HP OpenView Internet Services

ユーザーリファレンスガイド

Manufacturing Part Number: J4511-90008

2006 年 5 月

ご注意

1. 本書に記載した内容は、予告なしに変更することがあります。
2. 当社は、本書に関して特定目的の市場性と適合性に対する保証を含む一切の保証をいたしかねます。
3. 当社は、本書の記載事項の誤り、またはマテリアルの提供、性能、使用により発生した直接損害、間接損害、特別損害、付随的損害または結果損害については責任を負いかねますのでご了承ください。
4. 本製品パッケージとして提供した本書、CD-ROM などの媒体は本製品用だけにお使いください。プログラムをコピーする場合はバックアップ用だけにしてください。プログラムをそのままの形で、あるいは変更を加えて第三者に販売することは固く禁じられています。

Restricted Rights Legend

Trademark Notices

オープンソースに関する注意

本製品には、OpenSSL Project (http://www.openssl.org/) が開発したソフトウェアが含まれています (OpenSSL Toolkit で使用)。
本製品には、Eric Young (eay@cryptsoft.com) が作成した暗号化ソフトウェアが含まれています。
本製品には、Tim Hudson (tjh@cryptsoft.com) が作成したソフトウェアが含まれています。

他の open-source ライセンスについては `<install dir>¥license-agreements` を参照してください。

原典

本書は『HP OpenView Internet Services User's Reference Guide (HP Part No. J4511-90006)』を翻訳したものです。

サポート

次の HP OpenView web サイトをご参照ください。

http://www.managementsoftware.hp.com/

連絡先の情報および HP OpenView の提供する製品、サービス、サポートの詳細が掲載されています。

また、直接サポート Web サイトにアクセスすることもできます。

http://support.openview.hp.com/

HP OpenView オンラインソフトウェアサポートには、お客様がご自身で問題を解決していただける機能が備わっています。ビジネスを遂行するのに必要なインタラクティブなテクニカルサポートツールに簡単に効率良くアクセスすることができます。お客様は、以下の機能を利用することができます。

- 関心をお持ちの情報の検索
- サポート依頼の送信と進行状況のチェック
- サポート契約の管理
- HP サポート担当の一覧
- 利用可能なサービスについての調査
- 他のソフトウェアカスタマとの意見交換
- ソフトウェアトレーニングの調査と申し込み

大部分のサポートでは、HP Passport ユーザーとして登録して、ログインすることが必要です。また、多くの場合、サポート契約が必要です。

アクセスレベルの詳細は、以下の URL を参照してください。

http://support.openview.hp.com/access_level.jsp

HP Passport ID を登録するには、以下の URL にアクセスしてください。

https://passport.hp.com/hpp2/newuser.do

目次

1

Internet Services の概要

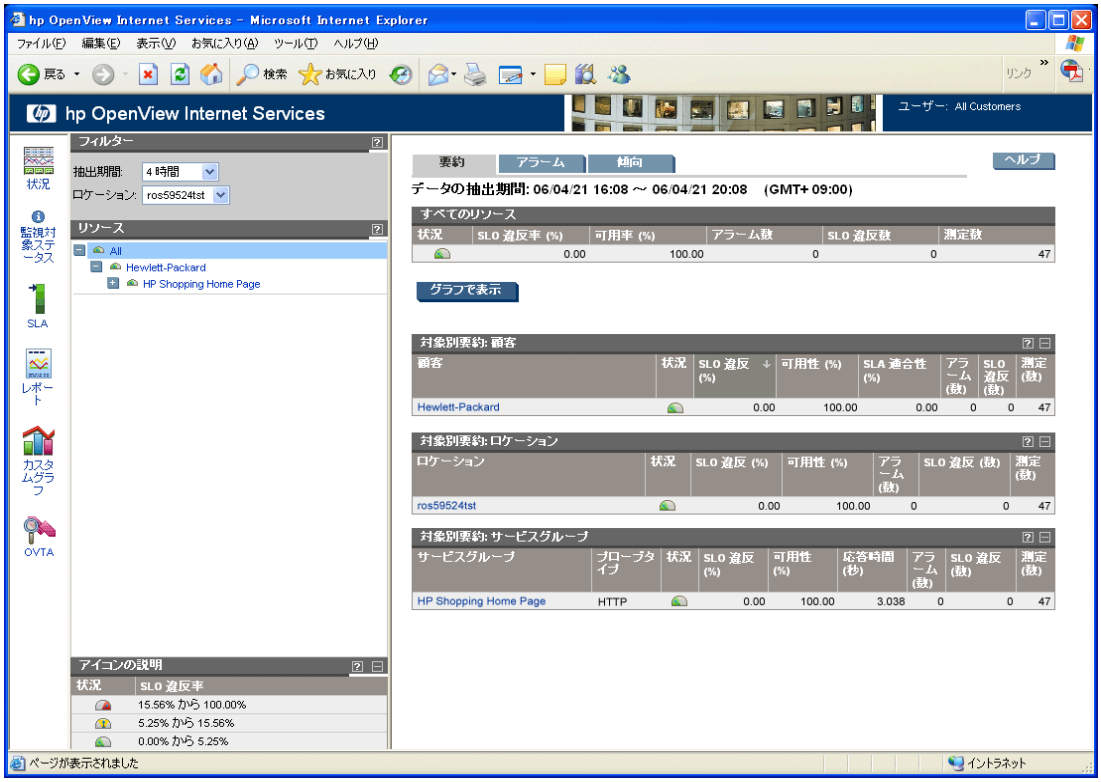
HP OpenView Internet Services (OVIS) では、IT サービスとビジネスサービスの統合ビューを使用して、IT 担当者は、問題の効率的な予測、分離、診断、トラブルシューティングを行ったり、容量不足を事前に予測したり、サービスレベル契約の管理やレポート作成ができるようになります。

また、従来のクライアントサーバーアプリケーション構造でサポートされているサービスもまた、サービスレベル契約に対応する、より積極的な管理が要求され始めています。サービスの可用性や性能が劣ると、ビジネスにかなりの影響を与えます。したがって、IT 部門は事業主に障害やスローダウンの通知や解決を提供するだけでなく、サービスの可用性と応答性の明確なサービスレベルを保証する必要があります。OVIS を使用すると、問題が起こった際に、IT およびネットワークの運用担当者は問題点を明確にして、すばやく解決したり、影響を与える顧客およびエンドユーザーに適切に連絡したりすることができます。

OVIS は、ソフトウェアプローブを使用してビジネスアクティビティをシミュレートします。これらのプローブは、インターネットと関連サービスの可用性、応答時間、および他のパフォーマンスメトリックを測定します。また、サービスレベル違反とサービスレベル契約の適合性についても監視し、報告します。プローブからのデータとサービスレベルに関する情報を表示するには、Internet Services ダッシュボードを起動します。ダッシュボードでは、グラフ、スナップショット、詳細なメトリックをまとめて、Web ブラウザ上に表示できます。

また、OVIS はアラームを生成でき、他の OpenView 製品で使用することもできます。アラームと定期的な更新情報により、顧客の IT サービスとビジネスサービスが効率的に動作しているかどうかを常に把握することができます。

Internet Services ダッシュボードを以下に示します。



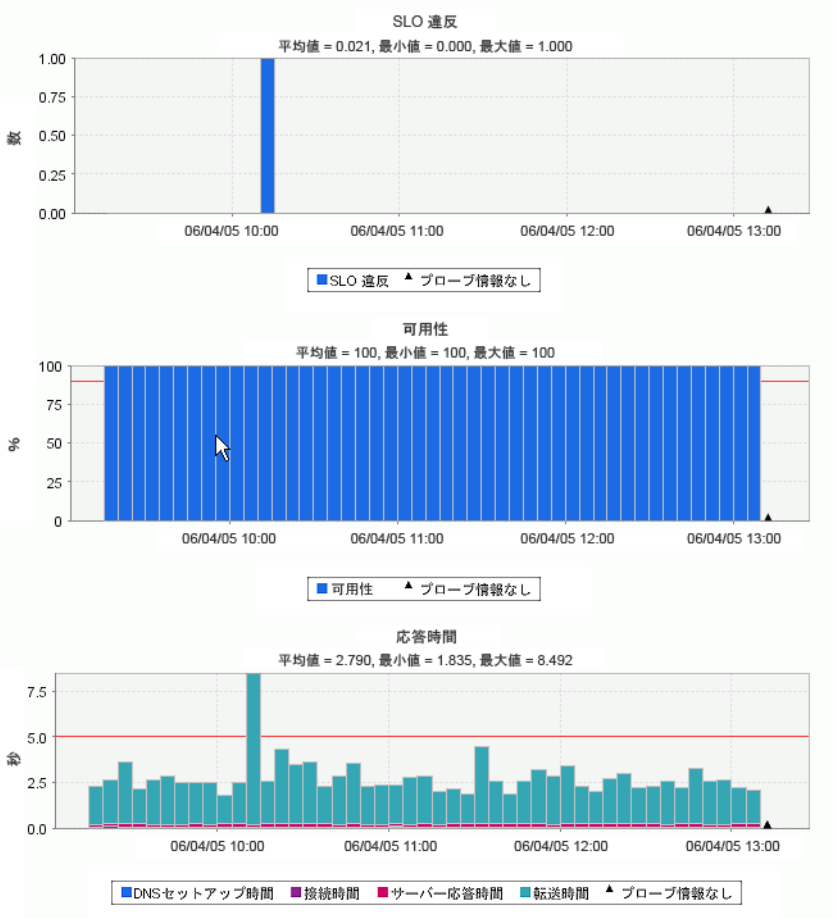
ダッシュボードには、以下の機能が用意されています。

- サービス状況の概要表示
- SLA、レポート作成 (夜間) とカスタムグラフビルダなどの機能へのアクセス
- 顧客、サービスグループ、プローブロケーション、および監視対象別のすべてのリソース状態の要約
- 可用性や応答時間などの主要な測定データの時系列データ表とグラフ

- 生成されたアラーム一覧
- 傾向グラフとベースライングラフ
- 診断ツールとコマンド (Troubleshooting Insight Packages (TIPs)) へのアクセス。これらを使用して問題を分析することができます (ツリービューから監視対象を選択し、TIPs リンクを使用するか、[アラーム] タブを選択してアラームに対応する TIP を使用します)。

ダッシュボードに関する詳細は、58 ページの「ダッシュボードによるデータの表示」を参照してください。

ダッシュボードから、監視対象を選択して、SLO 違反、可用性、応答時間、およびプローブの特定メトリックを示す時系列グラフを表示することができます。サービスレベル目標値はグラフの中で赤の水平線として示されます。グラフの棒上にマウスを置くとポップアップボックスが表示されメトリック値と時間間隔が表示されます。



Internet Services の動作

Internet Services を使用することにより、顧客のインターネットサービスを体系的に監視できます。インストールと設定が完了すると、可用性、応答時間、サービスレベルの適合性、および特定のサービスアクティビティの他のメトリックの測定が開始されます。

Internet Services では、HTTP、FTP、DNS、電子メールなどの数多くのサービスやプロトコル (**サービスの種類**) を監視できます。各サービスについての詳細は、第 4 章「サービスタイプとプローブの説明」を参照してください。

Internet Services **設定マネージャ**を使用して、Web サーバー上の Web ページへのアクセスなどのサービスの使用をシミュレートし、サービスのパフォーマンスと可用性を測定する**プローブ**を作成または設定します。その後、プローブを Windows または UNIX **プローブロケーション**に展開し、設定した間隔で自動的にサービスを測定します。

プローブの測定結果は、**Internet Services 管理サーバー**に返送され、データベース内に保存されます。データは整理統合され、Web ブラウザ上の Internet Services ダッシュボードに表示されます。

ダッシュボードから、監視対象すべてのサービスの現在の状態を確認し、可用性、応答時間、サービスレベル違反に関するより詳しいデータを取得することができます。また、データの長期間に渡る傾向グラフを表示したり、毎晩データを集約して作成される、カスタマイズ不要の**レポート**を参照することもできます。さらに、ダッシュボードから、診断ツールと **Troubleshooting Insight Packages (TIPs)** と呼ばれるコマンドを実行してサービスの問題やアラームを分析することができます。

サービスレベル契約は Internet Services 設定マネージャを使用して作成でき、その適合状況はダッシュボードで確認できます。

顧客のサービスの問題に関するサービス **アラーム** は、設定した測定しきい値に基づいて OVIS によって生成されます。それらのアラームを Network Node Manager (NNM)、OpenView Operations for Windows (OVO/Windows)、および OpenView Operations for UNIX (または IT Operations あるいは OVO として知られている)、または SNMP トラップを受信することができる他のイベントマネージャに転送することができます。これらアラームをダッシュボードに表示することもできます。

OpenView Transaction Analyzer (OVTA) によって収集されたデータをダッシュボードに統合して表示することができます。また、OVTA データのサービスレベル目標値とサービスレベル契約が定義されると、OVIS はこのデータのアラームを転送します。

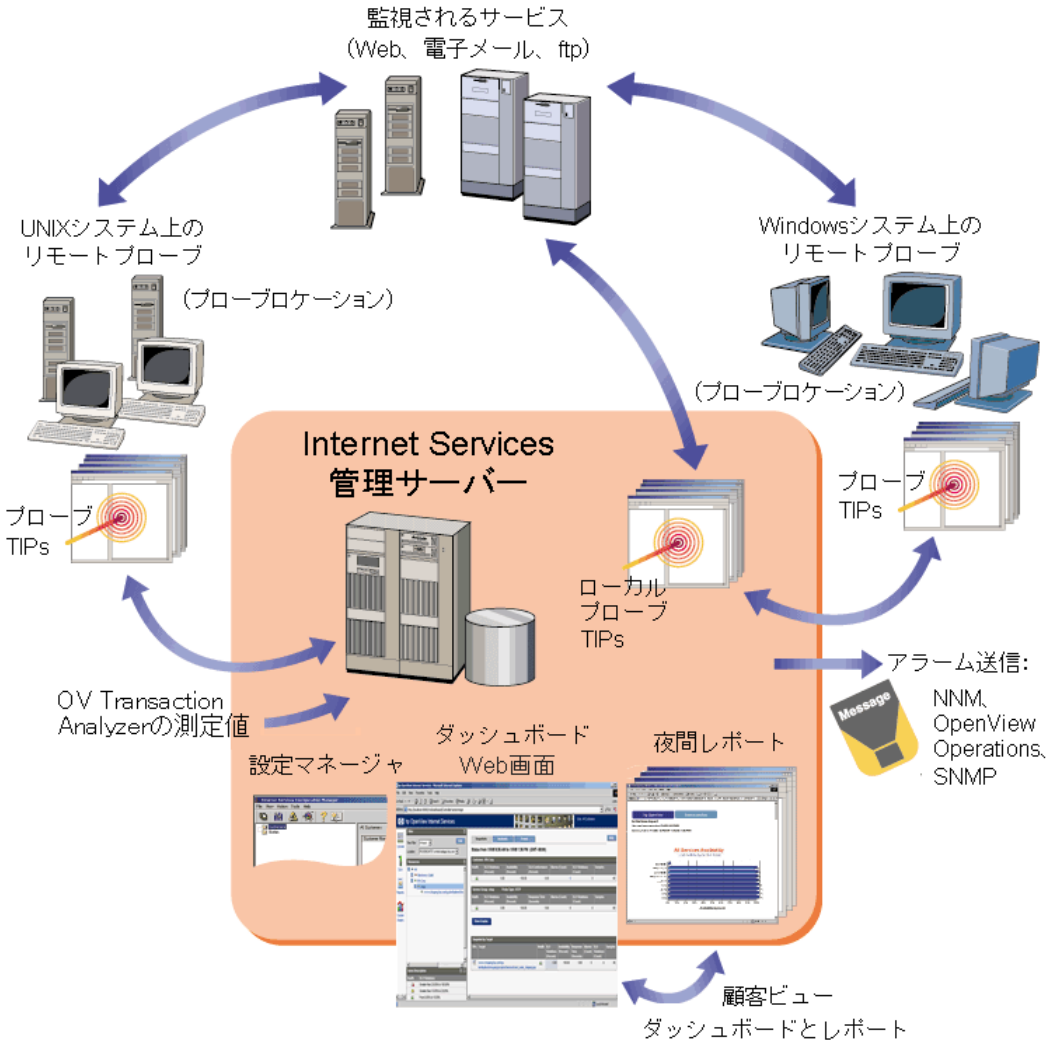


図 1　　Internet Services コンポーネントの概念図

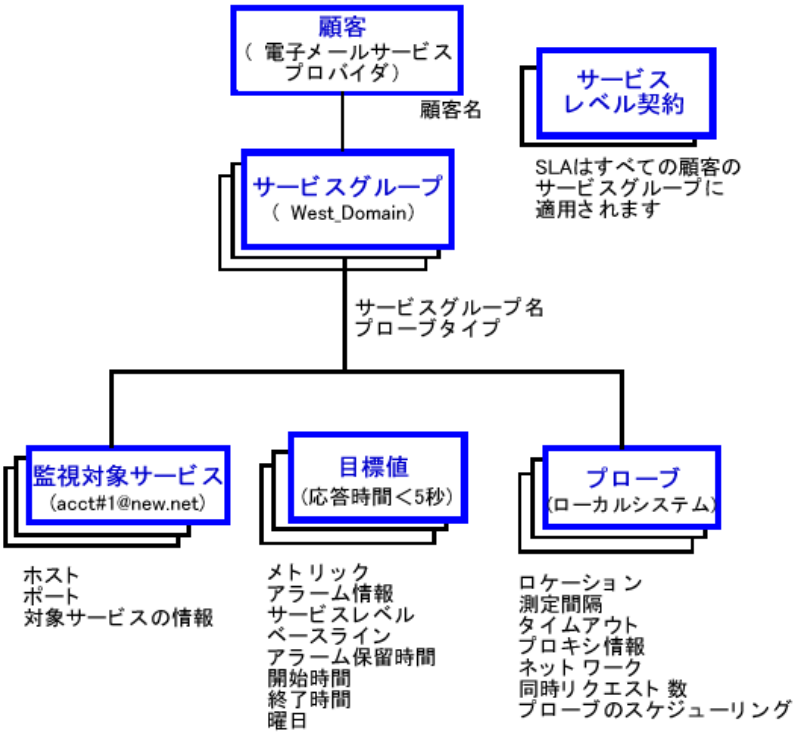
サービスの階層

Internet Services の設定マネージャを使用して、各サービスの監視対象サービスを設定します。サービス階層を形成している各顧客のサービスグループの下で、監視対象サービスをグループ化します。この構造により、サービスの種類別、顧客別のデータを表示できます。

サービス階層の最上位は顧客で、企業、インターネットサービスプロバイダ、または会社内の部署がこれにあたります。顧客の下には、サービスグループがあります。1 つの顧客には、1 つまたは複数のサービスグループがあり、各サービスグループは、同じ種類のサービスを含んでいる必要があります。すべてのサービスグループの下には、Internet Services がサービスを測定するためにプローブを作成し、プローブから受信したデータを評価し、レポートやアラームを生成するためにデータを統合およびグループ化する 3 つのコンポーネントがあります。これらの 3 つのコンポーネントを以下に示します。

- **監視対象サービス :** 測定するサービスとサービスの場所です。
- **サービス目標値 :** サービス目標 (サービスレベル目標値または SLO) を達成するのに満たさなければならないサービス値です。
- **プローブロケーション :** プローブを展開する場所です。プローブは、ローカルの OVIS 管理サーバー上で実行するか、リモートの Windows システムまたは UNIX システムに展開できます。リモートシステムに展開すると、企業内のさまざまな場所から測定データを収集できます。

図 2　　サービス階層


顧客
（ 電子メールサービス
プロバイダ）
顧客名
サービス
レベル契約
SLAはすべての顧客の
サービスグループに
適用されます
サービスグループ
（ West_Domain）
サービスグループ名
プローブタイプ
監視対象サービス
(acct#1@new.net)
ホスト
ポート
対象サービスの情報
目標値
(応答時間＜5秒)
メトリック
アラーム情報
サービスレベル
ベースライン
アラーム保留時間
開始時間
終了時間
曜日
プローブ
(ローカルシステム)
ロケーション
測定間隔
タイムアウト
プロキシ情報
ネットワーク
同時リクエスト数
プローブのスケジューリング

実装手順

Internet Services の使用手順を以下に示します。

1. OVIS CD から OVIS ソフトウェアをインストールします。
2. Internet Services の設定マネージャを使用して、顧客、サービスグループ、測定する監視対象サービス、サービスレベル目標値 (SLO)、サービスレベル契約 (SLA) の適合レベルを設定し、プローブを作成します。
3. Internet Services の設定マネージャを使用して、プローブロケーションを定義します。ローカルの OVIS 管理サーバーシステムから監視するようにプローブを設定することも、プローブをリモートの Windows システムまたは UNIX システムから実行するように設定することもできます。
4. プローブを実行する予定のリモートシステムに、OVIS CD からプローブソフトウェアをインストールします。プローブの設定ファイルをリモートシステムに配布すると、プローブによるデータの収集を開始できます。
5. プローブは、応答時間、可用性、および他のパフォーマンスメトリックを測定し、データを管理サーバーに送信します。設定マネージャの [ステータス] ノードを使用して、プローブが適切に動作していることを確認します。
6. プローブから受信されたデータは、OVIS ダッシュボードで表示するために管理サーバー上で整理統合されます。プローブが必要なデータを収集しているかを検証するために表示データを分析します。サービスレベル契約、可用性、応答時間のレポートは夜間に作成されることに注意してください。
7. 必要に応じて、OVIS CD から統合コンポーネントをインストールして、OVIS を OpenView Operations for UNIX (OVO)、OpenView Operations for Windows (OVO/Windows)、および Network Node Manager (NNM) と統合します。これらとその他 OpenView 製品の設定に関しては、第 5 章「 OpenView 製品との統合」の手順に従ってください。
8. 必要に応じて、アラームイベントを NNM、OVO、OVO/Windows 、または一般的な SNMP 管理ステーションに送信するように設定します。

第 2 章「Internet Services の使い方」、第 3 章「Internet Services の設定」、および第 4 章「サービスタイプとプローブの説明」 で、監視する各種サービスのプローブの設定方法について説明しています。これらの章では、サービスの編成方法、プロー

ブの作成方法、サービスレベル目標値、サービスレベル契約、およびアラームを設定する方法について説明しています。初期設定時の手順については、オンラインヘルプと設定ウィザードを参照してください。

他の OpenView 製品との統合

第 5 章「 OpenView 製品との統合」で説明されているように、Internet Services を次の製品に統合することができます。

- OpenView Transaction Analyzer
- OpenView Operations for UNIX
- OpenView Operations for Windows
- Network Node Manager (または SNMP トラップ受信が可能なイベントマネージャ)

Internet Services には、レポートの基本機能とカスタムグラフ機能を提供する OpenView Reporter と OpenView Performance Manager (OVPM) のコンポーネントが組み込まれています。Reporter または OVPM のフルバージョン (以下で説明されているその他の機能を装備) を OVIS と同じシステムにインストールすることができます。

Reporter: HP OpenView Reporter を Internet Services と同じシステムにインストールすると Internet Services と統合できます。Internet Services を含むエンタープライズレポートのすべてを、Web ページの同じ設定で表示することができます。これによって、Internet Services のパフォーマンスおよびサーバーまたはシステムのパフォーマンスの問題の両方を表示して確認することができます。また、Reporter を使用して、Internet Services のカスタムレポートを作成し、Reporter GUI を介して作業シフト定義を変更することができます。Reporter が Oracle や SQL Server データベースを使用するように設定されていて、Internet Services が同じシステムにインストールされている場合は、Internet Services は Reporter と同じデータベースを使用します。

OVPM: HP OpenView Performance Manager (OVPM) を Internet Services と同じシステムにインストールすると、Internet Services データを OVPM のグラフやレポートに表示することができます。新しい OVPM バージョンでは、システムパフォーマンスデータに加えて OVIS データを直接表示することができます。

OVPM の旧バージョン (PerfView) では、OpenView Performance Agent (OVPA) と Application Response Measurement (ARM) を使用して OVIS データとシステムパフォーマンスデータを表示することができます。次の項を参照してください。

OVPA と ARM: ARM は、アプリケーションのクリティカルトランザクションの応答時間を測定するための業界標準技術です。OVPA (旧名称 MeasureWare Agent) は ARM 2.0 標準をサポートし、ARM 実装のアプリケーションのパフォーマンスメトリックを収集します。OVIS のプローブに ARM を実装し、OVPA を OVIS と同じシステムにインストールすると、トランザクションデータは自動的にログされるようになります。OVPA を経由して収集された OVIS ARM データは、従来の OVPA 機能 (抽出など) で処理でき、SAS などの他のツールにエクスポートし、PerfView を介して表示できます。この OVIS データはシステムパフォーマンスデータの右横に並べて表示することができます。

次の表では、OVPA メトリックと OVIS との関連性を示しています。

OVPA メトリック	OVIS との関連性の説明
TT_APP_NAME	OVIS 顧客名
TT_NAME	OVIS サービスグループ名
TT_WALL_TIME_PER_TRAN	プローブの応答時間。arm_start および arm_stop 呼び出しを使用する代わりに、OVIS は arm_complete_transaction 呼び出しを使用します。これによって OVIS はこのメトリックに対して、OVPA に start および stop を使用して計算させるのではなく、OVIS が事前に計算した応答時間を OVPA に送ります。結果として、TT_WALL_TIME_PER_TRAN は OVIS の応答時間データと同じになります。
TT_SLO_COUNT	定義された SLO を超えたプローブ応答時間の数。ARM の SLO トランザクションデータは OVPA で定義され、OVIS で設定された SLO/SLA 情報は使用されないことに注意してください。
TT_USER_MEASUREMENT_*	可用性。
TT_USER_MEASUREMENT_*_2	セットアップ時間。
TT_USER_MEASUREMENT_*_3	転送スループット。

OVPA メトリック	OVIS との関連性の説明
TT_USER_MEASUREMENT_*_4	OVIS プローブメトリック 1。
TT_USER_MEASUREMENT_*_5	OVIS プローブメトリック 2。
TT_USER_MEASUREMENT_*_6	OVIS プローブメトリック 3。

これらメトリックに関する詳細は、『*OVPA Metrics Dictionary*』と『*OVPA Tracking Your Transactions Guide*』を参照してください。

ARM ライブラリが見つからなかった場合は、OVIS は、NO-OP (NO-OPeration) ライブラリを使用します。これは、arm_* 呼び出しがエラーの検出や処理を行わずに戻る原因となります。

デフォルトでは、この ARM トランザクションデータが収集されます。データ収集に関連するオーバーヘッドが平均して非常に低くなります。詳しくは、ARM 統合の OVIS ホワイトペーパーを参照してください。

Service Desk: Internet Services を OpenView Service Desk と統合すると、次のことが可能になります。

- 現在のサービスステータス情報をインシデント管理や問題管理に提供します。
- ビジネスサービスの管理 (Service Desk) と運用サービスの管理 (Internet Services) 間のサービス階層情報を同期させます。
- 顧客と合意した SLA に従ってサービス状況をレポートします。
- スマートアクションからのサービス呼び出しでダッシュボードを起動できます。

この統合を設定する方法の詳細は、『*Service Desk 管理者ガイド*』を参照してください。

Systems Insight Manager: Internet Services は、OVIS の `<install dir>¥contrib` ディレクトリから `ovis.mib` (SNMP) を使用して HP Systems Insight Manager (SIM) と統合することができます。

OpenView Business Process Insight (OVBPI): OVIS 6.0 からは OVBPI 1.1 と統合できます。

マニュアル

OVIS マニュアルは、CD または
<install dir>helpiops¥c¥ ディレクトリから入手できます。以下のマニュアルが使用できます。

- OVIS ユーザーリファレンスガイド (IS_User_Ref_Guide.pdf)
- OVIS Web Transaction Recorder ガイド (webrecorder.pdf)
- OVIS SQL Server および Oracle データベース設定ガイド (Reporter_Database_Config.pdf)
- OVIS Custom Probes API Guide (CustomProbes.pdf)
- OVIS リリースノート (IOpsReleaseNotes.pdf)
- OVIS ダッシュボードの新機能 (OVIS 60-dashboard.pdf)
- 新機能 - OVIS Troubleshooting Insight Packages (TIPs) (ovis60-tips.pdf)
- hp OpenView Tracing Concepts Guide (ov_tracing.pdf)
- hp OpenView AutoPass Licensing Guide (AutoPass-guide.pdf)

これらのマニュアルは次の URL からもオンラインで利用することができます。

http://ovweb.external.hp.com/lpe/doc_serv/

2

Internet Services の使い方

この章では、Internet Services のインストール、使用に必要な手順について説明します。ここでは、Internet Services の使い方を例を挙げて説明します。これらの例に従うことで、すばやく簡単に Internet Services を使用することができます。プローブの設定方法、プローブステータスの監視方法、およびダッシュボードを使用したパフォーマンスデータの表示方法を理解するためにも、例で示している手順に必ず従ってください。例で示している手順をすべて完了すれば、独自の監視対象サービスを容易に設定し、パフォーマンスデータを分析できるようになります。

ここでは、Internet Services のインストール、設定に関する以下の内容について説明します。

- インストールに関する留意事項
- インストールの前提条件
- Internet Services のインストール
- Internet Services 設定のクイックスタート

  プローブデータ収集ステータスの確認
- ダッシュボードによるデータの表示

  ダッシュボードのクイックスタート
- ダッシュボードの詳細

- Internet Services のアンインストール

インストールに関する留意事項

インストールを開始する前に、Internet Services をインストールするシステムが、最小要件を満たしていることを確認する必要があります。最小要件を満たしていれば、インストールし、サービスを設定する準備が整ったことになります。

Internet Services の以前のバージョンをすでにインストールしている場合は、『*OVIS リリースノート*』を参照して、ソフトウェアのアップグレードに関する情報を確認してください。

インストールの前提条件

Internet Services の最小要件を以下に示します。

サポートされているプラットフォームと、他の OpenView 製品との統合に関する詳細は、『*OVIS リリースノート*』を参照してください。

ハードウェア最小要件

システム規模要件の詳細は、512 ページの「スケーラビリティ情報」を参照してください。

Windows 管理サーバー

- Intel Pentium IV 2GHz 以上の CPU、1GB 以上のメモリを推奨
- 600MB の空きディスク容量。データの追加に伴って必要な容量は増加します。
- レポート生成時に必要な一時ディスク容量は、50 ～ 1000MB。測定するサービスの数によって異なります。
- 解像度 1024 x 768 以上のディスプレイを推奨

Windows プローブシステム

- Intel Pentium IV 1GHz 以上の CPU、512MB 以上のメモリを推奨。これらの要件は、並列実行するプローブの数と種類によって異なります。実行効率と測定の精度を高めるには、プローブ用に専用のシステムを使用することをお勧めします。
- プローブと設定ファイル用の 100MB のディスク容量、ネットワークがダウンした場合に一時的なキューファイル内のプローブデータを保存するための 10 ～ 100MB のディスク容量。必要なディスク容量は、監視対象サービス数と対応可能なネットワークダウンタイムの長さによって異なります。

UNIX プローブシステム

- 512MB 以上のメモリを推奨。
- プローブと設定ファイル用の 100MB のディスク容量、およびネットワークがダウンした場合にキューファイル内のプローブデータを保存するための 10 ～ 100MB のディスク容量。必要なディスク容量は、監視対象サービス数と対応可能なネットワークダウンタイムの長さによって異なります。

ソフトウェア要件

Windows 管理サーバー

OVIS 管理サーバーには、以下のバージョンのオペレーティングシステムと IIS が必要です。

- Microsoft Windows 2000 Professional/Server/Advanced Server (Service Pack 4) (Windows 2000 Advanced Server の各種バージョンがサポートされていますが、DataCenter Server の拡張機能はサポートされていません)

  Microsoft IIS 5.0 Web Server

  または

- Microsoft Windows XP Professional (Service Pack 1 以上)

  Microsoft IIS 5.1 Web Server

  または

- Microsoft Windows Server 2003 Standard および Enterprise エディション。

Microsoft IIS 6.0 Web Server

OVIS 管理サーバーにはさらに以下のソフトウェア要件があります。

- Windows 2000 または Windows XP の各システムでは Microsoft Windows Script 5.6 が必要です。これは、Microsoft Download Center (www.microsoft.com/downloads) からダウンロードできます。
- Internet Explorer 6.0 (最新のセキュリティアップデートとサービスパックが必要)。
- OVIS サーバー上で動作する IIS は、割り当てられている IP アドレスすべてを使用するよう、設定する必要があります。特に 127.0.0.1 はプローブ / サーバー間の通信に必要です。これを行うには、[既定の Web サイトのプロパティ] の [Web サイト] タブで IP アドレスを選択して、表示されているポートに割り当てるか、[IP アドレス] フィールドの [(未使用の IP アドレスすべて)] を選択して未使用の IP アドレスすべてを表示されているポートに割り当てるようにします。
- NTFS ファイルシステム
- Internet Services を実行しているシステムの仮想メモリは、初期サイズを 512MB 以上に設定する必要があります。その他のアプリケーションを実行しているシステムでは、それらのアプリケーションと Internet Services に対応できるように、仮想メモリをこれ以上の値に設定する必要があります。
- DHCP は管理サーバーではサポートされません (ホスト名が変らない限り、リモートプローブシステム上でサポート)。
- プローブをローカルシステムで実行し、ダイヤルアッププローブを使用したり、ダイヤルアップネットワーク接続を使用するように他のプローブ (WAP プローブなど) を設定する場合は、RAS (Remote Access Server) と少なくとも 1 つの電話帳エントリを、管理サーバー上に設定する必要があります。
- ストリーミングメディアプローブをローカルシステムで実行する場合は、Windows Media Player (バージョン 8 以上) または Real Player (バージョン Real8 Basic または RealOne) が必要です。Windows Media Player はプローブのインストール時にデフォルトでインストールされますが、Real Player を使用する場合は別途インストールする必要があります。Real Player の無償版は www.jp.real.com からダウンロードできます。

- Web Transaction Recorder (HTTP_TRANS) プローブを使用しており、Microsoft Script Debugger がインストールされている場合は、Internet Explorer のスクリプトデバッグをオフにすることをお勧めします。たとえば、IE で [**ツール**] > [**インターネット オプション**] > [**詳細設定**] を選択し、[スクリプトのデバッグを使用しない] をチェックします。
  スクリプトデバッグを有効にすると、ページにスクリプトエラーが含まれている場合に、Web Transaction Recorder の再生と記録に支障をきたします。
- 『*Internet Services ユーザーリファレンスガイド*』などのドキュメント (.pdf 形式) を表示するには、Adobe Acrobat Reader 4.0 以降が必要です。Acrobat Reader は、**http://www.adobe.co.jp/products/acrobat/** からダウンロードできます。
- 言語設定の異なる複数のシステムを使用する場合は、OVIS サーバー、OVIS/Reporter データベース、およびリモートプローブで、デフォルトの同じロケール設定を使用する必要があります。また、OVIS を OVO、OVO/Windows、NNM、SIP、および他の OpenView 製品と統合する場合は、これらについても同一のロケール設定を使用する必要があります。この時点では、OVIS は UTF-8 キャラクタセットを使用するために設定されたデータベースをサポートしていません。

他の OpenView 製品と統合する際の要件については、『*OVIS リリースノート*』を参照してください。

OVIS とクラスタ構成の OVO for Windows サーバー (7.5 以降) を同じシステム上にインストールすることはサポートされていません。また、OVIS と Windows 用のクラスタ構成 OVO との統合もサポートされていません。

Business Transaction Observer (BTO) を実行しているシステムに、Internet Services サーバーコンポーネントをインストールしないでください。BTO を設定したとおりに動作させるには、専用システムが必要です。

Windows プローブシステム

- Microsoft Windows 2000 (Service Pack 4)、Microsoft Windows XP Professional (Service Pack 1) または Microsoft Windows Server 2003 Standard および Enterprise エディション。

- Internet Explorer 6.0 (最新のセキュリティアップデートとサービスパックが必要)。
- ダイヤルアッププローブを使用したり、ダイヤルアップネットワーク接続を使用するように他のプローブ (WAP プローブなど) を設定する場合は、RAS (Remote Access Server) と少なくとも 1 つの電話帳エントリを、Windows プローブシステム上に設定する必要があります。
- リモートシステムでストリーミングメディアプローブを実行している場合は、Windows 版の Real Player (Real8 Basic または RealOne) または Windows Media Player (バージョン 8 以上) のインストールが必要です。Windows Media Player はプローブと共に自動的にインストールされます。Real Player を使用する場合は、無償版を www.jp.real.com からダウンロードしてください。

DHCP は、ホスト名が変らない限り、リモートプローブシステム上でサポートされています。

UNIX プローブシステム

- HP-UX 11.0、11.11、11.22、11.23 (Itanium 上の PA-RISC エミュレーションモードで動作)
- Sun Solaris 2.8 (パッチ 110934 が必要)、Sun Solaris 9
- Linux Red Hat 8.0、9.0、ES 2.1、ES 3.0。Red Hat Linux には compat-libstdc++7.3-2.96 以降が必要です。
- SUSE Linux Enterprise Server 8 および Professional 8.1 (32 bit)

UNIX システムに必要なその他のパッチに関する重要な情報は、『*OVIS リリースノート*』を参照してください。

UNIX システムで使用できないプローブ

- ストリーミングメディアプローブ
- SMS プローブ
- ODBC プローブ
- Exchange プローブ
- SYS_BASIC_WMI プローブ

- UNIX システムでは、Internet Explorer 高負荷モードの HTTP_TRANS プローブは使用できませんが、URL モードおよびナビゲーションポイントモードの HTTP_TRANS プローブは使用できます。
- DIAL プローブは SuSE Linux 以外の UNIX のサポートされているすべてのバージョンでサポートされています。

UNIX システムでのダイヤルアッププローブの要件

UNIX システム上でダイヤルアッププローブを使用する場合は、次のソフトウェアが必要です。

Solaris

サポートしているすべてのバージョンの Solaris に、次のソフトウェアがインストールされている必要があります。

SUNWbnur　ネットワーキング UUCP ユーティリティ (ルート)
SUNWbnuu　ネットワーキング UUCP ユーティリティ (ユーザー)

Solaris 8 および Solaris 7 (11/99) を使用している場合は、次のパッケージもインストールされている必要があります。

SUNWapppr　PPP/IP 非同期 PPP デーモン設定
SUNWapppu　PPP/IP 非同期 PPP デーモンと PPP ログインサービス
SUNWpppk　PPP/IP デバイスドライバと IP ダイヤルアップデバイスドライバ

Solaris 7 より前の Solaris を使用している場合は、次のパッケージもインストールされている必要があります。

SUNWpppk　Solstice PPP デバイスドライバ
SUNWapppu　PPP/IP 非同期 PPP デーモンと PPP ログインサービス
SUNWapppr　PPP/IP 非同期 PPP デーモン設定ファイル

64 ビット版の Solaris 7 または 8 がインストールされている場合は、次のパッケージもインストールされている必要があります。

SUNWpppkx　PPP/IP デバイスドライバと IP ダイヤルアップデバイスドライバ (64 ビット版)

HP-UX

PPP-RUN ソフトウェアが必要です。次の製品がインストールされている場合は、PPP ソフトウェアを追加インストールする必要はありません。

- システムに LAN/9000 ネットワーク製品があらかじめインストールされている場合 (インスタントイグニッション)。

- HP-UX swinstall プログラムを使用して Core Networking Bundle をインストールした場合。PPP-RUN ファイルセットは、このソフトウェアバンドルの一部です。

Linux

次のバージョンの PPP が必要です。

ppp-2.3.11-7

ダッシュボードを表示するためのブラウザ要件

OVIS ダッシュボードは、OVIS 管理サーバーやブラウザがインストールされているその他のシステムから表示できます。ダッシュボードとレポート表示用の Web ブラウザが必要です。Internet Explorer 6.0 (最新のセキュリティアップデートおよびサービスパックが必要)、および Mozilla 1.7.2 (HPUX Mozilla はバージョン 1.6) がサポートされています。

ブラウザを表示するシステムの表示設定を High Color (16K) 以上に設定する必要があります。

ダッシュボードレポートを表示する場合は、すべてのレポートイメージが正しく更新されるように、保存されているページの最新のバージョンを確認するようにブラウザを設定します。この設定方法については、次の例を参照してください。

IE の場合は、[**ツール**] > [**インターネットオプション**] > [**全般**] **タブ**を選択して、[インターネット一時ファイル] の [**設定**] ボタンをクリックします。[**ページを表示するごとに確認する**] が選択されていることを確認して、[**OK**] をクリックします。

OVIS で制限表示を有効にしている場合にダッシュボードにログインすると、メインダッシュボードを表示する前にユーザー ID とパスワードの入力が求められます (138 ページの「制限表示使用時のダッシュボードへのログイン」を参照)。

Internet Services のインストール

OVIS の以前のバージョンからアップグレードする場合は、『*OVIS リリースノート*』を参照して、アップグレードに関する重要な情報を確認してください。

管理サーバーに使用するシステム上に他の OpenView 製品がインストールされている場合は、インストールディレクトリおよびデータディレクトリの、デフォルトのドライブとディレクトリの設定は変更しないことをお勧めします。OVIS のインストールでは、他の OpenView 製品によって既に設定されているパスが使用されます。

Windows ベースのオペレーティングシステム上の HP OpenView ツールは、インストール時に ¥HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard ハイブのレジストリエントリを使用して、他の OpenView ツールが既にインストールされているかどうか、共通ディレクトリはどれか、を識別します。インストール時には、このハイブ内で、HP OpenView の下にある InstallDir および DataDir キーが参照されるか、Current Version の下に RPM ID というキーと CommonApplicationPath および CommonDataPath というパスキーを含む製品名エントリが参照されます。

OVIS を Windows Server (7.5 以上) のクラスタ構成 OVO 上にインストールすることはサポートされていません。

次の手順に従ってインストールを実行します。

- CD-ROM ドライブに CD を挿入し、画面の指示に従います。
- インストールが完了したら、システムを再起動します。

OVIS は複数のポートを使用します。インストール時には、次のデフォルトのポートが Tomcat Servlet Container 設定で使用されます。

  - 8080 (HTTP - OVIS ダッシュボード)
  - 8009 (Apache 経由の JK2 - AJP 通信)
  - 8005 (シャットダウン)

これらのポートのいずれかが使用できない場合は、インストールプログラムによって別のポートを選択することが求められます。`netstat -an` を実行すると、使用中のポートを調べることができます。また、インストール後に、OVIS で使用するこれらのポートや他のポートを変更できます (475 ページの「OVIS で行うポートの設定と変更」を参照してください)。

プローブに関する留意事項

OVIS をインストールしたら、設定マネージャを使用して監視対象サービスのプローブを作成します。プローブの設定の例については、46 ページの「Internet Services 設定のクイックスタート」を参照してください。

プローブは、ローカルの OVIS 管理サーバーシステム上で実行することも、リモートの Windows または UNIX システムに展開して実行することもできます。OVIS CD からリモートプローブソフトウェアをインストールする、およびリモートシステムにプローブ設定ファイルを配布する手順については、168 ページの「リモートプローブソフトウェアのインストールと削除」を参照してください。

ライセンスキー

OVIS を使用するにはライセンスキーパスワードが必要です。インストール時に、60 日間有効な試用ライセンスが付与されます。この 60 日の期間内に、試用延長用ライセンスキーパスワード (45 ページの「試用延長ライセンスを取得する必要がある場合」を参照) か、恒久ライセンスキーパスワードを取得する必要があります。

OVIS ライセンスウィザードの選択

OVIS の設定マネージャを初めて起動すると、OVIS の [ライセンスの構成] ダイアログボックスが表示されます。このダイアログには、現在のライセンスステータス、標準 OVIS 監視対象のライセンス数、およびカスタム監視対象 (カスタムプローブ SDK または Probe Builder を使ってユーザーが作成したプローブで設定された監視対象) のライセンス数が表示されます。このダイアログボックスにはライセンスウィザードを起動するボタンも含まれています。このウィザードにより、HP AutoPass ライセンスプログラムを実行して、恒久ライセンスキーを取得できます。

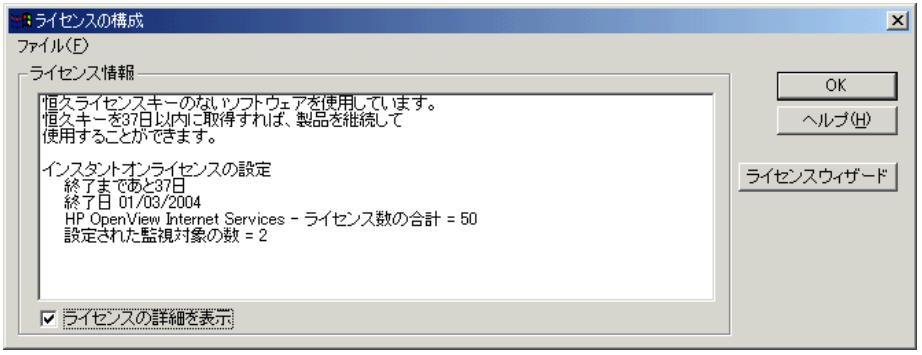
標準監視対象ライセンスとカスタム監視対象ライセンスは、個別に管理されます。

このダイアログには、設定した監視対象が標準監視対象ライセンス数やカスタム監視対象ライセンス数を超えているかどうかを知らせる警告メッセージが表示される場合もあります。

試用ライセンスの期限が切れ、標準監視対象ライセンス数やカスタム監視対象ライセンス数を超えると、ライセンス数の制限を超えた監視対象のデータは収集されません。

OVIS 6.0 ライセンス適用は、OVIS の標準監視対象ライセンスをカスタム監視対象に使用できないようにアップデートされました。アップグレードされるお客様で標準監視対象ライセンスを使用してカスタム監視対象を構成している場合には、当社の営業担当にお問合せください。

インストール時に、60 日間有効な試用ライセンスが付与されます。OVIS 監視対象のデータを引き続き収集するには、この 60 日の期間内に、試用延長用ライセンスキーパスワードか、恒久ライセンスキーパスワードを取得する必要があります。



購入された製品のライセンスキーパスワードを取得するには、OVIS 設定マネージャを起動すると表示される [ライセンスの構成] ダイアログボックスの [**ライセンスウィザード**] ボタンを選択します。**HP OpenView AutoPass** ライセンスプログラムの起動には 1 分ほどかかります。

最初のライセンスダイアログボックスで [OK] を押すと、ライセンスの取得をスキップできます。後でライセンスキーの取得を行うには、設定マネージャで [**ファイル**] > [**設定**] > [**ライセンス**] を選択して、表示されるダイアログで [**ライセンスウィザード**] ボタンを選択します。

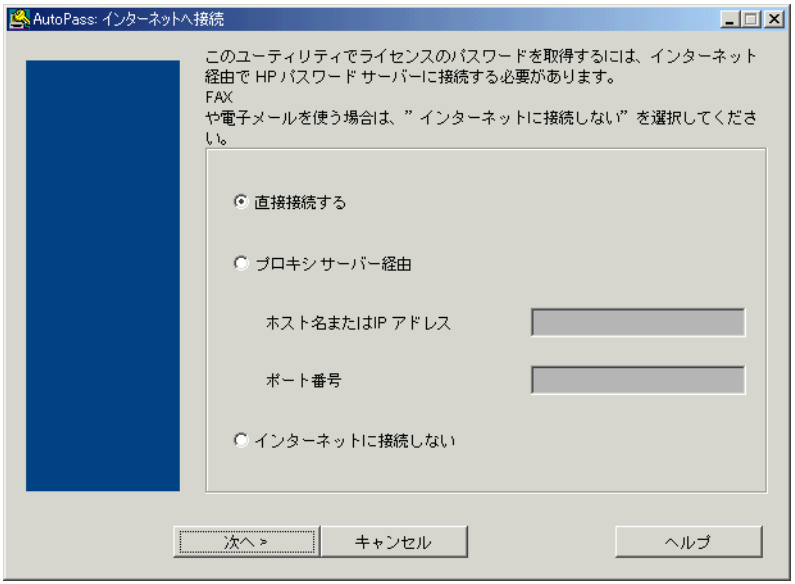
[**ライセンスウィザード**] ボタンを選択し、**HP AutoPass** プログラムに表示される指示に従って、恒久ライセンスキーを取得して、インストールします。

試用 (評価用) 延長ライセンスを取得する場合は、OVIS ライセンスウィザードではこれが行えないため、45 ページの「試用延長ライセンスを取得する必要がある場合」を参照してください。

権利証明書があり、インターネットにアクセスできる場合

OVIS をご購入になり、権利証明書を受け取り、OVIS サーバーをインストールしたシステムからインターネットにアクセスできる場合は、以下のステップに従って、恒久ライセンスキーパスワードを入力します。

1. OVIS で [ライセンスウィザード] を選択した後、表示された AutoPass プログラムのダイアログで [**OK**] をクリックします。
2. 表示されるダイアログで、[直接接続する] を選択するか、プロキシ情報を入力します。



3 表示されるダイアログで [恒久パスワードの取得] を選択し、権利証明書 (Entitlement Certificate) を元に HP OpenView Purchase Order 番号を入力します。

4 購入した LTU (License To Use) 製品を選択します。

5 顧客情報フォームに記入します。

6 完了すると、パスワードキーがインストールされます。

7 OVIS 設定マネージャを終了する前に、[**OK**] をクリックして設定の変更を保存します。

ライセンスキーを電子メールで受け取った場合

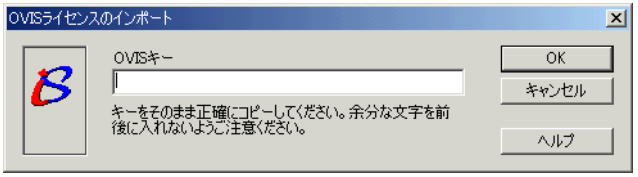
ライセンスウィザードではなく Web サイト (www.webware.hp.com) または電話でライセンスキーパスワードを申請し、電子メールで受け取った場合は、以下のとおりに OVIS にインポートする必要があります (ライセンスウィザードを使用して直接ライセンスキーを取得、インストールすることをお勧めします)。

電子メールでライセンスキーを取得して OVIS にインポートするには、次の手順に従う必要があります。

1 Web サイト (www.webware.hp.com) にアクセスし、手順に従ってライセンスキーパスワードを申請します。

2 ライセンスキーパスワード証明書 (Password Certificate) が電子メールで届きます。OVIS 管理サーバーの保存可能な場所にファイルを保存します。

3 設定マネージャを起動し、[**ファイル**] > [**設定**] > [**ライセンス**] を選択します。[ライセンスの構成] ダイアログで [**ファイル**] > [**OVIS ライセンス**] > [**ライセンスを直接入力**] を選択します。
次に、保存したファイルからライセンスパスワード / キーをコピーして、[OVIS キー] フィールドにペーストします。先頭や末尾にスペースを含めたり、引用符やその他のライセンスキーの値以外の文字を使用しないことが重要です。[OK] を選択すると、OVIS にライセンスがインポートされます。



試用延長ライセンスを取得する必要がある場合

試用 (評価用) ライセンスの延長 を申請する場合は、Web サイト (**www.webware.hp.com**) にアクセスして評価版ソフトウェア用パスワードの連絡先情報を入手してください。該当地域のライセンスセンター (Web サイトの試用 (評価用) 延長ライセンスのリンクを選択して) に問い合わせて試用 (評価用) ライセンスの延長を申請します。試用 (評価用) 延長ライセンスはお客様ごとに 1 度 (60 日の延長を 1 回) だけ付与され、その後も引き続き製品を使用するには、恒久ライセンスを購入する必要があります。必要に応じて、該当地域以外のパスワードセンターに連絡できます。

パスワードセンターでは、次の情報をお尋ねします。

ソフトウェア製品番号 : TRIAL-OVIS です。

IP アドレスまたはホスト名 : 評価版のソフトウェアがインストールされているシステムです。

問い合わせ先 : 会社名、氏名、住所、電話番号、電子メールアドレス。

パスワードキーは電子メールで送付されます。送付されたテキストファイルには標準監視対象用とカスタム監視対象用のライセンスが 2 行で示されています。これらを 44 ページの「ライセンスキーを電子メールで受け取った場合」に従ってインストールします。それぞれの試用延長ライセンスに対してコピーアンドペースト操作を行い、ペーストのたびに [OK] を選択して、ライセンスをインポートする必要があります。これらの試用延長ライセンスでは、監視対象の数は事実上制限がありません。

ライセンス情報の表示

インストールされたライセンスに関する詳細情報を表示するには、[ライセンスの構成] ダイアログで [**ライセンスの詳細を表示**] チェックボックスをオンにします。プローブロケーションごとに設定されたプローブ数に関する詳細情報については、設定マネージャで [**ツール**] > [**プローブの情報**] を選択します。

OVIS のライセンスについての詳細は、OVIS 製品 CD に収録されている『*HP OpenView AutoPass Licensing Guide*』を参照してください 。このマニュアルは、OpenView の Web サイト (http://ovweb.external.hp.com/lpe/doc_serv/) からもダウンロードできます。

Internet Services 設定のクイックスタート

この例では、Web ページ www.shopping.hp.com を、顧客 Hewlett-Packard の監視対象サービスとして設定します。プローブソフトウェアの設定とインストールプロセスについては、第 3 章「Internet Services の設定」でさらに詳しく説明します。

OVIS のドキュメンテーションセットには、設定マネージャの [ヘルプ] メニューと本のアイコンからアクセスできます。

サービスプローブの設定

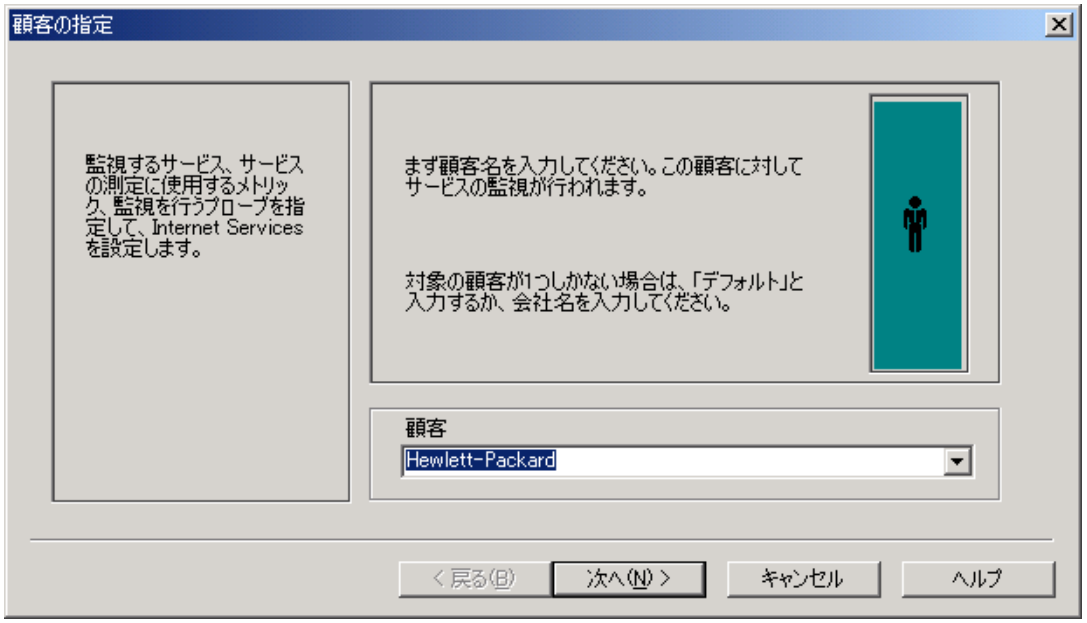
Windows 上の Internet Services 管理サーバーでプローブを設定するには、次の手順に従います。

1 [**スタート**] > [**プログラム**] > [**HP OpenView**] > [**internet services**] > [**設定マネージャ**] を選択して、設定マネージャを開きます。
複数のユーザーが同時に同じアイテムを追加 / 更新 / 削除 / 保存しようとした場合、複数ユーザーオプションの設定によってロックすることができます (複数ユーザーのロックを使用する上での追加要件については、101 ページの「その他の設定オプション」を参照してください)。

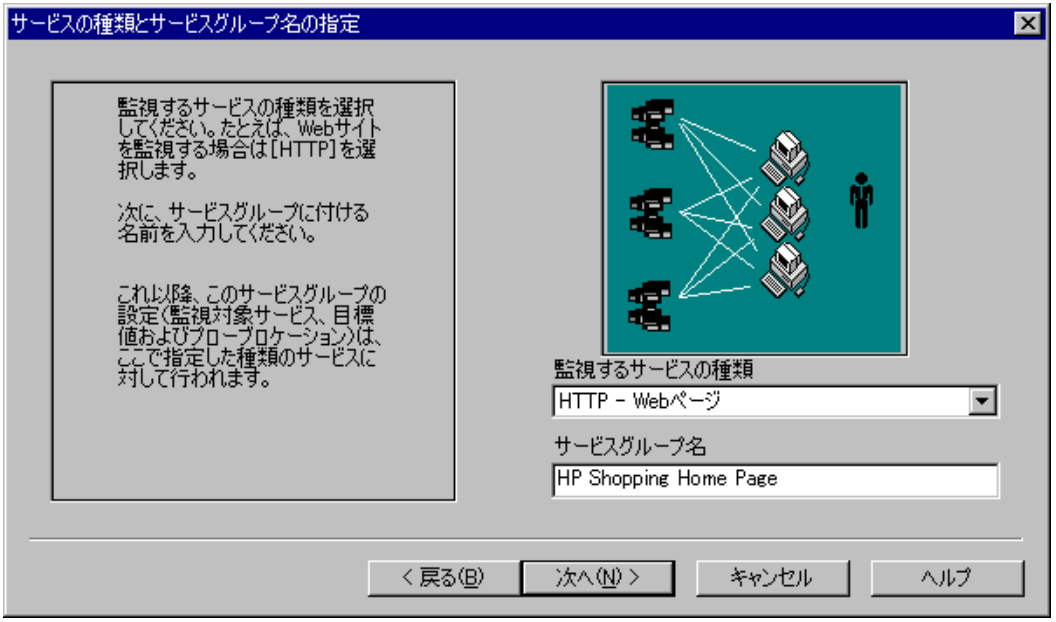
OVIS 設定マネージャを使用するには、管理者ユーザーでなければなりません。

2 [**設定ウィザード**] (ツールバーの左から 2 番目の) ボタンを選択するか、メニューから [**ファイル**] > [**設定ウィザード**] を選択します。

3 [**顧客の指定**] ダイアログが表示され、設定ウィザードが開始します。この例では、「**Hewlett-Packard**」と入力します。[**顧客**] には、監視対象サービスとなる顧客名を指定します。[**次へ**] をクリックします。

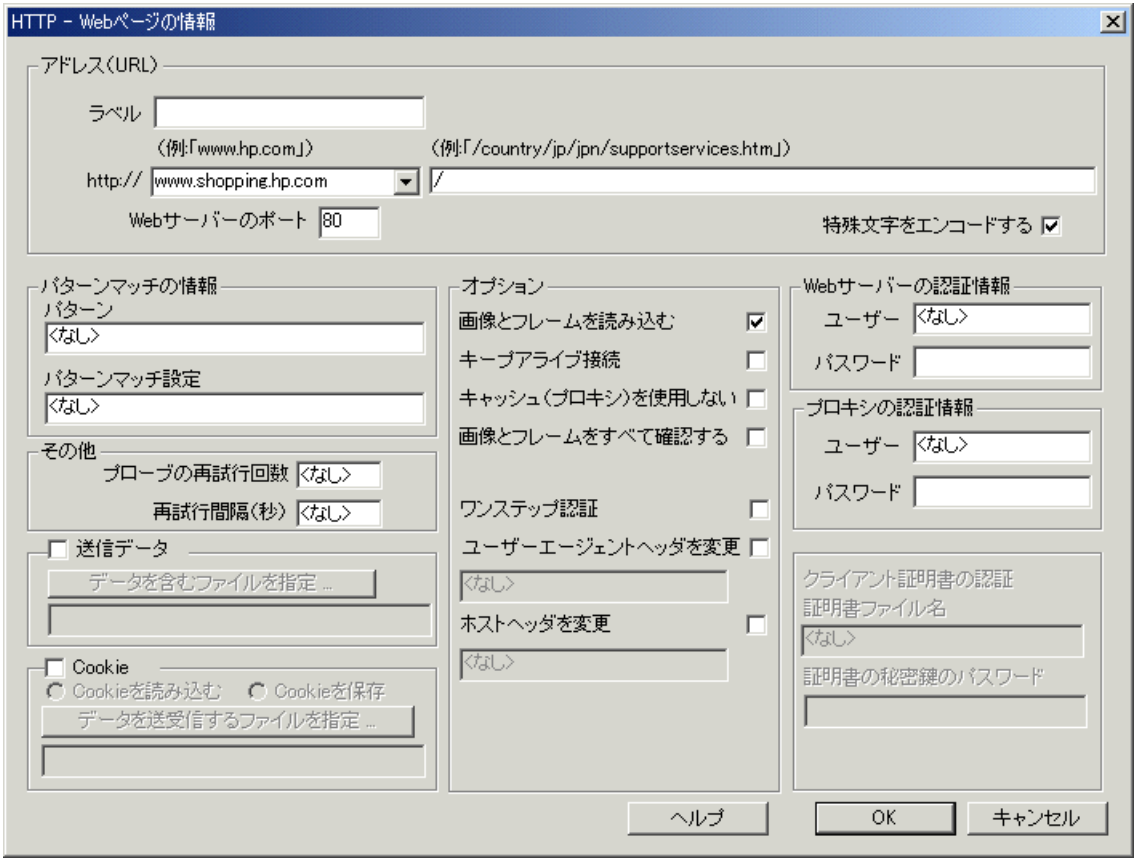


4 [**サービスの種類とサービスグループ名の指定**] ダイアログボックスで、監視対象のサービスの種類として [**HTTP-Web ページ**] を選択し、サービスグループ名に**「HP Shopping Home Page」**と入力して [**次へ**] をクリックします。

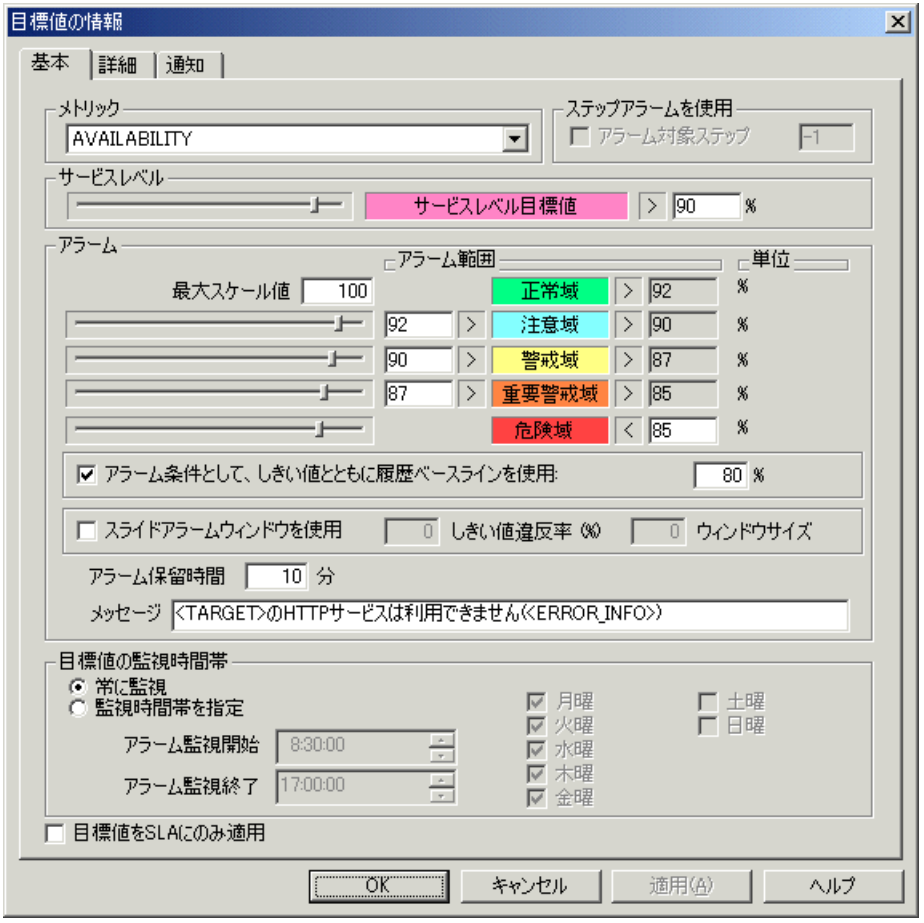


サービスをグループ化する際は、サービスグループ内の監視対象サービスが同じ種類になる必要があります。たとえば、「HTTP」(Web ページ) と「DNS」(ドメインネームサーバー) は異なる種類のサービスなので、同じグループにすることはできません。

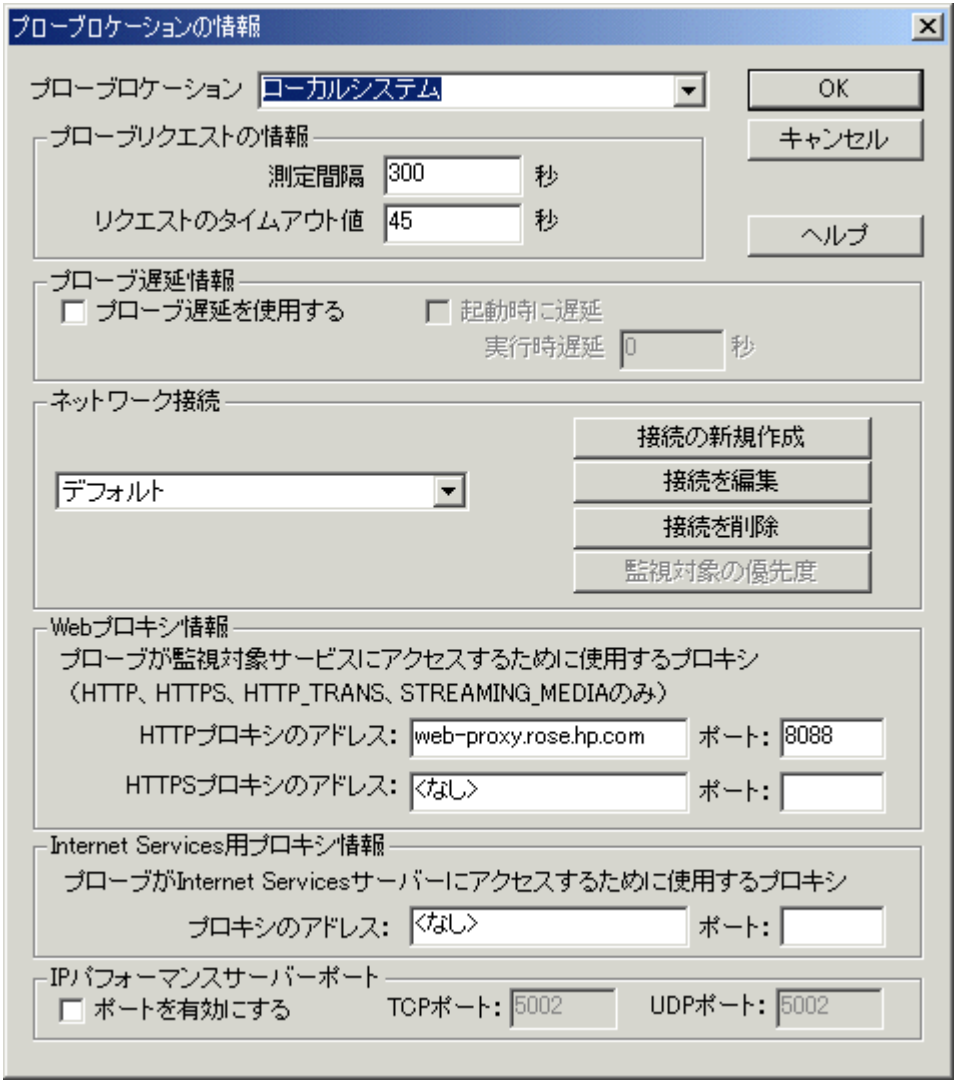
5 [**監視対象サービスの追加**] ダイアログで [**監視対象サービスを追加**] ボタンをクリックすると [**HTTP-Web ページの情報**] ダイアログが開きます。監視対象サービスとして URL アドレスのフィールドに「**www.shopping.hp.com**」と入力します。[**OK**] をクリックし、[**次へ**] をクリックします。



6 [**目標値の追加**] ダイアログで [**サービス目標値を追加**] ボタンを選択します。[**目標値の情報**] ダイアログで、サービスグループが 90% の時間可能であるという可用性目標値のデフォルトを了承して [**OK**] をクリックし、[**次へ**] をクリックします。



7 [**プローブロケーションの追加**] ダイアログで、[**プローブロケーションを追加**] ボタンを選択します。[**プローブロケーションの情報**] ダイアログが開きます。



[Web プロキシ情報] 以外の、すべてのフィールドでデフォルトを了承します。Web プロキシを使用して指定したサイト (ここでは、www.shopping.hp.com) にアクセスしている場合には、Web ブラウザに設定されているプロキシアドレスとポート番号を入力する必要があります。

Internet Explorer では、この情報は [**ツール**] **メニューの** [**インターネットオプション**] > [**接続**] **タブ** > [**ローカルエリアネットワーク (LAN) の設定**] の [**LAN の設定**] ボタンから確認できます。

[プローブロケーションの情報] ダイアログは、計測のタイミング (プローブリクエストの情報)、使用するネットワーク接続 (ダイヤルアップなど)、監視対象の優先度 (プローブのスケジューリング) を指定する場合にも使用します。詳細については、第 3 章「Internet Services の設定」を参照してください。

8 [**OK**] をクリックし、[**次へ**] をクリックします。[**完了**] をクリックして、ウィザードの手順を完了します。

9 [**設定マネージャ**] のツールバーで [**プローブ設定の保存**] ボタンをクリックするか、メニューから [**ファイル**] > [**プローブ設定の保存**] を選択します。

必ず設定を保存してください。設定を保存しないと、サービスは監視されません。設定を保存すると、ローカルシステムに指定したすべてのプローブが Internet Services 管理サーバーに登録され、プローブシステムへの配布の準備が整います。

設定マネージャの左ペインから [**ステータス**] を選択し、ウィンドウの [**リモート プローブの更新**] タブを使って、配布ステータスを表示できます。

10 下記の項を参照して、プローブの設定情報を表示し、プローブのステータスが緑色であるか確認します。

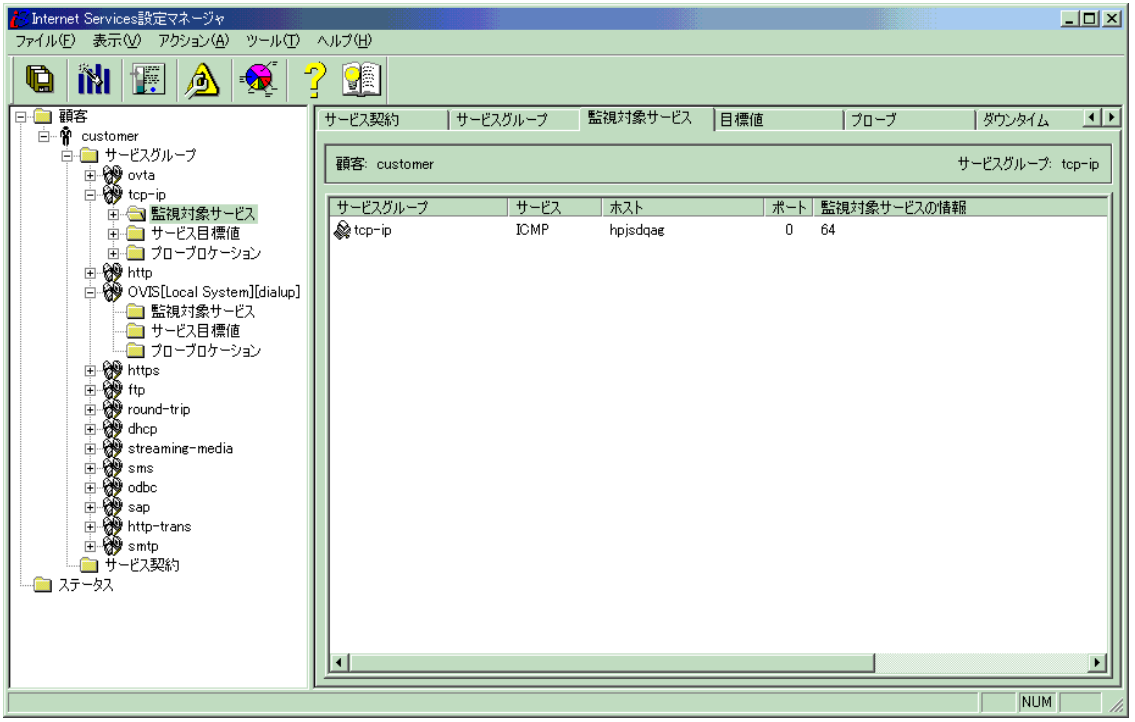
11 しばらく待って、プローブにいくつかのデータを収集させます。続いて、62 ページの「ダッシュボードのクイックスタート」に進んで、この例で設定したプローブが収集したデータの表示方法を調べてください。

設定情報の表示

設定マネージャで、作成した監視対象サービスの設定情報を表示できます。

設定マネージャのメインウィンドウの左ペインで、ツリー最上位の [顧客] を選択すると、設定されている全顧客のリストが右ペインに表示されます。

左ペインのサービスツリーで他の任意の項目を選択すると、右ペインにはいくつかのタブが付いた画面が表示されます。表示されるタブは、左ペインで選択した項目に対応しています。たとえば、左ペインで監視対象サービスをクリックすると、右ペインには [**監視対象サービス**] タブの内容が表示されます。



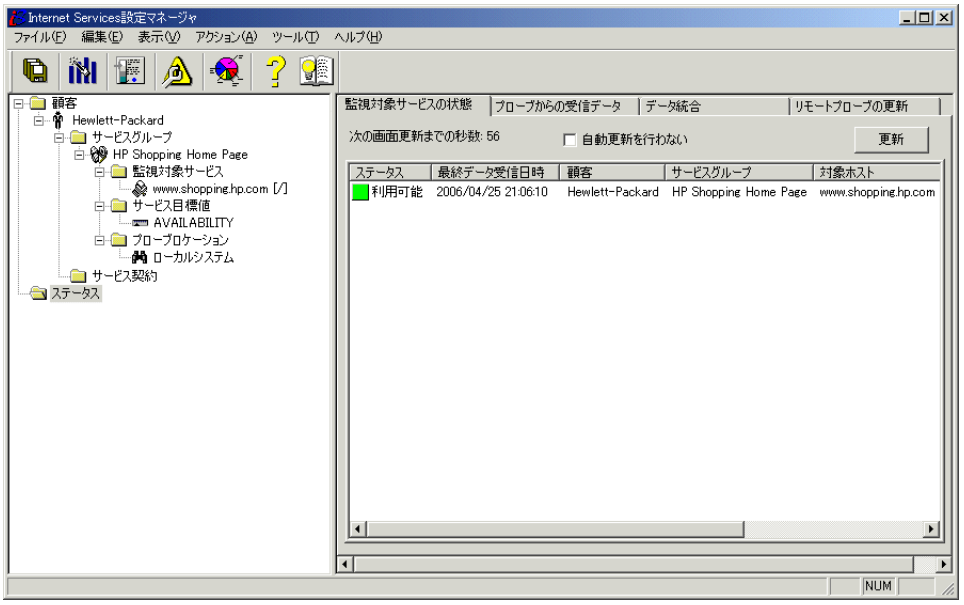
以下のタブがあります。

- [サービス契約]
- [サービスグループ]
- [監視対象サービス]
- [目標値]
- [プローブ]
- [ダウンタイム]

プローブデータ収集ステータスの確認

[設定マネージャ] ウィンドウの左ペインで [ステータス] (ツリー下部) を選択して、監視対象サービスへのプローブ問い合わせが成功したかどうかを確認します。監視対象サービスが正しく設定されている場合は、5 分以内にアイコンが緑色に変わります。アイコンが緑色になっていない場合の対処方法については、このガイドの第 6 章「トラブルシューティング情報」を参照してください。

注記 : 監視対象サービスが利用不可である間隔を定義することにより、監視対象サービスのステータスを黄色または赤色に変更するタイミングを設定できます。[ステータス] ページの設定値を変更するには、[**ファイル**] > [**設定**] > [**ダッシュボード**] を選択してください。



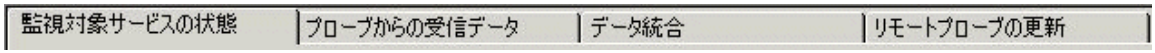
[ステータス] ページには以下のタブがあります (これらのタブに表示される内容については、以降の項で詳しく説明しています)。

- [監視対象サービスの状態]
- [プローブからの受信データ]
- [データ統合]
- [リモートプローブの更新]

[監視対象サービスの状態] ステータスタブ

[**ステータス**] ウィンドウの [**監視対象サービスの状態**] には、監視対象サービスのステータスが表示されます。ここには、プローブデータが Internet Services 管理サーバー上のトレーステーブル一時保存領域に到達したかどうかと、監視対象サービスが利用可能であるかどうかが表示されます。サーバー名や Web ページのスペルが間違っていたり、サービスがダウンしている場合、監視対象は利用不可であると表示されます。この表示は、設定を保存してから 5 分以内 (プローブが測定値を収集するまでの時間) に、監視対象が正しく設定されていて、利用可能であるかどうかを示します。

IOPS_TRACE_TABLE から監視対象の詳細データを表示したり、選択した監視対象サービスのダッシュボードを開くには、ステータス表示で監視対象を右クリックします。



赤色の円はアクションが失敗したことを示します。

黄色の三角形は、まだアクションが完了していないこと (処理中) を示します。

緑色の四角形は、アクションが正常に完了したことを示します。

[プローブからの受信データ] ステータスタブ

[ステータス] ウィンドウの [プローブからの受信データ] には、プローブが測定データを、Internet Services 管理サーバー上のトレーステーブル一時保存領域に正しく転送したかどうかが示されます。転送は、通常、設定を保存してから 5 分以内に実行され、画面を次回更新したときに表示されます。

IOPS_TRACE_TABLE から監視対象の詳細データを表示したり、強調表示した監視対象サービスのダッシュボードを開くには、ステータス表示の監視対象を右クリックします。

[データ統合] ステータスタブ

[ステータス] ウィンドウの [データ統合] には、収集したデータが、ダッシュボードのスナップショットページとレポートで表示できるように、IOPS_TRACE_TABLE 一時格納領域からレポートデータベースの **IOPS_PROBE_DATA_CACHE** テーブルに転送されたかどうかを表示します。転送は、通常、設定を保存してから 10 分以内に実行されます。

[リモートプローブの更新] ステータスタブ

[ステータス] ウィンドウの [リモートプローブの更新] には、リモートプローブ システムが、新しい設定情報を得るために、最後にサーバーに問い合わせた時間が表示されます。このステータスは配布マネージャから送られます (178 ページの「配布マネージャの動作」を参照してください)。

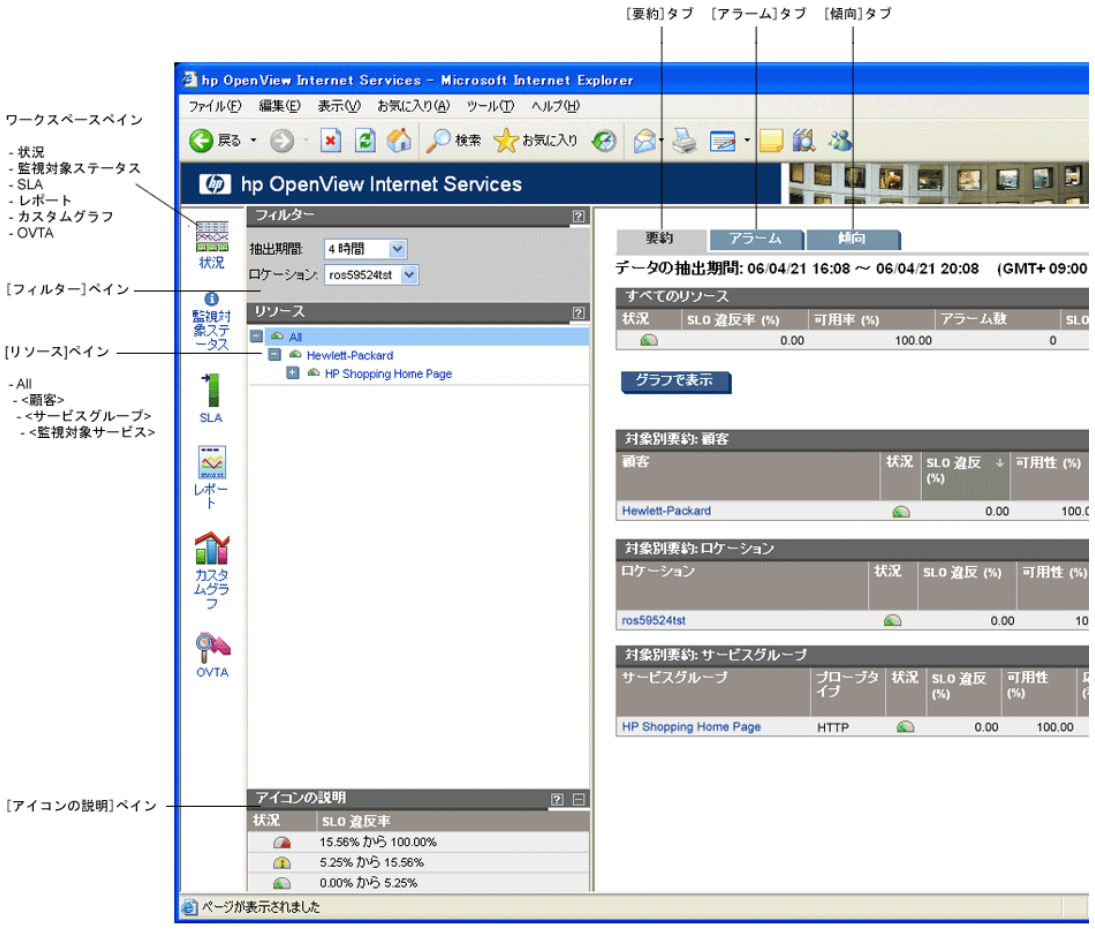
ダッシュボードによるデータの表示

OVIS ダッシュボードは、プローブによって収集されたデータを表示します。ダッシュボードの詳細を理解するには、次の事項を参照してください。

- 以下のダッシュボードのメインウィンドウの説明を読みます。
- 62 ページの「ダッシュボードのクイックスタート」を実行して、ダッシュボードのいくつかの主要機能を使用します。
- 74 ページの「ダッシュボードの詳細」を読みます。

ダッシュボードのメインウィンドウの説明

ダッシュボードには、いくつかのペインが表示されます。



ワークスペースペインは左端にあり、カスタムグラフ作成などの機能を選択できます。

ダッシュボードの初期表示は、**状況**ビューです。ダッシュボードのワークスペースペインに表示されるワークスペースリンクのいずれかをクリックすると、別のワークスペースにアクセスできます。

- [**状況**] - ダッシュボードのデフォルトのワークスペースです。75 ページの「[状況] ワークスペース」を参照してください。
- [**監視対象ステータス**] - 各監視対象のデータ収集のステータスを示します。設定マネージャでのステータス表示に類似しています。
- [**SLA**] - 各サービスレベル契約 (SLA) が規定されたしきい値を満たしているかどうかを示し、SLA の詳細を表示します。85 ページの「[SLA] ワークスペース」を参照してください。
- [**レポート**] - 毎晩自動的に生成される集計データのレポートを表示します。87 ページの「[レポート] ワークスペース」を参照してください。
- [**カスタムグラフ**] - OVIS データの標準装備のグラフを描いたり、カスタムグラフを作成します。90 ページの「[カスタムグラフ] ワークスペース」を参照してください。
- [**OVTA**] - OVIS と OVTA (OpenView Transaction Analyzer) を統合した場合は、OVTA Console を起動するリンクが表示されます。92 ページの「[OVTA] ワークスペース」を参照してください。

ダッシュボードのメインウィンドウ ([状況] ワークスペース) の中央にあるペインが [**リソース**] ペインです。これは、顧客、サービスグループ、監視対象サービスのサービス階層を表示します。このペインをナビゲーションツリーとして使用して各項目を選択すると、選択した項目の内容がダッシュボードに表示されます。このペインでは、すべてのサービス状況を赤色、黄色、緑色のアイコンで素早く表示できます。また、[**フィルター**] ペインでは表示するデータの範囲を選択したり、[**アイコンの説明**] ペインでは表示されるアイコンの簡単な説明を参照できます。

結果表示ペインは右側にあります。ここには、[リソース] ペインでの選択に基づいて、パフォーマンスデータが表示されます。状況ビューにある結果表示ペインの上部には、3 つのタブがあります。

[要約] タブ - サービスレベル目標値の違反数、アラーム数、サービス可用性などのリソースの状態を表示します。また、プローブにより収集されたメトリックを詳細に表示できます。

[アラーム] タブ - しきい値セットに基づいたアラームリストを表示します。

[傾向] タブ - メトリックのベースライングラフを表示します。

[**ヘルプ**] ボタンや表示ボックスの隅にある [**?**] をクリックすると、オンラインヘルプにアクセスできます。

[状況] ワークスペースは 5 分間隔で自動的に更新されます。

ダッシュボードのクイックスタート

この例では、OVIS ダッシュボードを使って、Web ページ **www.shopping.hp.com** のサービス状況を調べます。顧客「Hewlett-Packard」に、この監視対象サービスを設定する手順については、前述のクイックスタートの例 (46 ページの「Internet Services 設定のクイックスタート」) で説明しています。OVIS ダッシュボードの詳しい使い方は、74 ページの「ダッシュボードの詳細」で説明しています。

1 設定マネージャで OVIS ダッシュボードを開くには、初めに [**スタート**] > [**プログラム**] > [**HP OpenView**] > [**Internet Services**] > [**設定マネージャ**] を選択します。
続いて、ツールバーの [**Internet Services ダッシュボードの起動**] (円グラフ) ボタンを選択します。

制限表示が設定されている場合は、ダッシュボードのログイン画面が表示されることがあり、必要に応じてユーザー ID とパスワードを入力します。

2 ダッシュボードでは、最初に [**状況**] ワークスペースが表示されます。

表示されるデータは、[**フィルター**] ペイン (以下の画面を参照してください) で指定された期間のデータです。デフォルトでは 4 時間です。

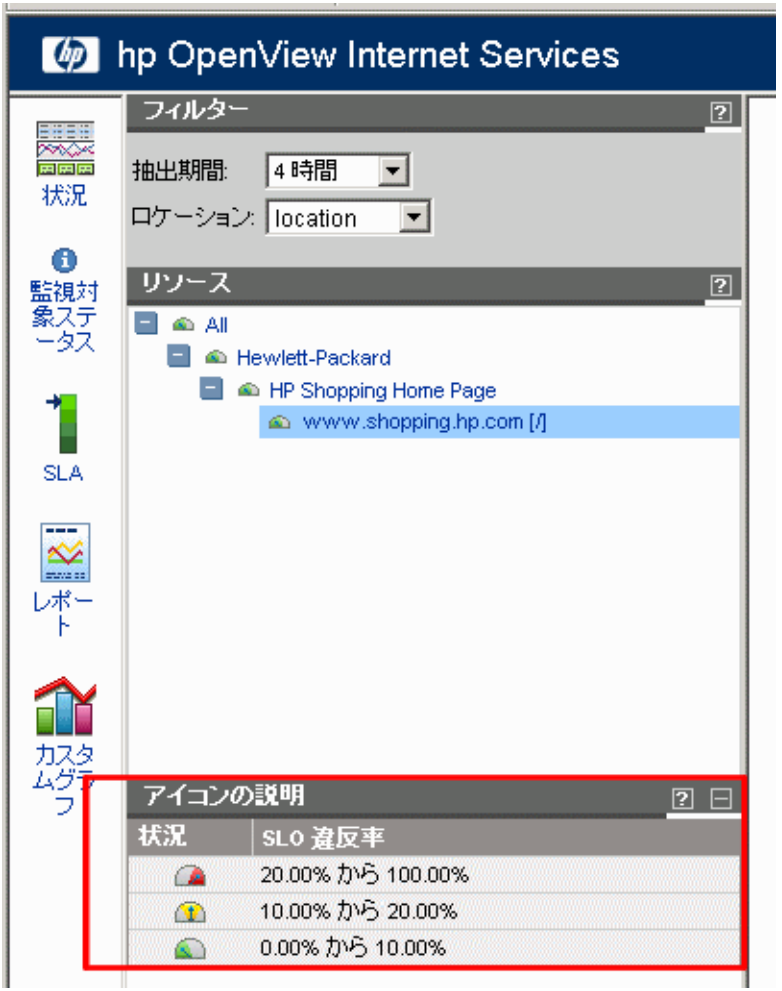
[**抽出期間**] ドロップダウンリストを使用して他の期間を選択できます。[カスタム] を選択すると、開始、終了の日付と時間を指定できます。

ここでは、デフォルトの 4 時間のまま、次に進みます。

3 [リソース] ペインの最上位の項目 [**All**] から、前述の「OVIS 設定マネージャのクイックスタート」で設定した顧客 [**Hewlett-Packard**] を見つけます。各項目のプラス記号 (+) をクリックしてツリーを展開し、**Hewlett-Packard** から **HP Shopping Home Page** および **www.shopping.hp.com** を表示します。その他の顧客や監視対象サービスを設定してある場合は、それらの項目も表示されます。

4 [リソース] ペインの各項目の横には、サービス状況を示す赤色、黄色、緑色のアイコンが表示されます。この状況は [**SLO 違反率**] に基づいています。顧客やサービスグループの状況は、その顧客やサービスグループに関連付けられた監視対象サービスに基づいています。以下の例では、HP Shopping Home Page サービスに 1 つの可用性 SLO が設定されています。

状況を示すアイコンは、表示下部の [**アイコンの説明**] ペインで説明されています。赤色、黄色、緑色に対するサービスレベル目標値の違反しきい値は、OVIS 設定マネージャでカスタマイズできます。

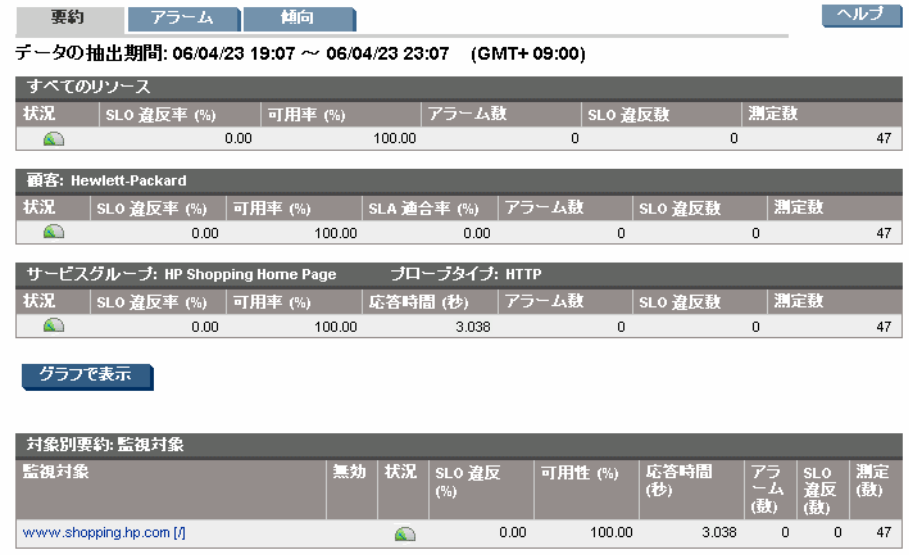


5 [**リソース**] ペインで [**All**] を選択します。**結果表示**ペイン (右側) では、デフォルトで [**要約**] タブが選択されています。ここには監視対象サービスのすべての情報のスナップショットが表示されます。以下の表が表示されます。

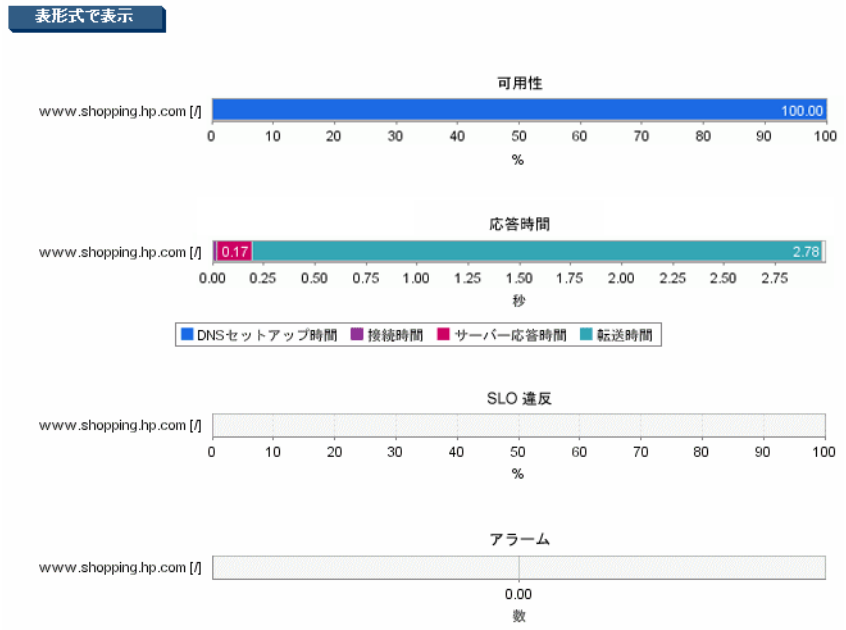
- すべてのリソース
- 対象別要約 : 顧客
- 対象別要約 : ロケーション
- 対象別要約 : サービスグループ

各フィールドについてのオンラインヘルプを参照するには、表の [**?**] ボタンをクリックします。

6 この結果表示ペインには、詳細を表示する選択肢もあります。[対象別要約 : サービスグループ] 表で [**HP Shopping Home Page**] サービスグループを選択します。結果表示ペインの表示は、選択した内容によって変わります。



7 [**グラフで表示**] ボタンを選択します。このサービスグループの要約データを示す棒グラフが表示されます。



顧客やサービスグループを選択すると、棒グラフ形式で要約を表示します。収集された実際のメトリックデータを見るには、次の 2 つの手順の説明に従って、監視対象レベルで表示する必要があります。

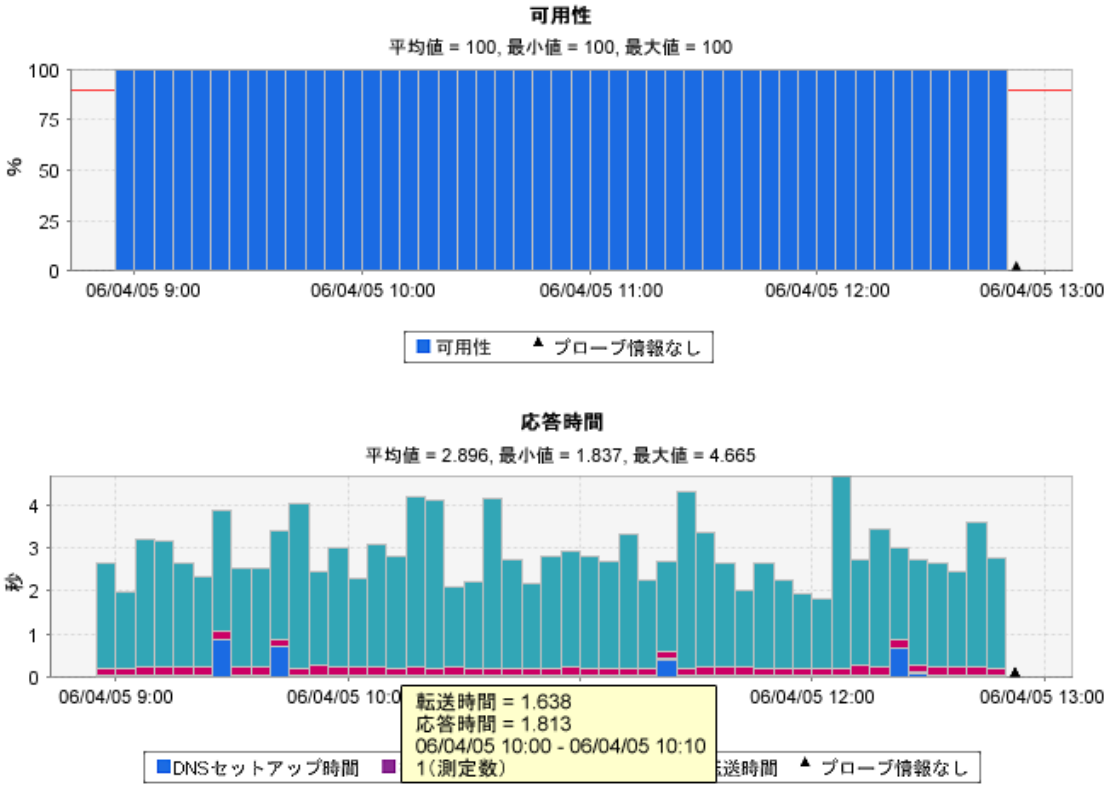
8 [リソース] ペインまたは結果表示ペインで、監視対象サービス **www.shopping.hp.com** を選択して ([リソース] ペインで選択するには、[Hewlett-Packard] > [HP Shopping Home Page] > [www.shopping.hp.com] を選択)、結果表示ペインに表示されるデータを確認します。

以下に示す例を参照してください。データ表には、顧客、サービスグループおよびこの監視対象に関連付けられたプローブシステムのロケーション情報が表示されます。

9 同じ監視対象 (www.shopping.hp.com) を選択した状態で、結果表示ペインを下方向にスクロールして、各メトリックのグラフを表示します。グラフは時間間隔に渡って収集された各データの数値を示します。以下のグラフの例を参照してください。

[可用性] メトリックに定義されたサービスレベル目標値 (SLO) は、可用性グラフに赤線で表示されます。SLO が他のメトリックに定義されている場合は、SLO を示す赤線は他のグラフにも表示されます。赤線が表示されない場合は、メトリックに SLO が定義されていないことを意味します。

グラフ上の棒や点にマウスを移動すると、メトリックの値や測定時刻がポップアップ表示されます (以下の応答時間グラフのポップアップウィンドウを参照してください)。

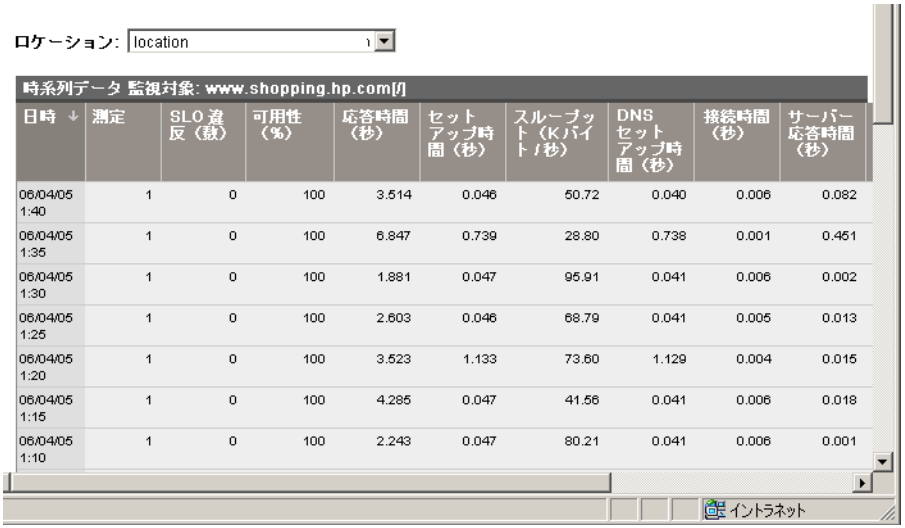


10 同じ監視対象 (www.shopping.hp.com) を選択した状態で、結果表示ペインを上方向に再度スクロールして、[**表形式で表示**] ボタンを選択します。

グラフは、プローブが 5 分ごとに行った測定値や、プローブにより収集され計算されたすべてのメトリックを示す表で置き換えられます。[**グラフで表示**] ボタンと [**表形式で表示**] ボタンを使うと、時系列データの表示を表形式やグラフ形式に切り替えることができます。

データはタイムスタンプに基づいてソートされます。さらに、列見出しをクリックすると、任意の列でソートできます。列を選択すると、列のソート順 (昇順または降順) を示す矢印が表示されます。ソート順を逆転させるには、列見出しの横の矢印を選択します。ダッシュボードでは他の場所でも同様のソート機能を利用できます。

この監視対象を測定するリモートプローブが複数ある場合は、別のプローブロケーションを選択して、そのロケーションで収集されている計測値を表示できます。

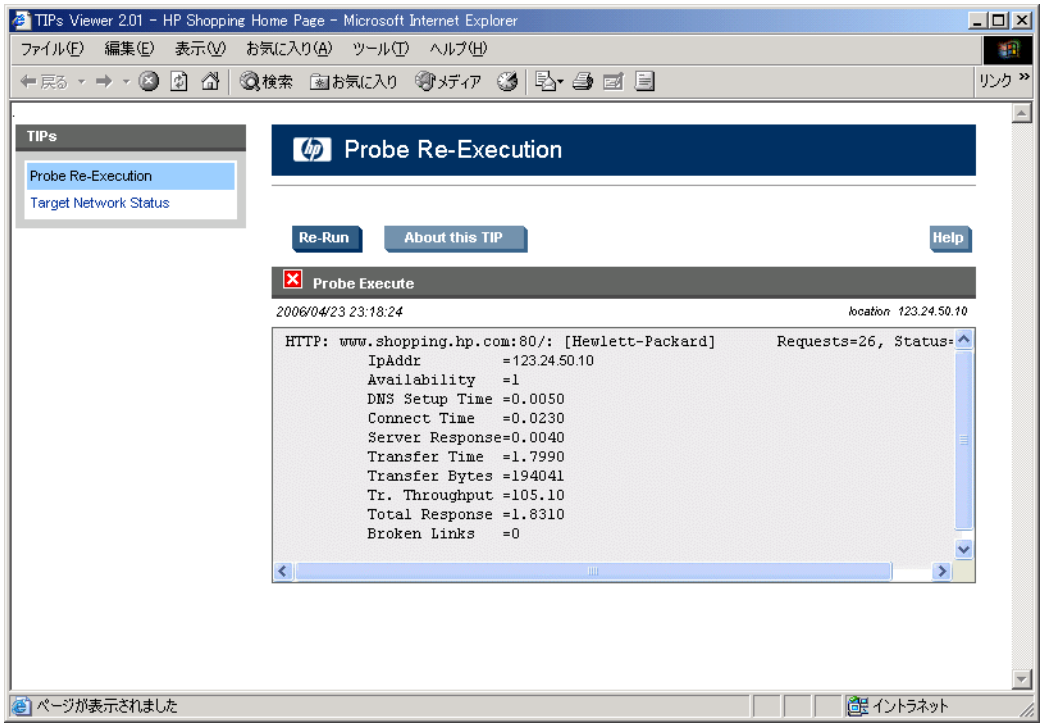


日時	測定	SLO 違反（数）	可用性（%）	応答時間（秒）	セットアップ時間（秒）	スループット（K バイト / 秒）	DNS セットアップ時間（秒）	接続時間（秒）	サーバー応答時間（秒）
06/04/05 1:40	1	0	100	3.514	0.046	50.72	0.040	0.006	0.082
06/04/05 1:35	1	0	100	6.847	0.739	28.80	0.738	0.001	0.451
06/04/05 1:30	1	0	100	1.881	0.047	95.91	0.041	0.006	0.002
06/04/05 1:25	1	0	100	2.603	0.046	68.79	0.041	0.005	0.013
06/04/05 1:20	1	0	100	3.523	1.133	73.60	1.129	0.004	0.015
06/04/05 1:15	1	0	100	4.285	0.047	41.56	0.041	0.006	0.018
06/04/05 1:10	1	0	100	2.243	0.047	80.21	0.041	0.006	0.001

11 同じ監視対象 (www.shopping.hp.com) を選択した状態で、結果表示ペインを上方向にスクロールして、[**ロケーション - 監視対象**] 表の最初の列で [**www.shopping.hp.com**] 監視対象の横にある [TIPs] (Troubleshooting Insight Packages) アイコンを選択します。

TIPs アイコンを選択すると、**TIPs Viewer** が表示され、このプローブに定義されたすべての TIPs がプローブシステム上で自動的に実行されます。この結果は TIPs Viewer の右ペインに表示されます。TIP コマンドが左ペインに表示され、右ペインに表示された結果とリンクされています。

起動した TIPs Viewer の最初の画面では、1 番上の TIP コマンドの結果が右ペインに表示されます。別の TIP コマンドの結果を表示するには、TIPs Viewer の左ペインにあるリストで別の TIP コマンドを選択します (この例では、[Target Network Status] コマンドを選択できます)。



左ペインで選択した TIP コマンドを再び実行するには、[**Re-Run**] ボタンを選択します。TIP コマンド結果の詳細情報を取得するには [**About this TIP**] ボタンを選択します。TIPs Viewer のオンラインヘルプを表示するには [**Help**] ボタンを選択します。

TIPs 設定プログラムを使用すると、TIPs をカスタマイズしたり、独自の TIPs コマンドを作成できます。TIPs をカスタマイズする方法については、163 ページの「TIPs の設定と使用」を参照してください。

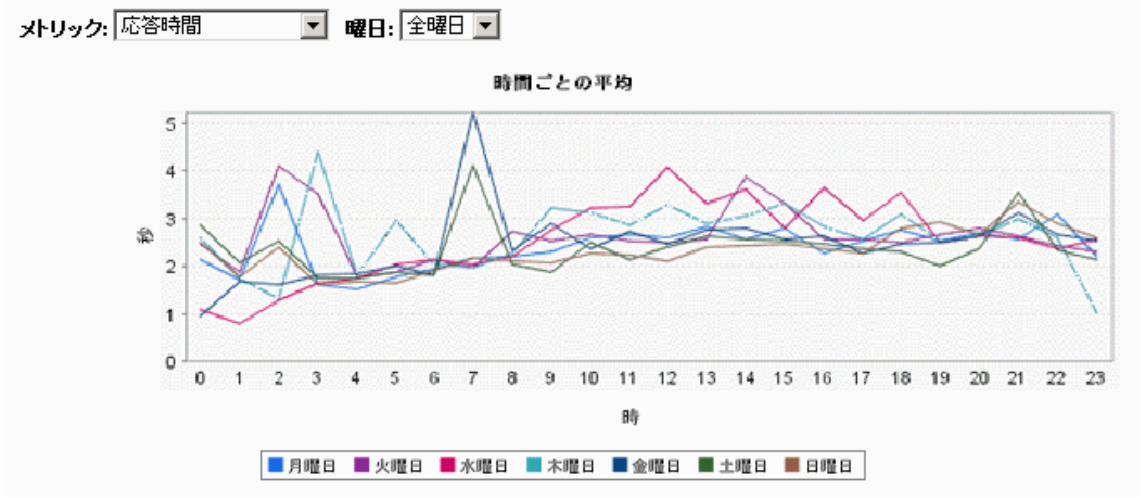
右上隅の赤いボタンをクリックして、TIPs Viewer を**閉じます**。

12 ダッシュボードの [リソース] ペインに戻り、[**All**] を選択します。結果表示ペインの上部にスクロールして、[**アラーム**] タブを選択します。アラームが生成された場合は、ここに表示されます。(前述の「設定マネージャのクイックスタート」で定義した [可用性] のサービスレベル目標値 (SLO) は SLO の違反があまり発生しないので、アラームが表示されない可能性があります。)

TIPs はそれぞれのアラームで使用できます。

アラームをダッシュボードに表示するには、アラームを発生させるアラームしきい値が設定され、かつ監視対象のアラームをダッシュボードに送信するように設定マネージャの [ファイル] > [設定] > [アラーム送信先] ダイアログで設定されている必要があります。

13 結果表示ペインの上部に再びスクロールして [**傾向**] タブを選択し、応答時間のような単一メトリックのデータに基づいてベースラインデータを表示します。以下のグラフ例を参照してください。[**ヘルプ**] ボタンを選択すると、各グラフの説明が表示されます。



[傾向] タブにより、ダッシュボードの [状況] ワークスペースが素早く表示されます。ダッシュボードの詳細については、以降の項を参照してください。

ダッシュボードの詳細

「ダッシュボードのクイックスタート」を完了後、ダッシュボードの詳細について、この項を参照してください。

ログイン

ダッシュボードにアクセスするには、いくつかの方法があります。

- 設定マネージャから、ツールバーの [**Internet Services ダッシュボードの起動**] (円グラフ) ボタンを選択します。
- 設定マネージャのメニューから、[**アクション**] > [**実行**] > [**Internet Services ダッシュボード**] を選択してダッシュボードを起動します。
- ダッシュボードをステータスに応じて起動することもできます。設定マネージャの [ステータス] 表示で、[監視対象サービスの状態] タブまたは [プローブからの受信データ] タブで監視対象サービスを右クリックしてダッシュボードを起動します。
- ブラウザのアドレスバーに以下の URL を入力して、ダッシュボードのデータ表示を開始することもできます。
  `http://<management server>:8080/OvisDashboard`

  ここで、*<management server>* は OVIS 管理サーバーで、*8080* はダッシュボードに設定されたポートです。ポートを変更する方法については、475 ページの「OVIS で行うポートの設定と変更」を参照してください。

別のログインを設定して、各ユーザーに異なるデータセットへのアクセスを許可することができます。たとえば、顧客に自分のデータだけを表示できるようにしたり、一部の顧客や選択したサービスグループを特定のオペレータに割り当てることができます。設定マネージャを使って、表示やユーザープロファイルを制限し、各ユーザーごとに表示できるデータを制御できます。詳細は、138 ページの「制限表示使用時のダッシュボードへのログイン」を参照してください。

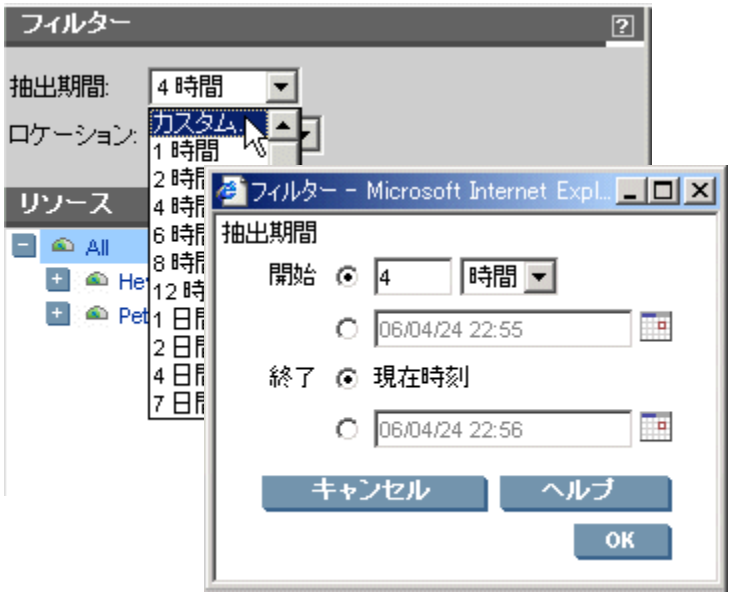
[状況] ワークスペース

[状況] ワークスペースを使用すると、すべてのサービス状況の表示、可用性、応答時間、サービスレベル違反および他の測定値などの詳細データの表示、OVIS が生成するアラームの表示、傾向グラフやベースライングラフの表示、問題の分析を実行する診断ツールやコマンド (Troubleshooting Insight Packages - TIPs) へのアクセスなどが行えます。

[フィルター] ペイン

フィルタを使用すると、プローブロケーションおよび期間によって、データをダッシュボードに表示できます。

[フィルター] ペインには、現在選択している**期間**が表示されます。データ表示の期間を変更したい場合は、ドロップダウンボックスから定義済みの期間を選択します。または、ドロップダウンボックスから [カスタム] を選択すると、特定の日付セットを入力できます。



現在選択されているプローブ**ロケーション**が、[フィルター] ペインに表示されます。異なるプローブロケーションのデータを表示するには、ドロップダウンボックスからロケーションを選択します。OVTA データの場合は、ロケーションにはサービス提供システムが含まれます。

デフォルトでは、設定マネージャ ([**ファイル**] > [**設定**] > [**ダッシュボード**]) で設定された期間の、すべての顧客とサービスグループのデータが表示されます。

[リソース] ペイン

[リソース] ペインには、すべてのサービス状況が素早く表示されます。[状況] アイコンについて以下の項で説明します。サービス状況は監視対象に対してサービスレベル目標値の違反率 (%) により示されます。各アイコンに割り当てられた割合 (%) は設定マネージャ ([**ファイル**] > [**設定**] > [**ダッシュボード**]) で変更できます。サービス状況はサービス階層を通じて伝達されます。

[リソース] ペインをナビゲーションに使用すると、ツリー表示 (+ で展開、- で折りたたみ) から項目を選択できます。ツリー表示のデータは以下のカテゴリ (サービス階層) にグループ化されます。

- [All] - すべての顧客の全監視対象
- [Customer] - サービスとサービス対象のグループ
- [Service group] - 顧客ごとの類似する監視対象サービスのグループ
- [Service target] - 1 つのプローブでモニターするサービスとプローブロケーション

選択した項目に関連付けられたデータは右ペインに表示されます。

ダッシュボードの [リソース] ペインのナビゲーションツリーで、「Unknown Target Name」という項目が表示される場合は、この監視対象のデータベースには収集されたデータは存在しません。この監視対象にホスト名が設定されている場合は、監視対象の識別に役立つように、ナビゲーションツリーで、ホスト名が表示されます。単一のサービスグループに複数の監視対象があり、その監視対象がデータを所有しない場合は、一意に監視対象を識別できるよう名前の後に連番のインデックスが表示されます。

[アイコンの説明] ペイン

[アイコンの説明] ペインでは、使用されるアイコンを説明しています。

[リソース] ペインおよび右ペインにある [要約] ビューには、サービス状況を表すアイコンが表示されます。サービス状況は、監視対象に対してサービスレベル目標値の違反率 (%) により示されます。サービス状況の測定方法については、136 ページの「ダッシュボードの設定」を参照してください。

サービスレベル目標値 (SLO) が定義されていない場合は、ステータスアイコンは緑色になります。顧客のいくつかの監視対象に SLO が定義されていない場合は、これらの監視対象はサービスグループや顧客の全体的なサービス状況表示には組み込まれません。これは、試作 / テストシステムや、プローブによる測定を実施したいシステムなど、全体のサービス状況 (health) が重要でない場合に役立ちます。また、設定したすべての SLO が応答時間に基づいている場合は、可用性はサービス状況に影響を与えません。

赤色、黄色、緑色に対するサービスレベル目標値の違反しきい値 は、OVIS 設定マネージャ ([**ファイル**] > [**設定**] > [**ダッシュボード**] ダイアログ) でカスタマイズできます。

[アラーム] タブには、アラーム状態の重要度を示すアイコンが表示されます。80 ページの「[アラーム] タブ」を参照してください。

[要約] タブ

[要約] タブを選択すると、監視対象サービスのステータス情報が表示されます。

[リソース] ペインで [All] が選択されると (デフォルト設定)、[要約] タブには次の表形式のデータが表示されます。

- 対象別要約 : 顧客
- 対象別要約 : ロケーション
- 対象別要約 : サービスグループ

[リソース] ペインのナビゲーションツリーまたはこれら表のいずれかのリストから、顧客、サービスグループ、または監視対象を選択できます。結果表示ペインにはこの選択に従ったデータが表示されます。この表から、赤色か黄色の [状況] アイコンで識別された特定の問題を簡単に詳細化できます。

表示対象をすべての顧客、顧客、顧客のサービスグループ、監視対象またはプローブロケーションから選択して、種々のデータを表示することができます。

たとえば、監視対象を選択した場合は、結果表示ペインには、この監視対象に関連付けられた顧客、サービスグループおよびプローブロケーションの各表形式のデータが表示されます。

顧客またはサービスグループを選択すると、結果表示ペインの下部に (スクロールして表示) 要約グラフが表示されます。(グラフが表示されない場合は、[**グラフで表示**] ボタンを選択します。[**グラフで表示**] ボタンと [**表形式で表示**] ボタンを使うと、データの表示を表形式とグラフ形式のいずれかに切り替えることができます。)

顧客を選択した際に表示される要約棒グラフを、以下に示します。

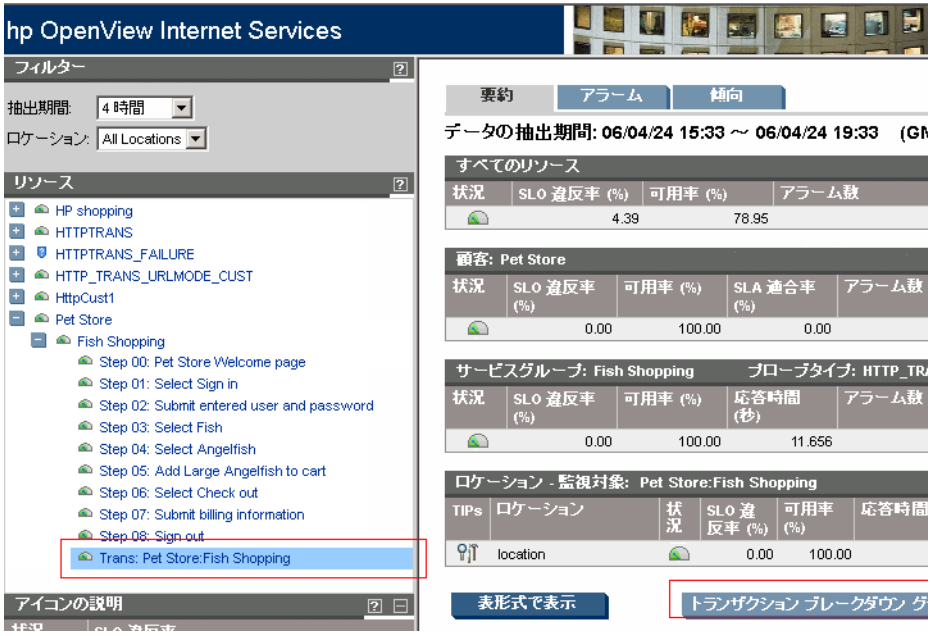
- 可用性 - このグラフは、選択した顧客の各サービスグループにおける可用性の割合を示します。
- SLO 違反 - このグラフは、選択した顧客の各サービスグループにおける SLO 違反率を示します。
- SLA 適合 - このグラフは、選択した顧客の各サービスグループにおける SLA 適合の割合を示します。
- アラーム - このグラフは、選択した顧客の各サービスグループにおけるアラーム数を示します。

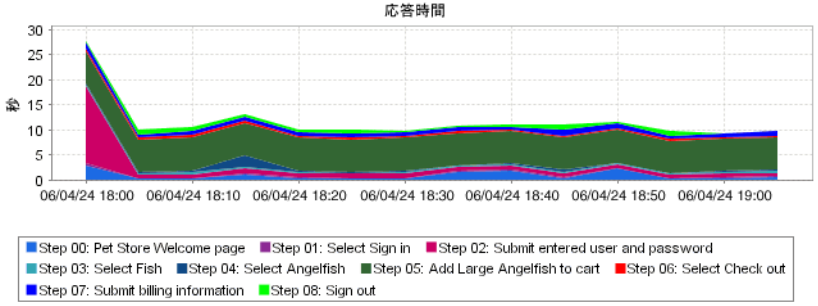
サービスグループを選択すると、表示される要約棒グラフは以下のようになります。

- 可用性 - このグラフは、選択したサービスグループの各監視対象における可能性の割合を示します。
- 応答時間 - このグラフは、選択したサービスグループの各監視対象における応答時間の構成要素を示します。
- SLO 違反 - このグラフは、選択したサービスグループの各監視対象における SLO 違反率を示します。
- アラーム - このグラフは、選択したサービスグループの各監視対象におけるアラーム数を示します。

監視対象を選択した場合は、プローブが収集する各メトリックの詳細な時系列データが表示されます。[**表形式で表示**] ボタンと [**グラフで表示**] ボタンを使用すると、時系列データの表示を表形式とグラフ形式のいずれかに切り替えることができます。監視対象レベルで [表形式で表示] ボタンを使用すると、プローブが行った各測定とプローブが収集や計算を行ったすべてのメトリックデータのタイムスタンプが表示されます。

Transaction Breakdown グラフは、HTTP_TRANS のような複数のステップから成るトランザクションのプローブがある場合に、この監視対象 (複数のトランザクションステップ全体を含む) を選択すると、使用可能になります。複数ステップの HTTP_TRANS トランザクションについては、以下の例を参照してください。





TIPs

監視対象サービスのレベルまで詳細表示させると、問題の特徴を詳細に把握するために TIPs (Troubleshooting Insight Packages) を使用できます。TIPs は、[アラーム] タブに表示された各アラームにも使用できます。

TIPs  アイコンを選択すると、TIPs Viewer が表示され、問題をトラブルシューティングするために定義されたすべての TIPs が、プローブシステムで自動的に実行されます。それぞれの TIP では、問題の監視対象サービスやアラームに対して 1 つまたは複数のコマンドを実行し、関連する情報を収集します。その結果が TIPs Viewer に表示されます。

TIPs には、サポートされるすべての OVIS プラットフォーム用に、多数のカスタマイズせずに使用できる TIPs やトラブルシューティングコマンドが含まれています。TIPs やコマンドの説明についてはヘルプの [**About This TIP**] を、また TIPs の実行方法については TIPs Viewer のヘルプを参照してください。TIPs の参照が終了したら、[TIPs Viewer] ウィンドウを閉じて、OVIS ダッシュボードに戻ることができます。

特定のトラブルシューティングを行うように、TIPs を編集したり、新しい TIPs やコマンドを作成することができます。TIPs Configuration プログラムを開くには、OVIS 管理サーバーで [**スタート**] > [**プログラム**] > [**HP OpenView**] > [**TIPs**] > [**TIPs Configuration**] を選択します。
TIPs の編集や独自の TIPs の作成方法については、TIPs Configuration プログラムのオンラインヘルプを参照してください。また、『*新機能 - Troubleshooting Insight Packages (TIPs)*』を CD やインストールしたディレクトリ `<install dir>¥help¥iops¥c¥ovis60-tips.pdf` から入手できます。

[アラーム] タブ

[アラーム] タブを選択すると、[リソース] ペインのナビゲーションビューで選択した項目のアラームが表示されます。

OVIS で生成されたアラームは、タイムスタンプ順に表示されます。アラームで表示される詳細情報は、ナビゲーションペインで選択した項目に応じて異なります。

列見出しをクリックすると、列ごとにアラームをソートできます。さらに、列見出しの矢印をクリックすると、降順または昇順でソートできます。

また、アラームをダッシュボードで表示するには、アラームの監視対象ダイアログの [データベース] チェックボックスをオンにする必要があります (設定マネージャの [**ファイル**] > [**設定**] > [**アラーム送信先**] で表示される内容を参照してください)。

 TIPs (Troubleshooting Insight Packages) - TIPs アイコンを選択すると、TIPs Viewer が起動し、アラームに関連したトラブルシューティング用のコマンドが実行されて、問題の診断に役立てることができます。

 トレース (OVTA 統合を設定している場合) - 表示された [トレース] タブで OVTA アイコンを選択すると、OVTA Console が起動します。表示されるデータは、OVIS で選択した監視対象トランザクションのアラームのコンテキストに従います。

重要度 - [重要度] 列に表示されるアイコンは、アラームの重要度に対応しています。これらは、[要約] タブに表示される [状況] アイコンとは異なります。[アイコンの説明] ペインには、危険域、重要警戒域、警戒域、注意域、正常域の定義が表示れます。これらアラームの重要度は、設定マネージャの [目標値] ダイアログで設定するアラームのしきい値に対応しています。

- 危険域
- 重要警戒域
- 警戒域
- 注意域
- 正常域

これらの重要度レベルは、OVIS 設定マネージャで設定された内容に基づいて、プローブごとに異なります。たとえば、応答時間は 5 秒以内とする SLO で、アラームしきい値を 10 秒として、それを超えたアラームを危険域の重要度とするような設定を行うことができます。

以下に、ダッシュボードでのアラーム表示の例を示します。

[傾向] タブ

[傾向] タブを選択すると、[リソース] ペインのナビゲーションビューで選択した項目のベースラインデータが表示されます。ベースライングラフは、ページ上部に表示されたデータ範囲の単一メトリックのデータに基づいています。このデータ範囲は、設定マネージャの [**ファイル**] > [**設定**] > [**データベースオプション**] と選択して、表示された [データベースオプション] ダイアログの [**プローブ / 監視対象サービスレベルのデータ**] で設定されたデータ量に基づきます。

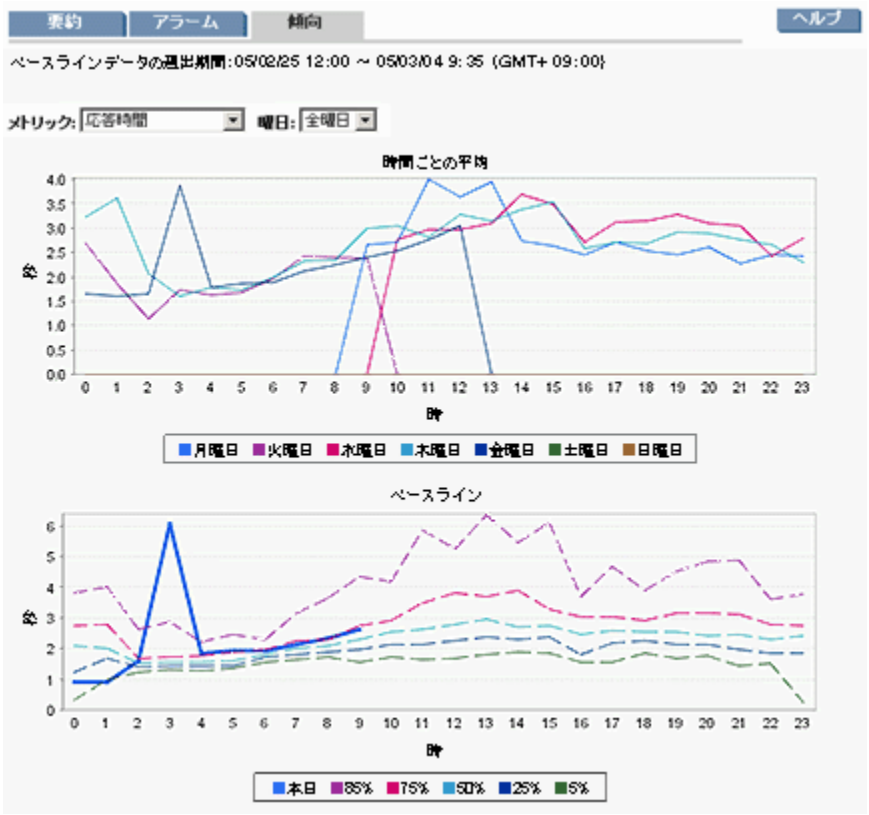
デフォルトでは、このデータベースは 7 日間の詳細データを保存するように設定されますが、30 日以上に設定すると、傾向がより明らかになります。これらのグラフを使用する場合、ディスクの空き容量に問題がなければ、[プローブ / 監視対象サービスレベルのデータ] のサイズを 30 日に増やすことをお勧めします。

[傾向] タブの詳細については、オンラインヘルプを参照してください。ベースライングラフには以下のものがあります。

- 時間ごとの平均 - 各曜日の 1 時間ごとのメトリック値の平均を表示します。

- ベースライン - メトリックの本日の値を、このメトリックの一般的な 1 時間ごとの値と比較できる形式で表示します。
- 応答時間分布 - 日付範囲でメトリックが特定の値になった回数を表示します (たとえば、応答時間 : 2.2 秒がその日付範囲で 38 回など)。これは、日付範囲で最も一般的なメトリックを簡単に見つけることができるヒストグラムを提供します。
- 累積分布 - メトリックが特定の値以下になった回数の割合を表示します (たとえば、応答時間 : 2.2 秒以下がその時点で 80%)。このグラフでは、サービス全体の品質を調べることができます。曲線の下の領域が大きいほど、よりよいサービスが提供されています。
- 時間ごとの統計 - 各曜日の 1 時間ごとのメトリックの平均値、中央値、正常域、最大値、最小値を表示します。

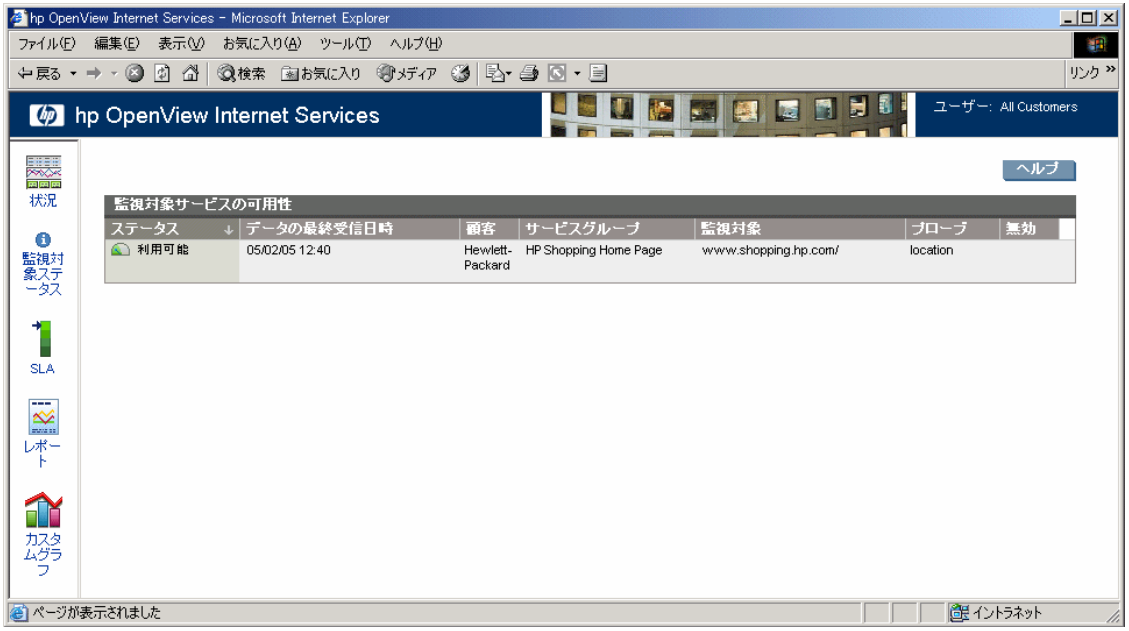
以下に傾向グラフの例を示します。



[監視対象ステータス] ワークスペース

ダッシュボードの左側にあるワークスペースペインで、[監視対象ステータス] ワークスペースのリンクを選択すると、監視対象サービスの可用性のステータスが表示されます。監視対象サービスのステータス表示は、プローブが監視対象に接続できるかどうかを示します。このページは自動リフレッシュされません。また、構成が大規模な場合は、このページの表示には多少時間がかかることがあります。

緑色は利用可能、赤色は利用不可を示します。利用できない監視対象には、エラー情報も表示されます。最も新しい通信エラーが画面の最上部に表示されます。このエラーのタイムスタンプは、該当するエラーが発生した時刻を示します。



ステータスを示す以下のアイコンが表示されます。

「プローブ情報なし」: 所定の時間内にこの監視対象の測定値はありません。

「利用不可」: この 監視対象は前回の測定で応答がありませんでした。

 「利用可能 - 応答待ち」: この監視対象は前回の測定で応答がありましたが、プローブ情報は、[**ファイル**] > [**設定**] > [**ダッシュボード**] と選択して、表示された [ダッシュボードとステータス] ダイアログでステータスを赤に設定した間隔内で受信されませんでした (デフォルトの間隔は 4)。

 「利用可能 - 応答待ち」: この監視対象は前回の測定で応答がありましたが、プローブ情報は、[**ファイル**] > [**設定**] > [**ダッシュボード**] と選択して、表示された [ダッシュボードとステータス] ダイアログでステータスを黄に設定した間隔内で受信されませんでした (デフォルトの間隔は 2)。

 「利用可能」: この監視対象は有効です。

 「無効」: 監視対象は無効です。

監視対象のステータスの色は、監視対象が応答しない間隔 (黄色または赤色表示にする) を指定して、決定します (たとえば、2 ～ 4 の間隔で応答なしの場合は、黄色のステータスを表示します)。[ステータス] ページで使用するこれらの値を設定マネージャで指定するには、[**ファイル**] > [**設定**] > [**ダッシュボード**] を選択します (詳しくは、101 ページの「その他の設定オプション」を参照してください)。

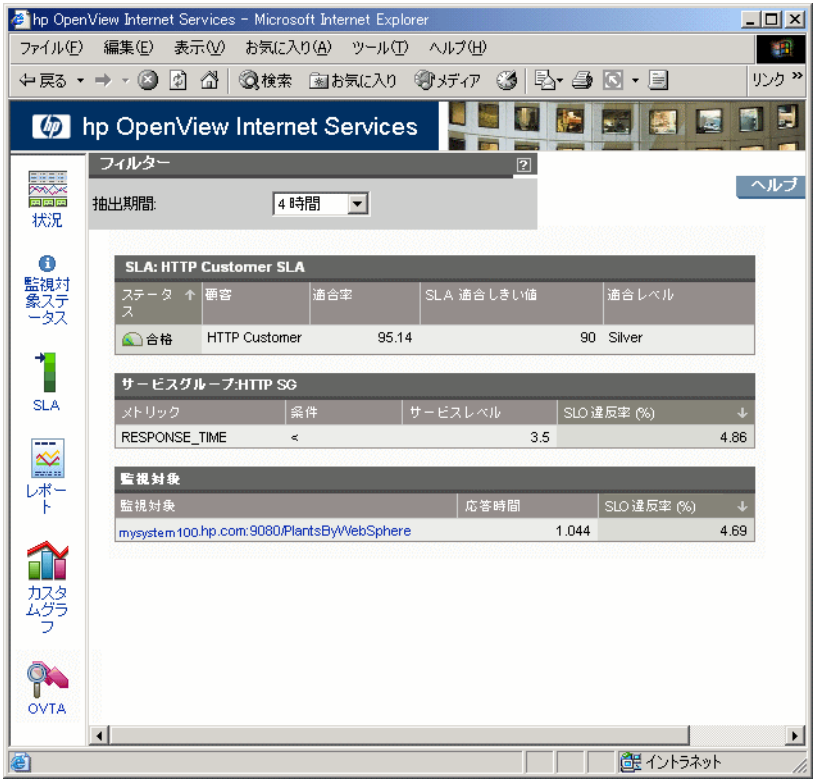
[SLA] ワークスペース

ダッシュボードの左側にあるワークスペースペインで、[SLA] ワークスペースのリンクを選択し、サービスレベル契約の適合性データを表示します。

適合値とは、SLA を構成する目標値 (SLO) がサービスレベルを満たした時間の割合です。たとえば、SLA に 2 つの SLO が設定されており、指定した間隔で 12 回測定します。1 つ目の SLO には 1 つの SLO 違反 (残り 11 つは適合) が報告され、別の SLO には 5 つの SLO 違反 (残り 7 つは適合) が報告されました。この場合、SLA 適合率は 75 パーセント ((11 + 7) ÷ 24 = 0.75) になります。サンプルの数は、ダッシュボードの時間フィルタの選択により決定されます。時間フィルタの値を変更すると、それに応じて報告される数が変わるため、計算結果である適合値の値も変わります。

SLA のステータスは**適合しきい値**により決定されます。適合値が適合しきい値と等しいかまたは上回る場合、[ステータス] 欄に [合格] というステータスが表示されます。適合値が適合しきい値を下回る場合は、[ステータス] 欄に [不

合格] というステータスが表示されます。SLA に対して [適合性しきい値] の値が選択されなかった場合、[ステータス] 欄のステータスは必ず [合格] となります。



現時点での月の SLA 適合を表示するには、[抽出期間] ドロップダウンボックスで [カスタム ...] を選択し、開始時間に今月初めの日時を、終了時間に [現在] を選択します。

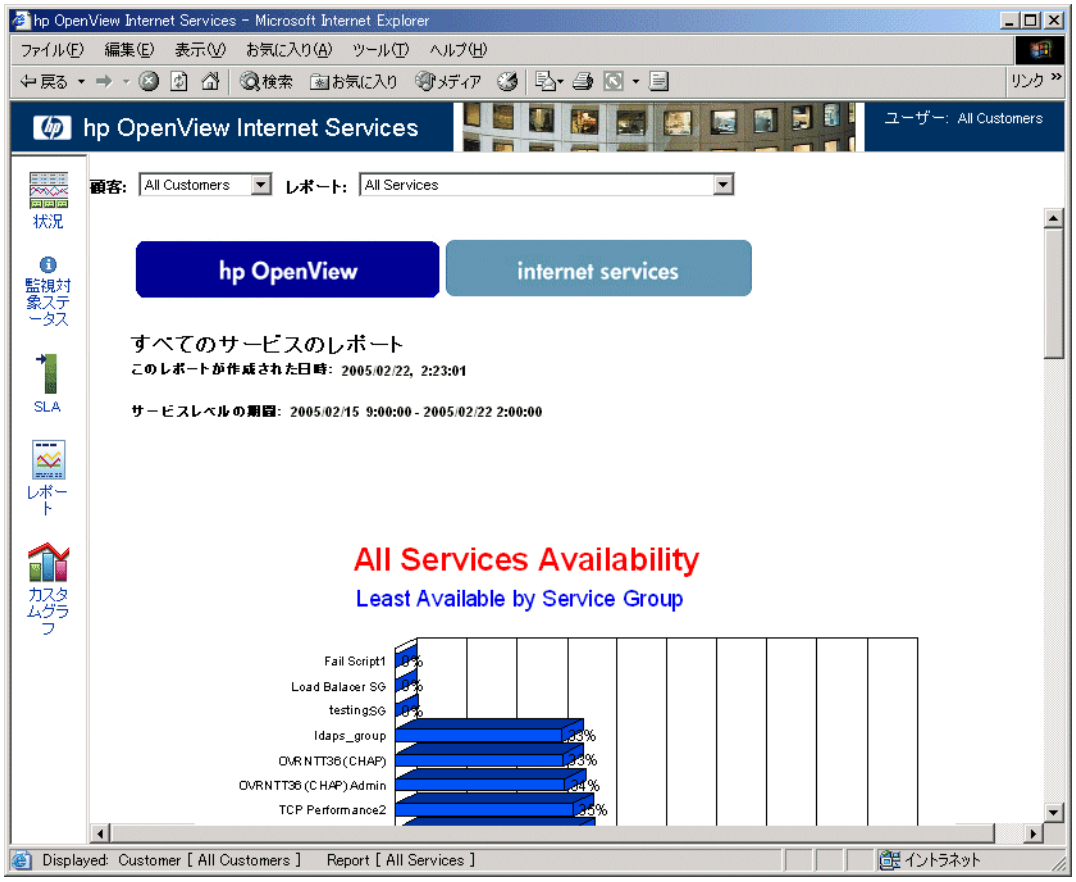
既定の SLA を構成する各 SLO の情報を表示するには、該当する SLA をクリックします。この詳細情報では、各サービスグループが SLA に関与している度合いを示します。また、詳細表示により、特定のメトリックのサービスレベル違反率 (%) や、サービスグループ内の監視対象ごとの平均メトリック値を調べることができます。

[レポート] ワークスペース

ダッシュボードの左側にあるワークスペースペインで、[レポート] ワークスペースのリンクを選択すると、要約レポートが表示されます。これらのレポートは、毎晩自動的に生成されるため、インストールと設定を行った場合には、翌日まで入手できません。OVIS で提供される標準のレポートには以下のものがあります。

- サービスグループごとの最小可用率レポート
- サービスグループごとの最大応答時間レポート
- サービスグループごとの最大のサービスレベル違反レポート
- ダイアルアップの失敗レポート

最初の 3 つでは、すべての監視対象サービスまたは特定のサービス、およびすべての顧客または特定の顧客を選択できます。



OVIS と OVTA の統合を予定していない場合に、OVTA レポートのテンプレートを削除するには、182 ページの「未使用の OVTA レポートの削除」を参照してください。

OVTA レポート

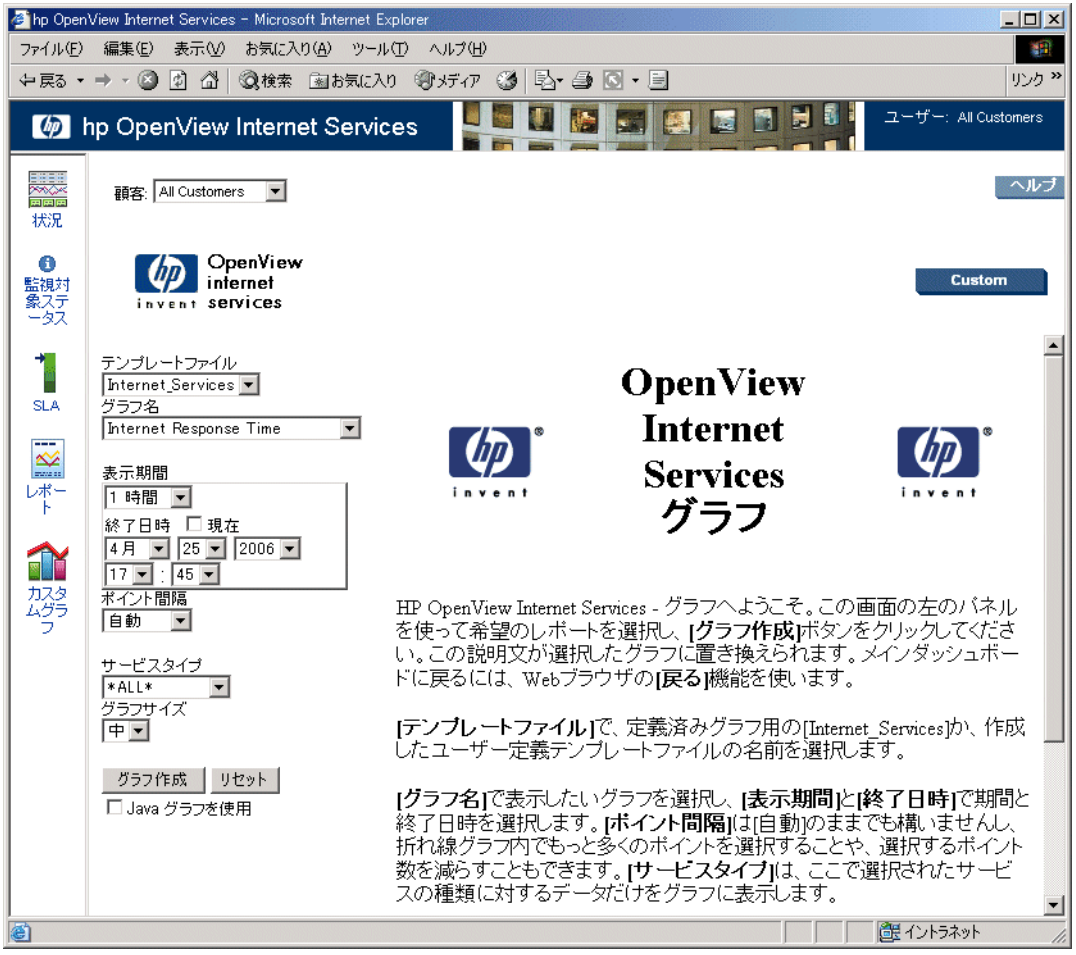
OVIS と OVTA (OpenView Transaction Analyzer) を統合している場合は、OVIS にインポートした OVTA データに基づいた以下のレポートが表示されます。これらのレポートの詳しい説明は、『*OVTA ユーザーガイド*』を参照してください。OVTA 統合の詳細は、第 5 章「OpenView 製品との統合」を参照してください。

- OVTA Service Group Summary (OVTA サービスグループの概要)
- OVTA Application Summary of Activity for the Last Day (OVTA アプリケーションの前日のアクティビティの概要)
- OVTA Application Summary of Activity for the Last Week (OVTA アプリケーションの先週のアクティビティの概要)
- OVTA Application Response Time Violations (OVTA アプリケーションの応答時間違反)
- OVTA Application Response Time (OVTA アプリケーションの応答時間)
- OVTA Application Transaction Volume (OVTA アプリケーションの処理量)
- OVTA Application Response Time Violations (Consumer Perspective) (OVTA アプリケーションの応答時間違反 (コンシューマの観点))
- OVTA Application Response Time Violations (Consumer/System Detail) (OVTA アプリケーションの応答時間違反 (コンシューマ / システム詳細))
- OVTA Application - Worst Performing Transactions (OVTA アプリケーション - 最低のパフォーマンスの処理)

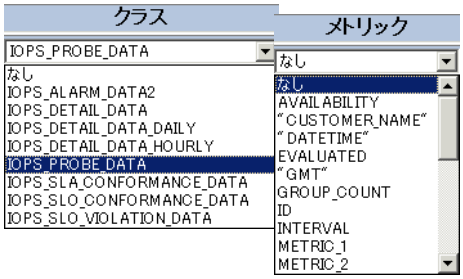
OVTA データを OVIS だけで使用する場合には、OVTA レポートテンプレートを削除できます。OVTA レポートテンプレートを削除する方法については、330 ページの「未使用の OVIS レポートを削除する (オプション)」を参照してください。

[カスタムグラフ] ワークスペース

種々のグラフを描画するには、[カスタムグラフ] ワークスペースを使います。カスタムグラフ機能を使うと、OVIS データに基づいて独自のグラフを作成できます。



グラフ表示内で、[**カスタム**] ボタンを選択し、[**ヘルプ**] ボタンを選択すると、メトリックの説明と共に各種の OVIS データベーステーブルに保存されたメトリックを表示できます。以下の例に、グラフ化できる OVIS データクラスといくつかのメトリックを示します。



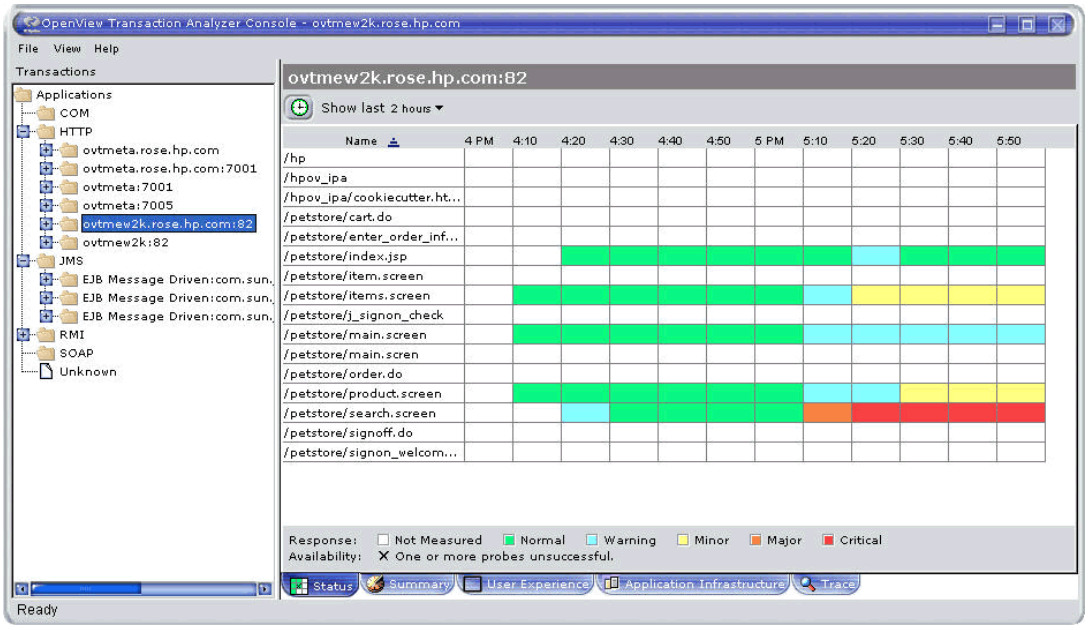
[OVTA] ワークスペース

OVIS と OVTA (OpenView Transaction Analyzer) を統合した場合は、OVIS ダッシュボードのワークスペースペインに OVTA Console へのリンク  が表示されます。

このリンクを選択すると、OVTA アプリケーションの起動に Java Web Start のインストールが必要であることを説明するページが表示されます。また、Java Web Start がない場合のダウンロード方法も含まれています。[Status] タブで [Launch OVTA Console] ボタンを選択して、表示された OVTA Console を起動します。

OVTA Console は、[アラーム] タブに表示される各 OVTA 監視対象のアラーム用の類似のアイコンからも起動できます。OVTA Console の表示内容はアラームのコンテキストに従います。

OVTA 統合については、第 5 章「 OpenView 製品との統合」を参照してください。



OVTA Console の詳細は、『*OVTA ユーザーガイド*』を参照してください。

Internet Services のアンインストール

Internet Services をアンインストールするには、次の手順に従います。

1 以下の Internet Services 関連サービスを停止します。たとえば、Windows 2000 の場合は、[**スタート**] > [**設定**] > [**コントロール パネル**] > [**管理ツール**] > [**コンポーネント サービス**] を選択します。
[コンポーネント サービス] ウィンドウで、[**サービス**] フォルダを選択し、表示されたサービスのリストから、停止するサービスを右クリックして [**停止**] を選択します。

   a Reporter Service
   b HP Internet Services
   c World Wide Web Publishing Service

2 [コントロールパネル] の [**アプリケーションの追加と削除**] で、HP OpenView Internet Services 製品を選択し、[**変更**] をクリックしてアンインストールします。

3 [アプリケーションの追加と削除] で、OVIS のパッチもすべて (以前のリリースのものも含む) アンインストールします。

4 リモートプローブをアンインストールするには、102 ページの「リモートプローブソフトウェアのインストールと削除」を参照してください。

OVIS アンインストールスクリプトで OVIS および TIPs を削除する場合、TIPs Configuration program で定義した TIPs が含まれるファイルは削除されません。このファイル名と場所は以下のようになります。

```
<data_dir>¥datafiles¥tips¥database¥SavedTIPsConfig.xml
```

同じシステムに再インストールする場合は、TIPs 定義を `SavedTIPsConfig.xml` ファイルから再インポートできます。これらの TIPs 定義を使用しない場合は、OVIS を同じシステム上に再インストールする前に、`SavedTIPsConfig.xml` ファイルを削除します。

TIPs 定義は複数の OVIS システムで使用できます。詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

3

Internet Services の設定

ここでは、以下の内容について説明します。

- サービスの設定
- 設定マネージャ
- サービスレベル目標値とアラームの設定
  - サービスレベル目標値とアラームの基本設定
  - サービスレベル目標値とアラームの詳細設定
  - 通知の設定
- ダッシュボードの設定
- サービスレベル契約 (SLA) の設定
- プローブのロケーション、タイミングとスケジューリング
  - ネットワーク接続の種類の設定
  - プローブのタイミングとスケジューリング
- ダウンタイムのスケジュールの設定
- プローブの動作
- TIPs の設定と使用
- リモートプローブソフトウェアのインストールと削除
- 設定ファイルの配布とアップデート

- 制限表示使用時のダッシュボードへのログイン
- 未使用の OVTA レポートの削除
- 大量の監視対象サービスの自動設定

サービスの設定

第 1 章で説明したとおり、Internet Services のサービス階層では、サービスを編成して、それらのサービスに関するレポートや問題の通知を受け取ることができます。

サービス階層の最上位は顧客で、企業、インターネットサービスプロバイダ、または会社内の部署名がこれにあたります。顧客の下には、サービスグループがあります。1 つの顧客には、1 つまたは複数のサービスグループがあり、各サービスグループは、同じ種類のサービスだけを含んでいる必要があります。各顧客には、その顧客のサービスグループに適用することが可能なサービスレベル契約を追加できます。

すべてのサービスグループの下には、Internet Services が測定および解釈して、レポートやアラームを生成する 3 つのコンポーネントがあります。これらの 3 つのコンポーネントを以下に示します。

- **監視対象サービス :** 測定するサービスとサービスの場所 (サービスの提供元) です。
- **サービス目標値 :** サービス目標値を達成するのに満たさなければならないサービス値 (可用性、応答時間など) です。
- **プローブロケーション :** プローブを実行する場所 (サービスの要求元) と、その場所への接続方法に関する情報です。

また、顧客にサービスレベル契約 (SLA) を設定して、各 SLA の適合レベルを設定できます。

Internet Services では、個別の顧客ごとに、独自のサービスグループや監視対象の組み合わせで、サービスの監視を編成できます。顧客が 1 人だけの場合、またはこの機能を使用しない場合は、すべてのサービスグループを配置することが可能なデフォルトの顧客を作成できます。

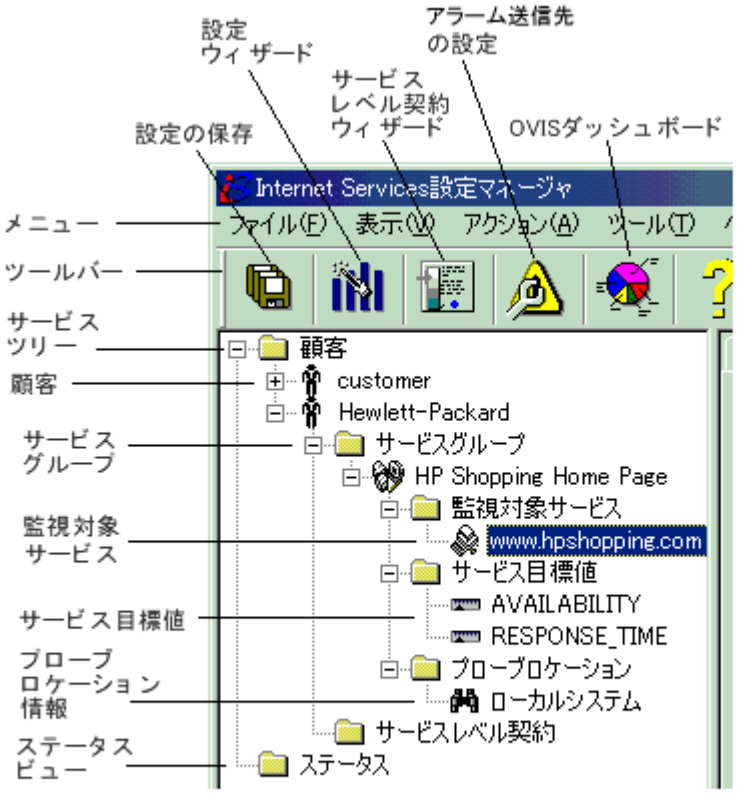
これらのサービスは、**設定マネージャ**を使用して手動で設定できます (以下の項を参照してください)。または、**設定ウィザード**を使用して、プローブで監視するサービスを順を追って設定できます。

また、大量の監視対象サービスの設定を一括して自動化する**一括設定**プログラムを使用することもできます (183 ページの「大量の監視対象サービスの自動設定」を参照してください)。

設定マネージャ

Internet Services の設定マネージャを使用して、サービスを追加、変更、削除したり、これらのサービスのプローブを設定したりすることができます。設定マネージャには、顧客、サービスグループ、監視対象サービス、サービスレベル目標値 (SLO)、プローブロケーション、およびサービスレベル契約の適合レベルの設定も含まれます。

[設定マネージャ] ウィンドウを開くには、[**スタート**] > [**プログラム**] > [**HP OpenView**] > [**Internet Services**] > [**設定マネージャ**] を選択します。



設定マネージャには、複数のユーザーが同時にログインできます。[**ファイル**] > [**設定**] > [**複数ユーザーオプション**] ダイアログボックスを使うと、あるユーザーが項目を追加 / 更新 / 削除している最中は、他のユーザーが変更できないように一時的にロックするかどうかを設定できます。複数ユーザーのロック機能を使用するための要件については、101 ページの「その他の設定オプション」を参照してください。

設定マネージャには**サービスツリー**表示があり、顧客 / サービスグループとその監視対象サービス、目標値、およびプローブロケーションの相互の上下関係を示します。

サービスツリー内では、コピー & ペーストを使って、項目を任意の顧客 / サービスグループ / 監視対象から別のものに追加できます。また、顧客やサービスグループの名前を変更できるユーティリティもあります。この `OvisDataRename` プログラムは `<install dir>¥bin` ディレクトリにあります。このユーティリティの実行により、新しい顧客名やサービスグループ名で設定ファイルが更新され、データベースに収集されたすべてのデータがこの新しい名前に変更されます。名前の変更処理を実行すると、複数のメッセージが表示されます。各メッセージに対応して、名前の変更を続けます。詳細はオンラインヘルプを参照してください。

設定マネージャには、設定ウィザードも用意されています。ウィザードを起動するには、ツールバーのボタンをクリックするか、[**ファイル**] > [**設定ウィザード**] メニューを選択します。このウィザードでは、顧客、サービスグループ、監視対象サービス、サービスレベル目標値、およびプローブロケーションを定義してプローブを設定するための手順が順に提示されます。また、階層内の任意の項目を右クリックして [設定ウィザード] を選択することでも、設定ウィザードにアクセスできます。

OVIS ダッシュボードには、設定マネージャのツールバーからアクセスできます。また、設定マネージャの**オンラインヘルプ**にもアクセスできます。

設定マネージャの使い方

設定マネージャで項目を追加、変更、削除するには、左ペインのツリービューで対象のフォルダを右クリックし、表示されるポップアップメニューから操作を選択します。ポップアップメニューからウィザードを実行することもできます。

サービスのプローブを設定するには、設定ウィザードを使用するか、次の一般的な手順を実行します。

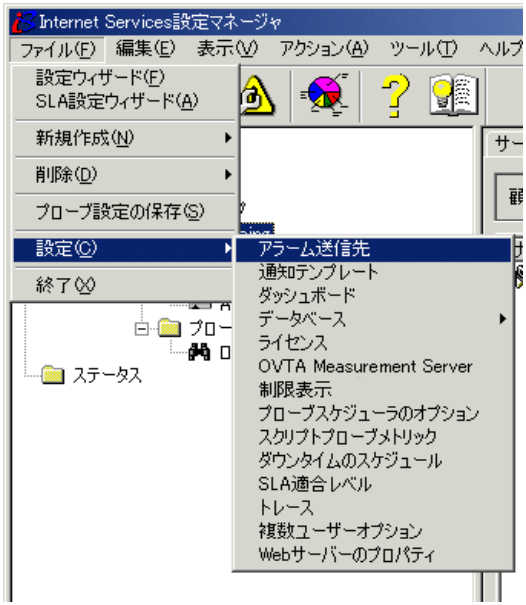
1. 顧客を作成します。
2. サービスグループを作成し、監視対象サービスのタイプ (HTTP、FTP、DNS サービスなど) を、表示されるリストから選択します。
3. 監視対象サービスを定義します。情報はサービスの種類によって異なります。
4. パフォーマンスメトリック (可用性、応答時間など) のサービス目標値を定義します。サービスレベル契約 (SLA) を定義することもできます。
5. プローブロケーションを定義し、リモートシステムとの接続の設定に必要なあらゆる情報を定義します。プローブのタイミングとスケジューリングの情報も必要に応じて定義します。
6. 設定の変更を保存して、設定マネージャを終了します。リモートプローブの場合は、リモートシステム上にもプローブソフトウェアがインストールされていることを確認する必要があります。さらに、プローブ設定ファイルをリモートシステムに配布します。

46 ページの「Internet Services 設定のクイックスタート」に、設定マネージャを使用したサービスの設定例を紹介しています。詳しい手順や各種サービスについては、オンラインヘルプも参照してください。

設定マネージャの左ペインのサービスツリー表示では、コピー (**Ctrl-C**) およびペースト (**Ctrl-V**) を使ってサービスレベル目標値などの項目を追加できます。また、メニューバーで、[**編集**] > [**コピー**] および [**編集**] > [**貼り付け**] を選択してもコピー & ペーストを行えます。

その他の設定オプション

OVIS 設定マネージャの [**ファイル**] > [**設定**] メニューで、次の項目を設定することもできます。



- [アラーム送信先]: OpenView Network Node Manager、OpenView Operations for UNIX、および OpenView Operations for Windows にアラームを送信します。この機能には、OVIS を NNM または OVO と統合する必要があります。詳細は、第 5 章「OpenView 製品との統合」を参照してください。

  また、アラームをダッシュボードに表示するには、設定マネージャで [アラーム送信先] の [データベース] チェックボックスをオンにする必要があります。

- [通知テンプレート]: アラーム発生時の通知用テンプレートを作成します。通知は電子メールで行うか、外部コマンドの実行が可能です。

- [ダッシュボード]: OVIS ダッシュボードのデフォルト設定を行います。たとえば、データ表示用のデフォルトの時間間隔を設定します。ダッシュボードの [状況] アイコンには、サービスレベル違反のデフォルトの最小値と最大値を設定し、アイコンがある重要度 (赤色、黄色、緑色) から別の重要度に変わるパーセンテージを定義します。

監視対象サービスが利用不可である間隔を定義することにより、監視対象サービスのステータスを黄色または赤色に変更するタイミングを設定できます (たとえば、2 ～ 4 の間隔で利用不可な場合、ステータスを黄色で表示します)。

- [データベース]: データベースへのログインおよびデータベースにデータを保存するためのオプションを設定します。
- [ライセンス]: ライセンスデータを表示したり、ライセンスキーを取得するためのライセンスウィザードを実行したり、電子メールで取得したライセンスキーを OVIS に直接インポートしたりします。
- [OVTA Measurement Server]: OVTA と OVIS との統合を設定する場合に使用する OVTA Measurement Server の場所を定義し、接続をテストします。
- [制限表示]: OVIS ダッシュボードのデータへのアクセスを顧客別に制限します。また、複数の顧客へのアクセスや、ある顧客の一部のサービスグループだけへのアクセス、またはこれらの任意の組み合わせでのアクセス制限を定義するために、プロファイルを設定できます。
- [プローブスケジューラのオプション]: 設定変更の保存後にプローブスケジューラが再起動しないように設定したり、ネットワーク接続が順番に実行される (シリアライズされる) ように設定したりします。
- [スクリプトプローブメトリック]: カスタマイズしたスクリプトプローブ SRP ファイルをロードして、プローブが定義した追加メトリックを収集できるようにします。
- [ダウンタイムのスケジュール]: サービスに適用するダウンタイム値を新規に設定します。
- [SLA 適合レベル]: サービスレベル契約 (SLA) の適合レベル (例 : ゴールド = 95%) を定義します。ここで設定したレベルを SLA に適用できます。
- [トレース]: トラブルシューティングを目的として、サーバーまたはプローブのより詳細なトレースを指定します。サーバーまたはプローブシステムのトレースファイルの最大サイズも指定します。
- [複数ユーザーオプション]: 設定 マネージャで、複数のユーザーが同時に設定項目を追加 / 編集 / 削除 / 保存しようとした場合にロック機能を使用するかどうかを指定します。誰かが設定ウィザードなどのウィザードを使用している場合は、他のユーザーの操作を制限するようにグローバルロックが使用されます。デフォルト設定はロック機能を使用しません。このデフォルト設

定では、複数のユーザーが設定マネージャにログインして、同時に変更を行うことができるため、変更が上書きされることがあります。

Windows 2000 システムでこのロック機能を使用するには、Service Pack 4 以降が必要です。Windows 2000 Service Pack 3 では動作しません。

さらに、この機能を使用するには、設定マネージャを実行するユーザーや、バッチ設定 (`IopsLoad.exe`) を使用するユーザーは、Windows の [**グローバル オブジェクトの作成**] セキュリティ権限セットが必要です。このセットは、コントロール パネル内の [**ローカルセキュリティポリシー**] からアクセスできます。コントロール パネルで、[**管理ツール**] > [**ローカル セキュリティ ポリシー**] に移動します。続いて、左ペインで [**ローカル ポリシー**] > [**ユーザー権利の割り当て**] を展開します。右ペインの [**グローバル オブジェクトの作成**] をダブルクリックして、必要に応じてこのポリシーにユーザーやグループを追加します。この [**グローバル オブジェクトの作成**] セキュリティ権限を設定せずに、ロック機能をオンにした場合は、すべてがロックされるため、変更が行えなくなります。

何らかの理由で、ロック解除できない状態になった場合は、ロック機能をオフにしてすべてのロックを解除してください。その方法が機能しない場合は、設定マネージャ (`IopsConfig.exe`) のすべてのインスタンスとバッチ設定 (`IopsLoad.exe`) を閉じて、すべてのロックを解除します。

- [Web サーバーのプロパティ]: サーバーとプローブシステム間の通信を設定し、ポートを設定します。

これらの項目については、オンラインヘルプを参照してください。

また、設定マネージャでは、[ツール] メニューから以下の項目を選択できます。

- [**ツール**] > [**プローブの情報**] により、設定した監視対象サービス数のレポートを取得できます。
- [**ツール**] > [**項目の検索**] により、サービスツリーの階層で特定の項目を見つけます。
- [**ツール**] > [**監視対象の一括更新**] により、複数の監視対象サービスに対して、パスワードなどのパラメータの一括更新を行えます。

管理者以外のユーザーで設定マネージャを実行する

設定マネージャは、恒久ライセンスまたは試用延長ライセンスをインストールするために、ローカル管理者の機能を必要とします。また、ローカル管理者として実行すると、正常に実行するために必要な機能、権限、およびセキュリティを使用できます。

設定マネージャを管理者権限のないユーザーで実行したい場合は、以下の手順を実行します。手順 4 から 5 は、OVIS パッチ、ホットフィックス、更新を適用した後に、繰り返す必要があります。これらは、適切な権限を持たない、新しいファイルやレジストリのエントリに適用されることがあるためです。

1 必須のライセンスは必ず管理者としてインストールしてください。

2 [**複数ユーザーオプション**] をオンにして設定マネージャを実行したい場合は、各ユーザーに [**グローバル オブジェクトの作成**] のポリシーを割り当てます。[**複数ユーザーオプション**] は、設定マネージャの [**ファイル**] > [**設定**] > [**複数ユーザーオプション**] から設定し、[**グローバル オブジェクトの作成**] のポリシーは、[**コントロール パネル**] > [**管理ツール**] > [**ローカル セキュリティ ポリシー**] > [**ローカル ポリシー**] > [**ユーザー権利の割り当て**] から割り当てます。

3 管理者として、保存後にプローブが再起動されないように [**プローブスケジューラのオプション**] を設定します。これを行うには、設定マネージャを起動して、[**ファイル**] > [**設定**] > [**プローブスケジューラのオプション**] を選択して [**スケジューラおよびネットワークオプション**] ダイアログを開きます。[**ローカルスケジューラ**] の [**保存した後にプローブを再起動しない**] チェックボックスをオンに指定して [**OK**] ボタンをクリックします。

4 以下の手順説明に従って、次のディレクトリに各ユーザーの変更権限を追加します。

`C:¥Program Files¥Common Files¥Hewlett-Packard¥HPOvLIC`

<OVIS のインストールディレクトリ >
(デフォルトでは `C:¥Program Files¥HP OpenView`)

> OVIS データディレクトリが OVIS のインストールディレクトリのサブディレクトリの場合は、以下のディレクトリは省略します。

<OVIS データディレクトリ >
(デフォルトでは `C:¥Program Files¥HP OpenView¥Data`)

ユーザーを次のようにディレクトリのセキュリティに追加できます。

a Windows エクスプローラを起動して、対象のディレクトリを右クリックして [**プロパティ**] を選択します。[**セキュリティ**] タブを選択し、[**追加**] ボタンを押して [**ユーザーまたはグループの選択**] ダイアログを開きます。

b 希望するグループ名やユーザー名を選択します。[**追加**] ボタンをクリックして下のペインに表示し、[**OK**] を押します。

c これにより、[**プロパティ**] ダイアログに戻り、[アクセス許可] 欄の [変更] の [**許可**] ボックスをクリックできます。必ず [**継承可能なアクセス許可を親からこのオブジェクトに継承できるようにする**] ボックスをオンにして、そのユーザーにパーミッションを割り当てるために [**OK**] をクリックします。

5 各ユーザーに `HKEY_LOCAL_MACHINE>SOFTWARE>Hewlett-Packard>Internet Services` への**読み取り**と**フルコントロール**のパーミッションを与えます。

これを行うには、[**スタート**] > [**ファイル名を指定して実行**] ウィンドウから `regedt32` を実行します。`HKEY_LOCAL_MACHINE > SOFTWARE > Hewlett-Packard` を展開し、続いて、`Internet Services` を選択します。regedt32 メニューバーから [**編集**] > [**アクセス許可 ...**] を選択して、[**Internet Services のアクセス許可**] ダイアログを開きます。目的のユーザーを選択し、[読み取り] および [フルコントロール] の両方のパーミッションの [**許可**] ボックスをオンにします。続いて、[**適用**] ボタンをクリックします。

以降では、次の項目について詳しく説明します。

- サービスレベル目標値 (SLO) 、アラームおよび通知
- ダッシュボードの設定
- サービスレベル契約 (SLA)
- プローブの動作
- プローブのタイミングとスケジューリング、およびプローブロケーションの定義
- ダウンタイムのスケジュール
- リモートプローブの設定とインストール

- 制限表示

サービスレベル目標値とアラームの設定

サービスグループの設定時には、グループの可用性や応答時間などの測定のための予想されるサービスレベル目標値 (SLO) を設定することができます。

SLO では、サービスの希望する可用性またはパフォーマンスレベルを (応答時間などのメトリックに基づいて) 定義します (例 : 可用性 =95%、または応答時間 =5 秒など)。プローブが特定の監視対象サービスを監視するときに、これらのメトリックに基づくデータを収集し、収集された値は SLO と比較されます。たとえば、SLO が 5 秒のときにプローブが応答時間を 10 秒であると検出した場合、SLO 違反が記録されます。SLO 違反は追跡され、ダッシュボードの [SLO] タブに表示されます。さらに、アラームのしきい値違反に基づいて、アラームを OVO または NNM に送信することもできます。SLO とアラームの生成については、この項でさらに詳しく説明します。

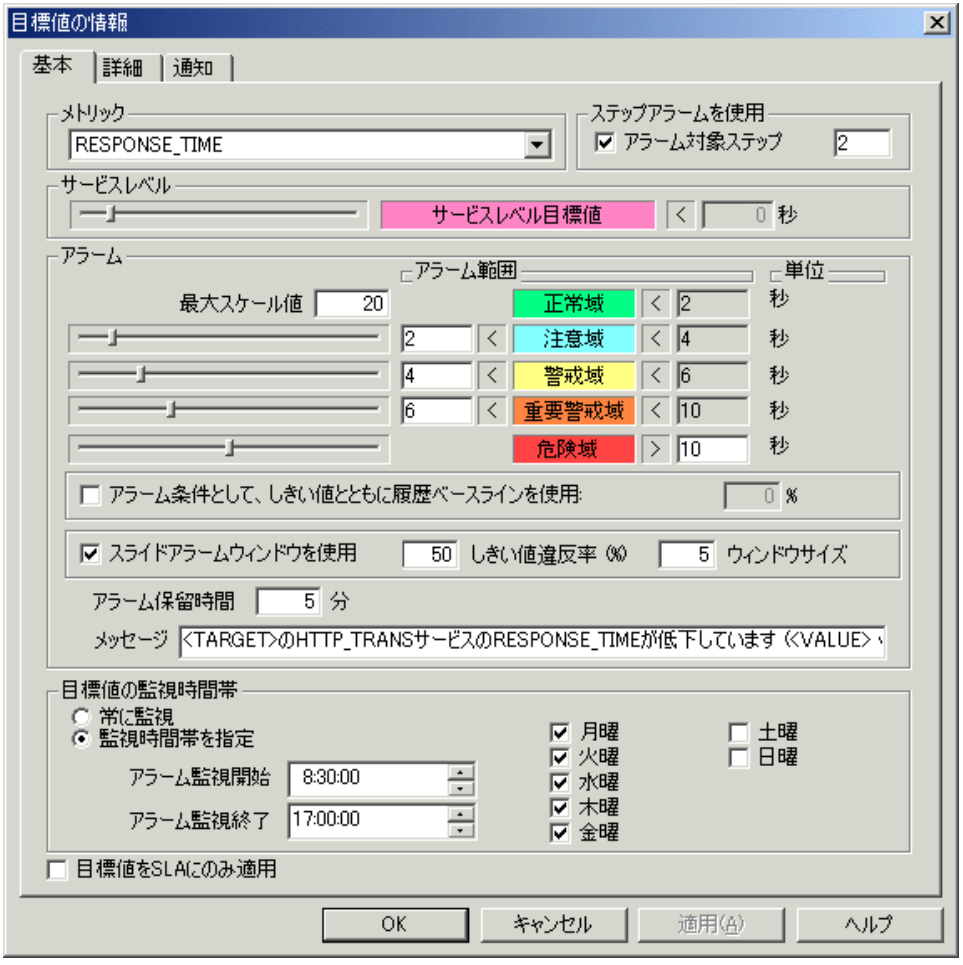
また、サービスレベル契約 (SLA) を設定することもできます。SLA は、基本的には複数のサービスレベル目標値 (SLO) の組み合わせです。SLA の適合レベルを設定できます (例 : 顧客によって適用可能な適合レベルをゴールド =95% と設定)。SLA の適合レベルは、ダッシュボードの [SLA] タブに表示されます。142 ページの「サービスレベル契約 (SLA) の設定」を参照してください。

サービスグループ内の監視対象をどのようにグループ化するかを決める 1 つの基準は、監視対象の予想されるパフォーマンス特性が似ているかどうかです。たとえば、グループの応答時間の SLO を設定したり、応答時間に関するアラームを設定するのであれば、応答時間が大幅に異なる 2 つの HTTP 監視対象サービスをグループ化するのは適切とはいえません。

設定マネージャでは、次に示す [目標値の情報] ダイアログの 3 つのタブで SLO やアラームのしきい値の設定を行うことができます。

- [**基本**] タブは、サービスレベル目標値の設定と基本的なアラームの定義に使用します。
- [**詳細**] タブは、アラーム式 (単一のメトリック値に基づくアラームではない) の指定に使用します。
- [**通知**] タブは、アラームの目標値の通知を設定するために使用します。

サービスレベル目標値とアラームの基本設定



このダイアログに入力した情報は、サービスグループに関係します。設定は、Internet Services ダッシュボードに表示される結果と、サービスレベル契約 (SLA) 評価に影響を与えます。

アラームは、他のイベントマネージャと統合するためのもので、サービスグループ内のすべての監視対象サービスに適用されます。サービスレベルとアラームの設定は、通常は目的が異なるものとして分けられていますが、サービ

スレベル違反に達する前にアラームを送信できるように、同じダイアログボックスで設定できるようになっています。これにより、運用グループは、契約違反になる前にそれに対処することができます。

Internet Services は、Network Node Manager (NNM)、OpenView Operations for UNIX、OpenView Operations for Windows、および SNMP を受信するその他のイベントマネージャにアラームを送信できます。

また、アラームを OVIS ダッシュボードに表示したい場合は、設定マネージャの [ファイル] > [設定] > [アラーム送信先] ダイアログで [**データベース (アラームと NNM の統合)**] チェックボックスをオンにする必要があります。

[アラーム送信先の設定] ダイアログの詳細は、134 ページの「アラームの送信」を参照してください。

このダイアログの多くの設定項目には推奨値が表示され、この値をそのまま使用することも変更することもできます。サービスグループの設定は、保存するまで適用されません。目標値を設定することによって、特定のメトリックの予想限界値を定義します。サービスグループの収集したメトリック値は、設定された値によって評価されます。これらの設定についての詳細は、この後の項を参照してください。

[メトリック] セクション :

[メトリック] セクションで、目的のメトリックを選択します。

[ステップアラームを使用] セクション :

ステップアラームを指定できます。Web トランザクション (HTTP_TRANS プローブ)、Script プローブまたはカスタムプローブの個々のステップでアラームを使用したい場合は、このボックスをオンにします。ステップアラームは、アラームにのみ適用されるため、このボックスをオンにすると、SLO フィールドは淡色表示になります。

ステップの番号を入力します。デフォルト設定は -1 で、この場合、アラームはトランザクション全体を対象とします。1 つのステップを選択するには、0 から始まる任意の数値を入力します。ステップ番号は 0 で開始されます。アラームのセットごとに 1 つのステップだけを選択できます。1 つのトランザクションの複数の個別ステップにアラームを作成するには、それぞれに個別のアラーム定義を作成します。同じメトリックをアラーム定義の複数のセットで使用できます。ステップアラームは応答時間メトリック用に使用され、可用性用ではありません。

これは、可用性はトランザクション全体に対して判断されるためです。あるステップが利用できない場合は、そのトランザクションは利用不可のマークが付けられます。

ステップ番号は、ダッシュボードの詳細ページと設定マネージャの [ステータス] ページで [詳細の表示] を選択すると表示されます。

[サービスレベル] セクション :

[サービスレベル] セクションで、メトリックのデフォルトを使用するか、しきい値を設定します。メトリックのすべての受信値は、このしきい値に対して比較されます。このしきい値を超える受信値は、違反としてカウントされ、Internet Services のダッシュボード表示で報告されます。また、サービスの稼働状況の判定に使用されます。サービスレベル設定は、アラームの生成には使用されません。

[アラーム] セクション :

- **[アラーム範囲]:** 次の各カテゴリのアラームイベント範囲の値を、スライダーバーで定義します。
  - 注意域
  - 警戒域
  - 重要警戒域
  - 危険域
  - メトリックがこれらのどの範囲にも該当しない場合は、ステータスは正常域にあるとみなされます。

  応答時間またはその他のメトリックの値がここで指定した値を下回る場合は、一番上 (注意域) の値から順に修正してください。可用性メトリックの値がここで指定した値を上回る場合は、一番下の値から順に修正します。

  応答時間タイプのメトリックの範囲には、大きい方の数字は含まれますが、小さい方の数字は含まれないことに注意してください。たとえば、「2 < 注意域 < 5」は、応答時間が 3、4、および 5 秒の場合に注意域ステータスであることを意味します。

> 可用性がゼロの場合 (すなわち、監視対象が利用不可の場合)、他のメトリックはすべて無効と見なされ、アラーム生成のために計算されません。監視対象が利用不可のときに応答時間を検討しても意味がありません。また、1 回の測定における 1 つの監視対象の可用性は 0 か 100% のいずれかです。スライダーバーでは 0 と 100% の間で設定が可能な場合でも、可用性メトリック目標値をデフォルトの 90% や 100% に設定してもアラーム生成やサービスレベル目標値に違いは生じません。これは、可用性は、特定の間隔のサービスグループにある任意の監視対象に対して、常に 0 か 100% のいずれかになるためです。

- **[アラーム条件として ... 履歴ベースラインを使用]:** チェックボックスをオフにすると、アラーム条件として使用されません。アラーム数を制限する場合は、チェックボックスをオンにします。ベースラインの値によって、*正常域* とするメトリック値の割合を指定します。ある曜日のある時間帯にメトリック値が 80% に収まる場合、この設定はメトリックのアラーム設定よりも優先されます。ベースラインの正常域とする範囲は自動的に計算されます。このベースラインは使用率が高い期間に適しており、メトリック値は上限に達しているが、正常範囲とみなす場合に有効です。詳しくは 126 ページの「ベースラインの動作」を参照してください。

  > このベースラインの値は、アラームがトリガーされるタイミングの決定にのみ使用され、ダッシュボードのベースライングラフには適用されません。

- **[スライドアラームウィンドウを使用]:** スライドアラームウィンドウを使用すると、間違ったアラームや、特定の時間枠内で繰り返される問題のような場合のアラームだけを減らすことができます。過剰なアラームを抑制するために、アルゴリズムを適用するには、このチェックボックスをオンにします。

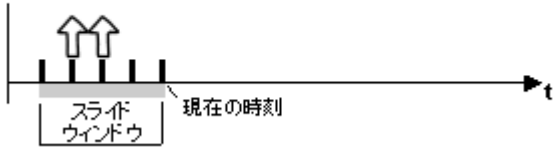
  スライドウィンドウは指定したプローブ測定の数として定義されます。たとえば、5 つの測定サンプルのウィンドウサイズを入力します。アルゴリズムは指定した数のサンプルをメモリーに保持します。新しいサンプルがログされると、ウィンドウが前方にスライドし、常に指定した数の測定値をメモリーに保持します。しきい値違反のアラーム数は、割合を算出するために、

ウィンドウ内のサンプル数と比較されます。この比率は指定した [違反しきい値 (%)] に比較されます。計算した比率が [違反しきい値 (%)] 以上の場合は、アラームがトリガーされます。

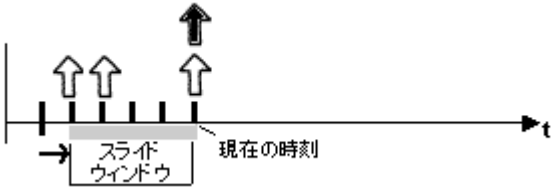
スライドアラームウィンドウ機能は起動したら、違反率の計算を行う前に、[ウィンドウサイズ] で指定したサンプルの数だけ待つ必要があります。

たとえば、[ウィンドウサイズ] が 5 で、最初の 5 つのプローブ測定値がアラームしきい値違反となった場合は、([違反しきい値 (%)] の値に関係なく) 5 番目の違反でアラームが生成されます。

以下のグラフは、スライドアラームウィンドウのアルゴリズムを図解しています。この例では、5 分間隔の測定サンプルが黒い縦棒で示されています。スライドウィンドウは灰色の横棒で示されます。ウィンドウサイズは 5 サンプルです。現在時刻が示され、アラームしきい値違反は白い上向き矢印で示されます。実際のアラームは黒い上向き矢印で示されます。スライドウィンドウ内のアラーム生成の [違反しきい値 (%)] は 50% に定義されています。

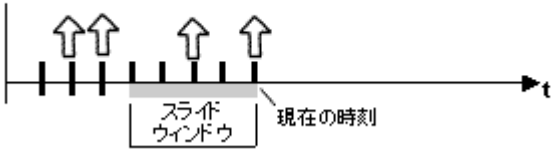


上の図では、スライドウィンドウに最新の 5 つのサンプルが含まれています。2 つの違反が発生し、それぞれ白い矢印で示されています。ウィンドウ内で発生した違反の比率は、「しきい値違反アラーム数 / ウィンドウ内のサンプル数 (2/5 = 40%)」で計算されます。40% は [違反しきい値 (%)] の 50% より小さいので、アラームはトリガーされません。

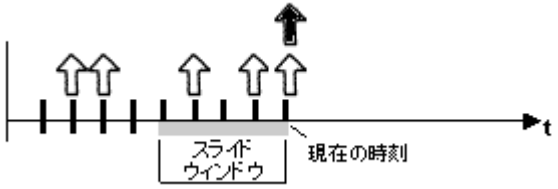


上の図では、スライドウィンドウは最新の 5 つのサンプルを含めるため、5 分間分シフトしています。新しい違反が発生し、3 つ目の白い矢印が示されます。これにより、ウィンドウ内には現在 3 つの違反があります。ウィンドウ内で発生した違反の比率は 3/5 = 60% です。これは [違反しきい値 (%)] が 50% であるため、アラームがトリガー (黒い矢印で示す) されます。

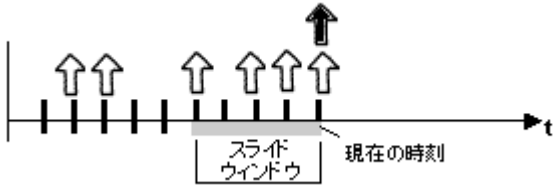
上の図では、スライドウィンドウは再びシフトして、1 つの違反がウィンドウの外に出ました。ウィンドウ内には現在 2 つの違反だけがあります。その結果、違反の比率は 2/5 = 40% になります。アラーム状態は正常域に戻り、正常域アラームが送信されます。[**ファイル**] > [**設定**] > [**アラーム送信先**] ダイアログボックスで正常域アラームの抑止を設定した場合は、このアラームは送信されません。[アラーム送信先] の詳細は 134 ページの「アラームの送信」を参照してください。



上の図では、別のアラームしきい値違反が発生していますが、ウィンドウ内には違反が 2 つだけしかないので、アラームはトリガーされません。

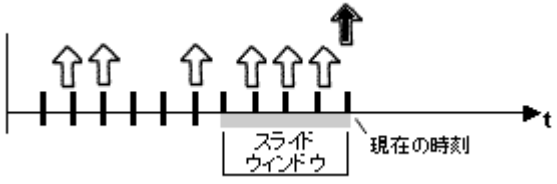


上の図では、違反が引き続き発生しています。ウィンドウ内には現在 3 つのアラームしきい値違反があるため、アラームがトリガーされます。



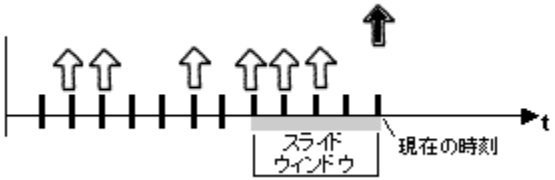
上の図では、違反が引き続き発生しています。ウィンドウ内には現在 4 つのアラームしきい値違反があり、「アラームを継続的に送信」が指定されている場合は、新しいアラームがトリガーされます。[アラームを継続的に送信] オプションは、[**ファイル**] > [**設定**] > [**アラーム送信先**] ダイアログボックスで設定します。

以下に示す 2 つの例では、ウィンドウ内で多数のアラームしきい値違反が発生している場合、アラーム状態が正常域に戻るにはしばらく時間がかかることを示しています。これは、違反がウィンドウから出るには、いくつかのサイクルを必要とするためです。つまり、3 つの違反がウィンドウ内にある限り、新しいアラームは現在時刻でトリガーされます。



上の図では、ウィンドウ内に 3 つの違反が含まれているので、現在のサンプルに違反がない場合でも、アラームがトリガーされます ([アラームを継続的に送信] がオンの場合)。

また、以下に示すように、次の間隔でもまだ 3 つの違反があるので、アラームは再びトリガーされます。スライドウィンドウがもう一度シフトすると、アラーム状態は正常域に戻ることができます。



- **[アラーム保留時間]:** 監視対象のプローブメトリック値が、短い時間予想限界値を超えても、アラームが発生しないよう指定できます。この設定を行うと、メトリックが、設定したアラーム保留時間にわたって設定しきい値を超え続けない限りアラームは発生しないため、アラームの数を減らすことができます。

  長い時間を指定すると、期間全体にわたって受信メトリック値が制限値を超えるまでアラームは発生しなくなります。デフォルトのプローブサンプリング間隔は 5 分間 (300 秒) であるため、5 分単位 (5、10、15 分など) で設定するようにしてください。ゼロを指定すると、アラームがすぐに発生します。

  [アラーム保留時間] 設定は、アラームにのみ適用されます。サービスレベル違反はこの設定に関係なくカウントされ、Internet Services ダッシュボードにレポートされます。

- **[メッセージ]:** アラームイベントの説明を入力し、アラームイベントから取得した情報を提供できます。この情報は、アラーム通知と共に NNM または OVO に送信できます。このメッセージは、アラーム定義にのみ使用され、サービスレベル目標値には何の影響も与えません。アラームイベントから取得したデータをメッセージに含めるには、特別なキーワードをメッセージに追加します。アラームメッセージに使用できるキーワードの一覧については、131 ページの「アラームメッセージ」を参照してください。

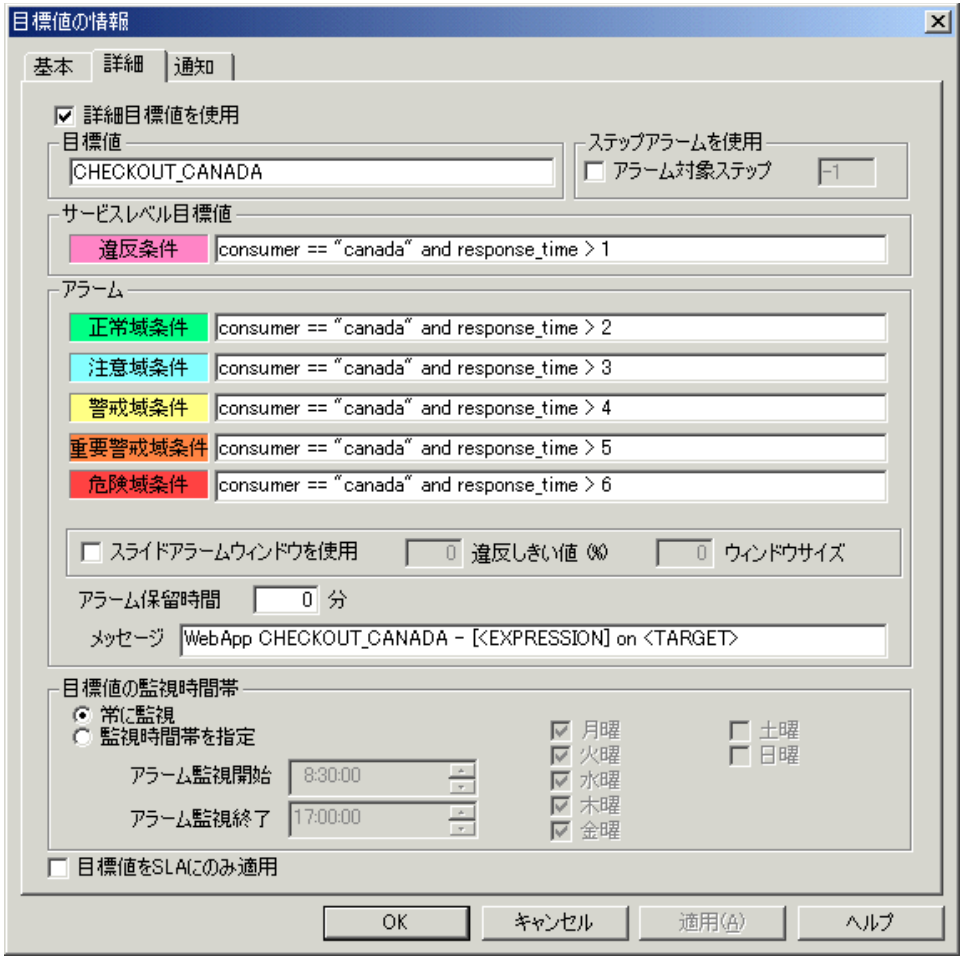
[目標値の監視時間帯] セクション :

アラーム期間をフィルターすることができます。この設定を行うと、バックアップ時のように、目標値に達しないことが予想される時間帯に不要なアラームが発生するのを防ぐことができます。

[SLA 目標値] セクション :

目標値をアラームに適用せず、サービスレベル契約 (SLA) にのみ適用する場合は、[目標値を SLA にのみ適用] ボックスをオンにします。SLA についての詳細は、「サービスレベル契約 (SLA) の設定」を参照してください。

サービスレベル目標値とアラームの詳細設定



このダイアログを使って、サービスレベル目標値 (SLO) とアラーム用の式を定義します。式は、特定のプローブの複数のメトリック (多変数の SLO/ アラーム) を組み合わせた SLO とアラームの条件を考慮します。たとえば、「response_time > 100 and transaction_rate > 10000」のような定義が可能です。主に、OVTA メトリックとともに使用されます。

式を使用するには、[目標値の情報] ダイアログで [詳細] タブに切り替えて、[詳細目標値を使用] ボックスをオンにします。定義する目標値に名前を付け、[目標値] フィールドに入力します。このラベルは OVO や NNM のような統合先に表示されます。

詳細目標値では、目標値を構成するメトリックはダッシュボードの詳細表示で色分けされません。また、詳細目標値では、メトリック値がサービスレベル目標値の範囲外の場合、結果が「true」を返すように式を記述する必要があります。たとえば、RESPONSE_TIME > 2 の場合、サービスレベル違反になるとします。詳細目標値は、基本の目標値指定の記述と、ロジックが逆になります。この場合、サービスレベルの式は RESPONSE_TIME <= 2 と記述する必要があります。

通常これらの式では、OVTA アプリケーションのパフォーマンスメトリックを使用します。メトリックについては、296 ページの「メトリックの一覧 (プローブタイプ別)」で説明しています。この一覧のメトリックは、AVAILABILITY を除き、すべて使用できます。式は、プローブが利用できる場合にのみ評価されるので、AVAILABILITY メトリックを式に追加しても意味がありません。基本目標値の Availability でも、プローブが利用不可を返す場合は、他の目標値は評価されません。

アラーム式の評価順序は、最も高い重要度 (危険域、重要警戒域、警戒域、注意域の順) から開始されます。評価がこれら重要度のいずれかに「true」を返すと、アラームがトリガーされ、その後の式はチェックされません。前回測定時のアラームの状態が正常域以外の場合は、正常域の式が最初にチェックされます。これが「true」と評価されると、アラームの状態は正常域に移行され、その他の式はチェックされません。「正常域アラームの抑止」がオフの場合は、正常域のアラームメッセージがトリガーされます。

詳細目標値にはベースライン機能はありません。スライドアラームウィンドウ機能は、指定すると、式が評価された後に適用されます。アラーム保留時間機能は最後に適用されます。

メッセージ変数 <EXPRESSION> は、アラームをトリガーした (つまり、true と評価された) 式を示すために使用できます。

このダイアログのその他のフィールドはすべて、基本目標値ダイアログと同じです。

SLO/ アラームの式の構文

構文 :

```
Variable | Relational-Operator | Constant | Factor
RESPONSE_TIME > 100 AND TRANSACTION_RATE > 10000
```

```
Boolean-Expression ::= Boolean-Term | Boolean-Term OR Boolean-Expression
Boolean-Term ::= Boolean-Negation | Boolean-Negation AND Boolean-Term
Boolean-Negation ::= Boolean-Factor | NOT Boolean-Factor
Boolean-Factor ::= ( Boolean-Expression ) | Variable | Variable Relational-
Operator  Constant
Relational-Operator ::= < | > | == | <= | >= | !=
Variable ::= OVIS Metric
Constant ::= Number | String
Number ::= Floating Point Number
String ::= "{character}+"
```

パラメータ :

変数 (Variable) - プローブタイプに固有の OVIS メトリック (OVIS メトリックは文字列か浮動小数値のいずれかです)

関係演算子 (Relational-Operator) - <, >, ==, <=, >=, != (関係演算子は、文字列を一致させる場合、大文字小文字を無視します。たとえば、“OVis” は “ovis” と同等です。

定数 (Constant) - 数値、文字列 (数値は浮動小数値、文字列は文字で引用符で括ります)

論理演算子 (Factor) - AND, OR, NOT

例 :

RESPONSE_TIME > 100 AND CONSUMER == “Probe”

RESPONSE_TIME > 100 AND TRANSACTION_RATE > 10000

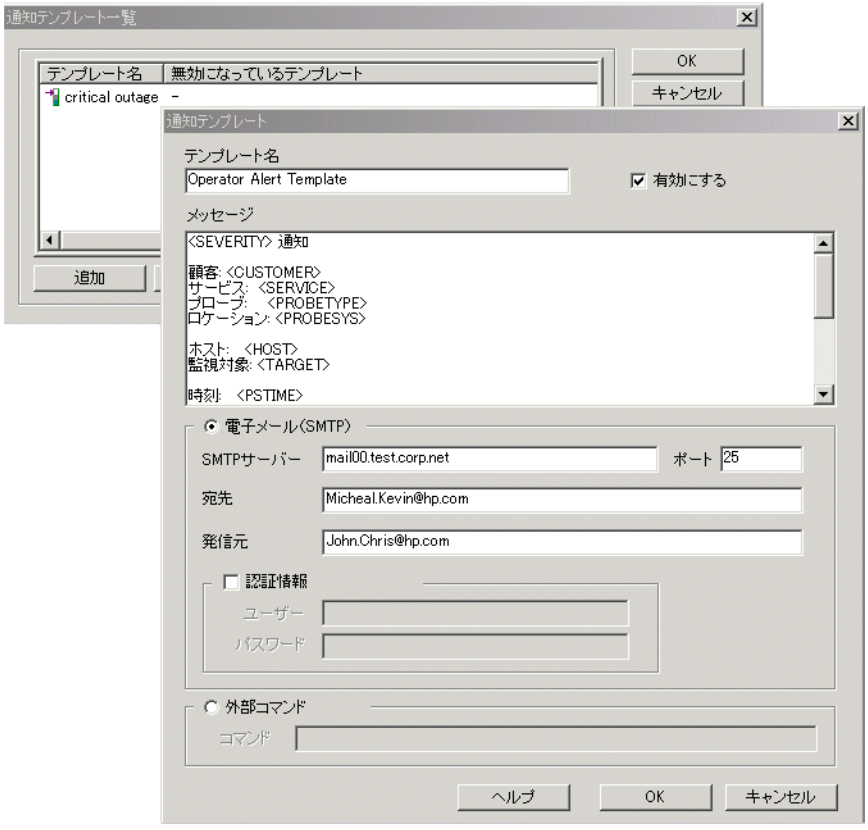
エラー処理 :

文字列と数値 (浮動小数) がサポートされています。異なる型での条件比較はエラーとなります。

通知の設定

通知用のテンプレートを作成して、アラームが発生したときに通知を行うことができます。[目標値の情報] ダイアログの [**通知**] タブを使って、通知を目標値アラームに追加します (124 ページの「目標値アラームへの通知の追加」を参照してください)。通知を追加するには、いくつかの目標値を定義する必要があります。

通知は電子メールで行うか、外部コマンドを実行します。通知テンプレートを作成するには、設定マネージャの [**ファイル**] > [**設定**] > [**通知テンプレート**] ダイアログを使用します。



電子メール (SMTP) で通知を送信するには、電子メールサーバーの情報と、電子メールを送受信する電子メールアカウントを入力します。

[認証情報] を選択すると、Microsoft Exchange Server の場合を除いて、指定したユーザー名とパスワードが SMTP サーバーに適用されます。Microsoft Exchange Server の場合は、ユーザーとパスワードは [発信元] アカウントで認証されます。

また、通知で使用するメッセージも作成できます。以下のキーワードを [メッセージ] フィールドで使用できます (これらは [目標値] ダイアログの [メッセージ] フィールドと同じ定義になります)。

<CUSTOMER>	この目標値を所有する顧客名
<SERVICE>	この目標値が属するサービスグループの名前
<PROBETYPE>	データを測定しているプローブタイプ (HTTP、ICMP、DNS など)
<PROBESYS>	プローブが実行されたシステムの名前
<HOST>	測定されたシステムの名前
<TARGET>	この目標値の監視対象サービス (URL、ホスト名など)
<PSTIME>	プローブが行った測定の時間 (書式変換済み)
<ERROR_INFO>	サーバーまたはプロトコルが返したプローブ固有のエラー情報 とプローブによりログされたエラー情報。たとえば、HTTP_TRANS プローブの場合は、エラーの発生部分、失敗したパターン、HTTP ステータスコードが表示されます。詳しくは、411 ページの「エラーメッセージとステータスコード」を参照してください。
<VALUE>	アラーム発生時のこの目標値のメトリック値

以下のキーワードは通知テンプレートでのみ使用できます。

<SEVERITY>	アラームの重要度
<METRICNAME>	メトリックの名前 (AVAILABILITY など)
<URL>	ダッシュボードへの詳細 URL
<MESSAGE>	書式変換済みアラームメッセージ

[メッセージ] フィールドで変更を行わない場合は、デフォルトのメッセージが使用されます。

以下にデフォルトメッセージの例を示します。

```
Critical Notification for

Customer: Hewlett-Packard

Service:  test http

Probe:    HTTP

Location: mylocation.hp.com

Host:   go.shop

Target: go.shop/

Time:   02/03/05 13:21:28

Metric: AVAILABILITY

Value:  0.000

Error:  [DNS Unable to resolve host (go.shop:80)] [URL] http://
go.shop:80/ [PROXY] (none)

URL:    http://mylocation.hp.com:8080/OvisDashboard/
Controller?action=login&enc=UTF-
8&LN0=All&LN1=Hewlett%2dPackard&LN2=test+http&LN3=go%2eshop/

Message:

HTTP Service for go.shop/ is unavailable ([DNS Unable to resolve
host (go.shop:80)] [URL] http://go.shop:80/ [PROXY] (none) )

Best regards,

  OVIS
```

通知テンプレートで設定するメッセージは、サービスレベル目標値のアラームが生成されたときにのみ適用されます。SLA アラームや OVIS ステータスアラームには使用されません。

外部コマンドを実行するには、[外部コマンド] チェックボックスをオンにします。**[コマンド]** テキストフィールドで置換できるパラメータは <CONTENTFILENAME> のみです。

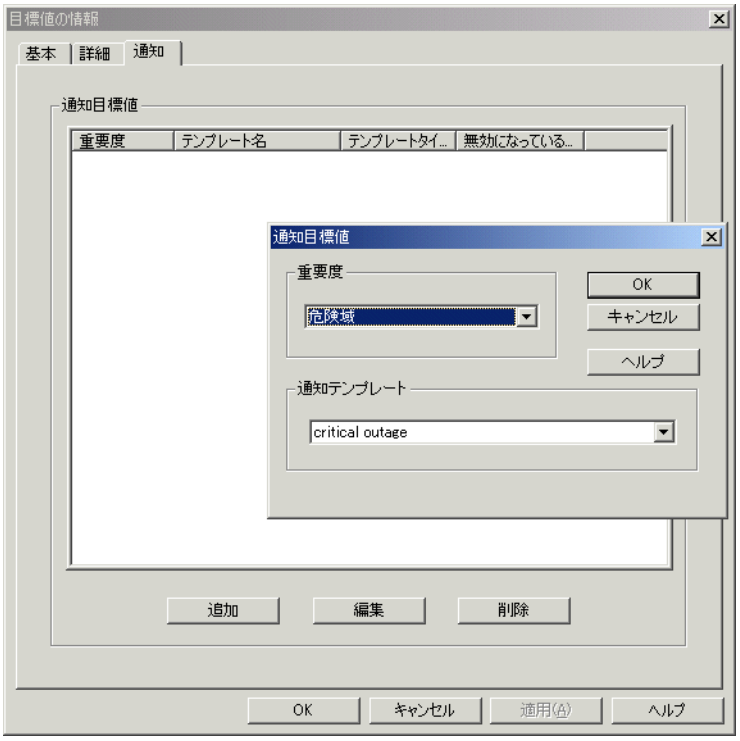
以下のテストスクリプト例は、処理後にファイルの削除を行います。

```
Set fsoObject = CreateObject("Scripting.FileSystemObject")
```

```
if Wscript.Arguments.Count <> 1 then
  Wscript.Echo "Filename expected"
  Wscript.Quit 1
end if
Rem Log the contents of the passed file
Set fLog = fsoObject.OpenTextFile("c:\\temp\\notifCmd.log", 8,
true)
Set fContentFile =
fsoObject.OpenTextFile(Wscript.Arguments.Item(0), 1)
sContent = fContentFile.ReadAll
fContentFile.close
fLog.Write sContent
fLog.close
Rem The script is responsible for deleting the passed file
fsoObject.DeleteFile(Wscript.Arguments.Item(0))
```

目標値アラームへの通知の追加

通知を送信するには、通知を目標値アラームに追加する必要があります。初めに編集する目標値 (メトリック) を選択し、続いて [目標値の情報] ダイアログで [**通知**] タブを選択します。[**追加**]、[**編集**]、[**削除**] ボタンを選択すると、通知を追加、編集したり、この目標値に設定した通知を削除できます。



その他の種類のアラーム用通知 (SLA および OVISstatus)

通知は、他の 2 つのアラーム種別である SLA アラームおよび ovisstatus アラームでも送信できます。SLA の一部である SLO に基づいてアラームに通知を設定すると、SLA アラームとしての通知メッセージも自動的に作成されます。SLA アラームの通知メッセージは、テンプレートのメッセージではなく、SLA の情報に基づきます。

例 : `SLA Conformance Threshold Violated:  SLA: "SLA Failure"`

例：`Customer: "http";  Threshold: 95.00   Conformance: 75.00.`
SLA は一時間ごとに評価され、通知付きの SLA アラームがトリガーされると、通知もこの時点で送信されます。

ovisstatus アラームの通知は、[ファイル] > [設定] > [アラーム送信先] ダイアログで設定します。使用する通知テンプレートを選択しますが、メッセージは、テンプレートのメッセージではなく、ovisstatus からの情報が使用されます。

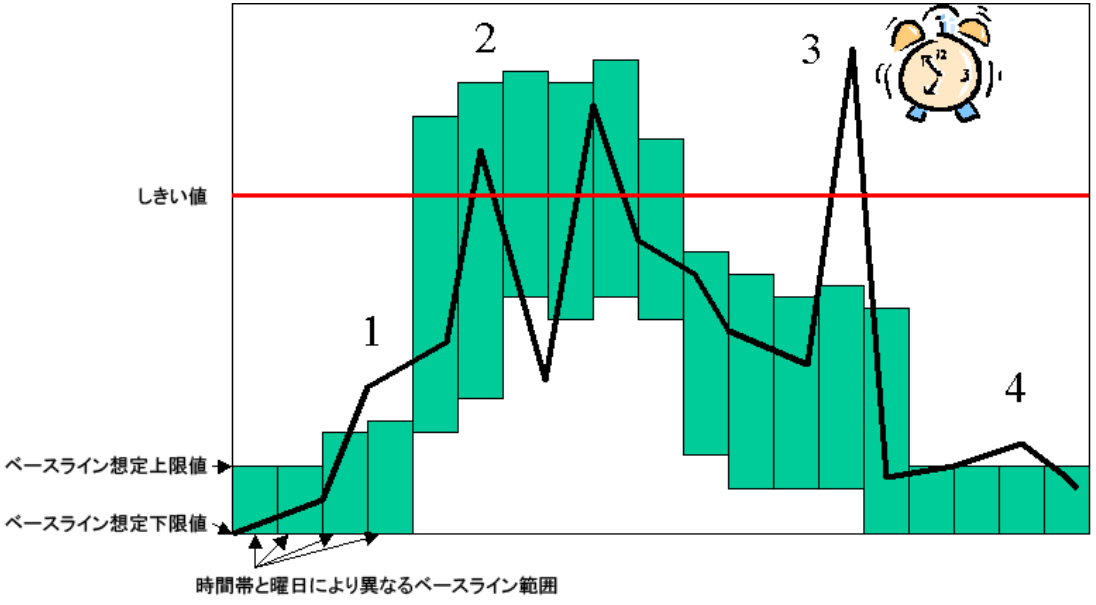
例：`Probe-Server Comm Delay:  ovruxd04.test.corp.com (09m:49s).`
ovisstatus は 5 分ごとに実行され、通知付きの ovisstatus アラームがトリガーされると、通知もその時点で送信されます。

通知テンプレートに設定されたメッセージは、サービスレベル目標値のアラームが作成されたときにのみ適用されます。SLA アラームや ovisstatus アラームには使用されません。

ベースラインの動作

ベースライン比較値は、受信プローブメトリック値を監視することで自動的に計算されます。十分な数の値が蓄積されると、メトリックの予測可能な値の範囲が確立されます。ベースラインは詳細目標値に使用できます。

アラームイベントは、各レベルの値の設定に従って発生しますが、メトリック値は固定値ではなく、ベースラインからの想定限界値 (上限または下限) に対して比較されます。[ベースライン] ダイアログボックスに設定されている値は、固定値ではありません。ベースライン値は、*正常域* (正常とみなす範囲) をどの程度厳密にするかを決定するパーセント値 (1 ～ 100) です。値は、正常域内に収まると想定されるすべてのメトリック値の割合を示します。[ベースライン] 値 80 は、全メトリック値の 80% が想定下限値と想定上限値の範囲内に収まることを示しています。同様に、80% という値は、メトリック値の 20% がベースライン範囲外になると予測していることも示しています。ベースラインに大きい値を指定すると、正常域であるとみなされるメトリック値の割合が増えるため、イベントの発生数は減少します。



上の図の例は、株取引ページの例で、応答時間のアラームしきい値は 3 秒です。月曜日の午前 10 時～午後 0 時にこの株取引ページは大量の買い注文を受け取り、ピーク期間 (上図の番号 2) になります。図中の番号 1 から 4 の期間のアラームの発生について、以下の説明を参照してください。

1. アラームイベントなし - 応答時間の値はベースラインの上にありますが、3 秒のしきい値より小さくなっています。

2. アラームイベントなし - 応答時間は 3 秒のしきい値の上にありますが、ベースラインを基準にすると、これは月曜日の午前 10 時～午後 0 時では正常域にあります。

3. アラームイベント生成 - 応答時間は 3 秒のしきい値より大きく、ベースラインの正常域の外にあり、もはやピーク時ではありません。

4. アラームイベントなし - 応答時間はベースラインの上にありますが、しきい値より小さくなります。

ベースラインの値は、以下の表のいずれかの値に調整されます。

ベースライン値	平均に対する標準偏差
50	0.6745
68.27	1.000
75	1.150
80	1.281 (デフォルト)
90	1.650
95	1.960
95.43	2.000
99	2.580
99.73	3.000
99.9	3.290
99.999	99.999

ベースライン目標値のいくつかの特別な機能を以下に示します。

- ベースラインが確立されるまでの時間は、その時々で異なります。ベースラインイベントは、現実的な予測範囲を決定するのに十分な数のメトリック値が処理されるまで無効です。受信メトリック値が比較的一定している場合、数個のメトリック値を受信したあとでベースラインが確立されます。それに

対してメトリック値が大幅に変動する場合は、現実的な予測範囲を決定するのにより多くのメトリック値が必要になります。予測の妥当性はベースラインによって判断され、予測が使用できるようになるまで目標値イベントは発生しません。

- ベースラインは、その日の時間によって変化します。アクティビティは、時間や曜日によって変化するため、ベースラインは各曜日の各時間ごとに個別の予測範囲を処理できるように計算されます。たとえば、一般的に値が低い日曜日の午前 4 時には、非常に低い値でイベントが発生します。一般的に受信メトリック値が高い月曜日の午前 9 時にイベントが発生するためにはより高い値が必要になります。
- ベースライン予測範囲は、サービスグループ間で異なります。あるサービスグループの監視対象が別のサービスグループの監視対象とは異なる値になっている場合、ベースラインフィールドに同じ値が指定されていても、それぞれのサービスグループで異なるレベルでイベントが発生します。
- サービスグループ内のすべての監視対象で 1 つのベースラインが維持されます。すべての監視対象の値は、予想されるベースライン範囲の設定に関係します。目標の評価時には、各監視対象はサービスグループのベースラインに対して個別に比較されます。

このため、サービスグループ内の監視対象は、ほぼ同じメトリック値を予想します。

注意 : テスト用途でアラームを作成する場合は、ベースラインをオフに設定してください。オンにすると、テスト対象のアラームが抑制される場合があります。

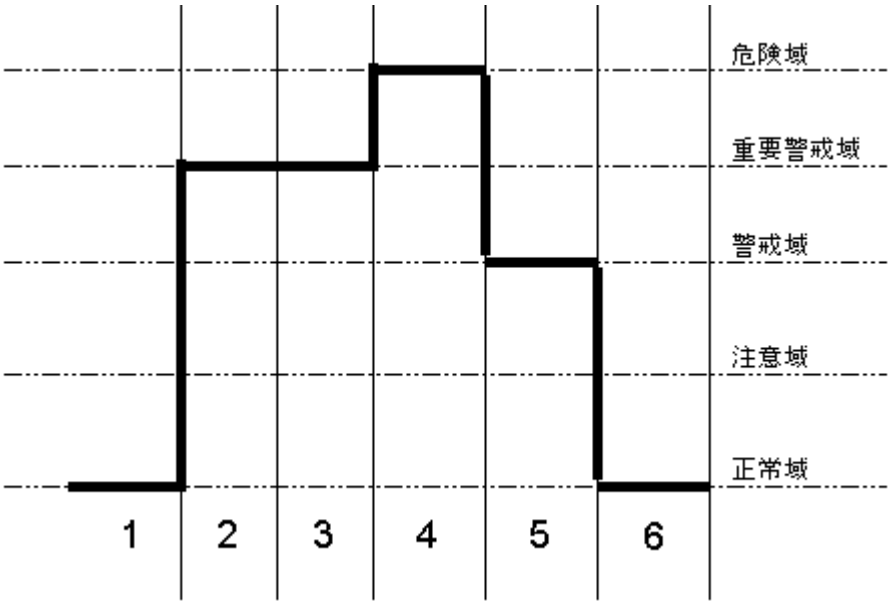
アラームのトリガー動作

ここでは、[目標値の情報] ダイアログ内の設定に従ってアラームがトリガーされるプロセスを説明します。

1. サービスグループ内の各監視対象の測定値が受信され、指定された目標値に対する評価が行われます。目標値は、監視対象ごとに、正常域の状態で開始されます。プローブから新しいデータが受信されると、そのデータは目標値の範囲と比較されます。
2. 値が正常域の範囲内にある場合は、目標値の状態は正常域のままとなり、アラームはトリガーされません。
3. **ベースラインがない場合：**アクションが発生するためには、アラーム保留時間が終了するまで受信メトリック値がしきい値を超え続ける必要があります。メトリック値がアラーム範囲 (つまり、注意域などの重要度) 内に入ると、アラーム保留時間のタイマーがリセットされます。タイマーのカウントが定義されているアラーム保留時間を超えると、目標値の状態がアラーム範囲の状態に変わります。これが、アラームイベントの「開始」(START) とみなされます。したがって、5 分の測定間隔と 5 分間のアラーム保留時間が設定されている監視対象は、連続する 2 つの測定期間にわたって制限値を超えた場合に、アラームがトリガーされます。
4. **アラーム範囲とベースラインが設定されている場合：**アラームイベントが発生するためには、プローブメトリック値が、設定されているアラームしきい値を違反し、ベースラインメトリック範囲外になっていなければなりません。メトリック値がアラーム設定を違反しているが、その時間の正常域範囲内に収まっている場合、アラームイベントは発生しません。メトリック値がベースラインからの想定範囲外であるが、アラームしきい値を超えていない場合、アラームイベントは発生しません。

   アラームの値とベースライン値の両方を設定すると、発生するイベント数は最も少なくなります。これは、メトリック値が、その値を想定していない時間帯にアラームしきい値を超えた場合だけアラームイベントが発生するためです。
5. メトリック値が前のアラーム保留時間と同じ範囲にとどまっている場合は、CONTINUED アラームイベントとみなされます。メトリック値が、指定されたアラーム保留時間内に別のアラーム範囲 (上下のどちらか) に変わった場合は、アラームイベントが新しい重要度で「開始」(START) されます。
6. メトリック値が正常域カテゴリに入ると、アラームイベントは正常域ステータスに戻ります。これがアラームイベントの「終了」(END) です。

サービスレベル目標値アラームのパスは、以下の例を参照してください。



1 正常域ステータス (アラームイベントなし)

2 重要警戒域ステータス (START イベント、severity=MAJOR を送信)

3 重要警戒域ステータス (CONTINUE イベント、severity=MAJOR を送信)

4 危険域ステータス (START イベント、severity=CRITICAL を送信)

5 警戒域ステータス (START イベント、severity=MINOR を送信)

6 正常域ステータス (END イベント、severity=NORMAL を送信)

アラームメッセージ

アラームしきい値を違反すると、アラームが発生し、状況を修正するように誰かに通知します。アラームには、重要度と追加情報のアラームメッセージを含むことができます。重要度はリストから選択し、オペレータはこれにより自分の行動を優先順位付けすることができます。アラームメッセージはアラームの内容を表します。また、アラームから取得した情報を入れることもできます。

アラームイベントから取得したデータをメッセージに含めるには、メッセージに特別なキーワードを追加します。アラームが処理されると、これらのキーワードは以下に示す情報で置き換えられます。

キーワード	置き換えられる内容
<SERVICE>	この目標値をもつサービスグループの名前
<CUSTOMER>	この目標値をもつ顧客名
<PROBETYPE>	データを測定しているプローブのタイプ (HTTP、ICMP、DNS など)
<PROBESYS>	プローブが実行されたシステムの名前
<TARGET>	この目標値の監視対象サービス (URL、ホスト名など)
<HOST>	測定されたシステムの名前
<THRESHOLD>	目標値の固定しきい値
<BASELINE>	目標値のベースラインパーセント値
<DURATION>	アラーム発生までに目標値に違反しなければならない秒数 (アラーム保留時間)
<VALUE>	アラーム発生時のメトリック値
<BASELOW>	設定された時間におけるベースライン予測範囲の下限
<BASEHIGH>	設定された時間におけるベースライン予測範囲の上限
<ERROR_INFO>	サーバーまたはプロトコルにより返されたプローブ固有のエラー情報およびプローブによりログされたエラー情報。たとえば、HTTP_TRANS プローブの場合は、エラーの発生部分、失敗したパターン、HTTP ステータスコードが表示されます。詳しくは、411 ページの「エラーメッセージとステータスコード」を参照してください。

キーワード	置き換えられる内容
<EXPRESSION>	アラームをトリガーしたアラーム式 (このプローブが式を提供している場合)
<PSTIME>	プローブにより測定値が取得された時刻 (書式済み)
<PSTS>	プローブにより測定値が取得された時刻 (1970 年 1 月 1 日の世界協定時刻 00:00:00 からの秒数)
<THRESHOLD_SW>	違反が発生したときのスライドウィンドウしきい値
<RESPONSE_TIME>	応答時間のメトリック値 (プローブが提供している場合)
<AVAILABILITY>	可用性のメトリック値 (プローブが提供している場合)
<SETUP_TIME>	セットアップ時間のメトリック値 (プローブが提供している場合)
<THRUPUT>	スループットのメトリック値 (プローブが提供している場合)
<METRIC1>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC2>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC3>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC4>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC5>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC6>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC7>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。
<METRIC8>	メトリックはプローブ固有。第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照。

たとえば、以下のメッセージ文字列の場合、

> **<PROBETYPE>** response time from **<PROBESYS>** to **<HOST>** is **<VALUE>** seconds (should be < **<THRESHOLD>** or between (**<BASELOW>** and **<BASEHIGH>**))

キーワードに値が挿入されて以下のようになります。

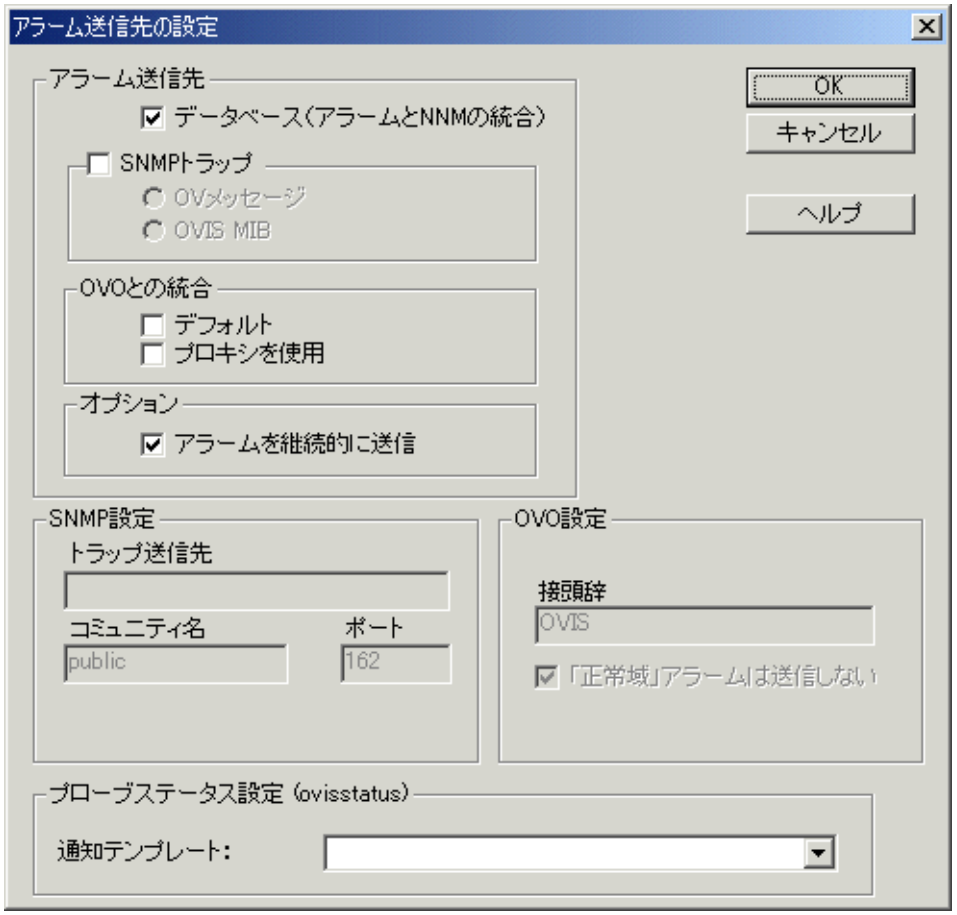
> **HTTP** response time from **curly.myhouse.com** to **webserver1.yourhouse.com** is **7** seconds (should be < **5.0** or between (**3.2** and **6.5**))

ここでは、メッセージ文字列のキーワードと、実際のメッセージで置き換えられた値を太字で示しています。

アラームの送信

Internet Services では、Network Node Manager (NNM)、OpenView Operations for UNIX、OpenView Operations for Windows、および SNMP トラップを受信するその他のイベントマネージャにアラームを送信できます。

最初に、アラームをトリガーするアラームしきい値を設定します。次に、[アラーム送信先の設定] ダイアログを使用してアラーム送信先を設定します。このダイアログにアクセスするには、設定マネージャの [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択します。



アラームを OVIS ダッシュボードに表示したい場合は、[**データベース (アラームと NNM の統合)**] チェックボックスをオンにします。

また、[**データベース (アラームと NNM の統合)**] チェックボックスをオンにすると、1 つまたは複数の NNM エージェントを使って、アラームイベントを OVIS データベースから取り出せます。Network Node Manager は OVIS 管理サーバーと同じシステム上にインストールする必要はありませんが、OVIS 管理サーバーにアクセスできるシステム上にインストールする必要があります。特別なアラームレコードが、NNM への転送や取得が可能な Internet Services EventDB に書き込まれます。Internet Services は、NNM マップのシステムアイコンにアイコンを追加して、監視されるサービスを表します。これらのアイコンの色は、対応するサービスの現在のステータスを表します。Internet Services で監視されるように設定されたサービスだけが、サービスアイコンに読み込まれます。

[**SNMP トラップ**] ボックスをオンにして、以下のいずれかを行います。

OV メッセージ : OVIS を設定して、各アラームイベントを一般 SNMP (Simple Network Management Protocol) トラップとして送信します。これは、NNM OV メッセージトラップを使用します。SNMP トラップを受信するように登録したプログラムは、このメッセージを受け取り、処理することができます。

OVIS MIB : OVIS MIB で定義された SNMP トラップを送信します。OVIS MIB は `<install dir>¥contrib` の OVIS ディレクトリにあり、SNMP 管理システムにアップロードする必要があります。

OVO 統合には、デフォルトモードを選択するか、プロキシを使います。

OVIS を OpenView Operations (OVO) または NNM と統合するには、第 5 章「OpenView 製品との統合」を参照してください。

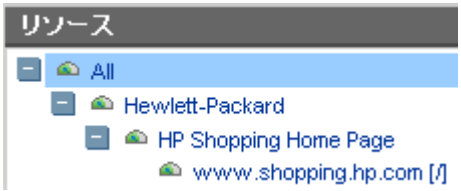
注記 : 変更を任意のサービス設定に保存すると、IIS が再起動されます。IIS が再起動すると、最後のアラーム状態が保存されます。このアラーム状態の情報は再起動時にロードし直されるため、アラーム状態は保持されます。

さらに、ovisstatus.exe プログラムが自動的に実行され、予測時間 + 10%(多少の遅れを許容する時間) 以内にデータがプローブシステムから受信されない場合は、OVO または NNM にアラームを送信します。通知テンプレートを、[通知テンプレート] フィールドを使って、これらのアラームに割り当てることができます (120 ページの「通知の設定」を参照してください)。通知は電子メールで行うかプログラムを実行します。

ダッシュボードの設定

OVIS ダッシュボード [状況] ワークスペースは、サービス状況を表示します。各項目 (顧客、サービスグループ、監視対象サービス) の横にはアイコンが表示され、サービスの稼働状況を示します。これらのアイコンのしきい値は設定マネージャでカスタマイズできます (次ページを参照してください)。

ダッシュボードの [状況] アイコンの例を以下に示します。



ステータスまたは状況は、監視対象でのサービスレベル目標値の違反率 (%) に基づきます。状況の測定方法の詳細は、137 ページの「SLO 違反に基づく状況の測定」を参照してください。アイコンは以下のように定義されます。

- 赤色アイコンは、項目のサービスレベル違反が 20 ～ 100% (デフォルト) の間にあることを示します。
- 黄色アイコンは、項目のサービスレベル違反が 10 ～ 20% (デフォルト) の間にあることを示します。
- 緑色アイコンは、項目のサービスレベル違反が 0 ～ 10% (デフォルト) の間にあることを示します。
- 青色アイコンはプローブデータを受信していないことを示します。

赤色、黄色、緑色の [状況] アイコンに対応するサービスレベル目標値の違反しきい値は、OVIS 設定マネージャの [**ファイル**] > [**設定**] > [**ダッシュボード**] で表示されるダイアログでカスタマイズできます。

このダイアログを使用して、設定マネージャのステータス表示およびダッシュボードの [監視対象ステータス] ワークスペースで表示される赤色、黄色、緑色のしきい値を設定できます。

SLO 違反に基づく状況の測定

状況 (Health) はサービス階層の上位レベルに伝達されます。上位レベル (顧客など) の状況は下位レベルの状況の平均に基づきます。

Health = 100% - SLO_VIOLATIONS(%)

SLO_VIOLATIONS(%) = (SLO 違反の数 / 測定サンプル数の合計) X 100

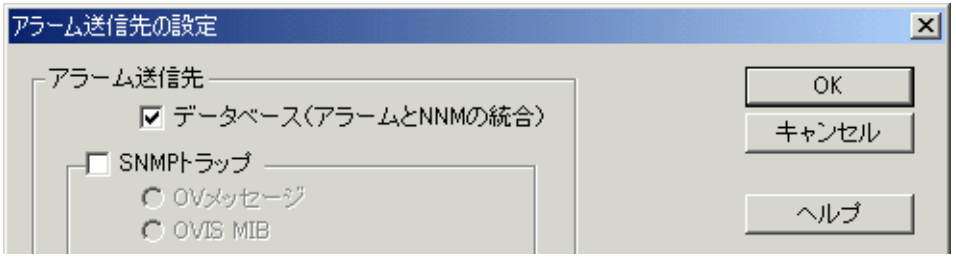
したがって、上位レベルの SLO_VIOLATIONS(%) は、下位レベルでのすべての SLO 違反の合計を下位レベル (監視対象) のすべての測定サンプル数の合計で割ったものです。また、監視対象により多くのサンプル (プローブからの有効なデータ) がある場合は、サンプルの少ない監視対象 (新しい監視対象や最近無効にされた監視対象など) に比べて状況全体により多くの影響を与えます。

状況の計算方法については、以下を参照してください。

- サービスレベル目標値 (SLO) が指定されていない場合は、[状況] アイコンは緑色になります。
- 顧客のいくつかの監視対象に SLO が定義されていない場合は、これらの監視対象はサービスグループや顧客全体の状況に対して計算されません。これは、試作生産システムやテストシステムなど、全体の状況に重要でないシステムで、プローブの測定値が必要な場合に役立ちます。
- たとえば、設定したすべての SLO が応答時間に基づく場合は、そのときの可用性は状況に反映されません。

アラームを表示するためのダッシュボードの設定

OVIS ダッシュボードにアラームを表示する場合は、設定マネージャの [ファイル] > [設定] > [アラーム送信先] で表示されるダイアログで、[**データベース (アラームと NNM の統合)**] チェックボックスをオンにします。

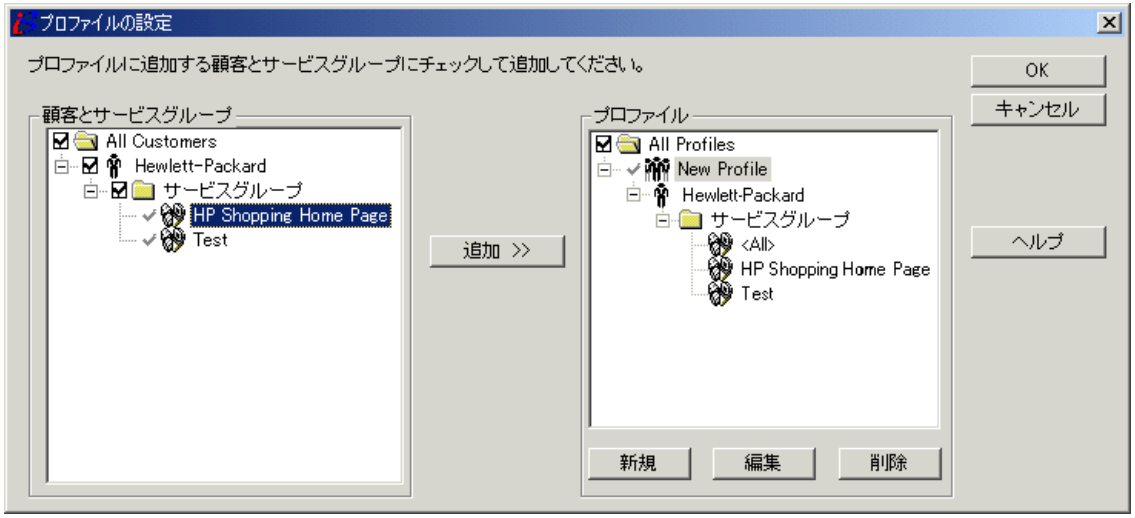


制限表示使用時のダッシュボードへのログイン

顧客やサービスグループを設定したら、オプションとして、ダッシュボード Web ページのデータ表示へのアクセスを制限できます。これを行うには、設定マネージャで [**制限表示**] を有効にしてから、各顧客を選択して顧客にパスワードを割り当てます。この設定は、設定マネージャのメインウィンドウの [**ファイル**] > [**設定**] > [**制限表示**] を順に選択して行います。[制限表示] を有効にすると、ダッシュボードへのログインでユーザー ID とパスワードを入力して、ダッシュボードのメインページを表示する必要があります。

ユーザー ID とパスワードは、顧客名とパスワードか、プロファイルとパスワードのいずれかです。[制限表示] 機能は、単一顧客のデータ表示のみに制限します。ただし、プロファイルを使用する場合には、プロファイルに複数の顧客に対するアクセスを設定したり、顧客のサービスグループを選択して、そのサービスグループのみへのアクセスを設定したり、それらを組み合わせることが可能です。

プロファイルを作成するには、[制限表示の設定] ダイアログの [**プロファイル**] ボタンを選択します。プロファイルの設定方法の詳細は、次ページの画面イメージや [プロファイルの設定] ダイアログのオンラインヘルプを参照してください。



注記 : ある顧客の一部のサービスグループのみにアクセス可能なプロファイルが設定されている場合は、ダッシュボードの [レポート] や [カスタムグラフ] にアクセスできません。これは、これらのコンポーネントが顧客別にデータを表示するためであり、またこの種のプロファイルはその顧客のすべてのデータにアクセスが許可されないためです。ある顧客のすべてのデータにアクセスできるプロファイルが設定されていて、別の顧客に対しては一部のサービスグループにしかアクセスできない場合は、[レポート] や [カスタムグラフ] にアクセスできますが、すべてのサービスグループにアクセスできる顧客のデータのみが表示可能です。

すべての顧客やレポートにアクセスできる [**All Customers**] という名前のスーパーユーザー / 管理者アカウントもあります。スーパーユーザーアカウントを使用すると、ダッシュボードにすべての顧客のデータを表示することができます。

OVIS および OpenView Performance Manager 5.0 (OVPM) を同じシステムにインストールして、[制限表示] を有効にした場合は、OVIS ダッシュボードのカスタムグラフ表示が正しく動作するように、パスワードを同期させる必要があります (388 ページの「カスタムグラフと制限表示のトラブルシューティング」を参照してください)。

デフォルトでは次の URL を使用してダッシュボードにアクセスできます。
`http://<management server>:8080/OvisDashboard`
ここで、<management server> は OVIS 管理サーバーで、"8080" はダッシュボードのポート番号です。他のシステムからダッシュボードにアクセスするには、ブラウザでこの URL を入力する必要があります。[制限表示] を有効にした場合は、表示されるログインページにユーザー ID とパスワードを入力する必要があります。

サービスレベル契約 (SLA) の設定

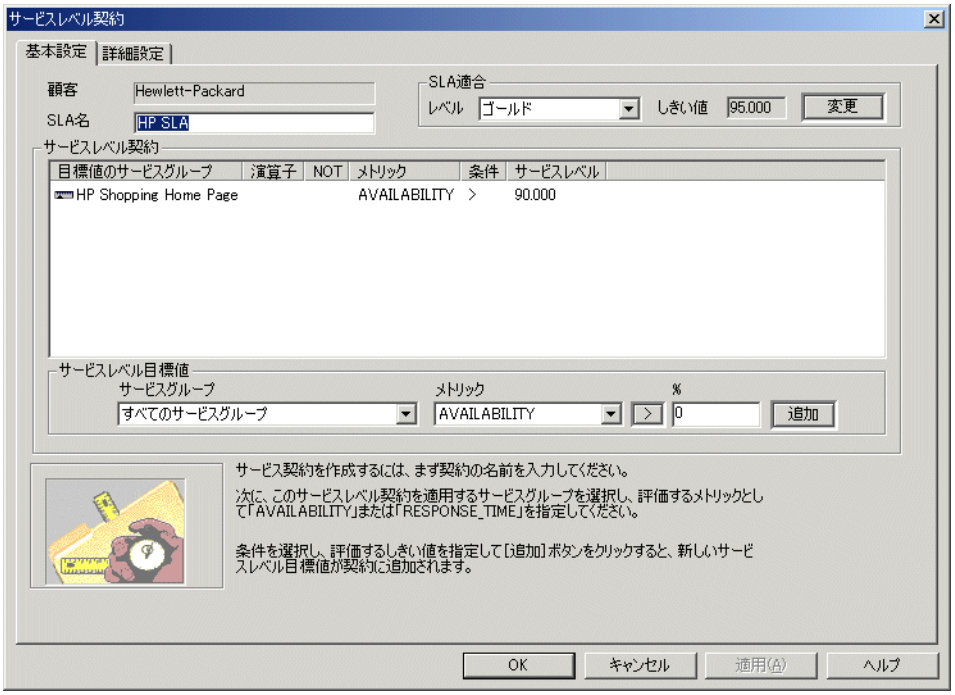
Internet Services でサービスレベル契約を構成することができます。

サービスレベル契約 (SLA) は、IT 組織と顧客間の契約に基づきます。SLA の基本概念は、複数のサービスレベル目標値 (SLO) を組み合わせて単一の SLA にすることです。各 SLO では、サービスの可用性やパフォーマンスを (応答時間などのメトリックに基づいて) 定義します。SLO の組み合わせによって、SLA が設定されている顧客に属するすべてのサービスグループを論理的に表します。

SLA は、**SLA 設定ウィザード** (設定マネージャの [**ファイル**] メニューからアクセス可能) または設定マネージャの [サービスレベル契約] ダイアログを使用して作成します。顧客のサービスグループを含む顧客用の SLA を設定します。ウィザードでは、[可用性] または [応答時間] に基づいて独自の SLA を作成する手順を案内します。

SLA を設定すると、Internet Services はサービスの可用性と契約レベルに対する適合性を追跡し、SLA 適合性に関してレポートします。

また、[サービスレベル契約] ダイアログ (SLA を右クリックして、[サービスレベル契約の編集] を選択) を使用して SLA を設定することもできます。このダイアログでは、SLA の基本設定と詳細設定があります。SLA の基本設定は、サービスレベル目標値の集まりで、全体を評価することによって SLA を形成します。SLA の詳細設定では、目標値をより複雑な論理で組み合わせることが可能で、基本設定とは別に評価されます。ウィザードでは、可用性または応答時間のいずれかで SLA の基本設定を作成する点に注意してください。SLA の設定の詳細はオンラインヘルプを参照してください。

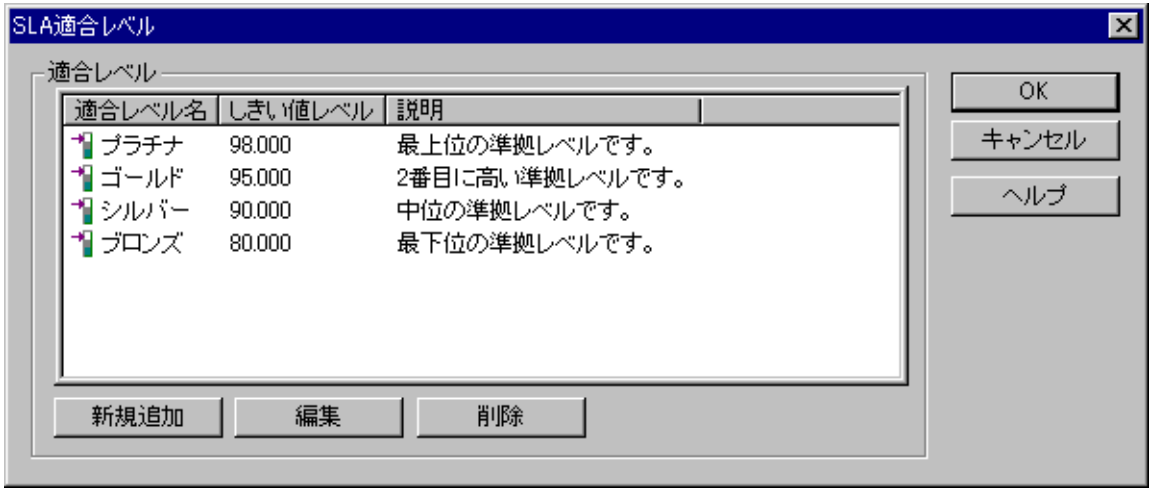


SLA の評価方法

Internet Services は、各 SLA ごとに、SLA 内の SLO を評価し、条件が満たされた割合を判断します。その結果の値を、SLA 適合といいます。たとえば、SLA に 5 つの SLO があり、1 つが SLO 違反になり他の 4 つが SLO 条件を満たした場合、SLA 適合は 80% になります。

SLA は、1 時間ごとに評価されます。基本設定の SLA の場合、ある時間に受信したすべての測定値が検査され、SLO 違反の数に対して重み付けされます。結果の SLA 適合は、ダッシュボードとレポートで表示できます。SLA の非適合に最も関係した SLO を検索することが可能なダッシュボード画面もあります。

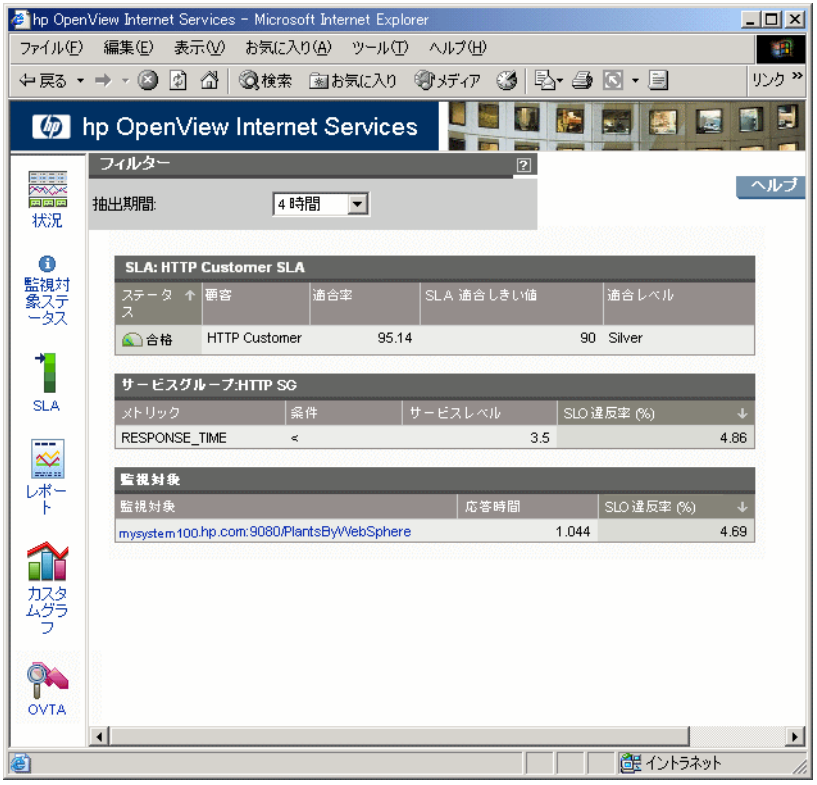
また、設定マネージャの [**ファイル**] > [**設定**] > [**SLA 適合レベル**] により、SLA 適合しきい値を設定することもできます (たとえば、プラチナ =98%、ゴールド =95%、シルバー =90%、ブロンズ =80%)。これらは、結果の SLA 適合と毎時比較されます。SLA が SLA 適合しきい値に満たない場合、この SLA パフォーマンスの問題を警告するアラームが発生します。



可用性と応答時間の、それぞれのメトリックと目標値は基本的に異なっているため、SLA を作成する場合にこれらを組み合わせてはいけません。両方のメトリックを評価するためには、2 つの個別の SLA を作成する必要があります。可用性は、SLA 全体の割合として計算されます。この場合、評価前に大量の測定値を収集する必要があります。応答時間 (および他のメトリック) は、測定値ご

とに個別に評価でき、これらの結果は 1 時間ごとに収集され評価されます。可用性と応答時間の両方のメトリックの SLA 評価が必要な場合は、可用性と応答時間の 2 つの SLA を作成します。

SLA 適合は OVIS ダッシュボードでレポートされます。メインページのワークスペースペインで、SLA アイコンを選択します。詳しくは、85 ページの「[SLA] ワークスペース」を参照してください。

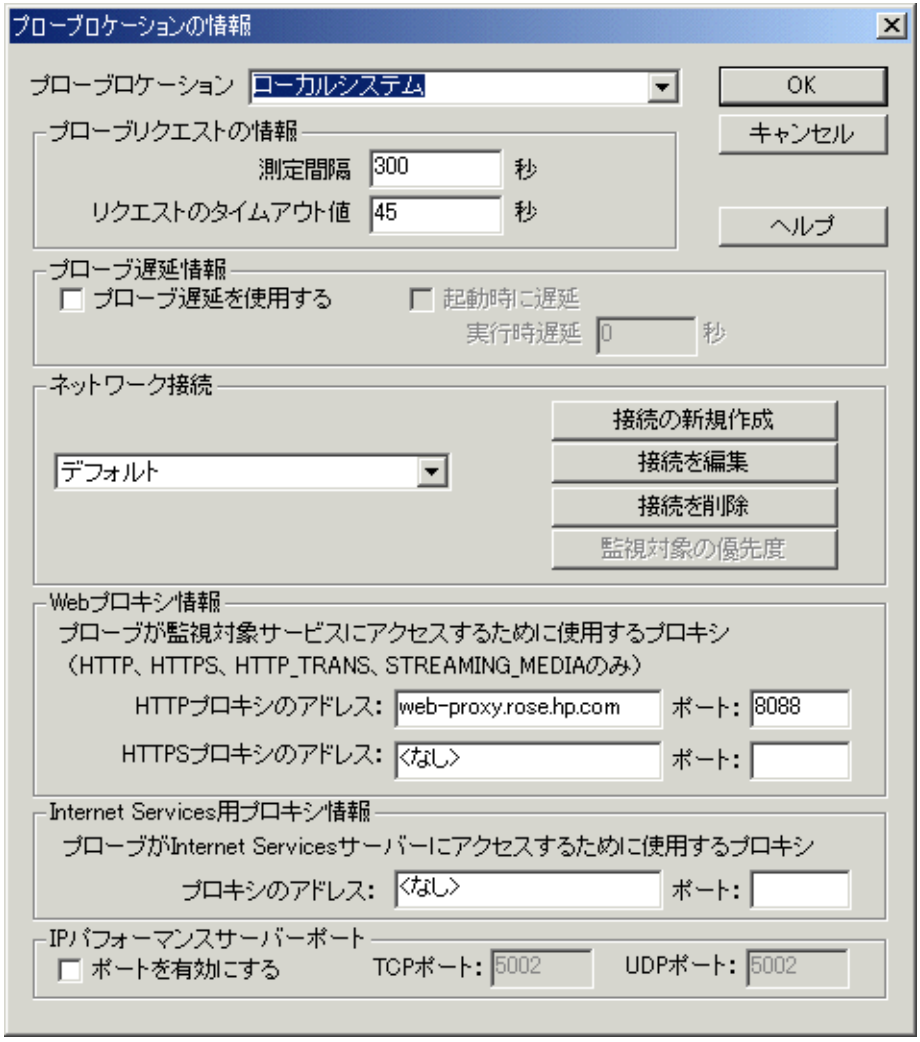


プローブのロケーション、タイミングとスケジューリング

[プローブロケーションの情報] ダイアログは、以下の設定を行うために使用します。

- プローブが実行される場所。OVTA データの場合は、ロケーションにはトランザクションを実行するマシン (Servicing Node) が含まれます。
- プローブで使用するネットワーク接続の種類
- プローブの測定を開始する頻度
- タイムアウトまでにプローブの再試行を行うタイミングと回数
- 測定をスケジューリングする場合のプローブの優先度
- スケジューラによるプローブ実行の遅延の有無
- 監視対象サービスへのアクセスやデータを管理サーバーに送り返すためにプローブに必要なプロキシ情報
- [TCP パフォーマンス] または [UDP パフォーマンス] プローブが使用するポート

プローブのタイミングとスケジューリングの設定については、512 ページの「スケーラビリティ情報」を参照してください。


プローブロケーションの情報
プローブロケーション
ローカルシステム
OK
キャンセル
ヘルプ
プローブリクエストの情報
測定間隔
300
秒
リクエストのタイムアウト値
45
秒
プローブ遅延情報
プローブ遅延を使用する
起動時に遅延
実行時遅延
0
秒
ネットワーク接続
デフォルト
接続の新規作成
接続を編集
接続を削除
監視対象の優先度
Webプロキシ情報
プローブが監視対象サービスにアクセスするために使用するプロキシ
（HTTP、HTTPS、HTTP_TRANS、STREAMING_MEDIAのみ）
HTTPプロキシのアドレス:
web-proxy.rose.hp.com
ポート:
8088
HTTPSプロキシのアドレス:
<なし>
ポート:
Internet Services用プロキシ情報
プローブがInternet Servicesサーバーにアクセスするために使用するプロキシ
プロキシのアドレス:
<なし>
ポート:
IPパフォーマンスサーバーポート
ポートを有効にする
TCPポート:
5002
UDPポート:
5002

ネットワーク接続の種類の設定

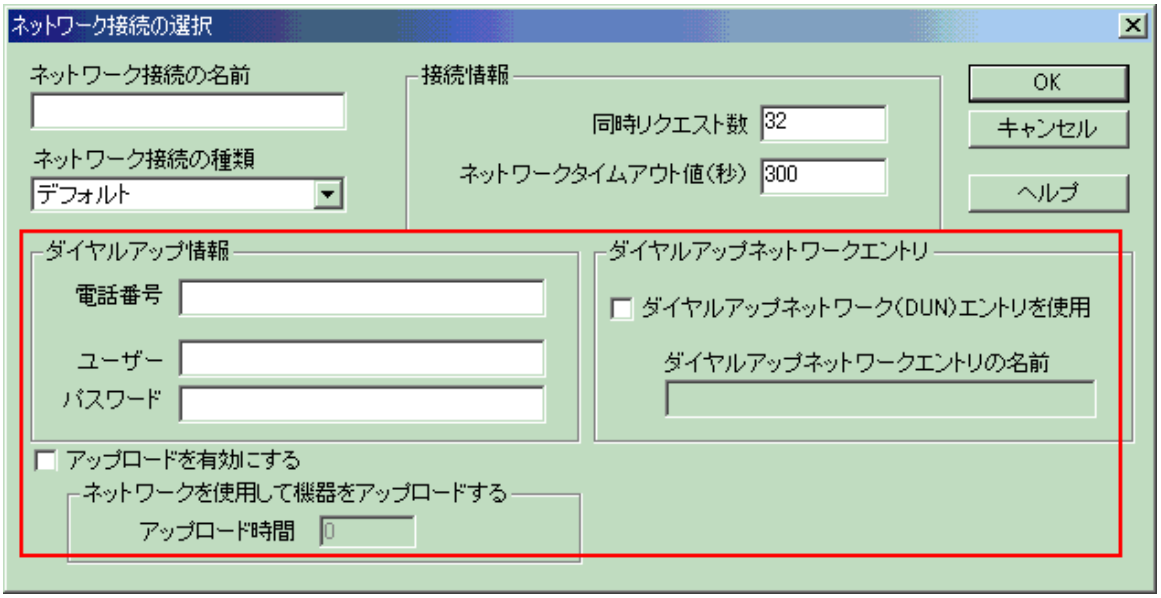
設定マネージャでプローブを設定する手順を実行していくと、プローブのネットワーク接続を設定するオプションがあります。デフォルト設定では、監視対象へ LAN 経由でプローブが接続します。ただし、[ネットワーク接続] オプションを使用して、他のネットワーク接続を設定し、各接続の同時リクエスト数を定義することができます。プローブが監視対象サービスに接続するために、ダイヤルアップを使用する場合は、[ネットワーク接続] オプションを使用してその接続を設定します。

[プローブロケーションの情報] ダイアログでは、[**接続の新規作成**]、[**接続を編集**]、[**接続を削除**] ボタンを押してネットワーク接続の追加、編集、削除を行います。

[接続の新規作成] ボタンを選択すると、[ネットワーク接続の選択] ダイアログが表示されます。このダイアログでダイヤルアップ接続の名前を指定すると、その名前が Internet Services データ表示にサービスグループ名として表示されます。

このダイアログでは、[**ネットワーク接続の種類**] (LAN またはダイヤルアップ) を選択します。

[**同時リクエスト数**] フィールドで、同時にプローブされる監視対象の数を指定します。[**ネットワークタイムアウト値**] では、ネットワークが接続状態を保つ秒数を指定します。この値は、このネットワーク接続で設定されるすべてのプローブに適用されます。これらのフィールドの詳細は、151 ページの「プローブのタイミングとスケジューリング」を参照してください。



ダイヤルアップネットワーク接続を設定するには、[ネットワーク接続の種類] で [ダイヤルアップ] を選択します。その後、ダイヤルアップ情報を直接入力するか、[ダイヤルアップネットワークエントリ] (DUN エントリ) を使用してプローブを設定します。DUN エントリは、Internet Services 以外で設定します。たとえば、Windows では、[**スタート**] > [**プログラム**] > [**アクセサリ**] でアクセス可能な、[ネットワークとダイヤルアップ接続] ウィンドウを使用します。

DUN エントリでは、より多くの設定オプションを選択でき、設定したり、接続を確認したり、プローブを再設定することなく接続設定を変更できるため、DUN エントリを使用することをお勧めします。

ダイヤルアップネットワーク接続を設定すれば、ダイヤルアッププローブが自動的に作成されます (ダイヤルアップネットワーク接続を設定したプローブと同じ [顧客] フォルダ内にダイヤルアッププローブが表示されます)。

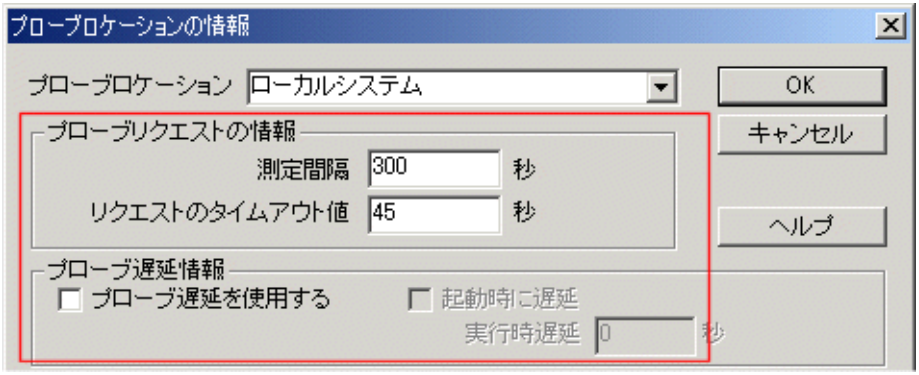
1 つのダイヤルアップ接続とログインで、複数のプローブを実行できます。[顧客] グループの下にある他のプローブでダイヤルアップ接続を使用するには、[プローブロケーション] ウィンドウを表示して、ネットワーク接続として、構成したダイヤルアップ接続を選択します。

ダイヤルアッププローブは、バックグラウンドで動作し、ダイヤルと監視対象サービスへの接続に必要な時間を追跡します。接続が正しく確立されると、このネットワーク接続に属するすべてのプローブはこの接続上で並列実行されます。

プローブデータをダイヤルアップ接続で送信するよう指定するには、[**アップロードを有効にする**] を選択します。ダイヤルアップでプローブデータを送信するために有効にできるネットワーク接続は 1 つだけで、さらにそれは Windows 上のダイヤルアップ接続でなければなりません。

プローブのタイミングとスケジューリング

スケジューラコンポーネントは、[プローブロケーションの情報] ダイアログの [**測定間隔**] フィールドで指定された間隔でプローブを実行します。



たとえば、スケジューラに対して値 300 を指定すると、スケジューラは、このサービスグループのこのプローブロケーションにあるすべての監視対象を、300 秒 (5 分) ごとに測定します。指定できる値の最小値は 60 秒です。

監視対象の測定可能時間は [**リクエストのタイムアウト値**] フィールドで指定します。リクエストのタイムアウト値はプローブタイプによって異なります。タイムアウトを超えると、監視対象が利用不可であると表示されます。

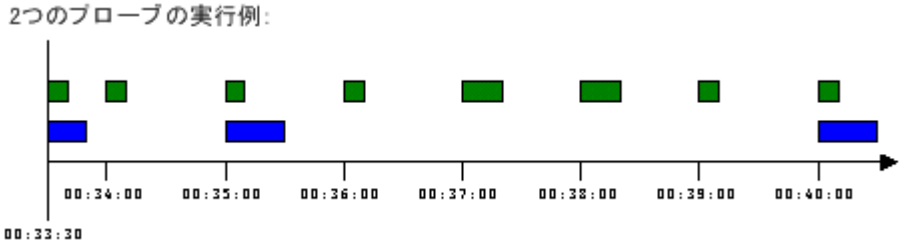
各プローブを実行する前に遅延を加えたい場合は、[**プローブ遅延を使用する**] ボックスをオンにします。遅延の秒数を入力します。デフォルトでは、これは 0 に設定され、遅延はありません。全プローブロケーションに対する最小測定間隔の 25% までの秒数を入力できます。たとえば、測定間隔が 300 秒の場合、300 秒の 25% =75 秒が最大プローブ遅延値になります。[起動時に遅延] ボックスをオンにすると、遅延は最初のプローブ実行に適用されます。

プローブは、プローブに指定したリクエストのタイムアウト値内で測定を行おうとします。プローブが測定を完了できない場合は、サービスが利用不可であると判定します。プローブがリクエストのタイムアウト値内にタイムアウトしない場合、プローブを起動したスケジューラは次の計算に従ってプローブを終了します。

(リクエストのタイムアウト値 + プローブ遅延 + (リクエストタイムアウト /3))

たとえば、20 + 5 + (20/3) = 31 秒と計算されます。これにより、指定したプローブ数が、ネットワーク接続の [同時リクエスト数] フィールドで設定した ([接続の新規作成] の選択時に定義される) もの以上にならないように同時に実行されます。このような例外ケースでは、データレコードはプローブの実行により作成されませんが、エラーはエラーログに記録されます。

プローブのスケジューラは、単一のプローブの実行を最大 10 秒まで遅らせることができます。これは、スケジューラがプローブの実行準備を確認するのに最大 10 秒かかるためです。

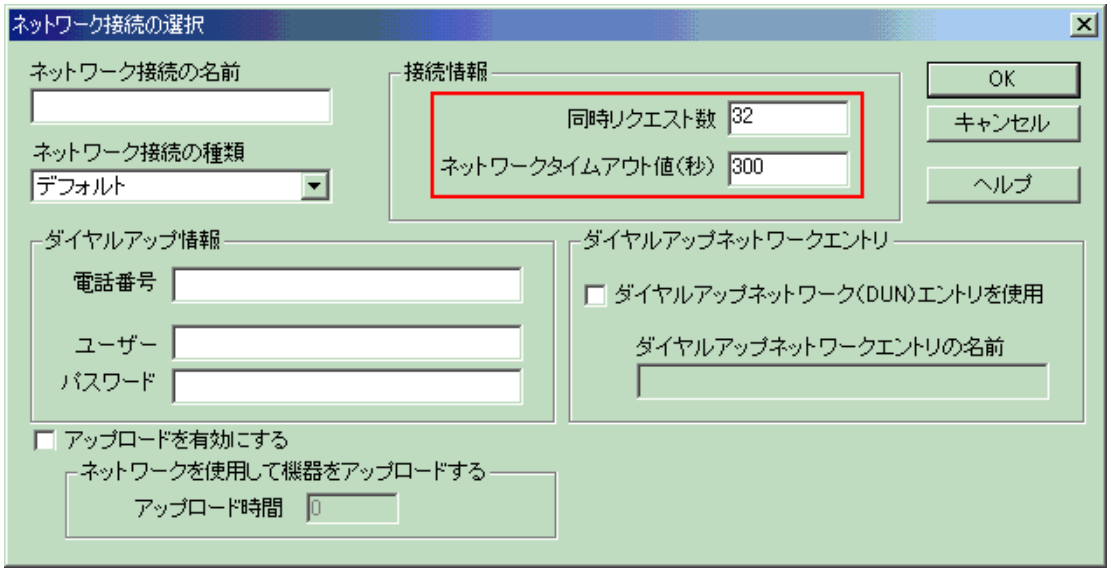


2 つのプローブの実行例 : 上の図の例では、2 つのプローブ (1 つは上の行、もう 1 つは下の行) が設定されています。上の行のプローブは、測定間隔が 60 秒、タイムアウトは 20 秒です。下の行のプローブは、測定間隔が 300 秒、タイムアウトは 30 秒です。

スケジューラを起動すると、10 秒後にプローブを実行します。上記の例では、プローブを 00:33:30 に実行します。その後、スケジューラは、測定間隔を調整します。たとえば、測定間隔が 300 秒のプローブは、毎時 xx:00:00、xx:05:00、xx:10:00、・・・、xx:55:00 (xx は任意) に実行されます。

さらにスケジューラは、1 つのプローブの実行を最大 10 秒遅延させるかもしれません。これは、プローブが実行可能な状態にあるかどうかをスケジューラが確認する時間を最大 10 秒と考えることができるためです。したがって、この例では、xx:05:00 にスケジュールされているプローブを、実際には xx:05:09 に開始する可能性があります。

同時に測定する監視対象数の設定 : 同時に測定する監視対象の数は、[ネットワーク接続の選択] ダイアログの [**同時リクエスト数**] フィールドで指定します (このダイアログには、[プローブロケーションの情報] ダイアログの [接続の新規作成]、[**接続を編集**] ボタンからアクセスできます)。



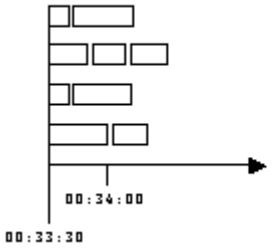
デフォルトでは、32 個の監視対象が同時に測定されます。この同時リクエスト数のパラメータは、プローブタイプ、ネットワーク帯域幅、システムパフォーマンスに依存します。詳細は、512 ページの「スケーラビリティ情報」を参照してください。

HTTP_TRANS プローブは、他のプローブより多くのシステムリソースを使用します。このパラメータで、このプローブタイプの並列実行数を制限できます。このプローブタイプには 1 ～ 10 の同時リクエスト数 ([プローブロケーション] ダイアログボックスで設定) が最適です。詳しくは、512 ページの「スケーラビリティ情報」を参照してください。

ネットワークタイムアウトでは、ネットワーク接続を確立しておく必要のある秒数を指定します。この値は、このネットワーク接続に設定されたすべてのプローブに適用されます。ネットワークタイムアウトには、この接続を使用するすべてのプローブがこの時間内に実行を完了できる十分な時間を設定する必要があります。設定する値は、同時に実行するプローブの数と各プローブのタイムアウトの値に依存します。プローブの実行がネットワークタイムアウトの値を超える場合、OVIS スケジューラは実行していないプローブを延期します。この場合、スケジューラは error.log に警告メッセージを記録します。

ダイヤルアップ接続のデフォルトのネットワークタイムアウトは、300 秒に設定されています。

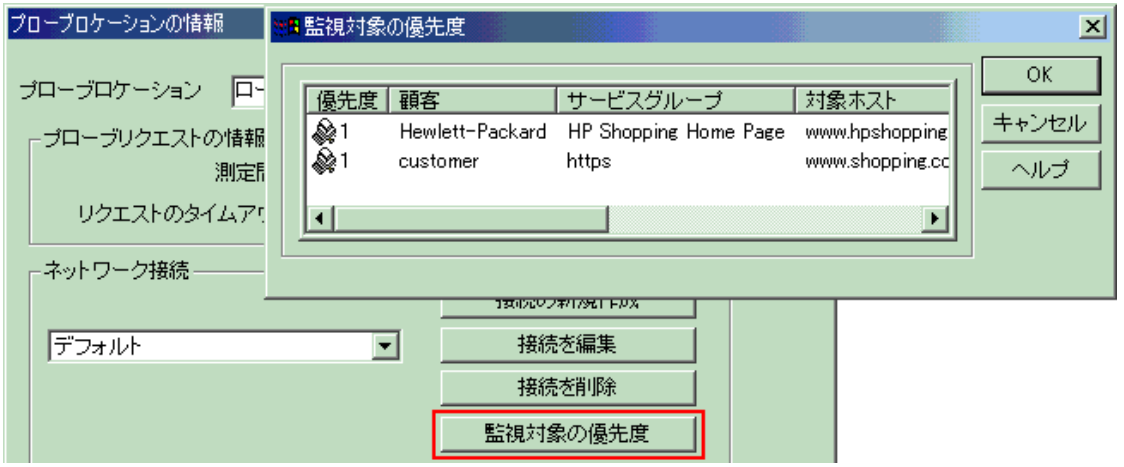
同時リクエスト 数4の9個のプローブの実行例:



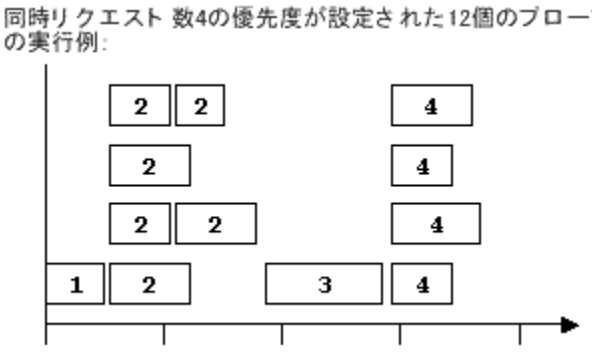
この例では、スケジューラによってプローブの同時リクエスト数が 4 に制限されています。プローブの測定間隔は、結果的に同時リクエスト数とタイムアウトのパラメータによって決まります。たとえば、監視対象のタイムアウトが 40 秒の場合は、64 個の監視対象について、同時リクエスト数を 32 として 60 秒ごとにプローブをスケジュールすることは不可能です。64 個の監視対象すべてがタイムアウトになるという最悪の場合に、すべてのプローブの総実行時間が 40 秒 +40 秒 =80 秒となり、測定間隔の 60 秒を超えてしまうためです。

プローブをスケジューリングする場合の監視対象の優先度の設定 : 監視対象の実行***優先度***を設定できます。これは、たとえば、HTTP_TRANS プローブを実行している間は他のプローブを同時実行しないようにする場合や、特定のタイプのプローブを最初に実行する必要がある場合など、負荷を分散するという意味で役立ちます。優先度を指定しなければ、プローブは同時リクエスト数の設定に基づいて実行されます。それでも実行順序が決まらない場合は設定順に実行されます。

プローブの優先度を指定するには、設定マネージャの [プローブロケーションの情報] ダイアログで [**監視対象の優先度**] ボタンをクリックします。



[監視対象の優先度] ダイアログには、このプローブロケーションに対して指定されたすべての監視対象と、OVIS で定義されたネットワーク接続が一覧表示されます。監視対象に関連付けられた優先度の値が小さいほど、その監視対象の測定順序は早くなります。複数の監視対象の優先度が同じ場合は、それらの監視対象は指定された同時リクエスト数の範囲内で同時に実行されます。



この例では、優先度 1 の監視対象が最初に測定され、次に優先度 2 のすべての監視対象が測定されます。優先度 2 の監視対象の測定がすべて完了すると、続いて優先度 3 の監視対象の測定が行われます。優先度 3 の監視対象の測定が完了すると、優先度 4 のすべての監視対象が測定されます。

デフォルトの優先度は 1 ですが、[監視対象の優先度] ダイアログで変更できます。通常は、優先度を使用すると、すべてのプローブの実行にかかる時間が長くなります。測定間隔を指定する際には、この点を計算に入れる必要があります。優先度を変更した後に新しい監視対象を追加すると、その監視対象には最も高い優先度が適用されます。たとえば、最高の優先度の値が 3 であれば、追加した監視対象の優先度も 3 になります。

ダイヤルアップ接続と LAN 接続 : ダイヤルアップ接続でプローブを実行するには、ネットワーク接続を設定します。DUN、ユーザー名、パスワード、電話番号などのダイヤルアップパラメータは、[ネットワーク接続の選択] ダイアログで入力できます。デフォルトのネットワークでは、LAN 経由でプローブが実行されます。

通常は、設定する必要があるネットワーク接続は 1 つまたは 2 つです。

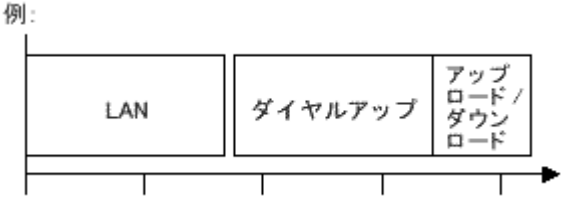
組み合わせは次のとおりです。

- LAN
- ダイヤルアップ
- LAN とダイヤルアップ

LAN とダイヤルアップを組み合わせると、LAN 経由でプローブを実行し、測定値のアップロードと設定のダウンロードはダイヤルアップ接続経由で行うことができます。

ダイヤルアップ経由の測定データ : スケジューラは、新しい設定を定期的にチェックし、キューディレクトリに保存されている測定値をアップロードします。この動作を変更して、すべての監視対象を測定した後に、特定のネットワークを使用して、新しい設定のダウンロードと測定値のアップロードを行うようにできます。このようにするには、[ネットワーク接続の選択] ダイアログの [**アップロードを有効にする**] チェックボックスをオンにします。これにより、スケジューラは、確立されたダイヤルアップ接続を使用してサーバーと通信できるようになります。

例:



この例では、デフォルトの LAN ネットワーク接続に関連付けられたすべての監視対象が実行されます。次に、ダイヤルアップネットワークが確立され、そのダイヤルアップネットワーク接続に関連付けられたすべての監視対象が実行されます。すべての監視対象の実行が終了すると、ダイヤルアップ接続経由で新しい設定のダウンロードと測定値のアップロードが行われます。

サーバーとの通信の最大秒数を、[ネットワーク接続の選択] ダイアログで指定できます。デフォルトは 10 秒です。この秒数は、測定値を生成する監視対象の数に応じて調整する必要があります。さらに、他のネットワークで監視対象の実行またはサーバーとの通信が続いている最中に監視対象が実行可能にならないよう、測定間隔を設定する必要があります。

また、いったんタイムアウトに達したら新しいプローブが実行されないようにネットワークタイムアウトを指定することも可能です。

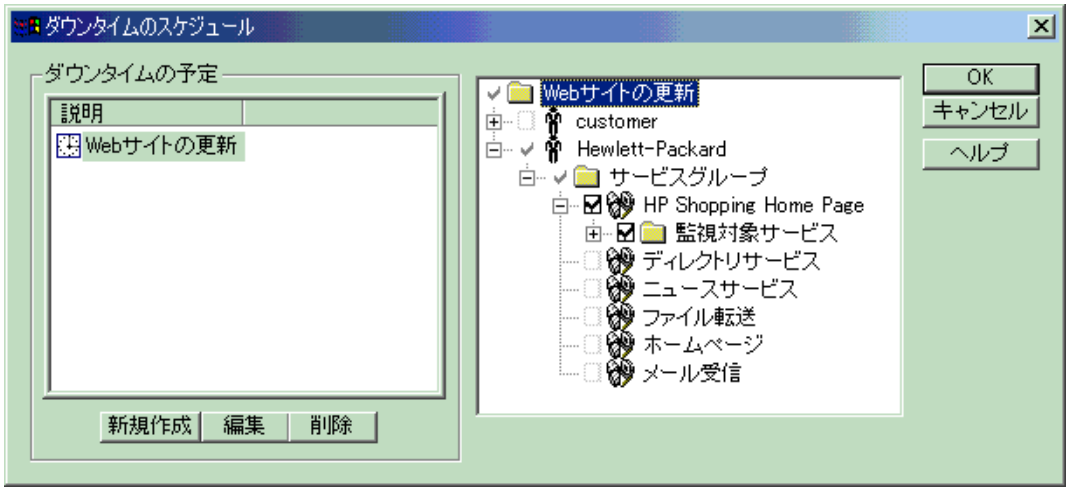
次の点に注意する必要があります。

- 分単位の境目に当たらない奇数の測定間隔 (たとえば「71 秒」) も同様に使用できますが、次に示す何らかの影響が考えられます。
  - 測定間隔が 5 分の倍数 (300 秒、600 秒など) 以外の場合は、HTTP_TRANS プローブに対して Cookie の「無効化」ができない可能性があります。
  - LAN とダイヤルアップが混在するネットワーク構成では、ダイヤルアップ中に LAN でプローブが実行される場合があります。
  - 測定間隔が 5 分の倍数 (300 秒、600 秒など) 以外の場合は、プローブの順序は保証されません。
- ネットワークタイムアウトが小さいと、プローブを開始できない可能性があります。
- 測定値の数が膨大な場合に、サーバー通信で使用されるダイヤルアップ接続が、バッファされた測定値に「追いつかない」可能性があります。その場合は、常に十分な通信時間を確保し、測定間隔を大きくします (たとえば、10 分)。

ダウンタイムのスケジュールの設定

プローブのダウンタイムのスケジュールを設定して、特定の時間帯に測定値が収集されないようにすることができます。

ダウンタイムを設定するには、[**ファイル**] > [**設定**] > [**ダウンタイムのスケジュール**] メニューを選択します。ダウンタイムを設定し、選択したダウンタイムをサービスツリー内の各項目 (顧客、サービスグループ、監視対象サービスなど) に適用できます。



[ダウンタイムのスケジュール] ダイアログで、ダウンタイムを作成する場合は [**新規作成**] ボタン、既存のダウンタイムを編集する場合は [**編集**] ボタン、既存のダウンタイムを削除する場合は [**削除**] ボタンを使用します。

[**新規作成**] ボタンまたは [**編集**] ボタンをクリックすると、[ダウンタイムスケジュールの項目] ダイアログが表示されます。ここで、ダウンタイムの [時間] と [日付] を入力します。ダウンタイムの [定期的なスケジュール] も設定できます。ダウンタイムの基本形式には、単発のダウンタイムと定期的なダウンタイムの 2 種類があります。単発のダウンタイムは特定の日時に適用されます。定期的なダウンタイムは、特定の時間帯に定期的に適用されます (たとえば、毎日 0:00 ～ 1:00)。

ダウンタイムを作成したら、次の手順に従って、個々の項目に対してダウンタイムをスケジュールできます。

1 リストからダウンタイムを選択し、[ダウンタイムのスケジュール] ダイアログの右ペインでツリーの各項目 (顧客、サービスグループ、または監視対象) のチェックボックスをオンにします。チェックマークは、ダウンタイムが適用されたことを示します。各項目に適用されたダウンタイムのみが有効になります。

2 ダウンタイムをグローバルに (テンプレートとして) 適用することもできます。その場合は、右ペインのツリー最上位のダウンタイムの横にあるチェックボックスをオンにします。チェックボックスをオンにすると、このダウンタイムをグローバルテンプレートにするかどうかを確認するメッセージが表示されます。[**はい**] をクリックすると、このダウンタイムがすべての顧客、サービスグループ、および監視対象サービスにグローバルに適用されます。グローバルに適用しない場合は、[**いいえ**] をクリックします。

   グローバルダウンタイムテンプレートを使用すると、新しく追加するすべての監視対象サービスに対して、このダウンタイムが自動的に適用されます。

   また、グローバルダウンタイムテンプレートを使用した場合は、ツリーで各項目のダウンタイムのチェックマークを個別にオン / オフにすることはできません。

   多数の監視対象を設定している場合は、ダウンタイムを個別に適用するよりも、グローバルダウンタイムテンプレートを使用する方が、パフォーマンスの点で有利です。

3 監視対象サービス、サービスグループ、または顧客に適用されているダウンタイムを確認するには、設定マネージャのメインビューに戻ります。左ペインで項目を選択すると、この項目に関する情報が右ペインに表示されます。この項目のダウンタイムのスケジュールを表示するには、右ペインで [ダウンタイム] タブを選択します。その項目が現在ダウンしている場合は、現在のダウンタイムが青く強調表示されます。また、[ダウンタイム] タブで右クリックして [ダウンタイムの設定] を選択し、ダウンタイム設定を変更することもできます。

ダウンタイムは、他の顧客、サービスグループ、監視対象サービスにも適用できます。

特殊なケースとして「常にダウン」という設定が可能です。「**Disable - Downtime 24/7**」というダウンタイムスケジュールを作成します。これは、開始時間が 0:00:00、終了時間が 23:59:59 のダウンタイムです。このダウンタイムを

作成しておくと、すべてのサービスグループとそのプローブに適用できます。これは、サービスグループ内のプローブが常時実行されない状態になります。ダウンタイムは深夜 0 時にまたがる時間帯にも適用できます。

プローブの動作

設定ウィザードを利用すれば、さまざまな監視対象サービスのプローブを簡単に設定できます。しかし、監視対象プローブがどのように動作するかを理解し、設定ウィザードでプローブに割り当てられているデフォルト設定を了承または変更する際に、何を考慮すべきかを知ることは重要です。各プローブタイプについての詳細は、第 4 章「サービスタイプとプローブの説明」を参照してください。

プローブは、サービスを使用しているユーザーを、エミュレートしようとします。また、サービスの可用性を確認し、特定のサービスプロトコル特性を測定します。たとえば、HTTP プローブは、Web サーバーから Web ページを要求し、設定時間 (ホスト名解決とサーバー接続時間) と、要求を処理するための合計応答時間を測定 (他のプロトコルでの処理時間を含む) します。スループットは、交換されたバイト数とそれらの転送時間から計算されます。

プロトコルステップの各測定値 (ホスト名解決と接続時間など) は、ボトルネックを特定したり、トラブルシューティングに役立ちます。たとえば、応答時間の大半が名前解決で使用されている場合、ネームサーバー (DNS) に問題がある可能性があります。

監視対象サービスの可用性の判断方法

プローブによる判断方法

指定したタイムアウトまでにプローブがすべての操作を完了すれば、監視対象サービスは利用可能とみなされます。たとえば、45 秒のタイムアウトまでに Web ページのダウンロードを完了しなかった場合、その測定間隔での可用性は 0% です。一部のページだけがダウンロードされた場合も、可用性は 0% です。

注記 : 何らかの理由でプローブがデータを Internet Services 管理サーバーに送信できなかった場合、プローブは管理サーバーに接続できるまでデータをキューファイルに入れます。この接続が確立されると、キューファイルからデータが処理されます。この処理が実行されるまで、管理サーバーの設定マネージャの [ステータス] ビューにはプローブシステムからの**「プローブの情報がありません」**とレポートされます (**「利用不可」**であるとはレポートされません)。

Web トランザクションで、いずれかのステップが利用不可である場合、トランザクション全体が利用不可になります。

管理サーバーによる判別方法

サービスグループに複数の監視対象サービスがある場合、可用性はデータ内のサービスの数で計算されます。たとえば、サービスグループに 5 つのサービスがあり、ある測定間隔で 4 つが利用可能で、1 つが利用不可の場合、サービスグループのその測定間隔での可用性は 80% になります。

1 つのサービスグループの中のある監視対象サービスが、4 つの異なる場所から測定された場合、そのサービスグループの可用性は、各サービスの可用性の合計をサービス数で除算した値になります。つまり、サービスが、4 つのプローブサイトの 2 つのサイトから利用可能な場合、サービスグループの可用性は 50% であるとみなされます。

TIPs の設定と使用

OVIS ではいくつかのカスタマイズせずに使用できる Troubleshooting Insight Packages (TIPs) を提供します。これらの TIPs を使用すると、サービスやインフラストラクチャの問題を素早くトラブルシューティングすることができます。ダッシュボードでは、特定の監視対象サービスやアラーム条件と結び付けられた任意の TIPs を実行できます (監視対象やアラームとともに表示される TIPs  アイコンを選択します)。

選択した TIP の実行時には、定義されたコマンド条件を満たすそれぞれの TIP コマンドがプローブシステムで自動的に実行され、トラブルシューティング情報が収集されます。コマンド結果はダッシュボードの TIPs Viewer に表示されます。

OVIS で提供される TIPs やトラブルシューティングコマンドの一部は、オーバーヘッドを回避するため、自動的に実行するようには設定されていません。これらの TIPs をご使用の環境で実行するように設定するには、既存の TIPs やコマンドを編集するか、新しい TIPs やコマンドを定義します。これには、TIPs Configuration プログラムを使用します。

TIPs Configuration プログラムには、[**スタート**] > [**プログラム**] > [**HP OpenView**] > [**TIPs**] > [**TIPs Configuration**] によりアクセスします。以下の処理を行うことができます。

- 種々のオペレーティングシステムそれぞれに対応するトラブルシューティングコマンドを作成する。
- 特定の TIP を実行する場合の条件を定義する。
- 特定のコマンドを実行する場合の条件を定義する。
- コマンドの実行結果の確認に使用する情報を指定する。
- トラブルシューティング結果を素早く評価するためのプレゼンテーションルールを指定する。
- 問題が報告された時点で自動的に情報を収集するよう TIPs を設定する。

TIPs Configuration プログラムの使い方を手順を追って説明する使用例については、TIPs Configuration オンラインヘルプを参照してください。

また、CD やインストールディレクトリ
`<install dir>¥help¥iops¥c¥ovis60-tips.pdf` の『新機能 - OVIS Troubleshooting Insight Packages』も参照してください。

TIPs の使い方の例

TIP を起動するには、以下の 2 つの方法があります。

1 オンデマンド - TIP 条件を満たす監視対象サービスやアラームでは、OVIS ダッシュボードの TIPs アイコンを選択すると、TIP をオンデマンドで実行できます。オンデマンドで実行された TIP 結果は、ダッシュボードの TIPs Viewer に表示されますが、保存されません。

2 アラームトリガード - アラームトリガード TIP は、指定されたアラームが発生すると実行されます。アラームトリガード TIP は TIPs Configuration プログラムで設定できます。アラームトリガード TIP データは TIPs データベースに保存され、後で同じ TIP をオンデマンドで実行して比較することができます。アラームトリガード TIP によって生成されたデータは、その TIP コマンドが TIP 設定から削除されるか、TIP の実行条件がデータソースになくなるまで、保存されます。

実行されたそれぞれの TIP 結果は、ダッシュボードの TIPs Viewer に表示されます。アラームトリガード TIP データは、TIP を起動したアラームのコンテキストに従って表示されます。アラームの発生時に収集されたデータは、TIPs Viewer の Triggered by Alarm に表示されます。

監視対象サービスそれぞれに、使用する TIPs の条件を定義して、適切な TIPs を監視対象サービスのトラブルシューティングに使用できます。これらの TIPs はオンデマンドで実行されます。

オンデマンドの TIP の例

オンデマンドの TIP の例を以下に示します。

IE モードを使って Web Transaction Recorder (HTTP_TRANS) のプローブを設定して、Web サーバーをモニタリングしているとします。ダッシュボードで、このプローブの関連する監視対象サービスに赤色の [状況] アイコンが表示されたとします。監視対象サービスの [要約] ページに移動して、TIPs アイコンを選択します。TIPs Viewer が表示され、Monitored Service Status TIP が実行されます。この TIP ではエラーログファイルと、Web Transaction Recorder のプローブにより取得されたエラー画面を表示します。この情報により、Web サーバーの現在の状態をトラブルシューティングして、Web サーバーの修復方法を見つけることができます。

それぞれのアラームに使用する TIPs の条件を定義して、適切な TIPs をアラームのトラブルシューティングに使用できます。これらの TIPs はオンデマンドで実行するか、アラーム発生時に実行するように設定できます。

アラームトリガード TIP の例

アラームトリガード TIP の例を以下に示します。

ネットワークで重要なドメインサーバーに対して、プローブ (DNS) を設定して、このサーバーの DNS アクティビティをモニタリングしているとします。ダッシュボードで、このプローブの監視対象サービスに黄色の [状況] アイコンが表示されたとします。監視対象サービスの [アラーム] ページに移動して、対象アラームの TIPs アイコンを選択します。TIPs Viewer が表示され、Target Network Status TIP が実行されます。この TIP は、ドメインサーバーに対する `nslookup`、`traceroute`、および `ping` コマンドの結果を表示します。これらの情報により、ドメインサーバーの現在の状態をトラブルシューティングして、ドメインサーバーの修復方法を見つけることができます。

ドメインサーバーの可用性がより危険な状態になった場合、アラームが発生した時点のネットワークの状態がどうであったかを知る必要があります。TIPs Configuration プログラムを使って、アラームが発生したときに Target Network Status TIP が起動されるように設定します。TIPs 設定を保存します。時間が経過し、ダッシュボードで、ドメインサーバーの監視対象サービスが危険域アラームをレポートした旨の警告を受けたとします。監視対象サービスの [アラーム] ページに移動して、危険域アラームの TIPs アイコンを選択します。TIPs Viewer が表示され、Target Network Status TIP が実行されます。このときには、TIP は、アラームが発生した時点で収集された `nslookup`、`traceroute`、および `ping` コマンドの結果を表示します。TIPs Viewer で、この TIP を再実行すると、ドメインサーバーの現在のネットワーク状態を表示できます。また、アラームが発生した時点のネットワーク状態の情報に再び切り替えることができます。この情報により、アラーム発生時のドメインサーバーの状態と現在の状態を対比して、トラブルシューティングを行うことができます。

TIP 定義をアラームトリガードに変更する方法については、TIPs Configuration プログラムのオンラインヘルプを参照してください。

デフォルトの TIPs

OVIS には、単独のコマンドやコマンドのグループを実行するいくつかの TIPs が付属しています。新しい TIPs や新しいコマンドを作成して、ご使用の環境のトラブルシューティング要求に対応できます。TIPs Configuration プログラムの使い方を手順を追って説明する使用例 については、TIPs Configuration のオンラインヘルプを参照してください。

以下の TIPs は、ご使用の環境で動作するように自動的に設定されます。

- Probe Re-Execution TIP
- Monitored Service Status TIP
- Target Network Status TIP

以下の TIPs をご使用の環境で動作させるには、設定作業を行う必要があります。

- Probe Network Status TIP
- Probe Resources TIP
- Probe Status TIP
- Probe OpenView Status TIP
- TIPs Runner Status TIP

これら OVIS の TIPs の詳細については、TIPs Viewer のオンラインヘルプを参照してください。また、ご使用の環境で動作するように TIPs を設定するには、TIPs Configuration プログラムのオンラインヘルプを参照してください。

OVIS には、いくつかの TIPs コマンドが付属しています。各コマンドは任意の数の TIPs に関連付けることができます。OVIS TIPs のトラブルシューティングコマンドのリストは、TIPs Viewer のオンラインヘルプで表示できます。以下の種類のコマンドがあります。

- OVIS Target コマンド (Target Ping コマンドや Target Traceroute コマンドなど)
- OVIS Probe コマンド (Probe CPU Utilization コマンドや Probe Environment コマンドなど)
- OVIS Exchange Probe コマンド (これらのコマンドをご使用の環境で実行するには、設定作業が必要です。これらの設定方法については、TIPs Configuration プログラムのオンラインヘルプを参照してください。)

- OVIS Web Transaction Recorder Probe コマンド
- TIPs Runner コマンド
- OpenView Software コマンド (OV Installed Software コマンドなど)

リモートプローブソフトウェアのインストールと削除

Internet Services では、プローブをローカルシステムで実行し、リモートシステムに設置できます。リモートプローブを設置することで、ユーザーの使用状況をより的確に表している場所にプローブを配置して、サービスを提供しているサーバーのローカルな測定結果と簡単に比較できます。リモートプローブは、収集したデータを、統合とレポート作成のために中央の OVIS 管理サーバーに送信します。

リモートプローブを設定し、その設定を保存すると、リモートプローブソフトウェアを Windows および UNIX のリモートシステムにインストールする必要があります。リモートプローブソフトウェアをインストールする必要があるのは、OVIS を初めてインストールする場合、または OVIS の新規バージョンにアップグレードする場合のみです。Windows システムの場合は、対話形式とサイレントモードのいずれかでインストールできます。

リモートプローブシステム上の TIPs Runner を設定する方法については、TIPs Configuration プログラムのオンラインヘルプを参照してください。

リモート Windows システム

Windows システムでのリモートプローブのインストール (対話形式)

リモートプローブソフトウェアをすでにシステムにインストールしている場合は、以下に説明する手順を使って、既存のプローブソフトウェア上にインストールするだけでアップグレードできます (*OVIS 6.0 にはアップグレード機能が追加されました*)。

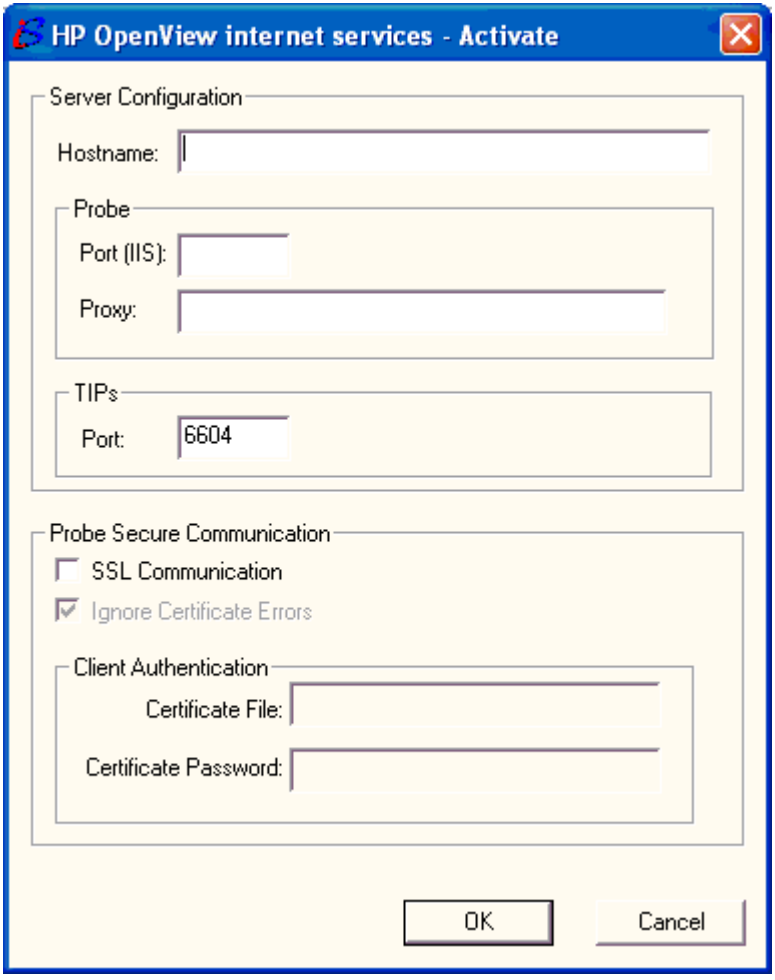
リモートの Windows システムにリモートプローブソフトウェアを対話形式でインストールするには、インストールファイルをリモートシステムに転送し (FTP を使用できます)、インストールプログラムを実行します。サイレントモードのインストール手順については、171 ページの「Windows システムでのリモートプローブのインストール (サイレントモード)」を参照してください。

1 `<install dir>¥newconfig¥remote_probes_install.exe` ファイルを Windows リモートプローブシステムにコピーします。

2 プログラムを実行します。インストールドライブとインストールディレクトリの指定ダイアログボックスが表示されます。システムに他の OpenView 製品 (旧バージョンのリモートプローブを含む) がインストールされていない場合は、ドライブとディレクトリをデフォルト以外に変更できます。

リモートシステムに他の OpenView 製品がすでにインストールされている場合は、リモートプローブソフトウェアのインストールで使用する、所定のインストールドライブとインストールディレクトリ (たとえば、`c:¥rpmtools` と `c:¥rpmtools¥data`) を変更することはできません。

3 表示される次のダイアログに、Internet Services 管理サーバーおよびその他の値を入力します。



ホスト名：これは Internet Services 管理サーバーのホスト名です。入力は必須です。

ポート (IIS): この入力はオプションで、Web サーバーがポート 80 で実行していない場合にのみ入力が必要です。

プロキシ：通信をプロキシ経由で行う必要がある場合は、プロキシを入力します。

TIPs ポート : この入力はオプションで、TIPs (Troubleshooting Insight Packages) ポートが 6604 ではない場合にのみ入力します。詳しくは、481 ページの「TIPs ポートの変更」を参照してください。

SSL 通信 : 通信のセキュリティ保護を有効または無効に設定します。デフォルトは**オフ**です。

証明書のエラーを無視 : 以下の 3 つの設定は、設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログでの指定と同じにします。プローブシステムにサーバーの証明書に関連するエラーを無視させたい場合は**オン**に設定します (たとえば、サーバーのホスト名や発行者などの証明書情報がプローブシステムで解決できない場合など)。証明書の検証が必要な場合は、[証明書のエラーを無視] をオフに設定します。続いて、対象プローブに、プローブがホストにアクセスして、監視対象からの証明書を検証するために使用する証明書を設定する必要があります。また、証明書のファイルとパスワードを以下の説明に従って入力する必要があります。詳しくは、489 ページの「セキュリティ保護された通信の設定」を参照してください。

証明書ファイル : クライアント証明書のファイル名を入力します。Base64 エンコードされた X.509 形式の証明書を、指定した名前 (**clientcert**) で `<data dir>¥conf¥probe` ディレクトリにインストールする必要があります。すべてのプローブロケーションは同じ証明書ファイルとパスワードを共有します。

証明書のパスワード : 証明書ファイルを保護するために使用するパスワードを入力します。

後で `ovisactivate` プログラムを実行して、これらのエントリをリモートプローブシステムで編集できます。

4 インストールが完了すると、Scheduler サービスが管理サーバーの新しいホスト名で再起動されます。

Windows システムでのリモートプローブのインストール (サイレントモード)

サイレントモードを使用してリモートプローブソフトウェアをリモート Windows システムにインストールするには、次の手順を実行します。

1 次のファイルを管理サーバーからリモートプローブシステムにコピーします。

```
<install dir>¥newconfig¥remote_probes_install.exe
<install dir>¥newconfig¥remote_probes_install.cmd
<install dir>¥newconfig¥setup.iss
```

.cmd ファイルによって、インストール時の質問に対する応答が対話形式で行われます。

2 remote_probes_install.cmd ファイルを、使用環境に合わせて編集します。SET [variable=[string]] 構文を使って編集し、REM を使って設定をコメントアウトします。

各環境変数については、remote_probes_install.cmd ファイル内の注釈で説明されています。

環境変数は次のとおりです。

- OVIS_SILENT=TRUE
- OVIS_WMF=TRUE
- OVIS_HOST=ManagementServer
- OVIS_PORT=80
- OVIS_PROXY=someproxy:8088
- TIPS_PORT=6604
- OVIS_SSL=0
- OVIS_IGNORE_CERT_ERRS=1
- OVIS_CERT_FILE=mycert.txt
- OVIS_CERT_PASSWORD=somepassword
- OVIS_INSTALLDIR=”c:¥Program Files¥HP OpenView”
- OVIS_DATADIR=”c:¥Program Files¥HP OpenView¥data”

これらの変数のうちの 2 つ (OVIS_INSTALLDIR、OVIS_DATADIR) は、インストールディレクトリとデータディレクトリに使用するドライブとディレクトリを設定します。リモートシステムに他の OpenView 製品がすでにインストールされている場合は、これらの 2 つの変数は設定「できません」。この場合は、それらの製品ですでに確立されているパスに従ってリモートプローブがインストールされます。

OVIS_WMF=TRUE は、ストリーミングメディアプローブにより使用される Windows Media Format プログラムがインストール可能であることを意味します。ユーザー名とパスワードを必要とするプロキシ認証を設定している場合は、Windows Media Format のインストールはサイレントインストールを失敗させます (これは、ユーザー名とパスワードの入力要求があるためです)。この場合は、OVIS_WMF=FALSE の設定を行い、Windows Media Format (`wmfdist.exe`) のインストールが実行されないようにします。システム上で Windows Media を使ってストリーミングメディアプローブを実行する予定の場合は、リモートプローブのインストールが完了した後で、Windows Media Format をインストールする必要があります。また、Windows XP システムにインストールする場合は、値は OVIS_WMF=FALSE に設定され、ストリーミングメディアプローブの実行を予定している場合は、インストールが完了した後で、Windows Media Format をインストールする必要があります。インストールするには、`<install dir>¥newconfig` ディレクトリにある `wmfdist.exe` ファイルをダブルクリックします。

3 変更を保存します。

4 リモートの Windows システムの [コマンドプロンプト] ウィンドウから `remote_probes_install.cmd` ファイルを起動します。

Windows リモートプローブシステムのインストールディレクトリの変更

リモートシステムのインストールディレクトリを変更するには、以下の手順で行います。

1 リモートプローブソフトウェアを対話形式またはサイレントモードでアンインストールします。

2 以下のファイルを管理サーバーからリモートプローブシステムにコピーします。

```
<install dir>¥newconfig¥remote_probes_install.exe
<install dir>¥newconfig¥remote_probes_install.cmd
<install dir>¥newconfig¥setup.iss
```

3 リモートプローブシステムの `remote_probes_install.cmd` ファイルで、新しいドライブやディレクトリを参照するように OVIS_INSTALLDIR および OVIS_DATADIR の環境変数を変更し、ファイルを保存します。

4 [コマンドプロンプト] ウィンドウで `remote_probes_install.cmd` プログラムを実行して、サイレントインストールを起動します。

Windows システムからのリモートプローブの完全削除

Windows システムからすべてのリモートプローブソフトウェアを対話形式で削除するには、次の手順を実行します。

1. OVIS 管理サーバーで設定マネージャを使用して、すべてのサービスグループからリモートプローブロケーションを削除し、変更を保存します。
2. コマンド行で以下のコマンドを入力して、リモートプローブシステム上の Scheduler サービスを停止します。

   ```
   ovc -stop ovprobes
   ```

3. リモートシステムの [コントロール パネル] の [**アプリケーションの追加と削除**] をダブルクリックします。[**hp OpenView internet services Remote Probes**] を選択して、[**追加と削除**] ボタンをクリックして削除します。

サイレントモードで Windows システムからすべてのリモートプローブを削除するには、次の手順を実行します。

1. OVIS 管理サーバーで設定マネージャを使用して、すべてのサービスグループからリモートプローブロケーションを削除し、変更を保存します。
2. `<install dir>¥newconfig¥remote_probes_uninstall.vbs` スクリプトを管理サーバーからリモートプローブシステムの `<install dir>¥bin` ディレクトリにコピーします。
3. [コマンドプロンプト] ウィンドウで次のように入力して、スクリプトを実行します。

   ```
   cscript remote_probes_uninstall.vbs -s //T:999
   ```

   `-s` はサイレントモードを指定しています。`//T:999` は cscript のパラメータで、タイムアウトを 999 秒に設定します。

アンインストールが成功したかどうかは、戻り値で確認できます。

リモート UNIX システム

リモートプローブソフトウェアの UNIX システムへのインストール

リモートプローブソフトウェアをすでにシステムにインストールしている場合は、以下の説明に従って既存のプローブソフトウェアの上にインストールすることにより、アップグレードできます (OVIS 6.0 にはアップグレード機能が追加されました)。

ここでは、HP-UX、Solaris、および Linux システムにリモートプローブソフトウェアをインストールする手順について説明します。

UNIX システムでは、IE 高負荷モードの HTTP_TRANS プローブは使用できませんが、低負荷モードは使用できます。また、ストリーミングメディア、SMS、Exchange、ODBC、SYS_BASIC_WMI および OVTA 統合プローブは、UNIX システムでは使用できません。

Internet Services のインストール

1. UNIX システムに `root` としてログインします。
2. CD-ROM ドライブに OVIS CD を挿入し、以下のコマンドを入力して CD をマウントします。

   ```
   /etc/mount /dev/dsk/<device_name> /cdrom
   ```

   <device_name> には、お使いの CD-ROM ドライブのデバイス名を入れてください。
3. 以下のコマンドを入力して、リモートプローブインストールプログラムが含まれているディレクトリに移動します。

   ```
   cd /cdrom/SETUP/Remote_Probes_Unix/<platform>/
   ```
4. 以下を入力します (インストールスクリプトが正常に機能するためには Korn シェル (ksh) が必要です)。

   ```
   sh remote_probes_install.bin
   ```

   または、`remote_probes_install.bin` を UNIX システムにコピーして、`chmod` コマンド (`chmod a+x remote_probes_install.bin`) を使って実行可能にし、それを実行します。

   ```
   ./remote_probes_install.bin
   ```

5 インストールが完了したら、表示される入力要求に対して Internet Services 管理サーバーのホスト名と変更するその他のパラメータを入力します (編集する項目の番号を選択します)。

Hostname: Internet Services 管理サーバーのホスト名です。必須の項目です。

IIS Port: これは任意の項目です。Web サーバーがポート 80 で実行されていない場合だけ入力する必要があります。

Proxy: プロキシを通じて通信する必要がある場合は、プロキシを入力します。

TIPs Port: これは任意の項目です。TIPs (Troubleshooting Insight Packages) ポートが 6604 でない場合だけ入力する必要があります。詳しくは、481 ページの「TIPs ポートの変更」を参照してください。

Secure: 通信の保護を有効または無効にします。デフォルトでは **off** になっています。

Ignore Certificate Errors: 以下の 3 つの設定は、設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログの定義と同じです。サーバー証明書に関するすべてのエラー (サーバーのホスト名や発行者などの証明書情報をプローブシステムで解決できないなど) をプローブシステムが無視するようにするには、これを **on** に設定します。証明書の検証を実行するには、[証明書のエラーを無視] を off に設定し、プローブがホストにアクセスしたり、監視対象サービスからの証明書を検証するために使用する証明書を、各グループに設定する必要があります。また、以下で説明しているように証明書ファイルとパスワードを入力する必要があります。詳細は、489 ページの「セキュリティ保護された通信の設定」を参照してください。

Certificate Password: 証明書ファイルの保護に使用するパスワードを入力します。

Certificate File: クライアント証明書のファイル名を入力します。Base64 エンコードされた X.509 形式の証明書が、指定した名前 (**clientcert**) で `<DataDir>/conf/probes` ディレクトリにインストールされている必要があります。そのリモートプローブシステム上のすべてのプローブが、同じ証明書ファイル名とパスワードを共有します。

必要な変更を行ったら、**10** を選択して、**変更を保存して終了**します。スケジューラが自動的に開始されます。インストール / アップグレード時に、変更をしない場合でも (「11 Exit」で終了するのではなく) 10 を選択して保存

および終了する必要があります。これは、TIPs を正常に設定するために必要です。

Internet Services の起動

通常、Internet Services は自動的に起動されますが、ここでは参考情報として手動で起動する方法を説明します。

1. リモートの UNIX プローブシステムの場合は、以下のコマンドを入力して、Internet Services の実行可能プログラムがあるディレクトリに移動します。

   ```
   cd /opt/OV/bin
   ```

2. 以下のコマンドを入力して、Internet Services を起動します。

   ```
   ovc -start ovprobes
   ```

3. 以下のコマンドを入力して、Scheduler が実行していることを確認します。

   ```
   ovc -status
   ```

UNIX システムで Internet Services を停止する必要がある場合は、以下のコマンドを入力します。

```
ovc -stop ovprobes
```

UNIX システムからのリモートプローブの完全削除

1. OVIS 管理サーバーで設定マネージャを使用して、すべてのサービスグループからリモートプローブロケーションを削除し、変更を保存します。
2. リモート UNIX システムに root としてログインします。
3. 以下のコマンドを入力して、`uninstall` スクリプトのディレクトリに移動します。

   ```
   cd /opt/OV/uninstall/RemoteProbes/
   ```

4. 必要であれば、Internet Services を停止します。

   ```
   ovc -stop ovprobes
   ```

5. 以下のコマンドを入力して、削除スクリプトを開始します。

   ```
   sh uninstall.sh
   ```

設定ファイルの配布とアップデート

プローブをリモートシステム上で正常に実行するには、リモートプローブソフトウェアをインストールし、設定ファイルおよびその他のスクリプトや特定のプローブに必要なデータファイルを、リモートシステムに配布する必要があります。

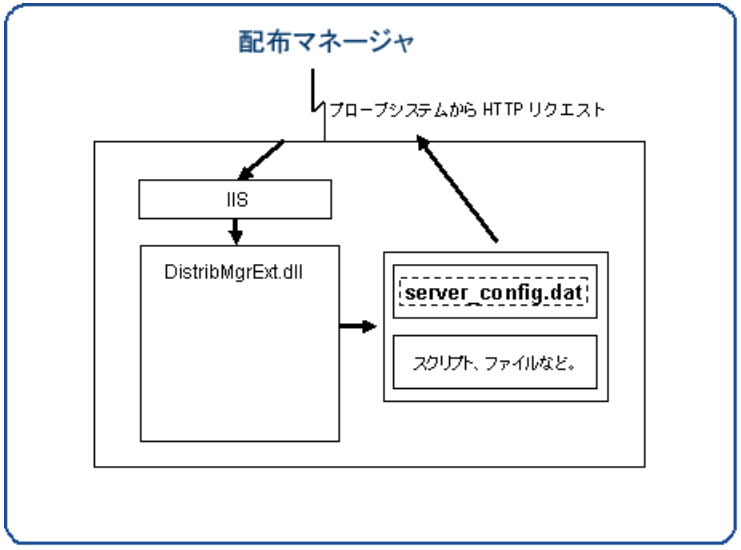
リモートプローブソフトウェアのインストール方法については、168 ページの「リモートプローブソフトウェアのインストールと削除」を参照してください。リモートプローブソフトウェアをインストールする必要があるのは、初めて OVIS をインストールする場合、または OVIS の新規バージョンにアップグレードする場合のみです。

プローブの設定情報は、設定マネージャを終了するときに保存されます。OVIS は自動的に config_<system_name>.dat ファイルを作成し、この設定ファイルを <install dir>¥newconfig¥ ディレクトリに格納します。<system_name> はシステム名です。

最初のリモートプローブソフトウェアをローカルシステムまたはリモートシステムにインストールすると、設定ファイルは管理サーバーから自動的にダウンロードされます。これは IIS の一部である配布マネージャから行われます。また、配布マネージャは、プローブが必要とするスクリプトやデータファイルをリモートおよびローカルシステムに配布するためにも使用されます。さらに、設定の更新を自動的に配布するためにも使用されます。

配布マネージャの動作

プローブソフトウェアは、OVIS 管理サーバーからの設定情報を毎分チェックするよう設計されています。設定更新を要求するプローブシステムからのリクエストは、配布マネージャにより処理されます。配布マネージャは、<install dir>¥newconfig¥ ディレクトリ下の config_<system_name>.dat ファイルを配布すると共に、<install dir>¥newconfig¥distrib¥ ディレクトリ下の該当するサブディレクトリに配置したスクリプトやデータファイルも配布します。



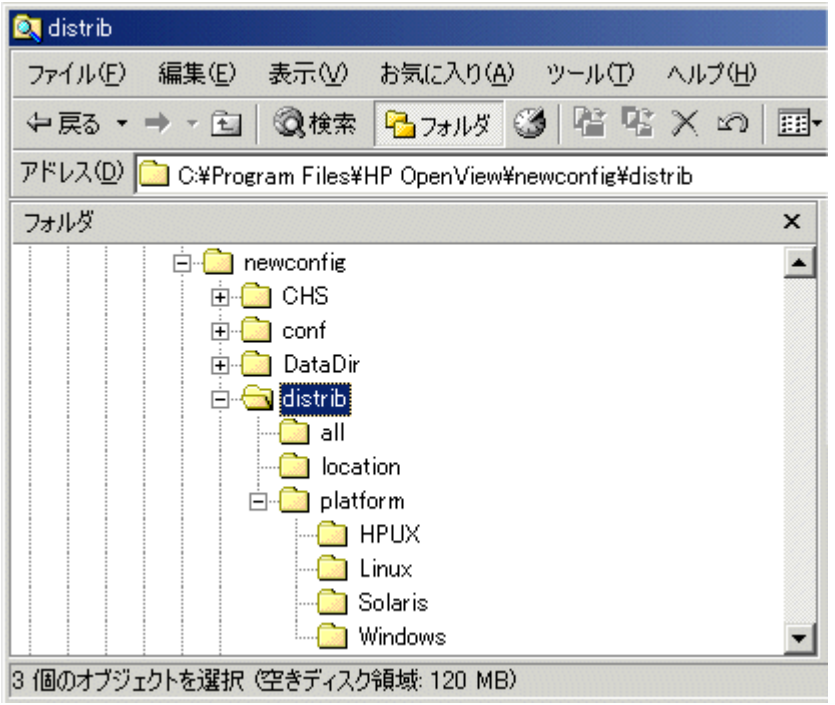
配布マネージャを使ってスクリプトやデータファイルを配布するには、プローブを作成する前に、<install dir>¥newconfig¥distrib¥ ディレクトリ下の OVIS 管理サーバーの適切なディレクトリにこれらのファイルを配置します (適切なサブディレクトリについては、以下の注記を参照してください)。設定を保存すると、<install dir>¥newconfig¥distrib¥ 下のファイルは、プローブシステム上の配布ディレクトリ <data dir>/bin/instrumentation/probe/scripts/ にコピーされます (Windows システム は ¥ を使い、UNIX システムは / を使います)。配布マネージャはファイルだけを配布し、ディレクトリは作成しません。

プローブシステムに新しい設定を配布するときには、配布マネージャはファイルを以下のディレクトリから検索します。配布するスクリプトやデータファイルは配布先のシステムに応じて、以下のディレクトリに格納する必要があります。

newconfig¥distrib¥all - すべてのプラットフォームやプローブロケーションに必要なファイルは all ディレクトリに格納する必要があります。

newconfig¥distrib¥platform¥{Windows|HPUX|Linux|Solaris} - プラットフォームに固有のファイルを Windows、HPUX、Linux、Solaris のディレクトリに格納できます。プローブシステムではプローブが動作しているオペレーティングシステムのファイルのみを受信します。

newconfig¥distrib¥location¥{ 設定マネージャで定義したプローブロケーション } - location ディレクトリ下に設定マネージャで設定されたプローブロケーションの名前のディレクトリを作成することも可能です (通常は、完全修飾のホスト名)。たとえば、プローブロケーションが mysystem.mydomain.com の場合は、同じ mysystem.mydomain.com を名前とするディレクトリを作成し、そこに配布用のファイルを格納します。



これらのディレクトリは、OVIS により追加、削除、変更されないことに注意してください。これらのディレクトリ名は OVIS で設定されたディレクトリと一致する必要があります。従って、ファイルは all と platform ディレクトリに配置して、絶対に必要な場合にのみ location ディレクトリを使うことをお勧めします。さらに、ローカルシステムの場合には、この名前は OVIS 管理サーバーシステムの完全修飾ドメイン名であることに注意してください。たとえば、管理サーバーの名前が ovis.domain.com であり、ローカルシステムのみにファイルを配布する場合は、ディレクトリ ovis.domain.com を作成します。

最初のリモートプローブソフトウェアをローカルまたはリモートのシステム にインストールした後で、プローブの設定を変更する場合は、更新された設定ファイルは配布マネージャを介して管理サーバーから自動的にダウンロードされます。また、変更はリモートプローブソフトウェアを再インストールすることなく、有効になります。

プローブは管理サーバーの新しい設定を毎分チェックします。新しい設定ファイルが利用可能な場合は、プローブにより設定ファイル (newconfig¥**config_<system_name>.dat**) がダウンロードされ、次回の測定間隔時に設定が反映されます。

設定マネージャのステータス画面 (設定マネージャの左ペインにある [ステータス] フォルダを選択) には、プローブが新しい設定をチェックした最後の時間と、配布マネージャにより最後にダウンロードされた時間が各プローブシステムごとに表示されます。

配布マネージャを再開すると、リモートプローブが配布マネージャに再度問い合わせるまで、ステータスは一時的に「**更新待ちのデータはありません。**」と表示されます。

注記 : Internet Services 管理サーバーによって解決できない DNS 名または IP アドレスがリモートプローブシステムに設定されている場合は、プローブ設定の自動更新は動作しないことがあります。この場合、ファイル <datadir>/conf/probe/nodeid.dat をリモートシステムに作成し、リモートシステムの IP アドレス (14.24.157.8 など) を最初の行に入力します。続いて、Hp Internet Services サービスを ovc -restart ovprobes と入力して再起動します。

未使用の OVTA レポートの削除

OVTA データを OVIS 管理サーバーにインポートしていない場合は、毎晩自動的に作成されるが使われることのない OVTA レポート (9 レポート) を削除することができます。これは、空のレポートを除外することで夜間のレポート作成サイクルを短縮できます。

次のファイルが付属しており、OVTA レポートだけを簡単に削除できます。

```
<install dir>¥newconfig¥packages¥remove¥reload_IOPS_remove
_OVTA_reports.SRP
```

不用な OVTA プローブレポートのテンプレートを夜間処理の実行から除外するには、次のコマンドを実行します。

```
reload -remove reload_IOPS_remove_OVTA_reports.SRP
```

OVTA データのインポートを将来使用することになった場合は、上の `reload` コマンドに、`-remove` オプションは指定しないで、この SRP ファイルを指定して、実行することで再開されます。

大量の監視対象サービスの自動設定

監視対象サービス数が多く、これらのサービスがすでに機械的に読み取り可能な形式になっている場合、Internet Services ではこれらのサービスをバッチファイルとして設定することができます。複数の監視対象サービスを設定するには、プログラムまたはスクリプトを記述してサービスのフォーマットを変更し、それらを一括設定インタフェースに送ります。また、設定マネージャで作成した設定を保存し、これらの設定を別の Internet Services 環境で使用できるようにすることも可能です。

ここでは、これらのことを実行するための一括設定インタフェースについて説明します。一括設定インタフェースは、必要に応じて使用します。一括設定インタフェースでは、Internet Services の設定に大量の情報を自動的に追加できます。ただし、設定マネージャへのユーザー入力ではなく、プログラムやスクリプトによる入力が必要となり、エラーに対しても敏感です。

一括設定の操作は複雑なため、プローブの設定について熟知していることが前提となります。

設定ファイルの構文を理解する最も簡単な方法は、設定マネージャを使用して、目的のタイプの設定済みの監視対象サービスを 1 つ作成し、結果として生成された XML 形式の設定ファイルを確認することです。詳細は、206 ページの「一括設定ファイルのサンプル作成」を参照してください。

一括設定の方法

一括設定機能は、XML 形式のテキストを含んでいる、単純な文字ファイルを使用します。XML は、データをテキストファイルで表すための業界標準形式で、インターネット拡張機能により HTML へ変換されます。ここでは、XML の構文については説明しませんが、Internet Services の複数の監視対象サービスを設定 (一括設定) するのに、どのように使用されているかについて説明します。

設定マネージャの [**ファイル**] > [**設定**] で設定された設定パラメータは、XML には保存されません。

IOPSLoad プログラム

IOPSLoad プログラムは一括設定機能をサポートしています。このプログラムは、Internet Services 管理サーバーの <install dir>¥bin¥ ディレクトリにあります。このプログラムは次のことを行えます。

- **load:** 設定ファイルの情報を Internet Services 製品に**ロード**する。
- **save:** Internet Services 製品に含まれている情報を設定ファイルに**保存**する。このファイルは、後続のロード操作に適しています。
- **remove:** Internet Services 製品内にある情報で、設定ファイル内にある情報と同じ情報を**削除**する。
- **removeall:** Internet Services の設定情報を**すべて削除**する。
- **check:** 設定ファイルの構文を**チェック**する。あらゆるエラーを報告しますが、Internet Services の設定には影響を与えません。
- **info:** プローブシステム上の**情報**とプローブ対象数を表示する。
- **disable:** 設定した監視対象を、入力した顧客 (-Customer)、サービス (-Service)、ロケーション (-Location)、監視対象 ID (-Targetid) の値に基づいて**無効**にする。
- **enable:** 設定した監視対象を、入力した顧客 (-Customer)、サービス (-Service)、ロケーション (-Location)、監視対象 ID (-Targetid) の値に基づいて**有効**にする。
- **refresh:** exportiops を実行して、新しい設定ファイルを作成し、MeasEvent と AlarmEvent を再ロードするが、HP Internet Services を再起動しない。設定マネージャの [**ファイル**] > [**設定**] > [**プローブスケジューラのオプション**] で「保存した後にプローブを再起動しない」設定と同じです。
- 次のオプションもあります。
  - **quiet** オプションを指定すると、コンソールウィンドウに出力が表示されずに操作が実行されます。-quiet を指定しないと、プログラムの出力はコンソールウィンドウに出力されます。どちらの場合も、<install dir>¥data ディレクトリにある status.iops ファイルで操作の概要を確認することができます。
  - **configfilename** は、XML 形式の設定情報を含んでいるテキストファイルの名前です。このパラメータの値は入力する必要があります。デフォルト値は用意されていません。

— **norestart** オプションは、IOPSload -load の実行時にサービスを再起動しないよう指定します。

IOPSLoad プログラムを実行するには、[コマンドプロンプト] ウィンドウを開き、以下のように構文を入力します。

```
IOPSload -load [-quiet] [-norestart] configfilename
IOPSload -save [-quiet] configfilename
IOPSload -remove [-quiet] configfilename
IOPSload -removeall
IOPSload -check configfilename
IOPSload -info
IOPSload -disable [-Customer] [-Service] [-Location] [-Targetid]
IOPSload -enable [-Customer] [-Service] [-Location] [-Targetid]
IOPSload -refresh
```

いずれかのパラメータを指定します。何も指定しなかった場合には、-check を指定したとみなされます。

コンポーネントレベルでの IOPSLoad のロードと削除

IOPSLoad プログラムは、コンポーネントの個々のフィールドを更新するようには設計されていません。コンポーネントは、CUSTOMER、SERVICE、TARGET、OBJECTIVE、LOCATION、CONFORMANCE_LEVEL、DOWNTIME、または NETWORK です。コンポーネントのフィールドを更新するには、そのコンポーネントを削除して、希望する変更が記述された XML ファイルから再びコンポーネントをロードする必要があります。CUSTOMER のような、他のコンポーネント (SERVICE、TARGET、OBJECTIVE、LOCATION など) を含むことができるコンポーネントを削除するには、含まれているすべてのコンポーネントを削除する必要があります。

たとえば、設定されたすべての監視対象のホスト名を name.oldcompany.com から name.newcompany.com に変更したい場合、初めに IOPSLoad -save config.date.txt を実行して、config.date.txt ファイルを config.date.mod.txt にコピーしてから、config.date.mod.txt を編集し、ホスト名を希望するものに変更して、同じ名前で保存します。次に、IOPSLoad -removeall を実行して現在の設定をすべて消去してから、IOPSLoad -load config.date.mod.txt で変更された設定をロードします。この例では、config.date.txt は現在指定した設定のすべてのコンポーネントを持っているので、IOPSLoad -remove config.date.txt は removeall オプションと同じ結果になります。

IOPSLoad 機能の正常な実行を自動的にチェックするには、> filename.txt をコマンドに付加し、IOPSLoad の標準出力をディスクのファイルに出力できます。

警告 : IOPSLoad ユーティリティの編集機能は設定マネージャより大幅に少ないため、自動化した処理が同じ名前や無効なデータを生成しないように注意する必要があります。

設定ファイルの構文 (全般)

設定ファイルは、ラインフィード (改行) 文字で終了している、UTF-8 エンコードデータを含んでいる単純なテキストファイルです。各行の最後に、キャリッジリターン文字を含めることもできます。行の配置は重要ではありません。ただし、トークンの途中で行を分割することはできません。

トークンは設定情報を識別する予約語です。これらのトークンについては、188 ページの「設定ファイルのトークンとエレメント」で説明しています。トークンは記述されているとおりに入力する必要があります。大文字と小文字は区別されるため、トークンに示されているとおりに入力します。通常、XML 構文は開始トークン、中間属性トークン、終了トークンを提供します。

例 : <LOCATION id="Denver"></LOCATION>

この例の各部分は以下のとおりです。

<LOCATION>	開始トークン
id=	属性トークン
"Denver"	名前属性に関連付けられているデータ。データは二重引用符で囲まれています。
</LOCATION >	終了トークン

山かっこ "<" と ">" の位置に注意してください。これらの位置は、XML コードを正しく解釈するのに重要です。開始トークンには、対応する終了トークンがなければなりません。たとえば、<LOCATION> に、対応する </LOCATION> が存在しない場合、エラーが発生します。

高度な使用方法 : 特殊な構文を使用して開始トークンと終了トークンを組み合わせることもできます。前述の例は、次のように表すこともできます。

< LOCATION id="Denver"/>

閉じ山かっこの前にスラッシュがあることに注意してください。XML を初めて使用する場合は、開始 / 終了トークンに慣れるまでこの構造は使用しないことをお勧めします。

一部の文字は、XML 構文の解釈には使用できますが、データフィールドでは使用できません。これらの文字を使用する必要がある場合は、特殊文字列で置き換える必要があります。データが使用される前に元の文字に置き換えられます。

表示する文字	使用する文字列
&	&amp;
<	&lt;
>	&gt;
"	&quot;

設定ファイルの構造

設定ファイルの先頭の 2 行は、ファイルが XML 構文であることを示し、オプションを指定します。独自の設定ファイルを生成する場合は、これらの行を正確にコピーしてください。

```
<?xml version="1.0" encoding="ASCII" standalone="yes" ?>
<!-- @version: -->
```

ファイルの残りの部分は、ネストされているトークンペアで設定されています。最も外側のトークンペアは、設定ファイルの内容を指定する、以下のトークンでなければなりません。

```
<CUSTOMERLIST>
</CUSTOMERLIST>
```

すべての構成情報は、<CUSTOMERLIST> トークンと </CUSTOMERLIST> トークンの間になければなりません。設定ファイルのトークンは、次に示す特殊なネストパターンに従う必要があります。

```
<CUSTOMERLIST>
  <CUSTOMER>
    <SERVICE>
      <TARGET>
      <PRIORITY></PRIORITY>
      </TARGET>
```

```
        <OBJECTIVE></OBJECTIVE>
        <LOCATION></LOCATION>
      </SERVICE>
      <SLA></SLA>
    </CUSTOMER>
    <CONFORMANCE_LEVEL></CONFORMANCE_LEVEL>
    <NETWORK></NETWORK>
    <DOWNTIME></DOWNTIME>
</CUSTOMERLIST>
```

この構文は、以下のことを示しています。

CUSTOMERLIST は、ゼロまたはそれ以上の CUSTOMER で構成されている。

(</CUSTOMER> の直後に次の <CUSTOMER> を指定することもできます)

CUSTOMER は、ゼロまたはそれ以上の SERVICE で構成されている (サービスグループともいわれます)。

CUSTOMER の間に SLA を指定することもできます。

SERVICE は、ゼロまたはそれ以上の TARGET、OBJECTIVE、および LOCATION で構成されている。

SERVICE、TARGET、OBJECTIVE、LOCATION は、任意の順序で何回でも繰り返すことができます。

SERVICE は、3 つのすべてのコンポーネント (TARGET、OBJECTIVE、LOCATION) を含んでいる必要はありません。

また、CUSTOMERLIST の CUSTOMER の後ろには、CONFORMANCE_LEVEL、NETWORK、DOWNTIME を任意の順番で何回でも繰り返すことができます。

設定ファイルのトークンとエレメント

ここでは、一括設定ファイルの構文の詳細を説明します。これらの設定エレメントの使用方法の詳細は、前述の項を参照してください。

<CUSTOMERLIST>

属性はありません。

<CUSTOMER name="customername">

- 属性 **"name="** は、顧客名を指定します。省くことはできません。

<SERVICE id="servicegroupname" probe="probename">

- 属性 **"id="** は、サービスグループ名を指定します。省くことはできません。
- 属性 **"probe="** は、このサービスグループ内の監視対象サービスを測定する、サービスプローブの名前を指定します。この名前は、Internet Services 製品が認識しているいずれかのプローブ名と一致する必要があります。詳細は、<install dir>¥newconfig¥packages¥reload_IOPS.SRP ファイルを参照してください。

<TARGET (...) >

監視対象サービスのプローブタイプによって、属性は異なります。

表 1　　プローブの属性

プローブタイプ	属性	説明
ANYTCP	host= port= pattern= patternConfig=	サーバーのシステム名 アクセスする TCP/IP ポート 検索するパターン パターン設定パラメータ
DHCP	host= port= clientport= acceptOffer= pattern= patternConfig= chaddr= retries= label=	DHCP サーバーのシステム名 TCP/IP ポート。デフォルト =67 使用するクライアントポート。デフォルトポートは 68 提供されたアドレスを了承するかどうか 検索するパターン パターン設定パラメータ クライアントハードウェアアドレス (MAC アドレス) 再試行回数 監視対象に使用する名前
DIAL	phoneNumber= username= password= phoneEntryName= stayConnected= retry= waittime=	ダイヤルする電話番号 ユーザー名 パスワード DUN エントリファイル名 ダイヤル後に接続を保持する (1) または保持しない (0) 要求の再試行回数 再試行の間隔

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
DNS	host= port= query= retries= pattern= patternConfig=	DNS のシステム名 TCP/IP ポート。デフォルト =53 DNS によって解決されるシステム名 再試行回数 検索するパターン パターン設定パラメータ
Exchange	host= port= username= password= domain= recipient= displayName= emailtype= usernameRT= passwordRT= domainRT= profilenameRT= runtype= checkinterval= mailbox= exchangeServer= mailboxRT= exchangeServerRT= datasize= label=	Exchange サーバーのシステム名 ポート。デフォルト =80 Exchange ユーザー名 パスワード ログオンしたユーザーのドメイン 送信先の電子メールアドレス 送信先のメールボックスの名前 EX または SMTP の 2 種類 (EX のみサポート) ログインユーザー名 (ラウンドトリップ用) パスワード ログインユーザーのドメイン (ラウンドトリップ用) プロファイル名 (ラウンドトリップ用) -1、0、1、2 (送信 / 読み取り、送信、読み取り、ラウンドトリップ) メールボックスをチェックする頻度 プロファイルメールボックスの作成 (自動) プロファイル Exchange サーバーの作成 (自動) ラウンドトリッププロファイルメールボックスの作成 (自動) ラウンドトリップ Exchange サーバーの作成 (自動) メッセージサイズ 監視対象に使用する名前
FTP	host= port= file= username= password= mode=	FTP サーバーのシステム名 TCP/IP ポート。デフォルト =21 転送するファイルの名前 ユーザー名 パスワード Automatic、Passive、Active

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
HTTP	host=	Web サーバーのシステム名
	port=	TCP/IP ポート。デフォルト =80
	urlfile=	Web ページの参照文字列
	username=	ユーザー名
	password=	パスワード
	options=	KeepAlive nocache host=<string> availCheck=1 bind sec=1 agent=<user agent> SOAPAction:<soap action> post version
	pattern=	検索するパターン
	patternConfig=	パターン設定パラメータ
	embedded=	画像とフレームを読み込むかどうか
	proxyusername=	プロキシサーバーのユーザー名
	proxypassword=	プロキシサーバーのパスワード
	retry=	要求の再試行回数
	waittime=	再試行の間隔
	ua=	ユーザーエージェントヘッダーのオーバーライド
	postFile=	ポストファイル名
	cookieFile=	Cookie の保存やロードに使用するファイル
	label=	監視対象に使用する名前

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
HTTPS	host= port= urlfile= username= password= options=	セキュア Web サーバーのシステム名 TCP/IP ポート。デフォルト =443 保護されている Web ページの参照文字列 ユーザー名 パスワード KeepAlive nocache host=<string> availCheck=1 bind sec=1 agent=<user agent> SOAPAction: <soap action> post version
	pattern= patternConfig= embedded= ignore=	検索するパターン パターン設定パラメータ 画像とフレームを読み込むかどうか 証明書エラーを無視するかどうかのフラグ (0 または 1)
	proxyusername= proxypassword= clientcertfile= clientcertpassword= retry= waittime= ua= postFile= secure= cookieFile= label=	プロキシサーバーのユーザー名 プロキシサーバーのパスワード 認証で使用するクライアント証明書ファイル クライアント証明書のパスワード 要求の再試行回数 再試行の間隔 ユーザーエージェントヘッダーのオーバーライド ポストファイル名 HTTPS の場合は 1 Cookie の保存とロードに使用するファイル 監視対象に使用する名前

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
HTTP_TRANS	transFile= embedded= ignore= version= retry= waittime=	トランザクションファイルの名前 (httptrans.dat) 画像とフレームを読み込むかどうか 証明書エラーを無視するかどうかのフラグ (0 または 1) IE モードの場合は 2。URL モードの場合はバージョン属性を含まない 要求の再試行回数 再試行の間隔
ICMP	host= packetsize= requests= label=	ポーリングするシステム名または TCP/IP アドレス 送信するバイト数 リクエスト数 監視対象に使用する名前
IMAP4	host= port= username= password= label=	IMAP4 メールサーバーのシステム名 TCP/IP ポート。デフォルト =143 ログイン用のユーザー名 ログイン用のパスワード 監視対象に使用する名前
LDAP	host= port= distinguishedName= filter= scope= pattern= patternConfig= enableauth= authtype= username= password= domain= ldaps= certfile= label=	LDAP サーバーのシステム名 TCP/IP ポート。デフォルト =389 LDAP 識別名パラメータ フィルター LDAP_SCOPE_SUBTREE、 LDAP_SCOPE_ONELEVEL、 LDAP_SCOPE_BASE 検索するパターン パターン設定パラメータ LDAP の認証を有効にする 認証タイプ ユーザー名 パスワード LDAP サーバーが常駐する Active Directory/ Windows のドメイン名 SSL を介した LDAP を有効にする 証明データベースへのパス 監視対象に使用する名前

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
MAILROUNDTRIP	host= port= rhost= sprotocol= sender= datasize= rport= rprotocol= recipient= rusername= rpassword= susername= spassword= pollinterval= ESMTP= label=	電子メール送信サーバーのシステム名 送信サーバーのポート 電子メール受信 (IMAP/POP3) サーバーのシステム名 送信サーバーで使用するプロトコル 電子メール送信者名 メッセージサイズ 受信サーバーのポート 受信サーバーで使用するプロトコル 電子メール受信者の、完全なメールアドレス 受信サーバーの電子メールアカウント用ユーザー名 受信サーバーの電子メールアカウント用パスワード 送信元の電子メールサーバー用ユーザー名 送信元の電子メールサーバー用パスワード 新着メッセージがあるか受信サーバーをチェックする間隔 ESMTP/SMTP-A サーバーを使用しているかどうか 監視対象に使用する名前
ODBC	host= query= username= password= pattern= patternConfig= label=	データベースに対する ODBC システム DSN データベース照会用の Select ステートメント データベースにログインするためのユーザー名 データベースにログインするためのパスワード 照会に適用するパターン パターン設定パラメータ 監視対象に使用する名前
ovtacollector (COMAPP、JMSAPP、RMIAPP、SOAPAPP、WEBAPP)	transactionid=	OVTA トランザクションのガイド識別子

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
NNTP	host= port= group= username= password= maxBytes=	NNTP ニュースサーバーのシステム名 TCP/IP ポート。デフォルト =119 ニュースグループ名 ユーザー名 (サーバーが認証を必要とする場合) パスワード (サーバーが認証を必要とする場合) ダウンロードする最大バイト数
NTP	host= port=	NTP サーバーのシステム名 TCP/IP ポート。デフォルト =123
POP3	host= port= username= password= label=	POP3 メールサーバーのシステム名 TCP/IP ポート。デフォルト =110 ユーザー名 パスワード 監視対象に使用する名前
RADIUS	host= port= username= password= protocol= sharedSecret= NASPort= retries calledstId= callingstId=	リモート認証サーバーのシステム名 TCP/IP ポート。デフォルト =1645 ユーザー名 パスワード PAP または CHAP ユーザーと RADIUS サーバー間の共有シークレット Network Access Server ポート 要求の再試行回数 NAS へ認証を要求するためにかけられた電話番号 NAS へ認証を要求するためにかけてきた電話番号

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
SAP	sapprobetype= sapsystemid= saphostname= sapinstance= sapclient= sapuser= sappassword= sapgwhost= saphwservice= saptcode= sapgrouplogon= sapgroup=	SAP プローブの種類 システムランドスケープ内の、システム固有の名前 (3 文字) SAP サーバーのシステム名 SAP インスタンス SAP クライアント番号 SAP トランザクションにアクセスするユーザー名 SAP トランザクションにアクセスするパスワード ゲートウェイホスト ゲートウェイサービス SAP トランザクションコード グループログオンの有効化 グループログオンに使用するグループの名前
Script	script= pattern= patternconfig= chkstat= ofile= options= username= password= multistep=	スクリプトまたはデータファイルの場所 スクリプトの戻り値で一致するパターン パターン設定パラメータ 戻り値ゼロの終了コードをチェック 出力ファイルのための結果ファイルスクリプト フラグ :checkInteractive addInternalParams noLog ログイン認証用のユーザー名 ログイン認証用のパスワード 複数ステップラベルの使用 (1 または 0)
SMS	phoneno= smscno= query= pattern= patternConfig= deviceEntry=	サービスセンターの送信先の電話番号 SMSC の番号 照会する情報 SMS メッセージに適用するパターン パターン設定パラメータ 特定の送信モデム / 受信モデム

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
SMTP	host= port= recipient= sender= dataSize= ESmtp= username= password= label=	SMTP メールサーバーのシステム名 TCP/IP ポート。デフォルト =25 メールの送信先のメールユーザー メールの送信元のメールユーザー メッセージのバイト数 ESMTP/SMTP-A サーバーを監視するかどうか ESMTP/SMTP-A サーバーでの認証用ユーザー名 ESMTP/SMTP-A サーバーでの認証用パスワード 監視対象に使用する名前
SOAP	host= port= urlfile= username= password= options= pattern= patternConfig= embedded= ignore= proxyusername= proxypassword= clientcertfile= clientcertpassword= retry= waittime= ua= postfile=	Web サーバーのシステム名 TCP/IP ポート。デフォルト =443 保護されている Web ページの参照文字列 ユーザー名 パスワード KeepAlive nocache host=<string> availCheck=1 bind sec=1 agent=<user agent> SOAPAction: <soap action> post version 検索するパターン パターン設定パラメータ 画像とフレームを読み込むかどうか フラグを無視 (0 または 1) プロキシサーバーのユーザー名 プロキシサーバーのパスワード 認証で使用するクライアント証明書ファイル クライアント証明書のパスワード 要求の再試行回数 再試行の間隔 ユーザーエージェントヘッダーのオーバーライド ポストファイル名

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
STREAM_MEDIA	host= port= file= protocol= playtime= playtype=	サーバーのシステム名 ストリーミングメディアのポート。デフォルト =80 サーバー上で再生するメディアファイル メディアクリップの再生に使用するプロトコル (HTTP、RTSP) クリップの再生時間 (秒) メディアファイルの形式
SYS_BASIC_WMI	host= username= password= interface=	メトリック元のシステム名 上記システムへの有効なユーザーログイン名 上記ユーザーのパスワード ネットワークインタフェースの正確な名前 (これは、プローブを作成する設定マネージャウィザードの実行により、設定画面に入力し、「接続」をクリックし、接続が正常に行われることで、バッチ設定に使用するネットワークインタフェースの正確な名前であることが判断できます。)
TCP - Performance	host= port= label= protocol= packetSize= duration=	サーバーのシステム名 TCP ポート。デフォルト =5002 監視対象に使用する名前 TCP または UDP プロトコル ペイロードのパケットサイズ (バイト単位) 転送時間

表 1　　プローブの属性 (続き)

プローブタイプ	属性	説明
TFTP	host= port= file= mode= retries=	サーバーのシステム名 TFTP ポート。デフォルト =69 TFTP で転送するファイルの名前 ファイルのダウンロードに使用するモード (Ascii または Octet) 要求の再試行回数
UDP - Performance	host= port= label= protocol= packetSize= duration= packetDelay=	サーバーのシステム名 TCP ポート。デフォルト =5002 監視対象に使用する名前 TCP または UDP プロトコル ペイロードのパケットサイズ (バイト単位) 転送時間 パケット間の遅延
WAP	host= port= url= pattern= patternConfig= retry= waittime=	WAP サーバーのシステム名 TCP/IP ポート。デフォルト =9200 Web ページの参照文字列 検索するパターン パターン設定パラメータ 要求の再試行回数 再試行の間隔

<PRIORITY priority=”1” location=”Local System” network=”Default”>

- 属性 **"priority="** は、プローブロケーションやネットワーク内でスケジュールされた、監視対象サービスの実行順序です。
- 属性 **"location="** は、監視対象サービスのサービスグループのプローブロケーション名を指定します。
- 属性 **"network="** は、監視対象サービスのサービスグループのネットワーク名を指定します。

<OBJECTIVE (...) >

属性は以下のとおりです。

objectiveid="id"
metric="metricname"
condition="comparison"
servicelevel="service level value"
warning="value for alarm severity level of warning"
minor="value for alarm severity level of minor"
major="value for alarm severity level of major"
critical="value for alarm severity level of critical"
baseline="baselinepercent"
duration="seconds"
starttime="hh:mm"
stoptime="hh:mm"
days="MTWTFSS"
message="textmessage">

- 属性 **"objectiveid="** は、この特定の目標値を表す固有の数値 ID を指定します。
- 属性 **"metric="** は、この目標値で使用するメトリックの名前を指定します。メトリック名は、このサービスのサービスプローブによって提供されるメトリックと一致する必要があります。
- 属性 **"condition="** は、メトリック値としきい値の比較条件を指定します。次の条件を指定できます。

表 2　使用可能な比較条件

シンボル	設定ファイルでの指定方法	説明
<	<	より小さい
>	>	より大きい
<=	<=	以下
>=	>=	以上
=	=	等しい
!=	!=	等しくない

- 属性 **"servicelevel="** は、このメトリックのサービスレベル目標値 (SLO) に対して定義される値を指定します。たとえば、90% なら「90.000」、2 秒なら「2.000」となります。

- 属性 **"warning="**、**"minor="**、**"major="**、**"critical="** は、注意域 (シアン)、警戒域 (黄色)、重要警戒域 (オレンジ)、危険域 (赤色) の重要度のアラームをトリガーする値を指定します。
- 属性 **"baseline="** は、メトリックの想定される標準値に基づいて、ベースライン比較を使用することを指定します。「baselinepercent」は、0 ～ 100 の数値で、小数を含むこともできます。
- 属性 **"duration="** は、アラームを発生する条件である目標値が、満たされている秒数を指定します。整数値を指定します。プローブサンプリング測定間隔の倍数が最も適切な値です。
- 属性 **"starttime="** は、**"stoptime="** と共に使用します。両方とも指定すると、開始時間から終了時間以外はアラームは発生しなくなります。どちらの値も時間 (0 ～ 23)、コロン (:)、分 (0 ～ 59) の値を指定します。たとえば、08:00 は午前 8 時で、17:30 は午後 5 時 30 分です。
- 属性 **"days="** は、この目標値でアラームが発生する曜日を指定します。値は 7 つの文字で構成され、各文字は曜日を表します。文字位置は、先頭が月曜日、次に火曜日、そして最後が日曜日になります。

  文字位置が X の場合、アラームは発生しません。M 、T 、F などの他の文字の場合、アラームが発生します。月曜日、水曜日、金曜日だけにアラームを発生させる場合、値は「MXWXFXX」となります。日曜日だけにアラームを発生させる場合、値は「XXXXXXS」となります。
- 属性 **"message="** は、この目標値で発生する、あらゆるアラームとともに送信されるメッセージのテキストを指定します。メッセージには、測定データのデータを置換する特殊コードを入れることもできます。すべてのデータフィールドでは、特殊フォーマット文字 <、>、&、" の置換文字を使用する必要があります。以下の表を参照してください。METRIC 1 ～ 8 の値については、第 4 章の「メトリックの一覧 (プローブタイプ別)」を参照してください。

表 3　シンボルの置換

シンボル	置換内容
<SERVICE>	サービスグループ名
<CUSTOMER>	顧客名
<PROBETYPE>	サービスプローブのタイプ (HTTP、DNS など)

表 3　シンボルの置換 (続き)

シンボル	置換内容
<PROBESYS>	測定を実施したプローブロケーション
<TARGET>	監視対象サービス (プローブのタイプによって異なる)
<HOST>	監視対象サービスが存在するシステムの名前
<THRESHOLD>	目標値の固定しきい値
<BASELINE>	目標値のベースライン割合 (%)
<DURATION>	目標値のアラーム保留時間 (秒)
<VALUE>	最新の測定値
<BASELOW>	ベースライン情報に基づいた想定下限値
<BASEHIGH>	ベースライン情報に基づいた想定上限値
<RESPONSE_TIME>	応答時間の値 (プローブから入手可能な場合)
<AVAILABILITY>	サービス可用性 (プローブから入手可能な場合)
<SETUP_TIME>	セットアップ時間値 (プローブから入手可能な場合)
<THRUPUT>	スループット値 (プローブから入手可能な場合)
<ERROR_INFO>	プローブ固有のエラー情報 (プローブから入手可能な場合)
<EXPRESSION>	アラームをトリガーしたアラーム式 (このプローブからその式が提供された場合)
<PSTIME>	プローブにより測定が行われた時刻
<THRESHOLD_SW>	違反が発生したときのスライドウィンドウのしきい値
<METRIC1>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC2>	プローブ固有の値 (プローブから入手可能な場合)

表 3　シンボルの置換 (続き)

シンボル	置換内容
<METRIC3>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC4>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC5>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC6>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC7>	プローブ固有の値 (プローブから入手可能な場合)
<METRIC8>	プローブ固有の値 (プローブから入手可能な場合)

<LOCATION id="locationname" interval="seconds" timeout="seconds">

- 属性 **"id="** は、プローブエージェントが存在するシステムの名前を指定します。id="Local System" を指定した場合は、プローブエージェントが Internet Services 管理サーバーと同じシステム上に存在することを示します。
- 属性 **"interval="** は、測定間隔 (秒) を指定します。
- 属性 **"timeout="** は、測定がタイムアウトになり、利用不可と記録されるまでの秒数を指定します。

<SLA (...) >

属性は以下のとおりです。

id="slaname"
type="slatype"
equation="slaequation"
threshold="thresholdvalue"
conformance_name="conformancename">

- 属性 **"id="** は、サービスレベル契約 (SLA) の名前を指定します。
- 属性 **"type="** は、設定タイプを指定します。0 = 基本、1 = 詳細
- 属性 **"equation="** は、SLA 評価式を指定します。
- 属性 **"threshold="** は、SLA 適合しきい値を指定します。

- 属性 **"conformance_name="** は、適合しきい値の名前を指定します (例 : プラチナ、ゴールド、シルバー、ブロンズ)。

<CONFORMANCE_LEVEL (...) >

属性は以下のとおりです。

name="conformancelevelname"
description="description"
threshold="thresholdvalue">

- 属性 **"name="** は、適合レベルの名前を指定します (例 : プラチナ、ゴールド、シルバー、ブロンズ)。
- 属性 **"description="** は、テキストによる説明です。
- 属性 **"threshold="** は、この適合レベルに関連付けられているしきい値 (数値) です。しきい値が複数ある場合は、個別の適合レベル文を設定する必要があります。

<NETWORK (...) >

属性は以下のとおりです。

name="networkname"
customer="customer name"
service="service name"
type="network type"
executable="probe executable name"
phonenumber="dialphone"
user="DIALuser"
password="DIALpassword"
dunentry="dial-up Net Entry"
timeout="seconds"
concurrency="num concurrent probes">

- 属性 **"name="** は、ネットワークの名前を指定します。
- 属性 **"customer="** は、ネットワークに関連付けられている顧客を指定します。このネットワークに関連付けられている特定の顧客が存在しない場合、値は空文字列 (" ") になります。
- 属性 **"service="** は、このネットワークに関連付けられているサービスグループの名前を指定します。このネットワークに関連付けられている特定のサービスグループが存在しない場合、値は空文字列 (" ") になります。

- 属性 **"type="** は、このネットワークエントリの接続タイプを指定します。有効な値は、Default、LAN、Dial-up です。
- 属性 **"executable="** は、このネットワークを開始するのに起動する実行可能プログラムを指定します。通常、ネットワークにアクセスするのに特別な実行可能プログラムは不要であるため、この値は空になっています。ダイヤルアップ接続の場合、この値は probeDial.exe になります。
- 属性 **"phonenumber="** は、ダイヤルアップ接続で使用する電話番号を指定します。
- 属性 **"user="** は、このダイヤルアップ接続で使用するユーザー名を指定します。
- 属性 **"password="** は、このダイヤルアップ接続で使用するパスワードを指定します。
- 属性 **"DUNEntry="** は、このダイヤルアップ接続で使用するユーザー定義の DUN (ダイヤルアップネットワーク) を指定します。
- 属性 **"timeout="** は、このネットワークでプローブが終了するまでの時間を指定します。たとえば、300 と指定します。
- 属性 **"concurrency="** は、このネットワークで一度に並列実行されるプローブの数を指定します。たとえば、32 と指定します。

<DOWNTIME (...)>

属性は以下のとおりです。

description="description"
downtimestring="downtime"
applied="appliedflag">

- 属性 **"description="** は、このダウンタイムの説明です。
- 属性 **"downtimestring="** は、開始、停止、繰り返しを含む、このダウンタイムのすべての設定を表す文字列を指定します。
- 属性 **"applied="** は、常時 TRUE を指定します。

一括設定ファイルのサンプル作成

独自のサンプル XML 設定ファイルを作成して、XML 設定ファイルを調査したり、実際の XML 設定ファイルを作成する際のテンプレートとして使用できます。サンプルの XML 設定ファイルは、以下の手順で作成できます。

1 **設定マネージャ**を開き、顧客、1 つまたは複数のサービスグループ、それらに関連付けられている監視対象サービス、目標値、プローブロケーションなどの環境に基づいて、設定を作成します。

2 [コマンドプロンプト] ウィンドウを開き、XML 設定ファイルを保存するディレクトリに移動し、次のコマンドを入力します。

```
IOPSLoad -save myconfig.txt
```

この時点で、設定マネージャで入力した情報に基づいた XML 設定ファイルが作成されます。このファイルは、myconfig.txt という名前で、IOPSLoad プログラムを実行したディレクトリに保存されます。通常使用しているテキストエディタを使用して設定ファイルを確認、変更できます。

設定ファイルを変更して、それらの変更を Internet Services に適用するには、[コマンドプロンプト] ウィンドウを開き、次のコマンドを入力します。

```
IOPSLoad -load myconfig.txt
```

一括設定ファイルのサンプル

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
<!-- @version: -->
<CUSTOMERLIST>
  <CUSTOMER name="IPA Company">
    <SERVICE id="Dns Services" probe="DNS">
      <TARGET     host="15.351.193.31"
                  port="53"
                  query="34604.loc.hp.com"
                  retries="4"
                  comment="DNS Service Monitor Request"
                  disable="0"
       >
       <PRIORITY priority="1" location="Local System"
          network="Default"> </PRIORITY>
       </TARGET>
      <OBJECTIVE  objectiveid="3"
                  metric="AVAILABILITY"
                  condition="&gt;"
                  servicelevel="90.000"
                  warning="90.000"
```

```
                baseline="0.000"
                duration="600"
                starttime="00:00"
                stoptime="00:00"
                days="MTWTFSS"
                message="DNS for &lt;TARGET&gt; unavail"
    > </OBJECTIVE>
    <LOCATION   id="Local System"
                interval="300"
                timeout="20"
                network="Default"
    > </LOCATION>
  </SERVICE>
</CUSTOMER>
<CUSTOMER name="Hewlett-Packard">
  <SERVICE id="HP Shopping Site" probe="HTTP">
    <TARGET     host="Sys5.loc.hp.com"
                port="80"
                urlfile="/"
                password="##"
                embedded="1"
                proxypassword="##"
                disable="0"
     >
     <PRIORITY priority="1" location="Local System"
         network="Default"> </PRIORITY>
     </TARGET>
    <TARGET     host="Sys66.loc.hp.com"
                port="80"
                urlfile="/hpov_reports/iops.htm"
                password="##"
                embedded="1"
                proxypassword="##"
                disable="0"
     >
     <PRIORITY priority="1" location="Local System"
        network="Default"> </PRIORITY>
     </TARGET>
    <OBJECTIVE  objectiveid="5"
                metric="AVAILABILITY"
                condition="&gt;"
                servicelevel="90.000"
                warning="90.000"
                baseline="80.000"
                duration="600"
                starttime="00:00"
                stoptime="00:00"
                days="MTWTFSS"
                message="HTTP for &lt;TARGET&gt; unavail"
    > </OBJECTIVE>
```

```
    <OBJECTIVE  objectiveid="2"
                metric="RESPONSE_TIME"
                condition="&lt;"
                servicelevel="3.000"
                warning="-91230000000000000000.000"
                baseline="0.000"
                duration="600"
                starttime="00:00"
                stoptime="00:00"
                days="MTWTFSS"
               message="HTTP RESPONSE_TIME slow
                  (&lt;VALUE&gt; vs &lt;THRESHOLD&gt;)
                    on &lt;TARGET&gt;"
     > </OBJECTIVE>
     <LOCATION   id="Local System"
                 interval="300"
                 timeout="45"
                 network="Default"
     > </LOCATION>
   </SERVICE>
   <SLA id="SLA_Name"
     type="0"
     equation="([1])"
     threshold="95.000"
     conformance_name="Gold">
    <SLO objectiveid="1"> </SLO>
   </SLA>
   <SLA id="SLA_Name2"
     type="0"
     equation="([2])"
     threshold="98.000"
     conformance_name="Platinum">
    <SLO objectiveid="2"> </SLO>
   </SLA>
 </CUSTOMER>
 <CONFORMANCE_LEVEL name="Bronze"
                    description="Lowest conformance."
                    threshold="80.000"
 > </CONFORMANCE_LEVEL>
 <CONFORMANCE_LEVEL name="Gold"
                    description="Second highest conformance"
                    threshold="95.000"
 > </CONFORMANCE_LEVEL>
 <CONFORMANCE_LEVEL name="Platinum"
                    description="Highest conformance."
                    threshold="98.000"
 > </CONFORMANCE_LEVEL>
 <CONFORMANCE_LEVEL name="Silver"
                    description="Mid-level conformance."
                    threshold="90.000"
```

```
  > </CONFORMANCE_LEVEL>
 <DOWNTIME description="SchedDown"
downtimestring="1011118202,1011118202,0;1;1011118202;0,1,1011118215,1,0,0;0,1
011118215,0,0,0,0,0,0,0;0,0,0,0,0"
            applied="FALSE"
  > </DOWNTIME>
  <NETWORK name="Default" customer="" service=""
           type="LAN"
           executable=""
           phoneNumber=""
           user=""
           password=""
           DUNEntry=""
           timeout="300"
           concurrency="32"
           upload="0"
  > </NETWORK>
  <NETWORK name="ODBC" customer="" service=""
           type="Default"
           executable=""
           phoneNumber=""
           user=""
           password="##"
           DUNEntry=""
           timeout="30"
           concurrency="1"
           upload="0"
  > </NETWORK>
</CUSTOMERLIST>
```

4

サービスタイプとプローブの説明

設定するすべてのサービスグループは、特定のサービスタイプで構成されています。それぞれのサービスタイプがどのように機能するかを理解すると、監視対象サービスや目標値を設定して、サービスのプローブを設定する際に役立ちます。

各種サービスのプローブによって収集したメトリックと各メトリックの定義の完全なリストについては、296 ページの「メトリックの一覧 (プローブタイプ別)」を参照してください。

Windows および UNIX システム上の Internet Services プローブ： Internet Services を使用することにより、以下のすべてのサービスタイプを Windows システム上で設定および監視できます。UNIX システムでは、Internet Explorer 高負荷モードの HTTP_TRANS プローブ、ストリーミングメディアプローブ、SMS プローブ、SYS_BASIC_WMI プローブ、Exchange プローブ、ODBC プローブ、および OVTA からインポートしたデータのサービスタイプを除くすべてのプローブを使用できます。

- ANYTCP (Transmission Control Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- DIAL (ダイヤルアップネットワーク)
- DNS (Domain Name System)
- Exchange (MAPI)

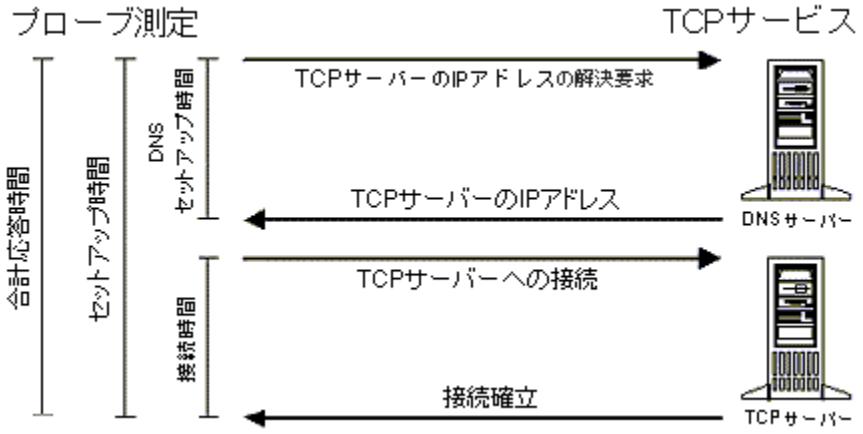
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- HTTPS (Hypertext Transfer Protocol Secure)
- HTTP_TRANS (Web Transaction Recorder)
- ICMP (Internet Control Message Protocol—Ping)
- IMAP4 (Internet Message Access Protocol)
- LDAP (Lightweight Directory Access Protocol)
- MAILROUNDTRIP (メールラウンドトリップ)
- NNTP (Network News Transfer Protocol)
- NTP (Network Time Protocol)
- ODBC (Open Database Connectivity)
- POP3 (Post Office Protocol 3)
- RADIUS (Remote Authentication Dial In User Service)
- SAP Basis
- Script (汎用スクリプト)
- SMS (Short Message Service)
- SMTP (Simple Mail Transfer Protocol)
- SOAP (Simple Object Access Protocol)
- STREAM_MEDIA (ストリーミングメディア)
- SYS_BASIC_WMI (基本システムメトリック)
- TCP - パフォーマンス
- TFTP (Trivial File Transfer Protocol)
- UDP - パフォーマンス
- WAP (Wireless Application Protocol)
- カスタムプローブ
- OVTA からのインポートデータ

ANYTCP (Transmission Control Protocol)

ANYTCP プローブは、TCP ステップがクライアントと指定されたホストとを、指定されたポートで接続終了するまでの時間を測定します。

詳しくは、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



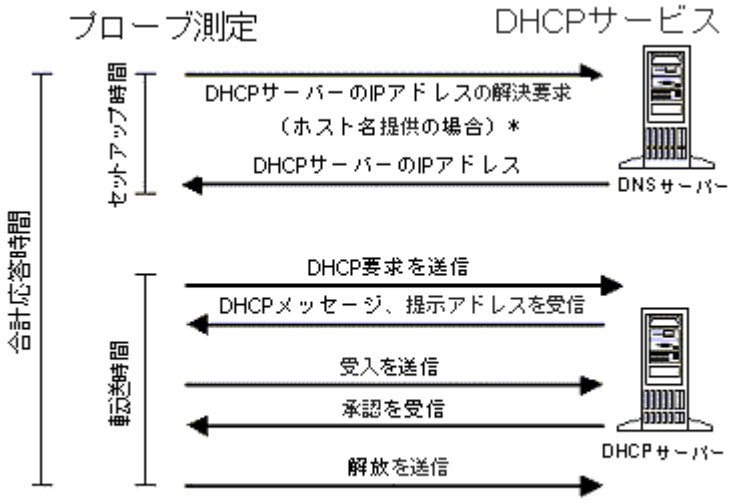
DHCP (Dynamic Host Configuration Protocol)

DHCP プローブは、DHCP サーバーが IP アドレス要求を処理するまでの時間を測定します。DHCP サーバーとの通信には UDP プロトコルを使用します。DHCP プローブは、特定のホスト (指定した場合) に要求を送信するか、ネットワークに要求をブロードキャストします。その後、DHCP サーバーから IP アドレスが提供されるのを待ちます。複数のサーバーがこれに応答するかも知れません。

プローブが要求をサブネットにブロードキャストした場合は、プローブは DHCP サーバーからのオファーを先着順に受け付けます。プローブが要求を特定のホスト (提供されている場合) に送信した場合は、プローブはその特定のホストで作成されたオファーだけを受け付けます。

プローブは、提供された IP アドレスを受け付け、サーバーからの受信確認を待ち、受信確認を受けると IP アドレスを解放します。

プローブが応答時間を測定するステップを以下の図に示します。



*DNSセットアップ時間は、ホスト名が提供された場合にのみ測定されます。

IP アドレスを拘束しないように、デフォルトでは、プローブは提供された IP アドレスを確保しません。一部の DHCP サーバーは、提供した IP アドレスを最大 2 分間は確保しますが、必要に応じてそれらを他の要求元に提供します。プローブの要求が DHCP サーバーによって受け付けられると、プローブはサーバーから提供された IP アドレスを正式に要求し、DHCP サーバーからの承認を待ちます。サーバーが要求を承認すると、プローブは提供された IP アドレスをすぐにサーバーに解放します。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

DIAL (ダイヤルアップネットワーク)

ダイヤルアップ (DIAL) プローブは、モデムからリモートサーバーへのポイントツーポイントプロトコル (ppp) 接続を確立します。このプローブはダイヤル、ハンドシェーク、および ppp 接続プロトコルを完了するまでの時間を測定します。このプローブは、測定後にネットワーク接続を切断するように設定したり、他のプローブを実行するためにネットワーク接続を確立したままにするように設定できます。

ダイヤルアッププローブを使用したり、ダイヤルアップネットワーク接続を使用するように他のプローブを設定する場合は、RAS (Remote Access Server) と、少なくとも 1 つの電話帳エントリをプローブシステム上に設定する必要があります。

ダイヤルアッププローブは、サポートされているすべての UNIX のバージョン (SuSE Linux を除く) で使用できます。

ダイヤルアッププローブを作成すれば、ダイヤルアップ接続を使用して監視対象サービスにアクセスする、任意の数のプローブがそのプローブを使用できます。他のプローブがダイヤルアッププローブを使用するように設定するには、設定マネージャの [プローブロケーションの情報] ダイアログでダイヤルアップネットワーク接続を選択します。

ダイヤルアップ接続が存在しない場合は、[プローブロケーションの情報] ダイアログの [接続の新規作成] ボタンを選択して作成できます。新しいダイヤルアップネットワーク接続を設定すれば、ダイヤルアップサービスグループと監視対象サービスが自動的に設定されます。ダイヤルアップネットワーク接続を設定したプローブと同じ [顧客] フォルダ内にダイヤルアッププローブが表示されま

す。このダイヤルアップサービスグループには、サービスレベル目標値や、他の OpenView 製品にアラームを送信するためのしきい値を設定できます。このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

DNS (Domain Name System)

DNS プローブは、ホスト名や IP アドレスを解決するための合計応答時間を測定します。DNS プローブは、UDP プロトコルを使用して DNS サーバーと通信します。DNS プローブが応答を受信すると、DNS サーバーが利用可能であるとみなされます。応答が、ホスト名または IP アドレスを解決できないことを示す場合でも、DNS サーバーは要求を処理し、有効な返答を返したため利用可能であるとみなされます。

再試行の回数とその間隔を設定して、要求のタイムアウト値に達するまでにプローブが要求を再送信する頻度をコントロールできます。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

Exchange (MAPI)

Exchange プローブは、Microsoft Exchange 2000/2003 Mail Service (MAPI) を監視します。**このプローブは Windows プラットフォームでのみ動作します。**

プローブを設定する前に、以下の前提条件を設定する必要があります。リモートシステム (OVIS 管理サーバーではなく) でプローブを実行する場合は、リモートプローブシステムにおいて以下の前提条件を設定する必要があります。

以下の前提条件を満たすことによって、適切な権限を持つユーザーアカウント (ドメインまたはローカルアカウント) でプローブを実行し、特定のアカウントに関連付けられた Exchange プロファイルを使用して、Exchange サーバー上のメールボックスにアクセスできます。

Exchange プローブの設定については、以下のセクションを参照してください。

前提条件

- Exchange プローブを実行するシステムを決定します。
- Exchange プローブを実行するシステムに、Exchange クライアント (Microsoft Outlook など) がインストールされていることを確認します。
- プローブシステムに、以下で説明されている特権を持つユーザーアカウント (ドメインまたはローカルアカウント) をセットアップします。Windows NT では、一方向の信頼関係で Exchange サーバードメインによって信頼されているクライアントユーザーであることを推奨します。

  必要な権限 : Exchange プローブを正常に動作させるには、特定の権限を設定する必要があります。

  まず、ユーザーアカウントにはローカルコンピュータの「ローカルログオン」権限が必要です。この権限は、ワークステーションとサーバーの場合はデフォルトですべてのユーザーに付与されていますが、ドメインコントロー

ラの場合は管理者にのみ付与されています。特定のユーザーとしてプローブを実行できない場合は、OVIS スケジューラから実行するときにローカルメッセージストアにアクセスできません。

次に必要な権限は、SE_TCB_NAME (オペレーティングシステムの一部として動作する権限) です。プローブが SE_TCB_NAME 権限を保持していない場合、またはこの権限が無効な場合は、OVIS スケジューラから実行するときにプローブが正常に機能しません。

管理者またはルート以外のユーザーは、その他のユーザー権限が必要な場合があります。Exchange プローブに関するユーザー権限の設定方法については、設定マネージャのオンラインヘルプを参照してください。

- プローブを実行する Exchange サーバー上にユーザーのメールボックスを設定します。
- プローブシステム上にプロファイルを作成するか、プローブの初回実行時にプロファイルを自動的に作成するように OVIS を設定します。メールプロファイルの作成手順の例は、221 ページの「Exchange プロファイルの手動による設定方法」を参照してください。

> Outlook XP や Outlook 2002 を使用している場合に、[プロファイルの自動生成] にチェックをしていても、メールのプロファイルは正常に作成されず、プローブは使用不可である旨を返します。
> Exchange の、該当ユーザーのメールプロファイルセクションを確認しても、メールボックスが設定されていません。
> この問題は、主にユーザー名とメールボックスのエイリアス名とが、同一でない場合に発生します。MAPI の障害の詳細は http://support.microsoft.com/default.aspx?kbid=329295 を参照してください。

- プローブシステム上で、Exchange メールサービスについて、[ログオン ネットワーク セキュリティ] が [NT パスワード認証] に設定されていることを確認します。221 ページの「Exchange プロファイルの手動による設定方法」の手順 10 を参照してください。
- 以下の Exchange サーバーとユーザーアカウントの情報を収集します。この情報は、設定マネージャでプローブを設定するときに使用します。Exchange の設定ダイアログの例は、223 ページの「Exchange プローブの設定方法」を参照してください。

  — Exchange サーバーの完全修飾名

— ユーザー用の Exchange メールボックス

— ユーザー名、ドメイン、パスワード

プローブシステムでプローブを実行する場合は、設定した Exchange メールボックスに関連付けられたユーザーとしてログインします。ログインしたユーザーがプローブシステムにローカルでログインする権限を持っていない場合、プローブシステムから Exchange アカウントにアクセスできない場合、または Exchange メールボックスに接続するときに手動による操作が必要な場合、Exchange プローブは正常に機能しません。以下のテスト手順を参照してください。

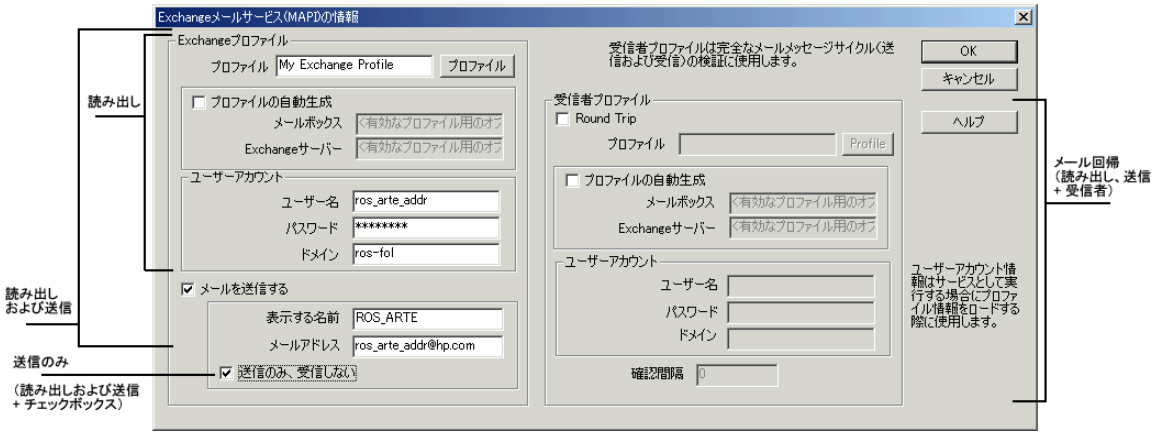
- プローブシステムから Exchange サーバーへのアクセスをテストします。225 ページの「Exchange サーバーへのアクセスのテスト方法」を参照してください。

Exchange プローブの設定

Exchange プローブは以下の方法で設定できます。

- 読み取りのみ - Exchange サーバーの可用性とサーバーへの接続を監視し、読み取り専用でメールボックスにアクセスします。Exchange プロファイルを入力するか、プロファイルを自動作成します。Exchange プロファイルへのアクセスに必要なユーザーアカウント情報もすべて入力します。
- 読み取りと送信 - Exchange サーバーの可用性とサーバーへの接続を監視し、メールボックスの読み取りと電子メールの送信を行います。表示する名前 (Exchange メールサービス (MAPI) 情報) と電子メールを送信するメールアドレスを入力します。プローブは最初にグローバルアドレスリストで表示する名前を検索して電子メールアドレスがそれに関連しているかどうかを確認します。
- 送信のみ - 送信だけを監視し、メールボックスの読み取りを無効にします。上記の「読み取りと送信」で説明した情報を入力し、[送信のみ、受信しない] ボックスをオンにします。
- ラウンドトリップ - Exchange サーバーの可用性とサーバーへの接続を監視し、電子メールを送受信するラウンドトリップ時間を設定します。基本的な Exchange プロファイルと上記の「読み取りと送信」で説明した電子メールの送信に関する情報に加え、受信者の Exchange プロファイルを入力するか、プロファイルを自動作成します。受信者のプロファイル情報のロードに必要なユーザーアカウント情報もすべて入力します。

Exchange プローブの設定に使用する Exchange のダイアログは以下のとおりです。上記の各設定方法でプローブを設定するときに入力するフィールドを示します。

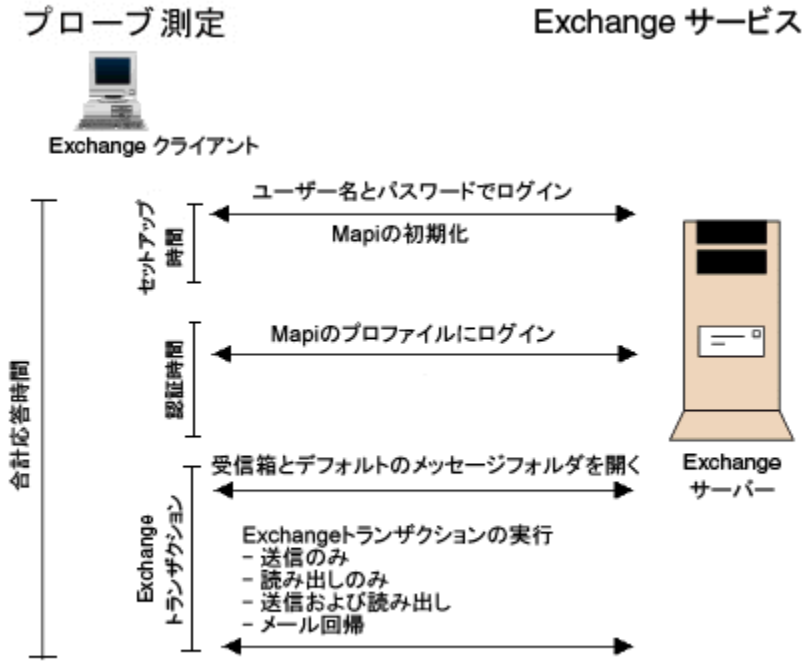


ラウンドトリップメッセージサイクルを監視するようにプローブを設定しない場合、プローブは Exchange プロファイルで指定された Exchange サーバーにログオンし、受信ボックスをダウンロードして読み取り、OVIS メッセージを削除します。

ラウンドトリップを監視するようにプローブを設定する場合、プローブはメッセージを送受信する電子メールメッセージサイクルが完了するまで受信ボックスのダウンロードと読み取りを延期します。

Exchange プローブでは、同じ Exchange サーバーとユーザー / メールボックスを監視するリモートプローブを数個に制限する必要があります。そうすることにより、Exchange サーバーの動作低下を防ぎます。

Exchange プローブが応答時間を測定するステップを以下の図に示します (プロファイルの自動作成を選択すると、MAPI のログインが完了する前の有効なプローブの初回実行中にプロファイルが作成されます)。



Exchange プロファイルの手動による設定方法

Exchange プローブが使用する Exchange プロファイルを設定するには、プロファイルを手動で設定する方法と、プローブによって Exchange メールプロファイルを作成する方法があります。いずれの場合にも、Exchange プローブが正常に機能するには、Exchange メールプロファイルを、プローブの設定時に指定したユーザーアカウントから使用する必要があります。これは、メールプロファイルがユーザーに固有であるためです。

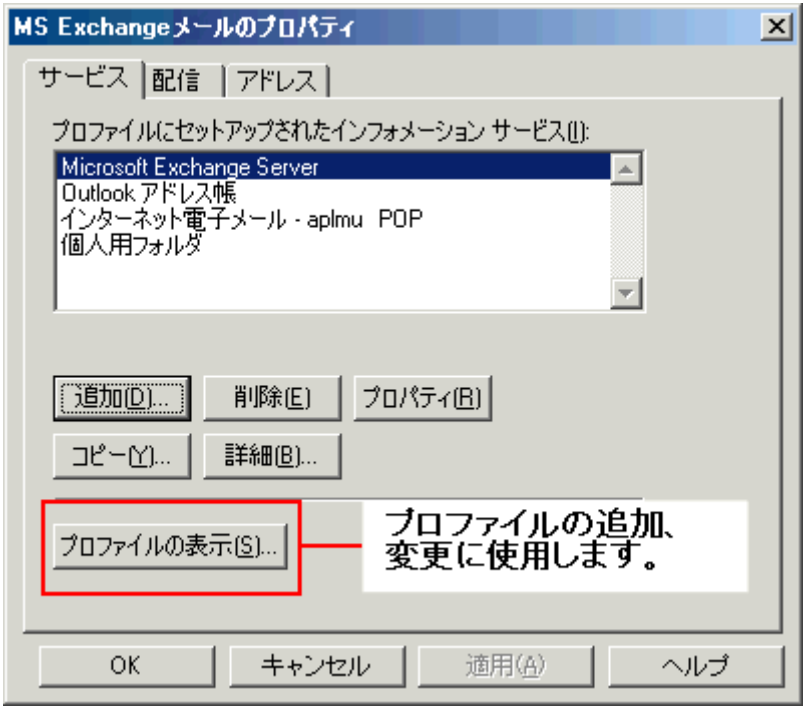
以下の手順では、Microsoft Outlook メールクライアントを使用します。

1 上記の「前提条件」セクションで説明した情報を収集します。

2 Exchange プローブを実行するシステムに Exchange メールボックスを所有するユーザーとしてログインします。

3 [**スタート**] > [**設定**] > [**コントロール パネル**] を選択し、[**メール**] をダブルクリックします。

4 表示された [プロパティ] ダイアログで [**プロファイルの表示**] ボタンを選択します。



5 表示された [メール] ダイアログで [**追加**] ボタンを選択します。

6 Microsoft Outlook のセットアップウィザードで、インフォメーションサービスとして [**Microsoft Exchange Server**] を選択し、[**次へ**] をクリックします。

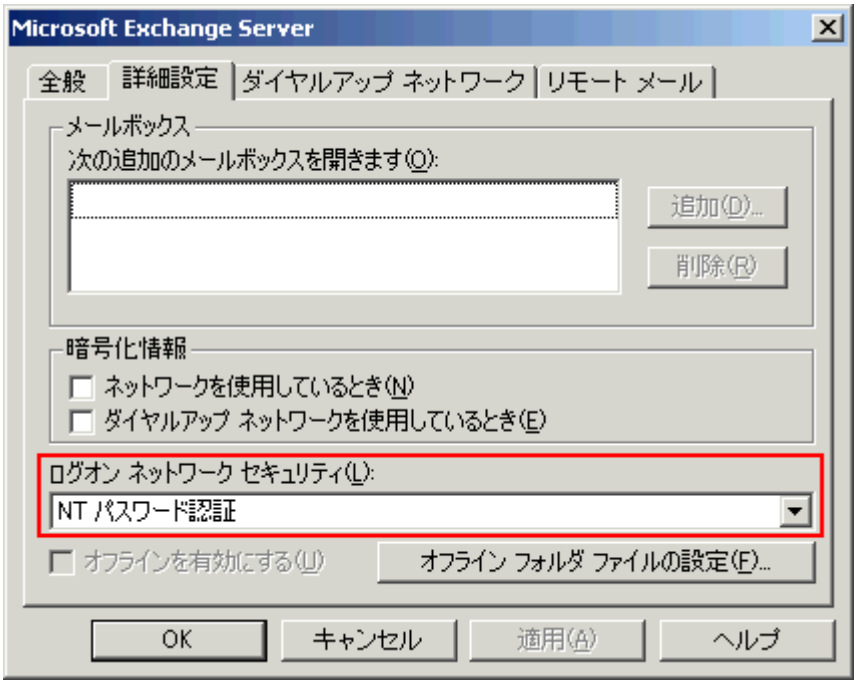
7 使用するプロファイル名を入力し、[**次へ**] をクリックします。

8 アクセスする Exchange サーバーとメールボックスを入力し、[**次へ**] をクリックします。

9 セットアップウィザードを完了し、[**完了**] をクリックします。

10 Exchange プローブが動作するために必要な特定のプロパティについて、[ログオン ネットワーク セキュリティ] を [NT パスワード認証] に設定します。これはプローブがアカウントにアクセスするユーザーとしてログインするためです。[NT パスワード認証] に設定しないと、プローブが Exchange サーバーにログインできません。

NT パスワード認証を設定するには、上記の手順 3 のとおりに [コントロール パネル] の [**メール**] を選択します。設定済みのプロファイルをダブルクリックすると、以下に示す Microsoft Exchange Server のダイアログが表示されます。[詳細設定] タブを選択し、[ログオン ネットワーク セキュリティ] のドロップダウンボックスから [NT パスワード認証] を選択します。

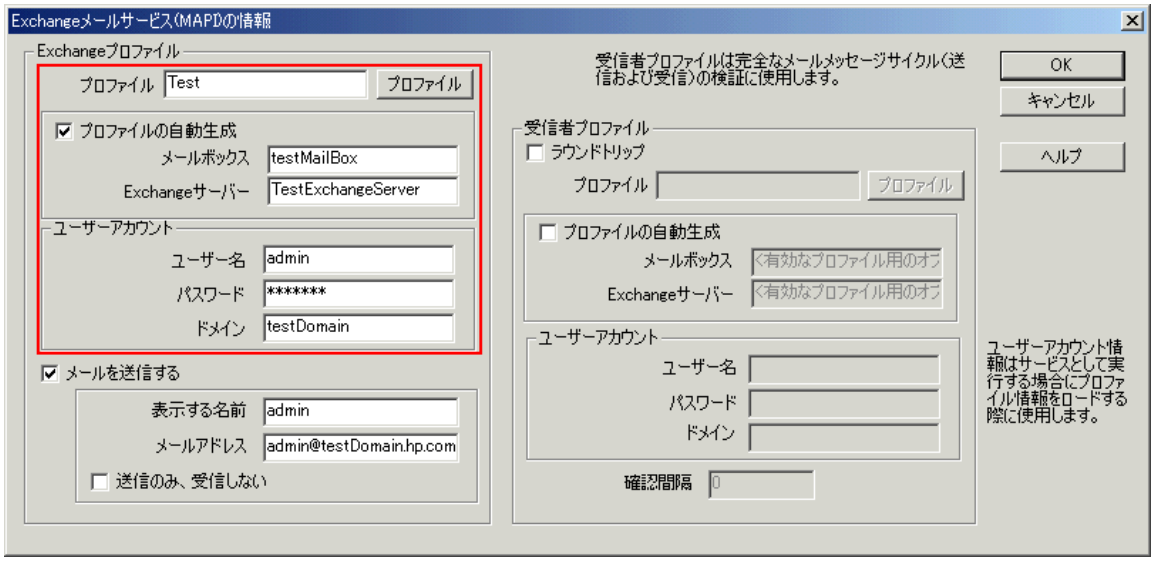


11 この手順を完了すると、特定のメールボックスへのアクセス権限を持つ特定のユーザー用の新しい Exchange プロファイルが作成されます。このプロファイルを Exchange プローブの設定時に使用できます。

Exchange プローブの設定方法

1 すべての前提条件を設定し、プローブの設定に必要な情報を収集したことを確認します。

2 OVIS 設定マネージャの Exchange メールサービスのダイアログで、プローブが読み込み、読み込みと送信、送信のみ、またはラウンドトリップを測定するのに必要な情報を入力します。これらのプローブの設定で必要なこのダイアログの値については、219 ページの「Exchange プローブの設定」を参照してください。また、このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。



3 Exchange プロファイルを手動で作成した場合は、プロファイル名とユーザーアカウント情報を入力します。

4 OVIS で自動的にプロファイルを作成する場合は、[プロファイルの自動生成] オプションを選択します。OVIS でプロファイルを作成するには、プローブシステム上に Exchange クライアント、ユーザーアカウント、およびパスワードが存在しており、またメールボックスが Exchange サーバーに設定されている必要があります。プローブシステムで最初にプローブを実行すると、ユーザーが設定した設定情報を使用してプロファイルが自動的に作成されます。このプロファイルは入力したユーザーアカウント情報に関連付けられます。

Outlook XP や Outlook 2002 を使用している場合に、[プロファイルの自動生成] にチェックをしていても、メールのプロファイルは正常に作成されず、プローブは使用不可である旨を返します。
Exchange の、該当ユーザーのメールプロファイルセクションを確認しても、メールボックスが設定されていません。
この問題は、主にユーザー名とメールボックスのエイリアス名とが、同一でない場合に発生します。MAPI の障害の詳細は http://support.microsoft.com/default (.aspx) を参照してください。

5 設定を保存します。

Exchange サーバーへのアクセスのテスト方法

Exchange サーバーを使用する上で、必要なアクセス権限をユーザーが持っていることを確認するのは重要です。ユーザーの権限を確認するには、以下の手順に従ってプローブをシミュレートすることをお勧めします。

1 ユーザーのユーザー名、パスワード、ドメインを使用して、プローブシステムにローカルでログインします。

2 特定のプロファイルを使用して、Microsoft Outlook などの Exchange メールクライアントを起動します。

この時点でユーザー名とパスワード情報を手動で入力する必要がある場合は、プローブはプロファイルにアクセスできません。

3 このアカウントからアカウント自身に電子メールを送信し、動作を確認します。

上記の手順を手動で実行するときに、いずれかの手順に失敗した場合、Exchange プローブも失敗します。

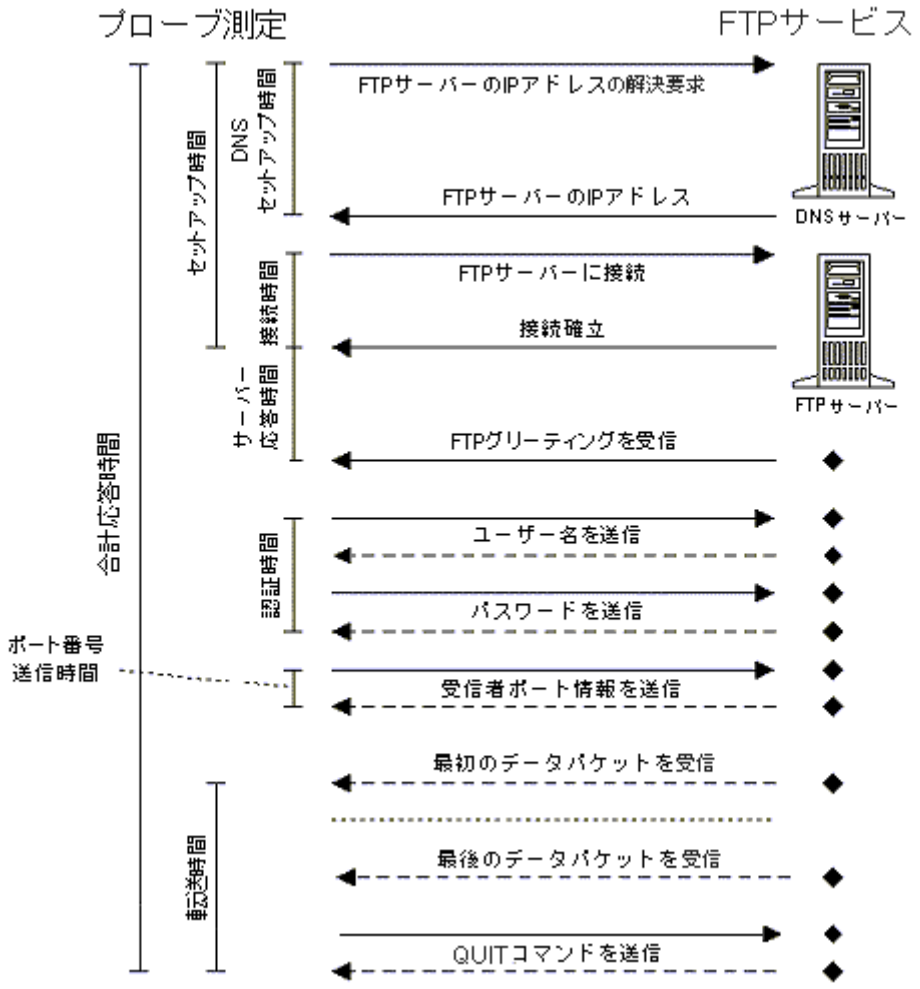
FTP (File Transfer Protocol)

FTP プローブは、単純なファイル取得、またはディレクトリ一覧作成を実行します。認証が必要な場合は、指定したユーザー名とパスワードを使用し、指定したファイルをダウンロードします。

FTP プロトコルは 2 つの接続を使用します。1 つはコマンド情報を交換するための接続で、1 つはデータをダウンロードするための接続です。プローブはデータ接続用に新しいソケットを開き、ソケットはコマンド接続を通じて FTP サーバーに送信されます (PORT プロトコルステップ)。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。

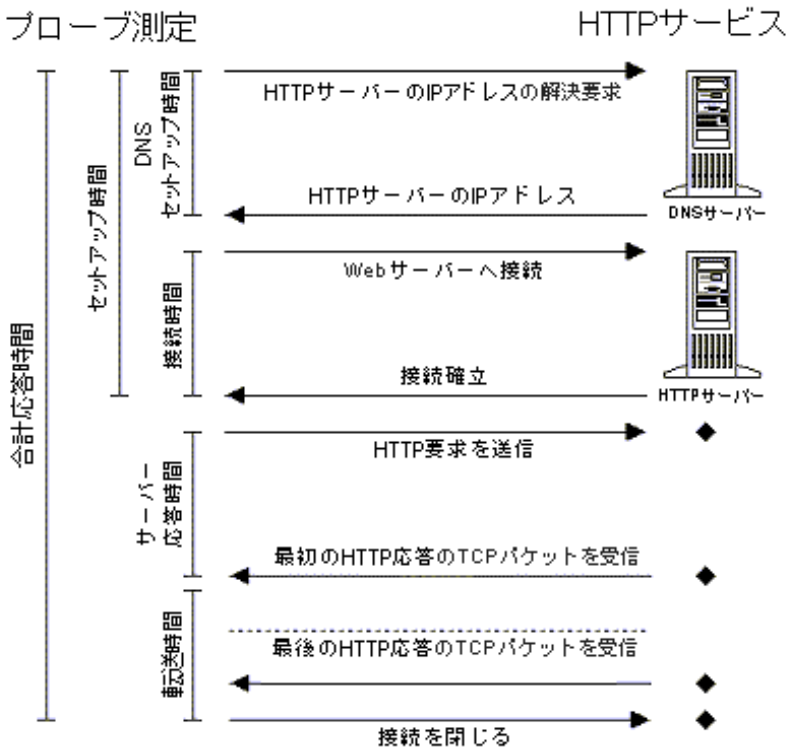


HTTP (Hypertext Transfer Protocol)

HTTP プローブは、一般的な HTTP 要求をエミュレートします。HTTP プローブはプロキシ、基本認証、およびフォームや画像のダウンロードをサポートしています。さらに、Web ページから取得した HTML 出力に適用する検索パターンを設定できます。UNIX の HTTP プローブでは、基本承認だけしかサポートしませんので注意してください。

HTTP プローブを設定すると、Web ページのダウンロードが正常に完了したことを確認するためにパターン検索を使用できます。プロキシを使用するようにプローブを設定できます。プローブによって Web ページをロードする方法と可用性を判断する際に考慮するページ要素をコントロールするために、さまざまなフラグを設定します。再試行の回数とその間隔を設定して、要求のタイムアウト値に達するまでにプローブが要求を再送信する頻度をコントロールします。このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



HTTPS (Hypertext Transfer Protocol Secure)

HTTPS プローブは、HTTP プローブ (上記を参照) と同様に機能しますが、安全なプロトコルを使用する点が異なります。

インストールされている Windows の暗号化強度 (輸出国向けまたは米国国内向け) に従って、プローブは SSL で保護された HTTP サーバーにアクセスできます。プローブが輸出国向けの暗号化強度のシステムで実行されていて、米国国内向けの暗号化強度で保護された HTTPS サーバーにアクセスしようとするとエラーが発生します。

サーバーのホスト名や発行者などの証明書情報をプローブシステムで解決できない場合は、プローブが証明書を無視するように指定できます。

[証明書のエラーを無視] チェックボックスをオンにしない場合は、プローブが監視対象サーバーの検証に使用する、信頼されたルート証明書を管理サーバー上に設定する必要があります。

信頼されたルート証明書のエクスポート

監視対象サービスの「信頼されたルート証明書」は、Base64 エンコードの X.509 (.CER) 形式でエクスポートし、`<data dir>¥conf¥probe` ディレクトリにある **trusted.txt** ファイルにコピーする必要があります。`trusted.txt` ファイルは、HTTPS プローブが対象サーバーの検証に使用します。

たとえば、Internet Explorer 5.5 で「信頼されたルート証明書」をエクスポートするには、次の手順に従います。

1. [**ツール**] > [**インターネットオプション**] で [**コンテンツ**] タブを選択し、[証明書] セクションの [**証明書**] をクリックします。[**信頼されたルート証明機関**] タブを選択し、エクスポートする証明書を選択します。
2. [**エクスポート**] をクリックして証明書のエクスポートウィザードを起動し、[**次へ**] を選択します。エクスポートする形式として [Base64 encoded X.509 (.CER)] を選択し、[**次へ**] をクリックします。
3. ファイル名 (たとえば「`c:¥<my_cert>.cer`」) を入力し (`.cer` 拡張子は自動的に追加されます)、[**次へ**] をクリックします。
4. [**完了**] をクリックします。「エクスポートは正常に完了しました。」というメッセージが表示されたら、[**OK**] をクリックします。

5 メモ帳でファイル (たとえば「c:¥my_cert.cer」) を開き、ファイルのすべての内容 (「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」) を <data dir>¥conf¥probe ディレクトリの **trusted.txt** にコピーします。

6 複数の証明書をエクスポートする場合は、この手順を繰り返します。

7 「-----BEGIN CERTIFICATE-----」行の上に、証明書の名前と有効期限を示すコメントを追加することもできます。

たとえば、次のように入力します。

RSA Commercial CA - exp. Jan 7, 2010

-----BEGIN CERTIFICATE-----

...

-----END CERTIFICATE-----

測定する監視対象サービスにクライアント認証が必要な場合には、クライアント認証を設定して、[HTTPS - セキュア Web ページの情報] ダイアログの [クライアント証明書の認証情報] セクションに証明書ファイル名とパスワードを入力する必要があります。保護された通信の詳細は、489 ページの「セキュリティ保護された通信の設定」を参照してください。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

HTTP_TRANS (Web Transaction Recorder)

HTTP_TRANS プローブは、カタログ検索、ログイン / ログアウト、ショッピングカートなどの、複数 URL の Web トランザクションを監視する目的で使用します。

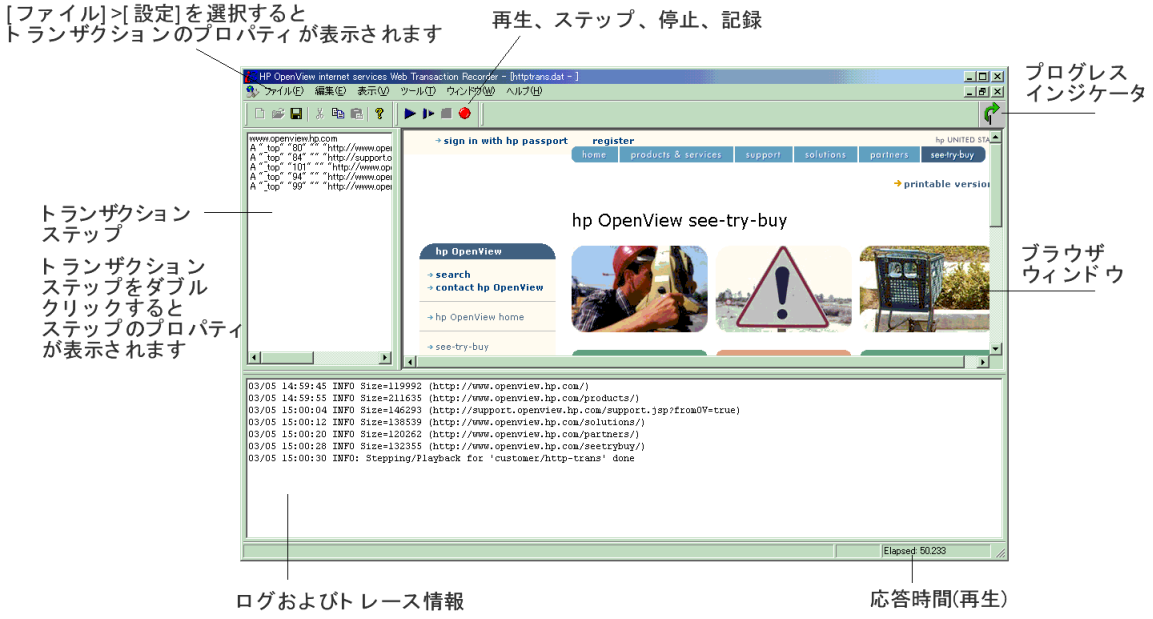
HTTP_TRANS 監視対象サービスを作成すると、Web Transaction Recorder が自動的に起動します。Web Transaction Recorder を使用すると、追跡するユーザーアクションを指定してそれを記録し、プローブで定期的に再生することができます。これにより、エンドユーザーの通常のアクティビティをシミュレートし、可用性と応答時間に関する重要なデータを収集することができます。**詳細は、『*OVIS Web Transaction Recorder ガイド*』を参照してください** (webrecorder.pdf)。

HTTP_TRANS プローブの設定に Web Transaction Recorder を使用すれば、エラーを軽減して設定時間を短縮できます。Web Transaction Recorder は、通常のエンドユーザートランザクションの各ステップを実行するだけで、ユーザーの操作とアクセスしたページやリンクの順序を自動的に取得します。複数の URL やページ参照を手動で入力する必要はありません。あとでトランザクションをテストおよび検証して、記録したトランザクションステップをもとに変更することができます。

Web Transaction Recorder を使用するには、Internet Explorer 5.5 以降がインストールされている必要があります (IE 6.0 (サービスパック 1) では、HTTP ステータスコードを取り出してログに記録する機能を提供しています)。

サービスグループあたり、1 つの Web トランザクションの監視対象サービスを指定できます。記録可能なステップの最大数は 100 です。

次に示す図は、Web トランザクションの記録に使用する Web Transaction Recorder の GUI です。



トランザクションを記録する基本ステップは次の通りです **(詳細は、『*OVIS Web Transaction Recorder ガイド*』を参照してください)**。

1. 記録する Web ページの計画を立てます。最初にブラウザの Web トランザクションステップを一通り実行し、正しく記録するための順序や選択方法を確認します。
2. トランザクションを記録する前に Web Transaction Recorder で [**ツール**] > [**キャッシュビューアー**] を選択してクッキーを削除します。[クッキーを無効にする] フラグを設定して再生中はクッキーを無効にすることができます。
3. Web Transaction Recorder で [**ファイル**] > [**設定**] > [**プロパティ**] を選択し、ダイアログボックスを表示して、全体的なランザクションプロパティを設定します。ポップアップおよびエラーダイアログの扱い方、タイムアウトおよび待機時間、エラーキャプチャ、プロキシ設定、トレースレベルなどを指定することができます。

4 トランザクションステップの記録を開始するには、メインウィンドウの [**記録**] ボタンを押します。

5 開始 URL を入力します。

右ペインのブラウザウィンドウに Web ページが完全に読み込まれたら (右上隅の緑の矢印の回転が停止した時)、表示された Web ページ内でトランザクションステップをナビゲートすることができます。

トランザクションステップは左のペインに表示されます。トランザクションステップのログとトレース情報は下のペインに表示されます。

6 [**停止**] を押して記録を停止します。

7 記録した内容を再生して、必要なすべてのステップが含まれているかどうか調べます。再生中に右下隅に表示される応答時間を確認します。

8 Web Transaction Recorder でオプションを使用して、必要な変更を行います。たとえば、次のように操作します。

- 左ペインでトランザクションステップを右クリックし [**プロパティ**] を選択し、[**ステップのプロパティ**] ダイアログボックスでトランザクションステップのプロパティを修正します。
- 左ペインでトランザクションステップを右クリックし、[**プロパティ**] を選択し、[**ステップのプロパティ**] ダイアログボックスで [**詳細**] タブを選択して、詳細スクリプト情報を入力します。

9 Web Transaction Recorder を終了して、[HTTP_TRANS - Web Transaction の情報] ダイアログで [OK] ボタンを押します。

10 Web Transaction Recorder で作成したプローブのプローブロケーションを設定します。

11 Web Transaction Recorder で作成した プローブのサービスレベル目標を設定します。

ステップアラームを指定することができます。HTTP_TRANS プローブトランザクションの個別のステップでのアラーム設定に関する詳細は、108 ページの「サービスレベル目標値とアラームの基本設定」を参照してください。ステップアラーム機能はアラームに対してのみで、ステップしきい値はサービスレベル目標に使用されません。

アラームのセットに対して 1 つのステップだけを選択できます。トランザクション内の複数の個別ステップのアラームを作成するには、それぞれ別々なアラームの定義を作成します。複数のアラーム定義に同じメトリックを使用することができます。

ステップアラームは、可用性メトリックではなく応答時間メトリックで使用されます。なぜなら、可用性はトランザクション全体に定義されるからです。もし可用性メトリックを使用すると、ステップが使用できない場合に、トランザクション全体が使用不可としてマークされてしまいます。

ステップ番号は、ダッシュボードの詳細ページと設定マネージャのステータスページの詳細に表示されます。

12 設定マネージャでプローブ変更を保存し、終了します。

HTTP_TRANS プローブは、他のプローブより多くのプローブリソースを使用します。これによって、このプローブタイプの同時実行数が制限されます。HTTP_TRANS プローブの同時実行数 ([プローブロケーション] ダイアログボックスで設定) は、1 ～ 10 が適しています。詳しくは、512 ページの「スケーラビリティ情報」を参照してください。

ICMP (Internet Control Message Protocol—Ping)

ICMP プローブは、指定したホストに、1 秒ごとに ICMP Echo 要求を送信し、各要求 / 返答の応答時間を測定します。プローブによって返された合計応答時間は、個別の要求 / 返答の応答時間の平均です。

再試行回数を設定すると、要求のタイムアウト値に達するまでにプローブが要求を再送信する頻度をコントロールできます。このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

IMAP4 (Internet Message Access Protocol)

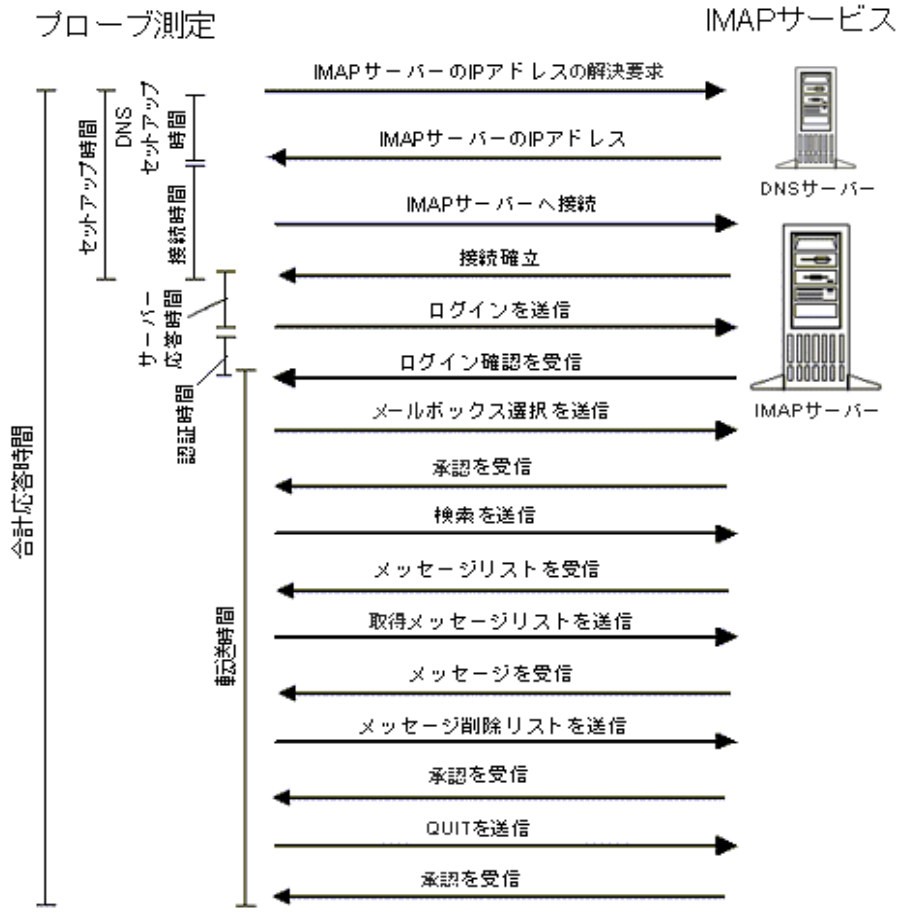
Internet Message Access Protocol (IMAP4) は、メールサーバー (通常は共有メールサーバー) に保存されている電子メールや電子掲示板メッセージにアクセスする方法を提供します。IMAP は、TCP ベースのサービスです。IMAP により、クライアント電子メールプログラムは、ローカルの場合と同様にリモートメッセージストアにアクセスできます。IMAP クライアントは電子メールのコピーを取得し、電子メール自身はサーバーにあります。IMAP プローブは、サーバーに接続してメッセージにアクセスする時に、クライアントで発生するステップを測定します。

SMTP プローブおよび IMAP4 プローブ専用のメールボックスを設定することを強くお勧めします。

プローブは、メールボックス内のすべてのメールを取得し、OVIS-Timestamp をすべてのメッセージで検索します。このフィールドは、SMTP プローブによって設定されます。このフィールドが検出されると、プローブは、そのメッセージに削除対象のマークを付けます。すべてのメッセージが読み取られると、プローブは、OVIS-Timestamp を含むメッセージを削除します。この削除により、メールボックスが SMTP プローブメッセージでいっぱいになるのを防ぐことができます。

Microsoft Exchange 2000/2003 Server を使用している場合は、IMAP プローブを使用して IMAP4 サービスを監視する上での留意事項があります。IMAP4 監視対象サービスに関する詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



LDAP (Lightweight Directory Access Protocol)

LDAP プローブは、LDAP サーバーへの接続時間を測定し、ユーザーが指定した特定の識別名に一致するデータを返します。検索条件に一致するすべてのエントリが返されると、プローブは LDAP サーバーへの接続を切断します。LDAP プローブは UDP プロトコルを使用して、LDAP サーバーと通信します。

LDAP プローブを設定するには、LDAP サーバーがアクセスするデータベースの構造を理解している必要があります。特定の LDAP 設定が `config.dat` ファイル内に表示される例を以下に示します。

```
[LDAP]
distinguishedName=emailaddress=j_jones@corp.com,ou=employees,o=corp.com
host=ldap.corp.corp.com port=389 scope=LDAP_SCOPE_SUBTREE
```

LDAPS の設定に関する注記 : このプローブを LDAPS プロトコルに設定する上での留意事項があります。LDAP プローブは、LDAPS プロトコルについて、現時点では Netscape iPlanet/SunOne Directory Server 5.X のみをサポートしています。

対応する LDAPS サーバーに必要な SSL 証明書が、Netscape Communicator 4.x が使用する cert7.db データベースファイルに保存されている必要があります。Netscape Communicator 4.x 以外のバージョンでは、証明書データベースに異なるファイル形式を使用します。証明書データベースの異なるバージョンを使用しようとすると、データベースエラーが発生します。

1. LDAPS が正常に機能するには、プローブを実行する各システムの `<install dir>¥bin` ディレクトリに iPlanet/SunOne client SDK 5.0 の以下のライブラリがコピーされている必要があります。これらのライブラリは iPlanet/SunOne Server 製品の一部として含まれています。また、Sun Microsystems から入手可能です。

   ```
   libnspr4.dll
   libplc4.dll
   libplds4.dll
   LibRfc32.dll
   librfc32u.dll
   nsldap32v50.dll
   nsldappr32v50.dll
   nsldapssl32v50.dll
   nss3.dll
   ```

ssl3.dll

2 Netscape Communicator 4.X によって作成した以下の証明書データベースファイルを、プローブを実行するシステムの <data dir>¥conf¥probe ディレクトリにコピーする必要があります。

cert7.db

key3.db

証明書データベースを作成するには、次の手順に従います。

1 Netscape 4.x ブラウザを起動して次の URL にアクセスします。

https://ldaps_hostname:ldaps_port/

ldaps_hostname は、LDAPS サービスをホストするサーバーのホスト名です。

Ldaps_port は、LDAPS サービスが提供されるポート番号です。

2 ブラウザに証明書を承認するプロンプトが表示され、一連のダイアログが表示され、最後に文書にデータが存在しないことを示すエラーメッセージが表示されます。証明書を承認して、ブラウザを閉じます。

必要な証明書データベースを作成する方法は他にもあります。詳細は、iPlanet/SunOne Server のドキュメントを参照してください。

3 ブラウザで次の URL を入力し、サーバーへの LDAPS 接続を確認します。

ldaps://ldaps_hostname:ldaps_port/dn=?

dn=? は、有効な識別名です。ブラウザには dn エントリが表示されます。

4 最後に、cert7.db と key3.db ファイルを ¥Netscape¥Users¥UserId フォルダから ¥probes フォルダへコピーします。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

MAILROUNDTRIP (メールラウンドトリップ)

「メールラウンドトリップ」メールサービスは、メールラウンドトリップ プローブ (MAILRTRIP) で監視できます。このプローブは、電子メールサーバー (SMTP/ESMTP/SMTP-A) に接続し、指定された電子メールサーバーに電子メールメッセージを送信し、その後、受信サーバー (POP/IMAP) にポーリングを実行して、メールがラウンドトリップを完了するまでの所要時間を測定します。このプローブは、受信者や送信者などのメッセージ情報を設定し、指定されたサイズのメッセージ本文を送信します。また、このプローブは、サービスが利用可能かどうかを判断し、実行時にそのサービスに関するその他の情報を収集します。エラーが返されない場合は、メッセージの送受信は正常に完了したことになります。

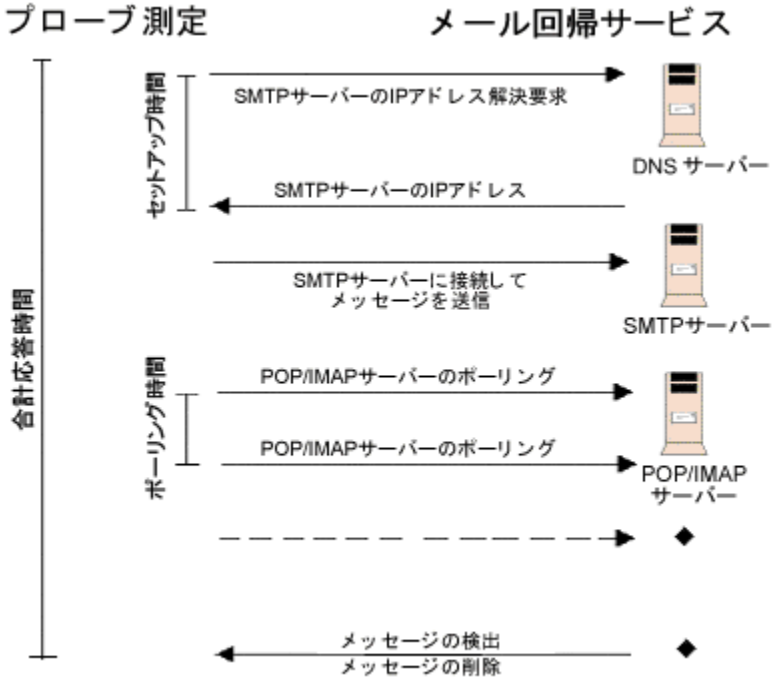
Microsoft Exchange 2000/2003 Server を使用している場合は、メールラウンドトリップ プローブを使用してメールサービスを監視する上での留意事項があります。詳細は、メールラウンドトリップ監視対象サービスに関するオンラインヘルプを参照してください。

メッセージを送信する電子メールサーバーとメッセージを受信する電子メールサーバーの両方に関する設定情報を入力する必要があります。さらに、電子メールの送信に使用される送信者情報と、電子メールの受信に使用されるプロトコル情報および電子メールアカウント情報を定義します。また、メッセージのサイズと、メッセージの受信をチェックする間隔も指定できます。

再試行の回数とその間隔を設定して、要求のタイムアウト値に達するまでにプローブが要求を再送信する頻度をコントロールします。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。

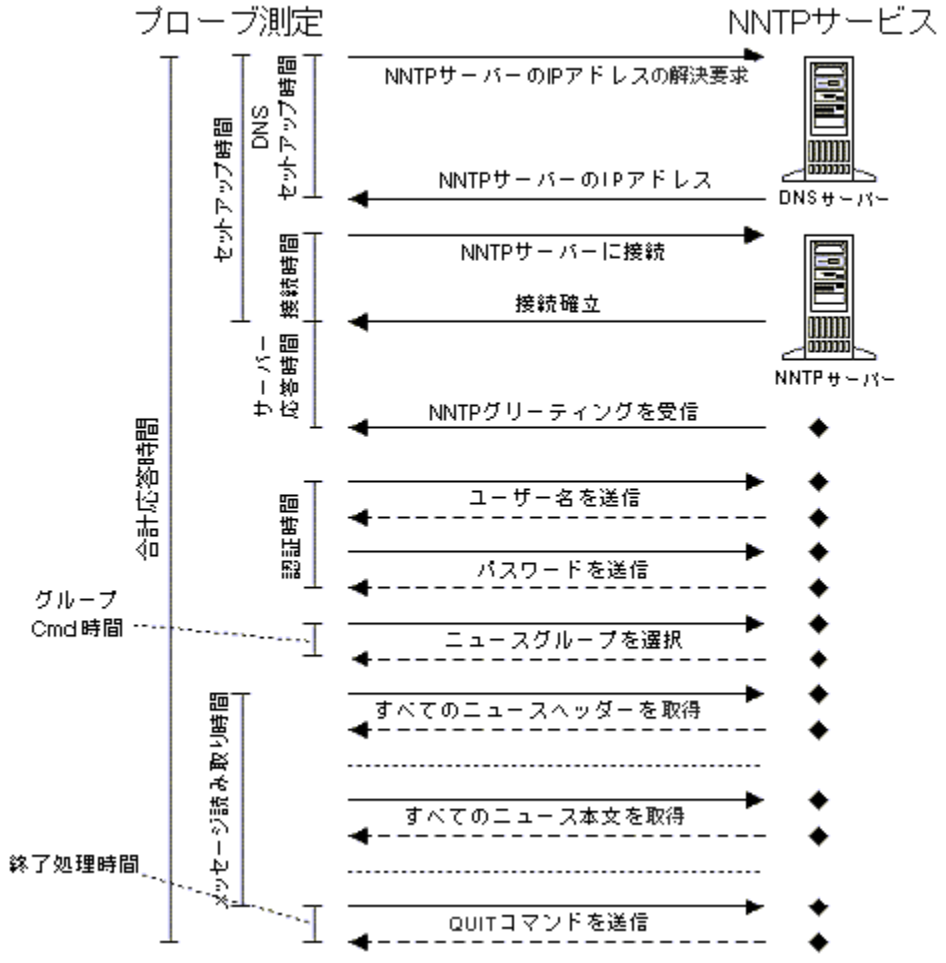


NNTP (Network News Transfer Protocol)

NNTP プローブは、一般的なニュースリーダーをエミュレートします。サーバーに認証を行った後 (認証を使用するかどうかは任意)、プローブは指定したニュースグループを選択し、すべてのメッセージヘッダーを取得します。ユーザーは、通常、ヘッダーを使用して件名行を表示し、メッセージの属性 (サイズ、識別子など) を取得します。ヘッダーをダウンロードした後、プローブは対応するメッセージテキストを取得して、ユーザーがメッセージを参照するのをシミュレートします。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。

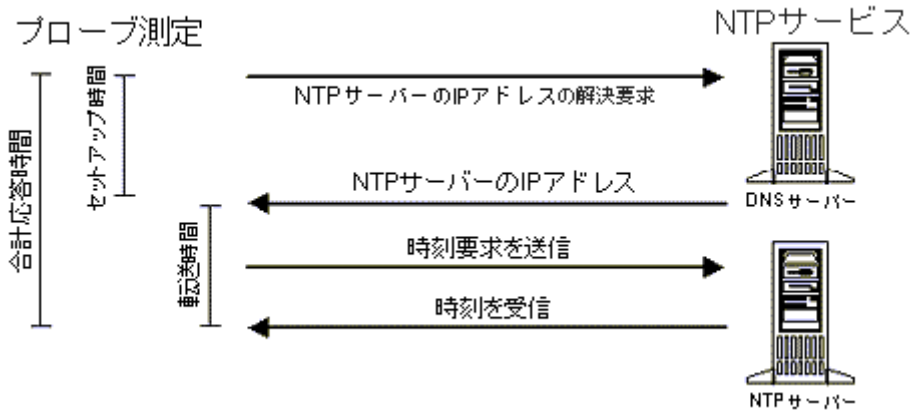


NTP (Network Time Protocol)

NTP (Network Time Protocol) は、コンピュータクライアントまたはサーバーの時間を、別のサーバーや参照タイムソース (無線または衛星レシーバーやモデムなど) に同期するのに使用します。NTP プローブは、設定した NTP ホストに時間要求を送信する時間と、NTP ホストの現在の時間を受信する時間を測定します。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



ODBC (Open Database Connectivity)

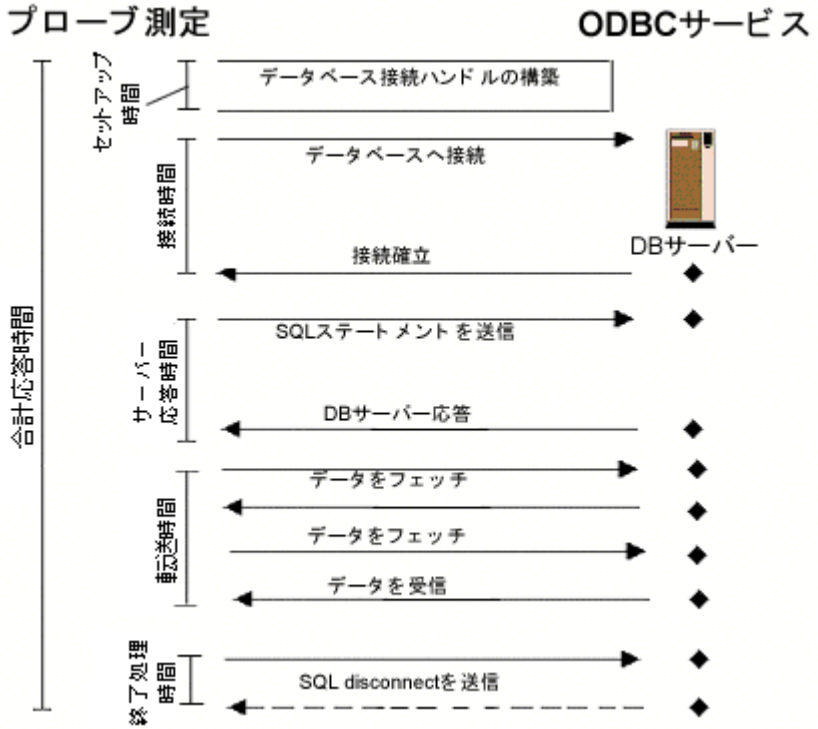
ODBC (Open Database Connectivity) サービスを監視するには、ODBC プローブを使用します。ODBC プローブは、一般的なデータベースプローブで、ユーザー定義の SQL Select ステートメントを使用してデータベースの可用性を監視します。**このプローブは、Windows システムでのみ動作します。**

ODBC プローブは、ローカルシステムまたはリモートシステムの ODBC データソースアドミニストレータで設定された、システムデータ ソース名 (DSN) の設定を使用してデータベースに接続します。

注記 : SQL Server の NT 認証を使用する場合は、ユーザー名とパスワードは空欄のままにします。代わりに、[HP Internet Services] サービスを、SQL Server データベースへのアクセス用に設定されたアカウントでログオンするように設定します。この設定には、ドメイン間におけるアカウントの信頼関係の設定も含まれます。また、NT 認証を使用する場合は、すべての ODBC データベースプローブに 1 つのアカウントを使用します。

ODBC プローブのプローブロケーションの設定時に、ODBC ネットワーク接続を作成し、**同時リクエスト数を 1 に設定します**。これにより、複数のデータベースプローブの起動時に ODBC マネージャが過負荷になるのを防ぐことができます。このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



POP3 (Post Office Protocol 3)

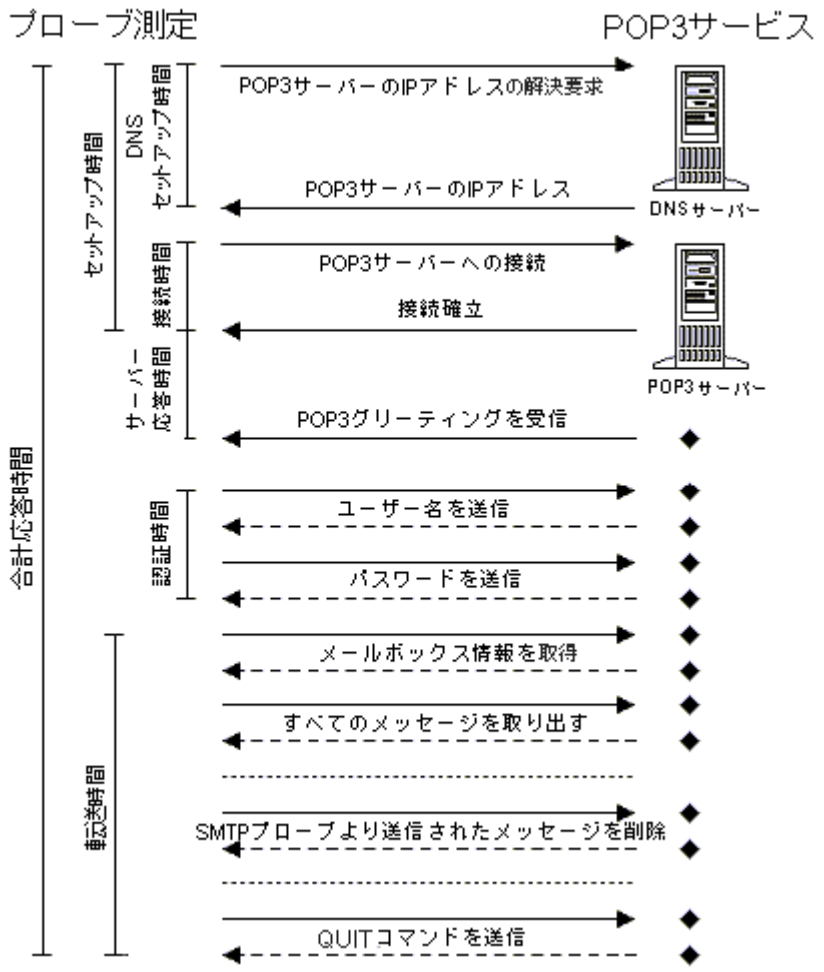
POP3 プローブは、ユーザーが電子メールをダウンロードする動作をエミュレートします。POP3 サーバーに接続した後、指定したユーザー名とパスワードでメールボックスが認証されます。UNIX サーバーでは、通常これは、ローカルユーザーのユーザー名とパスワードです。Windows (Exchange Server など) では、ユーザー名にはメールボックス名とアカウント名 (`MyAdminMailbox¥Administrator`) を含んでいる必要があります。

POP3 プローブは 、電子メールをサーバーから取り出してクライアントにダウンロードします (メッセージはサーバーに保存されません)。プローブは、メールボックス内のすべてのメールを検索し、OVIS-Timestamp ヘッダーフィールドをスキャンします。このフィールドは、SMTP プローブによって設定されます。このフィールドを検出すると、プローブはこのメッセージを削除用の内部リストに追加します。すべてのメッセージを読み取ると、プローブは OVIS-Timestamp を含んでいるメッセージを削除します。この削除メカニズムにより、SMTP プローブメッセージでメールボックスがいっぱいになることがなくなります。

Microsoft Exchange 2000/2003 Server を使用している場合は、POP3 プローブを使用してメールサービスを監視する上での留意事項があります。POP3 監視対象サービスに関する詳細は、設定マネージャのオンラインヘルプを参照してください。

SMTP および POP3 プローブ専用のメールボックスをセットアップすることを強くお勧めします。

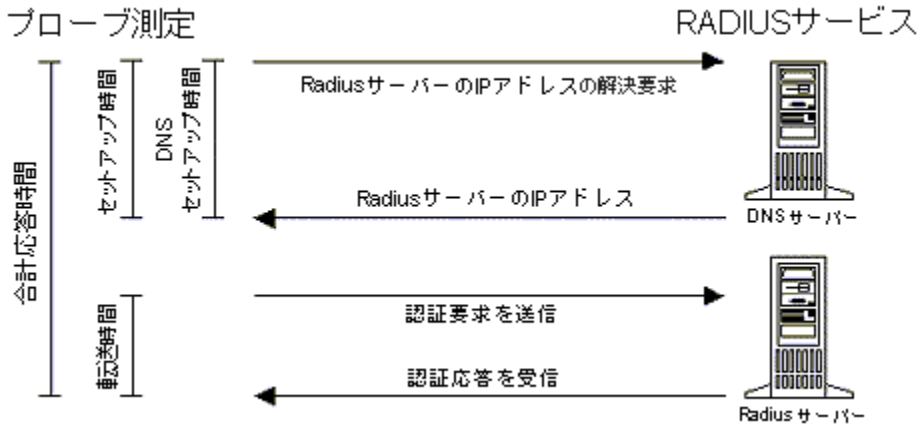
プローブが応答時間を測定するステップを以下の図に示します。



RADIUS (Remote Authentication Dial In User Service)

RADIUS プローブは、RADIUS 認証要求の合計応答時間を測定します。ホスト名または IP アドレスが解決されると、ユーザー名と暗号化されたパスワードを含む認証要求が、RADIUS サーバーに渡されます。RADIUS サーバーは要求を受信すると、送信元のホストが要求を行う許可を持っているかどうかを判断し、許可を持っている場合は指定したユーザーの認証を試みます。RADIUS サーバーは、信頼されているデータベースなどの既知の情報源から、ユーザーパスワードを取得し、共有シークレットを使用してそのパスワードを暗号化します。RADIUS サーバーが作成したこの暗号化パスワードが認証要求で送信された暗号化パスワードと一致すると、アクセス許可メッセージがプローブに返されます。UDP トランスポートプロトコルを使用して、RADIUS サーバーと通信します

プローブが応答時間を測定するステップを以下の図に示します。



RADIUS プローブは、ホスト名 /IP アドレスを解決するのに必要な時間と、アクセス許可メッセージの送受信時間を測定します。アクセス拒否メッセージがプローブに返された場合、RADIUS サーバーが利用できないとみなされますが、応答時間は測定されます。

RADIUS の公式ポートは 1812 ですが、一般的な RADIUS サーバーはポート 1645 を使用します。

このプローブは、現在以下のプロトコルをサポートしています。

- PAP (Password Authentication Protocol)
- CHAP (Challenge Handshake Authentication Protocol)

MS CHAP はサポートしていません。

共有シークレット、ユーザー名とパスワードを指定する必要があります。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

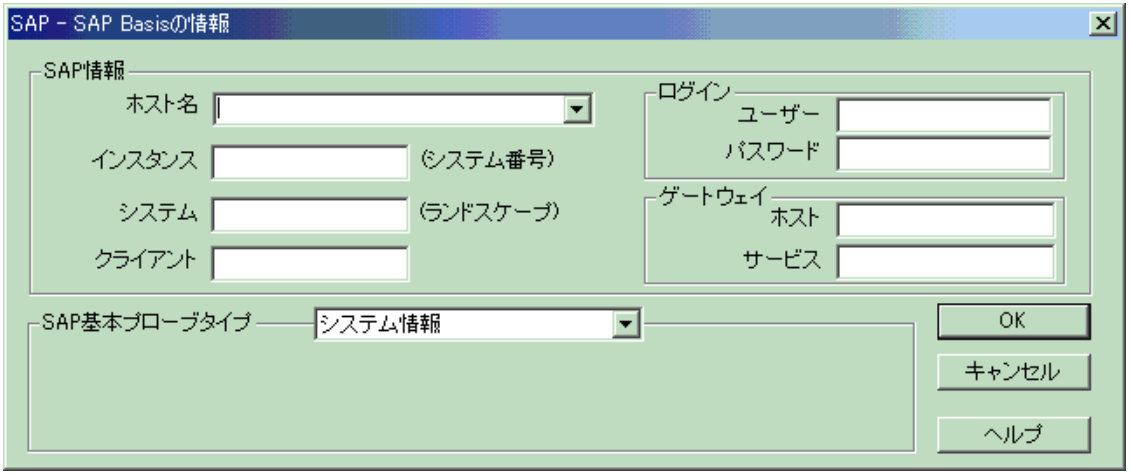
SAP Basis

SAP Basis (SAP_BASIS) プローブは、SAP アプリケーションサーバーの可用性を監視します。このプローブは、Windows および UNIX のプラットフォームで動作している SAP サーバーにアクセスできます。

このプローブは、2 種類の SAP 要求を作成するよう設定できます。

- **[システム情報]:** このタイプを選択すると、SAP ABAP/4 関数の RFC_SYSTEM_INFO (シンプルなコマンド要求) が SAP プローブによって作成されます。RFC_SYSTEM_INFO コマンドは、インタフェースが動作し、SAP アプリケーションサーバーが利用可能かどうかを判断する手段として使用されます。SAP ABAP/4 の関数 RFC_SYSTEM_INFO は、すべての SAP システムに含まれています。
- **[トランザクション]:** このタイプを選択すると、プローブが、ユーザー指定の SAP トランザクションコードを受け付けるように設定されます。プローブは、この要求 (RFC_CALL_TRANSACTION_USING) をサーバーに転送します。その後、プローブは、呼び出された SAP トランザクションを監視します。

次に示す図は [SAP - SAP Basis の情報] ダイアログです。



特定の属性を持つ SAP ユーザーを設定するか、そのような既存の SAP ユーザーを使用する必要があります。次の例では、SAP ユーザーの設定手順を説明します。S_A.ADMIN 認証により、[システム情報] タイプの SAP プローブに必要な権限が与えられます。[トランザクション] タイプの SAP プローブでは、RFC 関数呼び出しを行う権限も必要です。

また、[トランザクション] タイプの SAP プローブについては、RFC 転送先を SAP トランザクションの **sm59** で定義する必要があります。このトランザクションでは、RFC 接続を許可された SAP プローブのホストを指定します。

SAP ユーザーの設定

1. SAP R/3 にログインします。
2. トランザクション **/nsu01** を呼び出します。
3. ITOUSER という名前の新規ユーザーを作成し、以下のパラメータを設定します。この ITOUSER の例は、OpenView Operations SAP Smart Plug-in の場合と同じです。このユーザーをすでに設定している場合は、そのまま使用できます。あるいは、以下の属性が設定されていれば、別のユーザー名を使用することもできます。

   [User Type]: CPIC/System。このユーザータイプは、DIALOG タイプに相反して、パスワードの有効期限が切れないことが保証されます。

   [Initial Password]: HPSAP_30 *以外*の、SAP で受け付けられる任意の値、およびユーザー用パスワードとして使用する値。イニシャルパスワードの HPSAP_30 は、OpenView Operations SAP Smart Plug-in の設定と同じです。別のパスワードも使用できます。

   [Authorization]:

   S_A.ADMIN (SAP バージョン 3.1x、4.x の場合)

   [User Roles]:

   SAP_ALL_DISPLAY (SAP バージョン 4.6C のみ)

   BC、CA、HR を除くすべてのモジュールを表示する権限

   SAP_BC_BASIS_ADMIN (SAP 6.10/6.20 以降)

4 SAP バージョン 6.10 または 6.20 (Web アプリケーションサーバー) を使用している場合は、さらに次に示す操作を行う必要があります。

   a トランザクション **/nsu02** を呼び出します。

   b 新規プロファイルを、たとえば、OpenView Operations SAP Smart Plug-in で使用している ZSPIRFC という名前で作成し、このプロファイルに次のオブジェクトと権限を割り当てます。このプロファイルが必要なのは、OVIS SAP プローブが、プローブ実行中に SAP RFC 関数を呼び出す場合に、ここで定義する権限を必要とするためです。

オブジェクト	権限プロファイル
S_RFC	S_RFC_ALL
S_RFC_TAB	&_SAP_ALL
S_C_FUNCT	&_SAP_ALL
S_DATASET	&_SAP_ALL

   c このプロファイルを有効にし、これを、すでに作成した SAP プローブユーザーに割り当てます。

5 作成したユーザーとして SAP にログインします。

6 パスワードの変更を求めるプロンプトが表示されます。新しいパスワードとして、HPSAP_30 またはパスワードとして使用する値を入力します。

SAP プローブの設定

プローブの設定では、以下を入力する必要があります。

- SAP インスタンス (システム番号とも呼ばれます。インスタンスは、1 つまたは複数のサービスを提供する SAP システムのコンポーネントを組み合わせた管理エンティティです。インスタンス内のサービスは、同時に開始および停止されます。デフォルトは「00」です。
- システムランドスケープ内でシステムを表す一意の名前 (3 文字)。たとえば、DEV、QAS、PRD はそれぞれ、開発 (Development)、品質保証 (Quality Assurance)、生産 (Production) を表します。
- クライアント番号。システム内の各クライアントは独立しています。各クライアントは独自のデータ環境を持つため、固有のマスタデータやトランザクションデータ、割り当てられたユーザーのマスターレコードやアカウントのチャート、および特定のカスタマイズパラメータがあります。

- 前述の [トランザクション] タイプのプローブを選択した場合は、SAP トランザクションも指定します。SAP R/3 システムの各機能にはトランザクションコードが割り当てられます。たとえば、顧客のマスターデータを表示する場合は、トランザクションコード FD03 が使用されます。次の例は、一部のモジュールに使用されるトランザクションを示しています。

  SD (Sales and Distribution: 販売流通)　- VA01、VA02、VA21

  MM (Material Management: 資材管理)　- MB51、MB59

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

Script (汎用スクリプト)

Script プローブは、特定のスクリプトを実行し、可用性と応答時間を監視します (追加メトリックを収集する Script プローブを設定する方法に関しては、259 ページの「追加メトリックの収集」を参照してください)。Script プローブを使用すれば、カスタムプローブを作成することなく、スクリプトを通じて汎用アプリケーションを監視できます。スクリプトは、VBScript、Javascript、または Perl で記述します。また、バッチ処理、コマンド、および UNIX シェルを使用して実行します。

ファイルの配布

スクリプトまたはデータファイルへの絶対パスを使用するか、**配布マネージャ**を使用してリモートシステムとローカルシステムにファイルを配布します。配布マネージャを使用するには、プローブを作成する前に、OVIS 管理サーバーの <install dir>¥newconfig¥distrib¥ ディレクトリの下の適切なディレクトリにスクリプトとデータファイルを置く必要があります (適切なサブディレクトリについては、以下を参照してください)。設定を保存すると、¥newconfig¥distrib¥ にあるファイルがプローブシステムの <data dir>¥bin¥instrumentation¥probe¥scripts ディレクトリにコピーされます (Windows の場合は ¥、UNIX の場合は / を使用)。配布されるのはファイルのみで、ディレクトリは配布されない点に注意してください。

プローブが新しい設定を取得すると、配布マネージャは以下のディレクトリを対象にファイルを検索するため、配布先のシステムに応じて、これらのディレクトリにスクリプトとデータファイルを置いておく必要があります。

newconfig¥distrib¥all - all ディレクトリには、すべてのプラットフォームとプローブロケーションで有効なファイルを置きます。

newconfig¥distrib¥platform¥{Windows|HPUX|Linux|Solaris} - Windows、HPUX、Linux、Solaris ディレクトリには、プラットフォームに固有のファイルを置きます。プローブは、プローブが動作中のオペレーティングシステム用のファイルのみを取得します。

newconfig¥distrib¥location¥{ 設定マネージャで定義したプローブロケーション } - location ディレクトリの下に、設定マネージャで設定したプローブロケーションの名前 (通常は完全修飾ホスト名) の付いたディレクトリを作成できます。たとえば、プローブロケーションが mysystem.mydomain.com の場合、これと同じ名前の mysystem.mydomain.com というディレクトリを作成し、このディレクトリにファイルを置きます。

これらのディレクトリは、OVIS によって自動的に追加、削除、または変更されることはありません。これらのディレクトリ名が OVIS で設定した名前と一致していることを確認する必要があります。このため、all ディレクトリと platform ディレクトリにファイルを置き、絶対的に必要な場合にのみ location ディレクトリを使用することをお勧めします。また、ローカルシステムは、実際には OVIS 管理サーバーシステムの完全修飾ドメイン名

になります。たとえば、ローカルシステムにだけファイルを配布するには、管理サーバー名が ovis.domain.com の場合は、ovis.domain.com というディレクトリを作成します。

Script プローブの設定

設定マネージャの [スクリプトサービス] ダイアログボックスで Script プローブを設定します。スクリプトを実行するコマンド (適切な場所や必要なパラメータなど) を入力します。配布されたスクリプトファイルは、上記で説明したとおりに、Script プローブを実行するすべてのプローブシステムの <data dir>¥bin¥instrumentation¥probe¥scripts ディレクトリにコピーされています。この方法で配布されたスクリプトの場合は、スクリプトの適切な場所に相対パス scripts¥<script name> を使用できます。たとえば、スクリプト test.pl は、<install dir>¥newconfig¥distrib¥all ディレクトリにコピーされており、プローブの設定には次の相対パスを使用できます。

```
c:¥Perl¥bin¥Perl.exe scripts¥test.pl
```

アプリケーションまたはプログラムを起動し、可用性を示す適切な値 (1 または 0) を返し、エラー条件を処理するスクリプトを作成する必要があります。デフォルトでは、スクリプトが完了すると利用可能と判断されます。Script プローブがタイムアウト値に達した場合、利用不可と判断されます。可用性は、パターン検索を適用するか、終了コードを確認して判断することも可能です。

Script プローブは、スクリプトまたはアプリケーションに関連付けられた子プロセスを管理しません。Script プローブがタイムアウト値に達してスクリプトまたはアプリケーションを終了した場合は、そのスクリプトまたはアプリケーションに関連付けれらた子プロセスを手動で終了する必要があります。

Script プローブの設定時に、スクリプトの出力に適用するパターン検索を指定できます。可用性を判断するときにプローブがスクリプトの終了コードをチェックするように指定できます。プローブが対話型セッション (つまり、スクリプトを実行する前にユーザーがログオンしたこと) をチェックするように指定できます。OVIS の内部パラメータをスクリプトに追加して、結果をログに記録しないように指定できます。

Script プローブを別のログオンセッションで実行する場合は、認証に必要なユーザーとパスワードを設定します。このログオンセッションには特定の権限が必要です (これらのユーザー権限の設定については、設定マネージャのオンラインヘルプを参照してください)。

Script プローブで実行されるスクリプトは、特に UNIX/Linux で、環境設定によって影響されます。スクリプトが、OVIS スケジューラ (root .profile) で定義される環境で、実行するように設定されていることを確認してください。この OVIS スケジューラで定義される環境は、スクリプトが作成された環境 (ユーザーの login .profile) と異なる可能性があります。'en_US' または 'C' のロケール設定などが、影響を受ける環境変数の例としてあげられます。

アプリケーションテストツールスクリプト、またはマルチステップのトランザクションを実行する他のスクリプトを起動するために Script プローブを使用する場合では、2 番目のスクリプトとして結果ファイルスクリプトを指定して起動し、メインスクリプトまたはプログラムからの出力ファイルを分析することができます。詳しくは、以下の「結果ファイルの使用」を参照してください。マルチステップの トランザクション用ラベルを「顧客名 : サービスグループ名」に設定することもできます。

マルチステップのトランザクションには、サービスグループあたり 1 つの監視対象サービスのみを使用することをお勧めします。ステップの最大数は 100 です。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

結果ファイルの使用

マルチステップのトランザクションで、スクリプトに結果 (たとえば、StepResponseTime) を結果ファイルに送信させることができます。またはスクリプトが画面出力可能なら、結果を STDOUT に送信させることができます (ファイルに書込みしない)。Script プローブはどちらか一方の方法で出力をキャプチャします。設定マネージャの [スクリプトサービス] ダイアログで次のように設定します。

- 結果ファイルに送信する場合は、[結果ファイルスクリプト] フィールドに結果ファイルを入力します。
- スクリプトが画面に出力する場合は、[結果ファイルスクリプト] フィールドにスクリプトの名前をそのまま入力します。

結果ファイルまたは出力のフォーマットと例

結果ファイルのエントリの形式 (または画面への出力) は次の通りです。(これらエントリの定義に関しての詳細は、257 ページの「結果ファイル出力の注意事項」を参照してください。

マルチステップのスクリプト用 :

StepName
StepSetupTime
StepTransferTput
StepMetric_1
StepMetric_2
StepMetric_3
StepMetric_4
StepMetric_5
StepMetric_6
StepMetric_7
StepMetric_8
ErrorInfo
StepTimestamp
StepAvailability
StepResponseTime

最終メトリック用 (可用性と応答時間が必要):

Target
SetupTime

TransferTput
Metric_1
Metric_2
Metric_3
Metric_4
Metric_5
Metric_6
Metric_7
Metric_8
ErrorInfo
Timestamp
Availability
ResponseTime

これらのステップメトリックと最終 メトリックは、大文字小文字を区別するので、上記と全く同じ文字を使用する必要があります。Metric_1 から Metric_8 と StepMetric_1 から StepMetric_8 はスクリプトが収集する追加のユーザー定義メトリック用です。設定方法に関する詳細は、259 ページの「追加メトリックの収集」を参照してください。

結果ファイルの例

```
################ win_script3.sh

StepName=Test_00
StepAvailability=1
StepResponseTime=1.51
StepName=Test_01
StepAvailability=1
StepResponseTime=3.51
StepName=Test_02
StepAvailability=1
StepResponseTime=17.563451
StepName=Test_03
StepAvailability=1
StepResponseTime=22.7656542491
Availability=1
ResponseTime=42.16243
##############
```

結果ファイル出力の注意事項

結果ファイル出力に関する次の注意事項を参照してください。

- 結果ファイル (または出力) のパラメータは任意の順序になります。ただし、Script プローブは、ステップまたは最終要約のいずれかで**測定完了**を検出すると、ステップまたは測定が終了したとみなし、そのステップの追加出力を実行しません。ステップの測定完了のストリングは、ステップ名、ステップ応答時間、およびステップ可用性から構成され、最終トランザクションの測定完了は、応答時間と可用性から構成されます。
- スクリプトが出力対象を渡す場合は、**Target** パラメータを使用します。
- 結果が応答時間の構成要素としてセットアップ時間を含む場合は、**SetupTime** を使用します。結果が転送処理時間の測定を含む場合は、**TrasferTput** を使用します。
- 結果に **ErrorInfo** がある場合は、結果の最初または中間で出力されていることを確認してください。最後にある場合 (Script プローブが測定完了を見つけた後) は、Script プローブは ErrorInfo を次のステップの一部として含めてしまいます。
- 不具合がない場合は、スクリプトが ErrorInfo を出力していないことを確認します。
- また、ErrorInfo は 256 文字以下、StepName は 250 文字以下である必要があります。この制限を超えた場合は、フィールドが切り捨てられるか Script プローブが実行できなくなります。
- **Timestamp** と **StepTimestamp** によって、外部タイムスタンプを含むことができます。Timestamp と StepTimestamp の形式はエポックタイム (1/1/70 からの経過秒数) です。次の VB スクリプトは日付をタイムスタンプ形式に変換するのに使用されます。

```
TimeZoneSec = 28800 'PST

DateToEpoch = DateDiff("s", "00:00:00 1/1/1970", Now()) +
TimeZoneSec
```

- **Availability と ResponseTime** では、スクリプトはトランザクションの合計を加算する必要があります (すべてのステップの概要のまとめ)。Script プローブは、この計算を行いません。また可用性と応答時間は、結果出力の最後の行である必要があります。

- ステップのメトリックを収集する場合は、**StepMetric** が使用されます (たとえば、StepMetric_1)。すべてのステップの測定合計も報告する場合は、スクリプトですべてのステップの概要のまとめを、最終メトリックとして指定されたメトリック値 (たとえば、Metric_1) に設定する必要があります。Script プローブは計算を一切行いません。

追加メトリックの収集

Script プローブは、カスタマイズなしで可用性と応答時間のメトリックを収集します。実行しているスクリプトに基づいて追加メトリックを収集するように Script プローブを設定することもできます。

追加メトリックの収集を開始するための処理を次に示します (これらのステップの詳細は、次を参照してください)。

1. どのメトリックを収集するかを決定します。
2. スクリプトがそれらのメトリックを収集し、プローブで取得できるよう正しい形式で結果を出力するかを確認します。詳しくは、260 ページの「追加のメトリックを出力する結果スクリプト」を参照してください。
3. メトリックラベル、単位、および要約を必要とする個別のステップメトリックがあるかどうかを決定します。Script プローブは計算を一切しないので最終メトリックを出力するスクリプトによって要約が行われる必要があります。
4. Script プローブのカスタマイズ SRP ファイルを作成します。詳しくは、261 ページの「追加メトリック用の SRP ファイル」を参照してください。
5. スクリプトを、配布に備えて適切な場所に置きます。
6. 設定マネージャから SRP ファイルを読み込みます。詳しくは、269 ページの「SRP ファイルのロード」を参照してください。
7. Script プローブを設定します。読み込んだ各 Script プローブの SRP ファイルで、プローブタイプ選択画面にそれぞれのプローブタイプが一覧表示されます。詳しくは、270 ページの「プローブにメトリック収集を設定」を参照してください。

レポート (ダッシュボードのレポートワークスペースからの) はこれらのカスタマイズ Script プローブで使用できないので注意してください。

追加のメトリックを出力する結果スクリプト

ユーザー定義の追加メトリックを収集する Script プローブでは、正しい形式でメトリックを出力する結果スクリプトを作成する必要があります。作成したスクリプトが画面に出力できるのであれば、メトリック結果を STDOUT に送信させるか、または結果ファイルに書き込ませることができます。結果ファイルの形式に関する詳細は、256 ページの「結果ファイルまたは出力のフォーマットと例」を参照してください。

次の例の .vbs スクリプトを参照してください (合計ディスクサイズ、ディスクの合計空き容量、およびディスク未使用領域の割合を収集します)。

追加メトリックを収集するスクリプト例

```
strComputer = "."

totalsize = 0.0
totalfree = 0.0
totalAvail= 0.0
probeAvail= 0

Set objWMIService = GetObject("winmgmts:" _
    & "{impersonationLevel=impersonate}!\\" _
    & strComputer & "\root\cimv2")
Set colDisks = objWMIService.ExecQuery _
    ("Select * from Win32_LogicalDisk where DeviceID = 'c:'")
For Each objDisk in colDisks
    freePercent = 0.0
    if( objDisk.Size > 0 ) then
       freePercent = ((objDisk.FreeSpace)/(objDisk.Size))
       totalsize = totalsize + objDisk.Size
       totalfree = totalfree + objDisk.FreeSpace
    end if
Next

Wscript.Echo "Target=Drive(c)"
Wscript.Echo "ResponseTime=0"
Wscript.Echo "Metric_1=" _
   & totalsize

Wscript.Echo "Metric_2=" _
   & totalfree

if( totalsize > 0 ) then
```

```
   totalAvail = (totalfree/totalsize) * 100
end if

if( totalAvail > 0 ) then
   probeAvail= 1
end if

Wscript.Echo "Metric_3=" _
   & totalAvail

Wscript.Echo "Availability=" _
   & probeAvail

wscript.Quit(0)
```

追加メトリックがある結果ファイルの例

上記スクリプト例が実行されると、結果は次のようになります。

```
***-*Example output from script when excuted.
----------------------------------------
Target=Drive(c)
ResponseTime=0
Metric_1=60003868672
Metric_2=38358384640
Metric_3=63.9265192210839
Availability=1
```

追加メトリック用の SRP ファイル

追加のユーザー定義の Script プローブメトリックをダッシュボードに表示するには、メトリックをカスタマイズ Script プローブ SRP ファイルに追加し、SRP ファイルを OVIS に読み込見込ませる必要があります。(269 ページの「SRP ファイルのロード」を参照。) SRP ファイルを読み込ませる場合に構文チェックがないので、作成する場合に注意する必要があります。問題が発生した場合は、`trace.reload` を使用して読み込んだ内容を確認することができます。

SRP ファイルを読み込んだ後で、プローブ定義を変更しても、`ovtomcatA` サービスが更新されるまでダッシュボードに反映されないので注意してください。サービスを更新するには、コマンド行で次を実行します。

```
ovc -restart ovtomcatA
```

SRP ファイルにはプローブ、プローブパラメータ、収集されるメトリック、および SLO やアラームなどのデフォルト条件が記述されています。カスタマイズ Script プローブの SRP ファイルのレイアウトに関しては、以下の「スクリプト SRP ファイルの例 1」を参考にしてください。

カスタマイズ Script プローブ SRP ファイルからメトリックを追加または削除することができます。SRP ファイルを変更した場合は、SRP ファイルを再度読み込んで `ovtomcatA` サービスを再起動して変更を有効にしてください。269 ページの「SRP ファイルのロード」を参照してください。

Script プローブ SRP ファイルは複数の Script プローブメトリック定義を持つことができます。実行を予定している Script プローブごとに Script プローブ SRP ファイルを作成することができます。

Script プローブ SRP ファイルで変更することができないキー項目は、`PROBE: probeScript` です。これにより Script プローブであることを OVIS に伝えるためです。また SRP ファイルの PARAMETER の値も変更することができません。

たとえば、メトリックを追加するには、以下の行を SRP ファイルに追加します。

METRIC: DISK_METRIC

LABEL: Disk Free Space

STDMETRIC: M2

UNITS: MBytes

FORMAT: 0.0000

DEFAULT_CONDITION: <

METRIC の値は収集の対象を示します。LABEL は、ダッシュボードに表示される名前です。STDMETRIC の値は、M1 ～ M8 です。UNITS 値はメトリックの単位です。使用可能な単位には、%、秒、回、個、K バイト / 秒、ステータスコード、トランザクション / 秒、トランザクション失敗 / 秒、バイト (平均)、メガバイト / 分、M バイトがあります。DEFAULT_CONDITION は、"<" または ">" で、SLO が値より大きい (たとえば、95% より大きい可用性)、または値より小さい (たとえば、5 秒以下の応答時間) かどうかを識別します。

スクリプト SRP ファイルの例 1

「追加メトリックを収集するスクリプト例」で示したスクリプトに対応する Script プローブ SRP ファイルの例を次に示します。Script プローブ名は SCRIPT_DISK です。

```
# ############################################################
# OpenView Internet Services Example script probe SRP file
############################################################
PACKAGENAME: DiskSpace

PROBENAME:  SCRIPT_DISK
    DESCRIPTION:    SCRIPT_DISK_SPACE - WMI Disk space
    PROBEMETRICLIST:    IOPS_SCRIPT_DISK
    IDENTIFIER:     HOST
    INSTANCEID:     TARGET
    DEFAULT_TARGET:
    DEFAULT_PORT:
    PROBE:          probeScript
    TRANSPORT:
    PARAMETER1:     script
    PARAMETER2:     pattern
    PARAMETER3:     patternConfig
    PARAMETER4:     chkstat
    PARAMETER5:     ofile
    PARAMETER6:     options
    PARAMETER7:     username
    PARAMETER8:     password
    END_PROBENAME:


PROBEMETRICS:   IOPS_SCRIPT_DISK

    METRIC:     AVAILABILITY
    UNITS:  Percent
    DEFAULT_CONDITION:  >
    DEFAULT_SERVICE_LEVEL: 90.000
    DEFAULT_WARNING:    90.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
    DEFAULT_MESSAGE:    SCRIPT Service for <TARGET> is unavailable

    METRIC:     RESPONSE_TIME
    UNITS:  Seconds
    DEFAULT_CONDITION:  <
    DEFAULT_SERVICE_LEVEL: 2.000
    DEFAULT_WARNING:    4.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
    DEFAULT_MESSAGE:    SCRIPT Service RESPONSE_TIME is slow
(<VALUE> vs <THRESHOLD>) on <TARGET>
```

```
    METRIC:     SETUP_TIME
    UNITS:  Seconds
    DEFAULT_CONDITION:  <
    DEFAULT_WARNING:    3.000
    DEFAULT_BASELINE:   80.000
    DEFAULT_DURATION:   600
   DEFAULT_MESSAGE:    Script 'x' is slow  (<VALUE> vs <THRESHOLD>)
on <TARGET>

    METRIC:     TRANSFER_TPUT
    UNITS:  KBytes/Sec
    DEFAULT_CONDITION:  >

    METRIC:     DISK_SIZE
    LABEL: Disk Size
    STDMETRIC:  M1
    UNITS:  MBytes
    FORMAT: 0.000
    DEFAULT_CONDITION:  <

    METRIC:     FREE_SPACE
    LABEL: Free Space
    STDMETRIC:  M2
    UNITS:  MBytes
    FORMAT: 0.000
    DEFAULT_CONDITION:  <

    METRIC:     PERCENT_AVAILABLE
    LABEL: Percent Available
    STDMETRIC:  M3
    UNITS:  Percent
    FORMAT: 0.000
    DEFAULT_CONDITION:  >

    END_PROBEMETRICS:
```

スクリプト SRP ファイルの例 2

別の Script プローブ SRP ファイルの例を次に示します。さまざまな条件での結果ファイルの例が、この例の後に示されています。

この SRP ファイルには、FORMAT、COMPOSITE_METRIC、COMPOSITE_ORDER のパラメータが使用されています。これらのパラメータは SRP ファイルに手動でのみ追加することができます (設定マネージャからは入力

できません)。たとえば、積み上げ縦棒グラフを作成するといったパラメータは標準メトリックでは設定済みですが、Script プローブのユーザー定義メトリックでは、カスタマイズ Script プローブ SRP ファイルに指定する必要があります。

FORMAT は、メトリックの表示形式を設定するのに使用されます (たとえば、FORMAT: 0.000 は、小数点 3 桁の数字を表示します)。FORMAT の値は、Java フォーマッタ仕様に準拠します。

COMPOSITE_METRIC と COMPOSITE_ORDER は、OVIS ダッシュボードで積み上げ縦棒グラフを作成するために使用されます。COMPOSITE_METRIC は、親メトリック (通常は応答時間) を指定し、COMPOSITE_ORDER は、棒グラフ内のメトリックの位置を指定します。

```
############################################################
# OV internet services Example SRP File
############################################################

PROBENAME: TEST_PROBE_ALPHA
    DESCRIPTION:      Test - Test Probe Alpha
    PROBEMETRICLIST:  IOPS_TEST_PROBE_ALPHA
    IDENTIFIER:       URL
    INSTANCEID: URL
    DEFAULT_TARGET:
    DEFAULT_PORT:
    PROBE:       probeScript
    TRANSPORT:
    PARAMETER1:   script
    PARAMETER2:   pattern
    PARAMETER3:   patternConfig
    PARAMETER4:   chkstat
    PARAMETER5:   ofile
    PARAMETER6:   options
    PARAMETER7:   username
    PARAMETER8:   password
    END_PROBENAME:

PROBEMETRICS:     IOPS_TEST_PROBE_ALPHA

    METRIC:     AVAILABILITY
    UNITS:    Percent
    DEFAULT_CONDITION:    >
    DEFAULT_SERVICE_LEVEL: 90.000000
    DEFAULT_WARNING:  90.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
```

```
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    80.000000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service for <TARGET> is unavailable

    METRIC:    SETUP_TIME
    UNITS:    Seconds
    DEFAULT_CONDITION:    <
    DEFAULT_SERVICE_LEVEL: 1.000000
    DEFAULT_WARNING:  3.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    80.000000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service SETUP_TIME is slow  (<VALUE> vs
<THRESHOLD>) on <TARGET>

    METRIC:    METRIC_1_TIME
    STDMETRIC:    M1
    LABEL:   Transfer Time
    UNITS:   Seconds
    FORMAT:  0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        1
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL:   1.500
    DEFAULT_WARNING:    2.000
    DEFAULT_BASELINE:      80.000
    DEFAULT_DURATION:      600
    DEFAULT_MESSAGE: Test Service METRIC_1_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    METRIC_2_TIME
    STDMETRIC:    M2
    LABEL:    Auth Time
    UNITS:    Seconds
    FORMAT:   0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        2
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL:   1.500
    DEFAULT_WARNING:    2.000
    DEFAULT_BASELINE:     80.000
    DEFAULT_DURATION:     600
```

```
    DEFAULT_MESSAGE: Test Service METRIC_2_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    METRIC_3_TIME
    STDMETRIC:    M3
    LABEL:    Send Time
    UNITS:    Seconds
    FORMAT:   0.000
    COMPOSITE_METRIC:       RESPONSE_TIME
    COMPOSITE_ORDER:        3
    DEFAULT_CONDITION:    <
    DEFAULT_SERVICE_LEVEL:  1.500
    DEFAULT_WARNING:  2.000
    DEFAULT_BASELINE:    80.000
    DEFAULT_DURATION:    600
    DEFAULT_MESSAGE: Test Service METRIC_3_TIME is slow  (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:     RESPONSE_TIME
    UNITS:     Seconds
    DEFAULT_CONDITION:     <
    DEFAULT_SERVICE_LEVEL: 2.000000
    DEFAULT_WARNING:  0.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    0.000000
    DEFAULT_DURATION:    600
   DEFAULT_MESSAGE:    Test Service RESPONSE_TIME is slow (<VALUE>
vs <THRESHOLD>) on <TARGET>

    METRIC:    TRANSFER_TPUT
    UNITS:     Bytes/Sec
    DEFAULT_CONDITION:     >
    DEFAULT_SERVICE_LEVEL: 0.000000
    DEFAULT_WARNING:  0.000000
    DEFAULT_MINOR:    0.000000
    DEFAULT_MAJOR:    0.000000
    DEFAULT_CRITICAL:    0.000000
    DEFAULT_BASELINE:    0.000000
    DEFAULT_DURATION:   0
    DEFAULT_MESSAGE:

    END_PROBEMETRICS:
```

次の結果ファイルは、上に示されている SRP ファイルに一致する架空スクリプトからの出力の例です。最初の例はステップ 2 に問題があり、プローブが可用性と応答時間に 0 (ゼロ) を返す場合の結果を示しています。

結果例 1

```
Target=MyServer.test@80_To_HisServer.Test@90
StepSetupTime=0.001
StepTransferTput=123
StepMetric_1=1.5
StepMetric_2=5.5
StepMetric_3=9.5
StepResponseTime=16.501
StepAvailability=1
StepName=Connect To MyServer@80
StepMetric_1=0
StepMetric_2=0
StepMetric_3=0
StepResponseTime=0
StepAvailability=0
StepName=Connect To HisServer@90
ResponseTime=0
ErrorInfo=System down, error returned is x00005, status 500.
Metric_1=0 Metric_2=0 Metric_3=0 Availability=0
```

結果例 2

2 番目の例では、すべてのステップが使用できる場合の結果を示します。

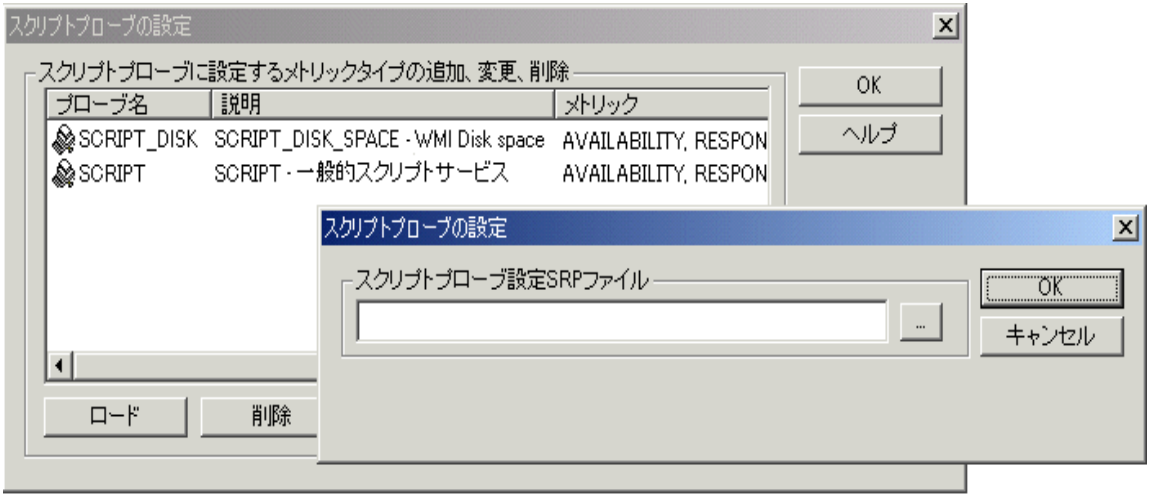
```
Target=MyServer.test@80_To_HisServer.Test@90
StepSetupTime=0.001
StepTransferTput=123
StepMetric_1=1.5
StepMetric_2=5.5
StepMetric_3=9.5
```

```
StepResponseTime=16.501
StepAvailability=1
StepName=Connect To MyServer@80
StepSetupTime=0.001
StepTransferTput=345
StepMetric_1=1.33
StepMetric_2=2.33
StepMetric_3=3.34
StepResponseTime=7.000
StepAvailability=1
StepName=Connect To HisServer@90
ResponseTime=23.502
Metric_1=2.83
Metric_2=7.83
Metric_3=12.84
Availability=1
```

SRP ファイルのロード

Script プローブ SRP ファイルを作成したら、設定マネージャで、[**ファイル**] > [**設定**] > [**スクリプトプローブメトリック**] を選択し、ダイアログで SRP ファイルを OVIS に読み込みます。SRP ファイルを読み込む場合に構文チェックはされません。問題が発生した場合は、`trace.repload` を使用して読み込まれた内容を確認します。

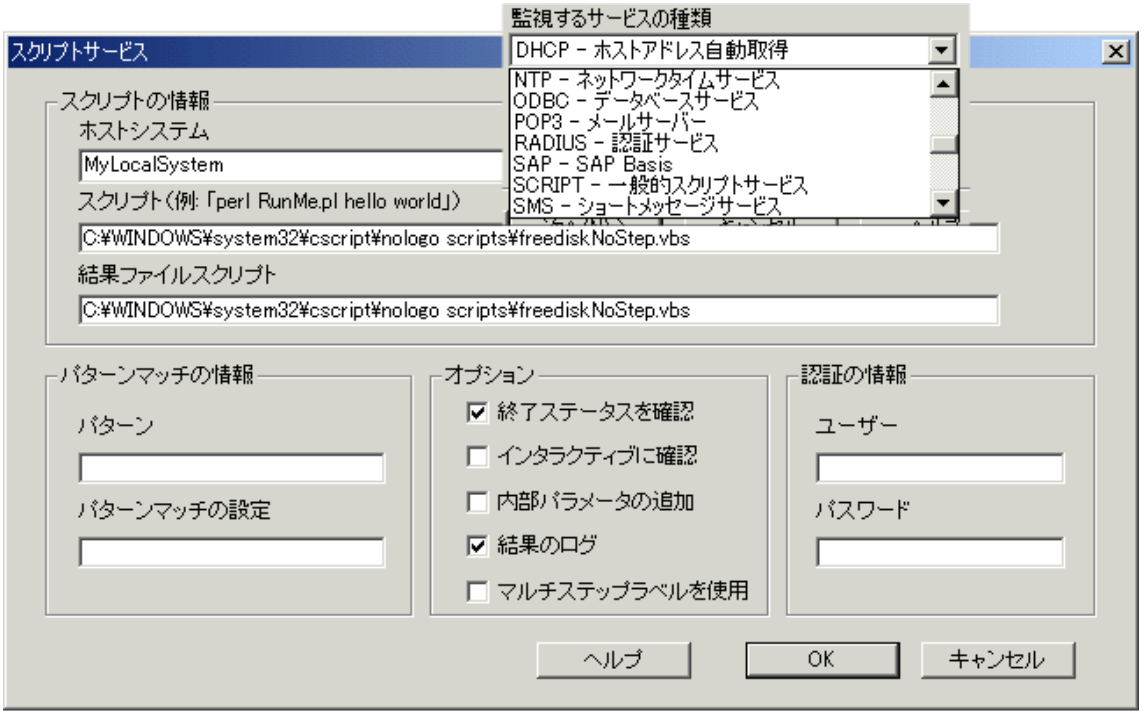
SRP ファイルを読み込んだ後でプローブ定義を変更しても `ovtomcatA` サービスが更新されるまでダッシュボードに反映されません。サービスを更新するには、コマンド行で `ovc -restart ovtomcatA` を実行します。



プローブにメトリック収集を設定

作成したカスタマイズ Script プローブ SRP ファイルを読み込んだ後で、設定マネージャで Script プローブを設定できます。

選択するプローブタイプは、SRP ファイルで設定したプローブの名前になります。上記の例では `PROBENAME: SCRIPT_DISK` です。次のスクリーンショットを参照してください。


監視するサービスの種類
スクリプトサービス
DHCP - ホストアドレス自動取得
NTP - ネットワークタイムサービス
ODBC - データベースサービス
POP3 - メールサーバー
RADIUS - 認証サービス
SAP - SAP Basis
SCRIPT - 一般的スクリプトサービス
SMS - ショートメッセージサービス
スクリプトの情報
ホストシステム
MyLocalSystem
スクリプト(例:「perl RunMe.pl hello world」)
C:¥WINDOWS¥system32¥cscript¥nologo scripts¥freediskNoStep.vbs
結果ファイルスクリプト
C:¥WINDOWS¥system32¥cscript¥nologo scripts¥freediskNoStep.vbs
パターンマッチの情報
パターン
パターンマッチの設定
オプション
終了ステータスを確認
インタラクティブに確認
内部パラメータの追加
結果のログ
マルチステップラベルを使用
認証の情報
ユーザー
パスワード
ヘルプ
OK
キャンセル

その他の Script プローブの例

コンソールに "Hello World" をエコーし、終了時に終了コード 0 を返す VBScript の例を以下に示します。

helloworld.vbs ファイルを作成し、以下のコードを追加して、OVIS 管理サーバーの `<install dir>¥newconfig¥distrib¥all` ディレクトリにファイルを保存します。

```
WScript.Echo "Hello World"
WScript.Quit 0
```

`helloworld.vbs` を実行する構文は次のとおりです。

```
cscript.exe /nologo scripts¥helloworld.vbs
```

cmd.exe シェルで `/c` オプションを使用し、処理が完了したらシェルを終了します。

```
cmd.exe /c dir c:¥winnt¥system32
```

追加の例 :

```
c:¥tests¥runA.bat
```

```
netstat /a
```

```
ping mysystem
```

Windows および UNIX プラットフォームで Script プローブを実行する場合は、エスケープ文字でパスのスペースを区切る必要があります。以下に例を示します。

```
"c:¥my tests¥runB.bat"
```

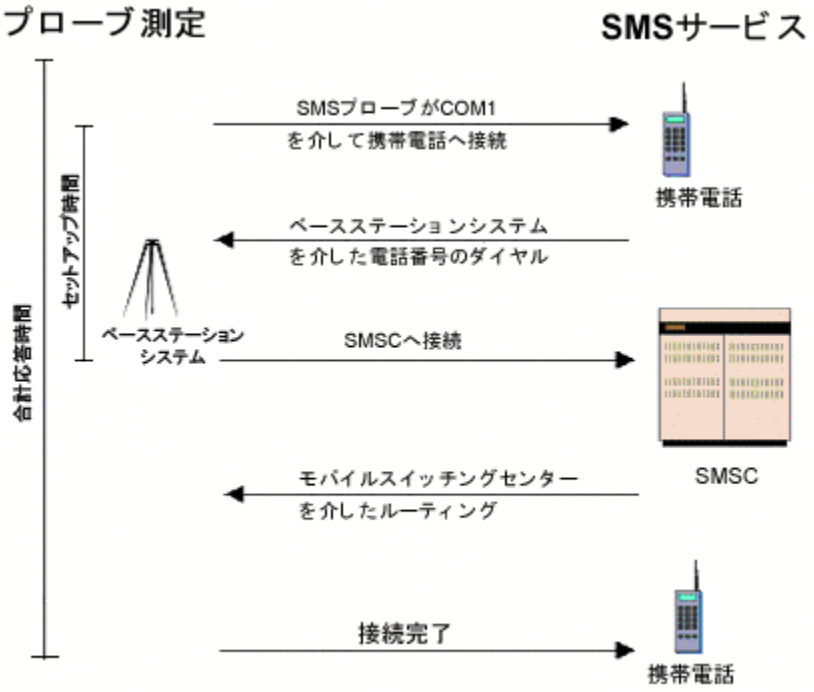
SMS (Short Message Service)

SMS (Short Message Service) プローブは、がワイヤレスインフラストラクチャ全体 (送信元の無線電話から、タワー、SMSC、送信先のタワー、送信先の無線電話まで) においてショートテキストメッセージを伝送するための所要時間を測定します。メッセージの送受信には同じ電話を使用します。**このプローブは、Windows プラットフォームでのみ動作します。**

電話は、データケーブルを使用して、PC の COM ポートに接続します。プローブは、送信元の電話の送信先 SMSC を自動的に変更できます。このため、同じ無線電話で複数の SMSC を計測できます。

プローブは、さまざまなモバイル機器メーカーが提供する機器と構成できます。構成用テキストファイル (管理サーバーの <data dir>¥conf¥probe ディレクトリの SMS2SMSConfig.txt) を編集し、特定のメーカーの電話用に構成を設定できます。

プローブが応答時間を測定するステップを以下の図に示します。



プローブをさまざまな電話と構成するための設定

SMS プローブは、さまざまなメーカーの電話と構成できます。SMS 構成用テキストファイル (管理サーバーの <data dir>¥conf¥probe ディレクトリにある SMS2SMSConfig.txt ファイル) の項目を変更することで、各メーカーのさまざまな電話およびスイッチを使用するプローブを簡単に設定できます。

編集後、構成用テキストファイルをリモートプローブシステムにコピーします。各種リモートシステムおよび電話に合わせて構成を作成できます。

SMS2SMSConfig.txt ファイルの各種セクションの例と説明を以下に示します。

```
#SMS から SMS を送信するための設定ファイル
[SendModem]
port = Com1
mode=pdu

#Nokia 製の電話の場合
DevControlStr = 115200,n,8,1   # 制御文字列フィールドはスペースで区切らない
PduSendFormat = 001100%02X81%s0000A7%02X   #Cingular (Nokia 製電話 ) 用
SetSmscFormat = "%s",145

#Ericsson 製の電話の場合
#DevControlStr = 115200,n,8,1   # 制御文字列フィールドはスペースで区切らない
#PduSendFormat = 01801100%02X81%s0000A7%02X   #Cingular (Ericsson 製電話 )
用
#SetSmscFormat = "%s",145

#Motorola 製の電話の場合
#baud = 57600, parity=N, data=8, stop=1
#DevControlStr = 57600,n,8,1   # 制御文字列フィールドはスペースで区切らない
#PduSendFormat = 0001FF%02X81%s0000%02X    #Vodafone (Motorola 製電話 ) 用
#SetSMSCFormat = "%s"145

[ReceiveModem]
port = Com1
mode=pdu
#baud=57600, parity=N, data=8, stop=1
DevControlStr = 115200,n,8,1   # 制御文字列フィールドはスペースで区切らない
TargetMessageStore = "SM"
SetSmscFormat = "%s",145

#Motorola 製の電話の場合
#baud = 57600, parity=N, data=8, stop=1
#DevControlStr = 57600,n,8,1   # 制御文字列フィールドはスペースで区切らない
#PduSendFormat = 0001FF%02X81%s0000%02X    #Vodafone (Motorola 製電話 ) 用
#SetSMSCFormat = "%s"145
```

このファイルは、[SendModem] と [ReceiveModem] の 2 つのセクションに分かれています。各セクションには、各種の設定属性を表す名前と値のペアが含まれます。SendModem セクションには、SMS メッセージを送信する電話設定の詳細が含まれます。ReceiveModem セクションには、SMS メッセージを受信する電話設定の詳細が含まれます。

このプローブの設定ファイルでは、複数のデバイスエントリをサポートできます。その場合はまず、SendModem と ReceiveModem のセクション名にデバイスエントリ名を追加します (たとえば、[SendModem:Nokia1] [ReceiveModem:Nokia1])。次にこの名前を、送受信ポートを指定する、設定マネージャの [SMS 情報] ダイアログの [**デバイス名**] に入力します。[SMS 情報] ダイアログで [デバイス名] が指定されていない場合は、プローブは [SendModem]、[ReceiveModem] エントリを使用します。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

SMTP (Simple Mail Transfer Protocol)

SMTP (Simple Mail Transfer Protocol) は電子メールを送信するために使用される主要なサービスです。SMTP を強化したものが ESMTP (拡張 SMTP) です。ESMTP は、Authenticated SMTP (A-SMTP) と同じです。SMTP/ESMTP/A-SMTP メールサービスは、SMTP プローブにより監視されます。このプローブは、指定されたアドレスの SMTP ポートとの TCP 接続を確立し、電子メールメッセージを SMTP/ESMTP/A-SMTP サーバーに送信してその所要時間を測定します。受信者や送信者などのメッセージ情報を設定し、指定したサイズのメッセージ本文を送信します。プローブはメッセージをインターネットに送信しますが、メッセージが受信されたことを検証しません。

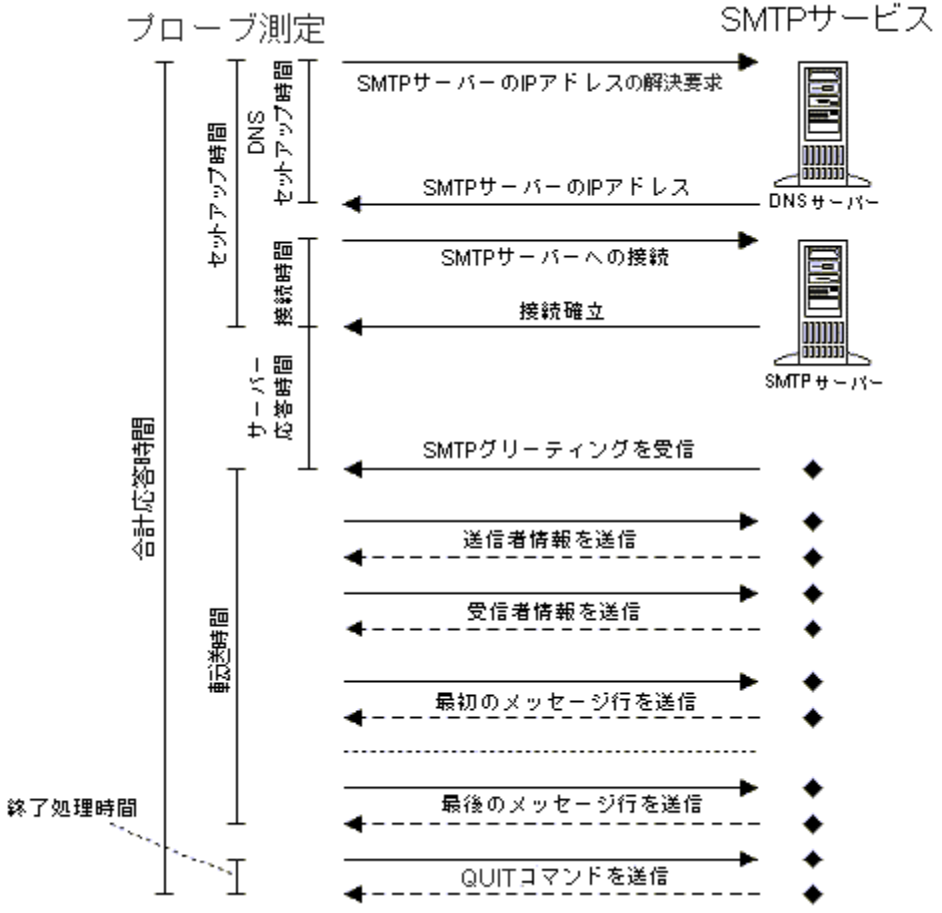
SMTP プローブを使用する場合は、必ず POP3 または IMAP4 プローブも使用してください。POP3 または IMAP4 プローブは、SMTP プローブが送信したメッセージを削除します。POP3 または IMAP4 プローブを使用しないと、受信者のメールボックスがメッセージでいっぱいになる可能性があります。

一部の SMTP サーバーでは、メッセージの転送 (リレー) は許可されていません。転送は、ローカルメールボックスへの SMTP が受信者のアドレスを解決できない場合に発生します。このような場合、サービスは利用不可であるとみなされます。また、一部の SMTP サーバーは、送信者のドメイン拡張子を要求します。

受信者フィールドには、SMTP サーバーが解決できる電子メールアドレスを指定します。通常は、<username>@<server>.<domain> (例 : info@hp.com) の形式を使用します。送信者フィールドはデフォルトでは、<> になっています (ユーザーが指定されていません)。メッセージサイズフィールドは、メッセージ本文の文字数を決定します。デフォルト値の 0 の場合、メッセージ本文に文字が含まれません。

ESMTP/SMTP-A サーバーを測定する場合は、メール送信要求の認証に必要なユーザー名とパスワードの情報を入力します。

プローブが応答時間を測定するステップを以下の図に示します。

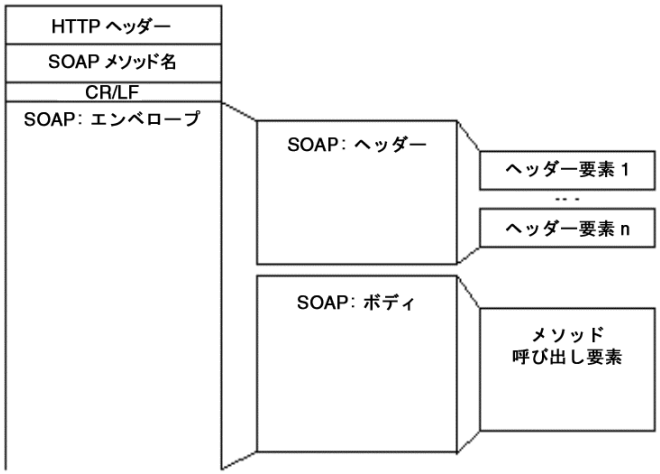


SOAP (Simple Object Access Protocol)

SOAP プローブ は、SOAP 1.1 の要求をサポートします。SOAP (Simple Object Access Protocol) は、非集中の分散環境において XML を使用して構造化されたタイプ別の情報の交換を可能にする、シンプルで軽量のプロトコルです。

- SOAP エンベロープ - メッセージの中に何があるのか、誰がそれを処理すべきなのか、それは任意か必須かといったことを表現するための枠組みを定義します。
- SOAP 符号化規則 - アプリケーションが定義したデータ型のインスタンスを交換するためのメカニズムを定義します。
- SOAP RPC 表現 - リモートプロシージャコールとそのレスポンスを表現するための規約を定義します。

すべての SOAP メッセージは XML を使用してエンコードされます。SOAP メッセージは XML 形式のドキュメントです。この中で SOAP ペイロードは、必須の SOAP エンベロープ内でカプセル化されます。SOAP エンベロープは、オプションの SOAP ヘッダーと必須の SOAP 本文から構成されます。SOAP ヘッダーはオプションですが、存在する場合はオープニングエンベロープ (root) XML タグの次にあります。ヘッダーが存在する場合は、通常はメソッド呼び出しに関するメタ情報を持つ 1 つ以上のヘッダー要素があります。SOAP 本文はメソッドの引数が連続しています。リモートメソッド名はメソッド呼び出しの XML 要素に名前を付けるのに使用され、SOAP 本文オープニング XML タグの次になければなりません。



SOAP プローブの設定には、HTTP プローブや HTTPS プローブと同じ設定マネージャのダイアログを使用しますが、さらに SOAPAction (SOAP 1.1 の要求用) を入力します。SOAP 1.2 は SOAPAction 要求ヘッダーを使用しません。

また、Web アプリケーションにポストされるデータを持つ **送信データファイル** のパスを指定することができます。このファイルはプローブが直接使用するため、ファイルがプローブシステムに存在し、指定されたパスがリモートシステムで有効であることを確認する必要があります。これにより SOAP 要求の送信ができます。最もよく使用されるのは、フォームデータをアプリケーション (たとえば、CGI、ASP、Java Servlet) に送信することです。

さらに、XML に適用する検索パターンを設定できます。

送信データファイルへの絶対パスを使用するか、**配布マネージャ**を使用してリモートシステムにデータファイルを配布します。配布マネージャを使用するには、プローブを作成する前に、OVIS 管理サーバーの `<install dir>¥newconfig¥distrib¥` ディレクトリの下の適切なディレクトリにデータファイルを置く必要があります (適切なサブディレクトリについては、以下を参照してください)。設定を保存すると、`newconfig¥distrib¥` にあるファイルが `<data dir>¥bin¥instrumentation¥probe¥scripts` ディレクトリにコピーされます。

プローブが新しい設定を取得すると、配布マネージャは以下のディレクトリを対象にファイルを検索するため、配布先のシステムに応じて、これらのディレクトリにデータファイルを置いておく必要があります。

newconfig¥distrib¥all - all ディレクトリには、すべてのプラットフォームとプローブロケーションで有効なファイルを置きます。

newconfig¥distrib¥platform¥{Windows|HPUX|Linux|Solaris} - Windows、HPUX、Linux、Solaris ディレクトリには、プラットフォーム固有のファイルを置きます。プローブは、プローブが動作中のオペレーティングシステム用のファイルのみを取得します。

newconfig¥distrib¥location¥{ 設定マネージャで定義したプローブロケーション } - location ディレクトリの下に、設定マネージャで設定したプローブロケーションの名前 (通常は完全修飾ホスト名) の付いたディレクトリを作成できます。たとえば、プローブロケーションが mysystem.mydomain.com の場合、これと同じ名前の mysystem.mydomain.com というディレクトリを作成し、このディレクトリにファイルを置きます。

OVIS がこれらのディレクトリの追加、削除、または変更を行うことはありません。これらのディレクトリ名が OVIS で設定した名前と一致していることを確認する必要があります。このため、all ディレクトリと platform ディレクトリにファイルを置き、どうしても必要な場合にのみ location ディレクトリを使用することをお勧めします。また、ローカルシステムは、実際には OVIS 管理サーバーシステムの完全修飾ドメイン名であることに注意してください。たとえば、管理サーバー名が ovis.domain.com の場合、ローカルシステムにだけファイルを配布するには、ovis.domain.com というディレクトリを作成します。

このプローブの設定の詳細と SOAP 要求と応答の例に関しては、設定マネージャのオンラインヘルプを参照してください。

STREAM_MEDIA (ストリーミングメディア)

ストリーミングメディアプローブは、Real Media Player (バージョン Real8 Basic または RealOne) と Windows Media Player (バージョン 8 以降) がサポートしているファイル形式をストリームし、パフォーマンスを監視します。Windows Media Player は、プローブのインストール時に自動的にインストールされます。Windows 版の Real Player を使用する場合は、プローブを実行するシステムに別途インストールする必要があります。Real Player の Web サイト (www.jp.real.com) を参照してください。**このプローブは、Windows プラットフォームでのみ動作します。**

Real Server は、次のファイルタイプをサポートしています : .rm、.ram、.ra、.rpm、.mp3、.mid、.rmi、.midi、.mpeg、.mpg、.mlv、.mp2、.mpa、.wav、.snd、.au、.aif、.asf、.wm、.wma、.wmv、.avi

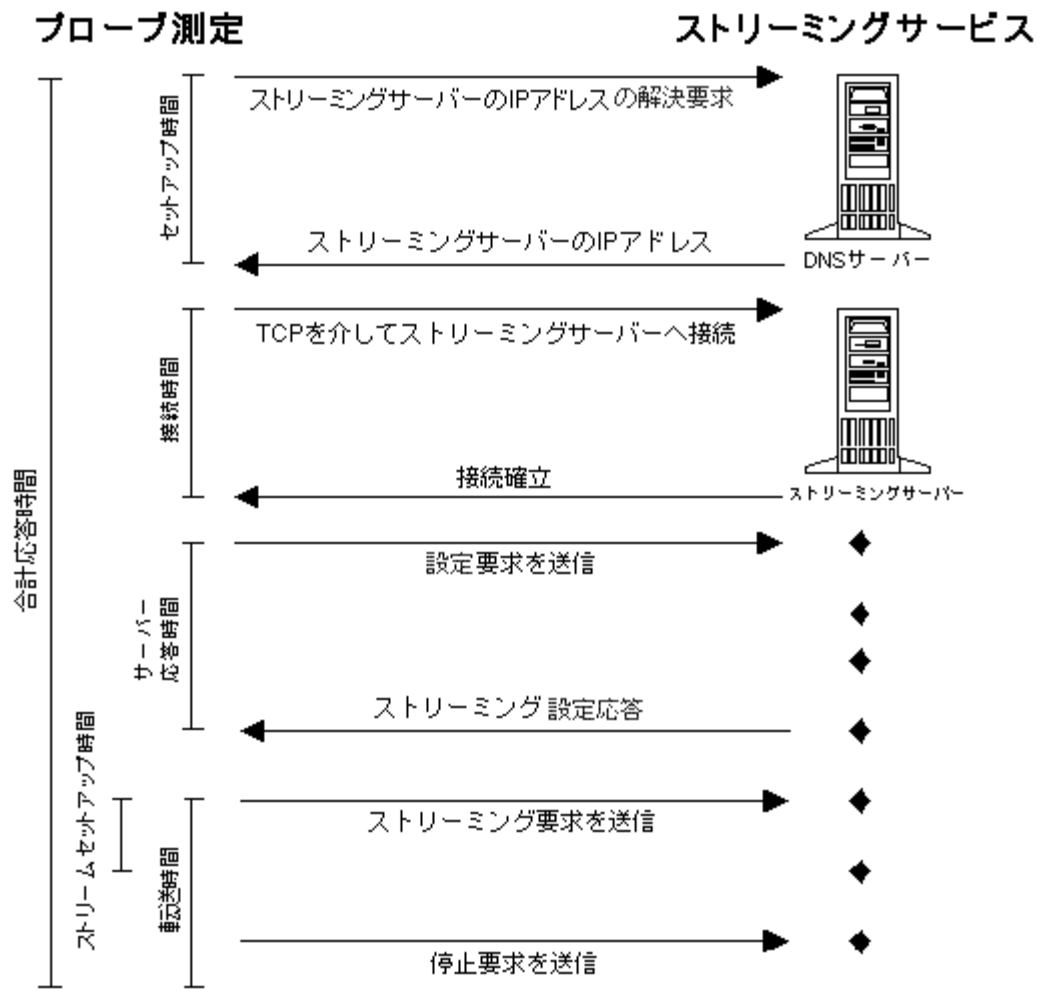
Windows Media Server は、次のファイルタイプをサポートしています : .mp3、.mms、.mid、.rmi、.midi、.mpeg、.mpg、.mlv、.mp2、.mpa、.wav、.snd、.au、.aif、.asf、.wm、.wma、.wmv、.avi

プローブがプロキシを実行し、プロキシ経由でサーバーにアクセスする場合、Player でプロキシ設定を有効にする必要があります。また、設定マネージャの [プローブロケーションの情報] ダイアログでプロキシ情報を設定する必要があります。

ストリーミングメディア監視対象のテストを行う場合は、少なくとも 60 秒間再生する必要があります。このプローブの設定と [**再生時間**] の値の詳細は、設定マネージャのオンラインヘルプを参照してください。

XP システムから、Windows Media Player で STREAM-MEDIA プローブを実行するのであれば、リモートプローブのインストールが終了した後でシステムに `wmfdist.exe` ファイルをインストールする必要があります。`<install dir>¥newconfig` ディレクトリにある実行形式ファイルをダブルクリックしてインストールを開始してください。

プローブが応答時間を測定する箇所を以下の図に示します。



SYS_BASIC_WMI (基本システムメトリック)

SYS_BASIC_WMI プローブは、Windows を実行しているコンピュータの 4 つのメインリソースグループ (CPU、メモリー、ディスクおよびネットワーク) の 基本 Windows システム メトリックを収集します。また、基本システムの可用性チェックも実施します。

このプローブを設定するには、システムメトリックを収集する対象システムのサーバー、ユーザー名、パスワードを入力します。これには、WMI へのアクセス権を持つ Winndows アカウントのユーザー名とパスワードを使用します。

このユーザーが、上記サーバーフィールドで指定したシステムの WMI へアクセスできることを確認してください。WMI コントロールを使用して WMI セキュリティを設定します。

ローカルユーザーを使用する場合は、ユーザー名に完全修飾名 (< ホスト名 >¥< ユーザー名 > または < ドメイン >¥< ユーザー名 >) を使用してください。

メトリックを、プローブを実行している同じシステムから収集する場合は、ユーザー名とパスワードを指定する必要はありません。それらを指定した場合は、エラー (0x80041064) が返されます。

ネットワーク稼働率メトリックで使用されるネットワークインタフェースも選択します。現在のところ、1 つのネットワークインタフェースだけがサポートされています。仮想ループバックインタフェース (127.0.0.1) がリストにも表示されますので確認してください。

メトリックは WMI を介して次のように収集されます。

CPU: CPU メトリックは、すべてのプロセッサ全体の CPU 使用率とすべてのプロセッサキューの長さから構成されます。このメトリックの値が長期間継続して高く、プロセッサキューの長さが長い場合は、プロセッサがボトルネックであることを示しています。ただし使用率メトリックでは、新しくプログラムが起動されたり、プログラムが CPU に負担のかかるタスクを実行する場合に急増することは正常ですので注意してください。プロセッサキューの長さの標準値は、通常 2 より長くなります。マルチプロセッサシステムでは、キューの長さは通常 2 倍になります (たとえば、2 つのプロセッサがあるシステムでは、キューは 4 から始まります)。ディスクまたはインタフェースカードの数ような他の要素が、標準プロセッサキューの長さを増加させることもあります。

メモリー : メモリーメトリックは、使用可能な MB 数 (コンピュータで実行しているプロセッサの使用可能な物理的なメモリー容量) とハードページフォルト (ページ / 秒) (ハードページフォルトを解決するために、ディスクからページを読み込み / 書き込みする割合) から構成されています。

サーバーの作業量に応じて、十分な使用可能物理メモリーを持つ必要があります (そうでない場合は、システムのメモリーページのスワップイン / スワップアウトによって、アプリケーションパフォーマンスが低下します)。1 秒につきページフォルトが 20 より大きければ、使用可能な物理メモリー容量が少なく、メモリーがボトルネックであることを示します。

ディスク : ディスクメトリックは、ディスクビジー時間の割合 (すべてのディスクドライブで、読み込みまたは書き込みのサービスがビジーだった経過時間の割合) と平均のキューの長さ (すべてのディスクについて、キューされていた読み込みおよび書き込み両方の平均の長さ) から構成されます。通常のディスクビジー時間の割合は 50% より小さく、平均のキューの長さは 4 より小さくなります。

注意 : これらのメトリックは、対象システムで `diskperf -y` を実行して有効にする必要があります。

ネットワーク : ネットワーク利用率メトリックは、選択されたインタフェースを利用する割合を表します。高い値が (つまり、40% 以上) が一定時間以上続く場合は、ネットワークがボトルネックであることを示します。

可用性 : メトリックは WMI を介してリモート収集されるので、可用性メトリックは、システムがリモート WMI エージェントに通信できるかどうかをチェックします。これは単に、システムは動作しているかを確認します。ping (ICMP) で通信できても、不正なセキュリティアクセス権またはファイアウォール設定では、システムはダウンしていると見なされます。

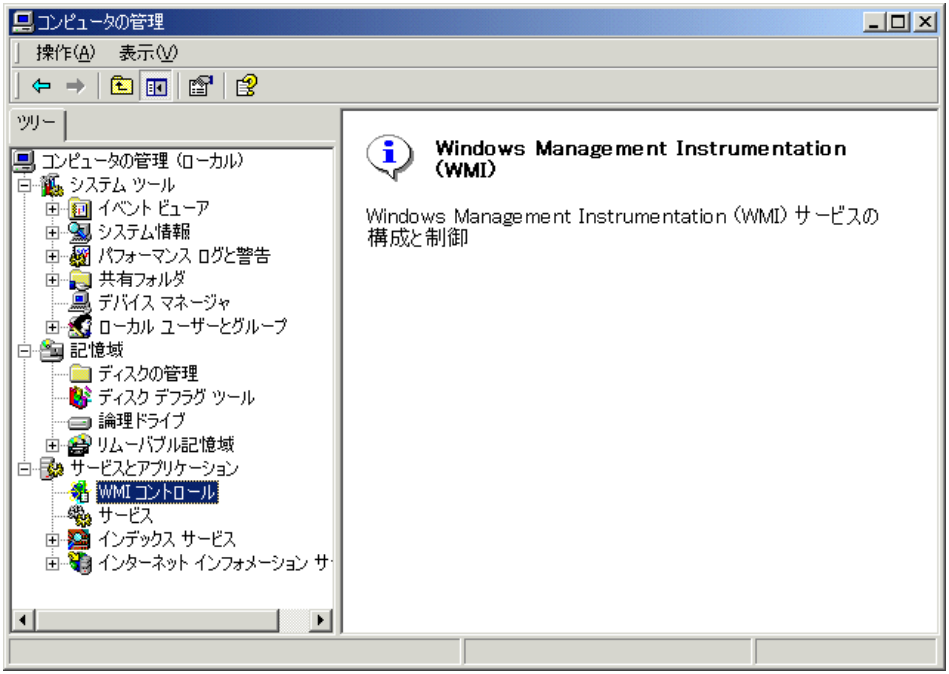
いずれのメトリックも個別に考えないでください。上記 4 つのリソースグループのすべてのメトリックを考慮することでのみ、リソース問題を検査および解決することができます。

測定は、各測定間隔毎に 1 回、SYS_BASIC_WMI プローブによって行われます。測定項目によっては、直前と現在の測定から平均値が取得されます。たとえば、デフォルトの間隔が 5 分の場合に、CPU 使用率は 10 分間の平均値になります。この場合、メトリック値が使用できるようになるまでに、最大で測定間隔の 2 倍の時間が必要になります。

メトリックの基本カウンタが折り返した場合、またはリモートプローブシステムが再起動された場合は、メトリックを計算することができません。この測定間隔のダッシュボード棒グラフには [データ不足] アイコンが表示されます。

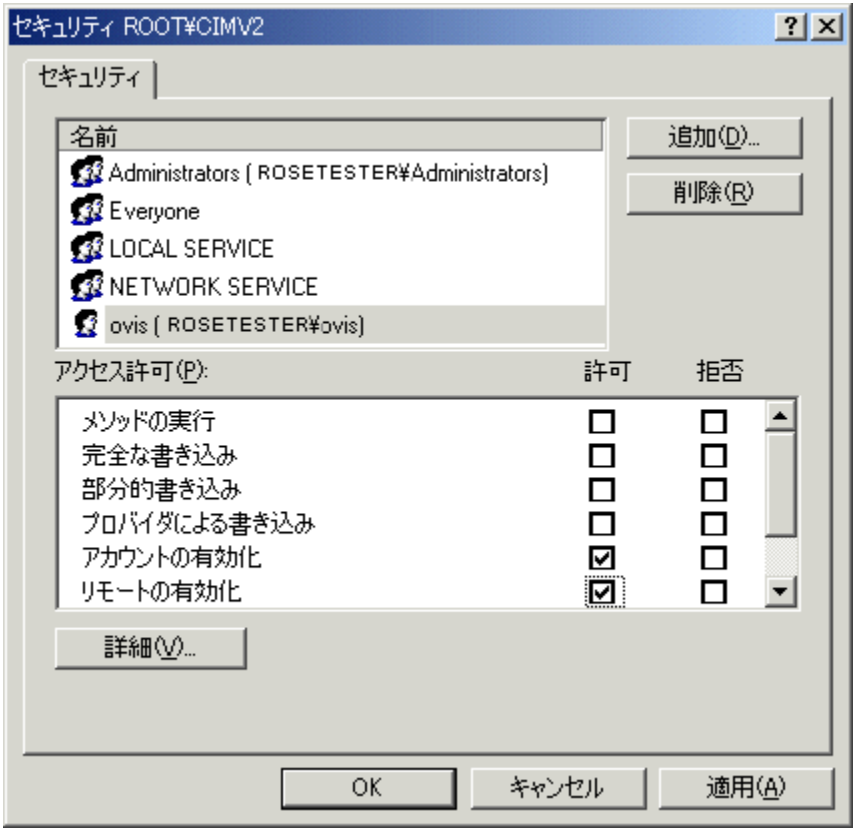
監視対象システムの WMI にアクセスするためには、Windows ユーザー名とパスワードの証明が必要になります。ユーザーが管理者グループ (ローカルまたはドメイン) でない場合は、以下のページに示されているように、ユーザーに WMI へのアクセス許可を設定します。

1 監視対象システムで、[マイ コンピュータ] を右クリックして、[**管理**] オプションを選択し、リストの中から [**WMI コントロール**] メニューを選択します。



2 [WMI コントロール] を右クリックし、[**プロパティ**] を選択して [**WMI コントロールのプロパティ**] ダイアログボックスで [**セキュリティ**] タブをクリックし、下に示すように [**Root**] > [**CIMV2**] を選択します。次に [**セキュリティ**] ボタンをクリックします。

3 [セキュリティ] ダイアログボックスで、このシステムの WMI にアクセスするために使用するユーザーを追加します。ユーザーがリストにない場合は、[**追加**] ボタンを使用します。ユーザーを選択し、次に表示されているようにチェックされていない場合は、[**リモートの有効化**] チェックボックスをチェックします。[**適用**] をクリックして設定を保存します。



注意 : ゲストアカウントを使用することはできません。

注意 : プローブシステムと監視対象との間のファイアウォールは、WMI DCOM トラフィックを使用することができません。詳しくは、**msdn.microsoft.com** から「WMI Connecting Through Windows Firewall」を検索して参照してください。

このプローブの設定に関する詳細は、設定マネージャのオンラインヘルプを参照してください。

TCP - パフォーマンス

TCP - パフォーマンス プローブは、プローブとサーバー間の ネットワークの帯域幅を測定します。

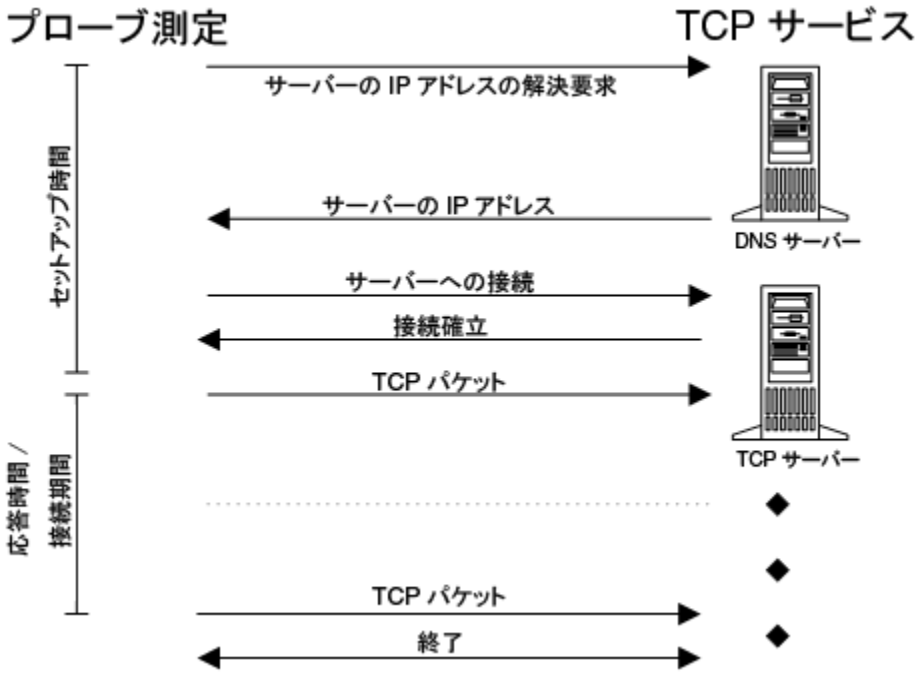
サーバーは、リモートプローブパッケージの一部で、デフォルトでは無効になっています。プローブを実行するには、リモートプローブパッケージを監視対象システムにインストールする必要があります。既存のリモートプローブシステムを使用することもできます。サーバーは、OVIS スケジューラプロセスの一部であり、設定マネージャで [プローブロケーションの情報] ダイアログボックスの [**IP パフォーマンスサーバーポート**] セクションの [**ポートを有効にする**] チェックボックスにより、有効または無効にすることができます。

レポートされる帯域幅は、プローブと監視対象サーバーシステムの利用可能なシステムリソース (CPU、メモリー、ネットワーク I/O) に依存します。システムにすでに高い負荷がある場合は、その負荷が測定に影響します。したがって、正しく測定を行うには他のプローブと同時にパフォーマンスプローブ (TCP および UDP) を実行しないようにしてください。設定マネージャの [プローブロケーションの情報] ダイアログボックスで [**監視対象の優先度**] を設定し、パフォーマンスプローブの実行中に、他のプローブを同時に実行しないようにします。

注意 : TCP パフォーマンスサーバーは、同時に 32 接続以上は処理できません。

このプローブの設定に関する詳細は、設定マネージャのオンラインヘルプを参照してください。

次の図は、応答時間を測定するプローブのステップを示しています。



サーバーの IP アドレスを解決し、サーバーに接続した後で、プローブは指定したサイズの TCP パケットを指定した期間、送信します。プローブはできる限り早くサーバーに TCP パケットを送信しようとします。プローブはサーバーから一切データを受信しないので、レポートされた帯域幅は送信データ用です。

接続期間には、接続確立および接続の切断を含みません。

帯域幅メトリックは、SI 基準に基づく Mbit/ 秒でレポートされます。1Mbit/ 秒は、10^6 = 1,000,000 bit/ 秒を意味し、ビットレートを測定するための単位として電気通信産業で広く行き渡っています。

TFTP (Trivial File Transfer Protocol)

Trivial File Transfer Protocol (TFTP) プローブ は、単一ファイルの検索を実行します。TFTP は、単純化したファイル転送プロトコルです。FTP とは違って、認証がありません。プローブは直接特定ファイルのダウンロードを要求します。TFTP プローブは、サービスが使用できるかどうかを決定し、プローブが実行しているこのサーバーに関するその他の情報も収集します。

このサービスを測定するには、正しく測定するために固定サイズのテストファイルをセットアップする必要があります。

このプローブの詳細に関しては、設定マネージャのオンラインヘルプを参照してください。

UDP - パフォーマンス

UDP - パフォーマンス プローブはプローブとサーバー間のネットワーク帯域幅とジッターを測定します。

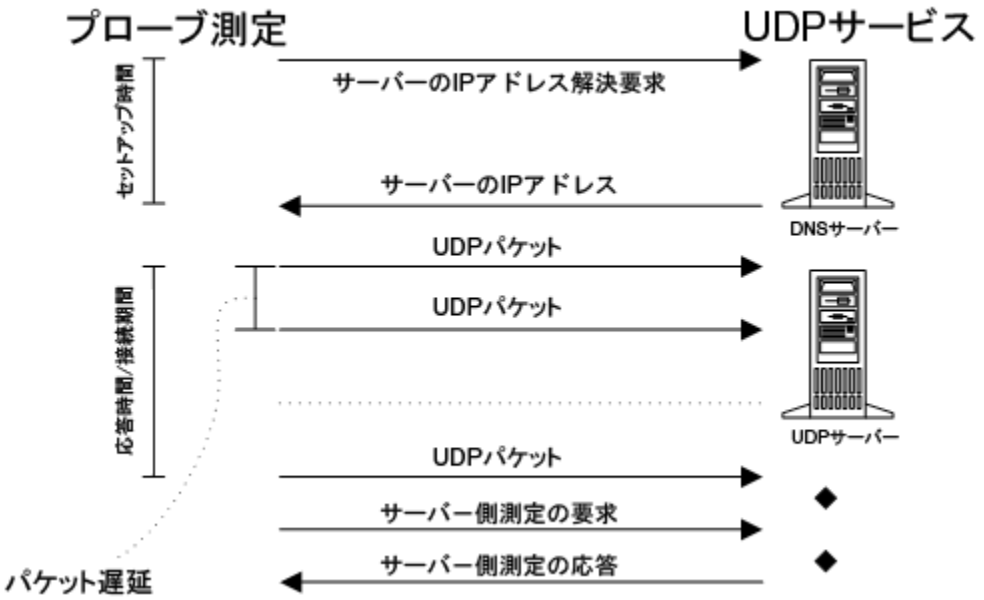
サーバーはリモートプローブパッケージの一部で、デフォルトでは無効になっています。プローブを実行するには、リモートプローブパッケージを監視対象システムにインストールする必要があります。既存のリモートプローブシステムを使用することもできます。サーバーは OVIS スケジューラプロセスの一部で、設定マネージャの [プローブロケーションの情報] ダイアログボックスの [**IP パフォーマンスサーバーポート**] セクションの [**ポートを有効にする**] チェックボックスにより有効または無効にすることができます。

レポートされる帯域幅とジッターは、プローブと監視対象サーバーシステムの利用可能なシステムリソース (CPU、メモリー、ネットワーク I/O) に依存します。システムにすでに高い負荷がある場合は、その負荷が測定に影響します。したがって、正しく測定を行うには、他のプローブと同時にパフォーマンスプローブ (TCP および UDP) を実行しないようにしてください。設定マネージャの [プローブロケーションの情報] ダイアログボックスで [**監視対象の優先度**] を設定し、パフォーマンスプローブの実行中に、他のプローブを同時に実行しないようにします。

注意 : UDP パフォーマンスサーバーは同時に 32 接続以上は処理できません。

このプローブの設定に関する詳細は、設定マネージャのオンラインヘルプを参照してください。

次の図は、応答時間を測定するプローブのステップを示します。



サーバーの IP アドレスを解決した後で、プローブは指定したサイズの UDP パケットを送信します。プローブは、指定したパケット遅延時間に応じて均等間隔でパケットを送信しようとします。たとえば、パケットを送信するのに 1ms かかり、パケットの遅延時間が 20ms の場合に、プローブは次のパケットを送信する前に 19ms 待機します。すべてのパケットが指定した継続時間に送信された後にプローブは、サーバー側の測定を要求します。測定の取得には多少時間がかかり、接続期間の一部ではないので、このプローブのタイムアウトパラメータに接続期間の 3 倍を設定してください。

帯域幅メトリックは、SI 基準に基づく Mbit/ 秒でレポートされます。1Mbit/ 秒は、10^6 = 1,000,000 bit/ 秒を意味し、ビットレートを測定するための単位として電気通信産業で広く行き渡っています。

WAP (Wireless Application Protocol)

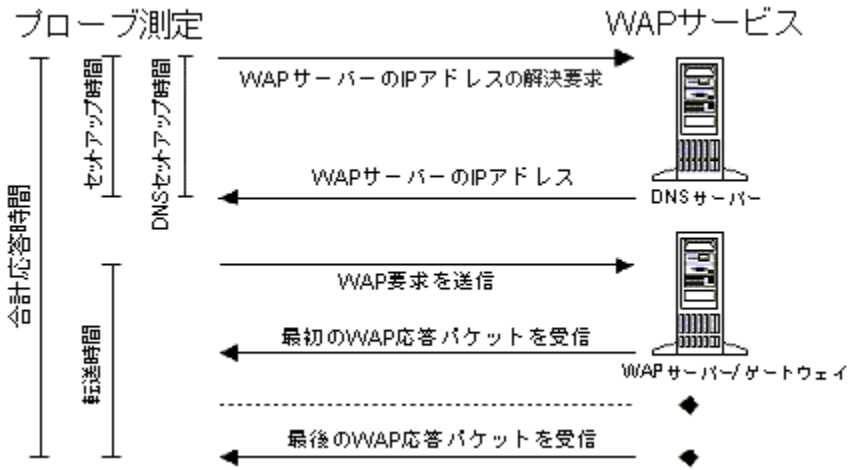
WAP (Wireless Application Protocol) プローブは、エミュレートした WAP 要求の合計応答時間を測定します。ホスト名または IP アドレスが解決されると、文書の WAP 要求は、WAP サーバーまたは WAP ゲートウェイに送信されます。WAP サーバーは、要求を受信すると、要求した文書を探してそれをプローブに返します。プローブは、ホスト名と IP アドレスを解決するのに必要な時間と、指定したファイルの送受信時間を測定します。WAP サーバーと通信するのに、UDP transport protocol を使用します。

現在、このプローブは WSP (コネクションレスプロトコル) だけをサポートしています。

WAP のデフォルトのポート番号は 9200 です。現在、WAP プローブは画像が埋め込まれていない文書だけをダウンロードします。WAP プローブをダイヤルアップネットワーク接続で動作するように設定する場合は、RAS (Remote Access Server) と、少なくとも 1 つの電話帳エントリをプローブシステムに設定する必要があります。

このプローブの設定の詳細は、設定マネージャのオンラインヘルプを参照してください。

プローブが応答時間を測定するステップを以下の図に示します。



カスタムプローブ

次のいずれかを使用してカスタムプローブを作成できます。

- カスタムプローブ SDK
- Probe Builder

Internet Services の今回のリリースでは、カスタムプローブ SDK と Probe Builder は英語版でのみサポートされています。

カスタムプローブ SDK には、ユーザー固有のサービスを測定したり、測定値を OVIS 管理サーバーに返すための、カスタムプローブ開発用 API (Application Programming Interfaces) が含まれています。SDK を使用するには、C/C++ のコーディングスキルが必要です。API は、コマンドライン解析、時間測定、プローブトレース、および OVIS 管理サーバーへのエラーロギングやデータロギングなどの機能を主に提供しています。

カスタムプローブ SDK の詳細は、『*Internet Services Custom Probes API Guide*』(CustomProbes.pdf) を参照してください。カスタムプローブ SDK は、OVIS 管理サーバーの `<install dir>¥Sdk` ディレクトリにあります。例もこのディレクトリに含まれています。

Probe Builder は 、スクリプト開発環境で JavaScript を使用するツールキットです。これを使用すると、カスタムプローブの作成、テスト、および展開を容易に行うことができます。Windows でのみサポートされています。

Probe Builder は、以下の当社の開発者向けリソース Web サイトの「hp OpenView unified developer toolset」からダウンロードできます。

http://devresource.hp.com/drc/unifieddev/probe.jsp

警告 : Internet Services のカスタムプローブ SDK と Probe Builder を使用したプローブの開発は、標準のサポートチャネルでは**サポートしていません。**Internet Services のカスタムプローブ SDK と Probe Builder に関するテクニカルサポートは、hp Partner Care Extended (U2461AA) を**ご購入**いただいた場合にのみご利用いただけます。hp Partner Care の詳細は、当社の営業担当または当社営業所にお問い合わせください。Partner Care Web サイト (www.hp.com/go/partnercare) に追加情報が掲載されています。

OVTA からのインポートデータ

以下の OVIS サービスタイプは、OpenView Transaction Analyzer (OVTA) から OVIS にトランザクションデータをインポートするために使用します。これらのサービスタイプの定義は以下のとおりです。

WEBAPP - Web コンテンツにアクセスするために HTTP プロトコルを使用して、Web ベースのアプリケーションから OVTA トランザクションデータをインポートします。

SOAPAPP - 他の Web サービスと通信するために SOAP プロトコルを使用して、Web サービス指向のアプリケーションから OVTA トランザクションデータをインポートします。SOAP プロトコルは一般に HTTP 上に実装されます。

RMIAPP - 他のアプリケーションコンポーネントにアクセスするために Java RMI (Remote Method Invocation) を使用して、J2EE アプリケーションから OVTA トランザクションデータをインポートします。リモート EJB は RMI 上に実装されます。

JMSAPP - 他のアプリケーションコンポーネントと通信するために Java Messaging Service を使用して、J2EE アプリケーションから OVTA トランザクションデータをインポートします。

COMAPP - 他のアプリケーションコンポーネントと通信するために COM (Component Object Model) を使用して、アプリケーションから OVTA トランザクションデータをインポートします。

OVTA によって収集されて OVIS にインポートされたトランザクションデータは、OVIS ダッシュボードに表示されます。さらに、OVTA データのサービスレベル目標値、アラームしきい値、サービスレベル契約を定義すると、OVIS は OVTA アラームを OVO と NNM に転送します。

上記のサービスタイプと各サービスで収集されるメトリックの詳細は、314 ページの「OpenView Transaction Analyzer との統合」を参照してください。

メトリックの一覧 (プローブタイプ別)

プローブタイプ別のメトリックの一覧は、次のファイルを参照してください。

```
<install directory>¥newconfig¥packages¥reload_IOPS.SRP
```

以下のリストにある「OVTA アプリケーション」は、COMAPP、JMSAPP、RMIAPP、SOAPAPP、WEBAPP のサービスタイプのメトリックを示します。

また、各プローブタイプの Metric 1 から Metric 8 を識別するために、メトリック識別子が示されています。この情報は、アラームメッセージの設定時に使用できます。131 ページの「アラームメッセージ」を参照してください。

メトリック一覧の先頭にあるのは、ダッシュボードに表示されるメトリック名、かっこの中にあるのは、設定マネージャで使用されるメトリック名です。

ANYTCP

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME*) - TCP サービスの合計応答時間 (DNS セットアップ時間 + 接続時間)。

セットアップ時間 (*SETUP_TIME*) - アドレスを解決して接続を確立するまでの時間。

スループット (*TRANSFER_TPUT*) - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 *(CONNECT_TIME) - Metric 2* - 解決された IP アドレスに接続する時間。

DHCP

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME*) - DHCP サービスの合計応答時間 (セットアップ時間 + 転送時間)。

セットアップ時間 (*SETUP_TIME*) - ホストを指定した場合の、アドレスを解決して接続を確立するまでの時間。

スループット (*TRANSFER_TPUT*) - 転送バイト数 / 転送時間 (KB/ 秒)。

提示時間 (*OFFER_TIME*) - *Metric1* - サーバーから最初の提示を受信するのにかかった時間。

解放時間 (*LEASE_TIME*) - *Metric2* - 提供された IP アドレスを解放するのにかかった時間。

転送時間 (*TRANSFER_TIME*) - *Metric5* - トランザクション全体を完了するのにかかった時間 (検出、提示、要求、確認、解放)。

転送されたバイト (*TRANS_BYTES*) - *Metric6* - 転送したバイト数。

DIAL

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME*) - PPP 接続を確立するのにかかった時間。

RAS 接続ステータス (*RAS_CONNECT_STATUS*) - *Metric1* - RAS ダイヤルが返したエラー。接続が成功した場合は、0 になります。

ボーレート (*BAUD_RATE*) - *Metric2* - ボーレート - モデムが報告する転送速度。

総接続時間 (*TOTAL_CONNECTION_TIME*) - *Metric3* - 合計接続時間。

終了ステータス (*TERMINATION_STATUS*) - *Metric4* - 接続が異常終了した場合は true (1)、それ以外の場合は false (0)。

DNS

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME*) - ホスト名 /IP アドレスの問い合わせ実行時間。

解決 (*ANSWER_DNS*) - *Metric 1* - ホスト名を解決できない場合は 0 に、解決できた場合は 1 に設定される。サーバーは、名前が解決できたかどうかにかかわらず問い合わせ応答ジョブを完了するため、どちらの場合も可用性は 1 (または true) になります。

Exchange

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

セットアップ時間 (*SETUP_TIME*) - Exchange サーバーにログインして名前を決定するのにかかった時間。

応答時間 (*RESPONSE_TIME*) - Exchange サービスの合計応答時間。セットアップ時間 + すべてのメッセージを読み込み、OVIS のメッセージを削除するように指定するためにかかった時間。

認証時間 *(AUTH_TIME) - Metric 4* - ユーザーを認証する時間。

転送時間 *(TRANSFER_TIME) - Metric 5* - データを受信するのにかかった時間の全体。

送信時間 *(SEND_TIME) - Metric 6* - メッセージの送信時間。

FTP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - FTP 要求の合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + 認証時間 + ポート番号送信時間 + 転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 (*DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 (*CONNECT_TIME) - Metric 2*- FTP サーバーに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* - FTP 開始ヘッダー (220) を受信するのにかかった時間。

認証時間 *(AUTH_TIME)* - ユーザー認証にかかった時間 (ユーザー名 / パスワードを送信し、応答を受信するのにかかった時間)。

ポート番号送信時間 *(PORT_TIME) - Metric 5* - FTP サーバーにクライアント接続ポートを送信するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 6* - データ接続でデータを受信するのにかかった時間。

転送されたバイト (*DATA_TRANS_BYTES) - Metric 7* - 転送したバイト数。

HTTP/HTTPS

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - Web ページ (またはセキュア Web ページ) アクセスの合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + データ転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / (転送時間 + サーバー応答時間) (KB/ 秒)。

DNS セットアップ時間 (*DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 (*CONNECT_TIME) - Metric 2* - HTTP/HTTPS サーバーまたはプロキシに接続するのにかかった時間。

サーバー応答時間 (*SERVER_RESP_TIME) - Metric 3* - HTTP/HTTPS GET 要求を送信し、最初の応答パケットを受信するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 4* - 要求を送信し、すべての応答パケットを受信するのにかかった時間。

転送されたバイト (*TRANS_BYTES) - Metric 5* - 転送したバイト数。

HTTP ステータス (*HTTP_STATUS*) - *Metric 6* - HTTP/HTTPS ステータスコード。

要求 (*REQUESTS*) - *Metric 7* - HTTP/HTTPS 要求の数。たとえば、ページがリダイレクトされた場合、または埋め込みオブジェクトをダウンロードした場合。

壊れたリンク (*BROKEN_LINKS*) - *Metric 8* - ダウンロードできなかった埋め込みオブジェクトの数 (たとえば、見つからなかった URL)。

HTTP_TRANS

URL/ ナビゲーションポイントモード

可用性 (*AVAILABILITY*) - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME*) -
ステップ : Web ページアクセスの合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + データ転送時間)。
トランザクション : すべてのステップの合計応答時間。

セットアップ時間 (*SETUP_TIME*) -
ステップ : アドレスを解決して接続を確立するのにかかった時間。
トランザクション : すべてのステップの合計セットアップ時間。

スループット (*TRANSFER_TPUT*) -
ステップ : 転送バイト数 / (転送時間 + サーバー応答時間) (KB/ 秒)。
トランザクション : トランザクションの合計転送処理量。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* -
ステップ : DNS を介してホスト名を解決する時間。
トランザクション : すべてのステップの合計 DNS セットアップ時間。

接続時間 *(CONNECT_TIME) - Metric 2* -
ステップ : HTTP/HTTPS サーバーまたはプロキシに接続するのにかかった時間。
トランザクション : すべてのステップの合計接続時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* -
ステップ : HTTP GET 要求を送信し、最初の応答パケットを受信するのにかかった時間。
トランザクション : すべてのステップの合計サーバー応答時間。

転送時間 (*TRANSFER_TIME) - Metric 4* -
ステップ : 要求を送信し、すべての応答パケットを受信するのにかかった時間。
トランザクション : すべてのステップの合計転送時間。

転送されたバイト (*TRANSFER_BYTES) - Metric 5* -
ステップ : 転送したバイト数。
トランザクション : すべてのステップの合計転送バイト。

HTTP ステータス *(HTTP_STATUS) - Metric 6* -
ステップ : HTTP ステータスコード。
トランザクション : 最終ステップの HTTP ステータスコード。

要求 *(REQUESTS) - Metric 7 -*
ステップ : HTTP 要求の数。たとえば、ページがリダイレクトされた場合、または埋め込みオブジェクトをダウンロードした場合。
トランザクション : すべてのステップの合計要求数。

壊れたリンク *(BROKEN_LINKS)* - Metric 8 -
ステップ : ダウンロードできなかった埋め込みオブジェクトの数 (たとえば、見つからなかった URL)。
トランザクション : すべてのステップの壊れたリンクの合計。

HTTP_TRANS

IE モード

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* -
ステップ : セットアップ時間 + サーバー応答時間 + 転送時間。
トランザクション : すべてのステップの合計応答時間。

セットアップ時間 (*SETUP_TIME)* -
ステップ : ステップを実行してから文書のダウンロードを開始するまでにかかった時間。
トランザクション : すべてのステップの合計セットアップ時間。

スループット (*TRANSFER_TPUT)* -
ステップ : 転送バイト数 / 応答時間 (KB/ 秒)。
トランザクション : トランザクションの合計転送処理量。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - 利用不可。

接続時間 *(CONNECT_TIME) - Metric 2* - 利用不可。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3 -*
ステップ : 文書のダウンロードを開始してから最初にダウンロードの進捗が変化するまでにかかった時間 (IE 進捗インジケータ)。
トランザクション : すべてのステップの合計サーバー応答時間。

転送時間 (*TRANSFER_TIME) - Metric 4 -*
ステップ : 最初に進捗が変化してからステップが完了するまでにかかった時間。
トランザクション : すべてのステップの合計転送時間。

転送されたバイト *(TRANSFER_BYTES) - Metric 5* -
ステップ : ページに含まれているすべての画像、フレーム、および JavaScript のバイト数。ただし、画像 /JavaScript が (クライアントまたはサーバー側で) キャッシュされている場合、この値は実際にダウンロードされたバイト数には対応しません。
トランザクション : すべてのステップの合計転送バイト数。

HTTP ステータス *(HTTP_STATUS) - Metric 6* -
ステップ : HTTP ステータスコード、IE WININET エラーコード、または -1 (最初の接続がタイムアウトになった場合)。
トランザクション : 最後のステップの HTTP ステータスコード。

要求 *(REQUESTS) - Metric 7* -
ステップ : 文書の数 (リダイレクトとフレームは含まれますが、他の埋め込みオブジェクトは含まれません)。
トランザクション : すべてのステップの完全なドキュメントの合計数。

壊れたリンク *(BROKEN_LINKS)* - 利用不可。

ICMP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - すべての ICMP パケットの平均ラウンドトリップ時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

応答時間最小値 *(MIN_RESPONSE) - Metric 1* - すべての ICMP パケットのラウンドトリップ時間の最小値。

応答時間最大値 *(MAX_RESPONSE) - Metric 2* - すべての ICMP パケットのラウンドトリップ時間の最大値。

消失したパケット *(PACKET_LOSS) - Metric 3* - 消失したパケット数。

IMAP4

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - IMAP4 サービスの合計応答時間 (セットアップ時間 + 接続時間 + サーバー応答時間 + 認証時間 + データ転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 *(CONNECT_TIME) - Metric 2* - IMAP サーバーに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* - IMAP サーバーが応答するのにかかった時間。

認証時間 *(AUTH_TIME) - Metric 4* - ユーザー認証にかかった時間 (ユーザー名 / パスワードを送信し、応答を受信するのにかかった時間)。

転送時間 (*TRANSFER_TIME) - Metric 5* - データ転送のみにかかった時間。

転送されたバイト (*DATA_TRANS_BYTES) - Metric 6* - 転送したバイト数。

LDAP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - LDAP サービスの合計応答時間 (セットアップ時間 + データ転送時間)。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME)* - DNS を介してホスト名を解決する時間。

エントリ数 *(NUM_ENTRIES)* - 返されたエントリの数。

接続時間 *(CONNECT_TIME) - Metric 3* -LDAP サーバーに接続するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 4* - データ転送のみにかかった時間。

転送されたバイト (*TRANS_BYTES) - Metric 5* - 転送したバイト数。

MAILROUNDTRIP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

応答時間 (*RESPONSE_TIME)* - SMTP メール送信と POP/IMAP 受信の合計応答時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

NNTP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - NNTP の合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + 認証時間 + グループ時間 + 読み取り時間 + 分解時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME)* - Metric 1 - DNS を介してホスト名を解決する時間。

接続時間 *(CONNECT_TIME) - Metric 2* - NNTP サーバーに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME)* - ファイルの読み取りにかかった時間 (データ接続でデータを受信)。

認証時間 *(AUTH_TIME) - Metric 4* - ユーザー認証にかかった時間 (ユーザー名 / パスワードを送信し、応答を受信するのにかかった時間)。

グループ Cmd 時間 *(GROUP_TIME) - Metric 5* - ニュースグループを選択して、それらの最新 100 記事の概要を取得するのにかかった時間。

読み取り時間 *(READ_TIME) - Metric 6* - 全体のサイズが 10000 バイトの記事を読み取る時間。

分解時間 *(TEAR_DOWN_TIME) - Metric 7* - QUIT 要求を送信して応答を受信するのにかかった時間。

転送されたバイト (*DATA_TRANS_BYTES) - Metric 8* - 転送したバイト数。

NTP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - NTP サービスの合計応答時間 (セットアップ時間 + データ転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

転送されたバイト (*DATA_TRANS_BYTES) - Metric 5* - 転送したバイト数。

転送時間 (*TRANSFER_TIME) - Metric 6* - データ転送のみにかかった時間。

ODBC

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - ODBC サービスの合計応答時間。

セットアップ時間 (*SETUP_TIME)* - データベース接続ハンドルを設定するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

接続時間 *(CONNECT_TIME) - Metric 1* - データベースに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 2* - SQL ステートメントに応答するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 3* - データ転送にかかった時間。

転送されたバイト (*TRANS_BYTES) - Metric 4* - 転送したバイト数。

OVTA アプリケーション (COMAPP、JMSAPP、RMIAPP、SOAPAPP、WEBAPP)

可用性 (*AVAILABILITY) - WEBAPP および SOAPAPP サービスタイプのみ*。最後の測定間隔で試行した要求の合計に対する、失敗した可用性プローブの要求の割合。

応答時間 (*RESPONSE_TIME)* - 測定間隔で正常に完了したトランザクションの平均応答時間。

トランザクション率 *(TRANSACTION_RATE) - Metric 1* - 最後の測定間隔で完了したトランザクションの秒単位の合計数。

応答時間違反回数 *(RESPONSE_TIME_VIOLATION_COUNT) - Metric 2* - 測定した応答時間が OVTA で設定した応答時間のしきい値を超えた、最後の間隔で正常に完了したトランザクションの数。

応答時間違反率 *(RESPONSE_TIME_VIOLATION_PERCENTAGE) - Metric 3* - 測定した応答時間が OVTA で設定した応答時間のしきい値を超えた、最後の間隔で正常に完了したトランザクションの割合。

トランザクションサイズ *(TRANSACTION_SIZE) - Metric 4* - WEBAPP サービスタイプのみ。正常に完了したトランザクションの平均サイズ。サイズは、アプリケーションのタイプとトランザクションのタイプによって異なります。

OVTA Browser Client Monitor を使用してブラウザで測定したトランザクションの場合、トランザクションのサイズは、ダウンロードしたページのサイズとすべての埋め込まれたコンテンツと画像を合計したサイズです。OVTA Web Server Monitor を使用して Web サーバーまたはアプリケーションサーバーで測定したトランザクションのサイズは、Content-Length HTTP ヘッダーでレポートされた、ダウンロードされたページのサイズです。これはページ自体のサイズであり、埋め込まれた画像は含まれません。さらに、一部の Web ベースのアプリケーションは、Content-Length フィールドを設定しません。この場合、このタイプのアプリケーションのトランザクションについては、このメトリックは 0 になります。

トランザクション失敗率 *(FAILED_TRANSACTION_RATE) - Metric 5* - 最後の間隔で失敗したトランザクションの秒単位の合計数。

POP3

可用性 *(AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - POP3 メール配信の合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + 認証時間 + データ転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 *(CONNECT_TIME) - Metric 2* - POP3 サーバーに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* - POP3 開始ヘッダー (+OK) を受信するのにかかった時間。

認証時間 *(AUTH_TIME) - Metric 4* - ユーザー認証にかかった時間 (ユーザー名 / パスワードを送信し、応答を受信するのにかかった時間)。

転送時間 (*TRANSFER_TIME) - Metric 5* - メールボックス内のすべてのメッセージを読み取って、IOPS テストメッセージを削除するのにかかった時間。

転送されたバイト (*DATA_TRANS_BYTES) - Metric 6* - 転送したバイト数。

RADIUS

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。サーバーに接続されたが、無効なパスワード、共有シークレットなどによりサーバーがアクセス拒否パケットを返した場合は 0 に設定されます。

応答時間 (*RESPONSE_TIME)* - RADIUS サービスの合計応答時間 (DNS セットアップ時間 + データ転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

転送時間 (*TRANSFER_TIME) - Metric 4* - データ転送のみにかかった時間。

転送されたバイト (*TRANS_BYTES) - Metric 5* - 転送したバイト数。

SAP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。測定値を取得するには、接続と RFC 呼び出しの両方に成功する必要があります。

応答時間 (*RESPONSE_TIME)* - SAP サービスの合計応答時間。RFC 呼び出し (ログオンチェックとログアウトを含む) を正常に完了するのにかかった時間 (セットアップ時間＋完了時間) です。

セットアップ時間 (*SETUP_TIME)* - RFC サーバーに正常に接続するのにかかった時間。

Script

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - スクリプトの合計実行時間。または、結果ファイルスクリプトからインポートされた合計応答時間。

SMS

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - SMS サービスの合計応答時間。

セットアップ時間 *(SETUP_TIME)* - 接続を確立するのにかかった時間。

スループット *(TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

SMTP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - SMTP メール要求の合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + データ転送時間 + 分解時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 (*DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解決する時間。

接続時間 *(CONNECT_TIME) - Metric 2* - SMTP サーバーに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* - SMTP 開始ヘッダー (220) を受信するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 4* - メール要求を転送するのにかかった時間 (MAIL FROM:, RCPT TO:, DATA, QUIT 等の要求に対する SMTP からの応答を含む)。

転送されたバイト (*TRANS_BYTES) - Metric 5* - 転送したバイト数。

分解時間 *(TEAR_DOWN_TIME) - Metric 6* - QUIT 要求を送信して応答を受信するのにかかった時間。

SOAP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - Web ページアクセスの合計応答時間 (DNS セットアップ時間 + 接続時間 + サーバー応答時間 + 転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを決定して接続を確立するのにかかった時間。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を決定するのにかかった時間。

接続時間 *(CONNECT_TIME) - Metric 2* - SOAP サーバーまたはプロキシに接続するのにかかった時間。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 3* - HTTP Get 要求を送信して最初の応答パケットを受信するのにかかった時間。

転送時間 (*TRANSFER_TIME) - Metric 4* - 要求を送信してすべての応答パケットを受信するのにかかった時間。

転送されたバイト (*TRANS_BYTES) - Metric 5* - 転送されたバイト数。

要求 *(REQUESTS) - Metric 7* - HTTP 要求の数。たとえば、ページがリダイレクトされた場合、または埋め込みオブジェクトがダウンロードされた場合。

STREAM_MEDIA

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - ストリーミングメディアサービスの合計応答時間 (セットアップ時間 + 接続時間 + サーバー応答時間 + 転送時間)。

セットアップ時間 (*SETUP_TIME)* - アドレスを解決するのにかかった時間。

スループット (*TRANSFER_TPUT)* - データ転送で使用した平均帯域幅 (KB/ 秒)。

接続時間 *(CONNECT_TIME) - Metric 1* - サーバーに接続するのにかかった時間。プロキシを使用している場合は、プロキシに接続するのにかかった時間です。

サーバー応答時間 *(SERVER_RESP_TIME) - Metric 2* - サーバーがパケットの送信を開始するのにかかった時間。これには、各種プロトコルのセットアップ時間が含まれます。

転送時間 *(TRANSFER_TIME) - Metric 3* - データを転送するのにかかった時間。

受信パケット *(PACKETS_RECEIVED) - Metric 4* - 受信した合計パケット数。

消失したパケット *(PACKET_LOSS) - Metric 5* - 消失したパケットの割合。

レイテンシ *(LATENCY) - Metric 6* - データ転送でのレイテンシ (秒)。サーバーは設定されている間隔で応答するため、要求を送信してから次の応答が行われるまでに待機時間が発生することがあります。

輻輳 *(CONGESTION) - Metric 7* - ストリームの合計再生時間に対するデータバッファリング時間の割合。これには初期バッファリング時間が含まれます。

ストリームセットアップ時間 *(STREAM_SETUP_TIME) - Metric 8* - 実際にクライアントでストリームの再生が開始される前の、初期バッファリング時間。

SYS_BASIC_WMI

可用性 *(AVAILABILITY)* - 対象システムの WMI からメトリックを取得できたかどうかを示します。

CPU:

CPU 総使用率 *(TOTAL_CPU_UTL) - Metric 1* - 指定された期間の合計 CPU 使用率。

プロセッサキュー長 *(PROCESSOR_QUEUE_LENGTH) - Metric 2* - プロセッサ待ち行列の長さの合計。

メモリー :

利用可能なメガバイト *(AVAILABLE_MBYTES) - Metric 3* - 使用可能な物理的メモリー (MB)。

ページ / 秒 (ハードページフォールト) *(MEM_PAGES_PER_SEC) - Metric 4* - ハードページフォルトを解決するためにディスクからページを読み込み / 書き込みする割合。

ディスク :

% ディスク時間 *(PERCENT_DISK_TIME) - Metric 5* - すべてのディスクドライブで読み込みまたは書き込みのサービスがビジーだった経過時間の割合。

平均のキュー長 *(DISK_AVG_QUEUE_LENGTH) - Metric 6* - すべてのディスクについて、キューされていた読み込みおよび書き込み要求両方の平均の数。

ネットワーク：

使用率 *(NET_UTIL) - Metric 7* - 指定されたインタフェースカードの稼働率。

TCP- パフォーマンス

可用性 *(AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

帯域幅 (SI 基準) *(SI_BANDWIDTH) Metric 1* - 帯域幅 (Mbit/ 秒) (実際に送信されたビット数を実際の接続期間で割った値。1 Mbit/ 秒 は 10^6 = 1,000,000 bit/ 秒)。

スループット *(TRANSFER_TPUT)* - 送信バイト数を、実際の接続期間で割った値 (KB/ 秒)。

送信メガバイト *(MB_SENT) Metric 2* - 送信メガバイト数。

応答時間 *(RESPONSE_TIME)* - 指定された接続期間とほぼ同じ。

セットアップ時間 *(SETUP_ TIME)* - DNS 名前解決とサーバーへの接続にかかった時間。

TFTP

可用性 *(AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 *(RESPONSE_TIME)* - TFTP サービスの合計応答時間 (セットアップ時間 + 転送時間)。

セットアップ時間 *(SETUP_ TIME)* - TFTP アドレスを解決する時間。

スループット *(TRANSFER_TPUT)* - 転送バイト / 転送 (KB/ 秒)。

転送時間 *(FILE_TRANSFER_TIME) - Metric 1* - 転送バイト / 転送時間 (KB/ 秒)。

転送されたバイト *(TRANSFER_BYTES) - Metric 2* - トランザクションで転送された合計バイト数。

UDP- パフォーマンス

可用性 *(AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

帯域幅 (SI 基準) (SI_BANDWIDTH) Metric 1 - 帯域幅 (Mbit/ 秒) (実際に送信されたビット数を実際の接続期間で割った値。1 Mbit/s は 10^6 = 1,000,000 bit/ 秒)。

ジッター *(JITTER) Metric 4* - RFC 1889、Real Time Protocol (RTP) に従ったジッター (ミリ秒) (送受信パケットの位相変動) 。

スループット *(TRANSFER_TPUT)* - 送信バイト数を、実際の接続期間で割った値 (KB/ 秒)。

% 消失したパケット *(PCT_PACKET_LOST) Metric 5* - 転送中の紛失パケットの割合。受信パケット数を送信パケット数で割った値。

送信メガバイト *(MB_SENT) Metric 2* - プローブが送信したメガバイト数。

受信メガバイト *(MB_RECEIVED) Metric 3* - サーバーで受信したメガバイト数。

順序誤りパケット *(PACKET_OUT_OF_ORDER) Metric 6* - 送信された順序とは異なる順序で受信されたパケット数。

応答時間 *(RESPONSE_TIME)* - 指定された接続期間とほぼ同じ。

セットアップ時間 *(SETUP_ TIME)* - DNS 解決にかかった時間。

WAP

可用性 (*AVAILABILITY)* - 測定値を取得できない場合は 0 に、取得できた場合は 1 に設定されます。

応答時間 (*RESPONSE_TIME)* - WAP サービスの合計応答時間 (DNS セットアップ時間 + 転送時間)。

スループット (*TRANSFER_TPUT)* - 転送バイト数 / 転送時間 (KB/ 秒)。

DNS セットアップ時間 *(DNS_SETUP_TIME) - Metric 1* - DNS を介してホスト名を解明する時間。

転送時間 (*TRANSFER_TIME) - Metric 4* - データ転送のみにかかった時間。

転送されたバイト *(TRANS_BYTES) - Metric 5* - 転送したバイト数。

5

OpenView 製品との統合

Internet Services (OVIS) は、OpenView Transaction Analyzer (OVTA)、OpenView Operations for UNIX (OVO for UNIX)、Network Node Manager (NNM)、または OpenView Operations for Windows (OVO for Windows) と統合できます。OVIS を OVTA と統合することで、Web ベースアプリケーションのパフォーマンスと可用性に対する徹底した管理ソリューションが実現します。OVIS を OVO または NNM と統合すると、統合された製品は、Internet Services 内で生成されたアラームやメッセージを取得できるようになります。Internet Services に設定されたサービスが、指定した目標値を満たしていない場合は、統合された製品のコンソールに警告が表示されます。統合することで、パフォーマンス監視領域を拡張したり、報告された問題をすばやく判断することができます。

OVIS は、Service Information Portal (SIP)、Reporter、Performance Manager および Performance Agent とも統合できます。この章では以下の内容について説明します。

OpenView Transaction Analyzer との統合

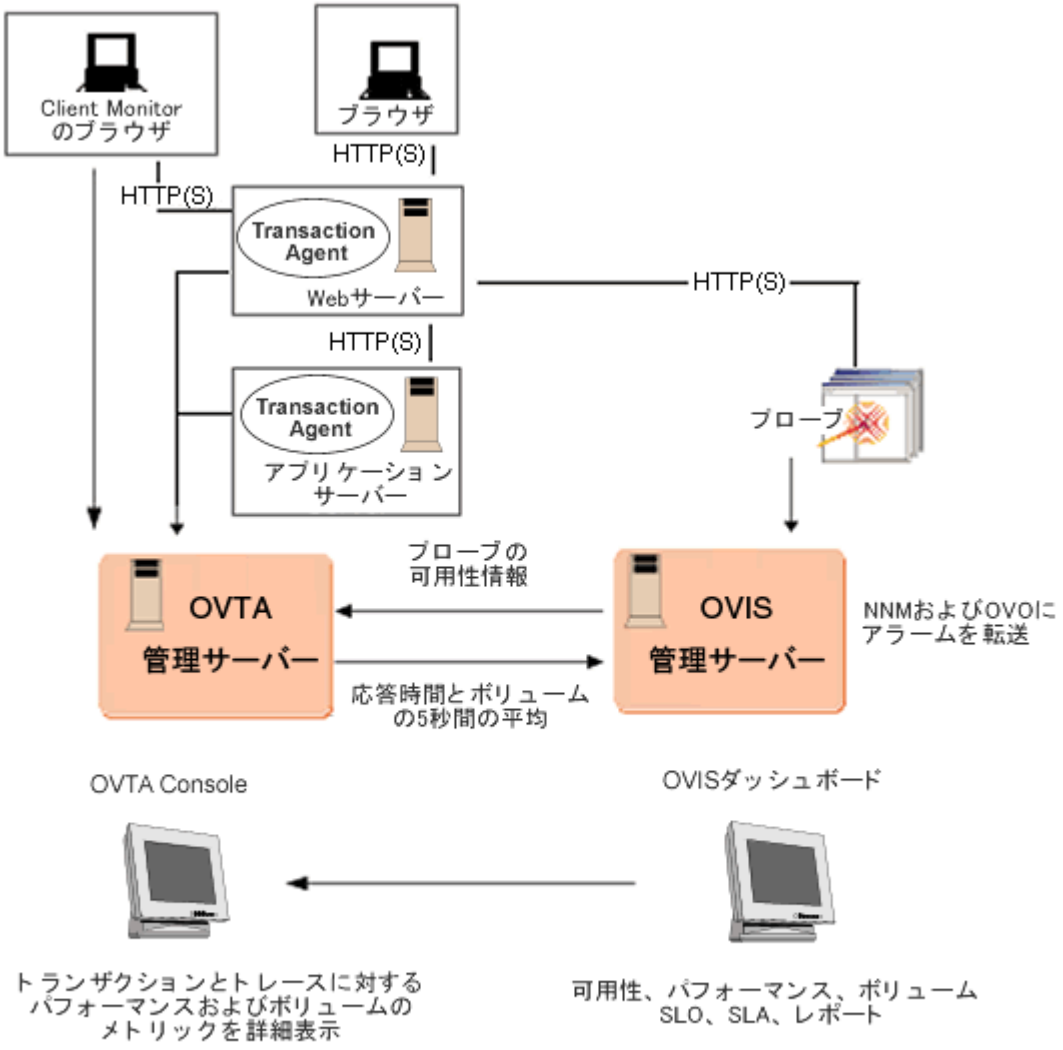
OVIS には、OpenView Transaction Analyzer (OVTA) で監視する各種アプリケーションにマップするサービスタイプがいくつかあります (COMAPP、JMSAPP、RMIAPP、SOAPAPP、WEBAPP)。OVIS のトランザクションパフォーマンスデータは OVIS にインポートされ、レポート間隔 (現在は 5 分に設定されています) でまとめられます。OVTA は、OVTA で監視するアプリケーションのトランザクションボリュームとトランザクション応答時間を測定および解析します。OVTA は、トランザクションモニターを使用して、エンドユーザーが実行する実際のひとまとまりの作業を測定します。これにより、実際のエンドツーエンドトランザクション応答時間を、エンドユーザーが実際に実行する場合と同様に確認できます。OVTA のトランザクションボリュームデータは、Web サイトの実際の利用状況を忠実に反映したものになります。

詳細は、『*OpenView Transaction Analyzer ユーザーガイド*』を参照してください。このマニュアルは、Openview の Web サイト (http://ovweb.external.hp.com/lpe/doc_serv/) からダウンロードできます。

OVTA に付属の OVIS ソフトウェアの評価版を使用した場合は、OVTA のサービスタイプに限り使用することができます。HTTP/S、HTTP_TRANS、またはその他の OVIS プローブを使用するには、OVIS 製品をご購入いただく必要があります。

次の図は、OVIS と OVTA の統合におけるデータフローの概要を示しています。

図 3　　OVIS と OVTA の統合におけるデータフロー



この統合により、次の機能が可能になります。

- パフォーマンスと可用性に関するサービスレベル目標値 (SLO) およびサービスレベル契約 (SLA) の強化。SLO と SLA のおもな対象領域は、可用性、ボリューム、および応答性に関連しています。OVIS の HTTP/S および

HTTP_TRANS プローブは、可用性と応答性を測定します。OVTA は、ボリュームと応答時間を測定します。OVIS プローブによる応答性の測定では、応答時間の測定値は合成プローブによるものに限られます。OVTA による測定は、エンドユーザーが実行する、実際のひとまとまりの作業のボリュームおよび応答時間を測定することで、OVIS プローブによる測定を補完します。OVIS と OVTA の測定を組み合わせることにより、実際のパフォーマンスと可用性についての SLO および SLA を設定、実施できます。

- OVTA の測定値に対してパフォーマンスアラームを設定し、これを NNM と OVO に転送することができます。これには、OVIS の既存の SLO および SLA の機構が使用されます。また、OVIS と OVTA の両方に対して、SLO と SLA、およびアラームの共通ソリューションが提供されます。
- OVIS プローブの測定値と OVTA トランザクションの測定値を、1 つのペイン (OVIS ダッシュボード) に表示できます。また、OVIS ダッシュボードから OVTA Console を起動して、詳細なトラブルシューティング情報を表示することもできます。
- OVTA 測定データに関するレポートが作成されます。

統合の概要

ここでは、OVIS と OVTA の統合について、概要を簡単に説明します。各ステップを実行して統合を設定する方法については、321 ページの「統合と設定の手順」を参照してください。

1. OVIS は、OVTA 管理サーバーが同じコンピュータにインストールされているかどうかを自動的に検出します。リモートの OVTA 管理サーバーの場合は、ホスト名、ポート、ユーザー名、パスワードを OVIS 設定マネージャで指定する必要があります。
2. 次に、OVTA トランザクションを、他の OVIS 監視対象サービスと同様に設定します。OVIS 設定マネージャを使用して、OVTA 統合に使用する顧客とサービスグループを設定します。サービスグループの設定時に、以下のいずれかのサービスタイプを [監視対象サービス] として選択します。

   WEBAPP

   SOAPAPP

   RMIAPP

   JMSAPP

COMAPP

次に、OVIS 設定マネージャで、OVIS に監視対象サービスとしてインポートする OVTA トランザクションを選択します。

[プローブロケーション] は必ずデフォルトの [ローカルシステム] に設定してください。この設定は、OVIS がデータを収集するために必要です。統合は OVIS サーバー (ローカルシステム) でのみサポートされるため、デフォルトのローカルなプローブロケーションを 1 つだけ設定します。

3 サービスグループのサービスレベル目標値(SLO)とサービスレベル契約(SLA)を設定します。アラームを OpenView Operations for UNIX、OpenView Operations for Windows、または NNM に転送する必要がある場合は、アラームの送信先を設定します。この場合は、対象の製品と OVIS との統合も設定する必要があります。

4 設定を保存します。データ収集が開始されたら、OVTA からインポートされた OVTA ベースの監視対象サービスのステータスを確認します。

5 データ収集が完了したら、OVIS へのインポート対象として設定した OVTA トランザクションを OVIS ダッシュボードで監視できます。より詳細な分析を行う場合は、ワークスペースペインで [OVTA] アイコン () を選択して、OVIS ダッシュボードから OVTA Console を起動します。

6 OVIS ダッシュボードの [状況] ワークスペースにある [アラーム] タブで、アラームの [トレース] 列にある [OVTA] アイコンをクリックします。OVTA Console が起動されて、トランザクションサブコンポーネントの詳細が表示されます。

7 OVIS で夜間のレポートが生成されたら、OVIS ダッシュボードのワークスペースペインにある [レポート] リンクを使用して、OVTA に固有なレポート情報を表示することができます。

8 より有益なアラームやレポートを取得するには、SLO および SLA のしきい値を必要に応じて調整します。

収集されるメトリック

OVTA に固有の測定値を以下に示します。これらは、OVIS にインポートされたトランザクションの概略を示す統計情報です。

RESPONSE_TIME ― 最後の測定間隔における、正常に完了したトランザクションの平均応答時間。

AVAILABILITY ー 最後の測定間隔における、試行した要求の合計に対する、失敗した可用性プローブ要求の割合 (WEBAPP、SOAPAPP だけ)。

TRANSACTION_RATE - Metric 1 ー 最後の測定間隔における、正常に完了したトランザクションの毎秒の総数。

RESPONSE_TIME_VIOLATION_COUNT - Metric 2 ー 最後の測定間隔における、正常に完了したトランザクションのうち、応答時間の測定値が OVTA で設定された応答時間しきい値を超えたものの数。

RESPONSE_TIME_VIOLATION_PERCENTAGE - Metric 3 ー 最後の測定間隔における、正常に完了したトランザクションのうち、応答時間の測定値が OVTA で設定された応答時間しきい値を超えたものの割合。

TRANSACTION_SIZE - Metric 4 ー 正常に完了したトランザクションの平均サイズ。サイズは、アプリケーションのタイプとトランザクションのタイプによって異なります。

WEBAPP: OVTA Browser Client Monitor を使用してブラウザで測定したトランザクションの場合、トランザクションのサイズは、ダウンロードしたページのサイズとすべての埋め込まれたコンテンツと画像を合計したサイズです。OVTA Web Server Monitor を使用して Web サーバーまたはアプリケーションサーバーで測定したトランザクションのサイズは、Content-Length HTTP ヘッダーでレポートされた、ダウンロードされたページのサイズです。これはページ自体のサイズであり、埋め込まれた画像は含まれません。さらに、一部の Web ベースのアプリケーションは、Content-Length フィールドを設定しません。この場合、このタイプのアプリケーションのトランザクションについては、このメトリックは 0 になります。

COMAPP、RMIAPP、SOAPAPP、JMSAPP:TRANSACTION_SIZE のメトリック値は利用できません。常に 0 です。

FAILED_TRANSACTION_RATE - Metric 5 ー 最後の測定間隔における、失敗したトランザクションの毎秒の総数。

可用性メトリックは、トランザクションが OVIS HTTP プローブの監視対象サービスとして設定されている場合にのみ有効です。これは、OVTA が提供する受動的な手段では非可用性を検出できないためです。OVIS HTTP または HTTP_TRANS プローブを、可用性の測定が含まれるトランザクションに対して設定することをお勧めします。

推奨される使い方

重要なトランザクションのみを設定することをお勧めします。アラーム、サービスレベル契約、またはレポートにとって不必要な OVTA トランザクションデータをインポートしないことで、これにより発生する余分なオーバーヘッドを避けることができます。

サービスレベル目標値 (SLO) を追加する場合には、サービスグループ内のトランザクションの必要に応じて SLO とアラームのしきい値を調整してください。デフォルトの目標値のしきい値は、メトリックごとに指定されます。

OVTA Console では、目的のトランザクションの応答時間平均、ヒストグラム、しきい値違反回数、およびトランザクションレートを監視できます。この情報を使用して、より有効な値でデフォルト値を上書きできます。

応答時間の SLO が設定されている場合は、OVTA Configuration Editor を使用して、デフォルトの応答時間しきい値を上書きする必要があります。RESPONSE_TIME メトリックのしきい値は、測定間隔の平均応答時間に適用されます。したがって、RESPONSE_TIME メトリックを使用する SLO は、あまり効果的ではありません。より正確な応答時間 SLO を使用するには、OVTA で応答時間しきい値を設定し、OVIS で SLO を指定する際に RESPONSE_TIME_VIOLATION_PERCENT または RESPONSE_TIME_VIOLATION_COUNT メトリックを使用します。331 ページの「SLO と SLA の例」を参照してください。

OVIS プローブロケーションには、OVTA 要求ノード情報が含まれます。これにより、OVIS ダッシュボードの [プローブロケーション] レベルの表示を使用して、1 つのトランザクションに対する各種の要求ノードを表示できます。要求ノードがプローブの場合は、プローブロケーションはプローブソースシステム名です。要求ノードが OVTA Browser Client Transaction Monitor のブラウザの場合は、プローブロケーションは、ブラウザが使用する時間帯、接続タイプ、および回線速度を示す文字列です。これらの値についての詳細は、『*OVTA ユーザーガイド*』を参照してください。

システム要件

OVIS と OVTA の両方を、インストールし設定する必要があります。しかし、OVIS と OVTA を同じシステムにインストールする必要はありません。OVIS の使用に慣れていない場合は、第 2 章「Internet Services の使い方」でインストール手順や使用例を参照してください。

OVTA と OVIS の管理サーバーが同じシステムにインストールされている場合は、システムに十分なリソースがあり、システムのサイズに問題がないことを確認してください。共通の管理サーバーのサイズを決定する際には、システム要件が記載された、OVIS と OVTA の両方のマニュアルを参照してください。また推奨されているサイズの決定方法については『*OVTA パフォーマンスとスケーラビリティガイド*』を参照してください。

OVIS サーバーと OVTA サーバーが異なるシステムに存在する場合は、それらシステムのクロックを 5 分以内の範囲で同期させておく必要があります。

制限事項

- OVTA からの測定値では、15 分程度の遅延が発生する可能性があります。これは、トランザクションを平均化するために、レポート間隔の開始を表すタイムスタンプを集計アルゴリズムが使用するためです。したがって、管理対象ノードからのデータが、OVIS 管理サーバーでアラームのために使用できるようになるまでには最大 10 分かかり、そのデータが OVIS ダッシュボードに表示されるまでにはさらに 5 分かかる可能性があります。
- 特定のトランザクションについては、OVIS ステータスが [プローブの情報がありません] と表示される場合があります。これは、最後のレポート間隔において OVTA インストルメンテーションモニターがトランザクションをまったく測定しなかったことを示します。原因は単純で、それらの Web ページがどのエンドユーザー、OVIS HTTP または HTTP_TRANS プローブからもアクセスされなかったためです。
- OVTA SLO 応答時間設定は、OVIS 設定マネージャに統合されていません。これらのしきい値は、目的のトランザクションごとに、OVTA Configuration Editor で設定する必要があります。詳細は、『*OVTA ユーザーガイド*』を参照してください。
- OVIS に同時に統合できる OVTA Measurement Server は 1 つだけです。

統合と設定の手順

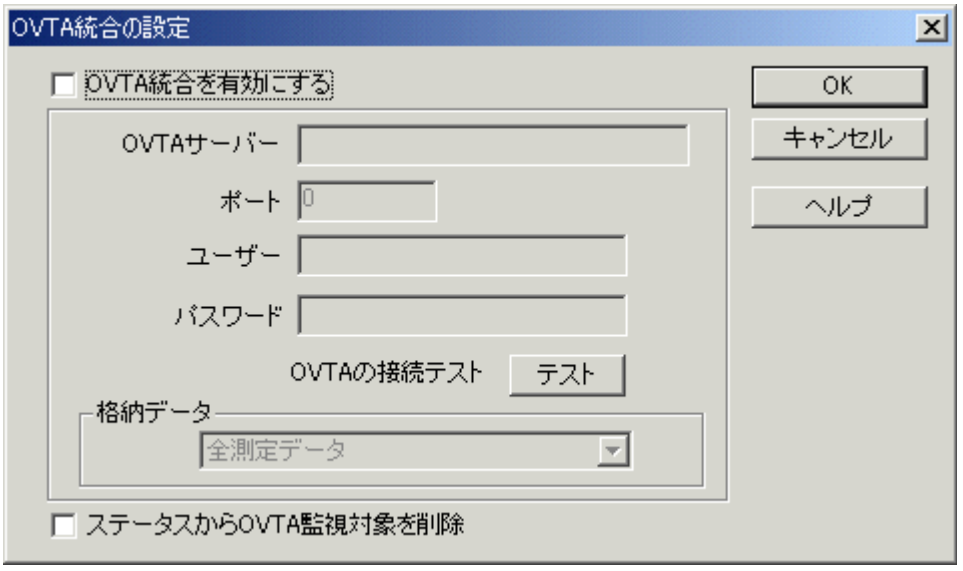
OVIS と OVTA を統合する手順は次のとおりです。

タスク 1: OVTA 管理サーバーの設定

まず、OVTA サーバーの識別を行います (ローカルでもリモートでもかまいません)。OVIS 設定マネージャで、[**ファイル**] > [**設定**] > [**OVTA Measurement Server**] を選択します。OVTA サーバー名、ポート番号、および OVTA Configuration Editor にアクセスするための OVTA ユーザー名およびパスワードを入力します。OVTA が OVIS と同じシステムにインストールされている場合は、[OVTA サーバー] と [ポート] はあらかじめ設定されています。OVTA サーバーへの接続をテストするには、[テスト] ボタンを選択します。

収集するデータは、OVTA サーブレットで選択することができます。特に指定しなければ、入手可能な計測データがすべて収集されます。収集対象データを指定する場合は、そのひとつとしてプローブ計測データを選択することができます。OVIS プローブから得られるこのデータは、OVTA クライアントレセプタで収集される場合と、OVTA をインスツルメントされたサーバー、または、トランザクションを監視するために設定した OVIS プローブ (HTTP プローブ) から収集される場合があります。収集対象データとしては、この他に、OVTA 計測データを選択することもできます。この計測データは、設定した監視対象サービスに基づいて OVIS へインポートされたものです。

OVTA の監視対象が多いと、OVIS ダッシュボードの [監視対象ステータス] ワークスペースページや設定マネージャの [ステータス] ページで表示が遅くなることがあります。[ステータスから OVTA 監視対象を削除] チェックボックスにチェックマークを付けて、OVTA の監視対象が常に OVIS のステータスページに表示されるようにしてください。



タスク 2: OVTA アプリケーショントランザクションの設定

他の OVIS サービスの場合と同様に、OVTA トランザクションを監視対象サービスとしてグループ化するための新しいサービスグループを作成し、SLO とプローブロケーションを設定します。

OVIS 設定マネージャで、設定ウィザードを選択するか、サービスグループの設定を行います。サービスグループを設定するには、まず、既存の顧客を選択するか、[顧客] を右クリックして [顧客の新規作成] を選択し、新しい顧客を追加します。

左ペインに新しい顧客名、[サービスグループ] と [サービス契約] がリストされます。[サービスグループ] を右クリックし、[サービスグループの新規作成] を選択します。

サービスグループ名を入力し、ドロップダウンリストから以下のいずれかのサービスタイプを [監視対象サービス] として選択します。これらのサービスタイプは、通常、ミドルウェアの種類とリモートアプリケーションコンポーネント間の通信に使用される基本プロトコルに対応します。

WEBAPP ― Web コンテンツにアクセスするために HTTP プロトコルを使用する Web ベースのアプリケーション。

SOAPAPP ー 他の Web サービスと通信するために SOAP プロトコルを使用する、Web サービス指向のアプリケーション。SOAP プロトコルは通常 HTTP 上に実装されます。

RMIAPP ー 他のアプリケーションコンポーネントにアクセスするためにJava RMI (Remote Method Invocation) を使用する、J2EE アプリケーション。リモート EJB は RMI 上に実装されます。

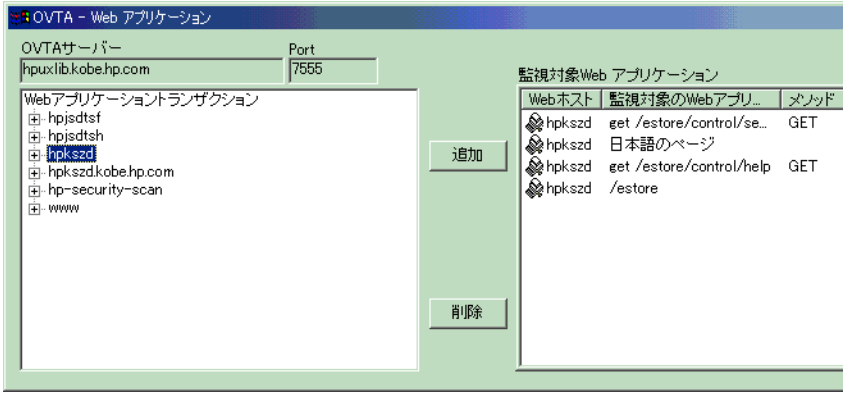
JMSAPP ー 他のアプリケーションコンポーネントと通信するために Java Messaging Service を使用する、J2EE アプリケーション。

COMAPP ー 他のアプリケーションコンポーネントと通信するために COM (Component Object Model) を使用するアプリケーション。

これらのサービスタイプの詳細は、『*OVTA ユーザーガイド*』を参照してください。

顧客にサービスグループが追加されます。[サービスグループ] には、[監視対象サービス]、[サービス目標値]、[プローブロケーション] がリストされます。

[監視対象サービス] を右クリックし、[監視対象サービスの新規作成] を選択します。[OVTA - 管理対象アプリケーション] ダイアログが表示されます (WEBAPP 監視対象サービスの例を以下に示します)。ここでは、設定したサービスタイプに対するトランザクションを、OVTA サーバーで現在検出されているトランザクションから選択することができます。データをすべて表示しようとすると、時間がかかる場合があります。



サービスタイプが WEBAPP の場合、OVTA からインポートされたトランザクションには、対応する URL から派生した名前が付きます。この派生は、OVTA Configuration Editor を使用して指定された分類規則に基づいています。WEBAPP サービスの例を示します。

```
/estore/control/category
/estore/control/product
get /petstore/cart.do
get /petstore/main.screen
```

トランザクション名の中には、http メソッドの **get** または **post** という接頭辞が付いているものがあります。それらは、Web サーバーで OVTA Web Sever Transaction Monitor を使用して測定される OVTA トランザクションです。名前に http メソッドの接頭辞がないトランザクションは、クライアント側で測定されるものです。クライアント側での測定は、OVIS HTTP プローブ、または OVTA Browser Client Transaction Monitor を使用するブラウザで行うことができます。

RMI、JMS、SOAP、COM など、他の OVTA アプリケーションのサービスタイプの場合、トランザクション名には要求元または応答元の接頭辞が付いています。要求元は要求を行うトランザクションで、応答元は要求に応答するサーバーです。

サービスグループを使用すると、関連するトランザクション (たとえば、ショッピングカート) を論理的にグループ化できます。または、OVTA クライアント側で測定されるトランザクションをサーバー上で測定されるトランザクションとは別にグループ化できます。これにより、エンドユーザーとサーバーの観点から把握することができます。詳細は、『*OVTA ユーザーガイド*』を参照してください。

OVIS との統合では、必要なトランザクションだけを設定することをお勧めします。必要なトランザクションの例を以下に示します。

- 警告やアラームのために設定する必要があるトランザクション。
- 夜間作成されるレポートに含める必要があるトランザクション。
- 詳細な監視を行うために、OVIS ダッシュボードに表示する必要があるトランザクション。これにより、OVTA トランザクションの測定値が、OVIS プローブの測定値とともに 1 つのペインに表示されます。ダッシュボードのワークスペースペインで OVTA Console を起動して使用すれば、トランザクションをより詳細に監視できます。

必ずプローブロケーションを追加してください。これは、OVIS が OVTA からの測定値のインポートを開始するときに必要です。OVTA との統合では、デフォルトのプローブロケーション、[ローカルシステム] を選択します。

測定値を収集するためには、OVIS 設定マネージャを終了する前に設定を保存する必要があります。

タスク 3: SLO と SLA の設定

OVIS と OVTA の測定を組み合わせると、可用性、応答性、ボリュームの領域で SLO (サービスレベル目標値) および SLA (複数の SLO で構成されるサービスレベル契約) を設定できます。応答性、ボリュームに関しては、OVTA の測定データを利用して、パフォーマンスの SLO および SLA を設定できます。

SLO の設定 : OVIS 設定マネージャの左ペインで、OVTA 統合用に設定した [監視対象サービス] の下にある [サービス目標値] を選択し、右クリックして [目標値の新規作成] を選択します。[目標値の情報] ダイアログで、収集するメトリックに基づいて、OVTA 用サービスレベル目標値を設定します。SLO を設定する方法については、このダイアログのオンラインヘルプを参照してください。

OVO または NNM へのアラーム送信の設定 : アラームを OVO または NNM に送信する場合は、アラームの送信先を設定する必要があります。OVIS 設定マネージャで、[**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、アラームの送信先を選択します。OVIS と OVO または NNM との統合を設定していない場合は、統合の設定も行う必要があります。詳しい手順は、この章で後述します。

OVIS ダッシュボードにアラームを表示するには、設定マネージャで [アラーム送信先] セクションの [**データベース (アラームと NNM　の統合)**] チェックボックスにチェックマークを付ける必要があります ([**ファイル**] > [**設定**] > [**アラーム送信先**])。

SLA の設定 : OVIS 設定マネージャの左ペインの、同じ OVTA サービスグループのツリービューで、[サービス契約] を右クリックし、[サービス契約の新規作成] を選択して SLA を設定します。

設定に加えた変更は、設定マネージャを終了する前に必ず保存してください。

331 ページの「SLO と SLA の例」 で、OVTA データに対して設定できる SLO および SLA の例を紹介しています。

各種トランザクションタイプについて SLO を設定する場合は、複数のサービスグループの設定が必要になることがあります。たとえば、1 つのサービスグループには、ボリュームの SLO について Web サーバーで測定されるトランザクショ

ンタイプだけが含まれ、別のサービスグループには、エンドツーエンドの応答性の SLO についてクライアント側で測定されるトランザクションタイプだけが含まれる場合があります。

タスク 4: 設定の保存とステータスの確認

測定値を収集するためには、OVIS 設定マネージャを終了する前に設定を保存する必要があります。

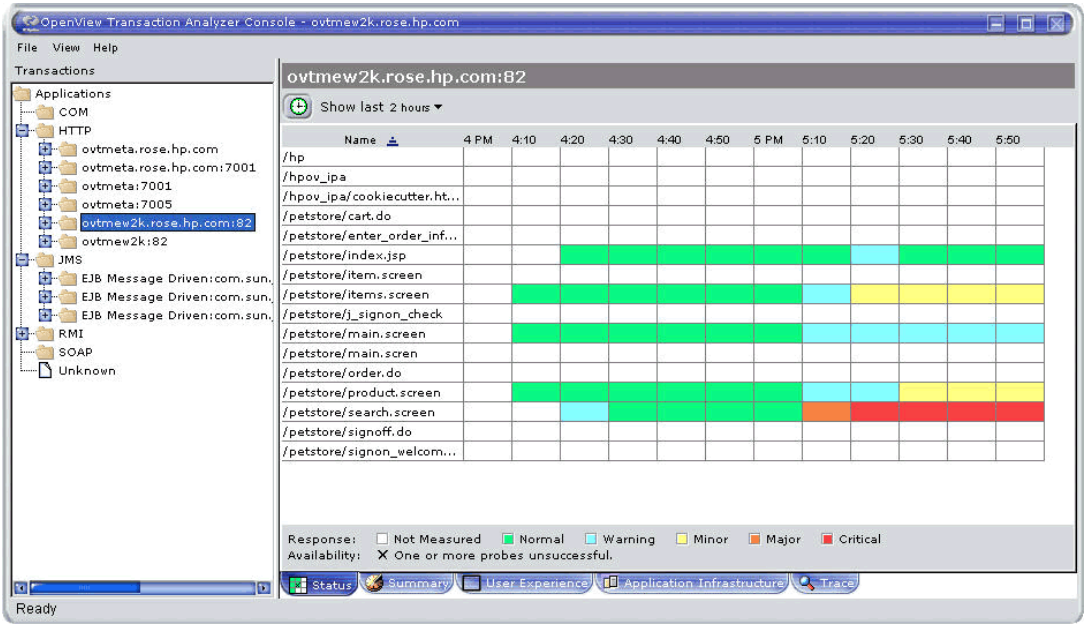
設定を保存してから 10 ～ 15 分経過すると、データが収集されます。データが収集されたら、OVTA からインポートされた新しい OVTA ベースの監視対象サービスのステータスを確認します。OVIS 設定マネージャで、左ペインの [**ステータス**] を選択します。最後のレポート間隔において、OVTA トランザクションモニタで測定されたトランザクションがある場合は、監視対象サービスのステータスが緑色になります。ステータスが赤色の場合は、単純にそれらのトランザクションを構成する Web ページに対するアクセスが行われなかったか、OVTA トランザクションモニタが有効になっていない可能性があります。詳細は、第 6 章「トラブルシューティング情報」を参照してください。

タスク 5: OVIS ダッシュボードを使用した、OVTA トランザクションの監視

OVIS ダッシュボードを使用して、OVIS で設定された OVTA トランザクションの監視を行うことができます。より詳細な監視が必要な場合は、OVIS ダッシュボードからワークスペースペインにある [OVTA] リンク () を選択して OVTA Console を起動します。

このリンクを選択すると、「OVTA アプリケーションを起動するには Java Web Start がインストールされている必要がある」ことを警告するページが表示されます。[**OVTA Console の起動**] ボタンを選択します。OVTA Console が起動して、[Stauts] タブが表示されます。

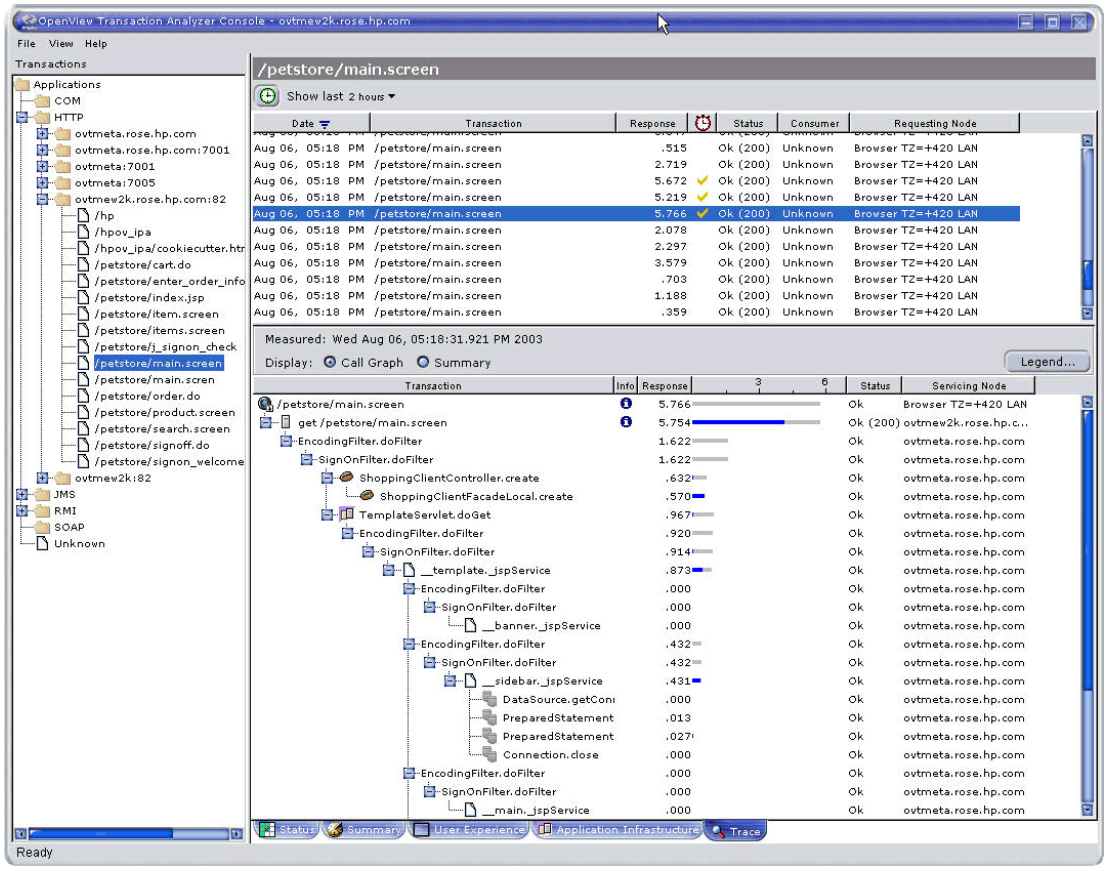
OVTA Console を次の図に示します。



タスク 6: OVIS ダッシュボードにあるトレース機能の使用

OVISダッシュボードの[状況]ワークスペースで[アラーム]タブの[トレース]列にある [OVTA] アイコン ( ) をクリックすると、状況に応じた OVTA Console が起動されます。対応するトランザクションが自動的に選択され、そのトランザクションのトレースビューが表示されます。

次の図に、OVTA Console にある [Trace] タブの例を示します。



OVIS はトレースデータを最大 30 日間保存しますが、OVTA の設定方法によってはこの大量のデータを保管できない場合があります。OVTA データベースから削除されているトランザクションを選択すると、トランザクションの定義が見つからないことを示すエラーメッセージが表示されます。

タスク 7: OVTA レポート

OVIS ダッシュボードの [レポート] ワークスペースで、OVTA 固有のデータを含むレポートを表示できます。これらのレポートの詳細は、『*OVTA ユーザーガイド*』を参照してください。

- OVTA Service Group Summary (OVTA サービスグループの概要)

- OVTA Application Summary of Activity for the Last Day (OVTA アプリケーションの前日のアクティビティの概要)
- OVTA Application Summary of Activity for the Last Week (OVTA アプリケーションの先週のアクティビティの概要)
- OVTA Application Response Time Violations (OVTA アプリケーションの応答時間違反)
- OVTA Application Response Time (OVTA アプリケーションの応答時間)
- OVTA Application Transaction Volume (OVTA アプリケーションの処理量)
- OVTA Application Response Time Violations (Consumer Perspective) (OVTA アプリケーションの応答時間違反 (コンシューマの観点))
- OVTA Application Response Time Violations (Consumer/System Detail) (OVTA アプリケーションの応答時間違反 (コンシューマ / システム詳細))
- OVTA Application - Worst Performing Transactions (OVTA アプリケーション - パフォーマンスの最低な処理)

タスク 8: SLO と SLA のしきい値の調整

生成されたアラームの内容、ダッシュボードに表示されたデータ、およびレポートに基づき、アラームとレポートをより意味のあるものにするために、しきい値を調整することができます。SLO と SLA を変更するには、OVIS 設定マネージャを使用します。応答時間しきい値を設定するには、OVTA Configuration Editor を使用します。

未使用の OVIS レポートを削除する (オプション)

OVIS 管理サーバーを OVTA データのインポートにだけ使用している場合は、夜間に自動生成される未使用の OVIS レポート (30 レポートを超える) を削除したほうがよい場合があります。そうすれば、空のレポートを削除して夜間のレポート生成周期を短縮することができます。

こうした OVIS だけのレポートを簡単に削除できるように、次のファイルが用意されています。

```
<install dir>¥newconfig¥packages¥remove
¥reload_IOPS_remove_OVIS_reports.SRP
```

夜間の処理から、使用されていない OVIS プローブレポートのテンプレートを削除するには、次のコマンドを実行します。

```
reload -remove reload_IOPS_remove_OVIS_reports.SRP
```

後で OVIS プローブを使用する必要が発生した場合は、上記のコマンドから "-remove" を外し、この SRP ファイルを指定して再実行します。

SLO と SLA の例

可用性

インポートした OVTA の測定データのために可用性の SLO および SLA を設定することは可能ですが、この設定は、実際には必要ありません。より直接的な方法は、OVIS で OVTA トランザクションに対応する OVIS HTTP 監視対象サービスを設定し、OVIS http プローブの測定値を使用して可用性の SLO および SLA を設定することです。

応答性

OVTA 測定データの RESPONSE_TIME メトリックは、5 分間の平均値です。したがって、このメトリックは概略的な監視にのみ有用です。応答性の SLO と SLA を実施するためには、応答時間違反の回数および割合 (RESPONSE_TIME_VIOLATION_COUNT および RESPONSE_TIME_VIOLATION_PERCENTAGE) について SLO を設定する必要があります。

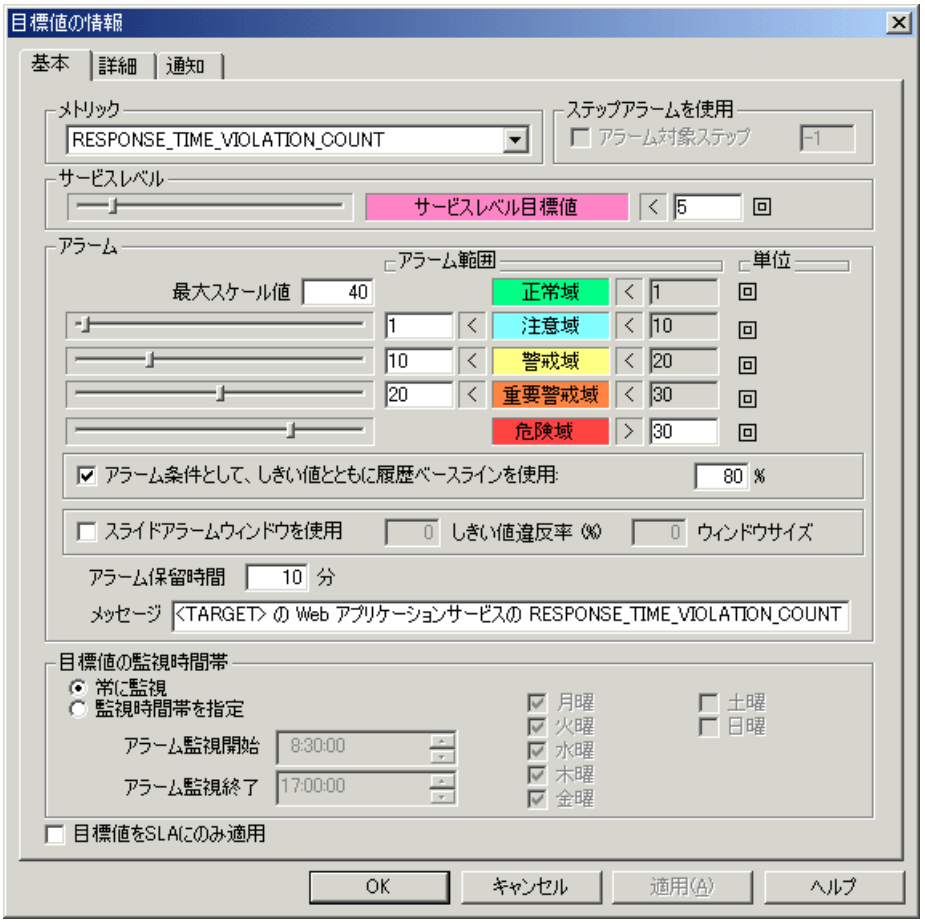
OVTA トランザクションの応答時間違反しきい値を、OVIS 設定マネージャで設定することはできません。目的のトランザクションについてしきい値を設定するには、OVTA Configuration Editor を使用します。RESPONSE_TIME_VIOLATION_COUNT メトリックと RESPONSE_TIME_VIOLATION_PERCENTAGE メトリックは、OVTA トランザクションエージェント内で、これらの設定済みしきい値に対して測定されます。詳細は、『*OVTA ユーザーガイド*』を参照してください。

応答性の SLO について WEBAPP サービスグループ内で選択されたトランザクションタイプは、クライアント側でも Web サーバー側でも測定できます。すでに説明したように、Web サーバーで測定されたトランザクションの名前には、http メソッドの接頭辞が付きます。OVTA Browser Client Monitor を使用している場合は、応答性の SLO をクライアントのトランザクションタイプに対して設定できます。ただし、このトランザクションタイプがプローブの対象でもある場合は、この SLO が、プローブと OVTA Browser Client Monitor の両方で測定される応答時間メトリックに対して適用されます。

以下の例では、WEBAPP サービスを使用します。

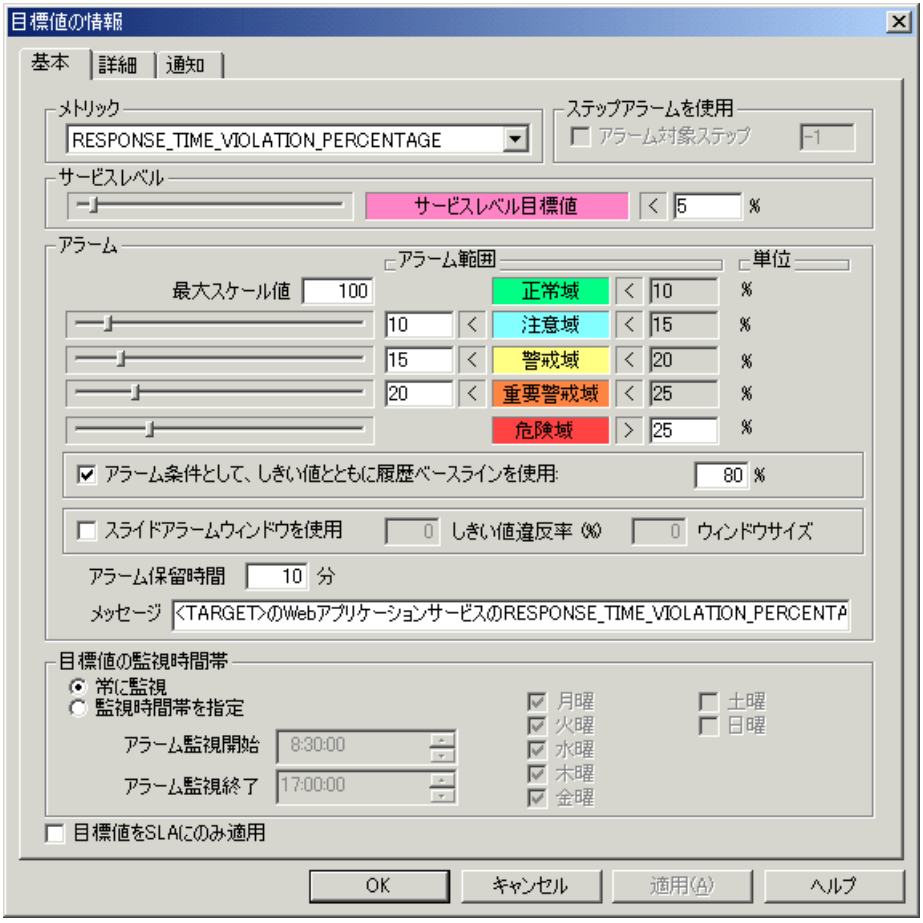
応答性の SLO の例 1

Web ページのヒット数が 5 未満であれば、5 分間の測定間隔の間にその応答が OVTA で設定された応答時間しきい値を必ず超えるように設定します。



応答性の SLO の例 2

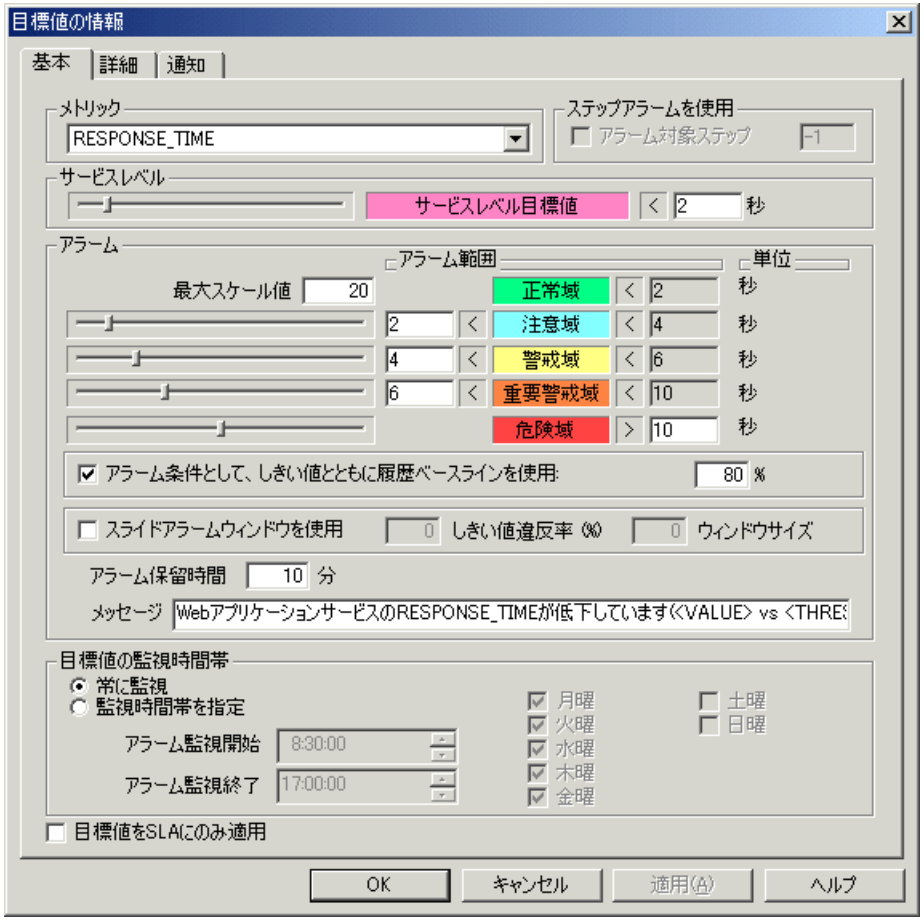
Web ページのヒット数が 5% 以下であれば、測定間隔の間にその応答時間が OVTA で設定された応答時間しきい値を必ず超えるように設定します。



応答性の SLO の例 3

平均応答時間が 2 秒未満になるように設定します。

注記 : これは単一トランザクションに適しています。SLO は 5 分間の平均に適用されるため、個々のトランザクションの応答時間の値が非常に高い (または低い) 場合があると、平均が偏る可能性があります。単一トランザクションの場合でも、平均が、エンドユーザーの実際の状況をよく表すとは限りません。すでに説明したように、応答時間しきい値の回数メトリックや割合メトリックは、応答時間の SLO を実施するうえでより有用です。

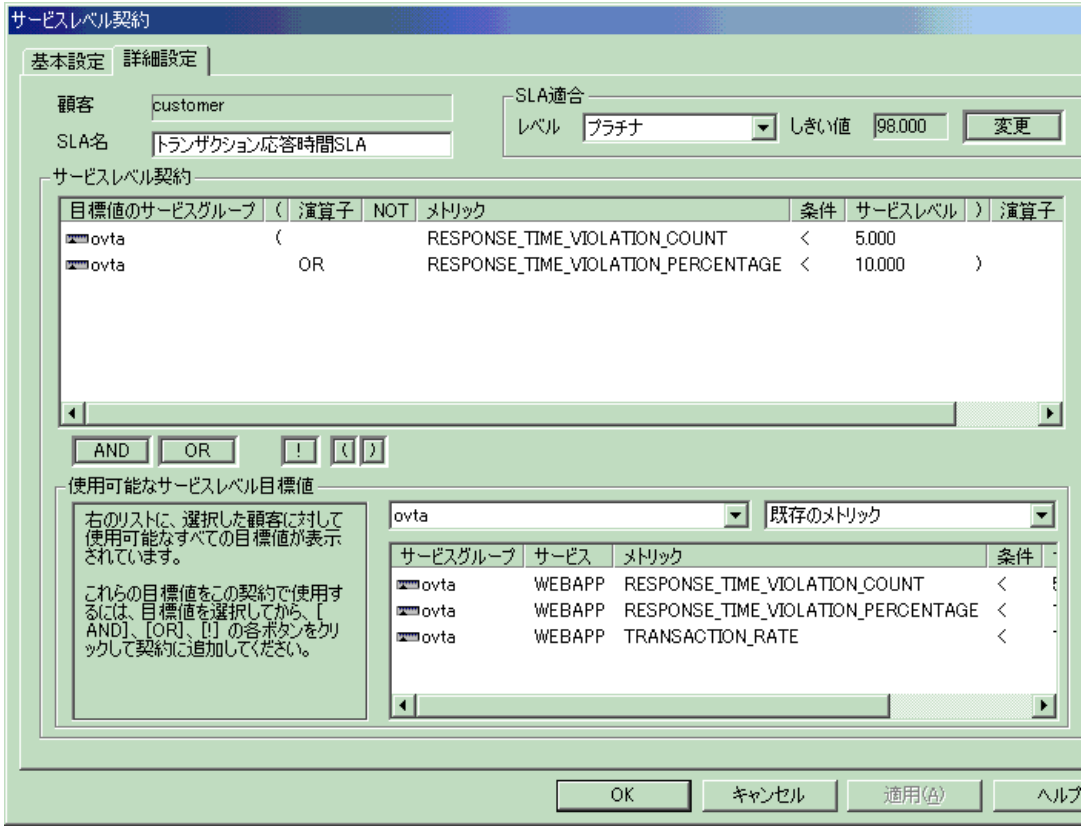


応答性の SLA

複数の SLO を組み合わせて SLA を強化することができます。

使用例 : Web ページのヒット数が 5% 以下であれば、5 分間の測定間隔の間に、その応答時間が、OVTA で設定された応答時間しきい値を超えるか、応答時間しきい値違反の総数が 10 を超えないように設定します。

応答時間違反の回数と割合の SLO をこのように組み合わせると、応答時間の SLO 違反率が高くなっても、総 SLO 違反数が高くならない限り (つまり、相応のサンプル数を収集できない限り)、SLA に違反するのを防ぐことができます。



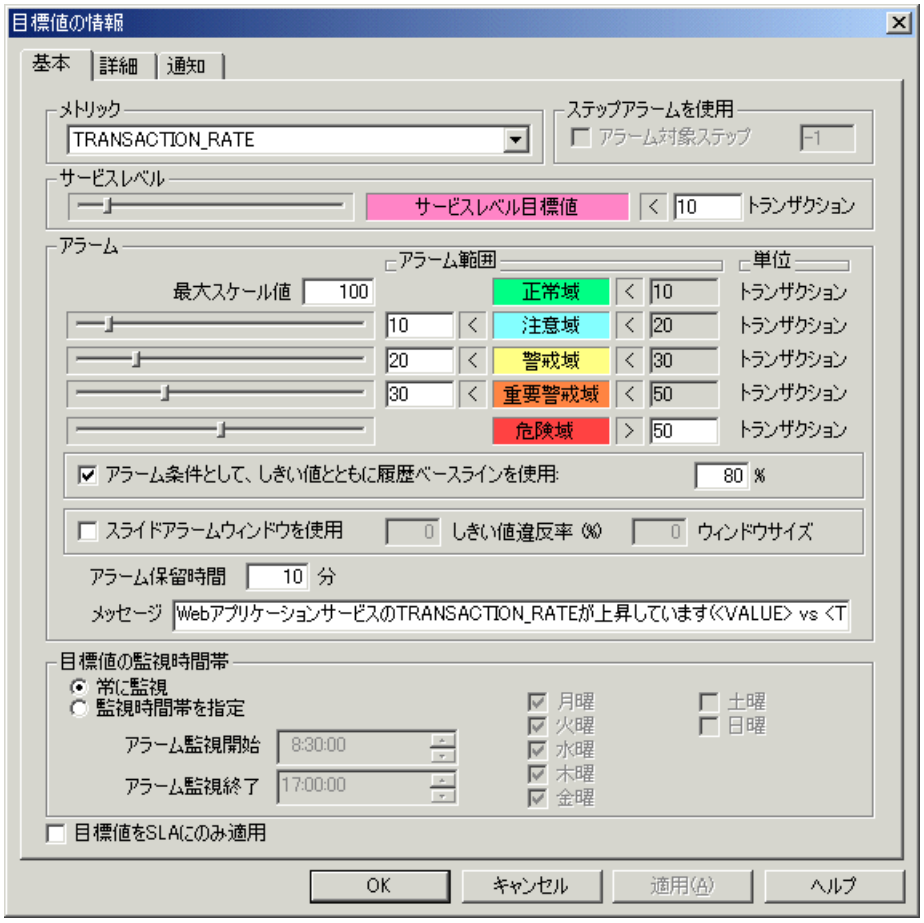
ボリューム

TRANSACTION_RATE メトリックを使用して、ボリュームの SLO を設定できます。これは、SLA の設定時に、応答性の SLO と組み合わせて使用することもできます。

注記 : 実際のボリュームの SLO は、Web サーバーで OVTA Web Server Transaction Monitor を使用してのみ、測定できます。したがって、ボリュームの SLO を設定する、サービスグループ内のトランザクションは、Web サーバートランザクションに限定する必要があります。これらのトランザクションの名前には、http メソッドの接頭辞 (**get** または **post**) が付きます。

ボリュームの SLO の例 1

使用例 : 秒当たりのヒット数が 10 以下になるように設定します。

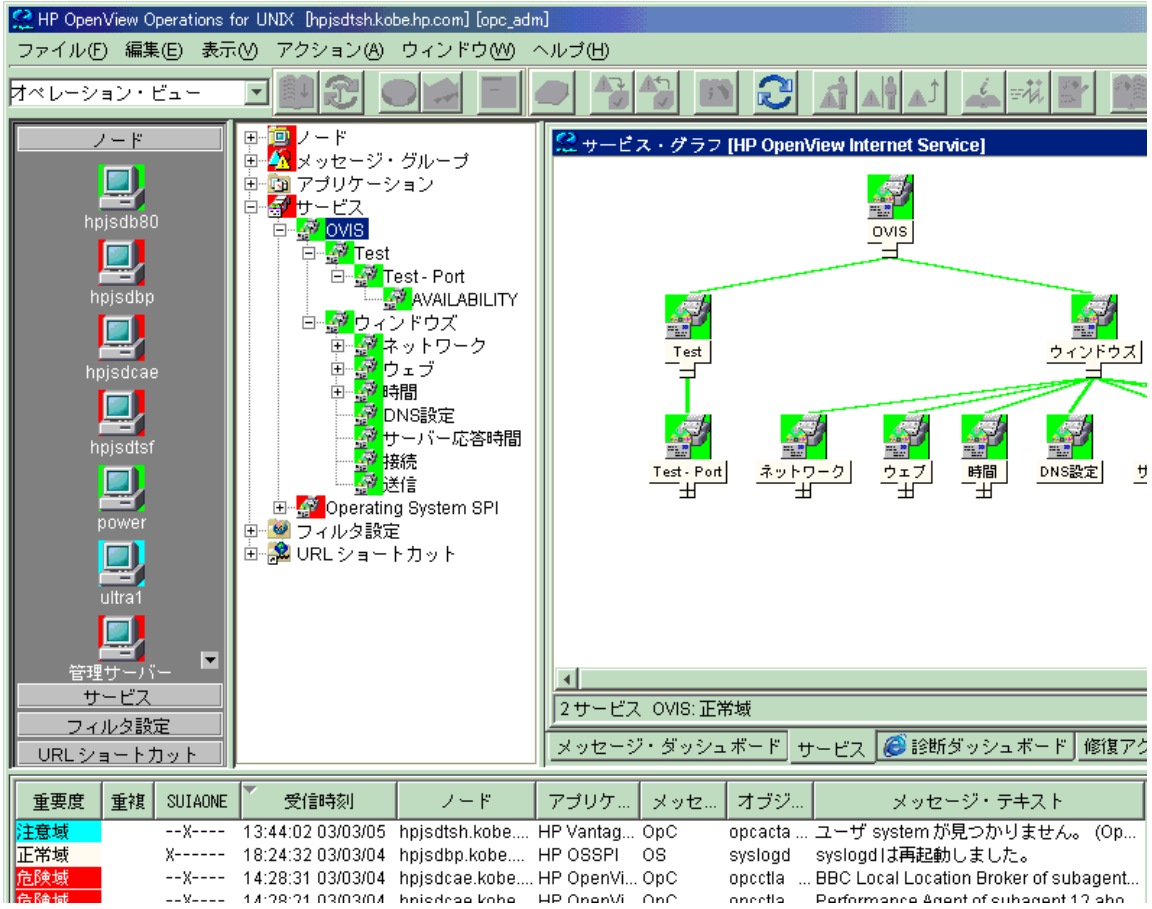


OpenView Operations for UNIX との統合

OVIS と OpenView Operations for UNIX (OVO) を統合するには、OVO for UNIX 管理サーバーに OVO for UNIX 用の OVIS 統合パッケージ (OVIS CD に収録) をインストールします。そうすれば、OVO コンソールで、Internet Services のテンプレートを OVIS 管理サーバーとプローブシステムへ配布して、プローブデータを OVO へ転送することができます。OVO と統合すると、次のことが行えるようになります。

- OVO メッセージブラウザで、Internet Services のサービス目標値違反をアラームとして表示する。
- OVO コンソールで、OVIS メッセージグループのアラームを整理統合したり、OVIS_Errors メッセージグループの、Internet Services 管理サーバーやプローブのエラーを整理統合する。
- OVO Service Navigator で、Internet Services の顧客 / サービスグループ / サービス目標値ツリーを表示する。
- OVO メッセージブラウザで、opcmsg テンプレート内のオペレータ操作の一部として、Internet Services ダッシュボードを起動する。
- Internet Services 管理サーバー上のログファイルテンプレートに基づいた、Internet Services ステータスログファイル (status.reporter および status.iops) から追加情報を取得する。
- Internet Services スケジューラと IIS Web Server の自己監視。
- 新しいメッセージインターセプタテンプレート (OVIS Alarms (3)) により、障害アラーム (危険域、警戒域、重要警戒域、注意域、および正常域) 間に状態ベースでの相関処理を提供。つまり、古いアラームが自動的に受諾され、履歴ブラウザに配置されることで、目標値の現在のステータスが反映されます。状態ベースの相関処理を行うには、[Continuous Alarming] オプションを有効にする必要があります。
- 顧客のコンテキストに合わせて、OVIS ダッシュボードの起動契機となる OVO アクションを設定できます。ただし、OVIS の表示設定を制限すると、ダッシュボードを起動したときにログイン画面が表示され、次に、その顧客に合わせた詳細な表示ではなく、ダッシュボードのメインページが表示されます。

- 統合パッケージは、日本語版 OVO for UNIX (6 および 7) を実行している日本語環境のシステムにインストール可能です。テンプレートはまだローカライズされていません。



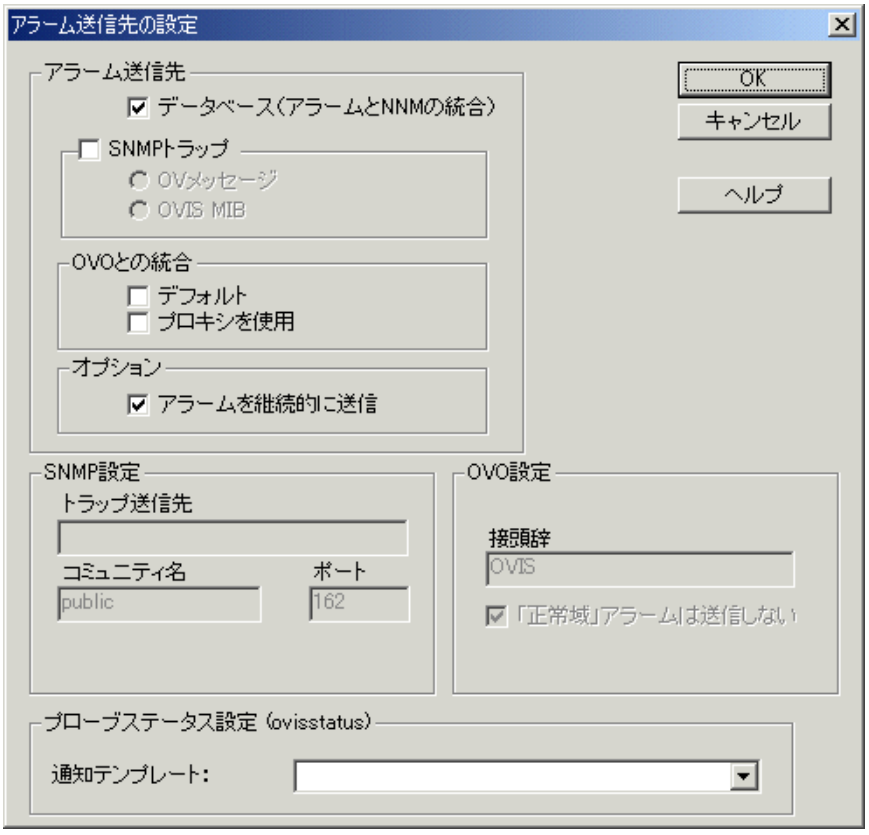
要件

- OVO の UNIX バージョンの要件については、『*Internet Services リリースノート*』を参照してください。
- Internet Services ダッシュボードの Web ページを表示するには、バージョン 1.7 以上の Mozilla を OVO 管理サーバーにインストールする必要があります。ブラウザは **ovweb** コマンドで起動されます。正しいセットアップ方法については、**ovweb** マンページを参照してください。
- Windows システムの OVO Java GUI で Internet Services ダッシュボードが正しく表示されるようにするには、[**編集**] > [**表示設定**] で Web ブラウザのオプションを [ActiveX Internet Explorer コントロール] に設定する必要があります。
- Internet Services ダッシュボードの統合、アラームメッセージの OVO への転送、および Service Navigator の統合には、OVIS 管理サーバー上に OVO エージェントをインストールして実行しておく必要があります (OpenView Operations、Service Navigator、swinstall の詳細は、OpenView Operations のマニュアルと swinstall マンページを参照してください)。
- OVO 7.x の場合は、OVO エージェントと OVIS を C ドライブにインストールする必要があります (最新の OVO NT エージェントパッチがインストールされている場合を除く)。
- アラームを OVO に転送するには、Internet Services 設定マネージャの [アラーム送信先の設定] ダイアログでチェックボックスを正しく選択する必要があります。
- 日本語環境の OVO システムに統合製品をインストールする場合は、LANG=ja_JP.SJIS で swagentd を開始する必要があります。
  root アカウントでログインし、以下のコマンドを実行します。
  export LANG=ja_JP.SJIS
  swagentd -r

設定オプション

Internet Services 設定マネージャを使用すれば、2 つのいずれかのオプションを選択して、Internet Services のデータを OpenView Operations for UNIX に転送できます。オプションは以下のとおりです ([**ファイル**] > [**設定**] > [**アラーム送信先**] を選択してアクセスできます)。[アラーム送信先] を選択した後、設定マネージャを終了する前に、必ず [**プローブ設定の保存**] を選択してください。

- **OVO との統合 - デフォルト :** デフォルトを選択すると、OVO for UNIX に送信される Internet Services メッセージだと識別するが、Internet Services 管理サーバーから送信されるようになります。この設定を行うには、Internet Services 管理サーバーが OVO for UNIX の管理対象ノードに追加されていて、Internet Services 管理サーバーが OVO エージェントを実行している必要があります。



- **OVO との統合 - プロキシを使用 :** このモードを選択すると、Internet Services 監視対象サービスのノードに応じて、各 Internet Services メッセージの送信元が識別されます。これを設定するためには、Internet Services 管理サーバー、Internet Services プローブがインストールされているシステム、および Internet Services 監視対象サービスのノードを OVO for UNIX の登録ノードに追加する必要があります。監視対象サービスのノードに、OVO for UNIX エージェントをインストールする必要はありません。
- **OVO 設定 - 接頭辞 :** 接頭辞 (OVIS など) を入力することで、OVIS 監視サービスのメッセージグループが自動的に作成されます。障害メッセージを自動的に受諾するには、[「正常域」アラームは送信しない] チェックボックスをオフにします (OVIS Alarms (2) または OVIS Alarms (3) テンプレートが必要)。

統合の手順

概要

Internet Services 統合パッケージをインストールして、OVO for UNIX とともに使用できるようにするには、次のタスクを実行する必要があります。手順の詳細は、後述のタスクを参照してください。

- 既存の統合パッケージをアンインストールします (テンプレートに行ったすべての変更が失われます)。
- Internet Services インストール CD を使用して、Internet Services コンポーネントを OVO 管理サーバーにインストールします。CD に収録されているインストール手順を参照してください。
- OVO for UNIX コンソールから、新しい OVIS テンプレートを割り当てて配布します。

タスク 1: 以前のバージョンからのアップグレードの準備

以前のバージョンからのアップグレード : 新しい統合パッケージをインストールする前に、以下の手順に従って既存のテンプレートを削除する必要があります。

テンプレートに行ったすべての変更が失われます。

すべての Internet Services OVO のテンプレートを、OVIS 管理サーバーおよびすべての OVIS プローブシステムから割り当て解除します。

1 OVO の [**メッセージソースのテンプレート**] ウィンドウで次の手順を実行します。

   a 左ペインの [テンプレートグループ] リストの [Internet Services] をダブルクリックします。

   b 右ペインの各エントリを選択し、以下の各グループについて、[**全てから削除 ...**] ボタンをクリックします。

   OVIS Probe NT
   OVIS Probe Unix
   OVIS Server
   OVIS Server (2)
   OVIS Server (3)
   OVIS ITO Mgmt Server

c 左ペインで [Internet Services] を再度選択し、[**全てから削除 ...**] ボタンをクリックします。

d 右ペインで以下のような「OVIS」を含む各アイテムを選択し、[**全てから削除 ...**] を選択します。

Message OVIS Alarms
Message OVIS Alarms (2)
Message OVIS Alarms (3)
Logfile OVIS Errors (Probe)
Logfile OVIS Error (Probe-Unix)
Logfile OVIS Errors (Server-OVIS)
Logfile OVIS Errors (Server-Reporter)
Monitor OVIS_SM_InetInfo
Monitor OVIS_SM_Sched
Monitor OVIS_SM_Sched_UX
Schedule OVIS Service Sync

e [登録メッセージグループ] ウィンドウにアクセスし、OVIS および OVIS_Errors グループを削除します (存在する場合)。

f swremove コマンドを使用して統合パッケージをアンインストールします (swremove HPVPIS-SP)。

グループを削除してもグループが削除されるだけで、グループメンバーは削除されません。すべてのグループメンバーを削除するには、上記の手順を完了する必要があります。

タスク 2: 統合パッケージのインストール

以前のバージョンからアップグレードする場合は、最初に上記のタスク 1 を完了して既存の OVIS/OVO 統合テンプレートを削除してから、新しい統合パッケージをインストールします。

1 OVIS インストール CD に収録されている OVO 統合インストール手順 (**readme.txt** または OVIS CD に付属のインストールドキュメントのハードコピー) に従います。

2 OVIS 設定マネージャで [**プローブ設定の保存**] ツールバーボタンを選択します。

3 次のタスクを実行して、新しいテンプレートを配布します。

タスク 3: Internet Services のプローブに基づいたアクティブモニタリング用テンプレートの配布

指定した OVO for UNIX 管理者 / オペレータ用メッセージブラウザでアラームやメッセージを表示、監視できるように、Internet Services システムを設定するには、以下の手順に従います。

1. 管理者として OVO コンソールを起動します (たとえば、`opc -user opc_adm -passwd OpC_adm` と入力します)。
2. Internet Services 管理サーバーシステムを OVO 管理対象ノードとして設定します ([**アクション**] > [**ノード**] > [**追加**])。[登録ノード階層] プルダウンメニューから [登録ノード階層] ウィンドウを選択します。

   [ホスト名] フィールドにノード名を入力し、[**Tab**] を押します。ウィンドウが更新されたら、以下の設定を確認します。

   [ネット・タイプ] - IP Network

   [マシン・タイプ] - Intel x86/Px

   [OS 名] - Windows NT/2000

   [管理対象ノードのタイプ] - VPO 管理対象
3. Internet Services 管理サーバーに OVO エージェントをインストールします。OVO エージェントのインストールについては、『*OVO for UNIX システム管理リファレンスガイド*』を参照してください。OVO 7.x の場合は、両方とも C ドライブにインストールする必要があります (OVO NT エージェントパッチがインストールされている場合を除く)。OVIS サーバーを再起動します。
4. Internet Services プローブがインストールされているすべてのシステムを、OVO 対象ノードとして設定し、プローブがインストールされている各システムに、OVO エージェントがインストールされていて実行されていることを確認します (これらのノードに OVO エージェントをインストールする必要がない場合については、以下の注記を参照)。

   OVIS で [**OVO との統合 - プロキシを使用**] をアラーム転送モードとして使用する場合は、すべての Internet Services 監視対象サービスノードを OVO ノードとして設定します。この場合、これらのノードに OVO エージェントをインストールする必要はありません。

5 Internet Services プローブがインストールされているシステム (ノード) を OVO ノードグループに追加します ([**ウィンドウ**] > [**登録ノードグループ**])。最初にノードグループが作成されていることを確認してから、OVIS ノードを [登録ノード階層] ウィンドウから新しいノードグループにドラッグアンドドロップします。

6 OVO ノードグループ (Internet Services ノード用) と、OVIS および OVIS-Error メッセージグループを、Internet Services のサービスの応答、監視を行う OVO ユーザー (オペレータや管理者) に割り当てます。これらの割り当てを行うことで、OVIS メッセージが OVO メッセージブラウザに表示されるようになります。[**ウィンドウ**] > [**登録ユーザ**] を選択します。適切なオペレータ (たとえば、opc_adm) を選択し、右クリックして [変更] を選択します。[ユーザーの変更] ウィンドウで [**作業範囲**] ボタンを選択して、OVIS メッセージグループおよび OVIS-Error メッセージグループを割り当てます。このウィンドウで [**閉じる**] を選択し、[ユーザーの変更] ウィンドウで [**OK**] を選択します。

7 [登録ノード階層] ウィンドウに移動します。

ログファイル **OVIS Errors (Server - Reporter)** および **OVIS Errors (Server - OVIS)** が、OVIS のインストールディレクトリを正しく参照するよう設定を変更します (例 : "C:¥Program Files¥HP OpenView¥Data" または C:¥rpmtools)。Windows では、パスにスペースが含まれている場合は、引用符で囲む必要があります。

a [登録ノード階層] ウィンドウで、OVIS サーバーノードを強調表示して、[**アクション**] > [**エージェント**] > [**テンプレートの指定**] を選択します。

b [ノード/テンプレートの指定] ウィンドウで [**追加**] ボタンを選択すると、[ノード / テンプレートの追加] ウィンドウが表示されます。

c [ノード/テンプレートの追加] ウィンドウで [**テンプレートウィンドウ**] ボタンを選択すると、[**メッセージソースのテンプレート**] ウィンドウが表示されます。

d 左ペインで Internet Services テンプレートグループを強調表示し、**Group OVIS Probe NT** と、**Group OVIS Server**、**OVIS Server (2)** または **OVIS Server (3)** グループのいずれかを選択します (グループの選択方法については、以下の注記を参照してください)。

テンプレートグループには OVIS Server、OVIS Server (2)、OVIS Server (3) の 3 つがあります。いずれか 1 つだけを割り当ててください。通常は、状態ベースの相関処理を行う場合は OVIS Server (3) テンプレートグループを使用し、正常 / 不正メッセージ相関処理を行う場合は、OVIS Server (2) を使用します。OVIS Server テンプレートグループは、相関処理機能を提供しないため、OVIS Server (3) テンプレートバージョンの使用をお勧めします。また、OVIS Server (2) または OVIS Server (3) テンプレートグループを使用する場合は、OVIS 設定マネージャの [アラーム送信先の設定] ダイアログ ([**ファイル**] > [**設定**] > [**アラーム送信先**] を選択) にある [「正常域」アラームは送信しない] チェックボックスをオフにする必要があります。

e [ノード/テンプレートの追加] ウィンドウに戻り、[**選択テンプレートの取得**] ボタンを選択して、[**OK**] をクリックします。

f [ノード / テンプレートの指定] ウィンドウで、[**OK**] をクリックします。

g [メッセージソースのテンプレート] ウィンドウを閉じます。

8 **OVIS Probe UNIX** または **OVIS probe NT** テンプレートグループを、上記で説明したとおり、プローブがインストールされている各システムに割り当てます。OVIS 管理サーバーをプローブシステムとしても使用するには、そのシステムに OVIS probe NT テンプレートグループも割り当てます。

Windows システムの場合、OVIS のインストールディレクトリを正しく参照するように **OVIS Errors (Probe)** ログファイルを変更します (例 : `"C:¥Program Files¥HP OpenView¥Data"` または `C:¥rpmtools`)。Windows では、パスにスペースが含まれている場合は、引用符で囲む必要があります。

タスク 4: Internet Services と OVO for UNIX Service Navigator (JAVA GUI がインストールされた VPO A.06.xx 以降) の統合

1 ローカル OVO エージェントが OVO 管理サーバー上で実行されていることを確認します。

2 **OVIS ITO Mgmt Server** テンプレートグループを OVO 管理サーバーに割り当てます。

3 **OVIS ITO Mgmt Server** テンプレートグループで、**OVIS Service Sync** スケジュール済みアクションテンプレートを選択して、Internet Services 管理サーバー名をコマンドラインに追加します。Internet Services 管理サーバーの完全修飾ホスト名を含めます (例 : `/opt/OV/OVIS/bin/vpispull.sh jester.dev.hp.com`)。このスクリプトは、Internet Services の顧客、サービスグループ、目標値の階層を Service Navigator に 5 分ごとに同期します。デフォルトでは、Internet Services のサービスは `OVO` 管理者 `opc_adm` に割り当てられます。追加のオペレータは、opcservice コマンドで割り当てる必要があります (OpenView Operations for UNIX のマニュアルを参照してください)。

タスク 5: 統合の完了

1 次にテンプレート (任意で Service Navigator 統合のスケジュールも) を、OVIS サーバー上で動作している OVO エージェントに配布する必要があります。

a 登録ノードから OVIS Server ノードを選択し、メニューからメニューオプション [**アクション**] > [**エージェント**] > [**ソフトウェアのインストール / 更新と設定**] を使用します。

b [**ソフトウェアと設定のインストール/更新**] ウィンドウで、[コンポーネント] の下の [エージェントソフトウェア] をオフにします。[強制アップデート] など、これ以外のオプション ([テンプレート]、[アクション]、[モニタ]、[コマンド]) はすべてオンにします。

c [**OK**] を押します。配布に成功すると、OVO メッセージブラウザに適切なメッセージが表示されます。

2 OVIS 設定マネージャで [アラームの送信先] を設定し、[**OVO との統合**] で以下のいずれかをオンにします。設定を変更した場合は、設定マネージャを終了する前に [**プローブ設定の保存**] を選択します。

デフォルト (詳細は、341 ページの「設定オプション」を参照してください)

または

プロキシを使用 (すべての Internet Services 監視対象サービスノードを OVO ノードとして設定する必要がありますが、各ノードに OVO エージェントをインストールする必要はありません)

タスク 6: Internet Services 管理サーバー上に OVO エージェントを再インストールした場合の手順

1 まず、IIS と hp OpenView Reporter サービスを停止します。

```
net stop iisadmin /y
net stop reporter
```

2 エージェントを再インストールして、IIS と Reporter サービスを開始します。

```
net start W3SVC
net start reporter
```

OVO に転送する OVIS メッセージ

OVIS は、アラームメッセージを転送するときに、以下の OVO 属性セット (opcmsg) を使用します。

opcmsg [-help] [-id] [severity=normal|warning|minor|major|critical]
application=<application> object=<object> msg_text=<text>
[msg_grp=<message group>] [node=<node>] [service_id=<svcid>]
[-option <var>=<value>]

表 4　メッセージ転送用の opcmsg 属性

OVO の属性 (opcmsg)	OVIS の値
object	監視対象ホスト : プローブシステム : 監視対象情報
msg_grp	OVIS_< プローブ名 >
node	OVIS サーバーの FQDN (プロキシが GUI で設定されている場合は、対象ノードの FQDN)
msg_txt	メッセージテキスト
application	OVIS
severity	OVIS の重要度
option 変数	host=< 監視対象ホスト > ps=< プローブシステム > target=< 監視対象情報 > vpis=<OVIS サーバーの FQDN> customer=< 顧客 > customerURLE=< 顧客 > serviceGroup=< サービスグループ > serviceGroupURLE=< サービスグループ > probeDesc=< プローブの説明 > probeDescURLE=< プローブの説明 > probeType=< プローブ名 > probeTypeURLE=< プローブ名 > metric=< メトリック > ipAddr=< 監視対象の IP アドレス (可能な場合)> psts=< 測定値が取得されたときのタイムスタンプ (UTC)>

さらに、ovisstatus.exe プログラムが自動的に実行され、予測時間 + 10% (多少の遅れを許容する時間) 以内にデータがプローブシステムから受信されない場合は、OVO または NNM にアラームを送信します。

Network Node Manager との統合

Internet Services を NNM と統合すると、NNM は Internet Services データベースから設定およびイベント情報を受信します。これらは NNM の以下の 2 つの領域を追加します。

1. **アラームとメッセージ**。これらは、NNM アラームシステムに自動的に転送され、新しい Internet Services アラームカテゴリに表示されます。これらのアラームは、NNM の他のアラームと同様、外部スクリプトの起動やオペレータの呼び出しなどの自動アクションを実行できます。
2. Internet Services の監視対象サービスがある、NNM 管理対象ノードの**新しいサブマップシンボル**。新しいシンボルは、ノードがサービスを提供する顧客、それらの顧客に提供するサービス、および各サービスのパフォーマンス目標値を表します。

Internet Services 設定マネージャのダイアログ ([**ファイル**] > [**設定**] > [**アラーム送信先**] でアクセス可能) でチェックボックスを選択することで、Internet Services はアラームを生成するようになります。アラームは、NNM に転送されると、[Internet Services] アラームカテゴリに表示されます。

さらに、ovisstatus.exe プログラムが自動的に実行され、予測時間 + 10%(多少の遅れを許容する時間) 以内にデータがプローブシステムから受信されない場合は、OVO または NNM にアラームを送信します。

Internet Services の統合を開始するには、まず Internet Services の NNM 統合ソフトウェアを NNM 管理ステーションにインストールします。Internet Services には、Solaris、HP-UX、または Microsoft Windows オペレーティングシステム向けの NNM 用統合ソフトウェアが付属しています。

NNM 統合の要件 / 推奨事項

- NNM のバージョンとパッチの要件に関する重要な情報については、『*Internet Services リリースノート*』を参照してください。
- Windows に Internet Services の NNM 統合ソフトウェアをインストールしているときに、ターミナルサービスが一時的に使用できなくなる場合があります。
- 統合パッケージに付属の OVIS-NNM 統合リリースノートを参照してください。パッケージをインストールした後、これらのリリースノートは、UNIX システムの場合、`/opt/OV/www/htdocs/C/ReleaseNotes/ovisnnm_releasenotes.html` で参照できます。Windows システムの場合は、インストール完了後に表示されます。
- HP OpenView Customer Views for Network Node Manager も利用される場合は、Internet Services で定義されている顧客 / 組織が追加され、それらに対応する監視対象が自動的に関連付けられ統合されます。
- NNM を統合するには、IP サブマップをすべてのレベルで固定する必要があります。これは、UNIX ベースの NNM ではデフォルトですが、Windows 上の NNM ではデフォルトではありません。固定サブマップレベルを [**All レベル**] に設定して、Internet Services を Windows 上の NNM と完全に統合すると、Windows 上の NNM は効率的に動作できるように大量のメモリを要求するようになります (以下の注釈を参照してください)。
- NNM 管理サーバーでサポートされている Internet Services ダッシュボード統合用のブラウザは、Internet Explorer (バージョン 6.0 以降) と Mozilla 1.7 です。

OVIS の NNM 統合ソフトウェアをインストールする場合は、その前に NNM IP マップアプリケーションを設定して、サブマップをすべてのレベルで固定することをお勧めします。ここでこの手順を実行しておくと、統合後の NNM の起動時に、手動で設定を実行しなくて済むようになります。

固定サブマップレベルについては、『*HP OpenView ネットワークノードマネージャの拡張 / 分散化ガイド*』を参照してください。第 2 章で、オンデマンドサブマップと固定サブマップレベルについて説明しています。第 4 章では、固定サブマップレベルの確認方法とリセット方法について説明しています。

NNM との統合方法

タスク 1: 管理サーバ上に Internet Services がインストールされていて動作可能であることを確認。

Internet Services が、Windows システムにスタンドアロンアプリケーションとして正常にインストールされて動作しないと、NNM の統合は実行できません。

タスク 2: Internet Services と統合する NNM 管理ステーションで残りの手順を実行。

Internet Services システムから情報を引き出す NNM 管理ステーションを、複数設定することもできます。使用可能な NNM 管理ステーションが複数あり、これらのステーションに Internet Services の情報を送信する場合は、これらの各 NNM 管理ステーションで次の手順を実行します。

1. **固定サブマップレベルを、前述の「NNM 統合の要件 / 推奨事項」に従って設定します。**固定サブマップレベルが [All レベル] に設定されていない場合、NNM は、必要なシンボルを作成できないというエラーをログに記録します。これらのエラーは情報として表示され、NNM が動作できるかどうかには影響を与えません。

2. **OVIS CDに収録されているOVIS-NNM統合ソフトウェアのインストール手順 (readme.txt またはインストールドキュメントのハードコピー) に従います。**インストール手順は、どのオペレーティングシステム (Windows、Solaris、HP-UX) 上の NNM と統合するかによって異なります

   統合パッケージに付属の OVIS-NNM 統合リリースノートを参照してください。パッケージをインストールした後、これらのリリースノートは、UNIX システムの場合、`/opt/OV/www/htdocs/C/ReleaseNotes/ovisnnm_releasenotes.html` で参照できます。Windows システムの場合は、インストール完了後に表示されます。

3. **インストール時に表示される画面の指示に従います。**統合する Internet Services 管理ステーションの完全修飾名 (ovis.testlab.megacorp.com) と OVIS ダッシュボードのポート番号を指定する必要があります。OVIS 管理サーバーの名前と OVIS ダッシュボードのポートは、インストールした後でも、NNM システムにある次のファイルを編集することで変更できます。

   ```
   <install dir>/conf/ovis.conf
   ```

4 NNM を**起動**します。固定サブマップレベルを [All レベル] に設定していない場合は、設定します。新しい [Internet Services] メニューで [Rebuild Internet Services Symbols] を選択します。

タスク 3: Internet Services 管理サーバーで、NNM 統合を設定します。

Internet Services の設定マネージャで [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、[イベント DB] (例 : [NNM との統合]) をオンにします。

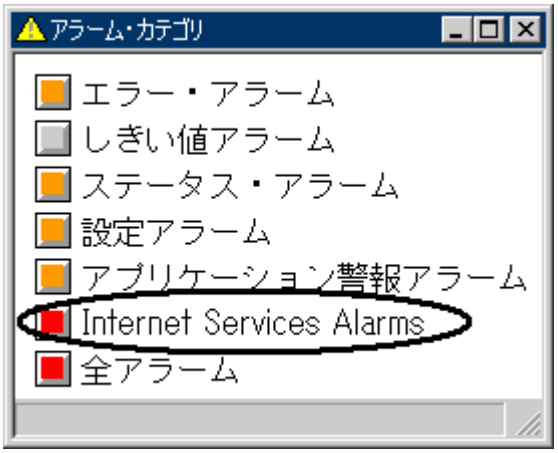
Internet Services との統合後の NNM の機能

Internet Services 統合ソフトウェアをインストールすると、NNM の以下の部分が変更されます。

- NNM の [アラームカテゴリ] ウィンドウに新しいアラームカテゴリ [Internet Services Alarms] が表示されます。
- メニューバーに新しいメニュー [Internet Services] が表示されます。
- NNM サブマップ内に、顧客、サービス、サービス目標値を表す、新しいシンボルが表示されます。
- 新しい定義済みの顧客が表示されます。HP OpenView Customer Views for NNM を使用する場合は、Internet Services によって提供されたノードとインタフェースが入力された [Servers] サブマップと [Access Links] サブマップとともに、Internet Services で定義した顧客が CV-NNM の [**Customers**] ビューに表示されます。
- Internet Services 管理サーバーと NNM コンソール間で、新しい通信メカニズムが使用されます。この通信メカニズムでは、NNM コンソールが何らかの理由でダウンしても、SNMP の場合のようにメッセージが**失われる**ことはありません。このメカニズムは HTTP プロトコルとポート 80 を使用して通信を行います。2 つのコンソールがファイアウォールによって分離されている場合は注意してください。

Internet Services Alarms

NNM の [アラームカテゴリ] ウィンドウに新しいカテゴリ [Internet Services Alarms] が表示されます。



このカテゴリのアラームは、Internet Services システムによって生成されます。Internet Services のアラームは、他の NNM アラームと同様に機能するため、標準の NNM メソッドを使用して必要に応じてそれらを設定および管理することができます。

- 特定の Internet Services アラームを着信した際に起動するスクリプトを設定できます。
- 通常の方法でアラームを受諾したり削除できます。ただし、アラームを削除するだけでは、マップ内の関連付けられているサービス目標値のシンボルのステータスは変更されません (後述の「NNM での Internet Services のシンボル」を参照してください)。ステータスは、Internet Services が収集するデータに基づいて更新されます。

[Internet Services] メニュー

Internet Services と統合すると、NNM メニューバーに新しいメニュー [Internet Services] が追加されます。

- **Rebuild Internet Services Symbols** – Internet Services によってマップ内に追加されたシンボルを、Internet Services 内の最新データに従って再構築できます。これは、Internet Services のシンボルが Internet Services と同期していない場合のみ実行してください。
- **Node Details** – 選択したノードに関する、Internet Services が持っているすべての詳細情報を参照する場合に特に役立ちます。このメニュー項目をクリックすると、現在選択しているノードに関する Internet Services Reports ページが表示されます。
- **Dashboard** – Internet Services ダッシュボードが起動されます。

NNM での Internet Services のシンボル

監視対象サービスがある、NNM 管理ドメイン内のすべてのノードには、3 つのサブマップが追加されています。これらのサブマップには、以下を表すシンボルがあります。

- そのノードが処理する**顧客**。
- **監視対象サービス** – 顧客は、顧客の監視対象サービスを表しているシンボルを含んでいる子サブマップを持っています。
- **サービス目標値アラーム** – サービスは、監視対象サービスのサービス目標値アラームを表示する子サブマップも持っています。

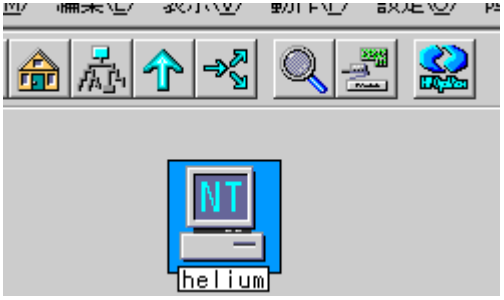
新しいシンボルについては、この節の後半で説明します。

イベントの設定について

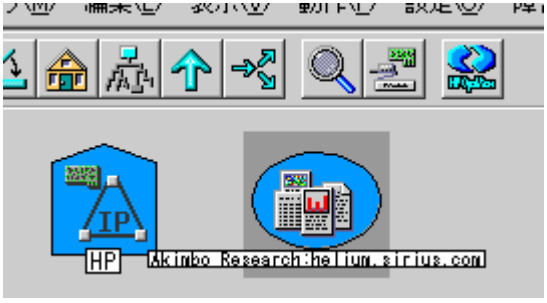
Internet Services の設定変更は、NNM の表示を変更するイベントです。これにより、新しい Internet Services 情報を反映するように NNM を更新することができます。たとえば、設定イベントは NNM で以下の動作を実行します。

1 監視対象サービスノード(サービスが実行されているノード)を表しているオブジェクトのステータスソースを [**複合 (伝達結果)**] に設定します。通常、マップ上のノードは、ノード上のインタフェースから自らのステータスを判

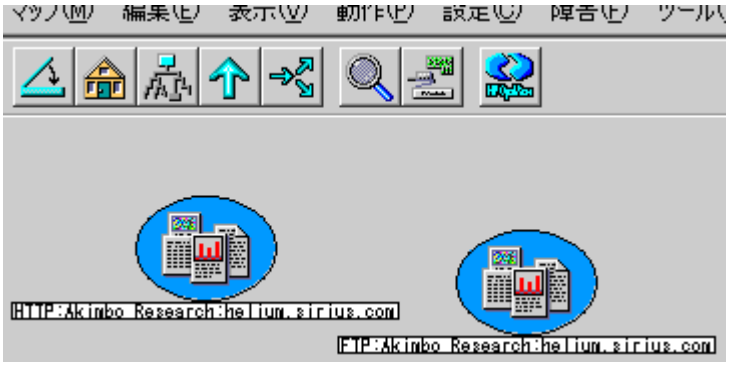
断します。ステータスソースを [複合] に変更することで、ノードはステータスを判断するのにすべての子オブジェクトのステータスを使用するようになります。



2 顧客を、監視対象サービスノードの子として表すシンボルを作成します。シンボル名は「customer_name:node_name」になります。たとえば、「Akimbo Research」という名前の顧客のサービスを提供する「helium.sirius.com」という名前のノードがあるとします。この場合、NNM は、「helium.sirius.com」の下 (ノードのネットワークインタフェースシンボルの隣) に新しいシンボルを作成し、そのシンボルに「Akimbo Research:helium.sirius.com」という名前を付けます。



3 前の手順で作成された各顧客シンボルに対して、NNM は、ノードが顧客に提供しているサービスを表している、1 つまたは複数のシンボルを作成します。サービスシンボルの名前は「service_name:customer_name:node_name」と表示されます。たとえば、「HTTP:Akimbo Research:helium.sirius.com」になります。



4 サービスの適切なケーパビリティを「true」に設定します。たとえば、DNS サービスを提供する監視対象サービスノードは DNS サーバーであるため (定義により)、NNM はノードの ovisIsDNSServer ケーパビリティを「true」に設定します。

アラームイベントについて

設定後、Internet Services からのアラームに対する応答として、NNM は次のステップを実行します。

1 サービス目標値を表すシンボルをサービスシンボルの子として作成します。シンボルの名前は以下の形式になります。

metric_name:service_name:customer_name:node_name:target_info:probe_location

たとえば、アラームが以下のサービス目標値違反を表しているとします。

顧客 :	Akimbo
サービスタイプ :	FTP
監視対象サービスのノード :	helium.sirius.com
監視対象サービスの情報 :	my_xyz_file
メトリック :	RESPONSE_TIME

プローブロケーション： zinc.sirius.com

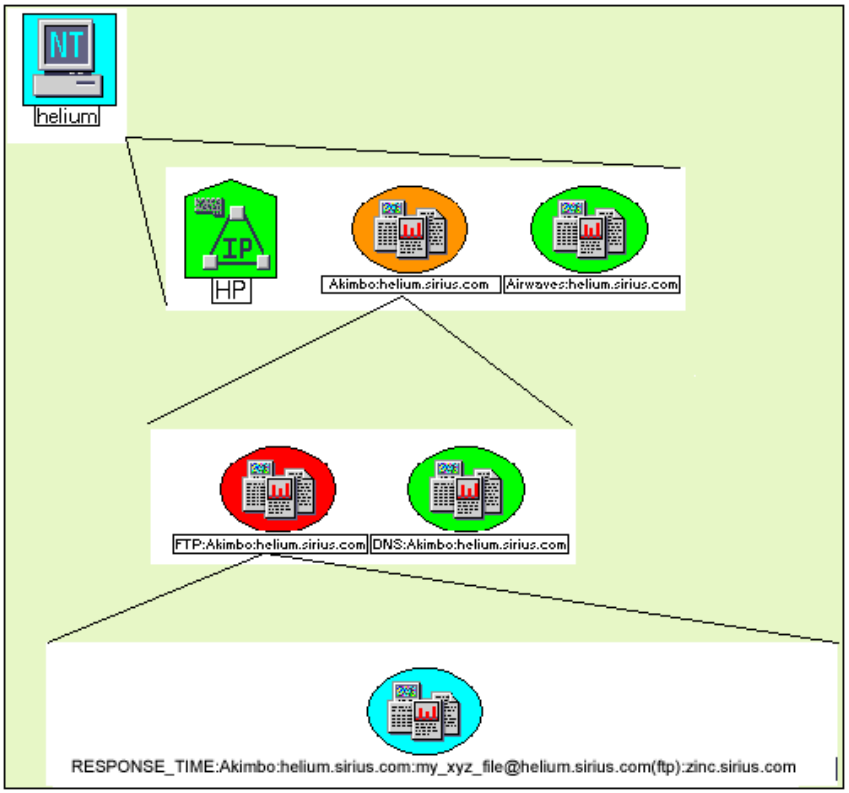
この場合、サービス目標値のシンボルの名前は次のようになります。

RESPONSE_TIME:FTP:Akimbo:helium.sirius.com:my_xyz_file@helium.sirius.com:zinc.sirius.com

サービス目標値のシンボルの名前は長くなります。必要に応じて、パナーを使用して (Windows の場合はシンボルを右クリックして)、より長いわかりやすい名前を取得できます。

2 サービス目標値シンボルのステータスをアラームの重要度に設定します。

ユーザー定義名が表示されたシンボルの例を以下の図に示します。



NNM 統合に関する簡単なトラブルシューティング

ovisclean.ovpl を使って行うデータのリセット

NNM が Internet Services と同期していないと思われる場合は、統合データの完全リセットを実行します。

ovisclean.ovpl を実行する前にすべての ovw セッションを閉じる必要があります。

NNM 統合パッケージは、そのためのスクリプトを提供しています。

$OV_BIN/ovisclean.ovpl

ovisclean.ovpl を使用して、NNM VP-IS コマンドデータベースを完全に消去し、OVIS ステーションから最新の設定とアラームデータをすべて取得することができます。スクリプトにより、NNM マップ内のすべての Internet Services シンボルが再構築されます。

NNM と OVIS の間でポートに矛盾がある場合の対処

NNM と OVIS を同じシステムにインストールしたときに、それらの間でポートの矛盾がある場合は、OVIS 管理サーバーで OVIS ダッシュボートのポート (Tomcat) を以下のように変更します (以下に示すポート番号はその例です)。

```
cd <installdir>¥bin
ovc -stop ovtomcatA
cscript /nologo OvTomcatCtl.vbs -setshutdownport 9005
cscript /nologo OvTomcatCtl.vbs -sethttpport 9080
cscript /nologo OvTomcatCtl.vbs -setjk2port 9007
ovc -start ovtomcatA
```

注記 : 上記のポート番号は単なる例です。どのポートにするかは、`nestat -an` を使用して調べてください。

注記 : ポートを変更したら、変更した http ポートを、OVIS 設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] で設定する必要があります。[Tomcat - ダッシュボード (Web サーバー) ポート] フィールドにポート番号を入力します。

NNM と OVIS の統合をアンインストールした後のクリーンアップ

NNM と OVIS の統合をアンインストールしたときは (`/opt/OV/bin/remove.ovisnnm`)、次の手順で Internet Services のアラームカテゴリを削除する必要があります。

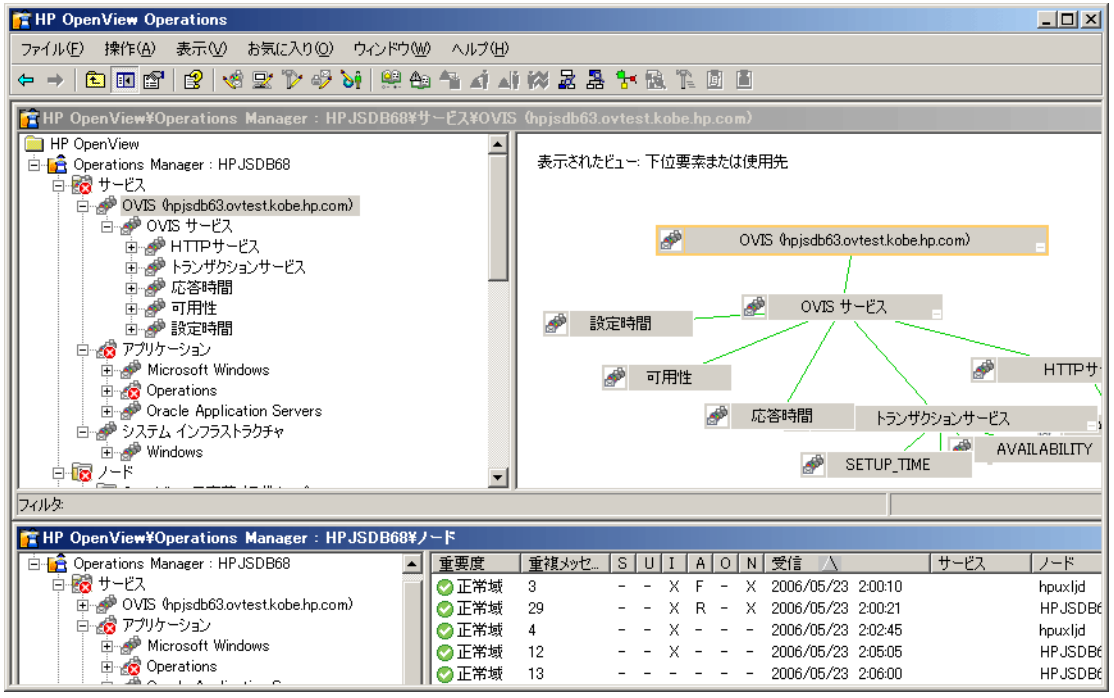
1. `ovw` を起動して、[**オプション**] > [**イベント設定**] を選択します。
2. [エンタープライズ ID] で、[**OpenView**] を選択します。**OVIS_** で始まるイベントをすべて選択して、[**編集**] > [**削除**] > [**イベント**] を選択します。
3. カテゴリを削除するために、[**編集**] > [**設定**] > [**アラームカテゴリ**] を選択します。[**Internet Services Alarms**] を選択して、[**削除**] を押します。

OpenView Operations for Windows との統合

OVIS と OpenView Operations for Windows (OVO for Windows) を統合すると、以下のようになります。

- OVO for Windows のサービスツリーに OVIS の顧客 / サービスグループが追加されて、サービスマップビューにそのグループが表示されるようになります。このサービスマップビューには、OVIS サービスグループのサービスレベル目標値 (SLO) と計測値が表示されます。
- サービスレベルの OVIS アラームが、アラームメッセージとして OVO for Windows に転送されて、コンソールメッセージブラウザに表示されるようになります。表示されるメッセージは、それぞれのサービスと関連しています。
- OVIS が生成したこれらのアラームに対してオペレータ起動コマンドを実行することで、OVIS ダッシュボードの画面を起動できるようになります。
- 選択されているサービスに対して [ツールの起動] を選択することで、特定の顧客やサービスグループまたは計測値のコンテキストで OVIS ダッシュボードを起動できるようになります。

次の図に、OVIS と統合した後の OVO for Windows コンソールの例を示します。


HP OpenView Operations
ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィンドウ(W) ヘルプ(H)
HP OpenView¥Operations Manager : HPJSDB68¥サービス¥OVIS (hpjsdb63.ovtest.kobe.hp.com)
HP OpenView
Operations Manager : HPJSDB68
サービス
OVIS (hpjsdb63.ovtest.kobe.hp.com)
OVIS サービス
HTTPサービス
トランザクションサービス
応答時間
可用性
設定時間
アプリケーション
Microsoft Windows
Operations
Oracle Application Servers
システム インフラストラクチャ
Windows
ノード
表示されたビュー: 下位要素または使用先
OVIS (hpjsdb63.ovtest.kobe.hp.com)
OVIS サービス
設定時間
可用性
応答時間
トランザクションサービス
SETUP_TIME
AVAILABILITY
フィルタ:
HP OpenView¥Operations Manager : HPJSDB68¥ノード
重要度
重複メッセ...
S
U
I
A
O
N
受信
サービス
ノード
正常域 3 - - X F - X 2006/05/23 2:00:10 hpuxljd
正常域 29 - - X R - X 2006/05/23 2:00:21
正常域 4 - - X - - - 2006/05/23 2:02:45 hpuxljd
正常域 12 - - X - - - 2006/05/23 2:05:05
正常域 13 - - - - - - 2006/05/23 2:06:00

要件

統合する OVO for Windows と OVIS は、同じシステムにあっても異なるシステムにあってもかまいません。ただし両者が異なるシステムにある場合は、OVIS 管理サーバーに OVO エージェントをインストールする必要があります。OVO for Windows と OVIS 6 を統合する場合は、OVIS 管理サーバーにバージョン 7.27 以降の OVOW Agent をインストールする必要があります (パッチ OVOW_00059)。

統合に際しては、その前に、OVIS で監視対象サービス、目標値、およびアラームしきい値を設定して、OVIS ダッシュボードにグラフが生成されることを確認する必要があります。

OVIS ダッシュボードの表示設定を制限していると、OVO コンソールからダッシュボードを起動したときにログイン画面が表示され、OVO で選択した項目のコンテキストに合った詳細表示ではなく、ダッシュボードのメインページが表示されます。

OVIS とクラスタ構成の OVO for Windows サーバー (バージョン 7.5 以降) は、同じシステムにインストールできません。

インストールの手順

OVO for Windows サーバーで、OVIS インストール用の CD を使用して [**Operations for Windows Integration**] を選択します (インストールプログラムが自動的に開始されない場合は、CD ドライブで `¥Autorun¥setup.exe` を実行します)。

OVIS の Operations for Windows Integration ソフトウェアをインストールします。その際、OVIS 管理サーバーのホスト名を入力します (入力をうながす指示が出ます)。

OVIS/OVOW Integration ソフトウェアをクラスタ構成の OVOW システムにインストールする場合は、そのための追加手順を実行する必要があります (詳しくは、OVO オンラインヘルプの「クラスタ対応アプリケーションの管理」を参照してください)。この追加手順では、サービスマップを更新するためのタスク、つまりそのためにスケジュール化されたタスクがそのときの有効な OVOW サーバー上でだけ実行されることを確認します。368 ページの「クラスタ構成の OVOW システムに対する手順」を参照してください。

OVO for Windows Integration コンポーネントをインストールすると、そのファイルは OVO for Windows サーバーにある次のディレクトリへインストールされます。

```
%OVINSTALLDIR%¥bin¥OvIS
```

設定手順

1. OVO for Windows コンソールで、Internet Services 管理サーバーを OVO for Windows の [ノード] フォルダに追加します。

   管理対象ノードの詳細な設定方法と、その関連情報については OVO for Windows のオンラインヘルプを参照してください。

2. OVIS 管理サーバーを OVO とは別のシステムにインストールして、その OVIS 管理サーバーを OVO for Windows のノードとして追加すると、自動検出機能が働いて、その OVIS 管理サーバーへ OVO エージェントが展開配備されます。しかし、何らかの理由でこの展開配備が行われなかったときは、OVIS 管理サーバーに OVO エージェントをインストールする必要があります。その場合、OVO のバージョンが 7.x で、しかも OVO エージェントに対する Windows の最新パッチがまだインストールされていないときは、OVO エージェントと OVIS を C ドライブにインストールする必要があります (OVO の説明書を参照してください)。

3. エージェントを展開配備した後、OVIS サーバーを再起動します。

クラスタ構成の OVOW システムに対する手順

OVIS/OVOW Integration コンポーネントをクラスタ構成の OVOW システムへインストールする場合は、以下の追加手順を実行する必要があります。

1. OVIS/OVOW Integrationコンポーネントを OVOW管理サーバーのすべてのクラスタノードにインストールして、前の項で説明した設定手順を実行します。
2. %OvOWShareInstallDir%¥instrumentation¥Windows Server 2003¥5.2¥VP_SM ディレクトリにある OvOWSelfManagement.apm.xml ファイルを修正して、<Application> の下に次の行を追加します。

   <Template>OvisUpdateServices</Template>

   ファイルの内容は次のようになっています。

```
<?xml version="1.0"?>
<APMApplicationConfiguration xmlns="http://www.hp.com/OV/opcapm/
cluster">
     <Application>
          <Name>OvOWSelfManagement</Name>
          <Template>OvSvcDiscServerLog</Template>
          <Template>VP_SM-Server_EventLogEntries</Template>
          <Template>VP_SM-Server_SyncAgentServices</Template>
          <Template>VP_SM_OVOWServices</Template>
          <Template>VP_SM-WMI-Restart</Template>
          <Template>VP_SM_DeleteNodesFromReporterDB</Template>
          <Template>VP_SM-Cluster Consistency Check</Template>
          <Template>OvisUpdateServices</Template>
     </Application>
</APMApplicationConfiguration>
```

3. すべてのクラスタノードにこの実装 (カテゴリ VP_SM) を再展開します。
4. それぞれのクラスタノードで以下のコマンドを実行して、エージェントを再起動します。

   opcagt -kill

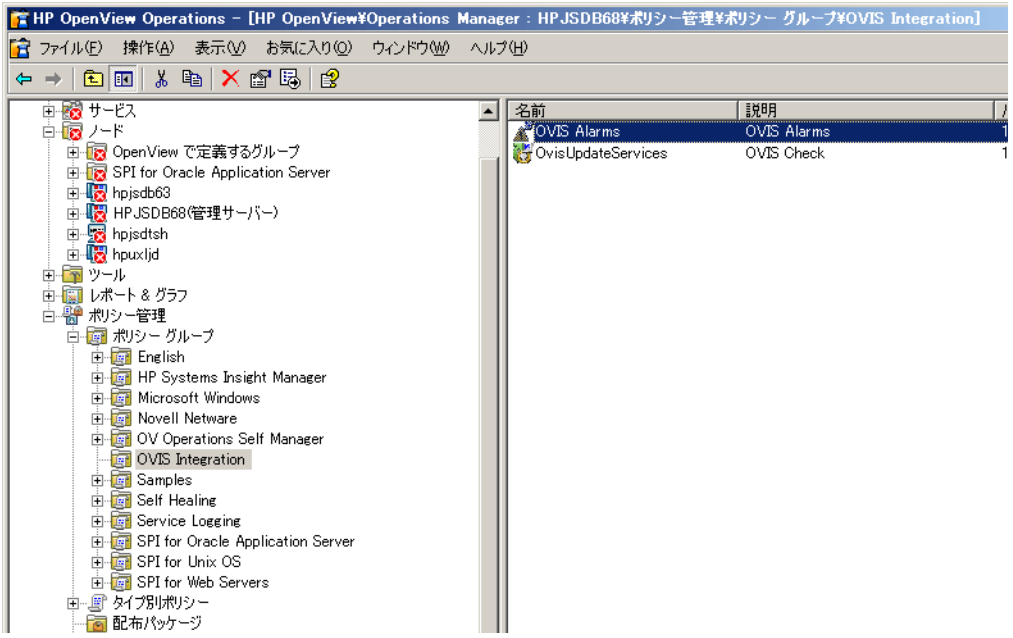
   opcagt -start

OVIS ポリシーの展開配備手順

OVIS の OVO for Windows Integration コンポーネントをインストールしたら、次の手順で OVIS ポリシーを 2 つ展開配備する必要があります。

1 OVISのアラーム転送モードとして[**OVOとの統合 - プロキシを使用**]を選択する場合は、Internet Services の監視対象サービスシステムを OVO for Windows のノードフォルダに追加します。

2 展開配備するポリシーの 1 つは、スケジュール化されたタスクポリシー `OvisUpdateServices` です。このポリシーは、OVIS Integration ポリシーグループにあるので、OVO for Windows コンソールの左ペインで [**HP OpenView**] > [**Operations Manager**] > [**ポリシー管理**] > [**ポリシーグループ**] > [**OVIS Integration**] の順に選択して、このフォルダを特定します。次の図を参照してください。



3 右ペインで`OvisUpdateServices`ポリシーを選択し、右クリックして[**すべてのタスク**] > [**配布先ノード**] を選択します。

4 [**ポリシーの配布先**] ダイアログボックスで、OVO for Windows の管理サーバーのノードツリーにあるチェックボックスにチェックマークを入れ (その他のチェックボックスはデフォルトのままにしておきます)、[**OK**] をクリックしてポリシーを展開配備します。

5 `OVIS Alarms` ポリシーのタイプは opcmsg インターフェイスです。このポリシータイプは OVIS Integration ポリシーグループにあって、`OVIS Alarms` ポリシーも同じフォルダにあるので、[**HP OpenView**] > [**Operations Manager**] > [**ポリシー管理**] > [**ポリシーグループ**] > [**OVIS Integration**] を選択します。

6 右ペインで `OVIS Alarms` ポリシーを選択し、右クリックして [**すべてのタスク**] > [**配布先ノード**] を選択します。

7 [**ポリシーの配布先**] ダイアログボックスで、OVIS の管理サーバーのノードツリーにあるチェックボックスにチェックマークを入れ (その他のチェックボックスはデフォルトのままにしておきます)、[**OK**] をクリックしてポリシーを展開配備します。

8 数分待ちます、OVO for Windows のサービスツリーに OVIS サービスが追加され、そこに以下の階層が表示されます。

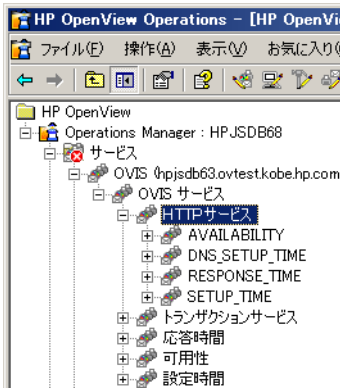
OVIS 管理サーバーノード

クラスタ

サービスグループ (計測値の表示はマップの [**+**] 記号をクリックする)

サービスグループ内で監視された監視対象サービスの SLO

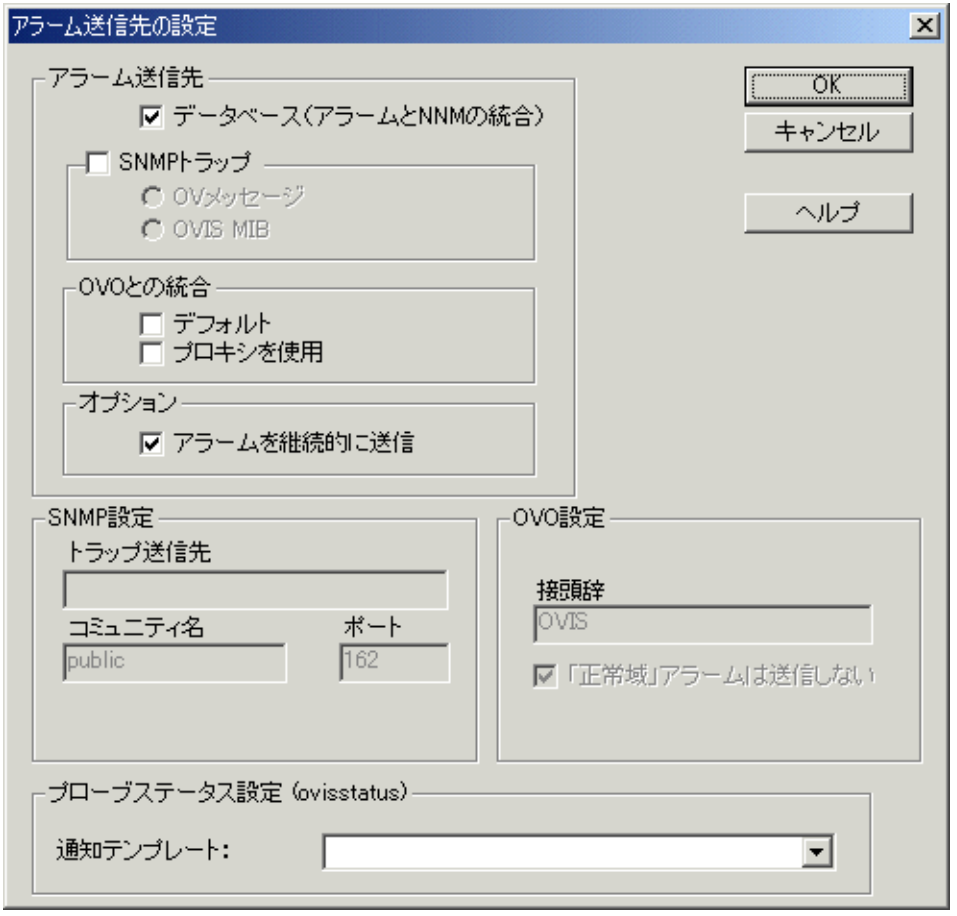
サービスレベル契約が定義されていれば、クラスタレベルにその定義があります。



9 OVO for Windows に送信する OVIS アラーム設定します。操作としては、OVIS 設定マネージャで [**ファイル**] > [**設定**] > [**アラーム送信先**] の順に選択してダイアログボックスを開き、OVIS データを OVO for Windows へ転送する方法を次の 2 つのオプションから選択します。アラームの送信先を設定したら、[**保存**] をクリックしてこの設定を必ず保存してください。

— **OVO との統合 - デフォルト :** このモード (デフォルト) を選択しておけば、OVO for Windows で受信した Internet Services メッセージは Internet Services サーバーから発信されたものとして扱うことができます。この設定では、Internet Services サーバーを OVO for Windows のノードとして設定しておくだけですみます。

— **OVO との統合 - プロキシを使用 :** このモードを選択した場合は、Internet Services メッセージの発信元を Internet Services の監視対象ノードに従って識別することになります。この設定では、Internet Services 管理サーバーと Internet Services 監視対象システムを OVO for Windows のノードフォルダに追加する必要があります。また、OVO エージェントを OVIS 管理サーバーシステムに展開配備する必要もあります (OVO エージェントを OVIS 監視対象システムに展開配備する必要はありません)。



OVO for Windows では、OVIS の Alarm ポリシーを使って、障害アラーム状態 (危険域、重要警戒域、警戒域、注意域、および正常域) をベースにした相関処理を行うことができます。

[アラーム送信先の設定] ダイアログボックス (上図) では、[**アラームを継続的に送信**] ボックスにチェックマークを付けて、[**「正常域」アラームは送信しない**] ボックスを無効、つまり変更できないようにすることもできます。このように設定しておくと、アラームになってから、そのアラーム状態が正常域に戻ってその変化が通知されるまで、OVIS アラームが定期的に生

成されます。OVO for Windows では、最初のアラームメッセージをメッセージブラウザに保持しておき、その後に最初のメッセージに似たメッセージが続くと、相関処理を行ってそのメッセージの日付を更新します。

10 ここまでの手順を実行すると、アラームメッセージは OVO for Windows へ転送されるようになります。転送されてきたアラームメッセージは OVO for Windows の [アクティブメッセージ] ビューに表示されます。また、サブサービスでアラームが発生すると、そのステータスがサービスツリーの上位に伝達されるので、項目の色がそのアラームの重大度に従って変わります。

さらに、ovisstatus.exe プログラムが自動的に実行され、予測時間 + 10% (多少の遅れを許容する時間) 以内にデータがプローブシステムから受信されない場合は、OVO または NNM にアラームを送信します。

OVO に転送する OVIS メッセージ

OVIS は、アラームメッセージを渡すときに以下の OVO 属性 (opcmsg) セットを使用します。

```
opcmsg [-help] [-id] [severity=normal|warning|minor|major|critical]
        application=<application> object=<object> msg_text=<text>
        [msg_grp=<message group>] [node=<node>] [service_id=<svcid ID>]
       [-option <var>=<value>]
```

表 5　　opcmsg 属性

OVO の属性 (opcmsg)	OVIS の値
object	監視対象ホスト : プローブシステム : 監視対象情報
msg_grp	OVIS_< プローブ名 >
node	OVIS サーバーの FQDN (プロキシが GUI で設定されている場合は、対象ノードの FQDN)
msg_txt	メッセージテキスト

表 5　　opcmsg 属性 (続き)

OVO の属性 (opcmsg)	OVIS の値
application	OVIS
severity	OVIS の重要度
option 変数	host=< 監視対象ホスト > ps=< プローブシステム > target=< 監視対象情報 > vpis=<OVIS サーバーの FQDN> customer=< 顧客 > customerURLE=< 顧客 > serviceGroup=< サービスグループ > serviceGroupURLE=< サービスグループ > probeDesc=< プローブの説明 > probeDescURLE=< プローブの説明 > probeType=< プローブ名 > probeTypeURLE=< プローブ名 > metric=< メトリック > ipAddr=< 監視対象の IP アドレス (可能な場合)> psts=< 測定が行われたときのタイムスタンプ (UTC)>

Internet Services 管理サーバーから想定どおりにメッセージが転送されるのを確認するには、OVIS サーバーで [コマンドプロンプト] ウィンドウを開いて、次のコマンドを実行します。OVO のメッセージブラウザに、対応するメッセージが表示されます。

```
opcmsg a=OVIS o=OVIS_Test msg_text="Test"
```

このテストは単純で、必要なオプションが一部しか含まれていません。たとえば、オペレータの起動するような動作はできないので注意してください。

使用方法のヒント

OVO for Windows コンソールから OVIS との統合機能を使用するには、次のようにします。

- OVO for Windows のサービスビューマップで、表示されている OVIS の顧客、サービスグループ、およびメトリックをそれぞれ右クリックして、[**すべてのタスク**] > [**ツールの起動**] を選択します。この操作で、選択した項目に合った OVIS ダッシュボードが起動されます。ダッシュボードには、詳細なパフォーマンスデータおよびグラフとともに、パフォーマンスデータの要約レポートが表示されます。OVO for Windows のサービスビューで選択できる各項目のダッシュボードは次のようになっています。
  - OVIS サーバー : ダッシュボードの [状況] ワークスペースに要約ページが表示されて、すべての顧客の情報が示されます。
  - 顧客 : ダッシュボードの [状況] ワークスペースに要約ページが表示されて、その顧客の詳細な情報が示されます。
  - サービスグループ : ダッシュボードの [状況] ワークスペースに要約ページが表示されて、そのサービスグループの詳細な情報が示されます。
  - メトリック : OVIS に SLO として設定されているメトリックだけが表示されます。ダッシュボードの [状況] ワークスペースに要約ページが表示されて、そのサービスグループの詳細な情報が示されます。
  - SLA : ダッシュボードの [SLA] ワークスペースが表示されます。
  - アラーム : ダッシュボードの [状況] ワークスペースに要約ページが表示されて、アラームを生成したサービスグループの詳細な情報が示されます。アラームが正常域の場合は、ダッシュボードの [状況] ワークスペースにメインページが表示されます。
- OVO for Windows の [アクティブメッセージ] ビューで、表示されている OVIS アラームをそれぞれ右クリックし、[**コマンド**] > [**開始**] > [**オペレータ起動**] を選択して OVIS ダッシュボードを起動します。
- ブラウザに「unmatched (不一致)」フラグの付いた OVIS メッセージが表示される場合は、別の opcmsg ポリシーでそのメッセージが生成された可能性があります。OVIS 管理サーバーに OVIS の Alarms ポリシーが展開配備されていることを確認し、次に、OVIS 管理サーバーに展開されている他の opcmsg ポリシーで不一致メッセージが作成されていなくても OVIS メッセー

ジが抑制されていないかどうかをチェックします。opcmsg ポリシーによって問題が発生している場合は、OVIS 管理サーバーからそのポリシーをアンインストールする必要があるかもしれません。

- OVIS を統合すると、OVO for Windows から OVIS ダッシュボードを起動するためのツールが数多く作成されます。これらツールは、[**HP OpenView**] > [**Operations Manager**] > [**ツール**] > [**OVIS Tools**] フォルダにあります。
- OVIS サーバーのホスト名は、統合コンポーネントをインストールするときに入力します。インストールした後にこの名前を変更する場合は、OVO サーバーにある `%OVINSTALLDIR%¥bin¥OvIS¥oviscnfg.ini` ファイルを読み込んで、たとえば、次のように変更します。

  ```
  [CONFIG]

  ovishost=your.ovis.host.fqdn.com

  trace=False
  ```

  トレースフラグ (`trace=`) はログファイルのトレースを有効または無効にするためのものです。ログファイル `OvisUpdateServices.log` は、OVO システムの `%OVINSTALLDIR%¥Data¥log` ディレクトリにあります。
- OVIS 設定マネージャで行って保存した変更 (顧客、サービスグループ、または SLO の追加および削除を含む) は、5 分ほど経過すると自動的に OVO のサービスツリーへ反映されます。
- インストールする統合コンポーネントには、`forceupdate.cmd` ユーティリティが含まれています。コマンドプロンプトからこのユーティリティを起動することにより、OVO のサービスツリーで OVIS を手動更新することができます。また、トレースを有効にしてその情報を `OvisUpdateServices.log` トレースファイルに書き込ませる場合は、このユーティリティに `-t` オプションを指定して実行します。`-t` オプションは上記の `trace=` オプションに似ています。このユーティリティに `-r` オプションを指定して実行すると、サービスツリーから手動で OVIS を削除することができます。ツリーから OVIS を取り除く場合は `-r` だけを使用します。スケジュール化された次回の更新でツリーが構築しなおされます。それまで待てない場合は、`forceupdate` を実行します。

6

トラブルシューティング情報

この章では、基本的なトラブルシューティング情報について説明します。扱う内容は次のとおりです。

- プローブステータスのトラブルシューティング
- ダッシュボードのトラブルシューティング
- カスタムグラフと制限表示のトラブルシューティング
- インストールのトラブルシューティング
- TIPs のトラブルシューティング
- OVIS のトレースファイルとログファイル
- エラーメッセージとステータスコード
- アラームのトラブルシューティング
- プローブごとのトラブルシューティング
- OVIS と OVTA の統合に関するトラブルシューティング
- 複数ユーザーによる設定マネージャの同時使用
- プローブのスケジューリングに関する検討項目
- トラブルシューティングのためのツール

ファイルの一覧とそのバージョン情報については、Internet Services CD の Support フォルダを参照してください。

プローブステータスのトラブルシューティング

ここでは、設定マネージャのステータスウィンドウに示される問題について説明します。[監視対象サービスの状態]、[プローブからの受信データ]、および [データ統合] タブページに表示されている項目の隣りに赤い円が表示されることがあります。

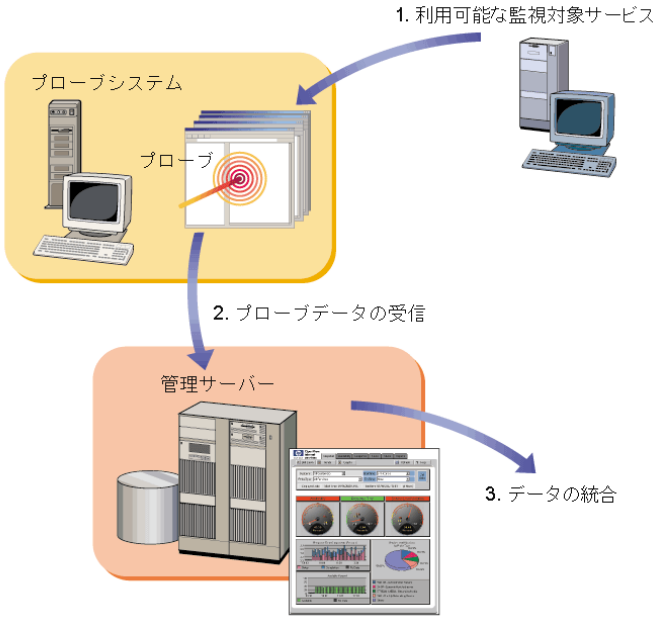
設定した監視対象サービスに関するデータを受信していない場合、この 3 つの領域のいずれかまたはこれら領域間の接続に問題がある可能性があります。

1 監視対象サービスの状態

2 プローブからの受信データ

3 データ統合

図 4　　プローブデータのデータフロー



前提条件 : 設定マネージャを使用してサービスグループを設定し、プローブが正しい場所に設置されていることを確認しておく必要があります。

[監視対象サービスの状態] に赤い円が表示される

ステータス表示の [監視対象サービスの状態] タブで、監視対象サービスが赤になっている場合、そのサービスが [**利用不可**]、または、[**プローブの情報がありません**] と表示されます (これらの状態は、画面の [**ステータス**] 列に表示されます)。

- **利用不可 :** 監視対象サービスのステータスが [**利用不可**] の場合は、プローブを実行しサービスにアクセスしようとしたが、何らかの理由でそのサービスが利用不可であると判断し、このことを OVIS に通知したことを表しています。380 ページの「監視対象サービスのステータスが [利用不可] になっている場合」を参照してください。
- **プローブの情報がありません :** 監視対象サービスのステータスが [**プローブの情報がありません**] の場合は、OVIS がプローブから測定情報を受信していないことを表しています。これは、プローブが実行されてから OVIS にデータを返すまでの時間が十分でなかったか、名前の解決問題があるか、あるいはプローブと OVIS 管理サーバー間の通信に問題があることを示しています。381 ページの「プローブ情報が存在しない場合」を参照してください。

監視対象サービスのステータスが [利用不可] になっている場合

監視対象サービスが [利用不可] になっている場合は、以下のことが原因として考えられます。444 ページの「プローブごとのトラブルシューティング」を参照してください。

- **監視対象サービスの情報が正しく入力されていない :** たとえば、HTTP サービスの URL を正しく入力しなかったり、FTP サービスのサーバーを正しく指定しなかった可能性があります。HTTP サービスでの確認方法の例については、383 ページの「考えられる原因 : URL が無効 (IOPS 1-11)」を参照してください。
- **プロキシ情報が入力されていない :** たとえば、イントラネット外の特定の Web サイトを取得するのに、Web プロキシを使用する必要があるサイトでは、プローブロケーションを設定するときにこの情報を入力する必要があります。確認方法については、384 ページの「考えられる原因 : プロキシ情報が正しく設定されていない」を参照してください。

- **プロキシが動作していない :** Web プロキシが正しく機能していない可能性があります。ブラウザを使用してこれを確認できます。または、ping を実行して、プロキシが応答するかどうかを確認できます。確認方法の例については、384 ページの「考えられる原因 : Web プロキシへの接続がタイムアウトになった」を参照してください。
- **名前または IP アドレスを解決できない :** DNS サーバーが、監視対象サービスのホスト名を解決できないことがあります。**`nslookup`** コマンドを使用して、ホスト名または IP アドレスが解決可能であることを確認してください (例 : `nslookup web.alt.hp.com`)。IP アドレスを受信できなかった場合、システムが DNS サーバーに登録されていないか、アクセスしている DNS サーバーの処理速度が低下しているかダウンしている可能性があります。
- **サービスを利用できない :** これは、サービスがダウンしたことを検出する、OVIS の機能の 1 つです。サービスが実際に稼働および機能していることを確認してください。たとえば、HTTP の場合は、ブラウザを使用して Web サイトにアクセスします。他のプローブの場合は、FTP 経由でファイルを送信したり、電子メールを送信します。

プローブ情報が存在しない場合

プローブ情報が存在せず、情報を収集して OVIS に送信するのに十分な時間がプローブに与えられていた場合、名前解決の問題があるか、プローブと OVIS 管理サーバー間の通信に問題がある可能性があります。考えられる原因とその解決策を以下に示します。

- **OVIS 管理サーバーで名前解決の問題が発生し、無効な管理サーバーの名前を含む config.dat ファイルが作成される :** プローブシステムは config.dat ファイルを受け取ります。管理サーバーにデータを返信できないため、サーバーにプローブ情報が存在しない状態となります。

  config.dat ファイル内の名前を修正し、このファイルを手動でプローブシステムに配布して対処します。
- **config.dat ファイル内の正しい OVIS 管理サーバー名をプローブシステムが正しく解決できない :** 名前解決の問題が解決されない限り、管理サーバーにデータが送信されません。上記のいずれの場合も、測定データが保存されると、プローブシステム上の管理サーバーへの送信待ち状態のキューファイルの数が増加します。

- **OVIS システム上の Web サーバーが稼働していない :** 383 ページの「考えられる原因 : ローカル Web サーバーとの接続が切断された」を参照してください。
- **プローブシステムと OVIS 管理サーバー間でプロキシが必要 :** プロキシが必要な場合は、[プローブロケーションの情報] ダイアログで設定されていることを必ず確認してください。
- **プローブシステムと OVIS 管理サーバー間で、通信のセキュリティ設定が正しくない :** プローブシステムと OVIS 管理サーバー間で、セキュリティ保護された通信を使用している場合は、証明書と Web サーバーが正しく設定されていることを確認してください。第 7 章の 489 ページの「セキュリティ保護された通信の設定」を参照してください。
- **HP Internet Services (プローブ) サービスが実行されていない :** Windows の [サービス] ダイアログで、HP Internet Services サービスが開始されていることを確認してください。

[プローブの情報がありません] と表示された場合の原因を特定する方法を以下に示します。

- プローブシステムの `<datdir>¥datafiles¥probe¥queue` ディレクトリにキューファイルが存在しない場合、プローブサービス (HP Internet Services) が実行されていない可能性があります。このディレクトリ内の SEQ ファイルのタイムスタンプを確認してください。最新のタイムスタンプになっていない場合、プローブは実行されていません。サービスをいったん停止してから開始し、問題が解決されるかどうか確認してください。
- プローブシステムの `<datdir>¥datafiles¥probe¥queue` ディレクトリにキューファイルが作成されている場合は、プローブサービス (HP Internet Services) は正常に実行されていても、名前解決の問題があるか、あるいは OVIS 管理サーバーが測定データを受け付けていない可能性があります。最初に config.dat ファイル内のホスト名がプローブシステムから適切に解決できているかを確認します。これを確認した後、サービスをいったん停止してから開始し、プローブサービスが正常に実行されていることを確認してください。

考えられる原因 : ローカル Web サーバーとの接続が切断された

解決策 : ローカル Web サーバーが正しく設定および実行されていることを確認する

1 Web ブラウザを開き、アドレスバーに以下の情報を入力します。

<system_name>/HPOV_IOPS/

たとえば、「nt-t30.xsys.corp.com/HPOV_IOPS/」と入力します。

2 正常な応答例を以下に示します。

```
[To Parent Directory]
   2002 年 1 月 8 日  10:56    <dir> cgi-bin
   2002 年 1 月 8 日  10:56    <dir> isapi
   2002 年 1 月 8 日  10:56    <dir> java
```

「HTTP 404 （ページが見つかりません）」などのエラーが表示された場合、Web サービスが開始されていない可能性があります。以下の手順に従ってサービスを開始してください。

a Windows で [コントロールパネル] を開き、[**サービス**] を選択して、[**World Wide Web Publishing Service**] を強調表示して [**開始**] ボタンをクリックします。

b [コントロールパネル] を閉じます。

c Web ブラウザを開き、アドレスバーに以下の情報を入力します。

<system_name>/HPOV_IOPS/

たとえば、「nt-t30.xsys.corp.com/HPOV_IOPS/」と入力します。

考えられる原因 : URL が無効 (IOPS 1-11)

「Socket error 11001 in 'gethostbyname'」エラーは、監視対象サービスの情報が正しく入力されていないために発生します。

解決策 : URL に Web ブラウザからアクセスできるかどうか確認する

1 設定マネージャを開きます。

2 確認する監視対象サービスを強調表示し、右クリックして [**監視対象サービスの編集**] を選択します。

3 ホストの URL を Web ブラウザのアドレスバーにコピーします。

4 「HTTP 404 (ページが見つかりません)」などのエラーが表示された場合は、URL が正しくない可能性があります。

5 監視対象サービスを編集して、正しい URL を入力してください。

考えられる原因 : プロキシ情報が正しく設定されていない

解決策 : プロキシ情報が正しいことを確認する

設定マネージャの [プローブロケーションの情報] ダイアログで、監視対象サービスのプロキシ情報を表示し、Internet Explorer の [**インターネットオプション**] > [**接続**] **タブ** > [**LAN の設定**] を選択してプロキシの設定を比較します。必要に応じてプロキシ設定を変更します。

考えられる原因 : Web プロキシへの接続がタイムアウトになった

解決策 : プロキシが解決可能であることを確認する

1 コマンドプロンプトで、**ping** に続けて Web プロキシサーバーのアドレスを入力します。たとえば、「`ping web-proxy.xsys.corp.com`」のように入力します。

2 「timed out」または「Bad IP address」と表示された場合は、ネットワーク管理者にお問い合わせください。

[プローブからの受信データ] に赤い円が表示される

ステータス表示のこのタブで、赤い円が表示されている場合、プローブからデータを受信していない可能性があります。この問題は、「プローブ情報が存在しない場合」と非常に似ています。381 ページの「プローブ情報が存在しない場合」の手順に従って、この問題の原因を特定することができます。

この画面には、前回データを受信してからの経過時間が表示されます。これにより、プローブデータが受信されなくなった時期を判断することができます。この情報は、サービスグループ別に編成および要約されているため、読みやすくなっています。

[データ統合] に赤い円が表示される

ステータス表示のこのタブで、赤い円が表示されている場合、プローブデータを受信して要約し、それをデータベースに保存する OVIS プログラムが、これらの処理を実行していない可能性があります。いくつかの原因が考えられます。

- **整理統合するデータが存在しない :** 前述の 381 ページの「プローブ情報が存在しない場合」に従って、この問題の原因を特定することができます。
- **Reporter サービスが実行されていない :** Windows の [コントロールパネル] から [サービス] ウィンドウを表示し、Reporter サービスが実行されていることを確認してください。サービスをいったん停止してから開始し、サービスが正常に実行されていることを確認してください。
  - Windows の [コントロールパネル] を開いて [**管理ツール**] > [**サービス**] を選択します。
  - [**Reporter Service**] を強調表示して、[**開始**] ボタンをクリックします。

ダッシュボードにデータが表示されない

ダッシュボード画面にデータが表示されない場合は、設定マネージャでステータス表示を確認してください。[プローブからの受信データ] タブに緑色のアイコンが表示されているが、[データ統合] タブに赤い円が表示されている場合は、Reporter サービスが正しく実行されていない可能性があります。[コントロールパネル] から [**サービス**] ダイアログを開いて、Reporter サービスが実行されていることを確認してください。

ダッシュボードのトラブルシューティング

問題 : メモリーが足りなくなったり、ダッシュボードが異常終了したりする

解決策 : OVIS ダッシュボード (Tomcat サーバー) の動作しているアプリケーションサーバーに対して HTTP_TRANS プローブ (IE モード) のようなプローブからそれぞれ異なるリクエストが繰返し行われると、アプリケーションサーバーのメモリーが足りなくなって、処理が異常終了したりブラウザにメモリー不足のエラーが返ったりすることがあります。セッションには必要なリソースが個別に割り当てられますが、Tomcat では、最後のリクエストが行われた後でも、これらのリソースが、ある程度の時間開かれたままになります。その長さは、途中でそのセッションが終了したかどうかに関係なく、最大で 2 時間にもなります。

通常の使用形態で OVIS ダッシュボードサーバーにこの問題が発生するようであれば、次のコマンドを実行してメモリーの割当てを増やしてください。

```
<install dir>¥nonOV¥tomcat¥a¥bin>tomcat5w //ES//OvTomcata
```

[Java] タブを選択し、[Initial Memory Pool] フィールドと [Maximum memory pool] フィールドでメモリーの割当てをそれぞれ希望する量 (最大 256MB) まで増やします。

問題 : ダッシュボードに表示されるはずのアラームが表示されない。

解決策 : ダッシュボードへアラームを表示させるには、設定マネージャで [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、[**データベース (アラームと NNM の統合)**] チェックボックスにチェックマークを付けておく必要があります。

問題 :「The Page Can Not Be Displayed」というエラーが表示される。

解決策 : Tomcat サービスが開始されているかどうかを確認します。コントロールパネルから [サービス] ダイアログを開き、「HP OpenView Tomcat(A) Servlet Container Service」の状態を調べてください。停止していれば、起動します。

問題 :「This graph cannot be displayed for this metric」というエラーが表示される。

説明 : ダッシュボードの [状況] ワークスペースにある [傾向] タブの [ベースライン] グラフと [時間ごとの統計] グラフでは、[可用性] や [SLO 違反] といった特定のメトリックに対して「This graph cannot be displayed for this metric」というメッセージが表示されることがあります。これは、そのメトリックの値が常に 0 か 1 であるため、パーセントで統計をとるほどデータが細かく分かれていないからです。

問題 :「Unknown Target Name」というエラー表示がされる

説明 : ダッシュボードの [リソース] ナビゲーションツリーまたは [監視対象ステータス] ページで、「Unknown Target Name」という表示が出た場合は、その監視対象から収集されたデータがデータベースに格納されていません。監視対象にホスト名が設定されていればその名前が表示されるので監視対象の識別に役立ててください。1 つのサービスグループにデータのないターゲットが複数個ある場合は、その名前の後ろにそのターゲットを識別するための一連のインデックスが表示されます。

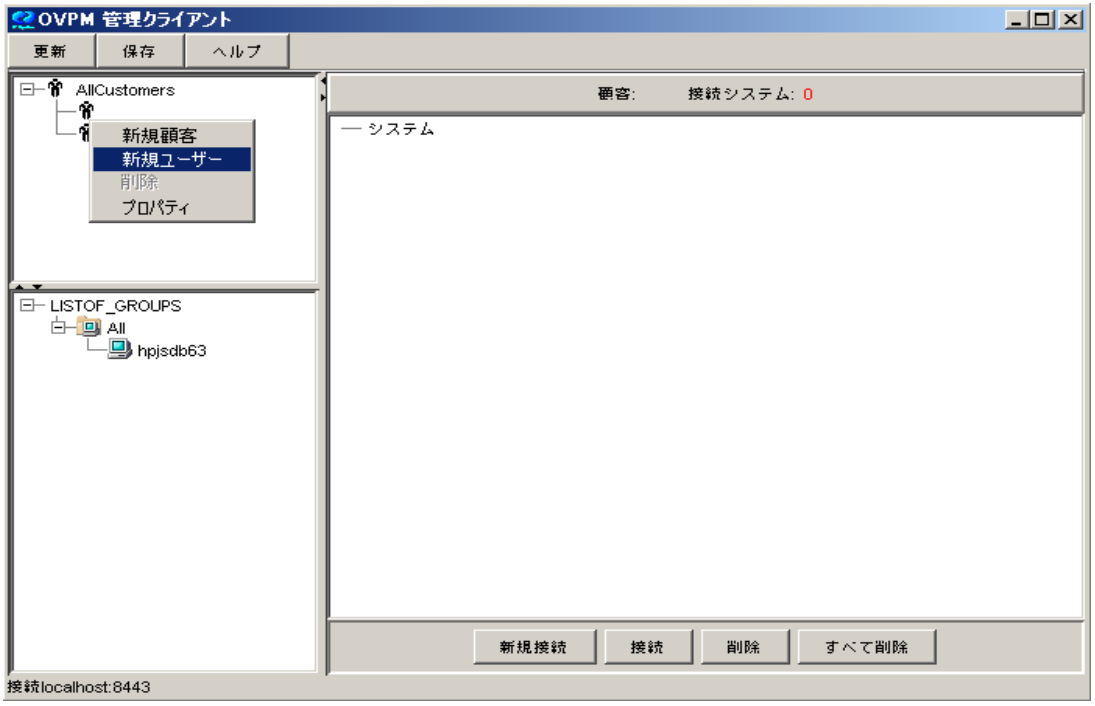
カスタムグラフと制限表示のトラブルシューティング

OVIS と OpenView Performance Manager 5.0 (OVPM) を同じシステムにインストールして制限表示をオンにした場合は、パスワードを同期させないと、OVIS ダッシュボードにカスタムグラフを正しく表示できません。そのため、OVIS ダッシュボードの [カスタムグラフ] ウィンドウに次のエラーメッセージが表示される場合があります。

```
Invalid password supplied for the admin customer (err18)
No data source was specified. Please select a system or other data
source (err203)
```

OVIS で制限表示 (またはプロファイル) を設定した後、OVPM Administrator の GUI で次のようにパスワードを同期させてください。

[**スタート**] > [**プログラム**] > [**HP OpenView**] > [**Performance Manager**] > [**Performance Manager Administration**] を選択します。次の画面を参照してください。



パスワードを同期させるには、OVPM Administration プログラムを使用して、制限表示を設定した OVIS の顧客とそのパスワードを OVPM へ追加する必要があります。[Customer] リストボックスを右クリックし、[新規顧客] を選択します。次に顧客名とパスワードを入力して (OVIS と同じパスワードを入力します)、[**保存**] ボタンを選択します。

このように設定すれば、OVIS ダッシュボードにその顧客名とパスワードでログインした後、顧客を選択して、カスタムグラフを描くことができます。

OVIS でプロファイルがすでに設定してある場合は、そのプロファイルを上記のようにして OVPM へ追加します。その際、顧客名としてそのプロファイルを入力するとともに、そのプロファイルのパスワードも追加します。これで、そのプロファイルのどの顧客についても、ダッシュボードでカスタムグラフ を描けるようになります。

OVIS の「All Customers」ログインアカウントを同期させるには、OVPM Administration プログラムの [Customer] リストボックスで空欄になっている顧客を選択します。右クリックして [プロパティ] を選択し、次にパスワードを設定します (OVIS の「All Customers」と同じパスワードを設定します)。これで、OVIS ダッシュボードに「All Customers」でログインし、すべての顧客についてカスタムグラフを描けるようになります。

OVIS の制限表示を変更する場合は (顧客 / パスワードまたはプロファイル)、OVPM の方でも変更する必要があります。

インストールのトラブルシューティング

ここでは、インストールで発生する問題について、そのトラブルシューティングに役立つ情報をいくつか説明します。

問題 : インストールエラー 1923

解決策 : [サービス] アプレットが開いたままになっている可能性があります。[サービス] アプレットを閉じて問題を解決します。

TIPs のトラブルシューティング

TIPs コンポーネントのトラブルシューティング情報については、TIPs Configuration program のオンラインヘルプを参照してください。

ここでは、TIPs のトラブルシューティングについて、次の項目を説明します。

- TIPs のログファイル確認
- TIPs Viewer に表示されるエラーのトラブルシューティング

TIPs のログファイル確認

さまざまなログファイルを調べることで、TIPs のトラブルシューティングに役立つ情報を見つけることができます。ログファイルは OVIS 管理サーバーシステムと TIPs Runner のインストールされているシステムで作成されます。OVIS で作成されるログファイルの詳細については、398 ページの「OVIS のトレースファイルとログファイル」を参照してください。

TIPs のログファイルは次の場所にあります。

- Windows: `<data_dir>¥log¥*`
- UNIX: `/var/opt/OV/log/*`

`"_0_<0-9>.log"` で終わるログファイルについては、2 つのプロセスが同じ名前で同時に同じログファイルへメッセージを記録しようとした場合、一方のプロセスが書き出すログファイルの名前は `FileName_0_<0-9>.log` となり、もう一方のプロセスが書き出すログファイルの名前は `FileName_1_<0-9>.log` となります。また、ログファイルのサイズが決められた最大値に到達するたびに、番号 `<0-9>` が増えていきます。

表 6　　TIPs のログファイル

ログファイル	内容	場所
OvTIPsConfig_0_<0-9>.log	TIPs Configuration program のログ情報です。	サーバーシステム
OvTIPsCreateDB_0_<0-9>.log	TIPs データベース作成スクリプトのログ情報です。 作成スクリプトはインストールの時に呼び出されます。	サーバーシステム
OvTIPsDataExchange_0_<0-9>.log	TIPs インポート / エクスポートバッチスクリプトのログ情報です。インポートはインストールの時にその一部として呼び出されます。エクスポートはアンインストールの時に呼び出されます。 注記： TIPs Configuration program からのインポートとエクスポートは、TIPs Configuration program のログファイルにログとして記録されます。	サーバーシステム
OvTIPsRunner.log.txt	TIPs Runner のログ情報です。	サーバーシステム および リモート TIPs Runner システム
OvTIPsServer_0_<0-9>.log	TIPs Server のログ情報と、アラームトリガードデータベースのクリーンアップログ情報です。	サーバーシステム

TIPs Viewer に表示されるエラーのトラブルシューティング

この項では、TIPs を実行している時に発生するエラーについて、その基本的なトラブルシューティング情報を説明します。

TIPs コマンドのタイミング問題

ダッシュボードの TIPs Viewer で、指定された時間内にコマンドが実行されなかったことを示すエラーメッセージが表示された場合は、次のようにします。

- TIPs Viewer で、その TIP の [**Re-Run**] ボタンをクリックします。コマンドのタイムアウトは、TIP を同時に複数個実行したためにシステムの負荷が大きくなって発生した可能性があります。多くの場合は、TIP を 1 つずつ実行することで問題を解決することができます。
- TIPs Server のログファイルを調べて、コマンドが実行できなかったときの関連エラーを確認します。詳しくは、391 ページの「TIPs のログファイル確認」と 393 ページの「コマンドのタイミング問題を解決する」の項を参照してください。
- TIPs Runner を再起動します。TIPs Runner は実行状態になければなりません。また実行状態にあっても、再起動が必要な場合もあります。停止しているかもしれない場合や再起動が必要かもしれない場合は、次のように再起動コマンドを使用してください。

TIPs Runner を再起動するには、以下の手順を実行します。

1. TIPs Runner がインストールされているシステムへ移動します。
2. コマンドウィンドウから次のコマンドを実行して、TIPs Runner を再起動します。

   Windows の場合：`<install dir>¥bin¥ovc -restart ovtiprn`

   UNIX の場合：`/opt/OV/bin/ovc -restart ovtiprn`

コマンドのタイミング問題を解決する

TIPs コマンドの実行は、予想より長くかかることがあります。その場合は、TIPs Server のログファイルに次の 2 つのメッセージが記録されているはずです。

```
Command <command name> with ID <identifier> did not complete
within <number> milliseconds.
```

```
Command <command name> with ID <identifier> that resulted in a
command time out message (received after <number> milliseconds),
has now completed (received after <number> milliseconds).
```

2 番目のメッセージは、必ずしも 1 番目のメッセージのすぐ後ろにあるとは限りません。*<command name>* と *<identifier>* を照合して、見つかったメッセージが同じコマンドに対するものかどうかを確認してください。

該当するメッセージがあった場合は、コマンドがタイムアウトした TIP について、ダッシュボードの TIPs Viewer にある [**Re-Run**] ボタンをクリックします。実行する TIP を 1 つだけにすれば、同時に処理するコマンドの数が少なくなるので、タイムアウトの可能性も少なくなります。

それでもなおコマンドがタイムアウトする場合は、コマンドのタイムアウト値を変更します。コマンドの設定については、TIPs Configuration program のオンラインヘルプを参照して下さい。

TIPs Viewer のブラウザで停止ボタンをクリックしたときの不具合

ダッシュボードの TIPs Viewer で TIP の実行結果を待っている間にブラウザの [**Stop**] ボタンをクリックすると、進行状態を示すインジケータはそのまま表示され続けますが、TIP の結果が表示されなくなります。

その場合は、TIPs Server のログファイルに、「クライアントの異常停止で例外が発生したために TIP の結果を表示できない」ことを知らせるエラーメッセージが記録されます。

この状況から回復するには、TIPs Viewer のウィンドウを閉じて再起動します。

TIPs に対する HTTP_TRANS プローブの設定

問題 : HTTP_TRANS プローブに対して Monitored Service Status TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
Specified directory does not exist
```

解決策 : Web Transaction Recorder の [**ファイル**] > [**設定**] > [**プロパティ**] ダイアログボックスで [**エラー時画面をキャプチャ**] オプションがチェックされているかどうかを確認する必要があります。このオプションにチェックマークを付けておかない限り、HTTP_TRANS プローブでは、TIP が取得しようとしたときのエラーログもエラー画面のイメージも作成しません。

問題： HTTP_TRANS プローブに対して Probe Re-Execution TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
No results returned for command
```

解決策： このメッセージは、Windows 2000 で IE モードのリモート HTTP_TRANS プローブを実行すると表示されます。その理由は、Windows 2000 システムではこのプローブを実行しても結果が作成されないからです。また Windows 2000 では、IE モードの HTTP_TRANS プローブ (probehttptrans2) に -print オプションを付けて実行しても結果は作成されません。その理由はこのプラットフォームでは Windows の GUI アプリケーションからコンソールへ書き出せないからです。

TIP の認証問題

問題： HP から提供している Expect コマンドまたは WMIC コマンドを新規または既存の TIP に 1 つ追加して TIP を実行すると、TIPs Viewer に以下のエラーがどちらか 1 つ表示される。

```
Error: User authorization is not configured for system
myserver.hp.com
```

```
Node - myserver.hp.com ERROR: Code = 0x80041003 Description
= Access denied Facility = WMI
```

考えられる解決策： そのシステム (上記の例では myserver.hp.com) の TIPs Authentication Data Manager にエントリを追加します。認証レコードの詳細な追加方法については、TIPs Configuration program のオンラインヘルプを参照してください。

問題： HP から提供している WMIC コマンドを新規または既存の TIP に 1 つ追加するとともに、ユーザーアクセス用のコマンドに /user オプションと /password オプションを追加して TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
Invalid UserID.
```

考えられる解決策： Windows で TIPs Runner を実行している場合は、TIPs Authentication Data Manager にエントリを 1 つ追加します。認証レコードの詳細な追加方法については、TIPs Configuration program のオンラインヘルプを参照してください。

監視対象システムのオペレーティングシステムに関係する問題

問題 : HP から提供している WMIC コマンドを新規または既存の TIP に 1 つ追加して、TIPs Runner が動作している Windows マシンから監視対象のリモート Unix マシンに対して TIP を実行すると、TIPs Viewer に以下のエラーがどちらか 1 つ表示される。

```
Node - myunixserver.hp.com ERROR: Code = 0x800706ba
Description = The RPC server is unavailable. Facility =
Win32
```

```
WARNING: Could not obtain host information from machine:
[myunixserver.hp.com]. Some commands may not be
available.The RPC server is unavailable.The network path was
not found.
```

考えられる解決策 : TIPs Runner が動作しているマシンとリモートマシンでオペレーティングシステムの種類が違っています。確認対象システムにインストールされているオペレーティングシステムの詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

問題 : HP から提供している Expect コマンドを新規または既存の TIP に 1 つ追加して、TIPs Runner が動作している Unix マシンから監視対象のリモート Windows マシンに対して TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
Error: Cannot connect to system mywindowsserver.hp.com
```

考えられる解決策 : TIPs Runner が動作しているマシンと確認対象マシンでオペレーティングシステムの種類が違っています。確認対象システムにインストールされているオペレーティングシステムの詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

TIP Runner のルーティング

問題 : HP から提供している Target TCP Connections コマンドを新規または既存の TIP に追加して、TIP Runner が動作している Windows マシンから監視対象のリモート Windows マシンに対して TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
The Routing and Remote Access Service is not currently
running on mywindowsserver.hp.com. Please use 'net start
remoteaccess' on the machine to start the service.
```

考えられる解決策 : TIP Runner の動作しているマシンで、ルーティングサービスを有効にして起動します。Windows システムにおけるルーティングコマンドの詳細な要件については、TIPs Configuration program のオンラインヘルプを参照してください。

WMIC TIPs コマンド

問題 : HP から提供している WMIC コマンドを新規または既存の TIP に 1 つ追加するとともに、ユーザーアクセス用のコマンドに /user オプションと /password オプションを追加して TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
Node - mymgmtserver.hp.com ERROR: Code = 0x80041064
Description = User credentials cannot be used for local
connections Facility = WMI
```

考えられる解決策 : TIPs Runner が動作しているローカルマシンで WMIC コマンドを実行する場合、/user オプションと /password オプションは不用です。WMIC コマンドの詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

問題 : HP から提供している WMIC コマンドを新規または既存の TIP に 1 つ追加して、TIP を実行すると、TIPs Viewer に次のエラーが表示される。

```
Node - myserver.hp.com ERROR: Code = 0x800706ba Description
= The RPC server is unavailable. Facility = Win32. Please
wait while WMIC is being installed.
```

考えられる解決策 : TIPs Runner マシンで WMIC が有効になっていません。WMIC は、WMIC コマンドをはじめて実行したときに有効になります。この場合は、TIP コマンドで WMIC が有効になっているので、それ以外のアクションは必要ありません。

OVIS のトレースファイルとログファイル

OVIS では、トラブルシューティングにトレースファイルとログファイルを使用できます。これらのトレース / ログファイルは主に弊社で使用するために用意されているので、ここではその詳細について説明しません。しかし、これらファイルを調べることで有用な情報を得られることがあります。

TIP のログファイルの詳細については、391 ページの「TIPs のログファイル確認」を参照してください。

OVIS のトレースファイルには、以下の 2 種類があります。

- プローブのエラーおよびトレースのファイル
- OVIS 管理サーバーのステータスおよびトレースのファイル

プローブのエラーおよびトレースのファイルは以下の場所にあります。

表 7　　プローブのエラーおよびトレースのファイル

タイプ	場所	コメント
エラー / ステータス情報	`<datadir>/log/probe/error.log`	プローブとスケジューラのエラーです。
トレース / デバッグ情報	`<datadir>/log/probe/trace.log`	プローブとスケジューラのトレースメッセージです。
	HP OpenView Tracing コンポーネント (詳細はコメント欄を参照)	UDP_PERF プローブ用と TCP_PERF プローブ用のレセプタが生成するトレースメッセージは、HP OpenView Tracing コンポーネントにログとして記録されています。 TIPs のトレースメッセージは HP OpenView Tracing コンポーネントにログとして記録されています。

管理サーバーのステータスおよびトレースのファイルは以下の場所にあります。

表 8　　管理サーバーのステータスおよびトレースのファイル

タイプ	場所	コメント
エラー / ステータス情報	<install dir>¥data¥ status.iops status.reporter status.PM	OVIS のステータス & エラーです。 Reporter のステータス & エラーです。 OVPM のステータス & エラーです。
	HP OpenView Tracing コンポーネント (詳細はコメント欄を参照)	OVIS と Reporter のステータス / エラーメッセージは、上記のファイルに加えて HP OpenView Tracing コンポーネントにログとして記録されています。

表 8　　管理サーバーのステータスおよびトレースのファイル

タイプ	場所	コメント
トレース / デバッグ情報	<install dir>¥data¥trace.<program name>	コンポーネントに特有なトレース情報です (たとえば、trace.measEvent2)。ダッシュボードと TIP は除きます。
	HP OpenView Tracing コンポーネント (詳細はコメント欄を参照)	OVIS と Reporter のトレース / デバッグ情報は、上記のファイルに加えて HP OpenView Tracing コンポーネントにログとして記録されています。 TIP のトレースメッセージは、HP OpenView Tracing コンポーネントにログとして記録されています。
	<install dir>¥nonOV¥tomcat¥a¥logs	Tomcat 関連のログファイルです (たとえば起動の問題や例外など)。
	<install dir>¥data¥log¥OvisDashboard*	OVIS ダッシュボード関連のトレース / ログファイルです。
	<install dir>¥data¥log¥OvTIPs*	TIP 関連のトレース / ログファイルです。
	<install dir>¥data¥log¥System.txt	インストールに関連した OpenView 全体のエラーメッセージです。

HP Openview Tracing コンポーネントを使用する

HP OpenView Tracing コンポーネントを使うことで、すべての OpenView 製品にわたって一貫性のあるトレースビューを実現することができます。詳しくは管理サーバーの次の場所にある『*HP OpenView Tracing - コンセプトとユーザガイド*』を参照してください。

`<InstallDir>¥help¥iops¥c¥ov_tracing.pdf`

OpenView Tracing ツールは、`<InstallDir>¥support` にあります。

OpenView Tracing コンポーネントを使用する場合は、最初にトレースの GUI を有効にしてシステム (Unix または Windows) へアクセスできるようにし、次に、`ovtrcadm -a <hostname>` を実行します (<*hostname*> にはトレースを表示するシステムの名前を指定します)。`ovtrcadm` コマンドは、トレースするシステムで実行します。トレースと表示をローカルシステムで行う場合でも、`-a localhost` を指定する必要があるので注意してください。

Windows 上でトレースを表示するには、`ovtrcgui` アプリケーションを使用します。ウィザードの指示に従ってください。

ステータスファイルの説明

OVIS 管理サーバーのトレースファイルは trace.<programname> という名前です。たとえば、Web サーバーからプローブデータを受信する OVIS モジュールの場合、トレースファイルの名前は **`trace.measEvent2`** です。またローカルの記憶領域 (IOpsTraceTable) から Reporter のデータベースへデータを移動するプログラムの場合、トレースファイルの名前は **`trace.iopscollector`** です。これらのファイルは、サポート担当者が OVIS の問題を特定できるように用意されています。

次に、OVIS のステータス / トレースファイルをいくつか簡単に説明します。

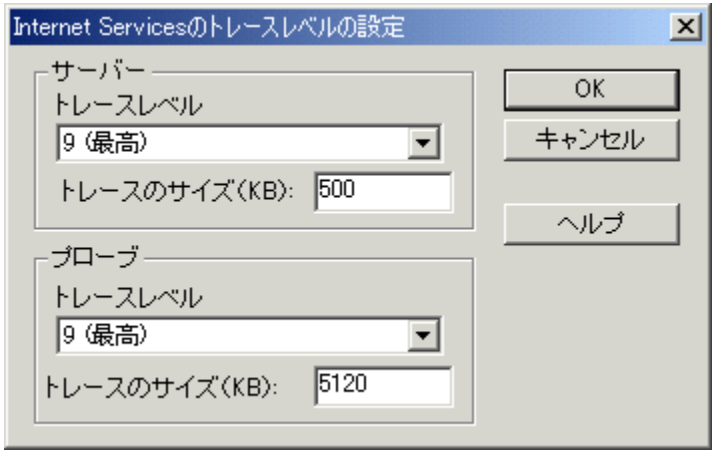
ステータスファイル	説明
status.iops	メインステータス
status.PM	グラフ作成コンポーネントのカスタムグラフのステータス
status.Reporter	レポート作成コンポーネントのステータス
trace.measEvent2	measEvent2.dll のトレース : measEvent2.dll は、アラームエンジンを使ってアラームを生成するとともに、(キューファイルから) 測定値を受け取って、そのデータを IopsTraceTable へ書き込みます
trace.DllVersion	Reporter dll のトレース

ステータスファイル	説明
trace.iopscollector	iopscollector のトレース：iopscollector は、IopsTraceTable にあるデータを Reporter のデータベースへ移します
trace.IOpsConfig	設定マネージャのトレース
trace.iopsmaint	データ保守のトレース：iopsmaint は、データを 1 時間ごとの加重平均と 1 日ごとの加重平均にまとめます
trace.iopsslaevaluator	SLA のトレース
trace.RepIOps	ダッシュボードのトレース
trace.RepCrys	夜間レポートのトレース
trace.RepMaint	データベース保守のトレース：RepMaint は、夜間に Reporter のデータベースを調べて、指定した保持日数より古いデータを削除します
trace.ExportIOps	ExportIOps プログラムのトレース：ExportIOps は、Reporter のデータベースにある設定情報を config.dat ファイルへ移します
trace.IOPSSQLUtils	renamedata ユーティリティで実行された SQL コマンドのトレース
trace.IOpsLoad	IOpsLoad プログラムのトレース：IOpsLoad は、Reporter のデータベースや config.xml との間で、設定情報を移します
trace.Scheduler	スケジューラプログラムのトレース：スケジューラからは、これらすべてのプログラムの実行に関する情報が得られます
trace.webrecorder	Web Transaction Recorder のトレース

IOPS の個々のエラーメッセージについては、411 ページの「エラーメッセージとステータスコード」を参照してください。また、IOPS のエラーメッセージに含まれているステータスコードとエラーコードについては、426 ページの「HTTP のステータスコード」と、429 ページの「SSL のエラーコード」を参照してください。

特定のプローブについてデバッグ用のトレース出力を得る方法

特定のプローブについてそのデバッグ用のトレース出力を収集する方法としては、Internet Services の設定マネージャで [**ファイル**] > [**設定**] > [**トレース**] を選択してトレースをオンにすることをお勧めします。



プローブのトラブルシューティングを行うには、トレースレベルを 9 に設定し、設定を保存します。変更した設定ファイル ([トレース] オプションが `config.dat` ファイルに追加されています) は自動的に展開配備しなおされ、プローブはトラブルシューティングで利用可能な、より詳細な情報をログへ記録するようになります。トラブルシューティングが完了したら、必ずトレースのレベルを元の値に戻してください。

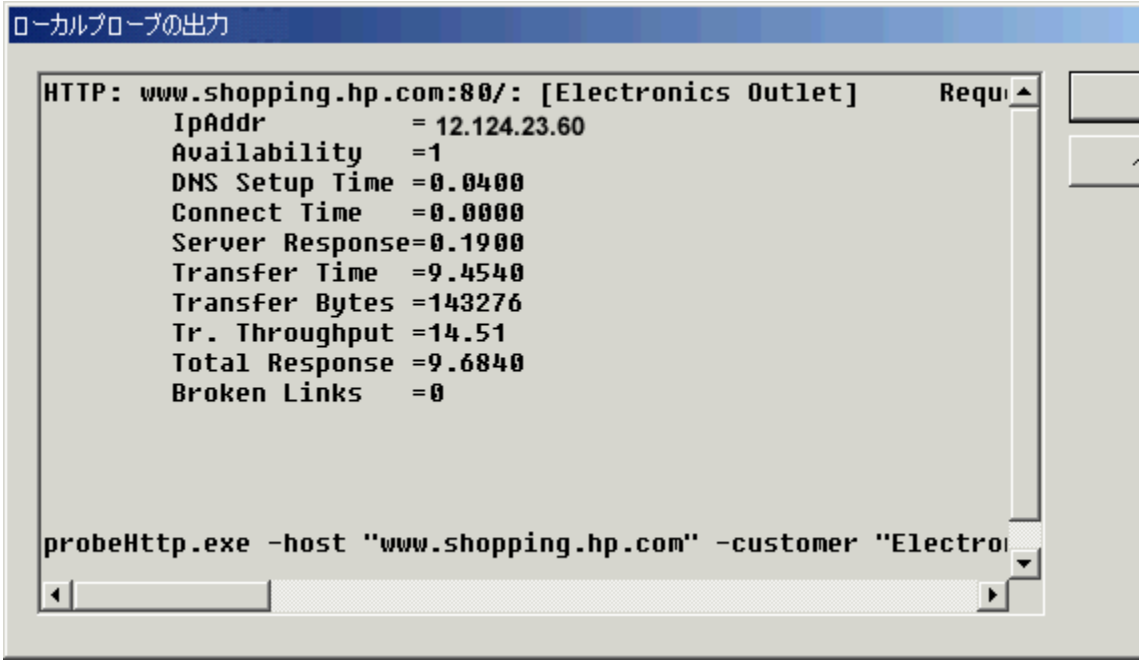
プローブのトレースファイルが作成されるので (`<datadir>¥log¥probe` ディレクトリにある `trace.log` と `error.log`)、そのファイルの内容を検索して ERROR ステートメントと WARNING ステートメントを見つけるとともに、それに続くテキストを確認して、エラーを解決する手がかりにしてください。詳細は 411 ページの「エラーメッセージとステータスコード」を参照してください。

特定のプローブについてデバッグ用のトレース出力を得るには、コマンドプロンプトから実行可能プローブを実行して、そのプローブのトレースファイルを調べます。以下に、Windows システムで行うこの例を説明します。

1 まず、プローブに対して実際に実行するコマンドを見つけます。

設定マネージャで、デバッグするプローブの監視対象サービスを右クリックし、[**管理サーバーでテスト**] を選択します。

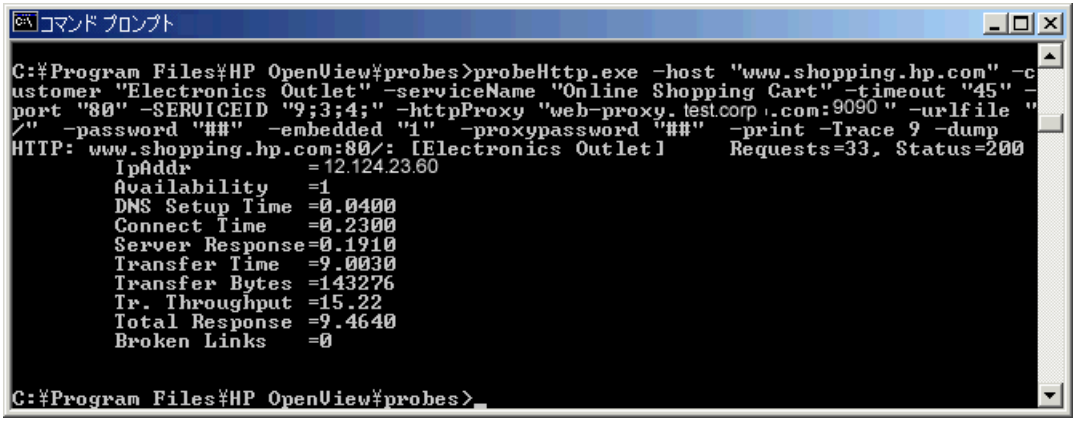
[ローカルプローブの出力] ダイアログボックスで、ダイアログボックスの下部にあるプローブのコマンド行をコピーします (コマンド行を見つけるにはスクロールダウンしなければならない場合があります)。



2. 次に、プローブシステムで、HP Internet Services サービスを停止させます (「net stop "HP Internet Services" 」かコントロールパネルを使用して、サービスを停止させます)。
3. `error.log` ファイルと `trace.log` ファイルがあれば、それらの名前をすべて変更し、コマンド行の実行で新しい `.log` が作成できるようにします。
4. [コマンドプロンプト] ウィンドウを開いて、`<install dir>¥bin` ディレクトリへ移動します。

5 [ローカルプローブの出力] ダイアログボックスで、コピーしたコマンド行をペーストし、**-print** オプションと **-dump** オプションを追加します。
[Return] キーを押す前に、-print オプションと **-dump** オプションを追加したことを確認してください。

.



6 次のファイルが作成されます。デバッグにはこれらのファイルを使用します。

— `<datadir>¥datafiles¥probe¥policies¥config.dat`

— `<datadir>¥tmp¥probe¥<dump file>`
ダンプファイルの名前は targetname.x.servicetype の形式で作成されます。たとえば、サービスが HTTP の場合は、`www.shopping.hp.com.0.HTTP` のようになります。このファイルにプロトコルのダンプ情報が含まれています。

`<datadir>¥log¥probe¥` ディレクトリに次のファイルが作成されます。

— `error.log`

— `trace.log`

7 HP Internet Services サービスを再起動する前にこれらのファイルを別の場所へコピーして、`error.log` ファイルと `trace.log` ファイルに必要なコマンド行のテストだけが含まれるようにします。

単純な HTTP プローブを例にとって、そのデバッグ出力を以下に示します。

プローブに対してコマンドプロンプトからコマンド行を実行した場合の例

```
probeHttp.exe -host "shopping.hp.com" -customer "HTTP_Test" -serviceName
"Test_HTTP" -timeout "45" -port "80" -SERVICEID "35;49;30;" -httpProxy "web-
proxy.test.corp.hp.com:9090" -httpsProxy "web-proxy.test.corp.hp.com:9090" -
urlfile "/"  -password "##" -embedded "1" -proxypassword "##"
-print -dump -trace 9


HTTP: shopping.hp.com:80/: [HTTP_Test]       Requests=6, Status=200
        IpAddr          =12.124.23.60
        Availability    =1
        DNS Setup Time =0.0160
        Connect Time    =0.0310
        Server Response=0.1410
        Transfer Time   =0.4060
        Transfer Bytes =79788
        Tr. Throughput =142.45
        Total Response =0.5940
        Broken Links    =0
```

ダンプファイル出力：

(この例の場合、ファイル名は <targetname>.x.<servicetype>、つまり www.shopping.hp.com.0.HTTP となります)。

ファイル名 (設定により異なります):

```
GET http://shopping.hp.com/ HTTP/1.0
Host: shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*

HTTP/1.0 200 OK
Connection: close
Date: Wed, 22 Oct 2003 16:22:37 GMT
Server: HP-UX_Apache-based_Web_Server/2.0.47 (Unix) DAV/2 mod_ssl/2.0.47
OpenSSL/0.9.6i
Last-Modified: Sun, 25 Aug 2002 22:12:19 GMT
ETag: "306b-aa-907fd6c0"
Accept-Ranges: bytes
Content-Length: 170
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=ISO-8859-1

<html>
<head>
```

```
<meta http-equiv="refresh" content="0;URL=http://www.shopping.hp.com/cgi-bin/
hpdirect/shopping/scripts/home/start_home.jsp">
…
GET http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/home/
start_home.jsp HTTP/1.0
Host: www.shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*

HTTP/1.0 200 OK
Connection: close
Date: Wed, 22 Oct 2003 16:22:37 GMT
Server: HP-UX_Apache-based_Web_Server/2.0.47 (Unix) DAV/2 mod_ssl/2.0.47
OpenSSL/0.9.6i
Set-Cookie:
hpshopping=1&session_info=%25VM)PXsPg.YT$$$i%5bk$DDHgXmASXJ%25VMlgNNsLP.YTmmm
mGqqRWW%3eW%3cRaAGww%3eWb%3cR%3cmmmmu%2bDD$iPX$ix%2bkiHHkiXiaGtDR&cart_id=102
463255&user_type=0&bivisitor=0&cart_empty=1&time=1066839757940;expires=Monday
, 30-Dec-06 22:00:00 GMT;path=/
P3P: CP="CAO DSP COR CURa ADMa DEVa TAIa PSAa PSDa CONi OUR DELa BUS PHY ONL
UNI PUR COM NAV INT STA"
Vary: Accept-Encoding,User-Agent
Content-Type: text/html; charset=ISO-8859-1

<script language="JavaScript">
```

この結果得られるトレースファイルの内容に注釈を加えて、以下に示します (Windows ホスト上でプローブが実行されている場合) 。注釈は先頭に「 ^^^」を付けて太字にしてあります :

```
Trace init - HTTP or HTTPS Probe
Probe Type was not a parameter or the value was empty, using HTTP value by
default
HTTP: retry=0 of 0, max timeout=45, run timeout=45, wait time=0
```
^^^ 再試行回数と待機時間の情報です。ここでは、再試行が指定されていません。
```
TCP: Scheduling: 'shopping.hp.com'
Connecting: (web-proxy) 12.124.23.60 @ 9090
```
^^^ ソケット接続のために connect() を呼び出す前の状態です。この行から、connect() で使用するホスト名、IP アドレス、およびポートがわかります。
```
HandleProtocol(shopping.hp.com): state=0
```
^^^ 状態マシンの状態です (「state 0」は、connect() が成功した後の状態です)。
```
Request: url='http://shopping.hp.com/'
Request: 'GET http://shopping.hp.com/ HTTP/1.0
Host: shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
```
^^^ 接続を介して送信しようとしている HTTP リクエストです。

```
Send[shopping.hp.com]: sb=204 (cnt=204)
Send[shopping.hp.com]: done
```
^^^ 送信が成功して、204 バイトが送られています。
```
Receive[shopping.hp.com]: num_recv=1 br=528
```
^^^ サーバーから最初のデータブロックを受信しています (recv() に対して 528 バイトが返されています)。
```
HTML: Meta refresh timer=0
```
^^^ パケットが HTML パーサーにそれぞれ転送されています。ここでは、<META refresh 属性 > を検出しています。
```
Receive[shopping.hp.com]: num_recv=2 br=0
```
^^^ recv() を呼び出して次のブロックを受信しようとしていますが、サーバー側から接続がクローズされたので、「br = 0」つまり「受信バイト数＝ 0」となっています。
```
Close
```
^^^ こちら側でも接続をクローズしています (つまりソケットをクローズしています)
```
Receive[shopping.hp.com]: connection closed
```
^^^ ヘッダーにも「接続：クローズ」が示されています。
```
received: 200 (bytes=528)
```
^^^ プローブで受信したデータは合計 528 バイトで、応答のステータスは「200」であったことがわかります。
```
Cookies received :
```
^^^ 応答にはクッキーが含まれていませんでした。
```
Close
Close
Connecting: (web-proxy) 12.124.23.60 @ 9090
HandleProtocol(www.shopping.hp.com): state=0
Request: url='http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/
home/start_home.jsp'
```
^^^ リダイレクトが行われています (<META refresh> タグあったからです)。
```
Request: 'GET http://www.shopping.hp.com/cgi-bin/hpdirect/shopping/scripts/
home/start_home.jsp HTTP/1.0
Host: www.shopping.hp.com
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
Send[www.shopping.hp.com]: sb=343 (cnt=343)
Send[www.shopping.hp.com]: done
Receive[www.shopping.hp.com]: num_recv=1 br=1072
Receive[www.shopping.hp.com]: num_recv=2 br=1072
Receive[www.shopping.hp.com]: num_recv=3 br=1460
...
Receive[www.shopping.hp.com]: num_recv=36 br=0
```
^^^ ブロックを 36 個受信した後、サーバー側から接続がクローズされています。
```
Close
Receive[www.shopping.hp.com]: connection closed
received: 200 (bytes=72452)
Cookies received : Set-Cookie:
hpshopping=1&session_info=%25VM)PXsPg.YT$$$i%5bk$DDHgXmASXJ%25VMlgNNsLP.YTmmm
mGqqRWW%3eW%3cRaAGww%3eWb%3cR%3cmmmmu%2bDD$iPX$ix%2bkiHHkiXiaGtDR&cart_id=102
463255&user_type=0&bivisitor=0&cart_empty=1&time=1066839757940;expires=Monday
, 30-Dec-06 22:00:00 GMT;path=/
```
^^^ サーバーから固定クッキーがいくつか返ってきています (expires=Monday,30-Dec-06

22:00:00 GMT)

```
Close
Connecting: (web-proxy) 12.124.23.60 @ 9090
HandleProtocol(hpshopping.speedera.net): state=0
Request: url='http://hpshopping.speedera.net/www.shopping.hp.com/shopping/
images/icons/icon_mpss_23x23.gif'
Request: 'GET http://hpshopping.speedera.net/www.shopping.hp.com/shopping/
images/icons/icon_mpss_23x23.gif HTTP/1.0
Host: hpshopping.speedera.net
User-Agent: Mozilla/4.0 (WinNT; I; OVIS)
Accept: */*'
```

エラーメッセージとステータスコード

IOPS のエラーメッセージは、設定したトレースレベルとは関係なく error.log ファイルにログとして記録されます。

IOPS エラーメッセージの中には HTTP のステータスコードや SSL のエラーコードを参照しているものがあるので注意してください。HTTP のステータスコードと SSL のエラーコードは IOPS のエラーメッセージとは別の表としてこの後にまとめてあります。

IOPS のエラーメッセージは、2 つの表に分けて示してあります。最初の表には、HTTP_TRANS プローブの IOPS エラーメッセージが、また 2 つ目の表には、その他のプローブの IOPS エラーメッセージがそれぞれ示してあります。

次に示す例は、IE モードの HTTP_TRANS プローブについて、error.log ファイルからその一部分を抜き出したものです。

```
2004-02-03 08:05:14 エラー probeHttpTrans2(3296)
[CIETransController.cpp:626]: IOPS 0-20018: ステップ #0 に 'ie2/ie2
SG' （ステータス =0x800c0005（サーバーまたはプロキシが見つかりませんでした））
が見つかりません
```

表 9　　IOPS のエラーメッセージ ― IE モードの HTTP_TRANS プローブ

IOPS 0-x エラー	メッセージ
IOPS 0-20001	トランザクションファイルをロードできません。
IOPS 0-20002	顧客 / サービス名 '< 顧客 >/< サービスグループ >' が < トランザクションファイル > に見つかりません。
IOPS 0-20003	トランザクションを '< ファイル >' に保存できません。
IOPS 0-20004	'< ファイル >' からトランザクションをロードできません。
IOPS 0-20005	再生用のタイマーを設定できません。
IOPS 0-20008	記録またはロードされたトランザクションがありません。
IOPS 0-20009	再生ファイル '< 名前 >' を保存できません。
IOPS 0-20010	以下を実行できません。'< プログラム >'

表 9　IOPS のエラーメッセージ ― IE モードの HTTP_TRANS プローブ (続き)

IOPS 0-x エラー	メッセージ
IOPS 0-20011	'<URL>' の解決に失敗しました！ 記録を停止します。
IOPS 0-20014	ステップを削除できません。
IOPS 0-20015	パターンが見つかりません。
IOPS 0-20016	'< 顧客 >'/'< サービスグループ >' のトランザクションがタイムアウトになりました。
IOPS 0-20017	ステップ '< 番号 >' が見つけられません。
IOPS 0-20018	ステップ #< 番号 > に '< 顧客 >'/'< サービスグループ >' にパターンが見つかりません (ステータス =<http ステータスコード >)。
IOPS 0-20019	'< プログラム >' を実行できません。
IOPS 0-20020	イベントメッセージを判別できません。
IOPS 0-20021	ステップ '< 番号 >' ('< 顧客 >'/'< サービスグループ >') を解決できません。
IOPS 0-20022	'<URL>'@< インデックス番号 > に最も近い一致が見つかりません。
IOPS 0-20023	フレーム '< 名前 >' が見つかりません。
IOPS 0-20024	FORM の input エレメント '< 名前 >' が不明です。
IOPS 0-20025	プロキシを設定できません (< エラーメッセージ >)。
IOPS 0-20039	記録の警告
IOPS 0-20042	パスワードが一致しません。もう一度入力してください。
IOPS 0-20043	プロキシパスワードが一致しません。もう一度入力してください。
IOPS 0-20046	パターンが失敗しました : '< パターン >'。
IOPS 0-20047	ステータス : <http ステータスコード >

表 9　IOPS のエラーメッセージ ― IE モードの HTTP_TRANS プローブ (続き)

IOPS 0-x エラー	メッセージ
IOPS 0-20048	ウィンドウを '< ファイルのパス >' へキャプチャします。
IOPS 0-20049	[タイムアウト]
IOPS 0-20050	再試行 #< 数字 >
IOPS 0-20051	可用性チェックスクリプトの手順 #< 数字 >('< 顧客 >'/'< サービスグループ >') が失敗しました。
IOPS 0-20052	スクリプトが失敗しました : '< 名前 >'。
IOPS 0-20053	ステータス : <IE モードからの http ステータスコード >
IOPS 0-20054	URL の構文解析に失敗しました
IOPS 0-20055	セッションは開始されませんでした
IOPS 0-20056	接続できません
IOPS 0-20057	サーバーまたはプロキシが見つかりませんでした
IOPS 0-20058	オブジェクトの実体が見つかりませんでした。例 : http: 404
IOPS 0-20059	接続しましたがデータの取り出しに失敗しました
IOPS 0-20060	一般的なダウンロードの失敗です (接続が切断されました)
IOPS 0-20061	このオブジェクトにアクセスするには認証が必要です。例 : http: 401
IOPS 0-20062	必要なタイプのオブジェクトがありません。http: 403 no object
IOPS 0-20063	インターネット接続がタイムアウトしました
IOPS 0-20064	要求が無効です
IOPS 0-20065	プロトコルが不明です。また、接続に使用可能なプロトコルが登録されていません。
IOPS 0-20066	[プローブは < 数字 > 秒後にタイムアウトします]

表 9　IOPS のエラーメッセージ ― IE モードの HTTP_TRANS プローブ（続き）

IOPS 0-x エラー	メッセージ
IOPS 0-20067	[<http ステータスコード ><http ステータステキスト >] [URL] < 現在の URL>
IOPS 0-20068	['< スクリプト名 >' でスクリプトチェックに失敗しました]
IOPS 0-20069	['< パターン >' でパターンチェックに失敗しました]
IOPS 0-20070	<IE モードからの http ステータスコード ><IE モードからの http ステータステキスト >] [URL] < 現在の URL>
IOPS 0-20071	不正なリクエスト
IOPS 0-20072	認証が必要
IOPS 0-20073	有料です
IOPS 0-20074	アクセス禁止
IOPS 0-20075	ファイル未検出
IOPS 0-20076	許可されないリクエスト
IOPS 0-20077	受付拒否
IOPS 0-20078	プロキシの認証要
IOPS 0-20079	タイムアウト
IOPS 0-20080	競合あり
IOPS 0-20081	転送先不明
IOPS 0-20082	長さ情報要
IOPS 0-20083	条件不一致
IOPS 0-20084	リクエスト過大
IOPS 0-20085	URI 過長
IOPS 0-20086	メディアタイプ不適

表 9　IOPS のエラーメッセージ ― IE モードの HTTP_TRANS プローブ（続き）

IOPS 0-x エラー	メッセージ
IOPS 0-20087	リクエスト範囲不適
IOPS 0-20088	期待値違反
IOPS 0-20089	サーバー内部エラー
IOPS 0-20090	未実装
IOPS 0-20091	ゲートウェイ不適
IOPS 0-20092	サービス不可
IOPS 0-20093	ゲートウェイタイムアウト
IOPS 0-20094	HTTP バージョン不適
IOPS 0-20095	[プロキシ] %s
IOPS 0-20096	不明なエラー
IOPS 0-20097	[プロキシ] (不在)
IOPS 0-20098	[URL] %s
IOPS 0-20099	[URL] (不明)

エラー番号 IOPS 0-20071 ～ IOPS 0-20094 は、HTTP のエラーコード 400 ～ 417、500 ～ 505 に対応しています。

次の表 10 に、その他すべてのプローブの IOPS エラーメッセージを示します。次に示す例は、HTTP プローブの error.log ファイルからその一部分を抜き出したものです。

```
2004-02-04 14:50:04 エラー probeHttp(1636) [CHttpService.cpp:2637]: IOPS
1-112: ERRORINFO: [1 Broken Link(s)] [403 Access Forbidden] http://
ros84007tst3.test.tst.com:80/reports/mypage.htm [URL]
http://ros84007tst3.test.tst.com:80/reports/mypage.htm [PROXY] (none)
Customer='HP' Service Group='MY PAGE' Target='
ros84007tst3.test.tst.com:80/reports/mypage.htm'
```

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ

IOPS 1-x エラー	メッセージ
IOPS 1-1	Unable to open file '<file name>'.
IOPS 1-2	Unable to write to file '<file name>'.
IOPS 1-3	Unable to read from file '<file name>'.
IOPS 1-4	Unable to allocate memory.
IOPS 1-5	Unable to create file '<file name>'.
IOPS 1-6	Function <name> returned error.
IOPS 1-7	Unable to access '<item>'.
IOPS 1-8	Unable to get file size of '<item>'.
IOPS 1-9	Unable to execute process '<name>'.
IOPS 1-10	Unable to create a thread.
IOPS 1-11	Socket error <number> in '<item>'.
IOPS 1-12	Required property '<item>' not found in section [<name>].
IOPS 1-13	WinInet API--Error <number> in Function '<name>'. Host='<hostname>'.
IOPS 1-14	<name> protocol error: Unexpected response from server '<server>': '<buffer>'.
IOPS 1-15	Connection to '<host>' timed out.
IOPS 1-16	Unable to resolve IP-address for '<host>'.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-17	RAS or TAPI Failure: <number> in Function '<name>'.
IOPS 1-18	LDAP failure: Error <number> in Function '<name>'.
IOPS 1-19	HTTP failure: Redirection to non-HTTP protocol from < protocol type > to <protocol type> not supported.
IOPS 1-20	Error loading transaction file ‘<name>'.
IOPS 1-21	Transaction file is required.
IOPS 1-22	Schema in URL '<name>' is not known.
IOPS 1-23	Error resolving navigation point '<step>' (type: '<step type>').
IOPS 1-24	Transaction '<customer>:<service group>' timed out.
IOPS 1-25	Too many HTTP/HTTPS redirects (infinite loop?).
IOPS 1-26	Unable to resolve name server.
IOPS 1-27	ICMP: Unable to do ioctlsocket (wsa=<error number>).
IOPS 1-30	Certificate chain bad (usually subject/issuer mismatch).
IOPS 1-31	Certificate has expired.
IOPS 1-32	Unknown and unprovided root certificate.
IOPS 1-33	Unknown Certificate chain validation error <number>.
IOPS 1-34	Trusted Root Certificate count = <total count>.
IOPS 1-35	Certificate validation Failed.
IOPS 1-36	Certificate Name could not be validated.
IOPS 1-37	InitSSLContext() Failed.
IOPS 1-38	SSLHandshake() Failed with error < ssl error number >.
IOPS 1-39	InitSSLCryptoEngineModules() Failed with error <ssl error number>.
IOPS 1-40	SSLInitialize() Failed with error < ssl error number >.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-41	SSL ConfigureContextForRandom() Failed with error < ssl error number >.
IOPS 1-42	SSLSetCheckCertificateChainFunc() Failed with error < ssl error number >.
IOPS 1-43	SSLSetProtocolSide() Failed with error < ssl error number >.
IOPS 1-44	SSLSetProtocolVersion() Failed with error < ssl error number >.
IOPS 1-45	SSLLoadTrustedCertificateFile() Failed with error < ssl error number >.
IOPS 1-46	SSL ConfigureContextForDB() Failed with error < ssl error number >.
IOPS 1-47	SSLDuplicateChildContext() Failed with error < ssl error number >.
IOPS 1-48	SSLSetIOSemantics() Failed with error < ssl error number >.
IOPS 1-49	SSLSetPeerID() Failed with error < ssl error number >.
IOPS 1-50	SSLGetNegotiatedCipher() Failed with error < ssl error number >.
IOPS 1-51	SSLGetCiphersuiteInfo() Failed with error < ssl error number >.
IOPS 1-52	Loading Client Certificate Failed with error <ssl error number>.
IOPS 1-53	Loading Client Certificate Failed with error <ssl error number>, verify password on private key.
IOPS 1-54	Loading Client Certificate Failed with error <ssl error number>, verify client certificate file exists in the probes directory.
IOPS 1-55	Unable to create directory '<name>'.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-56	Pattern not found in step #<number> for '<customer>'/'<service group>' (Status=<http status number>).
IOPS 1-57	Pattern not found for '<customer>'/'<service group>' (Status=<http status code>).
IOPS 1-58	Pattern not found for '<customer>'/'<service group>'.
IOPS 1-59	Pattern failed: '<pattern>'.
IOPS 1-60	Status: <http status code>.
IOPS 1-61	MeasureAll() Failed.
IOPS 1-62	Metric Logging Failed.
IOPS 1-63	SQL ERROR Message = SQLSTATE: <type> Native error: <number> Message: <SQL error message>.
IOPS 1-64	SQLAllocHandle() Environment Setup Failed.
IOPS 1-65	SQLAllocHandle() Connection to Datasource Failed.
IOPS 1-66	SQLConnect() Failed.
IOPS 1-67	SQLAllocHandle() Execute Failed.
IOPS 1-68	SQLExecDirect() Failed.
IOPS 1-69	SQLColAttributes() Failed.
IOPS 1-70	SQLFetch() Failed.
IOPS 1-71	SQLGetData() Failed.
IOPS 1-72	[Timeout].
IOPS 1-73	User login failed for user '<name>'.
IOPS 1-74	Impersonate logged on user failed.
IOPS 1-75	Create Pipe failed.
IOPS 1-76	Create process failed.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-77	Get password failed.
IOPS 1-78	Change directory failed.
IOPS 1-79	Create fork failed.
IOPS 1-80	Create exec failed.
IOPS 1-81	Unable to set pipe to non blocking.
IOPS 1-82	Web page contains <number> broken image links for '<customer>'/'<service group>'.
IOPS 1-83	Pattern '<pattern>' not found.
IOPS 1-84	Exit code status failed for script. Exit code check returned <number>.
IOPS 1-85	Exit code status failed for Results file script. Exit code check returned <number>.
IOPS 1-86	File '<name>' not found.
IOPS 1-87	File '<name>' access denied.
IOPS 1-88	Unable to impersonate user, error returned - <impersonate user error>
IOPS 1-89	Unable to logon to mapi profile <name>.
IOPS 1-90	Unable to get mapi session.
IOPS 1-91	Exchange server returned error '<type>', '<component>'.
IOPS 1-92	Exchange server (open inbox) returned error '<type>', '<component>'.
IOPS 1-93	Exchange server (list messages) returned error '<type>', '<component>'.
IOPS 1-94	Exchange server (Read New Message) returned error '<type>', '<component>'.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-95	Exchange server (open delete item folder) returned error '<type>', '<component>'.
IOPS 1-96	MAPIAllocateBuffer failed.
IOPS 1-97	MAPI - Open Address book failed.
IOPS 1-98	MAPI - GetProps from outbox folder object failed.
IOPS 1-99	MAPI - Message Store has no valid PR_IPM_OUTBOX_ENTRYID.
IOPS 1-100	MAPI - Open Entry of Outbox failed.
IOPS 1-101	MAPI - Folder object type of OpenEntry on lpFolder != MAPI_FOLDER.
IOPS 1-102	MAPI - CreateMessage failed.
IOPS 1-103	MAPI - SetProps failed.
IOPS 1-104	MAPI - Create custom address book entry failed.
IOPS 1-105	MAPI - CreateMessage failed.
IOPS 1-106	MAPI - Failed to SetProp on the custom message, will not send e-mail.
IOPS 1-107	MAPI - ModifyRecipients failed.
IOPS 1-108	Failed to create profile, mapi probe service will not run.
IOPS 1-109	Script step error info = <error message>.
IOPS 1-110	Script format incorrect on Step <number>.
IOPS 1-111	[<number> Broken Link(s)] <URL>.
IOPS 1-112	ERRORINFO: <error message> Customer='<name>' Service Group='<name>' Target='<name>'.
IOPS 1-113	Unable to load Trusted Certificate file <name>.
IOPS 1-114	Unable to load Client Certificate file <name>.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-115	Client Certificate Failed. Verify password on private key.
IOPS 1-116	The Root Certificate is not trusted.
IOPS 1-117	One of the certificates in the chain is expired.
IOPS 1-118	File <name> is not formatted properly, or is missing a certificate or private key.
IOPS 1-119	Certificate Name could not be validated with (<host name>).
IOPS 1-120	SSLDuplicateContext() Failed with error <number>.
IOPS 1-121	Certificate name (<certificate>) does not match server name (<server>).
IOPS 1-122	Unable to create socket for <host name>.
IOPS 1-123	Socket host connection failed for <host name>.
IOPS 1-124	[DNS Unable to resolve host (<error message>)].
IOPS 1-125	[TCP Internal - Check log files] <error message>.
IOPS 1-126	[<number> Broken Link(s)] <http error message>.
IOPS 1-127	[SSL Error] <ssl error message>.
IOPS 1-128	[SSL Internal - Check log files].
IOPS 1-129	[SSL Timeout after <number> second(s). Check log files].
IOPS 1-130	[Probe Timeout after <number> second(s) at <error message>].
IOPS 1-131	[Pattern Check Failed on '<pattern>'].
IOPS 1-132	[<http error message>].
IOPS 1-135	[PROXY] <proxy server>:<proxy port>.
IOPS 1-136	[PROXY] (none).
IOPS 1-137	[URL] <host:port/…>.
IOPS 1-138	[Probe Timeout after <number> second(s)].

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-139	[Error Unknown].
IOPS 1-140	[URL] http://<host:port/…>.
IOPS 1-141	[URL] https://<host:port/…>.
IOPS 1-142	Unhandled Global Exception on '<name>'.
IOPS 1-143	HPPT/S Unhandled Exception: Customer='<customer>' Service Group='<service group>' Host='<host>' URL='<URL string>' Port='<port>' Proxy='<proxy>' Timeout='<number>'.
IOPS 1-144	HPPT_TRANS Unhandled Exception: Customer='<customer>' Service Group='<service group>' Proxy='<proxy>' Timeout='<number>'.
IOPS 1-145	Packet size must be greater than '<number>' and smaller than 65536.
IOPS 1-146	Select failed (error=<error number>).
IOPS 1-147	Timeout while trying to connect to '<name>'.
IOPS 1-148	UDP: Unable to retrieve results from server.
IOPS 1-149	ssl_CreateConnectionContext() failed with error <ssl error number>.
IOPS 1-150	sslrad_CreateSessionDB() failed with error <ssl error number>.
IOPS 1-151	ssl_SetCipherSuites() failed with error <ssl error number>.
IOPS 1-152	ssl_CreateGlobalContext() failed with error <ssl error number>.
IOPS 1-153	ssl_SetPRNG() failed with error <ssl error number>.
IOPS 1-154	ssl_SetProtocol() failed with error <ssl error number>.
IOPS 1-155	ssl_Handshake() failed with error <ssl error number>.
IOPS 1-156	ssl_SetCheckCertificateChainFunc() failed with error <ssl error number>.

表 10　　IOPS のエラーメッセージ ― その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-157	ssl_AddTrustedCACertificates() failed wtih error <ssl error number>.
IOPS 1-158	InitSSLMasterContext() failed with error <ssl error number>.
IOPS 1-159	ssl_SetIOSemantics() failed with error <ssl error number>.
IOPS 1-160	ssl_GetNegotiatedCipher() Failed with error <ssl error number>.
IOPS 1-161	ssl_SetIOFuncs() Failed with error <ssl error number>.
IOPS 1-162	InitSSLCryptoEngineModules() Failed with error <ssl error number>.
IOPS 1-163	ssl_SetClientAuthModes() Failed with error <ssl error number>.
IOPS 1-164	ssl_Read() Failed with error <ssl error number>.
IOPS 1-165	ssl_Write() Failed with error <ssl error number>.
IOPS 1-166	HTTPS Service timed out during ssl_Handshake().
IOPS 1-167	One of the certificates in the chain is expired in the Trusted Certificate file '<cert filename>'.
IOPS 1-168	Certificate Name (<cert name>) could not be validated with Server Name (<server name>).
IOPS 1-169	Certificate validation failed during the SSL Handshake.
IOPS 1-170	Extracting certificate name with ssl_ExtractCertificateNameItem() Failed with error <ssl error number>.
IOPS 1-171	Certificates not found in ssl_CheckCertificateChainCallback().
IOPS 1-172	Certificate public key is of an unsupported type in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-173	Certificate corrupted in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-174	Unsupported certificate signature algorithm in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.

表 10　　IOPS のエラーメッセージ ー その他すべてのプローブ (続き)

IOPS 1-x エラー	メッセージ
IOPS 1-175	Certificate parsing error in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-176	Certificate chain not trusted in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-177	Invalid PEM encoded certificate in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-178	Certificate has no serial number in ssl_CheckCertificateChainCallback(). Error = <ssl error number>.
IOPS 1-179	ssl_CheckCertificateChainCallback() Failed with certificate error <ssl error number>.
IOPS 1-180	Certificate check failed with the warning: <string> in ssl_CheckCertificateChainCallback().
IOPS 1-181	ssl_GetNegotiatedProtocolVersion() Failed with error <ssl error number>.
IOPS 1-182	WMI authentication failed with error <ssl error number>.
IOPS 1-183	WMI connect failed with error <ssl error number>.
IOPS 1-184	WMI metric retrieval failed with error <ssl error number>.
IOPS 1-185	WMI counter rolled or system rebooted. No queue file will be created this interval.

HTTP のステータスコード

次の表 11 に、HTTP 1.1 のステータスコードを示します。表中の説明は、www.w3.org の文書から抜粋したものです。HTTP (HTTPS と HTTP_TRANS) プローブで、HTTP のステータスコード 200 ～ 299 が返された場合は、そのプローブが利用可能であることを示しています。

表 11　　HTTP 1.1 のステータスコード

HTTP 1.1 のステータスコード	説明
情報 - 1xx	
100	継続可能です。
101	プロトコルを切り替えています。
成功 - 2xx	
200	OK です。
201	生成しました。
202	受理しました。
203	不当な情報です。
204	コンテンツがありません。
205	コンテンツをリセットしてください。
206	コンテンツはまだ一部分です。
リダイレクション - 3xx	
300	選択肢が複数個あります。
301	恒久的に移動しました。
302	見つかりました。
303	他を参照してください。
304	変更されていません。

表 11　　HTTP 1.1 のステータスコード (続き)

HTTP 1.1 のステータスコード	説明
305	プロキシを使用してください。
307	一時的なリダイレクトです。
クライアントエラー - 4xx	
400	不正なリクエストです。
401	認証が必要です。
402	有料です。
403	アクセスが禁止されています。
404	ファイルが見つかりませんでした。
405	メソッドが許可されていません。
406	受け付けることができません。
407	プロキシによる認証が必要です。
408	タイムアウトしました。
409	競合しています。
410	移動しました。
411	長さ情報が必要です。
412	前提条件が満たされていません。
413	リクエストの対象が大きすぎます。
414	URI が長すぎます。
415	メディアのタイプがサポートされていません。
416	リクエストの範囲が不十分です。
417	期待したようには処理できません。

表 11　　HTTP 1.1 のステータスコード (続き)

HTTP 1.1 のステータスコード	説明
サーバーエラー - 5xx	
500	サーバーの内部エラーです。
501	実装されていません。
502	ゲートウェイで無効なレスポンスを受け取りました。
503	サービスは利用できません。
504	ゲートウェイがタイムアウトしました。
505	この バージョンの HTTP はサポートされていません。

SSL のエラーコード

次の表 12 に、SSL のエラーコードを示します (これらは HTTPS または HTTP_TRANS プローブでログに記録される場合もあります)。表中の説明には、Certicom 社の API 文書から抜粋したものが一部含まれています。

表 12　　SSL のエラーコード

エラー番号	SSL のエラーコード	説明
0x150	CERT_SERVER_NAME_MISMATCH	証明書とサーバーの名前が一致しません。
0x151	NO_CERTIFICATES_FOUND	証明書を検証しようとして、証明書が見つかりませんでした。
0x152	CERT_WARNING_FOUND	証明書を検証しているときに、証明書の警告が見つかりました。
0x00000000	CIC_ERR_NONE	成功しました。
0x80010000	CIC_ERR_INTERNAL	証明書の有効日を抽出しているときに、エラーが発生しました。
0x81010001	CIC_ERR_NO_PTR	NULL ポインタが渡されました。
0x81010002	CIC_ERR_ILLEGAL_PARAM	パラメータが無効です。
0x81010004	CIC_ERR_SMALL_BUFFER	バッファが小さすぎます。
0x81010005	CIC_ERR_WOULD_BLOCK	I/O でブロックしています。
0x81010006	CIC_ERR_TIMEOUT	タイムアウトエラーです。
0x81010007	CIC_ERR_BAD_LENGTH	長さが無効です。
0x81010008	CIC_ERR_NOT_FOUND	エラーまたはレコードが見つかりませんでした。
0x81010009	CIC_ERR_BAD_CTX	コンテキストが無効です。
0x8101000A	CIC_ERR_BAD_INDEX	インデックスが無効です。
0x8101000B	CIC_ERR_RANDOM	乱数が無効です。
0x8101000C	CIC_ERR_MEM_UNDERRUN	SSL のメモリーエラーです。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x8101000D	CIC_ERR_MEM_OVERRUN	SSL のメモリーエラーです。
0x8101000E	CIC_ERR_MEM_WAS_FREED	SSL のメモリーエラーです。
0x8101000F	CIC_ERR_MEM_NOT_OURS	SSL のメモリーエラーです。
0x81090001	CIC_ERR_CERT_UNSUPPORTED_PUBKEY_TYPE	証明書内の公開鍵は、タイプがサポートされていません。
0x81090002	CIC_ERR_CERT_CORRUPTED	証明書が壊れています。
0x81090003	CIC_ERR_CERT_UNSUPPORTED_SIG_ALG	証明書に署名するためのアルゴリズムが、以前に登録されたものと違うかサポートされていません。
0x81090004	CIC_ERR_CERT_NOT_PARSED	証明書を正しく初期化できませんでした。
0x81090005	CIC_ERR_CERT_NO_TRUSTED_ISSUER	証明書を検証しようとして、発行者が信頼できない者であることがわかりました。
0x81090006	CIC_ERR_CERT_ILLEGAL_ALLOCATION_TYPE	割当てのタイプが、不明か選択されたオプションに適していません。
0x81090007	CIC_ERR_CERT_BAD_PEM	証明書は Base64 でエンコードされていますが、区切り文字が無効です。
0x81090008	CIC_ERR_CERT_NO_SN	この証明書にはシリアル番号がありません。
0x810A0001	CIC_ERR_SSL_INCOMPLETE_IDENTITY	証明書のリストに秘密鍵も証明書も含まれていません。
0x810A0002	CIC_ERR_SSL_BAD_SIDE	今回のモードのプロトコルは、前回のモードで選択されたものと異なっています。
0x810A0003	CIC_ERR_SSL_OVERFLOW	受信したレコードが、読込みバッファまたは書込みバッファのサイズを越えています。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A0004	CIC_ERR_SSL_UNEXPECTED_MSG	予期せぬメッセージを受信しました。
0x810A0005	CIC_ERR_SSL_BAD_MAC	SSL レコードメッセージを検証できませんでした。
0x810A0006	CIC_ERR_SSL_DECRYPT_FAILED	SSL レコードを暗号化できませんでした。
0x810A0007	CIC_ERR_SSL_UNKNOWN_RECORD	レコードのタイプが不明です。
0x810A0008	CIC_ERR_SSL_NEGOTIATION	SSL のネゴシエーションエラーです。
0x810A0009	CIC_ERR_SSL_IO	コールバックからの I/O エラーです。
0x810A000A	CIC_ERR_SSL_FATAL_ALERT	致命的な警告を受信または送信しました。
0x810A000B	CIC_ERR_SSL_PROTOCOL	一般的なプロトコルエラーです。メッセージの形式が正しくない可能性があります。
0x810A000C	CIC_ERR_SSL_RESUMABLE_SESSION	通信相手が、異なるセッションパラメータを使用してセッションを続行しようとしています。
0x810A000D	CIC_ERR_SSL_BAD_FINISHED_MESSAGE	SSL でハンドシェイクを行っているときに無効な終了メッセージを受信しました。
0x810A000E	CIC_ERR_SSL_CONNECTION_CLOSED_GRACEFUL	SSL 接続は正常に切断できました。
0x810A000F	CIC_ERR_SSL_CONNECTION_CLOSED	SSL 接続を切断しました。
0x810A0010	CIC_ERR_SSL_BAD_MAX_FRAGMENT_LENGTH_EXTENSION	max_fragment_length の拡張子に必要な値が不明です。
0x810A0011	CIC_ERR_SSL_BAD_CERTIFICATE	不正な証明書に対する雑多な一般的エラーです。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A0012	CIC_ERR_SSL_ALERT_CB_FAILURE	アプリケーションの警告コールバックからエラーが返りました。
0x810A0013	CIC_ERR_SSL_SESSION_NOT_FOUND	セッションデータベースにセッションがありませんでした。
0x810A0014	CIC_ERR_SSL_NOT_SUPPORTED	SSL2 での再ネゴシエーションは、サポートされていません。
0x810A0015	CIC_ERR_SSL_BAD_MESSAGE_LENGTH	通信相手から受信したメッセージは、長さが正しくありません。
0x810A0016	CIC_ERR_SSL_NO_SUPPORTED_CIPHER_SUITES	暗号スイートのローカル ID がないか、RSA の輸出に必要な RSA 輸出鍵がないか、またはネゴシエートしているプロトコルで暗号スイートがサポートされていません。
0x810A0017	CIC_ERR_SSL_NO_MATCHING_CIPHER_SUITES	ハンドシェークの両端で暗号スイートの一致がとれません。
0x810A0018	CIC_ERR_SSL_TLS_EXTENSION_MISMATCH	ハンドシェークの両端で TLS 拡張子の一致がとれません。
0x810A0019	CIC_ERR_SSL_BAD_PROTOCOL_VERSION	サーバーが、ネゴシエートできないプロトコルバージョンで ServerHello を送信しました。
0x810A001A	CIC_ERR_SSL_BAD_EXPORT_KEY_LENGTH	サーバーが、輸出規制の条件に合わない輸出鍵で ServerKeyExchange メッセージを送信しました。
0x810A001B	CIC_ERR_SSL_BAD_DHPARAM_KEY_LENGTH	サーバーが、輸出規制の条件に合わない DH パラメータで ServerKeyExchange メッセージを送信しました。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A001C	CIC_ERR_SSL_BAD_PREMASTER_SECRET_VERSION	プレマスタシークレットには、バージョンロールバック攻撃を検出する目的で ClientHello と同じバージョン番号が含まれている必要があります。クライアントによって送信されたバージョンは正しくありません。
0x810A001D	CIC_ERR_SSL_BAD_PREMASTER_SECRET_LENGTH	通信相手から送られてきたプレマスターシークレットは、長さが正しくありません。
0x810A001E	CIC_ERR_SSL_NO_CERTIFICATE	相手から送られてきた証明書メッセージに証明書が含まれていませんでした。
0x810A001F	CIC_ERR_SSL_NO_MATCHING_CERTIFICATES	相手から証明書メッセージで送られてきた証明書には、信頼できる証明機関の署名がありませんでした。
0x810A0020	CIC_ERR_SSL_CERTIFICATE_VALIDATE_FAILED	相手から証明書が送られてきましたが、その正当性を検証できなかったため、ユーザーの証明書コールバックから、この証明書に対してエラーが返されました。
0x810A0021	CIC_ERR_SSL_CERT_CHECK_CALLBACK	証明書コールバックに渡された証明書はそのコールバックによって拒否されましたが、外部エラーはコールバックに入力されませんでした。
0x810A0022	CIC_ERR_SSL_NULL_CB	引数として NULL コールバックのポインタが渡されたか、コンテキストに NULL コールバックが設定されています。
0x810A0023	CIC_ERR_SSL_BAD_CERTIFICATE_REQUEST	証明書要求メッセージのフォーマットが正しくありませんでした。
0x810A0024	CIC_ERR_SSL_ENTROPY_COLLECTION	内部エントロピーの収集で十分なシードデータを作成できませんでした。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A0025	CIC_ERR_SSL_BAD_CLEAR_KEY_LEN	SSL2 の ClientMasterKey メッセージで指定されている CLEAR-KEY-LENGTH が無効です。
0x810A0026	CIC_ERR_SSL_BAD_ENCRYPTED_KEY_LEN	SSL2 の ClientMasterKey メッセージで指定されている ENCRYPTED-KEY-LENGTH が無効です
0x810A0027	CIC_ERR_SSL_BAD_KEY_ARG_LEN	SSL2 の ClientMasterKey メッセージで指定されている KEY-ARG-LENGTH が無効です。
0x810A0028	CIC_ERR_SSL_BAD_SECRET_KEY_LEN	SSL2 ClientMasterKey メッセージから得た SECRET-KEY-DATA の長さが無効です。
0x810A0029	CIC_ERR_SSL_BAD_PKCS1_PADDING	復号化して得られた平文は、暗号化のときにパディングが行われていませんでした。
0x810A002A	CIC_ERR_SSL_FAIL_SERVER_VERIFY	SSL2 の SERVER-VERIFY メッセージを検証できませんでした。
0x810A002B	CIC_ERR_SSL_READ_BUFFER_NOT_EMPTY	レコードの読込みバッファは、空になっていないので、解放できません。
0x810A002C	CIC_ERR_SSL_WRITE_BUFFER_NOT_EMPTY	レコードの書込みバッファは、空になっていないので、解放できません。
0x810A002D	CIC_ERR_SSL_BUFFERS_NOT_EMPTY	レコードの読込みバッファと書込みバッファは、両方とも空になっていないので、解放できません。
0x810A002E	CIC_ERR_SSL_UNSUPPORTED_CLIENT_AUTH_MODE	選択されている暗号スイートでは、有効にしたクライアント認証モードを使用できません。
0x810A002F	CIC_ERR_SSL_BAD_CONTEXT	グローバルなコンテキストが、正しく設定されていないか無効です。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A0030	CIC_ERR_SSL_HANDSHAKE_REQUIRED	ハンドシェークを最初に行う必要があります。
0x810A0031	CIC_ERR_SSL_HANDSHAKE_REQUESTED	接続相手からハンドシェークの再ネゴシエーションが要求されました。ただし、ハンドシェークは行わなくてもかまいません。
0x810A0032	CIC_ERR_SSL_RENEGOTIATION_REFUSED	接続相手からハンドシェークの再ネゴシエーションが拒否されました。
0x810A0033	CIC_ERR_SSL_HANDSHAKE_ALREADY_COMPLETED	ハンドシェークはすでに完了しています。
0x810A0034	CIC_ERR_SSL_RENEGOTIATION_ALREADY_REQUESTED	再ネゴシエーションはすでに要求されています。
0x810A0035	CIC_ERR_SSL_READ_REQUIRED	接続相手との間でまだ再ネゴシエーションが開始されていません。ハンドシェークを進める前に読み込む必要のあるアプリケーションデータがあります。
0x810A0036	CIC_ERR_SSL_UNSUPPORTED_PUBKEY_TYPE	指定されたタイプの公開鍵はサポートされていません。
0x810A0037	CIC_ERR_SSL_BAD_RECORD_LENGTH	受信レコードの長さがプロトコル仕様で想定されている最大長を超えています。
0x810A0038	CIC_ERR_SSL_NEEDS_CIPHER_OR_CLIENTAUTH	秘密鍵をインストールする前に、同じキー交換アルゴリズム (RSA 対 ECC) を使用する暗号スイートまたはクライアント認証スイートをインストールしておく必要があります。
0x810A0039	CIC_ERR_SSL_INVALID_PFX	この操作に対して PFX が無効です。証明書と秘密鍵がともに含まれていないか、秘密鍵が複数個含まれています。

表 12　　SSL のエラーコード (続き)

エラー番号	SSL のエラーコード	説明
0x810A003A	CIC_ERR_PKCS12_MISSING_ALG	PFX で、スイートパラメータを通してまだサポートされていないアルゴリズムを使用しています。
0x810A003B	CIC_ERR_SSL_NEEDS_PRNG	PRNG スイートがまだインストールされていません。
0x810A003C	CIC_ERR_SSL_CERT_CHAIN_WARNINGS	証明書チェーンの検証に関連して警告があります。
0x810A003D	CIC_ERR_SSL_WARN_TRUSTED_EXPIRED	証明書のリストには信頼できる証明書が載っていますが、その中に、期限の過ぎたものが 1 つ以上あります。
0x810A003E	CIC_ERR_SSL_PROTOCOL_VERSION_INVALID	使用しようとしているプロトコルバージョンが正しくありません。
0x810A003F	CIC_ERR_SSL_PROTOCOL_NOT_INSTALLED	使用しようとしているプロトコルバージョンはインストールされていません。
0xF001	CIC_ERR_MEMORY	メモリーの割当てエラーです。

アラームのトラブルシューティング

ダッシュボードにアラームが表示されない場合は、設定マネージャの [目標値の情報] ダイアログボックスにアラームのしきい値が設定されていることを確認してください。

次にトレースレベルを 9 に設定し、trace.measEvent2 ファイルの内容をチェックしてアラームが発生しているかどうかを調べます。アラームが発生していれば、そのトレース情報から、アラームがいつ発生したかを知ることができます。

なお、ダッシュボードへアラームを表示させるには、設定マネージャで [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、**[データベース (アラームと NNM の統合)]** チェックボックスにチェックマークを付けておく必要があります。

アラームの転送

アラームの転送を検証する方法としては、トレースレベルを 9 に設定して、`trace.measEvent2` ファイルの内容をチェックすることをお勧めします。トレースの情報から、アラームが発生した時刻とアラームの転送先がわかります。

アラームは、NNM へ転送されるときに IOPS_ALARM_DATA テーブルへ保存されます。このテーブルの内容は、IE 5.0 ブラウザで表示することができます。その際、URL に `http://<measurement_server's_hostname>/HPOV_IOPS/isapi/alarmEvent.dll?GetEvent` を指定します。

そうすれば、IOPS_ALARM_DATA テーブルの内容は XML 形式に変換されます。

アラームが OVO へ送られる場合は、`trace.measEvent2` に次のようなメッセージがログとして記録されます。

```
2000/10/17 07:25:19 (5): Alarm to ITO: OVIS Trans:
portico.hp.com:xxx.corp.hp.com:Trans:
HPWeb:PorticoNameLookup OVIS_HTTP_TRANS xxx.corp.hp.com
(ovis="xxx.corp.hp.com" customer="HPWeb"
serviceGroup="PorticoNameLookup" probeDesc="HTTP_TRANS - Web
Transactions" probeType="HTTP_TRANS" metric="RESPONSE_TIME")
```

OVIS では、以下の OVO 属性を設定します。

OVO 属性 (opcmsg)	OVIS の値
object	監視対象ホスト : プローブシステム : 監視対象情報
msg_grp	OVIS_< プローブ名 >
node	OVIS サーバーの FQDN (GUI で設定する場合は ipAddr)
msg_txt	メッセージテキスト
application	OVIS
severity	OVIS の重要度
option 変数	ovis=<OVIS サーバーの FQDN> customer=< 顧客 > seviceGroup=< サービスグループ > probeDesc=< プローブの説明 > probeName=< プローブ名 > metric=< メトリック >

たとえば、上記のトレースメッセージを例にとってアラームをエミュレートすると、opcmsg メッセージとそのパラメータは次のようになります。

```
opcmsg a=OVIS o="portico.hp.com:xxx.corp.hp.com:Trans:
HPWeb:PorticoNameLookup" msg_grp=OVIS_HTTP_TRANS
node=xxx.corp.hp.com msg_text="Test"
```

メッセージが OVO サーバーに送信されたかどうかを確認する

trace.measEvent2 ファイルを調べれば、OVO に送信された内容がわかります。以下にその例を示します。

```
2002/02/11 14:28:21 (5): Alarm to ITO (ret=0): OVIS
sev=Critical obj=127.0.0.1:xxx.corp.hp.com:81@127.0.0.1
grp=OVIS_ANYTCP node= (ovis="xxx.corp.hp.com"
customer="Test" serviceGroup="T1" probeDesc="TCP - TCP Port
Service" probeType="ANYTCP" metric="AVAILABILITY"
ipAddr="127.xx.0.1")
```

ret=0 は、メッセージが OVO キューに入れられたことを示しています。

したがって、最初に trace.measEvent2 ファイルをチェックして「Alarm to ITO」メッセージがあるかどうか調べ、もしあれば、そのリターンコードを確認します。メッセージがなければ、設定マネージャの [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、[**アラーム送信先の設定**] ダイアログボックスの [**OVO との統合**] で、[**デフォルト**] を選択して有効にします。継続してアラームを取得する場合は、[**アラームを継続的に送信**] ボックスを選択します (この機能はテストの場合に便利です。選択しておかないと、アラーム状態をいったんクリアした後で別のアラームを取得することになります)。

[アラームを継続的に送信] チェックボックス

設定マネージャの [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択し、[**アラーム送信先の設定**] ダイアログボックスで [**アラームを継続的に送信**] ボックスを選択し、サービスレベルの違反が発生した場合にアラームを継続して送信するように設定します。このボックスを選択しておかないと、アラーム状態が変わったときにしかアラームは送信されません。

つまり、このボックスを選択しておかないと、アラーム状態が変わるときにしかアラームを確認できないので、アラーム状態が変わらない限り、必要なアラームを確認できません。したがって、危険域のアラームが発生して、その状態が長時間にわたって継続すると、新しいアラームを知ることができません。新しいアラームを知ることができるのは、危険域の状態から別の状態へ変わったときだけです。

ベースラインの設定

設定マネージャでサービスグループにそのサービスの目標値を設定する場合は、[**目標値の情報**] ダイアログボックスの [**アラーム条件として、しきい値とともに履歴ベースラインを使用**] ボックスを選択して、ベースラインを選択します。ベースラインをオフにするには、そのボックスの選択を解除します。

チェックボックスを選択しておくと、確認したいアラームが確認できなくなることがあります。選択を解除して確認したいアラームが取得できるかどうかを確認してください。この機能の詳細については、126 ページの「ベースラインの動作」を参照してください。

[「正常域」アラームは送信しない] チェックボックス

設定マネージャの [**ファイル**] > [**設定**] > [**アラーム送信先**] ダイアログボックスで [「正常域」アラームは送信しない] を設定することができます。このボックスはデフォルトで選択されています。

アラーム状態が解消されたときに END ALARM イベントを OVO へ送信する場合は、このボックスの選択を解除します。OVO のデフォルトでは、END ALARM イベントを送信しないようになっています。[「正常域」アラームは送信しない] を有効にすることで、次の機能を使用できるようになります。つまり、OVO for UNIX 6.0 以降の状態ベースブラウザにある機能 (good/bad メッセージ自動相関処理) と OVO for Windows の似た機能、または、ITO の旧バージョンにある自動化されていないイベント相関処理が使用できるようになります。

アラームの遅延

IIS の [規定の Web サイトのプロパティ] ダイアログボックスには IP アドレスを設定するための [IP アドレス] フィールドがありますが、そこに設定されている IP アドレスによっては、アラームの表示が遅れることがあります。

IP アドレスは 「(未使用の IP アドレスすべて)」に設定する必要があります (この設定は、Web サーバーがローカルホストへアクセスできるようにするために必要です。また、OVIS は内部でローカルホストアクセスを使用しています)。

OVO for UNIX の統合機能が有効になっているが正しく動作していない

症状 : OVO for UNIX の統合機能が有効になっているが、OVO Browser にメッセージが表示されない。または、次のメッセージが status.iops に記録されている。

```
measEvent2 ERROR: Unable to locate VPO agent API - no VPO
alarming possible (ret=1)
```

解決策 :

OVO 7.x を使用している場合は、OVO NT エージェントパッチがインストールされている必要があります。

まず、OVO for UNIX エージェントがインストールされていて、統合テンプレートが機能していることを確認します。

OVIS で以下の手順を実行します。

- 設定マネージャで [**ファイル**] > [**設定**] > [**アラーム送信先**] を選択して、OVO for UNIX の統合機能が有効になっていることを確認します。
- 設定マネージャで、アラームメッセージを生成できる目標値が設定されていることを確認します (テスト時には、ベースラインを無効にして (0 に設定して)、アラーム保留時間を 1 に設定します)。

OVO for UNIX で以下の手順を実行します。

- **OVIS Server テンプレートグループ**が、OVIS 管理サーバーに割り当てられ、配布されていることを確認します。
- OVIS 管理サーバーノードが、ノードグループの一部になっていることを確認します。
- **OVIS** と **OVIS_Error** メッセージグループがオペレータの作業範囲の一部になっていることを確認します。

OVIS 管理サーバーのコマンド行で、以下のコマンドを実行します。

```
opcmsg a=OVIS o=o msg_t=Test
```

これにより、OVO メッセージブラウザにメッセージが表示されます。

メッセージが表示されない場合、システムの Path 環境変数に `opcapi.dll` の場所 (通常は、`¥usr¥OV¥bin¥OpC` ディレクトリや `¥usr¥OV¥bin¥OpC¥intel` ディレクトリ) が含まれていることを確認してください。OVIS は、システムの Path 環境変数にある OVO API ライブラリ `opcapi.dll` を必要とします。

[設定] > [コントロールパネル] > [システム] の [環境]、または [設定] > [コントロールパネル] > [システム] の [詳細] の [環境変数]

`¥usr¥OV¥bin¥OpC` と `¥usr¥OV¥bin¥OpC¥intel` を [システム環境変数] の [Path] に追加して、システムを再起動します。`¥usr¥OV¥bin¥OpC` と `¥usr¥OV¥bin¥OpC¥intel` を Path 環境変数の先頭に置く必要があるかもしれません。

これでもメッセージが OVO に転送されない場合は、OVO エージェント、OVIS、および IIS のすべてを同じドライブ (たとえば、C:) にインストールしてください。

ovisstatus

予定時間を過ぎても (+10% の遅延可能) プローブシステムからデータが送られてこない場合は、ovisstatus.exe プログラムが自動的に実行されて、OVO または NNM にアラームを送信します。

ovisstatus ではデータの着信予定時間を計算します。プローブシステムで有効かつ稼働状態の監視対象 (すなわち無効、計画的な停止状態を除く) すべてについて最短間隔を調べ、そのプローブシステムからデータが送られてくる予定時間を計算して、それに 10% の時間を追加します。たとえば、あるプローブシステムで有効になっている監視対象の最短プローブ間隔が 60 秒であれば、ovisstatus ではそれに 10% だけ時間を追加して (つまり合計で 66 秒)、その時間内にそのプローブロケーションから送られてくるデータを見つけようとします (ただしこの処理が行われるのは、そのプローブロケーションで 1 つ以上の有効かつ稼働状態にある監視対象がある場合のみです)。

OVIS 管理サーバーに Reporter のコンポーネントがすべてインストールされている顧客の場合は、Reporter の GUI に、ovisstatus.exe が「-alarm2 -probesystem -waitintervalp 10」のパラメータで 5 分ごとに実行されている様子が表示されます。デフォルト設定の -alarm2 が指定されているので、ovisstatus は、OVIS 設定マネージャの [**ファイル**] > **[設定**] > [**アラーム送信先**] ダイアログにある [アラームを継続的に送信] の設定に従って処理を行います。

ovisstatus のデフォルトパラメータをリセットするケースには、2 つの場合があります。1 つは、10% という値が一部の遅延にとって十分ではない場合で、その場合は、% 値 (-waitintervalp) を増やします。もう 1 つは、プローブシステムの中に、同じシステムに実装されている 2 つ以上のネットワークインタフェースカードから定期的にプローブデータを送信するものがある場合です。その場合は、ovisstatus から正しいステータスが返らないことがあります。この問題を解決するには、ovisstatus のデフォルト設定を変更して -probsystem を削除し、その代わりにプローブステーションの内部識別子を使用します。新しいコマンドは、「ovisstatus -alarm2 -waitintervalp 10」になります。OVIS では他のパラメータの変更をサポートしていないので、それらのパラメータを変更する場合は注意してください。

ovisstatus では、データベース側で管理している監視対象のステータス (有効または無効と、動作または計画的な停止) とリモートプローブの設定が一致しているものとして処理を行います。

通常は、OVIS オペレータが設定の変更を保存してから、その設定が自動的にリモートプローブシステムへ配布されるまでに、時間の遅れがいくらか伴います。

この時間の遅れは、リモートプローブシステムで監視対象が 1 つ以上動作していれば、特に問題とはなりません。しかし、設定マネージャのオペレータがリモートプローブシステムの監視対象をすべて無効にしてその設定を保存する場合を考えてみてください。当然ですが、その設定は自動的にそのリモートプローブシステムへ配布されることになります。

このような場合、ovisstatus ではその実行のたびにこのリモートプローブシステムにアクティブな監視対象がないことを知って、アラームを発行しません。ここまではすべてが期待どおりに機能します。

このような状態が 1 時間続いた後、オペレータがリモートプローブシステムの監視対象をすべて有効にして、その設定を保存し忘れたとします。すると、そのデータベースではリモートプローブロケーションにあるプローブシステムが有効になっているので、次に ovisstatus が実行されると、「最後の測定間隔 +10%」以内にデータが送られてきていないかどうかを調べることになります。しかし、1 時間以上にわたってデータが送られてきていないので、「そのロケーションからは送られてくるはずのプローブデータが送られてきていない」というアラームを発行することになります。

またオペレータがすぐに設定を保存した場合でも、その設定ファイルを受け取ったリモートプローブシステムがプローブデータを収集して Measurement Server へ返すまでの間に、ovisstatus が先に実行されてしまうという可能性があります。

このようなタイミングのずれは必ずあります。こうしたタイミングのずれに対する ovisstatus の脆弱性は、プローブロケーション上の監視対象がすべて停止 (無効、または計画的な停止) させられていた状態で、オペレータがその監視対象を 1 つ以上動作状態へ戻したときに、特に顕著となります。

ovisstatus は、計画的な停止に対してこうした問題の影響を最小化するようにプログラムが作成されており、「監視対象の停止が、計画された現在のものであるか 5 分前のものであるか」を判別して、処理を変えるようになっています。そのために、計画的な停止時間に入っている監視対象に対しては、特別なバッファが用意されています。しかし、無効になっている監視対象については、そのようなバッファが用意されていません。こうしたことから、プローブロケーション上の監視対象をすべて停止させておくときにその停止解除の時期が決まっていなければ、計画的な停止時間の定義として「365 日間終日」を使って、監視対象を実効的に無効化しておくことをお勧めします。

プローブごとのトラブルシューティング

プローブの実行方法とその結果への影響

プローブを実行する方法にはいくとおりかあり、その方法によっては、得られる結果も違ってきます。たとえばプローブ自体の成功 / 失敗や、メトリックの違いなども、そうした違いになって現れることがあります。以下に示すのはそうしたプローブ実行方法の一例です。

- プローブを設定して、OVIS スケジューラにプローブシステムのプローブを実行させる。
- 設定マネージャから [**管理サーバーでテスト**] を選択して、プローブをテストする。
- コマンド行からプローブを実行する。

この他に、別の方法で実行できるプローブもあります。たとえば HTTP_TRANS プローブは、Web Transaction Recorder (再生モード) の中から実行することができます。

これらプローブの実行方法でその結果を大きく左右する要因の 1 つは、プローブを実際に実行するユーザーです。

スケジューラを使ってプローブを実行する場合、プローブは「**ローカルシステム」のユーザー** ([HP Internet Services のプロパティ] ウィンドウに表示) として実行されます (HP Internet Services サービスを変更して他のユーザーとして実行している場合を除きます)。

コマンド行からプローブを実行する場合と、設定マネージャから [管理サーバーでテスト] を選択してプローブを実行する場合は、そのときにログインしているユーザーとして実行されます。ログインユーザーのパーミッションによってはプローブが成功したり成功しなかったりします。特に Script、Exchange、HTTP_TRANS の各プローブやカスタムプローブでは、その関係が明らかです。

また、スケジューラからプローブを実行する方法と、コマンド行または [管理サーバーでテスト] からプローブを実行する方法とでは、得られるメトリックの値が少し違ってきます。また、スケジューラからプローブを実行する場合は、現在設定されているプローブの数に合わせて、一度に 1 つ以上、プローブを実行することができます。結果として、スケジューラからプローブを実行する場合は、コマンド行または [管理サーバーでテスト] からプローブを実行する場合

よりシステムリソースが多く必要です。たとえば応答時間を 1 つ例にとっても、コマンド行または [管理サーバーでテスト] から実行するときより、スケジューラから実行するときの方が長くなります。

Exchange プローブと Script プローブのトラブルシューティング

問題 : Windows プローブシステムで Exchange プローブまたは Script プローブの監視対象サービスが利用不可の状態で、Windows 環境が初期化されない。

解決策 : プローブを設定したユーザーとして Windows プローブシステムにログインします。これにより、Windows 環境が初期化され、Windows ユーザープロファイルが設定されます。

HTTP_TRANS プローブのトラブルシューティング

Web Transaction Recorder を使用して HTTP_TRANS プローブを構成する際に発生する問題については、『*OVIS Web Transaction Recorder ガイド*』の「記録と再生に関する問題点」と「Web Transaction Recorder についてのヒント」を参照してください。

Windows 2000 で IE モードの HTTP_TRANS プローブ (probehttptrans2) に -print オプションを付けて実行しても、Windows GUI アプリケーションからコンソールに書き出せないので、結果は作成されません。つまり、Windows 2000 の設定マネージャで [**管理サーバーでテスト**] 機能を選択しても、IE モードの HTTP_TRANS プローブからは結果が返ってきません (Windows 2003 と Windows XP 以降では正常に動作します)。また Windows 2000 でこのプローブに対して Probe Re-Execution TIP を実行しても、「“No results returned for command”」というメッセージが表示されるだけです。

SOAP プローブのトラブルシューティング

要求が成功すると、HTTP の応答コードとして 200 が返ります。SOAP の応答を構成しているボディ要素には、有効な要求に対する応答要素の値が含まれています。

要求が失敗すると、HTTP の応答コードとして 500 (インターネットサーバーエラー) が返ります。SOAP サーバーからは、SOAP 応答の <soap:Body> 要素に <soap:Fault> 要素が入れられた状態でエラー状況が返されます。フォールト要素にはフォールトコード要素とフォールトストリング要素が含まれているはずです。

プローブのトレースレベルを 9 に設定することで、応答コードとエラー状況の情報を確認することができます。間違いのある要求の例については、次の例を参照してください。

```
HTTP/1.0 500 Internal Server Error.
Connection: close
Server: Microsoft-IIS/5.0
Date: Fri, 14 Nov 2003 01:49:43 GMT
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Content-Length: 597

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/
envelope/"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Client</faultcode>
      <faultstring>Server was unable to read request. --&gt;
There is an error in XML document (7, 54). --&gt; The
's0:getPopulationX' start tag on line '6' does not match the end
tag of 's0:getPopulation'. Line 8, position 9.</faultstring>
      <detail />
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

ストリーミングメディアプローブのトラブルシューティング

ストリーミングメディアプローブ実行時の問題については、次のことを確認してください。

考えられる原因 : プローブロケーションから監視対象メディアに Media Player がアクセスできない。

解決策 : 監視対象メディアに対して、プローブロケーションから Media Player を使用したアクセスが可能であることを確認し、各エラーメッセージを対処します。

考えられる原因 : メディアのコーデック、パッチ、アップデートに問題がある。

解決策 : 監視対象のメディアに適切な**コーデック**がインストールされていることを確認します。Real Player 8 ツールの [**表示**] > [**設定環境**] メニュー項目で [**アップグレード**] タブボックスを選択します。次に、[**アップデート通知**] セクションで [**今すぐアップデートをチェックする**] を選択します。最新の「Real One」プレイヤーをインストールするオプションを選択しないように注意してください。多数のコーデック、パッチ、アップデートがありますが、推奨されている適切なものをダウンロードします。

SYS_BASIC_WMI プローブのトラブルシューティング

ネットワークインタフェース情報を取得する接続時、または実際のプローブ実行時に、SYS_BASIC_WMI プローブでエラー 80041010 が発生する問題。この場合、WMI に対してシステムのパフォーマンスライブラリを再検出するように指示する必要があります。この指示は、ネットワークインタフェースの情報を得ようとして接続している最中か、実際にプローブを実行しているときかに関係なく、出す必要があります。再検索を指示するには、監視対象システムの DOS ウィンドウで次のコマンドを入力します。

```
wmiadap /c
wmiadap /f
wmiadap /r
```

TCP プローブのトラブルシューティング

問題 : TCP プローブの実行時に、TCP ポートに対する CLOSE_WAIT 状態の接続数が増加する問題。これは netstat コマンドを使用して確認できます。

考えられる原因 : 測定対象のポートが、プローブの要求に反してソケットを正常にシャットダウンしていないことが原因である可能性があります。これは通常、測定対象のアプリケーションがプローブからの要求時に、ソケットを正常に終了していないことと関連しています。

解決策 : プローブを停止するか、測定間隔を大きくします。

パターンマッチのトラブルシューティング

HTML 文字のエンコーディング

特定の HTML 文字はエンコードされます。(たとえば、「&」は「&」に、また「"」は「"」にエンコード)。パターンマッチの対象パターンを設定する場合は、HTML ソースを調べて (HTML ドキュメントを右クリックし、[ソースの表示] を選択) 、ブラウザへ表示される文字列にエンコードされた文字が含まれていないかどうかを確認する必要があります。文字列にエンコードされた文字が含まれている場合は、パターンマッチの対象パターンを調整する必要があります。

HTML の場合は、文字列 cats&dogs が cats&dogs にエンコードされているはずです。そのため、パターンマッチの対象パターンとして +"cats & dogs" を設定しても、この場合はうまく働きません。

また文字列が "See Spot & Fluffy Run!" の場合は、パターンマッチの対象パターンとして +""See Spot & Fluffy Run!"" を設定してもうまく働きません。その理由は、HTML ソースでは、& が & として、また引用符が " としてそれぞれエンコードされているためです。

しかし、文字列を単語に分解して特殊文字を削除すれば、つまり +"See"+"Spot" +"Fluffy"+"Run" にすれば一致します。

マイナス記号を使用して一致させないパターンを指定する

Web Transaction Recorder では、マイナス (-) 記号を使用することで、特定の単語が含まれているページを一致の対象から外すことができます。たとえば、ページが存在していなかったときに「The page cannot be found」というメッセージが返るようであれば、そのようなページを除外するように設定することができます。「-」記号を使用する場合は、一致させない単語と「-」記号との間に、スペースをいれないでください。上記の例では、パターンマッチの対象パターンとして -"The page cannot be found" と入力します。

検索する単語が 1 つだけである場合は、パターンとして -cannot と指定することもできます。ただし、「-」記号と単語との間にスペースを置くと、そのスペースは「+」記号として扱われるので注意してください。

OVIS と OVTA の統合に関するトラブルシューティング

ここでは、OVIS と OpenView Transaction Analyzer (OVTA) の統合に関するトラブルシューティングの参考となる情報を紹介します。

問題 : OVIS ダッシュボードに [**トレース**] ボタンが表示されない。

解決策 : OVIS-OVTA 統合に使用するレジストリエントリが OVIS Measurement Server 上に設定されていない可能性があります。設定方法については、『*OVTA Troubleshooting Guide*』を参照してください。

問題 : OVIS ダッシュボードで [**トレース**] ボタンをクリックすると、**「ページが見つかりません」**というエラーが表示される。

解決策 : ファイル `CorrRecords.asp` が、OVIS 管理サーバーのインストールディレクトリ内の適切な場所にコピーされていることを確認します。設定法方法については、『*OVTA Troubleshooting Guide*』を参照してください。このファイルの「`<form action=`」行で、OVIS 管理サーバー、ポート番号、およびプロトコルの参照を確認します。

問題 : OVIS ダッシュボードの [**トレース**] ボタンをクリックしてロードされたページに、空のテーブルが表示される。

解決策 : これは、OVIS データベース内に、トランザクション分析データ (OVTA データ) を持つ、利用可能なレコードが存在しないことを示します。この場合、OVTA Web Server Monitor を実行していない Web サーバー上のプローブ監視対象を使用していることが原因と考えられます。

問題 : OVIS ダッシュボードの [トレース] 画面の [**詳細**] ボタンをクリックしても、OVTA GUI が起動しない。

解決策 : 次の原因が考えられます。

Java WebStart がインストールされていない。この場合は、Java WebStart のダウンロードを行うページにリダイレクトされます。手順に従って、Java WebStart をダウンロードしてインストールします。

OVTA Measurement Server がダウンしている。

問題 : OVTA と同じサーバー上で OVIS を実行している場合に、OVTA Console にプローブデータが表示されない。

解決策 : 次のことを確認します。

1 プローブが、OVTA Web Server Monitor を実行してない Web サーバーにアクセスしている場合は、OVTA correlator がプローブに戻りません。Web サーバーから correlator を受信している場合にのみ、プローブがプローブデータを OVTA Measurement Server に転送することができるオプションがあります。デフォルトでは、OVTA correlator の有無に関係なく、プローブの送信データはすべて転送されます。この設定を変更するには、次のレジストリキーを true (ゼロ以外) の値に設定します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥HP
OpenView¥IPA¥CurrentVersion¥PostOnlyIfCorr
```

この値が 0 (ゼロ) の場合は、プローブの送信データはすべて OVTA Measurement Server に転送されます。

2 OVTA をインストールすると、OVTA Measurement Server への URL パスを含む OVTA レジストリエントリキーが設定されます。OVIS プローブは、これを使用してプローブデータを OVTA Measurement Server に送信 (転送) します。これが、OVTA Web Client Receptor Servlet に対する正しい URL であることを確認します。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥HP
OpenView¥IPA¥CurrentVersion¥ClientReceptorURL
```

3 OVIS のバージョンが 4.0 以降であることを確認します。

4 以上の項目を確認して問題がなければ、398 ページの「OVIS のトレースファイルとログファイル」の手順を参照し、トレースを有効にします。その後、`trace.measEvent2` トレースファイルを確認します。

複数ユーザーによる設定マネージャの同時使用

設定マネージャに複数のユーザーが同時にログインすることがある場合は、[**ファイル**] > [**設定**] > [**複数ユーザーオプション**] に [**同時更新のためのロック機構**] を設定することができます。ロックは、次のような場合に発生します。つまり、アクセスしようとしている項目またはその親項目に他のユーザーが現在アクセスしていると、同じ項目を変更してしまう可能性があるので、ロックが発生します。ロックが発生すると、ダイアログが開いて、「その項目は 他のユーザーがすでに使用しているので追加 / 更新 / 削除できない」という主旨のメッセージが表示されます。またロックは、保存しようとしている設定を他のユーザーが現在保存している最中にも適用されます。ここで注意しておかなければならないことは、設定に関係するようなウィザードを使用する場合は、グローバルなロックが使用されて、他のユーザーのできることがかなり制限されてしまうということです。逆に、他のユーザーが何かを変更しているときも、その間、設定ウィザードを開けません。複数ユーザーオプションの詳細については、101 ページの「その他の設定オプション」を参照してください。

デフォルトでは、ロックが使用されないようになっています。つまり、設定マネージャに複数のユーザーがログインして、変更操作を並行して行うことができるということです。そうなると、あるユーザーの変更した内容が別のユーザーによって上書きされてしまう可能性があります。

変更しようとしている対象が現在ロックされている場合は、そのロックが解除された後でもう一度試みるか、その対象をロックしている他のユーザーとの間で、変更方法を調整する必要があります (ロックメッセージにそのユーザーの ID が表示されます)。これができない場合は、[複数ユーザーオプション] ダイアログでロックをオフにしてロックをすべて解除します。ただし、あるユーザーがそのようにして行った変更は、ロックを行った他のユーザーが同じダイアログを開いていると、上書きされてしまう可能性があります。つまり、その別のユーザーがその変更を反映させないで [OK] をクリックしてしまうと、上書きされてしまう可能性があります。

[複数ユーザーオプション] ダイアログにロックがかかってアクセスできない場合は、設定マネージャ (`IopsConfig.exe`) とバッチ設定 (`IopsLoad.exe`) のインスタンスをすべて閉じることで、ロックをすべて解除することができます。

この方法でうまくいかない場合は、レジストリでロックをオフします。OVIS 管理システムにある HKEY_LOCAL_MACHINE¥SOFTWARE¥Hewlett-Packard¥Internet Services¥CurrentVersion キーの中で ConfigMgrShare の値を「2」に変更します。ロックをオンにする場合は、ConfigMgrShare の値を「1」にします。

プローブのスケジューリングに関する検討項目

測定間隔 : プローブに監視対象サービスの測定を開始させる間隔です。デフォルトは 5 分です (300 秒)。プローブはデフォルトの 300 秒を変えない限り、5 分ごとに実行されます。この値は、ネットワーク接続ごとに定義できます。つまり、ネットワーク接続が違えば、測定間隔の値も変えることができます。ただし、ここで注意しておかなければならないことは、「ネットワークに配置したそれぞれのプローブの実行が、次の実行間隔までの間にすべて完了する」ことを確認しておく必要があるということです。

リクエストのタイムアウト : 特定のプローブが実行できるようになってから測定値が返るまでの制限時間です。プローブがこの時間内に終了しないと、そのプローブは無効と見なされます。そのため、この値は大きくして余裕を持たせ、プローブが確実に完了できるようにしてください。つまり、値を大きくすることで、プローブがスケジューラによって停止されないようにします。それでもプローブがタイムアウトするようであれば、監視対象のアクセスに本質的な問題があると考えられます。この数値を大きくしても、プローブの測定には影響ありません。また、他のプローブの進行を妨げることもありません。たとえば値を 200 (秒) に設定しても、プローブにかかる時間が実際には 20 秒であれば、OVIS は残りの 180 秒間を待たずに次のプローブへ移ります。

ネットワークタイムアウト : 同じネットワーク内のすべてのプローブへ一律に割り当てる制限時間です。この制限時間を超えたプローブは、まだ完了していなくても終了させられてしまいます。そのため、この値を十分大きくして、このネットワークに配置したすべてのプローブが正常に機能するようにしてください。

並行実行数 : 1 つのネットワーク接続で一度に実行するプローブの数です。同じネットワークにプローブを 20 個配置して、並行実行数を 4 に設定すると、4 個のプローブがその完了まで同時に実行されます。この設定は HTTP_TRANS プローブを実行する場合に便利です。ただしこのプローブはリソースを多く使うので、並行実行数は少なくしてください。そうすれば、プローブがリソースを取り合うようなことはなくなります。並行実行数を少なくしないと、ユーザーの経験から予測される時間より長くかかることがあります。並行実行数とプローブのリソース使用に関する詳細は、『*OVIS Web Transaction Recorder ガイド*』を参照してください。並行実行数の最大値は 256 で、デフォルト値は 32 です。

プローブのタイミングとリソースの使用率に関する詳細は、146 ページの「プローブのロケーション、タイミングとスケジューリング」と 512 ページの「スケーラビリティ情報」を参照してください。

トラブルシューティングのためのツール

Perfstat

このスクリプトは、HP OpenView でパフォーマンスツールのステータスを監視するために使用できます。このスクリプトが最もよく使われるのは、システムでインストールされている HP OpenView ソフトウェアのバージョンを検索する場合です。よく使うオプションは、-v、-a、-z です。

使用法 : perfstat [オプション]

オプション	機能
-?	perfstat のすべてのオプションをリストにして表示します。
-a	パフォーマンス情報をすべて表示します。
-c	システムの設定情報を表示します。
-d	通信サービスをチェックします。
-e	パフォーマンスツールのステータスファイルから警告とエラーを検索します。
-f	パフォーマンスツールのステータスファイルをリストにして表示します。
-l	パフォーマンスツールで使用するすべてのライブラリをリストにして表示します。
-L	パフォーマンスツールで使用するすべてのライブラリファイルをリストにして表示します。詳細な情報が表示されます
-p [リモート Windows システム名]	プロセスをリストにして表示します。
-r	パフォーマンスツールのレジストリデータをリストにして表示します。

オプション	機能
-s [リモート Windows システム名]	パフォーマンスに関連したサービスのステータスを表示します。
-S [リモート Windows システム名]	パフォーマンスに関連したサービスのステータスを表示します。詳細な情報が表示されます。
-t	パフォーマンスツールのステータスファイルにある最後の数行を表示します。
-v	パフォーマンスツールのバージョン情報をリストにして表示します。
-V	パフォーマンスツールのバージョン情報をリストにして表示します。詳細な情報が表示されます。
-w	プログラムの終了でユーザーの入力を待たせます (ウィンドウは開いたままになります)。
-z	パフォーマンスのステータス、レジストリデータ、およびファイルを圧縮します。

OVIS の拡張 URL

プローブシステムから OVIS サーバーへポストできるかどうかをテストする

プローブシステムから OVIS サーバーへポストできるかどうかを確認するには、次のコマンドを実行します。

```
http://<Ovis_Server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh
```

問題がなければ、**空白のページ**が表示されます。そうでない場合は、HTTP のエラーコードが返ります。

プローブが配布されているシステムのリスト

OVIS 管理サーバーに認識されているノードの ID を確認するには、次の URL をロードします。

```
http://<Ovis_Server>/hpov_iops/isapi/
distribmgrext.dll?GetStatus
```

プローブの配布されているシステムがリストになって表示されます。対象となるプローブには、OVIS 管理サーバーに配布されているローカルプローブと他のシステムに配布されているリモートプローブが含まれています。`GetStatus` が機能しないと、配布マネージャはそのシステムに設定 (`config.dat` と関連ファイル) を送信できません。

7

高度なトピック

この章では、以下の高度なトピックについて説明します。

- Internet Services のアーキテクチャとデータフロー
- 設定を別のシステムに移動する方法
- システム名の変更
- セキュリティ
- OVIS で行うポートの設定と変更
- TIPs の通信
- ファイアウォール : ファイアウォールを経由してデータを返信
- プローブシステムとサーバーとの間の通信の設定
- カスタムレポート
- サポートしているデータベース
- データベースの調整
- データベースのバックアップ
- 初期状態に戻す方法
- TIPs データベースの復元

- スケーラビリティ情報
- NTFS セキュリティ設定

Internet Services のアーキテクチャとデータフロー

ここでは、Internet Services の各コンポーネントの基本的なデータフローについて説明します。

プローブ

プローブは、Internet Services 管理サーバー上でローカルに実行できます。または、設定情報とともに、リモートの UNIX システムや Windows システムに展開できます。リモートプローブを使用すると、さまざまな場所からサービスレベルを測定することができます。プローブは、標準的な動作を実行し、各サービスの応答時間、可用性、および他のパフォーマンスメトリックを測定します。

以下のタイプのプローブがあります。

- ANYTCP
- DHCP
- ダイヤルアップネットワーク
- DNS
- Exchange
- FTP
- HTTP
- HTTPS
- Web Transaction Recorder (HTTP_TRANS)
- 電子メール (IMAP4、POP3、Mail Round Trip、SMTP)
- ICMP (ping)
- LDAP
- NNTP (ニュースグループ)
- NTP
- ODBC

- Radius
- SAP
- Script
- SMS
- SOAP
- Streaming Media
- システム メトリック (WMI)
- TCP パフォーマンス
- TFTP
- UDP パフォーマンス
- WAP
- カスタムプローブ

プローブシステム上で OVIS のスケジューラコンポーネントが実行され、プローブがいつ実行されるかが決定されます。プローブは、それぞれ独立した実行可能プログラムであり、設定ファイルの監視対象サービス情報に基づき、スケジューラによって起動されます。

その後プローブは、測定を実施して、測定値をキューファイルに保存します。キューファイルは、プローブシステムによって HTTP または HTTPS プロトコル経由で Internet Services 管理サーバーへ送信されます。

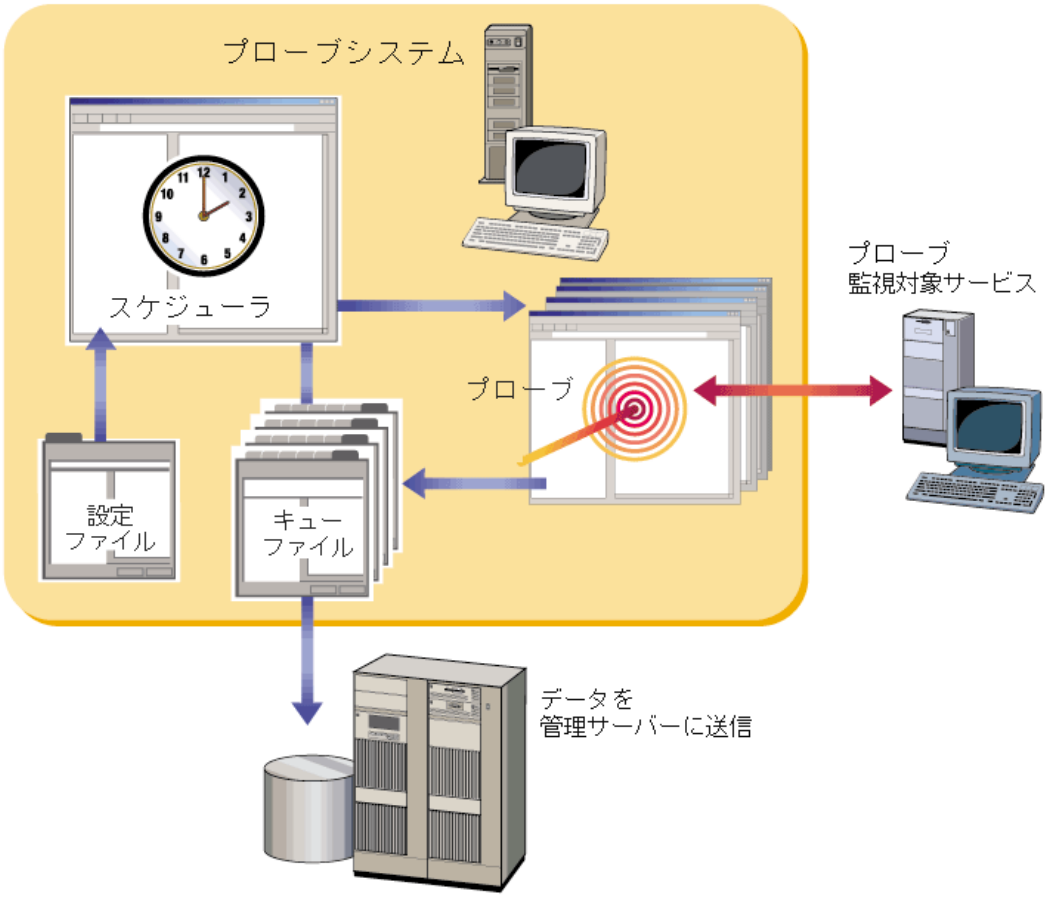


図 5　　プローブシステムのデータ図

管理サーバー

プローブは、収集したデータを Internet Services 管理サーバーに返信します。測定レシーバー measEvent2.dll は、データを測定トレーステーブル IopsTraceTable データバッファ (一時的なデータストア) に書き込みます。

Iopscollector が定期的に実行されて、データを IopsTraceTable から Reporter のデータベーステーブル IOPS_DETAIL_DATA と IOPS_PROBE_DATA_CACHE へ移動します。

続いて、iopsmaint がこれら 2 つのテーブルからデータを集計して、以下のように時間ごとの加重平均と日ごとの加重平均にまとめます。

IOPS_DETAIL_DATA: このデータベーステーブルには、プローブ / 監視対象サービスレベルのデータが 5 分単位で入っています。これらのデータが時間ごとの加重平均と日ごとの加重平均にまとめられて、次のテーブルに保存されます。

IOPS_DETAIL_DATA_HOURLY: プローブ / 監視対象サービスレベルの 1 時間ごとのデータ

IOPS_DETAIL_DATA_DAILY: プローブ / 監視対象サービスレベルの 1 日ごとのデータ

IOPS_PROBE_DATA_CACHE: サービスグループレベルのデータが 5 分単位で入っています。これらのデータが時間ごとの加重平均と日ごとの加重平均にまとめられて、次のテーブルに保存されます。

IOPS_PROBE_DATA: サービスグループレベルの 1 時間ごとのデータ

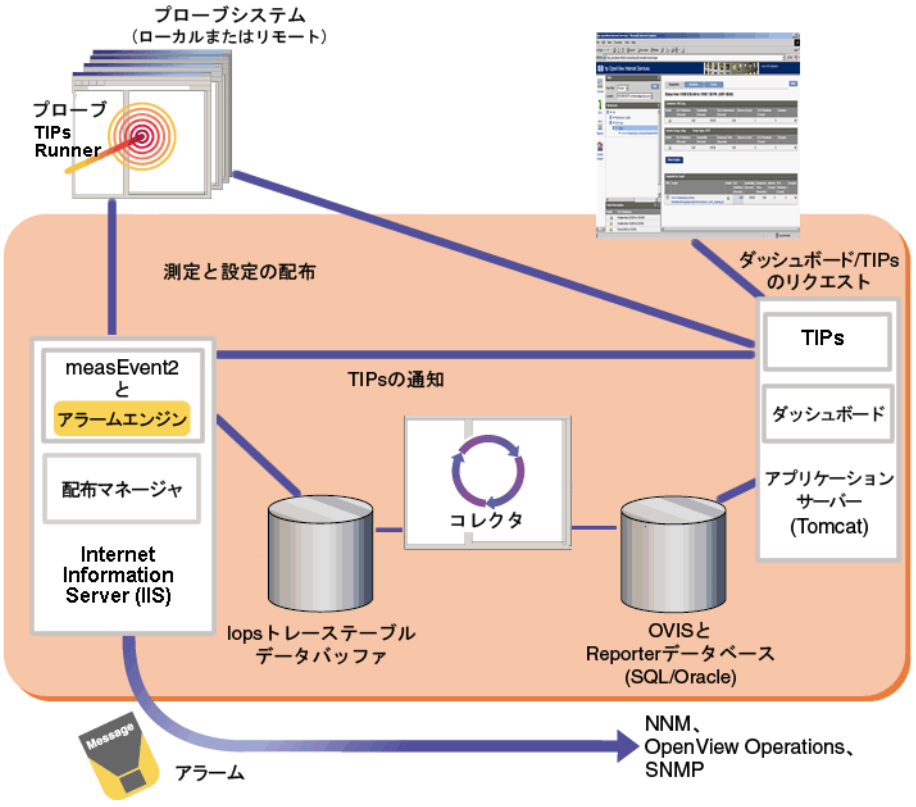
IOPS_PROBE_DATA_DAILY: サービスグループレベルの 1 日ごとのデータ

アラームとメッセージは、プローブからデータが送信されるたびに、measEvent2 内の アラームエンジンによって生成されます。アラームは、Network Node Manager、OpenView Operations for UNIX、OpenView Operations for Windows などの OpenView アプリケーション、または SNMP トラップを受信可能なイベントマネージャに送信されます。

Reporter データベースからのデータは、Internet Services ダッシュボード Web インタフェース、ほぼリアルタイムのグラフと夜間作成レポートに表示されます。ダッシュボードに表示される詳細データは、IOPS_DETAIL_DATA テーブルと IOPS_DETAIL_DATA_HOURLY テーブルから取得されます。

これらの各データテーブルのメトリックの情報については、OVIS ダッシュボードの [対象別要約] ページの [**グラフ**] ボタンを選択します。[グラフ] ページで、[**カスタム グラフ**] ボタン、[**ヘルプ**] ボタンの順に選択します。ヘルプトピックとともにデータテーブルのメトリックの説明へのリンクが表示されます。

図 6　　管理サーバーのデータ図



サービスレベル契約

サービスレベル契約 (SLA) は、サービスレベル目標値 (SLO) に基づいて設定され、その適合性を判断するために評価されます。たとえば、SLA は、監視対象サービスの応答時間が 4 秒未満でなければならないことを表します。また、可用性の SLA を設定する場合は、この SLA で監視するサービスグループを選択し、達成目標とする可用性の値 (パーセント) を SLA 適合しきい値に設定します。

SLA は、Internet Services 設定マネージャで SLO として設定します。

SLA エバリュエータは、受信した測定値と サービスレベル目標値を評価して、SLA と SLO の適合性を判断します。この適合性情報は、Reporter データベースに保存されます。

MeasEvent2 内のアラームエンジンは、測定値を受信すると、設定されている SLO に対して各データポイントを評価します。アラームエンジンは、目標値に達しなかった評価に関する情報を IOPS_SLO_VIOLATIONS_DATA テーブルに記録します。

SLA エバリュエータは 1 時間毎に実行され、SLO 情報と IOPS_PROBE_DATA テーブルからの情報を使用して、SLA の適合性を評価します。各評価における SLA 適合率と SLO 適合率は、Reporter データベースの IOPS_SLA_CONFORMANCE_DATA と IOPS_SLO_CONFORMANCE_DATA テーブルに保存されます。

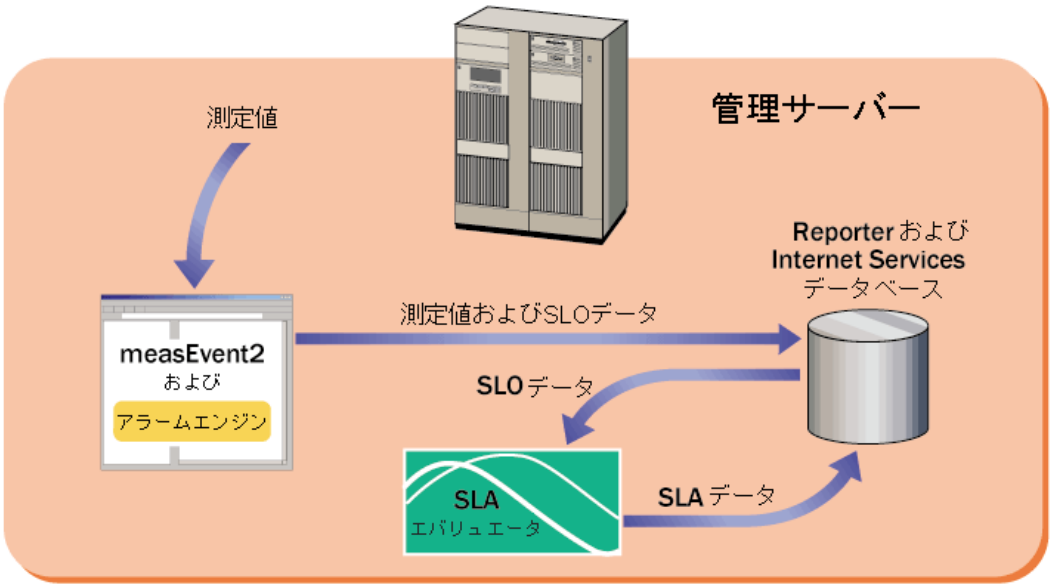


図 7　　サービスレベル契約のデータ図

TIPs コンポーネント

以下に、TIPs (Troubleshooting Insight Packages) の 5 つのコンポーネントを示します。TIPs の動作を理解するうえで役立ててください。

TIPs Server − OVIS 管理サーバー上で動作する Tomcat Web サーバーの Web アプリケーションです。OVIS でアラームが検出されたり、監視対象サービスの情報が必要な場合は、TIPs からトラブルシューティングのデータを求めるリクエストが自動的、またはオンデマンドで送信されます。このリクエストを受け取った TIPs Server では、TIPs Action Processor が専用ポートを使用して、そのリクエストを TIPs Runner へ転送します。

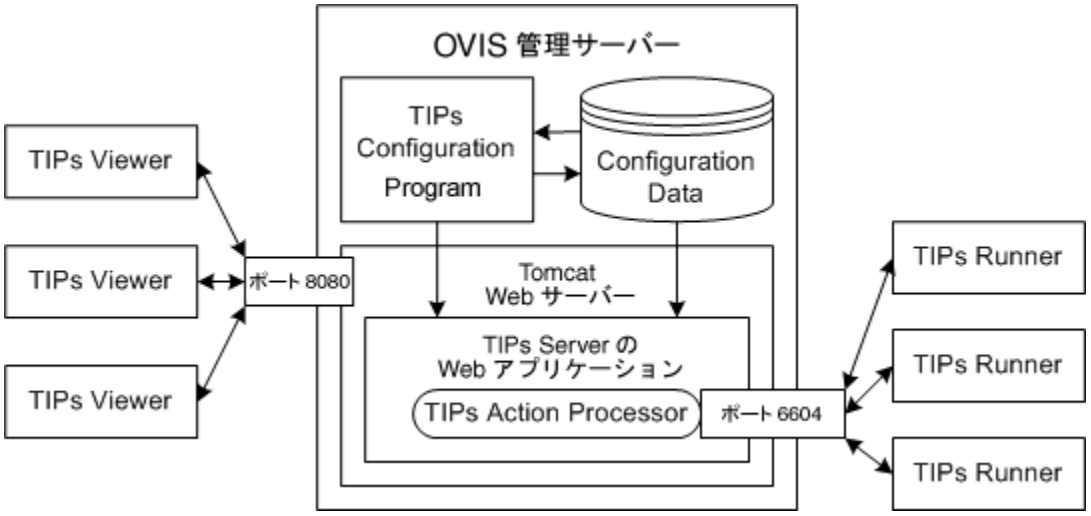
TIPs Configuration program − OVIS 管理サーバーにインストールされるコンポーネントです。管理者はこのコンポーネントを使用して、すでにある TIPs やコマンドを変更したり、新しい TIPs やコマンドを定義したりできます。

TIPs Configuration Data − サーバーシステムの TIPs データベースに保存されている設定データです。

TIPs Runner − OVIS 管理サーバー、または、プローブパッケージのインストールされている各リモートシステムに常駐し、トラブルシューティングコマンドを実行して、その結果を TIPs Server へ返します。

TIPs Viewer − Web クライアントになっていて、インターネットサービスの問題を素早く解決するためのトラブルシューティング情報を表示します。TIPs Viewer は OVIS ダッシュボードから起動します。

図 8　　TIPs のデータ図



TIP は、条件を指定してその条件が満たされるとコマンド / コマンドセットを実行するように設定することができます。その際、TIP 全体を実行するような条件を定義することも、コマンドごとにその実行条件を定義することもできます。コマンドごとに条件を割り当てて TIP を実行すると、その条件を満たすコマンドだけが実行されます。

ローカルシステムの TIPs Runner は、OVIS をインストールする時に、OVIS 管理サーバーへインストールされます。一方、リモートシステムの TIPs Runner つまりリモート TIPs Runner は、リモートプローブソフトウェアをインストールする時に、インストールと設定が行われます。監視対象サービスやアラームはプローブシステムが監視しているので、TIPs Server は、問題となっているプローブシステムの TIPs Runner にリクエストを送って、情報を入手します。

TIPs の詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

設定を別のシステムに移動する方法

設定をシステム間で移動するには、次の手順に従います。

設定のコピー元のシステムで、次の手順を実行します。

コマンドプロンプトウィンドウで以下のコマンドを入力します。

```
cd <installdir>
iopsload -save config.sysname.xml
```

設定をインポートするシステムの <install dir>¥probes ディレクトリに、config.sysname.xml と <datadir>¥datafiles¥probe¥policies¥httptrans.dat ファイルを転送します。コピー先のシステム上で、次の手順を実行します。

コマンドプロンプトウィンドウで以下のコマンドを入力します。

```
ovc -stop ovprobes
```

注記：関連付けられているサブサービスの停止が通知されることがあります。後で開始する場合のために、これらの名前を書きとめておきます。

注記 : Reporter Service が整理統合を実行できるように、5 分間待機します。

```
net stop "Reporter Service"
iopsload -load config.sysname.xml
```

警告 : 転送した設定内容にリモートプローブシステムが含まれる場合は、以降の手順を実行する前に、それらのすべてのシステムで HP Internet Services (Windows プローブの場合) またはスケジューラ (Unix プローブの場合) を停止する必要があります。

```
net start "Reporter Service"
net start "World Wide Web Publishing Service"
```

上記のコマンドにより、IIS Admin Services が起動します。前述の手順で停止した IIS Admin Services の他のサブサービスを開始することもできます。

設定マネージャで、設定した顧客とサービスが正常に転送されたことを確認します。転送されている場合は、[**プローブ設定の保存**] (ディスク) アイコンをクリックして、これらの監視対象サービスの測定を開始します。

設定内容にリモートプローブが含まれている場合は、このシステムから config.dat と httptrans.dat ファイルを再設置する必要があります。これは、データ送信先のシステム名が変わったためです。

システム名の変更

OVIS は管理サーバーのホスト名または IP アドレスの変更をサポートしていません。

OVIS 管理サーバーのシステム名または IP アドレスを変更する必要がある場合は、OVIS 管理サーバーを他のシステムにインストールし、各リモートプローブシステム上で `ovisactivate` を実行して新しい管理サーバーの場所を指すように変更することをお勧めします。

リモートプローブシステムを、別の OVIS 管理サーバーにデータを送信するように変更する場合は、`ovisactivate` を実行し、ダイアログで新しいホスト名を入力します。

プローブシステムのシステム名を変更する場合は、設定マネージャでそのプローブロケーションを更新し、設定を保存する必要があります。更新した設定はプローブによってダウンロードされます。

セキュリティ

プロキシおよびポートの設定

Internet Services には、プロキシやポートを使用可能な部分がいくつかあります。

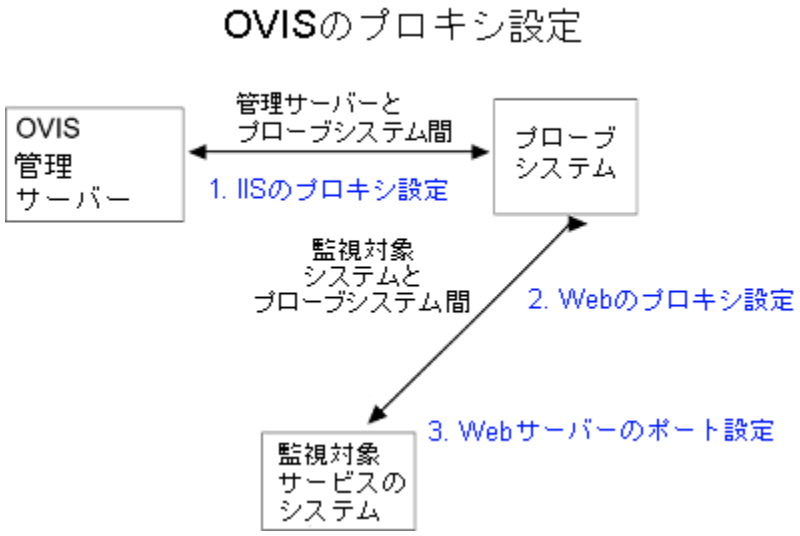
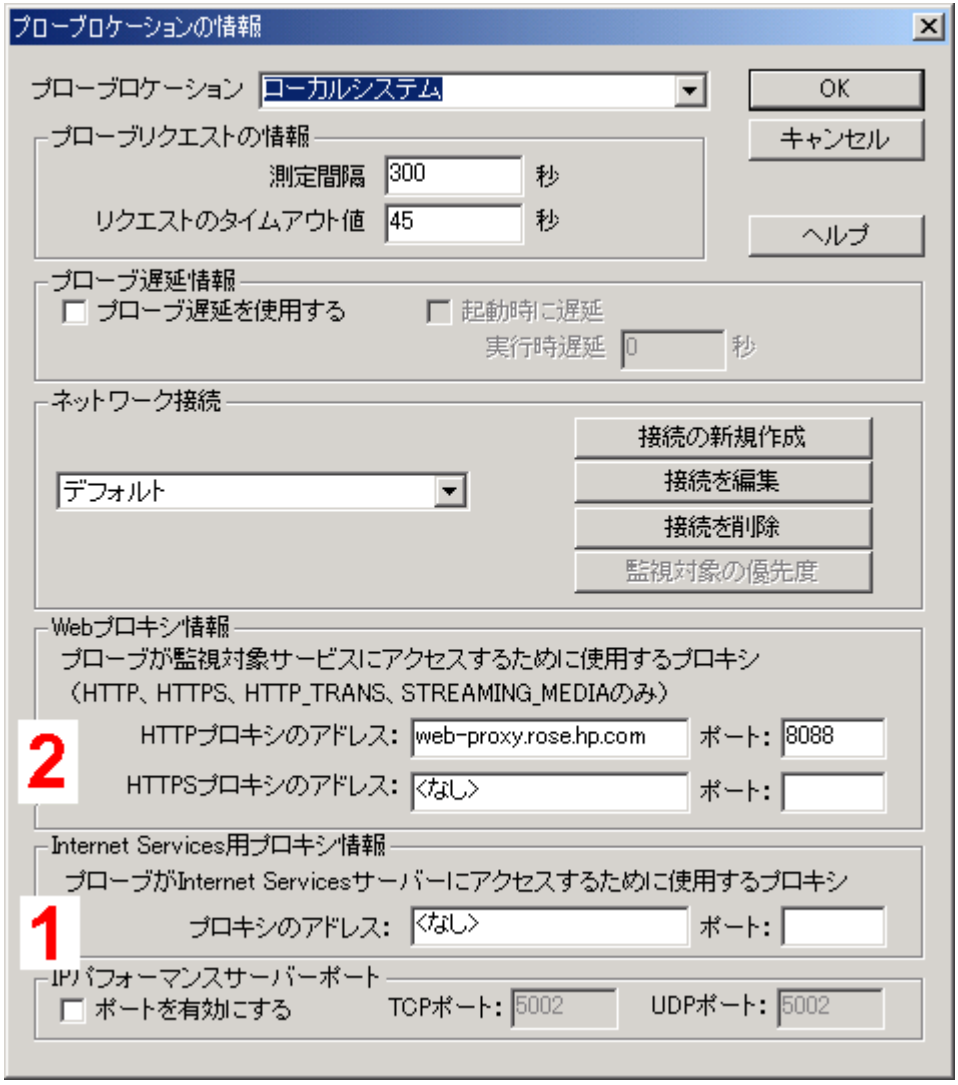


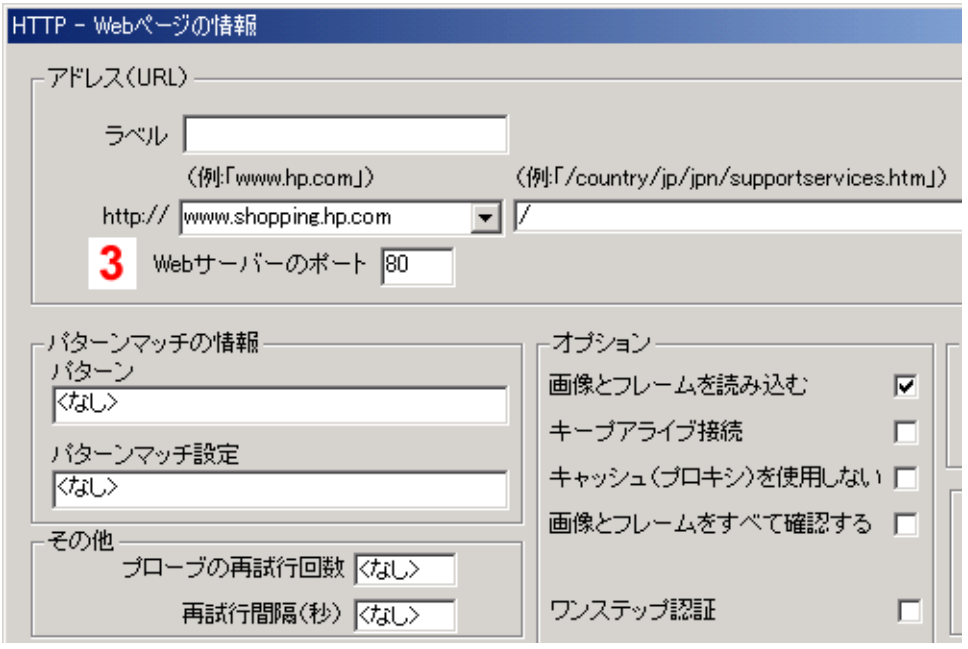
図 9　　Internet Services でのプロキシとポートの設定

上記の図は次のことを示しています。

1. OVIS 管理サーバーとリモートプローブ間にプロキシサーバーを設定することができます。この場合、[プローブロケーションの情報] ダイアログの [Internet Services 用プロキシ情報] を変更して、リモートプローブシステムが OVIS 管理サーバーとの間でデータを送受信できるようにします。
2. プローブ (ローカルまたはリモート) システムと監視対象サービスシステム間にプロキシサーバーを設定することができます。HTTP、HTTPS、または HTTP_TRANS プローブを使用している場合は、[プローブロケーションの情報] ダイアログの [Web プロキシ情報] のプロキシとポートの設定を、システム間でデータを転送できるように正しい値に変更する必要があります。


プローブロケーションの情報
プローブロケーション
ローカルシステム
OK
キャンセル
プローブリクエストの情報
測定間隔
300
秒
リクエストのタイムアウト値
45
秒
ヘルプ
プローブ遅延情報
プローブ遅延を使用する
起動時に遅延
実行時遅延
0
秒
ネットワーク接続
デフォルト
接続の新規作成
接続を編集
接続を削除
監視対象の優先度
Webプロキシ情報
プローブが監視対象サービスにアクセスするために使用するプロキシ
（HTTP、HTTPS、HTTP_TRANS、STREAMING_MEDIAのみ）
2
HTTPプロキシのアドレス:
web-proxy.rose.hp.com
ポート:
8088
HTTPSプロキシのアドレス:
<なし>
ポート:
Internet Services用プロキシ情報
プローブがInternet Servicesサーバーにアクセスするために使用するプロキシ
1
プロキシのアドレス:
<なし>
ポート:
IPパフォーマンスサーバーポート
ポートを有効にする
TCPポート:
5002
UDPポート:
5002

3 HTTP プローブの監視対象サービスシステムに使うポートを指定できます。このポートにはデフォルトポート (80) 以外のポートが設定することができます。その場合は、設定マネージャの [HTTP - Web ページの情報] ダイアログで指定します。



Internet Services のセキュリティ処理方法

MS インターネットインフォメーションサービス (IIS) とともに使用する場合、OVIS はデータを測定し、取得した値をデータベースに保存します。OVIS がこの方法で IIS と動作するためには、OVIS DLL に適切なパーミッションが設定されている必要があります。Internet Services は、NTFS と IIS の両方のセキュリティ設定を使用して、データの取得や保存を許可するとともに、データへの不正アクセスを防止します。Windows 管理者は、セキュリティ設定を調整してセキュリティレベルを下げることができます。セキュリティレベルを下げたり、追加機能への匿名アクセスを許可すると、ユーザーが重要なデータにアクセスできるようになるため注意する必要があります。IIS のセキュリティは、NTFS (NT ファイルシステム) レベルと IIS レベルの 2 つのレベルに対応しています。FAT (File Allocation Table) ファイルシステムはサポートされていません。これは、特定のパーミッションを設定することができないためです。また、IIS での NTFS パーミッションの変更を反映するには、IIS を停止して再起動する必要があります。

OVIS で行うポートの設定と変更

OVIS 管理サーバー には、TCP ポートでリスンするコンポーネントがいくつかあります。ファイアウォールを使用する場合は、これらのポートを通信のために開く必要があります。

- Microsoft インターネットインフォメーションサービス (IIS) ポート : サーバーの通信をプローブしたり、他の OpenView 製品との統合処理を行うためのポートです。
  - デフォルトのポート番号 : 80 (SSL を有効にした場合は 443)
- Tomcat ポート : OVIS ダッシュボードの処理と、TIPs Server と TIPs Viewer 間の通信処理を行うためのポートです。
  - デフォルトのポート番号 : 8005 (シャットダウン)、8009 (JK2) 、および 8080 (HTTP)
- TIPs ポート : TIPs Server・TIPs Runner 間の通信を処理するためのポートです。
  - デフォルトのポート番号 : 6604

OVIS をインストールするときに、Tomcat 用のデフォルトポートがすでに他の用途で使われていると、Tomcat 用の新しいポートを入力するように求められます。その場合は `netstat -an` を使って、使用されているポートを調べてください。

IIS ポートと Tomcat ポートの変更

既存の設定ですでにリモートプローブが展開配備されているときにポート番号を変更する場合は、特に注意する必要があります。その場合は、実際に存在するポート番号か、または OVIS 管理サーバー用に使用できるポート番号だけを選ぶ必要があります。サーバーのポートを OVIS サーバーと通信できないポートに変更すると、リモートプローブシステムが OVIS 管理サーバーと通信できなくなったり、測定データを送れなくなったりします。

IIS ポートの変更

IIS ポートは、Microsoft インターネットインフォメーションサービス (IIS) 管理ユーティリティ ([**コントロールパネル**] > [**管理ツール**] > [**インターネットインフォメーションサービス**]) を使って変更できます。IIS ポートを変更した場合は、この変更を設定マネージャにも反映させる必要があります。478 ページの「IIS ポートの変更例」を参照してください。

Tomcat ポートの変更

同じシステムに OVIS 管理サーバーと他の OpenView 製品 (NNM、OVPM、Reporter など) を共存させると、ポートが競合する可能性があります。この問題を解決するために、Tomcat (Dashboard) ポートは変更できるようになっています。インストールした後、`OvTomcatCtl.vbs` スクリプトを使って Tomcat ポートを変更します (以下に示すポートはその例です)。

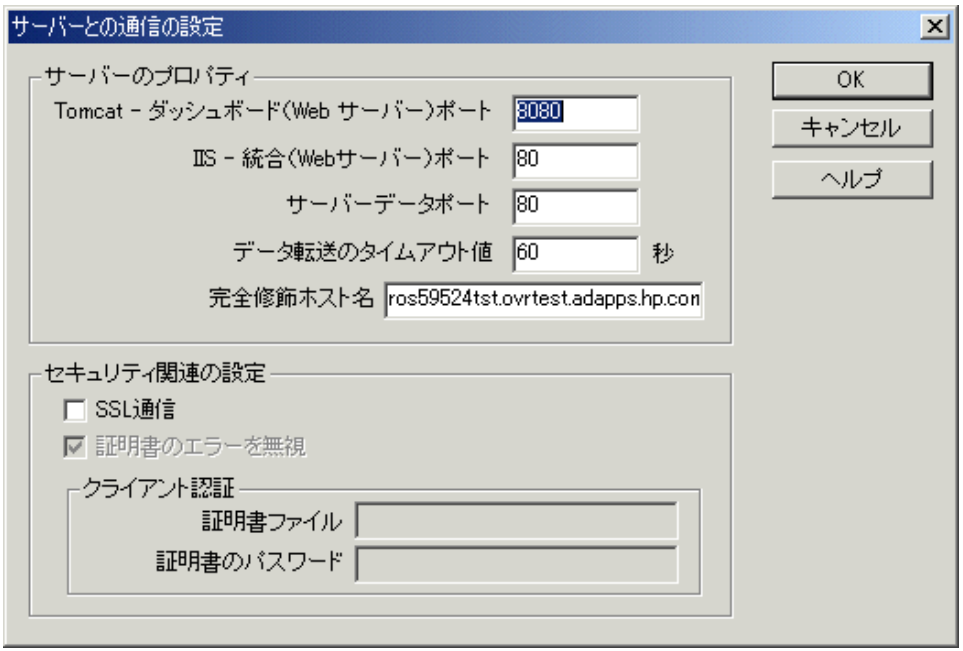
```
cd <installdir>¥bin
ovc -stop ovtomcatA
cscript /nologo OvTomcatCtl.vbs -setshutdownport 9005
cscript /nologo OvTomcatCtl.vbs -sethttpport 9080
cscript /nologo OvTomcatCtl.vbs -setjk2port 9007
ovc -start ovtomcatA
```

Tomcat に現在設定されているポートを調べるには、以下のスクリプトを実行します。

```
cscript /nologo OvTomcatCtl.vbs -getconf
```

設定マネージャで行う IIS ポートと Tomcat ポートの設定変更

IIS ポートまたは Tomcat ポートを変更したら、その一部のポートを OVIS 設定マネージャで再設定する必要があります ([**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**])。



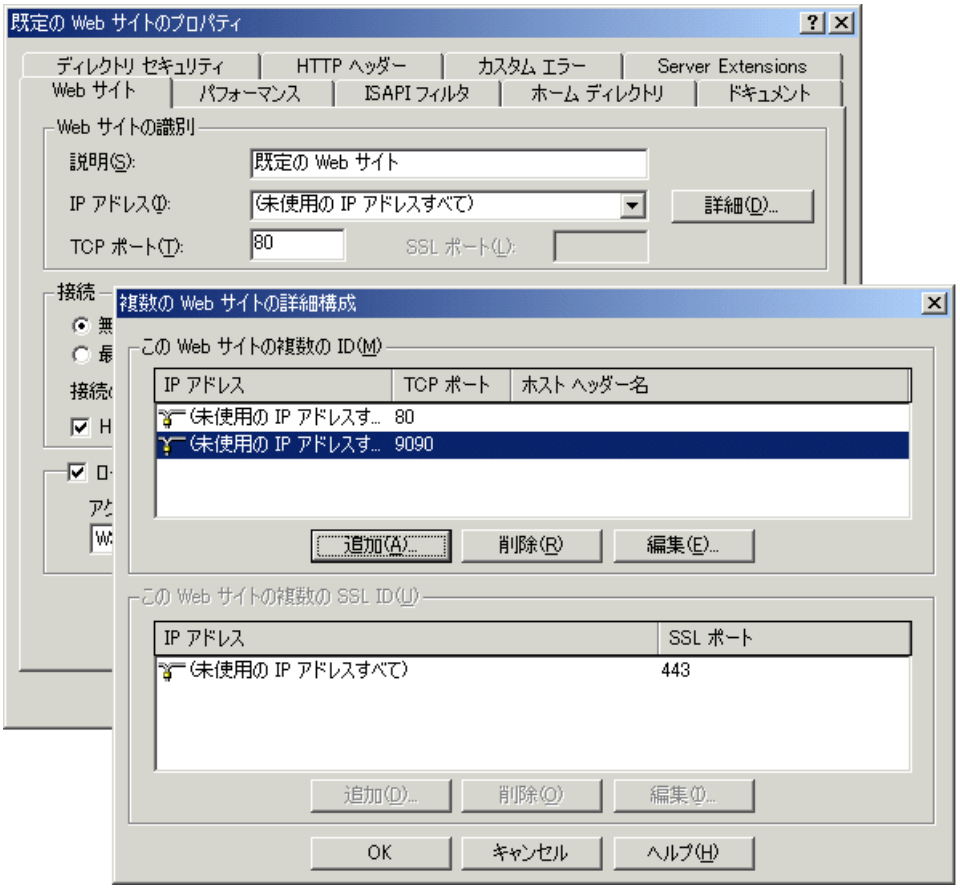
[Tomcat - ダッシュボード (Web サーバー) ポート] の値は、Tomcat の HTTP ポートと同じ番号にする必要があります。

[IIS - 統合 (Web サーバー) ポート] と [サーバーデータポート] は、IIS の動作するポートと同じ番号にする必要があります。

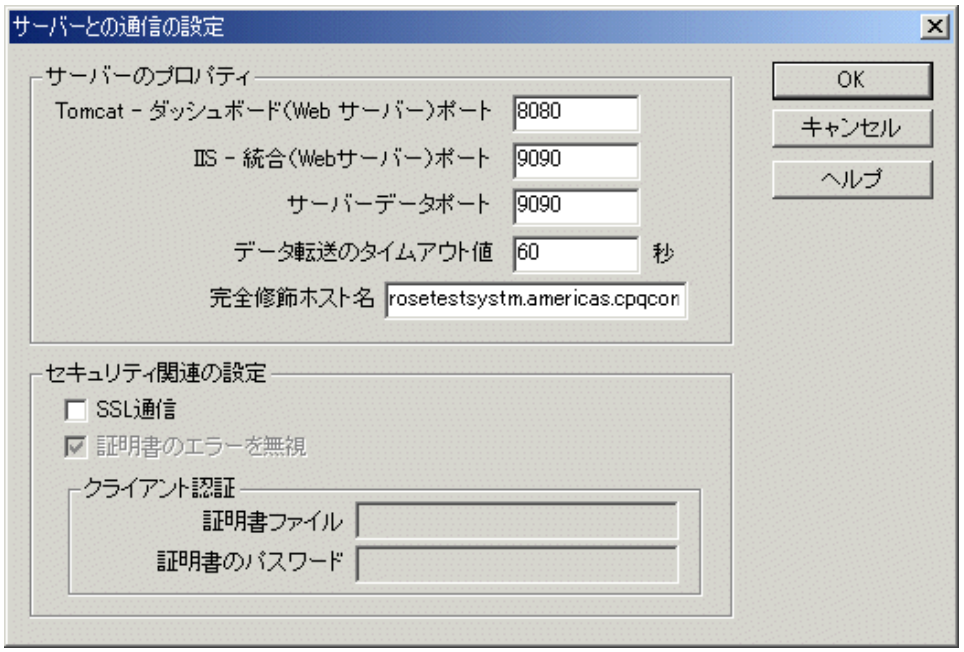
IIS ポートの変更例

以下の例で、IIS ポートの変更手順を示します (手順の実行順序が非常に重要なので注意してください)。

1 IIS を使って [既定の Web サイトのプロパティ] ダイアログに移動し、[**詳細**] ボタンをクリックします。現在のデフォルトポートを使う代わりに、新しいサーバーポートを追加します。**古い / 既存のデフォルトポートは決して削除しないでください** (以下の例では、ポート 80 とポート 9090 が設定されています)。変更を保存します。



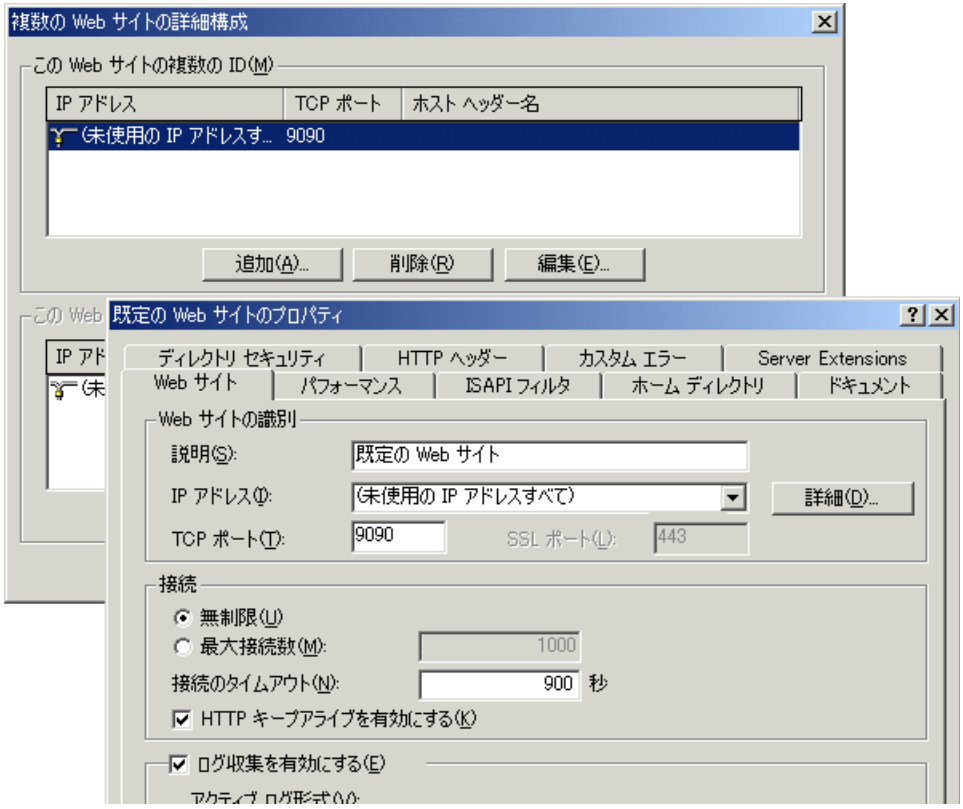
2 OVIS 設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログボックスを使って、サーバーデータポートを変更します。[**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログの詳細については、オンラインヘルプを参照してください。



3 変更した設定を保存して、それがローカルとリモートのプローブシステムへ展開配備されるのを待ちます。設定マネージャの [ステータス] の表示で、すべてのプローブシステムがアップデートを受け取ったことを確認します (すべてのシステムが緑色になります)。

4 次に、すべてのリモートプローブシステムが新しいポート番号を使用するように設定されたことを確認します。

5 OVIS 管理サーバーで IIS の [既定の Web サイトのプロパティ] ダイアログボックスに戻って、[**詳細**] ボタンをクリックします。使用しない古いポートは、削除します。[**OK**] ボタンをクリックします。次に、[既定の Web サイトのプロパティ] ダイアログボックスで、追加した新しいポートに TCP ポートを設定します。変更を保存します。IIS で変更したら、サービスを再起動する必要があります。


複数の Web サイトの詳細構成
この Web サイトの複数の ID(M)
IP アドレス
TCP ポート
ホスト ヘッダー名
(未使用の IP アドレスす...
9090
追加(A)...
削除(R)
編集(E)...
既定の Web サイトのプロパティ
ディレクトリ セキュリティ
HTTP ヘッダー
カスタム エラー
Server Extensions
Web サイト
パフォーマンス
ISAPI フィルタ
ホーム ディレクトリ
ドキュメント
Web サイトの識別
説明(S):
既定の Web サイト
IP アドレス(I):
(未使用の IP アドレスすべて)
詳細(D)...
TCP ポート(T):
9090
SSL ポート(L):
443
接続
無制限(U)
最大接続数(M):
1000
接続のタイムアウト(N):
900
秒
HTTP キープアライブを有効にする(K)
ログ収集を有効にする(E)

TIPs ポートの変更

IIS ポートと OVIS の Tomcat ポートに加えて、TIPs Server や TIPs Runner の通信ポート番号も変更できます。デフォルトのポートは 6604 です。

詳細については、TIPs Configuration program のオンラインヘルプを参照してください。

現在設定されているデフォルトの TIPs Runner ポートを表示するには、TIPs Runner システムのコマンドウィンドウで、次のコマンドを実行します。

```
Windows: <install_dir>¥bin¥ovtiprn -retrieve port

UNIX: /opt/OV/bin/ovtiprn -retrieve port
```

TIPs Server システムのポート番号を変更する場合は、その TIPs Server に登録されているすべての TIPs Runner システムについてポート番号を変更する必要があります。

TIPs Server とローカル TIPs Runner のポート番号を変更するには、以下の手順を実行します。

1. TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Server を停止させます。

   ```
   <install_dir>¥bin¥ovc -stop ovtomcatA
   ```

2. TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner を停止させます。

   ```
   <install_dir>¥bin¥ovc -stop ovtiprn
   ```

3. TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Server のポート番号を変更します。

   ```
   <install_dir>¥bin¥OvTIPsServer.bat -port <port number>
   ```

4. TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner のポート番号を変更します。

   ```
   <install_dir>¥bin¥ovtiprn -replace <host name> <port
   number>
   ```

   このコマンドの <*host name*> には、TIPs Runner がインストールされている TIPs Server システムの名前を指定します。

5 TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Server を起動します。

```
<install_dir>¥bin¥ovc -start ovtomcatA
```

6 TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner を起動します。

```
<install_dir>¥bin¥ovc -start ovtiprn
```

リモート TIPs Runner のポート番号を変更するには、以下の手順を実行します。

1 **各**リモート TIPs Runner システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner を停止させます。

Windows の場合

```
<install_dir>¥bin¥ovc -stop ovtiprn
```

UNIX の場合

```
/opt/OV/bin/ovc -stop ovtiprn
```

2 **各**リモート TIPs Runner システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner のポート番号を変更します。

Windows の場合

```
<install_dir>¥bin¥ovtiprn -replace <host name> <port number>
```

UNIX の場合

```
/opt/OV/bin/ovtiprn -replace <host name> <port number>
```

このコマンドの *<host name>* には、TIPs Runner が登録されている TIPs Server システムの名前を指定します。

3 **各**リモート TIPs Runner システムのコマンドウィンドウで次のコマンドを実行し、TIPs Runner を起動します。

Windows の場合

```
<install_dir>¥bin¥ovc -start ovtiprn
```

UNIX の場合

```
/opt/OV/bin/ovc -start ovtiprn
```

TIPs の通信

TIPs Server は複数の TIPs Runner および TIPs Viewer と通信します。

- TIPs Server と TIPs Runner との間の通信は、トラブルシューティングの情報を収集する目的で使用します。
- TIPs Server と TIPs Viewer との間の通信は、リクエストのあったトラブルシューティング情報を表示する目的で使用します。

TIPs Runner

ローカル TIPs Runner は、OVIS をインストールすると、OVIS のローカルプローブとともに自動的にインストールされます。またこのインストール中に設定値が自動的に適用されます。

リモート TIPs Runner は、各リモート OVIS プローブとともに、OVIS リモートプローブインストールパッケージを使用してインストールします。このとき、リモート TIPs Runner と OVIS プローブは一緒に設定されます。

TIPs Runner のパラメータは変更できます。TIPs Runner の設定方法については、TIPs Configuration program のオンラインヘルプを参照してください。

セキュリティ保護された TIPs 通信

TIPs Server は、ローカルプローブシステム、リモートプローブシステム、および TIPs Runner と通信します。この通信は、特に指定しない限り、標準的な HTTP プロトコルを使って行われます。しかしこの TIPs の通信は、SSL 証明書ベースの通信を使用することで、セキュリティの保護レベルを高めることができます。

通信をセキュリティ保護する場合は、TIPs Server とその通信相手の TIPs Runner をすべて、セキュアモードで動作させる必要があります。

TIPs Server と TIPs Runner の間でセキュリティ保護された通信を有効化する方法については、TIPs Configuration program のオンラインヘルプを参照してください。

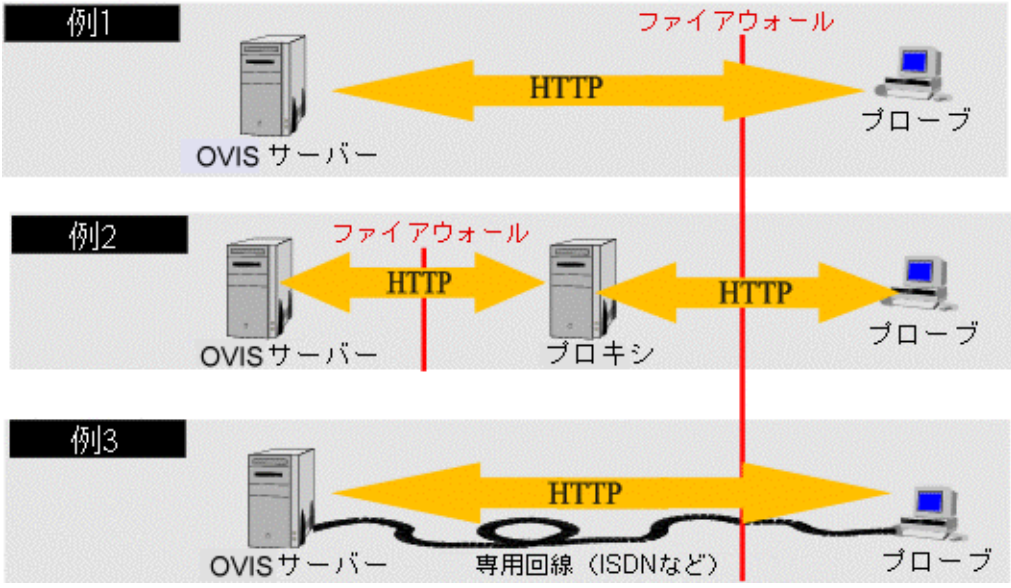
ファイアウォール：ファイアウォールを経由してデータを返信

Internet Services プローブは、標準の HTTP プロトコルを使用して測定情報を OVIS 管理サーバーに送信します。デフォルトでは、プローブは、OVIS 管理サーバー上でポート 80 を使用して HTTP POST 要求を送信します。管理サーバーの URL は以下のとおりです。

http://<management server>/HPOV_IOPS/isapi/measEvent2.dll

ファイアウォール経由でのプローブの通信方法

Internet Services プローブは、HTTP POST を使用して Internet Services 管理サーバーにデータを返します。サーバーの周囲にファイアウォールが存在する場合は、プローブが収集したデータを返すための開いているポートがなければなりません。以下の例は、プローブがファイアウォールを経由して Internet Services サーバーにデータを返す場合の、3 種類の一般的な設定を示しています。



例 1 では、Internet Services 管理サーバーは、ファイアウォールの内側に設置されています。この設定では、プローブはポート 80 (このポートは設定可能) で管理サーバーと通信する必要があります。管理サーバーのポート 80 を送信先としてプローブシステムから送信された TCP パケットを除く、あらゆるデータをブロックするようにファイアウォールを設定することをお勧めします。

例 2 では、ファイアウォールの内側の管理サーバーにプローブデータをリレーするために、プロキシサーバーが使用されます。これは、単純なプロキシサーバーを設定するだけ済む、効果的なセキュリティ設定です。プロキシは単純な HTTP 転送プロセスを実行するため、障害が起きたプロキシサーバーが他の ISP に影響を与えることはありません。

例 3 では、プローブは ISDN などの専用回線を使用して、OVIS 管理サーバーに測定値を送信します。専用回線はインターネットからの攻撃を受けにくいため、この設定では IP パケットの詐称 (スプーフィング) はより困難になります。

プローブシステムの保護方法

プローブシステムがファイアウォールの外部、または保護されていないサイトにある場合は、インターネットからの攻撃に対して保護する必要があります。プローブシステムは、基本的に次の 2 種類の方法で Internet Services サーバーに測定値を返します。

- インターネット経由 (例 1 と 2)
- イントラネットへの専用回線経由 (インターネットとイントラネット間の経路はありません)

最初の 2 つの例では、パケットが途中で傍受されて変更されるなど、返信データが攻撃されることがあります。ただし、重要な情報は転送されないため、このような攻撃はそれほど危険ではありません。例 3 では、プローブシステムから Internet Services サーバーへのメッセージ送信に、ISDN などの専用回線が使用されます。イントラネットへの個別の回線が存在するため、IP パケットの詐称 (スプーフィング) は困難になります。ただし、イントラネットへの回線が専用回線であるため、ファイアウォール外部に対するセキュリティ対策が損なわれることもあります。

どの場合も、ファイアウォール製品でプローブシステムを保護することをお勧めします。また、プローブシステム上でシステムポート (ポート 1024 未満) を開いた状態にしておかないことをお勧めします。これにより、HTTP や FTP などの標準サービスに対する攻撃を排除できます。

例 3 では、外部のファイアウォールは、プローブシステムから送信され、専用回線 (ポート 1024 以上) 経由で Internet Services 管理サーバーに入ってくるパケットのみを許可する必要があります。

プローブシステムとサーバーとの間の通信の設定

OVIS 管理サーバーとリモートプローブシステムとの間では データの受け渡しが必要です。データフローについては、459 ページの「Internet Services のアーキテクチャとデータフロー」を参照してください。

データ通信の設定を行うには、OVIS 設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] を選択して表示されるダイアログを使用します。OVIS 管理サーバーの完全修飾ホスト名を指定し、データ転送のタイムアウト時間を定義します。さらに、OVIS ダッシュボードを表示する Web サーバー用のポート番号、OpenView の統合 Web サーバー用ポート番号、および OVIS 管理サーバー用のポート番号を指定します。

また、プローブシステムと OVIS 管理サーバー間で、SSL でセキュリティ保護された通信を設定することもできます。これは、すべてのリモートプローブに作用します。

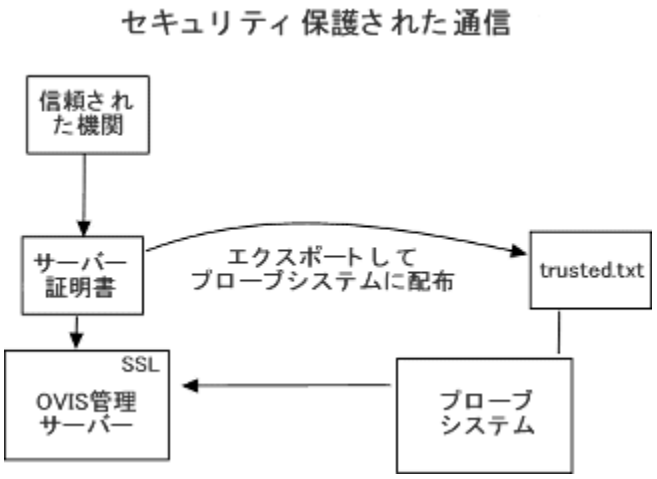
TIPs Server は、ローカルプローブシステム、リモートプローブシステム、および TIPs Runner と通信します。この通信は特に指定しない限り、標準的な HTTP プロトコルを使って行われます。しかしこの TIPs の通信は、SSL 証明書ベースの通信を使用することで、セキュリティの保護レベルを高めることができます。

通信をセキュリティ保護する場合は、TIPs Server とその通信相手の TIPs Runner をすべて、セキュアモードで動作させる必要があります。

TIPs でセキュリティ保護された通信を有効化する方法 (次の項の OVIS 用のプロセスとは異なります) については、TIPs Configuration program のオンラインヘルプを参照してください。

セキュリティ保護された通信の設定

OVIS は、プローブシステムとサーバー間の、SSL でセキュリティ保護された通信をサポートしています。セキュリティ保護された基本的な通信を使用するための条件は、プローブシステム上の trusted.txt ファイルにサーバー証明書がエクスポートされていることのみです。セキュリティを強化するには、プローブシステムのクライアント証明書をインストールします。



サーバー証明書

サーバー証明書をエクスポートするには、以下の手順に従います。trusted.txt ファイルの証明書の形式は、**Base64 encoded X.509** でなければなりません。

セキュリティ保護された Web サーバーを設定した場合は、すべてのプローブシステムでセキュリティ保護された通信を使用する必要があります。

1 各プローブシステム (ローカルおよびリモート) ですべてのプローブを停止します。

```
ovc -stop ovprobes
```

2 OVIS 管理サーバーをセキュリティ保護された Web サーバーとして設定します (Microsoft インターネットインフォメーションサービス (IIS) 製品のオンラインヘルプを参照してください)。

セキュリティ保護された通信を有効にするには、OVIS 管理サーバーシステム上で IIS サーバーのサーバー証明書を作成します。

a インターネットサービスマネージャ (IIS) プログラムを実行します。左側のツリーペインで [既定の Web サイト] を右クリックして [プロパティ] を選択します。

b [ディレクトリセキュリティ] タブを選択して [**サーバー証明書**] ボタンをクリックします。

c ウィザードに従ってキーまたは証明書を作成します。証明書要求を認証機関に転送します。信頼された機関から証明書を受け取るまでには数日かかる場合もあります。

d 信頼された機関から証明書を受け取ったら、前述のウィザードを使用して証明書を処理 (またはインポート) します ([保留中の要求を処理し、証明書をインストールする] を選択します)。

3 証明書の処理が完了したら、次の手順に従って、2 つの OVIS dll でセキュリティ保護された通信を設定できます。

a インターネットサービスマネージャ (IIS) プログラムを実行して、[既定の Web サイト] の左側のツリーペインで `HPOV_IOPS/isapi` に移動します。

b [`measEvent2.dll`] を右クリックして [**プロパティ**] を選択します。

c [ファイルセキュリティ] に進み、[セキュリティで保護された通信] グループボックスの [**編集**] ボタンをクリックします。

d [**このリソースにアクセスする時に、セキュリティで保護されたチャネルを必要とする**] をクリックします。[**OK**] をクリックしてインターネットサービスマネージャ (IIS) を終了します。

`DistribMgrExt.dll` に対して手順 3b、3c、3d を繰り返します。

4 ブラウザで `measEvent2.dll` へのセキュリティ保護されたアクセスをテストします。

認証エラーを防止するため、サーバー証明書と CA 証明書をブラウザにインポートします。

以下の URL にアクセスした場合、Internet Explorer にセキュリティ警告は表示されないはずです。

https://<ovis_server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh

上記 URL にアクセスすると、Internet Explorer に空のページが表示されます。

5 Internet Explorer を使用して、サーバー証明書と CA 証明書を Base64 encoded X.509 形式でエクスポートします。

a OVIS 管理サーバー上の Internet Explorer で、[**ツール**] > [**インターネットオプション**] > [**コンテンツ**] > [**証明書**] を選択します。

b OVIS 管理サーバーのサーバー証明書を選択し、Base64 encoded X.509 形式でエクスポートします。

c CA 証明書についても同じ操作を実行します。

d エクスポートした 2 つの証明書を、`<datadir>¥conf¥probe` ディレクトリにある **trusted.txt** ファイルに追加します (ファイルがない場合は作成します)。

6 OVIS 設定マネージャで [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログのチェックボックスをオンにして SSL 通信を有効にし、設定の変更を**保存**します。

7 各リモートプローブシステムに **trusted.txt** ファイルを配布します。他の設定ファイルはリモートプローブシステムに自動的に配布されます。

8 各プローブシステム (ローカルおよびリモート) で OVIS のサービスを再起動します。

```
ovc -start ovprobes
```

9 OVIS 設定マネージャの [**ステータス**] ビューで、プローブの測定値が受信されたこと確認します。

クライアント証明書

各プローブシステムにクライアント証明書をインストールすることによってセキュリティをさらに強化することができます。クライアント証明書は、Base64 encoded X.509 形式で、プライベートキーを含んでいる必要があります。クライアント証明書の作成は、使用している証明書サーバーまたは認証機関によって異なります。

1 各プローブシステム (ローカルおよびリモート) ですべてのプローブを停止します。

```
ovc -stop ovprobes
```

2 クライアント証明書を作成し、Base64 encoded X.509 形式であることを確認します。また、<datadir>¥conf¥probe ディレクトリに **clientcert** という名前でインストールされていることを確認します。各プローブシステムは、同じ証明書ファイル名とパスワードを共有します。証明書は異なっていてもかまいません。

3 クライアント証明書は、OVIS 設定マネージャによって要求されます。設定マネージャを使用しているすべてのユーザーの証明書にクライアント証明書を追加します。これを行うには、Internet Explorer でクライアント証明書を読み込みます。

4 証明書を正しい場所 (<datadir>¥conf¥probe¥clientcert) に読み込んだら、インターネットサービスマネージャ (IIS) のクライアント証明書の確認を有効にします。

   a [既定の Web サイト] の左側のツリーペインで [HPOV_IOPS/isapi] に移動します。

   b [measEvent2.dll] を右クリックして、[**プロパティ**] を選択します。

   c [ファイル セキュリティ] に進み、[セキュリティ保護された通信] グループボックスの [**編集**] ボタンをクリックします。

   d [**クライアント証明書を要求**] をクリックします。[**OK**] をクリックしてインターネットサービスマネージャを終了します。

   DistribMgrExt.dll について手順 4b、4c、4d を繰り返します。

5 Internet Explorer でクライアント証明書をインポートして、以下の URL にアクセスします。

   https://<ovis_server>/HPOV_IOPS/isapi/measEvent2.dll?Refresh

   選択ボックスにインポートした証明書とクライアント証明書名が表示され、URL へのアクセスが許可されます (空のページが表示され、エラーは表示されません)。

6 OVIS 設定マネージャの [**ファイル**] > [**設定**] > [**Web サーバーのプロパティ**] ダイアログで証明書ファイルの名前を入力し、**clientcert** ファイルを保護するためのパスワードを設定して、設定の変更を**保存**します。各リモートプローブシステムに **clientcert** ファイルを配布します。

7 各プローブシステム (ローカルおよびリモート) で OVIS のサービスを再起動します。

   ```
   ovc -start ovprobes
   ```

8 OVIS 設定マネージャの [**ステータス**] ビューで、プローブの測定値が受信されたことを確認します。

403.7 アクセスは許可されていません : クライアント証明書が必要です。

Internet Explorer でクライアント証明書をテストしたときにこのエラーが表示された場合は、ブラウザにクライアント証明書が存在することを確認してください。

空の選択ボックスが表示された場合は、クライアント証明書を署名したルート CA 証明書が、サーバーにインストールされていない可能性があります。ルート CA 証明書をインストールするには、Web サーバーシステムで Internet Explorer を実行します。インストールウィザードの 2 番目の手順で、[**証明書をすべて次のストアに配置する**] ラジオボタンを選択して、[**参照**] をクリックします。証明書ストアが表示されたウィンドウが開きます。[**物理ストアを表示する**] チェックボックスをクリックして、[**信頼されたルート証明機関**] を選択します。[ローカルコンピュータ] ノードを選択し、インストールを続行します。

Microsoft Support Database の Q218445 も参照してください。

証明書のエクスポート

Microsoft Certificate Server 1.x では、エクスポートしたクライアント証明書に含まれている秘密キーを取得する方法はありません。このため、キーを Internet Explorer にインポートした後、Internet Explorer から PKCS #12 形式でエクスポートします ([秘密キーのエクスポート] で [はい、秘密キーをエクスポートします] を必ずクリックしてください)。

その後、`openssl` ツール (`www.openssl.org`) を使用して、以下に説明するように PKCS #12 形式を Base64 encoded X.509 形式へ変換します。

1 コマンドプロンプトから、`openssl.exe pkcs12 -in <filename.pfx> -out <somename.txt>` コマンドを実行します。

2 次に、**インポートパスワード**を入力します。これは証明書に添付するパスワードです。

3 次に、**PEM パスフレーズ**を入力して確認します。このパスワードは自由に設定できます。ただし、HTTPS プローブと SSL サーバーの通信を設定するときに必要となるので、思い出せるものにしておく必要があります。

4 PEM パスワードを確認すると、手順 1 の openssl コマンドで名前を指定したテキストファイルが作成されます。作成されていることを確認したら、その .txt ファイルを <data dir>¥conf¥probe ディレクトリへコピーします。この場所にコピーしておかないと、プローブは正常に機能しません。

5 最後に、HTTPS プローブと SSL サーバーの通信を設定します。OVIS 設定マネージャで [HTTPS 監視対象サービスの設定] ダイアログボックスの右下に**証明書のファイル名**を指定する個所があるので、そこに <data dir>¥conf¥probe ディレクトリへ移動したテキストファイルを指定します (このファイルを働かせるためには、<data dir>¥conf¥probe ディレクトリに置いておく必要があったことを思い出してください)。また、**証明書の秘密鍵のパスワード**を指定する個所があるので、そこに openssl.exe コマンドを発行した後で入力した PEM パスワードを指定します。

OVIS 4.5、5.0、5.20 から OVIS 6.0 へのアップグレード

OVIS 4.5、5.0、5.20 から OVIS 6.0 へアップグレードする場合は、<install dir>¥probes ディレクトリにある設定済みの trusted.txt または ClienCert ファイルを、新しい証明書の場所である <data dir>¥conf¥probe へすべて移動する必要があります。

カスタムレポート

カスタムプローブに使用するカスタムレポートを作成するには、Crystal Decisions Crystal Reports バージョン 10.0 以降 (www.crystaldecisions.com) と hp OpenView Reporter バージョン A.03.60 以降が必要です。カスタムプローブの作成方法については、『*Internet Services Custom Probes API Guide*』(CustomProbes.pdf) を参照してください。

Crystal Reports でカスタムレポートを作成し、hp OpenView Reporter を使って OVIS で表示できるように、レポートを設定します。レポートを生成および表示するよう設定する方法については、『*Reporter コンセプトガイド*』を参照してください。また、詳細について、Reporter のオンラインヘルプの「*レポート定義の追加*」も参照してください。

カスタムレポートを作成して Internet Services に統合するには、次の手順を実行します。

1. カスタムレポートテンプレートを統合するには、カスタムレポートテンプレートを `data¥reports¥iops` フォルダに保存します。
2. hp OpenView Reporter を使用してカスタムレポートを追加します。以下の内容も設定してください。

   ```
   REPORT = IOPS_<probe name>
   CATEGORY = 190 Internet Services
   HTML_DIRECTORY = Webpages¥<a_custom_report_1>
   ```

   `<a_custom_report_1>` は、相対ディレクトリ `Webpages` 内のレポート名です。この方法については、`Reporter` のマニュアルを参照してください。
3. カスタムプローブを夜通し実行します。翌日、カスタムプローブの夜間レポートが、OVIS ダッシュボードの [レポート] ワークスペースに表示されるようになります。

サポートしているデータベース

OVIS と OpenView Reporter は、パフォーマンス情報とレポート情報の保存に同じデータベースを共有します。

Oracle および Microsoft SQL Server データベースの設定方法については、『*データベース設定ガイド*』(Reporter_Database_Config.pdf) を参照してください。このマニュアルは、OpenView Reporter のドキュメンテーションからデータベースの設定に関する情報を抜き出し、OVIS 製品に追加したものです。

『*データベース設定ガイド*』にはデータベースのパフォーマンス情報も記載されています。

OVIS のデフォルトのデータベースは Microsoft SQL Server Desktop Engine (MSDE) です。このデータベースは以下のいずれかに変更することができます。

- Oracle 8.1.7 for Solaris、または Oracle 8.1.7 for HP-UX
- Oracle 9.2 for Solaris、または Oracle 9.2 for HP-UX
- SQL Server 2000

データベースはローカルまたはリモートのどちらに置いてもかまいません。ただし MSDE データベースは、OVIS 管理サーバーと同じシステムに置きます。SQL Server は OVIS 管理サーバーと同じシステムに置いても、リモートの Windows システムに置いてもかまいません。Oracle はリモートの UNIX システムへ置くことになります。

使用可能なデータベースは、インストールされている OpenView 製品によって異なります。

Internet Services を今後インストールするシステムに、Reporter がインストールされている場合	OVIS をインストールすると、OVIS は Reporter 用に設定されているデータベースを検出し、同じデータベースを使用します。OVIS のインストールプログラムは、このデータベースへの接続を設定し、必要に応じて OVIS 用のテーブルエントリを追加します。

Reporter がインストールされておらず、Internet Services を初めてインストールする場合	デフォルトの MSDE データベースがインストールされます。OVIS に付属の『*OVIS データベース設定ガイド*』の説明に従って、インストール後に Oracle または SQL Server 2000 データベースを設定することもできます。
Reporter がインストールされておらず、Internet Services の以前のバージョンから本バージョンの OVIS にアップデートする場合	アップグレードには、既存のデータベースを使用します。OVIS に付属の『*OVIS データベース設定ガイド*』の説明に従って、Oracle 8.1.7/9.2 または SQL Server 2000 データベースを設定することもできます。

警告 : Internet Services では、古いデータベースから新しいデータベースへのデータの移行はサポートしていません。OVIS と Reporter が同じシステム上にある場合、Reporter データを新しいデータベースに移行しようとすると、OVIS で問題が発生することがあります。

データベースの調整

データレコードを削除してデータベースを調整したい場合は、<install dir>¥bin¥ovisdbclean ツールが役立ちます。たとえば、「ダウンタイムのスケジュール設定」機能が使用できなかったときは、このツールを使用してデータベースからデータを一部削除する、つまりダウンタイムに相当する部分を削除することで、ダウンタイムがスケジュール設定されていたかのようにデータベースを調整することができます。

データの集約にはさまざまな方法があるので、ovisdbclean が必ず最良のツールであるというわけではありません。ovisdbclean ツールが一番適しているのは、その日の集計が行われる前です。毎日行う集計は、その夜の午前 2 時にスケジュールされています。

ovisdbclean ツールで削除できるのは、可用率が 100% 未満のレコードだけなので注意してください。指定した時間範囲にあるレコードの可用率が 100% になっていると、アプリケーションではそのレコードを削除できません。

ovisdbclean ツールでは、「時間範囲または顧客のどちらか一方」、「プローブロケーション」、「サービスグループ」または「監視対象サービス」、および「特定の時間範囲」を指定できます。[照会] をクリックして、リストに表示されたデータレコードが削除したいものであることを確認した後 (必ず各タブをクリックしてください)、[**削除対象としてマークを付ける**] チェックボックスをオンにします (データを削除する各タブで [削除対象としてマークを付ける] ボックスがオンになっていることを確認してください)。照会の結果リストに削除したくないレコードがある場合は、時間の範囲を狭めてください。

ovisdbclean ツールでは、測定値、アラーム情報、および SLO/SLA データの主なテーブルから可用率が 100% 未満のデータを削除します。

測定値 :	OPS_DETAIL_DATA、IOPS_DETAIL_DATA_HOURLY、IOPS_DETAIL_DATA_DAILY、IOPS_PROBE_DATA_CACHE、IOPS_PROBE_DATA_HOURLY、IOPS_PROBE_DATA_DAILY
アラーム情報 :	IOPS_ALARM_DATA2
SLO/SLA データ :	IOPS_SLA_CONFORMANCE_DATA、IOPS_SLO_CONFORMANCE_DATA

削除する場合は、その前に必ずデータを確認してください。いったん削除してしまったデータは復元が非常に困難です。削除したデータは監査ログとともに <Data Dir>/Data/Datafiles/ovisdbclean に書き出されます。このディレクトリにデータの削除日時を名前にしたサブディレクトリが作成され、そこに監査ログと削除データが格納されます。

テーブルに削除マークまたは更新マークが付けられると、以下の処理が行われます。

削除 : データベースからそのレコードが削除されます。

更新 : 時間範囲の始めまたは終りが時間 / 日の区切りめから外れていると、そのレコードは、グループカウントを可用率のカウントに設定して更新されます。この処理は、データポイントがすでに集約されているため行われます。たとえば、時間の範囲として 9:30 ～ 11:30 が設定されている場合、アプリケーションでは 9:00 と 11:00 のレコードを更新して、10:00 のレコードを削除します。9:00 と 11:00 のレコードを更新した結果、カウントフィールドの値が可用率フィールドに設定されるので、その時間の可用率は実効上 100% に設定されてしまいます。したがって、時間範囲の初めと終りは、時間の区切りめに合わせて設定することをお勧めします。

ovisdbclean ツールの詳細な使用方法は、オンラインヘルプを参照してください。

データベースのバックアップ

OVIS で使用する Reporter のデータベースは、次のようにバックアップすることをお勧めします。

1 以下のサービスを停止します。

— Reporter Service

— HP Internet Services

— World Wide Web Publishing Service

2 通常の手順に従ってデータベースをバックアップします。MSDE に関する、いくつかの推奨手順を以下に示します。

デフォルトデータベースの場合

デフォルトの MSDE データベースを使用している場合は、Microsoft の Web サイトでバックアップ手順を参照できます。以下では、Microsoft のユーティリティを使用する方法を説明します。サポートに関する情報やこれらの製品の使用時に発生する可能性のあるエラーなどについては、Microsoft のドキュメントを参照してください。

オプション 1: SQL Server のクライアントツールを使用している MSDE の場合
SQL Server 2000 クライアントツールがインストールされている場合は、SQL Enterprise Manager を使用して MSDE データベースをバックアップします。

オプション 2: SQL Enterprise Manager を使用していない MSDE の場合
MSDE だけがインストールされている場合、TSQL BACKUP DATABASE コマンドを使用して、Osql.exe (コマンドライン クエリーツール) とともに実行することができます。

次に説明するストアドプロシージャの使用方法は、MSDN および SQL の Web サイトでも詳細に説明されています。以下で説明している構文を使用して、バックアップ / デタッチ / リストアプロシージャを作成します。

注記 : 以下の手順では、各種ストアドプロシージャと MSDE を使用して、バックアップやリストアを実行する方法について説明します。使用環境に応じて手順をカスタマイズしてください。たとえば、毎日のバックアップジョブの作成や、バックアップレポートの生成も可能です。`Osql` ユーティリティ、BACKUP

DATABASE および RESTORE DATABASE 文の他のオプションと機能については、Microsoft (MSDN) ドキュメントを参照してください。バックアップとリストア処理が正しく行われることは必ず確認してください。

この例では、ディレクトリ名、ユーザー名、およびパスワードに特定のデフォルト値を使用しているため、実際にはこれらの値を変更する必要があります。

MSDE のみがインストールされている場合のバックアップ手順

1. Reporter、HP Internet Services、および W3SVC サービスを停止し、他のクライアントツールが Reporter または Internet Services MSDE データベースにアクセスしていないことを確認します。
2. バックアップデバイスを作成して、以下の手順に従って MSDE データベースをバックアップします。
   コマンドプロンプトで、以下のコマンドを入力します。

```
c:¥>osql -S.¥OVOPS -Usa -P
1>USE Reporter
2>BACKUP LOG Reporter WITH TRUNCATE_ONLY
3>EXEC sp_addumpdevice 'DISK', 'Reporter_BKUP', 'C:¥Program
Files¥HP
Openiew¥Data¥Dataases¥backup¥Reporter_1.bak'
4>BACKUP DATABASE Reporter TO Reporter_BKUP WITH INIT, STATS
5>EXEC sp_dropdevice 'Reporter_BKUP'
6>go
The database will be backed up...
1>exit
```

3. Reporter、HP Internet Services、および W3SVC サービスを再起動します。

リストア手順の例

1. Reporter、HP Internet Services、および W3SVC サービスを停止し、他のクライアントツールが Reporter または Internet Services MSDE データベースにアクセスしていないことを確認します。
2. 以下の手順に従って、MSDE データベースのバックアップをリストアします。
   コマンドプロンプトで、以下のコマンドを入力します。

```
c:¥>osql -S.¥OVOPS -Usa -P
1>USE Master
2>RESTORE DATABASE Reporter FROM DISK='C:¥Program Files¥HP
OpenView¥Data¥Databases¥backup¥Reporter_1.bak' WITH RECOVERY,
REPLACE, STATS
3>go
The database will be restored...
1>exit
```

3 Reporter、HP Internet Services、および W3SVC サービスを再起動します。

初期状態に戻す方法

ここでは、Internet Services を初期状態に戻す方法について説明します。この手順を使用して、テスト設定を削除し、最初からやり直すことができます。また、設定を保ったままデータベースを再構築することもできます。データベースが破損した場合、または収集したすべてのデータを削除して最初からやり直す場合には、データベースの再構築が必要となることがあります。

Reporter と OVIS の最新リリースでは、デフォルトのデータベースとして MSDE を使用します。

レポートサービスを実行している他の製品の再起動

この手順を実行すると、レポートサービスを実行している他の製品が再起動されます。Reporter をインストールしている場合は、この手順を実行する前に製品のマニュアルを参照してください。

この手順を実行すると、Internet Services のデータが完全に削除されます。

手順を実行する前に現在のサービス設定情報を保存し、あとで再ロードできるようにする場合は、[コマンドプロンプト] ウィンドウを開いて以下のコマンドを入力し、すべての設定データを xml ファイルに保存します。

```
iopsload -save myconfig.xml
```

myconfig.xml は、適切なファイル名で置き換えてください。ファイルが作成され、設定情報は XML 形式で書き込まれます。このコマンドは `httptrans.dat` ファイルも保存します。

MSDE データベースの再作成

ここでは、既存の Reporter/Internet Services の MSDE データベースを削除して、MSDE データベースを再作成する方法について説明します。スクリプトは、`newdb.exe` がある、`<install dir>¥bin` ディレクトリから実行する必要があります。

1. 以下の Internet Services コンポーネントを停止します。
   a. Reporter Service
   b. HP Internet Services
   c. World Wide Web Publishing Service
2. Reporter GUI、Internet Services 設定マネージャ、およびダッシュボードを閉じていることを確認します。
3. [コマンド プロンプト] ウィンドウを開きます。
4. cd コマンドを使用して `<install dir>¥bin` ディレクトリに移動します。
5. コマンドプロンプトで以下のコマンドを入力します。

   ```
   cscript RecreateMSDEDB.vbe
   ```

6. `<install dir>¥Data¥status.Reporter` ファイル内で、`newdb` のステータスを確認します。
7. **任意 :** 保存した設定情報をリストアします。
   a. [コマンドプロンプト] ウィンドウを開きます。
   b. `iopsload` プログラムを実行して、xml ファイルをデータベースに転送します : `iopsload -load myconfig.xml` (*myconfig.xml* は、設定の保存で使用したものと同一のファイル名)。
8. [スタート] メニューから [**設定**] > [**コントロールパネル**] > [**サービス**] を選択して、Internet Services の以下のコンポーネントを再起動します。
   a. Reporter Service
   b. HP Internet Services
   c. World Wide Web Publishing Service

SQL Server データベースの再作成

ここでは、既存の Reporter/Internet Services の SQL Server データベースを削除して、新しい SQL Server データベースを再作成する方法について説明します。スクリプトは、`newdb.exe` がある、`<install dir>¥bin` ディレクトリから実行する必要があります。

1. 以下の Internet Services コンポーネントを停止します。
   a. Reporter Service
   b. HP Internet Services
   c. World Wide Web Publishing Service
2. Reporter GUI、Internet Services 設定マネージャ、およびダッシュボードを閉じていることを確認します。
3. データベースシステムのコントロールパネルで以下の項目を選択します。[**スタート**] > [**プログラム**] > [**Microsoft SQL Server**] > [**Enterprise Manager**]
4. 表示されたダイアログの左ペインで [**Microsoft SQL Servers**] > [**SQL Server グループ**] > [**< サーバーマシン名 >**] [**データベース**] > [**Reporter**] の順に選択し、右クリックして [**削除**] を選択します。これでデータベースが削除されます。
5. データベースを再作成するには、左ペインで上記と同様に選択した後、右クリックして [**新規データベース**] を選択します。[Reporter] と初期サイズを入力するとデータベースが再作成されます。詳細は、『*データベース設定ガイド*』(Reporter_Database_Config.pdf) を参照してください。
6. 管理サーバー上で設定マネージャを開くと、`NewDB.exe` プログラムと `Newiops.exe` プログラムが実行され、Internet Services のテーブルが再構築されます。
7. **任意 :** 保存した設定情報をリストアします。
   a. [コマンドプロンプト] ウィンドウを起動します。
   b. `iopsload` プログラムを実行して、xml ファイルをデータベースに転送します : `iopsload -load` *`myconfig.xml`* (*`myconfig.xml`* は、設定の保存で使用したものと同一のファイル名)。

8 [スタート] メニューから [**設定**] > [**コントロールパネル**] > [**サービス**] を選択して、Internet Services の以下のコンポーネントを再起動します。

a Reporter Service

b HP Internet Services

c World Wide Web Publishing Service

Oracle データベースの再作成

この操作を実行すると、Internet Services 固有のテーブルのみが削除されます。追加の Reporter テーブルは削除されません。同じレポートデータベースを使用している別の OpenView 製品を使用している場合は、これらの製品固有のテーブルの削除方法について、その製品のマニュアルで確認してください。

1. 以下の Internet Services コンポーネントを停止します。
   a. Reporter Service
   b. HP Internet Services
   c. World Wide Web Publishing Service
2. Reporter GUI、Internet Services 設定マネージャ、およびダッシュボードを閉じていることを確認します。
3. Internet Services がインストールされている Windows システム上の `<install dir>¥newconfig¥oracle¥<`*hp-ux または sun ディレクトリ*`>¥DropIOPS.sql` (hp-ux または sun ディレクトリのいずれかを指定) を UNIX システムのディレクトリ `$ORACLE_HOME/dbs/` にコピーします。
4. Oracle データベースがインストールされている UNIX システムで、`ORACLE_SID=REPORTER` の Oracle セッションを確認します。
5. oracle としてログインし、プロンプトに対して「`svrmgrl`」と入力し、Oracle サーバーマネージャプログラムを起動します。
6. `SVRMGR>` プロンプトに対して「connect <openview>/<openview>」と入力します。

   「<openview>/<openview>」は OVIS Reporter データベース用のユーザー名とパスワードです。
7. 以下のコマンドを入力して、データベースからデータを削除します。
   `@ORACLE_HOME/dbs/dropIOPS.sql`
8. Windows システム上で `<install dir>¥bin¥NewDB.exe` を実行して、データベース内に Reporter テーブルと Internet Services テーブルを作成します。
9. **任意 :** 保存した設定情報をリストアします。
   a. [コマンドプロンプト] ウィンドウを起動します。

b `iopsload` プログラムを実行して、xml ファイルをデータベースに転送します : `iopsload -load myconfig.xml` (*`myconfig.xml`* は、設定の保存で使用したものと同一ファイル名)。

10 [スタート] メニューから [**設定**] > [**コントロールパネル**] > [**サービス**] を選択して、Internet Services の以下のコンポーネントを再起動します。

a Reporter Service

b HP Internet Services

c World Wide Web Publishing Service

TIPs データベースの復元

TIPs データベースが破損した場合でも、バックアップファイルを作成していれば、その TIPs データベースは復元できます。バックアップファイルの作成方法については、TIPs Configuration program のオンラインヘルプを参照してください。ここでは、オンラインヘルプへアクセスできない場合に備えて、バックアップファイルからデータを復元する手順を示します。

HP から提供された TIPs とコマンドは、それらを含んだ TIPs 定義ファイルをインポートすることで、いつでも復元できます。TIPs の定義をインポート / エクスポートする方法については、TIPs Configuration program のオンラインヘルプを参照してください。

バックアップファイルから復元したデータはバックアップを行った時点のデータと同じであることにご注意ください。

以下のような状況が発生した場合は、TIPs データベースが破損している可能性があります。

- TIPs Viewer でデータベースのエラーが見つかる。
- TIPs Server のログでデータベースのエラーが見つかる。
- TIPs Configuration program が起動しない。

TIPs データベースの検証

以下の 3 つの TIPs データベースを検証してください。

- TIPs 定義のデータベース
- アラームトリガード TIPs のデータベース
- TIPs 認証と TIPs Runner 登録のデータベース

TIPs 定義のデータベースを検証するには、次の手順を実行します。

1 TIPs Server システムのコマンドウィンドウで次のコマンドをで実行し、TIPs 定義のデータベースをダンプします。

Windows の場合

```
<install_dir>¥contrib¥OvTIPsDumpDB TIP
```

2 出力を調べます。データベースが破損していなければ、設定されている TIPs がリストになって表示されます。データベースが破損していると、例外またはエラーメッセージが表示されます。

アラームトリガード TIPs のデータベースを検証するには、次の手順を実行します。

1 TIPs Server システムのコマンドウィンドウで次のコマンドを実行し、アラームトリガード TIPs のデータベースをダンプします。

Windows の場合

```
<install_dir>¥contrib¥OvTIPsDumpPregather
```

2 出力を調べます。データベースが破損していなければ、保存されているアラームリガード TIPs がリストになって表示されます。データベースが破損していると、例外またはエラーメッセージが表示されます。

TIPs 認証と TIPs Runner 登録のデータベースを検証するには、次の手順を実行します。

1 TIPs Server システムでのコマンドウィンドウで次の コマンドを実行し、TIPs 認証と TIPs Runner 登録のデータベースをダンプします。

Windows の場合

```
<install_dir>¥contrib¥OvTIPsDumpSrvltDB TIPRunner
```

2 出力を調べます。データベースが破損していなければ、登録されている TIPs Runner がリストになって表示されます。データベースが破損していると、例外またはエラーメッセージが表示されます。

TIPs データベースの復元

TIPs データベースを初期化しなおすと、アラームトリガード TIPs、TIPs 定義、TIPs Runner 登録、および TIPs 認証の各情報がすべて失われてしまいます。バックアップファイルが作成してあれば、これらの情報は復元することができます。

データベースの再初期化手順

1 コマンドウィンドウで次のコマンドを実行し、ローカル TIPs Runner を停止させます。

```
<install_dir>¥bin¥ovc -stop ovtiprn
```

2 コマンドウィンドウで次のコマンドを実行し、TIPs Server を停止させます。

```
<install_dir>¥bin¥ovc -stop ovtomcatA
```

3 次のディレクトリにあるファイルをすべて削除します。

```
<data_dir>¥datafiles¥tips¥database
```

4 コマンドウィンドウで次のコマンドを実行し、データベースを作成します。

```
<install_dir>¥bin¥OvTIPsCreateDB
```

5 データを復元する場合はこのステップを省略して、該当するデータ復元手順へ進みます。

データを復元しない場合はコマンドウィンドウで次のコマンドを実行し、TIPs Server を再起動します。

```
<install_dir>¥bin¥ovc -start ovtomcatA
```

コマンドウィンドウで次のコマンドを実行し、ローカル TIPs Runner を再起動します。

```
<install_dir>¥bin¥ovc -start ovtiprn
```

データを復元する場合は、TIPs Server とローカル TIPs Runner を停止させる必要があります。

バックアップデータファイルから復元できるデータは、TIPs 定義、アラームトリガード TIPs 、TIPs Runner 登録、および TIPs 認証の各情報です。

最後にバックアップしたデータファイルを復元する手順

1 任意 : システムのバックアップファイルから、TIPs 定義のデータベースを作成しなおすために必要な次のファイルを取得します。

```
TIPs.btx
```

```
TIPs.btd
```

次のディレクトリにこれらのファイルを置きます。

```
<data_dir>¥datafiles¥tips¥database
```

2 任意 : システムのバックアップファイルから、アラームトリガード TIPs のデータベースを作成しなおすために必要な次のファイルを取得します。

```
Pregather.btx
```

```
Pregather.btd
```

次のディレクトリにこれらのファイルを置きます。

```
<data_dir>¥datafiles¥tips¥database
```

3 任意 : システムのバックアップファイルから、TIPs 認証と TIPs Runner 登録のデータベースを作成しなおすために必要な次のファイルを取得します。

```
TIPsAuth.btx
```

```
TIPsAuth.btd
```

次のディレクトリにこれらのファイルを置きます。

```
<data_dir>¥datafiles¥tips¥database
```

4 コマンドウィンドウで次のコマンドを実行し、TIPs Server を再起動します。

```
<install_dir>¥bin¥ovc -start ovtomcatA
```

5 コマンドウィンドウで次のコマンドを実行し、ローカル TIPs Runner を再起動します。

```
<install_dir>¥bin¥ovc -start ovtiprn
```

データを復元する場合は、TIPs Server とローカル TIPs Runner を停止させる必要があります。

XML ファイルをインポートして TIPs 定義を復元する手順

1 エクスポートしておいた TIPs 定義ファイルをインポートします。TIPs 定義のインポート / エクスポート方法については、TIPs Configuration program のオンラインヘルプを参照してください。

2 コマンドウィンドウで次のコマンドを実行し、TIPs Server を再起動します。

```
<install_dir>¥bin¥ovc -restart ovtomcatA
```

3 コマンドウィンドウで次のコマンドを実行し、ローカル TIPs Runner を再起動します。

```
<install_dir>¥bin¥ovc -restart ovtiprn
```

スケーラビリティ情報

OVIS のパフォーマンスとスケーラビリティは、次の領域で調べることができます。

- プローブシステム
  - 必要なハードウェアリソースは何か？
  - プローブシステムごとに実行できる監視対象の数は何個か？
  - 異なるプローブシステムが何個必要か？
  - 専用のプローブシステムが必要か、それとも他のタスクに使用しているマシンをプローブシステムとして使用できるか？
  - プローブのタイプが異なれば、プローブシステムのリソース要件も異なるか？
- ネットワークの帯域幅
  - プローブシステムとプローブ監視対象との間で転送されるデータ量はどのくらいか？
  - プローブシステムと管理サーバーとの間で監視対象ごとに転送されるデータ量はどのくらいか？
  - データの転送量を左右するプローブシステムの設定要素は何か？
- 管理サーバーシステム
  - 必要なハードウェアリソースは何か？
  - どのようなデータベース構成が最適か？
  - データの処理、保在、収集
    - 1 台の管理サーバーで処理できるプローブシステム / 監視対象の数は何個か？
    - 管理サーバーのデータ処理能力に影響を与える設定要素は何か？
  - データベースのサイズ設定とアクセス
    - データベースのサイズを左右する構成要素は何か？
    - ダッシュボードの応答性が著しく影響を受けない範囲でデータベースに保存できるデータ量はどのくらいか？

– レポートの生成時間やデータベースのメンテナンス / 集約時間が著しく影響を受けない範囲でデータベースに保存できるデータ量はどのくらいか？

プローブシステム

OVIS のプローブシステムでは次の処理を実行します。

- プローブの実行スケジュールを設定する
- スケジュールポリシーに基づいてプローブを実行する
- プローブの結果を OVIS 管理サーバーへ転送する

1 個のプローブシステムで対応可能なプローブ監視対象の最大数は、プローブシステムのサイズと使用可能な処理能力に加えて、次の要素と変更可能な設定値で決まります。

- プローブシステムごとに設定される監視対象サービスの種類。
- 監視対象サービスの可用性 : 監視対象サービスが利用できないと、プローブがタイムアウトになって、順番どおりにしか実行できないプローブは進行が遅れます。
- プローブの間隔 : 間隔を短くすると、順番どおりにしか実行できないプローブの時間制限が厳しくなります。
- プローブのタイムアウト : タイムアウトの時間を長くすると、順番どおりにしか実行できないプローブは進行が遅れます。
- プローブの遅延 : プローブとプローブの間に遅延を設定すると、1 回の測定間隔で実行できるプローブの数が減ります。
- ローカルプローブシステムまたはリモートプローブシステムのロケーション : プローブから監視対象へアクセスするときに使うネットワーク接続の速度が遅いと、時間が余計にかかってタイムアウトの可能性が高くなるため、順番どおりにしか実行できないプローブは進行が遅くなる可能性があります。
- 並行して処理できるリクエストの数 : デフォルトでは、最大 32 個のプローブを並行処理できるようになっています。並行して処理できる数を多くすれば、1 回のプローブ間隔で実行するプローブの数は増えますが、それと同時に、プローブシステムで使用するシステムリソースも増えます。

必要なプローブシステム数の計算

必要なプローブシステムの数は、次の 式で計算することができます。

プローブシステムの数 ＝
（（監視対象÷同時リクエスト数）×（タイムアウト＋遅延））÷間隔

並行処理数 ＝ 同時に実行できる監視対象の数

タイムアウト値 ＝ 監視対象のタイムアウト値（秒単位）

遅延 ＝ [プローブロケーション] ダイアログで設定した場合は、[プローブ遅延情報] の値になります (単位は秒)。特に指定しない限り、遅延は設定されません。つまり遅延時間は 0 秒になります。

間隔 ＝ ポーリング間隔 (単位は秒)

これらの式では、プローブの実行時間として最悪のケース (すべてのプローブがタイムアウトになる場合) を想定しています。したがって、必要なプローブシステムの数を調べるときは、この式の結果を整数に切り上げて使います。

例

以下の環境では、タイムアウト値が 20 秒の監視対象サービス 100 個を 5 分間隔で実行しようとしていますが、この場合はプローブシステムが 1 個必要です。計算結果の正確な値 0.21 ですが、この値を整数に切り上げて使用するので、必要なプローブシステムの数は 1 になります。

監視対象サービス数	＝ 100
並行リクエスト数	＝ 32
タイムアウト値	＝ 20 （秒）
遅延	＝ 0 （秒）
間隔	＝ 300 （秒）
プローブシステム数	＝ (100 ÷ 32) × (20 ＋ 0) ÷ 300
	＝ 0.21
	＝ 1 プローブシステム

次の例では、式の使い方を少し変えるとともに、他のプローブ設定値をそのままにして、実行できる監視対象サービスの数を調べています。

プローブシステム数　＝ 1

並行リクエスト数　＝ 32

タイムアウト値　＝ 20　（秒）

遅延　＝ 0　（秒）

間隔　＝ 300 （秒）

1 プローブシステム　＝（監視対象サービス数 ÷ 32）×（20 ＋ 0）÷ 300

＝（監視対象サービス数 ÷ 8）× 5 ÷ 300

5 ×監視対象サービス数　＝ 8 × 300

監視対象サービス数　＝ 480

プローブシステムごとに実行できる監視対象サービスの数の計算

前の項で示した式は単純かつ初歩的なもので、合計タイムアウト時間までの間にプローブがすべて実行される場合しか想定していません。しかし、さらに重要なのは、これらの式でプローブ自体の実行に必要なシステムリソースの使用要件が考慮されていないということです。プローブシステムに関するリソース要件は次の設定要素から影響を受けます。

- プローブのタイプ : HTTP_TRANS プローブは他のプローブタイプに比べてリソースに対する依存度が高く、特にトランザクションシーケンスごとのステップが多いと、その依存度はさらに高くなります。これは、ステップが順番どおりにしか実行できなくて、ステップとステップの間に余裕がないためです。こうしたトランザクションが同時に多数実行されると、CPU の利用率は高くなります。また、各プローブを実行するための処理でメモリが 3MB ～ 20 MB 必要です (IE モードは、IE 以外のモードより多くのメモリが必要です)。

IE 以外のモードでは、各ステップの間でプローブの実行に遅延がないため (つまり余裕がないため)、CPU 時間をより多く使用することになります。これに加えてステップの数が非常に多いと、結果として CPU の使用が急増することになります。特に、監視対象ステップから短時間のうちに結果が返される場合はこの状況が顕著になります。モードが IE 以外のプローブでは、トランザクションごとに常駐メモリーを約 3K ～ 5K 使います。IE モードの場合、プローブ自体に使用する CPU 時間はそれ以外のモードより少なくなります。これは、IE モードのプローブでは各ステップの間で 1.5 秒間だけ一時停止するためです。1.5 秒という値はデフォルトの待機時間 (1500 ミリ秒) であり、その設定は変更できます。ただし、IE モードでは、表示するページの処理にクライアント側ブラウザのコントロールやブラウザ自体で実行するロジックが多く含まれているほど、使用する CPU 時間もそれだけ多くなります (実際の話、モードが IE 以外のプローブではこのようなコントロールは実行されません)。モードが IE 以外のプローブではトランザクションごとに約 10K ～ 15 K の常駐メモリを使用しますが、その量は、ダウンロードされたページの表示内容によって大きく異なります。

プローブシステムが OVIS プローブ専用になっている場合は、同時に実行する数に注意する必要があります。この数が多過ぎて、システムリソースやメモリリソースが足りなくなると、プローブがタイムアウトになって、処理を最後まで実行することができなくなります。また、他の処理タスクやアプリケーションに使用するプローブシステムで HTTP_TRANS プローブを実行する場合は、そのプローブの実行に必要なリソースの使用が増えて他の処理機能に悪影響しないよう、同時実行数には同じような注意を払う必要があります。

一般的にいえば、32 というデフォルトの同時リクエスト数は、各シーケンスのステップが 6 以上の HTTP_TRANS プローブにとって多すぎます。このように HTTP_TRANS の監視対象が多い環境では、同時リクエスト数として 10 以下が適しています。不確かな場合は、パフォーマンスツールでプローブシステムをモニターし、プローブの影響を評価したり、割り当てられた間隔でプローブが完了できるかどうかを評価したりします。

- 並行リクエスト数と監視対象数 : どのタイプのプローブもプロセスとして動作するので、システムリソースを使用します。そのため、1 回の間隔で同時に実行できるプローブの数には制限があります。プローブシステムは、パ

フォーマンスツールでモニターすることで、そのプローブの影響を評価したり、割り当てられた間隔でプローブが完了できるかどうかを評価したりすることができます。

- 間隔と遅延 : プローブシステムで実行する監視対象の数が非常に多い場合は、プローブ間隔をより長くするとともに、プローブの実行と実行の間の遅延をより長くすることでも、これらシステムで要求されるリソースの量を減らすことができます。また、同じ目的で並行数と優先度も使用できます。
- プローブが監視対象から応答を得るまでの待時間が長い場合は、並行数を増やすことでサイクル時間全体を大幅に減らすことができます。逆に、プローブの開始対象が高速で反応も早い場合は待機時間が短いので、並行数の多いプローブシステムでは処理要件の方が高くなります。

プローブシステムごとの監視対象数やプローブシステムの必要数として具体的な数値を記載することは困難です。正しい値は、上記の設定変数だけでなく、プローブシステムの全体的なサイズや処理能力に応じても異なります。また、他のアプリケーションを収容した場合の使用可能な空き容量にも影響されます。

プローブシステムの物理的な配置でプローブロケーションが重要な意味を持っていなくても、OVIS を展開配備したときの容量にかなり余裕がない限り、管理サーバーは「ローカルプローブ」システムとして使用しないでください。ほとんどの場合はプローブロケーションが重要ではないので、OVIS 管理サーバーから離れたリモートプローブシステムを使うことで、プローブの動作と管理サーバーの機能がリソースを求めて競合しないようにする方が得策です。

ネットワークの帯域幅

プローブシステムと監視対象との間の帯域幅

あるプローブシステムとプローブ対象システムとの間で 1 秒間に転送されるバイト数は、次の式で計算できます。

1 秒間に転送されるバイト数＝
（間隔ごとの監視対象数×監視対象ごとに転送されるバイト数）÷間隔（秒）

この結果をすべてのプローブシステムについて合計すると、OVIS の管理対象環境で間隔ごとに転送される 1 秒あたりの合計バイト数が得られます。

監視対象ごとに転送されるバイト数は、プローブタイプと監視対象の組み合わせでそれぞれ異なります。一般的に、タイプが HTTP、HTTP_TRANS、SOAP、FTP、NNTP、STREAM_MEDIA、EXCHANGE、SMTP、POP3 の各プローブでは、プローブを実行するたびに転送されるペイロードが非常に大きくなります。これらのプローブを設定するときは、監視対象のサイズを十分に把握しておく必要があります。たとえば、HTTP プローブの場合、返されたページに含まれている監視対象のサイズは、ダウンロードされたページのサイズとそこに組み込まれている画像やコンテンツを合計して決定することができます。同様に、プローブする FTP ファイルや電子メールメッセージのサイズも把握しておく必要があります。

タイプが HTTP_TRANS のプローブの場合は、1 個の監視対象が複数のステップで構成されていて、ステップごとにページがダウンロードされます。

プローブシステムと管理サーバーとの間の帯域幅

OVIS 管理サーバーに送信されるプローブ測定結果のサイズは、どのプローブタイプでもほぼ同じです。プローブの監視対象が実行されるとそのたびに測定レコードが OVIS 管理サーバーへ送信されますが、そのレコードのサイズは一般的に約 500 ～ 1200 バイトです (600 バイトが通常の平均サイズ)。すべてのプローブシステムで間隔ごとに実行される監視対象の数にこの値を掛けて、プローブ間隔ごとに OVIS 管理サーバーへ送信されるデータ量を見積ります。

測定レコードには次の可変長フィールドがあり、その長短が全体のサイズに最も大きく影響します。

- 顧客名
- サービスグループ名

- 監視対象
- エラー情報

タイプが HTTP_TRANS のプローブでは、トランザクションのステップごとにに URL フィールドも含まれています。また、同じ HTTP_TRANS 監視対象の 1 回の実行で、ステップごとに測定値が 1 組ずつ送信されます。

管理サーバーシステム

管理サーバーのスケーラビリティに関するサイズ設定は、顧客、サービスグループ、監視対象サービス、およびリモートプローブシステムの数に依存します。OVIS 管理サーバーへ送信されるプローブ測定値の数は、プローブ監視対象とプローブシステムの数、およびプローブ設定によって決まります。OVIS 管理サーバーでは、限られた割当て時間の範囲で、送られてきた測定値をすべてタイムリーに処理するとともに、データ収集やアクセスといった管理サーバーの他の機能も同様に実行しなければなりません。プローブ測定値を個々に処理するときは、しきい値とアラームの条件も適用されます。そのため、しきい値の条件と種類がどれだけ多いかが処理能力に影響します。これらの変数すべてと、顧客やサービスグループの数で、OVIS 管理サーバー上のデータベースへ保存されるデータ量が決まります。保存されるデータの量は、ダッシュボードの使用や夜間のレポート生成といった、データ収集あるいはアクセスオペレーションに直接影響します。

特別な理由がない限り、OVIS 管理サーバーには、最も高速で入手可能なハードウェアリソースを使い、システムに必要なメモリーも十分搭載します。また、データベースとしては、SQL Server や Oracle など、実用に耐える製品を使用する必要があります。さらに、データベースを別のサーバーに配置する場合は、OVIS 管理サーバーとデータベースサーバーとの間のネットワーク接続を高速にするとともに、ネットワークの容量に余裕を持たせてください。

OVIS の監視対象が少ない場合や、使用環境の規模が小さい場合は、OVIS 管理サーバーシステムを他のアプリケーションやアクティビティと共有できます。しかし、OVIS の展開配備が中〜大規模である場合は、専用のシステムを使用するようお勧めします。

プローブ測定の処理スループット

前の項では、5 分間 (300 秒) にすべてのプローブシステムから OVIS 管理サーバーへ送信されるプローブ測定レコードについて、その合計数を決定する際に役立つ式とガイドラインを説明しました。すべてのプローブ監視対象およびプロー

ブシステムで収集された 5 分間の合計レコード数を 300 (秒) で割れば、1 秒間に OVIS 管理サーバーへ到着するプローブ測定レコードのおよその数を知ることができます。

OVIS 管理サーバーが中規模サイズの Windows プラットフォーム (2 GHtz のシングルプロセッサ、1 GByte 以上のメモリー) で動作している場合は、1 秒間に約 150 レコードを処理できますが、この処理には、着信結果の構文解析、設定されているしきい値やアラーム条件の適用、アラームの生成 (必要な場合)、およびデータベースへのレコードの記録が含まれています。その最大レートは、サービスレベル目標値 (SLO) の設定に基づいてトリガーがかけられるしきい値の条件とアラームの条件が複雑な環境ほど、より小さくなります。

予測される 1 秒間の測定レコード数がこのレートより大幅に多い場合は、複数の OVIS 管理サーバーで、プローブ数やプローブ頻度を減らすか分散させる必要があります。OVIS 管理サーバーで行っているプローブ測定レコードの処理が限界に近づいていることを見つけるには、システムパフォーマンスモニターソフトウェアを使って、IIS inetinfo プロセスの CPU 使用率をモニターします。inetinfo の CPU 使用率が 50% 以上の状態で 5 分間続けば、測定レコードの到着レートが高すぎることを示しています。

レコードの到着レートが境界線上にあってまだ処理を続行できる場合は、時間の経過とともに、これらのレコードが履歴データベーステーブルへ大量に記録されます。その結果、ダッシュボードのさまざまな表示に必要なデータベースアクセス (レポート / クエリの作成) に悪い影響を与える可能性が高くなります (履歴データベースのテーブルサイズとデータアクセスの動作に与える影響については、後続の項で詳しく説明します)。また、データベースの集約とメンテナンスは、タイムリーに行える必要があります。OVIS 管理サーバーが行うレコード処理の負荷で利用可能なシステム処理能力をすべて使い切ると、これらのオペレーションは割り当てられた時間で完了できなくなります。

データベースのサイズ設定

可変長レコードのサイズに影響する要因や、ログに記録された各レコードの履歴データベーステーブルが増大する要因は、多数あります。たとえば、顧客、サービスグループ、ホスト、およびプローブロケーションの名前と監視対象サービス情報は、それらのサイズが可変なので動的に割り当てられます。また、プローブが失敗した場合、エラーメッセージのサイズも考慮する必要があります。マルチステップトランザクションを実行するプローブは、ステップごとに追加レコードを使用します。さらに、各データベースタイプもテーブル、インデックス、レコードを管理するために独自のオーバーヘッドを持っています。

以下のデータベースの増大の例では、5 分間隔で測定された単一ステップの HTTP 監視対象による、1 つの顧客とサービスグループをベースにした評価を示します。この評価では、設定された SLO または SLA や、SLO 違反によって生成されたアラームを考慮しません。評価結果は、監視対象サービスの数に必要な 1 日あたりの記憶領域と、監視対象サービスに必要な記憶領域の合計とデフォルトの「保存日数」を判断するのに役立ちます。

このサイズの評価結果は、データベースのインストールと運用に必要な記憶領域とは別に必要なサイズを示しています。長期にわたりデータベースの増大を監視および管理するには、HP OpenView Database Smart Plug-In を使用することをお勧めします。

OVIS データ記憶領域のテーブル

OVIS 監視対象サービスの場合、データ記憶領域に 6 つのテーブルを使用します。監視対象サービスの詳細データとサービスグループのデータにそれぞれ 3 つのテーブルを使用します。

監視対象サービスの詳細データのテーブル

- IOPS_DETAIL_DATA (5 分間隔の監視対象サービスのデータ)、デフォルトの保存日数 = 7
- IOPS_DETAIL_DATA_HOURLY (1 時間あたりの監視対象サービスデータの集計)、デフォルトの保存日数 = 30
- IOPS_DETAIL_DATA_DAILY (1 日あたりの監視対象サービスデータの集計)、デフォルトの保存日数 = 365

監視対象サービスの詳細データのテーブルの最大レコードサイズは、約 1200 バイトです。通常の HTTP 監視対象サービスでは、平均してレコードの合計サイズの半分 (600 バイト) を使用します。

以下の表の例では、600 バイトのレコードサイズを使用して、各監視対象サービスの詳細データのテーブルのサイズ (バイト / 日) を計算しています。

表 13　例 : 監視対象サービスの詳細データのテーブルのデータ記憶領域サイズの計算

データタイプ	1 日あたりの データ記憶領域の計算	バイト / 日
IOPS_DETAIL_DATA (5 分間隔の監視対象サービスのデータ)	600 (バイト / レコード) × 12 (レコード / 時) × 24 (時間 / 日) ＝	172800 バイト / 日
IOPS_DETAIL_DATA_HOURLY	600 (バイト / レコード) × 1 (レコード / 時) × 24 (時間 / 日) ＝	14400 バイト / 日
IOPS_DETAIL_DATA_DAILY	600 (バイト / レコード) × 1 (レコード / 24 時間) × 24 (時間 / 日) ＝	600 バイト / 日
	監視対象サービスの詳細データのテーブルの合計 ＝	187800 バイト / 日 (≒ 183KB/ 日)

サービスグループデータのテーブル :

- IOPS_PROBE_DATA_CACHE (5 分間隔のサービスグループデータ)、デフォルトの保存日数 ＝ 7
- IOPS_PROBE_DATA (1 時間あたりの監視対象サービスグループデータの集計)、デフォルトの保存日数 ＝ 30
- IOPS_PROBE_DATA_DAILY (1 日あたりの監視対象サービスグループデータの集計)、デフォルトの保存日数 ＝ 365

サービスグループデータの最大レコードサイズは約 350 バイトです。通常の HTTP 監視対象サービスでは、平均してレコードの合計サイズの半分 (175 バイト) を使用します。

以下の表の例では、175 バイトのレコードサイズを使用して、各監視対象サービスグループデータのテーブルのサイズ (バイト / 日) を計算しています。

表 14　例 : サービスグループのテーブルのデータ記憶領域サイズの計算

データタイプ	1 日あたりのデータ記憶領域の計算	バイト / 日
IOPS_PROBE_DATA_CACHE（5 分間隔のサービスグループのデータ)	175 (バイト / レコード) × 12 (レコード / 時) × 24 (時間 / 日) ＝	50400 バイト / 日
IOPS_PROBE_DATA (1 時間ごとの集計)	175 (バイト / レコード) × 1 (レコード / 時) × 24 (時間 / 日) ＝	4200 バイト / 日
IOPS_PROBE_DATA_DAILY	175 (バイト / レコード) × 1 (レコード /24 時間) × 24 (時間 / 日) ＝	175 バイト / 日
	サービスグループのデータのテーブル合計＝	54775 バイト ÷ 日 (≒ 54KB/ 日)

1 日ごとの監視対象サービスデータの記憶領域の合計

OVIS の 6 つの記憶領域テーブルの合計レコードサイズの半分を使用する HTTP 監視対象サービスは、1 日あたりデータ記憶領域の約 237 キロバイトを使用します (監視対象サービスの詳細データ ＝ 183 KB ＋ サービスグループデータ ＝ 54 KB)。

監視対象サービスごとのデータ記憶領域の合計の計算

上記の計算に基づいた HTTP 監視対象サービスの記憶領域と各テーブルのデフォルトの保存日数の値について説明します。

表 15　例 : 監視対象サービスあたりのデータ記憶領域のサイズの計算

データテーブル	保存日数	データ記憶領域の計算	必要なサイズ
IOPS_DETAIL_DATA	7	172800 (バイト / 日) × 7 (日) ＝	1209600 バイト (≒ 1181KB)
IOPS_DETAIL_DATA_HOURLY	30	1440 (バイト / 日) × 30 (日) ＝	432000 バイト (≒ 422KB)
IOPS_DETAIL_DATA_DAILY	365	600 (バイト / 日) × 365 (日) ＝	219000 バイト (≒ 214KB)
IOPS_PROBE_DATA_CACHE	7	50400 (バイト / 日) × 7 (日) ＝	352800 バイト (≒ 354KB)
IOPS_PROBE_DATA	30	4200 (バイト / 日) × 30 (日) ＝	126000 バイト (≒ 123KB)
IOPS_PROBE_DATA_DAILY	365	175 (バイト / 日) × 365 (日) ＝	63875 バイト (≒ 62KB)
		データベース領域の合計＝	≒ 2356KB または ≒ 2.3MB

上記 (1 日のデータをデフォルトで 365 日間保存する例) で示した計算と保存日数に基づき算出すると、5 分間隔で測定される 1 つの HTTP 監視対象サービスに対して 1 年間に必要なデータベースの記憶領域の合計は、約 2356 キロバイト、つまり 2.3 メガバイトです。この場合、次の計算式を使用すると、複数の監視対象サービスで 1 年間に必要なデータベース領域を計算できます。

すべての監視対象サービスのデータ記憶領域の合計 ＝ 2.3 MB × 監視対象サービスの数

予測されるデータベースのサイズが利用可能な容量より大きい場合は、設定可能な項目を以下のように調整することで、保存されるデータの量を減らすことができます。

- プローブロケーションの数を減らす
- プローブ頻度を減らす (プローブ間隔を長くする)
- 複数ステップ HTTP_TRANS 管理対象サービスのステップ数を制限する
- 顧客 / サービスグループの組み合わせの数を減らす
- データの保持期間を短くして、保持するデータを少なくする

データアクセスのパフォーマンス

保存するデータの量は、OVIS ダッシュボードの応答性、夜間レポートの生成にかかる時間、および、定期的なデータベースのメンテナンスと集約オペレーションにかかる時間に影響します。データベースの記憶容量に余裕があって非常に大きなテーブル (つまりレコードが 1000 万個以上あるようなテーブル) を保存できる場合でも、それほどにまでテーブルサイズが大きいと、それらに対するクエリアクセスのパフォーマンスは、ダッシュボードの応答速度が受け入れられないほど低下します。また、データベースのメンテナンス機能と集約機能が、新しい着信データに対応できなくなります。

ダッシュボードの応答性

ダッシュボードの応答性は、データベースでのデータ量だけでなく、リクエストされたデータの量によっても変わってきます。またリクエストの処理にかかる時間は、顧客の数が多いほど長くなります。さらに、時間間隔もダッシュボードの応答性に直接影響します。

グループ分けを粗くして時間間隔も長くすると、リクエストにかかる時間は長くなると予想されます。しかし、グループ分けを細かくして時間間隔も 4 時間以内にすれば、応答時間が 30 ～ 60 秒より長くなることはないと考えられます。ダッシュボードを使ったモニタリングでは応答性が重要ですが、通常の使用形態では、この程度の応答性で十分です。

ダッシュボードの応答性が受け入れられないほど長い場合は、応答時間を短くします。その方法としては、以下のオプションがあります。

- リクエストデータを少なくする : 顧客 / サービスのグループ分けを細かくするとともに、間隔を短くします。

- ダッシュボードの利用を、承認されているユーザーの中の一部の人に限定する : ダッシュボードを使用している Web クライアントの数が多すぎると、どのリクエストの応答性も低下します。
- ブラウザに読み込んだダッシュボードを使用しないときは、ダッシュボードを表示したままにしておかない : ダッシュボードの [状況] ワークスペースには自動リフレッシュ機能があるので、ダッシュボードのデータを使用しないで開いたままにしておくと、定期的なリフレッシュのために OVIS 管理サーバー からデータベースへクエリーが発行され続けます。
- OVIS 管理サーバーとデータベースサーバーでシステムとネットワークのパフォーマンスを定期的にモニターして、ハードウェアリソースが十分に利用できるようにする。
- データの保持サイクル (保持日数) を短く設定するとともに前の項で示した他のガイドラインに従って、データベースのデータ量を減らす。
- 以下のようにして、データベースのパフォーマンスを最適な状態で維持する。
  - インデックスを定期的に再構築 / コンパクト化して、最適な状態に保つ。
  - Oracle Analyze などのクエリーアナライザ機能を定期的に実行する。特に、データベースのサイズが増大したときに実行します。
  - テーブルのサイズを適切な範囲におさえる。
  - メモリの割当てを適切に行う : 使用できるメモリーに基づいてデータベースのバッファキャッシュサイズとプールサイズを最大化します。

OVIS 管理サーバーでダッシュボードの処理要求が著しく増えているかどうかは、システムパフォーマンスモニターを使って `RepIops` という名前のリクエスト生成プロセスを調べればわかります。

データベースのメンテナンスと集約

データベースのメンテナンスについては、1 時間分のメンテナンスが 5 分間隔で行われれ、1 日分のメンテナンスが毎時間行われます。集約については、OVIS の `IopsCollector` プロセスが 5 分ごとにトレースデータを集約します。また `IopsMaint` プロセスがその他のメンテナンス機能と集約機能を 5 分単位と 1 時間単位で実行します。一方、データの削除については、`Repmaint` プロセスが夜間に実行されて、指定保持日数より古くなったデータを Reporter のデータベースから削除します。

処理能力に余裕があってデータベースのサイズも適度な通常の動作環境では、これらのプロセスが比較的短い時間 (1 分以内) で処理を完了する必要があります。パフォーマンスモニターを使ってこれらのプロセスを追った結果、その実行時間が非常に長くなっていて次の間隔へくいこんでいれば、データの着信レートに追いつけなくなっています。

このような状況になったら、データベースの集約時間とメンテナンス時間を減らします。その方法としては、次のオプションがあります。

- OVIS 管理サーバーとデータベースサーバーでシステムとネットワークのパフォーマンスを定期的にモニターして、ハードウェアリソースが十分に利用できるようにする。
- データの保持サイクル (保持日数) を短く設定するとともに前の項で示した他のガイドラインに従って、データベースのデータの量を減らす。
- 以下のようにして、データベースのパフォーマンスを最適な状態で維持する。
  - インデックスを定期的に再構築 / コンパクト化して、最適な状態に保つ。
  - Oracle Analyze などのクエリーアナライザ機能を定期的に実行する。特に、データベースのサイズが増大したときに実行します。
  - テーブルのサイズを適切な範囲におさえる。
  - メモリの割当てを適切に行う : 使用できるメモリーに基づいてデータベースのバッファキャッシュサイズとプールサイズを最大化します。

レポートの作成

特に指定しない限り、夜間のレポート作成は午前 3 時に開始されます。このレポートの作成にかかる時間は、データベースのサイズと、使用できる OVIS 管理サーバーの処理能力によって大きく影響されます。レポートの作成処理は CPU にかなり負担がかかるので、CPU リソースが十分に利用できる夜間にレポートを作成させます。

そのため、レポートの作成サイクルは、営業日の最繁時間帯に合わせて管理サーバーの他のアクティビティが増加する翌朝までに、完了させる必要があります。CPU に負荷のかかるレポート作成サイクルが朝にまでずれ込むと、午前中にそのレポートが入手できなくなるだけでなく、レポートの作成処理自体で、最繁時の負荷を処理するために必要な他のアクティビティにも影響が出てしまいます。

このような状況になったら、レポートの作成にかかる時間を減らします。その方法としては、次のオプションがあります。

- 使用していないプローブタイプについて、不要なレポートパッケージを削除する。182 ページの「未使用の OVTA レポートの削除」を参照してください。
- ダウンタイムのスケジュール設定機能を使って、休みなく監視を行う必要があるプローブを閑散時にだけ無効にする。このようにすれば、OVIS 管理サーバーが閑散時に不要な処理を行わないようになるため、レポート作成タスクにリソースを最大限割り当てることができます。
- OVIS 管理サーバーとデータベースサーバーでシステムとネットワークのパフォーマンスを定期的にモニターして、ハードウェアリソースが十分利用できるようにする。
- データの保持サイクル (保持日数) を短く設定するとともに前の項で示した他のガイドラインに従って、データベースのデータ量を減らす。
- 以下のようにして、データベースのパフォーマンスを最適な状態で維持する。
  - インデックスを定期的に再構築 / コンパクト化して、最適な状態に保つ。
  - Oracle Analyze などのクエリーアナライザ機能を定期的に実行する。特に、データベースのサイズが増大したときに実行します。
  - テーブルのサイズを適切な範囲におさえる。
  - メモリの割当てを適切に行う。使用できるメモリーに基づいてデータベースのバッファキャッシュサイズとプールサイズを最大化します。

レポートの生成サイクルがいつ完了しているかは、ログファイル `Status.reporter` を調べることでわかります。また、システムパフォーマンスモニターを使えば、`RepCrys` という名前のレポート作成プロセスを見つけることができます。

NTFS セキュリティ設定

一部のファイルとディレクトリは、匿名のインターネットユーザーアカウント (`IUSR_<machine name>`) によってアクセスおよび変更できる必要があります。パス `Program Files¥HP OpenView` は、デフォルトのディレクトリであり、イ

ンストール時に設定を上書きすることができます。Internet Services のインストールプログラムは、ユーザー IUSR_<machine name> に以下の NTFS パーミッションを設定します。

表 16　　ユーザー IUSR に設定される NTFS パーミッション

パス	ACL の編集 / 置換	サブディレクトリを含むかどうか	パーミッション	コメント
¥Program Files¥HP OpenView	編集	含む	読み取り (RX)	
¥Program Files¥HP OpenView¥Data	編集	含む	変更 (RXWD)	
¥Program Files¥Common Files¥	編集	含む	読み取り (RX)	ODBC 構成
¥<Temp>	編集	含まない	変更 (RXWD)	
¥<Winnt>¥system32	編集	含まない	読み取り (RX)	
¥<Winnt>¥system32¥*.*	編集	含まない	読み取り (RX)	
¥<Winnt>¥system32¥inetsrv	編集	含まない	読み取り (RX)	
¥<Winnt>¥system32¥	編集	含む	読み取り (RX)	
inetsrv¥asp	編集			* 存在しない可能性あり

表 17　　ローカルの「Administrator」グループに明示的に設定される NTFS パーミッション

パス	ACL の編集 / 置換	サブディレクトリを含むかどうか	パーミッション	コメント
¥Program Files¥HP OpenView	編集	含む	フルコントロール	
¥Program Files¥HP OpenView¥Data	編集	含む	フルコントロール	
¥<Temp>	編集	含む	フルコントロール	

表 18　　「SYSTEM」アカウントに設定される NTFS パーミッション

パス	ACL の編集 / 置換	サブディレクトリを含むかどうか	パーミッション	コメント
¥Program Files¥HP OpenView	編集	含む	フルコントロール	

表 19　　レジストリ設定

パス	ACL の編集 / 置換	パーミッション	コメント
Path = HKEY_LOCAL_MACHINE¥SOFTWARE¥ODBC¥ODBC.INI¥Reporter	編集	読み取り (RX)	
Path = HKEY_LOCAL_MACHINE¥SOFTWARE¥ODBC¥ODBC.INI¥IopsTraceTable	編集	読み取り (RX)	

IUSR に対する Internet Services IIS 仮想ディレクトリの実行パーミッションは以下のとおりです。

表 20　　ユーザー IUSR の IIS パーミッション

パス	実行パーミッション
HPOV_IOPS	スクリプトのみ
HPOV_IOPS¥cgi-bin	スクリプトおよび実行可能ファイル
HPOV_IOPS¥isapi	スクリプトおよび実行可能ファイル
HPOV_IOPS¥java	スクリプトおよび実行可能ファイル
HPOV_reports	スクリプトのみ (すべてのサブディレクトリを含む)
HPOV_Help	スクリプトのみ (すべてのサブディレクトリを含む)

Windows 2003 の Internet Services では、IWAM と NETWORK_SERVICE ユーザーを次のように設定します。

IWAM, full control on:

Program Files¥HP OpenView¥data¥datafiles¥IopsTraceTable.mdb

Program Files¥HP OpenView¥data¥tmp¥probe

NETWORK_SERVICE, full control on:

Program Files¥HP OpenView¥data

Program Files¥HP OpenView¥data¥*.*

Program Files¥HP OpenView¥data¥datafiles¥IopsTraceTable.mdb

索引

N

O

P

Q

R

S

T

U

W

X

あ

か

さ

た

な

は

ま

や

ら