセンブリ バージョンが CA CEM 用の .NET エージェント拡張機能のバージョン番号と一致しない場合、.NET エージェントが再起動しません。

考えられる解決策

「エージェント.NET バージョンの設定」で定義されている手順に従います。

注: この手順は正確に実行する必要があります。machine.config ファイルを正しく更新しなかった場合、.NET エージェントは起動しなくなります。

CA Introscope に関するより大きな問題は以下のとおりです。

拡張機能のバージョン番号が .NET エージェントのバージョン番号と異なる場合、スタンドアロンのエージェント インストーラで拡張機能（DLL など）が正しくインストールされないケースがときおりあります。

このような状況の回避策は 2 つあります。

- アプリケーション単位で別のバージョン番号を受け入れるように設定します。

または

- すべてのアプリケーションで別のバージョン番号を受け入れるようにグローバルに設定します。

注: 選択できるオプションは 1 つのみです。両方のオプションを設定しないでください。

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。

イベントとログ

症状

監視の同期中、Enterprise Manager ログ ファイル メッセージが表示されます。

コレクタ Enterprise Manager へのドメイン設定 XML ファイルの送信に失敗しました。必須サービスは Enterprise Manager によって定義されませんでした。

注: CA CEM 4.x のエージェントを使用している場合、このような症状が発生する場合があります。

考えられる解決策

CEMDefinitionHandler Enterprise Manager 拡張機能が、MOM および各コレクタに、この順序でインストールされていることを確認します。

また、統合を完了するために、各 Enterprise Manager の JVM を再起動する必要があります。

詳細については、「[Enterprise Manager の構成](#) (P. 440)」を参照してください。

アップグレードに関する考慮事項

TESS は Enterprise Manager の一部になりました。

- 以前 CEMTracer で提供されていた機能は、現在 BizTrxHttpTracer によって提供され、デフォルトで有効です。（BizTrxHttpTracer もエージェント記録機能をサポートします。）
- [すべての監視を同期] をクリックすると、CA CEM は Enterprise Manager に通知を行います。また、ドメイン設定情報ファイル (*domainconfig.xml*) が共有 APM データベースに格納されます。
- TESS ログ ファイルがなくなりました。これまで TESS ログ ファイルに書き込まれていたメッセージは、<EM_Home>/logs の Enterprise Manager ログ ファイルに書き込まれるようになりました。

CA APM 統合用の CA CEM または CA Introscope をアップグレードする前に、特定の製品のアップグレード要件を「CA APM インストールおよびアップグレードガイド」で確認する必要があります。

CA CEM および CA Introscope 間の統合の場合、個々の手順を開始する前にアップグレードの計画を立てておくことを強くお勧めします。ユーザ独自の環境および特定の要件を考慮に入れると、途中で不必要な混乱を回避できます。

ビジネス アプリケーションのセットアップ

「CA APM トランザクション定義ガイド」の記載に従ってビジネス アプリケーションをセットアップする際には、CA SiteMinder の設定を使用していることを確認してください。

ビジネス アプリケーションの正しい設定を確認する方法

1. [認証タイプ] が [CA SiteMinder] であることを確認します。
2. [ユーザ識別パラメータ] タイプが [CA SiteMinder] で、パラメータ名が [UserName] または [DistinguishedName] であることを確認します。

CA SiteMinder 認証の一部のタイプ（匿名認証および証明書ベースの認証）の場合、SM_AGENTAPI_ATTR_USERNAME は空白です。この場合、ユーザを識別するために SM_AGENTAPI_ATTR_USERDN（識別名）の値を使用する必要があります。

3. [セッション識別パラメータ] タイプが [CA SiteMinder] で、パラメータ名が [セッション ID] であることを確認します。

第 25 章: CA SiteMinder と CA CEM の統合

CA CEM は CA SiteMinder セキュリティ ソフトウェアと連携します。CA SiteMinder は、シングル サインオン、Web アプリケーションへのユーザ アクセスの集中管理などのセキュリティ機能を提供します。

簡易認証では、CA SiteMinder プラグインを使用せずに（また、この章の手順を実行せずに）Cookie によってユーザおよびセッションを識別できる場合もあります。

ユーザ名とセッション ID が常にヘッダで確認されている場合、およびセッション ID に変更がなく、期限切れにもなっていない場合は、ユーザとセッションを識別するために Cookie パラメータ（たとえば、SMUSER と SMSESSION、HTTP_SM_USER と HTTP_SM_SESSION など）を使用することを検討してください。

シングル サインオン (SSO) または期限切れが近づいている Cookie が使用されている場合は、この章の記載に従って CA SiteMinder プラグインを使用する必要があります。このような場合、ユーザ名および静的な Cookie が要求ヘッダに常に含まれるわけではないため、Cookie を使用した簡易的な方法は使用できません。このため、TIM は CA SiteMinder サーバと通信して、ユーザとセッションを判別する必要があります。

このセクションには、以下のトピックが含まれています。

[CA SiteMinder のチェックリスト](#) (P. 456)

[CA CEM での CA SiteMinder の設定](#) (P. 456)

[カスタム CA SiteMinder エージェントの作成](#) (P. 458)

[CA CEM でのポリシー サーバの定義](#) (P. 459)

[CA CEM でのエージェントの定義](#) (P. 460)

[TIM SiteMinder ホスト設定の表示](#) (P. 461)

[CA SiteMinder の有効化](#) (P. 461)

[CA SiteMinder および CA CEM 間の統合のトラブルシューティング](#) (P. 462)

CA SiteMinder のチェックリスト

CA CEM と CA SiteMinder の統合について知っておく必要のあることを以下に示します。

CA SiteMinder と統合する方法

1. CA SiteMinder で、CA CEM のカスタム エージェント タイプを作成します。「[CA SiteMinder での CA CEM のカスタム エージェント タイプの作成](#) (P. 458)」を参照してください。
2. CA SiteMinder で、TIM ごとにカスタム エージェントを作成します。「[CA SiteMinder での TIM ごとのカスタム エージェントの作成](#)」を参照してください。
3. 共有秘密キーを定義します。「[CA CEM での CA SiteMinder の設定](#) (P. 456)」を参照してください。
4. ポリシー サーバを定義します。「[CA CEM でのポリシー サーバの定義](#) (P. 459)」を参照してください。
5. エージェント名を定義します。「[CA CEM でのエージェントの定義](#) (P. 460)」を参照してください。
6. CA SiteMinder を有効にします。「[CA SiteMinder の有効化](#) (P. 461)」を参照してください。
7. ビジネス アプリケーションをセットアップして、CA SiteMinder 認証を指定します。「[ビジネス アプリケーションのセットアップ](#) (P. 453)」を参照してください。
8. CA CEM が CA SiteMinder と連携していることを確認します。「[CA SiteMinder および CA CEM 間の統合のトラブルシューティング](#) (P. 462)」を参照してください。

CA CEM での CA SiteMinder の設定

CA CEM が CA SiteMinder と連携するためには、CA SiteMinder プラグインを設定する必要があります。

CA CEM で CA SiteMinder を設定する方法

1. [設定] - [プラグイン] を選択します。
[プラグイン] ページが表示されます。

2. [CA SiteMinder] を選択します。
[CA SiteMinder プラグイン] - [全般] ページが表示されます。
3. [SiteMinder プラグインの有効化] の下にある以下のいずれかのオプションを選択して、CA CEM と CA SiteMinder の統合をアクティブにします。
 - 4.x API
 - 5.x API

注: CA CEM-SiteMinder 統合は、ポリシー サーバへの通信に以下の 2 つの方法を使用しています。

- 4.x API と呼ばれる最初の方法は、プレーン共有秘密キーと呼ばれるプロセスを使用します。
- SiteMinder は、ホストベース登録と呼ばれるプロセスを使用した、より安全にエージェントをポリシー サーバに登録し、エージェントとポリシー サーバが通信できる方法もサポートしています。これは 5.x API と呼ばれます。

CA CEM-SiteMinder 統合は、両方の方法をサポートしています。

4. セッション Cookie 名を入力します。これにより、CA SiteMinder ユーザセッション情報が暗号化された形式で保存されます。

注: デフォルトのセッション Cookie 名は「SMSESSION」です。

5. 共有秘密キーを入力します。これは、カスタム エージェントと CA SiteMinder ポリシー サーバの間のトラフィックを暗号化するために、カスタム エージェント名と共に使用されます。

注: [共有秘密キー] フィールドは、手順 3 で 4.X API を選択した場合のみ表示されます。

共有秘密キーはテキスト値であり、CA CEM カスタム エージェント (複数可) を CA SiteMinder に設定する際に指定する値と一致している必要があります。

注: CA SiteMinder を設定する際には、すべての CA CEM エージェントに同じ共有秘密キーを使用する必要があります。

6. [Force Registration] をクリックします。

ホスト設定オブジェクト名を変更する場合や、TIM 内のホスト設定ファイルを再生成する場合には、[Force Registration] を使用できます。

注: [Force Registration] フィールドは、手順 3 で 5.X API を選択した場合のみ有効です。

7. [保存] をクリックします。

カスタム CA SiteMinder エージェントの作成

以下の手順は、CA CEM と CA SiteMinder ポリシー サーバを統合する方法を示しています。CA SiteMinder ポリシー サーバで、これらの手順を実行します。

CA SiteMinder での CA CEM のカスタム エージェント タイプの作成

以下の手順を 1 回実行する必要があります。複数の TIM がある場合でも、複数のカスタム エージェント タイプは必要ありません。

注: 以下の手順は、CA SiteMinder r6 の手順を示しています。それより新しいリリースでは、正確な手順は異なる場合がありますが、同じ機能を実行する必要があります。

CA SiteMinder で CA CEM のカスタム エージェント タイプを作成する方法

1. ブラウザを開き、ポリシー サーバ上の CA SiteMinder URL を入力します。
例：
`http://<IP_Address>/siteminder/smadmin2.html`
2. [ポリシーサーバーの管理] をクリックし、Java アプレットを使用して新しいエージェント タイプを定義します。
3. [オブジェクト] ペイン (左) で、[システム] タブをクリックします。
4. [表示] メニューで、[エージェントタイプ] がオンになっていることを確認します。
5. [オブジェクト] ペインで、[エージェントタイプ] アイコンをクリックします。
6. [編集] メニューから、[エージェント タイプの作成] を選択します。

7. カスタム エージェントが自らを識別するために使用する名前（たとえば *TIMAgent*）を入力します。
8. カスタム エージェント タイプの説明を入力します。
9. [エージェントタイプの定義] タブで、[RADIUS デバイス] チェックボックスをオフのままにし、[IETF ベンダー ID] テキストボックスを空のままにしておきます。
10. アクションが定義されていない場合は、新しいアクションを定義し、[タイプ] を [認証済み] に設定します。

CA CEM でのポリシー サーバの定義

ポリシー サーバは、Web アプリケーションを許可および認証する CA SiteMinder のコンポーネントです。CA SiteMinder の設定では、複数のポリシー サーバが含まれる場合があります。

ポリシー サーバを定義する方法

1. [設定] - [プラグイン] を選択します。[プラグイン] ページが表示されます。
2. [CA SiteMinder Web Access Manager] を選択します。
3. [CA SiteMinder プラグイン] ページで、[ポリシー サーバ] を選択します。
4. [新規] をクリックします。
[ポリシー サーバ] ページが表示されます。

5.x API で有効: 5.x API プラグインを選択すると、ホスト設定オブジェクトが存在する単一のポリシー サーバを追加できます。

ホスト設定オブジェクトには、複数のポリシー サーバを追加できます。

詳細については、「*CA SiteMinder* ポリシー サーバ管理ガイド」の「トラステッドホストのホスト設定オブジェクト」を参照してください。

5. ポリシー サーバがインストールされているコンピュータの IP アドレスおよび認証ポートを入力します。
6. **5.x API で有効**：5.x API プラグインを選択した場合は、以下のフィールドに情報を入力します。
 - SiteMinder 管理者ユーザ名
 - SiteMinder 管理者パスワード

注：登録を行うには、正しい権限を持つユーザ名およびパスワードを指定します。
7. [保存] をクリックします。

CA CEM でのエージェントの定義

CA SiteMinder エージェントは、セキュリティ保護されたリソースに対する要求を認可して CA SiteMinder ポリシー サーバに転送するソフトウェアモジュールです。

[プラグイン] > [エージェント] ページに、エージェントおよび関連する監視 (TIM) がリスト表示されます。初期状態では、エージェントと監視は同じ名前です。エージェントの CA SiteMinder によって使用される名前と正確に一致するように、エージェント名を変更します。

エージェントを定義する方法

1. [設定] - [プラグイン] を選択します。
[プラグイン] ページが表示されます。
 2. [CA SiteMinder] を選択します。
 3. [CA SiteMinder プラグイン] ページで、[エージェント] を選択します。
[エージェント] ページが表示されます。
- 5.0 API で有効**：5.0 API を使用して CA SiteMinder を有効にしている場合は、[エージェント] ページに [SiteMinder ホスト設定] フィールドも表示されます。

4. [エージェント] ページで、エージェントの IP アドレスをクリックします。
[監視] ページが表示されます。
5.0 API で有効：5.0 API を使用して CA SiteMinder を有効にしている場合は、[監視] ページに [SiteMinder エージェント名] および [SiteMinder ホスト設定] フィールドも表示されます。
5. CA SiteMinder によって使用される名前と正確に一致するように、CA SiteMinder エージェント名を更新します。
6. [保存] をクリックします。

TIM SiteMinder ホスト設定の表示

以下の手順に従います。

1. TIM システム設定ページにアクセスします。
2. [View TIM SiteMinder Host Configuration] をクリックします。
ホスト設定ファイルが表示されます。

注：[TIM System Setup] ページにアクセスする方法の詳細については、「CEM コンソールおよびセットアップ ページへのアクセス」を参照してください。

CA SiteMinder の有効化

CA CEM が CA SiteMinder と連携するためには、CA SiteMinder プラグインを有効にする必要があります。

CA CEM で CA SiteMinder を有効にする方法

1. [設定] - [プラグイン] を選択します。
[プラグイン] ページが表示されます。
2. [CA SiteMinder] を選択します。
3. [SiteMinder プラグインの有効化] チェック ボックスをオンにします。
4. [保存] をクリックします。

CA SiteMinder および CA CEM 間の統合のトラブルシューティング

CA CEM が CA SiteMinder と連携していることを確認する方法

1. CA SiteMinder が有効であることを確認します。
「[CA SiteMinder の有効化 \(P. 461\)](#)」を参照してください。
2. ポリシー サーバで正しい IP アドレスおよびポートが使用されていることを確認します。
「[CA CEM でのポリシー サーバの定義 \(P. 459\)](#)」を参照してください。
3. CA CEM および CA SiteMinder によって使用される共有秘密キーが同じであることを確認します。
「カスタム CA SiteMinder エージェントの作成」を参照してください。
4. CA CEM および CA SiteMinder によって使用されるエージェント名が同じであることを確認します。
「[CA CEM でのエージェントの定義 \(P. 460\)](#)」を参照してください。
5. ビジネス アプリケーションが正しく設定されていることを確認します。
「[ビジネス アプリケーションのセットアップ \(P. 453\)](#)」を参照してください。
6. CA CEM で、[設定] - [監視] - [すべての監視を同期] を選択して、監視を同期します。
7. CA CEM で、[設定] - [監視] - [IP アドレス] を選択して、TIM ログに確認のメッセージまたは CA SiteMinder に関するエラーメッセージがないかどうかを確認します。
8. CA SiteMinder エージェント ログにエラーメッセージがないかどうかを確認します。
9. CA SiteMinder で、ポリシー サーバ ログにエラーがないかどうかを確認します。

第 26 章: CA Service Desk と CA CEM の統合

必要に応じてチケットが生成およびトラッキングされるように、CA CEM インシデントおよび障害情報を CA Service Desk に送信できます。

CA Service Desk は、サービス サポート インシデント管理を自動化することで、Information Technology Infrastructure ライブラリ (ITIL) のベストプラクティスプロセスを使用します。

このセクションには、以下のトピックが含まれています。

[CA Service Desk と CA CEM について](#) (P. 463)

[CA Service Desk 統合の概要](#) (P. 463)

[CA CEM との統合用の CA Service Desk の設定](#) (P. 464)

[CA Service Desk と CA CEM の併用](#) (P. 468)

[CA Service Desk および CA CEM 間の統合のトラブルシューティング](#) (P. 469)

[CA Service Desk と CA CEM との統合で使用される用語](#) (P. 471)

CA Service Desk と CA CEM について

CA Service Desk は、ヘルプ デスク アナリストが行うインシデント管理のタスクをサポートします。インシデントの検出と記録、分類とサポート、追跡と解決などのタスクがあります。

CA CEM と CA Service Desk を設定することで、CA CEM によって検出されたインシデントに基づいて CA Service Desk 内にサービス要求（またはインシデント）が作成されるようにすることができます。

CA Service Desk 統合の概要

CA Service Desk を統合すると、CA CEM のインシデントからサービス要求を自動的に生成することにより、インシデント管理がサポートされます。

CA Service Desk で CA CEM インシデントを作成できるようにするには、CA Service Desk プラグインを設定して有効にしてください。設定により通信が確立され、インシデントが CA Service Desk に表示される方法が定義されます。

CA CEM によって生成されたインシデントを CA Service Desk 内で分離する場合は、CA Service Desk でリクエスト領域を作成してください。

統合関連の用語については、「[CA Service Desk と CA CEM との統合で使用する用語 \(P. 471\)](#)」を参照してください。すべての CA APM 用語および定義については、「CA APM 用語集」を参照してください。

CA CEM との統合用の CA Service Desk の設定

CA Service Desk を有効にするには、事前に CA Service Desk プラグインを設定する必要があります。

オプションで、CA Service Desk 要求領域を作成して、CA Service Desk 内の他のサービス要求から CA CEM インシデントを分離できます。

CA Service Desk プラグインの設定

CA Service Desk プラグインを実装するには、接続と要求の情報を収集する必要があります。

CA Service Desk と通信できるように CA CEM を設定する方法

1. [設定] - [プラグイン] を選択します。
[プラグイン] ページが表示されます。
2. [CA Service Desk] を選択します。
[CA Service Desk プラグイン] ページが表示されます。
3. [CA Service Desk プラグインの有効化] チェック ボックスをオンにします。

これにより、CA CEM から CA Service Desk にインシデント情報を送信できるようになります。

注: CA Service Desk プラグインを有効にしないと、統合が機能しません。

4. 外部で解決可能なホスト名 - ほとんどの場合、このフィールドには CA CEM のホスト名がすでに含まれています。含まれていない場合は、Enterprise Manager の IP アドレスまたはホスト名を入力します。

この情報は、CA Service Desk で生成される電子メール内のリンクに使用されます。CA Service Desk の電子メールには、CA CEM のインシデントへのリンクが含まれます。

5. ポート - ほとんどの場合、このフィールドには CA CEM のポートがすでに含まれています。
注: デフォルトのポートは 8081 です。これは、`IntroscopeEnterpriseManager.properties` ファイルに `introscope.enterprisemanager.webserver.port=8081` として定義されていますが、この番号は変更できます。
6. CA Service Desk の接続情報を以下のように入力します。
 - a. ホスト名 - CA CEM をホストする CA Service Desk システムのホスト名または IP アドレスを入力します。
 - b. ポート - CA CEM が CA Service Desk に接続するためのポートを入力します。CA Service Desk のデフォルトポート番号は 8080 です。
 - c. ユーザ名 - CA Service Desk にアクセスするための CA CEM ユーザ名を入力します。このユーザは、CA Service Desk で要求を作成するための適切な権限とアクセス レベルを持っている必要があります。
 - d. パスワード - ユーザ名に関連付けられたパスワードを入力します。
7. CA CEM のインシデントを CA Service Desk で（要求ではなく）インシデントとして作成したい場合は、[Service Desk で ITIL インシデントを作成] チェック ボックスをオンにします。
CA Service Desk でインシデントを作成したくない場合は、デフォルトの動作で要求が作成されます。
注: CA Service Desk のインシデントが作成されるのは、CA Service Desk が ITIL (Information Technology Infrastructure Library) 用に設定されている場合のみです。そうでない場合、CA CEM のインシデントは要求として作成されます。
8. [要求領域] の入力 - CA Service Desk で作成された要求領域を入力して、CA CEM に関する問題を分類します。
この要求領域は、CA Service Desk で作成した名前と同じである必要があります。
9. 必要な場合は、[要求フィルタ] を入力します。

ヒント：すべてのインシデントをすぐに CA Service Desk に転送できるようにする代わりに、要求フィルタを使用して、最初に 1 つのビジネス サービスとビジネス トランザクションの統合をテストすることができます。

| 構文例 | 説明 |
|---|--|
| <i>Request Filter=BusinessServiceName/BusinessTransactionName</i> | 指定したビジネス サービスとビジネス トランザクションに関するインシデントが発生した場合にのみ、CA Service Desk で要求を作成します。 |
| <i>Request Filter=BusinessServiceName/*</i> | 指定したビジネス サービスに関してトリガされたすべてのインシデントと任意のビジネス トランザクションに関して、CA Service Desk で要求を作成します。 |
| <i>Request Filter=BusinessServiceName/Tra*</i> | 指定したビジネス サービスに関してトリガされたすべてのインシデントと「Tra」で始まる任意のビジネス トランザクションに関して、CA Service Desk で要求を作成します。 |
| <i>Request Filter=*/*</i> | すべてのビジネス サービスとすべてのビジネス トランザクションに関連付けられたインシデントに関して、CA Service Desk で要求を作成します。 |

ビジネス サービス名またはビジネス トランザクション名にスラッシュ

(/) 文字が含まれる場合、フィルタではそれを二重のスラッシュ (//) に置き換える必要があります。

ビジネス サービス名またはビジネス トランザクション名にカンマ (,) 文字が含まれる場合、フィルタではそれをスラッシュとカンマ (/,) に置き換える必要があります。

たとえば、以下のような名前があるとします。

- ビジネス サービス名 =Trade
- ビジネス トランザクション名 = Sell Big/Medium Stocks

この場合は、フィルタを以下のようにします。

Request Filter=Trade/Sell Big//Medium Stocks

たとえば、以下のような名前があるとします。

- ビジネス サービス名 =Trade
- ビジネス トランザクション名 = Sell Big, Medium Stocks

この場合は、フィルタを以下のようにします。

Request Filter=Trade/Sell Big/, Medium Stocks

10. CA Service Desk のサマリに表示される [要求サマリ] を入力します。カスタマイズしたサマリを作成するには、以下の変数を使用します。

- *<defect_name>*
- *<business_service>*
- *<business_transaction>*

これらの変数を並べ替えて、独自の要求サマリを作成できます。各変数は、要求サマリが CA Service Desk に表示されるときに実際の値に置き換えられます。例：

<defect_name> for <business_service>,<business_transaction>

これは、「Slow Time for Support Desk, KB Lookup」のように表示されます。

Business Transaction: <business_transaction> Defect: <defect_name>

これは、「Business Transaction: CheckOut Defect: Slow Time」のように表示されます。

11. CA Service Desk の説明に表示される [要求の説明] を入力します。変数を使用して、カスタマイズした説明を作成します。

- *<incident_id>*
- *<defect_name>*
- *<business_service>*
- *<business_transaction>*
- *<user_count>*
- *<defect_count>*
- *<incident_link>*

変数を並べ替えて、独自の要求の説明を作成できます。各変数は、要求の説明が CA Service Desk に表示されるときに実際の値に置き換えられます。

<incident_link> 変数は、CA Service Desk にリンクを提供します。インシデントの概要情報（ [CEM] - [インシデント管理] - インシデントの [概要] ）に直接移動するリンクを使用できます。

12. インシデント重大度が以下の場合に **Service Desk** 要求を作成する - **CA Service Desk** でサービス要求を作成するために、選択したインシデントレベルを有効にします。以下の中から該当するチェックボックスをオンにします。

- 低
- 中程度
- 深刻
- クリティカル

13. [保存] をクリックします。

その後、保存した設定と一致する **CA CEM** インシデントが発生すると、すぐに **CA Service Desk** 内でサービス要求が開始されます。

注: **CA CEM** で既存のインシデントが開いている場合、それらは **CA Service Desk** 要求のトリガになりません。

CA Service Desk 要求領域の設定

CA CEM によって報告されたインシデントの要求領域を分離する場合は、**CA Service Desk** にリクエスト領域を作成する必要があります。

CA CEM の CA Service Desk に要求領域を設定する方法

1. 要求領域（たとえば *CEM_reported*）を作成します。
2. 以下の 3 つのプロパティを要求領域にアタッチします。
 - ビジネス サービス
 - ビジネストランザクション
 - インシデント

要求領域の作成および設定については、**CA Service Desk** オンラインヘルプの「*Defining Request Areas*」を参照してください。

CA Service Desk と CA CEM の併用

CA Service Desk では、**CA CEM** インシデント情報を参照できます。**CA Service Desk** から **CA CEM** へのリンクをクリックすると、インシデントの詳細を表示できます。

CA CEM 内を移動して、インシデントの根本原因をトラブルシューティングおよび検出することができます。

CA Service Desk および CA CEM 間の統合のトラブルシューティング

CA Service Desk との統合に関するトラブルシューティングが必要になる場合があります。このセクションでは、問題解決法を示します。

症状と解決策

ここでは、CA Service Desk と CA CEM の統合に関するトラブルシューティングに役立ついくつかのヒントを示します。

症状:

一部またはすべての CA CEM インシデントに対して CA Service Desk 要求が作成されません。

解決方法:

CA Service Desk プラグインが CA CEM で以下のように正しく設定されていることを確認します。

適切な CA Service Desk クレデンシャルが設定されている。

適切なビジネス サービスおよびビジネス トランザクションにフィルタが設定されている。

適切な重大度レベルが有効になっている。

以下のログ ファイルをチェックして、接続またはその他のエラーがあるかどうかを調べます。

`http://<IP_Address>/cgi-bin/wily/packages/cem/service-desk/index`

症状:

CA Service Desk 要求が要求領域なしで作成されます。

解決方法:

要求領域が CA Service Desk 管理者によって作成されていることを確認します。

CA CEM CA Service Desk プラグイン構成に適切な要求領域情報が含まれていることを確認します。

症状:

CA Service Desk のインシデントまたは要求に含まれる CA CEM インシデント詳細へのリンクが機能しません。

解決方法:

インシデントが CA CEM データベースから削除されている可能性があります。

[セットアップ] > [インシデント設定] > [インシデント エイジアウトルール] を確認します。

症状:

CA Service Desk の電子メールに含まれる CA CEM インシデント詳細へのリンクが機能しません。電子メール内のリンクは、以下のような場合があります。

<http://localhost.localdomain/wily/cem/tess/...>

解決方法:

CA CEM CA Service Desk プラグイン構成に CA CEM 用の外部で解決可能なホスト名が含まれていることを確認します。

インシデントが CA CEM データベースから削除されている可能性があります。 [セットアップ] > [インシデント設定] > [インシデント エイジアウトルール] を確認します。

症状:

CA CEM でクローズしたインシデントが、CA Service Desk ではクローズしません。

解決方法:

インシデント/サービス要求を CA Service Desk で個別にクローズする必要があります。

症状:

CA Service Desk でクローズしたインシデント/サービス要求が、CA CEM ではクローズしません。

解決方法:

CA CEM でインシデントを個別にクローズする必要があります。

CA Service Desk と CA CEM との統合で使用される用語

用語は製品統合における重要な要素です。製品に詳しくない場合は、使用される用語の意味をよく理解しておく必要があります。また、CA CEM の用語や定義が CA Service Desk の用語とどのように対応しているかも理解しておく必要があります。

CA Service Desk の用語

製品統合に関連する CA Service Desk の用語を以下に示します。

インシデント

IT インフラストラクチャのサービス品質の低下を引き起こすイベントです。

要求領域

CA Service Desk システム管理者は要求領域をセットアップして、サービス要求をタイプ別に分類します。たとえば、ハードウェア サポートやソフトウェア インストールなどです。

サービス要求

ユーザからのサポート、情報提供、またはヘルプに関する要求です。IT インフラストラクチャの障害は含まれません。

チケット

「チケット」は CA Service Desk で一般的に使用される用語です。これは、要求、インシデント、問題などを意味する場合があります。CA Service Desk 内の CA CEM インシデントは、要求またはインシデントのいずれかに分類されます。

CA Service Desk と CA CEM の用語の対応

展開のサイクルやマニュアルの対象読者は製品によって異なる場合があります。これらの違いは、多くの場合、製品の用語や定義も異なることを意味します。

1 対 1 に対応していることもあります（たとえば、ある製品のインシデントが別の製品のチケットに対応している場合があります）。また、同じ用語でも製品によって意味が微妙に異なることもあります。これにより、混乱が発生する場合があります。

用語の対応を理解しておくこと、製品の統合作業をスムーズに進めることができます。

| CA CEM の用語 | CA Service Desk の用語の対応 |
|------------|--|
| インシデント | CA CEM インシデントは、CA Service Desk 構成および CA CEM 構成（ [設定] - [プラグイン] ）に基づいて、サービス要求またはインシデントのいずれかをトリガします。 |

第 27 章: CA APM Cloud Monitor の CA APM への統合

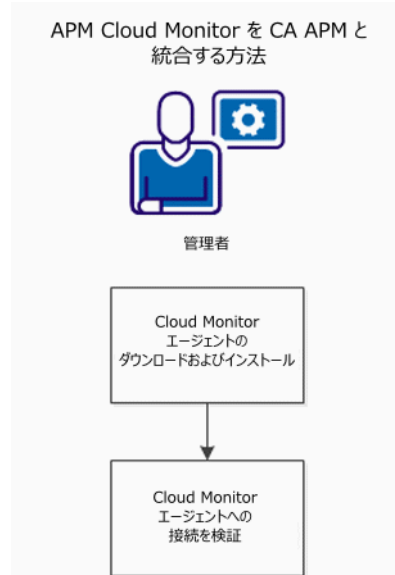
CA APM Cloud Monitor を使用すると、以下のタスクを実行できます。

- 40 以上の国々の 60 以上の監視ステーションからすべてのユーザエクスペリエンスを把握する。
- 実際のブラウザで監視を行い、ユーザエクスペリエンスを正確に計測する。
- SaaS ベンダーおよび MSP が提供するアプリケーションの監視により、SLA の遵守を図る。
- ファイアウォールの外部からのアプリケーション応答時間を（合成トランザクションによって）テストし、エンドユーザエクスペリエンスをグローバルに把握する。また、ユーザトラフィックが発生していない場合にもパフォーマンスを監視する。
- 実際のユーザトランザクションをレプリケートして、アプリケーションインフラストラクチャ全体にわたってパフォーマンスを監視することで、問題を迅速に特定、診断、および解決する。

CA APM 導入環境に CA APM Cloud Monitor を統合する方法

APM 管理者は、CA APM の導入環境に CA APM Cloud Monitor を統合して、監視および問題切り分けの機能を拡張できます。

以下のフローチャートは、オンプレミスの CA APM 導入環境に CA APM Cloud Monitor を統合する方法を示しています。



1. [CA APM Cloud Monitor エージェントをダウンロードしてインストールします。](#) (P. 476)
2. [エージェント接続を検証します。](#) (P. 477)

CA APM Cloud Monitor エージェントのダウンロードおよびインストール

このタスクでは、CA APM Cloud Monitor エージェントをダウンロードしてインストールします。このエージェントは、CA APM Cloud Monitor と CA APM を統合するために必要です。

注: CA APM Cloud Monitor エージェントは、ネットワーク上の任意のコンピュータにインストールできます。その機能は、インターネットを介して CA APM Cloud Monitor データを受信し、Enterprise Manager にそのデータを転送することです。任意のコンピュータにインストールすることができますが、サーバレベルの CPU/RAM を持ったコンピュータを選択する必要があります。

CA APM Cloud Monitor エージェントをダウンロードしてインストールする方法

1. CA APM Cloud Monitor エージェント アーカイブ ファイルをダウンロードします。そのファイルをコンピュータに保存します。

Windows、Linux、および Solaris 用のインストーラは、CA APM ソフトウェアダウンロード Web サイトにあります。

2. エージェントをインストールします。
 - a. CA APM Cloud Monitor インストーラ ファイルを起動します。
 - b. 使用許諾の条項に同意します。
 - c. <Agent_Home> ディレクトリを指定します。
 - d. エージェントが接続する Enterprise Manager ホストおよびポートを指定します。
 - e. [Cloud Monitor Account Settings] 画面で、CA APM Cloud Monitor のユーザ ID とパスワードを入力します。これらは、CA APM Cloud Monitor Web サイトへのログインに使用するのと同じクレデンシャルです。

CA APM Cloud Monitor エージェントのインストールが完了します。

注: エージェントの起動および接続の検証の手順については、「[CA APM Cloud Monitor エージェント接続の検証 \(P. 477\)](#)」を参照してください。

CA APM Cloud Monitor エージェント接続の検証

CA APM Cloud Monitor エージェントが正しくインストールされていることを検証するには、エージェントを起動し、CA APM WebView または Workstation を使用してデータをチェックします。CA APM Cloud Monitor からの受信データが最新であることを確認することによって、接続を検証します。

注: WebView または Workstation で CA APM Cloud Monitor データを確認するには、フォルダと監視を CA APM Cloud Monitor にセットアップしておく必要があります。この手順を実行していない場合は、「[CA APM Workstation ユーザガイド](#)」で CA APM Cloud Monitor の使用に関するセクションを参照してください。

以下の手順に従います。

1. CA APM Cloud Monitor エージェントがインストールされたディレクトリに移動し、以下のいずれかのファイルを実行してエージェントを起動します。
 - Windows の場合、APMCloudMonitor.bat をダブルクリックします。
 - Linux または Solaris の場合、APMCloudMonitor.sh を実行します。
エージェントがコンソール ウィンドウで起動します。
2. CA APM WebView または Workstation を起動します。
3. CA APM Cloud Monitor のデータを見つけます。
 - a. Investigator ウィンドウが開いていない場合は、[ファイル] - [新規 Investigator] を選択します。
 - b. [メトリック ブラウザ] タブを参照します。
 - c. 以下のノードを展開します。
SuperDomain | <Host_Name> | APMCloudMonitor |
APMCloudMonitorAgent | APM Cloud Monitor

<Host_Name> は、通常は CA APM Cloud Monitor エージェントがインストールされているコンピュータですが、[メトリック ブラウザ] ツリーに表示されるものが APMCloudMonitor.properties ファイルの apmcm.agent.hostName プロパティの値になります。
 - d. フォルダを展開して個別のメトリックを参照し、メトリックが最新であることを確認します。

トラブルシューティング

Enterprise Manager のインストール処理中に監視オプションとして「Cloud Monitor」を選択しなかった場合、WebView または Workstation は CA APM Cloud Monitor データの一部を表示しません。

問題の解決方法

- <EM_Home>¥examples¥CAAPMIntegrationForCloudMonitor¥ ディレクトリの内容を <EM_Home>/config/modules/ および <EM_Home>/ext/xmltv にコピーします。

これにより、Cloud Monitor メトリック データを正しく表示するのに必要な管理モジュールおよびその他のファイルが使用可能になります。

データを制限する方法

CA APM Cloud Monitor エージェントから Enterprise Manager に送信されるデータの量を制限して、パフォーマンスを向上させることができます。

CA APM Cloud Monitor プロパティの設定によるデータの制限

APMCloudMonitor.properties ファイル内のプロパティを使用して、CA APM Cloud Monitor エージェントが Enterprise Manager に送信するデータをフィルタできます。

CA APM Cloud Monitor エージェント プロパティの設定によりデータをフィルタするには、
<CloudMonitor_Agent_Home>/CloudMon/conf/APMCloudMonitor.properties 内の「Metric filters」セクションを編集します。

これらの設定の詳細については、[APMCloudMonitor.properties のプロパティ リファレンス \(P. 608\)](#)を参照してください。

チェックポイントの削除によるデータの制限

CA APM Cloud Monitor では、五大陸の 60 を超えるチェックポイントステーションにアクセスできます。Cloud Monitor は、これらのステーションの中からランダムに選択し、ステーションから Web サイトまたはアプリケーションへの可用性とパフォーマンスをチェックします。時間と共に、有効なすべてのステーションがこのチェックを実行し、その結果、60 を超える各サイトからデータがログ記録されます。

利用可能なチェックポイントステーションの一部を削除することで、CA APM Cloud Monitor が CA APM に送信するデータの量を制限できます。

以下の手順に従います。

1. CA APM Cloud Monitor の Web サイト (cloudmonitor.ca.com) にログインします。
2. [Subscriptions] - [Preferences] を選択します。
デフォルトでは、すべてのステーションが選択されています。

3. 以下のように、デフォルトの選択を変更します。
 - 個別のステーションのチェック ボックスをオフにします。または、
 - [Clear] をクリックしてすべてをクリアし、リストの先頭にあるグループの中から選択します。

たとえば、北米にあるステーションだけを選択するには、以下の手順に従います。

 - a. [Clear] をクリックします。
 - b. [North America] をクリックします。
4. ページ下部にある [Change] をクリックします。

スケジュールの調整によるデータの制限

デフォルトでは、監視は定期的（毎日 1 時間おき）に可用性とパフォーマンスをチェックします。この結果、時間が経過すると必要以上のデータが CA APM に返される場合があります。

以下の手順に従います。

1. Cloud Monitor の Web サイト (cloudmonitor.ca.com) にログインします。
2. [Settings] > [Monitors] を選択します。
3. 個別の監視を選択し、[More Options] を選択します。
4. 以下の設定をリセットします。
 - Delay between checks
 - Check period
 - Check on these days only
 - Maintenance schedule

付録 A: プロパティ ファイル リファレンス

以下のプロパティ ファイル（それぞれに併記されているディレクトリ内にあります）を使用して、Enterprise Manager、Workstation、および WebView を設定できます。

重要: プロパティ ファイルを Windows マシンで開いてパスを追加する場合、円記号については、もう 1 つ円記号を付加して（二重にして）エスケープ処理する必要があります。たとえば、「`C:\Introscope\lib\Agent.jar`」のようにします。

このセクションには、以下のトピックが含まれています。

[IntroscopeEnterpriseManager.properties](#) (P. 482)

[APMEnterpriseManager.properties](#) (P. 537)

[apm-events-thresholds-config.xml](#) (P. 541)

[ResourceMetricMap.properties](#) (P. 559)

[Catalyst.properties](#) (P. 562)

[EMservice.conf](#) (P. 571)

[Introscope Enterprise Manager.lax](#) (P. 578)

[IntroscopeWorkstation.properties](#) (P. 585)

[Introscope Workstation.lax](#) (P. 590)

[IntroscopeWebView.properties](#) (P. 596)

[Introscope WebView.lax](#) (P. 603)

[APMCloudMonitor.properties](#) (P. 608)

IntroscopeEnterpriseManager.properties

Enterprise Manager には 3 つのプロパティ ファイルがあり、その 1 つである *IntroscopeEnterpriseManager.properties* で定義されたプロパティは Enterprise Manager のさまざまな動作を制御します（他のファイルは [APMEnterpriseManager.properties](#) (P. 537) と [apm-events-thresholds-config.xml](#) (P. 541) です）。

ほとんどの Enterprise Manager のプロパティでは、設定後、変更を有効にするために Enterprise Manager を再起動する必要があります。

ただし、Enterprise Manager プロパティの中には、Introscope ホット設定サービスを使用するものもあります。これらの「ホット設定」プロパティに変更を加えた後は、Enterprise Manager を再起動する必要はありません。詳細については、「[ホット設定サービス](#) (P. 492)」を参照してください。

このファイルには以下のプロパティを設定できます。

[利用可能なプロセッサ \(P. 483\)](#)

[アラート動作 \(P. 484\)](#)

[通信 \(P. 484\)](#)

[Workstation Login Parameters Auto Fill セクション \(P. 490\)](#)

[EM Web サーバの設定 \(P. 490\)](#)

[ホット設定サービス \(P. 492\)](#)

[アプリケーション ヒューリスティック \(P. 492\)](#)

[ログ \(P. 493\)](#)

[永続コレクション-データベースへのデータの記録 \(P. 495\)](#)

[フラットファイルのプロパティ \(P. 497\)](#)

[トランザクション イベント データベース \(P. 497\)](#)

[トランザクション追跡サンプリング \(P. 498\)](#)

[Enterprise Manager のメトリック クランプ \(P. 499\)](#)

[SmartStor \(P. 502\)](#)

[ベースラインデータの保存 \(P. 508\)](#)

[SNMP コレクション \(P. 508\)](#)

[WebView \(P. 508\)](#)

[CA APM ChangeDetector \(P. 509\)](#)

[管理モジュールのブートストラップ \(P. 509\)](#)

[管理モジュールのデプロイ \(P. 510\)](#)

[クラスタ化の設定 \(P. 510\)](#)

[エージェントの相互作用 \(P. 515\)](#)

[Enterprise Manager フェールオーバー \(P. 520\)](#)

[設定ディレクトリ \(P. 521\)](#)

[アプリケーション問題切り分けマップ データ \(P. 522\)](#)

[ロケーションマップ データ \(P. 528\)](#)

[Web サービス \(P. 528\)](#)

[送信メッセージキュー \(P. 529\)](#)

[スレッドダンプ \(P. 531\)](#)

[Web サービスがパフォーマンスを処理するためのスレッドプロパティ \(P. 534\)](#)

[SNMP 問題切り分けマップ アラートアクション \(P. 535\)](#)

[アプリケーションマップ オブジェクト \(P. 536\)](#)

利用可能なプロセッサ

IntroscopeEnterpriseManager.properties の「Available Processors」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.availableprocessors

このプロパティを使用すると、利用可能なプロセッサの数を Enterprise Manager に設定することができます。ホスト上に Enterprise Manager が 1 つまたは複数ある場合は、これを使用してください。

デフォルト

(空)

アラート動作

IntroscopeEnterpriseManager.properties の「Alert State Metrics」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.alertstatemetric.prefix

アラート状態メトリックが表示される Investigator ノードの名前。

デフォルト

Alerts.

通信

IntroscopeEnterpriseManager.properties の「Port Settings」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.enabled.channels

Enterprise Manager が使用できる通信チャンネルを指定します。通信チャンネルを有効にするには、有効なチャンネルのカンマ区切りリストにチャンネルタイプを追加します。通信チャンネルを無効にするには、リストからそれを削除します。

`enabled.channels` プロパティは [introscope.enterprisemanager.port.<ChannelName>](#) (P. 485) プロパティと連携して動作します。

例

`channel1` および `channel2` という 2 つの通信チャンネルを使用する場合、以下のプロパティを設定します。

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

デフォルト

`channel1`

introscope.enterprisemanager.port.<ChannelName>

このリスナポートは、Enterprise Manager が Workstation およびエージェントと暗号化された通信を行うのに使用されます。

カスタム通信チャンネルを作成するには、以下のプロパティをプロパティファイルに追加します。

- `introscope.enterprisemanager.port.ChannelName`
- `introscope.enterprisemanager.serversocketfactory.ChannelName`
- `ChannelName` は、新しいチャンネルの名前です。

カスタムチャンネルを有効にするには、その名前を [introscope.enterprisemanager.enabled.channels](#) (P. 485) プロパティに追加します。

デフォルト

5001

introscope.enterprisemanager.serversocketfactory.<ChannelName>

このプロパティは、Enterprise Manager が、Workstation およびエージェントとの暗号化された通信に使用するサーバ ソケット ファクトリのクラス名を指定します。

カスタムの通信チャンネルを作成する場合は、以下のように新しいプロパティをプロパティ ファイルに追加します。

introscope.enterprisemanager.serversocketfactory.ChannelName

ChannelName は新しいチャンネルの名前で、このプロパティ値を、*com.wily.isengard.postofficehub.link.net.IServerSocketFactory* インターフェースを実装するカスタム サーバ ソケット ファクトリの完全修飾クラス名に設定します。

また、「[introscope.enterprisemanager.port.<ChannelName> \(P. 485\)](#)」の説明に従って、チャンネルのリスナ ポートを指定し、有効にする必要があります。

例

channel1 および channel2 を呼ばれる 2 つの通信チャンネルを使用する場合、以下のプロパティを設定します。

```
introscope.enterprisemanager.enabled.channels=channel1,channel2
introscope.enterprisemanager.port.channel1=5001
introscope.enterprisemanager.port.channel2=5002
```

serversocketfactory プロパティを以下のように設定します。

```
introscope.enterprisemanager.serversocketfactory.channel1=<classname>
introscope.enterprisemanager.serversocketfactory.channel2=<classname>
```

デフォルト

com.wily.isengard.postofficehub.link.net.DefaultServerSocketFactory

introscope.enterprisemanager.serversockets.reuseaddr

通信チャンネルサーバソケットが、継続的に *FIN_WAIT* または *TIME_WAIT* 状態にあるローカルポートと再度バインドするようにするには、このプロパティを **true** に設定します。Enterprise Manager が再起動されたら、このプロパティは無効になります。

正当な理由でポートが使用されている可能性があるので、このプロパティはデフォルトでは有効にしないでください。

デフォルト

False

introscope.enterprisemanager.disableInteractiveMode

対話コンソールを無効にするかどうかを指定します（コンソールで入力を受け付けるかどうかを指定します）。

注

多くの UNIX プラットフォームでは、アプリケーションが標準入力から読み込みを行うようになっていると、**nohup** が機能しません。実行モードを **nohup** モードにする場合は、このプロパティを **true** に設定し、アプリケーション問題切り分けマップデータファイルで、**lax.stdin.redirect** プロパティを **<blank>** に変更します。これらのプロパティの両方がここでの説明どおりに設定されていなければ、**nohup** モードでのアプリケーションの起動に失敗するか、CPU 使用率が最大になるおそれがあります。

デフォルト

True

introscope.enterprisemanager.webserver.port

Enterprise Manager の埋め込み Web サーバがリスンするポート。

デフォルト

8081

introscope.enterprisemanager.webserver.portinuse.fail

別のアプリケーションが Enterprise Manager と同じポートで実行されている場合に、Enterprise Manager が起動しないようにします。

別のアプリケーションが Enterprise Manager と同じポートで実行されている場合、これらのプロパティ設定は Enterprise Manager を起動するかどうかを制御します。

- このプロパティが **true** に設定されている場合、Enterprise Manager は起動しません。
- このプロパティが **false** に設定されている場合、ポートが使用中であるというエラーメッセージが表示されます。ただし、Enterprise Manager の起動は許可されています。

デフォルト

true

introscope.enterprisemanager.ipaddress

埋め込み Web サーバを含む、すべての Enterprise Manager 通信チャンネルを特定のローカル IP アドレスにバインドします。

このプロパティを設定しない場合、Enterprise Manager は、すべてのローカルアドレスで接続を許可します。

このプロパティの設定時に考慮する規則：

- このプロパティを IPv4 アドレスに設定すると、Enterprise Manager は、IPv4 システムが稼働しているマシン上のエージェントまたはクライアントからの接続しか受け付けません。
- このプロパティを IPv6 アドレスに設定すると、Enterprise Manager は、IPv6 準拠の JVM が稼働しているマシン上のエージェントまたはクライアントからの接続しか受け付けません。IPv4 JVM が稼働しているマシン上のエージェントまたはクライアントは、IPv6 アドレスを使用して接続することはできません。
- IPv6 対応システム上で稼働している Enterprise Manager または WebView のインスタンスを特定の IP アドレスにバインドしない場合、インスタンスはすべてのローカルアドレスにバインドされます。IPv4 環境と IPv6 環境両方からの接続を受け入れることができます。
- Workstation、エージェント、ブラウザやその他のクライアントは、Enterprise Manager または WebView のインスタンスに接続するためには IP アドレスではなく DNS 名を使用する必要があります。
- エージェントでサポートされている IPv6 は、エージェントが稼働している環境 (JVM、オペレーティングシステム、ハードウェア スタック) でサポートされる IPv6 によって異なります。

デフォルト

<コメントアウト。値なし>

introscope.enterprisemanager.workstation.connection.channel

Web Start Workstation への接続用チャンネルを指定します。

デフォルト

channel1

introscope.enterprisemanager.workstation.extendedLiveQuery

Workstation ユーザは、ライブ モードでデフォルト値である 8 分の時間範囲と 15 秒の精度の代わりに、カスタムの時間範囲と精度を入力することができます。

注: 時間範囲を 8 分より大きく設定すると、Smartstor からデータを取得する I/O オペレーションが原因で、Enterprise Manager のパフォーマンスが悪影響を受ける可能性があります。

デフォルト

TRUE

Workstation Login Parameters Auto Fill セクション

IntroscopeEnterpriseManager.properties の「Workstation Login Parameters」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.workstation.rememberLogin

Workstation が Webstart のログインパラメータ (Enterprise Manager ホスト、ポート、および UserId) を記憶するかどうかを制御します。FALSE に設定した場合、Workstation はログインパラメータを記憶しません。

デフォルト

TRUE

EM Web サーバの設定

IntroscopeEnterpriseManager.properties の「EM Web Server Settings」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.webserver.jetty.configurationFile

Jetty XML 設定ファイルへのパス。絶対パスまたは <EM_Home>/config ディレクトリへの相対パスのいずれか。このファイルは、HTTPS トラフィックのポート 8444 の SSL リスナを作成します。

注

introscope.enterprisemanager.webserver.jetty.configurationFile プロパティのコメント化を解除すると、IntroscopeEnterpriseManager.properties ファイルの introscope.enterprisemanager.webserver.port プロパティで指定したセキュアでない HTTP リスナは作成されません。ただし、Jetty XML 設定ファイルにはセキュアでない HTTP リスナを設定できます。

このプロパティは、ホット設定をサポートしていません。

デフォルト

em-jetty-config.xml

introscope.enterprisemanager.webserver.max.threads

Web サーバ内のリスナ スレッドの最大数です。つまり、Enterprise Manager の埋込み Web サーバが処理できる同時 HTTP クライアントの数です。

注

80 以上の HTTP トンネリング エージェントがこの Enterprise Manager に接続している場合にのみ、このプロパティを設定します。そのような場合、CA では、接続している HTTP トンネリング Agent の最大数に 20 を加えた値をプロパティに設定することをお勧めします。同時 HTTP エージェントの数が 80 に満たないと予想される場合は、このプロパティ値を変更しないでください。

デフォルト

100

ホット設定サービス

Enterprise Manager には、以下のプロパティに対してデフォルトで有効になっているホット設定が含まれています。

- log4j ログ プロパティ - 「[ログ \(P. 493\)](#)」を参照
- 永続コレクション-データベース プロパティへのデータの記録 - 「[永続コレクション-データベースへのデータの記録 \(P. 495\)](#)」を参照してください。
- Enterprise Manager メトリック クランプ プロパティ - 「[Enterprise Manager のメトリック クランプ \(P. 499\)](#)」を参照してください。
- クラスタ化プロパティ - 「[クラスタ化の設定 \(P. 510\)](#)」を参照してください。

introscope.enterprisemanager.hotconfig.enable

ホット設定サービスを有効化します。サービスを無効にするには、false に設定します。

デフォルト

true

introscope.enterprisemanager.hotconfig.pollingInterval

変更がないかどうかこのファイルをチェックする頻度を秒単位で指定します。

デフォルト

60 秒

アプリケーション ヒューリスティック

IntroscopeEnterpriseManager.properties の「Application Heuristics」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.application.overview.baselines=true

Enterprise Manager のパフォーマンスを向上させるには、このプロパティを `false` に設定してヒューリスティックを無効にします。

これを設定すると、Enterprise Manager により、JVM、アプリケーション、バックエンドの稼働状況に関する Enterprise Manager の評価が無効に設定されます。同時に、ベースラインも無効になります。これにより、Workstation 内のメトリックは非アクティブになり、値はレポートされなくなります。このメトリックは、`true` に設定しなおして再度アクティブになるまで、グレー表示されます。

デフォルト

True

ログ

ログプロパティを使用して、Enterprise Manager のログの詳細度、および Enterprise Manager のログファイルの名前と場所を定義することができます。高度な Log4J 機能の情報については、<http://jakarta.apache.org/log4j/docs/documentation.html> で Log4J のマニュアルを参照してください。

これらの Enterprise Manager プロパティは、Introscope ホット設定サービスを使用します。これらのホット設定プロパティに変更を加えた後は、Enterprise Manager を再起動する必要はありません。詳細については、「[ホット設定サービス \(P. 492\)](#)」を参照してください。

log4j.logger.Manager

ログメッセージの詳細度および出力先を制御します。

指定できる詳細度の値は、`INFO` または `VERBOSE#com.wily.util.feedback.Log4JSeverityLevel` です。

出力先の値には、`console` または `logfile` を指定できます。デフォルトの設定では、ログ情報はコンソールとログファイルに書き込まれます。

デフォルト

INFO, console, logfile

log4j.appender.logfile.File

Enterprise Manager ログファイルの名前。Enterprise Manager のホーム ディレクトリを基準にした相対的な場所です。

デフォルト

logs/IntroscopeEnterpriseManager.log

log4j.appender.logfile.layout.ConversionPattern

ログファイルをカスタマイズできます。

このプロパティは、以下の値を設定可能です。

`%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n`

パターンは log4j ライブラリに実装され、形式は <http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html> で説明されています。

日付/時刻の形式は、`%d{.}` で表示され、<http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html> で説明されているパターンに従います。

デフォルト

(空)

永続コレクション - データベースへのデータの記録

このセクションで説明するプロパティを使用して、追跡データを外部のリレーショナルデータベースへ記録するように設定できます。詳細については、*IntroscopeEnterpriseManager.properties* ファイルの「SQL Database Settings」セクションを参照してください。これらの設定は、ホット設定によりデプロイされるため、Enterprise Manager を手動で再起動する必要はありません。

Introscope には、履歴範囲に対するメトリック データおよびイベントデータを抽出し、Excel または SAS などのデータ分析ツールを使用して Introscope データを表示できるようにする API が含まれています。CA Technologies では、この API レコードデータを使用することをお勧めします。「[JDBC API \(P. 615\)](#)」を参照してください。コマンドライン Workstation のコマンドを使用して永続データを抽出することもできます。「[コマンドライン Workstation の使用](#)」を参照してください。

これらの Enterprise Manager プロパティは、Introscope ホット設定サービスを使用します。これらのいわゆる「ホット設定」プロパティを変更した後に Enterprise Manager を再起動する必要はありません。詳細については、「[ホット設定サービス \(P. 492\)](#)」を参照してください。

introscope.enterprisemanager.database.collection.agentExpression

これは、エージェントの正規表現のプロパティです。

IntroscopeEnterpriseManager.properties ファイルにこの設定を追加すると、ホット設定によってデプロイされます。

例：

```
Introscope.enterprisemanager.database.collection.agentExpression=rhart-dt1¥¥  
/EPAgentProcess1¥¥|EPAgent5
```

デフォルト

(空)

introscope.enterprisemanager.database.collection.metricExpression

これは、メトリックの正規表現のプロパティです。
IntroscopeEnterpriseManager.properties ファイルにこの設定を追加すると、ホット設定によってデプロイされます。

例

```
introscope.enterprisemanager.database.collection.metricExpression=Servlets¥¥/  
MyServlet:Average Response Time ¥¥(ms¥¥)
```

デフォルト

(空)

introscope.enterprisemanager.database.collection.frequencyinseconds

agentExpression はエージェントの正規表現、*metricExpression* はメトリックの正規表現、*frequencyinseconds* は、データを集約してデータベースに書き込む頻度を秒単位で表したものです。

IntroscopeEnterpriseManager.properties ファイルにこの設定を追加すると、ホット設定によってデプロイされます。

各永続コレクションは異なる値を保持することができるため、デフォルトの設定はありません。このプロパティは、それぞれの永続コレクションごとに設定する必要があります。

デフォルト

なし

introscope.enterprisemanager.database.recordingQueue.upperLimit.value

キューに入れるメトリック データ ポイントの最大数。メトリック データ ポイントは、1つのメトリックに1つのデータのタイム スライスになります。この設定は、ホット設定を使用して展開されます。

デフォルト

150k (1,000)

フラットファイルのプロパティ

フラットファイルとは、プレーンテキストのカンマ区切り値形式のファイル (.csv) です。Introscope はフラットファイルに書き込めますが、フラットファイルから読み取ることはできません。フラットファイルは数値解析ツールを使用して分析できます。

フラットファイルへの記録はデフォルトで有効になっており、`<EM_Home>/flatfiles` ディレクトリに記録されます。これらのファイルを Introscope のディレクトリの外部にあるディレクトリに格納するように指定することもできます。Windows 用のパスの場合、円記号 (¥) にはもう 1 つ円記号を付加して (二重にして) エスケープ処理する必要があります。たとえば、「`C:¥¥Introscope¥¥FlatFileDir`」のようにします。

トランザクション イベント データベース

Enterprise Manager は、そのファイルシステム上のローカルにキャプチャされたトランザクションイベントを決まった期間、または最大ディスク容量を超えるまで保存します。これらのイベントの保存先、および削除する時期については、トランザクションイベントのデータベースのプロパティを設定することにより制御することができます。

`introscope.enterprisemanager.transactionevents.storage.dir`

Introscope がトランザクションイベントデータを保存する場所を Enterprise Manager のホーム ディレクトリを基準にして指定します。

デフォルト

traces

`introscope.enterprisemanager.transactionevents.storage.max.data.age`

トランザクション イベント データの保存期間を日単位で指定します。

デフォルト

14

introscope.enterprisemanager.transactionevents.storage.optimize.frequency

古いデータのクリーンアップによって追跡ストレージを最適化する頻度を時間単位で指定します。

Enterprise Manager の開始時に、トランザクション追跡データの期間を有効化します。

デフォルト

24 時間

introscope.enterprisemanager.transactionevents.storage.optimize.timeoffsethour

ストレージを最適化するための時間補正值を指定します。この値により、ページをスケジュールして、時間補正值に対する毎日決まった時間に開始することができます。

たとえば、時間補正值を 02 に設定して、最適化頻度

(「[introscope.enterprisemanager.transactionevents.storage.optimize.frequency](#) (P. 498)」を参照) を 24 時間に設定すると、最適化は午前 2 時から開始され、24 時間ごとに実行されます。

この値は正の整数でなければならないので、プロパティに 00 の値を入力すると、エラーメッセージが表示されます。

デフォルト

02 (午前 2 時)

トランザクション追跡サンプリング

以下のトランザクション追跡サンプリングは、デフォルトでは *IntroscopeEnterpriseManager.properties* に保存されています。

introscope.agent.transactiontracer.sampling.perinterval.count

デフォルトではサンプル追跡の数は 1 に設定されています。このプロパティは、`introscope.agent.transactiontracer.sampling.interval.seconds` プロパティと共に機能します。

追跡間隔ごとの追跡の数は、プロパティ ファイル内でこの値を変更してコメント化を解除することで変更できます。

デフォルト

1

introscope.agent.transactiontracer.sampling.interval.seconds

デフォルトでは、2 分間隔で追跡を行う設定です。このプロパティは、`introscope.agent.transactiontracer.sampling.perinterval.count` プロパティと共に機能します。

サンプリング間隔は、プロパティ ファイル内でこの値を変更してコメント化を解除することで変更できます。

注

`sampling.perinterval` および `sampling.interval` プロパティのデフォルトを上書きする前に、サンプリング周期が上がったために Enterprise Manager 内での負荷が増大する可能性を考慮してください。

デフォルト

120 秒

Enterprise Manager のメトリック クランプ

これらのプロパティでは、スタンドアロンの Enterprise Manager またはコレクタから取得できるメトリックの結果の数について制限設定を定義します。これらはホット設定可能で、値はホット デプロイ中に Enterprise Manager によってプロパティ ファイルがチェックされる際に適用されません。ホット デプロイは、約 60 秒ごとに実行されます。

クランプを無効にする方法

1. IntroscopeEnterpriseManager.properties ファイルを開き、「EM Metric Clamping」セクションに移動して編集します。
2. クランプを無効にするには、クランプの値を 0 に設定します。
3. IntroscopeEnterpriseManager.properties ファイルを保存して閉じます。

その他の Enterprise Manager クランプは、<EM_Home>/config ディレクトリ内の [apm-events-thresholds-config.xml](#) (P. 541) ファイルにあります。

introscope.enterprisemanager.query.datapointlimit

このプロパティでは、以下のタイプの単一クエリに関する内部処理が完了した後で Enterprise Manager がクエリを発行したソフトウェアに返送するメトリック データ ポイントの最大数を定義します。

- JDBC
- CLW
- 上位 N (CLW と Workstation の両方)

クエリを発行するソフトウェアは、Workstation、拡張機能、または内部の計算機です。内部処理は、上位 N クエリまたはその他のフィルタです。

このクランプの効用は、クラスタ化されたコレクタまたはスタンドアロン Enterprise Manager が SmartStor から取得するメトリックの数を減らせる点です。ただし、Enterprise Manager は常に、少なくとも 1 つのメトリックのデータをすべて返します。このクランプは JDBC、CLW、または上位 N クエリごとに適用され、同時実行される複数のクエリには適用されません。

このプロパティは、[introscope.enterprisemanager.query.returneddatapointlimit](#) (P. 502) プロパティと連携して機能します。

introscope.enterprisemanager.query.datapointlimit プロパティと introscope.enterprisemanager.query.returneddatapointlimit プロパティの違いは、クランプが発生する場所です。

introscope.enterprisemanager.query.datapointlimit プロパティは、クエリを発行するソフトウェアにクエリを返送するときにメトリック データ ポイントをクランプします。 introscope.enterprisemanager.query.datapointlimit プロパティは、SmartStor のディスク読み取り数をクランプします。

例

例 1

introscope.enterprisemanager.query.datapointlimit プロパティが 10 に設定され、introscope.enterprisemanager.query.returneddatapointlimit プロパティが 0 (無制限) に設定されています。

ある CA APM ユーザが 10,000 個のデータポイントに一致する上位 100 クエリを実行しました。Enterprise Manager は、上位 100 のデータポイントのみを Workstation に返送しようとします。Enterprise Manager は SmartStor から 10,000 個のデータポイントを読み取り、処理します。しかし、introscope.enterprisemanager.query.datapointlimit プロパティが 10 に設定されているため、Enterprise Manager は最初の 10 個のデータポイントのみを Workstation に返送します。

例 2

introscope.enterprisemanager.query.datapointlimit プロパティが 0 (無制限) に設定され、introscope.enterprisemanager.query.returneddatapointlimit プロパティが 1000 に設定されています。

ある CA APM ユーザが 10,000 個のデータポイントに一致する上位 100 クエリを実行しました。Enterprise Manager は、上位 100 のデータポイントのみを Workstation に返送しようとします。Enterprise Manager は SmartStor から 1,000 個のデータポイントを読み取り、処理します。introscope.enterprisemanager.query.returneddatapointlimit プロパティが 1,000 に設定されているため、Enterprise Manager は上位 100 のデータポイントを Workstation に自由に送信できます。

注

このプロパティを設定して、MOM または CDV に対するクエリをクランプすることはできません。

デフォルト

0 (0 は無制限を意味します)

introscope.enterprisemanager.query.returneddatapointlimit

このプロパティでは、JDBC、CLW または上位 N（CLW と Workstation の両方）の単一クエリに対して SmartStor が返すデータ ポイントの数を制限します。このクランプの効用は、クラスタ化されたコレクタまたはスタンドアロン Enterprise Manager にデータが返されるメトリックの数を減らせる点です。このクランプは JDBC、CLW、または上位 N クエリごとに適用され、同時実行される複数のクエリには適用されません。

このプロパティは [introscope.enterprisemanager.query.datapointlimit](#) (P. 500) プロパティと連携して機能します。

例

注: 例については、[introscope.enterprisemanager.query.datapointlimit](#) (P. 500) プロパティを参照してください。

注

このプロパティを設定して、MOM または CDV に対するクエリをクランプすることはできません。

デフォルト

0 (0 は無制限を意味します)

SmartStor

このセクションのプロパティは、SmartStor データの保存先のディレクトリを定義し、3 つの保存層のデータ収集および保存期間を設定します。また、必要に応じて、SmartStor を無効にすることもできます。

注: 3 つの層をすべて定義する必要があります。4 つ以上の層は定義できません。

introscope.enterprisemanager.smartstor.enable

SmartStor を有効または無効にすることができます。SmartStor を無効にするとディスク容量を節約することができますが、統計が保存されないため、それらを監視することができなくなります。

False に設定すると、SmartStor が無効になります。

注

SmartStor セクションにプロパティが表示されていない場合は、SmartStor が有効になっています。SmartStor を無効にするには、プロパティファイルに `introscope.enterprisemanager.smartstor.enable=false` という行を追加します。

デフォルト

True

introscope.enterprisemanager.smartstor.directory

SmartStor が使用するディレクトリを、Enterprise Manager のホームディレクトリを基準にして指定します。

デフォルト

data

introscope.enterprisemanager.smartstor.directory.archive

アーカイブされたデータを保存するために SmartStor が使用するディレクトリを指定します。

デフォルト

data/archive

introscope.enterprisemanager.smartstor.dedicatedcontroller

SmartStor データを専用ディスクに書き込むかどうかを指定します。

SmartStor データを専用ディスクに書き込む場合は `true` に設定します。

このプロパティの使用法の詳細については、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。

デフォルト

false

introscope.enterprisemanager.smartstor.tier1.frequency

第一のデータ層のデータ収集間隔を秒単位で指定します。間隔は以下のようにしている必要があります。

- 15 秒の整数倍にする
- 1800 秒 (30 分) を超える値にしない
- 1 つ前の層の保存間隔の偶数倍にする (倍数は 1 にも設定できるので、すべての層の保存間隔を同じにすることもできます)

デフォルト

15

introscope.enterprisemanager.smartstor.tier1.age

SmartStor の最初のデータ層のデータを破棄するまでの日数を指定します。この値を 0 にすることはできません。

デフォルト

7

introscope.enterprisemanager.smartstor.tier2.frequency

2 番目のデータ層のデータ収集間隔を秒単位で指定します。間隔は以下のようにしている必要があります。

- 15 秒の整数倍にする
- 1800 秒 (30 分) を超える値にしない
- 1 つ前の層の保存間隔の偶数倍にする (倍数は 1 にも設定できるので、すべての層の保存間隔を同じにすることもできます)

デフォルト

60

introscope.enterprisemanager.smartstor.tier2.age

SmartStor の 2 番目のデータ層のデータを破棄するまでの日数を指定します。この値を 0 にすることはできません。

デフォルト

23

introscope.enterprisemanager.smartstor.tier3.frequency

3 番目のデータ層のデータ収集間隔を秒単位で指定します。間隔は以下のようにしている必要があります。

- 15 秒の整数倍にする
- 1800 秒 (30 分) を超える値にしない
- 1 つ前の層の保存間隔の偶数倍にする (倍数は 1 にも設定できるので、すべての層の保存間隔を同じにすることもできます)

デフォルト

900

introscope.enterprisemanager.smartstor.tier3.age

SmartStor の 3 番目のデータ層のデータを破棄するまでの日数を指定します。この値を 0 にすることはできません。

デフォルト

335

introscope.enterprisemanager.memoryCache.elements

このプロパティは、内部の圧縮メモリ キャッシュで Enterprise Manager が保持するデータ ポイントの数を制御して、履歴データのクエリを高速化します。

各データ ポイントには、15 秒間のメトリック データが含まれます。デフォルトの 32 個のデータ ポイントには、8 分間の履歴メトリック データが含まれます。

範囲は 32 (8 分) ~ 11520 (48 時間) で、32 で割り切れる必要があります。

Workstation での使用が急増した場合に、問題切り分けを行うために 32 個のデータ ポイントより大きなキャッシュを設定できます。たとえば、値を 240 個のデータ ポイントに設定すると、Enterprise Manager はメモリキャッシュから最近 1 時間のすべての履歴クエリを提供できます。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

この値は 32 未満のデータ ポイントに設定することはできません。32 未満に設定した場合、デフォルト値に設定されます。

値が 32 で割り切れない場合、その値は、32 で割り切れる最も近い数まで小さくなります。

重要: キャッシュ内のデータ ポイントの数を増やすには RAM が必要になります。数ギガバイトの追加のヒープメモリを持った 64 ビットのコンピュータを実行していない場合は、デフォルトより高い値を設定しないでください。ヒープチューニングの詳細については、「[CA APM サイジングおよびパフォーマンスガイド](#)」を参照してください。

以下の計算を使用して、キャッシュに必要なヒープメモリを計算します。キャッシュされたデータ ポイント 1 つにつき、平均 32 バイトと仮定します。

データ ポイントの数 × 32 バイト × メトリックの数 = 必要なキャッシュヒープメモリ

例

約 1 時間分のデータを保持するようにキャッシュを増加させることに決めて、値を 256 個のデータ ポイントに設定しました。以下の式を使用して、必要なキャッシュヒープメモリを計算します。

256 個のデータ ポイント × 32 バイト × 500,000 メトリック = 4.1 GB のキャッシュヒープメモリ

Enterprise Manager のヒープサイズを調べて、キャッシュヒープメモリの要件に基づいて調整する必要があるかどうかを確認します。

デフォルト

32 個のデータ ポイント

introscope.enterprisemanager.smartstor.reperiodizationOffsetHour

このプロパティにより、データ階層化のオフセット時間を設定することができます。

制約

0 ～ 23 の整数である必要があり、1 日の時間を表します。0 は午前 0 時を表し、13 は午後 1 : 00 を表します。

デフォルト

0 (0 の場合、データ階層化が午前 0 時に開始されます)。

例

2 に設定すると、データ階層化は午前 2 : 00 に開始されます。

introscope.enterprisemanager.smartstor.conversionOffsetMinute

このプロパティにより、スプールからのデータ変換のオフセット時間を設定することができます。

制約

0 ～ 59 の整数である必要があり、正時からの経過分数を表します。

デフォルト

0 (たとえば、xx:00 に値を設定した場合、変換が正時に開始することになります)。

例

値を 10 (xx : 10) に設定した場合、スプール変換は正時から 10 分後にスタートします。

ベースライン データの保存

IntroscopeEnterpriseManager.properties の「EM Object Database Settings」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.dbfile

Introscope がメトリック ベースライン情報を保存するデータベースのファイル名および場所を Enterprise Manager のホーム ディレクトリを基準にして相対的に指定します。

デフォルト

data/baselines.db

SNMP コレクション

IntroscopeEnterpriseManager.properties の「SNMP Adapter」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.snmp.enable

SNMP エージェントを有効にするかどうかを指定します (SNMPServices.jar がインストールされている場合のみ可)。

デフォルト

false

introscope.enterprisemanager.snmp.agent.port

Enterprise Manager のポートのうち、SNMP エージェントとの通信に使用するポート

デフォルト

161

WebView

IntroscopeEnterpriseManager.properties の「WebView Configuration」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.webview.disableLogin

WebView から Enterprise Manager への接続を確立できるようにするかどうかを指定します。

デフォルト

false

introscope.enterprisemanager.webview.password

WebView から Enterprise Manager に接続するとき使用するパスワードを指定します。

デフォルト

WebView

CA APM ChangeDetector

IntroscopeEnterpriseManager.properties の「CA APM ChangeDetector」セクションには、以下のプロパティが含まれています。

introscope.changeDetector.disable

このプロパティを使用すると、CA APM ChangeDetector を有効または無効にすることができます。

デフォルト

true

管理モジュールのブートストラップ

IntroscopeEnterpriseManager.properties の「Management Module Bootstrapping」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.managementModules.invalid.references.as.errors

無効な参照を警告としてログに記録します。true に設定すると、無効な参照によって Enterprise Manager が起動できなくなります。

デフォルト

false

管理モジュールのデプロイ

IntroscopeEnterpriseManager.properties の「Management Module Deployment」セクションには、以下のプロパティが含まれています。

introscope.enterprisemanager.hotdeploy.directory

デプロイを実施する更新済みアプリケーションがあるかどうかをチェックするディレクトリを、Enterprise Manager のホーム ディレクトリを基準にして相対的に定義します。

デフォルト

deploy

introscope.enterprisemanager.hotdeploy.checkFrequencyInSeconds

デプロイを実施する更新済み管理モジュールがあるかどうかをチェックする頻度を秒単位で指定します。

デフォルト

60

クラスタ化の設定

これらのプロパティの一部については、設定を有効にするために Enterprise Manager を再起動する必要があります。その他のプロパティは Introscope [ホット設定サービス](#) (P. 492)を使用します。これらの「ホット設定」プロパティに変更を加えた後は、Enterprise Manager を再起動する必要はありません。

introscope.enterprisemanager.clustering.manager.slowcollectorthreshold

このプロパティを設定すると、お使いの環境に ping メトリックのしきい値を定義することができます。ping メトリックは、MOM から各コレクタまでの往復応答時間の下限だけを監視します。

デフォルト

10000 (ミリ秒単位)

introscope.enterprisemanager.clustering.manager.slowcollectordisconnectthresholdseconds

このプロパティを設定すると、値を超えた場合に MOM が自動的に接続を解除するしきい値を定義することができます。クラスタ内にあるコレクタの 1 つのパフォーマンスが著しく低下した場合、その副作用でクラスタ全体がハングすることがありますが、この設定によって、ハングを防止することができます。

このプロパティを 0、または負の値に設定すると、この機能は有効になりません。ただし、これは推奨しません。

注

MOM は 7.5 秒ごとにコレクタをチェックするため、若干の変更では動作に影響しません。

デフォルト

60 (秒単位)

introscope.enterprisemanager.clustering.mode

このプロパティでは、CA APM 環境での Enterprise Manager の役割を指定します。

オプション

CDV - Enterprise Manager はクロス クラスタ データ ビューアとして動作します。

Collector - Enterprise Manager はコレクタとして動作します。

MOM - Enterprise Manager は Manager として動作します。

StandAlone - Enterprise Manager はスタンドアロン Enterprise Manager として動作します。

注

このプロパティ設定を有効にするには、Enterprise Manager を再起動します。

Enterprise Manager を CDV として設定した後で、以下のいずれかの役割に変更する場合は、マシンに APM データベースが必要です。

- MOM
- コレクタ
- スタンドアロン Enterprise Manager

デフォルト値

StandAlone

例

```
introscope.enterprisemanager.clustering.mode=StandAlone
```

introscope.enterprisemanager.clustering.login.<emName>.host

コレクタ Enterprise Manager のホスト名または IP アドレス。

デフォルト

(空)

`introscope.enterprisemanager.clustering.login.<emName>.port`

コレクタ Enterprise Manager の
[introscope.enterprisemanager.port.<ChannelName>](#) (P. 485) プロパティの値

デフォルト

(空)

`introscope.enterprisemanager.clustering.login.<emName>.publickey`

MOM がコレクタ Enterprise Manager との接続に使用するパスワードを暗号化するための公開鍵を指定します。

デフォルト

`config/internal/server/EM.public` (コメント化されています)

`introscope.enterprisemanager.clustering.privatekey`

MOM がコレクタ Enterprise Manager との接続に使用するパスワードをコレクタ Enterprise Manager が復号化するために使用する秘密鍵を指定します。

デフォルト

`config/internal/server/EM.private`

`introscope.enterprisemanager.clustering.collector.identifier`

オプションです。このコレクタにわかりやすい名前を付けたい場合は、このプロパティを設定します。

識別子を指定しない場合、Introscope ではデフォルトの識別子である `host@port` が使用されます。host は Enterprise Manager のホスト名で、port は Enterprise Manager の接続ポートです。

デフォルト

false

introscope.enterprisemanager.clustering.manager.staggeredstartdelay

クラスタ化されたコレクタに対して MOM が接続を試行する間隔の長さを変更するには、このオプションプロパティを設定します。このプロパティが設定されていない場合、接続試行間隔のデフォルト時間は 0 秒です。つまり、コレクタが利用可能になると、MOM はすぐに各コレクタを認識します。

このプロパティを設定すると、MOM の起動オーバーヘッドの安定化が図れます。接続試行間に時間があることで、MOM は各コレクタがオンラインになったとき、1 つの接続処理を終えてから、別の待機コレクタの接続処理を開始できます。

最小値は 0 秒です。

デフォルト

0 (秒) 最小値は 0 秒です。

introscope.enterprisemanager.loadbalancing.threshold

このプロパティを設定すると、ロードバランサの不均衡の許容レベルを定義することができます。ロードバランサがクラスタのバランスを再調整するには、コレクタ内のメトリック数が、重み調整されたクラスタの平均（全コレクタの平均など）としきい値以上の差がある必要があります。

バランスの再調整とは、コレクタ間のエージェントを再配分して、重み調整されたメトリックの負荷を等しくすることです。

デフォルト

20000 (メトリック)

introscope.enterprisemanager.loadbalancing.interval

このプロパティを設定すると、ロードバランサがバランスを再調整する頻度を秒単位で指定することができます。最小値は 120 秒です。

デフォルト

600 (10 分)

introscope.enterprisemanager.clustering.login.em1.weight

このオプションプロパティを設定すると、コレクタの関連負荷を制御することができます。

その他の負荷はすべて等しいため、クラスタの総重みで割った重みは、そのコレクタに割り当てられたメトリック負荷の割合になります。たとえば、コレクタの重みが 50 で、すべてのコレクタの重み合計が 250 の場合、コレクタはクラスタのメトリック負荷の 20% を負担しなければなりません。

クラスタの重みの平均値。これは Enterprise Manager コレクタで負荷分散されている重みです。

エージェントの相互作用

エージェントの相互作用に関するプロパティの一部については、設定後に Enterprise Manager を再起動する必要があります。その他のプロパティは、Enterprise Manager のホット設定サービスを使用して自動的にデプロイされます。ホットデプロイについては、プロパティの説明に記載されています。

エージェントの相互作用に関するプロパティの一部は、Enterprise Manager のプロパティファイルに含まれていません。これらのデフォルト値を変更するには、プロパティの値を *IntroscopeEnterpriseManager.properties* ファイルに追加して、このファイルを保存します。プロパティがホットデプロイされない場合は、新しい値を有効にするために Enterprise Manager をシャットダウンして再起動してください。

introscope.apm.agentcontrol.agent.allowed

エージェントが *loadbalancing.xml* 内のどの正規表現にも一致しない場合に、この設定によって以下の Enterprise Manager にエージェントが接続できるかどうかが決まります。

- 特定のスタンドアロン Enterprise Manager
- コレクタ

デフォルト

true

例

introscope.apm.agentcontrol.agent.allowed=true

注

この設定は、ホット設定を使用してデプロイされます。

このプロパティは、以下のように設定されます。

- IntroscopeEnterpriseManager.properties ファイルに存在しない場合、値は true になります。
- MOM 上で true に設定すると、loadbalancing.xml 内で一致しないすべてのエージェントがクラスタ内で許可されます。
- false に設定すると、loadbalancing.xml 内で一致しないすべてのエージェントが禁止対象として設定され、その結果以下ようになります。
 - **9.1 より前のエージェントで有効:** 9.1 より前のエージェントは、どの Enterprise Manager にも接続しません。
 - **9.1 エージェントで有効:** 9.1 エージェントは、パッシブに Enterprise Manager に接続し、メトリック データを送信しません。
 - これらのエージェントは、APM ステータス コンソールの [拒否エージェント] リストに追加されます。

9.1 より前のエージェントで有効: 9.1 より前のエージェントが以下の条件を満たす場合があります。

- Enterprise Manager に接続されている。
- このプロパティ設定の変更に基づいて禁止されている。

このような場合、Enterprise Manager はこのエージェントを切断します。エージェントがこのプロパティの変更または loadbalancing.xml の設定によって許可されるまで、Enterprise Manager は以降のエージェント接続の試行をすべて拒否します。エージェントは、[introscope.enterprisemanager.agent.disallowed.connection.limit](#) (P. 519) プロパティで設定された時間に基づいて、再接続を待機します。

introscope.apm.agentcontrol.agent.emlistlookup.enable

エージェントに接続を許可している Enterprise Manager のリストを以下のコンポーネントが各エージェントに送信できるかどうかを決定します。

- MOM
- コレクタ
- スタンドアロン Enterprise Manager

このリストは、エージェントが接続している以下のコンポーネントがダウンしたときに、そのエージェントが次にどの Enterprise Manager に接続すべきかを決定します。

- MOM
- スタンドアロン Enterprise Manager
- エージェントが最初に接続したコレクタ

デフォルト

true

例

```
introscope.apm.agentcontrol.agent.emlistlookup.enable=true
```

注

この設定は、ホット設定を使用してデプロイされます。

エージェントが再起動した場合、そのエージェントは自身のエージェントプロファイルの

`introscope.agent.enterprisemanager.connectionorder` プロパティを使用して、最初のコレクタ接続の情報を取得します。

introscope.apm.agentcontrol.agent.reconnect.wait

この設定は、エージェントがスタンドアロン Enterprise Manager またはコレクタに再接続しようとする前に待機する基本期間（秒単位）を指定します。

デフォルト

45（秒）

例

```
introscope.apm.agentcontrol.agent.reconnect.wait=45
```

注

この設定は、ホット設定を使用してデプロイされます。

最小値は 45 です。値を 45 未満に設定すると、デフォルト値の 45 になります。

多くのエージェントが同時に接続するのを避けるため、Enterprise Manager はこのプロパティ値にランダムな秒数 (-30、-15、0、15、30) を追加します。Enterprise Manager はこれらの計算値のいずれかをランダムに選択し、その値をエージェントに指定します。エージェントは、指定された期間だけ待機してから再接続しようとしています。

たとえば、値を 60 に設定した場合、Enterprise Manager は 60 に -30、-15、0、および 15 を追加します。これにより、30、45、60、75 および 90 という計算値のセットが作成されます。Enterprise Manager は 75 をランダムに選択し、この値をエージェントに指定します。エージェントは 75 秒間待機してから再接続を試行します。

introscope.enterprisemanager.agentconnection.metrics.enable

Enterprise Manager がエージェント接続のメトリックを生成するかどうかを制御します。このプロパティは、True または False に設定できます。

このプロパティは、Enterprise Manager プロパティ ファイルには含まれません。値を変更するには、プロパティ ファイルにプロパティを追加し、そのプロパティを有効にするため Enterprise Manager を再起動します。

デフォルト

True

introscope.enterprisemanager.agentconnection.metrics.agentTimeoutInMinutes

エージェントが Enterprise Manager との接続を切断した後、そのエージェント用に生成される接続メトリックを何分間中断するかを指定します。

このプロパティは、Enterprise Manager プロパティ ファイルには含まれません。値を変更するには、プロパティ ファイルにプロパティを追加し、そのプロパティを有効にするため Enterprise Manager を再起動します。

デフォルト

30 (分)

introscope.enterprisemanager.agent.disallowed.connection.limit

禁止対象として設定され、パッシブに Enterprise Manager に接続できるエージェントの数を制限します。パッシブに接続されたエージェントはメトリック データを送信しません。

このクランプ プロパティは、MOM、スタンドアロン Enterprise Manager、およびコレクタに適用されます。

このクランプ値に到達したときに、禁止されたエージェントが接続しようとする、Enterprise Manager は新しい接続を拒否します。また、Enterprise Manager はこのアクティビティをログに記録し、そのエージェントは APM ステータス コンソールの [拒否エージェント] リストに追加されます。

デフォルト

0 (無制限)

例

```
introscope.enterprisemanager.agent.disallowed.connection.limit=0
```

注

この設定は、ホット設定を使用してデプロイされます。

このプロパティは 9.1 以降のエージェントで有効です。

MOM 上でこのプロパティを設定した場合、MOM の値はコレクタの値を上書きしません。

introscope.enterprisemanager.autoUnmountDelayInMinutes

エージェントが一時的に切断された場合に Enterprise Manager でそのエージェントの追跡を続行する時間 (分単位)。この時間が経過すると、Enterprise Manager でエージェント追跡リソースが解放されます。

デフォルト

60 (分)

Enterprise Manager フェールオーバー

以下のプロパティを使用すると、フェールオーバーの設定を有効にして適用することができ、インストールディレクトリを共有する Enterprise Manager でも使用することができます。これらのプロパティを設定する場合は、Enterprise Manager フェールオーバーのルールを考慮してください。

introscope.enterprisemanager.failover.enable

このプロパティは、フェールオーバーを有効にします。

デフォルト

false

introscope.enterprisemanager.failover.primary

このプロパティでは、プライマリの Enterprise Manager のホスト名または IP アドレスを設定することができます。両方の Enterprise Manager をプライマリとして設定するには、プライマリ Enterprise Manager のホスト名、または IP アドレスの一覧をカンマで区切って設定します。たとえば、両方の Enterprise Manager をプライマリとして設定する場合は、次のようになります：*introscope.enterprisemanager.failover.primary=myhost1, myhost2*。

共有ファイルシステムではなく単一ホスト用の Enterprise Manager フェールオーバーを設定する場合、プライマリ Enterprise Manager をそれぞれに設定する必要があります。また、*introscope.enterprisemanager.failover.secondary* プロパティは、空白にする必要があります。

デフォルト

(空)

introscope.enterprisemanager.failover.secondary

このプロパティでは、Enterprise Manager のホストのホスト名、または IP アドレスを指定することにより、セカンダリ Enterprise Manager のホスト名、または IP アドレスを設定することができます。例:

`introscope.enterprisemanager.failover.secondary=myhost2`

デフォルト

(空)

introscope.enterprisemanager.failover.interval

このプロパティでは、プライマリ Enterprise Manager が起動待ちをしているかどうかを稼働中のセカンダリ Enterprise Manager がチェックする頻度を秒単位で設定することができます。この設定は、ホット設定を使用して展開されます。

デフォルト

120 (2分)

設定ディレクトリ

「EM Config Directory」セクション内にあるこのプロパティでは、Enterprise Manager *config* ディレクトリの場所を指定することができます。

introscope.enterprisemanager.directory.config

Enterprise Manager が構成に使用するディレクトリ。Windows では、円記号は二重にしてエスケープ指定する必要があります。例:

`C:¥¥Introscope¥¥config`

デフォルト

Introscope インストール時の config ディレクトリ。

アプリケーション問題切り分けマップ データ

このプロパティを使用して、アプリケーション問題切り分けマップデータ設定を有効にし、適用することができます。構成の手順については、「[アプリケーション問題切り分けマップの構成 \(P. 269\)](#)」を参照してください。

アプリケーション問題切り分けマップに関連する追加のプロパティは、*APMEnterpriseManager.properties* ファイル内で構成します。「[APMEnterpriseManager.properties \(P. 537\)](#)」を参照してください。

introscope.apm.data.agingTime

このプロパティはエージェントによってロードされ、エージェントがアプリケーション問題切り分けマップデータを Enterprise Manager にレポートする頻度を制御します。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために、エージェントと Enterprise Manager を再起動してください。

警告： このプロパティを変更する前に、APM データベースからマップデータを削除してください。この値が変更され、古いマップデータが新しいマップデータと共に使用されると、履歴クエリによって新しい値に一致しない結果が表示されます。APM データベースからのマップデータの削除の詳細については、「[アプリケーション問題切り分けマップデータの廃棄 \(P. 276\)](#)」を参照してください。

この値を 1 分より小さくすることはできません。1 分未満に設定すると、プロパティはデフォルト値の 1 日に設定されます。

この設定を決定する際、組織がアプリケーションに対して追加や変更を行う頻度を考慮してください。設定する値が低いほど、マップに表示されるアプリケーションの依存関係はリアルタイムなものになります。ただし、エージェントと Enterprise Manager のオーバーヘッドが増大する可能性があります。設定する値が高いほど、マップに表示されるアプリケーションの依存関係は最新のものでなくなります。ただし、エージェントと Enterprise Manager のオーバーヘッドが減少する可能性があります。

エージェントと Enterprise Manager のオーバーヘッドについては、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。

以下の時間単位のいずれかを使用してください。大文字と小文字は区別されません。それぞれ、どちらかを使用できます。

- 日 : days、D
- 分 : mins、M
- 時間 : hours、H

この `agingTime` プロパティは `introscope.apm.data.timeWindow` プロパティと連携して機能するため、`agingTime` は通常 `timeWindow` のサブセットになります。

例

`introscope.apm.data.agingTime` の値が 3 日で、`introscope.apm.data.timeWindow` の値が 10 日である場合、アプリケーション問題切り分けマップには、それまでの 10 日間にエージェントによってレポートされたアプリケーションの依存関係が表示されます。10 日間依存関係のデータがレポートされなかった場合は、`agingTime` 期間の 3 日が経過した後 `aged` として表示され、`timeWindow` の 10 日が経過するまでマップ上に `aged` エlement として残ります。

デフォルト

1 日

introscope.apm.data.timeWindow

このプロパティは、*introscope.apm.data.agingTime* プロパティ内に定義された期間とは別に、期間を定義します。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために **Enterprise Manager** を再起動してください。

この値を 1 分より小さくすることはできません。1 分未満に設定すると、プロパティはデフォルト値の 1 日に設定されます。

以下の時間単位のいずれかを使用してください。大文字と小文字は区別されません。それぞれ、どちらかを使用できます。

- 日 : days、D
- 分 : mins、M
- 時間 : hours、H
- 秒 : secs、S
- ミリ秒 : MS

このプロパティは *introscope.apm.data.timeWindow* プロパティと連携して機能するため、agingTime は通常 timeWindow のサブセットになります。

例

`introscope.apm.data.agingTime` の値が 3 日で、
`introscope.apm.data.timeWindow` の値が 10 日である場合、アプリケーション問題切り分けマップには、それまでの 10 日間にエージェントによってレポートされたアプリケーションの依存関係が表示されます。10 日間依存関係のデータがレポートされなかった場合は、`agingTime` 期間の 3 日が経過した後 `aged` として表示され、`timeWindow` の 10 日が経過するまでマップ上に `aged` エlement として残ります。

この設定を決定する際、組織がアプリケーションに対して追加や変更を行う頻度を考慮してください。設定する値が低いほど、マップに表示されるアプリケーションの依存関係はリアルタイムなものになります。ただし、エージェントと Enterprise Manager のオーバーヘッドが増大する可能性があります。設定する値が高いほど、マップに表示されるアプリケーションの依存関係は最新のものでなくなります。ただし、エージェントと Enterprise Manager のオーバーヘッドが減少する可能性があります。

エージェントと Enterprise Manager のオーバーヘッドについては、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。

デフォルト

3 日

`introscope.apm.pruning.enabled`

このプロパティは、APM データベースからアプリケーション問題切り分けマップデータの廃棄を有効にします。

注

- このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。
- このプロパティを `true` に設定すると、アプリケーション問題切り分けマップデータが APM データベースから廃棄されます。
- このプロパティを `false` に設定すると、アプリケーション問題切り分けマップデータは APM データベースから廃棄されず、無期限に保存されます。

デフォルト

アプリケーション問題切り分けマップデータの廃棄はデフォルトで、スタンドアロン Enterprise Manager および MOM 用のクラスタ環境内の APM データベース上で実行されます。

重要: アプリケーション問題切り分けマップデータの廃棄用のコレクタを設定することはできません。コレクタに対して `introscope.apm.pruning.enabled` プロパティを `true` に設定した場合、エラーが返されます。

introscope.apm.data.preserving.time

このプロパティは、アプリケーション問題切り分けマップデータを APM データベース内に保存する期間を制御します。保存期間の値より古いマップデータは、エイジアウトしているとみなされ、廃棄することができます。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

廃棄中、`introscope.apm.data.preserving.time` と `Introscope.apm.data.agingTime` の値の合計値より古いアプリケーション問題切り分けマップデータが削除されます。

たとえば、`introscope.apm.data.preserving.time` の値が 30 日で、`Introscope.apm.data.agingTime` の値が 1 日である場合は、 $30 + 1 = 31$ 日より古いマップデータが削除されます。

警告： 保存期間の設定が短すぎると（秒単位やミリ秒単位）、アプリケーション問題切り分けマップデータは、Enterprise Manager から届いた直後に APM データベースから削除される可能性があります。

以下の時間単位のいずれかを使用してください。大文字と小文字は区別されません。それぞれ、どちらかを使用できます。

- 日： days、 D
- 分： mins、 M
- 時間： hours、 H
- 秒： secs、 S
- ミリ秒： MS

デフォルト

365 日

introscope.apm.pruning.cron.trigger.expression

このプロパティは、アプリケーション問題切り分けマップデータを APM データベースから廃棄する頻度をスケジュールします。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

introscope.apm.pruning.cron.trigger.expression プロパティは、Open Symphony Quartz CronTrigger のスケジューラ式形式で設定されます。Quartz CronTrigger の詳細については、www.quartz-scheduler.org (www.quartz-scheduler.org) を参照してください。

この式は、スペースで区切られた 6 または 7 つのフィールドで構成される文字列です。文字列内のフィールドの順序は、左から右へ、以下のとおりです。

秒、分、時間、日、月、曜日、年

フィールドには、以下のものを含めることができます。

- 許可された値のいずれか
- 各フィールドで許可された特殊文字のさまざまな組み合わせ

許可された値、特殊文字、および式の例については、www.quartz-scheduler.org (www.quartz-scheduler.org) を参照してください。

デフォルト

`006**?` - このデフォルト式では、毎日午前 6 時にマップ データが廃棄されます。

ロケーション マップ データ

以下のプロパティを使用すると、ロケーション マップ 上の設定を構成できます。

introscope.workstation.locationmap.clamp

プロパティは、ロケーション マップ に含めることのできるエレメントの最大数を制御します。クランプの効用はロケーション マップ のサイズを制御することです。

注

返されるエレメントの数がクランプの値を超えると、一部のマップ エレメントは表示されません。ユーザに対しては、一部のエレメントが表示されないことを伝えるエラー メッセージが表示されます。

デフォルト

500

Web サービス

定期的に Web サービス API にアクセスする場合、多数の Web サービス呼び出しのため、パフォーマンスが低下していることに気づくかもしれません。Web サービス専用のスレッドの数はデフォルトでは 10 に設定されます。IntroscopeEnterpriseManager.properties ファイルにプロパティを追加することにより、この設定を変更できます。

introscope.apm.model.webservices.threadpool.numberofthreads

このプロパティは、スレッドプールで使用されるスレッドの数を指定します。このプロパティの使用は、オプションです。

警告： このプロパティに大きな数を設定するとパフォーマンスが低下する場合があります。このプロパティを設定するときに注意してください。

制約

整数である必要があります。

デフォルト値

10

例

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

このプロパティは、「*CA APM Catalyst Connector ガイド*」でも説明されています。

送信メッセージ キュー

これらのプロパティでは、送信メッセージ キューの設定を行うことができます。

transport.outgoingMessageQueueSize

このプロパティでは送信メッセージ キューのメッセージ数を指定します。

注

送信メッセージ キュー サイズを増加させるとより多くの RAM が使用されます。

制約

整数である必要があります。

デフォルト値

3000

例

```
transport.outgoingMessageQueueSize=3000
```

このプロパティについても「CA APM サイジングおよびパフォーマンス ガイド」で説明されています。

transport.override.isengard.high.concurrency.pool.max.size

このプロパティでは、同時出力ソケット接続の最大スレッド数を指定します。数値を大きくすることで直接的に応答時間の改善につながるわけではありませんが、速度の遅い接続を切り離すことで、Enterprise Manager が大幅に速度低下するのを防ぐことができます。

デフォルト値の 5 は、ほとんどのスタンドアロンエンタープライズマネージャおよびコレクタに適しています。MOM には 1 つのコレクタ当たり 1 つのスレッドが必要で、さらにおよそ 10 個の Workstation につき 1 つのスレッドが必要です。

特に MOM はネットワークトラフィックルータとして使用されるため、送信スレッド数を増やすメリットがあります。それは、より多くの Workstation にサービスを同時に提供できるという理由のためではなく、いずれかのコレクタが過負荷になった場合にクラスタ全体がフリーズすることを防止できるという理由のためでもあります。

重要: サイズを大きくしすぎないようにしてください。スレッドの追加によるオーバーヘッドは、特に 32 ビットの JVM では OutOfMemory 例外の原因になります。

制約

整数である必要があります。

デフォルト値

5

例

```
transport.override.isengard.high.concurrency.pool.max.size=5
```

このプロパティについても「CA APM サイジングおよびパフォーマンス ガイド」で説明されています。

スレッド ダンプ

これらのプロパティを使用すると、スレッド ダンプを設定できます。

スレッド ダンプの有効化および設定については、「CA APM Java Agent 実装ガイド」を参照してください。

この機能に対して以下のプロパティを設定できます。

[introscope.enterprisemanager.threaddump.enable](#) (P. 531)

[introscope.enterprisemanager.threaddump.storage.dir](#) (P. 532)

[introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days](#) (P. 532)

[introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days](#) (P. 532)

[introscope.enterprisemanager.threaddump.storage.max.disk.usage](#) (P. 533)

[introscope.enterprisemanager.threaddump.enable](#)

このプロパティを使用すると、Enterprise Manager に接続された任意のエージェントについて、メトリック ブラウザ ツリーのエージェント ノード上で [スレッド ダンプ] タブを有効にすることができます。

注

このプロパティはホット設定可能です。このプロパティを変更した場合、変更を有効にするために Enterprise Manager を再起動する必要はありません。

このプロパティは、IntroscopeAgentProfile

[introscope.agent.threaddump.enable](#) プロパティと連携して動作します。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。

このプロパティを *true* に設定し、IntroscopeAgentProfile

[introscope.agent.threaddump.enable](#) プロパティを *true* に設定すると、ユーザは [スレッド ダンプ] タブを表示できます。

このプロパティを *false* に設定すると、ユーザは [スレッド ダンプ] タブを表示できません。

デフォルト

true

introscope.enterprisemanager.threaddump.storage.dir

スレッド ダンプが保存されるディレクトリを、Enterprise Manager ホームディレクトリを基準にして指定します。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

<EM_Home>/threaddumps は、ユーザがスレッド ダンプ テキスト ファイルを保存するディレクトリではありません。ユーザは、任意の場所にスレッド ダンプ テキスト ファイルを保存できます。

デフォルト

threaddumps

introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days

CA Introscope がスレッド ダンプ ファイルをパージする頻度を日単位で指定します。

注

このプロパティは、
`introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days`
プロパティと連携して動作します。スレッド ダンプ ファイルの保存期間とパージ頻度を Enterprise Manager に対して指示するには、両方のプロパティを設定します。

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

デフォルト

1 (日)

introscope.enterprisemanager.threaddump.storage.clean.disk.olderthan.days

CA Introscope がスレッド ダンプ ファイルのパージを開始するまでの日単位の経過期間。

注

このプロパティは、
`introscope.enterprisemanager.threaddump.storage.clean.disk.freq.days` プロパティと連携して動作します。スレッドダンプファイルの保存期間とパージ頻度を Enterprise Manager に対して指示するには、両方のプロパティを設定します。

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

デフォルト

30 (日)

`introscope.enterprisemanager.threaddump.storage.max.disk.usage`

Enterprise Manager の上に保存できるスレッドダンプの数。

注

このプロパティはホット設定可能ではありません。このプロパティを変更した場合は、変更を有効にするために Enterprise Manager を再起動してください。

制約

8000 以下の整数である必要があります。

デフォルト値

5000

Web サービスがパフォーマンスを処理するためのスレッド プロパティ

定期的に Web サービス API にアクセスする場合、多数の Web サービス呼び出しのため、パフォーマンスが低下していることがわかります。Web サービス専用のスレッドの数はデフォルトでは 10 に設定されます。IntroscopeEnterpriseManager.properties ファイルにプロパティを追加することにより、この設定を変更できます。

プロパティの名前

introscope.apm.model.webservices.threadpool.numberofthreads

説明

スレッドプールで使用されるスレッドの数を指定します。このプロパティの使用は、オプションです。

制約

整数である必要があります。

デフォルト値

10

例

```
introscope.apm.model.webservices.threadpool.numberofthreads=15
```

このプロパティを使用する方法

1. IntroscopeEnterpriseManager.properties ファイルを編集用を開きます。
2. introscope.apm.model.webservices.threadpool.numberofthreads プロパティを追加し、値を指定します。
注: このプロパティに大きな数を設定するとパフォーマンスが低下します。このプロパティを設定するときに注意してください。
3. properties ファイルを保存して閉じます。

注: 変更を有効にするには、IntroscopeEnterpriseManager.properties ファイルを編集した後に Enterprise Manager を再起動する必要があります。

SNMP 問題切り分けマップ アラート アクション

SNMP 問題切り分けマップ アラート アクション プラグインは Enterprise Manager インストーラの一部としてインストールされます。SNMP 問題切り分けマップ アラート アクションのプロパティを指定するには、以下の構成を設定します。

注: SNMP 問題切り分けマップ アラート アクション プラグインのプロパティは、SNMP アラート アクション アダプタの既存のプロパティとは異なります。新しい SNMP 問題切り分けマップ アラートは、そのプレフィックス *introscope.apm.catalyst.triagemapalert.snmp* によって区別できます。

`introscope.apm.catalyst.triagemapalert.snmp.destination.host.ip`

APM コネクタの IP アドレスでこのプロパティを設定します。

`introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port`

SNMP トラップが送信される SNMP ポートでこのプロパティを設定します。

デフォルト

162

例

introscope.apm.catalyst.triagemapalert.snmp.destination.trap.port=162

`introscope.apm.catalyst.triagemapalert.snmp.community`

SNMP コミュニティ文字列でこのプロパティを設定します。

デフォルト

public

例

introscope.apm.catalyst.triagemapalert.snmp.community=public

introscope.apm.catalyst.triagemapalert.snmp.trigger

SNMP トラップ通知について望まれるトリガタイプでこのプロパティを設定します。

デフォルト

3

オプション

1

問題が発生している各期間で

2

重大度の増加時

3

重大度の変更時は常に

4

重大度の変更時に最終の状態のみレポート

例

introscope.apm.catalyst.triagemapalert.snmp.trigger=3

アプリケーション マップ オブジェクト

アプリケーション マップ オブジェクトが古いオブジェクトと見なされるための制限を指定するには、このプロパティを設定します。

デフォルト

300 (日)

例

introscope.apm.data.obsolete.time=300

APMEnterpriseManager.properties

APMEnterpriseManager.properties ファイルで定義されたプロパティは、Enterprise Manager のさまざまな動作を制御します。

APMEnterpriseManager.properties ファイルは、主にアプリケーション問題切り分けマップをサポートします (Enterprise Manager の動作を設定するために使用される他のプロパティ ファイルは、[IntroscopeEnterpriseManager.properties](#) (P. 482) と [apm-events-thresholds-config.xml](#) (P. 541) です)。

多くの Enterprise Manager プロパティを設定した後は、変更を有効にするために Enterprise Manager を再起動する必要があります。ただし、Enterprise Manager プロパティの中には、Introscope [ホット設定サービス](#) (P. 492)を使用するものもあります。これらのプロパティはホット設定プロパティと呼ばれます。ホット設定プロパティを設定した後は、Enterprise Manager を再起動する必要はありません。

c3p0 プロパティ

c3p0 プロパティ セクションでは、APM データベース接続プールのプロパティを設定します。c3p0 の完全なドキュメントについては、<http://www.mchange.com/projects/c3p0/index.html> を参照してください。

重要: プロパティ値に変更を加える前に「CA APM サイジングおよびパフォーマンス ガイド」内の c3p0 プロパティのドキュメントを参照することを強くお勧めします。

c3p0.dataSourceName

接続先のデータソース名。デフォルトの名前を、使用している APM データベース名に置換します。

デフォルト

apmDataSource

c3p0.acquireIncrement

プールから接続がなくなったときに c3p0 が一度に取得を試行する接続数を決定します。

デフォルト

3

c3p0.idleConnectionTestPeriod

接続がアイドル状態になったときに c3p0 が接続のテストを試行する時間（秒単位）。この時間が経過したら、c3p0 はこの間隔のプール内のアイドル接続をすべてテストします。

デフォルト

120

c3p0.maxIdleTime

アイドル状態の接続が接続プールから削除されるまで保持される時間（秒単位）。これを 0 に設定すると、接続はプールからタイムアウトされません。

デフォルト

0

c3p0.initialPoolSize

プールが起動時に取得を試行する接続数。値は minPoolSize と maxPoolSize の間である必要があります。

デフォルト

2

c3p0.minPoolSize

プールが常時保持する接続の最小数。

デフォルト

2

c3p0.maxPoolSize

プールが常時保持する接続の最大数。

デフォルト

4

Hibernate 固有のプロパティ

Hibernate 固有のプロパティ セクションでは、オープン ソース Hibernate API の各種要素を構成します。この API によって、透過的な永続性が可能になり、APM データベースのデータ格納が簡略化されます。Hibernate の詳細については、<http://www.hibernate.org/> を参照してください。

hibernate.jdbc.batch_size

JDBC バッチ サイズを指定します。

デフォルト

10

hibernate.order_inserts

バッチの挿入を有効化します。

これは、Hibernate による各エンティティへのバッチ挿入を有効化するために必要です。ユーザは、このプロパティを編集しないよう強く警告されています。

デフォルト

true

hibernate.order_updates

バッチの更新を有効化します。これは、**Hibernate** による各エンティティへのバッチ更新を有効化するために必要です。ユーザは、このプロパティを編集しないよう強く警告されています。

デフォルト

true

Hibernate キャッシュ設定

Hibernate キャッシュ設定セクションは、**APM** データベース内にデータをキャッシュするためのプロパティを設定します。

hibernate.cache.provider_class

使用する **Hibernate** キャッシュのタイプを指定します。

このプロパティは変更しないでください。

デフォルト

org.hibernate.cache.EhCacheProvider

hibernate.cache.use_second_level_cache

Hibernate のセカンドレベルキャッシュを有効にします。

デフォルト

true

hibernate.statement_cache.size

ステートメントキャッシュサイズを指定します。

デフォルト

10

ApplicationTriageMap 設定

このセクションを使用して、アプリケーション問題切り分けマップ設定をカスタマイズできます。

hibernate.cache.provider_configuration_file_resource_path

Hibernate ehCache 構成ファイルを指定します。

デフォルト

apm-ehcache.xml

introscope.apm.query.max.results

このプロパティを使用して、エージェントによってアプリケーション問題切り分けマップ表示に返されるデータ量のしきい値を指定します。値は、通常、フロントエンドまたはビジネス トランザクションの依存関係の数であり、フロントエンドまたはトランザクションがデプロイされ、クエリされている期間のデータをレポートするエージェントの数です。

デフォルト

20000

apm-events-thresholds-config.xml

Enterprise Manager の 3 つのプロパティ ファイルで定義されたプロパティは、Enterprise Manager のさまざまな動作を制御します。このセクションでは、*apm-events-thresholds-config.xml* 内のプロパティについて説明します（他のファイルは *IntroscopeEnterpriseMangager.properties* (482P.) と *APMEnterpriseManager.properties* (537P.) です）。`<EM_Home>/config` ディレクトリにある *apm-events-thresholds-config.xml* ファイルには、CA Introscope および CA CEM のクランプと CA APM の重要イベントのプロパティが含まれます。

- これらのクランプが設定されたしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [クランプ] タブにそれを通知します。
- 重要イベントが設定されたしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブル ビューにそれを通知します。

重要: *threshold value* フィールドのしきい値のみを設定してください。他の *clamp ID*、*importantEvent ID*、*description* などのフィールドは、CA Introscope がシステムの監視時に使用するフィールドなので、変更しないでください。

apm-events-thresholds-config.xml の設定変更を有効にするために Enterprise Manager や監視対象のアプリケーションを再起動する必要はありません。これらのプロパティは [Introscope ホット設定 \(P. 492\)](#) サービスを使用します。プロパティがホット設定を使用する場合は、設定変更を行った後で Enterprise Manager を再起動する必要はありません。

重要: 設定変更を行う前に、apm-events-thresholds-config.xml ファイルをバックアップしてください。設定によって apm-events-thresholds-config.xml ファイルにエラーが発生すると、Enterprise Manager はファイルを読み取ることができず、デフォルトのクランプしきい値設定が有効になります。たとえば、apm-events-thresholds-config.xml 内で右角かっこが欠落していると、Enterprise Manager はファイルを読み取ることができません。新しい設定や更新されたファイルが正しく機能しない場合は、以下のいずれかのアクションを実行します。

- できれば XML エディタを使用して、最後に変更されたファイルのトラブルシューティングを行います。
- 以前の正しく動作したバックアップを回復します。

Introscope クランプ プロパティ

これらのプロパティでは、Introscope に固有のクランププロパティについて制限設定を定義します。これらのプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールにそれを通知します。

これらのプロパティはホット設定可能です。つまり、ホットデプロイ中に Enterprise Manager がプロパティ ファイルをチェックしたときにこれらの値が適用されます。ホットデプロイは、約 60 秒ごとに実行されます。

その他の Enterprise Manager クランプは、<EM_Home>/config ディレクトリ内の [IntroscopeEnterpriseManager.properties \(P. 482\)](#) ファイルにあります。

introscope.clw.max.users

このプロパティでは、Enterprise Manager への接続を常に許可されるコマンドライン Workstation (CLW) の数を制限します。

このクランプは、CLW の接続によって Enterprise Manager の速度が低下する傾向がある場合に使用します。CLW を接続すると、抽出しようとするメトリックがあまりにも多いために Enterprise Manager に過度の負荷がかかる場合があります。

注

このクランプは、スタンドアロン Enterprise Manager、MOM、および CDV に使用できます。ただし、Workstation からコレクタへの接続は通常行われません。

ユーザが CLW コマンドを実行すると、Enterprise Manager は各クエリにつき 2 つの接続を作成します。1 つ目の接続は Enterprise Manager が利用可能かどうかを決定し、2 つ目の接続はクエリに使用されます。そのため、各 CLW コマンドにより `introscope.clw.max.users` 数は (1 つずつではなく) 2 つずつ増加します。さらに、一部の CLW では、Enterprise Manager に対して 3 つ以上の接続を作成します。`introscope.clw.max.users` プロパティのしきい値を設定する際は、これらの要素を考慮してください。

デフォルト

500

[introscope.enterprisemanager.agent.connection.limit](#)

`introscope.enterprisemanager.agent.connection.limit` プロパティは、Enterprise Manager に接続できるエージェントの数を制限します。

このプロパティはスタンドアロンの Enterprise Manager およびコレクタの両方に適用されます。

クランプのしきい値に到達し、新しいエージェントが Enterprise Manager に接続を試みると、以下のアクションが実行されます。

- Enterprise Manager はこのクランプのアクティブ化をログに記録します。
- Enterprise Manager は新しい接続を受け入れません。

注

Enterprise Manager は [em-jetty-config.xml ファイル](#) (P. 50) の `maxThreads` プロパティを使用して、Enterprise Manager が処理できる HTTPS エージェント接続の数を制限します。十分なスレッドがない場合、Enterprise Manager は、接続されたエージェントやエージェントからのプロセスメトリックを認識しません。

HTTPS を使用する場合、Enterprise Manager は `maxThreads` プロパティで設定されたエージェント数のみを処理します。`maxThreads` の値が `introscope.enterprisemanager.agent.connection.limit` の値以上であることを確認します。エージェントが HTTPS を介して接続するように設定されている場合、スレッドが不足すると、一部の HTTPS エージェントがクライアントに表示されないか、メトリックをレポートしない可能性があります。

`maxThreads` プロパティで Enterprise Manager が処理するエージェントの数を制限している場合、Enterprise Manager およびエージェントログには処理対象外のエージェントに関するエラー、警告、またはメッセージは含まれません。

デフォルトでは、オンプレミスインストールのエージェントは HTTPS を使用して接続しません。

デフォルト

400

例

```
introscope.enterprisemanager.agent.connection.limit=400
```


introscope.enterprisemanager.agent.error.limit

`introscope.enterprisemanager.agent.error.limit` プロパティはエラー スナップショットをクランプします。このプロパティでは、間隔ごとに各エージェントで Enterprise Manager が処理できるエラー スナップショット数の制限を定義します。

このプロパティはスタンドアロンの Enterprise Manager およびコレクタの両方に適用されます。

エージェントがレポートするエラー スナップショットの数が指定した制限を超えた場合、残りのエラーはすべて Enterprise Manager によってドロップされます。

デフォルト

10

例

```
introscope.enterprisemanager.agent.error.limit=10
```

introscope.enterprisemanager.agent.metrics.limit

このプロパティには、超過したときに Agent レポートがクランプされる値を設定します。

たとえば、メトリックのデフォルトの数 (1200,000) に達すると、以下の状況が発生します。

- エージェントは 120,000 個のメトリックのみをレポートします。
- エージェントは Enterprise Manager に新しいメトリックを送信しません。

エージェントの設定が適切でない場合、数千に上るメトリックが連続して作成され、Enterprise Manager が過負荷状態になる可能性があります。

このプロパティを使用すると、メトリックによる過負荷を防ぐことができます。指定した数を超えるメトリックをエージェントが生成した場合、Enterprise Manager はメトリックを削除します。このような場合は、エージェントの設定を変更して、レポートされるメトリックの量を減らしてください。

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

デフォルト

120000

注

このクランププロパティは、Introscope.Agent.profile ファイル内にある `introscope.agent.metricClamp` プロパティと連携して機能します。

`introscope.enterprisemanager.agent.metrics.limit` クランプ値が `introscope.agent.metricClamp` 値の前にトリガされた場合、Enterprise Manager はエージェントメトリックを読み取りますが、それを Investigator メトリック ブラウザ ツリー内でレポートしません。

`introscope.agent.metricClamp` クランプ値が `introscope.enterprisemanager.agent.metrics.limit` クランプ値の前にトリガされた場合、エージェントは Enterprise Manager へのメトリックの送信を停止します。

introscope.enterprisemanager.agent.trace.limit

`introscope.enterprisemanager.agent.trace.limit` プロパティはトランザクション追跡をクランプします。このプロパティでは、間隔ごとに各エージェントで Enterprise Manager が処理できるトランザクションイベント数の制限を定義します。

このプロパティはスタンドアロンの Enterprise Manager およびコレクタの両方に適用されます。

エージェントがレポートするトランザクション追跡の数が指定した制限を超えた場合、残りの追跡はすべて Enterprise Manager によってドロップされます。

デフォルト

1000

例

```
introscope.enterprisemanager.agent.trace.limit=1000
```

introscope.cdv.max.users

このプロパティでは、1つのコレクタに接続できるクロス クラスタ データ ビューア (CDV) の数を制限します。クロス クラスタ データ ビューアは、通常、2つ以上のクラスタにまたがって複数のコレクタに接続します。

CDV の接続によってメトリックが抽出され、コレクタのパフォーマンス負荷が増加する場合があります。このクランプを使用して、コレクタが受け入れることができる CDV 接続の数を制限してください。

デフォルト

5

introscope.enterprisemanager.disconnected.historical.agent.limit

このプロパティでは、切断されてもマウントされ続ける履歴エージェントの数を制限します。このクランプにより、Enterprise Manager のランタイムメモリの使用を最小限に抑えることができます。

このクランプは、以下の両方の履歴エージェントを制限します。

- Enterprise Manager が自動的にマウント解除できるエージェント。
- CA APM ユーザが手動でマウント解除する必要があるエージェント。

エージェントのマウントおよびマウント解除については、「CA APM Workstation ユーザ ガイド」を参照してください。

このクランプのしきい値に到達すると、Enterprise Manager は自動的にマウント解除できる最も古い切断済みの履歴エージェントをマウント解除しようとします。Enterprise Manager が自動的にマウント解除できる履歴エージェントがない場合、それは CA APM ユーザが切断された履歴エージェントをすべて手動でマウントしたことを意味します。Enterprise Manager は、CA APM ユーザが手動でマウントした切断済みの履歴エージェントをマウント解除しようとしません。

例

`introscope.enterprisemanager.disconnected.historical.agent.limit=400`

このクランプのしきい値クランプを 400 に設定しています。Tomcat という名前のエージェントと Other という名前の 399 個のエージェントが Enterprise Manager に接続されています。400 個のエージェントのうち、Tomcat エージェントは自動的にマウント解除できない最も古いエージェントです。Enterprise Manager は 400 個のエージェントをすべて切断します。エージェントが再接続するときに、Enterprise Manager は切断されてもマウントされ続けているエージェントの数がエージェントのしきい値である 400 個未満かどうかを評価します。Other という名前の 399 個のエージェントがすべて再接続した後、Tomcat エージェントが再接続しようとしています。Enterprise Manager は以下のアクションを実行します。

- Tomcat エージェントが 400 個の切断済みエージェントの中で自動的にマウント解除できる最も古いエージェントであることを特定します。
- Tomcat エージェントをマウント解除します。

Tomcat エージェントをマウント解除すると、切断されたエージェントの数が 399 個になり、再びエージェントクランプのしきい値である 400 個を下回ります。

注

Enterprise Manager は、以下の状況が発生したときに APM ステータス コンソールに通知します。

- 切断済みでマウントされているエージェントがクランプのためにマウント解除された。
- 手動によるエージェントのマウントが失敗した。

以下の状況が発生した場合、このクランプは切断済みでマウントされているエージェントを廃棄しません。

- Enterprise Manager のメモリが不足している。
- 切断された履歴エージェントがタイムアウトになり、自動的にマウント解除された。

以下の状況が発生した場合、切断された履歴エージェントはマウントされたままになります。

- 履歴エージェントが切断状態になり、自動的にマウント解除できる。
- 切断された履歴エージェントの数が `introscope.enterprisemanager.disconnected.historical.agent.limit` の値を下回っている。

以下の状況が発生した場合、Enterprise Manager は切断された履歴エージェントをマウントします。

- CA APM ユーザが切断された履歴エージェントを手動でマウントしようとした。
- 切断された履歴エージェントの数が `introscope.enterprisemanager.disconnected.historical.agent.limit` の値を下回っている。

以下の状況が発生した場合、Enterprise Manager は切断済みでマウントされているエージェントのうち、自動的にマウント解除できるものを検索します。

- 自動的にマウント解除できる履歴エージェントが切断状態になった。
- CA APM ユーザが履歴エージェントを手動でマウントしようとした。
- 切断された履歴エージェントの数が `introscope.enterprisemanager.disconnected.historical.agent.limit` の値と等しい。

Enterprise Manager は、切断済みでマウントされているエージェントを検出すると、最も古い切断済みの履歴エージェントをマウント解除し、新しく切断されたエージェントをマウントしたままにします。Enterprise Manager が自動的にマウント解除できる履歴エージェントがない場合、Enterprise Manager は新しく切断された履歴エージェントをすぐにマウント解除します。その後、CA APM ユーザが履歴エージェントを手動でマウントしようとする、以下のアクションが実行されます。

- いくつかの履歴エージェントをマウント解除して、新しい履歴エージェントをマウントするための空きを確保するようにユーザに指示するエラーメッセージが Workstation に表示されます。
- Enterprise Manager から APM ステータス コンソールに通知が送信されます。

デフォルト

400

introscope.enterprisemanager.events.limit

`introscope.enterprisemanager.events.limit` プロパティはトランザクション追跡をクランプします。このプロパティでは、間隔ごとに **Enterprise Manager** によって処理されるトランザクションイベント数の制限を定義します。

このプロパティはスタンドアロンの **Enterprise Manager**、コレクタ、および **MOM** に適用されます。

このクランプは、すべてのエージェントによって生成されたすべてのトランザクションイベントの総数に適用されます。クランプ値に到達すると、その間隔内のそれ以降にエージェントからレポートされたトランザクションイベントの残りのすべてがドロップされます。

デフォルト

1250

例

```
introscope.enterprisemanager.events.limit=1250
```

introscope.enterprisemanager.metrics.historical.limit

このプロパティは、**Enterprise Manager** 内の履歴メトリック数を制限します。制限は 15 秒ごとにチェックされるため、クランプが適用される前にこの値を超える場合があります。制限を超えたことが検出されると、**Enterprise Manager** はすべてのエージェントを停止するため、新しいメトリックを登録することができなくなります。古いメトリックは引き続きレポートされます。

デフォルト

1200000

introscope.enterprisemanager.metrics.live.limit

このプロパティは、エージェントから現在レポートされているライブメトリックを制限します。制限を超えたことが検出されると、Enterprise Manager はすべてのエージェントを停止するため、新しいメトリックを登録することができなくなります。制限は 15 秒ごとにチェックされるため、クランプが適用される前にこの値を超える場合があります。古いメトリックは引き続きレポートされます。履歴データのあるメトリックは、クランプされません。

例

エージェントに 60k のメトリックがある場合、これはクランプ前に Enterprise Manager にレポートされ、50k のクランプが適用されますが、60k の古いメトリックはすべてまだ、Enterprise Manager に登録することが可能です。ただし、履歴データがまだ収集されていない新しいメトリックを登録しようとしても、登録することはできません。

デフォルト

500000

introscope.enterprisemanager.transactionevents.storage.max.disk.usage

トランザクショントレースストレージに必要な最大ディスク容量を MB 単位で指定します。この値が最大値を超えると、履歴追跡ストレージのサイズがこのプロパティ値以下になるまで、毎日の履歴追跡保存データが最も古いものから順に削除されます。このプロパティ値のサイズを超えても、削除する履歴追跡データの決定時には追跡インデックスのサイズが考慮されないため、保存されている追跡データは削除されません。

この値が負または 0 の場合は、保存されているすべての履歴追跡値を削除する必要があります。

トランザクションイベントデータベースがこの値よりも大きい場合は、データベースサイズの合計がこの値より小さくなるまで、履歴保存ファイルが最も古い保存ファイルから削除されます。

これにより、履歴データは、古いと判断される日付になっていなくても削除される可能性があります。現在進行中の保存ファイルは、データベースのサイズが最大値を超えても削除されません。

トランザクション イベント データベースが大きすぎると判断した場合は、Enterprise Manager がシャットダウンされている間にデータベース ファイルを手動で削除できます。Enterprise Manager が再起動すると、トランザクショントレース ストレージシステムはファイルが手動で削除されていることを認識し、トレース インデックスを適切に調整します。

注

ファイルを手動で削除する場合は、追跡用ディレクトリの中にある、*traces_yyyyMMdd.db* という形式のファイルのみを削除してください。*yyyyMMdd* は、そのファイルに含まれる追跡データの年月日を表します。このディレクトリまたはサブディレクトリ内にあるその他のファイルは削除しないでください。

デフォルト

1024

introscope.workstation.max.users

このプロパティでは、Enterprise Manager への接続を常に許可される Workstation の数を制限します。

このクランプは、Workstation の接続によって Enterprise Manager の速度が低下する傾向がある場合に使用します。Workstation を接続すると、抽出しようとするメトリックがあまりにも多いために Enterprise Manager に過度の負荷がかかる場合があります。

注

このクランプは、スタンドアロン Enterprise Manager、MOM、および CDV に使用できます。しかし、Workstation からコレクタへの接続は通常行われません。

デフォルト

40

カスタマ エクスペリエンス クランプ プロパティ

これらのプロパティでは、CA CEM 固有のクランプ プロパティについて制限設定を定義します。これらのプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールにそれを通知します。

これらのプロパティはホット設定可能です。つまり、ホット デプロイ中に Enterprise Manager がプロパティ ファイルをチェックしたときにこれらの値が適用されます。ホット デプロイは、約 60 秒ごとに実行されます。

introscope.enterprisemanager.max.application.user.rows

取得されるアプリケーション ユーザの最大数です。

アプリケーション ユーザの数が多すぎると、パフォーマンスに悪影響が及ぶことがあります。

オプション

数値

デフォルト

1000

例

```
introscope.enterprisemanager.max.application.user.rows =1000
```

注

最大数に達すると、アプリケーション ユーザを一覧表示する CA CEM コンソールの Web ページの表示内容が制限されます。

前回の同期以降の変更のリストアップ数制限

監視を同期する前に、前回の同期以降に加えた構成変更を確認することができます。これについては、「[前回の同期以降の構成変更の表示 \(P. 349\)](#)」を参照してください。

構成変更は、[監視] ページの [ドメイン構成変更履歴] テーブルに表示されます。

introscope.enterprisemanager.max.number.domain.configuration.changes プロパティによって、このテーブル内の最大行数が決まります。

introscope.enterprisemanager.max.number.domain.configuration.changes

[前回の同期以降の変更を表示]（[設定] > [監視]）をクリックしたときに[ドメイン構成履歴]テーブルに表示する最大変更数を設定します。

値が -1 の場合は、すべての変更が表示されます。

オプション

数値

デフォルト

0（無制限）

例

```
introscope.enterprisemanager.max.number.domain.configuration.changes=1000
```

注

「[監視の同期](#) (P. 348)」を参照してください。

introscope.enterprisemanager.max.transaction.user.groups

自動的に作成されるユーザグループの最大数。

このプロパティは、要求属性によって、または IP サブネット別に、自動的に作成されるユーザグループと一緒に使用されます。

ユーザグループの数が多すぎると、ユーザがいないグループであっても、パフォーマンスに悪影響が及ぶことがあります。

オプション

数値

最大許容値は 10,000 です。

デフォルト

5000

例

```
introscope.enterprisemanager.max.transaction.user.groups=5000
```

注

最大値に達した場合は、以下のようになります。

- ユーザグループは自動的に作成されなくなります。
- 新しいグループを作成する代わりに、ユーザは [新規ユーザ] グループに割り当てられます。
- [システム] の [イベント] リストに、警告メッセージが表示されます。

「[CA CEM 上のユーザおよびグループの管理 \(P. 353\)](#)」を参照してください。

introscope.enterprisemanager.transaction.discovery.max.nonidentifying.components

現在定義されているトランザクションのために保持する、検出された非識別コンポーネントの最大数（このほかに、元の非識別コンポーネントがあります）。

オプション

数値（正の整数）

デフォルト

50

例

```
introscope.enterprisemanager.transaction.discovery.max.nonidentifying.component=60
```

注

この制限は、たとえば、コンポーネントが、毎日変更される GIF ファイルである場合など、非識別コンポーネントの変更頻度が高いトランザクションに重要です。この制限を設定することで、トランザクションに対して過剰な数の（使用されなくなったと思われる）非識別コンポーネントを保存することがなくなります。

新しい非識別コンポーネントが古い非識別コンポーネントに置き換わるたびに、「新規コンポーネントの追加で上限を超えました」という CA CEM イベントがログに記録されます。

非識別コンポーネントの自動検出に関する一般的な情報については、「CA APM トランザクション定義ガイド」を参照してください。

重要イベントのしきい値の設定

これらのプロパティでは、Enterprise Manager の状態監視にとって重要なイベントを APM ステータス コンソールに通知する際に使用される制限を定義します。これらはホット設定可能です。つまり、ホットデプロイ中に Enterprise Manager がプロパティ ファイルをチェックしたときにこれらの値が適用されます。ホットデプロイは、約 60 秒ごとに実行されます。

apm.events.thresholds.config.error

このプロパティでは、apm-events-thresholds-config.xml ファイルに構文エラーがないかどうかを監視します。Enterprise Manager は、エラーを検出すると以下のアクションを実行します。

- APM ステータス コンソールの [重要イベント] テーブルビューに通知します。
- apm-events-thresholds-config.xml ファイルのすべてのクランププロパティおよび重要イベントプロパティの値をデフォルト値に戻します。

このプロパティは、クラスタ内のすべてのコレクタまたはスタンドアロン Enterprise Manager に適用されます。

デフォルト

適用不可。このプロパティは通知のみを目的としたものであり、変更できません。

introscope.enterprisemanager.cpu.usage

このプロパティでは、Enterprise Manager の CPU 使用率を重要イベントと見なす率 (%) の制限を定義します。このプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブルビューにそれを通知します。

このプロパティは、Enterprise Manager の CPU Capacity (%) メトリックの監視に基づいています。60% を超える CPU 使用率は、Enterprise Manager のリソースに問題があることを示します。CPU 使用率と Enterprise Manager のパフォーマンスについては、「CA APM サイジングおよびパフォーマンスガイド」を参照してください。

このプロパティは、クラスタ内のすべてのコレクタまたはスタンドアロン Enterprise Manager に適用されます。

デフォルト

60

例

```
introscope.enterprisemanager.cpu.usage=60
```

introscope.enterprisemanager.database.connectivity

このプロパティでは、Enterprise Manager と APM データベースの接続を監視します。接続が切断されると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブルビューにそれを通知します。

このプロパティは、クラスタ内のすべてのコレクタまたはスタンドアロン Enterprise Manager に適用されます。

デフォルト

適用不可。このプロパティは通知のみを目的としたものであり、変更できません。

introscope.enterprisemanager.harvest.cycle.diff

このプロパティでは、コレクタと MOM の収集サイクルの同期が取れていないタイムスライス数の制限を定義します。このプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブルビューにそれを通知します。

このプロパティは、コレクタと MOM のメトリック収集サイクルを比較した結果に基づいています。15 秒ごとの収集サイクルの間に、以下のアクションが実行されます。

- コレクタは、エージェントのメトリック データを収集して集計します。
- コレクタは、MOM にメトリック データを送信します。
- MOM は、コレクタから送信されたデータを集計します。
- MOM は、Workstation にデータをレポートします。

コレクタは、その収集サイクルが完了するまで、MOM にデータを送信しません。コレクタの収集サイクルが MOM の収集サイクル中に完了しない場合は、コレクタと MOM の間でデータ集計の同期が取れていません。

コレクタと MOM の同期が取れていない MOM の収集サイクルがプロパティ値より長く続いた場合、CA APM はクラスタに異常があると見なします。

デフォルト

4

例

```
introscope.enterprisemanager.harvest.cycle.diff=4
```

注

このプロパティは MOM 上でのみ設定してください。

introscope.enterprisemanager.harvest.duration

このプロパティでは、Enterprise Manager の収集継続時間を重要イベントと見なすミリ秒数 (ms) の制限を定義します。このプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブル ビューにそれを通知します。

このプロパティは、Enterprise Manager の Harvest Duration (ms) メトリックの監視に基づいています。3500 ミリ秒より長い収集継続時間は、Enterprise Manager のリソースに問題があることを示します。収集継続時間と Enterprise Manager のパフォーマンスについては、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。

このプロパティは、クラスタ内のすべてのコレクタまたはスタンドアロン Enterprise Manager に適用されます。

デフォルト

3500

例

```
introscope.enterprisemanager.harvest.duration=3500
```

introscope.enterprisemanager.smartstor.duration

このプロパティでは、Enterprise Manager の SmartStor 持続時間を重要イベントと見なすミリ秒数 (ms) の制限を定義します。このプロパティがしきい値に到達するか、またはそれを超過すると、Enterprise Manager は APM ステータス コンソールの [重要イベント] テーブル ビューにそれを通知します。

このプロパティは、Enterprise Manager の SmartStor Duration (ms) メトリックの監視に基づいています。3500 ミリ秒より長い SmartStor 持続時間は、Enterprise Manager のリソースに問題があることを示します。SmartStor 持続時間と Enterprise Manager のパフォーマンスについては、「CA APM サイジングおよびパフォーマンス ガイド」を参照してください。

このプロパティは、クラスタ内のすべてのコレクタまたはスタンドアロン Enterprise Manager に適用されます。

デフォルト

3500

例

```
introscope.enterprisemanager.smarstor.duration=3500
```

ResourceMetricMap.properties

さまざまなエージェントから収集されたリソース メトリック カテゴリは、Workstation 内でレポートされます。リソース メトリック カテゴリは事前に定義されています。事前に定義されたリソース メトリック グループの追加や削除はできませんが、管理者権限がある場合は、各リソース メトリック グループに関してレポートされるデータを指定するリソース メトリック マッピングを追加、変更、削除できます。

リソース メトリックをリソース メトリック カテゴリにマップする方法

1. エージェント上で JMX レポートが有効であることを確認します。詳細については、「CA APM Java Agent 実装ガイド」の「JMX レポートの有効化」を参照してください。
2. MOM 上の `<EM_Home>/Config` ディレクトリにある `ResourceMetricMap.properties` ファイルを編集して、リソース メトリックをリソース メトリック カテゴリにマップします。リソース メトリックのマッピングの詳細については、アプリケーションサーバのマニュアルを参照してください。
 - a. `<categoryName>.path<recordID>:<agentMetricPath>` という形式でメトリック エントリを追加します。例：

```
threads.used.path.1=Tomcat|ThreadPool|getCurrentThreadsBusy.path.1=CPU:Processor Count
```

ここで、`memory.utilization` はメトリックの名前であり、`CPU:Processor Count` はそのデフォルトのメトリック パスです。
 - b. 数値を使った増分レコード ID メトリックを追加します。例：

```
cpu.utilization.path.1=Non Existent metric  
cpu.utilization.path.2=CPU|Processor 0:Utilization % (aggregate)
```

同じメトリック グループ内で複数のパスを使用することにより、同じ名前異なるパスを持つメトリックを設定します。これにより、たとえば、フロントエンドをデプロイした異なるアプリケーションサーバから同じメトリックを取得できます。
3. MOM とコレクタを再起動します。

新しくマップされたリソース メトリック値が Workstation 内でレポートされます。

同じメトリックの複数のインスタンス用に設定された ResourceMetricMap.properties ファイルの例

Threads in Use メトリックの複数のインスタンスがクラスタ内の 3 つのコレクタを指すように設定されている ResourceMetricMap.properties ファイルのセクションを以下に示します。

#CPU Utilization

```
cpu.utilization.path.1=CPU:Utilization % (process)
```

#Time Spent in GC

```
memory.utilization.path.1=GC Monitor|Percentage of Time Spent in GC during last 15 minutes
```

#Threads in Use

```
threads.used.path.1=WebSpherePMI|threadPoolModule|WebContainer:ActiveCount
```

```
threads.used.path.2=WebLogic|JMX Aggregate|Thread Pool:Waiting Request Count
```

```
threads.used.path.3=Tomcat|ThreadPool|default thread pool:getCurrentThreadsBusy
```

#JDBC Connections in Use

```
connections.used.path.1=WebSpherePMI|connectionPoolModule:WaitingThreadCount
```

```
connections.used.path.2=WebLogic|JMX Aggregate|JDBC Connection Pool:Waiting Thread Count
```

リソース メトリックを以下のリソース メトリック カテゴリにマップできます。

[CPU Utilization](#) (P. 561)

[Time Spent in GC](#) (P. 562)

[Threads in Use](#) (P. 562)

[JDBC Connections in Use](#) (P. 562)

CPU Utilization

CPU Utilization は、使用中の CPU のサイズを測定します。

マッピングの例

```
cpu.utilization.path.1=CPU:Utilization % (process)
```

```
cpu.utilization.path.2=Some other metrics path
```

Time Spent in GC

Time Spent in GC は、ガベージコレクタで費やされた時間を測定します。これは、その作業量がアプリケーションのパフォーマンスを大きく左右しているかどうかを理解するのに役立ちます。

マッピングの例

```
memory.utilization.path.1=memory utilization path
```

Threads in Use

Threads in Use は、使用中のスレッドの数を測定します。

マッピングの例

```
threads.used.path.1=threads used path
```

JDBC Connections in Use

JDBC Connections in Use は、アクティブな Java Database Connectivity インスタンスの数を測定します。

マッピングの例

```
connections.used.path.1=connections used path
```

Catalyst.properties

Catalyst プロパティを使用すると、CA Catalyst データをロードし、Catalyst データからレポートされるアラートをフィルタリングできるように CA APM を設定できます。

詳細:

[catalyst.host](#) (P. 563)

[catalyst.protocol](#) (P. 564)

[catalyst.port](#) (P. 564)

[catalyst.login](#) (P. 564)

[catalyst.password](#) (P. 564)

[catalyst.rest.entrypoint](#) (P. 565)

[catalyst.rest.alerts.pollingperiodsec](#) (P. 565)

[catalyst.rest.virtualhosts.pollingperiodsec](#) (P. 565)

[catalyst.product.url](#) (P. 566)

[catalyst.alert.filter.total](#) (P. 566)

[catalyst.alert.filter.time](#) (P. 566)

[catalyst.alert.filter.products](#) (P. 567)

[catalyst.alert.filter.types](#) (P. 567)

[catalyst.alert.filter.severities](#) (P. 568)

[catalyst.rest.maxFailures](#) (P. 568)

[catalyst.rest.maxAlertsPerPage](#) (P. 569)

[catalyst.rest.alerts.threads](#) (P. 569)

[catalyst.rest.virtualhosts.threads](#) (P. 569)

[catalyst.entity.cache.size](#) (P. 570)

[catalyst.entity.cache.expirationsec](#) (P. 570)

[catalyst.database.alerts.enabled](#) (P. 570)

[catalyst.database.map.name](#) (P. 571)

[Catalyst データをロードするための APM の設定](#) (P. 285)

[CA Catalyst データをロードするための CA APM の設定](#) (P. 286)

[CatalystPolicy.xml ファイルの設定](#) (P. 287)

catalyst.host

CA Catalyst RESTful API ホスト名でこの必須プロパティを設定します。この行のコメントを外した後、CA Catalyst に値を追加します。

デフォルト

このプロパティはデフォルトで無効になっています。

catalyst.protocol

CA Catalyst Web アクセス用のプロトコルでこの必須プロパティを設定します。

例

```
catalyst.protocol = http
```

catalyst.port

CA Catalyst Web アクセス用のポート番号でこの必須プロパティを設定します。

例

```
catalyst.port = 7070
```

catalyst.login

CA Catalyst へのログインに使用されるユーザ名でこの必須プロパティを設定します。

例

```
catalyst.login = <CA Catalyst ユーザ名を入力します>
```

catalyst.password

CA Catalyst へのログインに使用されるパスワードでこの必須プロパティを設定します。

例

```
catalyst.password = <CA Catalyst パスワードを入力します>
```

catalyst.rest.entrypoint

CA Catalyst RESTful API エントリ ポイント用の URL コンテキストでこの必須プロパティを設定します。

例

```
catalyst.rest.entrypoint = /ssaweb/search
```

catalyst.rest.alerts.pollingperiodsec

CA Catalyst で新しいアラートをチェックする頻度を指定するには、このオプションのポーリングプロパティを設定します。

デフォルト

15 (秒)

例

```
catalyst.rest.alerts.pollingperiodsec = 15
```

catalyst.rest.virtualhosts.pollingperiodsec

CA Catalyst で仮想ホストの更新をチェックする頻度を指定するには、このオプションプロパティを設定します。

デフォルト

60 (秒)

例

```
catalyst.rest.virtualhosts.pollingperiodsec = 60
```

catalyst.product.url

原因製品のベース URL アドレスでこのプロパティを設定します。

例

```
# Spectrum
# catalyst.product.url = CA:00005->http[s]://<host>[:CA
Portal]/spectrum/oneclick.jnlp?explorer={Entity.MdrElementID}
# eHealth
# catalyst.product.url = CA:00002->http[s]://<host>[:CA Portal]/{Alert.UrlParams}
# Insight
# catalyst.product.url = CA:00048->http[s]://<host>[:CA Portal]
# NetQoS
# catalyst.product.url = CA:00034->http[s]://<host>[:CA
Portal]/npc/Default.aspx?pg={Alert.UrlParams}
```

catalyst.alert.filter.total

Workstation にロードする CA Catalyst アラートの最大数を設定するには、このオプションプロパティを設定します。

デフォルト

250

例

```
catalyst.alert.filter.total = 250
```

catalyst.alert.filter.time

CA Catalyst アラートを Workstation に表示する時間の長さを設定するには、このオプションプロパティを設定します。

デフォルト

72 (時間)

例

```
catalyst.alert.filter.time = 72
```

catalyst.alert.filter.products

指定された製品のアラートをすべて除外するには、このオプションプロパティを設定します。

例

```
catalyst.alert.filter.products = CA:00030
```

catalyst.alert.filter.types

Workstation に表示しない CA Catalyst アラートタイプを指定するには、このオプションプロパティを設定します。アラートタイプを区切るにはコンマを使用します。

オプション

- Risk
- Risk-Capacity
- Risk-Change
- Risk-Fault
- Risk-Security
- Risk-Performance
- Risk-Root Cause
- Quality
- Compliance
- Cost

例

```
catalyst.alert.filter.types = Risk-Security,Compliance,Cost
```

catalyst.alert.filter.severities

Workstation に表示しない CA Catalyst アラート重大度を指定するには、このオプションプロパティを設定します。2つの重大度値の間にハイフン (-) を入れて範囲を定義するか、重大度値の右側または左側にハイフンを入れてオープン範囲を定義するか、コンマを使って複数の値を設定します。

デフォルト

Unknown

オプション

このプロパティには以下のオプションを設定でき、オープン範囲を使用できます。

- Normal
- Informational
- Unknown
- Minor
- Major
- Critical
- Fatal

例

catalyst.alert.filter.severities = -Unknown

catalyst.rest.maxFailures

ポーリングがキャンセルされるまで許可する CA Catalyst 障害の最大数を指定するには、このオプションプロパティを設定します。

デフォルト

10

例

catalyst.rest.maxFailures = 10

catalyst.rest.maxAlertsPerPage

1 回の REST クエリで返される CA Catalyst アラートの最大数を指定するには、このオプションプロパティを設定します。

デフォルト

250

例

```
catalyst.rest.maxAlertsPerPage = 250
```

catalyst.rest.alerts.threads

アラートに使用するスレッドの最大数を指定するには、このオプションプロパティを設定します。

デフォルト

2

例

```
catalyst.rest.alerts.threads = 2
```

catalyst.rest.virtualhosts.threads

仮想ホストに使用するスレッドの最大数を指定するには、このオプションのポーリングプロパティを設定します。

デフォルト

1

例

```
catalyst.rest.virtualhosts.threads = 1
```

catalyst.entity.cache.size

CA Catalyst に使用するメモリ内エンティティ キャッシュのサイズを指定するには、このオプションプロパティを設定します。

デフォルト

3000 (メガバイト)

例

```
catalyst.entity.cache.size = 3000
```

catalyst.entity.cache.expirationsec

エンティティ キャッシュの期限切れ時間を秒単位で指定するには、このオプションプロパティを設定します。

デフォルト

36000 (秒)

例

```
catalyst.entity.cache.expirationsec = 36000
```

catalyst.database.alerts.enabled

CA Catalyst データベース アラートを Workstation に送信するには、このプロパティを設定します。デフォルトでは、CA Catalyst データベース アラートは Workstation に送信されます。CA Catalyst データベース アラートの送信を停止するには、設定を *false* に変更します。

デフォルト

true

デフォルト

```
catalyst.database.alerts.enabled=true
```

catalyst.database.map.name

データベース接続文字列を CA Catalyst データベース パラメータにマップするファイルの場所を指定するには、このオプションプロパティを設定します。デフォルトのマッピングが正しく動作しない場合にのみ、このプロパティを設定してください。

Microsoft SQL データベースの例

1. <Agent_Home>/wily/core/config ディレクトリにある *IntroscopeAgent.profile* ファイルを開き、以下のプロパティを true に設定します。
`catalyst.database.map.name = CatalystDatabaseMap.txt`
2. <EM_Home>/config ディレクトリにある *CatalystDatabaseMap.txt* ファイルを開き、以下の式を定義します。
 - a. 式の左側は、JDBC の URL を照合するための完全な Java 正規表現を表します。
 - b. 式の左側と右側は式の区切り文字によって分けられます。式の区切り文字はパイプ (|)、矢印 (=>)、等号 (=)、または二重等号 (==) で、レコードの区切り文字として使用できます。
 - c. 式の右側にはデータベース パラメータを列挙します。データベース パラメータにはサーバ名、データベース名、およびデータベース インスタンス名があります。

例：

```
^jdbc:sqlserver.+1433.* = deviaat011|apmtest|default
^jdbc:sqlserver.+1533.* = deviaat011|apmtest|testinstance
```

EMservice.conf

<EM_Home>%bin にある *EMService.conf* ファイルには、Enterprise Manager が Windows のサービスとして実行されるときに使用される設定が含まれています。

注：以下のプロパティを設定するときは、先に Enterprise Manager サービスの登録を解除する必要があります。プロパティの設定が完了したら、Enterprise Manager サービスを再登録してください。

wrapper.java.command

Java アプリケーション ラッパ コマンド。

デフォルト

`jre¥¥bin¥¥java.exe`

wrapper.java.mainclass

Java メイン クラス ラッパ コマンド。

デフォルト

`org.tanukisoftware.wrapper.WrapperSimpleApp`

wrapper.java.classpath.x

`wrapper.jar` を含む Java Classpath。クラスパス エレメントは、以下のよう
に、順序だてて追加する必要があります。

- `wrapper.java.classpath.1=./lib/ServiceWrapper.jar`
- `wrapper.java.classpath.2=./launcher.jar`
- `wrapper.java.classpath.3=`

wrapper.java.library.path.1

Java ライブラリ パスは、`Wrapper.DLL` または `libwrapper.so` への場所を示し
ます。

デフォルト

`./lib`

wrapper.java.additional.x=

64 ビット Windows にのみ適用可能な追加の Java パラメータ。

最初の追加パラメータは、`-Xrs` になります。そこから、必要に応じてパラメータを追加できます。例：

- `wrapper.java.additional.1=-Xrs`
- `wrapper.java.additional.1=-Djava.awt.headless=false`
- `wrapper.java.additional.2=-showversion`
- `wrapper.java.additional.3=-XX:+UseConcMarkSweepGC`
- `wrapper.java.additional.4=-XX:+UseParNewGC`

デフォルト

`-Xrs`

wrapper.java.initmemory

ラッパの初期メモリ サイズ (MB 単位)。

デフォルト

128

wrapper.java.maxmemory

ラッパの最大メモリ サイズ (MB 単位)。

デフォルト

512

wrapper.app.parameter.x

アプリケーションパラメータ。必要に応じてパラメータを追加できます。
例：

- `wrapper.app.parameter.1=org.eclipse.core.launcher.Main`
- `wrapper.app.parameter.2=-consolelog`
- `wrapper.app.parameter.3=-noExit`
- `wrapper.app.parameter.4=-product`
- `wrapper.app.parameter.5=com.wily.introscope.em.product`
- `wrapper.app.parameter.6=-install`
- `wrapper.app.parameter.7=./product/enterprisemanager`
- `wrapper.app.parameter.8=-configuration`
- `wrapper.app.parameter.9=./product/enterprisemanager/configuration`

wrapper.startup.timeout

ラッパが JVM プロセスを開始した時間からラッパの JVM 側がアプリケーションの開始を応答するまでの時間間隔に許容される秒数。値 0 を入力することは、システムが決してタイムアウトしないことを意味します。

デフォルト

30 秒

wrapper.console.format

コンソール出力のフォーマット。

デフォルト

PM

wrapper.console.loglevel

コンソール出力のログ レベル。

デフォルト

INFO

wrapper.logfile

ラッパ出力ログ用に使用するログ ファイルの名前と場所。

デフォルト

./logs/EMService.log

wrapper.logfile.format

ログ ファイル出力用のフォーマット。

デフォルト

LPTM

wrapper.logfile.loglevel

ログ ファイル出力のログ レベル。

デフォルト

INFO

wrapper logfile.maxsize

ログがロールされるまでに増やすことが許されるログファイルの最大サイズ。サイズはバイト数で指定されます。**0**のデフォルト値は、ログロールを無効にします。**k**（キロバイト）または**m**（メガバイト）を後ろに付けることができます。たとえば、**10m = 10** メガバイトになります。

デフォルト

0

wrapper logfile.maxfiles

ロールされるログファイルの最大数。この最大数を超えると、古いファイルが削除されます。デフォルト値**0**は制限がないことを意味します。

デフォルト

0

wrapper syslog.loglevel

システムとイベントのログ出力のログレベル。

デフォルト

NONE

注

この設定ファイルを使用するアプリケーションをサービスとしてインストールするときに、以下のいずれの *ntservice* プロパティも変更しないでください。このセクションを変更する前に、サービスをアンインストールしてください。修正を行った後、サービスを再インストールできます。

wrapper.ntservice.name

サービスの名前。

デフォルト

IScopeEM

wrapper.ntservice.displayname

サービスの表示名。

デフォルト

Introscope Enterprise Manager

wrapper.ntservice.description

このサービスの説明。

デフォルト

Introscope Enterprise Manager

wrapper.ntservice.dependency.x

サービスの依存関係。依存関係を必要に応じて 1 から追加します。例：

- `wrapper.ntservice.dependency.1=`
- `wrapper.ntservice.dependency.2=`
- `wrapper.ntservice.dependency.3=`

wrapper.ntservice.starttype

サービスがインストールされるモード。設定には、`AUTO_START` または `DEMAND_START` があります。

デフォルト

AUTO_START

wrapper.ntservice.interactive

この値を *true* に設定すると、デスクトップと相互作用するサービスが開始されます。

デフォルト

false

Introscope Enterprise Manager.lax

Introscope Enterprise Manager.lax ファイルは、<EM_Home> ディレクトリにあります。このファイルで定義されるプロパティによって、Enterprise Manager のランタイム動作を制御します。

lax.application.name

Enterprise Manager 実行可能ファイルのデフォルトの名前

警告： 編集しないでください。

デフォルト

Introscope Enterprise Manager.exe

lax.class.path

このファイルを使用して設定するアプリケーションの実行に必要な Java クラスパス。

JDBC ドライバとライセンスを後に追加することができます。

これは、コロン (Mac OS/UNIX) またはセミコロン (Windows) で区切ることができます。

例

```
lax.class.path=launcher.jar;lax.jar
```

デフォルト

(空)

lax.command.line.args

このプロパティは、メインメソッドに渡されます。この値を入力するときには、スペース付きの引数を引用符で囲みます。例：

```
lax.command.line.args=$CMD_LINE_ARGUMENTS$ -consolelog -noExit -product  
com.wily.introscope.em.product -install ".¥¥product¥¥enterprisemanager"  
-configuration ".¥¥product¥¥enterprisemanager¥¥configuration"
```

デフォルト

(空)

lax.dir

LaunchAnywhere のネイティブのランチャを格納するディレクトリへのパス。

デフォルト

(空)

lax.main.class

アプリケーションのメインメソッドを含むクラス。

例

```
lax.main.class=org.eclipse.core.launcher.Main
```

デフォルト

main

lax.main.method

LaunchAnywhere の Java ランチャのメインメソッド。このプロパティでは、デフォルト値、*lax.nl.java.launcher.main.method=main* を変更しないでください。

デフォルト

main

lax.nl.current.vm

このプロパティは、Enterprise Manager の次回起動時に使用される仮想マシンを表します。インストール済みの JRE を使用するように設定できます。JVM バージョン要件の詳細については、「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。

例

バンドルされた JVM をこのプロパティに設定する場合、以下のように表示されます。

```
lax.nl.current.vm=jre¥¥bin¥¥java.exe
```

デフォルト

デフォルト値は、オペレーティング システムによって異なります。

lax.nl.java.launcher.main.class

LaunchAnywhere の java ランチャのメインクラス。このプロパティでは、デフォルト値、`lax.nl.java.launcher.main.class=com.zerog.lax.LAX` を変更しないでください。

デフォルト

```
com.zerog.lax.LAX
```

lax.nl.java.launcher.main.method

LaunchAnywhere の Java ランチャのメインメソッド。このプロパティでは、デフォルト値、`lax.nl.java.launcher.main.method=main` を変更しないでください。

デフォルト

```
main
```

lax.nl.java.option.additional

Java のオプションの引数 (ヒープ サイズなど)

例

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -Dosgi.clean=false
```

32 ビット Sun JVM の場合は、以下のスイッチが推奨されます。

```
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50 -XX:MaxPermSize=256m
```

例 :

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-showversion -XX:+UseConcMarkSweepGC -XX:+UseParNewGC  
-XX:CMSInitiatingOccupancyFraction=50
```

注: これらのスイッチは 32 ビットの Sun JVM 専用です : -showversion
-XX:+UseConcMarkSweepGC -XX:+UseParNewGC。

64 ビットのプラットフォームを使用している場合は、-Xss スwitchを
512k に設定します。

例 :

```
lax.nl.java.option.additional=-Xms512m -Xmx1024m  
-Djava.awt.headless=false -XX:MaxPermSize=256m  
-Dmail.mime.charset=UTF-8  
-Dorg.owasp.esapi.resources=./config/esapi -Xss512k
```

デフォルト

(空)

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list に示された仮想マシンが見つからなかった場合にユーザダイアログに表示されるメッセージ。このプロパティは、InstallAnywhere ランチャ専用です。Introscope には別の Java 要件があります。JVM 要件については、「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。

The *lax.nl.message.vm.not.loaded=LaunchAnywhere* either could not find a Java VM, or the Java VM on this system is too old.

(*lax.nl.message.vm.not.loaded=LaunchAnywhere* は Java VM を見つけることができないか、システムの Java VM が古すぎるかのいずれかです。)

LaunchAnywhere requires a Java 2 VM in order to launch Introscope.

(LaunchAnywhere では Introscope を起動するために、Java 2 VM が必要です。)

lax.nl.valid.vm.list

複数の [*ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ*] を含むストリングは、スペースまたはカンマで区切ります。ネイティブのランチャが現在の仮想マシンを見つけない場合、このリスト内で次の値を探します：*lax.nl.valid.vm.list=J2*。

デフォルト

J2

lax.nl.win32.microsoftvm.min.version

このランチャが実行される Microsoft の仮想マシンの最小バージョン。例：

lax.nl.win32.microsoftvm.min.version=2750

デフォルト

2750

lax.root.install.dir

installdir マジック フォルダへのパス。例：

lax.root.install.dir=.

デフォルト

(空)

lax.stderr.redirect

標準エラー出力。
以下のように設定します。

- 出力がない場合は空白
- コンソール ウィンドウに送信する場合は *console*
- ファイルに保存する場合はファイルへのパス

デフォルト

console

lax.stdin.redirect

以下のように設定します。

- 出力がない場合は空白
- コンソール ウィンドウに送信する場合は *console*
- ファイルに保存する場合はファイルへのパス

注

UNIX プラットフォームで、`nohup` モードで Enterprise Manager を実行している場合には、この設定は絶対に変更しないでください。変更すると、Enterprise Manager は起動できません。

ローカルの要件からこのプロパティを未指定にする必要がある場合には、必ず [introscope.enterprisemanager.disableInteractiveMode](#) (P. 487) を `true` に設定する必要があります。

デフォルト

`console`

lax.stdout.redirect

標準出力。

以下のように設定します。

- 出力がない場合は空白
- コンソール ウィンドウに送信する場合は *console*
- ファイルに保存する場合はファイルへのパス

デフォルト

`console`

lax.user.dir

このプロパティを空白のままで使用すると、ネイティブのランチャは、ユーザディレクトリを設定するためのプラットフォームのデフォルト動作を変更しません。
これを変更するには、このプロパティに相対パスか絶対パスを設定します。相対パスはランチャからの相対となります。

例

```
lax.user.dir=.
```

デフォルト

(空)

lax.version

プロパティファイルを作成した LaunchAnywhere のバージョン。例：
lax.version=<バージョン番号>

デフォルト

10.0

IntroscopeWorkstation.properties

このファイル内のプロパティによって、Workstation のさまざまな動作を制御します。

log4j.logger.Workstation

ログの詳細レベルとワークステーションのログの出力場所を制御します。

指定できる値の詳細度を以下に示します。

- *FATAL*
- *WARN*
- *INFO*
- *VERBOSE#com.wily.util.feedback.Log4JSeverityLevel*
(この値はログされる詳細のレベルを増大させます。)
- *DEBUG*
- *TRACE*

指定できる出力先の値は以下のとおりです。

- *console*
- *logfile*

デフォルト

INFO、*console*

log4j.appender.logfile.File

Workstation のログファイルの名前と場所。

デフォルト

IntroscopeWorkstation.log

introscope.workstation.graph.antialiased

これは、グラフの線や記号のアンチエイリアシングを制御します。この値を *false* に設定すると、アンチエイリアシングが無効になります。

デフォルト

true

transport.http.proxy.host

Workstation が HTTP を介してトンネルするホストを示す HTTP トンネルプロキシサーバのプロパティ。この方法を選択すると、プルキシサーバ（転送プロキシ）を通じて Enterprise Manager に接続する必要があります。指定したホストおよびポートを使用してプロキシサーバに到達できない場合、Workstation は Enterprise Manager への直接的な HTTP トンネル接続を試みた後で、接続が失敗します。

デフォルト

(空)

transport.http.proxy.port

Workstation が HTTP を介してトンネルするポートを示す HTTP トンネルプロキシサーバのプロパティ。この方法を選択すると、プルキシサーバ（転送プロキシ）を通じて Enterprise Manager に接続する必要があります。指定したホストおよびポートを使用してプロキシサーバに到達できない場合、Workstation は Enterprise Manager への直接的な HTTP トンネル接続を試みた後で、接続が失敗します。

デフォルト

(空)

transport.http.proxy.username

プロキシサーバが認証を必要とする場合のみ、このユーザ名が適用されます。その時点で、ユーザ名を表す値を入力することになります。

デフォルト

(空)

transport.http.proxy.password

プロキシサーバが認証を必要とする場合のみ、このパスワードが適用されます。その時点で、ユーザが入力する必要があるパスワードを表す値を入力することになります。

デフォルト

(空)

transport.tcp.truststore

SSLを設定する場合、このオプションのプロパティは信頼されている Enterprise Manager 証明書を含むトラストストアの場所を示します。この値は Workstation の絶対パスか、作業ディレクトリへの相対パスのいずれかです。

Windows では、円記号をエスケープする必要があります。例：

```
transport.tcp.truststore=C:\Introscope\config\internal\server\keystore
```

トラストストアを指定しないと、Workstation はすべての証明書を信頼します。

デフォルト

(空)

transport.tcp.trustpassword

トラストストアのパスワード

デフォルト

password

transport.tcp.truststore

Workstation の証明書を含むキーストアの場所です。絶対パスまたは Workstation の作業ディレクトリへの相対パス。Windows では、円記号をエスケープする必要があります。

例

```
..¥¥Introscope¥¥config¥¥internal¥¥server¥¥keystore
```

transport.tcp.keystore

キーストアの場所のプロパティ。これは、Enterprise Manager がクライアント認証を必要とする場合のみに必要です。

デフォルト

```
internal/server/keystore
```

transport.tcp.keypassword

キーストアのパスワード。

デフォルト

```
password
```

transport.tcp.ciphersuites

これをセットすると、暗号スイートのカンマ区切りのリストを使用する暗号スイートを有効にします。このプロパティを指定しない場合、デフォルトで有効にされた暗号スイートが使用されます。

デフォルト

(空)

注

このファイルは以下のプロパティを含みますが、通常の使用ではこれらを変更しないでください。

- log4j.additivity.Workstation=false
- log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender
- log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender
- log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout
- log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n
- log4j.appender.logfile.MaxBackupIndex=4
- log4j.appender.logfile.MaxFileSize=200MB

Introscope Workstation.lax

このファイルで定義されるプロパティによって、Workstation のさまざまな動作を制御します。

lax.application.name

重要: この実行ファイルの名前を編集しないことが重要です。

デフォルト

Introscope Workstation.exe

lax.class.path

このファイルを使用して設定するアプリケーションの実行に必要な Java クラスパス。これは、コロン (Mac OS/UNIX) またはセミコロン (Windows) で区切ることができます。

デフォルト

launcher.jar;lax.jar

lax.command.line.args

メインメソッドに渡すコマンドライン引数。このプロパティを定義すると、Workstation を起動するとき、ログイン画面を表示しなくても Workstation にログイン情報を渡すことができます。

デフォルト

\$CMD_LINE_ARGUMENTS\$

lax.dir

LaunchAnywhere のネイティブのランチャを格納するディレクトリへのパス。

デフォルト

(空)

lax.main.class

アプリケーションのメインメソッドを含むクラス。

デフォルト

org.eclipse.core.launcher.Main

lax.main.method

呼び出されるメインクラスのメソッド。

デフォルト

main

lax.nl.current.vm

WebView の次回起動時に使用する VM。インストール済みの JRE バージョンを指定できます。JVM バージョン要件の詳細については、「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。

デフォルト

オペレーティング システムによって異なります。

lax.nl.java.launcher.main.class

注

LaunchAnywhere の Java ランチャのメインクラスであるため、このプロパティを変更しないことが重要です。

デフォルト

com.zerog.lax.LAX

lax.nl.java.launcher.main.method

注

LaunchAnywhere の Java ランチャのメインクラスであるため、このプロパティを変更しないことが重要です。

デフォルト

main

lax.nl.java.option.additional

JVM 関連のその他のオプションの設定

最小ヒープ サイズと最大ヒープ サイズの初期値。

デフォルト

```
-client -Xms64m -Xmx256m -Dsun.java2d.noddraw=true
```

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list に示された仮想マシンが見つからなかった場合にユーザダイアログに表示されるメッセージ。

注

このプロパティは、InstallAnywhere ランチャ専用です。Introscope には別の Java 要件があります。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」の「システム要件」を参照してください。

デフォルト

LaunchAnywhere either could not find a Java VM, or the Java VM on this system is too old. (LaunchAnywhere は Java VM を見つけることができないか、このシステムの Java VM が古すぎます。) LaunchAnywhere requires a Java 2 VM in order to launch Introscope. (LaunchAnywhere では Introscope を起動するために、Java 2 VM が必要です。)

lax.nl.valid.vm.list

複数の [ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ] を含むストリングは、スペースまたはカンマで区切ります。ネイティブのランチャが現在の仮想マシンを見つけられない場合、このリストで定義されているものを探します。

デフォルト

J2

lax.nl.win32.microsoftvm.min.version

Microsoft 仮想マシンのランチャが動作する最小のバージョン。

デフォルト

2750

lax.root.install.dir

installdir マジック フォルダへのパス。

デフォルト

(空)

lax.stderr.redirect

標準エラー出力。

設定可能な値

- <空白> - 出力なし
- *console* - コンソール ウィンドウに出力を送信します。
- <ファイルのパス> - 指定されたファイルに出力を保存します。

デフォルト

(空)

lax.stdin.redirect

標準入力。

設定可能な値

- <空白> - 入力なし
- *console* - コンソール ウィンドウから読み取ります。
- <ファイルのパス> - 指定されたファイルから入力を読み取ります。

デフォルト

(空)

lax.stdout.redirect

標準出力。

設定可能な値

- <空白> - 出力なし
- *console* - コンソール ウィンドウに出力を送信します。
- <ファイルのパス> - 指定されたファイルに出力を保存します。

デフォルト

(空)

lax.user.dir

このプロパティを使用すると、ネイティブのランチャは、ユーザディレクトリを設定するためのプラットフォームのデフォルトの動作を変更しません。

これを変更するには、このプロパティに相対パスまたは絶対パスを設定します。ここでの相対パスとは、ランチャに対する相対パスです。

デフォルト

(空)

lax.version

このプロパティ ファイルを作成した **LaunchAnywhere** のバージョン。

デフォルト

9.0

IntroscopeWebView.properties

このファイルで定義されるプロパティによって、**WebView** のさまざまな動作を制御します。

introscope.webview.jetty.configurationFile

Jetty XML 設定ファイルへのパス。絶対パスまたは **config** ディレクトリへの相対パスのいずれか。このファイルは、**HTTPS** トラフィックのポート **8443** の **SSL** リスナーを作成します。

高度な **Jetty** 設定の場合、このプロパティのコメントを削除し、**Jetty** 設定ファイルの設定を変更します。

introscope.webview.tcp.port プロパティは **HTTP** リスナーを指定します。コメント化を解除すると、**HTTP** リスナーは作成されません。

デフォルト

webview-jetty-config.xml

introscope.webview.tcp.ipaddress

WebView を特定のローカル IP アドレスにバインドするための **WebView** **HTTP** サーバ設定プロパティ。これが設定されていないと、**WebView** はすべてのローカルアドレスの着信接続を受け付けます（ワイルドカードアドレス）。

デフォルト

(**WebView** マシンの有効な IP アドレスを設定)

introscope.webview.tcp.port

WebView の HTTP トラフィック リッスン ポート。

デフォルト

8080

introscope.webview.context.path

WebView のアプリケーション コンテキストパス。コンテキストパスは、WebView サーバの完全修飾ホスト名およびポート番号の末尾に追加され、WebView ルート (WebView にアクセスするための URL) を形成します。この機能を使用すると、ユーザが WebView のアプリケーション名を定義できます。

コンテキストパスが以下の場合

/webview

WebView にアクセスするための URL は以下のとおりです。

http://host:port/webview/

デフォルト

/

注: SAP 環境で WebView を使用している場合、デフォルトは */webview* です

introscope.webview.enterprisemanager.tcp.host

接続先の Enterprise Manager ホスト名

デフォルト

localhost

introscope.enterprisemanager.webview.disableLogin

WebView から Enterprise Manager への接続を確立できるようにするかどうかを指定します。

デフォルト

false

introscope.webview.enterprisemanager.tcp.port

接続先の Enterprise Manager ポート

デフォルト

5001

log4j.logger.WebView

WebView のログに記録する内容の詳細度。

指定できる値の詳細度を以下に示します。

- *INFO*
- *VERBOSE#com.wily.util.feedback.Log4JSeverityLevel*

指定できる出力先の値は以下のとおりです。

- *console*
- *logfile*

デフォルト

INFO、console

log4j.logger.WebServer

WebServer のログに記録する内容の詳細度。

指定できる値の詳細度を以下に示します。

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

指定できる出力先の値は以下のとおりです。

- *console*
- *logfile*

デフォルト

INFO、console

log4j.logger

サードパーティの **WebView** が使用するログ記録プロパティ。

指定できる値の詳細度を以下に示します。

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

指定できる出力先の値は以下のとおりです。

- *console*
- *logfile*

デフォルト

INFO、console

log4j.logger.com.wily

CA APM ログに記録する内容の詳細度。

指定できる値の詳細度を以下に示します。

- *INFO*
- *VERBOSE com.wily.util.feedback.Log4JSeverityLevel*

指定できる出力先の値は以下のとおりです。

- *console*
- *logfile*

デフォルト

INFO、console

log4j.logger.org.apache.myfaces

Apache Myfaces のログに記録する内容の詳細度。

ログファイルが上述のように指定されている場合、ログファイルの場所は、*log4j.appender.logfile.File* というプロパティで設定されます。適宜、完全パスが使用できます。

デフォルト

ERROR、console

log4j.logger.org.apache.jasper

Apache Jasper のログに記録する内容の詳細度。

ログファイルが上述のように指定されている場合、ログファイルの場所は、*log4j.appender.logfile.File* というプロパティで設定されます。適宜、完全パスが使用できます。

デフォルト

ERROR、console

log4j.logger.org.apache.struts

Apache Struts のログに記録する内容の詳細度。

ログ ファイルが上述のように指定されている場合、ログ ファイルの場所は、*log4j.appender.logfile.File* というプロパティで設定されます。適宜、完全パスが使用できます。

デフォルト

ERROR、console

log4j.logger.org.mortbay

Mortbay ログに記録する内容の詳細度。

ログ ファイルが上述のように指定されている場合、ログ ファイルの場所は、*log4j.appender.logfile.File* というプロパティで設定されます。適宜、完全パスが使用できます。

デフォルト

ERROR、console

ログ記録設定プロパティ

以下のプロパティは、通常の使用では変更しないでください。

- `log4j.additivity.WebView=false`
- `log4j.additivity.WebServer=false`
- `log4j.additivity.com.wily=false`
- `log4j.appender.console=com.wily.org.apache.log4j.ConsoleAppender`
- `log4j.appender.console.layout=com.wily.org.apache.log4j.PatternLayout`
- `log4j.appender.console.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n`
- `log4j.appender.logfile=com.wily.org.apache.log4j.RollingFileAppender`
- `log4j.appender.logfile.layout=com.wily.org.apache.log4j.PatternLayout`
- `log4j.appender.logfile.layout.ConversionPattern=%d{M/dd/yy hh:mm:ss a z} [%-3p] [%c] %m%n`
- `log4j.appender.logfile.MaxBackupIndex=4`
- `log4j.appender.logfile.MaxFileSize=200MB`

注

値が `true` に設定されている場合、グラフはアンチエイリアシングが有効になります（見やすく改善）。たとえば、`introscope.workstation.graph.antialiased=true`

デフォルト

デフォルト値はプロパティによって異なります。

`log4j.appender.console`

このプロパティは `WebView` プロパティ ファイルに追加され、コンソールにメッセージを出力します。

デフォルト

`logs/IntroscopeWebView.log`

log4j.appender.logfile

このプロパティは **WebView** プロパティファイルに追加され、ログファイルにメッセージを追加します。

デフォルト

`com.wily.org.apache.log4j.RollingFileAppender`

log4j.appender.logfile.File

WebView ログファイルの名前と、その **Enterprise Manager** のホームディレクトリを基準にした相対的な場所。

デフォルト

`logs/IntroscopeWebView.log`

Introscope WebView.lax

このファイルで定義されるプロパティによって、**WebView** のランタイム動作を制御します。

lax.application.name

WebView 実行可能ファイルのデフォルトの名前。

警告： 編集しないでください。

デフォルト

`Introscope_WebView.exe`

lax.class.path

このファイルを使用して設定するアプリケーションの実行に必要な Java クラスパス。

デフォルト

`lib/WebServices.jar:lib/IntroscopeClient.jar:lib/Workstation.jar:lib/WebViewAPI.jar:lib/WebViewServer.jar:lib/IntroscopeServices.jar`

lax.command.line.args

メインメソッドに渡すコマンドライン引数。このプロパティを定義すると、WebView を起動するとき、ログイン画面を表示しなくても WebView にログイン情報を渡すことができます。

デフォルト

`$CMD_LINE_ARGUMENTS$`

lax.dir

LaunchAnywhere のネイティブランチャが常駐するディレクトリへのパス。

デフォルト

(空)

lax.main.class

アプリケーションのメインメソッドを含むクラス。

デフォルト

`org.eclipse.core.launcher.Main`

lax.main.method

呼び出されるメインクラスのメソッド。

デフォルト

`main`

lax.nl.current.vm

WebView の次回起動時に使用する VM。インストール済みの JDK または JRE バージョンを指定できます。JVM バージョン要件の詳細については、「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。

デフォルト

オペレーティング システムによって異なります

lax.nl.java.launcher.main.class

LaunchAnywhere の java ランチャのメインクラス。

注

このプロパティを変更しないでください。

デフォルト

com.zerog.lax.LAX

lax.nl.java.launcher.main.method

LaunchAnywhere の java ランチャのメインメソッド。

注

このプロパティを変更しないでください。

デフォルト

main

lax.nl.java.option.additional

ヒープ サイズなど、JVM のオプションの設定。

デフォルト

-Xms128m -Xmx512m -Djava.awt.headless=false -Dsun.java2d.noddraw=true

lax.nl.message.vm.not.loaded

lax.nl.valid.vm.list の VM が見つからない場合に、ダイアログに表示されるメッセージ

注

このプロパティは、InstallAnywhere ランチャ専用です。Introscope には別の Java 要件があります。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」の「システム要件」を参照してください。

デフォルト

該当なし

lax.nl.valid.vm.list

複数の [ALL JDK JRE J1 J2 JRE_J1 JDK_J1 JRE_J2 JDK_J2 MSJ] を含むストリングは、スペースまたはカンマで区切ります。ネイティブのランチャが現在の仮想マシンを見つけられない場合、このリストで定義されているものを探します。

デフォルト

J2

lax.nl.win32.microsoftvm.min.version

このアプリケーションが実行される Microsoft の VM の最小バージョン。

デフォルト

2750

lax.root.installation.dir

installdir マジック フォルダへのパス。

デフォルト

(空)

lax.stderr.redirect

標準出力。

設定可能な値

- <空白> - 出力なし
- *console* - コンソール ウィンドウに出力を送信します。
- <ファイルのパス> - 指定されたファイルに出力を保存します。

デフォルト

console

lax.stdin.redirect

標準入力。

設定可能な値

- <空白> - 入力なし
- *console* - コンソール ウィンドウから読み取ります。
- <ファイルのパス> - 指定されたファイルから入力を読み取ります。

デフォルト

console

lax.stdout.redirect

標準出力。

設定可能な値

- <空白> - 出力なし
- *console* - コンソール ウィンドウに出力を送信します。
- <ファイルのパス> - 指定されたファイルに出力を保存します。

デフォルト

console

lax.user.dir

このプロパティは、ネイティブのランチャがユーザディレクトリを設定するためのプラットフォームのデフォルト動作を変更しないようにさせるため、空白のままにします。この動作を変更するには、このプロパティに相対パスまたは絶対パスを設定します。ここでの相対パスとは、ランチャに対する相対パスです。

デフォルト

(空)

lax.version

このプロパティ ファイルを作成した **LaunchAnywhere** のバージョン。

デフォルト

9.0

APMCloudMonitor.properties

APMCloudMonitor.properties ファイル内のプロパティを使用して、**CA APM Cloud Monitor** の動作を制御し、**CA APM Cloud Monitor** エージェントが **Enterprise Manager** に送信するデータをフィルタできます。

CA APM Cloud Monitor エージェント インストーラは、デフォルトでは以下の場所にこのファイルをインストールします。

<CloudMonitor_Agent_Home>/CloudMon/conf/APMCloudMonitor.properties

apmcm.folders.include

Enterprise Manager にデータを送信する CA APM Cloud Monitor フォルダを定義します。

デフォルト

コメント化されています

設定可能な値

- ALL
- 1つ以上のフォルダ名のリスト

形式

カンマ区切りのリスト

例

folder0,folder1,folder two,folder3

apmcm.monitors.include

Enterprise Manager にデータを送信する CA APM Cloud Monitor の監視を定義します。

デフォルト

コメント化されています

設定可能な値

- ALL
- 監視のカンマ区切りのリスト

例

monitor0,monitor1,monitor two,monitor3

apmcm.checkpoints.include

テストクエリを送信する CA APM Cloud Monitor チェックポイント（監視サイト）を定義します。

デフォルト

コメント化されています

設定可能な値

- ALL
- 1つ以上のチェックポイント名のリスト

形式

カンマ区切りのリスト

例

gr,uk,f2,mb,it,nl

注: [製品] - [監視ステーション] を選択することにより、チェックポイントの省略形の一覧を確認できます。

apmcm.include.inactive.monitors

非アクティブの CA APM Cloud Monitor の監視が Enterprise Manager にデータを送信するかどうかを定義します。

デフォルト

False

設定可能な値

- false
- true

apmcm.folder.metrics.include

エージェントが Enterprise Manager に送信する CA APM Cloud Monitor フォルダ メトリックを定義します。

デフォルト

コメント化されています

設定可能な値

properties ファイルのプロープのリストを参照してください。

形式

カンマ区切りのリスト

例

```
probes,probe_errors,checks,check_errors,uptime,ttime,ctime,ptime,dtime,dsizesize
```

apmcm.monitor.psp.metrics.include

メトリックを返す CA APM Cloud Monitor のパブリック ステータス ページを定義します。

デフォルト

```
color,errors,avg_uptime_cur,avg_uptime_day,avg_perf_cur,avg_perf_day
```

設定可能な値

properties ファイルのページのリストを参照してください。

形式

カンマ区切りのリスト

例

```
color,errors,avg_uptime_cur
```

apmcm.monitor.checkpoint.metrics.include

CA APM Cloud Monitor エージェントによって Enterprise Manager に送信される CA APM Cloud Monitor チェックポイント メトリックを定義します。

デフォルト

runtime,ctime,ptime,ttime,dtime,descry

設定可能な値

properties ファイルのメトリックのリストを参照してください。

形式

カンマ区切りのリスト

例

runtime,ctime,ptime

apmcm.force.global.update

デフォルトでは、CA APM Cloud Monitor エージェントは、以下のメタデータに対する変更を 3600 秒ごとにチェックします。

- 再ログイン
- 監視のリストの更新
- フォルダのリストの更新
- チェックポイントのリストの更新

これらのメタデータに対する変更や更新を即座にチェックすることをエージェントに強制する場合は、デフォルト値をほかの整数に変更します。

注: このプロパティの値は何も示しません。これは、その値が現在値以外の任意の値に変更されると、説明したとおりにメタデータのチェックを強制するメタデータです。

デフォルト値

1

設定可能な値

任意の整数

apmcm.log.adjustment

CA APM Cloud Monitor エージェントがログから取得するレコードの最大数。

エージェントはログにメトリックのクエリを実行するごとに、最後の項目を確認します。ログ項目の例を以下に示します。

```
[CloudMonitorIntegration.CloudMonitorAgent] Log record found with  
k=4/21
```

分母（この例では 21）はエージェントがログから 1 分ごとに取得できる項目の最大数であり、分子（この例では 4）は直近の 1 分間に実際に取得されたレコードの数です。

$k > 1$ になると、以下のメッセージがログに記録されます。

```
Some probe data may be missing. Automatically adjusting monitor log  
query. Please consider increasing apmcm.log.adjustment property.
```

このメッセージが示す自動調整は、エージェントが `apmcm.log.adjustment` の値を取得し、それを分母に追加することを意味します。したがって、`apmcm.log.adjustment = 1` を設定すると、取得される項目の最大数は 22 に変更されます。次に $k > 1$ になったとき、分母は、1 ずつ増えていきます。

デフォルト

0

設定可能な値

任意の整数

その他

このプロパティはホット設定可能です。このプロパティを変更した場合、変更を有効にするために Enterprise Manager を再起動する必要はありません。

付録 B: JDBC API

Introscope には、Introscope のデータを表示するために Excel または SAS などのデータ分析ツールを使用できるようにする API が含まれます。JDBC インターフェースを使用して、履歴範囲に対するメトリック データおよびイベントデータを抽出できます。データは、表のメタデータを記述する XML 文字列を含む単一の列を持つ表形式で返され、結果の表が含まれています。

このセクションには、以下のトピックが含まれています。

[JDBC API の設定](#) (P. 615)

[JDBC API の使用](#) (P. 615)

JDBC API の設定

ファイル *IntroscopeJDBC.jar* には、JDBC ドライバクラスおよびドライバが必要とするすべてのクラスが含まれています。これはクライアントアプリケーションのクラスパスに必要とされる唯一のファイルです。

ドライバクラスは、*com.wily.introscope.jdbc.IntroscopeDriver* です。

URL のフォーマットは以下のようになります(大文字/小文字の区別が重要です)。

```
jdbc:introscope:net://{username}:{password}@{host}:{em port}
```

例 :

```
jdbc:introscope:net//Admin:@localhost:5001
```

JDBC API の使用

Introscope JDBC API の構文は以下の仮想ビューをサポートします。

- `metric_data`
- `trace_headers`
- `traces`

メトリック クエリ

メトリックを実行すると、クエリでは、Introscope JDBC ドライバによってサポートされている、以下の日付形式のいずれかが使用されます。

- *mm/dd/yy hh:mm:ss*
- *EEE MMM dd HH:mm:ss zzz yyyy*

たとえば、メトリック クエリは以下ようになります。

```
select * from metric_data where agent={正規表現} and metric={正規表現} and
timestamp between {開始時刻} and {終了時刻}
```

または

```
select * from metric_data where agent='.*Custom Metric Host.*' and metric='.*'
and timestamp between '01/01/01 00:00:00' and '01/01/07 00:00:00'
```

修飾子は SQL ステートメントの中で以下の順序で記述する必要があります。

```
[sort by value {ascending|descending}] [maxmatches={max metrics}]
[period={period in seconds}] [aggregateall]
```

注: シャットダウンしているエージェントに JDBC ドライバを使用してクエリを実行すると、「0」が返されます。

以下の修飾子は Enterprise Manager のメトリック集約機能をサポートしています。

| 修飾子名 | 機能の内容 |
|----------------------------|--|
| <i>sort by value {a/d}</i> | Enterprise Manager が各タイムスライスのメトリック値に対して昇順または降順の <i>N</i> ソートを行うようにフラグを設定します。 <i>maxmatches</i> フラグと共にこの修飾子を使用すると、トップ <i>N</i> 個の一致だけにメトリック制限を指定できます。 |
| <i>maxmatches</i> | Enterprise Manager がここで指定した数を上限とするメトリックに対するデータのみを返すようにフラグを設定します。たとえば、 <i>maxmatches=2</i> の場合、2 つのメトリックのデータのみが返されます。 これは、返される行数を制限する sql の <i>limit</i> キーワードとは異なります。 <i>maxmatches=2</i> の例では、2 つのメトリックに対して 50 タイムスライス、つまり合計で 100 行のデータが返されます。 |
| <i>period</i> | Enterprise Manager がデータ ポイントを指定した期間に集約するようにフラグを設定します。たとえば、Enterprise Manager は通常 15 秒のデータ値をレポートしますが、 <i>period=60</i> の場合は 60 秒に集約できます。 |

aggregateall

Enterprise Manager が全メトリックデータを 1 つの要約されたタイムスライスに集約するようにフラグを設定します。たとえば、この修飾子を使用して、1 週間にわたる期間のメトリックに単一の平均応答時間を与えることができます。

aggregateall を *period* 修飾子と共に使用することは避けてください。いずれも集約を行うので、競合が発生します。

メトリック クエリの例

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' maxmatches=10
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' maxmatches=1
```

```
select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' maxmatches=1 period=120
```

```
// match one metric_data and aggregate all values. This returns one row of data select * from metrics where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' maxmatches=1 aggregateall
```

```
// this is a top 10 query select * from metric_data where agent='.*' and metric='.*Average Response.*' and timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' sort by value d maxmatches=10
```

トランザクション追跡クエリ

基本的なトランザクションヘッダクエリの構文は以下のとおりです。

```
select * from trace_headers where timestamp between {starttime} and {endtime} and query={lucene query string} [limit {rows}]
```

lucene query string は、Workstation の履歴クエリにあるような、有効な Lucene クエリ文字列です（詳細については、「CA APM Workstation ユーザガイド」を参照）。

オプションの *limit* フラグは、クエリが返す行数を制限します。制限が指定されない場合、サーバで定義されているデフォルトのトランザクション制限が使用されます。

追跡本体に対するクエリは同一ですが、異なるビューを参照します。

```
select * from traces where timestamp between {starttime} and {endtime} and query={lucene query string} [limit {rows}]
```

トランザクション追跡クエリの例

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' and query='s*'
```

```
select * from trace_headers where timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' and query='host:blink*'
```

```
select * from traces where timestamp between '01/01/01 00:00:00' and '07/01/01 00:00:00' and query='host:blink*' limit 100
```

追跡クエリが返したデータ行には、ドメイン、ホスト、プロセスとエージェントの名前、およびトランザクション追跡の XML 表現などのエージェント情報が含まれます。

付録 C: Introscope 拡張機能の構成

インストール時に Introscope 拡張機能を有効にした場合は、それらを設定する必要があります。インストールの詳細については、「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。

このセクションには、以下のトピックが含まれています。

[SNMP アダプタの構成 \(P. 619\)](#)

[Introscope アラート Web サービス拡張機能の構成 \(P. 630\)](#)

SNMP アダプタの構成

SNMP (Simple Network Management Protocol、簡易ネットワーク管理プロトコル) は、ネットワーク コンポーネントの監視と管理に使用される標準プロトコルです。SNMP アダプタを使用すると、Introscope で外部 SNMP フレームワークにメトリックをレポートできるようになります。SNMP アダプタの一般情報については、「CA APM Workstation ユーザガイド」を参照してください。

SNMP アダプタの制限事項

SNMP マネージャで Introscope 固有のメトリックを読み取れるのは、すべてのネットワーク コンポーネントを一元監視するうえで便利です。ただし、Introscope の SNMP 機能には以下の制限事項があることに注意してください。

- Introscope メトリックのみが SNMP マネージャで表示可能です。
- アラートやアクションなど、ほかの Introscope 機能は、Introscope 固有の情報の一部として発行されません。
- Introscope の情報は読み取り専用です。
- 「Set」はサポートされていません。

SNMP アダプタのコンポーネント

SNMP アダプタのコンポーネントを以下に示します。

SNMP コレクション

SNMP コレクションは、MIB ファイルに発行されるメトリックを定義する Introscope エlement です。SNMP コレクションは、管理モジュールに保存されます。

MIB ファイル(管理情報ベース)

MIB は、SNMP エージェントからレポートされる情報を記述したテキストファイルです。MIB ファイルは SNMP マネージャにロードできます。これにより、マネージャは、SNMP エージェントがレポートできる情報を把握します。

Introscope が生成する MIB ファイルは、現在アクティブな SNMP コレクションの、ある時点でのスナップショットであり、照合する Introscope メトリックを SNMP 準拠の形式で記述しています。

SNMP エージェント

Introscope SNMP エージェントは、Enterprise Manager のデプロイごとに 1 つインストールされています。SNMP エージェントは、Enterprise Manager から Introscope 固有のメトリックデータを収集して、SNMP 固有の形式に変換し、SNMP マネージャに送信します。

アラート通知

アラートがトリガされて、SNMP 通知アクションが発生すると、SNMP アダプタにより SNMP 通知 (トラップ) が送信されます。この通知には、Enterprise Manager のプロパティファイルに指定された設定済みの SNMP マネージャへのアラートが記述されています。

アラート

Enterprise Manager は次に、アラートに SNMP 通知アクションが設定されている場合にそのアラートがトリガされると、設定済みの SNMP マネージャに SNMP 通知（トラップ）を送信します。アラートメッセージを保持する通知の値オブジェクトのタイプは、オクテット文字列です。内容は、コンソール通知アクションと同じです。

これらの SNMP オブジェクトは、自動的に MIB で発行されます。

通知には、以下に示すような、固定の OID（一意のオブジェクト ID）が使用されます。xxxx は、ランダムに選択された SnmpAdapter 識別子です（例 5527）。

通知(数値形式)

値 : 1.3.6.1.4.1.10480.1.1.xxxx.5000

通知(名前形式)

値 :
iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapterxxxx.wilyAlertNotif

アラート(数値形式)

値 : 1.3.6.1.4.1.10480.1.1.xxxx.6000

アラートメッセージ(名前形式)

値 :
iso.org.dod.internet.private.enterprises.wily.products.introscope.snmpAdapterxxxx.wilyAlertNotifMessage

通知とアラートの設定

通知(トラップ)を設定する方法

- *IntroscopeEnterpriseManager.properties* を編集して、以下のプロパティを設定します。

introscope.agent.enterprisemanager.snmp.target.port

SNMP マネージャのポート

デフォルト

162

introscope.agent.enterprisemanager.snmp.target.destination

SNMP マネージャのホスト名または IP アドレス

デフォルト

localhost

introscope.agent.enterprisemanager.snmp.target.community

SNMP マネージャの SNMPv2 コミュニティ

デフォルト

public

introscope.enterprisemanager.snmp.notification.enable

通知のオン (*true*) またはオフ (*false*)

デフォルト

true

注

snmp.notification.enable プロパティはホット設定でサポートされているため、このプロパティの設定後に **Enterprise Manager** を再起動する必要はありません。その他のプロパティを有効にするには、**Enterprise Manager** を再起動する必要があります。

アラートおよび SNMP 通知アクションも **Workstation/Enterprise Manager** で設定できます。詳細については、「**CA APM Workstation ユーザガイド**」および本ガイド内の各種トピックを参照してください。

SNMP 機能の構成

Introscope 固有のメトリックを SNMP フレームワークで表示可能にするには、以下のタスクを実施します。

- Enterprise Manager のプロパティ ファイルで SNMP を有効にします。「[プロパティの設定による SNMP の有効化 \(P. 623\)](#)」を参照してください。
- SNMP コレクションを作成します。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。
- MIB を発行します。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。
- SNMP マネージャに MIB をロードします。「[SNMP フレームワークへの MIB ファイルのロード \(P. 624\)](#)」を参照してください。

プロパティの設定による SNMP の有効化

SNMP を有効にするには、ファイル *IntroscopeEnterpriseManager.properties* で 2 つのプロパティを設定します。

項目を設定する方法

1. Enterprise Manager が動作している場合はシャットダウンします。
2. ファイル `<EM_Home>/config/IntroscopeEnterpriseManager.properties` を開きます。
3. プロパティ `introscope.enterprisemanager.snmp.enable` で、値 `true` を入力します。
4. プロパティ `introscope.enterprisemanager.snmp.agent.port` で、デフォルト値の `161` にします。

注: UNIX プラットフォームを使用している場合、1000 未満のポート (SNMP エージェントのデフォルトポートは 161) を使用するには、root でログインするか、root 権限を持っている必要があります。

1. 変更を保存します。
2. Enterprise Manager を再起動します。

MIB ファイルについて

MIB ファイルは、ホスト名に従って名前付けされて、以下のディレクトリに保存されます。

`<EM_Home>/snmp/`

MIB ファイルは、以下の構文に従って名前を付けられて発行されます。

- HP LoadRunner: Introscope-<ホスト名>.lr.mib
- HP OpenView : Introscope-<ホスト名>.mib
- BMC Patrol
 - Introscope-<ホスト名>.bmc.mib
 - Introscope-<ホスト名>.bmc.smi
- その他 : Introscope-<ホスト名>.other.mib

ホスト名の無効な文字は削除されます。ホスト名のピリオドはダッシュに変換されます。

SNMP フレームワークへの MIB ファイルのロード

SNMP エージェントから利用可能なメトリックを識別するために、SNMP マネージャには MIB のコピーが必要です。MIB を発行したら、SNMP マネージャにその MIB をロードする必要があります。

以下のような場合に、SNMP マネージャに MIB ファイルをアップロードする必要があります。

- 新しい MIB を発行した場合
- Enterprise Manager またはマネージドアプリケーションを別のホストに移動した場合

Introscope が生成した MIB を SNMP フレームワークで使用するには、使用している SNMP フレームワークのマニュアルを参照して、MIB の作成方法を確認してください。サポートが必要な場合は、CA Technologies プロフェッショナル サービスにお問い合わせください。

HP LoadRunner へのアップロード

以下の情報は、このマニュアル発行時点で最新のものであります。最新情報については HP にお問い合わせください。

Introscope によって生成された MIB ファイルを HP LoadRunner にアップロードする方法

1. 以下の手順に従って、SNMP アダプタをインストールします。
 - a. *SNMPAdapter.jar* を `<EM_Home>/product/enterprisemanager/plugins` にコピーします。
 - b. *IntroscopeEnterpriseManager.properties* ファイル (`<EM_Home>/config/`にあります) を編集して、以下のプロパティを設定します。

```
introscope.enterprisemanager.snmp.enable=true
```
2. Enterprise Manager を再起動します。
3. SNMP コレクションを作成します。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。
4. 以下の手順に従って、MIB ファイルを発行します。
 - a. Introscope Investigator で管理モジュールエディタを開いていない場合は、[ファイル] - [新規管理モジュールエディタ] を選択して、管理モジュールエディタを起動します。
 - b. [マネージャ] - [MIB を発行...] をクリックして、MIB ファイルを発行します。
 - c. LoadRunner を選択します。
 - d. [発行] をクリックします。
5. 以下の手順に従って、MIB ファイルをコピーします。
 - コピー元: `<EM_Home>/snmp`
 - コピー先: SiteScope の `<SiteScope>/templates.mib`
6. SiteScope Windows サービスを再起動します。

7. SiteScope SNMP ブラウザを使用して、以下の手順に従って、MIB ファイルがロードされたことを確認します。
 - a. [スタート] - [プログラム] - [HP SiteScope] - [Open HP SiteScope LR] を選択します。
 - b. [Open SiteScope] をクリックします。
 - c. [Monitors] タブを開きます。
 - d. [SiteScope] - [Tools] - [SNMP Browser] を選択します。
 - e. Enterprise Manager のホスト名、バージョン V2 を入力します。
 - f. MIB ファイルを選択します。
 - g. [Browse] をクリックします。
8. 以下の手順に従って、測定値を追加します。
 - a. LoadRunner Controller を起動します。 [スタート] - [プログラム] - [HP LoadRunner] - [Applications] - [Controller] を選択します。
 - b. マニュアル シナリオを作成します。
 - c. [Scenario] ウィンドウで、 [Run] タブをクリックします。
 - d. [Available Graphs] - [System Resource Graphs] リストで、 [SNMP] をダブルクリックします。
 - e. [SNMP Graph] を選択します。
 - f. [Monitors] - [Add Measurements] をクリックします。
9. SNMP ダイアログ ボックスで、以下の手順を実行します。
 - a. [詳細設定] をクリックします。
 - b. [SiteScope] を選択し、 [OK] をクリックします。
 - c. [Add] をクリックして、新しい監視対象サーバマシンを追加します。
 - d. Enterprise Manager ホストを監視対象サーバとして設定して、 [OK] をクリックします。
 - e. [Add] をクリックして、リソース測定値を追加します。
 - f. [Server] が Enterprise Manager のマシン名になっていることを確認します。

- g. SNMP バージョンを V2 に変更します。
 - h. [Update Every...] の値を大きくします。設定値が小さすぎると、HP LoadRunner でエラーが発生する場合があります。
10. ツリーを展開して、目的の OID (メトリック) を選択します。
 11. HP LoadRunner でデータを確認します。

注:

HP LoadRunner を使用する場合は、以下の点に注意してください。

- 発行されたデータを表示するには、HP LoadRunner SNMP Monitor が必要です。
- SiteScope SNMP ブラウザに MIB が表示されない場合は、エラー ログ ファイルを確認してください。
- HP LoadRunner では、MIB 内のいずれのノードでも同じ名前を使用できないため、MIB 内の同じ名前のメトリックには、番号が追加されて表示されます。例：
fileInputRateBytesPerSecond23
- HP LoadRunner では負の数はグラフに表示されません。

HP OpenView へのアップロード

Introscope によって生成された MIB ファイルを HP OpenView にアップロードする方法

1. 以下の手順に従って、SNMP アダプタをインストールします。
 - a. *SNMPAdapter.jar* を <EM_Home>/product/enterprisemanager/plugins にコピーします。
 - b. *IntroscopeEnterpriseManager.properties* ファイル (<EM_Home>/config/にあります) を編集して、以下のプロパティを設定します。
introscope.enterprisemanager.snmp.enable=true
2. Enterprise Manager を再起動します。
3. SNMP コレクションを作成します。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。

4. 以下の手順に従って、MIB ファイルを発行します。
 - a. Introscope Investigator で管理モジュール エディタを開いていない場合は、[ファイル] - [新規管理モジュールエディタ] を選択して、管理モジュールエディタを起動します。
 - b. [マネージャ] - [MIB を発行...] をクリックして、MIB ファイルを発行します。
 - c. HP OpenView を選択します。
 - d. [発行] をクリックします。
5. 以下の手順に従って、MIB ファイルをコピーします。
 - コピー元 : <EM_Home>/snmp
 - コピー先 : HP OpenView がインストールされているマシン
6. HP OpenView マシンで、[スタート] - [プログラム] - [HP OpenView] - [Network Node Manager Admin] - [Network Node Manager] を選択します。
7. ルート コンソールで、[Settings] - [Load] を選択します。
8. [Unload the .mibs] の下で、SNMP を選択します。
9. [Load] をクリックします。
10. Introscope MIB ファイルを選択します。

ファイル名には、MIB ファイルを生成した Enterprise Manager の名前が含まれます。
11. アップロードが完了したら、[Close] をクリックします。
12. MIB ブラウザを開きます。[Tools] - [SNMP] を選択します。
 - a. [Name or Address] フィールドに、Enterprise Manager のホスト名を入力します。

この名前は、Introscope から参照される MIB ファイルの名前に使用されるホスト名と同じです。
 - b. [Community Name] フィールドに、「public」と入力します。
 - c. 以下のようにノードを展開します。

[iso] - [org] - [dod] - [private] - [enterprises] - [wily] - [products] - [introscope] - [snmpAdapter] - [hostname]

メトリックをグラフに表示するには、以下の手順に従います。

1. メトリックを選択します。
2. [Graph] をクリックします。

MIB でメトリックを検索するには、以下の手順に従います。

1. MIB でホスト名、エージェント名、リソース名を選択します。
2. [Start Query] をクリックします。

Introscope メトリックから SNMP メトリックへの変換

Introscope では、Introscope メトリック タイプと Introscope メトリック名の両方を SNMP 準拠の情報に変換します。

メトリック タイプの変換

SNMP エージェントは、Introscope メトリックを、以下に示すような SMIV2 メトリック タイプに変換します。

| Introscope メトリック タイプ | 汎用 MIB SMIV2 メトリック タイプ | HP OpenView または LoadRunner MIB SMIV2 メトリック タイプ | BMC MIB SMIV2 メトリック タイプ |
|----------------------|-------------------------------------|--|-------------------------------------|
| Int | INTEGER32(-2147483648...2147483647) | INTEGER32(-2147483648...2147483647) | COUNTER32(-2147483648...2147483647) |
| Long | INTEGER32 (同上) | INTEGER32 (同上) | COUNTER32 (同上) |
| String | OCTETSTRING | OCTETSTRING | OCTETSTRING |

SNMP では、32 ビットを超える整数はサポートされていません。Long は、以下のアルゴリズムを使用して 32 ビット整数に変換されます。

- Long が Integer.MAX_VALUE よりも大きい場合は、Integer.MAX_VALUE に設定されます。
- Long が Integer.MIN_VALUE よりも小さい場合は、Integer.MIN_VALUE に設定されます。
- その他の場合は、単純に Int にキャストされます。

メトリック名の変換

SNMP エージェントでは、以下のルールを使用して Introscope メトリック名のセグメントを MIB 識別子に変換します。

1. セグメントには有効な文字 (A-Z|a-z|-|0-9) のみ使用できます。セグメントにある無効な文字は削除されます。
2. 各セグメントの先頭文字は小文字である必要があります。セグメントの先頭文字が大文字の場合は、小文字に変換されます。セグメントの先頭が数字の場合は、数字の前に「a」が追加されます。
3. セグメントの終わりにハイフンは使用できません。終わりのハイフンは削除されます。
4. セグメントにハイフンを 2 つ連続して使用できません。一方のハイフンは削除されます。

セグメントは 64 文字以下である必要があります。セグメントが 64 文字を超える場合は、64 文字に切り捨てられます。切り捨てた結果、同じセグメントになった場合は、セグメントがさらに切り捨てられて、ダッシュと数字が追加されます (例 -2)。

Introscope アラート Web サービス拡張機能の構成

Introscope では、サードパーティ アプリケーションの使用時に CA Introscope をアラートおよびメトリックのソースとして使用できるよう、CA APM Web サービス API を提供しています。サードパーティ アプリケーションで CA Introscope アラートを使用できるように構成するには、CA Introscope アラート Web サービス拡張機能を構成します。

以下のプロパティは、IntroscopeEnterpriseManager.properties には表示されません。これらを設定するには、ファイル内に手動で追加する必要があります。

Enterprise Manager と共にインストールされる Web サービス ファイルの詳細については、「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。

Introscope アラート Web サービス拡張機能の構成方法

1. *IntroscopeEnterpriseManager.properties* ファイルを開きます。
<EM_Home>/config ディレクトリ内にあります。
2. *introscope.alerts.extension.managementmodules.enable* プロパティを追加し、アラートの提供元の管理モジュールをリスト表示します。プロパティ値を空のままにするか、「ALL」を指定すると、CA Introscope はすべての管理モジュールからのアラートを提供します。
3. プロパティ *introscope.alerts.extension.inventory.updatecheckintervalsecs* を追加します。このプロパティによって、アラート拡張機能がアラートを確認する頻度を秒単位で指定します。値を指定しない場合、デフォルトで 60 秒ごとに確認します。15 秒未満の値を指定することはできません。15 秒未満を指定すると、デフォルトの 15 秒に設定されます。

上記の時間間隔中に、エージェントの追加、エージェントの削除、または管理モジュールへの変更の保存を実行すると、CA Introscope によって、エージェントと管理モジュールに対して内部インベントリの確認が実行されます。Introscope は、アラートステータスの変更を処理する前にインベントリを更新します。

4. プロパティファイルの変更を有効にするために、Enterprise Manager を再起動します。

付録 D: デフォルトの `tess-default.properties` ファイル

`tess-default.properties` ファイルには、変更されることがほとんどない各種プロパティが含まれています。これらのプロパティの変更は、経験豊富な CA CEM 管理者のみが行うか、または CA サポートからの指示があった場合にのみ行ってください。

このセクションには、以下のトピックが含まれています。

- [tess-default.properties プロパティ デフォルト ファイルの変更 \(P. 633\)](#)
- [エビデンス コレクションの Perl パスまたは Python パスの設定 \(P. 634\)](#)
- [\[その他障害情報\] リンクのディレクトリ パスの設定 \(P. 636\)](#)
- [障害処理のパフォーマンスの向上 \(P. 638\)](#)
- [不正なファイルのディレクトリの場所の変更 \(P. 640\)](#)
- [その他の CA CEM デフォルト プロパティ \(P. 642\)](#)

tess-default.properties プロパティ デフォルト ファイルの変更

CA CEM `tess-default.properties` ファイルは `<EM_Home>/config` ディレクトリにあります。

重要: デフォルト プロパティのいずれかを編集する必要がある場合は、ファイルの専用バージョンを作成し、以下の名前を付ける必要があります。
`tess-customer.properties`

`tess-customer.properties` という専用のプロパティ ファイルを作成することにより、それ以降の CA CEM ソフトウェアのアップグレード時にプロパティの変更を確実に適用することができます。

警告: クラスタ化された環境では、`tess-customer.properties` ファイルを作成または編集した後で、このファイルを各 Enterprise Manager にコピーする必要があります。

それぞれの Enterprise Manager に *tess-default.properties* ファイルがあります。Enterprise Manager がそのローカルファイルから読み取るプロパティは、その Enterprise Manager 上で実行されているサービスによって異なります。たとえば、カスタマエクスペリエンスメトリックに関連するプロパティは、TIM コレクションサービスを実行している Enterprise Manager から読み取られ、ユーザグループの最大数に関連するプロパティは、Manager of Managers から読み取られます。

以下の手順に従います。

1. ファイルを見つけます。
`<EM_Home>/config/tess-default.properties`
2. 同じディレクトリに *tess-default.properties* ファイルの専用バージョンを作成し、*tess-customer.properties* という名前を付けます。
3. この *tess-customer.properties* ファイルを変更し、CA CEM 環境に合わせて変更する必要があるプロパティのみを追加します。

- a. 新しいプロパティ ファイルを編集します。

たとえば、vi エディタを使用します。

```
vi tess-customer.properties
```

重要: *tess-customer.properties* ファイルには、CA CEM システムのデフォルトとは異なる値を持つプロパティのみを格納してください。

tess-customer.properties ファイルにすべてのプロパティを残しておく、システムをアップグレードしたときに、今後のシステムパフォーマンスやプロパティのチューニング更新を生かすことができない可能性があります。

- b. *tess-customer.properties* ファイルを保存します。
4. *tess-customer.properties* ファイルを、クラスタ内のすべての Enterprise Manager にコピーします。
 5. クラスタ内の各 Enterprise Manager を再起動します

エビデンス コレクションの Perl パスまたは Python パスの設定

エビデンス コレクションを使用するには（「[ビジネスインパクトの設定およびインシデントエビデンスの収集](#) (P. 335)」）、MOM またはスタンドアロンの Enterprise Manager に Python または Perl をインストールしておく必要があります。python.path プロパティまたは perl.path プロパティを編集して、Python または Perl の場所を指定します。

perl.path

Perl がインストールされているディレクトリ。

オプション

Perl 実行可能ファイルへのディレクトリ パス

デフォルト

/usr/bin/perl

例

C:¥¥perl¥¥bin¥¥perl.exe

注

Windows プラットフォームで円記号を使用する場合、1 つの円記号 (¥) はエスケープシーケンスとして解釈されるため、二重の円記号 (¥¥) にする必要があります。

python.path

Python がインストールされているディレクトリ。

オプション

Python 実行可能ファイルへのディレクトリ パス

デフォルト

/usr/bin/python

例

C:¥¥python¥¥bin¥¥python.exe

注

Windows プラットフォームで円記号を使用する場合、1 つの円記号 (¥) はエスケープシーケンスとして解釈されるため、二重の円記号 (¥¥) にする必要があります。

[その他障害情報]リンクのディレクトリパスの設定

[その他障害情報] リンクを [障害詳細] ページに表示するには、障害番号を含む名前の HTML ファイルが必要です。

[障害詳細] ページは、追加の障害情報を表示できるカスタム Web ページにリンクすることができます。現在の [障害詳細] ページには、時間、スループット、Web サーバアドレスなど、障害に関するさまざまな詳細情報が表示されます。ただし、ほかにも障害に関する追加の詳細情報（会社のニーズに固有の詳細情報）がある可能性もあり、これらも [障害詳細] ページに追加できます。

CA Technologies プロフェッショナル サービスは、この障害情報を提供し、CA CEM のディレクトリに保管することができます。 [障害詳細] ページの [その他障害情報] リンクからアクセスする、この追加の障害情報は、エンドユーザの問題の切り分けに役立ちます。また、個々の障害に関連する前後関係の情報を示すこともできます。

[その他障害情報] リンクを所定の障害の [障害詳細] ページ下部に表示するには、以下の条件を満たす必要があります。

- defect-<defectId>.htm という規約に従った名前のファイルが必要です。
- このファイルは additionalDefectDetailFileLocation プロパティで指定されたディレクトリに存在する必要があります。

たとえば、このファイルが MOM の

<EM_Home>/cem/tess/additionaldefectdetails/defect-60000000000000026.htm に存在する場合、このページのリンクは、障害番号 60000000000000026 の [障害詳細] ページに表示されます。

[その他障害情報] リンクをクリックしたときに、HTML ファイルの読み取り権限があると、HTML ページが表示されます。

重要: 古い defect-<defectId>.htm ファイルを削除するためのスクリプトを作成してください。これらのファイルは、障害がエイジアウトしても自動的に削除されません。

additionalDefectDetailFileLocation

defect-<DefectID>.htm という名前のファイルが MOM のこのディレクトリ内にあると、そのファイルへのリンクが、その障害の [障害情報] ページの下部に表示されます。

クラスタ化された環境の場合

- ディレクトリは MOM にある必要があります。
- additionalDefectDetailFileLocation プロパティは、MOM の *tess-customer.properties* ファイルまたは *tess-default.properties* ファイルから読み取られます。

オプション

ディレクトリパス。絶対パス、または MOM<EM_Home> を基準とする相対パスを指定できます。

デフォルト

cem/tess/additionaldefectdetails

例

C:¥¥test¥¥evidence_for_defects (Windows の例)

/test/evidence_for_defects (UNIX の例)

注

Windows プラットフォームで円記号を使用する場合、1つの円記号 (¥) はエスケープシーケンスとして解釈されるため、二重の円記号 (¥¥) にする必要があります。

障害処理のパフォーマンスの向上

インシデントの影響を受けたユーザグループの数を判別するためにデータベースにクエリを実行すると、CPUに負荷がかかることがあります。特に、これはインシデントに含まれている障害が多い場合に発生します。影響を受けたユーザグループのクエリを実行すると、障害処理が遅延することがあります。これらの遅延は、クエリの回数を減らすことで軽減できます。

デフォルトでは、`affected-user-group` クエリは、障害がインシデントに追加されるたびに実行されます。しかし、障害が検出されるたびにではなく、特定の更新間隔で実行されるように、このクエリの回数を減らすことができます。

`affected-user-group` クエリが一定の間隔で実行される場合には、その間隔の間、現在の `affected-user-group` カウントを保持するためのキャッシュが作成されます。更新間隔を設定するほかに、アイドル状態のインシデントをキャッシュから削除する頻度を指定するエイジアウト間隔のプロパティも設定します。

注: このクエリの実行回数を減らすと、更新間隔の長さによって、またはまれにエイジアウト間隔の長さによって、`affected-user-group` のカウントが最新ではなくなる場合があるというマイナス面があります。しかし、障害処理のパフォーマンスが上がる代償が、カウント情報のわずかな遅れのみであれば、検討に値するかもしれません。

`affected-user-groups` のクエリの頻度を減らす方法

1. (オプション) 障害処理が遅延しているかどうかを確認します。

たとえば、[CEM] - [インシデント管理] - [障害] を選択して、すべての障害を表示します。障害の検出が速やかであるか、または遅延しているかを確認します。

2. 「[tess-default.properties プロパティ デフォルトファイルの変更 \(p. 633\)](#)」に記載されている手順に従います。以下のプロパティの値を指定します。
 - `defects.affectedUserGroupUpdateInterval_Secs` (更新間隔)
 - `defects.affectedUserGroupAgeoutInterval_Mins` (エイジアウト間隔)

例 :

```
defects.affectedUserGroupUpdateInterval_Secs=180
defects.affectedUserGroupAgeoutInterval_Mins=10
```

初期値として更新間隔に **180** 秒を指定し、エイジアウト間隔に **10** 分を指定することをお勧めします。 **affected-user-group** クエリが原因で障害処理が遅延している場合は、これらの値で改善されるかどうかを確認する必要があります。

これらのプロパティの詳細については、

「[defects.affectedUserGroupUpdateInterval_Secs \(P. 639\)](#)」および「[defects.affectedUserGroupAgeoutInterval_Mins \(P. 640\)](#)」を参照してください。

defects.affectedUserGroupUpdateInterval_Secs

インシデントに関連する影響を受けたユーザグループの数のクエリを実行する間隔（秒単位）。

オプション

数値（秒数）

- 最小値 **0** は、障害がインシデントに追加されるたびに **affected-user-group** クエリを実行することを指定します。
- 推奨される最大値は **3600**（1 時間）です。

デフォルト

0

例

```
defects.affectedUserGroupUpdateInterval_Secs=180
```

注

更新間隔の長さによって、またはまれにエイジアウト間隔の長さによって、レポートされた **affected-user-group** のカウントが最新ではなくなる場合があります。

defects.affectedUserGroupAgeoutInterval_Mins

インシデントがこの値よりも長い期間アイドルであると（更新されていないと）、そのインシデントは **affected-user-group** キャッシュから削除（エイジアウト）されます。

オプション

数値（分数）

- 最小値。エイジアウト間隔は、更新間隔の 2 倍より大きい値に設定します。このように設定しないと、**IntroscopeEnterpriseManager** ログに警告が表示され、値は更新間隔の 2 倍にリセットされます。
- 推奨される最大値は 121 分（2 時間を少し超える値）です。

デフォルト

1

例

defects.affectedUserGroupAgeoutInterval_Mins=10

注

この値は、更新間隔の 2 倍より大きく 4 倍より小さい値にする必要があります。たとえば、更新間隔が 180 秒の場合、エイジアウト間隔は 7～11 分の間にする必要があります。

インシデントがキャッシュから削除されると、**affected-user-group** クエリが実行され、インシデントの **affected-user-group** カウントが更新されます。これで、カウントの失効期間がエイジアウト間隔より長くなることなくなくなります。

不正なファイルのディレクトリの場所の変更

デフォルトでは、TIM から **Enterprise Manager** に送信されたデータ ファイルは、以下のディレクトリに格納されます。

- **cem/tess/badfiles**（問題があって処理できないファイルは、このディレクトリに格納されます。ログ ファイルに、ファイルがこのディレクトリにいつ移動されたかが報告されます。ファイルは、このディレクトリから自動的に削除されません。このディレクトリ内のファイルの数が多場合は、ファイルを削除してください）。

[tess-default.properties](#) ファイルを変更 (P. 633)することによって、これらのディレクトリを変更できます。

これらのディレクトリを設定する理由を以下に示します。

- ディスク空き容量の問題：より大容量のドライブにディレクトリを移動するため。
- ある Enterprise Manager から別の Enterprise Manager に TIM コレクションサービスを移動し、両方の Enterprise Manager にある `tess-customer.properties` ファイルが同一（3 台目）のマシンのディレクトリを参照している場合、TIM コレクションサービスを移動するときにデータは失われません。

デフォルト：TIM コレクションサービスを別の Enterprise Manager に移動する場合、元の Enterprise Manager に残る未処理のデータファイルは（サービスを元の Enterprise Manager に戻さない限り）処理されません。

collectors.badDataDirectory

エラーが発生しているために処理できないファイルは、このディレクトリに移動されます。

オプション

ディレクトリパス。相対パスの場合は、`<EM_Home>` を基準とします。絶対パスが指定された場合は、そのまま使用されます。

デフォルト

`cem/tess/badfiles`

例

`collectors.badDataDirectory=cem/TIMdatafiles/badfiles`

`collectors.badDataDirectory=/tmp/badfiles`

`collectors.badDataDirectory=N:¥¥cem¥¥badfilesfromtess`

`collectors.badDataDirectory=¥¥¥¥server2¥¥c$¥¥cem¥¥tess¥¥badfiles`

注

Windows プラットフォームで円記号を使用する場合、1 つの円記号 (¥) はエスケープシーケンスとして解釈されるため、二重の円記号 (¥¥) にする必要があります。

ディレクトリが存在しない場合は、作成されます。

その他の CA CEM デフォルト プロパティ

このトピックでは、その他の <wcem> デフォルト プロパティについて説明します。

[baseline.durationInDays](#) (P. 642)

[BTStatsMetricName.backwardCompatible](#) (P. 643)

[email.defaultFromAddress](#) (P. 643)

[invalid.importexport.filename.chars](#) (P. 644)

[timTessCommunication.useSsl](#) (P. 644)

baseline.durationInDays

ベースライン計算に必要な時間単位のデータの日数。

デフォルト値は **28** です。これは、ベースライン計算が、過去 **28** 日間に収集された時間単位のデータに基づくことを意味します。

使用例：CA CEM は 10 日間データを収集しましたが、最初の 3 日はトランザクション定義を試したり変更したりしたので無効であることがわかっています。そのため、値を 7 に設定しました。有効なデータを収集する日数が増えたら、後でこの値を増加します。

オプション

数値

デフォルト

28

例

baseline.durationInDays=7

注

通常は、監視対象トランザクションの一般的なビジネス サイクルは 1 週間なので、7 の倍数を使用します。

ベースラインに関する全般的な情報については、「CA APM トランザクション定義ガイド」を参照してください。

BTStatsMetricName.backwardCompatible

次のもので有効： CA CEM5.0 と 4.5 の互換性。

CA CEM 5.0 では、「ビジネス プロセス」という用語が「ビジネス サービス」に変更されました。このプロパティを使用すると、カスタマ エクスペリエンス メトリックに CA CEM 4.5 のダッシュボードメトリック名を引き続き使用することができます。

オプション

true または false

true の場合、CA CEM 4.5 のメトリック名「ビジネス プロセス」が使用されます。

false の場合、「ビジネス サービス」が使用されます。

デフォルト

false

例

```
BTStatsMetricName.backwardCompatible=false
```

注

この設定を true に変更する場合は、CA CEM 4.5 の Javascript 計算機を使用する必要があります。

email.defaultFromAddress

Embedded Entitlements Manager が認証に使用されていない場合や、ユーザの電子メールアドレスが Embedded Entitlements Manager で指定されなかった場合は、このアドレスが、SMTP サーバ設定のテストに使用されます。また、電子メールで送信されるレポートの差出人アドレスとして使用されることもあります。

オプション

有効な電子メールアドレス

デフォルト

```
support@catechnologies.com
```

例

```
email.defaultFromAddress=my.email@company.com
```

注

使用した場合、このプロパティは、[システム] - [電子メール設定] ページの [差出人アドレス] および [宛先アドレス] の各フィールドに表示されます。

invalid.importexport.filename.chars

エクスポートされたビジネス サービス名に使用できる特殊文字を指定します。

オプション

Linux ファイル名に使用できない特殊文字。

デフォルト

/¥¥:*?<>&;|

例

invalid.importexport.filename.chars=/ ¥¥ : * ? < > & ; |

注

ビジネス サービスがエクスポートされる場合、エクスポート ファイルの名前はビジネス サービスの名前に基づきます。ファイル名に使用できない文字が名前に含まれていると、エクスポートは失敗します。

この失敗を防ぐには、文字をこのプロパティ リストに挿入します。エクスポート ファイルの作成時に、文字はアンダースコアに置き換えられます。たとえば、my&BP という名前のビジネス サービスがエクスポートされる場合、エクスポート ファイル名は BTEExport_my_BP_<timestamp>.zip になります。

timTessCommunication.useSsl

Enterprise Manager/TIM の通信で HTTP を使用するか、HTTPS を使用するかを指定します。

オプション

0 または 1

0 の場合、Enterprise Manager と TIM は HTTP を使用して通信します。

1 の場合、Enterprise Manager と TIM は HTTPS を使用して通信します。

デフォルト

0

例

`timTessCommunication.useSsl=1`

注

このプロパティは `tess-default.properties` ファイルには存在しません。
ご使用の `tess-customer.properties` ファイルに追加する必要があります。