IBM Tivoli Monitoring
バージョン 6.3

管理者ガイド

SA88-5151-00
(英文原典：SC22-5446-00)

IBM Tivoli Monitoring
バージョン 6.3

管理者ガイド

SA88-5151-00
(英文原典：SC22-5446-00)

お願い

本書および本書で紹介する製品をご使用になる前に、 667 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM Tivoli Monitoring (製品番号 5724-C04) バージョン 6 リリース 3、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： SC22-5446-00
IBM Tivoli Monitoring
Version 6.3
Administrator's Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2013.4

目次

図 ix

表 xi

本書について xiii

第 1 章 概要 1
本リリースの新機能 1
バージョン 6.3 の新機能 1
IBM Tivoli Monitoring 製品ファミリー. 5
Tivoli Management Services コンポーネント 6
Tivoli Enterprise Portal クライアント 8
デスクトップ、ブラウザー、および Java Web Start クライアント 9
ヒストリカル・データ収集 10
システム管理者タスク 10
Performance Monitoring サービス・プロバイダー . . 11

第 2 章 Tivoli Enterprise Portal 環境の準備 15
ブラウザー・クライアント 15
Java ランタイム環境 (JRE) のバージョン . . . 15
最初のログオン 16
Internet Explorer のセキュリティー設定 16
Windows の書き込みおよび削除特権 17
会社のロゴおよび URL の追加. 17
Tivoli Enterprise Portal クライアントの開始. . . . 18
Web Start を使用した、デスクトップ・クライアントのダウンロードおよび実行 19
IBM JRE のインストール. 20
JRE に対するトレースを使用可能にする. . . . 22
デスクトップ・クライアントのダウンロードおよび実行 22
Web Start クライアントのショートカットを手動で作成する 24
別のポータル・サーバーでのデスクトップ・クライアントの開始. 25
別のポータル・サーバーでのブラウザー・クライアントの開始 26
アプリケーションの起動およびオンライン・ヘルプに使用するブラウザーの指定 27
ナビゲーター・ビューへの作動プラットフォームの追加. 30

第 3 章 ダッシュボード環境の準備 . . . 31
ロードマップ. 31
シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ 31
シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ 37
基本モニター・ダッシュボード環境から、シングル・サインオンおよびユーザーごとの許可による制御を使用するダッシュボード環境への移行 . . 51
IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成 60
モニター・データを表示するカスタム・ダッシュボード・ページの作成 63
UISolutions のインポートの制御 65

第 4 章 環境構成設定の編集 67
Tivoli Enterprise Portal クライアント構成設定 . . . 67
クライアント・パラメーターの編集 67
ポータル・クライアント・パラメーターのリスト 68
HTTP プロキシー・サーバーの使用可能化 . . . 75
Linux および UNIX システムのアプリケーション・プロパティーの設定 76
z/OS システムにハブがある場合の環境変数の設定 78
Tivoli Enterprise Portal Server 構成設定 79
ポータル・サーバー環境ファイルの編集. . . . 79
ポータル・サーバーの環境変数. 80
ポータル・サーバー・データベース上のイベントのプルーニング 82
イベントの添付ファイルのサイズの管理. . . . 83
ログオン試行回数の制御 84
Tivoli Enterprise Monitoring Server 構成設定 . . . 85
モニター・サーバー環境ファイルの編集. . . . 85
シチュエーションの最適化のための duper プロセス 86
Tivoli Enterprise Monitoring Automation Server 構成設定. 88
Tivoli Enterprise Monitoring Automation Server の編集. 88

第 5 章 ユーザー認証の使用可能化 . . . 89
ハブ・モニター・サーバーを使用したユーザー認証 92
ハブ・モニター・サーバー上で認証を構成する場合の前提条件. 92
構成手順 95
LDAP 情報の取得のための Ldapsearch 98
ポータル・サーバーを使用した LDAP ユーザー認証 100
ポータル・サーバー上で LDAP 認証を構成するための前提条件. 101
シングル・サインオンについて 104
ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ 106

Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する 110
Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する 115
TEPS/e 管理コンソールの使用 117
Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング 125
SSO 用ブラウザー・クライアントの再構成 . . 127
LTPA キーのインポートおよびエクスポート . . 128
新規 LDAP ユーザーの管理 130
ポータル・サーバーでの LDAP 認証の無効化 131
モニター・サーバーからポータル・サーバーへの LDAP 認証のマイグレーション 132
Tivoli Enterprise Monitoring Automation Serverを使用した認証 134
Microsoft Active Directory を使用した LDAP ユーザー認証 135
事前処理 136
ロードマップの概要 140
Active Directory 内でのモニター・サーバー・ユーザーおよびポータル・サーバー・ユーザーの計画および作成 141
ポータル・サーバーのユーザー・アカウントとアクセス権の作成および構成 (必要な場合) . . . 142
ポータル・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合) 142
必要な場合の TEPS/e for TLS/SSL の構成. . . 150
モニター・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合) 150
Active Directory の LDAP 検証ツール 152
ユーザー・シナリオ 155

第 6 章 Tivoli Enterprise Portal ユーザー許可の使用 171
ユーザー管理 173
ユーザーおよびユーザー・グループ 173
許可 174
アプリケーション 178
ナビゲーター・ビュー 179
構成メンバーおよびメンバー 180
ユーザー ID の管理 180
ユーザー ID の追加 180
ユーザー ID の表示と編集 182
ユーザー ID の削除 183
デフォルト・ユーザー 184
ユーザー・グループの管理 184
ユーザー・グループのメンバーシップの表示 . . 185
ユーザー・グループの追加 185
ユーザー・グループの検討および編集 186
ユーザー・グループの削除 187
ユーザー管理についての注意事項. 188
ログオン・エラー・メッセージのトラブルシューティング. 192

第 7 章 役割ベースの許可ポリシーの使用 195
許可ポリシーの概念 196
事前定義の役割と権限 199
許可ポリシーを有効にする準備 201
ポリシー管理のシナリオ. 202
許可ポリシーを作成する際のベスト・プラクティス 202
administrator 役割の作成および割り当て . . . 205
ポリシー・ディストリビューターの役割の作成および割り当て 206
ポリシー管理の例 207
ポータル・サーバーでの許可ポリシーの使用可能化 210
許可ポリシーの監査 215
インストールおよび構成後の許可ポリシー・サーバー構成プロパティーの変更 216
許可ポリシー・ストアの管理 218
複数のドメインに関する作業 219
デプロイメント・シナリオ 219
特定の IBM Tivoli Monitoring ドメイン用のポリシーの作成 221

第 8 章 通信の保護 227
ハブ・モニター・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成 230
Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成. 231
サード・パーティーの認証局によって署名された証明書のポータル・サーバーに対する使用. . . 231
Dashboard Application Services Hub サーバー用の TLS/SSL 通信の構成 234
許可ポリシー・サーバーとの TLS/SSL 通信の構成 235
WebSphere で生成された証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成 . . . 236
サード・パーティー証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成 237
TLS/SSL 用の tivcmd CLI 構成 240
ポータル・サーバーおよび許可ポリシー・サーバー間の TLS/SSL 通信の構成 241
IBM Tivoli Monitoring 用に FIPS を使用可能にする 242
ポータル・サーバーの鍵ファイル・データベースへの TEPS/e 証明書のインポート 248
GSKit コマンド行インターフェースによる鍵データベースおよび証明書の操作 249
GSKit iKeyman ユーティリティーによる鍵データベースおよび証明書の操作. 251
GSKit 向けの JRE の設定および Key Manager の起動. 251
新規鍵データベースの作成 252
新規公開鍵と秘密鍵のペアおよび認証要求の作成 253
自己署名証明書の一時的な使用 253
CA 署名証明書の受信 254
パスワードを stash ファイルに保存する . . . 254

第 9 章 監査ロギング 257
ITM 監査属性グループにマップされる監査ログの XML 要素 259
監査ログの XML 例 262
監査の環境変数. 264
アクション実行およびコマンド実行監査ロギング 267

第 10 章 Tivoli Enterprise Console を使用したシチュエーション・イベントの統合 269
シチュエーション・イベントから IBM Tivoli Enterprise Console イベントへのデフォルト・マッピング. 269
汎用イベント・メッセージのシチュエーションの記述の拡張 271
エージェント固有スロットの汎用マッピング . . 272
Tivoli Enterprise Console イベントの重大度の割り当て. 273
メッセージ・スロットのローカライズ 274
シチュエーション・イベント状況および IBM Tivoli Enterprise Console イベントの生成 . . . 274
シチュエーション・イベントの同期化 277
IBM Tivoli Enterprise Console イベント・キャッシュの確認 277
イベント・サーバー上のイベント同期の構成の変更 278
イベント・サーバー上のイベント同期用の追加モニター・サーバーの定義. 279
サンプル・イベントのクローズ 279
omegamon.rls ルール・セット・ファイルのルール・セット・パラメーターの変更 280
チューニング考慮事項 281
ルール検査ユーティリティーの使用 282
Event Integration Facility 構成の編集. 283
シチュエーション・イベントの EIF 転送の指定 287
イベント・メッセージのカスタマイズ 289
MCS 属性サービスによって使用される XML の更新 290
Tivoli Enterprise Console での Universal Agent からのイベントの表示 293
IBM Tivoli Enterprise Console イベント・ビューアーからの NetView コンソールの使用 294

第 11 章 Tivoli Netcool/OMNIbus によるシチュエーション・イベント統合. . 297

第 12 章 共通イベント・コンソール用コネクターの構成 299
「共通イベント・コンソール構成」ウィンドウ . . 299
「ITM コネクター」タブ 300
「TEC コネクター」タブ 301
「OMNIbus コネクター」タブ. 302
「特殊列の名前」タブ 304
イベント同期を使用する際のベスト・プラクティス 305
Linux システムでの Tivoli Enterprise Console サーバーへの接続に関する問題のトラブルシューティング 306

第 13 章 モニター・エージェントの保守 309
Tivoli Enterprise Portal のエージェント・タスク 309
Tivoli Enterprise Portal からのエージェントの追加 309
Tivoli Enterprise Portal からのエージェントの構成 311
Tivoli Enterprise Portalからのエージェント・プロセスの開始、停止、およびリサイクル 312
Tivoli Enterprise Portal からのエージェントの更新 313
Tivoli Enterprise Portal からのエージェントの削除 314
コマンド行インターフェースからのエージェントの更新 315
デプロイメント状況表のクリア 315
エージェントが接続するモニター・サーバーの変更 318
自己記述型モニター・エージェント 319
モニター・サーバーでの自己記述型のイベント・フロー. 324
自己記述型エージェントのインストール . . . 326
自己記述型機能の中断 332
自己記述型の自動最新表示およびシード . . . 333
モニター・サーバーでの自己記述型機能の有効化または無効化 335
エージェントでの自己記述型機能の有効化または無効化. 336
エージェントで自己記述が有効になっているかどうかの判断 337
自己記述型機能を制御する環境変数 339

第 14 章 エージェント管理サービス 343
Tivoli Agent Management Services の機能 343
Tivoli Agent Management Services のインストールおよび構成 345
エージェントの可用性のモニター. 350
エージェントの手動管理. 351

第 15 章 エージェント・オートノミー 353
オートノマス機能 353
オートノマス動作の環境変数 358
シチュエーション制限 365
UTF-8 エンコードされた XML ファイル 369
Tivoli System Monitor Agent でのエージェント管理サービスの構成. 369
専用シチュエーション 371
専用シチュエーション操作 371
専用シチュエーション XML 指定 374
エクスポートされたエンタープライズ・シチュエーション XML 指定 384
専用シチュエーションの例 390
専用ヒストリー. 395

エンタープライズ・シチュエーション・オーバーライド XML 指定 397
SNMP アラート 403
SNMP アラート構成 403
トラップ構成 XML 仕様 405
SNMP アラートおよびエージェント発行のための MIB 415
SNMP 用の OMNIbus 構成. 416
EIF イベント 422
EIF イベント構成 422
EIF イベント・マッピング XML 仕様 425
EIF イベント宛先構成 XML 仕様 431
EIF 発行イベントの共通スロット. 433
EIF ライフサイクル・イベント 435
EIF ハートビート・イベント 436
マスター・リセット・イベント 437
TLS/SSL 通信を使用した専用シチュエーション・イベントの送信 438
エージェント・サービス・インターフェース . . . 442
エージェント・サービス・インターフェースの開始 443
アクセス許可グループ・プロファイル 444
エージェント・サービス・インターフェース - エージェント情報 450
エージェント・サービス・インターフェース - シチュエーション 451
エージェント・サービス・インターフェース - ヒストリー 452
エージェント・サービス・インターフェース - 照会 453
エージェント・サービス・インターフェース - サービス・インターフェース要求. 454

第 16 章 一元化された構成. 473

一元化された構成の概要. 473
一元化された構成設計 474
構成ロード・リスト XML 仕様 478
構成ロード・リストのキーワード置換 486
構成ロード・リストの環境変数 487
ブートストラップ構成ロード・リスト 488
一元化された構成用の環境変数 489
z/OS 上の構成ファイルでパスワードの暗号化を使用可能にする 492
一元化された構成のセットアップ例 494
一元化された構成の開始. 498
エージェント環境変数を使用した一元化された構成の開始 498
ロード・リスト・ファイルを使用した一元化された構成の開始 501
サービス・インターフェース要求を使用した一元化された構成の開始 504
z/OS でのエージェント・オートノミー. 506

第 17 章 ヒストリカル・データの管理 509

ヒストリカル・データ収集について 509
ヒストリカル・データ収集の構成. 512
短期ヒストリー・ファイルのディレクトリーの変更 516
ヒストリカル・データ要求によるパフォーマンスへの影響. 517
モニター・サーバーまたはモニター・エージェントにある大量のヒストリカル・データによる影響 517
大規模なテーブルからのヒストリカル・データの要求 518
ヒストリカル・データのウェアハウジングのスケジューリング 519
データマートを使用した長い照会または複雑な照会の改善 519
Tivoli Data Warehouse および短期ヒストリー構成 522
Tivoli Data Warehouse 範囲区画のマイグレーション 524
非区画化表から区画化表へのマイグレーション (DB2 for Linux, UNIX, and Windows) 526
非区画化表から区画化表へのマイグレーション (DB2 for z/OS) 529
非区画化表から区画化表へのマイグレーション (Oracle) 534
要約とプルーニングの構成 537
Summarization and Pruning agentについて . . . 537
要約およびプルーニングのベスト・プラクティス 540
要約およびプルーニングされたデータの可用性 542
属性グループの要約およびプルーニングの構成 543
グローバル構成設定の変更 544
Summarization and Pruning agentを使用不可にする方法. 548
保管データのエラー・ロギング 548
エージェント・オペレーション・ログ・ヒストリーの収集. 549
区切り文字で区切られたフラット・ファイルを使用するための変換プロセス. 551
ヒストリカル・データ・テーブルを保持するために必要なスペースの見積もり 552
短期ヒストリー・ファイルの拡大の制限 . . . 553
短期ヒストリー・ファイル・ディレクトリーのサイズが制限に達した場合の処置 554
区切り文字で区切られたフラット・ファイルへの短期ヒストリー・ファイルの変換 554
krarloff プログラムを使用したファイルの変換 554
Windows システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換 557
IBM i システムでのヒストリー・ファイルの区切り文字で区切られたフラット・ファイルへの変換 559
UNIX システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換 560
HP NonStop Kernel システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換 562
z/OS システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換 563

第 18 章 Tivoli Common Reporting 569
Tivoli Common Reportingの概要 569
Tivoli Common Reporting の前提条件 570
以前のバージョンからのアップグレード 572
制限 573
ヒストリカル・レポート機能が使用可能であることを確認. 574
ディメンション表の作成および保守 574
ディメンション表を保守するための Summarization and Pruning agentの使用 575
手動によるディメンション表の作成および保守 581
レポート・インストーラーを使用したレポートのインポート 587
IBM Cognos レポートのインポートと実行. . . . 590
前提条件スキャンの実行. 590
ODBC を介するデータベース・クライアントを使用した Tivoli Data Warehouse への接続 . . . 591
Dashboard Application Services Hubを使用したレポートのインポート 592
Dashboard Application Services Hub レポートの作成 594
BIRT レポートのインポートと実行 594
BIRT レポート・パッケージのインポート . . . 594
データ・ソースの構成 596
サンプル BIRT レポートの生成 597

第 19 章 Tivoli Enterprise Portal Server データベースの複製. 601
Tivoli Enterprise Portal Server データベースの理解 601
migrate-export スクリプトの実行 603
migrate-import スクリプトの実行 604
ソース Windows からターゲット Windows への migrate-import の実行. 604
ソース Windows からターゲット Linux またはターゲット UNIX への migrate-import の実行 . 605
ソース Linux またはソース UNIX からターゲット Windows への migrate-import の実行 . . . 606
ソース Linux またはソース UNIX から、ターゲット Linux またはターゲット UNIX への migrate-import の実行. 607

付録 A. SOAP サーバー用の IBM Tivoli Monitoring Web サービス . . . 609
SOAP クライアントについて 609
Tivoli Monitoring Web Services の構成 (SOAP サーバー) 610
ハブの定義 610
ユーザーの追加. 611
UNIX および Linux システムでの IBM Tivoli Monitoring Web Services (SOAP サーバー) の構成 612
AIX システム上での SOAP トランザクションのパフォーマンスを調整 613
SOAP セキュリティーの使用可能化 613
IBM Tivoli Monitoring Web サービスの使用 . . . 614
ユーザー ID. 615
SOAP クライアントの開始と要求の作成 615
ブラウザーの使用方法 615
SOAP クライアント・コマンド行ユーティリティー (kshsoap) の使用 616
システム・コマンドとしての SOAP 要求の発行 617
SOAP メソッド. 618
第 2 レベル SOAP 要求の発行 628
サンプル CT_Get SOAP 要求 630
IBM Tivoli Monitoring Web サービス・シナリオ 631
日計の論理演算の要約と図表の生成 631
データ・スナップショットおよびオフラインのテーブルと図表の取得 631
IBM Tivoli Monitoring プラットフォームへのアラートの送信 633
SA IO を使用したコラボレーション自動化の作成 633
IBM Tivoli Monitoring プラットフォーム内でのイベントの確認通知 634
レポート内容 634

付録 B. IBM Tivoli Monitoring グラフ Web サービスの使用可能化. 637

付録 C. Tivoli Management Services ディスカバリー・ライブラリー・アダプターの使用. 639
OS エージェントの依存関係 641
プライベート・ネットワーク・アドレスのフィルタリング. 642

付録 D. z/OS Tivoli Management Services ディスカバリー・ライブラリー・アダプターの使用 645

付録 E. MIB SNMP エージェントのイベントの説明. 649

付録 F. エージェント・オペレーション・ログ. 655

資料ライブラリー 657
IBM Tivoli Monitoring ライブラリー. 657
基本エージェントの資料. 659
関連資料 659
その他の資料ソース 660

サポート情報. 663

特記事項. 667

索引 671

図

1. Tivoli Monitoring サーバー用の推奨の LDAP ユーザー階層 137
2. ポータル・サーバーのユーザー・プロパティー 138
3. LDAP ユーザー・プロパティー 139
4. Tivoli Enterprise Portal Server ユーザー許可 140
5. デフォルト値の受け入れ 143
6. リポジトリーの構成 144
7. レルムへのベース・エントリーの追加 147
8. TEPS/e 構成の更新の保存 147
9. TEPS/e の構成エラー・メッセージ 148
10. Tivoli Enterprise Portal の「ユーザー管理」画面 149
11. モニター・サーバーのユーザーについての「LDAP」構成パネル 151
12. LDP の照会結果 153
13. Active Directory ユーザーのリスト 156
14. 個々の Tivoli Monitoring ユーザーのプロパティー 157
15. ldapbrowser ウィンドウ 158
16. サーバーの LDAP パラメーターのモニター 159
17. モニター・サーバーのユーザー ID に関する ldapsearch の結果 160
18. Integrated Solutions Console の「構成」ノートブック・タブ 164
19. Integrated Solutions Console の「リポジトリーを管理」画面 164
20. Integrated Solutions Console の「一般プロパティー」画面 165
21. Integrated Solutions Console の確認画面 166
22. Integrated Solutions Console の「構成」ノートブック・タブ 166
23. Integrated Solutions Console の「構成」タブ 167
24. Integrated Solutions Console の「リポジトリー参照」画面 167
25. Integrated Solutions Console の確認画面 168
26. Integrated Solutions Console の「レルム内のリポジトリー」画面 168
27. Integrated Solutions Console の確認画面 168
28. Integrated Solutions Console のサインイン画面 169
29. Integrated Solutions Console の最初の画面 169
30. エージェント管理サービス・コンポーネントと IBM Tivoli Monitoring コンポーネントの対話 344
31. データ・スナップショットの図表およびテーブル 632
32. データ・スナップショットのテーブル 632
33. 受信したメッセージを示す Universal Message コンソール 633
34. メッセージ・ログ詳細 634
35. グラフ Web サービスの製品相互接続 638

表

1. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ. 33
2. シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップに必要な追加タスク 35
3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ . . . 40
4. シングル・サインオンおよびユーザーごとの許可による制御を使用する拡張モニター環境のセットアップに必要な追加タスク 48
5. 高度なダッシュボード環境に移行するためのロードマップ. 52
6. 言語とロケール・コード 74
7. UNIX および Linux システムでアプリケーション・プロパティーを変更するためのファイルの場所 76
8. ユーザー認証のためのロードマップ 92
9. 認証を構成する前に実行するタスク 93
10. LDAP 構成パラメーター 94
11. ハブと LDAP サーバー間の通信用の TLS/SSL パラメーター 95
12. ldapsearch コマンド行オプション、および対応するモニター・サーバーの構成パラメーター . 98
13. LDAP 構成パラメーター. 102
14. SSO パラメーター. 104
15. ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ 107
16. 許可ポリシーのリソース・タイプと、サポートされている許可および要素 197
17. RoleAdministrator の権限. 199
18. PolicyDistributor の権限 200
19. LinuxOperator、UNIXOperator、および WindowsOperator の権限 200
20. VCenterOperator の権限 200
21. 許可ポリシー・サーバーの構成情報 212
22. 共有の役割およびポリシーを使用する複数のドメインでのデプロイメント要件. 220
23. 通信を保護するためのタスク 229
24. ロードマップ: ダッシュボード・データ・プロバイダーの TLS/SSL セットアップ 231
25. ロードマップ: 許可ポリシー・サーバーの TLS/SSL セットアップ 236
26. IBM Tivoli Enterprise Console イベント・クラス属性. 270
27. 転送されたシチュエーション・イベントから生成された IBM Tivoli Enterprise Console イベントでの属性グループおよび属性名の特殊文字 273
28. シチュエーション名のサフィックスから Tivoli Enterprise Console イベント重大度へのマッピング 273
29. エンタープライズ・エージェントの接続時または切断時、あるいはシチュエーションが専用の場合のシチュエーション式関数の可用性 . 365
30. TrapDest 要素の XML 仕様. 406
31. TrapAttrGroup 要素の XML 仕様 409
32. シチュエーション要素 XML 仕様. 410
33. エージェントのライフサイクル・ステータス・トラップ 412
34. StatTrap 要素の XML 仕様 413
35. 発行された EIF イベントの共通スロット・セット 433
36. EIF ライフサイクル・イベント 436
37. EIF ライフサイクル・イベント ITM_StatEvent クラスのスロット値 436
38. マスター・リセット・イベントの内容 437
39. サービス・インターフェース・コマンドのためのアクセス許可グループの権限. 445
40. エージェント・サービス・インターフェース - サンプル属性の照会リスト 454
41. エージェント・サービス・インターフェース - 照会サンプル・レポート. 454
42. エージェント・サービス・インターフェースの <AGENTINFO> 要求 455
43. エージェント・サービス・インターフェースの <AGENTINFO> 要求の出力. 455
44. エージェント・サービス・インターフェースの <LISTSUBNODE> 要求 456
45. エージェント・サービス・インターフェースの <LISTSUBNODE> 要求の出力 456
46. エージェント・サービス・インターフェースの <ATTRLIST> 要求. 457
47. エージェント・サービス・インターフェースの <ATTRLIST> 要求の出力 457
48. エージェント・サービス・インターフェースの <READATTR> 要求 458
49. エージェント・サービス・インターフェースの <READATTR> 要求の出力 458
50. エージェント・サービス・インターフェースの <REPORT> 要求 460
51. エージェント・サービス・インターフェースの <REPORT> 要求の出力 461
52. エージェント・サービス・インターフェースの <TABLESIT> 要求. 464
53. エージェント・サービス・インターフェースの <TABLESIT> 要求の出力 464
54. エージェント・サービス・インターフェースの <PVTCONTROL> 要求 465

55. エージェント・サービス・インターフェースの <PVTCONTROL> 要求の出力 465
56. エージェント・サービス・インターフェースの <SITSUMMARY> 要求 466
57. エージェント・サービス・インターフェースの <SITSUMMARY> 要求の出力 466
58. エージェント・サービス・インターフェースの <AGENTSTAT> 要求 467
59. エージェント・サービス・インターフェースの <AGENTSTAT> 要求の出力 467
60. エージェント・サービス・インターフェースの <HISTREAD> 要求 469
61. エージェント・サービス・インターフェースの <HISTREAD> 要求の出力 470
62. 構成ロード・リストの <ConfigFile> 要素および Disp タイプで使用可能な Activate オプション。 485
63. 要約関数 539
64. krarloff ロールオフ・プログラムのパラメーター 556
65. 必要な DD 名 565
66. KPDXTRA パラメーター. 565
67. 「ハブの指定」ダイアログの TCP/IP フィールド 611
68. 「ハブの指定」ダイアログの SNA フィールド 611
69. agentStatusEvent の SNMP トラップ変数 649
70. agentSitSampledEvent の SNMP トラップ変数 650
71. agentSitPureEvent の SNMP トラップ変数 653

本書について

「*IBM®Tivoli® Monitoring 管理者ガイド*」では、IBM Tivoli Monitoring インフラストラクチャーである Tivoli Management Services の管理について説明します。

章のトピックには、次のタスクが含まれています。

- Tivoli Enterprise Portal クライアントおよびサーバーの構成、カスタマイズ、および保守
- 公開鍵ファイルと秘密鍵ファイルを使用した非対称暗号化のセットアップ
- ハブ・モニター・サーバー・システム・レジストリーまたは外部の LDAP レジストリーでのユーザー認証の使用可能化
- Tivoli Enterprise Portal でのユーザー ID とユーザー・グループの保守
- IBM Tivoli Enterprise Console® イベント・サーバーまたは Netcool/OMNIbus Probe for Tivoli EIF とハブ・もにtz-・サーバー間でのシチュエーション・イベント・アクティビティーの統合
- Tivoli Enterprise Portal にイベント情報を送信するイベント・システム用のコネクターの構成
- Tivoli Enterprise Portal を使用した、リモート・エージェント・デプロイメント機能をサポートするエージェントの保守
- オートノマス操作用の Tivoli Enterprise Monitoring Agent の構成
- 一元化された構成のセットアップと使用可能化
- ヒストリカル・データ収集および Tivoli Data Warehouse の管理
- Tivoli Enterprise Portal 上で実行され、レポート生成のためのヒストリカル・データのソースとして Tivoli Data Warehouse を使用する、製品に固有の Tivoli Common Reporting のレポートのインポート。この情報は、Tivoli Common Reporting をセットアップし、レポート・パッケージをインストールする管理者を対象としています
- 別のコンピューターへの Tivoli Enterprise Portal Server データベースの複製、またはバックアップとしての保持
- IBM Tivoli Monitoring Web Services SOAP メソッドを使用した、モニター対象環境の照会および制御

本書の読者は、パフォーマンス・モニターの概念および管理を理解している必要があります。Tivoli Data Warehouse を使用する場合は、ウェアハウスをホストするオペレーティング・システムに精通している必要があります。この製品ファミリーについて詳しくは、Tivoli solutions for Service Availability and Performance Managementを参照してください。

第 1 章 概要

本章では、Tivoli Enterprise Portal インターフェースおよび Tivoli Management Services の管理機能に対する新機能および機能拡張について説明した後で、実行が予想される管理用タスクのリストを示します。

バージョン 6.3 Tivoli Enterprise Portal の機能の使用方法について詳しくは、組み込みヘルプ (「ヘルプ」→「目次および索引」) または「*Tivoli Enterprise Portal* ユーザーズ・ガイド」を参照してください。

本リリースの新機能

「*IBM Tivoli Monitoring 管理者ガイド*」に関連した、Tivoli Enterprise Portal および Tivoli Management Services コンポーネントに対する最新の拡張機能について説明します。

バージョン 6.3 の新機能

バージョン 6.3 でシステム管理者に関係する Tivoli Management Services コンポーネントの機能拡張を以下に示します。

Jazz™ for Service Management

Jazz for Service Management は、データ、共有管理サービス、ダッシュボード、およびレポート・サービスをリンクするための Open Services for Lifecycle Collaboration (OSLC) コミュニティーのオープン仕様を 1 つにまとめます。Jazz for Service Management は、これらのファセットによって、IBM、パートナー、およびサード・パーティーのツール間でデプロイメント、統合、およびワークフローの自動化を加速します。IBM Tivoli Monitoring には、Jazz for Service Management が含まれています。

Jazz for Service Management には複数の統合サービスがあります (Administration、Registry、IBM Tivoli Common Reporting、Security、および IBM Dashboard Application Services Hub)。これらの統合サービスは、以下をはじめとする重要な機能を提供します。

- Jazz for Service Management によって統合される製品のための共有データ・リポジトリー。
- Jazz for Service Management の Dashboard Application Services Hub による一貫した UI 操作。
- Jazz for Service Management によって統合される製品およびソリューションの管理を簡素化。
- Jazz for Service Management の Tivoli Common Reporting によるセルフサービスの随時レポート作成機能。

Jazz for Service Management について詳しくは、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)を参照してください。

IBM Dashboard Application Services Hub ダッシュボードに表示するモニター・データを取得するための IBM Tivoli Monitoring ダッシュボード・データ・プロバイダー

IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーは、Jazz for Service Management の IBM Dashboard Application Services Hub コンポーネントに表示するモニター・エージェント・データを取得します。ダッシュボード・データ・プロバイダーは、Tivoli Enterprise Portal Server の構成時にオプションでインストールされます。ダッシュボード・データ・プロバイダーが有効になっている場合、Dashboard Application Services Hub ユーザーはハブ・モニター・サーバーとモニター・エージェントから読み取り専用データを取得し、エージェントのダッシュボードまたはカスタム・ダッシュボードにそのデータを表示できます。IBM Tivoli Monitoring V6.3 には、OS エージェントのデータを表示する Infrastructure Management Dashboards for Servers が含まれています。これらのサーバー・ダッシュボードはダッシュボード・データ・プロバイダーを使用してデータを取得します。Dashboard Application Services Hub で ダッシュボード・データ・プロバイダーへの接続が構成されている必要があります。 31 ページの『第 3 章 ダッシュボード環境の準備』および 60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』を参照してください。

Dashboard Application Services Hub V3.1 以降で実行される IBM Infrastructure Management Dashboards for Servers

IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーが有効になった状態で、Dashboard Application Services Hub ユーザーは、Infrastructure Management Dashboards for Servers アプリケーションを使用して、すべてのモニター・エージェントの管理対象システム・グループおよびイベントと、LinuxOS エージェント、UNIX OS エージェント、および Windows OS エージェントの正常性メトリックを取得できます。このアプリケーションは、Dashboard Application Services Hub V3.1 以降で IBM Installation Manager を使用してインストールおよび構成されます。詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『IBM Infrastructure Management Dashboards for Servers のインストールおよび構成』を参照してください。

Open Services Lifecycle Collaboration Performance Monitoring サービス・プロバイダー

Tivoli Enterprise Monitoring Automation Server コンポーネントには Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) サービス・プロバイダーが含まれています。また、このコンポーネントはハブ Tivoli Enterprise Monitoring Server と同じシステムにインストールされます。サービス・プロバイダーは、Jazz for Service Management Registry Services コンポーネントにモニター・リソースを登録し、OSLC リンク・データ・インターフェースを使用してその他の製品との統合をサポートします。詳しくは、 11 ページの『Performance Monitoring サービス・プロバイダー』を参照してください。

役割ベースの許可ポリシー

Tivoli 許可ポリシー・サーバー機能により、既存の Tivoli Enterprise Portal Server 許可モデルよりもアクセス制御機能が強化されます。IBM Dashboard Application Services Hub でモニター・ダッシュボードのユーザーによる無

許可アクセスからリソースを保護できます。許可ポリシー・サーバー 機能が有効に設定された IBM Tivoli Monitoring V6.3 では、以下の機能を使用できます。

- ダッシュボード・ユーザーに対して、特定の管理対象システム・グループおよび個別の管理対象システムへのアクセスを制限する機能。
- ポリシー管理を簡素化するために、統合 LDAP ユーザー・レジストリー内のユーザーおよびユーザー・グループに役割ベースのポリシーを割り当てる機能。
- 高度な自動化が可能な新しいコマンド行インターフェース。
- ドメインとも呼ばれる IBM Tivoli Monitoring 環境が複数ある場合向けの、許可ポリシーの集中管理。

この機能を実装するには、Tivoli 許可ポリシー・サーバーおよび許可ポリシーの tivcmd コマンド行インターフェース向けの IBM Installation Manager パッケージをインストールする必要があります。許可ポリシー・サーバーが Dashboard Application Services Hub と共にインストールされ、許可ポリシーを作成する管理者が使用するコンピューターに tivcmd CLI がインストールされます。この 2 つのパッケージのインストールが正常に完了したら、必要に応じて各種 CLI コマンドを使用して、役割の作成、権限の付与、権限の除外などを行うことができます。ポリシーの処理については、195 ページの『第 7 章 役割ベースの許可ポリシーの使用』を参照してください。

「OS Agents Reports 前提条件スキャナー」レポート

「OS Agents Reports 前提条件スキャナー」レポートは、OS エージェント・レポート・パッケージにより配布およびインストールされます。このレポートを使用して、システムの IBM Tivoli Monitoring の前提条件がエラーなしで Tivoli Common Reporting を使用するように正しく構成されていることを確認することができます。590 ページの『前提条件スキャンの実行』を参照してください。

Summarization and Pruning agentを使用した Tivoli Common Reporting に必要なディメンション表の作成および保守

IBM_TRAM スキーマを保守し、MANAGEDSYSTEM 表にデータを取り込むために Tivoli Common Reporting および OS エージェント・スクリプトを定期的に実行する必要がなくなりました。ディメンション表の作成、データ取り込み、および保守を行うようにSummarization and Pruning agentを構成できます。574 ページの『ディメンション表の作成および保守』を参照してください。

Tivoli Data Warehouse の範囲区画化

範囲区画化とは、大規模な Tivoli Data Warehouse データベースでプルーニングと照会のパフォーマンスを大幅に向上できるデータベース・データ編成機能です。既存の表を区画化表にマイグレーションすることで、区画化表の向上したパフォーマンスを活用することができます。範囲区画化により、データベースで区画化キーを構成する列を WHERE 節で使用すると、照会範囲を制限できます。524 ページの『Tivoli Data Warehouse 範囲区画のマイグレーション』を参照してください。

アクション実行 ID の監査

システム上で実行されたすべてのコマンドをエージェント・レベルで監査で

きます。発信元のユーザー ID とネットワーク情報がエージェントに安全に転送され、エージェントの監査ログに記録されます。監査ログはヒストリカル収集が可能です。シチュエーションを作成し、Tivoli Enterprise Portal から集中的にモニターできます。 267 ページの『アクション実行およびコマンド実行監査ロギング』を参照してください。

AAGP 許可の制御

アクセス許可グループ・プロファイル (AAGP) 許可フレームワークは、アクション実行 ID の監査と統合されています。AAGP ポリシーでは、特定のユーザーが、Tivoli Enterprise Portal から、または **tacmd executeaction** を使用してアクション実行を実行すること、**tacmd executecommand** を使用してコマンドを実行すること、またはアクション実行コマンドを指定するシチュエーションおよびワークフロー・ポリシーを作成および変更することを選択的に許可できます。AAGP ポリシーでは、AAGP ポリシーを配信するために中央構成サーバーが必要でなくなりました。ポリシーは、エージェント・サービス・インターフェースから構成し、エージェント自体にローカルに格納できます。 444 ページの『アクセス許可グループ・プロファイル』および 473 ページの『第 16 章 一元化された構成』を参照してください。

SOAP セキュリティー機能拡張

モニター・サーバーで SOAP_IS_SECURE 環境変数を使用して CT_EMail 要求と CT_Export 要求のセキュリティーを有効にできるようになりました 613 ページの『SOAP セキュリティーの使用可能化』を参照してください。

duper プロセスの最適化

duper プロセスで、リフレックス・アクションまたは表示項目が含まれているシチュエーションがサポートされています。 86 ページの『シチュエーションの最適化のための duper プロセス』を参照してください。

自己記述型エージェントのデフォルトの動作の変更と新しい tacmd コマンド

自動自己記述型エージェント・プロセスにより、モニター・サーバーとポータル・サーバーにインストールされる製品とバージョンを指定できます。 319 ページの『自己記述型モニター・エージェント』および 331 ページの『自己記述型機能によるインストールのオプションの動的更新』を参照してください。

専用シチュエーションの更新

- *REGEX 述部関数

  IBM Tivoli Monitoring では、イベントとサンプル・データ (名前、アドレス、メッセージ、およびログ・レコードなど) におけるテキスト・スキャンとパターン・マッチングが必要なことがよくあります。正規表現述部フィルターを専用シチュエーションに追加して、エージェント・モニター・イベント検出を強化できます。

- 専用シチュエーションの動的な削除

  専用シチュエーションで DELETE= 属性を使用して、エージェントのリサイクルやローカル専用シチュエーション XML ファイルの削除を行わずに、専用シチュエーションを動的に削除できます。

詳しくは、 374 ページの『専用シチュエーション XML 指定』を参照してください。

デプロイメント状況表トランザクションのクリア機能

IBM Tivoli Monitoring **tacmd** コマンドを実行するか、または Tivoli Enterprise Portal ナビゲーターを使用して Tivoli Enterprise Monitoring Agent をリモートで管理するたびに、トランザクションに関する情報が Tivoli Enterprise Monitoring Server デプロイメント状況表に保持されます。特に大規模環境でのこの表の内容の管理を容易にするため、完了したトランザクションをこの表から定期的に削除する操作をスケジュールできます。 315 ページの『デプロイメント状況表のクリア』を参照してください。

IBM Service Management Connect で入手可能なログイン・デーモン・スクリプトの使用 IBM Tivoli Monitoring V6.3 以降のモニター・サーバーでは、IBM Service Management Connect で入手できる IBM Tivoli Monitoring ログイン・デーモン・ソリューションを使用して、エージェントが接続するモニター・サーバーを変更できます。 318 ページの『エージェントが接続するモニター・サーバーの変更』を参照してください。

ブラウザー・クライアントのロケールの設定

管理者が Tivoli Enterprise Portal ブラウザー・クライアントのロケールをエンタープライズ全体で設定できなくなりました。基になる OS プラットフォームが Tivoli Enterprise Portal で使用するロケールと異なるロケールを使用してインストールされている場合、言語の変更はクライアント・コンピューターの Java™ 制御パネルを使用して行うことができます。 68 ページの『ポータル・クライアント・パラメーターのリスト』の **user.language** パラメーターおよび **user.region** パラメーターを参照してください。

Tivoli Integrated Portal の名称の変更

Tivoli Integrated Portal V3.1 リリースは Dashboard Application Services Hub という名称に変更されました。

i5/OS™ エージェントの名称の変更

i5/OS モニター・エージェントは IBM i モニター・エージェントという名称に変更されました。

IBM Tivoli Monitoring 製品ファミリー

以下では、IBM Tivoli Monitoring 製品ファミリーの各アプリケーションの概要を説明します。

IBM Tivoli Monitoring 製品は、分散されているオペレーティング・システムおよびアプリケーションのパフォーマンスおよび可用性を管理する際に役に立ちます。これらの製品は、総称して Tivoli Management Services と呼ばれる一連の共通サービス・コンポーネントをベースにしています。 Tivoli Management Services は、セキュリティー、データの転送と保管、通知メカニズム、ユーザー・インターフェースの表示、および通信サービスを、エージェント/サーバー/クライアント型のアーキテクチャーで提供します。これらのサービスは、IBM Tivoli OMEGAMON XE メインフレーム・モニターおよび IBM Tivoli Composite Application Manager など、多くの製品スイートに共通するものです。

Tivoli Management Services およびそれらに依存する製品のインストールおよび初期構成の完了後、分散環境をさらに細かくカスタマイズするには、本書を参照してください。 (*Tivoli Enterprise Monitoring Server on z/OS* の構成については、同名の資

料で説明します。)本書には、これらの共通サービスを共有する管理対象システムの一般管理情報も記載されています。製品固有の管理情報については、個々の製品のガイドを参照してください。

Tivoli Management Services コンポーネント

以下の Tivoli Management Services のコンポーネントは、ご使用の Tivoli Enterprise Monitoring Agent に対するインフラストラクチャーを提供します。

コンポーネントの完全なリストについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)」を参照してください。

クライアント

IBM Tivoli Monitoring クライアント、Tivoli Enterprise Portal は、エンタープライズ・ネットワークの表示およびモニターを行うための Java ベースのユーザー・インターフェースです。Tivoli Enterprise Portal は、インストール方法に応じて、デスクトップ・アプリケーションとして開始するか、Web アプリケーションとしてブラウザーを介して開始することができます。

表示サーバー

Tivoli Enterprise Portal クライアントは、Tivoli Enterprise Portal Server に接続します。 Tivoli Enterprise Portal Server は、クライアント用のソフトウェア・サービスの集合で、エンタープライズのモニター・エージェントからのデータの検索、操作、および分析を可能にします。

Tivoli Enterprise Portal Server には、オプションのダッシュボード・データ・プロバイダーも含まれています。これは、モニター・ダッシュボードに表示する読み取り専用のモニター・データを取得するために使用されます。

管理サーバー

Tivoli Enterprise Portal Server は、メインまたはハブ の Tivoli Enterprise Monitoring Server に接続します。モニター・サーバーは、エンタープライズ・モニター・エージェントから送られるアラートを収集および制御し、そこからパフォーマンスおよび可用性のデータを収集します。ハブ・モニター・サーバーは、モニター・エージェントが収集したモニター・データと任意のリモート・モニター・サーバーを相互に関連付け、それをポータル・サーバーに受け渡してポータル・コンソールに表示できるようにします。

オートメーション・サーバーである Tivoli Enterprise Monitoring Automation Server は、ハブ・モニター・サーバーと同じシステムにインストールすることができるオプションのコンポーネントです。このコンポーネントは、ハブ・モニター・サーバーの機能を拡張します。オートメーション・サーバーには Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) サービス・プロバイダーが含まれています。詳しくは、 11 ページの『Performance Monitoring サービス・プロバイダー』を参照してください。

ダッシュボード・サーバー

IBM Dashboard Application Services Hub は、ダッシュボードの可視化とレポート作成サービスを実現する Jazz for Service Management のコンポーネ

ントです。ダッシュボードのオペレーターは、Web ブラウザー・インターフェースからこれにアクセスします。IBM Dashboard Application Services Hub は、ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントを使用してモニター・データを取得します。

IBM Infrastructure Management Dashboards for Servers アプリケーションを Dashboard Application Services Hub にインストールして、Windows OS エージェント、 Linux OS エージェント、および UNIX OS エージェントのシチュエーション・イベント情報、管理対象システム・グループ、および主要な正常性メトリックを表示できます。また、モニター・データを表示するカスタムのダッシュボード・ページを作成することもできます。

許可ポリシー・サーバーおよび**許可ポリシーの tivcmd コマンド行インターフェース (tivcmd CLI)** をインストールして、役割ベースの許可ポリシーを使用することにより、モニター対象のうちどのリソースをダッシュボードに表示するかを制御することもできます。詳しくは、 195 ページの『第 7 章 役割ベースの許可ポリシーの使用』を参照してください。

ヘルプ・サーバー

IBM User Interface Help System Built on Eclipse は、ポータル・サーバーとともにインストールされ、組み込みヘルプ・システムの表示および検索の機能を提供します。

tacmd コマンド行インターフェース (tacmd CLI)

tacmd CLI は、モニタリング環境を管理するために使用され、また、 Tivoli Enterprise Portal を使用して実行される管理機能の多くを自動化するためにも使用できます。CLI コマンドは、ハブ・モニター・サーバーまたはポータル・サーバーに要求を送信します。

エージェント

Tivoli Enterprise Monitoring Agent は、モニター対象となるアプリケーションおよびリソースがあるシステムまたはサブシステムにインストールされます。エージェントは、*管理対象システム* からモニター・データを収集し、それを接続先のモニター・サーバーに渡します。ポータル・クライアントとダッシュボード・サーバーは属性の現行値を収集し、テーブル形式、グラフ形式、およびリレーショナル・テーブル・ベースのトポロジー・ビュー形式のレポートを生成します。エージェントおよびモニター・サーバーは、現在の属性の値をしきい値に対してテストすることもできます。しきい値を超えるか値が一致した場合は、アラート・アイコンをポータル・クライアントまたはモニター・ダッシュボードに表示でき、ハブ・モニター・サーバーはイベントを IBM Tivoli Netcool/OMNIbus などのイベント・サーバーに転送できます。属性値がテストされる条件は、*シチュエーション* と呼ばれます。

OS エージェントは、エンタープライズの外部に *Tivoli System Monitor Agent* としてインストールできます。このエージェントは、Tivoli Enterprise Monitoring Server に接続せず、依存することもありません。このエージェントは、モニター・サーバーに依存しない*専用シチュエーション* を実行可能であり、属性グループのデータ・サンプルを*専用ヒストリー* として保存し、IBM Tivoli Netcool/OMNIbus に SNMP アラートまたは EIF イベントを送信できます。

データウェアハウス

Tivoli Data Warehouse は、ご使用の環境内のエージェントから収集された

ヒストリカル・データを保管するためのオプション・コンポーネントです。データウェアハウスは、サポートされるデータベース (DB2®、Oracle、Microsoft® SQL など) 上に配置されます。

共有ユーザー・レジストリー

共有ユーザー・レジストリーは、ポータル・サーバー・ユーザー、 IBM Dashboard Application Services Hub ユーザー、および Netcool/OMNIbus Web GUI ユーザーのようなその他のアプリケーション・ユーザーを認証するために使用できる、 Tivoli Directory Server や Microsoft Active Directory などの LDAP サーバーです。 共有ユーザー・レジストリーが使用されている場合、ユーザーはアクセスした最初のサーバーによって認証され、ユーザーが資格情報を再度入力しなくて済むように、認証トークンが他のサーバーに渡されます。

イベントの同期

イベントの同期コンポーネントはオプションです。これは、IBM Tivoli Enterprise Console Event Server または Netcool/OMNIbus ObjectServer に転送されたシチュエーション・イベントの更新を、モニター・サーバーに送信し直すように構成されます。

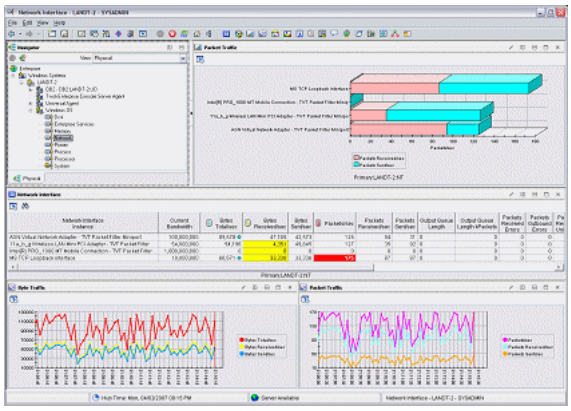
Tivoli Enterprise Portal クライアント

Tivoli Enterprise Portal は、 IBM Tivoli Monitoring ベース製品向けのユーザー・インターフェースの 1 つです。インターネット上でのナビゲーションの開始点としてブラウザーのホーム・ページを使用するのと同じ方法で、Tivoli Enterprise Portal を使用してネットワーク環境の概要を表示します。

ウィンドウの 1 つのセクションはナビゲーターです。このビューには、モニター・エージェントが収集したモニター対象ネットワークについての情報が、最上位レベルから個別のグループ・レベルまでのツリー形式で表示されます。ウィンドウの残りの部分には、ナビゲーター・ツリー内で選択された項目に関連するビューが表示されます。最上位レベルまたは自分のホーム・ワークスペースから特定のロケーションにナビゲートして、アクティビティーを検査し、問題を調査できます。

このワークスペースは、ツリー内の選択項目に合わせてカスタマイズされています。このワークスペースは、1 つの棒グラフ、2 つのプロット・グラフ、および一定のしきい値を超えたセル値に対して背景色を表示するテーブルが表示される設計になっています。ツリー内のすべての項目に対して、追加のワークスペースを作成したり、ワークスペースをカスタマイズしたりできます。

ツリー (ナビゲーター) 内に表示されるイベント・インディケーターには、モニター対象システム上で実行されるシチュエーションと呼ばれるテストの結果が反映されます。シチュエーション内に記述された条件が true である場合は、ツリー内の影響を受ける項目に、色付きのアイコンがオーバーレイされます。環境を自動的にモニターする条件付きアラートをセットアップするには、シチュエーション・エディターを使用します。環境を自動化するためのポリシーをセットアップするには、ワークフロー・エディターを使用します。



デスクトップ、ブラウザー、および Java Web Start クライアント

Tivoli Enterprise Portal クライアントは、3 通りの方法でデプロイすることができます。ここではそれらの方法について簡単に説明します。詳しい説明については、「*インストールおよび設定ガイド*」を参照してください。

デスクトップ

デスクトップ・クライアントの場合、そのデスクトップ・クライアントが実行されるそれぞれのコンピューター上で、インストール用ソフトウェアをロードして実行する必要があります。 Tivoli Enterprise Portal の開始方法は、ローカルにインストールされた他のアプリケーションの開始方法と同じです。デスクトップ・クライアントでは、異なるポータル・サーバーに接続する複数のインスタンスを作成することもできます。

ブラウザー

ブラウザー・クライアントのインストール用ソフトウェアは、Tivoli Enterprise Portal Server 上にあります。このクライアント・ソフトウェアは、ブラウザーからポータル・サーバーへの初回ログオン時に、そこからご使用のコンピューター上にダウンロードされ、それ以後は、ソフトウェアの更新があった場合にのみダウンロードされます。

ブラウザー・クライアントは、ブラウザーを使用可能な任意のコンピューターから、ポータル・サーバーの URL を入力することによって開始することができます。この操作モードでは、各ポータル・ワークスペースに URL があるため、ワークスペースを「お気に入り」リストに保存することができます。

ブラウザー・クライアントでは、Tivoli Enterprise Portal から他の Tivoli Web ベース・アプリケーションおよび Web 対応アプリケーションを起動できます。これらのアプリケーションから、ログオン資格情報を再入力しなくてもポータルを起動できます。シングル・サインオン・ソリューションでは、中央 LDAP ベースのユーザー・レジストリーを使用して、サインオン資格情報を認証します。

Java Web Start

Java Web Start の場合もブラウザー・クライアントの場合のように、クライアント・ソフトウェアは、URL を介してアクセスでき、ポータル・サーバーからダウンロードされます。常にブラウザーの内部で実行されるブラウザ

ー・クライアントと異なり、Web Start クライアントは、デスクトップ・アプリケーションとして実行されます。クライアント・ソフトウェアの更新が入手可能になると、常にポータル・サーバーから自動的にダウンロードされます。本書でデスクトップ・クライアント の動作について言及する場合、特に明記されていない限り、それは Java Web Start クライアントにも適用されます。シングル・サインオンはその一例であり、Web Start クライアントでも、ブラウザー・クライアントと同様にシングル・サインオンを使用できます。

ヒストリカル・データ収集

Tivoli Enterprise Portal ワークスペースが提供するリアルタイム・レポートのほか、ヒストリカル・レポートおよびシチュエーション用にモニター・エージェントが収集するデータを保管するヒストリカル・データ収集の構成を行うことができます。指定できる項目は以下のとおりです。

- ヒストリカル・データ収集の属性グループ
- データ収集間隔
- Tivoli Data Warehouse にデータを書き込む場合のデータウェアハウジング間隔
- Tivoli Data Warehouse からのプルーニングに関するデータ・サンプルのグループ化方法
- ウェアハウスに保管されたデータのプルーニング・スケジュール
- データウェアハウスに送信するまで短期ヒストリー・ファイルを保管しておく場所。データ・サンプルは、モニター・エージェントまたは Tivoli Enterprise Monitoring Server に保管することができます。

データ・サンプリングの結果を保存し、定義済みヒストリカル・ワークスペースに取り込むには、まず、ヒストリカル・データ収集を構成および開始する必要があります。リアルタイム・ワークスペースは、ヒストリカルな収集を開始した場合でも開始していない場合でも使用可能です。

システム管理者タスク

システム管理者は、最高レベルの権限を持っており、Tivoli Enterprise Portal 内で IBM Tivoli Monitoring のすべての機能にアクセスできます。

以下に、システム管理者が実行する可能性のあるタスクのタイプをリストします。

- 自身のジョブに対して適切な権限を持つ Tivoli Enterprise Portal ユーザー ID およびユーザー・グループの設定
- ナビゲーター項目用のワークスペースの設計、および設定された権限に基づく、ユーザーへのワークスペースの使用可能化
- 表ビューおよびグラフ・ビューに適用可能な照会の定義による、モニター・サーバーから検索する属性および属性値の範囲の指定
- アプリケーションを起動するための定義の作成、および設定された権限に基づく、ユーザーへの定義の使用可能化
- ポータル・クライアントから指定の管理対象システムで実行可能なコマンド行アクションの作成、および権限を付与されたユーザーへのアクションの使用可能化
- ビジュアル・プログラミング機能を使用したシチュエーションの作成

- 特定のナビゲーター項目のシチュエーションの重大度の設定、およびシチュエーションが true で、イベントが開始された場合に再生する音 (指定する場合) の設定
- 各シチュエーションが適用される管理対象システムの決定 (配布と呼ばれるプロセス)
- 特定のシチュエーションが true と評価された場合に表示する、エキスパートによる推奨事項の提供
- シチュエーションが true と評価された場合に実行するアクションであるポリシー・ワークフローの作成
- 中央の場所からのリモート・ホスト上のエージェントの作成、インストール、アップグレード、配布、および構成
- エージェント・プロセスの開始、停止、およびリサイクル

Performance Monitoring サービス・プロバイダー

Tivoli Enterprise Monitoring Automation Server コンポーネントには Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) サービス・プロバイダーが含まれています。また、このコンポーネントはハブ Tivoli Enterprise Monitoring Server と同じシステムにインストールされます。

Performance Monitoring サービス・プロバイダーは、モニター・リソースを Registry Services に登録します。Registry Servicesは、統合サービス管理環境で製品用の共有データ・リポジトリーを提供する Jazz for Service Management 統合サービスです。共有 IT リソースをディスカバーおよび管理する製品は、それらの IT リソースと提供するサービスをRegistry Servicesに登録できます。他の製品は、Registry Services に対して管理対象リソースまたは関連する必要なサービス・プロバイダーを照会することで、データを取り込むことができます。

Performance Monitoring サービス・プロバイダーは、コンピューター・システム、ソフトウェア・サーバー、ソフトウェア・モジュール、データベース、IP アドレス、サーバー・アクセス・ポイントなどのリソース・タイプをモニター・エージェントのために登録します。これらのリソース・タイプは、Common Resource Type Vocabulary (CRTV) を使用して定義されています。エージェントには、そのモニター・データを CRTV リソースにマップするテンプレートが用意されています。このテンプレートは、エージェントのモニター・サーバー・アプリケーション・サポートと共にインストールされています。

Performance Monitoring サービス・プロバイダーでは、モニター対象リソースに関するリンク・データの取得に OSLC-PM RESTful API も使用できます。 HTTP GET 要求で、RDF/XML、コンパクト XML および HTML コンテンツ・タイプを使用できます。RDF/XML コンテンツと HTML コンテンツが要求されると、API は OSLC-PM ドメインおよび IBM Tivoli Monitoring プライベート名前空間によって定義されているリソース正常性メトリックを返します。

Performance Monitoring サービス・プロバイダーは OSLC 照会機能を備えていないため、 Performance Monitoring サービス・プロバイダーから正常性メトリックを入手できるリソースを見つけるには、 Registry Servicesに照会を行う必要があります。Registry Servicesは、サービス・プロバイダー・レコード、リソース登録レコード、

および調整済みリソース・レコードを取得するための照会インターフェースを備えています。調整済みリソース・レコードおよび登録レコードに含まれている HTTP URL を使用することにより、リソースを登録したサービス・プロバイダーからリソースに関する情報を取得できます。 Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) の「*Jazz for Service Management Integration Guide*」に、Registry Servicesに対して照会を実行してサービス・プロバイダーおよびリソースに関する情報を得る方法が説明されています。

セキュリティー・サービスは、Performance Monitoring サービス・プロバイダーなどのような WebSphere ベースでないアプリケーションで、 LTPA ベースのシングル・サインオンを実行できるようにするオプションの Jazz for Service Management コンポーネントです。 Performance Monitoring サービス・プロバイダーが OSLC クライアントから受け取った要求を認証するようにする場合は、このコンポーネントをインストールし、構成する必要があります。これが、このサービス・プロバイダーでサポートされている唯一の認証方式です。詳しくは、 134 ページの『Tivoli Enterprise Monitoring Automation Serverを使用した認証』 を参照してください。

Performance Monitoring サービス・プロバイダーを Tivoli Business Service Manager V6.1.1 ダッシュボード・サーバーと共に使用すると、Tivoli Enterprise Portal をコンテキスト起動せずに、モニター・エージェントの主要な正常性メトリックをサービス・ツリーに表示できます。正常性メトリックを使用できるのは、Performance Monitoring サービス・プロバイダーによってコンピューター・システムやソフトウェア・サーバーなどのリソースが Registry Services に登録されており、かつこれらのリソースが IBM Tivoli Monitoring Discovery Library Adapter または Tivoli Application Dependency Discovery Manager センサー (TADDM OSLC サービス・プロバイダーも使用されている場合) によってディスカバーされている場合です。これらのメトリックは吹き出しプレビュー・ダイアログに表示されます。このダイアログには、同じリソースを登録している他のサービス・プロバイダーの情報も表示されます。例えば Tivoli Application Dependency Discovery Manager の OSLC サービス・プロバイダーは、登録されたリソースの構成および変更履歴情報を吹き出しプレビュー・ダイアログに表示します。 Performance Monitoring サービス・プロバイダー、Tivoli Business Service Manager、 Registry Services、およびその他のサポートされているサービス・プロバイダーの間の統合をセットアップする方法については、 IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) で「IBM Tivoli Monitoring での製品相互統合」を検索してください。

Registry Servicesからリソース情報を取得し、Performance Monitoring サービス・プロバイダーからこれらのリソースの正常性メトリックを取得する、独自の OSLC クライアント・アプリケーションを作成することもできます。あるいは、登録リソースに関して使用可能な情報を拡張する独自の OSLC サービス・プロバイダー実装を作成することもできます。このようなアプリケーションの作成方法について詳しくは、Jazz for Service Management Wiki のGetting started with Registry Servicesを参照してください。

OSLC および疎結合統合について詳しくは、以下のリンクを参照してください。

- OSLC community
- Performance Monitoring working group

- Reconciliation working group and Common Resource Type Vocabulary
- Loosely coupled integration at ISM Connect
- IBM Tivoli Monitoring OSLC プライベート名前空間スキーマ

Tivoli Enterprise Monitoring Automation Server および Performance Monitoring サービス・プロバイダーのインストールおよび構成については、*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)を参照してください。

第 2 章 Tivoli Enterprise Portal 環境の準備

Tivoli Enterprise Portal クライアント環境の追加構成については、以下のトピックを参照してください。

ブラウザー・クライアント

Tivoli Enterprise Portal Server 上で統合 HTTP サーバーの URL を入力することによって、ブラウザー・クライアントを開始します。

ブラウザー・クライアントの利点は以下のとおりです。

- デプロイメントが容易です。ブラウザー・クライアントは、ユーザーが Tivoli Enterprise Portal 統合 HTTP サーバーの URL に最初にログオンした時点でインストールされます。
- ソフトウェアが自動的にアップグレードされます。ユーザーがログオンする際にブラウザー・クライアントが Tivoli Enterprise Portal Server のクライアントと照合され、新しいバージョンが検出された場合は、それがサーバーからダウンロードされます。
- グローバル・パラメーター設定は、同じ Tivoli Enterprise Portal Server に接続されたすべてのユーザーに対して設定されます。
- ワークスペースには、Web ページで参照でき、別の Web 対応アプリケーションからの起動時に参照できる識別 URL があります。
- 企業ロゴおよび URL を使用してカスタマイズできるバナーが含まれています。

Java ランタイム環境 (JRE) のバージョン

Tivoli Enterprise Portal Server およびクライアントは、Java ベースのソフトウェアを実行します。ポータル・サーバーまたはデスクトップ・クライアントのインストール時に IBM Java 7 が自動的にインストールされます。

IBM Web Start for Java を使用して Tivoli Enterprise Portal Server からデスクトップ・クライアントをダウンロードする前に、次のステップを実行してください。

- Tivoli Enterprise Portal Server をインストールする必要があります (『*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)』を参照してください。)
- デスクトップ・クライアントのダウンロード先のコンピューター上に、IBM 32 ビットまたは 64 ビット Java Runtime Environment for Windows バージョン 7.0 がインストールされている必要があります。

  Tivoli Enterprise Portal Server から IBM JRE インストーラーをダウンロードできます。IBM JRE がシステム JVM としてインストールされている必要があります。

Tivoli Management Services 基本コンポーネント (モニター・サーバーまたはポータル・サーバーなど) をインストール済みのシステムでデスクトップ・クライアントを実行する場合は、IBM JRE をインストールする必要はありません。正しいバージョンの IBM JRE が、Tivoli Management Services コンポーネントとともにインストールされます。

ブラウザーからログオンすると、ブラウザーに関連付けられている Java のレベルが検査されます。 Java の必須バージョンはポータル・サーバーで制御されており、接続時に IBM Java 7 にアップグレードするようプロンプトが出されることがあります。

最初のログオン

Tivoli Enterprise Portal の URL を初めてシステムから入力したときに、Java プラグインは、Tivoli Enterprise Portal Server から必要なファイルを転送します (Windows ではファイルは *<install_dir>*¥cnb ブランチに、UNIX 系のオペレーティング・システムでは *<install_dir>*/cw ブランチにあります)。

その後は、新バージョンがインストールされるまでブラウザー・クライアント・ソフトウェアを再度ダウンロードする必要はありません。 Java プラグインは、ユーザー・コンピューターでファイルのバージョン・レベルを保持し、統合 HTTP サーバーでのバージョン・レベルと比較します。 HTTP サーバー上のファイルより古いファイルが検出された場合は、最新のファイルがダウンロードされます。

ダウンロードしたファイル用の十分なフリー・スペースが必要です。ダウンロード中にディスク・スペースが不足しても警告は出されません。

Internet Explorer のセキュリティー設定

このタスクについて

Internet Explorer のセキュリティー・レベルを「高」に設定している場合、Tivoli Enterprise Portal を実行するには設定を調整する必要があります。調整しないと、Tivoli Enterprise Portal ブラウザー・クライアントを実行することはできません。

セキュリティー設定の確認

現在のセキュリティー設定を確認するには、次の手順を使用する必要があります。

手順

1. Internet Explorer で、「**ツール**」→「**インターネット オプション**」を選択します。
2. 「**セキュリティ**」タブを選択します。
3. インターネット経由で Tivoli Enterprise Portal を実行している場合は、「**インターネット**」をクリックします。イントラネット経由で Tivoli Enterprise Portal を実行している場合は、「**イントラネット**」をクリックします。
4. セキュリティー設定を「**既定のレベル**」に変更します。
5. 「**OK**」をクリックして保存します。

現行のセキュリティー設定の保持

セキュリティー設定を変更せずに、Tivoli Enterprise Portal Web サイトを Internet Explorer に統合できます。現行のセキュリティー設定を保持する場合は、Tivoli Enterprise Portal Web サイトを「信頼済みサイト」ゾーンに追加できます。

手順

1. Internet Explorer で、「**ツール**」→ 「**インターネット オプション**」を選択します。
2. 「**セキュリティ**」タブを選択します。
3. 「**信頼済みサイト**」→ 「**サイト**」をクリックして Tivoli Enterprise Portal の URL を入力します。
4. 「このゾーンのサイトにはすべてサーバーの確認 (https:) を必要とする」のチェック・マークを外し、「**追加**」をクリックします。

   「**信頼済みサイト**」ゾーンのすべてのサイトに「中」以下のセキュリティー・レベルを選択します。
5. 「**OK**」をクリックして、変更を保存します。

Windows の書き込みおよび削除特権

Windows 2000 からは、特定のフォルダーおよびレジストリー・キーの書き込みおよび削除特権が Users グループから削除されました。これらの特権は、Java WebStart のクライアントまたはブラウザー・クライアントを使用する予定があるユーザーに必要なものです。これらがないと、製品を開始しようとしたときに、Java 例外エラーが発生します。

ユーザーが Java WebStart クライアントをダウンロードしたり、ブラウザー・クライアントを開始したりするには、Windows 管理者が個々のユーザー ID または Users グループに必要な権限を割り当てるか、必要な権限を持つ新規グループを作成して、そのグループと Users グループの両方にユーザーを割り当てる必要があります。必要な権限は以下のとおりです。

- Windows のインストール先ディレクトリー (C:¥WINDOWS など) に対する書き込みおよび削除権限。
- レジストリー・キー HKEY_LOCAL_MACHINE¥SOFTWARE に対する値の設定、サブキーの作成、および削除権限。

注: Windows 許可スキームは、Tivoli Enterprise Portal ブラウザー・モードと、Internet Explorer 経由でインストールされた他のサード・パーティー・ソフトウェアに影響します。

会社のロゴおよび URL の追加

Tivoli Enterprise Portal ブラウザー・アプリケーションは、デスクトップ・モードのときと同じように見えますが、ibm.com® へのリンクが付いたバナーがあります。Tivoli Enterprise Portal のブラウザー・クライアントをカスタマイズして、ロゴおよび URL を組織独自のもので置き換えることができます。

このタスクについて

ポータル・クライアント・バナーをカスタマイズするには、以下のステップを実行してください。

手順

1. Tivoli Enterprise Portal Server をインストールしたコンピューターにある以下のファイルを、HTML エディターまたはテキスト・エディターで開きます。

   install_dir ¥cnb¥bannerimage.html

2. 以下のように HREF および IMG SRC タグを編集し、組織の URL およびロゴ・グラフィック・ファイルに変更します。
   a. **href** ' + URL + ' プレースホルダーを、お客様の組織の URL に置換します。
   b. **img src** ' + URL + ' プレースホルダーを、お客様の組織で使用しているロゴの GIF ファイルまたは JPG ファイルの名前に置換します。
   c. **alt** ' + URL + ' プレースホルダーを、イメージの上にマウス・ポインターを置いたときに表示される URL などのテキストに置換します。
3. ファイルを保存して、エディターを終了します。
4. ロゴ・グラフィックを *install_dir* ¥cnb¥ ディレクトリーにコピーします。

タスクの結果

次にブラウザー・モードを開始すると、バナーの右側に会社のロゴが表示されます。

Tivoli Enterprise Portal クライアントの開始

Tivoli Enterprise Portal Server にログオンし、Tivoli Enterprise Portal ワーク・セッションを開始します。

始める前に

ポータル・クライアントを正常に開始するには、ハブ Tivoli Enterprise Monitoring Server およびポータル・サーバーが実行されている必要があります。また、有効なユーザー ID も必要です。

このタスクについて

IBM Tivoli Monitoring 環境のすべてのコンポーネントを正常にインストールし、構成した後、Tivoli Enterprise Portal を起動してモニター・データを表示することにより、インストールおよび構成を検査できます。ポータルには、デスクトップ・クライアントまたはブラウザー・クライアントのいずれかを使用してアクセスできます。デフォルトのユーザー ID は sysadmin です。

手順

- デスクトップ・クライアントを開始するには、以下のようにします。

– Windows 「スタート」→「プログラム」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Portal**」をクリックします。ログオン・ウィンドウが表示されたら、ユーザー ID とパスワードを入力して、「**OK**」をクリックします。

– Linux UNIX コマンド行で `./itmcmd agent start cj` を入力します。

- ブラウザー・クライアントを開始するには、以下のようにします。
  1. ブラウザーを開始します。
  2. 以下のような Tivoli Enterprise Portal Server の URL をブラウザーの**アドレス**・フィールドに入力します。ここで、*systemname* はポータル・サーバーがインストールされているコンピューターのホスト名であり、*15200* はブラウザー・クライアントのポート番号です。`http://systemname:15200`
  3. 「警告 - セキュリティー (Warning - Security)」ウィンドウで、「**はい**」をクリックします。
  4. ログオン・ウィンドウが表示されたら、ユーザー ID とパスワードを入力して、「**OK**」をクリックします。

Web Start を使用した、デスクトップ・クライアントのダウンロードおよび実行

Tivoli Enterprise Portal Server から IBM Web Start for Java を使用して取得したデスクトップ・クライアントには、サーバーからの中央管理による利点があります。ブラウザー・クライアントと同様、クライアントを開始するたびに最新の更新で自動的に構成されるため、アプリケーション・サポートを構成する必要がありません。

このセクションは、お客様への便宜のために「*IBM Tivoli Monitoring インストールおよび設定ガイド*」から複製されています。

IBM Web Start for Java を使用して Tivoli Enterprise Portal Server からデスクトップ・クライアントをダウンロードする前に、次のステップを実行してください。

- Tivoli Enterprise Portal Server をインストールする必要があります (『*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)』を参照してください。)
- デスクトップ・クライアントのダウンロード先のコンピューター上に、IBM 32 ビットまたは 64 ビット Java Runtime Environment for Windows バージョン 7.0 がインストールされている必要があります。

  Tivoli Enterprise Portal Server から IBM JRE インストーラーをダウンロードできます。IBM JRE がシステム JVM としてインストールされている必要があります。

  Tivoli Management Services 基本コンポーネント (モニター・サーバーまたはポータル・サーバーなど) をインストール済みのシステムでデスクトップ・クライア

ントを実行する場合は、IBM JRE をインストールする必要はありません。正しいバージョンの IBM JRE が、Tivoli Management Services コンポーネントとともにインストールされます。

IBM JRE のインストール

このタスクについて

IBM Tivoli Monitoring の基本コンポーネントがインストールされていないコンピューター上で、Web Start を使用してデスクトップ・クライアントをダウンロードし、実行する場合は、まず IBM Java 7 をインストールする必要があります。次のようにして、Tivoli Enterprise Portal Serverがインストールされているコンピューターからインストーラーをダウンロードします。

Windows: IBM JRE のインストール

Java Web Start を使用してデスクトップ・クライアントを起動する予定があるコンピューターに IBM Java ランタイム環境をインストールします。

このタスクについて

Tivoli Enterprise Portal Server から IBM JRE インストーラーをダウンロードして、Windows コンピューターに JRE をインストールするには、次のステップを実行します。

注: 以下の手順は、IBM JRE を 32 ビット Windows プラットフォームにインストールする場合を想定しています。64 ビット Windows プラットフォームをお使いの場合、 IBM JRE インストーラー実行可能ファイルの名前は `ibm-java7_64.exe` です。

手順

1. インストーラーのダウンロード先のコンピューターで、ブラウザーを始動します。
2. ブラウザーの「**アドレス**」フィールドに以下の URL を入力します。ここで、<*portal_server_host_name*> は、ポータル・サーバーがインストールされているコンピューターの完全修飾ホスト名です (例: `myteps.itmlab.company.com`)。

   ```
   http://<portal_server_host_name>:15200/java/ibm-java7.exe
   ```

3. プロンプトが出たら、**ibm-java7.exe** ファイルをご使用のハード・ディスクのディレクトリーに保存します。
4. **ibm-java7.exe** ファイルを保存したディレクトリーに移動し、このファイルをダブルクリックして、JRE インストーラーを起動してインストール・プログラムを開始します。
5. ポップアップ・ウィンドウで、ドロップダウン・リストから言語を選択し、「**OK**」をクリックします。
6. ウェルカム・ページで、「**次へ**」をクリックします。
7. ご使用条件を受諾するために「**はい**」をクリックします。
8. JRE をインストールするデフォルトのロケーションを受け入れるか、別のディレクトリーを参照します。「**次へ**」をクリックします。

9. 他のシステム JVM をインストールしていない場合は、この JRE をシステム JVM としてインストールするかどうかを尋ねるメッセージに対して「**はい**」をクリックします。それ以外の場合、「**いいえ**」をクリックします。
10. 現在、別の JRE がシステム JVM としてインストールされている場合で、現行システム JVM を上書きするようプロンプトが出されたら、「**いいえ**」をクリックします。 現行システム JVM を上書きすると、現在の JVM に依存しているアプリケーションに障害が起こります。
11. 「ファイルのコピーを開始 (Start Copying File)」ウィンドウで「**次へ**」をクリックして、JRE のインストールを開始します。
12. 「ブラウザー登録 (Browser Registration)」ウィンドウで、IBM JRE を関連付けるブラウザーを選択します。これは通常、ブラウザー・クライアントで使用するブラウザーになります。
13. 「**次へ**」をクリックします。
14. 「**完了 (Finish)**」をクリックして、インストールを完了します。

Linux: IBM JRE のインストール

Java Web Start を使用してデスクトップ・クライアントを起動する予定があるコンピューターに IBM Java ランタイム環境をインストールします。

このタスクについて

以下のステップを実行して、Tivoli Enterprise Portal Server から IBM JRE インストーラーをダウンロードし、Linux コンピューターに JRE をインストールします。または、コマンド行の rpm に以下の URL を入力し、インストーラーをダウンロードせずに JRE をインストールします。

```
rpm -ivh http://portal_server_host_name:15200/java/ibm-java7.rpm
```

注: 以下の手順は、IBM JRE を 32 ビット Linux プラットフォームにインストールする場合を想定しています。64 ビット Linux プラットフォームをお使いの場合、IBM JRE `.rpm` ファイルの名前は `ibm-java7_64.rpm` になります。

手順

1. インストーラーのダウンロード先のコンピューターで、ブラウザーを始動します。
2. ブラウザーの「**アドレス**」フィールドに、次の URL を入力します。

   ```
   http://portal_server_host_name:15200/java/ibm-java7.rpm
   ```

   この場合、*portal_server_host_name* は、ポータル・サーバーがインストールされているコンピューターの完全修飾ホスト名 (例えば、`myteps.itmlab.company.com`) です。
3. プロンプトが出たら、インストーラーをディスクに保存します。
4. `ibm-java7.rpm` ファイルを保存したディレクトリーに移動し、次のコマンドを使用して、インストーラーを起動し、インストール・プログラムを開始します。

   ```
   rpm -ivh ibm-java7.rpm
   ```

JRE に対するトレースを使用可能にする

Web Start によって起動されたデスクトップ・クライアントのログ・ファイルは、JRE に対するトレースを使用可能にしないと、作成されません。

始める前に

Web Start クライアントのログは、ブラウザー・クライアントのログや、メディアからインストールされたデスクトップ・クライアントのログとは異なる場所に置かれます。Windows コンピューターでは、Web Start クライアントのログは、`C:¥Documents and Settings¥Administrator¥Application Data¥IBM¥Java¥Deployment¥log` または `%USERPROFILE%¥AppData¥LocalLow¥IBM¥Java¥Deployment¥log` ディレクトリーにあります。Linux コンピューターおよび UNIX コンピューターの場合、ログは、Java JRE をインストールした際のユーザー ID のホーム・ディレクトリーの `.java/deployment/log` ディレクトリーにあります。Java Web Start は、アプリケーションが起動されるたびに、一意的に命名されたトレース・ファイルを作成します。ファイルは、`javaws.`*`nnnnn`*`.trace` という名前になります。ここで、*`nnnnn`* は任意の 5 桁の ID です。

このタスクについて

次のステップを実行して、トレースを使用可能に設定してください。

手順

1. IBM Control Panel for Java を起動します。
   - Windows の場合、「**スタート**」>「**コントロール パネル**」を選択し、「Java 用 IBM コントロール・パネル (IBM Control Panel for Java)」をダブルクリックします。「コントロール パネル」を表示し、選択するには、クラシック表示に切り替える必要があります。または**「スタート」>「ファイル名を指定して実行」>「C:¥Program Files¥IBM¥Java70¥jre¥bin¥javacpl.exe」**と操作して、「コントロール パネル」を起動します。
   - Linux の場合、 `<`*`install_dir`*`>/jre/<`*`platform`*`>/bin` に移動し、コントロール・パネル `./ControlPanel` を実行します。
2. 「**拡張**」タブを選択します。
3. 「**設定**」ツリーで、「デバッグ (Debugging)」ノードを展開し、「**トレースを使用可能にする (Enable Tracing)**」にチェック・マークを付けます。
4. 「**OK**」をクリックして設定を保存し、「Java コントロール パネル」を閉じます。

デスクトップ・クライアントのダウンロードおよび実行

Tivoli Enterprise Portal は、デスクトップ・アプリケーションまたは Web アプリケーションとして開始することができます。デスクトップ・アプリケーションをインストールするには、次の 3 通りの方法があります。ブラウザーで Tivoli Enterprise Portal Server 上の Java Web Start クライアントの URL を入力する方法、「IBM Java コントロール・パネル」からデスクトップ・クライアントを起動する方法、またはコマンド行から Java Web Start を使用してデスクトップ・クライアントを起動する方法です。

始める前に

以下は、Java Web Start を使用してデスクトップ・クライアントをダウンロードして、実行するための基本的な手順です。構成メモを含む詳細な手順については、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」を参照してください。

このタスクについて

Java Web Start を使用してデスクトップ・クライアントをインストールおよび起動するには、以下の手順のいずれかを実行します。

手順

- 次のように、ブラウザーにポータル・サーバーの URL を入力します。
  1. デスクトップ・クライアントを使用するコンピューターで、ブラウザーを始動します。
  2. ブラウザーの「**アドレス**」フィールドに以下の URL を入力します。ここで、<*portal_server_host_name*> は、Tivoli Enterprise Portal Server がインストールされているコンピューターの完全修飾ホスト名です。

     ```
     http://<portal_server_host_name>:15200/tep.jnlp
     ```

  3. セキュリティー・メッセージに対し、「**実行**」をクリックします。
  4. デスクトップ上に Tivoli Enterprise Portal のショートカットを作成するには、プロンプトが出されたら「**はい**」をクリックします。 デスクトップ・クライアントが開始し、ログオン・ウィンドウが表示されます。IBM Java 1.7 がシステム JVM でない場合、このショートカットは使用できません。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Web Start クライアント用のショートカットを手動で作成する』の説明に従って、独自のショートカットを作成する必要があります。
  5. ユーザー ID およびパスワードを入力して Tivoli Enterprise Portal にログオンするか、この時点でログオンしない場合は 「**キャンセル**」をクリックします。 デフォルトのユーザー ID は *sysadmin* です。

  Tivoli Enterprise Portal クライアントの RAS トレース・オプションを設定すると (「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照)、クライアントをリサイクルするときに、`kcjras1.log` がクライアントの起動場所に作成されているはずです。Windows の場合、これはデフォルトで `¥Documents and Settings¥<userid>¥Desktop` になります。
- IBM Java コントロール・パネルからデスクトップ・クライアントを起動します。
  1. 以下のようにして、「IBM Java コントロール パネル (IBM Java Control Panel)」を起動します。

     Windows Windows の「コントロール パネル」で、「**Java(TM) コントロール・パネル**」をダブルクリックします。「**IBM Java コントロール・パネル**」を表示するには、「クラシック」表示である必要があります。

     Linux <*install_dir*>/jre/<*platform*>/bin ディレクトリーに移動し、`./ControlPanel` と入力します。
  2. 「**一般**」タブの「インターネット一時ファイル」セクションで、「**設定**」をクリックします。「一時ファイルの設定 (Temporary Files Settings)」ウィンドウが表示されます。
  3. 「**アプリケーションの表示 (View Applications)**」をクリックします。

4. 「**ユーザー**」タブで、Tivoli Enterprise Portal を選択し、「**オンラインで起動**」をクリックします。

Java Web Start がデスクトップ・クライアントをダウンロードして、開始します。アプリケーションが起動されたら、コントロール・パネルのウィンドウを閉じることができます。

- コマンド行から Java Web Start を使用してデスクトップ・クライアントを起動してください。
  1. コマンド行ウィンドウを開き、Java Web Start がインストールされているディレクトリーに移動します。

     Windows

     ```
     C:¥Program Files¥IBM¥Java70¥jre¥bin
     ```

     Linux

     ```
     <install_dir>/jre/<platform>/bin
     ```
  2. 以下のコマンドを入力します。ここで、<*portal_server_host_name*> は Tivoli Enterprise Portal Server がインストールされているコンピューターの完全修飾ホスト名です。

     Windows

     ```
     javaws http://<portal_server_host_name>:15200/tep.jnlp
     ```

     Linux

     ```
     ./javaws http://<portal_server_host_name>:15200/tep.jnlp
     ```

     Java Web Start がデスクトップ・クライアントをダウンロードして、起動します。

Web Start クライアントのショートカットを手動で作成する

Windows では、デフォルトの Java JVM の Web Start 実行可能ファイルは、Windows¥System32 ディレクトリーにコピーされます。Web Start でデスクトップ・クライアントを起動するショートカットを作成すると、ターゲットとして System32 ディレクトリー内のそのファイルが使用されます。デフォルト JVM が IBM Java 1.7 でない場合、ショートカットは、デスクトップ・クライアントを起動しません。ショートカットを手動で作成する必要があります。

このタスクについて

Web Start を使用して、デスクトップ・クライアントの起動に使用するショートカットを作成するには、以下の手順を実行します。

手順

1. Windows デスクトップを右クリックして、ポップアップ・メニューから「**新規作成**」>「**ショートカット**」を選択します。
2. 「ショートカットの作成」ウィンドウで、次のパスを入力するか、「**参照**」をクリックして次に示されている実行可能ファイルにナビゲートします。

   ```
   C:¥Program Files¥IBM¥Java70¥jre¥bin¥javaws.exe
   ```
3. 「**次へ**」をクリックして、「名前の指定」ウィンドウでショートカットの名前を入力します。例:

ITM Web Start client

4. 「**完了**」をクリックします。 ショートカットがデスクトップに表示されます。

別のポータル・サーバーでのデスクトップ・クライアントの開始

デスクトップ・クライアントをインストールするときには、ホーム Tivoli Enterprise Portal Server を指定します。ご使用のモニター環境に複数のポータル・サーバーがある場合は、別のポータル・サーバーを指す別のデスクトップ・インスタンスを定義することができます。

始める前に

複数のポータル・サーバーがある典型的なシナリオとしては、テスト用と実動用のポータル・サーバーがある場合や、各ハブ・モニター・サーバーに 1 つのポータル・サーバーが接続された複数の管理対象ネットワークがある場合が挙げられます。

このタスクについて

別のポータル・サーバーに接続する別のポータル・クライアントのインスタンスを作成するには、以下のステップを実行します。

手順

- Windows
  1. デスクトップ・クライアントがインストールされているコンピューターで、「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Monitoring Services の管理**」を選択します。
  2. **Tivoli Enterprise Portal デスクトップ・クライアント**を右クリックして、「**インスタンスの作成**」をクリックします。別の Tivoli Enterprise Portal のインスタンスが作成されると、リストに複数のインスタンスが表示されるようになります。「**インスタンスの作成**」は、元の Tivoli Enterprise Portal インスタンス以外のインスタンスには使用できません。
  3. 「Tivoli Enterprise Portal」ウィンドウで、インスタンスを識別する名前を入力して「**OK**」をクリックします。
  4. 「アプリケーション・インスタンスの構成」ウィンドウに、接続先 Tivoli Enterprise Portal Server のホスト名を入力します。
  5. 「**OK**」をクリックします。
- Linux UNIX コマンド行を使用する場合:
  1. ディレクトリーを *install_dir* /bin に変更します (cd)。
  2. 以下のコマンドを使用して、新規インスタンスを作成します。

     ```
     ./itmcmd config -A cj
     ```
  3. 以下のコマンドを使用して、新規インスタンスを起動します。

     ```
     ./itmcmd agent -o <instance_name> start cj
     ```

     詳しい構文情報については、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

  GUI を使用する場合:

1. ディレクトリーを *install_dir* /bin に変更します (cd)。
2. Tivoli Enterprise Monitoring Services の管理 を開始するには、以下のコマンドを使用します。

   ```
   ./itmcmd manage
   ```

3. **Tivoli Enterprise Portal デスクトップ・クライアント**を右クリックして、「**構成**」をクリックします。
4. インスタンス名とポータル・サーバー・ホスト名を入力し、「**保存**」をクリックします。
5. インスタンスを開始するには、「**Tivoli Enterprise Portal デスクトップ・クライアント**」を右クリックして「**サービスの開始**」をクリックし、インスタンス名を入力します。

タスクの結果

新しい Tivoli Enterprise Portal インスタンスがリストに追加されます。

次のタスク

その項目をダブルクリックすると、いつでもインスタンスを開始することができます。

Tivoli Enterprise Portal インスタンスが不要になった場合は、その項目を右クリックして、「**インスタンスの削除**」をクリックすると削除できます。

別のポータル・サーバーでのブラウザー・クライアントの開始

別のブラウザー・インスタンスを開始して、別の管理対象ネットワークの Tivoli Enterprise Portal Server にログオンすることで、1 台のコンピューターから 2 つの管理対象ネットワークを監視できます。

始める前に

管理対象ネットワークは、ポータル・サーバーとハブ Tivoli Enterprise Monitoring Server を 1 つずつ含むことができます。ポータル・サーバーには、Windows Internet Explorer または Mozilla Firefox からログオンすることができます。

このタスクについて

ブラウザー・クライアント・インスタンスを開始する前に、接続先のポータル・サーバーがインストールされている各コンピューターに対して以下のステップを実行します。

手順

- Windows
  1. Tivoli Enterprise Monitoring Services の管理 で、「**Tivoli Enterprise Portal Server**」項目を右クリックし、 「**再構成**」を選択します。
  2. 開いた「Tivoli Enterprise Portal ブラウザーの構成」ウィンドウで、「**cnp.browser.installdir**」パラメーターをダブルクリックします。

3. 開いた「Tivoli Enterprise Portal ブラウザー・パラメーターを編集します」ウィンドウで、ブラウザー・ファイルのインストール先となるディレクトリーのパス (例: C:¥¥temp¥¥cnpBrowserFiles) を入力します。
4. ☑ 「**使用中**」チェック・ボックスを選択して、「**OK**」をクリックします。
5. 「**OK**」をクリックして、変更を保存します。

- Linux

1. applet.html が配置されている *install_dir* /platform/cw ディレクトリーに移動します。ここで、platform はオペレーティング・システムの現在のタイプです。
2. テキスト・エディターで applet.html を開きます。
3. 行 **<!--END OF PARAMS-->** を見つけ、その上に新しい行を追加します。
4. 新しい行に以下のパラメーターを追加します。ここで、*browser_install_dir* はブラウザー・ファイルがインストールされているディレクトリーのパスです。

```
document.writeln( '<PARAM NAME= "cnp.browser.installdir"
VALUE="browser_install_dir">' )
```

5. applet.html を保存して閉じます。

次のタスク

Internet Explorer を使用している場合は、必要なポータル・クライアントの各インスタンスを起動します。

Firefox ブラウザーを使用している場合は、開始するインスタンスごとに別のプロファイルを作成する必要があります。プロファイルの設定については、Mozilla サポート・サイトで「Managing Profiles」(http://support.mozilla.com/en-US/kb/Managing+Profiles) を参照してください。プロファイルを作成したら、コマンド ***<full_path_to_firefox>* -p *<profile_name>* -no-remote** を使用して、各インスタンスを起動します。

関連資料:

68 ページの『ポータル・クライアント・パラメーターのリスト』

Tivoli Enterprise Portal クライアント・パラメーターのほとんどは、デフォルト値のまま変更されません。クライアント・パラメーターを編集すると、特定の動作に影響を与えることができます。

アプリケーションの起動およびオンライン・ヘルプに使用するブラウザーの指定

Linux でデスクトップ・クライアントを実行する場合、またはデフォルト以外のブラウザーを使用してオンライン・ヘルプを表示する場合は、使用するブラウザーのロケーションをポータル・サーバーに指定します。

このタスクについて

以下のステップを実行して、オンライン・ヘルプおよびアプリケーションの起動に使用する異なるブラウザーを指定します。

手順

- Windows
  1. Tivoli Enterprise Monitoring Services の管理 を起動します (**「スタート」>「(すべての) プログラム」>「IBM Tivoli Monitoring」>「Tivoli Enterprise Monitoring Services の管理」**)。
  2. 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、ブラウザーまたはデスクトップ・クライアントを右クリックし、**「再構成」**を選択します。「Tivoli Enterprise Portal ブラウザーの構成 (Configure the Tivoli Enterprise Portal Browser)」ウィンドウが表示されます。(デスクトップ・クライアントを構成している場合は、「アプリケーション・インスタンスの構成」ウィンドウが表示されます。)
  3. `kjr.browser.default` 変数が表示されるまで、変数のリストをスクロールダウンします。
  4. `kjr.browser.default` をダブルクリックします。 「Tivoli Enterprise Portal ブラウザー・パラメーターの編集 (Edit Tivoli Enterprise Portal Browser Parm)」ウィンドウが表示されます。
  5. 「値」フィールドで、代替ブラウザー・アプリケーションのパスおよびアプリケーション名を入力します。 例えば、`C:¥Program Files¥Mozilla Firefox¥firefox.exe` と入力します。
  6. **「OK」**をクリックして編集ウィンドウを閉じ、変更を保存します。
  7. **「OK」**をクリックして再構成ウィンドウを閉じます。
- Linux UNIX
  1. *install_dir*/bin/cnp.sh に移動し、cnp.sh シェル・スクリプトを編集します。
  2. ファイルの最後の行に Web ブラウザーの場所を追加します。以下の例では、Web ブラウザー・ロケーションは */opt/foo/bin/launcher* です。`-Dkjr.browser.default=/opt/foo/bin/launcher` この行は非常に長く、他のプロパティーを定義するための各種 -D オプションをはじめとするさまざまなオプションが記述されています。オプションを正しい位置に追加することが非常に重要です。

  bin/cnp.sh の元の最終行が以下のようであるとします。

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

  ブラウザーの場所を */opt/foo/bin/launcher* に設定するには、この行を以下のように変更します。

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.browser.default=/opt/foo/bin/launcher
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

- Java Web Start:

Java Web Start でデプロイされるアプリケーションは、jnlp デプロイメント・ファイルに記述されます。IBM Tivoli Monitoring の場合、コア Tivoli Enterprise Portal フレームワーク・コンポーネントおよび関連の JAR ファイルを記述するデプロイメント・ファイルが 1 つと、インストール対象の Tivoli Enterprise Portal ベース・モニター・ソリューションのそれぞれに対するデプロイメント・ファイルが 1 つ存在します。コア Tivoli Enterprise Portal Server デプロイメント・ファイルの名前は、tep.jnlp です。通常、アプリケーション・デプロイメント・ファイルの名前は、k*xx*_resources.jnlp または k*xx*.jnlp です。ここで、*xx* はアプリケーション ID (nt、ux、または lz などの製品コード) です。 Tivoli Enterprise Portal Server がインストールされている Windows コンピューターの場合、ファイルは <*itminstall_dir*>¥CNB にあります (例: c:¥IBM¥ITM¥CNB)。Tivoli Enterprise Portal Server がインストールされている Linux コンピューターの場合、ファイルは <*itminstall_dir*>/<arch>/cw にあります (例: /opt/IBM/ITM/li6263/cw)。

デプロイメント・ファイル・インスタンスは、Tivoli Enterprise Portal Server がインストールされるか再構成されるとき (例えば、新規モニタリング・ソリューションを環境に追加しているとき) に常に生成されます。これらのファイルの内容は、2 つのテンプレート・デプロイメント・ファイル (.jnlpt) に基づいています。コア Tivoli Enterprise Portal テンプレート・デプロイメント・ファイルの名前は、tep.jnlpt です。アプリケーション・テンプレート・デプロイメント・ファイルの名前は、component.jnlpt です。 Tivoli Enterprise PortalTivoli Enterprise Portalがインストールされている Windows コンピューターの場合、ファイルは <*itminstall_dir*>¥Config にあります (例: c:¥IBM¥ITM¥Config)。UNIX コンピューターの場合、ファイルは <*itminstall_dir*>/config にあります (例: /opt/IBM/ITM/config)。

JVM 引数 (最大ヒープ・サイズなど) またはその他の Tivoli Enterprise Portal ベースのプロパティー (RAS1 トレース・オプションなど) を追加または変更するには、tep.jnlp デプロイメント・ファイルか tep.jnlpt デプロイメント・テンプレート・ファイルのいずれかを編集する必要があります。デプロイメント・ファイルは、デプロイされる Web Start アプリケーションを記述する XML 構文にすぎません。<resources> 要素は、JVM 引数、Tivoli Enterprise Portal プロパティー、JAR ファイル、およびコンポーネント・デプロイメント・ファイルへの参照を定義するために使用されます。

– 変更が一時的である場合は (例えば、追加で診断を収集するためのトレース・オプションの設定など)、tep.jnlp ファイルを変更します。
– 変更が永続的である場合は (例えば、モニター環境が大規模になったり、イベント負荷が増大した際に最大ヒープ・サイズを大きくするなど)、tep.jnlpt ファイルを変更します。

  デプロイメント・テンプレート・ファイルを変更する場合は、変更に伴いインスタンス・レベルの .jnlp デプロイメント・ファイルを再生成するために、必ず Tivoli Enterprise Portal Server を再構成してください。

オンライン・ヘルプを表示するために使用するブラウザーのロケーションを指定するには、次のプロパティーを、適切なファイルの <resources> セクションに追加します。

```
<property name="kjr.browser.default" value="<path where browser is located>" >
```

ナビゲーター・ビューへの作動プラットフォームの追加

Tivoli Enterprise Portal Server の `osnames` ファイルを編集して、他のオペレーティング・システム名に対応する追加の分岐を Tivoli Enterprise Portal のナビゲーター・ビュー内に作成します。

Tivoli Enterprise Portal の「物理」ナビゲーター・ビューには、エンタープライズ・レベルより下の作動プラットフォームが表示されます。作動プラットフォーム名の後には、システム という単語が付きます (Linux システムまたは z/OS® システムなど)。一部の作動プラットフォームは、さらに集約することができます。ご使用の環境にそのようなプラットフォームがあり、各プラットフォームに独自のナビゲーター項目を持たせ、そのタイプのすべてのシステムをその項目に含める場合は、ポータル・サーバー・ディレクトリー (例えば、C:¥IBM¥ITM¥CNPS および /opt/IBM/ITM/config) 内の `osnames` ファイルにそれらのシステムを追加することができます。

第 3 章 ダッシュボード環境の準備

ダッシュボード環境の追加構成については、以下のトピックを参照してください。

ロードマップ

環境を設定するためのタスクはさまざまな要因に左右されます。ダッシュボード環境の主なタイプは 2 つあります。1 つは、シングル・サインオンまたはユーザーごとの許可制御を使用しない基本環境です。もう 1 つは、シングル・サインオンおよびユーザーごとの許可制御を使用する高度な環境です。シングル・サインオンまたはユーザーごとの許可制御を使用しない環境を最初に作成した場合、後で設定を変更してシングル・サインオンおよびユーザーごとの許可制御を使用することができます。

シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ

IBM Dashboard Application Services Hub をモニター・ダッシュボード・アプリケーション (IBM Infrastructure Management Dashboards for Servers や IBM Infrastructure Management Dashboards for VMware など) またはカスタム・ダッシュボードと共に使用するが、シングル・サインオンまたはユーザーごとの許可制御を使用しない場合は、基本ダッシュボード環境をセットアップします。

ご使用の環境は以下の要件を満たしている必要があります。

- Dashboard Application Services Hub と Tivoli Enterprise Portal Server が、ユーザー認証に統合 LDAP ユーザー・レジストリーを使用するように構成されていない。
- ダッシュボード・ユーザーが IBM Dashboard Application Services Hub のページから Tivoli Enterprise Portal ブラウザー・クライアントを起動することがないか、または起動することがある場合はブラウザー・クライアントの起動時に資格情報を提供する必要がある。
- すべてのダッシュボード・ユーザーに対し、モニター・ダッシュボード・ページに同一の管理対象システムおよび管理対象システム・グループを表示することを許可できる。

ご使用の環境が上記の要件を満たしていない場合は、37 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ』のステップを実行してください。

注: 最初に基本ダッシュボード環境を使用して、IBM Dashboard Application Services Hub とモニター・ダッシュボードの操作に慣れてから、51 ページの『基本モニター・ダッシュボード環境から、シングル・サインオンおよびユーザーごとの許可による制御を使用するダッシュボード環境への移行』のステップに従って後からシングル・サインオンとユーザーごとの許可を追加することもできます。

Dashboard Application Services Hub は、ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントに HTTP または HTTPS 経由で接続し、モニター・データを取得します。リアルタイム・モニター・データがハブ・モニター・サーバーとモニター・エージェントから取得され、ヒストリカル・モニター・データが Tivoli Data Warehouse から取得されます。一部のモニター・ダッシュボード・アプリケーションでは Tivoli Data Warehouse からのヒストリカル・データの取得がサポートされていません。

Dashboard Application Services Hub でダッシュボード・データ・プロバイダー接続を構成します。この構成ではポータル・サーバーのホスト名、プロトコル、ポート、ユーザー名、およびパスワードを指定します。ダッシュボード・データ・プロバイダーへのすべての HTTP 要求には、Dashboard Application Services Hub にログインしてダッシュボード・アプリケーションを使用しているユーザーではなく、データ・プロバイダー接続用に構成されているユーザー ID が組み込まれます。接続ユーザーは Tivoli Enterprise Portal ユーザー ID として定義され、モニター・ダッシュボードにデータが表示されるモニター・アプリケーションを割り当てられる必要があります。Dashboard Application Services Hub では、ユーザーまたはユーザー・グループの役割を使用して、ユーザーがアクセスできるページが制御されます。ただし、これらのページに表示されるモニター・リソースの許可は、ダッシュボード・データ・プロバイダーによって実行されます。ダッシュボード・データ・プロバイダーは、データ・プロバイダー接続用に構成されているユーザーの資格情報のみを送信するため、ダッシュボード・ユーザーではなく、接続ユーザーの Tivoli Enterprise Portal 許可とモニター・アプリケーション割り当てを実施します。このため、すべてのモニター・ダッシュボード・ユーザーに対し、同一の管理対象システムまたは管理対象システム・グループのモニター・データが表示されます。

前提条件

- 「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の手順に従って基本 IBM Tivoli Monitoring モニター・サーバー、ポータル・サーバー、およびポータル・クライアント・コンポーネントをインストールして構成します。ポータル・サーバーを構成するときは、ダッシュボード・データ・プロバイダーを有効にします。
- モニター・ダッシュボードにデータが表示されるモニター・エージェントをインストールおよび構成します。、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の手順に従って、モニター・サーバー、ポータル・サーバー、およびデスクトップ・ポータル・クライアント (デスクトップ・ポータル・クライアントを使用する場合) にそのアプリケーション・サポートをインストールします。
- Dashboard Application Services Hub とダッシュボード・モニター・アプリケーションをインストールして構成します。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ダッシュボード環境のソフトウェア要件およびメモリー所要量』を参照してください。そのダッシュボード・アプリケーションをインストールする場合は、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『IBM Infrastructure Management Dashboards for Servers のインストールおよび構成』も参照してください。

ロードマップ

開始にあたって役立つロードマップを以下に示します。

表 1. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ

ステップ	説明	情報の入手先
1 (必須)	ポータル・サーバー構成でダッシュボード・データ・プロバイダーが使用可能であることを確認します。	詳しいステップについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ダッシュボード・データ・プロバイダーが使用可能であることの確認』を参照してください。
2 (必須)	ダッシュボード・データ・プロバイダー接続用に構成する Tivoli Enterprise Portal ユーザーを決定し、そのユーザーに次の許可があることを確認します。 • モニター・ダッシュボードにデータを表示するモニター・アプリケーションがユーザーに割り当てられている必要があります。 • ダッシュボード・アプリケーションにシチュエーション・イベントが表示される場合、ユーザーにはシチュエーション・イベントを表示する許可が必要です。	173 ページの『ユーザー管理』および 180 ページの『ユーザー ID の管理』
3 (必須)	IBM Dashboard Application Services Hub に管理ユーザーとしてログインし、HTTP プロトコルを使用し、かつシングル・サインオン構成を必要としないダッシュボード・データ・プロバイダー接続を作成します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択**しない**でください。
4 (オプションのベスト・プラクティス)	IBM Dashboard Application Services Hub に管理ユーザーとしてログインし、ダッシュボード・アプリケーション・ページへのアクセスを制御する役割を作成し、ダッシュボードのユーザーまたはユーザー・グループをこの役割に割り当てます。 **注:** IBM Infrastructure Management for VMware などの一部のダッシュボード・アプリケーションでは、ダッシュボード・アプリケーションのインストール時にそのページの役割が自動的に作成されます。しかし、IBM Infrastructure Management Dashboards for Servers などのその他のアプリケーションではインストール時に役割が作成されないため、役割を作成するか、または既存の役割にダッシュボード・ページを割り当てる必要があります。	ダッシュボード・ページへのアクセスを制御する役割の使用法について詳しくは、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。

表 1. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ (続き)

ステップ	説明	情報の入手先
5 (必須)	IBM Dashboard Application Services Hub に、ダッシュボード・ページを表示する許可を持つユーザーとしてログインし、ダッシュボード・アプリケーションを起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」**を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」**を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

表 1. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ (続き)

ステップ	説明	情報の入手先
6 (オプション)	Dashboard Application Services Hub とダッシュボード・データ・プロバイダーの間で HTTPS を使用する場合は、以下のタスクを実行します。	
	1. ダッシュボード・ハブとデータ・プロバイダーの間で TLS/SSL を構成します。	231 ページの『Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成』
	2. `administrator` 役割と `iscadmins` 役割が割り当てられている管理ユーザーとして IBM Dashboard Application Services Hub にログインし、以前に作成したダッシュボード・データ・プロバイダー接続を削除します。	データ・プロバイダー接続の操作方法については、IBM Dashboard Application Services Hub オンライン・ヘルプおよび Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Integration Guide*」を参照してください。
	3. IBM Dashboard Application Services Hub に管理ユーザーとしてログオンしたままの状態で、接続を再作成し、プロトコルとして HTTPS を指定します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択**しない**でください。
	4. ダッシュボード・ページを表示する許可を持つユーザーとして IBM Dashboard Application Services Hub にログインし、ダッシュボード・アプリケーションを再び起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、  「**システム状況および正常性**」 > 「**ダッシュボード・ヘルス・チェック**」を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、  「**システム状況および正常性**」 >を選択し、「**サーバー・ダッシュボード**」を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

基本ダッシュボード・モニター環境のセットアップが完了した後で、場合によっては以下のタスクも行う必要があります。

表 2. シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップに必要な追加タスク

タスク	情報の入手先
ダッシュボード・ユーザーがモニターするイベントのシチュエーション定義を作成します。	シチュエーションを処理するために使用する **tacmd** コマンドについては、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」のイベント・モニターのシチュエーションと「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

表 2. シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップに必要な追加タスク (続き)

タスク	情報の入手先
ダッシュボード・ページに表示する管理対象システムをグループ化するための管理対象システム・グループを作成します。	システム・リストを処理するために使用する **tacmd** コマンドについては、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」の環境の管理と「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。
ダッシュボード・ページにヒストリカル・データを表示する場合は、ヒストリカル・データ収集を構成します。 **注:** 一部のモニター・ダッシュボード・アプリケーションでは Tivoli Data Warehouse からのヒストリカル・データの取得がサポートされていません。	509 ページの『第 17 章 ヒストリカル・データの管理』
Dashboard Application Services Hub でダッシュボード・ページへの新規のユーザーまたはユーザー・グループのアクセスを許可します。	ダッシュボード・ページへのアクセスを制御する役割の使用法について詳しくは、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。 **ヒント:** ベスト・プラクティスは、ユーザー・グループを作成してユーザーをそのグループに追加してから、適切なダッシュボード・ページを表示する許可がある Dashboard Application Services Hub 役割をそのグループに割り当てることです。
Tivoli Enterprise Portal クライアントも使用する各ダッシュボード・ユーザーに対し、Tivoli Enterprise Portal ユーザー ID を作成し、ポータル・クライアントを使用するときに必要となるモニター・アプリケーションとその他の許可をそのユーザー ID に割り当てます。	173 ページの『ユーザー管理』および 180 ページの『ユーザー ID の管理』
カスタム・ダッシュボード・ページを作成し、カスタム・ページを表示する許可を持つ Dashboard Application Services Hub の役割がダッシュボード・ユーザーに割り当てられていることを確認します。	63 ページの『モニター・データを表示するカスタム・ダッシュボード・ページの作成』

表 2. シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップに必要な追加タスク (続き)

タスク	情報の入手先
Dashboard Application Services Hub に新しいモニター・ダッシュボード・アプリケーションをインストールし、ダッシュボードのページを新規または既存の役割に割り当て、ページへのアクセスを制御するその役割にユーザーまたはユーザー・グループを割り当てます。 ダッシュボード・データ・プロバイダー接続用に構成されている Tivoli Enterprise Portal ユーザーについて、新しいダッシュボード・アプリケーションにデータが表示されるモニター・アプリケーションが割り当てられていること、またダッシュボード・アプリケーションにシチュエーション・イベント・データが表示される場合にはイベントの表示許可が割り当てられていることを確認します。 **注:** 新しいダッシュボードにエージェントのデータを表示するには、エージェントのアプリケーション・サポートをポータル・サーバーとモニター・サーバーにインストールする必要があります。アプリケーション・サポートが自己記述型エージェント機能を使用してインストールされている場合は、ポータル・サーバーを再始動して、ダッシュボード・データ・プロバイダーが新しいサポート・パッケージを使用できるようにする必要があります。	ダッシュボード・アプリケーションのインストール資料の指示に従って作業します。 その後、ダッシュボード・ページへのアクセスを制御する役割の使用法の詳細について、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。 また、Tivoli Enterprise Portal ユーザーへのモニター・アプリケーションの割り当て方法の詳細を 173 ページの『ユーザー管理』で参照してください。 「*IBM Tivoli Monitoring インストールおよび設定ガイド*」には、アプリケーション・サポートのインストール手順が記載されています。
基本ダッシュボード環境から、シングル・サインオンおよびユーザーごとの許可を使用するダッシュボード環境に移行します。	51 ページの『基本モニター・ダッシュボード環境から、シングル・サインオンおよびユーザーごとの許可による制御を使用するダッシュボード環境への移行』
UISolutions のインポートを制御するかどうかを判断します (新規および更新されたダッシュボード・アプリケーションが UISolutions 定義を ダッシュボード・データ・プロバイダー に自動的にインポートします)。	65 ページの『UISolutions のインポートの制御』

シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ

IBM Dashboard Application Services Hub をモニター・ダッシュボード・アプリケーション (IBM Infrastructure Management Dashboards for Servers や IBM Infrastructure Management Dashboards for VMware など) またはカスタム・ダッシュボードと共に使用する場合は、ユーザーがダッシュボードでアクセスできるモニター・リソースを制御する許可とシングル・サインオンを使用して、拡張ダッシュボード環境をセットアップします。

シングル・サインオンを使用することで、IBM Dashboard Application Services Hub ユーザーが Tivoli Enterprise Portal ブラウザー・クライアントを起動するときに、資格情報を入力する必要がありません。許可ポリシーまたは Tivoli Enterprise Portal 許可を使用して、個別ユーザーまたはユーザー・グループのメンバーがダッシュボ

ードでどの管理対象システムと管理対象システム・グループにアクセスできるかどうかを制御し、またシチュエーション・イベントを表示できるかどうかを制御します。

シングル・サインオンを使用するには、IBM Dashboard Application Services Hub およびポータル・サーバーにログインするユーザーの資格情報が格納される、LDAP ユーザー・レジストリーをインストールして構成する必要があります。その後で、ユーザー認証に同じ LDAP ユーザー・レジストリーを使用し、Lightweight Third Party Authentication (LTPA) トークンを使用してシングル・サインオンを実行するように、IBM Dashboard Application Services Hub とポータル・サーバーを構成します。その他のアプリケーション (Netcool/OMNIbus WebGUI や Tivoli Business Service Manager など) のユーザーがポータル・クライアント・ブラウザーまたは Dashboard Application Services Hub を起動する場合は、同じ LDAP ユーザー・レジストリーを使用してこれらのユーザーを認証することもできます。

次に、Dashboard Application Services Hub からポータル・サーバーへのダッシュボード・データ・プロバイダー接続を構成し、シングル・サインオンを使用することを指定します。Dashboard Application Services Hub は、ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントに HTTP または HTTPS 経由で接続し、モニター・データを取得します。リアルタイム・モニター・データがハブ・モニター・サーバーとモニター・エージェントから取得され、ヒストリカル・モニター・データが Tivoli Data Warehouse から取得されます。一部のモニター・ダッシュボード・アプリケーションでは Tivoli Data Warehouse からのヒストリカル・データの取得がサポートされていません。

Dashboard Application Services Hub では、ユーザーまたはユーザー・グループの役割を使用して、ユーザーがアクセスできるページが制御されます。ただし、これらのページに表示されるモニター・リソースの許可は、ダッシュボード・データ・プロバイダーによって実行されます。ダッシュボード・ユーザーがアクセスできるモニター・リソースを許可するには次の 2 つのオプションがあります。

- Tivoli 許可ポリシー・サーバーおよび許可ポリシーの tivcmd コマンド行インターフェースを使用して役割と許可を作成する。これらの役割と許可をまとめて許可ポリシーと呼びます。

  許可ポリシーにより、ダッシュボード・ユーザーがアクセスできる管理対象システムと管理対象システム・グループが制御されます。職務権限に対応する役割が作成され、特定の管理対象システムまたは管理対象システム・グループを表示できる許可が役割に割り当てられます。ユーザーには、各自が属している役割に基づいて許可が付与されます。ユーザーを役割に直接割り当てるか、またはユーザーが属しているユーザー・グループを役割に割り当てることができます。この許可により、管理対象システムまたは管理対象システム・グループでアクセスできるオブジェクトのタイプも指定されます。サポートされているオブジェクト・タイプは、イベント (シチュエーション・イベントの場合) および属性グループ (エージェントから取得したモニター・データの場合) です。

  または

- ダッシュボード・ユーザーに Tivoli Enterprise Portal 許可アクセス権とモニター対象アプリケーションの割り当てを使用する。これは、ポータル・サーバー構成で許可ポリシーが使用できない場合のデフォルトの許可方式です。

このオプションでは、Tivoli Enterprise Portal ユーザー管理ダイアログを使用して、ダッシュボードの各ユーザーに対応する Tivoli Enterprise Portal ユーザーを作成します。同じダイアログを使用して、イベントを表示する許可をユーザーに付与し、表示できる 1 つ以上のモニター対象アプリケーションをそのユーザーに割り当てることができます。この手順は **tacmd** CLI を使用して実行することもできます。

Tivoli Enterprise Portal 許可の細分度は、許可ポリシーよりも低くなります。許可ポリシーでは特定の管理対象システムまたは特定の管理対象システム・グループに属する管理対象システムのみを表示する許可をダッシュボード・ユーザーに付与できますが、Tivoli Enterprise Portal 許可はモニター・アプリケーション・レベルです。つまり、特定のエージェント・アプリケーション・タイプ (例えば、すべての Windows OS エージェント) の管理対象システムをすべて表示する許可がユーザーに割り当てられます。

許可ポリシーは、モニター・ダッシュボードでアクセスできるモニター対象リソースのみを制御します。ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントも使用する場合は、ポータル・クライアントでアクセスできるモニター対象リソースは、Tivoli Enterprise Portal の許可とエージェント・アプリケーション割り当てによって制御されます。ユーザーがダッシュボードで表示できるモニター対象リソースのセットが、Tivoli Enterprise Portal クライアントで表示できるモニター対象リソースとは異なることがあります。これは、許可が矛盾している場合や、許可ポリシーがより限定的である場合に発生します。

より限定的な許可ポリシーの例

許可ポリシーにより、Dashboard Application Services Hub で Windows OS エージェントのサブセットを表示する許可がユーザーに付与されており、かつこのユーザーには Tivoli Enterprise Portal 許可で Windows OS アプリケーション・タイプが割り当てられているとします。このシナリオの場合、ダッシュボードでは、このユーザーに対し許可されている Windows OS エージェントのみが表示されますが、Tivoli Enterprise Portal クライアントにアクセスすると、すべての Windows OS エージェントが表示されます。

矛盾する許可の例

ユーザーに対し、許可ポリシーにより Dashboard Application Services Hubで Windows OS エージェントのサブセットを表示する許可が付与されているが、Tivoli Enterprise Portal 許可ではそのユーザーに対し Windows OS アプリケーション・タイプが割り当てられていないとします。このシナリオの場合、ダッシュボードでは、このユーザーに対し許可されている Windows OS エージェントが表示されますが、Tivoli Enterprise Portal クライアントにアクセスすると、Windows OS エージェントは表示されません。

モニターおよびダッシュボード環境を初めてセットアップする場合のベスト・プラクティスは、最初に Tivoli Enterprise Portal 許可とモニター対象アプリケーションの割り当てを行うことです。許可ポリシーの使用を開始する場合は、Dashboard Application Services Hub にモニター・データが表示され、管理者が許可ポリシーを作成した後で、ポータル・サーバーを再構成します。

注: Tivoli Enterprise Portal の許可と許可ポリシーは、ダッシュボードでのモニター対象リソースへのアクセスを制御するだけです。Tivoli Common Reporting を使用してレポートに表示されるモニター対象リソースへのアクセスは制御しません。

前提条件

- 「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の手順に従って基本 IBM Tivoli Monitoring モニター・サーバー、ポータル・サーバー、およびポータル・クライアント・コンポーネントをインストールして構成します。ポータル・サーバーを構成するときは、ダッシュボード・データ・プロバイダーを有効にします。
- モニター・ダッシュボードにデータが表示されるモニター・エージェントをインストールおよび構成します。、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の手順に従って、モニター・サーバー、ポータル・サーバー、およびデスクトップ・ポータル・クライアント (デスクトップ・ポータル・クライアントを使用する場合) にそのアプリケーション・サポートをインストールします。
- Dashboard Application Services Hub とダッシュボード・モニター・アプリケーションをインストールして構成します。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ダッシュボード環境のソフトウェア要件およびメモリー所要量』を参照してください。そのダッシュボード・アプリケーションをインストールする場合は、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『IBM Infrastructure Management Dashboards for Servers のインストールおよび構成』も参照してください。
- ダッシュボード・ユーザーに対して許可ポリシーと Tivoli Enterprise Portal 許可のいずれを使用するかを決定します。許可ポリシーを使用する場合は、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Authorization Policy Server および Authorization Policy コマンド行インターフェースのインストールおよび構成』の説明に従って、Tivoli 許可ポリシー・サーバーおよび許可ポリシーの tivcmd コマンド行インターフェース・コンポーネントをインストールして構成します。

ロードマップ

開始にあたって役立つロードマップを以下に示します。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ

ステップ	説明	情報の入手先
1 (必須)	Dashboard Application Services Hub およびポータル・サーバーのユーザーを認証する LDAP サーバー (Tivoli Directory Server や Microsoft Active Directory など) をセットアップし、ユーザーをそのレジストリーに追加します。	101 ページの『ポータル・サーバー上で LDAP 認証を構成するための前提条件』を参照してから、LDAP サーバーのドキュメントを参照してください。
2 (必須)	ポータル・サーバーと Dashboard Application Services Hub で時刻が UTC に同期されていることを確認します。	シングル・サインオンを使用するための情報と計画上の考慮事項について詳しくは、104 ページの『シングル・サインオンについて』を参照してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
3 (必須)	IBM Dashboard Application Services Hub の WebSphere® 管理者コンソールを使用して、LDAP ユーザー・レジストリーを使用してユーザーを認証し、シングル・サインオンを有効にするように Dashboard Application Services Hub アプリケーション・サーバーを構成します。 **注:** 構成時に、レルム名とドメイン名を指定します。ポータル・サーバー、およびポータル・サーバーまたはダッシュボード・サーバーでシングル・サインオンを実行するその他のアプリケーションを構成するときは、これらと同じ値を指定する必要があります。 • ドメイン名は、SSO が構成されているインターネット・ドメインまたはイントラネット・ドメイン (mycompany.com など) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。 • レルムは、ポータル・サーバーおよびその他のアプリケーション・サーバーによって使用される一連の統合リポジトリーを識別します。独自のレルム名を選択できますが、この値は、指定したドメイン内で SSO に対して構成されるすべてのアプリケーションで同じである必要があります。	中央ユーザー・レジストリーを使用するように Jazz for Service Management を構成する方法、SSO を構成する方法、LTPA トークンのタイムアウト値を構成する方法、LDAP サーバーへの TLS/SSL 接続を構成する方法については、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) の「*Jazz for Service Management 構成ガイド*」を参照してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
4 (必須)	LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成し、シングル・サインオンに使用するレルム名とドメインを指定します。 LDAP を使用するようにポータル・サーバーを構成するには、次のオプションを使用できます。 • IBM Tivoli Enterprise Monitoring Services の管理 ユーティリティー • Linux および UNIX の **itmcmd** コマンド行インターフェース • TEPS/e 管理コンソール IBM Tivoli Enterprise Monitoring Services の管理または **itmcmd** コマンドのいずれかを使用して、ポータル・サーバーに対する LDAP ユーザー検証を使用可能にします。また、これらのユーティリティーを使用して LDAP 接続パラメーターを構成することもできます。ただし、以下の場合を除きます。 • Microsoft Active Directory または Tivoli Directory Server 以外のサーバーを使用したい • ポータル・サーバーおよび LDAP サーバー間の TLS/SSL を構成したい • 拡張 LDAP 構成パラメーターを指定する必要がある これらのシナリオでは、ポータル・サーバーの構成時にタイプとして「**その他**」を指定し、その後 TEPS/e 管理コンソールを使用して LDAP 接続構成を完了します。 **注:** また、LDAP ユーザー認証の構成時にポータル・サーバーの LTPA キーのエクスポートまたは他のアプリケーションからの LTPA キーのインポートを実行することができます。これらのステップは、ポータル・サーバーの LDAP 認証が機能していることを確認してから実行することもできます。	以下のいずれかのトピックの説明に従って、ポータル・サーバーで LDAP ユーザーの検証を有効にします。 • 110 ページの『Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する』 • 115 ページの『Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する』 ポータル・サーバーの LDAP ユーザー検証を使用可能するときに、LDAP サーバー・タイプに「**その他**」を指定した場合は、この後 117 ページの『TEPS/e 管理コンソールの使用』の説明に従います。 **使用上の注意:** Microsoft Active Directory を使用している場合は、 135 ページの『Microsoft Active Directory を使用した LDAP ユーザー認証』を参照して、このタイプの LDAP サーバーに固有の計画情報と構成情報を確認してください。 Tivoli Directory Server を使用している場合は、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) の『Understanding single sign-on between IBM Tivoli Monitoring and Tivoli Integrated Portal using Tivoli Directory Server』を参照してください。これらの手順では、Tivoli Directory Server で構成されたエントリーを、TEPS/e 管理コンソールを使用して構成された情報にマップする方法を説明しています。 Tivoli Integrated Portal のためのステップは無視してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
5 (必須)	Tivoli Enterprise Portal クライアントに sysadmin としてログインし、sysadmin 以外の既存の Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップします。 sysadmin 以外の Tivoli Enterprise Portal ユーザー ID がない場合は、少なくとも 1 つの LDAP ユーザーの Tivoli Enterprise Portal ユーザー ID を作成します。ユーザー ID の作成時に、ユーザーの LDAP 識別名を入力します。 後で行うタスクでは、モニター・ダッシュボードにデータを表示できることを検証するため、LDAP ユーザーの 1 つを使用してログインします。Tivoli Enterprise Portal クライアントを使用して、ダッシュボードに表示されるモニター・アプリケーションと、イベントを表示する許可 (ダッシュボードにシチュエーション・イベント・データが表示される場合) をこのユーザーに割り当てます。	既存の Tivoli Enterprise Portal ユーザーがいる場合は、 125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』を参照してください。 新しい Tivoli Enterprise Portal ユーザー ID を作成する必要がある場合は、 180 ページの『ユーザー ID の追加』を参照してください。 Tivoli Enterprise Portal ユーザーへのモニター・アプリケーションと許可の割り当ての詳細については、 173 ページの『ユーザー管理』を参照してください。 Dashboard Application Services Hub とポータル・サーバーが同じコンピューター上に存在する場合は、 127 ページの『SSO 用ブラウザー・クライアントの再構成』を参照してください。
6 (オプションのベスト・プラクティス)	Tivoli Enterprise Portal ユーザー ID にマップされている LDAP ユーザーとして Tivoli Enterprise Portal クライアントにログインできることを確認します。	N/A
7 (オプションのベスト・プラクティス)	ポータル・サーバーと LDAP サーバーの間の通信をセキュリティーで保護する場合は、TLS/SSL 接続を構成します。	123 ページの『ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』
8 (オプションのベスト・プラクティス)	Tivoli Enterprise Portal ユーザー ID にマップされている LDAP ユーザーとして Tivoli Enterprise Portal クライアントにログインできることを確認します。	N/A

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
9 (必須)	以下のアプリケーションがポータル・サーバーと同じ LTPA キーを使用していることを確認する必要があります。 • Tivoli Enterprise Portal を起動する Web ベースまたは Web 対応のアプリケーション • Tivoli Enterprise Portal クライアントから起動できる Web ベースまたは Web 対応のアプリケーション • IBM Dashboard Application Services Hub • Tivoli Integrated Portal のように IBM Tivoli Monitoring グラフ Web サービスを使用する他のアプリケーション 他のすべての関連 SSO アプリケーションで使用する LTPA キーのソースになるアプリケーションを判断し、その LTPA キーをエクスポートします。キー・ファイルとキーの暗号化に使用するパスワードは、他の関連アプリケーションの管理者に提供する必要があります。	ポータル・サーバーが LTPA キーのソースになると判断した場合は、128 ページの『LTPA キーのインポートおよびエクスポート』のエクスポートの指示に従って、その LTPA キーをエクスポートします。 IBM Dashboard Application Services Hub が LTPA キーのソースになる場合は、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) の「*Jazz for Service Management 構成ガイド*」の『LTPA キーのエクスポート (Exporting LTPA keys)』を参照してください。 それ以外の場合は、LTPA キーをエクスポートするアプリケーションのドキュメントを参照して、エクスポート操作の実行方法を判断してください。
10 (必須)	他の関連 SSO アプリケーションの管理者は、前のステップでエクスポートされた LTPA キーをインポートする必要があります。キー・ファイルとキーの暗号化に使用されたパスワードが必要です。	LTPA キーをポータル・サーバーにインポートするには、128 ページの『LTPA キーのインポートおよびエクスポート』のインポートに関する説明を参照してください。 LTPA キーを IBM Dashboard Application Services Hub にインポートするには、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management 構成ガイド*」の『LTPA 鍵のインポート』を参照してください。 LTPA キーのインポート方法について詳しくは、他の関連 SSO アプリケーションの資料を参照してください。
11 (必須)	ダッシュボード・ハブ管理ユーザーでもある LDAP ユーザーとして IBM Dashboard Application Services Hub にログインし、ダッシュボード・データ・プロバイダー接続を作成します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
12 (必須)	IBM Dashboard Application Services Hub に管理ユーザーとしてログインし、ダッシュボード・アプリケーション・ページへのアクセスを制御する役割を作成し、ダッシュボードのユーザーまたはユーザー・グループをこの役割に割り当てます。 **注:** IBM Infrastructure Management for VMware などの一部のダッシュボード・アプリケーションでは、ダッシュボード・アプリケーションのインストール時にそのページの役割が自動的に作成されます。しかし、IBM Infrastructure Management Dashboards for Servers などのその他のアプリケーションではインストール時に役割が作成されないため、役割を作成するか、または既存の役割にダッシュボード・ページを割り当てる必要があります。	ダッシュボード・ページへのアクセスを制御する役割の使用法について詳しくは、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。
13 (オプションのベスト・プラクティス)	イベントを表示する許可とモニター・アプリケーションが割り当てられている Tivoli Enterprise Portal ユーザー ID を持ち、ダッシュボード・ページを表示する許可がある LDAP ユーザーとして、IBM Dashboard Application Services Hub にログインします。次にダッシュボード・アプリケーションを起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、「**システム状況および正常性**」 > 「**ダッシュボード・ヘルス・チェック**」を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、「**システム状況および正常性**」 >を選択し、「**サーバー・ダッシュボード**」を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
14 (オプションのベスト・プラクティス)	Dashboard Application Services Hub とダッシュボード・データ・プロバイダーの間で HTTPS を使用する場合は、以下のタスクを実行します。	
	1. ダッシュボード・ハブとデータ・プロバイダーの間で TLS/SSL を構成します。	231 ページの『Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成』
	2. `administrator` 役割と `iscadmins` 役割が割り当てられている管理ユーザーとして IBM Dashboard Application Services Hub にログインし、以前に作成したダッシュボード・データ・プロバイダー接続を削除します。	データ・プロバイダー接続の操作方法については、IBM Dashboard Application Services Hub オンライン・ヘルプおよび Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Integration Guide*」を参照してください。
	3. IBM Dashboard Application Services Hub に管理ユーザーとしてログオンしたままの状態で、接続を再作成し、プロトコルとして HTTPS を指定します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択してください。
	4. ダッシュボード・ページを表示する許可を持つユーザーとして IBM Dashboard Application Services Hub にログインし、ダッシュボード・アプリケーションを再び起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」**を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」**を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

表 3. ロードマップ: シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ (続き)

ステップ	説明	情報の入手先
15 (オプション)	許可ポリシーを使用する場合は、以下のタスクを実行します。	
	1. **tivcmd** CLI を使用して、許可ポリシーの管理者の割り当て、ユーザーへの許可ポリシー配布許可の割り当て、ダッシュボード・ユーザーがアクセスできるモニター対象リソースを制御する許可ポリシーの作成を行います。 **注: tivcmd** CLI を使用して許可ポリシー・サーバーにログインできることを確認したら、**tivcmd** CLI と許可ポリシー・サーバーの間で TLS/SSL を構成し、後続のコマンドが保護されるようにします。	201 ページの『許可ポリシーを有効にする準備』 および 235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』
	2. ポータル・サーバーで許可ポリシー検査を使用可能にします。 **注:** このタスクを実行すると、許可ポリシー役割が割り当てられているダッシュボード・ユーザーのみが、ダッシュボードでモニター対象リソースを表示できるようになります。	210 ページの『ポータル・サーバーでの許可ポリシーの使用可能化』
	3. ダッシュボード・ページに表示できる管理対象システムまたは管理対象システム・グループの属性グループ・データ、シチュエーション・イベント・データ、またはこの両方を表示する許可をユーザーに付与する許可ポリシー役割が 1 つ以上割り当てられており、ダッシュボード・ページを表示する許可がある LDAP ユーザーとして、IBM Dashboard Application Services Hub にログインします。 ダッシュボード・ページを起動し、ユーザーに対して表示が許可されているモニター対象リソースのみが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」** を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」** を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。
	4. 許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub から許可ポリシーを取得するときに TLS/SSL を使用するように、ポータル・サーバーを構成します。	235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』

拡張ダッシュボード・モニター環境のセットアップが完了した後で、場合によっては以下のタスクも行う必要があります。

表 4. シングル・サインオンおよびユーザーごとの許可による制御を使用する拡張モニター環境のセットアップに必要な追加タスク

タスク	情報の入手先
ダッシュボード・ユーザーがモニターするイベントのシチュエーション定義を作成します。	シチュエーションを処理するために使用する **tacmd** コマンドについては、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」のイベント・モニターのシチュエーションと「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。
ダッシュボード・ページに表示する管理対象システムをグループ化するための管理対象システム・グループを作成します。	システム・リストを処理するために使用する **tacmd** コマンドについては、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」の環境の管理と「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。
ダッシュボード・ページにヒストリカル・データを表示する場合は、ヒストリカル・データ収集を構成します。 **注:** 一部のモニター・ダッシュボード・アプリケーションでは Tivoli Data Warehouse からのヒストリカル・データの取得がサポートされていません。	509 ページの『第 17 章 ヒストリカル・データの管理』
新しいダッシュボード・ユーザーごとに、以下の操作を行います。 使用するダッシュボード・ページにアクセスする許可がダッシュボード・ユーザーに付与されていることを確認します。 Dashboard Application Services Hub 役割に割り当てられている既存の LDAP グループにユーザーを追加できるかどうかを確認します。ユーザーを割り当てることができる既存の LDAP グループがない場合は、次のいずれかのタスクを実行します。 • ベスト・プラクティスは、LDAP グループを新規に作成してそのグループにユーザーを追加してから、適切なダッシュボード・ページを表示できる許可を持つ Dashboard Application Services Hub 役割にグループを追加することです。 または • 適切なダッシュボード・ページを表示できる許可を持つ Dashboard Application Services Hub 役割にダッシュボード・ユーザーを直接割り当てます。	ダッシュボード・ページへのアクセスを制御する役割の使用法について詳しくは、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。 LDAP グループへのユーザーの追加について詳しくは、LDAP サーバーの資料を参照してください。

表 4. シングル・サインオンおよびユーザーごとの許可による制御を使用する拡張モニター環境のセットアップに必要な追加タスク (続き)

タスク	情報の入手先
新しいダッシュボード・ユーザーごとに、以下の操作を行います。 許可ポリシーを使用している場合は、ダッシュボード・ユーザーがモニターする管理対象システムまたは管理対象システム・グループの属性グループ・データ、シチュエーション・イベント・データ、またはこの両方を表示できる許可をユーザーに付与する 1 つ以上の許可ポリシー役割に、ダッシュボード・ユーザーが割り当てられていることを確認します。必要な許可を持つ許可ポリシー役割が既に割り当てられている既存の LDAP グループにユーザーを追加できるかどうかを確認します。ユーザーを既存の LDAP グループに追加できない場合は、次のいずれかのタスクを実行します。 • ベスト・プラクティスは、LDAP グループを新規に作成し、ユーザーをそのグループに追加し、そのグループを許可ポリシー役割に割り当てることです。 または • ダッシュボード・ユーザーを許可ポリシー役割に直接割り当てます。	LDAP グループへのユーザーの追加について詳しくは、LDAP サーバーの資料を参照してください。 許可ポリシーの作成と操作について詳しくは、 202 ページの『ポリシー管理のシナリオ』と「*IBM Tivoli Monitoring コマンド・リファレンス*」の **tivcmd** CLI に関する章を参照してください。

表 4. シングル・サインオンおよびユーザーごとの許可による制御を使用する拡張モニター環境のセットアップに必要な追加タスク (続き)

タスク	情報の入手先
新しいダッシュボード・ユーザーごとに、以下の操作を行います。 Tivoli Enterprise Portal の許可を使用してダッシュボードでアクセスできるモニター対象リソースを制御している場合、または新規ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントを使用する場合は、Tivoli Enterprise Portal ユーザーに正しい許可が設定されていることを確認します。 最初に、ダッシュボード・ユーザーの LDAP 識別名にマップされている Tivoli Enterprise Portal ユーザー ID があることを確認します。 次に、新規ダッシュボード・ユーザーに必要な許可とモニター・アプリケーションが割り当てられている既存の Tivoli Enterprise Portal グループに Tivoli Enterprise Portal ユーザーを割り当てるかどうかを確認します。使用できる既存のグループがない場合は、次のいずれかのタスクを実行します。 • ベスト・プラクティスは、Tivoli Enterprise Portal グループを新規に作成し、そのグループにユーザーを追加し、そのグループに適切な許可とアプリケーション・タイプを割り当てることです。 • Tivoli Enterprise Portal ユーザーに適切な許可とモニター・アプリケーションを直接割り当てます。 ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントを使用しない場合、このダッシュボード・ユーザーには、イベント表示許可のみが必要であり、これらのユーザーがダッシュボード・ページでモニターするモニター・アプリケーションが割り当てられている必要があります例えばダッシュボード・ユーザーが Infrastructure Management Dashboards for Servers を使用する場合は、アプリケーション・タイプとして Linux OS、UNIX OS、または Windows OS のいずれか 1 つ以上が割り当てられている必要があります。 ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントも使用する場合は、追加の許可が必要となります。	新規 Tivoli Enterprise Portal ユーザー ID の作成について詳しくは、 180 ページの『ユーザー ID の管理』を参照してください。 Tivoli Enterprise Portal ユーザー ID のグループへの追加について詳しくは、 184 ページの『ユーザー・グループの管理』を参照してください。 Tivoli Enterprise Portal ユーザーおよびグループへのモニター・アプリケーションと許可の割り当てについて詳しくは、173 ページの『ユーザー管理』を参照してください。
カスタム・ダッシュボード・ページを作成し、カスタム・ページを表示する許可を持つ Dashboard Application Services Hub の役割がダッシュボード・ユーザーに割り当てられていることを確認します。	63 ページの『モニター・データを表示するカスタム・ダッシュボード・ページの作成』

表 4. シングル・サインオンおよびユーザーごとの許可による制御を使用する拡張モニター環境のセットアップに必要な追加タスク (続き)

タスク	情報の入手先
Dashboard Application Services Hub に新しいモニター・ダッシュボード・アプリケーションをインストールし、ダッシュボードのページを新規または既存の役割に割り当て、ページへのアクセスを制御するその役割に LDAP ユーザーまたはユーザー・グループを割り当てます。 **注:** 一部のダッシュボード・アプリケーションでは、ダッシュボード・アプリケーションのインストール時にそのページの役割が自動的に作成されます。 許可ポリシーを使用している場合は、ダッシュボード・ユーザーが新しいダッシュボード・アプリケーションを使用してモニターする管理対象システムまたは管理対象システム・グループの属性グループ・データ、シチュエーション・イベント・データ、またはこの両方を表示できる許可をユーザーに付与する 1 つ以上の許可ポリシー役割に、新しいページへのアクセス権限を持つダッシュボード・ユーザーが割り当てられていることを確認します。 ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントも使用する場合、または許可ポリシーの代わりに Tivoli Enterprise Portal の許可を使用している場合は、ダッシュボード・ユーザーの Tivoli Enterprise Portal ユーザー ID を割り当てるか、新しいダッシュボード・アプリケーションに表示されるモニター・アプリケーションをグループ化します。 **注:** 新しいダッシュボードにエージェントのデータを表示するには、エージェントのアプリケーション・サポートをポータル・サーバーとモニター・サーバーにインストールする必要があります。アプリケーション・サポートが自己記述型エージェント機能を使用してインストールされている場合は、ポータル・サーバーを再始動して、ダッシュボード・データ・プロバイダーが新しいサポート・パッケージを使用できるようにする必要があります。	ダッシュボード・アプリケーションのインストール資料の指示に従います。 その後、ダッシュボード・ページへのアクセスを制御する役割の使用法の詳細について、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。 許可ポリシーの作成と操作について詳しくは、 195 ページの『第 7 章 役割ベースの許可ポリシーの使用』と「*IBM Tivoli Monitoring コマンド・リファレンス*」の **tivcmd** CLI に関する章を参照してください。 また、Tivoli Enterprise Portal ユーザーへのエージェント・アプリケーションの割り当て方法の詳細を 173 ページの『ユーザー管理』で参照してください。 「*IBM Tivoli Monitoring インストールおよび設定ガイド*」には、アプリケーション・サポートのインストール手順が記載されています。
UISolutions のインポートを制御するかどうかを判断します (新規および更新されたダッシュボード・アプリケーションが UISolutions 定義を ダッシュボード・データ・プロバイダー に自動的にインポートします)。	65 ページの『UISolutions のインポートの制御』

基本モニター・ダッシュボード環境から、シングル・サインオンおよびユーザーごとの許可による制御を使用するダッシュボード環境への移行

基本ダッシュボード環境から高度なダッシュボード環境に移行します。

31 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ』の説明に従って基本モニター環境を設定した後、シングル・サインオンを使用する高度なダッシュボード環境に移行できます。

ロードマップ

開始にあたって役立つロードマップを以下に示します。

表 5. 高度なダッシュボード環境に移行するためのロードマップ

ステップ	説明	情報の入手先
1 (必須)	Dashboard Application Services Hub およびポータル・サーバーのユーザーを認証する LDAP サーバー (Tivoli Directory Server や Microsoft Active Directory など) をセットアップし、ユーザーをそのレジストリーに追加します。	101 ページの『ポータル・サーバー上で LDAP 認証を構成するための前提条件』を参照してから、LDAP サーバーのドキュメントを参照してください。
2 (必須)	ポータル・サーバーと Dashboard Application Services Hub で時刻が UTC に同期されていることを確認します。	シングル・サインオンを使用するための情報と計画上の考慮事項について詳しくは、 104 ページの『シングル・サインオンについて』を参照してください。
3 (必須)	IBM Dashboard Application Services Hub の WebSphere 管理者コンソールを使用して、LDAP ユーザー・レジストリーを使用してユーザーを認証し、シングル・サインオンを有効にするように Dashboard Application Services Hub アプリケーション・サーバーを構成します。 **注:** 構成時に、レルム名とドメイン名を指定します。ポータル・サーバー、およびポータル・サーバーまたはダッシュボード・サーバーでシングル・サインオンを実行するその他のアプリケーションを構成するときは、これらと同じ値を指定する必要があります。 • ドメイン名は、SSO が構成されているインターネット・ドメインまたはイントラネット・ドメイン (mycompany.com など) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。 • レルムは、ポータル・サーバーおよびその他のアプリケーション・サーバーによって使用される一連の統合リポジトリーを識別します。独自のレルム名を選択できますが、この値は、指定したドメイン内で SSO に対して構成されるすべてのアプリケーションで同じである必要があります。	中央ユーザー・レジストリーを使用するように Jazz for Service Management を構成する方法、SSO を構成する方法、LTPA トークンのタイムアウト値を構成する方法、LDAP サーバーへの TLS/SSL 接続を構成する方法については、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) の「*Jazz for Service Management 構成ガイド*」を参照してください。

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
4 (必須)	LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成し、シングル・サインオンに使用するレルム名とドメインを指定します。 LDAP を使用するようにポータル・サーバーを構成するには、次のオプションを使用できます。 • IBM Tivoli Enterprise Monitoring Services の管理 ユーティリティー • Linux および UNIX の **itmcmd** コマンド行インターフェース • TEPS/e 管理コンソール IBM Tivoli Enterprise Monitoring Services の管理または **itmcmd** コマンドのいずれかを使用して、ポータル・サーバーに対する LDAP ユーザー検証を使用可能にします。また、これらのユーティリティーを使用して LDAP 接続パラメーターを構成することもできます。ただし、以下の場合を除きます。 • Microsoft Active Directory または Tivoli Directory Server 以外のサーバーを使用したい • ポータル・サーバーおよび LDAP サーバー間の TLS/SSL を構成したい • 拡張 LDAP 構成パラメーターを指定する必要がある これらのシナリオでは、ポータル・サーバーの構成時にタイプとして「**その他**」を指定し、その後 TEPS/e 管理コンソールを使用して LDAP 接続構成を完了します。 **注:** また、LDAP ユーザー認証の構成時にポータル・サーバーの LTPA キーのエクスポートまたは他のアプリケーションからの LTPA キーのインポートを実行することができます。これらのステップは、ポータル・サーバーの LDAP 認証が機能していることを確認してから実行することもできます。	以下のいずれかのトピックの説明に従って、ポータル・サーバーで LDAP ユーザーの検証を有効にします。 • 110 ページの『Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する』 • 115 ページの『Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する』 ポータル・サーバーの LDAP ユーザー検証を使用可能するときに、LDAP サーバー・タイプに「**その他**」を指定した場合は、この後 117 ページの『TEPS/e 管理コンソールの使用』の説明に従います。 **使用上の注意:** Microsoft Active Directory を使用している場合は、 135 ページの『Microsoft Active Directory を使用した LDAP ユーザー認証』を参照して、このタイプの LDAP サーバーに固有の計画情報と構成情報を確認してください。 Tivoli Directory Server を使用している場合は、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) の『Understanding single sign-on between IBM Tivoli Monitoring and Tivoli Integrated Portal using Tivoli Directory Server』を参照してください。これらの手順では、Tivoli Directory Server で構成されたエントリーを、TEPS/e 管理コンソールを使用して構成された情報にマップする方法を説明しています。 Tivoli Integrated Portal のためのステップは無視してください。

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
5 (必須)	Tivoli Enterprise Portal クライアントに sysadmin としてログインし、sysadmin 以外の既存の Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップします。 sysadmin 以外の Tivoli Enterprise Portal ユーザー ID がない場合は、少なくとも 1 つの LDAP ユーザーの Tivoli Enterprise Portal ユーザー ID を作成します。ユーザー ID の作成時に、ユーザーの LDAP 識別名を入力します。 後で行うタスクでは、モニター・ダッシュボードにデータを表示できることを検証するため、LDAP ユーザーの 1 つを使用してログインします。Tivoli Enterprise Portal クライアントを使用して、ダッシュボードに表示されるモニター・アプリケーションと、イベントを表示する許可 (ダッシュボードにシチュエーション・イベント・データが表示される場合) をこのユーザーに割り当てます。	既存の Tivoli Enterprise Portal ユーザーがいる場合は、 125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』を参照してください。 新しい Tivoli Enterprise Portal ユーザー ID を作成する必要がある場合は、 180 ページの『ユーザー ID の追加』を参照してください。 Tivoli Enterprise Portal ユーザーへのモニター・アプリケーションと許可の割り当ての詳細については、 173 ページの『ユーザー管理』を参照してください。 Dashboard Application Services Hub とポータル・サーバーが同じコンピューター上に存在する場合は、 127 ページの『SSO 用ブラウザー・クライアントの再構成』を参照してください。
6 (オプションのベスト・プラクティス)	Tivoli Enterprise Portal ユーザー ID にマップされている LDAP ユーザーとして Tivoli Enterprise Portal クライアントにログインできることを確認します。	N/A
7 (オプションのベスト・プラクティス)	ポータル・サーバーと LDAP サーバーの間の通信をセキュリティーで保護する場合は、TLS/SSL 接続を構成します。	123 ページの『ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』
8 (オプションのベスト・プラクティス)	Tivoli Enterprise Portal ユーザー ID にマップされている LDAP ユーザーとして Tivoli Enterprise Portal クライアントにログインできることを確認します。	N/A

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
9 (必須)	以下のアプリケーションがポータル・サーバーと同じ LTPA キーを使用していることを確認する必要があります。 • Tivoli Enterprise Portal を起動する Web ベースまたは Web 対応のアプリケーション • Tivoli Enterprise Portal クライアントから起動できる Web ベースまたは Web 対応のアプリケーション • IBM Dashboard Application Services Hub • Tivoli Integrated Portal のように IBM Tivoli Monitoring グラフ Web サービスを使用する他のアプリケーション 他のすべての関連 SSO アプリケーションで使用する LTPA キーのソースになるアプリケーションを判断し、その LTPA キーをエクスポートします。キー・ファイルとキーの暗号化に使用するパスワードは、他の関連アプリケーションの管理者に提供する必要があります。	ポータル・サーバーが LTPA キーのソースになると判断した場合は、 128 ページの『LTPA キーのインポートおよびエクスポート』のエクスポートの指示に従って、その LTPA キーをエクスポートします。 IBM Dashboard Application Services Hub が LTPA キーのソースになる場合は、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html) の「*Jazz for Service Management 構成ガイド*」の『LTPA キーのエクスポート (Exporting LTPA keys)』を参照してください。 それ以外の場合は、LTPA キーをエクスポートするアプリケーションのドキュメントを参照して、エクスポート操作の実行方法を判断してください。
10 (必須)	他の関連 SSO アプリケーションの管理者は、前のステップでエクスポートされた LTPA キーをインポートする必要があります。キー・ファイルとキーの暗号化に使用されたパスワードが必要です。	LTPA キーをポータル・サーバーにインポートするには、 128 ページの『LTPA キーのインポートおよびエクスポート』のインポートに関する説明を参照してください。 LTPA キーを IBM Dashboard Application Services Hub にインポートするには、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management 構成ガイド*」の『LTPA 鍵のインポート』を参照してください。 LTPA キーのインポート方法について詳しくは、他の関連 SSO アプリケーションの資料を参照してください。
11 (必須)	ダッシュボード・ハブ管理ユーザーでもある LDAP ユーザーとして IBM Dashboard Application Services Hub にログインし、既存のダッシュボード・データ・プロバイダー接続を**削除**します。次に、シングル・サインオンをサポートするダッシュボード・データ・プロバイダー接続を**新規作成**します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択してください。

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
12 (オプションのベスト・プラクティス)	イベントを表示する許可とモニター・アプリケーションが割り当てられている Tivoli Enterprise Portal ユーザー ID を持ち、ダッシュボード・ページを表示する許可がある LDAP ユーザーとして、IBM Dashboard Application Services Hub にログインします。次にダッシュボード・アプリケーションを起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」** を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」** を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
13 (オプションのベスト・プラクティス)	Dashboard Application Services Hub とダッシュボード・データ・プロバイダーの間に HTTPS をまだ構成**していない**場合は、以下のタスクを実行します。	
	1. ダッシュボード・ハブとデータ・プロバイダーの間で TLS/SSL を構成します。	231 ページの『Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成』
	2. `administrator` 役割と `iscadmins` 役割が割り当てられている管理ユーザーとして IBM Dashboard Application Services Hub にログインし、以前に作成したダッシュボード・データ・プロバイダー接続を削除します。	データ・プロバイダー接続の操作方法については、IBM Dashboard Application Services Hub オンライン・ヘルプおよび Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Integration Guide*」を参照してください。
	3. IBM Dashboard Application Services Hub に管理ユーザーとしてログオンしたままの状態で、接続を再作成し、プロトコルとして HTTPS を指定します。	60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』 接続を作成するときには、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」ボックスを選択してください。
	4. ダッシュボード・ページを表示する許可を持つユーザーとして IBM Dashboard Application Services Hub にログインし、ダッシュボード・アプリケーションを再び起動し、データが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」**を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」**を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
14 (オプション)	Tivoli Enterprise Portal の許可とモニター・アプリケーションの割り当てではなく、役割ベースの制御を行う場合は、許可ポリシーを作成し、許可ポリシーのチェックを有効にします。	
	1. **tivcmd** CLI を使用して、許可ポリシーの管理者の割り当て、ユーザーへの許可ポリシー配布許可の割り当て、ダッシュボード・ユーザーがアクセスできるモニター対象リソースを制御する許可ポリシーの作成を行います。 **注: tivcmd** CLI を使用して許可ポリシー・サーバーにログインできることを確認したら、**tivcmd** CLI と許可ポリシー・サーバーの間で TLS/SSL を構成し、後続のコマンドが保護されるようにします。	201 ページの『許可ポリシーを有効にする準備』 および 235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』
	2. ポータル・サーバーで許可ポリシー検査を使用可能にします。 **注:** このタスクを実行すると、許可ポリシー役割が割り当てられているダッシュボード・ユーザーのみが、ダッシュボードでモニター対象リソースを表示できるようになります。	210 ページの『ポータル・サーバーでの許可ポリシーの使用可能化』
	3. ダッシュボード・ページに表示できる管理対象システムまたは管理対象システム・グループの属性グループ・データ、シチュエーション・イベント・データ、またはこの両方を表示する許可をユーザーに付与する許可ポリシー役割が 1 つ以上割り当てられており、ダッシュボード・ページを表示する許可がある LDAP ユーザーとして、IBM Dashboard Application Services Hub にログインします。 ダッシュボード・ページを起動し、ユーザーに対して表示が許可されているモニター対象リソースのみが表示されることを確認します。	ダッシュボードの起動および使用方法の詳細については、ダッシュボード・アプリケーションのユーザー・ガイドを参照してください。 **ヒント:** 最初に、**「システム状況および正常性」** > **「ダッシュボード・ヘルス・チェック」** を選択して、環境が正しく動作していることを確認します。Infrastructure Management Dashboards for Servers を使用している場合は、**「システム状況および正常性」** >を選択し、**「サーバー・ダッシュボード」** を選択します。 Infrastructure Management Dashboards for Servers の使用について詳しくは、OS エージェントのユーザー・ガイドを参照してください。
	4. 許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub から許可ポリシーを取得するときに TLS/SSL を使用するように、ポータル・サーバーを構成します。	235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』

表 5. 高度なダッシュボード環境に移行するためのロードマップ (続き)

ステップ	説明	情報の入手先
15 (オプション)	新しいダッシュボード・ユーザーごとに、以下の操作を行います。 Tivoli Enterprise Portal の許可を使用してダッシュボードでアクセスできるモニター対象リソースを制御している場合、または新規ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントを使用する場合は、Tivoli Enterprise Portal ユーザーに正しい許可が設定されていることを確認します。 最初に、ダッシュボード・ユーザーの LDAP 識別名にマップされている Tivoli Enterprise Portal ユーザー ID があることを確認します。 次に、新規ダッシュボード・ユーザーに必要な許可とモニター・アプリケーションが割り当てられている既存の Tivoli Enterprise Portal グループに Tivoli Enterprise Portal ユーザーを割り当てるかどうかを確認します。使用できる既存のグループがない場合は、次のいずれかのタスクを実行します。 • ベスト・プラクティスは、Tivoli Enterprise Portal グループを新規に作成し、そのグループにユーザーを追加し、そのグループに適切な許可とアプリケーション・タイプを割り当てることです。 • Tivoli Enterprise Portal ユーザーに適切な許可とモニター・アプリケーションを直接割り当てます。 ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントを使用しない場合、このダッシュボード・ユーザーには、イベント表示許可のみが必要であり、これらのユーザーがダッシュボード・ページでモニターするモニター・アプリケーションが割り当てられている必要があります例えばダッシュボード・ユーザーが Infrastructure Management Dashboards for Servers を使用する場合は、アプリケーション・タイプとして Linux OS、UNIX OS、または Windows OS のいずれか 1 つ以上が割り当てられている必要があります。 ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントも使用する場合は、追加の許可が必要となります。	新規 Tivoli Enterprise Portal ユーザー ID の作成について詳しくは、 180 ページの『ユーザー ID の管理』を参照してください。 Tivoli Enterprise Portal ユーザー ID のグループへの追加について詳しくは、 184 ページの『ユーザー・グループの管理』を参照してください。 Tivoli Enterprise Portal ユーザーおよびグループへのモニター・アプリケーションと許可の割り当てについて詳しくは、 173 ページの『ユーザー管理』を参照してください。

IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成

IBM Dashboard Application Services Hub (IBM Infrastructure Management Dashboards for Servers や IBM Infrastructure Management Dashboards for VMware など) またはカスタム・ダッシュボードでモニター・ダッシュボード・アプリケーションからシチュエーション・イベントと管理対象システムに関するメトリックを取得するには、最初に Tivoli Enterprise Portal Server 上の IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーとの接続を確立する必要があります。

この接続手順は、ポータル・サーバーの構成が変更されていない場合には繰り返す必要はありません。

始める前に

接続は Dashboard Application Services Hub コンソールで定義します。接続を作成する前に、以下のステップが完了していることを確認してください。

- ポータル・サーバー構成でダッシュボード・データ・プロバイダーが使用可能であることを確認します。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ダッシュボード・データ・プロバイダーが使用可能であることの確認』を参照してください。

  IBM Tivoli Monitoring 環境がホット・スタンバイに対応して構成されている場合は、ダッシュボード・データ・プロバイダーに接続する前に、ポータル・サーバー構成でダッシュボード・データ・プロバイダーのドメイン・オーバーライド値を構成する必要があります。ドメイン・オーバーライド値により、ポータル・サーバーがスタンバイ・ハブ・モニター・サーバーに接続するように再構成されても、データ・プロバイダーの接続 ID は変更されません。
- Dashboard Application Services Hub の `administrator` 役割および `iscadmins` 役割が割り当てられているユーザーとして Dashboard Application Services Hub にログインする必要があります。これらの役割は、接続を作成および管理するために必要です。ユーザーへのこれらの役割の割り当てについては、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Administrator's Guide*」を参照してください。

  シングル・サインオンを使用する予定の場合は、接続の作成時に、ダッシュボード・ハブ・サーバーとポータル・サーバーにより共有される統合 LDAP ユーザー・レジストリーのメンバーであるユーザーとして Dashboard Application Services Hub にログインする必要もあります。シングル・サインオンを使用するデータ・プロバイダー接続の作成前に行う必要がある追加手順については、37 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ』を参照してください。
- ダッシュボード・データ・プロバイダーへの接続を定義するには、必要なネットワーク・プロトコル、ポータル・サーバーのホスト名とポート番号、ポータル・サーバーとの認証に使用する資格情報、およびシングル・サインオンを使用する必要があるかどうかが分かっている必要があります。
- プロトコル接続として HTTPS を使用する予定の場合は、データ・プロバイダー接続を作成する前に Dashboard Application Services Hub とポータル・サーバーの

間で TLS/SSL を構成する必要があります。詳しくは、231 ページの『Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成』を参照してください。

ヒント: 初期テストのために HTTP プロトコルを使用する接続を作成できます。ご使用の環境が動作したら、サーバー間で TLS/SSL を構成し、接続を削除し、HTTPS プロトコルを使用した接続を再び追加します。

手順

1. Dashboard Application Services Hub コンソールで 「**コンソール設定**」をクリックし、(「**一般**」の下の) 「**接続**」を選択します。
2. 「**新規リモート・プロバイダーの作成**」をクリックします。 ダッシュボード・データ・プロバイダーへの接続を指定するためのフィールドが表示されます。
3. 「**プロトコル**」フィールドで、ポータル・サーバー・コンピューターへの接続に使用するアプリケーション・プロトコルを選択します (HTTP、HTTPS-SSL (Secure Socket Layer)、または HTTPS-TLS (トランスポート層セキュリティー))。
4. 「**ホスト名**」フィールド内をクリックし、ポータル・サーバー・コンピューターの IP アドレスまたは完全修飾名を入力します。
5. 「**ポート**」フィールド内をクリックし、ポータル・サーバーの eWAS アプリケーションのポート番号 (HTTP の場合は 15200、HTTPS の場合は 15201) を入力します。
6. Dashboard Application Services Hub サーバーとポータル・サーバーの間にファイアウォールが導入されている構成の場合は、「**ファイアウォールを介して接続する (Connection goes through a firewall)**」チェック・ボックスを選択し、Dashboard Application Services Hub がインストールされているコンピューターの完全修飾ホスト名とポート番号 (デフォルトのポートは 16324) を入力します。
7. 「**名前**」フィールドに、ポータル・サーバーとの認証に使用できるユーザー名を入力し、「**パスワード**」フィールドにそのパスワードを入力します。

   シングル・サインオンおよびユーザーごとの許可を使用しない基本ダッシュボード環境をセットアップする場合は、31 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ』の 1 番目の表で説明した Tivoli Enterprise Portal 許可が付与されているユーザーを入力します。このユーザーは、接続を作成し、ダッシュボード・ユーザーに代わってダッシュボード・データ・プロバイダーに後続の要求をすべて送信するために作成されます。

   シングル・サインオンおよびユーザーごとの許可を使用するダッシュボード環境をセットアップする場合は、ユーザー名とパスワードを入力します。ユーザー名とパスワードは、ポータル・サーバーで使用可能なデータ・プロバイダーのリストを取得するよう求める要求をポータル・サーバーに送信するために使用されます。この時点以降に発行されるデータ・プロバイダーに対するすべての要求には、Dashboard Application Services Hub へログインしているユーザーの名前が組み込まれます。

8. 「**検索**」をクリックし、ポータル・サーバー・コンピューター上のデータ・プロバイダーを表に取り込みます。
9. ダッシュボード・データ・プロバイダーのラジオ・ボタンをクリックして選択し、その他のフィールドにデータを入力します。
10. 以下のフィールドの入力内容を編集します。
    - 「**名前**」は、元のデータ・プロバイダー名と同じです。このフィールドはそのままにしておくことができます。
    - 「**説明**」は、元のデータ・プロバイダーの説明と同じです。このフィールドはそのままにしておくことができます。
    - 「**プロバイダー ID**」は、デフォルトでは、最初はダッシュボード・データ・プロバイダー接続の `itm.`*`hub_monitoring_server_name`*`.`*`portal_server_host_name`* です。ポータル・サーバー構成でドメイン・オーバーライド値が構成された場合、元の ID ストリングの *hub_monitoring_server_name* 部分がオーバーライド値に置き換わります。

      以下のいずれかのアプリケーションを使用している場合は、「プロバイダー ID」を `ITMSD` に変更する必要があります。
      - IBM Tivoli Monitoring に含まれる IBM Infrastructure Management Dashboards for Servers
      - IBM Infrastructure Management Dashboards for VMware
      - IBM Infrastructure Management Capacity Planner for VMware
      - IBM Infrastructure Management Capacity Planner for PowerVM®

      上でリストされているダッシュボード・アプリケーションは使用しないが、他のモニター・エージェントのダッシュボード・アプリケーションをインストールしている場合は、該当するエージェントの資料を参照し、それらのダッシュボードで `ITMSD` を使用する必要があるかどうかを確認してください。上でリストされているダッシュボード・アプリケーションは使用していないが将来使用する可能性がある場合、または使用する「プロバイダー ID」がわからない場合は、`ITMSD` を使用するのがベスト・プラクティスです。
11. シングル・サインオンおよびユーザーごとの許可を使用するダッシュボード環境をセットアップする場合は、「**ユーザーの資格情報を使用する (SSO 構成が必要)**」チェック・ボックスを選択します。このオプションにチェック・マークが付いている場合、モニター・データの取得時に、ダッシュボード・データ・プロバイダーへの要求に Dashboard Application Services Hub にログインしているユーザーの LTPA トークンが組み込まれます。
12. 接続の定義が終了したら「**OK**」をクリックして定義を保存し、ダッシュボード・データ・プロバイダーに接続します。

タスクの結果

データ・プロバイダーへの接続が確立し、接続表の「**状況**」列に進行状況 (`Pending`、`Working`、`Failed`、`No data sources`、または `Not configured`) が表示されます。

データ・プロバイダー接続の作成時にエラーが発生する場合は、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。

実行する追加ステップについては、31 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用しない基本モニター環境のセットアップ』または 37 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ』を参照してください。

モニター・データを表示するカスタム・ダッシュボード・ページの作成

IBM Dashboard Application Services Hub では、カスタム・ダッシュボード・ページを作成できます。

ページ とは、コンソールの作業領域内に 1 つ以上のウィジェットを配置したものです。ウィジェット とは、コンソール・ダッシュボードに情報を表示するユーザー・インターフェース・コンポーネントです。Dashboard Application Services Hub には、一連の定義済みウィジェットが用意されています。各ウィジェットは、Dashboard Application Services Hub で定義された接続を持つデータ・プロバイダーから情報を取得するように構成されています。各データ・プロバイダーは、データをデータ・セットに分割します。

始める前に

定義済みウィジェット、各ウィジェット・タイプを編集およびカスタマイズする方法、およびウィジェットを使用してカタログおよびページを作成する方法について詳しくは、Dashboard Application Services Hub オンライン・ヘルプまたは Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management Integration Guide*」を参照してください。

このタスクについて

定義済みウィジェットをダッシュボード・ページに追加するか、定義済みウィジェットをカスタマイズして外観を変更できます。表、リスト、ゲージ、棒グラフ、円グラフ、トポロジーなどのためのウィジェットがあります。ウィジェットは、カタログに配置することにより論理的に整理することも可能です。

IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーのデータ・セットは、エージェント属性グループに対応します。これらは、Tivoli Enterprise Portal ワークスペース・ビューをカスタマイズするときに照会を作成する属性グループと同じです。ダッシュボード・データ・プロバイダーには、IBM Tivoli Monitoring for VMware モニター・エージェントなどのモニター・エージェントによって提供される場合には、トポロジー・データ・セットもあります。エージェントの属性グループの説明を参照したり、エージェントがトポロジー・データ・セットを提供するか判断したりするには、エージェントのユーザー・ガイドを参照してください。

ページを作成または編集するときは、ウィジェットと、それらのウィジェットのページ上での配置を選択します。各ウィジェットを編集してデータ・セットを選択し、ウィジェットで表示するデータ・セット内の情報を選択します。ウィジェットを編集するときは、以下の情報を指定します。

手順

1. データ・セットを選択してください。

   ウィジェットを編集するときは、Dashboard Application Services Hub で構成されているデータ・プロバイダーのリストからデータ・セットを選択します。すべてのデータ・セット名を表示するか、データ・セット名の検索条件を入力できます。すべてのデータ・セット名を表示した場合、アプリケーション・サポートが Tivoli Enterprise Portal Server にインストールされているすべてのエージェントのデータ・セットと、他のデータ・プロバイダーから利用できるデータ・セットが表示されます。リストに表示されるデータ・セットが多い可能性があるため、データ・セット名の一部で検索することにより、データ・セットをフィルタリングすることができます。例えば、Linux OS エージェントのすべてのデータ・セット (属性グループ) を表示するには、検索フィールドに「Linux」と入力します。

2. データ・セットの列をウィジェットの可視化属性にマップします。

   ウィジェットのタイプによっては、ウィジェットに表示するデータ・セットの列を指定するように求められる場合があります。例えば、Linux OS エージェントのディスク使用状況を表示するアナログ・ゲージ・ウィジェットを編集するには、ゲージ値用の「**使用ディスク率**」列を選択します。

3. ウィジェット可視化オプションを構成します。

   ラベルや単位など、ウィジェットの可視化オプションを構成することもできます。

4. データ・セット・構成パラメーターを指定します。

   エージェントの属性グループにマップするデータ・セットを選択した場合、データの取得対象である管理対象システムまたは管理対象システム・グループの名前を入力する必要があります。また、ウィジェットが時間枠に沿ったデータの表示をサポートしていて、ヒストリカル・データ収集を構成した場合、ヒストリカル・データを取得する時間フィルター値を指定することもできます。

   データ・セットには、ウィジェットに表示する情報をさらにフィルタリングするその他の構成パラメーターがある場合もあります。例えば、エージェント属性グループの単一の行の値を表示するゲージなどのウィジェットを編集している場合、データ・セット構成パラメーターを使用して、ウィジェットに表示するデータ行を一意に識別するその他のデータ・セット列 (属性) を指定できます。例えば、Linux OS エージェントのディスク使用状況を表示する場合、ゲージ・ウィジェットで Linux ディスクのデータ・セット構成パラメーターを使用して、使用状況を表示するディスクおよびマウント・ポイントを指定できます。

   また、ウィジェットが自動最新表示をサポートしていて、イベント・データ・セットを選択していない場合、ダッシュボード・データ・プロバイダーがデータを最新表示する頻度も指定できます。

   トポロジー・データ・セットの場合、以下の構成パラメーターを指定できます。

   SourceToken
   トポロジーのトラバースを開始する開始ノード識別子。

Depth
ダッシュボード・データ・プロバイダーがトラバースして返すトポロジーの最大深度 (レベル数)。

Breadth
ダッシュボード・データ・プロバイダーがトラバースして返すレベルごとの最大ノード数。

MaxNodes
ダッシュボード・データ・プロバイダーが返すノードの最大数。

TraversalOrder
トポロジーのノードをトラバースしてデータ・セットの結果に追加する順序。サポートされる値は以下のとおりです。

DepthFirst
トラバーサルは深度を優先して行われます。

BreadthFirst
トラバーサルはレベルを優先して行われます。

注: **Depth** パラメーターまたは **Breadth** パラメーターを指定した場合、**TraversalOrder** パラメーターは無視されます。

多くの Dashboard Application Services Hub ウィジェットでは、相互にメッセージを交換できるように、ウィジェット間の接続 (ワイヤー) をサポートできます。ソース・ウィジェットでアクションが発生すると、ソース・ウィジェットはその他のウィジェットに送信できる情報が含まれるイベントを作成します。ダッシュボード・データ・プロバイダーは、他のウィジェットとのイベントの交換をサポートしていません。

Dashboard Application Services Hub では、ユーザーまたはユーザー・グループの役割を使用して、ページの作成やウィジェットの操作ができるユーザー、およびユーザーが表示できるページを制御します。ただし、データ・プロバイダーのいずれかのデータ・セットを使用するウィジェットに表示されるモニター・リソースの許可は、ダッシュボード・データ・プロバイダーによって実行されます。カスタム・ダッシュボード・ページでは、モニター・ダッシュボード環境用に構成された許可タイプ、つまり許可ポリシーまたは Tivoli Enterprise Portal イベントの許可とモニター・アプリケーションの割り当てを使用します。

次のタスク

モニター・データを使用してカスタム・ダッシュボード・ページを作成する例については、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) の Creating custom monitoring dashboard pagesを参照してください。

UISolutions のインポートの制御

IBM Infrastructure Management Dashboards for Servers などのダッシュボード・アプリケーションを起動すると、ダッシュボード・アプリケーションはダッシュボード・データ・プロバイダーに要求を送信してアプリケーションの UISolutions をインポートします。ダッシュボード・データ・プロバイダーの UISolutions は、ダッ

シュボードで表示できるデータの特性を定義します。このインポートは、ダッシュボード・アプリケーションごとに 1 回発生し、自動的に行われます。ダッシュボード・アプリケーションが更新され、更新済みの UISolutions を含んでいる場合も、インポートが自動的に行われます。

すべてのダッシュボード・アプリケーションをインストールして起動した後に UISolutions のインポートを完全に無効にすることができます。または、ポータル・サーバーを構成することにより、UISolutions をインポートできるユーザーを制御できます。

このタスクについて

UISolutions を完全に無効にした場合、IBM Dashboard Application Services Hub で新しいダッシュボード・アプリケーションをインストールしたとき、または既存のダッシュボード・アプリケーションを更新したときに、UISolutions のインポートを再度有効にする必要があります。ダッシュボード・アプリケーションのインストールまたは更新が完了し、ダッシュボード・アプリケーションが起動し、データを表示できることを確認した後、UISolutions のインポートを再度無効にすることができます。

UISolutions をインポートできるユーザーを制御する場合、UISolutions を含む新規または更新後のダッシュボード・アプリケーションは、ポータル・サーバーの環境ファイルで指定されたユーザーがダッシュボード・アプリケーションを起動するまで使用できないので注意してください。

KD8_VM_IMPORT_ID 変数はオプションであり、デフォルトでは設定されません。つまり、認証されているダッシュボード・ユーザーは、ダッシュボード・アプリケーションを起動するときに、UISolutions のインポートの要求を開始できます。

手順

1. Tivoli Enterprise Portal Server 環境変数ファイルを開きます。

   Windows *install_dir* ¥CNPS¥kfwenv

   Linux UNIX *install_dir* /config/cq.ini
2. KD8_VM_IMPORT_ID 環境変数を設定します。

   インポートの実行を許可するユーザーを制御するには、この変数に特定の ID (KD8_VM_IMPORT_ID=user1 など) を設定します。

   すべてのユーザーが UISolutions のインポートを実行できないようにするには、KD8_VM_IMPORT_ID=$nouser@ を設定するか、またはダッシュボード・ユーザー ID と一致しないことが判明している名前を設定します。
3. 変更内容を実装するには、Tivoli Enterprise Portal Server を再始動してください。

第 4 章 環境構成設定の編集

Tivoli Enterprise Portal クライアントには、ユーザー・コンピューターの動作およびパフォーマンスを制御するためのパラメーターが数十個あります。また、Tivoli Enterprise Portal Server には環境ファイルがあり、ユーザーはこのファイルを編集することによって、接続するすべてのポータル・クライアントおよびハブ・モニター・サーバーとの対話に影響する変数を調整または追加することができます。Tivoli Enterprise Monitoring Server および Tivoli Enterprise Monitoring Automation Server で環境変数を制御することもできます。

以下のトピックには、「*管理者ガイド*」で言及される環境変数に関する情報が収録されています。すべての環境変数のリストについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『環境変数』を参照してください。

Tivoli Enterprise Portal クライアント構成設定

Tivoli Enterprise Portal クライアントには、イベント確認通知に添付するファイルの最大サイズやキャッシュ内に共通イベント・リストを保持しておく期間など、自身のパフォーマンスを制御するパラメーターがあります。

クライアント・パラメーターの編集

ブラウザー・クライアントに対して行う変更は、ポータル・サーバーを使用してインストールされた HTTP サーバーを介して自動的にダウンロードされるため、グローバルに適用されます。ユーザーが Java WebStart を使用して自分自身でデスクトップ・クライアントをデプロイしている場合にも、変更はグローバルに適用されます。それ以外の場合は、その変更をすべてのユーザーに適用したいのであれば、デスクトップ・クライアントがインストールされている各コンピューター上で、その変更を実行しなければなりません。

このタスクについて

クライアント・パラメーターを調整するには、以下のステップを実行してください。

手順

1. 「Tivoli Enterprise Monitoring Services の管理」を開始します。ブラウザー・クライアントおよび Java WebStart の場合、これはポータル・サーバーがインストールされているコンピューターです。それ以外の場合、これはデスクトップ・クライアントがインストールされているコンピューターです。
   - Windows 「**スタート**」 → 「**プログラム**」 → 「**IBM Tivoli Monitoring**」 → 「**Tivoli Enterprise Monitoring Services の管理**」の順にクリックします。
   - Linux *install_dir* /bin ディレクトリーに移動し、`./itmcmd manage` と入力します。
2. 「**Tivoli Enterprise Portal – デスクトップ (Tivoli Enterprise Portal – Desktop)**」または「**Tivoli Enterprise Portal – ブラウザー (Tivoli Enterprise**

Portal – Browser)」を右クリックし、「**再構成**」をクリックします。 デスクトップ・クライアントの場合には「アプリケーション・インスタンスの構成」ウィンドウが表示されます (Java WebStart の場合にも使用されます)。ブラウザー・クライアントの場合には、「Tivoli Enterprise Portal ブラウザーの構成」ウィンドウが表示されます。

3. 変更するパラメーター値をダブルクリックします。
4. パラメーターを活動化するには、値を入力して、「Tivoli Enterprise Portal パラメーターの編集」ウィンドウで「**使用中**」を選択します。
5. パラメーターの編集が終了したら、「**OK**」をクリックして変更を保存します。変更は、次にユーザーがポータル・サーバーにログオンしたときに有効になります。既にログオンしているユーザーに対しては、一度ログオフしてから再度ログオンするまで、変更は表示されません。

関連資料:

『ポータル・クライアント・パラメーターのリスト』

Tivoli Enterprise Portal クライアント・パラメーターのほとんどは、デフォルト値のまま変更されません。クライアント・パラメーターを編集すると、特定の動作に影響を与えることができます。

ポータル・クライアント・パラメーターのリスト

Tivoli Enterprise Portal クライアント・パラメーターのほとんどは、デフォルト値のまま変更されません。クライアント・パラメーターを編集すると、特定の動作に影響を与えることができます。

パラメーターには、デスクトップ・クライアントにのみ関連するもの、デスクトップ・クライアントおよび Java WebStart クライアントにのみ関連するもの、またはブラウザー・クライアントのみに関連するものがあり、一目でそれとわかるようになっています。

browser.cache.memory.capacity

デコードされたイメージおよびその他の機能をキャッシュする場合にブラウザー・ビューで使用される最大メモリー量 (ゼロでない正の整数) を KB 単位で示します。メモリー・キャッシュを無効にするには、値に 0 を指定してください。デフォルト: **-1** (これにより、キャパシティー値がメモリーの合計量に基づいて自動的に決定されます)。

物理メモリー	メモリー・キャッシュ (KB)
32 MB	2048
64 MB	4096
128 MB	6144
256 MB	10240
512 MB	14336
1 GB	18432
2 GB	24576
4 GB	30720
8 GB 以上	32768

cnp.agentdeploy.timeout

これは、エージェントのデプロイ要求がタイムアウトになるまでの時間です。デフォルト: **1800** 秒 (30 分)。

cnp.attachment.segment.maxsize

ネットワーク上で伝送される場合は、添付ファイルは複数のセグメントに分割され、Tivoli Enterprise Portal Server で再アセンブルされます。例えば、8 MB のファイルは 8 個の 1 MB のセグメントとして伝送されます。このパラメーターを調整して、ご使用の環境に最適なセグメント・サイズにしてください。最大サイズをバイト単位で入力します (250 KB であれば 250000)。デフォルト: **1000000** (1 MB)。

このパラメーターは、ポータル・サーバーの環境変数としても使用することができます。 83 ページの『イベントの添付ファイルのサイズの管理』を参照してください。

cnp.attachment.total.maxsize

確認通知に添付される各ファイルの最大サイズを設定するには、このパラメーターを使用します。最大サイズをバイト単位で入力します (2.5 MB であれば 2500000)。デフォルト: **10000000** (10 MB)。

このパラメーターは、ポータル・サーバーの環境変数としても使用できます。 83 ページの『イベントの添付ファイルのサイズの管理』を参照してください。

cnp.authentication.skip_dns

値:「N」。これにより、サーバー証明書の妥当性検査でホスト DNS 名の解決およびマッチングを試行するかどうかが決定します。

cnp.browser.installdir

ポータル・クライアントでは、WebRenderer Java ブラウザー・コンポーネントがブラウザー・ビュー機能として使用されます。最初にユーザーがブラウザー・ビューを作成したときに、サブディレクトリーがユーザーのコンピューター上に自動的に作成されます。

Windows *%HOMEPATH%*¥wr*WebRendererVersion*¥.webrendererswing.

例: C:¥Documents and Settings¥Administrator¥wr4.2.14¥.webrendererswing

Linux %HOME/wr*WebRendererVersion*/.webrendererswing

このサブディレクトリーでは、ブラウザーの JAR ファイルが抽出され、証明書やその他の WebRendererの成果物がブラウザー・ビューに対して作成されます。このパラメーターを使用すると、ユーザーのコンピューターに保存されるブラウザー・ビューのファイルに対して、異なるパスを指定することができます。ユーザーがポータル・クライアントの複数インスタンスを実行したり、ポータル・サーバーの異なるバージョンにログオンする可能性がある場合は、異なるバスが必要となります。

cnp.commonevent.cache.timeout

ユーザーが共通イベント・コンソール・ビューのない (つまり、キャッシュの使用されていない) ワークスペースに切り替えた場合に、共通イベント・コンソール用のキャッシュを保存しておく分数。この期間が経過するまでに再度キャッシュの利用がなかった場合、キャッシュは消去されます。その後キャッシュは、共通イベント・コンソール・ビューで必要になったときに再作成されます。

値が -1 の場合は、キャッシュが使用されていない場合でも常にキャッシュが保存されます。値が 0 の場合は、ユーザーが共通イベント・コンソール・ビューのないワークスペースに切り替えると、即時にキャッシュが消去されます。デフォルト: **30**。

cnp.databus.pageSize

Tivoli Enterprise Portal・ユーザー・インターフェースのプロパティー・エディターには、個々の照会ベース・ビューのページ・サイズを調整するためのフィールドがあります。このパラメーターは、すべての照会ベース・ビューの単一の論理ページ内にフェッチする行数を設定します。デフォルト: **100** 行。ここに設定可能な値に制限はありませんが、ページ・サイズが大きくなるほど、ポータル・クライアントおよびサーバーで必要になるメモリーの量が増加します。

例えば、より多数の行に対して表ビューで検索するために、より大きいページ・サイズを設定する必要がある場合があります。または、より多数の行 (またはインスタンス) を取り出すビューと対話する際に、スクロールするページを減らす必要がある場合があります。ただし、ページ・サイズ値を引き上げた結果として、追加されるデータを圧縮し、転送して、最終的にレンダリング処理できるだけの十分なリソースが、ポータル・クライアントとポータル・サーバーの両方になければなりません。このパラメーターの適正値を判断する最良の方法として、良好な状態にあるワークスペース・サンプリングの応答時間が遅延し始めるまで、値を徐々に増分させていく (例えば、100 ずつ) ことが考えられます。その時点で、最後の増分の分だけ数を減らす (100 行未満など) ことにより、環境にとっての最適値に近づけることができるはずです。

照会ベース・ビューの応答時間に影響を与える別の設定としては、ポータル・サーバーの環境変数である KFW_REPORT_NODE_LIMIT があります。

cnp.drag.sensitivity

ドラッグ操作が開始されるまでにマウスを移動させる必要のあるピクセル数。デフォルト: **7**。

cnp.encoding.codeset

ストリング・エンコード・コード・セット ID。

cnp.eventcon.autoresume.delay

Situation Event Console および Common Event Console に対する更新がスクロールのために一時停止した後で、更新を自動的に再開するまでに待機する秒数。デフォルト: **60** 秒。

cnp.heartbeat.interval

Tivoli Enterprise Portalのクライアントとサーバー間のハートビート ping 間隔。間隔を増やすと、ポータル・サーバーがオフラインのときに、クライアントで検出にかかる時間が長くなります。間隔を短くすると、クライアントはより早く通知を受けますが、クライアントとサーバーとの間のトラフィックも増大します。デフォルト: **30** 秒。

cnp.history.depth

後方または前方のヒストリー・ナビゲーション・スタック内に維持するワークスペースの数。デフォルト: **20**。

cnp.http.proxy.password
ブラウザー・ビューを使用したプロキシー認証に使用するパスワード。

cnp.http.proxy.user
ブラウザー・ビューを使用したプロキシー認証に使用するユーザー ID。

cnp.http.url.host
デスクトップ・クライアントおよび Java WebStart クライアントのみ: IOR フェッチのための URL ホスト。

cnp.http.url.path
デスクトップ・クライアントおよび Java WebStart クライアントのみ: IOR フェッチのための URL パス。

cnp.http.url.port
デスクトップ・クライアントおよび Java WebStart クライアントのみ: IOR フェッチのための URL ポート。

cnp.http.url.protocol
デスクトップ・クライアントおよび Java WebStart クライアントのみ: IOR フェッチのための URL プロトコル。

cnp.http.url.DataBus
デスクトップ・クライアントおよび Java WebStart クライアントのみ: `cnps.ior` ファイルの URL。ポータル・サーバーでグラフィック表示イメージおよびスタイル・シートを見つけるために必要となります。デフォルト設定 (表示されない) では、統合 HTTP サーバーを前提としています。何らかの理由でこれが無効になっている場合は、統合 HTTP サーバーの URL を入力する必要があります。詳しくは、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。このパラメーターを設定すると、プロトコル、ポート、およびパス用の他の cnp.http.url パラメーターの設定が指定変更されます。

cnp.pipeline.factor
サーバー・パイプライン・モニター因子へのデータ・バス (ハートビート・サイクル内)。デフォルト: **2**。

cnp.playsound.interval
同じサウンド・ファイルを再度再生できるようになるまでの秒数。イベントが頻繁に開く場合、この設定によって、サウンドが一時停止します。デフォルト: **10** 秒。

cnp.publishurl.delay
ブラウザー・クライアントのみ: ワークスペース切り替えを行うとき、ブラウザーが新規アプレットを初期化して古いアプレットを破棄する前に、ユーザー・インターフェースのレンダリングが完了できるようにします。デフォルト: **1** 秒。

重要: このパラメーターを変更する前に、必ず IBM ソフトウェア・サポートに相談してください。

cnp.systemtray.offset
表示するメニューおよびウィンドウのサイズ変更時に、画面の下部に表示される Windows タスクバー内の Tivoli Enterprise Portal 因子。デフォルト: **true**。

cnp.terminal.cache.entries
アクティブ端末エミュレーター・セッションの最大数。デフォルト: **50**。

cnp.terminal.host
デフォルトの端末エミュレーター・ホスト名。

cnp.terminal.port
デフォルトの端末エミュレーター・ポート番号。デフォルト: **23**。

cnp.terminal.script.entries
保存可能なユーザー端末エミュレーター・スクリプトの最大数。デフォルト: **256**。

cnp.terminal.type
デフォルトの端末エミュレーター・タイプ。端末タイプを指定するとき、端末タイプを二重引用符で囲み、サポートされる以下の名前のいずれかを入力してください。

IBM 3270 (24x80)

IBM 3270 (32x80)

IBM 3270 (43x80)

IBM 3270 (27x132)

IBM 5250 (24x80)

VT100 (24x80)

cnp.view.change_remove.warning
ユーザーがビューを変更または削除しようとしたときの警告メッセージ。

デフォルト: **True**。メッセージが表示されます。メッセージが表示されないようにするには、設定を False に変更してください。

cnp.workspace.switch.rate
ワークスペースを次に選択したワークスペースで置き換えられるようになるまでの最小経過時間。デフォルト: **1000** (1 秒)。

cnp.workspacerender.delay
ブラウザー・モードのみ: ワークスペースのポスト・レンダリング遅延 (ミリ秒単位)。

http:agent
統合 HTTP サーバーの名前を定義します。ブラウザー・ビューがインターネットにアクセスできるようにするために、事前に統合 HTTP サーバーまたはそのプロキシーで異なるブラウザー ID が必要となる場合は、ブラウザーに 1 語の名前を入力できます。プロキシー・サーバーによってリジェクトされない限り、どのような名前でもかまいません。通常は、ユーザーがワークスペース・ブラウザー・ビューからインターネットへのアクセスを試みた際にエラーを受け取った場合を除き、HTTP 名定義を追加する必要はありません。

http.nonproxyhosts
☑ 「**HTTP プロキシー・サーバー要求の使用可能化 (Enable HTTP Proxy Server Requests)**」が選択されている場合、このリスト内のサーバーはプロ

キシーを迂回します。縦線 (|) を使用して各サーバー名を区切ってください。 75 ページの『HTTP プロキシー・サーバーの使用可能化』を参照してください。

http.proxyHost
ブラウザー・クライアント: HTTP プロキシー・サーバーを使用している場合、そのプロキシー・サーバーのホスト名または IP アドレスの指定に使用します。

http.proxyPort
ブラウザー・クライアント: http.proxyHost パラメーターとともに使用して、HTTP プロキシー・サーバーの listen ポート番号を指定します。サード・パーティー製 HTTP サーバーの場合のデフォルトは、ポート **80** です。

kjr.browser.default
これは、コンテキスト・ヘルプの起動時に使用するブラウザー・アプリケーションのパスおよび名前です。特定のブラウザーまたはデフォルトとは異なるブラウザーを使用してヘルプを開くには、`C:¥Program Files¥Mozilla Firefox¥firefox.exe` などのように、パスおよびアプリケーション名を入力します。

kjr.trace.file
トレース・モードが LOCAL である場合、RAS1 トレース・ログのファイル名。

kjr.trace.mode
RAS1 トレース・オプション。デフォルト: LOCAL。

kjr.trace.params
RAS1 トレース・オプション。デフォルト: ERROR。

kjr.trace.qdepth
トレース・スレッドのキュー項目数をデフォルトで **15000** に設定します。

kjr.trace.thread
トレース呼び出しがスレッド化されているかどうかを決定します。デフォルト: **true**。

sun.java2d.noddraw
DirectDraw 画面描画機能をサポートしないエミュレーション環境内で Tivoli Enterprise Portal がクライアント・イメージとして実行されている場合に、ブラウザー・クライアントおよびデスクトップ・クライアントの両方でこの変数を true に設定することにより、この機能をオフにします。それ以外の場合は、Java プロセスで画面への書き込みが試行されるため、CPU 使用量が高い状態になります。デフォルト: **true**。

user.language
デスクトップ・クライアントおよび Java Web Startクライアントのみ: ユーザーのロケール設定の言語コードを指定します
(cs、de、en、es、fr、hu、it、ja、ko、pl、pt、ru、th、zh など)。デスクトップ・クライアントで別のインスタンスを作成し、この変数 (および user.region) を他のロケールに変更できます。このようにして、同じコンピューターで、それぞれ異なる言語を使用するデスクトップ・クライアントの

複数のインスタンスを実行することができます。サポートされないロケールを指定した場合、フェイルオーバーにより en_US が使用されます。

ブラウザー・クライアントのみ: クライアント・コンピューターで、ブラウザーにより使用される Java プラグイン・ランタイム・パラメーターに、以下のテキストを直接入力します。*xx* は言語、*XX* はロケールです。

```
-Duser.language=xx -Duser.region=XX
```

注: ポータル・クライアントはカスケード・スタイル・シートを使用して、アプリケーション・テキストをレンダリングします。ローカライズされたスタイル・シート (ws_press.css など) が使用可能でない場合は、英語バージョンが使用されます。
ランタイム・パラメーターを編集するには、以下のタスクを実行します。

1. 以下のように Java のコントロール・パネルを開きます。

   Windows 「**Java 用 IBM コントロール・パネル (IBM Control Panel for Java)**」または「**Java**」コントロール・パネルを起動します。

   Linux *jre_install_dir* にある Java の **ControlPanel** 実行可能ファイルを見つけて、起動します。例えば、 `/opt/IBM/ibm-java2-i386-70/jre/bin/ControlPanel` などです。
2. 「**Java**」タブをクリックします。
3. 「Java アプレットのランタイム設定」の領域で「**表示**」をクリックします。
4. Java のバージョンが複数ある場合は、「**場所**」列で Java ランタイムを調べて、JRE のパスが正しいことを確認し、適切なコントロール・パネルが開かれていることを確認してください。例えば、Windows の IBM Java の場合は `C:¥Program Files¥IBM¥Java70¥jre¥bin` です。
5. 変更したいパラメーターを編集します。
6. 変更内容を保存します。

user.region

ユーザーのロケール設定の国別コードを指定します
(BR、CN、CZ、DE、ES、FR、HU、IT、JP、KR、PL、RU、TH、TW、US など)。**user.language** についての説明も参照してください。

以下の表で言語コードとロケール・コードを確認してください。

表 6. 言語とロケール・コード

言語	言語コード (xx)	ロケール・コード (XX)
中国語 (簡体字)	zh	CN
中国語 (繁体字)	zh	TW
チェコ語	cs	CZ
英語	en	US
フランス語	fr	FR
ドイツ語	de	DE
ハンガリー語	hu	HU
イタリア語	it	IT

表 6. 言語とロケール・コード (続き)

言語	言語コード (xx)	ロケール・コード (XX)
日本語	ja	JP
韓国語	ko	KR
ポーランド語	pl	PL
ポルトガル語 (ブラジル)	pt	BR
ロシア語	ru	RU
スペイン語	es	ES
タイ語	th	TH

関連タスク:

67 ページの『クライアント・パラメーターの編集』
ブラウザー・クライアントに対して行う変更は、ポータル・サーバーを使用してインストールされた HTTP サーバーを介して自動的にダウンロードされるため、グローバルに適用されます。ユーザーが Java WebStart を使用して自分自身でデスクトップ・クライアントをデプロイしている場合にも、変更はグローバルに適用されます。それ以外の場合は、その変更をすべてのユーザーに適用したいのであれば、デスクトップ・クライアントがインストールされている各コンピューター上で、その変更を実行しなければなりません。

83 ページの『イベントの添付ファイルのサイズの管理』
デフォルト時、イベント確認通知に添付する各ファイルの最大サイズは 10 MB で、ネットワーク上で送信する情報セグメントのサイズは 1 MB です。 Tivoli Enterprise Portal または Tivoli Enterprise Portal Server での最大値の変更に使用できる環境変数が用意されています。デスクトップ・クライアントでイベントの添付ファイル設定が変更された場合、ポータル・サーバーの設定は指定変更されます。

26 ページの『別のポータル・サーバーでのブラウザー・クライアントの開始』
別のブラウザー・インスタンスを開始して、別の管理対象ネットワークの Tivoli Enterprise Portal Server にログオンすることで、1 台のコンピューターから 2 つの管理対象ネットワークを監視できます。

関連資料:

80 ページの『ポータル・サーバーの環境変数』
Tivoli Enterprise Portal Server の環境構成ファイルは、特定の環境設定を追加したり、他の設定値を変更したりするために編集することができます。

HTTP プロキシー・サーバーの使用可能化

HTTP プロキシー・サーバーを使用する環境で、Tivoli Enterprise Portal ワークスペースのブラウザー・ビューからの URL アクセスを有効にするには、追加のクライアント構成を行う必要があります。

このタスクについて

HTTP プロキシー・サーバーを有効にするには、(ブラウザー・ビューに HTTP プロキシーを使用する) Tivoli Enterprise Portal クライアントが使用されている、すべてのコンピューターで以下のステップを実行します。

手順

1. ブラウザー・ビューを含むワークスペースを開くか、または現行のワークスペースにブラウザー・ビューを追加します。
2. ブラウザー・ビューのアドレス・ボックスで、`about:config` と入力します。
3. ページの上部に表示されるフィルター・フィールドで、`network.proxy` と入力して、ネットワーク・プロキシー・フィールドを確認します。
4. 抽出された項目のうち、重要となるのは以下の 3 つです。1 つの項目をダブルクリックするか、または選択して Enter キーを押し、値を変更します。

   network.proxy.http
   HTTP プロトコルに使用するプロキシー・ホストの DNS ID、または IP アドレスを入力します。

   network.proxy.http_port
   デフォルトのポート番号である `80` を入力するか、またはプロキシー・ホストで使用する別の番号を入力します。

   network.proxy.no_proxies_on
   プロキシーなしでアクセスできる任意の完全修飾ホスト名または IP アドレスを付加します。この設定により、ローカル・システムおよびポータル・サーバー (myteps.uk.ibm.com) 上にある、ブラウザー・ビューからアクセスされる任意のファイルに対して、プロキシー・サーバーがバイパスされます。例えば、`localhost,127.0.0.1,myteps.uk.ibm.com` のように指定します。

タスクの結果

プロパティーの編集パネルで「**OK**」をクリックすると、変更が Tivoli Enterprise Portal クライアントに保存されます。

Linux および UNIX システムのアプリケーション・プロパティーの設定

プロパティー (UNIX で Tivoli Enterprise Portal ブラウザー・クライアントが Web ブラウザーを起動する場所など) を変更するには、実行するシェル・スクリプト・ファイル (複数可) と、これらのスクリプト・ファイルを作成するためにブラウザー・クライアントを構成したときに使用したテンプレートを更新します。

このタスクについて

以下の 1 つ以上のファイルを更新する必要があります。

注: すべてのファイル・パスは、IBM Tivoli Monitoring がインストールされている *install_dir* ディレクトリーを基準にしています。

表 7. UNIX および Linux システムでアプリケーション・プロパティーを変更するためのファイルの場所

ファイルの場所	ファイルの目的
bin/cnp.sh	Tivoli Enterprise Portal ブラウザー・クライアントを起動するデフォルトのシェル・スクリプト。

表 7. UNIX および Linux システムでアプリケーション・プロパティーを変更するためのファイルの場所 (続き)

ファイルの場所	ファイルの目的
bin/cnp_*instance*.sh	作成した特定のインスタンスのシェル・スクリプト。*instance* は、 Tivoli Enterprise Portal ブラウザー・クライアントを起動するインスタンスの名前です。
platform/cj/original/cnp.sh_template	構成中に bin/cnp.sh および bin/cnp_*instance*.sh シェル・スクリプトを生成するために使用されるテンプレート。ここで、*platform* は、IBM Tivoli Monitoring がインストールされているオペレーティング・システム・プラットフォームのコードです。例えば、32 ビット Intel CPU 上の Linux 2.4 の場合は、 *li6243* のようになります。 bin/cnp.sh または bin/cnp_instance.sh のみを変更し、このテンプレートを変更しないと、次回クライアントを構成するときに作成される新規バージョンのスクリプトに、bin/cnp.sh または bin/cnp_instance.sh の変更内容が反映されません。

Linux ではインスタンス名、ブラウザー、および Tivoli Enterprise Portal Server プロパティーも設定できます。詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

Web ブラウザーのロケーションを変更するには、以下の手順を実行して、新規プロパティーを含めるように、前述のファイル (複数可) を変更する必要があります。

手順

1. *install_dir* /bin/cnp.sh に移動し、cnp.sh シェル・スクリプトを編集します。
2. ファイルの最後の行に Web ブラウザーの場所を追加します。以下の例では、Web ブラウザー・ロケーションは */opt/foo/bin/launcher* です。
   ```
   -Dkjr.browser.default=/opt/foo/bin/launcher
   ```

   重要: この行は非常に長く、他のプロパティーを定義するための各種 -D オプションをはじめとするさまざまなオプションが記述されています。オプションを正しい場所に追加することは非常に重要です。
   bin/cnp.sh の元の最終行が以下のようであるとします。

   ```
   ${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
   -Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
   -Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
   -Dvbroker.agent.enableLocator=false
   -Dhttp.proxyHost=
   -Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
   ```

   ブラウザーの場所を */opt/foo/bin/launcher* に設定するには、この行を以下のように変更します。

```
${JAVA_HOME}/bin/java -showversion -noverify -classpath ${CLASSPATH}
-Dkjr.browser.default=/opt/foo/bin/launcher
-Dkjr.trace.mode=LOCAL -Dkjr.trace.file=/opt/IBM/ITM/logs/kcjras1.log
-Dkjr.trace.params=ERROR -DORBtcpNoDelay=true -Dcnp.http.url.host=
-Dvbroker.agent.enableLocator=false
-Dhttp.proxyHost=
-Dhttp.proxyPort=candle.fw.pres.CMWApplet 2>& 1 >> ${LOGFILENAME}.log
```

z/OS システムにハブがある場合の環境変数の設定

z/OS では GSKit は、Integrated Cryptographic Service Facility、つまり、ICSF と呼ばれています。Tivoli Enterprise Monitoring Server では、ICSF を使用したセキュアなパスワード暗号化がサポートされています。ICSF は、保管されているパスワードを強固に暗号化および暗号化解除できる、推奨のパスワード暗号化方式です。

このタスクについて

Tivoli Enterprise Monitoring Server が、ICSF がインストールされていない z/OS システム上にある場合は、代わりに、セキュア度の低い暗号化方式が使用されます。ハブ・モニター・サーバーとポータル・サーバーは、両方で同じ暗号化方式を使用する必要があります。したがって、ハブ・システムで ICSF を使用しない場合は、Tivoli Enterprise Portal も同様に安全性の低い方式 (EGG1) を使用するように構成する必要があります。これには、Tivoli Enterprise Portal Server 環境ファイルを編集して新規行を追加する作業も含まれます。

環境ファイルに新規行を追加するには、以下のステップを完了します。

手順

- Windows
  1. Tivoli Enterprise Portal Server がインストールされているシステムで、「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Monitoring Services の管理**」を選択します。
  2. 「Tivoli Enterprise Portal Server」を右クリックし、「**拡張**」をポイントし、リストから「**ENV ファイルの編集**」を選択します。
  3. 「Tivoli Enterprise Portal Server」のメッセージが表示されたら、「**OK**」をクリックしてメッセージを閉じます。
  4. 新規行 `USE_EGG1_FLAG=1` を追加します。
  5. 「**保存**」をクリックします。
  6. 「**はい**」をクリックして、変更を実装し、サービスを再開します。
- Linux UNIX
  1. ディレクトリーを *install_dir* /config に変更します (cd)。
  2. 次の行を cq.ini ファイルに追加します。`USE_EGG1_FLAG=1`
  3. ファイルを保存します。
  4. ポータル・サーバーをリサイクルします。

次のタスク

Tivoli Enterprise Monitoring Server on z/OS の構成 (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm)を参照してください。

Tivoli Enterprise Portal Server 構成設定

Tivoli Enterprise Portal Server は、KfwServices というプロセスを実行します。このプロセスには、特定の構成要件を満たすために編集して有効にすることが可能な一連の環境変数があります。この作業は、Tivoli Enterprise Monitoring Services の管理アプリケーションを使用するか、コマンド行で `itmcmd manage` を使用することによって実行できます。

例えば、セキュリティーが有効になっている場合は、ユーザーがポータルからロックアウトされるまでに試行されるログインの回数を制御することができます。

Tivoli Enterprise Portal ブラウザー・クライアントが起動する Web ブラウザーのロケーションなど、UNIX または Linux 上に拡張構成機能用のアプリケーション・プロパティーを設定する場合は、手動で行う必要があります。

Integrated Cryptographic Service Facility (ICSF) がインストールされていない z/OS システム上のハブ・モニター・サーバーにポータル・サーバーを接続する場合は、環境ファイルを編集して新しく行を追加する必要があります。

注: LDAP サーバーとの TLS/SSL 通信の構成など、TEPS/e 管理コンソール内で行ったカスタマイズはすべて、ポータル・サーバーの構成中に Manage Tivoli Monitoring Services を介して「**その他**」の LDAP タイプを選択しない限り、ポータル・サーバーが再構成されると、上書きされ、消去されます。これを回避するには、ポータル・サーバーの構成中に「**その他**」の LDAP タイプを選択します。「**その他**」が選択されている場合、LDAP ユーザー・レジストリー情報は TEPS/e で処理され、Tivoli Management Services による直接的な影響はありません。ステップ 5 (112 ページ) を参照してください。

ポータル・サーバー環境ファイルの編集

ポータル・サーバーのパラメーターを再構成するには、Tivoli Enterprise Portal Server 環境ファイルである KFWENV を編集します。

このタスクについて

ポータル・サーバー環境ファイルを編集するには、以下のステップを実行してください。

手順

1. ポータル・サーバーがインストールされているコンピューター上で、環境ファイルを開きます。
   - Windows 「Tivoli Monitoring Services の管理」(「**スタート**」→ 「**プログラム**」→ **IBM Tivoli Monitoring**」→ 「**Tivoli Monitoring Services の管理**」) から、「**Tivoli Enterprise Portal Server**」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックして `kfwenv` ファイルを開きます。
   - Linux UNIX *install_dir* `/config` ディレクトリーに移動し、`cq.ini` ファイルをテキスト・エディターで開きます。
2. このファイルを編集して、任意の環境変数を有効化 (行の先頭にある `#` を削除)、無効化 (行の先頭に `#` を入力)、または変更します。

3. kfwenv (Windows) または cq.ini (Linux および UNIX 系オペレーティング・システム) を保存して、テキスト・エディターを終了します。
4. サービスをリサイクルするかどうかを尋ねるメッセージが表示されたら、「**はい**」をクリックします。 行った変更が、ポータル・サーバーを手動でリサイクルしてから有効となるようにする必要がある場合は、「**いいえ**」をクリックします。

関連資料:

『ポータル・サーバーの環境変数』

Tivoli Enterprise Portal Server の環境構成ファイルは、特定の環境設定を追加したり、他の設定値を変更したりするために編集することができます。

ポータル・サーバーの環境変数

Tivoli Enterprise Portal Server の環境構成ファイルは、特定の環境設定を追加したり、他の設定値を変更したりするために編集することができます。

このファイルには、有効になっている環境変数の数、デフォルトで無効になっているその他の環境変数の数、またはユーザーがポータル・サーバーを構成した結果として無効になっている環境変数の数が示されています。このリストにあるその他の変数を有効にするには、それらを手動で追加しなければなりません。

KFW_AUTHORIZATION_MAX_INVALID_LOGIN=0

この環境変数を設定することにより、ユーザーが実行できるTivoli Enterprise Portal Serverへのログオン試行回数を制御することができます。値の範囲は 0 から 15 です。デフォルト値の 0 では、ユーザーの試行回数に制限はなく、何度失敗しても、ユーザーがロックアウトされることはありません。

84 ページの『ログオン試行回数の制御』のトピックで説明されているように、この構成設定は、ハブ・Tivoli Enterprise Monitoring Serverを使用してセキュリティーを使用可能にしている場合にのみ有効となります。

KFW_CMW_DETECT_AGENT_ADDR_CHANGE=N

エージェントの IP アドレスが見つかった場合、ナビゲーターの機能によって、それが検出されます。エージェント環境が、常時変化している場合や、ナビゲーター・ツリーの再作成が過度に行われる不適切な構成になっている場合は、この環境変数を追加して、見つかった IP アドレスの変更や追加が無視されるようにすることを検討してください。

KFW_CMW_DETECT_AGENT_HOSTNAME_CHANGE=N

この変数はエージェント・アドレスの変更を検出する変数と似ていますが、エージェント・ホスト名が変更された場合のナビゲーターの再作成が行われない点が異なっています。

KFW_CMW_DETECT_AGENT_PROPERTY_CHANGE=N

この変数はエージェント・アドレスの変更を検出する変数と似ていますが、エージェントのアフィニティーまたはアフィニティーのバージョンが変更された場合のナビゲーターの再作成が行われない点が異なっています。

KFW_CMW_SITUATION_ADMIN_SUPPRESS=N

シチュエーションが停止した場合、シチュエーション・イベント・コンソールにメッセージは送信されません。そのシチュエーションが配布された各システムのシチュエーション・イベント・コンソールにメッセージが書き込ま

れるようにするには、この環境変数を有効にします (行の先頭にある # を削除)。「停止」というメッセージは、シチュエーションが停止し、その状態が不明であることをユーザーに警告しています。

KFW_CMW_SPECIAL_HUB_ENTERPRISE=Y

シチュエーションを「物理」ナビゲーター・ビューのルート項目である「**エンタープライズ**」に関連付けます。デフォルト値は「**Y**」であり、管理対象システムのオンラインおよびオフラインのシチュエーションをエンタープライズ・ナビゲーター項目に関連付けることが可能になります。「**N**」に設定すると、*HUB 管理対象システム・グループのエンタープライズ・ナビゲーター項目への自動割り当てが使用不可になります。

KFW_ECLIPSE_HELP_SERVER_PORT=9999

Eclipse Help Server のデフォルトのポート番号は、9999 です。既に別のデバイスが 9999 を使用している場合は、この変数を追加して、1 から 65535 までの範囲のポート番号を指定してください。この値は、ログオン時に、ポータル・サーバーからクライアントにプロパティーとして渡されます。

KFW_FIPS_ENFORCED=N

Tivoli Management Services のモニター・サーバーおよびエージェント・コンポーネントは、既に FIPS に準拠しています。この変数は、ポータル・サーバーで使用される暗号化方式が、連邦情報処理標準 (FIPS) 140–2 仕様に準拠している必要があるかどうかを指定します。使用中の環境が FIPS 140–2 標準に準拠する必要がある場合は、`Y` と指定します。

KFW_REPORT_NODE_LIMIT=200

照会ベース・ビューのあるワークスペースが開かれるか最新表示されると、ビューの照会が、そのナビゲーター項目に割り当てられた管理対象システムのデータを要求します (ビューの QUERY 定義を編集して、特定の管理対象システムまたは管理対象システム・グループを割り当てた場合を除く)。照会がデータを取り出すことのできる管理対象システムの数は、最大 200 です。この制限は、管理対象環境のトラフィックおよびリソース使用量を許容可能なレベルに保持しておくために規定されます。最大数をこの変数で調整できますが、照会される管理対象システムの最大数を増やすと、ビューのレンダリングに使用できる時間が長くなることに注意してください。

フィルターが適用された照会を作成する、管理対象システム・グループを作成する、または、ナビゲーター項目に対して、データを取り出す管理対象システムの数を制限する管理対象システム割り当てが行われているカスタム・ナビゲーター・ビューを作成するといった方法を検討してください。これらの機能については、Tivoli Enterprise Portal のオンライン・ヘルプおよびユーザーズ・ガイドで説明されています。

照会ベース・ビューの応答時間に影響を与える別の設定として、`cnp.databus.pageSize` クライアント・パラメーターがあります。

KFW_REPORT_TERM_BREAK_POINT=86400

この設定を調整して、ヒストリカル要求が短期間または長期間のヒストリー・データを選択するポイントを (秒単位で) 変更することができます。デフォルトでは、短期間ヒストリー・データとしては*現在* から 24 時間前までのデータ、長期間ヒストリー・データとしては 24 時間より前のデータが収集されます。 **0** に設定すると、長期間ヒストリー・データのみが選択されます。

関連タスク:

79 ページの『ポータル・サーバー環境ファイルの編集』
ポータル・サーバーのパラメーターを再構成するには、Tivoli Enterprise Portal Server 環境ファイルである KFWENV を編集します。

関連資料:

68 ページの『ポータル・クライアント・パラメーターのリスト』
Tivoli Enterprise Portal クライアント・パラメーターのほとんどは、デフォルト値のまま変更されません。クライアント・パラメーターを編集すると、特定の動作に影響を与えることができます。

ポータル・サーバー・データベース上のイベントのプルーニング

イベント情報は、Tivoli Enterprise Portal Server (TEPS) データベースの KFW テーブルに保管されます。この情報の消費スペース量は増大する可能性があるため、自動的にプルーニングが行われます。

このタスクについて

デフォルトでは、閉じられたイベントは、それが閉じられた日の翌日の午前 12:00 から午前 4:00 (ローカル・ポータル・サーバー時刻) の間に TEPS データベースから削除されます。Tivoli Enterprise Portal Server 構成ファイルで以下の環境変数を変更することにより、このデータのプルーニングを制御することができます。

手順

1. Tivoli Enterprise Portal Server 環境ファイルを編集用に開きます。
   - Windows Manage Tivoli Monitoring Services で、「**Tivoli Enterprise Portal Server**」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックします。
   - Linux UNIX *install_dir* /config ディレクトリーに移動し、**cq.ini** をテキスト・エディターで開きます。
2. TEPS データベース・イベントのプルーニング・パラメーターを見つけ、必要に応じて編集します。
   - KFW_EVENT_RETENTION=0 は、閉じられたイベントを保持しておく日数。例えば、閉じられてから 2 日後にイベントのプルーニングを行うには、2 と指定します。
   - KFW_PRUNE_START=00:00 は、データのプルーニングを開始する時刻 (24 時間表記で指定)。例えば、午後 11:00 にデータのプルーニングを開始するには、23:00 と指定します。
   - KFW_PRUNE_END=04:00 は、データのプルーニングを停止する時刻 (24 時間表記で指定)。例えば、午前 1:00 にデータのプルーニングを終了するには、01:00 と指定します。
3. 環境ファイルを保存して閉じます。
4. サービスを再開するかどうかを確認するメッセージが表示されたら、「**はい**」をクリックします。または、後でポータル・サーバーを再開して変更を有効にする場合は、「**いいえ**」をクリックします。

イベントの添付ファイルのサイズの管理

デフォルト時、イベント確認通知に添付する各ファイルの最大サイズは 10 MB で、ネットワーク上で送信する情報セグメントのサイズは 1 MB です。 Tivoli Enterprise Portal または Tivoli Enterprise Portal Server での最大値の変更に使用できる環境変数が用意されています。デスクトップ・クライアントでイベントの添付ファイル設定が変更された場合、ポータル・サーバーの設定は指定変更されます。

このタスクについて

Tivoli Enterprise Portal または Tivoli Enterprise Portal Server の環境設定を編集する手順を完了します。

手順

- Tivoli Enterprise Portal 環境ファイルを編集します。
  1. Tivoli Enterprise Monitoring Services の管理 を開始します。
     Windows 「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Monitoring Services の管理**」をクリックします。
     Linux *install_dir* /bin ディレクトリーに移動し、./itmcmd manage と入力します。
  2. 「**Tivoli Enterprise Portal – デスクトップ (Tivoli Enterprise Portal – Desktop)**」または「**Tivoli Enterprise Portal – ブラウザー (Tivoli Enterprise Portal – Browser)**」を右クリックし、「**再構成**」をクリックします。 デスクトップ・クライアントの場合には「アプリケーション・インスタンスの構成」ウィンドウが表示されます (Java WebStart の場合にも使用されます)。ブラウザー・クライアントの場合には、「Tivoli Enterprise Portal ブラウザーの構成」ウィンドウが表示されます。
  3. 「**cnp.attachment.total.maxsize**」をダブルクリックし、イベント確認通知に添付される個々のファイルの最大サイズをバイト数単位で入力し (例えば 2.5 MB の場合は 2500000)、「☑ **使用中**」を選択します。
  4. セグメント・サイズ (デフォルトの 1000000 は 1 MB であり、添付ファイルが 5 MB の場合 1 MB のセグメントが 5 回送信されます) を変更する場合は、「**cnp.attachment.segment.maxsize**」をダブルクリックし、新しいセグメント・サイズをバイト数単位で入力して、「☑ **使用中**」を選択します。
  5. 「**OK**」をクリックして、変更を保存します。 変更は、次にユーザーがポータル・サーバーにログオンしたときに有効になります。既にログオンしているユーザーに対しては、1 度ログオフしてから再度ログオンするまで、変更は表示されません。
- Tivoli Enterprise Portal Server 環境ファイルを編集します。
  1. Tivoli Enterprise Portal Server 環境ファイルを編集用に開きます。
     Windows Tivoli Enterprise Monitoring Services の管理 で、「**Tivoli Enterprise Portal Server**」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックします。
     Linux UNIX *install_dir* /config ディレクトリーに移動し、**cq.ini** をテキスト・エディターで開きます。
  2. 2 つの KFW_ATTACHMENT 行の先頭にあるポンド記号 (#) を削除し、必要に応じて設定を編集します。
     KFW_ATTACHMENT_MAX=10000000 は 10 MB です。添付ファイルの新し

い最大サイズを指定します。
KFW_ATTACHMENT_SEGMENT_MAX=1000000 は 1 MB です。添付ファイルを送信用に分割するファイル・セグメントの新しい最大サイズを指定します。

3. 環境ファイルを保存して閉じます。
4. サービスを再開するかどうかを確認するメッセージが表示されたら、「**はい**」をクリックします。または、後でポータル・サーバーを再開して変更を有効にする場合は、「**いいえ**」をクリックします。

関連資料:

68 ページの『ポータル・クライアント・パラメーターのリスト』
Tivoli Enterprise Portal クライアント・パラメーターのほとんどは、デフォルト値のまま変更されません。クライアント・パラメーターを編集すると、特定の動作に影響を与えることができます。

ログオン試行回数の制御

KFW_AUTHORIZATION_MAX_INVALID_LOGIN 環境変数を設定することにより、ユーザーが実行できる Tivoli Enterprise Portal へのログイン試行回数を指定することができます。

このタスクについて

KFW_AUTHORIZATION_MAX_INVALID_LOGIN 設定に関係なく、ユーザーがポータルにアクセスできないようにするには、このトピックの終わりにある『**次の手順**』の手順を参照してください。ポータル・サーバーへのログオン試行回数を制御するには、以下の手順を実行します。

手順

1. Tivoli Enterprise Portal Server 環境ファイルを編集用に開きます。
   - Windows Manage Tivoli Monitoring Services で、「**Tivoli Enterprise Portal Server**」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックします。
   - Linux UNIX *install_dir* /config ディレクトリーに移動し、**cq.ini** をテキスト・エディターで開きます。
2. KFW_AUTHORIZATION_MAX_INVALID_LOGIN=0 を見つけ、0 から 15 までの値を指定します。 デフォルト値の **0** では、ユーザーの試行回数に制限はなく、何度失敗しても、ユーザーがロックアウトされることはありません。
3. 環境ファイルを保存して閉じます。
4. サービスを再開するかどうかを確認するメッセージが表示されたら、「**はい**」をクリックします。または、後でポータル・サーバーを再開して変更を有効にする場合は、「**いいえ**」をクリックします。

タスクの結果

次にユーザーがポータル・サーバーへのログオンを試みた場合、ログオン試行回数は、環境ファイルで KFW_AUTHORIZATION_MAX_INVALID_LOGIN に設定した値によって制限されます。

次のタスク

☑ **セキュリティー: ユーザーを検証**

無効なログイン設定は、ハブ・モニター・サーバーを使用してセキュリティーを使用可能にしている場合のみ有効です。

Linux UNIX モニター・サーバーの構成ファイルの検証設定をオンにして (KDS_VALIDATE_EXT="Y")、「**ログインのロックアウト (Login Lockout)**」機能も有効にする必要があります。

モニター・サーバーの構成ファイルは、*hostname*_ms_*address*.config および ms.ini という名前で、*install_dir* /config/ ディレクトリーにあります。

ユーザーのアクセス権限の復元

ロックアウトされたユーザーの Tivoli Enterprise Portal へのアクセス権限を回復するオプションには、次の 2 つがあります。

- Tivoli Enterprise Portal で、 「**ユーザー管理**」 をクリックし、ユーザー ID を選択します。「許可」タブで「**ユーザー管理**」をクリックし、☑ 「**ログオンの許可**」を有効にします。
- Tivoli Enterprise Portal Server がインストールされているコンピューターで、以下のコマンド行ユーティリティーを実行して、アクセス権限を有効または無効にします。

  Windows ディレクトリーを *install_dir* ¥cnps¥ に変更し、以下のように入力します。

  ```
  KfwAuthorizationAccountClient.exe ENABLE|DISABLE
    user_id
  ```

  例えば、KfwAuthorizationAccountClient.exe disable guest01 は、guest01 ユーザーを、そのユーザー ID を再度有効にするまでロックアウトします。

  Linux UNIX ディレクトリーを *install_dir* /bin に変更し、以下のように入力します。

  ```
  ./itmcmd execute cq "KfwAuthorizationAccountClient
     enable|disable user_name"
  ```

Tivoli Enterprise Monitoring Server 構成設定

Tivoli Enterprise Monitoring Server は、パフォーマンスおよび可用性データ、モニター・エージェントから受け取るアラートに対する収集および制御ポイントです。また、モニター・エージェントのオンラインまたはオフライン状況のトラッキングも担います。環境変数によりモニター・サーバーの動作が制御されます。

モニター・サーバー環境ファイルの編集

Tivoli Enterprise Monitoring Server 環境ファイル KBBENV を編集し、モニター・サーバーのパラメーターを再構成します。

このタスクについて

モニター・サーバー環境ファイルを編集するには、以下のステップを実行してください。

手順

1. モニター・サーバーがインストールされているコンピューター上で、環境ファイルを開きます。
   - Windows Tivoli Enterprise Monitoring Services の管理 (「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」) で「Tivoli Enterprise Monitoring Server」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックして、KBBENV ファイルを開きます。
   - Linux UNIX *install_dir* /config ディレクトリーに移動し、テキスト・エディターで ms.ini ファイルを開きます。
2. このファイルを編集して、任意の環境変数を有効化 (行の先頭にある # を削除)、無効化 (行の先頭に # を入力)、または変更します。
3. ファイルを保存して、テキスト・エディターを終了します。
4. サービスをリサイクルするかどうかを尋ねるメッセージが表示されたら、「**はい**」をクリックします。変更内容を実装するには、モニター・サーバーをリサイクルする必要があります。

シチュエーションの最適化のための duper プロセス

Tivoli Enterprise Monitoring Server は、*duper* というメカニズムを備えており、これにより、複数のシチュエーションが同一データを同一のサンプリング間隔で評価するときに、シチュエーションの活動化が最適化されます。このトピックでは、duper プロセスの動作、duper プロセスを使用するシチュエーションの特定方法、duper プロセスを使用不可にする場合があることの理由、および duper プロセスを使用不可にするよう Tivoli Enterprise Monitoring Server 環境ファイルを構成する方法について説明します。

duper プロセス

duper シチュエーションは、属性グループからデータを 1 回収集し、モニター・サーバーにアップロードするために、エージェントで作成され、実行されます。モニター・サーバーは duper シチュエーションによって収集されたデータを使用して、複数のシチュエーションを評価します。シチュエーションの評価はモニター・サーバーで行われるため、エージェントが切断されると、これらのシチュエーションは評価されなくなります。

エージェントが日常的にオフラインになったり、モニター・サーバーから切断されたりして、自律的に稼働している場合、それらのエージェントは、エージェントからモニター・サーバー以外のイベント受信側に、イベントを直接送信している可能性があります。モニター・サーバーで定義されているエンタープライズ・シチュエーションを使用するより、エージェントで*専用シチュエーション* を定義するほうが適切な場合があります。

duper の適格性

シチュエーションが duper プロセスに対して適格であるためには、シチュエーションが以下の品質を備えている必要があります。

- 同一の管理対象システム上の同一の属性グループを、少なくとも他の 1 つのシチュエーションと同じモニター間隔でモニターする。
- VALUE 式関数のみを使用している。
- 式のオーバーライドを使用して、パーシスタンス、Until 節、または動的しきい値処理を指定していない。
- AutoStart を実行するよう定義されている。
- 他のシチュエーションは組み込まれていない。
- 他のシチュエーションの表示項目名と一致する (表示項目が使用されている場合のみ該当)。

リフレックス・オートメーションに関する考慮事項

IBM Tivoli Monitoring V6.3 では、リフレックス・アクションが含まれているシチュエーションに duper が自動的に適用されます。追加構成は不要です。

Tivoli Enterprise Portal でリフレックス・アクションが ◉ **「管理対象システム (エージェント) でアクションを実行する」**に設定されているシチュエーションが多数存在する場合は、KBBENV ファイルでモニター・サーバーの環境変数 KMS_EVAL_REFLEX_AT_TEMS=Y を設定し、duper 最適化レベルを高くすることができます。

環境内の各モニター・サーバーで KMS_EVAL_REFLEX_AT_TEMS 環境変数を設定します。これにより、アクションの評価はモニター・サーバー上の duper により処理されます。ただし、アクションは引き続き管理対象システムに送信されます。この変数を実装する場合、アクションを実行するために管理対象システムがモニター・サーバーに接続している必要があります。

重要: KMS_EVAL_REFLEX_AT_TEMS 環境変数は注意してご使用ください。

注: ◉ **「管理システム (TEMS) でアクションを実行する」**を設定している場合、KMS_EVAL_REFLEX_AT_TEMS 変数はシチュエーションには影響しません。

duper シチュエーションの _Z_ ID

エージェントの LG0 ログ (例えば `C:¥ibm¥ITM¥TMAITM6¥logs¥Primary_IBM_MyComputer_NT.LG0`) を調べることにより、duper シチュエーションがエージェントからデータを収集していることを確認することができます。複数のシチュエーションがモニターしている属性グループでエージェントがシチュエーションを開始していることを示す、**_Z_** で始まる項目が生成されます。例: `Starting _Z_WTSYSTEM0 <3207594896,3996125040> for KNT.WTSYSTEM`。

duper の使用不可化

あるパラメーターをモニター・サーバーに追加することにより、duper プロセスを使用不可にできます。これを行うには、`CMS_DUPER=NO` という行を KBBENV ファイルに追加します。

モニター・サーバーのリサイクル時に、duper はスキップされます。

モニター・サーバー環境変数ファイル KBBENV (Windows) および KDSENV (z/OS) を編集するには、次の手順に従います。

Windows

Tivoli Enterprise Monitoring Services の管理 (「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」) を使用して、環境ファイルを編集します。変更するコンポーネントを右クリックして、「**拡張**」→「**ENV ファイルの編集**」をクリックします。変更内容を実装するには、コンポーネントをリサイクルする必要があります。

Linux UNIX

環境ファイルを直接編集します。*<install_dir>*/config/ms.ini ファイルの環境変数を編集してから、モニター・サーバーを再構成およびリサイクルして変更を実装します。

z/OS

詳しくは、「*Tivoli Enterprise Monitoring Server on z/OS の構成*」を参照してください。

Tivoli Enterprise Monitoring Automation Server 構成設定

Tivoli Enterprise Monitoring Automation Server はハブ Tivoli Enterprise Portal Server の機能を拡張し、Open Services Lifecycle Collaboration Performance Monitoring (OSLC) サービス・プロバイダーが含まれています。

Tivoli Enterprise Monitoring Automation Server の編集

Tivoli Enterprise Monitoring Automation Server 環境ファイル KASENV を編集し、オートメーション・サーバーのパラメーターを再構成します。

このタスクについて

オートメーション・サーバー環境ファイルを編集するには、以下のステップを実行してください。

手順

1. ハブ・モニター・サーバーがインストールされているコンピューター上で、環境ファイルを開きます。
   - Windows Tivoli Enterprise Monitoring Services の管理 (「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」) で「Tivoli Enterprise Monitoring Automation Server」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックして、KASENV ファイルを開きます。
   - Linux UNIX *install_dir* /config ディレクトリーに移動し、テキスト・エディターで as.ini ファイルを開きます。
2. このファイルを編集して、任意の環境変数を有効化 (行の先頭にある # を削除)、無効化 (行の先頭に # を入力)、または変更します。
3. ファイルを保存して、テキスト・エディターを終了します。
4. サービスをリサイクルするかどうかを尋ねるメッセージが表示されたら、「**はい**」をクリックします。変更内容を実装するには、オートメーション・サーバーをリサイクルする必要があります。

第 5 章 ユーザー認証の使用可能化

Tivoli Enterprise Portalクライアント へのログイン・アクセスは、Tivoli Enterprise Portal Server に対して定義されたユーザー・アカウントにより制御されます。パスワード認証は、レジストリー (ハブ・モニター・サーバーのオペレーティング・システムのユーザー・レジストリーか、ハブ・モニター・サーバーまたはポータル・サーバーで構成されている外部 LDAP ユーザー・レジストリーのいずれか) によって制御されます。

ハブ Tivoli Enterprise Monitoring Server への tacmd CLI ログイン・アクセスおよび SOAP クライアント要求は、モニター・サーバーのオペレーティング・システム・レジストリーまたはハブ・モニター・サーバーで構成されている外部 LDAP サーバーのいずれかを使用してハブ・モニター・サーバーに定義されているユーザー・アカウントによって制御されます。

IBM Dashboard Application Services Hub へのログイン・アクセスは、オペレーティング・システム・ユーザー・レジストリー、LDAP ユーザー・レジストリー、またはカスタム・スタンドアロン・ユーザー・レジストリーによって制御されます。IBM Dashboard Application Services Hub でモニター・ダッシュボード・アプリケーションまたはカスタム・モニター・ダッシュボードを使用する予定で、ダッシュボード・ユーザーが資格情報を求めるプロンプトなしで Tivoli Enterprise Portal クライアントを起動できるようにする場合、およびユーザーごとにモニター対象リソースに対する許可を制御する場合は、統合 LDAP ユーザー・レジストリーとシングル・サインオンを使用するように Tivoli Enterprise Portal Server および Dashboard Application Services Hub を構成する必要があります。31 ページの『第 3 章 ダッシュボード環境の準備』のロードマップを参照して、統合 LDAP ユーザー・レジストリーとシングル・サインオンを使用するかどうかを判別してください。

Tivoli Enterprise Monitoring Automation Server の Open Services Lifecycle Collaboration Performance Monitoring サービス・プロバイダー・コンポーネントへのログイン・アクセスは、LDAP ユーザー・レジストリーと Jazz for Service Management のセキュリティー・サービス・コンポーネントによって制御されます。

sysadmin ユーザー ID

完全な管理者権限がある初期の **sysadmin** ユーザー ID がインストール時に与えられるため、Tivoli Enterprise Portal クライアントにログオンしてユーザー・アカウントをさらに追加することができます。ハブ・モニター・サーバーが ☑ 「**セキュリティー: ユーザーを検証**」が使用可能に構成されている場合を除き、ポータル・クライアントへのログオンにパスワードは必要ありません。

Tivoli Enterprise Portalユーザー・プロファイル

Tivoli Enterprise Portal クライアントを使用してログインするには、ユーザーはポータル・サーバーで認証される必要があり、Tivoli Enterprise Portal ユーザー ID を持っていなければなりません。Tivoli Enterprise Portal に定義されている各ユーザー ID には、ユーザーに対してポータル・クライアントのどの機能を表示および使用することを許可するか、ユーザーに対してど

のモニター対象アプリケーションを表示することを許可するか、およびユーザーがどのナビゲーター・ビュー (およびビュー内の最上位レベル) にアクセスできるかを決定する一連の許可が割り当てられます。

同じ許可を持つユーザー ID をユーザー・グループとして編成し、許可に対する変更がすべてのメンバー・ユーザー ID に適用されるようにすることができます。

Dashboard Application Services Hub およびポータル・サーバーがシングル・サインオン用に構成されている場合は、モニター・ダッシュボード・ユーザーごとに Tivoli Enterprise Portal ユーザー ID が存在する必要があります。ダッシュボード・ユーザーがモニター・データに初めてアクセスすると、ユーザーの LDAP 識別名にマップされたユーザー ID がまだ存在しない場合は、そのユーザーの Tivoli Enterprise Portal ユーザー ID が自動的に作成されます。この場合、Tivoli Enterprise Portal ユーザー ID はランダム生成 ID になり、ユーザーには許可が一切割り当てられません。許可ポリシーではなく、Tivoli Enterprise Portal の許可を使用して、ダッシュボードでのモニター対象リソースへのアクセスを制御する場合、またはダッシュボード・ユーザーが Tivoli Enterprise Portal を起動できる場合は、ユーザー ID に許可とアクセスできるモニター対象アプリケーションを割り当てます。

Tivoli Enterprise Portal の許可およびモニター・アプリケーションの割り当てについて詳しくは、171 ページの『第 6 章 Tivoli Enterprise Portal ユーザー許可の使用』を参照してください。

ハブ・モニター・サーバーを使用した認証

ハブ・モニター・サーバーを介して認証されるユーザー ID は、ローカル・オペレーティング・システムのレジストリーまたは外部の LDAP 対応の中央ユーザー・レジストリーのいずれかによって認証を行うことができます。

ハブ・モニター・サーバーに要求を送信する **tacmd** コマンドを使用するユーザー ID または SOAP サーバー要求を行うユーザー ID は、ハブ・モニター・サーバーで認証される必要があります。

制限事項:

1. LDAP 認証は、z/OS 上のハブ・モニター・サーバーではサポートされていません。
2. Tivoli Enterprise Monitoring Server で使用される Tivoli Directory Server LDAP クライアントは、Microsoft Active Directory でサポートされているような LDAP 参照をサポートしません。
3. ハブ・モニター・サーバーが分散オペレーティング・システムにインストールされていて、Tivoli Enterprise Portal ユーザーの認証に使用される場合、Tivoli Enterprise Portal ユーザー ID は、10 文字以下でなければなりません。ただし、ハブ・モニター・サーバーで認証される SOAP クライアント・ユーザーおよび **tacmd** CLI ユーザーの場合、ユーザー ID は最大で 15 文字にすることができます。
4. ハブ・モニター・サーバーが z/OS にインストールされていて、z/OS で認証に RACF® (Resource Access Control Facility) セキュリティーを使用する場合は、ユーザー ID の長さは 8 文字に制限されます。

ポータル・サーバーを使用した LDAP 認証

ポータル・サーバーは、Tivoli Enterprise Portal ユーザー、モニター・デー

タにアクセスする Dashboard Application Services Hub ユーザー、IBM Tivoli Monitoring グラフ Web サービス・ユーザー、およびポータル・サーバーに要求を送信するコマンドを使用する **tacmd** CLI ユーザーを認証します。

デフォルトでは、ポータル・サーバーは、ハブ・モニター・サーバーに接続して認証を実行します。ただし、以下のシナリオでは、統合 LDAP ユーザー・レジストリーを使用して独自の認証を実行するようにポータル・サーバーを構成するのがベスト・プラクティスです。

- Tivoli Enterprise Portal が他の Web ベース・アプリケーションから起動され、ユーザーが資格情報を再入力しなくても済むようにする。
- Tivoli Enterprise Portal を使用して他の Web ベース・アプリケーションまたは Web 対応アプリケーションを起動し、ユーザーが資格情報を再入力しなくても済むようにする。
- IBM Dashboard Application Services Hub を使用して、ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントによって取得したモニター・データを表示する。この場合は、シングル・サインオンを使用するのがベスト・プラクティスです。これにより、ダッシュボード・ユーザーは、資格情報を再入力することなく、Tivoli Enterprise Portal を起動できるようになります。また、ユーザーごとにモニター対象リソースに対する許可を制御する場合にも、シングル・サインオンを使用する必要があります。
- IBM Tivoli Monitoring グラフ Web サービスが Tivoli Integrated Portal などの別のアプリケーションで使用されている。

LDAP サーバーで認証するようにポータル・サーバーを構成した場合、ユーザーは、Tivoli Enterprise Portal ユーザー ID ではなく、LDAP 相対識別名 (通常、`cn=` または `uid=` 値にマップされます) を使用して、Tivoli Enterprise Portal にログインします。ポータル・サーバーは Tivoli Enterprise Portal ユーザー ID を使用して許可を制御するため、LDAP 識別名を Tivoli Enterprise Portal ユーザー ID にマップする必要があります。Tivoli Enterprise Portal ユーザー ID は 10 文字までに制限されていますが、LDAP 識別名はこれより大幅に長いものにすることができます。

Tivoli Enterprise Monitoring Services の管理 ユーティリティー、**itmcmd** コマンド行インターフェース (Linux および UNIX の場合)、または TEPS/e 管理コンソール (ISCLite) を使用して、LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成できます。TEPS/e 管理コンソールを使用して LDAP を構成する場合は、各ポータル・サーバーの再始動後に Tivoli Enterprise Monitoring Services の管理を使用して ISCLite を手動で再始動する必要があります。

ハブ・モニター・サーバーおよびポータル・サーバーを使用した認証

ハブ・モニター・サーバーとポータル・サーバーは、両方のサーバーへのログイン・アクセスが必要なユーザーが存在する場合、同じ LDAP サーバーに接続できます。**tacmd login** コマンドで使用するものと同じユーザー ID でTivoli Enterprise Portal クライアントにログインできます。これを行うには、ポータル・クライアントで 「**ユーザー管理**」にアクセスして、Tivoli Enterprise Portal ユーザー ID を、ポータル・サーバーの LDAP ユーザー・

レジストリーで使用される識別名にマップする必要があります。レジストリーは、デフォルトでは、o=DEFAULTWIMITMBASEDREALM を使用する識別名ではなく、o=ITMSSOEntry を使用します。

ハブからポータル・サーバーへの LDAP 認証のマイグレーション

使用しているハブ・Tivoli Enterprise Monitoring Serverが LDAP ユーザー・レジストリーに対してユーザーを認証するよう既に構成されており、同じ LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成したい場合は、Tivoli Enterprise Portal の「ユーザー管理」ウィンドウでユーザー ID に設定されている識別名を変更する必要があります。

ユーザー認証のためのロードマップ

ユーザー認証を開始するには、以下のロードマップを使用します。

表 8. ユーザー認証のためのロードマップ

タスク	情報の入手先
ローカル・オペレーティング・システム・ユーザー・レジストリーまたは LDAP ユーザー・レジストリーのいずれかを使用して、ハブ・モニター・サーバーを介したユーザー認証をセットアップします。	『ハブ・モニター・サーバーを使用したユーザー認証』
シングル・サインオンが IBM Dashboard Application Services Hub または他のアプリケーションで使用される場合に、ユーザーの認証に LDAP ユーザー・レジストリーを使用するようにポータル・サーバーをセットアップします。	ハブ・モニター・サーバーが LDAP ユーザー・レジストリーを使用していない場合は、100 ページの『ポータル・サーバーを使用した LDAP ユーザー認証』を参照してください。 ハブ・モニター・サーバーが LDAP ユーザー・レジストリーを使用している場合は、132 ページの『モニター・サーバーからポータル・サーバーへの LDAP 認証のマイグレーション』を参照してください。
OSLC クライアントからの HTTP GET 要求を認証するように Tivoli Enterprise Monitoring Automation Server およびその Performance Monitoring サービス・プロバイダーをセットアップします。	134 ページの『Tivoli Enterprise Monitoring Automation Serverを使用した認証』

ハブ・モニター・サーバーを使用したユーザー認証

ハブ・モニター・サーバーを使用したユーザー認証は、ローカル・オペレーティング・システムのユーザー・レジストリーまたは LDAP 対応の外部中央レジストリーのいずれかを使用します。

ハブ・モニター・サーバー上で認証を構成する場合の前提条件

ハブ・モニター・サーバーでユーザー認証を使用可能化する前に、以下のタスクを完了します。

このタスクについて

表 9. 認証を構成する前に実行するタスク

タスク	情報の入手先
Tivoli Enterprise Portal ユーザー・アカウントのセットアップ。	180 ページの『ユーザー ID の追加』
認証レジストリーにおけるユーザー・アカウントのセットアップ。	ローカル・オペレーティング・システムまたは LDAP ディレクトリー・サーバーでユーザー・アカウントをセットアップするための資料を参照してください。 z/OS でのユーザーのセットアップについては、「*Tivoli Enterprise Monitoring Server on z/OS の構成*」を参照してください。 **注:** • ハブ・モニター・サーバーが分散オペレーティング・システムにインストールされていて、Tivoli Enterprise Portal ユーザーの認証に使用される場合、Tivoli Enterprise Portal ユーザー ID は、10 文字以下でなければなりません。ただし、ハブに要求を送信する **tacmd** CLI コマンドのみを使用するハブ・モニター・ユーザーまたは SOAP 要求を送信するハブ・モニター・ユーザーは、最大で 15 文字のユーザー ID を持つことができます。 SOAP および tacmd コマンド・ユーザーのパスワードも 15 文字以下に制限されます。 • ハブ・モニター・サーバーが z/OS にインストールされていて、z/OS で認証に RACF (Resource Access Control Facility) セキュリティーを使用する場合は、ユーザー ID の長さは 8 文字に制限されます。
ハブと LDAP サーバー間の TLS/SSL 通信のセットアップ。	230 ページの『ハブ・モニター・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』

ハブ・Tivoli Enterprise Monitoring Serverを使用して認証する予定の場合は、Tivoli Enterprise Portal Server のログイン ID に対するユーザー・アカウントが、認証が有効となる前に認証レジストリーでセットアップされていることを確認してください。認証が有効化された後に **sysadmin** がログインできるように、ハブ・コンピューターのローカル・オペレーティング・システムのユーザー・レジストリーには、少なくとも **sysadmin** ユーザー ID を追加します。

注: Windows の場合は、インストーラーによって **sysadmin** ユーザー・アカウントが Windows ユーザー・レジストリーに作成され、ユーザーはこの ID のパスワードを指定するよう要求されます。パスワード認証が使用可能でない場合、パスワードは必要ありません。

ヒント: Windows インストーラーでは、**sysadmin** アカウントが作成されている場合、「パスワードを無期限にする」オプションは設定されません。このオプション

を設定しないと、ハブ・コンピューターのセキュリティー・ポリシーに従ってパスワードの有効期限が切れるため、ユーザーはポータル・サーバーにログインすることができなくなります。Windows 管理ツールを使用すると、**sysadmin** ユーザー・アカウントに対して、「パスワードを無期限にする (Password never expires)」オプションが選択されていることを確認することができます。

認証を使用可能にする前に、以下の情報を取得します。

手順

- 認証に外部 LDAP サーバーを使用している場合は、以下のテーブルに示す情報を LDAP 管理者から取得してから、ユーザー認証を構成します。

表 10. LDAP 構成パラメーター

パラメーター	説明

LDAP ユーザー・フィルター	Tivoli Enterprise Portal ユーザー ID を LDAP ログイン ID にマップする場合に使用する属性。この属性には、Tivoli Enterprise Portal ログイン ID と同じ名前が含まれている必要があります。通常、LDAP ユーザー・フィルターでは、このポータル・ユーザー ID は「%v」と表示されます。例:
	`IBM Tivoli Directory Server: (&(mail=%v@yourco.com) (objectclass=inetOrgPerson))`
	`Microsoft Windows Active Directory: (&(mail=%v@yourco.com) (objectclass=user))`
	`Sun Java System Directory Server: (&(mail=%v@yourco.com) (objectclass=inetOrgPerson)`
	
	すべての LDAP にそのユーザーのメール属性があるわけではありません。例えば、LDAP 管理者が共通名のみを設定する場合もあり、この場合、フィルターは以下のようになります。
	`(&(cn=%v) (objectclass=inetOrgPerson))`
	
	Tivoli Enterprise Portal 管理者は、ユーザーの検索にどの LDAP 属性を使用する必要があるかを正確に検証する必要があります。例えば、Active Directory を使用する場合、cn は Active Directory ユーザーのフルネームと一致し、このフルネームは Tivoli Monitoring ユーザーのフルネームと正確に一致する必要があります。スペースは使用することができません (例えば、「S Smith」は「SSmith」となる必要があります)。

LDAP ベース	ユーザーの検索に使用される LDAP ユーザー・レジストリーの LDAP ベース・ノード。例:
	`IBM Tivoli Directory Server: dc=yourdomain,dc=yourco,dc=com`
	`Microsoft Windows Active Directory: dc=yourdomain,dc=yourco,dc=com`
	`Sun Java System Directory Server: dc=yourdomain,dc=yourco,dc=com`

LDAP バインド ID	バインド認証に使用する LDAP 表記の LDAP ユーザー ID。この LDAP ユーザー ID は、LDAP ユーザーの検索を許可されている必要があります。匿名ユーザーが LDAP ユーザーを検索できる場合、この値は省略可能です。
LDAP バインド・パスワード	LDAP バインド認証用のパスワード。匿名ユーザーがご使用の LDAP サーバーにバインドできる場合、この値は省略可能です。この値はインストーラーによって暗号化されます。
LDAP ホスト名	LDAP サーバーのホスト名。ご使用の LDAP サーバーが Tivoli Enterprise Monitoring Server と同じホスト上にある場合、この値は省略可能です (デフォルトは localhost です)。

表 10. LDAP 構成パラメーター (続き)

パラメーター	説明
LDAP ポート番号	LDAP サーバーのポート番号。ご使用の LDAP サーバーがポート 389 を listen している場合、この値は省略可能です。

- Microsoft Active Directory を使用している場合は、135 ページの『Microsoft Active Directory を使用した LDAP ユーザー認証』を参照して、このタイプの LDAP サーバーに固有の計画情報と構成情報を確認してください。
- ハブ・Tivoli Enterprise Monitoring Serverと LDAP サーバー間の TLS/SSL 通信を使用する予定の場合は、以下の表で説明されている情報を取得してください。

表 11. ハブと LDAP サーバー間の通信用の TLS/SSL パラメーター

パラメーター	説明
LDAP 鍵ストア・ファイル	GSKit 鍵ストアのデータベース・ファイルのロケーション。任意のロケーションを指定することができます。例: `C:¥IBM¥ITM¥keyfiles`
LDAP 鍵ストア・スタッシュ	GSKit データベース・パスワード・ファイルの場所。例: `C:¥IBM¥ITM¥keyfiles¥keyfile.sth`
LDAP 鍵ストア・ラベル	鍵ストア・ラベル例: `IBM_Tivoli_Monitoring_Certificate`
LDAP 鍵ストア・パスワード	鍵ストアにアクセスするために必要なパスワード

構成手順

Windows ベース、Linux ベース、または UNIX ベースのハブ・モニター・サーバー上で、ユーザー認証を構成します。

z/OS 上にインストールされたハブ・モニター・サーバーにおける認証の構成方法については、「*IBM Tivoli Management Services on z/OS: Tivoli Enterprise Monitoring Server on z/OS* の構成」を参照してください。外部の LDAP レジストリーによる認証は、z/OS ハブではサポートされていません。

Windows: ハブを使用したユーザー認証の構成

Windows 上でハブ・Tivoli Enterprise Monitoring Serverを構成し、ユーザーを認証します。

このタスクについて

Windows コンピューター上のハブ経由でユーザー認証を構成するには、次の手順を実行します。

手順

1. 「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Monitoring Services の管理**」の順に選択します。
2. ハブ・モニター・サーバーを右クリックし、「**再構成**」を選択します。

3. 表示される構成ウィンドウで、「**セキュリティー: ユーザーを検証**」を選択します。 オプション「**LDAP セキュリティー: LDAP でユーザーを検証**」を使用することができるようになります。
4. ユーザー認証に LDAP を使用する場合は、「**LDAP でのユーザー検証**」オプションをチェックし、「**OK**」をクリックして「LDAP」ウィンドウを開きます。ローカル・レジストリーを使用する必要がある場合は、ステップ 7 へスキップします。
5. 使用するサイトに適した値となるよう、必要な LDAP 値を指定します。
6. ハブと LDAP サーバー間の通信を保護するために TLS/SSL を使用する必要がある場合は、「**LDAP SSL 通信: SSL を使用しますか?**」をチェック・マークを付けます。次に、適切な値を指定します。必要に応じて、鍵ストアにパスワードを設定します。
7. 「**OK**」をクリックします。 「ハブ TEMS の構成」ウィンドウが表示されます。
8. 「**OK**」をクリックして、現行の設定を受け入れます。
9. 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、ハブ・モニター・サーバーの名前を右クリックし、「**開始**」を選択して再始動します。

Linux または UNIX: ハブを使用したユーザー認証の構成

Linux または UNIX にハブがインストールされた環境で、ユーザー認証を構成します。

コマンド行からのユーザー認証の構成:

以下の手順を使用して、コマンド行からユーザー認証を構成することができます。

このタスクについて

コマンド行からハブを構成するには、以下の手順を実行します。

手順

1. *install_dir*/bin ディレクトリーに移動して、以下のコマンドを実行します。

   ```
   ./itmcmd config -S -t tems_name
   ```

   ここで、*install_dir* とは IBM Tivoli Monitoring のインストール・ディレクトリーであり、*tems_name* とはハブ・モニター・サーバーの名前です。Linux または UNIX 上のデフォルトのインストール・ディレクトリーは、 /opt/IBM/ITM です。以下のようなプロンプトが表示されます。

   ```
   TEMS を構成中...
   ```

2. 以下のプロンプトに対して、デフォルトを受け入れます。インストール中に行われた選択内容がデフォルトに反映されているはずです。
3. 以下のようなプロンプトが表示されます。

   ```
   セキュリティー: ユーザーを検証しますか?
   ```

   1 と入力して Enter キーを押します。
4. 認証に LDAP を使用しないようにする必要がある場合は、Enter キーを押してデフォルト (いいえ) を選択します。認証に LDAP を使用する必要がある場合は、

1 と入力して Enter キーを押します。値を入力して、以下のプロンプトに応答します。ハブと LDAP サーバー間の TLS/SSL 通信を有効にするには、適切な値を指定します。

5. Tivoli Event Integration Facility およびワークフロー・ポリシー/Tivoli Emitter Agent 転送に対するデフォルトを受け入れます。
6. 以下のプロンプトで、6 (保存/終了) と入力し、Enter キーを押します。

   ```
   ハブ
   ##      CMS_Name
   1       ip.pipe:elsrmt1[4441]
   ```

7. 以下のように、ハブ・Tivoli Enterprise Monitoring Serverを再始動します。

   ```
   ./itmcmd server stop tems_name
   ./itmcmd server start tems_name
   ```

「Tivoli Enterprise Monitoring Services の管理」を使用した認証の構成:

「Tivoli Enterprise Monitoring Services の管理」を使用した認証を構成します。

このタスクについて

「Tivoli Enterprise Monitoring Services の管理」を使用して認証を構成するには、以下のステップを実行します。

手順

1. *install_dir* /bin ディレクトリーに移動して、以下のコマンドを実行します。

   ```
   ./itmcmd manage [-h install_dir ]
   ```

   ここで、*install_dir* は、IBM Tivoli Monitoring のインストール・ディレクトリーです。Linux または UNIX 上のデフォルトのインストール・ディレクトリーは、 /opt/IBM/ITM です。 「Tivoli Enterprise Monitoring Services の管理」ウィンドウが表示されます。
2. ハブ・モニター・サーバーを右クリックして、「**構成**」をクリックします。
3. 「**拡張設定**」タブをクリックします。「**セキュリティー: ユーザーの検証 (Security: Validate User)**」を選択します。
4. ユーザーの認証にシステム・レジストリーではなく LDAP を使用する必要がある場合は、「**LDAP ユーザー認証**」を選択します。
5. 「**OK**」をクリックします。 LDAP オプションを選択した場合は、LDAP 構成パネルが表示されます。
6. 値を指定して、「**OK**」をクリックします。
7. 「**OK**」をクリックします。
8. 以下のいずれかの方法で、ハブ・モニター・サーバーを再始動します。
   - 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、ハブ・モニター・サーバーを右クリックし、「**リサイクル**」を選択します。
   - コマンド行から、以下のように入力します。

     ```
     ./itmcmd server stop tems_name
     ./itmcmd server start tems_name
     ```

LDAP 情報の取得のための Ldapsearch

Ldapsearch は、構成の前に LDAP 情報を検証したり、構成中に発生した問題をトラブルシューティングしたりする場合に使用できるコマンド行ツールであり、LDAP サーバーのベンダーから入手できます。 **ldapsearch** を実行することにより、LDAP 認証用にハブ・モニター・サーバーを構成する前の LDAP 情報の検証時間を大幅に節約することができます。

注: このツールは、ハブ・モニター・サーバーを使用して LDAP 認証を構成する場合にのみ使用してください。Tivoli Enterprise Portal Serverを使用して LDAP 認証を構成する場合は、TEPS/e (Tivoli Enterprise Portal Server の拡張サーバー) 管理コンソールを使用して、構成パラメーターを検証します。

ldapsearch は、LDAP 管理者によって実行されるのが理想的です。**ldapsearch** コマンドは、ping コマンドのように動作します。コマンドへの入力として使用した値が正しい場合、コマンドは、検索で使用する値のバージョンを返します。値が正しくない場合、コマンドは何も返さないか、またはどの値に問題があるか (誤りのあるパスワードまたは無効なホスト名など) を判断するのに役立つエラー・メッセージを返します。

IBM Tivoli Directory Server **ldapsearch** は IBM Tivoli Monitoringに最適です。Tivoli Directory Server **ldapsearch** は、Tivoli Monitoring で使用される GSKit TLS/SSL 操作をサポートしており、LDAP TLS/SSL 検索をサポートする追加のコマンド行オプションを提供しています。 Tivoli Monitoring は、実動インストールには ldapsearch を組み込みません。Tivoli Directory Server ldapsearch については、IBM セキュリティー・システム・インフォメーション・センターの「*Tivoli Directory Server Command Reference*」の『Client utilities』」を参照してください。

ldp.exe は、**ldapsearch** ツールと同じ基本機能を備えた Microsoft Windows LDAP 検索ツールです。このツールは、ご使用の Windows のバージョンに合ったものを Microsoft の Web サイトからダウンロードできます。**ldp.exe** ツールは、Windows Server 2003 CD サポート・ツールに含まれています。Microsoft Windows **ldp** コマンドの使用について詳しくは、http://support.microsoft.com/kb/224543 を参照してください。

LDAP 構成に役立つほかのツールとして、Softerra が提供する LDAP Browser ツールがあります。

ldapsearch コマンド行オプション

以下の表は、コマンド行での ldapsearch オプションと、モニター・サーバー構成ファイルにある対応するパラメーターを示しています。

表 12. ldapsearch コマンド行オプション、および対応するモニター・サーバーの構成パラメーター

オプション	説明	モニター・サーバー構成ファイルの対応するパラメーター
-h *host*	LDAP サーバーのホスト名。	KGL_LDAP_HOST_NAME
-p *port*	LDAP ポート番号。	KGL_LDAP_PORT

表 12. ldapsearch コマンド行オプション、および対応するモニター・サーバーの構成パラメーター (続き)

オプション	説明	モニター・サーバー構成ファイルの対応するパラメーター
-D *dn*	LDAP バインド ID。 LDAP バインド ID を必要としない場合は、このコマンド行オプションは使用しないでください。	KGL_LDAP_BIND_ID
-w password	LDAP バインド・パスワード。 **ldapsearch** コマンド行オプションの暗号化されていない値を使用します。LDAP バインド ID を必要としない場合は、このコマンド行オプションは使用しないでください。	KGL_LDAP_BIND_PASSWORD
-b base_dn	LDAP ベース。	KGL_LDAP_BASE
-K keyfile	LDAP 鍵ストア・ファイル (LDAP SSL でのみ使用)。	KGL_KEYRING_FILE
-P key_pw	LDAP 鍵ストア・パスワード (LDAP TLS/SSL でのみ使用)。 ldapsearch コマンド行オプションの暗号化されていない値を使用します。	KGL_KEYRING_PASSWORD (暗号化解除された値)
-N key_name	LDAP 鍵ストア・ラベル (LDAP SSL でのみ使用)。	KGL_KEYRING_LABEL
フィルター	LDAP ユーザー・フィルター。%v を Tivoli Enterprise Portal、SOAP、または tacmd ユーザー ID に置き換えます。	KGL_LDAP_USER_FILTER

ldapsearch コマンドのサンプル (TLS/SSL 不使用)

TLS/SSL を使用不可に構成する場合の ldapsearch コマンドのサンプルおよび対応する出力データを以下に示します。

TLS/SSL が使用可能になっておらず、ユーザー ID やパスワードを必要としない環境で ldapsearch コマンドを構成するには、以下の値を使用します。

LDAP ホスト名	ldap.itm62.com
LDAP ポート名	389
LDAP ベース	ou=itm62users,o=itm62.com
LDAP ユーザー・フィルター	"(mail=%v@us.ibm.com)"

このサンプル構成には以下のコマンド構文を使用します。

```
ldapsearch -h ldap.itm62.com -p 389 -b "ou=itm62users,o=itm62.com"
 -s sub "(mail=sysadmin@itm62.com)"
```

以下の出力が生成されます。

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

ldapsearch コマンドのサンプル (TLS/SSL 使用)

TLS/SSL を使用可能に構成する場合の ldapsearch コマンドのサンプルおよび対応する出力データを以下に示します。

TLS/SSL が使用可能で、バインド ID とパスワードが必要な環境で ldapsearch コマンドを構成するには、以下の値を使用します。

LDAP ホスト名	ldap.itm62.com
LDAP ポート名	636
LDAP バインド ID	uid=1,ou=itm62users,o=itm62.com
LDAP バインド・パスワード	itm62
LDAP ベース	ou=itm62users,o=itm62.com
LDAP 鍵ストア	C:¥IBM¥ITM¥itm62keyfiles¥keyfile.kdb
LDAP 鍵スタッシュ	C:¥IBM¥ITM¥itm62keyfiles¥keyfile.sth
LDAP 鍵ストア・ラベル	BM_Tivoli_Monitoring_Certificate
LDAP 鍵ストア・パスワード	itm62
LDAP ユーザー・フィルター	"(mail=%v@us.ibm.com)"

このサンプル構成には以下のコマンド構文を使用します。

```
ldapsearch -h ldap.itm62.com -p 636 -D uid=1,ou=itm62users,o=itm62.com
    -w itm62 -b "ou=itm62users,o=itm62.com" -s sub
    -K C:¥IBM¥ITM¥itm62keyfiles¥keyfile.kdb -P itm62
    -N "IBM_Tivoli_Monitoring_Certificate" "(mail=sysadmin@itm62.com)"
```

以下の出力が生成されます。

```
uid=12345678,ou=itm62users,o=itm62.com
objectClass=person
objectClass=organizationalPerson
...
mail=sysadmin@itm62.com
...
```

ポータル・サーバーを使用した LDAP ユーザー認証

LDAP ユーザー・レジストリーを使用してユーザーを認証するように Tivoli Enterprise Portal Server を構成することができます。

以下のシナリオでシングル・サインオン (SSO) 機能を提供する場合は、これは必須です。

- Tivoli Enterprise Portal が他の Web ベース・アプリケーションから起動され、ユーザーが資格情報を再入力しなくても済むようにする。

- Tivoli Enterprise Portal を使用して他の Web ベース・アプリケーションまたは Web 対応アプリケーションを起動し、ユーザーが資格情報を再入力しなくても済むようにする。
- IBM Dashboard Application Services Hub を使用して、ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントによって取得したモニター・データを表示する。この場合は、シングル・サインオンを使用するのがベスト・プラクティスです。これにより、ダッシュボード・ユーザーは、資格情報を再入力することなく、Tivoli Enterprise Portal を起動できるようになります。また、ユーザーごとにモニター対象リソースに対する許可を制御する場合にも、シングル・サインオンを使用する必要があります。
- IBM Tivoli Monitoring グラフ Web サービスが Tivoli Integrated Portal などの別のアプリケーションで使用されている。

ポータル・サーバー上で LDAP 認証を構成するための前提条件

Tivoli Enterprise Portal Server で LDAP 認証を構成する前に、Tivoli Enterprise Portal のユーザー・アカウントおよび認証する LDAP レジストリーのユーザー・アカウントを作成し、LDAP レジストリー構成パラメーターを手元に用意する必要があります。

LDAP レジストリーのユーザー ID の検証

レジストリーにユーザー ID を追加するか、またはレジストリーのユーザー ID を確認します。ただし、認証を使用可能に設定して Tivoli Enterprise Portal にログインするまでは、**sysadmin** のアカウントを作成しないでください。

Tivoli Enterprise Portal Server の拡張サービス (TEPS/e) 管理者のデフォルトのユーザー名は **wasadmin** です。この UID がレジストリーに追加されている場合、ユーザー・レジストリー管理者にこの名前を変更してもらうか、またはこの項目を削除してもらいます。統合 LDAP ユーザー・レジストリーでは、同じ名前のエントリーが 2 つあると競合が発生します。

LDAP ユーザー・レジストリーには **sysadmin** を追加しないことがベスト・プラクティスです。LDAP サーバーが使用不可の場合は、LDAP ユーザー・アカウントを使用して Tivoli Enterprise Portal にログオンすることはできませんが、**sysadmin** を使用してポータルへログオンすることは可能です。これは、ポータルがハブ・モニター・サーバーによって認証されているデフォルトの Tivoli Monitoring レルムにマップされているためです。

Tivoli Enterprise Portal ユーザー・アカウントのセットアップ

LDAP レジストリーで認証するユーザー ID を追加します。これは、LDAP 認証のためにポータル・サーバーを構成する前でも後でも構いません。LDAP 構成の後、ポータル・クライアントの「ユーザー管理」ウィンドウに戻り、ユーザー ID を LDAP ユーザー・レジストリーの識別名に関連付ける必要があります。

Windows **sysadmin パスワード**

IBM Tivoli Monitoring Windows インストーラーによって **sysadmin** ユーザー・アカウントが、ハブ・モニター・サーバー・コンピューター上の

Windows ユーザー・レジストリーに作成され、この ID のパスワードを指定するようプロンプトが出されます。パスワード認証が使用可能でない場合、パスワードは必要ありません。

インストーラーでは、**sysadmin** アカウントの作成時に「パスワードを無期限にする」オプションは設定されません。このオプションを設定しないと、ハブ・Tivoli Enterprise Monitoring Serverのセキュリティー・ポリシーに従ってパスワードの有効期限が切れ、ポータル・サーバーにログインすることができなくなります。Windows の管理ツールを使用して、**sysadmin** ユーザー・アカウントに対して「パスワードを無期限にする」オプションを選択するようにしてください。

LDAP 構成情報

LDAP ユーザー認証のためにポータル・サーバーを構成する前に、以下の表に示す情報を LDAP 管理者から取得してください。ポータル・サーバーと関連 SSO アプリケーションは、同じ LDAP ユーザー・レジストリーを使用するように構成する必要があります。

表 13. LDAP 構成パラメーター

パラメーター	説明
LDAP タイプ	Tivoli Management Services インストール済み環境および構成ユーティリティーを使用して、ポータル・サーバーに対して以下のいずれかのタイプの LDAP サーバーを定義できます。 • Active Directory Server 2000 • Active Directory Server 2003 • Active Directory Server 2008 • Active Directory Server 2008 R2 • Tivoli Directory Server 6.x • その他 「**その他**」は、異なるタイプの LDAP サーバーを構成する場合、ポータル・サーバーと LDAP サーバー間で TLS/SSLを使用可能にする予定がある場合、またはこの表にリストされているパラメーター以外の拡張 LDAP 構成パラメーターを指定する必要がある場合に指定します。「**その他**」を選択するときは、TEPS/e 管理コンソール を使用して、LDAP ユーザー・レジストリーの詳細を構成および変更する必要があります。 117 ページの『TEPS/e 管理コンソールの使用』を参照してください。
LDAP ベース	このパラメーターは、LDAP レジストリーのベース・エントリーの識別名 (DN) を指定します。 これは、LDAP サーバー内のユーザー検索の開始点となります。例えば、`cn=John Doe,ou=Rochester,o=IBM,c=US` という識別名を持つユーザーの場合、このパラメーターに `ou=Rochester,o=IBM,c=US` と指定します。 **注:** TEPS/e 管理コンソールを使用して LDAP を構成する場合、TEPS/e 管理コンソールでは、このパラメーターは「**このリポジトリー内のベース・エントリーの識別名 (Distinguished name of the base entry in the repository)**」と呼ばれます。

表 13. LDAP 構成パラメーター (続き)

パラメーター	説明
LDAP DN ベース・エントリー	デフォルト値は o=ITMSSOEntry です。ただし、ベスト・プラクティスは、組織にとって意味が分かりやすい値を選択することです。 通常、このパラメーターは、ポータル・サーバー・ユーザーの LDAP レジストリーにおけるベース・エントリーの識別名に設定します。例えば、cn=John Doe,ou=Rochester,o=IBM,c=US という識別名を持つユーザーの場合、このパラメーターに ou=Rochester,o=IBM,c=US と指定します。 ただし、ポータル・サーバーに対して複数の LDAP リポジトリーが構成されている場合は、このフィールドを使用して、この LDAP サーバーの LDAP ユーザー・セットを一意的に識別する追加の識別名 (DN) を定義します。例えば、LDAP1 レジストリーと LDAP2 レジストリーがどちらもベース・エントリーとして o=ibm,c=us を使用するとします。このような場合は、このパラメーターを使用して、レルム内の各 LDAP サーバーに異なるベース・エントリーを一意的に指定します。例えば、LDAP1 レジストリーを構成するときは o=ibm1,c=us と指定し、LDAP2 レジストリーを構成するときは o=ibm2,c=us と指定します。 **注:** 複数の LDAP レジストリーがある場合、重複するユーザー名は使用できません。 Tivoli Enterprise Portal の「ユーザー管理」ダイアログで、Tivoli Enterprise Portal ユーザー ID にマップできる識別名をリストすると、このパラメーターの値が表示されます。 **注:** TEPS/e 管理コンソールを使用して LDAP を構成する場合、TEPS/e 管理コンソールでは、このパラメーターは「**レルム内のこのエントリー・セットを一意的に識別するベース・エントリーの識別名 (Distinguished name of the base entry that uniquely identifies this set of entries in the realm)**」と呼ばれます。
LDAP バインド ID	バインド認証に使用する LDAP 表記の LDAP ユーザー ID です。LDAP ユーザーの検索を許可されている必要があります。匿名ユーザーが LDAP ユーザーを検索できる場合、バインド ID は省略可能です。
LDAP バインド・パスワード	LDAP バインド認証用の LDAP ユーザー・パスワードです。匿名ユーザーがご使用の LDAP サーバーにバインドできる場合、この値は省略可能です。この値はインストーラーによって暗号化されます。
LDAP ポート番号	LDAP サーバーが listen しているポートの番号です。ポートが 389 である場合、この値は省略可能です。
LDAP ホスト名	これは、LDAP サーバーのホスト名または IP アドレスです。LDAP サーバーがポータル・サーバーと同じコンピューター上にある場合、この値は省略可能です。。 Microsoft Active Directory を使用している場合、ポータル・サーバー用のユーザー・アカウントをホストする Active Directory フォレスト内のドメイン・コントローラーのホスト名を使用します。

SSO 構成に関する情報

SSO を構成する場合、ポータル・サーバーでシングル・サインオンを使用する予定のある他のアプリケーションの管理者と協力して、以下の表にリストされているパラメーターの値を決定します。すべての関連 SSO アプリケーションで、これらのパラメーターの値を同じにする必要があります。

表 14. SSO パラメーター

パラメーター	説明
ドメイン名	は、SSO が構成されているインターネットまたはイントラネットのドメイン (例えば、mycompany.com) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。例: `ibm.com`
レルム名	レルムは、TEPS/e および他の WebSphere Application Server の統合リポジトリー・セットを識別します。独自のレルム名を選択できますが、この値は、指定したドメイン内で SSO に対して構成されるすべてのアプリケーションで同じである必要があります。同じドメイン名で構成されたアプリケーションでも、異なるレルム名で構成されている場合は、同じ SSO インフラストラクチャーの一部としては機能できません。 例: `ibm_tivoli_sso`

シングル・サインオンについて

シングル・サインオン (SSO) 機能を使用すると、ユーザー資格情報を再入力しなくても Tivoli Enterprise Portal から他の Tivoli Web ベース・アプリケーションまたは Web 対応アプリケーションを起動したり、他のアプリケーションから Tivoli Enterprise Portal を起動したりできます。また、SSO は IBM Dashboard Application Services Hub がポータル・サーバーからモニター・データを取得するときや、IBM Tivoli Monitoring グラフ Web サービスが他のアプリケーションによって使用されるときにも使用されます。

認証された資格情報は、LTPA (Lightweight Third Party Authentication) トークンを使用して、関連アプリケーションの間で共有されます。このトピックを読んで、SSO の使用法および要件を理解してください。

ユーザー・ログオン

ユーザーが関連アプリケーションのいずれか 1 つにログオンすると、ユーザー ID とパスワードが認証され、その後はユーザー ID とパスワードを再入力しなくても、元のアプリケーションから別のアプリケーションを起動して関連データを表示したり、必要なアクションを実行したりできます。

Tivoli Enterprise Portal ブラウザー・クライアントまたは Java Web Start クライアント ブラウザー・クライアントまたは Java Web Start クライアントを使用する場合、「**アプリケーションの起動**」を使用するか、またはアプリケーションの URL をブラウザー・ビューに入力することにより、Tivoli Enterprise Portal から別の関連する Tivoli web アプリケーションを起動できます。

SSO 対応 Web アプリケーションから Tivoli Enterprise Portal ブラウザー・クライアントを起動できます。Java Web Start クライアントの起動時にも SSO がサポートされます。

注: SSO を使用していて、Tivoli Enterprise Portal Server と同じコンピューター上のブラウザー・クライアントを使用する場合は、ホスト・コンピューターの完全修飾名を使用するようにクライアントを再構成する必要があります。

Tivoli Enterprise Portal デスクトップ・クライアント
デスクトップ・クライアントを使用すると、SSO を使用してワークスペースから別のアプリケーションを起動できます。そのためには、そのアプリケーションの URL をブラウザー・ビューのアドレス・フィールドに入力します。ただし、別のアプリケーションから Tivoli Enterprise Portal を起動してデスクトップ・クライアントを使用することはできません。

Dashboard Application Services Hub
ダッシュボード・ユーザーは、IBM Dashboard Application Services Hub にログオンします。ダッシュボード・ユーザーがモニター・データを表示するダッシュボードにアクセスすると、ダッシュボード・ハブがポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントに要求を送信、ログインしたユーザーの LTPA トークンを含めます。ポータル・サーバーはその LTPA トークンを検証し、LTPA トークンから LDAP ユーザー ID を取り出して、そのユーザーがアクセスを許可されているモニター対象リソースを判断します。

IBM Tivoli Monitoring グラフ Web サービス
ユーザーが Tivoli Integrated Portal にログオンすると、IBM Tivoli Monitoring グラフ Web サービスを使用するように構成されたグラフが表示されたページにアクセスできます。要求がポータル・サーバーのグラフ Web サービスに送信され、ログインしたユーザーの LTPA トークンが含まれます。ポータル・サーバーはその LTPA トークンを検証し、LTPA トークンから LDAP ユーザー ID を取り出して、そのユーザーがアクセスを許可されているモニター対象リソースを判断します。

SSO 対応アプリケーションは同一のセキュリティー・ドメインおよびレルムに属する
SSO を使用可能にする場合、すべての参加 Tivoli アプリケーションにより共有される外部 LDAP ユーザー・レジストリーに対して Tivoli Enterprise Portal Server を介して認証を構成する必要があります。これは、統合 LDAP ユーザー・レジストリーとも呼ばれます。すべての参加アプリケーションは、SSO 用に構成され、かつ同一のインターネットまたはイントラネットのドメインおよびレルムに属する必要があります。

このドメインは、SSO を構成する必要のある、mycompany.com のようなインターネットまたはイントラネットのドメインです。このドメインまたはそのサブドメイン内で使用できるアプリケーションのみを SSO で使用可能にします。

レルムは、LTPA SSO 実装を使用しているさまざまなアプリケーション全体で共有されるパラメーターです。

LTPA トークン
認証された資格情報は、LTPA トークンを使用して、関連アプリケーションの間で共有されます。 LTPA トークンは、共有 LDAP ユーザー・レジストリーを使用して既に認証されたユーザーの認証関連データを含む暗号化データです。関連 SSO アプリケーションは、ブラウザーの Cookie を使用してユーザーの LTPA トークンを渡します。

LTPA トークンは、セキュアな暗号方式を使用して作成されるため、セキュリティーで保護されています。トークンは、暗号化され署名されています。LTPA トークンを作成するサーバーは、暗号鍵セットを使用します。暗号鍵はトークンのエンコードに使用されます。このため、ユーザーのブラウザー

に渡された、エンコードされたトークンは、暗号鍵を持っていないユーザーにデコードされることはありません。暗号鍵は、トークンの完全性の確認や改ざんの迅速な検出を保証するトークンの検証にも使用されます。SSO サーバーは、HTTP 要求を受信して LTPA トークンが含まれていることを確認すると、そのトークンを共有の暗号鍵のコピーを使用して検証します。有効なトークンの情報により、サーバーがログイン・ユーザーを識別できます。

したがって、LTPA キーを関連 SSO サーバーの間で交換し、すべてのサーバーが同じ LTPA キーを使用するようにする必要があります。 LTPA キーのソースとするサーバーを 1 つ選択します。次に、その LTPA キーをエクスポートして、他のサーバーの管理者に提供し、インポートできるようにします。エクスポートの手順を実行するときは、キーをキー・ファイルにエクスポートする必要があります。キー・ファイルの名前とキーの暗号化に使用するパスワードを指定する必要があります。キー・ファイルとパスワードは、LTPA キーをインポートできるように、他の関連 SSO アプリケーションの管理者に提供する必要があります。

例えば、複数のアプリケーションが Tivoli Enterprise Portal クライアントを起動できる場合は、ポータル・サーバーから LTPA キーをエクスポートして、他のアプリケーション管理者にキー・ファイルとパスワードを提供し、LTPA キーをインポートできるようにすることができます。

関連サーバー間の時刻の同期化

LTPA トークンは、時間に依存します。ポータル・サーバー・コンピューターおよび関連 SSO アプリケーションのコンピューターの日付、時刻、およびタイム・ゾーンが協定世界時 (UTC) を基準として正しく設定さていることを確認します。例えば、ニューヨークのポータル・サーバーは UTC -5:00 に設定され、パリの Dashboard Application Services Hub は UTC +1:00 に設定されます。

関連タスク:

127 ページの『SSO 用ブラウザー・クライアントの再構成』
同一コンピューターからの Tivoli Enterprise Portal へのログオン時に SSO 機能を使用する場合、Tivoli Enterprise Portal Server の完全修飾名を指定するようにブラウザー・クライアントを再構成します。

ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ

シングル・サインオン (SSO) に使用できるユーザー ID を LDAP ユーザー・レジストリーに設定した後、このトピックのタスクを実行することによって SSO を使用可能にします。

- 認証およびシングル・サインオンを使用可能にするための前提条件をすべて満たしているか確認する。
- Tivoli Enterprise Portal ユーザー・アカウントを定義する。 (LDAP 認証および SSO が構成された後でも実行可能。)
- ポータル・サーバーを介して LDAP 認証および SSO を構成する。
- 関連 SSO アプリケーションと LTPA キーを交換する。
- Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップする。

ロードマップ

LDAP ユーザー・レジストリーとシングル・サインオンを使用するようポータル・サーバーをセットアップする際に役立つシナリオ・ロードマップを以下に示します。

表 15. ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ

ステップ	タスク	情報の入手先
1	LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成し、シングル・サインオンに使用するレルム名とドメインを指定します。 LDAP を使用するようにポータル・サーバーを構成するには、次のオプションを使用できます。 • IBM Tivoli Enterprise Monitoring Services の管理 ユーティリティー • Linux および UNIX の **itmcmd** コマンド行インターフェース • TEPS/e 管理コンソール IBM Tivoli Enterprise Monitoring Services の管理 または **itmcmd** コマンドのいずれかを使用して、ポータル・サーバーに対する LDAP ユーザー検証を使用可能にします。また、これらのユーティリティーを使用して LDAP 接続パラメーターを構成することもできます。ただし、以下の場合を除きます。 • Microsoft Active Directory または Tivoli Directory Server 以外のサーバーを使用したい • ポータル・サーバーおよび LDAP サーバー間の TLS/SSL を構成したい • 拡張 LDAP 構成パラメーターを指定する必要がある これらのシナリオでは、ポータル・サーバーの構成時にタイプとして「**その他**」を指定し、その後 TEPS/e 管理コンソールを使用して LDAP 接続構成を完了します。 **注:** また、LDAP ユーザー認証の構成時にポータル・サーバーの LTPA キーのエクスポートまたは他のアプリケーションからの LTPA キーのインポートを実行することができます。これらのステップは、ポータル・サーバーの LDAP 認証が機能していることを確認してから実行することもできます。	101 ページの『ポータル・サーバー上で LDAP 認証を構成するための前提条件』を参照してください。 次に、以下のいずれかのトピックの説明に従って、ポータル・サーバー上で LDAP ユーザー検証を使用可能にします。 • 110 ページの『Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する』 • 115 ページの『Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する』 ポータル・サーバーの LDAP ユーザー検証を使用可能するときに、LDAP サーバー・タイプに「**その他**」を指定した場合は、この後 117 ページの『TEPS/e 管理コンソールの使用』の説明に従います。 **使用上の注意:** Microsoft Active Directory を使用している場合は、135 ページの『Microsoft Active Directory を使用した LDAP ユーザー認証』を参照して、このタイプの LDAP サーバーに固有の計画情報と構成情報を確認してください。 Tivoli Directory Server を使用している場合は、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) の『Understanding single sign-on between IBM Tivoli Monitoring and Tivoli Integrated Portal using Tivoli Directory Server』を参照してください。これらの手順では、Tivoli Directory Server で構成されたエントリーを、TEPS/e 管理コンソールを使用して構成された情報にマップする方法を説明しています。 Tivoli Integrated Portal のためのステップは無視してください。

表 15. ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ (続き)

ステップ	タスク	情報の入手先
2	ポータル・サーバーと同じ LDAP ユーザー・レジストリー、レルム、およびインターネットまたはイントラネット・ドメイン名を使用するように他の関連 SSO アプリケーションを構成し、SSO を使用可能にします。 さらに、ポータル・サーバー・コンピューターおよび関連 SSO アプリケーションのコンピューターの日付、時刻、およびタイム・ゾーンが協定世界時 (UTC) を基準として正しく設定さていることを確認します。	Dashboard Application Services Hub を使用したシングル・サインオンを採用している場合は、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management 構成ガイド*」にあるトピック『中央ユーザー・レジストリーのための Jazz for Service Management の構成』および『アプリケーション・サーバーでの SSO の構成』を参照してください。 その他のアプリケーションに関しては、それぞれの製品資料を参照して、LDAP ユーザー・レジストリーを使用するように構成する方法、SSO を使用可能にする方法、およびポータル・サーバーとしてレルム名とドメイン名を指定する方法を確認してください。
3	Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップします。	125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』
4	ポータル・サーバーと同じコンピューターで他のアプリケーションによって Tivoli Enterprise Portal ブラウザー・クライアントが起動される場合は、ブラウザー・クライアントを SSO 用に再構成します。	127 ページの『SSO 用ブラウザー・クライアントの再構成』
5	Tivoli Enterprise Portal ユーザーがポータル・クライアントを起動し、正常にログインできることを検証します。 **注:** ポータル・クライアント・ユーザーは、ログイン時に相対識別名の値を指定する必要があります。例えば、相対識別名が `cn=John Doe`である場合、資格情報を求めるプロンプトが出されたら、`John Doe` と指定する必要があります。	Tivoli Enterprise Portal ユーザーが Tivoli Enterprise Portal にログインできない場合は、TEPS/e ログで診断情報を確認してください。これは、`SystemOut.log` という名前で、ポータル・サーバーがインストールされているコンピューターの *`install_dir`*`¥CNPSJ¥profiles¥ITMProfile¥logs`、*`install_dir`*`/Platform/iw/profiles/ITMProfile/log` にあります。 認証エラーが発生し、エラーを解決できない場合は、 131 ページの『ポータル・サーバーでの LDAP 認証の無効化』の手順に従って LDAP 認証を使用不可にすることができます。
6	ポータル・サーバーと LDAP サーバーの間の通信を保護したい場合は、両サーバー間で TLS/SSL を構成します。	123 ページの『ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』
7	Tivoli Enterprise Portal ユーザーが同様にログインできることを検証します。	N/A

表 15. ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ (続き)

ステップ	タスク	情報の入手先
8	以下のアプリケーションがポータル・サーバーと同じ LTPA キーを使用していることを確認する必要があります。 • Tivoli Enterprise Portal を起動する Web ベースまたは Web 対応のアプリケーション • Tivoli Enterprise Portal クライアントから起動できる Web ベースまたは Web 対応のアプリケーション • ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントを使用してモニター・データを取得する IBM Dashboard Application Services Hub • Tivoli Integrated Portal のように IBM Tivoli Monitoring グラフ Web サービスを使用する他のアプリケーション 他のすべての関連 SSO アプリケーションで使用する LTPA キーのソースになるアプリケーションを判断し、その LTPA キーをエクスポートします。キー・ファイルとキーの暗号化に使用するパスワードは、他の関連アプリケーションの管理者に提供する必要があります。	ポータル・サーバーが LTPA キーのソースになると判断した場合は、 128 ページの『LTPA キーのインポートおよびエクスポート』のエクスポートの指示に従って、その LTPA キーをエクスポートします。 モニター・ダッシュボードに IBM Dashboard Application Services Hub を使用しており、それを LTPA キーのソースにする場合は、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management 構成ガイド*」の『LTPA キーのエクスポート (Exporting LTPA keys)』を参照してください。 それ以外の場合は、LTPA キーをエクスポートするアプリケーションのドキュメントを参照して、エクスポート操作の実行方法を判断してください。
9	他の関連 SSO アプリケーションの管理者は、前のステップでエクスポートされた LTPA キーをインポートする必要があります。キー・ファイルとキーの暗号化に使用されたパスワードが必要です。	LTPA キーをポータル・サーバーにインポートするには、 128 ページの『LTPA キーのインポートおよびエクスポート』のインポートに関する説明を参照してください。 LTPA キーを IBM Dashboard Application Services Hub にインポートするには、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の「*Jazz for Service Management 構成ガイド*」の『LTPA 鍵のインポート』を参照してください。 LTPA キーのインポート方法について詳しくは、他の関連 SSO アプリケーションの資料を参照してください。

表 15. ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ (続き)

ステップ	タスク	情報の入手先
10	使用している SSO 環境に該当する以下のタスクを実行することにより、ポータル・サーバーと各関連 SSO アプリケーション間でシングル・サインオンが機能していることを確認します。 1. 他のアプリケーションが Tivoli Enterprise Portal を起動でき、ユーザーに資格情報を求めるプロンプトが出されないことを確認します。 2. Tivoli Enterprise Portal を使用して他のアプリケーションを起動でき、ユーザーが資格情報の再入力を求められないことを検証します。 3. データ・プロバイダーの接続が作成され、SSO 用に構成された後で、モニター対象リソースを Dashboard Application Services Hub のモニター・ダッシュボードに表示できることを検証します。 4. 別のアプリケーションが IBM Tivoli Monitoring グラフ Web サービスを使用してモニター・データを取得できることを検証します。	N/A
11	LDAP ユーザー・レジストリーに新規ユーザーが追加されたときに、Tivoli Enterprise Portal ユーザー ID を作成します。	130 ページの『新規 LDAP ユーザーの管理』

Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する

Tivoli Enterprise Monitoring Services の管理 を使用すると、ポータル・サーバーで LDAP ユーザー認証とシングル・サインオンを使用可能にできるだけでなく、オプションとして LDAP サーバー接続の詳細を構成することができます。

以下のすべての条件が当てはまる場合は、このユーティリティーを使用して LDAP サーバー接続情報を構成することができます。

- LDAP サーバーに Microsoft Active Directory Server または Tivoli Directory Server を使用している。
- ポータル・サーバーおよび LDAP サーバー間で TLS/SSL を構成する予定がない。
- 102 ページの表 13にリストされていない LDAP 構成パラメーターは構成する必要がない。

上記以外のシナリオでは、Tivoli Enterprise Monitoring Services の管理 を使用して、ポータル・サーバーに対して LDAP ユーザーの検証および SSO を使用可能にし、サーバー・タイプに「**その他**」を指定してください。次に、TEPS/e 管理コンソールを使用して、LDAP の構成を完了します。

ポータル・サーバーによる LDAP ユーザー・レジストリーの使用の構成には、バインド ID およびポート番号などの LDAP 情報をサーバー構成に追加することが含ま

れます。それと同時に、他の関連 SSO アプリケーションによって使用されるレルム名およびインターネットまたはイントラネットのドメイン名を指定することにより、シングル・サインオンを使用可能にするのがベスト・プラクティスです。これらのパラメーターについて詳しくは、101 ページの『ポータル・サーバー上で LDAP 認証を構成するための前提条件』を参照してください。

また、LTPA キーのソースとなるアプリケーションが既に決まっている場合は、ポータル・サーバーの LTPA キーのエクスポートまたは関連 SSO アプリケーションからの LTPA キーのインポートも可能です (すべての関連 SSO アプリケーションが同じキーを使用する必要があります)。LDAP ユーザー認証の設定作業に集中したい場合、またはインポートする LTPA キーがない場合は、エクスポートまたはインポート・ステップを後で実行することもできます。

始める前に

シングル・サインオン用のレルム、およびインターネットまたはイントラネットのドメイン名とともに、LDAP サーバーの構成情報を手元に用意します。

LTPA キーをエクスポートまたはインポートする場合、構成を開始する前に、ポータル・サーバーが実行されていることを確認します。構成中にポータル・サーバーが停止するというメッセージが表示されますが、構成手順の終了時に「**OK**」をクリックして最終ダイアログを閉じた後にのみ、サーバーは停止します。LTPA キーをインポートする場合は、キー・ファイルと、キー・ファイルが生成されたときに使用されたパスワードが必要です。

このタスクについて

以下のステップを実行して、LDAP レジストリーでのユーザー検証のためにポータル・サーバーを再構成し、SSO を使用可能にして、オプションで LTPA キーをエクスポートまたはインポートします。

手順

1. ポータル・サーバーがインストールされているコンピューターでTivoli Enterprise Monitoring Services の管理を始動します。
   - Windows 「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「**Tivoli Enterprise Monitoring Services の管理**」をクリックします。
   - Linux UNIX *install_dir* が IBM Tivoli Monitoring のインストール・ディレクトリーの場合、*install_dir* `/bin` ディレクトリーに移動して、`./itmcmd manage [-h` *install_dir* `]` を実行します。
2. **Tivoli Enterprise Portal Server** を右クリックして、以下のようにします。
   - Windows 「**再構成**」をクリックして、既存の構成を受け入れるために「**OK**」をクリックし、2 番目の「TEP サーバー構成」ウィンドウに進みます。
   - Linux UNIX 「**構成**」をクリックします。
3. 「LDAP セキュリティー」領域で、☑ 「**LDAP でのユーザー検証**」を選択します。 Linux および UNIX の場合、「LDAP セキュリティー」領域は「**TEMS 接続**」タブにあります。

4. オプション: SSO を使用する予定がある場合は、☑ 「**シングル・サインオンの使用可能化**」を選択します。
5. ▼ リストから、以下のいずれかの「**LDAP タイプ**」を選択します。
   - 「**AD2000**」。Active Directory Server 2000 の場合。
   - 「**AD2003**」。Active Directory Server 2003 の場合。
   - 「**AD2008**」。Active Directory Server 2008 の場合。
   - 「**IDS6**」。IBM Tivoli Directory Server バージョン 6.x の場合。
   - 「**その他**」。ご使用の LDAP サーバーが上記にリストされたもの以外の場合、Active Directory Server や Tivoli Directory Server 用の LDAP 構成をカスタマイズする場合、または LDAP サーバーへの SSL 通信を構成する場合。この手順を完了した後、TEPS/e 管理コンソールを開始して、LDAP サーバー構成を完了させます。 117 ページの『TEPS/e 管理コンソールの使用』を参照してください。

     重要: LDAP サーバーへの TLS/SSL 通信を構成するなど、後で Active Directory Server や Tivoli Directory Server の構成を編集する必要が出てきた場合は、必ず「**その他**」を選択し、TEPS/e 管理コンソールを使用してサーバーを構成してください (ステップ 6 は省略してください)。そうでないと、TEPS/e 管理コンソールで実施するカスタマイズがすべて、次にポータル・サーバーを再構成するときに失われてしまいます。
6. 「**LDAP タイプ**」として、「**AD2000**」、「**AD2003**」、または「**IDS6**」を選択した場合、LDAP サーバーを指定するために以下のようなその他のフィールドを入力します。
   - 「**LDAP ベース**」は、LDAP レジストリーにおけるベース・エントリーの識別名 (DN) です。

     これは、LDAP サーバー内のユーザー検索の開始点となります。例えば、`cn=John Doe,ou=Rochester,o=IBM,c=US` という識別名を持つユーザーの場合、このパラメーターに `ou=Rochester,o=IBM,c=US` と指定します。
   - 「**LDAP DN ベース・エントリー**」は通常、ポータル・サーバー・ユーザーの LDAP レジストリーにおけるベース・エントリーの識別名に設定されます。例えば、`cn=John Doe,ou=Rochester,o=IBM,c=US` という識別名を持つユーザーの場合、このパラメーターに `ou=Rochester,o=IBM,c=US` と指定します。

     ただし、ポータル・サーバーに対して複数の LDAP リポジトリーが構成されている場合は、このフィールドを使用して、この LDAP サーバーの LDAP ユーザー・セットを一意的に識別する追加の識別名 (DN) を定義します。例えば、`LDAP1` レジストリーと `LDAP2` レジストリーがどちらもベース・エントリーとして `o=ibm,c=us` を使用するとします。このような場合は、このパラメーターを使用して、各 LDAP サーバーに異なるベース・エントリーを指定します。例えば、`LDAP1` レジストリーを構成するときは `o=ibm1,c=us` と指定し、`LDAP2` レジストリーを構成するときは `o=ibm2,c=us` と指定します。

     注: 複数の LDAP レジストリーがある場合、重複するユーザー名は使用できません。

Tivoli Enterprise Portal の「ユーザー管理」ダイアログで、Tivoli Enterprise Portal ユーザー ID にマップできる識別名をリストすると、このパラメーターの値が表示されます。

- 「**LDAP バインド ID**」。バインド認証に使用する LDAP 表記の LDAP ユーザー ID です。LDAP ユーザーの検索を許可されている必要があります。匿名ユーザーが LDAP ユーザーを検索できる場合、バインド ID は省略可能です。
- 「**LDAP バインド・パスワード**」。LDAP バインド認証用の LDAP ユーザー・パスワードです。匿名ユーザーがご使用の LDAP サーバーにバインドできる場合、この値は省略可能です。この値はインストーラーによって暗号化されます。
- 「**LDAP ポート番号**」。LDAP サーバーが listen しているポートの番号です。ポートが 389 である場合、この値は省略可能です。
- 「**LDAP ホスト名**」。LDAP サーバーがポータル・サーバーと同じコンピューター上にある場合、この値は省略可能です。 デフォルトは「**localhost**」です。

7. 「**OK**」をクリックします。
   - ☑ 「**シングル・サインオンの使用可能化**」を選択している場合、「シングル・サインオン」ダイアログが表示され、そのダイアログには「**レルム名**」フィールド、「**ドメイン名**」フィールド、「**キーのインポート**」ボタン、および「**キーのエクスポート**」ボタンが表示されます。
   - この時点でシングル・サインオンを使用可能にしない場合は、「**OK**」をクリックして、他のポータル・サーバーの構成ダイアログを閉じ、ステップ 12 (114 ページ) に進んでください。
8. SSO の場合、「シングル・サインオン」ダイアログで、以下のようなレルムおよびドメインを指定します。
   a. 「**レルム名**」は、SSO 関連アプリケーション全体で共有されるパラメーターです。 同じドメイン名で構成されたアプリケーションでも、異なるレルム名で構成されている場合は、同じ SSO インフラストラクチャーの一部としては機能しません。
   b. 「**ドメイン名**」 は、SSO が構成されているインターネットまたはイントラネットのドメイン (例えば、mycompany.com) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。
9. ポータル・サーバーの LTPA キーを、他のすべての SSO 関連アプリケーションによって使用されるキーにする場合は、この時点でエクスポートすることができます。「**キーのエクスポート**」をクリックして、以下のステップを実行します。
   a. ファイルを作成したり、ファイル・タイプを変更したりするディレクトリーにナビゲートします。 最初に表示されるディレクトリーは、Windows では *ITM_dir*¥InstallITM、Linux および UNIX ではルート・ディレクトリーです。
   b. LTPA キーを置くファイルの名前を入力し、「**保存**」をクリックします。

c. 「キーのエクスポート」ウィンドウで、ファイルの暗号化に使用するパスワードを入力し、「**OK**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。

注: LDAP の構成が完了したら、Tivoli Enterprise Portal を起動するアプリケーションの管理者にキー・ファイルとパスワードを提供するか、IBM Dashboard Application Services Hub でダッシュボード・データ・プロバイダーを使用するか、IBM Tivoli Monitoring グラフ Web サービスを使用します。

10. 他の関連 SSO アプリケーションが LTPA キーを提供している場合、キー・ファイルとキーの暗号化に使用されたパスワードがあれば、この時点でそのキーをインポートできます。「**キーのインポート**」をクリックして、以下のステップを実行します。
    a. 表示された「**開く**」ウィンドウで、鍵ファイルが置かれているディレクトリーにナビゲートします。 最初に表示されるディレクトリーは、Windows では *ITM_dir*¥InstallITM、Linux および UNIX ではルート・ディレクトリーです。
    b. インポートするファイルの名前を入力し、「**開く**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。その他の参加サーバーからキーをインポートする場合は、このインポート処理を繰り返します。
    c. ファイルの暗号化解除に必要なパスワードを入力し、「**OK**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。
    d. その他の参加サーバーからキーをインポートする場合は、このインポート処理を繰り返します。
11. 「**OK**」をクリックします。
12. Windows ウェアハウス接続情報を再構成するプロンプトが表示された場合、「**いいえ**」と応答します。いくつか構成設定を処理した後、「共通イベント・コンソール構成」ウィンドウが表示されます。このウィンドウは、前景表示されずに他のウィンドウにより隠される場合があります。処理に時間がかかりすぎている場合は、他のウィンドウを最小化し、構成ウィンドウを探してください。「共通イベント・コンソール構成」ウィンドウが表示されたら、「**OK**」をクリックします。
13. 必要に応じ、**Tivoli Enterprise Portal Server** を選択して 「**リサイクル**」をクリックするか、またはポータル・サーバーを停止してから開始することによって、ポータル・サーバーを再開します。

次のタスク

LDAP タイプとして「**その他**」を選択した場合、TEPS/e 管理コンソールで LDAP 構成を完了する必要があります。 117 ページの『TEPS/e 管理コンソールの使用』を参照してください。

それ以外の場合、他のすべての LDAP タイプについて、前述の手順のステップ 1 および 2 に従って、「**LDAP でのユーザー検証**」が選択されているかどうか確認し

ます。選択されていない場合、構成ユーティリティーが LDAP サーバーに接続しようとしてエラーが発生し、LDAP 検証が使用不可になっています。使用不可になっている場合、*install_dir* /logs/ConfigureLDAPRepo.log ファイルを確認します。

LDAP レジストリーの構成が完了したら、Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップして、LDAP の構成を完了できます。**sysadmin** ユーザー ID または同等の管理権限があり LDAP ユーザーではないユーザー ID を使用して Tivoli Enterprise Portal にログオンする必要があります。 125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』を参照してください。

SSO を使用可能にした場合は、LTPA キーのエクスポートまたはインポートが必要になります。その手順を実行するタイミングは、 106 ページの『ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ』を参照して判断してください。

Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する

Tivoli Enterprise Portal Server が Linux または UNIX 上にある場合、ポータル・サーバーで LDAP ユーザー認証やシングル・サインオンを使用可能にすることができ、さらにオプションとして、itmcmd コマンド行インターフェースを使用して LDAP サーバー接続の詳細を構成することができます。

以下のすべての条件が当てはまる場合は、コマンド行を使用して LDAP サーバー接続情報を構成することができます。

- LDAP サーバーに Microsoft Active Directory Server または Tivoli Directory Server を使用している。
- ポータル・サーバーおよび LDAP サーバー間で TLS/SSL を構成する予定がない。
- 102 ページの表 13にリストされていない LDAP 構成パラメーターは構成する必要がない。

上記以外のシナリオでは、itmcmd コマンドを使用して、ポータル・サーバーに対して LDAP ユーザーの検証および SSO を使用可能にし、サーバー・タイプに「**その他**」を指定してください。次に、TEPS/e 管理コンソールを使用して、LDAP の構成を完了します。

ポータル・サーバーによる LDAP ユーザー・レジストリーの使用の構成には、バインド ID およびポート番号などの LDAP 情報をサーバー構成に追加することが含まれます。それと同時に、他の関連 SSO アプリケーションによって使用されるレルム名およびインターネットまたはイントラネットのドメイン名を指定することにより、シングル・サインオンを使用可能にするのがベスト・プラクティスです。これらのパラメーターについて詳しくは、 101 ページの『ポータル・サーバー上で LDAP 認証を構成するための前提条件』を参照してください。

このタスクについて

コマンド行からポータル・サーバーを構成するには、以下のステップを完了します。

手順

1. Tivoli Enterprise Portal Server がインストールされているコンピューターにログオンします。
2. コマンド行で、*install_dir* /bin ディレクトリーに移動します。ここで、*install_dir* はこの製品をインストールしたディレクトリーです。
3. コマンド **./itmcmd config -A cq** を実行して、Tivoli Enterprise Portal Server の構成を開始します。 メッセージ「エージェント構成が開始しました...」が表示され、続いて以下のようなプロンプトが出されます。

   ```
   「IBM Tivoli Monitoring 用の共通イベント・コンソール」設定を編集しますか?
   [1= はい、2= いいえ] (デフォルトは 1)
   ```

4. **2** と入力します。 以下のプロンプトが表示されます。

   ```
   このエージェントは TEMS に接続しますか? [1= はい、2= いいえ] (デフォルトは 1):
   ```

5. 以下のプロンプトが表示されるまで、このプロンプトおよび後続のプロンプトに対して、デフォルト値を受け入れます。 元の構成時に行われた選択内容がデフォルト値に反映されます。

   ```
   LDAP セキュリティー: LDAP でユーザーを検証しますか?
   ( 1 = はい、2 = いいえ。デフォルト: 2 ):
   ```

6. 1 と入力して LDAP 認証の構成を開始し、LDAP パラメーターの値を指定します。

   ```
   LDAP type: [AD2000, AD2003, AD2008, IDS6, OTHER](デフォルトは: OTHER):
   ```

   LDAP タイプには、ご使用の LDAP サーバーが上記にリストされたもの以外の場合、Active Directory Server や Tivoli Directory Server 用の LDAP 構成をカスタマイズする場合、またはポータル・サーバーと LDAP 間の TLS/SSL を構成する予定がある場合は、 「**その他**」を選択します。この手順を完了した後、TEPS/e 管理コンソールを開始して、LDAP サーバー構成を完了させます。 117 ページの『TEPS/e 管理コンソールの使用』を参照してください。

   重要: 例えばLDAP サーバーへの TLS/SSL 通信を構成するなど、後で Active Directory Server または Tivoli Directory Server の構成を編集する必要があると予想される場合は、必ず「**その他**」を選択し、TEPS/e 管理コンソールを使用してサーバーを構成してください。そうでないと、TEPS/e 管理コンソールで実施するカスタマイズがすべて、次にポータル・サーバーを再構成するときに失われてしまいます。

7. タイプに「**その他**」を指定しなかった場合は、追加の LDAP 構成値の入力を求めるプロンプトが出されます (それらのパラメーターについて詳しくは、 102 ページの表 13 を参照してください)。

   ```
   LDAP ベース: o=IBM
   LDAP DN ベース・エントリー (デフォルト: o=ITMSSOEntry):  o=IBM
   LDAP バインド ID: cn=root
   LDAP バインド・パスワード:
   LDAP バインド・パスワードを再入力してください:
   LDAP ポート番号 (デフォルト: 389):
   LDAP ホスト名 (デフォルト: localhost): itmxseries04
   ```

8. シングル・サインオンおよび LDAP 認証を有効にする必要がある場合は、以下のプロンプトで 1 と入力し、レルム名およびドメイン名を指定します。

   ```
   シングル・サインオンを使用可能にしますか? ( 1 = はい、2 = いいえ。デフォルト: 2 ):
   ```

a. **レルム名** は、SSO 関連アプリケーション全体で共有されるパラメーターです。 同じドメイン名で構成されたアプリケーションでも、異なるレルム名で構成されている場合は、同じ SSO インフラストラクチャーの一部としては機能しません。

b. **ドメイン名** は、SSO が構成されているインターネットまたはイントラネットのドメイン (例えば、mycompany.com) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。

インストーラーによって構成が完了すると、メッセージ「**エージェント構成が完了しました...**」が表示されます。

9. ポータル・サーバーを再開します。

```
./itmcmd agent stop cq
./itmcmd agent start cq
```

次のタスク

LDAP タイプとして「**その他**」を選択した場合、TEPS/e 管理コンソールで LDAP 構成を完了する必要があります。『TEPS/e 管理コンソールの使用』を参照してください。

LDAP レジストリーの構成が完了したら、Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップして、LDAP の構成を完了できます。**sysadmin** ユーザー ID または同等の管理権限があり LDAP ユーザーではないユーザー ID を使用して Tivoli Enterprise Portal にログオンする必要があります。 125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』を参照してください。

SSO を使用可能にした場合は、LTPA キーのエクスポートまたはインポートが必要になります。その手順を実行するタイミングは、 106 ページの『ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ』を参照して判断してください。

TEPS/e 管理コンソールの使用

Tivoli Enterprise Portal Server の拡張サービス (TEPS/e) には管理コンソール (ISCLite) が用意されています。この管理コンソールにアクセスして、IBM Tivoli Monitoring インストール・プログラムではサポートされない LDAP レジストリーを構成することができます (Tivoli Enterprise Monitoring Services の管理 および **itmcmd** コマンド行構成ユーティリティー)。

また、TEPS/e 管理コンソールを使用して、LDAP サーバーとの通信、およびダッシュボード・データ・プロバイダーまたは IBM Tivoli Monitoring グラフ Web サービスに要求を送信する他のアプリケーションとの通信用に SSL を構成することもできます。

インストール時にポータル・サーバーを構成したとき、または Tivoli Enterprise Monitoring Services の管理 ユーティリティーまたは **itmcmd** コマンド行インターフェースを使用したときに LDAP タイプとして「**その他**」を指定した場合は、TEPS/e 管理コンソールを使用して、ポータル・サーバーの LDAP ユーザー認証を構成する

必要があります。また、以下のタスクを実行する場合は、TEPS/e 管理コンソールを使用して、LDAP 接続の詳細を構成する必要もあります。

- Microsoft Active Directory Server または Tivoli Directory Server 以外の LDAP サーバーの使用。
- ポータル・サーバーと LDAP サーバー間の TLS/SSL 通信の構成。
- 他のポータル・サーバー構成ユーティリティーでは指定できないが、TEPS/e 管理コンソールで指定できる拡張 LDAP 構成パラメーターの構成。

重要: Manage Tivoli Monitoring Services または **itmcmd** コマンド行インターフェース構成ユーティリティーを使用したポータル・サーバーの構成時に LDAP タイプとして「**その他**」を選択していない場合は、TEPS/e 管理コンソール内で行われたすべての LDAP のカスタマイズは、ポータル・サーバーの再構成時に上書きされ、クリアされます。「**その他**」を選択した場合は、LDAP ユーザー・レジストリー情報は、TEPS/e によって処理され、他のポータル・サーバー構成ユーティリティーの影響を受けません。

TEPS/e 管理コンソールの開始

TEPS/e 管理コンソールを使用して、タイプが「**その他**」の LDAP サーバーを構成して、ポータル・サーバーと他のアプリケーション (LDAP サーバーなど) との間に SSL を構成し、また LDAP 構成を確認します。

始める前に

TEPS/e 管理コンソールは、セキュリティー上の理由のため、およびシステム・リソースの節約のため、デフォルトでは無効にされています。コンソールを有効にする前に、Tivoli Enterprise Portal Server が実行されている必要があります。

このタスクについて

TEPS/e 管理コンソールを有効にして開始するには、以下のステップを実行してください。

手順

1. 以下のようにして、TEPS/e 管理コンソールを有効にします。
   - Windows 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、「**Tivoli Enterprise Portal Server**」を強調表示させ、「**拡張**」→「**TEPS/e 管理**」→「**TEPS/e 管理の有効化**」を選択します。
   - Linux UNIX コマンド行によって、scripts ディレクトリー (Intel Linux では *ITM_dir*/li6263/iw/scripts、 zLinux では *ITM_dir*/ls3266/iw/scripts、AIX® では *ITM_dir*/aix533/iw/scripts) に移動して、以下のコマンドを入力します。ここで、true はコンソールの開始、false はコンソールの停止を意味します。

     ```
     ./enableISCLite.sh {true/false}
     ```

   これで、TEPS/e 管理コンソールは有効になりログオン可能です。ポータル・サーバーが停止されるまで、有効のままです。
2. コンソールを初めて有効にする場合は、以下のようにして、管理パスワードを設定する必要があります。

- Windows 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、「**Tivoli Enterprise Portal Server**」を強調表示させ、「**拡張**」→「**TEPS/e 管理**」→「**TEPS/e 管理パスワード**」を選択します。
- Linux UNIX scripts ディレクトリーで、以下のコマンドを入力します。ここで、*<username>* は **wasadmin**、*<password>* は新規パスワードです。

  ```
  updateTEPSEPass.sh <username> <password>
  ```

  続いて、TEPS/e 管理パスワードを入力すると、パスワードがリセットされます。

3. Internet Explorer ブラウザーまたは Firefox ブラウザーで、以下の URL を入力します。 `http://localhost:15205/ibm/console` または `https://localhost:15206/ibm/console`
4. ユーザー ID の **wasadmin**、および TEPS/e 管理パスワードとして入力したパスワードを使用して、コンソールにログオンします。

タスクの結果

Integrated Solutions Console (TEPS/e 管理コンソール) のウィンドウが開きます。管理コンソールをログアウトした後でも、Tivoli Enterprise Portal Server が停止されるまで、コンソールは有効のままです。各ポータル・サーバーの再始動後には Tivoli Enterprise Monitoring Services の管理を使用して TEPS/e 管理コンソール を手動で再始動する必要があります。

次のタスク

これで、外部 LDAP サーバー接続、SSLの構成、または構成の検証ができるようになりました。

ポータル・サーバーのリサイクル時に TEPS/e 管理コンソールが実行されている場合、ログアウトしてコンソールをポータル・サーバーと再同期化して、もう一度有効にする必要があります。

TEPS/e 管理コンソールを使用した LDAP 認証のためのポータル・サーバーの構成

ポータル・サーバーの構成時に LDAP タイプとして「**その他**」を指定した場合は、Tivoli Enterprise Portal Server の拡張サービス (TEPS/e) 管理コンソールを使用して、 LDAP サーバー接続パラメーターを構成する必要があります。

始める前に

TEPS/e 管理コンソールを始動します。

重要: 今後の変更内容が持続するようにするために、TEPS/e 管理コンソールを使用して LDAP サーバー構成を変更する前に、**itmcmd** コマンド行インターフェースの Tivoli Enterprise Monitoring Services の管理 ユーティリティーで LDAP タイプとして「**その他**」を選択しておくのがベスト・プラクティスです。例えば、itmcmd コマンドを使用してポータル・サーバーを構成したときに LDAP タイプとして「**IDS6**」を選択しており、TEPS/e 管理コンソールを使用して LDAP 接続パラメーターを変更した場合、ポータル・サーバーの次回再構成時にその変更が失われます。

手順

1. TEPS/e 管理コンソールのナビゲーション・ツリーで、「**セキュリティー**」→「**グローバル・セキュリティー**」をクリックします。
2. 表示されたページで、「**使用可能なレルム定義**」に「**統合リポジトリー**」が選択されている状態にし、「**構成**」をクリックします。
3. 以下のようにして、統合リポジトリーを構成します。
   a. 「**レルム名**」の値を確認または入力します。 レルムは、TEPS/e および他の WebSphere Application Server の統合リポジトリー・セットを識別します。独自のレルム名を選択できますが、この値は、指定したインターネット・ドメインまたはイントラネット・ドメイン内で SSO に対して構成されるすべてのアプリケーションで同じである必要があります。ポータル・サーバーの構成時にシングル・サインオンを有効にした場合は、このフィールドには、レルム名に指定した値が表示されます。ドメインの指定について詳しくは、ステップ 9 (121 ページ) を参照してください。
   b. 同じページで、「**レルムの基本項目の追加**」をクリックします。
4. 「**リポジトリー参照**」ページで、「**リポジトリーの追加**」をクリックし、ドロップダウン・リストから「**LDAP リポジトリー**」を選択します。 ページには、LDAP 接続に対して構成可能なポータル・サーバーのプロパティーが表示されます。
5. 以下のパラメーターごとに適切な値を入力します。
   - 「**リポジトリー ID**」に、LDAP リポジトリーでの使用タイプを識別するために意味があると思われるリポジトリー名を入力します。例えば、`ITMtepUsers` です。
   - 「**ディレクトリー・タイプ**」で、ご使用の環境で使用している LDAP サーバーのタイプを選択します。
   - 「**1 次ホスト名**」に、LDAP サーバーの完全修飾ホスト名または IP アドレスを入力します。
   - 「**ポート**」で、LDAP サーバーのポート番号を入力します。デフォルト値は 389 です。
   - 「**バインド識別名**」に、LDAP ユーザーを検索する権限を備えたユーザーの識別名を入力します。例えば、`cn=root` です。匿名ユーザーが LDAP ユーザーを検索できる場合、バインド ID は省略可能です。
   - 「**バインド・パスワード**」に、「**バインド識別名**」フィールドで指定したユーザーのパスワードを入力します。匿名ユーザーがご使用の LDAP サーバーにバインドできる場合、この値は省略可能です。

   必要に応じて、このページで他のパラメーターをご使用の LDAP サーバーの機能に合わせてカスタマイズすることもできます。このパネルで構成できる他のパラメーターについて詳しくは、TEPS/e 管理コンソールのオンライン・ヘルプを参照してください。
6. 「**OK**」をクリックして、設定を受け入れます。
7. 「**リポジトリー参照**」ページで、以下の値を入力します。
   - **「レルム内のこのエントリー・セットを一意的に識別するベース・エントリーの識別名 (Distinguished name of the base entry that uniquely identifies**

this set of entries in the realm)」に、接続を構成している LDAP サーバーの LDAP ユーザー・エントリー・セットを一意的に識別する値を入力します。

通常、このパラメーターは、ポータル・サーバー・ユーザーの LDAP レジストリーにおけるベース・エントリーの識別名に設定します。例えば、`cn=John Doe,ou=Rochester,o=IBM,c=US` という識別名を持つユーザーの場合、このパラメーターに `ou=Rochester,o=IBM,c=US` と指定します。

ただし、ポータル・サーバーに対して複数の LDAP リポジトリーが構成されている場合は、このフィールドを使用して、この LDAP サーバーの LDAP ユーザー・セットを一意的に識別する追加の識別名 (DN) を定義します。例えば、`LDAP1` レジストリーと `LDAP2` レジストリーがどちらもベース・エントリーとして `o=ibm,c=us` を使用するとします。このような場合は、このパラメーターを使用して、レルム内の各 LDAP サーバーに異なるベース・エントリーを一意的に指定します。例えば、`LDAP1` レジストリーを構成するときは `o=ibm1,c=us` と指定し、`LDAP2` レジストリーを構成するときは `o=ibm2,c=us` と指定します。

注: 複数の LDAP レジストリーがある場合、重複するユーザー名は使用できません。

Tivoli Enterprise Portal の「ユーザー管理」ダイアログで、Tivoli Enterprise Portal ユーザー ID にマップできる識別名をリストすると、このパラメーターの値が表示されます。¥

- 「**このリポジトリー内のベース・エントリーの識別名 (Distinguished name of the base entry in this repository)**」に、LDAP レジストリー内のベース・エントリーの識別名 (DN) を入力します。

  これは、LDAP サーバー内のユーザー検索の開始点となります。例えば、`cn=John Doe,ou=Rochester,o=IBM,c=US` という識別名を持つユーザーの場合、このパラメーターに `ou=Rochester,o=IBM,c=US` と指定します。レルム内のベース・エントリーの識別名をカスタマイズして、その識別名が LDAP サーバー内の識別名と一致しなくなっている場合を除いて、通常、このパラメーターは、LDAP ベース・パラメーターと同じです。

8. 「**OK**」をクリックして、設定を受け入れます。
9. SSO を有効にするには、「**グローバル・セキュリティー**」ページに戻って、以下を実行します。
   a. 認証メカニズムとして「**LTPA**」が選択されている状態にします。
   b. 「**Web セキュリティー**」オプションを展開します。
   c. 「**シングル・サインオン (SSO)**」リンクを選択して、SSO 構成を入力します。
10. 「**シングル・サインオン (SSO)**」ページで、以下を実行します。
    a. SSO が有効になっていることを確認します。
    b. 「**ドメイン名**」パラメーターが正しいことを確認します。「**ドメイン名**」は、SSO が構成されているインターネットまたはイントラネットのドメイン (例えば、mycompany.com) です。このドメインまたはそのサブドメイン内で使用可能なアプリケーションのみ、SSO が使用可能になります。すべ

ての関連 SSO アプリケーションも同じレルム名を使用して構成する必要があります。ポータル・サーバーの構成時にシングル・サインオンを有効にした場合は、このフィールドには、ドメイン名に指定した値が表示されます。

c. 「**OK**」を選択して、設定を受け入れます。

11. 変更を保存するには、画面上部付近の「**保存**」オプションをクリックしてから、管理コンソールをログアウトします。
12. ここで LTPA キーをエクスポートまたはインポートする場合は、 128 ページの『LTPA キーのインポートおよびエクスポート』のTEPS/e 管理コンソールのステップを参照してください。

    注: ここでキーをエクスポートまたはインポートする場合でも、SSO が動作していることを確認しようとする前に、 106 ページの『ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ』にリストされている他のステップを実行する必要があります。
13. Tivoli Enterprise Portal Serverを再始動します。

次のタスク

Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップする。 125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』を参照してください。

コンソールを再始動する前に、ポータル・サーバーのリサイクル後に管理コンソールを使用可能にする必要があります。

重要: ポータル・サーバーのインストール時または **itmcmd** コマンド行インターフェースの Tivoli Enterprise Monitoring Services の管理 ユーティリティーを使用したポータル・サーバー構成の実行時に、LDAP タイプとして「**その他**」を選択しなかった場合は、TEPS/e 管理コンソール内で行われたすべての LDAP のカスタマイズは、ポータル・サーバーの再構成時に上書きされ、クリアされます。「**その他**」を選択した場合は、レジストリー情報は TEPS/e によって処理され、これらの他の構成ユーティリティーの影響を受けません。 110 ページの『Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する』のステップ 5 (112 ページ) および 115 ページの『Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する』の6 (116 ページ)を参照してください。

TEPS/e の開始および停止

Tivoli Enterprise Portal Server が実行されている TEPS/e のアプリケーション・サーバー・インスタンスを開始または停止する必要がある場合は、Tivoli Enterprise Portal Server を開始または停止することによって、それを行います。

TEPS/e の start および stop コマンドを使って TEPS/e を制御することはできません。既に TEPS/e のコマンドを使用している場合は、以下の手順によってリカバリーできます。

Tivoli Enterprise Portal Server の開始および停止

- Windows 「Manage Tivoli Monitoring Services」ウィンドウで、「**Tivoli Enterprise Portal Server**」を強調表示させ、「**停止**」または「**開始**」を選択します。
- Linux UNIX ITM_home/bin にある itmcmd ユーティリティーを使用します。
  - 開始するには:

    ```
    cd ITM_home/bin
    ./itmcmd agent start cq
    ```
  - 停止するには:

    ```
    cd ITM_home/bin
    ./itmcmd agent stop cq
    ```

TEPS/e の他のサーバー・インスタンスの開始および停止

TEPS/e で自分のプロファイル、セル、サーバーを作成した場合など、異なるアプリケーション・サーバーのインスタンスを TEPS/e で開始または停止する必要がある場合は、以下の 2 つのスクリプトを使用する必要があります。

- Windows

  ```
  <ITM_home>/CNPSJ/profiles/<name_of_your_profile>/bin/startServer.bat
  <name_of_your_server>
  <ITM_home>/CNPSJ/profiles/<name_of_your_profile>/bin/stopServer.bat
   <name_of_your_server>
  ```
- UNIX

  ```
  <ITM_home>/<arch>/iw/profiles/<name_of_your_profile>/bin/startServer.sh
  <name_of_your_server>
  <ITM_home>/<arch>/iw/profiles/<name_of_your_profile>/bin/stopServer.sh
  <name_of_your_server>
  ```

例:

- Windows IBM Tivoli Monitoring で作成したプロファイル、および <*YourServer*> という自分のサーバーを使用している場合は、以下のコマンドを使用する必要があります。

  ```
  <ITM_home>/CNPSJ/profiles/<ITMProfile>/bin/startServer.bat
  <YourServer>
  ```
- UNIX <*YourProfile*> という自分のプロファイル、および TEPS/e という自分のサーバーを作成している場合、UNIX プラットフォーム (例えば RHEL4) 上のサーバーを停止するには、以下のコマンドを使用します。

  ```
  <ITM_home>/<arch>/iw/profiles/<YourProfile>/bin/stopServer.sh
  <YourServer>
  ```

ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成

TEPS/e 管理コンソール を使用して、ポータル・サーバーと LDAP サーバー間の TLS (Transport Layer Sockets) または SSL (Secure Socket Layers) を構成します。

始める前に

既に LDAP サーバーへの既存の接続が存在していて、Tivoli Enterprise Portal ユーザーはポータル・サーバーにログインでき、LDAP サーバーで認証されることを確

認します。さらに、Tivoli Enterprise Portal Server が「**その他**」の LDAP タイプを使用して構成されていることも確認する必要があります。これは、LDAP サーバー通信のための TLS/SSL の構成は、TEPS/e 管理コンソールを使用して行う必要があるからです。

LDAP サーバーは、TLS/SSL 接続を受け入れ、保護されたポート番号 (通常はポート 636) で実行されるように構成する必要があります。署名者証明書を作成する必要がある場合は、ご使用の LDAP サーバーの資料を参照してください。この作業の一環として、署名者証明書を LDAP サーバーから TEPS/e のトラストストアにインポートする必要があります。

LDAP TLS/SSL には、LDAP 管理者による操作が必要な部分がありますが、これについては Tivoli Monitoring の資料では説明していません。IBM セキュリティー・システム・インフォメーション・センターの以下のトピックでは、TLS/SSL 用に LDAP サーバーを設定する方法に関する情報を提供しています。

- SSL アクセス用 Microsoft Active Directory の構成
- SSL アクセス用 Tivoli Directory Server クライアントの構成
- SSL アクセス用 Oracle Java System Directory Server の構成

以下の手順を開始する前に、 118 ページの『TEPS/e 管理コンソールの開始』の説明に従って、 TEPS/e 管理コンソールを始動します。

手順

1. 以下のステップを実行し、LDAP サーバーの署名者証明書を TEPS/e トラストストアにインポートします。
   a. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」をクリックします。
   b. ページの「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表示された表内の「**NodeDefaultTrustStore**」リンクをクリックします。
   c. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、「**ポートから取得**」ボタンをクリックします。
   d. 関連フィールドで、ホスト名、ポート (SSL 接続の場合は通常 636)、SSL 構成の詳細、および LDAP サーバーの証明書の別名を指定します。次に、「**署名者情報の取得**」ボタンをクリックして、「**OK**」をクリックします。
2. 以下の手順に従って、LDAP サーバーへの TLS/SSL 通信を使用可能にします。
   a. 「**セキュリティー**」→「**グローバル・セキュリティー**」とクリックします。
   b. ページの下部近くにある「関連項目」領域で、「**リポジトリーを管理**」を選択します。
   c. リポジトリーの表で、LDAP サーバーのリポジトリー識別子へのリンクを選択します。
   d. 「**SSL 通信を必要とする**」チェック・ボックスを選択して、「**中央管理対象**」オプションを選択します。
   e. ポート番号を 389 から LDAP サーバーが SSL 接続に使用するポート番号 (通常は 636) に変更します。
   f. 「**OK**」をクリックします。
   g. 構成の変更を保存します。
3. ポータル・サーバーを再始動します。

次のタスク

Tivoli Enterprise Portal ユーザーがログインでき、LDAP サーバーによって認証されることを確認します。

Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング

ポータル・サーバーが LDAP ユーザー・レジストリーを使用してユーザーを認証するように構成されている場合、ユーザーは相対識別名の固有 ID (UID) を使用してポータル・サーバーにログインします。この名前は、必ずしも Tivoli Enterprise Portal で認識しているユーザー ID と同じではありません。このため、Tivoli Enterprise Portal ユーザー ID を LDAP 識別名 (UID を含む) にマップする必要があります。

LDAP ユーザー・レジストリー内のすべての項目には、識別名 (DN) があります。DN は、ディレクトリー内の項目を一意に識別するための名前です。例えば、DN は attribute=value のペアをコンマで区切ったものから構成されます。

```
cn=Jim Grey,ou=users,ou=SWG,o=IBM,c=US
```

```
cn=Sally White,ou=users,ou=SWG,o=IBM,c=US
```

属性値のペアの順序は重要です。DN は、ルートを基点として、項目が存在するレベルまでの各ディレクトリー階層レベルごとに、1 つのコンポーネントを含みます。LDAP の DN は、最も具体的な属性 (通常はある種類の名前) で始まり、その後に続く属性は次第に広義になり、多くの場合は国属性で終了します。DN の先頭のコンポーネントは、相対識別名 (RDN®) と呼ばれます。これは、同じ親を持つ他の項目同士を区別して識別します。上記の例では、RDN `cn=Jim Grey` は、最初のエントリーを、2 番目のエントリー (RDN `cn=Sally White` を持つ) から分離します。これらの 2 つの DN の例は、それ以外は同等です。この 2 人のユーザーは、Tivoli Enterprise Portal に `Jim Grey` および `Sally White` としてログインします。

Tivoli Enterprise Portal に対して作成する新規ユーザーのデフォルト識別名の構造は以下のとおりです。

```
UID=tep_userid,O=DEFAULTWIMITMBASEDREALM
```

この識別名は、ユーザーがハブ・モニター・サーバーによって認証されることを示しています。このトピックの手順を使用して、ポータルサーバーの LDAP ユーザー・レジストリーに定義されている Tivoli Enterprise Portal ユーザーの識別名を更新し、LDAP ユーザー・レジストリーに `UID=tep_userid,O=DEFAULTWIMITMBASEDREALM` ではなく、識別名を指定します。

TEPS/e ユーザー・レジストリーのデフォルトの DN サフィックスは `o=defaultWIMFileBasedRealm` です。TEPS/e ユーザー・レジストリーには、TEPS/e 管理コンソール・アクセスのための wasadmin ユーザー ID (`UID=wasadmin,o=defaultWIMFileBasedRealm`) が含まれます。

`o=defaultWIMFileBasedRealm` サフィックスを使用する Tivoli Enterprise Portal ユーザー ID の識別名は更新しないでください。

始める前に

Tivoli Enterprise Portal の「ユーザー管理」ウィンドウで、管理者権限を持つユーザーによってユーザー ID を LDAP 識別名にマップします。**tacmd** コマンド行インターフェースも、このマップを実行するときに使用することができます。詳しくは、「*IBM Tivoli Monitoring* コマンド・リファレンス」の **tacmd edituser** コマンドを参照してください。

LDAP 認証が Tivoli Enterprise Monitoring Server を介して構成されている場合は、代わりに、Tivoli Enterprise Monitoring Server 構成ファイルの KGL_LDAP_USER_FILTER 環境変数を編集することによってユーザー ID をマップします。

このタスクについて

Tivoli Enterprise Portal の「ユーザー管理」ダイアログ・ウィンドウを使用して Tivoli Enterprise Portal ユーザー ID を LDAP 識別名にマップするには、以下のステップを実行します。

手順

1. **sysadmin** または十分な管理者権限を持つ他のユーザー・アカウントを使用してポータルにログオンします。
2. 「**ユーザー管理**」をクリックします。
3. 「ユーザー管理」ウィンドウで、マップするユーザー ID の行を右クリックして、「**ユーザーの変更**」を選択します。
4. 「ユーザーの変更」ダイアログ・ボックスで、「**検索**」をクリックして、Tivoli Enterprise Portal ユーザー ID と関連付ける LDAP 識別名を見つけます。 例えば、UID=TEPUSER,O=SS などです。

   注:

   - Tivoli Enterprise Portal Server 構成ユーティリティーで構成される LDAP 識別名のデフォルトのサフィックスは o=ITMSSOEntry ですが、ポータル・サーバーが LDAP 用に構成されたときに、この値がカスタマイズされている可能性があります。
   - 選択した LDAP 識別名に非英数字が含まれている場合、マッピングを保存する前に、これらの非英数字をバックスラッシュ (円記号)でエスケープする必要があります。例えばユーザー ID にポンド記号 # が含まれている場合は、ポンド記号の前にバックスラッシュ (円記号) を挿入します (¥#)。
5. 「**OK**」をクリックしてマッピングを保存し、「ユーザー管理」ウィンドウに戻ります。
6. 構成された LDAP レジストリーで認証するすべてのユーザーをマップするまで、ステップ 3 からステップ 5 を繰り返します。
7. 「**OK**」をクリックして「ユーザー管理」ウィンドウを閉じます。

次のタスク

ポータル・サーバーと同じコンピューターで他のアプリケーションによって Tivoli Enterprise Portal ブラウザー・クライアントが起動される場合は、ブラウザー・クライアントを SSO 用に再構成します。『SSO 用ブラウザー・クライアントの再構成』を参照してください。

LDAP 識別名にマップされた ID を持つ Tivoli Enterprise Portal ユーザーが、Tivoli Enterprise Portal クライアントにログインできることを確認します。ユーザーは、自分の LDAP 相対識別名を使用してログインする必要があります。 Tivoli Enterprise Portal に正常にログインできない場合は、TEPS/e ログで診断情報を確認してください。これは `SystemOut.log` というファイルで、ポータル・サーバーのインストール先 (Windows *install_dir* `¥CNPSJ¥profiles¥ITMProfile¥logs` に、Linux UNIX *install_dir* /*Platform*/iw/profiles/ITMProfile/log) に格納されています。

Tivoli Enterprise Portal ユーザーがポータル・サーバーの LDAP ユーザー・レジストリーによって正常に認証された後で実行する追加の手順については、106 ページの『ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ』を参照してください。

SSO 用ブラウザー・クライアントの再構成

同一コンピューターからの Tivoli Enterprise Portal へのログオン時に SSO 機能を使用する場合、Tivoli Enterprise Portal Server の完全修飾名を指定するようにブラウザー・クライアントを再構成します。

始める前に

デフォルトでは、Tivoli Enterprise Portal Server と同じコンピューター上で実行中のブラウザー・クライアントに関連する起動 URL は、`localhost` です。ポータル・サーバーと同じコンピューター上のブラウザー・クライアントを使用する場合、この値はコンピューターの完全修飾名である必要があります (`dev1.myco.com` など)。サフィックス `myco.com` は、SSO 構成パネルで入力したドメイン値です。このサフィックスを使用すると、SSO トークン はドメイン・サフィックスが同じサーバーでのみ認識できるようになります。

このタスクについて

ブラウザー・クライアントを再構成するには、以下のステップを実行してください。

手順

1. Tivoli Enterprise Monitoring Services の管理 ユーティリティーを起動します。
2. Tivoli Enterprise Portal ブラウザー項目を右クリックして、「**再構成**」をクリックし、「Tivoli Enterprise Portalブラウザーの構成 (Configure Tivoli Enterprise Portal Browser)」ウィンドウを開きます。
3. ポータル・サーバー領域の下にある「**ホスト**」フィールドに、コンピューターの完全修飾名を入力します。 例えば、`myhost.mycompany.com` などです。

関連概念:

104 ページの『シングル・サインオンについて』
シングル・サインオン (SSO) 機能を使用すると、ユーザー資格情報を再入力しなくても Tivoli Enterprise Portal から他の Tivoli Web ベース・アプリケーションまたは Web 対応アプリケーションを起動したり、他のアプリケーションから Tivoli Enterprise Portal を起動したりできます。また、SSO は IBM Dashboard Application Services Hub がポータル・サーバーからモニター・データを取得するときや、IBM Tivoli Monitoring グラフ Web サービスが他のアプリケーションによって使用されるときにも使用されます。

LTPA キーのインポートおよびエクスポート

認証された資格情報は、LTPA キーを使用して、関連アプリケーションの間で共有されます。

以下のアプリケーションがポータル・サーバーと同じ LTPA キーを使用していることを確認します。

- Tivoli Enterprise Portal を起動する Web ベースまたは Web 対応のアプリケーション
- Tivoli Enterprise Portal クライアントから起動できる Web ベースまたは Web 対応のアプリケーション
- ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントを使用してモニター・データを取得する IBM Dashboard Application Services Hub
- Tivoli Integrated Portal のように IBM Tivoli Monitoring グラフ Web サービスを使用する他のアプリケーション

他のすべての関連 SSO アプリケーションで使用する LTPA キーのソースになるアプリケーションを判断し、その LTPA キーをエクスポートします。

ポータル・サーバーの LTPA キーをエクスポートする場合は、LTPA キーをキー・ファイルにエクスポートする必要があります。エクスポートの手順を実行するときは、キー・ファイルの名前とキーの暗号化に使用するパスワードを指定する必要があります。キー・ファイルとパスワードは、LTPA キーをインポートできるように、上にリストしたアプリケーションの管理者に提供する必要があります。

別のアプリケーションが LTPA キーを提供しない場合、そのアプリケーションの管理者はアプリケーションの LTPA キーをキー・ファイルにエクスポートしてから、キー・ファイルと、キーを暗号化するときに使用したパスワードを提供する必要があります。 提供された LTPA キーはポータル・サーバーにインポートし、パスワードを入力する必要があります。

始める前に

インポート操作およびエクスポート操作を実行するには、Tivoli Enterprise Portal Server が実行中である必要があります。

キーのインポートまたはエクスポートに TEPS/e 管理コンソールを使用する場合、コンソールを開始する必要があります。 118 ページの『TEPS/e 管理コンソールの開始』を参照してください。

LTPA キーをインポートするには、キーをエクスポートしたアプリケーションの管理者から、LTPA キーを含むキー・ファイルとキーの暗号化に使用されたパスワードがあらかじめ提供されている必要があります。

このタスクについて

ご使用の環境に応じて、以下のステップに従い、LTPA キーをインポートまたはエクスポートします。

手順

- **Tivoli Enterprise Monitoring Services の管理 ウィンドウでキーをエクスポートするには、以下の手順を実行します。**
  1. Tivoli Enterprise Portal Server を右クリックして、「**拡張**」→「**TEPS/e 管理**」→「**キーのエクスポート**」をクリックします。
  2. ファイルを作成したり、ファイル・タイプを変更したりするディレクトリーにナビゲートします。 最初に表示されるディレクトリーは、Windows では *ITM_dir*¥InstallITM、Linux および UNIX ではルート・ディレクトリーです。
  3. LTPA キーを置くファイルの名前を入力し、「**保存**」をクリックします。
  4. 「キーのエクスポート」ウィンドウで、ファイルの暗号化に使用するパスワードを入力し、「**OK**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。
- **Tivoli Enterprise Monitoring Services の管理 ウィンドウでキーをインポートするには、以下の手順を実行します。**
  1. Tivoli Enterprise Portal Server を右クリックして、「**拡張**」→「**TEPS/e 管理**」→「**キーのインポート**」をクリックします。
  2. 表示された「**開く**」ウィンドウで、鍵ファイルが置かれているディレクトリーにナビゲートします。 最初に表示されるディレクトリーは、Windows では *ITM_dir*¥InstallITM、Linux および UNIX ではルート・ディレクトリーです。
  3. インポートするファイルの名前を入力し、「**開く**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。その他の参加サーバーからキーをインポートする場合は、このインポート処理を繰り返します。
  4. ファイルの暗号化解除に必要なパスワードを入力し、「**OK**」をクリックします。 ファイルが作成および暗号化されている間コンソール・ウィンドウが表示され、その後「シングル・サインオン」ウィンドウに戻ります。
  5. その他の参加サーバーからキーをインポートする場合は、このインポート処理を繰り返します。
- **AIX® コマンド行および Linux コマンド行でキーをエクスポートするには、`./exportKeys.sh <filename> <password>` を実行します。** スクリプトは *ITM_dir*/*platform*/iw/scripts にインストールされています。 例えば、AIX では /opt/IBM/ITM/aix533/iw/scripts、Linux では /opt/IBM/ITM/li6263/iw/scripts、zLinux では /opt/IBM/ITM/ls3263/iw/scripts などです。

- **AIX コマンド行および Linux コマンド行でキーをインポートするには、`./importKeys.sh <filename> <password>` を実行します。** スクリプトは *ITM_dir*/*platform*/iw/scripts にインストールされています。
- **TEPS/e 管理コンソールで LTPA キーをエクスポートするには、以下の手順を実行します。**
  1. 「**セキュリティー**」→「**グローバル・セキュリティー**」と選択します。
  2. 「**LTPA**」を選択します。
  3. 「**パスワード**」フィールドと「**パスワードの確認**」フィールドに、鍵ファイルを暗号化するためのパスワードを入力します。
  4. 「**完全修飾鍵ファイル名**」フィールドに、鍵ファイルの完全修飾パスおよびファイル名を入力します。
  5. 「**キーのエクスポート**」をクリックします。
  6. 「**OK**」、「**保存**」の順にクリックします。
- **TEPS/e 管理コンソールで LTPA キーをインポートするには、以下の手順を実行します。**
  1. 「**セキュリティー**」→「**グローバル・セキュリティー**」と選択します。
  2. 「**LTPA**」を選択します。
  3. 「**パスワード**」フィールドと「**パスワードの確認**」フィールドに、鍵ファイルの暗号化を解除するためのパスワードを入力します。
  4. 「**完全修飾鍵ファイル名**」フィールドに、鍵ファイルの完全修飾パスおよびファイル名を入力します。
  5. 「**キーのインポート**」をクリックします。
  6. 「**OK**」、「**保存**」の順にクリックします。

次のタスク

ポータル・サーバーの LTPA キーをエクスポートした場合は、キー・ファイルと、キーの暗号化に使用したパスワードを他の関連 SSO アプリケーションの管理者に提供し、キーをインポートできるようにします。

新規 LDAP ユーザーの管理

Tivoli Enterprise Portal、または IBM Dashboard Application Services Hub などその他の関連 SSO アプリケーションにログインするためアクセス権限を持つ必要のある新規ユーザーがポータル・サーバーの LDAP ユーザー・レジストリーに追加されたときは、必ずそのユーザーの Tivoli Enterprise Portal ユーザー ID を作成し、LDAP 識別名にマップする必要があります。

Tivoli Enterprise Portal ユーザー ID には、Tivoli Enterprise Portal の許可とアクセスできるモニター・アプリケーションも割り当てる必要があります。180 ページの『ユーザー ID の管理』および 173 ページの『ユーザー管理』を参照してください。許可やモニター・アプリケーションの割り当てが不要な Tivoli Enterprise Portal ユーザーは、許可ポリシーが使用されるときに Tivoli Enterprise Portal クライアントを使用しないモニター・ダッシュボード・ユーザーだけです。

注: ダッシュボード・ユーザーがモニター・データに初めてアクセスすると、ユーザーの LDAP 識別名にマップされたユーザー ID がまだ存在しない場合は、そのユ

ーザーの Tivoli Enterprise Portal ユーザー ID が自動的に作成されます。この場合、Tivoli Enterprise Portal ユーザー ID はランダム生成 ID になり、ユーザーには許可が一切割り当てられません。許可ポリシーではなく、Tivoli Enterprise Portal の許可を使用して、ダッシュボードでのモニター対象リソースへのアクセスを制御する場合、またはダッシュボード・ユーザーが Tivoli Enterprise Portal を起動できる場合は、ユーザー ID に許可とアクセスできるモニター対象アプリケーションを割り当てます。

LDAP ユーザー・レジストリーと Tivoli Enterprise Portal ユーザーの自動化された同期を管理するために、スクリプトを使用することができます。LDAP サーバーのユーザー・アカウント管理用スクリプトを使用すると、ユーザー・アカウントに対する変更 (例えば、ユーザーの追加や削除) が、**tacmd createuser** および **tacmd deleteuser** コマンドによって対応する Tivoli Enterprise Portal ユーザー ID にも適用されるようになります。Tivoli Enterprise Portal と LDAP ユーザー・レジストリーのユーザーが確実に同期化されるよう、環境での必要性に応じた頻度で、スケジュールされたアクションとしてユーザー同期スクリプトを実行してください。

ポータル・サーバーでの LDAP 認証の無効化

エラーが発生する場合、ポータル・サーバーで LDAP 認証を無効にする必要があります。

このタスクについて

LDAP 接続が失敗し、LDAP ベースの認証をオフに切り替える通常の手順が機能しない場合は、以下のステップを実行する必要があります。

手順

Windows

1. Tivoli Enterprise Monitoring Services の管理アプリケーションを使用して、ポータル・サーバー・サービスを停止します。
2. *candle_home*¥CNPSJ¥ スクリプトで **disableLDAPRepository.bat** スクリプトを実行します。
3. Tivoli Enterprise Monitoring Services の管理アプリケーションを使用して、ポータル・サーバーを再構成し、「LDAP でのユーザー検証」オプションを使用不可にします。
4. Tivoli Enterprise Monitoring Services の管理アプリケーションを使用して、ポータル・サーバー・サービスを開始します。これで、モニター・サーバー経由のポータル・サーバー認証が使用可能になります。
5. モニター・サーバーも LDAP を使用するよう構成されている状況で、LDAP が使用できないためにこの手順を実行している場合は、モニター・サーバーの構成も、認証に LDAP を使用しないように変更する必要があります。モニター・サーバーの構成ヘルプを使用して、この構成変更を完了してください。

AIX Linux

1. コマンド・プロンプトで、インストール・ディレクトリーから **./itmcmd agent stop cq** コマンドを実行して、ポータル・サーバーを停止します。

2. *candle_home*/*arch*/iw/ スクリプト (*arch* は li6263 や aix533 といったマシンのアーキテクチャー) から、**./disableLDAPRepository.sh** スクリプトを実行します。
3. コマンド・プロンプトで、インストール・ディレクトリーから **./itmcmd config -A cq** コマンドを実行して、ポータル・サーバーを再構成し、LDAP 認証を使用不可にします。
4. コマンド・プロンプトで、インストール・ディレクトリーから **./itmcmd agent start cq** コマンドを実行して、ポータル・サーバーを開始します。これで、モニター・サーバー経由のポータル・サーバー認証が使用可能になります。
5. モニター・サーバーも LDAP を使用するよう構成されている状況で、LDAP が使用できないためにこの手順を実行している場合は、モニター・サーバーの構成も、認証に LDAP を使用しないように変更する必要があります。モニター・サーバーの構成ヘルプを使用して、この構成変更を完了してください。

モニター・サーバーからポータル・サーバーへの LDAP 認証のマイグレーション

ご使用の環境がハブ・モニター・サーバーを使用する LDAP 認証用に既に構成されていて、今度はシングル・サインオン用に LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成する場合は、このトピックのステップを実行します。

始める前に

手順を開始する前にすべてのユーザーが Tivoli Enterprise Portal からログオフしていることを確認し、手順が完了するまで再ログインしないようにしてください。

このタスクについて

以下のステップを実行して、ハブ・モニター・サーバーでのセキュリティー検証を一時的に無効にし、LDAP ユーザー・レジストリーを使用するようにポータル・サーバーを構成し、Tivoli Enterprise Portal ユーザー ID を LDAP ユーザー・レジストリーの識別名にマップしてから、ハブ・モニター・サーバーでのセキュリティー検証を再度有効化します。

手順

1. 一時的に Tivoli Enterprise Monitoring Server のセキュリティー検証を使用不可にします。
   - Windows Tivoli Enterprise Monitoring Services の管理 ユーティリティーを使用して、ハブ・モニター・サーバーを再構成します。
     a. Tivoli Enterprise Monitoring Server を右クリックし、「**再構成**」をクリックします。
     b. 「Tivoli Enterprise Monitoring Server の構成」ウィンドウで、□「**セキュリティー: ユーザーを検証**」を使用不可にし、「**OK**」をクリックします。
     c. 次のウィンドウで既存の設定を使用する場合は、「**OK**」をクリックします。
     d. ハブ・モニター・サーバーを再始動します。

- Linux UNIX コマンド行から以下を実行します。
  a. /opt/IBM/ITM/bin ディレクトリー (または Tivoli Management Services をインストールしたディレクトリー) に移動します。
  b. 次のコマンドを実行します。ここで、*tems_name* は、ご使用のモニター・サーバーの名前です (例えば、HUB_itmdev17)。

     ```
     ./itmcmd config -S -t tems_name
     ```

  c. 既存の値を使用する場合は、「**セキュリティー: ユーザーを検証**」のプロンプトが表示されるまで Enter キーを押します。
  d. セキュリティーを使用不可にするには、NO を入力します。
  e. 構成が完了するまで続けて Enter キーを押します。
  f. ハブ・モニター・サーバーを再始動します。

2. LDAP レジストリー内の **sysadmin** UID の名前を変更します (例えば、sysadmin_tems)。
3. ポータル・サーバーを介して LDAP 認証およびシングル・サインオンを構成します。Tivoli Enterprise Monitoring Services の管理 ユーティリティー、**itmcmd** コマンド行インターフェース (Linux および UNIX の場合)、または TEPS/e 管理コンソールを使用して、ポータル・サーバーを構成します。 手順については、100 ページの『ポータル・サーバーを使用した LDAP ユーザー認証』を参照してください。
4. Tivoli Enterprise Portal Server を開始し、Tivoli Enterprise Portalに **sysadmin** としてログオンします。
5. LDAP ユーザー ID へのすべてのユーザー・マッピングを調整します。
   a. 「**ユーザー管理**」をクリックして「ユーザー管理」ウィンドウを開きます。
   b. ユーザー ID の行を右クリックして再マップし、「**ユーザーの変更**」をクリックします。
   c. 「**検索**」をクリックして、ポータル・サーバーに関連付ける LDAP 識別名を見つけます。
   d. ユーザーの識別名を選択します。複数の項目が表示されている場合は、正しい LDAP サフィックスを持つ項目 (親項目) を選択してください。 例: UID=TIVOLIUSER,O=MYCOMPANY および uid=myname, dc=tivoli, dc=ibm, dc=us。 これらの編成値の 1 つを含む項目が表示されている場合、その項目は選択しないでください。O=DEFAULTWIMITMBASEDREALM は、ハブ・モニター・サーバー を使用して認証を受けるユーザー ID のデフォルト・サフィックスです。o=defaultWIMFileBasedRealm は、TEPS/e ユーザー・レジストリーのデフォルト・サフィックスです。
   e. 「**OK**」をクリックしてマッピングを保存し、「ユーザー管理」ウィンドウに戻って各ユーザー ID の DN の変更を続行します。
6. Tivoli Enterprise Portal からログアウトする前に、LDAP 管理者に LDAP sysadmin アカウントの名前を変更して **sysadmin** に戻してもらい、次に Tivoli Enterprise Portal の sysadmin ユーザー・アカウントを LDAP sysadmin DN にマップします。
7. 変更を保存し、Tivoli Enterprise Portal からログアウトします。

8. 再度ステップ 1 を実行して (ただし、今回はセキュリティー検証を有効にします)、Tivoli Enterprise Monitoring Server セキュリティー検証を再度有効化します。

タスクの結果

この時点でマイグレーションは完了です。

次のタスク

以下のステップを実行して、認証の変更を確認します。

1. **tacmd** ログイン・コマンドを使用して、ハブ・モニター・サーバーのセキュリティーが有効になっていることを確認します。有効なユーザー名とパスワード、および有効ではないユーザー名またはパスワードを使用して、ログインを試行します。
2. sysadmin ユーザーを使用して Tivoli Enterprise Portal にログインします。
3. ポータル・サーバー用に構成されている LDAP ユーザー・レジストリーのユーザーを使用して、Tivoli Enterprise Portal にログインします。

Tivoli Enterprise Monitoring Automation Serverを使用した認証

Tivoli Enterprise Monitoring Automation Server は、Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) サービス・プロバイダーを提供することで、ハブ・モニター・サーバーを拡張します。サービス・プロバイダーは、モニター・リソース (コンピューター・システム、ソフトウェア・サーバー、データベースなど) を Jazz for Service Management Registry Services・コンポーネントに登録し、また OSLC クライアントからのリソース正常性メトリックの HTTP GET 要求に応答します。

デフォルトでは、Performance Monitoring サービス・プロバイダーは、OSLC クライアントからの HTTP GET 要求を認証しません。Performance Monitoring サービス・プロバイダーがこれらの要求を認証するようにする場合は、Jazz for Service Management のセキュリティー・サービス・コンポーネントをインストールして構成する必要があります。セキュリティー・サービスにより、非 WebSphere ベース・アプリケーション (Performance Monitoring サービス・プロバイダーなど) でも Lightweight Third Party Authentication (LTPA) ベースのシングル・サインオンに参加できるようになります。Registry Servicesおよびセキュリティー・サービスは、同じ WebSphere Application Serverにインストールする必要があります。また、OSLC クライアント・アプリケーションと同じ LDAP ユーザー・レジストリーを使用するように構成する必要があり、さらにシングル・サインオン用に構成する必要があります。

注: Registry Servicesおよびセキュリティー・サービスと OSLC クライアント・アプリケーションは、同じインターネットおよびイントラネットのドメイン (例えば、mycompany.com) またはそのサブドメインのいずれかに配置されていなければなりません。また、LDAP リポジトリーを使用するように WebSphereApplication Server を構成する際に設定するのと同じレルム名を使用するように構成する必要もあります。

シングル・サインオン用にRegistry Servicesおよびセキュリティー・サービスを構成するには、それらがインストールされているアプリケーション・サーバーの LTPA キーを生成し、そのキーをエクスポートしてから、Performance Monitoring サービス・プロバイダーに HTTP GET 要求を送信する OSLC クライアント・アプリケーションにその LTPA キーをインポートします。Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)の『中央ユーザー・レジストリーのための Jazz for Service Management の構成』および『SSO 向けの Jazz for Service Management の構成』を参照してください。これらの章には、LDAP ユーザー・レジストリーを使用するためのRegistry Servicesとセキュリティー・サービスの構成、および LTPA キーの生成とエクスポートに関する説明が含まれています。

Performance Monitoring サービス・プロバイダーは、Tivoli Enterprise Monitoring Automation Server KAS_SECURITY_SERVICES_ENABLED 環境変数を YES に設定し、オートメーション・サーバーを再始動することで、セキュリティー・サービスを使用して OSLC クライアント要求を認証するように構成する必要があります。

Performance Monitoring サービス・プロバイダーが HTTP GET 要求を OSLC クライアントから受け取ると、要求の認証のために LTPA トークンをセキュリティー・サービスに転送します。要求に LTPA トークンが含まれていない場合、またはセキュリティー・サービスがトークンが無効であるか有効期限が切れていることを示した場合、Performance Monitoring サービス・プロバイダーは HTTP 401 状況コードを返し、要求を認証できなかったことを示します。

注: Performance Monitoring サービス・プロバイダーはRegistry Servicesに要求を送信する際に基本認証を使用するため、サービス・プロバイダーのリソース登録の対話では、LTPA トークンは関係しません。

Microsoft Active Directory を使用した LDAP ユーザー認証

Microsoft の LDAP ベースの Active Directory 製品を使用したユーザー認証を設定するには、以下のトピックを参考にしてください。

これらのトピックは、Active Directory 環境に実装されているように LDAP を組み込むために完了する必要のあるステップについて説明します。Active Directory の観点から手順が示されています。この処理を使用して、作業環境に Tivoli Monitoring のセキュリティーを実装する方法について説明する 2 つのユーザー・シナリオ (1 つはモニター・サーバーと Active Directory との統合を示し、もう 1 つはポータル・サーバーと Active Directory との統合を示す) が用意されています。 155 ページの『ユーザー・シナリオ』を参照してください。

この手順では、TEPS/e Web ブラウザー・インターフェースを使用してポータル・サーバーの構成を完了します。 117 ページの『TEPS/e 管理コンソールの使用』を参照してください。

注:

1. LDAP サーバーを使用してユーザーを認証するようにポータル・サーバーを構成する方法には、モニター・サーバー認証によって課せられる制限である 10 文字

より長いユーザー ID を使用できるという利点があります。また、モニター・サーバー認証ではサポートされない SSO (シングル・サインオン) がサポートされます。

モニター・サーバー・ベースのユーザー認証でのみ、ユーザー ID を使用して SOAP サーバー要求を実行したり、SOAP サーバー・メソッドを呼び出す CLI コマンドを発行したりすることができます。

2. IBM Tivoli Monitoring の LDAP ユーザー認証を有効化するための構成手順およびステップは、すべての LDAP の実装 (Active Directory、Tivoli Directory Server など) で同じですが、指定する構成値は異なります。 これらの違いは、LDAP 実装そのものの違いによるものです。最も顕著な違いは、ディレクトリーに存在するオブジェクトの識別名の構文です。 さらに、カスタマイズされた LDAP スキーマと LDAP の実装との LDAP スキーマの違いは、指定される LDAP ユーザー認証の構成値に大きな影響を与えます。
3. この一連のトピックのシナリオは、Microsoft Active Directory バージョン 2003 環境を前提としていますが、これらの説明およびシナリオは、Active Directory Server 2008 および Active Directory Server 2008 R2 でも検証済みです。

構成では、提供されるすべての情報を使用して、指定された LDAP ベースからターゲット LDAP ユーザー・レジストリーへの接続、バインド、照会、およびレコードのフィルター操作が行われ、ユーザーが認証されます。モニター・サーバーおよびポータル・サーバーの LDAP ユーザー認証の構成は別個の操作であるため、これらの構成は、(完了後に) 個別に有効および無効にできます。モニター・サーバーの LDAP ユーザー認証を構成するステップがポータル・サーバーの LDAP ユーザー認証に適合するとは考えないでください。その逆も同じです。

事前処理

稼働している Active Directory 環境が必要です。また、以下の Active Directory の概念に関する知識が必要です。

- 組織単位 (部門名)

  ADSI 編集 MMC スナップイン
- グループ・ポリシー管理
- ユーザー管理

  Active Directory ユーザー・オブジェクト・スキーマ

Tivoli Enterprise Monitoring Server および Tivoli Enterprise Portal Server を、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」で説明しているようにインストールしている必要があります。 89 ページの『第 5 章 ユーザー認証の使用可能化』に記載されている基本情報についてよく理解しておいてください。

モニター・サーバーまたはポータル・サーバーの認証で許可される LDAP ユーザーを決定する際は、ご使用のサイトの Active Directory の管理者に協力を求めてください。

ユーザーを含む OU 階層を作成することもベスト・プラクティスです。この階層の作成により、ベース名のディレクトリー検索が容易になり、また Tivoli Monitoring から LDAP へのユーザー認証のパフォーマンスを向上させながら検索時間を制限します。 137 ページの図 1 は、コンテナーの `ITMtepsUsers` と `ITMtemsUsers` を持つ

OU=ITMUsers の階層を含むサンプルの構成を示しています。このスキーマを使用すれば、認証するモニター・サーバーのユーザーの検索用のベースは CN=ITMtemsUsers,OU=ITMUsers,DC=*company*,DC=com になり、認証するポータル・サーバーのユーザーのベースは CN=ITMtepsUsers,OU=ITMUsers,DC=*company*,DC=com になります。

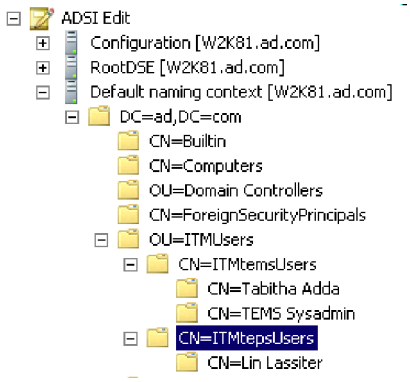


図 1. Tivoli Monitoring サーバー用の推奨の LDAP ユーザー階層

また、ご使用の Active Directory のユーザー・オブジェクト/属性スキーマについても認識しておく必要があります。この情報は、ご使用のモニター・サーバーの LDAP フィルター構成をコーディングする際に、またポータル・サーバーの TEPS/e のリポジトリー・セキュリティーのログイン・プロパティーのために必要です。138 ページの図 2 は、あるユーザーの可能なアカウント設定を示しています (この Tivoli Enterprise Portal Server ユーザーは Tivoli Enterprise Monitoring Server ユーザーとしても許可されている必要があります)。

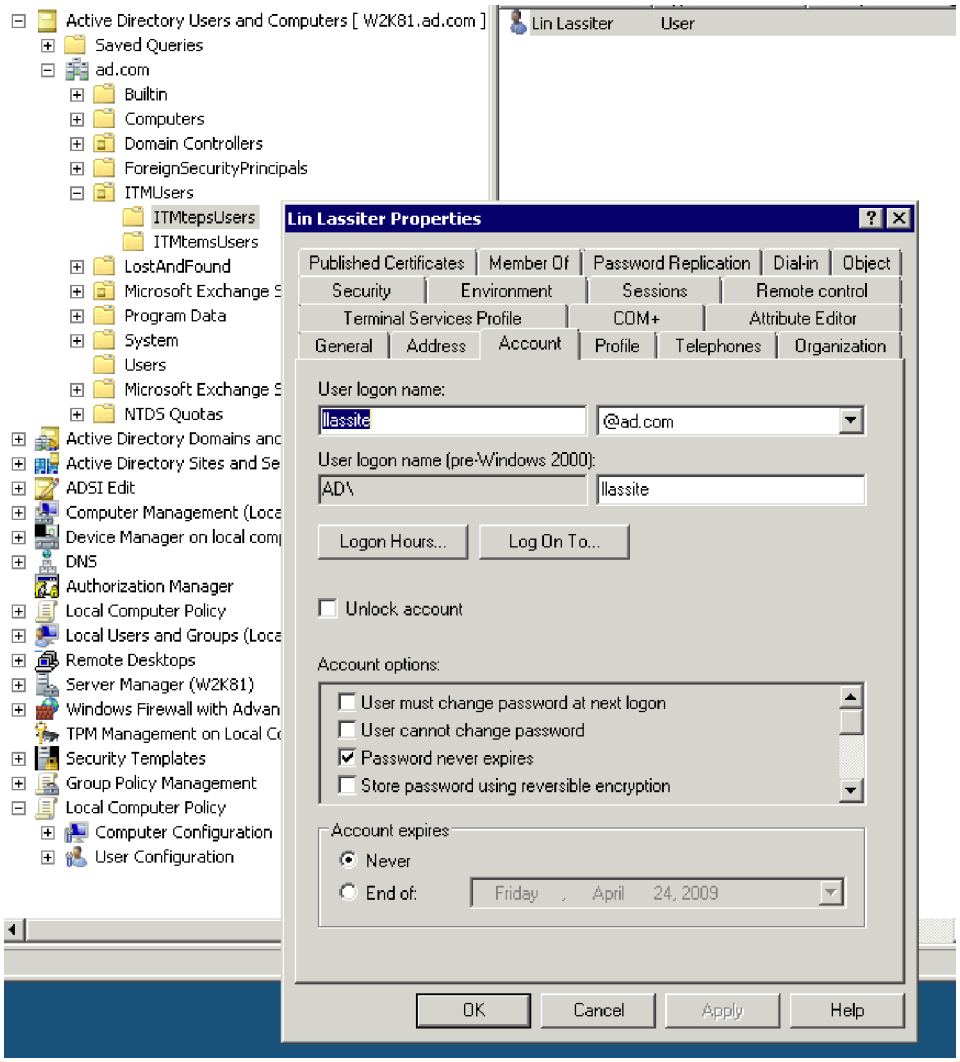


図 2. ポータル・サーバーのユーザー・プロパティー

TEPS/e の LDAP ユーザー認証用の構成では、Active Directory のユーザー・オブジェクト属性ログイン・プロパティーを指定する必要があります。このプロパティーには対応するユーザー名 (この例では *llassite*) が含まれます。 139 ページの図 3 は、ユーザー *llassite* の Active Directory ユーザー・クラスのインスタンスを示しています。

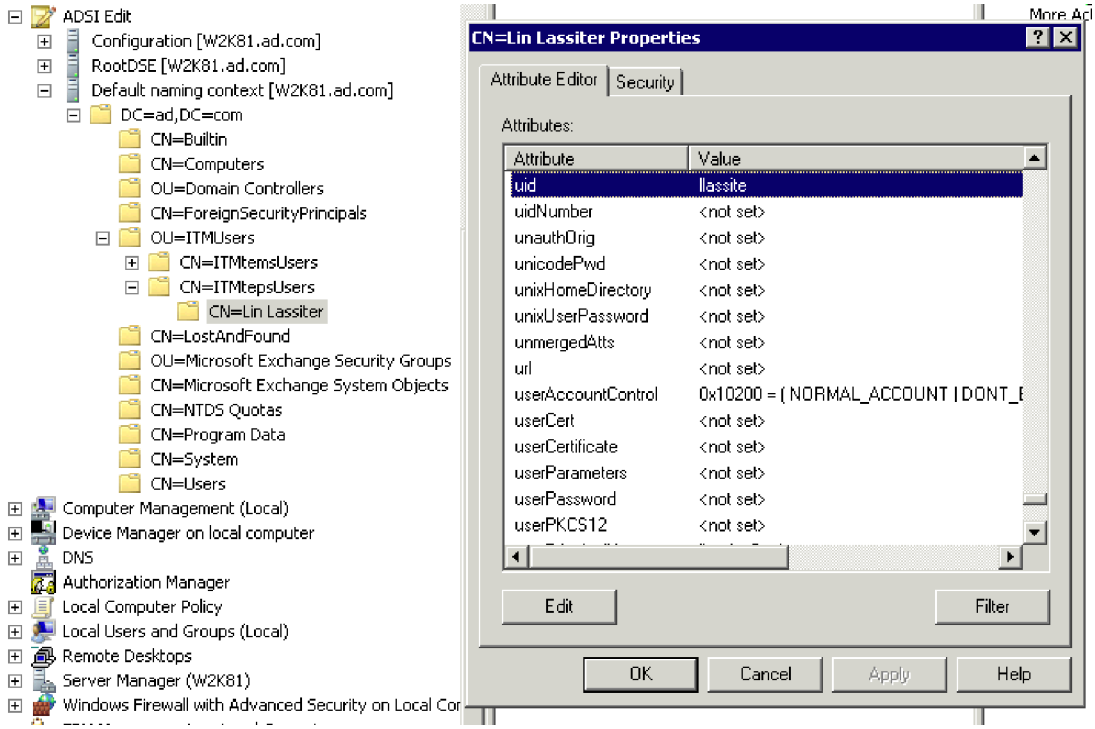


図 3. LDAP ユーザー・プロパティー

TEPS/e の「**uid**」の LDAP ユーザー認証プロパティーをポータル・サーバーのユーザー・アカウントと一致させる必要があります。これを行うには、ポータル・サーバーのユーザー・アカウント *llassite* が `CN=Lin Lassiter,CN=ITMtepsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com` LDAP オブジェクト (これは、`CN=ITMtepsUsers,OU=ITMUsers,DC=`*`company`*`,DC=com` ベース・レコードで始まるディレクトリーを検索することによって見つかります) 内の *uid=llassite* に一致するように、ユーザー *llassite* の Active Directory のユーザー/uid 属性を編集し、また「**uid=llassite**」を設定します。

137 ページの図 1、 138 ページの図 2、および図 3 は、LDAP 認証に使用される Active Directory のプロパティーについて理解しやすくするために提供されています。 LDAP ユーザーが Active Directory 内のどこに存在するかの認識 (このディレクトリー内の Tivoli Monitoring ユーザーの照会または検索を行うためのベース) とユーザー・スキーマ (認証に使用される正確なユーザー名が含まれたユーザー・オブジェクト属性) は、Tivoli Enterprise Monitoring Server または Tivoli Enterprise Portal Server の LDAP ユーザー認証の正常な構成にとって非常に重要です。

注: アプリケーション、ビュー、およびグループなどの Tivoli Monitoring の機能に対するポータル・サーバーのユーザー・アカウントの許可は、 140 ページの図 4 で示されるように、ポータル・サーバーのユーザー管理ツール内で引き続き管理されます。

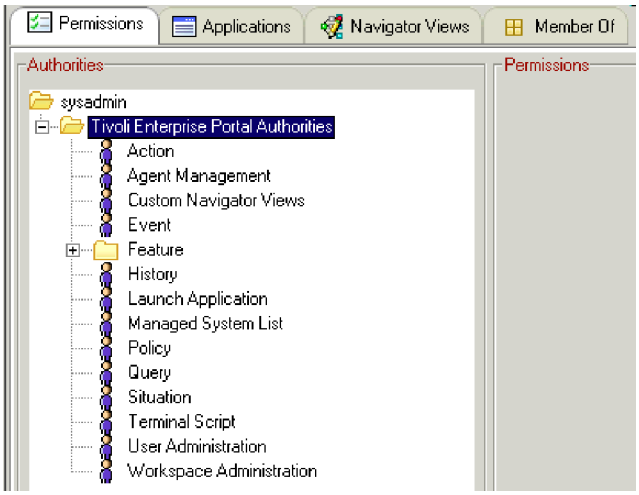


図 4. Tivoli Enterprise Portal Server ユーザー許可

LDAP ユーザー認証は、個々の Tivoli Monitoring ユーザーおよびユーザー・グループに対してのみ使用できます。個々の Tivoli Monitoring ユーザーに対する LDAP 認証の使用可能化によって、IBM Tivoli Monitoring の側と LDAP 側の両方に最大限の柔軟性が確保されます。 Active Directory ユーザーと Tivoli Monitoring ユーザーの自動化された同期を管理するために、スクリプトを使用することができます。Active Directory ユーザー・アカウントのデータ収集スクリプトにより、 Active Directory のアカウントに対する変更 (例えば、ユーザーの追加や削除) が、CLI の **tacmd** によって対応する Tivoli Enterprise Portal ユーザーに反映されることを保証することができます。

ロードマップの概要

IBM Tivoli Monitoring ユーザー認証環境をサイトの Active Directory 実装に組み込むには、このトピックで説明するステップを実行してください。

1. 141 ページの『Active Directory 内でのモニター・サーバー・ユーザーおよびポータル・サーバー・ユーザーの計画および作成』

   このトピックで説明するステップに従います。

2. 142 ページの『ポータル・サーバーのユーザー・アカウントとアクセス権の作成および構成 (必要な場合)』

   このステップをスキップ: Tivoli Enterprise Portal ユーザーの認証に LDAP サーバーを使用せず、IBM Dashboard Application Services Hub などの他の製品との統合用にシングル・サインオンを構成する必要がない場合。

   サイトでポータル・サーバーのユーザー認証が必要な場合は、Tivoli Enterprise Portal の「ユーザー管理」インターフェースまたは **tacmd** コマンド行インターフェースのいずれかを使用します。

   これらのユーザー・アカウントでは、認証に LDAP が使用されます。したがって、選択されるユーザー ID は、Active Directory で指定されるユーザー ID に正確に一致する必要があります。 選択する必要のある属性については、 139 ページの図 3 を参照してください。

3. 142 ページの『ポータル・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合)』

   このステップをスキップ: Tivoli Enterprise Portal ユーザーの認証に LDAP サーバーを使用せず、IBM Dashboard Application Services Hub などの他の製品との統合用にシングル・サインオンを構成する必要がない場合。

   サイトでポータル・サーバーの認証が必要な場合にこのステップを実行します。
4. 150 ページの『必要な場合の TEPS/e for TLS/SSL の構成』

   通常、TEPS/e はデフォルトで TLS/SSL 対応になっています。ポータル・サーバーと LDAP サーバー間の TLS/SSL 通信を構成する必要がある場合は、TEPS/e 管理コンソールを使用します。
5. 150 ページの『モニター・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合)』

   このステップをスキップ: モニター・サーバー・ユーザーの認証に LDAP ユーザーを使用しない場合。

   サイトでモニター・サーバーの認証が必要な場合にこのステップを実行します。

Active Directory 内でのモニター・サーバー・ユーザーおよびポータル・サーバー・ユーザーの計画および作成

Tivoli Enterprise Monitoring Server 向けまたは Tivoli Enterprise Portal Server 向けの Active Directory ユーザーを作成する場合は、次のようにします。

1. モニター・サーバー・ユーザーおよびポータル・サーバー・ユーザーの OU 階層を作成します。

   137 ページの図 1を参照してください。Microsoft Management Console (MMC) のスナップイン「**ADSI 編集**」を使用します。
2. Active Directory で、モニター・サーバー・ユーザーおよびポータル・サーバー・ユーザー (および、必要に応じてグループ) を作成します。

   138 ページの図 2を参照してください。MMC の「**Active Directory ユーザーとコンピューター**」機能を使用します。
3. 目的のユーザー/グループ・ポリシーを、Active Directory の新しいユーザーおよびグループに適用します。

   GPO に MMC スナップインを使用します。

Tivoli Monitoring および LDAP 間では、現在、ユーザーの同期は行われません。ユーザー・アカウントは、スクリプトを使用して同期できます。ユーザー・アカウントの修正 (IBM Tivoli Monitoring に適用される OU に限定されます) を継続して認識するには、Active Directory のスクリプトを使用します。 検出されたこれらの修正は、その後、CLI **tacmd** コマンド経由で Tivoli Monitoring ユーザーに、また、スクリプトを使用して Active Directory ユーザーに適用されます。 ご使用の環境で Tivoli Monitoring ユーザーと Active Directory ユーザーが確実に同期化されているようにするのに必要な頻度で、スケジュールされたアクションとしてユーザー同期スクリプトを実行する必要があります。

ポータル・サーバーのユーザー・アカウントとアクセス権の作成および構成 (必要な場合)

このステップをスキップ: Tivoli Enterprise Portal ユーザーの認証に LDAP サーバーを使用せず、IBM Dashboard Application Services Hub などの他の製品との統合用にシングル・サインオンを構成する必要がない場合。

既に作成されている各 Active Directory アカウントには、一致する、Tivoli Enterprise Portalのユーザー・アカウントが必要です。 Tivoli Enterprise Portalのユーザー ID は、TEPS/e 構成内での使用が予定されている、Active Directory の TEPS ユーザー・オブジェクトの属性フィールドに正確に一致する必要があります (139 ページの図 3 を参照してください)。

IBM Tivoli Monitoring 内でのユーザー・アカウント操作用に、必要なすべての許可、アプリケーション、ビュー、およびグループを構成します。詳しくは 171 ページの『第 6 章 Tivoli Enterprise Portal ユーザー許可の使用』を参照してください。(これらのユーザー・アカウントのアクセス権、アプリケーション、ビュー、およびグループは Active Directory では使用できないことに注意してください。また、Tivoli Monitoring から Active Directory に変換されることもありません。 140 ページの図 4 を参照してください。)

注: Active Directory のユーザー・オブジェクト・スキーマを更新して、IBM Tivoli Monitoring ユーザーのアクセス権、アプリケーション、ビュー、およびグループを Active Directory にマップすることができます。 その後、Tivoli Monitoring と Active Directory 間のユーザー同期に加え、Active Directory のスクリプトおよび Tivoli Monitoring CLI の **tacmd** コマンドを介した、Active Directory による管理に、これらの新しいスキーマ属性を役立てることができます。

LDAP ディレクトリーへのデフォルトの **sysadmin** アカウントの追加はお勧めしません。 **sysadmin** アカウントは、ローカルのモニター・サーバーの「**セキュリティー: ユーザーを検証**」許可用に予約しておく必要があります。これによって、モニター・サーバーおよびポータル・サーバーにアクセスするための LDAP 以外の方法が保持されます。

「**ユーザー ID**」および「**ユーザー説明**」の形式は任意ですが、Active Directory で既に作成済みの「**ユーザー名**」および「**ユーザー説明**」に合わせるようにすることが推奨されます。

TEPS/e の LDAP 構成に基づいて Tivoli Monitoring のユーザー ID を LDAP ユーザー・アカウントにバインドするには、「識別名」が不可欠です。この点は、もっと後で説明します。現時点では、エントリー `UID=userid,O=DEFAULTWIMITMBASEDREALM` を選択します。

ポータル・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合)

このステップをスキップ: Tivoli Enterprise Portal ユーザーの認証に LDAP サーバーを使用せず、IBM Dashboard Application Services Hub などの他の製品との統合用にシングル・サインオンを構成する必要がない場合。

目的の IBM Tivoli Monitoring 権限を持つTivoli Enterprise Portalのユーザー ID が作成され、これらの同じユーザー ID が Active Directory 内に存在するようになったので、これらのポータル・サーバー・ユーザーに対して LDAP ユーザー認証を有効にする必要があります。TEPS/e Web ブラウザー・インターフェースを使用して、ポータル・サーバーの LDAP ユーザー・レジストリー構成の詳細および Active Directory のベース名構成を設定します。TEPS/e LDAP 構成のすべての手順は、119 ページの『TEPS/e 管理コンソールを使用した LDAP 認証のためのポータル・サーバーの構成』で詳しく説明されています。

TEPS/e 管理コンソールの開始

`http://localhost:15205/ibm/console` へのアクセスに問題がある場合は、118 ページの『TEPS/e 管理コンソールの開始』で詳しく説明されている TEPS/e の有効化およびパスワード設定ステップが完了していることを確認してください。また、TEPS/e インターフェースを使用する場合は、ポータル・サーバーを再始動するたびにこのインターフェースを有効にする必要があります。 (TEPS/e を有効にすると TEPS/e インターフェースのみが制御され、ポータル・サーバーの LDAP の有効化は制御されないことに注意してください。) このアクティビティーのログ情報は次の場所にあります。

- Windows `%CANDLE_HOME%¥CNPSJ¥profiles¥ITMProfile¥logs¥ITMServer`
- Linux `$CANDLEHOME/$INTERP/iw/profiles/ITMProfile/logs/ITMServer`

119 ページの『TEPS/e 管理コンソールを使用した LDAP 認証のためのポータル・サーバーの構成』で説明されているステップを実行する際には、下記の注意事項を確認します。

- レルムは、TEPS/e および他の WebSphere Application Server の統合リポジトリー・セットを識別します。独自のレルム名を選択できますが、この値は、指定したインターネット・ドメインまたはイントラネット・ドメイン内で SSO に対して構成されるすべてのアプリケーションで同じである必要があります。SSO を構成しない場合、「**レルム名**」はデフォルトの名前をそのまま使用する必要があります。ただし、この名前が環境内ですでに使用されている場合を除きます。

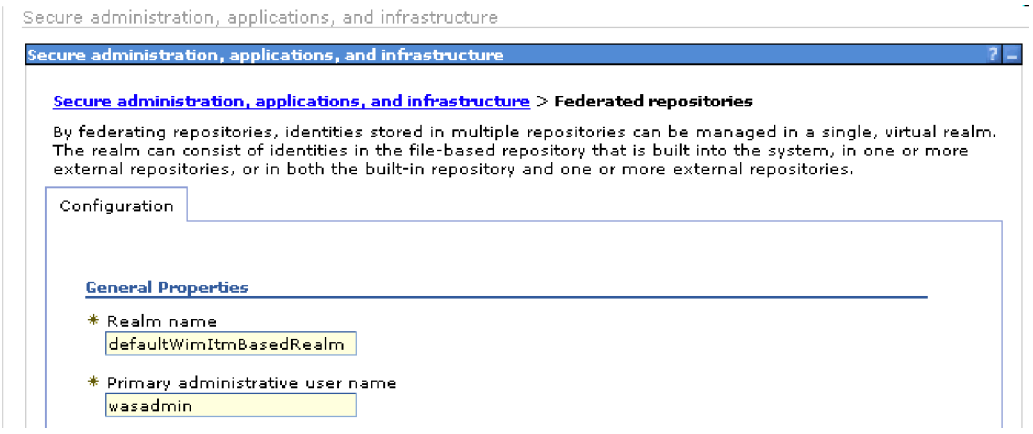


図 5. デフォルト値の受け入れ

- 「**リポジトリー ID**」 を入力するときは、分かりやすい名前を選択します。

「**リポジトリー ID**」は、LDAP サーバーの情報、**LDAP バインド・パスワード**、および **LDAP ログイン・プロパティー**を保持する TEPS/e 内の構成コンテナーへの参照ラベルになります。これは、正確に一致するポータル・サーバーのユーザー ID を検索するための、Active Directory のユーザー・クラス属性です (139 ページの図 3を参照してください)。

さらに、このリポジトリーはポータル・サーバーの LDAP 認証で検索対象となる 1 つ以上の LDAP ベース値 (コンテナー) と関連付けられます。ここでも、136 ページの『事前処理』で指摘したように、この構成ステップには OU 計画をお勧めします。 OU 計画が適切な場合、IBM Tivoli Monitoring LDAP ユーザー認証による検索はベース以下に制限されます。ベース検索の効率化および LDAP ユーザー認証のパフォーマンスのために、ITMtepsUsers OU 内のユーザーのグループ化 (137 ページの図 1 を参照してください) をお勧めします。

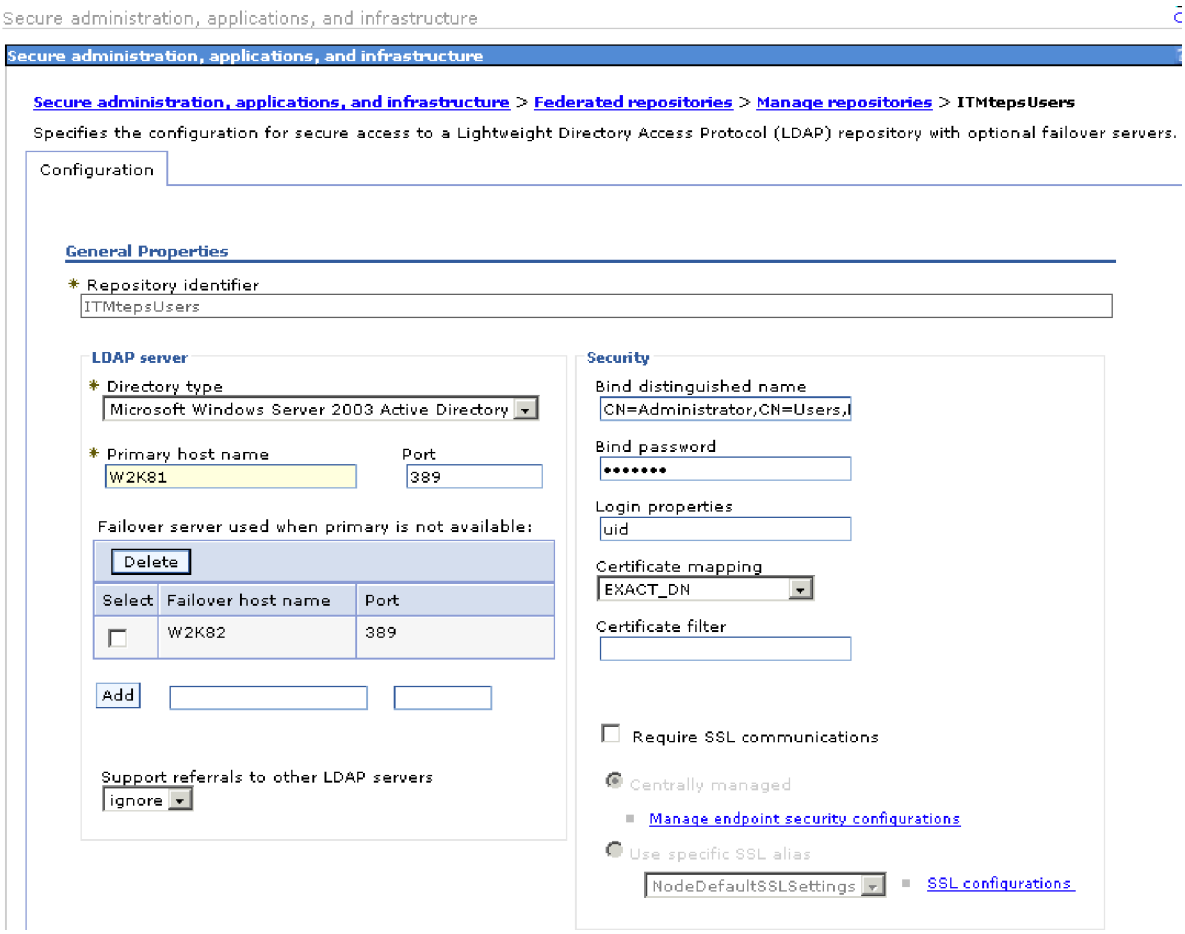


図 6. リポジトリーの構成

一般プロパティー → 「リポジトリー ID」

これは、任意の形式のフィールドです。ここでは、ご使用の Active Directory 環境で定義されているユーザーへの関連付けを管理者が容易に行うことができる、意味のある名前を選択することをお勧めします。 この場合は、ITMtepsUsers が指定されています。これが、ポータル・サーバーの LDAP ユーザー認証用に環境内に作成される唯一のリポジトリーになります。また、内部に構成されている「**LDAP バインド・パスワー**

ド」アカウントを反映する規則を使用して、リポジトリーを命名してもかまいません。 この場合に、要件を満たすために、さまざまなリポジトリーでさまざまな「**LDAP バインド・パスワード**」を構成できるようにする必要があれば、フォレスト名またはドメイン名から派生した名前を使用することもあります。

LDAP サーバーのプロパティー → 「ディレクトリー・タイプ」
ここで指定される値は、フォレスト・レベルと一致する必要があります。この例のフォレストは、Active Directory 2003 レベルで実行されています。

LDAP サーバーのプロパティー → 「基本ホスト名」
ポータル・サーバーの LDAP ユーザー認証用に以前、作成したユーザー・アカウントをホストする Active Directory フォレスト内のドメイン・コントローラー。 ここでの選択は、IBM Tivoli Monitoring ユーザーの OU を所有するフォレスト内の階層レベルに基づいて行う必要があります。 Active Directory のユーザー・オブジェクトの複製エラー、または Active Directory への接続が原因で発生する可能性のある、IBM Tivoli Monitoring LDAP 認証に関する問題を踏まえて、ここでの選択を検討します。

LDAP サーバーのプロパティー → 「ポート」
Active Directory の LDAP ポートのデフォルト値は 389 です。この値を、ご使用の LDAP 環境のポート割り当てに一致させます。

LDAP サーバーのプロパティー → 「1 次サーバーが使用できない場合に使用されるフェイルオーバー・サーバー」
ここに、複製または接続の問題に対応するための Active Directory LDAP (DC) サーバーを追加できます。 この値には、フェイルオーバー DC を入力する必要があります (GC の役割を持つものがより望ましいです)。

LDAP サーバーのプロパティー → 「他の LDAP サーバーへの参照のサポート」
これは任意です。ご使用の環境が閉じているのか、開いているのか (つまり、DMZ 内に DC がない) を考慮します。

セキュリティー → 「バインド識別名」
ここで指定されるユーザーには、Active Directory のディレクトリー「ベース」を検索するための十分な権限 (すなわち、適用ポリシー) が必要です。 このユーザーは、指定された「**ログイン・プロパティー**」に対する接続、バインド、および照会を行うアカウントです。 匿名ユーザーがレジストリーを検索できる場合には、この値を省略できます。

この例では、`CN=Administrator,CN=Users,DC=`*`company`*`,DC=com` が使用されていますが、指定されたユーザーが Active Directory の `CN=Users,DC=`*`company`*`,DC=com` コンテナーに存在する場合は、これは必ずしも必要ではありません。 ただし、これはお勧めしません。指定を明確にし、完全な識別名を使用するほうが望ましいためです。

セキュリティー → 「バインド・パスワード」
上記の「**バインド識別名**」アカウントのパスワード。

セキュリティー → 「ログイン・プロパティー」
この構成プロパティーは、ポータル・サーバーのユーザー名を正確に反映

するために使用される Active Directory の Name オブジェクトの属性名であるため、Active Directory に不可欠です (139 ページの図 3 を参照してください)。

セキュリティー → 「証明書」
Active Directory で DN の完全一致を検索するために、デフォルト値「**EXACT_DN**」が設定されています。このデフォルト値を保持することをお勧めします。

セキュリティー → 「証明書フィルター」
上記の「**証明書**」フィールドで「**CERTIFICATE_FILTER**」」を選択した場合、LDAP のフィルター・パラメーターが必要です。これらのパラメーターは、LDAP ディレクトリー内のエントリーにクライアント証明書内の属性をマップします。

セキュリティー → 「SSL 通信を必要とする」
TLS/SSL LDAP 通信が必要な場合は、これを選択します。TLS/SSL 実装に適用される次のオプションのラジオ・ボタンをクリックします。
中央管理対象
特定の SSL 別名を使用する

- 「**レルム内のこのエントリー・セットを一意的に識別するベース・エントリーの識別名 (Distinguished name of the base entry that uniquely identifies this set of entries in the realm)**」および「**このリポジトリー内のベース・エントリーの識別名 (Distinguished name of the base entry in this repository)**」を指定する場合は、147 ページの図 7 を参照してください。

  リポジトリーの構成が完了したので、Active Directory で定義されているポータル・サーバーのユーザーの OU を検索する場合の開始点として、ベース・エントリーを追加する必要があります。必要に応じて、複数のベース・エントリーをリポジトリーに定義できます。 Active Directory のポータル・サーバーのユーザーに複数のベース・ディレクトリー・ロケーション (複数の OU 階層) を定義した場合にのみ、複数のベース・エントリーが必要になります。

  このパネルでプロパティー「**レルム内でこのエントリー・セットを一意的に識別するベース・エントリーの識別名**」に入力された情報は、149 ページの図 10に示すように、Tivoli Enterprise Portal のユーザー識別名の選択に反映されます。ポータル・サーバーで定義されたユーザー ID を LDAP の接続、バインド、照会、または選択に関連付ける際に、 TEPS/e のポータル・サーバー構成内から使用できるようになるフィールドはこのフィールドです (ステップ 5 (120 ページ) のログイン・プロパティーを参照してください)。

  このプロパティーの形式は任意で、これは TEPS/e の構成 DN となります。規則 `O=DNofChoice` を使用することをお勧めします。 Active Directory で定義された TEPS のユーザー・ベース・コンテナーとの関連がわかるような DN を選択する必要があります (短いほうが望ましいです)。ここに示されている例では、「**ユーザー管理**」インターフェースで Tivoli Enterprise Portal ユーザーの識別名を明確に表示するために、`O=ITMtepsUser` が割り当てられています (149 ページの図 10 を参照してください)。リポジトリー名および基本 DN が非常に似ているため、ここで使用されている例には重複がありますが、このリポジトリーおよびベースが、Active Directory で定義されたユーザーにアクセスし、バインドするために構成されていることは明らかです。

「**このリポジトリー内のベース・エントリーの識別名 (Distinguished name of the base entry in this repository)**」には、LDAP レジストリー内のベース・エントリーの識別名 (DN) を指定します。これは、LDAP サーバー内のユーザー検索の開始点となります。

図 7. レルムへのベース・エントリーの追加： このエントリーはリポジトリーの ITMtepsUsers セクションと関連付けられることに注意してください。

- TEPS/e 構成作業を保存するときは、図 8を参考にしてください。「**保存**」をクリックします。

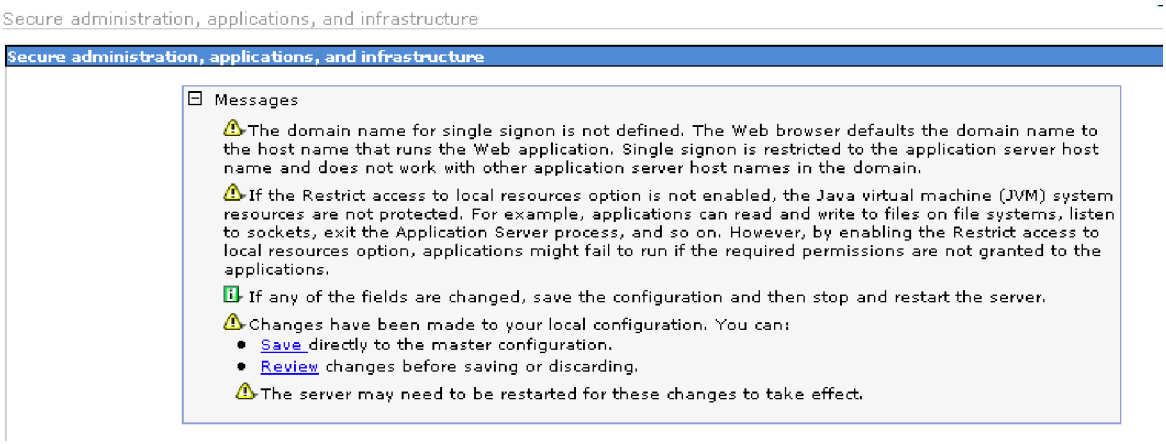


図 8. TEPS/e 構成の更新の保存

また、リポジトリーおよびベース設定の構成時に、構成設定を検証するよう求められた場合は、「OK」をクリックしてください。 「OK」または「適用」をクリックすると、更新された構成設定を使用して、Active Directory の LDAP データ

ベースに対する接続、バインド、および照会が行われます。問題が発生した場合は、図 9 に示されているような赤いエラー・メッセージが構成パネルに表示されます。

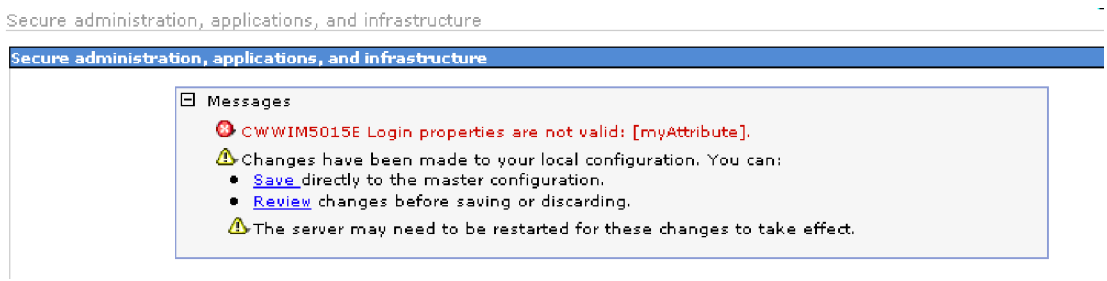


図 9. TEPS/e の構成エラー・メッセージ

構成を保存する前にこれらのエラーを修正する必要があります。

注: TEPS/e の構成が完了し、保存されたら、Tivoli Enterprise Portal Server をリサイクルして、TEPS/e で構成されているユーザーが識別名としてリストされていることを確認する必要があります (149 ページの図 10 の *llassite* の例を参照してください)。

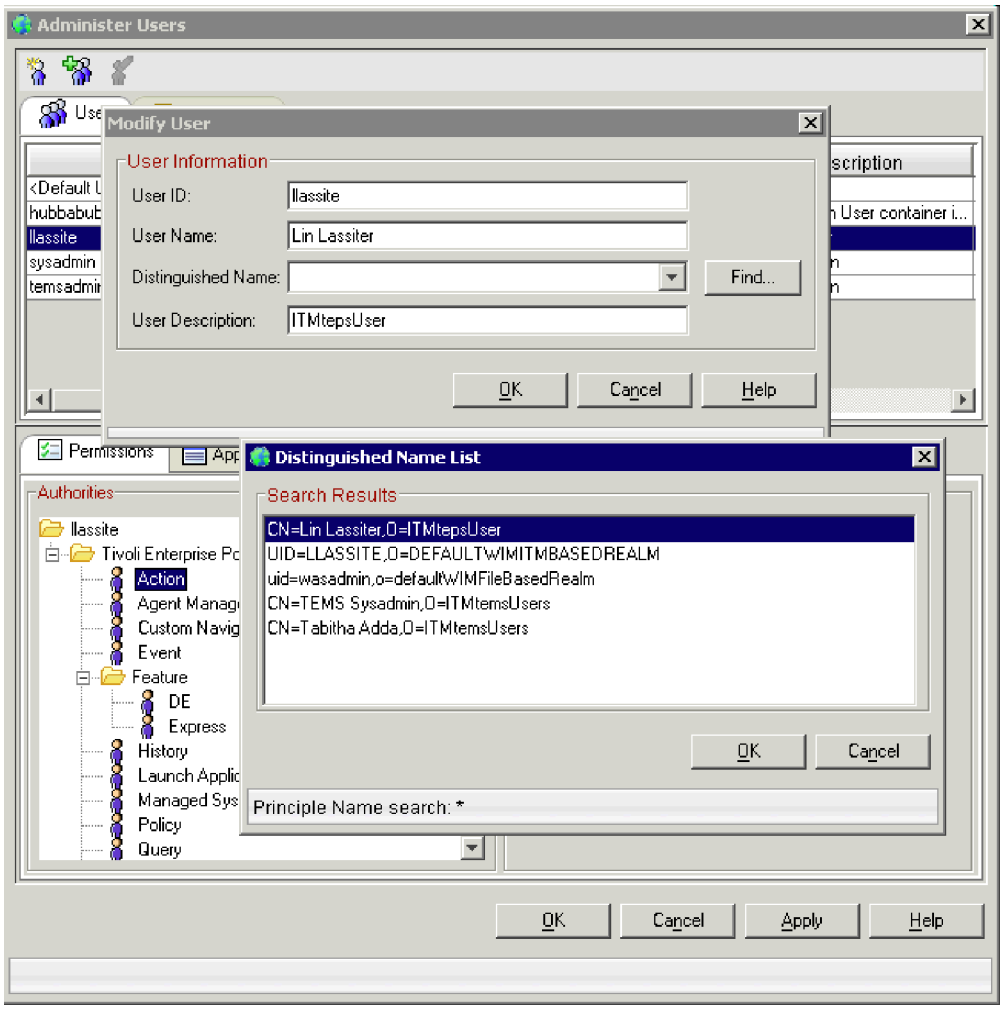


図 10. Tivoli Enterprise Portal の「ユーザー管理」画面： 識別名は、リポジトリーに対して TEPS/e 内で構成されているベース名に解決されます。ここに示されている値を、 138 ページの図 2 に示されている値と比較します。

ポータル・クライアントのユーザー ID の LDAP 識別名へのマッピング

125 ページの『Tivoli Enterprise Portal ユーザー ID の LDAP 識別名へのマッピング』は、ポータル・サーバーの新しいユーザー ID を、前の TEPS/e 構成ステップによって使用可能になった識別名に関連付けるのに必要なステップを示します。使用可能な識別名は、TEPS/e レジストリーに関連付けられたベース構成プロパティー「**レルム内でこのエントリー・セットを一意的に識別するベース・エントリーの識別名**」に直接関連します。

使用可能なすべての識別名を表示するには、最初に「**識別名**」フィールドのエントリーを削除してから、「**検索**」ボタンをクリックします。 「すべての構成済みレルム (All configured Realm)」 →「リポジトリー」→「基本識別名 (Base Distinguished Names)」の順に選択すると、レルム内でこのエントリー・セットを一意に識別する基本識別名が表示されます。また、「**ログイン・プロパティー**」値を使用して Active Directory に照会を実行したときに IBM Tivoli Monitoring によって返されたユーザーも表示されます。

これらのユーザーは Active Directory の CN 形式を使用して表示されます (149 ページの図 10 を参照してください)。

オプション: Active Directory の LDAP 構成ステップでは、Tivoli Enterprise Portal のユーザー ID を TEPS/e の構成前に作成することが推奨されています。オプションで、Active Directory のユーザー ID および TEPS/e の構成が完了してから、ポータル・サーバーのユーザー ID を作成することもできます。この場合の利点は、識別名にアクセスしながら「**ユーザー管理**」インターフェースのユーザーの作成機能を使用できることです。これによって、割り当てられるユーザー ID は、使用可能な識別名に一致するようになります。

ポータル・サーバー内での LDAP 認証の有効化

110 ページの『Tivoli Enterprise Monitoring Services の管理 を使用して LDAP 認証のためにポータル・サーバーを構成する』および 115 ページの『Linux コマンド行または UNIX コマンド行を使用して LDAP 認証のためにポータル・サーバーを構成する』には、LDAP ユーザー・レジストリーを使用してポータル・サーバーのユーザー認証を有効にするために必要なステップが示されています。

注: LDAP タイプを選択するように求められた場合は、「**その他**」を選択し、その他の LDAP パラメーターの値を指定しないようにします。

LDAP を使用するようにポータル・サーバーを構成したら、 106 ページの『ロードマップ: LDAP ユーザー・レジストリーとシングル・サインオンを使用するポータル・サーバーのセットアップ』を参照して、構成を完了するための追加のステップを確認します。

必要な場合の TEPS/e for TLS/SSL の構成

通常、TEPS/e はデフォルトで TLS/SSL 対応になっています。

TEPS/e 管理コンソール を使用して、ポータル・サーバーと LDAP サーバー間の SSL 通信を構成します。 123 ページの『ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』のステップを実行します。

モニター・サーバーの LDAP ユーザー認証の有効化および構成 (必要な場合)

このステップをスキップ: モニター・サーバー・ユーザーの認証に LDAP ユーザーを使用しない場合。

Tivoli Enterprise Monitoring Server のユーザー構成は、Tivoli Enterprise Portal Server のユーザー構成とは完全に分離されています。 TEPS/e は含まれていません。

ポータル・サーバーの LDAP の構成も有効化も、モニター・サーバーの LDAP の構成または有効化には影響しません。モニター・サーバーのユーザーは、Tivoli Enterprise Portalの「**ユーザー管理**」ユーザー・リスト内に作成される必要も存在する必要もありません。モニター・サーバーのユーザーは、「**セキュリティー: ユーザーを検証**」オプションを使用して認証可能なユーザー ID を作成する場合、または、モニター・サーバーの SOAP サーバーに対する SOAP 要求を使用可能にする

か禁止する場合にのみ、必要です (610 ページの『Tivoli Monitoring Web Services の構成 (SOAP サーバー)』を参照してください)。

92 ページの『ハブ・モニター・サーバーを使用したユーザー認証』には、Tivoli Enterprise Monitoring Server の LDAP ユーザー認証を有効にするために必要なステップが示されています。 ここには、この処理内の特定のステップに関する追加コメントが示されています。

注: モニター・サーバーのユーザー ID は 10 文字までです。これにより、ユーザーが選択する Active Directory のユーザー名も、10 文字以下にする必要があります。

モニター・サーバーの LDAP 構成では、1 つの LDAP ベースおよび 1 つの (ユーザー ID 属性に基づいて LDAP ディレクトリーを照会するための) LDAP ユーザー・フィルターのみが許可されます。 Active Directory のベース、および要件に最も適合する OU 階層を作成するために、OU 計画をお勧めします。 Active Directory の LDAP ユーザー認証のパフォーマンスを最大にしつつも、ディレクトリーのサブツリー検索を制限するベースを使用します (137 ページの図 1 を参照してください)。

- ステップ 5 (96 ページ): 図 11 を参照してください。

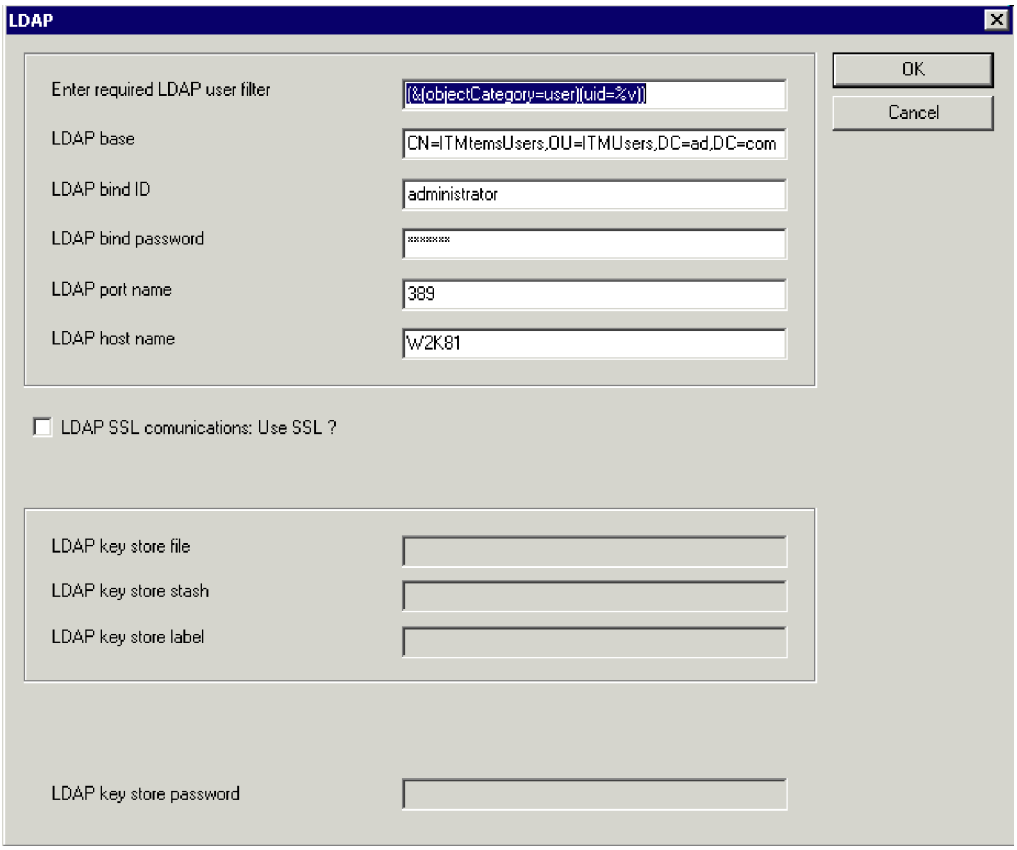


図 11. モニター・サーバーのユーザーについての「LDAP」構成パネル

必要な LDAP ユーザー・フィルターを入力します

これは、Tivoli Enterprise Monitoring Server の LDAP 認証で照会および

収集される属性を定義します。 ログイン (**tacmd login –s tems_name –u username –p password**) に使用されるモニター・サーバーの ID が、Active Directory でフィルタリングされた一致ユーザーに照らし合わせてチェックされ認証されます。

LDAP ユーザー・フィルター
例: (&(objectCategory=user)(userPrincipalName=%v@*company*.com)) (ここで %v は、IBM Tivoli Monitoring によって、ログイン時に入力されたユーザー ID に置換される変数です。)

このフィルターは Active Directory に対して照会を行い、指定されたベースからすべてのユーザー・オブジェクトを収集します。この照会によって返される **userPrincipalName** 属性値は、ストリング %v@*company*.com に照らし合わせて解析され、モニター・サーバーのユーザー ID は **userPrincipalName** の %v 置換部分とのみ比較されます (この場合、userPrincipalName=llassite@*company*.com | userPrincipalName=%v@*company*.com == llassite)。

LDAP ベース
Active Directory で定義されたモニター・サーバー・ユーザーを含む OU コンテナーの表示を可能にするために LDAPベースを入力することをお勧めします。

LDAP バインド ID
Active Directory で定義されたポータル・サーバー・ユーザーを見つけるために、Active Directory の OU 階層にアクセスできる LDAP ID を入力することをお勧めします。

LDAP バインド・パスワード
LDAP バインド ID のパスワード。

LDAP ポート名
この値は、Active Directory のデフォルトの LDAP ポートに対して設定されます。 LDAP が構成されたポート番号を入力します。

LDAP ホスト名
モニター・サーバーの LDAP ユーザー認証用に以前作成したユーザー・アカウントをホストする Active Directory フォレスト内のドメイン・コントローラー。ここでの選択は、Tivoli Monitoring ユーザーの OU を所有するフォレスト内の階層レベルに基づいて行う必要があります。 Active Directory のユーザー・オブジェクトの複製エラー、または Active Directory への接続が原因で発生する可能性のある、IBM Tivoli Monitoring LDAP ユーザー認証に関する問題を踏まえて、ここでの選択を検討します。

Active Directory の LDAP 検証ツール

Microsoft Active Directory は、サイトの LDAP 環境を管理する際に使用するいくつかのツールを提供します。次の 2 つのツールは、LDAP 環境を IBM Tivoli Monitoring にリンクする際に特に有用です。

ADSI 編集
この Microsoft Management Console スナップインを使用して、ユーザー・オブジェクトの属性を表示し、Tivoli Enterprise Portal Server の「**ログイ**

ン・プロパティー」に指定する属性および Tivoli Enterprise Monitoring Server の「**attributename=%v**」置換パラメーターが定義され、使用可能であることを確認します。

LDP.exe

モニター・サーバーおよびポータル・サーバーの LDAP 構成のベース設定を検証するには、このツールを使用します。このツールを使用すると、ユーザーのワークステーションから LDAP 環境に接続、バインド、および照会を行うことができます。図 12 を参照してください。

Windowx XP 用の LDP.exe は、Microsoft の URL (http://www.microsoft.com/downloads/details.aspx?FamilyID=49ae8576-9bb9-4126-9761-ba8011fabf38&displaylang=en) で入手できます。

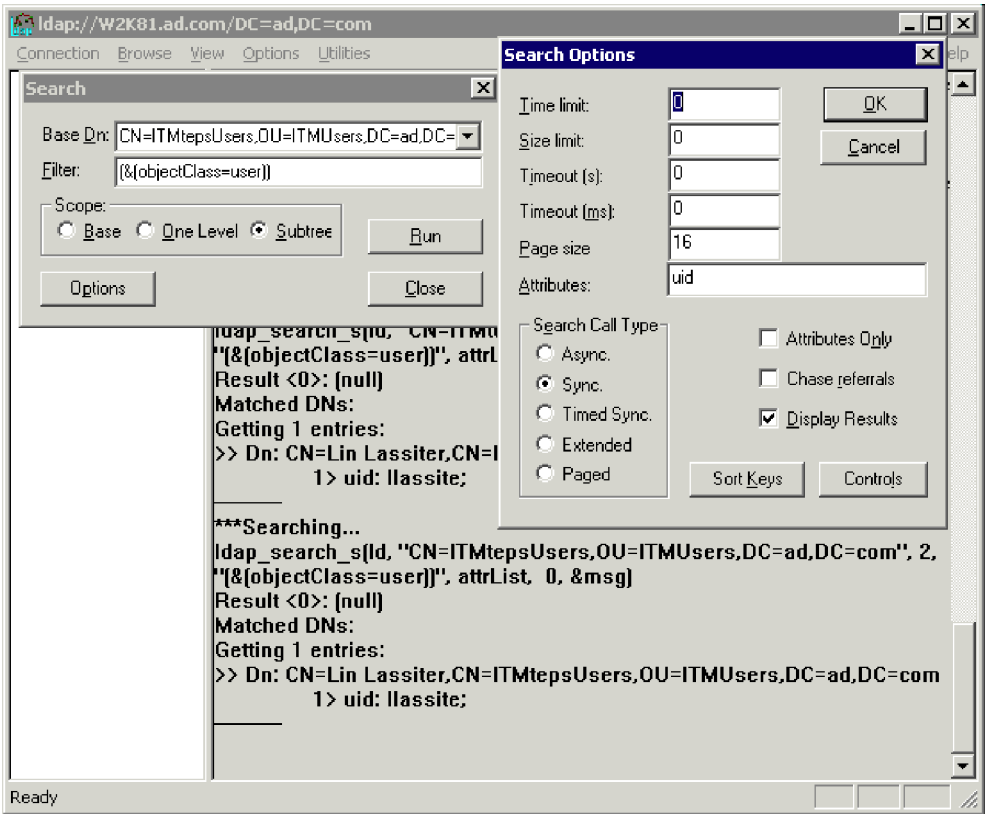


図 12. LDP の照会結果

このサンプルは、次のクエリーを使用して行った構成の検証を示します。

```
LDAP filter object = (&(objectCategory=user)(uid=%v))
LDAP base = CN=ITMtemsUsers,OU=ITMUsers,DC=company,DC=com
```

または、このサンプルは、次のクエリーを使用して行った構成の検証を示します。

```
LDAP base = CN=ITMtepsUsers,OU=ITMUsers,DC=company,DC=com
Login properties = uid
```

Microsoft Active Directory の LDAP 認証を正常に構成するには、ドメイン管理者のサポートを受けるか、または外部からの LDAP ディレクトリーの参照を可能にする非常に有用な 2 つのツールを入手する必要があります。 これらのツールを以下に示します。

ldapsearch

コマンド行から接続文字列をテストし、LDAP ユーザー・レジストリー内の正しい場所を指していることを確認するには、このツールを使用します。 160 ページの図 17 は `ldapsearch` の出力のサンプルを示します。

98 ページの『LDAP 情報の取得のための Ldapsearch』 には、このコマンドおよびその用途とオプションに関する追加情報が含まれています。

指定する `ldapsearch` オプション (98 ページの『ldapsearch コマンド行オプション』を参照してください) は、サイトの Tivoli Enterprise Monitoring Server の LDAP 構成に基づきます。

-h LDAP ホスト名です。

-p LDAP ポート名です。

-b LDAP ベース値です。

-D LDAP バインド ID です。

-w LDAP バインド・パスワードです。

> **注:** -w オプションを指定しない場合、キーボードで LDAP バインド・パスワードを入力するように求められます。

モニター・サーバーの LDAP クライアントは、Tivoli Monitoring ユーザーを認証するときに `ldapsearch -s` *sub* オプションを使用するため、このオプションは必ず指定します。 LDAP ユーザー・フィルターを指定する際には、`%v` を Tivoli Monitoring のユーザー ID に置換します (このストリングは、`ldapsearch` コマンド行の最後の部分です)。

例: 159 ページの図 16 で示したモニター・サーバーの LDAP 構成におけるユーザー `sysadmin` を確認するには、次の `ldapsearch` コマンドを指定します。

```
ldapsearch -h 192.168.1.241 -p 389 -b "DC=bjomain,CN=users,DC=bjomain,
      DC=com"
           -D "CN=Administator,CN=users,DC=bjomain,DC=com" -w admin10admin
           -s sub "(mail=sysadmin@bjomain.com)"
```

`ldapsearch` の無償バージョンをダウンロードするには、リンク http://publib.boulder.ibm.com/infocenter/wasinfo/v4r0/index.jsp?topic=/com.ibm.support.was40.doc/html/Security/swg21113384.html にアクセスします。

ldapbrowser

このツールを使用して、LDAP ユーザー・レジストリーをグラフィカルに全探索し、識別名のほか、構成を完了する必要のあるその他のパラメーターの詳細を出力します。IBM Tivoli Monitoring がネットワークを介して LDAP ユーザー・レジストリーにアクセスできることを確認するには、Tivoli Monitoring サーバーに LDAP ブラウザーをインストールします。 158 ページの図 15 は `ldapbrowser` の表示サンプルを示します。

LDAP ブラウザーを使用すると、ポータル・サーバー自体から LDAP 情報を取得することもできます。

`ldapbrowser` の無償バージョンをダウンロードするには、リンク http://www.ldapbrowser.com/download.htm にアクセスし、「**LDAP Browser**」タブをクリックします。また、`ldapbrowser` には UNIX/Linux 版も Windows 版もあり、http://www.mcs.anl.gov/~gawor/ldap/ で入手可能です。

ユーザー・シナリオ

これらのシナリオでは、すべてのユーザー認証はサイトの Microsoft Server 2003 Active Directory LDAP ユーザー・レジストリー経由で行われることが求められます。IBM Tivoli Monitoring ユーザーにこの認証を構成するには、2 つの方法が考えられます。

サーバーの LDAP 認証のモニター

Tivoli Enterprise Portal に入力されたユーザー ID (*name* など) を *name*`@`*company*`.com` にマップするユーザー名フィルターを使用して、Tivoli Enterprise Monitoring Server で認証を構成します。 ユーザーは *name* (これは必要な LDAP 参照に一致するようにフィルターを通して変換されます) としてログインします。

この方法は、『Microsoft Active Directory を使用した モニター・サーバーのユーザー ID の認証』に説明されています。

ポータル・サーバーの LDAP 認証

Tivoli Enterprise Portal Server で認証を構成し、Tivoli Enterprise Portal へのログイン時にユーザーが入力するユーザー ID が検索され、LDAP ユーザー・レジストリーに照らし合わせて認証されるようにします。このシナリオでは、ユーザーは *firstname*`.`*lastname*`@`*company*`.com` を使用してログインします。

この方法は、 160 ページの『Microsoft Active Directory を使用した ポータル・サーバーのユーザー ID の認証』に説明されています。

Microsoft Active Directory を使用した モニター・サーバーのユーザー ID の認証

このシナリオでは、モニター・サーバー・ユーザーを認証するために、どのようにすれば Microsoft Active Directory を使用するよう Tivoli Enterprise Monitoring Server を構成できるか示します。

このシナリオが機能するのに TEPS/e 構成は必要ありません。このソリューションの欠点は、SSO (シングル・サインオン) を実装できないことです。また、ユーザー ID が最大 10 文字に制限されます。利点は、モニター・サーバー・ベースのユーザー認証を使用すると、ユーザーが SOAP サーバー要求を実行でき、ハブ・モニター・サーバーに要求を送信する **`tacmd`** コマンドを使用できることです。

環境

環境は 2 つのシステムで構成されます。1 つは Tivoli Monitoring モニター・サーバーを実行し (IP アドレス 192.168.1.240)、もう 1 つは Microsoft Active Directory ドメイン・コントローラーとして構成された Microsoft Windows 2003 Advanced Server を実行します (IP アドレス 192.168.1.241)。Tivoli Monitoring システムは

itm6210 と呼ばれるスタンドアロン・サーバーであり、構成されたドメインの一部ではないことに注意してください。サンプル・ドメインは **bjomain.com** と呼ばれ、Active Directory サーバーは **msad** と呼ばれます。

Microsoft Active Directory 構成:

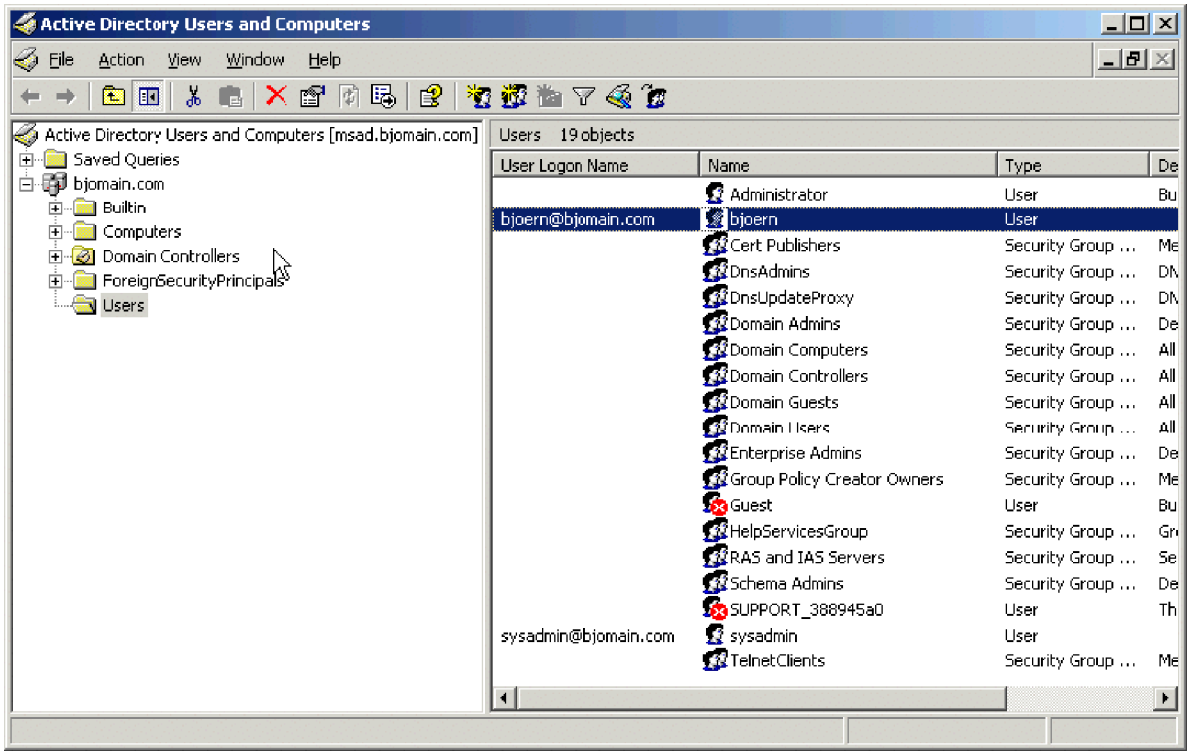


図 13. Active Directory ユーザーのリスト

図 13 に示すように、*sysadmin* および *bjoern* の 2 人のユーザーが Active Directory に構成されています。両方とも、 157 ページの図 14 に示すように電子メール・アドレスが設定されています (電子メール・アドレスが重要な理由は、IBM Tivoli Monitoring での LDAP フィルターの構成時に分かります)。 他のパラメーターを使用できますが、これが、 92 ページの『ハブ・モニター・サーバーを使用したユーザー認証』の手順で推奨されているパラメーターです。

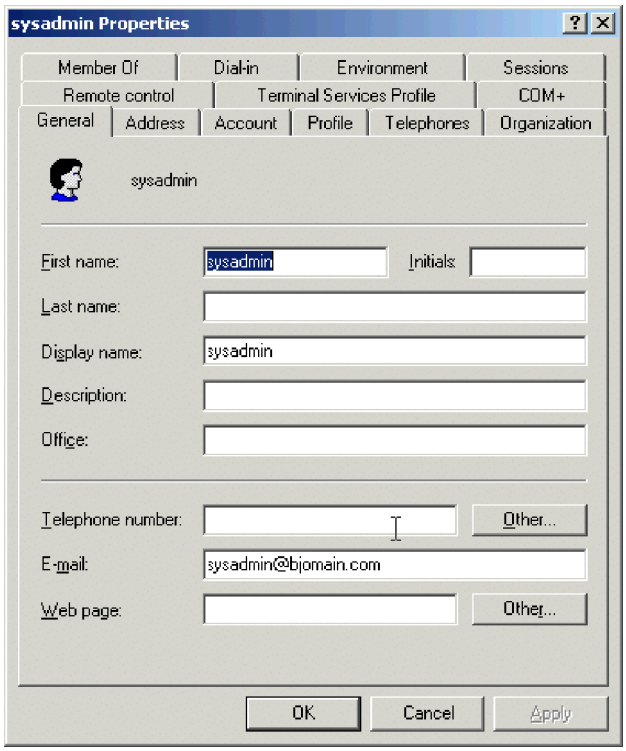


図 14. 個々の Tivoli Monitoring ユーザーのプロパティー

Active Directory の参照: Active Directory リポジトリーを GUI ブラウザーである `ldapbrowser` で参照すると、*sysadmin* ユーザーの識別名や E メール・アドレスなど、必要なパラメーターがすべて表示されます (158 ページの図 15 を参照)。

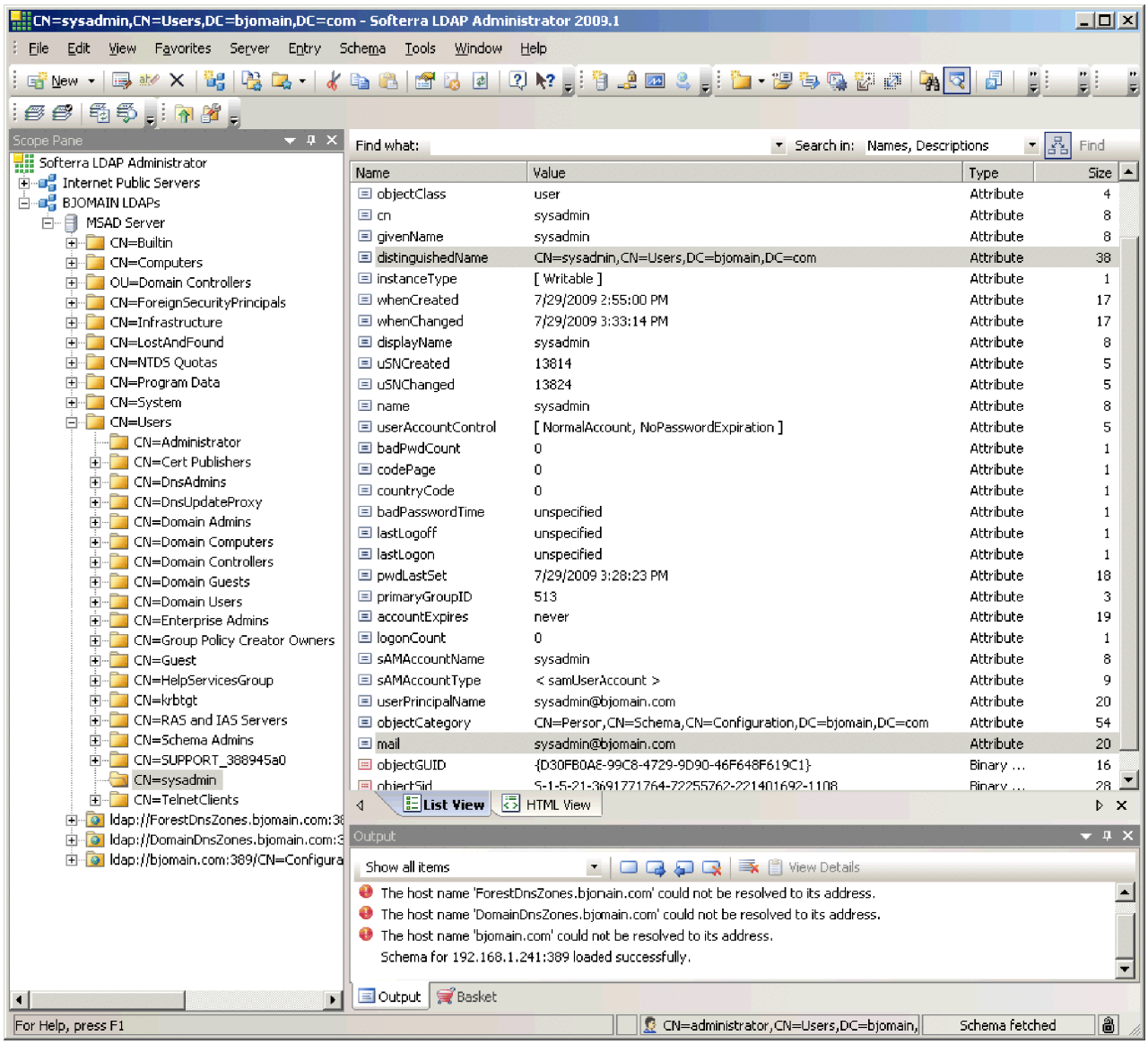


図 15. ldapbrowser ウィンドウ

ツリーの上部で **MSAD サーバー** を右クリックし、「**プロパティー**」を選択すると、Base DN (Tivoli Monitoring がユーザー検索を開始するポイント) が **DC=bjomain,DC=com** であることがわかります。

次のステップでは、この情報を Tivoli Enterprise Monitoring Server 構成ダイアログの適切なフィールドと突き合わせます。

全体像: 159 ページの図 16 は、*sysadmin* または *bjoern* としてのログインを可能にする、モニター・サーバーの LDAP 設定を示します (モニター・サーバーに定義されるのはこれらのユーザーのみです)。

注: Tivoli Monitoring と Active Directory 間の通信に対して Secure Sockets Layer (SSL) セキュリティーをアクティブにする必要がある場合は、 227 ページの『第 8 章 通信の保護』を参照してください。また、 95 ページの表 11 にリストされている

パラメーター値が手元にあることを確認してください。

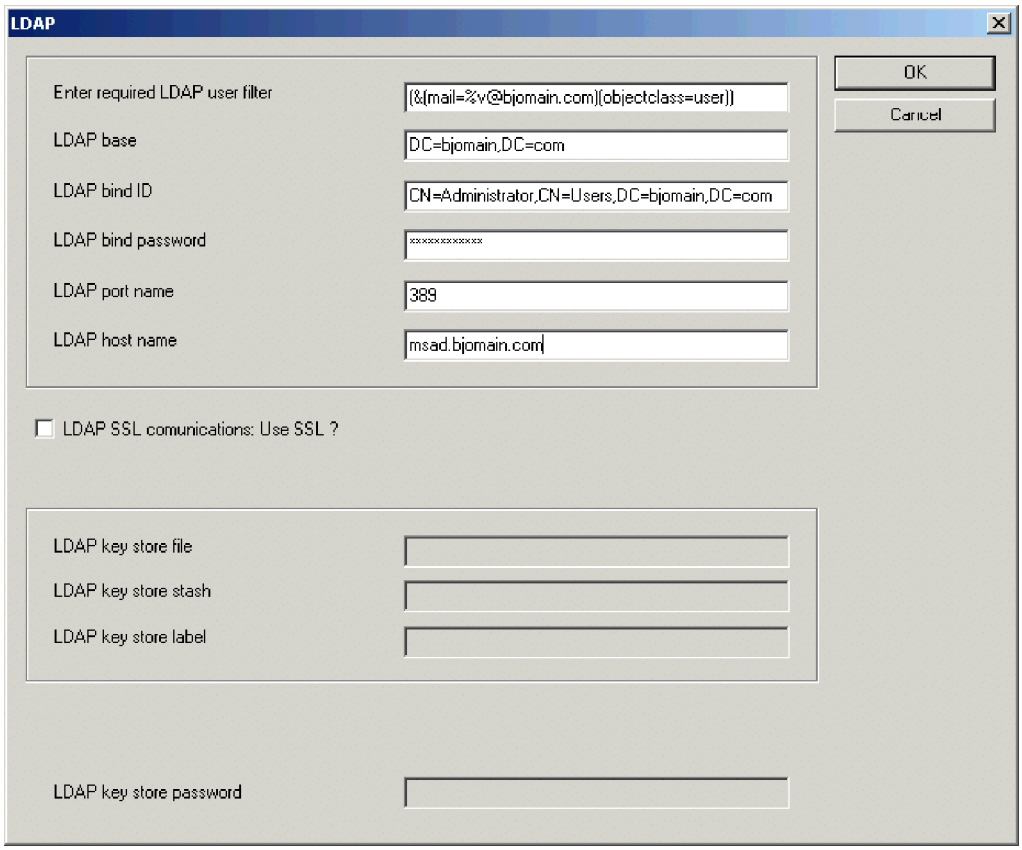


図 16. サーバーの LDAP パラメーターのモニター

図 16 に表示されている、重要度の高い一部のパラメーターを次に示します。

必要な LDAP ユーザー・フィルターを入力します
このパラメーターは、ユーザー・オブジェクト内の **mail** パラメーターを検索するよう指示します。

このために、ユーザーの Active Directory エントリーに電子メール・アドレスを含めました。

%v Tivoli Monitoring によって、ログイン画面で入力されたユーザー ID に置換される変数です。

LDAP ベース
157 ページの『Active Directory の参照』にリストされている完全な基本 DN です。

ユーザーが誤ったパスワードを入力したと IBM Tivoli Monitoring が表示する場合、それは、誤った LDAP 基本 DN がここで指定されたことを示します。この場合、Tivoli Monitoring は誤った LDAP ロケーションで検索を開始します。

LDAP バインド ID
Tivoli Monitoring によるユーザー検索の開始場所である基本 DN 全体に対する読み取り許可を持つユーザーの識別名を入力します。

注: *sysadmin* のように、ユーザー名のみを入力しても十分ではありません。

パラメーターを正しく定義したら、**grep** コマンドを使用してモニター・サーバーのログ・ファイルで LDAP ストリングを検索し、エラー・メッセージがないことを確認します。 オプションで、ldapsearch ユーティリティーを使用して、モニター・サーバーを開始せずにパラメーターをテストできます。ldapsearch が図 17 に示されているような出力を戻さない場合、入力が誤っています。 LDAP 構成が誤っているとユーザーがログインできなくなるため、モニター・サーバーを再始動する前に、サイトの LDAP パラメーターを確認する必要があります。

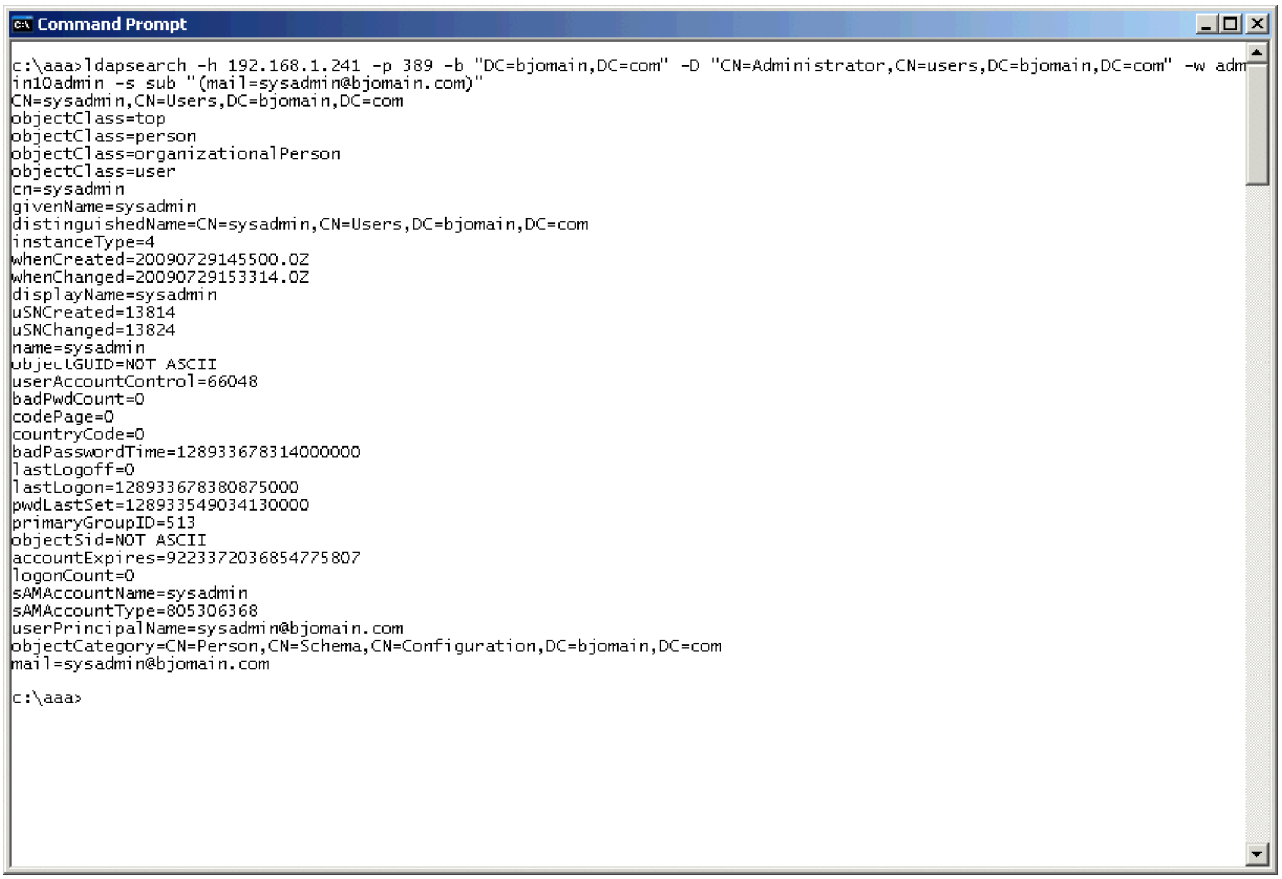


図 17. モニター・サーバーのユーザー ID に関する ldapsearch の結果

Microsoft Active Directory を使用した ポータル・サーバーのユーザー ID の認証

このシナリオでは、他のアプリケーションとのシングル・サインオンを使用するために、または Tivoli Enterprise Portal ユーザーが 10 文字を超えるユーザー ID でログインできるようにするために、サーバーを使用してユーザーを認証するようにポータル・サーバーを構成します。

このサイトでは、ポータル・サーバーの Tivoli Enterprise Monitoring Services の管理 ユーティリティーまたは **itmcmd** コマンド行インターフェースを使用して LDAP 認証を構成することを試みました。これは、組み込み認証メカニズムが **uid** という

名前の LDAP フィールドをルックアップする必要がある一方で、このお客様の Active Directory LDAP レコードに **uid** フィールドがないために失敗に終わることが確認されました。

このセクションの残りの部分では、TEPS/e 管理コンソール (この企業で Tivoli Enterprise Portal アクセス用のカスタム LDAP ユーザー・マッピングを定義しているポータル・サーバーの組み込み eWAS サーバー) で行う必要のある、ユーザー認証ステップについて説明します。

LDAP 環境についての必須情報

顧客の Active Directory LDAP ユーザー・レジストリーに対してユーザーを認証するには、次のようないくつかの情報が必要です。

1. LDAP インフォメーション・ストアのタイプおよび場所。
2. その情報の取得方法 — 特に、SSL を使用するかどうか。
3. **バインド ID** および**パスワード** (LDAP ストアにログインし、ユーザー・アカウントを検索するためにシステムによって使用されるユーザー ID/パスワードの組み合わせ)。

   この ID は、完全 LDAP 識別名形式である必要があります。
4. 使用する**ログイン・プロパティー** — すなわち、検索対象の LDAP フィールド。このフィールドは、LDAP インフォメーション・ストア内にあり、環境内のユーザーを一意に識別するものである必要があります。

   100 ページの『ポータル・サーバーを使用した LDAP ユーザー認証』の手順は、「**uid**」フィールドが使用可能であることを前提としていますが、これは、この顧客の LDAP ディレクトリーには該当しないことが分かっています。
5. **LDAP ベース** (LDAP ユーザー・レジストリーにおけるベース・エントリーの完全 LDAP 識別名)。

上記の例で、サイトの Active Directory 管理者が提供した LDAP 情報は次のとおりです。

1. LDAP タイプ: Microsoft Active Directory サーバーのバージョン 2003、ロケーション: ホスト名 `adhost.company.com`
2. 使用するポート: 636 (SSL が接続に必要とされることを示します)
3. `svc.tivolisec@company.com` のバインド ID および適切なパスワード
4. 使用する「**ログイン・プロパティー**」フィールド: ユーザーの「**電子メール・アドレス**」
5. **LDAP ベース**: `DC=US,DC=GLOBAL,DC=company,DC=COM`

必要なすべての接続情報があるにもかかわらず、LDAP ユーザー・レジストリーへの接続試行が毎回失敗します。152 ページの『Active Directory の LDAP 検証ツール』に説明されている LDAP ユーティリティーを使用して接続情報を検索および検証し、接続試行が毎回失敗する理由を調べることができます。

上記の例では、`LDP.exe` および `ldapbrowser` の 2 つのユーティリティーが使用されています。これらのユーティリティーは、この顧客の環境では SSL 通信が不要であることを示します。したがって、通常の暗号化されていない LDAP ポート 389

での接続は有効です。また、ツールによって、svc.tivolisec@*company*.com アドレスと関連付けられた完全 LDAP 識別名が CN=svc.tivolisec,OU=ServiceAccount,DC=us,DC=global,DC=*company*,DC=com であることが明らかになります。

これらのすべてのエントリーが検証されたら、TEPS/e 管理 (eWAS) ツールを使用して Tivoli Monitoring ユーザー管理用の LDAP 参照パラメーターを定義します。

TEPS/e 管理の有効化: TEPS/e 管理 (eWAS) コンソールである Integrated Solutions Console を有効にすると、次のステップを実行する必要があります。

注: ステップ 1 は 1 回のみ行う必要があります。残りのステップは、TEPS/e 管理コンソールを使用するたびに実行する必要があります。

***wasadmin* パスワードの定義:** TEPS/e 管理を完了する前に、eWAS サーバーにログインできるよう wasadmin アカウントのパスワードを設定する必要があります。設定するには、$CANDLEHOME/iw/scripts ディレクトリーでスクリプト updateTEPSEPass.sh を起動するか、Tivoli Enterprise Monitoring Services の管理インターフェースを使用します。

後で wasadmin ユーザー・パスワードを変更しない限り、この手順は一度だけ必要です。

コマンド行経由

コマンド行から wasadmin パスワードを定義するには、$CANDLEHOME/$INTERP/iw/scripts ディレクトリーにあるスクリプト updateTEPSEPass.sh を呼び出します。

```
# cd $CANDLEHOME/$INTERP/iw/scripts
# ./updateTEPSEPass.sh wasadmin newpw
WASX7209I: ノード ITMNode のプロセス "ITMServer" に
          SOAP コネクターを使って接続しました。
プロセスのタイプは UnManagedProcess です。
WASX7303I: 次のオプションはスクリプト環境に渡され、
argv 変数: "[wasadmin, newpw]" に格納される引数として使用可能になります。
```

Tivoli Enterprise Monitoring Services の管理経由

1. 「**Tivoli Enterprise Portal Server**」エントリーを右クリックし、メニュー・オプション「**TEPS/e 管理**」→「**TEPS 拡張機能パスワードの更新**」を選択します。
2. 「**パスワードの入力**」ウィンドウで、新しい wasadmin パスワードを入力し、「**OK**」を押します。

   パスワード変更の試行結果は、Tivoli Enterprise Monitoring Services の管理のメッセージ・ペインに表示されます。例:

   ```
   Password for user wasadmin was changed
   ```

ISCLite (TEPS/e eWAS サーバー管理) の有効化: ご使用のサイトの LDAP 認証を管理する必要があるときは必ず、最初に Integrated Solutions Console 経由で TEPS/e 管理を有効にする必要があります。 Tivoli Enterprise Portal Server を再構成、または停止して再始動すると必ず TEPS/e コンソールが自動的に無効化されることに注意してください。

コマンド行経由

コマンド行経由で TEPS/e コンソールを有効にするには、enableISCLite.sh スクリプトを呼び出します。(ポータル・サーバー・マシンの $CANDLEHOME/*platformcode*/iw/scripts サブディレクトリー):

```
# pwd /apps/TEPS_s11154cdc/li6263/iw/scripts

# ./enableISCLite.sh true
WASX7209I: ノード ITMNode のプロセス "ITMServer" に
           SOAP コネクターを使って接続しました。
プロセスのタイプは UnManagedProcess です。

WASX7303I: 次のオプションはスクリプト環境に渡され、
argv 変数: "[true]" に格納される引数として使用可能になります。

ISCLite 開始
```

Tivoli Enterprise Monitoring Services の管理経由

1. 「**Tivoli Enterprise Portal Server**」エントリーを右クリックし、メニュー・オプション「**TEPS/e 管理**」→「**TEPS/e 管理の有効化**」を選択します。
2. 有効化の試行結果は、Tivoli Enterprise Monitoring Services の管理のメッセージ・ペインに表示されます。例:

   ```
   ISCLite is enabled successfully
   ```

TEPS/e 管理コンソールへのログイン: ご使用のブラウザーに以下のアドレスを入力し、eWAS Integrated Solutions Console を呼び出します。

```
http://tepsserver.company.com:15205/ibm/console
```

このユーザー用に 162 ページの『wasadmin パスワードの定義』 で設定したユーザー名 wasadmin とパスワードを使用してログインします。

Integrated Solutions Console での LDAP ユーザー・レジストリーの定義:
Integrated Solutions Console を使って LDAP ユーザー・レジストリーを定義するには、以下のステップを実行します。

1. 「Integrated Solutions Console」基本画面の左側で、「**セキュリティー**」オプションのリストを展開し、「**グローバル・セキュリティー**」を選択します。 「**グローバル・セキュリティー**」パネルが表示されます。
2. 「**ユーザー・アカウント・リポジトリー**」セクションで、「**構成**」をクリックします。
3. 「**構成**」タブで、「**関連項目**」の下部にある「**リポジトリーを管理**」をクリックすると、LDAP ユーザー・レジストリーを定義できる画面が開きます。

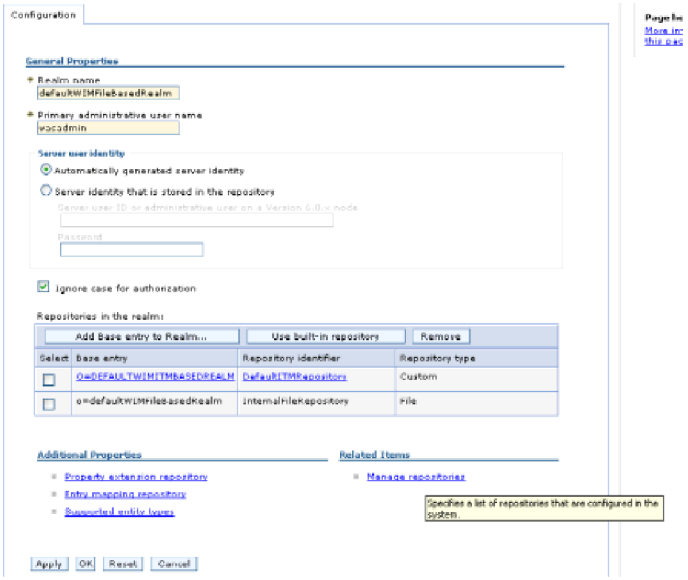


図 18. Integrated Solutions Console の「構成」ノートブック・タブ

4. 「**リポジトリーを管理**」画面で、「**追加**」をクリックします。

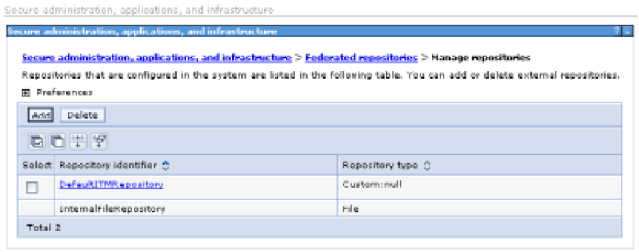


図 19. Integrated Solutions Console の「リポジトリーを管理」画面

「**一般プロパティー**」画面 (165 ページの図 20 に示す) が表示されます。LDAP ユーザー・レジストリーのロケーションと構成を定義する情報を、ここで提供します。

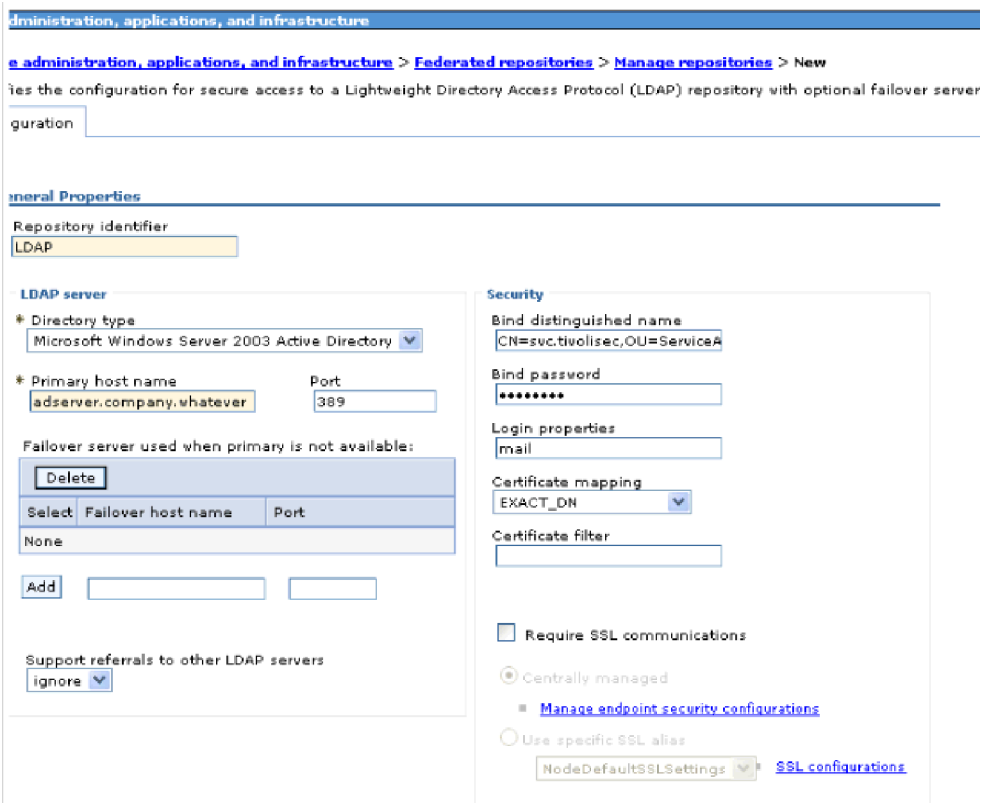


図 20. Integrated Solutions Console の「一般プロパティー」画面

5. この画面に、次の情報を入力します。

   リポジトリー識別子
   レジストリーに付けるフリー・フォームの名前で、この場合は簡単に **LDAP** とします。

   プライマリー・ホスト名
   LDAP サーバーのホスト名で、この場合は `adhost.company.com` とします。

   ポート LDAP サーバーが listen しているポート。この例では、389 が有効値です。

   バインド識別名
   バインド ID の完全 LDAP 識別名。この場合、サイトの LDAP 管理者が提供した `svc.tivolisec` アカウントの完全 LDAP 識別名は、`CN=svc.tivolisec,OU=ServiceAccount,DC=us,DC=global,DC=company,DC=com` となります。

   バインド・パスワード
   バインド ID のパスワード。

   ログイン・プロパティー
   識別名で使うログイン・プロパティー。この場合は、**mail** プロパティーです。

このページを完了したら、「**OK**」をクリックします。確認画面が表示されます。

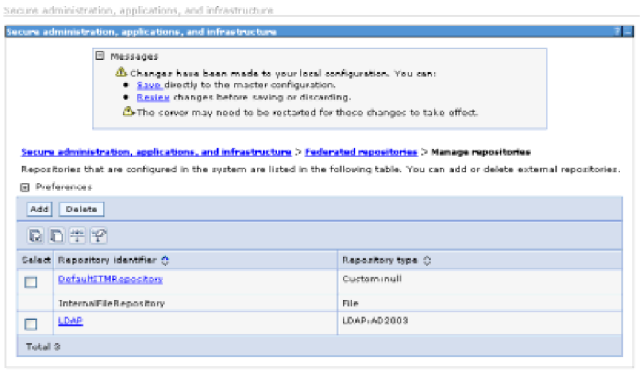


図 21. Integrated Solutions Console の確認画面

6. 「**保存**」をクリックします。

これで、ご使用のサイトの LDAP ユーザー・レジストリーが定義されました。

eWAS レルムへの LDAP ユーザー・レジストリーの追加: 次のステップは、新しく定義されたレジストリーを eWAS レルムに追加し、サイトでのユーザー ID の検索に LDAP を使用できるようにすることです。

1. 「Integrated Solutions Console」基本画面の左側で、「セキュリティー」オプションの中の「**グローバル・セキュリティー**」を選択します。
2. 「**ユーザー・アカウント・リポジトリー**」セクションで、「**構成**」をクリックします (「統合リポジトリー」の横の下方にあります)。

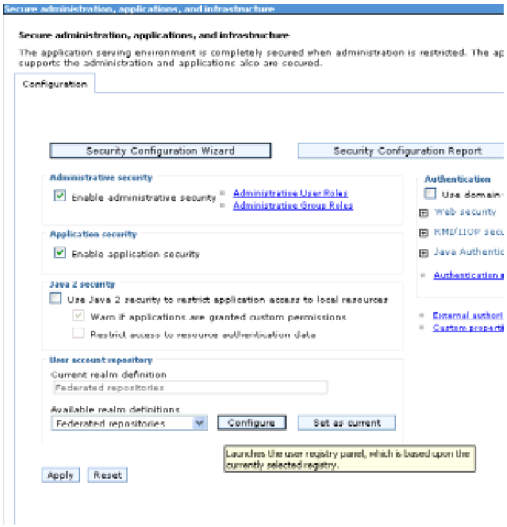


図 22. Integrated Solutions Console の「構成」ノートブック・タブ

これによって、レルムにレジストリーを追加するための画面が表示されます。

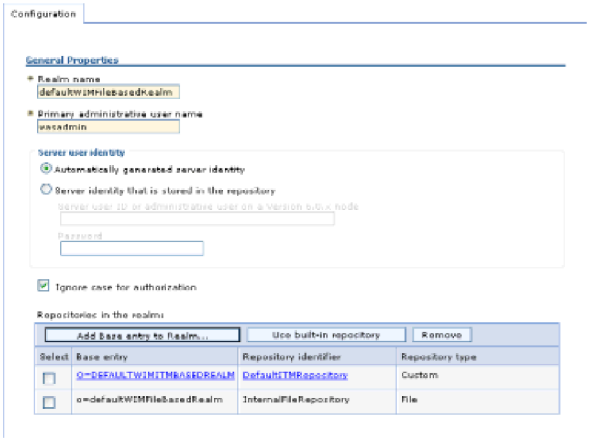


図 23. Integrated Solutions Console の「構成」タブ

3. 163 ページの『Integrated Solutions Console での LDAP ユーザー・レジストリーの定義』で定義されたリポジトリーを追加するには、「**レルムの基本項目の追加**」をクリックします。

   「**リポジトリー参照**」画面が表示されます。この画面では、サイトの eWAS レルムに LDAP ユーザー・レジストリーを追加できます。

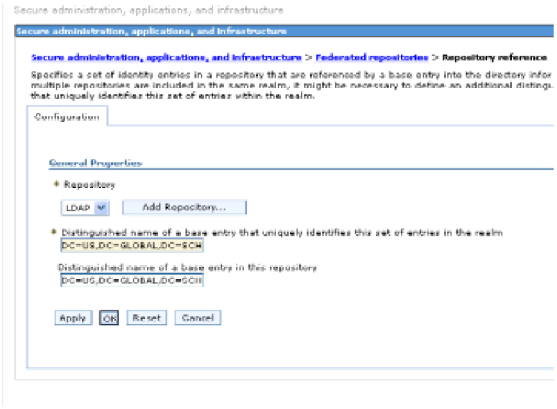


図 24. Integrated Solutions Console の「リポジトリー参照」画面

この画面では、「**リポジトリー**」が「**LDAP**」(または、 163 ページの『Integrated Solutions Console での LDAP ユーザー・レジストリーの定義』で割り当てた任意の「**リポジトリー ID**」) に設定されていることを確認します。 2 つの入力フィールドに、「**バインド識別名**」を入力します。この例では、`DC=US,DC=GLOBAL,DC=`*`company`*`,DC=COM` になるように定義されています。 次に、「**OK**」をクリックします。

4. Integrated Solutions Console の確認画面で、「**保存**」をクリックします。

図 25. Integrated Solutions Console の確認画面

5. これによって、現在のレルムにあるレジストリーのリストに戻ります。

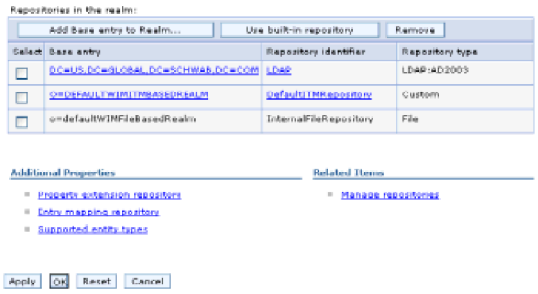


図 26. Integrated Solutions Console の「レルム内のリポジトリー」画面

「**OK**」をクリックします。

6. Integrated Solutions Console の確認画面で、「**保存**」をクリックします。

図 27. Integrated Solutions Console の確認画面

7. これによって、最初の Integrated Solutions Console サインイン画面に戻ります。

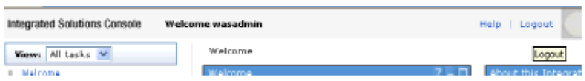


図 28. Integrated Solutions Console のサインイン画面

「**ログアウト**」をクリックします。

8. Tivoli Enterprise Portal Serverを再始動します。

(オプション) TEPS/e 内での LDAP 参照のテスト: TEPS/e コンソール内で LDAP 参照をテストできます。ここで参照が正しく機能すれば、参照は Tivoli Enterprise Portal Server 内で機能します。

1. TEPS/e コンソールを再度有効にし (162 ページの『ISCLite (TEPS/e eWAS サーバー管理) の有効化』を参照してください)、次に `wasadmin` ユーザー ID および新しく割り当てられたパスワードを使用してログインし直します (163 ページの『TEPS/e 管理コンソールへのログイン』を参照してください)。

   TEPS/e の最初の画面が表示されます。

図 29. Integrated Solutions Console の最初の画面

2. 「**ユーザーおよびグループ**」のリストを展開してから、「**ユーザーの管理**」を選択します。
3. 「**ユーザーの管理**」ペイン内で、「**次で検索 (Search by)**」を「**E メール (E-mail)**」に設定し、テスト用のユーザー ID (すなわち、電子メール・アドレス) を「**検索対象**」フィールドに指定します。
4. 「**検索**」をクリックします。

指定した電子メール・アドレスが見つかった場合は、「**ユーザーの管理**」ペインの下部にその特性がリストされます。

ポータル・サーバーのユーザー管理を使用したテスト用ユーザー ID の定義:

1. ユーザー ID `sysadmin` を使用してTivoli Enterprise Portal クライアントにログインします。 `sysadmin` が引き続きポータル・サーバーのローカルな ID として定義されていることに注意してください (つまり、LDAP ユーザー・レジストリーには格納されておらず、LDAP ユーザー・レジストリーから取得されることもありません)。
2. (100 ページの『ポータル・サーバーを使用した LDAP ユーザー認証』に説明されているように) Tivoli Enterprise Portalのユーザー管理を使用して、任意のユーザー ID を持つ新しいユーザーを作成します。
3. 「識別名」フィールドに、そのユーザーの電子メール・アドレスのうち、指定を一意にするのに十分な部分を入力し、「**検索**」ボタンをクリックします。

LDAP 検索が実行され、その電子メール・アドレスに対する完全 LDAP 識別名が検索されます。

4. その識別名を強調表示し、「**OK**」をクリックします。
5. そのユーザーの残りのユーザー ID フィールドを入力してから、「**OK**」をクリックして追加します。

これで、このユーザーは自分の電子メール・アドレス *longemailaddress*@*customer*.com をユーザー ID として使用し、自分の Active Directory のパスワードをパスワードに指定して、Tivoli Enterprise Portal クライアントにログインできるようになりました。 このユーザーは、自分のデフォルトの基本ワークスペースにログインします。

第 6 章 Tivoli Enterprise Portal ユーザー許可の使用

あらゆるポータル・ワーク・セッションは、まず Tivoli Enterprise Portal へ正常にログオンして接続することから開始します。ログオン・ユーザー ID およびユーザー・グループは、「ユーザー管理」ウィンドウを使用して作成およびプロファイル作成されます。

「ユーザー管理」ウィンドウは、複数のタブと 2 つのペインで構成されています。上部のフレームには、**「ユーザー」** および **「ユーザー・グループ」**という 2 つのタブがあります。これらのタブには、ユーザー ID、識別名 (LDAP ユーザー・レジストリーに対する認証用にポータル・サーバーが構成されている場合)、およびポータル・サーバーに保管されているユーザー・グループがリストされます。選択されているユーザーまたはユーザー・グループのプロファイルは、下部のフレームに反映されます。

「許可」 では、ポータルの機能が「権限」ボックス内にリストされます。右側には、選択されている機能について実行可能な操作が表示されます。 オンになっているチェック・ボックスは、現在選択されているユーザーまたはグループにその操作を実行する権限があることを示します。チェック・ボックスの横にある インディケーターは、当該ユーザーが属するユーザー・グループに許可が追加されていることを示します。

「アプリケーション」 には、現在モニターされており、ユーザーまたはユーザー・グループに割り当てることの可能なアプリケーションがすべて表示されます。例えば、ある 1 つのユーザーまたはユーザー・グループで OMEGAMON® アプリケーションのみを監視し、別のユーザーまたはユーザー・グループで Linux と Oracle、ミドルウェアのみを監視し、さらに別のユーザーまたはグループではすべてのアプリケーションを監視する、というようにプロファイルを作成できます。

「ナビゲーター・ビュー」 には、ポータル・サーバー上にある、ユーザーまたはユーザー・グループに割り当て可能なナビゲーター・ビューがすべて表示されます。ユーザーまたはユーザー・グループに対して、ナビゲーター・ビューの階層全体ではなく特定の分岐のみが表示されるように制限できます。

「メンバー」タブ (「ユーザー」タブが選択されている場合)、または **「メンバー」**タブ (「ユーザー・グループ」タブが選択されている場合) には、ユーザーが属するグループのリスト、またはグループ内のユーザー名のリストが表示されます。

「ユーザー管理」機能を使用して、ポータル・サーバー上のユーザー ID およびユーザー・グループを管理できるほか、次のような業務上の役割の組み合わせに応じて、管理対象環境の各機能およびビューへのアクセスをさまざまなレベルで提供できます。*オペレーター*: アラートに応答し、処理のためにそれらを適切なスタッフに転送します。*管理者*: モニター環境を計画、設計、カスタマイズ、および管理します。

一部の管理対象エンタープライズでは、1 人のユーザーがこれらの役割をすべて担当する場合があります。規模の大きいエンタープライズでは、通常これらの役割は

分担されます。個々のユーザーごとに役割を割り当てることも、ユーザー・タイプ別に割り当てることも、またはその両方を併用することも可能です。

また、IBM Dashboard Application Services Hub でモニター・ダッシュボードにアクセスするユーザーには、Tivoli Enterprise Portal ユーザー ID も必要です。ダッシュボード・ユーザーの管理方法は、ポータル・サーバーで構成された許可のタイプおよびダッシュボード・ユーザーが Tivoli Enterprise Portal クライアントも使用するかどうかによって異なります。 IBM Dashboard Application Services Hub でのモニター対象リソースへのアクセスを制御するために、以下の 2 つのタイプの許可を構成できます。

役割ベースの許可ポリシー

このポリシーは、許可ポリシーの tivcmd コマンド行インターフェースを使用して作成されます。Tivoli Enterprise Portal モニター・アプリケーションの割り当てよりも細分化された許可が可能です。役割ベースの許可ポリシーを使用して、特定の管理対象システム・グループまたは管理対象システムを表示する許可をユーザーに割り当てることができます。ポータル・サーバーで役割ベースの許可ポリシーが使用可能になっている場合は、ダッシュボード・ユーザーには Tivoli Enterprise Portal ユーザー ID が必要ですが、Tivoli Enterprise Portal クライアント・ユーザーでもない限り、Tivoli Enterprise Portal の許可やモニター・アプリケーションの割り当ては必要ありません。この場合、役割ベースの許可ポリシーが、モニター・ダッシュボードでアクセスできるリソースを制御し、Tivoli Enterprise Portal の許可およびモニター・アプリケーションの割り当てが、Tivoli Enterprise Portal クライアントでアクセスできるリソースを制御します。

Tivoli Enterprise Portal の許可

これは、ダッシュボード・ユーザーのデフォルトの許可メカニズムです。ダッシュボード・ユーザーは、Tivoli Enterprise Portal ユーザー ID を持っていて、モニター・ダッシュボードでのリソースへのアクセスを制御する許可およびモニター・アプリケーションが割り当てられている必要があります。ダッシュボード・ユーザーが Tivoli Enterprise Portal クライアント・ユーザーでもある場合は、両方のアプリケーションでアクセスできるモニター対象リソースを制御する単一の許可セットが割り当てられます。

LDAP ユーザー・レジストリーを共有するようにポータル・サーバーおよび Dashboard Application Services Hub を構成するのが、ダッシュボード・ユーザーと Tivoli Enterprise Portal クライアント・ユーザーの統合セットを用意するためのベスト・プラクティスの方法です。このシナリオでは、ダッシュボード・ユーザーは LDAP ユーザー名を使用してダッシュボード・ハブにログインするため、そのユーザーの LDAP 識別名を、必要な許可を備えた Tivoli Enterprise Portal ユーザー ID にマップする必要があります。

ダッシュボード・ユーザーがモニター・データを要求し、ユーザー ID がそのユーザーの識別名にマップされていない場合は、許可のない Tivoli Enterprise Portal ユーザー ID が自動的に作成されます。詳しくは、188 ページの『ユーザー管理についての注意事項』 を参照してください。

ユーザー管理

ご使用のユーザー ID およびメンバーとなっているユーザー・グループのプロファイルには、表示および使用が許可される Tivoli Enterprise Portal 機能、表示が許可されるモニター対象アプリケーションのリスト、およびアクセス可能なナビゲーター・ビューのリスト (およびビュー内の最高位レベル) を決定する一連の許可が指定されます。

「**ユーザー管理**」をクリックして「ユーザー管理」ウィンドウを開きます。このウィンドウには 2 つのペインがあり、「ユーザー」タブおよび「ユーザー・グループ」タブが上部フレームに、いくつかのタブが下部フレームにあります。この配置により管理者は、個々のユーザーごと、ユーザー・グループごと、またはこれら 2 つを組み合わせて、ユーザー・プロファイルを管理できます。 ユーザー・プロファイルを作成してから、それぞれの追加ユーザーに対してプロファイルをコピーし、必要に応じて (アクション機能で、1 人のユーザーに表示許可を与え、別のユーザーに変更許可を与えるなど) 設定を変更することができます。 あるいは、特定のプロファイルを持つユーザー・グループを作成し、そのグループにユーザーを追加することもできます。 その後、グループに対して許可を 1 回変更することで、すべてのメンバーに自動的に適用することができます。

Tivoli Enterprise Portal ユーザーまたはユーザー・グループの許可、またはモニター対象アプリケーションのリストを変更するとき、許可の変更はユーザーが Tivoli Enterprise Portal クライアントからログアウトし、再度ログインするまで有効になりません。ダッシュボード・ユーザーにモニター対象リソースを許可するために Tivoli Enterprise Portal の許可が使用されている場合、許可の変更はユーザーが Dashboard Application Services Hub からログアウトし、再度ログインするまで有効になりません。

関連タスク:

180 ページの『ユーザー ID の追加』
ポータル・クライアントまたは **tacmd tepsLogin** コマンドを使用して Tivoli Enterprise Portal Server にログオンできる必要があるすべてのユーザーのユーザー ID を作成します。モニター・データを要求する IBM Dashboard Application Services Hub ユーザーにもユーザー ID が必要です。デフォルトのユーザー・プロファイルを使用することも、既存のユーザーのプロファイルをコピーすることもできます。

182 ページの『ユーザー ID の表示と編集』
「ユーザー管理」ウィンドウの「**ユーザー**」リストに追加されたら、いつでもプロファイル設定の確認および編集を行うことができます。

ユーザーおよびユーザー・グループ

「**ユーザー**」タブおよび 「**ユーザー・グループ**」タブには、ポータル・サーバーに保管されているユーザー ID およびユーザー・グループがリストされます。

リストの 1 つからユーザーまたはユーザー・グループを選択した後、ウィンドウの下半分にあるいずれかのタブをクリックすると、与えられた許可の種類および割り当て済みの許可を表示することができます。 管理者は、ユーザー・グループを使用して、機能の許可、アプリケーションおよびナビゲーター・ビューの同一セットを、複数のユーザーに対して同時に許可することができます。ユーザー許可の管理

は、グループごとのほかに、個人ごとにも実行できます。 ユーザーは、1 つ以上のユーザー・グループに関連付けることができます。グループごとの許可は、排他的ではなく包含的に付与されます (ネストされたグループはサポートされます)。また、グローバル権限や、管理対象システムおよび管理対象システム・グループとの関連付けによっても許可が行われます。このセキュリティーは、外部の許可には依存しません。

許可

機能の許可の同一セットを、複数のユーザー、ユーザー・グループ、または個別ユーザー ID に対して同時に許可することができます。

以下の機能は、ユーザー ID またはユーザー・グループごとに、個別に使用可能または使用不可に設定されます。

アクション

☑ **「ビュー」**をチェックすると、アクション実行ビューおよびナビゲーター項目のポップアップ・メニューに選択可能なコマンドのリストを表示し、そこからアクション実行コマンドを実行できるようになります。

☑ **「変更」**をチェックすると、アクション実行コマンドの作成および保存ができるようになります。使用可能になると、**「アクションの編集」** がナビゲーターのポップアップ・メニューに表示されます。

アクション実行コマンドを実行する場合、要求されたコマンドを関連するシステム上で実行する権限が必要です。 例えば、TSO コマンドを実行するには、ご使用のユーザー ID が、有効な TSO ID であるとともに、ポータル・サーバーで有効なユーザー ID であることが必要です。このユーザー ID は、ポータル・サーバーのログオン時に入力する場合とまったく同様に、大/小文字まで正確に入力される必要があります。

エージェント管理

☑ **「管理」**をチェックすると、管理対象ネットワーク全体でのエージェント・デプロイメントができるようになります。デプロイメントには、モニター対象製品をインストールする作業、ソフトウェア改訂を最新の状態に維持する作業、および管理対象ネットワークからエージェントを削除する作業が含まれます。 この許可を使用可能にする場合も、「アクション」-「変更」が必要です。

☑ **「開始/停止」**をチェックすると、モニター・エージェントの開始および停止ができるようになります。

カスタム・ナビゲーター・ビュー

☑ **「変更」**をチェックすると、新規ナビゲーター・ビューを作成し、それを編集および削除できるようになります。「変更」をクリアすると、ユーザーにはナビゲーター・ツールバーの **「ナビゲーター・ビューの編集」** が表示されません。

イベント

☑ **「添付」**をチェックすると、シチュエーション・イベントにファイル (詳細なメモなど) を添付できるようになります。またこの許可では、確認および表示の許可をユーザーが保持している必要があります。

「**閉じる**」をチェックすると、ピュア・イベントや、シチュエーションを手動で停止する前に開いていたイベントをクローズできるようになります。これが使用可能になると、選択したイベントがピュア・イベントの場合、またはシチュエーションが停止している場合、シチュエーション・イベントの吹き出しリストのポップアップ・メニュー、イベント・ナビゲーター項目、およびシチュエーション・イベント・コンソール・ビューのポップアップ・メニューに「**シチュエーション・イベントをクローズする**」が表示されます。

「**ビュー**」をチェックすると、シチュエーションが true になったときに、ナビゲーターにシチュエーション・イベント・インディケーターが表示されるようになります。

「**確認**」をチェックすると、シチュエーション・イベントを確認できるようになります。この許可を有効にすると、「**確認イベント**」が、シチュエーション・イベントの吹き出しリストのポップアップ・メニュー、イベント・ナビゲーター項目、およびシチュエーション・イベント・コンソール・ビューに表示されます。

機能

「**有効**」は変更できないため、グレーアウト表示されています。この機能へのアクセス権限は、ユーザーの組織が所有する IBM Tivoli Monitoring ライセンスにより決定されます。

ヒストリー

「**構成**」 をチェックすると、「ヒストリカル収集の構成」ウィンドウのオープン、ヒストリー・ファイルおよびデータ・ロールオフの構成、およびさまざまな属性グループに関するデータ収集の開始および停止を実行できるようになります。この許可が使用可能になると、 「**ヒストリー構成**」 が、メイン・ツールバーに表示されます。

アプリケーションの起動

「**起動**」 をチェックすると、ナビゲーター項目、表ビュー、グラフ・ビュー、またはシチュエーション・イベント・コンソール・ビューで使用可能な任意の起動定義を呼び出せるようになります。この許可が使用可能になると、 「**ヒストリー構成**」 が、メイン・ツールバーに表示されます。

「**ビュー**」 をチェックすると、選択した起動定義の構成を確認できるようになります。

「**変更**」 をチェックすると、起動定義を作成、編集、および削除できるようになります。

管理対象システム・グループ

「**ビュー**」をチェックすると、管理対象システム・グループを表示するためにオブジェクト・グループ・エディターを使用できるようになります。オブジェクト・グループ・エディター・ツールを使用できるようにするには、「変更」許可も必要です。

「**変更**」をチェックすると、オブジェクト・グループ・エディターを開いて管理対象システム・グループを作成、編集、および削除できるようになります。

ポリシー

「**ビュー**」 をチェックすると、「ワークフロー」ウィンドウを開いて、

ポリシーおよびそれらの定義を表示できるようになります。表示許可により、  **「ワークフロー・エディター」** がメイン・ツールバーで使用可能になり、  **「ポリシーの管理」** が  エージェント・レベルのナビゲーター・ポップアップ・メニューで使用できるようになります。

☑ **「開始/停止」** をチェックすると、ポリシーを開始および停止できるようになります。この許可が使用可能になると、  **「ポリシーの開始」** および  **「ポリシーの停止」** が、ポリシーの選択時に使用できるようになります。

☑ **「変更」** をチェックすると、ワークフロー・エディターを開いて、ポリシーを作成および編集できるようになります。変更許可が使用可能になると、  **「新規ポリシー」** が、ユーザーがポリシーを選択した後に使用可能になります。その他の編集ツール  **「ワークフローの編集」**、  **「ポリシーのコピー」**、および  **「ポリシーの削除」** でも同様です。

照会

☑ **「ビュー」** をチェックすると、プロパティー・エディターから照会エディターを使用したり、選択した表またはグラフに関する照会を選択したりできるようになります。表示許可が使用可能になると、ユーザーは、プロパティー・エディターの「照会」タブによって、照会を割り当てることができます。

☑ **「変更」**をチェックすると、照会エディターで照会を作成、編集、および削除できるようになります。変更許可を使用可能にすると、  **「照会エディター」** のほか、照会の編集ツールもメイン・ツールバーから使用できるようになります。

シチュエーション

☑ **「ビュー」**により、シチュエーション・エディター、および「管理対象システム」ウィンドウの「シチュエーションの管理」でシチュエーション (式のオーバーライドなど) を表示できます。表示許可が使用可能になると、  **「シチュエーション・エディター」** が、メイン・ツールバーおよびナビゲーター項目 (プラットフォーム・レベルを除く) のポップアップ・メニューで使用できるようになります。

☑ **「変更」**をチェックすると、新規シチュエーションを作成および管理できるようになります。変更許可が与えられている場合、シチュエーション・エディターで、シチュエーション編集ツール、ポップアップ・メニュー・オプション、および「配布」タブの**「式の上書き」**ボタン (シチュエーションを限定するための機能) を使用できます。

☑ **「開始/停止」**により、シチュエーションを開始または停止し、シチュエーションのオーバーライドを有効または無効にできます。この許可を有効にすると、  **「シチュエーションの開始」** および  **「シチュエーションの停止」** が、シチュエーション・イベントの吹き出しリスト、シチュエーション・イベント・コンソール・ビュー、シチュエーション・エディターのポップアップ・メニュー、および「管理対象システム」ウィンドウの「シチュエーションの管理」で使用できるようになります。また、シチュエーショ

ン・エディターのポップアップ・メニューで **「シチュエーションの上書きを有効にする」** および **「シチュエーションの上書きを無効にする」** を選択できるようになります。

端末スクリプト

☑ **「ビュー」** をチェックすると、端末エミュレーター・スクリプトを実行または停止してスクリプトを表示できるようになりますが、編集することはできません。「表示」が無効の場合、ユーザーはスクリプトの実行または停止のみを行うことができます。

☑ **「変更」** をチェックすると、新規端末エミュレーター・スクリプトを作成、記録、編集、および削除できるようになります。

ユーザー管理

ユーザー自身のユーザー ID を表示している場合、「表示」および「変更」は無効になっており、ユーザー自身のユーザー管理権限は変更できません。

☑ **「ログオンの許可」** をチェックすると、このユーザー ID でポータル・サーバーにログオンできるようになります。管理者は、このチェック・ボックスをクリアして、ポータルへのユーザー・アクセスを拒否できます。このオプションは、Tivoli Enterprise Portal Server 環境構成ファイル *kfwenv* の、KFW_AUTHORIZATION_MAX_INVALID_LOGIN (デフォルトは 0 であり、この場合は試行回数に制限はありません) パラメーターとともに動作します。値が設定され、無効な試行の回数がその制限を超えると、チェック・ボックスは自動的にクリアされます。ログオン試行回数をリセットするには、管理者がこのチェック・ボックスを選択する必要があります。詳しくは、「*IBM Tivoli Monitoring 管理者ガイド*」を参照してください。☐ **「変更」** をチェックすると、ユーザー ID を編集および削除できるようになります。この許可が使用可能になると、 **「ユーザー管理」** がメイン・ツールバーで使用可能になり、ツールが「ユーザー管理」ウィンドウで使用できるようになります。

☑ **「適格な作成者モード」** をチェックすると、**「ワークスペース管理」** (後続の権限を参照) で、作成者モードの許可を有効または無効にできるようになりますが、他のユーザー ID についてこれを有効または無効にすることはできません。

☐ **「ビュー」** をチェックすると、「ユーザー管理」ウィンドウを開いて、ユーザー・プロファイルを表示できるようになります。

☑ **「適格な管理モード」** をチェックすると、**「ワークスペース管理」** (次の権限を参照) で、管理モードの許可を有効または無効にできるようになりますが、他のユーザー ID についてこれを有効または無効にすることはできません。

ワークスペース管理

☑ **「ワークスペース作成者モード」** をチェックすると、ワークスペース、リンク、および端末エミュレーター・スクリプトを作成および編集できるようになります。「ワークスペース作成者モード」を無効にすると、これらの変更を行うことはできませんが、引き続きモニターを行って、アラートに応答することはできます。ツールは引き続き表示可能ですが、使用不可になります。

☐ **「ワークスペース管理モード」** は、SYSADMIN ユーザー ID、および「ユーザーの追加作成」ウィンドウでその ID から作成された新規の ID に対してのみ使用可能です。管理モードが有効に設定されている場合、ワークスペースに対して行った変更は、同じポータル・サーバーにログオンしているすべてのユーザーに適用されます。無効に設定されている場合、ワークスペースに対する変更は、他のユーザーには共有されません。 管理モードでワークスペースを作成または編集する場合は、必ず「ワークスペース・プロパティー」の ☑ **「変更を許可しない」** を選択してください。これを行わないと、別のユーザーがそのワークスペースを編集した場合にワークスペースの所有者が変わってしまい、その変更を無効にできません。

WebSphere MQ 構成権限

IBM Tivoli OMEGAMON XE for Messaging: WebSphere MQ 構成をインストールすると、このフォルダーが表示されます。

☑ **「ビュー」**をチェックすると、ナビゲーター構成ビューでユーザー組織の WebSphere MQ 構成を確認できるようになりますが、変更することはできません。

☑ **「変更」**をチェックすると、構成ビューでユーザー組織の WebSphere MQ 構成を変更したり、更新をスケジュールに入れたりできるようになります。

ストレージ・サブシステム権限

IBM Tivoli OMEGAMON XE for Storage をインストールすると、このフォルダーが表示されます。☑ **「ビュー」**をチェックすると、データを表示できるようになりますが、変更することはできません。☑ **「変更」**をチェックすると、データを変更できるようになります。

「データ収集構成」をチェックすると、DFSMSrmm 状況ワークスペースとデータ・セット属性システム要約ワークスペースの収集制御間隔を表示および変更できるようになります。

「データ・セット・グループの収集間隔」をチェックすると、データ・セット・グループ要約ワークスペースの制御間隔を表示および変更できるようになります。

「データ・セット・グループの定義/更新」をチェックすると、データ・セット・グループ要約ワークスペースのグループ定義を表示および変更できるようになります。

アプリケーション

ユーザー ID の設定に応じて、モニター対象アプリケーション・タイプの一部またはすべてを表示できます。 例えば、あるユーザーが表示できるのはメインフレーム・アプリケーションのみで、別のユーザーはミドルウェアのみ、さらに別のユーザーはすべてのアプリケーションを表示できます。

許可されたアプリケーション

Tivoli Enterprise Portal からアクセスできるアプリケーションを表示します。

使用可能アプリケーション

選択されたユーザーへの割り当てで使用可能なアプリケーションを表示しま

す。「**<すべてのアプリケーション>**」が「**許可されたアプリケーション**」リストにある場合は、追加できる項目はありません。 アプリケーションのサブセットを割り当てるよう選択するには、それを「**使用可能アプリケーション (Available Applications)**」に移動して戻す必要があります。

追加するアプリケーションを選択するか、または「**<すべてのアプリケーション>**」を選択して、「**許可されたアプリケーション**」リストに◂ 移動します。最初にアプリケーションを 1 個選択し、次に Ctrl キーを押しながら他のアプリケーションをクリックすると、クリックしたアプリケーションを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したアプリケーションから次に選択したアプリケーションまでの間にあるすべてのアプリケーションを選択することもできます。

ナビゲーター・ビュー

ナビゲーター・ビューが作成されると、そのビューを表示できるのはその作成者だけですが、管理者は、ユーザーへの割り当てを実行できます。 ナビゲーター・ビューが割り当てるということは、ユーザーがそのビューを開くことができるということです。割り当てられた各ビューで、ユーザーが表示できるのは、すべての階層ではなく特定の分岐のみに制限されている場合があります。

割り当て済みビュー

ユーザーが確認しアクセスできるナビゲーター・ビューを表示します。 このリストの最初のナビゲーター・ビューは、そのユーザーのデフォルトであり、ユーザーがログオンした場合に自動的に表示されます。 ユーザーにアクセスさせたくないビューがあれば、それを選択し、➡ 右矢印をクリックしてそれを「**使用可能ビュー**」リストに移動します。 適切な項目を選択し、◂ 左矢印をクリックして、それを「**割り当て済みビュー**」に移動します。 あるナビゲーター・ビューをリストの先頭に移動し、デフォルトに設定するには、▲ 上矢印をクリックします。

使用可能ビュー

ユーザーに割り当てられていないが、割り当て可能なナビゲーター・ビューを表示します。 追加するナビゲーター・ビューを選択し、◂ 左矢印を使用して、それらを「**割り当て済みビュー**」リストに移動します。 最初にビューを 1 個選択し、次に Ctrl キーを押しながら他のビューをクリックすると、クリックしたビューを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したビューから次に選択したビューまでの間にあるすべてのビューを選択することもできます。

割り当て済みルート

「割り当て済みビュー」で選択されているナビゲーター・ビューを表示し、ユーザーに割り当てられたナビゲーター・ルートを強調表示します。 ルートは、ユーザーがアクセスできるそのナビゲーター・ビューの最高位のレベルです。 ユーザーは、ナビゲーターにおけるこの項目およびその下のすべての項目にアクセスできますが、その項目と並行する項目またはその上の項目にはアクセスできません。

例えば、UNIX システムを割り当て済みルートとして割り当てることができます。UNIX システムのワークスペースおよびその下の項目は表示されますが、エンタープライズ・ワークスペースや Windows システムの下にある項目は表示できません。

構成メンバーおよびメンバー

リストからユーザーまたはユーザー・グループを選択すると、タブの下部セットにある最後のタブに、(「ユーザー」または「ユーザー・グループ」のいずれを選択したかを反映して)「**構成メンバー**」または「**メンバー**」と表示されます。どちらのタブでも、グループへのユーザーの割り当てを実行できます。

ユーザー ID の管理

ユーザー ID の管理では、まず、ユーザーに対して付与する権限と、ユーザーをユーザー・グループに所属させるかどうかのプランニングを行います。

「ユーザー管理」ウィンドウには、ユーザー ID の作成と保守、および許可の調整を行うためのツールが用意されています。ポータル・サーバー経由でのユーザー認証が構成済みの場合、このウィンドウは、ユーザー ID が、LDAP ユーザー・レジストリー内のそのユーザー ID の固有 ID にマップされる場所でもあります。

ユーザー ID の追加

ポータル・クライアントまたは **tacmd tepsLogin** コマンドを使用して Tivoli Enterprise Portal Server にログオンできる必要があるすべてのユーザーのユーザー ID を作成します。モニター・データを要求する IBM Dashboard Application Services Hub ユーザーにもユーザー ID が必要です。デフォルトのユーザー・プロファイルを使用することも、既存のユーザーのプロファイルをコピーすることもできます。

始める前に

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

手順

1. 「**ユーザー管理**」をクリックします。
2. 新規ユーザー ID を作成するか、別のユーザー ID からユーザー ID を作成するには、以下のようにします。
   - デフォルト・ユーザー・プロファイルを持つ新規ユーザー ID を作成するには、「**新規ユーザーの作成**」をクリックします。
   - 既存のユーザー ID から新規のユーザー ID を作成するには、使用するプロファイルを「**ユーザー**」リストから選択し、「**ユーザーの追加作成**」をクリックします。
3. 「新規ユーザーの作成」ウィンドウで、以下のユーザー情報を入力してください。
   - **ユーザー ID**: ログオン名。名前は ASCII 文字である必要があり、最大 10 文字で、スペースを含むことはできません。ユーザー認証がハブ・モニター・サーバーで行われ、そしてその認証で z/OS に対して RACF (リソース・アクセス管理機能) セキュリティーが使用されている場合は、この名前の長さは 8 文字に制限されます。

- **ユーザー名**: ユーザーの名前またはジョブ種別、あるいはその両方。この名前にはスペースを含めることができ、最大長は 32 文字です。ユーザー名は、「**ユーザー**」リストに表示されます。
- **識別名:** 「**ユーザー ID**」フィールドで指定される名前に対応する、Lightweight Directory Access Protocol (LDAP) ユーザー・レジストリー内の固有 ID。識別名 (例えば、UID=FRIDA,O=DEFAULTWIMITMBASEDREALM) を見つけて挿入するには、「**検索**」をクリックします。
- **ユーザー説明:** ユーザーに関する説明 (オプション)。テキストには、スペースと句読点を含めることができます。

4. 「**OK**」をクリックしてウィンドウを閉じると、新規ユーザー ID がアルファベット順で「**ユーザー**」リストに表示されます。
5. **許可**を変更するには、機能を「**権限**」ツリーから選択し、変更する許可を持つすべての機能について、各オプションを適宜選択またはクリアします。
6. アプリケーションへのアクセス権 (管理対象システムのタイプ) を割り当てるには、**アプリケーション**タブをクリックして、「**<すべてのアプリケーション>**」またはユーザーに表示する個々のアプリケーションを選択し、 をクリックして「**許可されたアプリケーション**」リストに移動します。 最初にアプリケーションを 1 個選択し、次に Ctrl キーを押しながら他のアプリケーションをクリックすると、クリックしたアプリケーションを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したアプリケーションから次に選択したアプリケーションまでの間にあるすべてのアプリケーションを選択することもできます。
7. ナビゲーター・ビューを割り当てるには、 「**ナビゲーター・ビュー**」 タブをクリックします。
   a. 「**使用可能ビュー**」からナビゲーター・ビューを選択し (複数選択する場合は Ctrl または Shift を押しながらクリックする)、 をクリックして、ビューを「**割り当て済みビュー**」に移動させます。
   b. デフォルトにしたいビューをリストの一番上に配置するには、 を使用し、他のナビゲーター・ビューを、ナビゲーター・ツールバーのビューの リストに表示する順序に並べ替えるには、 および を使用します。
   c. 選択されたナビゲーター・ビューで、「**割り当て済みルート**」を必要に応じて変更します。
8. ユーザー・プロファイルの作成を完了した際に、「ユーザー管理」ウィンドウを開いたままにする場合は「**適用**」を選択して変更を保存します。ウィンドウを閉じる場合には、「**OK**」を選択します。

次のタスク

Tivoli Enterprise Portal クライアントの「ログオン」ウィンドウには、ユーザー ID とパスワードを入力するためのフィールドがあります。ユーザー ID とパスワードを認証する場合は、ユーザーを認証するようにモニター・サーバーまたはポータル・サーバーを構成します。詳細については、89 ページの『第 5 章 ユーザー認証の使用可能化』を参照してください。

関連資料:

173 ページの『ユーザー管理』
ご使用のユーザー ID およびメンバーとなっているユーザー・グループのプロファイルには、表示および使用が許可される Tivoli Enterprise Portal 機能、表示が許可されるモニター対象アプリケーションのリスト、およびアクセス可能なナビゲーター・ビューのリスト (およびビュー内の最高位レベル) を決定する一連の許可が指定されます。

ユーザー ID の表示と編集

「ユーザー管理」ウィンドウの「**ユーザー**」リストに追加されたら、いつでもプロファイル設定の確認および編集を行うことができます。

始める前に

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

このタスクについて

ユーザー ID を編集するには、以下のステップを実行してください。

手順

1. 「**ユーザー管理**」をクリックします。
2. 「**ユーザー**」リストで、以下のいずれかを実行してください。
   - 「**名前**」または「**説明**」フィールドの内側をクリックして、編集します。
   - 行内の任意の場所をダブルクリックして、フィールドを編集するための「ユーザーの変更」ウィンドウを開きます。
   - 編集するユーザー・プロファイルを右クリックし、「**ユーザーの変更**」をクリックします。
3. 「**ユーザー名**」、「**識別名**」、または「**ユーザー説明**」を編集して、「**OK**」をクリックします。ユーザー認証をポータル・サーバーを介して LDAP ユーザー・レジストリーに対して行う場合は、識別名が必要です。 1 語のユーザー ID は、大/小文字以外は変更はできません。1 語のユーザー ID を編集するには、ユーザー・プロファイルを削除してから新規のユーザー・プロファイルを作成します。
   - DN をまだ追加していない場合は、「**検索**」をクリックして、ユーザー ID に一致する名前を見つけてください。
     モニター対象である環境が、以前に Tivoli Enterprise Monitoring Server 経由で認証するように構成され、その後 Tivoli Enterprise Portal Server 経由で認証するように再構成された場合、同じ名前の項目が 2 つ表示されることがあります。o=defaultWIMFileBasedRealm となっている項目を選択し、O=DEFAULTWIMITMBASEDREALM は選択しないでください。
4. 許可を変更するには、機能を「**権限**」ツリーから選択し、変更する許可を持つすべての機能について、各オプションを適宜選択またはクリアします。 自分のユーザー許可は、ユーザー管理の作成と変更を除き、変更することができます。

5. アプリケーションにアクセス権 (管理対象システムのタイプ) を割り当てるには、「アプリケーション」タブをクリックして、削除するアプリケーションを「**許可されたアプリケーション**」リストから選択し、 をクリックしてそれらを「**使用可能アプリケーション**」リストに移動します。また、追加するアプリケーションを「**使用可能なアプリケーション**」リストから選択し (または「**<すべてのアプリケーション>**」を選択し)、 をクリックしてそれらを「**許可されているアプリケーション**」リストに移動します。

   最初にアプリケーションを 1 個選択し、次に Ctrl キーを押しながら他のアプリケーションをクリックすると、クリックしたアプリケーションを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したアプリケーションから次に選択したアプリケーションまでの間にあるすべてのアプリケーションを選択することもできます。
6. ナビゲーター・ビューの割り当てを変更するには、「ナビゲーター・ビュー」タブをクリックし、「**割り当て済みビュー**」リストでナビゲーター・ビューを追加または削除し、 を使用して、デフォルトにするビューをリストの先頭に移動します。各ナビゲーター・ビューで、「**割り当て済みルート**」を必要に応じて変更します。
7. ユーザー・プロファイルの編集を完了した際に、「ユーザー管理」ウィンドウを開いたままにする場合は「**適用**」を選択して変更を保存します。ウィンドウを閉じる場合には、「**OK**」を選択します。

タスクの結果

次回のユーザーのログオン時に、権限の変更内容が有効になります。

関連資料:

173 ページの『ユーザー管理』
ご使用のユーザー ID およびメンバーとなっているユーザー・グループのプロファイルには、表示および使用が許可される Tivoli Enterprise Portal 機能、表示が許可されるモニター対象アプリケーションのリスト、およびアクセス可能なナビゲーター・ビューのリスト (およびビュー内の最高位レベル) を決定する一連の許可が指定されます。

ユーザー ID の削除

必要に応じて、ユーザー ID を削除できます。

このタスクについて

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

ユーザー・グループを削除するには、以下のステップを実行してください。

手順

1. 「**ユーザー管理**」をクリックします。
2. 削除したいユーザー ID を選択します。 Ctrl キーを押しながらクリックすれば、複数のユーザー ID を追加で選択することができます。また、Shift キーを

押しながらクリックすれば、選択したユーザー ID から次に選択した ユーザー ID までの間にあるすべてのユーザー ID を選択することもできます。

3. 「**ユーザーの削除**」をクリックして、選択したユーザー ID とプロファイルをリストから削除します。
4. ユーザー ID の削除を確認するメッセージが表示されたら、「**はい**」をクリックします。 ユーザーがユーザー ID リストから完全に削除されます。 ユーザーが現在サインオンしている場合、ワーク・セッションには影響を与えませんが、再度ログオンできなくなります。

   注: (ログオンに使用している) ユーザー ID、または <デフォルト・ユーザー> の ID は削除できません。

デフォルト・ユーザー

「**ユーザー**」リストの最初のユーザー ID は、<デフォルト・ユーザー> です。

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

デフォルト・ユーザー ID は、「**新規ユーザーの作成**」を使用して作成されるユーザーのテンプレート ID として使用されます。デフォルト設定を変更する場合には、このユーザー ID を編集します。 デフォルト初期値の場合、「ユーザー管理」の「作成」と「変更」以外の Tivoli Enterprise Portal Authorities でリストされたすべての機能を使用することができます。 <デフォルト・ユーザー> の ID に加えたすべての変更は、ここから作成されたユーザーに適用されます。既存のユーザー ID の設定には、影響を与えません。

ユーザー・グループの管理

管理者は、ユーザー・グループを使用して、機能の許可、アプリケーションおよびナビゲーター・ビューの同一セットを、複数のユーザーに対して同時に許可することができます。ユーザー許可の管理は、グループごとのほかに、個人ごとにも実行できます。

1 人のユーザーを、1 つ以上のユーザー・グループに関連付けることができます。ユーザーに対して、ユーザー ID を使用して直接付与されている許可は、当該ユーザーの属するユーザー・グループでその許可が付与されない場合でも保持されます。 逆の場合も同様で、個々のユーザー ID に許可が付与されておらず、グループ ID には付与されている場合、ユーザーはユーザー・グループのメンバーシップ経由でその許可を付与されることになります。 つまり、ユーザーの許可セットは、個々のユーザー ID に付与されているものと、そのユーザーが属するすべてのユーザー・グループに付与されているものから取得されます。

また、グローバル権限や、管理対象システムおよび管理対象システム・グループとの関連付けによっても許可が行われます。このセキュリティーは、外部の許可には依存しません。

上部にあるアクティブなタブが 「**ユーザー**」である場合、下部のタブ・セットにある最後のタブは、 「**所属先**」です。 上部にあるアクティブなタブが

「**ユーザー・グループ**」である場合、 「**メンバー**」タブもあります。グループへのユーザーの割り当ては、これら下側にあるタブのいずれかで実行できます。

一番上の詳細ビューでグループをクリックして 「**メンバー**」タブに移動すると、このグループに属すユーザーのリストが表示されます。 同様に、ユーザーが属しているグループも確認できます。

ユーザー・グループのメンバーシップの表示

ユーザー ID が属するグループと、ユーザー・グループに属しているユーザー ID のリストの両方を表示できます。

このタスクについて

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

手順

1. 「**ユーザー管理**」をクリックします。 「ユーザー管理」ウィンドウは、上部の「**ユーザー**」および「**ユーザー・グループ**」タブと、下部の「**許可**」、「**アプリケーション**」、「**ナビゲーター・ビュー**」、および「**メンバー**」タブの、2 つの部分に分割されています。
2. ユーザーの所属しているグループを確認するには、「**ユーザー**」リストで名前を選択して、「**構成メンバー**」タブをクリックします。そのユーザーの属するグループが、「**割り当て済みメンバー**」リストに表示されます。
3. グループに割り当てられているユーザー ID を確認するには、 「**ユーザー・グループ**」リストで名前を選択して、「**メンバー**」タブをクリックします。そのグループに属するユーザーが、「**割り当て済みメンバー**」リストに表示されます。

ユーザー・グループの追加

新しいユーザー・グループを最初から作成することも、また、必要とする許可とユーザー割り当てにほぼ近い内容のグループをコピーしてそれを変更することもできます。

始める前に

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

このタスクについて

ユーザー・グループを追加するには、以下のステップを実行してください。

手順

1. 「**ユーザー管理**」をクリックして「ユーザー管理」ウィンドウを開きます。
2. 「**ユーザー・グループ**」 タブをクリックします。
3. 以下のいずれかを実行します。

- 新規ユーザー・グループを作成するには、「**新規グループの作成**」をクリックします。
- 既存のユーザー・グループをコピーするには、リストからグループ名を選択して、「**グループの追加作成**」をクリックします。

4. 「新規グループの作成」ウィンドウまたは「グループの追加作成」ウィンドウで、以下のユーザー情報を入力します。
   a. **グループ ID:** グループ ID です。この名前は最大 10 文字で指定し、スペースを含むことはできません。 ハブ・モニター・サーバーで z/OS の RACF (リソース・アクセス管理機能) セキュリティーを使用している場合は、名前の長さが 8 文字に制限されます。
   b. **グループ名:** このユーザー・グループの名前またはジョブ種別です。この名前には、スペースを含むことができます。
   c. **グループの説明:** ユーザー・グループを説明するテキストです (ユーザー・グループの役割など)。説明には、スペースと句読点を含めることができます。
5. 「**OK**」をクリックしてウィンドウを閉じると、新規ユーザー・グループがアルファベット順で「ユーザー・グループ」リストに表示されます。
6. グループへのメンバーの追加は「**メンバー**」タブで行います。「**選択可能メンバー**」リストでユーザー ID を 1 つ以上選択し、 をクリックして「**割り当て済みメンバー**」リストに移動します。
7. グループの 許可を変更するには、機能を「**権限**」ツリーから選択して、すべての機能について各オプションのチェック・ボックスを選択またはクリアします。
8. グループにアプリケーションへのアクセス権 (管理対象システムのタイプ) を割り当てるには、「アプリケーション」タブをクリックして、「**<すべてのアプリケーション>**」またはユーザーに表示する個々のアプリケーションを選択し、 をクリックして「**許可されたアプリケーション**」リストに移動します。最初にアプリケーションを 1 個選択し、次に Ctrl キーを押しながら他のアプリケーションをクリックすると、クリックしたアプリケーションを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したアプリケーションから次に選択したアプリケーションまでの間にあるすべてのアプリケーションを選択することもできます。
9. グループにナビゲーター・ビューを割り当てるには、「ナビゲーター・ビュー」タブをクリックして、「**割り当て済みビュー**」リストでナビゲーター・ビューを追加または削除し、 を使用してデフォルト・ビューをリストの先頭に配置します。各ナビゲーター・ビューで、「**割り当て済みルート**」を必要に応じて変更します。
10. ユーザー・グループの作成が終了したら、「ユーザー管理」ウィンドウを開いたままにする場合は「**適用**」を選択して変更を保存します。ウィンドウを閉じる場合には「**OK**」を選択します。

ユーザー・グループの検討および編集

「ユーザー管理」ウィンドウの「**ユーザー・グループ**」リストにユーザー・グループが追加されたら、いつでもプロファイル設定の確認および編集を行うことができます。

このタスクについて

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

ユーザー ID を編集するには、以下のステップを実行してください。

手順

1. 「**ユーザー管理**」 をクリックして、「ユーザー管理」ウィンドウを開きます。
2. 「**ユーザー・グループ**」 タブをクリックします。
3. 編集するユーザー・グループを右クリックして、 をクリックします。
4. 「**グループ名**」と「**グループ説明**」を編集して、「**OK**」をクリックします。 1 ワードのグループ ID は変更できません。 代わりに、このユーザー・グループから別のユーザー・グループを作成して新しい名前を付け、その後でこのユーザー・グループを削除します。
5. 許可を変更するには、機能を「**権限**」ツリーから選択し、変更する必要のある許可を持つすべての機能について、各オプションを適宜選択またはクリアします。
6. アプリケーションへのグループ・アクセス権 (管理対象システムのタイプ) を変更するには、「アプリケーション」タブをクリックし、削除するアプリケーションを「**許可されたアプリケーション**」リストで選択して をクリックするか、追加するアプリケーションを「**使用可能アプリケーション**」リストで選択して (または「**<すべてのアプリケーション>**」を選択して)、 をクリックします。 最初にアプリケーションを 1 個選択し、次に Ctrl キーを押しながら他のアプリケーションをクリックすると、クリックしたアプリケーションを追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択したアプリケーションから次に選択したアプリケーションまでの間にあるすべてのアプリケーションを選択することもできます。
7. グループのナビゲーター・ビューの割り当てを変更するには、「ナビゲーター・ビュー」タブをクリックして、「**割り当て済みビュー**」リストでナビゲーター・ビューを追加または削除し、 を使用してデフォルト・ビューにするビューをリストの先頭に配置します。各ナビゲーター・ビューで、「**割り当て済みルート**」を必要に応じて変更します。
8. ユーザー・グループの編集を完了した際に、「ユーザー管理」ウィンドウを開いたままにする場合は「**適用**」を選択して変更を保存します。ウィンドウを閉じる場合には、「**OK**」を選択します。 ユーザー・グループの変更内容は、各グループ・メンバーが次回ログオンする際に有効になります。

   注: 自分がメンバーとなっているグループで、「ユーザー管理」の「作成」と「変更」以外の許可を変更できます。

ユーザー・グループの削除

ユーザー・グループを削除できます。

このタスクについて

この機能を使用するには、ユーザー ID に、ユーザー管理に関する変更の許可が必要です。

ユーザー・グループを削除するには、以下のステップを実行してください。

手順

1. 「**ユーザー管理**」 をクリックして、「ユーザー管理」ウィンドウを開きます。
2. 「**ユーザー・グループ**」 タブをクリックします。
3. 削除するユーザー・グループをリストから選択して、「**選択したグループの削除**」をクリックします。 Ctrl キーを押しながらクリックすれば、複数のユーザー・グループを追加で選択することができます。また、Shift キーを押しながらクリックすれば、選択したユーザー・グループから次に選択したユーザー・グループまでの間にあるすべてのユーザー・グループを選択することもできます。
4. ユーザー・グループの削除を確認するメッセージが表示されたら、「**はい**」をクリックします。 グループが、ユーザー・グループのリストから完全に削除されます。 このユーザー・グループに属し、グループから許可を付与されているすべてのメンバーは、ポータル・サーバーに次回ログオンするまで影響を受けません。

ユーザー管理についての注意事項

以下の注意事項を確認し、Tivoli Enterprise Portal の機能およびモードでのユーザー ID の役割について理解してください。

ワークスペース管理モード

ワークスペース、リンク、およびTivoli Enterprise Portalの端末ホスト・セッション・スクリプトに対して行った変更は、変更したユーザーのユーザー ID でのみ使用可能です。ただし、ワークスペース管理モードが有効になっている間は例外となります。

ワークスペース管理モードでは、同一の Tivoli Enterprise Portal に接続するすべてのユーザー間で共有されるワークスペース、リンク、および端末エミュレーター・スクリプトをカスタマイズおよび追加できます。ワークスペース管理モードの開始を参照してください。

SYSADMIN ログオン ID

Tivoli Enterprise Portal でワーク・セッションを開始する際は常にログオン ID が必要です。すべての ID を ポータル・サーバー上に事前に登録する必要があります。**SYSADMIN** を使用してポータル・サーバーにログオンし、「ユーザー管理」ウィンドウを使用して他のユーザー ID を登録することができます。初期ユーザー ID **SYSADMIN** には、全アクセス権限と完全な管理者権限が与えられています。システム管理者は、追加ユーザーを登録して、アクセス権と権限を設定します。

ユーザー ID およびグループ

各ユーザー ID は、Tivoli Enterprise Portal Server に保管され、以下の情報を含んでいます。

- ユーザー名
- ジョブ記述
- Tivoli Enterprise Portal 機能を表示または変更するための許可
- 割り当てられたナビゲーター・ビューと、各ビューでルートとして表示されるナビゲーター項目 (デフォルトは最初の項目)
- 特定のモニター・アプリケーションへのアクセス
- そのユーザーが属するユーザー・グループ、および、ユーザー・グループによってそのユーザーに許可が付与されていることを示すインディケーター

各ユーザー・グループもポータル・サーバーに保管されており、個々のユーザー ID の場合と同じ内容が含まれています。 ただし、ユーザー・グループのリストの代わりに、そのグループに割り当てられているユーザー ID のリストが含まれています。

デフォルト・ユーザー

リスト内の先頭のユーザー ID は **<デフォルト・ユーザー>** であり、「新規ユーザーの作成」を使用して作成されるユーザーのテンプレート ID として使用されます。デフォルト設定を変更する場合には、このユーザー ID を編集します。 初期のデフォルトでは、「**ユーザー管理**」の「変更」許可を除く、「Tivoli Enterprise Portal の権限」にリストされたすべての機能を使用できます。 <デフォルト・ユーザー> の ID に加えたすべての変更は、これから作成されるユーザーに適用されます。既存のユーザー ID の設定には影響を与えません。

アクセス権のユーザーへの付与

各ユーザーのユーザー ID を作成する際に、特権の許可を設定します。 ユーザーに対する操作可能領域およびカスタマイズ・オプションへのアクセス権の付与では、十分な計画が必要です。 特権の許可を指定する際は、各ユーザーの職責と企業のセキュリティー要件を考慮してください。

重要: カスタム照会を作成する許可を持つすべてのユーザーは、Tivoli Enterprise Portal Server に作成されているすべての ODBC DSN (データ・ソース名) にアクセスできます。DSN で使用されるデータベース・ユーザー ID をデータベース・ソフトウェアに追加して、ユーザーのアクセスを、ユーザーの組織のセキュリティー・ポリシーで許可された表、列などにのみ制限されるようにします。

自動 Tivoli Enterprise Portal ユーザー ID 作成

新規ユーザーが IBM Dashboard Application Services Hub でモニター・ダッシュボードに初めてアクセスすると、そのユーザーの Tivoli Enterprise Portal ユーザー ID がまだ存在しない場合、Tivoli Enterprise Portal ユーザーID が自動的に作成され、ユーザーの LDAP 識別名にマップされます。Tivoli Enterprise Portal ユーザー ID はランダム生成ストリングです。Tivoli Enterprise Portal の許可およびモニター・アプリケーションをダッシュボード・ユーザーに割り当てる必要があり、そのユーザ

ーの Tivoli Enterprise Portal ユーザー ID が自動的に作成されている場合は、許可をランダム生成ユーザー ID に割り当てるか、または以下のステップを実行します。

1. 自動的に作成された Tivoli Enterprise Portal ユーザー ID を削除します。
2. 新しいユーザーの Tivoli Enterprise Portal ユーザー ID を作成し、それをユーザーの LDAP 識別名にマップしてから、そのユーザー ID に許可およびモニター・アプリケーションを割り当てます。

ユーザー・アクセスの検証

Tivoli Enterprise Portal Server は、ユーザーがログオンするたびにユーザー ID を検証します。ジョブ記述が変わって、ユーザーがポータル・サーバーへの異なるアクセス権を必要とする場合、そのユーザーのアクセス権を確認する必要があり、場合によってはそれを変更しなければならないことがあります。

ポータル・サーバーにログオンするためのユーザー ID には、パスワードを含めることができます。ポータルではパスワードを設定しないでください。 代わりに、それと一致するユーザー ID とパスワードを、以下のような、ネットワーク・ドメインのユーザー・アカウント、または、Tivoli Enterprise Monitoring Server があるオペレーティング・システムに対して定義する必要があります。

- Windows システムのユーザー・アカウント
- UNIX システムのパスワード・ファイル
- z/OS システムの RACF または ACF/2 ホスト・セキュリティー・システム

また、ユーザーを検証するようにモニター・サーバーを構成する必要があります。ユーザーがポータル・サーバーにログオンする際、ハブ・モニター・サーバーはドメインまたはオペレーティング・システムに対して、ユーザー ID とパスワードを検証するよう要求します。

モニター・サーバーが分散システム上にインストールされている場合は、以下のようにして、ユーザーを検証するように構成されているかどうかを確認できます。

1. Tivoli Enterprise Monitoring Services の管理プログラムを開始します。

   Windows 「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」。

   UNIX *install_dir* /bin ディレクトリーに移動し、./itmcmd manage [-h *install_dir*] コマンドを実行します (ここで *install_dir* はインストール・ディレクトリー (デフォルトは opt/IBM/ITM) です)。
2. TEMS1 (ハブ) の Tivoli Enterprise Monitoring Server 行を右クリックして、「**再構成**」を選択します。
3. 「Tivoli Enterprise Monitoring Server の構成」ウィンドウで、☑ 「**セキュリティー: ユーザーを確認**」 チェック・ボックスの設定を確認します。

   このオプションが選択されている場合、ユーザーがポータル・サーバーにログオンする際に常にパスワードが必要になります。選択されていない場合、ログオンする際にユーザー名は必要ですが、パスワードは必要ありません。

注: パスワードは、それぞれの組織のセキュリティー要件を満たしていなければなりません。 パスワードの定期的な変更が要件になっている場合は、ポータル・サー

バーにログオンしようとしたときに、「**ログオン・パスワードの有効期限が切れています**」というメッセージが表示されることがあります。 その場合、ログオンするためには、まずシステム・パスワードを変更する必要があります。 例えば、Windows では、「管理ツール」の「ユーザー アカウント」を使用して、パスワードを変更します。

他のアプリケーションからのポータルの起動

Tivoli Enterprise Portal を起動するためのセキュリティー要件 (シングル・サインオンの要件など) 以外にも、外部アプリケーションから起動された後に制御を受け取る Tivoli Enterprise Portal ユーザー ID は、ターゲットの管理対象システムおよびワークスペースへのアクセスを事前に許可されている必要があります。また、そのユーザー ID は、必要なアクション実行コマンドの発行を許可されている必要もあります。

アクション実行コマンド用のユーザー ID

Tivoli Enterprise Portal がアクション実行コマンドを管理対象システムに送信する際、そのアクションを実行する権限について、ユーザー ID がチェックされる場合と、チェックされない場合とがあります。最も簡単なケースでは、エージェントを実行しているユーザー ID が用いられて、コマンドが管理対象システムに送信されて実行されます。以下の場合に、Tivoli Enterprise Portal ユーザー ID がアクション・コマンドとともに送信されます。

- オンデマンド: 現在ログオンしているユーザー ID
- シチュエーション・アクション: 最後にシチュエーションを更新したユーザーのユーザー ID
- ワークフロー・アクション: 最後にポリシーを更新したユーザーのユーザー ID

ただし、ID はコマンド接頭部で通知しない限り、管理対象システムによって無視されます。これらは IBM Tivoli Monitoring 製品に実装されたコマンド・ハンドラーで、コマンドを実行するためにエージェントに渡す前に Tivoli Enterprise Portal ユーザー ID を検証する必要があるかどうかを制御します。

コマンド接頭部

「アクション実行」でコマンド接頭部が表示されている場合、エージェントはコマンドを実行する代わりに、アプリケーション・ハンドラーにコマンドを渡します。接頭部およびアクション実行コマンドの構文は **productcode:CNPuserID:command** です。エージェントはこのコマンドを、実行のためにアプリケーションに転送します。 アプリケーションでは、適切なユーザー ID を伴うコマンドであれば自由に実行できます。OMEGAMON XE for WebSphere MQ on z/OS の場合には、Tivoli Enterprise Portal ユーザー ID が使用されます。

特別な接頭部が欠落している場合、エージェントは、自身の実行に使用されているユーザー ID を用いてコマンドを実行します。

大部分のモニター製品では、コマンド接頭部を使用しません。ただし、IBM Tivoli Monitoring for WebSphere MQ では使用され、実際には、オンデマンドのアクション実行コマンドの前に非表示の **MQ:CNPuserID:** という接頭部が付加されます (ユーザーには表示されません)。

UNIX setuid コマンド

コマンド接頭部とセキュリティー出口に加えて、UNIX では setuid コマンドという別のオプションが用意されています。このコマンドを使用すると、プロセスのユーザー ID を動的に変更できます。 つまり、ID をパラメーターとして渡された値に設定してから、コマンドを実行し、その後でコマンドの実行後に ID を元に戻すようにエージェントを変更できます。

ログオン・エラー・メッセージのトラブルシューティング

ログオン・プロンプトと進行状況を示すメッセージは、「ログオン」ウィンドウのステータス・バーに表示されます。ユーザーがログオンできない場合、メッセージが表示されます。

ユーザーがログオンできない場合、次のメッセージのいずれかが表示されます。

「Tivoli Enterprise Portal Server への接続に失敗しました」

1. Tivoli Enterprise Portal Server がインストールされているシステムで、「**スタート**」-> 「**プログラム**」-> 「**IBM TivoliMonitoring**」- > 「**Tivoli Monitoring Services の管理**」とクリックします。
2. オプション: Tivoli Enterprise Portal Server の項目を右クリックして、「**スタートアップの変更**」をクリックします。 開いたウィンドウで、◉「**システム・アカウント**」 と☑「**サービスとデスクトップとの相互作用を許可**」 を選択して、「**OK**」をクリックします。

   こうすることで、Tivoli Enterprise Portal Server の起動時にコマンド行ウィンドウが開き、内部コマンドが表示されます。
3. Tivoli Enterprise Portal Server が起動したことを確認してください。

   起動している場合、リサイクルします。

   停止している場合、起動します。
4. 依然として接続できない場合には、以下の情報を検討します。この状態に該当しない場合は、IBM ソフトウェア・サポートに連絡してください。

ブラウザー・モードで実行中であり、ネットワークを経由して Tivoli Enterprise Portal Server に到達している場合、ネットワーク・システムによってホスト名を解決できないことがあります。 この場合は、以下のようにして問題を解決します。

1. Tivoli Enterprise Portal Server がインストールされているシステムで、「**スタート**」-> 「**プログラム**」-> 「**IBM TivoliMonitoring**」- > 「**Tivoli Monitoring Services の管理**」とクリックします。
2. Tivoli Enterprise Portal Browser サービスを右クリックして、「**再構成**」をクリックします。
3. 次の 2 カ所でホスト名を IP アドレスに変更します。

   「**URL を起動**」フィールドで、http://*hostname*:15200 の *hostname* を Tivoli Enterprise Portal Server の IP アドレスに変更します。 例えば、`http://10.21.2.166:15200` のように変更します。

   「**ホスト**」フィールドで、ホスト名を Tivoli Enterprise Portal Server の IP アドレスに変更します。

4. 「**OK**」をクリックします。
5. ホスト名の代わりに IP アドレスを使用して、 Tivoli Enterprise Portal のブラウザー・モードを開始します。
6. 上記の方法でも接続できない場合は、お客様サポートに連絡してください。

ログオン・パスワードの有効期限が切れています

ハブ Tivoli Enterprise Monitoring Server が「ユーザーを確認」に設定されている場合は、パスワードが必要になります。パスワードは、それぞれの組織のセキュリティー要件を満たしている必要があります。 パスワードの定期的な変更が要件になっている場合は、ポータル・サーバー にログオンしようとしたときに、このメッセージが表示されることがあります。 その場合、ログオンするためには、まずシステム・パスワードを変更する必要があります。 例えば、Windows では、「管理ツール」の「ユーザー アカウント」を使用して、パスワードを変更します。

「ユーザーの許可に失敗しました」または「ログオン要求を処理できません」

Tivoli Enterprise Portal は、TEPS データベースを使用して、ローカルでユーザーを検証します。 ご使用のハブ・モニター・サーバーがユーザー検証に設定されている場合 (Windows のデフォルト)、ユーザー ID もモニター・サーバーで検証されて、パスワードが検査されます。

ポータル・サーバーが入力されたユーザーの資格情報を確認できませんでした。 「ログオン要求を処理できません」というメッセージに対して、ポータル・サーバーでは、ユーザー資格情報の検証が可能でしたが、ログオン要求は完了しませんでした。いずれの場合も、ユーザーがログオンを再試行する必要があります。 再度メッセージが表示される場合、以下のようにします。

1. モニター・サーバーがインストールされているシステムで、 Manage Tivoli Monitoring Services 内でサーバーが稼働中であることを確認してください。
2. モニター・サーバーが稼働中の場合、ユーザー ID が Tivoli Enterprise Portal に定義されていることを確認してください。 「**ユーザー管理**」をクリックして、「**ユーザー**」リストで該当する ID を見つけます。
3. ユーザーが定義済みの場合、ハブ・モニター・サーバーでホスト・レベルのセキュリティーがオンになっていて、ユーザー ID がホスト環境に対して許可されているかどうか確認してください。

   「Tivoli Monitoring Services の管理」で、「**Tivoli Enterprise Monitoring Server**」を右クリックして、「**再構成**」をクリックします。ホスト・レベルのセキュリティーが構成されている場合には、「**セキュリティー: ユーザーを確認**」ボックスが選択されます。

   モニター・サーバーが「ユーザーを検証」に構成されている場合、Tivoli Enterprise Portal のユーザー ID も、ネットワーク・ドメインのユーザー・アカウント、またはモニター・サーバーがインストールされているオペレーティング・システムに追加する必要があります (パスワードを含む)。

非 ASCII 文字がユーザー ID に含まれていた場合、その文字はユーザー ID では保存されません。

4. 問題になっているユーザー ID を使用して、Tivoli Enterprise Portal へのログオンを試行します。
5. Tivoli Enterprise Portal にログオンできないが、モニター・サーバーは正常に稼働している場合は、 Tivoli Enterprise Portal Server に問題がある可能性があります。 ポータル・サーバーのリサイクルを試行してください。依然としてユーザーがログオンできない場合、IBM ソフトウェア・サポートにお問い合わせください。

このメッセージは、数分間の再試行期間の後でも表示されます (デフォルトは 10 分であり、 Manage Tivoli Monitoring Services を使用して変更できます)。その間、ステータス・バーには、「**ユーザー資格情報の妥当性検査を行っています**」が表示されています。 これは、モニター・サーバーが停止していることを表す症状である場合があります。

第 7 章 役割ベースの許可ポリシーの使用

Tivoli 許可ポリシー・サーバー機能では、 IBM Dashboard Application Services Hub のダッシュボード・ユーザーによる無許可アクセスからモニター・リソースを保護するために、役割ベースのアクセス制御機能が提供されます。

許可ポリシーを使用すると、以下の機能が得られます。

- ダッシュボード・ユーザーに対して、特定の管理対象システム・グループおよび個別の管理対象システムへのアクセスを制限する機能。
- ポリシー管理を簡素化するために、統合 LDAP ユーザー・レジストリー内のユーザーおよびユーザー・グループに役割ベースのポリシーを割り当てる機能。
- 高度な自動化が可能な新しいコマンド行インターフェース。
- ドメインとも呼ばれる IBM Tivoli Monitoring 環境が複数ある場合向けの、許可ポリシーの集中管理。

Tivoli Enterprise Portal 許可は、モニター・ダッシュボードでのリソースへのアクセスを制御するデフォルトの許可方式です。また、Tivoli Enterprise Portal クライアント・ユーザーを許可するために使用されるメカニズムでもあります。ただし、許可ポリシーの方がリソースへのアクセスに対して幅広い制御が可能です。許可ポリシーを使用すると、特定の管理対象システム・グループまたは管理対象システム内のデータを表示する許可をダッシュボード・ユーザーに付与できます。一方、 Tivoli Enterprise Portal 許可では、モニター・アプリケーション (モニター・エージェント) に対する表示許可が割り当てられます。つまり、Tivoli Enterprise Portal 許可では、特定のエージェント・アプリケーション・タイプ (例えば、すべての Windows OS エージェント) の管理対象システムをすべて表示する許可がユーザーに割り当てられます。

許可ポリシーによって提供される役割ベースのアクセス制御を使用する場合は、Tivoli 許可ポリシー・サーバーおよび許可ポリシーの tivcmd コマンド行インターフェースをインストールする必要があります。許可ポリシー・サーバー は、Infrastructure Management Dashboards for Servers などのモニター・ダッシュボード・アプリケーションやカスタムのダッシュボードと合わせて、 IBM Dashboard Application Services Hub とともにインストールされます。tivcmd CLI は、許可ポリシー管理者が使用するコンピューターにインストールされ、許可ポリシーの作成および処理のためのコマンド行インターフェースを提供します。この CLI は、マスター・ポリシー・ストアを維持する許可ポリシー・サーバーに HTTP または HTTPS 要求を送信します。インストールに関する情報は、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Authorization Policy Server および Authorization Policy コマンド行インターフェースのインストールおよび構成』を参照してください。

この 2 つのパッケージが正しくインストールされたら、必要に応じて tivcmd CLI コマンドを実行して役割の作成と処理、許可の付与、許可の除外、許可の取り消し、および役割に対するユーザーおよびユーザー・グループの割り当てを実行でき

るようになります。tivcmd CLI コマンドの完全なリストについては、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

許可ポリシーの初期セットが作成されたら、 Tivoli Enterprise Portal Server で許可ポリシーのチェックを有効にします。ポータル・サーバーは、定期的に許可ポリシーを許可ポリシー・サーバー・アプリケーションからダウンロードします。ダッシュボード・ユーザーがモニター・データを要求すると、IBM Dashboard Application Services Hub はその要求をポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントに転送します。ダッシュボード・データ・プロバイダーは、許可ポリシーを使用することにより、ユーザーがアクセスできるモニター対象リソースを決定します。

Dashboard Application Services Hub とポータル・サーバーの両方がダッシュボード・ユーザーを認識できる必要があるため、標準的なダッシュボード環境には LDAP サーバーによって提供される統合ユーザー・レジストリーおよびシングル・サインオンが含まれています。許可ポリシーを使用するダッシュボード環境の設定に関する一連のタスクについて詳しくは、 37 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ』を参照してください。

許可ポリシーの概念

許可ポリシーは、*リソース・タイプ* によって範囲が決定される*リソース* について、あるタイプの*オブジェクト* に対する*操作* を実行する許可をユーザー またはユーザー・グループ に対して付与または除外するものであり、 1 つまたは複数の*役割* を通じて機能します。

許可ポリシーの要素を以下に説明します。

ユーザー	操作を開始するユーザー。
ユーザー・グループ	操作を開始できるユーザーの集合。
役割	ユーザーまたはユーザー・グループに割り当てることができる許可の集合。
オペレーション	`create`、`delete`、`modify`、`distribute`、`view` などのアクション。
オブジェクト・タイプ	操作を実行する対象となるオブジェクトのカテゴリー。例えば、モニター・データ (`attributegroup`)、`event`、 `role` など。
リソース	管理対象システム・グループまたは管理対象システムなどの、実行される操作の対象となるエンティティー。
リソース・タイプ	リソースのカテゴリー。管理対象システム・グループ (`managedsystemgroup`)、管理対象システム (`managedsystem`)、および役割のセット (`rolegroup`) が、事前定義されているリソース・タイプです。

許可ポリシーを作成するには、以下のタスクを実行します。

1. アクセスを制御する対象となる管理対象システム・グループを作成します。管理対象システム・グループは、Tivoli Enterprise Portal クライアントと **`tacmd createsystemlist`** コマンドを使用して作成されます。

これらは、シチュエーションおよびヒストリカル収集を配布するために使用するものと同じ管理対象システム・グループにすることができます。

2. LDAP に、類似のジョブ機能を実行するユーザーを含むユーザー・グループを作成します。
3. 組織内でのジョブ機能を表す役割を作成します。

   例えば、東部地域のデータ・センターにいる Windows OS 管理者がアクセスできるモニター対象リソースについて、それを制御するために使用する `Eastern region Windows administrators` という役割を定義します。
4. 次に、役割に対して 1 つまたは複数の許可を付与または除外します。
   - *許可の付与* は、指定されたタイプの 1 つまたは複数のリソースについて、あるタイプのオブジェクトに対して実行できる操作を指定するものです。

     例えば、管理対象システム・グループ `EasternRegionWindowsComputers` について、モニター・データを表示する許可を付与できます。この際、操作は `view`、オブジェクト・タイプは `attributegroup` (モニター・データを表します)、リソースは `EasternRegionWindowsComputers`、リソース・タイプは `managedsystemgroup` です。
   - *許可の除外* では、管理対象システム・グループの 1 つまたは複数のメンバーに対するアクセスを制限できます。許可の除外は、ある役割で管理対象システム・グループの一部のメンバーにアクセスすることを禁止する場合に作成します。例えば、 `EasternRegionWindowsComputers` 管理対象システム・グループに、東部地域の Windows 管理者にアクセスさせたくないコンピューターが 2、3 台あるとします。この場合は、`EasternRegionWindowsComputers` 管理対象システム・グループに対する `view` 許可を付与し、特定の管理対象システムに対する `exclude` 許可を付与します。許可の除外では、ある管理対象システムのオブジェクトに対する任意の操作が実行できなくなります。
5. 最後のステップでは、1 つまたは複数のユーザーまたはユーザー・グループに役割を割り当てます。許可ポリシー役割に割り当てられたユーザーまたはユーザー・グループだけが、ダッシュボードでモニター対象リソースにアクセスできます。そのユーザー名およびユーザー・グループ名は、IBM Dashboard Application Services Hub とポータル・サーバーが共有する LDAP ユーザー・レジストリー内に定義されます。

また、役割から許可の付与または除外を削除する必要があると判断した場合は、役割の許可を取り消すこともできます。許可ポリシーは、どのユーザーが役割を作成および処理するかを制御するためにも使用されます。

次の表に、サポートされているリソース・タイプ、それに関連付けられているオブジェクト・タイプと操作、およびそのタイプのリソースに割り当てることができる許可のタイプをリストします。

表 16. 許可ポリシーのリソース・タイプと、サポートされている許可および要素

許可	オペレーション	オブジェクト・タイプ	リソース・タイプ	説明
grant	view	attributegroup	managedsystemgroup	この組み合わせを使用すると、管理対象システム・グループ内のすべての管理対象システムについて、メトリックやステータスといったモニター・データを表示する許可を付与できます。

表 16. 許可ポリシーのリソース・タイプと、サポートされている許可および要素 (続き)

許可	オペレーション	オブジェクト・タイプ	リソース・タイプ	説明
grant	view	event	managedsystemgroup	この組み合わせを使用すると、管理対象システム・グループ内のすべての管理対象システムのシチュエーション・イベントを表示する許可を付与できます。 **注:** シチュエーション・イベントをトリガーしたモニター・データを表示する許可を付与するには、管理対象システム・グループのモニター・データを表示する許可を付与する必要があります。
grant	view	attributegroup	managesystem	この組み合わせを使用すると、特定の管理対象システムについて、メトリックやステータスといったモニター・データを表示する許可を付与できます。
grant	view	event	managedsystem	この組み合わせを使用すると、特定の管理対象システムのシチュエーション・イベントを表示する許可を付与できます。 **注:** シチュエーション・イベントをトリガーしたモニター・データを表示する許可を付与するには、管理対象システム・グループのモニター・データを表示する許可を付与する必要があります。
exclude			managedsystem	この組み合わせを使用すると、特定の管理対象システムの任意の操作を実行する許可を除外できます。
grant	create	role	rolegroup	この組み合わせを使用すると、特定の管理対象システムで役割またはイベントを作成する許可を付与できます。
grant	delete	role	rolegroup	この組み合わせを使用すると、役割を削除する許可を付与できます。
grant	distribute	role	rolegroup	この組み合わせを使用すると、許可ポリシー・サーバーから Tivoli Enterprise Portal Server にポリシーを配布する許可を付与できます。
grant	modify	role	rolegroup	この組み合わせを使用すると、役割を変更する許可を付与できます。
grant	view	role	rolegroup	この組み合わせを使用すると、割り当てられている役割および許可を表示する許可を付与できます。この許可は、あるユーザーが自分の許可を表示することはできるが他のユーザーの許可は表示できないようにする場合に使用します。
grant	viewall	role	rolegroup	この組み合わせを使用すると、すべての役割および許可を表示する許可を付与できます。

管理対象システム・グループの属性グループ (モニター・データ) またはイベントを表示する許可を付与されると、グループを表示する許可が付与され、また、グループ・メンバーに関する許可の除外がない限り、グループのすべてのメンバーを表示する許可も付与されます。

IBM Tivoli Monitoring の大規模なデプロイメントでは、複数のモニター・ドメインが存在する場合があります。モニター・ドメイン は、特定のハブ・モニター・サーバーを中心とした、IBM Tivoli Monitoring コンポーネント (ポータル・サーバー、

モニター・サーバー、モニター・エージェント、Tivoli Data Warehouse など) の集合として定義されます。このようなタイプのデプロイメントでは、複数のモニター・ドメインに共通の許可ポリシーをいくつか用意し、それ以外に個々のドメインに固有の許可ポリシーを用意することが考えられます。許可を作成する際、tivcmd CLI では、許可ポリシーがすべてのドメインに適用されるか (デフォルトの動作) 個別のドメインに適用されるかを指定できます。

役割グループ とは、単一の許可ポリシー・サーバーを使用するすべての IBM Tivoli Monitoring ドメイン間で共有される役割の集合です。許可ポリシー・サーバーでサポートされるのは、`default` という名前の 1 つの役割グループだけです。これは、役割に対して操作を実行する許可を作成する際にリソース名として指定されます。

複数ドメインのデプロイメントのおける許可ポリシーの利用方法については、219 ページの『複数のドメインに関する作業』を参照してください。

事前定義の役割と権限

Tivoli 許可ポリシー・サーバー には、ユーザーが初めて製品を使用する際に役立つ事前定義の役割と権限があります。事前定義された役割は、*コア役割* とも呼ばれます。これらの役割は、変更、削除することはできませんが、コピーして新しい役割を作成することはできます。

以下の役割と権限が事前定義されています。

RoleAdministrator

すべての役割およびポリシーを管理する権限を持つ主要なセキュリティー管理者役割。

注: 許可ポリシー・サーバーのインストール時に、インストール・プログラムは IBM Dashboard Application Services Hub 管理ユーザーの ID とパスワードの入力を求めます。インストーラーは、ユーザー ID を RoleAdministrator 役割に割り当てます。他のユーザーが役割の作成や処理、および許可の割り当てができるようにするには、tivcmd CLI をインストールし、それを使用して、インストール時に指定された資格情報で許可ポリシー・サーバーにログインする必要があります。次に、tivcmd コマンドを使用して他のユーザーを RoleAdminisrator 役割またはカスタム役割に割り当てます。詳しくは、205 ページの『administrator 役割の作成および割り当て』を参照してください。

表 17. RoleAdministrator の権限

オペレーション	オブジェクト・タイプ	リソース・タイプ	リソース
ビュー (view)	attributegroup	managedsystemgroup	any
ビュー (view)	event	managedsystemgroup	any
ビュー (view)	attributegroup	managedsystem	any
ビュー (view)	event	managedsystem	any
create、 delete、 modify、 view、 viewall	role	rolegroup	デフォルト

PolicyDistributor
許可ポリシーをダウンロードする権限を備えた役割。

この役割、または同じ権限を持つカスタム役割を、ポータル・サーバーで許可ポリシーを有効にするときに指定するユーザー ID に割り当てる必要があります。ポータル・サーバーは、指定されたユーザー ID とその他の接続プロパティーを使用して定期的に許可ポリシー・サーバーに接続し、最新のポリシーをダウンロードします。許可ポリシー・サーバーは、許可ポリシーに対する要求を受け取ると、ポリシーを配布する権限がその要求を送信したユーザーに付与されていることを検証します。

表 18. PolicyDistributor の権限

オペレーション	オブジェクト・タイプ	リソース・タイプ	リソース
distribute	role	rolegroup	デフォルト

LinuxOperator
すべての Linux エージェントの属性グループおよびイベントを表示する権限を持つ役割。

UNIXOperator
すべての UNIX エージェントの属性グループおよびイベントを表示する権限を持つ役割。

WindowsOperator
すべての Windows エージェントの属性グループおよびイベントを表示する権限を持つ役割。

表 19. LinuxOperator、UNIXOperator、および WindowsOperator の権限

役割	オペレーション	オブジェクト・タイプ	リソース・タイプ	リソース
LinuxOperator	ビュー (view)	attributegroup および event	managedsystemgroup	*LINUX_SYSTEM
UNIXOperator	ビュー (view)	attributegroup および event	managedsystemgroup	*ALL_UNIX
WindowsOperator	ビュー (view)	attributegroup および event	managedsystemgroup	*NT_SYSTEM

VCenterOperator
すべての VMWARE Virtual Center および ESX Server へのアクセス権限を持つ役割。

表 20. VCenterOperator の権限

オペレーション	オブジェクト・タイプ	リソース・タイプ	リソース
ビュー (view)	attributegroup	managedsystemgroup	*VMWARE_VI_AGENT *VMWARE_VI
ビュー (view)	event	managedsystemgroup	*VMWARE_VI_AGENT *VMWARE_VI

許可ポリシーを有効にする準備

許可ポリシーを有効にする前に、このトピックに記載されている情報を読み、その内容に従って準備が完了していることを確認してください。

Tivoli Enterprise Portal Server をインストールした時点では、許可ポリシーの適用はデフォルトで無効になっています。Tivoli Enterprise Portal Server 構成パネルには、この機能を制御する「**許可ポリシーを有効にする**」チェック・ボックスがあります。このボックスのチェック・マークを外すと、ダッシュボード・データ・プロバイダーは、管理対象システム・グループおよび管理対象システムへのアクセスを制御するために、許可ポリシーを使用しません。代わりに Tivoli Enterprise Portal 許可を使用して、ダッシュボードでのモニター対象リソースへのアクセスを制御します。

許可ポリシーの適用を有効にする前に、以下のステップを実行します。

1. 許可ポリシーの管理を行う必要があるユーザーを識別します。

   許可ポリシー・サーバーのインストール時に、インストール・プログラムは IBM Dashboard Application Services Hub 管理ユーザーの ID とパスワードの入力を求めます。インストーラーは、ユーザー ID を事前定義された RoleAdministrator 役割に割り当てます。他のユーザーが役割の作成や処理、および許可の割り当てができるようにするには、tivcmd CLI をインストールし、それを使用して、インストール時に指定された資格情報で許可ポリシー・サーバーにログインする必要があります。次に、tivcmd コマンドを使用して他のポリシー管理者を事前定義されている RoleAdministrator 役割に追加するか、同様の許可を備えた同等の役割を作成し、その役割にポリシー管理者を追加します。詳しいステップについては、205 ページの『administrator 役割の作成および割り当て』を参照してください。

   tivcmd CLI のインストールについて詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Authorization Policy Server および Authorization Policy コマンド行インターフェースのインストールおよび構成』を参照してください。
2. 事前定義された PolicyDistributor 役割など、ポリシーを配布する許可を持っている役割に、少なくとも 1 人のユーザーを割り当てます。

   ポータル・サーバーを再構成する準備ができたら、許可ポリシーを有効にするために同じユーザーを Tivoli Enterprise Portal Server 構成パネルで指定する必要があります。

   ダッシュボード・データ・プロバイダーが許可ポリシー・サーバーからポリシーの更新を取得する権限を持てるように、ユーザーにポリシーを配布する許可を割り当てる必要があります。詳しいステップについては、206 ページの『ポリシー・ディストリビューターの役割の作成および割り当て』を参照してください。
3. ダッシュボード・ビューに表示できる既存のすべての管理対象システム・グループおよび管理対象システムに対し、役割と権限を作成します (または、事前定義の役割と権限を利用します)。次に、ユーザーまたはユーザー・グループをそれらの役割に追加します。詳細な例については、207 ページの『ポリシー管理の例』を参照してください。

注: 事前定義の役割と権限のセットは、一部のセキュリティー・ニーズ、およびおそらくは大半のセキュリティー・ニーズを簡単に満たすために用意されています。ただし、ご使用の環境内に、独自のポリシー定義を必要とする追加の管理対象システム・グループおよび管理対象システムが存在する可能性があります。『ポリシー管理のシナリオ』の情報は、tivcmd CLI を使用してこれらの追加ポリシーを作成する方法をより詳しく理解するために役立ちます。

4. ダッシュボード・データ・プロバイダーが許可ポリシーを許可ポリシー・サーバーから取得する頻度を決定します。

   ダッシュボード・データ・プロバイダーは、ネットワーク内で時間のかかるアクセスを行わずに済むよう、許可ポリシー・サーバーのマスター・ポリシー・ストアの独自のローカル・コピーを取得します。ポリシーの取得はダッシュボード・データ・プロバイダーの始動時に 1 回行われ、その後は一定の間隔 (デフォルトでは 30 分) で繰り返されます。デフォルトは、許可ポリシーを有効にするときに Tivoli Enterprise Portal Server 構成パネルから変更できます。指定できる値は、5 から 1440 分です。tivcmd CLI を使用して行われたポリシー変更は、次回、ポリシー・ストアを正常に取得するまで、ダッシュボード・データ・プロバイダーで有効にならない点に注意してください。

許可ポリシーの使用を開始する準備ができたら、許可ポリシーを有効にし、許可ポリシー・サーバーの接続プロパティーを指定するように、ポータル・サーバーを再構成します。接続プロパティーには、ポリシーを配布する許可を持つ役割を割り当てられたユーザー ID が含まれます。

許可ポリシーを有効にする前に実行するタスクのリストについては、 37 ページの『シングル・サインオンおよびユーザーごとの許可による制御を使用するモニター・ダッシュボード環境のセットアップ』を参照してください。

ポリシー管理のシナリオ

Tivoli 許可ポリシー・サーバーでは、ある役割に汎用的な権限を与えることにより、あるユーザーがすべてにアクセスできるようにすることはできません。役割には、特定の管理対象システム・グループまたは管理対象システムに対する明示的なアクセス権限を付与する必要があります。また、ダッシュボードのユーザーは、管理対象システム・グループまたは管理対象システムに対するアクセス権限がある役割に割り当てられている場合にだけ、モニター・ダッシュボードでリソースを表示できます。

許可ポリシーを作成する際のベスト・プラクティス

ユーザーの環境で許可ポリシーを作成する際のベスト・プラクティスを検討します。

- 許可の付与は、個別の管理対象システムではなく管理対象システムのグループに対して行います。

  この方法は、環境に管理対象システムが追加されたときに許可ポリシーの更新が不要であるという利点があります。許可ポリシーを更新する代わりに、既に表示許可が付与されている管理対象システム・グループ、および含まれるシステムが使用するシチュエーション定義およびヒストリカル収集定義のセットが類似して

いる管理対象システム・グループに、新しい管理対象システムを追加します。新しい管理対象システムに関しては、新しい許可ポリシーを作成する必要があるのは以下のような状況だけです。

- 管理対象システムを追加できる既存の管理対象システム・グループがない場合。この場合は、新しい管理対象システムを含む新しい新しい管理対象システム・グループを追加します。 その後、管理対象システム・グループの表示許可を 1 つまたは複数の役割に付与します。
- 新しい管理対象システムを含む管理対象システム・グループの表示許可を付与されたユーザーが管理対象システムにアクセスできないようにする必要があるため、この管理対象システムの許可の除外を作成する場合。

- 個別のユーザーを役割に割り当てるのではなく、ユーザー・グループを役割に割り当てます。

  この方法を採用した場合は、新しいダッシュボード・ユーザーを追加するときに許可ポリシーの更新が不要です。許可ポリシーを更新する代わりに、新しいユーザーのジョブ機能に一致する許可ポリシー役割に既に割り当てられている LDAP 内のユーザー・グループに、この新しいユーザーを追加します。

  新しいユーザーを追加できる既存のユーザー・グループがない場合は、このユーザー用の新しい許可ポリシーを作成します。この場合は、LDAP 内に新しいユーザー・グループを追加し、新しいユーザーをグループに追加してから、そのグループを 1 つまたは複数の許可ポリシー役割に割り当てます。必要であれば、新しいユーザー・グループの許可範囲に一致する新しい役割を作成します。
- 許可ポリシー管理者用に LDAP 内にユーザー・グループを作成し、役割の作成、変更、削除、および表示の許可が付与されている役割にそのユーザー・グループを割り当てます。事前定義されている RoleAdministrator 役割には、これらの許可があります。また、許可の更新を複数のユーザーが実行できるように、複数のユーザーがユーザー・グループのメンバーになるようにしてください。
- ダッシュボード・ユーザーがモニター・データ、およびリソースのシチュエーション・イベントを表示できるようにするには、モニター・データ (属性グループ) の表示許可が付与された役割と、作業するリソースのシチュエーション・イベントの表示許可が付与された役割を作成します。

  アクセスを制限する必要があるユーザーに対しては、イベントを表示する許可は付与してもモニター・データを表示する許可は付与しない、またはその逆にします。

  属性グループおよびイベントを表示する許可をユーザー・グループ (またはユーザー)に付与するときは、同じリソース・タイプ(管理対象システム・グループまたは管理対象システム) に対して両方のオブジェクト・タイプの表示許可を付与します。

  - ベスト・プラクティス例: 管理対象システム・グループのリソースについてイベントおよび属性グループを表示する許可を付与する。

    ```
    tivcmd grant --rolename "West Coast Administrators" --resourcetype
    managedsystemgroup --resources "West_Coast_Systems" --objecttype
    attributegroup --operations view
    ```

```
tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_Systems" --objecttype event
--operations view
```

– ベスト・プラクティスの変化形: イベントおよび属性グループを表示する許可を管理対象システムに付与する。

```
tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystem --resources "Primary:server1:NT" --objecttype
attributegroup --operations view

tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystem --resources "Primary:server1:NT" --objecttype event
--operations view
```

– ベスト・プラクティスの基準に準拠しないポリシーの例:

```
tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_Systems" --objecttype
attributegroup --operations view

tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystem --resources "Primary:server1:NT" --objecttype event
--operations view
```

ここで、Primary:server1:NT は West_Coast_Systems 管理対象システム・グループのメンバーです。

– ベスト・プラクティスの基準に準拠しないポリシーの例:

```
tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystem --resources "Primary:server1:NT" --objecttype
attributegroup --operations view

tivcmd grant --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_Systems" --objecttype event
--operations view
```

ここで、Primary:server1:NT は West_Coast_Systems 管理対象システム・グループのメンバーです。

- Infrastructure Management Dashboards for Servers アプリケーションに固有の追加的ベスト・プラクティスおよび考慮事項:
  – ダッシュボード・ユーザーが「**管理対象システム・グループ**」ページを使用できるようにするには、管理対象システム・グループのイベントまたは属性グループ、またはその両方を表示する許可のある役割をユーザーに割り当てる必要があります。ユーザーが割り当てられた役割が 1 つまたは複数の管理対象システムに関する表示許可しか持っていない場合、「**管理対象システム・グループ**」ページにモニター対象リソースはいっさい表示されません。
  – ダッシュボード・ユーザーが「**シチュエーション・イベント**」ページを使用できるようにするには、管理対象システム・グループ (ベスト・プラクティス) または個別の管理対象システムのイベントを表示する許可のある役割をユーザーに割り当てる必要があります。シチュエーション・イベントがオープンになる原因となったモニター・データをユーザーが表示できるようにするには、管理対象システム・グループ (ベスト・プラクティス) または個別の管理対象システムの属性グループを表示する許可のある役割にもユーザーを割り当てる必要があります。

administrator 役割の作成および割り当て

許可ポリシー・サーバーをインストールすると、事前定義された RoleAdministrators 役割に Dashboard Application Services Hub 管理ユーザーが割り当てられます。通常、これは tipadmin です。事前定義の RoleAdministrator 役割に独自の管理ユーザーを追加することも、同じ権限を持つ独自のカスタム役割を作成することもできます。

ベスト・プラクティスは、ポリシー管理者向けに LDAP 内にユーザー・グループを作成し、許可ポリシーの作成および処理の権限を持つ役割にそのユーザー・グループを割り当てます。この方法を使用すると、ポリシー管理者を追加または削除するときに、グループのメンバーシップを更新するだけで済みます (許可ポリシーを更新する必要はありません)。

このタスクについて

役割管理に使用される役割には、以下の権限が必要です。

役割管理権限の定義	
パラメーター	**値**
オペレーション	「create」、 「delete」、 「modify」、 「view」、 「viewall」
オブジェクト・タイプ	「role」
リソース・タイプ	「rolegroup」
リソース	「default」

手順

- 事前定義の RoleAdministrator 役割にユーザーまたはユーザー・グループを割り当てるには、次の手順を実行します。
  1. LDAP で、`uid=JohnDoe,cn=itm,o=ibm` のようにしてユーザーを定義するか、`cn=Administrators,cn=itm,o=ibm` のようにしてユーザー・グループを定義します。次に、`uid=JohnDoe,cn=itm,o=ibm` のようにしてポリシー管理者のユーザー ID を LDAP 内のグループに追加します。
  2. 以下のコマンドを使用して、ユーザー・グループを事前定義の RoleAdministrator 役割に追加します。

     ```
     tivcmd addtorole --rolename RoleAdministrator
     --groups gid=Administrators,cn=itm,o=ibm
     ```

  3. または、以下のコマンドを使用して、ユーザーを事前定義の RoleAdministrator 役割に追加します。

     ```
     tivcmd addtorole --rolename RoleAdministrator
     --users uid=JohnDoe,cn=itm,o=ibm
     ```

- RoleAdministrator 役割と同じ権限を持つ新規役割を作成するには、次の手順を実行します。
  1. LDAP でユーザー (例えば、`uid=JohnDoe,cn=itm,o=ibm`) を定義するか、LDAP でグループ (例えば、`cn=Administrators,cn=itm,o=ibm`) を定義してから、LDAP でポリシー管理者のユーザー ID をグループに追加します。

2. 新しい役割を作成し、許可ポリシーを作成および処理する権限をその新しい役割に追加します。次に、ユーザーまたはユーザー・グループをその新しい役割に割り当てます。次の例のコマンドでは、ポリシー管理のためのカスタム役割にユーザーおよびグループを追加しています。

```
tivcmd createrole --rolename EastCoastAdministrators --description
"East Coast users with permission to manage roles and policies"

tivcmd grant --rolename EastCoastAdministrators --resourcetype rolegroup
--resources default --objecttype role --operations create delete modify
view viewall

tivcmd addtorole --rolename EastCoastAdministrators
 --users uid=JohnDoe,cn=itm,o=ibm
 --groups cn=Administrators,cn=itm,o=ibm
```

3. または、既存の RoleAdministrator 役割を複製し、以下のコマンドによって新しい役割をユーザー・グループに割り当てることもできます。

```
tivcmd copyrole --fromrolename RoleAdministrator --torolename
EastCoastAdministrators --description "East Coast users allowed to
administer roles and policies for this authorization policy server"
--permissionsonly

tivcmd addtorole --rolename EastCoastAdministrators
 --groups cn=Administrators,cn=itm,o=ibm
```

ポリシー・ディストリビューターの役割の作成および割り当て

新しいダッシュボード環境を設定する際は、ダッシュボード・ユーザーおよびポリシー管理者ごとに LDAP ユーザー・レジストリーにユーザー ID を作成する必要があります。また、ポリシーを配布する権限を付与されているユーザー ID が必要です。このユーザー ID は、ポータル・サーバーで許可ポリシーを有効にするときに指定する必要があります。ポータル・サーバーでは、最新の許可ポリシーをダウンロードするために許可ポリシー・サーバーに送信する要求の中にこのユーザー ID を含めます。許可ポリシー・サーバーは、ユーザーがポリシーを取得する権限を持っていることを検証します。IBM Tivoli Monitoring には、この権限を持つ事前定義の PolicyDistributor 役割が既に用意されています。管理者は、この権限を持つ新規役割を作成することも、事前定義の役割を使用することもできます。

このタスクについて

ポリシー配布に使用される役割には、以下の権限が必要です。

ポリシー配布権限の定義	
パラメーター	**値**
オペレーション	「distribute」
オブジェクト・タイプ	「role」
リソース・タイプ	「rolegroup」
リソース	「default」

手順

- 事前定義の PolicyDistributor 役割にユーザーを割り当てるには、次の手順を実行します。
  1. LDAP でユーザー (例えば、uid=PolicyAdmin,cn=itm,o=ibm) を定義します。

2. 以下のコマンドを使用して、ユーザーを事前定義の PolicyDistributor 役割に追加します。

```
tivcmd addtorole --rolename PolicyDistributor
  --users uid=PolicyAdmin,cn=itm,o=ibm
```

- PolicyDistributor 役割と同じ権限を持つ新規役割を作成するには、次の手順を実行します。
  1. LDAP でユーザー (例えば、uid=PolicyAdmin,cn=itm,o=ibm) を定義します。
  2. 以下のコマンドを使用して、ポリシー配布権限を持つ新しい役割を作成し、ユーザーに割り当てます。

```
tivcmd createrole --rolename EastCoastDistributor --description
"East Coast user IDs for downloading policy"

tivcmd grant --rolename EastCoastDistributor --resourcetype rolegroup
--resources default --objecttype role --operations distribute

tivcmd addtorole --rolename EastCoastDistributor
--users uid=PolicyAdmin,cn=itm,o=ibm
```

  3. または、以下のコマンドを使用して、既存の PolicyDistributor 役割を複製します。

```
tivcmd copyrole --fromrolename PolicyDistributor --torolename
EastCoastDistributor --description "East Coast user IDs to
download policy" --permissionsonly

tivcmd addtorole --rolename EastCoastDistributor
  --users uid=PolicyAdmin,cn=itm,o=ibm
```

ポリシー管理の例

許可ポリシーの目的は、モニター対象リソースを細かく制御できるようにすることです。新しいダッシュボード環境を設定する際は、LDAP ユーザー・リポジトリーにダッシュボード・ユーザー ID を作成する必要があります。ベスト・プラクティスでは、LDAP グループも設定し、許可ポリシーの役割に割り当てるユーザーの集合をそこに含めます。これにより、個別のユーザー ID を役割に割り当てるよりもポリシー管理が簡単になります。ポリシーについての作業を開始するには、このトピックの例を参照してください。

ポリシーを管理するには、許可ポリシーの tivcmd コマンド行インターフェース・コマンドを使用します。これらのコマンドについて詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

この例では、West Coast Administrators という既存の役割があり、この役割に対し、West_Coast_DataCenter_Systems という管理対象システム・グループと West_Coast_Regional_Systems というもう 1 つの管理対象システム・グループのすべての属性グループ・データおよびイベントを表示する権限を付与して、この役割を cn=westcoastadmins,cn=itm,o=ibm というユーザー・グループに割り当てることを想定しています。

```
tivcmd grant --rolename "West Coast Administrators"
--resourcetype  managedsystemgroup --resources
"West_Coast_DataCenter_Systems"
--objecttype attributegroup --operations view

tivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources
"West_Coast_DataCenter_Systems"
```

```
--objecttype event  --operations view

tivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources "West_Coast_Regional_Systems"
--objecttype attributegroup --operations view

tivcmd grant --rolename "West Coast Administrators"
--resourcetype managedsystemgroup --resources "West_Coast_Regional_Systems"
--objecttype event  --operations view

tivcmd addtorole --rolename "West Coast Administrators"
--groups cn=westcoastadmins,cn=itm,o=ibm
```

この例では、cn=westcoastadmins,cn=itm,o=ibm ユーザー・グループのメンバーが Primary:server1:NT 管理対象システムの属性グループ・データおよびイベントを表示できないようにすることを想定しています。このシナリオでは、Primary:server1:NT は、前の例でユーザー・グループに表示許可が付与されていた West_Coast_DataCenter_Systems 管理対象システム・グループのメンバーです。

```
tivcmd exclude --rolename "West Coast Administrators" --resourcetype
managedsystem --resources Primary:server1:NT
```

この例では、West_Coast_DataCenter_Systems 管理対象システム・グループの属性グループ・データおよびイベントを表示する許可の付与を削除し、Primary:server1:NT 管理対象システムに関する許可の除外を West Coast Administrators 役割から削除するが、West_Coast_Regional_Systems 管理対象システム・グループに関する許可の付与は残すことを想定しています。

```
tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_DataCenter_Systems"
--objecttype attributegroup --operations view  --grantcommand

tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystemgroup --resources "West_Coast_DataCenter_Systems"
--objecttype event  --operations view --grantcommand

tivcmd revoke --rolename "West Coast Administrators" --resourcetype
managedsystem --resources Primary:server1:NT  --excludecommand
```

この例では、IBM Tivoli Monitoring 管理者として、Eastern、Central、Western という 3 つの地域に属する管理対象システムに対するダッシュボード・アクセスを制御します。モニター・サーバーには、それぞれの地域の管理対象システムを含む EasternRegionSystems、 CentralRegionSystems、および WesternRegionSystems の管理対象システム・グループ定義があります。管理者は 3 つの地域すべての管理対象システムにアクセスする必要がありますが、 Annette というオペレーターは Western 地域のシステムにのみアクセスできるようにします。この例では、ローカル LDAP ユーザー・レジストリーに EasternRegionOperators、CentralRegionOperators、WesternRegionOperators というユーザー・グループが含まれ、Annette は WesternRegionOperators グループのメンバーであることを想定しています。

1. 許可ポリシー・サーバー にログインします。

   ```
   tivcmd login --username <user> --password <password>
   ```

2. 3 つの地域それぞれに 1 つずつ新しい役割を作成します。

   ```
   tivcmd createrole --rolename EasternRegionOperator --description
   "A role to govern access to data for Eastern Region Systems"

   tivcmd createrole --rolename CentralRegionOperator --description
   ```

```
"A role to govern access to data for Central Region Systems"

tivcmd createrole --rolename WesternRegionOperator --description
"A role to govern access to data for Western Region Systems"
```

3. 新しい役割が作成されたことを確認します。

```
tivcmd listroles --rolename EasternRegionOperator --showdescription

tivcmd listroles --rolename CentralRegionOperator --showdescription

tivcmd listroles --rolename WesternRegionOperator --showdescription
```

4. **tivcmd grant** コマンドの使用法を表示します。

```
tivcmd grant -?
```

5. EasternRegionOperator 役割が EasternRegionSystems の属性データおよびイベントを表示するアクセス権限を持つことを許可する、権限付与コマンドを実行します。

```
tivcmd grant --rolename EasternRegionOperator --resourcetype managedsystemgroup
--resources EasternRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename EasternRegionOperator --resourcetype managedsystemgroup
--resources EasternRegionSystems --objecttype event --operations view
```

6. EasternRegionOperator 役割に正しい許可があることを確認します。

```
tivcmd listroles --rolename EasternRegionOperator --showpermissions
```

7. コマンドを繰り返して、他の 2 つの役割にそれぞれの地域に対する同じ許可を付与します。

```
tivcmd grant --rolename CentralRegionOperator --resourcetype managedsystemgroup
--resources CentralRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename CentralRegionOperator --resourcetype managedsystemgroup
--resources CentralRegionSystems --objecttype event --operations view

tivcmd grant --rolename WesternRegionOperator --resourcetype managedsystemgroup
--resources WesternRegionSystems --objecttype attributegroup --operations view

tivcmd grant --rolename WesternRegionOperator --resourcetype managedsystemgroup
--resources WesternRegionSystems --objecttype event --operations view
```

8. **tivcmd addtorole** コマンドの使用法を表示します。

```
tivcmd addtorole -?
```

9. 各 LDAP ユーザー・グループを、それぞれの対応する役割に関連付けます。

```
tivcmd addtorole --rolename EasternRegionOperator --groups
cn=EasternRegionOperators,cn=itm,o=tivoli

tivcmd addtorole --rolename CentralRegionOperator --groups
cn=CentralRegionOperators,cn=itm,o=tivoli

tivcmd addtorole --rolename WesternRegionOperator --groups
cn=WesternRegionOperators,cn=itm,o=tivoli
```

10. 各役割のメンバーを表示して、ユーザー・グループの関連付けが適切に完了したことを確認します。

```
tivcmd listroles --rolename EasternRegionOperator --showmembership

tivcmd listroles --rolename CentralRegionOperator --showmembership

tivcmd listroles --rolename WesternRegionOperator --showmembership
```

11. 必ず 3 つの地域すべてのシステムに対して管理者のアクセス権限を設定します。それには、管理者のユーザー ID を 3 つの新しい役割それぞれに追加します。

```
tivcmd addtorole --rolename EasternRegionOperator --users
uid=<userid>,cn=itm,o=tivoli

tivcmd addtorole --rolename CentralRegionOperator --users
uid=<userid>,cn=itm,o=tivoli

tivcmd addtorole --rolename WesternRegionOperator --users
uid=<userid>,cn=itm,o=tivoli
```

12. 管理者のユーザー ID を事前定義された PolicyDistributor 役割に追加します。このコマンドにより、管理者の ID をダッシュボード・データ・プロバイダーが使用して許可ポリシー・サーバーからポリシー・ファイル・ストアの更新をダウンロードできるようになります。

```
tivcmd addtorole --rolename PolicyDistributor
--users uid=<userid>,cn=itm,o=tivoli
```

13. 管理者のユーザー ID が含まれているすべての役割を表示します。

```
tivcmd listroles --username uid=<userid>,cn=itm,o=tivoli
```

セキュリティー・セットアップはこれで完了です。

- Annette がメンバーとなっているのは、`WesternRegionOperators` ユーザー・グループのみです。
- `WesternRegionOperators` ユーザー・グループは、`WesternRegionOperator` 役割にのみ割り当てられています。
- `WesternRegionOperator` 役割は、`WesternRegionSystems` 管理対象システム・グループへのアクセス権限のみを付与されています。
- Annette は、`WesternRegionSystems` に属している管理対象システムの属性データおよびイベントのみを表示できます。

ポータル・サーバーでの許可ポリシーの使用可能化

許可ポリシーの初期セットを作成し、ポリシーを配布する許可を備えた役割にユーザーを割り当てたら、 Tivoli Enterprise Monitoring Services の管理 またはコマンド行を使用して Tivoli Enterprise Portal Server を構成することによって、ダッシュボード・データ・プロバイダーで許可ポリシーの適用を有効にします。

手順

- Tivoli Enterprise Monitoring Services の管理 の使用
  1. ポータル・サーバーがインストールされているコンピューターで、Tivoli Enterprise Monitoring Services の管理 を始動します。

     Windows **「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」**をクリックします。

     Linux UNIX *install_dir* が IBM Tivoli Monitoring のインストール・ディレクトリーの場合、*install_dir* `/bin` ディレクトリーに移動して、`./itmcmd manage [-h` *install_dir* `]` を実行します。
  2. **Tivoli Enterprise Portal Server** を右クリックして、以下のようにします。

Windows 「**再構成**」をクリックして、既存の構成を受け入れるために「**OK**」をクリックし、2 番目の「TEP サーバー構成」ウィンドウに進みます。

Linux UNIX 「**構成**」をクリックします。「共通イベント・コンソール構成」ウィンドウが表示されます。「**OK**」をクリックして、現行値を受け入れます。「Tivoli Enterprise Portal の構成」ウィンドウで、「**ダッシュボード・データ・プロバイダー**」タブを選択します。

3. 構成ウィンドウのダッシュボード・データ・プロバイダー領域で、「**許可ポリシーを有効にする**」チェック・ボックスが選択されていることを確認します。選択されていない場合は、選択します。
   a. ダッシュボード・データ・プロバイダーを有効にすると、ドメイン・オーバーライド値を指定できるようになります。この値は任意指定です。これにより、許可ポリシーのデフォルトのダッシュボード・データ・プロバイダー ID およびドメイン名が `itm.<hub_monitoring_server_name>` から `itm.<domain_override_value>` に変更されます。値は 124 文字を超えてはなりません。ドメイン・オーバーライド値は、以下のシナリオに合わせて構成する必要があります。
      – ハブ・モニター・サーバー用にホット・スタンバイ高可用性機能が使用されている場合。ドメイン・オーバーライド値を構成しておくと、ポータル・サーバーが新規のアクティブ・ハブ・モニター・サーバーに接続するように構成されても、ダッシュボード・データ・プロバイダー ID およびドメイン名は変更されません。このシナリオでドメイン・オーバーライド値を構成しない場合、新しいアクティブ・ハブ・モニター・サーバーに接続するようにポータル・サーバーが構成されたときは、IBM Dashboard Application Services Hub とダッシュボード・データ・プロバイダーの間の接続を再構成し、ドメイン固有の許可ポリシーがあれば、それらをすべて更新する必要があります。
      – ダッシュボードのアクセスを制御するために共通の許可ポリシーのセットを使用している複数のハブ・モニター・サーバーがあり、ドメイン固有の許可ポリシーをいくつか作成する場合。このシナリオで、デフォルト値の `itm.<hub_monitoring_server_name>` よりもユーザーに分かりやすいドメイン名を許可ポリシー内で使用するには、ドメイン・オーバーライド値を指定する必要があります。

      Dashboard Application Services Hub でダッシュボード・データ・プロバイダーに対する接続を構成した後でドメイン・オーバーライドを変更した場合は、接続を削除してから再度追加する必要があります。ダッシュボード・データ・プロバイダー接続の構成方法について詳しくは、 60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』を参照してください。また、デフォルトのドメイン名を使用して作成したドメイン固有の許可ポリシーがある場合、ドメイン・オーバーライド値の変更時には、以前のドメイン名を使用している許可を削除し、新しいドメイン名を使用する新しい許可を作成する必要があります。
   b. ユーザーがモニタリング・ダッシュボードでアクセスできる管理対象システムおよび管理対象システム・グループを、許可ポリシーを使用して制御する場合は、「**許可ポリシーを有効にする**」オプションを選択します。許可ポリシーを有効にするのは、シングル・サインオンでダッシュボード環

境を設定している場合、許可ポリシーを使用してモニター・ダッシュボードへのアクセスを制御する予定の場合、およびダッシュボード・ユーザー・アクセスに関するポリシーの初期セットを管理者が既に作成してある場合に限定してください。

4. 「許可ポリシー・サーバー構成」ウィンドウで、以下の情報を指定します。

表 21. 許可ポリシー・サーバーの構成情報

フィールド	説明
ホスト名または IP アドレス	許可ポリシー・サーバーを含む IBM Dashboard Application Services Hub の IP アドレスまたは完全修飾ホスト名。 このパラメーターは必須です。
プロトコル	許可ポリシー・サーバーを含む IBM Dashboard Application Services Hub への接続に使用されるプロトコルを選択します。デフォルト値は HTTPS です。 このパラメーターは必須ではありません。 **注:** HTTPS は、既にポータル・サーバーと許可ポリシー・サーバーの間で TLS/SSL を構成している場合にのみ選択してください。詳しくは、235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』を参照してください。
ポート	許可ポリシー・サーバーを含む IBM Dashboard Application Services Hub への接続に使用されるポートを選択します。デフォルト値は、HTTPS プロトコルでは 16311、HTTP プロトコルでは 16310 です。ポートの有効な値は 1 から 65535 です。 このパラメーターは必須ではありません。
ポーリング間隔	ローカル・データ・ストアがポータル・サーバー上で実行中のポリシー・クライアントによって許可ポリシー・サーバーから更新される間隔。デフォルトは 30 分です。有効な値は 5 から 1440 です。 このパラメーターは必須ではありません。
ポリシー・ストアの有効期限インターバル	ポリシー・ストアを許可ポリシー・サーバーから更新できない場合、前回の更新からこの間隔の期間、ローカル・ポリシー・ストアが引き続き使用されます。このパラメーターによって指定された時間の間に許可ポリシー・サーバーにアクセスできない場合、ダッシュボード・データに対するその後のすべての要求は、許可ポリシー・サーバーが再び使用可能になるまで許可エラーで失敗します。デフォルトは 7 日 0 時間です。時間に対して指定する値は、0 から 23 時間でなければなりません。有効期限インターバルが 0 日 0 時間に設定されていると、ポリシー・ストアの有効期限は切れません。 このパラメーターは必須ではありません。
ユーザー ID	ポータル・サーバーが許可ポリシー・サーバーを含む IBM Dashboard Application Services Hub へのアクセスに使用するユーザーの名前。このユーザーは、PolicyDistributor 許可ポリシーのコア役割、または役割オブジェクト・タイプの配布操作を実行する許可を付与されたカスタム役割に追加する必要があります。 このパラメーターは必須です。

表 21. 許可ポリシー・サーバーの構成情報 (続き)

フィールド	説明
パスワード	ユーザーに対するパスワード。 このパラメーターは必須です。
パスワードの確認	確認のためにパスワードを再度入力します。 このパラメーターは必須です。

表示されているフィールドに許可ポリシー・サーバー接続パラメーターに関する必須の情報を入力し、「**OK**」をクリックします。

5. ウェアハウス接続情報の再構成を求めるプロンプトが出たら、「**いいえ**」と応答します。
6. Windows では、構成設定の処理がしばらくの間実行されてから、「共通イベント・コンソール構成」ウィンドウが表示されます。このウィンドウは、前景表示されずに他のウィンドウにより隠される場合があります。処理に時間がかかりすぎている場合は、他のウィンドウを最小化し、構成ウィンドウを探してください。「共通イベント・コンソール構成」ウィンドウが表示されたら、「**OK**」をクリックします。
7. 構成を変更した場合は、必ずポータル・サーバーを再始動してください。

- コマンド行を使用する場合:

  Tivoli Enterprise Portal Server が Linux または UNIX 上にある場合は、コマンド行からポータル・サーバーの構成を変更し、許可ポリシーが有効になっていなければ有効にすることができます。

  1. Tivoli Enterprise Portal Server がインストールされているコンピューターにログオンします。
  2. コマンド行で、*install_dir* /bin ディレクトリーに移動します。ここで、*install_dir* はこの製品をインストールしたディレクトリーです。
  3. 次のコマンドを実行して Tivoli Enterprise Portal Server を構成します:
     ./itmcmd config -A cq

     「エージェント構成が開始しました...」というメッセージが表示され、その後に以下のプロンプトが表示されます: Tivoli Enterprise Portal Server は構成中に停止されます。続行しますか? [1= はい、 2= いいえ] (デフォルトは 2)。
  4. 「1」と入力します。以下のプロンプトが表示されます: 「IBM Tivoli Monitoring 用の共通イベント・コンソール」設定を編集しますか? [1= はい、2= いいえ] (デフォルトは 1)。
  5. 「2」を入力します。以下のプロンプトが表示されます。このエージェントは TEMS に接続しますか? [1= はい、2= いいえ] (デフォルトは 1)。
  6. ダッシュボード・データ・プロバイダーの構成に関するプロンプトが表示されるまで、このプロンプトおよび後続のプロンプトに対して、デフォルト値を受け入れます。これが有効になっていない場合は、値「1」を選択して有効にします。
  7. 次に、ドメイン・オーバーライド値を指定するかどうか尋ねられます。指定する場合は「1」、しない場合は「2」を入力します。

ダッシュボード・データ・プロバイダーを有効にすると、ドメイン・オーバーライド値を指定できるようになります。この値は任意指定です。これにより、許可ポリシーのデフォルトのダッシュボード・データ・プロバイダー ID およびドメイン名が itm.*<hub_monitoring_server_name>* から itm.*<domain_override_value>* に変更されます。値は 124 文字を超えてはなりません。ドメイン・オーバーライド値は、以下のシナリオに合わせて構成する必要があります。

- ハブ・モニター・サーバー用にホット・スタンバイ高可用性機能が使用されている場合。ドメイン・オーバーライド値を構成しておくと、ポータル・サーバーが新規のアクティブ・ハブ・モニター・サーバーに接続するように構成されても、ダッシュボード・データ・プロバイダー ID およびドメイン名は変更されません。このシナリオでドメイン・オーバーライド値を構成しない場合、新しいアクティブ・ハブ・モニター・サーバーに接続するようにポータル・サーバーが構成されたときは、IBM Dashboard Application Services Hub とダッシュボード・データ・プロバイダーの間の接続を再構成し、ドメイン固有の許可ポリシーがあれば、それらをすべて更新する必要があります。
- ダッシュボードのアクセスを制御するために共通の許可ポリシーのセットを使用している複数のハブ・モニター・サーバーがあり、ドメイン固有の許可ポリシーをいくつか作成する場合。このシナリオで、デフォルト値の itm.*<hub_monitoring_server_name>* よりもユーザーに分かりやすいドメイン名を許可ポリシー内で使用するには、ドメイン・オーバーライド値を指定する必要があります。

Dashboard Application Services Hub でダッシュボード・データ・プロバイダーに対する接続を構成した後でドメイン・オーバーライドを変更した場合は、接続を削除してから再度追加する必要があります。ダッシュボード・データ・プロバイダー接続の構成方法について詳しくは、 60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』を参照してください。また、デフォルトのドメイン名を使用して作成したドメイン固有の許可ポリシーがある場合、ドメイン・オーバーライド値の変更時には、以前のドメイン名を使用している許可を削除し、新しいドメイン名を使用する新しい許可を作成する必要があります。

8. ダッシュボード・データ・プロバイダーが有効になっている場合は、許可ポリシーを有効にするかどうかを尋ねられます。 212 ページの表 21 の情報を使用します。

   許可ポリシーを有効にするのは、シングル・サインオンでダッシュボード環境を設定している場合、許可ポリシーを使用してモニター・ダッシュボードへのアクセスを制御する予定の場合、およびダッシュボード・ユーザー・アクセスに関するポリシーの初期セットを管理者が既に作成してある場合に限定してください。
9. コマンドによって構成が完了すると、「エージェント構成が完了しました...」というメッセージが表示され、ポータル・サーバーを再始動するかどうか尋ねられます。「1」を選択して再始動します。

タスクの結果

これにより、ポータル・サーバーで許可ポリシーが有効になりました。

「許可ポリシーを有効にする」 ボックスにチェック・マークを付けた状態で Tivoli Enterprise Portal Server をリサイクルすると、ダッシュボード・データ・プロバイダーは、ダッシュボード・ユーザーに対して管理対象システム・グループおよび管理対象システムへのアクセスを許可または除外する許可呼び出しを、そのローカル・ポリシー・ストアに対して開始します。

権限があるダッシュボード・ユーザーのダッシュボードにモニター対象リソースが表示されない場合、またはリソースの正しいセットが表示されない場合は、問題を診断する手順について *IBM Tivoli Monitoring トラブルシューティング・ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/trouble/itm_trouble.htm) を参照してください。

許可ポリシーの監査

許可ポリシーを変更する以下の tivcmd コマンド (addtorole、copyrole、createrole、deleterole、 exclude、grant、removefromrole、revoke) のいずれかをユーザーが実行すると、許可ポリシー・サーバーは監査メッセージを生成します。監査メッセージは、ユーザーが使用を許可されていない tivcmd コマンドを実行しようとしたときにも生成されます。

例えば、ユーザーが **tivcmd createrole** コマンドを実行したとき、役割を作成する許可を持つ役割にそのユーザーが割り当てられていない場合は、監査メッセージが生成されます。

監査メッセージは IBM Tivoli Monitoring 監査レコード形式に従っており、許可ポリシー・サーバーがインストールされているコンピューター上の監査ログ・ファイルに書き込まれます。デフォルトのロケーションは、`<JazzSM_install_dir>/AuthPolicyServer/PolicyServer/audit` です。許可ポリシー・サーバーのインストール時には、監査ログ・ファイルのディレクトリーのロケーション、監査ログ・ファイルの最大サイズ、および同時に保持できる監査ログ・ファイルの最大数をカスタマイズできます。インストール後、これらのパラメーターは 216 ページの『インストールおよび構成後の許可ポリシー・サーバー構成プロパティーの変更』の説明に従って変更できます。許可ポリシー・サーバーはモニター・エージェントに関連付けられていないため、その監査メッセージを Tivoli Enterprise Portal から表示したり、Tivoli Data Warehouse に保存することはできません。また、監査メッセージに対してシチュエーションを記述することはできません。監査メッセージを見るには、代わりに監査ログ・ファイルを表示する必要があります。

許可ポリシーの適用に関する監査メッセージは、Tivoli Enterprise Portal Server のダッシュボード・データ・プロバイダー・コンポーネントによって生成されます。ユーザーが要求した属性グループ・データまたはシチュエーション・イベントの管理対象システム・グループまたは管理対象システムに対する表示許可をユーザーが持っていない場合、ダッシュボード・データ・プロバイダーは監査メッセージを生成します。また、許可ポリシーが許可ポリシー・サーバーからダウンロードされ、ポリシーを取得できない場合にも、監査メッセージが生成されます。ダッシュボード・データ・プロバイダーはポータル・サーバー管理対象システムのコンポーネントなので、これらの監査メッセージは Tivoli Enterprise Portal クライアントから表示したり、Tivoli Data Warehouse に保存することができます。

ポータル・サーバーに関する監査メッセージの表示方法や監査レコードの形式など、監査について詳しくは、 257 ページの『第 9 章 監査ロギング』を参照してください。

インストールおよび構成後の許可ポリシー・サーバー構成プロパティーの変更

Tivoli 許可ポリシー・サーバー・パッケージをインストールおよび構成した後で、監査ロギングおよびポリシー配布用に許可ポリシー・サーバーの構成パラメーターを変更できます。

始める前に

監査プロパティー

許可ポリシー・サーバー監査ログ・ファイルの場所、監査ログ・ファイルの最大サイズ、および同時に保持される監査ログ・ファイルの最大数を指定するプロパティーを変更できます。

ポリシー配布プロパティー

許可ポリシー・サーバーは、配布できる許可ポリシーの現在のセットであるファイルを定期的に圧縮します。ポータル・サーバーのダッシュボード・データ・プロバイダー・コンポーネントは、定期的な間隔で許可ポリシー・サーバーに対して最新のポリシーの圧縮ファイルを要求します。新しいファイルがある場合は、それが取得されて抽出され、そのポリシー・セットが現在のポリシー・セットとしてダッシュボード・データ・プロバイダーによって使用されます。許可ポリシーが配布のために保存されるディレクトリー、および現在の許可ポリシーがこのディレクトリーにコピーされる頻度を指定するプロパティーを変更できます。

このタスクについて

許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub の WebSphere Application Server 管理者コンソールを使用して、ポリシー・サーバーの構成プロパティーを変更します。何らかの変更を行った場合は、Dashboard Application Services Hub がプロパティーの変更を検出できるように、WebSphere Application Server を再始動する必要があります。

以下のステップを実行して、監査ロギングおよびポリシー配布の構成プロパティーを変更します。

手順

1. 許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub の WebSphere 管理コンソールにログインします。
   a. ブラウザーで Dashboard Application Services Hub コンソールを開きます。デフォルトでは、URLは `https://hostname:16311/ibm/console` です。

      ご使用の環境がデフォルト以外のポート番号を指定して構成されている場合は、その番号を代わりに入力します。サーバーへのデフォルトのパスは、`/ibm/console` です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。

b. ユーザー名とパスワードを入力し、「**実行**」をクリックします。ユーザー名は、 Dashboard Application Services Hub の `administrator` および `iscadmins` の役割に割り当てる必要があります。

c. 「**コンソール設定**」アイコンをクリックし、「**WebSphere 管理コンソール**」を選択します。

d. 「**WebSphere 管理コンソールの起動**」をクリックします。

2. 監査ロギングおよびポリシー配布の構成プロパティーを含むページに移動します。

a. 「**リソース**」→「**リソース環境**」→ 「**リソース環境項目**」をクリックします。

b. 開いたページで、「**AuthzResourceReference**」リンクをクリックします。

c. 開いたページの「**追加プロパティー**」の下で「**カスタム・プロパティー**」をクリックします。

d. テーブルに以下のプロパティーが表示されます。

AUDIT_COUNT
同時に保持される監査ログ・ファイルの最大数。デフォルト値は 5 です。範囲は 2 から 99998 です。

AUDIT_FILE_SIZE
各ログ・ファイルの最大サイズ (メガバイト単位)。

AUDIT_ROOT_DIRECTORY
監査ログ・ファイルの保管先ディレクトリー。

デフォルト値は `<JAZZSM_INSTALL_DIR>¥AuthPolicyServer¥PolicyServer¥audit` です。

DIST_POLL_INTERVAL
このプロパティーは、ダッシュボード・データ・プロバイダーによってダウンロードされる、許可ポリシーを含む圧縮ファイルを許可ポリシー・サーバーが更新する頻度を指定します。

デフォルト値は 5 です。範囲は 1 から 1440 分です。

DIST_ROOT_DIRECTORY
配布するバージョンのポリシーが格納されるディレクトリー。

デフォルト値は `<JAZZSM_INSTALL_DIR>¥AuthPolicyServer¥PolicyServer¥dist` です。

SEED_ROOT_DIRECTORY
ポリシー・ストアのシード・ディレクトリー。このプロパティーは変更しないでください。

XACML_ROOT_DIRECTORY
ポリシー・ストアのルート・ディレクトリー。このプロパティーは変更しないでください。

3. プロパティーの値を変更します。

a. カスタム・プロパティー・テーブルで、**AUDIT_COUNT** などのプロパティー名リンクをクリックします。

b. 開いたページで、「**値**」フィールドを必要に応じて変更します。

c. 「**OK**」をクリックします。

d. このステップを、変更する各プロパティーについて繰り返します。

4. 変更を保存します。

a. 最初のプロパティー変更後に開いたメッセージ・ボックスで、「**保存**」をクリックします。

b. WebSphere 管理コンソールからログアウトします。

c. Dashboard Application Services Hub のWebSphere Application Server を再起動します。

許可ポリシー・ストアの管理

Tivoli 許可ポリシー・サーバーでは、ファイル・システム上の複数のファイルにポリシーが格納されます。ポリシー・ストアの管理方法について詳しくは、以下を参照してください。

高可用性

許可ポリシー・サーバーは、組み込みの高可用性メカニズムを備えておらず、 Dashboard Application Services Hub でロード・バランシングが設定されているとサポートされません。

ポータル・サーバーは独自に許可ポリシーを持っているため、許可ポリシー・サーバーが利用できないときでもポリシーを適用できます。ポータル・サーバーがローカル・ポリシー・ストアを最後の更新後に利用できる最大時間を構成できます。このパラメーターによって指定された時間の間に許可ポリシー・サーバーにアクセスできない場合、ダッシュボード・データに対するその後のすべての要求は、許可ポリシー・サーバーが再び使用可能になるまで許可エラーで失敗します。デフォルト値は 7 日です。

マイグレーションとバックアップ

許可ポリシー・サーバーは、ポリシー・ファイル・ストア用のマイグレーション、バックアップ、エクスポート、およびインポートのツールを備えていません。時間の経過とともに、作成したポリシー定義が増えていくことが考えられます。ポリシー・ストアが破損したり、誤って削除された場合、ポリシー定義を再作成することは容易ではありません。

ベスト・プラクティスは、zip または tar ユーティリティーで実行可能なバックアップを定期的に行うことです。ポリシー・ストアを構成しているファイルは、許可ポリシー・サーバーがインストールされたディレクトリーの下の `/xacml` サブディレクトリーで維持されています。例えば、許可ポリシー・サーバーを Windows で `C:¥Program Files¥IBM¥JazzSM¥AuthPolicyServer` にインストールしたとします。 すべてのファイルを `C:¥Program Files¥IBM¥JazzSM¥AuthPolicyServer¥PolicyServer¥xacml` ディレクトリーに zip 形式で保存すると、ポリシー・ストア全体を効率的にバックアップできます。この zip ファイルは後から、テストから実動の許可ポリシー・サーバーへのマイグレーションなどに利用できます。新しい実動システムでファイルを unzip すると、`/xacml` サブディレクトリーが作成されて、今までにテスト・システム上で定義したすべてのポリシーの役割および許可が取り込まれます。unzip されたこれらのファイルは、そのまま実動許可ポリシー・サーバーで使用できます。

複数のドメインに関する作業

許可ポリシー・サーバーを使用することにより、ドメインとも呼ばれるハブ・モニター・サーバー環境が複数存在する状況でポリシーを管理することができます。

ドメイン は、特定のハブ・モニター・サーバーを中心とした、IBM Tivoli Monitoring コンポーネント (ポータル・サーバー、モニター・サーバー、モニター・エージェント、ウェアハウス・プロキシー・エージェントなど) の集合として定義されます。各ドメインには、シチュエーション、アクション実行、管理対象システム名、管理対象システム・グループ、照会、ワークフロー・ポリシー、およびその他の IBM Tivoli Monitoring オブジェクトに関する固有の名前空間があります。

ドメイン名の指定なしで (または「any」というドメイン名で) 作成された許可ポリシーは、許可ポリシー・サーバーによって管理されているすべての IBM Tivoli Monitoring ドメインに適用されます。ドメイン名は、ダッシュボード・データ・プロバイダー ID と同じであり、`itm.`*`hub_monitoring_server_name`* という形式です。ポータル・サーバーの構成時に、ハブ・モニター・サーバー名の代わりにさらに使いやすい文字列を作成して、ダッシュボード・データ・プロバイダーを有効にすることができます。

ドメインをリストするには、**tivcmd listdomains** コマンドを使用します。例:

```
tivcmd listdomains
itm.HUB_DOMAIN1
itm.HUB_DOMAIN2
itm.HUB_DOMAIN3
```

tivcmd listdomains コマンドは、許可ポリシー・サーバーのインストール先の Dashboard Application Services Hub で接続が定義されているダッシュボード・データ・プロバイダーのリストを返します。また、許可の作成時に指定されたドメイン名があれば、それも返します。通常は、 Dashboard Application Services Hub ごとに 1 つのダッシュボード・データ・プロバイダー接続が定義されます。

各ドメインのハブ名を判別するには、以下の方法のいずれかを使用します。

- 各ハブ・モニター・サーバーに対して**tacmd listsystems** コマンドを実行して、ハブ・モニター・サーバーの管理対象システム名を調べます。モニター・サーバーは、 `EM` 製品コードを使用しています。
- または、ドメインごとに Dashboard Application Services Hub にログインし、ダッシュボード・データ・プロバイダー接続情報を表示します。一般的な環境では、プロバイダー ID がハブ名ではなく `ITMSD` に設定されていることがあります。しかし、接続名は接続の作成時にカスタマイズされていなければハブ名です。

ハブ・モニター・サーバーの名前がわかったら、ドメイン名は `itm.`*`hub_monitoring_server_name`* (例えば `itm.HUB_server1`) となります。

デプロイメント・シナリオ

このトピックに示すデプロイメント・シナリオは、環境内における意思決定に役立ちます。

共有の役割および許可ポリシーを使用する複数のドメイン

このデプロイメント・シナリオでは、ユーザー管理とセットアップに対して単一ドメインのデプロイメントと類似した方法が使用されますが、許可ポリシーを特定の IBM Tivoli Monitoring ドメインを対象に適用する機能が追加されています。

このデプロイメント・シナリオは、ドメインのセットに対して同じ許可ポリシー管理インフラストラクチャーを共有する場合に役立ちます。すべてのドメイン向けの共通の許可ポリシー・セットを作成することも、1 つまたは複数のドメインに固有のポリシーを作成することもできます。役割に対して許可を付与または除外するときは、ポリシーがすべてのドメインに適用されるか特定のドメインに適用されるかを指定します。**tivcmd grant**、**tivcmd exclude**、または **tivcmd revoke** コマンドでドメイン名を指定しないと、そのポリシーはすべてのドメインに適用されます。ドメイン固有のポリシーを作成するには、これらのコマンドで `--domain` 引数を使用します。tivcmd CLI コマンドについて詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

デプロイメントの準備

次の表では、このデプロイメントに必要な内容を説明します。

表 22. 共有の役割およびポリシーを使用する複数のドメインでのデプロイメント要件

数量	コンポーネント	説明
ドメインにつき 1 つ **注:** ロード・バランシングが使用されている場合は、1 つのドメインに複数のダッシュボード・サービス・ハブを設定できます。	Dashboard Application Services Hub	Infrastructure Management Dashboards for Servers のようなダッシュボード・アプリケーションも、各ドメインのダッシュボード・サービス・ハブとともにインストールされます。
1	Tivoli 許可ポリシー・サーバー	いずれかのドメイン用に 許可ポリシー・サーバーを Dashboard Application Services Hub とともにインストールすることも、許可ポリシー管理のためだけに使用する Dashboard Application Services Hub のインスタンスをインストールして、ダッシュボード・アプリケーションはいっさいインストールしないでおくこともできます。

表 22. 共有の役割およびポリシーを使用する複数のドメインでのデプロイメント要件 (続き)

数量	コンポーネント	説明
ドメインにつき 1 つ	ハブ Tivoli Enterprise Monitoring Server	ホット・スタンバイが使用されている場合は、各ドメインに 2 つのハブ・モニター・サーバーを設定できます。 各ハブ・モニター・サーバーには、複数のリモート・モニター・サーバーを接続できます。モニター・サーバーにはモニター・エージェントが接続されます。
ドメインにつき 1 つ	Tivoli Enterprise Portal Server	すべてのドメインで共有されるポリシー・サーバーが 1 つ存在するため、各ポータル・サーバーは、同じ許可ポリシー・サーバーから許可ポリシーを取得するように構成されています。
1 以上	LDAP ユーザー・レジストリー	許可ポリシーを共有するために、すべてのポータル・サーバーおよび各 Dashboard Application Services Hub が LDAP ユーザー・レジストリーの同じセットを使用するように構成します。

独自の許可ポリシーを使用する複数のドメイン

複数のドメインに共通の許可ポリシーを適用せず、ドメインごとに独自の許可ポリシー管理者セットを適用する予定である場合は、各ドメインに許可ポリシー・サーバーおよび Dashboard Application Services Hub をインストールして、許可ポリシーを個別に管理します。

各許可ポリシー・サーバーは 1 つのドメインのポリシーを管理するだけなので、このシナリオでは `--domain` 引数は使用しません。

特定の IBM Tivoli Monitoring ドメイン用のポリシーの作成

マルチドメイン・デプロイメントでは、ドメインごとに異なるアクセス権限を持つ役割を使用してユーザー用のポリシーを作成することがベスト・プラクティスとなります。

特定の IBM Tivoli Monitoring ドメインに使用されるポリシーには、以下の権限が必要です。

管理対象システム・グループまたは管理対象システムの権限の定義	
パラメーター	**値**
ドメイン	「any」または特定のドメイン名 **注:** 「any」値を指定するかドメイン・パラメーターを省略すると、権限はすべてのドメインに適用されます。

管理対象システム・グループまたは管理対象システムの権限の定義	
オペレーション	「view」
オブジェクト・タイプ	「attributegroup」、「event」
リソース・タイプ	「managedsystemgroup」、「managedsystem」
リソース	*managed_system_name* または *managed_system_group_name*

例: 共通のポリシーおよびドメイン固有のポリシーの作成

この例では、ユーザーにある特定のドメインのすべての UNIX OS エージェントへのアクセス権限を付与するが、別のドメインのエージェントへのアクセス権限は付与しない方法を示します。*ALL_UNIX 管理対象システム・グループは自動的に作成され、各ハブ・モニター・サーバーによって管理されます。また、管理者にはすべてのドメインのすべての UNIX OS システムへのアクセス権限が付与されます。

この例では、以下の管理対象システム・グループが使用されます。

管理対象システム・グループ		
Type	**ドメイン**	**Name**
managedsystemgroup	itm.eastcoast	*ALL_UNIX
managedsystemgroup	itm.westcoast	*ALL_UNIX

この例では、次の役割が使用されています。

- EastCoastOperators
- WestCoastOperators
- SuperAdministrator

1. LDAP でユーザー (例えば、`uid=John,cn=itm,o=ibm`) を定義し、LDAP でグループ (例えば、`cn=EastCoastMachineUsers,cn=itm,o=ibm`) を定義してから、LDAP でユーザー ID をグループに追加します。
2. LDAP でユーザー (例えば、`uid=Jane,cn=itm,o=ibm`) を定義し、LDAP でグループ (例えば、`cn=WestCoastMachineUsers,cn=itm,o=ibm`) を定義してから、LDAP でユーザー ID をグループに追加します。
3. LDAP でユーザー (例えば、`uid=Joe,cn=itm,o=ibm`) を定義し、LDAP でグループ (例えば、`cn=SuperAdministratorUsers,cn=itm,o=ibm`) を定義してから、LDAP でユーザー ID をグループに追加します。
4. 新しい役割を作成します。

```
tivcmd createrole --rolename EastCoastOperators --description
"East Coast users with permission to access the east coast machine
ITM Domain"

tivcmd createrole --rolename WestCoastOperators --description
"West Coast users with permission to access the west  coast machines
for the itm.westcoast domain"

tivcmd createrole --rolename SuperAdministrator --description
"Users with permission to access machines from all domains"
```

5. itm.eastcoast ドメインの *ALL_UNIX 管理対象システム・グループの属性グループおよびイベントに対するアクセス権限を、EastCoastOperators 役割に付与します。

```
tivcmd grant --rolename EastCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype attributegroup --operations view --domain itm.eastcoast

tivcmd grant --rolename EastCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype event --operations view --domain itm.eastcoast
```

6. itm.westcoast ドメインの *ALL_UNIX 管理対象システム・グループの属性グループおよびイベントに対するアクセス権限を、WestCoastOperators 役割に付与します。

```
tivcmd grant --rolename WestCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX" --objecttype
attributegroup --operations view --domain itm.westcoast

tivcmd grant --rolename WestCoastOperators --resourcetype
managedsystemgroup --resources "*ALL_UNIX" --objecttype event
--operations view --domain itm.westcoast
```

7. すべてのドメインの *ALL_UNIX 管理対象システム・グループの属性グループおよびイベントに対するアクセス権限を、SuperAdministrator 役割に付与します。

```
tivcmd grant --rolename SuperAdministrator --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype attributegroup --operations view  --domain any

tivcmd grant --rolename SuperAdministrator --resourcetype
managedsystemgroup --resources "*ALL_UNIX"
--objecttype event --operations view --domain any
```

8. 新しい役割にユーザー・グループを割り当てます。

```
tivcmd addtorole --rolename EastCoastOperators --groups
cn=EastCoastMachineUsers,cn=itm,o=ibm

tivcmd addtorole --rolename WestCoastOperators --groups
cn=WestCoastMachineUsers,cn=itm,o=ibm

tivcmd addtorole --rolename SuperAdministrator --groups
cn=SuperAdministrator,cn=itm,o=ibm
```

EastCoastOperators グループに属するユーザーが itm.eastcoast ドメインの Dashboard Application Services Hub にある「サーバー・ダッシュボード」ページにアクセスすると、そのドメインの *ALL_UNIX 管理対象システム・グループとそのメンバーが表示されます。同じユーザーが itm.westcoast ドメインの Dashboard Application Services Hub にログインすると、 *ALL_UNIX 管理対象システム・グループは表示されません。

WestCoastOperators グループに属するユーザーが itm.westcoast ドメインの Dashboard Application Services Hub にある「サーバー・ダッシュボード」ページにアクセスすると、そのドメインの *ALL_UNIX 管理対象システム・グループとそのメンバーが表示されます。同じユーザーが itm.eastcoast ドメインの Dashboard Application Services Hub にログインすると、 *ALL_UNIX 管理対象システム・グループは表示されません。

SuperAdministrator グループに属するユーザーがいずれかのドメインの Dashboard Application Services Hub にある「サーバー・ダッシュボード」ページにアクセスすると、ダッシュボード・サーバーの接続先ドメインの *ALL_UNIX 管理対象システム・グループとそのメンバーが表示されます。

例: 共通の管理対象システム・グループの許可ポリシーの作成

複数のドメインに同じ管理対象システム・グループ名が存在する場合に、ダッシュボード・ユーザーがすべてのドメインについてそれらの管理対象システム・グループのデータを表示できるようにするには、以下のコマンドの例のように、役割を作成して権限を付与します。

```
tivcmd createrole --rolename  WindowsDataCenterOperators

tivcmd grant --rolename WindowsDataCenterOperators  --operations view
--objecttype attributegroup  --resources DataCenterServers
--resourcetype managedsystemgroup

tivcmd grant --rolename WindowsDataCenterOperators  --operations view
--objecttype event   --resources DataCenterServers
--resourcetype managedsystemgroup
```

上の grant コマンドの例では --domain 引数が指定されていないため、許可ポリシーはすべてのドメインに適用されます。その結果、 WindowsAdministrators 役割に割り当てられたすべてのユーザーまたはユーザー・グループは、すべてのドメインの DataCenterServers 管理対象システム・グループのデータを表示できます。

例: 共通の役割を使用したドメイン固有リソースの管理

複数のドメインに同じ管理対象システム・グループ名が存在しなくても、複数のドメインに関して同じ役割を実行するユーザーまたはユーザー・グループが存在する場合は、以下のコマンドの例のように、ドメイン固有の権限を持つ共通の役割を作成できます。

```
tivcmd createrole --rolename  LinuxRegionalOperators

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype attributegroup  --resources SeattleServers
--resourcetype managedsystemgroup --domain itm.HUB_west

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype event   --resources SeattleServers
--resourcetype managedsystemgroup  --domain itm.HUB_west

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype attributegroup  --resources BostonServers
--resourcetype managedsystemgroup --domain itm.HUB_east

tivcmd grant --rolename LinuxRegionalOperators  --operations view
--objecttype event   --resources AustinServers
--resourcetype managedsystemgroup  --domain itm.HUB_east
```

この場合、LinuxRegionalOperators 役割に割り当てられたすべてユーザーまたはユーザー・グループは、itm.HUB_west ドメインの Dashboard Application Services Hub にログインすると SeattleServers 管理対象システム・グループのデータを表示でき、itm.HUB_east ドメインの Dashboard Application Services Hub にログインすると BostonServers 管理対象システム・グループのデータを表示できます。

例: ドメイン固有の許可ポリシーの作成

ドメイン間で共通でない役割については、以下のコマンドの例のように、単一のドメイン用の権限だけを持つ役割を作成します。

```
tivcmd createrole --rolename  ChicagoDataCenterOperators

tivcmd grant --rolename ChicagoDataCenterOperators   --operations view
--objecttype attributegroup  --resources ChicagoServers
--resourcetype managedsystemgroup --domain itm.HUB_midwest

tivcmd grant --rolename ChicagoDataCenterOperators   --operations view
--objecttype event   --resources ChicagoServers
--resourcetype managedsystemgroup  --domain itm.HUB_midwest
```

このシナリオでは、 ChicagoDataCenterOperators 役割に割り当てられたユーザーまたはユーザー・グループが表示できるデータは、単一のドメインの管理対象システム・グループのものだけです。

第 8 章 通信の保護

Tivoli Enterprise Monitoring Agent、Tivoli Enterprise Monitoring Server、および Tivoli Enterprise Portal Server 間の通信を保護するには、ポータル・サーバーとハブ・モニター・サーバー間、ハブとリモート・モニター・サーバー間、およびモニター・エージェントとモニター・サーバー間の通信を構成するときに、プロトコルとして SPIPE を使用します。

Tivoli Enterprise Portal クライアントとポータル・サーバーの間の通信を保護するには、2 つのプロトコルを追加で使用します。

- Secure Hypertext Transport Protocol (HTTPS)。ファイルおよび相互運用オブジェクト参照 (IOR) を検索します。
- Internet Inter-ORB Protocol (IIOP)。ポータル・サーバーとクライアントの間の通信を保護します。

注: デフォルトでは、両方のプロトコルが使用されます。ただし、HTTPS のみを使用してポータル・サーバーと通信するようにポータル・クライアントを構成できます。

HTTPS は、以下のコンポーネント間の通信を保護するためにも使用できます。

- Dashboard Application Services Hub と IBM Tivoli Monitoring ダッシュボード・データ・プロバイダー
- tacmd コマンド行インターフェースとハブ Tivoli Enterprise Monitoring Server
- 許可ポリシーの tivcmd コマンド行インターフェースと、Tivoli 許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub
- Open Services Lifecycle Collaboration Performance Monitoring サービス・プロバイダーと Registry Services、セキュリティー・サービス、および OSLC クライアント
- Tivoli Integrated Portal とポータル・サーバーの IBM Tivoli Monitoring グラフ Web サービス

さらに、以下のタイプの保護された通信がサポートされます。

- TLS/SSL を使用してハブ・モニター・サーバーと LDAP サーバーの間の通信を保護する
- TLS/SSL を使用してポータル・サーバーと LDAP サーバーの間の通信を保護する
- TLS/SSL を使用してモニター・エージェントと IBM IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF バージョン 12 以降の間の通信を保護する

保護された通信をサポートする IP.SPIPE や HTTPS などのプロトコルを選択することに加えて、公開鍵/秘密鍵ファイルを使用することにより TLS/SSL 非対称暗号化を設定します。この作業には、以下のタスクが含まれます。

- 鍵データベースを操作する

- 製品に付属する自己署名証明書を使用しない場合は、新しい公開鍵と秘密鍵のペアを要求する
- 製品に付属する自己署名証明書を使用しない場合は、認証局署名者証明書および署名付きデジタル証明書を鍵データベースに追加する
- IBM Tivoli Monitoring コンポーネントの要求の送信先であるアプリケーション用の署名者証明書を追加する
- コンポーネントが証明書の認証を実行できるようにする

注: 新しい証明書を要求するのがベスト・プラクティスですが、製品に付属する自己署名証明書をテスト環境で使用して、保護された通信を設定する手順に慣れることもできます。

IBM Tivoli Monitoring は、保護された通信の設定時に鍵および証明書ストアを操作するために使用する 2 つのアプリケーションを提供します。

- Global Security Toolkit (GSKit) プログラムは、IBM Tivoli Monitoring コンポーネントと共に分散プラットフォームにインストールされます。このプログラムは、証明書および鍵を操作するための iKeyman ユーティリティーとコマンド行インターフェースを含みます。
- Tivoli Enterprise Portal Server 拡張サービス (TEPS/e) 管理コンソール (別名 ISCLite) は、TEPS/e で実行されるサービスの通信を保護するためにポータル・サーバーで使用されます。

デフォルトの自己署名証明書および鍵は、IBM Tivoli Monitoring をインストールしたときに提供されます。認証局の署名済み証明書を使用する場合は、GSKit ユーティリティーを使用して証明書要求を作成してから、鍵データベースを作成し、証明書をインポートします。無人操作の場合は、stash ファイルが鍵データベース・パスワードを提供します。GSKit が IBM Tivoli Monitoring コンポーネントと共にインストールされる際、鍵ファイルの名前は、以下の環境変数を使用して指定されます。

- KDEBE_KEYRING_FILE=C:¥IBM¥ITM¥keyfiles¥keyfile.kdb
- KDEBE_KEYRING_STASH=C:¥IBM¥ITM¥keyfiles¥keyfile.sth
- KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate

IBM Tivoli Monitoring が通信する他の製品の管理者と協力して、保護された通信を設定してください。いずれかの Jazz for Service Management コンポーネント (Dashboard Application Services Hub、 Registry Services、または セキュリティー・サービス) を IBM Tivoli Monitoring と共に使用している場合は、WebSphere Application Server 管理コンソールを使用してそれらのトラストストアおよび証明書ストアを操作します。

以下の表に、保護可能な通信フローと、対話を保護する方法についての情報が得られる場所を示します。

注: 特に明記しない限り、以下のタスクは、TLS/SSL およびサーバー証明書認証を設定するために使用されます。サーバー証明書認証を使用する場合、クライアント (要求元) は、サーバー (要求先) から受信した証明書を認証します。

表 23. 通信を保護するためのタスク

通信を保護するためのタスク	情報の入手先
Tivoli Enterprise Portal クライアントとポータル・サーバー間で TLS/SSL を使用します。	「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ポータル・サーバーとクライアント間の SSL の使用』を参照してください。
IP.SPIPE を証明書の検証と共に使用して以下の対話の通信を保護します。 • ハブとリモート・モニター・サーバーの通信 • ハブ・モニター・サーバーとポータル・サーバーの通信 • モニター・サーバーとモニター・エージェントの通信 HTTPS を証明書の検証と共に使用して以下の対話の通信を保護します。 • tacmd CLI または SOAP クライアントからハブ・モニター・サーバーへの通信 • モニター・サーバー、ポータル・サーバー、およびモニター・エージェントのサービス・コンソールへの要求	IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) のITM Certificate Authentication Configuration Guide for ITM 6.2.2 and newer releasesを参照してください。
ハブ・モニター・サーバーと LDAP サーバーの間で TLS/SSL を使用します。	230 ページの『ハブ・モニター・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』
ポータル・サーバーと LDAP サーバー間で TLS/SSL を使用します。	123 ページの『ポータル・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成』
IBM Dashboard Application Services Hub が IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーに要求を送信するときに TLS/SSL を使用します。	231 ページの『Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成』
ダッシュボード・データ・プロバイダーが許可ポリシー・サーバーから許可ポリシーを取得するための要求を送信するときに TLS/SSL を使用します。	235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』
許可ポリシーの tivcmd コマンド行インターフェースが許可ポリシー・サーバーに要求を送信するときに TLS/SSL を使用します。	235 ページの『許可ポリシー・サーバーとの TLS/SSL 通信の構成』
モニター・エージェントから IBM Tivoli Netcool/OMNIbus Probe for Tivoli EIF にプライベート・シチュエーション・イベントを送信するために TLS/SSL を使用します。この対話では、プローブが証明書を使用してモニター・エージェント (クライアント) を認証できるように、クライアント証明書認証を構成します。	438 ページの『TLS/SSL 通信を使用した専用シチュエーション・イベントの送信』

表 23. 通信を保護するためのタスク (続き)

通信を保護するためのタスク	情報の入手先
Tivoli Business Service Manager または Tivoli Integrated Portal がポータル・サーバーのグラフ Web サービスに HTTPS 要求を送信するときに TLS/SSL を使用します。	*IBM Tivoli Monitoring インストールおよび設定ガイド*の『SSL を介した Tivoli Business Service Manager と Tivoli Enterprise Portal Server の統合』。
IBM Tivoli Monitoring コンポーネントに対して連邦情報処理標準 (FIPS) を有効にします。	242 ページの『IBM Tivoli Monitoring 用に FIPS を使用可能にする』
IBM Tivoli Monitoring 証明書を更新した後、TEPS/e 証明書をポータル・サーバーの鍵ファイル・データベースにインポートして、ポータル・サーバーの Web サーバー・プラグインと TEPS/e が保護された通信を継続できるようにします。	248 ページの『ポータル・サーバーの鍵ファイル・データベースへの TEPS/e 証明書のインポート』

ハブ・モニター・サーバーおよび LDAP サーバー間の TLS/SSL 通信の構成

ハブ・モニター・サーバーから LDAP サーバーへの TLS/SSL 通信を構成して、ユーザーおよびグループの認証の要求を保護することができます。

TLS/SSL 用に LDAP サーバーを設定し、公開署名者証明書を取得した後、ハブ・モニター・サーバーの GSKit iKeyman ユーティリティーまたはコマンド行インターフェースを使用して、CMS タイプの新しい鍵データベースと、鍵データベースのパスワードを含む stash ファイルを設定します。次に、LDAP サーバーの公開署名者証明書を新しい鍵データベースにインポートし、証明書のラベル名を指定します。GSKit の使用について詳しくは、 249 ページの『GSKit コマンド行インターフェースによる鍵データベースおよび証明書の操作』および 251 ページの『GSKit iKeyman ユーティリティーによる鍵データベースおよび証明書の操作』を参照してください。

次に、ハブ・モニター・サーバーを再構成して LDAP TLS/SSL 通信を有効にします。ハブ・モニター・サーバーを再構成するときは、鍵データベース (LDAP 鍵ストア・ファイルとも呼ばれます) の場所、鍵データベースを含む stash ファイル (LDAP 鍵ストア stash とも呼ばれます)、公開署名者証明書のラベル名、および鍵データベースのパスワードを指定する必要があります。また、LDAP サーバーの管理者に問い合わせて、LDAP ポートの値を変更する必要があるか確認します。これは、保護されたポート番号は通常ポート 636 であるからです。

注:

LDAP TLS/SSL には、LDAP 管理者による操作が必要な部分がありますが、これについては Tivoli Monitoring の資料では説明していません。IBM セキュリティー・システム・インフォメーション・センターの以下のトピックでは、TLS/SSL 用に LDAP サーバーを設定する方法に関する情報を提供しています。

- SSL アクセス用 Microsoft Active Directory の構成
- SSL アクセス用 Tivoli Directory Server クライアントの構成

- SSL アクセス用 Oracle Java System Directory Server の構成

Dashboard Application Services Hub およびダッシュボード・データ・プロバイダー間の TLS/SSL 通信の構成

HTTPS を使用する場合、Dashboard Application Services Hub からポータル・サーバーのダッシュボード・データ・プロバイダーへの TLS/SSL 通信を構成できます。

Dashboard Application Services Hub および IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーの間の通信には、Hypertext Transfer Protocol (HTTP) または Hypertext Transfer Protocol Secure (HTTPS) が使用されます。HTTPS は、Transport Layer Security (TLS) またはその先行プロトコルである Secure Sockets Layer (SSL) の上で動作するように設計されています。これらの層では、鍵交換を使用する暗号化が実施されます。

ロードマップ

HTTPS とそのセキュリティー暗号化機能を使用するには、以下のロードマップのタスクを実行します。

表 24. ロードマップ: ダッシュボード・データ・プロバイダーの TLS/SSL セットアップ

ステップ	説明および提供される情報
1	ポータル・サーバーによって使用される公開鍵と秘密鍵のペアを取得する方法は 2 つあります。 • IBM Tivoli Monitoring とともにインストールされるデフォルトの自己署名証明書を使用します。このオプションを選択した場合は、ステップ 2 に進みます。 または • 認証局が署名したデジタル証明書を使用します。この場合、証明書要求を作成し、認証局に送信して署名してもらう必要があります。デジタル証明書への署名が終了したら、認証局の署名者の証明書をポータル・サーバーのトラストストアに追加し、新しいデジタル署名をポータル・サーバーの鍵ストアに追加します。詳しくは、『サード・パーティーの認証局によって署名された証明書のポータル・サーバーに対する使用』を参照してください。
2	ポータル・サーバーのダッシュボード・データ・プロバイダーへの接続が構成された各 Dashboard Application Services Hub で、ポータル・サーバーにより使用される公開署名者証明書を Dashboard Application Services Hub WebSphere トラストストアに追加します。 234 ページの『Dashboard Application Services Hub サーバー用の TLS/SSL 通信の構成』のステップを実行します。

サード・パーティーの認証局によって署名された証明書のポータル・サーバーに対する使用

サード・パーティーの証明書を使用して、ダッシュボード・データ・プロバイダー用に TLS/SSL を構成できます。それには、署名者証明書とプライベート・デジタル証明書を GSKit が管理する鍵データベースおよび TEPS/e が使用するトラストストアおよび鍵ストアに追加します。

始める前に

認証局の署名者証明書を入手します。

TEPS/e 管理コンソール が使用可能であることを確認します。ログオンする方法を含む詳細な手順については、 118 ページの『TEPS/e 管理コンソールの開始』を参照してください。

手順

1. TEPS/e 管理コンソールまたは GSKit コマンド行インターフェースを使用して、認証局の署名を受けるプライベート証明書要求を作成します。以下の説明は、この手順を TEPS/e 管理コンソールを使用して実行する方法を示しています。
   a. TEPS/e 管理コンソール にログオンします。
   b. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
   c. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultKeyStore**」リンクをクリックします。
   d. 「追加プロパティー」領域で、「**個人証明書要求**」リンクをクリックし、表示されたページで「**新規**」をクリックします。
   e. 表示されたページで次の情報を指定します。
      - 「**ファイル名**」を、プライベート証明書要求を格納するロケーションに設定します。例えば、`C:¥dashboardcerts¥TEPSCertRequest.arm` です。
      - 「**鍵ラベル**」を、証明書の希望するラベルに設定します。例えば、`TEPS Certificate` です。
      - 「**鍵サイズ**」を `2048` に設定します。
      - 「**シグニチャー・アルゴリズム**」は「`SHA1withRSA`」のままにします。
      - 「**共通名**」を、TEPS/e コンピューターの固有の名前に設定します。通常、これはホスト名です。
      - 「**組織**」を、意味が分かりやすい値に設定します。通常、これは会社名です。
      - 「**組織単位**」を、意味が分かりやすい名前に設定します。例えば、`TEPS` です。
      - 「**国または地域**」を希望する値に設定します。例えば、`US` です。
   f. 「**OK**」、「**保存**」の順にクリックします。
2. 上記で生成した認証要求を認証局に送信し、新規のデジタル証明書を要求します。認証局が新規のデジタル証明書を生成するまでに 2 週間から 3 週間かかる場合があります。
3. 認証局から新しいデジタル証明書が返送されたら、ポータル・サーバーと TEPS/e がインストールされているコンピューター上のロケーションにそのデジタル証明書を保存します。例えば、`C:¥dashboardcerts¥TEPSSignedCert.arm` です。
4. GSKit コマンド行インターフェースを使用して、`CMS` タイプの新しい鍵データベースを作成し、鍵データベースのパスワードを stash ファイルに保存します。次に、認証局の署名者証明書と新しいデジタル証明書を新しい鍵データベースにインポートします。この鍵データベースは、ポータル・サーバーの内蔵 HTTP サーバーによって使用されます。

5. また、TEPS/e 管理コンソールを使用して、認証局公開署名者証明書を TEPS/e トラストストアに追加する必要があります。
   a. TEPS/e 管理コンソール にログオンします。
   b. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
   c. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultTrustStore**」リンクをクリックします。
   d. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、表示されたページで「**追加**」をクリックします。
   e. 表示されたページで次の情報を指定します。
      - 「**別名**」を証明書の適切なラベルに設定します。例えば、TEPS Signer Certificate です。
      - 「**ファイル名**」を、抽出した認証局署名者証明書のロケーションに設定します。例えば、C:¥dashboardcerts¥CASignerCert.arm です。
      - 「**データ・タイプ**」は「**Base64 エンコード ASCII データ**」のままにします。
   f. 「**OK**」、「**保存**」の順にクリックします。
6. TEPS/e 管理コンソールを使用して、TEPS/e 鍵ストアに対する署名付きデジタル証明書を受け取ります。
   a. TEPS/e 管理コンソール にログオンします。
   b. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
   c. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultKeyStore**」リンクをクリックします。
   d. 「追加プロパティー」領域で、「**個人証明書**」リンクをクリックし、表示されたページで「**認証局から受け取る**」をクリックします。
   e. 表示されたページで次の情報を指定します。
      - 「**ファイル名**」を、署名されたデジタル証明書のロケーションに設定します。例えば、C:¥dashboardcerts¥TEPSSignedCert.arm です。
      - 「**データ・タイプ**」は「**Base64 エンコード ASCII データ**」のままにします。
   f. 「**OK**」、「**保存**」の順にクリックします。
7. 新規のプライベート証明書をTEPS/eのデフォルトのサーバー証明書として設定します。
   a. TEPS/e 管理コンソール にログオンします。
   b. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
   c. 「関連項目」領域で、「**SSL 構成**」リンクをクリックし、表内の「**NodeDefaultSSLSettings**」リンクをクリックします。
   d. 表示されたページで、「**デフォルトのサーバー証明書別名**」をクリックし、署名された TEPS/e 証明書を選択します。例えば、TEPS Certificate です。
   e. 「**OK**」、「**保存**」の順にクリックします。
   f. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を再度選択します。
   g. 「**エンドポイント・セキュリティー構成の管理**」リンクをクリックします。

h. 「**インバウンド**」→「**thecellname**」→「**ノード**」の下にあるノード名のリンクをクリックします。

i. 「**鍵ストアの証明書別名**」をクリックし、署名された TEPS/e 証明書を選択します。例えば、TEPS Certificate です。

j. 「**OK**」、「**保存**」の順にクリックします。

Dashboard Application Services Hub サーバー用の TLS/SSL 通信の構成

TLS/SSL を構成するには、ポータル・サーバーにより使用される公開署名者証明書を Dashboard Application Services Hub WebSphere トラストストアに追加します。

注: ポータル・サーバー用の新しいデジタル証明書を要求した場合は、証明書が届くまで待ってから、この手順を実行します。

手順

1. Dashboard Application Services Hub WebSphere 管理コンソールにログインします。
   a. Internet Explorer ブラウザーまたは Firefox ブラウザーで、以下の URL を入力します。https://hostname:16311/ibm/console。

      ご使用の環境がデフォルト以外のポート番号を指定して構成されている場合は、その番号を代わりに入力します。サーバーへのデフォルトのパスは、/ibm/console です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。

   b. Dashboard Application Services Hub 管理ユーザー ID とパスワードを入力し、「**実行**」をクリックします。

      ユーザー ID は、administrator および iscadmins の各役割に割り当てる必要があります。

   c. 「コンソール設定」領域で、「**WebSphere 管理コンソール**」をクリックし、「**WebSphere 管理コンソールの起動**」ボタンをクリックします。
2. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
3. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultTrustStore**」リンクをクリックします。
4. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、表示されたページで「**ポートから取得**」をクリックします。
5. ポータル・サーバーのホスト名を入力します。
6. ポート 15201 を入力します。
7. 別名 (例えば、ITM-TEPS) を入力します。
8. 「**署名者情報の取得**」をクリックします。
9. 「**OK**」、「**保存**」の順にクリックします。

タスクの結果

これで Dashboard Application Services Hub サーバーとポータル・サーバーおよびそのダッシュボード・データ・プロバイダーの間の通信用の証明書が設定されました。

HTTP ではなく HTTPS を使用するようにダッシュボード・データ・プロバイダー接続を構成する方法については、31 ページの『第 3 章 ダッシュボード環境の準備』のロードマップの説明に戻ってください。

許可ポリシー・サーバーとの TLS/SSL 通信の構成

HTTPS を使用する場合は、Tivoli 許可ポリシー・サーバーとの TLS/SSL 通信を構成できます。

Hypertext Transfer Protocol (HTTP) または Hypertext Transfer Protocol Secure (HTTPS) のいずれかを使用して許可ポリシー・サーバーと通信する IBM Tivoli Monitoring コンポーネントには、以下の 2 つがあります。

- 許可ポリシーの tivcmd コマンド行インターフェースは、 CLI コマンドを処理するために許可ポリシー・サーバーに HTTP/HTTPS 要求を送信します。
- Tivoli Enterprise Portal Server は、最新のポリシー・ストアを取得するために HTTP/HTTPS 要求を許可ポリシー・サーバーに送信します。

HTTPS は、Transport Layer Security (TLS) またはその先行プロトコルである Secure Sockets Layer (SSL) の上で動作するように設計されています。これらの層では、鍵交換を使用する暗号化が実施されます。

ロードマップ

HTTPS とそのセキュリティー暗号化機能を使用するには、以下のロードマップのタスクを実行します。

注: 以下の手順は、ポータル・サーバーおよび tivcmd CLI から要求が直接 IBM Dashboard Application Services Hub アプリケーション・サーバーに送信され、ダッシュボード・ハブと組み合わせて使用されることがある HTTP サーバーには送信されないということが前提です。HTTP サーバーを IBM Dashboard Application Services Hub と組み合わせて使用する場合は、HTTP サーバーが使用する証明書も更新する必要があります。

表 25. ロードマップ: 許可ポリシー・サーバーの *TLS/SSL* セットアップ

ステップ	説明および提供される情報
1	許可ポリシー・サーバーがインストールされている Dashboard Application Services Hub の WebSphere Application Server 管理コンソールを使用し、以下のオプションのいずれかによって公開鍵と秘密鍵のペアを取得します。 • 『WebSphere で生成された証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成』 インストール時に、WebSphere Application Server が公開署名者証明書とデフォルトの秘密署名証明書を生成します。これらの証明書を必要に応じて使用できます。 • 237 ページの『サード・パーティー証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成』 サード・パーティーの署名者証明書をWebSphere Application Server のトラストストアに追加します。証明書要求は WebSphere Application Server で作成され、署名のために認証局に転送されます。署名された証明書は、WebSphere Application Server の鍵ストアに追加されます。秘密署名証明書をデフォルトの証明書として設定する必要があります。
2	各 許可ポリシーの tivcmd コマンド行インターフェース インストール済み環境で、次の手順を実行します。 1. 新規のクリーンな鍵データベースを作成します。 2. 許可ポリシー・サーバーが使用する公開署名者証明書をその新規の鍵データベースに追加します。 3. サーバー証明書の検証を可能にする環境変数を設定します。デフォルトの場合、tivcmd CLI と許可ポリシー・サーバーの間で使用される HTTPS では、証明書の交換は行われず、セキュリティー暗号化も使用されません。これらが実施されるようにするには、この環境変数を設定する必要があります。 240 ページの『TLS/SSL 用の tivcmd CLI 構成』のステップを実行します。
3	許可ポリシー・サーバーと通信するように構成されている各ポータル・サーバーで、許可ポリシー・サーバーが使用する公開署名者証明書を TEPS/e トラストストアに追加します。 241 ページの『ポータル・サーバーおよび許可ポリシー・サーバー間の TLS/SSL 通信の構成』のステップを実行します。
4	許可ポリシー・サーバーに要求を送信する際に HTTPS プロトコルを使用することを示すために、**tivcmd login** コマンドで `-s` 引数を使用します。 tivcmd CLI の環境変数 `ITM_AUTHENTICATE_SERVER_CERTIFICATE` が `Y` に設定されていると、TLS/SS 証明書の交換が発生し、CLI 要求データは暗号化されます。

WebSphere で生成された証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成

許可ポリシー・サーバーおよび Dashboard Application Services Hub が使用する WebSphere Application Server のインストール時に、公開署名者証明書および署名されたデフォルトのプライベート証明書が生成されます。これらの証明書は、公開署名者証明書を抽出することによって TLS/SSL 通信に使用できます。

手順

1. 許可ポリシー・サーバーおよび Dashboard Application Services Hub の WebSphere 管理コンソールにログインします。
   a. Internet Explorer ブラウザーまたは Firefox ブラウザーで、以下の URL を入力します。`https://hostname:16311/ibm/console`。

      ご使用の環境がデフォルト以外のポート番号を指定して構成されている場合は、その番号を代わりに入力します。サーバーへのデフォルトのパスは、`/ibm/console` です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。
   b. Dashboard Application Services Hub 管理ユーザー ID とパスワードを入力し、「**実行**」をクリックします。

      ユーザー ID は、`administrator` および `iscadmins` の各役割に割り当てる必要があります。
   c. 「コンソール設定」領域で、「**WebSphere 管理コンソール**」をクリックし、「**WebSphere 管理コンソールの起動**」ボタンをクリックします。
2. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
3. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultTrustStore**」リンクをクリックします。
4. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、表示された表の「`root`」エントリー・チェック・ボックスを選択します。
5. 「**抽出**」をクリックし、表示されたページの「**ファイル名**」フィールドに証明書ファイル名を入力します。例えば、`C:¥policyauthcerts¥PolicyAuthServerSignerCert.arm` です。
6. 「**データ・タイプ**」リストから、「**Base64 エンコード ASCII データ**」オプションを選択し、「**OK**」をクリックします。

次のタスク

これで、抽出した公開署名者証明書を、ポータル・サーバーおよび 許可ポリシーの tivcmd コマンド行インターフェース コンピューターにインポート用に配布できます。

サード・パーティー証明書を使用した許可ポリシー・サーバー用の TLS/SSL の構成

サード・パーティー証明書を使用して、許可ポリシー・サーバー用の TLS/SSL を構成することができます。

始める前に

以下のステップの多くでは、許可ポリシー・サーバーおよび Dashboard Application Services Hub の WebSphere 管理コンソールへのログインが必要です。このコンソールにログインするには、以下の手順を使用します。

1. Internet Explorer ブラウザーまたは Firefox ブラウザーで、以下の URL を入力します。`https://hostname:16311/ibm/console`。

ご使用の環境がデフォルト以外のポート番号を指定して構成されている場合は、その番号を代わりに入力します。サーバーへのデフォルトのパスは、/ibm/console です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。

2. Dashboard Application Services Hub 管理ユーザー ID とパスワードを入力し、「**実行**」をクリックします。

   ユーザー ID は、administrator および iscadmins の各役割に割り当てる必要があります。

3. 「コンソール設定」領域で、「**WebSphere 管理コンソール**」をクリックし、「**WebSphere 管理コンソールの起動**」ボタンをクリックします。

手順

- 認証局の公開署名者証明書をWebSphere Application Server のトラストストアに追加します。
  1. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
  2. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultTrustStore**」リンクをクリックします。
  3. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、表示されたページで「**追加**」をクリックします。
  4. 表示されたページで次の情報を指定します。
     - 「**別名**」を証明書の適切なラベルに設定します。例えば、許可ポリシー・サーバー Signer Certificate です。
     - 「**ファイル名**」を、認証局署名者証明書のロケーションに設定します。例えば、C:¥policyauthcerts¥CASignerCert.arm です。
     - 「**データ・タイプ**」は「**Base64 エンコード ASCII データ**」のままにします。
  5. 「**OK**」、「**保存**」の順にクリックします。

  これで、認証局の公開署名者証明書をポータル・サーバーおよび tivcmd CLI コンピューターに対してインポート用に配布できます。
- 認証局の署名を受けるプライベート証明書要求を作成します。
  1. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
  2. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultKeyStore**」リンクをクリックします。
  3. 「追加プロパティー」領域で、「**個人証明書要求**」リンクをクリックし、表示されたページで「**新規**」をクリックします。
  4. 表示されたページで次の情報を指定します。
     - 「**ファイル名**」を、プライベート証明書要求を格納するロケーションに設定します。例えば、C:¥policyauthcerts¥PolicyAuthServerCertRequest.arm です。
     - 「**鍵ラベル**」を、証明書の希望するラベルに設定します。例えば、許可ポリシー・サーバー Certificate です。
     - 「**シグニチャー・アルゴリズム**」は「**SHA1withRSA**」のままにします。
     - 「**鍵サイズ**」を 2048 に設定します。

- 「**共通名**」を、許可ポリシー・サーバーの固有の名前に設定します。通常、これはコンピューター名です。
- 「**組織**」を、意味が分かりやすい値に設定します。通常、これは会社名です。
- 「**組織単位**」を、意味が分かりやすい名前に設定します。例えば、PolicyAuth です。
- 「**国または地域**」を希望する値に設定します。例えば、US です。

5. 「**OK**」、「**保存**」の順にクリックします。

上記で生成した認証要求を認証局に送信し、新規のデジタル証明書を要求します。認証局が新規のデジタル証明書を生成するまでに 2 週間から 3 週間かかる場合があります。

認証局から新規のデジタル証明書が返送されたら、許可ポリシー・サーバー コンピューター上の特定のロケーションに保存します。例えば、C:¥policyauthcerts¥PolicyAuthServerSignedCert.arm です。

- 署名されたデジタル証明書を、WebSphere 管理コンソールを使用して受け取ります。
  1. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
  2. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultKeyStore**」リンクをクリックします。
  3. 「追加プロパティー」領域で、「**個人証明書**」リンクをクリックし、表示されたページで「**認証局から受け取る**」をクリックします。
  4. 表示されたページで次の情報を指定します。
     - 「**ファイル名**」を、署名されたデジタル証明書のロケーションに設定します。例えば、C:¥policyauthcerts¥PolicyAuthServerSignedCert.arm です。
     - 「**データ・タイプ**」は「**Base64 エンコード ASCII データ**」のままにします。
  5. 「**OK**」、「**保存**」の順にクリックします。
- 新規のプライベート証明書をデフォルトのサーバー証明書として設定します。
  1. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
  2. 「関連項目」領域で、「**SSL 構成**」リンクをクリックし、表内の「**NodeDefaultSSLSettings**」リンクをクリックします。
  3. 表示されたページで、「**デフォルトのサーバー証明書別名**」をクリックし、署名された許可ポリシー・サーバー証明書を選択します。例えば、許可ポリシー・サーバー Certificate です。
  4. 「**OK**」、「**保存**」の順にクリックします。
  5. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を再度選択します。
  6. 「**エンドポイント・セキュリティー構成の管理**」リンクをクリックします。
  7. 「**インバウンド**」 → 「**thecellname**」→ 「**ノード**」の下にあるノード名のリンクをクリックします。
  8. 「**鍵ストアの証明書別名**」をクリックし、署名された許可ポリシー・サーバー証明書を選択します。例えば、許可ポリシー・サーバー Certificate です。

9. 「**OK**」、「**保存**」の順にクリックします。

TLS/SSL 用の tivcmd CLI 構成

許可ポリシー・サーバーで TLS/SSL を使用するには、tivcmd コマンド行インターフェースを準備し、新規鍵データベースを作成して、この新規鍵データベースに許可ポリシー・サーバーが使用する公開署名者証明書を追加してから、tivcmd CLI 環境変数ファイルを変更する必要があります。

注: 許可ポリシー・サーバーのデジタル証明書を要求した場合は、その証明書を受け取ってからこの手順を実行してください。

始める前に

tivcmd CLI コンピューターで証明書を管理するための以下の手順では、 tivcmd CLI コンポーネントとともにインストールされる GSKit コマンド行ツールを使用します。これらの手順は、tivcmd CLI がインストールされている各コンピューターで実行する必要があります。

この手順で使用する用語については、 249 ページの『GSKit コマンド行インターフェースによる鍵データベースおよび証明書の操作』を参照してください。ほとんどの用語は tivcmd CLI のインストール先ディレクトリーに基づいています。

手順

1. 以下のコマンドを使用して、GSKit コマンド行ツールを呼び出すためのパスを設定します。
   - Windows 64 ビット:

     ```
     set PATH=<gskithome>¥lib64;%PATH%
     cd <gskithome>¥bin
     ```

   - Windows 32 ビット:

     ```
     set PATH=<gskithome>¥lib;%PATH%
     cd <gskithome>¥bin
     ```

   - Linux および UNIX 32 ビット:

     ```
     export LD_LIBRARY_PATH=<gskithome>/lib:$LD_LIBRARY_PATH
     cd <gskithome>/bin
     ```

   - Linux および UNIX 64 ビット:

     ```
     export LD_LIBRARY_PATH=<gskithome>/lib64:$LD_LIBRARY_PATH
     cd <gskithome>/bin
     ```

2. 既存の tivcmd CLI 鍵データベースを保存します。

   問題の修復を行うためのベスト・プラクティスは、インストール済みバージョンの tivcmd CLI 鍵データベースを各 tivcmd CLI コンピューターに保存しておくことです。

   拡張子が .crl、.kdb、.rdb、および .sth の以下のファイルを別のロケーションにコピーします。
   - Windows: *<keydbdir>¥<oldkeydbname>.**
   - Linux および UNIX: *<keydbdir>/<oldkeydbname>.**
3. 新規 tivcmd CLI 鍵データベースを作成します。

a. 次のコマンドを使用して、新規データベースを作成し、余分な公開署名者証明書をすべて削除します。

```
<gskittoolcmd> -keydb -create -db <newkeydb>
-pw <newkeydbpw> -expire 3650 -stash -fips
```

b. 次のコマンドを使用して、データベースが空であることを確認します。

```
 <gskittoolcmd> -cert -list -db <newkeydb>
-pw <newkeydbpw> -fips
```

データベースが空でない場合は、delete コマンドを使用して、残っている証明書を削除します。

4. 公開署名者証明書を新規の tivcmd CLI 鍵データベースに追加します。

このステップでは、公開署名者証明書が tivcmd CLI コンピューター上のロケーションに置かれていることを前提としています。例えば、C:¥policyauthcerts¥PolicyAuthSignerCert.arm または C:¥policyauthcerts¥CASignerCert.arm です。このステップでは、このロケーションは *<policyauthsignercert>* として示されます。

次のコマンドを使用して、公開署名者証明書を新規の tivcmd CLI 鍵データベースに追加します。

```
<gskittoolcmd> -cert -add -db <newkeydb> -pw <newkeydbpw>
-label "Authorization Policy Signer Certificate" -trust enable
-format ascii -file <policyauthsignercert> -fips
```

5. 各 tivcmd CLI コンピューターで TLS/SSL 証明書の交換を有効にします。

各 tivcmd CLI コンピューターで以下の手順を行って、公開署名証明書を使用する TLS/SSL 証明書の交換を有効にします。

a. 現在の鍵データベースを削除します。*<keydbdir>* ディレクトリーの *<oldkeydbname>*.* ファイルを削除します。

b. 新しい鍵データベース・ファイルの名前をすべて変更します。例えば、*<keydbdir>* ディレクトリーの *<newkeydbname>*.* を *<oldkeydbname>*.* に変更します。

c. 許可ポリシー・サーバー証明書の認証を有効にするよう、環境変数を設定します。

- Windows: KDEBE_KEY_LABEL 変数の後に変数 ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y を追加して、tivcmd CLI 環境ファイル *<authclidir>*¥KDQ¥bin¥KDQENV を編集します。
- Linux および UNIX: KDEBE_KEY_LABEL 変数の後に変数 export ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y を追加して、tivcmd CLI 環境ファイル *<authclidir>*/bin/tivcmd を編集します。

ポータル・サーバーおよび許可ポリシー・サーバー間の TLS/SSL 通信の構成

TLS/SSL を構成するには、Tivoli 許可ポリシー・サーバーが使用する公開署名者証明書をポータル・サーバーの TEPS/e トラストストアに追加します。

注: 許可ポリシー・サーバーの新しいデジタル証明書を要求した場合は、その証明書を受け取ってからこの手順を実行します。

始める前に

TEPS/e 管理コンソール が使用可能であることを確認します。ログオンする方法を含む詳細な手順については、 118 ページの『TEPS/e 管理コンソールの開始』を参照してください。

このタスクについて

このステップでは、公開署名者証明書がポータル・サーバー・コンピューター上に置かれていることを前提としています。例えば、
`C:¥policyauthcerts¥PolicyAuthSignerCert.arm` または
`C:¥policyauthcerts¥CASignerCert.arm` です。この手順では、このロケーションは <*policyauthsignercert*> として示されます。

手順

1. TEPS/e 管理コンソール にログオンします。
2. 「**セキュリティー**」→「**SSL 証明書および鍵管理**」を選択します。
3. 「関連項目」領域で、「**鍵ストアと証明書**」リンクをクリックし、表内の「**NodeDefaultTrustStore**」リンクをクリックします。
4. 「追加プロパティー」領域で、「**署名者証明書**」リンクをクリックし、表示されたページで「**追加**」をクリックします。
5. 表示されたページで次の情報を指定します。
   - 「**別名**」を証明書の適切なラベルに設定します。例えば、`許可ポリシー・サーバー Signer Certificate` です。
   - 「**ファイル名**」を、公開署名者証明書のロケーションに設定します。例えば、<*policyauthsignercert*> です。
   - 「**データ・タイプ**」は「**Base64 エンコード ASCII データ**」のままにします。
6. 「**OK**」、「**保存**」の順にクリックします。
7. 許可ポリシー・サーバー接続に HTTP ではなく HTTPS を使用するように、ポータル・サーバーを再構成します。許可ポリシー・サーバー接続パラメーターの再構成について詳しくは、 210 ページの『ポータル・サーバーでの許可ポリシーの使用可能化』を参照してください。

タスクの結果

これで、許可ポリシー・サーバーとポータル・サーバーの間で HTTPS が使用されるようになりました。

IBM Tivoli Monitoring 用に FIPS を使用可能にする

連邦情報処理標準 (FIPS) を使用できるように IBM Tivoli Monitoring コンポーネントを構成する必要があります。

手順

以下のコンポーネントで構成を行ないます。

- ポータル・サーバー

- モニター・サーバーおよびモニター・エージェント
- モニター・オートメーション・サーバー
- ウェアハウス・プロキシー
- 要約およびプルーニング
- ウェアハウス・データベース
- ポータル・クライアント
- tacmd コマンド行インターフェース
- tivcmd コマンド行インターフェース

注:

ベスト・プラクティスは、変更内容が確実に実装されるように、いかなるコンポーネントの再構成も、環境変数の編集後に行うということです。

Jazz for Service Management を IBM Tivoli Monitoring とともに使用する場合は、Jazz for Service Management インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.psc.doc_1.1.0/psc_ic-homepage.html)にある「*Jazz for Service Management*インストール・ガイド」で、そのコンポーネントで FIP を使用可能にする方法について参照してください。

ポータル・サーバーの構成:

1. ポータル・サーバーがインストールされているコンピューター上の Tivoli Enterprise Portal Server 環境ファイルを編集します。

   Windows KFWENV ファイルを編集します。

   Linux UNIX cq.ini ファイルを編集します。

   以下の環境変数を変更または追加します。

   KDEBE_FIPS_MODE_ENABLED=YES

   KFW_FIPS_ENFORCED=YES

   KFW_JAVA_PARMS を変更して -Dcom.ibm.crypto.provider.FIPSMODE=true を追加
2. java.security ファイルを編集します。次のコマンドを実行します。

   Windows

   cd *<ITM_dir>*¥*<install_dir >*

   CandleGetJavaHome.bat (JRE ロケーションを取得するため)

   notepad *<JRE_location>*¥lib¥security¥java.security

   Linux UNIX

   cd *<ITM_dir>*/*<install_dir >*

   CandleGetJavaHome (JRE ロケーションを取得するため)

   edit *<JRE_location>*/lib/security/java.security

   以下のようにプロバイダー・リストを変更します。

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL

com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

3. Windows <*ITM_dir*>¥CNPSJ¥java¥jre¥lib¥security¥java.securityファイルを編集します。

   Linux UNIX <*ITM_dir*>/<*platform*>/iw/java/jre/lib/security/java.security を編集します。

   以下のようにプロバイダー・リストを変更します。

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

   該当する場合は、WebSphere Socket Factories をコメント化し、以下の変数を設定します。

```
com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

モニター・サーバーおよびモニター・エージェントの構成:

1. 以下の環境ファイルを編集します。

   Windows KBBENV ファイルを編集し、モニター・エージェントごとに KXXENV ファイルを編集します (ここで、*XX* は 2 文字の製品コードです)。

   Linux UNIX モニター・サーバー上の ms.ini を編集し、モニター・エージェントごとに *.ini を編集します。

   以下の環境変数を変更または追加します。

   KDEBE_FIPS_MODE_ENABLED=YES

   オートノマス・エージェントを使用している場合は、上記の変数をカスタム環境ファイルに追加する必要があります。

モニター・オートメーション・サーバー

1. Tivoli Enterprise Monitoring Automation Server 環境ファイルを編集します。

   Windows KASENV ファイルを編集します。

   Linux UNIX オートメーション・サーバーがインストールされているコンピューターの as.ini ファイルを編集します。

2. 以下の環境変数を変更または追加します。

KDEBE_FIPS_MODE_ENABLED=YES

ウェアハウス・プロキシーの構成:

1. 以下の環境ファイルを編集します。

   Windows KHDENV ファイルを編集します。

   Linux UNIX hd.ini ファイルを編集します。

   以下の環境変数を変更または追加します。

   KDEBE_FIPS_MODE_ENABLED=YES

   KHD_JAVA_ARGS を変更して -Dcom.ibm.crypto.provider.FIPSMODE=true を追加

要約およびプルーニング・エージェントの構成:

1. java.security ファイルを編集します。次のコマンドを実行します。

   Windows

   cd <*ITM_dir*>¥<*install_dir* >

   CandleGetJavaHome.bat (JRE ロケーションを取得するため)

   notepad <*JRE_location*>¥lib¥security¥java.security

   以下のようにプロバイダー・リストを変更します。

```
security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.crypto.provider.IBMJCE
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.security.sasl.IBMSASL

com.ibm.jsse2.JSSEFIPS=true
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

2. 以下の環境ファイルを編集します。

   Windows KSYENV ファイルを編集します。

   Linux UNIX sy.ini ファイルを編集します。

   KSZ_JAVA_ARGS を変更して -Dcom.ibm.crypto.provider.FIPSMODE=true を追加

ウェアハウス・データベースの構成:

ウェアハウス・データベースの構成はインストール済み環境に固有で、この構成の適用範囲外にあります。TLS/SSL を使用してデータベース・サーバーにアクセスするように ODBC クライアントを構成する必要があります。FIPS 140-2 モードでデータベースを実行するための構成リンクを以下にリストします。

- MSSQL 2005

  FIPS 140-2 モードで実行されるように Microsoft SQL Server を構成する方法の詳細については、以下の Microsoft 知識ベースの記事を参照してください。
  http://support.microsoft.com/kb/920995 を参照してください。

- DB2® v9.1 フィックスパック 2 以降

  DB2 9.1 フィックスパック 2 およびそれ以降の場合、TLS/SSL 接続は常に FIPS 140-2 モードです。TLS/SSL ODBC 接続の構成についてさらに詳しく調べるには、以下の IBM 支援資料を参照してください。 http://www-01.ibm.com/support/docview.wss?uid=swg21249656 を参照してください。

- Oracle

  Oracle 10g (9.0.4) またはそれ以降の FIPS 140-2 モードでの構成については、以下の支援資料を参照してください。http://download.oracle.com/docs/cd/B14099_19/core.1012/b13999/fips.htm を参照してください。

ポータル・クライアントの構成:

1. cnp.bat ファイルを編集します。_CMD 行を編集して以下の定義を含めるようにします。

   ```
   -Dcom.ibm.crypto.provider.FIPSMODE=true
   -Dcom.ibm.TEPS.FIPSMODE=true
   ```

   このフラグは、非 FIPS JCE プロバイダーの機能を X509CertificateFactory および鍵ストア JKS/JCEKS 機能に限定します。

   Windows <*ITM_dir*>¥CNP¥cnp.batファイルを編集します。

   Linux UNIX 次のコマンドを使用します。

   ```
   set _CMD= %_JAVA_CMD% -Xms64m -Xmx256m -showversion -noverify -
   classpath %CPATH% -Dcom.ibm.crypto.provider.FIPSMODE=true -
   Dcom.ibm.TEPS.FIPSMODE=true -Dkjr.trace.mode=LOCAL -
   Dkjr.trace.file=C:¥IBM¥ITM¥CNP¥LOGS¥kcjras1.log -Dkjr.trace.params=ERROR -
   DORBtcpNoDelay=true -Dibm.stream.nio=true -Dcnp.http.url.host=9.42.15.121 -
   Dvbroker.agent.enableLocator=false -Dnv_inst_flag=%NV_INST_FLAG% -
   Dnvwc.cwd=%NVWC_WORKING_DIR% -Dnvwc.java=%NVWC_JAVA%
   candle.fw.pres.CMWApplet %1 %2 %3 %4 %5 %6 %7 %8 %9 %10
   ```

2. java.security ファイルを編集します。次のコマンドを実行します。

   Windows

   cd <*ITM_dir*>¥<*install_dir* >

   CandleGetJavaHome.bat (JRE ロケーションを取得するため)

   notepad <*JRE_location*>¥lib¥security¥java.security

   以下のようにプロバイダー・リストを変更します。

   ```
   security.provider.1=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.3=com.ibm.crypto.provider.IBMJCE
   security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.5=com.ibm.security.cert.IBMCertPath

   com.ibm.jsse2.JSSEFIPS=true
   ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
   ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
   ```

3. FIPS 140-2 で実行されるようにポータル・クライアントを再構成します。

   cnp.bat ファイルを編集して - Dcom.ibm.crypto.provider.FIPSMODE=true を追加します。

注: Windows の場合、com.ibm.TEPS.FIPSMODE プロパティーを true に設定することによって、ポータル・クライアントが部分的に構成される場合があります。

tacmd コマンド行インターフェースの構成:

Windows

1. <*ITM_dir*>¥BIN¥KUIENV ファイルを編集します。

   以下の環境変数を変更または追加します。

   TEPS_FIPS_MODE=YES

   KDEBE_FIPS_MODE_ENABLE=YES

Linux UNIX

1. <*ITM_dir*>/bin/ tacmd シェル・スクリプトを編集します。

   以下の環境変数を変更または追加します。

   export TEPS_FIPS_MODE=YES

   export KDEBE_FIPS_MODE_ENABLE=YES
2. java.security ファイルを編集します。次のコマンドを実行します。

   cd *<ITM_dir>¥<Install_dir>*

   CandleGetJavaHome.bat (JRE ロケーションを取得するため)

   notepad *<JRE_location>*¥lib¥security¥java.security

   以下のようにプロバイダー・リストを変更します。

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.7=com.ibm.security.cmskeystore.CMSProvider
security.provider.8=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

tivcmd コマンド行インターフェースの構成:

Windows

1. <*tivcmd_install_dir*>¥BIN¥KDQENV ファイルを編集します。

   以下の環境変数を変更または追加します。

   KDEBE_FIPS_MODE_ENABLE=YES

Linux UNIX

1. <*tivcmd_install_dir*>/bin/tivcmd シェル・スクリプトを編集します。

   以下の環境変数を変更または追加します。

   export KDEBE_FIPS_MODE_ENABLE=YES

結果

これで、FIPS 140-2 レベル 1 に準拠した構成を実行するようになりました。

次の作業

FIPS 140-2 モードの場合、Tivoli Management Services コンポーネントおよび Tivoli Enterprise Monitoring Agent は、FIPS 140-2 承認暗号プロバイダーである IBMJCEFIPS (証明書 497)、IBMJSSEFIPS (証明書 409)、および IBM Crypto for C (ICC (証明書 775)) を 1 つ以上暗号に使用します。これらの証明書は、NIST の Web サイト (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) でリストされています。

すべての IP.SPIPE 接続および TLS/SSL 対応 LDAP 接続は、TLS 1.0 プロトコルのみを使用します。Tivoli Enterprise Portal クライアントと Tivoli Enterprise Portal Server との間では TLS/SSL が使用可能になっている必要があります。これについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」のトピック『ポータル・サーバーとクライアント間の SSL の使用』で説明しています。 TLS/SSL の使用可能化に失敗すると、資格情報が公開される恐れがあります。

FIPS 140-2 準拠の暗号を使用してデータの完全性と機密性を保持するには、すべての IBM Tivoli Monitoring コンポーネント間で IP.SPIPE を使用可能にします。IP.SPIPE 通信で使用される証明書には、NIST および FIPS で規定された暗号強度が必要です。 89 ページの『第 5 章 ユーザー認証の使用可能化』では、暗号証明書の置き換え方法について詳しく説明しています。ご使用の環境で、提供されている GSKit ユーティリティーが使用されている場合は、すべての操作に `-fips` フラグを含める必要があります。FIPS 140-2 準拠について詳しくは、ローカルのセキュリティー管理者に問い合わせていただくか、または NIST の Web サイトを参照してください。

関連資料:

http://www-01.ibm.com/software/sysmgmt/products/support/IBMTivoliMonitoring.html
IBM Tivoli Monitoring サポートで、FIPS 140-2 準拠のコンポーネントの構成に関するガイドラインを検索します。

http://csrc.nist.gov/
米国連邦情報・技術局のコンピューター・セキュリティー部門には、FIPS 140-2 準拠に関する資料があります。

ポータル・サーバーの鍵ファイル・データベースへの TEPS/e 証明書のインポート

ポータル・サーバーがインストールされているコンピューター上にカスタム鍵ファイル・データベースを作成していて、そのカスタム鍵ファイル・データベースに新しい自己署名または CA 署名の IBM Tivoli Monitoring 証明書が含まれている場合、TEPS/e が使用する証明書も新しい鍵ファイル・データベースにインポートする必要があります。これにより、TEPS/e と Tivoli Enterprise Portal Server Web サーバー・プラグインは保護された接続を介して内部で通信できるようになります。

このタスクについて

TEPS/e 証明書をポータル・サーバーの IBM Tivoli Monitoring 鍵ファイル・データベースに手動でインポートするには、以下の手順を実行します。

手順

1. コマンド・プロンプト (Windows) またはシェル (AIX または Linux) を開きます。
2. 251 ページの『GSKit 向けの JRE の設定および Key Manager の起動』で説明されているとおりに *JAVA_HOME* 変数を設定します。ただし、GSKit Key Manager は始動しないでください。
3. GSKit ホーム・ディレクトリーの下の bin ディレクトリーに移動します。
4. 次のコマンドを実行します。
   - Windows
     ```
     <gskittoolcmd> -cert -import -file ../../cnpsj/profiles/itmprofile/
     config/cells/itmcell/nodes/itmnode/default-signers.p12 -pw WebAS -type
     pkcs12 -target ../../keyfiles/keyfile.kdb -target_pw <password>
     -target_type cms
     <gskittoolcmd> -cert -import -file ../../cnpsj/profiles/itmprofile/
     config/cells/itmcell/nodes/itmnode/key.p12 -pw WebAS -type pkcs12
     -target ../../keyfiles/keyfile.kdb -target_pw <password> -target_type
     cms
     ```
   - Linux AIX
     ```
     ./<gskittoolcmd> -cert -import -file ../../../<arch>/profiles/
     itmprofile/config/cells/itmcell/nodes/itmnode/default-signers.p12 -pw
     WebAS -type pkcs12 -target ../../../keyfiles/keyfile.kdb -target_pw
     <password> -target_type cms
     ./<gskittoolcmd> -cert -import -file ../../../<arch>/profiles/
     itmprofile/config/cells/itmcell/nodes/itmnode/key.p12 -pw WebAS -type
     pkcs12 -target ../../../keyfiles/keyfile.kdb -target_pw <password>
     -target_type cms
     ```

     <password> は、鍵ファイル・データベースのパスワードです。 Linux システムと AIX システムの場合、*<arch>* は、ポータル・サーバーがインストールされているアーキテクチャー・サブディレクトリーです。*<gskittoolcmd>* は、GSKit ツールを開始するコマンドです。
5. ポータル・サーバーを再始動します。

GSKit コマンド行インターフェースによる鍵データベースおよび証明書の操作

GSKit コマンド行ツールは、各 IBM Tivoli Monitoring コンポーネントと共に分散プラットフォームにインストールされ、鍵ファイルおよび証明書を管理するために使用されます。

GSKit コマンド行インターフェースについて詳しくは、「*IBM Global Security Kit GSKCapiCmd V8.0 User's Guide*」を参照してください。

事前処理

次の表に、GSKit に関連する手順で使用する用語を示します。ほとんどの用語は、IBM Tivoli Monitoring コンポーネントおよび GSKit がインストールされるディレクトリーに基づいています。

<*authclidir*> IBM Tivoli Monitoring コンポーネントのインストール先ディレクトリー。例:

- `c:¥IBM¥ITM` または `/opt/IBM/ITM` (モニター・サーバー、オートメーション・サーバー、ポータル・サーバー、tacmd CLI、およびエージェントの場合)
- `c:¥IBM¥TivoliMonitoring` または `/opt/IBM/TivoliMonitoring` (tivcmd CLI の場合)

<*interp*> マシン固有の interp。例えば、sol296、li6263、または aix536 です。

<*gskithome*> GSKit のインストール先ディレクトリー。

Windows 32 ビット: <*itmcompdir*>¥GSK8.

Windows 64 ビット: <*itmcompdir*>¥GSK8_64.

Linux および UNIX 32 ビット: <*itmcompdir*>/<*interp*>/gs

Linux および UNIX 64 ビット: <*itmcompdir*>/<*interp*>/gs

<*gskittoolcmd*> 実際の GSKit CLI コマンド構文。

Windows 32 ビット: <*gskithome*>¥bin¥gsk8capicmd.exe

Windows 64 ビット: <*gskithome*>¥bin¥gsk8capicmd_64.exe

Linux および UNIX 32 ビット: ./<*gskithome*>/bin/gsk8capicmd.exe

Linux および UNIX 64 ビット: ./<*gskithome*>/bin/gsk8capicmd_64.exe

<*keydbdir*> デフォルトの鍵データベースの保管先ディレクトリー。

Windows: <*itmcompdir*>¥keyfiles

Linux および UNIX: <*itmcompdir*>/keyfiles

<*oldkeydbname*> IBM Tivoli Monitoring コンポーネントと共にインストールされた鍵データベースのベース名。このベース鍵データベース名は keyfile です。この鍵データベースには、keyfile.crl、keyfile.kdb、keyfile.rdb、および keyfile.sth の 4 つのファイルが関連付けられています。

<*oldkeydb*> IBM Tivoli Monitoring コンポーネントと共にインストールされた鍵データベースの名前。この鍵データベース名は <*oldkeydbname*>.kdb です。

<*oldkeydbpw*> インストールされている鍵データベースのパスワード。デフォルトは IBM61TIV です。

<*newkeydbname*> 新しい鍵データベースのベース名。 keyfile 以外の任意の名前を選択できます。例えば、itmcompkeyfile です。

<*newkeydb*> 新しい鍵データベースの名前。この鍵データベース名は <*newkeydbname*>.kdb です。

<*newkeydbpw*> 新しい鍵データベースに関連付けられたパスワード。任意の有効パスワードを選択できます。

GSKit コマンド行ツールを起動するためのパスの設定

GSKit コマンド行ツールを実行するために、GSKit ツールの lib ディレクトリーをシステム・パスに含める必要があります。

Windows **32 ビット**

```
set PATH=<gskithome>¥lib;%PATH%
cd <gskithome>¥bin
```

Windows **64 ビット**

```
set PATH=<gskithome>¥lib64;%PATH%
cd <gskithome>¥bin
```

Linux UNIX **32 ビット**

```
export LD_LIBRARY_PATH=<gskithome>/lib:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

Linux UNIX **64 ビット**

```
export LD_LIBRARY_PATH=<gskithome>/lib64:$LD_LIBRARY_PATH
cd <gskithome>/bin
```

GSKit iKeyman ユーティリティーによる鍵データベースおよび証明書の操作

デフォルトの自己署名証明書および鍵は、IBM Tivoli Monitoring をインストールしたときに提供されます。認証局の署名済み証明書を使用する場合は、iKeyman ユーティリティーを使用して証明書要求を作成してから、鍵データベースを作成し、証明書をデータベースにインポートします。

注: iKeyman ユーティリティーは、モニター・サーバー、ポータル・サーバー、ポータル・クライアント・デスクトップ・クライアント、および tacmd CLI がインストールされている分散コンピューター上で使用できます。

iKeyman グラフィカル・ユーザー・インターフェースおよびそのコマンド行インターフェースについて詳しくは、「*IBM Developer Kit and Runtime Environment iKeyman V8.0 User's Guide*」を参照してください。

GSKit 向けの JRE の設定および Key Manager の起動

GSKit を起動する前に Java ランタイム環境へのパスを設定する必要があります。

この設定を行わないと、Failed to parse JAVA_HOME setting のようなエラーが表示されることがあります。

手順

- Windows
  1. コマンド・プロンプトから、以下のスクリプトを実行し、 IBM Java の場所を検出します。

     install_dir ¥InstallITM¥GetJavaHome.bat
  2. IBM Java の場所を指す JAVA_HOME 変数を設定します。
  3. 以下のスクリプトを実行し、GSKit の場所を検出します。

     install_dir ¥InstallITM¥GetGSKitHome.bat
  4. 以下のコマンドを実行します。

```
$JAVA_HOME¥jre¥bin¥ikeyman.exe [properties]
```

[properties] には、0 個以上のシステム・プロパティーを指定できます。

- AIX Linux Solaris
  1. コンソールから、以下のスクリプトを実行し、 IBM Java の場所を検出します。

     ```
     install_dir /bin/CandleGetJavaHome.sh
     ```
  2. IBM Java パスを指す変数 JAVA_HOME をエクスポートします。
  3. 以下のコマンドを実行します。

     ```
     $JAVA_HOME¥jre¥bin¥ikeyman.exe [properties]
     ```

     [properties] には、0 個以上のシステム・プロパティーを指定できます。
- HP-UX
  1. コンソールから、以下のスクリプトを実行し、 IBM Java の場所を検出します。

     ```
     install_dir /bin/CandleGetJavaHome.sh
     ```
  2. IBM Java パスを指す変数 JAVA_HOME をエクスポートします。64 ビットの場合、gsk7ikm が 64 ビット Java である必要があります。
  3. 以下のファイルを調べ、ローカル GSKit のパスを確認します。

     ```
     install_dir /config/gsKit.config
     ```

     GskitInstallDir は 32 ビット GSKit を指し、GskitInstallDir_64 は 64 ビット GSKit を指します。
  4. 以下のコマンドを実行して、IBM 鍵管理を (X Windows システムを必要とするグラフィカル・ユーティリティーを介して) 起動します。

     ```
     GskitInstallDir/bin/gsk7ikm_32
     ```

新規鍵データベースの作成

iKeyman ユーティリティーを使用して新しい鍵データベースを作成します。

このタスクについて

新規鍵データベースを作成するには、以下のステップを実行します。

1. まだ起動していない場合は、iKeyman を起動します。
2. 「**鍵データベース・ファイル**」→「**新規**」をクリックします。
3. 「**鍵データベース・タイプ**」フィールドで「**CMS**」を選択します。
4. 「**ファイル名**」フィールドに keyfile.kdb と入力します。
5. 「**位置**」フィールドに次の位置を入力します。*<itm_installdir>*/keyfiles
6. 「**OK**」をクリックします。 「パスワード・プロンプト」ウィンドウが表示されます。
7. 「**パスワード**」フィールドにパスワードを入力し、「**パスワードの確認**」フィールドでパスワードを再度確認します。「**OK**」をクリックします。
8. 確認ウィンドウが表示されます。「**OK**」をクリックします。

「IBM 鍵管理」ウィンドウが表示されます。このウィンドウでは、新しい CMS 鍵データベース・ファイルおよび署名者のデジタル証明書が反映されます。

新規公開鍵と秘密鍵のペアおよび認証要求の作成

公開鍵と秘密鍵の新規ペアおよび認証要求を iKeyman で作成します。

このタスクについて

新規の公開鍵と秘密鍵のペアおよび認証要求を作成するには、以下のステップを実行します。

手順

1. まだ起動していない場合は、iKeyman を起動します。
2. 「**鍵データベース・ファイル**」→「**オープン**」をクリックします。
3. keyfile.kdb 鍵データベースを選択して、「**オープン**」をクリックします。
4. 鍵データベースに対応するパスワードを入力して、「**OK**」をクリックします。
5. プルダウン・リストから「**個人証明書要求**」 を選択して、「**新規**」をクリックします。
6. 「**新規**」をクリックします。
7. 「**鍵ラベル**」フィールドに `IBM_Tivoli_Monitoring_Certificate` と入力します。
8. 「**共通名**」および「**組織**」を入力し、「**国**」を選択します。その他のフィールドでは、デフォルト値を受け入れるか、新しい値を入力または選択します。
9. ウィンドウの下部に、ファイルの名前を入力します。
10. 「**OK**」をクリックします。 確認ウィンドウが表示され、新しいデジタル証明書の要求を作成したことが確認されます。
11. 「**OK**」をクリックします。

タスクの結果

「IBM 鍵管理」ウィンドウが表示されます。

次のタスク

認証局 (CA) にファイルを送信して、新しいデジタル証明書を要求するか、CA の Web サイト上の要求フォームに要求をカット・アンド・ペーストします。

自己署名証明書の一時的な使用

CA 署名デジタル証明書を受信するには、2 から 3 週間かかる場合があります。IBM Tivoli Monitoring に付属しているもの以外のデジタル証明書を使用することを希望し、CA 署名のデジタル証明書をまだ受信していない場合は、ポータル・サーバー上で自己署名証明書を作成することができます。自己署名デジタル証明書は CA 署名証明書ほど安全性が確保されていません。つまり、厳密には、CA 署名証明書を入手するまでの一時的な手段です。

このタスクについて

自己署名証明書を作成して使用するには、以下の手順を実行します。

手順

1. CA 鍵データベースを作成します。
2. 自己署名証明書を作成します。
3. 自己署名証明書をエクスポートします。
4. ポータル・サーバー上の鍵データベースに自己署名証明書を受信します。

次のタスク

CA 署名証明書を受信する場合は、自己署名証明書を削除する必要があります。

CA 署名証明書の受信

このタスクについて

CA から新しいデジタル証明書が返送されたら、ポータル・サーバーが稼働しているコンピューター上にそのデジタル証明書を保存します。クライアントでもこの操作を繰り返します。CA から電子メール・メッセージの一部として証明書が返送される場合は、証明書をコピーして、電子メールからテキスト・ファイルに貼り付けます。

CA から各コンピューター上の鍵データベースにデジタル証明書を受信するには、次の手順を実行します。

手順

1. まだ起動していない場合は、iKeyman を起動します。
2. 「**鍵データベース・ファイル**」→「**オープン**」をクリックします。
3. keyfile.kdb データベースを選択して、「**オープン**」をクリックします。
4. データベースに対応するパスワードを入力して、「**OK**」をクリックします。
5. プルダウン・リストから「**個人証明書**」を選択します。
6. 「**受信**」をクリックします。
7. 「**データ・タイプ**」をクリックして、「**Base64 エンコード ASCII データ**」など新しいデジタル証明書のデータ・タイプを選択します。
8. 「**証明書ファイル名**」に `keyfile.sth` と入力し、新しいデジタル証明書の「**位置**」として `<itm_installdir>/keyfiles` を入力します。
9. 「**OK**」をクリックします。
10. 新しいデジタル証明書に `IBM_Tivoli_Monitoring_Certificate` と入力し、「**OK**」をクリックします。

パスワードを stash ファイルに保存する

IBM Tivoli Monitoring コンポーネントの多くはユーザーの介入なく機能するので、コンピューター上の stash ファイルに鍵データベースのパスワードを保存する必要があります。このパスワードを保存すると、ユーザーの介入なしで製品コンポーネントが TLS/SSL を使用できるようになります。

このタスクについて

パスワードを stash ファイルに保存するには、以下の手順を実行します。

手順

1. まだ起動していない場合は、iKeyman を起動します。
2. 「**鍵データベース・ファイル**」→「**Stash ファイル**」を選択します。 パスワードが stash ファイルに保存されたことを示す情報ウィンドウが表示されます。
3. 「**OK**」をクリックします。

第 9 章 監査ロギング

監査機能を使用すると、ご使用の IBM Tivoli Monitoring 環境で発生している重要なイベントをキャプチャーすることができます。これらのイベントを永続ストレージに記録しておき、後から取り出して分析することも可能です。各監査レコードには、IBM Tivoli Monitoring システムの状態を変化させたイベントが詳しく記述されます。

これらの監査レコードおよびログ・レコードは、Tivoli Data Warehouse に保管できます。標準レポートは、Tivoli Common Reporting 機能によって提供されます。

監査機能は、自己記述型エージェント (自動最新表示機能を含む)、ウェアハウス・プロキシー・エージェントのアクション、EIF-SSL 接続、自動化されたアクションの実行コマンド、および IBM Tivoli Monitoring と Tivoli Application Dependency Discovery Manager の統合を対象とします。

対応プラットフォームには、Windows、Linux、UNIX、IBM i、および z/OS のシステムがあります。

監査レコードは、次の 2 カ所に格納されます。

ポータル・クライアントからアクセス可能な、収集済み ITM 監査属性データ

管理対象システム状況ワークスペースで、モニター・コンポーネントを右クリックし、「監査ログ」を選択することで、そのコンポーネントの収集済み監査ログ情報を表示できます。その後、ITM 監査 テーブルに対するシチュエーションを作成して、Tivoli Data Warehouse で監査対象イベントのモニターと監査データのヒストリカル収集を行うことができます。

監査情報を調べる際には、値がゼロでない「結果」を探してください。値 0 は成功を表します。「結果」の値がゼロでないレコードをモニターするシチュエーションを作成すれば、一般情報メッセージをフィルターで除外するのに役立ちます。

Tivoli Enterprise Portal ユーザーズ・ガイド には、ITM 監査属性グループおよびワークスペースに関する詳しい情報が記載されています。監査ログ・ワークスペースと ITM 監査属性グループのヒストリカル収集を有効にする方法について詳しくは、管理対象システム状況ワークスペースを参照してください。属性の定義については、ITM 監査属性を参照してください。

ローカルに保存される XML フォーマットのログ・ファイル

ログ・ファイルは、サード・パーティー製品で監査情報の解析と評価を行うために使用できます。サード・パーティー製品を使用する際には、提供されている SAPM DTD を使用してください。DTD は、IBM Tivoli Monitoring ツール DVD の `XML` ディレクトリーで提供されています (`SAPMAudit.dtd` ファイルを参照してください)。

ログ・ファイルは、<install_dir> ディレクトリーの下の auditlogs ディレクトリーに保管されます。エージェント・プロセスごとに独自のログ・ファイルがあり、XML 形式になっています。以下のログ・ファイル名を参照してください。

Windows Linux UNIX

単一インスタンスの場合: *<UserID>.<hostname>_<pc>*_audit.log

マルチインスタンスの場合:
*<UserID>.<hostname>_<pc>_<instance>*_audit.log

IBM i

/QIBM/ProdData/IBM/ITM/support

z/OS

ログは SMF 機能から収集されます。

使用可能になっている場合、ITM 監査レコードはシステム管理機能フォーマット (SMF) のタイプ 112 レコードに、UTF8 でコード化されて書き込まれます。このタイプ 112 のレコードは、他のすべての z/OS イベント・データとともに共通のリポジトリー (SYS1.MANn データ・セット) に組み込まれています。詳しくは、*Tivoli Enterprise Monitoring Server on z/OS の構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm)を参照してください。

監査トレース・レベル

監査イベントには、最小、基本、および詳細の 3 つのトレース・レベルがあります。すべてのイベントにトレース・レベルが割り当てられます。トレース・レベルを増減させて追加のデータを収集できます。

最小: 製品の主要な状態変更

基本: オブジェクトを変更する、またはアクセス障害の原因となるすべてのアクション

詳細: アクセス制御が成功または失敗する原因となったすべてのアクション

イベント・レコード・タイプ

レコード・タイプは、各監査イベントに関連付けられ、監査レコードの特性を示します。次の表にイベント・レコード・タイプの分類を示します。

イベントのフルネーム	ショート・ネーム (ログに表示される)	説明
許可検査	CHECKING	特定の操作またはイベントを実行する権限がユーザーにあるかどうかのチェックに関連するイベント。
認証検証	VALIDATE	ユーザーまたはエンティティーの ID の認証に関連するイベント。

イベントのフルネーム	ショート・ネーム (ログに表示される)	説明
コンテキスト・イベント	CONTEXT	アプリケーション内で状況により発生する可能性があるその他のイベント。
オブジェクト保守	OBJMAINT	オブジェクトの変更に関連するイベント。例えば IBM Tivoli Monitoring のオブジェクトまたは表の更新、削除、作成、または移動などがあります。
システム管理	SYSADMIN	プログラムの開始とシャットダウン、監査と許可のシステム変更、構成変更、表の作成、およびデータの同期構成に関連するイベント。
セキュリティー保守	SECMAINT	特権の認可または取り消しに関連するイベント。

ITM 監査属性グループにマップされる監査ログの XML 要素

監査ログの XML には、ITM 監査属性に対応付けられる要素が含まれます。

XML 構文の詳しい情報については、IBM Tivoli Monitoring ツール DVD の `SAPMAudit.dtd` を参照してください。

属性については、ITM 監査属性を参照してください。

次の表を参照してください。

注:

- 監査ログの XML 構造を表すために、一部のセルは意図的にブランクにされています。空になっている ITM 監査属性のセルは、その対応する XML エレメントの対応属性がまだ作成されていないことを示します。
- 括弧 ( ) 内の XML エレメントと XML 属性は、IBM Tivoli Monitoring では実装されていないことを示します。
- *「特殊属性」は、XML 要素または属性が Name=Value ペアとして「監査ログ」表の「特殊属性」列に挿入されることを意味します。

論理グループ	XML 要素	XML 属性	ITM 監査属性
AuditEvt	AuditEvt	Domain	ドメイン
		Level	トレース・レベル
		Type	イベント・レコード・タイプ
		Ver	監査レコードのバージョン

論理グループ	XML 要素	XML 属性	ITM 監査属性
Who	AuthID		許可 ID
		(Repository)	
	RunAs		実行
		(Repository)	
	UserID		ユーザー ID
		(Repository)	
	Entity		エンティティー
		Type	エンティティー・タイプ
What	Op	(CDMID)	
		Name	操作名
		Type	操作タイプ
		OpObjType	操作オブジェクト・タイプ
	Msg	Text	メッセージ
		RBKey	リソース・バンドル・キー
	Param		特殊属性*
		Order	特殊属性*
	Result		結果
When	Corr		相関関係子
	Seq		シーケンス
	EvtTS	MS	タイム・スタンプ (ミリ秒)
		ITM	タイム・スタンプ
		(UTC)	
	(LogTS)		

論理グループ	XML 要素		XML 属性	ITM 監査属性
OnWhat	Obj		Type	オブジェクト・タイプ
			(Ver)	オブジェクト・バージョン
			Name	オブジェクト名
			(CDMID)	特殊属性*
			Path	オブジェクト・パス
	(SecMaint)	Grantee	Type	
		SecPolicy		
		Constraint		
	(SecPolicy)			セキュリティー・ポリシー名
	(Grantee)			付与対象
			Type	付与対象タイプ
	(PriAuthEvt)			特権または権限のイベント
			Type	特権または権限のタイプ
			AuthID	仮定権限 ID
			Repository	
	(AuthVal)			
	(AuthCheck)			特殊属性*
	(AuthPlugin)		Type	許可プラグイン・タイプ
			Server	特殊属性*
Where	Origin	Node	Name	起点名
			Type	起点タイプ
			AddrType	起点プロトコル
			Addr	起点アドレス
			Host	起点ホスト名
			Port	起点ポート
			SYSID	起点
	App		Code	アプリケーション・コード
			Ver	アプリケーション・バージョン
			Comp	アプリケーション・コンポーネント
	SvcPt			サービス・ポイント

論理グループ	XML 要素		XML 属性	ITM 監査属性
WhereFrom	Source	Node	Name	ソース名
			Type	ソース・タイプ
			AddrType	ソース・プロトコル
			Addr	ソース・アドレス
			Host	ソース・ホスト名
			Port	ソース・ポート
			SYSID	ソース
	Relay	Node	Name	
			Type	
			AddrType	
			Addr	
			Host	
			Port	
			SYSID	
WhereTo	Target	Node	Name	ターゲット名
			Type	ターゲット・タイプ
			AddrType	ターゲット・プロトコル
			Addr	ターゲット・アドレス
			Host	ターゲット・ホスト名
			Port	ターゲット・ポート
			SYSID	ターゲット

監査ログの XML 例

以下の監査レコード例は開始時に生成されたもので、特定のモニター・サーバーの自己記述型エージェント・サービスが無効になっていることを示しています。

```
<AuditEvt Domain="" Type="SYSADMIN" Level="Minumum" Ver="1">
 <Who>
  <UserID/>
  <AuthID>SYSTEM</AuthID>
 </Who>
 <What>
  <Op Name="Self-Describing Agent Status"
   OpObjType="ibm-prod-tivoli-itm:SelfDescribingAgentInstall" Type="Disable"/>
  <Msg Text="Self-Descrbing Agent Feature disabled at the local TEMS."
   RBKey="KFASD010"/>
  <Result>0</Result>
 </What>
 <When>
```

```
 <EvtTS MS="1307723083106" ITM="1110610162443106"/>
 <Seq>1</Seq>
</When>
<OnWhat>
 <Obj Type="ibm-prod-tivoli-itm:SelfDescribingAgentInstall" Name="SDA Services"/>
</OnWat>
<Where>
 <Origin>
  <Node Name=Tivoli Enterprise Monitoring Server" Type="SERVER" AddrType="IPv4"
   Addr="10.1.1.1" SYSID="HUB_NC051039"/>
 </Origin>
 <App Code="KMS" Ver="06.23.00" Comp="KFA"/>
 <SvcPt>system.nc051039_ms</SvcPt>
</Where>
<WhereFrom>
 <Source>
  <Node Name="Tivoli Enterprise Monitoring Server" Type"SERVER" SYSID="HUB_NC051039"
   Addr="10.1.1.1" AddrType="IPv4"/>
 </Source>
</WhereFrom>
<WhereTo>
 <Target>
  <Node Name="Tivoli Enterprise Monitoring Server" Type="SERVER" AddrType="IPv4"
   Addr="10.1.1.1" SYSID="HUB_NC051039"/>
 </Target>
</WhereTo>
</AuditEvt>
```

この例では、次のような質問に回答できます。

質問	タグ	値	解釈
Who	UserID	空	空の UserID タグは、このイベントが不明な UserID か、ユーザーによって直接開始されたのではないアクションを実行するオートノマス・プロセスによって生成されたことを示しています。
	AuthID	SYSTEM	このイベントに許可を与えた ID を示します。
What	Op	Self-Describing Agent Status	「Self-Describing Agent Status」の操作は正常に完了しており (結果が 0)、説明メッセージは自己記述型エージェント機能が使用不可になったことを示しています。
	Msg	Self-Describing Feature disabled at the local TEMS.	
	Result	0	
	Type	Disable	この特定の操作が一般的な「使用不可」タイプであることを示しています。操作は通常、見れば明らかに分かるようになっていますが、Tivoli Security and Information Event Manager で指定されているとおり、すべて総称イベント・モデル・タイプ (GEM) に分類されています。
When	ITM	1110610162443106	イベントが生成された日時 (ログに記録された時間ではありません)。協定世界時 (UTC) のフォーマット (CYYMMDDhhmmssms) で記録されます。この日時は、2011 年 6 月 10 日 04:24:43 106 ミリ秒を意味します。

質問	タグ	値	解釈
OnWhat	Name	SDA Services	オブジェクト名は、その操作を受ける対象となるコード、コンポーネント、あるいはその他の文脈的に適切な ID です。この例では、オブジェクト「SDA Services」が操作「Self-Describing Agent Status」を受け取っており、その操作はオブジェクト「SDA Services」に対して正常に完了しました (結果の値は 0)。
Where	SYSID	HUB_NC051039	これは、イベントのログが記録された場所です。管理対象システム ID HUB_NC051039 (IP 10.1.1.1) 上の KMS アプリケーションがこのイベントを記録しました。このシステム自体は Tivoli Enterprise Monitoring Server として識別されます。
	Addr	10.1.1.1	
	Name	Tivoli Enterprise Monitoring Server	
	App	KMS	
WhereFrom	SYSID	HUB_NC051039	このイベントは、MSN HUB_NC051039 (IP 10.1.1.1) 上で開始されました。このシステム自体は Tivoli Enterprise Monitoring Server として識別されます。
	Addr	10.1.1.1	
	Name	Tivoli Enterprise Monitoring Server	
WhereTo	SYSID	HUB_NC051039	このイベントは、MSN HUB_NC051039 (IP 10.1.1.1) をターゲットとしています。ターゲット・システムは Tivoli Enterprise Monitoring Server として識別されます。
	Addr	10.1.1.1	
	Name	Tivoli Enterprise Monitoring Server	

監査の環境変数

環境変数を変更して監査機能を制御できます。

環境変数

次の環境変数は監査機能の構成用に定義されています。

環境変数	説明	受け入れ可能な入力	定義されない場合のデフォルト
AUDIT_FILE	xml audit.log の作成を無効にするために使用します。監査イベントは引き続き ITM 監査表に作成されます。	• Disabled • Enabled **注:** Not Supported は、入力としては受け入れられず、監査ログを作成しないプラットフォーム (z/OS システムなど) で返される可能性がある状態です。	Enabled

環境変数	説明	受け入れ可能な入力	定義されない場合のデフォルト
AUDIT_LOG_DIR _PATH	監査ログ・ファイルが保持されるディレクトリーへのパス。z/OS システムでは使用不可です。**注:** 出力ディレクトリーを変更すると、pdcollect ツールは関連付けられた監査ログを収集できません。	オペレーティング・システムの特定のパスを指定します。	<*install_dir*>/auditlogs
AUDIT_LOG_FILE _LIMIT_MB	ログ・ファイルの最大サイズ (メガバイト (2^20 バイト) 単位)。	1 - MAXINT-1	9
AUDIT_LOG_FILE _NAME	ログ・ファイル名。z/OS システムでは使用不可です。	ログ・ファイル名を指定します。	<*UserID*>.<*hostname*> _<*pc*>_audit.log
AUDIT_LOG_MAX _FILES_COUNT	ロールオーバーするログ・ファイルの最大数。この変数は分散プラットフォームにのみ適用されます。 z/OS システムでは使用不可です。	1...MAXINT-1 (分散の場合)	5
AUDIT_MAX_HIST	直接照会のために短期メモリー内に保持するレコードの最大数。	1...MAXINT-1	100
AUDIT_TRACE	メッセージを受け渡すためのトレース・レベル。メッセージのトレース・レベルは、(低いものから順に) Minimum、Basic、Detail です。上位レベルでは、それより下位のすべてのレベルがトレースされます。	• Minimum • Basic • Detail • Disabled	Basic

環境変数	説明	受け入れ可能な入力	定義されない場合のデフォルト
ITM_DOMAIN	これらのレコードとの関連づけを行う際にオプションで使用される、分散システム上の 128 文字の ID および z/OS 上の 32 文字の ID。相互に関連付けられているエージェントを一般的に識別する場合に最適です。この変数を使用して、特定の顧客でレコードをソートできます。大/小文字の区別があります。	プラス (+)、マイナス (-)、セミコロン (;)、およびコロン (:) の文字を含む可能性のある英数字ストリング。	ドメインは提供されません。

監査の環境変数の変更

次の手順で、監査機能のトレースの環境変数を構成できます。前述のどの環境変数も変更することができます。

Windows

Tivoli Enterprise Monitoring Services の管理 (「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」) を使用して、環境ファイルを編集します。変更するコンポーネントを右クリックして、「**拡張**」→「**ENV ファイルの編集**」をクリックします。変更内容を実装するには、コンポーネントをリサイクルする必要があります。

Linux UNIX

1. *<install_dir>*/config ディレクトリーに移動し、次の調整ファイルを開きます。

   モニター・サーバーの場合: *<hostname>*_ms_*<tems_name>*.config

   ポータル・サーバーおよび単一インスタンス・エージェントの場合: *<pc>*.ini

   マルチインスタンス・エージェントの場合: *<pc>*_*<instance>*.config
2. 新規の行に、環境変数に続けて値を追加します。例えば、AUDIT_TRACE=BASIC などです。
3. ファイルを保存して閉じます。
4. コンポーネントを再開して、変更内容を有効にします。

z/OS

詳しくは、「*Tivoli Enterprise Monitoring Server on z/OS の構成*」を参照してください。

アクション実行およびコマンド実行監査ロギング

IBM Tivoli Monitoring V6.3 以降を使用している場合は、アクション実行および **tacmd executecommand** の実行に対して監査レコードが生成されます。アクション実行の実行に含まれるものには、 Tivoli Enterprise Portal から開始されるアクション実行、 **tacmd executeaction** コマンドの実行、シチュエーションのアクション実行コマンド、およびワークフロー・ポリシーのアクション実行コマンドがあります。アクション実行を開始したユーザーの ID が、セキュア・セッション・トークンを使用することによってモニター・エージェントに渡されます。

セッション・トークンは、共通の IBM Tivoli Monitoring 暗号鍵、および IBM Tivoli Monitoring サーバーとモニター・エージェントの間の時間の同期を利用します。暗号鍵が同期しないと、すべてのコマンドは ID の検証エラーによって無効として拒否されます。ポータル・サーバー (Tivoli Enterprise Portal ユーザーの場合) またはハブ・モニター・サーバー (tacmd コマンド・ユーザーの場合) とターゲットのモニター・エージェントとの間で Universal Coordinated Time (UTC) によるシステム時間のずれが 25 分を超えると、コマンドは許可タイムアウトのため無許可として拒否されます。

シチュエーションのアクション実行の実行およびワークフロー・ポリシーのアクション実行の実行では、最後にシチュエーションまたはワークフロー・ポリシーを変更したユーザーの ID が記録されます。

監査メッセージは、モニター・エージェントの監査ログまたは Tivoli Enterprise Portal から、監査ログの履歴データとして、またはリアルタイム照会によって入手できます。

TEMS セキュリティー互換モードでは、IBM Tivoli Monitoring V6.3 よりも前のバージョンのサーバー・コンポーネントで、Tivoli Enterprise Monitoring Agent Framework V6.3 以降を使用するモニター・エージェントに対してコマンドを実行したりアクション実行を行うことができます。TEMS セキュリティー互換モードが有効でなく、V6.3 よりも前のポータル・サーバーまたはモニター・サーバーを使用している場合、アクション実行または **tacmd executecommand** コマンドは、無許可であるとして拒否されて監査の対象になる可能性があります。TEMS セキュリティー互換モードが有効な場合は、元のユーザーの ID が監査レコードに記録されない可能性があります。ベスト・プラクティスとしては、インフラストラクチャーを IBM Tivoli Monitoring V6.3 以降にアップグレードし、最大限のセキュリティーを確保するために TEMS 互換モードを無効にして、アクション実行および **tacmd executecommand** の実行の ID が適切に監査されるようにします。

また、AAGP ポリシーを使用することにより、管理対象システムに対してアクション実行または **tacmd executecommand** を実行できるユーザーを制御することもできます。詳しくは、 444 ページの『アクセス許可グループ・プロファイル』を参照してください。

第 10 章 Tivoli Enterprise Console を使用したシチュエーション・イベントの統合

モニター環境に Tivoli Enterprise Console event serverが含まれており、ハブ Tivoli Enterprise Monitoring Server でシチュエーション・イベントの転送が構成されている場合は、Tivoli Enterprise Monitoring Agent によって生成されたシチュエーション・イベントをイベント・サーバーに転送できます。

「*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)」に、シチュエーション・イベントの転送を有効にするための説明 (イベントを受信するイベント・サーバーの構成、イベント・サーバーへのイベント同期コンポーネントのインストール、ハブ・モニター・サーバーでのシチュエーション転送の使用可能化、およびデフォルトの Event Integration Facility (EIF) 宛先の定義) が記載されています。

シチュエーション・イベントから IBM Tivoli Enterprise Console イベントへのデフォルト・マッピング

このセクションでは、シチュエーション・イベントから IBM Tivoli Enterprise Console イベントへの属性マッピングに関する情報を示します。このマッピング情報は、シチュエーション・イベントを IBM Tivoli Enterprise Console に転送する際に、IBM Tivoli Enterprise Console で相関ルールを作成する必要がある場合に使用できます。

シチュエーション・イベントの転送機能によって、そのシチュエーションと関連付けられた属性グループに基づくイベント・クラスを持つ IBM Tivoli Enterprise Console イベントが生成されます。シチュエーション・イベントをイベント・サーバーに転送すると、生成される関連イベント・クラスは、その親である *Omegamon_Base* クラスからイベント・クラス属性定義を (直接または間接に) 継承します。 IBM Tivoli Enterprise Console では階層イベント・クラスが使用されるため、イベント・サーバーに転送するすべてのシチュエーション・イベントに関してルールを作成する必要がある場合は、 Omegamon_Base 親クラスを使用してください。

Omegamon_Base は以下のように記述されます。

```
Omegamon_Base ISA EVENT
DEFINES {
   cms_hostname: STRING;
   cms_port: STRING;
   integration_type: STRING;
   master_reset_flag: STRING;
   appl_label:STRING;
   situation_name: STRING;
   situation_origin: STRING;
   situation_displayitem: STRING;
   situation_time: STRING;
   situation_status: STRING;
   situation_eventdata: STRING;
```

```
situation_type: STRING;
situation_thrunode: STRING;
 situation_group: STRING;
 situation_fullname: STRING;  }; END;
```

シチュエーション・イベントが既存の IBM Tivoli Enterprise Console イベント・クラスにマップされ、イベント階層を変更できない (Omegamon_Base を階層に追加できない) という特殊なケースの場合には、Omegamon_Base のスロットを階層内のいずれかの既存のイベント・クラスまたはクラスに組み込むことが重要です。この仕組みは、ルールによって、イベント階層内の Omegamon_Base の存在が認識されないという理由から、お勧めできません。

これらのシチュエーションの汎用マッピングの一環として、IBM Tivoli Monitoring イベント転送機能は、イベントを Tivoli Enterprise Console event server に転送するときにイベント・クラス属性で定義されている属性の関連値を割り当てます。これらのイベント・クラス属性のほかにも、可能な場合は、EVENT クラスから継承される属性 (ソース、ホスト名、fqhostname、発信元、副発信元、アダプター・ホスト、発信元、重大度、基本 EVENT クラスから継承されるメッセージ属性) に値が割り当てられます。

表 26. IBM Tivoli Enterprise Console イベント・クラス属性

イベント・クラス属性	**値と意味**
アダプター・ホスト	基本イベント・クラス属性。ホスト名と同じです (以下を参照)。 これは、イベントに関連したアプリケーション固有データです (ある場合)。
アプリケーション・ラベル	将来の使用のために予約済み。
cms ホスト名	イベントを転送する Tivoli Enterprise Monitoring Server の TCP/IP ホスト名。
cms ポート	Web サービスが listen しているモニター・サーバー・ポート。
fqhostname	完全修飾ホスト名を含む基本 EVENT クラス属性 (ある場合)。
ホスト名	イベントが発生した管理対象システムの TCP/IP ホスト名を含む基本 EVENT クラス属性 (使用可能な場合)。
統合タイプ	IBM Tivoli Enterprise Console パフォーマンスを支援するインディケーター。 • N は新規イベントを示します (イベントが初めて発生したとき)。 • U は更新イベントを示します (後続のイベント状況の変更)。
マスター・リセット・フラグ	マスター・リセット・イベント用に設定されるマスター・リセット・インディケーター。その他のすべてのイベントの場合、値は NULL です。 • R は Tivoli Enterprise Monitoring Server のリサイクル master_reset を示します。 • S はホット・スタンバイ・マスター・リセットを示します。
メッセージ	シチュエーション名と式を含む基本 EVENT クラス属性。

表 26. IBM Tivoli Enterprise Console イベント・クラス属性 (続き)

イベント・クラス属性	値と意味
発信元	イベントが発生した管理対象システムの TCP/IP アドレスに含まれる基本 EVENT クラス属性 (使用可能な場合)。このアドレスは、小数点付き 10 進数の形式です。
重大度	解決された重大度を含む基本 EVENT クラス属性。
シチュエーションの表示項目	関連するシチュエーションの表示項目 (使用可能な場合)。
シチュエーション・イベント・データ	イベント・データの 2 行目から開始される未加工のシチュエーション・イベント・データ (ある場合)。イベント・データ属性は、キーと値のペア形式です。Event Integration Facility のサイズ制限が 2 KB のため、イベント・データは切り捨てられる場合があります。
シチュエーションのグループ	シチュエーションがメンバーとなっている、1 つ以上のシチュエーションのグループ名 (5 つ以内)。
シチュエーションのフルネーム	関連するシチュエーションの表示名
シチュエーション名	シチュエーションに与えられた固有 ID。
シチュエーションの発信元	シチュエーション・イベント発信元である管理対象システムの名前。サブソースと同じ値です。
シチュエーションの状況	シチュエーション・イベントの現在の状況。
シチュエーション・タイム	シチュエーション・イベントのタイム・スタンプ。
シチュエーション・タイプ	シチュエーション・イベント・タイプは、サンプル・イベントの場合は **S**、ピュア・イベントの場合は **P** です。
シチュエーション thrunode	将来の使用のために予約済み。
ソース	**ITM** を含む基本 EVENT クラス属性。
サブ発信元	基本イベント・クラス属性。これは、関連シチュエーション表示項目の管理対象システム名と同じです (ある場合)。
サブソース	関連するシチュエーションの発信元の管理対象システム名を含む基本 EVENT クラス属性。

汎用イベント・メッセージのシチュエーションの記述の拡張

メッセージ・スロットでは、IBM Tivoli Enterprise Console 内のイベントの詳細を調べることができます。

さまざまなソースからの類似イベントが多数ある場合、シチュエーション名だけではイベントを詳細に識別できません。むしろ、ハブ・モニター・サーバーからイベント・サーバーに送信されたメッセージ・スロット内のシチュエーション名は、以下のイベント属性を組み込むように拡張されています。

Situation-Name [(formula) ON Managed-System-Name ON DISPLAY-ITEM (threshold Name-Value pairs)]

値の説明:

Situation-Name
シチュエーションの名前。

formula
シチュエーションの評価方法を示す式。

Managed-System-Name
エージェントまたは管理対象システム。

DISPLAY-ITEM
複数のインスタンスがある場合、シチュエーションをトリガーした ID。これはオプションであり、シチュエーション定義に表示項目が指定された場合にのみ使用されます。

threshold Name-Value pairs
シチュエーションをトリガーするかどうかの評価にシチュエーションが使用する未加工データ。

```
Examples:
NT_Critical_Process [(Process_CPU > 4 AND Thread_Count > 50)
  ON IBM-AGX02:NT
  (Process_CPU = 8 AND Thread_Count = 56)]

NT_Disk_Full [(Free_Megabytes < 1000000)
  ON "IBM-AGX02:NT"
  ON D: (Free_Megabytes = 100)]
```

エージェント固有スロットの汎用マッピング

汎用マッピングでは、トリガーされてイベント・サーバーに転送されるシチュエーションからの情報に基づいてターゲット・イベント・クラスを特定します。

IBM Tivoli Enterprise Console イベントのイベント・クラス名は、シチュエーションに関連する属性グループから派生します。このイベント・クラス名は、**ITM_** と、シチュエーションに関連する属性グループ名を組み合わせたものです。例えば、NT_Process 属性グループを使用するシチュエーションの場合、クラス *ITM_NT_Process* を持つ IBM Tivoli Enterprise Console イベントが生成されます。

注: 一部のエージェントは大変長い属性グループ名を持つため、生成されたイベント・クラス名がイベント・サーバーによって課せられている制限を越える場合があります。このような場合、イベント・クラス名は **ITM_** と、属性グループのテーブル名を組み合わせたものです。

追加のイベント・スロット値には、シチュエーション・イベント・データからのシチュエーション属性値が取り込まれます。スロット名は、特殊文字処理後の属性名です。

例えば、Process_CPU 属性を使用するシチュエーションの場合は、IBM Tivoli Enterprise Console イベント内にスロット process_cpu が生成されます。属性名が IBM Tivoli Enterprise Console EVENT クラスまたは Omegamon_Base クラス内のスロット名と競合する場合は、属性グループに関連づけられた *applname* (例: *knt_*) を属性名の前に付けたものをスロット名にします。

複合シチュエーションの場合、シチュエーション定義に複数の属性グループを含めることができます。この場合、使用される IBM Tivoli Enterprise Console イベント・クラスは、トリガー・シチュエーションのシチュエーション・イベント・データで検出される最初の属性グループから導き出されます。検出された最初の属性グ

ループがローカル時間または世界時の場合は例外です。この属性グループは使用されず、該当する場合は、次の別の属性グループが使用されます。

例えば、NT_Process 属性グループと NT_System 属性グループに関するシチュエーションが作成される場合に、NT_Process が最初の属性グループであれば、IBM Tivoli Enterprise Console イベント・クラス *ITM_NT_Process* が使用されます。追加のイベント・スロットは、選択された属性グループの属性に基づいて生成されます。

表 27. 転送されたシチュエーション・イベントから生成された IBM Tivoli Enterprise Console イベントでの属性グループおよび属性名の特殊文字

文字:	**変換後の文字:**
<大文字> (属性名にのみ適用される)	<小文字> (属性名にのみ適用される)
% (パーセント記号)	pct_
I/O	io
R/3	r3
/ (スラッシュ)	_per_
¥ (バックスラッシュ)	_ (下線)
<スペース>	_ (下線)
(始め括弧) 終わり括弧	_ (下線)
< 不等号 (より小) > 不等号 (より大)	_ (下線)

注: 特殊文字の処理後に、最終イベント・クラスまたはスロット名の先頭および末尾の下線があれば、それらは削除されます。

Tivoli Enterprise Console イベントの重大度の割り当て

シチュエーションと関連付けられた Tivoli Enterprise Console イベントの重大度は、シチュエーション名から自動的に割り当てられます。または、Tivoli Enterprise Portal シチュエーション・エディターで重大度を設定することもできます。

シチュエーションに関連付けられている Tivoli Enterprise Console イベントの重大度は、シチュエーション・エディターの「EIF」タブで直接指定できます。 Tivoli Enterprise Console の重大度がシチュエーションに指定されていない場合、イベント転送機能は次のルールを使用してシチュエーション名のサフィックスから重大度を導き出そうとします。

表 28. シチュエーション名のサフィックスから Tivoli Enterprise Console イベント重大度へのマッピング

シチュエーション名のサフィックス	**割り当てられる IBM Tivoli Enterprise Console 重大度**
Warn または _Warning	WARNING
Cri、_Crit、_Critical	CRITICAL
上記のいずれでもない	UNKNOWN

メッセージ・スロットのローカライズ

KMS_OMTEC_GLOBALIZATION_LOC 変数を編集して、Tivoli Enterprise Console event serverによってアラート要約にマップされる EIF イベント・メッセージ・スロットのグローバリゼーションを有効にすることができます。

このタスクについて

一部の製品には、イベント・マッピング・ファイルおよび言語バンドルが同梱されています。これらの定義済み IBM Tivoli Enterprise Console イベントのメッセージ・スロットは、グローバル化されています。言語の選択は、KMS_OMTEC_GLOBALIZATION_LOC と呼ばれる Tivoli Enterprise Monitoring Server 環境変数を介して行われます。

デフォルト時、この変数は米国英語に設定されており、メッセージ・スロットには米国英語のメッセージが入っています。ご使用の環境にインストールされている言語パックの 1 つを有効にするには、この変数を編集します。

手順

1. 次のようにして、ハブ Tivoli Enterprise Monitoring Server がインストールされているコンピューターで KBBENV ファイルを開きます。
   - Windows 「Tivoli Monitoring Services の管理」を開始し、「**Tivoli Enterprise Monitoring Server**」を右クリックして、「**拡張**」→「**ENV ファイルの編集**」をクリックします。
   - Linux UNIX テキスト・エディターで *<install_dir>*/config/*<tems_name>*_ms_*<address>*.cfg ファイルを開きます。ここで、*<tems_name>* は、モニター・サーバー構成中に提供された値で、*<address>* は、コンピューターの IP アドレスまたは完全修飾名です。
2. KMS_OMTEC_GLOBALIZATION_LOC 環境変数を位置指定 (追加) し、希望の言語および国別コードを入力します。ここで、xx は言語、XX は国別コードで、次のものがあります。de_DE、 en_US、 en_GB、 es_ES、 fr_FR、 it_IT、 ja_JP、 ko_KR、 pt_BR、 zh_CN、または zh_TW (ブラジル・ポルトガル語の場合は pt_BR、中国語 (簡体字) の場合は zh_CN など)。

   ```
   KMS_OMTEC_GLOBALIZATION_LOC=xx_XX
   ```
3. モニター・サーバー環境ファイルを保存して閉じます。

シチュエーション・イベント状況および IBM Tivoli Enterprise Console イベントの生成

このトピックでは、シチュエーション・イベント状況の意味と、生成された IBM Tivoli Enterprise Console イベントでの共通スロットの設定を示します。

シチュエーションが true である

統合タイプ: 最初にシチュエーションが true になった場合は N、それ以降のすべてのときは U。

シチュエーション状況: Y

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: シチュエーション定義で表示項目として選択された属性の値 (ある場合)

マスター・リセット・フラグ: なし

シチュエーションのリセット (既に true ではない)

統合タイプ: U

シチュエーション状況: N

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: シチュエーション定義で表示項目として選択された属性の値 (ある場合)

マスター・リセット・フラグ: なし

確認

統合タイプ: U

シチュエーション状況: A

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: シチュエーション定義で表示項目として選択された属性の値 (ある場合)

マスター・リセット・フラグ: なし

シチュエーションの開始

統合タイプ: なし

シチュエーション状況: S

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: なし

マスター・リセット・フラグ: なし

IBM Tivoli Enterprise Console イベントは転送されません。

シチュエーションの停止

統合タイプ: U

シチュエーション状況: P

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: なし

マスター・リセット・フラグ: なし

このTivoli Enterprise Monitoring Serverから発信されたすべての開いているシチュエーション・イベントが、イベント・サーバーで閉じられます。

シチュエーションの開始エラー

統合タイプ: なし

シチュエーション状況: X

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: なし

マスター・リセット・フラグ: なし

IBM Tivoli Enterprise Console イベントは転送されません。

有効期限が切れた確認

統合タイプ: U

シチュエーション状況: F

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: シチュエーション定義で表示項目として選択された属性の値 (ある場合)

マスター・リセット・フラグ: なし

確認で指定された有効期限が切れました。

再表示

統合タイプ: U

シチュエーション状況: E

シチュエーション名: シチュエーションの名前

シチュエーション表示項目: シチュエーション定義で表示項目として選択された属性の値 (ある場合)

マスター・リセット・フラグ: なし

確認通知は、期限が切れる前に削除されました。シチュエーションは true のままです。

ハブの開始

統合タイプ: なし

シチュエーション状況: N

シチュエーション名: “**'

シチュエーション表示項目: なし

マスター・リセット・フラグ: R

ハブ・モニター・サーバーが開始されると、マスター・リセット・イベントが situation_status=N で送信されます。マスター・リセットにより、イベント・サーバーはハブ・モニター・サーバー (cms_hostname の値) の開いているシチュエーション・イベントをすべて閉じます。

ハブの再始動

統合タイプ: なし

シチュエーション状況: N

シチュエーション名: “**'

シチュエーション表示項目: なし

マスター・リセット・フラグ: R

ハブ・モニター・サーバーが開始されると、マスター・リセット・イベントが situation_status=N で送信されます。マスター・リセットにより、イベント・サーバーはハブ・モニター・サーバー (cms_hostname の値) の開いているシチュエーション・イベントをすべて閉じます。

ハブのスタンバイ・フェイルオーバー

統合タイプ: なし

シチュエーション状況: N

シチュエーション名: “**”

シチュエーション表示項目: なし

マスター・リセット・フラグ: S

ハブ・モニター・サーバーの切り替えが発生すると、ホット・スタンバイ・マスター・リセット・イベントが situation_status=N で送信されます。 マスター・リセットにより、イベント・サーバーはハブ・モニター・サーバーからのすべての開いているシチュエーション・イベントを閉じます。古い 1 次ハブの名前は、**シチュエーション発信元**スロット内にあります。

注: **統合タイプ**の値は、そのパフォーマンスを向上させるために、IBM Tivoli Enterprise Console 同期規則のみによって使用されます。イベントに関連した意味は他にありません。

シチュエーション・イベントの同期化

イベント同期コンポーネントである Event Integration Facility (EIF) は、Tivoli Enterprise Console イベント・サーバーに転送されるシチュエーション・イベントへの更新情報を Tivoli Enterprise Monitoring Server に送り返します。シチュエーション・イベント・コンソール、共通イベント・コンソール、および Tivoli Enterprise Console イベント・ビューは、イベントの更新状況と同期されます。サポートされるイベント管理システムからのイベント・データを Tivoli Enterprise Console イベント・ビューまたは共通イベント・コンソール・ビューでモニターする場合、転送されたイベントをフィルターで除去することができます。

IBM Tivoli Enterprise Console イベント・キャッシュの確認

イベント・サーバーのルール・イベント・キャッシュは、常に、予想されるイベントのボリュームを格納するだけの十分な大きさでなければなりません。

稼働中のイベント・サーバーのルール・キャッシュ・サイズを確認するには、以下の IBM Tivoli Enterprise Console コマンドを実行します。

```
wlsesvrcfg -c
```

このルール・キャッシュ・サイズを設定するには、以下の IBM Tivoli Enterprise Console コマンドを実行します。

```
wsetesvrcfg -c number_of_events
```

注: この 2 つのコマンドについて詳しくは、「*Tivoli Enterprise Console コマンドとタスクのリファレンス* 」の『イベント・サーバー・コマンド』を参照してください。

ルール・イベント・キャッシュがフルになると、IBM Tivoli Enterprise Console ルール・エンジンは TEC_Notice イベント「**ルール・キャッシュがフル: クリーニングを強制実行しました (Rule Cache full: forced cleaning)**」を生成します。これは、イベントの 5 % がキャッシュから削除されたことを示します。イベントは経過時間の順に削除されます。つまり、最も古いイベントが先に削除されるので、より新しいイベントを処理できるようになります。

ハブ・モニター・サーバーが Tivoli Enterprise Console event server に以前に転送したシチュエーション・イベントの状況更新を転送するときに、オリジナルのシチュエーション・イベントがルール・イベント・キャッシュから削除されている場合

は、モニター・サーバーとイベント・サーバーが同期していないことを示す TEC_ITM_OM_Situation_Sync_Error イベントが生成されます。

任意の IBM Tivoli Enterprise Console ビューアーを使用して任意のシチュエーション・イベントを確認または閉じるときに、シチュエーション・イベントがルール・イベント・キャッシュから削除されている場合、その状況変更は IBM Tivoli Enterprise Console ルール・エンジンによって処理されません。また、シチュエーション・イベント更新は発信元の Tivoli Enterprise Monitoring Server に転送されません。このように動作するのは、ルール・イベント・キャッシュに含まれていないイベントに関して IBM Tivoli Enterprise Console ルール・エンジンがイベント状況変更を処理しないためです。この場合、イベント状況変更は IBM Tivoli Enterprise Console データベース内でのみ更新されます。

両方のシチュエーションを改善するには、IBM Tivoli Enterprise Console サーバー構成パラメーター分析およびパフォーマンス分析を実行して、最適な構成パラメーター設定および望ましいパフォーマンス要件を判断します。詳しくは、「*IBM IBM Tivoli Enterprise Console ルール開発者ガイド* 」の『ルール・エンジンの概要』を参照してください。

イベント・サーバー上のイベント同期の構成の変更

イベント・サーバー上のイベント同期の設定を変更する必要がある場合は、**sitconfig.sh** コマンドを使用します。

このタスクについて

以下のいずれかのオプションを使用してこのコマンドを実行できます。

手順

- イベント同期の構成ファイル (デフォルトでは `situpdate.conf` という名前のファイルで、UNIX 系オペレーティング・システムの場合には `/etc/TME/TEC/OM_TEC` ディレクトリーにあり、Windows の場合には %SystemDrive%¥Program Files¥TME¥TEC¥OM_TEC¥etc ディレクトリーにあります) を手動で変更した後、次のコマンドを実行します。

  ```
  sitconfig.sh update <config_filename>
  ```

- 変更が必要な設定のみを指定して、**sitconfig.sh** コマンドを直接実行する。このコマンドの完全な構文については、「*IBM Tivoli Monitoring: コマンド解説書*」を参照してください。

次のタスク

イベント同期の構成を変更した後に、`$BINDIR/TME/TEC/OM_TEC/bin` ディレクトリーから **stopSUF** および **startSUF** コマンドを使用して、シチュエーション更新転送機能プロセスを手動で停止して再始動する必要があります。

イベント・サーバー上のイベント同期用の追加モニター・サーバーの定義

シチュエーション・イベントをイベント・サーバーに転送する各モニター・サーバーについての必要なサーバー情報を定義し、シチュエーション更新転送機能プロセスでシチュエーション・イベントの更新情報を発信元のモニター・サーバーに転送できるようにする必要があります。

このタスクについて

以下のコマンドを実行して、新規のモニター・サーバー情報を追加します。

```
sitconfsvruser.sh add serverid=server userid=user password=password
```

値の説明:

serverid=*server*
モニター・サーバーの完全修飾ホスト名。

userid=*user*
モニター・サーバーが稼働中のコンピューターにアクセスするユーザー ID。

password=*password*
コンピューターにアクセスするためのパスワード。

追加する各モニター・サーバーについて、このコマンドを繰り返し実行します。

次のタスク

イベント同期の構成を変更した後に、`$BINDIR/TME/TEC/OM_TEC/bin` ディレクトリーから **stopSUF** および **startSUF** コマンドを使用して、シチュエーション更新転送機能プロセスを手動で停止して再始動する必要があります (Windows の場合は .cmd ファイル拡張子、UNIX 系オペレーティング・システムの場合は .sh です)。

サンプル・イベントのクローズ

サンプル・シチュエーションからのシチュエーション・イベントが IBM Tivoli Enterprise Console イベント・サーバーに転送され、続けてイベントが イベント・サーバー で閉じられると、イベント同期の動作により、要求が Tivoli Enterprise Monitoring Server に送信され、指定されたタイムアウトでシチュエーションを確認します。これは、サンプル・シチュエーションのイベントを閉じると、IBM Tivoli Monitoring でのクローズの後に起動するシチュエーションの機能に問題が生じるためです。

このタスクについて

シチュエーションの確認通知が期限切れであり、シチュエーションが true のままである場合は、IBM Tivoli Enterprise Console で新規シチュエーション・イベントが開かれます。シチュエーションが false になった場合は、IBM Tivoli Monitoring でそれ自体をリセットし、イベントは IBM Tivoli Enterprise Console で閉じたままになります。

デフォルトの確認通知有効期限は、59 分です。これは、イベント・サーバー上のシチュエーション・タイムアウト構成ファイル (sit_timeouts.conf) で変更できます。また、個々のシチュエーションの有効期限を、このファイルで構成できます。このファイルを編集した後に、$BINDIR/TME/TEC/OM_TEC/bin で sitconfig.sh リフレッシュ・コマンドを使用して、有効期限を動的に IBM Tivoli Enterprise Console ルールにロードできます。

omegamon.rls ルール・セット・ファイルのルール・セット・パラメーターの変更

omegamon.rls ルール・セット・ファイルには、環境に応じてユーザーが編集できるパラメーターがあり、これによってパフォーマンスの調整や、ユーザー独自のカスタマイズ値の設定ができます。これらのパラメーターを使用すると、IBM Tivoli Enterprise Console ルールの作成およびカスタマイズが可能になります。ユーザーはインストール時にルール・ベースのロケーションを選択できます。あるいは、wrb -lscurrb -path を使用して、現在のルール・ベースを検索できます。

ルールの動作を変更する理由を以下にいくつか示します。

- omegamon.rls ファイルの場合、ルール・セットの名前は *omegamon_admin* ですが、管理者の名前または他の値にちなんでルール・セットに名前を付けることができます。
- 同様に、*sit_ack_expired_def_action* ルール・セット名はデフォルトで REJECT に設定されています。この設定は、Tivoli Enterprise Portal でシチュエーション・イベントの確認通知が期限切れになり、イベントがポータルで OPEN になったときは常に、IBM Tivoli Enterprise Console イベント・サーバーがこのアクションを拒否し、ポータルでイベントを再確認することを意味します。ユーザーは、ポータルによって開始された変更を受け入れて、代わりに IBM Tivoli Enterprise Console での状況を変更することができます。

使用可能なユーザーが構成可能なパラメーターは以下のとおりです。

omegamon_admin
この ID は、このルール・セットに定義されたルールがイベントを閉じるときに使用します。この ID は、コンソール・オペレーターによって開始されたクローズ操作ではなく、自動的に発生したクローズ操作を区別するのに使用されます。

omsync_timeout
この属性には、単一イベントと複数イベントの同期を区別するために待機する必要のある期間 (秒) を設定します。デフォルトのタイムアウトは 3 秒です。

omsync_maxentries
この属性には、バッチ当たりで許可されるイベントの最大数を設定します。デフォルトのバッチ・サイズは 100 イベントです。

警告: この値を 20 イベントよりも小さく設定すると、IBM Tivoli Enterprise Console タスク・プロセス内で競合が発生し、それによってイベントを同期化して Tivoli Enterprise Monitoring Server に戻す処理のパフォーマンスが低下する可能性があります。

sit_resurface_def_action
この属性は、シチュエーション更新イベントが Tivoli Enterprise Monitoring Server から到着して、すでに確認済みのイベントを再表示または再オープンする場合のルールのデフォルト・アクションを決定します。可能な値は ACCEPT と REJECT の 2 つです。デフォルトは ACCEPT です。

sit_ack_expired_def_action
この属性は、シチュエーション更新イベントが Tivoli Enterprise Monitoring Server から到着して、すでに確認済みのイベントを再オープンする場合のルールのデフォルト・アクションを決定します。このような状況は、モニター・サーバーでのシチュエーションの確認通知が期限切れになり、シチュエーション・イベントが再オープンされるときに発生します。可能な値は ACCEPT と REJECT の 2 つです。デフォルトは REJECT です。

sf_check_timer
この属性には、シチュエーション更新転送機能の状態をチェックする間隔を指定します。この転送機能により、キャッシュ・ファイルからイベントが読み取られ、Web サービスを使用して Tivoli Enterprise Monitoring Server にイベントが送信されます。デフォルトは 10 分です。

構成パラメーターを変更して omegamon.rls を保存したら、ルール・ベースを再コンパイルおよび再ロードして、イベント・サーバーをリサイクルする必要があります。ルール・ベースを再コンパイルするには、以下のコマンドを入力します。ここで Rulebase_Name とは、omegamon.rls ルール・セットを含むアクティブにロードされたルール・ベースの名前です。

```
wrb -comprules Rulebase_Name
```

ルール・ベースを再ロードするには、以下のコマンドを実行します。

```
wrb -loadrb Rulebase_Name
```

イベント・サーバーを停止するには、以下のコマンドを実行します。

```
wstopesvr
```

イベント・サーバーを再始動するには、以下のコマンドを実行します。

```
wstartesvr
```

wrb、wstopesvr、および wstartesvr コマンドについて詳しくは、Tivoli Enterprise Console インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.itec.doc_3.9/welcome_nd.html)の「*コマンドとタスクのリファレンス*」を参照してください。

チューニング考慮事項

統合パラメーターがサポートする IBM Tivoli Enterprise Console イベント・コンソールでのアクションは Tivoli Enterprise Portal イベント・コンソールに反映されるので、適正なシステム・リソース投資による優れた応答時間が実現されます。

考慮すべきチューニング・パラメーターは以下のとおりです。

- omegamon.rls 内の omsync_timeout。デフォルトは 3 秒。
- イベント同期の PollingInterval。デフォルトは 3 秒。

- IBM Tivoli Enterprise Console イベント・コンソールの最新表示間隔。デフォルトは 60 秒。
- Tivoli Enterprise Portal イベント・コンソールの最新表示間隔。

注: より短い間隔にすると、より多くのシステム・リソースが消費されます。

シチュエーション変更を IBM Tivoli Enterprise Console イベント・コンソールから Tivoli Enterprise Portal イベント・コンソールに送信する時間は、並行して作用する `omsync_timeout` と `PollingInterval` の設定値によって決まります。応答時間を改善する場合は、これらの設定値を最低 1 秒に削減できます。.

2 つのコンソールの最新表示間隔は、以下のように調整することができます。

- IBM Tivoli Enterprise Console では、IBM Tivoli Enterprise Console イベント・コンソールの「構成」を使用して、許容範囲を変更します。次に表示されるイベント・ビューで、設定を調整します。
- Tivoli Enterprise Portal イベント・コンソールの場合は、**「表示」>「最新表示間隔」**をクリックして、最新表示間隔にアクセスします。

ルール検査ユーティリティーの使用

ルール検査ユーティリティーには、BAROC (Basic Recorder of Objects in C) イベント・クラスの設計が変更された場合は常に、ルールの既存セットへの影響を評価する機能があります。このユーティリティーを使用すると、これらのイベント・クラス定義の変更によって、どのルールが影響を受けている可能性があるかを検査できます。

ルール検査ユーティリティーが使用する、2 つの重要な必須ファイル・セットがあります。これらのファイル・セットは、イベント・クラスの設計変更がルールに与える可能性のある影響を検査するためのものです。

- BAROC イベント・クラス定義ファイル:

  IBM Tivoli Enterprise Console クラス定義は、継承性のある階層です。あるクラスは別のクラスから継承することができ、親クラスからのすべての属性は子クラスで使用可能です。EVENT クラスは、IBM Tivoli Enterprise Console の基本クラスです。その他のクラスは通常は IBM Tivoli Enterprise Console EVENT クラスから派生します。

  IBM Tivoli Enterprise Console では、BAROC イベント・クラス定義ファイル (*.baroc ファイル) は、アクティブにロードされたルール・ベースの TEC_CLASSES サブディレクトリーにあります。このファイルは、IBM Tivoli Enterprise Console Server によって使用されるイベント・クラス定義を提供します。このツールは IBM Tivoli Enterprise Console と密接に統合されており、アクティブ・ルール・ベースの TEC_CLASSES サブディレクトリーをデフォルト入力として使用します。ただし、ツールはこのサブディレクトリーには依存していないので、正しい BAROC ファイルが含まれていて、かつユーザーが読み取り特権を持っているディレクトリーが他にあれば、ツールはそのディレクトリーを代替入力として受け入れます。
- ルール・ファイル:

IBM Tivoli Enterprise Console 製品ルール言語も、IBM Tivoli Enterprise Console クラス定義の継承性をサポートします。IBM Tivoli Enterprise Console ルールの述部が特定のクラスを求めている場合、その特定クラスから継承を行うすべてのクラスもこのルール述部を満たします。

IBM Tivoli Enterprise Console では、ルール・セット・ファイル (*.rls ファイル) は、アクティブにロードされたルール・ベースの TEC_RULES サブディレクトリーにあります。このファイルはルール・セットを提供するものであり、IBM Tivoli Enterprise Console Server にデプロイされます。このツールは IBM Tivoli Enterprise Console と密接に統合されており、アクティブ・ルール・ベースの TEC_RULES サブディレクトリーをデフォルト入力として使用しますが、ツールはこのサブディレクトリーには依存していません。正しいルール・セットが含まれていて、かつユーザーが読み取り特権を持っているディレクトリーが他にあれば、ツールはそのディレクトリーを代替入力として受け入れます。

IBM Tivoli Monitoring には、ルール検査ユーティリティーが含まれています。このユーティリティーは、IBM Tivoli Enterprise Console イベント同期インストールの一部として $BINDIR/TME/TEC/OM_TEC/bin ディレクトリーにインストールされます。入出力ファイルにアクセスするのに必要な特権が付与されていれば、固有のディレクトリー構成は必要ありません。

ルール検査コマンドを実行するには、以下の権限が必要です。

- 入力として使用される *.rls ファイルおよび *.baroc ファイルに対する読み取りアクセス権限。
- 検査結果を保管するために使用される出力への書き込みアクセス権限。
- IBM Tivoli Enterprise Console 管理者権限。
- `-cd` オプションおよび `-rd` オプションが指定されていない場合、コマンドを実行するユーザーは、適切な TME 許可を保有し、必要な wrb サブコマンドのレベルを検証する必要があります。

ルール検査ユーティリティーを実行して出力例を確認するには、「*コマンド解説書*」を参照してください。

Event Integration Facility 構成の編集

「**Tivoli Event Integration Facility**」の EIF ファイルを編集すると、構成をカスタマイズすることができます。例えば、最大 5 台のフェイルオーバー EIF サーバーを指定したり、イベント・キャッシュのサイズを調整したりすることができます。

始める前に

Tivoli Event Integration Facility (EIF) がハブ・モニター・サーバーで使用可能になっており、デフォルトの EIF サーバー (Tivoli Enterprise Console event server または Netcool/OMNIbus EIF プローブ) およびポート番号が指定されていると、EIF 構成ファイルがその情報で更新されます。この構成ファイルは、転送済みシチュエーション・イベントのデフォルトの EIF 受信側を指定します。

パラメーターおよび値の詳細については、*Tivoli Event Integration Facility Reference* を参照してください。

ご使用の環境のインストールおよび構成が完了した後で EIF を使用可能にする場合は、Tivoli Enterprise Monitoring Services の管理 または CLI **itmcmd config -S** を使用して EIF を使用可能にし、次にモニター・サーバーとポータル・サーバーをリサイクルする必要があります。

Tivoli Event Integration Facility を使用可能にするようモニター・サーバーを構成する方法については、「*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)」を参照してください。

このタスクについて

EIF 構成ファイルを編集するには、以下のステップを実行してください。

手順

1. `om_tec.config` ファイルを開くには、以下のステップを実行します。
   - Windows 「Tivoli Monitoring Services の管理」ウィンドウで、「Tivoli Enterprise Monitoring Server」を右クリックし、「**拡張**」→「**EIF 構成の編集**」をクリックします。
   - Linux UNIX *install_dir* `/tables/ホスト名/TECLIB/om_tec.config` をテキスト・エディターで開きます。
2. Event Integration Facility のイベント・サーバー構成パラメーターを編集します。

オプション	説明
ServerLocation=	これは、イベント・サーバーのホスト名 または *IP* アドレス です。イベント・フェイルオーバーを提供するために、最大 5 つのデフォルト・イベント・サーバーを、それぞれコンマで区切って指定することができます。デフォルト・イベント・サーバーが使用できない場合は、シチュエーション・イベントはリスト内の次のサーバーに移ります。 値: **tec_server_addr**
ServerPort=	イベント・サーバー listen ポート (デフォルトでは 5529)。イベント・サーバーが Portmapper を使用する場合は、`0` を指定します。複数のサーバー・ロケーションを指定した場合は、それぞれに対応するポート番号を、コンマで区切ってここに追加します。 値: **[port:0]**
EventMaxSize=	1 つのイベントで使用することができる最大文字数。この数はデフォルトでは無効になっています。これを有効にするには、行の先頭にある # (ポンド記号) を削除します。 値: **4096**
RetryInterval=	イベント・サーバーとの接続を再試行する回数。これを超えると、エラーが返されます。 値: **5**

オプション	説明
getport_total_timeout_usec=	イベント・サーバーのポートに接続を試行し続ける秒数。これを過ぎると、タイムアウトになります。デフォルトは 14 時間です。 値: **50500**
NO_UTF8_CONVERSION=	イベントは既に UTF8 フォーマットになっているため、変換は不要です。このパラメーターは、必ず YES に設定してください。 値: **YES**
ConnectionMode=	接続モード。 値: **co**
BufferEvents=	EIF がイベントをバッファーに入れるかどうか。これは必ず YES に設定してください。 値: **YES**
BufEvtMaxSize=	イベント・キャッシュの最大サイズ。デフォルトは、最初は 4096 KB ですが、ここで変更できます。 値: **4096**
BufEvtPath=	イベント・キャッシュ・ファイルのパス。デフォルトは ./TECLIB/om_tec.cache です。 値: **./TECLIB/om_tec.cache**
FilterMode=	イベント・フィルターを有効にします。デフォルトでは、これは OUT に設定されています。 値: **OUT**
TcpTimeout=	このパラメーターは、コネクション指向モードで使用します。これにより、プライマリー・サーバーが使用できない場合、エージェントがプライマリー・サーバーへの接続呼び出しをタイムアウトにし、セカンダリー・サーバーにフェイルオーバーできます。例えば、ファイアウォールによって ICMP Ping 呼び出しがブロックされる場合にこのパラメーターを使用します。この値は秒単位です。 値: **75** **制約事項:** このパラメーターは、PingTimeout および NumberOfPingCalls パラメーターと共に使用することはできません。

オプション	説明
PingTimeout=	ping 呼び出しが宛先サーバーへのアクセスを試行する際の最大タイムアウト。PingTimeout が指定されていない場合、EIF はソケット接続呼び出し前に ping 呼び出しを実行しません。このパラメーターは、コネクションレスまたはコネクション指向のいずれの接続タイプでも使用できます。このパラメーターを使用する場合は NumberOfPingCalls も指定する必要があります。この値は秒単位です。 値: **75** **制約事項:** このパラメーターは、TcpTimeout パラメーターと共に使用することはできません。
NumberOfPingCalls=	宛先サーバーが使用不可であると判断されるまでの ping 関数の呼び出し回数。TCP/IP 構成によっては、宛先サーバーの接続解除直後の最初の ping 呼び出しが正常に戻ることがあります。このパラメーターは、コネクションレスまたはコネクション指向のいずれの接続タイプでも使用できます。このパラメーターを使用する場合は PingTimeout も指定する必要があります。 **制約事項:** このパラメーターは、TcpTimeout パラメーターと共に使用することはできません。
Filter:	特定のクラスをフィルターで除去するには、このキーワードを使用します。デフォルトでは、クラス *ITM_Generic* のシチュエーション・イベント、およびマスター・リセット・フラグを送信しないシチュエーション・イベントは転送されません。 Value: **Class=ITM_Generic; master_reset_flag='';**

3. `om_tec.config` を編集し終わったら、ファイルを保存します。
4. モニター・サーバーを再始動する必要があります。代替方法として、**refreshTECinfo** コマンドを使用すると、モニター・サーバーを再始動せずに更新を完了できます。このコマンドを使用するには、 **tacmd login** でコマンド行インターフェースにログインし、**tacmd refreshTECinfo -t eif** を実行して、EIF 構成を完了します。

タスクの結果

モニター・サーバーは、編集された EIF 構成を使用してイベントを受信側に転送します。

次のタスク

Tivoli Management Services をアップグレードした後に EIF 転送を構成したのはこれが初めてである場合は、Tivoli Enterprise Portal Server もリサイクルする必要があり、ユーザーは Tivoli Enterprise Portal も再起動する必要があります。それを実行しないと、EIF タブはシチュエーション・エディターから欠落します。

EIF 構成を編集する別の方法は、コマンド行インターフェース **tacmd createEventDest** を介して提供されます。詳しくは *IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

関連資料:

Tivoli Event Integration Facility リファレンス
パラメーターと値について詳しくは、Tivoli Enterprise Console インフォメーション・センターを参照してください。

Tivoli Monitoring インストールおよび設定ガイド
Tivoli Event Integration Facility を有効化するようにモニター・サーバーを構成します。

Tivoli Monitoring コマンド・リファレンス
tacmd refreshTECinfo による EIF 構成更新情報の入力、tacmd createEventDest による更新情報の作成

シチュエーション・イベントの EIF 転送の指定

Tivoli Enterprise Monitoring Server が **Tivoli Event Integration Facility** 用に構成されている場合は、シチュエーション・イベントをイベント受信側に転送できます。個別のシチュエーションに対して宛先イベント受信側を設定するには、Tivoli Enterprise Portal シチュエーション・エディターを使用します。

始める前に

Tivoli Enterprise Monitoring Server 構成オプションの 1 つに、「**Tivoli Event Integration Facility**」があります。このオプションを使用可能にすると、イベント・サーバーの「ロケーションとポート番号」ウィンドウが開いて、デフォルトの EIF 受信側が指定されます (*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)または*Tivoli Event Integration Facility Reference*に説明があります)。以降、すべてのシチュエーション・イベントは、デフォルトでその EIF 受信側に転送されます。このとき、シチュエーション名から派生する重大度か、または派生する重大度がない場合は クリティカルの重大度が使用されます。

Tivoli Enterprise Portal 内のシチュエーション・エディターの「EIF」タブを使用して、個々のシチュエーションごとにこのデフォルトを指定変更できます。

転送されるシチュエーション・イベントに対し、最大 8 つのイベント宛先を指定できます。イベント宛先の関連付けは、シチュエーション・エディターの「EIF」タブで行うことができます。イベント宛先は、**tacmd createEventDest** コマンドを使用し

て事前定義される必要があります。イベント宛先のリストに対する変更は、**tacmd refreshTECinfo** コマンドが実行されるか、ハブ・モニター・サーバーがリサイクルされてはじめて有効になります。また、Tivoli Management Services をアップグレードした後に EIF 転送を構成したのはこれが初めてである場合は、Tivoli Enterprise Portal Server もリサイクルする必要があり、ユーザーもシチュエーション・エディターで EIF タブを表示するために Tivoli Enterprise Portal を再起動する必要があります。

前のリリースの tecserver.txt ファイルで指定した代替イベント宛先は、tecserver.txt ファイルのマイグレーションの一環として、自動的に有効なイベント宛先として定義されます。

複数のデフォルト・イベント宛先が指定されている場合 (言い換えれば、複数のデフォルト・イベント宛先サーバーの「デフォルト」が「Y」に設定されている場合)、イベントが定義済みのすべてのデフォルト宛先に転送されるためには、それらがすべて Tivoli Enterprise Portal で選択されている必要があります。

このタスクについて

転送されるイベントについて、宛先 EIF 受信側および重大度を指定するには、次のステップを実行してください。

手順

1. 「Tivoli Enterprise Portal Navigator」ビューで、シチュエーションが関連付けられているナビゲーター項目を右クリックし、「**シチュエーション**」をクリックするか、メイン・ツールバーの 「**シチュエーション・エディター**」をクリックします。
2. 転送するシチュエーションを選択します。
3. 「**EIF**」タブをクリックします。
4. ☑ 「**EIF 受信側へのイベントの転送**」 を選択して、このシチュエーションのために開かれるイベント毎に EIF イベントが送信されることを指定します。
5. このシチュエーションの転送されたイベントに適用する「**EIF 重大度**」を選択します。 <デフォルトの EIF 重大度> では、このナビゲーター項目でシチュエーションに使用される重大度を使用します。
6. <デフォルトの EIF 受信側> の代わり、もしくはそれに加えて他の EIF 受信側を割り当てるには、以下のステップのいずれかを使用します。
   - 宛先を追加するには、「**使用可能な EIF 受信側**」 リストから宛先を選択し、◀ 割り当て済みリストに移動します。(最初に宛先を 1 個選択し、次に Ctrl キーを押しながら他の宛先をクリックすると、クリックした宛先を追加で選択することができます。また、Shift キーを押しながらクリックすると、最初に選択した宛先から次に選択した宛先までの間にあるすべての宛先を選択することもできます。)
   - 宛先を削除するには、「**割り当て済みの EIF 受信側**」 リストから該当する宛先を選択し、▶ 「使用可能」リストに移動します。

   「**使用可能な EIF 受信側**」リストには、「Tivoli Monitoring Services の管理」または **tacmd createEventDest** コマンドを使用して定義されたすべての定義済み

EIF 宛先が表示されます。*IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

7. シチュエーション・エディターを開いたままにする場合は「**適用**」をクリックし、シチュエーション・エディターを閉じる場合は「**OK**」をクリックして、変更を含むシチュエーション定義を保存します。

関連資料:

Tivoli Event Integration Facility リファレンス
パラメーターと値について詳しくは、Tivoli Enterprise Console インフォメーション・センターを参照してください。

Tivoli Monitoring インストールおよび設定ガイド
Tivoli Event Integration Facility を有効化するようにモニター・サーバーを構成します。

Tivoli Monitoring コマンド・リファレンス
tacmd refreshTECinfo による EIF 構成更新情報の入力、tacmd createEventDest による更新情報の作成

イベント・メッセージのカスタマイズ

シチュエーション・エディターの「**EIF**」タブから、EIF 受信側に送信されたシチュエーション・イベントのマップ定義を作成することができます。「**EIF**」タブから開く「EIF スロット・カスタマイズ」ウィンドウを使用すると、転送される EIF イベントにシチュエーション・イベントをマップする方法をカスタマイズできます。これにより、シチュエーション・イベントと、Tivoli Enterprise Console event server に転送されるイベントとのデフォルト・マッピングを指定変更できます。

基本スロット名が `msg` の場合、「リテラル値」列がメッセージ・テンプレートに使用されます。メッセージ・テンプレートは、固定メッセージ・テキストと変数置換参照 (つまりシンボル) で構成されます。シンボルでは、共通スロット・データ、イベント・スロット・データ、またはシチュエーション式に対する特殊参照を参照できます。共通スロットはすべての転送されるイベントに含まれるスロット (situation_name など) で、イベント・スロットはシチュエーションに固有のスロットです。イベント・スロットを設定する際は、以下の構文規則が適用されます。

- イベント・スロットの場合は、完全修飾された属性名 ($Attribute_Table.Attribute_Name$) を使用します。
- 共通スロットの場合、シチュエーション・シンボルのとき以外は、完全修飾されていない (ピリオド「.」が含まれていない) 変数名を使用します。
- シチュエーション式の場合は、$formula$ を使用します。

< (より小)、> (より大)、" (引用符)、' (単一引用符)、および & (アンパーサンド) の各文字はサポートされていません。この列は、「マップされた属性」列で値が選択されていない場合のみ使用可能です。詳しくは、Tivoli Enterprise Portal オンライン・ヘルプまたは *Tivoli Enterprise Portal ユーザーズ・ガイド* を参照してください。

msg スロットについては、通常のユーザーは、マップされた属性値ではなくリテラル値を指定します。値が msg スロットのマップされた属性列に指定された場合、以下が発生します。

- 「**すべての属性のマップ**」が選択されていない場合、msg のマップされた属性はイベントからなくなり、無視されます。
- 「**すべての属性のマップ**」が選択されている場合、Tivoli Enterprise Console イベントの msg スロットにはデフォルトのメッセージ・テンプレートのみが指定され、マップされた属性は指定されません。

MCS 属性サービスによって使用される XML の更新

複数コンソール・サポート (MCS) 属性サービスによって使用されるデフォルトの XML ファイルには、ハブ・モニター・サーバーのインストール済み環境の TECLIB ブランチ内にある、BAROC ファイルで定義されたイベント・クラスのみが含まれています。新規タイプのエージェントが Tivoli Management Services インフラストラクチャーに追加される場合、または、新規イベント・クラスが Tivoli Enterprise Console event serverに追加された場合は、EIF スロット・カスタマイズ用の新規 XML ファイルを生成してください。

始める前に

ルールに指定されたイベントクラスが現行のイベント・クラス定義セット内には見つからず、引き続き現行の定義セットでルールを作成する場合は、認識されないイベント・クラスはすべてルールから除外されます。

EIF イベント・カスタマイズ機能では、MCS 属性サービスを使用して、事前定義イベント・クラスのリストを「EIF スロット・カスタマイズ」ウィンドウの「**イベント・クラス名**」リストに表示します。このウィンドウは Tivoli Enterprise Portal シチュエーション・エディターの「EIF」タブから利用できます。OS エージェントに属するイベント・クラスのみが事前定義され、MCS 属性サービスの JAR ファイルに格納されます。新規タイプのエージェントが Tivoli Management Services インフラストラクチャーに追加された場合、またはエージェントの新規イベント・クラスが追加された場合は、新規イベント・クラスが「**イベント・クラス名**」リストに表示される前に、新規 MCS XML ファイルを生成し、Tivoli Enterprise Portal Server でこの新規 XML ファイルを指定する必要があります。

新規 MCS XML ファイルを生成するには、Tivoli Enterprise Console イベント定義生成プログラム (TEDGEN) ユーティリティーを使用します。このユーティリティーは IBM Tivoli Monitoring **Tools** DVD にあります。ハブ・モニター・サーバーまたはポータル・サーバーがインストールされている分散コンピューター、または Tivoli Enterprise Console がインストールされている分散コンピューターに TEDGEN ユーティリティーをインストールします。MCS XML ファイルを生成するコンピューターには必要な BAROC ファイルがなければなりません。

注: MCS XML ファイル内の定義は、同梱されている MCS 属性サービスの JAR ファイルに含まれる定義に置き換わります (マージは行われません)。OS エージェントおよび新規エージェントの両方のイベント・クラス定義を含む MCS XML ファイルを取得するには、TEDGEN ユーティリティーを実行して MCS XML ファイルを生成する前に、OS エージェントおよび新規エージェントに対するすべての

BAROC 定義が IBM Tivoli Enterprise Console にロードされているか、またはハブ・モニター・サーバーあるいはポータル・サーバーの同じディレクトリー内にあることを確認してください。

TEDGEN ツールをインストールして構成するには、以下のステップを実行します。

1. IBM Tivoli Monitoring **Tools** DVD から、ハブ・モニター・サーバー、ポータル・サーバー、または Tivoli Enterprise Console がインストールされているコンピューターに TEDGEN ユーティリティーをインストールします。このユーティリティーは **Tools**DVD の `tec/tedgen` ディレクトリーにあります。インストールと構成の手順は、同じディレクトリー内の `README.txt` ファイルに記述されています。
2. Linux UNIX TEDGEN ユーティリティーを Linux または UNIX システム上のポータル・サーバーにインストールした場合、以下の追加の構成ステップも実行してください。
   a. *install_dir* `/tables/cicatrsq/TECLIB` ディレクトリーが存在しない場合はこのディレクトリーを作成します。この *install_dir* は、IBM Tivoli Monitoring がインストールされているディレクトリーです。
   b. *install_dir* `/arch/cq/TECLIB` ディレクトリーの `om_tec.baroc` ファイルと `kib.baroc` ファイルを *install_dir* `/tables/cicatrsq/TECLIB` ディレクトリー (`arch` は ポータル・サーバー のアーキテクチャー・ディレクトリーです) にコピーします。

このタスクについて

これらのステップでは、TEDGEN ユーティリティーが、このツールを実行するコンピューター (Tivoli Enterprise Console イベント・サーバー、ハブ・モニター・サーバー、またはポータル・サーバー) にインストールされていることを前提としています。

EIF イベントがカスタマイズされているエージェントのアプリケーション・サポートを、このユーティリティーを実行するハブ・モニター・サーバーまたはポータル・サーバーにインストールする必要もあります。 TEDGEN ユーティリティーを Tivoli Enterprise Console で実行する場合は、エージェントの BAROC ファイルを、Tivoli Enterprise Console がインストールされているコンピューターにロードする必要もあります。

ユーティリティーとアプリケーション・サポートをインストールした後で、TEDGEN コマンドを実行して EIF スロット・カスタマイズ用の新規 XML ファイルを作成します。

注:

- Linux または UNIX にインストールされているポータル・サーバーに TEDGEN ユーティリティーをインストールしており、エージェントのアプリケーション・サポートのインストール時に「**リモート・シード用 TEMS のインストール**」オプションを選択していない場合、BAROC ファイルは存在しません。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『モニター・サーバーを持たないコンピューターへのアプリケーション・サポート・ファイルのインストール』を参照してください。このアクションにより、BAROC ファイルがポータル・サー

バーの *install_dir* /tables/ cicatrsq/TECLIB ディレクトリー (*install_dir* は IBM Tivoli Monitoring のインストール先ディレクトリー) に配置されます。

- TEDGEN ユーティリティーを Windows のポータル・サーバーにインストールしている場合、イベントをカスタマイズするエージェントの .baroc ファイルはポータル・サーバーの TECLIB ディレクトリーに含まれています。エージェントによっては、ポータル・サーバー・アプリケーション・サポートに .baroc ファイルが含まれていないことがあります。エージェントの .baroc ファイルが存在しない場合は、ハブ・モニター・サーバーの TECLIB ディレクトリーからコピーできます。

手順

1. 以下のいずれかのステップを実行して、TEDGEN コマンドを実行します。
   - ハブ・モニター・サーバーまたはポータル・サーバーがインストールされているコンピューターで、以下のコマンドを実行します。

     Windows

     ```
     set CANDLE_HOME=install_dir

     cd TEDGEN_Install_dir¥scripts

     tedgen -itmDir install_dir ¥{CMS|CNPS}
     ¥TECLIB -id server_id -xmlPath output_xml_file_path
     ```

     ここで、*install_dir* は IBM Tivoli Monitoring がインストールされているディレクトリー、*TEDGEN_Install_dir* は TEDGEN ユーティリティーがインストールされているディレクトリーです。

     Linux UNIX

     ```
     export CANDLEHOME=install_dir

     cd TEDGEN_Install_dir/scripts

     tedgen -itmDir
     install_dir /tables/{tems_name|cicatrsq}/
     TECLIB -id server_id -xmlPath output_xml_file_path
     ```

     ここで、*install_dir* は IBM Tivoli Monitoring がインストールされているディレクトリー、*TEDGEN_Install_dir* は TEDGEN ユーティリティーがインストールされているディレクトリーです。

     例 以下の例では、**mytems** という名前のハブ・モニター・サーバーの TECLIB ディレクトリーに BAROC ファイルがあります。出力ファイルは同じディレクトリーに入り、名前は **tems.xml** です。

     ```
     tedgen -itmDir C:¥IBM¥ITM¥CMS¥TECLIB -id mytems -xmlPath tems.xml
     ```

   - Tivoli Enterprise Console event serverが配置されているコンピューターで、イベント・サーバーのインストール・メディアに付属している「**ツール**」DVD から TEDGEN ユーティリティーをインストールします。次に、以下のようにして、新規 XML ファイルを作成します。

     a. **wrb -imprbclass** コマンドを発行して、新しく追加されるエージェントおよび OS エージェント (まだインストールされていない場合のみ) とともにインストールされる BAROC ファイルをインポートします。

     ```
     wrb -imprbclass class_file [ -encoding encoding ]
     [-before class_file | -after class_file] [-force] rule_base
     ```

b. 以下のように wrb -loadrb コマンドを発行して、ルール・ベースを再ロードします。

```
wrb -loadrb rule_base
```

c. 以下のようにコマンドを実行して、イベント・サーバーを停止および再始動します。

```
wstopesvr
wstartesvr
```

d. 以下のように TEDGEN コマンド発行して、XML ファイルを生成します。

```
tedgen [ -bcDir baroc_classes_directory | -rbName rule_base_name ]
-id server_id -xmlPath output_xml_file_path
```

例 以下の例では、現行ルール・ベースから **tec.xml** という名前の XML ファイルが **mytec** という名前の Tivoli Enterprise Console event server 上に生成されます。

```
tedgen -id mytec -xmlPath tec.xml
```

2. Tivoli Enterprise Portal Server がインストールされているコンピューターに、新しく生成した XML ファイルをコピーします。
3. 以下のようにポータル・サーバーの環境ファイルを編集して、XML ファイルへのパスを指定します。
   a. Windows 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで「**Tivoli Enterprise Portal Server**」を右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックして、テキスト・エディターで kfwenv ファイルを開きます。
   Linux UNIX *install_dir* /config/cq.ini をテキスト・エディターで開きます。
   b. KFW_MCS_XML_FILES 環境変数を指定し、MCS XML ファイルへのパスの前に = (等号) を入力します。
   c. 環境ファイルを保存して閉じます。
   d. Windows ポータル・サーバーを再始動します。
   Linux UNIX ポータル・サーバーを再構成してから再始動します。

Tivoli Enterprise Console での Universal Agent からのイベントの表示

すべての Universal Agent アプリケーションは、それぞれのカタログ、属性、および ODI ファイルを動的に生成するので、Universal Agent シチュエーション・イベントを Tivoli Enterprise Console で適切に表示するには、特定のステップを手動で行う必要があります。

始める前に

Tivoli Enterprise Console イベント転送機能によって Universal Agent シチュエーションを Tivoli Enterprise Console イベントに適切に変換するには、ハブの初期化中に Universal Agent 属性ファイルがハブ Tivoli Enterprise Monitoring Server に存在している必要があります。 Universal Agent がリモート・モニター・サーバーに接続されている場合は、Universal Agent カタログおよび属性ファイルはハブに伝搬されず、Universal Agent シチュエーション・イベントの変換が失敗します。

このタスクについて

以下のステップを実行して、Universal Agent 属性ファイルがハブ・モニター・サーバー上にあることを確認し、Universal Agent シチュエーション・イベント定義を使用して BAROC ファイルを生成します。これは、Universal Agent イベントを正しく解析し、Tivoli Enterprise Console で表示するために必要です。

手順

1. 以下のようにして、Universal Agent 属性ファイルがハブにあることを確認します。
   - 一時的に Universal Agent をハブ・モニター・サーバーに接続し、属性ファイルをアップロードできるようにします。正常に接続すると、リモート・モニター・サーバーに接続するように Universal Agent を再構成できるようになります。
   - Universal Agent 属性ファイルを、リモート・モニター・サーバーからハブに手動で移動します。属性ファイルのロケーション:
     Windows *install_dir* ¥CMS¥ATTRLIB
     Linux UNIX *install_dir* / tables/tems_name/ATTRLIB
   - ハブ・モニター・サーバーをリサイクルする。
2. Universal Agent アプリケーションのために必要な BAROC ファイルを取得します。
   a. IBM Integrated Service Management Library で *BAROC File Generator* を検索し、ダウンロードします。
   b. Universal Agent アプリケーション用の ODI ファイルを入力として提供して、BAROC 生成プログラムを実行します。Tivoli Enterprise Portal Server がインストールされているコンピューター上の ODI ファイルのロケーション (Universal Agent がモニター・サーバーに正常に接続している必要があります):
      Windows *install_dir* ¥cnps
      Linux UNIX *install_dir /platform*/cq/bin
      ODI ファイル名の形式は、*xxx*odi*nn* です。ここで、*xxx* はアプリケーション名の指定されたエージェントで、*nn* はバージョン番号です。
   c. BAROC ファイルを生成した後に、それをイベント・サーバーに移動し、コンパイルしてロードします。

IBM Tivoli Enterprise Console イベント・ビューアーからの NetView コンソールの使用

IBM Tivoli Enterprise Console ビューから IBM Tivoli NetView® Java コンソールを起動して、1 つのイベント行から関連するネットワーク・トポロジーおよび診断にナビゲートすることができます。イベントに関連するノードのトポロジー表示をサポートするには、選択したイベントに有効なホスト名または IP アドレスが含まれている必要があります。含まれていない場合は、特定のノードは選択されずに標準トポロジー・ビューが表示されます。

このタスクについて

Tivoli NetView によって転送されたイベントは、IBM Tivoli Enterprise Console ルールによって自動的に IBM Tivoli Enterprise Console サーバーに同期されます。イベント状況更新は、Netview イベント・コンソールを起動するシステム上に反映されます。

アクティブにロードされたルール・ベース内に netview.rls ファイルと netview BAROC ファイルがあることを確認してください。詳しくは、Tivoli Enterprise Console インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.itec.doc_3.9/welcome_nd.html)で「*ルール・セット・リファレンス*」を参照してください。

Tivoli Enterprise Portal 内の IBM Tivoli Enterprise Console ビューから NetView コンソールを使用する場合は、Tivoli Enterprise Portal クライアントを起動するシェル・スクリプト内で、NetView Web コンソールのインストール・ディレクトリーを指すように *NVWC_HOME* 変数を構成する必要があります。

NVWC_HOME 変数を設定するには、以下の手順を実行します。

手順

- Windows *install_dir* ¥cnp¥cnp.bat
- Linux または UNIX *install_dir* /bin/cnp.sh

次のタスク

IBM Tivoli Enterprise Console ビューから NetView コンソールを起動するには、Tivoli Enterprise Portal クライアントが稼働しているコンピューターに NetView Web コンソールをインストールする必要があります。

NetView コンソールの使用について詳しくは、IBM Tivoli Enterprise Console 製品資料を参照してください。

第 11 章 Tivoli Netcool/OMNIbus によるシチュエーション・イベント統合

Tivoli Event Integration Facility (EIF) インターフェースを使用して、エンタープライズ・シチュエーション・イベントを OMNIbus に転送します。イベントは Netcool/OMNIbus Probe for Tivoli EIF で受信されます。Netcool/OMNIbus Probe for Tivoli EIF はイベントを OMNIbus にマップし、その後、OMNIbus サーバーに挿入します。

これらのイベントへの更新は OMNIbus にも送信されます。転送されたイベントを OMNIbus ユーザーが確認、クローズ、または再オープンすると、これらの変更が OMNIbus から転送元のモニター・サーバーに返されます。

SNMP アラートとして Netcool/OMNIbus SNMP プローブ に送信された Tivoli Enterprise Monitoring Agent からのシチュエーション・イベントは、Netcool/OMNIbus との統合にも使用できます。

イベント転送を有効にする手順 (スクリプトからプログラムを実行するための OMNIbus サーバーの構成、OMNIbus DB スキーマの更新、EIF プローブの構成、ハブ・モニター・サーバーでのシチュエーション転送の有効化、およびデフォルトの Event Integration Facility (EIF) 宛先の定義) については、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Setting up event forwarding to Tivoli Netcool/OMNIbus』を参照してください。

第 12 章 共通イベント・コンソール用コネクターの構成

共通イベント・コンソール は、複数のイベント・システムのイベントを 1 カ所に統合して表示する Tivoli Enterprise Portal ビューです。共通イベント・コンソールにより、1 つのテーブルにイベント・システムのイベントが表示され、ユーザーは、これらのイベントでソート、フィルター、およびアクションの実行を行うことができます。以下のイベント・システムがサポートされます。

- IBM Tivoli Monitoring
- IBM Tivoli Enterprise Console
- IBM Tivoli Netcool/OMNIbus

共通イベント・コネクター (一般にコネクターと呼ばれます) は、共通イベント・コンソールで複数のイベント・システムのイベントを統合して表示できるソフトウェアです。コネクターは、イベント・システムからイベント・データを取得して、そのイベント・システムで実行される、ユーザーが開始したアクションを送信します。例えば、共通イベント・コンソールで Tivoli Enterprise Console または Netcool/OMNIbus イベントでアクションを実行する場合は、関連する共通イベント・コンソール・コネクターが、このアクションを元のイベント・システム (Tivoli Enterprise Console または Netcool/OMNIbus) に送信して、実行できるようにします。特定のイベント・システムのイベントを共通イベント・コンソールに表示するには、そのイベント・システムのコネクターを構成し、Tivoli Enterprise Portal Server 環境ファイルに変数を設定する必要があります。

「共通イベント・コンソール構成」ウィンドウ

イベント・システム・インスタンスごとに共通イベント・コンソール・コネクターを構成するには、「共通イベント・コンソール構成」ウィンドウを使用します。IBM Tivoli Monitoring 製品用のコネクターは、製品のインストール時に事前構成されるため、共通イベント・コンソールには、デフォルトでシチュエーション・イベントが組み込まれています。ただし、IBM Tivoli Enterprise Console または IBM Tivoli Netcool/OMNIbus イベントを共通イベント・コンソールに組み込むには、IBM Tivoli Monitoring 製品のインストール後に、これらのイベント・システムごとにコネクターを構成する必要があります。この構成では、共通イベント・コンソールで表示するイベントを取得するために使用されるイベント・システムを指定します。また、IBM Tivoli Monitoring コネクターの構成値の一部を変更したい場合もあります。

このタスクについて

コネクターを構成するには、Tivoli Enterprise Portal Server がインストールされているコンピューター上で次のステップを実行して、「共通イベント・コンソール構成」ウィンドウを開き、次の手順を実行します。

手順

- Windows

1. 「**スタート**」→「**プログラム**」→「**IBM Tivoli Monitoring**」→「Tivoli Enterprise Monitoring Services の管理」を選択します。
2. 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、**Tivoli Enterprise Portal Server** を右クリックします。
3. メニューで、「**再構成**」をクリックします。
4. 最初の構成ウィンドウで、「**OK**」をクリックします。
5. 2 番目の構成ウィンドウで、「**OK**」をクリックします。
6. 「Tivoli Enterprise Portal Server のウェアハウス接続情報を再構成しますか?」という質問に対しては、「**いいえ**」をクリックします。

- Linux または UNIX
  1. コマンド行で、*install_dir* /bin ディレクトリーに移動し (cd)、./itmcmd manage と入力します。
  2. 「Tivoli Enterprise Monitoring Services の管理」ウィンドウで、**Tivoli Enterprise Portal Server** を右クリックします。
  3. ポップアップ・メニューで、「**構成**」をクリックします。

タスクの結果

ポータル・サーバーは停止し、しばらくして「共通イベント・コンソール構成」ウィンドウが開き、次のタブが表示されます。
- ITM コネクター
- TEC コネクター
- OMNIbus コネクター
- 特殊列の名前

「ITM コネクター」タブ

IBM Tivoli Monitoring コネクターに関する情報を表示または変更するには、「**ITM コネクター**」タブをクリックします。 Tivoli Monitoring イベント・システム内にあるのは 1 つのハブ Tivoli Enterprise Monitoring Server であるため、構成するのは 1 つの IBM Tivoli Monitoring コネクターのみです。

以下の情報により、IBM Tivoli Monitoring コネクターを定義します。

このコネクターを有効にする
「はい」または「いいえ」を選択できます。「はい」の値は、IBM Tivoli Monitoring イベントが共通イベント・コンソールで使用可能であることを意味します。

コネクター名
このコネクターの共通イベント・コンソールに表示される名前。

このコネクターの最大イベント数
このコネクターの共通イベント・コンソールで使用可能になるイベントの最大数。

クローズされたイベントの表示
「はい」または「いいえ」を選択できます。「はい」の値は、このコネクターのクローズされたイベントが共通イベント・コンソールで使用可能であることを意味します。

「TEC コネクター」タブ

IBM Tivoli Enterprise Console コネクターに関する情報を表示または変更するには、「**TEC コネクター**」タブをクリックします。 Tivoli Enterprise Console Server のイベントを共通イベント・コンソールに表示するには、IBM Tivoli Enterprise Console コネクターを構成する必要があります。

コネクターを構成するには、「**新規**」をクリックします。結果の「TEC コネクター」ページには、IBM Tivoli Enterprise Console コネクターを定義する以下の情報が含まれています。

コネクター名
このコネクターの共通イベント・コンソールに表示される名前。

このコネクターの最大イベント数
このコネクターの共通イベント・コンソールで使用可能になるイベントの最大数。

イベント・システムのコンピューター名
このコネクターに関連付けられたイベント・システムのコンピューター名。

イベント・システムのポート番号
オブジェクト・ディスパッチャー (oserv) のポート番号 (通常 94)。これは、コネクターが Tivoli Enterprise Console イベント・システムからイベントを取り出すために使用するポートです。

これは、Tivoli Enterprise Console イベント・サーバーに接続するために使用されるポート (デフォルトで5529) ではありません。

イベント・システムにアクセスするためのユーザー名
このコネクターに関連付けられたイベント・システムにアクセスするときに使用するユーザー名。

パスワード
ユーザー名に関連付けられたパスワード。

共通イベント・コンソールのイベントを定義するイベント・グループ
共通イベント・コンソールで使用可能なイベントを定義する Tivoli Enterprise Console イベント・グループ。

イベント・グループを指定しない場合は、すべての Tivoli Enterprise Console イベントが共通イベント・コンソールで使用可能です。

イベントをさらに制限する場合は、「**共通イベント・コンソールのイベントを制限する SQL WHERE 節**」フィールドに節を定義することもできます。

共通イベント・コンソールのイベントを制限する SQL WHERE 節
この節は、Tivoli Enterprise Console の基本属性テーブルから構築したイベントの一部にのみ適用できます。例えば、`status <> 30` を指定すると、状況が 30 に等しくないすべてのイベントが共通イベント・コンソールで使用可能になります。

節を定義しない場合は、「**共通イベント・コンソールのイベントを定義するイベント・グループ**」フィールドに指定したイベント・グループによって除外されていない限り、すべての Tivoli Enterprise Console イベントが共通イベント・コンソールで使用可能です。

クローズされたイベントの表示

「はい」または「いいえ」を選択できます。「はい」の値は、このコネクターのクローズされたイベントが共通イベント・コンソールで使用可能であることを意味します。

イベント・システムをポーリングするための時間間隔 (分数) (Time interval (in minutes) for polling event system)

新しいイベントまたは変更されたイベントの有無についてイベント・システムをポーリングする間隔 (分数)。

イベントを同期化するための時間間隔 (分数) (Time interval (in minutes) for synchronizing events)

削除されたイベントを確認するためにイベント・システムをポーリングする間隔 (分数)。

再接続の試行の間隔 (秒数)

コネクターがイベント・システムとの接続を失ったときの再接続の試行の間の遅延 (秒数)。

再接続の試行回数 (Number of reconnection attempts)

コネクターがイベント・システムとの接続を失った場合に行う再接続の連続試行の最大数。

この値を -1 に設定した場合に、コネクターが接続を失うと、コネクターは無期限に再接続を試行します。

特殊テーブル列に関する情報 (Information for extra table columns)

共通イベント・コンソールには、カスタマイズ可能な 5 つの特殊テーブル列が含まれています。この「TEC コネクター」ページの残りのフィールドでは、これらのカスタマイズ可能な各列にマップされる属性を識別する Tivoli Enterprise Console 属性タイプと属性名を定義できます。

属性タイプでは、以下のいずれかの値を選択できます。

- **基本**。これは、属性が Tivoli Enterprise Console 基本属性テーブルからの属性であることを意味します。
- **拡張**。これは、属性が Tivoli Enterprise Console 拡張属性テーブルからの属性であることを意味します。

「OMNIbus コネクター」タブ

IBM Tivoli Netcool/OMNIbus コネクターに関する情報を表示または変更するには、「**OMNIbus コネクター**」タブをクリックします。 Tivoli Netcool/OMNIbus ObjectServer のイベントを共通イベント・コンソールに表示するには、IBM Tivoli Netcool/OMNIbus コネクターを構成する必要があります。

コネクターを構成するには、「**新規**」をクリックします。結果の「OMNIbus コネクター」ページには、IBM Tivoli Netcool/OMNIbus コネクターを定義する以下の情報が含まれています。

コネクター名

このコネクターの共通イベント・コンソールに表示される名前。

このコネクターの最大イベント数
このコネクターの共通イベント・コンソールで使用可能になるイベントの最大数。

イベント・システムのコンピューター名
このコネクターに関連付けられたイベント・システムのコンピューター名。

イベント・システムのポート番号
ObjectServer のポート番号 (通常 4100)。このコネクターはこの番号を使用して Tivoli Netcool/OMNIbus イベント・システムからイベントを取り出します。

イベント・システムにアクセスするためのユーザー名
このコネクターに関連付けられたイベント・システムにアクセスするときに使用するユーザー名。

パスワード
ユーザー名に関連付けられたパスワード。

共通イベント・コンソールのイベントを制限する SQL WHERE 節
この節は、Tivoli Netcool/OMNIbus `alerts.status` テーブルから構築したイベントの一部にのみ適用できます。例えば、`Severity <> 0` を指定すると、重大度が 0 に等しくないすべてのイベントが共通イベント・コンソールで使用可能になります。

節を定義しない場合は、すべての Tivoli Netcool/OMNIbus イベントが共通イベント・コンソールで使用可能です。

クリアしたイベントの表示
「はい」または「いいえ」を選択できます。「はい」の値は、このコネクターのクリアしたイベントが共通イベント・コンソールで使用可能であることを意味します。

イベント・システムをポーリングするための時間間隔 (分数) (Time interval (in minutes) for polling event system)
新しいイベントまたは変更されたイベントの有無についてイベント・システムをポーリングする間隔 (分数)。

Tivoli Netcool/OMNIbus ObjectServer は、新しいイベントまたは変更されたイベントが使用可能になると、これらのイベントを共通イベント・コンソールに自動的に送信します。そのため、これにチェック・マークを付ける主な目的は、サーバーとサーバーへの接続が正しく機能していることを確認することです。

再接続の試行の間隔 (秒数)
コネクターがイベント・システムとの接続を失ったときの再接続の試行の間の遅延 (秒数)。

再接続の試行回数 (Number of reconnection attempts)
コネクターがイベント・システムとの接続を失った場合に行う再接続の連続試行の最大数。

この値を `0` に設定した場合に、コネクターが接続を失うと、コネクターは無期限に作動不能なままになります。

この値を -1 に設定した場合に、コネクターが接続を失うと、コネクターは無期限に再接続を試行します。

特殊テーブル列に関する情報 (Information for extra table columns)
共通イベント・コンソールには、カスタマイズ可能な 5 つの特殊テーブル列が含まれています。このページの残りのフィールドでは、これらのカスタマイズ可能な各列にマップされるフィールドを識別する Tivoli Netcool/OMNIbus フィールド・タイプとフィールド名を定義できます。

フィールド・タイプでは、以下のいずれかの値を選択できます。

- `alerts.status`。これは、フィールドに、Tivoli Netcool/OMNIbus ObjectServer の `alerts.status` テーブルのデータが含まれていることを意味します。
- `alerts.details`。これは、フィールドに、Tivoli Netcool/OMNIbus ObjectServer の `alerts.details` テーブルのデータが含まれていることを意味します。
- **拡張**。これは、フィールドに、Tivoli Netcool/OMNIbus イベント・システムに転送された Tivoli Enterprise Console イベントの拡張属性が含まれていることを意味します。

「特殊列の名前」タブ

共通イベント・コンソールには、カスタマイズ可能な 5 つの特殊テーブル列が含まれています。デフォルトでは、以下の名前がこれらの列に使用されます。

- 特殊列 1
- 特殊列 2
- 特殊列 3
- 特殊列 4
- 特殊列 5

これらの列の名前を表示または変更するには、「**特殊列の名前**」タブをクリックします。

Tivoli Enterprise Console または Tivoli Netcool/OMNIbus コネクターの定義時に、これらのカスタマイズ可能な各列にマップされる情報を定義できます。

特殊テーブル列の目的

共通イベント・コンソールには、Tivoli Enterprise Console 基本属性テーブルおよび Tivoli Netcool/OMNIbus `alerts.status` テーブルと `alerts.details` テーブルからの基本的な情報セットのみが表示されます。

例えば、Tivoli Enterprise Console イベントの「origin」という名前の追加属性を表示するには、以下のステップを実行します。

1. 「TEC コネクター」ページの「**特殊列 1 の属性タイプ**」フィールドで、属性タイプ (例えば、「**基本**」) を選択します。
2. 「TEC コネクター」ページの「**特殊列 1 の属性名**」フィールドに、属性名 (例えば、「`origin`」) を入力します。

3. 「特殊列の名前」ページの「**特殊列 1 の名前**」フィールドに、カスタマイズした列に使用する名前を入力します。例えば、`Origin` と入力します。

Tivoli Enterprise Console イベントである各行の「Origin」列には、共通イベント・コンソールにより origin 属性の値が表示されます。

「TEC コネクター」タブ: 特殊テーブル列に関する情報の定義

「TEC コネクター」ページの以下のフィールドで、カスタマイズ可能な列にマップされる情報を定義します。

- 特殊列 1 の属性タイプ
- 特殊列 1 の属性名
- 特殊列 2 の属性タイプ
- 特殊列 2 の属性名
- 特殊列 3 の属性タイプ
- 特殊列 3 の属性名
- 特殊列 4 の属性タイプ
- 特殊列 4 の属性名
- 特殊列 5 の属性タイプ
- 特殊列 5 の属性名

「OMNIbus コネクター」タブ: 特殊テーブル列に関する情報の定義

「OMNIbus コネクター」ページの以下のフィールドで、カスタマイズ可能な列にマップされる情報を定義します。

- 特殊列 1 のフィールド・タイプ
- 特殊列 1 のフィールド名
- 特殊列 2 のフィールド・タイプ
- 特殊列 2 のフィールド名
- 特殊列 3 のフィールド・タイプ
- 特殊列 3 のフィールド名
- 特殊列 4 のフィールド・タイプ
- 特殊列 4 のフィールド名
- 特殊列 5 のフィールド・タイプ
- 特殊列 5 のフィールド名

イベント同期を使用する際のベスト・プラクティス

ご使用の環境で、Tivoli Monitoring イベントを、イベント同期のために Tivoli Enterprise Console または Tivoli Netcool/OMNIbus のイベント・システムに転送する場合は、共通イベント・コンソールで重複したイベント情報が使用されるのを避けるために、同じイベントの 1 つのコピーのみを取得するように共通イベント・コネクターを構成します。

以下のベスト・プラクティスに従って、Tivoli Monitoring イベントとして発生していない Tivoli Enterprise Console または Tivoli Netcool/OMNIbus のイベントのみを含めるように共通イベント・コンソールを制限します。

Tivoli Monitoring イベントを Tivoli Enterprise Console イベント・システムに転送する場合

1. Tivoli Enterprise Console Server で、Tivoli Monitoring イベントとして発生していない Tivoli Enterprise Console イベントのみを定義するイベント・グループを作成して、`All_but_ITM` などの名前を付けます。
2. TEC コネクターを構成する場合は、「**共通イベント・コンソールのイベントを定義するイベント・グループ**」フィールドに `All_but_ITM` と入力します。
3. ITM コネクターを構成する場合は、「**このコネクターを有効にする**」フィールドで「**はい**」をクリックします。

Tivoli Monitoring イベントを Tivoli Netcool/OMNIbus イベント・システムに転送する場合

1. OMNIbus コネクターを構成する場合は、「**共通イベント・コンソールのイベントを制限する SQL WHERE 節**」フィールドに `ITMStatus = ''` と入力します。ここで、`''` は間にスペースのない 2 つの単一引用符です。この節は、共通イベント・コンソール内の Tivoli Netcool/OMNIbus イベントを、Tivoli Monitoring イベントとして発生していないイベントのみに制限します。
2. ITM コネクターを構成する場合は、「**このコネクターを有効にする**」フィールドで「**はい**」をクリックします。

結果の構成により、共通イベント・コンソールは、Tivoli Enterprise Console または Tivoli Netcool/OMNIbus イベント・システムではなく、Tivoli Monitoring イベント・システムから直接 Tivoli Monitoring イベントを取得するようになります。これによって、共通イベント・コンソールで重複したイベント情報が使用されなくなります。

Linux システムでの Tivoli Enterprise Console サーバーへの接続に関する問題のトラブルシューティング

次の情報を使用すると、Linux システムでの Tivoli Enterprise Console サーバーへの接続に関する問題をトラブルシューティングできる場合があります。

問題 Tivoli Enterprise Console コネクターが Tivoli Enterprise Console Server に接続できません。そのため、共通イベント・コンソールで Tivoli Enterprise Console イベントを使用できません。

説明 Tivoli Enterprise Portal Server がインストールされているコンピューター上の /etc/hosts ファイルには、正しい IP アドレスのローカル・ホストが含まれている必要があります。デフォルトの Linux 構成は、以下の行に示すようになります。

```
127.0.0.1 my_hostname localhost
```

デフォルトの Linux 構成では、接続要求は、アドレスが `127.0.0.1` の Tivoli Enterprise Console Server に送信されます。これは、Tivoli Enterprise Portal Server がインストールされているコンピューターの正しい IP アドレスではありません。 Tivoli Enterprise Portal Server に接続するには、逆引き参照を行える必要があります。

解決方法

/etc/hosts ファイルに、IP アドレスが正しいローカル・ホストが含まれていることを確認します。以下の 2 行に、Linux の正しい構成例を示します。ここで、*xxx.xxx.xxx.xxx* は、Tivoli Enterprise Portal Server がインストールされているコンピューターの IP アドレスです。

```
127.0.0.1 localhost
xxx.xxx.xxx.xxx my_hostname
```

第 13 章 モニター・エージェントの保守

Tivoli Enterprise Monitoring Agent の保守では、最新リリースへのアップグレード、環境変数の編集による動作の変更、および Tivoli Enterprise Portal の「物理」ナビゲーター・ビューでの表示の制御などの作業を行います。

エージェントの保守に使用可能な方式は、管理対象ネットワークのサイズおよび構成、タスクのタイプ、および設定に応じて異なります。

Tivoli Enterprise Portal のエージェント・タスク

Tivoli Enterprise Portal の「物理」ナビゲーター・ビューには、モニター対象ネットワークにある管理対象システムが表示されます。「ナビゲーター」メニューから、分散オペレーティング・システムで実行され、分散オペレーティング・システムで実行される Tivoli Enterprise Monitoring Server に接続する Tivoli Enterprise Monitoring Agent をリモートでデプロイおよび管理できます。

エージェントをリモート側でインストールおよび構成する前に、事前に各ターゲット・コンピューターにオペレーティング・システム (OS) エージェントをインストールする必要があります。リモート・エージェント・デプロイメント機能をサポートしないモニター・エージェントでは、「ナビゲーター」ポップアップ・メニューに「**管理対象システムの追加**」、「**構成**」、および「**削除**」オプションが表示されません。コンピューターに追加できる管理対象システムのタイプは、OS エージェントの 接続先であるモニター・サーバーのエージェント・デポ内にあるエージェント・バンドルに応じて異なります。

Tivoli Enterprise Portal からのエージェントの追加

Tivoli Enterprise Portal クライアントを使用して、モニター対象ネットワークに個別の管理対象システムを追加します。

始める前に

コンピューターにリモートでインストールできるエージェントのタイプは、OS エージェントの接続先であるモニター・サーバーのエージェント・デポ内にあるエージェント・バンドルに応じて異なります。「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ご使用の環境へのモニター・エージェントのデプロイ』のトピックに、モニター・サーバーでのエージェント・デポの設定方法、およびエージェントのデプロイ先の各コンピューターでの OS エージェントの設定方法が記載されています。

OS エージェントがインストールされたら、「物理」ナビゲーター・ビューでオンライン管理対象システムごとに 1 つずつの項目が追加されます。

この機能を使用するには、ユーザー ID に**エージェント管理**用の**管理**許可が必要です。

このタスクについて

次の説明に従って、Tivoli Enterprise Portal から管理対象システムをインストールおよび構成してください。

手順

1. 「物理」ナビゲーター・ビューで、モニター・エージェントをインストールするコンピューターの システム・レベルのナビゲーター項目を右クリックします。 この例では、ORANGE、PEAR、CABBAGE、および ONION というコンピューターが使用可能になっています。
   - 「エンタープライズ」
     - Linux システム
       - ORANGE
       - PEAR
     - Windows システム
       - CABBAGE
       - ONION
2. 「**管理対象システムの追加**」をクリックして、「モニター・エージェントの選択」ウィンドウを開きます。 このリストに表示されるエージェントは、このコンピューターが実行されているオペレーティング・システムで使用可能なエージェントです。 この 2 桁のバージョン番号のあとに、2 桁のリリース番号、さらに 5 桁以内の修正番号が続きます。
3. インストールするモニター・エージェントのタイプを強調表示し、「**OK**」をクリックします。 エージェントのタイプによっては、新しい管理対象システムの操作がキューに入れられ、トランザクション ID が表示されます。その他のタイプのエージェントについては、表示されるウィザードで、このシステムにエージェントを構成できます。
4. フィールドに入力してエージェントを構成します。ページ間を移動する場合は、「**次へ**」および「**戻る**」をクリックします。
5. 「**エージェント**」ページで、管理対象システム上でエージェントを実行するためのオペレーティング・システム・ユーザー ID を設定します。 *Windows*: デフォルトを受け入れて、使用しているユーザー ID で管理対象システムを開始するか (「**サービスにデスクトップとの対話を許可する**」チェック・ボックスを選択して、リモート・コントロールを使用可能にすることもできます)、または、「**このアカウントを使用する**」を選択して、エージェントを実行する際のユーザー名およびパスワードを入力します。

   Windows 以外: エージェントを実行するときの **ユーザー名**および**グループ名**を入力してください。
6. 「**完了**」をクリックして、管理対象システムの構成を完了します。 入力した情報のいずれかが無効の場合は、エラー・メッセージが表示され、構成ウィンドウに戻ります。入力を確認し、適宜編集して、正しく構成してください。 インストールおよびセットアップが開始されます。ご使用の Tivoli Monitoring 構成、管理対象システムのロケーション、およびモニター・エージェントのタイプによっては、完了まで数分かかることがあります。

7. 管理対象システムがエンタープライズに追加されたら、ナビゲーター・ビューのツールバーの 「**保留中の更新の適用**」をクリックします。 新規の管理対象システム (Universal Database など) が、システム・ナビゲーター項目の下に表示されます。

Tivoli Enterprise Portal からのエージェントの構成

Tivoli Enterprise Portal クライアントには、個別の管理対象システムの構成に役立つ機能があります。OS エージェントはすでに構成済みで、実行中であるため、このエージェントの構成方法は OS エージェントには適用されません。

始める前に

この機能を使用するには、ユーザー ID にエージェント管理用の管理許可が必要です。

このタスクについて

モニター・エージェントを構成するには、次のステップを完了します。

手順

1. 構成またはアップグレードする エージェントのナビゲーター項目を右クリックします。
2. 「**構成**」をクリックして、「管理対象システムの構成」ウィンドウを開きます。
3. フィールドを編集してエージェントを構成します。ページ間を移動する場合は、「**次へ**」および「**戻る**」をクリックします。 「**エージェント**」の横のページはどれも、エージェント・タイプに固有のものです。
   - Performance Analyzer、要約およびプルーニング・エージェント、およびウェアハウス・プロキシー: 「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Data Warehouse ソリューション』を参照してください。
   - Universal Agent: メタファイルおよびスクリプト・ファイルを指定してください。これらの機能についての説明は、*IBM Tivoli Monitoring Universal Agent ユーザーズ・ガイド* に記載されています。
   - 基本エージェント以外: IBM Tivoli Monitoring インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/welcome.htm) または IBM Tivoli Documentation Central (http://www.ibm.com/tivoli/documentation) にある当該製品のインストール・ガイドを参照してください。
4. 「**エージェント**」ページで、エージェントの保守に使用されるユーザー ID を設定します。

   Windows:

   ご使用の Tivoli Enterprise Portal ユーザー ID を使用する場合は、デフォルトの ◉ 「**ローカル・システム・アカウントを使用**」を受け入れます。□ 「**サービスとデスクトップとの相互作用を許可**」 を選択して、リモート・コントロールを使用可能にすることもできます。または、○ 「**このアカウントの使用**」 を選択して、エージェントを制御する際のユーザー名とパスワードを入力してください。

Windows 以外 :
エージェントを実行するときの **ユーザー名**および**グループ名**を入力してください。

5. 「**完了**」をクリックして、管理対象システムの構成を完了します。 入力した情報のいずれかが無効の場合は、エラー・メッセージが表示され、構成ウィンドウに戻ります。入力を確認し、適宜編集して、正しく構成してください。

Tivoli Enterprise Portalからのエージェント・プロセスの開始、停止、およびリサイクル

Tivoli Enterprise Portal を使用して、オフラインになっている管理対象システムを開始したり、リサイクルまたは停止したりすることができます。

始める前に

この機能を使用するには、ユーザー ID に**エージェント管理**用の**管理**許可が必要です。

このタスクについて

すべてのデプロイメント・コマンドは、ターゲット・コンピューターにインストールされているオペレーティング・システム・エージェントを通じて渡されます。オペレーティング・システム・エージェントがインストールされていない場合は、デプロイしたエージェントを開始または停止できません。

手順

- Tivoli Enterprise Portal からモニター・エージェントを開始する手順
  1. 「物理」ナビゲーター・ビューで、オフラインのエージェントのナビゲーター項目 を右クリックします。
  2. 「**開始**」をクリックします。 モニター・エージェントの開始要求は、その接続先であるモニター・サーバーに送られます。 モニター構成に応じて、エージェントが実行を開始して、ナビゲーター項目が使用可能になるまで、少し時間がかかることがあります。 モニター・エージェントが開始せず、エラー・メッセージが表示される場合は、コンピューターが使用可能になっていない可能性があります。
- Tivoli Enterprise Portal からモニター・エージェントを停止する手順
  1. 「物理」ナビゲーター・ビューで、停止する エージェントを右クリックします。
  2. 「**停止**」をクリックします。 エージェントがオフラインになり、「ナビゲーター」項目がグレーアウト表示になります。このエージェントは手動で開始するまでオンラインになりません。また自動で開始するように設定されている場合は、接続先のモニター・サーバーを再始動するまでオンラインになりません。
- Tivoli Enterprise Portal からモニター・エージェントをリサイクルする手順
  1. 「物理」ナビゲーター・ビューで、停止する エージェントを右クリックします。

2. 「**再始動**」をクリックして、モニター・エージェントを停止してから開始します。ネットワーク・トラフィックによっては、少し時間がかかる場合があります。

Tivoli Enterprise Portal からのエージェントの更新

分散モニター・エージェントの新規バージョンがリリースされている場合は、その新規バージョンを、一度に 1 つの管理対象システムに対して、または同時に多数の管理対象システムに対して、ローカル側またはリモート側から適用できます。更新を適用するには、Tivoli Enterprise Portal クライアントの「管理対象システムの構成」ウィンドウを使用します。

始める前に

この機能は、OS モニター・エージェント、z/OS ベースのエージェント、またはリモート・エージェント・デプロイメント機能をサポートしない製品には適用されません。また、更新されるエージェントは、元々リモート・エージェント・デプロイメントを使用してインストールされている必要があります。 コンピューターに追加できる管理対象システムのタイプは、OS エージェントの接続先であるモニター・サーバーのエージェント・デポ内にあるエージェント・バンドルに応じて異なります。詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『ご使用の環境へのモニター・エージェントのデプロイ』のトピックを参照してください。

更新を開始する前に、後に続くプロシージャーを使用してデプロイするすべてのエージェント用に、Tivoli Enterprise Portal Server にアプリケーション・サポートをインストールする必要があります。

注: 自己記述型機能が無効でないかぎり、ご使用のモニター・エージェントが IBM Tivoli Monitoring バージョン 6.2.3 以降のインフラストラクチャーで稼働している場合は、エージェント・アプリケーション・サポートの更新は自動で行われるため、この手順は必要ありません。

このタスクについて

ポータル・クライアントからモニター・エージェントのパッチを適用するには、以下のステップを実行します。

手順

1. アップグレードするエージェントの ナビゲーター項目を右クリックします。
2. 「**構成**」をクリックして、「管理対象システムの構成」ウィンドウを開きます。
3. 「**エージェント**」タブをクリックします。
4. インストールされているモニター・エージェントのバージョンを、使用可能な製品アップデートと比較して、更新するエージェントの行を強調表示し、「**アップデートのインストール** 」をクリックします。

タスクの結果

更新のインストールが開始されます。完了するまで数分かかることがあります。表示されるリストは、デプロイメント・デポの内容を反映します。「**更新のインストール**」が使用不可になっている場合は、以下の状態が 1 つ以上存在しています。

- デポ・エントリーが製品タイプに一致していない。
- エージェントの **VVRR** フィールドとデポ・エントリーを同じにします。ここで、VV はバージョン番号、RR は改訂番号です。例えば、**0610** のエントリーでは、バージョン 6.2 エージェント用のフィックスパックを適用できません。
- デポ・エントリーのバージョンがエージェントのバージョンよりも古い。
- デポ・エントリーのホスト・バージョン・フィールドに、エージェントのホスト・プラットフォームが含まれていない。
- デポ・エントリーの前提条件フィールドに、エージェントそれ自体と同じタイプのエージェントが含まれていない。例えば、選択されているエージェントが 6.1 UD (DB2 モニター) の場合、デポ・エントリーの前提条件フィールドには、ud:061000000 などのデプロイメント・バンドル表記が含まれている必要があります。これは、パッチ・デプロイメント・バンドルを表記する方法の 1 つです。

Tivoli Enterprise Portal からのエージェントの削除

Tivoli Enterprise Portal からモニター・エージェントをアンインストールすることもできます。これを行うには、エージェントを停止して、その構成設定を削除します。エンタープライズからエージェントを削除した後、管理対象システムからエージェントを完全にアンインストールできます。エージェントを削除すると、そのエージェントの割り当て先の管理対象システム・グループ、シチュエーションまたはポリシー配布リスト、カスタム・ナビゲーター・ビュー項目から、そのエージェントが削除されます。

始める前に

この機能を使用するには、ユーザー ID に**エージェント管理**用の**管理**許可が必要です。

このタスクについて

以下のステップを完了してエージェントを削除およびアンインストールします (アンインストールはオプションです)。

注: エージェントのアンインストール時に Tivoli Enterprise Monitoring Services の管理ユーティリティーを実行していると、アンインストール・プロセスによって自動的にシャットダウンされます。

手順

1. 削除するエージェントのナビゲーター項目を右クリックします。
2. 「**削除**」をクリックします。
3. エージェントを削除するかどうか尋ねる確認メッセージが表示されたら、「**はい**」をクリックします。サブエージェントを持つエージェントを削除する場合は、別のメッセージが表示され、それらすべてを削除するかどうか尋ねられます。

4. エージェントを永久にアンインストールするかどうか尋ねる確認メッセージが表示されたら、アンインストールする場合は「**はい**」を、インストールされているエージェントをシステムに残す場合は「**いいえ**」をクリックします。

コマンド行インターフェースからのエージェントの更新

エージェントを更新するには、実行中のエージェントを停止し、変更を適用し、エージェントを再始動します。更新対象のモニター・エージェントの特性 (タイプやバージョンなど) を決定した後、コマンド行インターフェースから **tacmd updateAgent** コマンドを実行します。バージョンが指定されていない場合、エージェントは最新バージョンに更新されます。

このタスクについて

コマンド行インターフェースで次のステップを実行してください。このコマンドおよび関連コマンドに関する参考情報については、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

注: Tivoli 製品に付属の tacmd コマンドのみを使用して、バンドルを処理し、エージェント・デプロイメントを実行してください。デポ・ディレクトリー構造またはその中のバンドルおよびファイルの手動操作はサポートされておらず、ご使用の保証が無効になることがあります。

手順

1. **tacmd login** コマンドを使用して Tivoli Enterprise Monitoring Server にログインします。

```
tacmd login {-s|--server} {[{https|http}://]HOST[:PORT]}
[{-u|--username} USERNAME]
[{-p|--password}  PASSWORD]
[{-t|--timeout} TIMEOUT] [-t TIMEOUT]
```

   a. 例えば、システム *ms.austin.ibm.com* に、ユーザー名 *Admin*、パスワード *log1n* でログインするには、以下のコマンドを実行します。

```
tacmd login -s ms.austin.ibm.com -u Admin -p log1n
```

2. ログイン後に **tacmd updateAgent** コマンドを使用して、指定されたノードにエージェントの更新をインストールします。

```
tacmd updateAgent {-t|--type} TYPE {-n|--node} MANAGED-OS
 [{-v|--version} VERSION] [{-f|--force}]
```

   a. 例えば、以下のコマンドは *itmserver* 上の UNIX エージェント (タイプ *UX*) を更新します。

```
tacmd updateagent -t UX -n itmserver:KUX -v 6111
```

デプロイメント状況表のクリア

IBM Tivoli Monitoring **tacmd** コマンドを実行するか、または Tivoli Enterprise Portal ナビゲーターを使用して Tivoli Enterprise Monitoring Agent をリモートで管理するたびに、トランザクションに関する情報が Tivoli Enterprise Monitoring Server デプロイメント状況表に保持されます。特に大規模環境でのこの表の内容の管理を容易にするため、完了したトランザクションをこの表から定期的に削除する操作をスケジュールできます。

このタスクについて

完了したデプロイメント・トランザクションを随時レビューし、表を適度なサイズで維持することでモニター・サーバーのオーバーヘッドを削減するには、この機能を有効にします。完了したトランザクションをデプロイメント状況表から定期的にクリアする操作をスケジュールするには、クリア操作の実行頻度を指定する必要があります。

この機能はモニター・サーバーの CLEARDEPLOYSTATUSFREQ=*X* 環境変数により制御されます。この *X* は、表の自動クリアの実行間隔を時間数で指定します。*X* がゼロであるか、この環境変数が指定されていない場合、自動クリアは無効になります。有効な値は、0 から 720 です。

この機能は次の 2 とおりの方法で有効にできます。

- この環境変数をモニター・サーバーの構成ファイルに直接追加します。これにより、サーバーの始動時に自動クリアが有効になります。
- IBM Tivoli Monitoring Service Console を使用して、既に稼働中のモニター・サーバーでこの環境変数を設定します。

自動クリアが有効になっている場合、モニター・サーバーは完了しているデプロイ・トランザクションを自動的に検出してデプロイ状況表から削除し、削除したトランザクションに関する情報をログ・ファイルに記録します。ユーザーは後でこのログ・ファイルの情報を確認できます。自動クリアは、この環境変数の設定時に指定した間隔 (時間単位) で実行されます。

手順

- モニター・サーバー環境ファイルの変更
  1. モニター・サーバーがインストールされているコンピューター上で、環境ファイルを開きます。
     - Windows Tivoli Enterprise Monitoring Services の管理 (**「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」**) を使用します。 Tivoli Enterprise Monitoring Server を右クリックして、**「拡張」→「ENV ファイルの編集」**をクリックします。
     - Linux UNIX *install_dir* /config ディレクトリーに移動し、<*hostname*>_ms_<*temsname*>.config ファイルおよび ms.ini ファイルをテキスト・エディターで開きます。
  2. 環境変数を追加し、時間単位の間隔を指定します。例えば、CLEARDEPLOYSTATUSFREQ=1 などです。
  3. ファイルを保存します。
  4. 変更内容を実装するには、モニター・サーバーをリサイクルします。
- IBM Tivoli Monitoring Service Console を使用してモニター・サーバー環境ファイルを変更します。

  詳しくは、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」の『IBM Tivoli Monitoring Service Console の使用』を参照してください。

1. Web ブラウザーを開き、`http://hostname:1920` にアクセスします。ここで *hostname* は、モニター・サーバーが稼働しているシステムのホスト名または IP アドレスです。その後、このシステムで正しく実行されているコンポーネントに関する情報がユーティリティーに表示されます。
2. **ms** リンクを選択して、環境変数を変更します。
3. ご使用のユーザー ID とパスワードを入力します。
4. **BSS1 SET CLEARDEPLOYSTATUSFREQ=1** コマンドを入力します。この 1 は、時間単位の間隔です。

タスクの結果

モニター・サーバーの logs サブディレクトリー (Linux または UNIX の場合は *install_dir* /logs、Windows の場合は *install_dir* ¥logs) にあるログ・ファイル cleardeploystatus.log には、デプロイメント状況表でクリアされた各トランザクションを示すテキスト行が含まれています。モニター・サーバーを開始するたびに、---Clear Deploy Status Log--- がログ・ファイルに記録されます。

表からクリアされた各トランザクションに関する以下の情報がログ・ファイルに書き込まれます。

- トランザクション ID: 完了したトランザクションのグローバル・トランザクション ID。
- 実行依頼時刻: 処理のためにトランザクションが最初に実行依頼された時刻のタイム・スタンプ。
- コマンド: 処理されたデプロイメント・コマンド。
- 状況: 完了状況 (SUCCESS または FAILURE)。
- 再試行: トランザクションが完了までに再試行された回数。
- モニター・サーバー名: トランザクションを処理したモニター・サーバーの名前。
- 対象ホスト名: コマンドが実行された管理対象システムの名前または管理対象ノードの ID。
- プラットフォーム: ターゲットで稼働中の OS エージェントの報告されたプラットフォーム・アーキテクチャー。
- 製品: トランザクションが処理されたエージェントの製品コード。
- バージョン: トランザクションが試行された製品のバージョン。
- 完了メッセージ: 返された状況が失敗の場合に、失敗の理由を説明するメッセージ。

次のタスク

モニター・サーバーによってデプロイ状況表からクリアされたトランザクションが記録されるログ・ファイルの場所を変更できます。この場所を変更するには、ローカル・システム上の完全修飾パス名、またはマウントされたファイル・システム上の完全修飾パス名を指定するモニター・サーバーの構成ファイルに、環境変数 CLEARLOG を追加します。

モニター・サーバーとサーバー・バックアップがある場合には、マウントされたファイル・システムを使用すると便利です。マウントされたファイル・システムを宛先として使用し、両方のシステムのログに同じ完全修飾パス名を設定すると、フェイルオーバー状態に対応できます。

注: 活動中のハブ・モニター・サーバーによって、エンタープライズ全体のデプロイメント状況表の自動クリアが実行されます。ハブのバックアップ・モニター・サーバーがある場合は、バックアップの環境変数をハブと同じ値に設定してください。これにより、ハブのフェイルオーバーが発生するとクリア・プロセスが同時に実行されます。

エージェントが接続するモニター・サーバーの変更

複数の Tivoli Enterprise Monitoring Server が含まれているモニター対象環境では、すべてまたは一部のエージェントをリモート・モニター・サーバーに接続させることができます。エージェントを再構成することにより、エージェントの接続先となるモニター・サーバーを変更できます。

このタスクについて

以下のオプションのいずれかを使用して、モニター・エージェントを別のモニター・サーバーに再度割り当ててください。

手順

- エージェントがインストールされているコンピューター・システムで Tivoli Enterprise Monitoring Services の管理 アプリケーションを使用します。モニター・エージェントを右クリックして、「**再構成 (Reconfigure)**」をクリックします。1 番目の「エージェント拡張構成」ウィンドウで「OK」をクリックしてから、接続するモニター・サーバーの**ホスト名**または **IP アドレス**を入力します。使用するポートがデフォルトの 1918 以外の場合は、**ポート**番号を入力します。

  エージェントが Linux または UNIX にインストールされている場合は、**itmcmd agent -A <product_code>** コマンドを使用して再構成することもできます。
- **tacmd setAgentConnection** コマンドを使用してエージェントをリモートで再構成します。このコマンドについて詳しくは、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。
- IBM Tivoli Monitoring V6.3 以降のモニター・サーバーでは IBM Tivoli Monitoring ログイン・デーモン・ソリューションを使用してください。このソリューションは IBM Service Management Connect から入手できます。このログイン・デーモンは、接続するモニター・エージェントを処理し、以下の顧客提供スクリプトを呼び出すツールです。

  Select TEMS
  このスクリプトは、エージェントが正しくないモニター・サーバーに接続した場合に、エージェントを再構成して接続先として指定する必要があるプライマリー・モニター・サーバーとセカンダリー・モニター・サーバーを示す情報を返します。

After Login
このスクリプトは、エージェントが指定されたモニター・サーバーに接続した後に、そのエージェントのセットアップまたは構成を実行するときに使用できます。例えば、このスクリプトは、管理対象システム・グループにエージェントを追加するか、またはエージェントがインストールされているシステムをスキャンして、必要に応じて追加エージェントをリモートでデプロイする場合に使用できます。

ログイン・デーモン・ソリューションの詳細と、ご使用の環境でこのソリューションを使用できるかどうかについては、TEMS Login Policies for Agentsを参照するか、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) に直接アクセスして、「login policies」を検索してください。**注**: このソリューションは IBM Service Management Connect でのみ入手可能です。

次のタスク

Universal Agent を異なるモニター・サーバーに接続するよう再構成する場合は、管理対象システムに配布されているシチュエーションをすべて再始動します。再始動しないと、自動開始するように設定されているシチュエーションは、開始に失敗してエラーが発生します。

自己記述型モニター・エージェント

自己記述が有効な IBM Tivoli Monitoring V6.2.3 以降のモニター・エージェントには、Tivoli Management Services サーバーを更新するのに必要なすべてのアプリケーション・サポート・ファイルが含まれます。手動でサポート・インストール手順を実行したり、エージェントをサポートする個々のサーバー・コンポーネントをリサイクルしたりする必要はありません。

自己記述型モニター・エージェントによって、エージェントの接続時に他のコンポーネントに自動的にバージョン更新が適用されます。Tivoli Management Services のサーバーであるハブ・モニター・サーバー、リモート・モニター・サーバー、およびポータル・サーバーをリサイクルする必要はありません。製品サポートを自動的にインストールするこの機能によって、IBM Tivoli Monitoring サーバー上のアプリケーション・データの不整合なインストールにより発生する可能性があるエラーをなくすことができます。自己記述型機能を使用するには、Tivoli Management Services V6.2.3 以降を使用している必要があります。

モニター・エージェントで自己記述型機能がサポートされている場合、アプリケーション・サポートはエージェント・システムにインストールされます。モニター・エージェントに IBM Tivoli Monitoring V6.2.3 以降のエージェント・フレーム・ワークが含まれる場合、またはモニター・エージェントがインストールされているシステムに V6.2.3 以降のエージェント・フレームワークが既にインストールされている場合は、エージェントの開始後にモニター・サーバーとポータル・サーバーによってエージェントからアプリケーション・サポート・ファイルが取得され、自動的にサポートが適用されます。インフラストラクチャー・サーバーでは、まだアプリケーション・サポートが適用されていない、または以前のバージョンのアプリケーション・サポートが適用されている場合にのみ、自己記述型エージェントからアプリケーション・サポートが取得されます。

自己記述型の更新は、特定の各エージェント・バージョンに対して 1 回のみ行われます。エージェントがモニター・サーバーに接続したときに、使用可能なアプリケーション・サポートの更新についてモニター・サーバーに自動的に通知が行われるように、更新ファイルはエージェントに格納されます。自己記述型機能が有効にされている場合は、アプリケーション・サポートがエージェントから取得され、モニター・サーバーのサポートが更新されます。

モニター・サーバーを Linux またはUNIX にインストールした場合は、すべてのベース・モニター・エージェントとその他のサポート・エージェントのアプリケーション・サポート・ファイルがそのモニター・サーバーに自動的にインストールされています。このプロセスは、Windows にモニター・サーバーをインストールした場合と異なり、Linux または UNIX のインストールでは常にモニター・エージェントのアプリケーション・サポート・ファイルが自動的にインストールされます。モニター・サーバーとポータル・サーバーを検査して、自己記述型エージェント製品が予想通りにインストールされていることを確認してください。

IBM Tivoli Monitoring V6.3 の Tivoli Enterprise Monitoring Automation Server コンポーネントには、Open Services Lifecycle Collaboration Performance Monitoring (OSLC-PM) サービス・プロバイダーが含まれています。Performance Monitoring サーバー・プロバイダーでは、アプリケーション・サポート・ファイルの動的リフレッシュはサポートされていません。つまり、新しいアプリケーション・サポートがシステムに追加される場合、そのサポートが自己記述型エージェントを介して追加されたか、通常のインストールによって追加されたか、または手動コピーによるものかに関係なく、Tivoli Enterprise Monitoring Automation Server をリサイクルする必要があります。ただし、モニター・エージェントに OSLC サポートが含まれていない場合、オートメーション・サーバーをリサイクルする必要はありません。通常、IBM Tivoli Monitoring V6.3 より前のエージェントには OSLC サポートは含まれていません。エージェントの資料を参照し、エージェントに OSLC サポートが含まれているかどうかを確認してください。

自己記述型エージェント機能によってアプリケーション・サポートが Tivoli Enterprise Portal Server にインストールされ、ダッシュボード・データ・プロバイダー・コンポーネントを有効にした場合、新しいまたは変更されたアプリケーション・サポートをダッシュボード・データ・プロバイダーが発見し、それを使用してモニター・ダッシュボード向けにデータを取得できるようにするためには、ポータル・サーバーを再起動する必要があります。

ロードマップ

次のロードマップを使用すると、自己記述型の機能を構成、有効化、および使用する際に役立ちます。このロードマップは概要を示すものであるため、該当する場合は他の Tivoli Monitoring ガイドの関連セクションへのリンクが記載されています。

ステップ	説明および提供される情報
1	使用可能なインストール・シナリオには、初期インストールとアップグレード・インストールの 2 種類があります。*IBM Tivoli Monitoring インストールおよび設定ガイド*の『Configuring self-describing agent seeding』を参照してください。 **追加情報:** シードに関する情報は、 333 ページの『自己記述型の自動最新表示およびシード』にも記載されています。 **editSdaOptions** コマンドについては、「*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)」を参照してください。
2	ハブ・モニター・サーバーで自己記述型機能を構成します。この初期セットアップについて詳しくは、*IBM Tivoli Monitoring インストールおよび設定ガイド*の『Enabling self-describing agent capability at the hub monitoring server』を参照してください。このステップでは、各ハブ・モニター・サーバーの環境変数 `KMS_SDA=Y` の設定も行います。 **追加情報:** 今後の参照情報と初期セットアップ完了後の管理者の作業については、335 ページの『モニター・サーバーでの自己記述型機能の有効化または無効化』を参照してください。

ステップ	説明および提供される情報
3	**注**: IBM Tivoli Monitoring V6.3 を実行していない場合はこのステップをスキップしてください。 IBM Tivoli Monitoring V6.3 では、次のいずれかのコマンドを実行するまでは、デフォルトですべての自己記述型エージェントのインストールがハブ・モニター・サーバーによりブロックされます (ハブ・モニター・サーバーで、ステップ 2 の設定値 `KMS_SDA=Y` を使用して自己記述型機能が有効になっている場合を含む)。 • **`tacmd addSdaInstallOptions`**: 自己記述型エージェント機能のインストールを許可する製品とバージョンを指定します。 または • **`tacmd editSdaInstallOptions -t DEFAULT -i ON`**: すべての製品とバージョンでインストールを許可し、ブロックしません (この設定は基本的に、V6.2.3 および V6.2.3 FP1 でのデフォルトの自己記述型エージェント動作です)。 この機能により、自動自己記述型エージェント・プロセスによってモニター・サーバーとポータル・サーバーにインストールされる製品とバージョンをより細かく制御できます。 インストール・オプションを変更したら、**`tacmd listSdaInstallOptions`** コマンドを使用してハブ・モニター・サーバーの現在のインストール構成を表示できます。 詳細および **`tacmd`** コマンドについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『自己記述型エージェントのインストールの管理』および『Dynamically controlling the hub monitoring server self-describing agent capability』を参照してください。 **追加情報:** 完全な構文情報については、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。 今後の参考として、初期セットアップ後にこれらのインストール・オプションを更新または変更する方法を確認するには、331 ページの『自己記述型機能によるインストールのオプションの動的更新』を参照してください。

ステップ	説明および提供される情報
4	**tacmd listappinstallrecs** コマンドは、アプリケーション・サポートのインストール・レコードをモニターするために使用します。 **tacmd listSdaStatus** コマンドを使用して、ご使用の環境内のすべてのモニター・サーバーにおける自己記述型機能の状況 (有効および中断) をモニターします。 326 ページの『自己記述型エージェントのインストール』を参照してください。 **追加情報:** 再試行可能なインストール・レコードと再試行できないインストール・レコードについては、329 ページの『自己記述型エージェントのインストール・エラー』を参照してください。 完全な構文情報については、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。
5	自己記述型のアプリケーション更新が完了したら、次の新しいエージェント・データがポータル・クライアントに表示されます。 • ヒストリカル構成が新しい属性で更新されます • ワークスペースが更新されます • 新規または更新されたシチュエーション、ポリシー、およびアクション実行 (新しいシチュエーションが配布され、ユーザーが構成可能なシード・オプションを使用して自動開始されます) • 照会が更新されます • ヘルプ・サーバー・ファイルが更新されます アプリケーション・サポートは Tivoli Enterprise Portal クライアントに自動的に適用されません。 インディケーターがこれらのクライアントに表示され、クライアントをリサイクルして新規または変更されたアプリケーション・サポートを適用する必要があることをユーザーに示します。 • Tivoli Enterprise Portal デスクトップ・クライアントを使用している場合は、モニター・エージェントのインストール・イメージを使用して、Tivoli Enterprise Portal のアプリケーション・サポートを各デスクトップ・クライアントにインストールする必要があります。 • Tivoli Enterprise Portal ブラウザー・クライアントまたは Java WebStart クライアントを使用しており、更新されたアプリケーションを表示するのに必要なユーザー権限がある場合は、インディケーターが表示された後、このクライアントを閉じて再始動し、新しい更新を表示できます。 **追加情報:** サポート・インディケーターについて詳しくは、*Tivoli Enterprise Portal ユーザーズ・ガイド* のアプリケーション・サポート・イベントへの対応を参照してください。

ステップ	説明および提供される情報
6	事前診断テストを開始し、問題のトラブルシューティングを行うには、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」の『モニター・エージェントのトラブルシューティング』を参照してください。 **追加情報:** メッセージについて詳しくは、「*IBM Tivoli Monitoring Messages* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/messages/itm_messages.htm)」を参照してください。

モニター・サーバーでの自己記述型のイベント・フロー

自己記述型エージェント用に自動化されるイベント・フローは、エージェントがハブ・モニター・サーバーまたはリモート・モニター・サーバーに接続されている場合は異なります。

ハブ・モニター・サーバーに接続されている自己記述型エージェント

次のステップで、ハブ・モニター・サーバーに接続している自己記述型エージェントのイベント・フローの概要を示します。

1. ハブ・モニター・サーバーの自己記述型エージェント・マネージャーは、製品のアプリケーション・サポートのバージョンがハブ・モニター・サーバーにすでにインストールされているかどうかを確認します。その製品のアプリケーション・サポート・バージョンがまだインストールされていない場合、ハブ・モニター・サーバーはエージェントからサポート・ファイルを取得します。
2. ハブ・モニター・サーバーは、自己記述型エージェントの製品インストールと、モニター・サーバーの内部製品定義の構成の動的リフレッシュを開始します。このハブ・モニター・サーバーの自己記述型エージェントのインストールの完了状況は、以下の場所に記録されています。
   - ローカルの Tivoli Enterprise Monitoring Server のアプリケーション・プロパティー・テーブル。
   - Tivoli Enterprise Monitoring Server の監査ログ機能。
   - Tivoli Enterprise Monitoring Server の MSG2 ログ機能。
   - Tivoli Enterprise Monitoring Server の RAS1 ログ。
   - 配布された Tivoli Enterprise Monitoring Server プラットフォームの場合、自己記述型エージェントのインストール・プログラムのログ・ファイルは、`installsdsupport_*.trc` および `installsdsupport_*.log` です。 Windows コンピューターの場合、ログは *`install_dir`* `¥logs` ディレクトリーにあります。 Linux および UNIX コンピューターの場合、ログは *`install_dir`* `/logs` ディレクトリーにあります。
3. ハブ・モニター・サーバーの製品インストールが正常に完了すると、実行中かつハブ・モニター・サーバーに接続されているすべての Tivoli Enterprise Portal Server プロセスに、新規のまたは更新された製品サポートが通知されます。

   ホット・スタンバイ (FTO) に対応した環境では、自己記述型構成データがスタンバイ・ハブ・モニター・サーバーに複製されます。スタンバイ・ハブ・モニター・サーバーでは リモート・モニター・サーバーのエージェントからの直接接続はサポートされていません。つまり、自己記述型インストールではスタンバ

イ・ハブを直接開始できません。活動中のハブによる自己記述型インストールが完了すると、活動中のハブによりスタンバイ・ハブでの自己記述型インストールが開始されます。スタンバイ・ハブでの自己記述型インストール・プロセスでは、活動中のハブから製品サポート・ファイルが取得されます。FTO 環境について詳しくは、「*Tivoli IBM Tivoli Monitoring バージョン 6.2.1 分散システム用高可用性ガイド*」を参照してください。

4. Tivoli Enterprise Portal Server は、ハブ・モニター・サーバーと同じ基本ステップを実行します。そのバージョンの製品がすでに Tivoli Enterprise Portal Server にインストールされているかどうかを確認します。 ただし、製品サポート・ファイルは、ハブ・モニター・サーバーから直接取得され、接続されているエージェントからは取得されません。
5. Tivoli Enterprise Portal Server は、自己記述型エージェントの製品インストールと、ポータル・サーバーの内部製品定義の構成の動的リフレッシュを開始します。
6. Tivoli Enterprise Portal Server は、任意の実行中の Tivoli Enterprise Portal ブラウザー・クライアントおよび Tivoli Enterprise Portal Desktop Client に、新しいまたは更新済みの製品サポートが使用可能であることを通知します。このTivoli Enterprise Portal Serverの自己記述型エージェントの製品インストールの完了状況が、次の場所に記録されます。
   - Tivoli Enterprise Portal Server の監査ログ機能。
   - Tivoli Enterprise Portal Server の RAS1 ログ。
   - Tivoli Enterprise Portal Server の自己記述型エージェントのインストール・プログラムのログ・ファイル (`installsdsupport_*.trc` および `installsdsupport_*.log`)。 Windows コンピューターの場合、ログは *`install_dir`* `¥logs` ディレクトリーにあります。 Linux/UNIX コンピューターの場合、ログは *`install_dir`* `/logs` ディレクトリーにあります。

リモート・モニター・サーバーに接続されている自己記述型エージェント

次のステップで、リモート・モニター・サーバーに接続している自己記述型エージェントのイベント・フローの概要を示します。

1. リモート・モニター・サーバーの自己記述型エージェント・マネージャーは、その製品がハブ・モニター・サーバーに最初にインストールされていることを確認します。
2. 製品がハブ・モニター・サーバーに最初にインストールされていない場合、リモート・モニター・サーバーは、ハブ・モニター・サーバーにその製品を最初にインストールするように指示します。
3. ハブ・モニター・サーバーのインストールが完了すると、リモート・モニター・サーバーは、その製品がこのモニター・サーバーにローカルにインストールされているかどうかを確認します。
4. リモート・モニター・サーバーの製品インストールは、ハブ・モニター・サーバーと同様に実行されます。
5. 何らかの理由でハブ・モニター・サーバーの製品インストールが失敗した場合、リモート・モニター・サーバーはその製品をインストールしません。

モニター・サーバーは、既存のモニター・サーバーのエラー状況が修正され、失敗した自己記述型エージェントの製品インストール・レコードがモニター・サーバーのアプリケーション・プロパティー・テーブルから削除されるまで、他のすべての失敗した自己記述型エージェントのインストール要求の再試行を許可しません。詳しくは、 329 ページの『自己記述型エージェントのインストール・エラー』を参照してください。

注:

ハブ・モニター・サーバーで自己記述型エージェント機能が使用可能かどうかによって、リモート・モニター・サーバーでこの機能を利用できるかどうかが決まります。ハブ・モニター・サーバーで自己記述型エージェントのエラーが発生して、そのハブに接続されているリモート・モニター・サーバーで自己記述型エージェント機能が無効になる場合は、エラー・メッセージが表示されます。エラー・メッセージについて詳しくは、*IBM Tivoli Monitoring トラブルシューティング・ガイド*を参照してください。

ハブ・モニター・サーバーで自己記述型エージェントのエラーが修正されると、リモート・モニター・サーバーは、ハブへの次の再接続時に、自己記述型エージェント機能がそのハブで使用可能であることを検出します。結果として、リモート・モニター・サーバーでローカルに自己記述型エージェントが再度有効になります。

起動時にモニター・サーバーによって検出される変更

Tivoli Enterprise Monitoring Server は、起動時に次の情報を検出します。

- 手動でインストールされた製品 (例えば、自己記述型の機能を使用せずにインストールされたアプリケーション)。
- インストール済みの製品に対する手動の更新 (カタログおよびバージョン・ファイルの変更)。例えば、自己記述型エージェント・インストールの外側で発生する、ユーザーが開始する製品の変更です。
- 失敗した自己記述型エージェントのインストール。

Tivoli Enterprise Monitoring Server は、インストール済みの製品で検出された変更に基づいて、調整および修正を行います。有効なモニター・サーバーのバージョン・ファイル (VER ファイル) を持つ製品のみが、起動時に検出されます。このプロセスは、自己記述型エージェントのインストール・マネージャーがモニター・サーバーで有効になっている場合 (**KMS_SDA=Y**) に自動的に実行されます。この機能は、インストール済みの製品およびバージョンの正確なインベントリーを維持するために役立ちます。自己記述型エージェントのインストール・マネージャーが有効でない場合、この機能は実行されません。

自己記述型エージェントのインストール

ローカル・モニター・サーバー・アプリケーションのプロパティー表 (TAPPLPROPS) には、モニター・サーバーの自己記述型エージェントの製品インストール結果が格納されます。この表には、手動でインストールされたモニター・サーバー製品の現在検出されたバージョンが格納されます。

この表には、インストール・オプション、シード配布、中断レコードなどの自己記述型機能に関する情報も格納されます。 TAPPLPROPS の属性について詳しくは、

「*Tivoli Enterprise Portal* ユーザーズ・ガイド」の「アプリケーション・プロパティー・インストール」属性を参照してください。

モニター・サーバーの自己記述型機能の状況を調べるには 2 種類の **tacmd** コマンドを使用できます。

- **tacmd listSdaStatus** (稼働状況)
- **tacmd listappinstallrecs** (製品インストール状況)

tacmd listSdaStatus コマンドの使用

IBM Tivoli Monitoring V6.3 以降では、**tacmd listSdaStatus** コマンドはモニター・サーバーの自己記述型機能の有効化状況を表示します。モニター・サーバーのリストまたはすべてのモニター・サーバー (デフォルト) の、自己記述型機能の有効化状況を表示できます。 IBM Tivoli Monitoring V6.3 以降のハブ・モニター・サーバーに対してこのコマンドを実行すると、モニター・サーバーの自己記述型エージェント機能の稼働状態 (中断またはアクティブ) も表示されます。ハブの自己記述型エージェント機能の稼働状態 (中断またはアクティブ) から、このハブ・モニター・サーバーに接続されているすべてのモニター・サーバーの自己記述型アクティビティーがわかります。

自己記述型機能の有効化状況は、HUB/RTEMS name、STATE、および STATUS の値によって示されます。

以下の例では、自己記述型機能が現在中断されていることをメッセージが示しています。HUB_A と RTEMS_1 は両方とも自己記述型機能に対応しています。STATUS コード 0 は、自己記述型機能が有効であることを示します。自己記述型機能に対して RTEMS_2 が無効になっており、その説明として状況コード16 (KMS_SDA=N のため、SDA は使用不可です (SDA disabled because KMS_SDA=N)) が示されています。

```
tacmd listSdaStatus
KUILSS203I: SDA 機能は中断されています。
HUB/RTEMS   STATE   STATUS
HUB_A       ON      0
RTEMS_1     ON      0
RTEMS_2     OFF     16
```

tacmd listSdaStatus コマンドの STATUS コードの詳細、例、および説明については、*IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください

tacmd listappinstallrecs コマンドの使用

tacmd listappinstallrecs コマンドは、アプリケーション・サポートのインストール・レコードをモニターするために使用します。

このコマンドは、アプリケーション・サポートのインストール・レコードを返し、環境内のすべてのモニター・サーバーの自己記述型エージェントの製品インストール状況を表示します。モニター・サーバーが稼働していないときは、このコマンド

を使用できないことに注意してください。モニター・サーバーおよびポータル・サーバーの両方を始動した場合は、監査ログ・ワークスペースで自己記述型エージェントの情報および設定を確認することもできます。 257 ページの『第 9 章 監査ロギング』を参照してください。

tacmd listappinstallrecs コマンドは、環境内のすべてのモニター・サーバーに対する自己記述型エージェント製品の現在のインストール状況を表示します。

HUB/RTEMS	PRODUCT	VERSION	GRPID	ID	IDVER	SEEDSTATE	STATE	STATUS
HUB_LZ	A4	06300000	5655	TMS	06300000			0
HUB_LZ	HD	06300000	5655	TMS	06300000	Y	IC	0
HUB_LZ	HD	06300000	5655	TPW	06300000		IC	0
HUB_LZ	LZ	06230000	5655	TPS	06230000		IC	0
HUB_LZ	NT	06230000	5655	TMS	06230000			0
HUB_LZ	TM	06230000	5655	TMS	06230000			0
HUB_LZ	11	06230000	5655	TMS	06230000		ME	1005
RTEMS_LZ	A4	06230000	5655	TMS	06230000			0
RTEMS_LZ	LZ	06230000	5655	TMS	06230000	Y	IC	0
RTEMS_LZ	R6	06230000	5655	TMS	06230000			0
RTEMS_LZ	11	06230000	5655	TMS	06230000	Y	ME	1014

HUB/RTEMS の列には、レコードが収集された モニター・サーバーのノード名がリストされます。 STATE 列が IC の行は、自己記述型エージェントのインストールの完了を表します。また、この例ではハブ・モニター・サーバーとリモート・モニター・サーバーの両方に、モニター・サーバー・サポート (TMS) の appinstallrecs エントリーがあることを確認できますが、ハブ・モニター・サーバーにはこの他にポータル・サーバー・サポート (TPS) パッケージとポータル・ブラウザー・クライアント・サポート (TPW) パッケージの 2 つの appinstallrecs エントリーがあります。これらの追加パッケージはハブ・モニター・サーバーにのみインストールされているため、ポータル・サーバーに対しては使用可能です。

STATE 列がブランクの場合は、アプリケーション・サポートは手動でインストールされています。-d (詳細) オプションを使用した場合は MANUALINST 列に Y が表示されます。自己記述型エージェント appinstallrecs の状態は以下のとおりです。

IR　インストール要求: 作業キュー上の新しいインストール要求。

IM　メタデータのインストール: 作業キューからインストール要求を取得して、メタデータのインストールを開始し、作業の自動最新表示を行います。

MC　メタデータの完了: メタデータのインストールおよび自動最新表示が完了しました。

IC　インストールの完了: SDA アプリケーション・サポートは正常に完了しました。

ME　メタデータ・エラー: メタデータのインストール・エラー。STATUS コードは追加情報を提供します。

ヒント: IR、IM、および MC の appinstallrecords はすべて、自己記述型エージェントの通常のインストールが進行中であることを示します。STATE の値が ME であ

るアプリケーション・サポートのインストール・レコードについては、『自己記述型エージェントのインストール・エラー』を参照してください。

tacmd listappinstallrecs コマンドの STATUS コードについて詳しくは、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

IBM Tivoli Monitoring V6.3 以降では、**listappinstallrecs -t TEMS** オプションはサポートされていません。代わりに、**listSdaStatus** コマンドを使用します。

自己記述型エージェントのインストール・エラー

失敗コードは、**listappinstallrecs** 出力の **STATUS** 列で報告されます。エラーには、再試行可能なものと致命的なものがあります。

再試行可能な自己記述型エージェントのインストール・エラー

Tivoli Enterprise Monitoring Agent の自己記述型エージェント・サービスによって、以前に失敗した自己記述型エージェントの登録要求またはインストール要求のうち、いずれのタイプの要求を再試行するが判別されます。モニター・サーバーへの自己記述型エージェント登録要求のために、Tivoli Enterprise Monitoring Server から返される以下のタイプの失敗またはエラー・コードのみが再試行されます。

1006　重複した SDA インストール要求

1009　ハブがありません

1017　一時的なインストール・エラー

1021　サーバーはタイムアウトしました

再試行可能な自己記述型エージェント・インストール・エラーは、開始されたものの、まだ Tivoli Enterprise Monitoring Server のどのファイルまたは内部構造も変更していない登録要求またはインストール要求です。

再試行不能な自己記述型エージェントのインストール・エラー

STATE の値が ME であるエラー・レコードの場合、インストールは再試行されません。

次の例では、製品コード 11 のインストール・レコードで **STATE** の値が ME と表示されています。

HUB/RTEMS	PRODUCT	VERSION	GRPID	ID	IDVER	SEEDSTATE	STATE	STATUS
RTEMS_LZ	11	06230000	5655	TMS	06230000	Y	ME	1014

STATE の値が ME の場合は、自己記述型エージェントのメタデータのインストール・エラーが モニター・サーバー で発生しています。モニター・サーバーは、管理者がエラーを修正する何らかのアクションを行うまで、この製品コードに対する自己記述型エージェントのインストールの試行をすべて停止します。この修正を行うには、IBM ソフトウェア・サポートを利用する必要がある場合があります。このシナリオの場合、問題が解決したら **tacmd deleteappinstallrecs** コマンドを使用して、自己記述型エージェントのエラー・レコードを消去する必要があります。詳

しくは、*IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

自己記述型エージェントの製品インストールが再試行不能なエラー状態で失敗したかどうかを判断するには、**-e** オプションを使用して **tacmd listappinstallrecs** コマンドを実行し、エラー・レコードのみを表示します。**STATE** の値が ME であるエラー・レコードの場合、インストールは再試行されません。

自己記述型エージェントのインストールを再試行するには、次のステップを実行します。

1. 同じ失敗が再発しないようにするため、まずインストールが失敗する原因となった状態を修正します。また、モニター・サーバーのメッセージ機能 (監査、MSG2、および RAS1 メッセージ) によって、失敗の原因についての詳細が提供されます。この状態を修正するアクションを実行するか、IBM ソフトウェア・サポートまで連絡してください。
2. モニター・サーバーごとに、**tacmd deleteappinstallrecs** コマンドを実行してアプリケーション・プロパティー・テーブル内の失敗したインストールのレコードを削除します。このコマンドで、障害となっている自己記述型エージェント製品のインストール・レコードが削除されます。詳しくは、「*IBM Tivoli Monitoring* コマンド・リファレンス」を参照してください。
3. 各モニター・サーバーの製品インストール失敗レコードが消去されると、モニター・サーバーの自己記述エージェント機能によって、このレベルの製品サポートを提供できる稼働中の自己記述型エージェントに対し、製品のインストールを再試行するように即時に通知が行われます。例えば、製品 *pc* バージョン 06230000 の前回のインストール操作が、**STATE** が ME で失敗した場合、**deleteappinstallrecs** コマンドを実行すると、稼働中のバージョン 06230000 の *pc* エージェントが即座にインストールを再試行します。
4. 製品 *pc* に対して再度 **tacmd listappinstallrecs -t <pc>** を実行し、現在のインストール状態を判断します。

プライマリー・ハブ モニター・サーバー で自己記述型エージェントの製品インストールが失敗した場合、スタンバイ・ハブはサポートのインストールを試行しません。プライマリー・ハブでの失敗原因を修正してから、**deleteappinstallrecs** コマンドを使用してエラー・エントリーをプライマリー・ハブから削除します。エラーを消去することで、自己記述型エージェントの製品インストールが再試行されます。

自己記述型エージェントの製品インストールがスタンバイ・ハブでのみ失敗する場合、スタンバイ・ハブで失敗の原因を修正します。プライマリー・ハブにログオンしている間は、**deleteappinstallrecs** コマンドに **-n <standby_TEMS_name>** オプションを指定して実行し、スタンバイ・モニター・サーバーからエラー・エントリーを削除できます。これにより、自己記述型エージェントのインストールを再試行できます。アプリケーション・インストール・レコードをプライマリー・モニター・サーバーまたはリモート・モニター・サーバーから削除した場合とは異なり、アプリケーション・インストール・レコードをスタンバイ・ハブから削除しても、自己

記述型エージェントの製品インストールは自動的には再試行されません。スタンバイ・ハブでエージェント製品サポートが一時的に欠落していても問題はありません。

- スタンバイ・ハブがリサイクルされ、欠落している製品サポートがディスカバーされると、その時点で自己記述型エージェントの製品インストールが実行されます。
- スタンバイ・ハブが活動中のハブにプロモートされると、最初の自己記述型エージェントがプロモートされたハブに接続した時点で、自己記述型エージェントの製品インストールが実行されます。
- スタンバイ・ハブでは自己記述型エージェントのインストールを即時に強制再試行できます。このためには、プライマリー・ハブでの自己記述型エージェントのインストールを繰り返します。スタンバイ・モニター・サーバーでエラー・アプリケーション・インストール・レコードを削除した後で **deleteappinstallrecs -a** コマンドを使用し、プライマリー・モニター・サーバーからエラー以外の状態レコードを削除します。このコマンドは、プライマリー・モニター・サーバーで自己記述型エージェントのインストールを繰り返します。このインストールが正常に完了すると、スタンバイ・モニター・サーバーでのインストールが実行されます。

自己記述型機能によるインストールのオプションの動的更新

ハブ・モニター・サーバーの稼働中に、自動自己記述型エージェント・プロセスによってモニター・サーバーとポータル・サーバーにインストールできる自己記述対応の製品とバージョンを指定できます。

このタスクについて

ハブ・モニター・サーバーが開始している必要があります。以下の構成コマンドは、自己記述型機能が有効または無効のいずれであっても (KMS_SDA=Y|N) 実行できます。指定した構成設定が保存され、変数 KMS_SDA=Y によって自己記述型機能が有効になると、この構成設定が実装されます。詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の 『Dynamically controlling the hub monitoring server self-describing agent capability』 を参照してください。

手順

1. **tacmd suspendSda** コマンドを使用して、(ハブ・モニター・サーバーをリサイクルせずに) 自己記述型機能を中断します。 このコマンドを使用すると、オプションの更新中は自己記述型機能によるインストールが実行されません。
2. 以下のいずれかのコマンドを実行します。

   tacmd addSdaInstallOptions
   自己記述型エージェント機能によってインストールできる製品とバージョンを指定します。

   tacmd editSdaInstallOptions
   既存の製品バージョン構成またはデフォルトの自己記述型エージェント・インストール動作を変更します。

   tacmd deleteSdaInstallOptions
   製品の特定のバージョンの構成またはすべてのバージョンを削除します。

tacmd listSdaInstallOptions
ハブ・モニター・サーバーの既存の自己記述型エージェント・インストール構成を表示します。

構文と例については、*IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

3. **tacmd resumeSda** コマンドを使用して、(ハブ・モニター・サーバーをリサイクルせずに) 自己記述型機能を再開します。

タスクの結果

変数 KMS_SDA=Y を設定して自己記述型機能を有効にすると、指定したバージョンの新しい製品のみのインストールが行われます。

自己記述型機能の中断

モニター・サーバーをリサイクルせずにご使用の環境の自己記述型機能を中断および再開するには、**tacmd suspendSda** コマンドと **tacmd resumeSda** コマンドを使用します。自己記述型機能インストール・オプションを変更する場合や保守モードに切り替える場合など、さまざまな理由から自己記述型機能を中断することがあります。

始める前に

tacmd suspendSda コマンドと **tacmd resumeSda** コマンドによって自己記述型機能の動作が動的に変更されるのは、KMS_SDA=Y を使用してハブ・モニター・サーバーが構成されている場合のみです。 **tacmd suspendSda** コマンドと **tacmd resumeSda** コマンドを実行しても、KMS_SDA=N 設定は指定変更されません。 KMS_SDA=N が設定された状態で **tacmd resumeSda** コマンドを実行すると、KMS_SDA=Y が設定されるまでは、このコマンドは無視されます。

tacmd suspendSda コマンドまたは **tacmd resumeSda** コマンドを実行すると、TAPPLPROPS 表が更新されます。この設定は、KMS_SDA の設定に関係なく保存されます。ベスト・プラクティスは、ハブ・モニター・サーバーの環境変数を KMS_SDA=Y に設定してから、**tacmd suspendSda** コマンドまたは **tacmd resumeSda** コマンドを実行することです。

詳しい構文については、*IBM Tivoli Monitoring* コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

手順

- 自己記述型機能を中断するには、**tacmd suspendSda** コマンドを実行します。
- 自己記述型機能を再開するには、**tacmd resumeSda** コマンドを実行します。

次のタスク

tacmd listSdaStatus を実行して、モニター・サーバーの中断状態を表示できます。 326 ページの『自己記述型エージェントのインストール』を参照してください。

自己記述型の自動最新表示およびシード

自己記述機能を使用すると、モニター・インフラストラクチャーを自動的に最新表示にし、最新バージョンのアプリケーション・サポートでシードすることが可能になります。

*自動最新表示*は、モニター・インフラストラクチャーの継続的な、連続した更新を可能にするものです。自動最新表示が正常に実行されると、*シード*によってご使用の環境が最新の製品定義で更新されます。

自動最新表示

各製品で、アプリケーション・サポートが提供されます。 IBM Tivoli Monitoring V6.2.3 以降より前のバージョンでは、アプリケーション・サポートがモニター・サーバー、ポータル・サーバー、およびポータル・クライアントにインストールされており、新しいアプリケーション・サポートをアクティブにするために各コンポーネントのリサイクルが必要でした。 IBM Tivoli Monitoring V6.2.3 の場合、自動最新表示によってモニター・サーバーおよびポータル・サーバーで、自己記述型エージェントのインストール・イベント後に、動的なアプリケーションの最新表示が実現されます。

新しい自己記述型エージェントが IBM Tivoli Monitoring インフラストラクチャー経由でアプリケーションのインストールを開始すると、作を中断することなく自動最新表示処理が発生します。自己記述型エージェントからモニター・サーバーへの初めての接続で、アプリケーション・サポートがまだリモート・モニター・サーバーまたはハブ・モニター・サーバーに存在しないときに、この処理がトリガーされます。

アプリケーション・サポートは、最初にハブ・モニター・サーバーに、次にエージェントが現在接続されているリモート・モニター・サーバー (エージェントからサポートを取得する) に、その後ポータル・サーバー (ハブ・モニター・サーバーからサポートを取得する) に自動的にインストールされます。エージェントが、サポートが欠落している別のリモート・モニター・サーバーに切り替わると、新しいホストのリモート・モニター・サーバーでサポートが動的に更新されます。

自動最新表示は、メタデータのデプロイメントに続いてすぐにモニター・サーバーで行われます。メタデータのデプロイメントでは、属性ファイル、カタログ・ファイル、EIF マッピング・ファイル、すぐに使用可能な製品定義ファイル (シード・ファイル)、およびバージョン・ファイルが転送され、モニター・サーバーに格納されます。ファイルが正常にデプロイされると、モニター・サーバーの内部キャッシュが更新され、新しいメタデータがすぐにモニター・サーバーコンポーネントでモニター用に使用可能になります。自動最新表示は、ポータル・サーバーでも行われ、必要なすべてのファイルが更新されます。

まだ ポータル・サーバーが稼働している間にポータル・サーバー・データベースが再起動された場合は、サポートがポータル・サーバーの更新を完了するように、ポータル・サーバーを再起動する必要があります。ポータル・サーバーで自動最新表示が正常に作動するためには、ポータル・サーバーデータベースが稼働している必要があります。

自動最新表示によって、自己記述型エージェントの最新表示中のアクティビティーのモニターをサポートするために、製品のメタデータへの継続的なアクセスが保証されます。その際は、既存のメタデータが使用され、メタデータの自動最新表示が完了すると、新しいメタデータが利用可能になります。一部の内部モニター・サーバー・コンポーネントは、新しいメタデータが存在する場合 (例えば、pending wait シチュエーションを started に移行する場合) に通知を提供します。

シード

製品のアプリケーション・サポートには、すぐに実行可能なモニター定義 (定義の実行条件を含む) が付属しています。配布データまたは「条件」の適用は、通常、*配布*と呼ばれます。製品のモニターおよび配布の定義をモニター・サーバーに格納することを、*シード*するといいます。シードは、自己記述型エージェントの製品インストールの一部として自動的に行われ、デフォルトのモニター定義が有効になります。この動作は CLI から変更または無効にできますが、製品提供のモニター定義すべてが不要な場合にのみ行う必要があります。詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Configuring self-describing agent seeding』、および*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)の『tacmd editSdaOptions』を参照してください。

tacmd listappinstallrecs -d コマンドは、モニター・サーバーのアプリケーション・プロパティー・テーブルから、SEEDSTATE 列の値など、アプリケーション・サポートのインストール・レコードを戻します。詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。SEEDSTATE 列の次の値は、自己記述型エージェントでインストールされた製品のシード状態を反映しています。

<blank> これはデフォルト値です。この値は、シードがまだ実行されていないか、この製品に適用されないことを示します。 SEEDSTATE 状態は、TMS の ID を持つ自己記述型エージェントのレコードにのみ適用されます。

I 製品のシードが進行中です。

Y 製品はシードされました。

N 製品はシードされていません (SQL ファイルが見つかりません)。

E シード・エラー。

モニター・サーバーの起動時に、インストールされた製品での変更または自己記述型エージェントのインストール・エラーが検出されると、TEMS MSG2 ログおよび監査ログ機能にメッセージが生成されます。モニター・サーバーのアプリケーション・サポートのインストール・レコードは、MSG2 メッセージまたは監査ログに示されている変更を反映するために、必要に応じて更新されます。TEMS RAS1 ログには、アプリケーション・サポートの変更の成功または失敗を示すトレース・メッセージが含まれています。 MSG2 メッセージおよび監査ログのメッセージを「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」で確認し、次のアクションを完了します。

- インストールされた製品で検出された変更が予想されていたかどうかを確認します。その変更が予想外または適切でない場合、必要なアクションを実行して、自己記述型エージェント・インストールまたは手動インストールにより、適切な製品バージョンをインストールしてください。

- 自己記述型エージェントがインストールされた製品でエラーが指摘された場合は、必要に応じてアプリケーション・サポートのインストール・レコードをクリーンアップしてください。これは、**tacmd deleteappinstallrecs** コマンドを使用して失敗したインストールのレコードを削除することで実行できます。必要であれば、自己記述型エージェントのインストールを再び開始してください。これらのタスクの実行に使用できるコマンドについては、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

注: 自己記述型エージェント機能では、エージェント言語パックのインストールは自動化されません。自己記述型エージェントの言語パックのインストール手順は、標準のエージェントの手順と同じです。詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の 『言語パックのインストール』 を参照してください。

モニター・サーバーでの自己記述型機能の有効化または無効化

Tivoli Enterprise Monitoring Server で環境構成変数を使用して、特定のモニター・サーバーの自己記述型エージェント機能を有効または無効にできます。

特定のモニター・サーバーで自己記述型エージェント・アプリケーション・メタデータの自動更新および伝搬が必要ないときには、自己記述型機能を随時無効化してください。その場合、エージェントのアプリケーション・サポートを各モニター・サーバーとポータル・サーバーで手動でインストールおよびアクティブ化する必要があります。デフォルトでは、自己記述型機能はリモート・モニター・サーバーでは有効、ハブ・モニター・サーバーでは無効になっています。

このタスクについて

ベスト・プラクティスは、ハブ・モニター・サーバーで自己記述型エージェント機能を制御することです。これは、ハブ・モニター・サーバーにおける有効化または無効化が、このサーバーに接続するすべてのリモート・モニター・サーバーとエージェントに影響するためです。

特定のリモート・モニター・サーバーで自己記述型機能を有効または無効にした場合、影響を受けるのは、そのサーバーに接続するすべてのエージェントのみです。

1 つのモニター・サーバーの自己記述型機能を一時的に停止するため、ターゲット・モニター・サーバー環境変数を編集するには、以下のステップを実行します。

手順

- Windows
  1. モニター・サーバーがインストールされているコンピューターの「Tivoli Enterprise Monitoring Services の管理」アプリケーションで **Tivoli Enterprise Monitoring Server** を右クリックし、「**拡張**」→ 「**ENV ファイルの編集**」を選択します。
  2. 既存の環境変数を編集します (KMS_SDA=Y | N)。
- Linux UNIX
  1. モニター・サーバーがインストールされているコンピューターで、*<install_dir* >/config/ ディレクトリーに移動します。

2. *<tems_hostname>*_ms_*<tems_name>*.config ファイルを開きます。
3. 既存の環境変数を編集します (KMS_SDA=Y | N)。

- z/OS 「*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: 共通計画および構成ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)」の KMS_SDA に関する記述を参照してください。

次のタスク

モニター・サーバーを再始動します。

エージェント・サポートのバージョンは、次の方法で確認することができます。

- エージェントおよびモニター・サーバーのオペレーション・ログを確認して、エージェントが標準モードで作動しているか、自己記述エージェント・モードで作動しているかを判断します。管理対象システム状況ワークスペースには、各モニター・エージェントのオペレーション・ログへのリンクがあります。
- **tacmd listappinstallrecs** コマンドはアプリケーション・サポートのインストール・レコードを返し、**tacmd listSdaStatus** コマンドは環境内にあるすべてのモニター・サーバーの自己記述型エージェントにおける現在の稼働状況を表示します。モニター・サーバーが稼働していないときは、このコマンドを使用できないことに注意してください。 326 ページの『自己記述型エージェントのインストール』を参照してください。

エージェントでの自己記述型機能の有効化または無効化

自己記述エージェント機能は、モニター・エージェントの環境構成変数を使用して有効または無効にできます。

1 つ以上の個々のエージェントで、自己記述エージェント・アプリケーションのメタデータの自動更新および伝搬が必要ないときには、随時自己記述型機能を無効化してください。その場合、エージェントのアプリケーション・サポートをモニター・サーバーとポータル・サーバーで手動でインストールおよびアクティブ化する必要があります。デフォルトではエージェントの自己記述型機能は有効になっています。

始める前に

ベスト・プラクティスは、ハブ・モニター・サーバーで自己記述型エージェント機能を制御することです。詳しくは、 335 ページの『モニター・サーバーでの自己記述型機能の有効化または無効化』を参照してください。

手順

- Windows
  1. モニター・エージェントがインストールされているコンピューターの「Tivoli Enterprise Monitoring Services の管理」アプリケーションでエージェントを右クリックし、「**拡張**」→ 「**ENV ファイルの編集**」を選択します。
  2. 既存の環境変数を編集します (TEMA_SDA=Y | N)。
- Linux UNIX

1. モニター・エージェントがインストールされているコンピューターで、<*install_dir* >/config/ ディレクトリーに移動します。
2. 調整ファイルを開きます。
   単一インスタンス・エージェントの場合: <*pc*>.ini
   マルチインスタンス・エージェントの場合: <*pc*>_<*instance*>.ini ファイル
   ここで、*pc* は 2 文字の製品コードです。
3. 既存の環境変数を編集します (TEMA_SDA=Y | N)。

- IBM i
  1. /qautotmp/kmsparm.kbbenv を開きます。
  2. 既存の環境変数を編集します (TEMA_SDA=Y | N)。
- z/OS 「*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS: 共通計画および構成ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)」の TEMA_SDA に関する記述を参照してください。

次のタスク

モニター・サーバーを再始動します。

エージェント・サポートのバージョンは、次の方法で確認することができます。

- エージェントおよびモニター・サーバーのオペレーション・ログを確認して、エージェントが標準モードで作動しているか、自己記述エージェント・モードで作動しているかを判断します。管理対象システム状況ワークスペースには、各モニター・エージェントのオペレーション・ログへのリンクがあります。
- **tacmd listappinstallrecs** コマンドはアプリケーション・サポートのインストール・レコードを返し、**tacmd listSdaStatus** コマンドは環境内にあるすべてのモニター・サーバーの自己記述型エージェントにおける現在の稼働状況を表示します。モニター・サーバーが稼働していないときは、このコマンドを使用できないことに注意してください。 326 ページの『自己記述型エージェントのインストール』を参照してください。

エージェントで自己記述が有効になっているかどうかの判断

インストール前あるいはインストール後に、エージェントで自己記述が有効になっているかどうかを判断することができます。

始める前に

IBM Tivoli Monitoring V6.2.3 以降の基本オペレーティング・システムのエージェントでは自己記述が有効ですが、すべてのエージェントで自己記述が有効なわけではありません。

Tivoli Performance Analyzer および Universal Agent では自己記述が無効です。自己記述が有効なエージェントの詳細なリストについては、IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home)のIBM Tivoli Monitoring agents enabled for self-description (SDA)のトピックを参照してください。

このタスクについて

どのエージェントで自己記述が有効かを判断するには、次のステップを実行します。

手順

- インストール前に判断するには

  K<*PC*>MSMAN.txt 自己記述型マニフェスト・ファイルのインストール・イメージを探してください。

  – Windows このファイルは WINDOWS ディレクトリーにあります。 Windows Itanium 上で実行されているエージェントの場合は、このファイルは WIA64 ディレクトリーにあります。

  – Linux UNIX このファイルは unix ディレクトリーにあります。

  – Agent Builder を使用して作成されたエージェントの場合は、このファイルは K<*PC*>/support ディレクトリーにあります。

- インストール後に判断するには

  – Windows **kincinfo -e** コマンドを実行します。SDA STATUS 列を参照して、エージェントで自己記述が有効かどうかを確認します。

    次の例では、Universal Agent の SDA STATUS 列に Disabled と記載されていますが、これはこのエージェントで自己記述が有効ではない ことを意味します。

```
kincinfo -e
*************** Thursday, July 14, 2011 1:29:36 PM ***************
User: Administrator                         Group: NA
Host Name: ICVW3A03                         Installer: Ver: 062300000
CandleHome : C:¥IBM¥d1191a¥ITM
Installitm : C:¥IBM¥d1191a¥ITM¥InstallITM
********************************************************************
...Application support propagation
PC     PRODUCT DESC                         PLAT       VER            BUILD          SDA STATUS
NT     Monitoring Agent for Windows         WINNT      06.23.00.00    11871          Enabled
       OS
R2     Agentless Monitoring for Windows     WINNT      06.23.00.00    201107051647   Enabled
       Operating Sy
R3     Agentless Monitoring for AIX         WINNT      06.23.00.00    201107051650   Enabled
       Operating System
R4     Agentless Monitoring for Linux       WINNT      06.23.00.00    201107051653   Enabled
       Operating Syst
R5     Agentless Monitoring for HP-UX       WINNT      06.23.00.00    201107051655   Enabled
       Operating Syst
R6     Agentless Monitoring for Solaris     WINNT      06.23.00.00    201107051658   Enabled
       Operating Sy
UM     Universal Agent                      WINNT      06.23.00.00    d1184a         Disabled
```

– Linux UNIX **<*install_dir*>/bin/cinfo -e** コマンドを実行します。SDA STATUS 列を参照して、エージェントで自己記述が有効かどうかを確認します。

次の例では、Tivoli Performance Analyzer と Universal Agent の SDA STATUS 列に Disabled と記載されていますが、これはこれらのエージェントで自己記述が有効ではない ことを意味します。

```
<inst_dir>/bin/cinfo -e
*********** Thu Jul 14 13:19:41 EDT 2011 ******************
User: root                                  Groups: root bin daemon sys adm disk wheel
Host name : icvr5d06                        Installer Lvl:06.23.00.00
CandleHome: /data/tmv623-d1191a-201107110121/ITM
Version Format: VV.RM.FF.II (V: Version; R: Release; M: Modification; F: Fix; I: Interim Fix)
************************************************************************
...Application support propagation
PC     PRODUCT DESC                          PLAT       VER             BUILD          SDA STATUS
80     Monitoring Agent for Self Describing  lx8266     03.00.00.00     201106281135   Enabled
       Agent
hd     Warehouse Proxy                       lx8266     06.23.00.00     d1191a         Enabled
lz     Monitoring Agent for Linux OS         lx8266     06.23.00.00     11871          Enabled

pa     Tivoli Performance Analyzer           lx8266     06.23.00.00     11891          Disabled
r2     Agentless Monitoring for Windows      lx8266     06.23.00.00     201107051647   Enabled
       Operating Systems
r3     Agentless Monitoring for AIX          lx8266     06.23.00.00     201107051650   Enabled
       Operating Systems
r4     Agentless Monitoring for Linux        lx8266     06.23.00.00     201107051653   Enabled
       Operating Systems
r5     Agentless Monitoring for HP-UX        lx8266     06.23.00.00     201107051655   Enabled
       Operating Systems
r6     Agentless Monitoring for Solaris      lx8266     06.23.00.00     201107051658   Enabled
       Operating Systems
sy     Summarization and Pruning Agent       lx8266     06.23.00.00     d1177a         Enabled
ul     Monitoring Agent for UNIX Logs        lx8266     06.23.00.00     11751          Enabled
um     Universal Agent                       lx8266     06.23.00.00     d1184a         Disabled
```

自己記述型機能を制御する環境変数

環境変数によって、モニター・サーバー、ポータル・サーバー、またはエージェントで自己記述型機能がオンまたはオフにされます。

目的

環境変数によって、自己記述型機能の主要機能が制御されます。また、通常のユーザーが変更するパラメーターは、これらの環境変数のみです。自己記述型の他のすべての環境変数は、IBM サポート担当者の指示があったときのみ変更します。

重要: このトピックでは、自己記述型の主要な環境変数についてのみ説明します。自己記述型機能の環境変数の詳細なリストについては*IBM Tivoli Monitoring インストールおよび設定ガイド*の『環境変数』を参照してください。

パラメーター

YES または NO を指定するのではなく、常に Y または N を指定してください。

モニター・サーバーのパラメーター

KMS_SDA=Y | N
N を指定するとモニター・サーバーで自己記述型エージェント機能が無効になり、Y を指定すると有効になります。ハブ・モニター・サーバーで自己記述を無効にするとすべての 自己記述型機能が無効になります。

ハブ・モニター・サーバーの場合、デフォルト値は N です。

リモート・モニター・サーバーの場合、デフォルト値は Y です。

TEMS_MANIFEST_PATH=*file_loc*
モニター・サーバーで自己記述型エージェントから収集したマニフェスト・ファイルおよび JAR ファイルを保管するロケーション。お客様は指定のカスタム・ディレクトリーまたは代替ディレクトリーを作成して適切な許可を設定する必要があります。ディレクトリーは、モニター・サーバーによって作成されません。自己記述型機能を有効にするには、このパラメーターを設定する必要があります。通常は、コンポーネントのインストール時に設定します。

TEMS_JAVA_BINPATH
この変数によって、z/OS USS 環境内の Java インストール・パスが特定されます。これは、z/OS エンジンで USS のシェル・インターフェースが生成されるたびに、ローカルの構成ファイルによって動的に置き換えることができます。詳しくは、 *Tivoli Enterprise Monitoring Server on z/OS の構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/ztemsconfig/ztemsconfig.htm)を参照してください。

ポータル・サーバーのパラメーター

TEPS_SDA=Y | N
N を指定するとポータル・サーバーで自己記述型エージェント機能が無効になり、Y を指定すると有効になります。

デフォルト値は Y です。

TEPS_MANIFEST_PATH=*file_loc*
デフォルトでは、ポータル・サーバーが取得した製品サポートの JAR ファイルを書き込んで保管するロケーションに設定されます。通常、このパラメーターは、コンポーネントのインストール時に設定します。

エージェント・パラメーター

TEMA_SDA=Y | N
N を指定するとエージェントで自己記述型エージェント機能が無効になり、Y を指定すると有効になります。値が N の場合は、モニター・サーバーによってこのエージェントから製品サポート・ファイルが取得されなくなり、他の製品の

モニター・サーバーで自己記述型エージェント機能を停止することなく、エージェントごとの制御を行うことができます。

デフォルト値は Y です。

第 14 章 エージェント管理サービス

エージェント管理サービスを使用して、エージェントの可用性をモニターし、エージェントが正常でなくなったり、予期せず終了したりする場合は (再始動などにより) 自動的に応答します。これらのサービスを使用すると、エージェントの可用性格付けを向上させることができます。

Tivoli Agent Management Services の機能

エージェント管理サービスは、すべてのエージェントに共通の属性 (ファイル・システム・インストール・ロケーション、ファイル・システム・ログ・ファイル・ロケーション、実行可能ファイル名など) およびオペレーティング・システムに共通の API (実行中プロセスのリストの列挙など) にのみ依存します。この情報を使用して、エージェント管理サービスは、エージェントの可用性を向上し、エージェントの可用性を表示および制御するための簡単で統合されたインターフェースを提供します。

エージェントに変更を加えずに、エージェントをエージェント管理サービスの管理下に置くことができます。システムにエージェントを追加する場合、これらのエージェントは、簡単にエージェント管理サービスの管理下に置くことができます。

エージェント管理サービスは、次の機能を提供する Tivoli Monitoring・エージェントへの戦略的アプローチとなるものです。

- 他のエージェントの可用性をモニターし、ユーザー・ポリシーに従って、異常な状態に対して自動的に応答する機能。
- ポリシー設定による自動化メソッドと、エージェントの起動、停止、および*管理対象* と*非管理対象* の切り替えを手動で行う Tivoli Enterprise Portal アクション実行コマンドによる手動メソッド。
- エージェント管理サービスによって収集されている情報のビューを持つエージェント管理ワークスペース。エージェント管理ワークスペースは、配布されている基本的かつほとんどの Tivoli Enterprise Monitoring Agent 用に提供されています。

コンポーネント関係

エージェント管理サービスでは、3 つのインターフェースを使用して OS エージェント・プロセス内の他のコンポーネントと通信します。

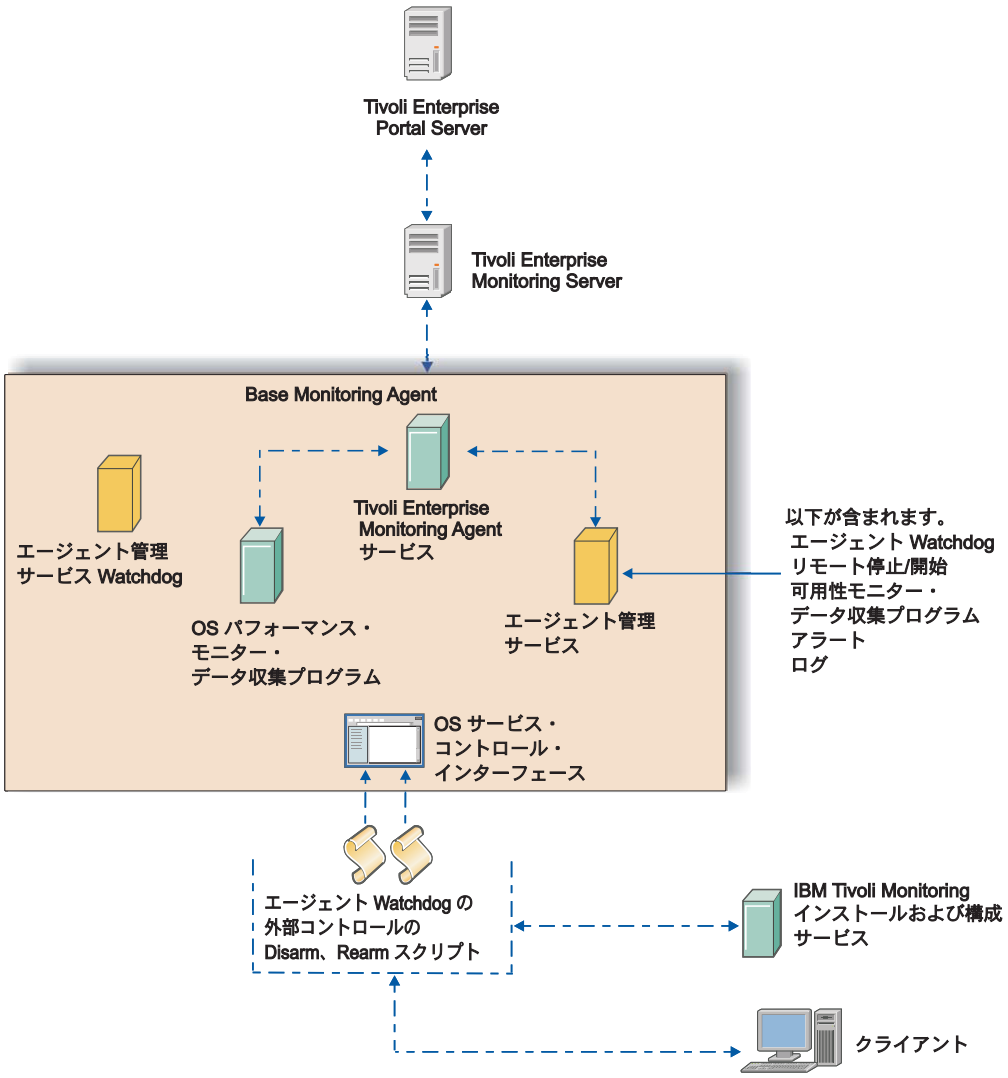


図 30. エージェント管理サービス・コンポーネントと IBM Tivoli Monitoring コンポーネントの対話

コンポーネントの説明

Agent Management Services には 2 つのコンポーネントがあります。エージェント Watchdog および エージェント管理サービス Watchdog です。

エージェント Watchdog

エージェント Watchdog は、エージェントの*共通エージェント・パッケージ* (CAP) ・ファイルのポリシーに基づいて、エージェントに対する特定の可用性モニター・アクションを実行します。このコンポーネントは、論理コンポーネントとして OS エージェント・プロセス内で実行されます。OS エージェントのインストール済み環境の CAP ディレクトリーに XML ファイルがあるモニター・エージェントは、OS エージェント自体ではなく、エージェント Watchdog によって監視されます。

エージェント管理サービス Watchdog

Watchdog は何によって監視されるのでしょうか。それは、エージェント管理サービス *Watchdog* (プロキシー・エージェント・サービス *Watchdog* とも呼ばれる) のジョブです。この Watchdog の状況は、Tivoli Enterprise

Portal の「**エージェントのランタイム状況**」ビューで確認できます。これは OS エージェント内の Watchdog と同様のモニター機能を備えていますが、OS エージェントを監視するためにのみ使用されます。OS エージェント内のエージェント Watchdog には、Tivoli Enterprise Portal Desktop の照会に対応してその他のエージェントをモニターし、OS エージェントの通信機能を使用してアクション実行を処理する追加機能があります。エージェント管理サービス Watchdog は、OS エージェントでスタンドアロン実行可能ファイルとして含められ、Linux および UNIX 系オペレーティング・システムではプロセス **kcawd** として、Windows ではプロセス **kcawd.exe** として実行されます。

Tivoli Enterprise Portal ユーザー・インターフェース

Tivoli Enterprise Portal は エージェント管理サービス サービスのユーザー・インターフェースであり、エージェント管理サービス によるエージェントの管理を手動で開始または停止し、エージェント管理サービス で管理されているエージェントを開始または停止するための事前定義アクション実行コマンドが組み込まれています。以下のアクション実行コマンドは、エージェント管理サービス ワークスペースのポップアップ・メニューから実行でき、リフレックス・オートメーションのシチュエーションで参照できます。

注: 引き続き、Tivoli Enterprise Monitoring Services の管理 や Tivoli Enterprise Portal ナビゲーターのポップアップ・メニューなど、使い慣れた方法を使用してエージェントを開始または停止することもできます。

Tivoli Agent Management Services のインストールおよび構成

エージェント管理サービスは、ホスト・プラットフォームに応じて、自動的に Linux OS エージェント、UNIX OS エージェント、または Windows OS エージェントとともにインストールされます。これらのエージェントのアプリケーション・サポート・プロファイルもTivoli Enterprise Monitoring Server および Tivoli Enterprise Portal Server にインストールされます。

IBM Tivoli Monitoring V6.2.3 フィックスパック 1 以降では、プロセス状況および `cinfo` の検査のほかに、ソケットを介して OS エージェントがモニターされます。モニターされるソケットは、外部要求のためにプロキシー・エージェント・サービスによって内部で使用されるパイプです。`KCA_MAX_RETRIES_ON_PIPE` 環境変数で指定されている回数だけ連続で試行しても OS エージェントがソケットに応答しない場合は、OS エージェントを再始動できます。エージェントの ENV ファイルでこの変数が変更された場合は、変更を反映するためにエージェントを再始動する必要があります。デフォルトでは、この変数は定義されていません。つまり、OS エージェントは再始動されることはありません。この変数には 5 よりも大きい値を使用する必要があります。

共通エージェント・パッケージ・ファイル

エージェント管理サービスの特定のエージェントに対するモニター動作は、*共通*エージェント・パッケージ (CAP) ファイルと呼ばれる XML ベースのポリシー・ファイル内の設定によって管理されます。エージェント管理サービスで管理可能なすべてのエージェントでは、k*pc*_default.xml (*pc* は製品コード) という名前の CAP

ファイルが、関連プラットフォームの OS モニター・エージェント構成ファイル内の **KCA_CAP_DIR** 環境変数で定義されているディレクトリーにインストールされます。64 ビットの Windows でネイティブに実行されるエージェントは、64 ビットの Tivoli Monitoring Agent ディレクトリーに CAP ファイルをプットします。その他のエージェントでは、32 ビットのディレクトリーにプットされます。

Windows *install_dir* ¥TMAITM6[_x64]¥CAP

Linux UNIX *install_dir* /config/CAP。

zLinux プラットフォームでの エージェント管理サービス の動作は次のとおりです。

- V6.2.3 フィックスパック 1 (新規インストール): デフォルトで有効
- V6.2.3 フィックスパック 1 (アップグレード): アップグレード前に検出された状態に基づき、有効または無効。
- V6.2.2 フィックスパック 2 以降: インストール時に無効、およびアップグレード時に無効 (アップグレード前にアクティブだったかどうかにかかわらず)。

アップグレード後に エージェント管理サービス を有効にするには、KCA_CAP_DIR 環境変数に、CAP ファイルが格納されている既存のディレクトリーを設定します。

Intel Linux およびサポートされているその他のプラットフォームでは、エージェント管理サービスはデフォルトで有効になっています。

CAP ファイルのカスタマイズ可能要素

エージェントによってインストールされる CAP ファイルは、読み取り専用として構成されるため、直接変更することはできません。このファイルのポリシー設定をカスタマイズする場合は、ファイルのコピーを作成し、*kpc*.xml という規則で名前を付けます。Watchdog は、新しい CAP ファイルが追加されるか、またはディレクトリーから CAP ファイルが削除されることを自動的に検出します。既存の CAP ファイルを変更した場合、その変更を反映するため、OS エージェントを再始動する必要があります。非 OS エージェント CAP ファイルを更新する場合は、OS エージェントを再始動する必要はありません。このアクションを完了するには、ディレクトリーから CAP ファイルを削除し、ファイルが削除されていることが Watchdog により検出されたら、更新後のファイルをディレクトリーにコピーします。OS エージェント CAP ファイルを更新した場合は OS エージェントを再始動する必要があります。

1 つの CAP ファイルで複数インスタンスのモニター・エージェントを管理することも、インスタンスごとに個別の CAP ファイルを作成することもできます。

CAP ファイルで定義されている要素は、「エージェント管理サービス」ワークスペースの Tivoli Enterprise Portal「エージェントの管理定義」ビューで確認できます。**注:** CAP ファイルに定義されていない属性は「エージェントの管理定義」ビューには表示されません。

要素の順序は重要です。kwgcap.xsd で、CAP ファイル・スキーマの式定義を確認します。

<checkFrequency>
管理対象エージェントのエージェント管理サービスによる可用性チェックの

間隔です。システム負荷が大きい場合は、KCA_CMD_TIMEOUT エージェント環境変数の設定とともに、checkFrequency の間隔を大きくすることを検討してください。

5 の倍数の秒数、最大 3600 秒 (1 時間) までで頻度の値を入力します。デフォルト: **120**。

<cpuThreshold>
異常と見なされてエージェント管理サービスによって再始動されるまでに、ある時間間隔にわたってエージェント・プロセスが消費できる CPU 時間の最大平均パーセントです。この時間間隔は、『checkFrequency』 の秒数と同じです。

しきい値のパーセンテージを 1 から 100 の正の整数で入力します。

<memoryThreshold>
異常と見なされてエージェント管理サービスによって再始動されるまでに、ある時間間隔にわたってエージェント・プロセスが消費できる実効ページ・セット・メモリーの最大平均量です。この時間間隔は、『checkFrequency』 の秒数と同じです。

しきい値と測定単位 (KB、MB、または GB) を入力します。例: 50 MB。

<managerType>
エージェントの可用性モニターを実行するエンティティー。

列挙値 (NotManaged または ProxyAgentServices) を入力します。デフォルト: **NotManaged**。

<maxRestarts>
異常停止したエージェントまたは正常ではないエージェントの 1 日当たりの再始動回数。実行し続ける必要がないエージェントには、値 0 を指定できます。

正の整数を入力します。デフォルト: **4**。

<subagent id>
特定のエージェント用にインスタンス固有の CAP ファイルを作成している場合のみ、この値を編集します。例えば、kud_default.xml ファイルにサブエージェント id="kudagent" がある DB2 エージェント・インスタンス用に CAP ファイルを作成する場合は、<subagent id="kud_instance"> などに設定します。エージェントの元の CAP ファイルとそのインスタンス固有の CAP ファイルの <agentName> 値は一致する必要があります。

ID のストリング値を入力します。

<instance>
この要素を使用して、ターゲットの CAP ファイル・ポリシーを適用する特定のインスタンス名を指定します。CAP ファイルの <agentName> 要素の後に指定します。例えば、CAP ファイルのインスタンスが Tivoli Monitoring DB2 エージェントの 2 つの特定インスタンス test1 および test2 に適用されるように指定するには、次の情報を入力します。

```
<subagent id="kud_instance">
<agentName>ITCAM Agent for DB2</agentName>
<instance>
   <name>test1</name>
   <name>test2</name>
</instance>
```

インスタンス名のストリング値を <name> と </name> タグで囲んで入力します。

Linux および UNIX でのデータベースおよびメッセージング・モニター・エージェント

データベースおよびメッセージング・エージェントは、通常、root 以外のユーザーとして開始されます。エージェント管理サービスでこの動作をサポートするには、CAP ファイルの開始スクリプトで、エージェントが特定ユーザーとして開始することを指定できます。

エージェント管理サービスは、自動スクリプト・ファイルと同じファイル **kcirunas.cfg** を使用して、エージェントが *RunAs* を実行するユーザーに関する構成情報を取得します。 この情報は、エージェントが正しいユーザーで実行されるようにエージェント管理サービスがエージェントを開始するときに使用します。エージェントがリモートでデプロイされている環境では、***hostname*_kdyrunas.cfg** ファイルを使用します。ファイルの *RunAs* 情報も確認されます。

古い CAP ファイルでこのサポートを有効にするには、次に示す Linux (lz) での Universal Agent (um) の例に従って CAP ファイルを更新します。

```
<startScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um START ##INSTANCE##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<startScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um START ##INSTANCE## ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>
```

古い CAP ファイルでこのサポートを有効にするには、停止スクリプトを更新します。

```
<stopScript>
  <command>$CANDLEHOME/$ITM_BINARCH/lz/bin/agentInstanceCommand.sh
  um STOP ##INSTANCE## ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

Linux の単一インスタンス・エージェントの場合は、次の構文を使用します。

```
<startScript>
  <command>su -c "$CANDLEHOME/bin/itmcmd agent start ul" -
  ##USER##</command>
  <returnCodeList>
```

```
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<stopScript>
  <command>su -c "$CANDLEHOME/bin/itmcmd agent stop ul" -
  ##USER##</command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

UNIX ログ・エージェントなどの単一インスタンス・エージェントの場合は、次の構文を使用します。- ##USER## が末尾ではなく su の後にあることを除いて、Linux の構文と同じです。

```
<startScript>
  <command>su - ##USER## -c "$CANDLEHOME/bin/itmcmd agent start ul"
  </command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</startScript>

<stopScript>
  <command>su - ##USER## -c "$CANDLEHOME/bin/itmcmd agent stop ul"
 </command>
  <returnCodeList>
    <returnCode type="OK">0</returnCode>
  </returnCodeList>
</stopScript>
```

V6.2.1 から V6.2.2 以降への Universal Agent の CAP ファイルのアップグレード

IBM Tivoli Monitoring V6.2.2 以降では、 <agentType> が V6.2.2 以降では必須の **ITM_Windows** または **ITM_UNIX** でなく **WinService** に設定されている場合、複数のエージェント・インスタンスはサポートされません。

- <agentType> に **ITM_Windows** または **ITM_UNIX** を設定すると、標準の Tivoli Monitoring kincinfo/cinfo インストール・ユーティリティーを使用して、モニター・エージェント・インスタンスが検出されます。
- 複数インスタンスのモニター・エージェントとして <agentType> に **WinService** を設定すると、Tivoli Monitoring インスタンス名は表示されなくなります。エージェント・タイプは、**ITM_UNIX** または **ITM_Windows** である必要があります。

V6.2.1 から V6.2.2 以降になった際にアップグレードされた CAP ファイル

V6.2.1 では、Linux OS エージェントは出荷時に $CANDLEHOME/$INTERP_BIN/lz/bin/CAP ディレクトリーに 5 つのデフォルト CAP ファイルを持っていました。V6.2.2 以降では場所が $CANDLEHOME/config/CAP に変更され、CAP ファイルは各エージェントに同梱されています。Linux OS エージェントが V6.2.1 から新しいリリースにアップグレードされると、$CANDLEHOME/config/CAP ディレクトリーにある CAP ファイルを使用するようになります。CAP ファイルのカスタマイズはすべて、$CANDLEHOME/config/CAP ディレクトリー内のファイルに基づいて行う必要があります。V6.2.1 の CAP ファイルが必要な場合、これらのファイルはシステムの元のディレクトリーに置かれています。

関連資料:

Linux または UNIX でのインストールの注意点: 自動開始スクリプト
エージェント RunAs の構成は kcirunas.cfg にあります。

エージェントの可用性のモニター

エージェント管理サービスは、停止または再構成されたエージェントに対応して、そのエージェントを再始動します。エージェント管理サービスは、エージェントのタイプ、または、CAP ファイルの <availabilityStatusScript> 要素に指定したコマンド、あるいはその両方に基づいてそのエージェントが停止しているかどうかを判断します。

タイプがコンソールのエージェントの場合、エージェント管理サービスはエージェントが停止しているかどうかを判断するために、CAP ファイルの <agentPath> 要素の値を使用して、オペレーティング・システムに実行しているアプリケーションを問い合わせます。

タイプが *WinService* のエージェントの場合は、Windows のサービス・コントロール・マネージャーに CAP ファイルの <serviceName> 要素で定義されているサービスのステータスを問い合わせることによって判断します。

タイプが *ITM_Windows* および *ITM_UNIX* のエージェントおよびインスタンスの場合、エージェント管理サービスは、CAP ファイルの <availabilityStatusScript> 要素に指定されたコマンドを使用して、エージェントが停止しているかどうかを判断します。そのコマンドは、kinconfg または cinfo を呼び出すスクリプトです。

オペレーティング・システムの実行中プロセスのリストにプロセスが表示されていない場合、エージェント管理サービスは、プロセスが中断されていると判断し、共通エージェント・パッケージ・ファイルの <startScript> 要素に定義されているコマンドまたはスクリプトを使用して、オペレーティング・システムの再始動を試みます。CAP ファイルがない場合は、オペレーティング・システムが検査されます。

構成されているものの開始されていない管理対象エージェントが、構成から 30 分以内に Watchdog によって自動的に開始されます。ユーザーによって開始された構成済みインスタンスが属している管理対象エージェントが即時に検出され、「エージェントの可用性状況 (Agents' Availability Status)」ビューに表示されます。

モニター・サーバーへの接続試行回数が CTIRA_MAX_RECONNECT_TRIES (デフォルト設定は 0) を超えると、エージェントはシャットダウンを試行します。エージェント管理サービス Watchdog が実行されている場合は、エージェントが即時に再始動されます。CTIRA_MAX_RECONNECT_TRIES を超えたときにエージェントがシャットダウンされるようにする場合は、この Watchdog プロセスを無効にする必要があります。AMS Stop Management アクションを使用して、Watchdog プロセスを停止します。

エージェントの手動管理

エージェントのエージェント管理サービス・ワークスペースから、アクション実行コマンドを実行して、エージェントの開始、停止、および管理対象と非管理対象の切り替えを行うことができます。

実行されたアクションは、反対のアクションを使用するか、あるいは他のメソッド (Tivoli Enterprise Portal、Tivoli Monitoring Services の管理、またはコマンド行) を使用してエージェントを開始または停止するまで持続されます。 「エージェント管理状況 *(Agents Management Status)*」表ビューで、状況を変更するエージェントの行を右クリックして、アクションを選択します。

AMS Recycle Agent Instance
このアクションを使用して、モニター・エージェントの特定インスタンスを停止して再始動します。

AMS Reset Agent Restart Count
このエージェントを使用して、エージェントが再始動を試行する回数を 0 に戻します。

AMS Start Agent
このアクションを使用して、IBM Tivoli Monitoring Agent Management Services の管理下にあるエージェントを開始します。マルチインスタンス・エージェントの場合は、**AMS Start Agent Instance** を使用します。

AMS Stop Agent
このアクションを使用して、IBM Tivoli Monitoring Agent Management Services の管理下にあるエージェントを停止します。

AMS Start Agent Instance
このアクションを使用して、モニター・エージェントの特定インスタンスを開始します。

AMS Start Management
このアクションを使用して、特定のエージェントを IBM Tivoli Monitoring Agent Management Services の管理下に置きます。このアクションは、意図的にオフラインにされていたエージェントの実行を再開し、管理対象にする場合に役立ちます。

AMS Stop Management
このアクションを使用して、特定のエージェントを IBM Tivoli Monitoring Agent Management Services の管理対象外にします。このアクションは、エージェントをオフラインにし、自動的に再始動しないようにする場合に役立ちます。

例えば、Universal Agent for Windows (エージェント管理サービス・ワークスペースの「エージェント管理状況 (Agent Management Status)」ビューに「*非管理対象*」として表示されている) の管理を開始するには、行を右クリックして、「**アクション実行**」>「**選択**」をクリックします。使用可能なアクションのリストから「AMS Start Management」アクションを選択します。コマンドは `NT:AMS_Start_Manage "Universal Agent for Windows"` のようになります。「**OK**」をクリックして、エージェントの管理を開始します。「**最新表示**」をクリックすると、Universal Agent の状況が「*管理対象*」に変更されます。

各コマンドおよび全般的なアクション実行コマンドの詳細情報は、「*Tivoli Enterprise Portal ユーザーズ・ガイド* 」および特定のエージェントのユーザーズ・ガイドを参照してください。

関連資料:

 アクション実行コマンド
Tivoli Enterprise Portal でアクション実行コマンドを使用および定義する方法

第 15 章 エージェント・オートノミー

Tivoli Enterprise Monitoring Agent は、Tivoli Enterprise Monitoring Server に依存せずに実行できます。モニター・エージェントに必要な機能、リソース制約、およびエージェントのモニター・サーバーに対する依存関係の度合いに基づいて、さまざまなレベルのオートノミーを構成できます。 IBM Tivoli Monitoring V6.2.2 FP2 以降のインフラストラクチャーを備えたモニター・エージェントは、オートノマス・モードで実行するように構成できます。

モニター・エージェントは、モニター・サーバーとは独立して開始され、モニター・サーバーから切断されているときに、データを収集し、シチュエーションを実行し、イベントを登録します。これはデフォルトの動作であり、オートノミーの度合いは調整できます。

Agent Builder または OS エージェントをオートノマスとして構成すると、Tivoli システム・モニター・エージェントになります。システム・モニター・エージェントは、モニター・サーバーとの依存関係や接続を持たないようにインストールされ、構成されます。システム・モニター・エージェントは、モニター・サーバーを介してのみ実行可能な処理を使用できないことを除き、他のモニター・エージェントと同様です。また、システム・モニター・エージェントは、Tivoli Management Services コンポーネントまたはエンタープライズ・モニター・エージェントと同じシステム上にインストールしないでください。

特殊 XML ファイルを構成して、モニター・サーバーに接続することなく、ローカルでシチュエーションを定義および実行したり、ローカルでヒストリカル・データを収集および保存したり、対応する受信側に Simple Network Management Protocol (SNMP) アラートまたは Event Integration Facility (EIF) イベント、またはその両方を発行したりできます。特殊 XML ファイルは、エンタープライズ・モニター・エージェントとシステム・モニター・エージェントの両方で使用できます。

オートノマス機能

Tivoli Enterprise Monitoring Agent および Tivoli System Monitor Agent の組み込みのオートノマス機能に加えて、Tivoli Enterprise Monitoring Server への接続が不要な特殊 XML ファイルを構成できます。この XML ファイルでは、シチュエーションをローカルに定義して実行し、シチュエーション・イベントを SNMP アラートまたは EIF イベントとして受信側に発行し、ヒストリカル・データをローカルに収集して保存し、一元化された構成を使用して XML ファイルの更新を選択したモニター・エージェントに配布できます。

Tivoli Enterprise Monitoring Agent

Tivoli Enterprise Monitoring Agent は、デフォルトでオートノマス操作用に構成されています。エージェントは、モニター・サーバーとの接続に関係なく開始され、実行を継続します。モニター・サーバーに接続していなくても、エージェントは引き続き自律してシチュエーションを実行できます。エージェントがモニター・サーバーに接続すると、切断中に発生したシチュエ

ーション・イベントがアップロードされます。これにより、エージェントで追加のディスク・スペースが使用されることになります。

一部のシチュエーションは、エージェント上のみでは完全に評価されず、モニター・サーバーに接続されていない場合に実行できないことがあります。例えば、COUNT、AVG などの式でグループ関数を使用するシチュエーションはモニター・サーバーで評価される必要があります。エージェントまたはホスト・システムが再起動された場合でも、イベントは引き続き保持され、再接続時にアップロードされます。これは、Tivoli Enterprise Monitoring Agent V6.2.2 以降フレームワークを使用するすべてのエージェントで自動的に実行されます。構成変更は不要です。

オートノマス・モード は、V6.2.1 で構成可能エージェント・パラメーター IRA_AUTONOMOUS_MODE として導入されています。 V6.2.2 からは、このパラメーターはデフォルトで使用可能に設定されています (**Y** に設定)。エージェントに対してオートノマスの動作を使用可能にしない場合は、このパラメーターを **N** に設定することにより使用不可に設定できます。このパラメーターの設定に関係なく、ヒストリカル・データ収集は常に自律的に実行され、シチュエーションのリフレックス・オートメーションはそのシチュエーションが TRUE になると実行されます。 358 ページの『オートノマス動作の環境変数』を参照してください。

z/OS OMEGAMON XE for z/OS および OMEGAMON XE for Storage エージェントは、ローカル RTE の Tivoli Enterprise Monitoring Server で構成されているため、接続状態で実行する必要があります。モニター・サーバーが使用できなくなると、これらのエージェントも使用できなくなります。モニター・サーバーに接続して実行した場合でも、SNMP トラップの発行および専用シチュエーションなどのオートノマス機能はサポートされます。 (OMEGAMON XE on z/OS エージェントは、スタンドアロンで (モニター・サーバー接続がなくても) 実行されるように構成できますが、それはアラートおよびシチュエーションに plex データを使用できないことを意味します。) OMEGAMON XE for IMS™ は、現在、オートノマス機能をサポートしていません。

Tivoli System Monitor Agent

Tivoli System Monitor Agent は、Tivoli Management Services のコンポーネントも Tivoli Enterprise Monitoring Agent もインストールされておらず、Tivoli Monitoring Agent Builder V6.2.2 以降でビルドされたエージェントのみがインストールされているコンピューターにインストールされます。

Tivoli System Monitor Agent のエージェントは、モニター・サーバーに接続することがない OS エージェントです。オートノマス・バージョンのエージェントで使用されるエージェント・コードは、フル OS エージェントにインストールされるエージェント・コードと同じですが、インストール・プロセスに Java は使用されず、構成ユーザー・インターフェースは提供されません。結果としてインストールは高速になり、インストール後の占有スペースも小さくなります。専用シチュエーション、SNMP アラートなどの機能を定義するローカルの XML 構成ファイルは、エージェントの始動時に処理されます。

専用シチュエーション

エンタープライズ・モニター・エージェントおよびシステム・モニター・エ

ージェントは、ローカルで定義されたシチュエーションを使用して完全に自律して動作できます。これらのローカルで定義された*専用*シチュエーションは、専用シチュエーション定義 XML ファイルで作成されます。専用シチュエーション・イベントは、モニター・エージェントから直接発生します。この機能を有効にするには、専用シチュエーション構成ファイルをエージェントのインストール済み環境に配置し、エージェントを再起動する必要があります。専用シチュエーション・イベントが開かれたときに SNMP アラートまたは EIF イベントを送信する場合は、SNMP トラップ構成ファイルまたは EIF イベント構成ファイルもエージェントのインストールに含める必要があります。

エンタープライズ・モニター・エージェント上の専用シチュエーションは、モニター・サーバーとの相互作用はなく、レポートも一切行っていません。専用シチュエーションおよびエンタープライズ・シチュエーションは、並行して実行可能です。

重要: 専用かエンタープライズかに関係なく、すべてのシチュエーションに固有の名前を付けるように注意してください。 そうしないと、あるシチュエーションで呼び出されたアクションが、同じ名前の他のシチュエーションに適用されます。 CLI **tacmd listSit** コマンドを使用すると、ハブ・モニター・サーバーでエンタープライズ・シチュエーションのリストを取得できます。

371 ページの『専用シチュエーション』を参照してください。

SNMP アラートおよび EIF イベント

IBM Tivoli Monitoring V.6.2.2 より前のバージョンでは、エンタープライズ・モニター・エージェントのシチュエーション・イベントは Tivoli Enterprise Monitoring Server によって EIF (Event Integration Facility) の受信側に転送できました。IBM Tivoli Monitoring V.6.2.2 以降では、SNMP アラートを構成し、モニター・サーバー を介してシチュエーション・イベントを渡さずに、エージェントから直接 SNMP 受信側にイベントのアラートを送信できます。IBM Tivoli Monitoring V.6.2.2 フィックスパック 1 以降では、専用シチュエーション・イベントを EIF 受信側に発行するために、EIF イベント構成ファイルを作成できます。

OMNIbus にイベントを送信するこれらの方式は共存可能であり、次のようにこれらを組み合わせて、モニター対象環境を構成できます。

- モニター・サーバーを使用してエンタープライズ・シチュエーション・イベントを IBM Tivoli Enterprise Console イベント・サーバー、Netcool/OMNIbus Probe for Tivoli EIF などの受信側に転送する。(『Tivoli Enterprise Console を使用したシチュエーション・イベントの統合』および『TivoliNetcool/OMNIbus によるシチュエーション・イベント統合』を参照。)
- エンタープライズ・シチュエーション・イベントの SNMP アラート、専用シチュエーション・イベント、またはその両方は、Netcool/OMNIbus SNMP プローブ などの受信側に送信する。
- 専用シチュエーション・イベントを、EIF イベント構成ファイルの定義どおりに EIF 受信側に直接発行する。

エンタープライズ・シチュエーション: トラップ構成 XML ファイルを作成すると、モニター・サーバーを介してルーティングせずに、SNMP アラートをエージェントから直接イベント受信側に送信できます。 エージェントは、エンタープライズ・シチュエーション定義を受信するために、少なくとも 1 回はモニター・サーバーに接続する必要があります。この機能を有効にするには、エージェントのインストール済み環境に SNMP トラップ構成ファイルを配置し、エージェントを再起動する必要があります。

専用シチュエーション: また、エンタープライズ・モニター・エージェントおよびシステム・モニター・エージェントは、Netcool/OMNIbus SNMP プローブ などの受信側に専用シチュエーションの SNMP アラートを直接送信するか、専用シチュエーションの EIF イベントを IBM Tivoli Enterprise Console イベント・サーバー、Netcool/OMNIbus Probe for Tivoli EIF などの EIF 受信側に発行することができます。

重要: エンタープライズ・シチュエーション・イベントを Netcool/OMNIbus Probe for Tivoli EIF に転送し、エンタープライズ・シチュエーション・イベントの SNMP アラートを Netcool/OMNIbus SNMP プローブ に発行している場合、EIF が転送するシチュエーション・イベントと SNMP アラートで、形式および含まれているデータがそれぞれ異なります。 同じ Netcool/OMNIbus ObjectServer に接続されている両方のプローブに送信されるシチュエーションのイベントは、OMNIbus の非重複化では同一のイベントとして検出されないことに注意してください。 このため、個別に処理される ObjectServer 内の同一イベントに対するエントリーが重複することになります。通常、これは推奨されておらず、管理しにくい場合があります。

403 ページの『SNMP アラート』 および 422 ページの『EIF イベント』を参照してください。

専用ヒストリー

ローカルにインストールされたエージェント用に専用シチュエーションを作成できるのと同様に、HISTORY 要素を使用して同じ専用シチュエーション構成ファイルに短期ヒストリカル・データを収集するように、専用ヒストリーを構成できます。結果の専用ヒストリー・バイナリー・ファイルは、エージェント・サービス・インターフェースを使用して表示できます。Tivoli Data Warehouse を構成済みの場合は、定期的にヒストリカル・データベースにロールオフされる短期データを持つことができます。

HISTORY 要素の属性は、ヒストリカル・データをコンピューターに保持し、それがトリムされるか、データウェアハウスにロールオフされるまでの時間数を設定します。ヒストリカル・データを保持する期間はデフォルトで 24 時間ですが、コンピューターのストレージ上の実質的な制限を除けば、データをローカルに保持できる時間に制限はありません。EXPORT パラメーターが構成されていない場合、krarloff などの付属のファイル変換プログラムを使用して、ヒストリー・ファイルのデータをテキスト・ファイルに移動できます。

WAREHOUSE 要素は、ヒストリカル・データのエクスポート先のウェアハウス・プロキシー・エージェントを指定します。

395 ページの『専用ヒストリー』を参照してください。

エンタープライズ・シチュエーションのオーバーライド

ローカルにインストールされているエンタープライズ・モニター・エージェントに対するシチュエーションのオーバーライドを、*pc*_thresholds.xml (*pc* は 2 文字の製品コード) 構成ファイルを使用して構成することができます。また、このオーバーライドはエージェントで手動で管理することも、一元化された構成で管理することもできます。更新されたシチュエーションしきい値は、モニター・エージェントの再始動後に有効になります。エージェントは、しきい値のオーバーライドをローカル・ファイルに送信し、エージェントを再始動してもアクティブなシチュエーションのしきい値が保持されるようにします。

スケジュールは、平日、月内の特定日、および 1 日の開始および終了時間に基づいて適用できます。エンタープライズ・モニター・エージェントは、アクティブなシチュエーションしきい値レコードをエージェント・オペレーション・ログに書き込むことで、動的シチュエーションしきい値のオーバーライドの監査証跡を維持します。これを Tivoli Enterprise Portal のワークスペースに追加して有効なシチュエーションしきい値をレビューすることができます。

397 ページの『エンタープライズ・シチュエーション・オーバーライド XML 指定』を参照してください。

エージェント・サービス・インターフェース

IBM Tivoli Monitoring サービス索引ユーティリティーにより、ローカルにインストールされた各モニター・エージェント用のエージェント・サービス・インターフェースへのリンクが提供されます。オペレーティング・システムにログインした後、エージェント情報、シチュエーション、ヒストリー、照会のいずれかのレポートを選択できます。

さらに、即時的な構成ダウンロードを開始したり、シチュエーションを再開するなどのサービス・インターフェース要求を直接行うこともできます。

442 ページの『エージェント・サービス・インターフェース』を参照してください。

一元化された構成

一元化された構成を使用して、*中央構成サーバー*から定期的に (デフォルトは 60 秒ごと) またはオンデマンドで取得される、モニター・エージェント構成 XML ファイルを 1 カ所で維持します。 一元化された構成に参加しているエージェントは、それぞれ独自の *構成ロード・リスト* の XML ファイルを持ちます。このファイルには、指定した構成ファイルの最新の更新内容を取得するための接続先が記述されています。

構成の更新用に 1 つ以上のモニター・エージェントが接続するコンピューターは、*中央構成サーバー*と呼ばれます。構成の更新をダウンロードする 1 つ以上のモニター・エージェントを持つコンピューターは、中央構成クライアントと呼ばれます。

『一元化された構成』を参照してください。

オートノマス動作の環境変数

エージェント・フレームワーク・サービスで提供された環境ファイルを使用して、エージェントが Tivoli Enterprise Monitoring Server から切断された場合の Tivoli System Monitor Agent または Tivoli Enterprise Monitoring Agent のオートノマス動作を制御します。

「*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)」には、Tivoli System Monitor Agent のインストールおよび構成について説明されています。また、付録では、共通エージェント環境変数の参照も示されています。

Tivoli Enterprise Monitoring Agent 環境ファイル

環境変数は、Tivoli Enterprise Monitoring Agent 環境ファイルで編集するか、このファイルに追加します。ここで、*pc* は 2 文字の製品コードです。

Windows *install_dir* ¥TMAITM6¥k*pc*cma.ini. エージェントを再構成して、変更内容を実装します。

Linux UNIX *install_dir* /config/*pc*.ini。システム・モニター・エージェントの場合、このファイルは *pc*.environment です。エージェントをリサイクルして、変更内容を実装します。

IBM i /qautotmp/kmsparm.kbbenv

z/OS *&hilev.&rte.*RKANPARU 内のメンバー名 *KPC*ENV

z/OS のベスト・プラクティス

構成ツール (Installation and Configuration Assistance Tool (ICAT) とも呼ばれる) の「非標準パラメーターの指定 (Specify Nonstandard Parameters)」パネルを使用して、メンバーを変更します。このエディターを使用して行われたすべての変更内容は、ランタイム環境が更新されたときに自動的に保存されます。つまり、設定は次回のランタイム環境の更新時に上書きされません。「*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS 共通計画および構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)」の『Adding, changing, or deleting a parameter in a runtime member』トピックを参照してください。

*&hilev.&rte.*RKANPARU データ・セットの KDSENV メンバーで定義されたオーバーライド・パラメーターは、アドレス・スペース内で実行されているすべてのエージェントに使用されます。すべてのエージェントが同じ EIF イベント宛先を共有する可能性があるため、これは IRA_EIF_DEST_CONFIG に関して適切に機能します。他のオーバーライド・パラメーターも使用できますが、識別されたデータ・セット・メンバーが複数のエージェントの定義をまとめる必要がある場合があります (推奨されていません)。ベスト・プラクティスは、同じアドレス・スペースで複数のエージェントを実行する場合に、ローカルの構成データ・セット・メンバーに対してデフォルトの命名規則を使用することです。

PARMGEN の使用について詳しくは、*IBM Tivoli OMEGAMON XE および Tivoli Management Services on z/OS: PARMGEN リファレンス・ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/

com.ibm.omegamon_share.doc_6.3/parmgenref/parmgenref.htm)の『ランタイム環境の保守シナリオ』を参照してください。

Tivoli Enterprise Monitoring Agent でのオートノミーの制御

以下の構成パラメーターにより、Tivoli Enterprise Monitoring Agent のオートノマス動作が開始され、制御されます。

IRA_AUTONOMOUS_LIMIT=50

このパラメーターは、オートノマス・モードのエージェントに保管できるイベントの数を設定するか、またはイベントが使用できるディスク・スペースを割り当てます。イベント限度または最大ディスク・スペースに達すると、イベントは収集されません。デフォルトは **50** イベントまたは **2MB** です。イベントの合計数またはディスク・スペース制限を指定します。*n* は数値です。

n = 保存できるイベントの最大数 (サンプルおよびピュア)。各イベントのスペースを推定するには、平均アプリケーション行サイズに 1200 を足します。

nKB = 1024 バイトの n 倍

nMB = 1,024,000 バイトの n 倍

nGB = 1,024,000,000 バイトの n 倍

IRA_AUTONOMOUS_MODE=Y

このパラメーターにより、エンタープライズ・モニター・エージェントでのオートノマス操作が制御されます。デフォルトで、オートノミーは使用可能です。使用不可にして、V6.2.1 より前のモニター・サーバーと同じ依存関係にエージェントを設定するには、このパラメーターを **N** に設定します。

IRA_EIF_DEST_CONFIG=*filename*

このパラメーターは、エージェント環境ファイルで使用して、EIF 宛先構成 XML ファイルの場所を指定します。絶対パスか、またはローカル構成ディレクトリーに対する相対パスを指定できます。

IRA_EIF_MSG_LOCALE=en_US

エージェント環境ファイルのこのパラメーターは、デフォルトで米国英語に設定します。事前定義されたマッピング・ファイルおよび言語リソース・バンドルを使用して生成されたイベント内のメッセージ・スロットに対してグローバル化されたメッセージ・テキストをサポートするエージェントの場合、デフォルトの言語ロケールを指定できます。

IRA_EVENT_EXPORT_CHECKUSAGE_INTERVAL=180

IRA_AUTONOMOUS_LIMIT に達したかどうかを確認する優先間隔を秒単位で指定します。デフォルトの間隔は、**180** 秒 (3 分) です。指定できる最小間隔は **60** 秒です。

IRA_EVENT_EXPORT_EIF=Y

エージェント環境ファイルのこのパラメーターは、EIF イベントのエクスポート機能を有効にするために設定します。機能を無効にするには、値を **N** に変更します。

IRA_EVENT_EXPORT_SIT_STATS=Y

エージェント・サービス・インターフェースを使用して、シチュエーション

操作統計のレポートを取得できます。このパラメーターにより、以下の基本シチュエーション操作の統計データ収集が使用可能 (Y) または使用不可 (N) に設定されます。

シチュエーション名

シチュエーション・タイプ - エンタープライズまたは専用

アプリケーション名

テーブル名

サンプル間隔

行データ・サイズ

最初に開始されたシチュエーションのタイム・スタンプ

最初にシチュエーションが作成したイベントのタイム・スタンプ (渡されたフィルター)

最後に開始されたシチュエーションのタイム・スタンプ

最後に停止されたシチュエーションのタイム・スタンプ

最後に TRUE と評価されたシチュエーションのタイム・スタンプ

最後に FALSE と評価されたシチュエーションのタイム・スタンプ

シチュエーションのリサイクル回数

シチュエーションがオートノマス・モードになった回数

デフォルト: **Y**。

IRA_EVENT_EXPORT_SIT_STATS_DETAIL=N

Y に設定すると、このパラメーターは、以下のイベント・メトリックの、エージェントからの収集を有効にします。

True サンプル数

False サンプル数

True サンプル比率

False サンプル比率

24 時間でカウントされたデータ行の数

24 時間でカウントされた True サンプルの数

24 時間でカウントされた False サンプルの数

エージェントは、これらのメトリックを毎日深夜 0 時にロールオフしながらディスクで 8 日間保持します。デフォルト: **N**。

IRA_EVENT_EXPORT_SNMP_TRAP=Y/N

IRA_EVENT_EXPORT_SNMP_TRAP=N を使用すると、*pc*_trapcnfg.xml ファイルが配置されていても、エージェントの SNMP アラートを使用不可にできます。デフォルト: **Y**。

IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG

デフォルトで、エージェントは、*install_dir* /localconfig/*pc*/*pc*_trapcnfg.xml ファイルが存在するかどうかを検査します。構成ファイルを別の場所に配置したり、別の名前を付けた場合は、このパラメーターを使用してそのファイルのパスおよび名前を指定します。絶対パスか、またはローカル構成ディレクトリーに対する相対パスを指定できます。

z/OS エージェントは、その環境の *&hilev.&rte.*RKANDATV データ・セット内でデフォルトの *PC*TRAP メンバー名を検索します。 SNMP トラップ・メンバーの名前が異なる場合は、そのメンバー名をこの変数に指定します。メンバーが別のデータ・セット内にある場合は、データ・セット名とメンバー名の両方を *member_name.dataset_name* という形式で指定します。

例えば、構成ファイルの名前が MYSNMP で、RKANDATV に含まれている場合は、`IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG=MYSNMP` と指定します。構成ファイルが別のデータ・セット内にある場合、例えば TIVOLI.ITM622.TVT1006.MYFILES(MYSNMP) にある場合は、`IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG=MYSNMP.MYFILES` と指定します。

IRA_LOCALCONFIG_DIR

専用シチュエーションなどのローカルにカスタマイズされた構成ファイル、EIF イベント構成および SNMP トラップ構成ファイルを含むデフォルトのローカル構成ディレクトリー・パスは、*CANDLE_HOME* 環境変数 (z/OS システムの RKANDATV *DD* 名) で指定されたディレクトリーの `localconfig` サブディレクトリーです。このパラメーターはパスを変更するために使用します。

KHD_REGWITHGLB

通常、Warehouse Proxy agent はハブ・モニター・サーバーに登録されます。ウェアハウス・プロキシーがモニター・サーバーに依存しないようにする場合は、KHD_REGWITHGLB=N をウェアハウス・プロキシーの環境ファイル (Windows `khdenv`、Linux UNIX `hd.ini`) に追加して、モニター・サーバーに登録しないようにします。

KHD_WAREHOUSE_LOCATION

Warehouse Proxy agent をハブ・モニター・サーバーに登録しない場合は、このパラメーターを、完全なオートノミーを持つすべてのエンタープライズ・モニター・エージェントの環境ファイルに追加する必要があります。エージェントから Tivoli Data Warehouse にヒストリカル・データを転送できる各ウェアハウス・プロキシーの完全修飾名を、セミコロン (;) で区切って入力します。 構文は、`KHD_WAREHOUSE_LOCATION=`*`family protocol:network address[port number]`* です。例えば、`KHD_WAREHOUSE_LOCATION=ip.pipe:DEPT-XP[63358];ip:MY-XP[63358];ip.pipe:#9.44.255.253[65538]` します。

KSY_AUTONOMOUS

通常、属性グループの要約およびプルーニングの設定は、Tivoli Enterprise Portal またはコマンド行インターフェース **tacmd histconfiguregroups** で構成して、Tivoli Data Warehouse の WAREHOUSESUMPRUNE テーブルに保存します。

要約およびプルーニング・エージェントが Tivoli Enterprise Portal Server に依存しないようにする場合は、要約およびプルーニング・エージェントの環境ファイルに KSY_AUTONOMOUS=Y を追加し、KSY_AUTONOMOUS_ODI_DIR 変数を使用してエージェントの説明ファイルの場所を追加します。

要約およびプルーニング・エージェントは、ポータル・サーバーにインストールされるエージェント・アプリケーション・サポート・ファイルを必要と

します。 KSY_AUTONOMOUS=Y を設定した場合に、要約およびプルーニング・エージェントがポータル・サーバーと同じコンピューター上にインストールされていないときは、必要なアプリケーション・サポート・ファイルを同じコンピューター上にコピーする必要があります。 **dockcj** (使用されていない) を除いて、サポート・ファイルは **dock*pc*** (*pc* は 2 文字の製品コード) ファイルで、ポータル・サーバーのディレクトリーにあります (Windows *install_dir* ¥cnps、Linux UNIX *install_dir* /*arch*/cq/data)。 *IBM Tivoli Monitoring インストールおよび設定ガイド*の『Running the warehouse agents autonomously』を参照してください。

KSY_AUTONOMOUS_ODI_DIR

ポータル・サーバーからSummarization and Pruning agentのオートノミーを構成できますが、ヒストリカル・データを収集するように構成されるすべてのエージェントに関して、ポータル・サーバーがインストールされ、アプリケーション・サポートが存在する必要があります。これは、自律的に稼働する際に、このアプリケーション・サポート・ファイルが要約およびプルーニング・プロセスで必要になるためです。このパラメーターは、アプリケーション・サポート・ファイルへのパスの入力に使用します。

自律的に実行されるようにエージェントを構成した場合、要約およびプルーニングの設定は、SQL の挿入コマンドを使用して、ウェアハウス・データベースの WAREHOUSESUMPRUNE テーブルに直接入力する必要があります。

専用シチュエーション

IRA_PRIVATE_SITUATION_CONFIG

専用シチュエーション構成ファイルの絶対パスのファイル名を指定します。エージェントの初期化時に、専用シチュエーション構成ファイル (*install_dir* /localconfig/*pc*/*pc*_situations.xml) が検査されます。ここで、*pc* は 2 文字の製品コードです。

z/OS z/OS 上のシチュエーション構成ファイルへの完全修飾パス ('TIVOLI.ITM622.TVT1006.RKANDATV(MYPSSIT)' where DDNAME RKANDATV is TIVOLI.ITM622.TVT1006.RKANDATV: IRA_PRIVATE_SITUATION_CONFIG=MYPSSIT など)。
DDNAME RKANDATV の PDS メンバーではないシチュエーション構成ファイルの場合は、'TIVOLI.ITM622.TVT1006.MYFILES(MYPSSIT)' where DDNAME MYFILES is TIVOLI.ITM622.TVT1006.MYFILES: IRA_PRIVATE_SITUATION_CONFIG=MYPSSIT.MYFILES を指定します。

専用シチュエーションについては、 371 ページの『専用シチュエーション』を参照してください。

専用ヒストリー

CTIRA_HIST_DIR

エージェント・ベースの短期ヒストリー・データ・ファイルが格納されるディレクトリーを指定します。モニター・サーバーの短期ヒストリー・データ・ファイルには適用されません。これは、エンタープライズ・ヒストリーまたは専用ヒストリーの各バイナリー・ファイル用のデフォルトのロケーションです。

Windows *install_dir* ¥TMAITM6¥logs

Linux UNIX *install_dir* */arch/pc/*hist

専用ヒストリー・データ収集については、395 ページの『専用ヒストリー』を参照してください。

シチュエーション式のオーバーライド

CTIRA_THRESHOLDS

XML ベースの適応 (動的) しきい値オーバーライド・ファイルの完全修飾名を指定します。デフォルトでは、エージェントは *install_dir* /localconfig/*pc*/*pc*_thresholds.xml (*pc* はエージェントの製品コード) ファイルが存在するかどうかを確認します。絶対パスか、またはローカル構成ディレクトリーに対する相対パスを指定できます。

z/OS デフォルトのファイル名は ***PC*THRES** です。完全なパスを指定するには、PDS が最後にリストされている必要があります (または省略して、デフォルトの RKANDATV を使用します)。

IRA_ADAPTIVE_THRESHOLD_MODE

適応 (動的) しきい値演算モード CENTRAL または LOCAL を指定します。デフォルトのモードは CENTRAL です。

CENTRAL モードの場合、Tivoli Enterprise Portal または CLI **tacmd setOverride** コマンドでシチュエーションのしきい値のオーバーライドが作成され、Tivoli Enterprise Monitoring Server によってターゲット・エージェントに配布されます。

CENTRAL オーバーライド配布ではなく、エージェントを LOCAL モードに設定して、ローカルに定義されたしきい値構成 XML がエージェントで使用されるようにできます。 LOCAL モードでは、エージェントへの中央配布は禁止されています (アフィニティーは登録されません)。また、しきい値のオーバーライドはローカルで作成され、管理されます。LOCAL モードを使用する場合、Tivoli Enterprise Monitoring Server のしきい値と、エージェントのしいき値が同期しなくなるため、注意して使用してください。

エージェントを LOCAL モードから CENTRAL モードに切り替えて戻した場合、CENTRAL オーバーライド指定はローカルの定義に置き換わり、モニター・サーバーにある CENTRAL オーバーライド・リポジトリーに同期されます。

ローカルのシチュエーションのオーバーライドについては、397 ページの『エンタープライズ・シチュエーション・オーバーライド XML 指定』を参照してください。

エージェント・サービス・インターフェース

以下のエージェント構成パラメーターは、サービス・インターフェース操作に影響を与えます。

IRA_SERVICE_INTERFACE_NAME

優先エージェント・サービス・インターフェース名を指定してより機能的に分かりやすい名前を定義し、エージェントが生成する k*pc*agent (*pc* は 2 文字の製品コード) の形式のデフォルト名 (kntagent、kmqagent など)、ま

たは *pc*agent の形式のデフォルト名 (uagent02 など) と置き換えて、システムに 2 番目にインストールされた Universal Agent インスタンスを識別します。

デフォルト:

Windows system.*hostname_pc*

Linux UNIX *hostname_pc*

IRA_SERVICE_INTERFACE_DEFAULT_PAGE

エージェント・サービス・インターフェースへのログオン時に、デフォルトの **navigator.htm** ページではなく、指定された製品固有の HTML ページを開くようエージェントに指示します。デフォルトでは、エージェントは分散システム上の *install_dir* /localconfig および z/OS システム上の RKANDATV データ・セットで製品固有のファイルを検索します。ただし、IRA_SERVICE_INTERFACE_DIR 環境変数が設定されている場合、エージェントはこの環境変数に指定されたディレクトリーを確認します。

IRA_SERVICE_INTERFACE_DEFAULT_PAGE (IRA_SERVICE_INTERFACE_DIR ではなく) を設定した場合、任意の製品固有の HTML ページを分散システム上の *install_dir* /localconfig/html ディレクトリーに配置する必要があります。そのため、**myPage.htm** を作成して *install_dir* /localconfig/html に配置した場合は、IRA_SERVICE_INTERFACE_DEFAULT_PAGE=/html/myPage.htm を設定します。

IRA_SERVICE_INTERFACE_DIR

エージェント・サービス・インターフェースの HTML ディレクトリーのパス指定を定義します。エージェントは、IRA_SERVICE_INTERFACE_DEFAULT_PAGE パラメーターと組み合わせて、要求された特定の HTTP GET オブジェクトのファイル・パスを構成します。デフォルトは、分散システム上の *install_dir* /localconfig です。

例: IRA_SERVICE_INTERFACE_DIR="¥mypath¥private" の場合にブラウザーに http://localhost:1920///kuxagent/kuxagent/html/myPage.htm と入力すると、myPage.htm が、*ITM_dir*¥localconfig¥html¥ ではなく ¥mypath¥private¥html¥ から取得されます。

z/OS ディレクトリー・パスの指定はありませんが、JCL DD (データ定義) 名で表されるデータ・セットがあります。そのため、IRA_SERVICE_INTERFACE_DIR は使用されず、IRA_SERVICE_INTERFACE_HTML の指定が有効になります。デフォルトは RKANDATV DD 名です。

IRA_SERVICE_INTERFACE の接頭辞が付いた一元化された構成の環境変数も参照してください。

診断およびトラブルシューティング

これらのパラメーターは、トラブルシューティング用にエージェントの環境ファイルに設定できます。すべての診断情報は、エージェントの RAS (信頼性、可用性、およびサービス性) トレース・ログに入力されます。

IRA_DEBUG_AUTONOMOUS=N

Y に設定すると、このパラメーターはすべてのオートノマス・エージェント操作のトレース・ロギングを有効にします。デフォルト設定は **N** です。

IRA_DEBUG_EIF=N

Y に設定すると、このパラメーターは EIF エミッター操作のトレース・ロギングを有効にします。デフォルト設定は **N** です。

IRA_DEBUG_EVENTEXPORT=N

Y に設定すると、このパラメーターは、SNMP トラップなどのイベント・エクスポート・アクティビティーのトレース・ロギングを有効にします。デフォルト設定は **N** です。

IRA_DUMP_DATA=N

Y に設定すると、このパラメーターはすべてのリモート・プロシージャー・コール (RPC) ・データのトレース・ロギングを有効にします。デフォルト設定は **N** です。

IRA_DEBUG_PRIVATE_SITUATION=N

Y に設定すると、専用シチュエーションの問題に関するすべてのトレース情報が RAS トレース・ログに入力されます。デフォルト設定は **N** です。

IRA_DEBUG_SERVICEAPI=N

Y に設定すると、このパラメーターはすべてのエージェント・サービス・インターフェース処理のトレース・ロギングを有効にします。デフォルト設定は **N** です。

KEF_DEBUG=N

Y に設定すると、このパラメーターは EIF ライブラリー操作のトレース・ロギングを有効にします。デフォルト設定は **N** です。

シチュエーション制限

専用シチュエーションで使用できる式関数のタイプには制限があります。また、Tivoli Enterprise Monitoring Server からの切断時にエージェントで処理できる、エンタープライズ・シチュエーションの式関数のタイプにも制限があります。

表 29. エンタープライズ・エージェントの接続時または切断時、あるいはシチュエーションが専用の場合のシチュエーション式関数の可用性

	モニター・サーバーから発行されたイベント	エンタープライズ・モニター・エージェントから発行されたイベント		
式関数	エンタープライズ・シチュエーションでのサポート	エンタープライズ・シチュエーション モニター・サーバーに接続されたエージェント モニター・サーバーでの評価	エンタープライズ・シチュエーション モニター・サーバーから切断されたエージェント エージェントでの評価	専用シチュエーションでのサポート エージェントでの評価 [1]
セル関数				

表 29. エンタープライズ・エージェントの接続時または切断時、あるいはシチュエーションが専用の場合のシチュエーション式関数の可用性 (続き)

	モニター・サーバーから発行されたイベント	**エンタープライズ・モニター・エージェントから発行されたイベント**		
式関数	**エンタープライズ・シチュエーションでのサポート**	**エンタープライズ・シチュエーション モニター・サーバーに接続されたエージェント モニター・サーバーでの評価**	**エンタープライズ・シチュエーション モニター・サーバーから切断されたエージェント エージェントでの評価**	**専用シチュエーションでのサポート エージェントでの評価 [1]**
CHANGE	使用可能	使用可能	使用可能	使用不可
DATE	使用可能	使用可能	使用可能	使用不可
MISSING	使用可能	使用可能	使用可能	使用可能
PCTCHANGE	使用可能	使用可能	使用可能	使用不可
SCAN	使用可能	使用可能	使用可能	使用不可
STR	使用可能	使用可能	使用可能	使用不可
TIME	使用可能	使用不可	使用不可	使用不可
VALUE	使用可能	使用可能	使用可能	使用可能
IN	使用可能	使用可能	使用可能	使用不可
「**グループ関数**」は、複数の行属性グループ、およびヒストリカル・データ収集用に構成された行属性グループに適用できます。 表ビューおよびグラフ・ビューは、データ・サンプリングの幅を示すために、時刻範囲を設定する必要があります。				
AVG	使用可能	使用不可	使用不可	使用不可
COUNT	使用可能	使用不可	使用不可	使用不可
MAX	使用可能	使用不可	使用不可	使用不可
MIN	使用可能	使用不可	使用不可	使用不可
SUM	使用可能	使用不可	使用不可	使用不可
シチュエーションの特性				
組み込み (相関シチュエーションを含む)	使用可能	使用不可	使用不可	使用不可
複数の属性グループ	使用可能	使用不可	使用不可	使用不可
有効な永続性	使用可能	使用可能 [2]	使用可能 [2]	使用不可
選択済み表示項目	使用可能	使用可能	使用不可 [3]	使用不可
大規模プロセスの使用	使用可能	使用可能	使用不可 [4]	使用不可
管理対象システム・グループへの配布	使用可能	使用可能	使用可能	使用不可

表 29. エンタープライズ・エージェントの接続時または切断時、あるいはシチュエーションが専用の場合のシチュエーション式関数の可用性 (続き)

	モニター・サーバーから発行されたイベント	エンタープライズ・モニター・エージェントから発行されたイベント		
式関数	エンタープライズ・シチュエーションでのサポート	エンタープライズ・シチュエーション モニター・サーバーに接続されたエージェント モニター・サーバーでの評価	エンタープライズ・シチュエーション モニター・サーバーから切断されたエージェント エージェントでの評価	専用シチュエーションでのサポート エージェントでの評価 [1]

[1] この列はシステム・モニター・エージェントにも適用されます。

[2] シチュエーションの永続性がエージェントで評価されません。トラップは、シチュエーションが true になるたびにトラップが発行される RC (継続上昇) と、シチュエーションが最初に true になったときにトラップが発行され、シチュエーションが true でなくなったときにクリア・トラップが発行される HY (ヒステリシス) の 2 つのモードで発行できます。また、永続性ルールを実装することにより、トラップ宛先で永続性を有効にすることができます。

[3] 表示項目 (複数行の属性グループで使用可能) を含んだシチュエーションは、true に評価される最初の行に対してのみ 1 つの SNMP アラートを送信でき、true に評価される後続の行に対してはアラートを送信できません。

[4] エージェントがモニター・サーバーから切断されている場合、トラップは発行されますが、シチュエーションは評価されません。

制約事項: MISSING 関数がサブノードに配布される専用シチュエーションの場合、DISTRIBUTION タグにサブノードのリストが存在する必要があります。 MISSING 関数がエージェントに配布される専用シチュエーションの場合、これは必要ありません。

サブノードを持つエンタープライズ・モニター・エージェントからの SNMP アラート

サブノードを使用するモニター・エージェント (Agent Builder、Monitoring for Energy Management、Agentless Monitoring for Operating Systems などを使用して作成されたサブノード・エージェント) では、シチュエーションが true に評価されるエージェント・インスタンス 1 つにつき 1 つのサブノードに対してのみ SNMP アラートを発行できます。同じシチュエーションが true に評価された場合でもそれ以外のサブノードに対してはアラートを発行できません。

エージェント・インスタンスごとに、データ・サンプルが 1 つの属性グループ・テーブルに収集されます。これらのメトリックは、Tivoli Enterprise Portal に表示されるときにサブノードによってフィルター操作されますが、1 つのエージェント・インスタンスの複数のサブノードで実行されるシチュエーションは、実際には単一テーブル上で評価されます。シチュエーションが 1 つのサブノードで true になると、そのシチュエーション用に定義された SNMP アラートが発行されますが、テー

ブル上で他の行は処理されていないため、他のサブノードでは、そのシチュエーションに対する SNMP アラートは発行されません。

以下に、サブノードを持つエージェントに SNMP アラートを発行することの代替手段をいくつか示します。

- モニター・サーバー から EIF 受信側にイベントを転送します。
- エージェントの構成時に、エージェント・インスタンス 1 つにつき 1 つのサブノードのみを定義します。
- サブノードごとに個別のシチュエーションを定義し、そのシチュエーションを単一のサブノードのみに配布します。以下の例では、

  シチュエーション **KAB_Log_Message** は **AB エージェント**の **ALL LOG** サブノードに配布されます。

  シチュエーション **KAB_Log1only_Message** は **AB:uxlog1:LOG** サブノードのみに配布されます。

  シチュエーション **KAB_Log2only_Message** は **AB:uxlog2:LOG** サブノードのみに配布されます。

  AB ログ・モニター・エージェントのインスタンス 1 は、**uxlog1**、**uxlog2**、および **uxlog3** という 3 つのログ (各ログ・ファイルに 1 つのサブノードがあります) をモニターします。

  サブノード **uxlog1** によってモニターされるファイルにメッセージが表示されると、シチュエーション **KAB_Log_Message** および **KAB_Log1only_Message** が true になります。

  サブノード **uxlog3** によってモニターされるファイルにメッセージが表示されると、シチュエーション **KAB_Log_Message** が true になります。

  エージェントの専用シチュエーション構成ファイル:

```
<PRIVATECONFIGURATION>
  <PRIVATESIT>
   <SITUATION>KAB_Log_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog:LOG</DISTRIBUTION>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>KAB_Log1only_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog1:LOG</DISTRIBUTION>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>KAB_Log2only_Message</SITUATION>
    <CRITERIA><![CDATA[ *IF *VALUE KAB_LOGFILE.Message *NE "" ]]>
   </CRITERIA>
   <INTERVAL>000000</INTERVAL>
   <DISTRIBUTION>AB:uxlog2:LOG</DISTRIBUTION>
 </PRIVATESIT>
</PRIVATECONFIGURATION>
```

UTF-8 エンコードされた XML ファイル

8 ビットのエンコード方式であるユニコード・トランスフォーメーション・フォーマットは、既存の ASCII ベースのシステムで容易に使用できるように設計されており、Unicode 標準でのすべての文字を使用可能にします。 付加記号が付いた文字や 2 バイト文字セットなど、ASCII 以外の文字セットでローカル構成 XML ファイルを作成した場合は、UTF-8 エンコード方式でファイルを保存できるエディターを使用します。

Windows Linux UNIX

ASCII 文字は 1 バイト文字を使用し、最初の 128 文字で構成されます。XML ファイルは、どのテキスト・エディターでも記述できます。付加記号を含む文字や漢字など、ASCII 以外の文字の場合は、UTF-8 でファイルを保存できるエディターが必要です。

z/OS

z/OS では、UTF-8 を簡単に表示または編集できないため、XML は UTF-8 にエンコードしたり、エージェントのコード・ページを使用できます。コード・ページは、LANG=en_US.IBM-1047 など、環境変数 LANG を使用してエージェントの環境ファイルに設定されます。環境ファイルは、メンバー名 K*PC*ENV で *&hilev.&rte.*RKANPARU に保存されています (ここで、*PC* は 2 文字の製品コードです)。ファイルの編集にエミュレーターを使用している場合、LANG 変数は端末エミュレーターと一致する必要があります。Windows、Linux、または UNIX でファイルを編集していて、そのファイルを ASCII テキストでホストにアップロードする場合、FTP のデフォルトのコード・ページは IBM-1047 です。

Tivoli Enterprise Monitoring Server on z/OS の構成の『z/OS 上のハブ・モニター・サーバーおよびリモート・モニター・サーバーの構成』を参照してください。

IBM i

(EIF イベント宛先構成はサポートされていません。SNMPv3 インフォームもサポートされていません。)IBM i では、UTF-8 を簡単に表示または編集できないため、XML を UTF-8 またはエージェントのコード・ページでエンコードできます。コード・ページは、LANG=/QSYS.LIB/EN_US.LOCALE など、環境変数 LANG を使用してエージェントの環境ファイルに設定されます。LANG 環境変数は、Qshell インタープリターである **qsh** を開始する前に設定するのが最善です。ロケールがジョブのコード化文字セット ID および言語 ID に対して有効でないと、ユーティリティーによっては正常に作動しない場合があります。

Tivoli System Monitor Agent でのエージェント管理サービスの構成

サービスを使用してエージェントの可用性をモニターし、制御する場合は、エージェント管理サービスをTivoli System Monitor Agent用に構成します。

始める前に

システム・モニター・エージェント環境では、エージェント管理サービスの構成内容が異なります。

- システム・モニター・エージェントは、デフォルトでエージェント管理サービスによって管理されます。管理を中断するには、システム・モニター・エージェントおよび Tivoli Monitoring Agent Builder を使用して同じシステム上に作成されたエージェントのエージェント管理サービス Watchdog を使用不可にする `disarmWatchdog` コマンドを使用します。エージェント管理サービスによる管理を再開するには、エージェント管理サービスで管理されているオートノマス・エージェントの Watchdog を有効にする `rearmWatchdog` コマンドを使用します。これらのコマンドについては、エージェントのユーザーズ・ガイドに記載されています。
- システム・モニター・エージェント環境にインストールされている Agent Builder エージェントは、デフォルトでは、エージェント管理サービス Watchdog で管理されません。エージェントが Watchdog で管理されるかどうかは、指定変更できます。

このタスクについて

システム・モニター・エージェント環境に Agent Builder エージェントをインストールした後、以下のステップを実行して、エージェント管理サービスの管理を開始または停止します。

手順

1. Watchdog プロセスの実行中に、共通エージェント・パッケージ (CAP) ・ファイル k*pc*_default.xml (*pc* は 2 文字の製品コード) を CAP ディレクトリーから一時ロケーションに移動します。 このファイルは、KCA_CAP_DIR ディレクトリーにあります。

   Windows *install_dir* ¥TMAITM6[_x64]¥CAP¥

   Linux UNIX *install_dir* /config/CAP

   CAP ディレクトリーからファイルを削除すると、エージェント管理サービスから不可視のエージェントがレンダリングされます。
2. CAP ファイルの <managerType> のすべてのインスタンスを変更して、管理を有効または無効にします。
   - 管理を有効にする場合は、<managerType>**ProxyAgentServices**</managerType>。
   - 管理を無効にする場合は、<managerType>**NotManaged**</managerType>。

   ベスト・プラクティスは、変更したファイルの名前を **k*pc*.xml** (*pc* は 2 文字の製品コード) に変更することです。 KCA_CAP_DIR にあるすべての CAP ファイルは、エージェント管理サービスによって処理されます。2 つ以上の CAP ファイルが同じ「サブエージェント ID」を共有している場合、これらのファイルはソート順に処理されます。例えば、kca.xml は kca_default.xml の前に使用されます。また、CAP ファイルを k*pc*.xml に名前変更すると、将来のアップグレード時に変更が上書きされません。
3. 更新したファイルを保存します。
4. Watchdog プロセス (kcawd) の実行中に、更新した CAP ファイルを再度 KCA_CAP_DIR に移動またはコピーします。

タスクの結果

更新したエージェント管理サービス設定は、CAP ファイルが KCA_CAP_DIR に配置された後に処理されます。

専用シチュエーション

ローカル・エージェント環境またはイベント受信側には関連し、Tivoli Enterprise Monitoring 環境には関連しないモニター基準の専用シチュエーションおよび結果のイベントを定義します。専用シチュエーションは Tivoli Enterprise Monitoring Agent および Tivoli System Monitor Agent に定義できます。

専用シチュエーション操作

専用シチュエーションは、Tivoli Enterprise Monitoring Server と対話しない XML 形式のファイルで作成されます。専用シチュエーションを効果的に使用するには、専用シチュエーションとエンタープライズ・シチュエーションの違いを理解する必要があります。

Tivoli Management Services エージェント・フレームワーク

ローカルで実行され、Tivoli Enterprise Monitoring Agent または Tivoli System Monitor Agent がインストールされたコンピューター上でイベントをトリガーするシチュエーションを作成する機能が、Tivoli Management Services インフラストラクチャーのエージェント・フレームワーク内に組み込まれています。

エンタープライズ・シチュエーションおよび専用シチュエーション

エンタープライズ・シチュエーションは、Tivoli Enterprise Portal シチュエーション・エディターまたは CLI **tacmd createSit** コマンドで作成されます。 エンタープライズ・シチュエーションは、モニター・サーバーにイベントを送信し、ハブ・モニター・サーバーがイベントを転送するよう構成されている場合は、イベントを IBM Tivoli Enterprise Console イベント・サーバーや Netcool/OMNIbus Probe for Tivoli EIF などの Event Integration Facility 受信側に転送できます。エンタープライズ・シチュエーション・イベントは、Netcool/OMNIbus SNMP プローブ などの受信側に SNMP アラートとして送信することもできます

専用シチュエーション は、エージェントのローカル専用シチュエーションの構成 XML ファイルに作成されます。モニター対象エンタープライズからエクスポートされた適格なシチュエーション定義をファイルに追加してシチュエーションを作成することもできます。専用シチュエーションで生成されたイベントは、ワークステーションにローカルのまま維持することも、Netcool/OMNIbus SNMP プローブ などの受信側に SNMP アラートとして送信することもできます。専用シチュエーション構成ファイルは、エージェントの `localconfig/pc` ディレクトリーにあります。エージェントごとに 1 つのファイルがあり、そのエージェントのすべての専用シチュエーション定義が含まれます。

専用シチュエーションの作成

この Windows OS エージェント用の専用シチュエーション構成 XML ファイルの例には、2 つのシチュエーションが定義されています。シチュエーションは、手動でファイルに入力して作成することができます。

また、CLI **tacmd bulkExportSit** を使用して、既存のエンタープライズ・シチュエーションをモニター・サーバーからエクスポートした後、エクスポートしたシチュエーションのうち、専用シチュエーションとしての使用に適格なシチュエーション

を XML ファイルからエージェントの専用シチュエーション構成ファイルにコピーすると、このファイルにシチュエーションを作成できます。例にある (Disk_Queue という名前の) 最後のシチュエーションは、エクスポートされたシチュエーション XML ファイルから抽出されたものです。

```
<PRIVATECONFIGURATION>
  <PRIVATESIT>
   <SITUATION>NT_Missing_Scheduler_pr</SITUATION>
    <CRITERIA>
     <![CDATA[ *MISSING NT_Process.Process_Name *EQ ("schedule")]]>
    </CRITERIA>
    <INTERVAL>001000</INTERVAL>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>NT_Paging_File_Critical_pr</SITUATION>
    <CRITERIA>
     <![CDATA[ *VALUE NT_Paging_File.%_Usage *GE 80 ]]>
    </CRITERIA>
    <INTERVAL>001500</INTERVAL>
  </PRIVATESIT>
  <PRIVATESIT>
   <SITUATION>Disk_Queue</SITUATION>
    <PDT><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
    *GE 0.004 ]]></PDT>
    <REEV_TIME>003000</REEV_TIME>
  </PRIVATESIT>
</PRIVATECONFIGURATION>
```

この CRITERIA 要素には次の式が含まれます。

- ***VALUE** 関数名または ***MISSING** 関数名。専用シチュエーションで使用できる式関数は、 **式の値** および **欠落している項目がないか確認する**のみです。
- 次の場所に記述されている **attribute_group.attribute_name**。
  - <*install_dir*>/TMAITM6/ATTRLIB/*pc* ディレクトリーにあるエージェントの .atr ファイルの **name** 要素
  - `tacmd bulkExportSit` CLI コマンドで生成された <*situation_name*>.xml ファイル出力の **<PDT>** 要素
  - エージェント・サービス・インターフェースを介して生成されたシチュエーション・サマリー・レポートの **<PREDICATE>** 要素
  - エージェント・サービス・インターフェースを介して生成された照会レポートの属性定義部分にある「**Display**」列
- ブール演算子 ***EQ**、***LT**、***GT**、***NE**、***LE**、または ***GE**。
- *VALUE 関数では**しきい値**、*MISSING 関数ではコンマ区切りのリスト。
- AND または OR のブール論理で複数の式を結合できますが、両方は使用できません。また、式には 1 つの属性グループのみを使用できます。 AND では最大 9 個の式を結合でき、OR では最大 10 個の式を結合できます。
- XML コーディングは大/小文字を区別しませんが、テキスト属性値はデータ・サンプルと一致する必要があります。例えば、欠落プロセス `notepad` を `NOTEPAD` というスペルで指定した場合は無効です。

活動化

エージェントが初期化されると、XML パーサーは専用シチュエーション定義を調べ、検証します。 XML 構文解析エラー・メッセージは、すべてエージェント・オペレーション・ログに記録されます。 (『*IBM Tivoli Monitoring トラブルシューティング・ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/trouble/itm_trouble.htm)』を参照してください。)

エージェントがシャットダウンされるまで、専用シチュエーションは継続して実行されます。

SNMP トラップ構成ファイルが作成され、 Netcool/OMNIbus SNMP プローブ などの受信側がそれらを受信するように構成されている場合、シチュエーションが true になったときに開かれるイベントを SNMPv1/v2 トラップまたは SNMPv3 インフォームとして送信できます。また、EIF イベント構成ファイルが作成され、IBM Tivoli Enterprise Console イベント・サーバーまたは Netcool/OMNIbus Probe for Tivoli EIF がそれらを受信するように構成されている場合は、EIF イベントとして送信できます。同様に、エージェント・サービス・インターフェースは、シチュエーション・アクティビティーのサマリー・レポートを提供します。

*pc*_situations.xml という名前の専用シチュエーション・ファイルを作成して、*install_dir* /localconfig/*pc* に保存します (ここで、*pc* は製品コードです)。異なる名前を付けたり、異なるパスを使用したりする場合は、エージェント環境変数 IRA_PRIVATE_SITUATION_CONFIG および IRA_LOCALCONFIG_DIR を使用して、ファイル名およびパスを変更できます。

ローカルまたはリモートでの専用シチュエーションの配布

専用シチュエーションを編集または削除するには、それが定義されている構成 XML ファイルを変更し、ローカルまたはリモートでシチュエーションを再配布します。

ローカル配布

専用構成ファイルを編集して保存した後、エージェントを再起動して、専用シチュエーション定義を再ロードできます。

または、エージェント・サービス・インターフェース にログオンし、個々の専用シチュエーションを開始、停止、再開するための専用シチュエーション要求を入力できます。 443 ページの『エージェント・サービス・インターフェースの開始』 および 465 ページの『エージェント・サービス・インターフェース要求 - 専用シチュエーションの制御』 を参照してください。

リモート配布

構成ロード・リストを使用して、中央構成リポジトリーからプルし、アクティブ化するモニター・エージェントの専用構成ファイルを指定します。 473 ページの『第 16 章 一元化された構成』を参照してください。

要約

専用シチュエーションは、ローカル・エージェント環境に関連する基準を使用して、ローカル管理者によって定義されたエージェント・モニター要求です。これは専用シチュエーションの特性の要約です。

- 簡単なエディターを使用してエージェントでローカルに作成されます。
- エージェント SNMP トラップで結果およびイベントを発行します。
- モニター・サーバーとの接続にかかわらず、エージェントの開始時から停止時まで実行されます。
- 1 つの式内に複数の式が存在する場合、論理結合子は論理積 AND か論理和 OR のいずれかに統一する必要があります。1 つの式に 2 つの結合子を混在させることはできません。

- AND のブール論理で結合すると、シチュエーション式で最大 9 個の式を使用でき、OR のブール論理で結合すると、最大 10 個の式を使用できます。
- すべてのエンタープライズ・シチュエーションしきい値演算子 (等しい (EQ)、等しくない (NE)、より大 (GT)、より小 (LT)、以上 (GE)、および以下 (LE)) をサポートします。
- リフレックス・オートメーション・アクション・コマンドのサポートを含みます。
- VALUE 式関数および MISSING 式関数のみを使用できます。グループ関数またはその他のセル関数は使用できません。
- 専用シチュエーションまたはシチュエーションのオーバーライドでは、ワイルドカード文字はサポートされていません。
- 1 つのシチュエーションに使用できる属性は 1 つのみです。2 つの異なる属性グループの使用はサポートされていません。
- エージェントがモニター・サーバーに接続されている場合、エンタープライズ・シチュエーションと並行して実行されます。
- Tivoli Enterprise Monitoring Agent (接続済みまたはオートノマス) または Tivoli System Monitor Agent 上で実行できます。
- IBM Tivoli Monitoring 中央管理対象インフラストラクチャーに対して不明のままです。Tivoli Enterprise Monitoring Server およびその他の IBM Tivoli Monitoring コンポーネントはその存在を認識せず、そのモニター・データとイベントも認識しません。そのため、エージェントがモニター・サーバーから切断されている間、専用シチュエーションは、エージェントの再始動をまたいでイベント・キャッシュを実行したり永続性を保持することはありません。
- ベスト・プラクティスとして、エンタープライズ・シチュエーションおよび専用シチュエーションには、一意のシチュエーション名が必要です。

専用シチュエーション XML 指定

専用シチュエーション XML 指定の要素を使用して、ご使用のコンピューター上のエージェントの専用シチュエーションを作成します。

デフォルトの専用シチュエーション・パスおよびファイル名

Windows *install_dir* ¥localconfig¥*pc*¥*pc*_situations.xml

Linux UNIX *install_dir* /localconfig/*pc*/*pc*_situations.xml

z/OS RKANDATV データ・セット内の *PC*SICNFG

異なる名前を付けたり、異なるパスを使用したりする場合は、エージェント環境変数 IRA_PRIVATE_SITUATION_CONFIG および IRA_LOCALCONFIG_DIR を使用して、ファイル名およびパスを変更します。 362 ページの『専用シチュエーション』および 359 ページの『Tivoli Enterprise Monitoring Agent でのオートノミーの制御』を参照してください。

要素

XML タグは大/小文字を区別しません。他のすべてのパラメーターには大/小文字の区別があります。例えば、<PRIVATESIT>、<PrivateSit>、または <privatesit> を入力できます。

<PRIVATECONFIGURATION>

PRIVATECONFIGURATION は、エージェント専用シチュエーション構成文書としてこの XML を識別するルート要素です。

```
<PRIVATECONFIGURATION>
<PRIVATESIT>
<SITUATION NAME="Check_Process_CPU_Usage"  INTERVAL="000500" />
<CRITERIA>
<![CDATA[ *VALUE NT_Process.%_Processor_Time *GE 65 *AND
  *VALUE NT_Process.Priority_Base *NE 0 *AND
  *VALUE NT_Process.Process_Name *NE _Total]]>
</CRITERIA>
<CMD><![CDATA[netstat >.¥logs¥netstat.dat]]></CMD>
<AUTOSOPT When="N" Frequency="N" />
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

<PRIVATESIT>

各シチュエーション定義を PRIVATESIT の開始タグと終了タグで囲みます。

<SITUATION>

PRIVATESIT の開始タグと終了タグの各セット内に SITUATION の開始タグと終了タグのセットを追加します。 SITUATION の開始タグと終了タグの各セットの内側は、完全なシチュエーション定義です。次の属性を使用してシチュエーションを定義します。

NAME=

シチュエーション名。先頭が文字で、31 文字以下の文字、数字、およびアンダースコアー (_) で構成します (例えば「Missing_Process_Helper_Harmless」)。専用かエンタープライズかに関係なく、すべてのシチュエーションに固有の名前を付けるように注意してください。 そうしないと、あるシチュエーションで呼び出されたアクションが、同じ名前の他のシチュエーションに適用されます。

INTERVAL=

ピュア・イベント・シチュエーションでない場合、サンプリング間隔を HHMMSS 形式で指定します。デフォルト: **001500** (15 分)。または、<INTERVAL> 要素を使用します。

CRITERIA=

シチュエーション式。 または、<CRITERIA> 要素を使用します。

```
<SITUATION NAME="High_CPU_Usage" INTERVAL="000500"
CRITERIA="*VALUE NT_Process.%_Processor_Time *GE 65
*AND *VALUE NT_Process.Priority_Base *NE 0
*AND *VALUE NT_Process.Process_Name *NE _Total" />
```

DELETE=

オプションです。 NAME= 属性に指定されているシチュエーションを削除するには Y を指定します。エージェントのリサイクルやローカル専用シチュエーション XML ファイルの削除を行わずに、専用シチュエーションを動的に削除するには、この属性を使用します。指定した名前の専用シチュエーションが未定義であるか既に削除されている場合、アクションは実行されません。複数の削除ステートメントを指定できます。

専用シチュエーションを動的に更新するには、新しい追加ステートメントの*前* に削除ステートメントを挿入してください。専用シチュエーション XML ファイルでの指定順序は、最終的な運用専用シチュエーションの定義と構成に影響します。XML ファイルの読み取り順序は、一元化された構成のロード・リストで定義されており、アルファベット順ではありません。

1 つの専用シチュエーションを削除する例を以下に示します。

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_Name" delete="Y" />
</privatesit>
</privateconfiguration>
```

複数の専用シチュエーションを削除する例を以下に示します。

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_Name" delete="Y" />
</privatesit>
<privatesit>
  <situation name="Check_DiskSpace_Low" delete="Y" />
</privatesit>
</privateconfiguration>
```

最初にシチュエーションを削除してから同じシチュエーションを追加することで、専用シチュエーションを更新する例を以下に示します。

```
<privateconfiguration>
<privatesit>
  <situation name="Check_Process_CPU_Usage" delete="y" >
  </situation>
</privatesit>
<privatesit>
  <situation name="Check_Process_CPU_Usage" interval="000500" >
  </situation>
    <criteria>
    <![CDATA[*VALUE NT_Process_64.%_Processor_Time *GE 10 *AND
             *VALUE NT_Process_64.Priority_Base *NE 1 *AND
             *VALUE NT_Process_64.Process_Name *NE _Total]]>
      </criteria>
</privatesit>
</privateconfiguration>
```

<INTERVAL>

シチュエーションのサンプリング間隔を HHMMSS 形式で指定します。値 000000 (6 つのゼロ) は、ピュア・イベント・シチュエーションを示します。サンプル・イベント・シチュエーションでは、最小間隔は 000030 (30 秒) で、最大間隔は 235959 (23 時間 59 分 59 秒) です。 デフォルト: **001500** (15 分)。この要素は、SITUATION 要素内に INTERVAL 属性が指定されていない場合に必須です。

<CRITERIA>

シチュエーション基準は、この要素および <![CDATA[ ]]> 要素内で指定されます。各式は、3 つの部分で構成されており、最初に *VALUE または *MISSING とそれに続く **attribute-table-name.attribute-name** があり、その後に論理演算子 (*EQ など) が続き、属性しきい値 (または MISSING 関数

の場合はコンマ区切りの名前のリスト) が続きます。エンタープライズ・シチュエーション式の構文で行われるように、*IF から式を開始することは可能ですが、必須ではありません。

属性には、「属性テーブル名ドット属性名」の形式の詳細な属性名を使用します。製品属性ファイルは、エージェント製品属性テーブルおよび関連属性を定義します。例えば、**knt.atr** ファイルまたは **kux.atr** ファイルは配布済みエージェントのインストール済み環境の ATTRLIB ディレクトリーにあります。

属性名を検索する別の方法として、エージェント・サービス・インターフェースから表を照会できます。「ASI」>「照会」を開き、表の名前を選択します。ASI は、表の表示名とすべての表列の表示名を含む完全な表のスキーマを返します。

演算子は、フィルター値およびデータの論理演算を定義します。サポートされている演算子は、*EQ (等しい)、*NE (等しくない)、*GE (以上)、*LE (以下)、*LT (より小)、および *GT (より大) です。<CRITERIA> 要素内では、XML 構文解析から除外するために、コマンドは文字データ・タグで囲まれています。この例は、使用可能なディスク領域が 35% 以下になったときにアラートをトリガーする式を示しています。

```
<CRITERIA> <![CDATA[*VALUE NT_Logical_Disk.%_Free *LE 35]]> </CRITERIA>
```

複数の式の場合は、*AND 結合子または *OR 結合子を使用します。式の結合子はすべて同じ (すべて *AND またはすべて *OR) である必要があります。*AND 論理結合子および *OR 論理結合子の混在はサポートされていません。1 つの式では、*AND 結合子を最大で 9 個、または *OR 結合子を最大で 10 個使用できます。

複数の式を持つ数式では、*MISSING 式を複数指定することはできません。また、*MISSING 式は、数式内の最後の式である必要があり、*AND 結合子のみ使用できます (🔍 **「欠落している項目がないか確認する」**の説明については、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」を参照してください)。

ワイルドカードはサポートされていません。例えば、「S」で始まる全プロセスを検索する *VALUE NT_Process.Process_Name *EQ S* は、専用シチュエーションでは無効です。同様に、*MISSING リストでワイルドカード (NT_Process.Process_Name *EQ ('DB2*') など) を使用して、DB2. から始まるすべてのプロセスを検索することはできません。

例:

```
<CRITERIA>
<![CDATA[ *VALUE NT_Process.%_Processor_Time *GE 65 *AND
  *VALUE NT_Process.Priority_Base *NE 0 *AND
  *VALUE NT_Process.Process_Name *NE _Total]]>
</CRITERIA>

<CRITERIA>
<![CDATA[ *MISSING NT_Process.Process_Name *EQ ('schedule','notepad')]]>
</CRITERIA>

<CRITERIA>
<![CDATA[ *VALUE Linux_Process.State *NE Running *AND
*MISSING Linux_Process.Process_Command_Name *EQ ('MyHelp','myhelpw')]]>
</CRITERIA>
```

列挙型属性には、値の事前定義セットがあります。列挙シンボルまたは列挙名を指定できます。例えば、プロセス実行状態 Stopped (T) の式は両方とも有効です。 SNMP アラートが送信されたり、アクションが実行された場合、名前ではなくシンボルが使用されます。

```
<CRITERIA><![CDATA[ *VALUE Process.Execution_State *EQ Stopped]]></CRITERIA>
<CRITERIA><![CDATA[ *VALUE Process.Execution_State *EQ T]]></CRITERIA>
```

専用シチュエーションで位取り属性が使用されている場合は、適切な評価のためにこの属性の値を正規化する必要があります。位取り属性値は、小数点をどれだけ左に桁移動するかを指定するために使用します。例えば、55.255 はスケール 3 で表示する属性では有効な値です。この値を正規化するには、小数点を右に 3 つ桁移動して 55255 にします。

SCAL (スケール)	整数比較値 (例として 5000 を使用)
未定義 (0)	5000
1	500 または 500.0 と表示されるが、5000 を表す
2	50 または 50.00 と表示されるが、5000 を表す
3	5 または 5.000 と表示されるが、5000 を表す

製品の属性の説明トピックに、値が位取りされるかどうかが記載されています。配布済みエージェントの場合は、属性ファイルで属性定義の scal を確認することもできます。例えば、ウェアハウス・プロキシー・エージェントの khd.atr で、作業キューの挿入率属性が scal 2 になっていたりします。k*pc*.atr ファイルの場所は次のとおりです。 Windows <*install_dir*>¥TMAITM6¥ATTRLIB; Linux UNIX <*install_dir*>/platform/<pc>/tables/ATTRLIB。ここで、platform はオペレーティング・システムで、pc は製品コードです。

以下の例は、比較値として 16 進整数を示しています。

```
<CRITERIA><![CDATA[ *VALUE Disk.Mount_Point_U *EQ '/opt' *AND
*VALUE Disk.Space_Used_64 *GT 0x80000000 ]]></CRITERIA>
```

<CRITERIA> 要素は、<SITUATION> 要素内に CRITERIA が指定されていない場合に必須です。

***REGEX**

IBM Tivoli Monitoring では、イベントとサンプル・データ (名前、アドレス、メッセージ、およびログ・レコードなど) におけるテキスト・スキャンとパターン・マッチングが必要なことがよくあります。正規表現述部フィルター関数を追加して、エージェント・モニターの機能性と適用可能性を強化できます。*REGEX 述部関数の指定構文は次のように定義されています。

*REGEX *attribute_name operator "Regular Expression"*

ここで、

attribute_name は選択フィルターの完全修飾属性名です。

operator はフィルター値およびデータの論理演算子です。サポートされている演算子は、*EQ (値が同等) および *NE (値が同等ではない) です。

" " は正規表現の区切り文字です。式で " を使用する必要がある場合は、他の文字 (@ @ など) を区切り文字として使用できます。例えば *REGEX *attribute_name operator @Regular Expression@* です。

Regular Expression は使用する正規表現定義を指定します。

*REGEX 述部関数の使用例を以下に示します。この例では、企業 ABC は私書箱には配送できないため、ユーザー入力で私書箱情報を調べ、私書箱情報がある場合はイベントを発生させます。

```
<privateconfiguration>
<privatesit>
<SITUATION NAME="Check_Valid_Address" INTERVAL="000030" >
 </SITUATION>
<criteria>
<![CDATA[*REGEX ABCCUSTOMER_PROFILE00.Address
  *EQ "(?:Post (?:Office )?|P[. ]?O¥.? )?[Bb]ox¥b"]]>
</criteria>
<DISTRIBUTION>ICVR5A05:ABC00</DISTRIBUTION>
</privatesit>
</privateconfiguration>
```

*REGEX 述部関数は、次の例に示すように他の述部関数と組み合わせて使用できます。

```
<privateconfiguration>
<privatesit>
<Situation Name="Check_Valid_Address" Interval="000030" />
<criteria>
<![CDATA[*VALUE ABCCUSTOMER_PROFILE00.Weight  *GE 5 *AND
  *REGEX ABCCUSTOMER_PROFILE00.Address
  *EQ $(?:Post (?:Office )?|P[. ]?O¥.? )?Box¥b$ ]]>
</criteria>
<Distribution>ICVR5A05:ABC00</Distribution>
</privatesit>
</privateconfiguration>
```

一般的な規則として *REGEX はデータ行ストレージ・バッファーのアプリケーション列データをフィルタリングします。したがって、列データの開始または終わりでマッチングを実行する場合、入力の始め (^ または ¥A) または行末 ($ または ¥Z) アンカーは適用されず、不要です。

使用上の注意:

- 正規表現の述部では整数属性はサポートされていません。
- 正規表現の述部では列挙型属性がサポートされていますが、正規表現自体の作成時には実際の列属性値を使用する必要があります。正規表現自体の自動変更を必要とする、正規表現での列挙値の置換はサポートされていません。

  例えば、Local_Time 表の Day_Of_Week 属性には、列挙型文字ストリング値 (Sunday、 Monday、 Tuesday、 Wednesday、 Thursday、 Friday、 Saturday) と、実際の列値 (00、01、02、03、04、05、06) があります。正規表現の作成時には実際の列値を使用する必要があります。

- サポートされていないデータ型 (整数、64ビット整数、整数列挙型、16 進数ストリングなど) の属性が含まれている正規表現はエラーとしてフラグが設定され、専用シチュエーション定義が拒否されます。

正規表現の実装は、サポート・エンジンによって多少異なります。専用シチュエーション *REGEX 述部フィルター関数は、ICU 正規表現エンジンとその仕様を利用します。詳しくは、「*ICU User Guide*」を参照してください。

<CMD>

オプションです。 シチュエーション基準が true の場合に呼び出すアクション・コマンドまたはアクション・スクリプトを定義します。 <CMD> 要素内では、構文解析から除外するために、コマンドは文字データ・タグで囲まれています。この例は、シチュエーションが true になったときに、エージェントのメッセージ・ボックス内にタイム・スタンプを表示するシステム・コマンドを示しています。 CDATA タグ付けを行わないと、アンパーサンド (&) およびブラケット ({}) は XML パーサーでエラーと見なされます。

```
<CMD>
<![CDATA[ net send &{Local_Time.Timestamp}  ]]>
</CMD>
```

<AUTOSOPT>

アクション <CMD> が指定されている場合に必須です。アクション・コマンドの実行オプション WHEN (X)、FREQUENCY (Y)、WHERE (Z) を定義します。デフォルトは NNN です。

WHEN= オプション。項目ごとにコマンドを実行する場合は「Y」、シチュエーション基準に合う返されたデータの最初の列でのみコマンドを実行する場合は「N」を指定します。属性グループが複数行のデータを戻し、さらに複数の行が条件を満たした場合、基準を満たす最初の行でのみコマンドを実行するか、基準を満たしている行ごとに 1 回ずつコマンドを実行するかを選択できます。 デフォルトは「**N**」です。

FREQUENCY= オプション。シチュエーションが true に評価されるたびにコマンドを実行する場合は「Y」、シチュエーションが true の場合にはコマンドを実行し、シチュエーションが false に評価された後で true の評価に戻るまで再度実行しない場合は「N」を指定します。デフォルトは「**N**」です。

WHERE= エージェントでコマンドを実行する場合は「N」を指定します。デフォルトは「**N**」です。「where」に指定できる設定は 1 つのみであるため、この設定を AUTOSOPT 要素に含める必要はありません。

```
<AUTOSOPT When="Y" Frequency="Y" />
```

<DISTRIBUTION>

サブノード (サブエージェント) を持つ製品では必須です。管理対象システム名またはセミコロン (;) で区切られた管理対象システム名のリストを指定します。デフォルト値はありません。

<HISTORY> タグを使用する場合は、<HISTORY> の中に <DISTRIBUTION> をネストします。

<LSTDATE>

オプションです。 シチュエーションの最終更新日のタイム・スタンプです。この要素が指定されていない場合、現行データ・タイムが自動的に生成されます。形式は、CYYMMDDHHMMSSmmm (2010 年 7 月 15 日 07:45:01 の場合は 1100715074501000) になります。各部の内容は以下のとおりです。

C = 世紀 (21 世紀の場合 1)

Y = 年

M = 月

D = 日

H = 時

M = 分

S = 秒

m = ミリ秒

<LSTUSRPRF>

オプションです。 このシチュエーション定義を最後に更新したユーザーの ID です。この要素が指定されていない場合、現行ログオン・ユーザー ID が使用されます。以下に例を示します。

```
<LSTUSRPRF>SYSADMIN</LSTUSRPRF>
```

<LSTRELEASE>

オプションです。 シチュエーション・バージョンを指定します。以下に例を示します。

```
<LSTRELEASE>V622</LSTRELEASE>
```

<SITINFO>

オプションです。 EIF イベントのシチュエーション修飾子を定義します。`<![CDATA[ ]]>` 要素で囲みます。または、パラメーターを使用して EIF イベントの修飾子を定義します。複数の修飾子は、セミコロン (;) で区切られます。

ATOM= オプション。複数行の属性グループ用。これは表示項目として使用するカタログ COLUMN の名前です。これにより、同じ表示項目値を持つ行のサブセットごとにイベントが生成されます。

COUNT= オプション。これは、Tivoli Enterprise Portal で「シチュエーションの永続性」と呼ばれています。イベントがオープンされるまでシチュエーションが true になっている必要のある間隔の数を指定します。

SEV= オプション。EIF イベントに割り当てられろ重大度: 致命的、クリティカル、注意、マイナー、安全、通知、または不明。

TFWD=[Y|N] オプション。デフォルトは **Y** です。SNMP アラートのみを送信し、EIF イベントは送信しない場合は、この属性を **N** に設定します。

TDST= オプション。イベントの送信先として 1 つ以上の EIF 受信側の宛先を指定します。最大 5 個の有効な宛先サーバー ID を入力でき、それぞれをコンマ (,) で区切ります。有効な宛先は、`pc_eventdest.xml` ファイルで定義します。TDST パラメーターを指定していない場合、EIF

イベントはイベント宛先構成ファイルに定義されているすべてのデフォルトのイベント宛先 (default="Y" に設定されている宛先項目) に送信されます。

例:

```
<SITINFO><![CDATA[SEV=Fatal;~;]]></SITINFO>
<SITINFO><![CDATA[SEV=Critical;TFWD=Y;TDST=1,3;]]></SITINFO>
```

<HISTORY>

オプションです。 ヒストリー要素を使用して、ヒストリカル・データの収集対象となる各属性グループを指定します。エージェントは、1 つの TABLE に対する複数の <HISTORY> 指定をサポートしません。

TABLE= 必須。このパラメーターは、アプリケーション属性グループ名を指定します。

EXPORT= オプション。このパラメーターは、Tivoli Data Warehouse へのヒストリカル・データのエクスポート間隔を分単位で指定します。最小エクスポート間隔は 15 分、最大エクスポート間隔は 1440 (24 時間) です。有効なエクスポート間隔は 15、30、および 60 で割り切れる値です。60 より大きい間隔は、最大 1440 までの 120、180、240 などの値です。また、エクスポート間隔は INTERVAL パラメーターの値でも割り切れる必要があります。無効な値を入力すると、指定された属性グループのヒストリカル・データは収集およびエクスポートされません。デフォルトは **none** です。

INTERVAL= オプション。このパラメーターは、ヒストリカル・データ収集間隔を分単位で指定します。最小収集間隔は 1 分であり、最大収集間隔は 1440 分 (24 時間) です。有効な間隔は 60 に等分できる値、または 60 で割り切れる値です。60 より小さい間隔は、1、2、3、4、5、6、10、12、15、20、および 30 です。60 より大きい間隔は、120、180、240、と続き 1440 までです。無効な値を入力すると、指定された属性グループのヒストリーは収集されません。デフォルトは「**15**」です。

RETAIN= オプション。RETAIN は、ヒストリー・データの短期保存期間を時間単位で定義します。デフォルトは 24 時間であり、最小保存期間は 1 時間です。コンピューターのストレージ・スペースによる制約がない限り、保存期間に上限はありません。保存限度に達した後は、新しいサンプルが到着すると一番古いデータ・サンプルが削除されます。デフォルトは「**24**」です。

重要: 専用シチュエーションでは、外部名 (表示名と同じ) のみを使用します。専用シチュエーションで内部名を使用すると、障害が発生します。

例:

Windows OS エージェントは、ヒストリー・ファイルに NT_System 表データを 15 分ごとに収集し、96 データ行を維持します (1 時間に 4 回ずつ、24 時間)。

```
<HISTORY TABLE="NT_System" />
```

UNIX OS エージェントは、システム表データを 5 分ごとに収集し、3 日分の短期ヒストリーを維持します。

```
<HISTORY TABLE="System" Interval="5" RETAIN="72"  />
```

Windows OS エージェントは、NT_Logical_Disk 表データを毎分収集します。

```
<HISTORY TABLE="NT_Logical_Disk" INTERVAL="1"  />
```

サブノード環境には <DISTRIBUTION> 要素が必要です。例えば、Universal Agent は、TS2TCPIOQ00 表データを 10 分ごとに収集し、SYSGTCPIOQ:TS200 というサブノードに 1 日分の短期ヒストリーを維持します。

```
<HISTORY TABLE="TS2TCPIOQ00" INTERVAL="10" RETAIN="24" >
<DISTRIBUTION>SYSGTCPIOQ:TS200</DISTRIBUTION>
</HISTORY>
```

Linux OS エージェントは、5 分おきに KLZ_Disk 表データを収集し、15 分おきにデータをエクスポートします。

```
<HISTORY TABLE="KLZ_Disk" INTERVAL="5" EXPORT="15" />
```

<WAREHOUSE>

オプションです。 WAREHOUSE エレメントを使用して、ヒストリカル・データのエクスポート先のWarehouse Proxy agentの場所を指定します。エージェントでは複数の <WAREHOUSE> の指定はサポートされていません。

LOCATION=

このパラメーターは、ヒストリカル・データのエクスポート先の各 Warehouse Proxy agent の場所を指定します。1 つの 1 次ロケーションと複数の 2 次ロケーションを、セミコロン (:) で区切って指定できます。このロケーションは、エージェントで完全なオートノミーが構成されており、かつ KHD_WAREHOUSE_LOCATION パラメーターが指定されていない場合に限り、エージェントによって使用されます。

エージェントから Tivoli Data Warehouse へヒストリカル・データを転送するWarehouse Proxy agentの登録された listen アドレス を指定します。構文は *family protocol:network address[port number]* です。ウェアハウス・プロキシー・エージェントの RAS1 トレース・ログを参照し、登録されたアドレスを確認します。

以下の RAS1 ログの例には、listen アドレスを登録しているウェアハウス・プロキシー・エージェントが示されています。

```
khdxrpcr.cpp,621,"register_interface") Registering
   "Candle_Warehouse_Proxy": ip.pipe:#9.44.255.253 [63358]
```

注: ヒストリカル・データを適切にエクスポートできるようにするため、モニター・エージェントでは、ウェアハウス・プロキシーのロケーションに対して指定された通信プロトコルと同じ通信プロトコルが必要です。KDC_FAMILIES_OVERRIDE パラメーターについて詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*の『システム・モニター・エージェントによるオペレーティング・システムのモニター』」を参照してください。

例:

```
<WAREHOUSE LOCATION="ip.pipe:DEPT-XP[63358]" />
<WAREHOUSE LOCATION="ip.pipe:#9.44.255.253[63358]" />
```

エクスポートされたエンタープライズ・シチュエーション XML 指定

エージェントの専用シチュエーション構成ファイルに設定を取り込むには、CLI コマンド **tacmd bulkExportSit** および **tacmd viewSit** から生成される *situation_name*.xml ファイルのシチュエーション定義を使用します。

tacmd 構文と例については、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

Tivoli Enterprise Monitoring Agent 用のエンタープライズ・シチュエーションが既にある場合は、シチュエーションの一括エクスポート・コマンドまたはシチュエーション表示コマンドを実行して、指定したエージェントのシチュエーション定義を、専用シチュエーション構成ファイルに使用できる XML 形式で取得することができます。エクスポートしたすべてのシチュエーションが有効であるとは限りません。*VALUE 式関数または *MISSING 式関数を使用しているシチュエーションのみが有効です。その他の制限については、365 ページの『シチュエーション制限』を参照してください。

要素

XML タグは大/小文字を区別しません。他のすべてのパラメーターには大/小文字の区別があります。例えば、<SITNAME>、<SitName>、または <sitname> と入力できます。

<TABLE>

これは、エクスポートされたシチュエーション XML ファイルのルート要素です。専用シチュエーション構成ファイルでは、エクスポートされたシチュエーションの TABLE タグ (およびそのタグの間にあるものすべて) が専用シチュエーション定義として処理されます。

<ROW>

TABLE の子要素です。

<SITNAME>

モニター・シチュエーション名。シチュエーション名は、先頭が文字である必要があり、31 文字以下の文字、数字、およびアンダースコアー (_) で構成します。 SITNAME の開始タグと終了タグの各セットの内側は完全なシチュエーション定義です。例:

```
<SITNAME>Free_DiskSpace_Low</SITNAME>
```

専用かエンタープライズかに関係なく、すべてのシチュエーションに固有の名前を付けるように注意してください。 そうしないと、あるシチュエーションで呼び出されたアクションが、同じ名前の他のシチュエーションに適用されます。

<PDT>

シチュエーション基準は、<PDT> 述部要素および <![CDATA[ ]]> 要素内で指定されます。各式は、3 つの部分で構成されており、最初に *IF *VALUE または *IF *MISSING とそれに続く **attribute-table-name.attribute-name** があり、その後に論理演算子 (*NE など) が続き、属

性しきい値 (MISSING 関数の場合はコンマ区切りリスト) が続きます。エクスポートされたエンタープライズ・シチュエーションは常に *IF で始まっており、これは許容されていますが、必ずしも式に *IF を含める必要はありません。

属性には、「属性テーブル名.(ドット) 属性名」の形式の詳細な属性名を使用します。製品属性ファイルは、エージェント製品属性テーブルおよび関連属性を定義します。例えば、**knt.atr** ファイルまたは **kux.atr** ファイルは配布済みエージェントのインストール済み環境の ATTRIB ディレクトリーにあります。

演算子は、フィルター値およびデータの論理演算を定義します。サポートされている演算子は、*EQ (等しい)、*NE (等しくない)、*GE (以上)、*LE (以下)、*LT (より小)、および *GT (より大) です。<PDT> 要素内では、XML 構文解析から除外するために、コマンドが文字データ・タグで囲まれています。この例は、使用可能なディスク領域が 35% 以下になったときにアラートをトリガーする式を示しています。

```
<PDT> <![CDATA[*IF *VALUE NT_Logical_Disk.%_Free *LE 35]]> </PDT>
```

複数の式の場合は、*AND 結合子および *OR 結合子を使用します。式の結合子はすべて同じ (すべて *AND またはすべて *OR) である必要があります。論理結合子 *AND および *OR の混在はサポートされていません。例:

```
<PDT> <![CDATA[*IF *VALUE NT_Process.%_Processor_Time *GE 65 *AND
*VALUE NT_Process.Priority_Base *NE 0 *AND
*VALUE NT_Process.Process_Name *NE _Total]]> </PDT>
```

専用シチュエーションではワイルドカードはサポートされていません。例えば、「DB2」で始まる全プロセスを検索する *VALUE NT_Process.Process_Name *EQ DB2* は無効です。位取り属性を持つエクスポートされたエンタープライズ・シチュエーションは、専用シチュエーションとして実行されている場合は正規化されません。手動で値を正規化する必要があります。例えば、エンタープライズ・シチュエーション式 `Avg Disk Queue Length >= 0.004` が、スケール 3 の浮動小数点属性用であるとします。**tacmd viewSit** コマンドを使用してシチュエーションがエクスポートされるときに、以下のエクスポート・モニター基準が示されます。

```
<PDT>  <![CDATA[*IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 0.004]]> < PDT>
```

これと同じサンプル定義が専用シチュエーションで指定されると、値の比較値がゼロ値として解釈されます。

```
<PRIVATECONFIGURATION>
<PRIVATESIT>
<SITUATION>SCALE_TEST</SITUATION>
<CRITERIA><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 0.004 ]]></CRITERIA>
<INTERVAL>000030</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

小数点を右に 3 つ桁移動して値を正規化します。0.004 が 4 または以下に示すような値になります。

```
<CRITERIA><![CDATA[ *IF *VALUE NT_Physical_Disk.Avg_Disk_Queue_Length
*GE 4.123 ]]></CRITERIA>
```

<CMD>

オプションです。 シチュエーションが true の場合に呼び出すアクション・コマンドまたはアクション・スクリプトを定義します。このコマンドは <![CDATA[ ]]> セクションで囲みます。例:

```
<CMD><![CDATA[netstat >.¥logs¥netstat.dat]]></CMD>
```

<AUTOSOPT>

アクション・コマンド <CMD> が指定されている場合に必須です。開始タグと終了タグの間にリフレックス・オートメーション・アクション・コマンド実行オプションを XYZ の順に定義します。デフォルトは NNN です。

- **最初の項目のみでアクションを実行**
- **続けて 2 回アクションを実行しないでください (シチュエーションが false になり、次にもう一度 true になるまで待ってください)**
- **管理対象システム (エージェント) でアクションを実行する**

X=Y 項目ごとにコマンドを実行します。

X=N 最初の項目でのみコマンドを実行します。

Y=Y 各サンプル間隔のコマンドを実行します。

Y=N 続けて 2 回コマンドを実行しないでください。

Z=N 専用シチュエーションでは常に N に設定され、コマンドをエージェントで実行することを意味します。エクスポートされたオプションが Y に設定されている場合、設定は無視され、N として扱われます。

<DISTRIBUTION>

サブノード (サブエージェント) を持つ製品では必須です。管理対象システムの名前またはコンマ (,) で区切られた複数の管理対象システムの名前を指定します。デフォルトは、エージェント管理対象システム名またはすべての既知のサブエージェントです。管理対象システム・グループは、アスタリスク (*) が前に付いた事前定義の管理対象システム・グループを含め、サポートされていません。

<LSTCCSID>

オプションです。 IBM コード化文字セット ID を指定します。許可されている値は、**en_US** のみです。

<LSTDATE>

オプションです。 シチュエーションの最終更新日のタイム・スタンプです。この要素が指定されていない場合、現行データ・タイムが自動的に生成されます。形式は、CYYMMDDHHMMSSmmm (2009 年 7 月 15 日 07:45:01 の場合は 1090715074501000) になります。各部の内容は以下のとおりです。

C = 世紀 (21 世紀の場合 1)

Y = 年

M = 月

D = 日

H = 時

M = 分

S = 秒

m = ミリ秒

<LSTRELEASE>

オプションです。 シチュエーション・バージョンを指定します。

<LSTUSRPRF>

オプションです。 このシチュエーション定義を最後に更新したユーザーの ID です。この要素が指定されていない場合、現行ログオン・ユーザー ID が使用されます。

<SITINFO>

オプションです。 EIF イベントのシチュエーション修飾子を定義します。 <SITINFO> 要素内で、シチュエーション式を <![CDATA[ ]]> タグで囲みます (<![CDATA[SEV=Critical]]> など)。または、パラメーターを使用して修飾子を定義します。複数の修飾子は、セミコロン (;) で区切られます。

ATOM= オプション。複数行の属性グループ用。これは表示項目として使用するカタログ COLUMN の名前です。これにより、同じ表示項目値を持つ行のサブセットごとにイベントが生成されます。

COUNT= オプション。これは、Tivoli Enterprise Portal で「シチュエーションの永続性」と呼ばれています。イベントがオープンされるまでシチュエーションが true になっている必要のある間隔の数を指定します。

SEV= オプション。EIF イベントに割り当てられろ重大度: 致命的、クリティカル、注意、マイナー、安全、通知、または不明。

TFWD=[Y|N] オプション。デフォルトは **Y** です。SNMP アラートのみを送信し、EIF イベントは送信しない場合は、この属性を **N** に設定します。

TDST= オプション。イベントの送信先として 1 つ以上の EIF 受信側の宛先を指定します。最大 5 個の有効な宛先サーバー ID を入力でき、それぞれをコンマ (,) で区切ります。有効な宛先は、pc_eventdest.xml ファイルで定義します。TDST パラメーターを指定していない場合、EIF イベントはイベント宛先構成ファイルに定義されているすべてのデフォルトのイベント宛先 (default="Y" に設定されている宛先項目) に送信されます。

<TEXT>

シチュエーションの説明。<TEXT> 要素内で、シチュエーション式を <![CDATA[ ]]> タグで囲みます。

<REEV_TIME>

シチュエーションのサンプリング間隔を HHMMSS 形式で指定します。値 0 (ゼロ) は、ピュア・イベント・シチュエーションを示します。デフォルトの間隔は 15 分 (001500) です。最小は 30 秒 (000030) であり、最大は 23 時間 59 分 59 秒 (235959) です。例:

```
<REEV_TIME>000500</REEV_TIME>
```

無視される要素

エクスポートされる XML 仕様の以下の要素は、使用することが注記されていない限り使用されません。

<FULLNAME> (EIF 用に処理されます)

<ADVISE>
<AFFINITIES>
<ALERTLIST>
<AUTOSTART>
<DESTNODE />
<HUB />
<LOCFLAG />
<NOTIFYARGS>
<NOTIFYOPTS>
<OBJECTLOCK>
<PRNAMES>
<QIBSCOPE>
<REEV_DAYS> (1 日を超えるとサポートされません)
<REFLEXOK>
<SENDMSGQ>
<SITINFO> (EIF 用に処理されます)
<SOURCE>

エクスポートされたエンタープライズ・シチュエーションの例

tacmd bulkExportSit または **tacmd viewSit** でエクスポートされた NT_System_File_Critical シチュエーションは NT_System_File_Critical.xml ファイルに保存されます。

```
<TABLE>
 <ROW>
  <SITNAME>NT_System_File_Critical</SITNAME>
  <FULLNAME>
    <![CDATA[ ]]>
  </FULLNAME>
  <ADVISE>
   <![CDATA[ ADVICE("knt:"+$ISITSTSH.SITNAME$);]]>
  </ADVISE>
  <AFFINITIES>%IBM.STATIC021 01000000000</AFFINITIES>
  <ALERTLIST>*NO</ALERTLIST>
  <AUTOSOPT>NNN</AUTOSOPT>
  <AUTOSTART>*YES</AUTOSTART>
  <CMD>
   <![CDATA[ *NONE  ]]>
  </CMD>
  <DESTNODE />
  <HUB />
  <LOCFLAG />
  <LSTCCSID />
  <LSTDATE>0961009010101000</LSTDATE>
  <LSTRELEASE />
  <LSTUSRPRF>IBM</LSTUSRPRF>
  <NOTIFYARGS />
  <NOTIFYOPTS />
  <OBJECTLOCK />
  <PDT>
    <![CDATA[ *IF *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </PDT>
  <PRNAMES />
  <QIBSCOPE>E</QIBSCOPE>
```

```
  <REEV_DAYS>0</REEV_DAYS>
  <REEV_TIME>001500</REEV_TIME>
  <REFLEXOK />
  <SENDMSGQ>*NONE</SENDMSGQ>
  <SITINFO>
   <![CDATA[ SEV=Critical ]]>
  </SITINFO>
  <SOURCE />
  <TEXT>
   <![CDATA[ Knt:KNT1359 ]]>
  </TEXT>
  <DISTRIBUTION>*NT_SYSTEM</DISTRIBUTION>
 </ROW>
</TABLE>
```

専用シチュエーション構成ファイル内で、<PRIVATESIT> タグと </PRIVATESIT> タグの組が作成され、次にタグの内側に NT_System_File_Critical.xml の内容が貼り付けられます。これは、エクスポートされた NT_System_File_Critical シチュエーション定義を Check_Process_CPU_Usage という別の専用シチュエーション定義の上に追加した後の nt_situations.xml 専用シチュエーション構成ファイルです。冗長な要素 (上述の『無視される要素』を参照) および使用されない要素 (AUTOSOPT および CMD、LSTCCSID、LSTRELEASE、DISTRIBUTION) はエクスポートされたシチュエーションから削除されますが、ファイル内に冗長な要素が残っていても XML パーサーはそれらを無視するため実際は問題ありません。

```
<PRIVATECONFIGURATION>
<TABLE>
 <ROW>
  <SITNAME>NT_System_File_Critical</SITNAME>
  <LSTDATE>09610090101010000</LSTDATE>
  <LSTUSRPRF>IBM</LSTUSRPRF>
  <PDT>
   <![CDATA[ *IF *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </PDT>
  <REEV_TIME>001500</REEV_TIME>
  <SITINFO>
   <![CDATA[ SEV=Critical ]]>
  </SITINFO>
  <TEXT>
   <![CDATA[ Knt:KNT1359 ]]>
  </TEXT>
  </ROW>
</TABLE>
<PRIVATESIT>
  <SITNAME>Check_Process_CPU_Usage</SITNAME>
  <PDT>
   <![CDATA[ *IF *VALUE NT_Process.%_Processor_Time *GE 65 *AND
   *VALUE NT_Process.Priority_Base *NE 0 *AND
   *VALUE NT_Process.Process_Name *NE _Total]]>
  </PDT>
  <REEV_TIME>000300</REEV_TIME>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

ヒント: エクスポートされた各シチュエーションには専用の XML ファイルが用意されます。専用シチュエーションが最初にエンタープライズ・シチュエーションのエクスポートから生成される場合は、PRIVATECONFIGURATION の開始タグと終了タグを指定して XML を作成し、含める必要があるシチュエーションごとに、TABLE の開始タグと終了タグおよびその内側にあるものすべてをファイルに貼り付けます。エクスポートされたシチュエーションでは、TABLE タグは PRIVATESIT タグと等価です。

専用シチュエーションの例

ローカル・エージェント環境に関連し、エンタープライズ環境に依存または関連しないモニター基準の専用シチュエーションを定義します。以下の例は、専用シチュエーションのテンプレートとして使用できます。

ヒント: Tivoli Monitoring Agent のインストール・メディアの PrivateConfigSamples ディレクトリーに専用シチュエーション構成ファイルのサンプルが提供されています。

Linux OS lz_situations.xml

```
<PRIVATECONFIGURATION>
<!--  Situation Description: Percentage of time the processor is busy
is extremely high -->
<PRIVATESIT>
  <SITUATION>Linux_High_CPU_Overload_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_CPU.Idle_CPU *LT 10  *AND  *VALUE Linux_CPU.CPU_ID
   *EQ Aggregate ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
  </PRIVATESIT>
<!-- Situation Description: Percentage of packet collisions during data
transmission is high -->
<PRIVATESIT>
  <SITUATION>Linux_High_Packet_Collisons_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Network.Collision_Percent *GT 10 ]]>
  </CRITERIA>
  <INTERVAL>000500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of available i-nodes is low -->
<PRIVATESIT>
  <SITUATION>Linux_Low_Pct_Inodes_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Disk.Inodes_Used_Percent *GT 80 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of space available on a filesystem
is low -->
<PRIVATESIT>
  <SITUATION>Linux_Low_Pct_Space_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Disk.Space_Available_Percent *LT 15 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Tests if the SSH Daemon, sshd, is up running -->
<PRIVATESIT>
  <SITUATION>Linux_Process_Missing_sshd_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *MISSING Linux_Process.Process_Command_Name
   *EQ ("/usr/sbin/sshd") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Percentage of Processor time used by
a process high -->
<PRIVATESIT>
  <SITUATION>Linux_Process_High_CPU_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Process.Busy_CPU_Pct *GT 60 ]]>
  </CRITERIA>
```

```
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: High number of stopped processes on this system -->
<PRIVATESIT>
  <SITUATION>Linux_Process_Stopped_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_Process.State *NE Running  *AND
   *VALUE Linux_Process.State *NE Sleeping  *AND
   *VALUE Linux_Process.State *NE Disk  *AND
   *VALUE Linux_Process.State *NE Trace ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of rejected RPC server or
client calls is high -->
<PRIVATESIT>
  <SITUATION>Linux_RPC_Bad_Calls_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_RPC_Statistics.RPC_Client_Calls_Retransmitted *GT 30
   *OR  *VALUE Linux_RPC_Statistics.RPC_Server_Calls_Rejected *GT 30 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: The swap space paging activity on this system
is extremely high  -->
<PRIVATESIT>
  <SITUATION>Linux_System_Thrashing_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE Linux_System_Statistics.Pages_paged_out_per_sec *GT 400
   *OR  *VALUE Linux_System_Statistics.Pages_paged_in_per_sec *GT 400 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

UNIX OS ux_situations.xml

```
<PRIVATECONFIGURATION>
<!--  Situation Description: Reports High CPU processes  -->
<PRIVATESIT>
  <SITUATION>UNIX_CMD_Runaway_Process_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *VALUE Process.CPU_Utilization *GT 95 ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Process CPU utilization is greater than
or equal to 85% -->
<PRIVATESIT>
  <SITUATION>UNIX_CPU_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *IF *VALUE Process.CPU_Utilization *GE 85 *AND *VALUE
   Process.Command *NE kproc *AND *VALUE Process.Command *NE swapper ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Notes typical I/O bound processor (NFS) -->
<PRIVATESIT>
  <SITUATION>UNIX_HD_Exces_IO_Wait_prv</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE System.Wait_I/O *GT 20  ]]>
  </CRITERIA>
  <INTERVAL>000200</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Tests if the Internet Services Daemon, inetd,
is up running -->
<PRIVATESIT>
```

```
  <SITUATION>UNIX_Process_Missing_inetd_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *MISSING Process.Command *EQ  ("/usr/sbin/inetd") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Checks the System CPU, Idle, I/O Wait,
and Load Averages for the Busy state  -->
<PRIVATESIT>
  <SITUATION>UNIX_System_Busy_Warning_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE System.System_CPU *GT 50 *AND
   *VALUE System.Idle_CPU *GT 0 *AND *VALUE System.Wait_I/O *GT 0 *AND
   *VALUE System.Load_Average_5_Min *GT 1 ]]>
  </CRITERIA>
  <INTERVAL>000200</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Windows OS nt_situations.xml

```
<PRIVATECONFIGURATION>
<!--  Situation Description: One of the NT Logs is close to capacity  -->
<PRIVATESIT>
  <SITUATION>NT_Log_Space_Low_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Monitored_Logs_Report.%_Usage *GE 95 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!-- Situation Description: Test if the NT Scheduler process is running -->
<PRIVATESIT>
  <SITUATION>NT_Missing_Scheduler_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *MISSING NT_Process.Process_Name *EQ ("schedule") ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the Page File in use is too high -->
<PRIVATESIT>
  <SITUATION>NT_Paging_File_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Paging_File.%_Usage *GE 80 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the Page File in use is rising  -->
<PRIVATESIT>
  <SITUATION>NT_Paging_File_Warning_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Paging_File.%_Usage *GE 75 *AND
   *VALUE NT_Paging_File.%_Usage *LT 80  ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the time the disk drive is busy
is too high -->
<PRIVATESIT>
  <SITUATION>NT_Phys_Disk_Busy_Crit_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Physical_Disk.%_Disk_Time *GT 90 *AND
   *VALUE NT_Physical_Disk.Disk_Name *NE _Total ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percent of the time the disk drive is busy
is rising  -->
```

```
<PRIVATESIT>
  <SITUATION>NT_Phys_Disk_Busy_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Physical_Disk.%_Disk_Time *GT 80 *AND
   *VALUE NT_Physical_Disk.%_Disk_Time *LE 90 *AND
   *VALUE NT_Physical_Disk.Disk_Name *NE _Total  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of processor time used is too high  -->
<PRIVATESIT>
  <SITUATION>NT_Proc_CPU_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Process.%_Processor_Time *GE 65 *AND *VALUE
   NT_Process.Priority_Base *NE 0 *AND *VALUE NT_Process.Process_Name
   *NE _Total  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Percentage of processor time used is high  -->
<PRIVATESIT>
  <SITUATION>NT_Proc_CPU_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Process.%_Processor_Time *GE 50 *AND
   *VALUE NT_Process.%_Processor_Time *LT 65 *AND
   *VALUE NT_Process.Priority_Base *NE 0 *AND
   *VALUE NT_Process.Process_Name *NE _Total  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: A Service Error was reported  -->
<PRIVATESIT>
  <SITUATION>NT_Service_Error_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_Event_Log.Source *EQ "Service Control Manager"
   *AND *VALUE NT_Event_Log.Type *EQ Error  ]]>
  </CRITERIA>
  <INTERVAL>001000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Rate of operations to file system devices
per second is too high  -->
<PRIVATESIT>
  <SITUATION>NT_System_File_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_System.File_Data_Operations/Sec *GE 100000 ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Rate of operations to file system devices per second
 is rising -->
<PRIVATESIT>
  <SITUATION>NT_System_File_Warn_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE NT_System.File_Data_Operations/Sec *GE 10000 *AND
   *VALUE NT_System.File_Data_Operations/Sec *LT 100000  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Tivoli Data Warehouse の要約および sy_situations.xml のプルーニング

```
<PRIVATECONFIGURATION>
<!--  Situation Description: No connectivity to Warehouse database  -->
<PRIVATESIT>
  <SITUATION>KSY_DB_Connectivity_Fail_pr</SITUATION>
```

```
  <CRITERIA>
   <![CDATA[  *VALUE KSY_CONNECTIVITY.DB_Connectivity *EQ No ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Failures occurred in pruning  -->
<PRIVATESIT>
  <SITUATION>KSY_Pruning_Failures_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_SUMMARIZATION_STATISTICS.Pruning_Failures *GT 0 ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Failures occurred in summarization  -->
<PRIVATESIT>
  <SITUATION>KSY_Summ_Failures_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_SUMMARIZATION_STATISTICS.Summarization_Failures
   *GT 0  ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: No connectivity to the
Tivoli Enterprise Portal Server  -->
<PRIVATESIT>
  <SITUATION>KSY_TEPS_Conn_Fail_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KSY_CONNECTIVITY.TEPS_Connectivity *EQ No  ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

Tivoli Data Warehouse warehouse_situations.xml

```
<PRIVATECONFIGURATION>
<!--  Situation Description: No connectivity to warehouse database  -->
<PRIVATESIT>
  <SITUATION>KHD_DB_Connectivity_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_DB_INFO.DB_Connectivity *EQ No ]]>
  </CRITERIA>
  <INTERVAL>001500</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Critical errors during the execution
of the Warehouse Proxy  -->
<PRIVATESIT>
  <SITUATION>KHD_Error_Critical_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_LAST_ERROR_DETAILS.Error_Severity *EQ Critical ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
<!--  Situation Description: Fatal errors during the execution
of the Warehouse Proxy  -->
<PRIVATESIT>
  <SITUATION>KHD_Error_Fatal_pr</SITUATION>
  <CRITERIA>
   <![CDATA[  *VALUE KHD_LAST_ERROR_DETAILS.Error_Severity *EQ Fatal ]]>
  </CRITERIA>
  <INTERVAL>000000</INTERVAL>
</PRIVATESIT>
</PRIVATECONFIGURATION>
```

専用ヒストリー

専用ヒストリーは、ローカル・モニター・エージェントからのデータの収集であり、これらのデータを短期間保管しておく場所です。エージェントの専用シチュエーション構成ファイルでヒストリカル収集を定義した後、エージェント・サービス・インターフェースを使用して短期ヒストリーを表示します。

専用ヒストリーは、専用シチュエーション構成ファイルで構成されます。

ローカル・ヒストリカル・データ収集は、ヒストリカル・データを保存する各属性グループのローカル専用シチュエーション構成ファイルに定義されています。専用ヒストリーは、専用モニター・シチュエーションを付けても、付けなくても定義できます。アクティブにできるヒストリー・データ収集は、アプリケーション・テーブル (属性グループ) ごとに 1 つのみです。

<HISTORY> タグを使用して、ヒストリカル・データの収集対象となる各属性グループを指定します。オプションで EXPORT パラメーターを使用して、Tivoli Data Warehouse へのデータのエクスポート間隔を分単位で指定できます。

<WAREHOUSE> タグを使用して、ヒストリカル・データのエクスポート先 Warehouse Proxy agent を指定します。

374 ページの『専用シチュエーション XML 指定』を参照してください。

エージェント・オペレーション・ログ

XML 検証エラー・メッセージは、すべてエージェント・オペレーション・ログに保存されます。専用ヒストリーは、IBM Tivoli Management Services 内のヒストリカル・データ収集および Tivoli Data Warehouse 構成とは完全に分離されており、独立しています。各専用短期ヒストリー・テーブル・データは、それぞれのヒストリー・バイナリー・ファイルにあります。

短期ヒストリー・ファイルの名前

属性グループのテーブル名は、**PVTHIST_** の接頭部が付いたヒストリー・バイナリー・ファイル名でもあり、テーブルごとに固有のヒストリー・バイナリー・ファイルです。専用ヒストリー構成の一部として、RETAIN® 属性を設定してヒストリー・ファイルのサイズを管理できます。代替の専用ヒストリー・ファイルのロケーションは、エージェント構成パラメーター CTIRA_HIST_DIR を使用して構成できます。

短期ヒストリー・ファイルのディレクトリー

エージェントにより、すべての専用ヒストリー・ファイルが以下のサブディレクトリーに出力されます。

Windows <install_dir> ¥TMAITM6¥logs

Linux UNIX <install_dir>/<arch>/<pc>/hist

代替の専用ヒストリー・ファイルのロケーションは、エージェント構成パラメーター CTIRA_HIST_DIR を使用して構成できます。

短期ヒストリー・ファイルの保守

krarloff (z/OS の場合は KPDXTRA) など、短期ヒストリー・ファイルのファイル変換ユーティリティーが、ヒストリカル・ファイルからデータを取り出して区切り文字で区切られたテキスト・ファイルへ移動する目的で用意されています。

z/OS に関する考慮事項

Tivoli Enterprise Monitoring Server on z/OS の永続データ・ストア (PDS) 機能により、Tivoli Monitoring のアプリケーションは、SQL の表データと同じ方法でヒストリカル・データにアクセスできます。OMEGAMON XE 製品では、PDS を活用し、Tivoli Management Services を使用せずに、PDS コンポーネント経由でヒストリカル・データを保管および取得します。

PDS ディクショナリーには、アプリケーション・テーブルの定義が含まれています。

- 各テーブルは、アプリケーション名 (通常はアプリケーション製品コード、テーブル名、および割り当て済みファイル・グループ) によって識別されます。
- テーブル列の定義はテーブル定義に従い、列名、データ・タイプ、およびデータ長が含まれています。テーブル列は、同じ ID を使用したテーブルに関連しています。

以下の PDS ディクショナリー・テーブル定義は、Tivoli OMEGAMON XE for Mainframe Network 製品 KN3 テーブル KN3BPG からの例です。

```
CREATE ID=N303 APPL=KN3      TABLE=KN3BPG     GROUP=KN3
ADDCOL ID=N303 COL=TMZDIFF    TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=WRITETIME  TYP=CHARACTER  LEN=16   BIT=72   REQ
ADDCOL ID=N303 COL=ORIGINNODE TYP=CHARACTER  LEN=32   REQ
ADDCOL ID=N303 COL=SYSID      TYP=CHARACTER  LEN=4    REQ
ADDCOL ID=N303 COL=TIMESTAMP  TYP=CHARACTER  LEN=16   REQ
ADDCOL ID=N303 COL=CATDESC    TYP=INTEGER    LEN=2    REQ
ADDCOL ID=N303 COL=CATPCT     TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=POOLNAME   TYP=CHARACTER  LEN=4    REQ
ADDCOL ID=N303 COL=CATEGORY   TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=SAMPLES    TYP=INTEGER    LEN=4    REQ
ADDCOL ID=N303 COL=INTERVAL   TYP=INTEGER    LEN=4    REQ
```

テーブルは PDS グループに属し、多数の VSAM ファイルがテーブル・データの保管用に PDS ファイル・グループに割り振られます。PDS OVERRIDE ステートメントを使用して、テーブルまたはグループの割り当て (またはその両方) およびプロパティーを変更できます。KN3 グループ仕様を以下に示します。

```
OVERRIDE TABLE=KN3BPG APPL=KN3 WRAP=0 GROUP=KN3
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS3
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS2
GROUP=KN3 FILE=DSN:CCAPI.COMMON.NV.CIDSSP13.RKN3HIS1
```

PDS は、VSAM ファイル・キーとしてアプリケーション名、テーブル名、WRITETIME、および任意の索引付き列を使用してテーブル・データを保管します。専用ヒストリーの場合 (KN3BPG テーブルを使用 – 例: VTAM_Buffer_Usage_By_Category)、以下の 2 つの構成ステップが必要です。

1. ヒストリー・データ収集に必要なアプリケーション・テーブルを新規テーブルとして PDS ディクショナリーのデータ・セット RKANPARU メンバー KN3PDICT に以下のように追加します。
   a. KN3BPG テーブル定義のコピーを作成します。
   b. TABLE=KN3BPG を TABLE=ZN3BPG に変更します。
   c. ID=N303 を固有の ID に変更します (例えば N399)。

2. アプリケーション・テーブルの OVERRIDE ステートメントをデータ・セット RKANPARU メンバー KN3PG に追加します。
   a. テーブル KN3BPG OVERRIDE ステートメントがある場合はそれをコピーします。
   b. TABLE=KN3BPG を TABLE=ZN3BPG に変更します。

上記 2 つの構成ステップの完了後には、以下の例のように次の情報を <pc>_situations.xml に追加することにより、専用ヒストリーを構成して取得できます。

```
<PRIVATECONFIGURATION>
 <HISTORY TABLE="VTAM_Buffer_Usage_By_Category" Interval="15" Retain="24" />
</PRIVATECONFIGURATION>
```

サービス・インターフェース要求の例:

```
<HISTREAD>
 <SQLTABLE>
  <TABLENAME>KN3BPG</TABLENAME>
  <FILTER><![CDATA[ *VALUE WRITETIME  *GE 1090728020000000 *AND
   *VALUE WRITETIME  *LE 1090728080000000]]&gt;</FILTER>
  <OUTLIMIT>5000</OUTLIMIT>
 </SQLTABLE>
</HISTREAD>
```

エンタープライズおよび専用の両方のヒストリー・テーブル・データは、固有のキーを使用して PDS によって同一の VSAM データ・セットに保管され、そこから読み取られます。代わりに、専用ヒストリーを独自の PDS ファイル・グループに割り当て、専用ヒストリー・グループに対して個別の VSAM データ・セットを割り振ることもできます。

エンタープライズ・シチュエーション・オーバーライド XML 指定

エンタープライズ・シチュエーションのしきい値セットは、オンデマンドまたはスケジュールで一時的にオーバーライドできます。 Tivoli Enterprise Monitoring Agent のしきい値 XML 指定にシチュエーション・オーバーライドを定義すると、そのシチュエーション・オーバーライドをローカルで管理できます。

重要: この情報は、専用シチュエーションには適用されません。専用シチュエーションについては、374 ページの『専用シチュエーション XML 指定』を参照してください。

ローカルの XML しきい値ファイルの更新は、エージェントの再始動後に有効になります。 Tivoli Enterprise Monitoring Server を調べるシチュエーション・オーバーライド (Tivoli Enterprise Portal または CLI tacmd setOverride で定義されている) またはエージェント・サービス・インターフェースによって適用されるシチュエーション・オーバーライドは、すぐに有効になります。

XML 文書の読み取り後に、エージェントは定義されたしきい値オーバーライド指定を、すべての定義済みのテーブル定義のすべてのデータ収集要求に対して同期させます。すべてのしきい値パラメーター、カレンダー、およびシチュエーションの更新および削除は、すぐに有効になります。エージェントは、完全なしきい値オーバーライド指定 XML 文書を、名前が付けられたローカルのしきい値ファイルに出力します。

デフォルトのシチュエーション・オーバーライドのパスとファイル名

Windows *install_dir* ¥TMAITM6¥*pc*_thresholds.xml

Linux UNIX *install_dir* /bin/*pc*_thresholds.xml

z/OS RKANDATV データ・セット内の *PC*THRESH

IBM i ctira_sit_path/hostname_pc_thresholds.xml

ローカルのシチュエーションのオーバーライド操作を有効にするエージェント環境変数については、363 ページの『シチュエーション式のオーバーライド』 を参照してください。

オーバーライド定義は、CENTRAL モードで作成される同一ファイル内で作成し、手動で書き込む必要があります。オーバーライドの指定時に使用される列の名前は、属性ファイルから取得されます (Windows OS エージェントの場合は C:¥ibm¥ITM¥TMAITM6¥ATTRLIB¥knt.atr など)。

オーバーライドの指定時に使用される列の名前を検索するもう 1 つの方法は、ASI を使用することです。「ASI」>「照会」の順に開き、テーブル名を選択します。ASI は、テーブル表示名およびすべてのテーブルの列の表示名を含む、完全なテーブル・スキーマを戻します。

要素

すべての値を二重引用符で囲みます (例えば、"NT_Available_Bytes_Warning")。

<OVERRIDE>

開始の <override> および終了の </override> タグで、これを動的なしきい値の構成として定義します。

ObjName=

シチュエーション・オーバーライドの文書名を指定します。

<CALENDAR>

オプションです。 名前が付けられているカレンダー定義を指定します。別の方法として、スケジュールされたオーバーライドを <threshold> 要素に指定できます。

Name=

カレンダーのシンボル名を指定します。

Action=

オプションです。 カレンダー定義の処理を指定します。値 Update の場合、名前が付けられたカレンダーが作成されるか、置き換えられます。値 Delete の場合、名前が付けられた既存のカレンダーが削除されます。

Start= Stop=

オプションです。 これらの属性は、同じ時間および同じ期間に開始されるオーバーライドを適用します。例えば、start=『08:15』 stop=『17:30』 を指定すると、オーバーライドは 8:15 AM から 5:30 PM まで有効になります。start=『21:45』" stop=『05:15』 を指定する

と、オーバーライドは 9:45 PM から翌日の 5:15 AM まで有効になります calendar= を定義しない場合は、start=、stop=、および cron= 値が使用されます。

Cron= オプションです。 時間定義を**分 時間 日 月 曜日**フォーマットで指定します。ここで、**分**は 0 から 59、**時間**は 0 から 23、**日**は 1 から 31、**月**は 1 から 12、**曜日**は 0 から 6 です (日曜日は 0 か 7 のいずれかにできます)。それぞれのフィールドはスペースで区切り、以下の記号を自由に組み合わせて使用します。

- そのフィールドで有効なすべての値を意味する場合は、アスタリスク (*) を使用します。例えば、月フィールドで * はあらゆる月を意味します。
- フィールドに複数の値を入力する場合は、コンマ (,) で区切ります。
- 値の範囲を示す場合は、ハイフン (-) を使用します。
- **月**および**曜日**フィールドには名前を使用することもできます。特定の曜日または月の最初の 3 文字を使用します。
- スラッシュ (/) が前に付いたステップ値は、スキップする数です。例えば、時間フィールドの */3 は、3 時間おきを意味します (0、3、6、9、12、15、18、21)。ステップ値は、分フィールドでは無効です。

CRON 定義は、時刻範囲 (開始時刻から終了時刻) を指定する必要があります。calendar= を定義しない場合は、start=、stop=、および cron= 値が使用されます。

LastUpdate=
オプションです。 最終更新日の 16 桁のタイム・スタンプです。既存の設定済みのタイム・スタンプより前の場合、そのタイム・スタンプは無視されます。デフォルトは、**0 0 0 0 0** です。

ObjName=
オプションです。 オーバーライド文書名を指定します。

<SITUATION>
シチュエーションしきい値の構成を定義します。

Name=
シチュエーション名を指定します。

Table=
オプションです。 テーブルの列名ではなく、キーまたはしきい値の定義属性名を使用する場合は、属性テーブル名を指定します。 SQL テーブル名または属性テーブル名を使用します。

Action=
オプションです。 シチュエーション定義の処理を指定します。指定がない場合、値 Update によって、シチュエーション指定が作成されます。そうでない場合は、一致するオーバーライドが変更されます。値 Delete の場合、シチュエーション・オーバーライドの指定全体が削除されます。

LastUpdate=
オプションです。 最終更新日の 16 桁のタイム・スタンプです。既存の設定済みのタイム・スタンプよりも前の場合は無視されます。

Calendar=
オプションです。 名前が付けられているカレンダー定義を指定します。このシチュエーション内のすべてのしきい値にカレンダーが適用されます。

Priority=
シチュエーション・オーバーライドの優先順位です。数値が小さいほど、優先順位は高くなります。エージェントは、優先順位の低いオーバーライドを、優先順位の高い更新と置き換え、同じ優先順位の更新は拒否します。デフォルトは、2147483647 です。

ObjName=
オプションです。 オーバーライド文書名を指定します。

<KEY> または <TRIGGER>
オプションです。 複数行のサンプル内のデータ行を一意に区別するために、データ値を含むテーブル列を定義します。ネストした <key> 定義は、暗黙に AND 条件を示しています。同じレベルの <key> 定義は、暗黙に OR 条件を示しています。

Column=
列名。例えば、*column=USAGE* などです。オーバーライドを適用するサブエージェントがある場合、列 ORIGINNODE をキーとして指定し、サブノードの管理対象システム名をキー値として指定できます。

Attr= 属性名。列名を指定する代替の方法として、属性名を指定することもできます。属性名を使用する場合は、<situation> 要素にテーブル名を指定するか、属性名を **table-name.attribute-name** 形式 (*attr=NT_Paging_File.%_usage* など) で指定する必要があります。

Value=
列または属性フィルター・データの値です。属性値は、Value パラメーターを使用しないで、開始および終了タグの間に指定することもできます。ただし、パラメーター・スタイルの方が推奨されます。

<THRESHOLD>
しきい値の指定を定義します。

Column=
列名。例えば、*column=CONATTMP* などです。

Attr= 属性名。列名を指定する代替の方法として、属性名を指定することもできます。属性名を使用する場合は、<situation> 要素にテーブル名を指定するか、属性名を **table-name.attribute-name** 形式 (*attr=HTTP_Service.Connection_Attempts* など) で指定する必要があります。

Position=
オプションです。 シチュエーション論理構成内での、属性シーケンスの位置です。値 1 から始まります。値ゼロ (0) は、暗にすべての属性が論理積または論理和、あるいはその両方のシチュエーション論理で出

現することを示しています。 このパラメーターは、同じ属性が複数回出現するような論理内で、特定のオーバーライド属性を指定する場合に便利です。例えば、A1 > 80% AND A2 < 95% などです。デフォルト: **0**

Operator=
オプションです。 論理演算は、同じ属性が複数回出現するようなシチュエーション構成内で、定義する属性を一意に限定します。演算子の値は、EQ、NE、GE、LE、GT、LT です。上記の例の A1 も、Operator=GT を使用して限定できます。

Value=
列または属性しきい値です。属性値は、Value パラメーターを使用しないで、開始および終了タグの間に指定することもできます。ただし、パラメーター・スタイルの方が推奨されます。

Calendar=
オプションです。 名前が付けられているカレンダー定義を指定します。このカレンダーは、<situation> 要素に指定されたカレンダー、start=、stop=、および cron= 属性をオーバーライドします。

Start= Stop=
オプションです。 これらの属性は、同じ時間および同じ期間に開始されるオーバーライドを適用します。例えば、start=『08:15』 stop=『17:30』 を指定すると、オーバーライドは 8:15 AM から 5:30 PM まで有効になります。start=『21:45』" stop=『05:15』 を指定すると、オーバーライドは 9:45 PM から翌日の 5:15 AM まで有効になります calendar= を定義しない場合は、start=、stop=、および cron= 値が使用されます。

Cron= オプションです。 時間定義を**分 時間 日 月 曜日**フォーマットで指定します。ここで、**分**は 0 から 59、**時間**は 0 から 23、**日**は 1 から 31、**月**は 1 から 12、**曜日**は 0 から 6 です (日曜日は 0 か 7 のいずれかにできます)。それぞれのフィールドはスペースで区切り、以下の記号を自由に組み合わせて使用します。

- そのフィールドで有効なすべての値を意味する場合は、アスタリスク (*) を使用します。例えば、月フィールドで * はあらゆる月を意味します。
- フィールドに複数の値を入力する場合は、コンマ (,) で区切ります。
- 値の範囲を示す場合は、ハイフン (-) を使用します。
- **月**および**曜日**フィールドには名前を使用することもできます。特定の曜日または月の最初の 3 文字を使用します。
- スラッシュ (/) が前に付いたステップ値は、スキップする数です。例えば、時間フィールドの */3 は、3 時間おきを意味します (0、3、6、9、12、15、18、21)。ステップ値は、分フィールドでは無効です。

CRON 定義は、時刻範囲 (開始時刻から終了時刻) を指定する必要があります。calendar= を定義しない場合は、start=、stop=、および cron= 値が使用されます。

<DEFAULT>

オプションです。 複数行のサンプルに適用される、1 つ以上のデフォルト・フィルターのしきい値を定義します。これは、<key> タグが定義されている場合に推奨されます。

例

```
<overrides>
  <situation name="Check_Event" table="NT_Event_Log">
    <threshold attr="Source"
               value="Symantec Antivirus"
               start="08:00" stop="17:00" />
  </situation>
  <situation name="NT_Available_Bytes_Critical" table="NT_Memory">
    <threshold attr="Available_Bytes"
               value="750000"
               start="08:00" stop="17:30"
               cron=" * * * * 1-5" />
  </situation>
  <situation name="NT_Disk_Space_Low">
   <threshold name="FREEMGBTES"
               value="10"
               cron="31-59 8-20 */2 * *"
    </threshold>
  </situation>
  <situation name="NT_Log_Space_Low">
      <threshold name="USAGE"
                 value="75"
                 start="08:00" stop="18:00"
                 cron="* * * * MON,WED,FRI"
     </threshold>
  </situation>
  <situation name="Message_Queue_Warning" table="Queue_Statistics">
    <KEY column="ORIGINNODE" value="SYSG:NETQ3">
      <threshold attr="Queue_Depth"
                 value="10"
                 cron="0-30 8-17 * 3,6,9,12 *"
      </threshold>
    </KEY>
  </situation>
  <situation name="NT_Process_CPU_Critical" table="NT_Process">
    <KEY attr="Process_Name" value="_Total">
      <threshold attr="%_Processor_Time"
                 value="70"
                 start="06:00" stop="21:30"
                 cron="* * * * 1-5" />
    </KEY>
  </situation>
  <situation name="NT_System_File_Critical" table="NT_System">
      <threshold attr="File_Data_Operations/Sec"
                value="50000"
                cron="* 6-22 * * SAT,SUN"
      </threshold>
  </situation>
  <situation name="DISKFULL">
    <key column="INSTCNAME" value="C:">
      <threshold column="PCFREE">5</threshold>
    </key>
    <key column="INSTCNAME" value="D:">
      <threshold column="PCFREE">10</threshold>
    </key>
    <default>
    <threshold column="PCFREE">0</threshold>
    </default>
  </situation>
  <situation name="Windows_Events">
```

```
    <key column="SOURCE" value="MSFTPSVC">
    <key column="EVENTID" value="10">
      <threshold column="SOURCE">MSFTPSVC</threshold>
    </key>
    <key column="EVENTID" value="100">
      <threshold column="SOURCE">MSFTPSVC</threshold>
    </key>
    </key>
    <key column="SOURCE" value="EventLog">
    <key column="EVENTID" value="6005">
      <threshold column="SOURCE">EventLog</threshold>
    </key>
    <key column="EVENTID" value="6009">
      <threshold column="SOURCE">EventLog</threshold>
    </key>
    </key>
    <default>
      <threshold column="SOURCE">NOPASS</threshold>
    </default>
  </situation>
</overrides>
```

SNMP アラート

Tivoli Enterprise Monitoring Agent および Tivoli System Monitor Agent は、Netcool/OMNIbus SNMP プローブ、または Tivoli NetView を使用して、Netcool/OMNIbus などの SNMP 受信側にアラートを送信するよう構成できます。重要な統合の考え方をいくつか説明するため、サンプルの OMNIbus ルール・ファイルが提供されています。

SNMP アラート構成

モニター・エージェントおよび SNMP トラップ構成ファイルを構成して、ライフサイクル・イベントまたはシチュエーション・イベントを SNMP イベント受信側に発行します。

トラップ構成ファイル

構成されたシチュエーションに対して、エージェントから SNMPv1/v2 トラップまたは SNMPv3 インフォームを発行するには、エージェントの開始時にトラップ構成ファイルが配置されている必要があります。正しく名前が付けられた trapcnfg.xml ファイルがエージェントのローカル構成ディレクトリーに配置されている場合、エージェントを開始すると、エージェントはファイルに定義されているトラップを発行します。ファイルには *pc*_trapcnfg.xml という名前が付けられます (ここで、*pc* はエージェントの 2 文字の製品コードです)。このファイルは *install_dir*/localconfig/*pc* ディレクトリーにあります。 このファイルには、*pc*_trapcnfg.xml という名前を付ける必要があります。ここで、*pc* は 2 文字の製品コードです。例えば、UNIX OS エージェントでは ux です。

IBM i IBM i エージェントは SNMPv1/v2 トラップを送信できますが、SNMPv3 inform を送信することはできません。

z/OS z/OS の場合、ファイルのデフォルト名は、RKANDATV データ・セット内の *PC*TRAPS です。

エージェント・パラメーター

エージェント環境ファイルの

IRA_EVENT_EXPORT_SNMP_TRAP_CONFIG パラメーターを設定して、トラップ構成ファイルに別の名前およびパスを指定することができます。SNMP アラートは、そのエージェント・タイプのトラップ構成 XML ファイルに構成されたシチュエーションに対してのみ発行されます。絶対パスか、またはローカル構成ディレクトリーに対する相対パスを指定できます。

完全なパスを指定するには、PDS が最後にリストされている必要があります (または省略して、デフォルトの RKANDATV を使用します)。

IRA_EVENT_EXPORT_SNMP_TRAP=N を使用すると、*pc*_trapcnfg.xml ファイルが配置されていても、エージェントの SNMP アラートを使用不可にできます。

XML 仕様

トラップ構成ファイルは以下の XML エレメントを含むことができます。

SNMP

TrapDest

TrapAttrGroup

シチュエーション

StatTrap

SNMP は最上位の XML エレメントです。TrapDest、TrapAttrGroup、および Situation は SNMP の開始タグおよび終了タグで囲まれている要素です。

サンプルのトラップ構成ファイル

以下の Windows OS エージェント用のサンプル nt_trapcnfg.xml を確認すると、トラップ構成ファイルの構成を理解できます。これは *install_dir*¥localconfig¥nt ディレクトリーに置かれており、Windows OS エージェントに対するトラップの発行を使用可能にします。このファイルは、nt2003infra ホスト上の SNMPv1 トラップをモニターする Tivoli Universal Agent に ステータス・トラップを送信したり、ホスト 10.21.32.234 で実行されている SNMPv3 を使用して、シチュエーション・イベントのインフォームを Netcool/OMNIbus SNMP プローブに送信するように構成されます。

```
<!—C:¥IBM¥ITM¥localconfig¥nt¥nt_trapcnfg.xml /-->
<SNMP>
   <TrapDest name="UAStatMon" Address=" nt2003infra " Version="v1"
   Community="{AES256:keyfile:a}P0hUrmUhCgfFwimS+Q6w+w==" Stat="Y" />

   <TrapDest name="Probe1" Version="v3" Address="10.21.32.234"
   SecLevel="authPriv" User="AuthPrivMD5DES" AuthType="MD5"
   AuthPassKey="{AES256:keyfile:a}yifHSbFcTKHBqvORpzxS6A=="
   PrivType="DES" PrivPassKey=
   "{AES256:keyfile:a}1le2SxljJR1MOIi0EDIvig==" Stat="N" />

   <TrapAttrGroup Table="NT_Paging_File" TrapAttrList="Server_Name,
   %_Usage" />

   <Situation name="NT_Log_Space_Low_pr" sev="2" cat="0"
   mode="HY"
   target="Probe1" />
   <Situation name="NT_Missing_Scheduler_pr" sev="5" cat="0"
   mode="HY" target="Probe1" />
   <Situation name="NT_Paging_File_Critical_pr" sev="5" cat="0"
   mode="HY" target="Probe1" />
   <Situation name="NT_Paging_File_Warning_pr" sev="2" cat="0"
```

```
    mode="HY" target="Probe1" />
    <Situation name="NT_Phys_Disk_Busy_Critical_pr" sev="5" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_Phys_Disk_Busy_Warn_pr" sev="2" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_System_File_Warn_pr" sev="2" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_Proc_CPU_Critical_pr" sev="5" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_Proc_CPU_Warn_pr" sev="2" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_Service_Error_pr" sev="2" cat="0"
    mode="RC" target="Probe1" />

    <Situation name="NT_System_File_Critical_pr" sev="5" cat="0"
    mode="HY" target="Probe1" />
    <Situation name="NT_System_File_Warn_pr" sev="2" cat="0"
    mode="HY" target="Probe1" />

    <StatTrap name="EE_HEARTBEAT" sev="1" interval="15" cat="3" />
    <StatTrap name="EE_AUTO_ENTER" sev="1" cat="3" />
    <StatTrap name="EE_AUTO_EXIT" sev="1" cat="3" />
    <StatTrap name="EE_AUTO_USE_LIMIT" sev="5" cat="3" />
    <StatTrap name="EE_TEMS_RECONNECT_LIMIT" sev="5" cat="3" />
    <StatTrap name="EE_TEMS_CONNECT" sev="1" cat="4" />
    <StatTrap name="EE_TEMS_DISCONNECT" sev="1" cat="4" />
    <StatTrap name="EE_SIT_STOPPED" sev="1" cat="4" />
</SNMP>
```

トラップ構成 XML 仕様

SNMP XML ファイルで SNMP、TrapDest、TrapAttrGroup、Situation、StatTrap の各要素を使用して、イベント受信側に指定するエージェント・タイプ用にトラップを構成します。

XML タグは大/小文字を区別しません。他のすべてのパラメーターには大/小文字の区別があります。例えば、ADDRESS、Address、または address と入力できます。

SNMP エレメント

トラップ構成 XML 仕様の SNMP エレメントは、最上位の XML エレメントです。TrapDest、TrapAttrGroup、および Situation は SNMP の開始タグおよび終了タグで囲まれている要素です。

```
<SNMP>
 <TrapDest name="OMNIbus2" Address="nswin21a" Stat="Y" />
 <situation name="*" target="OMNIbus2" />
</SNMP>
```

TrapDest 要素

トラップ構成 XML ファイルの TrapDest 要素を使用して、トラップ受信側を定義します。

TrapDest 要素には、名前属性およびターゲット属性が必要です。デフォルト値は、指定されていないその他すべての属性に使用されます。

```
<TrapDest name="LABEL" Address="HOSTNAME"/>
```

表 30. TrapDest 要素の XML 仕様

属性	説明	必須	デフォルト	SNMPv1/v2 または SNMPv3
Name=	トラップ宛先を識別するために使用される英数字のラベル。	必須		
Address=	トラップ受信側の TCP/IP アドレスまたはホスト名。	必須		すべて
IP=	ip プロトコル: “4”	“6” 4 は IPv4、6 は IPv6	オプション	"4"	すべて
Port=	トラップ受信側 TCP/IP トラップ・リスニング・ポート。	オプション	"162"	すべて
BindAddress=	SNMP トラフィックに使用するローカル・インターフェースを指定するために使用されます。指定されるインターフェースは IP 設定と一致する必要があります。	ホストに複数のネットワーク・インターフェースが定義されている場合は、必須です。指定しないと、トラップ送信がエラー番号 22 で失敗する可能性があります。	First available	すべて
Version=	SNMP トラップのバージョンを指定します。有効な文字列の値は、(大/小文字を区別しない) : **v1**、**v2**、**v3**	オプション	v1	すべて
Type=	Trap | Inform の Type が Version と一致している必要があります。Version= “v1” | “v2” タイプは “Trap” である必要があります。Version= “3” タイプは、“Inform”である必要があります。	オプション	Matches version	すべて

表 30. TrapDest 要素の XML 仕様 (続き)

属性	説明	必須	デフォルト	SNMPv1/v2 または SNMPv3
Stat=	Stat は、Stat=『Y』 に設定すると、すべてのステータス・トラップをその受信側に送信するために宛先上で使用されます。Stat を 『N』 に設定すると、TrapDest に対するすべてのステータス・アラートが使用不可になります。ステータス・アラートのサブセットのみを TrapDest に送信する場合も、『N』 に設定します。 StatTrap 要素を使用して個々のステータス・アラートを特定の TrapDest に送信できます。	オプション	『Y』	すべて
Community=	トラップ・コミュニティー名のストリングを指定します。 itmpwdsnmp を使用して暗号化する必要があります。ただし、平文も使用できます (1-63 文字)。	オプション	public	v1 および v2
SecModel=	セキュリティー・モデルを指定します。サポートされているのは、USM だけです。	オプション	USM	v3
SecLevel=	認証レベルおよびプライバシー・レベルを指定します。 サポートされているレベルは次のとおりです。 **noAuthNoPriv** – 認証なし、プライバシーなし **authNoPriv** – 認証あり、プライバシーなし **authPriv** – 認証あり、プライバシーあり (z/OS モニタリング・エージェントではサポートされていません)	v3 では必須。		v3

表 30. TrapDest 要素の XML 仕様 (続き)

属性	説明	必須	デフォルト	SNMPv1/v2 または SNMPv3
User=	アカウント名を指定します。	v3 では必須。		v3
AuthType=	認証プロトコルを指定します。サポートされるプロトコルは MD5 および SHA です。	v3 では必須。SecLevel= authNoPriv または authPriv		v3
AuthPassKey=	認証パスワードを指定します。itmpwdsnmp を使用して暗号化する必要がありますが、平文も使用できます (1-63 文字)。	v3 では必須。SecLevel= authNoPriv または authPriv		v3
PrivType=	プライバシー・プロトコルを指定します。サポートされているプロトコルは DES です。	v3 では必須。SecLevel= authPriv		v3
PrivPassKey=	プライバシー・パスワードを指定します。itmpwdsnmp を使用して暗号化する必要があります。ただし、平文も使用できます (1-63 文字)。	v3 では必須。SecLevel= authPriv		v3
Timeout=	SNMPv3 メッセージの確認応答のタイムアウト (整数の秒単位) を指定します (最小 1)。	オプション	2	v3
Retries=	タイムアウトが発生した場合の再送信の回数を指定します (最小 0、最大 5)。	オプション	3	v3

TrapAttrGroup 要素

trapcnfg.xml ファイルの TrapAttrGroup 要素を使用して、シチュエーション・イベント・トラップに含める属性グループの属性を指定します。

以下の構文例では、Windows OS のページング・ファイル属性グループに対して作成されたシチュエーションが、SNMP トラップをサーバー名、使用率、使用ピーク値とともにイベント受信側に送信します。

```
<TrapAttrGroup Table="NT_Paging_File" TrapAttrList="Server_Name,
%_Usage,%_Usage_Peak" />
```

この要素を使用すると、各トラップ要求で送信される属性データの量を削減し、トラップのフラグメント化の可能性を低下させ、受信データを関連するもののみに絞り込むことができます。

TrapAttrGroup 要素では、テーブルに対して実行するすべてのシチュエーションに送信されるデフォルト属性を設定します。個々のシチュエーションは、シチュエーション要素の TrapAttrList 属性を指定することにより、TrapAttrGroup 設定を上書きできます。

TrapAttrGroup 要素が属性テーブルに対して定義されない場合は、シチュエーションのデータ行のすべての属性が、この属性テーブルに基づくシチュエーションに送信されたトラップの sitAttributeList varbind に追加されます。シチュエーション述部で使用されている属性が最初に追加され、残りの属性は、PDU の最大長である 1500 バイトに到達するまで追加されます。

表 31. TrapAttrGroup 要素の XML 仕様

属性	説明
Table=	属性テーブルの名前。このファイルを手動で作成する場合は、エージェントの属性ファイル *pc*.atr を確認し、テーブル名を識別します。ここで、*pc* は 2 文字の製品コードです。
TrapAttrList=	この属性テーブルに基づいてシチュエーションに送信されたトラップの **sitAttributeList varbind** に含まれる、コンマで区切られた属性のリスト。

シチュエーション要素

トラップ構成 XML ファイルのシチュエーション要素を使用して、シチュエーションに送信されるトラップを定義します。

```
<situation name="Situation_ID" target="TrapDest_Name" />
```

シチュエーション要素には、名前属性およびターゲット属性が必要です。デフォルト値は、指定されていないその他すべての属性に使用されます。シチュエーション名またはターゲット名またはその両方に対して * (アスタリスク) ワイルドカードを指定できます。

- シチュエーション名に対してワイルドカードを指定すると、すべてのシチュエーションを表します。例えば、以下の行ではすべての定義済み true シチュエーションのトラップを trapProbe1 という名前の定義済み TrapDest に送信します。

  ```
  <situation name="*" target="trapProbe1" />
  ```

  シチュエーション名に対して * ワイルドカードを指定した場合、ヒステリシス・モードの動作は指定できません。
- ターゲット・パラメーターにワイルドカードを指定すると、シチュエーション名フィールドに指定されたシチュエーションをすべての定義済みターゲットに送信することができます。

  ```
  <situation name="NT_Disk_Low" target="*" />
  ```
- シチュエーション名とターゲットの両方にワイルドカードを指定すると、すべての定義済みのトラップ受信側にすべてのトラップを送信できます。
- 名前付きのシチュエーションは、ワイルドカード定義より優先されます。シチュエーション定義にワイルドカードが指定されており、別のシチュエーション定義でシチュエーションまたはターゲットが指定されている場合は、最初に出現する名前付きシチュエーション定義が優先されます。以下に例を示します。

```
<TrapDest name="MyReceiver" Address="UAHOST1" Version="v1" />
<TrapDest name="OMNIbus1" Address="OMNIbus1" Version="v2"
 Community="{AES256:keyfile:a}P0hUrmUhCgfFwimS+Q6w+w==" />
<TrapDest name="OMNIbus2" Version="v3" Address="9.42.10.164"
 SecLevel="authPriv" User="SnmpUser" AuthType="SHA"
 AuthPassKey="{AES256:keyfile:a}vgpNvf5Vx3XbPj1sKRRvYg==" PrivType="DES"
 PrivPassKey="{AES256:keyfile:a}OK5YOWvRIkPOw9k4JRy9ag==" />
<situation name="*" target="OMNIbus2" />
<situation name="My_Missing_Process" target="MyReceiver" />
<situation name="NT_AA_Missing_Test" target="OMNIbus1" />
<situation name="NT_AA_Missing_Test" target="OMNIbus2" />
<situation name="NT_ABC_Missing_Test" target="*" />
```

My_Missing_Process シチュエーションは、**OMNIbus2** ではなく **MyReceiver** にトラップを送信します。また、**NT_ABC_Missing_Test** は **OMNIbus2** だけでなく、**MyReceiver**、**OMNIbus1**、**OMNIbus2** に送信されます。これは、シチュエーションがワイルドカードを使用してではなく、明示的に定義されているためです。

シチュエーションが複数回定義されている場合は、最初に現れるシチュエーション定義が優先されます。再度例を確認すると、**NT_AA_Missing_Test** は **OMNIbus2** ではなく **OMNIbus1** に送信されます。これは、同一のシチュエーションに対して最初に現れる定義で、**OMNIbus1** が指定されているためです。

表 32. シチュエーション要素 XML 仕様

属性	説明	必須	デフォルト
Name=	これは、シチュエーションの ID または短縮名です。	必須	
Target=	直前の定義済み TrapDest を指定します。「*」はすべての定義済み宛先へのトラップの送信を暗黙指定します。	必須	
Sev=	トラップ重大度を指定します。標準のトラップ重大度は、次のとおりです。 0 – 解決済み 1 – 不定 2 – 警告 3 – マイナー 4 – メジャー 5 – 重大	オプション	2

表 32. シチュエーション要素 XML 仕様 (続き)

属性	説明	必須	デフォルト
Cat=	トラップ・カテゴリーを指定します。標準のトラップ・カテゴリーは、次のとおりです。 0 - しきい値 1 – ネットワーク・トポロジー 2 – エラー 3 – ステータス 4 – ノード構成 5 – アプリケーション・アラート 6 – すべてのカテゴリー 7 – ログのみ 8 – マップ 9 – 無視	オプション	0
Mode=	サンプル・シチュエーションでの SNMP トラップ出力の動作の指定に使用します。標準モードは、次のとおりです。 RC – 常時発信。true に評価されたシチュエーションごとにトラップが送信されます。(ピュア・イベントは必ず RC)。特定の消去トラップは送信されません。 HY – ヒステリシス。これは、トラップがサンプル・シチュエーションが初めて true に評価されたときにトラップが送信されます。消去トラップは、サンプル値がシチュエーションの基準を満たさなくなったら送信されます。ヒステリシス・モードでは、* ワイルドカードで指定するのではなく、シチュエーションの名前を指定する必要があります。	オプション	RC
Pred=	シチュエーションの述部 (式) がトラップの autoSit-Predicates varbind で送信されます。Pred 属性では Pred="N"を設定することにより、シチュエーションの述部を省略できます。これは、述部を受信する必要がない場合、または複雑な述部がトラップ PDU を過剰に使用している場合に、sitAttributeList varbind でシチュエーション属性を送信するための余地を確保するために役立ちます。	オプション	Y

表 32. シチュエーション要素 XML 仕様 (続き)

属性	説明	必須	デフォルト
Table=	属性グループの表の名前。**sitAttributeList varbind** の構成に使用される属性のサブセットを識別するために、TrapAttrlist で使用されます。	**TrapAttrList** を使用する場合にのみ必要です。	
TrapAttrList=	シチュエーションに送信されたトラップの sitAttributeList varbind に含まれるコンマで区切られた属性のリスト。 ここで指定されている値は、シチュエーションが実行されているテーブルの TrapAttrGroup 要素で指定されたすべての TrapAttrList 値をオーバーライドします。	オプション	

注: 表示項目を含んだ複数行の属性グループのシチュエーションは、true に評価される最初の行に対してのみ 1 つのトラップを送信でき、後続の行に対しては送信できません。

StatTrap

SNMP トラップ構成ファイルで StatTrap 要素を使用して、事前定義のエージェント・ライフサイクル・ステータス・トラップのデフォルト構成を変更します。

以下の構文例では、イベントに重大度 1 (不定)、30 分のサンプリング間隔、およびトラップ・カテゴリー 3 (ステータス) を指定するために EE_HEARTBEAT の定義済みトラップが変更されています。

```
<StatTrap name="EE_HEARTBEAT" sev="1" interval="30" cat="3" />
```

8 つの定義済みエージェント・ライフサイクル・トラップがあり、それらのデフォルト値は次の表で指定されています。デフォルトでは、これらのトラップは、Stat 属性が "Y" であるすべての TrapDest トラップ宛先に送信されます。Stat 属性が TrapDest 要素から省略される場合、デフォルト値は "Y" です。

表 33. エージェントのライフサイクル・ステータス・トラップ

属性	説明	重大度	カテゴリー
EE_HEARTBEAT	ハートビートでは、エージェントが実行されており、出力されたイベントがトラップの宛先に到達可能であることを示します。これは、設定間隔が 15 分であるステータス・トラップのみです。	1 – 不定	3 – ステータス
EE_AUTO_ENTER	エージェントがオートノマス・モードに遷移しました。	1 – 不定	3 – ステータス
EE_AUTO_EXIT	エージェントが自律モードを終了しました。	1 – 不定	3 – ステータス

表 33. エージェントのライフサイクル・ステータス・トラップ (続き)

属性	説明	重大度	カテゴリー
EE_AUTO_USE_LIMIT	エージェントが IRA_AUTONOMOUS_LIMIT 環境変数によって指定されたストレージ制限に到達しました。エージェントがモニター・サーバーから接続を切断されたときに生成された追加イベントを再接続時にアップロードできない場合があります。	1 – 不定	3 – ステータス
EE_TEMS_RECONNECT _LIMIT	エージェントは、CTIRA_MAX_RECONNECT_TRIES 環境変数によって指定された再試行制限に到達しました。エージェントは、モニター・サーバーへの接続を試行することはなく、シャットダウンされます。 IBM Tivoli Monitoring 6.2.2 以降では、CTIRA_MAX_RECONNECT_TRIES のデフォルト値が 0 に変更されたため、エージェントがシャットダウンされることはありません。	1 – 不定	3 – ステータス
EE_TEMS_CONNECT	エージェントはモニター・サーバーに正常に接続しました。	1 – 不定	4 – ノード構成
EE_TEMS_DISCONNECT	エージェントでモニター・サーバーとの接続が失われました。	1 – 不定	4 – ノード構成
EE_SIT_STOPPED	シチュエーションが停止しました。	1 – 不定	4 – ノード構成

StatTrap 要素を使用して、エージェントのライフサイクル・トラップを構成します。

表 34. StatTrap 要素の XML 仕様

ステータス・トラップ	説明	必須	デフォルト
Name=	このトラップ名は、定義済みのライフサイクル・ステータス・トラップの名前である必要があります。 EE_HEARTBEAT EE_AUTO_ENTER EE_AUTO_EXIT EE_AUTO_USE_LIMIT EE_TEMS_RECONNECT_LIMIT EE_TEMS_CONNECT EE_TEMS_DISCONNECT EE_SIT_STOPPED	オプション	
Target=	直前の定義済み TrapDest を指定します。アスタリスク (*) はすべての定義済み宛先へのトラップの送信を暗黙指定します。ターゲットが定義されていない場合、Stat=”Y”に指定されているすべての TrapDest がステータス・トラップを受信します。	必須	

表 34. StatTrap 要素の XML 仕様 (続き)

ステータス・トラップ	説明	必須	デフォルト
Sev=	トラップ重大度を指定します。標準のトラップ重大度は、次のとおりです。 0 – 解決済み 1 – 不定 2 – 警告 3 – マイナー 4 – メジャー 5 – 重大	オプション	変化する
Cat=	トラップ・カテゴリーを指定します。標準のトラップ・カテゴリーは、次のとおりです。 0 - しきい値 1 – ネットワーク・トポロジー 2 – エラー 3 – ステータス 4 - ノード構成 5 – アプリケーション・アラート 6 - すべてのカテゴリー 7 - ログのみ 8 – マップ 9 – 無視	オプション	変化する
Interval=	Interval では、EE_HEARTBEAT ステータス・トラップが出力される間隔を分単位で指定します。ピュア・イベントである、その他のステータス・トラップでは、Interval は無視されます。	オプション	EE_HEARTBEAT は 15 その他すべて 0

SNMP パス・キーの暗号化: itmpwdsnmp

パスワードを対話式に暗号化する場合、または SNMP トラップ構成 XML ファイルに追加して、すべての SNMP パスワードを暗号化する場合は、**itmpwdsnmp** CLI コマンドを使用します。

itmpwdsnmp は GSKIT を使用して、対話式にストリングを暗号化するか、またはトラップ構成 xml ファイル内のすべての SNMP パスワード・ストリングを暗号化します。

itmpwdsnmp [[-b |-n]your_agent_trapcnfg.xml][-?]

値の説明:
対話モードを指定する引数はありません。
-b ではバックアップ・ファイルの作成を指定します。バックアップ・ファイルの削除を求めるプロンプトが出されません。
-n では、作成するバックアップ・ファイルがないことを指定します。
your_agent_trapcnfg.xml は、非暗号化テキストの SNMP パスワード・ストリングを含むトラップ構成 xml ファイルです。
-? は、使用量を表示します。

トラップ構成 xml ファイルの暗号化の際にバックアップ・オプション **-b** または **-n** が指定されていない場合は、バックアップを削除するようプロン

プトで指示されます。入力トラップ構成 xml ファイルのバックアップは、元のファイル名に日付とタイム・スタンプが付加されて、元のファイルと同じディレクトリーに作成されます。

Windows *install_dir* ¥TMAITM6¥itmpwdsnmp.bat

Linux UNIX *install_dir* /bin/itmpwdsnmp.sh

CLI の例

次のコマンドは、ストリングを対話式に暗号化します。

```
itmpwdsnmp

Enter string to be encrypted:
********
Confirm string:
********
{AES256:keyfile:a}GbHOlF7KPYZS80Rripx4QQ==
```

次に、暗号化されたストリングをトラップ構成ファイルにコピーします。

次のコマンドは、トラップ構成ファイル内のすべての SNMP パスワード・ストリングを暗号化し、元のファイルのバックアップを削除します。

```
itmpwdsnmp -n nt_trapcnfg.xml
```

プログラムの要約

暗号化されたコミュニティー・ストリング 1

暗号化された AuthPassKey ストリング 2

暗号化された EncryptPassKey ストリング 1

SNMP アラートおよびエージェント発行のための MIB

Tivoli モニター・エージェントは、3 つのタイプの SNMP メッセージを発行します。エージェントの作動状況を伝える場合は? **agentStatusEvent**、定期的にサンプリングを行って true になるシチュエーションに対しては **agentSitSampledEvent**、非送信請求通知を受信するシチュエーションに対しては **agentSitPureEvent** を発行します。

これらのタイプは、IBM Tivoli Monitoring IBM Tivoli Monitoring Agent のインストール・メディアで入手できる canbase.mib ファイルおよび cansyssg.mib ファイルで定義されています。

agentStatusEvent

agentStatusEvent は、特定のエージェントの運用上のイベントについて情報を提供し、通知するために、Tivoli Autonomous Agent SNMP Event Exporter によって生成された、モニター・エージェントの作動状況情報トラップです。

agentSitSampledEvent

サンプリングされたシチュエーション・イベントが検出されました。このトラップは、データのサンプリング時にシチュエーションしきい値を超えたことに対する応答として、Tivoli Autonomous Agent SNMP Event Exporter によって作成されました。

agentSitPureEvent

ピュア・シチュエーション・イベントが検出されました。このトラップは、

シチュエーションしきい値を超えたことに対する応答として、Tivoli Autonomous Agent SNMP Event Exporter によって生成されました。ピュア・イベント・トラップ内の変数は、ピュア・イベントがサンプリングされず、agentSit-SampleInterval が存在しない場合を除き、サンプリングされたイベント・トラップの変数と同一です。モニター対象の属性グループから非送信請求データが着信すると、シチュエーションは true になります。例えば、属性グループを使用してシステム・ログ用に作成されたシチュエーションは、ログ項目を受信すると、ピュア・イベントを開きます。

SNMP 用の OMNIbus 構成

Tivoli Enterprise Monitoring Agent および Tivoli System Monitor Agent からシチュエーション・イベントの SNMP アラートを受け取るように IBM Tivoli Netcool/OMNIbus 環境を構成する必要があります。 Tivoli Monitoring Agent DVD インストール・メディアには、プローブ構成に追加する管理情報ベース (mib) およびサンプル・ルール・ファイルがあります。

SNMP アラートを受信するための OMNIbus の構成

Tivoli モニター・エージェントのシチュエーション・イベントの SNMP トラップおよび SNMP インフォームを受け入れるように SNMP プローブ を構成します。

始める前に

IBM Tivoli Monitoring V6.2.2 以降 Agent DVD を使用可能にします。 Tivoli Netcool/OMNIbus V7.x がインストールされており、SNMP プローブ がインストールされていることを確認します。

同じシチュエーションに対するイベントを ハブ・モニター・サーバー から Netcool/OMNIbus Probe for Tivoli EIF に転送するよう構成されている場合、SNMP プローブ に SNMP アラートを発行するようエンタープライズ・シチュエーションを構成しないでください。OMNIbus の非重複化ではこれらが同じイベントであることを検出しないためです。

このタスクについて

Tivoli Monitoring Agent からシチュエーション・イベントの SNMP アラートを受信できるように OMNIbus 環境を準備するには、次のステップを実行します。

手順

1. Tivoli Monitoring ルール・ファイルおよびルックアップ・ファイルをコピーします。
   a. Tivoli Monitoring V6.2.2 以降 Agent インストール・メディアの `mibs/sample_rules/omnibus` ディレクトリーを見つけます。
   b. SNMP プローブ がインストールされているコンピューター上の `$OMNIHOME/probes/arch/` にこれらの管理情報ベース (MIB)・ファイルをコピーします。
      `ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules`
      `ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup`
2. SNMP プローブ が使用しているルールのファイルを参照します。

a. テキスト・エディターでデフォルトのルール・ファイルを開きます。 mttrapd プロパティー・ファイルで指定されていない限り、デフォルトのルール・ファイルは、$OMNIHOME/probes/*arch*/mttrapd.rules です (ステップ 3)。

b. 最初の定義としてルックアップ・テーブル参照を追加します。

```
include "<path_to_lookup_file>/
ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup"
```

テーブル定義は、処理ステートメントの前にルール・ファイルの先頭に表示される必要があります。このステートメントを mttrapd.rules に追加する場合は、ファイルの先頭にあるコメントと最初の処理ステートメントの間にステートメントを配置します。完全修飾ファイル名は二重引用符で囲む必要があります。%OMNIHOME% または $OMNIHOME などの環境変数を使用できます。/ (スラッシュ) を使用してパスを区切る Linux および UNIX のファイル名の規則も Windows で使用されます。

c. 処理する順序でルール参照を追加します。

```
include "<path_to_rules_file>/
ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules"
```

このステートメントは、処理を実行する場所のルール・ファイルに追加する必要があります。例えば、デフォルトの mttrapd.rules ファイルに include を追加する場合、まず「SNMPv2 トラップであるかどうかを確認し、SNMPv1 スタイル・トークンに変換する」というデフォルトのルールが必要です。デフォルトの mttrapd.rules の次のコード・ブロックでは、汎用トラップを処理します。ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules の include 文がこの後に続きます。mttrap.rules の最後の行となる可能性があります。SNMP プローブ およびイベント・スペースに精通しているユーザーには、ルールをインクルードする場所がよくわかります。

3. SNMP プローブ プロパティー・ファイルを検討し、編集します。

a. テキスト・エディターで $OMNIHOME/probes/*arch*/mttrapd.props を開きます。

b. Protocol プロパティーを "UDP" または "ALL" に設定します。 Tivoli Monitoring SNMP アラートは、UDP を使用して送信されます。

c. プローブのデフォルトのルール・ファイルが mttrapd.rules ではない場合、RulesFile プロパティーを設定します。

d. MIBDirs プロパティーを mib ファイルがあるパスに設定します。

4. Tivoli Monitoring mib ファイルを SNMP プローブ から使用できるようにします。

a. Tivoli Monitoring インストール・メディアで mibs ディレクトリーを見つけます。

b. canbase.mib および cansyssg.mib を MIBDirs プロパティーによって mttrapd.props に指定されている mib の場所にコピーします。

c. canbase.mib および cansyssg.mib には共通の SNMP mib が含まれます。また、これらの mib は SNMP プローブで使用可能である必要があります。
RFC1155-SMI
RFC1213-MIB
SNMPv2-TC
RFC-1212

RFC-1215
これらの mib が MIBDirs プロパティーによって指定された mttrapd.props の場所にまだ存在しない場合、これらのファイルは公開されているので、インターネットからダウンロードしてください。

5. Tivoli Monitoring、Tivoli Business Service Manager、および Netcool/OMNIbus を統合中である場合、Netcool/OMNIbus SNMP プローブ ルールには、OMNIbus **BSM_Identity** 属性を設定する tbsm_snmp_event.rules という追加のファイルを含める必要があります。 Tivoli Monitoring Agent インストール・メディア (V6.2.2 以上) 上の mibs/sample_rules/omnibus/tbsm ディレクトリーには、tbsm_snmp_event.rules ファイルおよび README ファイルがあります。この README ファイルには、SNMP プローブ との使用方法および itm_tbsm_update.sql ファイルを使用して Netcool/OMNIbus データベース・スキーマに **BSM_Identity** 属性を追加する方法が説明されています。

タスクの結果

これで、プローブ・システムにこれらのファイルがインストールされました。

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup

Tivoli Monitoring インストール・メディアで提供される can*.mib ファイル

次のタスク

新しいルールをアクティブ化し、Tivoli Monitoring Agent からのアラートの受信を開始するには、SNMP プローブ をリサイクルします。

SNMP アラートの OMNIbus ルールのサンプル

IBM Tivoli Monitoring V6.2.2 以降 Agent インストール・メディアには、Netcool/OMNIbus SNMP プローブ 構成に追加するルール・ファイルのサンプルが含まれています。

Tivoli Monitoring SNMP トラップ mib

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules ファイルには、IBM Tivoli Monitoring SNMP トラップ変数を、OMNIbus のデフォルトの alerts.status フィールドにマッピングするサンプルが含まれています。

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.lookup ファイルには以下のテーブルが含まれています。

SituationCategory は、Tivoli Monitoring の **$autoSit-Category** を OMNIbus の **@AlertGroup** にマップします。

SituationSeverity は、Tivoli Monitoring の **$autoSit-Severity** を OMNIbus の **@Type** (1 - 問題、2 - 解決、および 13 - 情報) にマップします。また、autoSit-Severity=0 消去トラップの重大度を 1 に変更することにより、OMNIbus generic_clear 自動化でイベントを関連付けることができるようにします。

SituationSource は、シチュエーションが Tivoli Enterprise Monitoring Server で定義されているエンタープライズ・シチュエーションであるか、エージェントのインストール・ディレクトリー *<tema_install_dir>*/localconfig/*kpc* にある専

用シチュエーション構成ファイルで定義されている専用シチュエーションであるかを識別する **$agentSit-Source** を列挙します。次の表は、イベント・クラスの決定にも使用されます。

@Identifier および @AlertKey の作成に関する注

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules は、Tivoli Netcool/OMNIbus Deduplication Automation および Generic Clear Automation を使用します。これらのオートメーションは、ID フィールドおよびアラート・キー・フィールドなどのいくつかのアラート・フィールド (それぞれ最大 255 文字) を使用します。ID アラート・フィールドを SNMP アラートに設定するための Netcool/OMNIbus ルール・ファイル標準は、以下のとおりです。

```
@Identifier = @Node + " " + @AlertKey + " " + @AlertGroup + " " + @Type + " "
+ @Agent + " " + @Manager + " " + $specific-trap
```

アラート・キーは、ID の構成に使用される情報に含まれているため、ID の作成に 255 文字のアラート・キーが使用されると、切り捨てが発生する恐れがあります。

ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rule では、以下のように実装されています。

```
@Identifier = @Node + " " + @AlertKey + " " + $autoSit-Category + " " + @Type  +
" " + @Agent + " " + @Manager + " " + $specific-trap
```

$autoSit-Category は @AlertGroup (24 バイト) の列挙であり、最終の ID で 23 バイトを節約するために @AlertGroup の代わりに使用されます。以下は、ID を構成するために使用されるコンポーネントの最大フィールド長です。

フィールド	サイズ
@Node の最大長	32
$autoSit-Category の固定長	1
@Type の最大長	2
@Agent の最大長	31
@Manager の固定長	13
$specific-trap の固定長	2
6 個のスペース区切り文字	6
合計	87

これにより、@AlertKey には 168 文字 (255-87=168) が残ります。 @AlertKey が $agentSit-Name + " (" + $sitDisplayItem + ")" として定義されている場合、$sitDisplayItem は 133 文字 (168-35=133) 未満でなければなりません。

フィールド	サイズ
agentSit-Name	32
スペース区切り文字	1
括弧	2
合計	35

ベスト・プラクティスは、$sitDisplayItem を 128 文字に制限して、IBM Tivoli Monitoring EIF プローブ・ルールとの整合性を維持することです。サンプル・ルールでは、以下を使用してこのサンプル・ルールを実施します。

```
$sitDisplayItem=substr($sitDisplayItem, 1, 128)
```

ピュア・イベントを生成する属性グループ (例えば、イベント・ログ) 用に作成されたシチュエーションでは、$agentSit-Name を使用して重複を避けることができます。ただし、多くのシチュエーションでは、イベントを一意に識別するための追加情報が必須となります。この追加データを構成するには、$sitDisplayItem 属性を使用します。この場合、アラート・キーは以下のようになります。

```
$agentSit-Name + " (" + $sitDisplayItem + ")"
```

特定のテーブルに基づくすべてのイベントを識別するには、$agentSit-Table フィールドに基づく case ステートメントを使用します。

固有の $sitDisplayItems が個々のシチュエーションに必要な場合は、$agentSit-Name に基づく case ステートメントを使用します。

extract コマンドを使用すると、regex のパターン・マッチングを使用して、$sitAttributeList から任意の名前と値のペアの値を抽出することができます。サンプル・ルールには、NTEVTLOG の $agentSit-Table に基づく agentSitPureEvent トラップの例が提供されています。

```
$sitDisplayItem=extract($sitAttributeList,"Description=.(.+).;.*?")
```

このコマンドは、Description キーの値を抽出して、引用符を削除します。

互換性に関する注

@ExtendedAttr

OMNIbus V7.2 以上は、ObjectServer で @ExtendedAttr 列を定義します。**nvp** 関数は、@ExtendedAttr アラート・フィールド内の名前と値のペアの操作を可能にするために提供されています。sitAttributeList varbind は、@ExtendedAttr への直接マッピングが可能になるようにフォーマットされていますが、この関数は、MTTRAPD プローブが OMNIbus ObjectServer V7.0 または V7.1 に接続するときにルールによって構文解析できるようコメント化されています。イベントを OMNIbus V7.2 以上に転送する場合は、ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules ファイル内の、@ExtendedAttr を設定している次の 2 行をアンコメントしてください。

```
#            @ExtendedAttr = $sitAttributeList
```

@Class

@Class アラート・フィールドは、Tivoli Netcool/OMNIbus Tools を、Tivoli Netcool/OMNIbus EventList に表示されるイベントと関連付けるために使用されます。

Tivoli Netcool/OMNIbus 7.2x 以下の場合、クラスの作成と編集について詳しくは、Netcool/OMNIbus の資料を参照してください。デフォルトでは、これらのクラスの値は、ご使用の ObjectServer では定義されていません。

OMNIbus ObjectServer で定義されていない値に @Class を設定しても問題はありませんが、@Class を設定したくない場合は、イベントが OMNIbus に転送される前に、ibm-TIVOLI-CANSYSSG-MIB.include.snmptrap.rules ファイルの以下の行をアンコメントして、@Class フィールドをクリアしてください。# @Class = ""

OMNIbus ハートビート自動化機能を有効にする

Tivoli Enterprise Monitoring Agent が SNMP アラートまたは EIF イベントとしてシチュエーション・イベントを Netcool/OMNIbus に送信する場合は、OMNIbus 自動化機能を有効にして、EE_HEARTBEAT が延滞したときにイベントが送信されるようにできます。EE_HEARTBEAT ライフサイクル状況イベントは、モニター・エージェントが実行されており、アラートが宛先に到達可能であることを確認するために、ある一定の間隔で受信側に送信されます。

このタスクについて

SNMP および EIF からの HEARTBEAT イベントは、着信すると、OMNIbus イベント・コンソールに表示されます。新規イベントがエージェントから着信すると、カウントが増えます。

itm_heartbeat.sql ファイルには、EIF と SNMP の両方のオートノマス・エージェント・ハートビートを処理する自動化機能のサンプルが含まれています。自動化を有効にするには、この SQL ファイルを実行します。

手順

1. itm_heartbeat.sql を Tivoli Monitoring Agent DVD mibs/sample_rules/omnibus ディレクトリーからコピーします。
2. そのコピーを Netcool/OMNIbus インストール・パスに置き、以下のコマンドを実行します。
   - Windows ここで、『*user*』 は有効なユーザー名、『*password*』 はそれに対応するパスワード、『*server*』 は ObjectServer 名です。

     ```
     %NCHOME%¥bin¥redist¥isql.exe -U "user" -P "password" -S "server"
     < itm_heartbeat.sql
     ```

   - Linux UNIX ここで、『*servername*』 は ObjectServer 名、『*username*』 は有効なユーザー名、および 『*psswrd01*』 はそれに対応するパスワードです。

     ```
     $NCHOME/omnibus/bin/nco_sql -server servername -user username
      -password psswrd01 < itm_heartbeat.sql
     ```

タスクの結果

OMNIbus 自動化機能がインストールされた後、ハートビートが着信すると、自動化機能によって管理対象システムからのハートビートが登録されます。個々のハートビートはイベント・コンソールで表示されたりカウントされたりしなくなりましたが、予想されるハートビートが延滞すると、自動化機能によって以下を含む「ハートビートが欠落しています」というアラートが発せられます。

```
Summary = 'Heartbeat Missed for:' + heartbeat_missed.Node +
' last received at ' + to_char(heartbeat_missed.LastOccurrence)
```

次のタスク

EE_HEARTBEAT 状況を送信するデフォルトの間隔は 15 分です。この値を調整するには、SNMP アラート用の trapcnfg.xml ファイルと EIF イベント構成ファイル用の eifdest.xml ファイルで、ハートビート状況イベントの間隔属性を変更します。

特に SNMP の場合は、ハートビートが 1 つ欠落しても、そのことが必ずしも問題を示しているわけではないため、デフォルトでは、ハートビートが「(2 x ハートビート間隔) + 2 分」の延滞を起こした後にアラートを発します。これは、itm_heartbeat.sql 内で次の項目を使用して編集できます。

```
-- 2 heartbeats plus 2 minutes grace before agent missed
    set time_of_expiry = (new.ExpireTime * 2 * 60 + 120) + getdate();
```

例えば、さらに 2 分を追加すると、設定は次のようになります。

```
-- 2 heartbeats plus 4 minutes grace before agent missed
    set time_of_expiry = (new.ExpireTime * 2 * 60 + 240) + getdate();
```

EIF イベント

Tivoli Enterprise Monitoring Server を経由せずに、Tivoli Monitoring Agent から EIF 受信側に専用シチュエーション・イベントを直接送信します。

EIF イベント構成

モニター・エージェントとローカル EIF イベント構成 XML ファイルを構成して、ライフサイクル・イベントまたは専用シチュエーション・イベント、またはその両方を、IBM Tivoli Enterprise Console イベント・サーバーや Netcool/OMNIbus Probe for Tivoli EIF など 1 つ以上の EIF 受信側に送信します。

制約事項: iSeries® エージェントからイベントを直接送信するための EIF は、iSeries 上ではサポートされていません。

使用上の注意: 下のコード例では、以下の置換が使用されています。

- `<install_dir>` は、IBM Tivoli Monitoring がインストールされているディレクトリーです。
- `<pc>` は、小文字でのエージェントの 2 文字の製品コードです。
- `<PC>` は、大文字でのエージェントの 2 文字の製品コードです。

EIF イベント構成

IRA_EVENT_EXPORT_EIF 環境変数のデフォルト設定は Y で、これにより、エージェントの開始時に EIF エミッターが開始します。 EIF イベント転送を実行する前に、モニター・エージェントがインストールされているシステム上に、次のファイルが存在し、構成されている必要があります。

- 比較基準が true に評価される場合に、イベントを生成するシチュエーションを定義する、専用シチュエーション構成ファイル。専用シチュエーションは、エージェントの開始および終了手順の一部として開始および停止します。
- EIF 送信済みイベントを受信するイベント・リスナーを定義する、イベント宛先構成ファイル。

さらに、EIF 受信側に送信するイベント・データを制御する、イベント・マッピング・ファイルも使用できます。

エージェント・パラメーター

エージェント環境ファイルの **IRA_EVENT_EXPORT_EIF=Y** パラメーターを設定して、EIF イベント・エクスポート機能を有効にします。機能を無効にするには、値を **N** に変更します。

エージェント環境ファイルの **IRA_EIF_DEST_CONFIG=<filename>** パラメーターを設定して、EIF 宛先構成 XML ファイルの場所を指定します。デフォルトは <install_dir>/localconfig/<pc>/<pc>_eventdest.xml です。

エージェント環境ファイルの **IRA_LOCALCONFIG_DIR** パラメーターを設定して、EIF 宛先用またはオプションのイベント・マッピング・ファイル、あるいはその両方に別のディレクトリー・パスを指定できます。デフォルトは、<install_dir>/localconfig/<pc> です。

エージェント環境ファイルの **IRA_EIF_MSG_LOCALE=en_US** パラメーターは、デフォルトでは米国英語に設定されています。事前定義されたマッピング・ファイルおよび言語リソース・バンドルを使用して生成されたイベント内のメッセージ・スロットに対してグローバル化されたメッセージ・テキストをサポートするエージェントの場合、デフォルトの言語ロケールを指定できます。

エージェント EIF イベント宛先構成 XML 仕様

EIF イベント宛先 XML ファイルを使用して、イベント宛先サーバーとその構成を指定します。ルート要素は <EventDest> で、<Destination> および <Server> 要素と、オプションの <StatEvent> 要素が含まれ、EIF ハートビート間隔 (エージェントがハートビート・イベントを EIF 受信側に送信する頻度) を構成します。

イベント宛先構成ファイルは、次のデフォルトの場所にあります。

Windows <install_dir>¥localconfig¥<pc>¥<pc>_eventdest.xml

Linux UNIX <install_dir>/localconfig/<pc>/<pc>_eventdest.xml

z/OS RKANDATV、(メンバー名 <PC>EVDST で)

エージェント EIF イベント・マッピング構成 XML 仕様

オプションの EIF イベント・マッピング・ファイル構成 XML ファイルを使用して、生成された EIF イベントをカスタマイズできます。イベント・マッピング・ファイルが提供されていない場合、イベントは汎用マッピングによってフォーマットされます。イベント・マッピング・ファイルは、製品によって提供されるか、ユーザーが定義します。ユーザー定義のイベント・マッピング (ある場合) は、製品が提供するマッピングより優先されます。事前定義イベント・マッピング・ファイルの名前と場所 (ある場合):

Windows <install_dir>¥TMAITM6¥EIFLIB¥k<pc>.map (32 ビット・エージェント)、<install_dir>¥TMAITM6_x64¥EIFLIB¥k<pc>.map (64 ビット・エージェント)。

Linux UNIX <install_dir>/<platform>/<pc>/tables/EIFLIB/k<pc>.map

z/OS RKANDATV、(メンバー名 K<PC>MAP で)。

ユーザー定義のイベント・マッピング・ファイルを作成した場合、次の場所に保管されます。

Windows <install_dir>¥localconfig¥<pc>¥<pc>_eventmap.map

Linux UNIX <install_dir>/localconfig/<pc>/<pc>_eventmap.map

z/OS RKANDATV、(ファイル名 <PC>EVMAP で)

イベント・マップ構成ファイルのサンプル:

```
<?xml version="1.0" encoding="UTF-8"?>
<itmEventMapping:agent>
   <event_mapping>
      <situation name="Flipper*" mapAllAttributes="Y">
         <class name="ITM_ABC"/>
            <slot slotName="msg">
               <literalString value="The time now is
               $Local_Time.Timestamp.TIMESTAMP$ on $hostname$"/>
            </slot>
      </situation>
   </event_mapping>
</itmEventMapping:agent>
```

EIF イベント受信側に送信されるエージェントのハートビート・イベントのオンライン状況

EventDest 構成 XML ファイルには、ハートビート間隔を指定するオプションの要素があります。各間隔後に、エージェント状況がテストされ、結果がオンライン - オフライン状況として、EventDest ファイルで指定された EIF 受信側に送信されます。

バージョン 6.2.2 フィックスパック 1 より前にインストールされた Tivoli Enterprise Monitoring Agent

Tivoli Monitoring バージョン 6.2.2 フィックスパック 1 以降 の OS エージェントがインストールされている場合、そのコンピューターにインストールされているすべての Tivoli Enterprise Monitoring Agent は、バージョン 6.2.2 フィックスパック 1 より前にインストールされた場合であっても、オートノマス EIF イベント転送機能を使用できます。ただし、バージョン 6.2.2 フィックスパック 1 より前にインストールされたモニター・エージェントには、エージェント・インストール・バンドルには含まれていないが Tivoli Enterprise Monitoring Server のインストールで提供されているアプリケーション・サポートに含まれる一部のファイル (baroc ファイル、オプションのイベント・マッピング・ファイル、およびリソース・バンドル・ファイル) が必要になります。これらの以前のバージョンのエージェントで、EIF 機能を使用してイベントを転送するには、次の手順を実行する必要があります。

1. モニター・サーバー環境に以前のバージョンのエージェントをインストールして、baroc ファイルとオプションのイベント・マッピング・ファイルにアクセスします。エージェントの事前定義 baroc ファイルとオプションのイベント・マッピング・ファイルは、<install_dir>/CMS/TECLIB または <install_dir>/CNPS/teclib ディレクトリーにあります。
2. 提供されている k<pc>.map イベント・マッピング・ファイル (ある場合) を、エージェントのインストールの EIFLIB ディレクトリーにコピーします。
3. Tivoli Enterprise Console event server がイベント受信側として使用されている場合、各エージェントについて、baroc ファイルをイベント・サーバーがインストールされているシステムにコピーします。イベント・サーバーで baroc をコンパイルおよびロードします。

z/OS のハブ・Tivoli Enterprise Monitoring Server・アドレス・スペース内で実行されているエージェント

z/OS システムでは、ハブ・モニター・サーバーの同一アドレス・スペース

内で実行するようにエージェントを構成できます。 EIF イベント転送機能 (OTEA) はハブ・モニター・サーバーでも使用可能にできるため、ハブ・モニター・サーバーでのイベント転送機能とモニター・エージェントから直接エクスポートされた EIF イベントとの相互干渉を避けるために、しかるべき予防措置を取る必要があります。オーバーラップする可能性のある領域の 1 つとして、カスタム・イベント・マッピング・ファイルがあります。現在ハブ・モニター・サーバーでは、(Tivoli Enterprise Portal シチュエーション・エディターで作成してモニター・サーバー表に保管できるものに加えて) 独自のイベント・マッピングをコード化できます。これらのマッピング・ファイルの名前は **Q<xx>MAP** 形式 (<xx> は任意の 2 文字の英数字) で、RKANDATV データ・セットに配置される必要があります。オートノマス・エージェントに対してユーザー定義イベント・マッピング・ファイルをサポートするには (これも、RKANDATV データ・セットにあります)、別の命名規則を使用する必要があります。オートノマス・エージェントのユーザー定義イベント・マッピング・ファイルのファイル命名規則は、**<pc>EVMAP** です (<pc> は 2 文字のエージェント製品コードです)。

EIF イベント・マッピング XML 仕様

EIF イベント・マッピングは、1 つ以上の専用シチュエーションのイベントの変換方法を指定する XML ファイルです。カスタム・イベント・マッピング・ファイルを作成して、EIF 受信側に送信するデータを変更します。

イベント・マッピング・ファイル・フォーマット

```
<itmEventMapping:agent>
  <id>xx</id>
  <version>n.n</version>
  <event_mapping>
    <situation>
      <slot>
        <mappedAttribute/>
          または
        <mappedAttributeEnum/>
          または
        <literalString/>
      </slot>
      :    1 つ以上のスロット・タグ
    </situation>
```

または

```
    <attributeTable>
      <slot>
        <mappedAttribute/>
          または
        <mappedAttributeEnum/>
          または
        <literalString/>
      </slot>
      :    1 つ以上のスロット・タグ
    </attributeTable>
  </event_mapping>
</itmEventMapping:agent>
```

要素

XML タグは大/小文字を区別しません。他のすべてのパラメーターには大/小文字の区別があります。

<itmEventMapping:agent>

itmEventMapping:agent は、これをモニター・エージェントのイベント・マッピング定義として識別するルート要素です。

<id> 構文:

```
<id>pc</id>
```

ID は、2 文字の製品コードです (UNIX OS エージェントの場合は「UX」)。ユーザー定義のイベント・マップの場合は、ID に「99」を使用することが推奨されます。

<version>

構文:

```
<version>nnnn</version>
```

オプションです。 この要素を使用して、イベント・マッピング・ファイルのバージョンを指定します。

<valueList>

構文:

```
<valueList name="valueListName">
```

オプションです。 valueList 要素を使用して、1 つ以上の値項目の値リストを定義します。*valueListName* は、リストの名前です。

<valueItem>

構文:

```
<valueItem name="item_value">
```

この要素は、valueList を定義する場合に必要です。 ValueItem は、指定された valueList の有効な項目値を指定します。

<event_mapping>

構文:

```
<event_mapping>
```

event_mapping 要素は、マッピング・エントリーのグループを囲みます。

<situation>

構文:

```
<situation name="situation_name" [mapAllAttributes="Y"]
```

シチュエーション要素は、キーが situation_name の DM マッピング・エントリーを指定します。 situation_name ストリングには、ワイルドカード文字 (* アスタリスクと ? 疑問符) を含めることができます。ただし、先頭文字位置には使用できません。

mapAllAttributes=『Y』 は EIF イベント転送機能に、このマッピング・エントリー内の <slot> タグで明示的に指定されたスロットを除き、

汎用マッピングのように EIF イベント・スロットを作成するように指示します。この属性は、イベントの少数のスロットのみをカスタマイズする必要がある場合 (msg スロットなど) に便利です。これにより、すべてのスロットを EIF イベントに含めるように明示的に指定する必要が緩和されます。

<attributeTable>

構文:

```
<attributeTable name="attribute_table_name"
 [truncated="Y"] [freeSpace="nnnn"]
```

truncated=『Y』 により、「ITM Agent: Private Situation」ではなく「ITM_Agent: Private Situation: Truncated」が EIF イベントの「source」スロットに割り当てられます。これは、イベント・マッピング・ジェネレーターで定義されたサイズ制限により、イベント・データ内の一部の属性が EIF イベントに入りきらないことを示すインディケーターです。

freeSpace=『*nnnn*』 は、このイベント・マップで定義されたすべてのスロットが作成された後に、イベント・マッピング・ジェネレーターによって EIF イベント・バッファーで使用できる最大サイズとして決定された値です。 EIF イベント・エミッターはこの値を使用して、situation_eventdata スロットに含める未加工イベント・データの量を決定します。

<class>

構文:

```
<class name="eif_class_name" [valueList="valueList_name"]
 [defaultClass="default_eif_class_name"]>
```

name= は、生成された EIF イベントに使用する EIF クラス名を指定します。 eif_class_name ストリングに置換変数 (属性名) を含めて、EIF クラス名を生成できます。ランタイム中に指定された属性の値によっては、動的になります。 429 ページの『動的 EIF クラス名』を参照してください。

valueList= は valueList を指定して、動的 EIF クラス名生成を検索します。

defaultClass= は、eif_class_name ストリングに置換変数が含まれるが、指定された valueList に属性値と一致する項目がない場合に、EIF イベントに使用するデフォルトの EIF クラス名を指定します。

<slot> 構文:

```
<slot name="slot_name">
```

オプションです。 EIF イベントのスロットを定義します。スロットの名前は *slot_name* です。

<mappedAttribute>

構文:

```
<mappedAttribute name="attribute_name" [multiplier="nnn"]>
```

オプションです。 定義されるスロットの値ソースを指定します。使用可能な場合、これはイベント・データ内の attribute_name という名前の属性の

値です。それ以外の場合、ヌル値が使用されます。multiplier= 属性が指定されていて、属性値が数値の場合、スロットに割り当てられる値は、指定された数値で乗算された属性値です。

<mappedAttributeEnum>

構文:

```
<mappedAttributeEnum name="attribute_name">
```

オプションです。 MappedAttributeEnum は、属性が属性ファイルで列挙として定義されている場合、未加工の属性値ではなく列挙された表示テキストがスロット値として使用される点を除き、mappedAttribute タグと似ています。属性値と一致する列挙された表示テキストが定義されていない場合、未加工の属性値が使用されます。

<literalString>

構文:

```
<literalString value="text">
```

オプションです。 テキストは、定義されるスロットの値として使用します。「msg」スロットを定義する場合、テキスト内で変数置換を指定できます (次で説明します)。

カスタム msg スロット

msg スロットの値がリテラル・ストリング (<literalString> 要素) として定義されている場合、置換変数を含めることができます。置換変数は、$variable$ 構文で指定されます。msg スロットをフォーマットすると、EIF イベント転送機能は $variable$ シンボルをその置換値に置き換えます。

有効な変数:

$AttrGroup.Attribute$

属性置換には、完全修飾名が必要です (すなわち、ピリオドで区切られた属性グループと属性名の両方)。変数トークンは、イベント・データ内の指定された属性の値で置き換えられます。指定された属性がイベント・データにない場合、ヌル・ストリングが使用されます。

$AttrGroup.Attribute.TIMESTAMP$

これは $AttrGroup.Attribute$ 構文と同じですが、**.TIMESTAMP** サフィックス修飾子が付いています。これによって、属性値がタイム・スタンプ (属性ファイルでタイム・スタンプ・タイプとして定義されたもの) で、表示可能なタイム・スタンプ・フォーマット (MM/DD/YYYY HH:MM:SS) でフォーマットする必要があることを、EIF イベント転送機能に示します。属性値が有効なタイム・スタンプでない場合、未加工の属性値が使用されます。

$slotname$

イベント・スロット置換では、イベント・マッピングの実行後に、変数トークンを指定されたスロットの値に置き換えます。

次に、msg スロットが DM パリティー用にカスタマイズされた、定義済みイベント・マッピング・ファイルから取得した例を示します。

```
<slot slotName="msg">
  <literalString value="Distributed Monitoring $sub_source$/$monitor$
  on host $hostname$ $NT_LogicalDisk.Timestamp$"/>
</slot>
```

sub_source および monitor スロットの値に、値「tmpdisk」および「Disk Read Bytes/sec」がある場合、msg スロット・テキストは次の例のようになります。

```
Distributed Monitoring tmpdisk/Disk Read Bytes/sec on host
 elaix04 08/14/2009 10:23:11
```

動的 EIF クラス名

EIF イベント・クラス名は、**<class>** 要素の **name=** 属性によって定義されます。EIF クラス名ストリングには、EIF クラス名の動的生成用の置換変数を含めることができます。置換変数は、EIF クラス名ストリング内の先頭以外の任意の場所に置くことができます。置換変数には、$attributeGroup.attribute$ の構文があります。ランタイム中に、EIF イベント転送機能は指定された valueList (ある場合) で、置換変数で指定された属性の値があるかどうかを検索します。 valueList で属性値が見つかった場合、変数 (および区切りの $ 記号) は EIF クラス名ストリングで属性値 (正規化後) に置き換えられます。 valueList で一致が見つからない場合、または指定された valueList が定義されていない場合、**defaultClass=** 属性で定義された EIF クラス名がイベントの EIF クラス名として使用されます。**defaultClass=** が指定されていない場合、EIF クラス名の変数はヌル・ストリングに置き換えられます。

変数が数値属性を参照する場合、スケーリングまたは精度操作は実行されません。シチュエーション・イベント・レコードの数値フィールドのストリング表記が、何も調整されずに使用されます。変数が列挙型属性を参照する場合、列挙のテキスト表記が変数の値として使用されます。

シチュエーションが true でない場合 (ステータスが 『Y』 でない場合)、シチュエーション状況レコードにイベント属性データは含まれません。そのため、クラス名の置換変数値を決定する方法はありません。 EIF イベント転送機能は **defaultClass=** 属性を使用します (指定されている場合)。それ以外の場合、同じシチュエーション名に最後に送信された EIF イベントの EIF イベント・クラスを使用します。

これは、『Message_Number』 属性の値に基づいて、シチュエーション・イベント『Test_Syslog』 を一連の EIF イベントにマッピングするために使用する、サンプル・イベント・マッピング定義に関連がある部分です。

```
<situation name="Test_Syslog">
  <class name="SAP_Syslog_$R/3_System_Log.Message_Number$"
  valueList="SyslogIDList" defaultClass="SAP_Syslog_Default" />
  :
  :
</situation>
```

この例には、値項目 AB0、AB1、A08、BV7、EAS、および R45 を持つ「SyslogIDList」値リストと、メッセージ ID AB0、AB1、AB2、BV7、および BV8 をモニターする「Test_Syslog」シチュエーションがあります。「Test_Syslog」シチュエーションは、これらの各メッセージ ID に対して true に評価されます。生成される EIF イベントは次のクラスになります。

1. AB0: SAP_Syslog_AB0 x
2. AB1: SAP_Syslog_AB1
3. AB2: SAP_Syslog_Default
4. BV7: SAP_Syslog_BV7
5. BV8: SAP_Syslog_Default

属性値の正規化

EIF イベント・クラス名内の変数は、イベントの任意の有効な属性を参照できますが、その値に、EIF イベント・クラス名で使用するには有効でない文字が含まれる可能性があります。イベント・クラス名で変数置換を実行する前に、EIF イベント転送機能はすべての UTF-8 マルチバイト文字および無効な文字を単一の _ 下線に置き換えます。例えば、空白文字、< > ( ) & / は _ 下線に置き換えられます。

例

```
<itmEventMapping:agent
  xmlns:itmEventMapping="http://www.ibm.com/tivoli/itm/agentEventMapping"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ibm.com/tivoli/itm/agentEventMapping
  agentEventMap.xsd">

  <id>NT</id>
  <version>6.2.0</version>
  <event_mapping>
    <situation name="NT_LDDBPS*">
      <class name="w2k_LogDskDskBytesPerSec"/>
      <slot slotName="source">
        <literalString value="SENTRY"/>
      </slot>
      <slot slotName="probe">
        <literalString value="DskBytesPerSec"/>
      </slot>
      <slot slotName="probe_arg">
        <mappedAttribute name="NT_Logical_Disk.Disk_Name"/>
      </slot>
      <slot slotName="collection">
        <literalString value="w2k_LogicalDisk"/>
      </slot>
      <slot slotName="monitor">
        <literalString value="Disk Bytes/sec"/>
      </slot>
      <slot slotName="units">
        <literalString value="(per second)"/>
      </slot>
      <slot slotName="value">
        <mappedAttribute name="NT_Logical_Disk.Disk_Bytes/Sec"/>
      </slot>
      <slot slotName="effective_value">
        <mappedAttribute name="NT_Logical_Disk.Disk_Bytes/Sec"/>
      </slot>
      <slot slotName="msg">
        <literalString value="Distributed Monitoring $sub_source$/Disk
        Bytes/sec on host $hostname$ $NT_Logical_Disk.Timestamp.TIMESTAMP$"/>
      </slot>
    </situation>
  </event_mapping>
</itmEventMapping:agent>
```

Tivoli Monitoring Agent インストール・メディアの PrivateConfigSamples/EIF ディレクトリーに同じ EIF ファイルのサンプルが提供されています。

EIF イベント宛先構成 XML 仕様

EIF 宛先 XML ファイルで EventDest、Server、および Destination 要素を使用し、モニター・エージェントによって送信される EIF イベントの宛先を構成します。

要素

要素およびその属性は大/小文字を区別しません。例えば、
EVENTDEST=、EventDest=、または eventdest= と入力できます。

<EventDest>

EVENTDEST は、モニター・エージェント用のイベント宛先定義として識別するルート要素です。

<Destination>

イベント宛先定義を開始します。宛先索引を指定します。オプションの属性を選択すると、宛先タイプ、デフォルト・サーバー、キャッシュ・ファイルの最大サイズ、開始時にキャッシュ・ファイルをクリアするオプションを指定できます。

id= 必須。宛先索引で、0 から 999 までです。デフォルト: **0**

type= オプション。宛先タイプ: T=IBM Tivoli Enterprise Console、M=Netcool/OMNIbus。生成されるイベントの最大サイズは type=T で 4K、type=M で 32K です。デフォルト: **T**

default= オプション。ここに入力されるサーバーは、デフォルトの宛先として指定されます。デフォルト: **N**

clear_cache= オプション。この属性を使用して、宛先をインスタンス化するときに既存の EIF キャッシュ・ファイルをクリアするかどうかを指定します。clear_cache=Y で、EIF イベント・キャッシュ・ファイルがクリアされます。 z/OS システムでは、z/OS EIF がコア・イベント・キャッシュしかサポートしないため、この EIF イベント・キャッシュは常にクリアされます。デフォルト: **Y**

max_cache_size= オプション。イベント・キャッシュの物理ファイルの最大サイズをキロバイト単位で指定します。デフォルト: **4096**

stat= オプション。宛先がライフサイクル・イベントを受信するかどうかを指定します。デフォルト: **N**

master_reset= オプション。エージェント開始時にマスター・リセット・イベントが送信されるどうかを指定します。デフォルト: **N**

<Server>

宛先のイベント・サーバーを定義します。プライマリー・サーバーは 1 台、セカンダリー・サーバーは 7 台まで定義できます。各イベント・サーバーのホスト名、または IP アドレスとポートを指定します。最初の <サーバー> 定義がプライマリー・リスナーとなります。後続の <サーバー> 定義はバックアップ・サーバーとなります。

location= イベント・リスナーのホスト名または IP アドレスを指定します。

port= オプション。IBM Tivoli Enterprise Console イベント・サーバー、または Netcool/OMNIbus Probe for Tivoli EIF のリスニング・ポートを指定します。IBM Tivoli Enterprise Console イベント・サーバーのデフ

ォルトのポート番号は **5529** です。ただし、Linux や UNIX などのオペレーティング・システムでは **port=0** の設定を IBM Tivoli Enterprise Console で使用すると、イベント・リスナーがポートマッパーを使用していることを示すことができます。EIF プローブのデフォルトのポート番号は、**9998** です。値を指定しない場合は、ポート番号がサーバー・ロケーション定義で **0** にデフォルト設定されます。

SSL= オプション。イベントを暗号化して Secure Sockets Layer (SSL) 接続で送信するか、または暗号化せずに非 SSL 接続で送信するかを指定します。SSL 接続は、Netcool/OMNIbus イベント宛先 (type="M") でのみサポートされています。 IBM Tivoli Enterprise Console イベント宛先 (type="T") で有効に設定されている場合は、デフォルトの非 SSL 接続が使用されます。有効にするには Y を、無効にするには N を指定します。デフォルト: **N**。

<StatEvent>

オプションです。 StatEvent 要素を使用して、エージェントのオンラインまたはオフライン状況をイベント・サーバーに送信します。デフォルトでは、ハートビート・モニターは使用できません。

name= ハートビート・イベントの名前を指定します。

interval= オプション。ハートビート・イベントを送信する間隔 (分単位)。間隔がゼロの場合はハートビートを送信しないことを示します。デフォルト: **15**。

例: どちらのスタンザにも EE_HEARTBEAT というハートビート・イベントの名前がついているとします。最初のスタンザは 5 分間隔で、2 番目のスタンザではハートビート・イベントが使用不可になっています。

```
<StatEvent name="EE_HEARTBEAT" interval="5"/>
```

```
<StatEvent name="EE_HEARTBEAT" interval="0"/>
```

宛先サーバーは、"ITM_Heartbeat" という名前のクラス (値がハートビート間隔である "interval" という名前のスロットを含む) とともに、EIF イベントを受信します。受信された SNMP イベントには、"AlertGroup" 属性 (値は "ITM_Heartbeat") と、"HeartbeatInterval" 属性 (値はハートビート間隔) が含まれています。与えられたハートビート・ルールをカスタマイズしたり、独自のルールを作成してハートビート・イベントを処理することができます。

注: 複数の EE_HEARTBEAT イベントはサポートされていません。EE_HEARTBEAT の受信用に複数の宛先が構成されている場合は、各宛先に同じ EE_HEARTBEAT が送信されます。

例

以下の例は、複数のイベント宛先を含んでいるイベント宛先構成ファイルです。

```
<EventDest>
 <Destination  id="0" type="M" master_reset="Y" stat="Y" default="Y">
  <Server location="server.ibm.com" port="9998" />
 </Destination>
 <StatEvent name="EE_HEARTBEAT" interval="5" />
</EventDest>
```

以下の例は、2 つのイベント宛先を含んでいるイベント宛先構成ファイルです。

```
<EventDest>
 <Destination id="0" type="M" default="Y" master_reset="Y" stat="Y">
  <Server location="omniserver.ibm.com" port="9998" />
 </Destination>
 <Destination id="1" type="T" default="Y" master_reset="Y" stat="N">
  <Server location="tecserver.ibm.com" port="5529" />
 </Destination>
 <StatEvent name="EE_HEARTBEAT" />
</EventDest>
```

ここでは stat パラメーターが "N" に設定されているため、2 番目の宛先はライフサイクル・イベントを受信しません。

以下の例は、2 つのイベント宛先が SSL 接続を使用するように定義されているイベント宛先構成ファイルです。

```
<EventDest>
    <Destination id="0" type="M" default="Y" master_reset="Y" stat="Y" >
        <Server location="server1.ibm.com" port="9998" SSL="Y" />
    </Destination>
    <Destination id="1" type="M" default="Y" master_reset="Y" stat="Y" >
        <Server location="server2.ibm.com" port="9998" SSL="Y" />
        <Server location="server3.ibm.com" port="9998" SSL="N" />
    </Destination>
</EventDest>
```

ここで、2 番目の宛先は、複数のサーバー・ロケーションが定義されており、プライマリー・サーバーには SSL 接続を使用し、セカンダリー・サーバーには非 SSL 接続を使用する場合、同じ SSL 値を使用する必要がないことを示しています。

ヒント: Tivoli Monitoring Agent インストール・メディアの `PrivateConfigSamples/EIF` ディレクトリーに同じ EIF ファイルのサンプルが提供されています。

EIF 発行イベントの共通スロット

EIF 受信側で専用シチュエーションのイベント情報を理解できるよう、共通スロット・セットの記述を確認します。

発行された EIF イベントにはすべて、イベント属性データからのスロットに加え、共通スロットのセットが与えられます。非表示の属性を除き、イベントで使用される属性テーブルで定義された属性はすべて発行イベントに含まれます (イベントおよびスロットの合計サイズ制限の対象となります)。共通スロットのセットについては、以下の表で説明します。

表 35. 発行された EIF イベントの共通スロット・セット

スロット	値と意味
アダプター・ホスト	基本イベント・クラス属性。ホスト名と同じです (以下を参照)。 これは、イベントに関連したアプリケーション固有データです (ある場合)。

表 35. 発行された EIF イベントの共通スロット・セット (続き)

スロット	値と意味
アプリケーション・ラベル	イベントのソースが専用シチュエーションまたはエージェント・オンライン・ステータスからであることを示すために使用します。この値の構文は、以下のとおりです。 **source : sit_type : event_type** ここで **source** は、エージェントでは常に「A」です **sit_type** は、専用シチュエーションの場合は「P」、エンタープライズ・シチュエーションの場合は「E」です **event_type** は、シチュエーション・イベントの場合は「S」、ライフサイクル状況イベントの場合は「L」です 例えば A : P など **注:** エンタープライズ・シチュエーション・イベントでは、appl_label 値は設定されません。そのため、appl_label=A:E:S はありません。
cms ホスト名	エージェント発行イベントでは使用されないか、NULL です。 **注:** Tivoli Enterprise Monitoring Server が EIF 発行イベントでは使用されないため、IBM Tivoli Enterprise Console イベント・サーバーは、専用シチュエーション・イベントがクローズされた後はイベント同期の synch_trace.log ファイルにエラー・メッセージを記録しません。
cms ポート	エージェント発行イベントでは使用されないか、NULL です。
fqhostname	完全修飾ホスト名を含む基本 EVENT クラス属性 (ある場合)。
ホスト名	イベントが発生した管理対象システムの TCP/IP ホスト名を含む基本 EVENT クラス属性 (使用可能な場合)。
統合タイプ	パフォーマンスに役立つインディケーター。 • N は新規イベントを示します (イベントが初めて発生したとき)。 • U は更新イベントを示します (後続のイベント状況の変更)。
マスター・リセット・フラグ	マスター・リセット・イベント用に設定されるマスター・リセット・インディケーター。その他のすべてのイベントの場合、値は NULL です。 • エージェント再始動の場合は R です。 • それ以外の場合は NULL です
メッセージ	カスタマイズを使用せず、シチュエーション名と式を含む基本 EVENT クラス属性。
発信元	イベントが発生した管理対象システムの TCP/IP アドレスに含まれる基本 EVENT クラス属性 (使用可能な場合)。このアドレスは、小数点付き 10 進数の形式です。
重大度	解決された重大度を含む基本 EVENT クラス属性。

表 35. 発行された EIF イベントの共通スロット・セット (続き)

スロット	値と意味
シチュエーションの表示項目	関連するシチュエーションの表示項目 (使用可能な場合)。
シチュエーション・イベント・データ	イベント・データの 2 行目から開始される未加工のシチュエーション・イベント・データ (ある場合)。イベント・データ属性は、キーと値のペア形式です。合計イベント・サイズおよびスロット・サイズの制限が 2 KB のため、イベント・データは切り捨てられる場合があります。
シチュエーションのグループ	シチュエーションがメンバーとなっている、1 つ以上のシチュエーションのグループ名 (5 つ以内)。
シチュエーションのフルネーム	専用シチュエーション用にシチュエーション名が定義されている場合は、その名前を表示します。
シチュエーション名	シチュエーションに与えられた固有 ID。
シチュエーションの発信元	シチュエーション・イベント発信元である管理対象システムの名前。サブソースと同じ値です。
シチュエーションの状況	シチュエーション・イベントの現在の状況は、次のとおりです。 Y: シチュエーションが true の場合 N: シチュエーションが false の場合 P: シチュエーションが停止している場合
シチュエーション・タイム	シチュエーション・イベントのタイム・スタンプ。
シチュエーション・タイプ	シチュエーション・イベント・タイプは、サンプル・イベントの場合は **S**、ピュア・イベントの場合は **P** です。
シチュエーション thrunode	エージェントの管理対象システム名。
ソース	**ITM エージェント: 専用シチュエーション**、または **ITM エージェント: 専用シチュエーション:切り捨て**を含む基本 EVENT クラス属性。
サブ発信元	表示項目の値を含む基本 EVENT クラス属性 (ある場合)。
サブソース	関連するシチュエーションの発信元の管理対象システム名を含む基本 EVENT クラス属性。

EIF ライフサイクル・イベント

シチュエーションの開始や停止や状況イベントの発行に加え、Event Integration Facility イベント・エミッターは専用シチュエーションに関連のないライフサイクル・イベントを生成します。

*EIF ライフサイクル・イベントの表*に示されているように、エージェントやシチュエーションで状態が変更されるとライフサイクル・イベントが発行されます。ハートビート・イベントは、状態変更の発行を必要としないライフサイクル・イベントです。このイベントは通常の間隔で送信され、エージェントが実行していることを確認します。

表 36. EIF ライフサイクル・イベント

イベント	意味
EE_AUTO_ENTER	シチュエーションがオートノマス・モード操作に遷移しました。
EE_AUTO_EXIT	シチュエーションがオートノマス・モード操作を終了しました。
EE_CONFIG_UPDATE	構成ファイルがサーバーから引き出されたときに生成されます。
EE_HEARTBEAT	エージェントのハートビートです。
EE_TEMS_CONNECT	エージェントはモニター・サーバーに接続しています。
EE_TEMS_DISCONNECT	エージェントはモニター・サーバーから切断されました。
EE_TEMS_RECONNECT_LIMIT	エージェントによるモニター・サーバーへの再接続制限を超過しました。
EE_SIT_STOPPED	シチュエーションが停止されました。これはオプションです。 **注:** EIF イベントの situation_status スロットが、停止したシチュエーションのために自動的に P を送信します。

ライフサイクル EIF イベントはすべて Event の派生クラスである ITM_StatEvent であり、以下のスロット値を伴います。

表 37. EIF ライフサイクル・イベント ITM_StatEvent クラスのスロット値

スロット	値
source	ITM エージェント: 状況イベント
appl_label	A:E:L は停止したエンタープライズ・シチュエーション専用、A:P:L はその他専用。
hostname	エージェント・マシンのホスト名または IP アドレス
fqhostname	完全修飾ホスト名 (ある場合)
origin	エージェント・コンピューターの IP アドレス
situation_name	ライフサイクルのステータス値 (EE_AUTO_ENTER など)。ライフサイクル・イベントが EE_SIT_STOP の場合、停止中のシチュエーション名が situation_displayitem スロットに含まれます。
situation_time	ライフサイクル・イベントの発生日時
date	ライフサイクル・イベントの日付
severity	HARMLESS
メッセージ	ライフサイクル・イベントを説明するメッセージ

EIF ハートビート・イベント

Event Integration Facility イベント宛先 XML ファイルに StatEvent 要素を含め、モニター・エージェントのオンラインまたはオフライン状況をイベント・サーバーに送信することができます。与えられたハートビート・ルールをカスタマイズしたり、独自のルールを作成してハートビート・イベントを処理することができます。

宛先サーバーは、「ITM_Heartbeat」という名前のクラス (値がハートビート間隔である「interval」という名前のスロットを含む) とともに EIF イベントを受信します。受信された SNMP イベントには、「AlertGroup」属性 (値は「ITM_Heartbeat」) と、「HeartbeatInterval」属性 (値はハートビート間隔) が含まれています。situation_eventdata スロットはまた、ハートビート間隔に設定されます。

IBM Tivoli Enterprise Console **ITM_Heartbeat** クラスは、ハートビート・ルールのカスタマイズで使用可能です。このクラスは `om_tec.baroc` ファイルに存在し、IBM Tivoli Enterprise Console イベント・サーバーでのイベント同期によってインストールされます。これは、IBM Tivoli Monitoring ツール DVD に収録されています。特定のクラスやタイプにのみ適用するルールを作成できるよう、状況イベントはシチュエーション・イベントとは別に保持されます。

例: ITM_Heartbeat EIF イベントは 1 分間隔 (`interval='1';`、`situation_eventdata='1';`) で、ハートビート・イベントとして特徴付けられています。

```
ITM_Heartbeat;
 interval='1';
 source='ITM Agent: Heartbeat Event';
 sub_source='EE_HEARTBEAT';
 situation_name='**';
 situation_origin='SuperServer:TEST';
 situation_time='09/30/2009 09:03:24.000';
 situation_eventdata='1';
 appl_label='A:P:L';
 hostname='SuperServer.raleigh.ibm.com';
 fqhostname='SuperServer.raleigh.ibm.com';
 origin='9.25.111.201';
 severity='HARMLESS';
 date='09/30/2009';
 msg='ハートビート・メッセージ';END
```

マスター・リセット・イベント

モニター・エージェントのリサイクル時にマスター・リセット・イベントが送信されるように構成できます。マスター・リセット・イベントが受信されると、Netcool/OMNIbus または IBM Tivoli Enterprise Console ルールによって、この特定のエージェントとそのサブノードで開いているイベントはすべてクローズされます。

表 38. マスター・リセット・イベントの内容

スロット	値
source	ITM エージェント: 専用シチュエーション
appl_label	A:P:S
master_reset_flag	R
ホスト名	エージェント・マシンのホスト名または IP アドレス
fqhostname	完全修飾ホスト名 (ある場合)
origin	エージェント・マシンの IP アドレス
situation_name	“**”
situation_origin	エージェントの管理対象システム名
situation_time	ライフサイクル・イベントの発生日時
日付	イベントの日付

表 38. マスター・リセット・イベントの内容 (続き)

スロット	値
シチュエーションの状況	N
severity	MINOR
msg	エージェントが再始動したことを伝えるメッセージ。 er_reset_flag

TLS/SSL 通信を使用した専用シチュエーション・イベントの送信

TLS/SSL 通信を使用して、Netcool/OMNIbus EIF 受信側プローブに専用シチュエーション・イベントを送信できます。宛先の Netcool/OMNIbus Probe for Tivoli EIF のバージョンが 12.0 以降である必要があります。

TLS/SSL 通信を使用して専用シチュエーション・イベントを送信するには、以下のステップを実行します。

1. すべてのモニター・エージェントで、そのエージェントのシチュエーション XML ファイルに 1 つ以上の専用シチュエーションを定義します。371 ページの『専用シチュエーション』を参照してください。
2. モニター・エージェントのイベント宛先 XML ファイルに 1 つ以上の Netcool/OMNIbus イベント宛先 (type="M") を定義します。関連付けられている <Server> エレメントに SSL="Y" を指定します。431 ページの『EIF イベント宛先構成 XML 仕様』を参照してください。

   Netcool/OMNIbus での TLS/SSL の構成について詳しくは、*IBM Tivoli Netcool/OMNIbus Event Integration Facility* リファレンスの『SSL 用の EIF 受信側アプリケーションの構成』を参照してください。
3. モニター・エージェントの環境ファイルを編集します。ここで、*pc* は 2 文字の製品コードです。

   Windows *install_dir* ¥TMAITM6¥k*pc*cma.ini.

   Linux UNIX *install_dir* /config/pc.ini。システム・モニター・エージェントの場合、構成ファイルは *pc*.environment です。

   z/OS &hilev.&rte.RKANPARU 内のメンバー名 K*PC*ENV

   モニター・エージェントの環境ファイルで以下の環境変数を設定します。

   注: 示されている環境変数設定は、宛先 Netcool/OMNIbus EIF プローブとの間で確立された TLS/SSL 接続だけではなく、エージェントとすべての宛先 (モニター・サーバーおよびウェアハウス・プロキシー・エージェントなど) の間で確立されたすべてのセキュア接続に適用されます。

   - IRA_EVENT_EXPORT_EIF=Y (デフォルト)
   - KDEBE_FIPS_MODE_ENABLED=Y または N (デフォルト)

     EIF プローブの構成ファイルの *channel_name*SSLFIPSMode=ON|OFF の定義に相当する値を指定します。例えば *channel_name*SSLFIPSMode=ON の場合は KDEBE_FIPS_MODE_ENABLED=Y を設定します。
   - ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y または N (デフォルト)

EIF プローブの構成ファイルの *channel_name*SSLRequireClientAuthentication=ON|OFF の定義に相当する値を指定します。例えば *channel_name*SSLRequireClientAuthentication=ON の場合は ITM_AUTHENTICATE_SERVER_CERTIFICATE=Y を設定します。

サーバー証明書認証を有効にすると、CA 署名デジタル証明書を示すことが必須となるため、EIF プローブが信頼できるエンティティーになります。

注: モニター・エージェントのサーバー証明書認証を有効にすると、エージェントによって開始されるすべてのセキュア接続では、接続を確立するために、すべての宛先 (モニター・サーバー、ウェアハウス・プロキシー・エージェントなど) が有効な CA 署名デジタル証明書を提示する必要があります。

4. デフォルトでモニター・エージェントによってサポートされている TLS/SSL 暗号を以下に示します。
   - TLS_RSA_WITH_AES_256_CBC_SHA
   - TLS_RSA_WITH_AES_128_CBC_SHA
   - SSL_RSA_WITH_3DES_EDE_CBC_SHA

   これらの暗号の少なくとも 1 つが EIF プローブの構成ファイルの *channel_name*SSLcipherList パラメーターに指定されていることを確認します。このパラメーター値がデフォルトの TLS および SSL 暗号のいずれとも一致しない場合は、エージェントの環境ファイルで指定されている KDEBE_V3_CIPHER_SPECS 環境変数を使用して暗号オーバーライドを指定します。

   デフォルトでは、EIF プローブの構成ファイルには SSL_RSA_WITH_3DES_EDE_CBC_SHA が指定されています。これはモニター・エージェントの暗号の 1 つと一致するため、通常はエージェントの暗号リストをカスタマイズする必要はありません。ただし、EIF プローブの *channel_name*SSLCipherList パラメーターがモニター・エージェントのいずれの暗号とも一致しない場合は、KDEBE_V3_CIPHER_SPECS を使用して同じ暗号を指定する必要があります。これにより、TLS/SSL 交換が完了可能になります。この環境変数の形式は次のとおりです。

   KDEBE_V3_CIPHER_SPECS=*nn*

   この *nn* は暗号の短縮名です。

   暗号の短い名前と、対応する長い名前 (*channel_name*SSLCipherList パラメーターで定義) を以下の表に示します。

短い名前	長い名前
01	SSL_RSA_WITH_NULL_MD5
02	SSL_RSA_WITH_NULL_SHA
03	SSL_RSA_EXPORT_WITH_RC4_40_MD5
04	SSL_RSA_WITH_RC4_128_MD5
05	SSL_RSA_WITH_RC4_128_SHA
06	SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
09	SSL_RSA_WITH_DES_CBC_SHA

短い名前	長い名前
0A	SSL_RSA_WITH_3DES_EDE_CBC_SHA
2F	TLS_RSA_WITH_AES_128_CBC_SHA
35	TLS_RSA_WITH_AES_256_CBC_SHA

例えば *channel_name*SSLCipherList=SSL_RSA_WITH_DES_CBC_SHA が EIF プローブの構成ファイルで定義されている場合は、エージェントの環境ファイルで KDEBE_V3_CIPHER_SPECS=09 を設定します。

注: KDEBE_FIPS_MODE_ENABLED=Y が定義されている場合、KDEBE_V3_CIPHER_SPECS 変数は無視されます。その結果、デフォルトの TLS および SSL 暗号が使用されます。

5. モニター・エージェントをリサイクルし、エージェントの環境ファイル、専用シチュエーション XML ファイル、およびイベント宛先 XML ファイルの変更を処理します。

証明書管理

Netcool/Omnibus EIF プローブが CA 署名デジタル証明書を使用し、プローブの構成ファイルに *channel_name*SSLRequireClientAuthentication=YES が指定されている場合は、モニター・エージェントの鍵データベースに、対応する CA 署名デジタル証明書がインポートされていることを確認する必要があります。

モニター・エージェントの鍵データベースを構成するには、証明書管理ツールを使用する必要があります。証明書管理ツールは、GUI モードと CLI モードのいずれでも実行できます。いずれの操作モードでも、管理ツールを呼び出すローカル・システムで Java ランタイム環境が使用可能である必要があります。一般的な環境では、IBM JRE V6 以上が必要です。また、JAVA_HOME 環境変数が IBM Java の場所を指し示していることを確認する必要があります。251 ページの『GSKit 向けの JRE の設定および Key Manager の起動』を参照してください。

IBM Tivoli Monitoring と Netcool/OMNIbus は、SSL 実装に GSKit を使用します。IBM Tivoli Monitoring V6.3 以降では GSKit V8 がインストールされます。GSKit V8 では `gsk8ikm` バイナリーに GUI ユーティリティー、`<gskittoolcmd>` バイナリーに CLI ユーティリティーが含まれています。Netcool/OMNIbus は GSKit V8 に基づいていますが、これは CLI モードでのみ稼働します。GUI モードが必要な場合は、IBM JRE V6 以降に含まれている iKeyman ユーティリティーを使用する必要があります。

IBM Tivoli Monitoring では CMS タイプの鍵データベースが必要であり、Netcool/OMNIbus では Java Key Store (JKS) データベースが必要です。`keyfile.kdb` CMS 鍵データベース・ファイルは *`install_dir`* `¥keyfiles` ディレクトリーにインストールされます。ただし、SSL 接続を介して Netcool/OMNIbus EIF プローブにイベントを送信するときに CA 署名デジタル証明書を使用する必要がある場合は、このデータベースを現行形式で使用することはできません。

iKeyman ユーティリティーを使用してエージェント証明書管理タスクを実行します。次の例に示す手順は、以下のタスクの実行方法を示します。

- 新しい CMS 鍵データベースを作成します。このデータベースは、*`install_dir`* `¥keyfiles` またはその他のディレクトリーに配置できます。

- CA 署名デジタル証明書をインポートします。
- 製品付属のデータベースの代わりに、新規に作成したデータベースを使用します。

例

この例のモニター・エージェントは Windows システムで稼働します。鍵データベース・ファイルは omnieif.kdb、パスワードは ITMPWD です。以前に構成された Netcool/OMNIbus 鍵ストア・ファイルは omni.jks、パスワードは EIFPWD、証明書ラベルは eifca です。omni.jks ファイルのコピーは *install_dir* ¥keyfiles ディレクトリーでローカルに使用可能です。

GSKit キー・ストローク構成 (GUI モード): Windows システムで GSKit GUI ツールを呼び出すには、以下のステップを実行します。

1. *install_dir* ¥GSK8¥bin¥gsk8ikm.exe コマンド・ファイルを実行します。IBM 鍵管理 GUI が表示されます。エラーが発生した場合は、JRE がインストールされており、JAVA_HOME が正しく設定されているかどうかを確認します。
2. メニュー・バーで、「**鍵データベース・ファイル**」>「**新規**」をクリックします。以下の情報を入力して、「**OK**」をクリックします。

   鍵データベース・タイプ: CMS

   ファイル名: omnieif.kdb

   ロケーション: *install_dir* ¥keyfiles¥
3. 鍵ストア・パスワードを設定して、「**OK**」をクリックします。

   パスワード: ITMPWD

   パスワードの確認: ITMPWD

   ☑ 有効期限: 366 Days

   ☑ ファイルにパスワードを隠しておきます。
4. 「**鍵データベースの内容**」メニューに「**個人証明書**」が表示されていることを確認します。**インポート**して「**OK**」をクリックします。

   鍵ファイル・タイプ: JKS

   ファイル名: omni.jks

   ロケーション: *OMNIbus_keystroke_dir*¥
5. パスワード EIFPWD を入力してソース鍵データベースを開きます。「**OK**」をクリックします。
6. ソース鍵データベースの鍵リストから鍵を選択します。ラベル eifca を選択します。「**OK**」をクリックします。
7. 「インポート処理の完了前にこれらのラベルを変更しますか?」というプロンプトが出たら、ラベルを変更せずに「**OK**」をクリックします。
8. 「IBM 鍵管理」ウィンドウを終了します。
9. モニター・エージェントの環境ファイルを編集し、以下の値を設定します。

   KDEBE_KEYRING_FILE=*install_dir* ¥keyfiles¥omnieif.kdb

   KDEBE_KEYRING_STASH=*install_dir* ¥keyfiles¥omnieif.sth

   KDEBE_KEY_LABEL=eifca
10. エージェントを再始動します。新しい CMS 鍵データベースが使用されます。

GSKit 鍵ストアの構成 (CLI モード): 「IBM 鍵管理」GUI ユーティリティーが使用できない場合は、Windows で GSKit のCLI ツールを使用して証明書インポート機能を実行できます。GUI の例で選択したものと同じ値を使用したコマンドの例を以下に示します。

1. コマンド行から、*install_dir* ¥keyfiles ディレクトリーに移動 (cd) してデータベース・ファイルを作成します。

   ```
   install_dir ¥GSK8¥bin¥gsk8cmd.exe -keydb -create -db omnieif.kdb -pw
   ITMPWD -type CMS -stash -expire 366
   ```

2. 以下のコマンドを実行して Netcool/OMNIbus 証明書をインポートします。

   ```
   install_dir ¥GSK8¥bin¥gsk8cmd.exe -cert -import -file
   OMNIbus_keystore_dir¥omni.jks -pw EIFPWD -label eifca -type JKS -target
   omnieif.kdb -target_pw ITMPWD
   ```

   GUI の例と同様に、エージェントの環境ファイルの以下の値を更新する必要があります。

   KDEBE_KEYRING_FILE=*install_dir* ¥keyfiles¥omnieif.kdb

   KDEBE_KEYRING_STASH=*install_dir* ¥keyfiles¥omnieif.sth

   KDEBE_KEY_LABEL=eifca

エージェント・サービス・インターフェース

エージェント・サービス・インターフェースを使用して、インストール済みエージェント (Tivoli Enterprise Monitoring AgentまたはTivoli System Monitor Agent) からの情報を取得します。ローカル・オペレーティング・システムにログインすると、エージェント情報、専用シチュエーション、専用ヒストリー、照会、属性、および構成ロード・リスト・コマンドのような要求のレポートを取得できます。

エージェント・サービス・インターフェースには、IBM Tivoli Monitoring サービス索引ユーティリティーを介してアクセスします。このインターフェースは、インターネット・サーバーとして動作します。つまり、要求を受け入れて検証したり、処理用に要求をエージェントに送信したり、TCP/IP を介した HTTP アプリケーション・プロトコルまたは HTTPS アプリケーション・プロトコルによって応答データを収集およびフォーマットしたりします。

z/OS IBM i エージェント・サービス・インターフェースは、IBM i および z/OS オペレーティング・システムでのインストールには使用できません。ただし、IBM Support Assistant (ISA) に含まれる ITMSUPER ツールを使用することはできます。これは、無償で提供されるローカル・ソフトウェア保守ワークベンチで、IBM ソフトウェア製品に関する疑問や問題の解決に役立ちます。 ISA ソフトウェアをインストールするには、「IBM Support Assistant (http://www-01.ibm.com/software/support/isa)」を参照してください。ツール・セットの一部として、**itmsa.htm** では、IBM i、z/OS、Windows、Linux、および UNIX の各プラットフォーム上のエージェント・レポートへの直接アクセスを提供しています。また、**itmsuper.htm** では、ハブ・モニター・サーバーを介してアクセスできる Web サービス・ツールを提供しています。

エージェント・サービス・インターフェースの開始

ブラウザーからエージェント・サービス・インターフェースを開始して、エージェント情報のレポート、シチュエーション状況の取得、短期間ヒストリーの表示、および XML でのサービス要求の作成を行うための選択項目が含まれるメニューを取得します。

始める前に

エージェント・サービス・インターフェースとその機能にアクセスするには、モニター・エージェントがインストールされているオペレーティング・システムの管理者ユーザー ID が必要です。

このタスクについて

以下のステップに従って、IBM Tivoli Monitoring サービス索引ユーティリティーを開始し、情報を取得するエージェントのエージェント・サービス・インターフェースにログオンします。

手順

1. `http://<host name>:1920` または `https//<host name>:3661` を入力して、IBM Tivoli Monitoring サービス索引を開始します。ここで、host name は、エージェントがインストールされているコンピューターの完全修飾名または IP アドレスです。 開始済みサービスのリストが表示されます。
2. 作業するアプリケーションの ***pc* エージェント・サービス・インターフェース** (ここで、*pc* は 2 文字のコンポーネント・コード) リンクをクリックします。
3. プロンプトに従い、オペレーティング・システムの管理者レベルのユーザー名およびパスワードを入力します。

タスクの結果

認証されると、「**エージェント情報**」、「**シチュエーション**」、「**ヒストリー (History)**」、「**照会**」、および「**サービス・インターフェース要求 (Service Interface Request)**」の各リンクを含む「エージェント・サービス・インターフェース・ナビゲーター (Agent Service Interface Navigator)」ページが表示されます。ナビゲーター・ページは、以下の場所にデフォルトでインストールされる `navigator.htm` ファイルです。

Windows *install_dir* ¥localconfig¥html

Linux UNIX *install_dir* /localconfig/HTML

サブノード (Agentless Monitoring、VMware VI エージェント、Agent Builder を使用して作成されたサブノードなど) を使用するモニター・エージェントには、次のようなエージェント・サービス・インターフェースでのレポートの制限があります。

- 照会リンクが使用できない
- シチュエーションのリストに、サブノードを含む、エージェントのすべてのシチュエーションが表示されており、サブノードによるフィルター処理ができない

- 専用ヒストリーに、エージェント上で選択された属性に対する、すべての収集済みのヒストリカル・データが表示されており、サブノードによるフィルター処理ができない

アクセス許可グループ・プロファイル

アクセス許可グループ・プロファイル (AAGP) には、セキュリティー管理者が設定したアクセス許可グループ定義とユーザー ID 割り当てが含まれます。

セキュリティー管理者は、**制限付き**グループを除くすべてのアクセス許可グループの名前を定義できます。グループ名は必須です。各アクセス許可グループには、サービス・インターフェース (SIAPI 要素) や、エージェント・コンポーネントによって公開されたサービスなど、少なくとも 1 つのエージェント・コンポーネント・カテゴリーがあります。各エージェント・コンポーネントは、AAGP 機能を呼び出して、ユーザー ID、コンポーネント・カテゴリー、およびアクセス許可の要求されたサービス名を取得します。許可された場合、エージェント・コンポーネントは要求されたサービスを実行します。許可されなかった場合、エージェントは無許可のステータスを戻します。

AAGP は認証サービスではなく、提供されたユーザー ID が認証されていることを前提としています。同じ前提がサービス・インターフェースにもいえます。これは、すべてのユーザーは、有効な ID とパスワードを使用して、まずシステムにサインオンする必要があるためです。ただし、エージェントは、他のエージェントや Tivoli Enterprise Monitoring Server にかわってオートメーション・アクションなどの作業を実行でき、提供されているユーザー ID は、ローカル・システムには不明である可能性があります。このような場合、エージェントは、仮想ユーザーが信頼できる Tivoli Monitoring メンバーであるため認証済みであることを考慮し、AAGP を呼び出しで許可を求めます。または、このような機能が使用可能になる中央認証や許可サービスを利用するように AAGP を拡張することができます。

アクセス許可グループのタイプ

次のデフォルトの AAGP グループが事前定義されており、エージェントの開始時に自動的にロードされます。

制限付きグループ
デフォルトのグループ。このグループのサービス・インターフェース・カテゴリーは、システム情報、運用構成、ワークロード・モニター、およびヒストリカル・データ・レポートの機能を提供するサービスで構成されます。明確には定義されていないユーザーを含めて、すべてのユーザーはこの必須グループに存在します。

オペレーション・グループ
このグループには、**制限付き**グループ・カテゴリー・サービスと、運用コントロール、構成管理、アプリケーションによってカスタマイズされたアクセス機能を提供するサービス・インターフェース・サービスが含まれます。

管理グループ
このグループには、ファイル・オブジェクトの追加や AAGP の動的な更新とともに、すべてのサービス・インターフェース機能へのアクセス権限があります。

表 39. サービス・インターフェース・コマンドのためのアクセス許可グループの権限

サービス・インターフェース API	制限付き	オペレーション	管理
AgentInfo	x	x	x
AttrList	x	x	x
ReadAttr	x	x	x
ListSubnode	x	x	x
TableSit	x	x	x
SitStat	x	x	x
SitSummary	x	x	x
HistRead	x	x	x
Report	x	x	x
PvtControl		x	x
CnfgCommand		x	x
ConfigurationArtifact		x	x
PrivateConfiguration		x	x
Overrides		x	x
AAGP			x
ListAAGP		x	x
FileObj			x

制限付きグループの定義は必須です。その定義が AAGP に含まれていない場合、表 39 に示されるエージェントのデフォルトの指定が有効になります。

コンポーネント・カテゴリーにキーワード *NONE を指定すると、明確に定義されていないすべてのユーザーがそのコンポーネント・サービスにアクセスできなくなります。例えば、**制限付き**グループに指定された `<SIAPI>*NONE</SIAPI>` によって、エージェント・サービス・インターフェースへの通常のアクセスができなくなります。

FileObj では、HTTP 要求を使用して、エージェントのファイルをプッシュまたはプルできます。一元化された構成の場合、 FileObj は、モニター・エージェントが中央構成サーバーとして動作することを許可するために使用する API です。エージェント・サービス・インターフェースはモニター・エージェントの基本的なサービスで使用可能であり、ファイルを処理するために使用できます。または、ファイルをプッシュまたはプルするように、いずれかのエージェントに HTTP 要求を送信できます。AAGP 機能によって、セキュリティーが強化されます。デフォルトでは、Linux または UNIX の **root**、Windows の **Administrator** が FileObj API を使用する権限を持つ AD グループのメンバーです。476 ページの『中央構成サーバーとしてのモニター・エージェント』の例を参照してください。

AAGP に `<AAGROUP>` 指定が含まれていない場合、表 39 に示されるエージェントのデフォルトの指定が有効になります。有効なグループは、RE、OP、および AD です。AAGP によって異なる定義がされていない限り、すべてのユーザーは自動的に**制限付き**グループに割り当てられるため、R (制限付き) グループ・ユーザーを定義する必要はありません。

アクセス許可グループ・プロファイルの XML 指定

セキュリティー管理者は、単純な XML 指定フォーマットでエージェントのユーザー・グループ許可プロファイルを定義します。

<AAGP>
この要素は、XML ファイルをエージェントのアクセス許可グループのプロファイル文書として識別します。すべての AAGP 指定は、ルートレベルの <AAGP> 開始要素タグと </AAGP> 終了要素タグで囲まれる必要があります。AAGP ファイルの内容は、エージェントによって使用されている既存の AAGP とマージされ、デフォルトのアクセス許可グループにユーザーを追加できます。既存の AAGP を完全に置き換えるには、AAGP 要素に REFRESH 属性を使用します。

REFRESH="Y"
現行のアクティブな AAGP を削除し、この AAGP 指定の AAGP 定義と置き換えます。

LOCAL="LOCK | UNLOCK"
オプションで、デフォルト値はありません。LOCK および UNLOCK は、AAGP の更新が ASI から開始された場合にのみ受け入れられます。

LOCAL="LOCK" を指定するとローカル AAGP 構成がロックされ、ASI によっても一元化された構成機能の AAGP ファイルのダウンロードによっても更新できなくなります。

LOCAL="UNLOCK" を指定するとローカル AAGP 構成がアンロックされ、AAGP は ASI によっても一元化された構成機能のファイルのダウンロードによっても更新できるようになります。UNLOCK は、LOCK が有効なときにのみ有効です。それ以外の場合は無視されます。つまり、<AAGP LOCAL="UNLOCK"> の前にはあらかじめ <AAGP LOCAL="LOCK"> オペレーションが必要です。

<AAGP LOCAL="LOCK"></AAGP> と <AAGP LOCAL="UNLOCK"></AAGP> は、互いに独立したスタンドアロンの AAGP ASI トランザクションにすることができます。

<AAGROUP>
アクセス許可グループを定義します。一連のグループ定義は、<AAGROUP> 開始要素タグと </AAGroup> 終了要素タグで囲みます。

<GROUPNAME>
アクセス許可グループ名を定義します。名前は、<GROUPNAME> 開始要素タグと </GROUPNAME> 終了要素タグで囲みます。グループ名は 32 文字以下で指定し、最初の 2 文字はすべてのユーザー・グループ名で一意である必要があります。

<INCLUDE>
オプションです。 この AAGROUP に含める AAGROUP 定義を指定します。AAGROUP 名は、<INCLUDE> 開始タグと </INCLUDE> 終了タグで囲みます。

<SIAPI>
エージェントのサービス・インターフェース API 名を大/小文字を区別せずに指

定します。この時点では、コンポーネント・カテゴリーのみが定義されています。名前は、<SIAPI> 開始タグと </SIAPI> 終了タグで囲みます。

<other>
現行のリリースでは、<other> 要素は使用できません。将来のリリースで使用するために予約されています。これは、管理対象のなる他のエージェント・コンポーネント・サービスを指定します。

<AAUSER>
許可されたユーザー ID と、それに関連付けられたアクセス許可グループの名前を定義します。各ユーザー定義は、<AAUSER> 開始タグと </AAUSER> 終了タグで囲みます。

<ID >
許可ユーザーのサインオン ID を大/小文字を区別せずに指定します。ユーザー ID は、<ID> 開始タグと </ID> 終了タグで囲みます。

<ASSIGN>
アクセス許可グループの割り当てを大/小文字を区別せずに指定します。有効な AAGP タイプは RE (**制限付き**)、OP (**オペレーション**)、AD (**管理**) です。グループ名を完全に入力することも、先頭文字のみ入力することもできます。AAGP タイプは、<ASSIGN> 開始タグと </ASSIGN> 終了タグで囲みます。

例

```
<AAGP>
   <AAGROUP>
   <GROUPNAME>Restricted</GROUPNAME>
   <SIAPI>AgentInfo</SIAPI>
   <SIAPI>AttrList</SIAPI>
   <SIAPI>ReadAttr</SIAPI>
   <SIAPI>ListSubnode</SIAPI>
   <SIAPI>TableSit</SIAPI>
     <SIAPI>ListTable</SIAPI>
   <SIAPI>SitStats</SIAPI>
   <SIAPI>SitSummary</SIAPI>
   <SIAPI>HistRead</SIAPI>
   <SIAPI>Report</SIAPI>
   <REFLEXAUTO>ExecAction</REFLEXAUTO>
   </AAGROUP>
   <AAGROUP>
   <GROUPNAME>Operation</GROUPNAME>
   <INCLUDE>Restricted</INCLUDE>
   <SIAPI>PvtControl</SIAPI>
   <SIAPI>CnfgControl</SIAPI>
   <SIAPI>CnfgCommand</SIAPI>
   <SIAPI>ConfigurationArtifact</SIAPI>
   <SIAPI>PrivateConfiguration</SIAPI>
   <SIAPI>Overrides</SIAPI>
     <SIAPI>XMSClientSpec</SIAPI>
   <SIAPI>ListAAGP</SIAPI>
     <CLI>ExecCommand</CLI>
   <TAKEACTION>ExecAction</TAKEACTION>
  </AAGROUP>
  <AAGROUP>
   <GROUPNAME>Administrative</GROUPNAME>
   <INCLUDE>Operation</INCLUDE>
   <SIAPI>FileObj</SIAPI>
   <SIAPI>AAGP</SIAPI>
  </AAGROUP>
  <AAUSER>
```

```
  <ID>default</ID>
  <ASSIGN>OP</ASSIGN>
</AAUSER>
</AAGP>
```

アクセス許可グループの処理手順

すべての有効なシステム・ユーザーは、**制限付き**グループにアクセスすることが自動的に許可されています。 許可された、**管理**グループおよびその他のグループのユーザーが、エンタープライズ・セキュリティー管理者によって AAGP を使用して定義されます。次に、AAGP の処理手順を示します。

1. エンタープライズ・セキュリティー管理者が、カスタマイズされた AAGP を作成し、それをセキュアな中央構成サーバーに保存します。事前定義された許可グループの内容はカスタマイズでき、追加のカスタム認可グループを追加することもできます。例えば、<AUTOCMD>KILL</AUTOCMD> を**オペレーション**・グループに含めることができます。
2. モニター・エージェントは、デフォルトの AAGP を開始してアクティブにします。管理 ID は、デフォルトで**管理**グループのメンバーとして定義されます。Windowsでは *Administrator*、Linux または UNIX では *root* です。
3. モニター・エージェントは一元化された構成を使用し、カスタマイズされた独自の AAGP を中央構成サーバーから取得します。エージェントは、この操作に常に HTTPS プロトコルを選択します。エージェントの構成ロード・リストに AAGP が含まれない場合、または AAGP を中央構成サーバーからダウンロードできない場合、エージェントは次に再始動されるまで、このモードで動作します。
4. エージェント・コンポーネントは AAGP で許可を確認します。これによって、ユーザー ID、コンポーネント・カテゴリー、およびサービス名が提供されます。AAGP は、アクセス許可グループおよびユーザー ID 割り当てに基づいて、アクセス権限を付与または拒否します。
5. モニター・エージェントは、構成ロード・リストでの指定に従って定期的に、またはサービス・インターフェース構成コマンドが発行されたときに、AAGP の更新を確認します。
6. モニター・エージェントは、ユーザー許可プロファイルをローカルには保存しません。

ローカル AAGP の永続的構成

管理者は、一時的な必要性に対応するために AAGP をカスタマイズすることが必要な場合があります。例えば、一時的な請負業者ユーザー の ID を追加したり、ローカル環境のアクセス制限ごとにカテゴリー・サービスを調整するなどです。以下のステップは、エージェントを再起動しても永続する、ローカル AAGP 構成への変更を実装する手順を示しています。

1. エージェント・サービス・インターフェースを通じて、管理者のユーザー ID でローカル・システムにログオンします。
2. <ListAAGP> トランザクションを使用して、エージェントの現在の AAGP 仕様を取得します。
3. 新しい要件に合わせて ListAAGP 出力を編集します。例えば、別の許可ユーザー ID を追加します。

4. 更新した AAGP 定義を、エージェント・サービス・インターフェースを通じてエージェントに送信します。
5. エージェントは入力された AAGP 定義を処理します。この定義が現在のアクティブな AAGP 定義として有効になります。また、エージェントは、 AAGP 構成 XML をローカル・ファイルとして出力します。分散システムでは *ITM_HOME/localconfig/pc/pc*_aagpcnfg.txt、 z/OS システムでは暗号化形式の K*pc*AAGPX.UKANDATV として出力されます。
6. 次回、エージェントを起動すると、エージェントはローカルの永続 AAGP 構成ファイルを検索し、ファイルを暗号化解除して読み取り、そのすべての AAGP XML ステートメントを処理します。これらのアクションにより、今までにカスタマイズした AAGP 定義が復元されます。エージェントがローカル永続 AAGP 構成ファイルを発見できない場合は、デフォルトの AAGP 定義が有効になります。
7. ローカルでカスタマイズした AAGP 構成が有効になっている間、ローカルの AAGP カスタマイズ値が変更されないように、一元化された構成機能からのすべての AAGP の更新はエージェントによって中断されます。管理者は、エージェント・サービス・インターフェースを通じて <AAGP Resume="Y"> 要求を送信して、ローカルの AAGP 永続構成をアンロックする必要があります。これにより、一元化された構成機能は AAGP 更新操作のサポートを再開できます。

ローカル AAGP の許可による制御

エージェントのエンドポイントで管理者が厳格な許可による制御を行い、ユーザー ID がローカル・システムに定義されていない限り自動化要求の実行を一切許可しない場合は、以下の手順に従ってローカル AAGP の許可による制御を有効にします。

1. エージェント・サービス・インターフェースを通じて、管理者のユーザー ID でローカル・システムにログオンします。
2. <ListAAGP> トランザクションを使用して、エージェントの現在の AAGP 仕様を取得します。
3. ListAAGP 出力を編集して、デフォルトのユーザー定義を削除します。

```
<AAUSER>
   <ID>default</ID>
   <ASSIGN>OP</ASSIGN>
</AAUSER>
```

4. デフォルトのユーザー定義では、自動化を実行する権限のある内部的な秘密のユーザー ID を作成するように AAGP に指示されます。デフォルトのユーザー ID 定義がない場合、AAGP はエージェントに送信される各コマンド要求からユーザー ID を取り出します。取り出されたユーザー ID が AAGP で未定義の場合、許可エラーによってコマンド要求は拒否されます。この機能により、ローカル管理者はエージェントのエンドポイントで実行できる自動化を完全に制御できます。
5. 更新した AAGP 定義を、エージェント・サービス・インターフェースを通じてエージェントに送信します。

エージェント・サービス・インターフェース - エージェント情報

エージェント・サービス・インターフェース・メニューから「**エージェント情報**」を選択して、環境ファイル設定を含む、エージェントに関連するデータのレポートを取得できます。

HOSTNAME

myitm.raleigh.ibm.com のような、コンピューターの完全修飾名です。

NODENAME

Primary:MYITM:NT のような、管理対象システムの名前です。

SUBSYSID

エージェントにサブノード (サブエージェント) がある場合、その名前です。ない場合、サブシステム ID は **Primary** です。

NODEINFO

Win2003~5.2-SP2 のような、システムおよび作動プラットフォームのタイプです。

PRODUCT

NT のような、エージェントの 2 文字の製品コードです。

VERSION

06.22.00 のような、エージェントのインストール済みバージョンです。

LEVEL A=00:WINNT C=06.22.00.00:WINNT G=06.22.00.00:WINNT

PATCHLEVEL A=00:WINNT;C=06.22.00.00:WINNT;G=06.22.00.00:WINNT;

AFFINITY

Tivoli Management Services コンポーネントへのエージェントのアフィニティーを識別する値です。例えば、**%IBM.STATIC021 000000000A00000u0a4** のようになります。

BOOTTIME

Wed Jul 29 15:15:33 2009 のような、エージェントが始動を完了した日時および曜日です。

ENVFILE

エージェント環境ファイルの現在のパラメーター設定のリストです。値を変更する必要がある場合は、「Tivoli Monitoring Services の管理」か、または分散システム上のテキスト・エディターを使用して環境ファイルを開きます。

以下に、エージェント情報レポートに表示される Windows OS 環境ファイルの例を示します。

```
* CANDLE_HOME=d:¥IBM¥ITM
* KBB_RAS1=ERROR
* KBB_VARPREFIX=%
* KBB_VARPREFIX=$
* KBB_RAS1_LOG=d:¥IBM¥ITM¥tmaitm6¥logs¥$(computername)_nt_kntcma_$
(sysutcstart)-.log INVENTORY=d:¥IBM¥ITM¥tmaitm6¥logs¥$(computername)
_nt_kntcma.inv COUNT=03 LIMIT=5 PRESERVE=1 MAXFILES=9
* TIMEOUT=600
* ITMDEPLOY_AGENTDEPOT=d:¥IBM¥ITM¥tmaitm6¥agentdepot
* ICCRTE_DIR=d:¥IBM¥ITM¥GSK8
* CSV1_PATH=d:¥IBM¥ITM¥GSK8¥lib
* CSV2_PATH=d:¥IBM¥ITM¥GSK8¥bin * KBB_VARPREFIX=$
* PATH!=$(CSV1_PATH);$(CSV2_PATH);$(PATH)
```

```
* KEYFILE_DIR=d:¥IBM¥ITM¥keyfiles
* KDEBE_KEYRING_FILE=d:¥IBM¥ITM¥keyfiles¥keyfile.kdb
* KDEBE_KEYRING_STASH=d:¥IBM¥ITM¥keyfiles¥keyfile.sth
* KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate
* KBB_IGNOREHOSTENVIRONMENT=Y
* JAVA_HOME=d:¥IBM¥ITM¥java¥java70¥jre
* KBB_IGNOREHOSTENVIRONMENT=N
* PATH=d:¥IBM¥ITM¥GSK8¥LIB;C:¥WINDOWS¥system32;C:¥WINDOWS;C:¥WINDOWS¥
System32¥Wbem;D:¥IBM¥SQLLIB¥BIN;D:¥IBM¥SQLLIB¥FUNCTION;D:¥IBM¥SQLLIB¥
SAMPLES¥REPL;d:¥IBM¥ITM¥bin;d:¥IBM¥ITM¥bin¥dll;d:¥IBM¥ITM¥InstallITM;
d:¥IBM¥ITM¥TMAITM6;d:¥IBM¥ITM¥InstallITM
```

エージェント・サービス・インターフェース - シチュエーション

エージェント・サービス・インターフェースの「**シチュエーション**」オプションを使用すると、モニター・エージェントの各シチュエーション (専用シチュエーションおよびサブノードに配布されたシチュエーションを含む) の状態および統計を確認できます。

シチュエーション・レポートには、エージェントの各シチュエーションに関する重要な統計が記載されています。エージェントの環境変数 IRA_EVENT_EXPORT_SIT_STATS の設定により、指定する詳細レベルが決定されます。

Situation name
各シチュエーションの要約ページの上に、シチュエーションの名前が記載されます。専用シチュエーションの場合は、名前に **_pr** が付加されます。

TYPE Sampled または Pure。シチュエーションが一定の間隔でデータをサンプリングする場合、そのシチュエーションはサンプルです。ピュア・イベントは非送信請求通知です。 Windows イベント・ログ属性および Windows ファイル変更属性は、ピュア・イベントをレポートする属性グループの例です。

INTERVAL
データ・サンプルの間隔 (秒単位)。この属性グループのシチュエーションがピュア・イベントをトリガーする場合、サンプリング間隔がなくなり、値は 0 と表示されます。

ROWSIZE
行サイズです。

FIRSTSTARTTIME
エージェントの開始後、シチュエーションが最初に開始された日時および曜日です。

LASTSTARTTIME
シチュエーションが最後に開始された日時および曜日です。

LASTSTOPTIME
シチュエーションが最後に停止された日時および曜日です。

FIRSTEVENTTIME
シチュエーションの開始後、シチュエーションが最初に true になり、イベントが開かれた日時および曜日です。

LASTTRUETIME
シチュエーションが最後に true になり、イベントが開かれた日時および曜日です。

LASTFALSETIME
以前のサンプリングで true に評価された後、シチュエーションが false に評価された日時および曜日です。

TIMESRECYCLED
エージェントがオンラインになってから停止および開始された回数です。

TIMESAUTONOMOUS
シチュエーションの開始後に、エンタープライズ・モニター・エージェントがモニター・サーバーから切断されたためにシチュエーションがオートノマス状態になった回数です。後ろに以下のような DAY 統計が続きます。

DAY

DATE は、最後に統計データが収集された日付です。エンタープライズ・シチュエーションの場合は、エージェントが最後に接続されてからの日付になります。

TRUESAMPLES は、エージェントがモニター・サーバーから切断されている間に、シチュエーションが true に評価された回数です。

FALSESAMPLES は、エージェントがモニター・サーバーから切断されている間に、シチュエーションが最後に true に評価されてから false に評価された回数です。

TRUERATIO は、シチュエーションが false に評価された回数に対する、true に評価された回数のパーセントです。

FALSERATIO は、シチュエーションが true に評価された回数に対する、false に評価された回数のパーセントです。

HOURROWS は、レポートされたデータの行数です。

HOURTRUE は、エージェントがモニター・サーバーから切断されている間に、シチュエーションが true のままになっていた時間数です。

HOURFALSE は、エージェントがモニター・サーバーから切断されている間に、シチュエーションが false のままになっていた時間数です。

サブノードを含む、エージェントのすべてのシチュエーションが表示されます。ComputerA および ComputerB というサブノードを持つ、以下のサンプル・エージェント TestLab では、10 個のシチュエーションがリストされます。

TestLab

SubNodeA (4 つの固有のシチュエーションと、SubNodeB にも存在する 2 つのシチュエーション)

SubNodeB (4 つの固有のシチュエーションと、SubNodeA にも存在する 2 つのシチュエーション)

エージェント・サービス・インターフェース - ヒストリー

エージェント・サービス・インターフェースで「**ヒストリー (History)**」を選択し、選択された属性グループ・テーブル用に保存された専用ヒストリー・データ・サンプルを表示します。

不要な属性の横にあるチェック・ボックスをクリアすることで、必要な属性のみを表示するように、レポートをフィルター処理できます。開始日時および終了日時を選択し、「**レポート**」をクリックします。属性の下のテーブルにレポートが表示さ

れ、指定された期間の属性グループのヒストリカル・データ・サンプルが示されます。属性ごとに 1 列が使用され、サンプルごとに 1 行が使用されます。許容される行数は 5000 行までです。制限の 5000 行の中に必要な行が含まれていない場合は、期間を狭めてレポートを作成し直してください。

収集されたヒストリカル・データはすべて、サブノードを含む、エージェントに対して表示されます。

エージェント・サービス・インターフェース - 照会

エージェント・サービス・インターフェースの「**照会**」オプションを選択し、k*pc*.atr ファイルに、テーブル名で示される、選択済みの属性グループがないかを照会します。一方のレポートには、属性、列名と表示名、および特性のリストが記載されます。もう一方のレポートには、属性の現在のサンプル値が示されます。

▼ リストからテーブル名を選択し、コンポーネント属性と、サンプル・データのレポートを確認します。

Table name
<*install_dir*>/TMAITM6/ATTRLIB/k*pc*.atr ファイルから取得された、属性グループのテーブル名です (ここで *pc* は 2 文字の製品コードです)。

Name 属性の列名です。専用シチュエーションまたは専用ヒストリーでは使用されませんが、Tivoli Data Warehouse に保管されたデータを検索する場合は表示されます。

Display
Attribute_Group_Name.Attribute_Name のような形式の、属性の詳細な名前であり、専用シチュエーションおよび専用ヒストリーの定義に入力します。例えば、KHD_CONFIG.Connection_Pool_Size や NT_Registry.Server_Name のようになります。

Type この列には、属性のタイプを表す数値が表示されます。例えば、4 は整数列挙型の属性を表します。タイプは、専用シチュエーションまたは専用ヒストリーの定義で直接は使用されませんが、これにより、属性値に必要とされる形式を確認できます。

Length
バイト数、または属性値に許可されている最大バイト数です。TIMESTAMP 属性の場合、16 は CYYMMDDHHMMSSmmm の形式を意味します。例えば、1090819160501000 は 21 世紀、2009 年 8 月 19 日、午後 4:05:01 を表します。

Minimum
属性の値に許可された最小値がここに表示されます。空白の場合、その属性には最小値がありません。

Maximum
属性の値に許可された最大値がこの列に表示されます。空白の場合、その属性には最大値がありません。

ENUMS
属性の表す内容を示す列挙です。一部の列挙型属性には、複数の列挙があり

ます。列挙型属性の専用シチュエーションを作成する場合、式には、表示される値 (Tivoli Enterprise Portal に表示される値) ではなく、実際の値を使用します。

以下の 2 つのレポートは、Windows IP アドレスの属性グループ (テーブル名は NTIPADDR) に対する照会結果です。1 つ目のレポートは `kpc.atr` ファイルに表示されるテーブルの属性リストです。専用シチュエーションまたは専用ヒストリーの定義を作成する場合は、「**Display**」 列に示される名前を使用する必要があります。

表 40. エージェント・サービス・インターフェース - サンプル属性の照会リスト

Name	Display	Type	Length	Minimum	Maximum	ENUMS
ORIGINNODE	NT_IP_Address.System_Name	2	64			
TIMESTAMP	NT_IP_Address.Timestamp	2	16			
INTFNAME	NT_IP_Address.Network_ Interface_Name	3				Windows 2000 では使用不可
IPADDRESS	NT_IP_Address.IP_Address	2	50			
DNSNAME	NT_IP_Address.DNS_Name	10	388			DNS エントリーなし
IPVERSION	NT_IP_Address.IP_Version	4		-2147483648	2147483647	4 IPv4 6 IPv6 10 IPv4_IPv6
MACADDRESS	NT_IP_Address.MAC_Address	2	28			

2 つ目のレポートには、属性グループの現在のサンプル値が表示されます。

表 41. エージェント・サービス・インターフェース - 照会サンプル・レポート

ORIGINNODE	TIMESTAMP	INTFNAME	IPADDRESS	DNSNAME	IPVERSION	MACADDRESS
Primary:East:NT	1090819142128111	11a_b_g ワイヤレス LAN Mini PCI アダプター	9.52.100.111	East.ibm.com	4	00054e48f5bd
Primary:East:NT	1090819142128111	MS TCP ループバック・インターフェース	127.0.0.1	NO_DNS_ ENTRY	4	000d608b2938

エージェント・サービス・インターフェース - サービス・インターフェース要求

エージェント・サービス・インターフェースの「**サービス・インターフェース要求 (Service Interface Request)**」 を選択すると、XML 形式のコマンドを入力して、属性グループ定義などのエージェント情報を要求できます。

エージェント・サービス・インターフェース要求 - エージェント情報

エージェント ID 情報の要求です。取得されるデータは、エージェント ID (コンピューター・ホスト名、管理対象システム名、サブノード・リスト、オペレーティング・システム情報など)、製品 ID (製品名、バージョン、保守レベルとパッチ・レベ

ルのデータ、製品のアフィニティー、機能など)、および環境 ID (現在の環境変数の設定など) という 3 つのセクションに分かれています。

要求の入力

表 42. エージェント・サービス・インターフェースの <AGENTINFO> 要求

タグ	説明
<AGENTINFO>	AGENTINFO の開始タグおよび終了タグを入力して、エージェント・プロパティーの要求を行います。

要求の例:

```
<AGENTINFO>
</AGENTINFO>
```

レポートの出力

表 43. エージェント・サービス・インターフェースの <AGENTINFO> 要求の出力

出力タグ	説明
<HOSTNAME>	エージェントのホスト名
<NODENAME>	エージェントの管理対象システム名
<SUBSYSID>	エージェントのサブシステム ID
<NODEINFO>	エージェント・システムの OS 情報
<PRODUCT>	ITM 製品名
<VERSION>	エージェントのバージョン
<LEVEL>	エージェントのインストールおよび保守のレベル
<PATCHLEVEL>	エージェントの保守パッチ・レベル
<AFFINITY>	エージェントの有効なアフィニティー
<BOOTTIME>	エージェントのブート時間
<ENVFILE>	CDATA[] 制御データ・タグで囲まれた、エージェントの構成ファイル
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。

出力例: エージェントの戻りプロパティー・データ

```
<AGENTINFO>
  <HOSTNAME>dyang7</HOSTNAME>
  <NODENAME>Primary:DYANG7:NT</NODENAME>
  <SUBSYSID>Primary</SUBSYSID>
  <NODEINFO>WinXP~5.1-SP2</NODEINFO>
  <PRODUCT>NT</PRODUCT>
  <VERSION>06.22.00</VERSION>
 <LEVEL>A=00:WINNT C=06.21.00.00:WINNT G=06.21.00.00:WINNT</LEVEL>
 <PATCHLEVEL>A=00:WINNT;C=06.21.00.00:WINNT;G=06.21.00.00:WINNT;
 </PATCHLEVEL>
 <AFFINITY>0008000000000000000000000000000004000000u0a4</AFFINITY>
  <BOOTTIME>Mon Mar 02 22:48:27 2009</BOOTTIME>
  <ENVFILE>
   <![CDATA[
   CANDLE_HOME=C:¥IBM¥ITM
   KBB_RAS1=ERROR
   KBB_VARPREFIX=%
   TIMEOUT=600
   ITMDEPLOY_AGENTDEPOT=C:¥IBM¥ITM¥tmaitm6¥agentdepot
   IRA_AUTONOMOUS_MODE=Y
   CTIRA_HEARTBEAT=1440
```

```
   CTIRA_RECONNECT_WAIT=60
   IRA_DUMP_DATA=Y
   IRA_DEBUG_TRANSCON=N
   IRA_DEBUG_EVENTEXPORT=N
   IRA_DEBUG_AUTONOMOUS=Y
   IRA_DEBUG_SERVICEAPI=Y
   IRA_DEBUG_PRIVATE_SITUATION=Y
   IRA_EVENT_EXPORT_LISTSTAT_INTERVAL=300
   IRA_EVENT_EXPORT_SNMP_TRAP=Y
   ICCRTE_DIR=C:¥IBM¥ITM¥GSK8
   CSV1_PATH=C:¥IBM¥ITM¥GSK8¥lib
   PATH!=$(CSV1_PATH);$(PATH)
   KEYFILE_DIR=C:¥IBM¥ITM¥keyfiles
   KDEBE_KEYRING_FILE=C:¥IBM¥ITM¥keyfiles¥keyfile.kdb
   KDEBE_KEYRING_STASH=C:¥IBM¥ITM¥keyfiles¥keyfile.sth
   KDEBE_KEY_LABEL=IBM_Tivoli_Monitoring_Certificate
   JAVA_HOME=C:¥Program Files¥IBM¥Java70¥jre
   PATH=C:¥IBM¥ITM¥GSK8¥LIB;¥;C:¥WINDOWS¥system32;C:¥WINDOWS;
   C:¥WINDOWS¥System32¥Wbem;c:¥perl¥bin;C:¥Infoprint;
    C:¥IBM¥ITM¥InstallITM ]]>
 </ENVFILE>
</AGENTINFO>
```

エージェント・サービス・インターフェース要求 - エージェント・サブノード・リスト

サービス・インターフェース要求で <LISTSUBNODE> 要求を使用すると、このコンピューター上の既知のすべてのサブノードのリストが取得されます。

要求の入力

表 44. エージェント・サービス・インターフェースの <LISTSUBNODE> 要求

タグ	説明
<LISTSUBNODE>	サブノード・リストを要求するには、LISTSUBNODE の開始タグおよび終了タグを入力します。

要求の例:

```
<LISTSUBNODE>
</LISTSUBNODE>
```

レポートの出力

表 45. エージェント・サービス・インターフェースの <LISTSUBNODE> 要求の出力

出力タグ	説明
<SUBNODELIST>	サブノードのリスト。
<NODECOUNT>	サブノードの数。
<NAME>	サブノード名。

出力例: エージェントにより、エージェントの既知のすべてのサブノードのリストが戻される

```
<SUBNODELIST>
  <NODECOUNT>3</NODECOUNT>
  <NAME>dyang7ASFSdp:UAGENT00</NAME>
  <NAME>dyang7:TS100</NAME>
  <NAME>dyang7:TS200</NAME>
  </SUBNODELIST>
```

エージェント・サービス・インターフェース - 属性ファイル・リスト

サービス・インターフェース要求で <ATTRLIST> を使用すると、このコンピューター上で使用可能なすべての既知の属性ファイル (.atr) のリストを取得できます。

要求の入力

表 46. エージェント・サービス・インターフェースの <ATTRLIST> 要求

タグ	説明
<ATTRLIST>	ATTRLIST の開始タグおよび終了タグを入力して、属性ファイル・リストの要求を行います。

要求の例:

```
<ATTRLIST>
</ATTRLIST>
```

レポートの出力

表 47. エージェント・サービス・インターフェースの <ATTRLIST> 要求の出力

出力タグ	説明
<LISTATTRFILE>	使用可能な属性ファイル名のリストです。
<ATTRCOUNT>	リスト内の属性ファイルの総数です。
<NAME>	属性ファイルの名前です。

出力例: エージェントにより、コンピューターで使用可能なすべての既知の属性ファイルのリストが戻される

```
<LISTATTRFILE>
  <ATTRCOUNT>16</ATTRCOUNT>
  <NAME>DM3ATR00</NAME>
 <NAME>TS1ATR00</NAME>
 <NAME>TS2ATR00</NAME>
 <NAME>UAGATR00</NAME>
 <NAME>kdy.atr</NAME>
 <NAME>khd.atr</NAME>
 <NAME>kib.atr</NAME>
 <NAME>knt.atr</NAME>
 <NAME>kr2.atr</NAME>
 <NAME>kr3.atr</NAME>
 <NAME>kr4.atr</NAME>
 <NAME>kr5.atr</NAME>
 <NAME>kr6.atr</NAME>
 <NAME>ksh.atr</NAME>
 <NAME>ksy.atr</NAME>
 <NAME>kum.atr</NAME>
</LISTATTRFILE>
```

エージェント・サービス・インターフェース要求 - 属性ファイルの内容

サービス・インターフェース要求で <READATTR> を使用すると、このコンピューター上の指定した属性ファイル (.atr) の内容のリストが取得されます。

要求の入力

表 48. エージェント・サービス・インターフェースの <READATTR> 要求

タグ	説明
<READATTR>	属性ファイルを要求するには、開始と終了の READATTR タグを入力します。
<ATTRFILE>	属性ファイル名。

Universal Agent TS2ATR00 属性ファイルの要求の例:

```
<READATTR>
  <ATTRFILE>TS2ATR00</ATTRFILE>
</READATTR>
```

レポートの出力

表 49. エージェント・サービス・インターフェースの <READATTR> 要求の出力

出力タグ	説明
<ATTRFILE>	属性ファイル名。
<ATTRDATA>	属性ファイルのレコード。

以下の例では、TS2ATR00 属性ファイルの内容が示されます。

```
<ATTRFILE>TS2ATR00</ATTRFILE>
  <ATTRDATA>
 <![CDATA[//1090428005244020 TS200/06.00.00
 //Generated by Universal Agent
  //
  entr ATTR
  name TS2TCPIOQ00.Node_Name
  affi 00000000000000080000000000000000000000000000
  acod TS200
  usag I
  appl TS200
  stmp 1090428005244020
  cvrm 06.00.00
  lvrm 06.00.00
  tabl TS24601600
  mult 1
  samp 3
  colu ORIGINNODE
  type 2
  slng 32
  msid KUM0000
  opgr 0
  atid 065535
  //entr ATTR
  name TS2TCPIOQ00.LocalApplAddress
  atom y
  affi 00000000000000080000000000000000000000000000
  acod TS200
  colu UA1
  type 2
  slng 24
  msid KUM0000
  opgr 2
  atid 065535
  //
  entr ATTR
  name TS2TCPIOQ00.TargetApplAddress
```

```
affi 00000000000000080000000000000000000000000000
acod TS200
colu UA2
type 2
slng 24
msid KUM0000
opgr 2
atid 065535
//
entr ATTR
name TS2TCPIOQ00.SendQueueSize
affi 00000000000000080000000000000000000000000000
acod TS200
colu UA3
type 1
msid KUM0000
opgr 2
atid 065535
mini -2147483648
maxi 2147483647
//
entr ATTR
name TS2TCPIOQ00.RecvQueueSize
affi 00000000000000080000000000000000000000000000
acod TS200
colu UA4
type 1
msid KUM0000
opgr 2
atid 065535
mini -2147483648
maxi 2147483647
//
entr ATTR
name TS2TCPIOQ00._LocalTimeStamp
affi 00000000000000080000000000000000000000000000
acod TS200
colu UA5
type 2
slng 16
msid KUM0000
opgr 2
atid 065535
//
entr HIDDEN
name TS2TCPIOQ00.KUMHELP
affi 00000000000000080000000000000000000000000000
colu KUMHELP
type 3
opgr 0
cost 9
vali ^APPLICATION
vale "No Application Help Defined"
vali ^ATTRGROUP[TCPIOQ]
vale "No attribute group Help Defined"
vali LocalApplAddress
vale "No attribute Help Defined"
vali TargetApplAddress
vale "No attribute Help Defined"
vali SendQueueSize
vale "No attribute Help Defined"
vali RecvQueueSize
vale "No attribute Help Defined"
vali _LocalTimeStamp
vale "Universal Agent inserted attribute per metafile keyword
```

```
  AddTimeStamp specification. It is the 16-byte timestamp value
  when the data arrived."
 ]]></ATTRDATA>
</ATTROUTPUT>
```

エージェント・サービス・インターフェース要求 - 属性グループ・レポート

サービス・インターフェース要求で <REPORT> を使用すると、UNIXOS や NTPROCESS など、TABLENAME 属性で指定された属性グループのレポートを取得できます。

要求の入力

表 50. エージェント・サービス・インターフェースの <REPORT> 要求

タグ	説明
<REPORT>	指定した表のアプリケーション表データを取得するには、開始と終了の REPORT タグを入力します。
<SQLTABLE>	SQLTABLE の開始/終了タグでは、SQL 表定義セットを識別する TABLENAME タグのペアを囲みます。
<TABLENAME>	TABLENAME の開始/終了タグでは、レポートする表の名前を囲みます。これは、開始タグおよび終了タグで囲まれて表示される名前です。表のスペルが不明な場合は、ディレクトリー *<install_dir>*/TMAITM6/ATTRLIB にあるエージェント .atr ファイルのフィールド **tabl** で確認することができます。
<OUTPUT>	オプションです。 レポートのフィルター操作および詳細化には、OUTPUT の開始/終了タグおよびその従属タグを使用します。 **<COLUMN>** 選択した列名を開始タグおよび終了タグで囲んで定義します。 **<FILTER>** 出力データ行のフィルター基準を開始タグおよび終了タグで囲んで定義します。このフィルターは、専用シチュエーションの <CRITERIA> 要素と同じ構文規則に従います。 374 ページの『専用シチュエーション XML 指定』を参照してください。

要求の例 1: UNIX OS 表内のすべての属性のレポート

```
<REPORT>
 <SQLTABLE>
 <TABLENAME>UNIXOS</TABLENAME>
 </SQLTABLE>
</REPORT>
```

要求の例 2: フィルターおよび列を指定した Windows プロセス属性グループのサマリー・レポート

これは、*_Total* 行の値を求める要求です。

```
<REPORT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
   <OUTPUT>
    <COLUMN>ORIGINNODE</COLUMN>
    <COLUMN>TIMESTAMP</COLUMN>
    <COLUMN>INSTCNAME</COLUMN>
    <COLUMN>IDPROCESS</COLUMN>
    <COLUMN>PCTPRCSTME</COLUMN>
```

```
    <COLUMN>THREADCNT</COLUMN>
    <COLUMN>WRKINGSET</COLUMN>
   </OUTPUT>
 <FILTER>
 <![CDATA[ *VALUE INSTCNAME  *EQ _Total]]>
 </FILTER>
 </SQLTABLE>
</REPORT>
```

レポートの出力

表 51. エージェント・サービス・インターフェースの <REPORT> 要求の出力

出力タグ	説明
<REPORTDATA>	出力レポート・データ設定を識別します。
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。
<ROWCOUNT>	表の行数を出力します。
<ROW>	出力の行データを識別します。
<NAME>	出力の列名を開始タグおよび終了タグで囲んで定義します。
<DATA>	出力の列データ値を開始タグおよび終了タグで囲んで指定します。

数値の出力

レポートでは、数値の形式は設定されず、不定形式のままで出力されます。

例えば、取得したレポートにスケール係数が 2 の属性が含まれている場合、その属性の値 **7** は、Tivoli Enterprise Portal のテーブル・ビューには **0.07** と表示されます。このスケール係数は、以下の属性ファイル内の属性定義に scal として示されています。

Windows <*install_dir*>¥TMAITM6¥ATTRLIB¥k*pc*.atr

Linux UNIX <*install_dir*>/*platform*/<*pc*>/tables/ATTRLIB/k*pc*.atr。ここで、*platform* はオペレーティング・システムであり、*pc* は製品コードです。

列挙値も不定形式であるため、例えば、レポートに **1** や **2** のように示される値は、ポータル・クライアントではその等価のテキスト (「**開始済み**」や「**停止済み**」など) が表示されます。列挙型属性は、属性ファイル k*pc*.atr に定義されています。表示値は vale で定義され、不定形式値は vali で定義されます。

出力例 1: サンプルの <REPORT> 要求からの UNIX OS 出力

```
<REPORTDATA><SQLTABLE><TABLENAME>UNIXOS</TABLENAME>
 <ROWCOUNT>1</ROWCOUNT><ROW><COLUMN><NAME>ORIGINNODE</NAME>
 <DATA><![CDATA[fvaix26:KUX]]></DATA></COLUMN><COLUMN>
 <NAME>SAMPLENO</NAME><DATA>0</DATA></COLUMN><COLUMN>
 <NAME>ROWNO</NAME><DATA>0</DATA></COLUMN><COLUMN><NAME>TIMESTAMP</NAME>
 <DATA><![CDATA[1090629105627000]]></DATA></COLUMN><COLUMN>
 <NAME>SYSTEMTYPE</NAME><DATA><![CDATA[AIX]]></DATA> </COLUMN><COLUMN>
 <NAME>SYSTEMVERS</NAME><DATA><![CDATA[5.3]]> </DATA></COLUMN><COLUMN>
 <NAME>TOTREALMEM</NAME><DATA>3915776</DATA> </COLUMN><COLUMN>
 <NAME>TOTVIRTMEM</NAME><DATA>8634368</DATA> </COLUMN><COLUMN>
 <NAME>SYSUPTIME</NAME><DATA>6633819</DATA> </COLUMN><COLUMN>
 <NAME>NOUSRSESS</NAME><DATA>1</DATA> </COLUMN><COLUMN>
 <NAME>NOSYSPROCS</NAME><DATA>112</DATA> </COLUMN><COLUMN>
 <NAME>NETADDR</NAME>
  <DATA><![CDATA[9.42.11.174]]> </DATA></COLUMN><COLUMN>
 <NAME>UNIXUSRCPU</NAME><DATA>1</DATA> </COLUMN><COLUMN>
```

```
<NAME>UNIXSYSCPU</NAME><DATA>1</DATA> </COLUMN><COLUMN>
<NAME>UNIXIDLCPU</NAME><DATA>98</DATA> </COLUMN><COLUMN>
<NAME>UNIXWAITIO</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>VMINRUNQ</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>VMINPGWAIT</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>VMPGFAULTS</NAME><DATA>1538</DATA> </COLUMN><COLUMN>
<NAME>VMPGRCLM</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>VMPGIN</NAME><DATA>2</DATA></COLUMN> <COLUMN>
<NAME>VMPGOUT</NAME><DATA>1</DATA></COLUMN> <COLUMN>
<NAME>VMPGSIN</NAME><DATA>1</DATA></COLUMN> <COLUMN>
<NAME>VMPGSOUT</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>VMFREEMEM</NAME><DATA>7614492</DATA></COLUMN> <COLUMN>
<NAME>VMFREESWAP</NAME><DATA>1019876</DATA> </COLUMN><COLUMN>
<NAME>PSWITCH</NAME><DATA>5357</DATA> </COLUMN><COLUMN>
<NAME>SYSCALL</NAME><DATA>42598</DATA> </COLUMN><COLUMN>
<NAME>SYSFORK</NAME><DATA>337</DATA> </COLUMN><COLUMN>
<NAME>SYSEXEC</NAME><DATA>274</DATA> </COLUMN><COLUMN>
<NAME>BREAD</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>BWRITE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>LREAD</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>LWRITE</NAME> <DATA>0</DATA></COLUMN><COLUMN>
<NAME>PHREAD</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>PHWRITE</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>RCVINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>XMTINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>MDMINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETCONNECT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETSOCKET</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD1</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD2</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>NETLOAD3</NAME><DATA>2</DATA> </COLUMN><COLUMN>
<NAME>MEMFREE</NAME><DATA>108812</DATA> </COLUMN><COLUMN>
<NAME>MEMUSED</NAME><DATA>3806964</DATA> </COLUMN><COLUMN>
<NAME>VMSCAN</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>VMUSEDPRC</NAME><DATA>119</DATA></COLUMN> <COLUMN>
<NAME>VMFREEPRC</NAME><DATA>881</DATA></COLUMN> <COLUMN>
<NAME>CPUBUSY</NAME><DATA>2</DATA></COLUMN> <COLUMN>
<NAME>SYSREAD</NAME><DATA>5694</DATA></COLUMN> <COLUMN>
<NAME>SYSWRITE</NAME><DATA>749</DATA></COLUMN> <COLUMN>
<NAME>NSYSTHRD</NAME><DATA>-1</DATA></COLUMN> <COLUMN>
<NAME>PRUNABLE</NAME><DATA>112</DATA></COLUMN> <COLUMN>
<NAME>PRUNNING</NAME><DATA>-1</DATA></COLUMN> <COLUMN>
<NAME>PSLEEPING</NAME><DATA>0</DATA></COLUMN> <COLUMN>
<NAME>PIDLE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>PZOMBIE</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>PSTOPPED</NAME><DATA>0</DATA></COLUMN><COLUMN>
<NAME>THRDRUNQ</NAME><DATA>-1</DATA></COLUMN><COLUMN>
<NAME>THRDWAIT</NAME><DATA>-1</DATA></COLUMN><COLUMN>
<NAME>BOOTTIME</NAME>
 <DATA><![CDATA[1090413161248000]]> </DATA></COLUMN><COLUMN>
<NAME>PENDIOWT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>STARTIO</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>DEVINT</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
<NAME>UPTIME</NAME>
 <DATA><![CDATA[076d18:43:39]]> </DATA></COLUMN><COLUMN>
<NAME>ZATTRIB</NAME><DATA><![CDATA[ ]]> </DATA></COLUMN><COLUMN>
<NAME>ZVALUE</NAME><DATA><![CDATA[ ]]> </DATA></COLUMN><COLUMN>
<NAME>SWAPFREE</NAME><DATA>7436</DATA> </COLUMN><COLUMN>
<NAME>PGINRATE</NAME><DATA>9</DATA> </COLUMN><COLUMN>
<NAME>PGOUTRATE</NAME><DATA>6</DATA> </COLUMN><COLUMN>
<NAME>PGSCANRATE</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS1</NAME><DATA>1</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS5</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS15</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGINS60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT1</NAME><DATA>3</DATA> </COLUMN><COLUMN>
<NAME>AVPGOUT5</NAME><DATA>3</DATA> </COLUMN><COLUMN>
```

```
 <NAME>AVPGOUT15</NAME><DATA>3</DATA> </COLUMN><COLUMN>
 <NAME>AVPGOUT60</NAME><DATA>3</DATA> </COLUMN><COLUMN>
 <NAME>AVPGSCAN1</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>AVPGSCAN5</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>AVPGSCAN15</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>AVPGSCAN60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>AVPRRUNQ60</NAME><DATA>0</DATA> </COLUMN><COLUMN>
 <NAME>NETADDR6</NAME>
  <DATA><![CDATA[No DNS Entry]]> </DATA></COLUMN><COLUMN>
 <NAME>ZID</NAME><DATA>-1</DATA> </COLUMN><COLUMN>
 <NAME>ZONE</NAME><DATA><![CDATA[-1]]> </DATA></COLUMN>
</ROW></SQLTABLE>
</REPORTDATA>
```

出力例 2: フィルターおよび列が指定されたレポート

これは、行 *_Total* にある Windows プロセス属性の要求の例からの出力です。

```
<REPORTDATA>
 <STATUS>0</STATUS>
 <SQLTABLE>
  <TABLENAME>NTPROCESS</TABLENAME>
  <ROWCOUNT>1</ROWCOUNT>
  <ROW>
   <COLUMN>
    <NAME>ORIGINNODE</NAME>
    <DATA>Primary:DYANG7:NT</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>TIMESTAMP</NAME>
    <DATA>1090303122813634</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>INSTCNAME</NAME>
    <DATA>_Total</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>PCTPRCSTME</NAME>
    <DATA>99</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>IDPROCESS</NAME>
    <DATA>0</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>THREADCNT</NAME>
    <DATA>1057</DATA>
   </COLUMN>
   <COLUMN>
    <NAME>WRKINGSET</NAME>
    <DATA>1088495616</DATA>
   </COLUMN>
  </ROW>
 </SQLTABLE>
</REPORTDATA>
```

エージェント・サービス・インターフェース要求 - エージェント・テーブルおよびシチュエーション・リスト

サービス・インターフェース要求で <TABLESIT> を使用すると、<TABLENAME> 属性に指定されている属性グループと、そのグループで実行されているシチュエーションのレポートを取得できます。

要求の入力

表 52. エージェント・サービス・インターフェースの <TABLESIT> 要求

タグ	説明
<TABLESIT>	エージェント・テーブルおよびシチュエーション・リストを取得するには、TABLESIT の開始/終了タグを入力します。
<SQLTABLE>	SQLTABLE の開始/終了タグでは、SQL 表定義セットを識別する TABLENAME タグのペアを囲みます。
<TABLENAME>	TABLENAME の開始/終了タグでは、レポートする表の名前を囲みます。これは、開始タグおよび終了タグで囲まれて表示される名前です。表のスペルが不明な場合は、ディレクトリー *<install_dir>*/TMAITM6/ATTRLIB にあるエージェント .atr ファイルのフィールド **tabl** でスペルを確認できます。 値 ***ALL** により、既知のすべてのエージェント・テーブルが暗黙指定されます。

要求の例 1: プロセスおよび論理ディスクに対するアクティブな Windows OS シチュエーション

```
<TABLESIT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
 </SQLTABLE>
 <SQLTABLE>
 <TABLENAME>WTLOGCLDSK</TABLENAME>
 </SQLTABLE>
</TABLESIT>
```

レポートの出力

表 53. エージェント・サービス・インターフェースの <TABLESIT> 要求の出力

出力タグ	説明
<SITUATION>	出力シチュエーション設定を定義します。
<NAME>	シチュエーション名を指定します。
<TYPE>	E – エンタープライズ・シチュエーション、P – 専用シチュエーション
<STATUS>	開始/終了タグで囲んだ状況コードを戻します。

出力例: Windows OS エージェントにより、実行中のすべてのプロセス・シチュエーションおよび論理ディスク・シチュエーションが戻される

```
<TABLESIT>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
  <SITUATION>
   <NAME>Check_Process_CPU_Usage</NAME>
  </SITUATION>
  <TYPE>P</TYPE>
  <SITUATION>
   <NAME>Check_Process_CPU_Usage</NAME>
 </SITUATION>
  <TYPE>P</TYPE>
  <SITUATION>
   <NAME>Is_KFC_Running</NAME>
 </SITUATION>
 <TYPE>E</TYPE>
```

```
 </SQLTABLE> <SQLTABLE>
  <TABLENAME>WTLOGCLDSK</TABLENAME>
  <SITUATION>
  <NAME>Check_DiskSpace_Low</NAME>
 </SITUATION>
 <TYPE>P</TYPE>
 </SQLTABLE>
</TABLESIT>
```

エージェント・サービス・インターフェース要求 - 専用シチュエーションの制御

サービス・インターフェースの <PVTCONTROL> 要求を作成し、モニター・エージェント上の専用シチュエーションの開始、停止、または再開を行います。

モニター・エージェント (Tivoli Enterprise Monitoring Agent または Tivoli System Monitor Agent) が開始されると、そのモニター・エージェント用に作成された専用シチュエーションが自動的に開始されます。 PVTCONTROL コマンドにより、エージェントを停止して再開することなく、指定したシチュエーションの開始、停止または再開が可能になります。

要求の入力

表 54. エージェント・サービス・インターフェースの <PVTCONTROL> 要求

タグ	説明
<PVTCONTROL>	専用シチュエーションの制御要求を指定します。
<PVTCOMMAND>	専用シチュエーション・コマンドを指定します。
<PVTSITNAME>	専用シチュエーション名を指定します。
<PVTACTION>	START – 既知のシチュエーション要求を開始します。 STOP – アクティブなシチュエーションを停止します。 RECYCLE – アクティブなシチュエーションを停止して再開します。

要求の例 1: 専用シチュエーション Check_DiskSpace_Low の再開

```
<PVTCONTROL>
 <PVTCOMMAND>
  <PVTSITNAME>Check_DiskSpace_Low</PVTSITNAME>
  <PVTACTION>RECYCLE</PVTACTION>
 </PVTCOMMAND>
</PVTCONTROL>
```

レポートの出力

表 55. エージェント・サービス・インターフェースの <PVTCONTROL> 要求の出力

出力タグ	説明
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。

出力例 1: 専用シチュエーション Check_DiskSpace_Low の再開によりコマンド状況が戻される

```
<PVTCONTROL>
 <STATUS>300</STATUS>
<FILOBJ>
```

エージェント・サービス・インターフェース要求 - シチュエーションの要約

シチュエーション要約コマンドは、モニター・エージェントで実行されている専用シチュエーションのリストの要求に使用します。

要求の入力

表 56. エージェント・サービス・インターフェースの <SITSUMMARY> 要求

タグ	説明
<SITSUMMARY>	動的しきい値のオーバーライド指定を定義します。

```
<SITSUMMARY>
</SITSUMMARY>
```

要求による出力は、 390 ページの『専用シチュエーションの例』に示されている専用シチュエーション構成ファイルのようになります。

レポートの出力

表 57. エージェント・サービス・インターフェースの <SITSUMMARY> 要求の出力

出力タグ	説明
<ROW>	出力データ行を定義します。
<DATA>	Data のタグでダウンロード・ファイルの内容を囲みます。
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。

出力例 1: エージェントによりプロセス状況が戻される

```
<SITSUMMARY>
 <STATUS>0</STATUS>
<FILOBJ>
```

出力例 2: エージェントによりトレース・ログ・ファイルの内容が戻される

```
<SITSUMMARY>
  <STATUS>0</STATUS>
  <ROWCOUNT>5</ROWCOUNT>
 <ROW>
 <DATA><![CDATA[+49BDCB34.001C 00000000 3018060A 2B060106 03010104
 0100060A 0...+..... ]]></DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ +49BDCB34.001C 00000010 2B060104 018D0301 0315
 +.........]]></DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ (49BDCB34.001D-B90:kraaest1.cpp,92,
 "IRA_ConstructTrapVarBindV1") *TRAP-INFO: IRA_ConstructTrapVarBindV1
 - Entry pPDU<39B4C6A> pTrapWork<3CDA0A8> pTrapSit<2B8F098>
 dataBuffer<39BC948> offset<1363> resetTrap<0>]]> </DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ (49BDCB34.001E-B90:kraaesti.cpp,289,
 "addVarBindStringData") <0x39B4C6A,0x16>
 *TRAP-INFO: VarBind 1.3.6.1.4.1.1667.1.2.1.10.1.1 KNT ]]> </DATA>
 </ROW>
 <ROW>
 <DATA><![CDATA[ +49BDCB34.001E 00000000 3014060D 2B060104 018D0301
 02010A01 0...+..... ]]></DATA>
 </ROW>
</SITSUMMARY>
```

エージェント・サービス・インターフェース要求 - エージェント・モニター統計

エージェント・モニター統計コマンドを使用すると、モニター・エージェント・アクティビティーの情報を要求できます。

要求の入力

表 58. エージェント・サービス・インターフェースの <AGENTSTAT> 要求

タグ	説明
<AGENTSTAT>	エージェントの統計要求を指定します。
<SITUATION>	シチュエーションの選択属性を定義します。
<NAME>	シチュエーション名を指定します。既知のすべてのシチュエーションを要求する場合は、*ALL を指定します。デフォルト: ***ALL**
<DAYS>	オプションです。 表示する期間を指定します。例えば、1 を指定すると、今日のデータを取得できます。最大 7 日分のヒストリー・データを取得できます。
<DETAILS>	オプションです。 Yes の場合、1 時間ごとの詳細データを出力します No の場合、状態情報のみを出力します デフォルト: **No**

要求の例 1: 今日のシチュエーション状態統計の取得

```
<AGENTSTAT>
 <SITUATION>
  <NAME>*ALL</NAME>
 </SITUATION>
</AGENTSTAT>
```

要求の例 2: 今日の NT_Service_Error シチュエーション統計の取得

```
<AGENTSTAT>
 <SITUATION>
  <NAME>NT_Service_Error</NAME>
  <DAYS>1</DAYS>
  <DETAILS>Y</DETAILS>
</SITUATION>
</AGENTSTAT>
```

レポートの出力

表 59. エージェント・サービス・インターフェースの <AGENTSTAT> 要求の出力

出力タグ	説明
<TYPE>	シチュエーション・タイプ (Sample または Pure-Event)。
<INTERVAL>	シチュエーションのサンプル間隔 (0 の場合は Pure-Event)。
<ROWSIZE>	サンプル・データの行サイズ。
<FIRSTSTARTTIME>	シチュエーションの初期の開始時刻。
<LASTSTARTTIME>	シチュエーションの最新の開始時刻。
<LAST STOPTIME>	シチュエーションの最後の停止時刻。
<FIRSTEVENTTIME>	シチュエーションが最初にイベントを開いた時刻。
<LASTTRUETIME>	シチュエーションが最後に **True** に評価された時刻。

表 59. エージェント・サービス・インターフェースの <AGENTSTAT> 要求の出力 (続き)

出力タグ	説明
<LASTFALSETIME>	シチュエーションが最後に **False** に評価された時刻。
<TIMESRECYCLED>	シチュエーションの再始動回数。
<TIMESAUTONOMOUS>	シチュエーションがオートノマス・モードになった回数。
<DAY>	日次メトリックの開始。
<DATE>	日付の説明。
<TRUESAMPLES>	True サンプルの行数。
<FALSESAMPLES>	False サンプルの行数。
<TRUERATIO>	True サンプルのパーセント。
<FALSERATIO>	False サンプルのパーセント。
<HOURROWS>	毎時のサンプル行数。
<HOURTRUE>	毎時の True サンプル行数。
<HOURFALSE>	毎時の False サンプル行数。
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。

要求の例 2 の出力例: エージェントにより今日の NT_Service_Error シチュエーション統計が戻される

```
<SITSTATS>
 <SITUATION>
  <NAME>NT_Service_Error</NAME>
  <TYPE>Event</TYPE>
  <INTERVAL>0</INTERVAL>
  <ROWSIZE>3124</ROWSIZE>
  <FIRSTSTARTTIME>Thu Mar 12 23:09:36 2009</FIRSTSTARTTIME>
  <LASTSTARTTIME>NA</LASTSTARTTIME>
  <LASTSTOPTIME>NA</LASTSTOPTIME>
  <FIRSTEVENTTIME>NA</FIRSTEVENTTIME>
  <LASTTRUETIME>NA</LASTTRUETIME>
  <LASTFALSETIME>Fri Mar 13 22:53:31 2009</LASTFALSETIME>
  <TIMESRECYCLED>0</TIMESRECYCLED>
  <TIMESAUTONOMOUS>0</TIMESAUTONOMOUS>
 <DAY>
   <DATE>Fri Mar 13 00:00:00 2009</DATE>
    <TRUESAMPLES>0</TRUESAMPLES>
   <FALSESAMPLES>80</FALSESAMPLES>
   <TRUERATIO>0.00%</TRUERATIO>
   <FALSERATIO>100.00%</FALSERATIO>
    <HOURROWS>0 0 0 0 0 0 0 12 2 2 4 6 0 4 4 6 0 2 5 4 0 15 14 0
     </HOURROWS>
   <HOURTRUE>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
     </HOURTRUE>
   <HOURFALSE>0 0 0 0 0 0 0 12 2 2 4 6 0 4 4 6 0 2 5 4 0 15 14 0
   </HOURFALSE>
 </DAY>
 </SITUATION>
</SITSTATS>
```

エージェント・サービス・インターフェース要求 - ヒストリー・レポート

サービス・インターフェースの <HISTREAD> 要求を作成し、モニター・エージェント上の専用シチュエーションの開始、停止、または再開を行います。

Tivoli Enterprise Monitoring Agents からのヒストリカル・データは、Tivoli Enterprise Portal のテーブル・ビューまたはその他の照会ベース・ビューでタイム・スパンを選択すると表示されます。ポータル以外では、エージェント・サービス・インターフェースからヒストリー・レポートを取得するか、または HISTREAD サービス・インターフェース要求を作成することにより、エンタープライズ・モニター・エージェントからのヒストリカル・データ、あるいはエンタープライズ・モニター・エージェントまたはシステム・モニター・エージェントからの専用ヒストリー・データを確認できます。

要求の入力

表 60. エージェント・サービス・インターフェースの <HISTREAD> 要求

タグ	説明
<HISTREAD>	ヒストリー表データを取得します。
<SQLTABLE>	SQL 表定義設定を識別します。
<TABLENAME>	表の名前を開始タグおよび終了タグで囲んで定義します。表の名前は最長で 10 文字です。
<PVTHIST>	オプションです。 読み取る専用ヒストリーを指定します。エンタープライズの短期間ヒストリーを読み取る直接のエージェントはありません。
<OUTPUT>	オプションです。 出力する表の列の選択を定義します。
<COLUMN>	オプションです。 選択された列名を開始タグおよび終了タグで囲んで定義します。
<FILTER>	オプションです。 出力データ行のフィルター基準を開始タグおよび終了タグで囲んで定義します。詳しくは、専用シチュエーション <CRITERIA> の仕様を参照してください。開始と終了の WRITETIME 列を使用して、ヒストリー・データの読み取り範囲を指定します。特定の MSN ヒストリー・データを選択するには、ORIGINNODE 列を使用します。
<OUTLIMIT>	オプションです。 出力が大量になることに対する保護として、出力レコードの制限を OUTLIMIT の開始タグおよび終了タグで囲んで定義します。

要求の例 1: フィルターおよび列の選択を使用した Windows OS エージェントのプロセス・ヒストリーの取得

```
<HISTREAD>
 <SQLTABLE>
 <TABLENAME>NTPROCESS</TABLENAME>
 <OUTPUT>
  <COLUMN>ORIGINNODE</COLUMN>
  <COLUMN>TIMESTAMP</COLUMN>
  <COLUMN>INSTCNAME</COLUMN>
  <COLUMN>IDPROCESS</COLUMN>
  <COLUMN>PCTPRCSTME</COLUMN>
  <COLUMN>THREADCNT</COLUMN>
  <COLUMN>WRKINGSET</COLUMN>
 </OUTPUT>
 <FILTER>
 <![CDATA[ *VALUE ORIGINNODE *EQ Primary:DYANG3:NT  *AND
   *VALUE WRITETIME  *GE 1090408224500000  *AND
   *VALUE WRITETIME  *LE 1090408234500000]]>
```

```
 </FILTER>
 <OUTLIMIT>5000</OUTLIMIT>
 </SQLTABLE>
</HISTREAD>
```

レポートの出力

表 61. エージェント・サービス・インターフェースの <HISTREAD> 要求の出力

出力タグ	説明
<HISTREADDATA>	出力レポート・データ設定を識別します。
<STATUS>	開始タグおよび終了タグで囲んだ状況コードを戻します。
<ROWCOUNT>	表の行数を出力します。
<ROW>	出力の行データを識別します。
<NAME>	出力の列名を開始タグおよび終了タグで囲んで定義します。
<DATA>	出力の列データ値を開始タグおよび終了タグで囲んで指定します。

出力例 1: Windows OS エージェントにより、4 月 8 日の 午後 10:45 から午後 11:45 までの指定した 7 つの属性に関するプロセス・ヒストリー・データが戻される

```
<HISTREADDATA>
 <SQLTABLE>
  <TABLENAME>NTPROCESS</TABLENAME>
  <ROWCOUNT>212</ROWCOUNT>
  <ROW>
   <COLUMN>
  <NAME>ORIGINNODE</NAME>
    <DATA><![CDATA[Primary:DYANG3:NT]]></DATA>
   </COLUMN>
   <COLUMN>
  <NAME>TIMESTAMP</NAME>
    <DATA><![CDATA[1090408224551430]]></DATA>
   </COLUMN>
   <COLUMN>
   <NAME>INSTCNAME</NAME>
    <DATA>![CDATA[Idle]]> </DATA>
   </COLUMN>
   <COLUMN>
    <NAME>IDPROCESS</NAME>
   <DATA>0</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>PCTPRCSTME</NAME>
   <DATA>74</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>THREADCNT</NAME>
   <DATA>1</DATA>
   </COLUMN>
   <COLUMN>
   <NAME>WRKINGSET</NAME>
   <DATA>16384</DATA>
   </COLUMN>
  </ROW>
  ...
  ...
 </SQLTABLE>
</HISTREADDATA>
```

エージェント・サービス・インターフェース要求 - 構成コントロール

サービス・インターフェース要求を使用すると、構成ロード・リスト要求を処理できます。

許可

サービス・インターフェース要求は、完全な 構成ロード・リスト XML 構文を認識します。 許可される要求は、グループ・アクセス権によって異なります。

- ユーザー ID がアクセス許可グループ・プロファイル (AAGP) の**オペレーション**・グループのメンバーである場合は、既存の構成ロード・リストを使用してファイルをリフレッシュするために <CNFGCOMMAND> 要素を使用でき、<CNFGACTION> のリブート、再ロード、およびダウンロード要求を発行できます。
- ユーザー ID が AAGP の**管理**グループのメンバーである場合は、『構成ロード・リストの XML 仕様』にある構文を使用して、有効な構成ロード・リスト要求を送信できます。

要素

要素とその属性では大/小文字を区別しません。例えば、
<CNFGCOMMAND>、<CnfgCommand>、または <cnfgcommand> と入力できます。

<CNFGCOMMAND>
構成コマンド要求を指定します。次の構成コントロール要求の例では、現行の構成ロード・リストの内容を再ロードします。

```
<CNFGCOMMAND>
  <CNFGACTION>RELOAD</CNFGACTION>
</CNFGCOMMAND>
```

<CNFGACTION>
構成コマンド・アクションを指定します。

リブート
この属性は、構成ロード・リストをダウンロードします。

再ロード
再ロードは、現行のエージェント・ロード・リストの即時再送を実行するために使用します。これによって、指定したすべてのエージェント成果物が更新されている場合はダウンロードされます。 <CnfgCommand> の下の例を参照してください。

ダウンロード
ダウンロードは、送信するファイルを指定するために使用します。<CnfgFile> および <CnfgDisp> の下の例を参照してください。

<CNFGFILE>
オプションです。 <CNFGACTION> がダウンロードの場合、ファイル名の末尾にある 2 つの特定のセグメント。

ファイル名はロード・リストに存在する必要があります。ファイル alert.txt をダウンロードします。

```
<CNFGCOMMAND>
  <CNFGACTION>DOWNLOAD</CNFGACTION>
  <CNFGFILE>alert.txt</CNFGFILE>
</CNFGCOMMAND>
```

<CNFGDISP>

オプションです。 <CNFGACTION> がダウンロードの場合、ファイル名の ID としての既知の特定の構成ファイル属性指定。ファイル定義はロード・リストに存在する必要があります。次の要求の例では、専用シチュエーション構成の XML ファイルをダウンロードします。

```
<CNFGCOMMAND>
  <CNFGACTION>DOWNLOAD</CNFGACTION>
  <CNFGDISP>PVTSIT</CNFGDISP>
</CNFGCOMMAND>
```

<STATUS>

この要素は、<status> および </status> タグで囲まれたステータス・コードを戻す場合に使用します。次の例では、エージェントがコマンド・ステータスを戻します。

```
<CNFGCOMMAND>
  <STATUS>600 - 構成コントロール・コマンドは、正常に完了しました。
  </STATUS>
</CNFGCOMMAND>
```

第 16 章 一元化された構成

一元化された構成機能を使用して、エージェントが収集可能なセントラル・ロケーションでモニター・エージェントの構成ファイルを管理します。

一元化された構成の概要

一元化された構成によって、多数のモニター・エージェント上のローカル構成ファイルを Tivoli Enterprise Monitoring Server に接続せずに更新することができます。

一元化された構成の利点の一部を以下に示します。

- 一貫性のあるエージェントのインストールが保証される
- インストールの支援と構成の複雑さが軽減される
- エージェント・デプロイメントの効率が向上する
- Tivoli Monitoring のスケーラビリティーが向上する
- ユーザーの Web 管理スキルが活用される

一元化された構成とは、1 つの Tivoli モニター・エージェントまたは (可能であれば) 1 つの Web サーバーです。後者の Web サーバーは、同一または異なるコンピューター上のモニター・エージェントによって、そのモニター・エージェントのローカル*構成ロード・リスト* を使用してプルされるエージェント構成ファイルのリポジトリーとして機能します。このリポジトリーには、SNMP アラートと EIF イベント用の構成 XML、自動化スクリプト、他のすべての関連するエージェント運用ファイルなどのファイルを含めることができます。構成ロード・リストには、中央サーバーのロケーションと取得する構成ファイルを指定します。

中央構成サーバー は、バージョン 6.2.2 フィックスパック 2 以降の Tivoli Monitoring エージェントであることも、また WebSphere、IBM HTTP、Microsoft IIS、Apache などの任意の Web サーバーであることも可能です。 IBM では、セキュリティー上の理由から Web サーバーを選択することをお勧めします。

複数の中央構成サーバーを保持して、それらを中央構成サーバーの階層として論理的に配置することができます。

一元化された構成がエージェントによって開始されると、中央構成サーバーからすべてのファイル更新を 1 時間に 1 回プルするようにデフォルトの動作で指定されています。また、更新は、エージェント・サービス・インターフェース要求としてロード・リストを入力することによってオンデマンドで取得することもできます。

エージェントでは、専用シチュエーションや構成ロード・リストなどの、新しくダウンロードされた既知の構成ファイルを、エージェントの再始動なしで動的にアクティブにします。新規変更の有効化を可能にするために、エージェントが再始動する必要があるその他の構成変更には、エージェントの再始動の指定を含めることができるため、これらの構成の更新は介入なしで即時に有効になります。

既存のエージェント用の一元化された構成を実装するための基本的なタスクは、以下のとおりです。

1. 構成ファイルを編成して中央リポジトリーから配布するための戦略を決定し、また構成ファイルを作成します。
2. 中央構成サーバー を構成します。
3. エージェントで初期構成ロード・リストの収集を可能にします。
4. 必要に応じて、中央構成サーバー上の構成ファイルを更新します。

一元化された構成設計

定義する一元化された構成構造は、モニター対象エンタープライズのサイズや編成、管理するモニター・エージェントのタイプ、更新の種類およびその頻度によって異なります。

構成ロード・リスト

新規にインストールされたモニター・エージェントまたは既存のモニター・エージェントのすべてが、構成ロード・リストを使用して一元化された構成に参加できます。構成ロード・リストは、実行中のエージェントに固有の XML 構成ファイルです。これはエージェントに対して、1 つ以上の中央構成サーバーに接続する方法や、サーバーからダウンロードするファイルを指示します。

管理者は、この一元化されたリポジトリーで構成ファイルを管理および更新します。新規エージェントは、初期構成ファイルをこの場所から収集し、定期的または要求時にサーバーに接続して更新や変更を収集します。

中央構成サーバー

構成ロード・リストには、エージェントに対して中央構成サーバーへの接続方法を指示する 1 つ以上の ConfigServer 要素が含まれます。中央構成サーバーには、HTTP を使用するモニター・エージェントに対して提供されるファイルのリポジトリーが含まれます。

サーバーは、要求を認証し、構成アーティクルの最終更新タイム・スタンプ (GMT に設定) を検査します。要求されたファイルのクライアント側コピーがサーバー側コピーよりも古い場合は、構成アーティクルの内容をエージェントに返します。それ以外の場合は、HTTP ステータス 304 - Object Not Modified (オブジェクトが変更されていません) を返します。アーティクルの処理中にエラーが発生した場合、サーバーは他の HTTP ステータスを返します。

中央構成サーバーをデプロイする場合は、次の要因を考慮してください。

ユーザー・アクセス

管理者は、配布が予定されている構成ロード・リストにアクセスし、管理する必要があります。中央構成クライアントは、更新を収集するために中央構成サーバーにアクセスする必要があります。既に Web サーバーを使用していて、Web サーバー上のファイルのアクセスや管理を理解している場合は、任意の Web サーバーを中央構成サーバーとして機能させることができます。これには、エージェント・サービス・インターフェースで使用される Web サーバーも含まれます。

ディレクトリー構造

ファイルを編成できるサーバーおよびクライアントのディレクトリー構造を識別して、サーバーでの重複を最小限に抑えるとともに、管理が必要なファイルの数を削減します。

キーワード置換

構成ロード・リストでキーワード置換を使用すると、構成ファイルの編成を単純化することができます。

例えば、すべての Linux OS エージェントがイベントの定義された 1 セットの専用シチュエーションを実行し、Windows OS エージェントが別のセットを実行する場合、@PRODUCT@ キーワードを使用して、中央構成サーバーの適切なディレクトリーおよびファイルをエージェントに指示することができます。ファイルは、*install_dir* /localconfig ディレクトリー、または IRA_SERVICE_INTERFACE_CONFIG_HOME 環境変数で指定した場所に配置します。例えば、次のようになります。

common
    cnfglist.xml

lz
    lz_situations.xml
    lz_trapcnfg.xml

nt
    nt_situations.xml
    nt_trapcnfg.xml

cnfglist.xml ファイルでは、@PRODUCT@ キーワードを使用してエージェントに正しいファイルを指示できます。以下に例を示します。

```
<ConfigurationArtifact>
  <ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://icvr5a05.tivlab.raleigh.ibm.com/"
   User="itmuser"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="common"
   Disp="CNFGLIST"
   Activate="YES" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="@PRODUCT@_situations.xml"
   Path="@PRODUCT@"
   Disp="PVTSIT"
   Activate="YES" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="@PRODUCT@_trapcnfg.xml"
   Path="@PRODUCT@"
   Disp="TRAPCNFG"
   Activate="RESTART" />
</ConfigurationArtifact>
```

他のキーワードを使用して、各エージェントが正しいファイルを取得するために必要な細分度を作り出すこともできます。

中央構成サーバーとしての Web サーバー

Tivoli モニター・エージェントは、既存の Web サーバーを使用して構成ファイルを収集できます。エージェントが HTTP または HTTPS を使用してアクセスできる任意の Web サーバーを中央構成サーバーとして使用できます。

Web サーバーを使用するには、中央構成サーバー上のファイルへのアクセス権限を持つユーザー ID を作成し、構成ロード・リストでそれらの資格情報を参照します。中央構成サーバーがモニター・エージェントの場合と URL 仕様はわずかに異なりますが、これが、構成ロード・リストにおける唯一の違いです。ConfigServer 要素は、次のようになります。

```
<ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://webserver.domain.com/"
   User="itmuser"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
```

中央構成サーバーとしてのモニター・エージェント

Windows、Linux、および UNIX プラットフォームで実行されるすべてのモニター・エージェント (エンタープライズまたはシステム・モニター) には、中央構成サーバーとして使用できる HTTP ベースのサービス・インターフェースが含まれます。z/OS および i5 上のモニター・エージェントは、HTTP サービス・インターフェースを提供しないため、中央構成サーバーとして使用できません。

Web サーバーではなくモニター・エージェントを中央構成サーバーとして使用すると、Web サーバーを管理する必要がないという利点があり、複数のエージェントを使用してカスケード中央構成サーバーを構成することで、ある程度のワークロード・バランシングを実現できます。

中央構成サーバーへのユーザー・アクセス

エージェント・サービス・インターフェースへのアクセスは、アクセス許可グループ・プロファイル (AAGP) を使用して制御されます。エージェント上のファイルの要求または配置には、メトリックまたはヒストリカル・データの表示よりもさらに多くのセキュリティー権限が必要です。デフォルトでは、エージェントが実行中のホスト・コンピューターで有効な ID であれば、エージェント・サービス・インターフェースにアクセスできます。このようなユーザーは、エージェントによって収集されたメトリック、シチュエーション、およびヒストリカル・データを表示できます。ただしデフォルトの動作では、エージェント・サービス・インターフェースを介した中央構成ファイルへのアクセス権限は、ホストの**管理** ID のみに与えられます。

次のユーザー ID は、エージェントが実行中のプラットフォームにおいて、**管理**グループのデフォルトのメンバーです。

- Windows: Administrator
- Linux, UNIX: root
- z/OS: ITMUSER
- IBM i: QSECOFR

ユーザーは、構成ロード・リストを作成したり、**管理**資格情報を使用して中央構成サーバーとして機能しているモニター・エージェントに接続したりす

ることができます。クライアント・エージェントが中央構成サーバーに接続するために、ID がクライアント・エージェントに存在する必要はありません。

Windows システムの場合、エージェントは AAGP 管理者グループに属するすべてのユーザー・アカウントを自動的に検出し、開始時にこれらのアカウントを AAGP 管理グループに追加します。UNIX および Linux システムの場合、エージェントは root (スーパーユーザー) 権限を持つすべてのユーザー ID を自動的に検出します。エージェントは、開始時にこれらのユーザー ID を AAGP 管理グループに追加します。 (IBM i の QSECOFR および z/OS の ITMUSER というユーザー ID は、この時点では変更されません。)その結果、次のようになります。

- 顧客は、エージェント・サービスを使用するために特殊なユーザー・アカウントを作成する必要はありません。
- 管理者/root ID の公開は回避されます。
- システム上の許可されたアカウントであれば、ファイル・アクセスや AAGP カスタマイズなどの特権エージェント・サービスへのアクセスを自動的に獲得します。

ユーザー ID は暗号化形式で格納できますが、ほとんどの場合、中央構成サーバーをホスティングするシステムでユーザー ID を定義し、そのユーザーをエージェントの AAGP に追加します。

以下の例では、Linux OS エージェント上にユーザーを作成して、中央構成サーバーに管理権限を付与する手順を示します。

1. システムにユーザーを作成します。Linux オペレーティング・システムに「itmuser」という名前のユーザーが作成されます。Linux OS エージェント (lz) が中央構成サーバーです。
2. AAGP.xml ファイルを、*install_dir* /localconfig ディレクトリーに作成します。このファイルで新しい ID を**管理**グループに追加します。

   ```
   <AAGP>
     <AAUSER>
       <ID>itmuser</ID>
       <ASSIGN>AD</ASSIGN>
     </AAUSER>
   </AAGP>
   ```

   デフォルトのローカル構成ディレクトリーは、IRA_SERVICE_INTERFACE_CONFIG_HOME 環境変数で変更できます。

   ヒント: 各エージェントで AAGP ファイルを収集することを検討してください。これにより、エージェント・サービス・インターフェース経由で直接エージェントに接続して、root 以外の ID で構成アクションを実行できるようなります。管理権限でエージェント・サービス・インターフェースに直接接続すると、新規中央構成サーバーに接続したり、ファイルを配置または取得したり、構成ファイルの即時最新表示を強制実行したりするための資格情報を提供できます。
3. 中央構成サーバーとして機能するモニター・エージェントで、構成ロード・リストを編集して、AAGP XML ファイルを読み込むための DISP="AAGP" ConfigFile エントリーを追加します。

このロード・リストでは、自身に接続して新規ユーザー ID を AAGP に追加するために、資格情報 (Linux UNIX root、Windows Administrator) を使用する必要があります。編集後の構成ロード・リストは、次のようになります。

```
<ConfigurationArtifact>
   <ConfigServer
    Name="CENTRAL-CONFIG-SERVER"
    URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
    User="root"
    Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
   <ConfigFile
    Server="CENTRAL-CONFIG-SERVER"
    Name="AAGP.xml"
    Path="/"
    Disp="AAGP" />
</ConfigurationArtifact>
```

4. ロード・リストを、*install_dir* /localconfig/lz/lz_cnfglist.xml に保存します。このディレクトリーは、Linux システムにおけるデフォルトの場所であり、IRA_SERVICE_INTERFACE_CONFIG_LOADLIST 環境変数を使用して変更できます。
5. Linux OS エージェントを開始します。

この中央構成サーバーに接続するすべての中央構成クライアントは、「root」ではなく「itmuser」の資格情報を使用できるようになります。

```
<ConfigServer
  Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
```

カスケード中央構成サーバー

他のモニター・エージェントは、アクセス許可グループ・プロファイル (AAGP) の更新を中央構成サーバーから収集できるため、他のエージェントにファイルを配布するために使用できます。

カスケード・サーバーは、ConfigServer 要素の URL でエージェント・サービス・インターフェースを指定する構成ロード・リストを配布できるように構成する必要があります。

カスケード・サーバーは、他のエージェントに配布するコンテンツをダウンロードするために、DISP=CUSTOM ConfigFile 要素を使用します。

エージェント・サービス・インターフェース

エージェント・サービス・インターフェースを使用して、要求時に構成ロード・リスト要求を入力および処理することができます。 471 ページの『エージェント・サービス・インターフェース要求 - 構成コントロール』を参照してください。

構成ロード・リスト XML 仕様

構成ロード・リスト XML 仕様による XML 構文を使用して、一元化された構成用のロード・リストを作成します。

構成ロード・リストのデフォルトのパスおよびファイル名

以下の構成ロード・リストの各ファイル名がデフォルトです。ここで、*pc* は 2 文字の製品コードです。

Windows *install_dir* ¥localconfig¥*pc*¥*pc*_cnfglist.xml

Linux UNIX *install_dir* /localconfig/*pc*/*pc*_cnfglist.xml

z/OS IRA_SERVICE_INTERFACE_CONFIG_LOADLIST= *PC*CFGLST.RKANDATV

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/a4_cnfglist.xml

デフォルトのパスおよびファイル名を変更するには、IRA_SERVICE_INTERFACE_CONFIG_LOADLIST エージェント環境変数を使用します。489 ページの『一元化された構成用の環境変数』を参照してください。

要素

XML 要素タグおよびその属性は、**大/小文字を区別しません**が、値では**大/小文字を区別します**。例えば、<CONFIGSERVER>、<ConfigServer>、または <configserver> と入力できます。

<ConfigurationArtifact> </ConfigurationArtifact>

ConfigurationArtifact は、ロード・リスト構成文書として識別するルート要素です。ファイルの先頭に <ConfigurationArtifact>、末尾に </ConfigurationArtifact> と入力します。ロード・リスト・ファイルの例:

```
<ConfigurationArtifact>
 <ConfigServer
    Name="AGOURALAB"
    URL="http://9.55.100.99/"
    User="smith"
    Password="{AES256:keyfile:a}hjZM0YaLzpd5JQC5DeboJg==" />
 <ConfigFile
    Server="AGOURALAB"
    Name="Private_Situations.xml"
    Path="ITM/Config/@HOSTNAME@"
    Disp="PVTSIT"
    Activate="YES" />
 <ConfigFile
    Server="AGOURALAB"
    Name="TRAPCNFG.xml"
    Path="ITM/Config/common"
    Disp="trapcnfg"
    Activate="RESTART" />
  <ConfigFile
    Server="AGOURALAB"
  Name="THRESHOLDS.XML"
    Path="ITM/Config/@PRODUCT@"
    Disp="threshold"
    Activate="YES" />
</ConfigurationArtifact>
```

<ConfigServer>

中央構成サーバーを次の属性で定義します。

Name=

SERVER ステートメントのシンボル名を定義します。名前は 32 文字まで使用でき、ロード・リスト内で固有である必要があります。重複した名前は許可されません。

URL= 中央構成サーバーへの接続に使用される URL を定義します。次のいずれかのタイプを使用できます。

- 中央構成サーバーとして機能するエージェント・サービス・インターフェース。次のように指定します。

  HTTP メソッド://ホスト名:ポート
  ///*agent-ServicePoint*/*agent-ServicePoint*

- 中央構成サーバーとして機能する Web サーバー。次のように指定します。

  HTTP メソッド://ホスト名:[ポート]
  /[パス]

値の説明:

HTTP メソッド
: http または https

ホスト名
: 中央構成サーバーのホスト名。ローカル DNS によってホスト名が解決される保証がない場合は、IP アドレスを使用してください。

ポート
: Tivoli Monitoring サービス索引 (KDH コンポーネント・コード) の、またはポートがデフォルトの 80 と異なる場合は Web サーバーの、ターゲット中央構成サーバー・リスニング・ポート。Tivoli Monitoring サービス索引 のデフォルト・ポートは、HTTP の場合は 1920、HTTPS の場合は 3661 ですが、どちらもターゲット・エージェントの KDC_FAMILIES 環境変数を使用してカスタマイズできます。

agent-ServicePoint
: TMS/Engine に登録されたエージェント・サービス・インターフェース名。Windows OS エージェントの場合は `system.myhost_nt`、Linux OS エージェントの場合は `myhost_lz` など。機能をより識別しやすい名前になるように、IRA_SERVICE_INTERFACE_NAME エージェント環境変数を使用してターゲット・エージェントのサービス名をカスタマイズできます。例えば、`https://9.48.123.13:3661///Paris-CSF-A/Paris -CSF-A` のようにします。汎用の Web サーバー構成リポジトリーを使用している場合は、エージェント・インスタンス名定義を省略します。

パス
: 追加のターゲット中央構成サーバー・パス定義です。例えば、`http://9.48.132.40:80/ITM/config` のようにします。

User=
: オプションです。 ターゲット中央構成サーバーのサーバー・ホスト・システム・アカウントのユーザー ID を指定します。

Password=
: オプションです。 ユーザー・パスワードをプレーン・テキストで指定します。または itmpwdsnmp ユーティリティー・プログラムを使

用してユーザー・パスワードを暗号化し、ここで出力 AES データ文字列を指定します。 414 ページの『SNMP パス・キーの暗号化: itmpwdsnmp』を参照してください。

AltServer=

オプションです。 代替サーバー名を指定します。エージェントは、このサーバーに接続またはログオンできない場合、代替サーバー定義を使用してファイル要求 URL を構成します。代替サーバー定義には、追加の代替サーバー指定を含めることはできません。

次の HTTP 状況コードが生じると、エージェントは **AltServer** 指定を使用して要求を再試行します。

401 Unauthorized (許可されていません)

403 Forbidden (禁止されています)

404 Object not found (オブジェクトが見つかりません)

500 Internal server error (内部サーバー・エラー)

503 Service unavailable (サービスを使用できません)

AltServer 属性を使用して代替中央構成サーバーを指定する場合、代替 <ConfigServer> は、これを参照する <ConfigServer> 定義よりも前に定義してください。例:

```
<ConfigServer
 Name="CENTRAL-CONFIG-ALTERNATE"
 URL="http://lnxhostB:1920///lnxhostB_lz/lnxhostB_lz"
 User="itmconfig"
 Password="{AES256:keyfile:a}vHBiEqmmvylNPs90DhQ==" />
<ConfigServer
 Name="CENTRAL-CONFIG-REPOSITORY"
 URL="http://lnxhostA:1920///lnxhostA_lz/lnxhostA_lz"
 User="itmconfig"
 Password="{AES256:keyfile:a}hjZM0YaLzpd5JQC5DJg=="
 AltServer="CENTRAL-CONFIG-ALTERNATE" />
```

487 ページの『構成ロード・リストの環境変数』に記載されている例も参照してください。

<ConfigFile>

事前に定義された <ConfigServer> を名前で識別します。エージェントは、このファイルのダウンロード要求をこの**サーバー**に送信します。

<ConfigFile> 要素属性を定義するときは、環境変数を参照できます。変数を解決する場所は、中央構成サーバーのタイプによって異なります。

- 中央構成サーバーとして機能するモニター・エージェントに対する接続の場合、ConfigFile、Name、および Path 属性を定義するために使用される環境変数は、サーバーで解決されます。
- 中央構成サーバーとして機能する Web サーバーに対する接続の場合、すべて の環境変数がクライアントで解決されます。

Server=

事前に定義された <ConfigServer> を名前で識別します。エージェントは、このファイルのダウンロード要求をこの**サーバー**に送信します。

Name=

サーバー・ロケーションにあるファイル名を指定します。エージェントが環境変数を認識して解決できる場合は、名前に環境変数を含めることができます。

Path= ターゲット <ConfigServer> 上のファイル・ロケーションのパスを指定します。パスには、中央構成サーバーへの接続時にサーバーで解決される環境変数を含めることができます。Web サーバーへの接続の場合、変数は中央構成クライアントで解決されます。

Path は、構成サーバーの HTTP ルートからの相対で指定します。構成サーバーとしてモニター・エージェントを使用する場合、*install_dir* /localconfig ディレクトリーが HTTP ルートです。構成ファイル・アンカーは、IRA_SERVICE_INTERFACE_CONFIG_HOME 環境変数を使用して指定変更できます。

Disp= オプションです。 既知のエージェント構成ファイルのローカル・ファイル属性を指定します。DISP 属性が指定されると、エージェントはクライアント・エージェントの環境設定に基づいて、ダウンロードした ConfigFile (複数可) を 中央構成クライアント・システムの適切な場所に配置します。DISP 属性を使用すると、各 ConfigFile に適したアクティベーション・オプションも有効になります。エージェントは、これらのエージェント構成ファイルのローカル・ロケーションおよび名前を認識しているため、ファイルのダウンロード時にエージェント指定に従ってファイルを保存します。

Disp 属性が省略された場合は、デフォルトで CUSTOM が使用されます。Disp=CUSTOM を使用する時のファイル配置は、Tivoli Monitoring の *install_dir* 内のロケーションに制限されます。この制限は、セキュリティーを強化するためのものです。他の Disp ファイル・タイプでは、指定されたロケーションが *install_dir* ディレクトリー構造の外部にある場合でも、モニター・エージェントで想定するロケーションに配置されます。Disp=CUSTOM を指定する場合は、@ITMHOME@ キーワードを使用して LocalPath を指定すると便利です。

現在、次のファイル属性指定値が定義されています。

CNFGLIST
構成ロード・リスト・ファイル。

PVTSIT
専用シチュエーション XML ファイル。

TRAPCNFG
エージェント SNMP トラップ構成 XML ファイル。

THRESHOLD
シチュエーションしきい値指定変更構成 XML ファイル。

EIFCNFG
EIF 構成ファイル。

EIFMAP
EIF イベント・マッピング・ファイル。

UAMETA
Universal Agent アプリケーション・メタファイル。

PASCAP
プロキシー・エージェント・サービス (エージェント管理サービス) 共通エージェント・パッケージ (CAP) ファイル。PASCAP Disp は、エージェント管理サービスをサポートする Tivoli Monitoring OS Agent でのみ使用できます。これは、製品がインストールされている場合に、CAP ファイルをダウンロードしてアクティブにします。Options=NOPRODUCTCHECK は、CAP ファイルで管理する製品がインストールされていない場合でも、CAP ファイルを強制的に配置するために使用できます。(「Tivoli Agent Management Services のインストールおよび構成」を参照してください。)

AAGP
アクセス許可グループ・プロファイル。アクセス許可グループ定義、およびセキュリティー管理者によって定義されたユーザー ID のアクセス許可グループ割り当てが含まれます。(444 ページの『アクセス許可グループ・プロファイル』 を参照してください。)

CUSTOM
CUSTOM は、DISP が省略された場合に使用されるデフォルト値です。**LocalName** および **LocalPath** 属性は、DISP=CUSTOM で指定される必要があります。CUSTOM ファイルは、エージェントのディレクトリー構造内のロケーションにのみダウンロードできます。

Options=
構成ファイルのハンドリング・オプションを指定します。

NOPRODUCTCHECK
DISP=PASCAP の場合のみ有効です。CAP ファイルのダウンロード操作前に製品のインストール要件をバイパスします。現在のところ、これが定義されている唯一のオプション値です。

LocalName=
ローカル・システム・ファイル名を指定します。LocalName は、DISP が省略されている場合または CUSTOM に設定されている場合のみ使用されます。Disp=CUSTOM で LocalName が省略されている場合は、NAME 属性が使用されます。その他のすべての Disp 値の場合、エージェントはデフォルト値または指定変更パラメーターを使用してファイルのロケーションを識別するため、LocalName は無視されます。

LocalPath=
ローカル・システム・ファイル・パスを指定します。LocalPath は、DISP が省略されている場合または CUSTOM に設定されている場合のみ使用されます。Disp=CUSTOM で LocalPATH が省略されている場合は、PATH 属性が使用されます。その他のすべての Disp

値の場合、エージェントはデフォルト値または指定変更パラメーターを使用してファイルのロケーションを識別するため、LocalPath は無視されます。

Activate=

NO 現在のファイルをダウンロードしたコピーと置換しますが、アクティブにはしません。ダウンロードされたファイルは、既存の構成ファイルよりも新しいものである必要があります。これはデフォルト値です。

RESTART
ファイルのダウンロードに成功した後、エージェントを再起動します。

次の Disp タイプは、更新後の構成ファイルを読み取るためにエージェントを再起動する必要があります。

TRAPCNFG

EIFCNFG

EIFMAP

RESTART を PVTSIT とともに使用すると、専用シチュエーション定義を現在アクティブなシチュエーションとマージするのではなく、定義の置換を強制実行します。

RESTART は、Disp="CUSTOM" の場合も使用可能です。

RESTART は、z/OS と i5 ではサポートされていません。新しい構成をアクティブにするには、エージェント・プロセスを別の方法で再起動する必要があります。

エージェント管理サービス
RESTART コードは、エージェント管理サービスを使用してエージェントをリサイクルします。

- エージェントは、エージェント管理サービスの管理下にある必要があります。これを実現するには、エージェントの共有エージェント・パッケージ (CAP) ファイルで <managerType>ProxyAgentServices</managerType> を指定するか、AMS Start Management アクション実行コマンドを使用します。
- エージェント WATCHDOG がエージェントのリサイクルに使用できるように、OS エージェントがシステムで実行中である必要があります。

エージェントがエージェント管理サービスの管理下にない場合、または ConfigFile が中央構成サーバーから取得されるときに OS エージェントが実行中でない場合、次の結果が生じることが想定されます。

- エージェントは、再起動がバイパスされることを示すメッセージをログ・ファイルに書き込みます。

- モニター・エージェントからの SNMP または EIF イベントが有効な場合、オートノマス・ライフサイクル状況イベントが生成されます。
- ファイルは、エージェントが次回再起動するときにアクティブになります。

デフォルトでは、エージェント管理サービスは zLinux OS エージェントを除くすべての OS エージェントで有効です (zLinux OS エージェントの場合は無効です)。RESTART 機能を利用するには、zLinux OS エージェントのエージェント管理サービス WATCHDOG を手動で有効にする必要があります。手動で有効にしない場合、新しい構成をアクティブにするには、zLinux OS エージェントを別の方法で再起動する必要があります。

エージェント管理サービスを使用してエージェントの可用性をモニターする方法の詳細については、 343 ページの『第 14 章 エージェント管理サービス』を参照してください。

YES ダウンロードしたファイルを現在のファイルにマージするようにエージェントに指示します。新規の変更内容は、エージェントを再起動しなくても動的に反映されます。このオプションは、DISP 値が CNFGLIST、PVTSIT、threshold、および THRESHOLD の場合のみ有効です。

表 62. 構成ロード・リストの <ConfigFile> 要素および Disp タイプで使用可能な Activate オプション。

Disp=	**Activate="Yes"**	**Activate="Restart"**	**Activate="NO"**
CNFGLIST	デフォルト	N/A	N/A
PVTSIT	使用可能	使用可能	デフォルト
TRAPCNFG	N/A	使用可能	デフォルト
EIFCNFG	N/A	使用可能	デフォルト
EIFMAP	N/A	使用可能	デフォルト
THRESHOLD	使用可能	使用可能	デフォルト
UAMETA	N/A	使用可能	デフォルト
PASCAP	CAP ファイルはダウンロード時にアクティブになるため、Activate 属性は適用されません。		
AAGP	デフォルト	N/A	N/A
CUSTOM	N/A	使用可能	デフォルト

<ConfigParm>

オプションです。 エージェント環境変数の指定変更値を指定します。この値は、環境設定を即時更新し、次回の操作間隔またはインスタンスで有効になります。

Interval=

IRA_SERVICE_INTERFACE_CONFIG_INTERVAL を指定変更または設定します。

Backup=
IRA_SERVICE_INTERFACE_CONFIG_BACKUP を指定変更または設定します。

NumbTasks=
IRA_SERVICE_INTERFACE_CONFIG_POOL_SIZE を指定変更または設定します。

MaxWait=
IRA_SERVICE_INTERFACE_CONFIG_MAX_WAIT を指定変更または設定します。

構成ロード・リストのキーワード置換

キーワード置換を使用して、常にさまざまなエージェントやロケーションに適用できる構成ロード・リストを作成します。

Tivoli モニター・エージェントは構成ロード・リスト属性の特定のキーワードを認識し、中央構成クライアントのランタイム値を使用して置換します。

@ITMHOME@ を除き、英数字以外の文字はすべて、出力ではハイフン (-) に変更されます。構成ロード・リストのキーワードは以下のとおりです。

@PRODUCT@	モニター・エージェントの、小文字の 2 文字の製品コードです。例: Windows OS エージェントでは、@PRODUCT@_trapcnfg.xml は nt_trapcnfg.xml に解決されます。
@ITMHOME@	IBM Tivoli Monitoring のインストール・パスです。例: これが Linux システムでデフォルトのインストール・パスが使用されている場合、@ITMHOME@ は /opt/IBM/ITM/ に解決されます。
@MSN@	管理対象システム名です (サブノード名ではなく)。例: エージェントの管理対象システム名が primary:icvw3d62:nt の場合、@MSN@ は primary-icvw3d62-nt に解決されます。
@TASKNAME@	モニター・エージェントのプロセス名です。例: klzagent; kntcma。
@VERSION@	モニター・エージェントの製品バージョンです。例: エージェントのバージョンが 6.2.2 フィックスパック 2 の場合、@VERSION@ は 06-22-02 に解決されます。
@HOSTNAME@	コンピューターのホスト名です。例: myhost。
@IPADDRESS@	コンピューター・ネットワーク・インターフェースの IP アドレスです。例: エージェントの IP アドレスが 9.42.38.333 の場合、@IPADDRESS@ は 9-42-38-333 に解決されます。
@OSTYPE@	オペレーティング・システムのタイプです。有効な値には z/OS、Tandem、 AS/400、 Win98、 Win95、 WinNT、 Win2K、 WinXP、 Windows、 Win2003、 WinVista、 Windows7、および Win2008 があります。その他のすべてのプラットフォームを示す OSTYPE は、**uname** コマンドを使用して取得されます。特定のコンピューターの OSTYPE は、System Type の下にリストされる RAS1 ログ、またはサービス・コンソールを起動して表示される画面の右上隅で確認できます。
@OSVERSION@	オペレーティング・システムのバージョンです。例: Red Hat Enterprise Linux バージョン 5 (64 ビット) は 2-6-18-128-el5 に解決され、Windows 2003 (32 ビット) ServicePack 2 は 5-2-sp2 に解決されます。
@SYSTEMID@	コンピューター・システム ID です。例: システム ID icvr4a04.mylab.mycity.ibm.com は icvr4a04-mylab-mycity-ibm-com として出力されます。

474 ページの『中央構成サーバー』の、キーワード編成および構文の例を参照してください。

構成ロード・リストの環境変数

属性に固定値を入力する代わりに、構成ロード・リストで環境変数を参照できます。変数置換により、同じロード・リスト定義を異なる環境に適用できます。

構成ロード・リストで参照する際、環境変数はパーセント記号 (%) で囲みます。Windows オペレーティング・システムでは環境変数がパーセント記号で区切られるため、これは Windows のみの要件と思われるかもしれませんが、パーセント記号区切りはすべてのプラットフォームで構成ロード・リスト内の環境変数を識別するのに使用されます。

構成ロード・リストの環境変数が中央構成サーバーまたは中央構成クライアントのどちらで解決されるかは、モニター・エージェントまたは Web サーバーのどちらが中央構成サーバーとして機能しているかによって異なります。

- モニター・エージェントが中央構成サーバーとして機能している場合、構成ロード・リストの環境変数は、中央構成サーバーで環境を使用して解決されます。
- Web サーバーが中央構成サーバーとして機能している場合、構成ロード・リストの環境変数は、中央構成クライアント (要求を作成しているモニター・エージェント) で環境を使用して解決されます。

構成ロード・リストで変数置換を使用する方法を示すために、2 つのモニター・エージェントが中央構成サーバーとして機能している環境を想定します。環境変数 SALES_CNFG_FILES を使用して、会社の販売部門のシステムで使用される構成ファイルを含むディレクトリーを識別するとします。プライマリー中央構成サーバーは、**winhost** というサーバー上の Windows OS エージェントです。

```
IRA_SERVICE_INTERFACE_CONFIG_HOME=C:¥IBM¥ITM¥ConfigFiles
```

販売部門の構成は、C:¥IBM¥ITM¥ConfigFiles¥Sales というディレクトリーにあるため、以下を設定します。

```
SALES_CNFG_FILES=Sales
```

開発部門にも、**linuxhost** サーバー上の Linux OS エージェントで構成された中央構成サーバーがあります。開発部門では、販売システムの構成ファイルの現在のコピーも保持されます。**winhost** が使用できないときに新規エージェントがデプロイされる場合、開発部門のエージェントが代替中央構成サーバーとして使用されます。開発部門の Linux OS エージェントは、IRA_SERVICE_INTERFACE_CONFIG_HOME のデフォルト値 (/opt/IBM/ITM/localconfig) を使用します。

販売部門の構成ファイルを /opt/IBM/ITM/localconfig/eastcoast/sales に置くため、以下のように設定します。

```
SALES_CNFG_FILES=eastcoast/sales
```

これは販売部門のブートストラップ構成ロード・リストです。

```
<ConfigurationArtifact>
 <ConfigServer Name="BACKUP-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
```

```
  Password="{AES256:keyfile:a}8wNnAEj6uLMTTOeaC+2rfQ==" />
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://winhost:1920///primary.winhost_nt/primary.winhost_nt/"
  User="itmuser"
  Password="{AES256:keyfile:a}8wNnAEj6uLMTTOeaC+2rfQ=="
  AltServer="BACKUP-CONFIG-SERVER" />
  <ConfigFile Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="%SALES_CNFG_FILES%"
   Disp="CNFGLIST"
   Activate="YES" />
</ConfigurationArtifact>
```

エージェントが **winhost** に接続する場合、エージェントは C:¥ibm¥ITM¥ConfigFiles¥Sales¥cnfglist.xml を収集します。 **winhost** が使用できない場合、エージェントは **linuxhost** に接続して /opt/IBM/ITM/localconfig/eastcoast/sales/cnfglist.xml を収集します。

仕様の環境変数を使用して、個々の中央構成サーバーで追加のカスタマイズを行うことができます。

ブートストラップ構成ロード・リスト

初期構成ロード・リストを配置する場合、モニター・エージェントが中央構成サーバーから収集する必要のあるすべてのコンポーネントを即時に識別するファイルを配置できます。ただし、これは、すべてのエージェントに固有の構成ロード・リスト・ファイルを配置しなければならないことを意味します。中央構成クライアントが、常に構成サーバーから収集する項目の 1 つがロード・リストです。これにより、ロード・リストを構成サーバーから変更できます。

完全な構成ロード・リストを識別するため、一元化された構成操作を初期化するには、エージェントに最初の構成ロード・リストを取得するために接続先を通知するだけで済みます。 DISP=CNFGLIST ファイルを定義するために 1 つの ConfigServer 要素と 1 つの ConfigFile 要素で構成される簡単な構成ロード・リストを使用して、一元化された構成操作をブートストラップできます。

この例では、ConfigServer URL が中央構成サーバーの場所およびユーザー名とパスワードを識別して、そのサーバーにアクセスできるようになっています。 ConfigFile 要素は ConfigServer 要素で指定されたサーバーをポイントして、構成ロード・リスト・ファイルを製品のパスにある cnfglist.xml として識別します。

```
<ConfigurationArtifact>
  <ConfigServer
   Name="CENTRAL-CONFIG-SERVER"
   URL="http://winhost:1920///primary.winhost_nt/primary.winhost_nt/"
   User="Administrator"
   Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
  <ConfigFile
   Server="CENTRAL-CONFIG-SERVER"
   Name="cnfglist.xml"
   Path="@PRODUCT@"
   Disp="CNFGLIST"
   Activate="YES" />
</ConfigurationArtifact>
```

エージェントの正しいロード・リストを識別するブートストラップ構成ロード・リストの作成後、ファイルを配置してエージェントを再起動します。

一元化された構成用の環境変数

環境変数は、一元化された構成用のエージェント環境をカスタマイズするために使用することができます。このカスタマイズの目的は、ブートストラップ中央構成サーバー、中央構成クライアント動作の制御、およびモニター・エージェントが中央構成サーバーとして機能する場合の動作の制御です。

エンタープライズ・モニター・エージェントの場合、環境変数はエージェントの環境ファイル内に設定されます。システム・モニター・エージェントでは、環境変数は *pc*_silent_install.txt 応答ファイル内に設定されます。システム・モニター・エージェント のインストールについて詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『システム・モニター・エージェントによるオペレーティング・システムのモニター』を参照してください。

ブートストラップ中央構成サーバー

モニター・エージェントは、始動時にまず、その構成ロード・リストの XML ファイルを探します。構成ロード・リストが存在しない場合、エージェントはその環境ファイルに下の各変数が存在しないか確認します。エージェントでは、初期の、つまりブートストラップの ロード・リストを以下の環境値から構成し、中央構成サーバーに接続して構成ロード・リストをダウンロードします。

IRA_CONFIG_SERVER_URL
サーバーの URL を指定します。例えば、http://9.52.111.99 などです。

IRA_CONFIG_SERVER_USERID
サーバーのユーザー ID を指定します。デフォルト: itmuser。

IRA_CONFIG_SERVER_PASSWORD
プレーン・テキストまたは AES 暗号化パスワード・ストリングで、ユーザー・パスワードを指定します。

IRA_CONFIG_SERVER_FILE_PATH
中央構成サーバー上の構成ロード・リストへのパスを指定します。デフォルト: loadlist/@PRODUCT@。キーワードのリストについては、 486 ページの『構成ロード・リストのキーワード置換』を参照してください。

IRA_CONFIG_SERVER_FILE_NAME
中央構成サーバー上の構成ロード・リスト・ファイルの名前を指定します。デフォルト: **cnfglist.xml**。

中央構成クライアント動作

以下のエージェント環境変数は、エージェントが一元化された構成用のクライアントとして動作する方法に影響を与えます。これらのエージェント環境変数を使用して、デフォルトとは異なる構成ロード・リスト・ファイル、更新が存在しないかをチェックするために、中央構成サーバーに接続する頻度、および前回のダウンロード以降に変更された構成ファイルのみをダウンロードするか、すべてのファイルをダウンロードするかを指定します。

IRA_SERVICE_INTERFACE_CONFIG_LOADLIST
この変数を使用して、デフォルトの構成ロード・リストを指定変更します。

構成ロード・リストの絶対パスとファイル名を指定します。以下の構成ロード・リストの各ファイル名がデフォルトです。ここで、*pc* は 2 文字の製品コードです。

Windows *install_dir* ¥localconfig¥*pc*¥*pc*_cnfglist.xml

Linux UNIX *install_dir* /localconfig/*pc*/*pc*_cnfglist.xml

z/OS IRA_SERVICE_INTERFACE_CONFIG_LOADLIST= *PC*CFGLST.RKANDATV

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/a4_cnfglist.xml

IRA_SERVICE_INTERFACE_CONFIG_INTERVAL
エージェントで中央構成サーバーに更新が存在するかどうかのチェックを試行する頻度を指定します。間隔を分単位で指定します。 1 日は 1440 分で、1 週間は 10080 分 (最大値) です。デフォルト: **60** 分。

IRA_SERVICE_INTERFACE_CONFIG_BYPASS_TIMESTAMP
N に設定すると、エージェントは、ローカル・バージョンのタイム・スタンプよりも新しい UTC のタイム・スタンプのある構成ファイルのみをダウンロードして置き換えます。デフォルト: **N**。このパラメーターを **Y** に設定すると、エージェントはタイム・スタンプをバイパスして、間隔ごとの後に必ずファイルをダウンロードします。

ベスト・プラクティスとして、ネットワーク全体にわたってシステム時刻を同期し、ファイルがダウンロード後の時差内で変更された場合でも、中央構成サーバーよりも前の時刻で稼働しているモニター・エージェントが更新を見逃さないようにします。

IRA_SERVICE_INTERFACE_CONFIG_BACKUP
新規構成ファイルがダウンロードされると、エージェントは既存のローカル・ファイルを、サフィックス 1 から 5 までをファイル名に付加することで名前を変更し、そのファイルをバックアップ・ディレクトリーへ移動することでバックアップ・コピーにします。この変数では、保持するバックアップ・バージョン数を指定します。最小値はバックアップなしの 0 で、最大値は 5 です。デフォルトのバックアップ・バージョン数: **2**。

IRA_SERVICE_INTERFACE_CONFIG_BACKUP_DIR
この環境変数を使用して、デフォルトとは異なるバックアップ・ディレクトリーを設定します。デフォルトのバックアップ・ディレクトリーは、以下のとおりです。

Windows *install_dir* ¥localconfig¥*pc*¥backup

Linux UNIX *install_dir* /localconfig/*pc*/backup

z/OS RKANDATV DD データ・セット

IBM i /QIBM/UserData/IBM/ITM/localconfig/a4/backup

IRA_SERVICE_INTERFACE_CONFIG_MAX_WAIT
ロード・リストに指定されたすべての構成ファイルを中央構成リポジトリーからダウンロードするための、最大待機時間を秒単位で定義します。有効な時刻範囲は、15 秒から 300 秒までです。デフォルト: **60** 秒。

IRA_SERVICE_INTERFACE_CONFIG_PASCAP_FACTOR
Linux UNIX 中央構成クライアントのみ。モニター・エージェントでエージェント管理サービスの共通エージェント・パッケージ (CAP) フ

ファイルの出力遅延間隔を算出するために使用する時間の増倍係数です。遅延間隔は、この係数が乗算された KCA_DISCOVERY_INTERVAL 環境変数から導き出されます。エージェントでは、最小係数値の 1 が強制されます。デフォルト: **1.5**。

IRA_SERVICE_INTERFACE_CONFIG_POOL_SIZE
エージェントでは、複数のロード・リスト・アーティクルを同時に処理するためにタスクのスレッド・プールを作成します。エージェントでは、プール・タスクによって処理される FIFO キューに要求を出力します。デフォルトのタスク数: **10**。

中央構成サーバー動作

以下のエージェント構成パラメーターは、エージェントが一元化された構成用のサーバーとして動作する方法に影響を与えます。

IRA_SERVICE_INTERFACE_CONFIG_HOME
エージェントが構成サーバーとして使用されている場合、この設定はデフォルトの中央構成リポジトリーのロケーションを指定変更するために使用することができます。中央構成サーバーによって処理されるファイルを配置するために使用されるデフォルトのロケーションは、*install_dir* /localconfig です。

Web サーバーの HTTP ファイルのルートは、Web サーバー管理者によって定義され、変更できません。定義されたリポジトリーのロケーション以外にある成果物を参照するための ../../ などの相対パス指定は、使用することができません。また、新規のリポジトリー・ロケーションはルート・ディレクトリーにはできません。

IRA_SERVICE_INTERFACE_NAME
優先エージェント・サービス・インターフェース名を指定してより機能的に分かりやすい名前を定義し、エージェントが生成する k*pc*agent (*pc* は 2 文字の製品コード) の形式のデフォルト名 (kntagent、kmqagent など)、または *pc*agent の形式のデフォルト名 (uagent02 など) と置き換えて、システムに 2 番目にインストールされた Universal Agent インスタンスを識別します。

デフォルト:

Windows system.*hostname_pc*

Linux UNIX *hostname_pc*

例: Windows OS エージェント用のデフォルトの agent-ServicePoint は、***hostname*_nt** です。ホスト・システム winhost1 上で稼働する Windows OS エージェントの、中央構成サーバーに接続するための URL は、https://winhost1:3661///winhost1_nt/winhost1_nt です。
IRA_SERVICE_INTERFACE_NAME= **ConfigServer-A** の場合、URL は `https://winhost1:3661///ConfigServer-A/ConfigServer-A` です。

KDE_TRANSPORT
KDE_TRANSPORT 環境変数を使用して、デフォルトの HTTP 用の 1920、または HTTPS 用の 3661 とは異なるポートを指定します。

多機能の UNIX システムおよび Linux システムでは特に、デフォルトのポート設定を変更しないでください。これは、多くのコンポーネントが同じシ

ステムに配置され、それらのコンポーネントの一部が HTTP ポートおよび HTTPS ポートで使用されているデフォルト値に依存している場合があるためです。

注: KDE_TRANSPORT 変数は、KDC_FAMILIES 変数を置き換え、オーバーライドします。KDC_FAMILIES 変数がファイル内に存在する場合は、新しい KDE_TRANSPORT 変数に準拠させる KDC_FAMILIES 設定をコピーします。詳しくは、*IBM Tivoli Monitoring インストールおよび設定ガイド*のポータル・サーバーに関するトピック『ポート番号割り当ての制御』を参照してください。

問題判別

以下の診断オプションは、エージェント・コンポーネントに設定することができます。出力は、ras1 というログ・ファイルです。

IRA_DEBUG_SERVICEAPI=Y
エージェント・コンポーネント名: サービス・インターフェース

IRA_DEBUG_PRIVATE_SITUATION=Y
エージェント・コンポーネント名: 専用シチュエーション

IRA_DEBUG_TRANSCON=Y
エージェント・コンポーネント名: トランスポート・コンジット

KDH_DEBUG=D
エージェント・コンポーネント名: Tivoli Monitoring サービス索引の HTTP サービス。

z/OS 上の構成ファイルでパスワードの暗号化を使用可能にする

エージェント・オートノミーの構成 XML ファイルには、プレーン・テキストで入力できるパスワードを持つユーザー資格情報が含まれています。資格情報を保護するには、通常、これらの構成ファイルへのアクセスを保護することが適切です。また、パスワードを暗号化形式で構成ファイル内に保管することによって、セキュリティーの層を 1 つ追加することもできます。

始める前に

エージェントから SNMP アラートを使用可能にしている場合は、SNMP v1、v2c コミュニティー・ストリング、SNMP v3 認証、およびプライバシー・パスワードを、トラップ構成ファイルである *PC*TRAPS.RKANDATV に暗号化形式で保管することができます。

「一元化された構成」を使用可能にしている場合、ConfigServer パスワード属性が *PC*CFGLST.RKANDATV 構成ロード・リスト・ファイルに保管される際、またはそのパスワード属性で K*PC*ENV 環境ファイル内にある IRA_CONFIG_SERVER_PASSWORD パラメーターを使用しているときは、そのパスワード属性を暗号化できます。

Windows、Linux、および UNIX の各システムでは、パスワードとコミュニティー・ストリングは、Tivoli Management Services インフラストラクチャーで提供される GSKIT 暗号化ユーティリティーを使用して、暗号化および暗号化解除されます。

z/OS では GSKit は、Integrated Cryptographic Service Facility、つまり、ICSF と呼ばれています。これらのストリングが暗号化形式で z/OS に保管される場合、ICSF サブシステムが z/OS システム上で使用可能になっている必要があります。また、エージェントでの使用のためにストリングを暗号化解除できるように、ICSF モジュールを z/OS モニター・エージェント開始 PROC に追加する必要もあります。

手順

1. IBM 暗号化コプロセッサーを少なくとも 1 つインストール済みで、また ICSF もインストール済みであることを確認します。
2. z/OS エージェントのランタイム環境内の RKANPARU データ・セットに KAES256 というメンバーを作成します。必ずご使用の環境全体で使用される暗号鍵と同じ暗号鍵を使用してください。メンバーの KAES256 が z/OS 構成ツールによって Tivoli Enterprise Monitoring Server on z/OS 用の同じ暗号鍵で既に作成されていて、z/OS エージェントがモニター・サーバーと同じランタイム環境内で構成されている場合は、このステップをスキップすることができます。
   - メンバーの KAES256 をモニター・サーバーの RKANPARU データ・セットから z/OS エージェントの RKANPARU データ・セットにコピーします。
   - また、KAES256.ser ファイルを分散システムの `keyfiles` ディレクトリーからコピーすることもできます。このディレクトリーでは、itmpwdsnmp ツールを実行してパスワードとコミュニティー・ストリングを暗号化します。 z/OS エージェントの RKANPARU データ・セットのメンバー KAES256 に、KAES256.ser ファイルをバイナリー・モードでアップロードします。KAES256.ser は分散システム上で 48 バイトで、RKANPARU データ・セットのメンバー KAES256 内でブランクが埋め込まれます。
   - z/OS 構成ツールを使用してメンバーの KAES256 を作成する手順については、*Tivoli Enterprise Monitoring Server on z/OS* の構成のトピック『z/OS 上のハブ・モニター・サーバーおよびリモート・モニター・サーバーの構成』を参照してください。
3. z/OS エージェントの既存の開始 PROC RKANMODL DDNAME に ICSF モジュールを連結します。 z/OS エージェントの開始 PROC を編集し、ICSF サポートを RKANMODL DDNAME に追加します。 以下に RKANMODL 例を示します。ここで、CSF.SCSFMOD0 は ICSF 暗号化解除モジュールが含まれているデータ・セットです。

```
//RKANMODL DD DISP=SHR,DSN=my_load_modules
// DD DISP=SHR,DSN=TDOMPT.&LVMLVL..MODL
// DD DISP=SHR,DSN=TDOMPT.&CMSLVL..MODL
// DD DISP=SHR,DSN=CSF.SCSFMOD0
```

4. モニター・サーバーまたは z/OS モニター・エージェント、あるいはその両方を再始動します。

次のタスク

`itmpwdsnmp` ユーティリティーを使用して、暗号化されたパスワードとコミュニティー・ストリングを作成します。このユーティリティーは、分散プラットフォーム上の Tivoli Enterprise Monitoring Agent フレームワーク内でのみ使用できます。エージェント・フレームワークは、Tivoli Monitoring Base DVD または Tivoli Monitoring Agent DVD からインストールすることができます。分散システム上で、対話モードによって `itmpwdsnmp` ツールを実行して、構成ファイル内に配置される

パスワードを暗号化します。手順については、 414 ページの『SNMP パス・キーの暗号化: itmpwdsnmp』を参照してください。

一元化された構成のセットアップ例

このセットアップ例では、計画における考慮事項、および一元化された構成用に Tivoli Monitoring 環境とファイルを準備するために必要な手順を示します。

ディレクトリー構造の作成

提供するファイルの種類を決定し、各クライアント・エージェントが適切なファイルを収集できるように、構成ロード・リストで使用できるキーワードを許可するコンピューターでディレクトリー構造を作成します。

中央構成サーバーとして使用されるエージェントで、ファイルを提供するデフォルトのホーム・ディレクトリーは、すべてのプラットフォームで *install_dir* /localconfig です。このディレクトリーは、エージェントの環境ファイルで IRA_SERVICE_INTERFACE_CONFIG_HOME 環境変数を使用して再配置できます。

このセットアップ例では、中央構成サーバーのホーム・ディレクトリーを次のロケーションに再配置しています。

install_dir /configserver

次のサブディレクトリーを作成します。

install_dir /configserver/common には、すべてのエージェントで同じファイルが格納されます。

install_dir /configserver/nt には、Windows OS エージェントで使用されるファイルが格納されます。これらのファイルは、@PRODUCT@ キーワードを使用して場所が指定されます。

install_dir /configserver/lz には、Linux OS エージェントで使用されるファイルが格納されます。これらのファイルは、@PRODUCT@ キーワードを使用して場所が指定されます。

install_dir /configserver/ux には、UNIX OS エージェントで使用されるファイルが格納されます。これらのファイルは、@PRODUCT@ キーワードを使用して場所が指定されます。

install_dir /configserver/myfiles には、配布する他のファイルが格納されます。

キーワード @OSTYPE@ および @OSVERSION@ は、さまざまなファイルを異なるシステム・グループに提供するときに便利です。例えば、UNIX システムでは @OSTYPE@ を使用して、AIX シチュエーションを Solaris シチュエーションから分離します。 486 ページの『構成ロード・リストのキーワード置換』を参照してください。

中央構成サーバーの root パスワードの入手

このセットアップ例では、エージェントが始動するたびに AAGP ファイルをロードするために、中央構成サーバーで使用されるパスワードを構成ロード・リストに格納します。

V6.2.2 以降の任意のエージェントで使用可能な itmpwdsnmp ユーティリティーを使用して、パスワードを暗号化します。

Windows C:¥ibm¥ITM¥TMAITM6¥itmpwdsnmp.bat

Linux UNIX /opt/IBM/ITM/bin/itmpwdsnmp.sh

Linux コマンド行での表示例を次に示します。

```
itmpwdsnmp.sh

Enter the password to be encrypted:
Confirm string:
{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==
```

エージェントが中央構成サーバーにアクセスするために使用する ID の選択

このセットアップ例では、**itmuser** です。エージェントが中央構成サーバーに接続するために使用するパスワードは、構成ロード・リストに格納されます。

itmpwdsnmp ユーティリティーを使用して、itmuser ID のパスワードを暗号化します。(各エージェントでこの ID を定義します。ID は、エージェントの AAGP に追加されます。)

Windows C:¥ibm¥ITM¥TMAITM6¥itmpwdsnmp.bat

Linux UNIX /opt/IBM/ITM/bin/itmpwdsnmp.sh

AD グループに管理 ID を追加する AAGP.xml ファイルの作成

中央構成サーバーへのアクセスに使用される**管理** ID は、事前定義された AD 許可グループに追加されます。

このセットアップ例では、*install_dir* /configserver/common ディレクトリーの中央構成サーバーに保存されている AAGP.xml ファイルを保存します。

```
<AAGP>
 <AAUSER>
  <ID>itmuser</ID>
  <ASSIGN>AD</ASSIGN>
 </AAUSER>
</AAGP>
```

この AAGP.xml ファイルは、中央構成サーバーに AAGP を設定します。このセットアップ例で、中央構成サーバーは接続元のエージェントにこのファイルを提供します。そのため、このセットアップ例が単純化されます。ただし、異なるエージェント・セットを使用して、固有の AAGP ファイルを収集することができます。その場合、エージェントのエージェント・サービス・インターフェースで操作するために異なるアクセス権セットが設定されるように、ID とグループの各種組み合わせを使用します。ダウンロードされる AAGP は、エージェント・サービス・インターフェースへ 接続するときに使用されます。エージェントは、中央構成サーバーに接続するために、エージェントが収集した AAGP で定義された ID を使用します。

中央構成サーバー用構成ロード・リストの作成

このセットアップ例では、Linux OS エージェントを中央構成サーバーとして使用し、*install_dir* /localconfig/lz_cnfglist.xml を作成します。これは、エージェントの構成ロード・リストのデフォルトの場所です。(ロード・リスト・ファイルを localconfig ディレクトリーに配置するのは、IRA_SERVICE_INTERFACE_CONFIG_HOME を使用してデフォルトの中央構成リポジトリーの場所を移動した理由の 1 つです。エージェントは、他のエージェントに提供するのと同じ localconfig ファイルを使用できます

が、中央構成サーバーが配布するファイルとは別にしておくほうが便利なこともあります。)cnfglist.xml を使用すると、中央構成サーバーが自身に AAGP をロードできます。

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="root"
  Password="{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
</ConfigurationArtifact>
```

汎用ブートストラップ構成ロード・リストの作成

特定のロード・リストを検索するためにエージェントが使用する汎用ブートストラップ構成ロード・リストを作成します。このロード・リストは、エージェントが収集する必要のあるファイルの完全なリストを提供するために使用されます。この手順は必須ではありませんが、実行すると、中央構成サーバーでファイルを編成する方法を変更できます。実行する方法はいくつかあります。

このセットアップ例では、以下の設定を使用して *install_dir* /configserver/common/bootstrap_cnfglist.xml ファイルを作成します。

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
  Path="@PRODUCT@"
  Disp="CNFGLIST"
  Activate="YES" />
</ConfigurationArtifact>
```

ブートストラップ CNFGLIST にエージェントの AAGP を含める必要はありません。エージェントはこのファイルを使用して、エージェントが使用する固有の構成リストを見つけます。この CNFGLIST の有効期間は数秒間です。この例では、エージェントは @PRODUCT@ キーワードで識別されるディレクトリーで cnfglist.xml という名前のファイルを探します。ベスト・プラクティスは、構成サーバーのブートストラップ CNFGLIST を見つけ、(各エージェントの中央構成操作の開始メカニズムを変更するのではなく) 各エージェントが構成サーバー上でこのファイルを直接変更することで自身の CNFGLIST を識別できるようにすることです。

すべての Windows OS エージェントで使用する CNFGLIST の作成

この例では、構成ロード・リストを *install_dir* ¥configserver¥nt¥confglist.xml に作成します。

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="root"
  Password="{AES256:keyfile:a}qNf3u5TzYsiNXRacS4/sXQ==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
```

```
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
  Path="@PRODUCT@"
  Disp="CNFGLIST"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="@PRODUCT@_situations.xml"
  Path="@PRODUCT@"
  Disp="PVTSIT"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="@PRODUCT@_trapcnfg.xml"
  Path="@PRODUCT@"
  Disp="TRAPCNFG"
  Activate="RESTART" />
</ConfigurationArtifact>
```

すべての Linux OS エージェントで使用する CNFGLIST の作成

この例では、構成ロード・リストを *install_dir* /configserver/lz/cnfglist.xml に作成します。これらは、*install_dir* /configserver/myfiles 内のすべてのファイルを収集させるエージェントです。

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="AAGP.xml"
  Path="common"
  Disp="AAGP" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="cnfglist.xml"
  Path="@PRODUCT@"
  Disp="CNFGLIST"
  Activate="YES" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="myfile1.sh"
  Path="myfiles"
  LocalPath="@ITMHOME@/tmp" />
<ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="myfile2.sh"
  Path="myfiles"
  LocalPath="@ITMHOME@/tmp" />
</ConfigurationArtifact>
```

配布する他のファイルの作成

他のエージェント製品コードの構成ロード・リスト、およびデプロイする他のファイルを作成し、それらを中央構成サーバーに配置します。

モニター・エージェントを有効化して一元化された構成の使用を開始する

498 ページの『一元化された構成の開始』では、一元化された構成の使用を開始するいくつかの方法を説明しています。

このセットアップ例では、クライアント・エージェントの環境ファイルで以下の環境変数を設定できます。

```
IRA_CONFIG_SERVER_URL=http://linuxhost:1920///linuxhost_lz/linuxhost_lz
IRA_CONFIG_SERVER_USERID=itmuser
IRA_CONFIG_SERVER_PASSWORD={AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==
IRA_CONFIG_SERVER_FILE_PATH=common
IRA_CONFIG_SERVER_FILE_NAME=bootstrap_cnfglist.xml
```

または、次のような *install_dir* /localconfig/*pc*/*pc*_confglist.xml ファイルを作成する方法もあります。

```
<ConfigurationArtifact>
 <ConfigServer Name="CENTRAL-CONFIG-SERVER"
  URL="http://linuxhost:1920///linuxhost_lz/linuxhost_lz/"
  User="itmuser"
  Password="{AES256:keyfile:a}2fhfCvELPHKm94/OkbOjyw==" />
 <ConfigFile Server="CENTRAL-CONFIG-SERVER"
  Name="bootstrap_cnfglist.xml"
  Path="common"
  Disp="CNFGLIST"
  Activate="YES" />
</ConfigurationArtifact>
```

一元化された構成の開始

エージェントごとの構成ロード・リストの設計と中央構成サーバーの作成が完了すると、各エージェントで一元化された構成に接続して、その使用を開始する準備が整います。

一元化された構成を使用するためにエージェントを使用可能にすることができます。これは、デフォルトの中央構成サーバーを指定するためにエージェント環境変数を編集するか、構成ロード・リスト・ファイルをコンピューターに配置してエージェントを再始動するか、またはサービス・インターフェース要求を送信することによって実行します。

エージェント環境変数を使用した一元化された構成の開始

一元化された構成用のエージェント環境変数を使用して、中央構成サーバーのロケーションを特定し、初期 (ブートストラップ) 構成ロード・リストをダウンロードすることができます。これらの環境変数は、ローカルの構成ロード・リストが存在しない場合にのみ使用されます。

初期構成ロード・リスト・ファイルが設定されると、モニター・エージェントではそのファイルを使用し始め、環境変数の使用を試行しなくなります。ローカルの構成ロード・リストを削除する (システム・モニター・エージェントについては、サイレント・インストールを実行する必要もあります) と、エージェントでは再び環境変数を使用してブートストラップ構成ロード・リストをダウンロードするようになります。 (488 ページの『ブートストラップ構成ロード・リスト』 を参照してください。)

エンタープライズ・モニター・エージェントの環境変数の開始

中央構成サーバーを指示し、また初期の構成ロード・リストをダウンロードするには、Tivoli Enterprise Monitoring Agentの一元化された構成環境変数を使用します。

手順

1. エンタープライズ・モニター・エージ ェントがインストールされているコンピューターで、以下のように「Tivoli Enterprise Monitoring Services の管理」またはコマンド行でエージェントの環境ファイルを開きます。
   - 以下のようにして、Tivoli Enterprise Monitoring Services の管理 を開始します。

     Windows **「スタート」→「プログラム」→「IBM Tivoli**

Monitoring」→「Tivoli Enterprise Monitoring Services の管理」をクリックします。

Linux UNIX *ITM_dir* が IBM Tivoli Monitoring のインストール・ディレクトリーの場合、*ITM_dir*/bin ディレクトリーに移動して、./itmcmd manage [-h *ITM_dir*] を実行します。モニター・エージェントを右クリックして、**「拡張」 → 「ENV ファイルの編集」**をクリックします。

- コマンド行で、下の各エージェント構成ディレクトリーに変更して移動し、テキスト・エディターで環境ファイルを開きます。ここで、*pc* は 2 文字の製品コードです。

  Windows *install_dir* ¥TMAITM6[_x64]¥k*pc*env

  Linux UNIX *install_dir* /config/*pc*.ini

2. 中央構成サーバーへの接続方法、および初期 (ブートストラップ) 構成ロード・リストのダウンロード方法を以下のように指定します。

   IRA_CONFIG_SERVER_URL
   サーバーの URL を指定します。例えば、http://9.52.111.99 などです。

   IRA_CONFIG_SERVER_USERID
   サーバーのユーザー ID を指定します。デフォルト: itmuser。

   IRA_CONFIG_SERVER_PASSWORD
   プレーン・テキストまたは AES 暗号化パスワード・ストリングで、ユーザー・パスワードを指定します。

   IRA_CONFIG_SERVER_FILE_PATH
   中央構成サーバー上の構成ロード・リストへのパスを指定します。デフォルト: loadlist/@PRODUCT@。キーワードのリストについては、486 ページの『構成ロード・リストのキーワード置換』を参照してください。

   IRA_CONFIG_SERVER_FILE_NAME
   中央構成サーバー上の構成ロード・リスト・ファイルの名前を指定します。デフォルト: **cnfglist.xml**。

3. 環境ファイルを保存し、変更内容を適用するエージェントをリサイクルします。

システム・モニター・エージェントのインストール時の一元化された構成環境変数の設定

システム・モニター・エージェントのサイレント応答ファイル内にある一元化された構成環境変数を使用して、中央構成サーバーをポイント、初期 (ブートストラップ) 構成ロード・リストをダウンロードすることができます。

このタスクについて

システム・モニター・エージェントは、そのサイレント・インストールの終了時に開始されます。ローカル構成ファイルがない場合、エージェントは実行されますが、専用シチュエーションを実行することも、SNMP アラートまたは EIF イベントを送信することもありません。一元化された構成を使用すると、エージェントでは、これらのファイルを取得し、すぐに使用できます。システム・モニター・エージェントのインストールでは、サイレント応答ファイル内のエントリーを使用して、エージェントの環境ファイル内にエントリーを作成します。

サイレント応答ファイル、その構成方法、およびその起動方法について詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『システム・モニター・エージェントによるオペレーティング・システムのモニター』を参照してください。

手順

1. Tivoli Monitoring Agent インストール・メディアで *pc*_silent_install.txt 応答ファイル (ux_silent_install.txt など) を見つけて、そのコピーを作成します。
2. テキスト・エディターでこのコピーしたサイレント応答ファイルを開きます。
3. 中央構成サーバーへの接続方法、および初期構成ロード・リストのダウンロード方法を指定します。

   SETENV_ IRA_CONFIG_SERVER_URL
   サーバーの URL を指定します。例えば、http://9.52.111.99 などです。

   SETENV_ IRA_CONFIG_SERVER_USERID
   サーバーのユーザー ID を指定します。デフォルト: itmuser。

   SETENCR_IRA_CONFIG_SERVER_PASSWORD
   AES 暗号化パスワード・ストリングでユーザー・パスワードを指定します。パスワード・ストリングをプレーン・テキストで入力する場合は、環境変数の接頭部に SETENCR_ ではなく SETENV_ を付けます。

   SETENV_ IRA_CONFIG_SERVER_FILE_PATH
   中央構成サーバー上の構成ロード・リストへのパスを指定します。デフォルト: loadlist/@PRODUCT@。キーワードのリストについては、486 ページの『構成ロード・リストのキーワード置換』を参照してください。

   SETENV_ IRA_CONFIG_SERVER_FILE_NAME
   中央構成サーバー上の構成ロード・リスト・ファイルの名前を指定します。デフォルト: **cnfglist.xml**。

   SETENV_parameter=value ステートメントにより、エージェントの環境ファイル内に *parameter=value* ステートメントが作成されます。また、*SETENCR_parameter=value* ステートメントにより *parameter={AES256:keyfile:a}encryptedvalue* ステートメントが作成されます。
4. 以下のようにサイレント・インストールのプロシージャーを起動します。
   Windows システム上で起動される nt_silent_installcc.txt という名前のサイレント・インストール・ファイルの例

   ```
   silentInstall.cmd -p nt_silent_installcc.txt
   ```

   UNIX システム上の /opt/IBM/sma パスにある ux_silent_installcc.txt という名前のサイレント・インストール・ファイルの例

   ```
   silentInstall.sh -h /opt/IBM/sma/ -p ux_silent_installcc.txt
   ```

例

この例では、システム・モニター・エージェントをローカル・コンピューターにインストールして、それを一元化された構成用に構成するために、インストール・メディアからの nt_silent_install.txt のコピーがどのように編集される場合があるかを示しています。

変更前

```
;License Agreement=I agree to use the software only in accordance with
the installed license.

;SETENV_IRA_CONFIG_SERVER_URL=http://configserver.domain.com:1920
;SETENV_IRA_CONFIG_SERVER_USERID=itmuser
;SETENCR_IRA_CONFIG_SERVER_PASSWORD=plaintext_or_encrypted_using_itmpwdsnmp
;SETENV_IRA_CONFIG_SERVER_FILE_PATH=initloadlist/@PRODUCT@
;SETENV_IRA_CONFIG_SERVER_FILE_NAME=cnfglist.xml
```

変更後

```
License Agreement=I agree to use the software only in accordance with
the installed license.

SETENV_IRA_CONFIG_SERVER_URL=http://mysystem.mydomain.ibm.com:1920
SETENV_IRA_CONFIG_SERVER_USERID=itmuser
SETENCR_IRA_CONFIG_SERVER_PASSWORD={AES256:keyfile:a}encryptedpassword
SETENV_IRA_CONFIG_SERVER_FILE_PATH=bootstraploadlist
SETENV_IRA_CONFIG_SERVER_FILE_NAME=cnfglist.xml
```

ロード・リスト・ファイルを使用した一元化された構成の開始

構成ロード・リスト・ファイルの作成が完了したら、一元化された構成を適切なロケーションに配置し、エージェントを開始して、これを開始します。これは、非エージェント・デプロイ・バンドルを使用するか、またはコマンド行インターフェースによって **tacmd putfile** を使用して手動で実行することができます。

ロード・リスト・ファイルの手動での配置による開始

一元化された構成は、エージェント構成ディレクトリーに構成ロード・リスト・ファイルを配置して、エージェントをリサイクルすることによって開始することができます。

始める前に

478 ページの『構成ロード・リスト XML 仕様』で説明されている XML タグ付けを使用して、構成ロード・リスト・ファイルを作成します。

手順

1. システムにローカルでアクセスして、構成ロード・リスト の *pc*_cnfglist.xml をエージェントの *install_dir* /localconfig/*pc* ディレクトリーに配置します。ここで、*pc* は 2 文字の製品コードです。

   Windows *pc*_cnfglist.xml

   Linux UNIX *pc*_cnfglist.xml

   z/OS *PC*CFGLST.RKANDATV

   IBM i a4_cnfglist.xml

2. エージェントをリサイクルします。

タスクの結果

開始時に、構成ロード・リスト・ファイルが、中央構成サーバーの接続 URL とそのサーバーからダウンロードするファイルを取得するために読み取られます。

非エージェント・バンドルのリモート・デプロイメントを使用した開始

ご使用の環境に Tivoli Enterprise Monitoring Server に接続された既存のエージェントが多数含まれている場合、リモート・デプロイメントを使用して構成ロード・リストをエージェントに配布することができます。 Agent Builder を使用して、非エージェント・デプロイメント・バンドルを作成できます。

手順

1. Agent Builder を使用して、非エージェント・デプロイ・バンドルを作成します。 詳しくは、*IBM Tivoli Monitoring Agent Builder* ユーザーズ・ガイド (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/builder/agentbuilder_user.htm)を参照してください。
   a. このバンドルに共通ブートストラップ構成ロード・リストの confglist.xml ファイルを追加します。
   b. デプロイを計画しているエージェントの正しいロケーションにファイルをコピーする独自のコピー・コマンドを作成します。 Linux OS エージェント用のインストール・コマンドの例を次に示します。

      ```
      cp |DEPLOYDIR|/cnfglist.xml |CANDLEHOME|/localconfig/lz/lz_cnfglist.xml
      ```

   c. 新規構成ロード・リストがデプロイされた後にその使用を開始するために、エージェントをリサイクルします。
      - 必要に応じて、エージェント管理サービス WATCHDOG を使用するインストール後コマンドを作成して、エージェントをリサイクルします。エージェントのバイナリー・アーキテクチャー・ディレクトリーにある pasctrl ユーティリティーへの完全修飾パスを指定する必要があるため、このコマンドはサポート予定のプラットフォームごとに 1 つ作成します。
      - 使用できるインストール後コマンドをいくつか以下に示します。

        Windows

        ```
        install_dir ¥TMAITM6[_x64]¥kcapasctrl.exe recycle nt
        ```

        Linux

        ```
        install_dir /lx8266/lz/bin/pasctrl.sh recycle lz
        ```

        UNIX

        ```
        install_dir /aix526/ux/bin/pasctrl.sh recycle ux
        ```

      - 非 OS エージェントでは、OS エージェントからの WATCHDOG を引き続き使用します。この例としては、Windows 上のマルチインスタンス DB2 エージェントがあります。このエージェントは、インストール後コマンドでインスタンス名を指定する必要があるエージェント管理サービスによって管理されます。したがって、デプロイ・バンドル内に再始動を組み込むことは、最良の方法ではない可能性がありますが、標準のインスタンス名が使用される場合は、この組み込みを行うことができます。

        ```
        install_dir ¥tmaitm6¥kcapasctrl.exe recycle –o db2inst1 ud
        ```

      - また、さらに拡張されたロジックが含まれたスクリプトをデプロイ・バンドル内に組み込んで、エージェント・インスタンスをリサイクルした後、インストール後コマンドでそのスクリプトを呼び出すこともできます。

        ```
        Deploy_dir/afterscript.sh
        ```

d. リモート・デプロイメント・バンドルを生成します。

e. エージェントがデプロイ・バンドル内のインストール後コマンドを使用して再始動されなかった場合は、エージェントをリサイクルして構成ロード・リストをアクティブにします。

- 312 ページの『Tivoli Enterprise Portalからのエージェント・プロセスの開始、停止、およびリサイクル』を参照してください。
- OS エージェントは、AMS Recycle Agent Instance TakeAction を使用してポータル・クライアント内でリサイクルすることができます。
- AMS Recycle Agent Instance アクション実行コマンドは、CLI の tacmd executeAction を使用して実行することもできます。 OS エージェントの例をいくつか以下に示します。

Windows

```
tacmd executeaction -n "AMS Recycle Agent Instance" -t nt –m
Primary:winhost:NT -c value="Monitoring Agent for Windows OS,
kntcma.exe,,"
```

Linux

```
tacmd executeaction -n "AMS Recycle Agent Instance" -t lz –m
linuxhost:LZ -c value="Monitoring Agent for Linux OS,klzagent,,"
```

UNIX

```
tacmd executeaction -n "AMS Recycle Agent Instance" -t ux –m
unixhost:KUX -c value="Monitoring Agent for Unix OS,kuxagent,,"
```

2. CLI の **tacmd addbundles** を使用してデポにバンドルを追加します。
3. エージェントにバンドルをデプロイします。このデプロイは、ポータル・クライアント内の「管理対象システムの追加」を使用する (309 ページの『Tivoli Enterprise Portal からのエージェントの追加』を参照) か、またはモニター・サーバーから CLI を介して **tacmd addSystem** を使用して (*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照) 行います。
4. エージェントがデプロイ・バンドル内のインストール後コマンドを使用して再始動されなかった場合は、ステップの 1.e で説明しているようにエージェントをリサイクルして構成ロード・リストをアクティブにします。

tacmd putfile を使用した開始

一元化された構成は、CLI の **tacmd putfile** を使用してモニター・エージェントに構成ロード・リストを転送して開始することができます。

このタスクについて

以下のステップを実行して、一元化された構成を開始するモニター・エージェントに構成ロード・リストをプッシュします。 *IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)には、tacmd とそれらの構文についての説明があり、また各種例が記載されています。

手順

1. 次のようにして、ハブ・モニター・サーバーにログオンします。

   ```
   tacmd login –s myhubserver –u myusername –p mypassword –t 1440
   ```

   ここで、*myhubserver* はハブ・モニター・サーバーの完全修飾ホスト名で、また *myusername* と *mypassword* がモニター・サーバーのオペレーティング・システムにログオンするための有効なユーザー ID です。
2. ファイルを次のコマンドでプッシュします。tacmd putfile –m Primary:winhost:NT -s C:¥config¥cnfglist.xml -d C:¥IBM¥ITM¥localconfig¥nt¥nt_cnfglist.xml -t text
3. エージェントをリサイクルして、構成ロード・リストをアクティブにします。Tivoli Enterprise Portal からのエージェントの開始、停止、およびリサイクルを参照してください。
   - OS エージェントは、次のように AMS Recycle Agent Instance タスク・インスタンスを使用して、ポータル・クライアント内でリサイクルすることができます。OS Agent の「エージェント管理サービス」ワークスペースを開きます。「エージェントのランタイム状況」表ビュー内の OS エージェントを右クリックして、「**アクション実行**」 - 「**選択**」をクリックします。「**AMS Recycle Agent Instance**」を選択します。
   - AMS Recycle Agent Instance アクション実行コマンドは、CLI の **tacmd executeAction** を使用して実行することもできます。 OS エージェントのサンプルをいくつか以下に示します。

     Windows

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t nt -m
     Primary:winhost:NT -c value="Monitoring Agent for Windows OS,
     kntcma.exe,,"
     ```

     Linux

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t lz -m
     linuxhost:LZ -c value="Monitoring Agent for Linux OS,klzagent,,"
     ```

     UNIX

     ```
     tacmd executeaction -n "AMS Recycle Agent Instance" -t ux -m
     unixhost:KUX -c value="Monitoring Agent for Unix OS,kuxagent,,"
     ```

サービス・インターフェース要求を使用した一元化された構成の開始

サービス・インターフェース要求は、ブラウザーで対話式に送信でき、また kshsoap を使用してスクリプトから送信することもできます。サービス・インターフェースを使用して、構成ロード・リストを要求として送信することによって、一元化された構成を開始します。

エージェント・サービス・インターフェースでの開始

エージェント・サービス・インターフェースを使用して、構成ロード・リストを要求として送信することによって、一元化された構成を開始します。

このタスクについて

以下のステップを実行して、エージェント・サービス・インターフェースで構成ロード・リストを要求として入力します。

手順

1. ブラウザーを開き、URL の http://*hostname*:1920 または https://*hostname*:3661 でエージェントのサービス索引にアクセスします。ここで、hostname は、モニター・エージェントがインストールされているコンピューターの完全修飾名または IP アドレスです。
2. 「**IBM Tivoli *pc* エージェント・サービス・インターフェース**」リンクをクリックします。ここで、*pc* は 2 文字の製品コードをです。
3. プロンプトが出されたら、ユーザー名とパスワードを入力します。この ID は、中央構成クライアント・エージェント上のアクセス許可グループ・プロファイルの**管理**グループのメンバーである必要があります。
4. サービス・インターフェース要求へのリンクを選択します。
5. 構成ロード・リスト XML ファイルの内容を「エージェント・サービス・インターフェース要求」テキスト・ボックスに貼り付けた後、この要求を送信します。

次のタスク

ローカル構成をオンデマンドで最新表示する場合はいつでも、エージェント・サービス・インターフェースを使用して、構成ロード・リストをサービス・インターフェース要求として送信することができます。

サービス・インターフェース API (kshsoap) の使用の開始

サービス・インターフェースは、カスタム・インターフェースの作成を可能にする API です。エージェントには、サービス・インターフェースの機能を示すサンプル HTML ファイルが用意されています。この API は、Java、Visual Basic、Perl、HTML およびその他の言語を使用してプログラムでアクセスすることもできます。Tivoli Enterprise Monitoring Server には、*kshsoap* というコマンド行ユーティリティーがあり、これをスクリプト内で使用してこれらのサービス・インターフェース要求を送信できます。 kshsoap を使用して、一元化された構成を開始できます。

手順

1. <UUSER> および <UPASS> 要素を使用して **request.xml** というファイルを作成し、kshsoap がエージェント・サービス・インターフェースに接続する際に必要な資格情報を指定します。 この ID は、要求の送信先のターゲット・システムで定義する必要があります。また ID は、ターゲット・エージェントのアクセス許可グループ・プロファイルの**管理**グループのメンバーであることが必要です。
   例:

```
<ConfigurationArtifact>
  <UUSER>root</UUSER>
  <UPASS>{AES256:keyfile:a}ENRUCXLW40LpR0RtGSF97w==</UPASS>
    <ConfigServer
        Name="CENTRAL-CONFIG-SERVER"
        URL="http://winhost:1920///system.winhost_nt/system.winhost_nt/"
        User="Administrator"
        Password="{AES256:keyfile:a}vHBiEqmmvylNPs90Dw1AhQ==" />
    <ConfigFile
        Server="CENTRAL-CONFIG-SERVER"
        Name="cnfglist.xml"
```

```
        Path="@PRODUCT@"
        Disp="CNFGLIST"
        Activate="YES" />
</ConfigurationArtifact>
```

パスワードを暗号化せずにプレーン・テキストで入力する場合は、<UUSER> および <UPASS> 要素を <UNAME> および <UWORD> に置き換えることができます。

2. エージェント・サービス・インターフェース要求の URL を含む、**urls.txt** という名前の別のテキスト・ファイルを作成します。以下に例を示します。

```
http://linuxhost:1920///linuxhost_lz/linuxhost_lz
http://unixhost:1920///unixhost_ux/unixhost_ux
```

3. kshsoap を使用して、**request.xml** を **urls.txt** にリストされているサービス・インターフェースに送信します。 Windows ベースのモニター・サーバーでは、kshsoap.exe は *install_dir* ¥CMS ディレクトリーにあり、Linux または UNIX ベースのモニター・サーバーでは、kshsoap.exe は *install_dir* /*interp*/ms/bin ディレクトリーにあります。

   - Windows

     install_dir ¥CMS¥kshsoap *path_to_file*¥request.xml *path_to_file*¥urls.txt

   - Linux UNIX

     install_dir /*interp*/ms/bin/kshsoap
     path_to_file/request.xml *path_to_file*/urls.txt

z/OS でのエージェント・オートノミー

エージェント・オートノミーのトピック全体が、z/OS ベースのモニター・エージェントでのファイルおよび例外の参照となっています。このトピックではそのような情報をまとめています。

中央構成サーバー

中央構成サーバーは、分散システム上に配置する必要があります。z/OS システムはサポートされていません。

構成ロード・リスト

モニター・エージェントは、エージェント開始時にすべての項目を構成ロード・リストにダウンロードします。このエージェントは、初回のファイル・ダウンロードのタイム・スタンプを参照として使用し、構成ファイルの最終変更日時の追跡を開始します。このタイム・スタンプ後にファイルのサーバー・コピーに行った変更はダウンロードされ、ファイルの最終変更日時のタイム・スタンプが更新されます。

RKANDATV データ・セットにおける z/OS モニター・エージェントのローカル構成メンバーのデフォルト名

ここで、*PC* は 2 文字の製品コードです。

*PC*CFGLST
: ローカル構成ロード・データ・セット・メンバー名

*PC*THRES
: ローカルのしきい値指定変更ファイル名

*PC*TRAPS
ローカルの SNMP トラップ構成ファイル名

*PC*SICNFG
ローカル・エージェントの専用シチュエーション構成ファイル名

*PC*EIF ローカル・エージェントの EIF イベントマップ構成ファイル名

*PC*EVMAP
ローカル・エージェントの EIF 宛先構成ファイル名

Activate="RESTART" は z/OS ではサポートされていません
RESTART オプションは、ファイルのダウンロードが正常に完了した後にエージェントを再始動するために使用されます。z/OS および i5 オペレーティング・システムではサポートされていません。新しい構成をアクティブにするには、エージェント・プロセスを別の方法で再起動する必要があります。

同じアドレス・スペース内で実行されている複数のエージェント
*&hilev.&rte.*RKANPARU データ・セットの KDSENV メンバーで定義されたオーバーライド・パラメーターは、アドレス・スペース内で実行されているすべてのエージェントに使用されます。すべてのエージェントが同じ EIF イベント宛先を共有する可能性があるため、これは IRA_EIF_DEST_CONFIG に関して適切に機能します。他のオーバーライド・パラメーターも使用できますが、識別されたデータ・セット・メンバーが複数のエージェントの定義をまとめる必要がある場合があります (推奨されていません)。ベスト・プラクティスは、同じアドレス・スペースで複数のエージェントを実行する場合に、ローカルの構成データ・セット・メンバーに対してデフォルトの命名規則を使用することです。

パスワードの暗号化
ローカル構成 XML ファイルには、プレーン・テキストで入力できるパスワードが必要な資格情報が含まれています。資格情報を保護するには、通常、これらの構成ファイルへのアクセスを保護することが適切です。また、パスワードを暗号化形式で構成ファイル内に保管することによって、セキュリティーの層を 1 つ追加することもできます。

エージェントから SNMP アラートを使用可能にしている場合は、SNMP v1、v2c コミュニティー・ストリング、SNMP v3 認証、およびプライバシー・パスワードを、トラップ構成ファイルである *PC*TRAPS.RKANDATV に暗号化形式で保管することができます。

一元化された構成を使用可能にしている場合、構成ロード・リスト・ファイルである xxCFGLST.RKANDATV に、ConfigServer パスワード属性が格納する際に、IRA_CONFIG_SERVER_PASSWORD 環境変数を使って、このパスワードの属性を暗号化することができます。

方法については、*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS 共通計画および構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)の『z/OS 上の構成ファイルでパスワードの暗号化を使用可能にする』を参照してください。

第 17 章 ヒストリカル・データの管理

Tivoli Management Services で提供されるツールを使用すると、データ・サンプルの収集と保存、ヒストリカル・レポートの表示、リレーショナル・データベースへのデータのアップロード (長期保存用、または短期ヒストリーを区切り文字で区切られたフラット・ファイルに変換するため)、およびデータの集約とプルーニングを行うことができます。これらのトピックでは、ヒストリカル・データ収集に使用されるコンポーネント、データの格納方法、およびデータ収集の構成とデータベースの管理に関するベスト・プラクティスについて説明します。

「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Data Warehouse ソリューション』のトピックでは、Tivoli Data Warehouse のインストール方法および構成方法と、必須のエージェント (ウェアハウス・プロキシー、要約およびプルーニング・エージェント) について説明されています。

*Tivoli Enterprise Portal ユーザーズ・ガイド*の『ヒストリカル収集の構成』のトピックでは、属性グループに対するヒストリカル・データ収集の構成方法、指定した時刻範囲に対するヒストリカル・データのレポートの取得方法、トレンド分析用のグラフに対するヒストリカル・ベースラインの適用方法、およびヒストリカル・データを使用したシチュエーションしきい値のモデル化の方法について説明されています。

IBM Tivoli Monitoring コマンド・リファレンス (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)には、コマンド行に指定可能な **tacmd** ヒストリー・コマンドについて説明されています。これにより、ヒストリカル・データ収集の構成、その定義の表示、およびヒストリカル・データ収集の定義のインポート/エクスポートを行うことができます。

ヒストリカル・データ収集について

レポート作成および分析にヒストリカル・データを使用できるようにするには、ヒストリカル・データ収集を設定する必要があります。これらの 1 つ以上の収集は、ヒストリカル・データを収集する各属性グループに対して構成され、指定する管理対象システムに配布されます。

ヒストリカル・データ収集

構成プログラムを使用すると、ヒストリカル・データが収集されるように指定できます。ヒストリカル・データは、Tivoli Enterprise Monitoring Server またはモニター・エージェントの短期ヒストリー・ファイルに保管されます。長期保管するために、ヒストリカル・データを Tivoli Data Warehouse データベースに送信するように指定することができます。データ・モデルは、長期ヒストリカル・データと短期ヒストリカル・データで、同じものを使用します。

属性グループの収集定義のコピーを作成し、そのコピーで、収集間隔、ウェアハウス間隔、管理システム配布、または属性のフィルタリングなどの基準について異なる値を構成することができます。ただし、収集ロケーション

(TEMA または TEMS) と、要約およびプルーニングの設定は、属性グループに定義されている各ヒストリカル収集で同一のまま保持されます。

管理対象システム (エージェント) または管理システム (TEMS) への配布

各ヒストリカル・データ収集には配布方法があります。

「**管理対象システム (エージェント)**」はデフォルトの方式であり、配布におけるすべての管理対象システムが Tivoli Enterprise Monitoring Server バージョン 6.2.2 以降に接続する必要があります。この配布は、管理対象システムのサブセットに対して実行されます。このサブセットとは、個別に、または管理対象システム・グループの一部として割り当てられるエージェント・タイプの管理対象システムです。代わりに、その収集が属するヒストリカル構成グループに配布する管理対象システムを割り当てることもできます。

「**管理システム (TEMS)**」は、IBM Tivoli Monitoring Version 6.2.1 以前での配布に使用されていた方式です。これは、管理対象システムが V6.2.1 以前のモニター・サーバーに接続する場合の配布に必要な方式です。この配布は、Tivoli Enterprise Monitoring Server に接続するエージェント・タイプの管理対象システムに対して実行されます。収集の定義で管理システム (TEMS) の方式が選択されている場合、その収集はヒストリカル構成グループのメンバーシップに対して不適格になります。

バージョン 6.2.2 より前のリリースから Tivoli Management Services Version 6.2.2 以降にアップグレードした場合、構成されていた各属性グループのヒストリカル収集定義が表示されます。配布方式は「**管理システム (TEMS)**」 のまま変わりません。配布が管理対象システムごとに実行される場合に使用可能な配布の手法を使用する場合は、収集定義ごとに配布方式を「**管理対象システム (エージェント)**」に変更します。

ヒストリカル構成オブジェクト・グループ

ヒストリカル収集定義の一部は、ヒストリカル・データのサンプルが保存される管理対象システムが指定されている配布リストです。ヒストリカル収集にこの配布を直接追加することも、ヒストリカル構成オブジェクト・グループを使用して間接的に追加することも、またはその両方を組み合わせて追加することもできます。

- **直接の配布**では、個々の管理対象システムまたは管理対象システム・グループ、あるいはその両方をヒストリカル収集に割り当てます。この方法のメリットは、配布がこの収集のみ適用されるので、必要に応じて、管理対象システムを簡単に追加および削除することができることです。
- **間接的な配布**では、管理対象システムまたは管理対象システム・グループ、あるいはその両方をヒストリカル収集が所属するヒストリカル構成グループに割り当てます。この方法のメリットは、1 つの配布リストを設定して、その配布リストを複数のヒストリカル収集に適用できることです。これは、それらの収集をヒストリカル・グループ・メンバーシップに追加することにより実行できます。

同じ配布リストを複数のヒストリカル収集定義に割り当てる方法として、ヒストリカル構成グループを使用します。こうすると、グループの収集を制御でき、ヒストリカル収集定義を個々に選択する必要がなくなります。この機能は、Tivoli Enterprise Portal Server および Tivoli Enterprise Monitoring

Server がバージョン 6.2.2 以降であり、収集の配布方法が **管理対象システム (エージェント)** に設定されている場合に使用できます。

ウェアハウス・スキーマ

データウェアハウスには製品ごとに 1 つ以上のテーブルがあります。テーブルの列名は、そのデータの内容に関連しています。このプラットフォームでは、属性の概念に基づいた単純なデータ・モデルに従っています。属性とは、管理対象オブジェクト (ノード) の特性を指します。例えば、Disk Name は、管理対象オブジェクトであるディスクの属性です。

属性は単一行にすることも、複数行にすることもできます。単一行の属性は、地方時の属性など、1 セットのデータのみを収集します。これは、地方時にはどの時点においても 1 セットの値しかないからです。複数行の属性は、複数セットのデータを収集できます。システムに存在するキューごとに 1 セットのデータを戻す平均キュー属性などです。各属性は属性グループに属し、各属性項目には、その属性グループの特定のプロパティーに対するデータが保管されます。

属性グループごとにテーブルが生成され、それらのテーブル名がヒストリカル・データの収集に使用されます。モニター・エージェントの各ユーザー・ガイドには、該当するエージェントに固有の属性グループに関する完全な説明が記載されています。

ウェアハウス・プロキシー

データ収集構成の分散先である管理対象システムは、データをウェアハウス・プロキシー・エージェント経由で Tivoli Data Warehouse に送信します。ウェアハウス・プロキシーは、マルチスレッドのサーバー・プロセスであり、複数のモニター・エージェントからの同時要求を処理できます。ウェアハウス・プロキシーに到達できない場合、エージェントは指定されたウェアハウス間隔後 (1 時間後や 1 日後など設定によって異なる) での送信を試行します。次の間隔で送信時にウェアハウス・プロキシーがその状況を送り返してこない場合は、トランザクションが再開されます。その後、15 分後にウェアハウス・プロキシーに対してデータが再送されます。ウェアハウス・プロキシーが障害を示す状況を送り返してきた場合には、次のウェアハウス間隔でそのトランザクションが再始動されます。

1 つのモニター対象環境内で複数のウェアハウス・プロキシー・エージェントを置くことができます。大規模な環境に複数のウェアハウス・プロキシー・エージェントをインストールして、ヒストリカル・データをモニター・エージェントから受信し、ウェアハウス・データベースに挿入する作業を分散できます。

ヒストリカル・データをデータウェアハウスに保存しない場合は、ウェアハウス・プロキシーと要約およびプルーニング・エージェントのインストールおよび構成は不要です。データウェアハウスを使用しない場合、短期ヒストリー・ファイルを削除するには、別途プログラムを使用する必要があります。

ウェアハウスの要約およびプルーニング

ウェアハウスの要約およびプルーニング・エージェントでは、データウェアハウスでデータを保存する期間のカスタマイズ (プルーニング) と、データを集約する頻度のカスタマイズ (要約) が可能です。要約したデータを使用

すると、照会のパフォーマンスが大幅に改善されます。また、データ要約とデータ・プルーニングを連携させると、ディスク・スペースの使用量をより適切に管理できます。

ウェアハウスの要約は、テーブル (属性グループ) ごとに制御されます。各テーブル内の行の要約方法は、各テーブル内に*基本キー* として指定されている一連の属性によって決まります。 ORIGINNODE (サーバー名やシステム名と呼ばれることが多い) という 1 つの基本キーが常に存在します。これは、データが管理対象リソース別に要約されるということを意味しています。そのテーブルの要約のレベルをさらに詳細に指定するには、1 つ以上の追加基本キーを指定します。例えば、OS エージェント・ディスク・テーブルでは、基本キーとして*論理ディスク名* を使用し、コンピューター内の各論理ディスクについてのヒストリカル情報が報告されるようにする場合などがあります。

管理対象環境で使用できる要約およびプルーニング・エージェントは 1 つのみです。このエージェントは直接 Tivoli Data Warehouse に接続します。

ヒストリカル・データ収集の構成

構成したヒストリカル・データ収集がデータ・サンプルの保存を開始したら、プロビジョンを作成して、ヒストリカル・データ収集を管理します。この追加アクションを行わないと、ヒストリー・データ・ファイルが際限なく増大し、貴重なディスク・スペースが使い果たされてしまうおそれがあります。

ヒストリカル・データ収集の定義

「ヒストリカル収集の構成」ウィンドウは、Tivoli Enterprise Portal から使用できます。ヒストリカル・データの収集および保管は、Tivoli Enterprise Monitoring Server で指定することも、モニター・エージェントがインストールされているリモート・システムで指定することもできます。ヒストリカル・データ収集を柔軟に使用できるように、以下を行うことができます。

- 同一の属性グループに対する複数の収集の構成。それぞれの収集には異なる配布があり、異なる収集間隔、および異なるウェアハウス間隔を設定できます。
- 収集されたデータ量を、作成したフィルターを満たしたもののみに削減します。例えば、プロセッサーのビジー時間が 80% を超えているデータ・サンプルだけを収集します。
- 配布が「管理システム (TEMS)」に設定されている場合は、特定のモニター・サーバー上のすべての管理対象システムに対してヒストリカル収集を構成し、配布が「管理対象システム (エージェント)」に設定されている場合は、任意の管理対象システムまたは管理対象システムのセットに対してヒストリカル収集を構成。
- ヒストリカル収集ごとに、モニター・サーバーまたはモニター・エージェントで短期ヒストリーを保存する「**収集ロケーション** 」の設定。
- 短期ヒストリー・ファイルにデータ・サンプルを送信する頻度 (各ヒストリカル収集に対して 1 分に 1 回から 1 日に 1 回まで) に関する「**収集間隔** 」の設定。

- Tivoli Data Warehouse にデータを保存する頻度 (各ヒストリカル収集に対して 15 分ごとから 1 日に 1 回まで) に関する「**ウェアハウス間隔**」の設定。
- データウェアハウスに保管されたデータを要約およびプルーニングする方法および時期の決定。要約とプルーニングは、1 つ以上のヒストリカル収集が定義されている属性グループごとに構成されます。
- 管理対象システム (またはそれが属する管理対象システム・グループ) を、ヒストリカル収集の配布リストに追加するか、またはその収集が属するヒストリカル構成グループに追加することによる、管理対象システムでの収集の開始。
- 管理対象システム (またはそれが属する管理対象システム・グループ) をヒストリカル収集の配布リストから削除するか、またはその収集が属するヒストリカル構成グループから削除することによる、管理対象システムでの収集の停止。
- 配布リストとともにヒストリカル構成グループを作成し、配布を使用するグループに収集を割り当てます。

コマンド行からのヒストリカル・データ収集の定義

また、ヒストリカル・データ収集は、以下のコマンド行インターフェースの **tacmd hist** コマンドを使用して構成することもできます。

histconfiguregroups

histcreatecollection

histdeletecollection

histeditcollection

histlistattributegroups

histlistcollections

histlistproduct

histstartcollection

histstopcollection

histunconfiguregroups

histviewattributegroup

histviewcollection

bulkExportSit (ヒストリカル・データ収集のエクスポート)

bulkImportSit (ヒストリカル・データ収集のインポート)

テスト環境がある場合は、ヒストリカル・データ収集を構成するための tacmds を使用するスクリプトを作成して、別のテスト・コンピューターまたは実動システムでスクリプトを実行することができるので、システムごとに同じ構成を繰り返す必要がありません。これらのコマンドについて詳しくは、*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)を参照してください。

冗長なデータ収集の防止

1 つの管理対象システムの同じ属性グループで 2 回以上データを収集する可能性があります。これは、同一の属性グループに対して複数のヒストリカ

ル収集を構成し、それを同一の管理対象システムに配布した場合に発生します。これにより、データ・トラフィックが増加し、不必要にストレージ・スペースが使用されるだけでなく、要約の値が偏ります。この偏りは、同一の属性グループに対する複数の収集によって送信される追加の値が要約の計算に使用されることが原因で発生します。

特定のヒストリカル収集に対して、同一の管理対象システムがヒストリカル収集の配布に、誤って複数回割り当てられる心配はありません。ヒストリカル機能は、収集が配布される管理対象システムを認識して、各管理対象システムに対して 1 回のみデータ・サンプルを収集します。管理対象システムは、以下の場合にヒストリカル・データ収集の配布に組み込まれます。

- コレクション定義で直接参照される場合
- コレクション定義で参照される管理対象システム・グループに含まれている場合
- そのヒストリカル収集が属しているヒストリカル構成グループの配布に含まれている場合
- そのヒストリカル収集が属しているヒストリカル構成グループの配布に含まれる管理対象システム・グループ内にある場合

細分性の高いデータ収集のフィルター式の作成

ヒストリカル収集の構成エディターの「**フィルター**」タブには、収集するデータを指定するフィルター基準を作成するための式エディターがあります。データ・サンプルのヒストリカル収集は、データ行の値がフィルター基準を満たす場合のみ発生します。例えば、ディスク書き込み時間 (%) の属性値が 50% を超えるとデータ・サンプルは短期ヒストリーに保存されます。それ以外の場合、このサンプルは保存されません。

フィルター基準は、収集定義ごとに構成可能です。ヒストリカル・データ収集にフィルターを適用すると、ネットワーク・トラフィックやディスク・スペースの無駄を軽減し、要約とプルーニングのパフォーマンスを改善することができます。

データ収集をフィルタリングすると、グラフのベースライン処理とシチュエーションのモデル化によって実行されるトレンド計算の結果、およびヒストリカル・データを含む照会ベース・ビューの結果に影響する可能性があることを認識しておいてください。例えば、プロセスが 80% 以上の CPU を使用する行のみを収集するフィルターを適用することは、平均値の計算が、すべての値ではなく 80% 以上の値のみで行われることを意味します。

短期ヒストリー・ファイルのトリミング

ウェアハウス・プロキシーを使用して Tivoli Data Warehouse にデータをアップロードすることを選択した場合、モニター・サーバーまたはモニター・エージェント上の短期ヒストリー・ファイルはアップロード後に自動的にトリミングされます。

管理システム (TEMS) 収集タイプ

ヒストリカル・データ収集は、個々のモニター・サーバー、製品、および属性グループに対して指定できます。ただし、同じモニター・サーバーに直接レポートする同一タイプのすべてのエージェントには、同一のヒストリー収集オプションが設定されている必要があります。また、指定の属性グループ

では、その収集が現在使用可能になっているすべてのモニター・サーバーに対して、同一のヒストリー収集オプションが適用されます。

収集ロケーション

「**収集ロケーション**」は、短期ヒストリカル・データ・ファイルが配置されている場所です。TEMA (Tivoli Enterprise Monitoring Agent) または TEMS (Tivoli Enterprise Monitoring Server) のいずれかです。デフォルトのロケーションは TEMA であり、ヒストリカル・データ管理によるモニター・サーバー上のパフォーマンスの影響を最小限にします。ただし、製品と属性グループの組み合わせによっては、特定の場所 (モニター・サーバーまたはモニター・エージェントのいずれか) でのみ収集される場合もあります。

z/OS OMEGAMON XE 製品の場合、短期ヒストリーの格納に永続データ・ストアが使用されるため、永続データ・ストアは収集ロケーションで構成する必要があります。どのエージェントであれ、収集ロケーションを変更しないでください。製品のヒストリカル・データはすべて、モニター・エージェントかモニター・サーバーのいずれかで収集してください。モニター・サーバーと同じアドレス・スペースに構成されたエージェントの場合 (OMEGAMON XE for z/OS および OMEGAMON XE for Storage on z/OS の場合は必須)、同じアドレス・スペースで永続データ・ストアを構成し、収集ロケーションとして TEMS を指定してください。

ウェアハウス・データの集約およびプルーニング

要約およびプルーニング・エージェントは、Tivoli Data Warehouse 内のデータを管理する仕組みです。ウェアハウス内のデータは、ユーザーのエンタープライズにおけるアクティビティーおよび状態のヒストリカル・レコードです。 データの要約とは、ヒストリカル・データを時間ベースのカテゴリー (時間単位、日単位、週単位など) に集約する処理です。データを要約すると、時間に沿ったデータのヒストリカル分析を行うことができます。データをプルーニングすることで、データベースを管理可能なサイズに保持し、パフォーマンスを向上できます。 データベースのプルーニングは定期的に実行する必要があります。

重要: 単一の Tivoli Data Warehouse データベースを共有する複数のモニター・サーバーがある場合においても、実行できる要約およびプルーニング・エージェントは 1 つのみです。複数の要約およびプルーニング・エージェントを実行すると、データベースのデッドロックおよび競合が発生します。これは、複数のインスタンスが表内のデータの要約またはプルーニングを同時に試行する場合があることが原因です。

区切り文字で区切られたフラット・ファイルへの短期ヒストリー・ファイルの変換

Tivoli Data Warehouse を使用しない場合は、ヒストリー・データ・ファイルを定期的に変換して空にするロールオフ・ジョブを設定する必要があります。ロールオフ・プログラムが提供されます。これらのスクリプトは、ヒストリー・データ・ファイルの削除だけでなく、フラット・ファイルの生成も行います。サード・パーティーのツールでこのファイルを使用すると、トレンド分析のレポートとグラフィックスを生成できます。また、ヒストリー・ファイルの最大サイズを設定するための環境変数もあります。

553 ページの『短期ヒストリー・ファイルの拡大の制限』を参照してください。

一部の属性グループがヒストリカル・データ収集に不適切

エージェントによっては、そのすべての属性グループに対してヒストリー・データの収集を使用可能にしていない場合があります。使用可能にしない理由は、そのエージェントの製品開発チームが、特定の属性グループに対するヒストリー・データの収集が不適切であると判断したか、またはパフォーマンスに悪影響を及ぼす可能性があると判断したためです。生成されるデータが膨大になることも理由として考えらます。そのため、  「モニター中のアプリケーション」をクリックすると、「ヒストリーの収集の構成」ウィンドウには、ヒストリー収集が使用可能な属性グループのみが製品ごとに表示されます。

短期ヒストリー・ファイルのディレクトリーの変更

ヒストリカル・データがエージェント (TEMS ではなく、TEMA) で収集されるように構成されている場合は、エージェントの環境変数 CTIRA_HIST_DIR を使用してヒストリカル・データが収集されるディレクトリーを変更します。例えば、デフォルトのヒストリー・データ・ファイルのロケーションが提供する記憶容量よりも大容量のディスクにヒストリー・ファイルを格納する場合などに変更します。

始める前に

ディレクトリーは既存のディレクトリーであり、絶対パスを指定する必要があります。また、オペレーティング・システムのユーザー ID にこのディレクトリーに対する書き込み許可が必要です。ディレクトリーが存在しない場合、エージェントはヒストリカル・データを収集しません。

このタスクについて

以下のステップを実行してエージェントの環境変数 CTIRA_HIST_DIR を編集し、短期ヒストリー・ファイルを格納する別のディレクトリーを設定します。

手順

- Windows
  1. 「Tivoli Enterprise Monitoring Services の管理」ウィンドウでモニター対象のアプリケーションを右クリックし、「**拡張**」→「**変数の編集**」をクリックします。
  2. 「ローカル変数設定のオーバーライド」ウィンドウで「**追加**」をクリックします。
  3. 変数  リストをスクロールして、「**CTIRA_HIST_DIR**」を選択します。
  4. 「値」フィールドで、`@LogPath@` を短期ヒストリーを保存するディレクトリーの絶対パスに置き換えます。
  5. 「**OK**」をクリックして、「**変数**」列の CTIRA_HIST_DIR、および「**値**」列の新規のパスを確認し、「**OK**」を再度クリックしてウィンドウを閉じます。 この値は、KNTENV などの K*pc*ENV ファイルに記録されます。
  6. エージェントを再開して、変更内容を有効にします。
- Linux UNIX
  1. `<itm_install_dir>/config` ディレクトリーに移動して、テキスト・エディターで `pc.ini` を開きます (ここで、*pc* は 2 文字の製品コードです)。 例え

ば、UNIX OS エージェントでは、/opt/IBM/ITM/config/ux.ini です。製品コードのリストについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『IBM Tivoli 製品、プラットフォーム、およびコンポーネント・コード』を参照してください。

2. 新規の行に、この環境変数に続けて短期ヒストリーを保存するロケーションへの絶対パスを以下のように追加します。

   ```
   CTIRA_HIST_DIR=
   ```

3. ファイルを保存して閉じます。
4. エージェントを再開して、変更内容を有効にします。

ヒストリカル・データ要求によるパフォーマンスへの影響

Tivoli Management Services コンポーネントでのヒストリカル・データ収集およびウェアハウジングがパフォーマンスにどの程度影響を及ぼすかは、収集間隔、データウェアハウスへのロールオフの頻度、収集するヒストリカル・テーブルの数とサイズ、システム・サイズなど、複数の要因によって決まります。

モニター・サーバーまたはモニター・エージェントにある大量のヒストリカル・データによる影響

短期ヒストリカル・データのデフォルトの保管場所はモニター・エージェントですが、ある種の構成ではモニター・サーバーの方が望ましいこともあります。

このトピックでは、次の事柄を決定する際に考慮すべき要因を示します。

- ヒストリカル・データを収集する属性グループ
- 短期データ・ファイルの保存場所
- ヒストリカル・データ・サンプルを短期収集ロケーションに送信する頻度
- 属性グループからのデータをウェアハウスに保管するかどうか、および保管する場合は、短期ヒストリー・ファイルからのデータをデータウェアハウスに送信する頻度

大量のデータが処理されると、収集ロケーションに悪影響を及ぼす可能性があります。これは、モニター・サーバーまたはモニター・エージェントでのウェアハウジング処理で短期ヒストリー・ファイルから大量の行セットを読み取る必要があるためです。その後、データは ウェアハウス・プロキシー によってデータウェアハウスに送信される必要があります。データ・セットが大きいと、これはメモリー、CPU リソースに影響し、また特に収集場所がモニター・サーバーである場合に、ディスク・スペースに影響します。

多数の要求を同時に処理できるため、モニター・サーバーへの影響はモニター・エージェントへの影響ほど大きくはありません。ただし、ヒストリカル収集ロケーションがモニター・サーバーである場合は、1 つの属性グループのヒストリー・データ・ファイルに多数のエージェント (モニター・サーバーにデータを保管するすべてのエージェント) のデータを含めることができるため、データ・セットが大きくなることに注意が必要です。同様に、大規模データ・セットに対する要求も、Tivoli Enterprise Portal Server にあるメモリーおよびリソースに影響を及ぼします。

ヒストリカル・データがエージェントに保管される場合、1 つの属性グループのヒストリー・ファイルには、そのエージェントのデータのみが格納され、モニター・

サーバーに保管されるヒストリー・ファイルよりはるかにサイズが小さくなります。直前の 24 時間内のデータは、短期ヒストリー・ファイルから取得されます。24 時間より前のデータは Tivoli Data Warehouse から取得されます。(KFW_REPORT_TERM_BREAK_POINT ポータル・サーバー環境変数を使用して、ブレークポイントを変更できます)。このアクションはユーザーには透過的ですが、大容量のデータを戻す要求は モニター・サーバー、モニター・エージェント、およびネットワークのパフォーマンスに悪影響を与える可能性があります。

照会が短期ヒストリー・ファイルに到達し、大容量のデータが取得される場合、この取得によって、CPU およびメモリーが大量に消費される可能性があり、データの取得中にシステム・パフォーマンスが低下することがあります。大量のデータ要求を処理している場合は、この処理が完了するまで他の要求をエージェントが処理できない場合があります。このことは多くのモニター・エージェントにとって重要です。エージェントが 1 度に処理できるビュー照会またはシチュエーションは、通常 1 つのみであるためです。

ヒストリカル収集、ビュー照会、またはその両方に適用できるベスト・プラクティスとして、データの収集やレポートの*前に* フィルターを使用してデータを制限することがあります。ヒストリカル収集の場合、事前フィルタリングは、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」の*IBM Tivoli Monitoring コマンド・リファレンス* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/cmdref/itm_cmdref.htm)およびヒストリカル収集の作成で説明しているように、ヒストリカル収集の構成エディターの「**フィルター**」タブ、または CLI **tacmd histcreatecollection** コマンドのフィルター・オプションで実行されます。ワークスペース・ビューの場合、事前フィルタリングは、「*Tivoli Enterprise Portal ユーザーズ・ガイド*」のモニター・サーバーに対する別の照会の作成で説明しているように、照会エディターで事前定義照会から別の照会を作成し、その仕様にフィルターを追加することによって実行されます。

大規模なテーブルからのヒストリカル・データの要求

大量のデータを収集するテーブルからヒストリカル・データを要求すると、関連する Tivoli Management Services コンポーネントのパフォーマンスが低下します。ご使用のシステムのパフォーマンスへの影響を軽減するには、大量のデータを収集するテーブルについては、収集間隔を長く設定するか、フィルターを作成するかのいずれか、またはその両方を実行します。

収集間隔とフィルター基準は、「ヒストリーの収集の構成」ウィンドウで指定します。 IBM Tivoli Monitoring 製品でのテーブルのディスク・スペース所要量を調べるには、各エージェントの資料を参照してください。

照会ベース・ビューを表示している場合、以前にサンプリングしたデータを取り出す時間スパン間隔を設定できます。レポート時間スパンに長い時間のスパン間隔を選択すると、処理するデータの量が増加し、パフォーマンスが低下する可能性があります。大量のレポート・データを処理するには、プログラムは、より多くのメモリーおよび CPU サイクルを占有する必要があります。この場合、特に大量のデータを収集するテーブルには短い時間スパン設定を指定してください。

レポート行セットが大きすぎると、エージェントが要求の処理に費やす時間が長くなりすぎるため、レポート要求がタスクを除去し、行を取得せずに Tivoli Enterprise

Portal に戻ってしまう場合があります。ただし、レポート・データが表示できない場合でも、エージェントは引き続きレポート・データを最後まで処理し、ブロックされたままになります。

また、z/OS 永続データ・ストアからのヒストリカル・レポート・データを使用できない場合もあります。原因として、メンテナンス・ジョブの実行中に永続データ・ストアが使用できない場合があることが考えられます。

ヒストリカル・データのウェアハウジングのスケジューリング

ヒストリカル・レポートに大量の行セットを要求する場合の問題は、ヒストリカル・データのウェアハウジングを 1 日に 1 回しかスケジュールしない場合にも当てはまります。収集および保管するデータが多くなるほど、データをメモリーに読み取ってデータウェアハウスに送信するために必要となるリソースも多くなります。可能な場合は、ウェアハウジングの負荷を各設定時間ごとに分散させる (つまり、ウェアハウスの間隔を 1 日ではなく 1 時間に 1 回に設定する) ことにより、ウェアハウジングの対象とする行セットを小さくしてください。

データマートを使用した長い照会または複雑な照会の改善

このセクションでは、データマートを使用してプライマリー・データ・ストアのパフォーマンスを向上させる方法を説明します。

Tivoli Management Services インフラストラクチャーでは、ウェアハウス・プロキシーは定期的に短期ヒストリー・ファイルからの新規データをデータウェアハウス・テーブルに挿入します。この詳細データは、この情報をレポートする照会によって、ヒストリカル・ビューから取得されます。また、照会によって外部レポート・ツールからも取得できます。アクティブ・データ・ストアはすべて、データ・ストアのパフォーマンスを最大にするために、読み取り/書き込みアクティビティーのバランスを取る必要があります。データウェアハウスには、レポートをフォーマットおよび作成するために頻繁に行われる読み取りアクティビティーと、それとバランスを取る形で行われる定期的な書き込みアクティビティーがあります。特定の状況 (特に長時間にわたりレポートをフォーマットしたり、複雑な照会を実行したりする場合) では、データベースの読み取りおよび書き込みアクティビティーがバランスよく行われなくなり、結果として異常な待ち時間が生じる場合があります。このような状況では、レポート用の第 2 のデータ・ストア (一般的にデータマート と呼ばれます) を追加することにより、時間がかかるデータ照会や複雑なデータ照会を元のデータ・ストアで処理する必要がなくなり、パフォーマンスを大幅に改善できます。

レポート要件に応じて、ウェアハウスとともに提供されるオープン・インターフェースを利用する次の 2 つの手段を取ることができます。

1. 完全なデータベースが必要な場合、Tivoli Data Warehouse RDBMS のデータベース複製機能を使用します。
2. Tivoli Data Warehouse V1.x の ETL スクリプトに類似した SQL 抽出スクリプトを記述およびスケジュールし、スケジュールした間隔で、Tivoli Data Warehouse から所要のデータ要素を抽出し、レポート・データベースに取り込みます。このレポート・データベースは、Tivoli Data Warehouse V1.x で使用され

たデータマートと同じく、外部レポート・ツールによる使用のために最適化できます。使用可能なスクリプトは、SQL スクリプト、シェル・スクリプト、および PERL スクリプトです。

IBM Tivoli Monitoring 用のデータマート SQL スクリプトのサンプル

以下の SQL スクリプトは、データマートの作成方法および取り込み方法を示すサンプル・スクリプトです。実際のスクリプトでは、ご使用の環境に応じた修正が必要です。

```
-----------------------------------------------------
-- Example data mart SQL Script for TDW 2.1
-----------------------------------------------------
-- This scripts demonstrates the creation and population
-- of a data mart (similar to the data marts in TDW 1.x)
-- starting from the "flat" tables in TDW 2.1.
-- This script can be run using the DB2 UDB CLP:
-- db2 -tvf myscript
-----------------------------------------------------
-- 1. Create hourly "flat" table from TDW 2.1 (simulated)
-- One row per hour per Windows system
drop table itmuser."Win_System_H";
create table itmuser."Win_System_H" (
 WRITETIME                      CHAR( 16 ),
 "Server_Name"                  CHAR( 64 ),
 "Operating_System_Type"        CHAR( 16 ),
 "Network_Address"              CHAR( 16 ),
 "MIN_%_Total_Privileged_Time"  INTEGER,
 "MAX_%_Total_Privileged_Time"  INTEGER,
 "AVG_%_Total_Privileged_Time"  INTEGER,
 "MIN_%_Total_Processor_Time"   INTEGER,
 "MAX_%_Total_User_Time"        INTEGER,
 "AVG_%_Total_User_Time"        INTEGER );

-- 2. Insert example data

insert into itmuser."Win_System_H" values (
'1050917030000000', 'Primary:WinServ1:NT', 'Windows_2000', '8.53.24.170',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917040000000','Primary:WinServ1:NT','Windows_2000','8.53.24.170',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917030000000','Primary:WinServ2:NT','Windows_2000','8.53.24.171',
20, 40, 30, 10, 30, 20 );

insert into itmuser."Win_System_H" values (
'1050917040000000','Primary:WinServ2:NT','Windows_2000','8.53.24.171',
  20, 40, 30, 10, 30, 20 );

-- 3. Create a dimension table for the hosts
-- primary key is Server_ID, a generated value
-- alternate key is Server_Name, Network_Address

drop table itmuser."D_Win_System";
create table itmuser."D_Win_System" (
 "Server_ID" INTEGER GENERATED ALWAYS AS IDENTITY
    PRIMARY KEY NOT NULL,
 "Server_Name"                  CHAR( 64 ),
 "Operating_System_Type"        CHAR( 16 ),
 "Network_Address"              CHAR( 16 ) );
```

```
-- 4. Create an hourly fact table for the System facts
-- Server_ID is a foreign key to D_Win_System

drop table itmuser."F_Win_System_H";
create table itmuser."F_Win_System_H" (
 WRITETIME                      CHAR( 16 ) NOT NULL,
 "Server_ID"                    INTEGER NOT NULL,
 "MIN_%_Total_Privileged_Time"  INTEGER,
 "MAX_%_Total_Privileged_Time"  INTEGER,
 "AVG_%_Total_Privileged_Time"  INTEGER,
 "MIN_%_Total_Processor_Time"   INTEGER,
 "MAX_%_Total_User_Time"        INTEGER,
 "AVG_%_Total_User_Time"        INTEGER,
 constraint SERVID foreign key ("Server_ID")
  references itmuser."D_Win_System" ("Server_ID")
);

-- 5. Insert into the dimension table
-- only insert rows that do not already exist

insert into itmuser."D_Win_System" (
 "Server_Name",
 "Operating_System_Type",
 "Network_Address" )
select
 "Server_Name",
 min("Operating_System_Type") as "Operating_System_Type",
 "Network_Address"
from
  itmuser."Win_System_H" h
where
 not exists ( select 1 from
 itmuser."D_Win_System" d
 where d."Server_Name" = h."Server_Name"
 and d."Network_Address" = h."Network_Address"
 )
group by
 "Server_Name",
 "Network_Address"
;

-- 6. Check values in dimension table
select * from itmuser."D_Win_System"
;

-- 7. Insert into the fact table
-- only insert rows that do not already exist
insert into itmuser."F_Win_System_H"
select
 h.WRITETIME   ,
 d."Server_ID" ,
 h."MIN_%_Total_Privileged_Time" ,
 h."MAX_%_Total_Privileged_Time" ,
 h."AVG_%_Total_Privileged_Time" ,
 h."MIN_%_Total_Processor_Time"  ,
 h."MAX_%_Total_User_Time"       ,
 h."AVG_%_Total_User_Time"
from
 itmuser."Win_System_H" h,
 itmuser."D_Win_System" d
where d."Server_Name" = h."Server_Name"
 and d."Network_Address" = h."Network_Address"
 and not exists ( select 1 from
 itmuser."F_Win_System_H" f
  where f.WRITETIME = h.WRITETIME
  and f."Server_ID" = d."Server_ID"
  )
```

```
;

-- 8. Check values in fact table
select * from itmuser."F_Win_System_H"
;

-- 9. Repeat"5. Insert into the dimension table"
-- and "7. Insert into the fact table" on a daily basis
```

リファレンスおよび追加のサンプル SQL 抽出スクリプトが必要な場合は、IBM Redbooks® 発行の『*Introduction to Tivoli Enterprise Data Warehouse (http://www.redbooks.ibm.com/)*』を参照してください。

Tivoli Data Warehouse および短期ヒストリー構成

このセクションでは、Tivoli Data Warehouse データベースに関連するいくつかの短期ヒストリーの構成について説明します。

Tivoli Data Warehouse のヒストリー・テーブルと列の命名

Tivoli Data Warehouse データベースのヒストリー・テーブルの名前は、ヒストリー・テーブルおよび列のグループ名と同じです。例えば、グループ名 NT_System の Windows NT ヒストリーは、WTSYSTEM という名前の短期ファイルに収集されます。このファイル (WTSYSTEM) のヒストリカル・データは、NT_System という名前のテーブルでデータベースに格納されます。

ウェアハウス・プロキシーでは、完全な製品属性名を使用して DBMS テーブルおよび列の ID を作成します。これには、属性名にある特殊文字もすべて含まれます。属性名の長さが DBMS 製品によってサポートされるテーブル名または列名の最大長を超える場合、ウェアハウス・プロキシーは製品属性ファイルで定義された内部テーブル名および列名を使用します。

WAREHOUSEID テーブルは、Tivoli Data Warehouse データベース内に格納されています。このテーブルに含まれるレコードでは、DBMS の名前の最大長を超え、内部のテーブル名または列名へ変換済みであるすべての属性名またはテーブル名を記述しています。このテーブルを照会すると、内部的に変換されたテーブルまたは列の正しい名前が分かります。このテーブルの各属性グループ名には、「TAB」という RECTYPE 値があります。TABLENAME 値および OBJECTNAME 値のみが、埋め込まれています。各属性列名には、「COL」という RECTYPE 値があります。WAREHOUSEID の他のすべての列の値は、埋め込まれています。WAREHOUSE ID テーブルには以下の定義があります。

RECTYPE CHAR(3)
レコードのタイプを示します。テーブルの場合は「TAB」、列の場合は「COL」です。

TABLENAME CHAR(20)
内部テーブル名を示します。

OBJECTNAME CHAR(140)
属性グループ名を示します。

COLUMNNAME CHAR(20)
内部列名を示します。

ATTRNAME CHAR(140)
属性名を示します。

ウェアハウス・プロキシーは、ウェアハウス・データベースのデータ・テーブルごとに関連付けられた索引を自動的に作成します。この索引は、WRITETIME および ORIGINNODE (表示名は、テーブルに応じて「Server_Name」、「System_Name」など) と、TMZDIFF (タイム・ゾーンの差) の列を基にして作成されます。索引名は、テーブルの短縮名にサフィックス「_IDX」を付けた名前になります。

全データへの正しいアクセスを確保するための二重引用符の使用

すべての主要な DBMS 製品のすべてのデータウェアハウス・テーブル名または列名は、DBMS でサポートされる引用符付き ID 文字で囲んで作成されます。ウェアハウス・データベースのヒストリカル・データを参照する場合は、そのデータに正しくアクセスできるように二重引用符文字を使用する必要があります。Microsoft SQL Server などの一部のデータベース製品では二重引用符は不要です。

旧バージョンのヒストリカル・データ収集プログラムで使用する目的で IBM Tivoli Monitoring V6.2.1 より前の SQL 照会またはストアード・プロシージャーを作成した場合は、それらの変更が必要になる場合があります。一部のリレーショナル・データベース製品 (Oracle など) では、 IBM ヒストリー・データにアクセスするために、すべてのテーブル名および列名を二重引用符で囲む必要があること、なんらかのエージェントがデータ属性を変更したり、新規列を追加した可能性があることを、SQL では考慮に入れる必要があります。

ウェアハウス・プロキシーの ATTRLIB ディレクトリー

ウェアハウス・プロキシーの ATTRLIB ディレクトリーは、製品のインストール時に自動的に作成されます。 Windows システムの場合、このディレクトリーは *ITM_dir*¥tmaitm6¥attrlib にあります。 UNIX 系オペレーティング・システムの場合、このディレクトリーは *ITM_dir*/hd/tables にあります。

インストール時に、他のエージェントがインストールされている同じコンピューターにウェアハウス・プロキシーがインストールされると、インストール・プログラムでアクセス可能なエージェント製品の属性ファイルが ATTRLIB ディレクトリーに追加されます。ウェアハウス・プロキシーが属性ファイルを使用するのは、モニター・エージェントが 6.1.0 よりも前のバージョンである場合のみです。

属性名の長さが、ウェアハウス DBMS 製品でサポートされるテーブル名または列名の最大長を超えている場合には、属性ファイルを使用することで、テーブルまたは列の内部名を判別できます。先に説明した条件が成立してさえいれば、この属性ファイルは必ず ATTRLIB ディレクトリーにあるはずです。ウェアハウス・プロキシーを別のコンピューターにインストールし、最新レベルではないモニター・エージェントを使用している場合は、ウェアハウス・プロキシーがインストールされている ATTRLIB ディレクトリーにそのエージェントの属性ファイルをコピーする必要があります。

特定の製品属性ファイルがこのディレクトリーから欠落していたことが原因でエクスポートに失敗したことを示すエラー・メッセージが出された場合は、欠落している製品属性ファイルを見つけて、その属性ファイルを ATTRLIB ディレクトリーにコピーしてください。

一連の収集済み属性の変更

属性が追加された新しいバージョンのエージェントがデプロイされた場合など、一連の収集済み属性が変更されたことが検出されると、ヒストリカル・プログラムは以下の機能を実行します。

- 現在のヒストリカル・データ収集要求でウェアハウジングが指定されている場合は、そのテーブルのすべての収集済みヒストリカル・データがデータウェアハウスにエクスポートされます。ウェアハウジング操作が正常に完了すると、短期ヒストリー・データおよびメタファイルをすべて削除します。

  操作に失敗した場合 (例: ウェアハウス・プロキシーが使用不可である場合)、短期ヒストリカル・データおよびメタファイルは名前変更されます。z/OS オペレーティング・システム環境では、データの格納に汎用テーブルを使用する場合、ウェアハウジング操作が成功したかどうかにかかわらずテーブルの短期ヒストリカル・データを削除します。

  – Windows および UNIX オペレーティング・システム環境

    これらのオペレーティング・システム環境では、ヒストリー・データおよびメタファイルは名前変更され、それぞれサフィックス **.prv** および **.prvhdr** が付けられます。

  – IBM i オペレーティング・システム環境

    このオペレーティング・システム環境では、ヒストリー・データおよびメタファイルは名前変更され、それぞれサフィックス **P** および **Q** が付けられます。

    名前変更されたファイルがすでに存在する場合は、名前変更操作の前にそれらのファイルが削除されます (つまり、変更された短期ヒストリー・ファイルは 1 つの生成だけ保持されます)。

- 現在のヒストリカル・データ収集要求でウェアハウジングが指定されていない場合は、上述のように、ヒストリー・データおよびメタファイルが名前変更されます。z/OS では、データの格納に汎用テーブルを使用する場合、テーブルのすべての短期ヒストリー・データが、そのメタ・レコードとともに削除されます。

Tivoli Data Warehouse 範囲区画のマイグレーション

範囲区画化とは、大規模な Tivoli Data Warehouse データベースでプルーニングと照会のパフォーマンスを大幅に向上できるデータベース・データ編成機能です。既存の表を区画化表にマイグレーションすることで、区画化表の向上したパフォーマンスを活用することができます。

区画化表を使用するには、Summarization and Pruning agentとWarehouse Proxy agentがいずれも区画化が使用可能な状態で構成されている必要があり、Tivoli Data Warehouse で区画化が可能になっていなければなりません。

マイグレーションと必要なクリーンアップは、マイグレーション・モードのスキーマ・パブリケーション・ツールによって生成されたスクリプトを使用して処理されます。スクリプトの機能を以下に示します。

tdw_migrate_setup.sql
このスクリプトは、ソース表を新しい区画化表に再定義するためのストアー

ド・プロシージャーを作成し、マイグレーションに必要な制御表 (WAREHOUSE_MIGRATION_STATUS 表など) を作成します。

tdw_migrate_step1.sql
このスクリプトは、セットアップ・スクリプトで作成されたストアード・プロシージャーを呼び出します。このストアード・プロシージャーは、ソース表の名前を MIGRATING_<*short table name*> に変更し、新規の区画化表を作成し、ソース表のデータを新規表にロードし、その後にソース表の名前を DONE_<*short table name*> に変更します。

tdw_migrate_step2.sql
このスクリプトは、新規の区画化表に索引を再作成し、ソース表を削除し、表で PUBLIC に対して SELECT を認可します。

また、Tivoli Data Warehouse 区画化スキーマとは異なる区画化スキーマを使用して区画化された表をマイグレーションすることもできます。 Tivoli Data Warehouse スキーマを使用して区画化された表のみを、Summarization and Pruning agentによって管理できます。ユーザー定義の区画化スキームを引き続き使用する場合は、KSY_TABLE_FILTER 変数を使用して、マイグレーションする表のみをリストします。

マイグレーションされた表の区画は、表の保持期間と「将来の区画数」パラメーターに基づいて定義されます。*「将来の区画数」パラメーター* は、要約およびプルーニング 構成ファイルで変数 KSY_PARTITIONS_UPWARD を使用して定義されている構成パラメーターです。*保存期間* は、Tivoli Enterprise Portal の「ヒストリー構成」ダイアログまたはコマンド行を使用して選択された属性グループに対して定義されているプルーニング・パラメーターです。

範囲の区画化について詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Data Warehouse の範囲区画化』を参照してください。

状況表 WAREHOUSELOG および WAREHOUSEAGGREGLOG もマイグレーションできます。これらの表をフィルタリングするには、KSY_TABLE_FILTER 変数でこれらを指定するか、KSY_PRODUCT_FILTER 変数で、WAREHOUSELOG の場合は製品コード KHD、WAREHOUSEAGGREGLOG の場合は製品コード KSY を指定します。KSY_SUMMARIZATION_FILTER が使用されている場合、これらの表は詳細表として扱われます。

前提条件とベスト・プラクティス

開始前に、以下の条件を満たしていることを確認します。

- 十分なディスク・スペースがあることを確認します。これは、マイグレーション中、ソース表が削除されるまでは、同一データのコピーが 2 つ存在しているためです。マイグレーションする表が占有するディスク・スペースの 2 倍以上のスペースが必要です。
- マイグレーション*前* に、マイグレーションするすべての表でプルーニングを定義します。これにより、表が区画化された後にデータが適切にプルーニングされます。
- マイグレーション期間中は、Summarization and Pruning agentおよびWarehouse Proxy agentを停止します。また、マイグレーションする表のレポートまたは外部ユーザーもすべて停止します。

- ご使用の Tivoli Enterprise Portal Server のアプリケーション・サポートが更新されていることを確認します。ポータル・サーバーとエージェントのアプリケーション・サポートは一致していなければなりません。

ベスト・プラクティスは、表をバッチでマイグレーションすることです。このようにすることで、マイグレーションに必要なディスク・スペースの容量と、Summarization and Pruning agent および Warehouse Proxy agent をオフラインにする必要がある時間が削減されます。表の一括マイグレーションは保守の時間帯に実行できます。

非区画化表から区画化表へのマイグレーション (DB2 for Linux, UNIX, and Windows)

DB2 for Linux, UNIX, and Windows を使用している場合は、以下のステップに従って非区画化表をマイグレーションします。

始める前に

525 ページの『前提条件とベスト・プラクティス』を確認してください。十分なディスク・スペースがあることを確認してください。

Tivoli Data Warehouse ユーザーには以下の権限が付与されている必要があります。

- CREATE TABLE
- LOAD
  DB2 マイグレーションでは、ロード・ユーティリティーを使用してデータをコピーします。ロード権限を付与するには、SYSADM 権限または DBA 権限を持つユーザーとして DB2 にログインし、`db2 grant load on database to <Tivoli Data Warehouse user ID>` SQL コマンドを実行します。
- ADMIN_CMD プロシージャーの実行特権
  権限を付与するには、SYSADM 権限または DBA 権限を持つユーザーとして DB2 にログインし、`db2 grant execute on procedure sysproc.admin_cmd to user <Tivoli Data Warehouse user ID>` SQL コマンドを実行します。

マイグレーションに必要な特権は、実行する必要があるすべてのマイグレーションの完了後に取り消すことができます。

このタスクについて

Tivoli Data Warehouse DB2 for Linux, UNIX, and Windows データベースでの非区画化表から区画化表へのマイグレーションでは、スキーマ・パブリケーション・ツールによって生成されたストアード・プロシージャーが使用されます。ストアード・プロシージャー自体は DB2 LOAD ユーティリティーを使用します。

手順

1. 区画化表に対して Summarization and Pruning agent を構成します。詳しいステップについては、*IBM Tivoli Monitoring インストールおよび設定ガイド*の『Specifying range partitioned tables for the Summarization and Pruning Agent』を参照してください。
2. すべてのWarehouse Proxy agentおよびSummarization and Pruning agentのインスタンスを停止します。

3. Tivoli Data Warehouse データベースをバックアップします。
4. スキーマ・パブリケーション・ツールの応答ファイルを編集します。
   a. 応答ファイルを開きます。

      Windows *install_dir* ¥TMAITM6¥tdwschema.rsp

      Linux UNIX *install_dir* /*arch*/bin/tdwschema.rsp

   b. 以下の変数を構成します。

      KSY_PRODUCT_SELECT = migrate

      KSY_PRODUCT_FILTER = *マイグレーションする製品のリスト*
      ある特定の製品のみが含まれることを示すためのオプション・フィルター。(フィルターを指定しないと、指定されたカテゴリー内のすべての製品がデフォルトで含まれます。) 含める製品の 3 文字の製品コードをコンマで区切って指定します。これらのコードを見つけるには、**tacmd histListProduct** コマンドを使用します (詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください)。

      KSY_TABLE_FILTER = *マイグレーションする表のリスト*
      特定の表のみを示すオプション・フィルター。このフィルターは、KSY_PRODUCT_FILTER 変数に追加して使用できます。特定の製品で使用できる表のリストを取得するには、次のコマンドを使用します。属性グループ名の各スペースは下線文字に置き換えます。表名のリストを取得するには、次のコマンドを使用します。
      tacmd histListAttributeGroups -t <productcode>

      KSY_SUMMARIZATION_SELECTION = *マイグレーションする集約期間のリスト*
      KSY_PRODUCT_FILTER および KSY_TABLE_FILTER 変数に追加して使用できるオプション・フィルター。マイグレーション・モードを使用するときは、この変数に追加オプションがあります。 **R** オプションを使用すると、詳細表をマイグレーションできます。その他のオプションは以下のとおりです。

      R: 詳細表のみをマイグレーション

      H: 毎時

      D: 毎日

      W: 毎週

      M: 毎月

      Q: 毎四半期

      Y: 毎年

      フィルターは組み合わせることができます。例えば、Windows OS エージェントに関する詳細表、毎時の表、および毎日の表をマイグレーションするには、次のようにします。

      ```
      KSY_PRODUCT=KNT
      KSY_SUMMARIZATION_SELECTION=R,H,D
      ```

KSY_SQL_OUTPUT_FILE_PATH = *SQL 出力のオプション・ファイル・パス*
生成された SQL ファイルを書き込むディレクトリーへのオプション・パス。このキーワードを含めないと、現行作業ディレクトリーが使用されます。

各変数の詳細および完全な構文については、応答ファイルのコメントを参照してください。

5. Tivoli Enterprise Portal Server が始動していることを確認します。
6. CANDLEHOME 変数をエクスポートしていない場合は、エクスポートします。次のコマンドを実行します。

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. スキーマ・パブリケーション・ツール・スクリプトを実行して、マイグレーションに必要なスクリプトを生成します。

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` マイグレーション用に生成されるスクリプトは、tdw_migrate_setup.sql、tdw_migrate_step1.sql、および tdw_migrate_step2.sql です。
8. tdw_migrate_setup.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

   ```
   db2 -td# -f tdw_migrate_setup.sql
   ```

   tdw_migrate_setup.sql スクリプトは、バッチでマイグレーションする場合でも 1 回のみ実行します。このスクリプトを 2 回以上実行すると、エラーが発生した場合にマイグレーション・プロセスを再開できなくなります。このスクリプトには、オブジェクトがまだ存在しない場合に失敗する可能性がある、drop ステートメントが含まれています。これらの障害はエラーと見なさないでください。これらは無視して構いません。予想される障害では、メッセージ DB21034E および SQL0204N が返される可能性があります。
9. tdw_migrate_step1.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

   ```
   db2 -tf tdw_migrate_step1.sql
   ```

   このスクリプトの実行後にエラーが発生した場合は、tdw_migrate_step2.sql スクリプトの実行前にエラーを解決しておく必要があります。すべてのエラーが解決されるまで、このスクリプトを繰り返し実行します。

   以下の戻りコードが適用されます。

   - -2: 表は既に区画化されています
   - -1: 無効なパラメーターが渡されました
   - 0: エラーなし

- 1: 非区画化表の MIGRATING_* への名前変更が失敗しました
- 2: 区画化表の作成が失敗しました
- 3: 区画化表のデータのロードが失敗しました
- 4: ソース表の DONE_* への名前変更が失敗しました

10. tdw_migrate_step2.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

    ```
    db2 -tf tdw_migrate_step2.sql
    ```

    エラーを解決するために、このスクリプトを複数回実行できます。このスクリプトは、正常にマイグレーションされなかった表には影響しません。

    注: バッチでマイグレーションする場合は、バッチごとに tdw_migrate_step1.sql スクリプトと tdw_migrate_step2.sql スクリプトを実行します。

11. データベースをバックアップします。 マイグレーション・パフォーマンスを向上するためにロード・ユーティリティーがリカバリー不能モード使用されているため、このステップを実行する必要があります。新しいバックアップが作成されるまでは、マイグレーションされた表をバックアップからリストアすることができません。

タスクの結果

これで、指定した表が区画化され、ソース表が削除されました。

次のタスク

マイグレーション中にエラーが発生した場合は、
WAREHOUSE_MIGRATION_STATUS 表を確認してください。詳しくは、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。

非区画化表から区画化表へのマイグレーション (DB2 for z/OS)

DB2 for z/OS を使用している場合は、以下のステップに従って非区画化表をマイグレーションします。

始める前に

525 ページの『前提条件とベスト・プラクティス』を確認してください。十分なディスク・スペースがあることを確認してください。

この手順を使用するには DB2 for z/OS V9 以降が必要です。

スキーマ・パブリケーション・ツールは、UNIX や Windows などの分散プラットフォームでのみ実行できます。生成されるスクリプトは、DB2 クライアントがリモート DB2 z/OS データベースに接続された分散プラットフォームから実行する必要があります。

生成されたマイグレーション・スクリプトは DB2 クライアントから実行する必要があります。

tdw_migrate_setup.sql スクリプトを実行するには、Tivoli Data Warehouse ユーザーに以下に示す権限のうちの 1 つ以上が必要です。

- セットアップ・スクリプトで使用されるパッケージ DSNADMJS および DSNADMJF に対する所有権および EXECUTE 特権
- SYSADM 権限
- パッケージ・コレクションに対する PACKADM 権限
- デーモン権限
  BPX.DAEMON がアクティブな場合、アドレス・スペースにロードされるストアード・プロシージャーを、RACF プログラム制御に対して定義する必要があります。このようにしないと、エラー「EDC5139I 操作が許可されていません」が返されます。この問題について詳しくは、IBM Support Portal の APAR II13698 を参照してください。

マイグレーションに必要な特権は、実行する必要があるすべてのマイグレーションの完了後に取り消すことができます。

ストアード・プロシージャーを DSNTIJSG サンプル・インストール・ジョブを使用して DB2 に対して定義したら、すべてのストアード・プロシージャーが RACF プログラム制御に対して定義されていることを確認する必要があります。さらに、これらのストアード・プロシージャーを実行するために必要なアプリケーション環境を WLM で定義する必要があります。また、WLMENV 値も指定する必要があります。 DB2 に対するストアード・プロシージャーの定義について詳しくは、DB2 for z/OS インフォメーション・センターにある DB2 9 以降に関する「*DB2 for z/OS インストールおよびマイグレーション・ガイド*」および「*DB2 for z/OS 管理ガイド*」を参照してください。

このタスクについて

Tivoli Data Warehouse DB2 for z/OS データベースでの非区画化表から区画化表へのマイグレーションでは、スキーマ・パブリケーション・ツールによって生成されたストアード・プロシージャーが使用されます。ストアード・プロシージャー自体は、DB2 LOAD ユーティリティーを使用する JCL ジョブを使用します。JCL ジョブは、マイグレーションされる各表ごとに作成され、実行依頼されます。

手順

1. 区画化表に対して Summarization and Pruning agent を構成します。詳しいステップについては、*IBM Tivoli Monitoring インストールおよび設定ガイド*の『Specifying range partitioned tables for the Summarization and Pruning Agent』を参照してください。
2. すべてのWarehouse Proxy agentおよびSummarization and Pruning agentのインスタンスを停止します。
3. Tivoli Data Warehouse データベースをバックアップします。
4. 以下のコマンドを使用して z/OS データベースをカタログします。

   ```
   db2 catalog tcpip node <node_Name> remote <DB_server_hostname>
     server <port_number> ostype OS390
   db2 catalog dcs database <db_name> as <db_name>
   db2 catalog db <database_name_on_server> as <alias_on_client_database_name>
     at node <node_Name> authentication dcs
   ```

5. スキーマ・パブリケーション・ツールの応答ファイルを編集します。
   a. 応答ファイルを開きます。

Windows *install_dir* ¥TMAITM6¥tdwschema.rsp

Linux UNIX *install_dir* /*arch*/bin/tdwschema.rsp

b. 以下の変数を構成します。

KSY_PRODUCT_SELECT = migrate

KSY_PRODUCT_FILTER = *マイグレーションする製品のリスト*
ある特定の製品のみが含まれることを示すためのオプション・フィルター。(フィルターを指定しないと、指定されたカテゴリー内のすべての製品がデフォルトで含まれます。) 含める製品の 3 文字の製品コードをコンマで区切って指定します。これらのコードを見つけるには、**tacmd histListProduct** コマンドを使用します (詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください)。

KSY_TABLE_FILTER = *マイグレーションする表のリスト*
特定の表のみを示すオプション・フィルター。このフィルターは、KSY_PRODUCT_FILTER 変数に追加して使用できます。特定の製品で使用できる表のリストを取得するには、次のコマンドを使用します。属性グループ名の各スペースは下線文字に置き換えます。表名のリストを取得するには、次のコマンドを使用します。
tacmd histListAttributeGroups -t <productcode>

KSY_SUMMARIZATION_SELECTION = *マイグレーションする集約期間のリスト*
KSY_PRODUCT_FILTER および KSY_TABLE_FILTER 変数に追加して使用できるオプション・フィルター。マイグレーション・モードを使用するときは、この変数に追加オプションがあります。 **R** オプションを使用すると、詳細表をマイグレーションできます。その他のオプションは以下のとおりです。

R: 詳細表のみをマイグレーション

H: 毎時

D: 毎日

W: 毎週

M: 毎月

Q: 毎四半期

Y: 毎年

フィルターは組み合わせることができます。例えば、Windows OS エージェントに関する詳細表、毎時の表、および毎日の表をマイグレーションするには、次のようにします。

```
KSY_PRODUCT=KNT
KSY_SUMMARIZATION_SELECTION=R,H,D
```

KSY_SQL_OUTPUT_FILE_PATH = *SQL 出力のオプション・ファイル・パス*
生成された SQL ファイルを書き込むディレクトリーへのオプション・パス。このキーワードを含めないと、現行作業ディレクトリーが使用されます。

各変数の詳細および完全な構文については、応答ファイルのコメントを参照してください。

6. CANDLEHOME 変数をエクスポートしていない場合は、エクスポートします。次のコマンドを実行します。

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. Tivoli Enterprise Portal Server が始動していることを確認します。
8. スキーマ・パブリケーション・ツール・スクリプトを実行して、マイグレーションに必要なスクリプトを生成します。

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` マイグレーション用に生成されるスクリプトは、tdw_migrate_setup.sql、tdw_migrate_step1.sql、および tdw_migrate_step2.sql です。
9. tdw_migrate_setup.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

   ```
   db2 -td# -f tdw_migrate_setup.sql
   ```

   tdw_migrate_setup.sql スクリプトは、バッチでマイグレーションする場合でも 1 回のみ実行します。このスクリプトを 2 回以上実行すると、エラーが発生した場合にマイグレーション・プロセスを再開できなくなります。このスクリプトには、オブジェクトがまだ存在しない場合に失敗する可能性がある、drop ステートメントが含まれています。これらの障害はエラーと見なさないでください。これらは無視して構いません。予想される障害では、メッセージ DB21034E および SQL0204N が返される可能性があります。
10. tdw_migrate_step1.sql スクリプトで、次の情報を使用して INSERT INTO WAREHOUSE_MIGRATION_CONFIG ステートメントを更新します。
    - マイグレーションのストアード・プロシージャーを実行するために必要なユーザー ID とパスワードを指定します。以下の状況では、ユーザー ID とパスワードに NULL を指定できます。
      - オペレーティング・システムが z/OS バージョン 1 リリース 13 以降であり、ストアード・プロシージャーのアドレス・スペースに関連付けられている許可 ID にデーモン権限がある。
      - オペレーティング・システムが z/OS バージョン 1 リリース 13 以降であり、ストアード・プロシージャーのアドレス・スペースに関連付けられている許可 ID に、デーモン権限はないが BPX.SRV.*userid* SURROGAT クラス・プロファイルに対する権限がある (*userid* はストアード・プロシージャーの許可 ID)。この場合は APAR OA36062 をインストールする必要があります。詳しくは、「*DB2 for z/OS 管理ガイド*」を参照してください。
    - システム LOAD および UNLOAD ユーティリティーが含まれている JCL プレフィックス・ライブラリーを指定します。

11. tdw_migrate_step1.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

    ```
    db2 -tf tdw_migrate_step1.sql
    ```

    このスクリプトの実行後にエラーが発生した場合は、tdw_migrate_step2.sql スクリプトの実行前にエラーを解決しておく必要があります。すべてのエラーが解決されるまで、このスクリプトを繰り返し実行します。

    以下の戻りコードが適用されます。

    - -5: 無効なシステム名が指定されました
    - -4: 無効なジョブ・クラスが指定されました
    - -3: プレフィックス・ライブラリーが NULL です
    - -2: 表は既に区画化されています
    - -1: 無効なパラメーターが渡されました
    - 0: エラーなし
    - 1: ソース表の名前変更が失敗しました
    - 2: 区画化表の作成が失敗しました
    - 3: マイグレーション JCL ジョブの作成または実行依頼が失敗しました
    - 4: マイグレーション JCL ジョブ状況の照会が失敗しました
    - 5: マイグレーション JCL ジョブ出力の取得が失敗しました
    - 7: ロードに失敗しました
    - 8: ソース表の名前変更が失敗しました

    戻りコード 6 は、意図的に空白にされています。
12. tdw_migrate_step2.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

    ```
    db2 -tf tdw_migrate_step2.sql
    ```

    エラーを解決するために、このスクリプトを複数回実行できます。このスクリプトは、正常にマイグレーションされなかった表には影響しません。

    注: バッチでマイグレーションする場合は、バッチごとに tdw_migrate_step1.sql スクリプトと tdw_migrate_step2.sql スクリプトを実行します。

    tdw_migrate_step2.sql スクリプトが実行されると、
    WAREHOUSE_MIGRATION_CONFIG、
    WAREHOUSE_JCLJOB_MIGRATION_STATUS、 および
    WAREHOUSE_JCLJOB_OUTPUT の各表からの行は削除されます。
13. データベースをバックアップします。 マイグレーション・パフォーマンスを向上するためにロード・ユーティリティーがリカバリー不能モード使用されているため、このステップを実行する必要があります。新しいバックアップが作成されるまでは、マイグレーションされた表をバックアップからリストアすることができません。

タスクの結果

これで、指定した表が区画化され、ソース表が削除されました。

次のタスク

マイグレーション中にエラーが発生した場合は、
WAREHOUSE_MIGRATION_STATUS、
WAREHOUSE_JCLJOB_MIGRATION_STATUS、 および
WAREHOUSE_JCLJOB_OUTPUT の各表を確認してください。詳しくは、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。

非区画化表から区画化表へのマイグレーション (Oracle)

Oracle を使用している場合は、以下のステップに従って非区画化表をマイグレーションします。

始める前に

525 ページの『前提条件とベスト・プラクティス』を確認してください。十分なディスク・スペースがあることを確認してください。

Tivoli Data Warehouse ユーザーに対し、以下のシステム特権を直接付与する必要があります。これらの特権を役割を使用して付与することはできません。

- ALTER ANY TABLE
- CREATE ANY TABLE
- DROP ANY TABLE
- LOCK ANY TABLE
- SELECT ANY TABLE
- DBMS_REDEFINITION パッケージの実行特権
  権限を付与するには、`grant execute on DBMS_REDEFINITION TO <Tivoli Data Warehouse user ID>` コマンドを使用します。

マイグレーションに必要な特権は、実行する必要があるすべてのマイグレーションの完了後に取り消すことができます。

このタスクについて

Tivoli Data Warehouse Oracle データベースでの非区画化表から区画化表へのマイグレーションでは、スキーマ・パブリケーション・ツールによって生成されたストアード・プロシージャーが使用されます。ストアード・プロシージャー自体は DBMS_REDEFINITION パッケージを使用して、非区画化表のデータを区画化表にロードします。

手順

1. 区画化表に対して Summarization and Pruning agent を構成します。詳しいステップについては、*IBM Tivoli Monitoring インストールおよび設定ガイド*の『Specifying range partitioned tables for the Summarization and Pruning Agent』を参照してください。
2. すべてのWarehouse Proxy agentおよびSummarization and Pruning agentのインスタンスを停止します。
3. Tivoli Data Warehouse データベースをバックアップします。
4. スキーマ・パブリケーション・ツールの応答ファイルを編集します。

a. 応答ファイルを開きます。

Windows *install_dir* ¥TMAITM6¥tdwschema.rsp

Linux UNIX *install_dir* /*arch*/bin/tdwschema.rsp

b. 以下の変数を構成します。

KSY_PRODUCT_SELECT = migrate

KSY_PRODUCT_FILTER = *マイグレーションする製品のリスト*
ある特定の製品のみが含まれることを示すためのオプション・フィルター。(フィルターを指定しないと、指定されたカテゴリー内のすべての製品がデフォルトで含まれます。) 含める製品の 3 文字の製品コードをコンマで区切って指定します。これらのコードを見つけるには、**tacmd histListProduct** コマンドを使用します (詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください)。

KSY_TABLE_FILTER = *マイグレーションする表のリスト*
特定の表のみを示すオプション・フィルター。このフィルターは、KSY_PRODUCT_FILTER 変数に追加して使用できます。特定の製品で使用できる表のリストを取得するには、次のコマンドを使用します。属性グループ名の各スペースは下線文字に置き換えます。表名のリストを取得するには、次のコマンドを使用します。
tacmd histListAttributeGroups -t <productcode>

KSY_SUMMARIZATION_SELECTION = *マイグレーションする集約期間のリスト*
KSY_PRODUCT_FILTER および KSY_TABLE_FILTER 変数に追加して使用できるオプション・フィルター。マイグレーション・モードを使用するときは、この変数に追加オプションがあります。 **R** オプションを使用すると、詳細表をマイグレーションできます。その他のオプションは以下のとおりです。

R: 詳細表のみをマイグレーション

H: 毎時

D: 毎日

W: 毎週

M: 毎月

Q: 毎四半期

Y: 毎年

フィルターは組み合わせることができます。例えば、Windows OS エージェントに関する詳細表、毎時の表、および毎日の表をマイグレーションするには、次のようにします。

```
KSY_PRODUCT=KNT
KSY_SUMMARIZATION_SELECTION=R,H,D
```

KSY_SQL_OUTPUT_FILE_PATH = *SQL 出力のオプション・ファイル・パス*
生成された SQL ファイルを書き込むディレクトリーへのオプション・パス。このキーワードを含めないと、現行作業ディレクトリーが使用されます。

各変数の詳細および完全な構文については、応答ファイルのコメントを参照してください。

5. Tivoli Enterprise Portal Server が始動していることを確認します。
6. CANDLEHOME 変数をエクスポートしていない場合は、エクスポートします。次のコマンドを実行します。

   Windows

   ```
   set CANDLE_HOME=install_dir
   ```

   Linux UNIX

   ```
   CANDLEHOME=/install_dir
   export CANDLEHOME
   ```

7. スキーマ・パブリケーション・ツール・スクリプトを実行して、マイグレーションに必要なスクリプトを生成します。

   Windows `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX `tdwschema.sh -rspfile tdwschema.rsp` マイグレーション用に生成されるスクリプトは、tdw_migrate_setup.sql、tdw_migrate_step1.sql、および tdw_migrate_step2.sql です。
8. tdw_migrate_setup.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

   ```
   sqlplus <TDW userid>/<password>@<Oracle SID> @./tdw_migrate_setup.sql
   ```

   tdw_migrate_setup.sql スクリプトは、バッチでマイグレーションする場合でも 1 回のみ実行します。このスクリプトを 2 回以上実行すると、エラーが発生した場合にマイグレーション・プロセスを再開できなくなります。このスクリプトには、オブジェクトがまだ存在しない場合に失敗する可能性がある、drop ステートメントが含まれています。これらの障害はエラーと見なさないでください。これらは無視して構いません。予想される障害では、メッセージ DB21034E および SQL0204N が返される可能性があります。
9. tdw_migrate_step1.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

   ```
   sqlplus <TDW userid>/<password>@<Oracle SID> @./tdw_migrate_step1.sql
   ```

   このスクリプトの実行後にエラーが発生した場合は、tdw_migrate_step2.sql スクリプトの実行前にエラーを解決しておく必要があります。すべてのエラーが解決されるまで、このスクリプトを繰り返し実行します。

   tdw_migrate_step1.sql スクリプトが正常に完了すると、メッセージが表示されます。例:

   ```
   Partitioning table "AIXTST"."KSY_TABLE_STATISTICS"

   PL/SQL procedure successfully completed.

   Table AIXTST.KSY_TABLE_STATISTICS successfully migrated.

   PL/SQL procedure successfully completed.
   ```

   このスクリプトでエラーが発生すると、標準出力にメッセージが記録されます。例:

```
Code: -20002 Message: ORA-20002:
Table "ITMUSER630"."K4X_USGS_STREAM_FLOW" is already partitioned.
```

以下のエラー・メッセージが適用されます。

- 20000: 無効なパラメーターが渡されました
- 20001: ソース表が存在していません
- 20002: 表は既に区画化されています
- 20003: ソース表が区画化可能かどうかを確認中にエラーが発生しました
- 20004: ターゲット区画化表の作成が失敗しました
- 20005: 再定義の中断時または終了時にターゲット表を除去できません
- 20006: マイグレーションが異常終了しました
- 20007: 表の再定義の終了中にエラーが発生しました
- 20008: 最終的な表の名前変更中にエラーが発生しました

10. tdw_migrate_step2.sql スクリプトを実行し、その結果を表示してスクリプトが正常に実行されたことを確認します。

    ```
    sqlplus <TDW userid>/<password>@<Oracle SID> @./tdw_migrate_step2.sql
    ```

    エラーを解決するために、このスクリプトを複数回実行できます。このスクリプトは、正常にマイグレーションされなかった表には影響しません。

    注: バッチでマイグレーションする場合は、バッチごとに tdw_migrate_step1.sql スクリプトと tdw_migrate_step2.sql スクリプトを実行します。
11. オプションで、データベースをバックアップできます。

タスクの結果

これで、指定した表が区画化され、ソース表が削除されました。

次のタスク

マイグレーション中にエラーが発生した場合は、スクリプトの実行によって出されるエラー・メッセージを確認してください。

要約とプルーニングの構成

Tivoli Management Services のインストールが完了したら、初期セットアップ・タスクの 1 つとして、要約およびプルーニング・エージェントの一般的な動作 (要約およびプルーニングのスケジュールや頻度など) を構成します。同様に、監視対象のアプリケーションで、ヒストリカル・データが収集されている属性グループの要約およびプルーニングを指定する必要があります。

Summarization and Pruning agentについて

このトピックでは、Summarization and Pruning agentの計画および構成に役立つ背景情報について説明します。

Tivoli Enterprise Portal では、**「ヒストリーの収集の構成」**ウィンドウで、または tacmd histconfiguregroups (「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照) を使用してコマンド行から、選択した属性グループの要約およびプルーニン

グを設定することができます。ウェアハウス・プロキシーおよびSummarization and Pruning agent用にデータ接続をセットアップする方法について詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」を参照してください。

収集済みデータの要約およびプルーニングの計画

Summarization and Pruning agent は、インストール中は構成されず、開始もされません。これは、すべてのインストール済みモニター・エージェントについて、ユーザーが事前にヒストリー収集を構成できるようにするためです。これは、初めて Summarization and Pruning agent を開始する前に実行する必要があるタスクです。

「ヒストリーの収集の構成」ウィンドウ

Tivoli Enterprise Portal の「**ヒストリカル収集の構成**」ウィンドウには、集約する期間、およびプルーニングする同一または異なる期間を指定するオプション (「毎年」、「毎四半期」、「毎月」、「毎週」、「毎日」、または「毎時」) があります。

「要約およびプルーニング・エージェントの構成」ウィンドウ

Summarization and Pruning agent自体は、「Tivoli Enterprise Monitoring Services の管理」ウィンドウを使用して構成します。リソースの使用状況を確認したり、ピーク負荷の時間を判別したりするには、午前 9 時から午後 5 時などの一連の時間をシフト として定義します。特定の日を通常の営業日または休日に指定するには、通常の営業日でない日を*休日* として分類します。シフトおよび休暇日を定義すると、Tivoli Data Warehouse のデータ量が増加するのでご注意ください。

Tivoli Data Warehouse の時間帯と、データを収集している一部のエージェントの時間帯が異なる場合は、*時間帯インディケーター* によって、使用する時間帯を指定します。Tivoli Data Warehouse の時間帯を使用する選択をした場合は、Tivoli Data Warehouse の時間帯を反映するようにすべてのデータが変更されます。エージェントの時間帯を選択した場合、データはそのエージェントの元の時間帯のまま変更されません。

Tivoli Data Warehouse の要約テーブル

以下は要約テーブルの名前です。*x* は、詳細データの元のテーブル名を表します。元のテーブル名の末尾に、特定の属性グループについて選択された要約期間が付加されます。データベース名には長さの制限があるため、詳細データ・テーブルと要約テーブルの名前が異なる場合があります。

毎年 x_Y

毎四半期
x_Q

毎月 x_M

毎週 x_W

毎日 x_D

毎時 x_H

このテーブルは、詳細テーブル内の要約列の名前とそれらの意味を示しています。 *x* は、元の列名を表します。数式値はエージェントにより設定さ

れ、属性グループごとに異なります。データベース名には長さ制限があるため、詳細データ・テーブルと要約テーブルの属性名を異なるものにすることができます。

表 63. 要約関数

名前	**式**
平均	AVG_x
デルタ高	HI_x
デルタ低	LOW_x
デルタ合計	TOT_x
最新 (モニター・エージェントでヒストリカル・データが収集された時刻を基準とする)	LAT_x
最大	MAX_x
最小	MIN_x
合計	SUM_x

データベース名には長さの制限があるため、詳細データ・テーブルと要約テーブルの名前が異なる場合があります。

要約とプルーニングのメトリック

以下の例で、Summarization and Pruning agentが、時間とともに累積されるメトリックをどのように計算するかを説明します。この結果を使用して、ご使用のリソースを管理することができます。この例では、メトリックは、最後にサーバーを再始動してからのキャッシュ・ヒット数を表します。

直近 1 時間のキャッシュ・ヒットの総数は、「**合計**」値で示されます。「**低**」値は、その時間のすべての詳細データ値に基づいた、時間内で最低のキャッシュ・ヒット数を表します。「**高**」値は、その時間のすべての詳細データ値に基づいた、時間内で最高のキャッシュ・ヒット数を表します。

1 時間の詳細データ値が 9、15、12、20、22 であるとすると、デルタ・ベースの処理のルールは以下のようになります。

- 現行値が直前の値より大か等しい場合、出力は直前の値から現行値を引いた値に等しくなります。
- 現行値が直前の値より小の場合、出力は現行値に等しくなります。
- 15 は 9 より大きいため、出力は 6 に等しくなります。
- 12 は 15 より小さいため、出力は 12 に等しくなります。
- 20 は 12 より大きいため、出力は 8 に等しくなります。
- 22 は 20 より大きいため、出力は 2 に等しくなります。
- TOT_ 値は 28 で、これは出力の合計です。
- LOW_ 値は 2 で、これは出力の最低値です。
- HI_ 値は 12 で、これは出力の最高値です。

要約およびプルーニングされるデータのテーブルおよびグラフにおける null 値

表セルまたはグラフ店の値として null が示されている場合、 Tivoli Data Warehouse に値が保管されていないことを意味します。 これは、指定の要約期間中に、無効と識別された値がモニター・エージェントから報告される際に発生します。エージェント・サポート・ファイルがアップグレードされ

ている可能性があるか、一部のデータは要約テーブルで計算できません (例えば、カウンターの値およびデルタ・ベースの値は、1 つの値のみが存在している場合は計算できません)。

例えば、特定の属性に対して無効な値が -1 であるとします。指定の要約期間 (毎時、毎日、毎週、毎月、毎四半期、または毎年) の間に要約およびプルーニング計算が実行される際、その時点までのすべての収集間隔 (1、5、15、または 30 分、1 時間、1 日) に対して、エージェントが -1 を報告する場合は、計算を実行すべきデータがないということになり、指定の要約に対して null が書き込まれます。

Tivoli Data Warehouse でのヒストリカル・データ収集のキャパシティー・プランニングについての提案事項

ディスク・キャパシティー・プランニングとは、ヒストリカル・データを収集する各属性グループで消費されるディスク・スペースの容量を予測することです。必要なディスク・ストレージを判別することは、データ収集ルールおよびヒストリカル・データ収集の戦略を定義する際に考慮すべき重要な要素の一つです。

DB2 データベースのパフォーマンス・チューニングについて詳しくは、「IBM Integrated Service Management Library」で、「Relational database design and performance tuning for DB2 database servers」という句の一部またはすべてを検索してください。Tivoli Data Warehouse のキャパシティー・プランニングおよびスケーリングについて詳しくは、*IBM Tivoli Monitoring インストールおよび設定ガイド*を参照してください。

エージェント・サポートのアップグレード後の要約

更新された製品のサポートをポータル・サーバーに適用した後に、 ☑ **「要約データを使用」**を選択してタイム・スパンを設定すると、ビューのステータス・バーに、欠落している列名または不明な列名についての要求エラー・メッセージが表示されることがあります。

解決策は、次にスケジュールされている要約およびプルーニングの手順が行われるまで、要約データを表示するのを待つことです。必要であれば、すぐに要約およびプルーニングを実行するようにスケジュールを変更することができます。詳しい情報は、*IBM Tivoli Monitoring インストールおよび設定ガイド*および製品の「Tivoli Enterprise Monitoring Agent ユーザーズ・ガイド」に記載されています。

要約およびプルーニングのベスト・プラクティス

Tivoli Data Warehouse に保管されているデータ・サンプルの要約およびプルーニングの方法を決定するには、ベスト・プラクティスの手法を使用します。

ヒストリカル収集を使用可能にする前に、そのデータのビジネス要件について考慮します。ヒストリカル・データには、4 つの一般的なユース・ケースがあります。属性グループごとに要件は異なるため、ヒストリカル収集の構成時にはユース・ケース (問題判別およびデバッグ、レポート、キャパシティー・プランニングと予測アラート、適応モニターなど) を考慮します。

要約およびプルーニング・エージェントおよびその他のモニター・コンポーネントのパフォーマンス・チューニングのベスト・プラクティスについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『パフォーマンス・チューニング』を参照してください。

これらのユース・ケースのそれぞれに異なるヒストリカルの要件があります。以下のセクションでは、これらの各ユース・ケース、および望ましいヒストリカル収集のタイプについて説明します。

問題判別およびデバッグ

これらのタイプのメトリックは、問題判別およびデバッグに使用され、性質上、比較的短期になる傾向があります。場合によっては、過去からの長期にわたるパフォーマンスを比較する必要がありますが、ほとんどの場合、対象エキスパート (SME) は過去数日間のデータを用意し、サーバーまたはアプリケーションのパフォーマンスを評価して、現在のパフォーマンスと比較します。この場合、データの要約は必要ありません。

レポート

ヒストリカル収集を構成する場合は、レポートの目的を考慮する必要があります。レポートには、長期間のトレンド分析に使用されるものや、SLA を満たしているかを示すためのものがあります。また、サーバーの正常性を示すための比較的短期間のレポートもあります。ヒストリカル収集の主要な推進要因はレポートの期間です。短期レポートの場合は、**詳細**データを使用できます。短期から中期のレポートの場合には、**毎時**の要約データを使用します。中期から長期のレポートの場合には、**毎日**または**毎週**の要約を使用します。

要約の構成時には、すべての間隔を構成する必要はないことに注意してください。例えば、**毎週**の要約を使用する場合、**毎日**や**毎時**も構成する必要はありません。各要約の間隔は、個別に構成できます。

キャパシティー・プランニングおよび予測アラート

キャパシティー・プランニングおよび予測分析の場合は、一般的に長期間のトレンド分析を実行します。例えば、パフォーマンス・アナライザーでは、事前定義の分析機能に対して**毎日**の要約データを使用します。そのため、ほとんどの場合、毎日の要約を構成します。ユーザー独自の分析機能を定義し、**毎時**または**毎週**の要約データを使用することもできます。

分析機能を正しく実行するには、要約テーブルに適切な数のデータ・ポイントがあるようにします。データが少ないと、統計分析は正確になりません。少なくとも 25 から 50 のデータ・ポイントが必要と考えられます。**毎日**の要約を使用して 50 個のデータ・ポイントを確保するには、プルーニングの前にデータを 50 日間保持する必要があります。データ・ポイントが多いと、統計的な予測はより正確になりますが、レポートおよび統計分析のパフォーマンスに影響を与えます。評価対象のリソースごとのデータ・ポイントが 200 から 300 を超えないように考慮してください。**毎時**の要約を使用する場合は、2 週間ごとに 336 個のデータ・ポイントが取得されます。

適応モニター (動的しきい値処理)

シチュエーションのオーバーライド機能により、ヒストリカル・データを分

析して、過去のパフォーマンス特性に基づいたしきい値を定義できます。時刻およびシフトを定義してヒストリカル・データを分析し、推奨するしきい値を提示できます。

例えば、2 週間の基本シフト・データを評価し、しきい値を「通常」の 1 標準偏差に設定します。適応モニターでは、**詳細**データを使用して評価を行い、推奨するしきい値を提示します。そのため、評価を実行するには、一定期間にわたる**詳細**データを保持する必要があります。この期間は、シフトの定義内容によって決まります。「曜日」が含まれているシフトを定義した場合、データの有効な分析を行うには、より長期のデータを保持する必要があります。すべての平日の「基本シフト」のみを確認する場合は、それほど長期のデータを保持する必要はありません。

すべての就業日を比較する場合は、7 から 30 日間の詳細データを保持します。月曜日と月曜日を比較する場合は、トレンドをつかめるように、さらに長期の詳細データを保持する必要があります。週の特定の曜日を比較する場合は、少なくとも 60 日間のデータが必要になるとお考えください。適応モニターを構成する前に、データの用途について考慮する必要があります。ディスク・スペースなど、特定タイプのデータには、適応モニターを実行する価値がありません。フリー・スペース (%)、または使用可能ディスク・スペース容量のいずれかの静的しきい値を設定する必要があります。ただし、CPU のモニターは、サーバーの動作が異常であるかの把握に非常に役立つため、適応モニターの最適な候補です。

エージェントおよび属性グループに関する考慮事項

各エージェントおよび各属性グループは、ヒストリカル収集の定義時には個別に考慮する必要があります。多くの Tivoli Monitoring 製品には、ヒストリカル収集について一連のベスト・プラクティスが定義されています。これには、要約およびプルーニングの間隔は含まれていませんが、ヒストリカル収集の設定時に有用な手引きとなります。

これらの推奨事項を調べる場合には、適応モニター、短期の問題判別、長期のレポート、またはキャパシティー・プランニングと予測分析のいずれを使用する計画であるか考慮します。要約およびプルーニングの間隔を構成する場合に、このことを考慮する必要があります。

要約およびプルーニングされたデータの可用性

要約およびプルーニング・ツールを初めて実行する場合、予期した結果が得られないことがあります。要約およびプルーニングされた Tivoli Data Warehouse のデータを予測するには、実行する必要のあるインストールおよび構成タスクを確認します。

要約およびプルーニング・プロシージャーは、データウェアハウス内に処理する十分なデータがあること、データ収集間隔およびウェアハウス間隔の設定内容、および「ヒストリーの収集の構成」ウィンドウで要約およびプルーニングの仕様が設定されているかどうか、などに依存します。要約およびプルーニングされたデータをウェアハウスから使用可能にするには、これらのインストールおよび構成タスクを完了する必要があります。

1. モニター・エージェントをインストールした後、Tivoli Enterprise Monitoring Server および Tivoli Enterprise Portal Server 上にそのモニター・エージェント用のアプリケーション・サポートを追加します。
2. エージェントの 1 つ以上の属性グループに対してヒストリカル・データ収集の構成を行います。
3. ヒストリカル収集を管理対象システムに配布して、データの収集を開始します。
4. ヒストリカル・データ収集を実行する属性グループごとに、要約およびプルーニングの間隔を構成します。
5. 最低でも 1 つのウェアハウス間隔の間、待機します。詳細テーブルでウェアハウスにデータがあることを確認します。最初の 24 時間はデータウェアハウスからではなく、短期ヒストリー・ファイルからデータが取得されるため、Tivoli Enterprise Portal でヒストリカル・データを照会するだけでは不十分です。
6. 要約およびプルーニング・エージェントを構成して、データベースに対するテスト接続を機能させ、エージェントの作業実行時刻をスケジュールするようにしてください。より前の段階でエージェントの構成を行うことは可能ですが、スケジュールされた実行が完了するまでは、ウェアハウス・データの要約およびプルーニングは期待できません。

スケジュールされた実行時刻が過ぎた後、ウェアハウスに要約データがあるはずです。

属性グループの要約およびプルーニングの構成

Tivoli Data Warehouse の要約およびプルーニングを構成して、データを集約し、データベースのサイズを管理可能なレベルに保ちます。

始める前に

「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の説明に従って、要約およびプルーニング・エージェントをインストール、構成、および開始する必要があります。

ご使用のユーザー ID に、「ヒストリー収集の構成」ウィンドウを開くためのヒストリー構成許可がある必要があります。この許可がない場合、ヒストリカル構成のメニュー項目やツールは表示されません。

このタスクについて

ウェアハウスに格納されているデータの場合、要約およびプルーニングは必須ではありませんが、要約およびプルーニングにより、データベースが不適切なサイズまで増大することを防ぎ、Tivoli Enterprise Portal に取得されるデータの量が最小限に抑えられます。属性グループのデータ収集が構成されていない場合でも、要約およびプルーニングを設定できます。属性グループに対して収集が作成および配布されていない場合、ウェアハウスにデータが送信されず、要約およびプルーニングは実行されません。

手順

1. 「ヒストリカル収集の構成」ウィンドウが開いていない場合は、**「ヒストリー構成」**をクリックします。

2. ツリーから「**モニター中のアプリケーション**」を選択します。
3. 表内の属性グループを確認します。 属性グループに対して要約およびプルーニングが既に構成されている場合は、要約およびプルーニングのセルに値が表示されます。ツリーを省略するか、枠をドラッグするか、または表を右側にスクロールして、すべてのセルを確認します。
4. 構成する 1 つ以上の属性グループを選択します。複数のグループを選択するには Ctrl キーを押しながら各グループをクリックし、最初に選択したグループからこのポイントまでのすべてのグループを選択するには、Shift キーを押しながらクリックします。 選択されたその他のグループでの設定に関係なく、選択された最初のグループの設定がそのまま表示されます。 これにより、いったん構成制御設定を調整し、同じ設定を選択したすべての属性グループに適用することが可能になります。すべてのフィールドをクリアしてやり直すには、「**すべてクリア**」ボタンを使用します。
5. 「**要約**」域で、集約するすべての期間のチェック・ボックスを選択します (「毎年」、「毎四半期」、「毎月」、「毎週」、「毎日」、または「毎時」)。
6. 「**プルーニング**」域で、プルーニングするすべての期間のチェック・ボックスを選択します (「毎年」、「毎四半期」、「毎月」、「毎週」、「毎日」、または「毎時」)。元のデータ・サンプルを維持するには、「**詳細データ**」チェック・ボックスを選択します。対応するフィールドで、データを保持する日数、月数、または年数を指定します。
7. 「**適用**」をクリックし、選択されている属性グループの構成を保存します。 属性グループの要約およびプルーニングのセルは更新され、新規設定を反映します。

次のタスク

要約およびプルーニングが次回に実行されるときに、要約およびプルーニング・エージェントにより、データウェアハウスに保管されている長期データに構成が適用されます。要約データの表示を確認するには、次回のスケジュール期間が経過するまで待ってください。

グローバル構成設定の変更

データの要約、プルーニング、または収集に関するシステム規模の構成設定を変更するには、「要約およびプルーニング・エージェントの構成」ウィンドウを使用します。

このタスクについて

要約およびプルーニング・エージェントの構成を編集するには、以下のステップを実行します。

手順

1. 「Tivoli Enterprise Monitoring Services の管理」で、Summarization and Pruning agentを右クリックします。
2. 「**再構成**」をクリックします。
3. 「ウェアハウスの要約およびプルーニング・エージェント: 拡張構成」ウィンドウで、「**OK**」をクリックします。

4. 次のウィンドウで「**OK**」をクリックします。
5. 「ウェアハウスの要約およびプルーニング・エージェント」ウィンドウで「**はい**」をクリックして、要約およびプルーニング・エージェントを構成します。
6. 以下のように、「**ソース**」タブに Tivoli Data Warehouse データベースおよび Tivoli Enterprise Portal サーバー情報を入力します。
   a. 「**JDBC ドライバー**」フィールドで、「**追加**」をクリックしてファイル・ブラウザー・ウィンドウを呼び出し、JDBC ドライバーを選択します。「**OK**」 をクリックしてこのブラウザーを閉じ、JDBC ドライバーをリストに追加します。 また、「JDBC ドライバー」リストの項目を強調表示させ、「**削除**」をクリックすると、ドライバーを削除できます。これにより、Tivoli Data Warehouse データベースと通信する JDBC ドライバーを収集できるようになります。JDBC ドライバーは別個にインストールされており、各データベースは一連の JDBC ドライバーを提供しています。

      注:

      - Tivoli Data Warehouse データベースが UNIX 系オペレーティング・システム上にある場合、DB2 がインストールされているディレクトリーを検出し、jdbc ドライバー・ディレクトリーで db2jcc.jar ファイルと db2jcc_license_cu.jar ファイルを選択します。例えば、*<db2_installdir>*/java/db2jcc.jar および *<db2_installdir>*/java/db2jcc_license_cu.jar です。
      - Tivoli Data Warehouse データベースが MS SQL Server 2000 または 2005 上にある場合、Microsoft SQL Server の Web サイトから MS SQL Server 2005 JDBC ドライバーをインストールします。sqljbc.jar ファイルが必要になります。Microsoft のオペレーティング・システムのインストール手順書を参照して、ファイルを検索します。
      - Tivoli Data Warehouse データベースが Oracle を使用している場合は、ojdbc14.jar ファイルを使用します。Windows での場所は、*%ORACLE_HOME%*¥jdbc¥lib で、UNIX 系オペレーティング・システムでの場所は、*$ORACLE_HOME*/jdbc/lib です。

   b. ドロップダウン・リストで、Tivoli Data Warehouse のデータベースのタイプを選択します。
   c. これが正しくない場合は、Tivoli Data Warehouse の URL、ドライバー、スキーマ、ユーザー ID、およびパスワードを入力します。

      重要: ウェアハウス・プロキシーの構成時に、データベース・ユーザー (デフォルトでは ITMUser) が作成されます。ここで入力するユーザー ID は、このデータベース・ユーザーと一致している必要があります。

   d. 「**データベース接続のテスト (Test database connection)**」をクリックし、Tivoli Data Warehouse データベースと通信できることを確認します。
   e. デフォルトを使用しない場合は、Tivoli Enterprise Portal Server のホストおよびポートを入力します。 「**TEP Server ポート (TEP Server Port)**」フィールドは、数値専用です。
7. 「**スケジューリング**」タブで、スケジューリング情報を選択します。

- 「固定」- エージェントを実行する間隔 (*x* 日ごと) およびその時刻 (すぐに実行する場合は、現時点から少なくとも 5 分後) をスケジュールします。デフォルトでは、毎日午前 2:00 に実行します。
- 「柔軟」- *x* 分ごとに実行するようエージェントをスケジュールします。「**追加**」ボタンの上のテキスト・ボックスには、エージェントを実行しない時間帯を指定できます。その場合、HH:MM-HH:MM の形式 (例えば、正午 12 時から午後 8 時まで実行しない場合は 24 時間クロックで 12:00-20:00 のように指定) を使用し、「**追加**」ボタンをクリックして「**除外**」ボックスにその時刻範囲を追加します。

「**固定**」を選択した場合、要約およびプルーニング・エージェントを*開始* しても、すぐには要約およびプルーニングを実行しません。要約およびプルーニング・エージェントを*実行* すると、要約およびプルーニングが行われます。要約およびプルーニング・エージェントは、「スケジューリング」タブの設定に従って実行されます。「**柔軟**」を選択した場合、要約およびプルーニング・エージェントは開始直後に 1 回実行され、その後は、停電時を除いて、「**実行間隔 (Run Every)**」で指定した間隔で実行されます。

8. 「**就業日**」タブで勤務時間情報と休日設定を指定します。
   a. 「**週の開始**」として日曜日または月曜日を選択します。
   b. 勤務時間の場合、「**シフトの指定**」を選択します。このフィールドのデフォルト設定は、ウィンドウの右側にある「**ピーク勤務時間 (Peak Shift Hours)**」ボックスにリストされます。これらの設定を変更するには、「**オフピーク・シフト時間**」ボックスで任意の時間を選択し、右矢印ボタンをクリックして「**ピーク・シフト時間**」ボックスにそれらの時間を追加します。

      重要: 勤務時間の指定は推奨されません。データウェアハウスに必要なディスク・スペースおよび 要約およびプルーニング に必要な処理時間を増加させるためです。

      制約事項: データを要約した後に勤務時間情報を変更すると、データに不整合が生じる場合があります。以前に収集および要約されたデータを新しい勤務時間値で再計算することはできません。
   c. 休暇日設定を変更する場合は、「**休暇日の指定**」を選択します。「**はい**」または「**いいえ**」をクリックし、休日として週末を指定します。「**追加**」を選択してカレンダーを開いてから、追加する休暇日を選択します。 選択した日が、「**休日の選択 (Select vacation days)**」フィールドの下にあるボックスに表示されます。以前に選択した日を削除する場合は、その日を選択して「**削除**」をクリックします。

      Linux UNIX 右クリックして月と年を選択します。
9. 「**ログ・パラメーター**」タブで使用するオプションを選択します。 このタブでは、ウェアハウス・プロキシーと要約およびプルーニング・エージェントによって取り込まれるログ・テーブルをプルーニングするパラメーターを定義します。
   a. □「**次の WAREHOUSEAGGREGLOG データを保持**」を選択して、WAREHOUSEAGGREGLOG テーブルをプルーニングします。このテーブルのデータは、要約およびプルーニング・エージェントによって追加されます。このオプションを使用可能にした後、テーブルでデータを保持する日

数、月数、または年数を指定します。指定した時間よりも古いデータは、要約およびウェアハウスのプルーニング・エージェントによって削除されます。

b. □「**次の WAREHOUSELOG データを保持**」を選択して、WAREHOUSELOG テーブルをプルーニングします。このテーブルのデータは、ウェアハウス・プロキシーによって追加されます。このオプションを使用可能にしてから、テーブルでデータを保持する日数、月数、または年数を指定します。指定した時間間隔よりも古いデータは、要約およびプルーニング・エージェントによって削除されます。

10. 「**追加のパラメーター**」タブで、以下のオプションを選択します。

a. 単一のデータベース・トランザクションで削除できる最大行数を指定します。値は 1 から n で指定します。デフォルトは 1000 です。

b. 「**これより古い毎時データを要約**」フィールドおよび「**これより古い日次データを要約**」フィールドで、要約するデータの経過時間を指定します。値は 0 から n で指定します。デフォルトは、時間単位データでは 1、日単位データでは 0 です。

c. 「**使用する時間帯オフセット (Use timezone offset from)**」ドロップダウン・リストから、使用する時間帯を選択します。 Tivoli Data Warehouse の時間帯と、データを収集している一部のエージェントの時間帯が異なる場合に、すべてのデータを同じデータベースに格納するには、このオプションを使用して、使用する時間帯を指定します。

d. 「**ワーカー・スレッドの数**」で、要約およびプルーニング・エージェントがデータを処理するときに使用する同時実行スレッドの数を指定します。推奨値は、CPU 数の 2 倍です。スレッドを増やすと、要約およびプルーニング・エージェントの完了は速まりますが、要約およびプルーニング・エージェントを実行しているマシンのリソースと、接続およびトランザクション・ログのスペースなどのデータベース・リソースがより多く使用されることになります。

e. 要約およびプルーニングでは、メモリー内で発生した最新のエラーをキャッシュに入れます。この情報は属性グループで提供され、要約およびプルーニング・エージェントで提供されるワークスペースで表示できます。「**表示するノード・エラーの最大数**」設定では、メモリー内に格納するエラーの最大数を指定します。最新のエラーのみが保持されます。いったん制限に到達すると最も古いエラーが除去されます。

f. 要約およびプルーニングでは、実行された最新の実行に関する情報をキャッシュに入れます。この情報は属性グループで提供され、要約およびプルーニング・エージェントで提供されるワークスペースで表示できます。「**表示する要約およびプルーニングの実行の最大数**」設定では、メモリー内に格納する実行の最大数を指定します。最新の実行のみが保持されます。いったん制限に到達すると最も古い実行が除去されます。

g. 要約およびプルーニング・エージェントでは、エージェントがデータウェアハウス・データベースと通信できることを定期的に確認します。「**データベース接続キャッシュ時間**」設定では、この確認の実行頻度を決定します。

h. パフォーマンスを向上させるため、要約およびプルーニング・エージェントではデータウェアハウス・データベースに対する更新をバッチ処理します。

「**バッチ・モード**」パラメーターでは、バッチの実行方法を指定します。「**単一の管理対象システム**」および「**複数の管理対象システム**」という 2 つのオプションがあります。

11. Linux UNIX 設定がすべて正しい場合は「**保存**」ボタン、元の値を再ロードする場合は「**再ロード**」ボタン、「要約およびプルーニング・エージェントの構成」ウィンドウを取り消して閉じる場合は任意の時点で「**キャンセル**」ボタンをクリックします。

Summarization and Pruning agentを使用不可にする方法

要約およびプルーニング・エージェントは、エンタープライズ全体で使用不可にすることも、特定の製品または属性グループ一式で使用不可にすることもできます。

このタスクについて

エンタープライズ全体の要約およびプルーニングを使用不可にする場合は、

1. 「Tivoli Enterprise Monitoring Services の管理」の「サービス/アプリケーション」列で、Summarization and Pruning agentを右クリックします。
2. 「**停止**」を選択します。

「**ヒストリカル収集の構成**」ウィンドウで、特定の製品について、または一連の属性グループについて、要約およびプルーニングをオフにする場合は、以下のようにします。

手順

1. Tivoli Enterprise Portal で、ツールバーにある「**ヒストリカル収集の構成**」ボタンをクリックします。
2. 「**製品**」を選択します。
3. 1 つ以上の**属性グループ**を選択します。
4. 「**グループの構成を解除**」ボタンをクリックします。

保管データのエラー・ロギング

Tivoli Data Warehouse へのデータのロールオフ時にウェアハウス・プロキシー・エージェントでエラーが発生した場合、これらのエラーはイベント・ログに記録されます。トレース・オプションを設定して追加のエラー・メッセージを収集し、問題の検出に役立つログを表示できます。

手順

- 以下のように、ウェアハウス・プロキシーのエラーがリストされているイベント・ログを開きます。
  - Windows 「**スタート**」→「**プログラム**」→「**管理ツール**」→「**イベント・ビューアー**」をクリックしてイベント・ビューアーを開始し、「ログ」メニューから「**アプリケーション**」を選択します。データのロールオフ時にエラーが発生した場合、エントリーは Windows アプリケーション・イベント・ログに挿入されます。
  - Linux ファイル *ITM_dir*/logs/*hd*.log を開きます。

– いずれのプラットフォームの場合も、エラーはウェアハウス・データベース内の表 WAREHOUSELOG にも表示されます。

- 以下のようにトレース・オプションをアクティブにします。
  1. 「Tivoli Monitoring Services の管理」で、「**ウェアハウス・プロキシー**」を右クリックし、「**トレース・パラメーターの拡張編集 (Advanced Edit Trace Parms)**」を選択します。
  2. RAS1 フィルターを選択します。デフォルト設定は **ERROR** です。
  3. 残りのフィールドではデフォルト設定を受け入れます。
  4. 「**はい**」をクリックしてサービスを再開します。
- エラー・メッセージが含まれているトレース・ログを以下のように表示します。
  1. 「Tivoli Monitoring Services の管理」で、「**ウェアハウス・プロキシー**」を右クリックして、「**拡張**」→「**トレース・ログの表示**」を選択します。「ログ・ビューアー (Log Viewer)」ウィンドウにウェアハウス・プロキシーのログ・ファイルのリストが表示されます。
  2. 「ログ・ファイルの選択 (Select Log File)」で該当するログ・ファイルを選択します。このウィンドウには、すべてのログ・ファイルが最新のものから順番にリストされます。
  3. 「**OK**」をクリックします。

エージェント・オペレーション・ログ・ヒストリーの収集

エージェント・オペレーション・ログは、エンタープライズ内の分散エージェントで発生したメッセージを収集します。このログは、Tivoli Management Services エージェント・フレームワークの一部です。 Windows の場合、ヒストリカル・データ収集構成にエージェント・オペレーション・ログ属性グループ (OPLOG 表) が含まれているときは、ヒストリカル・データ用のディレクトリーを作成し、各エージェントの構成ファイルを編集する必要があります。

始める前に

同一コンピューターでヒストリカル・データを収集するすべてのエージェントに対し、手動でヒストリー・データ・ディレクトリーを作成してから、同一コンピューター上にあるエージェント構成ファイルをそれぞれ編集して、短期データ収集の新規パスを指定する必要があります。この操作は、Windows で必要となります。なぜなら、すべてのエージェント・ログがデフォルトで同じ *install_dir*¥tmaitm6¥logs¥ ディレクトリーに保管され、それぞれのエージェントが、短期ヒストリー・データを保管する OPLOG という名前のエージェント・オペレーション・ログ・ファイルを作成するからです。つまり、同じ OPLOG ヒストリー・ファイルが、すべてのエージェントによって共有されており、複数のエージェント・プロセスが同じ短期ヒストリー・バイナリー・ファイルからヒストリー・データをウェアハウスに保管しようとすると、同じデータが Tivoli Data Warehouse に何度も転送される可能性があります。

例えば、Windows OS および Active Directory モニター・エージェントがインストールされていたとします。各プロセスでは、オペレーション・ログ・ヒストリー・データが作成され、C:¥IBM¥ITM¥TMAITM6¥logs¥OPLOG というファイルに保管されます。この時点で、同じヒストリー・データ・ファイルを共有しようとしているプロ

セスが少なくとも 2 つあります。複数エージェントからのデータを同じファイルに書き込むことができますが、ウェアハウス・アップロード・プロセスではこのセットアップで問題が生じます。エージェント・プロセスでは、別のエージェント・プロセスが同じ短期ヒストリー・ファイルから同じウェアハウス・データのアップロードを実行している可能性が常にあることは認識されません。そのため、ウェアハウス・データベースに転送されるヒストリー・データが重複することがあります。

このタスクについて

Windows 上でヒストリカル・データを収集するエージェントごとに、次のステップを実行してください。

手順

1. *install_dir* ¥tmaitm6¥logs¥ の history 子ディレクトリーを作成します。
2. *install_dir* ¥tmaitm6¥logs¥history の k?? 子ディレクトリーを作成します。ここで、?? は、2 文字の製品コードです。例えば、c:¥ibm¥itm¥tmaitm6¥logs¥history¥k3z は、*IBM Tivoli Monitoring Agent for Active Directory* 短期ヒストリー・ファイルへのパスです。このエージェントのシステム・ユーザー ID は、このディレクトリーの読み取りおよび書き込み許可を持っている必要があります。
3. テキスト・エディターで、*install_dir* ¥tmaitm6¥k??cma.ini エージェント構成ファイルを開きます (ここで、?? は 2 文字の製品コードです)。 エージェント構成で使用されるファイルの名前については、Monitoring 製品のユーザーズ・ガイドを参照してください。
4. CTIRA_HIST_DIR=@LogPath@ パラメーターを見つけ、¥history¥k?? を付加します (ここで、?? は 2 文字の製品コードです)。例えば、CTIRA_HIST_DIR=@LogPath@¥history¥knt は、このコンピューター上の Windows OS エージェントのヒストリカル・データ収集用に c:¥ibm¥itm¥tmaitm6¥logs¥history¥knt を指定します。
5. k??cma.ini 構成ファイルを保存します。
6. *install_dir* ¥tmaitm6¥logs¥khdexp.cfg ウェアハウス・アップロード状況ファイルを ¥history¥k?? ディレクトリーにコピーします。 このファイルが新規エージェント・ヒストリー・ディレクトリーにコピーされない場合は、既存のヒストリー・データが複数回ウェアハウスに保管される場合があります。ヒストリー・ウェアハウス・オプションが使用可能になっていない場合は、このファイルが存在しない可能性があります。
7. エージェントのすべての .hdr ファイルと、そのファイルのベース名を持つファイル (ファイル拡張子なし) を新規ロケーションにコピーします。 例えば、c:¥ibm¥itm¥tmaitm6¥logs¥history¥knt ディレクトリーは、次のようになります。

```
khdexp.cfg
netwrkin
netwrkin.hdr
ntprocssr
ntprocssr.hdr
wtlogcldsk
wtlogcldsk.hdr
wtmemory
wtmemory.hdr
wtphysdsk
```

```
wtphysdsk.hdr
wtserver
wtserver.hdr
wtsystem
wtsystem.hdr
```

ターゲット・エージェントによって管理されていない tmaitm6¥logs ディレクトリーからヒストリー・データ・ファイルをコピーする場合があることに注意してください。例えば、ディレクトリーに Oracle データベース・ヒストリー・データが含まれている可能性があるが、ファイルを新規 Windows OS エージェント・ヒストリー・ディレクトリーにコピーするとします。 Windows OS エージェントによって使用されないコピーされたファイルは必要とされず、安全に削除することができます。

8. Tivoli Enterprise Monitoring Services の管理 で、モニター・エージェント・サービスを右クリックし、「**再構成**」をクリックしてから「**OK**」を 2 回クリックして、構成ウィンドウの設定を受け入れます。次に、  「**開始**」をクリックしてエージェントを開始します。

区切り文字で区切られたフラット・ファイルを使用するための変換プロセス

データをウェアハウスに保管しないことを選択した場合、収集したデータを、区切り文字で区切られたフラット・ファイルに変換する必要があります。データの変換を手動または自動で行うように、スケジュールすることができます。区切り文字で区切られたフラット・ファイルへのデータ変換を引き続き行う選択をした場合は、データ変換を自動にするようスケジュールします。製品レポートに表示される短期ヒストリーをサポートすることのみを目的として、ヒストリカル・データを収集する場合であっても、定期的にデータ変換を実行するようにしてください。

KHD_TOTAL_HIST_MAXSIZE 環境変数が使用されている場合、短期ヒストリー・ファイルの制限に達すると、エージェントは短期ヒストリー・ファイルにヒストリカル・データを書き込めなくなります。この変数はエージェントに対する制限があります。

データ変換プログラム

短期ヒストリー・ファイルから区切り文字で区切られたフラット・ファイルへの変換は、データ・ロールオフ・プログラムを実行することにより行われます。

Linux UNIX Windows **krarloff**

z/OS **KPDXTRA**

ヒストリー・データ・ファイルおよびメタ記述ファイルに追加される列

ヒストリー・データ・ファイルおよびメタ記述ファイルには、以下の 4 つの列が自動的に追加されます。

- **TMZDIFF**。世界時 (GMT) との時間帯の差。この値は秒で示されます。
- **WRITETIME**。レコードが書き込まれたときの CT タイム・スタンプ。これは 16 文字の値で構成されるフォーマットです。ここで、c は世紀、yymmdd は年、月、日、hhmmssttt は時間、分、秒、cyymmddhhmmssttt はミリ秒です。

- **SAMPLES**。SAMPLES 列は、同じサンプル中に収集される値毎に増分し、その後、再度開始値にリセットされます。同じサンプルで収集される行は、異なる SAMPLES 列の値を持っています。
- **INTERVAL**。サンプル間の時間 (ミリ秒単位)。

注: データウェアハウスのプロセスにより、2 つの列 (TMZDIFF および WRITETIME) のみが Tivoli Data Warehouse データベースに追加されます。

メタ記述ファイル

メタ記述ファイルは、ソース・ファイルのデータのフォーマットを記述するものです。メタ記述ファイルは、ヒストリカル・データ収集処理の開始時に生成されます。

オペレーティング・システム環境ごとに、使用されるファイルの命名規則は異なります。ここに、一部のオペレーティング・システム環境のルールを示します。

- IBM i および HP NonStop Kernel: 記述ファイルは基準としてデータ・ファイルの名を使用します。名前の最後の文字は「M」です。例えば、テーブル QMLHB の場合、ヒストリー・データ・ファイルの名前は QMLHB、記述ファイルの名前は QMLHBM となります。
- z/OS: 記述レコードは、データとともに PDS ファシリティーに格納されます。
- UNIX および Linux: *.hdr ファイル命名規則を使用します。
- Windows: *.hdr ファイル命名規則を使用します。

サンプル *.hdr メタ記述ファイル

```
TMZDIFF(int,0,4) WRITETIME(char,4,16)
QM_APAL.ORIGINNODE(char,20,128) QM_APAL.QMNAME(char,148,48)
QM_APAL.APPLID(char,196,12) QM_APAL.APPLTYPE(int,208,4)
QM_APAL.SDATE_TIME(char,212,16)
QM_APAL.HOST_NAME(char,228,48)
QM_APAL.CNTTRANPGM(int,276,4) QM_APAL.MSGSPUT(int,280,4)
QM_APAL.MSGSREAD(int,284,4) QM_APAL.MSGSBROWSD(int,288,4)
QM_APAL.INSIZEAVG(int,292,4) QM_APAL.OUTSIZEAVG(int,296,4)
QM_APAL.AVGMQTIME(int,300,4) QM_APAL.AVGAPPTIME(int,304,4)
QM_APAL.COUNTOFQS(int,308,4) QM_APAL.AVGMQGTIME(int,312,4)
QM_APAL.AVGMQPTIME(int,316,4) QM_APAL.DEFSTATE(int,320,4)
QM_APAL.INT_TIME(int,324,4) QM_APAL.INT_TIMEC(char,328,8)
QM_APAL.CNTTASKID(int,336,4) SAMPLES(int,340,4)
INTERVAL(int,344,4)
```

例えば、エントリーは以下の形式です。ここで、*int* はデータが整数であることを示し、*75* はデータ・ファイルのバイト・オフセットであり、*20* はファイルにおけるこの属性のフィールドの長さです。

```
attribute_name(int,75,20)
```

ヒストリカル・データ・テーブルを保持するために必要なスペースの見積もり

製品のヒストリカル・データ・テーブルは、製品の文書に定義されています。ヒストリカル・データが保管されるテーブルの名前とそのサイズ、およびデフォルトのテーブルを調べるには、該当するエージェント・ガイドを参照してください。

短期ヒストリー・ファイルの拡大の制限

ご使用の環境がデータウェアハウスを備えているか、または短期ヒストリーを区切り文字で区切られているフラット・ファイルに変換するように設定されているかにかかわらず、ヒストリー・ファイルの最大サイズを設定することをお勧めします。

始める前に

オペレーティング・システムのユーザー ID にこのディレクトリーに対する書き込み許可が必要です。

これらのエージェント環境変数は、z/OS では使用できません。

このタスクについて

構成に Tivoli Data Warehouse へのデータのロールオフを備えている場合、短期ヒストリー・ファイルのサイズは収集するデータ量、収集頻度、およびデータウェアハウスのロールオフの頻度で制御されます。そのうえ、ウェアハウスのプロキシー・エージェントまたはデータウェアハウスが使用できなくなる可能性があります。これは、短期ヒストリー・ファイルが際限なく拡大する可能性があるということを意味します。

ヒストリカル・データ収集が行われているすべての Tivoli Enterprise Monitoring Agent、または Tivoli Enterprise Monitoring Server (こちらでデータ収集が行われている場合のみ) で、環境変数 KHD_TOTAL_HIST_MAXSIZE および KHD_HISTSIZE_EVAL_INTERVAL を設定します。

短期ヒストリー・ファイルが保存されるディレクトリーのサイズ制限およびこの抑制の実行頻度を指定するには、以下のステップを実行します。

手順

1. エージェントの環境ファイルを開きます。
   - Windows 「Tivoli Monitoring Services の管理」ウィンドウで、コンポーネントを右クリックし、「**拡張**」→「**ENV ファイルの編集**」をクリックします (これらは *install_dir* ¥TMAITM6¥K<pc>ENV ファイルです。ここで、<pc> は C:¥IBM¥ITM¥TMAITM6¥KNTENV などの 2 文字の製品コードです)。
   - Linux UNIX *install_dir* /config ディレクトリーに移動し、テキスト・エディターで <pc>.ini を開きます。ここで、<pc> は 2 文字の製品コードです。例えば、UNIX OS エージェントでは、/opt/IBM/ITM/config/ux.ini です。

   製品コードのリストについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『IBM Tivoli 製品、プラットフォーム、およびコンポーネント・コード』を参照してください。
2. ファイルに新しい 2 行を追加します。ここで、5 は、短期ヒストリー・ファイルが置かれているディレクトリーを拡大できる最大メガバイト数です。また、900 (15 分) はディレクトリー・サイズの評価間隔の秒数です。

   ```
   KHD_TOTAL_HIST_MAXSIZE =5
   KHD_HISTSIZE_EVAL_INTERVAL=900
   ```
3. ファイルを保存して閉じます。

4. コンポーネントをリサイクルします。

タスクの結果

最大値を設定すると、ディレクトリーの制限に到達した後は、短期ヒストリー・ファイルに新しいレコードが書き込まれなくなり、収集されたデータに欠落が生じます。ただし、データがウェアハウスに格納されている場合、ウェアハウス・プロキシーでは、最新の 24 時間のデータのみが格納されるように、短期ヒストリー・ファイルを切り取ります。これにより、エージェントはヒストリカル・データを再び書き込むことができるようになります。結果として、再度制限に到達し、このプロセスが繰り返される可能性があります。また、このプロセスでもデータに途切れが出現する可能性があります。

短期ヒストリー・ファイル・ディレクトリーのサイズが制限に達した場合の処置

Tivoli Enterprise Monitoring Agent (データ収集が Tivoli Enterprise Monitoring Server で行われている場合は Tivoli Enterprise Monitoring Server) に対して KHD_TOTAL_HIST_MAXSIZE 環境変数と KHD_HISTSIZE_EVAL_INTERVAL 環境変数が設定されている場合、最大ディレクトリー・サイズに達すると、ヒストリカル・データのサンプルはそれ以上短期ヒストリー・ファイルに追加されません。

ヒストリー・ファイルへのデータ・サンプルの保存を再開するには、短期ヒストリー・ファイルが際限なく拡大する原因を解決する必要があります。データがエージェントで収集されている場合は、この状況が発生した際報告を行うカスタム SQL 照会またはシチュエーション、あるいはその両方を作成することができます。

以下は、実行可能なカスタム SQL 照会の例です。

```
SELECT ORIGINNODE, CATEGORY, SEVERITY, TABLE, TIMESTAMP, MESSAGE
FROM O4SRV.KRAMESG WHERE ORIGINNODE = $NODE$
```

区切り文字で区切られたフラット・ファイルへの短期ヒストリー・ファイルの変換

データをデータベースに格納するオプションを選択した場合は、そのオプションを指定したままでは、このセクションで説明するファイル変換プログラムを実行することはできません。これらの変換手順を使用するには、Tivoli Enterprise Portal の「ヒストリーの収集の構成」ウィンドウでウェアハウス・オプションに「**オフ**」を指定しておく必要があります。

変換手順を実行するとヒストリー累積ファイルが空になるため、ヒストリー・ファイルが不必要にディスク・スペースを消費しないように、変換手順を定期的に実行する必要があります。

krarloff プログラムを使用したファイルの変換

krarloff ロールオフ・プログラムは、Tivoli Enterprise Monitoring Server 上か、またはモニター・エージェントが実行されているディレクトリーで、ヒストリー・ファイルが保管されているディレクトリーから実行できます。

属性の書式設定

表示目的のために、一部の属性を書式設定する必要があります。例えば、浮動小数点数では、小数点の左側に出力する有効数字の桁数が指定されます。これらの表示書式設定における考慮事項は、製品の属性ファイルに明記されています。

krarloff ロールオフ・プログラムを使用してヒストリカル・データをテキスト・ファイルへロールオフする際には、属性ファイルで指示されている書式指定子を必要とする属性はすべて、無視されます。ロールオフ後のヒストリー・テキスト・ファイルには未加工の数値のみが出力されます。したがって、45.99% や 45.99 とは表示されずに数値 4599 が表示されます。

データは、ウェアハウス・プロキシーにより、属性ファイルに指定されているタイプ、長さ、およびデータ精度に応じて挿入されます。ただし、Tivoli Data Warehouse データベースでは、浮動小数点数の形式で整数を使用する属性のみ が正しい書式設定で表示されます。

Linux や UNIX で krarloff ロールオフ・プログラムを使用して、Tivoli System Monitor Agent のヒストリー・ファイルをテキスト・ファイルに変換することができます。UNIX や Linux では Tivoli System Monitor Agent がコマンド **itmcmd history** を提供しないため、krarloff ロールオフ・プログラムが使用されます。

手順

Windows

krarloff ロールオフ・プログラムは、コマンド・プロンプトで以下のように入力して、モニター・サーバーまたはモニター・エージェントが実行されているディレクトリーから実行します。

```
krarloff [-h] [-g] [-x] [-d delimiter] [-m metafile] [-r rename-to-file]
[-o output-file] {-s source | source-file name}
```

ここで、[ ] 大括弧はオプションのパラメーターを表し、{ } 中括弧は必須パラメーターを表しています。

Linux

1. 環境変数を次のように設定します。

   ```
   export PATH=$PATH: $CANDLEHOME/tmaitm6/<interp>/bin/
   export ATTRLIB=$CANDLEHOME/<interp>/lz/tables/ATTRLIB
   export LD_LIBRARY_PATH=$CANDLEHOME/<interp>/gs/lib
   ```

2. ヘッダーとデータ・ファイルを別のディレクトリーにコピーします。

   ```
   mkdir $CANDLEHOME/<interp>/lz/hist/tmp
   cp PVTHIST_LNXCPU* $CANDLEHOME/<interp>/lz/hist/tmp
   cd tmp
   ```

3. krarloff プログラムを実行し、ヒストリー・ファイルをテキスト・ファイルに変換します。例:

   ```
   krarloff -h -d ";" -m PVTHIST_LNXCPU.hdr -o PVTHIST_LNXCPU.out
   -s PVTHIST_LNXCPU
   ```

UNIX

1. 環境変数を次のように設定します。

   ```
   export PATH=$PATH: $CANDLEHOME/tmaitm6/<interp>/bin/
   export ATTRLIB=$CANDLEHOME/<interp>/ux/tables/ATTRLIB
   ```

2. ヘッダーとデータ・ファイルを別のディレクトリーにコピーします。

```
mkdir $CANDLEHOME/<interp>/ux/hist/tmp
cp PVTHIST_UNIXDISK* $CANDLEHOME/<interp>/ux/hist/tmp
cd tmp
```

3. krarloff プログラムを実行し、ヒストリー・ファイルをテキスト・ファイルに変換します。例:

```
krarloff -h -d ";" -m PVTHIST_UNIXDISK.hdr -o PVTHIST_UNIXDISK.out
-s PVTHIST_UNIXDISK
```

変換が終了したら、ヒストリー・ファイルの名前を *.old に変更します。例: PVTHIST_LNXCPU becomes PVTHIST_LNXCPU.old。

エージェントにより、すべての専用ヒストリー・ファイルが以下のサブディレクトリーに出力されます。

Windows *install_dir* ¥TMAITM6¥logs

Linux UNIX *install_dir* /<*arch*>/<*pc*>/hist

制約事項: krarloff ロールオフ・プログラムは、AS400 システムの IBM i エージェントではサポートされていません。

Krarloff ロールオフ・プログラム・パラメーター

以下の表に、krarloff ロールオフ・プログラムのパラメーター、その目的、およびデフォルト値をリストします。

表 64. krarloff ロールオフ・プログラムのパラメーター

パラメーター	デフォルト値	説明
-h	off	出力ファイルでのヘッダーの有無を制御します。存在する場合は、最初の行としてヘッダーが出力されます。ヘッダーによって、属性列名を識別します。
-g	off	出力ファイルのヘッダーにおける製品の group_name の有無を制御します。ヘッダーに group_name.attribute_name を組み込むには、krarloff ロールオフ・プログラムの起動行に -g を追加します。
-x	off	出力ファイルで SAMPLES 属性と INTERVAL 属性を除外します。
-d	tab	出力テキスト・ファイルのフィールドを分離するために使用する区切り文字。有効な値は任意の単一の文字 (コンマなど) です。
-m	source-file.hdr	ソース・ファイルにおけるデータの形式を記述するメタファイル。コマンド行でメタファイルを指定しないと、デフォルトのファイル名が使用されます。
-r	source-file.old	ソース・ファイルの名前変更に使用する、名前変更後のファイル名を指定するパラメーター。名前変更操作に失敗した場合、スクリプトは 2 秒待機してから操作を再試行します。
-o	source-file.*nnn*。ここで、*nnn* はユリウス日です。	出力ファイル名。出力テキスト・ファイルを含むファイルの名前。

表 64. krarloff ロールオフ・プログラムのパラメーター (続き)

パラメーター	デフォルト値	説明
-s	なし	**必須パラメーター**。読み取る必要があるデータを含むソース短期ヒストリー・ファイル。中括弧の中で、縦棒 (|) は -s source オプションを使用できることを示します (オプションなしで名前を指定すると、それがソース・ファイル名と見なされます)。ソース・ファイルのデフォルトは想定されません。

Windows システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換

ヒストリカル・データ収集構成プログラムで設定したルールを使用して収集したヒストリー・ファイルを、各種の一般アプリケーションでの使用のために、区切り文字で区切られたフラット・ファイルへ変換すると、容易にデータを操作し、レポートおよびグラフを作成できるようになります。自動的にファイル変換をスケジュールするには、Windows **AT** コマンドを使用します。手動でファイル変換を起動するには、krarloff ロールオフ・プログラムを使用します。最良の結果を得るには、変換を毎日実行するようにスケジュールしてください。

AT コマンドを使用した変換処理

収集したヒストリー・ファイルを区切り文字で区切られたフラット・ファイルに変換する処理をセットアップする場合は、Windows の **AT** コマンドを使用して自動的に処理をスケジュールするか、krarloff ロールオフ・プログラムを実行して手動で処理をスケジュールしてください。ヒストリー・ファイル変換は、Tivoli Enterprise Monitoring Server またはエージェントが実行されているかどうかにかかわらず行われます。

注: ヒストリー・ファイル変換は 24 時間ごとに実行してください。

Windows の AT コマンドを使用したアーカイブ手順:

AT コマンドを使用して Tivoli Enterprise Monitoring Server 上およびリモート管理対象システム上でヒストリカル・データ・ファイルをアーカイブするには、以下の手順を使用します。コマンドの形式を調べるには、MS/DOS コマンド・プロンプトに **AT /?** と入力します。

1. AT コマンドを機能させるには、タスク・スケジューラー・サービスを開始する必要があります。タスク・スケジューラー・サービスを開始するには、「**設定**」 > 「**コントロール パネル**」 > 「**管理ツール**」 > 「**サービス**」を選択します。

   結果: 「サービス」ウィンドウが表示されます。
2. 「サービス」ウィンドウで「**Task Scheduler**」を選択します。サービスの「スタートアップの種類」を「自動」に変更します。「**開始**」をクリックします。

   結果: タスク・スケジューラー・サービスが開始されます。

   AT コマンドを使用してヒストリー・ファイルをアーカイブする例を以下に示します。

   ```
   AT 23:30 /every:M,T,W,Th,F,S,Su c:¥sentinel¥cms¥archive.bat
   ```

この例では、Windows が毎日午後 11:30 に c:¥sentinel¥cms にある archive.bat ファイルを実行します。archive.bat の内容の例を以下に示します。

```
krarloff -o memory.txt wtmemory
krarloff -o physdsk.txt wtphysdsk
krarloff -o process.txt wtprocess
krarloff -o system.txt wtsystem
```

Windows 実行可能ファイルとヒストリカル・データ収集テーブル・ファイルの場所:

このセクションでは、ヒストリカル・データを変換するために必要な Windows プログラムの場所について説明します。

プログラムは以下の場所にあります。

- Tivoli Enterprise Monitoring Server上の *install_dir* ¥cms ディレクトリー
- エージェントがインストールされたリモート管理対象システムの *install_dir* ¥tmaitm6 ディレクトリー。

エージェント・ヒストリー・データをエージェント・コンピューターに保管するように構成していて、しかも、ヒストリー・ファイルの保管を、デフォルトのヒストリー・データ・ファイル保管場所で提供されるストレージ容量よりも多くの容量が提供されるディスクへ行いたい場合は、エージェントの既存の *CTIRA_HIST_DIR* 環境変数を使用して、この保管場所をオーバーライドできます。ヒストリー・データが Tivoli Enterprise Monitoring Server に保管されている場合、この処理は実行できません。

同じ Windows システムで実行されている、同一エージェントの複数インスタンスがある場合、インストーラーは、エージェントに保管されるプロセス・ヒストリー・ファイル用の個別のディレクトリーを作成します。Windows オペレーティング・システム上で実行されているエージェントのデフォルトのロケーションは、C:¥IBM¥ITM¥TMAITM6¥LOGS です。新規ディレクトリーは、TMAITM6¥LOGS ディレクトリー History¥*<3 文字のコンポーネント・コード>(KUM や KUD など)*¥*<指定したマルチプロセス・インスタンスの名前>* の下に作成されます。

例えば、同じ Windows システムに、*UDBINST1* という名前の DB2 モニター・エージェントの 2 番目のインスタンスを構成する場合、C:¥IBM¥ITM¥TMAITM6¥LOGS¥History¥KUD¥UDBINST1 という名前のディレクトリーが作成され、その中にヒストリー・データが保管されます。DB2 エージェント環境変数 CTIRA_HIST_DIR のこのインスタンスは、この値に設定されます。

***Windows* ヒストリカル・データ・テーブル・ファイルの場所:**

次のセクションでは、Windows のヒストリカル・データ・テーブル・ファイルの場所を特定します。

krarloff ロールオフ・プログラムに対し、これらのファイルの場所を知らせる必要があります。

モニター・サーバーおよびエージェントをプロセスまたはサービスとして実行する場合、ヒストリカル・データ・テーブル・ファイルは以下の場所に置かれます。

- モニター・サーバー上の *install_dir* ¥cms ディレクトリー

- 管理対象システム上の *install_dir* ¥tmaitm6¥logs ディレクトリー

IBM i システムでのヒストリー・ファイルの区切り文字で区切られたフラット・ファイルへの変換

ヒストリカル・データ収集構成プログラムで設定したルールを使用して収集したヒストリー・ファイルを、各種の一般アプリケーションでの使用のために、区切り文字で区切られたフラット・ファイルへ変換すると、容易にデータを操作し、レポートおよびグラフを作成できるようになります。手動でファイル変換を起動するには、krarloff ロールオフ・プログラムを使用します。

注: ヒストリー・ファイル変換は 24 時間ごとに実行してください。

IBM i システムに保管されているヒストリカル・データの保管

ユーザー・データは、構成変数 *CTIRA_HIST_DIR* に設定されている IFS ディレクトリー内に保管されます。この変数のデフォルト値は */qibm/userdata/ibm/itm/hist* です。IBM i システムでは、各テーブルごとに、ヒストリカル・データ収集に関連する 2 つのファイルが保管されます。

例えば、システム状況属性のデータを収集している場合は、以下の 2 つのファイルがあります。

- KA4SYSTS: これは、IBM i エージェントによる出力として表示される短期データです。
- KA4SYSTS.hdr: これはメタファイルです。このメタファイルには、単一行の列名が含まれます。

WRKLNK */qibm/userdata/ibm/itm.hist* コマンドを使用すると、両方のファイルの内容を表示させることができます。

IBM i システムでの変換処理

krarloff ロールオフ・プログラムは、Tivoli Enterprise Monitoring Server で実行することも、ヒストリー・ファイルが格納されているディレクトリーから、モニター・エージェントが実行されているディレクトリーで実行することもできます。

krarloff ロールオフ・プログラムは、コマンド・プロンプトに以下のように入力して実行します。

```
call qautomon/krarloff parm (['-h'] ['-g'] ['-x'] ['-d' 'delimiter']
['-m' metafile] ['-r' rename-source-file-to] ['-o' output-file]
{'-s' source-file | source-file )}
```

ここで、[ ] 大括弧はオプションのパラメーターを表し、{ } 中括弧は必須パラメーターを表しています。

エージェントが実行されているディレクトリーで、IBM i システムから krarloff ロールオフ・プログラムを実行する場合は、`qautomon` を、ご使用のエージェントの実行可能ファイルの名前で置き換えてください。例えば、MQ エージェントはコマンド・ストリングで `kmqlib` を使用します。

注: コマンドは 1 行で入力します。

krarloff ロールオフ・プログラムを実行した後

上記のシステム状況の例を使用すると、krarloff ロールオフ・プログラムを実行した後にファイル KA4SYSTS は KA4SYSTSO になります。別のデータの行が使用可能な場合は、新しい KA4SYSTS ファイルが生成されます。

KA4SYSTSM はそのままの状態になります。

KA4SYSTSH は、krarloff ロールオフ・プログラムによる出力として表示されるファイルであり、区切り文字で区切られたフラット・ファイル・フォーマットのデータが含まれています。このファイルは、ファイル転送プログラム (FTP) を使用して IBM i からワークステーションに転送することができます。

UNIX システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換

このトピックでは、UNIX **itmcmd history** スクリプトを使用して、ヒストリー・データ・ファイルに保存されたヒストリカル・データを区切り文字で区切られたフラット・ファイルに変換する方法について説明します。区切り文字で区切られたフラット・ファイルは、さまざまな一般的アプリケーションで使用して、容易にデータを操作し、レポートおよびグラフを作成できます。

ヒストリー・データ変換の概要

次のセクションでは、他のソフトウェア製品で使用するために、ヒストリカル・データ・テーブルを他のファイル・タイプに変換する手順を説明します。

UNIX 環境では、**itmcmd history** スクリプトを使用して、選択した Tivoli Monitoring 短期ヒストリカル・データ・テーブルを他のソフトウェア製品で使用可能な形式に変換するために使用される変換手順のアクティブ化およびカスタマイズを行います。ヒストリカル・データはバイナリー・フォーマットで収集されるため、サード・パーティー製品で使用するには ASCII に変換する必要があります。各短期ファイルは個別に変換します。Tivoli Enterprise Monitoring Server によって収集されたヒストリカル・データは、 Tivoli Enterprise Monitoring Server のホスト側またはレポート・エージェントに置くことができます。 Tivoli Enterprise Monitoring Server またはエージェントがアクティブかどうかにかかわらず、任意の時点で変換を実行できます。

変換は、データが Tivoli Enterprise Monitoring Server とモニター・エージェントのどちらによって書き込まれたかにかかわらず、単一の Tivoli Enterprise Monitoring Server に関連付けられた現行の *install_dir* の下に収集されたすべてのヒストリー・データに適用されます。

以下のコマンドを入力すると、

```
itmcmd history -h
```

コマンド行に、以下の出力が表示されます。

```
itmcmd history [ -h install_dir ] -C [ -L nnn[Kb|Mb] ] [ -t masks*,etc ]
   [ -D delim ] [ -H|+H ] [ -N n ] [ -p cms_name ]
   prod_code itmcmd history -A?itmcmd history [ -h install_dir ]
   -A perday|0 [ -W days ] [ -L nnn[Kb|Mb] ] [ -t masks*,etc ]
   [ -D delim ] [ -H|+H ] [ -N n ]
   [ -i instance|-p cms_name ] [ -x ] prod_code
```

注: 一部のパラメーターは必須です。垂直バー「|」で区切られた項目は同時に指定できないことを示します (例えば、Kb|Mb は Kb と Mb のいずれか一方であり、両方ではないことを示します)。通常、UNIX コマンド行ではパラメーターを 1 行で入力します。

このコマンドで使用するすべてのパラメーターについては、「*IBM Tivoli Monitoring コマンド・リファレンス* 」を参照してください。

ヒストリー・データ変換の実行

itmcmd history スクリプトは、区切り文字で区切られたフラット・ファイルへのヒストリカル・データの変換をスケジュールします。一回限りの変換を実行する手動処理と、自動変換のスケジュールをできるようにする変換スクリプトの両方について、ここで説明します。

構文およびオプションの詳しい説明については、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

変換の実行後、その結果として生成される区切り文字で区切られたフラット・ファイルの名前は、入力ヒストリー・ファイルと同じ名前で、拡張子として 1 桁の数字を付けた名前になります。例えば、入力ヒストリー・ファイル・テーブル名が KOSTABLE の場合、変換後のファイルの名前は KOSTABLE.0 となります。次の変換では KOSTABLE.1 となります (以下同様です)。

1 回限りの変換の実行:

1 回限りの変換処理を実行するには、*install_dir* /bin に移動し、コマンド行に以下のように入力します。

```
./itmcmd history -C prod_code
```

基本的な自動ヒストリー変換のスケジューリング:

UNIX *cron* 機能による自動変換をスケジュールするには、**itmcmd history** を使用します。基本的な自動変換をスケジュールするには、コマンド行に以下のように入力します。

```
./itmcmd history -A n prod_code
```

ここで、*n* は 1 から 24 の数値です。この数値は、1 日にデータ変換プログラムを実行する回数を指定し、最も近い 24 の除数に切り上げられます。製品コードも必要です。

例えば、以下のコマンドは 3 時間ごとにヒストリー変換を実行することを意味します。

```
itmcmd history -A 7 ux
```

ヒストリー変換のカスタマイズ:

itmcmd history スクリプトを使用して、追加のオプションを指定することによってヒストリー収集をさらに詳細にカスタマイズできます。例えば、あらかじめ設定した特定のサイズ制限を超えるファイルを変換するように選択できます。また、特定の曜日にヒストリー変換を実行するように選択することもできます。

すべてのヒストリー変換パラメーターの詳細については、「コマンド・リファレンス」を参照してください。

HP NonStop Kernel システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換

データをデータウェアハウスに収集および格納するオプションを選択した場合は、そのオプションを指定したままこの章で説明するファイル変換プログラムを実行することはできません。これらの変換手順を使用するには、Tivoli Enterprise Portal の「**ヒストリカル収集の構成**」ウィンドウで、「**ウェアハウス**」オプションに「**オフ**」を指定しておく必要があります。

ヒストリー構成プログラムで設定したルールを使用して収集したヒストリー・ファイルを、各種の一般アプリケーションでの使用のために区切り文字で区切られたフラット・ファイルに変換すると、容易にデータを操作し、レポートおよびグラフを作成できるようになります。手動でファイル変換を起動するには、krarloff ロールオフ・プログラムを使用します。最良の結果を得るには、変換を毎日実行するようにスケジュールしてください。

HP NonStop Kernel オペレーティング・システム (旧 Tandem) で実行される IBM Tivoli Monitoring for WebSphere MQ Configuration および IBM Tivoli Monitoring for WebSphere MQ Monitoring に対するサポートが提供されています。ヒストリカル・データ収集に関する IBM Tivoli Monitoring for WebSphere MQ Monitoring 固有の事項について詳しくは、ご使用のバージョンの製品の資料に記載されている『モニター・オプションのカスタマイズ (Customizing Monitoring Options)』トピックを参照してください。

HP NonStop Kernel システムでの変換処理

区切り文字で区切られたフラット・ファイルに収集済みヒストリー・ファイルを変換する処理をセットアップする際、krarloff ロールオフ・プログラムを実行することで手動で処理をスケジュールします。ヒストリー・ファイル変換は 24 時間ごとに実行してください。

HP NonStop Kernel での krarloff ロールオフ・プログラムの使用:

ヒストリー・ファイルは、デフォルトの <$VOL>.CCMQDAT の下にある DATA サブボリュームに保持されます。ただし、ヒストリー・ファイルの場所はモニター・エージェントの開始場所によって変わります。CCMQDAT サブボリュームから STRMQA を使用してモニター・エージェントを開始した場合は、ファイルは CCMQDAT に格納されます。

DATA サブボリュームから krarloff ロールオフ・プログラムを実行するには、以下のように入力します。

RUN <$VOL>.CCMQEXE.KRARLOFF <parameters>

CCMQDAT および CCMQEXE はあくまでデフォルトです。インストール処理中に、これらのファイルに独自の名前を割り当てることもできます。

属性の書式設定:

表示目的のために、一部の属性を書式設定する必要があります。例えば、浮動小数点数では、小数点の左側に出力する有効数字の桁数が指定されます。これらの表示書式設定における考慮事項は、製品の属性ファイルに明記されています。

krarloff ロールオフ・プログラムを使用してヒストリカル・データをテキスト・ファイルへロールオフする際には、属性ファイルで指示されている書式指定子を必要とする属性はすべて、無視されます。ロールオフ後のヒストリー・テキスト・ファイルには未加工の数値のみが出力されます。したがって、45.99% や 45.99 とは表示されずに数値 4599 が表示されます。

z/OS システムでのヒストリー・ファイルの、区切り文字で区切られたフラット・ファイルへの変換

z/OS システムで、手動によるアーカイブ手順によって、または永続データ・ストアの保守手順の一部として、短期のヒストリー・ファイルを区切り文字で区切られたフラット・ファイルに変換することができます。

短期のヒストリー・ファイルは、永続データ・ストア保守手順の一部として、区切り文字で区切られているフラット・ファイルに自動的に変換することも、MODIFY コマンドによって手動で変換することもできます。区切り文字で区切られたフラット・ファイルは、データ操作やレポート作成のアプリケーションで入力として使用できます。詳しくは、*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS 共通計画および構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)を参照してください。

収集して格納したデータは永続データ・ストアから削除されるため、このデータを抽出することはできません。これらの変換手順を使用するには、「ヒストリーの収集の構成」ウィンドウで、「**ウェアハウス間隔**」を「**オフ**」に設定しておく必要があります。「ヒストリーの収集の構成」ウィンドウについて詳しくは、 Tivoli Enterprise Portal オンライン・ヘルプまたは「*Tivoli Enterprise Portal ユーザーズ・ガイド*」のヒストリカル収集の作成 を参照してください。

関連資料:

567 ページの『手動アーカイブの手順』

Tivoli Enterprise Monitoring Server 上、およびリモート管理対象システム上で、ヒストリカル・データ・ファイルの手動変換を行うには、以下の MODIFY コマンドを実行します。

z/OS システムでの自動変換とアーカイブ処理

このセクションには、z/OS システムで行われる自動変換とアーカイブ処理の情報が記されています。

ご使用の IBM Tivoli Monitoring 環境をカスタマイズした場合は、保守のために EXTRACT オプションを指定することができます。EXTRACT オプションを指定すると、ヒストリー・データ・テーブルに格納された情報を変換およびアーカイブする処理が確実に、自動的にスケジュールされます。ユーザー側でそれ以上のアクションを行う必要はありません。アプリケーションがヒストリカル・データをヒストリー・データ・テーブルに書き込むと、永続データ・ストアは、所定のデータ・セットがいっぱいになった時点を検出し、データ・セットをコピーするための

KPDXTRA プロセスを起動し、そのデータ・セットがヒストリカル情報の受信に再度使用できるようになったことを Tivoli Enterprise Monitoring Server に通知します。永続データ・ストアについて詳しくは、「*IBM Tivoli Management Services on z/OS: Tivoli Enterprise Monitoring Server on z/OS の構成*」を参照してください。

変換を自動的にスケジュールする代わりに、ヒストリカル・データ・ファイルを変換するためのコマンドを手動で発行することもできます。

注: KPDXTRA プロセスでは、現在、UTF8 カラムをサポートしていません。

KPDXTRA プログラムを使用したファイルの変換:

変換プログラム KPDXTRA は、保守のために EXTRACT オプションが指定されている場合に永続データ・ストア保守手順によって呼び出されます。このプログラムは、収集されたヒストリカル・データを含んでいるデータ・セットを読み取り、データが収集された各テーブルにそれぞれ 2 つのファイルを書き出します。このデータの処理は、実行中の連続した収集には干渉しません。

この処理は自動的に行われるため、ここでは KPDXTRA プログラムを使用するための概要について説明します。KPDXTRA プログラムについて詳しくは、Tivoli Monitoring 製品とともに配布されるサンプル JCL を参照してください。サンプル JCL は、サンプル・ライブラリー RKANSAM および TKANSAM に含まれるサンプル・ジョブ KPDXTRA プログラムの一部になっています。

属性の書式設定:

表示目的のために、一部の属性を書式設定する必要があります。例えば、浮動小数点数では、小数点の左側に出力する有効数字の桁数が指定されます。これらの表示書式設定における考慮事項は、製品の属性ファイルに明記されています。

KPDXTRA を使用してヒストリカル・データをテキスト・ファイルにロールオフすると、属性ファイルに示された書式指定子を必要とする属性は、すべて無視されます。ロールオフ後のヒストリー・テキスト・ファイルには未加工の数値のみが出力されます。したがって、45.99% や 45.99 とは表示されずに数値 4599 が表示されます。

KPDXTRA の概要:

KPDXTRA プログラムは、保守手順の一部としてバッチ環境で実行されます。このプログラムでは、デフォルトの列セパレーターの変更を許可するパラメーターを取ることができます。このコマンドを実行するための z/OS JCL 構文は以下のとおりです。

```
// EXEC PGM=KPDXTRA,PARM='PREF=dsn-prefix [DELIM=xx] [NOFF]'
```

このジョブを実行するには、いくつかのファイルを割り当てる必要があります。

データ・セットがアクティブでなくても、すべてのデータ・セットは読み取り/書き込み状態で保持されます。そのため、Tivoli Enterprise Monitoring Server が実行中の場合には、データ・セットは使用不可になります。つまり、アクティブなデータ・セットに対してジョブを実行することはできず、また非アクティブなデータ・セットはオフラインにする必要があるということです。

以下のコマンドを実行することによって、データ・セットを Tivoli Enterprise Monitoring Server から削除することができます。

```
F stcname,KPDCMD DELFILE FILE=DSN:datastorefile
```

DELFILE は PDS からファイルを除去するだけで、ファイルの削除はしません。以下の RESUME コマンドを実行すれば、このファイルを PDS GROUP に追加し直すことができます。

```
F stcname,KPDCMD RESUME FILE=DSN:datastorefile
```

アクティブなデータ・ストアに対してユーティリティー・プログラムを実行する必要がある場合は、このコマンドを実行する前に SWITCH コマンドを実行してください。

KPDXTRA に割り振る必要がある DD 名:

KPDXTRA プログラムに割り振る必要がある DD 名の要約を以下に示します。詳しくは、製品とともに配布されるサンプル・ライブラリーにあるサンプル JCL を参照してください。

表 65. 必要な DD 名

DD 名	説明
RKPDOUT	KPDXTRA ログ・メッセージ
RKPDLOG	PDS メッセージ
RKPDIN	構成ツールによってセットアップされるテーブル定義コマンド・ファイル (PDS サブタスクに対する入力)
RKPDIN1	データの抽出元の PDS ファイル
RKPDIN2	DUMMY DD ステートメントとして定義されたオプションの制御ファイル

KPDXTRA パラメーター:

次の表には、KPDXTRA のパラメーターとデフォルト値およびその説明が示されています。

表 66. KPDXTRA パラメーター

パラメーター	デフォルト値	説明
PREF=	なし	必須パラメーター。出力ファイルを書き込む高位修飾子を識別します。
DELIM=	tab	出力ファイルの列の間に使用する分離文字を指定します。デフォルトはタブ文字 X'05' です。他のなんらかの文字を指定するには、その文字を表す、2 バイトの 16 進表現を指定します。例えば、コンマを使用するには DELIM=6B を指定します。
QUOTE	NQUOTE	すべての文字タイプ・フィールドを二重引用符で囲むためのオプション・パラメーター。末尾ブランクは出力から削除されます。KPDXTRA プログラムの出力フォーマットを、分散 krarloff ロールオフ・プログラムによって生成される出力のフォーマットと同じにします。

表 66. KPDXTRA パラメーター (続き)

パラメーター	デフォルト値	説明
NOFF	off	テーブルの形式を含む別個のファイル (ヘッダー・ファイル) を作成するか (ON に設定した場合)、または省略します (OFF に設定した場合)。また、抽出操作の結果として作成される出力データ・ファイルでのヘッダーの有無も制御します。OFF を指定した場合、ヘッダー・ファイルは作成されませんが、データ・ファイルの先頭行としてヘッダー情報が組み込まれます。このヘッダー情報は、抽出したデータの形式を示します。

KPDXTRA プログラム・メッセージ:

保守手順を実行して作成された RKPDOUT sysout ログには以下のメッセージがあります。

```
Persistent datastore Extract program KPDXTRA - Version V130.00
Using output file name prefix: CCCHIST.PDSGROUP
The following characters are used to delimit output file tokens:
Column values in data file.............:  0x05
 Parenthesized list items in format file:  0x6b
Note: Input control file not found; all persistent data is extracted.

Table(s) defined in persistent datastore file  CCCHIST.PDSGROUP.PDS#1:
```

アプリケーション名	テーブル名	抽出の状況
PDSSTATS	PDSCOMM	除外
PDSSTATS	PDSDEMO	包含
PDSSTATS	PDSLOG	包含
PDSSTATS	TABSTATS	包含

```
Checking availability of data in data store file:
  No data found for Appl: PDSSTATS Table: PDSDEMO  . Table excluded.Table excluded.
  No data found for Appl: PDSSTATS Table: TABSTATS . Table excluded.Table excluded.
The following 1 table(s) are extracted:
```

アプリケーション名	テーブル名	行数	最も古い行	最新の行
PDSSTATS	PDSLOG	431	1997/01/10 05:51:20	1997/02/04 02:17:54

```
Starting extract operation.
Starting extract of PDSSTATS.PDSLOG.
The output data file, CCCHIST.PDSGROUP.D70204.PDSLOG, does not exist; it is created.
The output format file, CCCHIST.PDSGROUP.F70204.PDSLOG, does not exist;
  it is created.
Extract completed for PDSSTATS.PDSLOG. 431 data rows retrieved, 431 written.
Extract operation completed.
```

z/OS 実行可能ファイルとヒストリカル・データ・テーブル・ファイルの場所

次のセクションでは、z/OS 実行可能ファイルおよびヒストリカル・データ・テーブル・ファイルの場所を特定します。

z/OS 実行可能ファイルは、*&rhilev.&rte.*RKANMOD または *&thilev.*TKANMOD ライブラリーにあります。ここで、各項目は以下のとおりです。

- *&rhilev* は、ランタイム環境の高位修飾子です。
- *&rte* は、ランタイム環境の名前です。
- *&thilev* は、SMP/E によってインストールされたターゲット・ライブラリーの高位修飾子です。

抽出プログラムによって作成された z/OS ヒストリカル・データ・ファイルは以下のライブラリー構造に置かれます。

- *&hilev.&midlev.&dsnlolev.tablename.*D
- *&hilev.&midlev.&dsnlolev.tablename.*H

手動アーカイブの手順

Tivoli Enterprise Monitoring Server 上、およびリモート管理対象システム上で、ヒストリカル・データ・ファイルの手動変換を行うには、以下の MODIFY コマンドを実行します。

```
F stcname,KPDCMD SWITCH GROUP=cccccccc EXTRACT
```

それぞれの説明:

- *stcname* は、Tivoli Enterprise Monitoring Server またはエージェントのいずれかを実行している開始済みタスクの名前を示します。
- *cccccccc* は、永続データ・ストアの割り振りに関連したグループ名を示します。*cccccccc* の値は、インストールした製品によって異なります。標準のグループ名は GENHIST です。

このコマンドを実行すると、グループ ID に関連したテーブルのみが抽出されます。複数の製品がインストールされている場合は、それぞれの製品を別個の SWITCH コマンドによって制御できます。

インストール・スケジューリング機能または自動化製品を使用すると、この切り替えを自動化できます。

また、Tivoli Enterprise Portal の拡張自動化機能を使用して SWITCH コマンドを実行することもできます。これを行うには、true になったときにアクションとして SWITCH コマンドを実行するシチュエーションを定義します。

永続データ・ストアの保守

PDS を z/OS Tivoli Enterprise Monitoring Server またはエージェント上で実行するオプションがあります。この機能により、記録されたデータの索引を保守しながら、1 日 24 時間対応で表形式の関係データを記録および検索できます。

永続データ・ストアの構成手順については、*Tivoli Enterprise Monitoring Server on z/OS の構成* の 『永続データ・ストアの構成』 を参照してください。

第 18 章 Tivoli Common Reporting

この『Tivoli Common Reporting』のトピックには、Tivoli Enterprise Portal 上で実行され、レポート生成のためのヒストリカル・データのソースとして Tivoli Data Warehouse を使用する製品に固有の情報が含まれています。この情報は、Tivoli Common Reporting をセットアップし、ユーザー用のレポート・パッケージをインストールする管理者を対象としています。

Tivoli Common Reportingの概要

Tivoli Common Reporting ツールは、Tivoli 製品のユーザーが使用できるレポート機能です。Tivoli Common Reporting を使用すると、管理対象環境の重要なトレンドを整合的かつ総合的に収集、分析、およびレポートできます。

個々のリソース、複数リソース、およびエンタープライズ・リソースのモニター用に、一連の事前定義レポートが Tivoli Monitoring OS エージェントおよび他の製品で提供されています。

Tivoli Common Reporting の利用者

- TCP/IP に関する問題のトラブルシューティングするネットワーク・システム・プログラマー
- アプリケーション・アナリストまたはドキュメンテーション・マネージャー
- サービス・レベル・アグリーメントを検証する IT マネージャーまたはサービス・レベル・アドバイザー
- キャパシティー・プランナー
- サービス・マネージャー
- システム管理者
- ストレージ管理者

Tivoli Common Reporting コンポーネント

Tivoli Common Reporting は以下の複数のコンポーネントで構成されています。

- レポート設計、レポート、およびサポートするリソースを格納し、編成するためのデータ・ストア。データ・ストアは、Tivoli Common Reporting インフラストラクチャー内の場所であり、レポートに関連したすべてのファイルとレポートが管理および保守されています。
- レポート・パラメーターおよびその他のレポート・プロパティーを指定し、書式設定されたレポートを生成し、レポートを表示する Web ベースのユーザー・インターフェース。
- データ・ストアのオブジェクトを操作し、追加の管理機能を実行するためのコマンド行インターフェース。

- レポート・パッケージ。レポート、ドキュメンテーション、グラフィックス、およびダイナミック・リンク・ライブラリーを含むアーカイブ・ファイル。
  - Tivoli Common Reporting 製品では、サンプルのレポート・セットが提供されています。その他のセットは、インポート機能を使用してダウンロードして、インストールできます。
  - Tivoli Monitoring エージェント・レポートの Cognos® バージョン用の CD があります。
  - 一部のモニター・エージェント用の BIRT レポート・パッケージが、Tivoli Monitoring Agent インストール・メディア上の REPORTS/k*pc* ディレクトリーに zip ファイルとして入っています。ここで、*pc* は 2 文字の製品コードです。レポート・パッケージは、IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary) 上にいくつかの Tivoli Monitoring 製品別に用意されています。IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary) で「Tivoli Common Reporting」を検索すると、レポート・パッケージが見つかります。

  IBM developerWorks® Tivoli Common Reporting space には、他の IBM 以外のユーザーによって生成されたその他のレポート・パッケージ、ビジネス・レポート・テンプレート、および「*Tivoli Common Reporting 開発およびスタイル・ガイド (Tivoli Common Reporting: Development and Style Guide)*」があります。
- レポートを変更したり、独自のレポートを作成するために使用するオープン・ソース Eclipse BIRT Report Designer。このツールは、IBM developerWorks Tivoli Common Reporting space からダウンロードできます。

Tivoli Common Reporting についての詳細 (Tivoli Common Reporting のインストールと管理、およびレポートの作成方法など) については、IBM Tivoli Common Reporting インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html)を参照してください。

Tivoli Common Reporting の前提条件

Tivoli Monitoring 製品で Tivoli Common Reporting パッケージをインストールおよび実行するための前提条件コンポーネントがあります。

レポートを使用するには、以下のコンポーネントが必要です。

- IBM Tivoli Monitoring
- Tivoli Common Reporting
  - IBM Tivoli Monitoring バージョン 6.3 には、Tivoli Common Reporting 3.1 (Jazz for Service Management のコンポーネント) が含まれています。
  - IBM Tivoli Monitoring バージョン 6.2.3 には、Tivoli Common Reporting 2.1.1 が含まれています。
  - IBM Tivoli Monitoring 6.2 フィックスパック 2 には、Tivoli Common Reporting for Asset および Performance Management バージョン 1.3 が含まれ

ています。このバージョンの Tivoli Common Reporting には、Cognos Business Intelligence and Reporting バージョン 8.4 が含まれています。

IBM Tivoli Monitoring バージョン 6.3 オペレーティング・システム・エージェント向けのレポートは Tivoli Common Reporting 3.1 または 2.1.1 と共にインストールできます。その他のモニター・エージェントについては、該当エージェントのユーザーズ・ガイドを参照し、サポートされている Tivoli Common Reporting のバージョンを確認してください。

まだインストールしていない場合は、IBM Tivoli Common Reporting インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html)に掲載されている情報を使用して、Tivoli Common Reporting をインストールし、構成します。

Tivoli Common Reporting が実行されていることを確認するには、`http://computer_name:port_number/ibm/console/` に進みます。 http と HTTPS のデフォルトのポート番号は、それぞれ 16310 と 16311 です。サーバーへのデフォルトのパスは、`/ibm/console` です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。

既に以前のバージョンの Tivoli Common Reporting がインストールされており、異なるディレクトリーに新しいバージョンをインストールした場合、競合を避けるために異なるポートが割り当てられています。

- レポート・パッケージ

  製品に、解凍する必要のある別個のレポート・パッケージが含まれている場合があります。説明については、製品のユーザーズ・ガイドを参照してください。これは、インストールの一環として解凍される OS エージェント・レポートには当てはまりません。

- IBM Tivoli Monitoring バージョン 6.2 フィックスパック 1 以降でサポートされているデータベース・マネージャー製品に保管されているヒストリカル・データ
- このガイドの BIRT レポートは、ヒストリカル・レポートであり、Tivoli Data Warehouse 6.2 フィックスパック 1 以降で収集されたデータに対してレポートを作成します。サポートされているデータベースについては、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『Tivoli Data Warehouse でサポートされているデータベース』を参照してください。
- IBM Tivoli Monitoring エージェント・レポート Cognos パッケージについては、モニター・エージェントのユーザーズ・ガイドを参照してください。各レポートについての説明が記載されています。特に、各レポートに必要なビューが記載されています。これらのビューがないと、レポートは機能しない場合があります。必要なビューが存在することを確認するには、Tivoli Data Warehouse に対して次の照会を実行します。
  - DB2

    ```
    select distinct "VIEWNAME" from SYSCAT.VIEWS where "VIEWNAME" like '%V'
    ```

  - Oracle

    ```
    select distinct "VIEW_NAME" from USER_VIEWS where "VIEW_NAME" like '%V'
    ```

  - MS SQL Server

    ```
    select distinct "NAME" from SYS.VIEWS where "NAME" like '%V'
    ```

注:

1. Tivoli Common Reporting for Asset and Performance Management 内では、BIRT と Cognos の両方のレポート・エンジンが共存できます。
2. 必須ではありませんが、Eclipse BIRT Report Designer バージョン 2.2.1 をインストールすることができます。Eclipse BIRT Report Designer は、「*Tivoli Common Reporting 開発およびスタイル・ガイド (Tivoli Common Reporting: Development and Style Guide)*」と併用することにより、レポート・テンプレートを編集したり、新しいレポートを作成することができます。

BIRT Report Designer を実行するためのソフトウェア要件や BIRT Report Designer のダウンロード方法については、Eclipse Web サイトの「ビジネス・インテリジェンスおよびレポート作成ツール (Business Intelligence and Reporting Tools)」(英語) または IBM developerWorks Tivoli Common Reporting space を参照してください。開発およびスタイル・ガイドは、IBM Tivoli Common Reporting インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr.doc_211/ic-home.html)からダウンロードしてください。

以前のバージョンからのアップグレード

BIRT OS モニター・エージェントのレポートは、引き続き IBM Integrated Service Management Library (旧 OPAL) 上で配布されます。以前 OPAL で配布され、Tivoli Common Reporting V1.1.1 で実行されていたその他のモニター・エージェントの場合、IBM Integrated Service Management Library からダウンロードするか製品メディアから入手したレポート・パッケージを再インストールせずに、Tivoli Common Reporting をバージョン 1.3 以降にアップグレードできます。

BIRT レポート・パッケージは、IBM Integrated Service Management Library (http://www.ibm.com/software/brandcatalog/ismlibrary) 上に基本 OS モニター・エージェント別に用意されています。IBM Tivoli Monitoring エージェント・レポートの Cognos バージョン用の DVD が用意されています。 Tivoli Management Services インフラストラクチャー・バージョンに対応したパッケージをダウンロードしてください。

Tivoli Common Reporting バージョン 1.1.1 は、Integrated Solutions Console 上で実行され、Tivoli Common Reporting バージョン 1.2 またはそれ以降とは別の場所にインストールされます。バージョン 1.2 は、Dashboard Application Services Hub 上で実行され、インフラストラクチャー・サポートに関してこの製品に依存しています。バージョン 1.1.1 および 1.3 は同一のコンピューター上で共存することができます。また、IBM Integrated Service Management Library からダウンロードしたレポートをバージョン 1.3 にマイグレーションすることができます。レポート・パッケージを再インストールする必要はありません。バージョン 1.1.1 からバージョン 1.3 にレポートをマイグレーションするには、以下の 2 つのオプションがあります。

- Tivoli Common Reporting バージョン 1.3 のインストール時に、バージョン 1.1.1 がインストールされている場合にはインストーラー・プログラムによってそれが検出され、これらのレポートをマイグレーションするかどうか尋ねられます。「**はい**」と指定します。

注: IBM Integrated Service Management Library からダウンロードしたレポート・パッケージを Tivoli Common Reporting バージョン 1.3 にマイグレーションした場合は、以前にインストールされたレポートが上書きされていることを確認してください。レポート・パッケージをインポートする場合は、「**インポート・レポート・パッケージ**」 テキスト・ボックスの 「**拡張オプション**」 をクリックし、「**上書き (Overwrite)**」チェック・ボックスを選択します。

- レポート・パッケージを手動でマイグレーションします。

これらのオプションの両方について、バージョン 1.3 の「*Tivoli Common Reporting ユーザーズ・ガイド*」で説明されています。

注: Tivoli Common Reporting では、セキュリティーが強化され、レポートのハイパーテキスト・リンクへのセキュリティー・ストリングの割り当てが可能になりました。「*Tivoli Common Reporting ユーザーズ・ガイド*」では、セキュリティー・セットを入力する手順を説明しています。

制限

このセクションでは、Tivoli Common Reporting で生成されるレポートの制限について説明します。

- Tivoli Monitoring エージェントの Cognos レポートは、Tivoli Common Reporting で「TDW」というデータ接続に接続するようにコーディングされています。
- Tivoli Monitoring エージェント・レポートは、Tivoli Data Warehouse に対して実行されます。DB2 では列の長さが 30 文字に制限されます。Tivoli Data Warehouse は列ヘッダーとして属性グループ名を使用しているため、DB2 Tivoli Data Warehouse では、30 文字を超える属性名は、内部列名、つまり属性の短縮形を使用したデータベース名 (CPU Utilization や Disk Utilization ではなく、CPU_UTIL または DISK_UTIL など) に置き換えられます。
- 長期間にわたる属性または処理が集中する属性に対応するレポートでは、SQL の算術オーバーフローが発生する可能性があります。
- 一部のレポートは、Tivoli Data Warehouse Summarization and Pruning agent のオプションであるシフト時間の定義をサポートしていません。顧客はシフト時間サポートを使用して、収集データにピーク期間またはオフピーク期間のいずれかのフラグを設定できます。ただし、データが収集されたのがピーク期間であるかオフピーク期間であるかにかかわらず、一部のレポートには、顧客が選択したレポートの開始時刻から終了時刻までに収集されたすべてのデータが含まれます。537 ページの『Summarization and Pruning agentについて』 および 544 ページの『グローバル構成設定の変更』 を参照してください。
- Summarization and Pruning agentのシフト時間構成が変更された場合は、直近の構成がレポートに使用されます。複数の構成にまたがっている可用性レポートに日付範囲を指定すると、誤った可用性メトリックになる場合があります。例えば、ピーク時間を編集して 1 時間追加すると、ピーク時間とオフピーク時間の要約は、エージェントが再構成される前と後では異なってきます。再構成の前または後の時刻範囲のみが有効です。2 つの構成にまたがる時刻範囲を指定するのは避けてください。

ヒストリカル・レポート機能が使用可能であることを確認

レポートの実行の準備をする最初のステップは、ヒストリカル・レポート機能が使用可能であることを確認することです。

このタスクについて

レポートは、Tivoli Data Warehouse 内に保管されている長期のヒストリカル・データに対して実行されます。レポートを実行する前に、必要なコンポーネントがインストールされ、ヒストリカル・データ収集が構成済みであることを確認します。

手順

1. Tivoli Data Warehouse およびウェアハウス・エージェント (Warehouse Proxy agentおよびSummarization and Pruning agent) をインストールして構成します。*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)を参照してください。
2. Tivoli Enterprise Portal でヒストリカル収集構成機能を使用してヒストリカル収集をセットアップします。ヒストリカル収集の構成を参照してください。

   z/OS ベースのモニター・エージェントの場合は、構成ツールを使用して永続データ・ストアを構成します。「*Tivoli Enterprise Monitoring Server on z/OS の構成*」の『永続データ・ストアの構成』を参照してください。また、*IBM Tivoli OMEGAMON XE and Tivoli Management Services on z/OS 共通計画および構成* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.omegamon_share.doc_6.3/zcommonconfig/zcommonconfig.htm)も参照してください。
3. オプションで、Tivoli Data Warehouse で要約データへのアクセスを使用可能にします。 レポートの要約データの使用は、表示レポートの分析を単純化し、レポート生成のパフォーマンスを向上できます。

次のタスク

Tivoli Data Warehouse、ウェアハウス・エージェント、およびデータ収集を開始した後、Tivoli Data Warehouse が、要求されたレポート期間のヒストリカル・データや要約レポート用に適切な量のデータを保存するのに十分な期間をとってください。例えば、月次レポートが必要な場合は、少なくとも 1 カ月分の保管データが必要です。

ディメンション表の作成および保守

Tivoli Common Reporting 用に Tivoli Data Warehouse を準備する作業として、ディメンション表の作成があります。ディメンション表は、Cognos レポートを実行し、データ・モデルを使用するのに必要です。

ディメンション表を作成および保守するには、2 とおりの方法があります。

- 575 ページの『ディメンション表を保守するためのSummarization and Pruning agentの使用』

IBM Tivoli Monitoring V6.3 以降では、Summarization and Pruning agentを使用して表を作成できます。

または

- 581 ページの『手動によるディメンション表の作成および保守』

IBM Tivoli Monitoring V6.3 より古いバージョンでは、ディメンション表を手動で作成および保守する必要があります。引き続きディメンションの更新を手動で行う場合には、この方法を使用できます。

開始前のヒストリカル・データ収集の構成

最初に、ヒストリカル・データ収集を構成する必要があります。

リソース・ディメンション表を作成するには、レポートを取得するオペレーティング・システムに応じて、以下の 1 つ以上の属性グループに対してヒストリカル・データ収集を構成します。

Type	属性グループ	テーブル	要約
Linux	Linux IP アドレス	Linux_IP_Address	毎日
UNIX	UNIX IP アドレス	UNIX_IP_Address	毎日
Windows	コンピューター情報	NT_Computer_Information	毎日
Warehouse の要約およびプルーニング・エージェント	KSY 要約の構成	KSY_Summarization_Config_DV	毎日
IBM i	その他	i5OS_Miscellaneous	毎日

ヒストリカル・データ収集は、Tivoli Enterprise Portal またはコマンド行インターフェースで構成できます。以下の例は、NT コンピューター情報のローカル・ヒストリカル収集がどのように CLI から作成および配布されたかを示しています。

```
tacmd login -s MyComputer -u MyUser -p MyPassword
tacmd tepslogin -s localhost -u sysadmin
tacmd histconfiguregroups -t knt -o "NT Computer Information" -m -d YQMWDH
  -p Y=2y,Q=2y,M=1y,W=1y,D=6m,H=14d,R=7d
tacmd histcreatecollection -t knt -o "NT Computer Information"
  -a "ComputerInformation" -c 15m -i 15m -l TEMA -e
 "Needed for resource dimension table for TCR."
tacmd histstartcollection -n TEMS_NAME -t "knt" -o "NT Computer Information"
```

警告: サイトにおいて IBM Tivoli Monitoring データ・モデルまたはオペレーティング・システム・エージェント・レポートのいずれかが変更されると、更新されたデータ・モデルおよびレポートはサポートされなくなります。また、保守を Tivoli Monitoring に適用したり後続のリリースに移行したりすると、これらの更新は失われる場合があります。

ディメンション表を保守するためのSummarization and Pruning agentの使用

Tivoli Common Reportingに必要なディメンション表を保守するように Summarization and Pruning agentを構成できます。

ディメンション表には以下の 2 つのグループがあります。

共有ディメンション表

共有ディメンション表 TIME_DIMENSION、MONTH_LOOKUP、および WEEKDAY_LOOKUP は、Tivoli Common Reporting で必要です。

これらの表は、 578 ページの『スキーマ・パブリケーション・ツールを使用したディメンション表の作成』タスクでスキーマ・パブリケーション・ツールを使用して作成および更新されます。

リソース・ディメンション表

リソース・ディメンション表は MANAGEDSYSTEM、MANAGEDSYSTEMLIST、および MANAGEDSYSTEMLISTMEMBERS です。

これらの表は以下の 2 つの方法のいずれかで作成されます。

- Summarization and Pruning agentが停止している間に、 578 ページの『スキーマ・パブリケーション・ツールを使用したディメンション表の作成』タスクでスキーマ・パブリケーション・ツールを使用する。

  または

- 『ディメンション表を保守するためのSummarization and Pruning agentの構成』タスクでSummarization and Pruning agentを構成した後で、Summarization and Pruning agentを始動する。

ベスト・プラクティスを以下に示します。

1. 『ディメンション表を保守するためのSummarization and Pruning agentの構成』のステップを実行します。構成後にSummarization and Pruning agentを再始動しないでください。
2. 578 ページの『スキーマ・パブリケーション・ツールを使用したディメンション表の作成』のステップに従い、スキーマ・パブリケーション・ツールを更新モードで使用して、共有ディメンション表とリソース・ディメンション表の両方を作成するために必要な DDL を生成し、生成されたスクリプトを実行します。
3. Summarization and Pruning agentを再始動します。

重要: Summarization and Pruning agentをオートノマス・モードで実行している場合は (KSY_AUTONOMOUS=YES)、Summarization and Pruning agentにより MANAGEDSYSTEMLIST 表と MANAGEDSYSTEMLISTMEMBERS 表を保守または作成することはできません。

ディメンション表を保守するためのSummarization and Pruning agentの構成

ディメンションを保守するようにSummarization and Pruning agentを構成します。

始める前に

- IBM Tivoli Monitoring V6.3 以降をインストールする必要があります。
- レポート実行前にこのタスクを完了します。
- この手順では、WAREHOUSETCRCONTROL 表の情報が MANAGEDSYSTEM 表に取り込まれます。WAREHOUSETCRCONTROL 表はSummarization and Pruning agentを初めて開始するとき、またはスキーマ・パブリケーション・ツールを使用

して作成するとき (578 ページの『スキーマ・パブリケーション・ツールを使用したディメンション表の作成』を参照) の、いずれか最初に行われた操作で作成されます。

WAREHOUSETCRCONTROL 表への項目の取り込みは、各モニター・エージェントにより行われます。モニター・エージェントによる項目の追加では、スクリプトを使用する場合と手動で操作される場合があります。詳しくは、ご使用のエージェントのユーザーズ・ガイドを参照してください。

例えば OS エージェント・レポート・パッケージの場合、インストール・ステップで WAREHOUSETCRCONTROL 表にデータが取り込まれます。つまり、このタスクを完了する前に OS エージェント・レポート・パッケージをインストールする必要があります。

このタスクについて

このタスクでは、TIME_DIMENSION 表、MONTH_LOOKUP 表、WEEKDAY_LOOKUP 表、および MANAGEDSYSTEM 表を保守するように Summarization and Pruning agentを構成します。表が既に存在している場合は、Summarization and Pruning agent により表に必要な列がすべて含まれていることが確認され、欠落している列と索引があれば追加されます。表データを既にカスタマイズしている場合は、カスタマイズしたデータが保持されます。

手順

1. Summarization and Pruning agent 環境変数ファイルを開きます。

   Windows

   Summarization and Pruning agentがインストールされているコンピューターの「Tivoli Enterprise Monitoring Services の管理」アプリケーションでエージェントを右クリックし、「**拡張**」→「**ENV ファイルの編集**」を選択します。

   Linux UNIX

   Summarization and Pruning agent がインストールされているコンピューターで、*install_dir* /configディレクトリーに移動します。

   テキスト・エディターで sy.ini ファイルを開きます。
2. 以下の環境変数を構成します。
   - KSY_TRAM_ENABLE=Y

     フィーチャーの機能を制御します。デフォルト値は N です。
   - KSY_TRAM_TD_GRANULARITY=*minutes*

     データが TIME_DIMENSION 表に挿入される間隔 (分数) です。最小値は 1 です。デフォルト値は 5 です。
   - KSY_TRAM_TD_INITIAL_LOAD=*months*

     TIME_DIMENSION 表が空であるかまたは初めて作成された場合に、この表にロードするデータの量 (月数) です。最小値は 1 です。デフォルト値は 24 カ月です。
3. ファイルを保存します。

4. Summarization and Pruning agentを再始動します。

タスクの結果

ディメンション表はSummarization and Pruning agentによって保守されます。

Tivoli Data Warehouse に以下の表が作成されます。これにより、管理対象システムのグループに基づいてレポートおよび照会を作成できるようになります。

- MANAGEDSYSTEMLIST: モニター・サーバーの管理対象システム・グループの名前、製品、および説明 (デフォルトでは空白、カスタマイズ可能) が含まれています。
- MANAGEDSYSTEMLISTMEMBERS: MANAGEDSYSTEMLIST 表で定義されている特定の管理対象システム・グループのメンバーである管理対象システムが含まれています。

Summarization and Pruning agentは新しいシステムのみを MANAGEDSYSTEM 表に追加します。つまり、カスタマイズしたデータがある場合、それらは保持されます。

次のタスク

表の内容を確認し、翌月のデータが含まれていることを確認します。Summarization and Pruning agentでは、現在の月の翌月のデータが保持されます。

スキーマ・パブリケーション・ツールを使用したディメンション表の作成

スキーマ・パブリケーション・ツールを使用して、Tivoli Common Reporting と IBM Tivoli Monitoring に必要なディメンション表を作成します。

このタスクで作成される共有ディメンション表は TIME_DIMENSION、MONTH_LOOKUP、および WEEKDAY_LOOKUP です。このタスクでは、リソース・ディメンション表 MANAGEDSYSTEM、MANAGEDSYSTEMLIST、および MANAGEDSYSTEMLISTMEMBERS も作成されます。

始める前に

- IBM Tivoli Monitoring V6.3 以降をインストールする必要があります。
- 各エージェントで、MANAGEDSYSTEM 表で必要なヒストリカル収集と要約が有効になっていることを確認します。詳しくは、575 ページの『開始前のヒストリカル・データ収集の構成』およびエージェントの資料を参照してください。
- レポート実行前にこのタスクを完了します。
- データベース管理者である必要があります。
- Oracle ユーザーの場合、以下の要件に対応している必要があります。
  - JDBC ドライバーのバージョンが 10.2.3.0 以降である必要があります。
  - IBM_TRAM ユーザーを作成する必要があります。ユーザーを作成するには、Oracle Enterprise Manager ユーザー・インターフェースまたは以下の SQL Plus コマンドを使用します。

```
CREATE USER IBM_TRAM IDENTIFIED BY <password> [DEFAULT TABLESPACE
<deftbsp> TEMPORARY TABLESPACE <temptbsp>];
GRANT CONNECT, CREATE TABLE, CREATE SYNONYM, CREATE VIEW, CREATE
PROCEDURE TO IBM_TRAM;
GRANT UNLIMITED TABLESPACE TO IBM_TRAM;
GRANT CREATE SEQUENCE TO ITM_USER;
```

ここで、

<password> は IBM_TRAM ユーザーのパスワードです

<deftbsp> は IBM_TRAM ユーザーのデフォルトの表スペースです

<temptbsp> は IBM_TRAM ユーザーの一時表スペースです

[] はステートメントのオプション部分を示します。

- Microsoft SQL Server の場合、スキーマを作成する必要があります。Microsoft SQL Management Studio または以下の SQL ステートメントを使用してスキーマを作成できます。

```
CREATE SCHEMA IBM_TRAM;
```

このタスクについて

以下のスキーマ・パブリケーション・ツール・モードがサポートされています。

- インストール済み: すべての Tivoli Reporting and Analytics Model (TRAM) 表の DDL を生成し、WAREHOUSEID 表にデータを取り込みます。このモードでは、必要な関数、ビュー、および索引のステートメントも作成されます。
- 構成済み: すべての TRAM 表の DDL を生成し、ヒストリカル収集と要約が構成されている属性グループのみの WAREHOUSEID 表にデータを取り込みます。このモードでは、必要な関数、ビュー、および索引のステートメントも作成されます。
- 更新済み: このモードはベスト・プラクティスです。 TRAM 表の DDL を生成し、WAREHOUSEID 表にデータを取り込みます。データを取り込む際に、現在のヒストリカル収集および要約の構成が分析され、存在していない属性と属性グループが追加されます。このモードでは、必要な関数、ビュー、および索引のステートメントも作成されます。

スキーマ・パブリケーション・ツールの実行に関する追加情報については、「*IBM Tivoli Monitoring インストールおよび設定ガイド*の『データウェアハウス・テーブル用 SQL の生成』」を参照してください。

重要: 以下の手順では更新モードを使用します。

手順

1. 応答ファイルを開きます。

   Windows *install_dir* ¥TMAITM6¥tdwschema.rsp

   Linux UNIX *install_dir /arch*/bin/tdwschema.rsp

2. 以下の環境変数を構成します。
   - KSY_PRODUCT_SELECT = updated
   - KSY_TABLE_FILTER = TIME_DIMENSION,MONTH_LOOKUP,WEEKDAY_LOOKUP

- KSY_SQL_OUTPUT_FILE_PATH = *SQL 出力のオプション・ファイル・パス*

3. Tivoli Enterprise Portal Server が始動していることを確認します。
4. 以下のスキーマ・パブリケーション・ツールのスクリプトを実行します。

   Windows: `tdwschema -rspfile tdwschema.rsp`

   Linux UNIX: `tdwschema.sh -rspfile tdwschema.rsp`

   応答ファイルで指定した製品用の SQL ファイルが生成され、KSY_SQL_OUTPUT_FILE_PATH キーワードで指定されたディレクトリー、または出力ディレクトリーが指定されていない場合は現行作業ディレクトリーに書き込まれます。
5. 以下のスクリプトをリストされている順に実行します。
   - Oracle または Microsoft SQL Server を使用している場合は、TRAM ユーザー IBM_TRAM としてスクリプトを実行します。
   - DB2 for Linux, UNIX, and Windows または DB2 for z/OS を使用している場合は、Tivoli Data Warehouse データベースに対する管理者権限を備えたユーザーとしてスクリプトを実行します。

   ```
   tdw_schema_table.sql
   tdw_schema_index.sql
   tdw_schema_view.sql
   tdw_schema_function.sql
   tdw_schema_insert.sql
   ```

   DB2 の場合の例:

   ```
   db2 -tvf tdw_schema_table.sql
   db2 -tvf tdw_schema_index.sql
   db2 -tvf tdw_schema_view.sql
   db2 -td# -f tdw_schema_function.sql
   db2 -tvf tdw_schema_insert.sql
   ```

   MSSQL の場合の例:

   ```
   osql -S <SQL server> -U <user ID> -P <password> -d <database name>
    -I -i tdw_schema_table.sql
   osql -S <SQL server> -U <user ID> -P <password> -d <database name>
    -I -i tdw_schema_index.sql
   osql -S <SQL server> -U <user ID> -P <password> -d <database name>
    -I -i tdw_schema_view.sql
   osql -S <SQL server> -U <user ID> -P <password> -d <database name>
    -I -i tdw_schema_function.sql
   osql -S <SQL server> -U <user ID> -P <password> -d <database name>
    -I -i tdw_schema_insert.sql
   ```

   Oracle の場合の例:

   ```
   sqlplus <user ID>/<password>@<TDW Database SID> @tdw_schema_table.sql
   sqlplus <user ID>/<password>@<TDW Database SID> @tdw_schema_index.sql
   sqlplus <user ID>/<password>@<TDW Database SID> @tdw_schema_view.sql
   sqlplus <user ID>/<password>@<TDW Database SID> @tdw_schema_function.sql
   sqlplus <user ID>/<password>@<TDW Database SID> @tdw_schema_insert.sql
   ```

   重要: これらのスクリプトはリストされている順に実行する必要があります。このように実行しないと失敗します。

タスクの結果

ディメンション表が作成されました。

次のタスク

tdw_schema_insert.sql スクリプトの実行中にエラーを受け取った場合は、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。

手動によるディメンション表の作成および保守

ディメンション表を作成するには、データベース・スクリプトを使用してディメンション表を手動で作成および保守します。

共有ディメンション・テーブルの作成と時間ディメンション・テーブルへのデータの取り込み

Tivoli Common Reporting 用に Tivoli Data Warehouse を準備する作業として、IBM_TRAM ディメンションの作成があります。これは、Cognos レポートを実行し、データ・モデルを使用するのに必要です。

このタスクについて

この手順で、以下のディメンション・テーブルが作成されます。

IBM_TRAM スキーマ
TRAM は「Tivoli Reporting and Analytics Model」の略であり、Tivoli 製品で使用される共通データ・モデルです。

警告: サイトにおいて IBM Tivoli Monitoring データ・モデルまたはオペレーティング・システム・エージェント・レポートのいずれかが変更されると、更新されたデータ・モデルおよびレポートはサポートされなくなります。また、保守を Tivoli Monitoring に適用したり後続のリリースに移行したりするときに、これらの更新は失われる場合があります。

TIME_DIMENSION 表
時間ディメンション・データの年数および指定した分数への細分度を含むテーブルです。このテーブルの各行は、時間、平日、日、四半期など、それに関連したさまざまなディメンションを持つ、固有の分キーです。

MONTH_LOOKUP テーブル
時間ディメンションの月の名前をグローバル化します。

WEEKDAY_LOOKUP テーブル
時間ディメンションの週日の名前をグローバル化します。

その他のディメンション
ComputerSystem、BusinessService、および SiteInfo など、Tivoli Common Data Model に準拠した他のディメンション。

db_scripts ディレクトリーの下に解凍されたレポート・パッケージに含まれているデータベース・スクリプトが必要になります。

インストーラーとともにレポートが配布されている場合は、レポート・インストーラーによって以下の手動の手順を自動的に処理できます。自動化 TRAM の作成については、エージェント固有のユーザーズ・ガイドを参照してください。

複数のレポート・パッケージをインストールする際にも、以下のステップを実行する必要があるのは一度だけです。複数のレポート・パッケージをインストールする際は、同じ TIME_DIMENSION テーブルが使用されます細分度や、開始時刻および終了時刻をリセットしたい場合は、この手順を繰り返してください。

手順

- **IBM DB2**
  1. レポート・パッケージ内のデータベース・スクリプト (.db2 ファイル) を、Tivoli Data Warehouse に対してそれらのスクリプトを実行できる場所にコピーします。 スクリプトは、レポート・パッケージが解凍されたディレクトリーの db_scripts ブランチに入っています。
  2. db2admin としてログインします。 IBM_TRAM スキーマを作成するには、ユーザー ID に管理者権限が必要です。
  3. ディメンション・テーブルの作成対象となるデータベースに接続します。これは、Tivoli Data Warehouse です。

     ```
     db2 connect to WAREHOUS
     ```
  4. 古いバージョンのデータベース・スクリプトが既にインストールされている場合は、データベースをクリーンアップします。

     ```
     db2 -tf clean.db2
     ```
  5. スキーマおよびテーブルを作成します。

     ```
     db2 -tf create_schema_IBM_TRAM.db2
     ```

     コマンドが正常に完了すると、IBM_TRAM の下に TIME_DIMENSION、MONTH_LOOKUP、WEEKDAY_LOOKUP、ComputerSystem、 BusinessService、SiteInfo などいくつかのテーブルが表示されます。
  6. 時間ディメンションを生成するためのストアード・プロシージャーを作成します。

     ```
     db2 -td@ -vf gen_time_dim_granularity_min.db2
     ```
  7. TIME_DIMENSION テーブルにデータを取り込むには、タイム・スタンプを生成するための日付と細分度を指定して時間ディメンション・ストアード・プロシージャーを呼び出します。 最大 5 年間を一度に生成するか、毎日データが再生成されるようにすることができます。

     ```
     db2 "call IBM_TRAM.CREATE_TIME_DIMENSION('start_date',
     'end_date', granularity_of_data)"
     ```

     ここで、start_date および end_date は、フォーマット YYYY-MM-DD-HH.MM.SS.MILSEC で、granularity_of_data は分単位の頻度です。例えば、以下のコマンドは、2010 年 1 月 1 日から 2015 年 1 月 1 日までのデータを 60 分の細分度で取り出します。

     ```
     db2 "call IBM_TRAM.CREATE_TIME_DIMENSION('2010-01-01-00.00.00.000000',
     '2015-01-01-00.00.00.000000', 60)"
     ```

ヒント: 時間ディメンションを取り込む際は、以下のガイドラインに従ってください。

- 年次データを表示するには、上記の例で示されているように、その年の最初の日を指定します。
- 新しい着信データが正しくマップされてレポートで表示されるように、終了日は余裕を持って指定します。
- ベスト・プラクティスは、細分度に 60 分の値を使用することです。

- **Microsoft SQL Server**
  1. レポート・パッケージ内のデータベース・スクリプト (.sql ファイル) を、Tivoli Data Warehouse に対してそれらのスクリプトを実行できる場所にコピーします。 スクリプトは、レポート・パッケージが解凍されたディレクトリーの db_scripts ブランチに入っています。
  2. データベース名がデフォルトと異なる場合は、use ステートメント内のデフォルトのデータベース名を変更して (USE IBM を置換します)、提供されたスクリプトをカスタマイズします。Tivoli Data Warehouse の名前が warehouse である場合、ステートメントは `USE warehouse` となります。
     a. 古いバージョンのデータベース・スクリプトが既にインストールされている場合は、**clean.sql** コマンドを使用してデータベースをクリーンアップします。
     b. **createSchema.sql** コマンドを実行します。
     c. **createProcedure.sql** コマンドを実行します。
     d. **populateTimeDimension.sql** コマンドを実行します。また、時間ディメンションおよび細分度の境界パラメーターを変更します。例えば、次のようにします。

        ```
        @startDate    = '2010-01-01 00:00:00',
        @endDate      = '2012-12-31 00:00:00',
        @granularity  = 60,
        ```

        月曜日をその週の最初の曜日としなければならない場合、1 に設定された 4 番目のパラメーターを加えます。そうでない場合は、3 つのパラメーターを解放します。

        ```
        @weekday      = 7
        ```
  3. 古いバージョンのデータベース・スクリプトが既にインストールされている場合は、データベースをクリーンアップします。

     ```
     sqlcmd -i clean.sql [-U username -P password] [-S hostname]
     ```
  4. MS SQL コマンド行で、以下の順序でスクリプトを実行します。

     ```
     sqlcmd -i createSchema.sql [-U username -P password] [-S host]
     sqlcmd -i createProcedure.sql [-U username -P password] [-S host]
     sqlcmd -i populateTimeDimension.sql [-U username -P password] [-S host]
     ```

- **Oracle** 手動インストール
  1. レポート・パッケージ内のデータベース・スクリプト (.sql ファイル) を、Tivoli Data Warehouse に対してそれらのスクリプトを実行できる場所にコピーします。 スクリプトは、レポート・パッケージが解凍されたディレクトリーの db_scripts ブランチに入っています。
  2. SQL *Plus セッションがまだ実行されていない場合は、開始します。

3. sys ユーザーとしてリモートからアクセスできることを確認します。
4. 古いバージョンのデータベース・スクリプトが既にインストールされている場合は、データベースをクリーンアップします (プロシージャーは sys ユーザーが呼びだす必要があります)。

   ```
   clean.sql
   ```

5. 以下のいずれかのステップを実行します。
   - sys ユーザーとしてリモートからアクセスできる場合は、以下のコマンドを実行し、スクリプトに必要なすべての情報を提供します。

     ```
     @MY_PATH¥setup_IBM_TRAM.sql
     ```

   - sys ユーザーとしてリモートからアクセスできない場合は、以下のコマンドを Oracle サーバーでローカルで実行し、スクリプトに必要なすべての情報を提供します。

     ```
     @MY_PATH¥local_setup_IBM_TRAM.sql
     ```

- **Oracle** バッチ・インストール
  1. レポート・パッケージ内のデータベース・スクリプト (.sql ファイル) を、Tivoli Data Warehouse に対してそれらのスクリプトを実行できる場所にコピーします。 スクリプトは、レポート・パッケージが解凍されたディレクトリーの db_scripts ブランチに入っています。
  2. SQL *Plus セッションがまだ実行されていない場合は、開始します。
  3. 古いバージョンのデータベース・スクリプトが既にインストールされている場合は、データベースをクリーンアップします (プロシージャーは sys ユーザーが呼びだす必要があります)。

     ```
     clean.sql
     ```

  4. ユーザー IBM_TRAM を作成します (スクリプトは、SYS/SYSTEM などのシステム権限を持つユーザーが呼びだす必要があります)。

     ```
     @MY_PATH¥create_IBM_TRAM.sql TCR_PASS USER_TBSPC TEMPORARY_TBSPC
     ```

     ここで、TCR_PASS は新規ユーザーのパスワード、*USER_TBSPC* はデフォルトのユーザー・テーブル・スペース名 (存在していなければなりません)、および *TEMPORARY_TBSPC* はデフォルトの一時テーブル・スペース名 (存在していなければなりません) です。
  5. IBM_TRAM テーブルを作成します (スクリプトは、前のステップで作成された IBM_TRAM ユーザーが呼びだす必要があります)。

     ```
     @MY_PATH¥create_schema.sql USER_TBSPC
     ```

     ここで、*USER_TBSPC* は、デフォルトのユーザー・テーブル・スペース名 (存在していなければなりません) です。
  6. ITMUSER など、ユーザーに特権を付与します (スクリプトは、IBM_TRAM ユーザーが呼びだす必要があります)。

     ```
     @MY_PATH¥grant_IBM_TRAM.sql USER
     ```

     ここで、*USER* は、特権を付与されるユーザーの名前です。
  7. プロシージャーを作成します (スクリプトは、IBM_TRAM ユーザーが呼びだす必要があります)。

     ```
     @MY_PATH¥gen_time_dim_granularity_hr.sql
     ```

8. ルックアップ・データをロードします (スクリプトは、IBM_TRAM ユーザーが呼びだす必要があります)。

   ```
   @MY_PATH¥populateLookup.sql
   ```

9. 時間ディメンションを生成します (プロシージャーは、IBM_TRAM ユーザーが呼びだす必要があります)。

   ```
   @MY_PATH¥populateTimeDimension.sql StartDate EndDate Granularity
   ```

   ここで、StartDate はフォーマット「yyyy-mm-dd HH:MM」の開始日、*EndDate* はフォーマット「yyyy-mm-dd HH:MM」の終了日、*Granularity* は分数です。例:

   ```
   @MY_PATH¥populateTimeDimension.sql '2010-01-01 00:00' '2012-
              12-31 00:00' '60'
   ```

タスクの結果

共有ディメンション・テーブルと時間ディメンション・テーブルが完成しました。

トラブルシューティング

DB2 コマンドが次のエラーで失敗する場合:
UDA-SQL-0107 "prepare" 処理中に一般例外が発生しました。[IBM][CLI Driver][DB2/NT64] SQL0551N "ITMUSER" は、オブジェクト"IBM_TRAM" で処理 "SELECT" を実行する特権を持っていません.....

問題を解決するには、以下のコマンドを実行します。

1. DB2 特権を持つユーザーとして Tivoli Data Warehouse に接続します。
2. 以下の権限付与を実行します。

   IBM_TRAM."ComputerSystem" の select 権限を ITMUSER に付与します。

   IBM_TRAM.MONTH _LOOKUP の select 権限を ITMUSER に付与します。

   IBM_TRAM.TIMEZONE_ DIMENSION の select 権限を ITMUSER に付与します。

   IBM_TRAM.TIME_DIMENSION の select 権限を ITMUSER に付与します。

   IBM_TRAM.WEEKDAY_LOOKUP の select 権限を ITMUSER に付与します。

   IBM_TRAM.CREATE_TIME_DIMENSION プロシージャーの execute 権限を ITMUSER に付与します。

次のタスク

リソース・ディメンション・テーブルを作成し、それにデータを取り込みます。

リソース・ディメンション・テーブルの作成とデータの取り込み

Tivoli Common Reporting 用に Tivoli Data Warehouse を準備する作業として、リソース・ディメンション表「ManagedSystem」の作成とこのテーブルへのデータの取り込みがあります。このテーブルは、Cognos レポートを実行し、データ・モデルを使用するのに必須です。

始める前に

最初に、ヒストリカル・データ収集を構成する必要があります。詳しくは、 575 ページの『開始前のヒストリカル・データ収集の構成』を参照してください。

このタスクについて

サイトで Tivoli Data Warehouse を実行する場合は、1 つ以上のモニター・エージェントをインストールするたびに、ウェアハウスの ManagedSystem テーブルを更新する必要があります。

重要: ハードコーディングされたユーザー・スキーマを使用するスクリプトを以下に示します。別のスキーマを使用する場合は、ハードコーディングされているスキーマのすべてのインスタンスを、指定したユーザーで置き換える必要があります。

手順

- **IBM DB2**
  1. **db2admin** としてログインします。 リソース・ディメンションを作成するには、ユーザー ID に管理者権限が必要です。
  2. リソース・ディメンション・テーブルの作成対象となるデータベースに接続します。これは、Tivoli Data Warehouse です。

     ```
     db2 connect to WAREHOUS
     ```
  3. ウェアハウスに接続するために デフォルトの ITMUSER とは異なるユーザーを指定した場合は、提供されたスクリプト gen_resources.db2、populate_resources.db2、populate_resources_zos.db2 をカスタマイズして、ハードコーディングされたスキーマ "ITMUSER" のすべてのインスタンスを、指定したユーザーで置換します。
  4. テーブルを作成します。

     ```
     db2 -tf gen_resources.db2
     ```

     コマンドが正常に完了すると、ITMUSER スキーマの下に新規テーブル ManagedSystem が表示されます。
     注: テーブル「ITMUSER.ManagedSystem」が既に作成されている場合は、gen_resources.db2 スクリプトの実行時に次のメッセージが表示されますが、このメッセージは無視できます。表示されるメッセージは「DB21034E コマンドが、有効なコマンド行プロセッサー・コマンドでないため、SQL ステートメントとして処理されました。SQL 処理中に、そのコマンドが返されました。SQL0601N 作成されるオブジェクト名が、タイプ "TABLE" の既存の名前 "ITMUSER.MANAGEDSYSTEM" と同じです。SQLSTATE=42710)」です。
  5. ManagedSystem テーブルにデータを取り込むためのストアード・プロシージャーを作成します。

     ```
     db2 -td@ -vf populate_resources.db2
     ```
  6. ManagedSystem テーブルにデータを取り込むには、ストアード・プロシージャーを呼び出します。

     ```
     db2 "call ITMUSER.POPULATE_OSAGENTS()"
     ```

     注: デフォルトとは異なるユーザーを指定した場合は、ITMUSER を、ウェアハウス構成時に指定したユーザーで置換してください。
- **Microsoft SQL Server**
  1. 以下のようにして、提供されたスクリプトをカスタマイズします。

a. **create_table.sql** で、デフォルトと異なる場合は、use ステートメント内のデフォルトのデータベース名を変更します (USE WAREHOUS を置換します)。

b. **create_procedure.sql** で、デフォルトと異なる場合は、use ステートメント内のデフォルトのデータベース名を変更します (USE WAREHOUS を置換します)。

c. **populate_agents.sql** で、デフォルトと異なる場合は、use ステートメント内のデフォルトのデータベース名を変更します (USE WAREHOUS を置換します)。

2. MS SQL コマンド行で、以下の順序でスクリプトを実行します。

```
sqlcmd -i create_table.sql [-U myusername -P mypassword] [-H myhost])
sqlcmd -i create_procedure.sql [-U myusername -P mypassword] [-H myhost])
sqlcmd -i populate_agents.sql [-U myusername -P mypassword] [-H my_host])
```

- **Oracle** 手動インストール
  1. SQL *Plus セッションがまだ実行されていない場合は、開始します。
  2. このコマンド (スペースを含まないパスを指定します) を実行し、スクリプトに必要なすべての情報を提供します。

```
@MY_PATH¥setup_populate_agents.sql
```

- **Oracle** バッチ・インストール
  1. SQL *Plus セッションがまだ実行されていない場合は、開始します。
  2. ITMUSER.ManagedSystem テーブルを作成します。スクリプトは、Tivoli Data Warehouse ユーザーが呼びだす必要があります。このユーザーは、デフォルトでは ITMUSER です。異なるユーザー名を使用した場合は、正しい名前が指定されるようにスクリプトを変更します。

```
@MY_PATH¥create_table.sql USER_TBSPC
```

  3. テーブルにデータを取り込むためのプロシージャーを作成します。

```
@MY_PATH¥create_procedure.sql
```

  4. 以下のようにプロシージャーを開始して、ManagedSystem テーブルにデータを取り込みます。

```
begin
POPULATE_OSAGENTS('ITMUSER');
end;
/
```

タスクの結果

リソース・ディメンション・テーブルが完成しました。

次のタスク

IBM Cognos レポートをインストールして実行します。

レポート・インストーラーを使用したレポートのインポート

レポート・インストーラーは、インストーラーにバンドルされているレポートを含む特定のエージェントに対してのみ使用できます。このインストール方式は、利用可能である場合のみ使用できます。

始める前に

レポート・インストーラーは、Tivoli Common Reporting バージョン 2.1 およびそれ以降をサポートします。Tivoli Common Reporting バージョン 1.3 を使用している場合は、たとえレポートに互換性があったとしても、レポートをインストールすることができません。これは、レポート・インストーラーが Tivoli Common Reporting バージョン 2.1 およびそれ以降でしか機能しないためです。

ご使用のエージェントでの追加のインストール手順および可能なトラブルシューティング項目については、エージェント固有のユーザーズ・ガイドを参照してください。

Tivoli Common Reportingに関する追加の情報については、IBM Tivoli Common Reporting インフォメーション・センターを参照してください。

このタスクについて

レポート・インストーラーを使用してバンドルされているレポートをインポートするには、以下の手順を使用します。この手順は、バージョン 6.2.3 以降の OS エージェントおよび TivoliPerformance Analyzer レポートで使用できます。

手順

- GUI を使用する場合:
  1. 製品 CD の ¥osreports ディレクトリーから、ご使用のオペレーティング・システムに適したコマンドを実行してください。

     Windows `setup_platform.exe`

     Linux UNIX `setup_platform.bin`

     インストーラー・ウィンドウが開きます。
  2. 言語を選択して、「**OK**」をクリックします。
  3. 「ようこそ」ページで「**次へ**」をクリックします。
  4. tipv2Components¥TCRComponents などの Tivoli Common Reporting インストール・ディレクトリーを指定します。 (インストール・ディレクトリーは、tcr21Components など、異なる場合があります。) デフォルト・フォルダーを使用するか、「**選択**」ボタンを使用してパスを提供します。「**次へ**」をクリックします。
  5. インストールするレポートを選択します。「**次へ**」をクリックします。
  6. Tivoli Common Reporting ユーザー名とパスワードを入力します。「**次へ**」をクリックします。
  7. 以下のように、データ・ソースおよびデータ・スクリプトごとに、データ・ソース構成情報を入力します。
     - 該当する場合、「**Cognos データ・ソース**」構成ウィンドウで、Tivoli Data Warehouse のデータベース・ユーザー名、パスワード、データベース・タイプ、およびデータベース名を入力します。DB2 または Oracle の場合は、データベース名を入力してください。SQL の場合は、 ODBC データ・ソース名を入力してください。

– 該当する場合、以下のように、「**BIRT データ・ソース**」ウィンドウおよび「**データ・スクリプトの構成 (Configure Data Script)**」ウィンドウで構成情報を入力します。

「**JDBC ユーザー資格情報**」タブで、インストール時に使用される Tivoli Data Warehouse のデータベース・ユーザー名とパスワードを入力します。データ・ソースの定義を今はスキップする場合は、ボックスをオンにします。

「**JDBC データベース資格情報**」タブで、リストからデータベース・タイプを選択し、その後データベース JDBC URL を入力して JDBC ドライバー・ファイルを指定します。この JAR ファイルは、「**参照**」ボタンを使用して検索するか、ファイル名を入力します (複数ある場合は、セミコロン (;) で区切って入力します)。ドライバー JDBC クラスを入力します。データ・ソースの定義を今はスキップする場合は、ボックスをオンにします。

注: 1 つのデータ・ソースに複数の JAR ファイルが必要な場合があります。JDBC の場合、特定のドライバー・ファイルが、Tivoli Common Reporting ディレクトリーに自動的にコピーされ、レポートのデータを収集するためにデータベース接続を作成する際に、そのディレクトリーから使用されます。

「**次へ**」をクリックします。

8. プリインストールの要約が表示されます。この要約を注意して読み、情報が正しいことを確認します。正しい場合は、「**インストール**」をクリックします。あるいは、前に指定したパラメーターのいずれかを変更するには、「**戻る**」ボタンを使用します。
9. インストールの進行状況を示すウィンドウが表示されます。
10. インストール後レポートが表示されます。インストールが正常に完了したことを確認し、「**完了**」をクリックします。

- コマンド行を使用する場合:
  1. `setup_<platform>.exe/.bin -i console` コマンドを実行します。
  2. インストール言語を選択します。
  3. `TCRComponent` ディレクトリーのロケーションを入力します。
  4. インストールするレポートのタイプを選択します。
  5. Tivoli Common Reporting ユーザー名とパスワードを入力します。
  6. データ・ソースおよびデータ・スクリプトを構成します。一部のレポート・パッケージにはデータ・スクリプトがないことがあります。
  7. インストールの要約が表示されたら、**Enter** キーを押してインストールを開始します。
- サイレント・モードを使用する場合:
  1. サイレント・インストーラー応答ファイルを作成し、このファイルに `silent_installer.properties` という名前を付けます。
  2. `setup_<platform>.exe/.bin -i silent -f <path_to_response_file>` コマンドを実行します。

タスクの結果

これで、エージェント・レポートが Tivoli Common Reporting サーバーにインストールされました。

次のタスク

これで、レポートを使用して、モニター・エージェントによって収集されたモニタリング・データを表示できます。Tivoli Common Reporting でのレポートの実行、管理、および編集方法については、レポートの処理トピックを参照してください。

追加のレポート情報については、エージェント固有のユーザーズ・ガイドを参照してください。

IBM Cognos レポートのインポートと実行

Cognos ディメンション・テーブルを作成してそれにデータを取り込み、次にレポート・パッケージをインポートして、モニター・エージェントに対して Tivoli Common Reporting を使用可能にします。

このタスクについて

ご使用のレポートがレポート・インストーラーに含まれている場合は、 587 ページの『レポート・インストーラーを使用したレポートのインポート』を参照してください。

ご使用のレポートがレポート・インストーラーに含まれていない場合は、 592 ページの『Dashboard Application Services Hubを使用したレポートのインポート』を参照してください。

レポートのインストールについて詳しくは、IBM Tivoli Common Reporting インフォメーション・センターを参照してください。

前提条件スキャンの実行

「OS Agents Reports 前提条件スキャナー」レポートは、OS エージェント・レポート・パッケージに含まれています。このレポートを使用して、IBM Tivoli Monitoring OS エージェントのレポート・ソリューションと Tivoli Common Reporting を使用するためのシステムの前提条件を検査できます。このヘルス・チェック・レポートを実行して、前提条件の概要を確認し、共有ディメンション表、時間ディメンション表、およびリソース・ディメンション表が使用可能であることを確認します。

始める前に

このレポートが機能するためには、Tivoli Common Reporting で、Tivoli Data Warehouse に接続するようにデータ・ソース接続を定義する必要があります。

このタスクについて

「OS Agents Reports 前提条件スキャナー」レポートは以下の前提条件に関するデータを返します。

- Tivoli Common Reporting 共有ディメンションの前提条件。
- IBM Tivoli Monitoring 共有ディメンションの前提条件。
- レポート別の前提条件。

システムが正しく構成されている場合は、共有ディメンションは条件を満たしているものとして報告されます。レポート・セットが条件を満たしていないものとして返される場合、これが収集しないレポート・セットに関するものであれば無視できます。

制約事項: 各国語でレポート機能を使用する場合、一部のテキスト・ストリングが英語のみで表示されます。

手順

1. Tivoli Common Reporting ナビゲーター・ツリーで「パブリック・フォルダー」→「IBM Tivoli Monitoring OS Agents Reports」→「前提条件の検証」→「**OS Agents Reports 前提条件スキャナー」レポート**を選択します。
2. 使用可能な 2 つのレポート・タイプのいずれかを選択します。
   - すべてのセクションの表示: このオプションを選択すると、失敗 (満たされなかった前提条件) と成功 (満たされた前提条件) を含むすべてのセクションが表示されます。
   - 失敗したセクションのみの表示: このオプションを選択すると、失敗 (満たされなかった前提条件) のセクションのみが表示されます。
3. 返されたレポート情報を確認します。満たされていない前提条件を解決するために必要な処置を実行します。 「**凡例**」表で返された情報を参照し、「**状況**」列と「**詳細**」列で要約情報を確認します。

次のタスク

レポートを参照するときには、「**詳細**」列で  をクリックすると、追加情報に関する「**表の詳細**」レポートが表示されます。

注: 「**表の詳細**」レポートを表示する方法は、「**詳細**」列のアイコンをクリックする方法のみです。「パブリック・フォルダー」→「IBM Tivoli Monitoring OS Agents Reports」→「前提条件の検証」→「**表の詳細**」からこのレポートを直接実行すると、エラーが返されます。

ODBC を介するデータベース・クライアントを使用した Tivoli Data Warehouse への接続

Cognos は、ODBC を使用してデータベースに接続します。最初に Tivoli Common Reporting サーバーにデータベース・クライアントをインストールし、それを Tivoli Data Warehouse と接続させることが重要です。データベースと Tivoli Common Reporting サーバーが同じコンピューター上にある場合は、データベース・クライアントは必要ありません。

手順

- **IBM DB2**

1. Cognos ベースの Tivoli Common Reporting エンジンがインストールされているコンピューターに DB2 データベース・クライアントをデプロイしていることを確認します。クライアントは、Tivoli Data Warehouse が使用しているデータベースと同じバージョンでなければなりません。

   Linux UNIX Cognos ベースの Tivoli Common Reporting エンジンがインストールされている場所に DB2 サーバーがインストールされている場合、DB2 クライアント・ファイルは既に使用可能になっています。ただし、DB2 ライブラリー・ファイル (libdb2.a) を *Cognos_8_Install_dir*/bin ディレクトリーにコピーして、Tivoli Data Warehouse が存在しているデータベース・サーバーに Cognos が正常に接続できるようにする必要があります。
2. DB2 構成アシスタントを実行し、ローカル・ネット・サービス名構成を設定してからシステムを再始動することによって、DB2 データベース・クライアントをデータベース・サーバーに接続します。
3. 作成した接続の名前はレポート・インストーラーによって Tivoli Common Reporting で使用されるため、その名前を書き留めてください。

- **Microsoft SQL Server**
  1. Cognos ベースの Tivoli Common Reporting エンジンがインストールされているコンピューターに MS SQL データベース・クライアントをデプロイしていることを確認します。
  2. MS SQL Management Studio Express® を実行し、ローカル・ネット・サービス名構成を構成してからシステムを再始動することによって、MS SQL クライアントをデータベース・サーバーに接続します。
  3. 作成した接続の名前はレポート・インストーラーによって Tivoli Common Reporting で使用されるため、その名前を書き留めてください。
- **Oracle**
  1. Cognos ベースの Tivoli Common Reporting エンジンがインストールされているコンピューターに Oracle データベース・クライアントをデプロイしていることを確認します。
  2. Oracle Net Configuration Assistant を実行し、ローカル・ネット・サービス名構成を構成してからシステムを再始動することによって、Oracle データベース・クライアントをデータベース・サーバーに接続します。
  3. 作成した接続の名前はレポート・インストーラーによって Tivoli Common Reporting で使用されるため、その名前を書き留めてください。

タスクの結果

これで、レポートをインポートして実行できます。

Dashboard Application Services Hubを使用したレポートのインポート

Dashboard Application Services Hub ユーザー・インターフェースを使用して、Tivoli Monitoring OS エージェントのレポートをインポートすることができます。

始める前に

モニター・エージェント・レポート・モデルは、IBM Cognos がベースになっています。レポートをインストールするコンピューター上に、Tivoli Common Reporting V1.3 (Cognos エンジンを含む) をインストールし、実行しておく必要があります。また、 581 ページの『共有ディメンション・テーブルの作成と時間ディメンション・テーブルへのデータの取り込み』および 585 ページの『リソース・ディメンション・テーブルの作成とデータの取り込み』に示されているとおりにディメンション・テーブルを作成してデータを追加し、 591 ページの『ODBC を介するデータベース・クライアントを使用した Tivoli Data Warehouse への接続』に示されているとおりにデータウェアハウスに接続しておく必要もあります。

制約事項: このインポート方式は、Cognos レポートに対してのみ使用できます。

このタスクについて

処理するレポート・パッケージを取得する必要があります。IBM Integrated Service Management Library からパッケージをダウンロードするか、「コンテンツ管理」インターフェースを使用してパッケージを作成することができます。インポートするすべてのパッケージは、`TCR_component_dir¥cognos¥deployment` ディレクトリーに格納する必要があります。

手順

1. Dashboard Application Services Hub 管理コンソールを起動してログインします。
2. 「**共通のレポート処理 (Common Reporting)**」に進みます。
3. **右側にある「レポートの処理」**ウィンドウで、「**起動**」ドロップダウン・リストから「**管理**」をクリックします。
4. 「**構成 (Configuration)**」タブに移動して、「**コンテンツ管理**」セクションを開きます。
5. 「**インポート**」をクリックして、新規パッケージ・インポートを作成します。これにより、「**新規インポート**」ウィザードが開きます。
6. ウィザードに従って新規パッケージをインポートします。

タスクの結果

これで、OS エージェント・レポートが Tivoli Common Reporting サーバーにインストールされました。

次のタスク

これで、レポートを使用して、OS モニター・エージェントによって収集されたモニタリング・データを表示できます。Tivoli Common Reporting での Cognos レポートの実行、管理、および編集方法については、レポートの処理のトピックを参照してください。

レポートに関する追加の情報については、オペレーティング・システム・エージェントごとのユーザーズ・ガイドを参照してください (例えば、*Windows OS Agent ユーザーズ・ガイド*の Tivoli Common Reporting の付録)。

レポート・パッケージのインストールで問題が発生した場合は、「*IBM Tivoli Monitoring トラブルシューティング・ガイド*」を参照してください。

Dashboard Application Services Hub レポートの作成

Dashboard Application Services Hub では、レポートを作成することができます。

このタスクについて

Dashboard Application Services Hub グラフを作成するには、以下のステップを実行します。

手順

1. Dashboard Application Services Hub に `tipadmin` または `chartAdministrator` 役割が付与されたユーザーとしてログインします。
2. 「**設定**」 > 「**ページ管理**」 > 「**新規ページ**」を選択して、新規ページを作成します。
3. グラフ作成ポートレットを選択して、「**OK**」をクリックします。
4. ページを保存し、新しい名前を指定します。
5. グラフ作成ポートレットで 「**IBM グラフ / Tivoli グラフ**」を選択します。
6. Tivoli Enterprise Portal Server に接続します。 60 ページの『IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーへの接続の作成』を参照してください。
7. 正常に接続すると、IBM Tivoli Monitoring ワークスペースに類似したグループのリストが表示されます。表にデータを取り込むには、グループを選択します。
8. グラフを選択して「**完了**」をクリックします。グラフが表示されます。

BIRT レポートのインポートと実行

Eclipse BIRT (Business Intelligence and Reporting Tools) Report Designer を使用して、独自のレポートを開発したり既存のレポートを編集したりできます。Eclipse BIRT Report Designer は、レポートのダウンロードやインストールに必須ではありません。

BIRT レポート・パッケージのインポート

監視対象のアプリケーションのレポート・パッケージをインポートし、BIRT レポートを定義するために必要なファイルを取得します。

始める前に

レポート・パッケージ は、1 つ以上のレポートを定義するために必要なすべてのデータを含む .zip ファイルです。これには、必要なデザインとリソース、およびレポートを包含するレポート・セットの階層が含まれます。モニター・エージェントのレポートは、REPORTS ディレクトリーのエージェント・イメージ上に .zip ファイルとして含まれます。例えば、Windows コンピューターでイメージ・ドライブのラベルが D: である場合、レポートは D:¥REPORTS¥kqb などのディレクトリーにあります。レポートの場所については、エージェントのレポート機能の章または「*Product reporting guide*」を参照してください。

このタスクについて

trcmd コマンドの **-import** コマンド・フラグを使用すると、BIRT および Cognos のレポート・パッケージおよびレポート・デザインがインポートされます。パッケージのタイプは自動的に認識されます。このコマンドは、シングルボックスのインストールの場合で、かつレポート・エンジンに対してのみ使用できます。それ以外のシナリオに対してはサポートされていません。

詳しくは、Tivoli Common Reporting インフォメーション・センターの『共存サポート』の説明を参照してください。

Tivoli Common Reporting V2.1 の場合は、以下の手順を使用します。

手順

1. レポート・パッケージをインポートするには、以下の構文を使用します。
   trcmd -import -bulk *pkgFile* [**-reportSetBase** *rsBase*] [**-resourceBase** *resourceBase*] [**-designBase** *designBase*] [**-help**]

   次の例では、avail_skills.zip という名前の BIRT パッケージをインポートし、そのリソース・ディレクトリーを C:¥download からインポートします。`trcmd -import -bulk C:¥download¥sth¥report¥avail_skills.zip -reportSetBase myReportSetBase -resourceBase myResourceBase -designBase myDesignBase -user tipadmin -password admin`
2. レポート設計をインポートし、その設計に関連付けられた新規レポートを作成するには、以下の構文を使用します。
   trcmd -import -design *designPath* [**-resourceDir** *resourcePath*] -**reportSetBase** *rsBase*

   使用上の注意:
   - Cognos レポートのインポート時に、**-resourceBase**、**-designBase**、および **-resourceDir** パラメーターは無視されます。
   - **-design** パラメーターを使用して、単一の Cognos レポートを .xml ファイルからインポートできます。

タスクの結果

ナビゲーション・ツリーでは、レポートの項目およびレポートのサブセット項目を表示します。

次のタスク

レポートのデータ・ソースを変更すると、すべてのレポートのデータ・ソースが変更されます。すべてのレポートに対してこの変更を繰り返す必要はありません。

関連資料:

Tivoli Common Reporting インフォメーション・センター - レポート・パッケージのインポート
レポート・パッケージのインポート > 拡張オプションの説明。

データ・ソースの構成

BIRT レポート・パッケージのすべてのレポートは、同じデータ・ソースを参照する必要があります。ご使用の Tivoli Data Warehouse を参照するようにデータ・ソース・ポインターを変更する必要があります。

このタスクについて

Tivoli Common Reporting をインストールし、最初のレポートのセットをインポートした後、管理者または管理者権限を持つユーザーが、Tivoli Data Warehouse を実行するために使用しているローカルまたはリモートのデータベース・マネージャーから Tivoli Common Reporting サーバー・ディレクトリーに JDBC ドライバーをコピーする必要があります。 「**データ・ソースの編集**」ウィンドウでこれらのファイルを指定します。以下のステップを実行して、これらのドライバーをインストールしてください。

手順

1. 以下の JDBC ドライバー・ファイルを見つけます。

   IBM DB2 db2jcc.jar および db2jcc.license_cu.jar

   Windows C:¥Program Files¥IBM¥SQLLIB¥java

   Linux UNIX *db2_installdir*/java

   例えば、ワークステーション・バージョン 9 上のデフォルトの DB2 インストール・ディレクトリーは、AIX では /usr/opt/db2_09_01 であり、Linux および Solaris では /opt/IBM/db2/V9.1 です。

   JDBC ドライバーは、通常、このデフォルトの DB2 インストール・パスにあるか、または DB2 インストールで指定した任意の代替パスの java ディレクトリーにあります。

   IBM DB2 Driver for JDBC and SQLJ は、IBM Web サイトからもダウンロードできます。

   Microsoft SQL Server sqljdbc.jar

   Microsoft SQL Server JDBC Driver を Microsoft Web サイトからダウンロードします。インストール後の SQL Server 2005 JAR ファイルの名前およびロケーションは、*mssql2005installdir*/sqljdbc_1.1/enu/sqljdbc.jar です。

   Oracle oraclethin.jar

   JDBC Type 4 driver を Oracle Web サイトから入手します。インストール後の Oracle JDBC ドライバー JAR ファイルの名前およびロケーションは、*oracleinstalldir*/jdbc/lib/oraclethin.jar です。

2. JDBC ドライバーを以下の Tivoli Common Reporting インストール・ディレクトリーにコピーします。

- *tcr_install_dir*TCR_component_dir¥lib¥birt-runtime-2_2_2 ¥ReportEngine¥plugins¥org.eclipse.birt.report.data.oda.jdbc_2.2.2. r22x_v20071206¥drivers
- DB2 データ・ソースの場合は、DB2 JDBC ドライバーとライセンス JAR ファイルを同じロケーションにコピーします。db2jcc.jar および db2jcc_licence_cu.jar ファイルを、ロケーション *db2_installdir*/java (例: C:¥Program Files¥IBM¥SQLLIB¥java) から DB2 サーバー・システム上にコピーできます。

3. **trcmd -modify** コマンドを実行して、データ・ソースを構成します。詳細な説明については、Tivoli Common Reporting インフォメーション・センターの『trcmd-modify コマンド』トピックを参照してください。

次のタスク

追加情報については、IBM developerWorks Tivoli Common Reporting spaceにある「*IBM Tivoli Common Reporting: Development and Style Guide*」の JDBC ドライバーに関するセクションを参照してください。

Tivoli Data Warehouse の接続に関する問題の詳細については、「*IBM Tivoli Monitoring インストールおよび設定ガイド* (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/topic/com.ibm.itm.doc_6.3/install/itm_install.htm)」の『第 5 部 データウェアハウスのセットアップ』を参照してください。

サンプル BIRT レポートの生成

Tivoli Common Reporting BIRT レポート・パッケージは製品ごとに編成されています。レポートを生成するには、レポート・セットを選択します。

手順

1. Tivoli Common Reporting と互換性のあるブラウザーを起動し、アドレス https://<address>:16311/ibm/console/logon.jsp を入力します。ここで、<address> は、Tivoli Common Reporting がインストールされているシステムの IP アドレスまたはホスト名です。 ご使用の環境がデフォルト以外のポート番号を指定して構成されている場合は、その番号を代わりに入力します。サーバーへのデフォルトのパスは、/ibm/console です。ただし、このパスは構成可能であり、お使いの環境ではデフォルトと異なっている可能性があります。
2. 左側のナビゲーション・ツリーで、「**レポートの処理**」項目を展開します。
3. 「**共通のレポート処理 (Common Reporting)**」をクリックします。使用可能なすべてのレポート (インポートしたすべてのレポート・パッケージ) が、画面のテキスト域に表示されます。
4. 「**ナビゲーション**」タブで、「**Tivoli 製品**」項目を展開します。
5. 使用可能な製品のリストから使用するレポートの Tivoli 製品を選択します。
6. Tivoli Data Warehouse のデータに基づいてレポートを初めて実行する場合、以下のステップを実行します。
   a. レポートのデータ・ソースとして Tivoli Data Warehouse を定義します。詳しくは、596 ページの『データ・ソースの構成』を参照してください。デー

タ・ソースについては、「*IBM Tivoli Common Reporting* ユーザーズ・ガイド」または Tivoli Common Reporting のオンライン・ヘルプを参照してください。

b. Tivoli Data Warehouse の実行に使用しているローカルまたはリモートのデータベース・マネージャーから Tivoli Common Reporting サーバー・ディレクトリーに、必要な JDBC ドライバーをコピーする必要があります。

Tivoli Common Reporting サーバーを始動するために、Java コマンドで Java 仮想マシン (JVM) のデフォルトのヒープ・サイズを増やす必要がある場合があります。レポートを作成するときに以下のメッセージが表示される場合は、デフォルトのヒープ・サイズを増やさなければならない可能性があります。

```
予期しないエラーにより処理が終了しました。(Processing has ended because of an
unexpected error.)
詳しくは、Tivoli Common Reporting のログ・ファイルを参照してください。
```

デフォルトのヒープ・サイズを増やす方法については、「*OMEGAMON XE and Tivoli Management Services on z/OS: Reports for Tivoli Common Reporting*」を参照してください。

7. 「アクション」列で、起動するレポートの実行 アイコンをクリックし、HTML (デフォルト)、PDF、Microsoft Word、 Microsoft Excel、または Adobe Postscript からレポート形式のタイプを選択します。

Tivoli Common Reporting からレポートを選択すると、「**レポート・パラメーター**」 ウィンドウが表示され、レポートの生成に使用する情報についてプロンプトが出されます。パラメーター・ウィンドウのタイトルが、生成されるレポートのタイプを示します。レポート・タイプの説明については、ご使用になっているエージェントまたは製品について、エージェントのユーザーズ・ガイドまたは製品のレポート・ガイドを参照してください。

「レポート・パラメーター」ウィンドウには、すべてのレポートで共通のいくつかのフィールド (時間フレーム など) が含まれています。その他のフィールドはレポートを実行するエージェントに固有です。ほとんどのレポートでは、時間フレーム、リソース、データの要約レベル、およびグラフ化する属性を選択します。表示されているすべてのデフォルトを受け入れるには、 をクリックします。

8. 「**実行**」をクリックすると、パラメーター定義に一致するレポートを生成します。

タスクの結果

Tivoli Common Reporting がレポート・データを収集し、フォーマット済み出力を作成している間は、砂時計が表示されます。処理が完了したら、レポートが Dashboard Application Services Hub で表示されます。

次のタスク

レポートが生成されない場合、または要求されたデータが使用できないことを示すメッセージが表示された場合は、「*IBM Tivoli Common Reporting* ユーザーズ・ガイド」でデータ・ソースの定義に関する情報を参照してください。

HTML 形式または PDF 形式のレポートを表示する場合は、任意の埋め込みリンクをクリックして、ドリルスルー・レポートを開くことができます。ドリルスルー埋め込みリンクをクリックすると、新しいパラメーターを指定したレポートまたは第 2 のレポート (ドリルダウンまたは要約) に再度リンクされます。ドリルスルー・リンクの例には、棒グラフ、折れ線グラフ、表のヘッダーなどがあります。

第 19 章 Tivoli Enterprise Portal Server データベースの複製

Tivoli Enterprise Portal Server で提供されているユーティリティーを使用して、TEPS データベースに格納されている Tivoli Enterprise Portal カスタマイズをマイグレーションします。この内容には、ユーザー ID、ナビゲーター・ビュー、カスタム照会、カスタム・ワークスペース、およびローカル端末スクリプトも含まれています。

migrate-import スクリプトおよび migrate-export スクリプトを使用して、同一オペレーティング・システムで 32 ビット Tivoli Enterprise Portal Server から 64 ビット Tivoli Enterprise Portal Server に切り替えることもできます。

Tivoli Enterprise Portal Server データベースの理解

Tivoli Enterprise Portal Server データベースを複製する前に、データベースに含まれているものや開始前に必要となるものを確認してください。

Tivoli Enterprise Portal のカスタマイズ

Tivoli Enterprise Portal のカスタマイズは、ポータル・サーバーの TEPS データベースに格納されます。この内容には、ユーザー ID、ナビゲーター・ビュー、カスタム照会、カスタム・ワークスペース、およびローカル端末スクリプトも含まれています。シチュエーション、ポリシー、および管理対象システム・グループは格納されません。

インストール済み環境を ポータル・サーバーの新規バージョンにアップグレードした場合は、TEPS データベースが新規または変更された任意の事前定義ナビゲーター・ビュー、照会、およびワークスペースで更新されます。作成したカスタム・ナビゲーター・ビュー、照会、およびワークスペースには影響しません。

テスト環境から実稼働環境に移行するには、TEPS データベースを複製する必要があります。また、この手順に従うと、フィックスパックの適用前や新バージョンへのアップグレード前に、予防手段としてデータベースをバックアップすることもできます。

宛先環境で既に作成されているワークスペースは、すべてソース環境で作成されたワークスペースに置き換えられます。また、宛先環境で過去に行ったユーザーによる変更内容も置き換えられます。

複製要件

Tivoli Enterprise Portal Serverをマイグレーションする前に、環境が以下の要件を満たしていることを確認してください。

- ソース・コンピューターおよびターゲット・コンピューター上のポータル・サーバーは、同じハブ・モニター・サーバーに接続されるよう構成する必要があります。

- ソース・コンピューターおよびターゲット・コンピューター上のポータル・サーバーは、バージョン 6.2.1 またはそれ以降でなければなりません。また、両方とも同じ Tivoli Monitoring Base DVD からインストールされているのが理想です。
- ソース・コンピューターおよびターゲット・コンピューター上のポータル・サーバーは、同じ方法でインストールされていなければならない。
  - 選択したアプリケーションが同じである。例えば、ソース・ポータル・サーバーで、UNIX 、Windows サーバー、および MQ Series のインストール済みアプリケーションがサポートされている場合は、ターゲット・ポータル・サーバーにおいても、同じアプリケーションがサポートされている必要があります。
  - ポータル・サーバー・データベースに同じデータベース・プログラムを使用している。例えば IBM DB2 UDB など。

選択複製用の CLI tacmds

コマンド行インターフェースには、特定の IBM Tivoli Monitoring オブジェクトをエクスポートおよびインポートするための tacmds があります。これらの各コマンドおよび構文の説明については、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

tacmd exportworkspaces
tacmd importworkspaces
あるポータル・サーバーから別のポータル・サーバーにワークスペースを選択してコピーします。

tacmd exportQueries
tacmd importQueries
カスタム照会を XML ファイルにエクスポートし、それらをポータル・サーバーにインポートします。

tacmd bulkExportSit
tacmd bulkImportSit
あるハブ・モニター・サーバーからすべての Tivoli Monitoring エンタープライズ・シチュエーションをエクスポートして、別の方にインポートします。

tacmd bulkExportPcy
tacmd bulkImportPcy
あるハブ・モニター・サーバーからすべての Tivoli Monitoring ポリシーをエクスポートして、別のハブ・モニター・サーバーにインポートします。

tacmd exportNavigator
tacmd importNavigator
カスタム・ナビゲーター・ビューとそのビューに割り当てられているワークスペース、照会、およびシチュエーション関連付けを XML ファイルにエクスポートし、それらをポータル・サーバーにインポートします。

tacmd exportSitAssociations
tacmd importSitAssociations
ナビゲーター・ビューまたは特定のナビゲーター項目のすべてのシチュエーション関連付けを XML ファイルにエクスポートし、それらををポータル・サーバーにインポートします。

tacmd exportSysAssignments
tacmd importSysAssignments
ナビゲーター・ビューまたは特定のナビゲーター項目のすべての管理対象システムの割り当てを XML ファイルにエクスポートし、それらをポータル・サーバーにインポートします。

migrate-export スクリプトの実行

Tivoli Enterprise Portal Server をエクスポートして、別のコンピューターに適用するための TEPS データベースのコピーを作成したり、バックアップとして保持したりできます。

始める前に

migrate-export スクリプトは、ポータル・サーバーの実行中および停止中に開始することができます。サーバーが停止している場合、サーバーはスクリプトによって一時的に制限モードで開始され、エクスポートを実行します。migrate-export が完了するまで、ポータル・サーバーを手動で開始しないでください。

このタスクについて

ソース Tivoli Enterprise Portal Server がインストールされたコンピューター上で、以下のステップを実行し、TEPS データベースのコピーを作成します。

手順

- Windows
  1. コマンド・プロンプト・ウィンドウを開きます。「**スタート**」→「**ファイル名を指定して実行**」を選択し、CMD と入力します。
  2. *install_dir* ¥CNPS ディレクトリーに移動します。
  3. migrate-export と入力します。

  migrate-export スクリプトによって、*install_dir* ¥CNPS¥sqllib サブディレクトリーに **saveexport.sql** という名前のファイルが生成されます。このファイルには、Tivoli Enterprise Portal Server のすべてのデータが含まれています。
- Linux UNIX
  1. ソース・システム上で、端末ウィンドウを開きます。
  2. IBM Tivoli Monitoring インストール済み環境の bin サブディレクトリー (cd /opt/IBM/ITM/bin など) に移動します。
  3. ./itmcmd execute cq "runscript.sh migrate-export.sh" と入力します。 単一引用符 (') ではなく、必ず二重引用符 (") を使用するようにしてください。

  migrate-export スクリプトによって、*install_dir* /$platform/cq/sqllib サブディレクトリーに **saveexport.sql** という名前のファイルが生成されます。このファイルには、Tivoli Enterprise Portal Server のすべてのデータが含まれています。

migrate-import スクリプトの実行

Tivoli Enterprise Portal Server データベースの saveexport.sql という名前のコピーがある場合は、設定を複写する任意のポータル・サーバー (同じバージョン) のインストール済み環境に、このコピーをインポートします。

saveexport.sql の内容に応じて、このプロセスによって既存の TEPS データベースを完全に置き換えることができます。

import スクリプトに組み込まれている一部のテーブルは、Tivoli Enterprise Portal Server の従来製品である CandleNet Portal Server にのみ適用できます。Tivoli Enterprise Portal Server データベースをインポートしない場合を除き、migrate-import のログ・ファイルに未定義の名前に関する次のような SQL エラーが記録されます。「SQLExecDirect rc=-1: SQL_ERROR SQLSTATE: 42S02, ERR: -204, MSG: [IBM][CLI Driver][DB2/LINUX] SQL0204N "ITMUSER.TAGGROBJ" は未定義の名前です。SQLSTATE=42704 RC = -1」
(ITMUSER.TMANOBJS、ITMUSER.TMANTMPL、ITMUSER.TTMPLSIT、ITMUSER.TTMPLSTA、ITMUSER.TSTUSERA も同様。) これらのエラーは無視してください。

ソース Windows からターゲット Windows への migrate-import の実行

migrate-import スクリプトを実行すると、Windows コンピューターから別の Windows コンピューターへ、Tivoli Enterprise Portal Server データベースのコピーをインポートすることができます。

始める前に

このプロシージャーは、ターゲット・コンピューター上の TEPS データベースを上書きします。

このタスクについて

ターゲット・ポータル・サーバーがインストールされた Windows コンピューター上で、以下のステップを実行し、別の Window コンピューターから migrate-export を使用してコピーされた TEPS データベースをインポートします。

手順

1. ターゲット・システム上のポータル・サーバーを停止します。
2. ソース・システム上でコマンド・プロンプトを開きます (「**スタート**」→ **ファイル名を指定して実行**」をクリックし、CMD と入力します)。
3. migrate-export.bat スクリプトによってソース・システムから生成したファイル **saveexport.sql** を宛先システム上の *install_dir* ¥CNPS¥sqllib にコピーします。ここで、<*mapped drive on destination system*> とは、このファイルが置かれているソース・システム上のディスク・ドライブのことです。 例:

   ```
   copy <mapped drive on destination system>:¥IBM¥ITM¥CNPS¥sqllib
        ¥saveexport.sql c:¥ibm¥itm¥cnps¥sqllib
   ```

   まだドライブを定義していない場合は、**net use** コマンドを使用して、宛先システムからソース・システムにドライブをマップする必要があります。

4. ターゲット・システム上で *install_dir* ¥CNPS ディレクトリーに移動し、migrate-import と入力します。 ポータル・サーバーが現在実行中の場合に migrate-import プロセスを実行すると、ポータル・サーバーは停止します。
5. migrate-import 機能を使用して TEPS データベースをあるリリースから別のリリースへ移動中の場合は、以下のようにデータベースをマイグレーションしてアプリケーション・サポートを追加した後、このタスクを実行します。
   a. <*install_dir*>¥CNPS¥kfwalone をテキスト・エディターで開きます。
   b. KFW_MIGRATE_FORCE=Y を設定した後、ファイルを保存して閉じます。
   c. このスクリプトを呼び出して、現行のポータル・サーバーのアプリケーション・サポートを新しくマイグレーションされた TEPS データベースに適用します (<*install_dir*>¥CNPS¥buildpresentation.bat)。
6. ポータル・サーバーを再始動します。

ソース Windows からターゲット Linux またはターゲット UNIX への migrate-import の実行

migrate-import スクリプトを実行すると、Windows コンピューターから Linux または UNIX コンピューターへ、Tivoli Enterprise Portal Server データベースのコピーをインポートすることができます。

始める前に

このプロシージャーは、ターゲット・コンピューター上の TEPS データベースを上書きします。

このタスクについて

ターゲット・ポータル・サーバーがインストールされた Linux または UNIX コンピューター上で、以下のステップを実行し、Window コンピューターから migrate-export を使用してコピーされた TEPS データベースをインポートします。

手順

1. ターゲット・システム上のポータル・サーバーを停止します。
2. ソース・システム上でコマンド・プロンプトを開きます (「**スタート**」→ **ファイル名を指定して実行**」をクリックし、CMD と入力します)。
3. migrate-export.bat スクリプトによってソース Windows システムから生成した **saveexport.sql** をターゲット・システムの *install_dir* /*$platform*/cq/sqllib ディレクトリーにコピーします。ここで、*$platform* は、宛先システムが Intel Linux の場合には li6243、宛先システムが zSeries® Linux の場合には ls3263 となります。
4. ターゲット・システム上で端末ウィンドウを開きます。
5. Tivoli Monitoring インストール済み環境の bin サブディレクトリー (*Install_dir*/bin) に移動します。 例:

   ```
   cd /opt/IBM/ITM/bin
   ```

6. 端末ウィンドウで、./itmcmd execute cq "runscript.sh migrate-import.sh" と入力します。 単一引用符 (') ではなく、必ず二重引用符 (") を使用するようにしてください。このスクリプトは、*install_dir* /*$platform*/cq/sqllib ディ

レクトリーにある **saveexport.sql** という名前のファイルを処理します。 saveexport.sql ファイルの内容に応じて、このプロセスによって既存のポータル・サーバー・データを完全に置き換えることができます。

7. migrate-import 機能を使用して TEPS データベースをあるリリースから別のリリースへ移動中の場合は、以下のようにデータベースをマイグレーションしてアプリケーション・サポートを追加した後、このタスクを実行します。
   a. *Install_dir*/cq/bin/lnxnocmsenv をテキスト・エディターで開きます。
   b. KFW_MIGRATE_FORCE=Y を設定した後、ファイルを保存して閉じます。
   c. 次のスクリプトを呼び出して、現行のポータル・サーバーのアプリケーション・サポートを新しくマイグレーションされた TEPS データベースに適用します (*Install_dir*/bin/itmcmd execute cq InstallPresentation.sh)。 例:

      ```
      /opt/IBM/ITM/bin/itmcmd execute cq InstallPresentation.sh
      ```

8. *Install_dir*/bin ディレクトリーから以下のコマンドを使用してポータル・サーバーを再始動します。

   ```
   ./itmcmd agent start cq
   ```

ソース Linux またはソース UNIX からターゲット Windows への migrate-import の実行

migrate-import スクリプトを実行すると、Linux コンピューターまたは UNIX コンピューターから Windows コンピューターへ、Tivoli Enterprise Portal Server データベースのコピーをインポートすることができます。

始める前に

このプロシージャーは、ターゲット・コンピューター上の TEPS データベースを上書きします。

このタスクについて

ターゲット・ポータル・サーバーがインストールされた Windows コンピューター上で、以下のステップを実行し、Linux または UNIX コンピューターから migrate-export を使用してコピーされた TEPS データベースをインポートします。

手順

1. ターゲット・システム上のポータル・サーバーを停止します。
2. migrate-export スクリプトによってソース Linux またはソース UNIX システム (/opt/IBM/ITM/$platform/cq/sqllib) から生成したファイル **saveexport.sql** をターゲット・システム上の *install_dir* ¥CNPS¥sqllib にコピーします。
3. ターゲット・システム上で *install_dir* ¥CNPS ディレクトリーに移動し、migrate-import と入力します。 ポータル・サーバーが現在実行中の場合に migrate-import プロセスを実行すると、ポータル・サーバーは停止します。
4. migrate-import 機能を使用して TEPS データベースをあるリリースから別のリリースへ移動中の場合は、以下のようにデータベースをマイグレーションしてアプリケーション・サポートを追加した後、このタスクを実行します。
   a. <*install_dir*>¥CNPS¥kfwalone をテキスト・エディターで開きます。
   b. KFW_MIGRATE_FORCE=Y を設定した後、ファイルを保存して閉じます。

c. このスクリプトを呼び出して、現行のポータル・サーバーのアプリケーション・サポートを新しくマイグレーションされた TEPS データベースに適用します (<*install_dir*>¥CNPS¥buildpresentation.bat)。

5. ポータル・サーバーを再始動します。
6. Tivoli Enterprise Portal Serverを再始動します。

ソース Linux またはソース UNIX から、ターゲット Linux またはターゲット UNIX への migrate-import の実行

migrate-import スクリプトを実行すると、Linux または UNIX コンピューターから別の Linux または UNIX コンピューターへ、Tivoli Enterprise Portal Server データベースのコピーをインポートすることができます。

始める前に

このプロシージャーは、ターゲット・コンピューター上の TEPS データベースを上書きします。

このタスクについて

ターゲット・ポータル・サーバーがインストールされた Linux または UNIX コンピューター上で、以下のステップを実行し、別の Linux または UNIX コンピューターから migrate-export を使用してコピーされた TEPS データベースをインポートします。

手順

1. ターゲット・システム上のポータル・サーバーを停止します。
2. migrate-export スクリプトによってソース Linux またはソース UNIX システム *install_dir* /*$platform*/cq/sqllib ディレクトリーから生成されたファイル **saveexport.sql** を、ターゲット・システムの同じディレクトリーにコピーします。ここで、*install_dir* は、/opt/IBM/ITM/ など、宛先システム上のインストール・ディレクトリーで、*$platform* は、li6243 for Intel Linux や ls3263 for zSeries Linux などのオペレーティング・システムです。
3. ターゲット・システム上で端末ウィンドウを開きます。
4. Tivoli Monitoring インストール済み環境の bin サブディレクトリー (*Install_dir*/bin) に移動します。 例:

   ```
   cd /opt/IBM/ITM/bin
   ```

5. 端末ウィンドウで、次のコマンドを入力します。

   ```
   ./itmcmd execute cq "runscript.sh migrate-import.sh"
   ```

   単一引用符 (') ではなく、必ず二重引用符 (") を使用するようにしてください。このスクリプトは、IBM/ITM/$platform/cq/sqllib サブディレクトリーにある saveexport.sql という名前のファイルを処理します。 saveexport.sql ファイルの内容に応じて、このプロセスによって既存のポータル・サーバー・データを完全に置き換えることができます。
6. migrate-import 機能を使用して TEPS データベースをあるリリースから別のリリースへ移動中の場合は、以下のようにデータベースをマイグレーションしてアプリケーション・サポートを追加した後、このタスクを実行します。

a. *Install_dir*/cq/bin/lnxnocmsenv をテキスト・エディターで開きます。
b. KFW_MIGRATE_FORCE=Y を設定した後、ファイルを保存して閉じます。
c. 次のスクリプトを呼び出して、現行のポータル・サーバーのアプリケーション・サポートを新しくマイグレーションされた TEPS データベースに適用します (*Install_dir*/bin/itmcmd execute cq InstallPresentation.sh)。 例:

```
/opt/IBM/ITM/bin/itmcmd execute cq InstallPresentation.sh
```

7. *Install_dir*/bin ディレクトリーから以下のコマンドを使用してポータル・サーバーを再始動します。

```
./itmcmd agent start cq
```

付録 A. SOAP サーバー用の IBM Tivoli Monitoring Web サービス

この付録では、SOAP サーバーの IBM Tivoli Monitoring Web サービス機能について説明します。IBM Tivoli Monitoring Web サービス・ソリューションは、IBM Tivoli Monitoring ソリューションに業界標準のオープン・インターフェースを提供します。このオープン・インターフェースを使用すると、Tivoli のパフォーマンスおよび可用性のデータに簡単にアクセスできるため、自動化および統合の拡張機能にこの情報を使用できます。

IBM Tivoli Monitoring Web サービスは、クライアント/サーバー・アーキテクチャーを実装します。クライアントは、ハブ・モニター・サーバーにインストールされている SOAP サーバーに Simple Object Access Protocol (SOAP) 要求を送信します。サーバーはクライアントから SOAP 要求を受信し、その要求を処理します。

定義済み SOAP メソッドを使用すると、モニター対象環境内で多数の関数を実行できます。SOAP メソッドの使用は即時に開始できます。これらの SOAP メソッドを、独自の拡張メソッドを作成するときのテンプレートとして使用することもできます。

SOAP は、任意のプログラミング言語またはスクリプト言語、任意のオブジェクト・モデル、および任意のインターネット・ワイヤー・プロトコルと組み合わせて使用できます。Tivoli SOAP メソッドは、
PERL、Javascript、VBSCRIPT、JSCRIPT、C++、Java、およびブラウザーを使用して呼び出すことができます。

注: Web サービスは、シチュエーションの作成をサポートしません。シチュエーションの作成には、Tivoli Enterprise Portal シチュエーション・エディターまたは CLI **tacmd createSit** 関数を使用してください。 SOAP サーバーが照会できるのは、エージェントおよび管理対象システム属性だけです。

SOAP クライアントについて

Simple Object Access Protocol (SOAP) は、インターネット経由でのアプリケーション間の情報交換を可能にする XML ベースの通信プロトコルです。

SOAP は、プラットフォームや言語には依存していません。SOAP は、要求および応答の構造を指定するために XML を使用します。要求の発行および応答の受信のためのトランスポート・メカニズムとして HTTP を使用します。

重要: IBM のソリューションを使用するにあたっては、SOAP、Extensible Markup Language (XML) と XML ネーム・スペース、および Web サービス記述言語 (WSDL) についての基本的な知識が必要です。

Tivoli Monitoring Web Services の構成 (SOAP サーバー)

デフォルトでは、SOAP サーバーはハブ Tivoli Enterprise Monitoring Server にインストールされます。ハブ・モニター・サーバー間で SOAP サーバー通信を確立し、SOAP サーバーでセキュリティーを確保するには、構成トピックを参照してください。

この章では、SOAP、XML と XML ネーム・スペース、および Web サービス記述言語 (WSDL) についての基本的な知識があることを前提としています。以下は、SOAP の構成に必要なステップです。

- SOAP サーバーが通信するハブを定義します。
- ユーザーを作成して、アクセス権限を付与します。
- SOAP を正常に構成したことを確認します。

注: 旧バージョンの SOAP サーバーに SOAP 要求を出すことはできません。

ハブの定義

以下の手順では、Tivoli Enterprise Monitoring Services の管理 を使用して、SOAP サーバーを活動化し、SOAP サーバーと通信するハブを定義します。

このタスクについて

SOAP ハブを定義するには、以下のステップを使用します。

手順

1. ハブ・モニター・サーバーがインストールされているコンピューターで、「Tivoli Enterprise Monitoring Services の管理」を開始します。
   a. Windows 「**スタート**」 → 「**プログラム**」 → 「**IBM Tivoli Monitoring**」 → 「**Tivoli Enterprise Monitoring Services の管理**」の順にクリックします。
   b. Linux または UNIX *install_dir* /binディレクトリーに移動し、`./itmcmd manage` と入力します。
2. Tivoli Enterprise Monitoring Server を右クリックして、「**再構成**」をクリックします。
3. □「**セキュリティー: ユーザーを検証**」フィールドを選択またはクリアします。
4. Tivoli Enterprise Monitoring Services の管理 を開きます。
5. **Tivoli Enterprise Monitoring Server**を右クリックします。
6. 「**拡張**」→「**SOAP サーバー・ハブの構成**」をクリックします。
7. 「**ハブの追加**」をクリックします。「ハブの指定」ウィンドウが表示されます。
8. 「**プロトコル**」メニューから、使用する通信プロトコルを選択します。
9. 「**別名**」フィールドで別名を指定します (例えば、HUB2)。別名は、最小 3 文字、最大 8 文字で指定します。
10. 以下のいずれかのステップを実行します。
    a. TCP/IP または TCP/IP パイプ通信を使用する場合は、以下のフィールドに入力します。

表 67. 「ハブの指定」ダイアログの TCP/IP フィールド

フィールド	説明
ホスト名または IP アドレス	ホスト・コンピューターのホスト名または TCP/IP アドレス。
ポート	ホスト・コンピューターの TCP/IP listen ポート。

b. SNA 通信を使用する場合は、以下のフィールドに入力します。

表 68. 「ハブの指定」ダイアログの SNA フィールド

フィールド	説明
ネットワーク名	ご使用のサイトの SNA ネットワーク ID。
LU 名	モニター・サーバーの LU 名。この LU 名は、SNA 通信ソフトウェアにおける「ローカル LU の別名」に対応します。
LU6.2 ログモード	LU6.2 ログモードの名前。デフォルト: CANCTDCS。
TP 名	モニター・サーバーのトランザクション・プログラム名。

注: リモート・モニター・サーバーに接続する場合は、プロトコル情報は、ハブ・モニター・サーバーに使用される情報と同じでなければなりません。

11. 「**OK**」をクリックします。 サーバー・ツリーが表示されます。

ユーザーの追加

以下の手順に従って、各ハブでユーザーを定義し、ユーザーごとにアクセス権限 (照会または更新) を指定します。

このタスクについて

ユーザーを定義し、アクセス権限を指定するには、以下の手順を実行します。

手順

1. 必要な場合は、サーバーを選択します (表示されるサーバー・ツリー内の任意の場所をクリックします)。
2. 「ユーザー・データの追加」に、ユーザー名を入力します。ユーザー ID は、モニター・サーバーのログオン時の検証で指定された ID と同一である必要があります。アクセスできるモニター・サーバーは、ユーザーがアクセス権を持つモニター・サーバーのみに限定されます。

   注: ユーザー ID を指定しない場合は、すべてのユーザーにデータを更新する許可が与えられます。
3. ユーザー・アクセスのタイプとして「**照会**」または「**更新**」をクリックします。
4. 「**ユーザーの追加**」をクリックします。サーバー・ツリーが更新され、ユーザーとアクセスのタイプが表示されます。
5. ユーザーを削除するには、ツリーからユーザー名を選択し、「**項目の削除**」をクリックします。

6. ハブを削除するには、ハブのツリー内の任意の場所をクリックし、「**ツリーのクリア**」をクリックします。

   重要: SOAP セキュリティーが有効の場合、ユーザーの「**照会**」許可と「**更新**」許可により、ハブ・モニター・サーバーへの要求および他の SOAP クライアントからの要求を送信する **tacmd** コマンドの許可が制御されます。SOAP CT_EMail および CT_Export 要求を発行できるユーザーを制御する場合は、ハブ・モニター・サーバーの SOAP_IS_SECURE 環境変数も YESに設定する必要があります。

   照会許可では、ユーザーは作成操作、更新操作、削除操作、およびコマンドのリモート・デプロイおよび実行のための **tacmd** コマンド (**executeaction** や **executecommand** など) を実行することはできません。

   更新許可は、すべての SOAP 操作を実行するための許可を付与し、ハブ・モニター・サーバーに要求を送信するすべての **tacmd** コマンド (**tacmd getFile** コマンドと **tacmd putFile** コマンドを除きます) に適用されます。**tacmd getFile** コマンドと **tacmd putFile** コマンドを実行するための許可は、ハブ・モニター・サーバーの KT1_TEMS_SECURE 環境変数によって制御されます。これら 2 つのコマンドを実行するための許可を有効にする方法について詳しくは、「*IBM Tivoli Monitoring コマンド・リファレンス*」を参照してください。

UNIX および Linux システムでの IBM Tivoli Monitoring Web Services (SOAP サーバー) の構成

UNIX および Linux コンピューター上の SOAP サーバーを構成します。

このタスクについて

以下のステップを実行して、UNIX または Linux 上で「Tivoli Enterprise Monitoring Services の管理」を使用して SOAP ハブを定義します。

手順

1. *install_dir* /bin ディレクトリーに移動し、以下のコマンドを入力して Tivoli Enterprise Monitoring Services の管理 を開始します。

   ```
   ./itmcmd manage
   ```

   「Tivoli Enterprise Monitoring Services の管理」ウィンドウが表示されます。
2. 「**Tivoli Enterprise Monitoring Server**」を右クリックし、ポップアップ・メニューから「**構成**」を選択します。 「TEMS の構成 (Configure TEMS)」ウィンドウが表示されます。
3. 「**保存**」をクリックします。 「SOAP サーバー・ハブ構成」ウィンドウが表示されます。現行ホストが「ハブ」ツリーに表示されない場合は、ホストを定義してからそれが通信するハブを定義してください。
4. ハブ・モニター・サーバーのホスト名または IP アドレス、ポート番号、プロトコルが正しいことを確認します。正しくない場合は、訂正してください。 ローカル・ハブの名前がツリーに表示されない場合は、ローカル・ハブを定義してからそれが通信するハブを定義してください。ローカル・ハブの別名は、常に「SOAP」でなければなりません。
5. 別のハブを追加する手順は、次のとおりです。

a. ホストの名前または IP アドレス、およびポート番号を該当フィールドに入力します。
b. 「**別名**」フィールドに別名を指定します。 別名は、最小 3 文字、最大 8 文字で指定します (例: HUB2)。
c. 「**トランスポート**」メニューから、そのハブで使用する通信プロトコルを選択します。

6. 「**ホストの追加**」をクリックします。 サーバー・ツリーが、新しく定義されたハブと一緒に表示されます。

AIX システム上での SOAP トランザクションのパフォーマンスを調整

遅延確認応答を許可するかしないかを決定することにより、AIX での SOAP トランザクション・パフォーマンスを変更できます。このパフォーマンスを調整するには、以下の手順に従います。

このタスクについて

Transmission Control Protocol (TCP) 接続の場合、AIX システムでは、デフォルトで遅延確認通知 (*Ack* パケット) が最大 200 ms まで許可されます。この動作は、**tcp_nodelayack** ネットワーク・オプションによって制御されます。この遅延により、パケットを応答と組み合わせてシステムのオーバーヘッドを最小化することができます。**tcp_nodelayack** を **1** に設定すると、確認通知は即時に送信側に返されます。この設定により、送信側が受信側からの確認通知を待っている場合に、システム・オーバーヘッドが若干多く生成されますが、ネットワーク転送のパフォーマンスが大幅に向上します。**tcp_nodelayack** オプションの詳細については、IBM System p® および AIX インフォメーション・センター・ホームを参照してください。

このパラメーターを設定するには、次の手順で行います。

手順

root 特権を持っているユーザー・アカウントにアクセスし、次のコマンドを実行します。

```
no -p -o tcp_nodelayack=1
```

タスクの結果

通常、次の出力が表示されます。

```
Setting tcp_nodelayack to 1
Setting tcp_nodelayack to 1 in nextboot file
```

これは、すぐに有効になる動的変更です。**-p** フラグは変更を永続的にするため、次回オペレーティング・システムを始動したときも、変更が有効になります。

SOAP セキュリティーの使用可能化

ハブ・モニター・サーバーを構成するときに「**セキュリティー: ユーザーの検証**」オプションを有効にした場合、CT_EMail 要求と CT_Export 要求を除くすべての SOAP 要求が認証されます。

SOAP ユーザーを検証するようにハブ・モニター・サーバーを構成する方法について詳しくは、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」を参照してください。CT_EMail または CT_Export SOAP 要求を送信している SOAP ユーザーも認証するには、ハブ・モニター・サーバーで SOAP_IS_SECURE 環境変数を有効にする必要があります。

このタスクについて

SOAP_IS_SECURE 環境変数は、デフォルトでは無効になっていますこの変数を使用可能にするには、CT_EMail または CT_Export 要求を実行依頼するすべてのユーザーが、ハブ・モニター・サーバーの資格情報を把握している必要があります。
SOAP_IS_SECURE=YES の設定は、ハブ・モニター・サーバーでユーザー検証が有効になっている場合にのみ機能します。

手順

1. 次のようにして、ハブ・モニター・サーバーがインストールされているコンピューターで KBBENV または ms.ini ファイルを開きます。

   Windows

   Tivoli Enterprise Monitoring Services の管理 (「スタート」→「プログラム」→「IBM Tivoli Monitoring」→「Tivoli Enterprise Monitoring Services の管理」) を使用して、環境ファイルを編集します。変更するコンポーネントを右クリックして、「**拡張**」→「**ENV ファイルの編集**」をクリックします。変更内容を実装するには、コンポーネントをリサイクルする必要があります。

   Linux UNIX

   環境ファイルを直接編集します。<*install_dir* >/config/ms.ini ファイル内の環境変数を編集します。
2. # SOAP_IS_SECURE=YES という行を見つけてコメント化を解除します。 例: SOAP_IS_SECURE=YES
3. モニター・サーバー環境ファイルを保存して閉じます。
4. Windows の場合、変更内容を実装するには、コンポーネントをリサイクルする必要があります。Linux または UNIX の場合、変更内容を実装するには、モニター・サーバーを再構成してリサイクルする必要があります。

IBM Tivoli Monitoring Web サービスの使用

IBM Tivoli Monitoring Web サービスには、多数の SOAP メソッドが組み込まれています。これらのメソッドを使用すると、IBM Tivoli Monitoring 環境を動的に照会および制御できます。

この SOAP メソッドを使用すると、次の操作が可能になります。

- ポリシーおよびシチュエーションを停止または開始する
- System Automation for Integrated Operations Management からのトラップ・メッセージを転送し、そのメッセージを Universal Message コンソール上に表示する
- 図表内またはレポート内に表示できる属性データを検索する
- イベントをオープンおよびクローズする
- データをリアルタイムに要求する

- Tivoli Enterprise Portal 内のシステム・コマンドとして SOAP 要求を発行する

この製品を使用して、要求が正しく機能するかどうかをテストすることもできます。その後、複数の要求の処理を実行依頼するポリシーを作成できます。また、日常の処理の要約を生成することもできます。

ヒストリカル・データ収集ガイドで説明したように、Tivoli Data Warehouse 内に検索済みデータを格納できます。

注: IBM Tivoli Monitoring Web サービスは、XML データ行を提供します。グラフおよび表内にデータを表示するには、IBM の SOAP メソッドと独自のスクリプトを組み合わせて使用します。

SOAP 照会応答はアルファベット順になっているように見えますが、アルファベット順に従っていない属性もあります。自動化タスクは、順序に関係なく内容を調べる必要があります。

ユーザー ID

インストール時および構成時に、モニター・サーバー・データへのアクセス権を必要とするユーザーのユーザー ID を指定するように求められます。ユーザー ID を指定しないと、すべてのユーザーにデータを更新する許可が与えられます。

ユーザー ID は、モニター・サーバーのログオン時の検証で指定された ID と同一である必要があります。アクセスできるモニター・サーバーは、ユーザーがアクセス権を持つモニター・サーバーのみに限定されます。

モニター・サーバー・データへのユーザーのアクセス権の追加または削除は、後で変更することもできます。詳しくは、「*IBM Tivoli Monitoring: インストールおよび設定ガイド*」を参照してください。

SOAP クライアントの開始と要求の作成

Internet Explorer または SOAP クライアント・コマンド行ユーティリティー (z/OS システムでは使用できません) を使用して、SOAP クライアントを開始します。

このタスクについて

SOAP クライアントを Internet Explorer とともに使用して SOAP 要求を発行するときには、必要に応じてタグまたはテキストを変更できます。これに対して、コマンド行ユーティリティーは、単に、コマンド行に要求の出力を表示するだけです。

注: 新規に作成した Universal Agent オブジェクトにアクセスできるようにするには、SOAP サーバーが実行されているハブ・モニター・サーバーをリサイクルする必要があります。ハブ・モニター・サーバーの構成手順については、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」を参照してください。

ブラウザーの使用方法

Windows Internet Explorer または Mozilla Firefox を使用して、SOAP サービス・コンソールの URL を入力します。

このタスクについて

Tivoli Monitoring Web Services SOAP クライアントをインストールした後で、次のアクションを実行します。

手順

1. Internet Explorer バージョン 5 以降または Mozilla Firefox を開始します。Internet Explorer のセキュリティー設定で「**ドメイン間でのデータ ソースのアクセス**」オプションが有効になっていることを確認します。
2. 「アドレス」フィールドで、SOAP クライアントの URL を入力します。同じシステム上で実行される SOAP サーバーにアクセスするときには、`localhost` をリテラル定数として使用できます。この値を、別のシステム上で実行される SOAP サーバーの適切なホスト名またはネットワーク・アドレスに変更することもできます。

   ```
   http://localhost:1920///cms/soap/kshsoap.htm
   ```

   HTTP サービスのポート番号は 1920 です。

   注: 「アドレス」フィールド内の **soap** をアクセス先のハブの別名 (以下の例では **HUB_localhost**) に置き換えることにより、要求をリモート・ハブに経路指定することもできます。別名は、SOAP サーバーに事前に定義しておく必要があります (ハブ別名の定義について詳しくは、インストールに関する文書を参照してください)。例: `http://localhost:1920///cms/HUB_localhost/kshsoap.htm`
   SOAP クライアント HTML ページが表示されます。
3. 最初のフィールド内のリストから SOAP メソッドを選択します。メソッドを選択すると、その他のフィールドに値が自動的に更新されます。
4. 必要な場合には、「ペイロードの編集 (XML) (Edit Payload (XML))」領域内でタグまたはテキストを変更します。
5. 「**SOAP 要求の作成 (Make SOAP Request)**」をクリックします。 要求の出力が「SOAP 応答ペイロード (Your SOAP Response Payload)」領域内に表示されます。

次のタスク

特定のエージェント・タイプに対して CT_Get 要求を発行する場合、SOAP サーバーを実行しているモニター・サーバーは、そのエージェント・タイプに応じて構成され、同エージェント・タイプに応じたアプリケーション・サポートがインストールされている必要があります。例えば、z/OS モニター・サーバーに接続している z/OS エージェントに CT_Get 要求を発行する場合、SOAP サーバーを実行しているモニター・サーバーは、その z/OS エージェントに応じて構成され、同エージェントに応じたアプリケーション・サポートがインストールされている必要があります。

SOAP クライアント・コマンド行ユーティリティー (kshsoap) の使用

SOAP クライアント・コマンド行ユーティリティー (kshsoap) は HTTP クライアントです。直接 SOAP 要求を発行し、出力をコマンド行に表示します。

このタスクについて

SOAP 要求ファイル、SOAP URL 受信側ファイルを作成して、要求を送信するには、以下のステップを実行します。

手順

- Windows
  1. SOAP サーバーがインストールされている Tivoli Enterprise Monitoring Server システムで、*install_dir* ¥cms ディレクトリーに移動します。
  2. 「SOAPREQ.txt」という名前のテキスト・ファイルを作成し、次の SOAP 要求を入力します。

     ```
     <CT_Get><object>ManagedSystem</object></CT_Get>
     ```

     セキュリティーが有効になっている場合は、次のように入力します。

     ```
     <CT_Get><userid>logonid</userid><password>password</password>
     <object>ManagedSystem</object></CT_Get>
     ```
  3. SOAP 要求を受信する URL を含む、「URLS.txt」という名前の別のテキスト・ファイルを作成します。 この例では、affiliatecompanylocalhost は受信システムの名前であり、ハブ・モニター・サーバーのインストール先です。

     ```
     http://affiliatecompanylocalhost:1920///cms/soap
     ```
  4. コマンド行で、**kshsoap SOAPREQ.txt URLS.txt** と入力します。
- Linux UNIX *install_dir* /*interp*/ms/bin ディレクトリーにある kshsoap スクリプトを実行します。 kshsoap クライアントを呼び出す前に、モニター・サーバー構成の設定を現行シェルに取り込む必要があります。設定を取り込むには、次のコマンドを入力します。 *install_dir* /config/*hostname*_ms_*temsname*.config。このステップを検証するには、***env*** コマンドを使用して環境変数を表示し、項目を .config ファイルに指定されているものと比較します。
- APPN がインストールされたシステム上で **kshsoap** コマンドを実行すると、APPN ファイルの構成が必要であることを示すエラー・メッセージが表示されることがあります。この状態を解決するには、**kshsoap** コマンドを実行するコマンド行ウィンドウから環境変数 **KDE_WAPPC32** を変更します。

  ```
  SET KDE_WAPPC32=none
  ```

タスクの結果

この kshsoap ユーティリティーは、SOAPREQ ファイルを処理し、URL 宛先と要求を表示します。URLS ファイル内にリストされた各 URL に SOAP 要求を送信し、その後で URL および受信した応答メッセージを表示します。

システム・コマンドとしての SOAP 要求の発行

Tivoli Enterprise Portal で、「アクションの実行」機能を使用して、ポリシーまたはシチュエーション内で SOAP 要求をシステム・コマンドとして発行できます。

SOAP 要求はテキスト・ファイル内に格納されます。詳しくは、*Tivoli Enterprise Portal* ユーザーズ・ガイド の アクションの指定 および アクション設定 のトピックを参照してください。

soap コマンドは次のとおりです。

```
soap:CT_Execute,filename=SOAPREQ
```

ここで:

CT_Execute は、ファイルに保管されている SOAP 要求を実行することができる SOAP メソッドの名前です。

SOAPREQ は、CT_EMail SOAP 要求が含まれている、ユーザーが作成したファイルの名前です。

以下に、SOAPREQ の例を示します。

```
<CT_EMail><server>n-smtpmta</server>
<sender>soap@ibm.com</sender>
<receiver>jane_brown@ibm.com</receiver>
<subject>AFDATA untouched by human hands</subject>
<attachmenttitle>AFData.htm</attachmenttitle>
<request><attach>res.pfx</attach></request>
<request id="XMLID">
<CT_Redirect endpoint="http://sp22.ibm.com:18882">
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
  "http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" >
<SOAP-ENV:Body><AF_Execute><Exec>SOAP0002</Exec></AF_Execute></SOAP-ENV:Body>
  </SOAP-ENV:Envelope></CT_Redirect></request>
<request><attach>res.sfx</attach></request></CT_EMail>
```

SOAP メソッド

定義済み SOAP メソッドを使用して、
PERL、Javascript、VBSCRIPT、JSCRIPT、C++、Java、およびブラウザーによる呼び出し要求を構成します。各メソッドには、サポートされているタグと使用法の例のリストがあります。ここでは、IBM が提供する各 SOAP メソッドと、各メソッドがサポートしているタグについて説明します。

CT_Acknowledge

イベント確認応答を IBM Tivoli Monitoring プラットフォームに送信します。

<name>
シチュエーションの名前。これは必須です。

<source>
イベントのソース (エージェント名またはモニター・サーバー名)。ソースが指定されていない場合、指定されたアラートのすべてのアクティブなソースに確認応答が送信されます。

<data>
これが指定されていない場合は、「データが指定されていません (No data was provided)」が挿入されます。

<item> 表示項目です。

<userid>
オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
オプションです。 ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<type> オプションです。 イベント・タイプを指定します。値は、「sampled」または「0」、「pure」または「1」、および「meta」または「2」です。デフォルト: 「**sampled**」

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

<expire>
オプションです。 ここに入力された分数が経過すると、確認応答の有効期限が切れます。

以下に例を示します。

```
<CT_Acknowledge>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <data>Jack is taking care of this failure</data>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
  <type>pure</type>
  <expire>60</expire>
</CT_Acknowledge>
```

CT_Activate

IBM Tivoli Monitoring プラットフォームで実行されるシチュエーションまたはポリシーを開始します。

注: リモートの Tivoli Enterprise Monitoring Server に接続するエージェントのシチュエーションを、このメソッドを使用して開始することはできません。

<name>
シチュエーションの名前。これは必須です。

<type>
活動化されるオブジェクトのタイプ。これは必須です。

<userid>
オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

以下に例を示します。

```
<CT_Activate>
  <hub>z/OSPROD</hub>
  <name>name_of_situation_or_policy</name>
  <type> situation</type>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Activate>
```

CT_Alert

イベントを IBM Tivoli Monitoring プラットフォームに送信します。

<name>
シチュエーションの名前。これは必須です。

<source>
イベントのソース (エージェント名またはモニター・サーバー名)。これは必須です。

<data>
これが指定されていない場合、またはオプションの object.attribute タグが指定されていない場合は、「データが指定されていません (No data was provided)」が挿入されます。

<item> 表示項目です。

<userid>
オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
オプションです。 ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<type> オプションです。 イベント・タイプを指定します。値は、「sampled」または「0」、「pure」または「1」、および「meta」または「2」です。デフォルト: 「**sampled**」

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

<data><object.attribute>
指定されている属性 (複数可) の値をイベント結果ワークスペースの「初期属性 (Initial Attributes)」ビューに返します。

以下に例を示します。

```
<CT_Alert>
  <hub>z/OSPROD</hub>
  <name>situation_from_XXX</name>
  <source>XXX_supported_system</source>
  <data><NT_Logical_Disk.Disk_Name>
C:</NT_Logical_Disk.Disk_Name></data>
```

```
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Alert>
```

注: data タグ内で object.attribute を指定するときには、下線 (_) 以外の非英数字を除外してください。例えば、NT_System.%_Total_Processor_Time は NT_System.Total_Processor_Time として入力します。

CT_Deactivate

IBM Tivoli Monitoring プラットフォーム上のシチュエーションまたはポリシーを停止します。

注: このメソッドを使用して、リモート Tivoli Enterprise Monitoring Server に接続するエージェントのシチュエーションを停止することはできません。

<name>
シチュエーションまたはポリシーの名前です。これは必須です。

<type> オブジェクトのタイプ (シチュエーションまたはポリシー)。これは必須です。

<userid>
ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

以下に例を示します。

```
<CT_Deactivate>
  <hub>z/OSPROD</hub>
  <name>name_of_situation_or_policy</name>
  <type>situation</type>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Deactivate>
```

CT_EMail

CT_Get などの別の CT SOAP メソッドからの出力を、電子メールを使用して SMTP サーバー経由で定義済み電子メール・アドレスに送信します (z/OS では使用不可)。

<server>
SMTP サーバー名/ネットワーク・アドレスは必須です。

<sender>
送信側の電子メール・アドレスは必須です。

<receiver>
受信側の電子メール・アドレスは必須です。

<subject>
オプションです。 電子メールの件名です。

<message>
オプションです。 電子メール・メッセージです。

<attachmenttitle>
オプションです。 添付ファイルのタイトルです。

<request>
CT_GET などの第 2 レベルの要求を指定する場合は、<request> </request> タグ内に各サブ要求を含める必要があります。

オプション: id=" " エレメントを <request> タグに追加すると、そのサブ要求に対応する応答を囲む <request id="XMLID"> エレメントが生成されます。

追加のセキュリティーが有効になっている場合 (モニター・サーバー環境変数の SOAP_IS_SECURE=YES)、以下のタグも必要です。

<userid>
ハブ・モニター・サーバーにアクセスするためのユーザー ID です。

<password>
ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーのログオン時の検証のために必須です。

以下に例を示します。

```
<CT_EMail>
  <server>smtp.server</server>
  <sender>myemail@something.com </sender>
  <receiver>youremail@whatever.com </receiver>
  <subject>Here's your data.</subject>
  <message>Table data supplied as attachment below. It is
  presented in csv format to be used by MS/Excel.</message>
  <attachmenttitle>tabledata.csv</attachmenttitle>
  <request id="XMLID">
    <CT_Get>
      <object>NT_Process </object>
      <target>TlPrimary:DCSQLSERVER:NT</target>
      <userid>sysadmin</userid>
      <password>xxxxxxxx</password>
    </CT_Get>
  </request>
</CT_EMail>
```

追加セキュリティーの例:

```
<CT_EMail>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
  <server>smtp.server</server>
  <sender>myemail@something.com </sender>
  <receiver>youremail@whatever.com </receiver>
  <subject>Here's your data.</subject>
  <message>Table data supplied as attachment below. It is
  presented in csv format to be used by MS/Excel.</message>
  <attachmenttitle>tabledata.csv</attachmenttitle>
  <request id="XMLID">
    <CT_Get>
```

```
   <userid>sysadmin</userid>
   <password>xxxxxxxx</password>
       <object>NT_Process </object>
       <target>TlPrimary:DCSQLSERVER:NT</target>
    </CT_Get>
  </request>
</CT_EMail>
```

この追加のセキュリティーにより、CT_EMail は許可のためにユーザー ID とパスワードを要求します。 CT_Get が指定されている場合は、同じ資格情報を使用して CT_Get が実行されます。

CT_Execute

ファイル内に保管されている SOAP 要求を実行します。

<filename>

実行する SOAP 要求が含まれているファイル名を指定します。このファイルは ¥html ディレクトリー内になければなりません。z/OS では、ファイルは RKANDATV になければなりません。これは必須です。

以下に例を示します。

```
<CT_Execute>
  <filename>execute1.xml</filename>
</CT_Execute>
```

CT_Export

CT_GET などの別の CT SOAP メソッドからの出力を、定義済みファイルに送信します (z/OS では使用できません)。

<filename>

エクスポートされたデータを格納するファイルの名前。これは必須です。

注: C++ など特定のプログラム言語の引用符付きストリング・リテラルに filename タグを挿入するときには、バックスラッシュを 2 つ並べて指定する必要があります。

<filename> タグには、オプションの date/time スタンプ変数を追加できます。変数はドル記号 ($) で囲まれ、yy/mm/dd/hh/mm/ss の組み合わせ (年/月/日/時/分/秒に対応) を格納できます。date/time スタンプ属性は、任意の順序で指定できますが、mm の前には yy または hh を配置する必要があります。これは、mm が月 (年の後) であるか分 (時の後) であるかを識別するためです。例:

```
<filename>g:¥exchange¥excel¥ntprocess$yymmdd$.htm</filename>
```

<warehouse/>

ODBC を使用して Tivoli Enterprise Portal データウェアハウスにデータをエクスポートすることを指定します。<filename> および <warehouse/> は相互に排他的ですが、いずれか 1 つを指定する必要があります。

<request>

CT_GET などの第 2 レベルの要求を指定する場合は、<request> </request> タグ内に各サブ要求を含める必要があります。

オプション: id=" " エレメントを <request> タグに追加すると、そのサブ要求に対応する応答を囲む <request id="XMLID"> エレメントが生成されます。

追加のセキュリティーが有効になっている場合 (モニター・サーバー環境変数の SOAP_IS_SECURE=YES)、以下のタグも必要です。

<userid>
ハブ・モニター・サーバーにアクセスするためのユーザー ID です。

<password>
ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーのログオン時の検証のために必須です。

以下に例を示します。

```
<CT_Export>
  <filename>g:¥exchange¥excel¥ntprocess$yymmddhhmmss$.htm</filename>
  <request>
    <attach>prefix.xsl</attach>
  </request>
  <request id="XMLID">
    <CT_Get>
      <object>NT_Process</object>
      <target>Primary:DCSQLSE RVER:NT</target>
      <userid>sysadmin</userid>
      <password>xxxxxxxx</password>
    </CT_Get>
  </request>
  <request>
    <attach>suffix.xsl</attach>
  </request>
</CT_Export>
```

追加セキュリティーの例:

```
<CT_Export>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
  <filename>g:¥exchange¥excel¥ntprocess$yymmddhhmmss$.htm</filename>
  <request>
    <attach>prefix.xsl</attach>
  </request>
  <request id="XMLID">
    <CT_Get>
   <userid>sysadmin</userid>
   <password>xxxxxxxx</password>
       <object>NT_Process</object>
       <target>Primary:DCSQLSE RVER:NT</target>
    </CT_Get>
  </request>
  <request>
    <attach>suffix.xsl</attach>
  </request>
</CT_Export>
```

この追加のセキュリティーにより、CT_Export は許可のためにユーザー ID とパスワードを要求します。 CT_Get が指定されている場合は、同じ資格情報を使用して CT_Get が実行されます。

CT_Get

任意の IBM Tivoli Monitoring プラットフォーム・エージェントから XML オブジェクトのグループまたは個別の XML オブジェクトを受信します。これを使用して、リアルタイム・データを取得できます。

重要: 特定のエージェント・タイプに対して CT_Get 要求を発行するときには、SOAP サーバーが実行されているモニター・サーバーをそのエージェント・タイプに応じて構成およびシードする必要があります。

<object>
検索されるオブジェクトの名前。必須です (デフォルトでは、オブジェクトのすべての公開エレメントを取り出します)。

<userid>
ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<target>
エージェントの名前。

注意: デフォルトは「*ALL」です。すべての選択可能なターゲットを検索します。

<history>
Y の場合、ヒストリカル・データが使用可能であれば、それを取り出します。

<results>
PARSE の場合は、状況ヒストリー・イベント属性を取り出します。Status_History オブジェクトの場合のみ有効です。複数: 複数の指定が可能です。

<attribute>
オブジェクトの属性名。このタグは複数回指定できます。

<hub>
ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

<afilter>
属性、演算子、値演算子 (EQ、 NE、 GE、 GT、 LE、 LT、 LIKE) などのフィルター基準に一致する行を戻します。LIKE パターン文字:「*」は 1 文字以上に一致します。文字属性でのみサポートされます。複数の afilter は、結合として (例えば、AND を使用して結合する) のみサポートされます。

以下に例を示します。

```
<CT_Get>
  <hub>z/OSPROD</hub>
  <object>NT_System</object>
  <target>Primary:DCSQLSERVER:NT</target>
```

```
  <userid>sysadmin</userid>
  <password></password>
  <history>Y</history>
  <attribute>Server_Name</attribute>
  <attribute>Processor_Queue_Length</attribute>
  <afilter>Write_Time;GT;1020804</afilter>
  <afilter>Write_Time;LT;1020805</afilter>
</CT_Get>
```

注: attribute タグ内で属性を指定するときには、下線 (_) 以外のすべての非英数字を除外してください。例えば、%_Total_User_Time は `Total_User_Time` として入力します。

CT_Redirect

IBM Tivoli Monitoring プラットフォームのドメインの外部にある別の登録済み SOAP メソッドに SOAP 要求を転送します。

<request endpoint=" ">

<request endpoint= " "> の値は、リダイレクトされた SOAP 要求のターゲットを指定している必要があります。request エレメントの値として指定された XML 全体が、そのエンドポイントに送信されます。CT_Redirect が CT_Export などの第 2 レベル要求内で指定された場合、<endpoint=" "> 属性は CT_Redirect メソッド内でのみ 指定されます。これは必須です。

以下に例を示します。

```
<CT_Redirect>
  <request endpoint= ¥"http://services.xmethods.net:80/soap/servlet/rpcrouter¥">
    <SOAP-ENV:Envelope xmlns:SOAP-ENV=¥"http://schemas.xmlsoap.org/soap/envelope/¥">
      <SOAP-ENV:Body>
        <ns1:getTemp xmlns:ns1=¥"urn:xmethods-Temperature¥"SOAP-ENV:
        encodingStyle=¥"http://schemas.xmlsoap.org/soap/encoding/¥">
          <zipcode>93117</zipcode>
        </ns1:getTemp>
      </SOAP-ENV:Body>
    </SOAP-ENV:Envelope>
  </request>
</CT_Redirect>
```

CT_Reset

IBM Tivoli Monitoring プラットフォームにイベント・リセット (クローズ・イベント) を送信します。

<name>

シチュエーションの名前。これは必須です。

<source>

イベントのソース (エージェント名またはモニター・サーバー名)。ソースが指定されていない場合、指定されたアラートのすべてのアクティブ・ソースにリセットが適用されます。

<item> 表示項目です。

<userid>

オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
オプションです。 ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

<type> オプションです。 イベント・タイプを指定します。値は、「sampled」または「0」、「pure」または「1」、および「meta」または「2」です。デフォルト: 「**sampled**」

以下に例を示します。

```
<CT_Reset>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Reset>
```

注: シチュエーションが停止または削除されている場合のみ、サンプル・イベントを閉じることができます。CT_Reset でピュア・イベントを閉じる場合は、<type> タグを使用します。

CT_Resurface

確認されたイベントを IBM Tivoli Monitoring プラットフォームに再表示します。

<name>
シチュエーションの名前。これは必須です。

<source>
イベントのソース (エージェント名またはモニター・サーバー名)。ソースが指定されていない場合は、指定されたアラートのすべてのアクティブなソースに再表示が適用されます。

<item> 表示項目です。

<userid>
オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
オプションです。 ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

<type> オプションです。 イベント・タイプを指定します。値は、「sampled」または「0」、「pure」または「1」、および「meta」または「2」です。デフォルト: 「**sampled**」

以下に例を示します。

```
<CT_Resurface>
  <hub>z/OSPROD</hub>
  <name>situation_from_CT</name>
  <source>CT_supported_system</source>
  <item>subsystem</item>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_Resurface>
```

CT_WTO

IBM Tivoli Monitoring プラットフォームに Universal Message を送信します。

<data>
送信されるメッセージ。これは必須です。

<category>
オプションです。 デフォルトはブランクです。

<severity>
オプションです。 デフォルトはブランクです。

<userid>
オプションです。 ハブ・モニター・サーバーにアクセスするためのユーザー ID です。指定されていない場合は、「nnn.nnn.nnn.nnn」が挿入されます。

<password>
オプションです。 ハブ・モニター・サーバーにアクセスするためのパスワードです。モニター・サーバーまたはハブのログオン時の検証のために必須です。

<hub>
オプションです。 ハブ・リスト内に構成されているリモート・ハブの別名を指定します。SOAP 要求はこのハブに経路指定されます。

以下に例を示します。

```
<CT_WTO>
  <hub>z/OSPROD</hub>
  <data>This is Universal Message</data>
  <category>Critical Messages</category>
  <severity>High Severity</severity>
  <userid>sysadmin</userid>
  <password>xxxxxxxx</password>
</CT_WTO>
```

第 2 レベル SOAP 要求の発行

一部の第 2 レベル SOAP メソッドは、埋め込み下位レベル・メソッドを使用して、検索されたデータを使用する特定の関数を実行します。CT_EMail と CT_Export は、この関数を実行する第 2 レベル・メソッドです。

下位レベル・メソッドは、次のとおりです。

- <CT_Get>
- <CT_Redirect>
- <attach>
- <insert>

<CT_Get> および **<CT_Redirect>** タグは、 618 ページの『SOAP メソッド』 で説明したように使用されます。**<attach>** タグを使用して、ファイルをロードします。このファイルは、<*install_dir* >¥cms¥html ディレクトリー (Windows) または <*install_dir* >/tables/HUB_Name/HTML(Linux および UNIX) にあるはずです。<attach> タグでは相対パスは使用できません。**<insert>** タグを使用すると、XML 要求内の埋め込みテキストの位置と対応する場所にある検索済み (出力) データ・ストリームに、組み込みテキストをロードできます。

第 2 レベル要求の使用方法の例を次に示します。この XML からファイル tabledata.htm が作成されます。このファイルには prefix.xls のデータが書き込まれます。次に、**<insert>** タグを使用して組み込みデータが入力され、**<CT_Get>** コマンドを使用した要求が行われます。この要求の ID 値は "NTDATA" であるため、データ・タグ **<XML id=”NTDATA”>** 内にその特定の要求データが入ります。**<CT_Redirect>** コマンドは、要求を http://services.xmethods.net:80/soap/servlet/rpcrouter に転送するために使用され、suffix.xls から tabledata.htm にデータを挿入するために最終要求が出されます。

```
<CT_Export>
  <filename>tabledata.htm</filename>
  <request>
    <attach>prefix.xls</attach>
  </request>
  <request>
    <insert>
    <insertelement>
      <insertdata>
        This data has been inserted compliments of CT SOAP server.
      </insertdata>
    </insertelement>
    </insert>
  </request>
  <request id="NTDATA">
    <CT_Get>
      <userid>sysadmin</userid>
      <password></password>
      <object>NT_System</object>
      <target>*ALL</target>
    </CT_Get>
  </request>
  <request>
    <CT_Redirect endpoint="http://services.xmethods.net:80/soap/servlet/rpcrouter">
      <SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
        <SOAP-ENV:Body>
          <ns1:getTemp xmlns:ns1="urn:xmethods-Temperature" SOAP-
          ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
            <zipcode>93117</zipcode>
          </ns1:getTemp>
        </SOAP-ENV:Body>
      </SOAP-ENV:Envelope>
    </CT_Redirect>
  </request>
```

```
  <request>
    <attach>suffix.xls</attach>
  </request>
</CT_Export>
```

サンプル CT_Get SOAP 要求

以下は、送信される **CT_Get** SOAP 要求と受信される応答のサンプルです。

SOAP エンドポイント http://esada.ibm.com:19221/SOAP に送信される SOAP 要求

```
<?xml.version="1.0" encoding="UTF-8" standalone="no"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
"http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
   <CT_Get>
    <Object>NT_System</Object>
    <Source>Primary:ESADA:NT</Source>
   </CT_Get>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SOAP エンドポイント http://esada.ibm.com:19221/SOAP からの SOAP 応答

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV=
"http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<SOAP-ENV:Body>
 <SOAP-CHK:Success xmlns:SOAP-CHK = "http://soaptest1/soaptest/">
 <PARMS> </PARMS>
 <TABLE name="KNT.WTSYSTEM">
  <OBJECT>NT_System</OBJECT>
  <DATA>
   <ROW>
     <Server_Name>Primary:ESADA:NT</Server_Name>
     <Timestamp >1011127123323391</Timestamp>
     <User_Name>SYSTEM</User_Name>
     <Operating_System_Type>Windows_NT</Operating_System_Type>
     <Operating_System_Version>4.0</Operating_System_Version>
     <Network_Address>10.21.2.154</Network_Address>
     <Number_of_Processors  dt:dt="number">1</Number_of_Processors>
     <Processor_Type dt:dt="number">586</Processor_Type>
     <Page_Size dt:dt="number">4096</Page_Size>
     <_Total_Privileged_Time dt:dt="number">1</_Total_Privileged_Time>
     <_Total_Processor_Time dt:dt="number">7</_Total_Processor_Time>
     <_Total_User_Time dt:dt="number">6</_Total_User_Time>
     <Context_Switches_Sec dt:dt="number">1745</Context_Switches_Sec>
     <File_Control_Bytes_Sec dt:dt="number">4500</File_Control_Bytes_Sec>
     <File_Control_Operations_Sec dt:dt="number">98
      </File_Control_Operations_Sec>
     <File_Data_Operations_Sec dt:dt="number">28
      </File_Data_Operations_Sec>
     <File_Read_Bytes_Sec dt:dt="number">800</File_Read_Bytes_Sec>
     <File_Read_Operations_Sec dt:dt="number">27
      </File_Read_Operations_Sec>
     <File_Write_Bytes_Sec dt:dt="number">9772</File_Write_Bytes_Sec>
     <File_Write_Operations_Sec dt:dt="number">1
      </File_Write_Operations_Sec>
     <Processor_Queue_Length dt:dt="number">0</Processor_Queue_Length>
     <System_Calls_Sec dt:dt="number">2368</System_Calls_Sec>
     <System_Up_Time dt:dt="number">956388</System_Up_Time>
     <Total_Interrupts_Sec dt:dt="number">1076</Total_Interrupts_Sec>
    </ROW>
   </DATA>
```

```
  </TABLE>
 </SOAP-CHK:Success>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

IBM Tivoli Monitoring Web サービス・シナリオ

以下に、IBM Tivoli Monitoring Web サービスの使用例をいくつか示します。これらの例は、独自のアプリケーションを作成するための提案として使用できます。

注: 以下のシナリオには、シナリオを作成するために使用された実際のコードは記述されていません。以下の例で示す図表およびテーブルを生成するには、独自にスクリプトを作成する必要があります。

日計の論理演算の要約と図表の生成

有効なハブに対して SOAP サーバーを使用して、複数のエージェントからデータを取得することにより、日計の論理演算の要約を生成できます。**CT_EMail** SOAP メソッドを使用して、これらの要約を電子メールとして管理部門に送信できます。

<insert> タグを **CT_EMail** に追加できます。このタグには、要約の設定済みフォーマットの指示が含まれています。管理部門では、これらの要約を Internet Explorer を使用してデスクトップ上で表示できます。要約を使用すると、夜間に発生した可能性のある問題を効率的に素早く参照することができます。

一般機能以外の機能をテーブルおよび図表に追加することがあります。

- トランザクション・ボリューム/応答回数およびサービス・レベルを満たしているかどうかを、リソース・トレンドおよびエラー条件と関連付けてプロットできます。
- 複数のセグメントにわたって図表をプロットできるため、表示や印刷が容易になります。
- X 軸で可変スケールを使用して、基本シフトをより詳細に表示できます。
- 複数のソースからの複数のオブジェクト/属性をプロットでき、時間軸に沿って例外を相関させることができるため、問題領域にフォーカスを当てることができます。
- 状況マップでシチュエーションの状況を表示できます。

データ・スナップショットおよびオフラインのテーブルと図表の取得

有効なハブに対して SOAP メソッド **CT_Get** を使用して、複数のエージェントからデータ・スナップショットを取得することにより、図表とレポートを生成できます。データのスナップショットを要求する AF REXX スクリプトを作成することもできます。

一般機能以外の機能をテーブルおよび図表に追加することがあります。このタイプの要求には以下の機能が含まれることがあります。

- 複数のセグメントにわたって図表をプロットできるため、表示や印刷が容易になります。

- 凡例ボックス内の属性名をクリックすると、Y 軸にその属性が表示され、しきい値が表示されます。
- しきい値が変更された場合は、新規のしきい値として使用できます。

以下のグラフィックスは、日常の業務処理の要約のサンプルを示しています。

以下のグラフィックスは、このタイプの要求に対して生成される図表/レポートのサンプルを示しています。

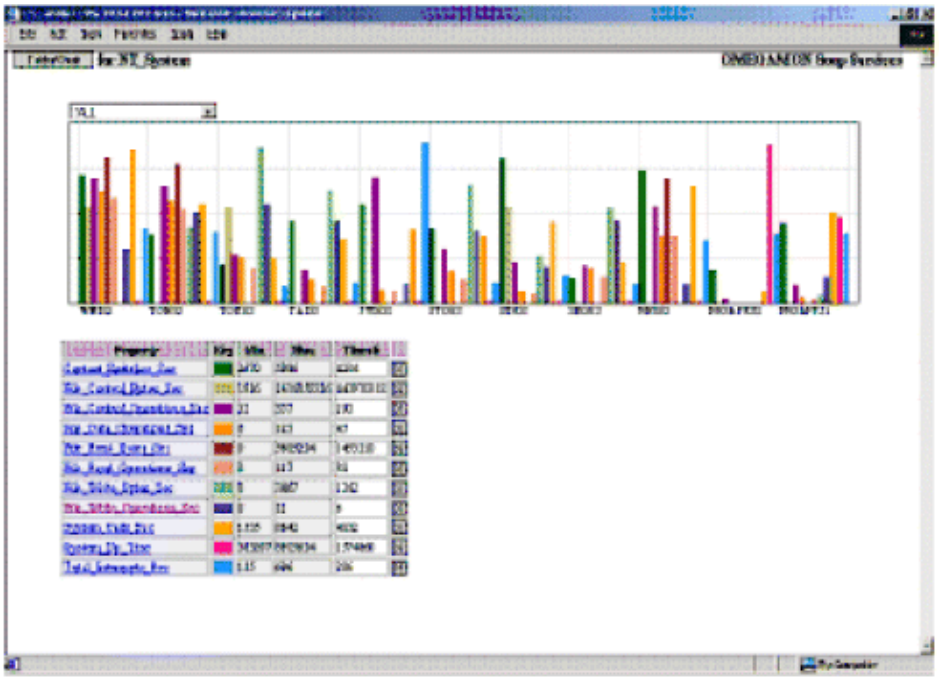


図 31. データ・スナップショットの図表およびテーブル

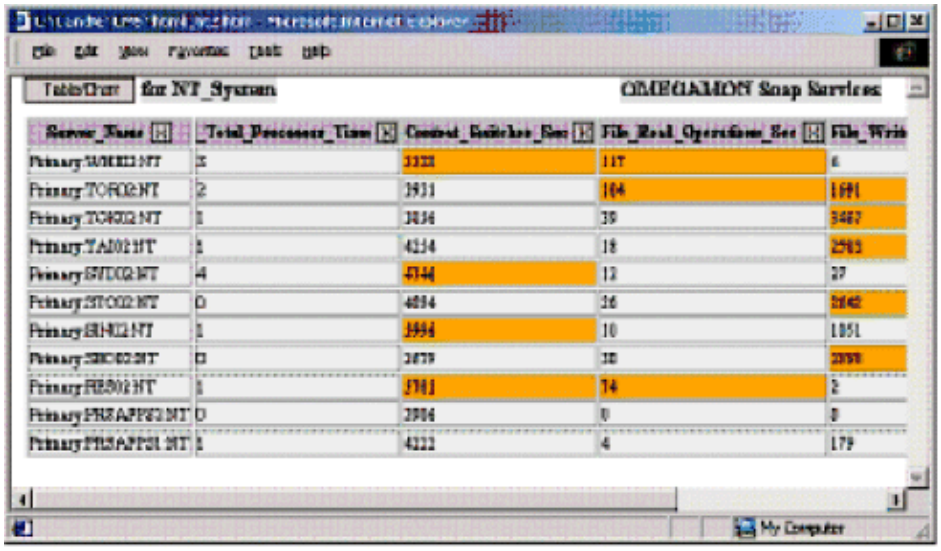


図 32. データ・スナップショットのテーブル

IBM Tivoli Monitoring プラットフォームへのアラートの送信

SOAP メソッド **CT_Alert** を使用して、IBM Tivoli Monitoring プラットフォームに新規のアラートを送信できます。

例えば、System Automation for Integrated Operations Management は HP NonStop Kernel システム上の問題を検出し、IBM Tivoli Monitoring プラットフォーム内でアラートを生成します。その後、IBM Tivoli Monitoring プラットフォームは、HP NonStop Kernel プラットフォームからのアラート情報を表示します。

SA IO を使用したコラボレーション自動化の作成

JSCRIPT SOAP 関数を呼び出す System Automation for Integrated Operations Management REXX アプリケーションを作成して、任意の SA IO トラップ・メッセージを転送し、そのメッセージを Universal Message コンソール上に表示できます。SA IO スクリプトを使用すると、ログ・メッセージやコンソール・メッセージなどの任意のメッセージをトラッピングし、SOAP メソッドを使用する IBM Tivoli Monitoring に送信できます。

以下の利点を提供するアプリケーションを作成できます。

- VT100 メッセージをトラッピングし、Universal Message を生成することにより、HP NonStop Kernel などのデバイスをモニターできます。
- コマンドを SA IO のモニター対象の Telnet セッションに送信し、これらのコマンドに応答を返すことができます。
- 強力な正規表現を使用する任意の基準に基づいて、ソース・メッセージを除外するか含めるかを選択できます。
- ローカル・ログにより、受信したメッセージおよび送信したメッセージの状況についての監査情報を記録できます。
- ローカル・ログにより、ソース・ハブ接続/再試行状況についての情報を記録できます。

以下のグラフィックスは、サンプル Telnet セッション、受信したメッセージを示す Universal Message コンソール、およびサンプル・メッセージ・ログを示しています。

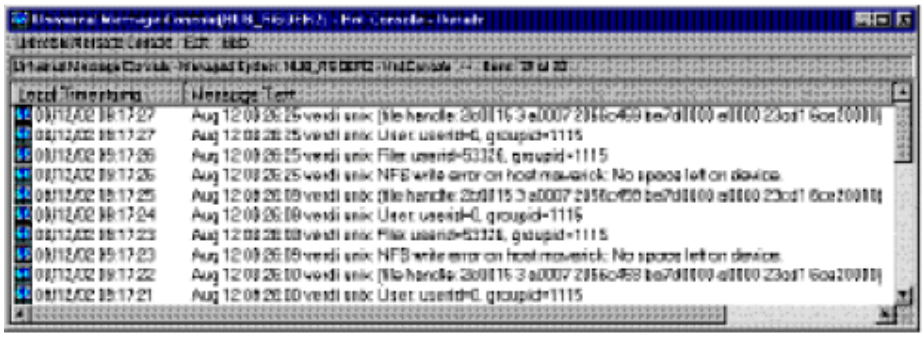


図 33. 受信したメッセージを示す Universal Message コンソール

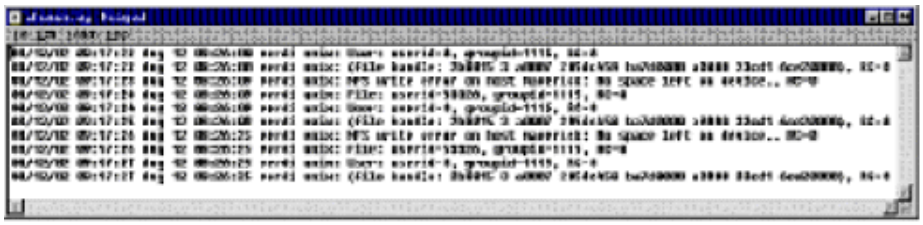


図 34. メッセージ・ログ詳細

IBM Tivoli Monitoring プラットフォーム内でのイベントの確認通知

IBM Tivoli Monitoring プラットフォーム内でイベントを確認できます。

例えば AF/Operator または System Automation for z/OS V3.2 以降での処理は以下のとおりです。

1. シチュエーション・イベントは、ハブ Tivoli Enterprise Monitoring Server から受信される
2. 処理を実行するパーティーが呼び出され、そのパーティーが確認通知を返信する
3. アラートの確認通知がモニター・サーバーに転送される

このタスクを実行するには、**CT_Acknowledge** SOAP メソッドを使用します。このメソッドを使用すると、IBM の自動化ソリューションによって取得および検出された情報に基づいて、IBM Tivoli Monitoring 環境でイベントを制御することができます。

レポート内容

表ビューとグラフ・ビューの両方を含むレポートを設計できます。グラフ・ビューと表ビューを切り替えることができるように、「**テーブル/図表 (Table/Chart)**」ボタンを追加できます。

グラフ・ビューの機能

図表には、以下の作業を行えるように固有の機能を持たせることができます。

- 検索されたデータに応じて、さまざまなタイプの図表を表示します。
- ドロップダウン属性リストから追加属性を選択すると、Y 軸が選択されます。
- 図表のタイトルと説明を変更します。
- プロットされた各項目の上にマウスを置くと、プロットされた属性の名前と値を示す吹き出しテキストが表示されます。

表ビュー機能

テーブルには、固有の機能を持たせることができます。例えば、以下の機能を持つテーブルを設計できます。

- プロットされた各項目の上にマウスを置くと、プロットされた属性の名前と値を示す吹き出しテキストが表示されます。
- 表示される属性をフィルター操作して、テーブルを変更します。
- 属性名の横にある X ボタンをクリックして、テーブルから属性を削除します。

付録 B. IBM Tivoli Monitoring グラフ Web サービスの使用可能化

Tivoli Integrated Portal V2.2 プラットフォーム・ベースの製品を使用している場合、グラフ作成機能を使用して、Tivoli Monitoring 環境で照会した値を使用したグラフを表示することができます。 Tivoli Enterprise Portal Server で IBM Tivoli Monitoring グラフ Web サービス (ITMWebService) を使用可能にする必要があります。グラフ Web サービスは、Tivoli Business Service Manager ポリシー・ベース・データ・フェッチャー機能でも使用されます。

注: IBM Dashboard Application Services Hub でモニター・データを表示する際には、IBM Tivoli Monitoring ダッシュボード・データ・プロバイダーが、グラフ Web サービスの代わりに使用されます。

始める前に

Tivoli Integrated Portal コンソールおよび Tivoli Enterprise Portal Server のユーザーに対してシングル・サインオンが使用可能になっている必要があります。グラフ Web サービスからのデータが含まれたグラフを表示するユーザーは、データをグラフで表示するモニター・アプリケーションが割り当てられている Tivoli Enterprise Portal ユーザー ID を持っている必要があります。

このタスクについて

Tivoli Enterprise Portal Server がインストールされ、稼働しているコンピューターで以下のステップを実行し、Tivoli Monitoring グラフ Web サービスを使用可能にします。

手順

1. **kfwtipewas.properties** ファイルをポータル・サーバー・ディレクトリーにコピーします。

   Windows *install_dir* ¥CNPS¥SQLLIB¥ から *install_dir* ¥CNPS へコピーします。

   Linux UNIX *install_dir* /*platform*/cq/sqllib/ から *install_dir* /*platform*/cq/ へコピーします。
2. Tivoli Enterprise Portal Server を再構成します。

次のタスク

Tivoli Enterprise Portal ユーザーには、許可に基づいて、特定のワークスペース (特定のモニター対象アプリケーションに属する) を表示する資格が与えられます。例えば Linux のワークスペースを表示する資格がある場合は、Tivoli Integrated Portal でグラフを作成するためにそれらのワークスペースの照会を使用できます。

グラフ Web サービスとの間の通信を保護するために HTTPS を使用する場合は、「*IBM Tivoli Monitoring インストールおよび設定ガイド*」の『SSL を介した Tivoli Business Service Manager と Tivoli Enterprise Portal Server の統合』を参照してください。

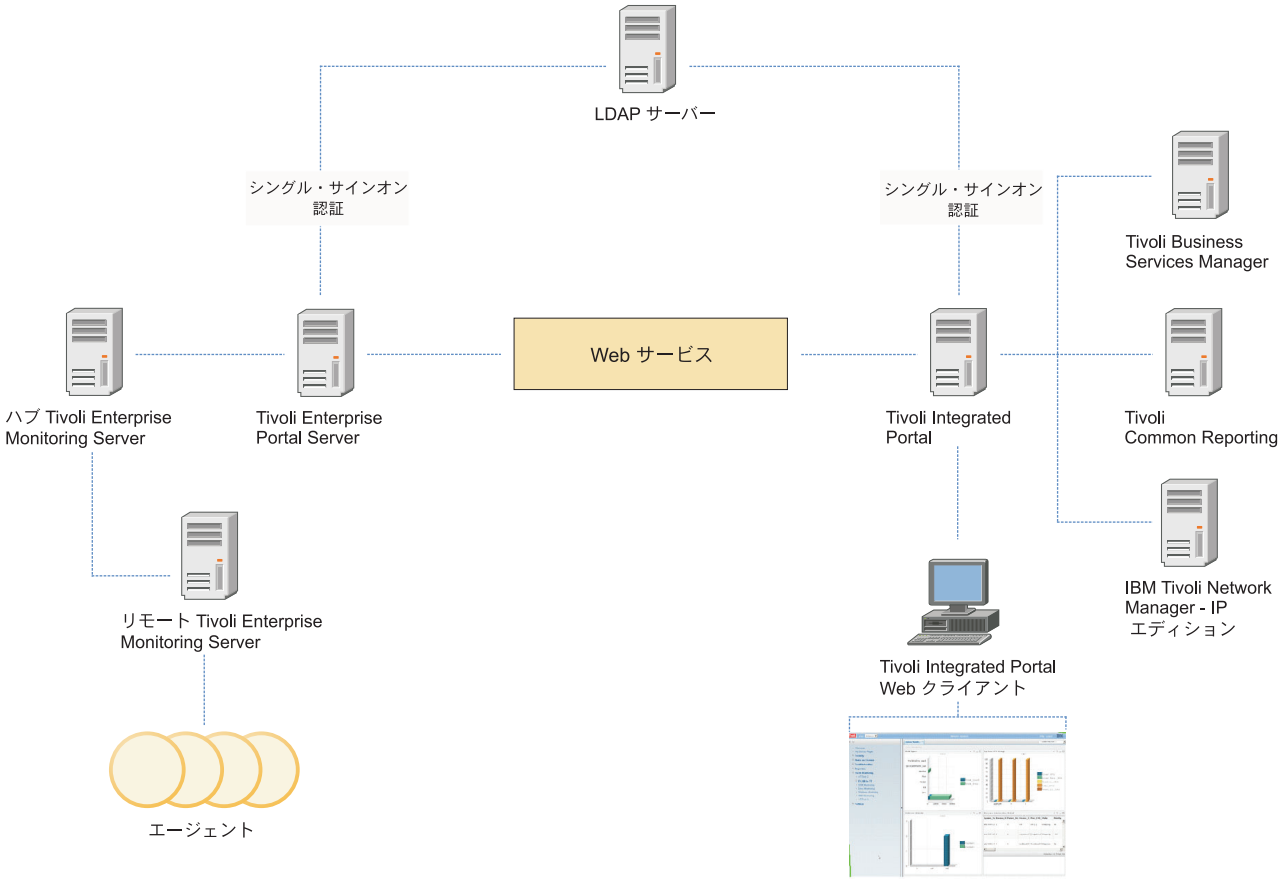


図 35. グラフ Web サービスの製品相互接続

付録 C. Tivoli Management Services ディスカバリー・ライブラリー・アダプターの使用

Tivoli Management Services ディスカバリー・ライブラリー・アダプター (TMS DLA) プログラムを使用してモニター対象環境をスキャンし、管理対象システムを識別します。そのため、この情報 (XML 出力ファイル) を Change and Configuration Management Database (CCMDB)、Tivoli Application Dependency Discovery Manager (TADDM)、または Tivoli Business Service Manager (TBSM) に送ることができます。

TMS DLA は、Tivoli Management Services に登録されたすべての分散システムおよび z/OS 管理対象システムを識別します。

始める前に

tmsdla スクリプトが起動されると、TMS DLA はすべての管理対象システムのハブ・モニター・サーバーを照会し、エージェント製品コードおよび管理対象システムの名前フォーマットに基づいて、それらのシステムを共通データ・モデルのリソースにマッピングすることで、情報を収集します。各製品によって提供される XML 入力ファイルで指定された照会が実行され、その結果が単一の出力ファイルに保存されます。

エージェントのモニター対象リソースと共通データ・モデルのリソース間で、TMS DLA およびマッピング可能な情報用の入力 XML ファイルをエージェントが提供しているかどうかについては、エージェント固有のユーザーズ・ガイドを参照してください。

このような照会では、モニター・サーバーおよび Tivoli Enterprise Portal Server が実行されている必要があります。また、オンライン状態ではない管理対象システムはすべて無視されます。

このタスクについて

ポータル・サーバーがインストールされているコンピューター上のコマンド行から、以下の TMS DLA スクリプトを実行します。

手順

- Windows 作成タイプの IDML ブックを作成するには、以下のコマンドを入力します。

  ```
  install_dir ¥CNPS¥tmsdla.bat
  ```

  あるいは、最新表示タイプの IDML ブックを作成するには、以下のコマンドを入力します。TADDM へのインポート後は、オフラインのシステム (保守作業の場合など) はすべて TADDM から削除されます。Tivoli Business Service Manager (TBSM) の場合も同様です。

  ```
  install_dir ¥CNPS¥tmsdla.bat -r
  ```

- Linux UNIX 作成タイプの IDML ブックを作成するには、以下のコマンドを入力します。

  ```
  install_dir /bin/itmcmd execute cq "tmsdla.sh"
  ```

  あるいは、最新表示タイプの IDML ブックを作成するには、以下のコマンドを入力します。TADDM へのインポート後は、オフラインのシステム (保守作業の場合など) はすべて TADDM から削除されます。TBSM の場合も同様です。

  ```
  install_dir /bin/itmcmd execute cq "tmsdla.sh -r"
  ```

タスクの結果

TMS DLA はポータル・サーバーの同じディレクトリーに XML 出力ファイルを生成します。このファイル名は、標準のディスカバリー・ライブラリー・ファイル名フォーマットに従います。CCMDB、TADDM、または TBSM でこの情報を使用するには、ディスカバリー・ライブラリー・ファイルのストアに XML ファイルを転送して、ディスカバリー・ライブラリーのバルク・ローダーを使用する必要があります。

TMS DLA はまた、関係が削除される前の TMS DLA 出力が含まれる、`.xml.original` 拡張子を持つ出力ファイルを作成します。削除された関係は、`tmsdla.log` に書き込まれます。TMS DLA XML 出力ファイルから関係が削除される可能性のあるシナリオの例については、641 ページの『OS エージェントの依存関係』 を参照してください。

使用法

以下の使用上の注意を参照してください。

```
tmsdla [ [-? | -h] [-d directory] [-f outputFilename] [-l] [-m listOfManagedSystems]
         [-o] [-p portNumber] [-r] [-s] [-t threadCount] [-w waitTime] ]
```

値の説明:

-? | -h 構文ヘルプ情報を表示します。

-d テンプレート・ディレクトリーの場所を指定します。

-f 結果出力ファイル名を指定します。

-l 論理ビューをディスカバーします。

-m 管理対象システムのリストを指定します。

リストは次の構文に従って二重引用符で囲みます。

```
  "os_msys1, os_apptype1, [msys1, apptype1]
~ [os_msys2, os_apptype2, [msys2, apptype2]] ~ ..
~ [os_msysN, os_apptypeN, [msysN, apptypeN]]"
```

-o オフライン管理対象システムの処理を強制的に実行します。

-p ポータル・サーバーのポート番号を指定します (デフォルト値の 1920 でない場合)。ポート番号は出力ブックに含まれており、TADDM または TBSM によって Tivoli Enterprise Portal を起動する URL を生成するために使用されます。

-r 最新表示タイプの出力 XML ファイルを生成します。最新表示タイプの出力ファイルを TADDM にインポートすると、保守操作などのためにオフラ

インになっている管理対象システムのオブジェクトおよびそのモニター対象リソースは TADDM データベースから削除されます。最新表示タイプ出力ファイルを TBSM または CCMDB にインポートする場合も同じことが該当します。このオプションを指定しない場合、オンラインの管理対象システムとそのモニター対象のリソースのみを含む、作成タイプの出力 XML ファイルが生成されます。作成タイプの出力 XML ファイルを TADDM、TBSM、または CCMDB にインポートすると、管理対象システムおよびモニター対象リソースが追加または更新されますが、削除は行われません。

-s クリーンアップ・プロセスで `.original` ファイルの生成を抑止します。

-t 使用するスレッド数を指定します。

-w タイムアウトになるまでの、エージェントによる照会の処理を待機する秒数を指定します。照会対象システムでの負荷が高いことが原因でモニター・エージェントが妥当な期間内に照会を処理できない可能性がある場合に、このオプションを使用します。**デフォルト値**: 120 秒。

最小値: 50 秒。50 秒未満の値は無視され、デフォルト値が使用されます。

最大値: 600 秒。

注: タイムアウトになった場合、またはエージェント・データが欠落していた場合は、ブックの完了時に警告を示す戻りコードが返されません。デフォルトよりも大きい値を設定する必要があるかどうかを確認するには、ブックを分析し、すべてのエージェントが応答していることを確認します。

関連資料:

Tivoli Change and Configuration Management Database
CCMDB インフォメーション・センターで「ディスカバリー・ライブラリー・ファイルのストア」と「ディスカバリー・ライブラリーのバルク・ローダー」を検索

Tivoli Monitoring DLA での問題
Tivoli Monitoring DLA で発生する共通問題のソリューション

Tivoli Monitoring コマンド・リファレンス
Linux および UNIX の Tivoli Enterprise Monitoring Server でのみ使用可能な itmcmd コマンドについては、ここで説明

OS エージェントの依存関係

Tivoli Management Services ディスカバリー・ライブラリー・アダプター (TMS DLA) はオペレーティング・システム (OS) エージェントに対し、DLA のテンプレートを提供するアプリケーション・エージェントと同じシステムをモニターするよう要求します。

一部のアプリケーション・エージェント (DB2 エージェントなど) は OS エージェントに依存することにより、エージェントが実行されているコンピューター・システムやオペレーティング・システムを説明する DLA ブックで要素を作成します。このようなアプリケーション・エージェントは DLA テンプレートで、OS エージェントが関係要素を使って作成するコンピューター・システムやオペレーティン

グ・システムの要素を参照します。例えば Db2System runsOn a ComputerSystem の場合、runsOn は関係タイプ、Db2System はソース要素、そして ComputerSystem はターゲット要素です。

OS エージェントがアプリケーション・エージェントと同じシステムをモニターしていなかったり、OS エージェントとアプリケーション・エージェントが異なる IBM Tivoli Monitoring 環境に接続している場合は、関係要素のソースまたはターゲットが DLA ブックに存在しない可能性があります。次の場合、コンピューター・システムやオペレーティング・システムに対する関係のソースとターゲットが存在しない可能性があります。

- Windows OS エージェントが Windows 2000 システムをモニターしている場合。この場合 OS エージェントは Windows 2000 システムの IP アドレスをディスカバーできないため、DLA ブックにコンピューター・システムの要素を作成しません。
- エージェントレス OS エージェントは DLA ブックに入力を提供しないため、エージェントレス OS エージェントを使用してモニターしているシステムが、アプリケーション・エージェントがモニターしているシステムと同一である場合。

関係のソースとターゲットのいずれかが DLA に存在しない場合、このブックは Tivoli Application Dependency Discovery Manager (TADDM) や Tivoli Business Service Manager (TBSM) に正しくロードされません。そのため DLA は、関係のソースやターゲットがブックに存在しない場合、DLA ブックからその関係を削除します。これによって DLA ブックが正しくロードされるようになります。しかし、関係が削除されると、影響を受けるリソース (データベース・システムなど) を TADDM や TBSM のコンピューター・システムやオペレーティング・システムにマップする情報が DLA ブックに含まれなくなります。

DLA は、**tmsdla** コマンドが実行されるたびに以下の 2 つの XML ファイルを作成します。 is run:

- `.xml` 拡張子を持つブック
- `.xml.original` 拡張子を持つブック

`.xml.original` 拡張子を持つファイルには、関係が削除される前の DLA ブックのコンテンツが含まれます。削除された関係は、`tmsdla.log` に書き込まれます。

TADDM および TBSM にロードされる DLA ブックのコンピューター・システムやオペレーティング・システムにリソースをマップする場合は、アプリケーション・エージェントでモニターされているシステムに OS エージェントをインストールしてください。

プライベート・ネットワーク・アドレスのフィルタリング

プライベート・ネットワーク・アドレスが重複していない環境では、この動作を変更し、Tivoli Management Services ディスカバリー・ライブラリー・アダプター (TMS DLA) によってこれらのコンピューター・システムにデータが取り込まれるようにできます。

始める前に

TMS DLA は、Internet Engineering Task Force (IETF) RFC 1918 および IETF RFC 4193 に従って構成されているプライベート・ネットワーク・インターフェースのデータをコンピューター・システムに取り込みません。RFC について詳しくは、RCF Index (http://tools.ietf.org/rfc/index) を参照してください。これは、複数のプライベート・ネットワークで重複するアドレス範囲が使用されている場合に、誤ったコンピューター・システム同士がマージされないようにするための動作です。

このタスクについて

プライベート・ネットワーク・インターフェースでのコンピューター・システムのディスカバリーを有効にするには、TMS DLA の動作を制御する XML テンプレート・ファイルで IP アドレス・フィルターを編集します。

手順

1. 編集する前に、テンプレート・ファイルのバックアップをとってください。
   - Linux UNIX テンプレート・ファイルは Tivoli Enterprise Portal Server の `$ITM_HOME/arch/cq/tmsdla` に格納されています。
   - Windows テンプレート・ファイルは Tivoli Enterprise Portal Server の `%ITM_HOME%¥CNPS¥tmsdla` に格納されています。
2. 各モニター・エージェントのテンプレートはディスカバリー・データを提供します。
   a. 各テンプレート・ファイルを調べ、ファイルに `<tmsdla:filter>` セクションが 1 つ以上あるかどうかを確認します。 オペレーティング・システム・エージェントのテンプレート・ファイル名の例を以下に示します。

      `knt_tmsdla.xml` (Windows OS エージェント)

      `kux_tmsdla.xml` (UNIX OS エージェント)

      `klz_tmsdla.xml` (Linux OS エージェント)

   b. 各テンプレート・ファイルで複数の `<tmsdla:filter>` セクションを更新し、ループバック・アドレスのフィルター (IPv4 の場合は 127.0.0.1、IPv6 の場合は ::1) のみを含むようにします。次に例を示します。

```
<tmsdla:filters>
    <tmsdla:filter name="IF_IP_ADDR" exclude="127¥.0¥.0¥.1"/>
    <tmsdla:filter name="IF_IP_ADDR" exclude="::1"/>
</tmsdla:filters>
```

次のタスク

Tivoli Enterprise Portal Server でエージェントのアプリケーション・サポートが更新されると、変更を行ったエージェントの現行 DLA テンプレート・ファイルの名前の拡張子が `.bak` に変更され、最新バージョンのテンプレート・ファイルがインストールされます。アプリケーション・サポートのインストールが完了したら、エージェントの新しいバージョンの DLA テンプレート・ファイルを更新し、`*.bak` バージョンのテンプレート・ファイルでの IP アドレス・フィルタリングの編集内容を追加します。

付録 D. z/OS Tivoli Management Services ディスカバリー・ライブラリー・アダプターの使用

z/OS Tivoli Management Services ディスカバリー・ライブラリー・アダプター (zTMS DLA) は V6.2.2 フィックスパック 7 以降、および IBM Tivoli Monitoring V6.2.3 フィックスパック 1 以降で使用可能で、IBM Tivoli Monitoring 環境をスキャンし、OMEGAMON エージェントがモニターするリソースをディスカバーします。

zTMS DLA は、z/OS オペレーティング・システム上のリソースのみを識別します。分散システムのリソースをディスカバーするには、Tivoli Monitoring Services ディスカバリー・ライブラリー・アダプターも実行する必要があります。

始める前に

zTMS DLA により生成される IDML ブックのデータを使用して、z/OS DLA が収集したデータを補完することができます。これにより、Tivoli Business Service Manager (TBSM) または Tivoli Application Dependency Discovery Manager (TADDM) の z/OS オブジェクトまたはイベントから Tivoli Enterprise Portal をコンテキストに基づいて起動できます。

zTMS DLA により作成される共通データ・モデル (CDM) オブジェクトを以下に示します。

- sys.zOS.Sysplex
- sys.zOS.SysplexGroup
- sys.zOS.ZSeriesComputerSystem
- sys.zOS.ZOS
- sys.zOS.CICSRegion
- sys.zOS.DB2Subsystem
- sys.zOS.IMSSubsystem
- sys.zOS.MQSubsystem
- sys.zOS.AddressSpace

重要: zTMS DLA ブックに対応するには、z/OS DLA V3.1 (PTF UA61720 適用) が必要です。zTMS DLA により生成される IDML ブックには、各種 z/OS CDM オブジェクトに必要な属性がすべて含まれているわけではありません。zTMS DLA ブックをコンシューム・アプリケーションにインポートする前に、まず IBM Tivoli Monitoring OMEGAMON エージェントによりモニターされているすべてのシステムで z/OS DLA を実行し、実行結果として作成される z/OS DLA ブックをコンシューム・アプリケーションにインポートする必要があります。その後、zTMS DLA ブックをインポートできます。すべてのオブジェクトが、z/OS DLA ブックで検出された既存のオブジェクトに合わせて調整されます。z/OS DLA ブックを最初にインポートせずに zTMS DLA ブックをインポートすると、TBSM UI でオブジェクトが  NO_LABEL_SUPPLIED として表示されることがあります。

ユーザー・シナリオ

1. z/OS LPAR では、すべての該当する z/OS LPAR に対して z/OS DLA を実行します。
2. Tivoli Enterprise Portal Server では、z/OS エージェントが接続するポータル・サーバーで zTMS DLAを実行します。
3. TBSM を使用している場合は、以下のステップを実行します。
   a. TBSM データ・サーバーで、TBSM ディスカバリー・ライブラリー・ツールキットを使用して z/OS DLA ブックを TBSM にインポートします。
   b. TBSM データ・サーバーで、TBSM ディスカバリー・ライブラリー・ツールキットを使用して zTMS DLA ブックを TBSM にインポートします。
   c. TBSM サーバーのグラフィカル・ユーザー・インターフェースで、TBSM オブジェクトを右クリックし、IBM Tivoli Monitoring コンテキスト起動メニュー項目を表示します。
4. TADDM を使用している場合は、以下のステップを実行します。
   a. TADDM サーバーで、バルク・ロード・ユーティリティーを使用して z/OS DLA ブックを TADDM にインポートします。
   b. TADDM サーバーで、バルク・ロード・ユーティリティーを使用して zTMS DLA ブックを TADDM にインポートします。

このタスクについて

Tivoli Enterprise Portal Server がインストールされているコンピューター上のコマンド行から、以下の DLA スクリプトを実行します。

手順

- Windows IDML ブックを作成するには、以下のコマンドを入力します。

  install_dir ¥CNPS¥ztmsdla.exe

  出力ファイルは *install_dir* ¥CNPS¥tmsdla ディレクトリーに書き込まれます。
- Linux UNIX IDML ブックを作成するには、以下のコマンドを入力します。

  install_dir /bin/itmcmd execute cq "ztmsdla"

  出力ファイルは *install_dir* /*arch*/cq/bin/tmsdla ディレクトリーに書き込まれます。

タスクの結果

DLA により、上記に示すディレクトリーに XML 出力ファイルが生成されます。このファイルの名前はストリング ZTMSDISC100-Bで始まり、標準 Discovery Library ファイル形式に基づきます (例: ZTMSDISC100-B.<*hostname*>.<*timestamp*>.refresh.xml)。

このブックを TADDM または TBSM にインポートするには、ディスカバリー・ライブラリー・ファイル・ストアに XML ファイルを転送して、ディスカバリー・ライブラリー・バルク・ローダーを使用する必要があります。

使用法

以下の使用上の注意を参照してください。

```
ztmsdla [/?] [/b] [/d] [/o orgname] [/s] [/p port] [/x outputfile]
```

値の説明:

/? 構文ヘルプ情報を表示します。

/b ブラウザーを開き、ディスカバリー・ライブラリー・アダプターの出力ファイルを表示します (Windows のみ)。

/d ディスカバリー・プロセスで診断ファイルを作成します。このファイルはデバッグに使用できます。このファイルは、DLA IDML ブックと同じディレクトリーに作成されます。ファイル名は DLA IDML ブックと同じですが、ファイル名の末尾に拡張子 `.log` が付きます (例: `ZTMSDISC100-B.<hostname>.<timestamp>.refresh.log`)。

/o orgname
組織のグローバル名を設定します。この引数を指定しない場合、グローバル名はデフォルトで `<defaultOrg>` になります。

/s このオプションを指定すると、HTTPS プロトコルを使用して ManagementSoftwareSystem クラスの sourceContactInfo 属性が作成されます。この URL は、Tivoli Enterprise Portal のコンテキスト起動を実行するときに TBSM および TADDM により使用されます。

/p port
sourceContactInfo 属性に対して作成された URL で使用されるポートを設定します。デフォルト・ポートは 1920 (HTTP) です。/s オプションが指定されている場合、デフォルト・ポートは 3661 (HTTPS) です。IBM Tivoli Monitoring 管理者が、ポータル・サーバーへの接続に使用する Web サーバーのデフォルト・ポートを変更している場合は、このオプションを使用します。

/x outputfile
XML 出力ファイルの名前を指定します。

既知の制限

z/OS Tivoli Enterprise Monitoring Server と OMEGAMON エージェントの間で IP.PIPE 通信ではなく SNA を使用する場合には、制限があります。同じ CICS® 領域を表す 2 つの CICS オブジェクトが TBSM に表示されますが、右クリックして TBSM CICS オブジェクトの 1 つを OMEGAMON CICS Tivoli Enterprise Portal ワークスペースで起動できるのは、いずれか 1 つのみです。

付録 E. MIB SNMP エージェントのイベントの説明

Tivoli モニター・エージェントは、エージェントの作動状況、サンプル・シチュエーション・イベント、ピュア・シチュエーション・イベントという 3 つのタイプの情報を通知する SNMP アラートを発行します。これらのアラート・タイプは、canbase.mib ファイルと cansyssg.mib ファイルで定義されています。これらのファイルは、IBM Tivoli Monitoring および IBM Tivoli Monitoring Agent のインストール・メディアにあります。

エージェントのシチュエーション状態 SNMP トラップは、エンタープライズ 1.3.6.1.4.1.1667.1.3 (Candle-BASE-MIB::candle-Alert-MIB) を使用して送信されます。

agentStatusEvent

agentStatusEvent は、特定のエージェントの運用上のイベントについて情報を提供し、通知するために、Tivoli Autonomous Agent SNMP Event Exporter によって生成された、モニター・エージェントの作動状況情報トラップです。

固有トラップ:20

アクセス: 読み取り専用

ステータス: 必須

表 69. agentStatusEvent の SNMP トラップ変数

変数	説明	OID
agentSit-Name	状況イベントの名前と特性を識別するシチュエーション名 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	シチュエーションが評価された管理対象システムの名前 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	シチュエーション状態が変化したときのタイム・スタンプ。形式は CYYMMDDHHMMSSmmm です (例えば、2009 年 4 月 15 日 09:45:01 の場合は 1090415094501000)。ここで、 C = 世紀 (21 世紀の場合 1) Y = 年 M = 月 D = 日 H = 時 M = 分 S = 秒 m = ミリ秒	1.3.6.1.4.1.1667.1.2.1.10.1.5

表 69. *agentStatusEvent の SNMP トラップ変数 (続き)*

変数	説明	OID
autoSit-Category	割り当て済みのシチュエーション・カテゴリー。有効な値は以下のとおりです。 0 - しきい値 1 – ネットワーク・トポロジー 2 - エラー 3 - ステータス 4 - ノード構成 5 – アプリケーション・アラート 6 - すべてのカテゴリー 7 - ログのみ 8 - マップ 9 – 無視	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	割り当て済みのシチュエーション重大度。有効な値は以下のとおりです。 0 - 解決済み 1 - 不定 2 - 警告 3 - マイナー 4 - メジャー 5 - 重大	1.3.6.1.4.1.1667.1.2.1.7
autoSit-StatusText	エージェント状況トラップの説明メッセージ・テキスト (0 から 256 バイト)。	1.3.6.1.4.1.1667.1.2.1.9
autoSit-Interval	エージェント状況トラップ間隔。通常は、ハートビート間隔で使用します。ハートビート間隔 `<StatTrap name="EE_HEARTBEAT" sev="1" interval="15" cat="3" />` の設定の例については、403 ページの『SNMP アラート構成』の『サンプルのトラップ構成ファイル』を参照してください。	1.3.6.1.4.1.1667.1.2.1.11

agentSitSampledEvent

サンプリングされたシチュエーション・イベントが検出されました。このトラップは、データのサンプリング時にシチュエーションしきい値を超えたことに対する応答として、Tivoli Autonomous Agent SNMP Event Exporter によって作成されました。

固有トラップ: 21

アクセス: 読み取り専用

ステータス: 必須

表 70. *agentSitSampledEvent の SNMP トラップ変数*

属性	説明	OID
agentSit-Application	これは、製品アプリケーション名です (1 から 8 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.1

表 70. *agentSitSampledEvent* の *SNMP* トラップ変数 (続き)

属性	説明	OID
agentSit-Table	これは、製品アプリケーション・テーブル (属性グループ) の名前です (1 から 12 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.2
agentSit-Name	状況イベントの名前と特性を識別するシチュエーション名 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	シチュエーションが評価された管理対象システムの名前 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	シチュエーション状態が変化したときのタイム・スタンプ。形式は CYYMMDDHHMMSSmmm です (例えば、2009 年 10 月 31 日 18:30:05 の場合は 1091031183005000)。ここで、 C = 世紀 (21 世紀の場合 1) Y = 年 M = 月 D = 日 H = 時 M = 分 S = 秒 m = ミリ秒	1.3.6.1.4.1.1667.1.2.1.10.1.5
agentSit-Context	固有のシチュエーション・コンテキスト ID であり、整数 (-2147483647 から 2147483647) で表現されます。これは、エージェントが実行している要求を識別するハンドル番号です。SNMP 環境では、通常、トラップ・ダイレクト・ポーリングが使用されます。これにより、トラップが受信され、ネットワーク・マネージャーが追加の詳細情報がないか発信元のエージェントをポーリングします。この ID は、要求を問題の原因に関連付けるために、ターゲット・エージェントのコンテキストを提供する場合に使用されます。agentSit-Context は送信されますが、このリリースでは使用されません。	1.3.6.1.4.1.1667.1.2.1.10.1.6
agentSit-SampleInterval	サンプリングされたシチュエーション間隔 (単位は秒で、0 から 86400 秒)。	1.3.6.1.4.1.1667.1.2.1.10.1.7
agentSit-Source	シチュエーションの現在の状況。有効な値は以下のとおりです。 0 - 未定義 1 - エンタープライズ。つまり、シチュエーションは Tivoli Enterprise Monitoring Server で定義されました。 2 - 専用。つまり、シチュエーションは、ローカルの専用シチュエーション構成ファイルで定義されました。	1.3.6.1.4.1.1667.1.2.1.10.1.20

表 70. agentSitSampledEvent の SNMP トラップ変数 (続き)

属性	説明	OID
autoSit-Category	割り当て済みのシチュエーション・カテゴリー。有効な値は以下のとおりです。 0 - しきい値 1 – ネットワーク・トポロジー 2 - エラー 3 - ステータス 4 - ノード構成 5 – アプリケーション・アラート 6 - すべてのカテゴリー 7 - ログのみ 8 - マップ 9 – 無視	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	割り当て済みのシチュエーション重大度。有効な値は以下のとおりです。 0 - 解決済み 1 - 不定 2 - 警告 3 - マイナー 4 - メジャー 5 - 重大	1.3.6.1.4.1.1667.1.2.1.7
autoSit-Predicates	これは、「属性名 演算子 比較値」という形式のシチュエーション式です (最大 3210 バイト)。この数式が複数の式で構成されている場合は、式のブール結合子 AND または OR が表示されます。	1.3.6.1.4.1.1667.1.2.1.8
sitAttributeList	モニター・エージェントに割り当てられているシチュエーションの属性値 (0 から 3200 バイト)。	1.3.6.1.4.1.1667.1.2.1.5

agentSitPureEvent

ピュア・シチュエーション・イベントが検出されました。このトラップは、シチュエーションしきい値を超えたことに対する応答として、Tivoli Autonomous Agent SNMP Event Exporter によって生成されました。ピュア・イベント・トラップ内の変数は、ピュア・イベントがサンプリングされず、agentSit-SampleInterval が存在しない場合を除き、サンプリングされたイベント・トラップの変数と同一です。モニター対象の属性グループから非送信請求データが着信すると、シチュエーションは true になります。例えば、属性グループを使用してシステム・ログ用に作成されたシチュエーションは、ログ項目を受信すると、ピュア・イベントを開きます。

固有トラップ: 22

アクセス: 読み取り専用

ステータス: 必須

表 71. agentSitPureEvent の SNMP トラップ変数

属性	説明	OID
agentSit-Application	これは、製品アプリケーション名です (1 から 8 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.1
agentSit-Table	これは、製品アプリケーション・テーブル (属性グループ) の名前です (1 から 12 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.2
agentSit-Name	状況イベントの名前と特性を識別するシチュエーション名 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.3
agentSit-OriginNode	シチュエーションが評価された管理対象システムの名前 (最大 32 バイト)。	1.3.6.1.4.1.1667.1.2.1.10.1.4
agentSit-LocalTimeStamp	シチュエーション状態が変化したときのタイム・スタンプ。形式は CYYMMDDHHMMSSmmm です (例えば、2009 年 10 月 31 日 18:30:05 の場合は 1091031183005000)。ここで、 C = 世紀 (21 世紀の場合 1) Y = 年 M = 月 D = 日 H = 時 M = 分 S = 秒 m = ミリ秒	1.3.6.1.4.1.1667.1.2.1.10.1.5
agentSit-Context	固有のシチュエーション・コンテキスト ID であり、整数 (-2147483647 から 2147483647) で表現されます。これは、エージェントが実行している要求を識別するハンドル番号です。SNMP 環境では、通常、トラップ・ダイレクト・ポーリングが使用されます。これにより、トラップが受信され、ネットワーク・マネージャーが追加の詳細情報がないか発信元のエージェントをポーリングします。この ID は、要求を問題の原因に関連付けるために、ターゲット・エージェントのコンテキストを提供する場合に使用されます。agentSit-Context は送信されますが、このリリースでは使用されません。	1.3.6.1.4.1.1667.1.2.1.10.1.6
agentSit-Source	シチュエーションの現在の状況。有効な値は以下のとおりです。 0 - 未定義 1 - エンタープライズ。つまり、シチュエーションは Tivoli Enterprise Monitoring Server で定義されました。 2 - 専用。つまり、シチュエーションは、ローカルの専用シチュエーション構成ファイルで定義されました。	1.3.6.1.4.1.1667.1.2.1.10.1.20

表 71. agentSitPureEvent の SNMP トラップ変数 (続き)

属性	説明	OID
autoSit-Category	割り当て済みのシチュエーション・カテゴリー。有効な値は以下のとおりです。 0 - しきい値 1 – ネットワーク・トポロジー 2 - エラー 3 - ステータス 4 - ノード構成 5 – アプリケーション・アラート 6 - すべてのカテゴリー 7 - ログのみ 8 - マップ 9 – 無視	1.3.6.1.4.1.1667.1.2.1.6
autoSit-Severity	割り当て済みのシチュエーション重大度。有効な値は以下のとおりです。 0 - 解決済み 1 - 不定 2 - 警告 3 - マイナー 4 - メジャー 5 - 重大	1.3.6.1.4.1.1667.1.2.1.7
autoSit-Predicates	これは、「属性名 演算子 比較値」という形式のシチュエーション式です (最大 3210 バイト)。この数式が複数の式で構成されている場合は、式のブール結合子 AND または OR が表示されます。	1.3.6.1.4.1.1667.1.2.1.8
sitAttributeList	モニター・エージェントに割り当てられているシチュエーションの属性値 (0 から 3200 バイト)。	1.3.6.1.4.1.1667.1.2.1.5

付録 F. エージェント・オペレーション・ログ

Tivoli Enterprise Monitoring Agent は、データ・サンプルを取得してイベントを保存しながら、不特定期間の間、自律的に稼働できます。監査証跡ログをレビューして、自律的に実行されていた期間も含めて、エージェント・アクティビティーの検査およびレビューを行います。

エージェントが自律的に実行されている場合は、すべてのイベントの監査証跡レコードと、サンプリングされた TRUE のアプリケーション・データ行がオペレーション・ログに書き込まれます。エージェントは既存のエージェント・オペレーション・ログ機能を利用し、監査証跡レコードをこのログに出力します。エージェント・オペレーション・ログは、エージェントがオンラインの場合に Tivoli Enterprise Portal で表示できます。

- 分散システムでは、エージェントは自動的にオペレーション・ログ・ファイルをエージェントのインストール・ディレクトリーに作成します。現在実行中のログ・ファイルに `ComputerName_product.LG0` という名前を付け、以前のログ・ファイルの名前を `ComputerName_product.LG1` (バックアップ・ファイル) に変更します。
- z/OS システムでは、エージェントは、エージェント・オペレーション・ログ・レコードを `SYSOUT` クラスに書き込み、レコードの一部をメモリー・キャッシュ内に保存します。

エージェント・オペレーション・ログには、専用シチュエーションのアクティビティーも示されます。

オートノマス・アクティビティー・ログ・レコードには、以下のフィールドが含まれています。

- エージェント・システム名
- メッセージ ID: KRAIRA005
- グローバル・タイム・スタンプ。イベント・アクティビティーの実際のローカル・タイムを示します。
- シチュエーション名、アプリケーション・テーブル名、システム名、フィルター列名、フィルター値、および実際のサンプル値またはイベント値を示すメッセージ。シチュエーション・フィルター条件で複数のしきい値名および値の組が指定されているために、出力がオペレーション・ログのレコード・サイズを超えた場合、エージェントは複数のログ・レコードを出力します。

エージェントのオートノマス操作アクティビティー・レポートを取得するには、Tivoli Enterprise Portal で、メッセージ KRAIRA005 をフィルタリングするエージェント・オペレーション・ログ・カスタム照会を作成し、この照会を「物理」ナビゲーター・ビューのエージェント・レベルのワークスペース内の表ビューに割り当てます。または、定義済み照会エージェント・オペレーション・ログ を表ビューに割り当て、メッセージ KRAIRA005 の行を除くすべての行をフィルタリングするプロパティー・エディターの「フィルター」タブによるポスト・フィルターを適用する

ことができます。以下に、このような照会によって生成される可能性のあるオートノマス・アクティビティー・ログの例を示します。

以下は、エージェントのオートノミー・メッセージ「v == KRAIRA005」のみが含まれるようフィルタリングされたエージェント・オペレーション・ログの結果の表ビューです。

サーバー名	メッセージ番号	グローバル・タイム・スタンプ	管理対象システムのタイプ
Primary:East:NT	KRAIRA005	02/16/2009 12:35:42	KNT.WTPROCESS リセットのシチュエーション NT_Process_CPU_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:34:43	KNT.WTPROCESS がトリガーされた (03) Process_Name [_Total] 値 <kdsmain> のシチュエーション NT_Process_CPU_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:34:42	KNT.WTPROCESS がトリガーされた (02) Priority_Base [0] 値 <8> のシチュエーション NT_Process_CPU_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:34:42	KNT.WTPROCESS がトリガーされた (01) %_Processor_Time [65] 値 <66> のシチュエーション NT_Process_CPU_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:34:21	KNT.WTPROCESS がトリガーされた %_Usage [95] 値 <100> のシチュエーション NT_Log_Space_Low
Primary:East:NT	KRAIRA005	02/16/2009 12:32:42	KNT>WTPROCESS がトリガーされた (02) Working_Set [40000000] 値 <48832512> のシチュエーション NT_Process_Memory_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:32:41	KNT>WTPROCESS がトリガーされた (01) Process_Name [_Total] 値 <Rtvscan> のシチュエーション NT_Process_Memory_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:31:21	KNT.WTSYSTEM がトリガーされた Operating_System_Version [5.0] 値 <5.1> のシチュエーション NT_System_CPU_Critical
Primary:East:NT	KRAIRA005	02/16/2009 12:29:41	KNT.IPSTATS がトリガーされた (06) Datagrams_Received_Header_Errors [0] 値 <0> のシチュエーション CHECK_NETWORK_STAT
Primary:East:NT	KRAIRA005	02/16/2009 12:29:41	KNT.IPSTATS がトリガーされた (05) Datagrams_Outbound_Header_Errors [0] 値 <0> のシチュエーション CHECK_NETWORK_STAT

注: 配布済みのエンタープライズ・モニター・エージェントのエージェント環境変数 CTIRA_LOG_PATH により、そのエージェントのオペレーション・ログ・ファイルが格納されるディレクトリー (Windows: <*install_dir*>¥TMAITM6¥logs、Linux および UNIX: <*install_dir*>/config/logs) が指定されます。ファイル名には、.LG0 および .LG1 のサフィックスが使用されます。

資料ライブラリー

この付録には、IBM Tivoli Monitoring 関連の資料、および Tivoli Management Services の一般共有コンポーネント関連の資料に関する情報が記載されています。

これらの資料は、以下のカテゴリー別にリストされています。

- IBM Tivoli Monitoring ライブラリー
- 関連資料

資料へのアクセスおよび使用法については、IBM Tivoli Monitoring および OMEGAMON XE インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp) の「**目次**」ペインの「**マニュアルの使用法**」を参照してください。

新規および変更済みの資料のリストを検索するには、IBM Tivoli Monitoring および OMEGAMON XE インフォメーション・センターのウェルカム・ページで「**新機能 (What's new)**」をクリックします。製品の前のバージョンの資料を検索するには、「**目次**」ペインの製品名にある「**以前のバージョン (Previous versions)**」をクリックしてください。

IBM Tivoli Monitoring ライブラリー

以下の資料には、IBM Tivoli Monitoring に関する情報および Tivoli Management Services の一般共有コンポーネントに関する情報が記載されています。

- *Quick Start Guide*

  IBM Tivoli Monitoring のコンポーネントについて説明します。
- *インストールおよび設定ガイド*, SA88-5150

  Windows、Linux、および UNIX の各システムでの IBM Tivoli Monitoring コンポーネントのインストールおよび構成について説明します。
- *Program Directory for IBM Tivoli Management Services on z/OS*, GI11-4105

  z/OS での Tivoli Management Services コンポーネントの SMP/E インストールについて説明します。
- *分散システム用高可用性ガイド*, SA88-5155

  IBM Tivoli Monitoring コンポーネントの可用性を確実にするいくつかの方法に関して説明します。
- *IBM Tivoli zEnterprise Monitoring Agent インストールおよび構成ガイド*, SA88-4855

  Windows、Linux、および UNIX システムで Tivoli zEnterprise Monitoring Agent コンポーネントをインストールおよび構成する手順を説明しています。また、マイグレーションとバックアップに関する情報、Enterprise Common Collector のトラブルシューティング、Hardware Management Console の構成、およびコマンド

行インターフェースまたは API を使用してコレクターをカスタマイズする方法についても説明しています。このガイドは、「*Tivoli zEnterprise Monitoring Agent ユーザーズ・ガイド*」を補足するものです。

- *管理者ガイド*, SA88-5151

  Tivoli Enterprise Portal ユーザー管理などの、Tivoli Enterprise Portal Server およびクライアントに必要なサポート・タスクおよび機能について説明します。

- *コマンド・リファレンス*, SA88-5153

  構文とパラメーターの詳細情報、および IBM Tivoli Monitoring で使用できるコマンドのサンプルがあります。

- *メッセージ*, SA88-5162

  すべての IBM Tivoli Monitoring コンポーネントおよび z/OS ベースの Tivoli Management Services コンポーネント (Tivoli Enterprise Monitoring Server on z/OS および TMS:Engine など) が生成するメッセージをリストし、説明しています。

- *トラブルシューティング・ガイド*, GA88-5152

  ソフトウェアに関する問題のトラブルシューティングに役立つ情報を記載しています。

- Tivoli Enterprise Portal のオンライン・ヘルプ

  Tivoli Enterprise Portal のすべてのフィーチャーおよびカスタマイズ・オプションに関するコンテキスト依存の参照情報を記載しています。 Tivoli Enterprise Portal の使用方法および管理方法についても説明しています。

- *Tivoli Enterprise Portal ユーザーズ・ガイド*, SA88-5154

  Tivoli Enterprise Portal オンライン・ヘルプの補足です。 この資料には、実践演習のほか、すべての Tivoli Enterprise Portal 機能の詳細な説明が記載されています。

- *Agent Builder ユーザーズ・ガイド*, SC88-4765

  Agent Builder を使用してモニター・エージェントおよびそれらのインストール・パッケージを作成する方法および既存のエージェントに機能を追加する方法について説明しています。

- *Performance Analyzer ユーザーズ・ガイド*, SA88-4463

  Performance Analyzer の使用方法を説明しています。これは、リソース消費の傾向を理解し、問題を判別し、問題を素早く解決し、将来の問題を予測して回避するために役立ちます。

- *IBM Tivoli zEnterprise Monitoring Agent ユーザーズ・ガイド*, SA88-4856

  Tivoli zEnterprise Monitoring Agent オンライン・ヘルプの補足資料です。このガイドには、インターフェースに関する参照情報、使用シナリオ、エージェントのトラブルシューティング情報、および Tivoli Common Reporting のレポートに関する情報が記載されています。このガイドは、「*Tivoli zEnterprise Monitoring Agent インストールおよび構成ガイド*」を補足するものです。

基本エージェントの資料

IBM Tivoli Monitoring を製品として購入した場合、製品の一部として基本モニター・エージェント・セットが含まれています。Tivoli Management Services の一般共有コンポーネントを含むモニター・エージェント製品 (OMEGAMON XE 製品など) を購入した場合、基本エージェントは用意されていません。

基本エージェントの使用に関する情報は、以下の資料に記載されています。

- オペレーティング・システム・エージェント
  - *Windows OS Agent ユーザーズ・ガイド*, SA88-5156
  - *UNIX OS Agent ユーザーズ・ガイド*, SA88-5157
  - *Linux OS Agent ユーザーズ・ガイド*, SA88-5158
  - *IBM i Agent ユーザーズ・ガイド*, SA88-5159
- エージェントレス・オペレーティング・システム・モニター
  - *Agentless Monitoring for Windows Operating Systems ユーザーズ・ガイド*, SC88-5782
  - *Agentless Monitoring for AIX Operating Systems ユーザーズ・ガイド*, SC88-5784
  - *Agentless Monitoring for HP-UX Operating Systems ユーザーズ・ガイド*, SC88-5785
  - *Agentless Monitoring for Solaris Operating Systems ユーザーズ・ガイド*, SC88-5783
  - *Agentless Monitoring for Linux Operating Systems ユーザーズ・ガイド*, SC88-5781
- ウェアハウス・エージェント
  - *Warehouse Summarization and Pruning Agent ユーザーズ・ガイド*, SA88-5160
  - *Warehouse Proxy Agent ユーザーズ・ガイド*, SA88-5161
- System P エージェント
  - *AIX Premium エージェント ユーザーズ・ガイド*, SA88-4132
  - *CEC Base エージェント ユーザーズ・ガイド*, SC88-5750
  - *HMC Base エージェント ユーザーズ・ガイド*, SA88-4149
  - *VIOS Premium エージェント ユーザーズ・ガイド*, SA88-4133
- その他の基本エージェント
  - *Tivoli Log File Agent ユーザーズ・ガイド*, SA88-4868
  - *Systems Director base Agent User's Guide*, SC27-2872

関連資料

関連製品および資料については、IBM Tivoli Monitoring および OMEGAMON XE インフォメーション・センター (http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp) の「**目次**」ペインの「**OMEGAMON XE 共有資料**」またはその他の項目を選択してください。

その他の資料ソース

IBM Tivoli Monitoring および関連製品に関する技術文書は、以下のソースからも入手可能です。

- Service Management Connect (SMC)

  SMC に関する基本的な情報については、IBM Service Management Connect (http://www.ibm.com/developerworks/servicemanagement) を参照してください。

  Tivoli 製品については、IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) で、SMC の Application Performance Management コミュニティーを参照してください。

  サービス管理の専門家との連絡、学習、および共有を行います。開発者や製品サポートの技術者と交流して、見解や専門知識を得ることができます。SMC を使用すると、以下のことができます。

  – 透過的な開発、つまり外部ユーザーと Tivoli 製品の開発者の間で進められているオープンな連携に参加する。これにより、初期設計、スプリント・デモ、製品ロードマップ、プレリリース・コードにアクセスできます。
  – 専門家に直接連絡を取って、Tivoli および統合サービス管理についてコラボレーションし、ネットワークを形成する。
  – ブログを使用して、他のユーザーの専門知識や経験を取り入れる。
  – Wiki やフォーラムを使用して幅広いユーザー・コミュニティーとコラボレーションする。

- Tivoli Wiki

  IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) には、関連する Tivoli Wiki のリストが用意されています。これらの Wiki は、Tivoli 製品を使用する場合のベスト・プラクティスとシナリオ、IBM 社員が投稿したホワイト・ペーパー、製品ユーザーやビジネス・パートナーが作成したコンテンツを提供します。

  以下の 2 つの Wiki は、IBM Tivoli Monitoring に特に関連しています。

  – IBM Tivoli Monitoring Wiki (https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Monitoring/page/Home) は、IBM Tivoli Monitoring およびそれに関連する配布製品 (IBM Tivoli Composite Application Management 製品を含む) に関する情報を提供します。
  – Tivoli System z® Monitoring and Application Management Wiki では、OMEGAMON XE 製品、NetView for z/OS、Tivoli Monitoring Agent for z/TPF、およびその他の System z モニタリングおよびアプリケーション管理製品に関する情報を提供します。

- IBM Integrated Service Management Library

  http://www.ibm.com/software/brandcatalog/ismlibrary/

  IBM Integrated Service Management Library は、統合資料およびその他のダウンロード可能な製品の拡張機能を含む、オンライン・カタログです。

- Redbooks®

  http://www.redbooks.ibm.com/

  IBM Redbooks および Redpapers には、プラットフォームとソリューションの観点からの製品に関する情報が含まれています。

- Technotes

  Technote には、製品の既知の制限事項および予備手段に関する最新情報が記載されています。Technotes は IBM Software Support Web サイト (http://www.ibm.com/software/support/) にあります。

サポート情報

ご使用の IBM ソフトウェアに問題がある場合は、速やかに解決する必要があります。IBM では、お客様が必要なサポートを得るための方法を提供しています。

オンライン

以下のサイトにはトラブルシューティング情報が記載されています。

- IBM Support Portal (http://www.ibm.com/support/entry/portal/software) にアクセスし、指示に従います。
- IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) にアクセスして、該当する wiki を選択してください。

IBM Support Assistant

IBM Support Assistant (ISA) は無償で提供されるローカルのソフトウェア保守容易性ワークベンチで、IBM ソフトウェア製品に関する疑問や問題の解決に役立ちます。ISA を使用すると、サポート関連の情報や問題判別のための保守ツールに素早くアクセスすることができます。ISA ソフトウェアをインストールするには、「IBM Support Assistant (http://www-01.ibm.com/software/support/isa)」を参照してください。

トラブルシューティング・ガイド

問題の解決について詳しくは、製品のトラブルシューティング・ガイドを参照してください。

IBM Support Assistant の使用

以下は英語のみの対応となります。IBM Support Assistant は、どのワークステーションにもインストールできる、無償のスタンドアロン・アプリケーションです。このアプリケーションは、ご使用の IBM 製品の製品固有のプラグイン・モジュールをインストールすることで拡張できます。

IBM Support Assistant では、製品、サポート、およびトレーニングに関するリソースを短時間で検索できます。問題管理レコード (PMR) を提出する必要がある場合、IBM Support Assistant はサポート情報の収集に役立ち、お客様は、この PMR を使用して問題を追跡することができます。

製品固有のプラグイン・モジュールでは、以下のリソースが提供されます。

- サポート用リンク
- トレーニング用リンク
- 問題管理レポートの提出機能

詳細、および IBM Support Assistant のダウンロードについては、http://www.ibm.com/software/support/isa を参照してください。IBM Support Assistant をダウンロードしてインストールし終えたら、以下のステップに従って、Tivoli 製品向けのプラグインをインストールしてください。

1. IBM Support Assistant アプリケーションを開始します。

2. ウェルカム・ページで「**Updater**」を選択します。
3. 「**New Properties and Tools**」を選択するか、「**New Plug-ins**」タブを選択します (どちらを選択するかは、インストールされている IBM Support Assistant のバージョンによって異なります)。
4. 「**Tivoli**」で、製品を選択し、「**Install**」をクリックします。ご使用条件および説明を必ずお読みください。

   「**Tivoli**」のリストにご使用の製品が含まれていない場合、その製品のプラグインは用意されていません。
5. ご使用条件および説明を読んだら、「**I agree**」をクリックします。
6. IBM Support Assistant を再始動します。

フィックスの入手

以下は英語のみの対応となります。お客様の問題の解決に、プロダクトのフィックスが有効な場合があります。ご使用の Tivoli ソフトウェア・プロダクトに使用可能なフィックスを判別するには、以下のステップを実行してください。

1. IBM ソフトウェア・サポートの Web サイト (http://www.ibm.com/software/support) にアクセスします。
2. 「**Select a brand and/or product**」で、「**Tivoli**」を選択します。

   「**Go**」をクリックした場合は、「**Search within all of Tivoli support**」セクションが表示されます。「**Go**」をクリックしない場合は、「**Select a product**」セクションが表示されます。
3. 製品を選択して「**Go**」をクリックします。
4. 「**Download**」で、フィックスの名前をクリックしてその説明を参照し、必要に応じてそのフィックスをダウンロードします。

   選択した製品で「**Download**」という見出しが表示されない場合は、「**Search Support (製品名)**」の下のフィールドに、検索語、エラー・コード、または APAR 番号を入力して、「**Search**」をクリックします。

入手可能なフィックスのタイプについて詳しくは、「*IBM Software Support Handbook*」(http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) を参照してください。

各週のサポート更新情報の入手

以下は英語のみの対応となります。フィックスおよびその他のソフトウェア・サポート・ニュースに関する E メール通知を毎週受け取るには、次のステップを実行します。

1. IBM ソフトウェア・サポートの Web サイト (http://www.ibm.com/software/support) にアクセスします。
2. ページの右上隅の、「**Personalized support**」の下にある「**My support**」をクリックします。

3. 「**My support**」に登録済みの場合は、サインインして次のステップにスキップします。登録が済んでいない場合は、「**register now**」をクリックします。IBM ID として E メール・アドレスを登録フォームに記入し、「**Submit**」をクリックします。
4. 「**Edit profile**」タブが表示されます。
5. 「**Products**」の下の 1 つ目のリストで、「**Software**」を選択します。 2 つ目のリストで、製品カテゴリー (例えば、「**Systems and Asset Management**」) を選択します。 3 つ目のリストで、製品サブカテゴリー (例えば、「**Application Performance & Availability**」や「**Systems Performance**」) を選択します。該当する製品のリストが表示されます。
6. 更新情報を受け取る製品を選択します。
7. 「**Add products**」をクリックします。
8. 関心のある製品をすべてを選択したら、「**Edit profile**」タブの「**Subscribe to email**」をクリックします。
9. 「**Documents**」リストで、「**Software**」を選択します。
10. 「**Please send these documents by weekly email**」を選択します。
11. 必要であれば、お客様の E メール・アドレスを更新します。
12. 受け取る資料のタイプを選択します。
13. 「**Update**」をクリックします。

「**My support**」フィーチャーで問題が発生した場合は、以下のいずれかの方法でヘルプを入手できます。

オンライン

erchelp@ca.ibm.com に、問題を説明した E メールを送信してください。

電話 1-800-IBM-4You (1-800-426-4968) に電話してください。

IBM ソフトウェア・サポートへの連絡

以下は英語のみの対応となります。IBM ソフトウェア・サポートでは、製品の問題点に関するサポートを提供します。この支援を入手する方法としては、IBM Support Assistant から PMR または ETR を直接提出する方法が一番簡単です。

IBM ソフトウェア・サポートにご連絡いただく前に、お客様の会社が現在有効な IBM ソフトウェア保守契約をお持ちであり、お客様が IBM への問題報告の権限をお持ちであることを確認してください。必要なソフトウェア保守契約は、ご使用の製品に応じて異なります。

- IBM 分散ソフトウェア製品 (Tivoli、Lotus®、Rational® 製品のほか、Windows または UNIX オペレーティング・システムで稼働している DB2 および WebSphere 製品を含みますが、これだけに限定されません) の場合には、以下のいずれかの方法で、Passport Advantage® に登録してください。

  オンライン

  パスポート・アドバンテージの Web サイト (http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm) にアクセスします。

  電話 お客様の国の連絡先の電話番号を調べるには、IBM ソフトウェア・サポ

ートの Web サイト (http://techsupport.services.ibm.com/guides/contacts.html) にアクセスし、地域名をクリックしてください。

- サブスクリプションとサポート (S & S) 契約を締結されているお客様は、Software Service Request の web サイト (https://techsupport.services.ibm.com/ssr/login) にアクセスしてください。
- Linux、iSeries、pSeries®、zSeries、およびその他のサポート契約をお持ちのお客様は、IBM Support Line の web サイト (http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006) にアクセスしてください。
- IBM eServer™ ソフトウェア製品 (zSeries、pSeries、および iSeries 環境で実行されている DB2 および WebSphere 製品を含みますが、これだけに限定されません) の場合は、IBM 営業担当員または IBM ビジネス・パートナーに直接ご相談いただくことによって、ソフトウェア保守契約を購入することができます。eServer ソフトウェア・プロダクトのサポートについての詳細は、IBM Technical Support Advantage の Web サイト (http://www.ibm.com/servers/eserver/techsupport.html) にアクセスしてください。

必要なソフトウェア保守契約のタイプが不明な場合は、アメリカ合衆国の 1-800-IBMSERV (1-800-426-7378) に電話してください。その他の国からは、Web 上の「*IBM Software Support Handbook*」の「Contacts」ページ (http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html) にアクセスし、地域名をクリックして、お客様の地域でサポートを提供する担当者の電話番号を調べてください。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものであり、本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。 これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。

国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラット

フォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、 IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Adobe、Acrobat、PostScript およびすべての Adobe 関連の商標およびロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

IT Infrastructure Library は英国 Office of Government Commerce の一部である the Central Computer and Telecommunications Agency の登録商標です。

インテル、Intel、Intel ロゴ、Intel Inside、Intel Inside ロゴ、Centrino、Intel Centrino ロゴ、Celeron、Xeon、Intel SpeedStep、Itanium、Pentium は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

ITIL は英国 The Minister for the Cabinet Office の登録商標および共同体登録商標であって、米国特許商標庁にて登録されています。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Cell Broadband Engine は、Sony Computer Entertainment, Inc.の米国およびその他の国における商標であり、同社の許諾を受けて使用しています。

Linear Tape-Open、LTO、LTO ロゴ、Ultrium および Ultrium ロゴは、HP、IBM Corp. および Quantum の米国およびその他の国における商標です。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

アーカイブ手順
  Windows の AT コマンドを使用した 559
アクション実行コマンド
  のユーザー ID 193
アクションの実行
  SOAP 要求の 619
アクセス許可グループ・プロファイル 446, 481
アクセス制御リスト
  セキュリティー 197
一元化された構成 475
  開始 500
  開始、エージェント環境変数を使用した 500
  開始、サービス・インターフェース要求を使用した 506
  開始、リモート・デプロイメントを使用した 504
  開始、ロード・リスト・ファイルを使用した 503
  概要 475
  環境変数 491
  キーワード、ロード・リスト 488
  計画 476
  セットアップ例 496
  AAGP セキュリティー 446
  Disp=Custom セキュリティー 481
  XML 仕様 481
イベント
  添付ファイルのサイズの管理 83
  同期化、IBM Tivoli Enterprise Console の 279
イベントの同期 281, 307
  変更、構成の 280
  sitconfig.sh コマンド 280
イベント・キャッシュ 279
イベント・コンソール 283
イベント・サーバー上
  参照： TEC
イベント・メッセージ 273, 291
インストール 20
インポート
  ポータル・サーバーのデータベース 606
  ポータル・サーバー・データベース、Linux または UNIX システム 609
ウィンドウ
  Tivoli Enterprise Portal パラメーターの編集 67
ウェアハウス・プロキシー
  ATTRLIB ディレクトリー 525
ウェアハウス・プロキシー・エージェント (warehouse proxy agent)
  エラー・ロギング 550
エージェント
  自己記述型
    参照： 自己記述型エージェント
エージェント (agent)
  インストール 329
  スロット 274
エージェント Watchdog 346
エージェント管理 サービス Watchdog 346
エージェント管理サービス 345
  アクション実行コマンド 353
  インストールおよび構成 347
  エージェントの可用性のモニター 352
  エージェントの手動管理 353
  機能 345
  システム・モニター・エージェント上 371
エージェント・オートノミー
  アクティビティー・ログ 657
  エージェント (agent)
    オペレーション・ログ 657
  概要 355
  環境変数 360
  機能 355
  サービス・インターフェース 444
  OMNIbus SNMP プローブ 418
  z/OS 508
エージェント・オペレーション・ログ
  ヒストリーの収集 551
エージェント・サービス・インターフェース 444
  エージェント情報 452
  開始 445
  開始、一元化された構成の 506
  サービス・インターフェース要求 456
  シチュエーション 453
  照会 455
  専用ヒストリー・レポート 454
エージェント・サービス・インターフェース *(続き)*
  要求 CNFGCONTROL 473
  要求、AGENTINFO 457
  要求、AGENTSTAT 469
  要求、ATTRLIST 459
  要求、HISTREAD 471
  要求、LISTSUBNODE 458
  要求、PVTCONTROL 467
  要求、READATTR 460
  要求、REPORT 462
  要求、SITSUMMARY 468
  要求、TABLESIT 466
エージェント・サブノード
  シチュエーション制限 369
  専用ヒストリー配布 376
永続データ・ストア 569
エクスポート
  ポータル・サーバーのデータベース 605
エクスポートされたエンタープライズ・シチュエーション 386
エンタープライズ・シチュエーションおよび専用シチュエーション 373
エンタープライズ・モニター・エージェント 500
オートノマス・エージェント
  シチュエーションの duper プロセス 86
オートノマス・エージェントの動作
  シチュエーション制限 367
オートノミー
  参照： エージェント・オートノミー
お客様サポート 665, 667
  受信、各週の更新情報 666
オペレーション・ログ 657
オンライン・ヘルプ 27

[カ行]

開始、一元化された構成の 500
開始、一元化された構成の、ファイルの配置による 503
鍵データベース、作成 254
カスタマイズ、ヒストリー変換の 564
環境 20
環境構成
  ポータル・サーバー 79
環境ファイル
  オートメーション・サーバー 88
  ポータル・サーバー 79

環境ファイル *(続き)*
モニター・サーバー 86
環境変数
エージェント (agent) 560
エージェント・オートノミー 360
構成ロード・リスト 489
中央構成サーバーおよびクライアント 491
CMS_DUPER 86
KCA_CAP_DIR 347
KCA_CMD_TIMEOUT 347
KCA_MAX_RETRIES_ON_PIPE 347
KMS_EVAL_REFLEX_AT_TEMS 86
SOAP_IS_SECURE 616
監査
アクション実行 (Take Action) 269
イベント・レコード・タイプ 259
環境変数 266
許可ポリシー 217
属性にマップされる XML 261
トレース・レベル 259
ログ・ファイル 259
tacmd executecommand 269
XML の例 264
監査ログ 259
管理
システム管理者の役割 5
管理コンソール 119
外部 LDAP サーバーの構成 121
管理対象システム
説明 6
ポータルからの構成 313
管理対象システム (managed system)
追加、ポータルによる 311
ポータルからのパッチの適用 315
管理対象システムの構成 313
管理対象システムの追加 311
管理対象システム・グループ
セキュリティー 197
キーワード、構成ロード・リスト 488
起動、アプリケーション 27
キャパシティー・プランニング
Tivoli Data Warehouse 542
共通イベント・コンソール 301
特殊列 306
共通エージェント・パッケージ 347
許可ポリシー・サーバー 197
概念 198
監査 217
構成
SSL 237
SSL、サード・パーティー証明書の使用 239
SSL、ポータル・サーバーの準備 244
許可ポリシー・サーバー *(続き)*
構成 *(続き)*
SSL、Tivoli 許可ポリシー CLI の準備 242
SSL、WebSphere 証明書の使用 239
コマンド行インターフェース (CLI) 209
シナリオ
デプロイメント 222
デプロイメント、共有の役割およびポリシーを使用する複数のドメイン 222
デプロイメント、独自のポリシーを使用する複数のドメイン 223
ポリシー管理 204
ポリシー管理、ドメインに基づいた 223
ポリシー管理、PolicyDistributor 208
ポリシー管理、RoleAdministrator 207
前提条件 220
ドメイン、複数 221
ベスト・プラクティス 204
ポリシーの作成、ベスト・プラクティス 204
役割、管理 209
役割、事前定義 201
役割グループ 221
有効にする準備 203
区切り文字で区切られているフラット・ファイル 556
組み込み WebSphere Application Server 250
クライアント (client)
エミュレーション環境内の 73
グローバル・パラメーター 67
デスクトップ 9
ブラウザー 9
Java Web Start 9
SOAP の使用 616
グラフ (chart) 633
グラフィックス
ポータル・バナーのカスタマイズ 18
グラフ・ビューのページ・サイズ 70
グローバル・パラメーター 67
公開鍵と秘密鍵のペア
作成 255
更新、エージェントの 317
構成
共通イベント・コンソール 301
コネクター 301
構成ウィンドウ 301
構成ロード・リスト 490, 503
構成ロード・リスト *(続き)*
開始、一元化された構成の、tacmd putfile を使用した 505
環境変数 489
キーワード 488
kshsoap コマンド 507
XML 仕様 481
コマンド
sitconfig.sh 280
コマンド行 98
コンポーネント 6

[サ行]

再構成
ブラウザー・クライアント 129
最大ディレクトリー・サイズ 556
削除、エージェントの 316
作成、ショートカット 24
サポート・アシスタント 665
サンプル (sample)
データマート
SQL スクリプト 522
サンプル・シチュエーション 281
しきい値オーバーライド XML 399
識別名 128
TEP ユーザー ID へのマッピング 184
TEPS/e 管理コンソール 119
自己記述型エージェント 321, 329
インストール・エラー 331
インストール・オプション 333
エージェントでの無効化 338
エージェントでの有効化 338
環境変数 341
サーバー・イベント・フローのモニター 326
再開 334
再試行可能なエラー 331
再試行不能なエラー 331
シード 335
自動最新表示 335
中断 334
リモート・モニター・サーバーでの無効化 337
リモート・モニター・サーバーでの有効化 337
SDA が有効なエージェント 339
STATUS コード 331
自己署名証明書 255
システム管理者 10
システム・モニター・エージェント
エージェント管理サービス 371
開始、一元化された構成の 501
シチュエーション
イベント統合、OMNIbus との 299

シチュエーション *(続き)*
オートノマス・エージェントの動作 367
状況、エージェント・サービス・インターフェース 453
専用
参照： 専用シチュエーション
duper プロセス 86
シチュエーション (situation)
サウンド・パラメーター 71
SOAP 要求 619
シチュエーションの説明 273
シチュエーション・イベント 291
マップ 271
シチュエーション・オーバーライド XML 399
指定、ブラウザー 27
手動変換 563
照会
エージェント・サービス・インターフェースの k<pc>.atr 455
バックアップ 603
証明書
自己署名証明書、使用 255
CA 証明書の受信 256
CA 証明書の要求 255
CA 証明書要求の作成 255
シングル・サインオン (single sign-on) 106, 129
ポータル・サーバーと LDAP レジストリーのロードマップ 108
モニター・サーバー認証を使用して使用できない 137, 157
スキーマ・パブリケーション・ツール
Tivoli Common Reporting ディメンション表の作成 580
スクリプト
端末の最大 72
スケジュール
ヒストリー・データ変換 563
正規表現 380
生成 633
セキュリティー
アクセス制御リスト 197
管理対象システム・グループ 197
許可ポリシー・サーバー 197
役割ベース 197
LDAP および SSO 対応のポータル・サーバー 102
参照： アクセス許可グループ・プロファイル
セキュリティー設定 16, 17
接続
ダッシュボード・データ・プロバイダー 60
前提条件
認証の構成 103
専用シチュエーション 373
エクスポートされたエンタープライズ・シチュエーションから 386
開始、停止、再開 467
制限 367
特性 373
例 392
XML 仕様 376
専用ヒストリー 373
エージェント・サービス・インターフェース・レポート 454
操作
要約 633
属性の書式設定 565, 566
ソフトウェア・サポート
連絡 667

[タ行]

ダッシュボード 31
カスタム・ダッシュボードの作成 63
構成
SSL、サード・パーティー証明書の使用 234
SSL、Dashboard Application Services Hub サーバー 236
ロードマップ
SSO およびポリシー 37
SSO およびポリシーなし 31
SSO およびポリシーへの移行 52
KD8_VM_IMPORT_ID 66
SSL 233
UISolutions 66
ダッシュボード・データ・プロバイダー
接続の作成 60
短期ヒストリー
制限、ファイル・サイズの 555
データ変換プログラム 553
短期ヒストリー・ファイル 556
端末ビュー
パラメーター 72
遅延確認通知 615
チューニング
Tivoli Data Warehouse 542
チューニング・パラメーター 283
中央構成サーバー
としての Web サーバー 476
Web サーバー
中央構成サーバーとして 476
重複したイベント情報 307
通信
ハートビート間隔 70
パイプライン因子 71
HTTP プロキシー・サーバー 72
データウェアハウス
キャパシティー・プランニング (capacity planning) 542
チューニング 542
データ変換
使用、PDS での KPDXTRA の 566
UNIX システムでの 563
z/OS システムでの自動的な 565
データマート 521
データ・スナップショット 633
定義
モニター・サーバー
参照： TEMS
ディスカバリー・ライブラリー・アダプター 641, 643, 645
z/OS 647
デスクトップ・クライアント 9
開始 18
複数インスタンス 25
ポータル・サーバーからのダウンロード 23
ログ、場所 22
Web Start を使用した、起動用ショートカットの作成 24
デスクトップ・クライアントを起動するショートカット 24
デスクトップ・モード
データ・バス・パラメーター 71
デプロイメント状況表 318
同期化、シチュエーション・イベントの
IBM Tivoli Enterprise Console 279
統合化暗号サービス機能 78, 79
統合パラメーター 283
閉じる
イベント 281
トラップ XML 仕様 407
シチュエーション 411
SNMP 407
StatTrap 414
TrapAttrGroup 410
TrapDest 407
トラブルシューティング
エミュレーション環境内のクライアント 73
接続 308
トレース・パラメーター 73
Java アプレット 15
Java 例外 17
トレース
パラメーター 73

[ナ行]

認証
外部 LDAP レジストリーを使用 137
使用可能化 91

認証 *(続き)*
マイグレーション 134
Active Directory の使用 137
認証の構成 97, 98, 99

[ハ行]

ハートビート
EIF 宛先 XML 433
パスワード
トラップ構成ファイル内での暗号化 416
パスワード、stash ファイルへの保存 256
バックアップ
照会 603
バナー、ブラウザー・モードの 18
パフォーマンスの影響
ウェアハウジング 521
大規模なテーブルからのヒストリカル・データの要求 520
ハブ・モニター・サーバー 94, 95, 97
Linux または UNIX でのユーザー認証の構成 98
SSL と LDAP サーバー 232
Windows でのユーザー・セキュリティーの構成 97
パラメーター
参照： 環境変数
パラメーター (parameter)
アクティブ端末セッション 72
イベント・サウンドの一時停止 71
エージェントのデプロイ 69
エンコード・コード・セット 70
外部 HTTP サーバー上のデスクトップ・モード用データ・バス 71
グローバル、編集 67
スレッド化されたトレース呼び出し 73
端末エミュレーター localhost 72
端末エミュレーター・タイプ 72
端末エミュレーター・ポート 72
端末スクリプトの最大 72
添付ファイルのサイズ 69
トレース・オプション 73
トレース・クライアント ID 69, 73
トレース・スレッドの qdepth 73
トレース・ファイル名 73
トレース・ローカルまたはリモート 73
ハートビート間隔 70
パイプライン因子 71
ビューのページ・サイズ 70
ビュー変更の警告プロンプト 72
マウス・ドラッグ感度 70
ワークスペース切り替え遅延 71, 72
ワークスペース・ヒストリー 70
パラメーター (parameter) *(続き)*
HTTP プロキシー・サーバー 72, 73
user.language 73
user.region 74
Windows タスクバー 71
汎用マッピング 274
ヒストリー
ウェアハウス・プロキシーのエラー・ロギング 550
エージェント・オペレーション・ログ 551
サービス・インターフェース要求 471
専用 397
参照： 専用ヒストリー
データ収集 10
データ収集について 511
ベスト・プラクティス 542
変換、短期からフラット・ファイルへの 557
変更、短期ディレクトリー 518
要約およびプルーニング 539
ワークスペース・パラメーター 70
ヒストリカル
Windows でのファイルの場所 560
ヒストリカル・データ
影響、大量データ収集の 519
管理 511, 514
tacmd 514
ヒストリカル・データ収集
設定、短期ファイル・サイズ制限の 555
パフォーマンスへの影響、大規模なデータ要求の 519
要約およびプルーニングの構成 545
ヒストリカル・データの変換 553
HP NSK での 564
IBM i 561
Linux または UNIX 上での 562
Windows 上で 559
z/OS 上 565
ヒストリカル・データ・ファイル
デフォルト・テーブル 555
z/OS 上 569
ヒストリカル・レポート
大規模なテーブルのパフォーマンスへの影響 520
非対称暗号化
鍵データベース、作成 254
公開鍵と秘密鍵のペア、作成 255
自己署名証明書、使用 255
設定 229
パスワード、stash ファイルへの保存 256
CA 証明書、受信 256
CA 証明書要求、作成 255
stash ファイル 256
表ビューのページ・サイズ 70
ブートストラップ 490
フィックス、入手 666
複製、ポータル・サーバーの 603
前提条件 603
「物理」ナビゲーター・ビュー 311
プライベート・ネットワーク 645
ブラウザー・クライアント 9, 15
開始 18
設定、プロパティーの、Linux または UNIX の 76
バナーのカスタマイズ 18
ファイル・パッケージおよび Cookie 16
複数インスタンスの有効化 26
IE のセキュリティー設定 16
Linux または UNIX
設定、ブラウザー・クライアント・プロパティーの 76
Windows の許可 17
ブラウザー・モード
ワークスペース切り替え遅延 71
プロキシー
HTTP サーバー・パラメーター 72
プロキシー・エージェント・サービス
Watchdog 346
プロセス
kfwServices 79
変換
短期ヒストリカル・データ・テーブル 562
変換、データの
z/OS システムでの自動的な 565
変換処理
HP NonStop Kernel システムでの 564
ポータル・クライアント
パラメーター 68
変数 68
ポータル・クライアント 68
ポータル・サーバー
同じコンピューターから 2 つにログオン 26
環境変数 80
データベースのインポート 606
データベースのエクスポート 605
バックアップ 603
複製 603
複製の前提条件 603
別の接続 25
変数 80
ポータル・サーバー 80
マイグレーション、認証の 134
無効化、LDAP 認証の 133
ユーザー認証 171

ポータル・サーバー *(続き)*
ユーザー ID およびアクセス権の作成 144
ユーザー ID の識別名へのマッピング 151
ユーザー・シナリオ 162
Active Directory の有効化および構成 144
LDAP 認証の有効化 152, 162
Active Directory 経由のユーザー認証 137
FIPS の使用可能化 244
LDAP の SSL 125
LDAP を構成する Linux コマンド行または UNIX コマンド行 117
「Tivoli Enterprise Monitoring Services の管理」による LDAP の構成 113
参照： TEPS
参照： Tivoli Enterprise Portal Server
ポータル・サーバー環境変数
KFW_ATTACHMENT_SEGMENT_MAX 83
KFW_ATTACHMENT_MAX 83
KFW_EVENT_RETENTION 82
KFW_PRUNE_END 82
KFW_PRUNE_START 82
ポータル・サーバーと LDAP サーバー間の SSL 119
ポータル・サーバーの環境変数
KFW_AUTHORIZATION_MAX_INVALID_LOGIN 84
ポータル・デスクトップ・クライアント
開始 18
IBM Java Web Start を使用したダウンロード 19
ポータル・ブラウザー・クライアント
開始 18
保持 17
保存、データをデータベースに 556
ポリシー (policy)
SOAP 要求 619
本書について xiii
本リリースの新機能 1

[マ行]

マイグレーション
認証 134
マップ
カスタマイズ可能な列 307
メタ記述ファイル 553
モニター (monitoring)
エージェント管理サービス 345
モニター・エージェント 311
一元化された構成、管理する 475
開始 314
モニター・エージェント *(続き)*
可用性のモニター 352
接続先、別のモニター・サーバー 320
停止 314
デプロイメント状況表のクリア 318
ポータルからの構成 313
ポータルからのパッチの適用 315
ポータル・クライアントでの管理 311
リサイクル 314
割り当て、ポータルによる 311
参照： エンタープライズ・モニター・エージェント
モニター・エージェントの開始 314
モニター・エージェントの停止 314
モニター・エージェントのリサイクル 314
モニター・サーバー
接続、エージェントを別のモニター・サーバーに 320
マイグレーション、認証の 134
ユーザー認証
ポータル・サーバー認証と比較した場合の欠点 137, 157
ユーザー ID の制限 153, 157
ユーザー・シナリオ 157
有効化および構成 152
Active Directory 経由 137
参照： TEMS
問題解決 665

[ヤ行]

ユーザー ID 128, 182
デフォルト・ユーザー 186
認証の使用可能化 91
ユーザー ID の削除 185
ユーザー ID の追加 182
ユーザー ID の表示と編集 184
IBM Tivoli Monitoring Web サービス 617
Windows Users グループ 17
ユーザー管理 173, 175
アクション実行コマンド用のユーザー ID 193
アクセス権のユーザーへの付与 191
アプリケーション 180
許可 176
主要な制御 190
デフォルト・ユーザー 191
ナビゲーター・ビュー 181
メンバー 182
ユーザー ID およびグループ 191
ユーザー ID の管理 182
「ユーザーおよびユーザー・グループ」ウィンドウ 175
ユーザー・アクセスの検証 192
ユーザー管理 *(続き)*
ユーザー・グループの管理 186
ログオン・エラー・メッセージのトラブルシューティング 194
ワークスペース管理モード 190
Dashboard Application Services Hub のユーザー ID 191
SYSADMIN ログオン ID 190
ユーザー検証 95
参照： ユーザー認証
ユーザー認証 94, 95, 97, 98, 99
オートメーション・サーバー 136
新規 LDAP ユーザー 132
シングル・サインオン 106
ポータル・サーバー 102
Active Directory 経由 137
LDAP を使用するシングル・サインオンのロードマップ 108
ユーザー・グループ 186
検討および編集 189
削除 190
追加 187
メンバーシップの表示 187
ユーザー・セキュリティー
Linux または UNIX でのハブ・モニター・サーバーの構成 98
Windows でのハブ・モニター・サーバーの構成 97
要約およびプルーニング 513, 545
グローバル構成 546
構成 539
使用不可にする 550
説明 539
データの可用性 544
要約およびプルーニング・エージェント
Tivoli Common Reporting の制限 575
「要約およびプルーニング・エージェントの構成」ウィンドウ 546

[ラ行]

ランタイム 20
リリース 情報 1
ルール検査ユーティリティー・ツール 284
レポート
参照： IBM Cognos レポート
レポート・インストーラー 590
ログイン・デーモン 320
ログオン
試行回数の制御 84
ログオン・エラー・メッセージ 612
ログオン・エラー・メッセージのトラブルシューティング 194

［ワ行］

ワークスペース (workspace)
　ヒストリー・パラメーター　70

［数字］

1 回限りの変換　563

A

AAGP
　参照： アクセス許可グループ・プロファイル
Active Directory、Microsoft　137
　モニター・サーバー認証
　　ユーザー ID の制限　153
　ユーザー・アカウント　158
　　データ収集スクリプト　142
　IBM Tivoli Monitoring
　　同期　142
　　OU 階層、作成された　138
　LDAP tools
　　LDP.exe　163
　LDAP スキーマ
　　カスタマイズ　137
　　ユーザー・オブジェクト/属性スキーマ　138
　LDAP ツール　154
　　ldapbrowser　156, 159, 163
　　ldapsearch　156, 162
　　LDP.exe　155
　LDAP ユーザー認証　137
　LDAP リポジトリー
　　識別名のマッピング　151
　　定義　145
　　SSL 通信のための構成　160
　　TLS/SSL 通信のための構成　152
AF REXX　633
AIX　615
APPN エラー　619
ASCII と非 ASCII
　ユーザー ID　182
as.ini 環境ファイル　88
AT コマンド、Windows システムの　559
atr ファイル　455
ATTRLIB ディレクトリー　525

B

BAROC
　ファイル生成プログラム　295
BAROC イベント・クラス　284
BIRT レポート　596
　インストール、レポートの　596
BIRT レポート *(続き)*
　インポート、レポートの　596
　構成、データ・ソースの　598
　生成、レポートの　599

C

CA 証明書
　受信　256
　要求　255
CLEARDEPLOYSTATUSFREQ　318
cleardeploystatus.log　318
CLI　98, 317
CMS_DUPER　86
ConfigurationArtifact ルート要素　481
cookie　16
CTIRA_HIST_DIR　518, 561
CT_Get　633
CT_* SOAP メソッド　620

D

Dashboard Application Services Hub
　インポート、IBM Cognos レポートの　595
　カスタム・ダッシュボード　63
　ユーザー ID　191
DD 名、KPDXTRA の
　z/OS 上　567
developerWorks　662
disableLDAPRepository.sh　133
DLA　641
duper プロセス　86

E

EIF　291
　イベント宛先 XML 仕様　433
　イベント構成 XML　424
　イベント・マッピング XML 仕様　427
EIF イベント
　共通スロット　435
　直接送信、エージェントから受信側に　424
　ハートビート　439
　ハートビート・イベント　439
　マスター・リセット　439
　ライフサイクル　437
　SSL　440
enableISCLite.sh スクリプト　165
Enterprise Integration Facility
　複数コンソール・サポート (MCS)　292
　TEDGEN ユーティリティー　292
Event Integration Facility
　グローバリゼーションの有効化　276
　デフォルトを無効にする　289
Event Integration FacilitycreateEventDest
　構成の編集　285
　tacmd　285
eWAS
　インポート、証明書の　250

F

FIPS のサポート　244

G

GSKit
　JRE の設定および Key Manager の起動　253

H

HP NonStop Kernel　564
HP NSK
　krarloff ロールオフ・プログラムの使用　564
HTTP
　使用可能なプロキシー・サーバー　75
　プロキシー・サーバーの使用可能化　75
　kshsoap コマンド　619
HTTP サーバー
　外部を指定するデータ・バス・パラメーター　71

I

IBM Cognos レポート　592
　インポート　595
　インポート、レポート・インストーラーを使用した　590
　Dashboard Application Services Hub グラフの作成　596
IBM i
　ヒストリカル・データの変換　561
IBM Java Web Start
　デスクトップ・クライアントをダウンロードするために使用　19
IBM JRE
　インストール　20
IBM Redbooks　665
IBM Support Assistant　665
IBM Tivoli Enterprise Console
　イベント統合　271
IBM Tivoli Monitoring
　コンポーネント　6

IBM Tivoli Monitoring *(続き)*
Performance Monitoring サービス・プロバイダー 11
統合 137
HP NSK システムでの実行 564
WebSphere MQ 製品用 564
IBM Tivoli Monitoring Web サービス 612
概要 611
クライアントの開始 617
サンプル CT_Get SOAP 要求 632
システム・コマンドとしての SOAP 要求 619
シナリオ 633
第 2 レベル要求 630
定義済み SOAP メソッド 620
ユーザー ID 617
ユーザーの追加 613
レポート内容 636
SOAP クライアント 616
SOAP の説明と URL 611
IBM Tivoli Monitoring グラフ Web サービス 639
IBM ランタイム環境
インストール 20
Linux 21
Windows JRE 20
IFS ディレクトリー 561
Infrastructure Management Dashboards 31
Integrated Service Management Library 662
Integrated Solutions Console
参照： TEPS/e 管理コンソール
Internet Explorer
オプション - セキュリティ 16
ior URL 71
ISA 665
ITM 監査ログ 259
ITM コネクター 302
itmcmd history の実行、UNIX システムでの 563
itmcmd ヒストリー 562, 563
itmc_kdy.properties 318
itmpwdsnmp コマンド 416

J

Java 20
エミュレーション環境内の 73
Java Web Start 用の Windows の JRE 20
Java Web Start
ダウンロードに使用、デスクトップ・クライアントの 19
デスクトップ・クライアントのダウンロード 23
Java Web Start クライアント 9
Java ランタイム環境 15
GSKit 向け 253
JRE 20
トレースを使用可能にする 22
JRE に対するトレースを使用可能にする 22

K

KASENV ファイル 88
KBBENV ファイル 86
kcacap.xsd 347
KD8_VM_IMPORT_ID 66
KFWENV ファイル 79
KFW_AUTHORIZATION_MAX_INVALID_LOGIN 84
KFW_MCS_XML_FILES 292
KHD_HISTSIZE_EVAL_INTERVAL 555, 556
KHD_TOTAL_HIST_MAXSIZE 555, 556
KMS_EVAL_REFLEX_AT_TEMS 86
KMS_OMTEC_GLOBALIZATION_LOC 276
KPDXTRA 566
パラメーター 567
割り振る DDNAMES 567
KPDXTRA 属性 566
KPDXTRA プログラム
概要 566
メッセージ 568
krarloff 557
krarloff ロールオフ属性 565
krarloff ロールオフ・プログラム
HP NonStop Kernel システム
ヒストリカル・データの変換 564
HP NSK での 564
HP NSK でのファイルの変換 564
IBM i 561
Linux または UNIX 上での 562
Windows
ヒストリカル・データの変換 559
Windows 上で 559
z/OS
ヒストリカル・データの変換 565
z/OS 上 565
kshsoap 619
KSY_Summarization_Config_DV 587
KSY_TRAM_ENABLE 578
KSY_TRAM_TD_GRANULARITY 578
KSY_TRAM_TD_INITIAL_LOAD 578
kwgcap.xsd 347

L

LDAP 128
外部サーバーの構成 121
新規ユーザー 132
ポータル・サーバー構成 113, 117
ポータル・サーバーに SSL を使用する 125
無効化、ポータル・サーバー認証 133
ldapsearch 100
サンプル・コマンド (TLS/SSL 不使用) 101
SSL を使用したサンプル・コマンド 102
ldapsearch コマンド行オプション 100
Lightweight Directory Access Protocol
Active Directory、Microsoft 137
Linux 308, 614
Linux OS lz_situations.xml 392
Linux から 608
Linux へ 607
Linux または UNIX
ヒストリカル・データの変換 562
Linux_IP_Addres 587
LTPA キー 130
LTPA キーのインポート 130
LTPA キーのエクスポート 130

M

MANAGEDSYSTEMLIST 578
MANAGEDSYSTEMLISTMEMBERS 578
MCS 属性サービス 292
Microsoft 管理コンソール 143
「ADSI 編集」スナップイン 154
migrate-export スクリプト 605
migrate-import 606, 607, 608
Linux または UNIX から Linux または UNIX への 609
migrate-import スクリプト 606
ms.ini 環境ファイル 86

N

Netcool/OMNIbus
証明書 442
EIF、SSL を使用 440
NetView
コンソール 297
NT_Computer_Information 587

O

OMNIbus
エンタープライズ・シチュエーション・イベント統合 299
ハートビート自動化機能 423
有効にする、ハートビート自動化機能 423
EE_HEARTBEAT 状況イベント 423
EIF イベント
OMNIbus ハートビート自動化機能 423
SNMP アラート
OMNIbus ハートビート自動化機能 423
SNMP アラートのルールのサンプル 420
OMNIbus コネクター 304, 307
Open Services Lifecycle Collaboration Performance Monitoring サービス・プロバイダー 11
OS Agents Reports 前提条件スキャナー 592
OS エージェントの依存関係 643
OSLC-PM 11

P

PDS 569
Performance Monitoring サービス・プロバイダー 11
PolicyDistributor 208
putfile 505

Q

qi.ini 環境ファイル 79

R

Redbooks 662, 665
REGEX 380
RoleAdministrator 207, 209

S

SA IO REXX アプリケーション 635
Service Management Connect 662, 665
Simple Object Access Protocol (SOAP) クライアント要求 611
sitconfig.sh コマンド 280
SMC 662, 665
SNMP
シチュエーション要素 411
パス・キーの暗号化 416
SNMP *(続き)*
MIB エージェント・イベントのタイプ 417, 651
TrapAttrGroup XML エレメント 410
SNMP アラート 405
構成 405
サブノードを持つエージェントから 369
サンプルのトラップ構成ファイル 405
トラップ XML 仕様 407
OMNIbus ルールのサンプル 420
SNMP アラートおよびエージェント発行のための MIB
agentSitPureEvent 417, 651
agentSitSampledEvent 417, 651
agentStatusEvent 417, 651
SNMP アラートを受信する OMNIbus セットアップ 418
SNMP エレメント 407
SNMP トラップ
OMNIbus Multi-threaded Trapd プローブの構成 418
SOAP 611, 615
サーバー (server) 614
ブラウザーの開始 618
SOAP クライアント要求 611
SOAP サーバー 633
構成 612
セキュリティー 616
ハブの定義 612
ユーザーの追加 613
SOAP メソッド
CT_Acknowledge 620, 636
CT_Activate 621
CT_Alert 622, 635
CT_Deactivate 623
CT_EMail 623
CT_Execute 625
CT_Export 625
CT_Get 627, 632
CT_Redirect 628
CT_Reset 628
CT_Resurface 629
CT_WTO 630
SOAP_IS_SECURE 616
SSL 236
鍵データベース、作成 254
許可ポリシー・サーバーとの 237
公開鍵と秘密鍵のペア、作成 255
自己署名証明書、使用 255
ダッシュボード・データ・プロバイダーとの 233
パスワード、stash ファイルへの保存 256
ハブ・モニター・サーバーおよび LDAP サーバー間 232
SSL *(続き)*
非対称暗号化の設定 229
ポータル・サーバーと LDAP サーバー間 125
CA 証明書、受信 256
CA 証明書要求、作成 255
EIF イベント 440
Netcool/OMNIbus の証明書管理 442
stash ファイル 256
SSO 129
stash ファイル 256
StatTrap 要素 414
Summarization and Pruning agent
レポート表の自動化 578
Support Assistant 665
SYSADMIN 190
sysadmin 91
sy_situations.xml の要約およびプルーニング 395

T

tacmd 505
bulkExportPcy 603
bulkExportSit 373, 386, 603
bulkImportPcy 603
bulkImportSit 603
createSit 373, 611
exportNavigator 603
exportQueries 603
exportSitAssociations 603
exportSysAssignments 603
exportworkspaces 603
histconfiguregroups 360, 539
importNavigator 603
importQueries 603
importSitAssociations 603
importSysAssignments 603
importworkspaces 603
setOverride 360, 399
updateAgent 317
viewSit 386
z/OS
エージェント環境変数 360
tacmd addSdaInstallOptions 333
tacmd deleteSdaInstallOptions 333
tacmd editSdaInstallOptions 333
tacmd listappinstallrecs 329
tacmd listSdaInstallOptions 333
tacmd listSdaStatus 329
tacmd resumeSda 333, 334
tacmd setAgentConnection 320
tacmd suspendSda 333, 334
tacmdrefreshTECinfo
createEventDest 289
TCP 615

TEC イベントの同期化 271
TEC コネクター 303, 307
Technotes 662
TEDGEN ユーティリティー 292
TEP
参照： Tivoli Enterprise Portal
TEPS データベース
イベントのプルーニング 82
TEPS/e
開始 124
停止 124
TEPS/e 管理コンソール
開始 120, 124
基本 DN の変更 119
停止 124
ポータル・サーバーと LDAP サーバー間の SSL 119
有効化 120
TEPS/e 124
tivcmd CLI 197
Tivoli Common Reporting 571
以前のリリースからのアップグレード 574
制限 575
接続、Tivoli Data Warehouse への 593
前提条件 572
データベース・クライアント、ODBC を介する 593
ディメンション表 576
共有ディメンション表 583
時間ディメンション・テーブル 583
自動化 578
スキーマ・パブリケーション・ツールの使用 580
リソース・ディメンション表 587
Summarization and Pruning agentの構成 578
背景情報 571
レポート実行のためのヘルス・チェック 592
レポート・インストーラー 590
BIRT レポート 596
Dashboard Application Services Hub グラフの作成 596
IBM Cognos レポート 592
OS Agents Reports 前提条件スキャナー 592
Tivoli Data Warehouse
キャパシティー・プランニング (capacity planning) 542
短期ヒストリー構成 524
チューニング 542
範囲区画のマイグレーション 526
Tivoli Data Warehouse *(続き)*
DB2 for Linux, UNIX, and Windows 528
DB2 for z/OS 531
Oracle 536
ヒストリー
短期ファイル構成 524
Tivoli Common Reporting のための構成 576
Tivoli Data Warehouse
warehouse_situations.xml 396
Tivoli Enterprise Console
イベントの重大度 275
シチュエーション・イベント状況 276
ビュー (view) 297
Tivoli Enterprise Monitoring Agent
参照： エンタープライズ・モニター・エージェント
Tivoli Enterprise Monitoring Automation Server
環境変数 88
編集 88
Tivoli Enterprise Monitoring Services の管理 99
グローバル・パラメーター 67
SOAP ハブの定義 612
Tivoli Enterprise Portal 316
クライアント (client) 6
クライアントのタイプ 9
説明 6, 8
本リリースの新機能 1
Tivoli Enterprise Portal Server
参照： ポータル・サーバー
Tivoli Management Services
コンポーネント 6
Tivoli Monitoring Web Services
コマンド行ユーティリティー 619
ブラウザーの開始 618
SOAP
コマンド行ユーティリティー 619
Tivoli Monitoring サービス索引
エージェント・サービス・インターフェース 445
Tivoli 許可ポリシー CLI 209
Tivoli 許可ポリシー・サーバー
参照： 許可ポリシー・サーバー
TLS
参照： SSL
TMS DLA 641
tmsdla 641
TrapDest 要素 407

U

UISolutions
インポート 66
Universal Agent
イベント、Tivoli Enterprise Console への 295
UNIX 614
UNIX OS ux_situations.xml 393
UNIX から 608
UNIX へ 607
UNIX 変換 563
UNIX または Linux
ヒストリカル・データの変換 562
UNIX_IP_Address 587
updateTEPSEPass.sh スクリプト 164
URL 16
Users グループ特権 17
user.language 73
user.region 74
USE_EGG1_FLAG 78
UTF-8 エンコードされた XML 371

W

WAREHOUSEID 524
Web Start 24
Web サービス 611
構成 614
ハブの定義 612
Windows
場所、実行可能ファイルの 560
ヒストリカル・データ・テーブル・ファイルの場所 560
ユーザー・グループ 17
Windows OS nt_situations.xml 394
Windows から 606, 607
Windows システムの AT コマンド 559
Windows へ 606, 608

X

XML
しきい値 399
専用シチュエーション 376
専用ヒストリー 376
AGENTINFO 457
AGENTSTAT 469
ATTRLIST 459
CNFGLIST 481
EVENTDEST 424
EVENTMAP 424
HISTREAD 471
LISTSUBNODE 458
PVTCONTROL 467
READATTR 460
REPORT 456, 462
SITSUMMARY 456, 468

XML *(続き)*
situation_name (エクスポート済み) 386
TABLESIT 466
TRAPCNFG 405, 407
UTF-8 エンコード方式 371
z/OS
UTF-8 エンコードされた XML 371
参照： ローカル構成ファイル

Z

z/OS
エージェント・オートノミー 355, 508
手動アーカイブの手順 569
専用ヒストリーと PDS 397
データ変換、KPDXTRA を使用した 566
統合化暗号サービス機能 78, 79
場所、ヒストリカル・データ・ファイルの 569
ユーザー検証用の RACF または ACF/2 192
LDAP はハブではサポートされない 91
SNMP アラート、PCTRAPS 内の 405

［特殊文字］

*REGEX 380

Printed in Japan

SA88-5151-00

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21