



HP Network Capture

ソフトウェアバージョン: 7.11

ユーザーズ・ガイド

ドキュメントリリース日: 2015 年 6 月 (英語版)
ソフトウェアリリース日: 2015 年 6 月

ご注意

保証

HP製品、またはサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。ここでの記載は、追加保証を提供するものではありません。ここに含まれる技術的、編集上の誤り、または欠如について、HPはいかなる責任も負いません。

ここに記載する情報は、予告なしに変更されることがあります。

権利の制限

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPからの有効な使用許諾が必要です。商用コンピューターソフトウェア、コンピューターソフトウェアに関する文書類、および商用アイテムの技術データは、FAR12.211および12.212の規定に従い、ベンダーの標準商用ライセンスに基づいて米国政府に使用許諾が付与されます。

著作権について

© Copyright 2002 - 2015 Hewlett-Packard Development Company, L.P.

商標について

Adobe® は、Adobe Systems Incorporated (アドビシステムズ社) の登録商標です。

Microsoft® およびWindows® は、米国におけるMicrosoft Corporationの登録商標です。

UNIX® は、The Open Groupの登録商標です。

ドキュメントの更新情報

このマニュアルの表紙には、以下の識別情報が記載されています。

- ソフトウェアバージョンの番号は、ソフトウェアのバージョンを示します。
- ドキュメントリリース日は、ドキュメントが更新されるたびに変更されます。
- ソフトウェアリリース日は、このバージョンのソフトウェアのリリース期日を表します。

更新状況、およびご使用のドキュメントが最新版かどうかは、次のサイトで確認できます。

<https://softwaresupport.hp.com>

このサイトを利用するには、HP Passportへの登録とサインインが必要です。HP Passport IDの登録は、次のWebサイトから行なうことができます。<https://softwaresupport.hp.com> にアクセスして、[Register] をクリックしてください。

サポート

HPソフトウェアサポートオンラインWebサイトを参照してください。<https://softwaresupport.hp.com>

このサイトでは、HPのお客様窓口のほか、HPソフトウェアが提供する製品、サービス、およびサポートに関する詳細情報をご覧いただけます。

HPソフトウェアオンラインではセルフソルブ機能を提供しています。お客様のビジネスを管理するのに必要な対話型の技術サポートツールに、素早く効率的にアクセスできます。HPソフトウェアサポートのWebサイトでは、次のようなことができます。

- 関心のあるナレッジドキュメントの検索
- サポートケースの登録とエンハンスメント要求のトラッキング
- ソフトウェアパッチのダウンロード
- サポート契約の管理
- HPサポート窓口の検索
- 利用可能なサービスに関する情報の閲覧
- 他のソフトウェアカスタマーとの意見交換
- ソフトウェアトレーニングの検索と登録

一部のサポートを除き、サポートのご利用には、HP Passportユーザーとしてご登録の上、サインインしていただく必要があります。また、多くのサポートのご利用には、サポート契約が必要です。HP Passport IDを登録するには、次のWebサイトにアクセスしてください。 <https://softwaresupport.hp.com> にアクセスして、[Register] をクリックしてください。

アクセスレベルの詳細については、次のWebサイトをご覧ください。

<https://softwaresupport.hp.com/web/softwaresupport/access-levels>

HP Software Solutions統合とベストプラクティス

HP Software Solutions Now (<https://h20230.www2.hp.com/sc/solutions/index.jsp>) では、HPソフトウェアのカタログ記載製品がどのような仕組みで連携、情報の交換、ビジネスニーズの解決に対応するのかが確認いただけます。

Cross Portfolio Best Practices Library (<https://hpln.hp.com/group/best-practices-hpsw>) では、ベストプラクティスに関するさまざまなドキュメントや資料をご覧ください。

目次

HP Network Capture	6
どのメトリックを選択すべきか	8
測定精度を高めるためのヒント	11
インストールとアップグレード	13
Network Capture のインストール	14
システム要件とリソース使用率	15
Network Capture でのセキュア通信	17
Network Capture サーバのインストール	19
Network Capture エージェントのインストール	21
Network Capture エージェントのインストール	21
Network Capture エージェントのアンインストール	22
ファイアウォール構成	23
インストールの取り消し	25
アップグレードの互換性	26
ログ・ファイルと構成ファイル	27
ログイン	28
Network Capture のライセンス管理	29
インストール後の通信のセキュリティ保護の切り替え	31
セキュリティ保護された通信の有効化	32
セキュリティ保護された通信の無効化	33
Network Capture の使用	34
操作	35
エンドポイントの作成	35
モニタの構成	37
モニタ用フォルダの追加と削除	38
同時帯域幅モニタのインターバルの定義	39
遅延とパケット損失の構成	40
帯域幅の構成	42
Web サーバ・パラメータの構成	44
モニタリングの開始	45
データの表示	45
拡大と縮小	48
データの検索	51
データの分析	51
パフォーマンス統計情報	52

ネットワーク・プロファイルの使用	52
データのエクスポート	55
ユーザの定義と更新	56
アカウント設定	57
スケジュールの設定	58
よくある質問とトラブルシューティング	58
テクニカル・サポート	63
フィードバックをお送りください	65

HP Network Capture

HP の Network Capture では実際のネットワーク条件を記録することで、ネットワーク環境をプリプロダクションおよびテスト用ラボにインポートして再現できます。さらに、ネットワーク・プロファイルでは、世界中の主要都市のモバイル・ユーザやブロードバンド・インターネット・ユーザの実際のネットワーク条件を含むデータを利用します。このデータは、HP のアプリケーションを使用して、分散アプリケーションのパフォーマンスを正確に評価・分析するのに使用します。

ネットワーク条件を記録するのは、多くの場合、さまざまなネットワーク・パラメータにアプリケーションがどのように反応するかを確認することが目的です。データ・サーバの統合を行う場合、実稼働のネットワーク条件で各種アプリケーションがどのように動作するかを確認する場合、新機能をテストする場合、ビジネス・プロセスが実稼働環境で正しく動作することを確認する場合などがあります。

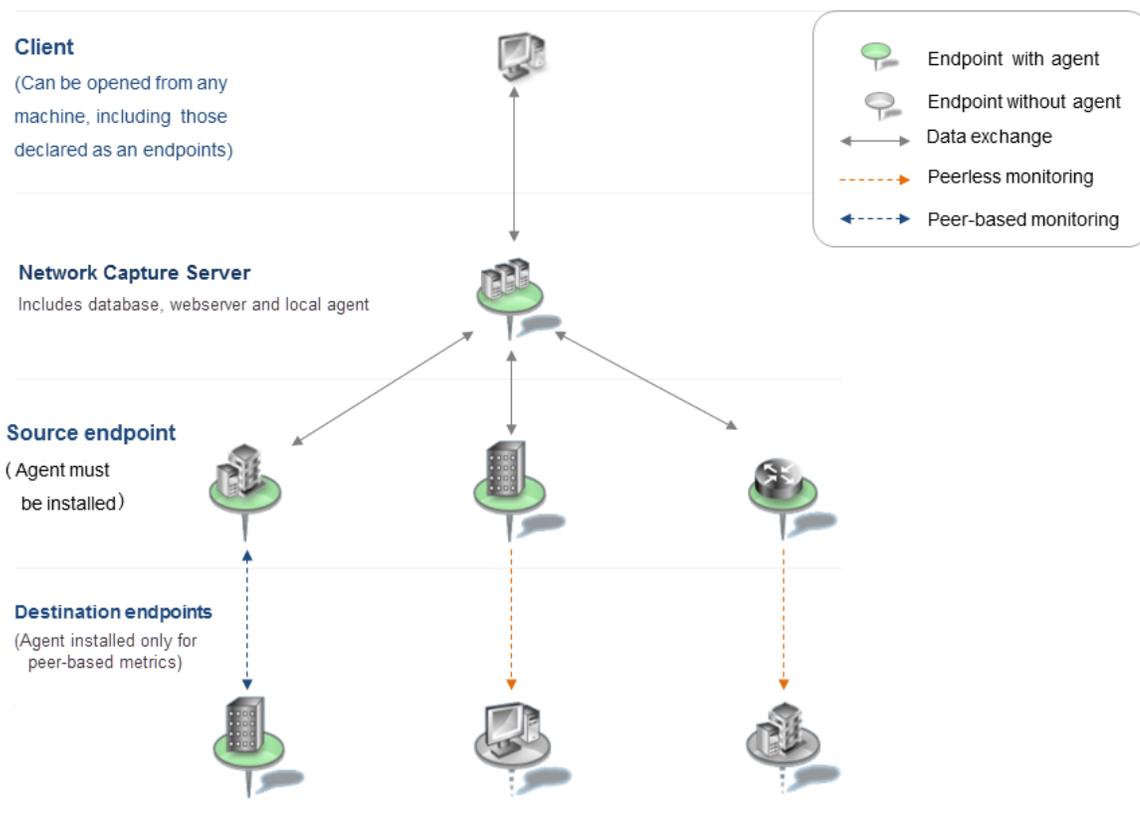
Network Capture を使用し、特定のネットワーク・トポロジ内での遅延、パケット損失、帯域幅の可用性などのネットワーク条件を測定することで、リモートの場所で発生しているアプリケーション・パフォーマンスの問題を記録して識別します。Network Capture では、世界中の実稼働用ネットワークを最長 1 か月にわたって測定できます。

記録が完了したら、レポート用にデータをエクスポートできます。また、HP のネットワーク・エミュレーション製品で記録したネットワーク条件をエミュレートすることもできます。実行全体をエクスポートすることも、実行中の特定期間（遅延が最も大きな期間など）をエクスポートすることもできます。

Network Capture の Web ベースのインタフェースでは、最大 25 のリンクを同時に記録でき（ライセンスに依存）、実際の場所を動的なマップに表示できます。また、特定のモニタ、ユーザ、および結果を容易に検索できます。モニタのスケジュール設定では、さまざまな時間にモニタを起動および停止し、さまざまな期間にわたって実行できます。必要に応じて反復を使用することもできます。

Network Capture の強力な分析オプションを利用すると、記録したデータから最低、平均、最高の条件を選択できます。各種の測定や計算により、さまざまな条件でアプリケーションの応答時間を評価するのに使用できる詳細な情報を得ることができます。

次の図は、Network Capture 構成内でのコンポーネントの関係を表しています。



複数のメトリックの同時測定

遅延、損失、ジッタは同時に測定できますが、帯域幅を平行して測定することはできません。これは測定の精度に影響するためです。そのため、Network Capture では、帯域幅の測定と遅延、パケット損失およびジッタの測定との間での配分率（システム全体での時間割り当て）が最適化されます。

最高のシステム構成条件では、測定期間の少なくとも 75% が遅延、損失、ジッタの測定に割り当てられ、最大 ±25% が帯域幅に割り当てられます。最低のネットワーク構成条件で測定を行う場合は、測定期間の少なくとも ±75% が遅延、損失、ジッタに割り当てられます。詳細については、[「同時帯域幅モニタのインターバルの定義」\(39ページ\)](#)を参照してください。

スケジューリング・アルゴリズムは、トポロジの中心（ルート）がすべてのモニタのソースとして設定されるスター型トポロジをサポートするように最適化され自動的に調整されます。

関連項目：

- [「どのメトリックを選択すべきか」\(8ページ\)](#)
- [「測定精度を高めるためのヒント」\(11ページ\)](#)

どのメトリックを選択すべきか

次の表は、ネットワーク条件を測定するのに使用する各メトリックの特徴を比較したものです。

注: エンドポイントでCPU 負荷の高いプロセスが実行されている場合、すべてのメトリックの精度が低下します。負荷を発生させるタスクをエンドポイント・マシンで実行しないようにする必要があります。Network Capture トラフィックをインターセプトするネットワーク・アクセラレータやプロキシ・サーバは、結果の精度を損なう可能性があります。

ネットワーク・オーバーヘッドは、プローブ・インターバルやその他の要因の影響を受けます。

メトリック	要件	最も精度が高い場合	最も精度が低い場合	測定対象	ネットワーク・オーバーヘッド
ICMP エコー (Ping)	ICMP 要求に回答するようにターゲット・マシンを構成すること。	ICMP パケットが UDP および TCP パケットと同じ優先度で処理される場合	ICMP パケットの優先度が低い場合	ICMP エコー要求およびエコー応答	最小
UDP	Network Capture エージェントが両方のエンドポイントにインストールされていること。ファイアウォールで UDP ポートが許可されていること。	一般に高精度。VOIP 動作を測定するのに最適	UDP パケットの優先度が低い場合	UDP 送信時間	最小
TCP (ピアレス)	ピアレス・ターゲットでのみ使用	一般に高精度	ターゲット・マシンで Windows	TCP 接続セッアップ (TCP ハ	最小

メトリック	要件	最も精度が高い場合	最も精度が低い場合	測定対象	ネットワーク・オーバーヘッド
	可能。選択したポートをリッスンしている TCP サーバが必要。パス上に TCP プロキシが存在しないこと。		XP が実行されている場合	エンドシェーク)	
TCP (ピアベース)	TCP 応答時間の測定に使用。Network Capture エージェントが両方のエンドポイントにインストールされていること。ファイアウォールで TCP ポートが許可されていること。	Windows 7 がオペレーティング・システムである場合	ジッタが非常に大きい場合 (パケット間で最大 3 倍の変動)。またターゲット・マシンで MS Windows XP が実行されている場合	データ・パケットごとの TCP 応答時間	最小
HTTP 応答時間	ターゲット・エンドポイントに HTTP サーバ (Web サーバなど) が必要。	HTTP 要求/ 応答のラウンドトリップ時間	サーバの HTTP 処理時間による小さな変動。プロキシやキャッシュが結果に影響することに注意	HTTP 応答時間	選択した HTTP 要求に依存 (通常は最小)。

メトリック	要件	最も精度が高い場合	最も精度が低い場合	測定対象	ネットワーク・オーバーヘッド
一方向推定	ターゲット・エンドポイントがNTP ICMP エコー、または ICMP タイムスタンプ 要求に応答すること。ソースおよびターゲット間のファイアウォールでUDP ポートが許可されていること。	受信リンクが使用可能な場合	受信リンクが輻輳し、ICMP が「Ping プロトコル」として選択されている場合	送信使用可能帯域幅	大きい
双方向推定	Network Capture エージェントが両方のエンドポイントにインストールされていること。ソースおよびターゲット・エンドポイント間のファイアウォールでUDP ポートが許可されていること。	精度の向上につながる他の依存要因なし	トラフィックがバースト性でスループットが高い場合	送信および受信使用可能帯域幅	中程度
ロバスト双	Network	帯域幅が小	トラフィッ	送信および	大きい

メトリック	要件	最も精度が高い場合	最も精度が低い場合	測定対象	ネットワーク・オーバーヘッド
方向サンプル	Capture エージェントが両方のエンドポイントにインストールされていること。ファイアウォールでTCPポートが許可されていること。	さく（50Mb未満）、ラウンドトリップ時間が小さい（120ミリ秒未満）の場合に高精度	クがバースト性でスループットが高い場合	受信使用可能帯域幅	

注:

TCP パケット損失: TCP ヘッダの確認応答が受信されない場合、オペレーティング・システムに応じて接続を確立するための再試行が（通常 3 ~ 4 回）行われます。

TCP プロトコルを使用するパケットは、次の場合に損失と定義されます。

- Network Capture で再送信の発生が検出された場合。

HTTP パケット損失:

HTTP プロトコルで測定を行う前に、両方のエンドポイント間の接続を定義する必要があります。接続が確立されると、ヘッダ要求が送信されます。

パケットは次の場合に損失とみなされます。

- モニタのエンドポイント間に接続が確立されていない。
- サーバ応答がユーザによって定義されたものではない。
- 応答時間にタイムアウト・パラメータを使用してユーザが定義した受け入れ可能な値よりも長い時間がかかる。

測定精度を高めるためのヒント

- 特定のターゲット・エンドポイントに対して一方向帯域幅を測定しているときに、同じターゲットに対して他の帯域幅メトリックを測定しないようにします。

- より精度の高い帯域幅測定値を得るには、遅延と帯域幅を同時に測定しないようにします（特に使用可能な帯域幅が小さい場合）。これは、ピアレス・メトリック（ICMP, TCP, HTTP）で帯域幅プローブと同時に測定が行われ、使用可能帯域幅の一部を使用する可能性があるためです。
- 帯域幅測定に関する関連情報については、[「同時帯域幅モニタのインターバルの定義」](#) (39ページ) を参照してください。

インストールとアップグレード

HP の Network Capture では実際のネットワーク条件を記録し、ネットワーク環境をプリプロダクションおよびテスト用ラボにインポートして再現できます。このデータは、HP Network Virtualization ネットワーク・アプライアンスおよびデスクトップ・アプリケーションを使用して、分散アプリケーションのパフォーマンスを正確に評価・分析するのに使用します。

この項では、以下の製品のインストール、アップグレード、およびライセンス管理の手順について説明します。

- [Network Capture のインストール](#) 14
- [インストールの取り消し](#) 25
- [アップグレードの互換性](#) 26
- [ログ・ファイルと構成ファイル](#) 27
- [ログイン](#) 28
- [Network Capture のライセンス管理](#) 29
- [インストール後の通信のセキュリティ保護の切り替え](#) 31

Network Capture のインストール

Network Capture サーバのインストーラでは、サーバ、Web サーバ、エージェントのコンポーネントがインストールされます。ピアベースのプローブを実行するには、Network Capture エージェントをターゲット・マシンにもインストールする必要があります。Network Capture のコンポーネントをインストールするには、Windows™ のローカルの管理者権限が必要です。

注: 一部のインストール・エラーは MS Windows インストーラのログに表示され、Network Capture のログには表示されません。詳細については、[「ログ・ファイルと構成ファイル」 \(27 ページ\)](#)を参照してください。

- [システム要件とリソース使用率](#) 15
- [Network Capture でのセキュア通信](#) 17
- [Network Capture サーバのインストール](#) 19
- [Network Capture エージェントのインストール](#) 21
- [ファイアウォール構成](#) 23

システム要件とリソース使用率

システム要件は、特定のサーバおよびエージェント・マシンでの使用状況に応じて変わる可能性があります。

エージェントに関して、次の3つの使用レベルが定義されています。

- 低：エージェント（ソースまたはターゲット）が最大5個の同時実行モニタで使用される
- 中：エージェント（ソースまたはターゲット）が最大10個の同時実行モニタで使用される
- 高：エージェント（ソースまたはターゲット）が最大25個の同時実行モニタで使用される

注: エージェントはサーバのインストールの一部としてサーバ・マシン上に必ずインストールされるため、システム要件を判断するにはエージェントの要件を考慮します。

Network Capture サーバのシステム要件

Network Capture サーバの最小要件（Web サーバ・コンポーネントを含む）は、次のとおりです。

プロセッサ	1.3 GHz（32 ビットまたは 64 ビット）
メモリ	2 GB RAM
ハードディスクの空き容量	100 GB の空きディスク容量（記録用の容量を含む）
ネットワーク・アダプタ	ネットワーク・インタフェース・カード、WIFI、携帯電話用カード、または仮想 NIC
ブラウザ	<ul style="list-style-type: none">• Internet Explorer 7.0 以上• FireFox 4.0 以上 注：サポートされる画面の解像度は 1280 x 800 以上（ズームレベル 100%）です。
オペレーティング・システム（英語版のみ）	Microsoft Windows : <ul style="list-style-type: none">• Server 2003 SP2（32/64 ビット版）• Server 2003 R2 SP2（32/64 ビット版）• Server 2008 SP2（32/64 ビット版）• Server 2008 R2（64 ビット版）• Server 2008 R2 Hyper-V（64 ビット版）• Windows 8.1（32/64 ビット版）• Windows 2012 R2（64 ビット版）
リモート・アクセス	サポート対象オペレーティング・システムの Microsoft RDP

仮想化	VMware ESXi 4.0 Windows 2008 HyperV (64 ビット版) VMware Workstation 6.0 以上
-----	--

Network Capture エージェントのシステム要件

Network Capture エージェントの要件は、次のとおりです。

プロセッサ	<ul style="list-style-type: none"> 低使用レベル : 1.3 GHz (32 ビットまたは 64 ビット) 中使用レベル : 2 GHz (32 ビットまたは 64 ビット) 高使用レベル : 3 GHz デュアルコア (32 ビットまたは 64 ビット)
メモリ	<ul style="list-style-type: none"> 低使用レベル : 1 GB RAM 中使用レベル : 2 GB RAM 高使用レベル : 4 GB RAM
ハードディスクの空き容量	1 GB の空きディスク容量
ネットワーク・アダプタ	Ethernet またはネットワーク・インタフェース・カード, WIFI, 携帯電話用カード, 仮想 NIC
仮想化	<ul style="list-style-type: none"> VMware ESXi 4.0 Windows 2008 HyperV (64 ビット版) VMware Workstation 6.0 以上
Network Capture エージェント (スタンドアロン) 英語版のみ	Microsoft Windows : <ul style="list-style-type: none"> Server 2008 SP2 (32/64 ビット版) Server 2008 R2 (64 ビット版) Windows 7 (32/64 ビット版) *
*低および中使用レベルのみ	

高使用レベルでのリソース使用率

	エージェントの CPU	サーバの CPU	エージェントのメモリ
Windows Server 2008 32 Core 2 Duo E7500 3 GHz 4 GB RAM	30%	7%	1 GB
Windows 7 Enterprise Core 2 Duo E7500 3 GHz 4 GB RAM	30%	-	1 GB

Network Capture でのセキュア通信

Network Capture では、次の通信の暗号化がサポートされています。

- クライアント（ブラウザ）から Web サーバ・コンポーネントへの通信
- Web サーバ・コンポーネントからサーバへの通信
- エージェントからサーバへの通信

Network Capture では、次の通信の暗号化はサポートされていません。

- エージェントから別のエージェントへの通信（サーバ・マシンにインストールされたローカル・エージェントを含む）

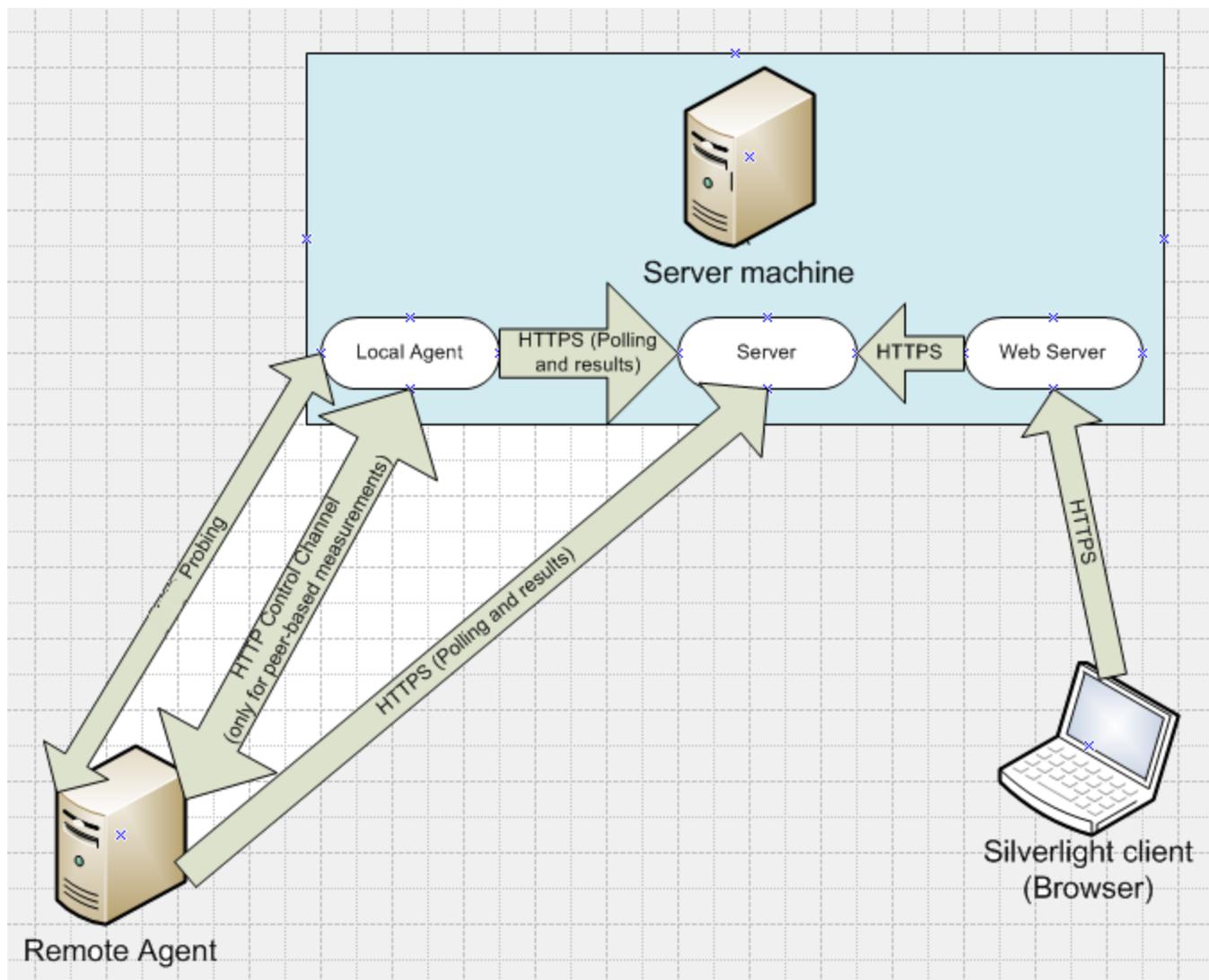
Network Capture サーバでセキュア通信を有効にすると、自己署名証明書がサーバ・マシン上に作成されます。

注: サーバとのセキュア接続中に使用されるサーバ証明書を検証する手段は、クライアントにもエージェントにも存在しません。そのため、

- ユーザが Network Capture の UI にログオンするときにセキュリティ警告が表示されます。ブラウザではサーバ証明書が認識されないため、この警告は Web ブラウザによって表示されません。
- エージェントは証明書情報を含む警告メッセージをログ記録し、警告表示なしにそれを受け入れます。

そのため、確立された接続では HTTPS が使用されていますが、中間者攻撃に対する脆弱性があります。

次の図は、サーバとエージェントでセキュア通信が有効になっている場合の、セキュア・チャネルとセキュアでないチャネルを示しています。



注: 図の「矢印」ごとにファイアウォール・ルールを定義する必要があります。詳細については、「[ファイアウォール構成](#)」(23ページ)を参照してください。

たとえば、次の構成の場合：

- リモートの Network Capture エージェントがポート 80 をリッスンしている
- Network Capture サーバがポート 443 をリッスンしている
- ローカルの Network Capture エージェントがポート 90 をリッスンしている
- モニタがローカル・エージェントをソース、リモート・エージェントを宛先として構成されており、ポート 997 (標準設定のポート) で TCP プロトコルを使用して遅延を測定している

次のチャンネルで以下のポートが使用されます。

- ソース・エージェントと宛先エージェントは、ポート 443 経由でセキュア通信を使用してパブリッシュとポーリングを行います。ソース・エージェントは結果をサーバに返します。

- 宛先エージェントで再起動やクラッシュからの回復が発生した場合、宛先エージェントはポート 90 を使用してセキュリティ保護されていない制御チャネルを介してソース・エージェントに接続します。
- ソース・エージェントはポート 80 でセキュリティ保護されていない制御チャネルを介して宛先エージェントに接続します。
- ソース・エージェントは、ポート 997 でセキュリティ保護されていない通信を使用して遅延をブロープします。

Network Capture サーバのインストール

Network Capture サーバのインストーラでは、Network Capture Web サーバとローカルの Network Capture エージェントもインストールされます。

前提条件

- **IIS** (Network Capture サーバのインストールの前にインストールしておく必要があります)。IIS 7.0 の場合は、IIS 6.0 メタベース互換を有効にする必要があります。

注: Windows 8.1 および Windows 2012 R2 では、次の設定が必要です。

- Web サーバ > HTTP 共通機能 > 静的コンテンツ
- Web サーバ > パフォーマンス > 静的および動的なコンテンツの圧縮
- .NET Framework 4.5 の機能 > WCF サービス > HTTP および TCP アクティブ化

- **MySQL Standard Edition** 以上 (以下を含む) :

- MySQL Server バージョン 5.1 以上

注:

- MySQL Server バージョン 5.5.42 および 5.5.43 はサポートされません。
- テスト済みの最新の MySQL Server バージョンは 5.6.24 です。

- MySQL Connector/NET バージョン 6.8.3 以上

注: Network Capture のインストールの完了後に、ポート設定、「root」ユーザ・パスワード、データベース接続タイプなどの MySQL 構成を変更することはできません。MySQL 構成の変更が必要な場合は、サポート (<https://softwaresupport.hp.com/>) にお問い合わせください。

- **WinPcap** 4.1.2 以上 <https://www.winpcap.org/install/default>

注: Windows 8.1 および Windows 2012 R2 の場合は、WinPcap 4.1.3 以上を使用します。

マシン上にインストールされていない場合、次のコンポーネントはサーバ・インストールの一部としてインストールされます。

- Microsoft .NET Framework 4.0 Full
- Microsoft Visual C++ 2005 SP1 再頒布可能パッケージ
- IIS の動的なコンテンツの圧縮（パフォーマンスを強化してネットワーク・リソースへの負荷を軽減することを強く推奨。マシンのリソースを追加で使用する可能性あり）

Network Capture サーバをインストールするには：

1. 管理者として **NC.Server.Setup.exe** を実行し、ウィザードの手順に従います。必要な場合は、インストール中にカスタマイズしたポートを選択できます。インストール中に、Network Capture サーバとローカル・エージェントのポート番号を変更できます。別のアプリケーション（Skype など）が標準設定のポートを使用している場合は、変更が必要になる可能性があります。

注： 動的 IP アドレスが使用されている場合、マシンの再起動時に IP アドレスが変わる可能性があるため、IP アドレスは推奨されません。ホスト名、URL、または FQDN を使用してください。

注： サーバ・マシンが NAT 越しに存在する場合は、外部アドレスのみを定義します。内部ホスト名または IP をサーバ・アドレスとして使用しないでください。サーバとともにインストールされるローカル・エージェントについては、「[Network Capture エージェントのインストール](#)」(21ページ)を参照してください。

インストール中に定義した Network Capture サーバ・ポートのポート・フォワーディングが有効になるように NAT デバイスを構成します（80\443 またはユーザ定義）。

2. インストールが完了したらホスト・マシンを再起動します。
3. Network Capture サーバおよびエージェント・サービスが稼働していることを確認します。

サーバでのセキュア保護された通信（HTTPS）の有効化

Network Capture サーバではインストール・ウィザードの中でセキュア通信（HTTPS）を有効化します。必ず **[HTTPS]** オプションを選択してください。

注： 標準設定以外のポートで HTTPS を有効にする場合は、インストール後に次の手順を実行する必要があります。

IIS マネージャの **[サイトバインド]** ダイアログ・ボックスで、次のパラメータを使用して、IIS の既定の Web サイトに対するバインドを追加します。

- 種類：https
- IP アドレス：未使用の IP アドレスすべて
- ポート：<それぞれのカスタム・ポート>
- SSL 証明書：<Network Capture で作成した証明書を選択>

セキュア通信は、インストール後にもいつでも有効にすることができます。詳細については、「[インストール後の通信のセキュリティ保護の切り替え](#)」(31ページ)を参照してください。

セキュア通信のコンポーネントの詳細については、「[Network Capture でのセキュア通信](#)」(17ページ)を参照してください。

Network Capture コンポーネントのアンインストール

次の3つのコンポーネントを個別にすべて削除します。

- Network Capture Web サーバ
- Network Capture エージェント
- Network Capture サーバ

Network Capture サーバのコンポーネントをアンインストールするには：

1. UI にログインし、実行中のすべてのモニタを停止します。
2. 記録用ファイル（標準設定では C:\Program Files\HP\NetworkCapture\CatcherFiles に存在）を、ハード・ドライブの別のフォルダまたは別の場所にバックアップします。
3. 管理者として [コントロールパネル] で [プログラムの追加と削除] アイコンをダブルクリックし、HP Network Capture コンポーネントを選択して [変更と削除] ボタンをクリックします。画面の手順に従います。

または

NC. <コンポーネント> .Setup.exe を実行して [削除] を選択し、ウィザードの手順に従います。

アンインストール中には、将来使用できるようにデータベースを保持するかどうかを選択できます。MySQL の「root」ユーザ・パスワードを知っている必要があります。

すべてのコンポーネントのアンインストールが完了したらホスト・マシンを再起動します。

Network Capture エージェントのインストール

どのような種類の測定を行う場合でも、Network Capture エージェントがソース・エンドポイントにインストールされている必要があります。加えて、双方向の帯域幅やその他のピアベースの測定では、ターゲット・エンドポイントにエージェントが必要です。詳細については、「[よくある質問とトラブルシューティング](#)」(58ページ)を参照してください。

Network Capture エージェントのインストール

前提条件

- WinPcap 4.1.2 以上

注: Windows 8.1 および Windows 2012 R2 の場合は、WinPcap 4.1.3 以上を使用します。

マシン上にインストールされていない場合、次のコンポーネントはサーバ・インストールの一部としてインストールされます。

- Microsoft .NET Framework 4.0 Full
- Microsoft Visual C++ 2005 SP1 再頒布可能パッケージ

Network Capture エージェントをインストールするには：

Network Capture のユーザ・インタフェースにログインします。[Options (オプション)] メニューから [Download Agent (エージェントのダウンロード)] を選択し、**NC.Agent.Setup.exe** ファイルをダウンロードします。このファイルはインストール・パッケージでも利用できます。

注: ブラウザで、ポップアップ・ウィンドウが許可され、ブラウザのセキュリティ設定で「ファイルのダウンロード」オプションが有効になっていることを確認します。

管理者として **NC.Agent.Setup.exe** ファイルを実行し、ウィザードの手順に従います。インストール中に、Network Capture エージェントのポート番号を変更できます。別のアプリケーション (Skype など) が標準設定のポートを使用している場合は、変更が必要になる可能性があります。サーバでセキュア通信が構成されている場合は、[Secure Connection (HTTPS) (セキュア接続 (HTTPS))] オプションを選択します。セキュア通信は、インストール後いつでも有効にできます。詳細については、「[Network Capture エージェントのインストール](#)」(21ページ)を参照してください。セキュア通信のコンポーネントの詳細については、「[Network Capture でのセキュア通信](#)」(17ページ)を参照してください。

注:

- 動的 IP アドレスが使用されている場合、マシンの再起動時に IP アドレスが変わる可能性があるため、IP アドレスは推奨されません。ホスト名、URL、または FQDN を使用してください。
- Network Capture エージェントのインストール中に Network Capture サーバのアドレスとポートを指定する際には、Network Capture サーバの詳細を Network Capture サーバのインストール時に入力したのと同じ形式で入力する必要があります。

たとえば、Network Capture サーバのインストール中にホスト名を入力した場合は、Network Capture エージェントのインストール時に、IP アドレスではなく同じホスト名を使用します。

- Network Capture エージェントが NAT 越しに存在していて、同じ NAT 越しに存在しないソース・エージェントやターゲット・エージェントと通信する必要がある場合は、内部アドレスと外部アドレスの両方を指定する必要があります。インストール中に定義した Network Capture エージェントのポートのポート・フォワーディングが有効になるように NAT デバイスを構成します (80 またはユーザ定義)。加えて、モニタで使用する任意のメトリックのポートのポート・フォワーディングを有効にします。詳細については、「[ファイアウォール構成](#)」(23ページ)のポートの指定を参照してください。

Network Capture エージェントのアンインストール

Network Capture エージェントをアンインストールするには：

1. UI にログインし、実行中のすべてのモニタを停止します。
2. 標準設定では \\AgentRootFolder>\Bin に存在するファイル **NC.Agent.Host.exe.GUID** をバックアップします（このファイルはすべての構成に存在しない可能性があります）。
3. 管理者として [コントロールパネル] で [プログラムの追加と削除] アイコンをダブルクリックし、[**HP Network Capture Agent (HP Network Capture エージェント)**] を選択して [変更と削除] ボタンをクリックします。画面の手順に従います。

または

NC.Agent.Setup.exe を実行して [削除] を選択し、ウィザードの手順に従います。

4. 再インストールまたはアップグレードする場合は、ファイル **NC.Agent.Host.exe.GUID** をバックアップした元のファイルに置き換えます。
5. インストールが完了したらホスト・マシンを再起動します。
6. 再インストールまたはアップグレードする場合は、次の手順を実行します。
 - a. Network Capture の UI にログインします。
 - b. [Endpoint (エンドポイント)] ページのツールバーで、[**Scan All Endpoints Availability (すべてのエンドポイントの可用性をスキャンする)**] をクリックします。同じアドレスの 2 つのエンドポイントが表示されます。ステータスが到達不可 (赤いアイコン) のエンドポイントを削除します。

ファイアウォール構成

Network Capture の内部通信とモニタリングに必要なポートがファイアウォールによってブロックされないようにします。

Network Capture サーバ

一般に次のポートが使用されます。

- 443 : セキュア通信 (オペレーティング・システムによって異なる場合があります)
- 80 : セキュアでない通信 (オペレーティング・システムによって異なる場合があります)

注: Network Capture サーバにはローカル・エージェントも含まれるため、以下の各項の説明に従って、ファイアウォール上に必要なエージェント・ポートを構成する必要があります。

Network Capture ソース・エージェント

Network Capture サーバとの通信の場合 :

- 送信 TCP ポート 80\443 (または Network Capture サーバのインストール中に定義した別の TCP ポート)

Network Capture ターゲット・エージェントとの通信の場合 :

- 送信 TCP ポート 80 (または Network Capture ターゲット・エージェントのインストール中に定義した別の TCP ポート)

次のメトリックの場合：

- **TCP ピアレス**：送信 TCP 80（または別のユーザ構成可能なポート）
- **TCP ピアベース**：送信 TCP 997（または別のユーザ構成可能なポート）
- **UDP**：送信 UDP 997（または別のユーザ構成可能なポート）
- **一方向推定**：
 - 送信 UDP 53（または別のユーザ構成可能なプローブ・ポート）
 - 送信 ICMP タイムスタンプまたは ICMP エコー応答（選択した Ping プロトコルに準拠）
- **双方向推定**：送信 UDP 998（または別のユーザ構成可能なポート）
- **ロバスト双方向サンプル**：送信 TCP 995（または別のユーザ構成可能なポート）

ターゲット・エージェント・ベースのエンドポイント

Network Capture ソース・エージェントとの通信の場合：

- 受信 TCP ポート 80（または別のユーザ構成可能な TCP ポート）がオープン

次のメトリックの場合：

- **ICMP メトリック**：ICMP エコー応答
- **TCP ピアレス**：受信 TCP 80（または別のユーザ構成可能な TCP ポート）
- **TCP ピアベース**：受信 TCP 997（または別のユーザ構成可能な TCP ポート）
- **UDP**：受信 UDP 997（または別のユーザ構成可能なポート）
- **一方向推定**：
 - 受信 UDP 53（または別のユーザ構成可能なプローブ・ポート）
 - 受信 ICMP タイムスタンプまたは ICMP エコー応答（選択した Ping プロトコルに準拠）
- **タイムスタンプ\ICMP Echo 応答\受信 UDP**：123（選択した Ping プロトコルに準拠）
- **双方向推定**：受信 UDP 998（または別のユーザ構成可能なポート）
- **ロバスト双方向サンプル**：受信 TCP 995（または別のユーザ構成可能なポート）

ターゲット・エージェント・レスのエンドポイント

次のメトリックの場合：

- **ICMP**：ICMP エコー応答
- **TCP ピアレス**：（受信 TCP 80\カスタマイズ済み）
- **一方向推定**：
 - 受信 UDP 53（または別のユーザ構成可能なプローブ・ポート）
 - 受信 ICMP タイムスタンプまたは ICMP エコー応答（選択した Ping プロトコルに準拠）

インストールの取り消し

インストールが停止した場合、Network Capture では2つの方法を利用して PC を以前の状態に戻すことができます。

インストールのロールバック

- ロールバックは統合された機能です。ロールバックをトリガするのにユーザ操作は必要ありません。
- ロールバック・アクションはセットアップが中止されたときにトリガされます（自動エラー処理または手動キャンセル処理）。
- セットアップ・プログラムによって実行された変更は取り消されます。
 - インストールされたファイルは削除されます。
 - 追加されたショートカットやレジストリ・エントリも削除されます。
 - インストールによって作成された新規ディレクトリおよびログ・ファイルは削除されません。

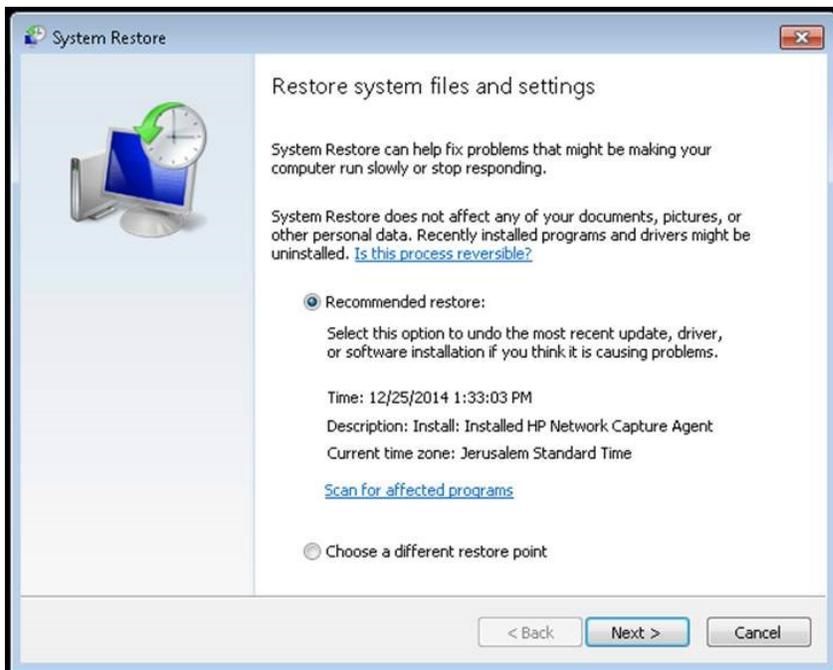
システム復元ポイント

ソフトウェアのインストール中に PC に破損が生じた場合は、Windows の標準機能であるシステムの復元を実行できます。この機能は、PC への重要なシステム変更を自動的に監視して記録します。Network Capture のインストールはシステムの復元をサポートしており、ファイル転送の開始前を含めて複数のシステム復元ポイントが設定されます。システムの復元ウィザードを使用すると、システムを最新の正常な復元ポイントに戻すことができます。または、別の復元ポイントを手動で選択することもできます。

注: Windows のすべてのバージョンでシステムの復元が使用される訳ではありません。

- サポート対象のバージョン（これらに限定されません）：Windows XP, Windows 7, Windows 8
- サポート対象外のバージョン（これらに限定されません）：Windows Server 2008

システムの復元を開始するには、[スタート] > [システムの復元] を選択します。



アップグレードの互換性

Network Capture v6.0 または v7.0 から v7.11 へのアップグレード

注: HP Network Capture の以前のバージョンは、Shunra NetworkCatcher v6.0 または v7.0 です。

Network Capture サーバをアップグレードするには :

注: 以前のバージョンの HP Network Capture から Network Capture v7.11 にアップグレードする場合、すべてのエージェントに v6.0 または v7.0 で定義されていたのと同じ値の名前とアドレスを形式どおりに指定する必要があります。

1. MySQL の「NC」および「Security」データベースをバックアップし、必要に応じて元のデータにアクセスできるようにします。標準設定では、データベースは次の場所にあります。
 - Win 2003 の場合 : C:\Documents and Settings\All Users\Application Data\MySQL\MySQL Server 5.1\Data
 - Win 2008, Win 8.1, Win 2012 R2 の場合 : C:\ProgramData\MySQL\MySQL Server 5.1\data
2. Network Capture にログインし、実行中のすべてのモニタを停止します。
3. すべての Network Capture コンポーネントをアンインストールします。 [「Network Capture コンポーネントのアンインストール」 \(21ページ\)](#) を参照してください。
4. Network Capture サーバ v7.11 をインストールします。詳細については、 [「Network Capture の](#)

[インストール](#) (14ページ)を参照してください。ライセンスの問題が生じるのを回避するため、必ず元のインストール・パスに Network Capture サーバをインストールするようにします。

注: 既存のデータベースが非常に大きい場合、インストールに時間がかかる可能性があります。データの破損を回避するため、インストールを途中で中断しないでください。

5. ホスト・コンピュータを再起動します。

リモート・エージェントのアップグレード

1. 標準設定では `\<AgentRootFolder>\Bin` に存在するファイル `NC.Agent.Host.exe.GUID` (v7.0 からアップグレードする場合) をバックアップします。
2. Network Capture エージェントをアンインストールします。 [「Network Capture エージェントのアンインストール」](#) (22ページ)を参照してください。
3. 新しくインストールした Network Capture のユーザ・インタフェースにログインします。
[Options (オプション)] メニューから [Download Agent (エージェントのダウンロード)] を選択し、`NC.Agent.Setup.exe` ファイルをダウンロードします。このファイルはインストール・パッケージでも利用できます。
4. Network Capture エージェントをインストールします。詳細については、 [「Network Capture エージェントのインストール」](#) (21ページ)を参照してください。
5. ファイル `NC.Agent.Host.exe.GUID` をバックアップした元のファイルに置き換えます (v7.0 からアップグレードする場合)。
6. Network Capture の UI にログインします。
7. [Endpoint (エンドポイント)] ページのツールバーで、[Scan All Endpoints Availability (すべてのエンドポイントの可用性をスキャンする)] をクリックします。同じアドレスの2つのエンドポイントが表示されます。ステータスが「到達不可」(赤いアイコン)のエンドポイントを削除します。

ログ・ファイルと構成ファイル

標準設定のログ・レベルは「Info (情報)」です。このログ・レベルでは問題のみが示され、説明は記載されません。ログ・レベルは、コンポーネントごとに構成ファイルで「Error (エラー)」やその他のレベルに変更できます。

構成ファイル

ログ・レベルを変更するための構成ファイルは、標準設定では次の場所に配置されます。

- **サーバ** : `NC.Server.Host.exe.config` (...\HP\Network Capture\Server\Bin)
- **エージェント** : `NC.Agent.Host.exe.config` (...\HP\Network Capture\Agent\Bin)
- **Web サーバ** : `web.config` (...\HP\Network Capture\Web Server\)

ログ・ファイル

次にサポートされるログ・レベルを示します（情報量の多い順に記載）。

- **DEBUG（デバッグ）**：最も詳細な情報で、各データベース操作をログ記録します。サーバの動作が著しく遅くなります。
- **INFO（情報）**：通常の問題のトラブルシューティングを行うのに十分な情報を提供します。
- **WARN（警告）**：警告のみ
- **ERROR（エラー）**：問題が発生したことを示します。一般にトラブルシューティングを行うのに十分な情報は含まれません。

64 ビット・システムでは、ログ・ファイルは標準設定では次のフォルダに存在します。

- C:\Program Files (x86)\HP\Network Capture\Server（または Agent または Web Server）\Logs

32 ビット・システムでは、ログ・ファイルは標準設定では次のフォルダに存在します。

- C:\Program Files\HP\Network Capture\Server（または Agent または Web Server）\Logs
- 割り当てられた記憶容量を超えると、以前のログ・ファイルが上書きされます。

MS Windows インストーラのログ

一部のインストール・エラーは MS Windows インストーラのログに表示され、Network Capture のログには表示されません。通常、これらのログはトラブルシューティングを行う場合に必要になります。

- セットアップのログは \%Temp% フォルダに配置されます。
- Windows インストーラのログは標準設定では生成されません。 \%Temp フォルダ内のログを表示するには、次のキーをインストール前にレジストリに追加する必要があります。

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer] "Logging"="voicewarmupx"

ログイン

Network Capture サーバがインストールされたら、ブラウザで次の URL にアクセスします：**http(s):// <Network Capture サーバ・アドレス>/network_capture**

ユーザ名とパスワードには **Administrator/Administrator** を使用し、その後アクセスを制限するためユーザ名とパスワードを変更します。

注: Network Capture のユーザ・インタフェースを初めて開いたときに、Microsoft Silverlight がインストールされます。Web サーバ・コンポーネントからコンテンツが転送されるため、最初のログインには数分かかることがあります。

Network Capture のライセンス管理

Network Capture **試用ライセンス**で利用できる機能：

- 最大 10 の同時実行モニタ
- 最大 100 のエンドポイント
- 30 日間の使用期限（実行ごとに最大 7 日間記録可能）

Network Capture **標準ライセンス**で利用できる機能：

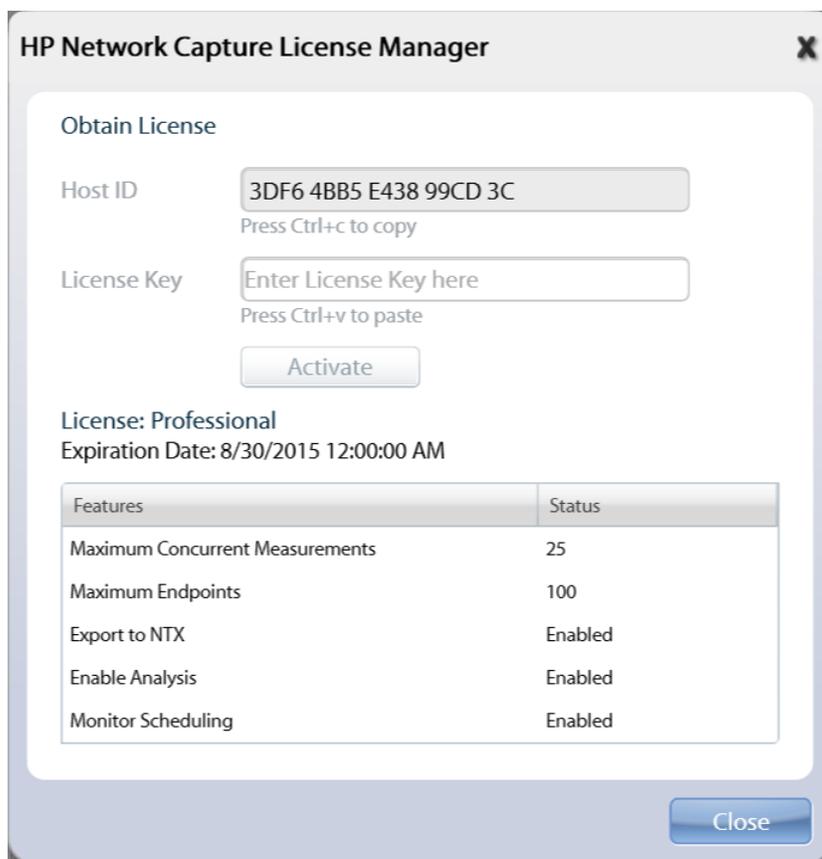
- 最大 25 の同時実行モニタ
- 最大 100 のエンドポイント
- 分析
- スケジュール設定
- エクスポート
- 使用期限なし（実行ごとに最大 31 日間記録可能）

ライセンス・キーの要求とインストール

試用ライセンスが期限切れになったら、ホスト ID を HP に送信してライセンスを取得する必要があります。ホスト ID はライセンス・キーを生成するのに使用します。ライセンス・キーは 1 営業日以内に電子メールで返送されます。Network Capture License Manager で受け取ったライセンス・キーを入力します。

ライセンス・キーを要求するには：

1. Network Capture の UI に Network Capture の管理者としてログインします。
2. ツールバーから、**[Options (オプション)]** > **[License Manager]** をクリックします。



3. ホスト ID を記録します。
4. HP Licensing サイト (<http://www.hp.com/software/licensing>) にアクセスし、次のいずれかを実行します。
 - 有効なライセンスの EON (Entitlement Order Number) を持っている場合は、EON を入力してライセンスをアクティブ化します。
 - 新規ライセンスを取得する場合は、[Contact HP Licensing (HP Licensing に問い合わせる)] をクリックして地域のライセンス・サポート・センタを見つけます。

ライセンス・アクティブ化要求は HP ライセンス・チームに送付されます。HP ライセンス・チームから連絡して、お使いの Network Capture マシンのホスト ID を要求します。

ライセンスをインストールするには：

1. Network Capture の管理者として、ツールバーから、[Options (オプション)] > [License Manager] をクリックします。
2. [License Key (ライセンスキー)] テキスト・フィールドに、HP から提供されたライセンス・キーを入力します。[Activate (アクティブ化)] ボタンがアクティブになります。
3. [Activate (アクティブ化)] をクリックし、続いて [Close (閉じる)] をクリックします。

インストール後の通信のセキュリティ保護の切り替え

この項には、次の内容が含まれます。

- [セキュリティ保護された通信の有効化](#)32
- [セキュリティ保護された通信の無効化](#)33

セキュリティ保護された通信の有効化

Network Capture サーバでセキュリティ保護された通信を有効にするには：

1. Network Capture の UI で、実行中のすべてのモニタを停止します。

注: IIS 役割サービスである「IIS 6.0 メタベース互換」がインストールされている必要があります。

2. コマンド・ウィンドウを開きます（ [スタート] > [ファイル名を指定して実行] > CMD ）。
3. <サーバ・ルート・ディレクトリ>\bin ディレクトリに移動し、次のコマンドを実行します。

```
SimpleNCServerSecurity.exe -m=all -s -p=<customized port (default is 443)>
```

注:

- 次の構成を実行する前に、このコマンドを最初に「試行」として実行することをお勧めします。

```
SimpleNCServerSecurity.exe -m=all -s -p=<customized port/default is 443> -n
```

出力ウィンドウにエラーが表示されないことを確認します。

- 標準設定以外のポートで HTTPS を有効にする場合は、インストール後に次の手順を実行する必要があります。

IIS マネージャの [サイトバインド] ダイアログ・ボックスで、次のパラメータを使用して、IIS の既定の Web サイトに対するバインドを追加します。

種類：https

IP アドレス：未使用の IP アドレスすべて

ポート：<それぞれのカスタム・ポート>

SSL 証明書：<Network Capture で作成した証明書を選択>

4. HP Network Capture サーバ・サービスを再起動します。
5. ローカル・エージェント・モードの変更については、次の項を参照してください。

エージェントでセキュア通信を有効にするには：

1. UI にログインし、実行中のすべてのモニタを停止します。
2. Network Capture エージェントをアンインストールします。詳細については、[「Network Capture エージェントのアンインストール」](#) (22ページ)を参照してください。
3. [「Network Capture エージェントのインストール」](#) (21ページ)に従ってエージェントをインストールし、**[Secure communication (セキュア通信)]** チェックボックスを選択します。

注: エージェントを再インストールすることなく、エージェントでセキュア通信を有効にすることができます。ただし、手動のシステム構成ファイルが含まれている場合は、データが破損する可能性があります。そのため、この作業を行う際には、変更される Network

Capture エージェント・ファイルを事前にバックアップします。バックアップの手順については、サポートまでお問い合わせください (<https://softwaresupport.hp.com/>)。

4. Network Capture エージェント・サービスを再起動します。

セキュリティ保護された通信の無効化

サーバでセキュリティ保護された通信を無効にするには：

1. Network Capture の UI で、実行中のすべてのモニタを停止します。
2. コマンド・ウィンドウを開きます（ [スタート] > [ファイル名を指定して実行] > CMD ）。
3. <サーバ・ルート・ディレクトリ>\bin ディレクトリに移動し、次のコマンドを実行します。

```
SimpleNCServerSecurity.exe -m=all -p=<customized port/default is 80>
```

注: 次の構成を実行する前に、このコマンドを最初に「試行」として実行することをお勧めします。

```
SimpleNCServerSecurity.exe -m=all -p=<customized port/default is 80> -n
```

出力ウィンドウにエラーが表示されないことを確認します。

4. HP Network Capture サービスを再起動します。
5. ローカル・エージェント・モードの変更については、次の項を参照してください。

エージェントでセキュア通信（HTTPS）を無効にするには：

1. UI にログインし、実行中のすべてのモニタを停止します。
2. Network Capture エージェントをアンインストールします。詳細については、「[Network Capture エージェントのアンインストール](#)」(22ページ)を参照してください。
3. 「[Network Capture エージェントのインストール](#)」(21ページ)に従ってエージェントをインストールし、[Secure communication (セキュア通信)] チェックボックスを選択しません。

注: エージェントを再インストールすることなく、エージェントでセキュア通信を無効にすることができます。ただし、手動のシステム構成ファイルが含まれている場合は、データが破損する可能性があります。そのため、この作業を行う際には、変更される可能性のある Network Capture エージェント・ファイルを事前にバックアップします。バックアップの手順については、サポートまでお問い合わせください (<https://softwaresupport.hp.com/>)。

4. Network Capture エージェント・サービスを再起動します。

セキュア通信のコンポーネントの詳細については、「[Network Capture でのセキュア通信](#)」(17ページ)を参照してください。

Network Capture の使用

HP の Network Capture では、1 つ以上の宛先間でデータ・パケットを送受信することでネットワーク条件をモニタします。また、ネットワーク・プロファイルを作成し、特定のネットワークのネットワーク条件を提供します。概要については、[「HP Network Capture」\(6ページ\)](#)を参照してください。

ここでは、HP Network Capture の使い方とネットワーク条件を記録、分析、エクスポートする方法について説明します。

• 操作	35
• エンドポイントの作成	35
• モニタの構成	37
• モニタリングの開始	45
• データの表示	45
• データの分析	51
• ネットワーク・プロファイルの使用	52
• データのエクスポート	55
• ユーザの定義と更新	56
• スケジュールの設定	58
• よくある質問とトラブルシューティング	58
• テクニカル・サポート	63

操作

画面の解像度は 1280 x 800 以上（ズームレベル 100%）に設定することをお勧めします。Network Capture のインターフェースは 32 ビット・ブラウザのみで表示できます。

Network Capture では、複数の方法で情報の表示および入力方法をカスタマイズできます。

- アイテムを選択するには、アイテムをクリックします。たとえば、モニタの結果を表示する場合は、[ICMP] をクリックして ICMP の結果を表示します。再度クリックすると、結果は非表示になります。
- モニタや結果をツリー/リストのいずれで表示するか、マップ付き/マップなしのいずれで表示するかを選択します。
- ツリーまたはグリッド・アイコンを選択して、特定のエンドポイント、モニタ、プロファイル、またはユーザに関する詳細を表示します。

ドラッグアンドドロップ

「Monitors（モニタ）」および「Profiles（プロファイル）」表示では、ツリー内でフォルダやサブフォルダをドラッグアンドドロップできます。

マップ表示

モニタまたはエンドポイントの構成中に、[map（マップ）] アイコンをクリックして、マップを表示または非表示にすることができます。

保存

モニタなどのアイテムを離れるときに、追加内容や更新内容が自動的に保存されます。また、[Save（保存）] ボタンを選択して変更内容を手動で保存することもできます。

元に戻す

変更をキャンセルするには、[Undo（元に戻す）] ボタンを選択します。これにより、データが以前に保存されたデータに戻ります。

すべて更新

[Refresh All（すべて更新）] を使用すると、Network Capture サーバからの最新のデータがユーザ・インターフェースに表示されます。UI は 15 分おきに自動的に更新されます。

エンドポイントの作成

エンドポイントとは、所定のアドレスに存在するネットワーク・ノードを表します。モニタ内でエンドポイントはソース・エンドポイント（測定元の場所）またはターゲット（測定先）のいずれかで

す。エンドポイントは、データ・センタ、Web サーバ、アプリケーション・サーバ、ネットワーク要素などとして定義できます。ソース・エンドポイントには、Network Capture エージェントがインストールされている必要があります。ターゲット・エンドポイントでは、エージェントは特定のメトリックでのみ必要です。

エージェントがマシンにインストールされると、エージェントは UI にエンドポイントとして表示されます。そのため、エージェントをインストールする前にエンドポイントを作成しないことをお勧めします。

エンドポイントを手動で作成するには（非推奨）：

1. 管理者としてモニタ・ページから [Endpoints (エンドポイント)] を選択します。
2. [New Endpoint (新規エンドポイント)] アイコンをクリックし、以下を入力します。
 - 名前：最大 100 文字の英数字
 - アドレス：マシンのアドレス。最大 255 文字のホスト名、FQDN、IP、または URL を使用できます。

注:

- エンドポイントが NAT 越しに存在する場合は、エンドポイントの手前にある NAT デバイスのアドレスを入力し、[Advanced Settings (詳細設定)] アイコンを使用して内部アドレスを構成します。これはエンドポイントのマシン・アドレスを表し、最大 255 文字のホスト名または FQDN を使用できます。
- モニタの初期化時にサーバがソース・エージェントを認識しない場合は、DNS 解決の問題が原因になっている可能性があります。サーバがソース・エージェントを認識できるようにするため、次のいずれかを使用します。
 - 完全修飾ドメイン名（「server1.company.com」など）（このプロパティを確認するには、[マイ コンピュータ] アイコンを右クリックし、[プロパティ] を選択して [フル コンピュータ名] までスクロールします）
 - 動的 IP アドレスが使用されている場合、マシンの再起動時に IP アドレスが変わる可能性があるため、IP アドレスは推奨されません。
- タイプ：データ・センタやリモート・オフィスなどのカテゴリから 1 つを選択します。マップ上の場所に選択したタイプのアイコンが表示されます。
- 説明：エンドポイントを識別するための詳細情報を最大 255 文字で入力します（オプション）。
- HP エージェントのインストール：この場所に Network Capture エージェントをインストールする必要があるかどうかを選択します。ソース・エンドポイントの場合は必須です。

注: エージェントをインストールする前にエンドポイントを定義する場合は、エージェントのインストール時に、Network Capture の UI でエンドポイントを作成したときに定義したエージェン

トのアドレスと名前を入力する必要があります。

エンドポイントを編集するには：

エンドポイントのリストでエンドポイントを選択し、詳細を編集します。変更したデータは手動で保存できます。また、変更したエンドポイントを離れるときに自動的に保存されます。

エンドポイントを削除するには：

削除するエンドポイントを選択し、[Delete (削除)] アイコンをクリックします。

注: エンドポイントが既存のモニタで使用されている場合、エンドポイントの削除やエンドポイント・アドレスの編集を行うことはできません。

エンドポイントのステータス

	未解決：エンドポイントがホスト・マシンにインストールされる前に UI で追加されました
	到達可能：エージェントが Network Capture サーバにポーリングを行い、コマンドを取得できます
	到達不可：エージェントがポーリングを行えず、サーバからコマンドを受信できません
	エージェントレス：エージェントがインストールおよび構成されていません

エンドポイントのステータスは約 5 分ごとに更新されます。緑のアイコンはエンドポイントが到達可能で、Network Capture サーバにアクセスできることを示します。

注: 同じマシンでピアレスとピアベースの両方のエンドポイントを定義できますが、この場合、同時測定の精度が低下する可能性があります。詳細については、「[測定精度を高めるためのヒント](#)」(11ページ)を参照してください。

モニタの構成

最大で 25 のモニタを同時に実行できます (ライセンスに依存)。

- [モニタ用フォルダの追加と削除](#) 38
- [同時帯域幅モニタのインターバルの定義](#) 39
- [遅延とパケット損失の構成](#) 40
- [帯域幅の構成](#) 42
- [Web サーバ・パラメータの構成](#) 44

モニタ用フォルダの追加と削除

ツリー表示には「Monitors」ルート・フォルダが存在します。このフォルダやその他のフォルダにフォルダやサブフォルダを追加できます。また、ツリー内でフォルダをドラッグアンドドロップすることもできます。フォルダ名は最大 255 文字です。

フォルダを追加するには：

[New Folder (新規フォルダ)] アイコンをクリックし、必要な詳細情報を指定します。

サブフォルダを追加するには：

親フォルダを選択して [New Folder (新規フォルダ)] アイコンをクリックし、必要な詳細情報を指定します。

フォルダを削除するには：

フォルダまたはサブフォルダにアクティブな実行が存在しないときに、フォルダを選択し、ツールバーの [Delete (削除)] アイコンまたはキーボードの [Delete] ボタンを選択します。

モニタを構成するには：

1. [Monitors (モニタ)] ビューで、[New Monitor (新規モニタ)] アイコンをクリックします。
2. 以下を定義します。
 - **Name (名前)**：名前を入力します (最大 100 文字の英数字)。
 - **Source (ソース)**：エンドポイントを選択します (エージェントがインストールされているエンドポイントのみが表示されます)。
 - **Target (ターゲット)**：リストからエンドポイントを選択します。
 - **Duration (期間)**：スクロールまたは矢印を使用して、記録する期間を設定します。
 - 遅延と帯域幅の設定では、必要なメトリックの横のチェックボックスを選択します。設定を調整するには、メトリックの横の [Settings (設定)] ボタンをクリックします。詳細については、「[遅延とパケット損失の構成](#)」(40ページ)および「[帯域幅の構成](#)」(42ページ)を参照してください。
 - **Description (説明)**：オプション (最大 255 文字)。
3. [Save (保存)] をクリックします (モニタを離れるときにも自動的に保存されます)。パラメータは「Save (保存)」操作の際に検証されます。
4. 測定を開始するには、[Run Monitor (モニタの実行)] アイコンをクリックします。

注: 以下のメトリックで同じターゲット・エージェントに対して測定を行う場合、これらが同じモニタに存在しない場合でも、同じポートを使用する構成を指定することはできません。

ロバスト双方向サンプル帯域幅と

- TCP (ピアベース)
- TCP (ピアレス)
- HTTP

TCP (ピアベース) と

- TCP (ピアレス)
- HTTP

モニタを削除するには :

モニタが実行されていないときに、ツールバーで [Delete Monitor (モニタの削除)] アイコンをクリックします。

実行を削除するには :

結果ビューで [Delete Run (実行の削除)] (ごみ箱) アイコンをクリックします。

同時帯域幅モニタのインターバルの定義

ピアレス帯域幅測定ではソース・エージェントがプローブ中に他の測定を実行できなくなり、ピアベース帯域幅メトリックではソース・エージェントとターゲット・エージェントの両方がプローブ中に他の測定を実行できなくなります。

これにより、エージェントのキューに登録されている他のモニタの実行に遅延が発生します。輻輳を回避するため、エージェントはアクティブなモニタの帯域幅インターバル設定を再定義して、75%の遅延とパケット損失と25%の帯域幅の比率を維持します。

この比率によって、帯域幅インターバルと相互に関連する「タイム・ウィンドウ」の計算が決まります。タイム・ウィンドウは、特定のエージェントに対する帯域幅メトリックのタイプと数によって決まります。一方向帯域幅のプローブ時間は約20秒です。そのため、同一のエージェントが20秒ごとに測定するように定義された3つの一方向帯域幅モニタのソースである場合、他の測定はまったく実行されません。この状況を防ぐため、各ソース・エージェントの実際の帯域幅インターバルは次のように定義されます。

インターバル = $No \times TW$

各帯域幅メトリックは異なる係数 (C) を使用して、タイム・ウィンドウ (TW) を計算します。

ここで :

No = 特定のエージェントからの送信帯域幅測定の数

TW (タイム・ウィンドウ) = $C \times (Ni + 1)$

一方向帯域幅の場合は $C=80$

双方向帯域幅の場合は $C=20$

ロバスト双方向の場合は $C=120$

N_i =特定のエージェントへの受信帯域幅測定の数

3つの一方向帯域幅モニタを使用する上記の例では、タイム・ウィンドウは80秒（帯域幅プローブに20秒、遅延とパケット損失の測定に60秒）になります。各帯域幅モニタのインターバルは240秒になります。

注: タイム・ウィンドウはエージェントごとに計算され、その最大値によって実行中のすべてのモニタのタイム・ウィンドウが決まります。

実際のプローブ・インターバル（プローブ・サンプル間の時間）を小さくするため、以下を推奨します。

- 標準設定の帯域幅メトリック（双方向帯域幅）を使用します。
- 同じエージェントに対して複数のモニタを実行しないようにします。代わりに、モニタをより多くのエージェントに分散するか、モニタを1つずつ実行します。

注: 同じ場所に複数のエージェントをインストールすると、それらが同じ物理リンクを使用する場合に競合が発生する可能性があります。

遅延とパケット損失の構成

遅延とパケット損失を測定するには、次のいずれかのプローブ・メトリックを選択します。

- [「TCP（ピアベース）」（40ページ）](#)
- [「TCP（ピアレス）」（41ページ）](#)
- [「UDP」（41ページ）](#)
- [「ICMP」（42ページ）](#)

TCP（ピアベース）

ソース・エンドポイントはTCP接続を介してピアにパケットを送信し、TCP応答時間を測定します。大きなジッタが存在する場合、得られる結果の精度が低くなります。

- **Interval（インターバル）**：値を選択するか、標準設定の5秒を使用します。
- **Packet Size（パケット・サイズ）**：プローブ時に使用するパケット・サイズ（バイト単位）。
- **Peer Port（ピア・ポート）**：サーバがリッスンしていない使用可能なポートの番号を入力するか、**【Auto Select（自動選択）】**を使用して事前定義のポート・リストをスキャンし、使用可能なポートを見つけます。

注: MS Windows XPのTCP/IPスタックの実装に問題があるため、TCP使用可能帯域幅で測定されるパケット損失率が不正確になる可能性があります。可能であれば、エンドポイントのオペレー

ティング・システムが Windows XP である場合は、TCP を使用するモニタの使用を避けてください。XP を実行しているエンドポイント・マシンが1つのみの場合は、このエンドポイントをターゲットにすることをお勧めします。

TCP (ピアレス)

新規 TCP セッションを確立するのに要する時間を測定します (SYN パケットを送信し、SYN ACK パケットを受信します)。エージェントレス TCP を使用するネットワーク測定では、ターゲット・エンドポイントに TCP/HTTP サーバが必要です。

注: ネットワーク・アクセラレータやプロキシ・サービスがネットワーク・パスに存在する場合、要求されたサーバの代わりにアクセラレータやプロキシが要求に応答するため、ネットワーク測定が不正確になる可能性があります。

- **Interval (インターバル)** : 値を選択するか、標準設定の 3 秒を使用します。
- **Peer Port (ピア・ポート)** : ターゲット・サーバに接続するポートのポート番号を入力します。
- **Include DNS Resolution (DNS 解決を含める)** : ドメイン名の IP アドレス解決を測定の一部に含めます。

注: MS Windows XP の TCP/IP スタックの実装に問題があるため、TCP で測定されるパケット損失率が不正確になる可能性があります。可能であれば、エンドポイントのオペレーティング・システムが Windows XP である場合は、TCP を使用して測定を行うモニタの使用を避けてください。XP を実行しているエンドポイント・マシンが1つのみの場合は、このエンドポイントをターゲットにすることをお勧めします。

UDP

このプロトコルは、UDP でパケットを送信する場合に受信するエコー応答を測定します。UDP は指定されたポート番号とチェックサムを使用して、パケットが正しく到達したことを確認します。ただし、パケットが正しい順序で再構成されたことを保証するものではありません。

- **Interval (インターバル)** : 値を設定するか、標準設定の 3 秒を使用します。
- **Packet Size (パケット・サイズ)** : プロブとして使用するソース・エンドポイントから送信されるパケットのサイズを定義して、バイト単位の値を選択します。
- **Timeout (タイムアウト)** : 受信ホストによって受信されない場合に送信済みパケットをパケット損失とみなすまでの時間を定義します (または、標準設定を使用します)。
- **Peer Port (ピア・ポート)** : ソースおよびターゲット・マシン間のファイアウォール上で開かれているポートのみで正確な結果が得られます。ポートが閉じている場合、測定値は完全なパケット損失を示します。Network Capture で [Auto Select (自動選択)] を選択して事前定義のポート・リストをスキャンし、使用可能なポートを見つけます。
- **Specific port (特定ポート)** : ポート番号を入力または選択します。自動スキャンでは、<Network Capture エージェント・ホーム・ディレクトリ>\Bin\AgentImplementation にある NC.Protocols.config ファイルで設定された標準設定に基づいてポートが選択されます。このファイルを変更すると、代替のスキャン対象ポートを定義できます。

ICMP

ソース・エンドポイントは ICMP エコー要求 (ping) をターゲット・エンドポイントに送信します。ターゲットが使用可能な場合、ターゲット・ホストは ICMP 応答をソース・エンドポイントに返信して応答します。遅延の測定値はラウンドトリップ時間です。

注: ICMP エコー要求および応答メッセージを受信して処理するようにターゲット・エンドポイントのオペレーティング・システムを適切に構成し、ICMP エコー要求/応答メッセージがソース・マシンとターゲット・マシンとの間のパスに沿って伝送されるようにします。

Interval (インターバル) : 100 ミリ秒より大きな値を選択するか、標準設定の 1 秒を使用します。1 秒未満の値を選択する場合は、モニタで短い期間を使用します。このようにしないと、取得されるサンプル数が多くなり、データベースが満杯になる可能性があります。帯域幅は複数のモニタで同時に測定できます。詳細については、「[同時帯域幅モニタのインターバルの定義](#)」(39ページ)を参照してください。

Packet Size (パケット・サイズ) : バイト単位の値を選択します。値には IP ヘッダと ICMP ヘッダを含みます。

Timeout (タイムアウト) : エージェントによって応答が受信されない場合に送信済みパケットをパケット損失とみなすまでの時間を定義します。

帯域幅の構成

帯域幅の測定は、送信トラフィックまたは受信トラフィック (あるいはその両方) を対象に行うことができます。一方方向帯域幅の記録時には、送信帯域幅が測定され、受信帯域幅は事前定義の比率に従って推定されます。双方向メトリックの測定時には、送信メトリックと受信メトリックの両方が測定されます。

次の 3 つのメトリックを記録できます。

- 一方方向帯域幅
- 双方向推定帯域幅
- ロバスト双方向サンプル帯域幅

一方方向帯域幅

送信帯域幅の可用性を測定し、受信帯域幅の可用性を推定します。このメトリックは、ターゲット・エンドポイントにエージェントを配置できない場合に使用します (例: <http://www.example.com> などの Web サーバ)。このプロトコルでは、ネットワークに中程度の負荷がかかります。ネットワークが混雑している場合、正確な結果が得られるとは限りません。

- **Interval (インターバル) :** 2 分以上に設定します。通常、各プローブに約 15 秒必要です。帯域幅は複数のモニタで同時に測定できます。詳細については、「[同時帯域幅モニタのインターバルの定義](#)」(39ページ)を参照してください。
- **Pinging Protocol (Ping プロトコル) :** [Auto Select (自動選択)] を使用することをお勧めします。この場合、次の順序で使用可能な最初のプロトコルが選択されます: NTP, ICMP タイムスタ

ンプ、ICMP エコー。これらはそれぞれ個別に選択することもできます。NTP と ICMP タイムスタンプでは、より精度の高い結果が得られます。戻りの応答がネットワーク条件に影響されることはありません。

注: NTP ping プロトコルを使用して一方向帯域幅を測定するには、NTP サービスが有効である必要があります。

- **ポート:** 有効なポート番号を入力するか、Network Capture で [Auto Select (自動選択)] を選択して事前定義のポート・リストをスキャンし、使用可能なポートを見つけます。Network Capture は選択されたポートが実際に使用可能であること（ファイアウォールでブロックされていないこと）を検証します。使用可能でない場合は、実行を中止します。自動スキャンでは、< Network Capture エージェント・ホーム・ディレクトリ > \Bin\AgentImplementation にある **NC.Protocols.config** ファイルで設定された標準設定に基づいてポートが選択されます。このファイルを変更すると、代替のスキャン対象ポートを定義できます。

双方向推定帯域幅

このプロトコルは、双方向帯域幅の可用性を測定します。ソース・エンドポイントとターゲット・エンドポイントの両方に、インストールされた HP エージェントが必要です。双方向推定は、アップストリームとダウンストリームの両方の帯域幅の可用性を測定する場合に選択します。ポーリングは通常 3 秒のインターバルで実行されます。

- **Interval (インターバル):** 2 分以上に設定します。帯域幅は複数のモニタで同時に測定できません。詳細については、「[同時帯域幅モニタのインターバルの定義](#)」(39 ページ)を参照してください。
- **ポート:** Network Capture で [Auto Select (自動選択)] を選択して事前定義のポート・リストをスキャンし、使用可能なポートを見つけます。特定ポートを選択するには、有効なポート番号を入力するか、上/下矢印を使用します。Network Capture は選択されたポートが実際に使用可能であること（ファイアウォールでブロックされていないこと）を検証します。使用可能でない場合は、実行を中止します。
- **Probing Protocol (プローブ・プロトコル):** これには、ネットワーク・トラフィックの生成に使用されるプロトコルが表示されます。

ロバスト双方向サンプル帯域幅

双方向帯域幅の可用性を測定します。ソース・エンドポイントとターゲット・エンドポイントの両方に、インストールされた HP エージェントが必要です。帯域幅容量が 50 Mbps 未満でラウンドトリップ時間が 120 秒未満の場合に精度の高い測定値が得られます。双方向サンプルでは、ネットワークに大きなトラフィック負荷がかかります。

注: MS Windows XP の TCP/IP スタックの実装に問題があるため、ラウンドトリップのパケット損失率が (2%より) 高く、プローブ・マシンが Windows XP である場合、ロバスト双方向の測定値が使用可能な帯域幅よりも小さくなる可能性があります。これは、ターゲット・エンドポイントで Windows XP が実行されている場合はダウンストリームの使用可能帯域幅の結果が影響を受け、ソース・エンドポイントで XP が実行されている場合はアップストリームの結果が影響を受ける可能性があることを意味します。

- **Interval (インターバル)** : 2 分以上に設定します。帯域幅は複数のモニタで同時に測定できません。詳細については、「[同時帯域幅モニタのインターバルの定義](#)」(39ページ)を参照してください。
- **ポート** : ソースとターゲットの両方に、インストールされた HP エージェントが必要です。または、Network Capture で **[Auto Select (自動選択)]** を選択して事前定義のポート・リストをスキャンし、使用可能なポートを見つけます。特定ポートを選択するには、有効なポート番号を入力するか、上/下矢印を使用します。Network Capture は選択されたポートが実際に使用可能であること(ファイアウォールでブロックされていないこと)を検証します。使用可能でない場合は、実行を中止します。自動スキャンでは、< **Network Capture エージェント・ホーム・ディレクトリ** > \Bin\AgentImplementation にある **NC.Protocols.config** ファイルで設定された標準設定に基づいてポートが選択されます。このファイルを変更すると、代替りのスキャン対象ポートを定義できます。
- **Probing Protocol (プローブ・プロトコル)** : これには、ネットワーク・トラフィックの生成に使用されるプロトコルが表示されます。

Web サーバ・パラメータの構成

HTTP 応答時間では、ターゲット・エンドポイントから HTTP 応答を受信するのに要した時間の長さを測定します。これには、DNS 参照の時間、TCP 接続の確立、サーバの処理時間、ネットワーク遅延が含まれます。

HTTP 応答時間

ターゲット・エンドポイントに Web サーバが必要です。

- **Interval (インターバル)** : 値を選択するか、標準設定の 30 秒を使用します。
- **HTTP Method (HTTP メソッド)** : **Get** または **Head** を選択します(通常、Head の方が高い精度が得られます)。
- **Timeout (タイムアウト)** : Web サーバから応答を受信しない場合に要求を損失とみなすまでの時間を定義します。値を選択するか、標準設定値を使用します。
- **Resource Path (リソース・パス)** : 要求されたリソースへのパス(例 : / または /index.html)。
- **ポート** : TCP/HTTP サーバが受信要求をリスンしているポート番号(標準設定では 80 または 443)を選択するか、特定のポート番号を入力します。
- **Max Redirections (最大リダイレクト数)** : 追従するリダイレクトの数。ターゲット・サーバからの応答を想定しているため、通常は「0」です。
- **User Agent (ユーザ・エージェント)** : Web サーバに接続する際に使用するユーザ・エージェント文字列。一部の Web サーバは事前定義されたエージェントにのみ応答できます。標準設定値では Firefox 4.0 のユーザ・エージェント文字列を使用します。
- **Status Code (ステータス・コード)** : Web サーバから受信することを想定しているステータス・コードを選択します。受信したステータス・コードが指定されたものと一致しない場合、要求は失われたとみなされます。特定のステータス・コードを選択するか、エラーを意味しない任意の

タイプのステータス・コードを受け入れる場合は [Any status code (任意のステータス コード)] を選択します。

- **Schema (スキーマ) : セキュア通信 (HTTPS) またはセキュアでない通信 (HTTP) を選択します。**

モニタリングの開始

モニタの構成が済んだら、ツールバーの [Run Monitor (モニタの実行)] ボタンをクリックして記録を開始します。各種コンポーネントの検証は、次の順序で行われます。

1. ソース・エンドポイントが Network Capture サーバにポーリングを行い、コマンドを取得できる
2. Network Capture サーバ、関連するエージェント、および結果を表示するホストの間でのクロック同期
3. ソース・エンドポイントが結果を Network Capture サーバに送信できる
4. ソース・エンドポイントがターゲット・エンドポイントと通信できる (ピアベースのモニタのみ)
5. ポートの競合が発生しない

注: 初期化後にモニタが起動しない場合は、[「よくある質問とトラブルシューティング」](#) (58ページ) を参照してください。

データの表示

モニタ・ページの [Results (結果)] をクリックすると、Network Capture に該当するモニタの選択した実行の実行時の結果が表示されます。標準設定では、最後の 15 分の結果が折れ線グラフに表示されます。オフラインの結果を表示するには、[Max (最大)] をクリックして期間全体を表示します。



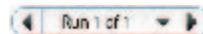
上部の進捗状況バーには、開始時間と終了時間、および経過時間の割合が表示されます。現在の記録と以前の記録を表示できます。

注: 一定期間ソース・エージェントにアクセスできない場合は、最後のデータが取得されたポイントとタイムアウト後の結果がつながり、連続する線が表示されます。

[Percentile Distribution Graph (パーセンタイル分布グラフ)] アイコン  をクリックすると、パーセンタイル分布グラフ形式でデータが表示されます。



モニタに複数の実行が存在する場合は、矢印を使用して必要な実行を選択します。



現在および以前の記録を開くことができます（進捗状況バーは現在実行中のモニタでのみ表示されます）。



モニタの名前の横にあるアイコンに従って、各モニタのステータスが表示されます。

	現在実行中
	このモニタの最後の実行でメトリックが正常に実行されなかったことを示します
	アイドル状態。現在実行中でないか、正常に終了済み
	現在実行中であるが、一部のプロトコルで実行が停止している



エラー：エラーで実行が停止した場合に [Results (結果)] ボタンの下に表示されます。このアイコンを選択すると問題の説明が表示されます。

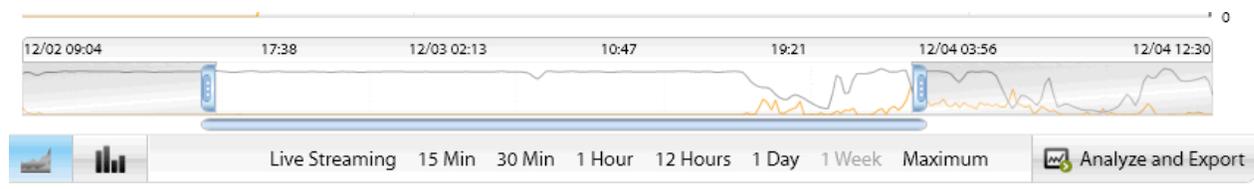
注: Network Capture サーバ、エージェントおよび結果を表示するホストのクロックが同期されていない場合、結果に表示される時間は正しくありませんが、結果は有効です。各ホスト・コンピュータでクロックを同期するには、時刻の設定で [インターネット時刻サーバーと同期する] オプションを選択します。

拡大と縮小

表示される結果の細かさは、記録の長さに依存します。そのため、長い期間の記録で結果をより詳細に表示する場合は、ズームを使用して特定の期間を選択します。標準設定では直近の結果が表示されるため、12 時間の期間を選択すると、記録の最初の 12 時間ではなく、最後の 12 時間が表示されます。以下のオプションのほとんどは、折れ線グラフとパーセント分布グラフの両方で使用できます。

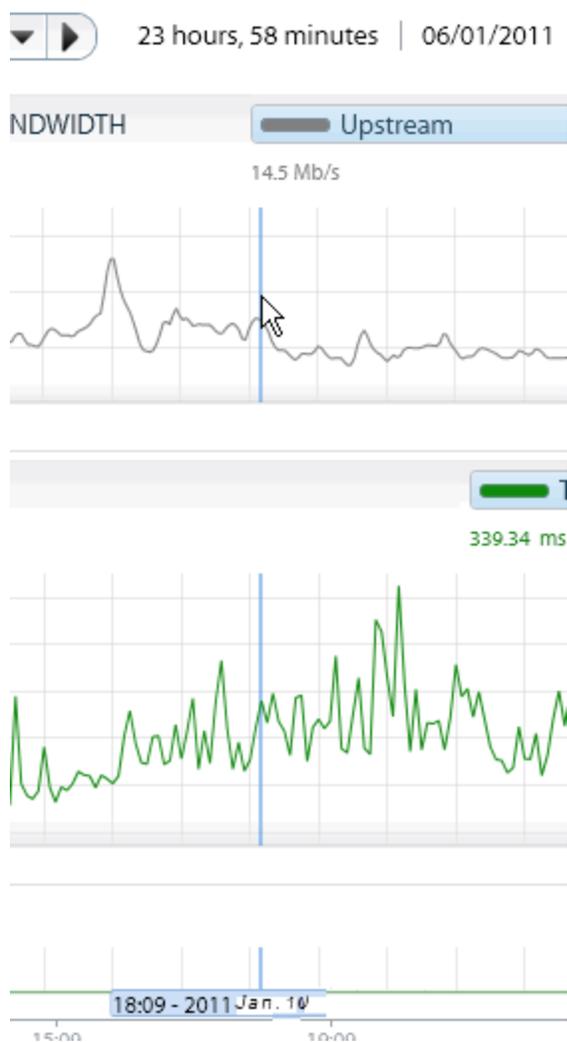
時間範囲を選択するには：

- 結果ページの下部に表示された、15 分から最大（記録のすべての範囲）までの期間をクリックします。Live Streaming（ライブ・ストリーミング）は、新規サンプルごとに更新されます。

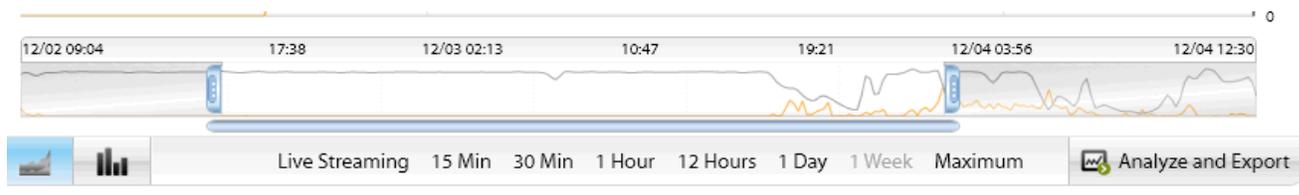


次の方法を使用して、特定の期間を選択します。

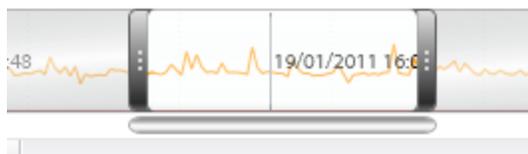
- 実行内のイベントを正確に見つけるには、結果表示の青い縦線のツールヒントを使用して日付と時刻を表示します。



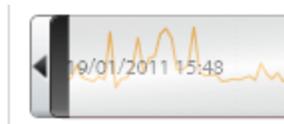
- 左と右のスライダ・バーを使用して範囲を調整し、グラフを選択した範囲に合わせます。



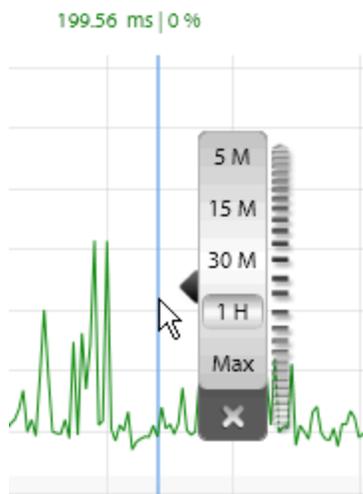
- スライダで拡大鏡を必要な期間までスライドします。



- スライダの左端と右端にある矢印を使用して、前の時間フレーム/次の時間フレームにジャンプします。

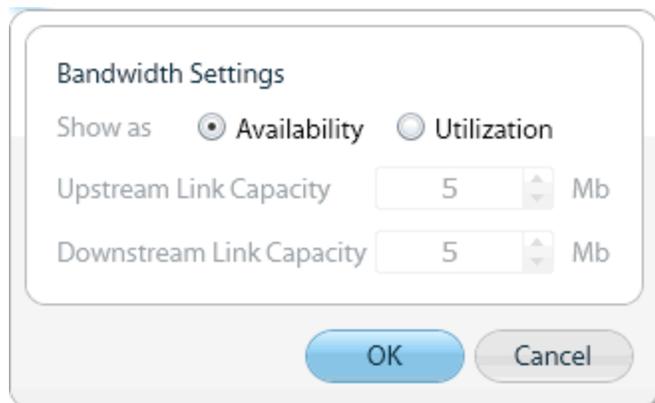


グラフをダブルクリックし、マウス・ホイールを使用して必要な時間フレームを選択します。



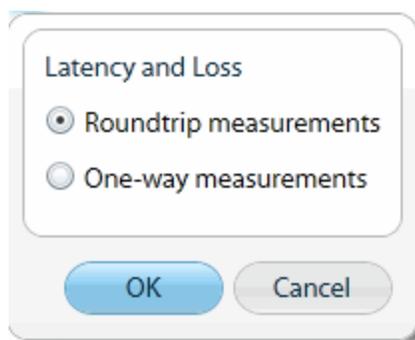
帯域幅を可用性または使用率として表示するには：

1. 結果ページで [Bandwidth Settings (帯域幅設定)] アイコンをクリックします。
2. [Bandwidth Settings (帯域幅設定)] ウィンドウで、[Availability (可用性)] または [Utilization (使用率)] を選択します。[Utilization (使用率)] を選択する場合は、リンク容量の値を指定します。



遅延と損失の設定を構成するには：

1. 結果ページで [Latency and Loss Settings (遅延と損失の設定)] アイコンをクリックします。



2. 遅延の設定で， [Roundtrip measurements (ラウンドトリップ測定)] または [One-way measurements (一方向測定)] を選択します。

データの検索

現在の表示でデータを検索するには，フリー・テキストを入力するか，いずれかのドロップダウン・オプションを選択します。事前定義の検索では，特定のステータスを持つすべてのモニタが表示されます。

データの分析

Network Capture でデータを収集する際には，HP のパフォーマンス・アプリケーションで条件をエミュレートする際に，どのようにすれば収集したデータを最大限に利用できるかを思案します。約 30 分のデータを含むファイルをエクスポートする際には，各ファイルがネットワークの状況をそれぞれ有意義な期間で示すようにしたいと考えます。

データを分析するには：

1. 結果ページで，グラフの下の [Analyze and Export (分析とエクスポート)] をクリックします。
2. 特定の期間をすばやく表示するには， [Analyze (分析)] セクションで期間を選択します。
これらの条件を表示する期間を選択します。通常，1分または5分で十分です。期間を長くする場合は，15分または30分を選択します。結果をエクスポートするには，遅延または帯域幅の計算に従い，表示されている期間または実行全体を選択します。詳細については，「[データのエクスポート](#)」(55ページ)を参照してください。
3. より詳細な統計情報については， [Performance Statistics (パフォーマンス統計情報)] を選択します。

パフォーマンス統計情報

帯域幅

結果には使用可能な帯域幅が表示されます。

【**Lowest (最低)**】は、選択した期間に観測された最も低い帯域幅の結果を示します。

【**5th Percentile (5 パーセンタイル)**】は、選択した期間に測定された最も低い帯域幅条件（発生頻度の低いものを除く）を示します。

【**95th Percentile (95 パーセンタイル)**】は、選択した期間に観測された最も高い帯域幅の結果（発生頻度の低いバーストやはずれ値を除く）を示します。

【**Typical (標準)**】は、選択した期間の相乗平均を示します。これは最も代表的な帯域幅条件を表します。

【**Highest (最高)**】は、選択した期間に測定された最も高い帯域幅条件を示します。

遅延 (ラウンドトリップ) とパケット損失

【**Low (低)**】は、選択した時間フレーム中の遅延/損失が最も低い期間を示します。

【**95th Percentile (95 パーセンタイル)**】は、選択した期間に観測された遅延とパケット損失の最も低い結果を示します（発生頻度の低いものは無視）。

【**Mean (平均)**】値は、遅延とパケット損失（標準設定）または帯域幅測定値の相乗平均を示し、ネットワーク内の最も一般的なネットワーク条件を表します。アプリケーション応答時間をテストする際には、この値を使用して標準的なトランザクション応答をシミュレートします。

【**5th Percentile (5 パーセンタイル)**】は、選択した期間に観測された最も高い遅延とパケット損失を示します（発生頻度の低いピークは無視）。

【**Highest (最高)**】は、選択した時間フレーム中の遅延/損失が最も高い期間を示します。

【**Average Loss (平均損失)**】（パケット損失の場合のみ）は、定義された期間に失われたパケットの平均数を示します。

ヒント

スライダ・バーを使用して特定の時間帯のネットワーク条件を見つけるか、分析を使用して最低、平均、または最高の 1 分/5 分/15 分/30 分の時間フレームを見つけます。

ネットワーク・プロファイルの使用

ネットワーク・プロファイルでは、Network Capture で記録したモニタまたは外部ソースのデータを使用します。これらの記録を分析することで、記録期間中に取得した最高、最低、標準の条件を切り

分けることができます。これらの条件は、テスト用エミュレーションで使用する .ntx 形式でエクスポートできます。

注: HP Network Virtualization Modeler のクラウド・シェイプに記録をインポートする場合、HP Network Capture の以前のバージョン（旧 Shunra NetworkCatcher）で表示されていたモニタの代わりにネットワーク・プロファイルが表示されます。

ネットワーク・プロファイルでは、次の種類のモニタの実際に記録したネットワーク条件が利用できます。

- モバイル
- 固定
- モニタベース

データは地理的なソースとターゲット、通信のタイプ、期間に基づいて選択できます。

モバイル・プロファイルを作成するには：

1. **[New Profile (新規プロファイル)]** アイコンを選択します。標準設定では、モバイル・プロファイルが作成されます。プロファイル名は最大 255 文字です。

注: 固定プロファイルまたはモニタベース・プロファイルを作成するには、ドロップダウン・リストで必要なオプションを選択します（下記を参照）。

2. **[From (接続元)]** および **[To (接続先)]** のリストから、ソースとターゲットの都市を選択します。
3. 接続の種類 (WiFi または携帯電話) を選択します (**[Settings (設定)]** アイコンをクリックすると、追加オプションが利用できます)。
4. デバイスを選択します。
5. 遅延または帯域幅 (あるいはその両方) と、次のいずれかの条件を選択します。
 - **Best (最高) :** 選択した期間に測定される最も好ましい条件
 - **Typical (標準) :** 相乗平均 (最も代表的な条件を示す)
 - **Worst (最低) :** 選択した期間に測定される最低の条件
6. 記録のエミュレーション時間 (期間) を選択します (1 分 ~ 2 時間)。
7. **[OK]** を選択するか、**[Save and Add Another (保存して追加)]** します。Network Capture で選択したパラメータに従って条件が計算され、結果が表示されます。

固定プロファイルを作成するには：

1. **[New Profile (新規プロファイル)]** アイコンの横のドロップダウン・リストから **[Stationary (固定)]** を選択します。
2. ソース (クライアントまたはデータ・センタ) を選択します。ターゲットはデータ・センタです。
3. 遅延または帯域幅 (あるいはその両方) と、次のいずれかの条件を選択します。

- **Best (最高)** : 選択した期間に測定される最も好ましい条件
 - **Typical (標準)** : 相乗平均 (最も代表的な条件を示す)
 - **Worst (最低)** : 選択した期間に測定される最低の条件
4. 記録のエミュレーション時間 (期間) を選択します (1 分 ~ 2 時間)。
 5. **[OK]** を選択するか, **[Save and Add Another (保存して追加)]** します。Network Capture で選択したパラメータに従って条件が計算され, 結果が表示されます。

プロファイル・モジュールからモニタベース・プロファイルを作成するには :

1. **[New Profile (新規プロファイル)]** アイコンの横のドロップダウン・リストから **[Monitor-based (モニタベース)]** を選択します。
2. モニタを選択して **[Run (実行)]** を選択します。
3. 遅延のメトリック (TCP または HTTP など) を選択します。
4. 帯域幅を測定した場合は, 帯域幅のメトリック (双方向推定など) を選択します。
5. 次のいずれかの条件を選択します。
 - **Best (最高)** : 選択した期間に測定される最も好ましい条件
 - **Typical (標準)** : 相乗平均 (最も代表的な条件を示す)
 - **Worst (最低)** : 選択した期間に測定される最低の条件
6. 記録のエミュレーション時間 (期間) を選択します (1 分 ~ 2 時間)。
7. **[Find by Latency (遅延で検索)]** を選択し, 遅延の値に基づいて必要な条件を含むインターバルを表示するか, **[Find by Bandwidth (帯域幅で検索)]** を選択して帯域幅の測定値に基づいて必要な条件が示されるインターバルを表示します。
8. **[OK]** を選択するか, **[Save and Add Another (保存して追加)]** します。Network Capture で選択したパラメータに従って条件が計算され, 結果が表示されます。

モニタリング・モジュールからモニタベース・プロファイルを作成するには :

1. モニタを選択して **[Run (実行)]** を選択します。
2. 必要な条件に基づいて分析を行うか, 必要な時間インターバルを手動で選択します。
3. 帯域幅以外にメトリックが 1 つだけ選択されていることを確認します。
4. **[Analyze and Export (分析とエクスポート)]** を開きます。
5. **[Save as Network Profile (ネットワーク プロファイルとして保存)]** を選択します。
6. プロファイルのフォルダを選択し, プロファイル名を指定して **[Save (保存)]** をクリックします。

データのエクスポート

実際のネットワーク条件を使用してネットワーク・エミュレーションを実行するには、Network Capture から .ntx ファイル形式でデータをエクスポートします。その後、HP Network Virtualization ネットワーク・アプライアンスまたは HP Network Virtualization デスクトップ・アプリケーションで、ファイルをインポートして記録したネットワーク条件をエミュレートします。各 .ntx ファイルには、遅延とパケット損失または帯域幅のいずれか1つのメトリックのみを含めることができます。

HP Network Virtualization デスクトップ・アプリケーションを使用してエミュレートする場合、メトリックごとに最大 900 の遅延とパケット損失のサンプルをエクスポートできます。エクスポート・ファイル内に存在するサンプル数は、メトリックごとの標準設定のインターバル設定にも依存します。エクスポート対象のデータでこのインターバルを変更するには、ズーム・バーを使用して、データをエクスポートする時間フレームを選択します。

HP Network Virtualization ネットワーク・アプライアンスを使用してエミュレートする場合、最大 90,000 のサンプルをエクスポートできます。この設定は管理モジュールの設定で変更できます。

注: 当初データが更新されるまでの間、エクスポート・オプションは無効な状態が表示されることがあります。エクスポートには追加ライセンスが必要です。

データをエクスポートするには：

1. 結果またはネットワーク・プロファイル・ページで、グラフの下の **[Analyze and Export (分析とエクスポート)]** をクリックします。
2. 次のエクスポート・オプションを選択します。
 - 表示された時間フレームをエクスポート（現在の表示が実行全体の一部を示している場合）
または
 - ネットワーク・プロファイルとして保存（HP Network Virtualization エミュレーション・アプリケーションから、これらのプロファイルをアップロードできる）
3. ファイルを必要な場所に保存します。

エクスポート設定を変更するには：

1. 結果またはネットワーク・プロファイル・ページで、グラフの下の **[Analyze and Export (分析とエクスポート)]** をクリックします。
2. **[Settings (設定)]** を選択します。これは、**[Administration (管理)]** > **[Settings (設定)]** > **[Export (エクスポート)]** にリンクされています。これらの設定には、管理モジュールで直接アクセスすることもできます。

ユーザの定義と更新

新規ユーザの定義、変更、削除を行うことができるのは、管理者権限を持つユーザのみです。オペレータは各自および他のユーザの詳細を表示できますが、これらを変更することはできません。オペレータは自分のパスワードのみを変更できます。詳細については、[「アカウント設定」\(57ページ\)](#)を参照してください。

新規ユーザを定義するには：

注: ユーザを追加できるのは管理者のみです。

1. 管理モジュールで **[Users (ユーザ)]** をクリックします。
2. **[New User (新規ユーザ)]** アイコンをクリックし、プロパティを定義します。次のアカウント・タイプを選択します。
 - 管理者：すべての権限
 - オペレータ：モニタの作成と変更を行うことができるが、ユーザ、エンドポイント、その他の設定の作成や変更はできない
3. 最大 20 文字の英数字のパスワードを定義します。

ユーザの詳細またはユーザのパスワードを変更するには：

注: ユーザの詳細を変更できるのは管理者のみです。

1. 管理者ページで、Network Capture ツールバーの **[Users (ユーザ)]** をクリックします。
2. ユーザをダブルクリックし、必要に応じてユーザのプロパティを変更します。ユーザ名、電話番号、パスワードのみを変更できます。

ユーザを削除するには：

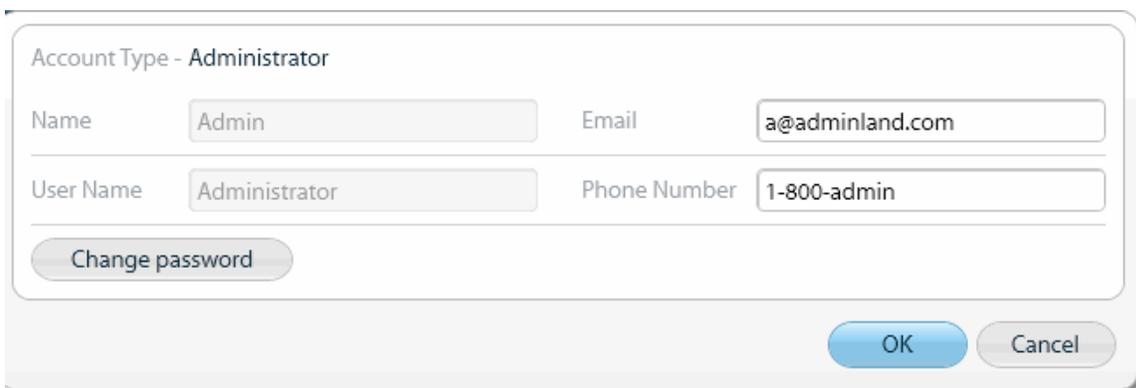
注: ユーザを削除できるのは管理者のみです。ただし、システム定義の管理者を削除することはできません。

1. 管理ページで **[Users (ユーザ)]** をクリックします。
2. ユーザを選択し、**[Delete User (ユーザの削除)]** アイコンをクリックします。

すべてのユーザは **[Regenerate and send password by email (パスワードを再生成して電子メールで送信する)]** アイコンをクリックして各自のパスワードをリセットできます。

アカウント設定

各自のアカウントの詳細を表示するには、ツールバーの [Account Settings (アカウント設定)] アイコンをクリックします。[Name (名前)] と [User Name (ユーザ名)] は変更できませんが、その他のフィールドは更新できます。



Account Type - Administrator

Name: Admin Email: a@adminland.com

User Name: Administrator Phone Number: 1-800-admin

Change password

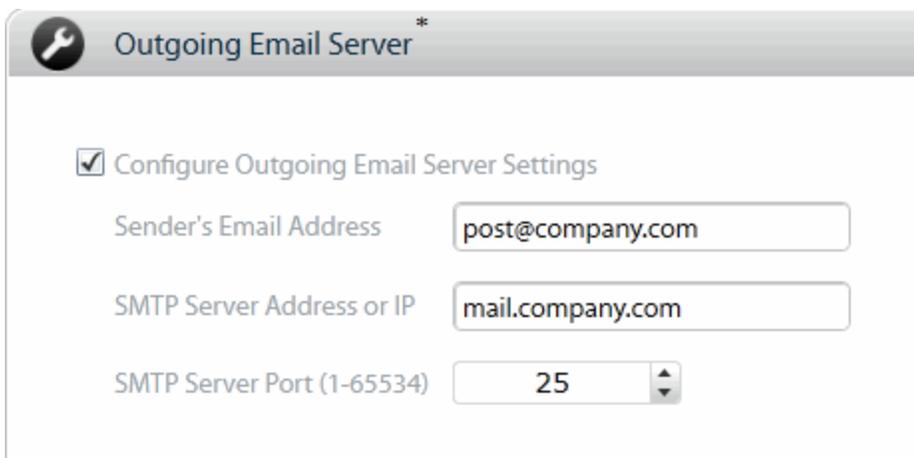
OK Cancel

送信電子メールの設定

パスワードのリセットやその他の特定のアカウント更新を実行するには、有効な SMTP メール設定が設定されている必要があります。これらの設定はインストール中に構成できます。また、[管理モジュール] > [Settings (設定)] > [Outgoing Email Server (送信電子メール サーバ)] を選択してインストール後に構成することもできます。

- 送信元電子メール・アドレス：電子メールの送信元の電子メール・アドレスを入力します。
- SMTP サーバ：電子メールを送信する SMTP サーバの DNS または IP アドレスを入力します。
- ポート：標準設定ではポート 25、または別のポート番号を入力します。

この構成は電子メールの送信を保証するものではありません。ネットワーク接続、認証、その他の要因によって電子メールを送信できない場合があります。これらの問題については、システム管理者に問い合わせてください。



Outgoing Email Server*

Configure Outgoing Email Server Settings

Sender's Email Address: post@company.com

SMTP Server Address or IP: mail.company.com

SMTP Server Port (1-65534): 25

スケジュールの設定

特定のタイムテーブルに基づいてモニタの記録の開始と終了を行うには、スケジューラを使用します。スケジュールはモニタを定義する際に作成できます。また、後から作成することもできますが、モニタの実行中に作成することはできません。スケジューラの時間は、モニタを定義するマシンの時間に基づいて設定されます。

スケジュールを設定するには：

1. モニタを定義または編集する際に、**[Scheduling (スケジュール設定)]** ボタンをクリックします。
2. 開始時間と終了時間を定義し、必要に応じて繰り返しを設定します。毎日、毎週、毎月の単位で記録を繰り返し実行するように設定できます。
3. 各記録の期間を定義します。

よくある質問とトラブルシューティング

新しいネットワーク・プロファイルを作成できません。[From (接続元)] および [To (接続先)] のドロップダウン・リストが空です。どうすればいいですか。

これは、Network Capture サーバとの間にプロキシが存在する場合に発生します。

HP Network Capture サーバ・サービスを見つけます。サービスのプロパティに移動し、**[Log on (ログオン)]** タブで **[This account (このアカウント)]** を選択します。管理者のユーザ名とパスワードを入力し、サービスを再起動します。

Network Capture サーバをインストールしたところ、Network Capture Web ページを開くことはできますが、ログインできません。代わりに「Communication with Server failed (サーバとの通信に失敗しました)」というエラーが表示されます。どうすればいいですか。

最初に Network Capture サーバ・サービスが起動していることを確認します。

Web サーバ (IIS) , IIS マネージャで ASP.NET 4.0.30319 が許可されていることを確認します (オペレーティング・システムに依存)。

.svc ファイル・タイプが aspnet_isapi.dll にマップされていることを確認します。詳細については、次の URL を参照してください。 <http://msdn.microsoft.com/en-us/library/ms752252.aspx>

セキュリティ保護された Network Capture サーバのインストールに失敗し、ログに次のエラーが表示されます。「エラー：入力は有効な Base-64 文字列ではありません。」

Base-64 以外の文字が含まれるか、3 個以上の埋め込み文字があるか、または埋め込み文字の間に空白以外の文字が含まれます。」

1. Windows 7 および Windows 2008 R2 の IISCertObj コンポーネントのバグに関する情報については、次の URL を参照してください：<http://support.microsoft.com/kb/982386/en-us>
2. 上記の記事で推奨されている修正プログラムをインストールします。
3. Network Capture サーバを再インストールします。

Network Capture サーバが起動しません。どうすればいいですか。

MySQL Instance Configuration Wizard を開き、標準インスタンスを構成します。

エンドポイントが到達不可（赤）です。どうすればいいですか。

最初に [Scan all endpoints (すべてのエンドポイントのスキャン)] ボタン  をクリックします。前回のスキャン以降に問題が解決している可能性があります。また、スキャンがまだ実行されていない場合、[Endpoint (エンドポイント)] アイコンが赤になる可能性があります。スキャン後も引き続きアクセス不可の場合は、以下を確認します。

- Network Capture エージェント・サービスがアクティブであることを確認します。
- ファイアウォール設定を確認します（詳細については、「[ファイアウォール構成](#)」(23ページ)を参照)。
- リモート・エージェントの場合は、エージェント・ホストからサーバ・ホスト名に「ping」できることを確認します。
- 問題がソースからターゲットまたはターゲットからソースのどちらにあるのかを確認するため、ソースとターゲットの両方で異なる2つのモニタを起動します。エラー・メッセージには問題が発生する接続内の要素が表示されます。
- インストール中に Network Capture エージェントで必要となるポート 80 がすでに使用されていることを示すメッセージが表示される場合があります。この状況を修正するには、このポートを使用しているコンポーネントを特定し、別のポートをコンポーネントに割り当てます。HP NC エージェント・サービスを再起動し、[Scan all Endpoints (すべてのエンドポイントのスキャン)] をクリックすると、問題が解決されるはずですが。
- これでうまくいかない場合は、サポート (<https://softwaresupport.hp.com/>) までご連絡ください。

Internet Explorer を使用しているのですが、Network Capture エージェントをダウンロードできません。

ブラウザを使用してエージェントをダウンロードできるようにするには、次の設定を調整する必要があります。

1. Internet Explorer で [ツール] > [インターネット オプション] を開き、[セキュリティ] タブを選択します。
2. [セキュリティ設定を表示または変更するゾーンを選択してください] の下の [インターネット] を選択します。

3. [レベルのカスタマイズ] を選択します。
4. 設定で [ダウンロード] を選択し、次の設定を有効にします。
 - ファイルのダウンロード時に自動的にダイアログを表示
 - ファイルのダウンロード

ピアベースの測定が開始されないのはなぜでしょうか。

ピアベースのプロトコルを選択したときに、ターゲット・マシンで選択したポートがすでに使用されている場合、Network Capture は測定を実行できません。

モニタの初期化ページが途中で停止してしまいます。どうすればいいですか。

モニタの初期化ページを閉じ、[Refresh All (すべて更新)] をクリックしてモニタを再起動します。

情報を探す方法について教えてください。

Network Capture には、モニタ、エンドポイント、結果などを検索するための広範な検索機能が用意されています。詳細については、[「データの検索」\(51ページ\)](#)を参照してください。

一方向帯域幅と双方向帯域幅を測定するようにモニタを設定したのですが、モニタが停止します。この問題の原因として何が考えられますか。

この問題にはいくつかの原因が考えられますが、一般的な原因の1つは NetworkCatcher v7.0 でサポートされていない IPv6 が有効になっていることです。この問題を解決するには、ソース・エージェント・ホストで、IPv6 を選択解除します（お使いのオペレーティング・システムによりますが、通常は [ローカル エリア接続のプロパティ] の [ネットワーク] タブにあります）。

パスワードをリセットしましたが、新しいパスワードを使用した電子メールが受信されませんでした。

[Outgoing Email Server (送信電子メールサーバ)] の設定 (管理モジュール) が最新の状態になっていることを確認します。これで問題が解決されない場合は、SMTP 構成の問題に関連する可能性があるため、システム管理者にお問い合わせください。

ユーザ・インタフェースのデザインは気に入っていますが、一部の表示がおかしく、ボタンが重なって表示されたり、一部の画像が曲がって表示されたりします。どうしてですか。

画面の解像度を 1280 x 800 以上 (ズームレベル 100%) に設定してください。

結果を保存するにはどうすればいいですか。

結果ビューで [Analyze and Export (分析とエクスポート)] を選択し、.ntx ファイル形式でデータを保存します。詳細については、[「データのエクスポート」\(55ページ\)](#)を参照してください。

Windows 2008 で Network Capture を実行していますが、一部のモニタが停止し、「パケット重複」に関する内容のエラーが表示されます。どうすればいいですか。

1. 一部のピアベース測定を実行するには、IP ルーティングを無効にする必要があります。IP ルーティングを無効にするには（上級ユーザのみ）：レジストリ・エディタで以下に移動します。
HKEY_LOCAL_MACHINE \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
IPEnableRouter エントリを選択します。
2. このコンピュータで使用されるインストールされたすべてのネットワーク接続で IP ルーティングを無効にするには、値 0 を割り当てます。
または
regedit.exe で、エントリを右クリックして [変更] をクリックします。regedt32.exe で、必要なエントリをクリックして [編集] をクリックし、該当するメニュー・エントリをクリックします。
3. レジストリ・エディタを閉じて再起動します。

Network Capture で記録中に結果を表示することはできますか。

もちろんです。[Run Monitor (モニタの実行)] アイコンをクリックすると、すぐに結果ビューが表示されます。Network Capture でデータを収集しているため、グラフに結果が表示されるまで少し時間がかかる場合があります。モニタが全期間の実行を完了するまでは、遅延、パケット損失、帯域幅の折れ線グラフまたはパーセンタイル分布グラフをすぐに参照できるはずですが、ある程度時間が経過した場合は、特定の期間または全期間を表示できます。詳細については、「データの表示」(45 ページ)を参照してください。

【Refresh All (すべて更新)】または【Scan Endpoints (エンドポイントのスキャン)】を選択したのですが、停止しません。

Network Capture サービスを確認し、停止している場合はサービスを開始します。その後 F5 を選択してブラウザ・ページを更新します。これでうまくいかない場合は、サポート (<https://softwaresupport.hp.com/>) までご連絡ください。

モニタはいくつまで同時に実行できますか。

プロフェッショナル・ライセンスをお持ちの場合は、最大 25 のモニタを同時に実行できます。

フォルダが必要なのはどうしてですか。

必ずしも必要という訳ではなく、Network Capture を最初に開いたときに存在する標準設定のフォルダにすべてのモニタを保管しても構いません。ただし、フォルダを使うとモニタを整理できます。Network Capture を使用していると、シナリオの種類が多くなる場合があります。地理的な場所やアプリケーションの種類など、さまざまな基準に基づいてモニタをグループ化できます。

- フォルダを追加するには、[Add Folder (フォルダの追加)] アイコンをクリックしてフォルダ名を変更します。

- サブフォルダを追加するには、各フォルダの下で、フォルダが選択されているときに [New Folder (新規フォルダ)] アイコンをクリックしてフォルダ名を変更します。
- モニタをフォルダから別のフォルダにドラッグアンドドロップすることもできます。

フォルダを削除できますか。

はい。ただし、フォルダやフォルダ内のサブフォルダに現在記録中のアクティブな実行が含まれていない場合に限りです。

エージェントはいくつインストールすればいいのですか。

Network Capture エージェントは Network Capture サーバの一部としてインストールされます。

そのため、他の場所に Network Capture エージェントをインストールしなくても、サーバから遅延、パケット損失、またはアップストリームの帯域幅可用性を測定できます。

たとえば、ニューヨークのデータセンタに Network Capture をインストール済みで、ネットワークを介してアドレス指定可能な他の場所に対する遅延、パケット損失、アップストリーム帯域幅を測定する必要がある場合は、追加の Network Capture エージェントを導入しなくても、これらの測定を行うことができます。Network Capture サーバが NAT 越しに存在する場合、サーバはピアレスとピアベースの両方のモニタリングに関与できます。

ただし、次のようにいくつかのシナリオでは、追加のエージェントが必要になります。

- 「別の場所からの測定」(62ページ)
- 「双方向帯域幅の可用性の測定」(62ページ)
- 「同時帯域幅モニタのインターバルの定義」(39ページ)

別の場所からの測定

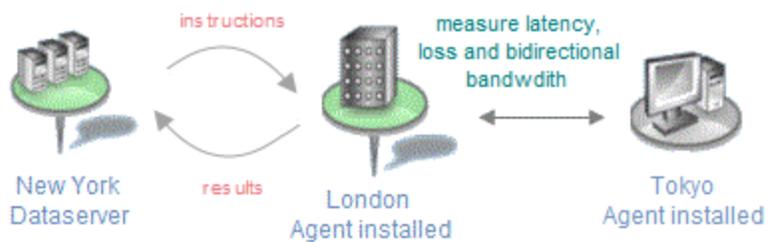
たとえば、ニューヨークのデータセンタに Network Capture サーバをインストール済みで、ロンドンから東京の宛先に対して遅延、パケット損失、アップストリーム帯域幅の測定を行う必要がある場合は、ロンドンで Network Capture エージェントをインストールできます。その後、これらのメトリックをロンドンから東京の間で測定できます。



双方向帯域幅の可用性の測定

任意の場所に対する双方向帯域幅を測定するには、ターゲットの場所にもエージェントが必要になります。たとえば、ニューヨークから東京に対して測定を行うには、エージェントを東京にインストールする必要があります。これは、ロンドンから東京への測定にも当てはまります。

測定によって同じエージェントがターゲットにもソースにもなることに注意してください。



テクニカル・サポート

HP Software Ltd. のすべてのお客様は、HP NV サイト (<http://hp.com/go/nv>) を通じてテクニカル・サポートを利用できます。テクニカル・サポートは、サポート・サイト (<https://softwaresupport.hp.com/>) を通じて利用できます。

フィードバックをお送りください



ユーザーズ・ガイドについて何かお気づきのことはありませんか？

ご意見をお聞かせください。 SW-Doc@hp.com