管理者ガイド

CA Application Delivery Analysis

バージョン 10.1

ca technologies

CA Technologies 製品リファレンス

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

- CA Application Delivery Analysis
- CA GigaStor
- CA GigaStor コネクタ
- CA Multi-Port Monitor
- CA Performance Center
- CA NetQoS Performance Center
- CA Standard Monitor
- CA Virtual Systems Monitor

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: Application Delivery Analysis へようこそ 17

Application Delivery Analysis について 17
Application Delivery Analysis のアーキテクチャ概要 19
Application Delivery Analysis での監視 21
Application Delivery Analysis における管理者役割 22
管理コンソールにアクセスする方法 22
推奨のブラウザ設定 23
［環境管理］ページをナビゲートする方法 24
TCP セッションの監視 25
クライアント ネットワークのリストの表示 26
サーバのリストの表示 27
アプリケーションのリストの表示 29
CA Application Delivery Analysis のセットアップおよび保守の方法 31

第 2 章: クライアント ネットワークの管理 33

クライアント ネットワークの仕組み 34
ネットワーク リストの仕組み 35
ネットワーク ベース レポートの仕組み 36
ネットワーク領域の仕組み 38
命名規則 41
クライアント ネットワークの検索 41
クライアント ネットワークの管理 44
デフォルト クライアント ネットワーク 45
CSV ファイルからのクライアント ネットワークのインポート 46
クライアント ネットワークの追加 51
クライアント ネットワークの編集 53
クライアント ネットワークの削除 54
ルータに対するクライアント ネットワークの SNMP ポーリング 56
CSV ファイルへのクライアント ネットワークのエクスポート 58
ネットワーク タイプ別のクライアント ネットワークのグループ化 59
ネットワーク タイプの仕組み 60
ネットワーク タイプが有用な理由 61
ネットワーク タイプの追加 63
ネットワーク タイプの編集 64

ネットワーク タイプの削除 65
クライアント ネットワークへのネットワーク タイプの割り当て 66
Web サービス メソッドを使用したクライアント ネットワークの管理 67
パラメータ説明 67
Web サービス メソッド 69
Web サービス API をテストする方法 72
エラー レポートの仕組み 73
サンプル Perl スクリプト 74

第 3 章: サーバの管理 79

サーバの仕組み 79
サーバ サブネット リストの仕組み 80
サーバ リストの仕組み 81
/32 クライアント ネットワークの仕組み 82
TCP セッション ID 83
ホスト名の解決 83
サーバ サブネットの管理 84
サブネットの追加 85
サーバ サブネットの編集 87
サーバ サブネットの削除 88
サーバの管理 89
命名規則 90
サーバの検索 91
サーバの追加 92
サーバの編集 93
サーバの削除 95
CSV ファイルからのサーバ定義のインポート 96
CSV ファイルへのサーバ定義のエクスポート 101
サーバへの監視フィードの固定 102
サーバ保守のスケジュール 103
保守スケジュールの仕組み 104
保守スケジュールの追加 105
サーバ保守スケジュール名の変更 106
保守スケジュールの削除 107
保守スケジュールへの保守期間の追加 108
保守期間の編集 109
保守期間の削除 110
サーバへの保守スケジュールの割り当て 111

第 4 章: テナントの管理 113

テナンシーの概要 113
前提条件 114
ドメインによるトラフィックの分離方法 115
データ ソースの同期 116
ドメインベースのレポートの動作 117
ドメインへのクライアント ネットワークの追加 117
ドメインへのサーバの追加 118
監視フィードへのドメインの割り当て 119

第 5 章: アプリケーションの管理 121

アプリケーションの仕組み 122
優先アプリケーションの仕組み 123
アプリケーションの検索 124
命名規則 125
アプリケーション ポート除外 125
ポート除外の仕組み 126
ポート除外リストの仕組み 127
ポート除外の追加 128
ポート除外の編集 130
ポート除外の削除 131
システム定義のアプリケーションの管理 132
システム定義のアプリケーションの編集 133
システム定義のアプリケーションの削除 135
ユーザ定義のアプリケーションの管理 137
標準アプリケーションの作成 139
Web アプリケーションの作成 141
FTP アプリケーションの作成 146
コントロール ポート アプリケーションの作成 149
アプリケーションへのサーバの割り当て 150
ユーザ定義アプリケーションの編集 153
ユーザ定義アプリケーションの削除 155
多層アプリケーションの管理 156
多層アプリケーションの仕組み 157
多層アプリケーションを監視する方法 158
アプリケーションのキープアライブ メッセージ 162

第 6 章: パフォーマンスしきい値の管理 165

パフォーマンスしきい値の仕組み 165
アプリケーション パフォーマンスの評価方法 167
パフォーマンス メトリックの仕組み 168
パフォーマンスしきい値をカスタマイズするオプション 172
インシデントのオープンおよびクローズの仕組み 175
NetQoS Performance Center （CA NPC） 176
CA Performance Center （CA PC） 177
パフォーマンスしきい値の編集 178
［環境管理］ページからのしきい値の編集 179
［操作］ページからのしきい値の編集 181
パフォーマンスしきい値の追加 183
ネットワーク グループ用のデフォルト パフォーマンスしきい値の有効化 185
WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の編集 186
最適化されたアプリケーション上の最適化されていないトラフィックのしきい値の編集 187
最適化されたクライアント セグメントのしきい値の編集 189
最適化された WAN セグメントのしきい値の編集 191
最適化されたサーバ セグメントのしきい値の編集 193

第 7 章: インシデント レスポンスの管理 195

インシデント レスポンスの仕組み 195
インシデント レスポンスの開始法 196
電子メール通知 198
SNMP トラップ通知 199
アプリケーション接続時間の調査 200
パケット キャプチャ調査 201
SNMP 経由のパフォーマンス調査 202
ping レスポンス時間調査 204
トレース ルート調査 205
インシデント レスポンスの追加 207
インシデント レスポンスの編集 208
インシデント レスポンスの削除 209
ネットワークまたはサーバのインシデント レスポンスへのアクションの追加 210
応答アクションの編集 211
応答アクションの削除 212
インシデント レスポンスの割り当て 212
アプリケーションへのインシデント レスポンスの割り当て 213
サーバへのインシデント レスポンスの割り当て 214

ネットワーク タイプへのインシデント レスポンスの割り当て 215
インシデント レスポンスのトラブルシューティング 216
Web サービス メソッドを使用したインシデントの管理 216
オブジェクト識別子仕様 217
Web サービス仕様 219
SNMP トラップの説明 223

第 8 章: アプリケーション パフォーマンス OLA の管理 225

パフォーマンス OLA の仕組み 226
パフォーマンス OLA レポートの仕組み 227
パフォーマンス OLA しきい値の仕組み 228
運用レベル メトリックの仕組み 229
パフォーマンス OLA のヒント 230
履歴データからの運用レベルの確立 231
ネットワークのグループのアプリケーション パフォーマンス OLA の作成 233
アプリケーション パフォーマンス OLA の編集 235
アプリケーション パフォーマンス OLA の削除 237

第 9 章: アプリケーション可用性の管理 239

可用性監視の仕組み 239
システム定義のアプリケーションはなぜ除外されるか 241
アプリケーション可用性のサーバ インシデントの仕組み 242
アプリケーション可用性レポートの仕組み 243
可用性監視の有効化 243
アプリケーション可用性 OLA の仕組み 247
可用性 OLA レポートの仕組み 247
アプリケーション可用性 OLA の有効化 248

第 10 章: ユーザ アカウント権限の管理 249

ユーザ アカウントの権限設定の仕組み 250
統合セキュリティ 252
製品権限 253
役割 254
ユーザおよびグループ 256
FAQ 260

第 11 章: システム管理 261

Windows 管理者の認証情報 261
データベースの管理 261
必要なサービス 262
データベースのステータス 263
データベース ストレージ基本設定の編集 264
データベースからのデータのパージ 265
データベースのバックアップとリストア 266
コンソール設定の管理 267
IP アドレスの変更 268
SNMP プロファイルの管理 269
SNMP プロファイル ディスカバリの仕組み 270
SNMP プロファイルの追加 271
SNMP プロファイルの編集 272
SNMP プロファイルの削除 273
ネットワーク デバイスの管理 274
ネットワーク デバイスの追加 274
ネットワーク デバイス調査の表示 275
ネットワーク デバイスの編集 276
ネットワーク デバイスの削除 276
調査用のグループ ネットワーク デバイス 277
スケジュール済み電子メールの管理 280
電子メール レポートのスケジュールの編集 280
スケジュール済みレポートの削除 281
システム保守の実行 281
ハードディスク ドライブをメンテナンスする方法 282
システム セキュリティの更新と Windows アップデートをインストールする方法 283
データ整合性の確認とアンチウイルス ソフトウェアの使用 284
サードパーティ ソフトウェアに関する問題 285
ドメイン グループ ポリシーに関する問題 285
製品アップグレードのサポート 285
ハードウェア交換の要求 286

第 12 章: 監視デバイスの管理 287

監視デバイスの動作 287
監視フィードの動作 288
監視フィード割り当ての仕組み 289
監視デバイス同期の動作 290

監視フィードのペアの作成 291
セッション数情報の表示 292
［監視フィード］でのアクティブ セッション数の表示 293
セッション数の 1 時間ごとのサマリの表示 295
管理コンソールによるデータベース増加の管理方法 296
データベース容量 297
データベース増加の制御 298
監視デバイスの比率 300
監視デバイスに関する推奨事項 302
基本操作の実行 304
監視デバイス インシデントの管理 305
監視デバイス インシデントの表示 306
監視デバイス インシデントのしきい値の編集 307
可用性監視の有効化と無効化 309
監視デバイスへのインシデント レスポンスの追加 310
監視デバイス インシデント レスポンス名の編集 311
監視デバイス インシデント レスポンスの削除 312
監視デバイス インシデント レスポンスへのアクションの追加 313
応答アクションの編集 314
応答アクションの削除 315
監視デバイス インシデント レスポンスの割り当て 316
監視のトラブルシュート 316
監視デバイス ステータスの表示 317
通信問題のトラブルシューティング 318
データ欠落のトラブルシューティング 319

第 13 章: CA Standard Monitor による監視 321

CA Standard Monitor が監視デバイスとして動作する仕組み 321
CA Standard Monitor の動作 322
必要なサービス 324
監視フィードの動作 325
監視フィード割り当ての仕組み 325
パケット キャプチャ調査の仕組み 326
監視デバイスに関する考慮事項 327
XFF 翻訳のサポート 328
XFF 翻訳の動作 329
XFF 翻訳の有効化 330
CA Standard Monitor の追加 331
前提条件 332

CA Standard Monitor の追加 333
NAT ファイアウォール通信 334
パケット キャプチャ調査ファイルの保護 335
CA Standard Monitor の編集 336
パケット監視フィードの編集 337
監視デバイスのパフォーマンスの管理 338
監視デバイス操作 339
キープアライブ メッセージのフィルタ除外 341
CA Standard Monitor の削除 344
パケット監視フィードの無効化 345
CA Standard Monitor のトラブルシューティング 346
アクティブ セッション数の確認 347
監視フィード統計の表示 348
SPAN レシーバ統計の表示 350
CA ADA Monitor サービスのトラブルシューティング 353
重複したクライアント ネットワークの確認 360
データ欠落のトラブルシューティング 361
ドロップされたパケット数のトラブルシューティング 362

第 14 章: CA Virtual Systems Monitor による監視 365

CA Virtual Systems Monitor が監視デバイスとして動作する仕組み 366
展開の計画 368
ポート使用率とファイアウォール 369
システム要件 370
CA Virtual Systems Monitor の追加 371
仮想スイッチの設定 371
仮想マシンの作成 379
ネットワーク接続の設定 381
CA Application Delivery Analysis セットアップ プログラムの実行 385
時間を時間サーバに同期させる 386
セットアップの完了 387
インストール後の手順 387

第 15 章: CA GigaStor による監視 389

CA GigaStor は監視デバイスとしてどのように機能するか 390
CA GigaStor コネクタの仕組み 391
監視フィード割り当ての仕組み 392
パケット キャプチャ調査の仕組み 393

サイズ変更に関する推奨事項 393
監視デバイスに関する考慮事項 394
CA GigaStor 監視デバイスの追加 395
前提条件 396
GigaStor アプライアンスでのソフトウェアのインストールと設定 396
CA GigaStor 監視デバイスの追加 398
監視デバイスへの CA GigaStor の割り当て 399
ユーザのコンピュータへの CA Observer のインストール 401
パッシブ プローブ インスタンスに対する権限の付与 402
CA GigaStor 入力ポートのブロック 403
CA GigaStor 監視デバイスの編集 404
GigaStor 監視フィードの編集 405
CA GigaStor の割り当て解除 407
GigaStor Incidents 408
基本操作の実行 409
CA GigaStor 監視デバイスの削除 410
CA GigaStor の削除 411
CA GigaStor 監視デバイスのトラブルシューティング 411
GigaStor 監視フィードのアクティブ セッション数の表示 412
GigaStor カウンタ統計の表示 413

第 16 章: Cisco WAAS による監視 415

監視デバイスとしての Cisco WAAS の動作方法 416
Cisco WAAS の仕組み 417
監視フィード割り当ての仕組み 418
ネットワーク セグメントの動作方法 419
WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の動作方法 420
最適化停止時における監視の仕組み 420
サイズ変更に関する推奨事項 422
監視デバイスに関する考慮事項 423
Cisco WAE 監視デバイスの追加 424
前提条件 425
レスポンス時間をエクスポートするための Cisco WAE の設定 426
監視デバイスへの Cisco WAE の割り当て 428
Cisco WAE 監視デバイスの編集 430
WAN 最適化監視フィードの編集 431
Cisco WAE の割り当て解除 433
WAAS Incidents 433
Cisco WAE 監視デバイスの削除 434

Cisco WAE 上のフロー監視の無効化 435
Cisco WAE 監視デバイスの削除 436
最適化アプリケーションのリセット 437
Cisco WAE 監視デバイスのトラブルシューティング 438
アクティブ セッションの表示 438
WAN 最適化カウンタ統計の表示 439
Cisco WAE ネットワーク設定の確認 442
Cisco WAE デバイス グループによるサーバの監視 443
ソース セットの動作方法 443
Cisco WAE デバイスへのソース セットの割り当て 444
サーバへのソース セットの割り当て 445
ソース セットの名前の変更 446
ソース セットの削除 446
管理コンソール間の最適化データの共有 447
WAN 最適化パフォーマンス データの共有 449
共有設定の更新 451
監視デバイスの削除 452
トラブルシューティングのヒント 453

第 17 章: Cisco NAM による監視 455

監視デバイスとしての Cisco NAM の動作方法 455
Cisco NAM の仕組み 456
監視フィード割り当ての仕組み 456
監視デバイスに関する考慮事項 458
Cisco NAM 監視デバイスの追加 459
前提条件 460
レスポンス時間データをエクスポートするための Cisco NAM の設定 461
Cisco NAM の 管理コンソール への接続を確認 462
NAM 監視フィードの有効化 463
Cisco NAM 監視デバイスの編集 464
NAM 監視フィードの編集 465
NAM Incidents 466
Cisco NAM 監視デバイスの削除 467
Cisco NAM 監視デバイスのトラブルシューティング 469

第 18 章: Riverbed Steelhead による監視 473

概念 473
はじめに 474

アーキテクチャ 475
ネットワーク セグメント 477
監視フィード割り当て 478
ネットワーク セグメントのインシデントしきい値 478
パケット キャプチャ調査 478
最適化停止時の監視 479
監視デバイスの追加 482
監視デバイスに関する考慮事項 483
監視デバイスのプロビジョニング 484
ネットワーク トラフィックのミラーリング 484
監視デバイスの追加 489
監視デバイスの管理 490
監視デバイスの編集 491
監視フィードの編集 492
監視パフォーマンスの管理 493
監視デバイスの削除 494
監視デバイスのトラブルシューティング 495
Steelhead レシーバ統計の表示 496
SPAN レシーバ統計の表示 498
アクティブ セッションの表示 501

用語集 503

第 1 章: Application Delivery Analysis へようこそ

このセクションには、以下のトピックが含まれています。

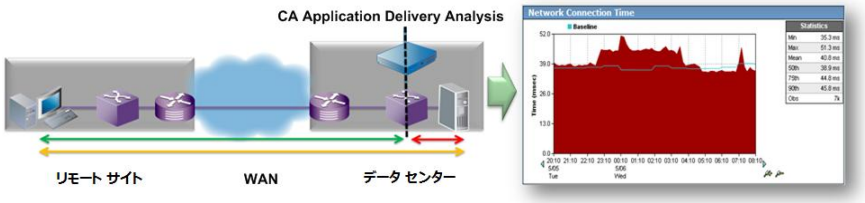
Application Delivery Analysis について (P. 17)
管理コンソールにアクセスする方法 (P. 22)
TCP セッションの監視 (P. 25)
CA Application Delivery Analysis のセットアップおよび保守の方法 (P. 31)

Application Delivery Analysis について

CA Application Delivery Analysis は、CA Performance Center（CA PC）および CA NetQoS Performance Center（CA NPC）のアプリケーション パフォーマンス管理モジュールです。 CA Application Delivery Analysis はエンド ユーザのレスポンス時間を、デスクトップ/サーバ エージェントなしで追跡および測定します。 CA Application Delivery Analysis は、クライアントとサーバ間のネットワークを横断する IPv4 ベースの TCP パケットをパッシブに監視し、すべてのミッション クリティカルなアプリケーションに対して、ネットワーク、サーバ、アプリケーションの遅延などのメトリックを提供します。

TCP トランザクションはインフラストラクチャ内を転送される場合、基本的にインフラストラクチャの 3 つの主要コンポーネント、ネットワーク、サーバおよびアプリケーション内を移動します。 これらのコンポーネントのいずれかのパフォーマンスが低下すると、エンド ユーザに対するトランザクション時間に悪影響を及ぼす場合があります。

CA Application Delivery Analysis は、各 TCP クライアントとサーバ上のアプリケーション ポートの間の TCP トランザクション時間をサーバ スイッチによって測定します。 下の例に示すように、サーバ スイッチとクライアントの間のレスポンス時間はネットワーク レスポンス時間（緑の矢印で示されている）です。また、サーバ スイッチとサーバの間のレスポンス時間はサーバ レスポンス時間（赤い矢印で示されている）です。ネットワーク レスポンス時間とサーバ レスポンス時間の合計（黄色い矢印で示されている）は、エンド ユーザのアプリケーションの操作性を反映しています。



CA Application Delivery Analysis は、タイム フレーム、アプリケーション ポート、サーバ、ネットワーク、およびパフォーマンス メトリックの一意の組み合わせについてレポートします。 たとえば、過去 24 時間に Development I クライアント ネットワークと通信したすべてのアプリケーションおよびサーバの平均ネットワーク接続時間をレポートすることができます。

タイムフレーム: 過去 24 時間
ドメイン: すべて
アプリケーション: すべて
サーバ: 191.168.2.68
ネットワーク: すべて [クリア]
メトリック: すべての相対メトリック

CA Application Delivery Analysis をパフォーマンス管理で使用する場合、CA PC または CA NPC にデータ ソースとして登録できます。 CA Application Delivery Analysis がパフォーマンス管理で使用されない場合は、CA NPC に登録する必要があります。CA PC または CA NPC のセキュリティ機能（ユーザ、役割、製品権限、グループを含む）によって、管理コンソール内の特定のデータを参照できるユーザを制御することができます。

Application Delivery Analysis のアーキテクチャ概要

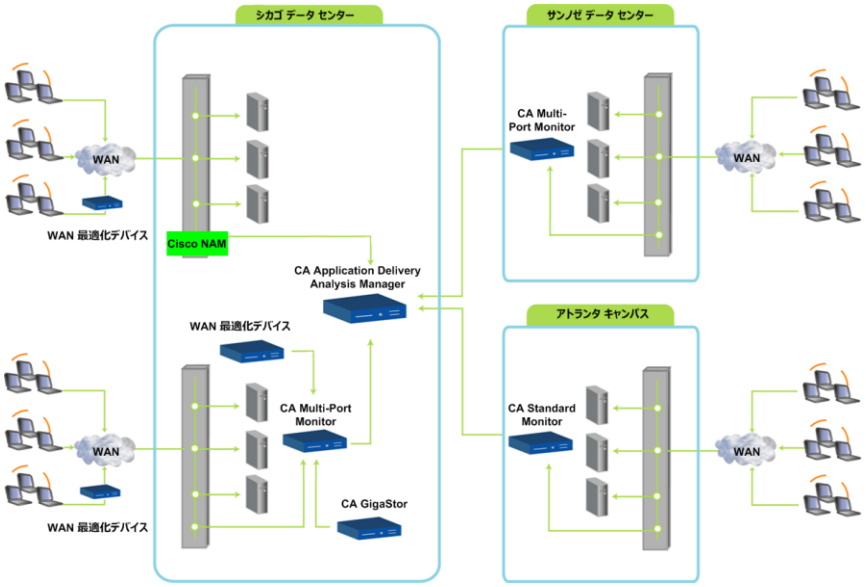
CA Application Delivery Analysis は CA Application Delivery Analysis Manager および 1 つ以上の 監視デバイス から構成されます。 CA Application Delivery Analysis Manager は、データベース エンジンおよびレポート コンソールを実行するアプライアンスです。 監視デバイス は TCP トランザクションを監視するアプライアンスです。 CA Application Delivery Analysis Manager は、1 つ以上の 監視デバイス からのレスポンス時間データを統合します。

CA Application Delivery Analysis は複数の監視オプションを提供します。

- CA Multi-Port Monitor は、SPAN または TAP データ用の機能が豊富な最も拡張性の高いオプションです。 1 ギガビット オプションと 10 ギガビット オプションがあります。
- CA Standard Monitor は最大で 1 ギガビットの SPAN または TAP データを処理します。
- CA Virtual Systems Monitor は、同じ VMware ESX Host 上の仮想サーバ間の双方向のトラフィックを監視します。
- NAM（Cisco Network Analysis Module）。 Cisco NAM は、詳細なトラブルシューティングを実行できる、CA Application Delivery Analysis 用の 監視デバイス です。

CA Standard Monitor または CA Multi-Port Monitor は、次のものからのパケット要約を処理します。

- Cisco WAAS および Riverbed Steelhead などの WAN 最適化デバイス
- CA GigaStor コネクタ。CA GigaStor は、長期的なパケット キャプチャ アプライアンスとして、CA Application Delivery Analysis にパフォーマンス データを送信するだけでなく、時間をさかのぼってパケット分析を行ったりセッション データを再生したりする遡及ネットワーク分析を可能にします。



すべてのサーバ トラフィックが単一のスイッチ ポートからミラーリングできる環境において、スタンドアロン CA Application Delivery Analysis Manager を使用できるのは、その CA Application Delivery Analysis Manager が、監視 NIC 上でミラーリングされた TCP パケットを受信する場合です。

Application Delivery Analysis での監視

CA Application Delivery Analysis は、エンド ツー エンド パフォーマンスを以下のとおり自動的に監視します。

- デフォルトのサーバ サブネットとクライアント ネットワーク、および指定したサーバ サブネットとクライアント ネットワークに基づいて、アプリケーションに対して IPv4 ベースの TCP トランザクション時間を収集および計算。
- 指定したサーバ割り当てに基づいたユーザ定義アプリケーションの監視
- 正常とは何かを理解するためのアプリケーション パフォーマンスの基準を生成。
- 受け入れ可能なパフォーマンスの上限しきい値の設定
- しきい値を超えた場合にインシデントを作成。
- IPv4 トランザクションに対してすべてのパフォーマンス メトリックの 5 分間サマリを表示。

デフォルトでは、CA Application Delivery Analysis はパッシブにエンドツーエンド レスポンス時間を監視します。 この製品をさらにアクティブにすることができます。たとえば、ネットワーク インシデントに対してネットワーク トレース ルート調査を有効にしたり、アプリケーションの可用性に対して OLA （運用レベル契約）を設定したりします。

詳細:

CA Application Delivery Analysis のセットアップおよび保守の方法 (P. 31)

Application Delivery Analysis における管理者役割

CA Application Delivery Analysis 管理者は以下の責任を負います。

- 監視デバイス を設定。
- ネットワーク管理者との共同作業により、ネットワーク内の適切な場所に 監視デバイス を配置し、適切な TCP トラフィックを各 監視デバイス にミラーリング。
- 監視するサーバ サブネット、アプリケーションおよびクライアント ネットワーク定義の指定
- インシデント レスポンスの割り当て、アプリケーションの作成および特定のサーバの割り当てなどを行うために、管理コンソール がすべての監視対象サーバ トラフィックから自動的に作成するアプリケーションの管理
- パフォーマンスと可用性のサービス レベルの指定
- 管理コンソール にログインしたり、アプリケーション、サーバ、およびクライアント ネットワークの特定のグループを管理したりできるようにするためのセキュリティの管理 CA PC または CA NPC にデータ ソースとして登録された場合、これらのタスクは、CA PC または CA NPC 管理コンソールの［管理］（Admin）タブで実行されることに注意してください。

管理コンソールにアクセスする方法

CA Application Delivery Analysis Manager がインストールされ、エンタープライズ ネットワークで利用可能になったら、Web ブラウザを開き、CA Application Delivery Analysis Manager をホストするサーバの IP アドレスを入力します。 DNS がホスト名を解決するように設定されている場合は、サーバのホスト名を入力します。

注 CA Application Delivery Analysis のインストールと設定の詳細については、「*インストール ガイド*」を参照してください。

適切な URL を指定して 管理コンソール Web インターフェースにアクセスします。

CA PC の状態	指定する URL
管理コンソール サーバにインストールされている	http://*hostname/sa*

CA PC の状態	指定する URL
管理コンソール サーバにインストールされていない	http://*hostname*

管理コンソール は、Microsoft Internet Explorer バージョン 8 または 9、Mozilla Firefox で表示できるよう設計されており、Adobe Flash Player を必要とします。 Internet Explorer バージョン 6 および 7 はサポートされていません。 Web インターフェースに初めてアクセスしたときに、Internet Explorer のセキュリティ強化から Web サイトがブロックされているというセキュリティ プロンプトが表示された場合は、ブラウザ設定を調整することをお勧めします。

CA Application Delivery Analysis 管理者アカウントがない場合は、CA PC または CA NPC の管理者にお問い合わせください。 初めてログオンする場合、事前定義済みの管理者アカウント admin とデフォルト パスワード admin を使用できます。

［ログイン］ページで、ユーザ名とパスワードを入力します。 ログイン認証情報では大文字と小文字を区別することに注意してください。 正常に認証されたらすぐに、管理コンソール に自動的にリダイレクトされます。 ログインが正しくない場合は、［ログイン］ページに戻ります。

セキュリティが向上するように、事前定義済みユーザ アカウントのデフォルト パスワードを変更することをお勧めします。 これは、管理者がログインしてユーザ アカウントを編集することで可能になります。

詳細:

ユーザ アカウント権限の管理 (P. 249)
推奨のブラウザ設定 (P. 23)

推奨のブラウザ設定

ポップアップのブロックを無効にするよう Web ブラウザ設定を更新することをお勧めします。Internet Explorer の場合のみ、信頼されたインターネット サイトのリストに 管理コンソール を追加することをお勧めします。

Internet Explorer 8 を使用して管理コンソールにアクセスすると、ページ上部のフォーマットが正しく表示されません。

この問題を回避するには、Internet Explorer で F12 キーを押して、次に［ブラウザ モード］を［Internet Explorer 8］、［ドキュメント モード］を［Quirks モード］に設定します。

ポップアップ ブロックの無効化

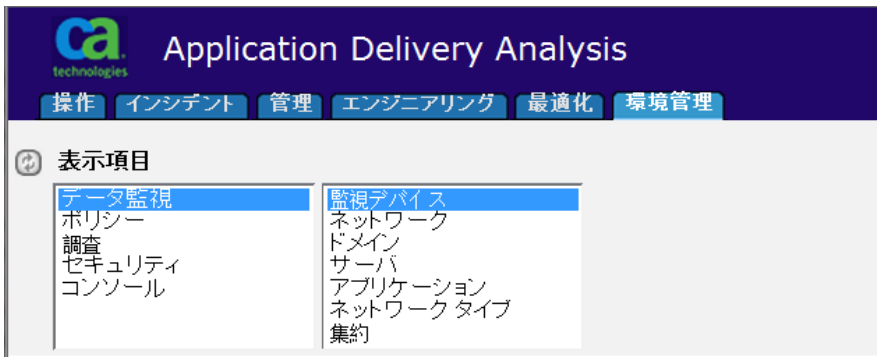
調査を手動で開始する場合は、Web ブラウザでポップアップ ブロッカを無効にします。そうしないと、調査が実行できません。 調査を実行しても、調査のステータスを示すポップアップが表示されない場合は、ポップアップ ブロッカがおそらくまだ有効になっているために、調査が実行されていません。

信頼されたインターネット サイトの更新

ユーザ インターフェースのパフォーマンスを改善するため、Internet Explorer ブラウザ インスタンス内の信頼されたインターネット サイトのリストに 管理コンソール サーバのホスト名を追加することをお勧めします。 デフォルトでは、Internet Explorer は、高いセキュリティ設定を使用して、信頼されたサイトにナビゲーションを制限したり、ユーザが信頼されたサイトのリストに載っていないサイトへ移動するときに繰り返し警告メッセージを表示したりします。 この推奨事項は Internet Explorer にのみ適用可能です。

［環境管理］ページをナビゲートする方法

［環境管理］ページには、管理者権限を持った CA Application Delivery Analysis ユーザがアクセスできます。



CA Application Delivery Analysis を管理するには、［環境管理］ページで［表示項目］メニュー項目をクリックします。

- データ監視 -- ユーザ環境内のアプリケーション、サーバおよびネットワークからアプリケーション レスポンス時間データを収集する 監視デバイス を指定します。
- ポリシー -- アプリケーション、サーバ、ネットワークのパフォーマンスのしきい値、パフォーマンスの低下に対する対応、パフォーマンスと可用性に対する OLA を指定します。
- 調査 -- サーバまたはネットワーク デバイスをポーリングするために使用される SNMP プロファイルを指定します。
- セキュリティ -- ユーザ権限を指定します。CA PC または CA NPC にデータ ソースとして登録されている場合、ユーザ権限は CA PC または CA NPC から管理されます。
- コンソール -- CA Application Delivery Analysis Manager データベース、レポートおよび 監視デバイス インシデントを管理します。

TCP セッションの監視

管理コンソール がエンド ユーザのレスポンス時間を追跡および測定できるようにするには、監視デバイス は、クライアントとサーバ上のアプリケーション ポートの間の IPv4 ベース トランザクションを監視する必要があります。 指定されたサーバ サブネットおよびクライアント ネットワークを使用して、管理コンソール は、TCP トランザクションに一致するパフォーマンス メトリックを自動的に計算します。

通常、CA のテクニカル サポートが、ユーザが監視するクライアント ネットワーク、サーバおよびアプリケーションを指定するのを支援します。

重複するサーバ IP アドレスまたはクライアント IP アドレスのある ISP を管理するには、TCP トラフィックを分離するドメインを使用する必要があります。

CA ADA には、「キャッチ オール」デフォルト クライアント ネットワークに対して以下のデフォルト エントリが含まれます。

- その他すべて： 0.0.0.0/0
- その他すべての 10 ネットワーク： 10.0.0.0/8
- その他すべての 172.16 ネットワーク： 172.16.0.0/12
- その他すべての 192.168 ネットワーク： 192.168.0.0/16

詳細:

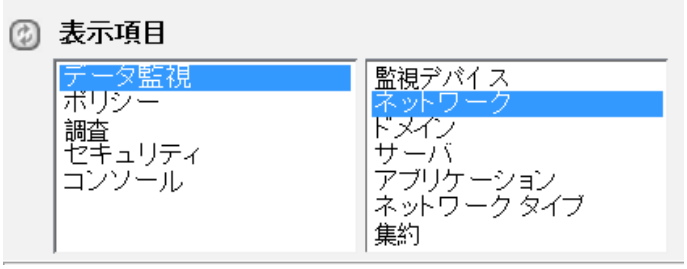
テナントの管理 (P. 113)

クライアント ネットワークのリストの表示

管理コンソール が監視するクライアント ネットワークのリストを管理するには、［ネットワーク リスト］を使用します。 各 監視デバイス は、［ネットワーク リスト］に指定されたクライアント ネットワークとアプリケーション サーバ間のレスポンス時間メトリックを計算します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。



［ネットワーク リスト］が表示されます。以下の例では、/24 サブネット マスクを持つ 2 つの IPv4 クライアント ネットワークが定義されています。

CA Application Delivery Analysis には、「キャッチ オール」デフォルト クライアント ネットワークに対して以下のデフォルト エントリが含まれます。

- その他すべて： 0.0.0.0/0
- その他すべての 10 ネットワーク： 10.0.0.0/8
- その他すべての 172.16 ネットワーク： 172.16.0.0/12
- その他すべての 192.168 ネットワーク： 192.168.0.0/16

詳細:

クライアント ネットワークの管理 (P. 33)

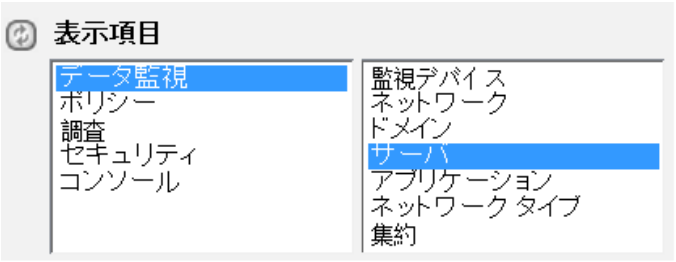
サーバのリストの表示

管理コンソール が監視するサーバのリストを表示し管理するには、［サーバ リスト］を使用します。

サーバがリストに表示されない場合は、一致するサーバ サブネットが存在することを確認するために、［サーバ サブネット リスト］を参照します。 管理コンソール は、サーバ上で一致するアプリケーション ポート トラフィックを検出すると、そのサーバを自動的に［サーバ リスト］に追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。



［サーバ リスト］が表示されます。 以下の例で、［サーバ リスト］内の IPv4 アドレスのリストは［サーバ サブネット リスト］内の IPv4 サーバ サブネットに対応します。

注: Application Delivery Analysis には、サブネット 0.0.0.0 マスク 0 上に「*Monitor All Servers*」と呼ばれるデフォルトのサーバ サブネットが含まれます。 デフォルトのサーバ サブネットにより、新しい監視が追加された場合にデータ収集が自動的に発生するようになります。

詳細:

サーバの管理 (P. 79)

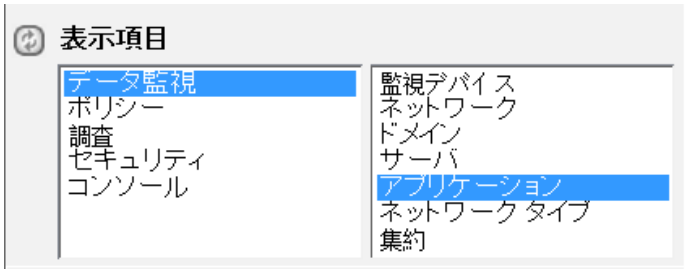
アプリケーションのリストの表示

管理コンソール が監視するアプリケーションを管理するには、［アプリケーション リスト］を使用します。 CA Application Delivery Analysis は、指定されたサーバ サブネットとクライアント ネットワークの間のアプリケーション トラフィックをすべて自動的に監視します。

アプリケーションがリストに表示されない場合は、必ずアプリケーションを監視するように 管理コンソール を設定します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。



［アプリケーション リスト］が表示されます。以下の例では、ウェルノウン ポート上のアプリケーション トラフィックが自動的に指定されています。

詳細:

アプリケーションの管理 (P. 121)

CA Application Delivery Analysis のセットアップおよび保守の方法

CA Application Delivery Analysis がどのように動作するかを理解したら、一般的な管理者タスクを実行することができます。

タスク	詳細
■ 監視デバイス の追加または削除 ■ 監視デバイス パフォーマンスの管理 ■ 監視デバイス アクティビティの表示	監視デバイスの管理 (P. 287)
■ 監視するクライアント ネットワークの指定 ■ ネットワーク タイプを使用したネットワークのグループ化	クライアント ネットワークの管理 (P. 33)
■ 監視するサーバの指定 ■ サーバ保守を実行するようにスケジュールされる期間の指定	サーバの管理 (P. 79)
■ 監視するアプリケーションの指定	アプリケーションの管理 (P. 121)
■ ネットワーク グループへのデフォルト パフォーマンスしきい値の追加 ■ ネットワーク グループを介したユーザ定義アプリケーションのパフォーマンスしきい値のカスタマイズ ■ アプリケーション、サーバおよびネットワーク レスポンス時間の変化への CA Application Delivery Analysis の感度を向上または低下させるパフォーマンスしきい値の調整	パフォーマンスしきい値の管理 (P. 165)
■ CA Application Delivery Analysis による自動的なユーザへの通知およびサーバ インシデントまたはネットワーク インシデントの調査	インシデント レスポンスの管理 (P. 195)
■ アプリケーション パフォーマンスの運用レベルの指定	アプリケーション パフォーマンス OLA の管理 (P. 225)
■ アプリケーション可用性の監視と可用性の運用レベルの指定	アプリケーション可用性の管理 (P. 239)

タスク	詳細
■ ユーザの追加または削除 ■ ユーザ権限の管理	ユーザ アカウント権限の管理 (P. 249)
■ 週単位のデータベース バックアップのスケジュールおよび実行 ■ システム環境設定の指定 ■ SNMP プロファイルの管理	コンソールの管理 (P. 261)
■ システム保守の実行	システム保守の実行 (P. 281)

第 2 章: クライアント ネットワークの管理

このセクションには、以下のトピックが含まれています。

クライアント ネットワークの仕組み (P. 34)
クライアント ネットワークの管理 (P. 44)
ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)
Web サービス メソッドを使用したクライアント ネットワークの管理 (P. 67)

クライアント ネットワークの仕組み

クライアント ネットワークは、監視する一連のクライアント IPv4 アドレスを指定し、ユーザ環境内の物理的な場所またはユーザ グループに対応します。

クライアント トラフィックがどこで発生するかに基づいて（たとえば、リモートサイト、データ センター、またはインターネットなどの外部にアクセスするアプリケーション）、クライアント ネットワークを作成することをお勧めします。 たとえば、192.168.0.0/22 として定義されるクライアント ネットワークが Austin に存在する場合は、管理コンソール を使用して、同じネットワーク アドレスおよびサブネット マスクで Austin クライアント ネットワークを作成します。

管理コンソール ユーザがクライアント ネットワークのパフォーマンス問題を迅速に分析し対応できるようにするには、ユーザ環境内の実際のクライアント ネットワークに対応するクライアント ネットワークを作成します。

サーバが［サーバ リスト］に追加された場合、管理コンソール は、多層アプリケーションでサーバ間のトラフィックを監視するために、対応する /32 クライアント ネットワークを自動的に作成します。

必要なクライアント ネットワークを正しく指定することで、利用可能なシステム リソースが最適化されます。

Application Delivery Analysis には、「キャッチ オール」デフォルト クライアント ネットワークに対して以下のデフォルト エントリが含まれます。

- その他すべて： 0.0.0.0/0
- その他すべての 10 ネットワーク： 10.0.0.0/8
- その他すべての 172.16 ネットワーク： 172.16.0.0/12
- その他すべての 192.168 ネットワーク： 192.168.0.0/16

注: クライアント ネットワークがオーバラップする場合、管理コンソール はより具体的なクライアント ネットワークでアプリケーション トラフィックをレポートします。

詳細:

/32 クライアント ネットワークの仕組み (P. 82)
管理コンソールによるデータベース増加の管理方法 (P. 296)

ネットワーク リストの仕組み

管理コンソール によって監視されるネットワークを表示し管理するには、ネットワーク リストを使用します。 ネットワーク リストには、/32 クライアント ネットワークに加えて、指定するクライアント ネットワークが含まれます。

*/32 クライアント ネットワーク*は単一の IPv4 アドレスを持ったクライアント ネットワークです。CA Application Delivery Analysis は、多層アプリケーションを監視するために /32 クライアント ネットワークを使用します。サーバが[サーバ リスト]に追加されると、管理コンソール は対応する /32 クライアント ネットワークを自動的に作成します。

注: /32 クライアント ネットワークを削除するには、対応するサーバをサーバ リストから削除します。 管理コンソール によって作成された /32 クライアント ネットワークは削除できません。

詳細:

多層アプリケーションの管理 (P. 156)

ネットワーク ベース レポートの仕組み

ネットワーク全体でのアプリケーション パフォーマンスを監視するため、管理コンソール は、個別の TCP セッションのレスポンス時間についてレポートせず、クライアント ネットワーク全体の平均アプリケーション レスポンス時間をレポートします。 ネットワーク レベルのレポートでは、管理コンソール がパフォーマンスの問題を特定のネットワークに分離できます。

24 ビット以上 (24 ビットから 32 ビット) のサブネット マスクで定義されたクライアント ネットワークを監視する場合、管理コンソール は指定された期間内にアプリケーションと通信する実際のクライアント IP アドレスをレポートします。 たとえば、191.168.1.0/24 のネットワークについてのレポートでは、アプリケーションにアクセスした実際のクライアント IP アドレスが表示されます。

管理コンソール はネットワーク全体のアプリケーション レスポンス時間の平均値を取るため、この情報によって、パフォーマンス問題があるクライアント コンピュータを特定することはできません。正確には、これは、指定された期間中にアプリケーションと通信したクライアントのリストにすぎません。 この詳細レベルでは、パフォーマンス問題の原因としてのネットワークを特定することはできません。

アドレス - ユーザのためのマスク リスト

アドレス	マスク	ホスト
191.168.0.2	255.255.255.255	(使用不可)
191.168.0.3	255.255.255.255	(使用不可)
191.168.0.4	255.255.255.255	(使用不可)
191.168.0.5	255.255.255.255	(使用不可)
191.168.0.6	255.255.255.255	(使用不可)
191.168.0.7	255.255.255.255	(使用不可)
191.168.0.8	255.255.255.255	(使用不可)
191.168.0.9	255.255.255.255	(使用不可)
191.168.0.10	255.255.255.255	(使用不可)
191.168.0.11	255.255.255.255	(使用不可)
191.168.0.12	255.255.255.255	(使用不可)
191.168.0.13	255.255.255.255	(使用不可)
191.168.0.14	255.255.255.255	(使用不可)
191.168.0.15	255.255.255.255	(使用不可)

1 / 1 ページ: 1 サイズ: 100

24 ビット未満のサブネット マスクでクライアント ネットワークを作成した場合、管理コンソール はアプリケーションと通信するクラス C ネットワークをレポートします。 たとえば、22 ビット サブネット マスク（192.168.0.0/22 など）でクライアント ネットワークを作成した場合、管理コンソール は、アプリケーションにアクセスした実際のクライアント IP ではなく、クラス C のクライアント ネットワーク（191.168.0.0/24 ～ 191.168.3.0/24）からのメトリックをレポートします。

サービス品質レポート

アドレス	マスク	ホスト
138.42.67.2	255.255.255.255	nclabrtr01.ca.com
138.42.67.3	255.255.255.255	(使用不可)
138.42.67.13	255.255.255.255	nclabep1.ca.com
138.42.67.14	255.255.255.255	
138.42.67.15	255.255.255.255	(使用不可)
138.42.67.16	255.255.255.255	(使用不可)
138.42.67.17	255.255.255.255	(使用不可)
138.42.67.18	255.255.255.255	(使用不可)
138.42.67.23	255.255.255.255	(使用不可)
138.42.67.53	255.255.255.255	(使用不可)
138.42.67.54	255.255.255.255	(使用不可)
138.42.67.55	255.255.255.255	(使用不可)
138.42.67.62	255.255.255.255	(使用不可)
138.42.67.98	255.255.255.255	nclabpe2.ca.com
138.42.67.99	255.255.255.255	(使用不可)
138.42.67.105	255.255.255.255	(使用不可)
138.42.67.106	255.255.255.255	(使用不可)
138.42.67.107	255.255.255.255	(使用不可)
138.42.67.108	255.255.255.255	(使用不可)
138.42.67.109	255.255.255.255	(使用不可)

1 / 1　ページ: 1　サイズ: 100

注: セッション レベルのレポートが必要な場合は、監視デバイス として CA Multi-Port Monitor を使用します。 5 分間隔で TCP セッションをネットワーク レベルで分析する CA Standard Monitor と異なり、CA Multi-Port Monitor は、1 分間隔でサーバと特定クライアントの間の TCP セッションを分析できます。 さらに、CA Multi-Port Monitor を使用すると、TCP および非 TCP トラフィックなど、監視されているすべてのネットワーク トラフィックのトラフィック ボリュームを分析できます。

ネットワーク領域の仕組み

管理コンソール ユーザがリモート サイトのパフォーマンス問題を迅速に分析し対応できるようにするには、ユーザ環境内の実際のクライアント ネットワークに対応するクライアント ネットワークを作成します。

管理コンソール がアプリケーションと通信する実際の IPv4 ベースのクライアント IP アドレスをレポートできるようにするには、クライアント ネットワークに 24 ビット以上のサブネット マスクが必要です。

必要に応じて、管理コンソール が領域別に監視されている TCP トラフィックをレポートできるようにするには、大規模なクライアント ネットワークを小規模なネットワーク領域に変換します。 *ネットワーク領域*はクライアント ネットワークの小規模なサブネットです。たとえば、/22 のクライアント ネットワークがある場合は、それを 4 つの /24 ネットワーク領域に変換します。

ネットワークの定義	作成する領域の数
/24	1
/23	2
/22	4
/21	8
/20	16
/19	32
/18	64
/17	128
/16	256

クライアント ネットワークを領域に変換すると、管理コンソール は、定義されたクライアント ネットワーク別ではなく、領域別に監視されている TCP トラフィックをレポートします。前の例からの続きで /22 のクライアント ネットワークを /24 のネットワーク領域に変換すると、/22 のクライアント ネットワークは［環境管理］ページでのみ表示でき、レポート目的には利用できません。 レポートでは、代わりに個別のネットワーク領域を探す必要があります。

管理コンソール ユーザが、特定の /24 ネットワーク領域に対して監視されたトラフィックではなく、定義されたクライアント ネットワークにおけるアプリケーション パフォーマンスについてレポートできるようにするには、CA PC または CA NPC を使用して、すべてのネットワーク領域から成るグループを作成します。

クライアント ネットワークに対応するネットワーク領域を容易に識別するには、よく知られている命名規則を使用します。 以下の例では、Austin グループには、192.168.0.0/22 のクライアント ネットワークから変換された /24 のネットワーク領域が含まれています。

ネットワーク領域のグループについてレポートする場合、［エンジニアリング］ページのパフォーマンス詳細レポート（［レスポンス時間構成: 平均］レポートなど）には、すべての /24 ネットワーク領域からのデータが集約されます。 これに対して、［操作］ページのレポートおよび［エンジニアリング］ページのパフォーマンス マップなど、その他すべてのレポートには、/24 の各ネットワーク領域が別々にリスト表示されます。 ネットワーク グループに関するレポートの詳細については、「*ユーザ ガイド*」を参照してください。

以下の表は、いくつかのサンプル ネットワーク設定とネットワーク領域を示しています。

ネットワークの設定	/24 のネットワーク領域
名前： ABC サブネット： 10.10.1.0 マスク： 24 領域： 1 ネットワーク タイプ： 128K	10.10.1.0
名前： DEF サブネット： 10.10.0.0 マスク： 22 領域： 4 ネットワーク タイプ： 128K	10.10.0.0 10.10.1.0 10.10.2.0 10.10.3.0
名前： XYZ サブネット： 10.10.0.0 マスク： 16 領域： 256 ネットワーク タイプ： 128K	10.10.0.0 10.10.1.0 」を参照してください。 」を参照してください。 」を参照してください。 10.10.255.0

詳細:

命名規則 (P. 41)

命名規則

クライアント ネットワーク用に推奨するいくつかの命名規則を以下に示します。領域を使用してクライアント ネットワークを定義している場合、クライアント ネットワークについてレポートすることはできません。 したがって、レポートの観点からはクライアント ネットワーク領域名が重要です。

対象	使用	例:
クライアント ネットワーク	*Location-Description*	Singapore-Backbone
クライアント ネットワーク領域	*Location-Region-Bandwidth*	Austin-Subnet10-128K

クライアント ネットワークの検索

管理コンソール によって現在監視されているクライアント ネットワークを見つけるには、ネットワーク リストを検索します。 または、［エンジニアリング］ページの QoS ユーザ レポートを使用して、アプリケーションと通信しているクライアント IP を確認します (たとえば「キャッチ オール」デフォルト クライアント ネットワーク上の IP) 。

詳細:

デフォルト クライアント ネットワーク (P. 45)

ネットワーク リストの検索

すでに定義されているクライアント ネットワークを検索するには、ネットワーク リストを検索します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。
3. （オプション）検索するドメインを選択します。
4. ［ネットワーク リスト］内の青い歯車型メニュー（ ）をクリックし、［ネットワークの検索］を選択します。
5. ネットワーク名またはサブネットによって検索する場合は、ネットワーク リスト内の［検索］をクリックします。
6. ［検索対象］フィールドに検索文字列を指定します。 検索パターンの先頭または終わりに、次のものを含むパターン一致文字を指定できます。

   *

   すべての文字に一致します。

   %

   1 つの文字に一致します。
7. ［検索］をクリックして、一致するネットワークを検索します。

   注: クライアント ネットワークのプロパティを編集するためにハイパーリンクをクリックします。

詳細:

テナントの管理 (P. 113)
クライアント ネットワークの編集 (P. 53)

QoS ユーザ レポートによる不明なクライアント ネットワークの検索

通常、アドレス範囲は徐々に増大します。「すべてを捕捉する」ネットワークを作成しておけば、増大が発生した場合でも、CA Application Delivery Analysis でその増大が計算されます。広範なスーパーセット ネットワークにわたってクライアント IP のトラフィックが発生した場合は、QoS ユーザ レポートを使用して、トラフィックを示している /24 クライアント ネットワークを確認し、次に、それらのサブセット ネットワークを明示的に限定します。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. QoS ユーザ レポート内の青い歯車型メニュー（ ）をクリックし、［ユーザを一覧表示］をクリックして、クライアント ネットワーク上の監視対象トラフィックを 8 ビット以上の小さな特定サブネットでフィルタします。たとえば、192.168.0.0/16 の「キャッチ オール」ネットワークなどの /16 ネットワークについてレポートする場合、［ユーザ リスト］には、管理コンソール がクライアント IP トラフィックを検出した、対応する /24 ネットワークが表示されます。以下の例では、/24 ネットワークが 30-39 の範囲内にあることが前提になっていますが、管理コンソール により 192.168.112.0/24 のクライアント ネットワーク内に予期しないクライアント IP が確認されます。

   192.168.112.0/24 のクライアント ネットワーク内の実際のクライアント IP を確認するには、192.168.112.0/24 クライアント ネットワークを作成し、QoS ユーザ レポートを使用して /32 のユーザの IP アドレスをリスト表示します。

CA Application Delivery Analysis には、「キャッチ オール」のデフォルト クライアント ネットワークに対して以下のデフォルト エントリが含まれます。

- その他すべて： 0.0.0.0/0
- その他すべての 10 ネットワーク： 10.0.0.0/8
- その他すべての 172.16 ネットワーク： 172.16.0.0/12
- その他すべての 192.168 ネットワーク： 192.168.0.0/16

詳細:

デフォルト クライアント ネットワーク (P. 45)

クライアント ネットワークの管理

アプリケーション ポート トラフィックを監視するネットワークを指定して、クライアント ネットワークを管理します。

- 設定をすばやく行うために CSV ファイルからネットワーク情報をインポートします。
- クライアント ネットワークを追加します。
- ルータをポーリングしてネットワーク情報をインポートします。

管理コンソール へクライアント ネットワークを追加する場合は、レポートのため、およびネットワーク上でインシデント レスポンスを起動するため、ネットワーク タイプ別にクライアント ネットワークをグループ化することを計画します。

詳細:

ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)

デフォルト クライアント ネットワーク

通常、アドレス範囲は徐々に増大します。「キャッチ オール」ネットワークにより、増大が発生した場合でも、CA Application Delivery Analysis でその増大が計算できます。 クライアント IP のトラフィックが広範なデフォルト クライアント ネットワークに発生した場合は、QoS ユーザ レポートを使用して、トラフィックを示している /24 クライアント ネットワークを確認し、それらのサブセット ネットワークを明示的に定義します。

CA Application Delivery Analysis には、「キャッチ オール」デフォルト クライアント ネットワークに対して以下のデフォルト エントリが含まれます。

- その他すべて： 0.0.0.0/0
- その他すべての 10 ネットワーク： 10.0.0.0/8
- その他すべての 172.16 ネットワーク： 172.16.0.0/12
- その他すべての 192.168 ネットワーク： 192.168.0.0/16

注: クライアント ネットワークがオーバーラップする場合、管理コンソールは、より具体的なクライアント ネットワークでアプリケーション トラフィックをレポートします。

DMZ 内のインターネットにアクセスするアプリケーションは、サブネット 0.0.0.0 の「その他すべて」クライアント ネットワークで監視できます、マスク 0 は、明示的に定義されていないクライアント ネットワークに対するアプリケーション アクティビティを監視します。 他のタイプのアプリケーションを監視するためにこのクライアント ネットワークを使用しないでください。 使用すると、［操作］ページと［エンジニアリング］ページに、「正常」な基準がないためにしきい値を超えている多くの異常なクライアント IP アドレスが表示されます。

注:「その他すべて」のクライアント ネットワークでは TCP セッションを表示できませんが、管理コンソール により他のクライアント ネットワークからのアプリケーション アクティビティがレポートされます。

詳細:

ネットワーク ベース レポートの仕組み (P. 36)
クライアント ネットワークの検索 (P. 41)

CSV ファイルからのクライアント ネットワークのインポート

IPv4 クライアント ネットワークを CSV ファイルからインポートし、目的のクライアント ネットワークを容易に指定できるようにします。

最初に、IPv4 クライアント ネットワークのリストをエクスポートし（たとえば DHCP 管理ツールから）、次にリストを編集して /24 のクライアント ネットワークを記述します。

ユーザのクライアント ネットワークをインポートした後で編集せずに済むようにするため、CSV ファイルの各ネットワークのネットワーク プロパティをすべて定義することをお勧めします。 ネットワークをインポートした後は、管理コンソール からネットワークを編集する必要があり、そのプロパティを更新するために既存のネットワークを再インポートすることはできませんので注意してください。

CSV ファイルを作成するときは、ネットワーク タイプを省略しないでください。 ネットワーク タイプはアプリケーション パフォーマンスを監視する際に重要な役割を果たします。

注: CA PC または CA NPC でドメインを定義している場合、クライアント ネットワークのリストを同じドメインにインポートする必要があります。サポートされている CSV ファイル構文では、ネットワーク定義ごとにドメインを指定することができません。

詳細:

クライアント ネットワークの編集 (P. 53)
ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)

CSV ファイルの作成

監視する IPv4 クライアント ネットワークを指定する CSV ファイルを作成するには、以下の手順に従います。

CSV ファイルは、以下の要領で作成します。

- 各フィールドをカンマで区切り、カンマの後にスペースを入れないようにします。
- 埋め込まれたカンマまたは二重引用符は、二重引用符で囲みます。
- 1 つ以上のスペースが含まれる文字列は二重引用符で囲みます。例："Houston Office"。

次の手順に従ってください:

1. .csv ファイル拡張子を付けてファイルを作成します。
2. ネットワーク定義ごとに別々の行を追加します。
3. 各ネットワーク定義については、以下の形式を使用します。

   network_name,subnet,mask,regions,network_type

   以下の例で、Houston Office のエントリはネットワーク タイプを指定していないため、管理コンソール ではデフォルトで［未割り当て］になります。

   ```
   "Atlanta Lab",192.168.100.0,24,1,LAN
   "Houston Office",192.168.200.0,24,1
   ```

   network_name

   実際のクライアント ネットワークの名前を 50 文字以内で定義します。*Location-Description* などの命名規則を使用することをお勧めします。

   ネットワーク領域を使用してネットワーク サブネットを /24 のサブネットに変換することを計画している場合は、*Location-Region-Bandwidth* などの命名規則を使用することをお勧めします。

   サブネット

   ネットワークの IPv4 アドレスは、ドット付き 10 進表記法で 4 つの構成要素により定義します（例： 192.168.100.0）。

   mask

   実際のクライアント ネットワークのサブネット マスクを指定します。

管理コンソール はサーバごとに /32 ネットワークを自動的に作成し、クライアント リクエストに対応するサーバ、および別のサーバに対応するクライアントの両方として機能するサーバを監視します。

regions

（オプション）より広範なネットワーク サブネットから変換可能な /24 サブネットの数を指定します。 たとえば、ネットワーク サブネットが /22 の場合、4 つの領域は、/22 を 4 つの /24 サブネットに変換します。

network_type

（オプション）ネットワークおよびそのネットワーク領域（該当する場合）に割り当てるネットワーク タイプを指定します。 ネットワーク タイプを指定しない場合は、［未割り当て］に設定されます。

4. ファイルを保存し、管理コンソール にインポートします。

詳細:

多層アプリケーションの管理 (P. 156)
ネットワーク領域の仕組み (P. 38)
ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)

CSV ファイルのインポート

CSV ファイルを作成した後、IPv4 クライアント ネットワーク定義を 管理コンソール にインポートします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。
3. （オプション）クライアント ネットワークをインポートするドメインを選択します。

   ［ネットワーク リスト］が表示されます。
4. 青い歯車型メニュー（ ）をクリックし、［ファイルからのインポート］を選択します。

   ［ネットワーク定義のインポート］が表示されます。
5. ［参照］をクリックして CSV ファイルを選択します。
6. ［次へ］をクリックします。

   ［ネットワークのプロパティ］が表示されます。
7. CSV ファイルからインポートした定義と 管理コンソール 内の既存のネットワーク定義の間の重複をすべて解消します。 重複がある場合は以下のように強調表示されます。

   赤

   サブネット定義が、すでに定義されているサブネット定義に一致することを示します。 ネットワークを削除するか、そのサブネット定義を変更するには、赤い X （ ）をクリックします。

   同じサブネット定義は 2 回以上追加できません。たとえば、256 のクライアント領域を持った 11.2.0.0/16 ネットワークがすでに定義されている場合、11.2.3.0/24 クライアント ネットワークをインポートできません。

   黄色

   サブネット定義が、より広範な既存のサブネット定義と重複していることを示します。 より広範なサブネット定義が必要でなくなった場合は、インポートを完了した後で削除します。

管理コンソール は、重複するネットワーク定義をインポートしますが、常により限定されたネットワーク内のクライアント アクティビティをレポートします。たとえば、/24 ネットワークと重複する /26 ネットワークをインポートすると、管理コンソール は /26 のネットワーク内の一致するクライアント トラフィックをレポートします。

緑

サブネット定義が、より狭い既存のサブネット定義と重複していることを示します。 より狭いサブネット定義が必要でなくなった場合は、インポートを完了した後で削除します。

管理コンソール は、重複するネットワーク定義をインポートしますが、常により限定されたネットワーク内のクライアント アクティビティをレポートします。たとえば、/24 ネットワークと重複する /26 ネットワークをインポートすると、管理コンソール は /26 のネットワーク内の一致するクライアント トラフィックをレポートします。

8. ［OK］をクリックします。
9. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

クライアント ネットワークの追加

管理コンソール がクライアント ネットワーク全体のすべてのアプリケーション サーバのパフォーマンスを監視できるように、クライアント ネットワークを追加します。 クライアント ネットワークは特定のアプリケーション サーバには割り当てられません。

迅速かつ簡単にユーザのクライアント ネットワークをすべてインポートするには、CSV ファイルからネットワーク定義をインポートします。

クライアント ネットワークを手動で追加する方法

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。
3. （オプション）クライアント ネットワークを作成するドメインを選択します。
4. ［表示項目］メニュー下で、IPv4 クライアント ネットワークをクリックして追加します。
5. ［ネットワークのプロパティ］の各フィールドに入力してから、［OK］をクリックします。

   ネットワーク プロパティの詳細については、［ヘルプ］をクリックしてください。
6. CSV ファイルからインポートした定義と 管理コンソール 内の既存のネットワーク定義の間の重複をすべて解消します。 重複がある場合は以下のように強調表示されます。

   赤

   サブネット定義が、すでに定義されているサブネット定義に一致していることを示します。 ネットワークを削除するか、そのサブネット定義を変更するには、赤い X （  ）をクリックします。

   既存のサブネット定義を置き換えることはできません。たとえば、256 のクライアント領域を持った 11.2.0.0/16 ネットワークがすでに定義されている場合、11.2.3.0/24 クライアント ネットワークをインポートできません。

   黄色

サブネット定義が、より広範な既存のサブネット定義と重複していることを示します。 より広範なサブネット定義が必要でなくなった場合は、インポートを完了した後で削除します。

管理コンソール は、互いに重複するネットワーク定義をインポートしますが、より限定されたネットワーク内のクライアント アクティビティを常にレポートします。たとえば、/24 ネットワークと重複する /26 ネットワークをインポートすると、管理コンソール は /26 のネットワーク内の一致するクライアント トラフィックをレポートします。

緑

サブネット定義が、より狭い既存のサブネット定義と重複していることを示します。 より狭いサブネット定義が必要でなくなった場合は、インポートを完了した後で削除します。

管理コンソール は、重複するネットワーク定義をインポートしますが、常により限定されたネットワーク内のクライアント アクティビティをレポートします。たとえば、/24 ネットワークと重複する /26 ネットワークをインポートすると、管理コンソール は /26 のネットワーク内の一致するクライアント トラフィックをレポートします。

7. ［OK］をクリックします。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
CSV ファイルからのクライアント ネットワークのインポート (P. 46)

クライアント ネットワークの編集

クライアント ネットワークまたはその領域の 1 つを編集するには、［ネットワーク リスト］を使用します。 管理コンソール がネットワーク上のトラフィックを検出した後で、IP アドレスまたはサブネット マスクを変更することはできません。

ネットワークが割り当てられているドメインは変更できませんので注意してください。 必要な場合は、クライアント ネットワークを削除し、次に、正しいドメインを使用してクライアント ネットワークを再作成します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

   ［ネットワーク リスト］が表示されます。
3. （オプション）編集するクライアント ネットワークが含まれるドメインを選択します。
4. ネットワークを編集するために編集アイコン ( ) をクリックします。
5. ［ネットワークのプロパティ］の各フィールドに入力してから、［OK］をクリックします。

   ネットワーク プロパティの詳細については、［ヘルプ］をクリックしてください。
6. （オプション）特定のネットワーク領域を編集する方法
   a. + をクリックして、クライアント ネットワーク用の領域のリストを展開します。
   b. ［ネットワーク リスト］で、ネットワーク領域の名前を変更するか、またはネットワーク タイプを割り当てます。
   c. ［OK］をクリックします。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

クライアント ネットワークの削除

クライアント ネットワーク上の TCP セッションの監視を停止するには、クライアント ネットワークを削除します。 既存のネットワーク データは、引き続きレポート目的に利用可能です。

クライアント ネットワークを削除する場合は、以下を削除できないことに注意してください。

- クライアント ネットワークからのネットワーク領域。ユーザがクライアント ネットワークを削除すると、そのネットワーク領域がすべて削除されます。
- 管理コンソールによって自動的に作成された /32 または /128 クライアント ネットワーク。 対応するサーバをサーバ リストから削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

   ［ネットワーク リスト］が表示されます。
3. （オプション）削除するクライアント ネットワークが含まれるドメインを選択します。
4. ［ネットワーク リスト］で、ネットワークを削除するために赤い X（）をクリックします。
5. ［削除の確認］プロンプトで、［削除を続行］をクリックします。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
/32 クライアント ネットワークの仕組み (P. 82)

ルータに対するクライアント ネットワークの SNMP ポーリング

ルータに対して IPv4 ネットワーク定義の SNMP ポーリングを実行し、結果を 管理コンソール にインポートします。管理コンソール がルータに対してポーリングを行っている間は、管理コンソール 内で他のタスクを実行することはできませんので注意してください。

ルータのネットワーク情報をクエリする場合は、ルート コストがゼロの直接接続されたネットワークのインポートを試行してください。 たとえば、リモートサイトの単一のルータをポーリングすることで、1 つのサイトで 6 ～ 7 個のルータをポーリングする代わりに、LAN タイプのコストのかかるすべてのネットワーク（たとえば 5 個、10 個または 18 個未満）を取得します。 ［最大コスト］を使用すると、取得されるネットワークがローカル ネットワークに制限されるため、それらを特定のリモートサイトに関連付けることができます。そのためには、たとえば標準的な命名規則に従い、ネットワーク タイプを使用してネットワークをグループ化します。

管理コンソール が SNMP ポーリングできるようにするには、割り当てられた SNMP プロファイルを使用するネットワーク デバイスをルータに追加します。デバイスへ SNMP プロファイルを割り当てない場合は、管理コンソール は利用可能な SNMP プロファイルのリストから有効な SNMP プロファイルを検出しようとします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。
3. （オプション）クライアント ネットワークをインポートするドメインを選択します。
4. ［ネットワーク リスト］で、青い歯車型メニュー（ ）をクリックし、［SNMP からのインポート］を選択します。

   ［ネットワーク定義のインポート］が表示されます。
5. フィールドに入力し、［ポーリング］をクリックします。

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

［ポーリングの確認］メッセージにより、ポーリングに数分かかる可能性があることがユーザに通知されます。管理コンソール がルータに対してポーリングを行っている間は、管理コンソール 内で他のタスクを実行することはできませんので注意してください。

6. ［ポーリングの確認］で［続行］をクリックします。
7. 管理コンソール がポーリングを完了したら、［ステータス ウィンドウを閉じる］をクリックして結果を表示します。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
ネットワーク デバイスの管理 (P. 274)

CSV ファイルへのクライアント ネットワークのエクスポート

既存のクライアント ネットワークを 管理コンソール から CSV ファイルにエクスポートする場合、たとえば、ネットワークのフォーマットされたリストが生成されるので、これを編集して 管理コンソール にインポートすることができます。 管理コンソール では既存のクライアント ネットワークを再インポートできないことに注意してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

   ［ネットワーク リスト］が表示されます。
3. （オプション）クライアント ネットワークをエクスポートするドメインを選択します。
4. 青い歯車型メニュー( )をクリックし、［ネットワークのエクスポート］を選択します。
5. ［ファイルのダウンロード］ダイアログ ボックスでオプションを選択します。
   - Microsoft Excel でファイルを開くには、［開く］をクリックします。
   - ファイルを保存するには、［保存］をクリックします。 ［名前を付けて保存］ダイアログ ボックスで、ファイルのディレクトリおよびファイル名を選択し、［保存］をクリックします。

詳細:

テナントの管理 (P. 113)

ネットワーク タイプ別のクライアント ネットワークのグループ化

ネットワーク タイプを使用すると、類似の遅延特性を持ったクライアント ネットワークをグループ化、管理できます。 たとえば、Cary のサイトのクライアント ネットワークをグループ化し、管理コンソール がそのサイトのパフォーマンスを管理する方法をカスタマイズできます。

デフォルトでは、CA Application Delivery Analysis にはあらかじめ設定された VPN およびワイヤレス ネットワーク タイプが含まれます。 VPN およびワイヤレス ネットワーク タイプに対するパフォーマンスしきい値は、その他のタイプのネットワーク感度の 2 分の 1 に設定されます。これは遅延が増加するためです。

ネットワーク タイプの仕組み

*ネットワーク タイプ*の本質はネットワークのグループです。 このグループは、クライアント ネットワーク上のユーザによって経験された遅延を反映している必要があります。

一般的に、遅延の最大要因はサブネットの地理的場所および帯域幅です。管理コンソール では、T1 などの帯域幅を指定するためにデフォルト ネットワーク タイプが取り込まれます。ただし、管理コンソール は、アプリケーション トラフィックを監視する 監視デバイス からの相対パスを使用してネットワークの場所を想定することはできません。 そのため、長さ 200 マイルである T1 と長さ 1,500 マイルである T1 とではパフォーマンスに大きな違いがあるので、ネットワーク タイプを組織のレイアウトに合わせてカスタマイズすることが重要です。

必要なネットワーク タイプの数は、組織のサイズによって決まります。ネットワーク タイプは、同じネットワーク パスを介して通信するために同じ遅延が発生する必要があるサブネットをグループ化するのに使用します。 基本方針としては、ネットワーク タイプは、同じ物理ネットワーク リソースを共有するために距離、シリアル化、およびキューイング遅延のために同じ遅延が発生するサブネットのグループにする必要があります。 正確なネットワーク図があることは、ネットワーク タイプを構築するうえで非常に役に立ちます。

注: デフォルトでは、CA Application Delivery Analysis には、遅延が著しく変動するネットワークからのユーザに対してあらかじめ設定された VPN およびワイヤレス ネットワーク タイプが含まれます。 VPN およびワイヤレス ネットワーク タイプ用のパフォーマンスしきい値は、その他のネットワーク タイプの感度の 2 分の 1 にあらかじめ設定されています。 管理者は、管理コンソール がチームによって解決可能なインシデントのみを作成するようにします。 この場合、ロンドンやシンガポールのホテルなどからインターネットでネットワークにアクセスするリモート ユーザで発生する遅延問題を解決するのは困難です。

詳細:

パフォーマンスしきい値の編集 (P. 178)

ネットワーク タイプが有用な理由

ネットワーク タイプは、いくつかの利点を提供します。

- レポート用にクライアント ネットワークを自動的にグループ化します。 CA PC または CA NPC のデータ ソースとして定義されている場合、定義するネットワーク タイプごとに［ネットワーク地域タイプ］システム グループが作成されます。

  ネットワーク タイプをクライアント ネットワークに割り当てない場合、CA PC または CA NPC にグループを作成し、管理コンソール および CA PC または CA NPC 内のクライアント ネットワークのグループについてレポートできます。

  リモート サイトを管理するために CA PC または CA NPC にルール ベースのサイト グループを実装することを考慮します。

- ネットワーク タイプ別にパフォーマンスのしきい値を調整し、同じアプリケーションについて、クライアント ネットワークによってしきい値を高めか低めにします。

  管理コンソール は、すべてのアプリケーション ポート、サーバおよびクライアント ネットワークの間の全 TCP セッションについて、感度のしきい値を計算します。 ただし、ネットワーク タイプを使用すれば、特定のネットワーク グループ上のアプリケーションの感度を調整することができます。

  静的なしきい値を使用することを計画している場合は、ネットワーク タイプを使用することで、特定のネットワーク グループ上で静的なしきい値を設定できます。

- ネットワーク タイプによってネットワーク インシデント レスポンスをカスタマイズします。 以下に例を示します。

  - 電子メールまたは SNMP トラップによって該当のユーザに通知する。
  - 特定のネットワーク グループ上のネットワーク インシデントに応じてトレース ルート調査を起動する。

- リモート ネットワークとローカル ネットワークが個別のパフォーマンス OLA（運用レベル契約）しきい値を持てるように、ネットワーク タイプ別にパフォーマンス OLA を作成します。ネットワーク タイプを使用して類似の遅延があるネットワークをグループ化すると、ネットワーク タイプ別に OLA を設定できるので、ネットワーク ラウンドトリップ時間と合計トランザクション時間のメトリックについて OLA を正しく設定できるようになります。

詳細:

パフォーマンスしきい値の管理 (P. 165)
アプリケーション パフォーマンス OLA の管理 (P. 225)

ネットワーク タイプの追加

リモートサイトのクライアント ネットワークのグループなど、共通の遅延特性を共有するクライアント ネットワークのグループを識別するためのネットワーク タイプを追加します。これは、ドメイン コントローラへの同じ物理パスを共有します。

グループ化するクライアント ネットワークが含まれるリモート サイトと同じ名前を使用して、ネットワーク タイプの名前を付けます。ネットワーク タイプを命名するときは、TCP パケットがクライアントとサーバ間でたどるネットワーク パスを 管理コンソール が判定できないことに注意してください。 たとえば、128 Kbps 回線を使用する Austin の Subnet 10 ネットワークと Subnet 50 ネットワーク用にネットワーク タイプを作成する場合は、ネットワーク タイプを Austin と命名します。

デフォルトでは、管理コンソール は、クライアント ネットワークを［未割り当て］ネットワーク タイプに割り当てます。 ネットワーク タイプを実装する場合は、デフォルト ネットワーク タイプではなく、ネットワーク グループの共通の遅延特性を表すネットワーク タイプをクライアント ネットワークに割り当てます。

注: クライアント ネットワークを作成する最も容易な方法は、ネットワークおよび関連するネットワーク タイプ情報の Excel チャート（リスト）を作成し、CSV ファイルとして 管理コンソール にインポートすることです。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク タイプ］をクリックします。
3. ［表示項目］メニュー下の［ネットワーク タイプの追加］をクリックします。
4. ［ネットワーク タイプのプロパティ］の各フィールドに入力してから、［OK］をクリックします。

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

詳細:

CSV ファイルのインポート (P. 49)
クライアント ネットワークへのネットワーク タイプの割り当て (P. 66)

ネットワーク タイプの編集

ネットワーク タイプの名前またはネットワーク インシデント レスポンスを変更するには、ネットワーク タイプを編集します。 ネットワーク タイプへの変更は、そのネットワーク タイプが割り当てられている、当該のクライアント ネットワークに適用されます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク タイプ］をクリックします。
3. ［ネットワーク タイプ］で、ネットワーク タイプを編集するための編集アイコン（）をクリックします。
4. ［ネットワーク タイプのプロパティ］の各フィールドに入力してから、［OK］をクリックします。

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

詳細:

インシデント レスポンスの管理 (P. 195)

ネットワーク タイプの削除

ネットワークに割り当てられているネットワーク タイプを削除すると、管理コンソール は自動的にデフォルト ネットワーク タイプの［未割り当て］をクライアント ネットワークに再割り当てします。 ［未割り当て］ネットワーク タイプにはインシデント レスポンスを割り当てることができることに注目してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク タイプ］をクリックします。
3. ネットワーク タイプを削除するために赤い X () をクリックします。
4. ［削除を続行］をクリックし、ネットワーク タイプを削除することを確認します。

   管理コンソール は、削除されたネットワーク タイプに以前割り当てられていたネットワークに、［未割り当て］ネットワーク タイプを割り当てます。

詳細:

ネットワーク タイプの編集 (P. 64)

クライアント ネットワークへのネットワーク タイプの割り当て

ネットワーク インシデントに応じて特定のアクションを起動するクライアント ネットワークにネットワーク タイプを割り当てます。 ネットワーク タイプを以下に割り当てることをお勧めします。

- クライアント ネットワーク。 ネットワーク タイプにインシデント レスポンスを割り当てるときは、そのネットワーク タイプを割り当てているすべてのクライアント ネットワーク上のネットワーク インシデントに対して、管理コンソール が指定されたアクションを開始しますので注意してください。

  管理コンソール にクライアント ネットワークを追加するときは、必ずネットワーク タイプも割り当ててください。デフォルトでは、管理コンソール は、新しいクライアント ネットワークにネットワーク タイプを割り当てません。 必要な場合は、1 つ以上のクライアント ネットワークを編集してネットワーク タイプを割り当てることができます。

- サーバ サブネット。 管理コンソール は、指定されたネットワーク タイプを、対応するサーバ トラフィックから作成された /32 および /128 クライアント ネットワークに自動的に割り当てます。

詳細:

/32 クライアント ネットワークの仕組み (P. 82)
クライアント ネットワークの編集 (P. 53)
サーバ サブネットの編集 (P. 87)

Web サービス メソッドを使用したクライアント ネットワークの管理

管理コンソール の設定およびレポートのための 3 大エレメントであるアプリケーション、ネットワークおよびサーバのうち、ネットワークは最も数が多く、保守が困難です。

Web サービス メソッドを使用し、管理コンソール によってネットワークを追加する代わりに、Network Configuration Service アプリケーション プログラミング インターフェース（API）を使用して、プログラムによってネットワーク定義の作成、読み取り、更新、削除を行うことができます。

Web サービス メソッドを使用したネットワークの設定の詳細については、以下のセクションを参照してください。

パラメータ説明

以下のセクションでは、説明されている Web サービス メソッドを通じて使用されるパラメータについて説明します。

ClientId

タイプ： 符号なしの 4 バイト整数

定義： ネットワーク定義識別子（クライアント テーブル エントリ）。 設定されているサブ領域の数に応じて、通常、複数のネットワーク（client_cache テーブル エントリ）にマップされます。

［環境管理］ページの［ネットワーク リスト］内の各ネットワーク定義には、一意のクライアント ID がありますが、このクライアント ID は表示されません。

ClientSetId

タイプ： 符号なしの 4 バイト整数

定義： この定義が属するネットワーク セット。 このフィールドは表示されず、常にデフォルトで最初のアクティブなクライアント セット識別子に設定されます。

説明

タイプ： 50 文字以内の文字列（latin1）

定義： 追加するネットワーク定義のユーザ指定ラベル。

各ネットワーク定義の説明は、［環境管理］ページ内の［ネットワーク リスト］の［ネットワーク］列にリストされます。

NetworkType

タイプ： 50 文字以内の文字列（latin1）

定義： 定義に割り当てられているタイプを識別します。定義が必要でない場合は、空/Null/*未割り当て*として識別します。 このパラメータは一致するうえで大文字と小文字を区別しません。 一致がない場合は、新しいネットワーク タイプが追加されます。

各ネットワーク定義に関連付けられているネットワーク タイプは、［環境管理］ページの［ネットワーク リスト］内の［ネットワーク タイプ］列に表示されます。 定義がネットワーク タイプに割り当てられていない場合、定義は未割り当てとしてマークされます。

領域

タイプ： 1 ～ 256 の間の、2 の累乗の整数。領域はサブネット マスクの選択によって制限されます。たとえば、/31 は 2 つのサブ領域にのみ展開できます。

定義： この定義を展開できるサブ領域の数。

各ネットワーク定義が展開されるサブ領域の数は、［環境管理］ページの［ネットワーク リスト］内の［領域］列に表示されます。 表示される領域は最小に設定されます。つまり、1 つの定義あたり 1 つの領域が表示されます。

サブネット

タイプ： x.x.x.x/m 形式の文字列。x.x.x.x は有効な IP アドレスで、m は 1 ～ 32 の整数です。

定義： このネットワーク定義に対するサブネットのアドレスおよびマスク。

必要なアドレス/マスク入出力形式でのネットワーク定義のサブネットは、［ネットワーク リスト］の［サブネット］列に表示されます。

Web サービス メソッド

このセクションでは、Web サービス メソッドについて説明します。

詳細:

エラー レポートの仕組み (P. 73)

InsertNetworkDefinition

目的： ネットワーク定義を作成します。

［環境管理］ページの［ネットワークのプロパティ］内のサブミットされた新しいエントリはそれぞれ、1 つのメソッド コールに相当します。

入力パラメータ：

- 説明（オプション）
- サブネット（必須）
- 領域（必須）
- NetworkType（オプション。空の値は*未割り当て*と同等）

戻り値： ルート ノード *InsertNetworkDefinition*、および挿入されたネットワークの新しく作成された ClientId が含まれる *ClientId* エレメントで構成される XML ドキュメント。 失敗した場合は、ClientId はゼロになります。

返されるエラー： 標準エラー レポートが提供されます。

UpdateNetworkDefinition

目的： 渡されたクライアント ID によって識別されるネットワーク定義を変更します（サブネット説明、IP アドレスおよびマスクを含む）。

［環境管理］ページのネットワーク定義編集はそれぞれ 1 つのメソッド コールに相当します。

入力パラメータ：

- ClientId（必須）
- 説明（オプションですが、空の値を指定すると古い説明が消去されます）
- 領域（必須）
- NetworkType（オプション。空の値は*未割り当て*と同等、新しい値を指定すると新しい NetworkType が作成されます）

戻り値： 更新の成功または失敗を示す true または false。

返されるエラー： 標準エラー レポートが提供されます。

DeleteNetworkDefinition

目的： 渡されたクライアント ID によって識別されるネットワーク定義を削除します。内部では、クライアント ネットワークは*非アクティブ*とマークされます。 すでに削除されているネットワークを削除すると、*false* の戻りコードが返されます。

［環境管理］ページでは、［ネットワーク リスト］からネットワークを削除することは 1 つのメソッド コールに相当します。

入力パラメータ： ClientId （必須）

戻り値： ルート ノード *DeleteNetworkDefinition*、および削除された ClientId が含まれる *ClientId* エレメントで構成される XML ドキュメント。

返されるエラー： 標準エラー レポートが提供されます。

NetworkDefinitionsList

目的： クライアント ID によってネットワーク定義を取得します。

［環境管理］ページの［ネットワーク リスト］には、デフォルト ネットワーク セットからのすべてのネットワーク定義が含まれます。

入力パラメータ： なし。

戻り値： ネットワーク定義ごとに 1 つのエントリが含まれる XML ドキュメント。 エントリにはそれぞれ以下のパラメータが含まれます。

- ClientId
- 説明
- NetworkType
- サブネット
- 領域

返されるエラー： 標準エラー レポートが提供されます。

ReloadCollectors

目的: 設定データを選択して再起動するために、すべての 監視デバイス のリセットをトリガします。

［環境管理］ページの［表示項目］メニューで、［データ監視］、［監視デバイス］の順にクリックします。 ［ADA 監視デバイス リスト］で、青い歯車型メニュー（ ）をクリックし、［監視デバイスを同期］を選択します。

入力パラメータ： なし

戻り値： ルート ノード *ReloadCollectors*、および各 監視デバイス のステータス レポート用の *Collector* エレメントで構成される XML ドキュメント。 Status/Message 属性は、再ロード プロセスの成功を示します。同期の結果については、各 監視デバイス を個別にチェックしてください。

返されるエラー： 標準エラー レポートが提供されます。

ShowVersion

目的: この API の文字列/数値のバージョン番号を表示します。このメソッドはこの Web サービス API にのみ適用可能です。

入力パラメータ： なし。

戻り値： 文字列としてのバージョン番号。

返されるエラー： 標準エラー レポートが提供されます。

Web サービス API をテストする方法

Network Configuration Service API をテストおよびアクセスし、ネットワーク定義をプログラムによって管理します。

次の手順に従ってください:

1. http://localhost/SuperAgentWebService/NetworkConfigService.asmx に移動します。このサイトは、NetworkConfigService およびそのサービス定義への有益なユーザ インターフェースです。

   NetworkConfigService テスト サイトに、アクセス可能なリモート コンピュータからアクセスするには、localhost を <ADA_Server_FQDN> に置き換えます。
2. 失敗の追加の説明メッセージについては、SuperAgent NwkConfig WS 下の Application EventLog を参照してください。
3. スクリプトによる操作については、サンプル Perl スクリプト (P. 74) を参照して API の演習を行ってください。

詳細:

サンプル Perl スクリプト (P. 74)

エラー レポートの仕組み

ShowVersion() 以外のインターフェースはすべて XmlDocument オブジェクトを返します。 ドキュメントのルート ノードは、NetworkDefinitionsList または UpdateNetworkDefinition のように、メソッドにちなんで命名されます。以下の属性がこのルート ノードに付けられています。

- ステータス： 実行が成功したかどうかを示す True または False の文字列のリテラル。 ReloadCollectors() については、True ステータスは操作が成功したことを必ずしも意味しません。これは、監視 がオフラインか利用不可能なとき、再ロードで内部的に例外がレポートされない場合があるためです。
- メッセージ： 失敗の特定のエラー メッセージが含まれる文字列。 操作が成功した場合は、メッセージは空です。 スタック トレースを含む完全な詳細が Windows EventLog 内に表示されます。

以下の例はオブジェクトと属性を示しています。

```
<NetworkDefinitionsList Status="True" Message="">
  <Network>
  <ClientId>3</ClientId>
  <Description>192.168.0.2</Description>
  <SubnetMask>192.168.0.2/32</SubnetMask>
  <Regions>1<_/Regions>
  </Network>
</NetworkDefinitionsList>

<?xml version="1.0" encoding="utf-8" ?> <ReloadCollectors Status="False"
Message="Can't connect to MySQL server on 'localhost' (10061)" />
<?xml version="1.0" encoding="utf-8" ?> <UpdateNetworkDefinition Status="True"
Message=""><ClientId>7</ClientId></UpdateNetworkDefinition>
<?xml version="1.0" encoding="utf-8" ?> <InsertNetworkDefinition Status="True"
Message=""><ClientId>8</ClientId></InsertNetworkDefinition>
```

サンプル Perl スクリプト

```
##########################################################################
##############
##########################################################################
# Network Configuration API の演習を行うためのサンプル Perl スクリプト
# CA
##########################################################################
#
##########################################################################
# 注: ADA コンソールがホストされる場所を指すように $url を変更してください。
##########################################################################
#
##########################################################################
#!/usr/local/bin/perl
use Data::Dump qw(dump);
use SOAP::Lite (
#       +trace => all,
        maptype => {}
);
$SOAP::Constants::DO_NOT_USE_CHARSET = 1;
#
#
##########################################################################
my $uri = "http://www.netqos.com/networkconfig";
my $url = "http://localhost/SuperAgentWebService/NetworkConfigService.asmx";
#
my ($method, $result, $networks, @nodes, @params);
my ($clientId, $description, $subnetCidr, $regionCount, $networkType);
#
sub SOAP::Transport::HTTP::Client::get_basic_credentials {
   return $user => $pass;
}
#
##########################################################################
my $soap = SOAP::Lite
    -> uri($uri)
    -> on_action( sub { join '/', @_ } )
    -> proxy($url);
#
#
##########################################################################
# NetworkDefinitionsList
##########################################################################
$method = SOAP::Data->name('NetworkDefinitionsList')->attr({xmlns => $uri});
$networks = $soap->call($method);
print "¥nNetworkDefinitionsList:¥n";
```

```
if ($networks->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
   if ($networks->dataof('//NetworkDefinitionsList')->{_attr}->{Status} eq
"False") {
        print $network->dataof('//NetworkDefinitionsList')->{_attr}->{Message},
"¥n";
   } else {
    print "¥n¥nClientID¥tDescription¥tSubnet¥t¥tRegions¥t¥tNetworkType¥n";
    @nodes = $networks->valueof('//Network');
    foreach $n (@nodes)
    {
       print $n->{'ClientId'}, "¥t", $n->{'Description'},"¥t¥t",
       $n->{'Subnet'},"¥t¥t", $n->{'Regions'}, $n->{'NetworkType'},"¥t", "¥n";
    }
  }
}
#
################################################################################
# UpdateNetworkDefinition
################################################################################
print "¥n¥nUpdateNetworkDefinition:¥n";
$method = SOAP::Data->name('UpdateNetworkDefinition')->attr({xmlns => $uri});
$clientId = $networks->valueof('//Network/ClientId');
$description = $networks->valueof('//Network/Description') . " UPDATED";
$description = substr($description, 0, 50);
$regionCount = $networks->valueof('//Network/Regions');
$networkType = "unassigned";
@params = ( SOAP::Data->name(ClientId => $clientId),
        SOAP::Data->name(Description => $description),
        SOAP::Data->name(Regions => $regionCount),
        SOAP::Data->name(NetworkType => $networkType)
);
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
   if ($result->dataof('//UpdateNetworkDefinition')->{_attr}->{Status} eq "False")
{
        print $result->dataof('//UpdateNetworkDefinition')->{_attr}->{Message};
   } else {
       print "UpdateNetworkDefinition($clientId, $description, $regionCount,
$networkType):¥n";
       print dump($result->result), "¥n";
   }
}
#
################################################################################
# DeleteNetworkDefinition
```

```
################################################################################
print "¥n¥nDeleteNetworkDefinition:¥n";
$method = SOAP::Data->name('DeleteNetworkDefinition')->attr({xmlns => $uri});
$clientId = $networks->valueof('//Network/ClientId');
$description = $networks->valueof('//Network/Description');
@params = (SOAP::Data->name(ClientId => $clientId)->attr({xmlns => $uri}));
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
   if ($result->dataof('//DeleteNetworkDefinition')->{_attr}->{Status} eq "False")
{
        print $result->dataof('//DeleteNetworkDefinition')->{_attr}->{Message};
   } else {
    print "DeleteNetworkDefinition($clientId, $description):¥n";
    print dump($result->result), "¥n";
   }
}
#
################################################################################
# InsertNetworkDefinition
################################################################################
print "¥n¥nInsertNetworkDefinition:¥n";
$method = SOAP::Data->name('InsertNetworkDefinition')->attr({xmlns => $uri});
$description = $networks->valueof('//Network/Description');
$subnetCidr = $networks->valueof('//Network/Subnet');
$regionCount = $networks->valueof('//Network/Regions');
$networkType = "unassigned";
@params = ( SOAP::Data->name(Description => $description),
        SOAP::Data->name(Subnet => $subnetCidr),
        SOAP::Data->name(Regions => $regionCount),
        SOAP::Data->name(NetworkType => $networkType)
);
$result = $soap->call($method => @params);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
   if ($result->dataof('//InsertNetworkDefinition')->{_attr}->{Status} eq "False")
{
        print $result->dataof('//InsertNetworkDefinition')->{_attr}->{Message};
   } else {
    print "InsertNetworkDefinition($description, $subnetCidr, $regionCount,
$networkType):¥n";
    print dump($result->result), "¥n";
   }
}
#
#
################################################################################
```

```
# ReloadCollectors
################################################################################
$method = SOAP::Data->name('ReloadCollectors')->attr({xmlns => $uri});
print "¥n¥nReloadCollectors():....¥n";
$result = $soap->call($method);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
   if ($result->dataof('//ReloadCollectors')->{_attr}->{Status} eq "False") {
        print $result->dataof('//ReloadCollectors')->{_attr}->{Message};
   } else {
      @nodes = $result->valueof('//Collector');
      foreach $node (@nodes)
      {
         print $node->{'Address'}, "¥t", $node->{'Status'}, "¥t",$node->{'Info'},
"¥n";
      }
   }
}
#
#
################################################################################
# ShowVersion
################################################################################
$method = SOAP::Data->name('ShowVersion')->attr({xmlns => $uri});
print "¥n¥nShowVersion():¥n";
$result = $soap->call($method);
if ($result->fault) {
    print join ', ', $result->faultcode, $result->faultstring, $result->faultdetail;
} else {
    print $result->result, "¥n";
}

#
```

第 3 章: サーバの管理

このセクションには、以下のトピックが含まれています。

サーバの仕組み (P. 79)
サーバ サブネットの管理 (P. 84)
サーバの管理 (P. 89)
サーバへの監視フィードの固定 (P. 102)
サーバ保守のスケジュール (P. 103)

サーバの仕組み

server には、監視するサーバ IPv4 アドレスを指定します。管理コンソールは、サーバ サブネットを監視するように設定されたときに、最適に動作します。 サーバ サブネットは、管理コンソール で監視するサーバ IPv4 アドレスの範囲を指定し、一致するサーバ上のアプリケーション トラフィックを 管理コンソール が自動的に監視できるようにします。

デフォルトでは、管理コンソール は、サブネット 0.0.0.0 マスク 0 上の「*すべてのサーバを監視*」と呼ばれる事前定義済みサーバ サブネットを自動的に監視します。 新しい監視を追加すると、デフォルトの「*すべてのサーバを監視*」サブネットは自動的なデータ収集を有効にします。

詳細:

管理コンソールによるデータベース増加の管理方法 (P. 296)

サーバ サブネット リストの仕組み

管理コンソールによって監視されるサーバ IP アドレスの範囲を識別するサーバ サブネットを指定するには、サーバ サブネット リストを使用します。 指定したサーバ サブネットに基づいて、監視デバイス がサーバとクライアント ネットワーク間の一致するアプリケーション トラフィックを観測すると、管理コンソール はサーバに 監視デバイス を割り当てて、サーバ リストにそのサーバを追加します。 手動でサーバ リストにサーバを追加することもできます。

デフォルトでは、管理コンソール は、サブネット 0.0.0.0 マスク 0 上の「*すべてのサーバを監視*」と呼ばれる事前定義済みサーバ サブネットを自動的に監視します。 新しい監視を追加すると、デフォルトの「*すべてのサーバを監視*」サブネットは自動的なデータ収集を有効にします。

サーバ リストの仕組み

管理コンソール によって監視されるサーバを表示し管理するには、サーバ リストを使用します。 管理コンソール は、自動的にサーバ リスト内の各サーバ上のアプリケーション トラフィックをすべて監視します。

通常、サーバ リストには、サーバ サブネット リスト内の指定された IP アドレスの範囲に対応するサーバが入力されます。 必要な場合は、管理コンソール で監視する特定のサーバを追加すると、管理コンソール により、すぐにサーバ リストにサーバが追加されます。

CA PC または CA NPC にデータ ソースとして登録されている場合、CA PC または CA NPC はレポート用にサーバを自動的にグループ化します。

詳細:

サーバ サブネットの管理 (P. 84)
システム グループ (P. 257)

/32 クライアント ネットワークの仕組み

サーバが[サーバ リスト]に追加されると、管理コンソール は対応する /32 クライアント ネットワークを自動的に作成します。 /32 クライアント ネットワークは単一の IPv4 アドレスを持ったクライアント ネットワークです。

多層アプリケーションを監視するために、/32 クライアント ネットワークを使用します。 多層アプリケーションは複数のサーバを使用するアプリケーションで、サーバ間の通信は、クライアントへのリクエストを処理するサーバとして機能すると同時に共に別のサーバのクライアントとしても機能するサーバによって実行されます。

管理コンソール ユーザが多層アプリケーションに関するネットワーク問題を迅速に分析し対応できるようにするには、/32 クライアント ネットワークにネットワーク タイプを割り当てます。

サーバ サブネットを追加すると、管理コンソール が対応する /32 クライアント ネットワークを作成するときに正しいネットワーク タイプが割り当てられるように、デフォルト ネットワーク タイプを割り当てることができます。

管理コンソール によって作成された /32 クライアント ネットワークは削除できません。/32 クライアント ネットワークの対応するサーバがサーバ リストから削除されると、管理コンソール は自動的にその /32 クライアント ネットワークを削除します。

詳細:

クライアント ネットワークの仕組み (P. 34)
多層アプリケーションの管理 (P. 156)

TCP セッション ID

管理コンソール がサーバからのアプリケーション レスポンス時間を正確にレポートできるようにするには、監視デバイス は、クライアント/サーバ TCP セッションのサーバ側を識別できる必要があります。監視デバイスは、TCP セッションのどの 2 つのエンドポイントがサーバ側を表すか決定するために以下の基準を使用します。

- 新しい TCP セッション。 新しい TCP 通信のサーバ側を識別するために、SYN 受信者である IP アドレスがサーバ サブネット定義と照合されます。SYN 受信者の IP アドレスが、指定されたサーバ サブネットのいずれかにある必要があります。 SYN および SYN-ACK の両方を観測する必要があります。
- 既存の TCP セッション（TCP 接続セットアップが確認されなかった通信のトラフィック）。 どちらのエンドポイント IP もサーバ サブネットの 1 つの指定範囲以内にない場合は、通信が無視されます。

  2 つの IP アドレスの 1 つのみがサーバ サブネットの範囲内にある場合、そのエンドポイントはサーバであると推定されます。

  IP アドレスが 1 つ以上のサーバ サブネットから成る範囲内にあり、どれも有名なアプリケーションとして記録されていない場合、監視デバイス は最も小さい番号のポートがサーバであると仮定します。

ホスト名の解決

管理コンソール が CA PC または CA NPC にデータ ソースとして登録されている場合、CA PC または CA NPC は、プロキシ サーバを使用して、管理コンソール がサーバを［サーバ リスト］に追加すると自動的に DNS にクエリを実行します。 または、管理コンソール はデフォルト ポート、UDP-53 でその DNS サーバにルックアップ要求を送信します。

以下の操作を行う場合、管理コンソール が自動的にサーバのホスト名を解決することはありません。

- 手動によるサーバの追加
- サーバのリストのインポート

サーバのホスト名を手動で解決するには、サーバのプロパティを編集します。

詳細:

サーバの管理 (P. 89)
コンソール設定の管理 (P. 267)

サーバ サブネットの管理

サーバ サブネットは、監視するサーバ IP アドレスの連続した範囲を指定します。 監視デバイス が、指定されたサーバ サブネットに一致するアプリケーション トラフィックを観測した場合、管理コンソール は以下を実行します。

- 一致するすべてのシステム アプリケーションにサーバを追加します。
- サーバ リストにサーバを追加します。サーバ リストでは、たとえばインシデント レスポンスを割り当てるために、サーバのプロパティを表示および管理できます。
- サーバを /32 または /128 クライアント ネットワークとしてネットワーク リストに追加します。

ユーザのサーバ VLAN 定義と厳密に一致するサーバ サブネットを CA Application Delivery Analysis に追加することをお勧めします。管理コンソール が各サーバ サブネット上で監視する TCP ポートを制限するには、サーバ サブネットにポート除外を割り当てます。

Application Delivery Analysis には、サブネット 0.0.0.0 マスク 0 上に「*すべてのサーバを監視*」と呼ばれるデフォルトのサーバ サブネットが含まれます。 新しい監視を追加すると、デフォルト サーバ サブネットは自動的なデータ収集を有効にします。

詳細:

/32 クライアント ネットワークの仕組み (P. 82)
アプリケーション ポート除外 (P. 125)
アプリケーションの仕組み (P. 122)
管理コンソールによるデータベース増加の管理方法 (P. 296)
サーバの管理 (P. 89)

サブネットの追加

一致するサーバ トラフィックを自動的に監視するサーバ サブネットを追加します。 サーバ サブネットを指定するとき、管理コンソール で監視するアプリケーション サーバを表す、IP アドレスの範囲を指定します。 通常、この範囲は、サーバ VLAN 定義に厳密に一致させます。

サーバ サブネットを追加した後、サーバ IP アドレスの指定された範囲内の特定のサーバからのトラフィックを無視する除外を追加するために、サーバ サブネットを編集します。

指定するサーバに以下の処理を行う場合	指定するサブネット マスクの範囲
含める	■ IPv4： /16 および /31。/32 サーバ サブネット マスクは指定できません。
除外	■ IPv4： /17 および /32。

必要な場合は、監視デバイス でトラフィックが観測されていないサーバを 管理コンソール に追加することができます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）サーバ サブネットを追加するドメインを選択します。
4. ［サーバ サブネット リスト］までスクロールし、サーバ サブネットをクリックして追加します。

   ［サーバ サブネットの追加］が表示されます。
5. ［サーバ サブネット］内のフィールドに入力し、［OK］をクリックします。

   サーバ サブネット プロパティの設定の詳細については、［ヘルプ］を参照してください。

   管理コンソール は、定義されたあらゆる既存のサーバ サブネットとサーバ サブネットが競合しないことを検証した後で、サーバ サブネットを追加します。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

   5 ～ 10 分後、サーバ リストは、指定されたサーバ サブネットに一致するサーバを自動的に表示します。

詳細情報:

テナントの管理 (P. 113)
サーバの追加 (P. 92)

サーバ サブネットの編集

サーバ サブネットを編集して IP アドレスの範囲を変更し、特定のサーバを除外したり、管理コンソール が一致するサーバ トラフィックから自動的に作成するクライアント ネットワークのデフォルト ネットワーク タイプを指定したりします。

更新した IP 範囲の外部にある既存のデータは、引き続きレポート対象になります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）編集するサーバ サブネットが含まれるドメインを選択します。
4. ［サーバ サブネット リスト］までスクロールし、 をクリックしてサーバ サブネットを編集します。

   ［サーバ サブネットのプロパティ］が表示されます。
5. ［サーバ サブネットのプロパティ］内のフィールドに入力し、［適用］をクリックします。

   サーバ サブネット プロパティの設定の詳細については、［ヘルプ］を参照してください。

   管理コンソール は、サーバ サブネットが、定義されたあらゆる既存のサーバ サブネットと競合しないことを検証した後で、そのサーバ サブネットを追加します。
6. ［除外の追加］をクリックし、サーバ サブネットによって指定された IP アドレスの範囲内の特定の IP アドレスを除外します。

   /16（およびそれより大きい）サブネット マスクを指定します。
7. ［OK］をクリックします。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
/32 クライアント ネットワークの仕組み (P. 82)

サーバ サブネットの削除

管理コンソール がサーバ サブネットに一致する新しいサーバを自動的に監視するのを防ぐ場合は、そのサーバ サブネットを削除します。 管理コンソール は、サーバ サブネットに一致する既存のサーバを引き続き監視します。

必要な場合は、サーバ リストからサーバを削除します。既存のデータは、引き続きレポート対象になります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。

   ［サーバ リスト］が表示されます。
3. （オプション）編集するサーバ サブネットが含まれるドメインを選択します。
4. をクリックし、［サーバ サブネット リスト］内のサーバ サブネットを削除します。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

サーバの管理

［サーバ リスト］を使用して、以下をはじめとするサーバのプロパティを管理します。

- SNMP プロファイル。 管理コンソール でサーバに対して SNMP 経由のパフォーマンス調査を実行するには、有効な SNMP ユーザ認証情報を含む SNMP プロファイルが必要です。

  有効な SNMP プロファイルを指定しなかった場合は、管理コンソールが SNMP プロファイルを検出しようとします。

- 監視フィード割り当て。 サーバに特定の 監視フィード を割り当てるように 管理コンソール が自動的に保守する 監視フィード 割り当てを上書きできるほか、この割り当てを永久に上書きすることもできます。

  ネットワークが別のネットワーク パスにフェールオーバしたり、サーバ トラフィックの負荷が 2 つのスイッチ間で分散されたりするときのように、管理コンソール で複数の 監視フィード からのサーバ トラフィックを監視する場合は、サーバに割り当てられた 監視フィード にセカンダリ 監視フィード を割り当てることができます。

- TCP/IP ホスト名の解決。 管理コンソール は、指定されたサーバ サブネットに一致するサーバの DNS ホスト名を自動的に解決します。

  手動で追加またはインポートされたサーバについては、サーバのプロパティを編集してホスト名を入力します。

- サーバ保守スケジュール。管理コンソール は、デフォルトの保守スケジュールをサーバに割り当てますが、ユーザはスケジュールされた保守期間を割り当てる必要があります。

- インシデント レスポンス。 デフォルトでは、管理コンソール はサーバ インシデントに対してアクションを起動しません。

  SNMP 経由のパフォーマンス調査を有効にする場合は、サーバに SNMP プロファイルを割り当てることをお勧めします。

管理コンソール が監視する TCP ポートを制限するには、ポート除外にサーバまたはサーバ サブネットを割り当てます。

詳細:

ネットワークまたはサーバのインシデント レスポンスへのアクションの追加 (P. 210)
監視フィードのペアの作成 (P. 291)
監視フィード割り当ての仕組み (P. 289)
SNMP プロファイルの管理 (P. 269)
サーバ保守のスケジュール (P. 103)

命名規則

以下の表は、サーバの推奨命名規則のリストを示しています。

Server Type	推奨命名規則	例
単一機能サーバ	*DNSName-IPAddress*	Goliath-196.128.34.1
ファームに複数のサーバ、1 つのアプリケーション	*ApplicationName-DNSName*	DocMgr-Zeus DocMgr-Athena DocMgr-Mercury
1 つのアプリケーション、複数のサーバ、複数の場所	*ApplicationName-DNSName-Location*	DocMgr-Hamlet-NewYork DocMgr-Romeo-Milan DocMgr-Othello-London

サーバの検索

現在監視されているサーバを検索するには、サーバ リストを検索します。

管理コンソール がサーバ上で監視しているアプリケーションを表示するには、［サーバ リスト］で拡大鏡 アイコンをクリックします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）編集するサーバ サブネットが含まれるドメインを選択します。
4. ［サーバ リスト］までスクロールし、フィールドに検索文字列を入力して、［検索］をクリックします。

   * または % などのパターン一致文字はサポートされていません。
5. リストをリセットするには、［クリア］をクリックします。

詳細:

テナントの管理 (P. 113)

サーバの追加

指定されたサーバ サブネットに一致し、定義したすべてのポート除外にも一致しないアプリケーション ポート トラフィックが観測されたサーバが、管理コンソール によりサーバ リストに自動的に入力されます。

管理コンソール でトラフィックが観測されていないアプリケーションにサーバを割り当てるには、そのサーバを追加し、アプリケーションに割り当てます。

サーバを追加するときは、サーバの自動的な 監視フィード 割り当てを上書きしないようにします。 むしろ、必要な場合は、管理コンソール が自動的に 監視フィード を再割り当てできるようにします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）サーバを追加するドメインを選択します。
4. ［サーバ リスト］までスクロールし、IPv4 サーバをクリックして追加します。

   ［サーバのプロパティ］が表示されます。
5. ［サーバのプロパティ］内のフィールドに入力し、［OK］をクリックします。

   サーバのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細情報:

テナントの管理 (P. 113)

サーバの編集

管理コンソールによって監視されるサーバを表示し管理するには、サーバリストを使用します。

- 管理コンソールが特定のサーバ上で監視しているアプリケーションを表示するには、［アプリケーション］列の拡大鏡アイコンをクリックします。
- サーバを編集するのは、たとえば、監視フィード統計を表示したりプロパティを変更したりする場合です。サーバのプロパティを変更すると、[ユーザ変更済み]ステータスが[はい]に変わります。監視フィード統計には次のものが含まれます。
  - フィード別のサーバトラフィック（過去 24 時間）：各監視フィード上のサーバによるトラフィックボリュームを示します。これにより、監視の自動割り当てによる割り当てと確保されていた割り当ての両方で監視フィード割り当てが正しいことを確認できるようになります。
  - 割り当てられた監視デバイスのボリューム統計（過去 7 日間）：サーバに割り当てられていた監視デバイスによって過去 7 日間から観測されたトラフィックボリュームを示します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）必要なサーバが含まれるドメインを選択します。
4. ［サーバリスト］までスクロールし、をクリックしてサーバを編集します。

   （オプション）複数のサーバを編集するには、各サーバを選択し、をクリックして、選択したすべてのサーバを一括で編集します。加えたすべての変更は選択されたすべてのサーバに適用されますので注意してください。

   ［サーバのプロパティ］が表示されます。
5. ［サーバのプロパティ］内のフィールドに入力し、［OK］をクリックします。

   サーバのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

サーバの削除

サーバのアプリケーション ポート トラフィックの監視を停止するには、そのサーバを削除します。 サーバを削除した後も、既存のデータは引き続きレポート対象になります。

サーバ サブネットに一致するサーバを削除した場合は、サーバが一時的にのみ削除されます。 監視デバイス がサーバ サブネットに一致するサーバ トラフィックを観測すると、その後、管理コンソール はそのサーバをリストに追加します。 削除するサーバがサーバ サブネットに一致した場合は、サーバ サブネットを編集し、管理コンソール がそのサーバを監視しないようにするサーバ除外を追加します。

サーバの特定のポートまたはポートの範囲が必要でない場合に、ポート除外を追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）削除するサーバが含まれるドメインを選択します。
4. ［サーバ リスト］までスクロールし、をクリックしてサーバを削除します。
5. サーバを削除するかどうかを尋ねるプロンプトで、［削除を続行］をクリックします。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
アプリケーション ポート除外 (P. 125)
サーバ サブネットの編集 (P. 87)

CSV ファイルからのサーバ定義のインポート

新しいサーバを 管理コンソール に迅速に追加するには、サーバ ホスト名および IPv4 アドレスのカンマ区切りリストを CSV ファイルに追加し、次にそのファイルを 管理コンソール にインポートします。 以下を実行することはできません。

- サーバ サブネット定義のインポート
- 既存の IPv4 アドレスの再インポート

インポート プロセスの一環として、サーバのリストを一括で編集して、たとえばサーバ保守スケジュールを割り当てることができます。 完了後、指定されたプロパティを使用してサーバの監視を開始するように 監視デバイス を同期します。

CSV ファイルの作成

迅速に使用を開始するには、CSV ファイルにサーバ名および IPv4 アドレスのカンマ区切りリストを追加します。

サーバ名と IP アドレスの一方のみが含まれる場合は、インポートを実行する前に、定義のリストを編集できます。 たとえば、IP アドレスのみを含む CSV ファイルを作成し、対応するサーバ名を指定してからインポートを実行することができます。 管理コンソール は、インポートされるサーバのホスト名を解決するために DNS をクエリすることはありません。

管理コンソール で監視するサーバを指定する CSV ファイルを作成するには、以下の手順に従います。 CSV ファイルを作成するときは、カンマで各フィールドを区切り、以下のものを二重引用符で囲みます。

- 埋め込まれているカンマまたは二重引用符。
- 二重引用符の中に 1 つ以上のスペースが含まれる文字列。例: "Houston Office"。

CSV 形式のサーバ定義の一例を以下に示します。 Austin DNS Server エントリは、CA Standard Monitor である ref-sa-coll がその「Packets」監視フィード 上で 192.168.100.2 のサーバ トラフィックを参照することを指定すると共に、デフォルトでは、「netqos」という SNMP プロファイルを使用してサーバをポーリングすることを指定しています。

```
"Austin DNS Server", 192.168.100.2, "ref-sa-coll", "Packets",
"netqos"
```

次の手順に従ってください:

1. austin_servers.csv などの .CSV 拡張子のテキスト ファイルを作成します。
2. 独立した行にカンマ区切りの各サーバ定義を指定します。
3. 各エントリでは、*Server_Name,Server_IP,Monitoring_Device,Monitor_Feed,SNMP_Profile* の形式を使用します。

   Server_Name

   サーバの名前を 管理コンソール で表示する場合は、50 文字以内で定義します。

   サーバのリストをインポートするとき 管理コンソール が DNS ホスト名を自動解決しませんので注意してください。

   Server_IP

ドット付き 10 進表記法の 4 つの構成要素により、サーバの IPv4 アドレスを定義します。 アドレス形式を正しく指定しない場合は、インポートではサーバ名として IP アドレスが使用されます。

Monitoring_Device

（オプション）サーバのトラフィックを参照する 監視デバイス を定義します。 監視デバイス を指定する場合は、デバイス上の 監視フィード も指定する必要があります。 サーバをインポートすると、必要に応じて、管理コンソール が自動的に 監視デバイス および 監視フィード を再割り当てします。監視フィード を指定しない場合は、管理コンソール が自動的に最適な 監視フィード を割り当てます。

Monitor_Feed

（オプション）サーバのトラフィックを参照する、監視デバイス 上の 監視フィード を定義します。 監視デバイス を指定する場合、Packets 監視フィード の Packet など、デバイス上の 監視フィード も指定する必要があります。 サーバをインポートすると、必要に応じて、管理コンソール が自動的に 監視デバイス およびフィード を再割り当てします。

監視フィード を指定しない場合は、管理コンソール が自動的に最適な 監視フィード を割り当てます。

監視デバイス 上の利用可能な 監視フィード 名のリストを参照するには、CA Standard Monitor または CA Multi-Port Monitor を編集します。

SNMP_Profile

（オプション）。たとえば、SNMP 経由のパフォーマンス調査の一環としてサーバをポーリングするときに 管理コンソール で使用する SNMP プロファイル名を定義します。 有効な SNMP プロファイルが 管理コンソール によって検出されるようにする場合は、NULL 値（""）を指定します。

4. ファイルを保存し、管理コンソール にインポートします。

詳細:

監視デバイスの動作 (P. 287)
SNMP プロファイル ディスカバリの仕組み (P. 270)

サーバ定義のインポート

サーバ定義をインポートする場合は、テキスト ファイルに .CSV ファイル拡張子があることを確認します。 インポートの一環として、サーバ定義を一括で編集できます（たとえば SNMP プロファイルを割り当てる）。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）サーバをインポートするドメインを選択します。
4. ［サーバ リスト］までスクロールし、青い歯車型メニュー（ ）をクリックして［ファイルからのインポート］を選択します。

   ［サーバ定義のインポート］が表示されます。
5. CSV ファイル形式に関する情報を確認し、必要な場合は、例をコピーして CSV ファイルに貼り付けます。
6. ［参照］をクリックし、CSV ファイルを選択して［次へ］をクリックします。

   ［インポートしたサーバ定義の保存］が表示されます。
7. インポートされるサーバ定義のリストを確認し、必要な場合は変更を加えて、［OK］をクリックします。
8. CSV ファイルからインポートした定義および 管理コンソール 内の既存のサーバ定義のあらゆる問題を解決します。

   ［インポートしたサーバ定義の保存］では、競合するサーバ定義が強調表示されます。
9. 強調表示されたサーバ定義を編集し、問題を解決して、［OK］をクリックします。

   黄色

   指定された 監視デバイス が存在しないか、サーバの IP アドレスが無効であることを示します。 管理コンソール でインポートを続行することはできますが、続行する前に、これらのタイプの問題を解決する必要があります。

   赤

サーバの IP アドレスが重複していることを示します。 インポートを続行するには、 をクリックして重複する IP アドレスをすべて削除します。

10. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

    監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

CSV ファイルへのサーバ定義のエクスポート

新しいサーバ定義をインポートするためのテンプレートとして使用するため、IPv4 サーバ定義を .CSV ファイルにエクスポートします。既存の IPv4 サーバ アドレスは再インポートできないことに注意してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）サーバをエクスポートするドメインを選択します。
4. ［サーバ リスト］までスクロールし、青い歯車型メニュー（ ）をクリックして［サーバのエクスポート］を選択します。

   ［サーバ定義のエクスポート］が表示されます。
5. エクスポート オプションを選択し、［OK］をクリックします。

   一意の IP アドレスのみ

   IP アドレスのみをエクスポートすることを指定します。

   すべてのエクスポート フィールド

   サーバ ホスト名および IP アドレスに加えて、割り当てられている監視デバイス と 監視フィード、および割り当てられている SNMP プロファイル名もエクスポートすることを指定します。

   ［ファイルのダウンロード］ダイアログ ボックスが表示されます。
6. CSV ファイルの内容を表示する場合は［開く］をクリックし、CSV ファイルを保存する場合は［保存］をクリックします。

詳細:

テナントの管理 (P. 113)

サーバへの監視フィードの固定

監視フィードを固定することにより、特定の監視フィードがサーバに永続的に割り当てられるようにします。たとえば、管理コンソールがサーバを監視する元の監視デバイスがわかっている場合、管理コンソールでそれが変更されないようにしたい場合などです。

監視デバイスを削除すると、対応する監視フィードに固定されていたすべてのサーバは解除され、別の監視フィードが自動的に割り当てられます。監視フィードの割り当てを更新するのに 10 分程度かかる可能性があります。

サーバを追加する場合、監視フィードを固定するかどうかを選択できます。または、サーバ プロパティを編集し、特定の監視フィードをサーバに割り当てます。

詳細情報:

サーバの編集 (P. 93)

サーバ保守のスケジュール

サーバ保守スケジュールは、たとえばバックアップまたはソフトウェア更新など、サーバのパフォーマンスが定期保守タスクのために異常になることが予想されるときを指定します。

定期サーバ保守の期間中、管理コンソール は以下の操作を行うか、または行いません。

- 以下を実行します。
  - 保守期間が開始すると、既存のサーバ インシデントをクローズします。

    サーバ インシデントの状態が保守期間終了後も引き続き存在している場合でも、管理コンソール は新しいサーバ インシデントを開きます。
  - アプリケーション、サーバ、ネットワーク パフォーマンスに関するデータの収集を続け、パフォーマンスを［正常］、［マイナー］（黄色）または［メジャー］（オレンジ）として評価します。 このデータは、保守期間の前、最中、後のパフォーマンスを理解するのに使用できます。
- 以下の操作を行いません。
  - 保守期間中に作成された新しいサーバ インシデントに対するレスポンスをトリガします。
  - 保守期間中に収集されたデータを使用して感度のしきい値を計算します。
  - 保守期間中に収集されたデータを使用してベースラインを計算します。
  - パフォーマンス OLA または可用性 OLA を計算します。

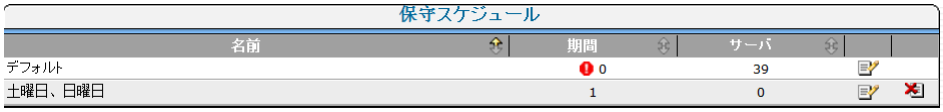
注: 保守期間中、管理コンソール ユーザは、低下したアプリケーション、サーバ、ネットワーク パフォーマンスについてレポートするかどうかを選択できます。 レポート設定で、保守期間中に収集されたパフォーマンス データの表示/非表示を選択するには、［定期保守を含みます］オプションを使用します。

保守スケジュールの仕組み

［保守スケジュール］リストを使用すると、以下の操作を行うことができます。

- 保守スケジュールに少なくとも 1 つの保守期間があるかどうかを判別します。
- 保守スケジュールが割り当てられているサーバ数を表示します。

管理コンソール には［デフォルト］と［週単位］の保守スケジュールが用意されていますが、これらの保守スケジュールには保守期間が含まれていません。 以下の例では、管理コンソール 管理者は、各保守スケジュールに少なくとも 1 つの保守期間を割り当てています。



管理コンソール は、新しく観測されたサーバにデフォルトの保守スケジュールを自動的に割り当てます。 ［デフォルト］の保守スケジュールに保守期間を追加し、必要に応じてサーバにカスタム スケジュールを割り当てることをお勧めします。

特定のサーバに割り当てられた保守スケジュールを表示するには、サーバのプロパティを編集します。

詳細:

サーバの編集 (P. 93)
保守スケジュールへの保守期間の追加 (P. 108)

保守スケジュールの追加

デフォルトの保守スケジュールより優先させるには、適切な保守期間で保守スケジュールを追加し、その保守スケジュールを適切なサーバに割り当てます。

重要: デフォルトの保守スケジュールには必ず保守期間を定義します。管理コンソール は、新しいサーバにデフォルトの保守スケジュールを自動的に割り当てます。

保守スケジュールを追加した後、スケジュールに保守期間を割り当てます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。
3. ［表示項目］メニュー下の［保守スケジュールの追加］をクリックします。

   ［スケジュールのプロパティ］ダイアログ ボックスが表示されます。
4. スケジュール名を入力し、［適用］をクリックします。

   これで、保守スケジュールに保守期間を追加することができます。
5. 終了したら、［OK］をクリックします。

詳細:

保守スケジュールへの保守期間の追加 (P. 108)

サーバ保守スケジュール名の変更

既存のサーバ保守スケジュールに対応する名前にサーバ保守スケジュールの名前を変更します。管理コンソール に用意されている［デフォルト］保守スケジュールおよび［週単位］保守スケジュールの名前は変更できます。

保守スケジュールについては、名前を変更できるだけでなく、保守期間を追加するなど、保守期間を変更することもできます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。

   ［保守スケジュール］が表示されます。
3.  をクリックして、保守スケジュールを編集します。
4. 3 番目の［表示項目］メニュー内の［スケジュール名の編集］をクリックして、保守スケジュールの名前を変更します。
5. ［スケジュールのプロパティ］に新しい名前を入力し、［OK］をクリックします。

   ［保守スケジュール］に、名前を変更された保守スケジュールが表示されます。

詳細:

保守スケジュールへの保守期間の追加 (P. 108)
保守期間の削除 (P. 110)
保守期間の編集 (P. 109)

保守スケジュールの削除

使用中の保守スケジュールを削除すると、管理コンソール は影響を受けるすべてのサーバに［デフォルト］保守スケジュールを自動的に割り当てます。 保守スケジュールがサーバに割り当てられているかどうかを決定するには、サーバのプロパティを表示します。

［デフォルト］保守スケジュールに保守期間を追加していない場合は、そうすることをお勧めします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。
3. をクリックして、［保守スケジュール］から保守スケジュールを削除します。
4. 保守スケジュールを削除するかどうかを尋ねるプロンプトで、［削除を続行］をクリックします。

詳細:

サーバの編集 (P. 93)
保守スケジュールへの保守期間の追加 (P. 108)

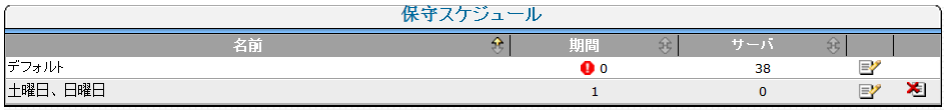
保守スケジュールへの保守期間の追加

保守スケジュールに 1 日あたり 1 つ以上の保守期間を追加します。保守スケジュールに保守期間を追加したら、サーバに保守スケジュールを割り当てることができます。

1 つの保守期間は複数の日付にわたることはできません。 たとえば、土曜日の午後 10 時から日曜日の午前 4 時までの保守期間を毎週設定する場合は、以下の 2 つの保守期間を作成する必要があります。

- 土曜日の午後 10 時から深夜 12 時
- 日曜日の午前 0 時から午前 4 時

保守スケジュールには少なくとも 1 つの保守期間を割り当てることをお勧めします。 以下の例では、［期間］列の［警告］アイコンは、デフォルトの保守スケジュールに対して保守期間が定義されていないことを示しています。



次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。

   ［保守スケジュール］リストが表示されます。
3. をクリックして、保守スケジュールを編集します。

   ［スケジュール済み期間］リストが表示されます。
4. ［表示項目］メニュー下の［期間の追加］をクリックします。

   スケジュール済み期間のプロパティが表示されます。
5. スケジュール期間の設定を指定し、［OK］をクリックします。

   スケジュール期間設定の指定の詳細については、［ヘルプ］を参照してください。

詳細情報:

サーバへの保守スケジュールの割り当て (P. 111)

保守期間の編集

サーバ保守を実行する期間を指定するには、保守期間を編集します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。

   ［保守スケジュール］が表示されます。
3. をクリックして、保守スケジュールを編集します。

   ［スケジュール済み期間］が表示されます。
4. をクリックして、保守期間を編集します。

   ［スケジュール期間のプロパティ］が表示されます。
5. スケジュール期間の設定を指定し、［OK］をクリックします。

   スケジュール期間設定の指定の詳細については、［ヘルプ］を参照してください。

保守期間の削除

サーバ保守スケジュールから保守期間を除去するには、保守期間を削除します。 保守スケジュールをサーバに割り当てた場合、スケジュールには少なくとも 1 つの有効な保守期間が含まれている必要がありますが、管理コンソール は、割り当てられた保守スケジュールに保守期間が含まれていることを要求しません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニュー内の［ポリシー］、［保守スケジュール］をクリックします。
3.  をクリックして、［保守スケジュール］のリスト内の保守スケジュールを編集します。

   ［スケジュール済み期間］のリストが表示されます。
4. 保守期間を削除するには、  をクリックします。
5. ［削除の確認］で、［削除を続行］をクリックして保守期間を削除します。

   ［スケジュール済み期間］から保守期間が除去されます。

詳細:

保守スケジュールの仕組み (P. 104)

サーバへの保守スケジュールの割り当て

サーバ保守スケジュールでは、定期保守アクティビティのためにサーバのパフォーマンスが正常でないことが予想される 1 つ以上の保守期間を特定します。 サーバ保守を実行する期間を指定するには、保守スケジュールを 1 つ以上のサーバに割り当てます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。
3. （オプション）必要なサーバが含まれるドメインを選択します。
4. ［サーバ リスト］までスクロールし、  をクリックしてサーバを編集します。

   ［サーバのプロパティ］が表示されます。

   （オプション）複数のサーバを編集するには、各サーバを選択し、  をクリックして、選択したすべてのサーバを一括で編集します。 加えたすべての変更は選択されたすべてのサーバに適用されますので注意してください。
5. ［保守スケジュール］をクリックし、リストからスケジュールを選択して、［OK］をクリックします。

   サーバのプロパティの詳細については、［ヘルプ］を参照してください。

   複数のサーバを編集する場合、すべての変更は全サーバに適用されます。 ［変更なし］という値は、各サーバ上の既存の値が保持されることを示します。
6. ［OK］をクリックします。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
保守スケジュールへの保守期間の追加 (P. 108)

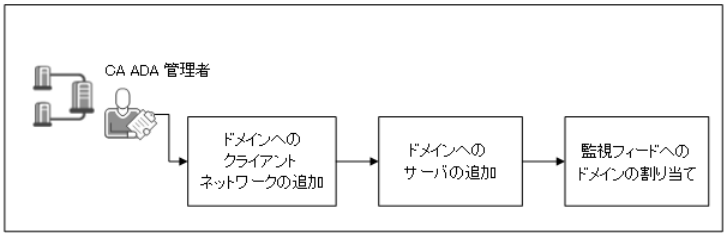
第 4 章: テナントの管理

ドメインを使用して、CA Application Delivery Analysis 内のテナント データを管理することができます。 CA Application Delivery Analysis は、テナントを認識しませんが、ドメインによってテナント トラフィックを分離できます。 非 ISP 環境では、ドメインはオーバラップ（重複）するクライアント ネットワーク IP アドレスを持つアプリケーション トラフィックを分離します。

重要: CA Application Delivery Analysis で、管理者の役割はすべてのドメイン データおよびドメイン設定にアクセスできます。 CA Application Delivery Analysis 上で管理者の役割をテナント ユーザに付与しないでください。

テナンシーの概要

ドメインを使用して、監視フィード上のサーバとクライアント ネットワーク間のトラフィックを一意に識別します。 ドメインによってテナント データを分離することは、CA Application Delivery Analysis によるマルチテナンシーのサポートによって実現します。



以下のタスクを完了します。

1. クライアント ネットワークをドメインに追加します (P. 117)。
2. サーバをドメインに追加します (P. 118)。
3. ドメインを監視フィードに割り当てます (P. 119)。

前提条件

CA Application Delivery Analysis のテナントを CA PC で管理する場合、以下を確認します。

- CA PC が以下の要件を満たしている。
  - CA Application Delivery Analysis が登録済みのデータ ソースです。
  - テナント ユーザに、適切な IP ドメイン グループに対する権限があります。 テナント ユーザに対して、他のテナントからのドメイン データに対するアクセス権を与えないでください。
  - テナント ユーザに、CA Application Delivery Analysis に対する管理者役割がありません。管理者の役割は、CA Application Delivery Analysis ユーザに対し、すべてのドメインおよび［環境管理］ページ上の全データに対するアクセス権を付与します。
  - CA Application Delivery Analysis データ ソースが同期されています。
- CA Application Delivery Analysis が以下の要件を満たしている。
  - 監視デバイス上の監視 NIC は、パケット ヘッダから VLAN タグ情報を読み取ることができます。VLAN によるトラフィックを分離する必要がない場合、これは該当しません。

    注: 設定ユーティリティを使用して VLAN タグ情報が使用可能であることを確認するか、または監視デバイスからパケット キャプチャを取得します。
  - 管理コンソールは、CA PC または CA NPC 内のドメインのリストと同期されます。

    注:［環境管理］ページで、［データ監視］-［ドメイン］をクリックし、使用可能なドメインのリストを表示します。

CA Application Delivery Analysis のテナントを CA NPC で管理する場合、以下を確認します。

- CA NPC が以下の要件を満たしている。
  - CA Application Delivery Analysis が登録済みのデータ ソースです。
  - テナント ユーザに、適切なドメイン グループに対する権限があります。 テナント ユーザに対して、他のテナントからのドメイン データに対するアクセス権を与えないでください。

- テナント ユーザに、CA Application Delivery Analysis に対する管理者役割がありません。管理者の役割は、CA Application Delivery Analysis ユーザに対し、すべてのドメイン グループおよび [環境管理] ページ上の全データに対するアクセス権を付与します。
- CA Application Delivery Analysis データ ソースが同期されています。

- CA Application Delivery Analysis が以下の要件を満たしている。
  - 管理コンソールは、CA NPC 内のドメインのリストと同期されます。

ドメインによるトラフィックの分離方法

ドメインは以下によってトラフィックを分離します。

- 監視フィード
- クライアント ネットワーク
- サーバ サブネットおよびサーバ

サーバ、ネットワーク、監視フィードに同じドメインを割り当てている場合、管理コンソールは、監視フィードからのクライアントとサーバ間の一意のアプリケーション トラフィックをレポートします。

VLAN にタグ付けされたトラフィックは、VLAN タグ定義に基づいて監視フィードで別のドメインに分離できます。 VLAN にタグ付けされたトラフィックをドメイン別に分けることにより、単一の監視フィードが複数のドメインを監視できるようになります。

アプリケーションはドメイン独立です。 レポートは、複数のアプリケーション定義（たとえば Exchange Company A および Exchange Company B など）を必要とせずに、ドメイン間でのアプリケーションのパフォーマンスを表示できます。

ドメインは、アプリケーション プロパティには適用されません。 たとえば、アプリケーションの名前を変更する場合、アプリケーション名はドメインをまたいで同じです。しかし、アプリケーションのパフォーマンス、パフォーマンス OLA、可用性 OLA に別々のしきい値を設定する場合には、ドメインごとにアプリケーションを作成する必要があります。

データ ソースの同期

CA PC および CA NPC は、ドメインのリストを CA Application Delivery Analysis と同期します。管理コンソールがそのドメイン リストを更新するのに 5 分程かかる可能性があります。

ドメインが CA PC から削除された場合、管理コンソールは以下を実行します：

- そのドメインに関連付けられたクライアント ネットワーク、サーバ サブネット、サーバ、およびポート除外をすべて削除し、関連するサーバ割り当てをユーザ定義アプリケーションから削除します。

  既存のドメインに固有のデータは、引き続きレポートの目的に利用可能です。

  ユーザ定義のアプリケーションは特定のドメインには関連付けられていません。したがって、ドメインを削除した後、管理コンソールが残りのドメインに属するサーバとクライアント ネットワーク間にアプリケーション トラフィックを観測する場合、管理コンソールはアプリケーションに関するレポートを継続します。
- そのドメインに関連付けられたすべての監視フィードをデフォルト ドメインに再割り当てします。デフォルト ドメインは削除できません。

詳細:

ユーザおよびグループ (P. 256)

ドメインベースのレポートの動作

特定のドメインに対応するサーバおよびネットワークについてレポートするには、［設定］ページを使用します。 アプリケーションはドメインに非依存であるため、ドメイン別にアプリケーションをフィルタリングする必要はありません。

CA PC および CA NPC でドメイン グループ権限を使用し、テナント ユーザにドメインのレポート データに対する権限を付与します。

選択するレポート設定は、CA Multi-Port Monitor にドリル インする場合に保持されます。

管理コンソール内の［表示項目］ボックスに［ドメイン］列が表示されない場合は、テナントを管理するための前提条件を確認してください。

詳細:

前提条件 (P. 114)

ドメインへのクライアント ネットワークの追加

ドメインへのクライアント ネットワークの追加 サーバ、ネットワーク、監視フィードに同じドメインを割り当てている場合、管理コンソールは、クライアント ネットワークとサーバ間の一意のアプリケーション トラフィックをレポートします。

クライアント ネットワークを追加する場合は、正しいドメインが指定されていることを確認してください。 クライアント ネットワークを追加した後、そのドメインを変更することはできません。 必要な場合はクライアント ネットワークを削除してから正しいドメインに追加します。

詳細情報:

クライアント ネットワークの追加 (P. 51)

ドメインへのサーバの追加

ドメインにサーバを追加します。 サーバ、ネットワーク、監視フィードに同じドメインを割り当てている場合、管理コンソールは、クライアントネットワークとサーバ間の一意のアプリケーション トラフィックをレポートします。

サーバを追加する場合、正しいドメインが指定されていることを確認してください。 サーバを追加した後、そのドメインを変更することはできません。 必要な場合はサーバを削除してから正しいドメインに追加します。

詳細情報:

サブネットの追加 (P. 85)
サーバの追加 (P. 92)

監視フィードへのドメインの割り当て

ドメインを割り当てることにより、管理コンソールの以下のレポート先を指定します。

- タグ付けのないトラフィック。タグ付けされていないトラフィックはすべて、監視フィードに対するドメインに割り当てられます。
- VLAN にタグ付けされたトラフィック VLAN をドメインに割り当てることにより、監視フィード上の VLAN にタグ付けされたトラフィックを分離します。

  未割り当ての VLAN トラフィックにドメインを割り当てることもできます。

デフォルトでは、監視フィード上のすべてのトラフィックは、デフォルトドメインに割り当てられます。

重要: Multi-Port Monitor を CA CEM TIM と使用する場合、TIM に対する論理ポート上の VLAN トラフィックをドメインに割り当てないでください。TIM は VLAN ベースの監視フィードをサポートしません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］にスクロールし、監視デバイスを編集するための編集アイコン（）をクリックします。

   ［監視のプロパティ］が表示されます。
4. ［監視フィード］までスクロールします。
5. 監視フィードを編集するための編集アイコン（）をクリックします。

   ［監視フィード］リストが展開します。

   a. ［ドメイン］をクリックして、VLAN 情報でタグ付けされていないトラフィックにドメインを割り当てます。

   b. ［適用］をクリックします。
6. ［VLAN の割り当て］をクリックします。

   ［VLAN の割り当て］で、監視フィードに対する VLAN 割り当てを編集します。

a. 各ドメインに割り当てる VLAN を指定します。

b. ［未割り当て VLAN］列で、割り当てられていない VLAN トラフィックに対するドメインを指定します。

   詳細を参照するには、［ヘルプ］をクリックしてください。

c. ［OK］をクリックします。

7. これらの手順を繰り返して、監視フィードごとにドメインを割り当てます。

詳細:

テナントの管理 (P. 113)

第 5 章: アプリケーションの管理

このセクションには、以下のトピックが含まれています。

アプリケーションの仕組み (P. 122)
アプリケーション ポート除外 (P. 125)
システム定義のアプリケーションの管理 (P. 132)
ユーザ定義のアプリケーションの管理 (P. 137)
多層アプリケーションの管理 (P. 156)
アプリケーションのキープアライブ メッセージ (P. 162)

アプリケーションの仕組み

アプリケーションは、管理コンソール でサーバ IP アドレスの範囲全体に対して監視する TCP のポートまたはポート範囲を指定します。 たとえば、管理コンソール で、/29 サーバ サブネット全体の TCP-80 トラフィックを監視することができます。

デフォルトでは、管理コンソール は、全クライアント ネットワークに対して、すべてのアプリケーション ポートおよびサーバの TCP セッションを監視するシステム定義のアプリケーションを自動的に作成します。 たとえば、/24 のいくつかのサーバ サブネットを監視するように 管理コンソール を設定すると、管理コンソール は、全サーバに対して TCP-1433 トラフィックを監視するシステム定義の［Microsoft SQL サーバ］アプリケーションを作成します。 一致する IP アドレスを持った新しいサーバがプロビジョニングされると、管理コンソール は自動的にそれらを監視します。

すべてのサーバ サブネット、特定のサーバ サブネットまたは特定のサーバにおいて特定のポートまたはポート範囲の TCP セッションを無視するには、ポート除外を作成します。

アプリケーションをホストする実際のサーバについてレポートするため、システム定義のアプリケーションから、TCP ヘッダから入手できる情報だけでなくユーザの専門知識に基づいて、ユーザ定義のアプリケーションを作成することができます。たとえば、特定のデータベース アプリケーション パフォーマンスについてレポートするには、ユーザ定義の SQL Server アプリケーションを作成し、アプリケーションをホストする適切なサーバを識別するアプリケーション サブネットを割り当てます。

あるいは、特定のアプリケーションが常に特定のポート上で実行されることがわかっている場合は、管理コンソール により、全サーバにおけるアプリケーションの自動的な監視を行うことができます。

CA PC または CA NPC にデータ ソースとして登録されている場合、CA PC または CA NPC はすべてのアプリケーションをレポート用に自動的にグループ化します。

CA PC または CA NPC にドメインを定義している場合は、観測されたアプリケーション トラフィックをフィルタするためにドメインを選択できます。

詳細:

テナントの管理 (P. 113)
アプリケーション ポート除外 (P. 125)

優先アプリケーションの仕組み

データベースの増大を管理するため、CA Application Delivery Analysis Manager は必要に応じてボリュームが小さいアプリケーションの 5 分間のデータを整理します。 CA Application Delivery Analysis Manager がデータを整理すると、アプリケーションのデータは 5 分間隔でのみ提供され、［操作］ページのレスポンス時間データは市松模様として表示されます。

CA Application Delivery Analysis Manager でシステムまたはユーザ定義のアプリケーションの 5 分データを消去しないようにする場合は、［アプリケーションのプロパティ］を編集し、［優先度］チェック ボックスをオンにします。 CA Application Delivery Analysis Manager が優先アプリケーションのデータを消去しなくなります。

詳細:

管理コンソールによるデータベース増加の管理方法 (P. 296)
ユーザ定義アプリケーションの編集 (P. 153)

アプリケーションの検索

目的のアプリケーションを検索するには、［アプリケーション リスト］をフィルタします。

サブネット | サーバの表示

割り当てられている観測済みサーバ情報を表示するオプションを指定します。

- *［サブネット］*は、アプリケーション トラフィックがホストされている対応するサーバ サブネットを表示します。
- *［サーバ］*は、アプリケーションをホストしている実際のサーバを表示します。

検索

［アプリケーション リスト］内で一致するエントリを検索します。検索結果をクリアするには、［検索のクリア］をクリックします。

リストをリセット

現在表示できないリストのページを含め、［アプリケーション リスト］内のユーザの現在の選択内容をすべて削除します。オブジェクトが選択されているかどうかが不確かな場合は、目的のオブジェクトを選択する前に、［リストをリセット］コマンドをクリックします。

アプリケーション リストを表示

システムおよびユーザ定義のアプリケーションをフィルタします。

1 ページあたりの最大数

1 ページあたりのアプリケーション エントリの最大数を指定します。 アプリケーションのリストが 1 ページを超える場合は、ユーザがページ間を移動したときでも、すべての選択内容がリストに保持されます。

ドメイン

（オプション）観測されたアプリケーション サーバ ポート トラフィックをフィルタするためにドメインを指定します。

詳細:

テナントの管理 (P. 113)
ユーザ定義のアプリケーションの管理 (P. 137)
システム定義のアプリケーションの管理 (P. 132)

命名規則

以下の表は、アプリケーションの推奨命名規則のリストを示しています。

Application Type	推奨命名規則	例
1 つのアプリケーション、単一のポート	User-Defined-*portnum*	User-Defined-80
1 つのアプリケーション、複数のポート	User-Defined-*portnumStart-portnumEnd*	User-Defined-1024-5000 User-Defined-135-145 User-Defined-110-120 User-Defined-25-50

アプリケーション ポート除外

すべてのサーバ サブネット、特定のサーバ サブネットまたは特定のサーバにおいて特定のポートまたはポート範囲の TCP セッションを無視するには、ポート除外を作成します。 デフォルトでは、管理コンソール は、指定されたサーバ サブネットに一致するすべてのサーバ上のアプリケーション ポートをすべて監視するシステム定義のアプリケーションを作成します。

詳細:

サーバ サブネットの管理 (P. 84)

ポート除外の仕組み

ポート除外は、監視デバイスでアプリケーション ポート トラフィックをフィルタし、管理コンソール上で使用可能リソースを最大化する一方で、同時に管理コンソール ユーザの注意を当該アプリケーションに集中させます。監視デバイスは、ポート除外に一致する TCP セッションを無視します。 たとえば、ユーザがリモート共有（¥¥myserver¥sharename など）に接続するたびに、SMB（Server Message Block）プロトコルは 2 つの TCP セッション（TCP-139 および TCP-445）を開きます。リモート セッションが 445 で確立された場合（Windows 2000 以降では任意の Windows ベース システム）、SMB プロトコルは 139 のセッションをリセットし（RST）、TCP ポート 445 の上で確立されたセッションを使用します。 TCP-139 は、Windows 2000 より前の Windows マシンへの SMB に対して使用されます。指定されたすべてのサーバ サブネット上で短命な TCP-139 セッションを監視しないようにするには、ポート 139 に対してポート除外を作成し、必要に応じてドメインに割り当てます。

ポート除外はシステム定義およびユーザ定義のアプリケーションより優先されます。 たとえば、ユーザ定義のアプリケーションを作成する場合に、目的のポート範囲に一致する既存のポート除外があるときは、ポート除外を編集して 管理コンソール でポート範囲を監視できるようにし、その後でアプリケーションを作成します。

また、ポート除外を使用して、管理コンソール によって自動的に監視される不要なアプリケーション サーバ トラフィックを無視することもできます。たとえば、すべての Microsoft SharePoint サーバが 192.168.43.0/24 のサーバ サブネット上でホストされているが、192.168.43.14 と 192.168.43.15 はテスト サーバのため監視しないとします。 管理コンソール で自動的に実稼働 SharePoint サーバをすべて監視できるようにする方法

- SharePoint-80 という名前のアプリケーションを作成し、192.168.43.0/24 サーバ サブネットを割り当てます。
- テスト用 SharePoint サーバを無視するには、192.168.43.14 と 192.168.43.15 に対して TCP-80 に関するポート除外を作成します。

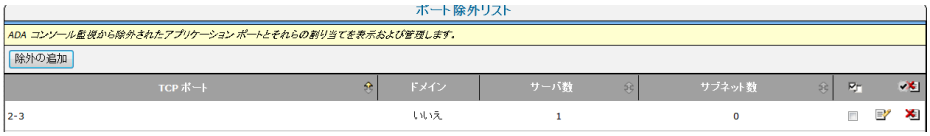
詳細:

テナントの管理 (P. 113)

ポート除外リストの仕組み

ポート除外リストを使用して、無視するアプリケーション ポートを指定するポート除外ルールを参照および管理します。 ［サーバ数］列および［サブネット数］列は、ポート除外が適用されるサーバまたはサブネットの数を示します。

CA Application Delivery Analysis は、ポート除外に一致したアプリケーション トラフィックを監視しません。 ポート除外に一致するポート範囲を使用するアプリケーションは作成できません。



ポート除外の追加

以下において 管理コンソール で無視するポート範囲を指定するポート除外を追加します。

- ドメインのすべてのサーバ。 ドメインを定義していない場合は、デフォルト ドメインへのポート除外の追加によりすべてのサーバにおけるポート トラフィックを無視するように 管理コンソール を設定できます。
- サーバ サブネット内のすべてのサーバ。 必要な場合は、サーバ IP アドレスの特定の範囲上のアプリケーション ポート トラフィックを無視するカスタム サーバ サブネットを作成できます。
- 1 つまたは複数のサーバ。 管理コンソール で、特定の 1 つ以上のサーバのポート トラフィックを無視することができます。 必要な場合は、ポート除外にサーバを追加できます。

ポート除外を追加すると、そのポート除外に一致する既存のアプリケーションがある場合に、管理コンソール はそれらのアプリケーションの監視を停止します。

アプリケーションを削除する場合、管理コンソール がその後アプリケーションを自動的に監視しないようにするため、ポート除外をオプションで作成できます。

ポート除外を追加するには、以下の手順に従います。

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ポート除外を追加するドメインを選択します。 重複した IP トラフィックを分離するようにドメインを定義していない場合、このオプションはデフォルト ドメインのすべての 監視デバイス におけるポート トラフィックを除外します。
4. ページの下部の［ポート除外リスト］までスクロールし、［除外の追加］をクリックします。

   ［ポート除外のプロパティ］が表示されます。
5. 特定のポートまたはポート範囲を除外するために、［開始ポート］と［終了ポート］を指定します。

   ［開始ポート］は［終了ポート］と同じかまたはそれより小さい番号であることが必要です。

6. （オプション）現在選択されているドメインのすべてのサーバに対するポート範囲を除外するには、［ドメイン内のすべてのサーバ上のアプリケーション ポート トラフィックを無視します］を選択します。ドメインを定義していない場合は、デフォルト ドメインがすべてのサーバに適用されます。

   このオプションを選択した場合、管理コンソール は、ドメイン上のポート トラフィックを無視することを確認するようにユーザに促します。

7. （オプション）サーバ範囲に対してポート範囲を除外する方法

   a. ［サブネットの割り当て］をクリックします。

   b. ［ポート除外サブネット］で、既存のサーバ サブネットを割り当てるか、またはアプリケーション サブネットを作成し、一連のサーバにおいてポート トラフィックを除外します。

      アプリケーション サブネットを作成するには、IP アドレスとマスクを指定し、［アプリケーション サブネットの追加］をクリックします。

      既存のサーバ サブネットを割り当てるには、対象のサブネットをダブルクリックします。 使用可能なサブネットのリストには、管理コンソール が環境内のサーバを監視するために使用するサーバ サブネットと、作成したあらゆるアプリケーション サブネットが含まれます。

   c. ［適用］をクリックします。

8. （オプション）特定の 1 つ以上のサーバに対してポート範囲を除外する方法

   a. ［サーバの割り当て］をクリックします。

   b. ［ポート除外サーバ］で、利用可能なサーバをダブルクリックして、ポート除外に追加します。

   c. ［適用］をクリックします。

9. ［OK］をクリックします。

10. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

    監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

サーバの管理 (P. 79)
テナントの管理 (P. 113)
ユーザ定義アプリケーションの削除 (P. 155)

ポート除外の編集

管理コンソール で無視するポートおよびサーバの範囲を更新するために、ポート除外を編集します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ポート除外を編集する対象のドメインを選択します。
4. ページの下部の［ポート除外リスト］までスクロールし、 をクリックしてポート除外を編集します。

   ［ポート除外のプロパティ］が表示されます。
5. ポート除外のプロパティを指定し、［OK］をクリックします。

   ポート除外プロパティの指定の詳細を参照するには、［ヘルプ］をクリックしてください。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

ポート除外の削除

以前に除外されたポート トラフィックの監視を再開するには、ポート除外を削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ポート除外を削除するドメインを選択します。
4. ページの下部の［ポート除外リスト］までスクロールし、をクリックして除外を削除します。

   （オプション）複数のアプリケーション除外を削除するには、該当する除外を選択し、をクリックして、選択した除外をすべて削除します。
5. プロンプトで［削除を続行］をクリックすると、一致するアプリケーション ポート トラフィックの自動監視を 管理コンソール が開始します。

   除外が削除されます。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

システム定義のアプリケーションの管理

管理コンソールでは、一致する各サーバ上で最もビジーな標準アプリケーションとアクティブな FTP（TCP-20 および TCP-21）アプリケーションを監視するために、指定されたクライアント ネットワークとサーバ サブネットのリストに基づいて、システム定義のアプリケーションを作成します。

可能な場合は、管理コンソール ですべてのサーバにおけるアプリケーション トラフィックを自動的に監視します。 ユーザ定義のアプリケーションと異なり、システム定義のアプリケーションにはサーバを割り当てることはできません。アプリケーションを監視するために TCP パケット内で利用可能な情報を超えた追加の情報が 管理コンソール で必要になる場合は、ユーザ定義のアプリケーションを作成します。 たとえば、以下を監視するユーザ定義のアプリケーションを作成します。

- ポート範囲上で通信するアプリケーション
- TCP-80 上で通信する特定の Web アプリケーション

システム定義のアプリケーションに対しては、パフォーマンス OLA や可用性 OLA は設定できません。 ただし、管理コンソール で監視されるすべてのサーバに OLA を適用する場合は、ユーザ定義のアプリケーションを作成し、それにドメインのサーバをすべて割り当てます。

管理コンソール で自動監視するアプリケーション ポート数を削減する方法

- アプリケーションを削除します。
- ポート除外を作成します。

詳細情報:

システム定義のアプリケーションの削除 (P. 135)
アプリケーション ポート除外 (P. 125)
アプリケーションへのサーバの割り当て (P. 150)

システム定義のアプリケーションの編集

たとえば、以下のように、システム定義のアプリケーションを編集します。

- アプリケーションの名前を変更します。 デフォルトでは、ウェルノウン ポート上のシステム アプリケーションには 管理コンソール によって名前が付けられます。
- アプリケーションに優先順位を付けて、管理コンソール がアプリケーションのデータを消去したりフィルタしたりするのを回避します。
- デフォルトのインシデント レスポンスを変更します。 デフォルト アプリケーション インシデント レスポンスでは応答アクションを指定しないので注意してください。

システム定義のアプリケーションのステータスは変わりません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. CA PC または CA NPC にドメインを定義している場合、ドメインを選択する必要はありません。システム定義のアプリケーション プロパティに加えたすべての変更は、全ドメインに対して適用されます。
4. ［アプリケーション リスト］の［設定者］列を参照し、システムによって設定されたアプリケーションを特定します。

   必要に応じて、［アプリケーション リスト］を再編成するために［リストをリセット］をクリックします。

   複数のシステム定義アプリケーションを編集するには、目的のアプリケーションを選択します。 複数のアプリケーションの名前を同じ名前に変更することはできません。
5. 名前を変更するアプリケーションを選択し、［編集］をクリックします。

   ［アプリケーションのプロパティ］が表示されます。
6. ［アプリケーションのプロパティ］内のフィールドに入力し、［OK］をクリックします。

   アプリケーションのプロパティの設定の詳細については、［ヘルプ］を参照してください。

7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
ユーザ定義のアプリケーションの管理 (P. 137)

システム定義のアプリケーションの削除

管理コンソール およびその 監視デバイス 上で利用可能なシステム リソースを最適化するには、システム定義のアプリケーションを削除します。管理コンソール が、アプリケーションの削除後にそのアプリケーションが自動的に監視されるのを回避するには、ポート除外を作成します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. CA PC または CA NPC にドメインを定義している場合、ドメインを選択する必要はありません。アプリケーションに加えるどのような変更もドメインにわたって適用されます。
4. ［アプリケーション リスト］内の［設定者］列を参照し、システムによって設定されたアプリケーションを選択して、［削除］をクリックします。

   必要に応じて、［アプリケーション リスト］を再編成するために［リストをリセット］をクリックします。

   複数のシステム定義アプリケーションを削除するには、目的のアプリケーションを選択します。複数のアプリケーションの名前を同じ名前に変更することはできません。
5. アプリケーションを削除するオプションを選択します。

   ポート除外の削除および追加

   選択したアプリケーションを削除し、管理コンソール が自動的にアプリケーションを監視するのを回避します。

   削除

   選択したアプリケーションを削除しますが、管理コンソール が一致するアプリケーション トラフィックを確認した場合は自動的にそのアプリケーションを検出できるようにします。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
アプリケーション ポート除外 (P. 125)

ユーザ定義のアプリケーションの管理

可能な場合は、管理コンソール ですべてのサーバにおけるアプリケーション トラフィックを自動的に監視します。 アプリケーションを監視するために TCP パケット内で利用可能な情報を超えた追加の情報が 管理コンソール で必要になる場合は、ユーザ定義のアプリケーションを作成し、特定のサーバまたはサーバ IP アドレスの範囲を割り当てます。たとえば、以下を監視するユーザ定義のアプリケーションを作成します。

- ポート範囲上で通信するアプリケーション
- 特定の 1 つ以上のサーバの TCP-80 トラフィック

システム定義のアプリケーションのリストを使用して最もビジーなアプリケーション ポートを識別し、アプリケーションについての専門知識を活用して、トラフィック ボリュームが最も大きくビジネス クリティカルで、短時間に完了する必要のある TCP アプリケーションを監視するユーザ定義のアプリケーションを作成します。

システム アプリケーションによって現在監視されているアプリケーション サーバ トラフィックを監視するユーザ定義のアプリケーションを作成する際、ユーザ定義のアプリケーションを作成した後で、以下のことに注意してください。

- システム アプリケーションは、ユーザ定義のアプリケーションに割り当てられているサーバの中の一致したサーバについてレポートすることを停止します。 管理コンソール がユーザ アプリケーションのサーバ割り当てによって識別されていないサーバ上のアプリケーション トラフィックを観測した場合、管理コンソール により、システム アプリケーションのアプリケーション サーバ レスポンス時間がレポートされます。
- 管理コンソール は、ユーザ定義のアプリケーションについてレポートするために新しいデータを収集します。管理コンソール は、ユーザ アプリケーション内の既存のシステム アプリケーション データについてはレポートしません。
- ポート除外はシステム定義およびユーザ定義のアプリケーションより優先されます。 必要な場合は、すべてのポート除外から目的のポートを削除し、ユーザ定義のアプリケーションを作成します。

詳細:

アプリケーション ポート除外 (P. 125)
アプリケーションへのサーバの割り当て (P. 150)

標準アプリケーションの作成

標準アプリケーションは、サーバのポートに接続する標準的な TCP アプリケーションです。 すべてのトラフィックは、サーバのポートとクライアントのポートの間で発生します。 標準アプリケーションは任意のタイプの 監視デバイス で監視できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. 以下のいずれかの方法を使用して、ユーザ定義のアプリケーションを作成します。

   アプリケーションの新規作成

   ［アプリケーションの新規作成］をクリックします。

   既存のシステム定義のアプリケーションからの新しいアプリケーションの作成

   システム アプリケーションをクリックして、［アプリケーションの新規作成］をクリックします。 ポート範囲上で通信するアプリケーションを作成するには、必要なシステム アプリケーションをクリックします。

5. ［アプリケーション タイプ］を［標準］に設定し、［アプリケーションのプロパティ］内のフィールドに入力します。
   - アプリケーション名。
   - これを優先アプリケーションに設定します。 管理コンソールがアプリケーションを整理またはフィルタしないように指定する場合は、このオプションを選択します。
   - 開始ポート。 このポート範囲の開始 TCP ポート番号です。
   - 終了ポート。 このポート範囲の終了 TCP ポート番号です。
   - ポート側。 標準アプリケーションがクライアント リクエストにどのように応答するかを指定するオプションを選択します。

- アプリケーションはこれらのポートでリスンします。指定されたポート範囲内のクライアント リクエストをサーバがリスンする場合に、このオプションを選択します。 これがデフォルトになります。
- アプリケーションはこれらのポートにトークします。クライアント上の指定されたポート範囲内のクライアント リクエストにサーバが応答する場合に、このオプションを選択します。 Cisco NAM 監視デバイスでアプリケーションを監視する場合には、このオプションは適用されません。

- インシデント レスポンス アプリケーション インシデント レスポンスを選択し、Application Delivery Analysis が、アプリケーションに影響するネットワーク/サーバ インシデントにどのように応答するかを指定します。
- 可用性監視 アプリケーションの可用性監視を有効化または無効化するオプションを選択します。 有効にした場合、管理コンソールはアプリケーションの可用性を受動的に観測し、必要であれば能動的に可用性をチェックします。
- **注**: （オプション）アプリケーションに関する追加情報。

標準アプリケーションのプロパティの設定の詳細については、［ヘルプ］を参照してください。

6. ［次へ］をクリックしてアプリケーションにサーバ サブネットおよびサーバを割り当て、［OK］をクリックします。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。

7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
アプリケーションへのサーバの割り当て (P. 150)

Web アプリケーションの作成

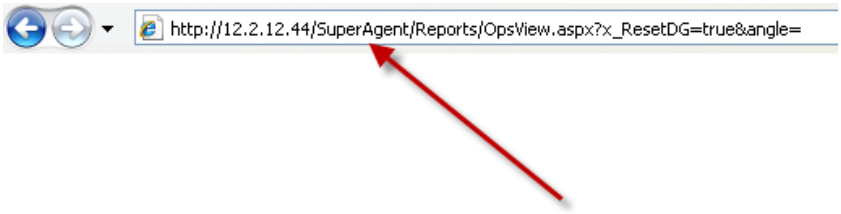
Web アプリケーションを作成して、HTTP トラフィックの TCP レスポンス時間についてレポートできます。 HTTP トラフィックを監視するには、CA Standard Monitor を使用する必要があります。

監視する Web アプリケーションのリソース パスを指定します。 リソース パスは、HTTP 要求ヘッダ（GET、POST、HEAD、TRACE）の内容と一致している必要があります。管理コンソール は、リソース パスを使用して、Web サーバ上の特定の HTTP トラフィックを識別します。

重要: 管理コンソールが *appname* - [その他] アプリケーションについてのみレポートする場合は、指定したリソース パスが HTTP 要求ヘッダに一致することをパケット キャプチャによって確認します。 プロキシをトラバースしている Web トラフィックを監視する場合など、場合によっては完全な URL を指定することが必要になることもあります。たとえば、以下の例に示されるようなリソース パスではなく、http://*server/resource* のように指定します。

/SuperAgent

CA Application Delivery Analysis へのすべての HTTP トラフィックを特定します。 以下に例を示します。



/pc

CA NPC への HTTP トラフィックをすべて識別します。 以下に例を示します。

管理コンソールは、定義したリソース パスごとに個別の Web アプリケーションを作成すると共に、そのアプリケーションに割り当てたすべてのサーバにおけるそのアプリケーション以外のすべての HTTP トラフィックを監視する <appname>（その他）アプリケーションを作成します。 この <appname>（その他）アプリケーションを使用して、Web サイト上のリソース変更を分析します。 たとえば、<*appname*>（その他）アプリケーションのパフォーマンスが低下した場合は、サーバ上の HTTP トラフィックを分析し、必要に応じてリソース パスを追加します。

Web アプリケーションの負荷が分散されている場合は、そのアプリケーションにサーバ サブネットを割り当てると、サーバがプロビジョニングされると同時に、管理コンソールが自動的に各リソース パスのレスポンス時間を監視できるようになります。

詳細:

インターネットに接続する Web サービス (P. 144)

Web アプリケーションの考慮事項

Web アプリケーションを作成するときは、以下の情報も考慮してください。

- Web アプリケーションを監視するには、パケット フィード CA Standard Monitor を使用する必要があります。 CA Standard Monitor は、Web アプリケーションを監視する唯一の監視デバイスです。Web アプリケーションを作成した後、Packets 監視フィードが Web アプリケーションに属するすべてのサーバに割り当てられたことを確認します。
- サーバ上のすべての HTTP トラフィックを監視する Web アプリケーションは作成しないでください。 サーバ上の TCP-80 または 8080 のトラフィックをすべて監視する場合は、標準アプリケーションを作成します。 監視 が HTTP ヘッダを処理する必要があるため、Web アプリケーションは 監視デバイス を集中的に使用するプロセスです。
- 3 つ以上の非標準ポートで Web アプリケーションを監視しないでください。 非標準ポートとは TCP-80 や TCP-8080 以外のポートです。 たとえば、TCP-80 と TCP-8080、その他 2 つのポートで Web アプリケーションを監視できます。 非標準ポートを処理するには、追加のリソースが必要になるため、管理コンソール パフォーマンスに悪影響を与える可能性があります。
- ユーザがプロキシ サーバによって Web アプリケーションにアクセスすると、管理コンソール はプロキシ サーバのクライアント ネットワーク内のアプリケーション トラフィックをレポートします。

  プロキシ サーバが X-Forwarded-For （XFF）を使用する場合、管理コンソール は XFF ヘッダを変換し、プロキシ サーバのクライアント ネットワークではなく実際のクライアント ネットワークについてレポートすることができます。
- 管理コンソール は、Web アプリケーションからの HTTP セッションはレポートしません。
- 管理コンソール は、HTTPS（TCP-443）上の Web アプリケーション トラフィックを監視できません。これは、URL が暗号化されるためです。このようなトラフィックはすべて、［その他］アプリケーションに表示されます。

詳細:

サーバの編集 (P. 93)
XFF 翻訳のサポート (P. 328)

インターネットに接続する Web サービス

レスポンス時間の計算を行うとき、管理コンソール は、アプリケーション サーバの隣に位置しているものと想定します。 サーバの近くでレスポンス時間を監視することで、管理コンソール が正確にネットワークおよびサーバのレスポンス時間を測定できます。

管理コンソールはサーバではなくクライアントの隣にあるため、インターネット上の Web サイトを監視すると、メトリックに歪みが生じます。 クライアントで測定されたサーバ レスポンス時間には、サーバへのネットワーク遅延が含まれます。

インターネットに接する Web アプリケーションを監視する場合、ネットワーク パフォーマンス メトリックに対するパフォーマンスしきい値を無効にし、サーバ パフォーマンス メトリックに対するパフォーマンスしきいのみを監視することをお勧めします。 ネットワーク メトリックでしきい値を設定することは、特定の回線を共有する、特定のサイト専用のクライアント サブネットでのみ意味を持ちます。 インターネットは、意味のあるネットワーク パフォーマンスしきい値を設定するためのカテゴリとしては広すぎます。

google.com などのサードパーティ サービスを監視する場合は、IPSLA テストを使用してレスポンス時間を記録しますが、インターネット遅延、サーバ レスポンス、またはアプリケーションの問題が原因でいつスパイクが発生するかを知ることはできません。

詳細:

パフォーマンスしきい値の編集 (P. 178)

Web アプリケーションの作成

監視する Web サーバ上のリソースのパスを指定して、Web アプリケーションを作成します。 管理コンソール が自動的に作成する Web アプリケーションは、そのアプリケーションに割り当てられるすべてのサーバにおいて一致した HTTP トラフィックについてレポートします。

重要: 特定のリソースに対して HTTP トラフィックを監視するには、CA Standard Monitor 上で パケット監視フィードを使用する必要があります。

監視するリソース パスを少なくとも 1 つ指定する必要があります。

重要: サーバ上の すべての HTTP トラフィックを監視する場合は、TCP-80 または TCP-8080 トラフィックを監視する［標準アプリケーション］を作成します。

Web アプリケーションを作成するには、以下の手順に従います。

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. ［アプリケーション リスト］までスクロールし、［アプリケーションの新規作成］をクリックします。
5. ［アプリケーション タイプ］を［Web］に設定します。
6. ［アプリケーションのプロパティ］内のフィールドに入力します。

   Web アプリケーションのプロパティの設定の詳細については、［ヘルプ］を参照してください。
7. ［次へ］をクリックしてアプリケーションにサーバ サブネットおよびサーバを割り当て、［OK］をクリックします。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

9. アプリケーションに割り当てられているすべてのサーバが CA Standard Monitor 上の Packets 監視フィードにも割り当てられるように、サーバのプロパティを編集します。 Packets 監視フィードは Web アプリケーションを監視するのに必要です。

詳細:

テナントの管理 (P. 113)
サーバの編集 (P. 93)
アプリケーションへのサーバの割り当て (P. 150)

FTP アプリケーションの作成

特定のサーバ上のアクティブな FTP を監視するには、FTP アプリケーションを作成します。 管理コンソール はアクティブな FTP セッションをすべて自動的に監視します。FTP アプリケーションは、任意のタイプの 監視デバイス で監視できます。

アクティブな FTP では、要求アクションとレスポンス アクションが別々のポートで発生するので、管理コンソール はレスポンス時間を決定するためにコマンド ポートとデータ ポートをペアとして監視します。

アクティブな FTP では以下のようになります。

TCP ポート	内容
20	データ ポート。クライアントにデータを転送する、FTP サーバのローカル データ ポート。
21	コマンド ポート。クライアントは、このポートに接続して、FTP コマンドを送信します。

複数のポートを使用するアクティブな FTP アプリケーションを監視する場合は、コントロール ポート アプリケーションを作成します。

管理コンソール が自動的にパッシブ FTP を監視することにも注目してください。ただし、パッシブ FTP はクライアントにデータを転送するためにサーバ上のランダムで権限不要のポートを開くため、アプリケーション アクティビティのボリュームは少量です。このため、パッシブ FTP アプリケーションが 管理コンソール の［操作］ページに表示されることはまれです。

アクティブな FTP アプリケーションを作成するには、以下の手順に従います。

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. ［アプリケーション リスト］までスクロールし、［アプリケーションの新規作成］をクリックします。
5. ［アプリケーション タイプ］を［FTP］に設定します。
6. ［アプリケーションのプロパティ］内のフィールドに入力します。

   FTP アプリケーションのプロパティの設定の詳細については、［ヘルプ］を参照してください。
7. ［次へ］をクリックしてアプリケーションにサーバ サブネットおよびサーバを割り当て、［OK］をクリックします。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
コントロール ポート アプリケーションの作成 (P. 149)
アプリケーションへのサーバの割り当て (P. 150)

コントロール ポート アプリケーションの作成

コントロール ポートが要求情報を送受信すると共にデータ ポートが実際のデータを送受信するアプリケーションを監視するには、コントロール ポート アプリケーションを作成します。 管理コンソール は、トランザクションのレスポンス時間を決定するために、両方のポートを監視する必要があります。 コントロール ポート アプリケーションは、任意のタイプの監視デバイス で監視できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. ［アプリケーション リスト］までスクロールし、［アプリケーションの新規作成］をクリックします。
5. ［アプリケーション タイプ］を［コントロール ポート］に設定します。
6. ［アプリケーションのプロパティ］内のフィールドに入力します。

   コントロール ポート アプリケーションのプロパティの設定の詳細については、［ヘルプ］を参照してください。
7. ［次へ］をクリックしてアプリケーションにサーバ サブネットおよびサーバを割り当て、［OK］をクリックします。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細情報:

テナントの管理 (P. 113)
アプリケーションへのサーバの割り当て (P. 150)

アプリケーションへのサーバの割り当て

アプリケーション リストを使用して、アプリケーションをホストするサーバを参照および管理することができます。

アプリケーションをホストする複数のサーバの IP アドレスが連続する範囲にある場合は、アプリケーションに特定のサーバではなくサーバ サブネットを割り当てます。 サーバ サブネットの指定は 管理コンソール パフォーマンスを最適化し、自動的なサーバ割り当てを有効にします。

既存のサーバ サブネットを再利用するか、またはアプリケーションをホストする実際のサーバをより正確に反映したアプリケーション サブネットを作成します。

*アプリケーション サブネット*は一連のサーバ IP アドレスにわたってデータを収集します。また、そのサブネット マスクはユーザの既存のサーバ サブネットよりも長いか短くなる場合があります。 複数のアプリケーションにアプリケーション サブネットを割り当てることによりそれを再利用できます。

アプリケーションにはサーバ サブネットまたはアプリケーション サブネットを割り当てることを推奨します。 この方法は、サーバ管理者が連続している IP 範囲を使用して、アプリケーション サーバをセットアップする場合に最適です。 アプリケーションへサーバを割り当てないようにします。 ホスト リソースが変更された場合、アプリケーションの監視を続行するためにアプリケーションのサーバ割り当てを更新する必要があります。

その場合は以下を割り当てることができます。

- ドメイン

  管理コンソール が、ドメイン内の一致するサーバをすべてアプリケーションに自動的に割り当てて、サーバ サブネットの変更に応じてアプリケーション サーバ割り当てを最新に保つことができるようにします。

  トラフィックを分離するためにドメインを作成していない場合、デフォルトのドメインを割り当てると、管理コンソール によって監視されているすべてのサーバが割り当てられます。

- 既存のサーバ サブネットまたはアプリケーション サブネットによって指定されたサーバ IP アドレスの範囲。

たとえば、管理コンソール を設定しサーバ VLAN 定義に密接に連携するサーバ サブネットを使用してサーバを監視する場合、同じサーバ サブネットをアプリケーションに割り当てることができます。

- 新アプリケーション サブネット。

  たとえば、既存の/22 サーバ サブネットがあるが、特定のアプリケーションに関して、その/26 サーバ サブネット定義がわかっている場合は、/26 アプリケーション サブネットを作成し、アプリケーションにそれを割り当てます。

- サーバ。

  ［サーバ リスト］からサーバを割り当てるか、または新しいサーバを追加できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. ［アプリケーション リスト］までスクロールし、アプリケーションを選択し、［編集］をクリックします。

   ［アプリケーションのプロパティ］が表示されます。
5. ［割り当て］をクリックし、サーバをアプリケーションに割り当てます。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。
6. （オプション）サーバ サブネット、アプリケーション サブネットまたはサーバを選択解除し、それを割り当て解除します。 アプリケーション サブネットがどのアプリケーションにも割り当てられない場合は、コンソールによって自動的に削除されることに注意してください。
7. アプリケーション可用性モニタリングが有効で、ロード バランサが、サーバ間のアプリケーション トラフィックを分散する場合、管理コンソール がサーバ可用性を確認できるよう、利用可能である必要があるサーバの数を指定します。
8. ［OK］をクリックします。

［OK］ボタンが無効な場合は、サーバまたはサブネットをアプリケーションに割り当てていることを確認し、［プロパティ］をクリックしてアプリケーション プロパティが正しく指定されていることを確認します。

9. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
サーバの可用性の確認 (P. 245)

ユーザ定義アプリケーションの編集

たとえば URL を Web アプリケーションへ追加する場合などは、ユーザ定義アプリケーションのプロパティを編集します。

同時に複数のアプリケーションを編集する場合は、可用性監視など共通のアプリケーション プロパティを指定できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. （オプション）ドメインを選択し、利用可能なサーバ サブネットおよびサーバのリストをフィルタします。
4. ［アプリケーション リスト］までスクロールし、編集するアプリケーションを選択し、［編集］をクリックします。

   必要に応じて［リストをリセット］をクリックし、［アプリケーション リスト］からいずれかの選択内容を削除します。
5. ［プロパティ］をクリックし、アプリケーション設定を編集します。

   アプリケーション プロパティの詳細については、［ヘルプ］をクリックしてください。
6. ［割り当て］をクリックし、アプリケーションへのサーバ割り当てを編集して、［OK］をクリックします。

   アプリケーションへのサーバの割り当ての詳細については、［ヘルプ］をクリックしてください。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   指示がない場合は、アプリケーション プロパティの変更において 監視デバイス の同期は要求されなかったことになります。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

ユーザ定義アプリケーションの削除

ユーザ定義アプリケーションを削除し、［アプリケーション リスト］からそれを削除します。またオプションとして、ポート除外を作成し 管理コンソール が対応するアプリケーション ポートを自動的に監視しようとするのを防ぎます。

どのアプリケーションを削除するかを検討するときは、以下のポイントを覚えておきます。

- アプリケーションのレスポンス時間がそれほど重要でないバックアップ アプリケーションなど、時間的制約のないアプリケーションのモニタリングを回避します。
- 監視デバイスおよび管理コンソール上で、フィルタで除外するよりも処理に多くのリソースを使用するアプリケーション、およびそれほどクリティカルでないものは、削除の対象として検討します。たとえば、バックアップ アプリケーションはユーザの環境内のすべてのクライアント IP にわたってトラフィックを生成する場合があり、これによりデータベースで多くの行が消費され、各監視デバイス上の負荷がより高くなる可能性があります。

アプリケーションを削除した後、既存のデータはユーザのデータベース設定に応じてレポート目的に引き続き利用可能です。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. CA PC または CA NPC にドメインを定義している場合、ドメインを選択する必要はありません。アプリケーションに加えるどのような変更もドメインにわたって適用されます。
4. ［アプリケーション リスト］までスクロールし、リストからアプリケーションを選択して、［削除］をクリックします。

   管理コンソール により削除を確認し、オプションとして、一致するポート除外の追加によって 管理コンソール が自動的にアプリケーションを監視するのを回避するようメッセージが表示されます。

   - ［削除］をクリックしてアプリケーションを削除し、管理コンソール が観測されたアプリケーション トラフィックからアプリケーションを再作成できるようにします。

- ［ポート除外の削除および追加］をクリックしてアプリケーションを削除し、またポート除外ルールを作成して 管理コンソール が観測されたアプリケーション トラフィックからアプリケーションを再作成することを回避します。

5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
データベース ストレージ基本設定の編集 (P. 264)

多層アプリケーションの管理

管理コンソール を使用して、ネットワーク、サーバおよび多層アプリケーションの各層のアプリケーション パフォーマンスの可視性を取得します。多層アプリケーションは複数のサーバを使用するアプリケーションで、サーバ間の通信は、クライアントへのリクエストを処理するサーバとして機能すると同時に共に別のサーバのクライアントとしても機能するサーバによって実行されます。

詳細情報:

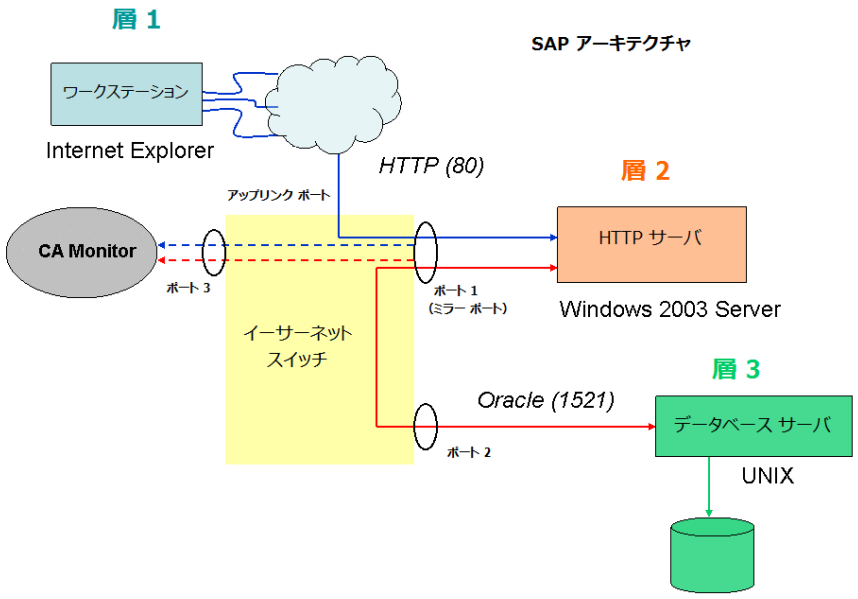
多層アプリケーションの仕組み (P. 157)
多層アプリケーションを監視する方法 (P. 158)

多層アプリケーションの仕組み

以下の層から構成される N 層 SAP アーキテクチャを考えます。

- 層 1 -- Internet Explorer がユーザ ワークステーション上で実行されています。
- 層 2 -- HTTP ベースのアプリケーションが Windows 上で実行されています。
- 層 3 -- データベース サーバが UNIX 上で Oracle を実行しています。

多層アプリケーションにおいて、少なくとも 1 つのサーバは、他のアプリケーション サーバに対しサーバおよびクライアントの両方としての機能を果たします。 上記の例において、層 2 は、層 1 からのユーザ リクエストに対するサーバであり、かつ層 3 サーバからのリクエストに対するクライアントです。



以下のプロセスが行われます。

1. Internet Explorer を使用して、ユーザは、青色の線で示される層 2 HTTP サーバへの接続を開始します。
2. 接続が確立された後、ユーザはアプリケーション データをリクエストします。
3. HTTP サーバは、赤い線で示す、層 3 Oracle データベース サーバへこのリクエストを転送します。
4. Oracle サーバはユーザ クエリを実行し、層 2 HTTP サーバに結果を返します。
5. HTTP サーバは層 1 クライアントにデータを返信します。

アプリケーション層にわたる複数のハンドオフにより、パフォーマンスの問題が N 層アプリケーションで発生した場合にソースの識別が困難になる場合があります。 操作上、層 2 が層 3 のレスポンスを待つとき、そのパフォーマンスは層 3 のパフォーマンスによって決まります。

多層アプリケーションを監視する方法

以下の手順を行い、N 層アプリケーション アーキテクチャを監視しレポートするための 管理コンソール を設定します。

- 監視デバイス に対象のアプリケーション通信をミラーリングします。
- アプリケーション アーキテクチャを監視するために 管理コンソール を設定します。

詳細:

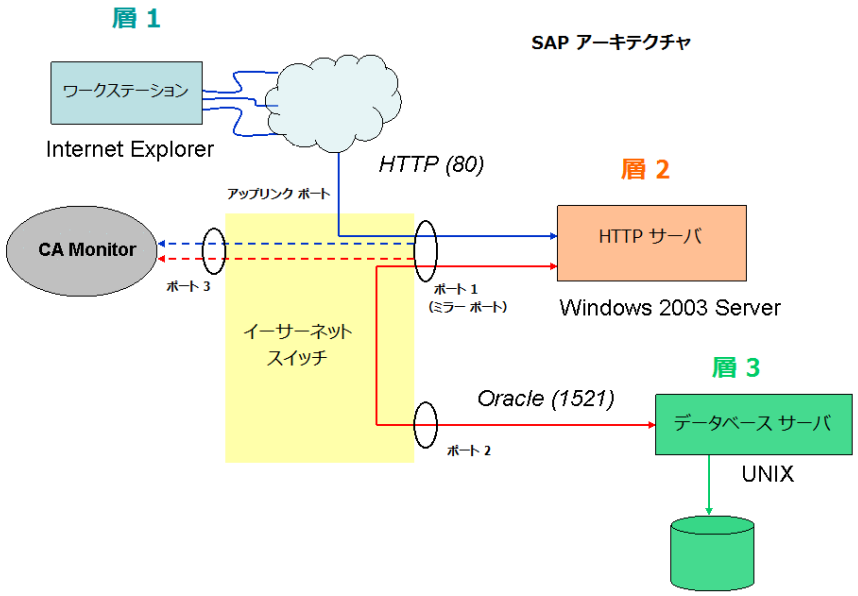
アプリケーション通信をミラーリングする方法 (P. 159)

アプリケーション通信をミラーリングする方法

管理コンソール が N 層アプリケーションの可視性を取得するには、各層の間のホスト通信を 監視デバイス へミラーリングする必要があります。このプロセスを開始するには、サーバおよび 監視デバイス が接続されるイーサネット スイッチにミラーリング コマンドを実行します。ミラー コマンドにより、さまざまなホスト間のパケットが 監視デバイス にコピーされます。 このコピー機能は、スイッチに最小限のパフォーマンス インパクトを及ぼします。

多層アプリケーションが仮想化される場合は、サーバ間のトラフィックを ESX ホスト上の仮想スイッチにミラーリングし、またフロントエンドのサーバ トラフィックを物理 監視 にミラーリングすること考慮します。

以下の図はスイッチ ポート ミラーリングを示しています。



3 つ以上のサーバがある複雑な環境では、複数のポートをミラーリングしてアプリケーション アーキテクチャのすべての層をキャプチャすることが必要な場合があります。 この環境では、ミラーリングするポートを慎重に選択し、同じ通信を 2 回キャプチャしないようにします。

詳細:

監視デバイスに関する推奨事項 (P. 302)

多層アプリケーションの作成

多層アプリケーションを監視するには、各層のアプリケーションを作成し、一部またはすべての層を容易に識別しレポートするのに役立つ命名規則を使用します。

管理、レポートおよび分析を容易にする命名規則を使用して、管理コンソール ユーザが各アプリケーション層の間に従属的関係が存在することをすぐに認識できるようにします。通常、層 2 としてタグ付けされたアプリケーションのパフォーマンスは多くの場合、層 3 としてタグ付けされたアプリケーションのパフォーマンスに依存します。層 2 のアプリケーションのパフォーマンスを分析するときは、層 3 のアプリケーションのパフォーマンスを確認します。

以下のテーブルでは、多層アプリケーションの例を示しています。 このようにアプリケーションの各層を定義すると、各アプリケーションが 管理コンソール で互いに隣り合って表示されます。 この方法では複数のアプリケーション アーキテクチャが表示され、アプリケーションとプロセスのさまざまなエレメントにおいて従属的関係があることがわかります。

アプリケーション名	開始ポート	終了ポート	ポート側	関連サーバ
SAP-HTTP-(80)- 層 2	80	80	アプリケーションはこれらのポートでリスンします。	HTTP
SAP-Oracle-(1521)- 層 3	1521	1521	アプリケーションはこれらのポートでリスンします。	Oracle

次の手順に従ってください:

1. 層 1 のクライアント ネットワークを[ネットワーク リスト]に追加し、24 ビット（以上）のサブネット マスクを必ず指定します。
2. アプリケーション層で使用するすべてのサーバを［サーバ リスト］に追加し、正しい 監視フィード がサーバと関連付けられていることを確認します。

   サーバを追加すると、32 ビット マスクを持つホストとして［ネットワーク リスト］に自動的に追加されます。それはサーバが N 層アーキテクチャの場合と同様にクライアントとして動作することを示します。前記の例では、HTTP サーバは Oracle データベース サーバへのクライアントとして動作します。
3. アプリケーションを 管理コンソール に追加します。 N 層アプリケーションに対し以下の命名規則を使用します。

   <*ApplicationName*>-<*Protocol/Function*>-(<*TCPPort*>)-<*Tier#*>

   変数は、以下のように定義されます。

   <*ApplicationName*>

   アプリケーションの名前です。

   <*Protocol/Function*>

   サーバ上で実行されるアプリケーション デーモンです。

   <*TCPPort*>

   デーモン ポート番号です。

   <*Tier#*>

   層番号です。
4. これらの手順を繰り返し各アプリケーション層を定義します。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

クライアント ネットワークの管理 (P. 33)
サーバの管理 (P. 79)
ユーザ定義のアプリケーションの管理 (P. 137)

アプリケーションのキープアライブ メッセージ

クライアントとサーバの間でやりとりされる定期的なキープアライブ メッセージは、IP ネットワーク内によく見られ、それにより、サーバはクライアントがまだアクティブかまたは到達可能かどうかを決定できます。管理コンソール は通常、TCP キープアライブが RFC 1122 の基準に準拠する場合はそれらを無視し、バイト数および観測合計から関連する統計を除外します。

ただし、カスタム キープアライブの仕組みを使用するように設計されているアプリケーションもあります。 クライアントからのレスポンスがペイロードを含む認識である場合、管理コンソール はクライアントのレスポンスをデータのリクエストとして扱い、サーバ レスポンス時間（SRT）タイマを開始します。 これにより、サーバが通常別のパケットを送信するとき、一旦キープアライブ タイマが終了すると、不正確な SRT 測定および SRT 観測カウントが生じます。

キープアライブを使用する一般的なアプリケーションには、Citrix および Microsoft Exchange が含まれます。 別のアプリケーションがキープアライブを送信していると考えられる場合、観測と SRT の逆比例の関係を調べ、またミリ秒範囲の代わりに秒範囲内の SRT 平均を確認します。

CA Standard Monitor または CA Multi-Port Monitor は、サーバ レスポンス時間によってアプリケーションのキープアライブ メッセージをフィルタするように設定でき、サーバ メトリックを歪曲しないようにできます。

管理コンソール は、NRTT 観測数を使用してアプリケーション キープアライブを使用するアプリケーションをフィルタします。 必要に応じて、5 分間隔で NRTT 観測数の最小数に対するしきい値を調節できます。

詳細:

コンソール設定の管理 (P. 267)
キープアライブ メッセージのフィルタ除外 (P. 341)

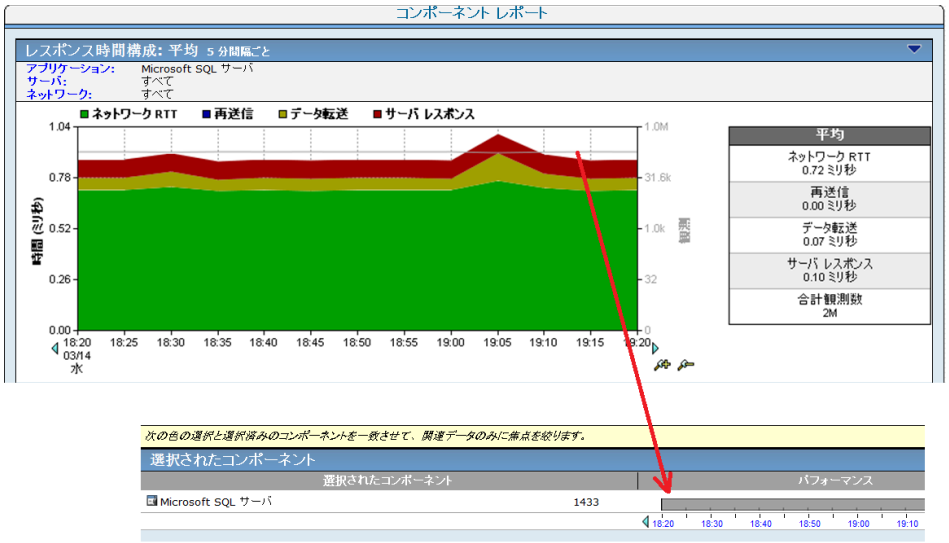
第 6 章: パフォーマンスしきい値の管理

このセクションには、以下のトピックが含まれています。

パフォーマンスしきい値の仕組み (P. 165)
インシデントのオープンおよびクローズの仕組み (P. 175)
パフォーマンスしきい値の編集 (P. 178)
パフォーマンスしきい値の追加 (P. 183)
ネットワーク グループ用のデフォルト パフォーマンスしきい値の有効化 (P. 185)
WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の編集 (P. 186)

パフォーマンスしきい値の仕組み

パフォーマンスしきい値は、［エンジニアリング］ページから詳細なトレンド レポートを、簡単に読み取れる［操作］ページ上の棒グラフ レポートに変換します。



パフォーマンスしきい値により、パフォーマンスの問題を認識することができ、また 管理コンソール は問題を通知するか調査するためのレスポンスを自動的に開始できます。

しきい値は、各システムおよびユーザ定義のアプリケーションに対して存在する、許容範囲内のパフォーマンス動作の境界です。 しきい値は、以下の理由で重要です。

- 管理コンソール がデータを評価することを有効にします。
- インシデント作成とその結果として起こるインシデント レスポンスおよび調査に役立ち、適時のトラブルシューティングおよび問題解決を可能にします。

パフォーマンスしきい値が正しく設定されると、棒グラフ上の色は実際のパフォーマンス問題またはメトリックの劣化に相当します。 正確にしきい値を調整すれば、単に色を一致させるだけでこれらの問題の原因を特定できます。

黄色とオレンジの重大度インジケータは、マイナーなおよびメジャーなパフォーマンスの低下に注意を向けるよう意図されています。 ネットワーク ユーザがヘルプ デスク チケットをサブミットする要因となる実際の状況に、重大度インジケータが確実に対応するようにしきい値設定を調整することを推奨します。

管理コンソール がサーバまたはネットワーク上で低下したアプリケーションのパフォーマンスを確認すると、管理コンソール は自動的にインシデントをオープンします。 ［インシデント］ページから利用可能なインシデントは、パフォーマンスの問題に関する情報の記録を作成します。

パフォーマンスしきい値設定が正しく調節された後、管理コンソール がネットワークとサーバのインシデントにどのように応答するかを選択します。たとえば、特定のクライアント ネットワーク上のアプリケーションのパフォーマンスが低下したときは電子メール通知を送信するなどです。

詳細情報:

インシデント レスポンスの管理 (P. 195)
インシデントのオープンおよびクローズの仕組み (P. 175)

アプリケーション パフォーマンスの評価方法

管理コンソール は、TCP トランザクションを観測し以下を計算することにより、アプリケーションのパフォーマンスを評価します。

- アプリケーションと通信する各クライアント ネットワークのネットワーク メトリック。 ネットワーク メトリックの 5 分平均がしきい値を超え、管理コンソール がメトリックを最小回数観測した場合、管理コンソール は、クライアント ネットワークの対応する 5 分間隔をマイナー（黄色）またはメジャー（オレンジ）と評価し、ネットワーク インシデントを作成します。
- アプリケーションをホストする各サーバのサーバ メトリック。サーバ メトリックの 5 分平均がしきい値を超え、管理コンソール がメトリックを最小回数観測した場合、管理コンソール は、サーバの対応する 5 分間隔をマイナー（黄色）またはメジャー（オレンジ）と評価し、サーバ インシデントを作成します。
- アプリケーション自体の結合メトリック。それにはネットワークおよびサーバ メトリックの両方が含まれます。結合メトリックの 5 分平均がしきい値を超え、管理コンソール がメトリックを最小回数観測した場合、管理コンソール は、アプリケーションの対応する 5 分間隔をマイナー（黄色）またはメジャー（オレンジ）と評価します。

  管理コンソール がアプリケーション インシデントを作成しないことに注意します。ただし、結合メトリックには、ネットワークおよびサーバの メトリックの両方が含まれるので、管理コンソール はサーバまたはネットワークをマイナー（黄色）またはメジャー（オレンジ）と評価し、アプリケーション自体への相当するパフォーマンス インパクトを評価できます。 たとえば、サーバ メトリックが低下する場合、管理コンソール はアプリケーションの結合メトリックをマイナーと評価することもできます。

パフォーマンス データを正常、マイナー（黄色）、またはメジャー（オレンジ）と評価するには、管理コンソール で、GMT の午前 0 時から次の午前 0 時までを 1 営業日として数えて、2 営業日全体のデータを収集する必要があります。 たとえば、管理コンソール がサーバ ポートとクライアント ネットワークとの間の TCP セッションのデータ収集を EST の月曜日午後 3 時 30 分に開始した場合、EST の水曜日午後 7 時まで、管理コンソール はそのネットワークのアプリケーションのパフォーマンスを評価できません。管理コンソール が 2 営業日全体のデータを収集していない場合、管理コンソール はサーバ ポートとクライアント ネットワークとの間の TCP セッションを「未評価」とみなします。

比較によって：

- ［操作］ページの［エクスプローラ］ボタンから利用可能なベースラインは、サーバ上のアプリケーション ポートとクライアント ネットワーク間のすべての TCP セッションの履歴標準をレポートします。 管理コンソール は、すべてのアプリケーション ポート、サーバおよびクライアント ネットワークの間の 1 時間ごとのベースラインを計算し、曜日、日付のそれらおよび先週のアクティビティを追跡します。 管理コンソール はベースラインを使用して、パフォーマンス状態がその日のその時間いつ正常かを示します。管理コンソール は、ベースラインを計算するために 2 営業日全体のデータを要求します。
- ［管理］ページから利用可能な運用レベル契約（OLA）レポートは、現在のパフォーマンスおよびパフォーマンス トレンドを数値で表します。パフォーマンス OLA は、時間単位で特定のしきい値より速いトランザクションの割合を計算することによりアプリケーションがどれくらいよく動作しているかを示します。

詳細:

アプリケーション パフォーマンス OLA の管理 (P. 225)
結合メトリック (P. 171)
ネットワーク メトリック (P. 169)
サーバ メトリック (P. 170)

パフォーマンス メトリックの仕組み

以下のセクションでは、アプリケーションのパフォーマンスを評価するために 管理コンソール が使用するメトリックについて説明します。 アプリケーションが Cisco WAAS または Riverbed Steelhead によって WAN 最適化されている場合、すべてのパフォーマンス メトリックがクライアント、WAN およびサーバ セグメントに適用されるとは限りません。

管理コンソール は、標準的な TCP トランザクションから以下のメトリックを計算します。

- ネットワーク メトリック
- サーバ メトリック
- 結合メトリック

ネットワーク メトリック

ネットワーク メトリックは、アプリケーション パフォーマンスの問題がアプリケーションと通信しているネットワークによって引き起こされることを示します。

ネットワーク ラウンドトリップ時間

ネットワーク上のサーバとクライアントの間をパケットが移動するのにかかる時間（ロスを除く）を測定します。 アプリケーション、サーバおよびクライアント処理時間は除外されます。

ネットワーク接続時間

サーバによって送信された SYN-ACK と、クライアントから受け取った ACK の間の時間です。 ネットワークが混雑していない場合、それは距離およびシリアライゼーションによる最低限の遅延を表すネットワーク遅延を示し、現在のネットワーク アーキテクチャで可能な最良のラウンドトリップ時間を示します。

この値が突然上昇した場合は、一般に輻輳状態が原因と考えられますが、停滞している（上昇したままになる）場合は通常パス変更が原因です。

実効ネットワーク ラウンドトリップ時間

ネットワーク ラウンドトリップ時間と再送信遅延から構成されます。再送信遅延が再送信による遅延ではないことに注意します。それは 1 往復あたりの再送信遅延の平均時間です。管理コンソール が 2 つの平均を追加しており実際 2 つのメトリックを組み合わせていることに注目する必要があります。

再送信遅延

元のパケット送信と最後の重複したパケット送信の間の経過時間です。管理コンソール は再送信パケット数に対してだけではなく観測を通した平均としての再送信遅延をレポートします。 10 個で 1 セットの 1 つのパケットが 300 ミリ秒の再送信時間を必要とする場合、再送信遅延は 30 ミリ秒（300 ミリ秒/10 パケット）としてレポートされます。

サーバ メトリック

アプリケーション パフォーマンスの問題がアプリケーションをホストするサーバによって引き起こされることを示します。

サーバ レスポンス時間

サーバが初期のレスポンスをクライアント リクエストに送信するのに必要な時間、またはサーバの最初の「思考時間」です。サーバ レスポンス時間の増加は通常以下を示します。

- CPU、メモリ、ディスクまたは I/O などサーバ リソースの不足
- アプリケーションの設計に問題がある
- 多層アプリケーション内にパフォーマンスの悪い層がある

サーバ接続時間

サーバが、クライアントの SYN パケットに応えて Syn-Ack を送信することにより、初期クライアント接続リクエストを確認するために要する時間です。

拒否されたセッションの割合

3 方向ハンドシェーク (504以下のページで定義参照：)中にサーバによって明示的に拒否された接続リクエストの割合です。 未対応の TCP/IP セッション リクエスト レポートの一部です。

無応答セッションの割合

接続リクエストは送信されたが、サーバが応答しない場合のセッションの割合です。 未対応の TCP/IP セッション リクエスト レポートの一部です。

結合メトリック

アプリケーションをホストするサーバ、およびアプリケーションと通信しているネットワークの両方によってアプリケーション パフォーマンスの問題が引き起こされることを示します。

トランザクション時間

完全なアプリケーション レスポンスを送信するのにかかる時間で、最初のレスポンス（サーバ レスポンス時間の終了）からそのリクエストで送信された最後のパケットまでの時間で測定され、アプリケーションの設計、サーバやネットワークのパフォーマンスによって影響を受けます。

管理コンソール は、［エンジニアリング］ページの［レスポンス時間構成: 平均］レポート内にこの種のレスポンス時間のデータを表示します。管理コンソール は、トランザクション時間のしきい値を超えた場合にインシデントをオープンしません。

データ転送時間

サーバが応答を開始し、データの送信が完了するまでの経過時間です。レスポンス サイズ、ネットワークで利用可能な帯域幅、およびアプリケーションとネットワークの間の相互作用など要因は、値に影響します。

管理コンソール は、データ転送時間のしきい値を超えた場合にインシデントをオープンしません。

パフォーマンスしきい値をカスタマイズするオプション

パフォーマンスしきい値は、以下の方法で指定できます。

- 感度レベルの入力。管理コンソール は、感度レベルに基づき動的にしきい値を生成します。
- ミリ秒で静的な値を入力または割合を指定。
- メトリックのしきい値の無効化。

デフォルトでは、感度オプションは有効です。 どちらの方法を使用しても、しきい値には常に最小観測数に見合う値が含まれます。 *観測*は、管理コンソール が TCP トランザクションからメトリックを計算する機会です。メトリックのパフォーマンスを正常、マイナー（黄色）またはメジャー（オレンジ）と評価するために、監視デバイス は、最小観測数を参照する必要があります。

あるいは、ネットワーク、サーバまたはアプリケーションのパフォーマンスを評価するとき、特定のメトリックを含まないことを選択できます。

感度レベル（動的な値）

感度レベルを指定すると、管理コンソール は、適切な設定を決定するために過去 30 日間のパーセンタイル統計を使用して、GMT の午前 0 時ごとにメトリックの新しいしきい値を自動的に生成します。 管理コンソール は、各クライアント ネットワークからアプリケーションにアクセスするユーザのためのしきい値の個別のセットを生成します。

その結果、管理コンソール は、待ち時間の長いリモート リンク上のユーザに対して、ローカル LAN 上のユーザと同じしきい値を適用しません。しきい値は履歴上の極端なパフォーマンスを表します。 たとえば、マイアミのデータ センターにあるアプリケーション サーバで、アプリケーションにローカルにアクセスするユーザとミュンヘン（ドイツ）のリモートサイトからアクセスするユーザがいると考えます。

感度レベルを使用してこのアプリケーションのパフォーマンスしきい値を設定すると、管理コンソール は各クライアント ネットワークからアプリケーションにアクセスするユーザのためのしきい値の個別のセットを生成します。 また、感度レベルを指定することは、ミュンヘンとのやりとりおよびマイアミとのやりとりなどのように同じアプリケーションを 2 回定義して遠隔地でのアプリケーションのパフォーマンス用の別のしきい値を設定する必要がないことを意味します。

しきい値の感度が上がると、パフォーマンス レベルに基づいてより多くのインシデントを受信することが目的となるので、しきい値は低下します。管理コンソール 感度しきい値は痛覚感度に似ています。 痛感感受性の高い人は、痛みのしきい値が低く、痛みを訴える頻度も多くなります。 それほど敏感でない人は、ある程度の痛みに対応でき、頻繁には痛みを訴えません。

感度は、0 （無感覚）～ 200 （非常に敏感）の値から調節できます。

- 感度を 200 に設定すると、75 パーセンタイルを超えるトラフィック測定をマイナー（黄色）またはメジャー（オレンジ）として評価することになります。
- 感度を低く設定すると、高いしきい値が生成され、インシデント数も少数になります。

管理コンソール がしきい値を再計算した場合、感度レベルは変わりません。 感度レベルの今日のしきい値を表示するには、感度計算機を使用します。

詳細:

［環境管理］ページからのしきい値の編集 (P. 179)

静的なしきい値（静的な値）

ミリ秒または百分率によるしきい値の設定を選択することで、特定のメトリックに対し静的なしきい値を指定できます。 この値は変更しない限り変わりません。

静的なしきい値は、高度に不変であるか、または低品質のパフォーマンスに対する値がわかっているメトリックのターゲット値を定義するために使用できます。たとえば、正常なサーバは、クライアントからのセッション リクエストを拒否する必要はないので、マイナー（黄色）に対する拒否として 1%、メジャー（オレンジ）に対して 3% の静的なしきい値を設定することで、管理コンソール がセッションを頻繁に拒否するサーバのサーバ問題を無視するのを防ぐことができます。

静的なしきい値を使用するのが適切であるその他のメトリックには以下があります。

- 無応答セッション。 正常なサーバではゼロである必要があります。 5 ～ 10% の低いしきい値に設定します。
- サーバ接続時間。サブミリ秒にする必要があります。管理コンソールがアプリケーション サーバと同じスイッチ上でデータを収集している限りは 2 ～ 5 ミリ秒間隔のアラームを設定します。

また、ミリ秒または百分率の静的な値を設定することは、しきい値がもはやネットワークおよびサーバによって自動的に分離されないことを意味します。 この問題を解決するには、ネットワーク タイプ別に同様の遅延があるネットワークをグループ化し、次に、しきい値のカスタム セットを各ネットワーク タイプに割り当てる必要があります。

指定されたアプリケーションの静的なしきい値を設定する前に、［エンジニアリング］ページのレポートを表示し、［設定］ボタンを使用して問題のメトリックを選択します。 メトリックの確認や根本的な問題を修正することなく、恒久的に低下したしきい値レベルでサーバ、ネットワークまたはアプリケーションを設定しないでください。

詳細情報:

パフォーマンスしきい値の追加 (P. 183)

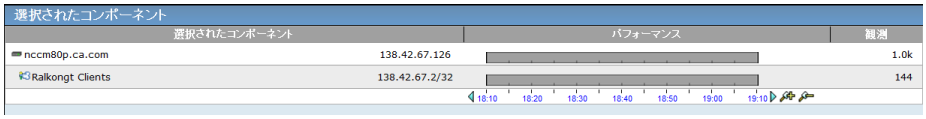
インシデントのオープンおよびクローズの仕組み

管理コンソール は、ネットワークまたはサーバのメトリックの 5 分平均がしきい値を超えると、ネットワークおよびサーバのインシデントをオープンします。

管理コンソール は以下の場合、自動的にインシデントをクローズします。

- 許容範囲のパフォーマンス動作が 1 時間きっかり（正時から次の正時まで）発生した。
- ネットワークまたはサーバ インシデントと関連付けられるサーバが保守ウィンドウに入る。 予定した保守期間が終了した後にパフォーマンスの問題が続く場合、管理コンソール は新規のインシデントをオープンする場合があることに留意してください。
- 24 時間を経過したインシデント。 パフォーマンスの問題が続く場合、管理コンソール は新規のインシデントをオープンする場合があることに留意してください。

インシデントを確認し、問題を認識することもできます。 以下の例で、管理コンソール は、191.168.1.0/24 ネットワーク上のネットワーク インシデントを午前 7 時 5 分にオープンしました。午前 7 時 20 分を過ぎると、その後のネットワークしきい値違反がないため、管理コンソール は午前 9 時にそのインシデントをクローズしました。管理コンソール は 00 分にインシデントをクローズするので、インシデントを確認すると、レポートはそのインシデント前の時間、つまり午前 7 時をマーキングし、インシデントのタイム フレームを示すことに留意してください。



ユーザが可用性の OLA を設定している場合、アプリケーションが使用不可と考えられるとき、管理コンソール はサーバ インシデントをオープンします。

詳細情報:

アプリケーション可用性の管理 (P. 239)
サーバ保守のスケジュール (P. 103)
アプリケーション パフォーマンスの評価方法 (P. 167)

NetQoS Performance Center（CA NPC）

管理コンソール がデータ ソースとして CA NPC に登録されている場合、管理コンソール が新しいマイナー（黄色）またはメジャー（オレンジ）の状態を検出すると、管理コンソール はインシデントをオープンし、CA NPC は対応するイベントをオープンします。

- CA Application Delivery Analysis インシデントを引き起こしたマイナーまたはメジャー状態が 1 時間、正常なパフォーマンスを示すと、管理コンソール はそのインシデントをクローズし、イベント マネージャは対応するイベントをクリアします。 その後、マイナーまたはメジャーのインシデント状態が戻ると、管理コンソール は新規インシデントをオープンし、CA NPC は対応するイベントをオープンします。
- 管理コンソール インシデントが 24 時間オープンのままであると、管理コンソール は、その状態に関係なく自動的にインシデントをクローズします。 マイナーまたはメジャーのインシデント状態がまだ存在する場合、管理コンソール は新規インシデントをオープンし、CA NPC は、対応するイベントの数を増分します。 それ以外の場合、およそ 10 分の同期遅延の後、CA NPC はイベントをクリアします。

サーバがオフラインの状態で CA NPC が CA Application Delivery Analysis インシデントと関連付けられたイベントをクリアできるようにするには、イベント マネージャが対応するイベントをクリアできるように、管理コンソール がマイナーまたはメジャーのインシデント状態に対して「データなし」を 1 時間レポートする必要があります。サーバがオンラインに戻った後、管理コンソール が新しいマイナーまたはメジャーの状態を検出した場合、管理コンソール はインシデントをオープンし、CA NPC は対応するイベントをオープンします。

CA NPC では、ユーザが 管理コンソール インシデントに対応するイベントをクローズすると、インシデント ステータスは［確認済み］に変わります。インシデントの状態が 1 時間の正常なパフォーマンスを示した後、管理コンソール は自動的にそのインシデントをクローズします。

CA Performance Center（CA PC）

管理コンソール がデータ ソースとして CA PC に登録されている場合、CA Application Delivery Analysis インシデントは CA PC に表示され、CA Application Delivery Analysis 管理コンソールによって管理されます。 CA PC は、CA Application Delivery Analysis インシデントを確認またはクローズしません。

CA PC の［パフォーマンス イベント］ページには、CA Application Delivery Analysis インシデントがリストされ、サーバおよびネットワーク別のインシデント数が表示されます。 このページから、CA Application Delivery Analysis インシデントをクリックし、インシデント詳細を表示してインシデントを確認するために CA Application Delivery Analysis 管理コンソール にドリル インできます。

- CA Application Delivery Analysis インシデントの原因となったマイナーまたはメジャーの状態が 1 時間正常なパフォーマンスを示すと、管理コンソール はそのインシデントをクローズし、CA PC は対応するインシデントをクリアします。 その後、マイナーまたはメジャーのインシデント状態が戻ると、管理コンソール は新規インシデントを オープン し、CA PC は対応するインシデントをリスト表示し、そのインシデント数を増分します。
- 管理コンソール インシデントが 24 時間オープンのままであると、管理コンソール は、その状態に関係なく自動的にインシデントをクローズします。 マイナーまたはメジャーのインシデント状態がまだ存在する場合、管理コンソール は新規インシデントをオープンし、CA PC は、対応するイベント数を増分します。 それ以外の場合、約 10 分の同期遅延の後、CA PC は対応するインシデントをクリアします。

CA PC が、サーバがオフラインの状態で CA Application Delivery Analysis インシデントをクリアできるようにするには、CA Application Delivery Analysis が、マイナーまたはメジャーのインシデント状態に対して［データなし］を 1 時間レポートする必要があります。サーバがオンラインに戻った後に、管理コンソール が新しいマイナーまたはメジャーの状態を検出すると、管理コンソール はインシデントをオープンし、CA PC は対応するインシデントをリスト表示して、そのインシデント数を増分します。

パフォーマンスしきい値の編集

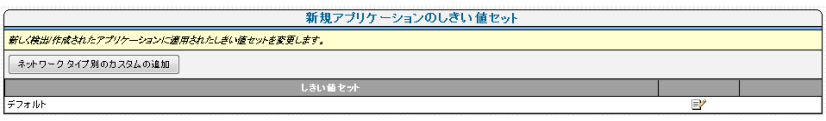
パフォーマンスしきい値を使用すると、管理コンソール によってパフォーマンスを評価し、インシデントをオープンすることができます。必要な場合、クライアント ネットワークのグループまたはすべてのクライアント ネットワークにわたってアプリケーションのパフォーマンスしきい値をきつくするか緩めることができます。

ネットワーク タイプ別にパフォーマンスしきい値をカスタマイズすることで、ネットワーク インシデント レスポンスをカスタマイズします。

パフォーマンスしきい値リストを使用して、各ネットワークのパフォーマンスしきい値のリストを管理します。以下の例では、DCOM Service Control Manager アプリケーションには、オースティンおよびサンディエゴのネットワーク タイプにクライアント ネットワーク用のカスタムしきい値があります。管理コンソール はデフォルト ネットワーク タイプでパフォーマンスしきい値を使用し、ネットワーク タイプが割り当てられていないクライアント ネットワーク上でアプリケーション パフォーマンスを監視します。

新規アプリケーションに適用されるパフォーマンスしきい値の管理には、［新規アプリケーションのしきい値セット］リストを使用します。

また、特定のネットワーク タイプ用のしきい値を作成して、アプリケーションが作成または検出されたときに、カスタムしきい値がそのネットワーク上のアプリケーションに自動的に適用されるようにもできます。たとえば、VPN を介してアクセスするアプリケーションに対しては、ネットワーク レスポンス時間のパフォーマンスしきい値を緩くするか無効にします。 デフォルトでは、新しいアプリケーションはすべて、そのネットワーク タイプに対して確立されたパフォーマンスしきい値のセットを使用します。



[環境管理]ページからのしきい値の編集

パフォーマンスしきい値は以下のような場合に編集します。

- すべての関連付けられたクライアント ネットワークの共通のしきい値を設定します。たとえば、すべてのクライアント ネットワークに対してアプリケーションのサーバ メトリックを調整できます。

  一般に、サーバはそのクライアント リクエストをすべて同じ方法で処理する必要があります。

- クライアント ネットワークのグループと通信するすべてのアプリケーションの共通のしきい値を設定します。 たとえば、オースティン ネットワーク タイプに属するクライアント ネットワークと通信するすべてのアプリケーションのネットワーク メトリックを調整することができます。

管理コンソール でアプリケーション、サーバ、またはネットワークを評価するときにメトリックを含めたくない場合は、メトリックを無効にできます。メトリックを無効にすると、管理コンソール は利用可能なメトリックを使用して、アプリケーション、サーバまたはネットワークを評価します。

管理コンソール がアプリケーションのパフォーマンスを評価するのを防ぐには、アプリケーション上のネットワーク、サーバ、および結合メトリックをすべて無効にします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値]リストにスクロールし、目的のアプリケーションのパフォーマンスしきい値を探して、 をクリックして編集します。加えた変更は、割り当てられたネットワーク タイプを持つすべてのクライアント ネットワークに適用されます。

   ［アプリケーションしきい値の編集］が表示されます。
4. 編集するメトリック上の［変更］をクリックします。
5. マイナーおよびメジャーのインシデントのメトリックしきい値をカスタマイズします。
   - しきい値を測定する方法を選択し、次に、しきい値を指定します。

- ［最小観測数］下で、最小観測数、または 管理コンソール が 5 分間隔でメトリックを計算する必要がある回数を指定します。 たとえば、管理コンソール は、TCP トランザクションにつき 1 回サーバ接続時間を計算できます。しかし、クライアント/サーバ ペアがパケットを交換するごとに、管理コンソール は NRTT を計算します。管理コンソール がメトリックを最小回数計算しない場合、メトリックのステータスは 5 分間間隔で［未評価］となります。

しきい値プロパティの設定の詳細については、［ヘルプ］をクリックしてください。

6. ［適用］をクリックします。
7. これらの手順を繰り返し追加のメトリックについてマイナーおよびメジャーのしきい値を編集します。
8. ［OK］をクリックします。

詳細:

パフォーマンス メトリックの仕組み (P. 168)

[操作]ページからのしきい値の編集

［操作］ページの［エクスプローラ］ボタンから、管理コンソール 管理者またはネットワーク オペレータは、特定のメトリックのしきい値を変更できます。 ［操作］ページからしきい値を変更するには、クライアント ネットワーク、サーバ、アプリケーションおよびメトリックを選択することで、その問題を分離します。 次に、［エクスプローラ］をクリックし選択されたメトリックのしきい値を編集します。

選択したネットワークにネットワーク タイプが割り当てられている場合、パフォーマンスしきい値の編集はそのネットワーク タイプに属するすべてのクライアント ネットワークに適用されます。たとえば、ユーザがセールス アプリケーション上の NRTT のしきい値を変更し、ロンドン ネットワーク タイプに属するクライアント ネットワークを選択した場合、しきい値の変更はロンドン ネットワーク タイプに割り当てられるすべてのクライアント ネットワークに適用されます。

注: ［エクスプローラ］ボタンの詳細については、「*ユーザ ガイド*」を参照してください。

次の手順に従ってください:

1. ［操作］ページをクリックします。
2. ［設定］をクリックします。
3. ［設定］ダイアログ ボックスが表示されます。
4. 必要なクライアント ネットワーク、サーバ、アプリケーションおよびメトリックを選択します。

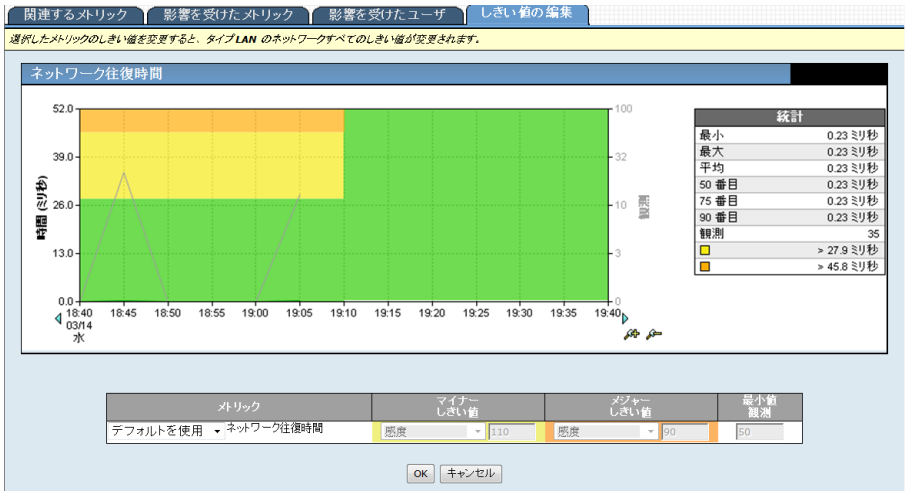
   レポート設定の指定の詳細については、［ヘルプ］をクリックしてください。
5. ［エクスプローラ］をクリックします。

   ［メトリック詳細］が表示されます。

6. ［しきい値の編集］タブをクリックします。

   選択したネットワークにネットワーク タイプが割り当てられている場合、パフォーマンスしきい値の編集はそのネットワーク タイプに属するすべてのクライアント ネットワークに適用されます。

   以下の例では、NetQoS LAN ネットワークは T1 ネットワーク タイプに割り当てられます。 NRTT の LDAP ［クライアント］アプリケーション パフォーマンスのしきい値の変更は、T1 ネットワーク タイプに割り当てられるすべてのネットワークに適用されます。



7. パフォーマンス メトリックを編集して、［最小観測数］とともに、必要なマイナーおよびメジャーのしきい値を指定します。

8. ［OK］をクリックします。

詳細情報:

［環境管理］ページからのしきい値の編集 (P. 179)

パフォーマンスしきい値の追加

特定のネットワーク グループにおけるユーザ定義アプリケーションのパフォーマンスしきい値を厳しくまたは緩く設定します。 このためには、ネットワーク タイプ別にアプリケーションのパフォーマンスしきい値をカスタマイズします。

前提条件： ネットワーク グループを定義するにはネットワーク タイプを割り当てます。 ネットワーク タイプを使用すると、デフォルト パフォーマンスしきい値をネットワーク グループに追加できます。

ネットワーク グループのカスタムしきい値セットを使用して新規アプリケーションを自動的に監視するには、新規アプリケーション用のパフォーマンスしきい値を作成します。

あるいは、アプリケーションのデフォルトしきい値の設定を編集できます。デフォルトしきい値の設定は、割り当てられたネットワーク タイプがないすべてのネットワークに適用されます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値］リストまでスクロールします。
4. ［ネットワーク タイプ別のカスタムの追加］をクリックします。

   ［ネットワーク タイプ別のしきい値のカスタマイズ］が表示されます。
5. パフォーマンスしきい値を定義するユーザ定義アプリケーションおよびネットワーク タイプを指定して、［OK］をクリックします。

   ［アプリケーションしきい値の編集］が表示されます。
6. 目的のネットワーク タイプに対するアプリケーションのパフォーマンスしきい値をカスタマイズし、［適用］をクリックします。
7. ［OK］をクリックします。

詳細情報:

ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)
パフォーマンスしきい値の編集 (P. 178)
ネットワーク グループ用のデフォルト パフォーマンスしきい値の有効化 (P. 185)

ネットワーク グループ用のデフォルト パフォーマンスしきい値の有効化

ネットワーク グループ上で新しく検出されたアプリケーションに対してより厳しいまたは緩いパフォーマンスしきい値を設定するには、目的のネットワーク グループにデフォルト パフォーマンスしきい値を追加します。 このしきい値は、新しいシステムまたはユーザ定義アプリケーションに自動的に適用されます。

デフォルトのしきい値を有効にすると、これらは新規アプリケーションにのみ適用されます。 既存のアプリケーションは、既存のパフォーマンスしきい値を保持します。 既存のアプリケーションのパフォーマンスしきい値を一括編集するには、［表示項目］メニューの［データ監視］ - ［アプリケーション］下の［アプリケーション リスト］を使用します。

前提条件： ネットワーク グループを定義するにはネットワーク タイプを割り当てます。 ネットワーク タイプを使用すると、デフォルト パフォーマンスしきい値をネットワーク グループに追加できます。

目的のアプリケーションがすでに存在する場合、ネットワーク グループのパフォーマンスしきい値をアプリケーションに追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［新規アプリケーションのしきい値セット］リストにスクロールします。
4. ［ネットワーク タイプ別のカスタムの追加］をクリックします。

   ［ネットワーク タイプ別のしきい値のカスタマイズ］が表示されます。
5. 目的のネットワーク タイプを選択し、［OK］をクリックします。

   ［アプリケーションしきい値の編集］が表示されます。
6. ネットワーク タイプ別にアプリケーションのパフォーマンスしきい値をカスタマイズします。

   パフォーマンスしきい値設定の詳細については、［ヘルプ］をクリックしてください。
7. ［適用］をクリックします。

指定するパフォーマンスしきい値は、ネットワーク タイプが割り当てられているクライアント ネットワーク上で新たに検出された全アプリケーションに適用されます。

8. ［OK］をクリックします。

詳細:

ユーザ定義アプリケーションの編集 (P. 153)
システム定義のアプリケーションの編集 (P. 133)

WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の編集

管理コンソール は個別のアプリケーションを作成し、ネットワークの最適化されたクライアント、WAN およびサーバ セグメントにわたってアプリケーションのパフォーマンスをレポートします。 各ネットワーク セグメントのパフォーマンスしきい値をカスタマイズし、アプリケーション パフォーマンス変動に対する 管理コンソール の感度を増減させます。 また、最適化されていないアプリケーション トラフィックのパフォーマンスしきい値を指定します。

最適化されたアプリケーション上の最適化されていないトラフィックのしきい値の編集

各ネットワーク セグメントのパフォーマンスしきい値を編集する一方で、管理コンソール でどのトラフィックが最適化されていないかを観測するアプリケーション トラフィックのしきい値を編集できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値］リストまでスクロールします。
4.  をクリックし、WAN 最適化アプリケーションを編集します。

   ［セグメント］列は WAN 最適化アプリケーションを識別します。 管理コンソール がネットワーク セグメント別に最適化されたアプリケーション トラフィックを観測している場合、［セグメント］列のステータスは［はい］になります。
5. 3 番目の［表示項目］メニューで［しきい値］をクリックします。

   管理コンソール が最適化されていないアプリケーション トラフィックからのレスポンス時間メトリックを計算していない場合、［しきい値］コマンドが表示されません。

   ［アプリケーションしきい値の編集］が表示されます。
6. マイナー（黄色）およびメジャー（オレンジ）のインシデントのメトリックしきい値をカスタマイズします。
   - しきい値を測定する方法を選択し、次に、しきい値を指定します。
   - ［最小観測数］下で、最小観測数、または 管理コンソール が 5 分間隔でメトリックを計算する必要がある回数を指定します。 管理コンソール がメトリックを最小回数計算しない場合、メトリックのステータスは 5 分間間隔で［未評価］となります。

   しきい値プロパティの設定の詳細については、［ヘルプ］をクリックしてください。
7. ［Apply］をクリックします。
8. これらの手順を繰り返し、追加のメトリックのしきい値を設定します。
9. ［OK］をクリックします。

詳細情報:

［環境管理］ページからのしきい値の編集 (P. 179)

最適化されたクライアント セグメントのしきい値の編集

WAN 最適化アプリケーションの場合は、各ネットワーク セグメントのパフォーマンスしきい値を編集します。

管理コンソール は、クライアント セグメントから以下のメトリックを計算します。

ネットワーク ラウンドトリップ時間

ネットワーク上のサーバとクライアントの間をパケットが移動するのにかかる時間（ロスを除く）を測定します。 アプリケーション、サーバおよびクライアント処理時間は除外されます。

再送信遅延

再送信によるネットワーク ラウンドトリップ時間の追加遅延を測定します。 表示されたデータはすべての観測の平均で、各トランザクションの実際の再送信時間ではありません。

トランザクション時間

クライアントがリクエストを送信する時間（パケット レベルまたはトランザクション レベル）からクライアントがレスポンスで最後のパケットを受信する時間までの経過時間を測定します。

管理コンソール は、［エンジニアリング］ページの［レスポンス時間構成: 平均］レポート内にこの種のレスポンス時間のデータを表示します。 管理コンソール は、トランザクション時間のしきい値を超えた場合にインシデントをオープンしません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値］リストまでスクロールします。
4.  をクリックし、WAN 最適化アプリケーションを編集します。 ［セグメント］列は WAN 最適化アプリケーションを識別します。 管理コンソール がネットワーク セグメント別に最適化されたアプリケーション トラフィックを観測している場合、［セグメント］列のステータスは［はい］になります。
5. 3 番目の［表示項目］メニューで［クライアント セグメント］をクリックします。

管理コンソール がクライアント ネットワーク セグメントからのレスポンス時間メトリックを計算していない場合、［クライアント セグメント］コマンドが表示されません。

クライアント セグメントのしきい値が表示されます。

6. 各レスポンス時間メトリックに対し、マイナー (黄色) およびメジャー（オレンジ）でパフォーマンスしきい値をカスタマイズします。
   - しきい値を測定する方法を選択し、次に、しきい値を指定します。
   - ［最小観測数］下で、最小観測数、または 管理コンソール が 5 分間隔でメトリックを計算する必要がある回数を指定します。 管理コンソール がメトリックを最小回数計算しない場合、メトリックのステータスは 5 分間間隔で［未評価］となります。

   しきい値プロパティの設定の詳細については、［ヘルプ］をクリックしてください。
7. ［Apply］をクリックします。
8. これらの手順を繰り返し、追加のメトリックのしきい値を編集します。
9. ［OK］をクリックします。

詳細情報:

［環境管理］ページからのしきい値の編集 (P. 179)

最適化された WAN セグメントのしきい値の編集

WAN 最適化アプリケーションの場合は、各ネットワーク セグメントのパフォーマンスしきい値を編集します。

管理コンソールは、WAN セグメントから以下のメトリックを計算します。

ネットワーク ラウンドトリップ時間

ネットワーク上のサーバとクライアントの間をパケットが移動するのにかかる時間（ロスを除く）を測定します。 アプリケーション、サーバおよびクライアント処理時間は除外されます。

ネットワーク接続時間

サーバの接続確認を確定するためにクライアントが必要とする時間を測定します。 遅延はネットワーク遅延によって引き起こされる可能性が高いです。

実効ラウンドトリップ時間

ネットワーク ラウンドトリップ時間と再送信によって引き起こされた遅延が含まれます。 このメトリックのしきい値を設定し、再送信によるパフォーマンスの低下を監視します。

再送信遅延

再送信によるネットワーク ラウンドトリップ時間のさらなる遅延を測定します。 表示されたデータはすべての観測の平均で、各トランザクションの実際の再送信時間ではありません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値］リストまでスクロールします。
4. をクリックし、WAN 最適化アプリケーションを編集します。 ［セグメント］列は WAN 最適化アプリケーションを識別します。 管理コンソールがネットワーク セグメント別に最適化されたアプリケーション トラフィックを観測している場合、［セグメント］列のステータスは［はい］になります。
5. 3 番目の［表示項目］メニューで［WAN セグメント］をクリックします。

管理コンソールが WAN ネットワーク セグメントからのレスポンス時間メトリックを計算していない場合、［WAN セグメント］コマンドが表示されません。

WAN セグメントのしきい値が表示されます。

6. マイナー（黄色）およびメジャー（オレンジ）のインシデントのメトリックしきい値をカスタマイズします。
   - しきい値を測定する方法を選択し、次に、しきい値を指定します。
   - ［最小観測数］下で、最小観測数、または 管理コンソール が 5 分間隔でメトリックを計算する必要がある回数を指定します。 管理コンソール がメトリックを最小回数計算しない場合、メトリックのステータスは 5 分間間隔で［未評価］となります。

   しきい値プロパティの設定の詳細については、［ヘルプ］をクリックしてください。
7. ［Apply］をクリックします。
8. これらの手順を繰り返し追加のメトリックについてマイナーおよびメジャーのしきい値を編集します。
9. ［OK］をクリックします。

詳細情報:

［環境管理］ページからのしきい値の編集 (P. 179)

最適化されたサーバ セグメントのしきい値の編集

WAN 最適化アプリケーションの場合は、各ネットワーク セグメントのパフォーマンスしきい値を編集します。

管理コンソール は、サーバ セグメントから以下のメトリックを計算します。

サーバ レスポンス時間

サーバが、クライアントによって行われたリクエストに対し応答を開始するのにかかる時間を測定します。 この値はサーバ速度、アプリケーション設計およびリクエストのボリュームの影響を受けます。

サーバ接続時間

初期クライアント接続リクエストを確認するためにサーバが必要とする時間を測定します。

拒否されたセッションの割合

3 方向ハンドシェーク中にサーバによって明示的に拒否された接続リクエストの割合を測定します。 未対応の TCP/IP セッション リクエスト レポートの一部です。

無応答セッションの割合

接続リクエストが送信され、クライアントまたはサーバが応答しなかった場合のセッションの割合を測定します。 未対応の TCP/IP セッション リクエスト レポートの一部です。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。
3. ［パフォーマンスしきい値］リストまでスクロールします。
4. をクリックし、WAN 最適化アプリケーションを編集します。 ［セグメント］列は WAN 最適化アプリケーションを識別します。 管理コンソール がネットワーク セグメント別に最適化されたアプリケーション トラフィックを観測している場合、［セグメント］列のステータスは［はい］になります。
5. 3 番目の［表示項目］メニューで［サーバ セグメント］をクリックします。

管理コンソール がサーバ ネットワーク セグメントからのレスポンス時間メトリックを計算していない場合、［サーバ セグメント］コマンドが表示されません。

サーバ セグメントのしきい値が表示されます。

6. マイナー（黄色）およびメジャー（オレンジ）のインシデントのメトリックしきい値をカスタマイズします。
   - しきい値を測定する方法を選択し、次に、しきい値を指定します。
   - ［最小観測数］下で、最小観測数、または 管理コンソール が 5 分間隔でメトリックを計算する必要がある回数を指定します。 管理コンソール がメトリックを最小回数計算しない場合、メトリックのステータスは 5 分間間隔で［未評価］となります。

   しきい値プロパティの設定の詳細については、［ヘルプ］をクリックしてください。
7. ［Apply］をクリックします。
8. これらの手順を繰り返し、追加のメトリックのしきい値を編集します。
9. ［OK］をクリックします。

詳細情報:

［環境管理］ページからのしきい値の編集 (P. 179)

第 7 章: インシデント レスポンスの管理

このセクションには、以下のトピックが含まれています。

インシデント レスポンスの仕組み (P. 195)
インシデント レスポンスの追加 (P. 207)
インシデント レスポンスの編集 (P. 208)
インシデント レスポンスの削除 (P. 209)
ネットワークまたはサーバのインシデント レスポンスへのアクションの追加 (P. 210)
応答アクションの編集 (P. 211)
応答アクションの削除 (P. 212)
インシデント レスポンスの割り当て (P. 212)
インシデント レスポンスのトラブルシューティング (P. 216)
Web サービス メソッドを使用したインシデントの管理 (P. 216)

インシデント レスポンスの仕組み

問題が発生した際にトラブルシューティングし、かつ平均修復時間を短縮できるように、ユーザのビジネス上重要なアプリケーション、サーバおよびネットワークに対しインシデント レスポンスを割り当てます。 インシデント レスポンスは以下を行います。

- ユーザのチームにパフォーマンスの低下を知らせます。
- 問題を積極的に調査し、パフォーマンス低下の根本的原因を特定するのに役立つ追加情報を収集します。

デフォルトでは、管理コンソール はインシデント レスポンスを自動的に開始しません。

［インシデント］ページから調査を手動で開始して、より詳細にインシデントをトラブルシューティングすることもできることに留意してください。 詳細については、「*ユーザ ガイド*」を参照してください。

インシデント レスポンスの開始法

管理コンソール がネットワークまたはサーバのメトリックのしきい値違反を見つけると、管理コンソール は自動的にネットワークまたはサーバのインシデントをオープンします。 ［インシデント］ページから利用可能な*インシデント*は、影響を受けたアプリケーションを含むサーバまたはネットワーク上のパフォーマンスの問題に関する情報の記録を作成します。

管理コンソール が以下のインシデントをオープンする場合。

- サーバ： 管理コンソール はサーバ インシデントを評価し、影響を受けたサーバ上、およびそのサーバ上で実行される低品質なアプリケーションに対し一連のアクションを起こします。
- ネットワーク： 管理コンソール はネットワーク インシデントを評価し、ネットワーク上、およびネットワーク上で実行される低品質なアプリケーションに対し一連のアクションを起こします。

管理コンソール は、結合メトリックを使用してアプリケーションのパフォーマンスを評価しますが、管理コンソール はアプリケーション インシデントを作成しません。ただし、管理コンソール によりアプリケーション インシデント レスポンスを定義できます。 *アプリケーション インシデント レスポンス*はネットワークまたはサーバのインシデントに対するアプリケーション レスポンスです。 たとえば、Exchange アプリケーション用のアプリケーション インシデント レスポンスを設定すると、管理コンソール は以下の場合にインシデント レスポンスを開始します。

- ネットワーク インシデントが Exchange アプリケーションにアクセスするクライアントによって作成される場合。
- サーバ インシデントが、アプリケーションをホストするサーバによって作成される場合。

データ転送時間など結合メトリックのしきい値を超えた場合、管理コンソール はアプリケーション インシデント レスポンスを開始しません。

デフォルトでは、管理コンソール はネットワークまたはサーバのインシデントに応答して通知や調査を開始しません。 デフォルトのインシデント レスポンスを編集して、1 つ以上のアクションを追加し、必要に応じて追加のインシデント レスポンスを作成します。

ネットワーク インシデント レスポンス

ネットワーク インシデント レスポンスはネットワーク インシデントに応答して開始されます。 以下のレスポンスはネットワーク インシデントに利用可能です。

- 電子メール通知 (P. 198)
- SNMP トラップ通知 (P. 199)
- トレース ルート調査 (P. 205)

サーバ インシデント レスポンス

サーバ インシデント レスポンスはサーバ インシデントに応答して開始されます。 以下のレスポンスはサーバ インシデントで利用可能です。

- 電子メール通知 (P. 198)
- SNMP トラップ通知 (P. 199)
- ping レスポンス時間調査 (P. 204)
- SNMP 経由のパフォーマンス調査 (P. 202)
- パケット キャプチャ調査 (P. 201)

アプリケーション インシデント レスポンス

アプリケーション インシデント レスポンスはネットワークまたはサーバのインシデントに応答して開始されます。 以下のアプリケーション レスポンスが利用可能です。

- 電子メール通知 (P. 198)
- SNMP トラップ通知 (P. 199)
- アプリケーション接続時間調査 (P. 200)

  管理コンソールは、［使用不可］と評価されるアプリケーションに応答してこの調査を開始しないことに注意してください。
- パケット キャプチャ調査 (P. 201)

詳細:

アプリケーション可用性のサーバ インシデントの仕組み (P. 242)

電子メール通知

電子メール通知は、影響を受けたアプリケーション、サーバ、またはネットワークの最新のステータスを知らせます。

管理コンソール は、CA PC によって指定された SMTP サーバに電子メール通知を送信します。 そうでない場合、管理コンソール は、CA Application Delivery Analysis コンソール設定によって指定された SMTP サーバに電子メール通知を送信します。 CA NPC の電子メール仕様は、CA NPC からのスケジュール済みレポートまたはアドホック レポートを送信するために使用されます。 CA NPC で設定された SMTP サーバは、管理コンソールによって電子メール通知を送信するために使用されません。

同じ電子メール内に複数のアプリケーション、サーバまたはネットワークを含めるには、同じインシデント レスポンスを複数のアプリケーション、サーバまたはネットワーク タイプに割り当てます。

割り当てられたサーバまたはネットワークがそのインシデント期間および重大度基準に適合する場合、この情報は 管理コンソール が 2 時間ごとに送信するステータス更新メールに含まれます。

期間および基準しきい値を編集し、以下に関する電子メール通知を送信します。

- 時々発生する短期間のマイナーなパフォーマンス低下。 監視が必要な何らかの問題が発生している可能性があります。
- 10 分間続くメジャーなパフォーマンス低下、または 5 分間続く［使用不可］状態。 これらのタイプの状況はすぐに調査してください。

詳細:

コンソール設定の管理 (P. 267)
アプリケーション可用性レポートの仕組み (P. 243)

SNMP トラップ通知

SNMP トラップ通知を使用して、影響を受けたアプリケーション、サーバ、またはネットワークの「オープン」または「クローズ」のインシデント ステータスに関する最新情報を SNMP マネージャに知らせます。

SNMP トラップ通知を任意のインシデント レスポンスに割り当てることができます。 管理コンソール は 管理コンソール コンピュータから SNMPv2 トラップ通知を送信します。

電子メール通知と異なり、管理コンソール は以下の場合に SNMP トラップを送信します。

- サーバまたはネットワークのインシデントをオープンするかクローズするとき。
- （オプション）重大度の変更がサーバまたはネットワークのインシデント上で発生したとき（たとえば、マイナーからメジャーに変更された場合）。

同じ SNMP トラップ内に複数のアプリケーション、サーバまたはネットワークを含めるには、同じインシデント レスポンスを複数のアプリケーション、サーバまたはネットワーク タイプに割り当てます。 複数のアプリケーション、サーバまたはネットワークが影響を受ける場合、SNMP トラップには詳細な URL が含まれます。

デフォルトでは、管理コンソール は *SuperAgent* という名前の SNMPv2 コミュニティを使用して、SNMP トラップを送信します。デフォルトの SNMP プロファイルは、SNMP トラップ通知のみに適用されます。

SNMP マネージャが 管理コンソール からの SNMP トラップ通知を理解できるようにするには、管理コンソール MIB を SNMP マネージャ上のトラップ レシーバにコンパイルします。 コンパイル方法は SNMP マネージャによって異なります。

管理コンソール MIB は 管理コンソール ディストリビューションに含まれていません。 http://support.ca.com で CA サポート Web サイトから CA Application Delivery Analysis MIB をダウンロードします。

CA Application Delivery Analysis トラップ通知では、パフォーマンス メトリックについて以下の省略形を使用します。

省略形	メトリック

省略形	メトリック
ERTT	実効ラウンドトリップ時間
NCT	ネットワーク接続時間
NRTT	ネットワーク ラウンドトリップ時間
RS	拒否されたセッション（割合）
RTNS	再送信遅延
SCT	サーバ接続時間
SRT	サーバ レスポンス時間
US	無応答セッション（割合）

詳細:

SNMP トラップの説明 (P. 223)

アプリケーション接続時間の調査

アプリケーション接続時間の調査を実施して、TCP/IP アプリケーション ポートへ接続するのにかかる時間に関する情報を収集します。 これには、サーバが接続確認で応答する時間が含まれます。

アプリケーション接続時間の調査をアプリケーション インシデント レスポンスに割り当てることができます。 アプリケーションをホストするサーバが CA Standard Monitor によって監視される場合、管理コンソールは 監視デバイス からこの調査を開始します。 そうでない場合、管理コンソール は、管理コンソール から調査を開始します。

管理コンソール が［使用不可］アプリケーションに応答してこの調査を開始しないことに注意してください。

管理コンソール 管理者は、［インシデント］ページからこの調査を開始またはスケジュール設定することもできます。 詳細については、「*ユーザ ガイド*」を参照してください。

アプリケーション接続時間の調査では、成功したおよび失敗した試行数と接続時間に関するレポートが作成されます。

詳細:

アプリケーション可用性のサーバ インシデントの仕組み (P. 242)

パケット キャプチャ調査

パケット キャプチャ調査を実施して、問題が発生している特定のサーバ、アプリケーション ポート、およびネットワークのフィルタされたキャプチャを実行します。

パケット キャプチャ調査をサーバ インシデントに応答するアプリケーション、またはサーバ、およびそのサーバ上で実行される低品質のアプリケーションに割り当てることができます。 管理コンソール は、自動的に適切な 監視デバイス からパケット キャプチャをとります。パケット キャプチャは、以下のように動作します :

- CA Standard Monitor によって取得された場合、キャプチャ ファイルは TCP-8080 上で監視デバイスからユーザのコンピュータにコピーされます。 ユーザのコンピュータが監視デバイスにアクセス権があることを確認してください。
- CA Multi-Port Monitor によって取得された場合、キャプチャ ファイルはユーザのコンピュータにコピーされません。 ユーザは監視デバイス上のキャプチャ ファイルを参照します。

以下の 監視デバイス は、CA Application Delivery Analysis に対しパケット キャプチャ調査を行いません。

- Cisco WAE デバイス
- Cisco NAM デバイス

管理コンソール 管理者は、［インシデント］ページからこの調査を開始またはスケジュール設定することもできます。 詳細については、「*ユーザ ガイド*」を参照してください。

パケット キャプチャ調査レポートには、サーバ、アプリケーション、ネットワークに関する情報と、パケット キャプチャ結果を表示するリンクが含まれます。

SNMP 経由のパフォーマンス調査

SNMP 経由のパフォーマンス調査を実施して、サーバの SNMP ポーリングをそのメモリや CPU 使用率などのパフォーマンス情報について実行します。

SNMP 経由のパフォーマンス調査をサーバ インシデント レスポンスに割り当てます。 サーバが CA Standard Monitor によって監視される場合、管理コンソール は 監視デバイス からこの調査を開始します。そうでない場合、管理コンソール は、管理コンソール から調査を開始します。

管理コンソール 管理者は、［インシデント］ページからサーバまたはルータ上でこの調査を開始したりスケジュールすることもできます。 パフォーマンス情報についてルータを SNMP ポーリングするには、管理コンソール 管理者は、ルータをネットワーク デバイスとして 管理コンソール に追加する必要があります。

- 有効な SNMP プロファイルをサーバまたはネットワーク デバイスに割り当てていない場合、管理コンソール は有効な SNMP プロファイルの検出を試行します。 または、別の CA 製品を使用して、パフォーマンス情報についてサーバおよびルータを SNMP ポーリングすることができます。
- 管理コンソール がサーバまたはネットワーク デバイスを SNMP ポーリングできるようにするには、有効な SNMP プロファイルを 管理コンソール に追加する必要があります。

管理コンソール は以下の基準を使用して、全体のプロセッサおよびプロセス CPU 使用率値をレポートします。

- 個別のプロセッサの割合は、最後まで（最初のポーリング寸前）ホストによってメンテナンスされた HrProcessorTable（1.3.6.1.2.1.25.3.3.1.2）を使用してポーリングされます。これはスナップショットです。
- 個別のプロセス リストは HrSWRunPerfTable (1.3.6.1.2.1.25.5.1.1.1、 .2, cpu および mem)を使用してポーリングされます。CPU 値は生の時間です。 したがって、2 回ポーリングされて減算されました。 割合は、利用可能な CPU 時間で割られた使用済み CPU 時間の合計から算出されます。 メモリの割合は利用可能なメモリで割られた前回のポーリングです。

調査では、以下の MIB に対し、調査時に 2 回 サーバのポーリングを行います。つまりインシデントがオープンしたときと 5 分後に 1 回ずつ行われます。

- システム mib (1.3.6.1.2.1.1.*.0)
- インターフェース mib (1.3.6.1.2.1.2.2.1)
- Cisco CPU mib (1.3.6.1.4.1.9.2.1.*)
- ホスト リソース プロセッサ (1.3.6.1.2.1.25.3.3.1)
- ホスト リソース ストレージ (1.3.6.1.2.1.25.2.3.1)
- IP アドレス テーブル (1.3.6.1.2.1.4.20.1)
- ソフトウェア mib を実行しているホスト リソース (1.3.6.1.2.1.25.4.2.1)
- ソフトウェア パフォーマンス mib を実行しているホスト リソース (1.3.6.1.2.1.25.5.1.1)
- ホスト リソース メモリ (1.3.6.1.2.1.25.2.2.0)

以下で開始またはスケジュールされた場合。

- サーバ： SNMP 経由のパフォーマンス調査では、サーバのパフォーマンスおよびインターフェース統計に関するレポートが生成されます。
- ネットワーク デバイス： SNMP 経由のパフォーマンス調査では、デバイスのパフォーマンスおよびインターフェース統計に関するレポートが生成されます。

詳細:

SNMP プロファイルの管理 (P. 269)
ネットワーク デバイスの追加 (P. 274)

ping レスポンス時間調査

ping レスポンス時間調査を実施して、サーバが ping リクエストに応答できレスポンスを受信する往復の時間を測定できることを確認します。

ping レスポンス時間調査をサーバ インシデント レスポンスに割り当てます。サーバが CA Standard Monitor によって監視される場合、管理コンソールは 監視デバイス からこの調査を開始します。 そうでない場合、管理コンソール は、管理コンソール から調査を開始します。

ユーザは、［インシデント］ページからこの調査の開始またはスケジュール設定を行うこともできます。 詳細については、「*ユーザ ガイド*」を参照してください。

ping レスポンス時間調査では、パケットのラウンドトリップ時間およびレスポンス時間に関するレポートが作成されます。

トレース ルート調査

トレース ルート調査を実施して、遅延とルーティングの問題を監視する監視デバイス とエンドポイントの間のパスおよび各ホップを記録します。またオプションで、パフォーマンス情報に関し各ルータを SNMP ポーリングします。

トレース ルート調査をネットワーク インシデント レスポンスに割り当てます。 アプリケーションをホストするサーバが CA Standard Monitor によって監視される場合、管理コンソール は 監視デバイス からこの調査を開始します。 そうでない場合、管理コンソール は、管理コンソール から調査を開始します。

ネットワーク インシデント中に、管理コンソール は、監視デバイス からトレース ルート調査を開始し、インシデントが発生したネットワーク サブネット上のデバイスにアクセスを試行します。サブネットが /24 かさらに特定できる場合、サブネット内の IP アドレスはターゲットとして使用されます。管理コンソール は、このアドレスのレスポンス時間のデータを収集しておく必要があります。サブネットが /24 内で特定できない場合、管理コンソール は別のメソッドを使用して、サブネット範囲内のアドレスを選択します。トレース ルート アクション プロパティ内でオプション［SNMP 経由でのルータ調査］が有効な場合、トレース ルートがまず実行され、その後、ルート内のネットワーク デバイスのリストが SNMP 調査に使用されます。 管理コンソール が有効な SNMP プロファイルを検出すると、管理コンソール によって、調査結果に含まれるパフォーマンス情報のクエリがデバイスに対して実行されます。

TCP トレース ルートを実行するよう設定された場合、TCP トレース ルートは、発信トラフィックおよび ICMP TTL 期限切れメッセージについて、監視されているアプリケーションの TCP ポートを使用して、発信パケットを強制終了したパスにあるルータを分離します。

管理コンソール 管理者は、［インシデント］ページからこの調査を開始またはスケジュール設定することもできます。

トレース ルート調査では、パス、ホップ、遅延および使用率に関するレポートが作成されます。

必要に応じて、パスにある各デバイスに対してデバイスおよびパフォーマンス インターフェース統計の SNMP 経由のパフォーマンス調査を起動するためにトレース ルート調査を設定できます。

パスに沿って各ホップを SNMP ポーリングするには、ネットワーク デバイスを 管理コンソール に追加する必要はありません。ただし、サーバまたはネットワーク デバイスを SNMP ポーリングするには、有効な SNMP プロファイルを定義する必要があります。SNMP 経由のパフォーマンス調査では、デバイスのパフォーマンスおよびインターフェース統計に関するレポートが作成されます。

パスに沿って各ホップを SNMP ポーリングする場合、有効な SNMP プロファイルを使用して、管理コンソール でネットワーク デバイスを定義していないと、管理コンソール は各ネットワーク デバイス上の有効な SNMP プロファイルを検出することを試行します。 または、別の CA 製品を使用してパフォーマンス情報に関してデバイスを SNMP ポーリングすることもできます。

詳細:

SNMP プロファイルの管理 (P. 269)
ネットワーク デバイスの追加 (P. 274)

インシデント レスポンスの追加

管理コンソール がネットワークまたはサーバのインシデントに応答して通知を送信するかまたは調査を開始できるようにするには、以下を行います。

1. ネットワーク、サーバ、またはアプリケーション インシデント レスポンスを追加。
2. インシデント レスポンスに 1 つ以上のアクションを追加。
3. 特定のネットワーク、サーバまたはアプリケーションに対するインシデント レスポンスの割り当て。

または、デフォルトのネットワーク、サーバおよびアプリケーション インシデント レスポンスを編集して応答アクションを追加します。 デフォルトでは、管理コンソール はネットワークまたはサーバのインシデントに応答して通知や調査を開始しません。

管理コンソール で通知を開始するには、インシデントの期間および重大度の基準を両方満たす必要があります。 期間および重大度の基準を使用して、以下についてインシデント レスポンスを開始します。

- 時々発生する短期間のマイナーなパフォーマンス低下。監視が必要な何らかの問題が発生している可能性があります。
- 1 時間続くメジャーなパフォーマンス低下、または 10 分間続く［使用不可］状態。 これらのタイプの状況はすぐに調査してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. ［表示項目］メニュー下で、クリックしてアクションを追加します。

ネットワーク レスポンスの追加

リモートサイト用のクライアント ネットワークを所有者に通知するか、またはトレース ルート調査を実行します。

サーバ レスポンスの追加

サーバの所有者に通知するか、またはパケット キャプチャ、ping レスポンス時間または SNMP 経由のパフォーマンス調査などサーバベースの調査を実行します。

アプリケーション レスポンスの追加

アプリケーションの所有者に通知するか、またはアプリケーション接続時間調査を実行します。

4. ［適用］をクリックします。

アクションをインシデント レスポンスに追加 (P. 210)できるようになりました。

詳細:

アプリケーション可用性の管理 (P. 239)
インシデント レスポンスの割り当て (P. 212)
監視デバイス インシデントの管理 (P. 305)

インシデント レスポンスの編集

インシデント レスポンスを編集してその名前を変更します。 インシデント レスポンスの名前を変更すると同時に、アクションの編集やアクションの追加など、その応答アクションを変更できます。

インシデント レスポンスの名前を変更するには、以下の手順に従います。

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. インシデント リストを参照し、 をクリックして、ネットワーク、サーバ、またはアプリケーションのインシデント レスポンスを編集します。

   少なくとも 1 つの応答アクションが各インシデント レスポンスに割り当てられていることを確認します。
4. 3 番目の［表示項目］メニューで［インシデント レスポンスの編集］をクリックします。
5. ［インシデント レスポンス名］に新しい名前を入力して、［OK］をクリックします。

詳細:

ネットワークまたはサーバのインシデント レスポンスへのアクションの追加 (P. 210)
応答アクションの編集 (P. 211)
応答アクションの削除 (P. 212)

インシデント レスポンスの削除

インシデント レスポンスの削除により、インシデント レスポンスおよびその応答アクションが削除されます。 インシデント レスポンスが割り当てられると、管理コンソール はデフォルトのインシデント レスポンスを、影響を受けたアプリケーション、サーバまたはネットワークに再割り当てします。

ネットワーク、サーバまたはアプリケーションのデフォルトのインシデント レスポンスは削除できません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. インシデント レスポンス リストを参照し、 をクリックし、ネットワーク、サーバまたはアプリケーションのインシデント レスポンスを削除します。デフォルトのインシデント レスポンスは削除できないことに注意してください。
4. ［削除の確認］で、［削除を続行］をクリックしてインシデント レスポンスを削除します。

ネットワークまたはサーバのインシデント レスポンスへのアクションの追加

ネットワークまたはサーバのインシデントに応じて通知または調査を起動するためのアクションを追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. インシデント レスポンス リストを参照し、 をクリックして、ネットワーク、サーバ、またはアプリケーションのインシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。
5. ［表示項目］メニュー下の［アクションの追加］をクリックします。

   ［アクション タイプ］が表示されます。
6. アクションを選択し、［次へ］をクリックします。

   ［アクションのプロパティ］が表示されます。
7. 応答アクション設定を指定して、［OK］をクリックします。詳細については、［ヘルプ］をクリックしてください。

   ［インシデント レスポンス アクション］に新しいアクションが表示されます。

応答アクションの編集

デフォルトのネットワーク、サーバおよびアプリケーション インシデント レスポンスを編集し、1 つ以上の応答アクションを追加し、かつ必要に応じ追加のインシデント レスポンスを作成します。 デフォルトでは、管理コンソール はネットワークまたはサーバのインシデントに応答して通知や調査を開始しません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. インシデント レスポンス リストを参照し、 をクリックし、ネットワーク、サーバまたはアプリケーションのインシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。

   ［インシデント レスポンス アクション］が表示されます。
5. をクリックして、アクションを編集します。

   ［アクションのプロパティ］が表示されます。
6. 応答アクション設定を指定して、［OK］をクリックします。 詳細については、［ヘルプ］をクリックしてください。

詳細:

監視デバイス インシデントの管理 (P. 305)

応答アクションの削除

管理コンソール で、特定の応答アクションを起動しないようにする場合は、そのネットワーク、サーバまたはアプリケーションのインシデント レスポンスからアクションを削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. インシデント レスポンス リストを参照し、 をクリックし、ネットワーク、サーバまたはアプリケーションのインシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。

   ［インシデント レスポンス アクション］が表示されます。
5. をクリックして、アクションを削除します。
6. プロンプトで［削除を続行］をクリックし応答アクションを削除します。

インシデント レスポンスの割り当て

管理コンソール がネットワークまたはサーバのインシデントに応答できるようにするには、少なくとも 1 つの応答アクションを持つインシデント レスポンスをアプリケーション、サーバまたはネットワーク タイプに割り当てます。

デフォルトのインシデント レスポンスには応答アクションは含まれませんが、それらを追加することはできます。

インシデント レスポンスを割り当てる対象	アクションを起動する場所
アプリケーション	サーバまたはネットワーク上のマイナー（黄色）またはメジャー（オレンジ）なパフォーマンス低下を伴うアプリケーション。

インシデント レスポンスを割り当てる対象	アクションを起動する場所
サーバ	マイナー（黄色）またはメジャー（オレンジ）なパフォーマンス低下を伴うサーバ。
ネットワーク タイプ	マイナー（黄色）またはメジャー（オレンジ）なパフォーマンス低下を伴うネットワーク。 インシデント レスポンスをネットワーク タイプに割り当てると、インシデント レスポンスが対応するネットワーク タイプを持つすべてのネットワークに割り当てられることに注意してください。

詳細情報:

ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)
応答アクションの編集 (P. 211)

アプリケーションへのインシデント レスポンスの割り当て

インシデント レスポンスをアプリケーションに割り当てて、管理コンソール でアプリケーションを調査し、かつアプリケーションに影響を及ぼすネットワークまたはサーバのインシデントについてユーザのチームに通知できるようにします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールし、必要なアプリケーションを選択して、［編集］をクリックします。

   ［アプリケーションのプロパティ］が表示されます。
4. ［インシデント レスポンス］をクリックし、必要なインシデント レスポンスを指定して［OK］をクリックします。

サーバへのインシデント レスポンスの割り当て

インシデント レスポンスをサーバに割り当てて、管理コンソール でサーバを調査し、かつ対応するサーバ インシデントについてユーザのチームに通知できるようにします。 管理コンソール は、デフォルトのインシデント レスポンスをすべてのサーバに割り当てます。しかし、CA Application Delivery Analysis はパッシブな監視ソリューションなので、デフォルトではアクションを起こしません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールし、 をクリックしてサーバを編集します。

   ［サーバのプロパティ］が表示されます。

   （オプション）同じインシデント レスポンスを複数のサーバに割り当てるには、適切なサーバを選択し、 をクリックして選択したアプリケーションをすべて編集します。
4. ［サーバのプロパティ］で、［インシデント レスポンス］をクリックして必要なサーバ インシデント レスポンスを割り当て、［OK］をクリックします。

ネットワーク タイプへのインシデント レスポンスの割り当て

インシデント レスポンスをネットワーク タイプに割り当て、管理コンソール がネットワークを調査し、かつ対応するネットワーク インシデントについてユーザのチームに通知することを有効にします。

インシデント レスポンスをネットワーク タイプに割り当てると、同じインシデント レスポンスが対応するネットワーク タイプを持つすべてのネットワークに適用されることに注意してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク タイプ］をクリックします。

   ［ネットワーク タイプ］が表示されます。
3. をクリックし、ネットワーク タイプを編集します。

   ［ネットワーク タイプのプロパティ］が表示されます。
4. ［インシデント レスポンス］をクリックし、必要なインシデント レスポンスを指定して［OK］をクリックします。

詳細:

クライアント ネットワークへのネットワーク タイプの割り当て (P. 66)

インシデント レスポンスのトラブルシューティング

管理コンソール がユーザの期待する応答アクションを起動しない場合は、以下について確認します。

- 適切なインシデント レスポンスがアプリケーション、サーバまたはネットワーク タイプに割り当てられているか。 クライアント ネットワークについては、適切なネットワーク タイプがクライアント ネットワークに割り当てられていることを確認します。
- インシデント レスポンスに割り当てられる応答アクションが正しく設定されているか。一般的には、管理コンソール によって作成されたネットワークまたはサーバ インシデントがインシデント レスポンスの最小の重大度および期間の基準を上回ることを確認します。 詳細については、応答アクションのプロパティを確認して、［ヘルプ］を参照してください。

Web サービス メソッドを使用したインシデントの管理

Web サービスを使用して、SNMP トラップ アクションをインシデント レスポンスに追加するときに、送信されるデータを超えるインシデント データについてクエリを行います。 インシデント レスポンスに［ステータスの更新の送信］オプションを使用します。

オブジェクト識別子仕様

- Incident Id .1.3.6.1.4.1.4498.2.20.1.1.1
- Server Name .1.3.6.1.4.1.4498.2.20.1.2.1
- Server IP .1.3.6.1.4.1.4498.2.20.1.3.1
- Application Name .1.3.6.1.4.1.4498.2.20.1.4.1
- Network Name .1.3.6.1.4.1.4498.2.20.1.5.1
- Metric Name .1.3.6.1.4.1.4498.2.20.1.6.1
- Incident Time .1.3.6.1.4.1.4498.2.20.1.7.1
- Severity .1.3.6.1.4.1.4498.2.20.1.8.1
- Impact % .1.3.6.1.4.1.4498.2.20.1.9.1
- Duration .1.3.6.1.4.1.4498.2.20.1.10.1
- Incident URL .1.3.6.1.4.1.4498.2.20.1.11.1
- Response Type .1.3.6.1.4.1.4498.2.20.1.12.1 Server | Network | Application
- Incident State Type .1.3.6.1.4.1.4498.2.20.1.13.1 Open | Update | Close
- Web Service IP .1.3.6.1.4.1.4498.2.20.1.14.1

サーバ名と IP

- すべてのサーバ インシデントの場合、サーバ名およびサーバ IP フィールドには、関連するサーバの特定の名前および IP アドレスが含まれます。
- 関連するサーバが 1 つのみのネットワーク インシデントの場合、これらのフィールドには、関連するサーバの特定の名前および IP アドレスが含まれます。
- 複数の関連するサーバがあるネットワーク インシデントの場合、これらのフィールドには、重大度状態のサーバの数を n またはそれ以上などと示すために［n+ サーバ］または［n+ アドレス］が含まれます。
- データ非アクティブ状態（白いステータス）のためにクローズしているネットワーク インシデントについて、これらのフィールドは［なし］です。

アプリケーション名

- 関連アプリケーションが 1 つのみのサーバまたはネットワークのインシデントについて、このフィールドには、そのアプリケーションの特定の名前が含まれます。
- サーバまたはネットワークのインシデントに対するアプリケーション インシデント レスポンスについて、このフィールドには、そのアプリケーションの特定の名前が含まれます。
- 複数の関連アプリケーションがあるサーバまたはネットワークのインシデントについて、n が重大度状態のアプリケーションの数である場合、このフィールドには［n アプリケーション］が含まれます。
- データ非アクティブ状態（白いステータス）のためにクローズしているサーバまたはネットワークのインシデントについては、このフィールドは［なし］です。
- サーバの利用不可によって引き起こされたサーバ インシデントについて、このフィールドは［すべて］です。

ネットワーク名

- すべてのネットワーク インシデントについて、このフィールドには、関連するネットワークの特定の名前およびサブネットが含まれます。
- 関連するネットワークが 1 つのみのサーバ インシデントについて、このフィールドには、関連するネットワークの特定の名前およびサブネットが含まれます。
- 複数の関連するネットワークがあるサーバ インシデントについて、このフィールドには、重大度状態のネットワークの数を n またはそれ以上などと示すために［n+ ネットワーク］が含まれます。
- データ非アクティブ状態（白いステータス）のためにクローズしているサーバ インシデントについては、このフィールドは［なし］です。

メトリック名

- しきい値を越えるメトリックによって引き起こされたインシデントについて、このフィールドは省略形がカンマで区切られた羅列です。
  - NRTT ネットワーク ラウンドトリップ時間
  - RTNS 再送信遅延
  - NCT ネットワーク接続時間
  - ERTT 実効ラウンドトリップ時間
  - SRT サーバ レスポンス時間
  - SCT サーバ接続時間
  - RS 拒否されたセッション（割合）
  - US 無応答セッション（割合）
- 利用不可によって引き起こされたインシデントについて、このフィールドは［可用性］です。
- データ非アクティブ状態（白いステータス）のためにクローズしているインシデントについて、このフィールドはデータが不足しています。

Web サービス仕様

いずれかの Web サービス インターフェース メソッドを使用してデータを取得します。 これらの Web サービスは XML 出力をサポートします。

ここから Web サービスにアクセスします。
`http://WebServiceIP/SuperAgentWebService/PublishedService.asmx`

入力

FetchServersByIncident または FetchServersByIncidentSeverityDuration を使用して、サーバ リストを取得します。

入力

- インシデント ID
- 最小の重大度（オプション）
- 最小の期間（オプション）

出力

- server_id、32 ビットの無署名識別子
- server_desc、最大 50 文字の文字列名
- アドレス、32 ビットの無署名 IP アドレス
- なし、データが収集されなかったインシデント中の時間の浮動小数点パーセンテージ
- 未評価、しきい値が存在しなかったインシデント中の時間の浮動小数点パーセンテージ（まだ計算されていない、またはオフにした）
- 正常、通常（しきい値より下）のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 劣化、劣化した（過度ではない）データが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 過剰、過度のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 使用不可、サーバまたはアプリケーションが使用不可だったインシデント中の時間の浮動小数点パーセンテージ（サーバ インシデントのみ）

入力

アプリケーション リスト FetchApplicationsByIncident または FetchApplicationsByIncidentSeverityDuration を取得します。

入力

- インシデント ID
- 最小の重大度（オプション）
- 最小の期間（オプション）

出力

- app_id、32 ビットの無署名識別子
- applications_desc、最大 50 文字の文字列名
- port_beg、範囲内の 16 ビット無署名の最初のポート
- port_end、範囲内の 16 ビット無署名の最後のポート
- なし、データが収集されなかったインシデント中の時間の浮動小数点パーセンテージ
- 未評価、しきい値が存在しなかったインシデント中の時間の浮動小数点パーセンテージ（まだ計算されていない、またはオフにした）
- 正常、通常（しきい値より下）のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 劣化、劣化した（過度ではない）データが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 過剰、過度のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 使用不可、サーバまたはアプリケーションが使用不可だったインシデント中の時間の浮動小数点パーセンテージ（サーバ インシデントのみ）

入力

ネットワーク リスト FetchNetworksByIncident または FetchNetworksByIncidentSeverityDuration を取得します。

入力

- インシデント ID
- 最小の重大度（オプション）
- 最小の期間（オプション）

出力

- client_id、ネットワーク定義用の 32 ビットの無署名識別子
- client_address、ネットワーク サブネットの 32 ビットの無署名アドレス構成要素
- client_mask、ネットワーク サブネットの 32 ビットの無署名マスク コンポーネント（展開された CIDR）
- client_desc、最大 50 文字の文字列名
- サブネット、x.x.x.x/m にフォーマットされたサブネット仕様
- なし、データが収集されなかったインシデント中の時間の浮動小数点パーセンテージ
- 未評価、しきい値が存在しなかったインシデント中の時間の浮動小数点パーセンテージ（まだ計算されていない、またはオフにした）
- 正常、通常（しきい値より下）のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 劣化、劣化した（過度ではない）データが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 過剰、過度のデータが収集されたインシデント中の時間の浮動小数点パーセンテージ
- 使用不可、サーバまたはアプリケーションが使用不可だったインシデント中の時間の浮動小数点パーセンテージ（サーバ インシデントのみ）

  注: インシデント Web サービスからの重大度パーセンテージは、［操作］および［インシデント］ビューのエクスポートに一致しています。

ステータスの更新の送信仕様

アプリケーション、サーバ、およびネットワークのインシデント レスポンス トラップ オプションは重大度の増分更新を送信します。 重大度のすべての更新は期間にかかわらず送信されます。 このオプションをオフにすると、オープンおよびクローズのインシデント トラップのみが十分な重大度/期間に送信されます。

アプリケーション インシデント レスポンス トラップの仕様

アプリケーション インシデント レスポンス トラップは、アプリケーションに固有のネットワークおよびサーバのインシデント レスポンスとしてのみ送信されます。通常、ネットワーク インシデントには集約アプリケーションおよびサーバのデータが含まれます。 同様に、サーバ インシデントには集約アプリケーションおよびネットワークのデータが含まれます。ネットワークおよびサーバのインシデントに対するアプリケーション インシデント レスポンスでは、しきい値を超えるネットワーク/アプリケーションおよびサーバ/アプリケーションの組み合わせごとに警報が発せられ、集約サーバおよびネットワークのデータがそれぞれ含まれます。

SNMP トラップの説明

以下の表では、トラップの行をそれぞれの説明とともにリスト表示しています。

トラップ	説明
1.3.6.1.4.1.4498.2.20.1.1.1 netQoSIncident7Number **17841**	インシデント識別子。
1.3.6.1.4.1.4498.2.20.1.2.1 netQoSIncident7Server **dc1.netqos.local**	サーバ名が含まれます。
1.3.6.1.4.1.4498.2.20.1.3.1 netQoSIncident7ServerAddress **192.168.0.6**	サーバのアドレスが含まれます。
1.3.6.1.4.1.4498.2.20.1.4.1 netQoSIncident7Application **Lightweight Directory Access Protocol**	アプリケーションが含まれます。
1.3.6.1.4.1.4498.2.20.1.5.1 netQoSIncident7ClientRegion **SuperAgent LAN - 192.168.245.0/24**	ネットワークが含まれます。
1.3.6.1.4.1.4498.2.20.1.6.1 netQoSIncident7Regards **NRTT,ERTT**	メトリックが含まれます。

トラップ	説明
1.3.6.1.4.1.4498.2.20.1.7.1 netQoSIncident7Time **02/20/2007 20:40 GMT-4**	イベントの終了スタンプ。
1.3.6.1.4.1.4498.2.20.1.8.1 netQoSIncident7Severity **Excessive**	違反されたしきい値および重大度の分類。
1.3.6.1.4.1.4498.2.20.1.9.1 netQoSIncident7Impact **91.5%**	影響する観測の加重割合。 影響度値は前の netQoSIncident7Duration 分間の netQoSIncident7Severity の影響度です。 ネットワークの場合は、app/メトリック ペアごとのサーバ観測のピーク パーセントで表されます。 サーバの場合は、app/メトリック ペアごとのネットワーク観測のピーク パーセントで表されます。
1.3.6.1.4.1.4498.2.20.1.10.1 netQoSIncident7Duration **10.0 分**	イベントの期間。
1.3.6.1.4.1.4498.2.20.1.11.1 netQoSIncident7URL **http://192.168.100.131/SuperAgent/Investigator/Incidents/IncidentsViewFocus.aspx?Nav=13,0,0&Stack=T|M|N|A|S&I=1017841**	インシデントの UI への URL リンク。
1.3.6.1.4.1.4498.2.20.1.12.1 netQoSIncident7ResponseType **ネットワーク**	このトラップを生成したインシデント レスポンスのタイプ。
1.3.6.1.4.1.4498.2.20.1.13.1 netQoSIncident7State **オープン**	トラップのオープン、更新またはクローズ状態。
1.3.6.1.4.1.4498.2.20.1.14.1 netQoSIncident7WebServiceIP **192.168.100.131**	より詳細な Web サービスを検索できるコンソールの IP アドレス。

第 8 章: アプリケーション パフォーマンス OLA 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。

パフォーマンス OLA の仕組み (P. 226)
履歴データからの運用レベルの確立 (P. 231)
ネットワークのグループのアプリケーション パフォーマンス OLA の作成 (P. 233)
アプリケーション パフォーマンス OLA の編集 (P. 235)
アプリケーション パフォーマンス OLA の削除 (P. 237)

パフォーマンス OLA の仕組み

パフォーマンス運用レベル アグリーメント（パフォーマンス OLA）は、リモートサイトのアプリケーション パフォーマンス目標の適合を評価することができます。 デフォルトでは、管理コンソールは、アプリケーション パフォーマンスの運用レベルを定義していません。

パフォーマンス OLA は、時間の経過に伴いパフォーマンスが最も悪い IPv4 ベースのトランザクションの動作を追跡することによってレポートを強化します。 このトラッキングは、パフォーマンスの低下がいつ、どこで最も深刻になるかを示します。 このトラッキングにより、ユーザはパフォーマンスが 管理コンソール でレポートされた中間データ ポイントからどのように変化しているかを理解できます。

デフォルトでは、管理コンソール はパフォーマンス OLA をレポートしません。 システム定義アプリケーションではなく、ユーザ定義アプリケーション用に OLA を作成できます。

管理コンソール が OLA データを収集し、OLA コンプライアンスを測定する方法により、すべての場所にわたってではなくリモート ロケーションごとにコンプライアンスを測定するよう OLA を設定することをお勧めします。 各リモート ロケーションで OLA を確立するには、ネットワーク タイプを使用します。

（オプション）アプリケーション用のパフォーマンス OLA を設定し、OLA を 管理コンソール によって監視されたすべてのサーバに適用するには、ユーザ定義のアプリケーションを作成し、ドメインに割り当てます。 管理コンソール は、自動的にアプリケーション サーバ割り当てをサーバ サブネットの変更に合わせて最新に維持します。

詳細:

ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)

パフォーマンス OLA レポートの仕組み

パフォーマンス OLA は、1 時間ごとに、指定されたしきい値より速い IPv4 ベースのトランザクションの割合を計算することにより、ユーザ定義のアプリケーションがどの程度効果的に実行されているかを示します。 パフォーマンス OLA の一例として、サーバ レスポンス時間の 90 パーセントが 20 ミリ秒未満である必要があるとします。 パフォーマンス OLA の結果はレポート内に表示され、1 時間ごとにアプリケーションが運用レベル契約に適合しているかどうかを示します。

管理コンソール は、指定するしきい値に基づいて、1 時間ごとの運用レベルに対する適合度を測定します。 しきい値は、93.999 のように小数第 3 位まで指定できます。OLA コンプライアンス違反をレポートするのに 1 時間かかる場合があります。

管理コンソール は 5 分データと同じ方法で OLA データを収集しません。パフォーマンス OLA の場合、監視デバイス は以下を行います。

- すべてのトランザクションを比較し、それが OLA のしきい値に適合しているかどうかを確認します。
- 1 時間ごとに適合するトランザクションと不適合のトランザクションの数を記録します。

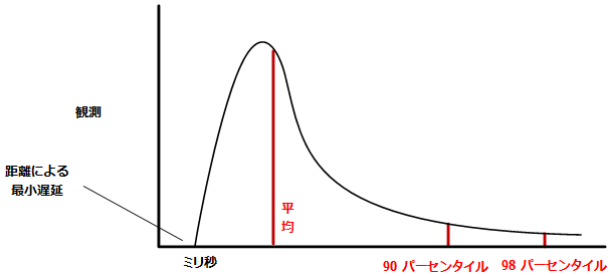
たとえば、州間ハイウェイを走る自動車の平均速度を 5 分ごとに記録する代わりに、管理コンソール は、車が 40mph を超えて移動しているかを記録し、1 時間ごとに成功数と失敗数をレポートします。

一方、管理コンソール は、しきい値を使用して 5 分間隔で特定のメトリックの平均レスポンス時間に基づいてアプリケーションのパフォーマンスを監視します。

パフォーマンス OLA しきい値の仕組み

パフォーマンス OLA は最も速度の遅いトランザクションについての洞察をさらに示すので、パフォーマンスの一般的なタイム スライスがどのようなものかを理解することが重要です。 ほとんどの人は標準分布または釣鐘曲線に精通しており、パーセンタイルの観点では、通常の場合これらのことを想起します。 しかし、TCP トランザクションは正規分布に従いません。 その代わりに、サーバ レスポンス時間（SRT）でのネットワーク ラウンドトリップ時間の間隔および I/O による最小の遅延が考慮されます。 できるだけ多くのトランザクションがこの最小値に近くなることが理想です。できるだけこの最小に近いトランザクションが多くあることが理想です。

以下の例では、ネットワーク ラウンドトリップ時間の指定された期間に管理コンソール で検出される理想的なバージョンを示します。 パフォーマンスが低下すると、曲線全体が右に移動するか、または曲線のテール部分が伸びる場合があります。 この状況は OLA が有用となる一例です。



OLA を使用して、ユーザは第 90 および第 98 パーセンタイル用のしきい値を指定できます。 ユーザはどのパーセンタイルでも指定できることに注意してください。 レポートには、これらの値のどのパーセンタイルが実際にしきい値に到達したかが示されます。 しきい値を調節することで、後部の動作を監視し、目標指向の方式で OLA を設定できます。

運用レベル メトリックの仕組み

パフォーマンス OLA は、以下のキー メトリックを使用して運用レベル コンプライアンスを測定します。OLA 内の一部、またはすべての運用レベルを監視するかどうかを選択できます。

運用レベル メトリック	詳細
ネットワーク ラウンドトリップ時間	■ 特に WAN リンクに対して、ネットワーク タイプ別に設定します。 ■ 同様の遅延があるネットワークが一まとめになっていることを確認します。 ■ 特に WAN リンクに対して、ビジネス上重要なアプリケーションを監視します。 ■ より多くの観測を行って統計的有意性を持たせるために、各サイトに対し最大量（または最も定常的な量）のトラフィックを示すアプリケーションを選択します。
サーバ レスポンス時間	■ ネットワーク タイプ別に分離しません。 ■ サーバは、どのネットワークから来たかを問わずリクエストを独立して処理する必要があります。 ■ 多層アプリケーションで最も影響力のある層を監視し、フロントエンド サーバのレスポンス時間にはバックエンド サーバのリクエストが含まれることに留意します。 ■ ビジネス上重要なアプリケーション用のサーバを監視します。
合計トランザクション時間	■ サーバ レスポンス時間、ネットワーク ラウンドトリップ時間およびデータ転送時間に依存するので、エンド ユーザ全体の経験の最適なインジケータです。 ■ ネットワーク ラウンドトリップ時間によって異なるので、ネットワーク タイプごとに設定します。 ■ ビジネス上重要なアプリケーションを監視します。

パフォーマンス OLA のヒント

より多くの観測を行って統計的有意性を持たせるために、各サイトに対し最大量（または最も定常的な量）のトラフィックを示すユーザ定義アプリケーション用にアプリケーション パフォーマンス OLA を作成することを推奨します。 システム定義のアプリケーションには運用レベルを設定できません。

パフォーマンス OLA を設定するときは以下を行います。

- ネットワーク メトリックからデータ センター メトリックを分離します。すべてのメトリックがすべてのネットワークで重要だとは限りません。たとえば、バックエンド アプリケーションで、ネットワーク ラウンドトリップ時間のトラッキングを参照しない場合があります。
- OLA しきい値を決定するときは、一時的な上昇または低下を除外するために、長いタイムラインを使用することが適切です。 OLA から特定のメトリックを除外することもできます。
- 2 つまでのしきい値を定義し、たとえば内部および外部の運用レベルを設定するために、運用レベルに対するアプリケーション コンプライアンスを測定します。一般に、90 パーセント以上で運用レベルを定義し、管理コンソール がパフォーマンスの可変性に対してさらなる洞察を提供できるようにします。 あるいは、OLA メトリック用にパフォーマンスしきい値レベルを設定しないことも可能です。

各しきい値レベルの正しい値を使用して、管理コンソール は、5 分平均で各リモート ロケーションのユーザが経験している最もパフォーマンスが悪い（最も高いパーセンタイル）トランザクションに関する履歴トレンド データを取得します。

詳細:

アプリケーション パフォーマンス OLA の編集 (P. 235)

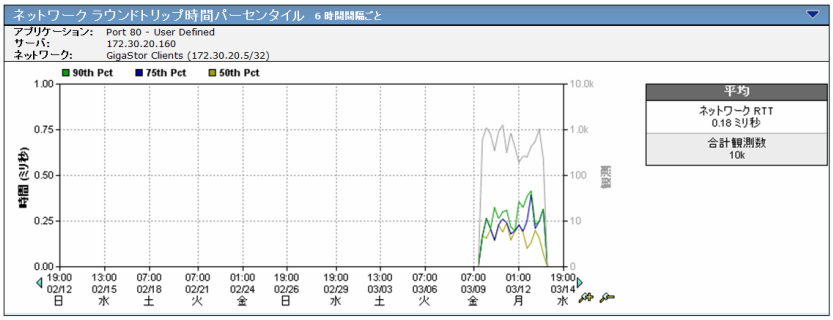
履歴データからの運用レベルの確立

履歴レポート データを、新しい運用レベル 契約を設定するための出発点として使用します。 管理コンソール がアプリケーションの「通常」動作を決定するためのデータを十分に収集できるまで 1 か月間待機することをお勧めします。

次の手順に従ってください:

1. ［エンジニアリング］ページをクリックします。
2. ［表示項目］メニュー上の［設定］をクリックします。

   ［設定］ダイアログ ボックスが表示されます。
3. アプリケーションを選択します。
4. サーバを選択します。
5. ネットワークを選択します。
6. 月単位のレポートを表示するようタイムフレームを設定し、［OK］をクリックします。
7. ネットワーク ラウンドトリップ時間レポートなど、コンポーネント レポートで必要な運用レベル メトリックを検索します。以下の例では、ロサンジェルス ネットワークおよび Exchange アプリケーションをホストするすべてのサーバのレスポンス時間データが含まれます。



8. ［統計］で、90 番目および最大の値を書きとめます。 以下の例では、90 パーセンタイルは 12.4 ミリ秒で、最大値は 41.7 ミリ秒です。

統計	
最小	6.33 ミリ秒
最大	1.03 秒
平均	85.7 ミリ秒
50 百分位	14.6 ミリ秒
75 百分位	47.5 ミリ秒
90 百分位	329 ミリ秒
観測	139

注: 月単位のタイム フレームでレポートする場合、管理コンソール はレポート統計を 6 時間刻みで集約します。 詳細については、「*ユーザ ガイド*」を参照してください。

9. これらの手順を繰り返し、ネットワーク ラウンドトリップ時間およびサーバ レスポンス時間を含む、運用レベル メトリックの各々に対する 90 および最大のパーセンタイルを収集します。トランザクション時間の場合、ネットワーク ラウンドトリップ時間、サーバ レスポンス時間、再送信遅延、データ転送時間の 90 および最大のパーセンタイルを合計および平均します。
10. 初期の運用レベルを決定するには、これまでの月ごとの 90 および 98 パーセンタイル値を 2 倍にします。 上記の統計例に基づいて、90 および 98 のパーセンタイルを 2 倍にすると、25 ミリ秒の 90 パーセンタイルおよび 81 ミリ秒の 98 パーセンタイルと同等になります。
11. それが最初のレポート期間で実行するときの OLA を監視します。それが最初に OLA に適合しない場合も中止しないでください。調整する前に完全にレポート期間が完了するのを待ちます。 管理コンソール は 1 時間ごとに運用レベル コンプライアンスを測定するので、OLA がコンプライアンス違反を表示するまでに最大 1 時間のラグがある場合があります。
12. レポート期間が終了した後にしきい値を調節し、達成可能なしきい値を設定します。 その結果によってしきい値のより洗練された評価を行うことができます。

詳細:

ネットワークのグループのアプリケーション パフォーマンス OLA の作成 (P. 233)

ネットワークのグループのアプリケーション パフォーマンス OLA の作成

パフォーマンス OLA を作成し、同様の遅延特性があるクライアント ネットワークのグループにわたるユーザ定義のアプリケーションに対するサービスの予想水準を定義します。

管理コンソールは、各ユーザ定義のアプリケーションに対するデフォルト OLA を作成し、割り当て済みのネットワーク タイプがないすべてのネットワークを通じてパフォーマンスを測定します。 一般に、これは、リモート ロケーション間のネットワーク遅延に差があるために、ネットワーク ラウンドトリップ時間および合計トランザクション時間の監視には推奨されません。

デフォルト OLA 内のしきい値を更新すると、その変更は、デフォルトの OLA 値を使用するように設定される、そのアプリケーション用のあらゆる新しい OLA に動的に適用されます。 たとえば、POP3 アプリケーションのデフォルト OLA で、1 時間間隔におけるネットワーク ラウンドトリップ時間の観測の少なくとも 90% が最低でも 5ms である必要がある場合、オースティン ネットワーク タイプで POP3 アプリケーション用の OLA を作成すると、デフォルトの観測率は 90% で、ネットワーク ラウンドトリップ時間のしきい値は 5 ミリ秒になります。 POP3 のネットワーク ラウンドトリップ時間のデフォルト OLA のしきい値を変更すると、管理コンソールは、POP3 オースティンの OLA のネットワーク ラウンドトリップ時間のしきい値を動的に更新し、新しいデフォルト値が使用されるようにします。

OLA を作成するとき、しきい値をカスタマイズして動的なデフォルト値を無効にできます。しきい値をカスタマイズせずに、OLA メトリックのしきい値または最小観測数を変更すると、その変更がデフォルト OLA に適用されます。

OLA を作成する前に、1 か月間アプリケーションを監視してその正常なパフォーマンスを測定することを推奨します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンス OLA］をクリックします。

3. ［パフォーマンス OLA リスト］内の OLA のリストを参照します。リストにアプリケーションがない場合、ユーザ定義のアプリケーションは存在しません。

   デフォルトでは、管理コンソール は、割り当て済みネットワーク タイプのないネットワークに適用される、各ユーザ定義のアプリケーション用のデフォルト OLA を作成します。

4. ［ネットワーク タイプによるカスタムの追加］をクリックし、クライアント ネットワークのグループ用のアプリケーション OLA を作成します。

   ［ネットワーク タイプ別のしきい値のカスタマイズ］が表示されます。

5. 適切なリモート ロケーションに相当するアプリケーションおよびネットワーク タイプを選択し、［OK］をクリックします。

   ［OLA しきい値の編集］が表示されます。

6. 各 OLA メトリックのしきい値設定を編集して、［OK］をクリックします。

   OLA しきい値の編集の詳細については、［ヘルプ］をクリックしてください。

7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

8. 完全なレポート サイクルを最大 1 時間まで待機し、どの程度のしきい値の変更が 管理コンソール によって観測された実際のレスポンス時間に見合うかを確認します。

   a. ［管理］ページの［表示項目］メニュー内の［パフォーマンス詳細 OLA］をクリックします。

   b. 必要に応じ、アプリケーションがリモートサイト用の運用レベル契約に適合するように、運用レベルのしきい値割合の値を調節するか、またはしきい値レベルの値を増やします。

詳細:

アプリケーション パフォーマンス OLA の編集 (P. 235)
履歴データからの運用レベルの確立 (P. 231)

アプリケーション パフォーマンス OLA の編集

パフォーマンス OLA を編集し、ネットワーク タイプによって識別されるネットワークのグループのユーザ定義のアプリケーションに対するサービスの予想水準を変更します。

管理コンソール は、各ユーザ定義のアプリケーションに対するデフォルト OLA を作成し、割り当て済みのネットワーク タイプがないすべてのネットワークを通じてパフォーマンスを測定します。 一般に、これは、リモート ロケーション間のネットワーク遅延に差があるために、ネットワーク ラウンドトリップ時間およびトランザクション合計時間の監視には推奨されません。

デフォルト OLA 内のしきい値を更新すると、その変更は、デフォルトの OLA 値を使用するように設定される、そのアプリケーション用のあらゆる新しい OLA に動的に適用されます。 たとえば、POP3 アプリケーションのデフォルト OLA で、1 時間間隔におけるネットワーク ラウンドトリップ時間の観測の少なくとも 90% が最低でも 5ms である必要がある場合、オースティン ネットワーク タイプで POP3 アプリケーション用の OLA を作成すると、デフォルトの観測率は 90% で、ネットワーク ラウンドトリップ時間のしきい値は 5 ミリ秒になります。 POP3 のネットワーク ラウンドトリップ時間のデフォルト OLA のしきい値を変更すると、管理コンソールは、POP3 オースティンの OLA のネットワーク ラウンドトリップ時間のしきい値を動的に更新し、新しいデフォルト値が使用されるようにします。

しきい値をカスタマイズせずに、OLA メトリックのしきい値または最小観測数を変更すると、その変更がデフォルト OLA に適用されます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールし、必要なアプリケーションを選択して、［OLA］をクリックします。

   ［アプリケーション OLA の編集］が表示され、選択されたアプリケーションの OLA がネットワーク タイプ別にリスト表示されます。
4. をクリックし、クライアント ネットワークのグループのパフォーマンス OLA に相当するネットワーク タイプを編集します。

（オプション）複数のリモート ロケーションのパフォーマンス OLA を編集するには、適切なネットワーク タイプを選択し、  をクリックし選択された OLA を編集します。

［OLA しきい値の編集］が表示されます。

5. 各 OLA メトリックのしきい値設定を編集して、［OK］をクリックします。

   サーバのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

7. 完全なレポート サイクルを最大 1 時間まで待機し、どの程度のしきい値の変更が 管理コンソール によって観測された実際のレスポンス時間に見合うかを確認します。

   a. ［管理］ページの［表示項目］メニュー内の［パフォーマンス詳細 OLA］をクリックします。

   b. （オプション）運用レベルしきい値の値を調整します。たとえば、ネットワーク ラウンドトリップ時間のしきい値が「90% パーセンタイルで 11 ミリ秒未満」であるが、観測値の 67.744 パーセントのみがこのしきい値レベルを満たす場合は、しきい値レベルのパーセンタイルまたはしきい値レベルを調整し、アプリケーションがリモート サイトの OLA を満たすようにします。

詳細:

ネットワークのグループのアプリケーション パフォーマンス OLA の作成 (P. 233)

アプリケーション パフォーマンス OLA の削除

リモートサイトで 1 つ以上のアプリケーションに対するサービスの予期される水準を削除するには、パフォーマンス OLA を削除します。 リモート ロケーションでクライアント ネットワーク用のアプリケーション パフォーマンス OLA を削除するには、クライアント サブネットワークが割り当てられるネットワーク タイプを識別します。

あるいは、アプリケーション パフォーマンス OLA から特定のパフォーマンス メトリックを削除できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールし、必要なアプリケーションを選択して、［OLA］をクリックします。

   ［アプリケーション OLA の編集］が表示され、選択されたアプリケーションの OLA がネットワーク タイプ別にリスト表示されます。
4. をクリックし OLA を削除します。

   プロンプトで［削除を続行］をクリックし指定された OLA を削除します。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)
アプリケーション パフォーマンス OLA の編集 (P. 235)

第 9 章: アプリケーション可用性の管理

このセクションには、以下のトピックが含まれています。

可用性監視の仕組み (P. 239)
アプリケーション可用性 OLA の仕組み (P. 247)

可用性監視の仕組み

CA Application Delivery Analysis は、パッシブ データ観察を通じてユーザ定義アプリケーションの可用性を追跡します。 アプリケーションの可用性を判断するため、監視デバイスは、アプリケーションに割り当てられている各サーバ上の IPv4 ベースのクライアント アクティビティを観測します。

可用性の監視には、以下が必要です。

- CA Standard Monitor または Virtual Systems Monitor
- CA Multi-Port Monitor

監視デバイスが 5 分間隔でサーバ上のアプリケーション ポートへの不十分なユーザ トラフィックを観測した場合、監視デバイスはアプリケーションにアクティブなリクエストを作成することにより可用性を検証します。

可用性基準	説明
成功した TCP トランザクションが 10 未満	5 分の間に、アプリケーション ポート上で成功した TCP トランザクションが 10 未満である場合、監視デバイスは積極的にアプリケーションの可用性を確認します。
拒否されたセッションが 10% を超える	アプリケーション ポートが 5 分の間に 10% （以上）の接続リクエストを拒否した場合、監視デバイスは積極的にアプリケーションの可用性を確認します。

監視デバイスは、サーバ上のアプリケーション ポートに TCP SYN パケットを送信することにより、積極的にアプリケーションの可用性を確認します。ポート範囲によって定義されたアプリケーションについては、範囲内の最初の 8 つのポートそれぞれで接続が試行されます。

監視デバイスがアプリケーション サーバから SYN-ACK パケット レスポンスを受信しない場合、以下が発生します。

- アプリケーションは「使用不可」と評価されます。
- 監視デバイスは、サーバに ping リクエストを送信することにより、アプリケーションをホストするサーバの可用性を積極的に確認します。アプリケーションが「使用不可」と評価されない限り、サーバの可用性は確認されません。 サーバが、
  - ping に応答する場合、サーバは「使用可能」と評価されます。
  - ping に応答しない場合、サーバは「使用不可」と評価されます。

負荷分散されたアプリケーションについては、割り当て済みの各サーバ上のアプリケーションの可用性を確認する代わりに、割り当て済みサーバの最小数に基づいてアプリケーションの可用性を評価するよう選択できます。 たとえば、ロード バランサが最低 2 つから最大 5 つまでのサーバの間でアプリケーション トラフィックを配布する場合、アプリケーションが少なくとも 2 つのサーバ上でアクティブであることが正常です。アプリケーションを「使用可能」と評価するには、5 つのサーバのうち少なくとも 2 つで許容可能なアプリケーション アクティビティが発生する必要があります。 負荷分散されたアプリケーションが「使用不可」と評価された場合、どのサーバが使用可能であるかを判断するため、割り当てられた各サーバの可用性 (P. 245)が確認されます。

詳細:

サーバの可用性の確認 (P. 245)

システム定義のアプリケーションはなぜ除外されるか

可用性インシデントを誤って開かないようにするために、管理コンソールは、システム定義のアプリケーションの可用性を自動的に監視しません。たとえば、管理コンソール がはじめてサーバのポート 80 上の TCP トラフィックを観測する時、それは自動的に HTTP アプリケーションのインスタンスを作成します。 しかし、そのアプリケーションの可用性監視を有効にすると、多くの誤った可用性インシデントが作成される場合があり、それは 管理コンソール がトラフィックが最初に確認されたサーバだけでなくドメイン上のすべてのサーバで実行される HTTP を確認する予定であるためです。

（オプション）アプリケーション用の可用性 OLA を設定し 管理コンソール によって監視されたサーバのすべてに OLA を適用するには、ユーザ定義のアプリケーションを作成しそれにドメインを割り当てます。 管理コンソール は、自動的にアプリケーション サーバ割り当てをサーバ サブネットの変更に合わせて最新に維持します。

アプリケーション可用性のサーバ インシデントの仕組み

管理コンソール は、「使用不可」ステータスのアプリケーションに応答してサーバ インシデントを自動的に開きます。 インシデント レスポンスを、

- アプリケーションをホストするサーバに割り当て、そのアプリケーションが「使用不可」である場合、以下のような割り当て済みインシデント レスポンスが起動されます。
  - 電子メール通知
  - SNMP トラップ通知
  - ping レスポンス時間調査
  - SNMP 経由のパフォーマンス調査
  - パケット キャプチャ調査
- アプリケーションに割り当て、そのアプリケーションが「使用不可」である場合、以下のような割り当て済みインシデント レスポンスが起動されます。
  - 電子メール通知
  - SNMP トラップ通知
  - パケット キャプチャ調査

  アプリケーション接続時間調査は、「使用不可」アプリケーションに応答して開始されないことに注意してください。これは、調査結果でアプリケーションのステータスに関する追加情報が発見されないためです。

アプリケーション可用性レポートの仕組み

管理コンソールは、［設定］で［すべてのサーバ メトリック］をクリックすると、アプリケーションの可用性をレポートします。 デフォルトでは、［設定］に［すべての相対メトリック］が表示されます。これは、アプリケーション可用性ステータスを表示しません。

この評価は、管理コンソール管理者がサーバを割り当てているユーザ定義アプリケーションにのみ適用されます。管理コンソール は以下をレポートします。

- アプリケーションが 5 分間隔でサーバ上で使用可能だったかどうか。
- アプリケーションが使用可能だった時間の割合。

負荷分散されたアプリケーションについては、アプリケーションの可用性は、アプリケーションが最小数のサーバ上で使用可能だった時間の割合として評価されます。

詳細:

サーバの可用性の確認 (P. 245)

可用性監視の有効化

管理コンソール はすべてのクライアント ネットワークにわたってアプリケーション可用性を測定します。 特定のネットワーク上のアプリケーションの可用性は監視できません。

重要: テナント データを分離するためにドメインを使用する場合、可用性監視を無効にすることにより、誤検出の可用性インシデントを回避してください。 ISP 環境では、監視デバイスがアプリケーション ポートの可用性を積極的に確認するためにアプリケーション サーバに接続できる可能性はあまりありません。

アプリケーション上で、およびオプションでアプリケーションをホストするサーバ上で可用性監視を有効にします。

アプリケーション可用性の監視

アプリケーション可用性を監視するには、アプリケーションのプロパティを編集し可用性監視を有効にします。 デフォルトでは、可用性監視は無効です。

どのアプリケーションの可用性を監視するかを決定する場合、以下を監視することをお勧めします。

- 割り当て済みサーバを持つユーザ定義のアプリケーション。 管理コンソールは、アプリケーションが以下の場合にアプリケーション可用性を監視しません。
  - 自動的に監視されている（システム定義）
  - ユーザ定義である（サーバ サブネットが割り当てられている）
  - ドメイン内のすべてのサーバに割り当てられている
- 優先アプリケーション。優先アプリケーションでないアプリケーション上で可用性 OLA を設定し、管理コンソール がアプリケーションをグルーミングするか、アプリケーション データをフィルタすると、管理コンソール は不必要にアプリケーションの可用性を確認します。管理コンソール は優先アプリケーションのグルーミングやフィルタリングを行いません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールして、必要なユーザ定義のアプリケーションを選択し、［編集］をクリックします。

   ［アプリケーションのプロパティ］が表示されます。

   ユーザ定義のアプリケーションをより簡単に見つけるには、［表示］メニューを使用してシステム定義のアプリケーションを非表示にします。
4. ［可用性監視］リストをクリックして［有効］を選択し、［OK］をクリックします。
5. ロード バランサがサーバ間でアプリケーションのトラフィックを配布する場合は、アプリケーションのサーバ割り当てを編集し使用可能にすべきサーバの数を指定します。

6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

サーバの可用性の確認 (P. 245)
優先アプリケーションの仕組み (P. 123)

サーバの可用性の確認

CA Application Delivery Analysis 監視デバイスは、サーバによってホストされたアプリケーションが使用不可であることを能動的に確認した後、サーバの可用性を確認します。サーバの可用性を確認することで、アプリケーション可用性の問題がアプリケーションまたはアプリケーションをホストするサーバに関連するかどうかを決定できます。

アプリケーションをホストするサーバの可用性を積極的に確認しないようにするには、割り当て済み各サーバ上で可用性監視を無効にします。デフォルトでは、サーバの可用性監視は有効です。

サーバの可用性を確認することに加えて、負荷分散されたアプリケーションの可用性を監視するには、使用可能になっている必要があるサーバの最小数を指定する必要があります。 たとえば、負荷分散されたアプリケーションで、ロード バランサはそのサーバのすべてにわたってアプリケーションの負荷を共有しない可能性があります。したがって、最小数のサーバがアプリケーションをホストしていることを確認することのみが必要です。

注: アプリケーションのステータスが「使用可能」である場合はサーバの可用性は確認されません。そのため、一部のサーバが実際には使用可能でなくても、負荷分散されたアプリケーションの割り当て済みサーバのすべてのステータスが「使用可能」である可能性があります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［アプリケーション］をクリックします。
3. ［アプリケーション リスト］までスクロールして、ユーザ定義のアプリケーションを選択し、［編集］をクリックします。

   ［アプリケーションのプロパティ］が表示されます。
4. ［割り当て］をクリックします。
5. （オプション）アプリケーションをホストするサーバがロード バランスのとれたファームの一部である場合は、以下の手順に従い使用可能である必要があるサーバの最小数を指定します。
   a. ［サーバはロード バランスのとれたファームでアプリケーションをサポートします。］を選択します。 このオプションが使用できない場合、［プロパティ］をクリックしてアプリケーションの可用性監視を有効にします。
   b. ［アプリケーションが使用可能であると判断されるために必要な最小限のサーバ。］に対する値を入力します。
6. ［OK］をクリックします。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

サーバの編集 (P. 93)

アプリケーション可用性 OLA の仕組み

可用性運用レベル契約（可用性 OLA）は、現在のアプリケーションとサーバの可用性、および可用性傾向を幅広い読者に提示できるレポートで数値化します。 サーバまたはアプリケーションが実行されていないかどうかを把握することから有用な情報が得られます。 これらのシナリオは別の問題を指摘しています。

- アプリケーションは実行されていませんが、それをホストするサーバは実行されています。
- TCP ポートは、このアプリケーションのみ（Web アプリケーション用の TCP-80 など）に対してロックされます。

可用性 OLA レポートは、受け取った停止または不調の数に基づいて単にパフォーマンスを監視するのではなく、アプリケーションおよびその割り当て済みサーバの可用性を示す明確なメトリックを管理側に提供します。 管理コンソール はネットワークの可用性を追跡しません。

可用性 OLA レポートの仕組み

可用性 OLA は、アプリケーションがすべてのネットワークにわたり使用可能な時間の割合をレポートします。 たとえば、可用性 OLA は、特定のサーバによってホストされるアプリケーションが 1 か月間にわたる時間の 95.999% ですべてのネットワークに使用可能であると指定できます。 管理コンソール は、5 分ごとに可用性 OLA レポートを更新し、アプリケーションがその運用レベル契約に適合するかどうかを示します。

アプリケーション可用性 OLA の有効化

可用性 OLA リストを使用して、アプリケーション用の可用性 OLA レポートを有効にし、運用レベル コンプライアンスのしきい値を指定します。しきい値を指定するときは、レポートに対して使用する予定の期間を考慮します。たとえば、12 か月間の可用性をレポートする場合、1 月間のレポートに対して使用したのとは異なるしきい値を設定する場合があります。同じアプリケーションに対して複数の可用性 OLA を作成できないことに注意してください。

可用性 OLA を指定するときは、必ずアプリケーション自体の可用性監視も有効にしてください。 可用性 OLA を指定しても、アプリケーションは自動的に更新されません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［可用性 OLA］をクリックします。

   ［可用性 OLA リスト］が表示されます。
3.  をクリックして OLA を編集します。

   ［運用レベル契約の設定］が表示されます。
4. ［可用性 OLA の有効化］を選択し、このアプリケーションを使用可能にする時間の最小の割合を入力し、［OK］をクリックします。 しきい値は、93.999 のように小数第 3 位まで指定できます。

   管理コンソール により、アプリケーション上の可用性監視を有効にする確認が表示されます。

詳細:

ユーザ定義アプリケーションの編集 (P. 153)

第 10 章: ユーザ アカウント権限の管理

このセクションには、以下のトピックが含まれています。

ユーザ アカウントの権限設定の仕組み (P. 250)
FAQ (P. 260)

ユーザ アカウントの権限設定の仕組み

ユーザ アカウントのセキュリティはログイン アクセス権限に基づいており、CA PC および CA NPC に対して完全な互換性があります。管理コンソール 管理者は、管理コンソール、CA PC、CA NPC で有効な、安全なユーザ アカウントを作成および管理します。 これらのアカウントにより、他のオペレータは 管理コンソール の管理機能およびレポート データにアクセスできます。レポート データへのアクセスは、CA PC または CA NPC のグループに基づいてさらに制限できます。

アクセスの安全なシステムを作成するには、許可されたユーザが、ユーザ アカウントと関連付けられた役割および製品権限に基づいて製品機能へアクセスします。 管理コンソール が CA PC または CA NPC に登録されている場合、これらのアカウントの作成および変更に関連付けられたタスクはすべて CA PC の［管理］ページまたは CA NPC の［Administration］ページで実行されます。

管理コンソール 管理者は、追加のユーザ アカウントを作成し、選択されたコンポーネントのパフォーマンスを追跡する必要がある場合があります。 セキュリティー強化のために、管理者は、あらかじめ設定された管理者およびユーザ アカウントのデフォルトのパスワードも変更する必要があります。

管理コンソール は、CA PC または CA NPC のいずれかでデータ ソースとして登録されている必要があります。 管理コンソールの［環境管理］ページの対応する管理タスクは無効です。 CA PC または CA NPC からのユーザ、役割、製品権限、およびグループを管理します。

CA PC に 管理コンソール ユーザを設定する前に、CA PC または CA NPC で管理コンソール ユーザ役割、グループ、および製品権限について理解します。 CA PC または CA NPC のセキュリティ機能には、ユーザ、役割、製品権限、グループ、およびドメインが含まれ、どのユーザが 管理コンソール 内の特定のデータを表示できるかを制御します。

まだの場合は、管理コンソール を CA PC または CA NPC にデータ ソースとして登録します。 CA PC または CA NPC 用のデータ ソースとして 管理コンソール を登録し、CA PC または CA NPC 内のユーザ セキュリティを管理する方法の詳細については、オンライン ヘルプを参照してください。

管理コンソール が CA PC にデータ ソースとして登録されると、管理コンソール のツールバーには CA PC のハイパーリンクが表示されます。 管理コンソール が CA NPC にデータ ソースとして登録されると、管理コンソール のツールバーには CA NPC のハイパーリンクが表示されます。

管理コンソール データ ソースを登録しているが、CA PC または CA NPC のハイパーリンクが表示されない場合は、ログアウトしてから 管理コンソール に再度ログインします。

統合セキュリティ

ユーザ アカウントは以下を指定します。

- 管理コンソール へログインするために使用できるデータベース認証情報および認証方式。CA PC または CA NPC でデータ ソースとして登録された場合、ユーザ アカウントは 管理コンソール および CA PC または CA NPC へのログインに使用できます。
- ユーザがアクセスできる［インシデント］ページなどの 管理コンソール のレポート ページを定義する管理コンソール の役割。
- ユーザがアクセスできる特定のドメインに関するデータなどのレポート データを定義する権限グループ。
- ［環境管理］ページにアクセスする権限などの 管理コンソール 内の管理者レベル権限を定義する製品権限。

  管理コンソール データ ソース上でユーザ セキュリティを管理するには、管理者の製品権限があるユーザ アカウントで 管理コンソール にログインする必要があります。

デフォルトの管理者アカウント admin は、製品権限の変更を防ぐためにロックされます。 このアカウントは、すべての登録済みデータ ソースで管理者権限を得るために必要です。admin アカウントを含むアカウントのグループを選択すると、選択されたいずれのアカウントの製品権限も編集できません。

以下のデフォルトのユーザ アカウントを使用するか、またはユーザ自身で作成します。 できるだけ早くデフォルトのパスワードを変更することを推奨します。

ユーザ アカウント	デフォルトのプロパティ	デフォルトのパスワード
user	権限： ユーザ 役割： ネットワーク オペレータ 権限グループ： すべてのグループ URL を生成する権限： なし	user

ユーザ アカウント	デフォルトのプロパティ	デフォルトのパスワード
管理者	権限： 管理者 役割： ネットワーク管理者 権限グループ： すべてのグループ URL を生成する権限： あり このアカウントを使用して 管理コンソール ユーザを管理します。	管理者
inv	権限： パワー ユーザ 役割： ネットワーク エンジニア 権限グループ： すべてのグループ URL を生成する権限： あり	inv

製品権限

管理コンソール にログインするには、CA Application Delivery Analysis データ ソースに対する製品権限が必要です。 製品権限は、［環境管理］ページへのアクセスも指定します。

ユーザ

［環境管理］ページ以外の、管理コンソール のすべてのページへのアクセスが許可されます。

管理者

［環境管理］ページを含め、管理コンソール のすべてのページへのアクセスが許可されます。

パワー ユーザ

ユーザ レベルの製品権限、および［表示項目］メニューから［環境管理］ページの［SNMP プロファイル］、［ネットワーク デバイス］、および［デバイス グループ］へのアクセスが許可されます。

ヒント： ユーザが 管理コンソール ユーザ インターフェースにログインできない場合は、CA Application Delivery Analysis データ ソース上の製品権限を与えられているかを確認します。

役割

役割ベースのセキュリティにより、CA Application Delivery Analysis ユーザは以下の操作を行うことができます。

- 管理コンソール の部分へのアクセス。
- CA PC または CA NPC ビューから 管理コンソール 内のレポートにドリル イン。

詳細:

データ ソースへのドリル イン権限 (P. 255)
役割の権限 (P. 254)

役割の権限

以下のテーブルでは CA Application Delivery Analysis （以前の名称： NetQoS SuperAgent）管理コンソールに適用可能な役割の権限の概要について説明します。

役割権限の名前	説明
エンジニアリング	［エンジニアリング］セクションに移動し、エンジニアリング レポートを作成します。
操作	［オペレーション］セクションに移動し、オペレーション レポートを作成します。
管理	［管理］セクションに移動し、管理レポートを作成します。
インシデント	［インシデント］セクションに移動し、インシデント レポートを表示します。
調査	［調査］を起動し、［調査］のデータにドリル ダウンします。

役割の権限は、CA Application Delivery Analysis ユーザに以下の許可を与えません。

- CA Application Delivery Analysis 管理コンソール の［環境管理］ページにアクセスする権限。

  ユーザに［環境管理］ページへのアクセスを許可するには、CA Application Delivery Analysis データ ソースに対する［管理者］製品権限または［パワー ユーザ］製品権限を付与します。

- CA Application Delivery Analysis 管理コンソール 内の実際のレポート データへのアクセス。

  ユーザがレポート データを参照できるようにするには、適切なグループをユーザに割り当てます。

詳細情報:

製品権限 (P. 253)
ユーザおよびグループ (P. 256)

データ ソースへのドリル イン権限

［データ ソースへのドリル イン］役割権限によって、ユーザは CA PC または CA NPC ビューから CA Application Delivery Analysis などのサポートされたデータ ソースにドリル インできます。 この役割権限は、ユーザの役割に割り当てられたすべてのデータ ソースに適用されます。

CA Multi-Port Monitor で設定された場合、この役割権限は、CA Application Delivery Analysis から CA Multi-Port Monitor へのドリル インも可能にします。

重要: Multi-Port Monitor は、CA PC または CA NPC からの権限セットを強制適用しません。 たとえば、ユーザにサーバの特定のグループに対する権限があり、Multi-Port Monitor がグループ内のサーバの少なくとも 1 つを監視できる場合、Multi-Port Monitor はドメイン内のすべてのサーバに対するパフォーマンス データを表示します。

詳細:

役割 (P. 254)

ユーザおよびグループ

CA PC または CA NPC のグループベースのセキュリティ モデルを使用して、管理コンソール 内のレポート データへのアクセス権を付与できます。 デフォルトでは、CA PC または CA NPC の役割は、管理コンソール データ ソースのレポート データへのアクセス権をユーザに付与しません。

グループを作成し、管理コンソール データ ソース内のすべてのアプリケーション、サーバ、ネットワークのアクセス件を与えるのではなく、一部のアプリケーション、サーバ、およびネットワークにアクセスする権限をユーザに与えます。 ユーザが 管理コンソール 内のグループについてレポートできるようにするには、グループにアクセスするためのユーザ権限を与える必要があります。

システム グループにより、管理コンソール データへのユーザ アクセスが与えられます。 必要に応じて、カスタム グループを作成しユーザがアクセスするデータを指定することができます。 たとえば、ユーザがシステム定義のアプリケーションについてレポートできるようにするには、対象のアプリケーション ポートをホストするサーバを含むサーバ グループを作成します。

システム グループ

複数の 管理コンソール またはドメインからのデータについてレポートするためにシステム グループを作成します。

すべてのアプリケーション

各 管理コンソール データ ソースによってレポートされるアプリケーションをすべて含みます。

すべてのドメイン

各ドメインのグループ メンバシップを含みます。

ドメイン

ドメイン用のグループ メンバシップを含みます。 デフォルトでは、［デフォルト ドメイン］が表示されます。

All Servers

各 管理コンソール データ ソースによってレポートされたサーバ、および他のデータ ソースに定義されたサーバをすべて含みます。

Application Delivery Analysis ネットワーク

すべての 管理コンソール データ ソースからのネットワークを含みます。

データ ソース

CA PC または CA NPC に設定情報をレポートした 管理コンソール データ ソースが含まれます。管理コンソール データ ソースにはそれ自身のシステム グループが含まれます。

CA PC ユーザ アカウントをすべてのシステム グループが含まれる［すべてのグループ］グループに割り当てると、ユーザは自分の役割選択に含まれるすべてのレポート内の 管理コンソール データをすべて参照できます。

データ ソース システム グループ

データ ソース システム グループは、CA PC および CA NPC によって自動的に生成され、CA Application Delivery Analysis 管理コンソールおよび特定の CA Application Delivery Analysis データ ソース上の CA PC または、CA NPC 管理コンソールの両方からのグループ ベースのレポートを可能にします。以下のデータ ソース システム グループが生成されます。

すべてのアプリケーション

データ ソースによってレポートされたすべてのアプリケーションを含み、以下のタイプ別にアプリケーションを整理します。

- コントロール ポート アプリケーション。
- FTP アプリケーション。
- 標準的なアプリケーション。
- Web アプリケーション。

すべてのネットワーク

データ ソースによってレポートされたすべてのクライアント サブネットワークを含み、以下によってネットワークを整理します。

- ドメイン。 重複した IP トラフィックを分離するためのドメインを実装していない場合、すべてが［デフォルト ドメイン］に含まれています。
- ネットワーク地域タイプ。

All Servers

データ ソースによってレポートされたすべてのサーバを含み、以下によってサーバを整理します。

- 監視デバイス。 監視デバイス に割り当てられるサーバを表示します。
- 割り当てられていません。 監視デバイス に割り当てられないサーバを表示します。

関係

関係別に整理された、サーバおよびアプリケーションを含みます。

- サーバへのアプリケーション。 アプリケーションに割り当てられたすべてのサーバを含みます。
- アプリケーションへのサーバ。 サーバに割り当てられたすべてのアプリケーションを含みます。

詳細:

テナントの管理 (P. 113)
サーバの管理 (P. 89)
ネットワーク タイプ別のクライアント ネットワークのグループ化 (P. 59)
コントロール ポート アプリケーションの作成 (P. 149)
FTP アプリケーションの作成 (P. 146)
標準アプリケーションの作成 (P. 139)
Web アプリケーションの作成 (P. 145)

グループに関するヒント

レポート目的で、アプリケーション、ネットワーク、およびサーバをグループ化するときは、以下の点を考慮します。

- アプリケーション。 同じアプリケーションの複数層のみを 1 つのグループに含めます。 異なる層で複数のアプリケーションに含まれる可能性があるアプリケーション トラフィックのグループ化を試行すると、予期しない結果をもたらす場合があります。 たとえば、Telnet アプリケーションは、企業全体にわたる異なる多層アプリケーションの一部であるサーバ上で実行される場合があります。 レポートのため Telnet アプリケーション トラフィックすべてをグループ化すると、誤解を招きやすく、管理コンソール データの解釈が難しくなります。
- ネットワーク。 カスタム ネットワーク グループを作成することを推奨します。 これらのグループは、同様のネットワークを比較するときや、レポートでの特定の帯域幅を持ったネットワークをすべて確認するのに役立ちます。同様のネットワーク ラウンドトリップ時間を持つネットワークは、同様の帯域幅を持つことが多いためグループ化できます。または、ファイナンス、テスト、および開発などの部門別にネットワークをグループ化して運用レベルを比較できます。
- サーバ。サーバ グループは、特定のアプリケーションの問題をトラブルシューティングする際に有用です。アプリケーションによって使用されるすべてのサーバを含むグループを作成し、異常なパフォーマンスを探すことができます。

FAQ

- 管理コンソール にログインできないのはなぜですか。

  ユーザが 管理コンソール にログインできない場合は、管理コンソール データ ソースに対して CA PC または CA NPC での製品権限 (P. 253)があるかどうかを確認します。

- 管理コンソール にログインした後、ページの一部が表示されないのはなぜですか。

  ユーザが［操作］、［インシデント］、［管理］、または［エンジニアリング］ページを表示できない場合は、ユーザが正しい役割 (P. 254) を持ち、その役割が適切な選択をしているかを確認します。 各レポート ページへのアクセスはユーザの割り当てられた役割内の選択内容によって制御されます。

- ユーザが［環境管理］ページを表示できない場合は、管理コンソール データ ソースに対して CA PC または CA NPC での製品権限 (P. 253) があるかどうかを確認します。

- 管理コンソール 内にレポート データはなぜないのですか。

  管理コンソール 内のページが適切なデータを表示しない場合は、管理コンソール データ ソースに対して CA PC または CA NPC での製品権限 (P. 253)があるかどうかを確認します。

- CA PC または CA NPC から 管理コンソール にドリル インできないのはなぜですか。

  ユーザの役割に、［データ ソースへのドリル イン (P. 255)］役割権限と、管理コンソール データ ソースの適切なページに対する役割権限が必要です。

第 11 章: システム管理

このセクションには、以下のトピックが含まれています。

Windows 管理者の認証情報 (P. 261)
データベースの管理 (P. 261)
コンソール設定の管理 (P. 267)
IP アドレスの変更 (P. 268)
SNMP プロファイルの管理 (P. 269)
ネットワーク デバイスの管理 (P. 274)
スケジュール済み電子メールの管理 (P. 280)
システム保守の実行 (P. 281)

Windows 管理者の認証情報

CA アプライアンスには、以下のデフォルト管理者アカウントが設定されています。

Windows 2008 オペレーティング システム

netqos/Changepassword1

Windows 2003 オペレーティング システム

netqos/changeme

nqadmin/qosisking

データベースの管理

管理コンソール は、データ保存およびレポートのために MySQL データベースをホストします。

必要なサービス

正常に動作している場合、管理コンソール は下にリスト表示されたサービスを自動的に開始します。

警告： データの損失を回避するために、これらのサービスを手動で停止または再起動しないでください。 支援情報については、CA サポート（**エラー! ハイパーリンクの参照に誤りがあります。**）までお問い合わせください。

- **CA ADA Availability Poller。** アプリケーションをホストするサーバが CA Standard Monitor によって監視される場合、監視 上の CA ADA Availability Poller サービスがアプリケーションの可用性を確認します。そうでない場合は、CA Standard Monitor 上の CA ADA Availability Poller サービスが、アプリケーションの可用性を確認します。
- **CA ADA Data Transfer Manager。** Cisco WAE デバイスを同期して、管理コンソール 上で定義されたアプリケーション、サーバ、およびクライアント ネットワークに基づいてアプリケーションのパフォーマンスを監視します。
- **CA ADA Inspector。** CA ADA Master Batch サービスによって処理された 5 分間の .dat ファイルをデータベースにロードし、CA ADA Inspector Agent サービスと通信して調査を開始します。
- **CA ADA Inspector Agent。** アプリケーションをホストするサーバが CA Standard Monitor によって監視される場合、監視 上の CA ADA Inspector Agent サービスがアプリケーション、サーバおよび関連するネットワーク上で調査を開始します。そうでない場合は、CA Standard Monitor 上の CA ADA Inspector Agent サービスが調査を開始します。
- **CA ADA Messenger。** モニタリング CA Standard Monitor、CA Multi-Port Monitor および CA GigaStor 監視デバイス を同期して、管理コンソール 上で定義されたアプリケーション、サーバ、およびクライアント ネットワークに基づいてアプリケーションのパフォーマンスを監視します。
- **NetQoS MySql51 サービス。** 管理コンソール データベースをホストする MySql サーバを開始および停止します。
- **CA ADA Monitor。**管理コンソール または CA Standard Monitor 上にある CA ADA Monitor サービスは、CA GigaStor、Cisco WAE、または Cisco NAM デバイスからミラーリングされた TCP パケットを受信しファイルを要約します。
- **CA ADA Data Pump。**管理コンソール データベース上で週単位で保守を実行します。

- **CA ADA Master Batch サービス。** 5 分間の .dat ファイルに処理するために CA Standard Monitor 上の CA ADA Batch サービスからデータ ファイルを受信します。

データベースのステータス

［データベース ステータス］ページでは、使用可能なディスク空き容量、現在監視されているサーバ、アプリケーション、ネットワークの数、およびデータベースの増大速度について概要を示します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［データベース］、［ステータス］をクリックします。

   ［データベース ステータス］が表示されます。
3. データベース増加に関するサマリ統計が表示されます。

   データベース サマリ統計の詳細については、［ヘルプ］をクリックしてください。

詳細:

管理コンソールによるデータベース増加の管理方法 (P. 296)

データベース ストレージ基本設定の編集

データベース ストレージの基本設定を編集して以下について指定します。

- データベース内でレポート データを保存する期間
- 週単位のデータベース保守を実行する時期
- 使用可能なディスク空き容量が指定されたしきい値を下回ったときに、電子メールまたは SNMP トラップの通知を受信する人

ハード ドライブの全部またはほぼ全部が、既存データのレポートおよび新しいデータの収集に影響します。 データ保存の期間および保持するデータのタイプの設定が可能なオプションもあります。 詳細については、以下のセクションを参照してください。 デフォルトでは、管理コンソール は、以下のタイプのデータを以下の期間保存します。

データ タイプ	保存期間	保管期間
履歴インシデント レコード	5 分データと同じ保存期間	1 ～ 12 か月
5 分データ	1 か月	1 ～ 12 か月
1 時間ごとのデータ	6 か月	1 ～ 12 か月
OLA データ	13 か月	1 ～ 25 か月

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［データベース］、［保守］をクリックします。

   ［データベース保守］が表示されます。
3. データベース ストレージの基本設定を編集します
4. 使用可能なディスク空き容量がしきい値より下回ったときに、管理コンソール がユーザに通知する方法を指定します。

   データベース ストレージの基本設定の設定の詳細については、［ヘルプ］をクリックしてください。
5. ［OK］をクリックします。

データベースからのデータのパージ

管理コンソール は、ユーザの指定したアプリケーション、サーバおよびネットワーク定義に従ってレスポンス時間データを自動的にメンテナンスします。したがって、データをパージすることは通常必要ではありません。 必要ならば、すべてのデータおよび定義をパージするか、または特定の期間に、特定のタイプのデータ（たとえば 5 分データなど）をパージできます。

パージ後は、データを回復できません。 CA サポート によってリクエストされた場合のみデータをパージすることを推奨します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［データベース］、［データをパージ］をクリックします。

   ［データをパージ］ダイアログ ボックスが表示されます。
3. データベースからすべてのデータをパージするオプションを選択するか、または特定のタイプのデータをパージするタイムフレームを指定し、［OK］をクリックします。

   管理コンソール が CA PC または CA NPC にデータ ソースとして登録されている場合、管理コンソール データベースからデータをすべてパージする前に 管理コンソール を登録解除します。 パージが完了した後、管理コンソール を CA PC または CA NPC にデータ ソースとして再度登録します。 管理コンソール を登録解除する詳細については、CA PC または CA NPC のオンライン ヘルプを参照してください。
4. プロンプトで［削除を続行］をクリックし指定されたデータをパージします。

データベースのバックアップとリストア

初めて 管理コンソール をインストールする場合、管理コンソール はその週単位のデータベース保守の一部としてデータベース バックアップを自動的に実行しません。

さまざまな状況が回復不可能なデータベースに結びつく場合があるので、週単位のデータベース バックアップをスケジュール設定し実行することをお勧めします。 詳細については、CA サポート Web サイト http://support.ca.com を参照してください。

コンソール設定の管理

管理コンソール 設定を使用して以下を行います。

- 管理コンソール の名前を表示します。
- 電子メール設定を管理します。

  CA PC または CA NPC にデータ ソースとして登録された場合、電子メール設定は CA PC または CA NPC によって管理されます。管理コンソールがデータ ソースとして登録されない場合は、以下の設定を指定します。

  - SMTP サーバの IPv4 アドレス。
  - 管理コンソールから指定された SMTP サーバへの TCP-25 発信アクセス。
  - 電子メール アドレスへの返信。有効な返信用電子メール アドレスを指定して、スパム プログラムが 管理コンソール からの電子メール通知をフィルタするのを防ぎます。
  - 電子メール送信されるレポートの推奨チャート画像形式： PNG または JPEG。
- NRTT しきい値を設定して、キープアライブ メッセージを使用するアプリケーションをフィルタします。
- 管理 IP アドレスおよび NIC の指示を確認し、管理コンソール の管理 IP アドレスをその 監視デバイス に送信します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［設定］をクリックします。

   ［コンソール設定］が表示されます。
3. コンソール設定を編集して、［OK］をクリックします。

   コンソール設定の詳細については、［ヘルプ］をクリックしてください。

詳細:

アプリケーションのキープアライブ メッセージ (P. 162)
IP アドレスの変更 (P. 268)

IP アドレスの変更

ユーザのニーズを満たすように管理コンソールの IP アドレスを変更します。 IPv4 アドレスは、ドット区切りで 4 つの部分に分け、10 進表記法で指定する必要があります。

IP アドレスを変更すると、管理コンソールは、その 監視デバイス を更新する前に、新しい IP アドレスを使用するようユーザに要求します。 監視は、管理コンソール 関連サービスが再起動される間一時的に中断されます。

監視 NIC の IP アドレスがルーティングできない場合、それを変更する必要はありません。

次の手順に従ってください:

1. 開始する前に、管理コンソール からログアウトします。
2. 管理コンソール コンピュータで、Windows にログインし、以下のタスクを完了します。
   a. 管理 NIC プロパティを更新し、IPv4 アドレスをドット区切りの 4 つの部分からなる 10 進表記法で指定します。
   b. ［サービス］コントロール パネルで、CA ADA 関連のサービスを再起動します。
   c. ログオフします。
3. Web ブラウザで、管理コンソール にログインします。

   管理コンソール により、管理コンソール の IP アドレスが変更されたことが通知され、使用する IP アドレスを選択するよう促されます。
   a. 新しい IP アドレスを選択し、新しい IP アドレスの監視デバイスすべてに通知するオプションを選択します。
   b. ［OK］をクリックします。
4. 監視デバイス がコンソールの更新された IP アドレスと通信していることを確認します。
   a. ［環境管理］ページをクリックします。
   b. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
   c. ［ADA 監視デバイス リスト］までスクロールし、監視 がそれぞれ［実行中］のステータスであることを確認します。

必要に応じて、青い歯車型メニュー（ ）をクリックし、［コンソールの設定］をクリックして、次に［監視デバイスを同期］をクリックしてすべての 監視デバイス 上の 管理コンソール の IP アドレスを更新します。

SNMP プロファイルの管理

SNMP プロファイルには、管理コンソール が以下を行うために必要な SNMP ユーザの認証情報が保存されています。

- SNMP エージェントに以下を問い合わせます。
  - サーバまたはネットワーク デバイスのパフォーマンス データ（サーバまたはネットワーク デバイス上のインシデントに対応するか、または調査として）。
  - トレース ルート調査の一部としてネットワーク定義を収集する、またはパフォーマンス情報を収集するルータ。

    SNMP プロファイルを編集して、管理コンソール が SNMP エージェントにクエリを行うポートを指定できます。 デフォルトでは、管理コンソール は、UDP-161 上で SNMP エージェントにクエリを行います。
- サーバ、アプリケーション、ネットワークまたは 監視デバイス 上のインシデントに応答して SNMP トラップ メッセージを送信します。

  管理コンソール が SNMP トラップを送信するポートは変更できないことに注意してください。 管理コンソール は、常に SNMP トラップを UDP-162 に送信します。

管理コンソール は、SNMPv1、SNMPv2 および SNMPv3 を使用してデバイスへの認証をサポートし、読み取り専用権限を必要とします。

CA Performance Center または CA NetQoS Performance Center に登録されると、CA Performance Center または CA NetQoS Performance Center は、管理コンソール と、CA Performance Center または CA NetQoS Performance Center のそのインスタンスに登録されている他の CA 製品との間で SNMP プロファイルの変更を同期します。 CA Performance Center および CA NetQoS Performance Center が SNMP プロファイルを同期する方法の詳細については、オンライン ヘルプを参照してください。

SNMP プロファイル ディスカバリの仕組み

管理コンソール が SNMP ポーリング リクエストを実行するとき、サーバまたはルータが有効な SNMP プロファイルを割り当てられない場合、管理コンソール は、使用可能な SNMP プロファイルのリストを使用して、SNMP エージェントと通信を試行することにより、有効な SNMP プロファイルを検出します。

CA Application Delivery Analysis がデータ ソースとして CA PC または CA NPC に登録された場合、CA Application Delivery Analysis Manager は、ディスカバリに含まれるように設定もされている CA PC または CA NPC から同期された SNMP プロファイルを使用して、有効な SNMP プロファイルを検出します。

管理コンソール が有効な SNMP プロファイルを検出すると、管理コンソール は SNMP プロファイルをサーバまたはネットワーク デバイスに割り当てます。 管理コンソール が有効な SNMP プロファイルを検出できない場合、SNMP ポーリング リクエストはタイムアウトになります。

管理コンソール SNMP は、以下の目的で、サーバまたはネットワーク デバイスをポーリングします。

- SNMP 経由のパフォーマンス調査を実行するため
- トレース ルート調査の一部として
- ルータからネットワーク定義をインポートするため

SNMP プロファイルをディスカバリ プロセスに含まれないよう設定できることに注意してください。ディスカバリに使用できる SNMP プロファイルの数を制限することを推奨します。

SNMP プロファイルの追加

SNMP プロファイルを追加して、管理コンソール がサーバまたはネットワーク デバイスにクエリを行い、SNMP ユーザ認証情報の指定されたセットを使用して、SNMP トラップを送信できるようにします。

管理コンソール が CA PC または CA NPC にデータ ソースとして登録されている場合、CA PC または CA NPC で SNMP プロファイルを管理します。CA PC または CA NPC は、管理コンソール およびその他の登録済みデータ ソースが有効なプロファイルを検出する順序を指定できるようにして、SNMP プロファイル デスカバリを向上させます。

管理コンソール ディスカバリ プロセスに含まれる SNMP プロファイルの数を制限することを推奨します。 CA PC または CA NPC から SNMP プロファイルを設定する詳細については、オンライン ヘルプを参照してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［SNMP プロファイル］をクリックします。

   ［SNMP プロファイル］が表示されます。
3. ［SNMP プロファイルの追加］をクリックします。

   ［SNMP プロファイルのプロパティ］が表示されます。
4. SNMP プロファイルを指定して、［OK］をクリックします。

   SNMP プロファイルのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

詳細:

テナントの管理 (P. 113)
SNMP プロファイル ディスカバリの仕組み (P. 270)

SNMP プロファイルの編集

［SNMP プロファイル］リストを使用して、管理コンソール と CA PC または CA NPC の間の SNMP プロファイルのリストを表示および管理します。

CA PC または CA NPC に 管理コンソール が登録されており、CA PC または CA NPC が SNMP プロファイルを変更した場合、変更は 管理コンソール と自動的に同期されます。 管理コンソール 内の SNMP プロファイルの変更が CA PC または CA NPC にも登録されている他のデータ ソースにどのように影響するかについては、オンライン ヘルプを参照してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［SNMP プロファイル］をクリックします。

   ［SNMP プロファイル］が表示されます。
3.  をクリックし、SNMP プロファイルを編集します。

   ［SNMP プロファイルのプロパティ］が表示されます。
4. SNMP プロファイルのプロパティを編集して、［OK］をクリックします。

   SNMP プロファイルのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

SNMP プロファイルの削除

管理コンソール から削除するには、SNMP プロファイルを削除します。CA PC または CA NPC に 管理コンソール を登録している場合、CA PC または CA NPC は他の登録済みのデータ ソースと変更を同期します。

削除された SNMP プロファイルがサーバまたはネットワーク デバイスに割り当てられた場合、管理コンソール は SNMP プロファイルを割り当て解除します。 管理コンソール が SNMP ポーリング リクエストを実行する必要があり、サーバまたはルータには割り当て済みの SNMP プロファイルがない場合、管理コンソール は 1 つ検出します。

SNMP トラップ通知に割り当てられる SNMP プロファイルを削除すると、管理コンソール は自動的に SNMP トラップ通知を更新し、SNMP トラップに予約済みの特別な SNMPv2 プロファイル、*SuperAgent* を使用します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［SNMP プロファイル］をクリックします。

   ［SNMP プロファイル］が表示されます。
3.  をクリックし、SNMP プロファイルを削除します。
4. プロンプトで［削除を続行］をクリックし SNMP プロファイルを削除します。

詳細:

SNMP プロファイル ディスカバリの仕組み (P. 270)

ネットワーク デバイスの管理

たとえば、パフォーマンス情報についてルータを SNMP ポーリングするなど、管理コンソール にそのデバイスで SNMP クエリを実行させる予定の場合、ネットワーク デバイスを 管理コンソール に追加することを推奨します。

SNMP プロファイルをネットワーク デバイスに割り当てないと、管理コンソール は有効な SNMP プロファイルの検出を試行します。

管理コンソール は、以下の場合に SNMP クエリを実行します。

- ネットワーク情報についてルータを SNMP ポーリング (P. 56) する。
- SNMP 経由のパフォーマンス調査 (P. 202) の開始
- トレース ルート調査 (P. 205) の開始。

詳細:

SNMP プロファイル ディスカバリの仕組み (P. 270)

ネットワーク デバイスの追加

任意のタイプのネットワーク デバイスを追加し、そのデバイス上で調査を実行します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［ネットワーク デバイス］をクリックします。
3. ［表示項目］メニュー下の［ネットワーク デバイスの追加］をクリックします。

   ［デバイスのプロパティ］が表示されます。
4. ネットワーク デバイスのプロパティを指定して［OK］をクリックするか、または［保存してほかを追加］をクリックして、別のデバイスを追加します。

   ネットワーク デバイスのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

ネットワーク デバイス調査の表示

ネットワーク デバイス リストを使用して、任意のネットワーク デバイス調査の結果を表示します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［ネットワーク デバイス］をクリックします。

   ［ネットワーク デバイス］が表示されます。
3. デバイスの隣の  をクリックし、［調査レポート］ページを開きます。
4. ［調査レポート］で、検索条件を指定し、［検索］をクリックして調査のリストをフィルタします。

   ［調査レポート］内容はユーザのフィルタ選択内容によって変わります。

   検索条件の設定の詳細については、［ヘルプ］をクリックしてください。

ネットワーク デバイスの編集

ネットワーク デバイスを編集して、たとえば SNMP プロファイルの割り当てることにより、そのプロパティを更新します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［ネットワーク デバイス］をクリックします。
3. ［ネットワーク デバイス］が表示されます。
4.  をクリックしてデバイスを編集します。

   ［デバイスのプロパティ］が表示されます。
5. ネットワーク デバイスのプロパティを指定して［OK］をクリックするか、または［保存してほかを追加］をクリックして、別のデバイスを追加します。

   ネットワーク デバイスのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

ネットワーク デバイスの削除

管理コンソール がそのデバイス上で調査を実行するのを防ぐためにネットワーク デバイスを削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［ネットワーク デバイス］をクリックします。
3. ［ネットワーク デバイス］が表示されます。
4.  をクリックし、ネットワーク デバイスを削除します。
5. プロンプトで［削除を続行］をクリックし、ネットワーク デバイスを削除します。

調査用のグループ ネットワーク デバイス

ネットワーク デバイス グループを作成して、管理コンソール 管理者がネットワーク デバイスのグループ上で調査をスケジュールまたは開始できるようにします。 たとえば、パフォーマンス情報についてルータのグループを SNMP ポーリングできます。

ネットワーク デバイス グループの追加

管理コンソール 管理者がネットワーク デバイスのグループ上で調査をスケジュールまたは開始できるようにするには、ネットワーク デバイス グループを追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［デバイス グループ］をクリックします。

   ［ネットワーク デバイス グループ］が表示されます。
3. ［デバイス グループの追加］をクリックします。

   ［デバイス グループのプロパティ］が表示されます。
4. ［デバイス グループ名］ボックスに名前を入力して、［OK］をクリックします。
5. ［使用可能なデバイス］リストでデバイスを選択し、右方向矢印をクリックして[含まれるデバイス]リストにそれらを移動することによってデバイスをグループに追加します。

   ［含まれるデバイス]リストでデバイスを選択し､左方向矢印をクリックして［使用可能なデバイス］リストにそれらを移動することによってグループからデバイスを削除します。

ネットワーク デバイス グループの調査の表示

［ネットワーク デバイス グループ］リストを使用して、ネットワーク デバイスのグループ上で 管理コンソール 管理者によって実行された調査を表示します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［デバイス グループ］をクリックします。

   ［ネットワーク デバイス グループ］が表示されます。
3. デバイス グループの隣りの  をクリックし、その調査を表示します。
4. ［調査レポート］が表示されます。
5. （オプション）条件を指定して調査のリストをフィルタします。

   調査タイプ

   表示する調査のタイプ。 ［すべての調査］または特定の調査タイプをクリックします。

   ターゲット タイプ

   表示する調査のターゲットのタイプです。［すべてのターゲット］または特定のターゲット タイプ（デバイス、グループなど）をクリックします。

   ターゲット

   表示する調査のターゲットです。 名前または IP アドレスによる特定のターゲットを選択します。

   ［調査レポート］内容はユーザのフィルタ選択内容によって変わります。

ネットワーク デバイス グループの編集

ネットワーク デバイス グループを編集して、グループに属するネットワーク デバイスのリストを変更します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［デバイス グループ］をクリックします。
3. ［ネットワーク デバイス グループ］が表示されます。
4.  をクリックしてデバイスを編集します。

   ［デバイスのプロパティ］が表示されます。
5. ネットワーク デバイスのプロパティを指定して［OK］をクリックするか、または［保存してほかを追加］をクリックして、別のデバイスを追加します。

   ネットワーク デバイスのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

デバイス グループの削除

管理コンソール がデバイスのグループ上で調査を実行するのを防ぐためにネットワーク デバイス グループを削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［調査］、［デバイス グループ］をクリックします。

   ［ネットワーク デバイス グループ］が表示されます。
3.  をクリックし、デバイス グループを削除します。
4. プロンプトで［削除を続行］をクリックし、デバイス グループを削除します。

スケジュール済み電子メールの管理

管理コンソール ユーザの製品権限により、ユーザがレポートで何をできるかが決定します。たとえば、以下のようになります。

- レポートを表示する権限を持つユーザは、電子メールでレポートを送信するためのスケジュールを作成できます。
- 管理者の製品権限を持つユーザは、電子メール送信されるレポートのスケジュールまたは電子メールの設定を調節し、監視デバイス に関するレポートをスケジュールおよび送信できます。

電子メール レポートのスケジュールの編集

スケジュール済み電子メール レポートのリストを表示および管理し、たとえば、電子メールおよびスケジュール オプションを変更します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［スケジュール済み電子メール］をクリックします。
3. ［スケジュール済み電子メール］が表示されます。
4.  をクリックし、スケジュール済み電子メールを編集します。

   ［スケジュール済み電子メールのプロパティ］が表示されます。
5. スケジュール済み電子メールのプロパティを指定して、［OK］をクリックします。

   スケジュール済み電子メールのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。

スケジュール済みレポートの削除

スケジュール済みレポートをキャンセルするには、スケジュール済み電子メールを削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［スケジュール済み電子メール］をクリックします。
3. ［スケジュール済み電子メール］が表示されます。
4.  をクリックし、スケジュール済みレポートを削除します。
5. ［削除の確認］で、［削除を続行］をクリックしスケジュール済み電子メールを削除します。

システム保守の実行

このセクションでは、システム管理者が CA Application Delivery Analysis をセットアップおよびメンテナンスする方法について情報を説明します。

ハードディスクドライブをメンテナンスする方法

管理コンソール には、読み取り/書き込み操作のため常にアクセスするいくつかのテーブルが含まれます。これらのテーブルは、管理コンソール がインストールされているドライブ上のディスク空き容量の大部分を占めます。これらの I/O 操作によりディスクのフラグメント化が徐々に起こる場合があります。

ハードディスク ドライブをメンテナンスするには、以下のタスクを実行します。

- 10 ギガバイトより大きなデータベースについては、D ドライブまたは管理コンソール が毎月インストールされるドライブをデフラグします。
  - デフラグ プロセスを開始する前に、このドライブに少なくとも 20% のディスク空き領域が含まれることを確認します。
  - デフラグの前に、NetQoS MySql51 サービスを含む、すべての CA ADA 関連のサービスを停止します。
  - デフラグが完了した後に、これらのプロセスを再開します。
- CA 製品は、絶えずディスクに書き込んでいます。 レポート コンパイルのためのデータ シーク中に、ドライブ ヘッドは書き込みと読み取りを同時に行います。ディスク ドライブのように、この負荷は徐々に障害を引き起こす場合があります。最小のデータ損失で迅速に回復するには、標準のデータベース バックアップをスケジュールします。

詳細:

データベースのバックアップとリストア (P. 266)

システム セキュリティの更新と Windows アップデートをインストールする方法

管理コンソール には出荷時に使用可能な最新の Windows アップデートが含まれます。 Windows アップデートおよび最新のアンチウイルス ソフトウェアのインストールの保守を続行します。 セキュリティおよび管理ポリシーが異なるため、Microsoft の自動更新機能は無効です。 以下の手順に従い自動更新を有効にします。

1. Windows コントロール パネルから［自動更新］を有効にします。
2. ［更新を通知するのみで、自動的なダウンロードまたはインストールを実行しない］オプションを選択します。 このオプションは、システムの不安定を引き起こす更新の自動的なインストールを防ぎます。
3. 重要な Microsoft 更新をインストールします。 推奨された更新またはドライバ更新はインストールしないでください。
4. 更新を適用した後、サーバを再起動します。 サードパーティの管理システムで更新を管理する場合は、更新を適用した後にシステムを自動的に再起動させます。

警告： CA Application Delivery Analysis は Microsoft .NET Framework 3.5 を必要とします。 CA Application Delivery Analysis は Microsoft .NET バージョン 4 以降とは互換性がありません。 Windows Update が .NET バージョン 4 以上の Framework をインストールした場合、CA Application Delivery Analysis は動作を停止する可能性があります。 この問題を修正するには、.NET バージョン 4 以上をアンインストールし、.NET バージョン 3.5 を必要に応じて再インストールします。Microsoft は、NET Framework 4 をアンインストール方法についてナレッジベース記事を発行しています。

データ整合性の確認とアンチウイルス ソフトウェアの使用

以下のガイドラインに従いデータの整合性を確認します。

- 管理コンソール アプライアンスにアンチウイルス ソフトウェアをインストールした場合は、データベース破損を回避するためにリアルタイムおよびスケジュール済みのスキャンからすべての NetQoS ディレクトリを除外します。
- 一元的なアンチウイルス システムからルールをプッシュするように環境を設定した場合は、以下のディレクトリをスキャンから除外するルールを追加します。
  - C:¥Windows¥Temp
  - D:¥NETQOS （または CA Application Delivery Analysis がインストールされているディレクトリ）およびすべてのサブディレクトリ。
- データ書き込み操作中にバックアップによってデータベースがロックされた場合、自動バックアップでデータベースが破損する可能性があります。 このような状態が発生する場合は、データベースを手動でリストアします。
- 管理コンソール ではドライブ領域の圧縮はサポートされません。ドライブ領域を大きくしても、データベース消失の可能性やシステム パフォーマンスの低下に対するメリットはありません。 詳細については、Microsoft Knowledge Base Article の「SQL Server databases not supported on compressed volumes」を参照してください。 また、この記事で説明された圧縮関連の問題は、MySql データベースにも当てはまります。

詳細:

データベースのバックアップとリストア (P. 266)

サードパーティ ソフトウェアに関する問題

アンチウイルス、システム管理、および時間同期のソフトウェアを除いて、サードパーティ製ソフトウェア（特に *Wireshark* などのサードパーティ製ネットワーク監視ソフトウェア）をスタンドアロンの 管理コンソール や CA Standard Monitor にインストールしないでください。サードパーティ製のパケット ドライバは、パケット監視を妨げる可能性があり、保証が無効になることがあります。

スタンドアロン 管理コンソール や CA Standard Monitor にサードパーティ ソフトウェアがインストールされている場合、CA サポート では、トラブルシューティングの前にこれらのソフトウェアをアンインストールするように要求することがあります。

ドメイン グループ ポリシーに関する問題

管理コンソール および CA Standard Monitor アプライアンスは、Windows オペレーティング システムを実行し、Windows ドメインに追加できます。環境によっては、セキュリティ ポリシーおよびサードパーティ ソフトウェアが CA Application Delivery Analysis アプライアンスにプッシュされることがあります。 セキュリティ ポリシーおよびサードパーティ ソフトウェアは、このアプライアンスの通常動作に問題を生じる場合があります。CA Application Delivery Analysis アプライアンスを Windows ドメインに 追加する前に、セキュリティ ポリシーやソフトウェアがサーバにプッシュされないようにこれらを除外してください。

製品アップグレードのサポート

CA Application Delivery Analysis の以前のバージョンを実行している場合で、保守 プランを購入済みの場合は、http://ca.com/support の CA サポート Web サイトから最新のバージョンをダウンロードしてください。

ヒント： ソフトウェア アップグレードまたはビルドをインストールする前には、確実に Windows Update を適用しておくため、サーバを再起動してください。 再起動しない場合、システム障害が生じてオペレーティング システムの再構築が必要となることがあります。

ハードウェア交換の要求

CA Application Delivery Analysis アプライアンスでハードウェア（ハードディスク、ネットワーク インターフェース カード、RAID コントローラなど）の障害が発生した場合、CA サポート に連絡して交換を要求してください。 CA サポート では、ハードウェアの必要な交換時期を確認します。また、以下の情報が必要です。

- サーバのシリアル番号
- 障害が発生したハードウェア コンポーネント
- サーバにロードされている CA Application Delivery Analysis ソフトウェアおよびバージョン
- サーバにロードされているオペレーティング システムのバージョン
- 送付先住所および担当者名

到着した交換用部品やサーバには、返送の出荷ラベルが同梱されています。故障部品やサーバを再梱包し、返送の出荷ラベルを梱包に貼り付けてください。

第 12 章: 監視デバイスの管理

このセクションには、以下のトピックが含まれています。

監視デバイスの動作 (P. 287)
監視フィードのペアの作成 (P. 291)
セッション数情報の表示 (P. 292)
管理コンソールによるデータベース増加の管理方法 (P. 296)
基本操作の実行 (P. 304)
監視デバイス インシデントの管理 (P. 305)
監視のトラブルシュート (P. 316)

監視デバイスの動作

管理コンソール では、Cisco スイッチ インフラストラクチャ、監視およびパケット キャプチャの専用アプライアンス、WAN 最適化デバイスから埋め込まれた計装を任意に組み合わせることができます。 この広範な監視アーキテクチャは、リモート プローブやエージェントなしで作動し、各種のネットワーク グループにとって、それらのアプリケーション配信の目標を達成するためのコスト効率の高い手段となります。

管理コンソール は、以下のタイプの 監視デバイス からのレスポンス時間データを統合します。

監視デバイス	詳細情報の参照先
CA Multi-Port Monitor	*CA Multi-Port Monitor ユーザ ガイド*
CA Standard Monitor	CA Standard Monitor による監視 (P. 321)
CA Virtual Systems Monitor	CA Virtual Systems Monitor による監視 (P. 365)
CA GigaStor	CA GigaStor による監視 (P. 389)
Cisco WAAS	Cisco WAAS による監視 (P. 415)
Cisco NAM	Cisco NAM による監視 (P. 455)
Riverbed Steelhead	Riverbed Steelhead による監視 (P. 473)

監視フィードの動作

監視デバイスは、1つまたは複数の監視フィードからのレスポンス時間メトリックを計算します。*監視フィード*はレスポンス時間データのソースです。たとえば、以下のようになります。

- CA Standard Monitor上のパケット監視フィードは、ミラーリングされたTCPパケットを受信します。
- CA Multi-Port Monitor上のマルチポート監視フィードは、ミラーリングされたTCPパケットを受信します。
- CA Standard MonitorまたはCA Multi-Port Monitor上のWAN最適化監視フィードは、Cisco WAEデバイスからパケット要約ファイルを受信します。
- CA Standard Monitor上のSteelhead監視フィードは、Steelheadで最適化されたパケットを受信します。
- CA Standard MonitorまたはCA Multi-Port Monitor上のGigaStor監視フィードは、CA GigaStorからパケット要約ファイルを受信します。
- CA Application Delivery Analysisマネージャ上のNAM監視フィードは、Cisco NAMからメトリック要約ファイルを受信します。

複数の監視デバイスが同じサーバのトラフィックを観測する場合、管理コンソールでは、特定のサーバに対するレスポンス時間データの最適ソースに関連付けられた監視フィードを自動的に割り当てます。

必要に応じて、割り当てる監視フィードを編集できます。

- セカンダリ監視フィード。管理コンソールは、最適な監視フィードを自動的にサーバに割り当てます。管理コンソールで自動的に別の監視フィードのサーバ（たとえば、そのサーバが別の場所に移行する場合など）を監視するには、セカンダリ監視フィードを監視フィードに割り当てます。
- ドメイン。監視フィードにドメインを割り当てることで、CA Application Delivery Analysisが一意にサーバトラフィックを識別できるようになります。重複したIPトラフィックを監視する場合は、各監視フィードにドメインを割り当てます。

詳細情報:

監視フィードのペアの作成 (P. 291)
監視フィード割り当ての仕組み (P. 289)
監視フィードへのドメインの割り当て (P. 119)

監視フィード割り当ての仕組み

管理コンソール は、各 監視フィード からのサーバ トラフィックを自動的に評価し、最も適切な 監視フィード をサーバに割り当てます。

監視デバイス が最初に TCP セッションを観測する際、管理コンソール は、最大の着信パケット ボリュームを参照する 監視フィード をサーバに割り当てます。 最初の 1 時間は、パケット ボリュームが最大の 監視フィード に対応して、割り当てを 5 分ごとに変更できます。1 時間後、管理コンソール が 監視フィード 割り当てを自動的に変更するには、監視フィード 上のパケット ボリュームが著しく大きいことが必要になります。

パケット ボリュームが同等である場合、管理コンソール は、サーバ接続時間（SCT）が最速の 監視フィード を割り当てます。 監視フィード の自動割り当てを無効にし、特定の 監視フィード を永続的にサーバに割り当てることもできます。

WAN に最適化された環境では、管理コンソール は、サーバ セグメントの監視に最適なパケット数の 監視フィード を割り当て、すべての WAN 最適化デバイスからレスポンス時間メトリックを自動的に計算します。

サーバがネットワーク上の別の場所へ移動する場合、自動的に割り当てられた 監視フィード は、そのサーバ トラフィックを参照する 監視フィード に自動的に変更されます。 管理コンソール が 監視フィード の割り当てを変更するのに、最大で 1 時間かかることがあります。

ロードバランス設定や惨事復旧およびフェールオーバなどの目的で、管理コンソール が複数の 監視フィード からのトラフィックを即座に観測できるようにするには、セカンダリ 監視フィード を 監視フィード に割り当てます。

詳細情報:

監視フィードのペアの作成 (P. 291)
サーバの編集 (P. 93)

監視デバイス同期の動作

管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネットおよびアプリケーション定義に基づいて、アプリケーションのパフォーマンスを監視するには、監視デバイス を同期します。

同期中の監視への一時的な割り込み数を最小限にするには、監視デバイスを同期する前に変更をすべて完了します。

監視デバイス が同期されない場合、それらを同期するように求められます。

あるいは、特定の CA Standard Monitor や CA Multi-Port Monitor、または CA GigaStor を同期 (P. 304)することもできます。

詳細:

基本操作の実行 (P. 304)

監視フィードのペアの作成

サーバ トラフィックが 2 つのスイッチ間でロードバランスされている場合や、フェールオーバの目的でプライマリ スイッチおよびセカンダリ スイッチがある場合には、監視フィード のペアを作成して、割り当て済みのサーバを 管理コンソール が自動的に両方の 監視フィード から監視できるようにします。監視フィード のペアを使用することで、管理コンソール は、いずれの 監視フィード からのアプリケーション トラフィックも即座にレポートできるようになります。

警告： 監視フィード のペアが同じトラフィックを参照する場合、データの重複が生じます。

フェールオーバの発生時には、監視フィード のペアを作成していない場合、サーバが別の場所に移動すると、管理コンソール が新しい 監視フィード を割り当て、そのサーバによってホストされるアプリケーションの監視を再開するまでに最大で 1 時間かかることがあります。

たとえば、ロードバランス設定におけるピアとして機能する 2 つのスイッチがある場合、クライアント ネットワークとサーバの間のトラフィックはいずれかのスイッチに存在する可能性があり、また、各スイッチからの SPAN データは別の 監視デバイス に送信されます。 これらの 監視フィード のペアのいずれか一方とサーバが関連付けられている場合、そのサーバのレスポンス時間データは両方の 監視フィード から収集され、実質的には、そのサーバの「最適」 監視フィード が 2 つ存在することになります。

WAN に最適化された環境の場合、管理コンソール はすべての WAN 最適化デバイスからのレスポンス時間を自動的に計算します。したがって、WAN 最適化 監視フィード をサーバに割り当てる必要はありません。

監視フィード のペアを作成する場合には、観測されるレスポンス時間は監視フィード のプライマリとセカンダリの間で差があることに注意が必要です。これは、その場所から利用可能な 監視デバイス およびサーバ トラフィックの場所の影響などが原因です。また、サーバ トラフィックに対する 監視デバイス の近接状態が変化することにもに注意が必要です。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして CA Standard Monitor または CA Multi-Port Monitor を編集します。

   ［監視のプロパティ］が表示されます。

4. ［監視フィード］までスクロールします。
5. をクリックして 監視フィード を編集します。
6. ［セカンダリ フィード］リストをクリックして、セカンダリ 監視フィード を以下の項目に割り当てます。
   - CA Standard Monitor 上のパケット 監視フィード
   - CA Standard Monitor または CA Multi-Port Monitor 上の WAN 最適化 監視フィード または GigaStor 監視フィード
   - CA Multi-Port Monitor 上のマルチポート 監視フィード
7. ［更新］をクリックして変更を適用します。

詳細:

テナントの管理 (P. 113)
監視デバイスの動作 (P. 287)

セッション数情報の表示

管理コンソール には、監視フィード、監視デバイス、またはすべての 監視デバイス に存在する IPv4 ベースの TCP セッション アクティビティの量に関する情報が表示されます。

アクティブ セッション数情報は、監視フィード が TCP セッションを監視していることを確認するため使用します。 管理コンソール は、サーバ上の 監視 によって観測されるアクティブな TCP セッションの数をアプリケーション ポート別にレポートします。このレポートでは、子アプリケーションは親アプリケーションのインスタンスとして扱われます。たとえば、同じ Web アプリケーション サーバの 2 つの URL は、その Web サーバのアクティビティとしてカウントされます。 そのサーバの設定済みアプリケーションとしてはカウントされません。

[監視フィード]でのアクティブ セッション数の表示

直近の 5 分間のレポート間隔において 監視フィード によってレポートされたアクティブな IPv4 ベースのセッション数を表示するには、[アクティブ セッション数] ページを使用します。

また、監視 または 管理コンソール では、直近の 1 時間のアクティブ セッション数情報を表示することができます。

ただし、NAM 監視フィード ではアクティブ セッション数情報はレポートされません。Cisco NAM Metric Agent は、独自のレスポンス時間メトリックを計算し、セッション数情報の計算に必要な TCP ヘッダは含んでいないためです。

次の手順に従ってください:

1. [環境管理] ページをクリックします。
2. [表示項目] メニューの [データ監視]、[監視デバイス] をクリックします。
3. [ADA 監視デバイス リスト] までスクロールし、 をクリックして目的の 監視フィード のある CA Standard Monitor または CA Multi-Port Monitor を編集します。

   [監視のプロパティ] が表示されます。

   Cisco WAE または CA GigaStor が割り当てられている CA Standard Monitor または CA Multi-Port Monitor を検索するには、[割り当て先] 列を使用します。
4. [監視フィード] の下の [アクティブ セッションを確認] をクリックします。ただし、Cisco NAM 監視フィード にはアクティブ セッション数情報は該当しません。

   [アクティブ セッション数] が表示されます。
5. クリックすると、サーバが展開され、そのアクティブ セッション数情報が表示されます。
6. (オプション) アクティブ セッション数情報を電子メール送信するには、[電子メール] をクリックします。 電子メールのプロパティの指定については、[ヘルプ] をクリックしてください。

   電子メールを送信するには、管理コンソール の電子メール設定 (P. 267) が正しく設定されている必要があります。

7. （オプション）青い歯車型メニュー（ ）をクリックし、［再ロード セッション］を選択すると、リストが更新され、アクティブ セッション数の情報に過去 5 分間のレポート間隔の情報が反映されます。
8. （オプション）同じ 監視デバイス 上の別の 監視フィード のアクティブ セッション数情報を表示するには、［フィードのアクティブ セッションを表示］をクリックし、アクティブ セッション数情報を表示する 監視フィード を選択します。

詳細:

セッション数の 1 時間ごとのサマリの表示 (P. 295)

セッション数の 1 時間ごとのサマリの表示

1 時間ごとのサマリ情報を使用して、アプリケーション、サーバ、および監視 別に IPv4 ベースの TCP セッション数を表示できます。たとえば以下の目的に使用できます。

- 各 監視 のセッションの総数を表示し、特定の 監視 によって観測される各サーバでのセッション数を表示する。
- アプリケーションごとのセッションの総数を表示し、そのアプリケーションをホストする各サーバでのセッション数を表示する。
- サーバごとのセッションの総数を表示し、そのサーバによってホストされる各アプリケーションのセッション数を表示する。

管理コンソール は、セッション数情報を直近の 5 分間隔で観測された IPv4 ベースの TCP セッション数に自動的に更新します。 ただし、Cisco NAM 監視デバイス のセッション数情報は利用できません。

1 時間ごとのサマリ情報をリセットすると、最新のセッション数情報のレポートが開始されます。 また、特定の 監視フィード における直近の 5 分間隔のセッション数情報を表示することもできます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［セッション リスト］をクリックします。

   ［セッション リスト］が表示されます。
3. ［監視デバイス］、［アプリケーション］、［サーバ］を使ってセッション数リストを参照し、リストを展開して必要な情報を検索します。
4. （オプション）［再ロード セッション］をクリックすると、1 時間ごとのサマリがリセットされます。
5. （オプション）青い歯車型メニュー（ ）をクリックすることにより、リストのサマリ情報を電子メールで送信できます。

詳細:

［監視フィード］でのアクティブ セッション数の表示 (P. 293)

管理コンソールによるデータベース増加の管理方法

管理コンソール は、指定されたサーバ サブネット、クライアント ネットワーク、およびポート除外に基づいて、各サーバ上の最もビジーなアプリケーションを監視します。管理コンソール では、そのデータベース リソースを最大限に活用するように試行しながら、データベースが管理不能にならないように保証する必要もあります。

データベース容量

管理コンソール では、そのデータベースの増加を自動的に 1 億 2000 万行に制限します。 それぞれの*行*には、特定のサーバにホストされた特定アプリケーションと特定クライアント ネットワークの間の TCP セッションにおける 5 分間隔のパフォーマンス メトリックが含まれます。 ただし、その組み合わせのネットワーク部分は、実際のクライアント IP アドレスの場合と、ネットワークを /23 マスク（またはそれ以下）として定義している場合はサブネット内のすべてのクライアント IP アドレスの集約の場合があります。

管理コンソール が 5 分間隔の行データを保持する日数に応じて、管理コンソール が監視する組み合わせが増減することがあります。 デフォルトでは、管理コンソール は 5 分間隔のデータを 1 か月間保持するため、平均して、1 日あたりおよそ 400 万の新規行がデータベース内に保存されることになります。

管理コンソール がデータベースの増加をどのように制御するかを分かりやすく説明するために、以下の例で考えます。

- 254 名の会計士のグループが、すべて同じ /24 ネットワーク上にいて、単一のサーバでホストされた同一のアプリケーションにアクセスします。
- これらの会計士は、1 日 8 時間の勤務ですが、昼食と休憩があるため、実質的に会計アプリケーションにアクセスする時間は 1 日およそ 6 時間です。
- この場合、管理コンソール は 1 日あたりおよそ 18,000 行をデータベースに作成します。
  （会計士 254 名 x アプリケーション 1 x サーバ 1 台 x 6 時間 x 12 行/時間（5 分ごとに 1 行） =18,288 行）

この例の場合、管理コンソール は、データベースのサイズの管理なしで、およそ 220 の会計士グループを監視可能です。

データベース増加の制御

管理コンソール は以下のように動作して、最大 1 億 2000 万行を管理します。

- ネットワーク ラウンド トリップ レスポンス時間（NRTT）の最小しきい値を使用して、各組み合わせをフィルタリングし、レポートの統計情報の監視においてキープアライブなどの定期的なクライアント/サーバのメッセージの影響を制限するとともに、データベース増加を制御します。

  5 分間隔における NRTT 観測数が最小しきい値に満たない場合、管理コンソール はその組み合わせの行をデータベースに作成しません。

  レポートの観点からは、組み合わせがフィルタリングされた場合、フィルタリングされた 5 分間隔のセッション レベル統計情報を 管理コンソール がレポートすることはありませんが、ネットワーク全域でのアプリケーションのレスポンス時間メトリックは引き続き有効です。

  管理コンソール でアプリケーションのフィルタリングやグルーミングをしないようにする場合は、アプリケーションに優先順位 (P. 123)を付けます。

  デフォルトでは、管理コンソール は、5 分間隔において10 未満の NRTT が観測 (P. 267)された非優先アプリケーションの組み合わせをフィルタリングします。

- 管理コンソール では、行作成率の移動平均が高すぎる場合、アプリケーション/サーバ/ネットワークの組み合わせ数が最小の低ボリューム アプリケーションをグルーミングすることによって、受信行の数を制限します。管理コンソール は、アプリケーションを *グルーミング* する場合、そのアプリケーション/サーバ/ネットワークの組み合わせの行をデータベースに作成しません。 管理コンソール は、優先アプリケーションやサーバ上で最もビジーなアプリケーションのグルーミングは行いません。

  グルーミングすることにより、管理コンソール がデータベースで最大 1 億 2000 万行を維持することが可能になると同時に、アプリケーション/サーバ/ネットワークの組み合わせが最大数の最重要アプリケーションに関するレポートを、必要な月単位の期間に作成することができます。 行作成率の移動平均が許容可能な率に戻ると、管理コンソール はグルーミングを無効にします。

  レポートの観点から、管理コンソール は、グルーミングされたアプリケーション データを「データなし」（空白）と評価します。

管理コンソール でアプリケーションのフィルタリングやグルーミングをしないようにする場合は、アプリケーションに優先順位 (P. 123) を付けます。

- グルーミングしても行作成率の移動平均が正常に低下しない場合、管理コンソール はパケット ボリュームが最小の非優先アプリケーションの組み合わせの行を作成しません。行作成率の移動平均が許容可能な率に戻ると、管理コンソール は非優先アプリケーションの通常の監視を再開します。

  レポートの観点から、組み合わせがフィルタリングされた場合には、フィルタリングされた 5 分間隔のセッション レベル統計情報を 管理コンソール がレポートすることはありませんが、ネットワーク全域でのアプリケーションのレスポンス時間メトリックは引き続き有効です。

  管理コンソール でアプリケーションのフィルタリングやグルーミングをしないようにする場合は、アプリケーションに優先順位 (P. 123) を付けます。

監視デバイスの比率

監視デバイス 比率は、環境および 管理コンソール で監視する対象の設定に応じて異なります。 特に、クライアント ネットワークの数は、生成されるデータの量に重大な影響を及ぼす傾向があります。

管理コンソール を評価している場合には、その評価による日単位のデータベース増加率 (P. 263)を使用して、本稼働の日単位データベース行の増加を予測します。

平均的には、デフォルトのデータ保持設定の場合、管理コンソール は 1 日あたり最大 400 万行を作成できます。条件によっては、特にクライアント ネットワークの数が大きい場合、CA Multi-Port Monitor は 1 日あたり 400 万行を生成することがあります。 日単位のデータベース行増加率がしきい値を超過する場合、管理コンソール は自動的にデータベースのサイズを管理します。

管理コンソール に 監視デバイス を追加したことよって生じる処理負荷は、*監視単位*で表現されます。 たとえば、CA Standard Monitor は 1 つの監視単位を利用します。管理コンソール は最大 15 の監視単位をサポートします。

以下の一覧は、監視デバイス の各タイプに対して等価な処理負荷を監視単位で示しています。

監視デバイス	監視単位
CA Multi-Port Monitor	5
CA Standard Monitor	1
CA Virtual Systems Monitor	0.5 （ESX ホスト上の層間のトラフィック）
CA GigaStor	SPAN の 1 Gbps あたり 1 監視単位
Cisco WAE （50,000 までの最適化された接続）	1
Cisco NAM-2 ブレード（最大 1 Gbps）	1
Cisco NAM 2204 アプライアンス（最大 2 Gbps）	2
Cisco NAM 2220 アプライアンス（最大 5 Gbps）	5

日単位のデータベース増加に関する情報なしでも、管理コンソール が以下のいずれかの 監視デバイス 設定をサポートできると推測できます。

- ESX ホスト上のサーバ間トラフィックを監視する CA Virtual Systems Monitor 監視デバイス 30 台
- CA Multi-Port Monitor アプライアンス 3 台
- Cisco NAM-2 ブレード 10 台および CA Multi-Port Monitor 1 台
- CA GigaStor アプライアンス 5 台

監視デバイスに関する推奨事項

管理コンソール データベース リソースを最適化するには、以下のガイドラインに従います。

- 可能な限り、CA Virtual Systems Monitor を使用した仮想スイッチからではなく、物理的な 監視 を使用した物理スイッチから監視します。 たとえば、Web サーバ層を持つ ESX ホスト上の CA Virtual Systems Monitor ではなく、物理的なディストリビューション層スイッチからクライアント/サーバのトラフィックを監視します。

  物理スイッチは、最適な SPAN/VACL 機能を持ち、その機能の実行時にパフォーマンス ロスが生じることがありません。 CA Virtual Systems Monitor は、ESX ホスト上のゲストであり、そのためのシステム リソースを消費します。 また、Web 層は、クライアント ネットワークを処理するため、監視が最も困難な層です。 物理領域に優れた選択肢がある場合は、ESX のパフォーマンスに影響しない方法を選択してください。

- 物理 監視 を使用して物理スイッチから監視する場合は、可能な限りサーバに接近して監視します。監視デバイス がサーバに接近している場合、サーバ メトリックの精度が向上するため、管理コンソール はネットワークとサーバのインシデントを明確に区別できます。

- CA Multi-Port Monitor がある場合は、ハードウェアベースのフィルタリングを使用して 監視 上で SPAN 集約を活用することにより、効率を大幅に向上できます。

  また、ミラーリングされたスイッチ ポートと 監視 の間にマトリクス スイッチを配置する方法もあります。 この投資は、大規模な環境で大きなリターンを得ることができます。マトリクス スイッチまたはネットワーク ツール オプティマイザを使用して、不要なトラフィックを回線速度でフィルタリングし、精巧に構成されたパケット ストリームを CA Multi-Port Monitor または CA Standard Monitor の各ポートに送信します。 この方法には、以下のような利点があります。

  - スイッチ管理者と協調して変更ウィンドウ中に物理スイッチを設定するのではなく、マトリクス スイッチからデータを頻繁に調節することができます。
  - 回線速度でハードウェアベースのフィルタリングを実行しても、システム CPU やメモリに影響しません。
  - CA Standard Monitor や CA Virtual Systems Monitor で利用可能なソフトウェアベースのフィルタリングでは、大きな CPU 処理能力が必要とされ、監視 スループットが低下します。

- イニシャル コストおよび総所有コストの両面で低コストです。
- 効率が高いため、多くの場合、ディストリビューション層のみならず、アクセス層での（サーバに接近した）収集が可能になります。

- 規模に関するガイダンスは一般的な内容です。すべての環境で異なります。 経験則は有用ですが、実際の容量は、アプリケーション トラフィックの性質と設定に応じて異なります。

  管理コンソール には、監視するアプリケーション、サーバ、CPU、クライアント ネットワークの数に関する制限はありません。 管理コンソール 管理者は、それぞれの特定環境における固有の特性によって決定される最大容量に対して 管理コンソール および 監視デバイス を自由に使用できます。

- 以下の項目を慎重に定義することによって、管理コンソール が監視を試みる内容を限定します。
  - アプリケーション ポート除外
  - サーバ サブネット
  - クライアント ネットワーク
- バックアップ アプリケーションなど、重要度の低いアプリケーションを削除します。
- 24 ビット クライアント ネットワークを、より広範囲のサブネット（/22 ネットワークなど）に集約します。 この方法の場合、パフォーマンス低下の影響を受ける TCP クライアントを 管理コンソール が判別する機能が限定されますが、データベースに作成される行数が減少します。

詳細:

クライアント ネットワークの仕組み (P. 34)
システム定義のアプリケーションの削除 (P. 135)
ユーザ定義アプリケーションの削除 (P. 155)
ポート除外の仕組み (P. 126)
サーバの仕組み (P. 79)

基本操作の実行

青い歯車型メニュー（ ）を使用して、リスト内の 監視デバイス のすべての基本操作を実行できます。 内容は以下のとおりです。

- ［ADA 監視デバイス リスト］には、CA Standard Monitor、CA Virtual Systems Monitor、および CA Multi-Port Monitor が含まれます。
- ［WAN 最適化デバイス リスト］には、Cisco WAE デバイスが含まれます。
- ［CA GigaStor デバイス リスト］には、CA GigaStor アプライアンスが含まれます。

Cisco NAM 上で実行する基本操作はありません。

監視デバイス インシデントの管理

監視デバイス の正常動作を保証できるように、監視デバイス インシデントを管理します。 デフォルトでは、管理コンソール は以下の場合に 監視デバイス インシデントをオープンします。

- 管理コンソール が 監視デバイス からのデータを 15 分間受信しない。たとえば、Cisco WAE が CA Multi-Port Monitor に割り当てられており、Cisco WAE がレスポンス時間データの生成を停止した場合、15 分後に管理コンソール が Cisco WAE に関する 監視デバイス インシデントを作成します。CA Multi-Port Monitor がその論理ポートの少なくとも 1 つに関するレスポンス時間データの処理を続行している場合、管理コンソール は CA Multi-Port Monitor に関する 監視デバイス インシデントを作成しません。
- CA Standard Monitor または CA GigaStor が受信パケットの 5 パーセント以下しか処理できない。
- 管理コンソール が CA Standard Monitor または CA Multi-Port Monitor と 5 分間通信できない。

監視デバイス の所有者にインシデントを通知するには、インシデント レスポンスを 監視デバイス に割り当てます。

監視デバイス インシデントをトリガした条件が存在しなくなると、管理コンソール は自動的に 監視デバイス インシデントを閉じます。 したがって、監視デバイス インシデントに確認応答する必要はありません。

CA Multi-Port Monitor では、ある程度の自己監視を実行し、SNMP トラップ通知を送信することにより、パフォーマンスに影響する可能性のある状態をアラートで通知することができます。

詳細:

監視デバイス インシデント レスポンスの割り当て (P. 316)

監視デバイス インシデントの表示

監視デバイス インシデントのサマリを表示し、特定のインシデントに関するレポートの詳細を表示するには、［監視デバイス インシデント］リストを使用します。リストをフィルタリングして、必要なインシデント ステータスおよび 監視デバイス を選択することができます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［コンソール］、［監視デバイス インシデント］をクリックします。
3. ［監視デバイス インシデント］リストでインシデントの履歴を確認します。

   インシデント ステータスについては、［ヘルプ］をクリックしてください。
4. 以下のオプションを選択して、必要なインシデントのリストをフィルタリングします。

   デバイス

   リストから 監視デバイス を選択します。各 CA Standard Monitor のインシデントをすべて表示する場合は、デフォルト（［すべて］）を使用します。

   インシデントの状態

   ［オープン］、［クローズ］、または［オープンおよびクローズ］から、必要なインシデントの状態を選択します。

   最小の重大度

   インシデントのリストをフィルタする場合は、［メジャー］または［使用不可］を選択します。 他のしきい値と異なり、監視デバイス インシデントのしきい値には「メジャー」または「使用不可」の重大度があります。
5. インシデント レポートの詳細を表示するには、［インシデント発生日］の列のタイム スタンプ エントリをクリックします。

詳細:

監視デバイス インシデントのしきい値の編集 (P. 307)
可用性監視の有効化と無効化 (P. 309)

監視デバイス インシデントのしきい値の編集

すべての 監視デバイス が確実に 管理コンソール にデータを送信するように、監視デバイス インシデントのしきい値を設定します。 監視デバイス のタイプに応じて、ドロップされたパケットやフラグメント化されたパケットに関する追加のしきい値を設定できます。

監視デバイス の可用性に関するインシデントのしきい値は調節できません。

以下の 監視デバイス のしきい値を指定します。

- データ非アクティブ状態。 管理コンソール ですべてのタイプの 監視デバイス からのデータ受信が停止すると、管理コンソール は「メジャー」（オレンジ）の 監視デバイス インシデントを作成します。

  管理コンソール では、監視デバイス からのパフォーマンス データの受信が停止すると、監視デバイス は*非アクティブ*であると見なします。これは、以下のような場合が考えられます。

  - ネットワークがダウンしている： データが生成されていない。
  - 監視デバイス がダウンしている： データは生成されているが、監視デバイス がアクティブでない。
  - SPAN が失われている： データは生成されているが、SPAN がアクティブでない。

- 監視 によってドロップされたパケット。 CA Standard Monitor または CA GigaStor がビジーなために受信パケットのすべては処理することができず、パケット キャプチャ ドライバがドロップするパケットが多すぎる場合、管理コンソール は「メジャー」（オレンジ）の 監視デバイス インシデントを作成します。 管理コンソール は、監視 上のスイッチ ポートや監視 NIC でのパケット ロスの監視を行いません。このしきい値は、CA Standard Monitor または CA GigaStor のみに適用されます。

  CA Standard Monitor または CA GigaStor が継続的にパケットをドロップする場合には、ドロップされたパケットのトラブルシューティング (P. 362)を実施してください。

- フラグメント化されたパケット。 CA Standard Monitor または CA GigaStor がフラグメント化されたパケットを受信する場合、管理コンソール は「メジャー」（オレンジ）の 監視デバイス インシデントを作成します。 デフォルトでは、このしきい値は無効になっています。このしきい値は、CA Standard Monitor または CA GigaStor のみに適用されます。

フラグメント化されたパケットが継続的に発生する場合には、以下のいずれかの条件が存在する可能性があります。

- 悪意のある攻撃がネットワーク上で発生した。
- ルータまたはサーバなど、ネットワーク上のデバイスに不適当な MTU （Maximum Transmission Unit）が設定されている。 フラグメンテーションを防止するには、ネットワーク全域で一貫した MTU 設定が適用されていることを確認してください。 MTU サイズが大きすぎる場合、そのサイズを処理できないルータにパケットが遭遇すると、再伝送が発生する可能性があります。 MTU サイズが小さすぎる場合は、ヘッダのオーバーヘッドおよび送信、処理の必要な確認応答の数が増加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［パフォーマンスしきい値］をクリックします。

   ［監視デバイスしきい値リスト］が表示されます。
3. をクリックして、監視デバイス のしきい値を編集し、［OK］をクリックします。

   ［監視デバイスしきい値］が表示されます。

   監視デバイス のインシデントしきい値の設定については、［ヘルプ］をクリックしてください。

可用性監視の有効化と無効化

デフォルトでは、管理コンソール が CA Standard Monitor、CA Virtual Systems Monitor、または CA Multi-Port Monitor と 5 分間通信できない場合、管理コンソール は「使用不可」のインシデントをオープンします。管理コンソール が 監視デバイス で 「使用不可」の 監視デバイス インシデントをオープンしないようにするには、デバイスの可用性監視を無効にします。

可用性監視は、他のタイプの 監視デバイス には適用されません。 可用性に対して 監視デバイス のしきい値を指定することはできません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして CA Standard Monitor または CA Multi-Port Monitor を編集します。

   ［監視のプロパティ］が表示されます。
4. ［可用性監視］をクリックして可用性の監視を有効にし、［OK］をクリックします。

監視デバイスへのインシデント レスポンスの追加

管理コンソール が 監視デバイス インシデントに対応して通知を起動できるようにするには、インシデント レスポンスを追加します。 アプリケーション、サーバ、ネットワークに関するインシデント レスポンスと異なり、監視デバイス インシデント レスポンスは重大度（「メジャー」または「使用不可」）によってフィルタリングできますが、期間でフィルタリングすることはできません。

デフォルトでは、管理コンソール は 監視デバイス インシデントに対応した通知を起動しません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。
3. ［表示項目］メニューの下の［監視デバイス レスポンスの追加］をクリックします。

   ［監視デバイス インシデント レスポンスのプロパティ］が表示されます。
4. インシデント レスポンス名を入力し、［適用］をクリックします。
5. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。
6. ［表示項目］メニュー下の［アクションの追加］をクリックします。

   ［監視デバイス アクション タイプ］が表示されます。
7. アクションをクリックし、［次へ］をクリックします。

   ［監視デバイス アクションのプロパティ］が表示されます。
8. ［監視デバイス アクションのプロパティ］のフィールドの入力が完了したら、［OK］をクリックします。

   監視デバイス のアクション プロパティの設定については、［ヘルプ］をクリックしてください。

   変更は、そのインシデント レスポンスが割り当てられた 監視デバイス に自動的に適用されます。

詳細:

監視デバイス インシデント レスポンスへのアクションの追加 (P. 313)

監視デバイス インシデント レスポンス名の編集

名前を変更する 監視デバイス インシデント レスポンスを編集します。監視デバイス インシデント レスポンス名の変更は、そのインシデント レスポンスが割り当てられたすべての 監視デバイス に適用されます。

監視デバイス インシデント レスポンスの編集時に、その応答アクションの変更（アクションの編集や追加など）を行うこともできます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。

   ［監視デバイス インシデント レスポンス］が表示されます。
3. をクリックして、監視デバイス インシデント レスポンスを編集します。

   少なくとも 1 つの応答アクションが各インシデント レスポンスに割り当てられており、インシデント レスポンスが各 監視デバイス に割り当てられていることを確認します。
4. 3 番目の［表示項目］メニューの［インシデント レスポンスの編集］をクリックします。

   ［インシデント レスポンス名］が表示されます。
5. インシデント レスポンス名を入力し、［OK］をクリックします。

詳細:

監視デバイス インシデント レスポンスへのアクションの追加 (P. 313)
応答アクションの削除 (P. 315)
応答アクションの編集 (P. 314)

監視デバイス インシデント レスポンスの削除

インシデント レスポンスの削除により、インシデント レスポンスおよびその応答アクションが削除されます。 インシデント レスポンスが割り当てられると、管理コンソール はデフォルトのインシデント レスポンスを、影響を受けたアプリケーション、サーバまたはネットワークに再割り当てします。

インシデント レスポンスを削除する前に、デフォルトのインシデント レスポンスが正しくセットアップされていることを確認するか、影響を受けるアプリケーション、サーバ、ネットワークに新しいインシデント レスポンスを割り当ててください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。

   ［監視デバイス リスト］が表示されます。
3.  をクリックして、監視デバイス インシデント レスポンスを削除します。 ただし、ネットワーク、サーバ、アプリケーションのデフォルトのインシデント レスポンスは削除できません。

   管理コンソール は、監視デバイス をデフォルトのインシデント レスポンスに戻します。

監視デバイス インシデント レスポンスへのアクションの追加

監視デバイス インシデントに対応して 管理コンソール が 1 つまたは複数の通知や調査を起動できるようにするには、インシデント レスポンスにアクションを追加します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。

   ［監視デバイス インシデント レスポンス］が表示されます。
3. をクリックして、インシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。
5. ［表示項目］メニュー下の［アクションの追加］をクリックします。

   ［アクション タイプ］が表示されます。
6. アクションを選択し、［次へ］をクリックします。

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

   アクション プロパティの設定については、［ヘルプ］をクリックしてください。

   ［インシデント レスポンス アクション］に新しいアクションが表示されます。

応答アクションの編集

監視デバイス インシデントに対するレスポンスを変更するには、応答アクションを編集します。 デフォルトでは、管理コンソール は 監視デバイス インシデントに対応した通知や調査を起動しません。

デフォルトのインシデント レスポンスを編集して、1 つまたは複数の応答アクションを追加し、必要に応じて追加のインシデント レスポンスを作成します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。

   ［インシデント レスポンス］が表示されます。
3. をクリックして、監視デバイス インシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。

   ［インシデント レスポンス アクション］が表示されます。
5. をクリックして、アクションを編集します。

   ［アクションのプロパティ］が表示されます。
6. 応答アクションの設定を編集し、［OK］をクリックします。 詳細については、［ヘルプ］をクリックしてください。

応答アクションの削除

管理コンソール で特定の応答アクションを起動する必要がなくなった場合は、その 監視デバイス インシデント レスポンスからアクションを削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［ポリシー］、［インシデント レスポンス］をクリックします。

   ［インシデント レスポンス］が表示されます。
3. をクリックして、監視デバイス インシデント レスポンスを編集します。
4. 3 番目の［表示項目］メニューで［アクションの編集］をクリックします。

   ［インシデント レスポンス アクション］が表示されます。
5. をクリックして、アクションを削除します。
6. ［削除の確認］で［削除を続行］をクリックすると、応答アクションが削除されます。

詳細:

監視デバイスへのインシデント レスポンスの追加 (P. 310)

監視デバイス インシデント レスポンスの割り当て

管理コンソール は、監視デバイス インシデントに対応して以下の送信ができます。

- 電子メール通知
- SNMP トラップ通知

必要な応答アクションのインシデント レスポンスを作成するか、デフォルトの 監視デバイス インシデント レスポンスにアクションを割り当てます。 デフォルトのインシデント レスポンスには、アクションは含まれていません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

   監視デバイスのリストが表示されます。
3. 監視デバイスのリストを参照し、 をクリックして 監視デバイス を編集します。

   ［監視のプロパティ］が表示されます。
4. ［インシデント レスポンス］をクリックしてリストからインシデント レスポンスを選択し、［OK］をクリックします。

監視のトラブルシュート

このセクションでは、TCP トラフィック監視する際に発生する可能性のある一般的な問題と、それらの問題の修正手順について説明します。

詳細:

監視デバイスの動作 (P. 287)

監視デバイス ステータスの表示

CA Standard Monitor、CA Virtual Systems Monitor、および CA Multi-Port Monitor は、受信した 管理コンソール のレスポンス時間データを処理します。 CA Standard Monitor、CA Virtual Systems Monitor、または CA Multi-Port Monitor のステータスを表示したり、最近 監視 がその 監視フィードからの受信データを処理したことを確認するには、［ADA 監視デバイス リスト］を使用します。

監視 に「実行中」のステータスがない場合には、監視 および割り当て済みの 監視デバイス（CA GigaStor など）のトラブルシュートを開始します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

   ［ADA 監視デバイス リスト］が表示されます。
3. 監視 のステータスを判別するには、［ステータス］列を使用します。

   実行中

   監視 はその 監視フィード のどれからもパフォーマンス データを受信します。

   停止

   管理コンソール が現在 監視 からパフォーマンス データを受信していないが、監視 の IP アドレスに接続できることを示します。

   接続できません

   管理コンソール が 監視 の管理 IP アドレスに接続できないことを示します。

   接続されていません

   管理コンソール が 監視 に接続されておらず、管理コンソール 上で現在定義されているクライアント ネットワーク、サーバ サブネットおよびアプリケーションに基づくパフォーマンス データを収集するために 監視 を同期する必要があることを示します。必要であれば、［コンソールの設定］コマンドを使用し、管理コンソール と通信する 監視 を更新します。

   停止 - データなし

パケット監視が無効で、Cisco WAE デバイス、Cisco NAM デバイス、または CA GigaStor から 監視 が要約ファイルを受信していないことを示します。

4. 監視 がその 監視フィード からの受信データを過去の 5 分内に処理したことを確認するには、［最終監視］列を使用します。
5. ステータス情報を即座に更新するには、青い歯車型メニュー（ ）をクリックし、［ステータスの更新］をクリックします。

詳細:

監視デバイス操作 (P. 339)

通信問題のトラブルシューティング

アプリケーションのレスポンス時間についてレポートするには、ADA マネージャとその監視デバイスが互いに通信できることが必要です。

検証	通信が必要な対象
ADA Manager	■ TCP-3308 上のローカルの mySQL データベース ■ TCP-1000、TCP-1001、TCP-7878 上の Standard Monitor または Virtual Systems Monitor ■ TCP-80 および TCP-8080 上の Multi-Port Monitor ■ TCP-8381 上の SSO
Standard Monitor または Virtual Systems Monitor	■ TCP-80 および TCP-8080 上の ADA マネージャ
Multi-Port Monitor	■ TCP-80 および TCP-8080 上の ADA マネージャ
Cisco NAM 上の Cisco NAM Metric Agent	■ TCP-9996 上の ADA マネージャ
Cisco WAE デバイス上の Cisco WAAS Flow Agent	■ TCP-7878 上の Standard Monitor ■ TCP-7878 上の Multi-Port Monitor ■ TCP-7878 上の ADA マネージャ

検証	通信が必要な対象
GigaStor 上の GigaStor Connector	■ UDP-9995 上の Standard Monitor ■ UDP-9995 上の Multi-Port Monitor ■ TCP-1001 上の ADA マネージャ

データ欠落のトラブルシューティング

管理コンソール がアプリケーション、サーバ、またはネットワークをレポートしない場合は、コンソールがアプリケーションやサーバの TCP セッションを参照していることを確認 (P. 292)します。

このソールが TCP セッションを参照していない場合には、以下の確認を行います。

- ポート除外によってアプリケーション データがフィルタ除去されていないこと。 詳細については、「アプリケーション ポート除外 (P. 125)」を参照してください。
- アプリケーション トラフィックをホストする少なくとも 1 台のサーバでサーバ サブネットが定義 (P. 84) されていること。
- アプリケーションと通信するクライアント IP でクライアント ネットワークが定義 (P. 44) されていること。
- 監視デバイス が 管理コンソール 上で定義されたアプリケーション、サーバ、およびネットワークを監視するように同期 (P. 290) されていること。
- ドメインを実装している場合は、監視デバイス、サーバ、およびクライアント ネットワークに正しいドメインが割り当てられていることを確認します。

第 13 章: CA Standard Monitor による監視

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 Standard Monitor が監視デバイスとして動作する仕組み (P. 321)
XFF 翻訳のサポート (P. 328)
CA Standard Monitor の追加 (P. 331)
NAT ファイアウォール通信 (P. 334)
パケット キャプチャ調査ファイルの保護 (P. 335)
CA Standard Monitor の編集 (P. 336)
パケット監視フィードの編集 (P. 337)
監視デバイスのパフォーマンスの管理 (P. 338)
監視デバイス操作 (P. 339)
キープアライブ メッセージのフィルタ除外 (P. 341)
CA Standard Monitor の削除 (P. 344)
パケット監視フィードの無効化 (P. 345)
CA Standard Monitor のトラブルシューティング (P. 346)

CA Standard Monitor が監視デバイスとして動作する仕組み

CA Standard Monitor は、CA Application Delivery Analysis の 監視デバイス の一種として機能します。 CA Standard Monitor は、最大 2 つのポートからのデータ センター トラフィックをパッシブに監視し、エンド ツー エンドのシステム パフォーマンスを継続的に記録するのに役立ちます。 CA Standard Monitor は、管理コンソール と同じサーバ上に配置されるため、管理コンソール は 監視 を認識しています。 追加の 監視デバイス を展開して、ミラーリングされた TCP トラフィックをサーバ スイッチ ポートから受動的に監視することができます。 また、CA Standard Monitor は、CA GigaStor など､別のタイプの 監視デバイス のレスポンス時間メトリックを計算します。

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

CA Standard Monitor の動作

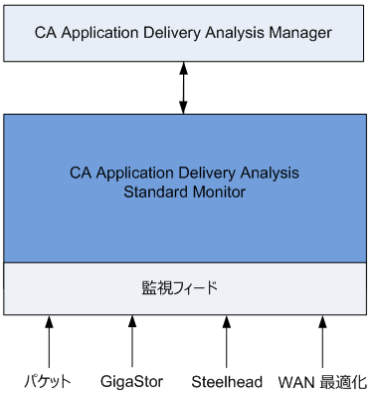
下図に示すように、CA Standard Monitor は、以下のような各種のソースからパフォーマンス データを受信し処理することができます。

- パケット 監視フィード。SPAN やミラー ポートまたはネットワーク タップから IPv4 ベースの TCP パケットを監視 NIC 上で受信し、CA Standard Monitor でデータを処理した後、レポートでの表示用にレスポンス時間統計情報を計算して 管理コンソール に送信します。 最適な結果を得るためには、ホスト スイッチからのローカル SPAN が推奨されます。
- GigaStor 監視フィード。CA GigaStor からのパケット要約ファイルを管理 NIC 上で受信し、IPv4 ベースの TCP ヘッダ情報を処理した後、レポートでの表示用にレスポンス時間統計情報を 管理コンソール に送信します。
- Steelhead 監視フィード （Steelhead アプライアンスから IPv4 Steelhead で最適化されたパケットを受信）。
- WAN 最適化 監視フィード（IPv4 Cisco WAE デバイスからパケット要約ファイルを受信）。

監視 は、指定のアプリケーション ポート、サーバ、およびクライアント ネットワークのリストに基づいて、観測対象のすべての該当サーバ-アプリケーション-ネットワーク トラフィックに関するレスポンス時間統計を作成します。 管理コンソール は、この情報を使用して、各サーバ上の最もビジーな TCP アプリケーションを自動的に監視します。また、監視するアプリケーションを定義した後、この設定を CA Standard Monitor にロードすることもできます。

管理コンソール は、すべての 監視デバイス からのレスポンス時間メトリックを評価することにより、最適な 監視フィード を各サーバに割り当て、各サーバで最もビジーな TCP アプリケーションを監視します。

CA GigaStor からパケット要約を受信するように CA Standard Monitor を設定する場合、ミラーリングされたパケットも同時に受信するように 監視 を設定しないことをお勧めします。



スタンドアロン 管理コンソール は、その パケット 監視フィード 上でミラーリングされた TCP パケットを受信します。

詳細:

アプリケーションの管理 (P. 121)
監視フィード割り当ての仕組み (P. 325)

必要なサービス

CA Standard Monitor は、以下にリスト表示されたサービスを自動的に開始します。

警告： データの損失を回避するために、これらのサービスを手動で停止または再起動しないでください。 支援情報については、CA サポート（**エラー! ハイパーリンクの参照に誤りがあります。**）までお問い合わせください。

- CA ADA Monitor Management。監視 から 管理コンソール に .dat ファイルを転送するという 管理コンソール からのリクエストに応答します。
- CA ADA Data Transfer Manager。 CA Standard Monitor 上で定義されたアプリケーション、サーバ、および クライアント ネットワークに基づいて、監視を Cisco WAE デバイスに同期させます。
- CA ADA Inspector Agent。 アプリケーションをホストするサーバが CA Standard Monitor によって監視される場合、監視 上の CA ADA Inspector Agent サービスがアプリケーション、サーバおよび関連するネットワーク上で調査を開始します。それ以外の場合は、管理コンソール 上の CA ADA Inspector Agent サービスが調査を開始します。
- CA ADA Messenger サービス。 CA Standard Monitor 上で定義されたアプリケーション、サーバ、およびクライアント ネットワークに監視を同期させます。
- CA ADA Monitor。 このサービスは、管理コンソール または CA Standard Monitor に配置され、ミラーリングされた TCP パケットおよび要約ファイルを、CA GigaStor などの割り当てられた 監視デバイス から受信します。
- CA ADA Batch。 CA Standard Monitor 上の Stages .dat データ ファイルであり、管理コンソール 上で CA ADA Master Batch サービスによって処理されます。

監視フィードの動作

*監視フィード*は、レスポンス時間データのソースです。たとえば以下のようなものです。

- パケット 監視フィード は、ミラーリングされた TCP パケットを監視 NIC 上で受信します。
- Riverbed WAN 監視フィード は WAN の最適化されたパケットを Riverbed Steelhead アプライアンスから受信します。
- GigaStor 監視フィード は、CA GigaStor からのパケット要約ファイルを管理 NIC 上で受信します。
- WAN 最適化 監視フィード は、Cisco WAE デバイスから管理 NIC 上でパケット要約ファイルを受信します。

管理コンソール は、サーバ上で TCP トラフィックを監視するためのソースとしてサーバに最も接近している 監視フィード を自動的に割り当てます。

以下の操作を実行するには、監視フィード を編集します。

- 特定のドメインを割り当てる。デフォルトでは、新規の 監視フィード は「デフォルト ドメイン」に割り当てられます。 重複する IP トラフィックを分けるためにドメインを使用していない場合には、適用されません。
- 冗長データを監視するためのセカンダリ 監視フィード をペアにする。
- アクティブ セッション数を表示する。アクティブ セッション情報は、監視フィード がアクティブな TCP セッションを監視しているかどうかを確認するために役立ちます。

詳細:

テナントの管理 (P. 113)
監視フィードのペアの作成 (P. 291)

監視フィード割り当ての仕組み

CA Standard Monitor 上の 監視フィード の 1 つがサーバ上の TCP トラフィックを監視するための最適なソースである場合、管理コンソール は自動的にこの 監視フィード をサーバに割り当てます。

詳細:

監視フィード割り当ての仕組み (P. 289)

パケット キャプチャ調査の仕組み

パケット 監視フィード がサーバに割り当てられると、管理コンソール は、パケットを参照する関連の CA Standard Monitor から、そのサーバ上でパケット キャプチャ調査を実行します。

CA Standard Monitor は、CA GigaStor や CA Multi-Port Monitor と異なり、以下のように動作します。

- 管理コンソール がインシデントを作成した後、パケット キャプチャ調査を起動します。
- 一度に 1 つのパケット キャプチャ調査を実行します。
- パケット キャプチャ調査を表示するために、監視 からユーザのローカル コンピュータにパケット キャプチャ ファイルをコピーします。 パケット キャプチャ ファイルのサイズによっては、パケット キャプチャ調査を開くのに長時間を要する場合があります。
- CA Standard Monitor には、長期的なパケット保存のサポートは含まれません。

CA Standard Monitor によって作成されたパケット キャプチャ調査を 管理コンソール ユーザが開くには、ネットワーク パケット アナライザが必要です。

監視デバイスに関する考慮事項

CA Standard Monitor を 監視デバイス として使用する場合は、以下の点を考慮する必要があります。

- 通常、CA 技術担当者は、ユーザが TCP トラフィックを 監視デバイス にミラーリングするための支援をします。 TCP トラフィックのミラーリングに関する詳細については、「*Best Practices for Data Acquisition Guide*」を参照してください。
- PacketMon は、CA Standard Monitor やスタンドアロン 管理コンソール にインストールすることが認定された唯一のパケット スニファです。パケット キャプチャ ドライバとの競合を回避するため、他のパケット スニファ（*Wireshark* など）を CA Standard Monitor やスタンドアロン 管理コンソール にインストール**しない**でください。
- パケット キャプチャ調査を設定する際、CA Standard Monitor にはパケット キャプチャの長期保存のサポートが含まれない点を考慮する必要があります。 利用可能なリソースを最大限に活用するために、以下の制限を付けてパケット キャプチャを設定します。
  - 最大ファイル サイズ。
  - 1 パケットあたりのバイト数。
- パケット キャプチャの潜在的な機密内容へのアクセスを制限する必要がある場合は、CA Standard Monitor でのパケット キャプチャを無効化 (P. 335)することができます。
- CA Standard Monitor は、管理コンソール に定義されたクライアント ネットワーク、サーバ サブネット、およびポート除外に基づいて、該当するアプリケーション トラフィックを自動的に監視します。
- CA Standard Monitor は、すべてのタイプのアプリケーションを監視します。

XFF 翻訳のサポート

たとえば、ユーザがプロキシ サーバ経由で Web アプリケーションにアクセスする場合において、そのプロキシ サーバがプロキシとして機能するクライアントとは異なるサブネットにそのプロキシ サーバが属している場合、管理コンソール は、実際のクライアント ネットワークではなく、プロキシ サーバの該当クライアント ネットワークからの Web アプリケーション トラフィックを間違ってレポートします。

プロキシ サーバが XFF を使用する場合には、CA Application Delivery Analysis Manager の XFF 翻訳を有効にすることにより、Web アプリケーションの監視サポートを拡張し、プロキシ サーバの該当クライアント ネットワークからではなく実際のクライアント ネットワークからの Web アプリケーション トラフィックをレポートすることができます。

XFF 翻訳を有効にすると、各 CA Standard Monitor で新たなリソースが消費されます。デフォルトでは、CA Application Delivery Analysis Manager は XFF 翻訳を実行しません。

詳細情報:

Web アプリケーションの作成 (P. 145)
XFF 翻訳の有効化 (P. 330)

XFF 翻訳の動作

クライアントが XFF （X-Forwarded-For）を使用する HTTP プロキシ サーバ経由で Web アプリケーションに接続すると、管理コンソール は、XFF HTTP ヘッダを使用してクライアントの送信元 IP アドレスを識別します。 標準的な XFF HTTP ヘッダの形式を以下に示します。

```
TCP ソース IP： proxy3
X-Forwarded-For： client1、proxy1、proxy2
```

IP アドレスのリストには、最も遠いダウンストリーム クライアント、リクエストが通過した一連のプロキシのそれぞれ、およびそのクライアントがリクエストを受信したプロキシが含まれます。 例として、リクエストが proxy1、proxy2、proxy3 （サーバに最も近いプロキシ）を通過したとします。

XFF 翻訳を使用することで、管理コンソール は、各クライアントの Web トラフィックを、それがフィットするサブネットに属するものとして正しくレポートします。 管理コンソール では、クライアントとの間の Web アプリケーション トラフィックの適切なボリュームの参照を開始できます。 また、プロキシ サーバ上の少量のトラフィックを参照することもできます。 このトラフィックは、トランザクションのトラフィックではなく、プロキシ サーバ Web サーバに送信する確認応答で構成されます。

ヒント： プロキシ サーバを、プロキシ環境における固有のネットワークとして定義する場合、Web サーバ上でのプロキシ サーバ リンクまでのパフォーマンスと、Web サーバ上でのクライアント サブネットの完全パスまでのパフォーマンスを区別することができます。 この情報は、プロキシ サーバがクライアントと同じ場所に配置されていない場合に有用です。

XFF 翻訳の有効化

XFF 翻訳を有効にするには、管理コンソール データベース上で MySQL コマンドを実行する必要があります。必要な MySQL コマンドを実行するには、以下の手順に従います。

1. Windows 管理者アカウントを使用して 管理コンソール サーバにログインします。
2. 正しいデータベース名とデータベース ポートを使用して、管理コンソール データベースにアクセスします。

   データベース名

   デフォルトの 管理コンソール データベース名は、super です。

   データベース ポート

   管理コンソール データベースのデフォルト ポートは、TCP-3308 です。

MySQL コマンドの使用に関する詳細については、www.mysql.com で提供されている MySQL ドキュメントを参照してください。

次の手順に従ってください:

1. Windows 管理者アカウントを使用して、管理コンソール コンピュータにログインします。
2. コマンド プロンプトを開きます。
3. 次のコマンドを実行して、MySQL にログインします。
   ```
   mysql -P3308
   ```
4. MySQL に次のプロンプトが表示されます。
   ```
   mysql>
   ```
5. MySQL プロンプトで次のコマンドを実行して、管理コンソール データベースに切り替えます。
   ```
   use super;
   ```
   MySQL に次の応答が表示されます。
   ```
   Database changed
   ```
6. MySQL プロンプトで次のコマンドを実行して、XFF 翻訳を有効にします。
   ```
   INSERT IGNORE INTO parameter_descriptions (Parameter, Level, Type,
   DefaultValue, Description) VALUES ('XFFEnabled', 'System',
   'boolean', '1', 'Non-zero to enable XFF endpoint extraction in URL
   monitoring.');
   ```

MySQL に次の応答が表示されます。

```
Query OK, 1 row affected (0.00 sec)
```

7. （オプション）XFF 翻訳を有効化した後に無効化する場合は、次のコマンドを実行します。

```
UPDATE parameter_descriptions SET DefaultValue='0' WHERE
parameter='XFFEnabled';
```

MySQL に次の応答が表示されます。

```
Query OK, 1 row affected (0.02 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

8. コマンドプロンプトを閉じます。
9. 変更を適用するには、監視デバイス を同期 (P. 339) します。

詳細:

Windows 管理者の認証情報 (P. 261)

CA Standard Monitor の追加

以下の情報を受信するには、CA Standard Monitor を追加します。

- SPAN スイッチ ポートからの TCP パケット
- CA GigaStor (P. 389) からのパケット要約
- Cisco WAE デバイス (P. 415) からのパケット要約

前提条件

CA Standard Monitor を追加する前に、以下の点について確認します。

- 監視デバイス比率 (P. 300)が正しくサイズ設定されていること。
- 管理コンソールは、TCP-80、TCP-1000、TCP-1001 上の CA Standard Monitor と通信できます。
- アウトバウンド UDP-161 が利用可能であること。たとえば、サーバまたはネットワーク デバイスの SNMP ポーリングに使用可能であること。
- アウトバウンド UDP-162 が利用可能であること。たとえば、SNMP トラップの送信に使用可能であること。
- アウトバウンドとインバウンの ICMP が利用可能であること。たとえば、サーバが ping リクエストに応答可能であることを確認し、ラウンドトリップ時間を測定するために使用可能であること。
- TCP-3389 上の CA Standard Monitor に Windows Terminal Services （RDP）を使用してアクセスできます。

CA Standard Monitor の追加

CA Standard Monitor を追加すると、管理コンソール によって、ユーザ指定の管理 IP アドレスを使用して 監視 との通信が試みられます。現在ネットワークで利用できない 監視 を追加する場合、管理コンソール によって即座に管理 IP アドレスがポーリングされます。この後、残りの 監視 プロパティの指定が可能になります。 監視 がネットワークで利用可能になったら、監視デバイス を同期 (P. 290)して、監視 と 管理コンソール の間の通信を確立してください。

TCP パケット監視を無効にすることにより、監視 上の利用可能なリソースを最適化できます。 たとえば、CA GigaStor からパケット要約ファイルを受信するための専用 監視 を追加する計画において、監視 はその監視 NIC 上で TCP トラフィックを監視する必要がない場合は、パケット監視を無効にします。

監視 を追加すると、それが［ADA 監視デバイス リスト］に表示されます。CA PC または CA NPC にドメイン (P. 113)を定義している場合、CA Standard Monitor 上の パケット 監視フィード にドメインを割り当てます。

次の手順に従ってください:

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

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

   監視デバイス プロパティの設定については、［ヘルプ］をクリックしてください。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

NAT ファイアウォール通信

CA Standard Monitor が NAT ファイアウォール後方の 管理コンソール と通信できるようにするには、LockConsoleAddress ユーティリティを使用して、監視 設定を、その割り当てられたコンソールの NAT アドレスに更新します。

この手順が必要となるのは、たとえば 管理コンソール が NAT ファイアウォール後方のプライベート ネットワーク上に配置されている場合などです。 この環境の場合、ファイアウォールの反対側にある CA Standard Monitor から、その NAT アドレス上の 管理コンソール に ping を送信することは可能ですが、管理コンソール は 監視 からのレポート データを受信しません。

このユーティリティを実行する前に、監視 を割り当てる 管理コンソール の IPv4 NAT アドレスが既知であることが必要です。

次の手順に従ってください:

1. CA Standard Monitor で、コマンド プロンプトを開きます。
2. コマンド プロンプトで、ディレクトリを <ADA_HOME>¥bin ディレクトリ（たとえば D:¥NetQoS¥bin）に変更します。
3. 以下コマンドを入力し、Enter キーを押します。
   `LockConsoleAddress <NAT_IP>`

   ここで、NAT_IP は 管理コンソール の IPv4 NAT アドレスです。ユーティリティによって、次のレジストリ キーが、指定した IPv4 NAT アドレスに更新されます。
   `HKEY_LOCAL_MACHINE¥SOFTWARE¥NetQos¥SACollector¥Parameters¥NAT_MasterDB`
4. （オプション） 監視 が 管理コンソール との通信に使用する IPv4 NAT アドレスを確認するには、次のコマンドを入力し、Enter キーを押します。
   `LockConsoleAddress`

   結果には、NAT ファイアウォール後方に配置されたコンソールの現在の IP アドレスが示されます。
5. （オプション） 監視 から 管理コンソール の NAT アドレスを削除するには、次のコマンドを入力し、Enter キーを押します。
   `LockConsoleAddress -d`

   ユーティリティによって、次のレジストリ キーが更新され、IPv4 NAT アドレスが削除されます。

HKEY_LOCAL_MACHINE¥SOFTWARE¥NetQos¥SACollector¥Parameters¥NAT_MasterDB

パケット キャプチャ調査ファイルの保護

CA Standard Monitor は、そのパケット キャプチャ調査ファイルを、暗号化されていない形式で保存します。 デフォルトでは、パケット キャプチャ調査でヘッダ情報のみが収集されるため、暗号化の必要性が大幅に小さくなります。

パケット キャプチャ調査ファイルのセキュリティを高めるには、以下の方法があります。

- ヘッダ情報のみをキャプチャするようにパケット キャプチャ調査を設定する。
- 監視 上のパケット キャプチャ調査を無効にする。ただし、CA Standard Monitor をアップグレードすると、パケット キャプチャ調査が有効になります。 アップグレードした後は、手動で 監視 設定を変更してパケット キャプチャを無効にする必要があります。

パケット キャプチャ調査の有効化を選択する場合は、パケット キャプチャ調査の作成および表示を行える人物を制限するルール (P. 254)を設定する必要があります。

次の手順に従ってください:

1. CA Standard Monitor で、Windows エクスプローラを開き、<ADA_HOME>¥SuperAgent¥dotnet¥InspectorAgent に移動します。
2. InspectorAgent.exe.config ファイルで、次のエントリをコメント解除します。
   <add key="Capture.CaptureTcp" value="disable" />
3. 監視 上の NetQoS Inspector Agent サービスを再起動して、変更を適用します。
4. 監視 上の既存のパケット キャプチャ調査ファイルを手動で削除するには、<ADA_HOME>¥SuperAgent¥Web¥batch¥snifferfiles に移動し、既存のパケット キャプチャ調査 (.enc) ファイルを削除します。データベースの保守の一環として 5 分データがパージされる際には、その 5 分データに結び付けられたパケット キャプチャ調査ファイルも自動的にパージされる点に注意が必要です。

CA Standard Monitor の編集

CA Standard Monitor のプロパティを編集して、以下を実行できます。

- インシデント レスポンスを割り当てる。または可用性監視を有効にする。
- 各 監視フィード のアクティブ セッション数情報を表示する。
- CA Standard Monitor の 監視デバイス インシデントを表示する。
- CA Standard Monitor 上の任意の 監視フィード のプロパティを編集する。
- 監視デバイス の同期、監視 の停止と開始、再起動、シャットダウンなど、CA Standard Monitor 上で基本的な操作を実行する。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして CA Standard Monitor を編集します。

   ［Standard Monitor のプロパティ］が表示されます。

   注: Standard Monitor タイプには、CA Standard Monitor および CA Virtual Systems Monitor の両方が含まれます。監視 が仮想マシン上で実行されているかどうかが不明な場合は、その IP アドレスを確認します。
4. ［Standard Monitor のプロパティ］のフィールドの入力が完了したら、［OK］をクリックします。

   監視デバイス プロパティの設定については、［ヘルプ］をクリックしてください。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

パケット監視フィードの編集

パケット監視フィードは、CA Standard Monitor 上の監視 NIC からミラーリングされた TCP パケットを受信します。 以下の操作を実行するには、パケット 監視フィードを編集します。

- 監視フィードのデフォルト名を変更する。
- 特定のドメインを割り当てる。デフォルトでは、新規の 監視フィードは「デフォルト ドメイン」に割り当てられます。 重複する IP トラフィックを分けるためにドメインを使用していない場合には、適用されません。
- 監視フィードのペアを作成 (P. 291)して、管理コンソール が両方の 監視フィードから割り当て済みサーバのデータを自動的に収集できるようにする。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

   ［ADA 監視デバイス リスト］が表示されます。
3. をクリックして、CA Standard Monitor のアクティブ パケット 監視フィードを編集します。

   ［Standard Monitor のプロパティ］が表示されます。

   注: Standard Monitor タイプには、CA Standard Monitor および CA Virtual Systems Monitor の両方が含まれます。必要に応じて、監視 IP アドレスを確認します。
4. ［監視フィード］の下の をクリックして、パケット 監視フィードを編集します。
5. パケット 監視フィードのプロパティを編集して、セカンダリ フィードまたはドメインを割り当てます。
6. ［更新］をクリックします。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細情報:

テナントの管理 (P. 113)
監視デバイスの動作 (P. 287)

監視デバイスのパフォーマンスの管理

CA Standard Monitor が以下の状態になると、管理コンソール は自動的にメジャー 監視デバイス インシデントを作成します。

- 1 時間を超えて 管理コンソール へのデータ送信を停止している
- 受信パケットの 5 パーセント以下しか処理していない

詳細:

監視デバイス インシデントのしきい値の編集 (P. 307)

監視デバイス操作

管理コンソール 上に現在定義されているクライアント ネットワーク、サーバ サブネット、およびアプリケーションに基づいてパフォーマンス データを収集するには、一部またはすべての 監視デバイス 上で、監視デバイス を同期するなどの基本操作を実行します。 基本操作を実行するには、［ADA 監視デバイス リスト］で、青い歯車型メニュー（ ）を使用します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、青い歯車型メニュー（ ）をクリックすると、リスト内の監視デバイスすべてに対して基本操作を実行できます。
4. （オプション）特定の 監視デバイス に対して基本操作を実行するには、リストを参照して編集アイコン（ ）をクリックします。 ［Standard Monitor のプロパティ］ページで、青い歯車型メニュー（ ）をクリックして、コマンドを選択します。

   開始

   ステータスが「停止」の 監視 上でデータ監視を開始します。 監視が「停止」の間、監視 はその 監視フィード からのレスポンス時間メトリックを処理しません。

   管理コンソール が 監視 と通信できない場合は、CA Standard Monitor にログオンして CA ADA Monitor サービスを開始してください。

   停止

   ステータスが「実行中」の 監視 上のデータ監視を停止します。 監視 が「停止」の間、監視 はその 監視フィード からのレスポンス時間メトリックを処理しません。

   監視デバイスを同期

   監視 上のデータ監視設定を更新し、現在定義されているクライアント ネットワーク、サーバ サブネット、およびアプリケーションに基づいてパフォーマンス データを収集します。

   リブート

CA Standard Monitor または CA Virtual Systems Monitor をリブートします。このコマンドは、CA Multi-Port Monitor には適用されません。

管理コンソール が 監視 と通信できない場合は、監視 にログオンしてリブートしてください。

シャットダウン

CA Standard Monitor または CA Virtual Systems Monitor の電力をオフにします。 CA Standard Monitor や CA Virtual Systems Monitor のシャットダウン後に電源をオンにするには、監視 から電源オンの操作を行う必要があります。このコマンドは、CA Multi-Port Monitor には適用されません。

管理コンソール が 監視 と通信できない場合は、CA Standard Monitor にログオンしてシャットダウンしてください。

詳細:

監視デバイス同期の動作 (P. 290)
基本操作の実行 (P. 304)

キープアライブ メッセージのフィルタ除外

CA Standard Monitor には、レポートでの統計情報の監視に対するアプリケーションのキープアライブ メッセージの影響を制限するオプションがあります。 このテクニックでは、選択したアプリケーションのサーバ レスポンス時間（SRT）またはデータ転送時間（DTT）を最大値に制限することで、不要な SRT や DTT の観測が無視されるようにします。 値には、キープアライブの頻度をわずかに下回る任意の秒数を設定します。

アプリケーションがキープアライブを送信していると考えられる場合、観測値と SRT の逆比例の関係を調べ、ミリ秒範囲の代わりに秒範囲内の SRT 平均を確認します。アプリケーションに対する最大 SRT を制限するために CA Standard Monitor を設定します。

非常に高いデータ転送時間（DTT）を生じるキープアライブをアプリケーションが使用していると判別される場合にも、同様の制限を適用して DTT をフィルタリングすることができます。

コンソールのビルトイン NRTT フィルタリング (P. 267)を使用して、CA Standard Monitor 上で SRT および DTT のフィルタリングを実行します。 通常、クライアントがアイドル状態の場合、アプリケーションのキープアライブによって SRT データが非対称になります。 NRTT フィルタリングは、業務時間外など、すべてのクライアントがアイドルである場合に便利です。ただし、日中は、クライアント ネットワークで 10 のアイドル接続と 30 のアクティブ接続というのも容易にありえます。 NRTT しきい値を超えることは可能ですが、その場合も、その組み合わせの中の 10 のアイドル接続によってデータが非対称になります。

選択したアプリケーションのキープアライブの頻度が不明確な場合は、安全を見越して 10 秒から開始することをお勧めします。 サーバがユーザ リクエストの応答を開始する時間が 10 秒を超えることはまずないでしょう。ほとんどの場合（必ずではありません）、キープアライブの頻度は 10 秒を超えます。

ランダムなポートを使用するアプリケーション（Microsoft Exchange 2007 など）の場合、ポートを識別する最も簡単な方法は、Outlook を使う方法です。コンピュータで Outlook を開き、netstat コマンドを実行して、Outlook が接続する動的ポートを記録します。

必要な設定は、CA Multi-Port Monitor でも利用できます。 ただし、デフォルト設定を変更するための手順は異なります。 詳細については、CA Multi-Port Monitor の製品ドキュメントを参照してください。

次の手順に従ってください:

1. Microsoft リモート デスクトップを使用して、CA Standard Monitor にアクセスします。
2. インストール ディレクトリ（例: C:¥CA¥Bin）に移動します。
3. フィルタリングするポートごとに SRT しきい値を指定します。
   a. LimitServerResponseParams.ini.sav ファイルをコピーし、LimitServerResponseParams.ini に名前を変更します。
   b. メモ帳で、この .ini ファイルを編集して、フィルタリングするポートごとに SRT しきい値を指定します。

      LimitServerResponseParms.ini テキスト ファイルには、改行で分離した複数のエントリを指定できます。 ポート番号、および許可する SRT の最大を指定することにより、各アプリケーションの SRT を制限します。SRT の最大値を、キープアライブの頻度よりわずかに小さい値に設定します。 たとえば、60 秒間隔で発生する Citrix キープアライブを無視するには、次のエントリを指定します。

      ```
      /port=1494 /max seconds=59
      ```

   c. ポート範囲をフィルタするには、以下の構文を使用します。

      ```
      /min port=<lowerPort> /max port=<higherPort> /max seconds=59
      ```

      ポートが指定されていない場合、またはポートに 0 が指定されている場合、指定された制限はすべてのポートに適用されます。ポート範囲の下限に 0 が指定されている場合も、結果は同じになります。このときポート範囲の上限の指定は関係ありません。

      ファイル内で先に出現するエントリは、後に出現するエントリよりも優先度が高くなります。 このために、ポート範囲が重複するさまざまなルールがある場合、最初により特殊なエントリをリストすることが必ず必要となります。そうしない場合、あまり特殊でないエントリによってマスクされることになります。 以下に例を示します。

      ```
      /port=23 /max seconds=15

      /min port=100 /max port=200 /max seconds=50

      /max seconds=120
      ```

      このファイルは、SRT または DTT をポート 23 に対しては 15 秒、ポート［100-200］に対しては 50 秒、および他のすべてのポートに対しては 120 秒に制限します。

   d. ファイルを保存します。

4. 必要に応じて、フィルタリングするポートごとに DTT しきい値を指定します。
   a. LimitDTTParams.ini.sav ファイルをコピーし、LimitDTTParams.ini に名前を変更します。
   b. 上述の手順に従って DTT フィルタ条件を指定します。
   c. ファイルを保存します。
5. 管理コンソール を開き、監視デバイス を同期して、変更を適用します。
   a. ［環境管理］ページをクリックします。
   b. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
   c. ［ADA 監視デバイス リスト］までスクロールし、青い歯車型メニュー（ ）をクリックして、［監視デバイスを同期］を選択します。

CA Standard Monitor の削除

CA Standard Monitor の監視デバイスを削除して、レスポンス時間データのソースとして削除するようにします。 監視デバイスを削除する場合：

- 対応する監視フィードに固定されていたすべてのサーバは固定が解除され、別の監視フィードが自動的に割り当てられます。 監視フィードの割り当てを更新するのに 10 分程度かかる可能性があります。
- 既存のデータはレポート目的のために保持されます。

監視フィードにサーバを固定していた場合、監視デバイスが一時的にオフラインである場合でもサーバ トラフィックの監視を続行するには、以下のオプションを考慮します。

- 監視デバイスをオフラインにする前に、別の監視フィードにサーバを固定します。 監視デバイスをオンラインに戻す場合、監視フィードに適切なサーバを固定します。
- 監視デバイスを削除します。 別の監視フィードが自動的に割り当てられますが、監視フィード割り当てを更新するのに 10 分程度かかる可能性があります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. をクリックし、ADA 監視デバイス リストから CA Standard Monitor を削除します。

   Standard Monitor タイプには、CA Standard Monitor と CA Virtual Systems Monitor の両方が含まれます。 必要に応じて、監視 の IP アドレスを確認します。
4. ［監視デバイス確認の削除］で、［削除を続行］をクリックして 監視デバイス を削除します。

詳細:

サーバへの監視フィードの固定 (P. 102)

パケット監視フィードの無効化

Cisco NAM、Cisco WAE、Riverbed Steelhead、CA GigaStor からの受信要約ファイルの処理に使用可能な CA Standard Monitor リソースを最適化するには、CA Standard Monitor 上のパケット監視を無効にします。パケット監視を無効にすると、パケット 監視フィード が削除されます。

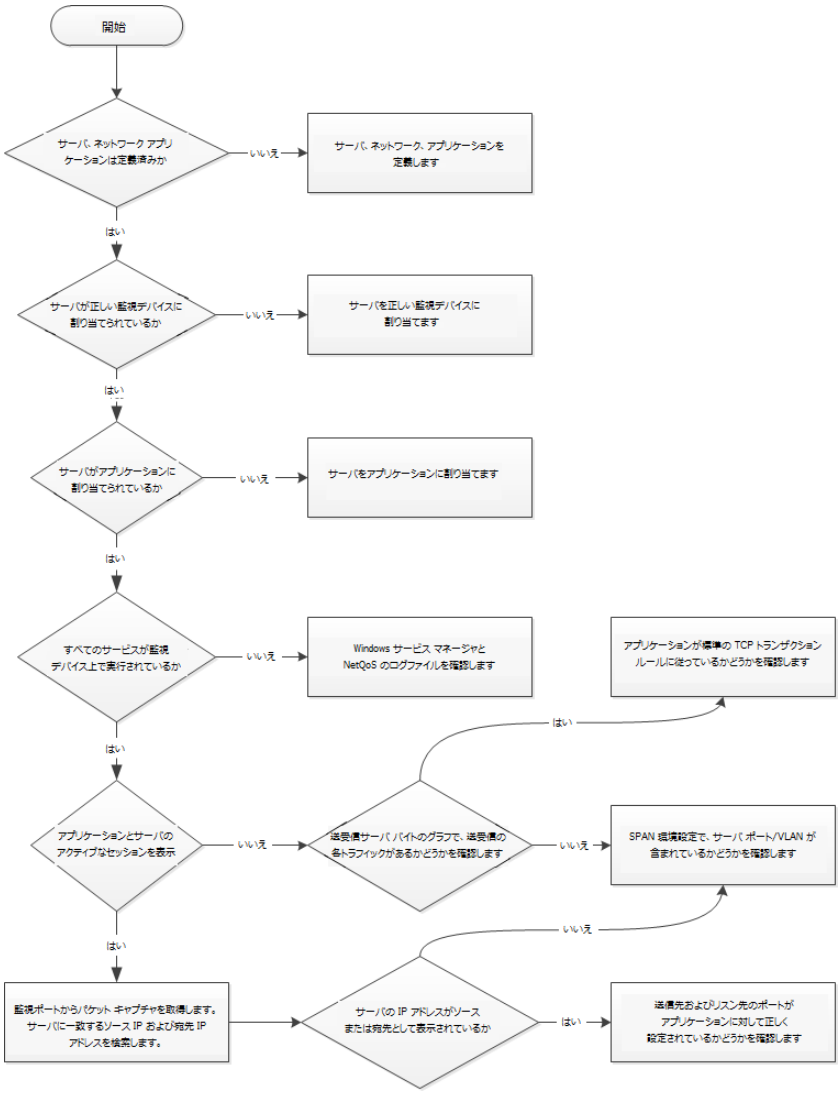
CA Standard Monitor を追加する際に、パケット監視の無効化を選択できます。 CA Standard Monitor を追加した後は、パケット監視の無効を選択できません。 必要に応じて、CA Standard Monitor を削除した後、パケット監視を無効化した CA Standard Monitor を追加してください。 CA Standard Monitor に 監視デバイス を割り当てていた場合には、CA Standard Monitor を追加した後、その再割り当てが必要です。

詳細:

CA Standard Monitor の追加 (P. 331)

CA Standard Monitor のトラブルシューティング

CA Standard Monitor によって監視される予定のレポート データが欠落している原因を特定するには、CA Standard Monitor のトラブルシュートを行います。Cisco WAE または CA GigaStor に関するデータ監視の問題をトラブルシュートしている場合には、対応する要約ファイルを CA Standard Monitor が受信し、処理していることを確認してください。



アクティブ セッション数の確認

直近の 5 分間のレポート間隔において CA Standard Monitor または CA Virtual Systems Monitor 上の各 監視フィードによってレポートされたアクティブな IPv4 ベースの TCP セッションの数をレポートするには、［アクティブ セッション数］ページを使用します。CA Virtual Systems Monitor は、パケット 監視フィード のみを受信する点に注意が必要です。

監視フィードにサーバやアプリケーションのアクティブ セッションがない場合は、以下の確認を行います。

- パケット 監視フィード が TCP トラフィックを参照していること。
- CA ADA Monitor サービスが実行中であること。

詳細:

［監視フィード］でのアクティブ セッション数の表示 (P. 293)
CA ADA Monitor サービスのトラブルシューティング (P. 353)
監視フィード統計の表示 (P. 348)

監視フィード統計の表示

CA Standard Monitor において、CA ADA Monitor サービスは、その 監視フィード のそれぞれから受信する受信データから 5 分平均を計算しています。

監視フィード カウンタを使用することで、サービスの実行内容の把握が容易になります。

パケット レシーバ

CA Standard Monitor にミラーリングされるパケット データ。

GigaStor レシーバ

CA GigaStor から受信したパケット要約ファイル。このカウンタを表示するには、CA GigaStor が CA Standard Monitor に割り当てられている必要があります。

Steelhead レシーバ

Riverbed Steelhead アプライアンスから受信したパケット要約ファイル。

WAN 最適化レシーバ

Cisco WAE デバイスから受信したパケット要約ファイル。 このカウンタを表示するには、Cisco WAE デバイスが CA Standard Monitor に割り当てられている必要があります。

重要: 開始前に、監視デバイスを同期します。 データ監視の同期が完了するまで、カウンタ ウィンドウは表示されません。

監視フィード カウンタを表示するには、CA Standard Monitor コンピュータにログオンする必要があります。

次の手順に従ってください:

1. CA Standard Monitor コンピュータにログオンするか、Microsoft Remote Desktop Connection （RDC）を使用して CA Standard Monitor コンピュータにリモートで接続します。

   リモート デスクトップを使用して Windows Server 2003 ベースのサーバに接続する場合は、/admin スイッチを使用して物理コンソール セッションに接続します。 フィード レシーバ カウンタを表示するには、物理コンソール セッションに接続する必要があります。 /admin スイッチの詳細については、Microsoft KB 947723 を参照してください。

以下はそれぞれの統計を表示する方法です。

パケット データの統計情報

ミラーリングされた TCP パケットを受信する CA Standard Monitor または 管理コンソール にログオンします。

WAN 最適化デバイスまたは CA GigaStor からのパケット要約ファイルの統計情報

パケット要約ファイルを受信する CA Standard Monitor にログオンします。

2. CA Standard Monitor をホストするオペレーティング システムのバージョンに応じて、監視フィード 統計を表示するための手順は異なります。 CA Standard Monitor が実行されている OS による違いは以下のとおりです。
   - Windows Server 2003： フィード レシーバ カウンタは自動的に表示されます。 表示されない場合は、物理コンソール セッションへの接続を確認してください。
   - Windows Server 2008： フィード レシーバ カウンタを表示するには、デスクトップで［ADA 監視アクティビティ］ショートカットをダブルクリックします。
3. カウンタの説明が正しく表示されない場合は、カウンタのウィンドウをいったん閉じ、デスクトップ［ADA 監視アクティビティ］ショートカットをダブルクリックして再度開いてください。
4. フィード レシーバ カウンタがまったく表示されない場合には、以下を確認してください。
   - CA ADA Monitor サービスが実行されていること。
   - 監視 が 管理コンソール と同期されていること。

詳細:

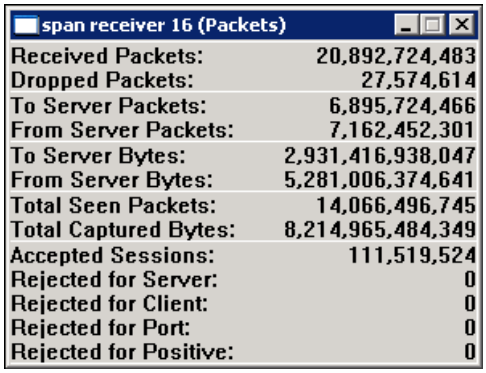
監視デバイス同期の動作 (P. 290)
監視デバイス操作 (P. 339)
GigaStor カウンタ統計の表示 (P. 413)
SPAN レシーバ統計の表示 (P. 350)

SPAN レシーバ統計の表示

CA Standard Monitor が特定の監視 NIC 上で受信する、最適化されていない TCP パケット データの詳細については、パケット カウンタ統計を参照してください。

重要: 開始前に、監視デバイスを同期します。カウンタ ウィンドウを表示するには、監視デバイスを同期する必要があります。

パケット カウンタは以下の情報を表示します。



受信済みパケット数

CA Standard Monitor 上の監視 NIC によって受信されてはいるが未検査のパケットの総数です。

注: パケット ヘッダの検査によって、アプリケーション レスポンス時間メトリックを計算するためにこれらのパケットを使用できるようになります。 詳細については、「参照されたパケット総数」を参照してください。

ドロップされたパケット数

監視 NIC には到達したがパケット ヘッダは検査されなかったパケットの総数です。 CA Standard Monitor が他のパケットの処理で高負荷状態であり、パケット キャプチャ ドライバ バッファがいっぱいであった場合、パケットはドロップされます。

サーバへのパケット数

クライアントからサーバに送信されたパケットの総数です。

サーバからのパケット数

サーバからクライアントに送信されたパケットの総数です。

サーバへのバイト数

クライアントからサーバに送信されたバイト総数です。

サーバからのバイト数

サーバからクライアントに送信されたバイト総数です。

参照されたパケット総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総数です。

注: 監視 が正常に実行されている場合、［参照されたパケット総数］は［受信済みパケット数］と一致します。監視 が受信するすべてのパケットを検査できない場合、［参照されたパケット総数］は、［受信済みパケット数］および［ドロップされたパケット数］より少なくなります。 詳細については、「ドロップされたパケット数」を参照してください。

キャプチャされたバイト総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総バイト数です。

注: CA Standard Monitor は、各パケット ヘッダを検査して、パケットが指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するかどうかを判別します。詳細については、「参照されたパケット総数」を参照してください。

承認済みセッション数

管理コンソール 上の有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッションの数です。

サーバ関連の拒否

サーバ サブネットにサーバ IP が一致しなかった TCP セッションの数です。

クライアント関連の拒否

クライアント ネットワークにクライアント IP が一致しなかった TCP セッションの数です。

ポート関連の拒否

管理コンソール が無視するポートのリストにサーバ ポートが一致する TCP セッションの数です。

ポジティブ関連の拒否

将来の使用に備えて予約されています。

詳細:

クライアント ネットワークの仕組み (P. 34)
アプリケーションの仕組み (P. 122)
サーバの仕組み (P. 79)
CA Standard Monitor の編集 (P. 336)

CA ADA Monitor サービスのトラブルシューティング

CA ADA Monitor サービスは、受信 監視フィード データを処理します。 以下のように動作します。

- CA Standard Monitor または 管理コンソール 上の監視 NIC をトラバースする各 TCP パケットを読み取るパケット ドライバのロード、初期化、および制御を行います。
- 割り当て済みの CA GigaStor など、管理 NIC からのパケット要約ファイルを処理します。
- 管理コンソール では、Cisco NAM からのメトリック要約ファイルを処理します。
- 各 監視フィード によって観測される TCP トラフィックに関してレポートします。

CA ADA Monitor サービスの状態が「停止」の場合、再起動を試みてください。 CA ADA Monitor サービスを開始できない場合は、詳細なトラブルシューティング情報について以降のセクションを参照してください。 この情報は、CA Standard Monitor に適用されます。また、監視 NIC 上で TCP パケットを受信したり、CA GigaStor など別のタイプの 監視デバイス からのパケット要約ファイルを処理する 管理コンソール にも適用されます。

次の手順に従ってください:

1. Windows デスクトップで［スタート］メニューをクリックし、［コントロール パネル］をクリックします。
2. ［コントロール パネル］で、［管理ツール］をダブルクリックします。
3. ［サービス］をダブルクリックします。
4. CA ADA Monitor サービスを右クリックし、［開始］をクリックします。

管理コンソール ログ ファイルの確認

CA ADA 管理サービスが開始されない場合は、ログ ファイルを開き、根本原因の判別につながる可能性のあるエラー メッセージを探します。 デフォルトでは、ログ ファイルは <ADA_HOME>¥Logs¥SACollectorErrors[date].log に保存されます。

NIC のステータスおよび優先度の確認

CA ADA Monitor サービスが開始されない場合は、2 つの NIC のみが有効化されており、管理 NIC に最高優先度が設定されていることを確認します。

次の手順に従ってください:

1. Windows デスクトップで［スタート］メニューをクリックし、［コントロール パネル］をクリックします。
2. ［コントロール パネル］で、［ネットワーク接続］をダブルクリックします。
3. ［ネットワーク接続］ウィンドウで、以下の確認を行います。
   - 管理 NIC および監視 NIC のステータスが「有効」であること。
   - 他のすべての NIC のステータスが「無効」であること。

   注: ステータスが「Network cable unplugged/ネットワーク ケーブルが接続されていません」の場合も、CA ADA Monitor サービスが開始されない原因となります。
4. NIC を無効にするには、NIC を右クリックし、［無効］をクリックします。
5. ［ネットワーク接続］ウィンドウで、［詳細設定］メニューから［詳細設定］をクリックします。 最初に管理 NIC、次に監視 NIC が表示されており、その後に他の未使用の接続が表示されていることを確認します。
6. CA ADA Monitor サービスを開始します。 サービスが開始されない場合は、次のセクションのトラブルシューティング手順に従ってください。

ネットワーク アダプタのレジストリ設定の確認

CA ADA Monitor サービスが開始されてない場合は、ネットワーク アダプタの Windows レジストリ設定を確認します。

次の手順に従ってください:

1. Windows デスクトップで［スタート］メニューをクリックし、［ファイル名を指定して実行］をクリックします。
2. ［開く］ボックスに、「regedit」と入力します。
3. 以下のキーに移動します。
   `HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control¥Class¥{4D36E972-E325-11CE-BFC1-08002BE10318}`

   0000 から 0008 までのサブキーがあるはずです。 それぞれのサブキーは、Windows にロードされたネットワーク アダプタを表します。
4. それぞれのサブキーを展開して、Linkage サブフォルダがあることを確認します。 サブキーに Linkage サブフォルダがない場合は、そのサブキーをエクスポートおよび削除します。
5. サブキーのエクスポートは、以下の手順で行います。
   a. サブキーを選択します。
   b. ［レジストリ エディタ］メニューで［ファイル］をクリックした後、［エクスポート］をクリックします。
   c. エクスポート先とファイル名を選択します。
   d. ［保存］をクリックします。
6. サブキーを削除するには、サブキーを右クリックし、［削除］をクリックします。
7. Linkage サブフォルダがないサブキーのすべてについて、手順 5 および 6 を繰り返します。
8. CA ADA Monitor サービスを開始します。 サービスが開始されない場合は、次のセクションのトラブルシューティング手順に従ってください。

NIC 設定の確認

CA ADA Monitor サービスが開始されない場合は、statstconsole.exe プログラムを使用して NIC 設定を確認します。

次の手順に従ってください:

1. Windows エクスプローラで、<ADA_HOME>¥bin を参照します。
2. satstconsole.exe をダブルクリックします。
3. ［SuperAgent コンソール］ダイアログ ボックスで、［アダプタ］フィールドの監視 IP アドレスを確認します。 これは、管理コンソール が検索する IP アドレスです。
4. ［アダプタ］フィールドに、監視 NIC に現在割り当てられている IP アドレスを入力します。
5. Microsoft Windows の［ネットワーク接続］ウィンドウを使用して、管理 NIC に静的な IP アドレスが割り当てられていることを確認します。

   注: 管理 NIC に DHCP アドレスを使用すると、問題が発生します。
6. 管理コンソール で、［開始］をクリックします。
7. CA ADA Monitor サービスを開始します。 サービスが開始されない場合は、次のセクションのトラブルシューティング手順に従ってください。

監視サービス用のレジストリ設定の確認

CA ADA Monitor サービスが開始されてない場合は、Windows のレジストリを確認します。

次の手順に従ってください:

1. Windows デスクトップで［スタート］メニューをクリックし、［ファイル名を指定して実行］をクリックします。
2. ［開く］ボックスに、「regedit」と入力します。
3. 以下のキーに移動します。
   `HKEY_LOCAL_MACHINE¥SOFTWARE¥NetQoS¥SuperAgent¥Parameters`
4. MasterDB キーが 管理コンソール または CA Standard Monitor の IP アドレスに設定されていることを確認します。
5. Role キーが以下の*いずれか*に設定されていることを確認します。
   - CA Standard Monitor： Slave
   - スタンドアロン 管理コンソール： Standalone
6. LastManagementAddress が、CA Standard Monitor または 管理コンソール の管理 NIC IP アドレスの UNIX 同等アドレスに設定されていることを確認します。
7. UNIX の同等 IP アドレスを検索するには、MySQL がインストールされているサーバにログインします。 以下のクエリを実行します。
   `SELECT INET_ATON('x.x.x.x');`

   x.x.x.x は、CA Standard Monitor または 管理コンソール 上の管理 NIC の IP アドレスです。たとえば、以下のようになります。
   `mysql> SELECT INET_ATON('209.207.224.40');`
8. CA ADA Monitor サービスを開始します。 サービスが開始されない場合は、次のセクションのトラブルシューティング手順に従ってください。

管理コンソール との通信の確認

CA ADA Monitor サービスが開始されない場合は、CA Standard Monitor が TCP-80 上で CA Application Delivery Analysis Manager と通信できることを確認します。

以下の手順は、管理コンソール 上に存在する CA Standard Monitor に適用されます。

次の手順に従ってください:

1. CA Standard Monitor でコマンド プロンプトを開き、次のコマンドを入力します。
   `telnet <host> <port>`

   項目の説明

   <host>

   管理コンソール の IP アドレスです。

   <port>

   80 です

   「接続に失敗しました」というエラー メッセージが表示される場合は、ポートがブロックされているので、ポートを開く必要があります。 黒いブランク画面が表示されると、接続は成功です。
2. CA ADA Monitor サービスを開始します。 サービスが開始されない場合は、次のセクションのトラブルシューティング手順に従ってください。

少なくとも 1 つの監視フィードがアクティブであることの確認

CA ADA Monitor サービスが開始されない場合は、Standard Monitor のプロパティでパケット監視が無効に設定されていないことを確認します。

CA Standard Monitor を追加したときに［パケット監視の無効化］オプションが選択された場合は、CA ADA Monitor サービスが開始するように、CA GigaStor などの 監視デバイス を 監視 に割り当てる必要があります。

パケット キャプチャの実行

CA Standard Monitor 上の監視ポートで受信された TCP パケットのパケット キャプチャを実行し、パケット ヘッダおよび内容を確認するには、PacketMon を使用します。

PacketMon は、CA Standard Monitor やスタンドアロン 管理コンソール にインストールすることが認定された唯一のパケット スニファです。 パケット キャプチャ ドライバとの競合を回避するために、他のパケット スニファ（*Wireshark* など）を 監視 にインストール**しない**でください。

次の手順に従ってください:

1. 監視 に PacketMon をインストールします。
2. インストールが完了した後、PacketMon を起動します。
3. PacketMon で［開始］をクリックして、パケット キャプチャを開始します。

   結果が表示されない場合や、UDP/Unknown のパケット タイプが表示される場合は、SPAN の設定が間違っているか、ネットワーク タップが正しくインストールされていません。 SPAN 設定またはネットワーク タップを確認し、別のパケット キャプチャを実行してください。
4. 有効な TCP パケットが返されたら、CA ADA Monitor サービスを開始します。

重複したクライアント ネットワークの確認

サーバ、アプリケーション、クライアント ネットワークを設定している場合は、クライアント ネットワークの重複がないようにする必要があります。

大規模な設定（数 100 万の組み合わせ）の場合、CA ADA Monitor サービスは、起動に数分かかります（すぐには起動しません）。 数百台のサーバが定義されており、そのすべては監視する必要がない場合には、それらを設定から削除します。 ベストプラクティスとして、必要なサーバ、アプリケーション、およびクライアント領域のみに 管理コンソール 設定を削減してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

   ［ネットワーク リスト］が表示されます。
3. ネットワークの一覧を調べ、同じクライアント領域が 2 回設定されていないことを確認します。

データ欠落のトラブルシューティング

CA Standard Monitor がトラフィックを監視しているが、管理コンソール にデータが表示されない場合やデータが最新でない場合には、管理コンソール と 監視 の間の通信に問題がある可能性があります。

次の手順に従ってください:

1. TCP-8080 上の 管理コンソール から CA Standard Monitor に telnet 接続できることを確認します。
2. 接続できない場合は、ファイアウォールや ACL によって通信が妨げられていないことを確認します。 TCP-8080 は、管理コンソール が CA Standard Monitor からデータ ファイルを取得するために使用されます。
3. すべての CA ADA 関連サービスが 管理コンソール および CA Standard Monitor 上で開始されていることを確認します。
4. 管理コンソール の <ADA_HOME>¥Datafiles ディレクトリが数時間または数日間にまたがるファイルで占有されていないことを確認します。

ドロップされたパケット数のトラブルシューティング

CA Standard Monitor で、短期間または長期間にドロップされたパケット数がレポートされることがあります。 この状態が持続する時間の長さは、さまざまな要因によって異なりますが、これらは以下のトラブルシューティング手順を実行することにより識別できます。

次の手順に従ってください:

1. 監視 に対する SPAN 内の集約トラフィックの総量を評価します。 インバウンド データ レート（監視 によって監視されたアクティブ セッションの数ではなく）が原因でデータがドロップされている可能性があります。 これが、そのポートの使用率割合の統計です。

   監視デバイス に着信するデータ トラフィックの純量が多すぎる場合は、監視 上の監視ポートに SPAN （ポート ミラーリング）するデータの量を減らします。管理コンソール がトラフィックのすべてを監視するように設定されている場合は、監視 を追加し、監視デバイス の間でサーバ SPAN の負荷を分散させる必要が生じることがあります。

2. パケット 監視フィード 内のアクティブ セッションの総数を評価します。 監視 は、アクティブ セッションごとにレスポンス時間データを分離して計算するため、アクティブ セッション数が多くなるほど、新規の受信データの処理に与える影響が大きくなります。

   監視 は、管理コンソール に定義されたアプリケーション ポート、サーバ、およびクライアント ネットワークに一致する SPAN トラフィックを観測する際に、*アクティブ セッション*を作成します。

   管理コンソール を更新することによって、監視されたアプリケーション ポート、サーバ、およびクライアント ネットワークのリストを最適化できる場合には、監視 上の処理リソースを最適化できます。 管理コンソール が正しいアプリケーション、サーバ、ネットワークを監視している場合は、監視 を追加し、監視デバイス の間のサーバ SPAN をロードバランスする必要性が生じることがあります。

3. ウィルス スキャン、スパイウェア スキャンおよび削除プログラム、システム バックアップ プロセスなどのバックグラウンド プロセスを評価します。 監視 上で実行される追加の各アプリケーションは、プロセッサの総使用率に影響を与え、監視 のインバウンド データ トラフィック処理能力を低下させます。これらのプロセスでメモリ、CPU、プロセッサ、ディスク IO バスが多く消費されるほど、パケットがドロップされるまでに 監視 が実際に処理できるパケット数が少なくなります。

利用可能な 監視 リソースを最適化するには、これらのアプリケーションを 監視 から削除します。

第 14 章: CA Virtual Systems Monitor による監視

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 Virtual Systems Monitor が監視デバイスとして動作する仕組み (P. 366)
システム要件 (P. 370)
CA Virtual Systems Monitor の追加 (P. 371)

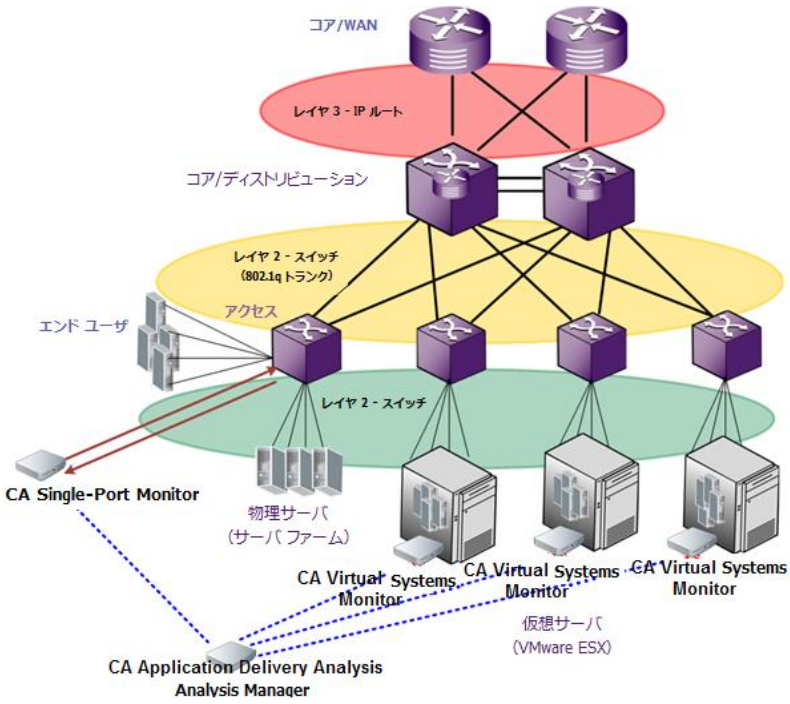
CA Virtual Systems Monitor が監視デバイスとして動作する仕組み

レスポンス時間 CA Virtual Systems Monitor（CA Virtual Systems Monitor）は、CA Application Delivery Analysis の一種の 監視デバイス として機能します。CA Virtual Systems Monitor を使用して、同じ VMware ESX ホスト上の仮想サーバ間の IPv4 ベースのトラフィックを監視します。 CA Virtual Systems Monitor は、同じ ESX Host 上の VM の間のサーバ間トラフィックを監視し、CA Virtual Systems Monitor 上の負荷を最小化します。また、拡張によって、ESX Host 上の利用可能なリソースを最大化します。

別の ESX Host からのトラフィックや、ESX Host 内の仮想サーバと通信するリモート サブネットからのトラフィックなど、仮想環境の外部からのトラフィックを監視するには、物理サーバ スイッチからのサーバ トラフィックを、CA Multi-Port Monitor などの物理 監視デバイス にミラーリングします。

CA Virtual Systems Monitor は、VMware ESX Host の「内部」の仮想サーバ間の通信を監視することだけを目的としています。 物理（外部）デバイスと仮想サーバの間のトラフィックの監視に CA Virtual Systems Monitor を使用しないでください。 物理デバイス間や物理デバイスと仮想サーバ間の通信を監視するには、CA Multi-Port Monitor などの物理 監視デバイス を使用します。

下記の例に表すように、CA Virtual Systems Monitor は同じ ESX Host 上の VM の間のサーバ間トラフィックを監視し、物理 監視デバイス は物理スイッチから SPAN データを取得します。



CA Virtual Systems Monitor は、CA Standard Monitor とよく似ていますが、物理アプライアンスではなく、VMware 仮想マシンにインストールされます。 CA Virtual Systems Monitor は、CA Standard Monitor と同様に、ミラーリングされたポートからデータを収集し、パケット ヘッダからパフォーマンス関連情報を調べて、関連するパフォーマンス メトリックをレポートおよび表示の目的で 管理コンソール に渡します。

CA Standard Monitor とは異なり、CA Virtual Systems Monitor は Cisco WAE デバイスまたは CA GigaStor から要約ファイルを受信しません。

CA Virtual Systems Monitor は、Cisco Nexus 1000V 経由の SPAN （ポート ミラーリング）をサポートします。 VMware vSwitch を使用している場合、CA Virtual Systems Monitor では、仮想スイッチ上のミラーリングされたトラフィックを参照するプロミスキャス ポート グループが必要になります。

詳細:

CA Standard Monitor による監視 (P. 321)

展開の計画

CA Virtual Systems Monitor は、ESX Host の外側の外部トラフィックは参照することなく、ESX Host 上の仮想サーバ間のトラフィックを「参照」できる必要があります。 インストールの計画時には、以下を考慮する必要があります。

- 監視する必要があるのはどの多層アプリケーションか。
- ESX Host 上のどのサーバがサーバ間トラフィックを作成するのか。 CA Virtual Systems Monitor がこの仮想サーバ間通信のネットワーク トラフィックを参照できるように設定してください。
- どのサーバが外部デバイス（別の ESX Host 上の仮想サーバなど）や物理サーバと通信するのか。 CA Virtual Systems Monitor がこの通信を参照することを許可しないでください。 その代わりに、CA Multi-Port Monitor などの物理 監視デバイス にトラフィックをミラーリングしてください。

  注: 監視デバイス で 外部トラフィックを分離することにより、管理コンソール では、仮想サーバ間トラフィックを監視するように CA Virtual Systems Monitor を自動的に割り当て、物理サーバと仮想サーバ間のトラフィックを監視するように物理 監視 を自動的に割り当てることができます。
- 監視予定の仮想マシンが複数の仮想 NIC に割り当てられる場合、その仮想マシンの管理 IP アドレスは、ESX Host （仮想 NIC）上の最後の物理 NIC に属するネットワーク アダプタに割り当てられる必要があります。 これは VMware の問題です。VMware は、ネットワーク アダプタの選択時、最後の仮想 NIC に割り当てられているネットワーク アダプタの IP アドレスのみを開示します。 たとえば、VMNIC1、VMNIC2、VMNIC3 という 3 つの仮想 NIC に関連付けられた仮想マシンは、VMNIC1 や VMNIC2 ではなく VMNIC3 に割り当てられているネットワーク アダプタの IP アドレスをレポートします。

詳細:

監視デバイスに関する推奨事項 (P. 302)

ポート使用率とファイアウォール

CA Virtual Systems Monitor をセットアップし、これを 監視デバイス として追加する準備をする際には、CA Virtual Systems Monitor （仮想マシン上に配置）と 管理コンソール （物理コンピュータ上に配置）の間の通信を妨げる可能性のあるあらゆるファイアウォールを考慮する必要があります。以下を決定しておく必要があります。

- どのファイアウォール ポートが開いているか。
- どのタイプのトラフィックがそれらのポートで許可されているか。

CA Virtual Systems Monitor には、管理コンソール と通信するための Web サービスが含まれています。 管理コンソール は、その 監視デバイス に監視手順を定期的に送信する必要があります。また、CA Virtual Systems Monitor は、5 分間の集約データが含まれるファイルを 管理コンソール に送信する必要があります。5 分間のデータ ファイルは集約されたデータで構成されるため、アップリンク ポート上で消費されるネットワーク帯域幅は最小です。

以下の表には、管理コンソール と CA Virtual Systems Monitor の間で通信できるようにするために開いておく必要のあるファイアウォール ポートの概要を示します。

ポート	方向	説明
TCP-1000	インバウンド (管理コンソール から CA Virtual Systems Monitor へ)	管理コンソール アクセスの HTTP
TCP-80	インバウンド	データに対する Web サービス リクエスト
TCP-161	インバウンド	SNMP MIB クエリ
UDP-162	アウトバウンド	SNMP アラート トラップ

システム要件

CA Virtual Systems Monitor は、Microsoft® Windows オペレーティング システム上にインストールされる必要があります。 Windows オペレーティング システムについては、お客様の責任でライセンスされたバージョンをインストールしていただく必要があります。 CA には、CA Virtual Systems Monitor をインストールする Windows オペレーティング システムのライセンスは含まれていません。

CA Virtual Systems Monitor を正しく展開するには、仮想マシンが以下の要件を満たす必要があります。

要件	説明
仮想スイッチ	■ VMware vSwitch を使用する VMware ESX® および VMware ESXi® 3.5 または 4.1 ■ Cisco Nexus® 1000V を使用する VMware ESX および ESXi 4.1
CA Virtual Systems Monitor をホストする仮想マシン	プロセッサ： 仮想プロセッサ x 1 基（*最小*） メモリ： 1 GB （*最小*） 仮想ディスク ■ Windows Server 2003： 16GB ■ Windows Server 2008 R2： 30GB ネットワーク： 仮想ネットワーク アダプタ x 2 基（最小 1 Gbit） アップリンク ポート（ESX Host を基点とする物理ポート）は、CA Virtual Systems Monitor がその対応する 管理コンソール と通信できることが必要です。
ゲスト オペレーティング システム	CA Virtual Systems Monitor は次のいずれかを必要とします。 ■ SP2 対応の Microsoft Windows Server 2003 Standard Edition （x64 または 32 ビット） ■ Microsoft Windows Server 2008 R2 Standard Edition （x64 のみ）

CA PC または CA NPC に 管理コンソール を登録している場合、CA PC または CA NPC は CA Virtual Systems Monitor からのパフォーマンス データと共に、VMware からの仮想マシン関連のパフォーマンス統計をレポートします。

CA PC または CA NPC で VMware からの仮想マシン関連パフォーマンス統計を表示できるようにする方法

- 監視予定の VM に VMware Tools がインストールされていることが必要です。
- 監視予定の仮想マシンが複数の仮想 NIC に割り当てられる場合、その仮想マシンの管理 IP アドレスは、ESX Host （仮想 NIC） 上の最後の物理 NIC に属するネットワーク アダプタに割り当てられる必要があります。 これは VMware の問題です。VMware は、ネットワーク アダプタの選択時、最後の仮想 NIC に割り当てられているネットワーク アダプタの IP アドレスのみを開示します。 たとえば、VMNIC1、VMNIC2、VMNIC3 という 3 つの仮想 NIC に関連付けられた仮想マシンは、VMNIC1 や VMNIC2 ではなく VMNIC3 に割り当てられているネットワーク アダプタの IP アドレスをレポートします。

CA Virtual Systems Monitor の追加

CA Virtual Systems Monitor をプロビジョニングするには、以下のタスクを完了する必要があります。

1. 仮想スイッチの設定 (P. 371)
2. 仮想マシンの作成 (P. 379)
3. ネットワーク接続の設定 (P. 381)
4. CA Application Delivery Analysis セットアップ プログラムの実行 (P. 385)
5. セットアップの完了 (P. 387)
6. CA Virtual Systems Monitor の管理 (P. 387)

仮想スイッチの設定

CA Virtual Systems Monitor は、VMware vSwitch や Cisco Nexus 1000V と共に動作します。

VMware vSwitch の設定方法

VMware vSwitch 上の VM 内トラフィックを監視するには、専用監視ポート グループをプロミスキャス モードを有効にして作成し、CA Virtual Systems Monitor 上の監視 NIC を監視ポート グループに割り当てます。

CA Virtual Systems Monitor は、仮想環境の「内部」における仮想サーバ対仮想サーバの通信を監視するように設計されています。 以下のような場合、手順に従います。

- フロントエンドおよびバックエンド サーバで別々の vSwitches を使用している。
  - バックエンドの vSwitch でプロミスキャス モードを有効にします。
  - フロントエンド サーバ トラフィックを物理監視デバイスにミラーリングします。
- フロントエンドおよびバックエンド サーバで別々の vSwitches を使用していない。
  - vSwitch でプロミスキャス モードを有効にします。
  - フロントエンド サーバ トラフィックを物理監視デバイスにミラーリングし、フロントエンド サーバを物理監視デバイスに「固定」します。

CA Virtual Systems Monitor 上の管理ネットワーク アダプタが ESX ホストの外部にある 管理コンソール と通信できるようにするには、既存の仮想ネットワーク アダプタを使用するか、新しい管理ポート グループを作成するように CA Virtual Systems Monitor を設定します。管理ポート グループ上のプロミスキャス モードを有効にする必要はありません。 プロミスキャス モードの詳細については、VMware 製品ドキュメントを参照してください。

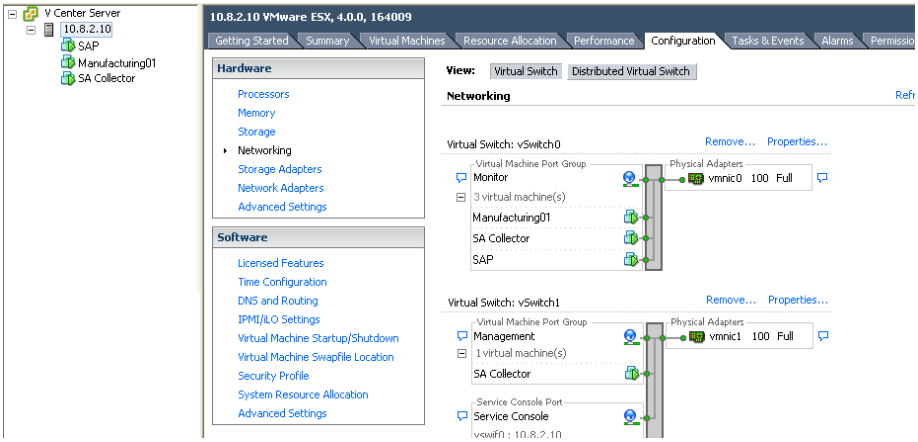
以下の例では、管理コンソール仮想マシン（SA Collector）は、監視と管理のネットワークを使用するように設定されています。 ESX ホスト（10.8.2.10）は以下によって設定されます。

- vSwitch0。 この仮想スイッチには vmnic0 デバイスが割り当てられます。また、セキュリティ ポリシーは仮想スイッチおよび監視ポート グループ上でプロミスキャス モードを許容するように設定されます。プロミスキャス モードによって、CA Virtual Systems Monitor は、Manufacturing01 と SAP 仮想マシンを含む監視ネットワークに接続する VM サーバ対サーバ トラフィックを参照できます。

vmnic0 ネットワーク アダプタは、バックエンド SAP サーバ上の SAP アプリケーションにクライアント リクエストを送信する外向き Web サーバなど、仮想スイッチ上のサーバと通信するために仮想スイッチ外部からのクライアント トラフィックを有効にするアップリンク ポートです。

外部の物理クライアント（図示せず）へのフロントエンド Web サーバ トラフィックを監視するには、CA Multi-Port Monitor など物理 監視 を使用して、物理スイッチからミラーリングされたサーバ トラフィックを監視します。

- vSwitch1。この仮想スイッチには vmnic1 ネットワーク アダプタが割り当てられます。また、仮想スイッチ用のセキュリティ ポリシーおよび仮想スイッチ上の管理ポート グループは、プロミスキャス モードを拒否するように設定されています。 vmnic1 ネットワーク アダプタは、CA Virtual Systems Monitor が 管理コンソール と通信できるようにするアップリンク ポートです。これは ESX ホスト上ではホストされません。



次の手順に従ってください:

1. VMware vSwitch 上で、プロミスキャス モードを有効にして専用ポート グループを作成します。

   a. 監視するアプリケーション トラフィックを参照する VMware vSwitch を識別します。

   b. VMware vSwitch で、以下の設定で専用監視ポート グループを作成します。

      ネットワーク ラベル

      ネットワークを Monitor と命名します。 その後、仮想マシンを設定するとき、ミラーリングされたアプリケーション トラフィックを持つネットワーク アダプタを容易に識別できます。

      VLAN ID

      監視するアプリケーション トラフィックを持った VLAN ID を指定するか、［すべて］を選択します。 VLAN タグが使用されていない場合は、このフィールドを空白にしておきます。

      ESX 3.5 サーバ上で VLAN をすべて監視する場合は、VLAN ID を 4095 と指定します。

      仮想マシンに AMD アダプタがある場合、Intel E1000 ドライバを使用するためにゲスト オペレーティング システムを設定する必要があります。 詳細については、http://kb.vmware.com/kb/1004252 を参照してください。

      プロミスキャス モード

      セキュリティ ポリシーでプロミスキャス モードが許可されるように設定します。これにより、監視ポート グループが VMware vSwitch 上のすべてのトラフィックを参照できるようになります。

2. 監視ポート グループ上でプロミスキャス モードを有効にするには、VMware vSwitch および監視ポート グループがプロミスキャス モードを許可するように設定する必要があります。

   プロミスキャス モードが VMware vSwitch 上で有効にならない場合は、VMware vSwitch のセキュリティ ポリシーがプロミスキャス モードを許可するように設定します。

3. vSwitch に管理データ用の既存のポート グループがある場合は、このポート グループを使用して CA Virtual Systems Monitor が 管理コンソール と通信できるようにします。

必要であれば、「Management」という名前のポート グループを作成して、ミラーリングされたスイッチ トラフィックを受信していないネットワーク アダプタを識別します。

Cisco Nexus 1000V の設定方法

CA Virtual Systems Monitor が Cisco Nexus 1000v 上のトラフィックを監視できるようにするには、CA Virtual Systems Monitor の専用ポート プロファイルを作成して、適切な VLAN トラフィックを観測します。 仮想マシンをプロビジョニングした後、VLAN トラフィックを仮想マシン上の監視インターフェースに SPAN することができます。 VLAN トラフィックをミラーリングする方法の詳細については、Cisco 製品ドキュメントを参照してください。

監視する VLAN を選択するとき、以下のような場合、手順に従います。

- フロントエンド サーバ（ESX 外部からのトラフィック）およびバックエンド サーバ（ESX 内部のトラフィック）で別々の VLAN を使用している場合、フロントエンド サーバ トラフィックを物理監視デバイスにミラーリングします。
- フロントエンドおよびバックエンド サーバで別々の VLAN を使用していない場合、ESX 内の全トラフィックをミラーリングし、ESX 外部からのトラフィックを物理コレクタにミラーリングして、フロントエンド サーバを物理監視デバイスに「固定」します。

次の手順に従ってください:

1. Cisco Virtual Supervisor Module （VSM）で、該当する VLAN の SPAN トラフィックを確認するには、CA Virtual Systems Monitor が使用できる専用監視ポート プロファイルを作成して有効にします。 ポート プロファイル作成方法の詳細については、Cisco 製品ドキュメントを参照してください。

   管理データ用の既存のポート グループまたはポート プロファイルがある場合は、それを使用して CA Virtual Systems Monitor が 管理コンソール と通信できるようにします。 必要であれば、「Management」という名前のポート プロファイルを作成し、CA Virtual Systems Monitor 上でネットワーク接続を設定するときに、ミラーリングされたスイッチ トラフィックのないネットワーク アダプタを容易に識別できるようにします。

2. CA Virtual Systems Monitor をホストする仮想マシンを作成し（P. 379）、監視および管理用のネットワーク アダプタを使用するための仮想マシンを設定します。

3. CA Virtual Systems Monitor 仮想マシン上の監視インターフェース（P. 381）まで、仮想サーバ対仮想サーバの VLAN トラフィックを SPAN します。

SPAN に関するその他の注意事項

SPAN を設定するときは、次の点に留意してください。

- ソース ポートは、Ethernet ポート、仮想 Ethernet ポートまたは VLAN インターフェースのいずれかです。 標準の SPAN セッションは、同じ物理（ESX）ホスト上のソースと宛先のみを SPAN します。
- 宛先ポートは任意の物理（または仮想）Ethernet ポートです。 ポートチャネルではありません。
- SPAN セッションの宛先はすべて、同じホスト上にあります。 たとえば、1 つの SPAN セッションで VLAN をソース（1 つのホスト上）に、2 つの宛先を別の物理ホスト上に置くということはできません。
- Cisco Nexus 1000V には 16 の SPAN セッションという制限が あります。しかし、同じソースを持つことができるのは（VLAN など）4 つまでです。 以下の例では、どちらの監視セッションも VLAN 152 をソースとして参照します。したがって、VLAN 152 をソースとして使用して設定できるのはあと 2 つの監視セッションまでです。

```
monitor session 1
  source vlan 152 both
  destination interface Vethernet6
  no shut
monitor session 2
  source vlan 152 both
  destination interface Vethernet9
  no shut
```

VLAN 上の重複したパケットを除去する

たとえば、CA Virtual Systems Monitor がパケットの 2 つのコピーを受信したとき、CA Virtual Systems Monitor へ VLAN を SPAN する場合、［エンジニアリング］ページのパケット ロスの割合レポートは、失われたパケットの割合を非常に高くレポートします。

このセクションでは、CA Virtual Systems Monitor を有効にして TCP パケットを重複排除する方法について説明します。

次の手順に従ってください:

1. C:¥CA¥bin ディレクトリ内に RetransPacketDefs.ini.sav ファイルを置きます。
2. ファイル名から .sav 拡張子を削除します。
3. RetransPacketDefs.ini ファイルを編集します。デフォルトでは、ファイルに以下のエントリが含まれます。

   ```
   <no logging>
   50 1000
   10 20 30 40 50 60
   ```

   最初の行は、重複パケットに関する情報をどこにログ記録するかを CA Virtual Systems Monitor に伝えます。 <no logging> という句を C:¥CA¥bin¥duppkts.txt のようなログ記録ファイルへのパスに置き換えると、CA Virtual Systems Monitor は情報をログ記録します。 ログ ファイルを有効にしておくことは、バッファ サイズが適切かどうかを判断するときなどにも役に立ちます。

   2 行目の最初の数字 50 は、重複を探すために CA Virtual Systems Monitor が 50 パケットのバッファをメンテナンスすることを指定します。 このパラメータを小さくすると、CA Virtual Systems Monitor が重複を探すために消費する CPU サイクルが少なくなります。 これは CA Virtual Systems Monitor のパフォーマンスを改善しますが、おそらく検出される重複も少なくなります。2 番目の数字である 1000 は使用されません。

   ファイル内の最後の行では、重複のヒストグラムのビンについて説明します。これはログ ファイルの最初の行に表示されます。ヒストグラムは、重複がそれぞれそのオリジナルからどれくらい離れたところで見つかったかを示します。 この情報は、バッファ サイズ パラメータの調整に役立ちます。 理想的には、失われた重複は最初のわずかなビンで発生し、リモート ビンではビン数が減少したりなくなります。高い番号のビンのカウントが高いままである場合は、バッファ サイズがおそらく小さすぎます。

4. 変更を適用するには、CA ADA Monitor サービスを再起動し、管理コンソール が重複排除データをレポートするのを 10 分間待ってから、［パケット ロスの割合］レポートを参照してパケット ロスの割合が減少したかを確認します。

   必要であれば、バッファ サイズを増加させて CA Virtual Systems Monitor がより多くのパケット数で重複を検索できるようにします。

仮想マシンの作成

CA Virtual Systems Monitor をホストする仮想マシンを作成します。 CA Virtual Systems Monitor を使用して、同じ VMware ESX Host 上の仮想サーバ間でアプリケーションのパフォーマンスを監視します。

仮想スイッチ インフラストラクチャに Cisco 1000v を使用している場合は、適切な VLAN トラフィックを監視 NIC に SPAN させることを覚えておいてください。

仮想マシンが以下の要件を満たしているかを確認します。

設定	説明
仮想マシン名	仮想マシン（たとえば「CA Virtual Systems Monitor」）の名前を指定します。
データ ストア	使用可能な空き容量を持つデータ ストアを選択します。 仮想マシンには 10 GB を割り当てる予定にしてください。

設定	説明
ゲスト オペレーティング システム	CA Virtual Systems Monitor は次のいずれかを必要とします。 ■ Microsoft Windows Server 2003 Standard Edition（64 または 32 ビット） SP2 ■ Microsoft Windows Server 2008 R2 Standard Edition（64 ビットのみ） オペレーティング システムをインストールした後、以下の手順に従います。 ■ Microsoft .NET Framework 3.5 SP1 を Windows Server 2003 にインストールします。 Windows Server 2008 R2 にはすでに Microsoft .NET Framework 3.5 SP1 が含まれています。 ■ SNMP をインストールし、public が承認されたコミュニティ名であることを確認します。 ■ ASP.NET（ネットワーク COM+ アクセスおよび IIS が含まれる）をインストールします。 インストール時に IIS を設定するとき、クリックして SMTP Service をインストールし、デフォルト IIS コンポーネント（共通ファイル、インターネット情報サービス マネージャ、ワールド ワイド Web サービス）および IIS 6 メタベース互換性コンポーネントをインストールします。 ■ 重大または重要な更新をインストールします。 ■ 推奨されている更新（「*ソフトウェア*、*オプション*」としても表示）はどれもインストールしません。 ■ ドライバ更新（「*ハードウェア*、*オプション*」としても表示）はどれもインストールしません。 ■ 推奨されている更新とドライバ更新は、オフにする必要があり、［今後表示しない］チェックボックスを選択して今後のスキャンには表示されないようにしてください。支援情報については、CA サポート（**エラー! ハイパーリンクの参照に誤りがあります。**）までお問い合わせください。 ■ Windows Server 2003 上の Internet Explorer セキュリティ強化の構成をアンインストールします。 ■ VMware Tools をインストールします（必須）。
仮想 CPU	仮想 CPU を 1 つ割り当てます。

設定	説明
メモリ	1GB （1024 MB）を割り当てます。
NIC	管理用と監視用の NIC に対して 2 つのネットワーク接続を作成します。 ■ ネットワーク アダプタ 1 で管理ネットワークを選択します。 ■ ネットワーク アダプタ 2 で監視ネットワークを選択します。
仮想ディスク	■ Windows Server 2003 で、新しい仮想ディスクを作成し、16GB の仮想ディスク空き容量を割り当てます。［すべての空き容量を今すぐ割り当てる］オプションを必ず選択してください。 ［詳細］オプションで［独立］をオンにし、［永続的］を選択します。 ■ Windows Server 2008 R2 で、新しい仮想ディスクを作成し、30GB の仮想ディスク空き容量を割り当てます。［すべての空き容量を今すぐ割り当てる］オプションを必ず選択してください。 ［詳細］オプションで［独立］をオンにし、［永続的］を選択します。
管理者アカウント	■ 管理者アカウントのパスワードを指定し、［パスワードを無期限にする］を選択します。 ■ ローカルの管理者グループに、*netqos* という名前の新規ユーザを作成し、パスワードは *changeme* にして、［パスワードを無期限にする］を選択します。

詳細:

Cisco Nexus 1000V の設定方法 (P. 376)

ネットワーク接続の設定

以下の手順に従って、ゲスト オペレーティング システム上にネットワーク接続を設定します。

1. ネットワーク接続の名前を変更します。（P. 382）
2. ネットワーク接続の詳細設定を設定します。（P. 383）
3. ネットワーク接続に IP アドレスを割り当てます。（P. 384）

ネットワーク接続の名前の変更

仮想スイッチを設定したときに作成したネットワーク接続をより容易に識別し設定するには、仮想マシンにバインドされる 監視および管理用のネットワーク アダプタに対応するゲスト オペレーティング システム内のネットワーク接続の名前を変更します。

次の手順に従ってください:

1. VMware vSphere クライアントで、管理および監視用ネットワーク アダプタの MAC アドレスを識別します。
   a. 仮想マシンを右クリックし、［Edit Settings］をクリックします。
   b. ［Virtual Machine Properties］で、監視および管理用ネットワーク アダプタの MAC アドレスを書きとめます。
2. ゲスト オペレーティング システムで、各ネットワーク接続の MAC アドレスを識別します。
   a. Windows デスクトップで、［スタート］メニューをクリックし、［マイ ネットワーク プレース］を右クリックして［プロパティ］をクリックします。または、［スタート］-［コントロール パネル］をクリックします。［ネットワーク接続］を右クリックし、［開く］をクリックします。
   b. Windows Network Connections で、接続を右クリックし、［プロパティ］をクリックします。プロパティ ダイアログ ボックスで［サポート］タブをクリックし、［詳細］をクリックします。［物理アドレス］は、監視および管理用ネットワーク アダプタの MAC アドレスに対応します。

   ヒント： コマンド プロンプトから、MAC アドレスを確認するために ipconfig/all コマンドを実行できます。
3. ［閉じる］をクリックします。
4. ネットワーク接続ウィンドウで、適切なインターフェースに対応させるため、デフォルトの名前を次のように編集します。
   a. 管理
   b. Monitor

詳細:

仮想スイッチの設定 (P. 371)

ネットワーク接続の詳細設定の設定

ゲスト オペレーティング システムで、正しい接続順序とバインディングを指定するために詳細ネットワーク接続設定を設定します。

次の手順に従ってください:

1. ネットワーク接続の［詳細］メニューで［詳細設定］をクリックします。
2. ［アダプタとバインド］タブで、右側の上向き矢印を使用し、最上部の管理 NIC に移動します。 この操作は優先度を設定するものであり、CA Virtual Systems Monitor が正しく動作するために必要です。
3. ［バインド］ボックスで、以下のバインド上のすべての NIC 用インターネット プロトコル（TCP/IP）オプションをクリアします。
   - Microsoft ネットワーク用に共有するファイルとプリンタ
   - Microsoft ネットワーク用のクライアント
4. ［OK］をクリックします。

ネットワーク接続への IP アドレスの割り当て

ゲスト オペレーティング システムで、IPv4 アドレス、サブネット マスクおよび管理ネットワーク接続までのデフォルト ゲートウェイを割り当てます。

VMware vSwitch を使用している場合、ルーティング不能 IP アドレスを使って監視ネットワーク接続を設定します。 ルーティング不能 IP アドレスを使用する場合は、デフォルト ゲートウェイ割り当てを指定する必要がありません。

NIC に割り当てる IP アドレスを書きとめます。 この情報は、CA Virtual Systems Monitor を 管理コンソール に追加するとき必要になります。

次の手順に従ってください:

1. Windows デスクトップで［スタート］メニューをクリックし、［コントロール パネル］をクリックします。
2. ［コントロール パネル］で［ネットワーク接続］をクリックします。
3. ［管理］を右クリックし、［プロパティ］をクリックします。
4. ［全般］タブで、［インターネットプロトコル（TCP/IP）］、［プロパティ］の順にクリックします。
5. ［次の IP アドレスを使用する］を選択し、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。［OK］をクリックします。
6. 監視ネットワーク接続についてもこれらの手順を繰り返します。ただし、ルーティング不能 IP アドレスとサブネット マスクは指定しますが、デフォルト ゲートウェイは指定しません。 以下の値をお勧めします。

   監視 1

   IP アドレス： 1.1.0.1

   サブネット マスク： 255.0.0.0

詳細:

VMware vSwitch の設定方法 (P. 372)

CA Application Delivery Analysis セットアップ プログラムの実行

仮想マシンに CA Virtual Systems Monitor をインストールするために CA Application Delivery Analysis セットアップ プログラムを実行します。 セットアップ プログラムを実行する前に、リモート デスクトップによって仮想マシンにアクセスできることを確認します。

CA Application Delivery Analysis セットアップ プログラムは CA Application Delivery Analysis.iso ダウンロード ファイルに同梱されています。必要であれば、CA サポート Web サイト（http://ca.com/support）から CA Application Delivery Analysis.iso をダウンロードしてください。

CA Application Delivery Analysis セットアップ プログラムを実行する前に、仮想マシンのスナップショットを作成しておいてください。必要になったときに CA Virtual Systems Monitor をアンインストールできます。 CA Application Delivery Analysis セットアップ プログラムでは CA Virtual Systems Monitor はアンインストールされません。アンインストールするには、以前の（インストール前の）スナップショットに戻す必要があります。仮想マシンのスナップショットを作成する方法の詳細については、VMware ドキュメントを参照してください。

次の手順に従ってください:

1. 管理者権限を持つユーザとして仮想マシンにログインします。
2. CA Application Delivery Analysis セットアップ プログラムの実行が許可されていることを確認します。 この手順を完了するには、セットアップ実行可能ファイルを右クリックし、［プロパティ］をクリックします。 このダイアログ ボックスから、［禁止の解除］ボタン（有効な場合）をクリックし、［OK］をクリックします。
3. CA Application Delivery Analysis セットアップ プログラムの実行 セットアップ プログラムでは、以下の入力を求めます。

   エンドユーザ使用許諾契約

   インストールを続行するには、使用許諾契約に同意します。

   インストール パス

   CA Virtual Systems Monitor を C:¥CA にインストールします。

   インストール タイプの選択

   Virtual Systems Monitor をクリックして CA Virtual Systems Monitor をインストールします。

4. セットアップ プログラムが完了したら、ゲスト オペレーティング システムを再起動する必要があります。
5. もう一度ゲスト オペレーティング システムにログインし、CA Virtual Systems Monitor が SPAN トラフィックを観測していることを確認 (P. 350)します。

時間を時間サーバに同期させる

異なるタイム ゾーンに 監視デバイス が存在する場合、各 CA Virtual Systems Monitor をそのローカル タイム ゾーンに設定し、NTP などの時間サーバを使用して時間が正確であるかを確認します。 時間はグリニッジ標準時（GMT）に変換されます。

次の手順に従ってください:

1. コマンド プロンプトを開き、以下のコマンドを実行します。
   ```
   net time /querysntp
   ```
   SNTP サーバ名を書きとめます。
2. 以下のコマンドの *<NTPServer>* をクエリで返された SNTP サーバ名に置き換えます。
   ```
   net time /setsntp:<NTPServer>
   ```
3. Windows Time Service が自動的に開始するように設定します。
4. コンピュータを再起動します。

セットアップの完了

以下のインストール後タスクを実行します。

1. CA Support Web サイト（http://support.ca.com）で、CA Virtual Systems Monitor のソフトウェア更新が行われていないかを確認します。
2. （オプション）重複したパケットをフィルタする (P. 378) ように CA Virtual Systems Monitor を設定します。
3. アンチウイルス ソフトウェアをインストールしますが、以下のディレクトリはスキャンから除外します。
   - C:¥Windows¥Temp
   - インストール ディレクトリ（デフォルトでは C:¥CA）およびそのすべてのサブディレクトリ。
4. システム時刻とタイム ゾーンを確認します。これらの値を変更する場合は、コンピュータを再起動します。

インストール後の手順

インストールが完了したら、管理コンソール に CA Virtual Systems Monitor を追加する準備ができています。 以下の点に注意してください。

- CA Virtual Systems Monitor の追加は、CA Standard Monitor を追加したときと同じ方法です。 CA Virtual Systems Monitor を追加するときは、CA Virtual Systems Monitor 上の管理および監視用 NIC の IP アドレスを提示します。
- CA Virtual Systems Monitor の管理は CA Standard Monitor の管理と同様です。ADA 監視デバイス リストを使用して、CA Virtual Systems Monitor 監視デバイス を表示および管理します。

  ADA 監視デバイス リストでは、CA Virtual Systems Monitor のタイプは CA Standard Monitor と同じ Standard Monitor です。 CA Virtual Systems Monitor と CA Standard Monitor を区別するには、CA Virtual Systems Monitor 上の管理 NIC のホスト名または IP アドレスを知っておく必要があります。
- Cisco WAE デバイスまたは CA GigaStor を CA Virtual Systems Monitor に割り当てないでください。

第 15 章: CA GigaStor による監視

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 GigaStor は監視デバイスとしてどのように機能するか (P. 390)
CA GigaStor 監視デバイスの追加 (P. 395)
CA GigaStor 入力ポートのブロック (P. 403)
CA GigaStor 監視デバイスの編集 (P. 404)
GigaStor 監視フィードの編集 (P. 405)
CA GigaStor の割り当て解除 (P. 407)
GigaStor Incidents (P. 408)
基本操作の実行 (P. 409)
CA GigaStor 監視デバイスの削除 (P. 410)
CA GigaStor 監視デバイスのトラブルシューティング (P. 411)

CA GigaStor は監視デバイスとしてどのように機能するか

CA GigaStor アプライアンス（CA GigaStor）は、一種の CA Application Delivery Analysis 用 監視デバイス として機能します。CA Application Delivery Analysis は、パフォーマンス問題の時間およびソースを特定し、CA GigaStor はその問題の根本原因を詳細に分析します。 CA GigaStor とは

- すべての IPv4 ベースのパケットをキャプチャする常時キャプチャ デバイスです。 複数の宛先インターフェースを持つ単一の SPAN セッションは、CA GigaStor および CA Standard Monitor が SPAN を共有できるようにします。 タップの必要はありません。
- CA Standard Monitor と異なり、CA GigaStor はパケット キャプチャのみに特化しており、複数の SPAN ポートから複数のインターフェース（8 つ以上）の TCP パケットを受信できます。
- 完全な通信分析および再構築用に全パケットをキャプチャします。
- 複数インターフェースの TCP ヘッダを組み合わせて、1 つの GigaStor 監視フィード にまとめます。

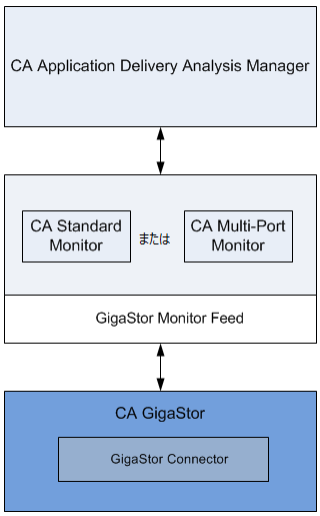
CA GigaStor コネクタにより、管理コンソール ユーザは、キャプチャされて CA GigaStor アプライアンスに保存された大量の IPv4 パケット データを迅速かつ容易に分析できます。それにより、ネットワーク エンジニアはネットワークやサーバの間をシームレスに移動でき、管理コンソール でのアプリケーション パフォーマンス ビューや CA Observer Expert での 徹底的なパケット検査によって、容易で迅速なトラブルシューティングが可能になります。

CA GigaStor コネクタの仕組み

CA GigaStor は、たとえば SPAN やミラー ポート、またはネットワーク タップから受動的にコピーされたすべてのパケットをキャプチャします。また、完全な通信分析や再構築用にも全パケットをキャプチャします。

CA GigaStor 上の CA GigaStor コネクタは、サーバ サブネット、クライアント ネットワークおよびポート除外のリスト用に 管理コンソール をポーリングします。 パケットは CA GigaStor 上のメモリ内にあり、それらがディスクに書き込まれる前に、CA GigaStor コネクタは一致する TCP ヘッダ データをパケット要約ファイルにコピーし、割り当てられている 監視デバイス に要約ファイルを送信します。 必要に応じて、CA GigaStor を複数の 監視デバイス に割り当てることができます。 CA GigaStor を CA Application Delivery Analysis Manager に割り当てることはお勧めしません。

CA GigaStor コネクタは、パケット要約ファイルを割り当て済み CA Standard Monitor または CA Multi-Port Monitor に送信し、各アプリケーション/サーバ/ネットワーク組み合わせに対するレスポンス時間メトリック処理および計算を行います。 CA GigaStor コネクタはレスポンス時間メトリックを計算しません。



パケット要約ファイルは 監視デバイス 上で GigaStor 監視フィード が受信します。 そして、管理コンソール がすべての 監視デバイス からのレスポンス時間メトリックを評価して、最適な 監視フィード を各サーバに割り当てるとともに、各サーバで最もビジーな TCP アプリケーションを監視します。

管理コンソール で監視するアプリケーションを定義し、CA GigaStor にこの設定をロードすることもできます。

詳細:

アプリケーションの管理 (P. 121)

監視フィード割り当ての仕組み

CA GigaStor が所定サーバにとって最適な監視ポイントである場合、管理コンソール は対応する GigaStor 監視フィード を自動的にそのサーバへ割り当てます。

負荷分散のために複数の CA Standard Monitor や CA Multi-Port Monitor に CA GigaStor を割り当てている場合、管理コンソール はサーバ割り当ての際 GigaStor 監視フィード を単一の 「論理」フィードとして扱います。 GigaStor 監視フィード を手動で割り当てるとき、いずれかの GigaStor 監視フィード をサーバに割り当てることができます。

詳細:

監視フィード割り当ての仕組み (P. 289)

パケット キャプチャ調査の仕組み

CA GigaStor 監視フィードがサーバに割り当てられているとき、管理コンソール はパケットを観測する対応の CA GigaStor からサーバ上でパケット キャプチャ調査を実行します。

管理コンソール が CA GigaStor 上でパケット キャプチャ調査を開始すると、管理コンソール は CA Observer Expert にシームレスなドリルインを提供します。 CA Observer Expert は、パフォーマンス問題の根本原因を特定するために、パケット レベルの詳細と専門家分析を提供します。

CA GigaStor 上では、もう 1 つのタイプの 監視デバイス で行うように、パケット キャプチャ調査を開始したりスケジュールを立てることができます。パケット キャプチャ調査レポートで、パケット キャプチャ調査レポートのリンクをクリックすると、CA Observer Expert フィルタが作成され、CA Observer Expert の CA GigaStor 上に希望するパケットを表示することができます。CA Standard Monitor 上のパケット キャプチャ調査と異なり、ユーザのローカル コンピュータにコピーするパケット キャプチャ ファイルはありません。

サイズ変更に関する推奨事項

CA GigaStor は、割り当て済みの 監視デバイス 上の管理 NIC にパケット要約ファイルを処理のため送信します。 CA GigaStor がどのようにロードされるかにもよりますが、少なくとも 1 つの 監視デバイス に CA GigaStor を割り当てるべきです。 1 つの 監視デバイス に複数の CA GigaStor を割り当てることはできません。

割り当て済み 監視デバイス 上の管理 NIC に過負荷をかけないようにするには、Cisco WAE デバイスなど別の 監視デバイス からもパケット要約を受信している 監視デバイス に CA GigaStor を割り当てないようにします。

監視デバイスに関する考慮事項

CA GigaStor を 監視デバイス として使用するときは、次の点に留意してください。

- 通常、CA 技術担当者は、ユーザが TCP トラフィックを 監視デバイス にミラーリングするための支援をします。

  注: データ取得のベストプラクティスの詳細については、「*インストール ガイド*」を参照してください。

- CA GigaStor 上でパケット キャプチャ調査を実行するために 管理コンソール を設定する場合、以下を指定する必要はありません。
  - 最大ファイル サイズ。 CA GigaStor がすべてのパケットをキャプチャして保存するので、キャプチャ ファイルはありません。したがって最大ファイル サイズは適用されません。 パケット キャプチャ調査によって、希望のパケットを表示するための CA Observer Expert フィルタが作成されます。
  - 1 パケットあたりのバイト数。 CA GigaStor は全パケットをキャプチャします。
- 秘密事項に関わる可能性があるキャプチャ内容へのアクセスを制限するには、CA GigaStor 上のパッシブ プローブ インスタンスへのユーザ権限を付与 (P. 396)します。
- CA GigaStor は、管理コンソール 上で定義されているクライアント ネットワーク、サーバ サブネットおよびポート除外に基づいて、一致するアプリケーション トラフィックを自動的に監視します。
- CA GigaStor コネクタはパケット要約ファイルを保存しないので、CA GigaStor コネクタが割り当て済みの CA Standard Monitor または CA Multi-Port Monitor と通信できない場合、管理コンソール は欠落データについてレポートします。 ただし、CA GigaStor は絶えず TCP パケットをキャプチャします。また、Observer を使用して CA GigaStor 上でデータを表示できます。
- 管理コンソール は、CA GigaStor コネクタから TCP ベースのパフォーマンス データを使用して、Web アプリケーションのパフォーマンスを監視できません。CA GigaStor コネクタからのパフォーマンス データには、Web アプリケーションの関連 URL を決定するのに必要な HTTP ヘッダ情報が含まれていません。

管理コンソールが CA GigaStor アプライアンスで Web アプリケーションを監視できるようにするには、すべての TCP-80 トラフィックを監視する標準アプリケーションを定義するか、または CA Observer Expert を使用して Web アプリケーションを監視します。

CA GigaStor 監視デバイスの追加

CA GigaStor を CA Application Delivery Analysis 用の 監視デバイス として追加するには、以下のタスクを実行します。

1. 必要なポート アクセスなど、前提条件を確認 (P. 396) します。
2. CA GigaStor アプライアンス上に必要なソフトウェアをインストールして設定 (P. 396) します。
3. CA GigaStor 監視デバイス を追加します。 (P. 398)
4. CA GigaStor を 監視デバイス に割り当て (P. 399) ます。
5. ユーザのクライアント コンピュータに必要な CA Observer ソフトウェアをインストール (P. 396) します。
6. CA GigaStor のパッシブ プローブ インスタンスにアクセスするための権限をユーザに付与 (P. 402) します。

前提条件

CA GigaStor 監視デバイス を追加するための前提条件は以下のとおりです。

- CA GigaStor に CA Observer ソフトウェアがインストールされていること。 コネクタをアップグレードする場合は、CA サポート Web サイト（http://ca.com/support）から CA Observer アップグレード プログラムをダウンロードできます。
- CA GigaStor 上の日時が、割り当てられた CA Standard Monitor または CA Multi-Port Monitor 上の日時設定に一致するように設定されていること。

  CA GigaStor によって収集されたパフォーマンス データが、割り当てられた 監視 のタイム スタンプを使用して日時が記録されていること。 ネットワーク タイム プロトコル（NTP）を使用するように 監視 を設定した場合は、CA GigaStor 上で NTP を設定します。
- 監視デバイス比率 (P. 300)が正しくサイズ設定されていること。
- CA Standard Monitor または CA Multi-Port Monitor を利用して、CA GigaStor コネクタからの要約ファイルをレスポンス時間データに処理できます。 CA Standard Monitor 上の使用可能リソースを最大化するには、CA Standard Monitor を追加 (P. 331)するときに、パケット監視を無効にします。
- 管理コンソール が TCP-1001 上の CA GigaStor と通信できること。
- CA GigaStor が、UDP-9995 上の割り当て済みの CA Standard Monitor または CA Multi-Port Monitor と通信できること。
- CA GigaStor 上のパケット キャプチャ調査を開始する 管理コンソール ユーザは、TCP-25901 ～ TCP-25903 上の CA GigaStor と通信できること。
- TCP-3389 上で Windows Terminal Services（RDP）でリモート デスクトップによって CA GigaStor にアクセスできること。

GigaStor アプライアンスでのソフトウェアのインストールと設定

以下のタスクを実行して、必要なソフトウェアをインストールします。

- CA GigaStor Connector を CA GigaStor アプライアンス上にインストールします。
- 各 管理コンソール ユーザに対して CA GigaStor 上でパッシブ プローブ インスタンスを作成します。

CA Gigastor Connector のインストール

CA GigaStor アプライアンスを CA Application Delivery Analysis 用の監視デバイスとして使用するため、CA GigaStor Connector を GigaStor アプライアンス上にインストールします。 このコネクタのバージョン番号は、CA Observer のバージョンに一致している必要があります。正しいバージョンをダウンロードするには、CA サポート にお問い合わせください。

GigaStor Connector をインストールするには、Connector セットアップを GigaStor デスクトップ上で実行します。セットアップが完了したら再起動します。

各ユーザのパッシブ プローブ インスタンスの作成

管理コンソール ユーザが CA GigaStor のパケット キャプチャの調査を開くことができるようにするには、CA GigaStor へのアクセスを許可する 管理コンソール ユーザごとに、パッシブ プローブ インスタンスを作成します。

誤って CA Observer Expert から 管理コンソール ユーザが切断されないように、管理コンソール ユーザ間のパッシブ プローブ インスタンスを共有させないようにします。 すでに使用中の CA GigaStor プローブ インスタンスを使って、管理コンソール ユーザが CA GigaStor パケット キャプチャの調査を開くと、既存のユーザが CA GigaStor から切断されます。

CA GigaStor のパッシブ プローブ インスタンス作成の詳細については、CA GigaStor 製品マニュアルを参照してください。

CA GigaStor 監視デバイスの追加

管理コンソール のデータ ソースとして CA GigaStor 監視デバイス を追加します。 ドメインごとに重複した IP トラフィックを分離する必要がある場合は、CA GigaStor を追加した後、GigaStor 監視フィード を編集 (P. 405) して希望のドメインに GigaStor 監視フィード を割り当てます。

CA GigaStor を追加した後、CA GigaStor を 監視デバイス に割り当て (P. 399) ます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［表示項目］メニューの［GigaStor の追加］をクリックします。

   ［GigaStor のプロパティ］が表示されます。
4. ［GigaStor のプロパティ］内のフィールドに入力し、［OK］をクリックします。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

監視デバイスへの CA GigaStor の割り当て

管理コンソールに CA GigaStor を追加した後、CA Standard Monitor または CA Multi-Port Monitor にそれを割り当てて、CA GigaStor コネクタからの要約ファイルをレスポンス時間データに処理します。 CA GigaStor を CA Virtual Systems Monitor に割り当てないでください。

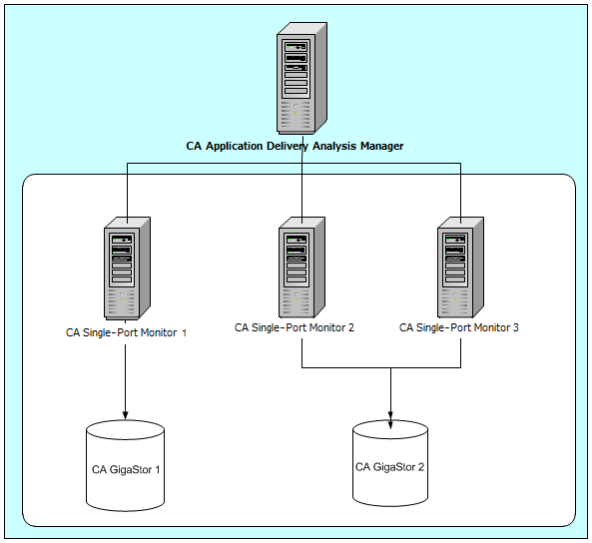
CA Standard Monitor 上の使用可能リソースを最大化するには、CA Standard Monitor を追加 (P. 331)するときに、パケット監視を無効にします。

スケーラビリティ上の理由により単一の CA GigaStor から 監視フィードを負荷分散させるため、CA GigaStor を複数の CA Standard Monitor または CA Multi-Port Monitor に割り当てます。 2 つの 監視デバイス の間で CA GigaStor を負荷分散させるとき、CA GigaStor コネクタは、自動的にエンドポイントの 1 つの IP アドレスに基づいて各 監視デバイス にトラフィックを分散させます。

- サーバ IP アドレス（クライアント/サーバ接続の場合）
- 最小の IP アドレス（多層アプリケーション、サーバ/ サーバ接続の場合）

CA GigaStor コネクタは、IP アドレスが偶数であるサーバからのトラフィックのパケット要約ファイルをある 監視デバイス に送信し、奇数 IP アドレスのサーバからのトラフィックを他に送信します。

以下の例のように、CA GigaStor を複数の CA Standard Monitor または CA Multi-Port Monitor に割り当てることができます。



展開が単一の 管理コンソール および CA GigaStor から構成されている場合は、CA GigaStor を 管理コンソール 上の 監視 に割り当てます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして、CA GigaStor を割り当てる CA Standard Monitor または CA Multi-Port Monitor を編集します。 ［アクティブ フィード］列を使用して、CA GigaStor が 監視 に割り当てられるかどうかを判定します。
4. 3 番目の［表示項目］メニューで［監視デバイス］をクリックします。

   ［監視デバイス］が表示されます。
5. GigaStor デバイス リストから CA GigaStor をクリックし、［OK］をクリックします。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細情報:

CA Standard Monitor による監視 (P. 321)
GigaStor アプライアンスでのソフトウェアのインストールと設定 (P. 396)

ユーザのコンピュータへの CA Observer のインストール

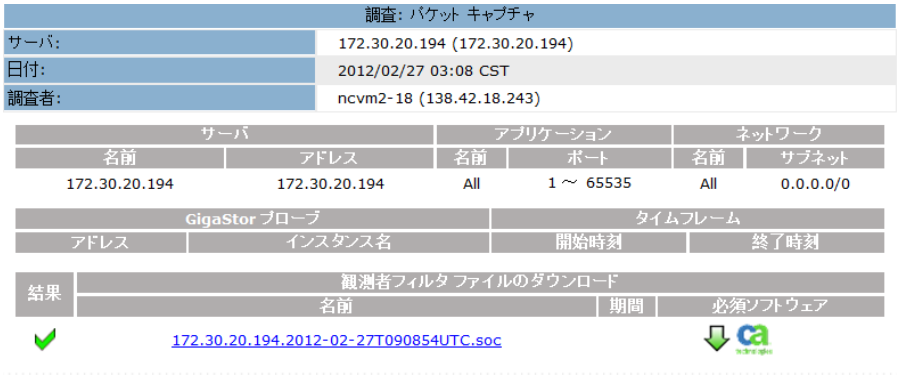
管理コンソール ユーザが CA GigaStor のパケット キャプチャの調査を開くことができるようにするには、ユーザのコンピュータに以下のソフトウェア コンポーネントをインストールする必要があります。

- CA Observer Expert。 CA GigaStor の CA Observer Expert では、CA Application Delivery Analysis からのグローバル アプリケーション レスポンス時間の監視を拡張して、根本原因解析のためにパケット レベルのデータへのドリルダウンを提供します。

  CA Observer Expert は、TCP-25901 ～ TCP-25903 上で CA GigaStor に接続できる必要があります。 管理コンソール コンピュータへの CA Observer Expert のインストールとライセンスの詳細は、CA GigaStor 管理者にお問い合わせください。CA Observer Expert Connector と異なり、ユーザは 管理コンソール から CA Observer Expert をインストールできません。

- CA Observer Expert Connector。 管理コンソール ユーザが初めて CA GigaStor のパケット キャプチャ調査を開く場合には、パケット キャプチャ調査のレポートに CA Observer Expert Connector のインストールを促すリンクが表示されます。

  ［必須ソフトウェア］の下の矢印リンクをクリックして、コネクタ セットアップ プログラムを実行します。



調査: パケット キャプチャ	
サーバ:	172.30.20.194 (172.30.20.194)
日付:	2012/02/27 03:08 CST
調査者:	ncvm2-18 (138.42.18.243)

サーバ		アプリケーション		ネットワーク	
名前	アドレス	名前	ポート	名前	サブネット
172.30.20.194	172.30.20.194	All	1 ～ 65535	All	0.0.0.0/0

GigaStor プローブ		タイムフレーム	
アドレス	インスタンス名	開始時刻	終了時刻

結果	観測者フィルタ ファイルのダウンロード		
	名前	期間	必須ソフトウェア
✔	172.30.20.194.2012-02-27T090854UTC.soc		

パッシブ プローブ インスタンスに対する権限の付与

管理コンソール ユーザが CA Observer の CA GigaStor でパケット キャプチャの調査を開くことができるようにするには、CA GigaStor のパッシブ プローブ インスタンスへの権限を CA Application Delivery Analysis ユーザに付与します。

CA GigaStor に複数のアクティブなプローブ インスタンスがある場合は、適切なアクティブ プローブ インスタンスに対応するパッシブ プローブ インスタンスへのユーザ権限を与えます。 同じ CA GigaStor 上の複数のパッシブ プローブ インスタンスに 管理コンソール ユーザ権限を与えることはできません。 デフォルトでは、管理コンソール は CA GigaStor の最初のアクティブなプローブ インスタンスに接続します。 管理コンソールによって CA GigaStor の別のアクティブ インスタンスへに接続できるようにするには、CA サポート にお問い合わせください。

プローブ インスタンス管理の詳細については、CA GigaStor 製品マニュアルを参照してください。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［セキュリティ］-［GigaStor インスタンス］をクリックします。

   ［ユーザ別 GigaStor インスタンス］が表示されます。

   ［GigaStor インスタンス］コマンドが表示されない場合は、少なくとも 1 つの CA GigaStor が 管理コンソール に追加 (P. 398)されていることを確認してください。
3. をクリックして 管理コンソール ユーザを編集します。

   <user> の GigaStor インスタンスが表示されます。
4. 管理コンソール ユーザが CA GigaStor でアクセスするパッシブ インスタンス名を入力し、［OK］をクリックします。

   ［ユーザ別 GigaStor インスタンス］で、［GigaStor デバイス [インスタンス名]］列が更新され、GigaStor のパッシブ インスタンス名が表示されます。

CA GigaStor 入力ポートのブロック

予想される観測の 2 倍の数および 2 倍長の NRTT があることに気付いた場合、CA GigaStor デバイス上で選択された監視ポートからすべてのパケットを除外しなければならない可能性があります。 ポートをブロックする機能は多層環境で監視する効果的な方法です。 別のポートが、他の有利なポイントから同じサーバ トラフィックをレポートするように CA GigaStor を設定した場合、たとえばアクセス スイッチと分散スイッチの場合は、分散スイッチからデータを除外し、アクセス スイッチから収集されたパケットの重複としてそれらのパケットが表示されることはありません。

次の手順に従ってください:

1. CA GigaStor にログインします。
2. C:¥NetQoS¥GigaStorReader にディレクトリを変更してから、BlockedGigaStorPorts.ini という名前のファイルを作成します。
3. BlockedGigaStorPorts.ini を開き、以下の形式でエントリを追加します。
   `/exclude port=`*`port`*

   *ポート*の値がゼロから 7 の範囲にある場合、それは CA GigaStor インターフェースの 1 ～ 8 の範囲に対応します。 CA GigaStor の複数の入力ポートを指定するには、カンマで各エントリを区切ります。

CA GigaStor 監視デバイスの編集

CA GigaStor 監視デバイス の編集は、たとえば下記の場合に必要です。

- CA GigaStor アプライアンスの CA GigaStor コネクタおよび CA Observer Expert ソフトウェアのバージョン情報を表示する。
- 割り当てられた 監視 にパケット要約ファイルを送信する CA GigaStor のプロセスのステータスを表示する。
- 監視デバイス にインシデントのレスポンスを割り当てる
- CA GigaStor コネクタの開始および停止などの特定の CA GigaStor の基本的な処理を実行する。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. をクリックして、GigaStor デバイス リスト 内の CA GigaStor を編集します。

   ［GigaStor のプロパティ］が表示されます。
4. ステータス情報を確認し、指定された設定に変更を加えて、［OK］をクリックします。

   CA GigaStor プロパティの設定の詳細については、［ヘルプ］をクリックしてください。

   CA GigaStor に対する 監視デバイス インシデントを表示するには、3 番目の［表示項目］メニューで［インシデント］をクリックします。

詳細:

監視デバイス インシデントの表示 (P. 306)

GigaStor 監視フィードの編集

*GigaStor 監視フィード*は CA GigaStor 監視デバイス からパケット要約ファイルを受信します。GigaStor 監視フィード の編集は、下記の場合に必要です。

- 特定のドメインを割り当てる。デフォルトでは、新規の 監視フィードは「デフォルト ドメイン」に割り当てられます。 重複する IP トラフィックを分けるためにドメインを使用していない場合には、適用されません。
- 監視フィード のペアを作成して、管理コンソール が両方の 監視フィード から割り当て済みサーバのデータを自動的に収集できるようにする。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］の［アクティブ フィード］列を参照して、アクティブな GigaStor 監視フィード のある 監視デバイス を検索します。
4. をクリックし、監視デバイス を編集します。

   編集対象の 監視デバイス が明確でない場合、［GigaStor デバイス リスト］の［割り当て先］列で、CA GigaStor が割り当てられた 監視デバイス を検索します。
5. 監視デバイス のプロパティ ダイアログ ボックスで、［監視フィード］までスクロールします。
6. をクリックし、GigaStor 監視フィード を編集します。
7. GigaStor 監視フィード 設定に変更を加えて、［更新］をクリックします。

   GigaStor 監視フィード プロパティの設定の詳細については、［ヘルプ］をクリックしてください。
8. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
監視フィードのペアの作成 (P. 291)
監視デバイスの動作 (P. 287)

CA GigaStor の割り当て解除

CA GigaStor の割り当てを解除して、レスポンス時間データのソースとして削除されるようにします。 監視デバイスの割り当てを解除すると、対応する監視フィードに固定されていたすべてのサーバは固定が解除され、別の監視フィードが自動的に割り当てられます。 監視フィードの割り当てを更新するのに 10 分程度かかる可能性があります。

GigaStor 監視フィードにサーバを固定しており、GigaStor が一時的に割り当て解除されている間もサーバ トラフィックの監視を続行するには、以下のオプションを考慮します。

- GigaStor の割り当てを解除する前に、別の監視フィードにサーバを固定します。 GigaStor を再割り当てする場合、GigaStor 監視フィードに適切なサーバを固定します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして、CA GigaStor が割り当てられている CA Standard Monitor または CA Multi-Port Monitor を編集します。
4. 3 番目の［表示項目］メニューで［監視デバイス］をクリックします。
5. ［割り当て済みデバイス リスト］で をクリックして、CA GigaStor の割り当てを解除します。
6. プロンプトで［割り当て解除を続行］をクリックして処理を続行します。

   管理コンソールは［割り当て済みデバイス リスト］を更新します。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

GigaStor Incidents

CA GigaStor において以下の状況の場合、管理コンソール は自動的にメジャー 監視デバイス インシデントを作成します。

- 1 時間を超えて 管理コンソール へのデータ送信を停止している
- 受信パケットの 5 パーセント以下しか処理していない

詳細:

監視デバイス インシデントのしきい値の編集 (P. 307)

基本操作の実行

CA GigaStor デバイス リストで、青い歯車型メニュー（ ）を使用して、すべての CA GigaStor アプライアンスで基本操作（CA GigaStor コネクタの開始および停止、モニタリングの同期など）を実行します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. GigaStor デバイス リストで、青い歯車型メニュー（ ）をクリックして、すべての CA GigaStor アプライアンスで基本操作を実行します。基本操作を実行するには、リストを参照して編集アイコン( )をクリックし、青い歯車型メニュー（ ）をクリックします。

   開始

   コネクタを開始します。 コネクタには実行中ステータスがありますが、これはパケット要約ファイルを 管理コンソール レポートの割り当て済み 監視 に送信します。

   停止

   コネクタを停止します。 コネクタが停止ステータスになっている間、CA GigaStor はディスクにパケットを書き込み続けます。しかし、コネクタは割り当て済み 監視 にパケット要約ファイルを送信しません。 管理コンソール レポート内のデータ ギャップは、CA Observer Expert を使用して CA GigaStor 上の実際のデータを参照することにより解決できます。

   監視デバイスを同期

   CA GigaStor を同期して、「コンソール」で現在定義されているクライアント ネットワーク、サーバ サブネットおよびアプリケーションに基づいてパフォーマンス データを収集します。

詳細:

監視デバイス同期の動作 (P. 290)

CA GigaStor 監視デバイスの削除

CA GigaStor 監視デバイス を削除して、管理コンソール のレスポンス時間のデータのソースとしてそれを削除します。 監視デバイス として CA GigaStor を使用しなくなった場合は、その割り当て済みの 監視 から CA GigaStor の割り当てを解除し、次に、CA GigaStor を削除します。

または、別の CA Standard Monitor または CA Multi-Port Monitor に、CA GigaStor を割り当てる (P. 399)こともできます。

詳細情報:

監視デバイスへの CA GigaStor の割り当て (P. 399)

CA GigaStor の削除

CA GigaStor を削除して、管理コンソール のレスポンス時間データのソースとしてそれを削除します。

CA GigaStor を削除する場合、それを CA Standard Monitor または CA Multi-Port Monitor に割り当てることができません。 CA GigaStor の割り当てを解除した後、管理コンソール から CA GigaStor を削除 (P. 407) します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. をクリックして、GigaStor デバイス リスト から CA GigaStor を削除します。
4. プロンプトで［削除を続行］をクリックして、CA GigaStor を削除します。

   CA GigaStor が GigaStor デバイス リストから削除されます。
5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

CA GigaStor 監視デバイスのトラブルシューティング

CA GigaStor の監視対象であるレポート データ欠落の原因を特定するために、CA GigaStor のトラブルシューティングを行います。 CA GigaStor 監視デバイス を追加した後、10 分以内で 管理コンソール からパフォーマンス データがレポーティングされます。

GigaStor 監視フィードのアクティブ セッション数の表示

［アクティブ セッション数］ページを使用して、直近の 5 分間のレポート間隔で GigaStor 監視フィードによってレポートされたアクティブな IPv4 ベースの TCP セッション数をレポートします。GigaStor 監視フィードには、監視デバイスに割り当てられるあらゆる CA GigaStor アプライアンスからのセッション情報が含まれます。

アクティブ セッション情報を表示 (P. 293)して、監視フィードが TCP セッションを監視していることを確認します。管理コンソールは、アプリケーション ポートのサーバ上のアクティブな TCP セッション数をレポートします。 監視フィードにサーバまたはアプリケーションのアクティブ セッションがない場合、CA GigaStor の設定に問題があります。

GigaStor カウンタ統計の表示

GigaStor カウンタは、割り当て済みの CA GigaStor コネクタから受信するパケット要約の情報を表示します。これらの情報には、パケット要約を転送する Netflow パケットに関する情報も含まれます。

GigaStor カウンタを表示するには、CA GigaStor が割り当てられる CA Standard Monitor にログイン (P. 348) します。

重要: 開始前に、監視デバイスを同期します。 データ監視の同期が完了するまで、カウンタ ウィンドウは表示されません。

GigaStor カウンタは以下の統計を表示します。

良好なフロー

Netflow パケットの送信順に受信される パケット数を示します。

ドロップされたフロー

CA ADA Monitor サービスで処理されなかった Netflow パケット数を示します。 ドロップされた Netflow パケット内に含まれていたパケット要約のレスポンス時間データは、管理コンソール レポートに含まれません。

順不同フロー

Netflow パケットは 監視 で受信されましたが、送信順では受信されなかった Netflow パケット数を示します。

サーバへのパケット数

クライアントからサーバへ送信された、パケット数を示します。

サーバからのパケット数

サーバからクライアントへ送信された、パケット数を示します。

サーバへのバイト数

クライアントからサーバへ送信された、バイト数を示します。

サーバからのバイト数

サーバからクライアントへ送信された、バイト数を示します。

参照されたパケット総数

CA GigaStor コネクタによって検査されたパケット数を示して、パケット ヘッダが指定のアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットと一致したかどうかを判定します。

キャプチャされたバイト総数

指定したアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総バイト数を示します。

注: 監視 は各パケット ヘッダを検査して、指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットにパケットが一致するかどうかを判定します。 詳細については、「参照されたパケット総数」を参照してください。

承認済みセッション数

管理コンソール で有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッション数を示します。

サーバ関連の拒否

サーバ IP が、管理コンソール によって監視されるサーバ サブネットに一致しなかったことを示します。

クライアント関連の拒否

クライアント IP が、管理コンソール によって監視されるクライアント ネットワークのリストに一致しなかったことを示します。

ポート関連の拒否

サーバ ポートが 管理コンソール で拒否するポート リストに一致したことを示します。

ポジティブ関連の拒否

将来の使用に備えて予約されています。

詳細情報:

クライアント ネットワークの仕組み (P. 34)
アプリケーションの仕組み (P. 122)
サーバの仕組み (P. 79)

第 16 章: Cisco WAAS による監視

このセクションには、以下のトピックが含まれています。

監視デバイスとしての Cisco WAAS の動作方法 (P. 416)
Cisco WAE 監視デバイスの追加 (P. 424)
Cisco WAE 監視デバイスの編集 (P. 430)
WAN 最適化監視フィードの編集 (P. 431)
Cisco WAE の割り当て解除 (P. 433)
WAAS Incidents (P. 433)
Cisco WAE 監視デバイスの削除 (P. 434)
Cisco WAE 上のフロー監視の無効化 (P. 435)
最適化アプリケーションのリセット (P. 437)
Cisco WAE 監視デバイスのトラブルシューティング (P. 438)
Cisco WAE デバイス グループによるサーバの監視 (P. 443)
管理コンソール間の最適化データの共有 (P. 447)

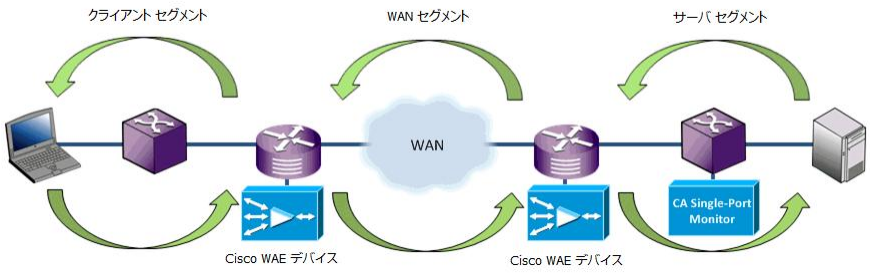
監視デバイスとしての Cisco WAAS の動作方法

Cisco WAE デバイス（Cisco WAE）は CA Application Delivery Analysis の 監視デバイス の 1 タイプとして機能します。Cisco WAE デバイスを使用すると、最適化を可視化できます。 サーバ SPAN を監視する 監視デバイス と異なり、Cisco WAE デバイスはネットワーク上に分散されます。

Cisco WAE デバイス間の WAN 最適化を監視すると、Cisco WAAS 最適化がネットワークの各セグメントでどのように個別のアプリケーション レスポンス時間に影響するかを確認できます。

以下の例では、ブランチおよびデータ センターにある Cisco WAE デバイスから、最適化されたアプリケーション パフォーマンス データが CA Standard Monitor に送信されています。 CA Standard Monitor では以下を実行します。

- クライアントおよび WAN セグメント上の最適化されたトラフィックのパフォーマンス メトリックを計算します。
- データ センターの WAE からのサーバ セグメント パフォーマンス データを、サーバのミラーリング スイッチ ポートから CA Standard Monitor によって収集された、より正確なパフォーマンス データに置換します。
- 自動的に、サーバ SPAN のアプリケーション トラフィックを監視し、すべての 監視デバイス によって監視されるサーバ リストで 管理コンソール を更新します。



Cisco WAAS 環境を監視するには、サーバのミラーリング スイッチ ポートを監視する必要はありません。

詳細情報:

監視デバイスに関する考慮事項 (P. 423)

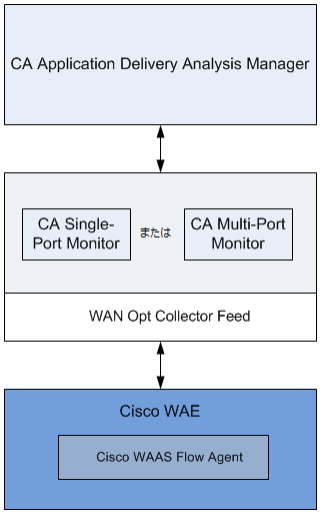
Cisco WAAS の仕組み

Cisco WAE デバイス上の Cisco WAAS Flow Agent は、監視する サーバ IP アドレスのリストに対して 5 分ごとに 管理コンソール をポーリングします。 Cisco WAAS Flow Agent は、最適化されたトラフィックの一致する TCP ヘッダを持つパケット要約ファイルを、その割り当て済み CA Standard Monitor または CA Multi-Port Monitor に送信します。 分散 管理コンソール は必須です。

パケット要約ファイルは、CA Standard Monitor または CA Multi-Port Monitor の「WAN 最適化」監視フィード で受信され、そこで監視対象のアプリケーション/サーバ/ネットワークの各組み合わせのレスポンス時間メトリックへと処理されます。

Cisco WAAS Flow Agent は、管理コンソール に保存されているサーバのリストに基づいてアプリケーション トラフィックを監視します。 Cisco WAAS Flow Agent で自動的に新しいサーバ トラフィックを監視できるようにするには、追加の 監視デバイス でサーバ SPAN を監視する必要があります。

Cisco WAAS Flow Agent では、最適化されていないトラフィックの TCP ヘッダは送信せず、レスポンス時間メトリックは計算されません。



Cisco NAM Metric Agent とは異なり、Cisco WAAS Flow Agent は以下を送信します。

- 計算されたレスポンス時間メトリックではなく TCP ヘッダが含まれるパケット要約ファイル。
- すべての最適化されたトラフィックではなく、サーバ リストに一致する最適化されたトラフィックの TCP ヘッダ。

監視フィード割り当ての仕組み

管理コンソール は自動的に、すべての Cisco WAE デバイスからのレスポンス時間メトリックを結合して、各ネットワーク セグメント上のアプリケーションのレスポンス時間を計算します。サーバ SPAN を監視している監視 があり、その 監視 がサーバの最も近くにある場合、管理コンソールは、サーバ セグメントを監視するためにその 監視フィード を割り当てます。それ以外の場合には、管理コンソール は WAN 最適化 監視フィード をサーバに割り当てます。

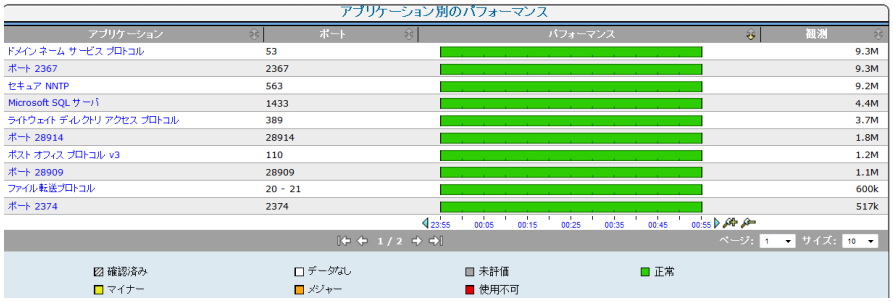
ネットワーク セグメントの動作方法

管理コンソール では、アプリケーション-サーバ-ネットワークの単一の組み合わせに対してネットワーク上の複数のポイントから監視しているため、管理コンソール は 3 つのネットワーク セグメントのそれぞれに対して個別のメトリック セットを生成し、別個のアプリケーションとして各ネットワーク セグメントを処理します。 管理コンソール では以下のメトリックのセットをそれぞれ個別に生成します。

- クライアント セグメント。ブランチにあるクライアント IP とブランチ WAE デバイス間のネットワーク セグメントです。 このネットワーク セグメントをレポートするには、管理コンソール は、レスポンス時間データをエクスポートするブランチ WAE デバイスを必要とします。
- WAN セグメント。ブランチ WAE デバイスとデータ センター WAE デバイスとの間のネットワーク セグメントです。 このネットワーク セグメントをレポートするには、管理コンソール は、レスポンス時間データをエクスポートするデータ センター WAE デバイスを必要とします。
- サーバ セグメント。データ センター WAE デバイスとデータ センター サーバ間のネットワーク セグメントです。 このネットワーク セグメントをレポートするには、管理コンソール は、レスポンス時間データをエクスポートするデータ センター WAE デバイスを必要とします。

  監視デバイス を使用して、サーバ SPAN を監視する場合、管理コンソール はデータ センター Cisco WAE からのサーバ セグメント データをより正確なサーバ SPAN データに置換します。 それは、サーバの SPAN ソースが実際のサーバに近いため、より正確です。管理コンソール が、サーバ SPAN 内の最適化されていないアプリケーション トラフィックを参照する場合は、最適化されていないアプリケーション（たとえば SMTP）のメトリックのセットを個別に生成します。

管理コンソール はネットワーク セグメントをアプリケーション名に追加します。たとえば、SMTP [Client]、SMTP [WAN]、SMTP [Server] のようになります。 以下の例では、SMTP アプリケーションは最適化されていないアプリケーションのパフォーマンスを示します。 データがデータ センター内のローカル ユーザからくるため、最適化されていないアプリケーション レスポンス時間がより速くなっていることに注意してください。



WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の動作方法

管理コンソール では個別のアプリケーションを作成して、ネットワークのクライアント、WAN、およびサーバ セグメントのアプリケーション パフォーマンスについてレポートします。 各ネットワーク セグメントのアプリケーション パフォーマンスしきい値をカスタマイズし、パフォーマンス変動に対する 管理コンソール の感度を増減させます。

詳細情報:

WAN 最適化ネットワーク セグメントのパフォーマンスしきい値の編集 (P. 186)

最適化停止時における監視の仕組み

最適化の中断時間の長さに応じて、管理コンソール では、影響を受けるトラフィックに対して異なるレポーティング方法を使用します。 必要に応じて 管理コンソール をリセットして、最適化の最新の変更を無視し、現在利用可能な最適化情報に基づいて、最適化トラフィックおよび最適化されていないトラフィックをレポートすることができます。 詳細については、以下のセクションを参照してください。

一時的な中断

管理コンソール が Cisco WAE からのセグメント化されたアプリケーション パフォーマンス データの受信を一時的に停止した場合、管理コンソール は、最適化されていないサーバ SPAN からのデータを使用して、サーバ セグメントのアプリケーションについてレポートします。 管理コンソール では複数の基準を使用して、中断が一時的か永続的かを判定しますが、一時的な中断は通常 20 分以内です。

管理コンソール で一時的に、サーバ セグメントにおけるサーバのミラーリング スイッチ ポートからくる、最適化されていないアプリケーション データをレポートしているときには、以下の状態となります。

- ［最適化］ページのすべてのメトリックは正確です（ただし、すべてのメトリックの入力があるとは限りません）。
- 最適化されていないセッションの測定はクライアントまたは WAN のセグメントに影響しません。
- 管理コンソール では常にサーバのミラーリング スイッチ ポートからのより正確なデータを使用するので、サーバ セグメントは正確です。
- 「ネットワーク ラウンドトリップ時間 [Server]」が［エンジニアリング］ページに表示されます。ここでは 100% のローカル ACK を取得しないために増大を示します。 あふれ測定によって、実際のネットワーク ラウンドトリップ時間がクライアントに示されます。
- RetransDelay ［Server］および PacketLossPct ［Server］もまた増大を示す可能性があります。

最適化データが再開すると、管理コンソール では自動的にアプリケーションのクライアント、WAN、およびサーバの各セグメントのセグメント化されたアプリケーション データをレポートします。

最適化された監視において、たとえば以下の場合に一時的な中断が起こります。

- 最適化の停止。これは、追加のセッションの最適化に際して Cisco WAE にリソースがない場合に起こります。 最適化されていないセッションは*あふれ*と呼ばれます。
- 監視の停止。 これは、CA Standard Monitor または CA Multi-Port Monitor が、割り当てられた Cisco WAE からくるパケット要約の受信を停止したときに起こります。たとえば、Cisco WAE デバイスとその割り当て済み 監視デバイス との間のリンクが中断したり、Cisco WAE がレスポンス時間データをエクスポートするよう設定されていない場合などです。

恒久的な変更

管理コンソール では複数の基準を使用して、中断が一時的か永続的かを判定しますが、Cisco WAE がセグメント化されたアプリケーション パフォーマンス データの送信を 20 分以上停止した場合、管理コンソール は中断が永続的であるとみなします。 この場合、管理コンソール は、アプリケーションのサーバ セグメントのミラーリング スイッチ ポートからくる最適化されていないトラフィックのレポーティング、たとえば HTTP [Server] を停止します。代わりに最適化されていないアプリケーション HTTP の SPAN データをレポーティングします。 最適化が再開すると、管理コンソール は自動的にネットワーク セグメントの最適化アプリケーションの監視を再開します。

WAAS の最適化を設定しているときや（たとえば、異なるアプリケーションの最適化の利点を測定するため）、最適化の変更を直ちに 管理コンソール によってレポーティングさせたいときは、管理コンソール をリセット (422P. , 437P.)することができます。

サイズ変更に関する推奨事項

Cisco WAE デバイスは、パケット要約ファイルを、その割り当て済み CA Standard Monitor または CA Multi-Port Monitor の Management NIC に送信して処理します。

CA Standard Monitor または CA Multi-Port Monitor では、少なくとも 50,000 の最適化された接続に対して 3 セグメントすべて（クライアント、WAN、サーバ）からのパケット要約ファイルを処理できます。 可能な限り、同一の 監視 に複数のデータ センター WAE を割り当てないようにします。利用可能な CA Standard Monitor または CA Multi-Port Monitor 間でブランチ Cisco WAE デバイスの負荷を分散します。

CA Standard Monitor または CA Multi-Port Monitor 上の Management NIC が過負荷にならないようにするには、CA GigaStor からくるパケット要約も受信する 監視 に Cisco WAE デバイスを割り当てないようにします。

監視デバイスに関する考慮事項

監視デバイス として Cisco WAE を使用する際、次の点に注意します。

- 管理コンソール は、クライアント ネットワーク セグメント上のアプリケーション レスポンス時間をエクスポートするために、ブランチ WAE デバイスを必要とします。必要に応じて、データ センター WAE デバイスを使用するだけで、WAN およびサーバ セグメントにわたる 管理コンソール に対して、アプリケーション パフォーマンスをレポーティングすることができます。
- 管理コンソール では、以下に対するネットワーク セグメントによってアプリケーション パフォーマンスをレポートすることができません。
  - FTP アプリケーション。Cisco WAAS で FTP が最適化されないため。
  - URL による Web アプリケーション。 別の方法として、「標準」アプリケーションを定義して、クライアント、WAN および サーバ セグメントにおいてすべての TCP-80 トラフィックを監視することができます。
- Cisco WAE デバイスとその割り当て済み CA Standard Monitor または CA Multi-Port Monitor との間で通信が中断された場合、Cisco WAAS Flow Agent では一時的にそのパケット要約ファイルを格納して、レポーティング データの喪失を回避します。
- Cisco WAAS Flow Agent は、監視するサーバ IP アドレスのリストに対して、5 分ごとに 管理コンソール をポーリングします。

  Cisco WAE デバイスが、サーバ サブネットに一致する新規サーバ トラフィックを監視できるようにするには、CA Multi-Port Monitor などのサーバ SPAN を監視するように 監視デバイス を設定します。 レスポンス時間データを収集するために Cisco WAE デバイスのみを使用している場合は、手動でコンソールを更新し、監視するサーバ IP アドレスを追加します。

  管理コンソール によって監視されるサーバのリストを表示するには、［表示項目］リストで［データ監視］-［サーバ］をクリックします。
- Cisco WAE デバイスは、最適化されていない、パススルー トラフィックに関するパフォーマンス情報をキャプチャしません。パススルー アプリケーションに対するアプリケーション パフォーマンスを監視するには、CA Multi-Port Monitor などの、サーバ SPAN を監視するための監視デバイス を設定します。

- Cisco WAE デバイスは重複データを認識し、それを除去します。したがって、CA Standard Monitor または CA Multi-Port Monitor を設定して「WAN 最適化」 監視フィードから重複パケットを除去する必要はありません。
- パケット キャプチャ調査を、Cisco WAE デバイスから実行することはできません。ただし、たとえば CA Multi-Port Monitor で、サーバ SPAN を監視する場合、管理コンソール はこのデバイスを使用してパケット キャプチャを行います。

Cisco WAE 監視デバイスの追加

管理コンソール に Cisco WAE 監視デバイス を追加するには、以下のタスクを実行します。

1. アプリケーション レスポンス時間データをエクスポートするよう Cisco WAE デバイスを設定 (P. 426) します。
2. CA Standard Monitor または CA Multi-Port Monitor に Cisco WAE を割り当てます (P. 428)。
3. Cisco WAE デバイスが監視するサーバのリストに対して CA Application Delivery Analysis Manager をポーリングし、管理コンソール に最適化アプリケーションのデータを表示するまで、最大で 10 分ほど待機します。

   必要に応じて、Cisco WAE デバイスのトラブルシューティング (P. 438) を行い、Cisco WAE デバイスが最適化されたアプリケーションを監視していることを確認します。

前提条件

Cisco WAE 監視デバイスを追加するには、以下の前提条件を満たしている必要があります。

- Cisco WAE で、Cisco WAAS ソフトウェアのサポートされたバージョンを実行している。管理コンソール は Cisco WAAS 4.0.17 ～ 4.4.3a をサポートし、パケット要約ファイルを以下に送信します。
  - CA Standard Monitor
  - CA Multi-Port Monitor
- 時間と日付が、各 Cisco WAE、および割り当てられた CA Standard Monitor または CA Multi-Port Monitor で同じ。 Cisco WAE によって収集されたパフォーマンス データの時間は、デバイスのタイム スタンプを使用して得られます。 管理コンソール を設定して「ネットワーク タイム プロトコル」（NTP）を使用する場合、WAAS Central Manager を使用して Cisco WAE デバイスで NTP を設定します。 詳細については、「Cisco Wide Area Application Services Configuration Guide 」を参照してください。
- 監視デバイス比率 (P. 300)が正しくサイズ設定されていること。
- Cisco WAE が、TCP-7878 上で、割り当てられた CA Standard Monitor または CA Multi-Port Monitor、および 管理コンソール との通信が可能。

レスポンス時間をエクスポートするための Cisco WAE の設定

Cisco WAE CLI または Central Manager GUI から、Cisco WAE デバイスを設定して、アプリケーション レスポンス時間データがエクスポートされるようにします。

次の手順に従ってください:

1. Cisco WAE で、以下のコマンドを実行して、設定モードを変更します。
   `config`
2. コマンド ライン プロンプトが次のように変わります。
   `WAE<config>#`
3. 以下のコマンドを実行して、Cisco WAE 上のフロー監視を無効にします。
   `no flow monitor tcpstat-v1 enable`
4. 以下のコマンドを実行して、管理コンソール の IP アドレスに Cisco WAE を登録します。
   `flow monitor tcpstat-v1 host <MCAddress>`

   ここで、*<MCAddress>* には 管理コンソール の IP アドレスを指定します。
5. 以下のコマンドを実行して、Cisco WAE 上のフロー監視を有効にします。
   `flow monitor tcpstat-v1 enable`
6. 以下のコマンドを実行して、権限モードに戻ります。
   `exit`
7. コマンド ライン プロンプトが次のように変わります。
   `WAE#`
8. Cisco WAAS Flow Agent が CA Application Delivery Analysis Manager に接続されていることを確認するには、以下のコマンドを実行します。
   `show statistics flow monitor tcpstat-v1`

   結果は［Configured Host Address］が CA Application Delivery Analysis Manager の IP アドレスであることを示している必要があります。正常な場合は、Cisco WAE が CA Application Delivery Analysis Manager をポーリングしている場合を除いて、［Host Connection State］が［Waiting to Poll］となることに注意してください。
9. Cisco WAE が 管理コンソール 上の WAN 最適化デバイスのリスト内に表示されていることを確認します。
   a. 管理コンソール を開きます。
   b. ［環境管理］ページをクリックします。
   c. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

d. ［WAN 最適化デバイス リスト］までスクロールします。Cisco WAE が表示される場合、Cisco WAE を CA Standard Monitor または CA Multi-Port Monitor に割り当てる (P. 428)ことができます。

監視デバイスへの Cisco WAE の割り当て

レスポンス時間データをエクスポートするよう Cisco WAE デバイスを設定したら、Cisco WAE を CA Standard Monitor または CA Multi-Port Monitor に割り当てることができます。 Cisco WAE を CA Virtual Systems Monitor には割り当てないでください。

利用可能な 監視デバイス リソースを最大化するには、CA Standard Monitor を追加 (P. 331)するときに、パケットの監視を無効にします。

どのデバイスに Cisco WAE を割り当てるか決める場合、単純に CA Standard Monitor と CA Multi-Port Monitor の監視デバイス 間で負荷分散します。 可能な限り、同じ 監視 に複数のデータ センター WAE を割り当てないようにし、ブランチ Cisco WAE デバイスの負荷を分散します。

Cisco WAE では以下を実行します。

- 監視するサーバのリストを取得するために、割り当て済み 監視デバイス を 5 分ごとにポーリングする。
- その割り当てられた 監視デバイス にパケット要約ファイルを送信する。

サーバ SPAN を監視している 監視デバイス、または Cisco WAE デバイスからのパケット要約ファイルの受信専用の 監視デバイス に、Cisco WAE を割り当てます。 CA Standard Monitor の「管理ポート」に負荷がかかり過ぎないようにするために、CA GigaStor からのパケット要約ファイルも受信する CA Standard Monitor には Cisco WAE は割り当てないようにします。

重複する IP トラフィックを分離するためにドメインを使用している場合は、WAN 最適化 監視フィード を編集 (P. 431)し、ドメインに割り当てます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］で、 をクリックして CA Standard Monitor または CA Multi-Port Monitor を編集します。

   ［アクティブ フィード］列で、［WAN 最適化］は、Cisco WAE デバイスなどの WAN 最適化デバイスが 監視 に割り当てられていることを示しています。

4. 3 番目の［表示項目］メニューで［監視デバイス］をクリックします。
5. ［監視デバイス］で、［WAN 最適化］にスクロールし、［使用可能］列のデバイスをクリックします。 右矢印をクリックして、［割り当て済み］列へ移動させます。 ［割り当て済み］列の Cisco WAE デバイスは、監視 に現在割り当てられています。

   割り当てる Cisco WAE がリストに表示されていない場合は、Cisco WAE が 管理コンソール と通信するように 設定 (P. 426)されていることを確認します。
6. 手順を繰り返して、別の Cisco WAE を割り当てるか、または［OK］をクリックして終了します。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。
8. 5 ～ 10 分後に、管理コンソール の［最適化］ページに、最適化されたネットワーク セグメントのアプリケーション パフォーマンス データが表示されます。 管理コンソール の［最適化］ページで、［過去 1 時間］でフィルタすると、受信したパフォーマンス データを表示できます。

   アプリケーションのデータが表示されない場合は、Cisco WAE 監視デバイスのトラブルシューティング (P. 438)を行ってください。

詳細:

CA Standard Monitor の追加 (P. 331)
WAN 最適化監視フィードの編集 (P. 431)

Cisco WAE 監視デバイスの編集

Cisco WAE 監視デバイス を編集して、そのプロパティを更新します。たとえば、インシデント レスポンスを割り当てます。 Cisco WAE を編集しているときに、任意の 監視デバイス インシデントを表示することもできます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］までスクロールします。
4. （オプション）［ソース セットの選択］リストからソース セットをクリックすると、Cisco WAE デバイスの対応するグループを表示できます。
5.  をクリックして、Cisco WAE 監視デバイス を編集します。

   ［WAN 最適化プロパティ］が表示されます。
6. ［インシデント レスポンス］をクリックして、インシデント レスポンスを選択し、［OK］をクリックします。

   監視デバイス に対するインシデントを表示するには、3 番目の［表示項目］メニューで［インシデント］をクリックします。

詳細:

Cisco WAE デバイス グループによるサーバの監視 (P. 443)
監視デバイス インシデントの表示 (P. 306)

WAN 最適化監視フィードの編集

［WAN 最適化］ 監視フィードを編集して、Cisco WAE デバイスのグループに特定のドメインを割り当てます。デフォルトでは、新規の 監視フィードは「デフォルト ドメイン」に割り当てられます。 ［*WAN 最適化*］ 監視フィードは、CA Standard Monitor または CA Multi-Port Monitor で利用可能であり、Cisco WAE デバイスなど WAN 最適化デバイスからパケット要約ファイルを受信します。

注: WAAS 環境で、WAN 最適化 監視フィードのペアを作成する必要はありません。 冗長性のために Cisco WAE が追加されている場合は、単にそれを CA Standard Monitor または CA Multi-Port Monitor に割り当てます。 WAAS 環境の冗長性のサポートを有効にするには、サーバ SPAN を監視する監視フィードのペアを作成 (P. 291)します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして CA Standard Monitor または CA Multi-Port Monitor を編集します。

   ［アクティブ フィード］列で、［WAN 最適化］は、Cisco WAE デバイスなどの WAN 最適化デバイスが 監視 に割り当てられていることを示しています。

   編集対象の 監視 が明確でない場合、［WAN 最適化デバイス リスト］の［割り当て先］列で、その割り当てられた 監視 を検索します。

   ［監視のプロパティ］が表示されます。
4. ［監視フィード］セクションにスクロールし、 をクリックして WAN 最適化 監視フィードを編集し、WAN 最適化 監視フィード設定を指定します。

   WAN 最適化 監視フィードに対する 監視フィード設定では、セカンダリ フィードを設定できないことに注意してください。 セカンダリ 監視フィードは、WAN 最適化デバイスに適用可能ではありません。
5. ［更新］をクリックします。
6. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)

Cisco WAE の割り当て解除

割り当てられた 監視 から Cisco WAE の割り当てを解除します。 監視 からすべての WAN 最適化デバイスを割り当て解除すると、管理コンソール は自動的にその［WAN 最適化］ 監視フィード を削除します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして、Cisco WAE が割り当てられている CA Standard Monitor または CA Multi-Port Monitor を編集します。

   ［アクティブ フィード］列で、［WAN 最適化］は、Cisco WAE デバイスなどの WAN 最適化デバイスが 監視 に割り当てられていることを示しています。
4. 3 番目の［表示項目］メニューで［監視デバイス］をクリックします。

   ［監視デバイス］が表示されます。
5. Cisco WAE の割り当てを解除するには、 をクリックします。
6. プロンプトで［割り当て解除を続行］をクリックして、Cisco WAE の割り当てを解除します。

   管理コンソール は［割り当て済みデバイス リスト］を更新します。
7. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

WAAS Incidents

Cisco WAE デバイスが 管理コンソール へのデータ送信を 15 分以上停止した場合、管理コンソール は自動的に「メジャー」の 監視デバイス インシデントを作成します。

詳細情報

監視デバイス インシデントのしきい値の編集 (P. 307)

Cisco WAE 監視デバイスの削除

Cisco WAE を削除して、管理コンソール のレスポンス時間データのソースとしてそれを削除します。 Cisco WAE 監視デバイス を削除すると、管理コンソール は自動的に、WAN 最適化 監視フィード が割り当てられていたサーバに、別の 監視フィード を割り当てます。 管理コンソール が 監視フィード の割り当てを更新するのに最大 10 分かかることがあります。

Cisco WAE 監視デバイス を削除すると、自動的に Cisco WAE がその CA Standard Monitor または CA Multi-Port Monitor から割り当てを解除されます。

次の手順に従ってください:

1. 割り当てられた CA Standard Monitor または CA Multi-Port Monitor 監視デバイス から、Cisco WAE を割り当て解除 (P. 433) します。 または、別の 監視デバイス に、Cisco WAE デバイスを再度割り当てる (P. 428) こともできます。
2. Cisco WAE 上のフロー監視を無効 (P. 435) にして、管理コンソール の Cisco WAE 監視デバイス リストから割り当て解除した Cisco WAE を削除します。
3. 管理コンソール から Cisco WAE を削除 (P. 436) します。

Cisco WAE 上のフロー監視の無効化

割り当て解除された Cisco WAE 監視デバイス のリストから Cisco WAE を削除するには、まず Cisco WAE 上のフロー監視を無効にする必要があります。

次の手順に従ってください:

1. Cisco WAE で、以下のコマンドを実行して、設定モードを変更します。
   `config`
2. コマンド ライン プロンプトが次のように変わります。
   `WAE<config>#`
3. 以下のコマンドを実行して、Cisco WAE 上のフロー監視を無効にします。
   `no flow monitor tcpstat-v1 enable`
4. 以下のコマンドを実行して、権限モードに戻ります。
   `exit`
5. コマンド ライン プロンプトが次のように変わります。
   `WAE#`
6. フロー監視が無効であることを確認するには、以下のコマンドを実行します。
   `show statistics flow monitor tcpstat-v1`
7. コマンド実行の結果によって、フロー監視が無効であることを確認します。
   フロー アプリケーションは無効であり、利用できません。

Cisco WAE 監視デバイスの削除

Cisco WAE 監視デバイス を削除する前に、Cisco WAE を設定してレスポンス時間データのエクスポートを無効にします。Cisco WAE 監視デバイス を管理コンソール から削除し、Cisco WAE デバイスがレスポンス時間データをエクスポートするように設定されている場合、Cisco WAE は 監視デバイス として引き続き利用可能になります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］にスクロールし、 をクリックして、Cisco WAE 監視デバイス を削除します。
4. プロンプトで［削除を続行］をクリックして、Cisco WAE を削除します。

   Cisco WAE が［WAN 最適化デバイス リスト］から削除されます。

最適化アプリケーションのリセット

すべての最適化アプリケーションをリセットして、管理コンソール で現在受信するセグメント化されたアプリケーション データに基づいて、管理コンソール のアプリケーション パフォーマンスのレポーティングを有効にします。 通常は、 (P. 420)最適化をリセットする必要はありません。最適化が中断された場合も、管理コンソール はアプリケーションのレポーティングを続行するからです。

管理コンソール を使用して、異なるアプリケーションを最適化する利点を示そうとしている場合、最適化をリセットすると WAAS 最適化の変更をすばやく比較することができます。 たとえば、最適化を停止すると、管理コンソール は、アプリケーションのサーバ セグメントにおける最適化されていないサーバ SPAN のレポーティングを最大 20 分間継続します。その後、最適化解除されたアプリケーションの最適化解除トラフィックをレポーティングします。

最適化をリセットした後は、サーバ セグメントでレポートされていたすべての最適化解除のアプリケーション トラフィックは、最適化解除されたアプリケーションでレポートされ、現在最適化されているアプリケーションはネットワーク セグメントによってレポートされます。 ただし、10 分間以内で、管理コンソール がアプリケーションの サーバ セグメントにサーバ SPAN メトリックを代用できます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］にスクロールし、 ⚙ をクリックし、［最適化をリセット］を選択します。
4. 10 分間待って、［最適化］ページで、更新済みのレポート データを参照します。

詳細:

最適化停止時における監視の仕組み (P. 420)

Cisco WAE 監視デバイスのトラブルシューティング

足りないレポート データの原因を特定するために、Cisco WAE のトラブルシューティングを行います。 Cisco WAE 監視デバイス を追加した後、管理コンソール は 10 分以内に、ネットワーク セグメントによる最適化されたアプリケーション パフォーマンスをレポーティングします。

管理コンソール がブランチ場所またはすべてのブランチ場所に対してセグメント化されたアプリケーション データを表示しない場合、対応する Cisco WAE デバイスにアクティブ セッションがあり、Cisco WAE デバイスが、適切なアプリケーション トラフィック用のレスポンス時間データをエクスポートしていることを確認します。

ネットワーク セグメント データが以下に対して存在しない場合

クライアント セグメント

ブランチ WAE デバイスを確認します。

WAN セグメント

データ センター WAE デバイスを確認します。

サーバ セグメント

データ センター WAE デバイスとデータ センター サーバ間のトラフィックを監視する 監視デバイス を確認します。 監視デバイス がサーバ SPAN を監視するよう設定されていない場合は、データ センター WAE デバイスを確認します。

アクティブ セッションの表示

［アクティブ セッション］ページを使用して、レポート間隔の最後の 5 分間に WAN 最適化 監視 によってレポートされる、アクティブ セッション数をレポートします。

アクティブセッション情報を使用して、WAN 最適化 監視フィード が TCP セッションを監視 (P. 293)していることを確認します。 管理コンソール は、アプリケーション ポートのサーバ上のアクティブな TCP セッション数をレポートします。 監視フィード にサーバまたはアプリケーションのアクティブ セッションがない場合、WAE の設定に問題があります。

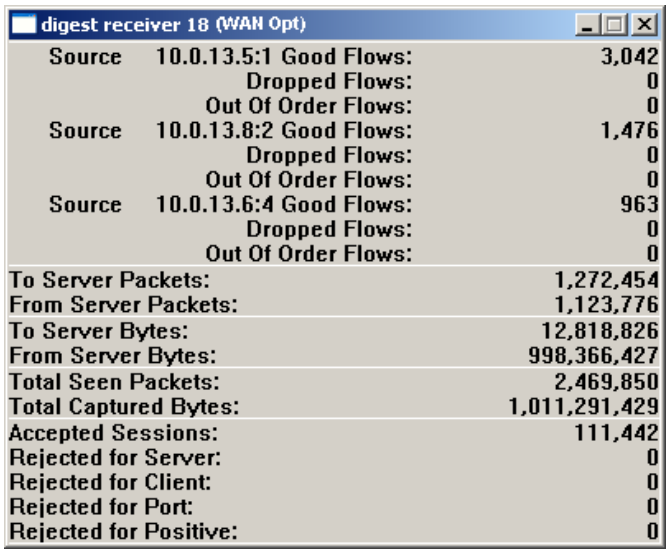
WAN 最適化カウンタ統計の表示

WAN 最適化カウンタを表示して、割り当て済み Cisco WAE デバイスから受信するパケット要約の情報を表示します。この情報のなかには、パケット要約を転送する Netflow パケットに関する情報も含まれます。

WAN 最適化カウンタ ウィンドウを表示するには、Cisco WAE が割り当てられている CA Standard Monitor にログイン (P. 348)する必要があります。

重要: 開始前に、監視デバイスを同期します。データ監視の同期が完了するまで、カウンタ ウィンドウは表示されません。

WAE 最適化カウンタでは、監視 に割り当てられている Cisco WAE デバイスからの統計が表示されます。



良好なフロー

Netflow パケットの送信順に受信された パケット数を特定します。

ドロップされたフロー

CA ADA Monitor サービスで処理されなかった Netflow パケット数を特定します。 ドロップされた Netflow パケット内に含まれていたパケット要約のレスポンス時間データは、管理コンソール レポートに含まれません。

順不同フロー

Netflow パケットは 監視 で受信されましたが、送信順では受信されなかった Netflow パケット数を特定します。

サーバへのパケット数

クライアントからサーバへ送信されたパケット数を特定します。

サーバからのパケット数

サーバからクライアントへ送信されたパケット数を特定します。

サーバへのバイト数

クライアントからサーバへ送信されたバイト数を特定します。

サーバからのバイト数

サーバからクライアントへ送信されたバイト数を特定ます。

参照されたパケット総数

検査されたパケット数を示して、パケット ヘッダが指定のアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットと一致したかどうかを判定します。

キャプチャされたバイト総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総バイト数です。

注: Cisco WAAS Flow Agent は各パケット ヘッダを検査し、指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットにパケットが一致するかどうかを判断します。 詳細については、「参照されたパケット総数」を参照してください。

承認済みセッション数

管理コンソール で有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッションの数を特定します。

サーバ関連の拒否

サーバ IP が、管理コンソール によって監視されるサーバ サブネットに一致しなかったことを示します。

クライアント関連の拒否

クライアント IP が、管理コンソール によって監視されるクライアント ネットワークのリストに一致しなかったことを示します。

ポート関連の拒否

サーバ ポートが 管理コンソール で拒否するポート リストに一致したことを示します。

ポジティブ関連の拒否

将来の使用に備えて予約されています。

詳細情報:

クライアント ネットワークの仕組み (P. 34)
アプリケーションの仕組み (P. 122)
サーバの仕組み (P. 79)

Cisco WAE ネットワーク設定の確認

Cisco WAE で以下を確認します。

- 監視するサーバを最適化していること。
- Cisco WAAS Flow Agent が最適化されたサーバのレスポンス時間データをエクスポートしていること。

次の手順に従ってください:

1. Cisco WAE で、以下のコマンドを実行して、その最適化されたトラフィックを表示します。

   WAAS/WAE **バージョン** 4.1.x

   show statistics connection all

   WAAS/WAE **バージョン** 4.0.x

   show tfo connection summary

2. サーバ IP アドレスおよびポートのリストを確認して、Cisco WAE が対象のアプリケーション トラフィックを最適化していることを確認します。
3. 以下のコマンドを実行し、Cisco WAAS Flow Agent がレスポンス時間データをエクスポートしているサーバのリストを表示します。
   `show statistics flow filters`

   サーバのリストが、前の手順の最適化されたサーバ リストに一致しない場合、以下を確認します。

   a. 管理コンソール がサーバを監視していることを確認。

   b. サーバがアプリケーションに割り当てられていることを確認。
4. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。
5. 5 分間待った後、Cisco WAE が監視しているサーバのリストが 管理コンソール のサーバ リストに対応していることを確認します。以下のコマンドを実行します。
   `show statistics flow filters`

   サーバが追加され、フロー ヒット数が 0 を超えていることを確認できます。

詳細:

サーバの管理 (P. 89)
アプリケーションへのサーバの割り当て (P. 150)

Cisco WAE デバイス グループによるサーバの監視

Cisco WAE デバイスがネットワーク全体に分散されているため、一般的に全 Cisco WAE デバイスが全サーバを監視できるようにすることを推奨します。個々の Cisco WAE デバイスでは以下の監視が可能です。

- 特定のサーバへの（からの）全トラフィックを対象にする
- 特定のサーバへの（からの）全トラフィックを対象にしない
- 特定のサーバへの（からの）一部のトラフィックを対象にする

ソース セットの動作方法

ソース セットは Cisco WAE デバイスのグループです。 通常、ソース セットを設定する必要はありません。管理コンソール はすべてのサーバと Cisco WAE デバイスを同じソース セットに割り当てることにより、すべての Cisco WAE デバイスが全サーバを監視できるようにします。必要に応じて、ソース セットを作成して、特定のサーバを監視する Cisco デバイスのグループを指定することができます。

ソース セットでは、これらのデバイスによってレポートされるトラフィックの独自性を確認できません。 必要な場合は、ドメインを使用して重複するトラフィックを分離 (P. 113)します。

Cisco WAE デバイスのグループでサーバを監視するには、以下のタスクを実行します。

- 適切な Cisco WAE デバイスへの ソース セットの割り当て (P. 444)。
- 適切なサーバへのソース セットの割り当て (P. 445)。

Cisco WAE デバイスへのソース セットの割り当て

Cisco WAE デバイスにソース セットを割り当てて、Cisco WAE デバイスのグループを作成します。 レポートティング目的のため、ソース セットをサーバに割り当てて、確実にソース セットの Cisco WAE デバイスのみがサーバ上の WAN 最適化アプリケーション トラフィックを監視するようにします。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］にスクロールし、［ソース セットの選択］をクリックして WAE デバイスのリストをフィルタします。

   ［ソース セットの選択］リストが表示されない場合、追加のソース セットは定義されていません。

   デフォルトでは、管理コンソールは、新規 WAE デバイスを［デフォルト展開］という名前のデフォルト ソース セットに割り当てます。［デフォルト展開］を選択して、現在デフォルト ソース セットに割り当てられている WAE デバイスのリストを表示します。
4. をクリックして、Cisco WAE 監視デバイス を編集します。

   ［WAN 最適化デバイスのプロパティ］が表示されます。
5. ［ソース セットの選択］をクリックして、Cisco WAE を割り当てる ソース セットを選択するか、または［追加］をクリックして新規ソース セットを追加し、ソース セット名を入力して［OK］をクリックします。

   管理コンソール で、現在選択されているソース セットに属する Cisco WAE デバイス リストが更新されます。

   ［ソース セット］リストが表示されない場合、追加のソース セットは定義されていません。
6. 上記手順を繰り返し、各 Cisco WAE 監視デバイス にソース セットを割り当てます。

サーバへのソース セットの割り当て

通常、ソース セットをサーバに割り当てる必要はありません。管理コンソール が自動的に全 Cisco WAE デバイスで全サーバを監視します。

必要に応じて、Cisco WAE デバイスのグループ (P. 444)を指定し、ソース セットをサーバに割り当てることで、サーバを監視できます。

複数のソース セットを作成した場合は、［サーバのプロパティ］ページに［ソース セット］オプションが表示され、特定のソースをサーバに割り当てることができます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［サーバ リスト］にスクロールし、 をクリックしてサーバを編集します。

   ［サーバのプロパティ］が表示されます。
4. ［ソース セット］をクリックして、別のソース セットを選択し、［OK］をクリックします。

   ［ソース セット］リストが表示されない場合、追加のソース セットは定義されていません。

ソース セットの名前の変更

ソース セットを編集して、その名前を変更します。 Cisco WAE 監視デバイス が割り当てられているソース セットを変更する場合は、Cisco WAE 監視デバイスを編集 (P. 430)します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］にスクロールし、［ソース セットの選択］をクリックして WAE デバイスのリストをフィルタします。
4. ⚙ をクリックし、［ソース セットの編集］をクリックします。
5. ［ソース セット］で、ソース セットの新しい名前を入力し、［OK］をクリックします。

ソース セットの削除

ソース セットを削除すると、管理コンソール では対応する Cisco WAE デバイス、および、削除済みのソース セットに割り当てられたすべてのサーバも［デフォルト展開］ソース セットに割り当てられます。

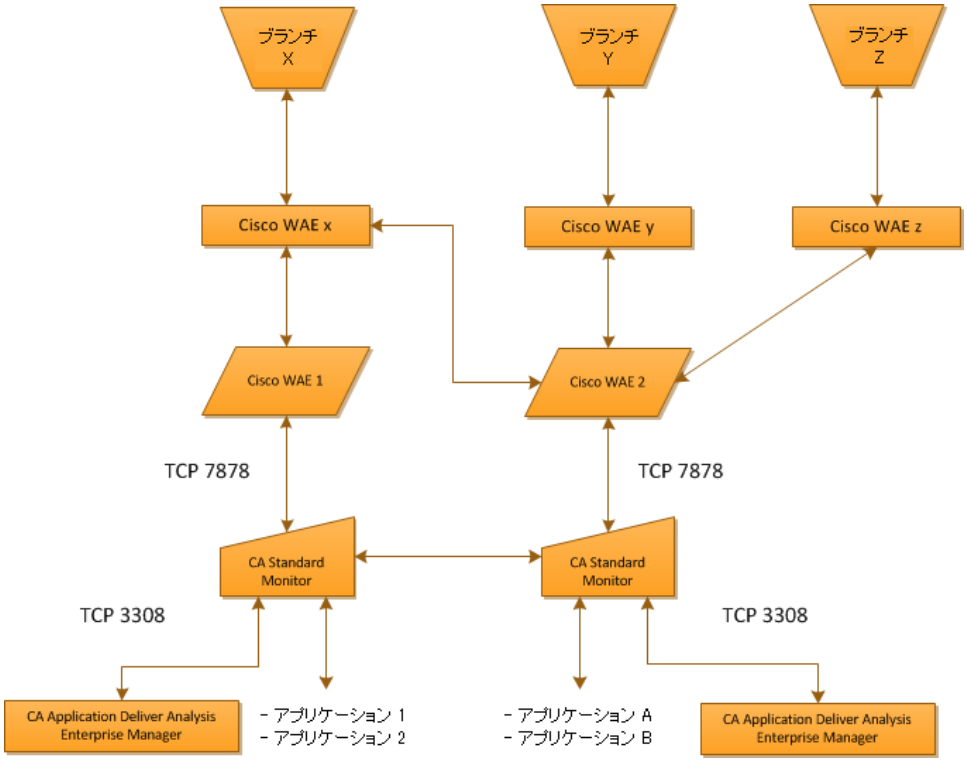
次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［WAN 最適化デバイス リスト］にスクロールし、［ソース セットの選択］をクリックして、削除するソース セットを選択します。
4. ⚙ をクリックし、［ソース セットの削除］をクリックします。
5. ［ソース セットの削除］で、削除の確認のためのプロンプトが表示されます。

管理コンソール間の最適化データの共有

管理コンソール は通常、環境内のすべての Cisco WAE デバイスをサポートできます。 ただし、WAAS 展開で最適化されるアプリケーションが単一の管理コンソール でサポートできる数より多くの Cisco WAE 監視デバイスの展開を必要とする場合、複数の 管理コンソール 間のリモートサイトでクライアント、WAN および サーバ セグメントのアプリケーション パフォーマンス データを共有します。

以下の例では、WAN 最適化アプリケーション パフォーマンス データを共有することによって、右側の 管理コンソール で Branch X と WAE x 間で App A および App B セグメント トラフィックの クライアント セグメントをレポートすることができるようになります。 共有しない場合は、右側の 管理コンソール は、Branch X 内の App A および App B の WAN および サーバ セグメントのみをレポートします。



あるいは、左側の 管理コンソール を設定して、リモート ブランチにわたって App A および App B のパフォーマンスを監視する場合、WAN 最適化アプリケーション パフォーマンス データを共有することによって、コンソールは、Branch X で App A と App B に対する WAN および サーバ セグメントをレポートできるのに加え、Branch Y および Branch Z で App A と App B に対するクライアント、WAN、およびサーバ セグメントをレポートできるようになります。共有しない場合は、左側の 管理コンソール は、Branch X、または Branch Y および Branch Z で、App A と App B の WAN および サーバ セグメントをレポートしません。

Cisco WAE デバイスからのパケット要約ファイルを複数の 管理コンソール 間で共有します。これは、管理コンソール が、共有しているそれぞれの 管理コンソール をポーリングして、CA Standard Monitor および CA Multi-Port Monitor の 監視デバイス リストを得た後、共有のコンソールに属している 監視 とパケット要約を共有することによって行われます。 たとえば、CA Standard Monitor で、監視を想定していないサーバのパケット要約ファイルを受信する場合、監視 は、共有している 管理コンソール に属する 監視 とパケット要約ファイルを共有します。 共有データ量を最小にするには、アプリケーションに最も近い 監視 を含む 管理コンソール からのアプリケーションを監視します。

WAN 最適化パフォーマンス データの共有

WAN 最適化アプリケーション パフォーマンス データを共有するには、以下の処理が必要です。

- すべての Cisco WAE デバイスおよびサーバを同じソース セットに割り当てます。ソース セットを設定しない場合は、「デフォルト展開」ソース セットを使用できます。
- パケット要約ファイルを受信する 監視デバイス を設定して、アプリケーション パフォーマンス データを共有します。
- すべての共有 監視デバイス が以下と通信可能であることを確認します。
  - TCP-3308 上の各 管理コンソール。 Cisco WAE からパケット要約ファイルを受信する全 監視デバイス が、TCP-3308 上の各 管理コンソール と通信可能である必要があります。
  - TCP-7878 上のすべての Cisco WAE デバイス。 管理コンソール は自動的に 監視デバイス 間での共有を設定します。

すべての 監視デバイス で共有を有効した後は、25 分間以内に Cisco WAE が割り当て済みの 監視 をポーリングして、サーバの更新リストを取得し、共有データのレポーティングを開始します。

監視 で WAN 最適化アプリケーション パフォーマンス データを共有できない場合には、共有がリストアされるまで、データはそこに保存されます。ただし、監視 で保存できる共有データは 1GB までです。 監視 に保存できない共有データは喪失し、復元できません。

次の手順に従ってください:

1. Cisco WAE からパケット要約ファイルを受信する CA Standard Monitor および CA Multi-Port Monitor の 監視デバイス が TCP-3308 上の各 管理コンソール に通信可能であることを確認します。 すべての 監視デバイス が、TCP-3308 上の 管理コンソール と通信可能である必要があります。
2. すべての 監視デバイス が TCP-7878 上で相互に通信できることを確認します。
3. すべての 監視デバイス を設定して、WAN 最適化アプリケーション パフォーマンス データを共有させます。
   a. DTMDistributedConsoles.ini という名前の設定ファイルを作成します。

b. DTMDistributedConsoles.ini で、共有する各 管理コンソール の IP アドレスを入力します。監視 に割り当てられている 管理コンソール の IP アドレスを必ず含めます。IP アドレスを指定する際には、ドット 10 進表記を使用して、各 IP アドレスを 1 行ごとに分けて入力します。

c. すべての 監視デバイス に同じ DTMDistributedConsoles.ini ファイルをコピーします。 以下のようにコピーします。

   - CA Standard Monitor の場合、<ADA_HOME>¥bin フォルダにファイルをコピー。
   - CA Multi-Port Monitor の場合、/opt/NetQoS/bin フォルダにファイルをコピー。

d. .ini ファイルの設定に従って、以下のように共有を開始します。

   - 各 CA Standard Monitor で、Windows サービスのコントロール パネルを開き、CA ADA Data Transfer Manager サービスを再起動します。
   - 各 CA Multi-Port Monitor では、［プロセス ステータス］ページを開き、caperformancecenter_devicemanager プロセスを再起動します。

   25 分間以内に 管理コンソール によって、共有される WAN 最適化クライアント セグメント データがレポーティングされます。

共有設定の更新

共有 管理コンソール 設定を更新して、共有する 管理コンソール を追加または削除します。

次の手順に従ってください:

1. DTMDistributedConsoles.ini ファイルを編集します。
2. IP アドレスのリストを更新し、必要な 管理コンソール について 1 行に 1 つの IP アドレスを入力して追加します。 各 IP アドレスの指定には、ドット 10 進表記を使用します。
3. 更新した DTMDistributedConsoles.ini ファイルを、すべての 監視デバイス にコピーします。 以下のようにコピーします。
   - CA Standard Monitor の場合、<ADA_HOME>¥bin フォルダにファイルをコピー。
   - CA Multi-Port Monitor の場合、/opt/NetQoS/bin フォルダにファイルをコピー。

   設定ファイルから 管理コンソール を削除する場合は、関連付けられた監視デバイス から設定ファイルを必ず削除してください。
4. 更新された .ini ファイルの設定に従って、以下のように共有を開始します。
   - 各 CA Standard Monitor で、Windows サービスのコントロール パネルを開き、CA ADA Data Transfer Manager サービスを再起動します。
   - 各 CA Multi-Port Monitor では、［プロセス ステータス］ページを開き、caperformancecenter_devicemanager プロセスを再起動します。

   25 分以内に、各 管理コンソール 間で WAN 最適化クライアント セグメント データの共有が開始されます。

監視デバイスの削除

WAE パフォーマンス データを共有する CA Standard Monitor または CA Multi-Port Monitor を削除する場合、できるだけ早く他の共有 監視デバイス の設定をリセットしてください。それによってデータ共有はそれらの間でのみ行われることになります。

共有される 監視 を削除しても、他の共有 監視デバイス の設定は自動的にリセットされません。 管理コンソール では、監視デバイス 間のデータ共有は継続されており、削除された 監視 との共有データは失われます。

次の手順に従ってください:

1. 削除する CA Standard Monitor または CA Multi-Port Monitor に割り当てられている Cisco WAE の割り当てを解除 (P. 428) します。
2. CA Standard Monitor を削除 (P. 344) します。
3. 残りの全ての 監視デバイス で Data Transfer Manager サービスを再起動します。 共有の設定を更新するのに最大 25 分間かかります。
4. Cisco WAE デバイスを更新して、Cisco WAE のフロー監視を再起動することで使用可能な 監視デバイス とパフォーマンス データを共有します。

   CLI を使用して、フロー監視を再起動するには、以下の処理を行います。

   a. Cisco WAE で、以下のコマンドを実行して、設定モードを変更します。

      ```
      config
      ```

   b. コマンド ライン プロンプトが次のように変わります。

      ```
      WAE<config>#
      ```

   c. 以下のコマンドの実行して、フロー監視を無効にします。

      ```
      no flow monitor tcpstat-v1 enable
      ```

   d. 以下のコマンドの実行して、フロー監視を有効にします。

      ```
      flow monitor tcpstat-v1 enable
      ```

   e. 以下のコマンドを実行して、権限モードに戻ります。

      ```
      exit
      ```

   f. コマンド ライン プロンプトが次のように変わります。

      ```
      WAE#
      ```

   g. 以下のコマンドを実行して、フロー監視ステータスを確認します。

```
show statistics flow monitor tcpstat-v1
```

トラブルシューティングのヒント

管理コンソール で共有データが正しく表示されない場合は、以下を検証します。

- ソース セット内で、同一のサーバ IP が複数の 管理コンソール によって管理されていないこと。この場合、アプリケーション データの一部が複数の 管理コンソール に表示されたり、アプリケーション サーバに最も近い Cisco WAE とは通信しない 管理コンソール で、すべてのデータが予期せず表示されることがあります。
- Cisco WAE デバイス上のフロー フィルタが最新であること。監視 を設定してデータを共有するようにした後、25 分間以内に 監視 は各共有管理コンソール と通信し、Cisco WAE デバイス上のフロー フィルタを更新します。 フロー フィルタのサーバ リストは、すべての Cisco WAE デバイスで同一である必要があります。
- Cisco WAE デバイスからパケット要約を受信するすべての 監視デバイス が、TCP-7878 上で相互に通信可能であること。
- Cisco WAE デバイスからパケット要約を受信するすべての 監視デバイス が、TCP-3308 上で各 管理コンソール と通信可能であること。
- 同じ設定ファイルが各 監視 上にあること。

第 17 章: Cisco NAM による監視

このセクションには、以下のトピックが含まれています。

監視デバイスとしての Cisco NAM の動作方法 (P. 455)
Cisco NAM 監視デバイスの追加 (P. 459)
Cisco NAM 監視デバイスの編集 (P. 464)
NAM 監視フィードの編集 (P. 465)
NAM Incidents (P. 466)
Cisco NAM 監視デバイスの削除 (P. 467)
Cisco NAM 監視デバイスのトラブルシューティング (P. 469)

監視デバイスとしての Cisco NAM の動作方法

Cisco NAM ブレードまたはアプライアンス（Cisco NAM）は、CA Application Delivery Analysis 用の 監視デバイス の 1 タイプとして機能し、IP アドレス レベルでのトラブルシューティングを 30 秒で解決できます。 監視デバイス として Cisco NAM を使用すると、CA Application Delivery Analysis 用の サーバ フットプリントを削減できます。 さらに Cisco NAM では以下の処理を実行します。

- スイッチまたはルータからのネットワークの監視
- トラフィック使用状況に関するレポーティング
- パケットのキャプチャおよびデコード
- レスポンス時間の追跡。ネットワークまたはサーバに対するアプリケーションの問題を突き止めます。

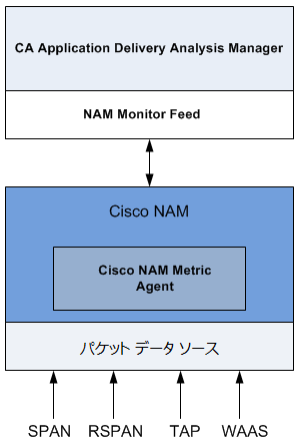
Cisco NAM の仕組み

Cisco NAM Metric Agent によって、メトリック要約ファイルが作成されます。このファイルには、Cisco NAM にミラーリングするすべてのトラフィックについて計算されたレスポンス時間メトリックが含まれます。

CA Application Delivery Analysis Manager 上の NAM 監視フィードでは、管理 NIC 上の Cisco NAM からメトリック要約ファイルを受信し、レスポンス時間統計を処理して、最もビジーなアプリケーションおよびあらゆるユーザ定義のアプリケーションを自動的に監視します。

分散 CA Application Delivery Analysis Manager は必須です。

以下の図に表示されるように、SPAN、ミラー ポート、ネットワーク タップ、および Cisco WAE デバイスからパケットを収集できます。 データは Cisco NAM Metric Agent によって処理され、計算されたレスポンス時間統計は、CA Application Delivery Analysis Manager に送信されます。



CA Application Delivery Analysis Manager は、その NAM 監視フィード上のパケット要約ファイルを受信します。

監視フィード割り当ての仕組み

Cisco NAM が最適な監視ポイントの場合、管理コンソールは自動的に NAM 監視フィードをサーバに割り当てます。

詳細:

監視フィード割り当ての仕組み (P. 289)

監視デバイスに関する考慮事項

監視 として Cisco NAM を使用している場合は、以下の点を考慮してください。

- Cisco NAM Metric Agent は、監視対象のすべてのアプリケーション、サーバ、ネットワークの組み合わせに対してレスポンス時間統計を計算します。 CA Application Delivery Analysis Manager では、CA Application Delivery Analysis Manager 上のサーバ サブネット、クライアント ネットワーク、およびアプリケーションの定義に一致しないアプリケーション、サーバ、ネットワークの組み合わせを破棄します。
- 処理できる以上のデータを Cisco NAM Metric Agent の SPAN に送ることができます。SPAN では慎重に CPU リソースの消費を最小限にし、Cisco NAM Metric Agent が処理できないパケットをドロップせずに、できるだけ多くの正確な測定を行うことができるようにします。
- ドメインを使用して Cisco NAM 監視デバイス間のデータ収集を分離することはできません。 すべての Cisco NAM 監視デバイスは CA Application Delivery Analysis Manager 上の同じ NAM 監視フィードに属します。
- Cisco WAE デバイスをデータ ソースとして使用するように Cisco NAM を設定すると、Cisco NAM Metric Agent は、Cisco WAE デバイスによって送信される TCP ヘッダからのレスポンス時間の統計を計算できます。
- Cisco NAM ではパケット要約ファイルを一時的に格納しません。 Cisco NAM が割り当て済み 管理コンソール と通信できない場合、管理コンソール レポートではデータの一部が欠落します。
- Cisco NAM からのメトリック要約ファイルには、セッション レベル情報が含まれず、そのため「アクティブ セッション数」レポートが NAM 監視フィードに提供できません。代わりに、[Metric Receiver Counter] ウィンドウを使用して、Cisco NAM から CA Application Delivery Analysis Manager に送信される内容のサマリ統計を表示します。
- アプリケーションがクライアント上の指定されたポート範囲内でクライアント要求に応答することにより、クライアントと通信する場合、Cisco NAM はアプリケーションを監視できません。 Cisco NAM Metric Agent では、サーバから TCP パケットが送信されるクライアント上のポートではなく、サーバ ポートからの SYN-ACK レスポンスに基づいてアプリケーションをホストするサーバを特定します。 管理コンソールでアプリケーションを定義する場合、Cisco NAM でアプリケーションを監視するには、アプリケーションのポート側を「アプリケーションはこれらのポートでリスンします」に設定する必要があります。

- 管理コンソール では、Cisco NAM からパケット キャプチャの調査を開始できませんが、Cisco NAM はトリガされたパケット キャプチャの調査をサポートします。
- Cisco NAM が 監視 として動作するとき、URL レポーティングは、管理コンソール ではなく Cisco NAM Traffic Analyzer コンソールでサポートされます。

詳細:

ユーザ定義のアプリケーションの管理 (P. 137)
Cisco NAM 監視デバイスのトラブルシューティング (P. 469)

Cisco NAM 監視デバイスの追加

Cisco NAM 監視デバイス の設定に必要な手順の要点を下記に示します。詳細については、以下のセクションを参照してください。

1. Cisco NAM を設定し、計算されたレスポンス時間統計が 管理コンソール にエクスポートされるようにします (P. 461)。
2. Cisco NAM を設定し、計算されたレスポンス時間統計が CA Application Delivery Analysis Manager にエクスポートされるようにします。
3. Cisco NAM を確認 (P. 462) し、CA Application Delivery Analysis Manager に接続され、Cisco NAM Metric Agent からレスポンス時間統計を受信していることを確認します。
4. 管理コンソール で NAM 監視フィード を有効にします (P. 463)。
5. *(オプション)* Cisco NAM の利用可能リソースを最適化するには、手動で Cisco NAM 上の SPAN データ ソースを設定して、管理コンソールで監視されているのと同じネットワーク、サーバ、およびアプリケーションを監視するようにします。Cisco NAM Metric Agent は、SPAN データ ソースのすべてのアプリケーション トラフィックのレスポンス時間メトリックを自動的に計算します。
6. *(オプション)*非アクティブ状態の 監視デバイス インシデントしきい値を編集 (P. 307) します。

前提条件

Cisco NAM 監視デバイス を追加するための前提条件は以下の通りです。

- Cisco NAM ソフトウェア バージョンが 4.2.x ～ 5.1(2) であること。

  管理コンソール では、そのブランチにローカルなサーバおよびアプリケーションのデータを処理する場合に限り、Cisco ブランチ ルータ シリーズ NME-NAM をサポートします。 対象のブランチ NAM にまたがるデータのみが、そのブランチのローカル サーバ用であることが不確かな場合、ブランチ NAM データを 管理コンソール にエクスポートできません。
- 監視デバイス比率 (P. 300)が正しくサイズ設定されていること。
- Cisco NAM が TCP-9996 上の 管理コンソール と通信可能であること。

レスポンス時間データをエクスポートするための Cisco NAM の設定

Cisco NAM Metric Agent を設定して、SPAN、Remote SPAN （RSPAN）、ネットワーク タップ、または Cisco WAE から CA Application Delivery Analysis Manager にレスポンス時間データがエクスポートされるようにします。Cisco WAE と異なり、Cisco NAM は、レスポンス時間メトリックを計算し、CA Application Delivery Analysis Manager に直接送信します。また、Cisco NAM は、受信するすべてのネットワーク トラフィックのレスポンス時間データを計算します。

SPAN データを処理するときは、ホスト スイッチから SPAN を設定することを推奨します。 層から層へのトラフィックを監視できるように、SPAN データを使用することを推奨します。RSPAN データは Cisco NAM で処理する前に、遅延が生じることがあります。しかし、場合によってはその使用が要求されます。

計算されたレスポンス時間統計を CA Application Delivery Analysis Manager にエクスポートするよう Cisco NAM Metric Agent を設定したら、管理コンソール は自動的に Cisco NAM を利用可能な 監視デバイス のリストに追加します。

Cisco NAM Traffic Analyzer コンソールを使用して、以下の処理を行います。

- 計算されたレスポンス時間メトリックのエクスポートを有効にします。
- 実行設定で必要なアクティブ SPAN セッションを検証し、それを起動設定に保存します（Cisco IOS ソフトウェアのみを実行するスイッチに対して）。
- Cisco NAM の SPAN データを表示します。

次の手順に従ってください:

1. Cisco NAM 上でレスポンス時間データ エクスポートを有効にします。
   a. NAM Traffic Analyzer コンソールを開きます。
   b. ［Admin］タブをクリックします。
      ［Admin］タブが表示されます。
   c. ［System］をクリックします。
      ［System Overview］が表示されます。
   d. ［Response Time Export］をクリックします。
      ［External Response Time Reporting Console Export］が表示されます。

e. ［Enable Export］を選択して［Apply］をクリックします。

f. ［Admin］タブの［Diagnostics］をクリックして、Cisco NAM がデータを 管理コンソール にエクスポートするためにその設定を更新していることを確認します。

［System Alerts］ページには Cisco NAM のログ記録メッセージが表示されます。

2. 実行設定でアクティブな SPAN セッションを検証し、そのセッションを起動設定で保存します。

a. NAM Traffic Analyzer ユーザ インターフェースで、［Setup］-［NAM Data Sources］をクリックします。

b. リストから SPAN セッションを選択し、［Save］をクリックして、実行設定のアクティブ SPAN セッションを スタートアップ設定に保存します（Cisco IOS ソフトウェアのみを実行するスイッチ用）。

c. 管理コンソール に表示したい各 SPAN セッションについて、前の手順を繰り返します。

3. SPAN データを表示します。

a. NAM Traffic Analyzer ユーザ インターフェースで、［Monitor］-［Server］-［Response Time］をクリックします。 クライアント数の多い順でサーバをソートし、クライアント数が最も多いサーバを見つけます。

b. 詳細情報を表示するには、サーバを選択し、［Details］をクリックします。

Cisco NAM の 管理コンソール への接続を確認

管理コンソール を使用して、Cisco NAM がレスポンス時間データを 管理コンソール にエクスポートしていることを確認します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［NAM デバイス リスト］にスクロールし、各 Cisco NAM が 管理コンソール に最後に通信した時間を確認します。

NAM 監視フィードの有効化

デフォルトでは、NAM 監視フィードは無効です。

管理コンソールでは、単一の NAM 監視フィードを作成して、環境内の Cisco NAM デバイスからのメトリック要約ファイルを処理します。 メトリック要約ファイルを処理するには、NAM 監視フィードを有効にします。

管理コンソールの監視デバイスとして Cisco NAM を今後使用しないことにした場合、NAM 監視フィードを無効にすることで利用可能なシステムリソースを最適化できます。 NAM 監視フィードを無効にするには、管理コンソール上の CA Standard Monitor を削除 (P. 344)します。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、リストを参照して、管理コンソールと同じ管理 IP アドレスの CA Standard Monitor を検索します。

   ［アドレス］列を使用し、監視の管理 IP アドレスを特定できます。CA Standard Monitor とコンソールは同じ管理 IP アドレスを共有します。
4. をクリックして、管理コンソールと同じ管理 IP アドレスの CA Standard Monitor を編集します。 必要に応じて、［ADA 監視の追加］をクリックして、管理コンソールと同じ管理 IP アドレスの CA Standard Monitor を追加します。

   ［Standard Monitor のプロパティ］が表示されます。
5. 以下のオプションを選択して、NAM 監視を有効または無効にし、［OK］をクリックします。
   - NAM 監視を有効にする
   - パケット監視を無効にする

   ［NAM デバイス リスト］には、管理コンソールにレスポンス時間データをエクスポートしているあらゆる Cisco NAM ブレードまたはアプライアンスが表示されます。

詳細:

コンソール設定の管理 (P. 267)
CA Standard Monitor の追加 (P. 333)
CA Standard Monitor の編集 (P. 336)

Cisco NAM 監視デバイスの編集

Cisco NAM 監視デバイス を編集して、その 監視デバイス インシデント レスポンスの変更、および追加詳細の表示を行います。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［NAM デバイス リスト］にスクロールし、 をクリックして、Cisco NAM を編集します。

   ［NAM のプロパティ］が表示されます。
4. ［インシデント レスポンス］をクリックして、監視デバイス インシデント レスポンスを選択し、［OK］をクリックします。

NAM 監視フィードの編集

管理コンソールでは、NAM 監視フィードを作成して、Cisco NAM からレスポンス時間データを受信します。 NAM 監視フィードを編集して、以下の処理を行います。

- 特定のドメインを割り当てる。デフォルトでは、新規の監視フィードは「デフォルト ドメイン」に割り当てられます。 重複する IP トラフィックを分けるためにドメインを使用していない場合には、適用されません。
- 監視フィードのペアを作成する。デフォルトでは、サーバは単一の監視フィードによって監視されます。

Cisco NAM Metric Agent は、5 分間のレスポンス時間メトリックを計算するため、管理コンソールでは、Cisco NAM 監視フィードのアクティブ セッション情報を表示しません。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして、管理コンソールと同じ管理 IP アドレスの CA Standard Monitor を編集します。すべての Cisco NAM デバイスは、管理コンソール上の NAM 監視フィードに自動的に割り当てられます。

   ［Standard Monitor のプロパティ］が表示されます。
4. ［監視フィード］にスクロールし、 をクリックして NAM 監視フィードを編集します。
5. セカンダリ フィードまたはドメインを割り当てて、［更新］をクリックします。

   サーバのプロパティの設定の詳細については、［ヘルプ］をクリックしてください。
6. 管理コンソール上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細:

テナントの管理 (P. 113)
監視フィードのペアの作成 (P. 291)

NAM Incidents

Cisco NAM が 管理コンソール へのデータ送信を 15 分以上停止した場合、管理コンソール は自動的に「メジャー」の 監視デバイス インシデントを作成します。 監視デバイス インシデントしきい値を編集して (P. 307)、適切なしきい値を指定します。

Cisco NAM 監視デバイスの削除

Cisco NAM 監視デバイスを削除して、レスポンス時間データのソースとして削除されるようにします。 Cisco NAM 監視デバイスを削除すると、その NAM 監視フィードに固定されていたすべてのサーバは固定が解除され、別の監視フィードが自動的に割り当てられます。 監視フィードの割り当てを更新するのに 10 分程度かかる可能性があります。

NAM 監視フィードにサーバを固定していた場合、監視デバイスが一時的にオフラインである場合でもサーバ トラフィックの監視を続行するには、以下のオプションを考慮します。

- 監視デバイスを削除する前に、別の監視フィードにサーバを固定します。監視デバイスをオンラインに戻す場合、NAM 監視フィードに適切なサーバを固定します。
- Cisco NAM 監視デバイスを削除します。 別の監視フィードが自動的に割り当てられますが、監視フィード割り当てを更新するのに 10 分程度かかる可能性があります。

Cisco NAM 監視デバイスを削除し、Cisco NAM がレスポンス時間データをエクスポートするよう設定されている場合、Cisco NAM は引き続き 監視デバイス として利用可能です。

次の手順に従ってください:

1. Cisco NAM 上で Cisco NAM Metric Agent のデータ エクスポートを無効にします。
   a. NAM Traffic Analyzer コンソールを開きます。
   b. ［Admin］タブをクリックします。
      ［Admin］タブが表示されます。
   c. ［System］をクリックします。
      ［System Overview］が表示されます。
   d. ［Response Time Export］をクリックします。
      ［External Response Time Reporting Console Export］が表示されます。
   e. ［Enable Export］の選択を解除して［Apply］をクリックします。
   f. ［Admin］タブの［Diagnostics］をクリックして、Cisco NAM が 管理コンソール へのデータ エクスポートを無効にするためにその設定を更新していることを確認します。

［System Alerts］ページには Cisco NAM のログ記録メッセージが表示されます。

2. 管理コンソール で、［NAM デバイス リスト］から Cisco NAM を削除します。
   a. ［環境管理］ページをクリックします。
   b. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
   c. ［NAM デバイス リスト］にスクロールし、  をクリックして、Cisco NAM を削除します。
   d. ［監視デバイス確認の削除］で、［削除を続行］をクリックして NAM 監視デバイス を削除します。

      Cisco NAM が［NAM デバイス リスト］から削除されます。

Cisco NAM 監視デバイスのトラブルシューティング

受信される NetFlow に関する情報を表示するには、NAM カウンタを表示します。

NAM カウンタ ウィンドウを表示するには、管理コンソール にログイン (P. 348)する必要があります。

重要: 開始前に、監視デバイスを同期します。 データ監視の同期が完了するまで、カウンタ ウィンドウは表示されません。

Cisco NAM のトラブルシューティングを行い、CA Standard Monitor で収集されるはずのレポート データが欠落している原因を特定します。 Cisco NAM を 管理コンソール に追加した後、管理コンソール が Cisco NAM から アプリケーション パフォーマンス データをレポーティングするまで最大 10 分かかることに注意してください。

他の 監視デバイス と異なり、Cisco NAM はセッション レベルの統計を生成しないため、管理コンソール でそれらをレポートしません。 Cisco NAM が 管理コンソール に送信する内容に関してサマリ統計を参照するには、管理コンソール で NAM カウンタ統計を表示してください。

次の手順に従ってください:

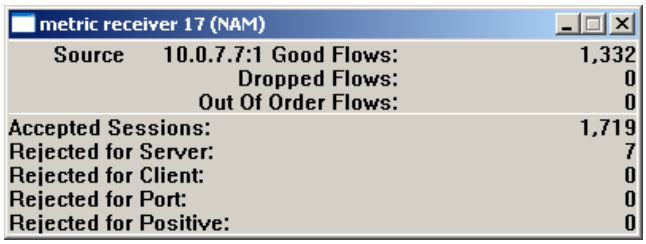
1. 管理コンソール コンピュータにログオンするか、または Microsoft Remote Desktop Connection (RDC) クライアントを使用してリモート接続します。

   リモート デスクトップを使用して Windows Server 2003 ベースのサーバに接続する場合は、/admin スイッチを使用して物理コンソール セッションに接続します。 物理コンソール セッションでは、フィード レシーバ カウンタを表示できます。 /admin スイッチの詳細については、Microsoft KB 947723 を参照してください。

2. NAM 監視フィード 統計を表示するには、オペレーティング システム に応じて以下の手順に従います。

   - Windows Server 2003 で 管理コンソール が 実行されている場合、フィード レシーバ カウンタは自動的に表示されます。表示されない場合は、物理コンソール セッションへの接続を確認してください。
   - Windows Server 2008 で 管理コンソール が 実行されている場合、デスクトップで［ADA 監視アクティビティ］のショートカットをダブルクリックして、フィード レシーバ カウンタを表示します。

NAM カウンタは、すべての Cisco NAM デバイスからの統計を表示します。



カウンタの説明が正しく表示されない場合は、カウンタのウィンドウをいったん閉じ、デスクトップ上の［ADA 監視アクティビティ］ショートカットをダブルクリックして再度開いてください。

いずれのフィード レシーバ カウンタも表示されない場合には、CA ADA Monitor サービスが実行中であり、かつ 監視 が 管理コンソール と同期していることを確認してください。

3. NAM カウンタ統計を解釈して、問題を特定します。

良好なフロー

Netflow パケットの送信順に受信された パケット数を特定します。

ドロップされたフロー

CA ADA Monitor サービスで処理されなかった Netflow パケット数を特定します。ドロップされた Netflow パケット内に含まれていたメトリック要約のレスポンス時間データは、管理コンソール レポートに含まれません。

順不同フロー

Netflow パケットは 監視 で受信されましたが、送信順では受信されなかった Netflow パケット数を特定します。

承認済みセッション数

管理コンソール 上の有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッションの数です。

サーバ関連の拒否

管理コンソール によって監視されるサーバ サブネットに一致しなかった、サーバ IP を特定します。

クライアント関連の拒否

管理コンソール によって監視されるクライアント ネットワークのリストに一致しなかったクライアント IP を特定します。

ポート関連の拒否

サーバ ポートが 管理コンソール で拒否するポート リストに一致したことを示します。

ポジティブ関連の拒否

将来の使用に備えて予約されています。

詳細:

クライアント ネットワークの仕組み (P. 34)
アプリケーションの仕組み (P. 122)
サーバの仕組み (P. 79)
基本操作の実行 (P. 409)

第 18 章: Riverbed Steelhead による監視

このセクションには、以下のトピックが含まれています。

概念 (P. 473)
監視デバイスの追加 (P. 482)
監視デバイスの管理 (P. 490)
監視デバイスのトラブルシューティング (P. 495)

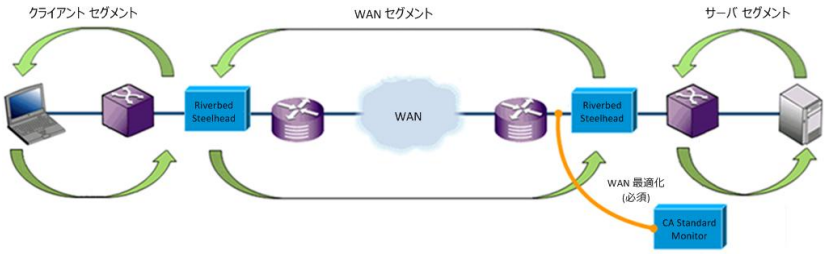
概念

このセクションでは、CA Application Delivery Analysis が Steelhead で最適化されたネットワークをどのように監視するかについて説明します。

はじめに

CA Standard Monitor は、Steelhead で最適化された IPv4 ベース トラフィックに対して監視デバイスの一種として機能します。CA Standard Monitor は、WAN で最適化されたトラフィックを受動的に監視し、エンド ツー エンドのシステム パフォーマンスの連続的な記録の維持に役立ちます。

以下の Steelhead 物理インパス設定で、データ センターの監視デバイスは、WAN ネットワーク セグメントにわたって最適化された WAN トラフィックを監視します。



データ センター内の CA Standard Monitor は、WAN セグメントの最適化されたトラフィックおよびサーバ セグメントの最適化されていないトラフィックの両方を監視できます。

最適化されたトラフィックおよび最適化されていないトラフィックには、個別の監視 NIC が必要です。

アーキテクチャ

データ センターでは、CA Standard Monitor は、最適化されたトラフィックおよび最適化されていないトラフィックの両方を監視するために個別の監視フィードを使用します。

Steelhead 監視フィード

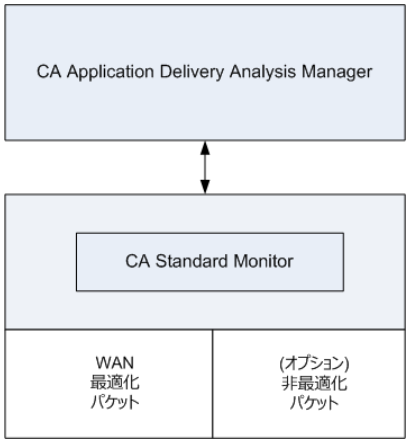
WAN の最適化されたパケットをデータ センターから受信し、監視された各アプリケーション/サーバ/ネットワークの組み合わせの WAN セグメントに対してレスポンス時間メトリックを計算します。

パケット ミラー監視フィード

サーバから最適化されていないパケットを受信し、監視された各アプリケーション/サーバ/ネットワークの組み合わせのサーバ セグメントに対してレスポンス時間メトリックを計算します。 CA Application Delivery Analysis は、サーバ ネットワーク セグメントをレポートするために最適化されていないサーバ トラフィックを監視する必要があります。

Steelhead で最適化された WAN トラフィックおよび最適化されていないサーバ トラフィックを監視するには、個別の監視 NIC が必要です。

管理コンソール は、新しいアプリケーション トラフィックが管理コンソールで定義されているクライアント ネットワークおよびサーバ サブネットと一致した場合、そのトラフィックについて自動的にレポートします。



ブランチで WAN に最適化されたアプリケーションのレスポンス時間をレポートするには、CA Standard Monitor はそのブランチ場所で必要になります。 Riverbed クライアント セグメント監視フィードは、クライアント コンピュータおよびブランチの Steelhead アプライアンス間の最適化されていないトラフィックを受信し、クライアント セグメントに対してレスポンス時間メトリックを計算します。 監視デバイスがブランチに展開されていない場合でも、CA Application Delivery Analysis は WAN のパフォーマンス情報を提供できます。

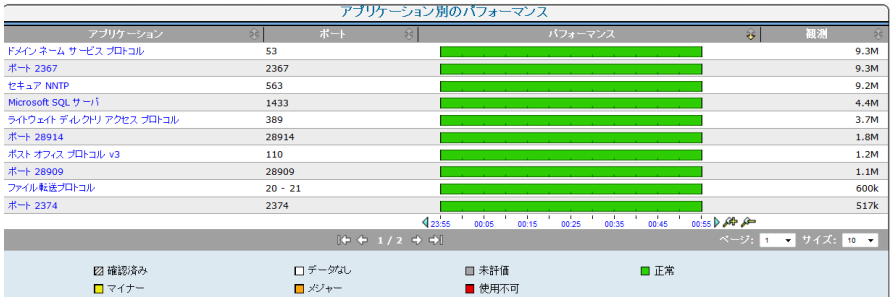
ネットワーク セグメント

管理コンソールは 3 つのネットワーク セグメントごとに個別のメトリック セットを生成し、各ネットワーク セグメントを個別のアプリケーションとして扱います。 管理コンソール では以下のメトリックのセットをそれぞれ個別に生成します。

- **クライアント セグメント**。ブランチにあるクライアントとブランチ Steelhead アプライアンスの間のネットワーク セグメントです。 最適化されていないクライアント ネットワーク セグメントを監視するには、目的のブランチに CA Standard Monitor を展開します。
- **WAN セグメント**。ブランチ Steelhead アプライアンスとデータ センター Steelhead アプライアンスの間のネットワーク セグメントです。 Steelhead で最適化された WAN ネットワーク セグメントを監視するには、目的のデータ センターに CA Standard Monitor を展開します。
- **サーバ セグメント**。データ センター Steelhead アプライアンスとデータ センター サーバの間のネットワーク セグメントです。 最適化されていないサーバ ネットワーク セグメントを監視するには、目的のデータ センターに CA Standard Monitor を展開します。

  必要に応じて、データ センターで CA Standard Monitor を使用し、Steelhead で最適化された WAN ネットワーク セグメントおよび最適化されていないサーバ ネットワーク セグメントの両方を監視します。

管理コンソール はネットワーク セグメントをアプリケーション名に追加します。たとえば、SMTP [Client]、SMTP [WAN]、SMTP [Server] のようになります。 以下の例では、SMTP アプリケーションは最適化されていないアプリケーションのパフォーマンスを示します。 データ センター内のローカル ユーザからデータが送信されるため、最適化されていないアプリケーション レスポンス時間はより速くなります。



監視フィード割り当て

CA Standard Monitor 上の監視フィードがサーバ上の最適化されていない TCP トラフィックを監視するための最適なソースである場合、管理コンソールは自動的にこの監視フィードをサーバに割り当てます。

ネットワーク セグメントのインシデントしきい値

管理コンソール では、WAN 最適化ネットワークの各セグメントに対して、異なるパフォーマンスしきい値を設定します。 パフォーマンス変動に対する 管理コンソール の感度を増減させるには、各ネットワーク セグメントのパフォーマンスしきい値を編集します (P. 186)。

Steelhead で最適化されたトラフィックを監視する場合、クライアント ネットワーク セグメントに対して設定したインシデントしきい値は、監視デバイスが展開されているブランチに適用されます。 アプリケーション パフォーマンスを評価し、インシデントを作成するには、監視デバイスはクライアント コンピュータとブランチ Steelhead アプライアンスとの間のトラフィックを観測する必要があります。

パケット キャプチャ調査

最適化されていないサーバ トラフィックを監視する監視デバイスは、パケット キャプチャ調査も実行します。

最適化されていないサーバ トラフィックを監視するために CA Standard Monitor を使用している場合、監視デバイスは以下の事柄を実行します。

- 管理コンソールがインシデントを作成した後、パケット キャプチャ調査を起動します。
- 一度に 1 つのパケット キャプチャ調査を実行します。
- 最適化されていないサーバ セグメントをキャプチャします。別の監視デバイスの方がサーバ SPAN に近い場合、対応する監視フィードがサーバに割り当てられます。
- 監視デバイスからユーザのローカル コンピュータにパケット キャプチャ ファイルをコピーします。 パケット キャプチャ ファイルのサイズによっては、パケット キャプチャ調査を開くのに長時間を要する場合があります。
- CA Standard Monitor は、長期的なパケット格納を提供しません。

最適化停止時の監視

最適化の中断時間の長さに応じて、管理コンソール では、影響を受けるトラフィックに対して異なるレポーティング方法を使用します。 必要な場合、管理コンソール をリセットして、最適化における最近の変更およびレポートを最適化として無視します。

一時的な中断

監視フィードが Steelhead で最適化されたパケットの受信を一時的に停止した場合、管理コンソール は、最適化されていないサーバ SPAN からのデータを使用して、サーバ セグメントのアプリケーションについてレポートします。 複数の基準を使用して中断が一時的か永続的かを判断しますが、一時的な中断は通常 20 分以内です。

サーバ セグメントでミラーリング スイッチ ポートから最適化されていないアプリケーション データが 管理コンソール で一時的にレポートされるときには、以下の状態になります。

- ［最適化］ページのすべてのメトリックは正確です（ただし、すべてのメトリックの入力があるとは限りません）。
- 最適化されていないセッションの測定はクライアントまたは WAN のセグメントに影響しません。
- 管理コンソール は、目的のサーバに最も近いミラーリング スイッチ ポートからのより正確なデータを使用するため、サーバ セグメントは正確です。
- ［エンジニアリング］ページの［ネットワーク ラウンドトリップ時間［サーバ］］は、100 パーセントのローカル ACK が取得されなくなったため、増大を示します。 パススルー測定では、クライアントに対する実際のネットワーク ラウンドトリップ時間が示されます。
- ［再送信遅延［サーバ］］および［パケット ロスの割合［サーバ］］は増加する場合があります。

最適化データが再開すると、管理コンソール では自動的にクライアント、WAN、およびサーバの各セグメントのセグメント化されたアプリケーション データをレポートします。

最適化された監視に対する一時的な中断は、たとえば以下の場合に発生します。

- 最適化の停止。 この種の中断は、Steelhead アプライアンスに、さらにセッションを最適化するためのリソースがない場合に発生します。
- 監視の停止。 この種の中断は、Steelhead アプライアンスと監視デバイスの間のリンクに断絶がある場合に発生します。 監視デバイスが監視 NIC でパケットを受信しなくなった場合、監視は停止します。

恒久的な変更

20 分を超えて監視デバイスが最適化されたパケット データを受信しなくなった場合、管理コンソール では障害が永続的であると通常見なされます。 この場合 管理コンソール は、アプリケーションのサーバ セグメント内の最適化されていないトラフィック（たとえば HTTP ［サーバ］）をレポートすることを停止します。 代わりに 管理コンソール は、最適化されていないアプリケーションでのサーバ SPAN データ（HTTP）についてレポートします。 最適化が再開すると、管理コンソール は自動的にネットワーク セグメントの最適化アプリケーションの監視を再開します。

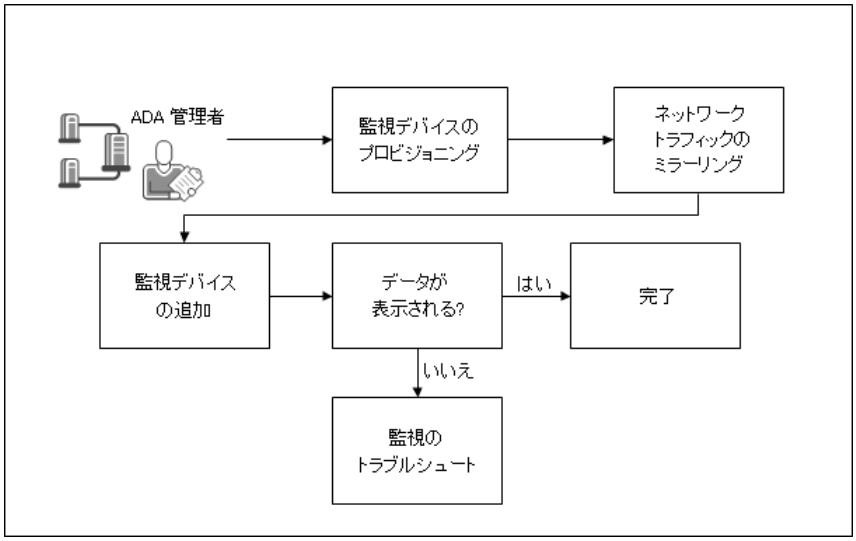
たとえば、様々なアプリケーションを最適化する利点を測定するために WAN 最適化をセットアップするとき、待機する必要はありません。 最適化における変化をすぐにレポートするため、管理コンソール 上で最適化されたアプリケーションをリセット (422P. , 437P.)できます。

詳細:

最適化アプリケーションのリセット (P. 437)

監視デバイスの追加

データ センターおよび支社の Steelhead アプライアンス間の WAN 最適化状況を可視化するには、監視デバイスを追加します。 Steelhead アプライアンス間の WAN 最適化を監視することで、ネットワークの各セグメントにおいて、WAN 最適化が個々のアプリケーション レスポンス時間に及ぼす影響を確認できます。



次の手順に従ってください:

1. 監視デバイスをプロビジョニング (P. 484) します。
2. ネットワーク トラフィックをミラーリング (P. 484) します。
3. 監視デバイスを追加 (P. 489) します。
4. （オプション）監視をトラブルシュート (P. 495) します。

監視デバイスに関する考慮事項

Steelhead で最適化されたトラフィックを監視する場合、以下の点に留意します。

- CA Standard Monitor は、以下の Steelhead 設定を監視します。
  - 物理インパス
  - WCCP（GRE または レイヤ 2 リダイレクト）設定を使用した仮想インパス
- CA Standard Monitor では、自動的に以下の Steelhead WAN 表示モードがサポートされています。
  - *Correct addressing*： WAN を介して Steelhead アプライアンスのアドレスおよびポートを使用します。
  - *Full Transparency*： パケット ヘッダ フィールドのクライアントとサーバの IP アドレスおよびポート番号を保持します。
- WAN セグメントをレポートするには、データ センターの CA Standard Monitor は WAN ネットワーク セグメントの Steelhead 最適化トラフィックを監視する必要があります。 2 つの NIC で設定されている場合、単一の CA Standard Monitor で 2 つまでの Steelhead アプライアンスを監視できます。
- サーバ セグメントをレポートするには、監視デバイスはデータ センターの最適化されていないサーバ トラフィックを監視する必要があります。必要な場合、データ センターの CA Standard Monitor を使用して、最適化されていないサーバ トラフィックを監視します。Steelhead で最適化された WAN トラフィックおよび最適化されていないサーバ セグメント トラフィックを監視するには、個別の監視 NIC が必要です。
- クライアント セグメントをレポートするには、ブランチの CA Standard Monitor はブランチ クライアント コンピュータとブランチ Steelhead との間のトラフィックを監視する必要があります。
- CA Application Delivery Analysis は Web アプリケーションの監視に URL は使用しませんが、たとえば ポート 80 上で全 HTTP トラフィックを監視できます。

監視デバイスのプロビジョニング

データ センターで（および必要に応じブランチで） Steelhead で最適化されたトラフィックを監視するには、CA Standard Monitor をプロビジョニングします。

監視デバイスの場所に基づいてメモリを割り当てます。

- データ センター（推奨） : 2 GB （2048 MB）
- ブランチ オフィス（推奨） : 1 GB （1024 MB）

Steelhead で最適化されたトラフィックを監視する場合、データ センターの CA Standard Monitor はデータ センター LAN 上の最適化されていないトラフィックも監視できます。 同じ監視デバイスを使用して WAN で最適化されたトラフィックおよび最適化されていないトラフィックの両方を監視するには、個別の監視 NIC が必要です。

監視デバイスをプロビジョニングする場合、以下の点に留意します。

- CA Application Delivery Analysis セットアップ プログラムを使用して CA Standard Monitor をインストールします。 CA サポート Web サイト support.ca.com から CA Application Delivery Analysis.iso をダウンロードします。
- 管理コンソール が NTP （Network Time Protocol）を使用する場合、監視デバイス上で NTP を設定します。
- 監視デバイスが、TCP-7878 上の割り当て済み CA Standard Monitor と通信できること。

注: CA Standard Monitor をプロビジョニングする詳細については、CA Standard Monitor の「インストール ガイド」を参照してください。

ネットワーク トラフィックのミラーリング

ネットワーク タップを使用するか、CA Standard Monitor にネットワーク トラフィックをミラーリングします。 どのネットワーク セグメントであるかによって、パケット ミラーの要件は変わります。

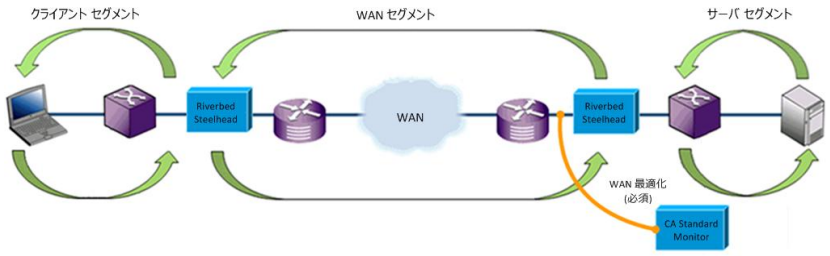
WAN ネットワーク セグメント - 物理インパス

WAN ネットワーク セグメントをレポートするには、データ センターの CA Standard Monitor は、Riverbed Steelhead アプライアンス間の最適化された TCP トラフィックを受信する必要があります。

CA Application Delivery Analysis では、Steelhead 物理インパス設定がサポートされています。 ネットワーク タップを使用するか、データ センター Steelhead アプライアンスからのトラフィックを監視デバイス上の監視 NIC にミラーリングします。

CA Application Delivery Analysis がデータ センターの最適化されていないサーバ ネットワーク セグメントをまだ監視していない場合、CA Standard Monitor を使用して WAN で最適化されたサーバ トラフィックおよび最適化されていないサーバ トラフィックの両方を監視します。

以下の Steelhead 物理インパス設定では、CA Standard Monitor は WAN ネットワーク セグメントの最適化されたトラフィックのミラー コピーを受信します。



詳細情報:

サーバ ネットワーク セグメント (P. 488)

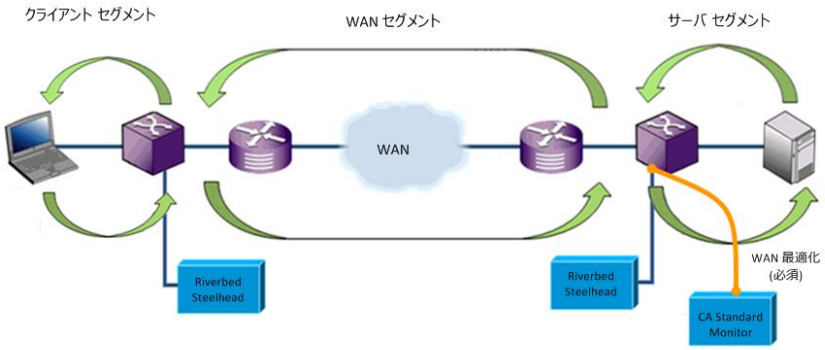
WAN ネットワーク セグメント - 仮想インパス

WAN ネットワーク セグメントをレポートするには、データ センターの CA Standard Monitor は、Riverbed Steelhead アプライアンス間の最適化された TCP トラフィックを受信する必要があります。

CA Application Delivery Analysis では、WCCP（GRE または レイヤ 2 リダイレクト）を使用した Steelhead 仮想インパス設定がサポートされています。ネットワーク タップを使用するか、データ センター Steelhead アプライアンスからのトラフィックを監視デバイス上の監視 NIC にミラーリングします。

CA Application Delivery Analysis がデータ センターの最適化されていないサーバ トラフィックをまだ監視していない場合、CA Standard Monitor を使用して WAN で最適化されたサーバ トラフィックおよび最適化されていないサーバ トラフィックの両方を監視します。

以下の Steelhead 仮想インパス設定では、CA Standard Monitor は WAN ネットワーク セグメントの最適化されたトラフィックのミラー コピーを受信します。



詳細情報:

サーバ ネットワーク セグメント (P. 488)

クライアント ネットワーク セグメント

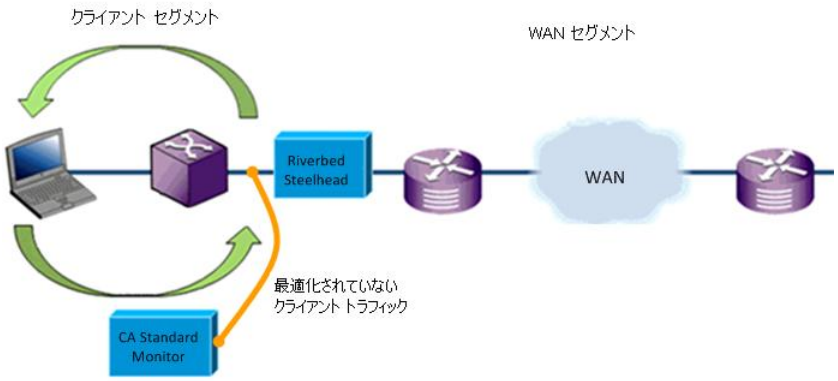
クライアント ネットワーク セグメントをレポートするには、ブランチ オフィスの CA Standard Monitor は、クライアント コンピュータおよびブランチ Riverbed Steelhead アプライアンス間の最適化されていない TCP トラフィックを受信する必要があります。

ネットワーク タップを使用するか、ブランチ スイッチからのトラフィックを監視デバイス上の監視 NIC にミラーリングします。

ブランチで最適化されたアプリケーションのリストを可視化する必要のあるリモートの場所にブランチ監視デバイスを展開することをお勧めします。 ブランチでクライアント セグメントを監視しない場合でも、CA Application Delivery Analysis ユーザは WAN ネットワーク セグメントのすべてのアプリケーションのリストを表示できます。このリストから、WAN およびサーバ ネットワーク セグメントの詳細なパフォーマンス レポートにドリルダウンできます。

または、CA PC または CA NPC で、「WAN」または「サーバ」を含むすべてのアプリケーションが含まれるグループを作成してから、そのグループおよび特定のクライアント ネットワーク上の [エンジニアリング] ページ レポートをフィルタします。

クライアント コンピュータとブランチ Steelhead アプライアンスの間の最適化されていないトラフィックを、監視デバイス上の監視 NIC へミラーリングします。 以下の Steelhead 物理インパス設定では、クライアント コンピュータとブランチ Steelhead アプライアンスとの間のクライアント トラフィックは、CA Standard Monitor にミラーリングされます。



サーバ ネットワーク セグメント

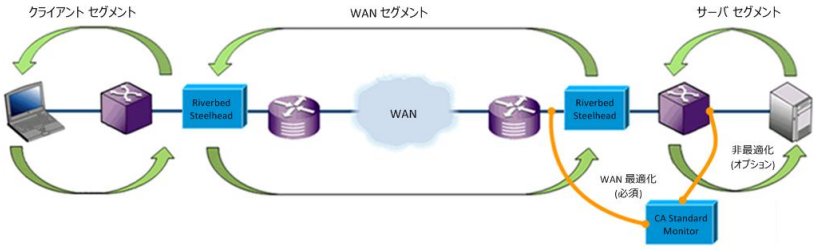
サーバ ネットワーク セグメントをレポートするには、データ センターの CA Standard Monitor は、データ センター サーバおよびデータ センター サーバ スイッチ間の最適化されていない TCP トラフィックを受信する必要があります。

ネットワーク タップを使用するか、サーバ スイッチからのトラフィックを監視デバイス上の別の監視 NIC にミラーリングします。

CA Application Delivery Analysis では、データ センターの CA Standard Monitor がサーバ ネットワーク セグメントの最適化されていないトラフィックを監視することを必要とします。

CA Application Delivery Analysis がデータ センターの最適化されていないサーバ トラフィックをまだ監視していない場合、CA Standard Monitor を使用して WAN で最適化されたサーバ トラフィックおよび最適化されていないサーバ トラフィックの両方を監視します。

サーバとデータ センター スイッチとの間の最適化されていないパケットを監視デバイス上の別の監視 NIC にミラーリングします。 以下の Steelhead 物理インパス設定では、CA Standard Monitor は WAN セグメントの最適化されたトラフィックおよびサーバ セグメントの最適化されていないトラフィックの両方を監視します。



監視デバイスの追加

レポート作成を開始するために、CA Standard Monitor を管理コンソールに追加します。

ネットワーク上で現在利用可能でない監視デバイスを追加する場合、監視がネットワークで利用可能になった後、監視デバイス を同期 (P. 290)して、監視 と 管理コンソール との間の通信を確立します。

次の手順に従ってください:

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

   ［Standard Monitor のプロパティ］が表示されます。
4. ［Standard Monitor のプロパティ］のフィールドに入力します。 監視デバイス プロパティの指定については、［ヘルプ］をクリックしてください。

   監視 NIC を指定するときには、パケット ソースの指定も忘れないようにします。 たとえば、パケットのソースが Steelhead 物理インパス設定である場合は、［Riverbed WAN 物理インパス］オプションを選択します。
5. ［OK］をクリックします。

   監視 が［ADA 監視デバイス リスト］に表示されます。
6. リンクをクリックし、管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義と 監視デバイス を同期します。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

   5 ～ 10 分後に［最適化］ページが表示されます。
7. WAN に最適化されたアプリケーションに関するレポートについて参照するには、［最適化］ページの［ヘルプ］をクリックしてください。

   アプリケーションのデータが表示されない場合は、監視デバイスのトラブルシューティングを行います。

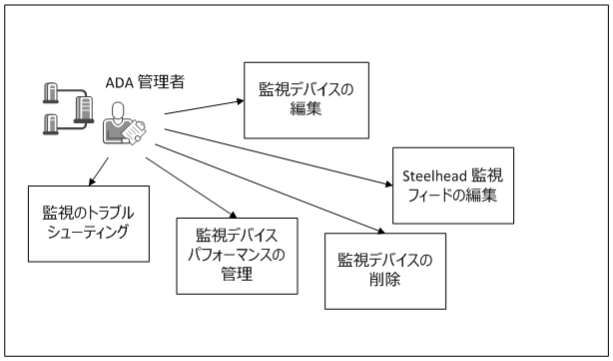
8. 重複する IP トラフィックを分けるためにドメインを使用している場合は、Steelhead 監視フィードを編集してドメインを割り当てます。

詳細:

監視フィードの編集 (P. 492)

監視デバイスの管理

監視デバイスの管理では、以下のタスクの実行します。



タスク
監視デバイスの編集 (P. 491)
Steelhead 監視フィードの編集 (P. 492)
監視デバイスのパフォーマンスの管理 (P. 493)
監視デバイスの削除 (P. 491)
監視のトラブルシュート (P. 495)

監視デバイスの編集

たとえば、インシデント レスポンスを割り当てるには、監視デバイスを編集します。監視デバイスを編集しているときに、任意の 監視デバイス インシデントを表示することもできます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして編集します。
4. 3 番目の［表示項目］メニューで［プロパティ］をクリックします。

   ［Standard Monitor のプロパティ］が表示されます。

   監視デバイス に対するインシデントを表示するには、3 番目の［表示項目］メニューで［インシデント］をクリックします。
5. ［インシデント レスポンス］をクリックし、［OK］をクリックします。この手順によってインシデント レスポンスが選択されます。

詳細:

監視デバイス インシデントの表示 (P. 306)

監視フィードの編集

特定のドメインを監視デバイスに割り当てるには、監視フィードを編集します。デフォルトでは、新規の監視フィードは「デフォルト ドメイン」に割り当てられます。

管理コンソールは、パケット ソースに基づいて監視フィードに名前を付けます。

IP アドレス 物理 Riverbed または *IP アドレス* 仮想 Riverbed

監視フィードが WAN ネットワーク セグメントから Steelhead で最適化されたパケットを受信することを示します。たとえば、IP 1.1.6.44 である監視 NIC および Steelhead 物理インパス設定は、「1.1.6.44 物理 Riverbed」と命名されます。

IP アドレス パケット

監視フィードがサーバ ネットワーク セグメントから最適化されていないパケットを受信することを示します。 たとえば、IP 1.1.5.43 である監視 NIC は「1.1.5.43 パケット」と命名されます。

IP アドレス クライアント セグメント

監視フィードがクライアント ネットワーク セグメントから最適化されていないパケットを受信することを示します。たとえば、IP 1.1.6.44 である監視 NIC は「1.1.6.44 クライアント セグメント」と命名されます。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

   ［ADA 監視デバイス リスト］にスクロールし、目的のパケット監視フィードまたは Steelhead 監視フィードを持つ Standard Monitor を探して、 をクリックします。
3. ［監視フィード］セクションにスクロールし、 をクリックして監視フィードを編集します。 詳細については、［ヘルプ］をクリックしてください。
4. ［更新］をクリックします。

5. 管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義を 監視デバイス と同期するリンクをクリックします。

   監視デバイスが同期中にアプリケーション パフォーマンスの監視を一時的に停止します。 監視への割り込み数を最小限にするには、監視デバイス を同期する前に変更をすべて完了します。

詳細情報:

テナントの管理 (P. 113)
監視フィードのペアの作成 (P. 291)

監視パフォーマンスの管理

監視デバイスから 管理コンソール へのデータ送信が 15 分を超えて停止した場合、管理コンソール は自動的に「メジャー」 監視デバイス インシデントを作成します。

詳細情報:

監視デバイス インシデントのしきい値の編集 (P. 307)

監視デバイスの削除

CA Standard Monitor の監視デバイスを削除して、レスポンス時間データのソースとして削除するようにします。 監視デバイスを削除すると、対応する監視フィードに固定されていたすべてのサーバは解除され、別の監視フィードが自動的に割り当てられます。 監視フィードの割り当てを更新するのに 10 分程度かかる可能性があります。

監視フィードにサーバを固定していた場合、監視デバイスが一時的にオフラインである場合でもサーバ トラフィックの監視を続行するには、以下のオプションを考慮します。

- 監視デバイスを削除する前に、別の監視フィードにサーバを固定します。 監視デバイスをオンラインに戻す場合、監視フィードに適切なサーバを固定します。
- 監視デバイスを削除します。別の監視フィードが自動的に割り当てられますが、監視フィード割り当てを更新するのに 10 分程度かかる可能性があります。

次の手順に従ってください:

1. ［環境管理］ページをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。
3. ［ADA 監視デバイス リスト］までスクロールし、 をクリックして監視デバイスを削除します。
4. プロンプトで［削除を続行］をクリックします。 この手順によって監視デバイスが削除されます。

   監視デバイスは、［ADA 監視デバイス リスト］から削除されます。

監視デバイスのトラブルシューティング

監視デバイスのトラブルシューティングを行い、特定のネットワーク セグメントのレポート データが存在しない問題を解決します。

監視デバイスを追加するときは、監視デバイス を同期 (P. 290) して 監視 と管理コンソール の間の通信を確立します。 監視デバイスの追加後、ネットワーク セグメント上の最適化されたアプリケーション パフォーマンスがレポートされるまでに、最大 10 分程度の時間がかかります。

セグメント化されたアプリケーション データが 管理コンソール に表示されない場合、各セグメントをトラブルシューティングします。

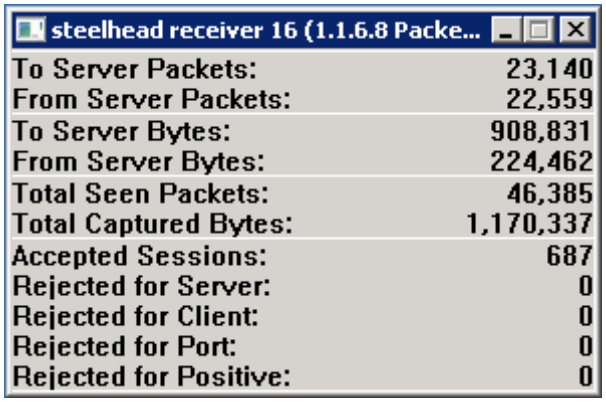
- WAN ネットワーク セグメント
  - Steelhead レシーバ統計を表示して、監視デバイスに Steelhead 監視フィード上のアクティブ セッションがあることを確認します。
  - Standard Monitor のプロパティを開いて、Steelhead で最適化されたトラフィックを受信する監視 NIC に、データ センター内の Steelhead アプライアンスの正しいインパス IP アドレスが設定されていることを確認します。
  - 監視デバイスの監視ポートからのパケット キャプチャを取得し、Steelhead アプライアンスの MAC アドレスが含まれていることを確認します。
- サーバ ネットワーク セグメント
  - SPAN レシーバ統計を表示して、データ センター内の監視デバイスに、パケット ミラー監視フィード上のアクティブ セッションがあることを確認します。
  - Standard Monitor のプロパティを開いて、最適化されていないサーバ トラフィックを受信する監視 NIC が、パケット ミラーのデータ ソースであることを確認します。
- クライアント ネットワーク セグメント
  - SPAN レシーバ統計を表示して、ブランチ内の監視デバイスに、パケット ミラー監視フィード上のアクティブ セッションがあることを確認します。
  - Standard Monitor のプロパティを開いて、最適化されていないクライアント トラフィックを受信する監視 NIC が、クライアント セグメント監視のデータ ソースであることを確認します。

Steelhead レシーバ統計の表示

CA Standard Monitor が特定の監視 NIC 上で受信する、Steelhead で最適化された TCP パケット データの詳細については、パケット カウンタ統計を参照してください。

重要: 開始前に、監視デバイスを同期します。カウンタ ウィンドウを表示するには、監視デバイスを同期する必要があります。

パケット カウンタは以下の情報を表示します。



サーバへのパケット数

クライアントからサーバに送信されたパケットの総数です。

サーバからのパケット数

サーバからクライアントに送信されたパケットの総数です。

サーバへのバイト数

クライアントからサーバに送信されたバイト総数です。

サーバからのバイト数

サーバからクライアントに送信されたバイト総数です。

参照されたパケット総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総数です。

注: 監視 が正常に実行されている場合、［参照されたパケット総数］は［受信済みパケット数］と一致します。監視 が受信パケットの一部を検査できない場合、［参照されたパケット総数］が［受信済みパケット数］を下回ります。また、この場合、［ドロップされたパケット数］が増加します。 詳細については、「ドロップされたパケット数」を参照してください。

キャプチャされたバイト総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総バイト数です。

注: CA Standard Monitor は、各パケット ヘッダを検査して、パケットが指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するかどうかを判別します。詳細については、「参照されたパケット総数」を参照してください。

承認済みセッション数

管理コンソール 上の有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッションの数です。

サーバ関連の拒否

サーバ サブネットにサーバ IP が一致しなかった TCP セッションの数です。

クライアント関連の拒否

クライアント ネットワークにクライアント IP が一致しなかった TCP セッションの数です。

ポート関連の拒否

管理コンソール が無視するポートのリストにサーバ ポートが一致する TCP セッションの数です。

ポジティブ関連の拒否

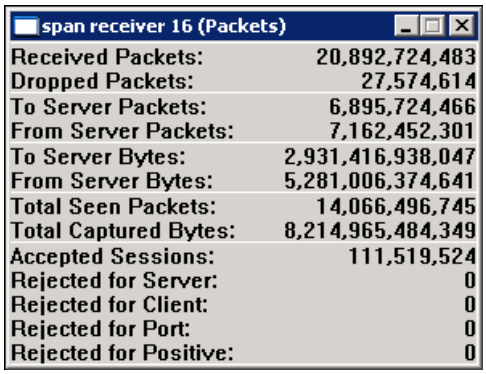
将来の使用に備えて予約されています。

SPAN レシーバ統計の表示

CA Standard Monitor が特定の監視 NIC 上で受信する、最適化されていない TCP パケット データの詳細については、パケット カウンタ統計を参照してください。

重要: 開始前に、監視デバイスを同期します。カウンタ ウィンドウを表示するには、監視デバイスを同期する必要があります。

パケット カウンタは以下の情報を表示します。



受信済みパケット数

CA Standard Monitor 上の監視 NIC によって受信されてはいるが未検査のパケットの総数です。

注: パケット ヘッダの検査によって、アプリケーション レスポンス時間メトリックを計算するためにこれらのパケットを使用できるようになります。 詳細については、「参照されたパケット総数」を参照してください。

ドロップされたパケット数

監視 NIC には到達したがパケット ヘッダは検査されなかったパケットの総数です。 CA Standard Monitor が他のパケットの処理で高負荷状態であり、パケット キャプチャ ドライバ バッファがいっぱいであった場合、パケットはドロップされます。

サーバへのパケット数

クライアントからサーバに送信されたパケットの総数です。

サーバからのパケット数

サーバからクライアントに送信されたパケットの総数です。

サーバへのバイト数

クライアントからサーバに送信されたバイト総数です。

サーバからのバイト数

サーバからクライアントに送信されたバイト総数です。

参照されたパケット総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総数です。

注: 監視 が正常に実行されている場合、［参照されたパケット総数］は［受信済みパケット数］と一致します。監視 が受信するすべてのパケットを検査できない場合、［参照されたパケット総数］は、［受信済みパケット数］および［ドロップされたパケット数］より少なくなります。 詳細については、「ドロップされたパケット数」を参照してください。

キャプチャされたバイト総数

指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するパケットの総バイト数です。

注: CA Standard Monitor は、各パケット ヘッダを検査して、パケットが指定されたアプリケーション ポート、クライアント ネットワーク、およびサーバ サブネットに一致するかどうかを判別します。詳細については、「参照されたパケット総数」を参照してください。

承認済みセッション数

管理コンソール 上の有効なアプリケーション/サーバ/ネットワークの組み合わせに一致する TCP セッションの数です。

サーバ関連の拒否

サーバ サブネットにサーバ IP が一致しなかった TCP セッションの数です。

クライアント関連の拒否

クライアント ネットワークにクライアント IP が一致しなかった TCP セッションの数です。

ポート関連の拒否

管理コンソール が無視するポートのリストにサーバ ポートが一致する TCP セッションの数です。

ポジティブ関連の拒否

将来の使用に備えて予約されています。

詳細:

クライアント ネットワークの仕組み (P. 34)
アプリケーションの仕組み (P. 122)
サーバの仕組み (P. 79)
CA Standard Monitor の編集 (P. 336)

アクティブ セッションの表示

直近の 5 分のレポート間隔中にレポートされたアクティブな IPv4 ベースの TCP セッションの数を表示するには、［アクティブ セッション数］ページを使用します。

アクティブ セッション情報を使用して、CA Application Delivery Analysis が TCP セッションを監視していることを確認できます。 管理コンソール は、アプリケーション ポートおよびネットワーク セグメント別にサーバ上のアクティブ TCP セッション数をレポートします。たとえば、「ポート 9088［WAN］」は、WAN ネットワーク セグメントのポート 9088 アプリケーション トラフィックに関するセッション情報を表示します。

詳細:

［監視フィード］でのアクティブ セッション数の表示 (P. 293)

用語集

3 方向ハンドシェーク

TCP プロトコルにおける *3 方向ハンドシェーク*は、クライアントとサーバの間で接続を確立するために使用されます。 SYN パケット (P. 508)がクライアントからサーバに送信され、接続準備が開始されます。 すると、SYN-ACK パケット (P. 508)がサーバからクライアントに送信され、クライアントからの SYN の受信の確認応答が行われます。最後に、ACK パケット (P. 504)がクライアントからサーバに送信され、サーバからの SYN-ACK の受信の確認応答が行われた後、TCP 接続が確立されます。監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で 3 方向ハンドシェイクを使用します。

5 分サマリ ファイル

*5 分サマリ ファイル*は、CA Application Delivery Analysis Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor、または Cisco NAM によって作成されます。各パフォーマンス メトリック/アプリケーション/サーバ/ネットワークの組み合わせ (P. 513)に対する 5 分間の平均から構成されます。

ACK パケット

TCP 接続の設定中、サーバからの SYN-ACK パケット (P. 508)の受信を確認するために、*ACK パケット*がクライアントによってサーバに送信されます。

CA ADA Availability Poller サービス

CA ADA Availability Poller サービスは、アプリケーションの可用性をチェックします。 アプリケーションをホストするサーバが CA Standard Monitor によって監視されている場合、このチェックは監視デバイスによって実行されます。 それ以外の場合は、CA ADA マネージャ上の CA ADA Availability Poller サービスがアプリケーションの可用性をチェックします。

CA ADA Batch サービス

*CA ADA Batch サービス*は、CA ADA マネージャ上で CA ADA Master Batch サービスによって処理される .dat データ ファイルをステージングします。このサービスは CA Standard Monitor 上で実行されます。

CA ADA Data Pump サービス

*CA ADA Data Pump サービス*は、CA ADA マネージャ上でデータベース メンテナンスを毎週実行します。

CA ADA Data Transfer Manager サービス

*CA ADA Data Transfer Manager サービス*は、CA ADA マネージャ上で定義されたアプリケーション、サーバ、クライアント ネットワークに基づいて、Cisco WAE デバイス監視を同期します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Inspector Agent サービス

CA ADA Inspector Agent サービスは、アプリケーション、サーバ、および関連するネットワーク上で調査を起動します。 アプリケーションをホストするサーバが CA Standard Monitor によって監視されている場合、調査は監視デバイスから起動されます。 そうでない場合、CA ADA マネージャ上の CA ADA Inspector Agent サービスが調査を起動します。

CA ADA Inspector サービス

*CA ADA Inspector サービス*は、CA ADA Master Batch サービスによって処理される 5 分間の .dat ファイルを CA ADA マネージャ データベースにロードし、CA ADA Inspector Agent サービスと通信して調査を起動します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Master Batch サービス

*CA ADA Batch サービス*は、管理コンソール 上で実行され、CA Standard Monitor で CA ADA Batch サービスから受信したデータ ファイルを 5 分の .dat ファイルに格納します。 このサービスは CA ADA マネージャ上で実行されます。

CA ADA Messenger サービス

*CA ADA Messenger サービス*は、CA ADA マネージャ上に定義されたアプリケーション、サーバ、クライアント ネットワークに基づいて、割り当てられた CA Standard Monitor、CA Multi-Port Monitor、CA GigaStor 監視デバイス 上で監視を同期します。このサービスは CA ADA マネージャ上で実行されます。

CA ADA Monitor Management サービス

*CA ADA Monitor Management サービス*は、CA ADA マネージャからの要求に応答し、.dat ファイルを転送します。 このサービスは CA Standard Monitor 上で実行されます。

CA ADA Monitor サービス

*CA ADA Monitor サービス*は、ミラーリングされた TCP パケットおよびパケット要約ファイルを CA ADA 監視デバイスから受信します。 このサービスは、CA Standard Monitor および CA ADA マネージャ上で実行されます。

CA ADA Reader サービス

*CA ADA Reader サービス*は、CA GigaStor 上で実行され、TCP ヘッダから構成されるパケット要約ファイルを、割り当てられた CA ADA Standard Monitor または Multi-Port Monitor にメトリック計算のために送信します。

CA Application Delivery Analysis マネージャ（CA ADA マネージャ）

*CA Application Delivery Analysis マネージャ（CA ADA マネージャ）*は、CA ADA アーキテクチャのコンポーネントで、複数の監視デバイスに対して中央での設定、分析、管理、およびレポーティング機能を提供します。 CA ADA マネージャは、割り当てられた監視デバイスからレスポンス時間メトリックを受信します。これには、CA ADA Standard Monitor、Multi-Port Monitor、Virtual Systems Monitor、CA GigaStor、または Cisco NAM が含まれます。

CA Observer Expert

CA Observer Expert は CA GigaStor にバンドルされています。これは、CA ADA からのアプリケーション レスポンス時間の監視を、根本原因解析のためにパケット レベル データへのドリル イン機能と組み合わせます。

FIN パケット

TCP プロトコルでは、サーバへの TCP 接続を確立するときは、SYN パケットがクライアントによって使用されます。 同様に、FIN パケットは TCP 接続の切断または終了を開始するために使用されます。監視デバイスは、FIN パケットまたは RST パケットを受信したときに、TCP 通信が終了されていると判断します。

NetQoS MySql51 サービス

CA ADA マネージャ データベースをホストする MySql サーバを開始および停止します。

OLA

パフォーマンス OLA（運用レベル契約） (P. 522)および可用性 OLA（運用レベル契約） *(P. 511)を参照*。

ping レスポンス時間調査

ping レスポンス時間調査は、ping 要求を送信してから ping 応答を受信するまでにかかる時間を測定するサーバ インシデント レスポンス (P. 515)であり、パケットのラウンドトリップ時間についてレポートします。 CA Application Delivery Analysis 管理者は、この調査を開始またはスケジュールすることもできます。

ping レスポンス時間とパケット サイズの比較調査

*ping レスポンス時間とパケット サイズの比較調査*は、さまざまなサイズの ping 要求（データ パケット）に対する ping 応答を受信するのにかかる時間を測定します。 この調査は、さまざまなパケット サイズでの過度の遅延や接続不良状態を追跡するのに役立ちます。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

RST パケット

RST パケットは、TCP セッションを正常に終了するための方法です。 Web ブラウザは通常 FIN ではなく RST でセッションを終了します。 管理コンソールは、接続ハンドシェークの間、RST パケットのみを「未対応のセッション リクエスト」としてカウントします。 監視デバイスが、TCP 3 方向ハンドシェークが完了する前に RST を検出した場合、管理コンソールはセッションが拒否されたものと認識します。

severity

重大度は、特定の期間にわたるパフォーマンス データを指定したしきい値によって分類（［なし］、［未評価］、［マイナー］、［メジャー］、および［使用不可］）します。

SNMP 経由のパフォーマンス調査

*SNMP 経由のパフォーマンス調査*は、SNMP が CPU 使用率およびメモリ使用率などのパフォーマンス情報をサーバに対してポーリングするサーバ インシデント レスポンス (P. 515)です。CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

SNMP トラップ通知

SNMP トラップ通知は、影響を受けたアプリケーション、サーバ、ネットワークの［オープン］または［クローズ］のインシデント ステータスについて SNMP マネージャに通知するアプリケーション インシデント レスポンス (P. 510)、ネットワーク インシデント レスポンス (P. 520)、またはサーバ インシデント レスポンス (P. 515)です。

SNMP プロファイル

SNMP プロファイルは、SNMPv3 ユーザ認証情報および SNMPv1 コミュニティ名と SNMPv2 コミュニティ名を管理するために管理コンソールによって使用されます。 SNMP プロファイルには、サーバまたはネットワーク デバイス上の SNMP エージェントにクエリしたり、SNMP トラップ メッセージを送信するために管理コンソールが必要とする SNMP ユーザ認証情報があります。

SPAN

SPAN（*Switched Port Analyzer*）は、ポート ミラーリングとしても知られており、1 つのスイッチ ポート上で確認されたすべてのネットワーク パケットのコピーを、別のスイッチ ポート上のネットワーク監視接続に送信するために、Cisco ネットワーク スイッチ上で使用されます。これは、通常、ネットワーク トラフィックを監視するためにネットワーク アプライアンスによって使用されます。 SPAN により、監視デバイス が、もう 1 つのスイッチ ポート上の複数のブロードキャスト ドメイン上で発生するトラフィックを確認できるようになります。 SPAN の機能はシャーシによって異なります。

SYN-ACK パケット

TCP 接続セットアップ中、クライアントからの SYN パケットの受信を確認するために、SYN-ACK パケット (P. 508)がサーバによってクライアントに送信されます。 監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で SYN-ACK パケットを使用します。

SYN パケット

TCP プロトコルでは、クライアントとサーバの間の通信（接続）は 3 方向ハンドシェークによって確立されます。SYN パケットがクライアントからサーバに送信され、接続準備が開始されます。 監視デバイスは、ネットワーク上で監視されている接続の時間調整および分析で SYN パケットを使用します。

Traceroute

Traceroute は、インシデント分析で使用される 2 種類の診断ツール（ICMP または TCP）のいずれかを指します。

WAN

WAN（広域ネットワーク）は、通常複数の LAN（ローカル エリア ネットワーク）で構成される広いさまざまな地域をカバーするネットワークです。WAN は、1 つの企業の複数のオフィスで私的に使用されることも、インターネットなどで公的に使用されることもあります。

WAN 最適化デバイス

WAN 最適化デバイスは、圧縮または他のアルゴリズムによってデータ センターとリモート オフィスの間で転送されるトラフィック ボリュームを削減します。 WAN 最適化デバイスの例は、Cisco WAE デバイスや Riverbed Steelhead アプライアンスなどです。

アクション

応答アクション *(P. 511)を参照*。

アクセス層

標準的な 3 層（アクセス、ディストリビューション、コア）LAN ネットワークでは、*アクセス層*はサーバに最も近い層で、サーバをネットワークに接続します。 スイッチとハブは、通常アクセス層に分類されます。 通常、すべてのサーバ トラフィックはこの層で発生しますが、これには最多の監視ポイントが必要になります。

アプリケーション

アプリケーションは、一連のサーバ IP アドレスにわたって監視すべき TCP ポートまたはポートの範囲を指定します（たとえば /29 サーバ サブネットにおける TCP-80 トラフィックなど）。

アプリケーション インシデント

ネットワーク インシデントまたはサーバ インシデントがアプリケーションのパフォーマンスに影響を与える場合、アプリケーション インシデントが発生します。

基盤のネットワーク インシデントまたはサーバ インシデントによって、アプリケーションの結合メトリックがパフォーマンスしきい値を超える場合、結合メトリックがしきい値を超過します。

結合メトリックがしきい値を超えると場合、管理コンソールはアプリケーションへのパフォーマンス影響度を「メジャー」（オレンジ）または「マイナー」（黄色）と評価しますが、アプリケーション インシデント レスポンスを作成しません。 基盤のネットワークまたはサーバのインシデントがアプリケーションに対して発生する場合に起動するアプリケーション インシデント レスポンスを定義する必要があります。

アプリケーション インシデント レスポンス

*アプリケーション インシデント レスポンス*は、ネットワーク インシデント (P. 520)またはサーバ インシデント (P. 515)に対するアプリケーション レスポンスです。 たとえば、Exchange アプリケーションに対してアプリケーション インシデント レスポンスを設定した場合、ネットワーク インシデントが Exchange アプリケーションにアクセスするクライアントによって作成されるか、またはサーバ インシデントがアプリケーションをホストするサーバによって作成されたら、管理コンソール がインシデント レスポンスを起動します。 データ転送時間などの結合メトリック (P. 513)のしきい値を超えた場合、管理コンソール はアプリケーション インシデント レスポンスを開始しません。 管理コンソール では、アプリケーションに次のレスポンスを割り当てることができます。電子メール通知 (P. 519)、SNMP トラップ通知 (P. 507)、およびアプリケーション接続時間調査 (P. 510)。

アプリケーション接続時間調査（用語）

アプリケーション接続時間調査は、IT 部門のスタッフが TCP/IP アプリケーション ポートへの接続にかかる時間を知ることができるアプリケーション インシデント レスポンス (P. 510)です。 これには、サーバが接続確認で応答する時間が含まれます。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

インシデント

インシデントは、アプリケーション、サーバ、またはクライアント ネットワーク上の異常な動作の期間に対する注意を喚起するために、管理コンソールによってオープンされます。 「応答アクション (P. 511)」を参照してください。

インシデント レスポンス

インシデント レスポンスを使用すると、問題が発生した時点でトラブルシューティングを行い、平均修復時間を短縮することができます。 インシデント レスポンスは、ビジネス クリティカルなアプリケーション、サーバおよびネットワークに割り当てます。 インシデント レスポンスは、パフォーマンス低下についてユーザのチームに通知すると共に、パフォーマンス低下の根本原因を識別する助けになる詳細を収集するため、精力的に問題を調査するものです。

応答アクション

応答アクションは、通知の送信や調査の開始など、パフォーマンスしきい値違反に対する応答です。

可用性 OLA（運用レベル契約）

可用性 OLA は、アプリケーションが使用可能である時間の割合をレポートします。たとえば、サーバ上のアプリケーションが 1 か月の期間の 99% の間使用可能である必要があります。

監視単位

監視単位は、監視デバイスの追加によって、CA ADA マネージャ上で作成される処理の負荷です。 たとえば、CA Standard Monitor は 1 つの監視単位を利用します。CA ADA マネージャは最大 15 までの監視単位をサポートします。

監視デバイス

監視デバイスは、TCP トランザクションを監視し、アプリケーション、サーバおよびネットワークのレスポンス時間メトリックを計算します。

監視デバイス インシデント

監視デバイス インシデントは、監視デバイスのパフォーマンスおよび可用性のしきい値に対する違反が発生した場合に管理コンソールによって作成されます。 たとえば、デバイスが到達不可になった場合、デバイスではデータが表示されないか、またはデバイスがパケットを破棄します。

監視デバイスの同期

管理コンソール 上の現在のクライアント ネットワーク、サーバ サブネット、およびアプリケーション定義に基づいて TCP セッションを監視する場合に、監視デバイスを同期します。 同期中の監視への一時的な割り込み数を最小限にするには、監視デバイスを同期する前にすべての変更を完了します。

監視フィード

監視フィードは、CA Standard Monitor など、レスポンス時間情報のソースです。

観測数

観測数は、5 分間の監視の間に、監視デバイスが特定のアプリケーション/サーバ/ネットワークの組み合わせに対してパフォーマンス メトリックを計算した回数を測定します。 1 つの TCP トランザクション内でも、メトリックによって観測数が異なる場合があります。 たとえば、ネットワーク ラウンドトリップ時間の観測数の方が、サーバ レスポンス時間の観測数よりも多い場合が考えられます。 また、常に観測数が同じである、リンクなどのメトリックもあります。たとえば、各 TCP トランザクションに、それぞれ 1 つのサーバ レスポンス時間およびデータ転送時間の観測があります。 メトリックを正常、マイナー（黄色）またはメジャー（オレンジ）として評価するには、メトリックに最小観測数があることが必要です。

感度レベル

感度レベルは、0 から 200 の尺度で表される単位のない基準値です。これは、クライアント、サーバ、およびアプリケーションの各組み合わせに対して、その履歴データに基づいて新しいしきい値を計算するための固有の計算式に適用されます。 管理コンソールは、過去 30 日のパーセンタイル統計を使用して、毎晩 GMT の午前 0 時にメトリックの新しいしきい値を自動的に生成します。 管理コンソールは、各クライアント ネットワークからアプリケーションにアクセスするユーザのために、独立したしきい値のセットを自動的に生成します。

キープアライブ メッセージ

要求/レスポンスごとに新しい TCP 接続を確立するのではなく、TCP 接続を永続的に確立し、アクティブにしておくメソッドです。TCP *キープ アライブ メッセージ*は既知の形式に従うため、レスポンス時間メトリックが不正確になることはありません。 アプリケーションのキープ アライブは、シーケンス番号を 1 増やし、ペイロードを持っており、SRT（サーバ レスポンス時間）などいくつかのサーバ メトリックの測定値を不正確にする可能性があります。

拒否されたセッションの割合

*拒否されたセッションの割合*は、サーバがレポート間隔中に明示的に拒否した接続要求の割合を測定するサーバ メトリック (P. 515)です。 このメトリックは、CA ADA 管理コンソールの「未対応の TCP/IP セッション リクエスト」レポートに含まれます。

組み合わせ

*組み合わせ*は、CA ADA がレスポンス時間メトリックを計算したタイムフレーム、アプリケーション ポート、サーバ、ネットワーク、およびパフォーマンス メトリックを特定します。たとえば、管理コンソールは、過去 24 時間に Development クライアント ネットワークと通信したすべてのアプリケーションおよびサーバの平均ネットワーク接続時間をレポートすることができます。

結合メトリック

*結合メトリック*は、アプリケーションのパフォーマンス問題の原因が、アプリケーションをホストするサーバ、またはアプリケーションと通信しているネットワークのいずれか、または両方にあることを示します。CA ADA 管理コンソールでは、結合メトリックである［データ転送時間 (P. 518)］と［トランザクション時間 (P. 519)］のそれぞれに対して、パフォーマンスしきい値を設定できます。 管理コンソールはアプリケーション インシデントを作成しないことに注意してください。 ただし、結合メトリックには、ネットワークおよびサーバの両方のメトリックが含まれるので、管理コンソールはサーバやネットワークをマイナー（黄色）またはメジャー（オレンジ）と評価し、アプリケーションへの対応するパフォーマンス インパクトを評価できます。 たとえば、サーバ メトリックがマイナーと評価された場合は、管理コンソールでもアプリケーションの結合メトリックがマイナーと評価されます。

権限セット

ユーザが表示する権限を持つアプリケーション集約、サーバ集約、およびネットワーク集約の定義されたリスト。集約は 1 つ以上の権限セットのメンバになります。

コア層

標準的な 3 層（アクセス、ディストリビューション、コア）LAN ネットワークでは、*コア層*は、ディストリビューション層デバイスの高速相互接続を可能にします。 コア層には、通常、ネットワークで最も強力なルータとスイッチおよび最高速の相互接続があります。 通常、この層では、クライアントからサーバへのトランザクションのみが確認できます。

コントロール ポート アプリケーション

コントロール ポート アプリケーションは 2 つの TCP ポートを使用します。コントロール ポートはリクエスト情報を送受信します。また、データ ポートは実際のデータを送受信します。同じ監視デバイスは、トランザクション レスポンス時間を決定するためにコントロール ポートおよびデータ ポート トラフィックの両方を監視する必要があります。 どのタイプの監視デバイスも、コントロール ポート アプリケーションを監視できます。

サーバ インシデント

サーバ インシデントは、5 分間隔中に特定のアプリケーション、サーバ、ネットワークの組み合わせに対してサーバ レスポンス時間、サーバ接続時間、拒否されたセッションの割合、無応答セッションの割合など、サーバ メトリックのしきい値を超えた場合に、管理コンソールによって作成されます。

サーバ インシデント レスポンス

サーバ インシデント レスポンスは、サーバ インシデント (P. 515)に対する管理コンソールのレスポンスです。 管理コンソールでは、サーバ インシデントに次のレスポンスを割り当てることができます： 電子メール通知 (P. 519)、SNMP トラップ通知 (P. 507)、ping レスポンス時間調査 (P. 507)、SNMP 経由のパフォーマンス調査 (P. 507)、パケット キャプチャ調査 (P. 521)。

サーバ サブネット

サーバ サブネットは、各監視デバイスによって監視されるサーバ IP アドレスの連続した範囲を指定します。 アプリケーションを定義する際、アプリケーションに特定のサーバ サブネットを割り当てることで、サーバ IP アドレスの連続する範囲において管理コンソールがアプリケーションのパフォーマンスを自動的に監視できるようになります。

サーバ接続時間

SCT（サーバ接続時間）は、サーバがクライアントの SYN パケットに対して Syn-Ack を送信することで初期クライアント接続要求を確認するのにかかる時間の長さを測定するサーバ メトリック (P. 515)です。

サーバ メトリック

サーバ メトリックは、アプリケーションのパフォーマンス問題の原因が、アプリケーションをホストするサーバにあることを示します。 CA ADA 管理コンソールを使用して、次の各サーバ メトリックのパフォーマンスしきい値をカスタマイズできます： サーバ レスポンス時間 (P. 515)、サーバ接続時間 (P. 515)、拒否されたセッションの割合 (P. 513)、無応答セッションの割合 (P. 524)。

サーバ レスポンス時間

*サーバ レスポンス時間*は、サーバがクライアント要求に対して最初のレスポンスを送信するのにかかる時間または初期サーバ思考時間を測定する サーバ メトリック (P. 515)です。 サーバ レスポンス時間が増加した場合、通常は CPU、メモリ、ディスク /O などのサーバ リソースが不足しているか、アプリケーションの設計に問題があるか、または多層アプリケーション内にパフォーマンスの悪い層があることを示しています。

再送信遅延

再送信遅延は、元のパケット送信から最後の重複するパケット送信までに経過した時間を測定するネットワーク メトリック (P. 521)です。 管理コンソールは、再送信パケット数に対してだけではなく観測を通した平均としての再送信遅延をレポートします。 たとえば、10 個で 1 セットの 1 つのパケットが 300 ミリ秒の再送信時間を必要とする場合、再送信遅延は 30 ミリ秒（300 ミリ秒/10 パケット）としてレポートされます。

しきい値

「パフォーマンスしきい値 (P. 522)」を参照してください。

失効したセッション

失効したセッションは、CA ADA Monitor サービスが TCP セッションの終了（FIN または RST パケット）を検出しなかった TCP セッションの数を測定します。 一定期間非アクティブであるセッションは、メモリからクリアされ、「期限切れ」としてマークされます。 管理コンソールは、15 分間の間にパケットを観測しない場合、セッションを［期限切れ］として分類します。 オープンのままになっている期限切れセッション数が多すぎると、サーバが応答しなくなる可能性があります。

実効ネットワーク ラウンドトリップ時間

実効ネットワーク ラウンドトリップ時間は、再送信遅延 (P. 516)とネットワーク ラウンドトリップ時間 (P. 521)から構成されるネットワーク メトリック (P. 521)です。 再送信遅延は、再送信による遅延ではなく、1 ラウンドトリップあたりの再送信遅延の平均時間であることに注意してください。管理コンソールでは、2 つの平均が追加され、実際に 2 つのメトリックを組み合わせています。

推定ホップ遅延

推定ホップ遅延は、2 つのノード間で発生した遅延時間の推定値です。 管理コンソール は、たとえばトレース ルート調査 (P. 519)中に採取したすべてのサンプルの平均を使用してこの推定値を決定します。

製品権限

*製品権限*は、［環境管理］ページでユーザが実行できるアクションを決定します。

多層アプリケーション

多層アプリケーションは複数のサーバを使用するアプリケーションで、サーバ間の通信は、クライアントへのリクエストを処理するサーバとして機能すると同時に共に別のサーバのクライアントとしても機能するサーバによって実行されます。

タップ

「ネットワーク タップ (P. 520)」を参照してください。

調査

調査とは、アプリケーション、ネットワーク、およびサーバの特定のパフォーマンス データをアクティブに照会することです。 管理コンソールは、インシデントに対して調査を自動的に起動することができます。 CA ADA 管理者は、この調査を起動またはスケジュールすることもできます。

ディストリビューション層

標準的な 3 層（アクセス、ディストリビューション、コア）LAN ネットワークでは、*ディストリビューション層*はルーティング、フィルタリング、およびポリシー管理が処理される場所です。 この層には、通常、ルータおよび第 3 層のスイッチが含まれます。 アクセス スイッチがディストリビューション層にデータを送信すると、データが収集されます。 サーバが別々のスイッチ上にある場合、一部のサーバからサーバへのトランザクションはこの層で発生する可能性があります。

データ転送時間

*データ転送時間*は、最初のレスポンス（サーバ レスポンス時間 (P. 515)の終了）からその要求で送信された最後のパケットに至るアプリケーション レスポンス全体を送信するのにかかる時間を測定する結合メトリック (P. 513)です。

TCP ウィンドウに収容しきれない大量のデータを送信する場合は、データ転送時間から初期サーバ レスポンス時間を除外し、ネットワーク ラウンドトリップ時間を含めます。 レスポンス時間は、アプリケーションの設計またはサーバやネットワークのパフォーマンスの影響を受ける場合があります。

管理コンソールは、データ転送時間のしきい値を超えた場合にインシデントをオープンしません。

デバイス

デバイスは、監視されているネットワークに接続された任意の TCP/IP システムです。

電子メール通知

電子メール通知は、アプリケーション インシデント レスポンス (P. 510)、サーバ インシデント レスポンス (P. 515)、またはネットワーク インシデント レスポンス (P. 520)であり、影響を受けたアプリケーション、サーバ、またはネットワークのしきい値違反について受信者に通知します。

ドメイン

*ドメイン*は、レポート目的のためクライアント IP トラフィックを分離し、サーバのホスト名を解決するために管理コンソールが使用する DNS サーバを特定します。

トランザクション

トランザクションは、TCP 要求および後続のすべてのレスポンスのことです。 Web ページのロードなどの単一のアプリケーション トランザクションが、複数の TCP トランザクションから構成されている場合があります。

トランザクション時間

トランザクション時間は、クライアントが要求を送信してからレスポンスの最後のパケットを受信するまでに経過した時間の長さを測定する結合メトリック (P. 513)です。 トランザクション時間は、サーバ レスポンス時間 (P. 515)、ネットワーク ラウンドトリップ時間 (P. 521)、再送信遅延 (P. 516)、データ転送時間 (P. 518)の合計です。 トランザクション時間のしきい値を超えた場合、管理コンソールはインシデントをオープンしません。

トレース ルート調査

トレース ルート調査はネットワーク インシデント レスポンス (P. 520)であり、遅延とルーティングの問題を監視するために、監視デバイスとエンド ポイントの間のパスとすべてのホップを記録します。必要な場合は、各ルータに対してパフォーマンス情報を SNMP ポーリングします。 CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

ドロップされたパケット

*ドロップされたパケット*は、CA Standard Monitor 上のパケット キャプチャ ドライバか、または CA GigaStor 上の GigaStor Connector によって分析されなかったパケットです。分析されなかった理由は、監視デバイスが極度のビジー状態のため、受信したパケットの一部を処理できなかったためです。監視デバイスによってドロップされるパケットの数が多すぎる場合は、管理コンソールがメジャーの監視デバイス インシデントを作成します。 管理コンソールは、監視デバイス上の監視 NIC またはサーバ スイッチ ポートにおけるパケットのロスを監視しません。

ネットワーク インシデント

特定のアプリケーション、サーバ、ネットワークの組み合わせについて、ネットワーク ラウンドトリップ時間、ネットワーク接続時間、実効ラウンドトリップ時間、再送信遅延などのネットワーク メトリックのしきい値を 5 分間超えた場合、管理コンソールはネットワーク インシデントを作成します。

ネットワーク インシデント レスポンス

*ネットワーク インシデント レスポンス*は、ネットワーク インシデント (P. 520)に対する CA ADA のレスポンスです。 CA ADA 管理者は、電子メール通知 (P. 519)、SNMP トラップ通知 (P. 507)、トレース ルート調査 (P. 519)をネットワーク インシデントに割り当てることができます。

ネットワーク接続時間

ネットワーク接続時間（*NCT*）は、サーバが Syn-Ack を送信してからクライアントが Ack を返送するまでの時間の長さを測定するネットワーク メトリック (P. 521)です。 ネットワークが混雑していない場合、それは距離およびシリアライゼーションによる最低限の遅延を表すネットワーク遅延を示し、現在のネットワーク アーキテクチャで可能な最良のラウンドトリップ時間を示します。 この値が突然上昇した場合は、一般に輻輳状態が原因と考えられますが、停滞している（上昇したままになる）場合は通常パス変更が原因です。

ネットワーク タイプ

アプリケーションへの同じ物理アクセスを共有するネットワークのグループ。 たとえば、リモートサイトでのサブネットはすべて、データ センターへの同じ WAN リンクを共有します。

ネットワーク タップ

ネットワーク タップは、コンピュータ ネットワークで転送されるデータにアクセスするためのハードウェア デバイスです。タップの設置後、タップに監視デバイスを接続できます。この場合、監視されているネットワークには影響を与えません。タップを使用する場合、表示できるトラフィックは、スイッチ ネットワークのただ 1 つのブロードキャスト ドメインにおいて両方向（アップストリームおよびダウンストリーム）で発生するトラフィックです。

ネットワーク メトリック

ネットワーク メトリックは、アプリケーションのパフォーマンス問題がアプリケーションと通信しているネットワークによって引き起こされていることを示します。 CA Application Delivery Analysis 管理コンソールを使用して、次の各ネットワーク メトリックのパフォーマンスしきい値をカスタマイズできます： ネットワーク ラウンドトリップ時間 (P. 521)、ネットワーク接続時間 (P. 520)、実効ネットワーク ラウンドトリップ時間 (P. 516)、および再送信遅延 (P. 516)。

ネットワーク ラウンドトリップ時間

*ネットワーク ラウンドトリップ時間*は、ロスしたパケットを除くパケットがネットワーク上のサーバとクライアントの間（双方向）を送信されるのにかかる時間を測定するネットワーク メトリック (P. 521)です。 アプリケーション、サーバおよびクライアント処理時間は除外されます。

ネットワーク領域

ネットワーク領域は、広範のサブネット定義をより狭いサブネットに自動的に展開するために使用される管理コンソール ツールです。 ネットワークは最大 256 の領域まで定義できます。たとえば 256 の /24 ネットワークを定義するために /16 ネットワークの 256 の領域を定義します。 ネットワーク領域を使用する場合、管理コンソールは広範のネットワーク定義ではなく狭い方のネットワーク領域サブネット定義をレポートします。

廃棄パケット

廃棄パケットは、パケットが管理コンソールで指定されたアプリケーション、サーバ、およびクライアント ネットワークのリストに一致しなかったために、監視デバイスによって意図的に破棄されたパケットのことです。

パケット キャプチャ調査

パケット キャプチャ調査は、問題が発生している特定のサーバ、アプリケーション ポート、およびネットワークをフィルタしてキャプチャするアプリケーション インシデント レスポンス (P. 510)またはサーバ インシデント レスポンス (P. 515)です。CA ADA 管理者はこの調査を起動またはスケジュールすることもできます。

パケット要約ファイル

パケット要約ファイルには、Cisco WAE デバイスまたは CA GigaStor Connector からの TCP ヘッダが含まれます。

パケット ロスの割合

*パケット ロスの割合*は、サーバの隣にある監視デバイスからのネットワーク内のデータ全体に対して再送信されたデータの比率を測定するネットワーク メトリック (P. 521)です。監視デバイスは、ネットワーク パスにおけるサーバからクライアントへの方向でのデータ ロスにより、サーバによって再送信されたパケットを確認できます。 データ ロスがクライアントからサーバへの方向でサーバに到達する前に発生した場合、監視デバイスはパケット ロスを観測できないため、そのロスは［パケット ロスの割合］には含まれません。 管理コンソールの［エンジニアリング］ページでは、パケット ロスの割合は QoS レポートに含まれます。

パフォーマンス運用レベル アグリーメント（パフォーマンス OLA）

パフォーマンス運用レベル アグリーメント（パフォーマンス OLA）は、リモートサイトのアプリケーション パフォーマンス目標の適合を評価することができます。 デフォルトでは、管理コンソールは、アプリケーション パフォーマンスの運用レベルを定義していません。

パフォーマンスしきい値

パフォーマンスしきい値は、許容可能なパフォーマンス挙動の境界値です。これは、すべてのアプリケーションに対してデフォルトで存在します。管理コンソールは、しきい値によってデータを評価できます。 インシデント作成、インシデント レスポンス、および調査に貢献します。

フラグメント化されたパケット

フラグメント化されたパケットとは、ネットワークをトラバースするときに複数のパケットに分割されたパケットです。

ベースライン

ベースラインは、ネットワークの過去の標準的なパフォーマンスを参照できるようにします。管理コンソールは、サーバ上のアプリケーション ポートとクライアント ネットワークの間の全 TCP セッションのベースラインを自動的にレポートします。 ベースラインは、アプリケーションの現在のパフォーマンスを過去のパフォーマンスの平均と比較するために使用します。 ベースラインを超えた場合でも、問題が発生しているとは限りません。ベースラインは 1 時間ごとに計算され、時刻、曜日および日付が考慮されます。

ポート除外

ポート除外は、監視デバイスでアプリケーション ポート トラフィックをフィルタし、管理コンソール上で使用可能リソースを最大化する一方で、同時に管理コンソール ユーザの注意を当該アプリケーションに集中させます。監視デバイスは、ポート除外に一致する TCP セッションを無視します。

ホップ

ホップとは、ネットワーク内の 2 つのゲートウェイの間の論理的なリンクです。 データ パケットがネットワークをトラバースする場合、通常 1 つ以上のルータまたはゲートウェイを通過します。論理上隣接している 2 つのゲートウェイ間のパスは、「*ホップ*」と考えられます。

マイナーのパフォーマンス評価

マイナーのパフォーマンス評価は、管理コンソールで使用される重大度の状態の 1 つ（黄色）で、メトリックの値がマイナーのしきい値を超えたことを示します。 管理コンソールでは、マイナーおよびメジャーの両方のパフォーマンス低下に対してしきい値を設定します。

未評価のパフォーマンス評価

未評価のパフォーマンス評価は、管理コンソール［操作］ページでグレーの重大度状態によって示され、しきい値を設定するには過去のデータが不十分である（正味 2 営業日分のデータが必要）ことを意味するか、または、観測数が少なかったために、設定された最小の観測しきい値を超える観測がなかったことを意味します。

無応答セッションの割合

*無応答セッションの割合*は、接続要求が送信されたがサーバが応答しなかったセッションの割合を測定するサーバ メトリック (P. 515)です。 このメトリックは、［未対応の TCP/IP セッション リクエスト］ビューに含まれています。

メジャーのパフォーマンス評価

メジャーのパフォーマンス評価は、管理コンソールで使用される重大度の状態の 1 つ（オレンジ）で、メトリックの値がメジャーのしきい値を超えたことを示します。 管理コンソールでは、マイナーおよびメジャーの両方のパフォーマンス低下に対してしきい値を設定します。

メトリック要約ファイル

メトリック要約ファイルには、事前に計算された Cisco NAM からのレスポンス時間メトリックが含まれます。CA ADA マネージャは、Cisco NAM からメトリック要約ファイルを受信します。

役割

*役割*は、CA ADA ユーザに表示される CA ADA 管理コンソールのページを指定します。

レポート ページ

管理コンソールは、標準 *レポート ページ*の下にレポート データを整理し、特定のタイプのユーザ（運用担当者、経営者、エンジニアなど）用にわかりやすく表示します。