HP Server Automation

Enterprise Edition

ソフトウェアバージョン: 10.0

レポートガイド

ドキュメントリリース日: 2013年6月13日 (英語版)

ソフトウェアリリース日: 2013年6月

invent

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。ここでの記載で追加保証を意図するものは一切ありません。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

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。

Intel®およびItanium®は、Intel Coporationの米国およびその他の国における登録商標です。

Microsoft®、Windows®、およびWindows® XPは，Microsoft Corporationの米国における登録商標です。

OracleとJavaは、Oracle Corporationおよびその関連会社の登録商標です。

UNIX®は、The Open Groupの登録商標です。

サポート

次のHPソフトウェアサポートオンラインのWebサイトを参照してください。

http://support.openview.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。

http://h20229.www2.hp.com/passport-registration.html (英語サイト)

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。

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

サポートマトリックス

サポートおよび互換性情報については、関連する製品リリースのサポートマトリックスを参照してください。サポートマトリックスと製品マニュアルは、次のHPソフトウェアサポートオンラインのWebサイトで参照できます。

http://h20230.www2.hp.com/sc/support_matrices.jsp

また、本リリースの『HP Server Automation Support and Compatibility Matrix』は、次のHPソフトウェアサポートオンラインの製品マニュアルWebサイトからダウンロードできます。

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

ドキュメントの更新情報

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。

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

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、HP Passportのサインインページの [**New users - please register**] リンクをクリックしてください。

適切な製品サポートサービスをお申し込みいただいたお客様は、更新版または最新版をご入手いただけます。詳細は、HPの営業担当にお問い合わせください。改訂状況については、「ドキュメントの更新情報」を参照してください。

製品エディション

Server Automationには、次の2つの製品エディションがあります。

- Server Automation (SA) は、Server AutomationのEnterprise Editionです。Server Automationについては、『SA Release Notes』および『SAユーザーガイド: Server Automation』を参照してください。
- Server Automation Virtual Appliance (SAVA) は、Server AutomationのStandard Editionです。SAVAの機能については、『SAVA Release Notes』および『SAVAクイックガイド』を参照してください。

目次

第 1 章　Server Automationレポート

本書では、Server Automation (SA) レポートについて説明します。SA レポートは、SA クライアントで利用できるSAクライアントレポートと、HP Live Networkを通じて配布されるBSA Essentials (BSAE) レポートという2つの形で提供されます。

ストリームコンテンツをもつBSA Essentials レポートについては、最新版ドキュメントを HP Live Network (http://www.hp.com/go/livenetwork (英語サイト)) から入手できます。追加情報は、BSAEレポートの前提条件 (9ページ) を参照してください。

BSA Networkコネクターは、Live Network Communicator (LNc) としても知られています。

本項の内容

SAクライアントレポート

SAクライアントレポートは、環境内の管理対象サーバー、仮想サーバー、ネットワークデバイス、ユーザーのアクセス権とセキュリティ権限に関する情報をリアルタイムで提供します。これらはパラメーター化されたアクショナブルレポートで、オブジェクトに対してレポート内でポリシーや監査などの適切なアクションを実行できます。また、組織で使用しやすいように (.htmlファイルや.pdfファイル、.xlsファイルとして)、ローカルファイルシステムにエクスポートすることもできます。

SAクライアントレポート (69ページ) を参照してください。

BSA EssentialsのSAレポート

BSA Essentials (BSAE) は、Server Automation (SA) に関するデータセンターの自動化プロセスについて、ハイレベルかつ詳細な履歴レポートを提供します。BSAE の豊富なレポートを通して、データセンター自動化プロセスの費用対効果や投資収益率 (ROI) について、理解を深めることができます。また、BSAE には、サーバー、デバイス、ビジネスアプリケーションをコンプライアンス状態にするためのウィンドウが用意されています。

BSA Essentials Javaクライアントレポートストリーム

次のSAレポートストリームをダウンロードすることにより、BSA Essentials Javaクライアントを使って各SAレポートにアクセスできます。

- **sar78_reports**: BSAE Javaクライアント経由でSAコンプライアンスレポートをストリームします。SA 7.8以上のバージョンに対応しています。
- **software_discovery_reports**: BSAE Javaクライアント経由でソフトウェア検出レポートをストリームします。

BSAE Javaクライアントは、SARという名称で提供されていました。

BSA Essentials Javaクライアントレポート

BSA Essentials Javaクライアントでは、次の2つのタイプのSAレポートを表示できます。

- **SA一般レポート**

  SAの各種機能と統合モジュール (インストール済みのSAサーバーエージェント、パッチ適用 (Windows)、仮想化、デプロイメントの自動化、ストレージ、ソフトウェア検出など) に関するレポートです。

  HP Live Networkから**bsae_sa_reports**ストリームでダウンロードできます。

  BSAE Javaクライアント経由で提供されるSA一般レポート (11ページ) に、これらのレポートの説明があります。

- **SAコンプライアンスレポート**

  全体的なサーバーのコンプライアンスステータス、ポリシー別の全体的なコンプライアンス、アプリケーション構成/Windowsパッチ/監査/ソフトウェア管理などの機能に対する特定のコンプライアンスカテゴリといった、データセンターのコンプライアンス状態を表示するレポート。

  HP Live Networkから**sar78_reports**ストリームでダウンロードできます。

  BSAE Javaクライアント経由のSAコンプライアンスレポート (39ページ) に、これらのレポートの説明があります。

BSAEレポートをはじめにご使用の際は、BSAEレポートの前提条件 (9ページ) を参照してください。

BSA Essentials Webクライアント

本書では、BSA Essentials Webクライアントレポートについては説明しません。BSA Essentials Webクライアントの詳細は、次のHPソフトウェアサポートオンライン (SSO) ポータルに掲載されているBSAE製品マニュアルを参照してください。

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

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、HP Passportのサインページの [**New users - please register**] リンクをクリックしてください。

BSAEレポートの前提条件

BSAEのSAレポートを実行するには、次の要件を満たす必要があります。

- BSA Essentialsアカウントを保持していること。
  - BSA Essentialsアカウントは、HP Live Networkからリクエストできます。
- BSA Essentials Javaクライアントをインストール済みであること。
- コアサーバーにHP Live Network connector (LNc) をインストール済みかつ構成済みであること。これはHP Live Networkのクライアントで、内容の更新、ダウンロード、製品 (SAS、BSAE、SAR) へのインポートを自動化します。

  LNcはServer Automationと合わせてインストールされます。構成手順については、LNcのドキュメントを参照してください。

重要: 適切な製品を指定しない限り、LNcは内容のリスト表示、ダウンロード、プレビュー、インポートを実行しません! 製品を有効化する手順については、HP Live Networkの『Live Network connector Users Guide』を参照してください。

- ご使用のSAバージョンに適したレポートストリームと、実行したいレポートの登録があること。レポートストリームをダウンロードするには:
  - HP Live Networkにアクセスし、Live Network connectorのリンクをクリックします。
  - HP Live Networkの使用手順と正しいレポートストリームの情報に関する『LNc Users guide』をダウンロードします。
  - 特定の製品についてLNcの構成が完了すると、以下を経由して使用できるストリームの一覧も参照可能です。

    `live-network-connector list-streams`

    個別のストリームに関する追加情報は、“`describe`”コマンドを使用して入手できます。この情報には、特定のストリーム/コンテンツに関する追加情報を見つけるための詳しいテキスト説明とURLの記載があります。

URL:

- HP Live NetworkのURL＝ http://www.hp.com/go/livenetwork (英語サイト)
- HPドキュメントポータルのURL＝ http://support.openview.hp.com/selfsolve/manuals

これらのレポートへのアクセスと実行に関する追加情報については、各BSAEクライアントのオンラインヘルプを参照してください。

第 2 章　BSAE Javaクライアント経由で提供されるSA一般レポート

ここでは、BSAE Javaクライアント経由で入手可能なServer Automation (SA) 一般レポートについて説明します。レポートは、HP Live Networkから**bsae_sa_reports**ストリームでダウンロードできます。

本章の内容

レポートへのアクセスと実行に関する追加情報については、BSAE Javaクライアントのオンラインヘルプを参照してください。SAクライアントに付属するBSAE Javaクライアントのインストールに関する情報は、BSA EssentialsのSAレポート (7ページ) を参照してください。

デプロイメントライフサイクルレポート

ここでは、デプロイメントライフサイクルレポートについて説明します。

本章の内容

Server Deployments by Operating System

ここでは、Server Deployments by Operating Systemレポートについて説明します。

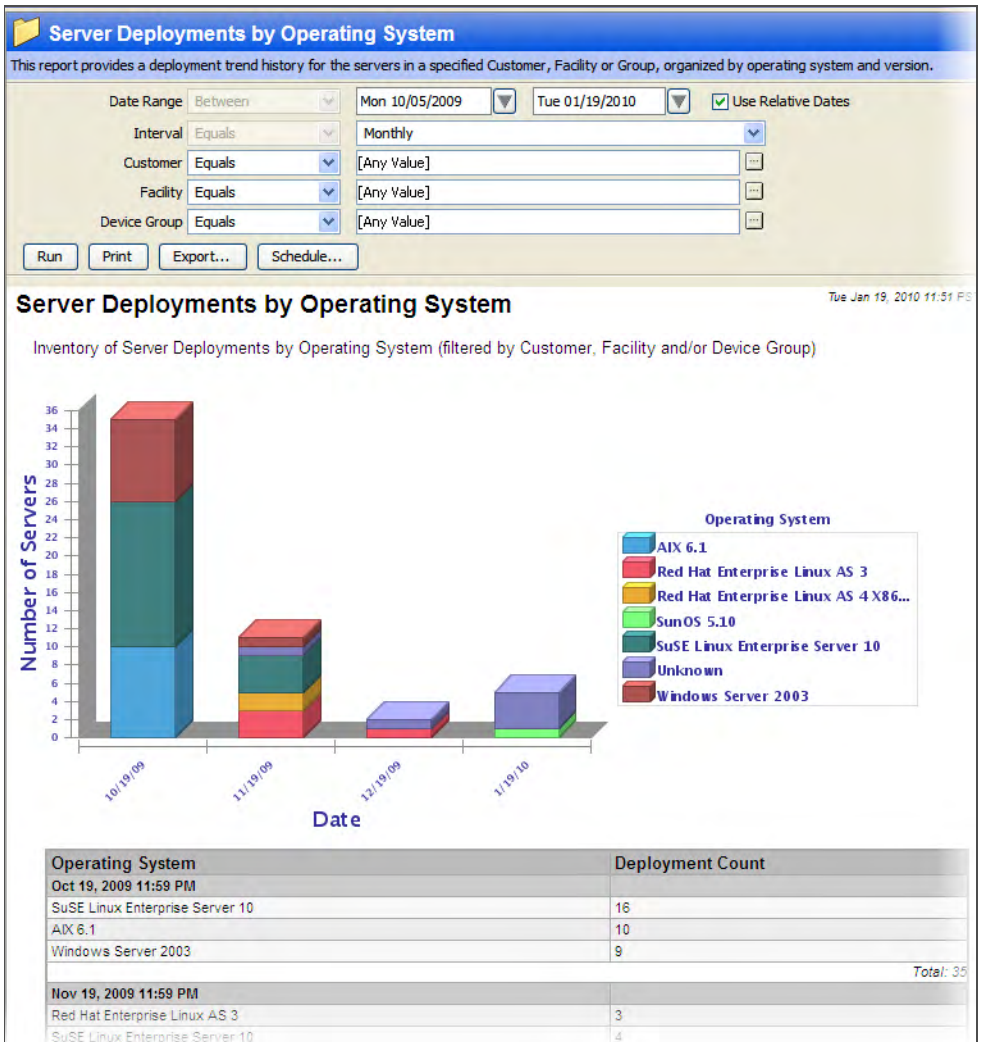
表

- サーバーデプロイメントの数は、オペレーティングシステムと期間別にグループ化されています。
- 合計の数値は、指定期間にデプロイされたサーバーの合計数を表します。

グラフ

- y軸の単位は、指定期間にデプロイされたサーバー数を示します。
- カウントは、オペレーティングシステム別にグループ化されています。
- x軸は、期間別にグループ化されています。

図 1　　Server Deployments by Operating System



その他のデプロイメントライフサイクルレポート

表1では、BSAE Javaクライアントで提供されているその他のデプロイメントライフサイクルレポートをまとめています。

表 1　　デプロイメントライフサイクルレポート

レポートタイトル	説明
Devices by Type	選択したサーバー上にあるすべてのデバイスを、デバイスタイプ別に表示します。
Network Devices by Device Type	選択したサーバー上にあるネットワークデバイスを、デバイスタイプ別に表示します。
Servers by Architecture	サーバーをアーキテクチャ別に表示します。
Servers by Operating System	サーバーをオペレーティングシステム別に表示します。

検出されたソフトウェアのレポート

Server Automation (SA) のソフトウェア検出モジュールでは、WindowsとUnixの管理対象サーバーで署名ベースのソフトウェア検出を実行する機能を使って、SAの管理対象ではないアプリケーションとソフトウェアの管理をサポートします。

ソフトウェア検出モジュールでは、次に示すレポートが提供されています。

このレポートを使用するには、software_discovery_reportsストリームの登録が必要です。ソフトウェア検出モジュールを使用するための前提条件など、詳細については『SA Software Discovery Guide』を参照してください。

表2では、検出されたソフトウェアのレポートをまとめます。このレポートは、ソフトウェア検出モジュールを稼働するシステム上で、BSAE Javaクライアント経由で使用できます。

表 2　検出されたソフトウェアのレポート

レポートタイトル	説明
Discovered Applications	選択したサーバー上で検出されたアプリケーションを表示します。
Servers with Discovered Software	選択したソフトウェアがインストールされているサーバーを表示します。
Discovered Software by Server	検出されたアプリケーションをサーバーごとに表示します。
Discovered Software by Application	検出されたアプリケーションを、インストールされているサーバーごとに表示します。

ストレージレポート

ストレージレポートは、ユーザー環境内に設置されている管理対象サーバーのストレージ構成、ストレージハードウェア、ストレージソフトウェアについて、包括的な情報をリアルタイムで提供します。このレポートは、ストレージ不足が発生するタイミングの予測や、アプリケーションによるストレージ使用量のトレンド分析などに活用できます。

レポートはパラメーター化され、グラフと表の形式で表示されます。また、アクショナブルなレポートなので、レポート内のオブジェクトで適切なアクションの実行が可能です。また、使用しやすい形式 (.pdf、.html、.xlsファイルなど) を使ってローカルファイルシステムにエクスポートできます。

ストレージレポートは、次のフォルダーに分類されています。

- [Reports] > [Storage Reports] > [Database Storage Reports]
- [Reports] > [Storage Reports] > [Host and Application Storage Reports]
- [Reports] > [Storage Reports] > [Storage Array Reports]
- [Reports] > [Storage Reports] > [Storage Switch and Fabric Reports]

ストレージレポートは、Storage Host Agent Extension (SHA) がインストールされ、稼働している管理対象サーバーのみで使用できます。SHAのインストールについては、『Storage Visibility and Automationインストールおよび管理ガイド』を参照してください。

本章の内容

データベースストレージレポート

BSAE Javaクライアントでは、表3で示すデータベースストレージレポートが提供されています。

表 3　　データベースストレージレポート

レポートタイトル	説明
Database Allocation Trend	データベースへの割り当て容量と使用容量の変化を時系列で示し、今後の変化を予測します。
Database Capacity and Utilization Trend Data	データベースの容量と使用率の変化を時系列で示し、今後の変化を予測します。
Database Inventory	システムで認識されているデータベース (Oracle) と基本的なインベントリ情報を表示します。
Database Utilization Trend	データベースの使用率の変化を時系列で示し、今後の変化を予測します。
Tablespace Allocation Trend	1つまたは複数のデータベースについて、1つまたは複数の表領域の割り当て容量と使用容量の変化を時系列で示し、今後の変化を予測します。
Tablespace Capacity and Utilization Overview	表領域、表領域の容量、使用率をデータベースごとに表示します。
Tablespace Capacity and Utilization Trend Data	1 つまたは複数のデータベースまたは表領域の使用率の変化を時系列で示し、今後の変化を予測します。
Tablespace Utilization Trend	1つまたは複数のデータベースについて、1つまたは複数の表領域の使用率の変化を時系列で示し、今後の変化を予測します。

ホストおよびアプリケーションに関するストレージレポート

BSAE Javaクライアントでは、表4で示すホストおよびアプリケーションストレージレポートが提供されています。

表 4　　ホストおよびアプリケーションに関するストレージレポート

レポートタイトル	説明
Host Capacity and Utilization Detail	このレポートでは、ホスト上の各エンティティについて、容量および使用率に関する詳細情報を表示します。
Host Capacity and Utilization Overview	ホストの容量および使用率に関する詳細情報を、カスタマー、ファシリティ、デバイスグループごとにまとめて表示します。
Host Capacity and Utilization Trend Data	ホストの容量および使用率に関するトレンド情報を、カスタマー、ファシリティ、デバイスグループごとにまとめて表示します。
Host DB Storage Allocation Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、データベースストレージの割り当て容量と使用容量の変化を時系列で示し、今後の変化を予測します。
Host DB Storage Utilization Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、データベースストレージの使用率の変化を時系列で示し、今後の変化を予測します。
Host File System Storage Allocation Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、ファイルシステムストレージの割り当て容量と使用容量の変化を時系列で示し、今後の変化を予測します。
Host File System Storage Utilization Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、ファイルシステムストレージの使用率の変化を時系列で示し、今後の変化を予測します。
Host Reclaimable Storage Overview	ホスト用に再利用可能なストレージ容量をストレージタイプ別に表示します。
Host Storage Detail	選択したホストについて、すべてのストレージ関連情報を詳細に表示します。
Host Storage Inventory	ホストに関する基本的なインベントリ情報とストレージ統計情報を表示します。

表 4　ホストおよびアプリケーションに関するストレージレポート (続き)

レポートタイトル	説明
Host Total Storage Allocation Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、ストレージの割り当て容量の合計と使用容量の合計の変化を時系列で示し、今後の変化を予測します。
Host Total Storage Utilization Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、データベースストレージの総使用率の変化を時系列で示し、今後の変化を予測します。
Host Volume Manager Storage Allocation Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、ボリュームマネージャーのストレージ割り当て容量と使用容量の変化を時系列で示し、今後の変化を予測します。
Host Volume Manager Storage Utilization Trend	ホスト (カスタマー、ファシリティ、デバイスグループ別) について、ボリュームマネージャーのストレージ使用率の変化を時系列で示し、今後の変化を予測します。
Hypervisor Host Storage Detail	選択した VMware ハイパーバイザーについて、詳細なストレージ関連情報 (データストアやボリュームの情報など) を表示します。
Host Capacity and Utilized DB Storage > Distribution of Utilized DB Storage	データベースストレージの使用容量について、カスタマー、ファシリティ、デバイスグループの内訳と概要を表示します。

ストレージアレイレポート

BSAE Javaクライアントでは、表5で示すストレージアレイレポートが提供されています。

表 5　　ストレージアレイレポート

レポートタイトル	説明
Array Capacity and Utilization Overview	SAN ストレージアレイと NAS ファイラーの容量と使用率に関する統計情報を、指定したカスタマー、ファシリティ、デバイスグループごとにサマリーで表示します。
Array Inventory	SANストレージアレイとNASファイラーについて、基本的なイベント理情報とストレージ統計情報を表示します。
Storage Allocated to Hosts Unmanaged by the SA Storage	SA ストレージでは認識されていないホストまたは管理対象外のホストにストレージを提供しているアレイとファイラーを表示します。

ストレージスイッチとファブリックに関するレポート

BSAE Javaクライアントでは、表6で示すストレージスイッチおよびファブリックのレポートが提供されています。

表 6　　ストレージスイッチとファブリックに関するレポート

レポートタイトル	説明
Zone Inventory	指定したファブリック / ゾーンセットのゾーン構成インベントリを簡単に表示します。ゾーンがわかりやすく表示されているので、トラブルシューティング、プロビジョニング、現在の構成の分析に使用すると便利です。

プロセス自動化に関するレポート

BSAE Javaクライアントでは、表7で示すプロセス自動化レポートが提供されています。

表 7　　PASレポート

レポートタイトル	説明
PAS Run History Summary by Device	プロセス自動化デバイスの情報をサマリーで表示します。
PAS Run History Summary by Flow	プロセス自動化フローの情報をサマリーで表示します。
PAS Run History Details by Device	プロセス自動化デバイスの履歴情報を詳細に表示します。
PAS Run History Details by Flow	プロセス自動化フローの履歴情報を詳細に表示します。

仮想化レポート

この項では、仮想サーバー環境に関するレポートについて説明します。

本項の内容

Managed Virtual vs. Physical Servers Trend Data

このレポートには、ある期間における管理対象仮想サーバーと管理対象物理サーバーの割合が表示されます。各タイプのサーバーの割合が、時間とともにどのように変化しているかを示します。

グラフ

- y軸は、各サーバータイプ (仮想サーバーと物理サーバー) の割合を示します。
- x軸は、日付を示します。
- 下の図2では、約10%が管理対象サーバーと仮想サーバー、残りの90%が物理サーバーとなっています。

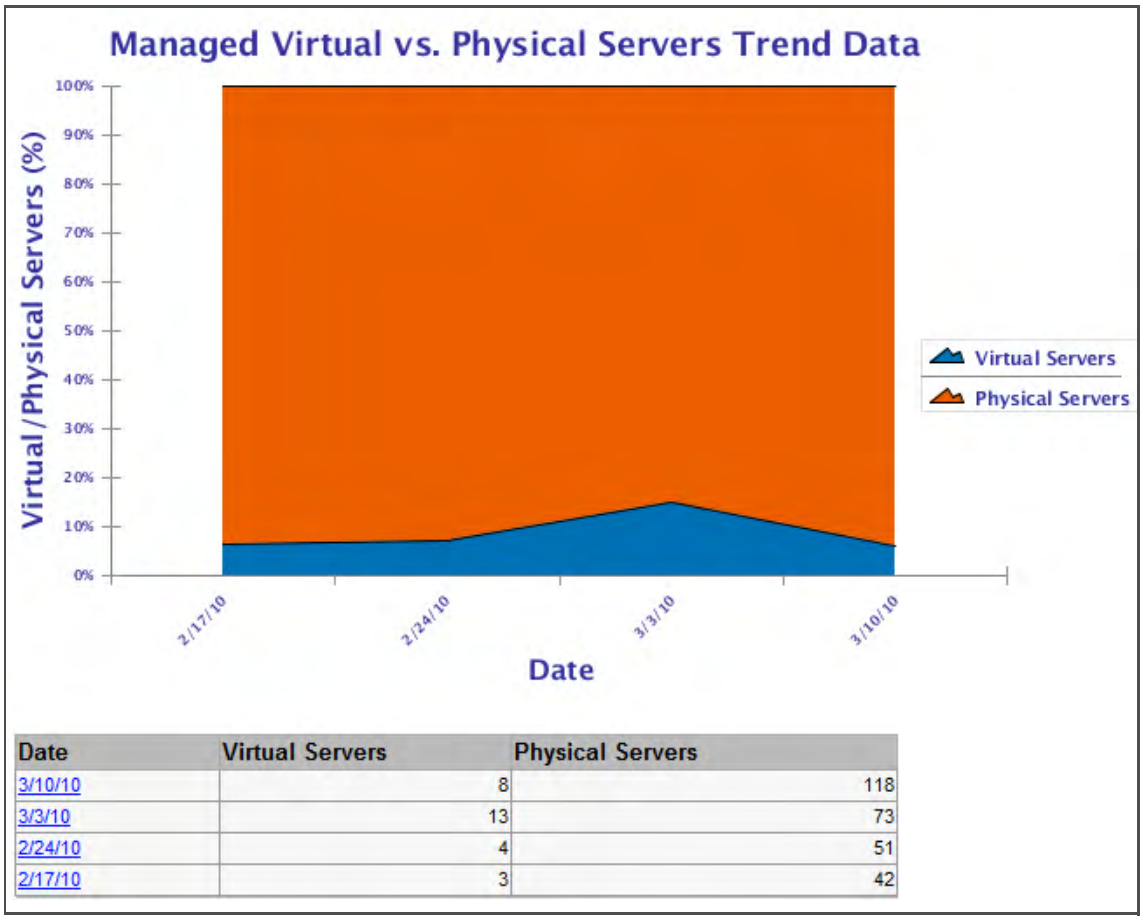
表

- 表は、指定した日付の範囲と期間における各日の仮想サーバーと物理サーバーの数を表します。

詳細を得るには

- 表の日付をクリックすると、その日付の全サーバーが一覧表示されます。

図 2　　Managed Virtual vs. Physical Servers Trend Data



Date	Virtual Servers	Physical Servers
3/10/10	8	118
3/3/10	13	73
2/24/10	4	51
2/17/10	3	42

Virtual Servers Running/Not Running Ratio

このグラフには、実行中の仮想サーバーの数と実行していない仮想サーバーの数が、経時的に表示されます。これはどの仮想サーバーが使用されておらず、削除候補となる可能性があるか、判断するのに役立ちます。

グラフ

- y軸は、サーバーの数を示します。
- x軸は、測定が行われた日付を示します。

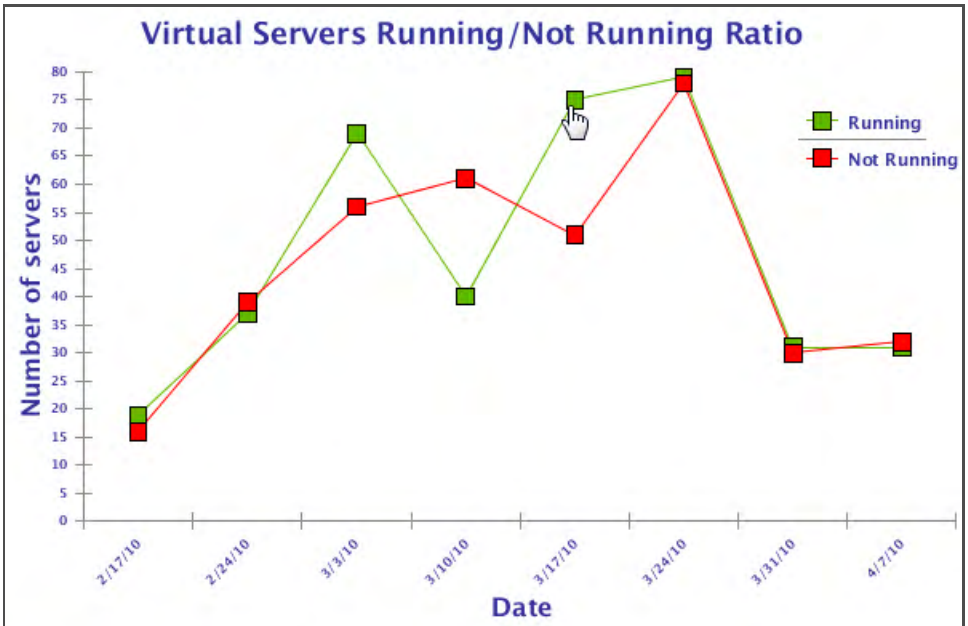
表

- 表は、指定期間における各日のカテゴリ別合計サーバー数の一覧を示します。
- 実行していない合計サーバー数は、指定した日付に電源がオフになっていたか、実行していなかったすべての管理対象/非管理対象仮想サーバーを表します。
- 実行中の合計サーバー数は、指定した日付に電源がオンになっており、実行していたすべての管理対象/非管理対象仮想サーバーを表します。

詳細を得るには

- グラフのデータポイントまたは表の日付をクリックすると、その日付の当該カテゴリの全仮想サーバーが一覧表示されます。

図 3　　Virtual Servers Running and Not Running



Date	Running	Not Running
4/7/10	31	32
3/31/10	31	30
3/24/10	79	78
3/17/10	75	51
3/10/10	40	61
3/3/10	69	56
2/24/10	37	39
2/17/10	19	16

Virtualization Infrastructure Overview

このレポートでは、管理対象仮想/物理サーバー、管理対象/非管理対象仮想サーバー、ハイパーバイザー /非ハイパーバイザー物理サーバーを比較します。

グラフ

これらの3つのグラフは、環境全体における仮想化のタイプと度合いを示します。

- [Number of Managed Virtual vs. Managed Physical Servers] では、すべての管理対象仮想サーバーをすべての管理対象物理サーバーと比較し、(VMware、Hyper-V、Solarisなどの) 仮想環境全体における仮想化の度合いを表示します。
- [Number of Managed vs. Unmanaged Virtual Servers] では、すべての管理対象仮想サーバーをすべての非管理対象仮想サーバーと比較します。
- [Number of Hypervisor vs. Non-Hypervisor Physical Servers] では、すべての管理対象ハイパーバイザー物理サーバーをすべての管理対象非ハイパーバイザー物理サーバーと比較します。

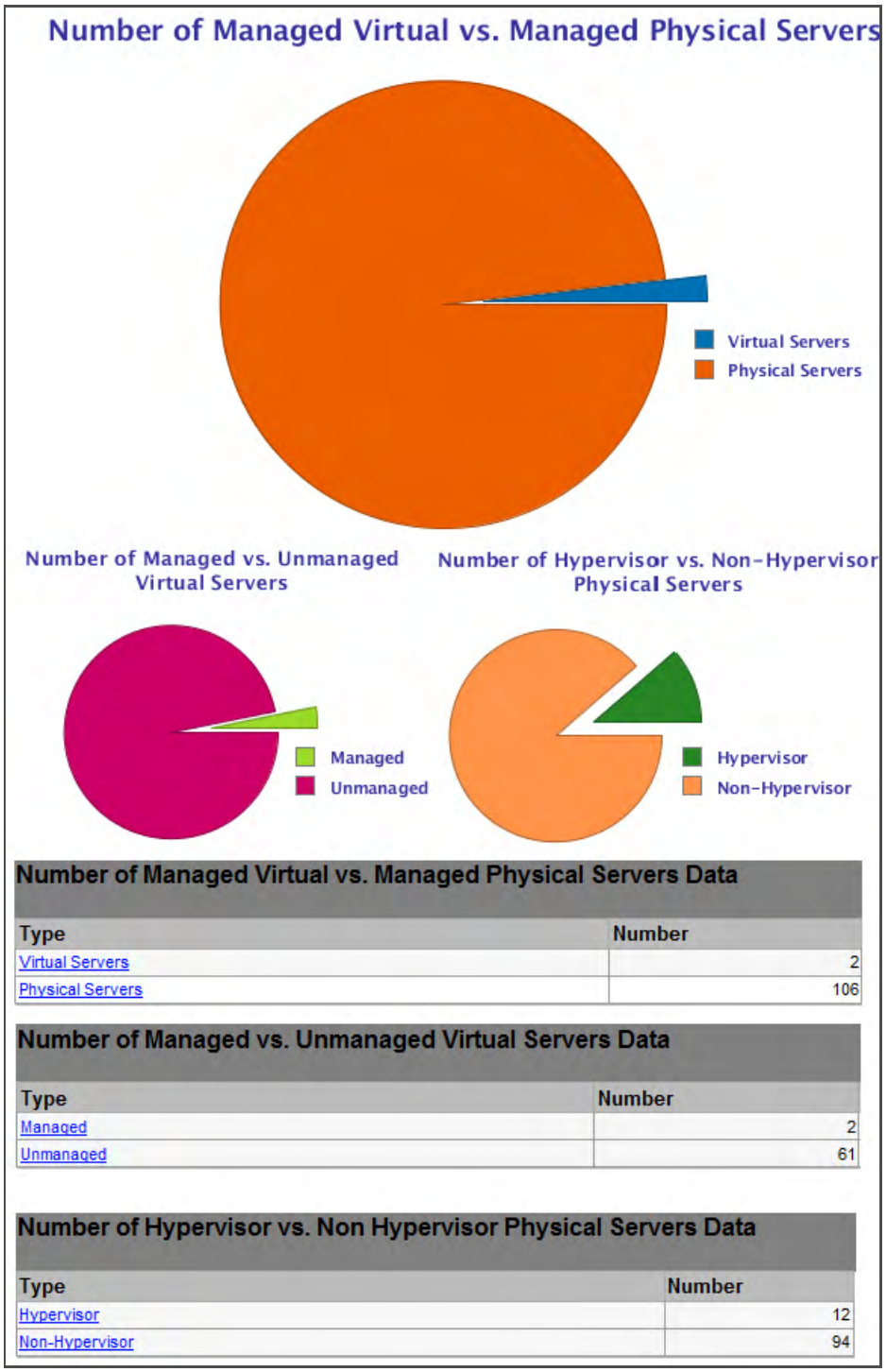
表

- 各表は円グラフの対応するデータを示します。

詳細を得るには

- いずれかの円グラフの項目または表のリンクをクリックすると、そのグループの全サーバーが一覧表示されます。

図 4　　仮想サーバーと物理サーバーを示す円グラフ



Number of Managed Virtual vs. Managed Physical Servers Data

Type	Number
Virtual Servers	2
Physical Servers	106

Number of Managed vs. Unmanaged Virtual Servers Data

Type	Number
Managed	2
Unmanaged	61

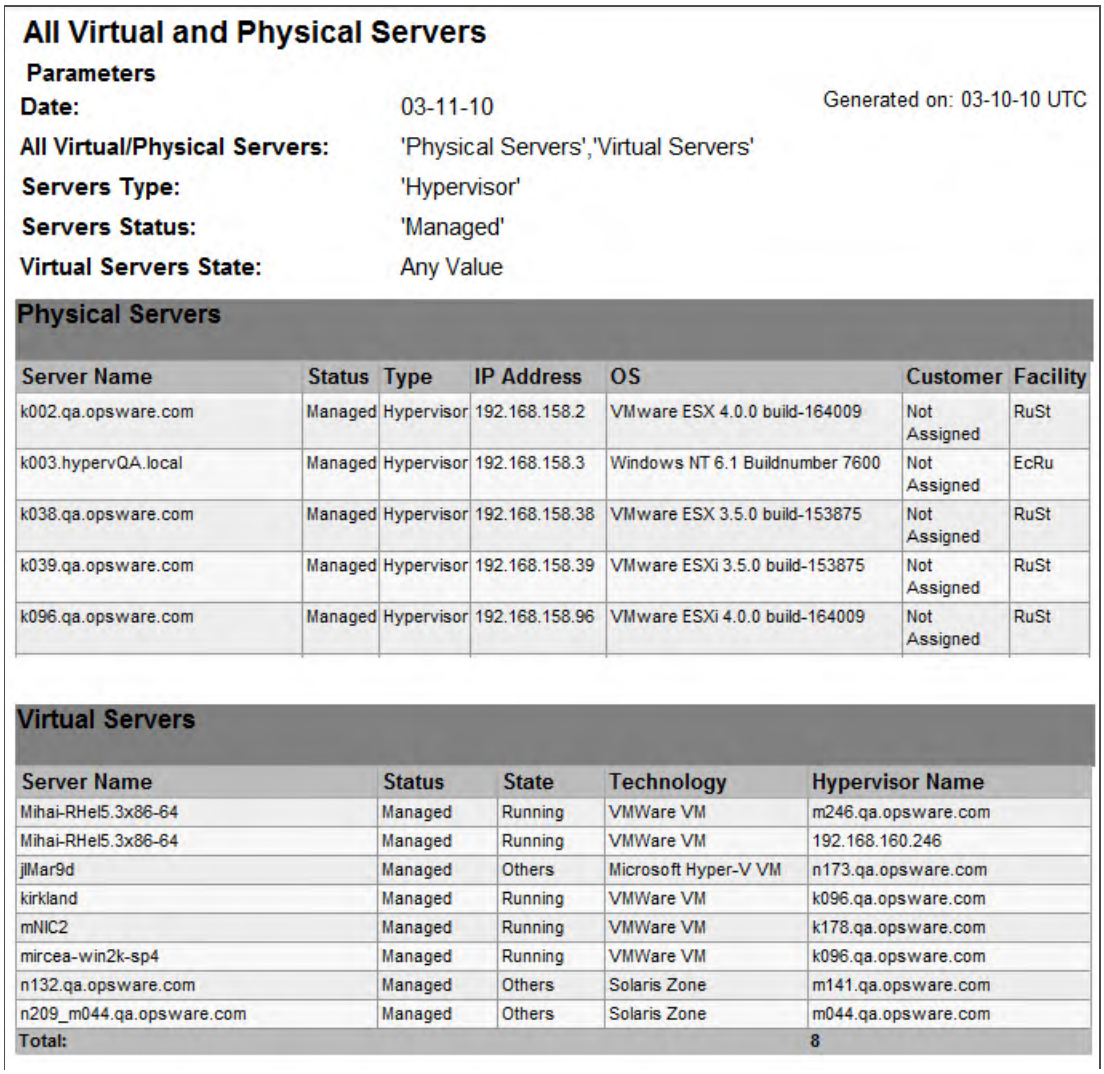
Number of Hypervisor vs. Non Hypervisor Physical Servers Data

Type	Number
Hypervisor	12
Non-Hypervisor	94

All Virtual and Physical Servers

このレポートには、指定した日付のすべての仮想サーバーと物理サーバーの詳細が表示されます。また、サーバータイプ、ハイパーバイザー /非ハイパーバイザー、サーバーが管理対象/非管理対象か、サーバーが実行中/停止中かも表示します。下の図5は、この表の一例を示しています。

図 5　　すべての仮想サーバーと物理サーバーを示す表



All Virtual and Physical Servers

Parameters

Generated on: 03-10-10 UTC

Date:	03-11-10
All Virtual/Physical Servers:	'Physical Servers','Virtual Servers'
Servers Type:	'Hypervisor'
Servers Status:	'Managed'
Virtual Servers State:	Any Value

Physical Servers

Server Name	Status	Type	IP Address	OS	Customer	Facility
k002.qa.opsware.com	Managed	Hypervisor	192.168.158.2	VMware ESX 4.0.0 build-164009	Not Assigned	RuSt
k003.hypervQA.local	Managed	Hypervisor	192.168.158.3	Windows NT 6.1 Buildnumber 7600	Not Assigned	EcRu
k038.qa.opsware.com	Managed	Hypervisor	192.168.158.38	VMware ESX 3.5.0 build-153875	Not Assigned	RuSt
k039.qa.opsware.com	Managed	Hypervisor	192.168.158.39	VMware ESXi 3.5.0 build-153875	Not Assigned	RuSt
k096.qa.opsware.com	Managed	Hypervisor	192.168.158.96	VMware ESXi 4.0.0 build-164009	Not Assigned	RuSt

Virtual Servers

Server Name	Status	State	Technology	Hypervisor Name
Mihai-RHel5.3x86-64	Managed	Running	VMWare VM	m246.qa.opsware.com
Mihai-RHel5.3x86-64	Managed	Running	VMWare VM	192.168.160.246
jlMar9d	Managed	Others	Microsoft Hyper-V VM	n173.qa.opsware.com
kirkland	Managed	Running	VMWare VM	k096.qa.opsware.com
mNIC2	Managed	Running	VMWare VM	k178.qa.opsware.com
mircea-win2k-sp4	Managed	Running	VMWare VM	k096.qa.opsware.com
n132.qa.opsware.com	Managed	Others	Solaris Zone	m141.qa.opsware.com
n209_m044.qa.opsware.com	Managed	Others	Solaris Zone	m044.qa.opsware.com
Total:				**8**

アプリケーションデプロイメントレポート

この項では、HP Server Automationで実行されるアプリケーションデプロイメント アクティビティに関するレポートについて説明します。

本章の内容

アプリケーションデプロイメントの詳細については、『HP Server Automation Application Deployment User Guide』を参照してください。

Time to Production

このレポートでは、アプリケーションがアプリケーションライフサイクルを完了するまでにかかる時間を確認できます。アプリケーションの各リリースについて、このレポートではアプリケーションがアプリケーションライフサイクルの最後のステージ (通常はプロダクション環境) に到達するまでの所要時間を示します。

リリースの最初のバージョンが作成されてから、ライフサイクルの最終ステージに初めて問題なくデプロイされるまでの時間を計算します。アプリケーションが最後のライフサイクルステージからロールバックされる場合、アプリケーションは正常にデプロイされたとみなされません。

パラメーター

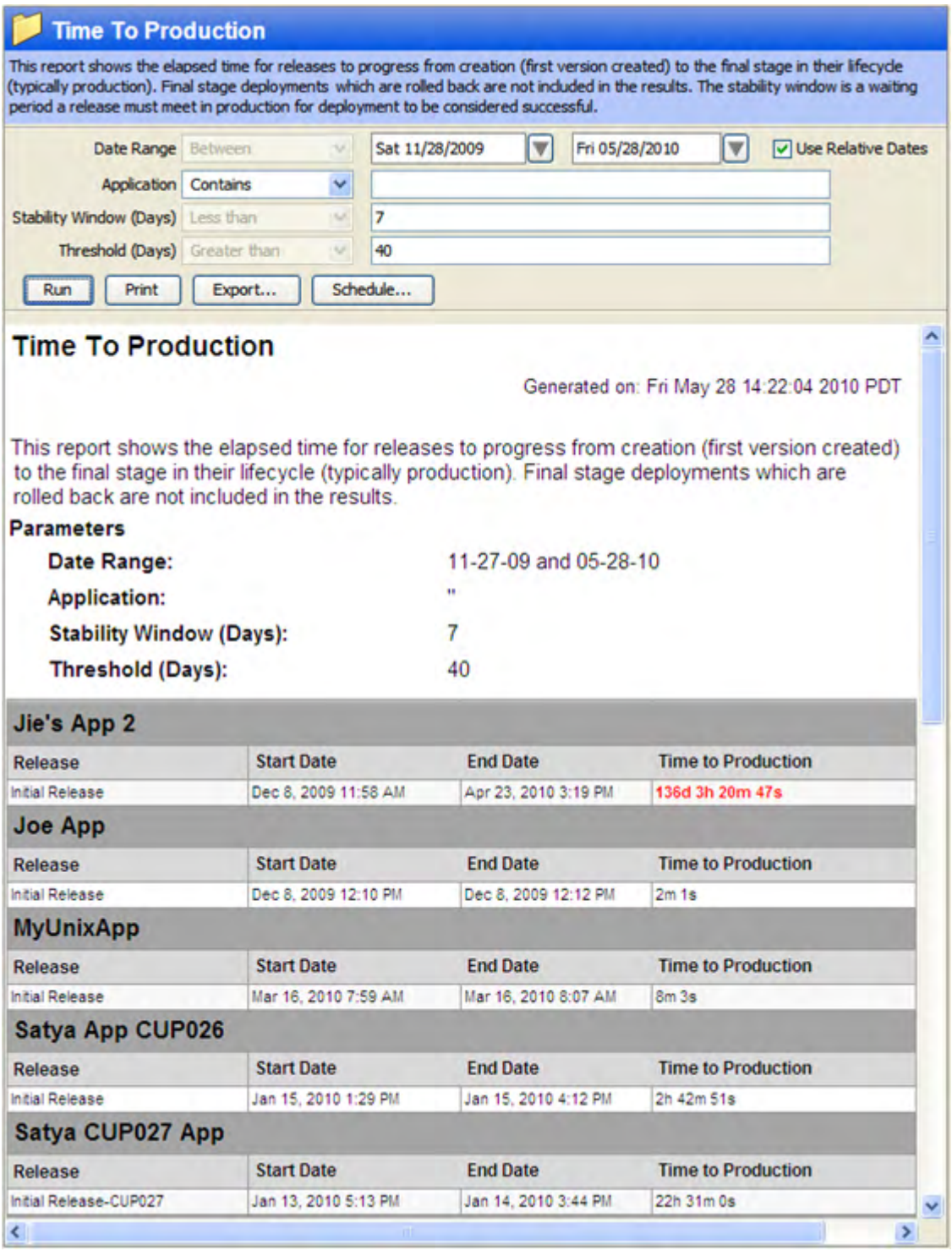
プロダクションに要した時間レポートは、次のパラメーターを組み合わせてフィルター処理できます。

- **Date Range**: すべてのアプリケーションがプロダクション環境へ正常にデプロイされた日付の範囲をカウント。
- **Application**: デプロイされる指定アプリケーション。
- **Stability Window (Days)**: アプリケーションが正常なリリースとみなされるために、ライフサイクルの最終環境 (通常はプロダクション) にデプロイされた状態を保持しなければならない日数。このウィンドウの範囲内にアプリケーションがロールバックされる場合、リリースは「プロダクション」にあるとはみなされません。
- **Threshold (Days)**: このしきい値より高い場合、プロダクションに要した時間を赤で表示。つまり、プロダクションに至るまでこの日数より長くかかったアプリケーションは赤で表示されます。

表

レポートはアプリケーション別にグループ化、またリリース別にサブグループ化されます。

図 6　　Time To Production レポート



詳細を得るには

このレポートでは、ドリルダウンは使用できません。

デプロイメント成功レポート (アプリケーション別と環境別)

これらのレポートでは、アプリケーションデプロイメントの成功頻度を表すデータを表示できます。選択した日付の範囲の各月について、レポートはデプロイメントジョブの試行回数と成功回数を示します。また、選択した日付の範囲の各月について、この情報を比率の形で表します。アンデプロイメントとロールバックジョブは計算に含まれません。

Deployment Success by Applicationレポートのパラメーター

Deployment Success by Applicationレポートは、次の項目を組み合わせてフィルター処理できます。

- **Date**: データをレポートする12か月間の終了日。
- **Application**: デプロイされる指定アプリケーション。
- **Threshold (%)**: このしきい値より低い場合、成功率を赤で表示。

Deployment Success by Environmentレポートのパラメーター

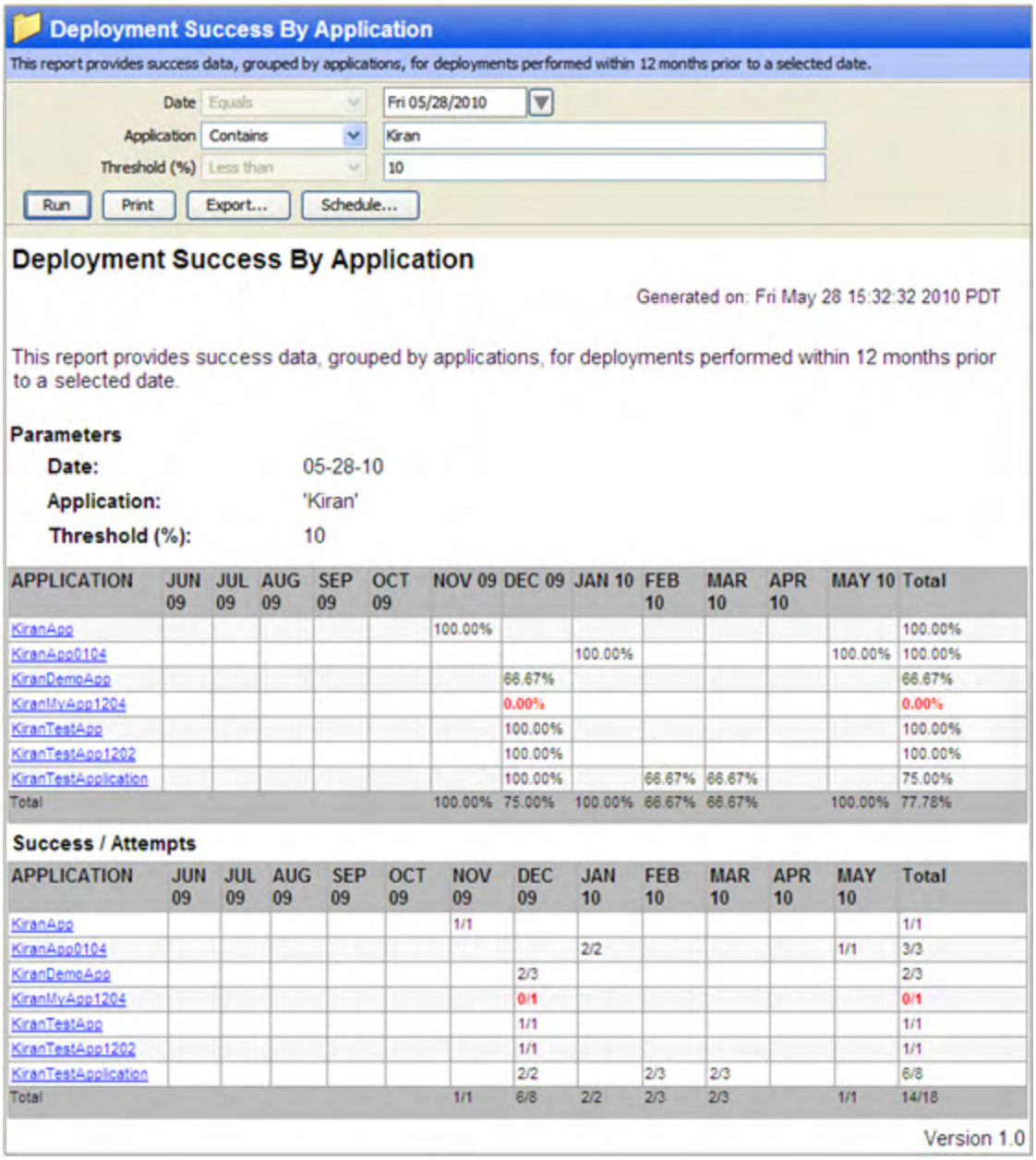
Deployment Success by Environmentレポートは、次のいずれかの組み合わせを用いてフィルター処理できます。

- **Date**: データをレポートする12か月間の終了日。
- **Environment**: QAまたは本番などのアプリケーションデプロイメント環境。アプリケーションデプロイメント環境は、SAデバイスグループとしてミラーリングされます。
- **Threshold (%)**: このしきい値より低い場合、成功率を赤で表示。

表

テーブルの各行は、環境またはアプリケーションごとの成功データを表します。指定日以前の12か月のウィンドウの各月と、期間全体の成功データがレポートされます。

図 7　　Deployment Success by Application レポート



Deployment Success By Application

This report provides success data, grouped by applications, for deployments performed within 12 months prior to a selected date.

Date: Equals — Fri 05/28/2010

Application: Contains — Kiran

Threshold (%): Less than — 10

Run | Print | Export... | Schedule...

Deployment Success By Application

Generated on: Fri May 28 15:32:32 2010 PDT

This report provides success data, grouped by applications, for deployments performed within 12 months prior to a selected date.

Parameters

Date: 05-28-10

Application: 'Kiran'

Threshold (%): 10

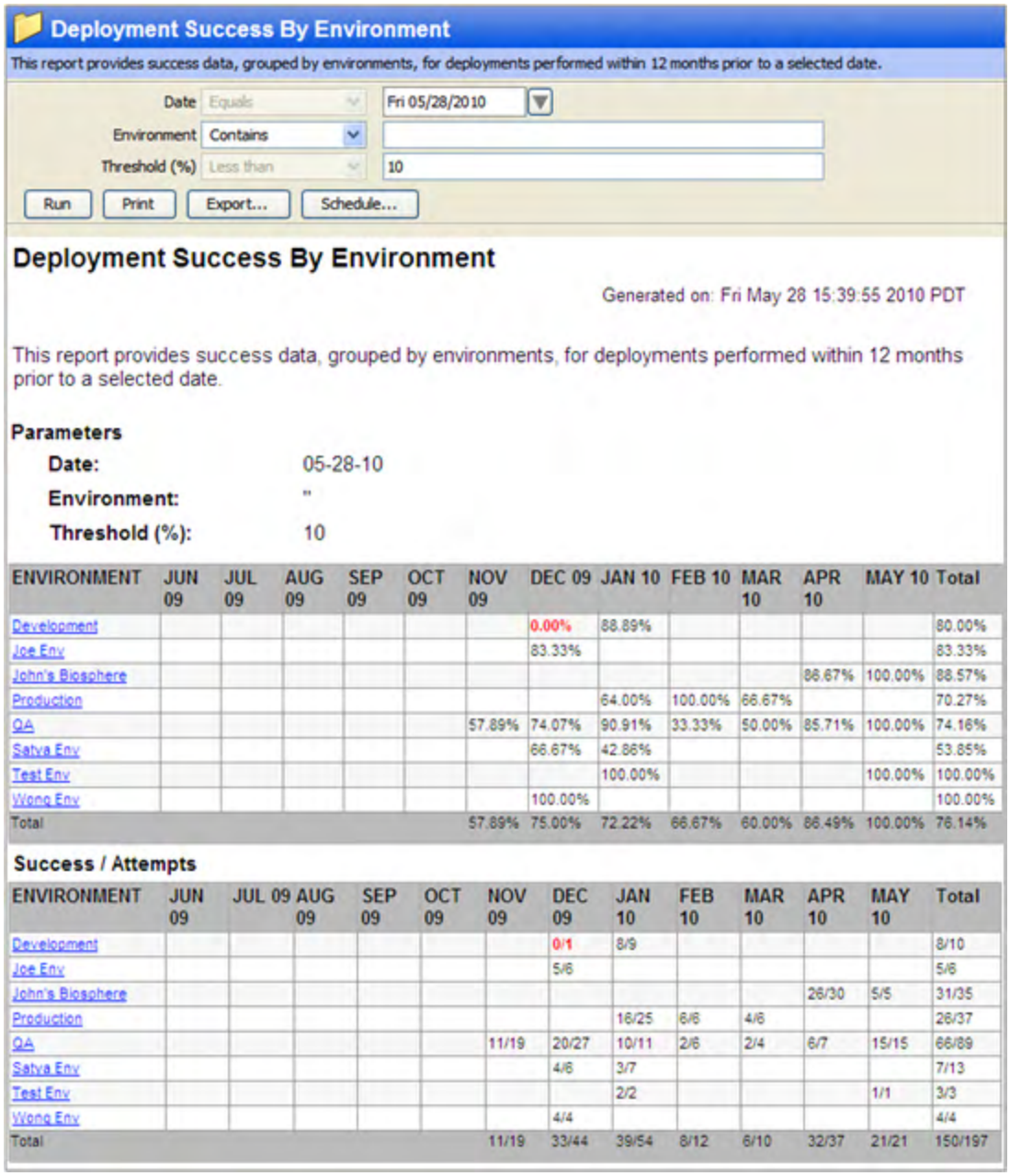
APPLICATION	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
KiranApp						100.00%							100.00%
KiranApp0104								100.00%				100.00%	100.00%
KiranDemoApp							66.67%						66.67%
KiranMyApp1204							0.00%						0.00%
KiranTestApp							100.00%						100.00%
KiranTestApp1202							100.00%						100.00%
KiranTestApplication							100.00%		66.67%	66.67%			75.00%
Total						100.00%	75.00%	100.00%	66.67%	66.67%		100.00%	77.78%

Success / Attempts

APPLICATION	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
KiranApp						1/1							1/1
KiranApp0104								2/2				1/1	3/3
KiranDemoApp							2/3						2/3
KiranMyApp1204							0/1						0/1
KiranTestApp							1/1						1/1
KiranTestApp1202							1/1						1/1
KiranTestApplication							2/2		2/3	2/3			6/8
Total						1/1	6/8	2/2	2/3	2/3		1/1	14/18

Version 1.0

図 8　　Deployment Success by Environmentレポート



Deployment Success By Environment

This report provides success data, grouped by environments, for deployments performed within 12 months prior to a selected date.

Date: Equals Fri 05/28/2010

Environment: Contains

Threshold (%): Less than 10

Run | Print | Export... | Schedule...

Deployment Success By Environment

Generated on: Fri May 28 15:39:55 2010 PDT

This report provides success data, grouped by environments, for deployments performed within 12 months prior to a selected date.

Parameters

Date: 05-28-10

Environment: ''

Threshold (%): 10

ENVIRONMENT	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
Development							0.00%	88.89%					80.00%
Joe Env							83.33%						83.33%
John's Biosphere											86.67%	100.00%	88.57%
Production								64.00%	100.00%	66.67%			70.27%
QA						57.89%	74.07%	90.91%	33.33%	50.00%	85.71%	100.00%	74.16%
Satya Env							66.67%	42.86%					53.85%
Test Env								100.00%				100.00%	100.00%
Wong Env							100.00%						100.00%
Total						57.89%	75.00%	72.22%	66.67%	60.00%	86.49%	100.00%	76.14%

Success / Attempts

ENVIRONMENT	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
Development							0/1	8/9					8/10
Joe Env							5/6						5/6
John's Biosphere											26/30	5/5	31/35
Production								16/25	6/6	4/6			26/37
QA						11/19	20/27	10/11	2/6	2/4	6/7	15/15	66/89
Satya Env							4/6	3/7					7/13
Test Env								2/2				1/1	3/3
Wong Env							4/4						4/4
Total						11/19	33/44	39/54	8/12	6/10	32/37	21/21	150/197

詳細を得るには

- Deployment Success by Environment レポートのアプリケーション名をクリックすると、当該アプリケーションのApplication Deployment Activityレポートがドリルダウンされます。
- Deployment Success by Environmentレポートの環境名をクリックすると、当該環境のApplication Deployment Activityレポートがドリルダウンされます。

ROIレポート (アプリケーション別と環境別)

ROI レポートでは、アプリケーションデプロイメントを使って、投資収益率 (ROI) を確認することができます。レポートは、[Application] または [Environment] 別にグループ化して作成できます。

(ターゲットマシンごとの) ROI 値を、Application Deployment Manager のリリースに割り当てることができます。アプリケーションの ROI は、このアプリケーションのすべてのリリースが正常にデプロイされた全ターゲットのROI値の合計になります。

ROI 値は、意図的に単位を付けずに表示されます。通貨や使用時間、またはお客様の組織に合った単位をご使用になれます。

ROI by Applicationレポートのパラメーター

ROI by Applicationレポートは、次のいずれかの組み合わせを用いてフィルター処理できます。

- **Date**: ROIをレポートする12か月間の終了日。
- **Application**: デプロイされる指定アプリケーション。

ROI by Environmentレポートのパラメーター

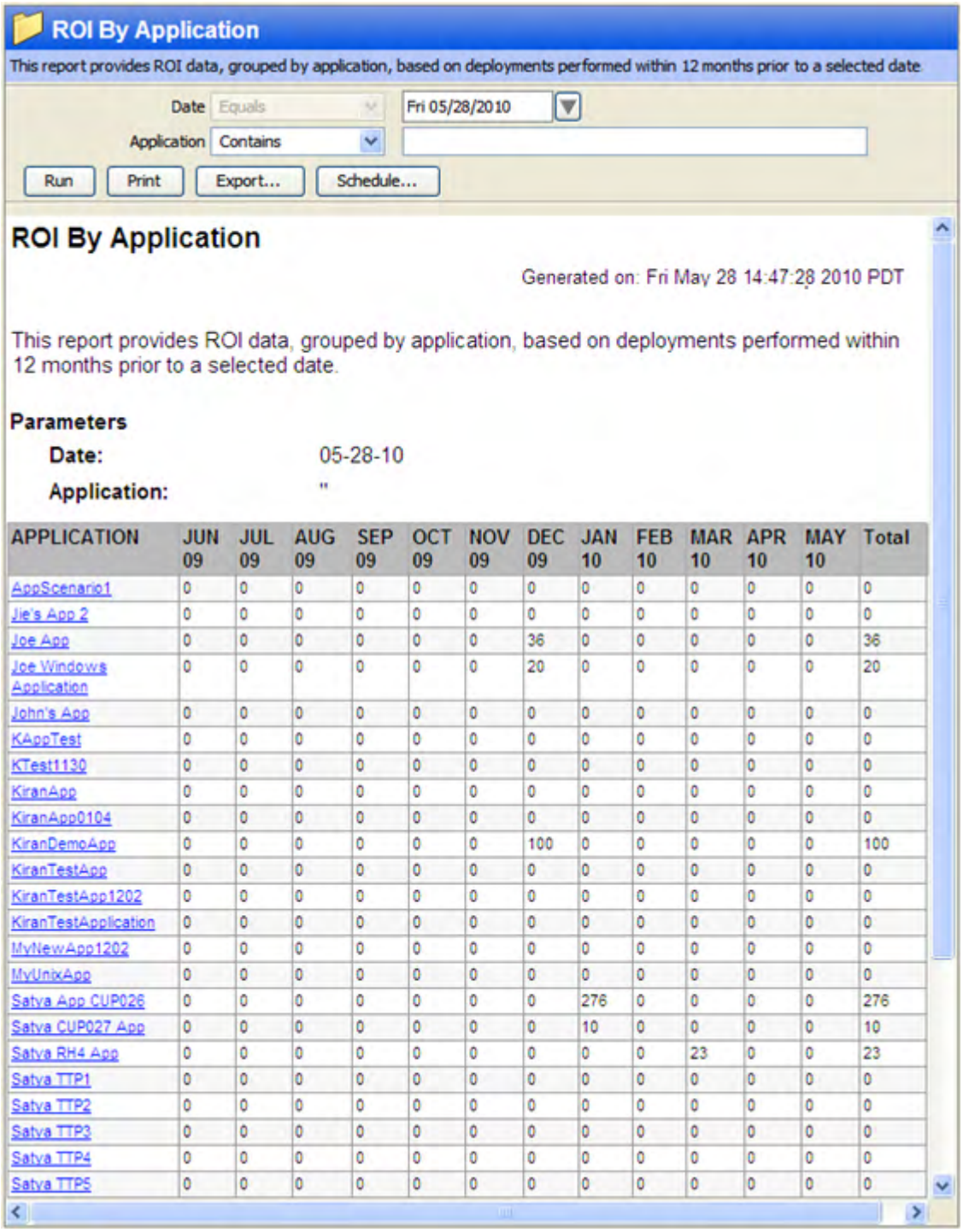
ROI by Environmentレポートは、次のいずれかの組み合わせを用いてフィルター処理できます。

- **Date**: ROIをレポートする12か月間の終了日。
- **Environment**: QA または本番などのアプリケーションデプロイメント環境。アプリケーションデプロイメント環境は、SAデバイスグループとしてミラーリングされます。

表

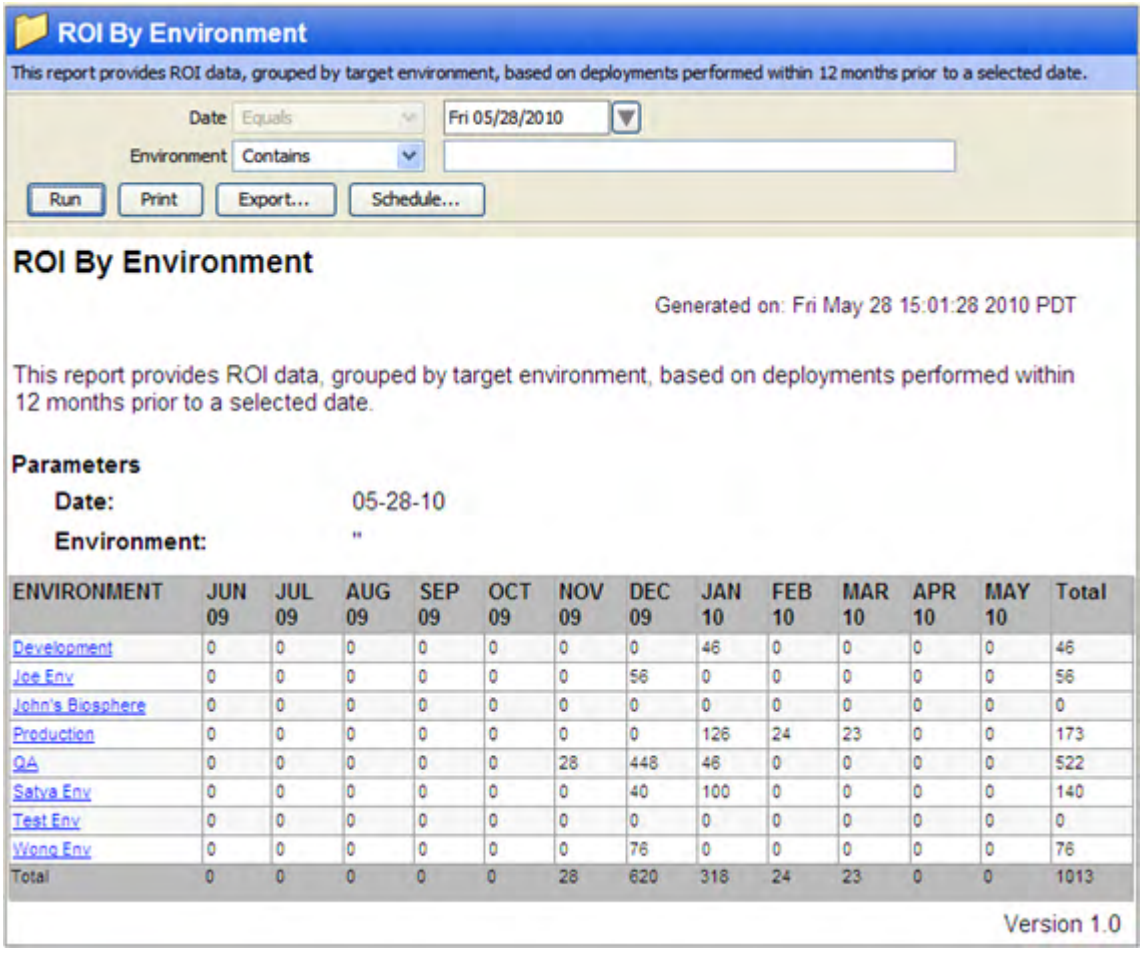
テーブルの各行は、指定期間の各月に達成されるROIと、期間全体のROI合計を表します。

図 9　　Application Deployment ROI by Application レポート



APPLICATION	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
AppScenario1	0	0	0	0	0	0	0	0	0	0	0	0	0
Jie's App 2	0	0	0	0	0	0	0	0	0	0	0	0	0
Joe App	0	0	0	0	0	0	36	0	0	0	0	0	36
Joe Windows Application	0	0	0	0	0	0	20	0	0	0	0	0	20
John's App	0	0	0	0	0	0	0	0	0	0	0	0	0
KAppTest	0	0	0	0	0	0	0	0	0	0	0	0	0
KTest1130	0	0	0	0	0	0	0	0	0	0	0	0	0
KiranApp	0	0	0	0	0	0	0	0	0	0	0	0	0
KiranApp0104	0	0	0	0	0	0	0	0	0	0	0	0	0
KiranDemoApp	0	0	0	0	0	0	100	0	0	0	0	0	100
KiranTestApp	0	0	0	0	0	0	0	0	0	0	0	0	0
KiranTestApp1202	0	0	0	0	0	0	0	0	0	0	0	0	0
KiranTestApplication	0	0	0	0	0	0	0	0	0	0	0	0	0
MyNewApp1202	0	0	0	0	0	0	0	0	0	0	0	0	0
MyUnixApp	0	0	0	0	0	0	0	0	0	0	0	0	0
Satya App CUP026	0	0	0	0	0	0	0	276	0	0	0	0	276
Satya CUP027 App	0	0	0	0	0	0	0	10	0	0	0	0	10
Satya RH4 App	0	0	0	0	0	0	0	0	0	23	0	0	23
Satya TTP1	0	0	0	0	0	0	0	0	0	0	0	0	0
Satya TTP2	0	0	0	0	0	0	0	0	0	0	0	0	0
Satya TTP3	0	0	0	0	0	0	0	0	0	0	0	0	0
Satya TTP4	0	0	0	0	0	0	0	0	0	0	0	0	0
Satya TTP5	0	0	0	0	0	0	0	0	0	0	0	0	0

図 10　Application Deployment ROI by Environmentレポート



ENVIRONMENT	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
Development	0	0	0	0	0	0	0	46	0	0	0	0	46
Joe Env	0	0	0	0	0	0	56	0	0	0	0	0	56
John's Biosphere	0	0	0	0	0	0	0	0	0	0	0	0	0
Production	0	0	0	0	0	0	0	126	24	23	0	0	173
QA	0	0	0	0	0	28	448	46	0	0	0	0	522
Satya Env	0	0	0	0	0	0	40	100	0	0	0	0	140
Test Env	0	0	0	0	0	0	0	0	0	0	0	0	0
Wong Env	0	0	0	0	0	0	76	0	0	0	0	0	76
Total	0	0	0	0	0	28	620	318	24	23	0	0	1013

詳細を得るには

- ROI by Applicationレポートのアプリケーション名をクリックすると、当該アプリケーションのApplication Deployment Activityレポートがドリルダウンされます。
- ROI by Applicationレポートの環境名をクリックすると、当該環境のApplication Deployment Activityレポートがドリルダウンされます。

Application Deployment Activity

このレポートでは、指定した時間の範囲内で実行されるすべてのアプリケーションデプロイメント アクションの一覧を、これらのアクションに関する詳細とともに提供します。

パラメーター

[Application Deployment Activity] は、次のいずれかの組み合わせを用いてフィルター処理できます。

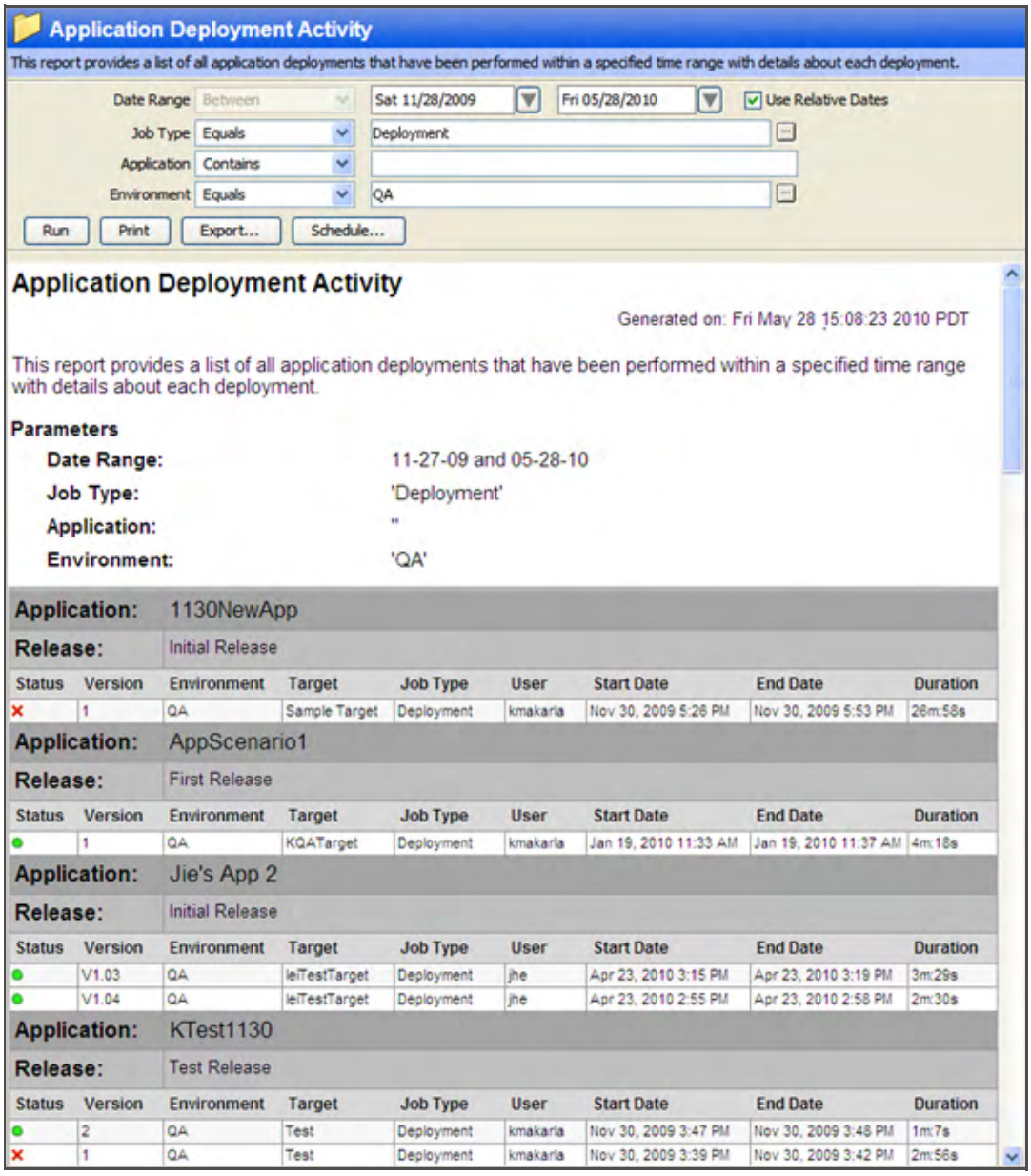
- **Date Range**: アプリケーションデプロイメント アクティビティが実行された日付の範囲。
- **Job Type**: デプロイメント、アンデプロイメント、またはロールバック。
- **Application**: デプロイされる指定アプリケーション。

- **Environment**: QA または本番などのアプリケーションデプロイメント環境。アプリケーションデプロイメント環境は、SAデバイスグループとしてミラーリングされます。

表

- レポートはアプリケーション別にグループ化、またアプリケーションのリリース別にサブグループ化されます。
- レポートの各行は、デプロイメント、アンデプロイメント、ロールバックのいずれかのアクションを表します。
- [Status] 列は、アクションの成功または失敗を示します。
- [Version] 列は、デプロイ、アンデプロイ、またはロールバックされたアプリケーション/リリースのバージョンを示します。
- [Environment] 列は、アプリケーションをデプロイ、アンデプロイ、ロールバックした環境を示します。
- [Target] 列は、アクションのターゲットを示します。アプリケーションのデプロイ、アンデプロイ、ロールバック対象となる1台以上のサーバーからなるグループを、ターゲットとします。
- [Job Type] 列は、デプロイ、アンデプロイ、ロールバックのうち、どのアクションが実行されたかを示します。
- [User] 列は、操作を開始したユーザーのHP SAログインIDを示します。
- [Start Date] および [End Date] 列は、ジョブの開始日時と完了日時を示します。
- [Duration] 列は、ジョブの合計経過時間を表します。

図 11　Application Deployment Activityレポート



詳細を得るには

このレポートでは、詳細のドリルダウンは使用できません。

パッチ

この項では、Windowsパッチポリシーのコンプライアンスに関するレポートについて説明します。

本章の内容

- Time to Patch Policy Compliance (Windows)

ROI by Servers Affected (Windows)

このレポートには、Windowsパッチポリシー更新の影響を受けてポリシーがアタッチされ、修復されたサーバーの数が表示されます。

たとえば、Microsoft Windowsパッチは毎月第2火曜日に入手できます。SAWindowsパッチポリシーは、新しいパッチを自動ダウンロードして、指定のサーバーにインストールするように構成できます。

SAの自動パッチは、新しい更新の影響を受けるすべてのWindowsサーバーを最新かつMicrosoftパッチポリシーに準拠した状態にし、優れた投資効果をもたらします。

このレポートは、負の数の入力をサポートしません。

パラメーター

- **Date Range**: 選択したWindowsパッチポリシーが更新された日付の範囲をフィルターできる。
- **Policy Name**: 指定した日付の範囲に更新により変更されたすべてのポリシー名。
- **Per Server Cost**: サーバーをパッチポリシーに準拠させるためのコストを示すのに用いる値。この単位には、$や時などの希望する任意の値を取ることが可能です(このフィールドは負の数をサポートしません)。
- **Per Patch Cost**: サーバーに1つのパッチをインストールするためのコストを示すのに用いる値。この単位には、$や時などの希望する任意の値を取ることが可能です(このフィールドは負の数をサポートしません)。

[Per Server Cost] と [Per Patch Cost] のパラメーターでは [Contains] 演算子を使用しますが、これらのフィールドの入力値と等しい (「equals」) とみなされます。

表

- 結果はポリシー別にグループ化されます。
- 行にはポリシーの各変更日 (指定した日付の範囲内) が表示されます。
- 各ポリシー変更日に関連するカウントとコスト。ポリシー変更による影響を受けたサーバーと適用されたパッチを反映します。
- サーバー / パッチあたりコストは、ドルや時などユーザー定義による任意の数値を単位にとることが可能です。
- [Affected Servers] の合計値は、サーバーがパッチポリシー更新の影響を受けた回数を表します (固有のサーバーではない)。影響を受けたとマークされるサーバーの合計数が1以上の場合、実際にはパッチポリシーの更新により単一サーバーが2回更新されているケースもあります。たとえば、レポートの [Affected Servers] に次のような値が表示される場合です。

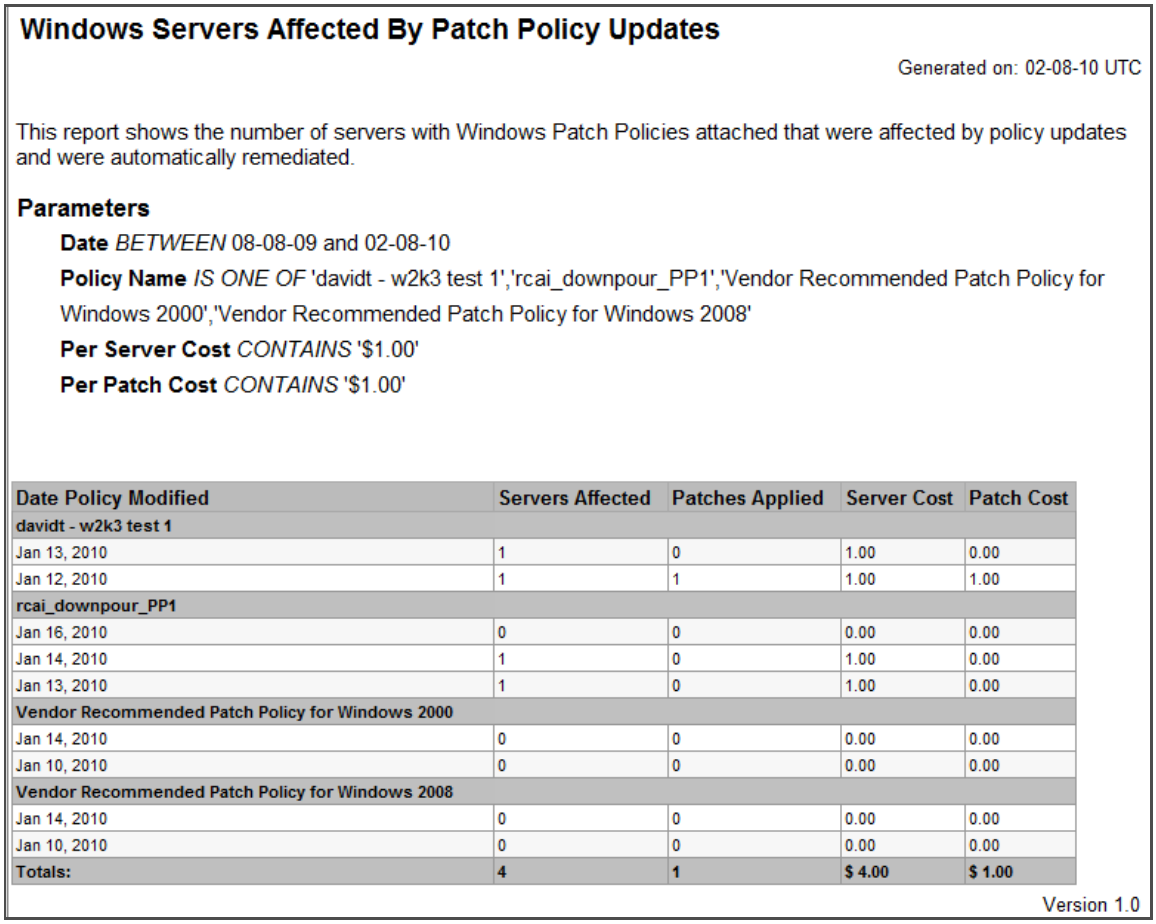
— 3月10日: Affected Servers = 1

— 2月10日: Affected Servers = 1

— 合計: Affected Servers = 2

この場合、3月10日の行項目にある影響を受けたサーバーは、2月10日の行項目でカウントしているサーバーと同じ可能性があります。合計数 (1＋1＝2) が示す2台のサーバーは、実際には2回カウントされた同一サーバーです。同一サーバーが3月10日と2月10日に影響を受けた理由は、このサーバーに適用可能なパッチが2月10日にポリシーへ追加された後、別の適用可能なパッチが3月10日に追加されたためです。ROI の観点ではこのサーバーは2回影響を受けたことになるため、合計数として表示されています。

図 12　Windows Servers Affected by Patch Policy Updates



Windows Servers Affected By Patch Policy Updates

Generated on: 02-08-10 UTC

This report shows the number of servers with Windows Patch Policies attached that were affected by policy updates and were automatically remediated.

Parameters

Date *BETWEEN* 08-08-09 and 02-08-10

Policy Name *IS ONE OF* 'davidt - w2k3 test 1','rcai_downpour_PP1','Vendor Recommended Patch Policy for Windows 2000','Vendor Recommended Patch Policy for Windows 2008'

Per Server Cost *CONTAINS* '$1.00'

Per Patch Cost *CONTAINS* '$1.00'

Date Policy Modified	Servers Affected	Patches Applied	Server Cost	Patch Cost
davidt - w2k3 test 1				
Jan 13, 2010	1	0	1.00	0.00
Jan 12, 2010	1	1	1.00	1.00
rcai_downpour_PP1				
Jan 16, 2010	0	0	0.00	0.00
Jan 14, 2010	1	0	1.00	0.00
Jan 13, 2010	1	0	1.00	0.00
Vendor Recommended Patch Policy for Windows 2000				
Jan 14, 2010	0	0	0.00	0.00
Jan 10, 2010	0	0	0.00	0.00
Vendor Recommended Patch Policy for Windows 2008				
Jan 14, 2010	0	0	0.00	0.00
Jan 10, 2010	0	0	0.00	0.00
Totals:	**4**	**1**	**$ 4.00**	**$ 1.00**

Version 1.0

Time to Patch Policy Compliance (Windows)

このレポートには、ご使用の Windows サーバーが Windows パッチポリシーの変更から準拠までに要した平均日数が表示されます。

Windows パッチポリシーが (パッチの追加などで) 変更されると、ポリシーのアタッチ対象となるサーバーは、パッチポリシーの定義に一致するよう修復されるまで非コンプライアンスとみなされます。

このレポートで [日付の範囲] パラメーターを使用して、時刻の範囲を指定できます。これにより、Windows パッチポリシーの変更から任意の指定時間のあいだで、Windows サーバーがポリシー準拠に要した時間を確認できます。

サーバー数には、[scan needed] または [scan failed] 状態のサーバーは含まれません。

パラメーター

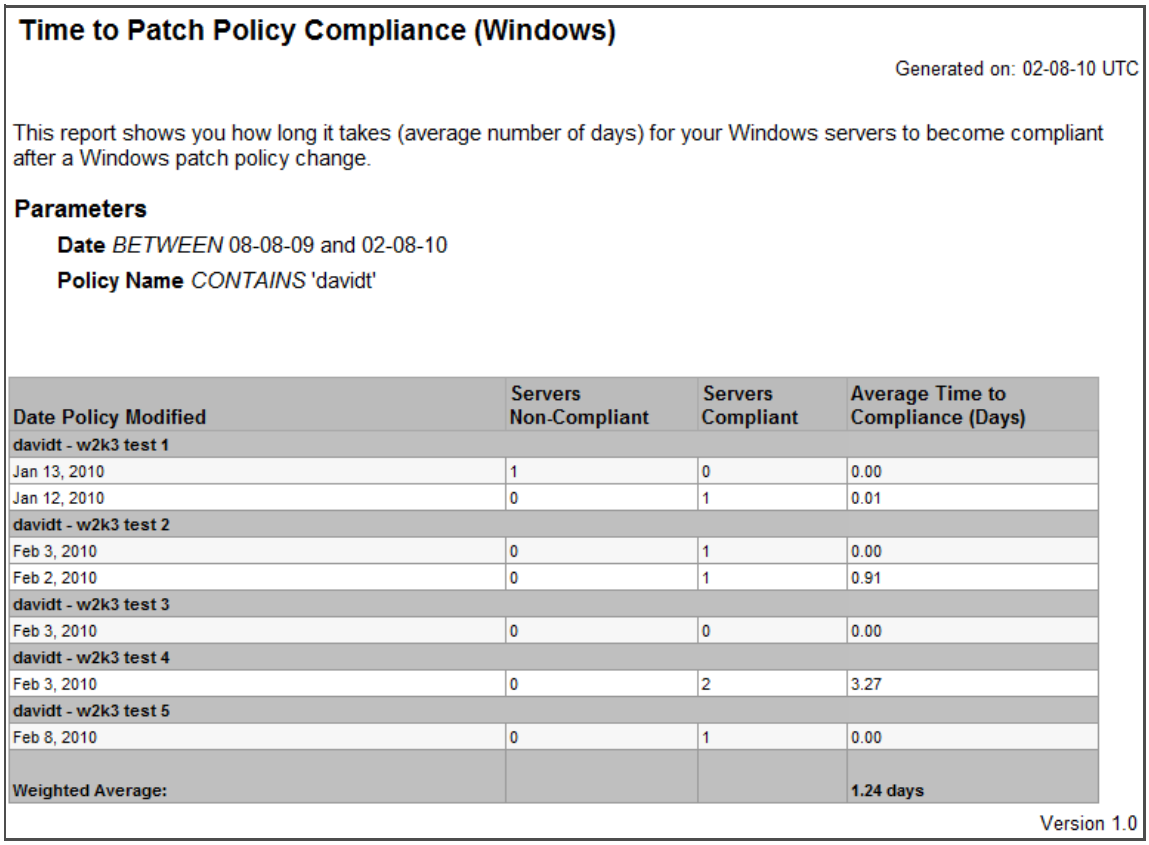
- **Date Range**: 開始日と終了日の条件を指定。このフィルターには開始日と終了日が両方含まれ、結果に表示するポリシー変更の範囲を決定します。
- **Patch Policy**: レポート結果に返したいWindowsパッチポリシーを指定。選択条件は、[Equals]、[Contains]、[Begins With]、[Ends With] です。[Equals]、[Any Value] を選択すると、すべてのWindowsパッチポリシーが選択されます。

すべての検索には指定された値を使用し、大文字と小文字を区別しません。

表

- **Date Policy Modified**: レポートパラメーターで選択した各パッチポリシーと、指定ポリシーが指定した日付の範囲内で変更された各回の情報がリスト表示されます。
- **Servers Non-Compliant**: パッチポリシー変更の影響を受けたが非コンプライアンス状態のサーバー数を示します。
- **Servers Compliant**: パッチポリシー変更の影響を受けコンプライアンス状態のサーバー数を示します。
- **Average Time to Compliance**: ポリシーが変更されてからサーバーが最初に準拠するまでの平均日数 (小数第2位まで)。
- **Weighted Average**: パッチポリシー変更の影響を受けたすべてのサーバーが、レポートで選択したすべてのポリシーに準拠するまでの平均日数。

図 13　Time To Patch Policy Compliance (Windows)



Time to Patch Policy Compliance (Windows)

Generated on: 02-08-10 UTC

This report shows you how long it takes (average number of days) for your Windows servers to become compliant after a Windows patch policy change.

Parameters

Date *BETWEEN* 08-08-09 and 02-08-10

Policy Name *CONTAINS* 'davidt'

Date Policy Modified	Servers Non-Compliant	Servers Compliant	Average Time to Compliance (Days)
davidt - w2k3 test 1			
Jan 13, 2010	1	0	0.00
Jan 12, 2010	0	1	0.01
davidt - w2k3 test 2			
Feb 3, 2010	0	1	0.00
Feb 2, 2010	0	1	0.91
davidt - w2k3 test 3			
Feb 3, 2010	0	0	0.00
davidt - w2k3 test 4			
Feb 3, 2010	0	2	3.27
davidt - w2k3 test 5			
Feb 8, 2010	0	1	0.00
Weighted Average:			**1.24 days**

Version 1.0

第 3 章　BSAE Javaクライアント経由のSAコンプライアンスレポート

ここでは、BSAE Javaクライアント経由で入手可能な最新のServer Automation (SA) コンプライアンスレポートについて説明します。HP Live Networkから**sar78_reports**ストリームでダウンロードできます。

この項では、次の事項を説明します。

BSAE Javaクライアントは、SAクライアントに付属しています。BSAE JavaクライアントでSAレポートを実行する設定を行う方法については、BSA EssentialsのSAレポート (7ページ)を参照してください。レポートへのアクセスと実行に関する追加情報については、BSAE Javaクライアントのオンラインヘルプを参照してください。

コンプライアンスレポートの用語

用語	説明
Generated On	レポートの作成日。SAS Webクライアントの SAユーザープロファイルで指定した日付-時刻形式で表示されます。
Status	• Compliance Status of Server /Item: ステータスのロールアップは、累積ステータスとして最低値を算出します。ステータスは最高から最低へと、[コンプライアンス] > [部分コンプライアンス (パッチのみ)] > [非コンプライアンス] > [スキャンが必要] > [スキャン失敗] のように、バブルアップまたはロールアップします。 • Compliance Status of Policy: ステータスのロールアップは、スキャン失敗の最低値を算出します。最高から最低までステータスの優先順位は、[コンプライアンス] > [非コンプライアンス] > [スキャンが必要] > [スキャン失敗] となります。
Last Scan	コンプライアンスステータスが計算された前回のスキャン日。日付形式はSAユーザープロファイルで指定したユーザーのものと同じです。
Compliant Rules/Items/Files	分子には、指定ポリシー内のコンプライアンスルール/アイテム/ファイルの数を指定します。一方、分母には、ポリシー内のルール/アイテム/ファイルの合計数を指定します。
Compliant Servers	分子には、指定ポリシーに対するコンプライアンスサーバーの数を指定します。一方、分母には、ポリシーにアタッチされるサーバーの合計数を指定します。
On Server	特定バージョンのパッチアイテム、ソフトウェアユニット、アプリケーション構成ファイルがサーバー上に存在するかどうかを決定します。
Exceptions	例外はポリシー内で作成され、例外の内容や有効期限などの詳細を保持できます。

コンプライアンス

ここでは、BSA Essentials Javaクライアントで提供されるSAコンプライアンスレポートについて説明します。

Summary of Compliance by Server

グラフ

- y軸の単位は、指定ポリシーがアタッチされるサーバーの数を示します。カウントは、ポリシータイプ別にサーバーにアタッチされる各ポリシーに対するポリシーコンプライアンスステータスの合計を示します。
- カウントは、サーバーにアタッチされる一意のポリシーインスタンス数を示すものではありません。たとえば、1つのポリシーを1台以上のサーバーにアタッチする場合、そのポリシーはそのサーバー以外に対して非コンプライアンスの可能性があり、複数回カウントされることになります。

- x軸は、ポリシータイプ別にカテゴリ化されます。

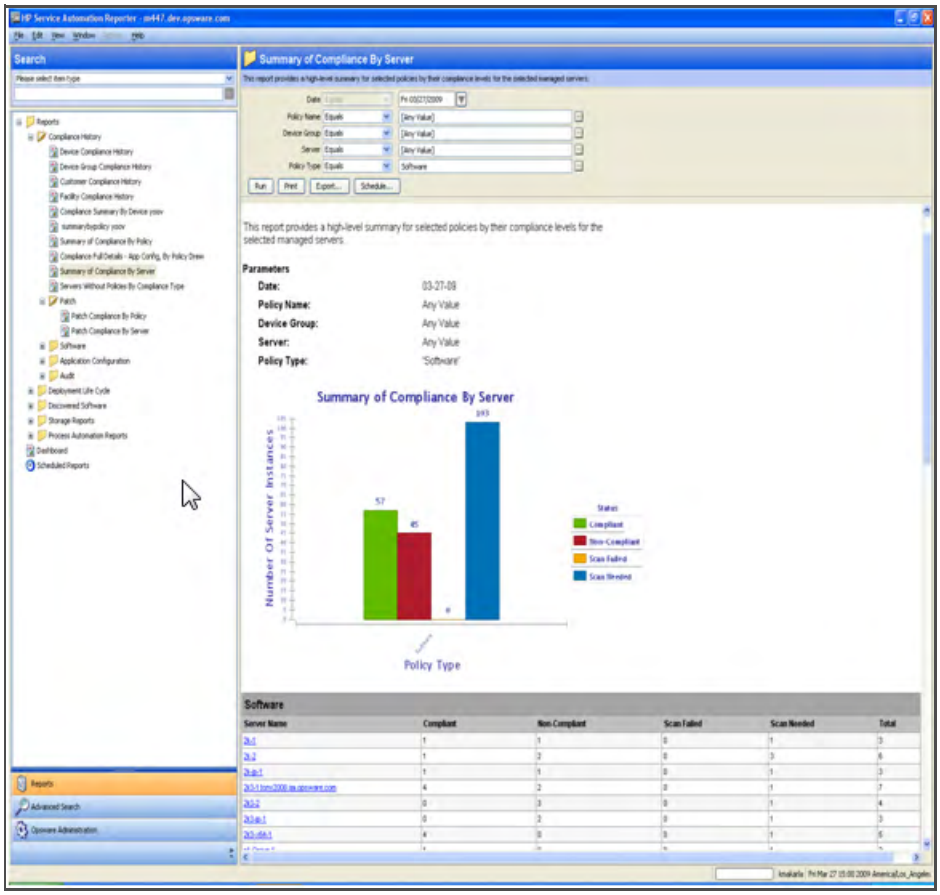
表

- [Total] 列の値は、指定サーバーにアタッチされる一意のポリシーインスタンスの合計数を表します。
- サーバーは、アタッチされるポリシーのタイプ、つまりポリシータイプ別に、一覧の各サーバー名とともにグループ化されます。
- ポリシータイプ内で重複したサーバー名をもつことはできません。
- サーバー名は、ポリシータイプ全体では繰り返しが可能です。たとえば、サーバー S1 が監査ポリシー「A1」とソフトウェアポリシー「SP1」にアタッチされる場合、S1は監査ポリシータイプとソフトウェアポリシータイプの両方にリスト表示されます。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

詳細を得るには

- レポートのサーバー名をクリックすると、レポートの全詳細がドリルダウンされます。これにより、アタッチされるポリシー内の各ポリシーとアイテムに対するコンプライアンスステータス別に、選択したサーバーのブレークダウンを確認できます。
- レポートパラメーターの選択条件は保持され、選択したサーバー名のドリルダウンレポートに反映、適用されます。
- ドリルダウンレポートはサマリーレポートとの関連および枠組みで表示されるため、ユーザーはサマリーレポートに戻って確認できます。

図 14　Summary of Compliance By Server



Summary of Compliance by Policy

グラフ

- y 軸の単位は、各ポリシータイプについて、アタッチされるポリシー / ポリシーインスタンスに対するサーバーのコンプライアンスステータスの合計数を示します。
- カウントは、すべてのポリシーがアタッチされた一意のサーバー数を示すものではありません。たとえば、1台のサーバーが1つ以上のポリシーにアタッチされる場合、そのサーバーは各ポリシーに対して非コンプライアンスの可能性があり、複数回カウントされることになります。
- x軸は、ポリシータイプ別にカテゴリ化されます。

表

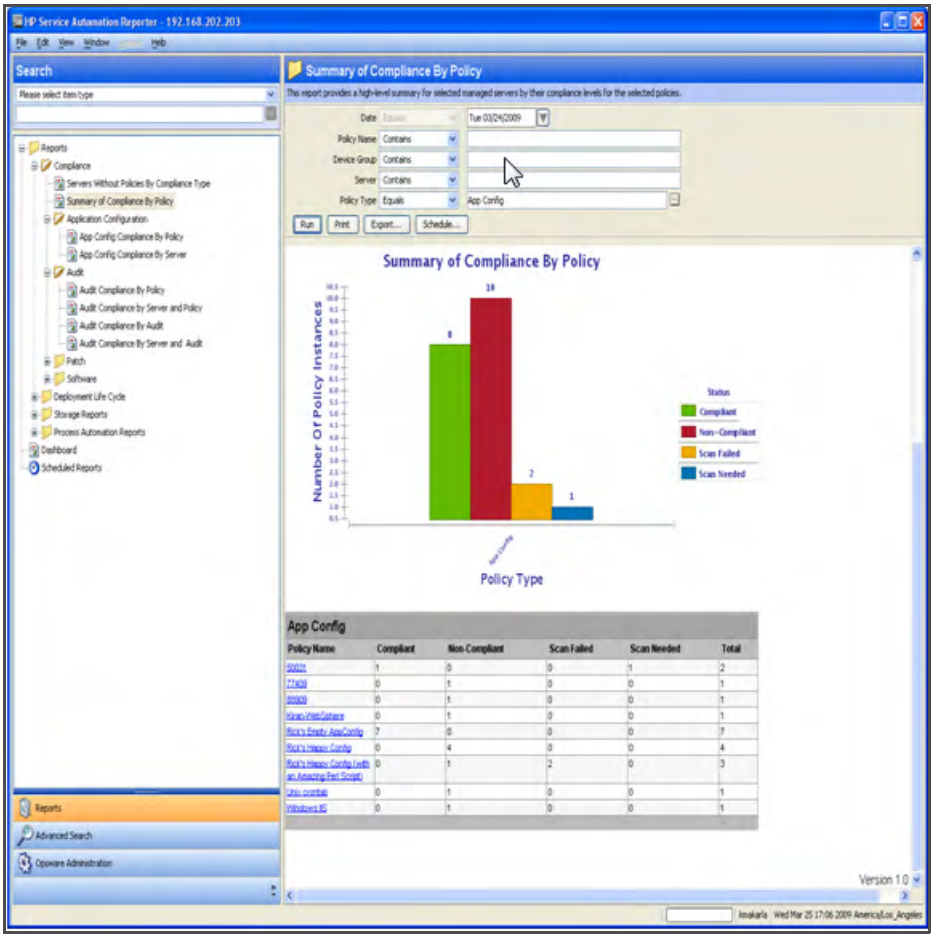
- ポリシーはポリシータイプ別に、一覧の各ポリシー名とともにグループ化されます。
- ポリシー名はポリシータイプ全体で重複しても構いません。たとえば、監査ポリシーを「P1」と名付け、同様にソフトウェアポリシーを「P1」と名付けることができます。
- ポリシータイプ内で重複した名前のポリシーをもつことはできません。
- [Total] 列の値は、個別のポリシーにアタッチされる一意のサーバーの合計数を表します。ただし、単一サーバーに同じ「アプリケーション構成」のインスタンスを複数保持できる「アプリケーション構成」インスタンスは除きます。

- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

詳細を得るには

- レポートのポリシー名をクリックすると、レポートの全詳細がドリルダウンされます。これにより、ポリシーがアタッチされる各サーバーについて、コンプライアンスステータス別に、選択したポリシーとアイテムのブレークダウンを確認できます。
- レポートパラメーターの選択条件は保持され、選択したポリシー名のドリルダウンレポートに反映、適用されます。
- ドリルダウンレポートはサマリーレポートとの関連および枠組みで表示されるため、ユーザーはサマリーレポートに戻って確認できます。

図 15　Summary of Compliance By Policy



Servers Without Policies by Compliance Type

表

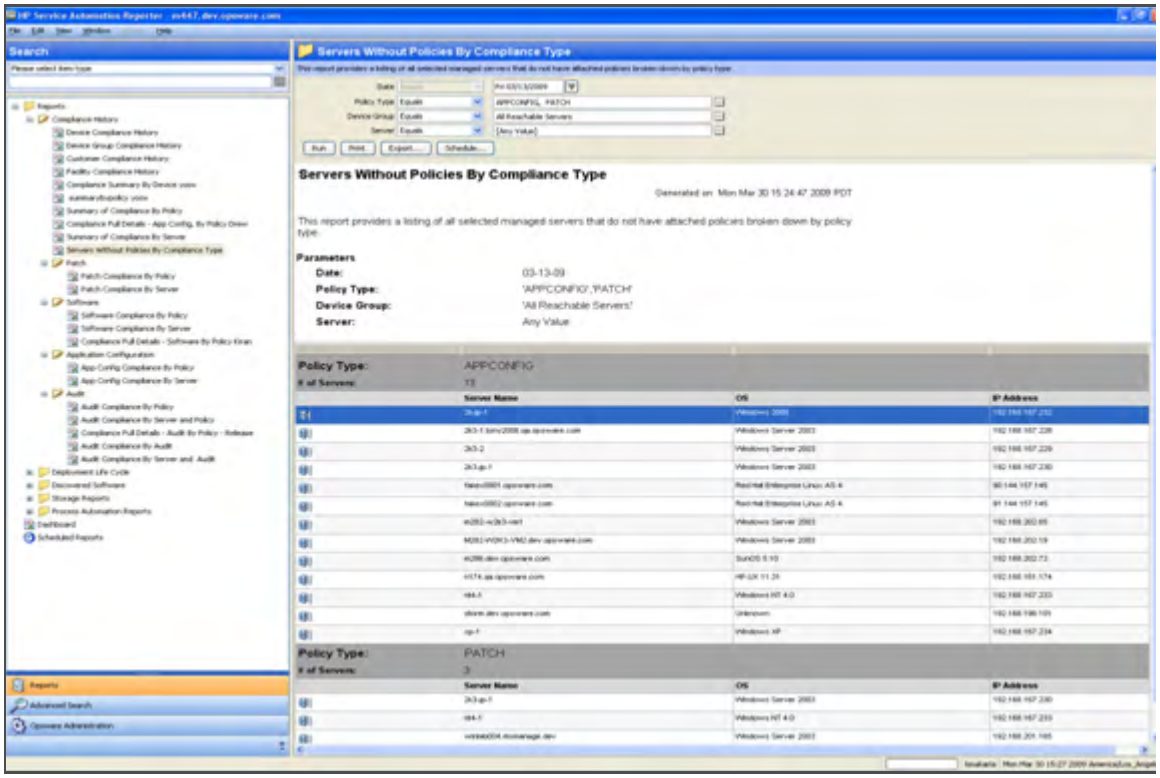
- レポートには、アタッチされるポリシーを1つももたないサーバーが表示されます。
- サーバーはコンプライアンスタイプ別に、一覧の各サーバー名とともにグループ化されます。
- 1つのサーバーを複数のコンプライアンスタイプのセクションに表示可能です。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

アタッチ済みだがプッシュされていないアプリケーション構成ポリシーをもつサーバーは、このレポートに表示されません。

詳細の実行

サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 16　Servers Without Policies by Compliance Type



アプリケーション構成

App Config Compliance by Server

サーバーサマリー

- Compliant: コンプライアンスサーバーの合計数
- Non-Compliant: 非コンプライアンスサーバーの合計数。アタッチされるポリシー内のポリシーまたはアイテムが1つ以上、非コンプライアンスの場合、サーバーは非コンプライアンスとみなされます。
- Scan Needed: スキャンを必要とするサーバーの合計数。アタッチされるポリシーが1つ以上、変更されると、サーバーはスキャンが必要な状態になります。サーバーコンプライアンスを決定するには、サーバーのスキャンが必要です。

- Scan Failed: Partially Complaintコンプライアンスのためのサーバースキャンのジョブ完了に失敗したサーバーの合計数。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

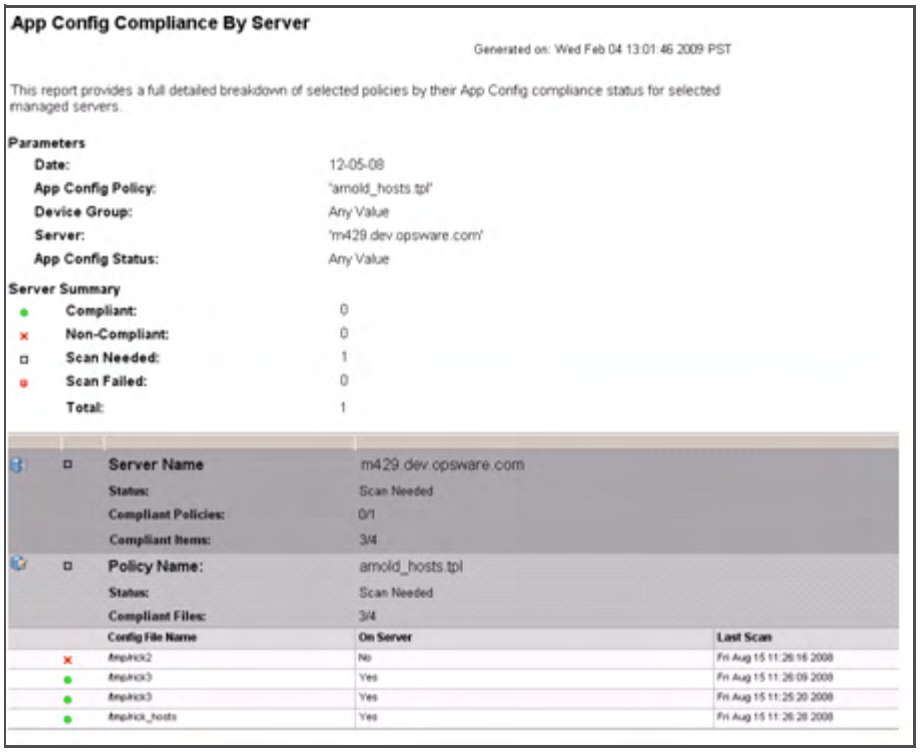
表

- アプリケーション構成ポリシーは、デバイスグループまたはサーバーに直接アタッチできます。ポリシーがデバイスグループにアタッチされる場合、サーバー / ポリシーのアタッチをシステムが認識するにはスキャンが必要となります。また、一致するプラットフォーム上のサーバーのみレポートされます。
- 表は、最初にサーバー別にグループ化されます。各サーバーは、インストールされるアプリケーション構成の各インスタンスに対するコンプライアンス数を有します。
- 各構成ファイルはインスタンス内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、アプリケーション構成P1、アプリケーション構成P2は、サーバー S1とサーバー S2にアタッチされます。P1は構成ファイルF1、構成ファイルF2を保持し、S1に対してコンプライアンス、S2に対して非コンプライアンスとします。P2は、S1に対して非コンプライアンス、S2に対して非コンプライアンスとします。この場合、S1とS2に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。
- アプリケーション構成内の構成ファイルは、インストール先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- アプリケーション構成はサーバー上に複数のインスタンスを保持できます。つまり、たとえばWebSphere 4.0の構成ファイルは、サーバーの/optおよび/homeディレクトリにインストールできます。この場合、正味のサーバーコンプライアンスは、各アプリケーションインスタンスのコンプライアンスステータスの組み合わせにより決定されます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 17　AppConfig Compliance By Server



App Config Compliance by Policy

サマリー

- Compliant Policies: サーバーにアタッチされる選択したポリシーの合計数に対する、選択したコンプライアンスポリシーの数。
- Compliant Config Items: サーバーにアタッチされる選択した全ポリシー内の一意の構成アイテムの合計数に対する、選択した全ポリシー内の一意のコンプライアンス構成アイテムの数。
- Compliant Severs: 一意のサーバーの合計数に対する、一意のコンプライアンスサーバーの数。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

表

- アプリケーション構成ポリシーは、デバイスグループまたはサーバーに直接アタッチできます。ポリシーがデバイスグループにアタッチされる場合、サーバー / ポリシーのアタッチをシステムが認識するにはスキャンが必要となります。また、一致するプラットフォーム上のサーバーのみレポートされます。
- 表は、最初にポリシー別にグループ化されます。各ポリシーは、ポリシーをアタッチする各アイテムやサーバーに対するコンプライアンス数を有します。
- 各アイテムはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、アプリケーション構成ポリシー P1が、サーバー S1とサーバー S2にアタッチされます。ポリシー P1は Item1というアイテムを保持し、サーバー S1に対してコンプライアンス、サーバー S2に対して非コンプ

ライアンスとなります。この場合、Item1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Item1はポリシー P1の一部のため、P1はサーバー S1とサーバー S2に対しても非コンプライアンスとなります。

- サーバーに対するポリシーコンプライアンス詳細内のポリシーとアイテムは、サーバーがスキャンされたときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- アプリケーション構成はサーバー上に複数のインスタンスを保持できます。つまり、たとえばWebSphere 4.0の構成ファイルは、サーバーの/optおよび/homeディレクトリにインストールできます。この場合、正味のサーバーコンプライアンスは、各アプリケーションインスタンスのアグリゲート コンプライアンスステータスにより決定されます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 18　AppConfig Compliance By Policy

監査

Audit Compliance by Policy

サマリー

- Compliant Policies: サーバーにアタッチされる選択したポリシーの合計数に対する、選択したコンプライアンスポリシーの数。
- Compliant Rules: サーバーにアタッチされる選択した全ポリシー内の一意のルールの合計数に対する、選択した全ポリシー内の一意のコンプライアンスルールの数。
- Compliant Severs: 一意のサーバーの合計数に対する、一意のコンプライアンスサーバーの数。
- カウントには、定期監査に対する最新の管理対象/アクティブサーバーのみ反映されます。

表

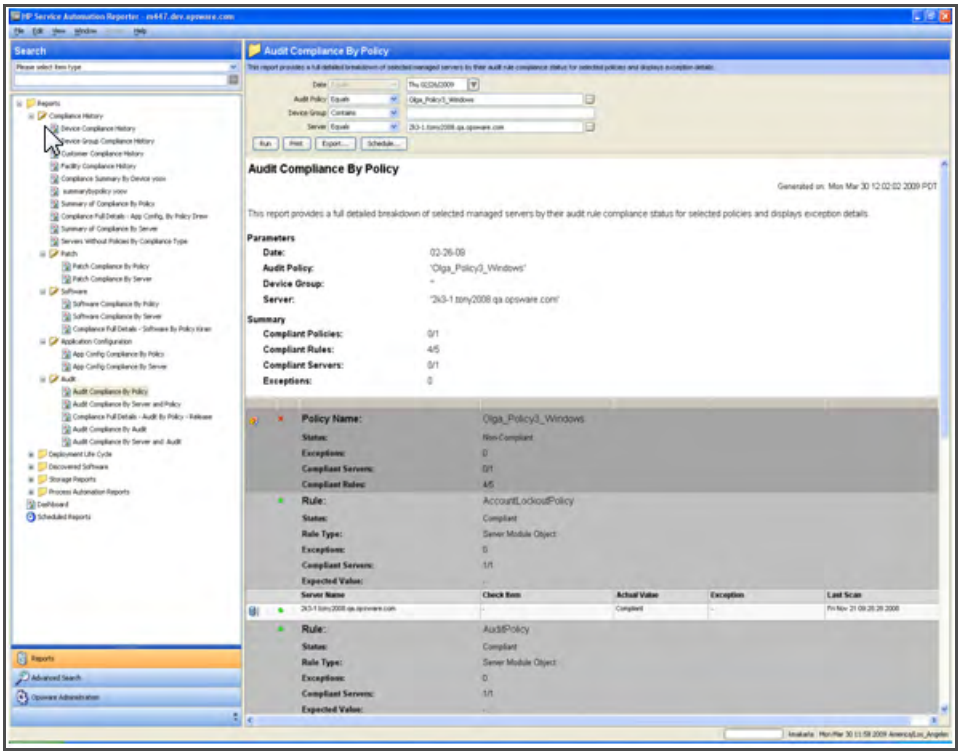
- 監査ポリシーには、別のポリシー内で定義されるルール、または別のポリシーから拡張されるルールが含まれます。複数レベルのポリシー階層をサポートし、合成ポリシーを作成できます。
- 表は、最初にポリシー別にグループ化されます。各ポリシーは、監査チェック済みの各ルールやサーバーに対するコンプライアンス数を有します。
- 各ルールはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、監査ポリシー P1 は Rule1 というルールを保持し、サーバー S1 とサーバー S2 で監査チェック済みです。Rule1は、S1に対してコンプライアンス、S2に対して非コンプライアンスとします。この場合、Rule1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Rule1 はポリシー P1 の一部のため、P1はS1とS2に対しても非コンプライアンスとなります。
- ポリシー内のルールは、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- 各ターゲットサーバーについて取得される監査の詳細は、個別のルールタイプやチェックのタイプによって異なります。「値ベース」、「比較ベース」などのタイプで実行できます。
- 「値ベース」のチェックでは、ターゲットサーバーの特定の値 (例: パスワードの最小文字数＝8) について検証します。監査ではユーザーが指定した「予期される値」とともに、「実際の値」がレポートされます。
- 「比較ベース」のチェックでは、ソースサーバーとターゲットサーバー上のオブジェクト、ファイル、ディレクトリを比較します。監査結果は、これらのオブジェクトがソースとターゲットの両方に存在するか、また存在する場合はその差異によって異なります。
- 「比較ベース」のチェックの監査レポートでは、ソースサーバーとターゲットサーバーの差異のみ表示されます。
- 監査レポートは、次の列で構成されます。
  - Server Name
  - Check Item (ルールタイプによる)
  - Actual Value or Differences (ルールタイプによる)
  - Exception Details
  - Last Scan

値ベースのチェック

次に挙げるのは、「値ベース」のチェックを実行できるルールタイプの一覧です。

- チェックポリシー /プラグ可能チェック
- アプリケーション構成ポリシー
- カスタムスクリプト
- ネットワークデュプレックス
- サーバーモジュールオブジェクト
- ストレージイニシエーター

図 19　Audit Compliance By Policy - Value-Based Checks



比較ベースのチェック

次に挙げるのは、「比較ベース」のチェックを実行できるルールタイプの一覧です。

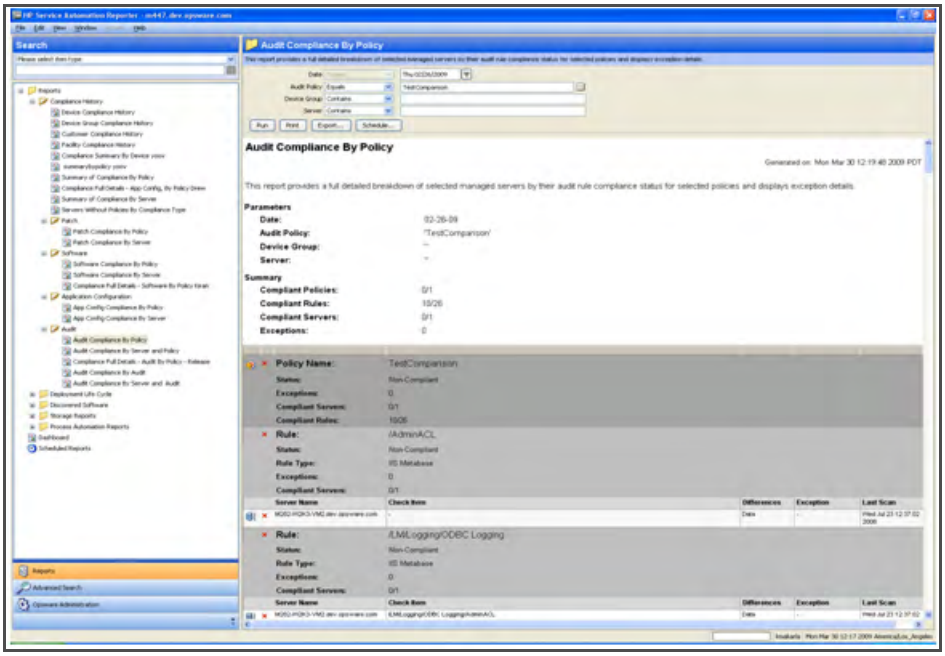
- ストレージイニシエーター
- チェックポリシー /プラグ可能チェック
- Windowsサービス
- レジストリ
- COM+
- カスタムスクリプト
- ストレージ
- ファイルシステム

- IISメタベース
- サーバーモジュールオブジェクト
- ハードウェア
- 監査の例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。特定のターゲットサーバーが例外条件を満たす場合、そのサーバーは「コンプライアンス」とみなされます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 20　Audit Compliance By Policy - Comparison-Based Checks



Audit Compliance by Audit

サマリー

- Compliant Audits: サーバー上で実行される選択した監査の合計数に対する、選択したコンプライアンス監査の数。
- Compliant Rules: サーバー上で実行される選択した全監査内の一意のルールの合計数に対する、選択した全監査内の一意のコンプライアンスルールの数。
- Compliant Severs: 一意のサーバーの合計数に対する、一意のコンプライアンスサーバーの数。
- カウントには、選択条件により、定期監査、定期および非定期監査に対する最新の管理対象/アクティブサーバーが反映されます。

表

- 監査は、単一または複数の監査ポリシーに基づく一連のルールで構成されます。また、包括的な監査作成のため、内部で定義される暗黙のルールを監査に適用することもできます。
- ルールで構成済みのポリシーを使用する一連のサーバーに対する監査のスナップショット仕様を作成できます。仕様の結果は、将来の監査のベースラインとして使用できます。
- 監査は、以前に取得した監査のスナップショット仕様の結果を使用する一連のターゲットサーバー、最新のスナップショット仕様の結果、またはソースとなる普通の単一ルサーバーに対して作成できます。
- 表は、最初に監査別にグループ化されます。各監査は、監査チェック済みの各ルールやサーバーに対するコンプライアンス数を有します。
- 各ルールは監査内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、監査A1は、サーバー S1とサーバー S2で監査チェック済みです。監査A1はRule1というルールを保持し、サーバー S1に対してコンプライアンス、サーバー S2に対して非コンプライアンスとします。この場合、Rule1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Rule1は監査A1の一部のため、A1も非コンプライアンスとなります。
- 監査内のルールは、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、監査とサーバーのアタッチ詳細のみレポートされます。
- 各ターゲットサーバーについて取得される監査の詳細は、個別のルールタイプやチェックのタイプによって異なります。「値ベース」、「比較ベース」などのタイプで実行されます。
- 「値ベース」のチェックは、ターゲットサーバーの特定の値 (例: パスワードの最小文字数＝8) を検証するために実行されます。監査ではユーザーが指定した「予期される値」とともに、「実際の値」がレポートされます。
- 「比較ベース」のチェックは、ソースサーバーとターゲットサーバー上のオブジェクト、ファイル、ディレクトリを比較するために実行します。監査結果は、これらのオブジェクトがソースとターゲットの両方に存在するか、また存在する場合はその差異によって異なります。
- 「比較ベース」のチェックの監査レポートでは、ソースサーバーとターゲットサーバーの差異のみ表示されます。
- 監査レポートは、次の列で構成されます。
  - Server Name
  - Check Item (ルールタイプによる)
  - Actual Value or Differences (ルールタイプによる)
  - Exception Details
  - Last Scan

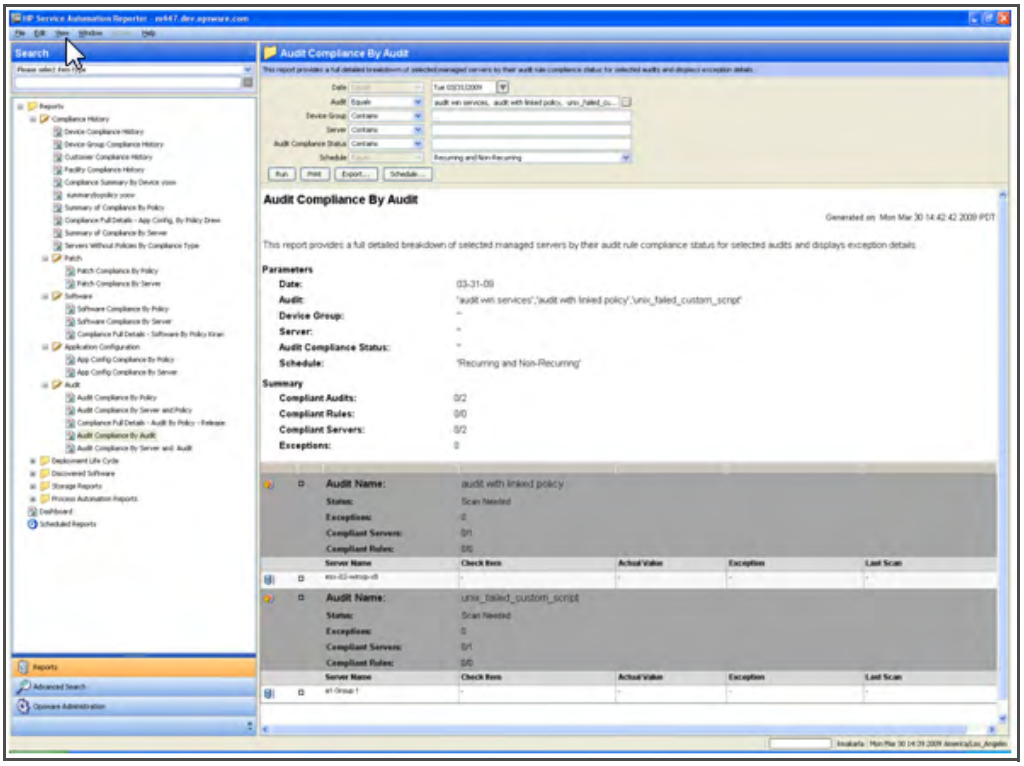
値ベースのチェック

次に挙げるのは、「値ベース」のチェックを実行できるルールタイプの一覧です。

- チェックポリシー /プラグ可能チェック
- アプリケーション構成ポリシー
- カスタムスクリプト
- ネットワークデュプレックス

- サーバーモジュールオブジェクト
- ストレージイニシエーター

図 21　Audit Compliance By Audit - Value-Based Checks



比較ベースのチェック

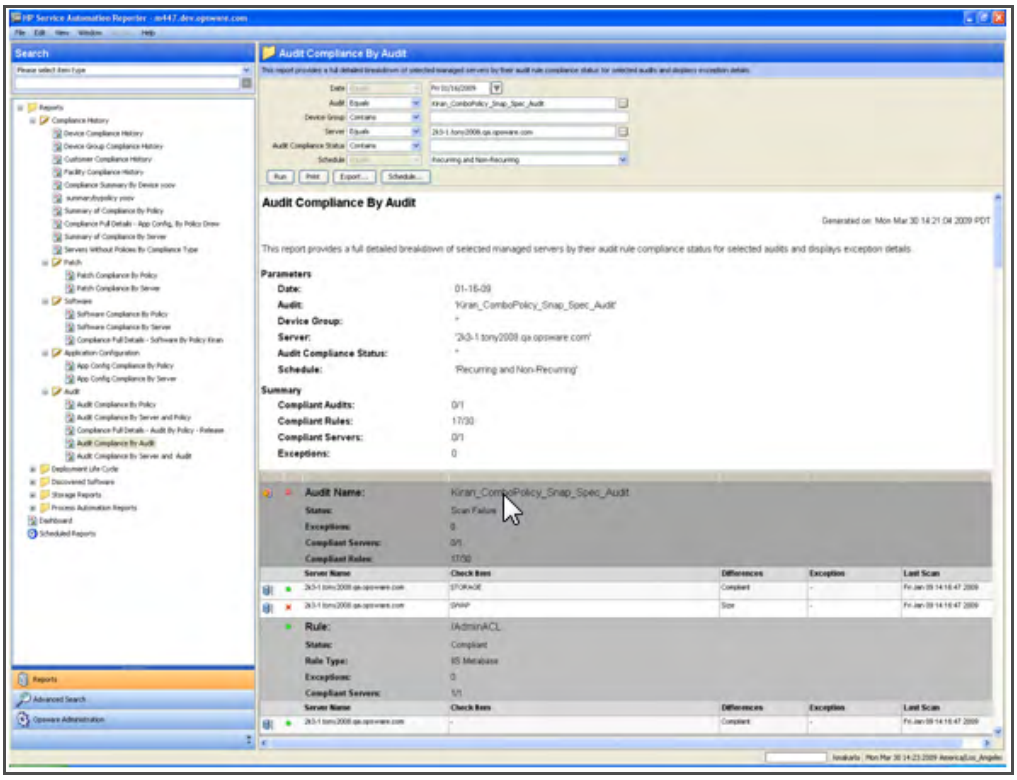
次に挙げるのは、「比較ベース」のチェックを実行できるルールタイプの一覧です。

- ストレージイニシエーター
- チェックポリシー /プラグ可能チェック
- Windowsサービス
- レジストリ
- COM+
- カスタムスクリプト
- ストレージ
- ファイルシステム
- IISメタベース
- サーバーモジュールオブジェクト
- ハードウェア
- 監査の例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。特定のターゲットサーバーが例外条件を満たす場合、そのサーバーは「コンプライアンス」とみなされます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 22　Audit Compliance By Audit - Comparison-Based Checks



Audit Compliance by Server and Policy

サーバーサマリー

- Compliant: コンプライアンスサーバーの合計数。
- Non-Compliant: 非コンプライアンスサーバーの合計数。アタッチされるポリシー内のポリシーまたはルールが1つ以上、非コンプライアンスの場合、サーバーは非コンプライアンスとみなされます。
- Scan Needed: スキャンを必要とするサーバーの合計数。アタッチされるポリシーが1つ以上、変更されると、サーバーはスキャンが必要な状態になります。サーバーコンプライアンスを決定するには、サーバーのスキャンが必要です。
- Scan Failed: コンプライアンスのためのサーバースキャンのジョブ完了に失敗したサーバーの合計数。
- カウントには、定期監査に対する最新の管理対象/アクティブサーバーのみ反映されます。

表

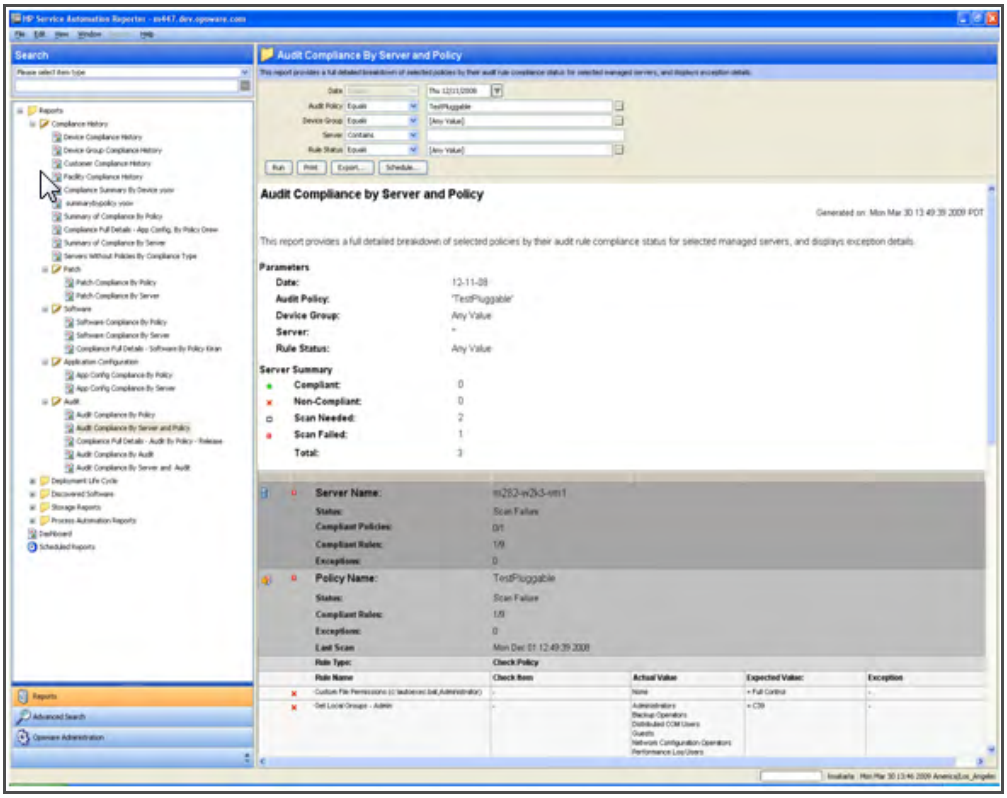
- 監査ポリシーには、別のポリシー内で定義されるルール、または別のポリシーから拡張される一連のルールが含まれます。複数レベルのポリシー階層をサポートし、合成ポリシーを作成できます。
- 表は、最初にサーバー別にグループ化されます。各サーバーは、監査チェック済みポリシー内の各ポリシーやルールに対するコンプライアンス数を有します。
- 各ルールはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、監査ポリシー P1は、サーバー S1とサーバー S2で監査チェック済みです。ポリシー P1はRule1というルールを保持し、サーバー S1 に対してコンプライアンス、サーバー S2 に対して非コンプライアンスとします。この場合、Rule1 に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Rule1はポリシー P1の一部のため、P1も非コンプライアンスとなります。P1はサーバー S1にアタッチされるため、S1は非コンプライアンスとなります。
- ポリシー内のルールは、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- 各ターゲットサーバーについて取得される監査の詳細は、個別のルールタイプやチェックのタイプによって異なります。「値ベース」、「比較ベース」などのタイプで実行されます。
- 「値ベース」のチェックは、ターゲットサーバーの特定の値 (例: パスワードの最小文字数＝8) を検証するために実行されます。監査ではユーザーが指定した「予期される値」とともに、「実際の値」がレポートされます。
- 「比較ベース」のチェックは、ソースサーバーとターゲットサーバー上のオブジェクト、ファイル、ディレクトリを比較するために実行します。監査結果は、これらのオブジェクトがソースとターゲットの両方に存在するか、また存在する場合はその差異によって異なります。
- 「比較ベース」のチェックの監査レポートでは、ソースサーバーとターゲットサーバーの差異のみ表示されます。
- 監査レポートは、次の列で構成されます。
  - Server Name
  - Check Item (ルールタイプによる)
  - Actual Value or Differences (ルールタイプによる)
  - Exception Details
  - Last Scan

値ベースのチェック

次に挙げるのは、「値ベース」のチェックを実行できるルールタイプの一覧です。

- チェックポリシー /プラグ可能チェック
- アプリケーション構成ポリシー
- カスタムスクリプト
- ネットワークデュプレックス
- サーバーモジュールオブジェクト
- ストレージイニシエーター

図 23　Audit Compliance By Server and Policy - Value-Based Checks



比較ベースのチェック

次に挙げるのは、「比較ベース」のチェックを実行できるルールタイプの一覧です。

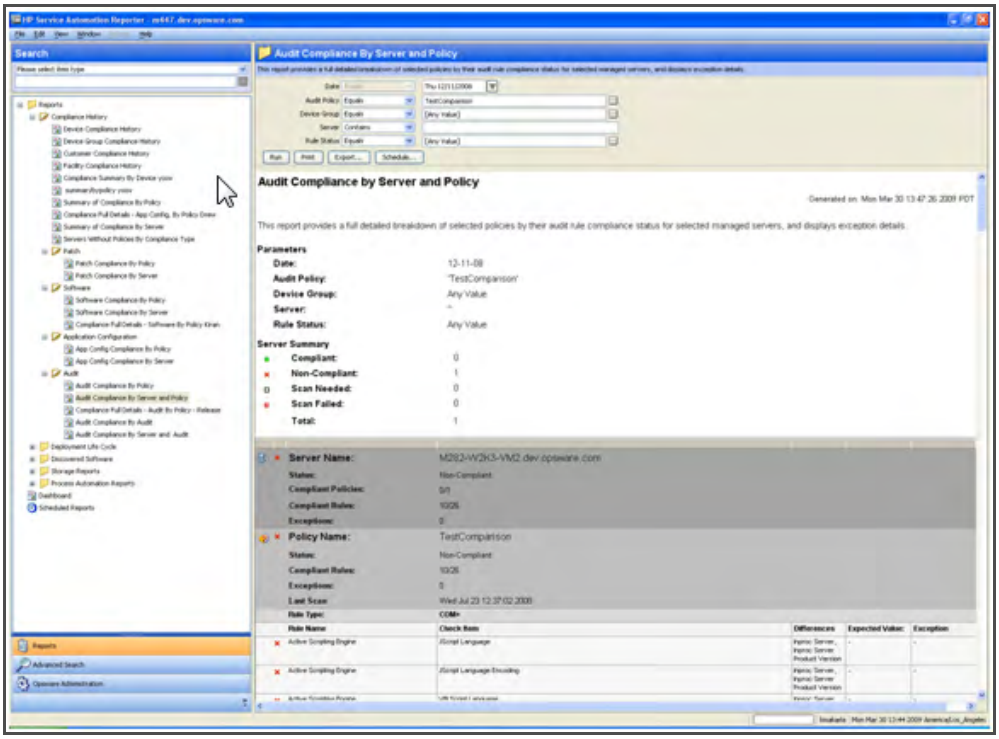
- ストレージイニシエーター
- チェックポリシー /プラグ可能チェック
- Windowsサービス
- レジストリ
- COM+
- カスタムスクリプト
- ストレージ
- ファイルシステム
- IISメタベース
- サーバーモジュールオブジェクト
- ハードウェア

監査の例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。特定のターゲットサーバーが例外条件を満たす場合、そのサーバーは「コンプライアンス」とみなされます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 24　Audit Compliance By Server and Policy - Comparison-Based Checks



Audit Compliance by Server and Audit

サーバーサマリー

- Compliant: コンプライアンスサーバーの合計数。
- Non-Compliant: 非コンプライアンスサーバーの合計数。アタッチされるポリシー内のポリシーまたはルールが1つ以上、非コンプライアンスの場合、サーバーは非コンプライアンスとみなされます。
- Scan Needed: スキャンが必要なサーバーの合計数。アタッチされているポリシーが1つ以上、変更された場合、サーバーは [Scan Needed] 状態になります。サーバーコンプライアンスを決定するには、サーバーのスキャンが必要となります。
- Scan Failed: コンプライアンスのためのサーバースキャンのジョブ完了に失敗したサーバーの合計数。
- カウントには、定期監査に対する最新の管理対象/アクティブサーバーのみ反映されます。

表

- 監査ポリシーは、別のポリシー内で定義されるルール、または別のポリシーから拡張される一連のルールで構成されます。複数レベルのポリシー継承をサポートしており、合成ポリシーを作成できます。

- ルールで構成済みのポリシーを使用する一連のターゲットサーバーに対する監査のスナップショット仕様を作成できます。仕様の結果は、将来の監査のベースラインとして使用できます。
- 監査は、以前に取得した監査のスナップショット仕様の結果を使用する一連のターゲットサーバー、または単一サーバーがソースである最新のスナップショット仕様の結果に対して作成できます。
- 表は、最初にサーバー別にグループ化されます。各サーバーは、監査チェック済みポリシー内の各ポリシーやルールに対するコンプライアンス数を有します。
- サーバー Mが2つのポリシー (AおよびB) にアタッチされており、Aは「コンプライアンス」、Bは「非コンプライアンス」の場合、サーバー M全体のサーバーコンプライアンスステータスは「非コンプライアンス」と決定 (ロールアップ) されます。レポートでは、サーバー M、コンプライアンスステータス「コンプライアンス」、ポリシー「A」および「B」を選択する場合、サーバー Mのロールアップステータスが「非コンプライアンス」のため、検索結果は存在しません。
- 各ルールはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、監査ポリシー P1はサーバー 1 (S1) およびサーバー 2 (S2) に対する監査チェックです。P1ポリシーはルール1を保持し、S1とコンプライアンス、S2と非コンプライアンスとします。この場合、ルール1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Rule1 はポリシー P1 の一部のため、P1も非コンプライアンスとなります。P1はサーバー S1にアタッチされるため、S1は非コンプライアンスとなります。
- ポリシー内のルールは、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーのサーバーへのアタッチ詳細のみレポートされます。
- 各ターゲットサーバーについて取得される監査の詳細は、「値ベース」、「比較ベース」などの個別のルールタイプやチェックのタイプによって異なります。
- 「値ベース」のチェックは、「パスワードの最小文字数＝8」のようなターゲットサーバーの特定の値を検証するために実行します。監査ではユーザーが指定した「予期される値」とともに、「実際の値」がレポートされます。
- 「比較ベース」のチェックは、ソースサーバーとターゲットサーバー上のオブジェクト、ファイル、ディレクトリを比較するために実行します。監査結果は、ソースとターゲットの両方に存在するこれらのオブジェクト、またその差異によって異なります。
- 「比較ベース」のチェックの監査レポートでは、ソースサーバーとターゲットサーバーの差異のみ表示されます。
- 監査レポートには、次の列が表示されます。
  - Server Name
  - Check Item (ルールタイプによる)
  - Actual Value or Differences (ルールタイプによる)
  - Exception Details
  - Last Scan

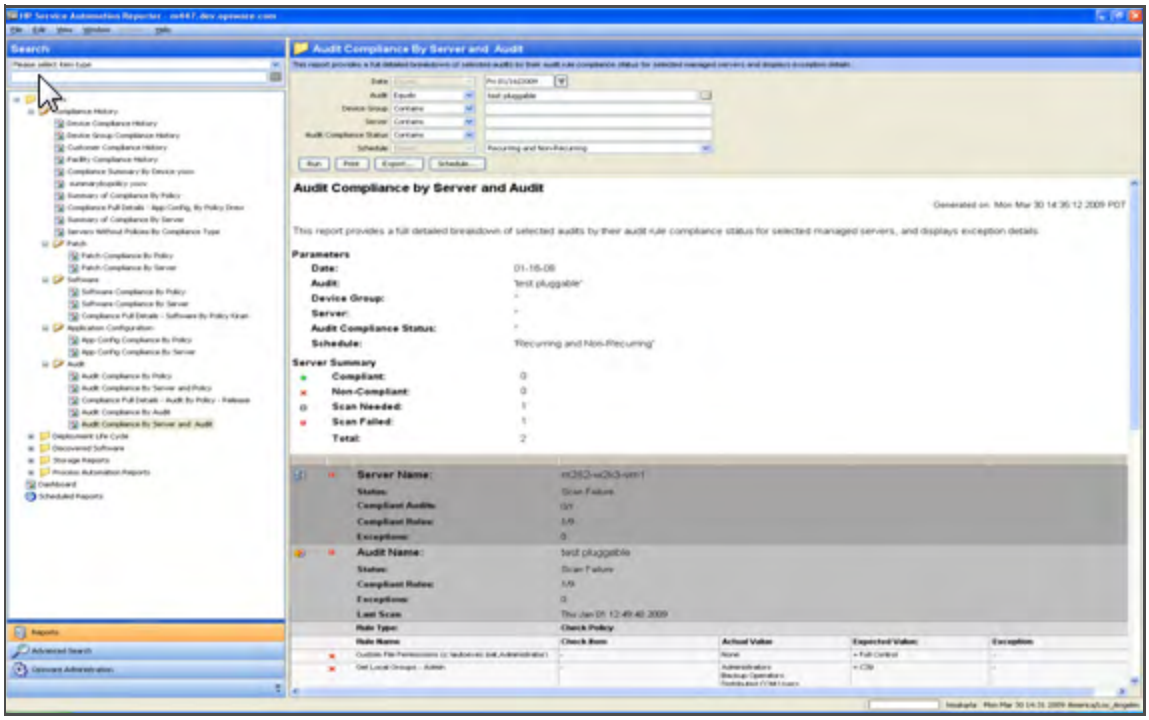
値ベースのチェック

「値ベース」のチェックは、次のルールタイプを使って実行できます。

- チェックポリシー /プラグ可能チェック
- アプリケーション構成ポリシー
- カスタムスクリプト

- ネットワークデュプレックス
- サーバーモジュールオブジェクト
- ストレージイニシエーター

図 25　Audit Compliance By Server and Audit - Value-Based Checks



比較ベースのチェック

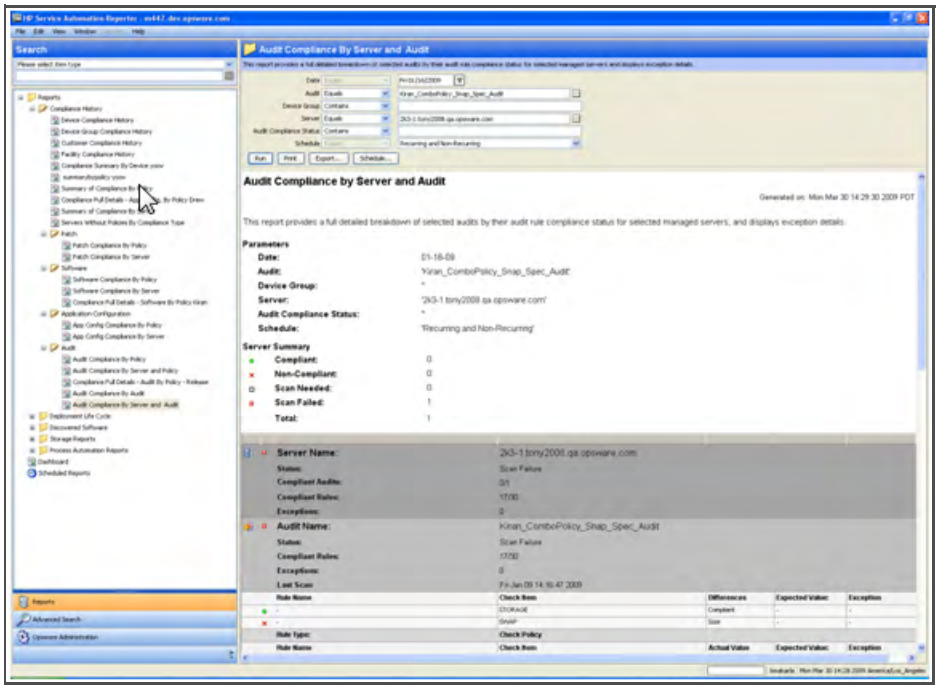
「比較ベース」のチェックは、次のルールタイプを使って実行およびレポートできます。

- ストレージイニシエーター
- チェックポリシー /プラグ可能チェック
- Windowsサービス
- レジストリ
- COM+
- カスタムスクリプト
- ストレージ
- ファイルシステム
- IISメタベース
- サーバーモジュールオブジェクト
- ハードウェア
- 監査の例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。特定のターゲットサーバーが例外条件を満たす場合、そのサーバーは「コンプライアンス」とみなされます。

詳細の実行

- 監査を選択して右クリック、次に [開く] を選択してSAポリシーブラウザーを開きます。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーを選択して右クリック、次に [開く] を選択してSAサーバーブラウザーを開きます。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 26　Audit Compliance By Server and Audit - Comparison-Based Checks



パッチ

Patch Compliance By Server

サマリー

- コンプライアンスサーバーの合計数。
- Non-Compliant: 非コンプライアンスサーバーの合計数。アタッチされるポリシー内のポリシーまたはパッチが1つ以上、非コンプライアンスの場合、サーバーは非コンプライアンスとみなされます。
- Scan Needed: スキャンを必要とするサーバーの合計数。アタッチされるポリシーが1つ以上、変更されると、サーバーはスキャンが必要な状態になります。サーバーコンプライアンスを決定するには、サーバーのスキャンが必要です。
- Scan Failed: コンプライアンスのためのサーバースキャンのジョブ完了に失敗したサーバーの合計数。
- Partially-Compliant: 管理者が設定したパッチコンプライアンス標準を完全に満たしていないサーバーの合計数。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

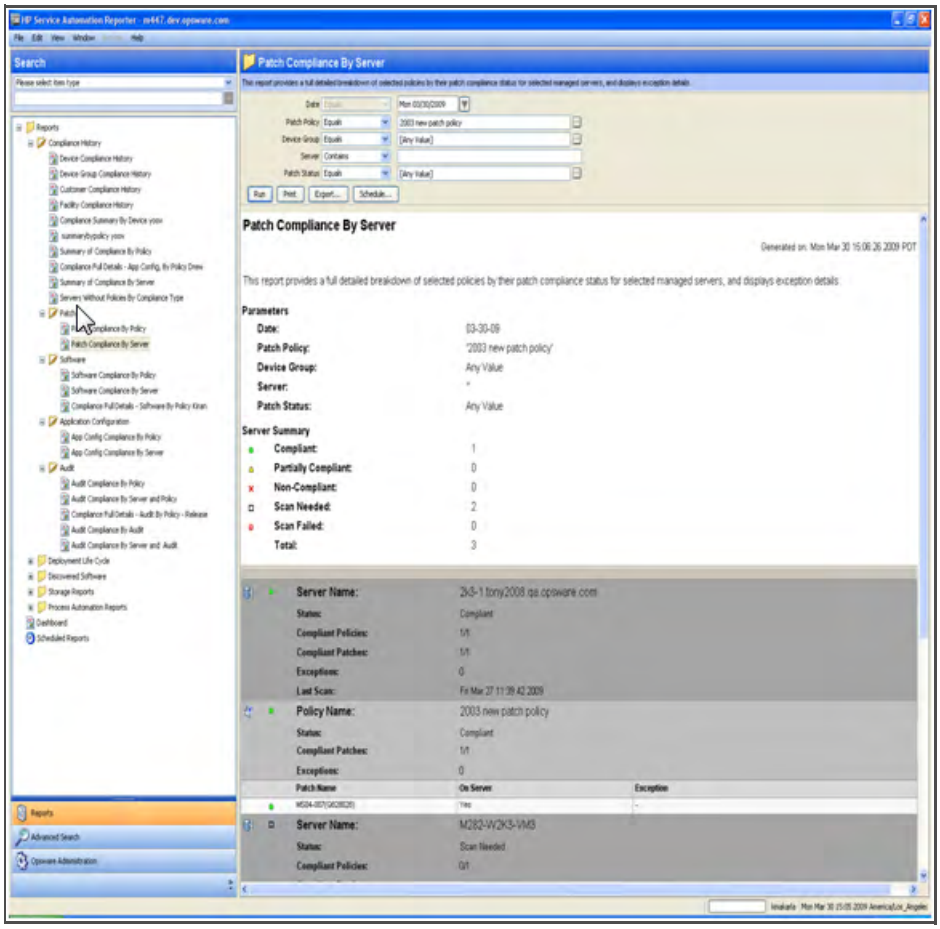
表

- パッチポリシーは、デバイスグループまたはサーバーに直接アタッチできます。一致するプラットフォーム上のサーバーのみレポートされます。
- デバイスグループは別のデバイスグループ、つまりネストされたデバイスグループを保持できます。パッチポリシーはネストされたデバイスグループにアタッチできます。デフォルトで親デバイスグループをユーザーのレポート条件の一部として選択すると、親デバイスグループに直接アタッチされたサーバーのみレポートされます。
- ネストされたデバイスグループのコンプライアンスの詳細を決定するには、ユーザーはレポート条件でネストされたデバイスグループを選択する必要があります。
- 表は、最初にサーバー別にグループ化されます。各サーバーは、アタッチされる各ポリシーとそのポリシーの一部である各パッチに対するコンプライアンス数を有します。
- 各パッチアイテムはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、パッチポリシー P1は、サーバー S1とサーバー S2にアタッチされます。ポリシー P1はItem1というパッチアイテムを保持し、サーバー S1 に対してコンプライアンス、サーバー S2 に対して非コンプライアンスとします。この場合、Item1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Item1 はポリシー P1 の一部のため、P1 も非コンプライアンスとなります。同様に、サーバー S1も非コンプライアンスとなります。
- ポリシー内パッチアイテムのコンプライアンスの詳細は、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- [部分コンプライアンス] のパッチアイテムにより、ポリシーは「非コンプライアンス」の一部となります。しかし、サーバーは [部分コンプライアンス] ステータスとなります。
- パッチアイテムの例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。例外条件を満たす場合、SA のパッチコンプライアンス ユーザー設定により、パッチはコンプライアンスまたは部分コンプライアンスになります。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 27　Patch Compliance By Server



Patch Compliance By Policy

サマリー

- Compliant Policies: サーバーにアタッチされる選択したポリシーの合計数に対する、選択したコンプライアンスポリシーの数。
- Compliant Patches: サーバーにアタッチされる選択した全ポリシー内の一意のパッチの合計数に対する、選択した全ポリシー内の一意のコンプライアンスパッチの数。
- Compliant Severs: 一意のサーバーの合計数に対する、一意のコンプライアンスサーバーの数。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

表

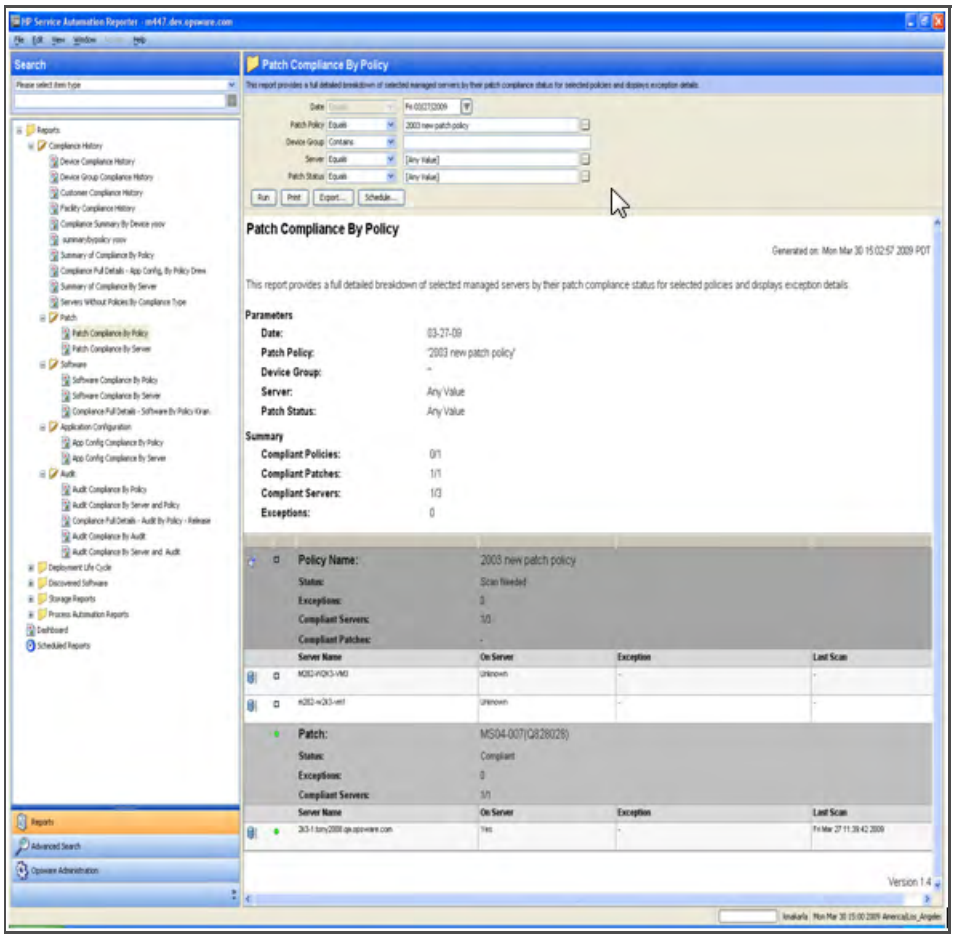
- パッチポリシーは、デバイスグループまたはサーバーに直接アタッチできます。一致するプラットフォーム上のサーバーのみレポートされます。
- デバイスグループは別のデバイスグループ、つまりネストされたデバイスグループを保持できます。パッチポリシーはネストされたデバイスグループにアタッチできます。デフォルトで親デバイスグループをユーザーのレポート条件の一部として選択すると、親デバイスグループに直接アタッチされたサーバーのみレポートされます。

- ネストされたデバイスグループのコンプライアンスの詳細を決定するには、ユーザーはレポート条件でネストされたデバイスグループを選択する必要があります。
- 表は、最初にポリシー別にグループ化されます。各ポリシーは、ポリシーをアタッチする各パッチやサーバーに対するコンプライアンス数を有します。
- 各パッチアイテムはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、パッチポリシー P1は、サーバー S1とサーバー S2にアタッチされます。ポリシー P1はItem1というパッチアイテムを保持し、サーバー S1 に対してコンプライアンス、サーバー S2 に対して非コンプライアンスとなります。この場合、Item1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Item1はポリシー P1の一部のため、P1も非コンプライアンスとなります。
- ポリシー内パッチアイテムのコンプライアンスの詳細は、アタッチ先のサーバーがスキャン済みのときのみレポートされます。スキャン失敗またはスキャンが必要なケースでは、ポリシーとサーバーのアタッチ詳細のみレポートされます。
- [部分コンプライアンス] のパッチアイテムにより、ポリシーは「非コンプライアンス」の一部となります。しかし、サーバーは [部分コンプライアンス] ステータスとなります。
- パッチアイテムの例外は、「Exception Details」、「Exception Expiration Date」の有無に関わらず作成できます。例外条件を満たす場合、SA のパッチコンプライアンス ユーザー設定により、パッチはコンプライアンスまたは部分コンプライアンスになります。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 28　Patch Compliance By Policy



ソフトウェア

Software Compliance by Policy

サマリー

- Compliant Policies: サーバーにアタッチされる選択したポリシーの合計数に対する、選択したコンプライアンスポリシーの数。
- Compliant Items: サーバーにアタッチされる選択した全ポリシー内の一意のアイテムの合計数に対する、選択した全ポリシー内の一意のコンプライアンスアイテムの数。
- Compliant Severs: 一意のサーバーの合計数に対する、一意のコンプライアンスサーバーの数。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

表

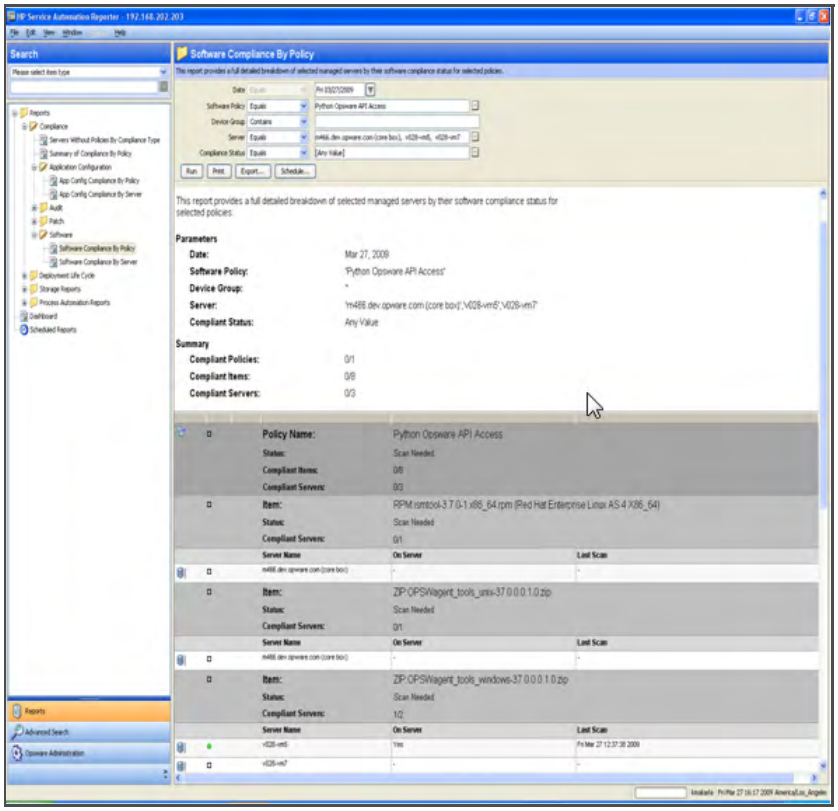
- ソフトウェアポリシーは、デバイスグループまたはサーバーに直接アタッチできます。ポリシーがデバイスグループにアタッチされる場合、一致するプラットフォーム上のサーバーのみレポートされます。

- 表は、最初にポリシー別にグループ化されます。各ポリシーは、ポリシーをアタッチする各アイテムやサーバーに対するコンプライアンス数を有します。
- 各アイテムはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。コンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、ソフトウェアポリシーP1はItem1というアイテムを保持し、サーバーS1に対してコンプライアンス、サーバーS2に対して非コンプライアンスとします。この場合、Item1に対する正味のコンプライアンスステータスは、非コンプライアンスとなります。Item1はソフトウェアポリシーP1の一部のため、P1もサーバーに対して非コンプライアンスとなります。
- アイテムにSMO (Server Module Objects) をもつソフトウェアポリシーは、レポートされません。
- アイテム名は、(ZIP、MSI、RPMなどの) ユニットの具体的なアイテムタイプと、アプリケーション構成インスタンスAppConfig_Instanceとの組み合わせで、それぞれの名前とともに表示されます。
- しかし、サーバー上に存在する必須/強制ソフトウェアアイテムがコンプライアンスとみなされるケースで、RPMの新バージョンがサーバーにインストール済みかつ旧バージョンがモデルに存在する場合、必須アイテムのバージョンがサーバー上に存在しないにも関わらずコンプライアンスとみなされることがあります。このような例外は当該サーバーの横に「*」マークが付き、レポートにその旨を記した脚注が表示されます。
- アタッチされたポリシーが空の場合も、サーバーは「コンプライアンス」とみなされます。ただし、レポートする詳細がないため、アイテム情報は表示されません。同様に詳細に欠けるため、[On Server] フィールドには「Unknown」とマークされます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 29　ポリシー別ソフトウェアコンプライアンス



Software Compliance by Server

サマリー

- Compliant: コンプライアンスサーバーの合計数。
- Non-Compliant: 非コンプライアンスサーバーの合計数。アタッチされるポリシー内のポリシーまたはアイテムが1つ以上、非コンプライアンスの場合、サーバーは非コンプライアンスとみなされます。
- Scan Needed: スキャンを必要とするサーバーの合計数。アタッチされるポリシーが1つ以上、変更されると、サーバーはスキャンが必要な状態になります。サーバーコンプライアンスを決定するには、サーバーのスキャンが必要です。
- カウントには、最新の管理対象/アクティブサーバーのみ反映されます。

表

- ソフトウェアポリシーは、デバイスグループまたはサーバーに直接アタッチできます。ポリシーがデバイスグループにアタッチされる場合、一致するプラットフォーム上のサーバーのみレポートされます
- 表は、最初にサーバー別にグループ化されます。各サーバーは、アタッチされる各ソフトウェアポリシーに対するコンプライアンス数を有します。
- 各アイテムはポリシー内でさらにグループ化され、詳細なレベルのコンプライアンス情報を提供します。サーバーコンプライアンスステータスは、このレベルからロールアップまたはバブルアップされます。たとえば、ソフトウェアポリシー P1はItem1というアイテムを保持し、サーバー S1に対してコンプライ

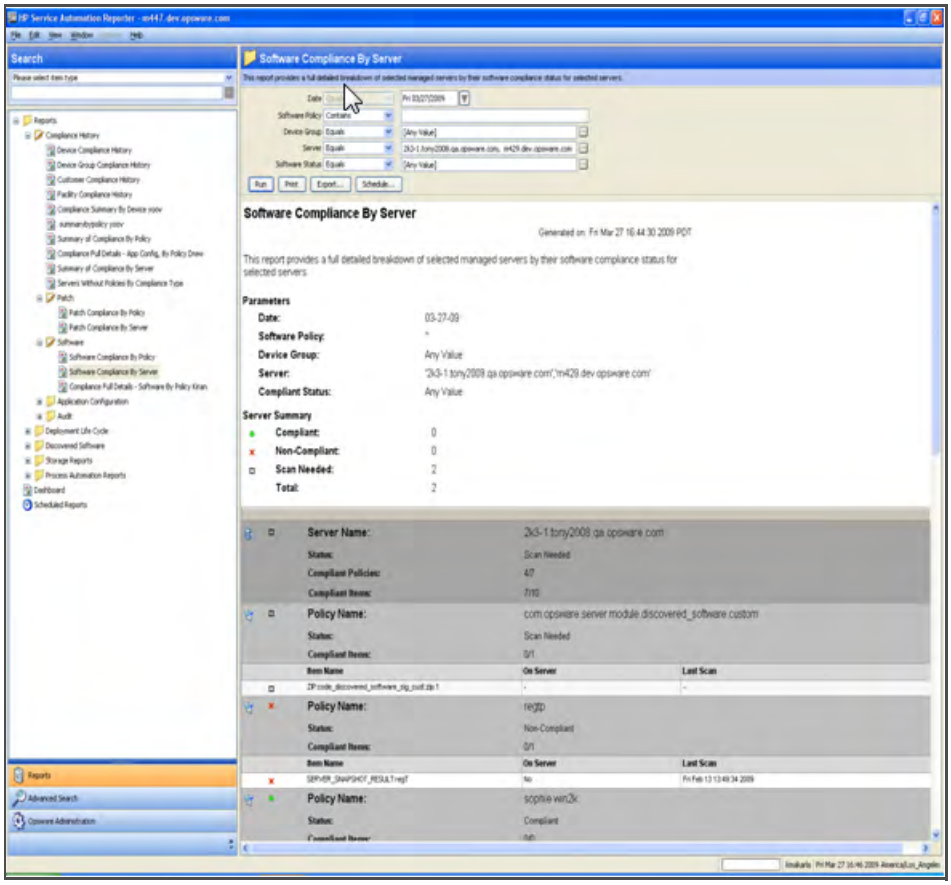
アンスとします。同様に、別のソフトウェアポリシー P2はItem2というアイテムを保持し、サーバー S1に対して非コンプライアンスとします。ポリシー1はコンプライアンス、ポリシー2は非コンプライアンスのため、正味のサーバーコンプライアンスステータスは非コンプライアンスとなります。

- アイテムにSMO (Server Module Objects) をもつソフトウェアポリシーは、レポートされません。
- アイテム名は、(ZIP、MSI、RPMなどの) ユニットの具体的なアイテムタイプと、アプリケーション構成インスタンスAppConfig_Instanceとの組み合わせで、それぞれの名前とともに表示されます。
- しかし、サーバー上に存在する必須/強制ソフトウェアアイテムがコンプライアンスとみなされるケースで、RPMの新バージョンがサーバーにインストール済みかつ旧バージョンがモデルに存在する場合、必須アイテムのバージョンがサーバー上に存在しないにも関わらずコンプライアンスとみなされることがあります。このような例外は当該サーバーの横に「*」マークが付き、レポートにその旨を記した脚注が表示されます。
- アタッチされたポリシーが空の場合も、サーバーは「コンプライアンス」とみなされます。ただし、レポートする詳細がないため、アイテム情報は表示されません。同様に詳細に欠けるため、[On Server] フィールドには「Unknown」とマークされます。

詳細の実行

- ポリシーをダブルクリック/右クリックして [開く] を選択し、SAポリシーブラウザーを起動します。ポリシーに関する操作は、ユーザーのアクセス権に基づきます。
- サーバーをダブルクリック/右クリックして [開く] を選択し、SAサーバーブラウザーウィンドウを起動します。サーバーに関する操作は、ユーザーのアクセス権に基づきます。

図 30　サーバー別ソフトウェアコンプライアンス



第 4 章　SAクライアントレポート

SA クライアントレポートでは、環境内の管理対象サーバー、仮想サーバー、ネットワークデバイス、ユーザーのアクセス権とセキュリティ権限に関する包括的な情報がリアルタイムで提供されます。これらのパラメーター化されたレポートはグラフと表の形式で提示され、アクショナブルです。つまり、オブジェクトに対してレポート内でポリシーや監査などの適切なアクションを実行できます。また、組織で使用しやすいように (.htmlファイルや.pdfファイル、.xlsファイルとして)、ローカルファイルシステムにエクスポートすることもできます。

この項には、SA クライアントレポートのタイプ、レポートパラメーターの変更方法、レポートの実行方法、レポート内でのアクション実行方法などに関する情報が含まれます。

SAクライアントの追加レポート機能は、BSA Essentialsクライアントで使用できます。詳細については、BSA EssentialsのSAレポート (7ページ) を参照してください。

この項では、次の事項を説明します。

レポートの各種機能

SAクライアントレポートには、エンタープライズの正常性評価を実行するための、次の機能が用意されています。

- オブジェクトに対してレポート内で適切なアクションを実行できるアクショナブルレポート。たとえば、コンプライアンスレポートのリストビューでは、サーバーを選択して [リモートターミナル] または [サーバーエクスプローラー] を開いて参照したり、監査を実行したり、スナップショットを作成したり、パッケージを作成したりできます。
- 全レポート対応のSAクライアントダッシュボードで単一のエントリポイント。
- ユーザーのアクセス権で管理され、データがセキュリティ保護されたレポート。読み取りアクセス権をもつすべてのオブジェクトを表示可能です。書き込みアクセス権をもつオブジェクトに対するアクションを実行可能です。
- .html、.pdf、.xls形式にエクスポート可能なレポート。組織で使用するために、ローカルファイルシステムにレポートをエクスポートできます。

HP Server Automationクライアントレポート

次のテーブルは、レポートフォルダーごとのSAクライアントレポートの一覧です。

表 8　SAクライアントレポート

レポート フォルダー	レポートタイトル
サーバー レポート	• カスタマーごとのサーバー • ファシリティごとのサーバー • メーカーごとのサーバー • モデルごとのサーバー • オペレーティングシステムごとのサーバー • 使用状況ごとのサーバー
仮想化レポート	• Solaris 10 — ハイパーバイザーごとの仮想サーバー (Zonesのみ) — ハイパーバイザーごとのリソース割り当て (Zonesのみ)
ユーザーおよびセキュリティ レポート	• クライアントおよび機能のアクセス権 • カスタマー / ファシリティアクセス権およびデバイスグループアクセス権のオーバーライド • ユーザーグループのメンバーシップ • ユーザーログイン • 管理者アクション • ユーザーと承認、ユーザーグループ別 • ユーザーと承認、個別ユーザーグループ別 • 管理者カスタマーグループ • サーバーアクセス権、ユーザー別 • サーバーアクセス権、サーバー別 • OGFSアクセス権、ユーザー別 • OGFSアクセス権、サーバー別
ネットワーク レポート	• ネットワークデバイスごとの接続 • サーバーごとの接続 • デュプレックスコンプライアンス (すべてのサーバー) • カスタマーごとのデュプレックスコンプライアンス • ファシリティごとのデュプレックスコンプライアンス 『SA統合ガイド』の「ネットワークレポート」も参照してください。

SAクライアントの追加レポート機能は、BSA Essentialsクライアントで使用できます。詳細については、BSA EssentialsのSAレポート (7ページ) を参照してください。

レポートのユーザーアクセス権

各レポートは、ユーザーのアクセス権で管理されます。読み取りアクセス権をもつすべてのオブジェクトを表示できます。また、書き込みアクセス権をもつオブジェクトに対するアクションを実行できます。

ネットワークレポートを表示または実行するには、SA/NA統合の構成が必要です。『SA統合ガイド』を参照してください。

ユーザーおよびセキュリティレポートを表示または実行するには、システム管理者のアクセス権が必要です。

レポート機能の起動

Reports機能を起動するには、次のいずれかの手順を実行します。

- [**表示**] メニューから、[**レポート**] > [**ダッシュボード**] を選択。
- [**表示**] メニューから、[**レポート**] > [**レポート**] を選択。
- ナビゲーションペインで [レポート] を選択。

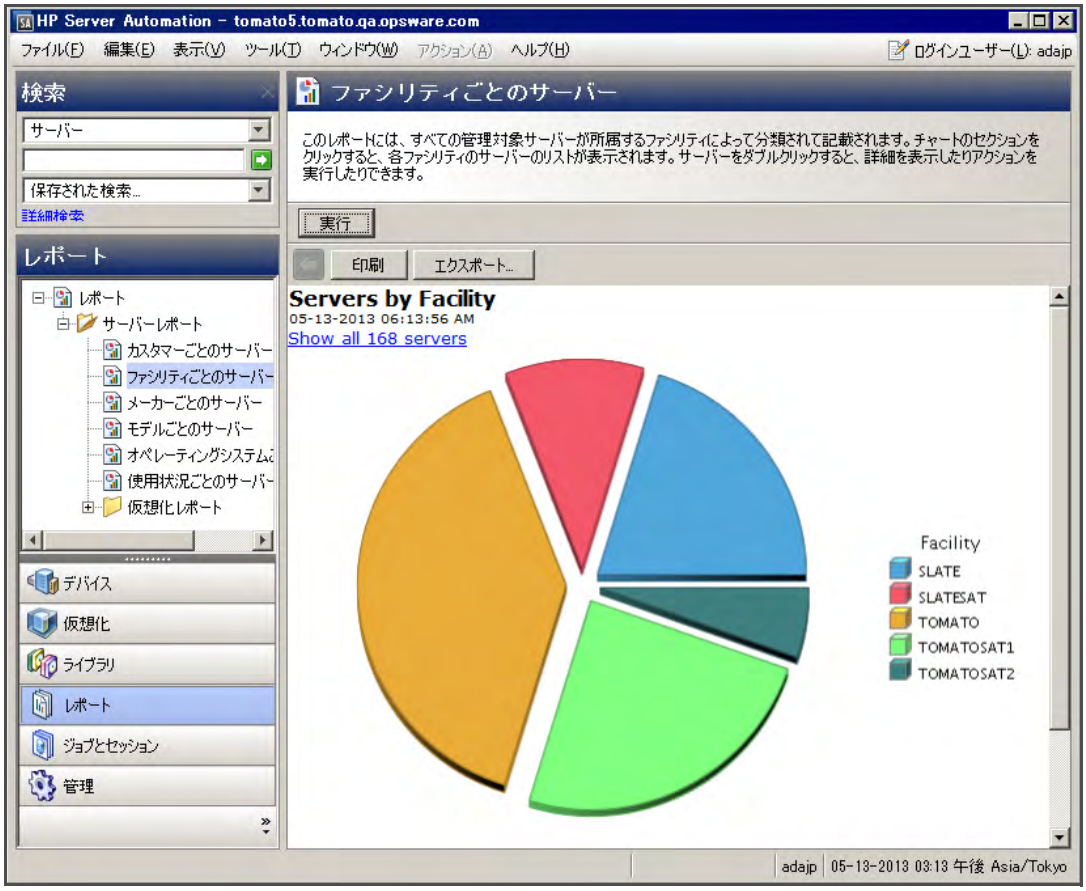
Reports表示

SAクライアントのレポートウィンドウは、検索ペイン、レポートパラメーター、レポートフォルダー、その他フィルタリングツールで構成されます。

この項では、次の事項を説明します。

- 検索ペイン
- レポートフォルダー
- レポートパラメーター

図 31　レポート機能の表示



検索ペイン

すべてのタブビューには検索ペインがあり、コンポーネントカテゴリを選択し、検索テキストフィールドにキーワードを入力して、SAクライアントの情報を検索できます。追加のフィルター条件を指定するオプションとともに、内容ペインの構成可能なリストに結果が表示されます。詳細については、『SAユーザーガイド: Server Automation』を参照してください。

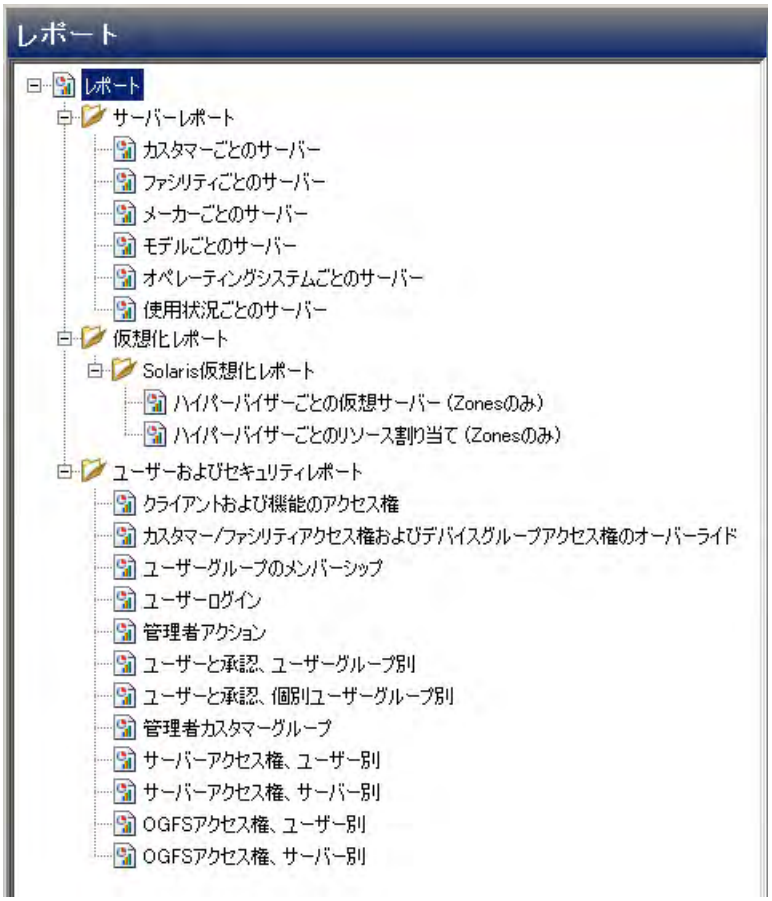
レポートフォルダー

規制基準やITのベストプラクティスに従い、各レポートはフォルダに整理されています。

- **サーバーレポート**: このフォルダーには、カスタマー、ファシリティ、メーカー、モデル、オペレーティングシステム、サーバー使用状況ごとのサーバーに関するレポートが含まれます。
- **仮想化レポート**: このサブフォルダーには、テクノロジーごと、またハイパーバイザーごとの仮想サーバーとリソース割り当てに関するレポートが含まれます。
- **ネットワークレポート**: このフォルダーには、ネットワークデバイスおよびサーバーの接続およびデュプレックスのコンプライアンスに関するレポートが含まれます。このフォルダーを参照するには、NAのインストールが必要です。
- **ユーザーおよびセキュリティレポート**: このフォルダーには、クライアントおよび機能のアクセス権、カスタマー /ファシリティ /デバイスグループのアクセス権、ユーザーグループのメンバーシップに関するレポートが含まれます。このフォルダーを参照するには、システム管理者のアクセス権が必要です。

次の図は、ナビゲーションペインに表示された [レポート] フォルダーと、各フォルダーに含まれるレポートを示しています。

図 32　レポートフォルダー



レポートパラメーター

多くのレポートでは、実行するために入力パラメーターが必要です。こうしたレポートはデフォルトのパラメーター値で実行できるほか、パラメーター値の変更も可能です。特定のサーバーやカスタマー、ハードウェアモデルを含む、あるいは含まないレポートを実行したいときは、レポートパラメーターで条件を指定する必要があります。レポートの実行 (73ページ) を参照してください。

レポートの実行と変更

この項では、次の事項を説明します。

- レポートの実行
- レポートパラメーターの変更

レポートの実行

レポートを実行するには、次の手順を実行します。

1　ナビゲーションペインで [**レポート**] を選択します。

2　[レポート] フォルダーを展開し、次に [サーバーレポート] と [仮想化レポート] を展開します。

3 フォルダーに表示された仮想化レポートの1つを選択します。

4 [コンテンツ] ペインにレポートパラメーターが存在しない場合、[**実行**] をクリックします。

5 [コンテンツ] ペインにレポートパラメーターが存在する場合、デフォルトパラメーターを使用またはパラメーターを変更します。

- デフォルトのレポートパラメーターを使用するには、[**実行**] をクリックしてレポートを実行します。レポート結果は、内容ペインに表示されます。レポート結果 (74ページ) を参照してください。
- レポートパラメーターを変更するには、レポートパラメーターの変更 (74 ページ) を参照してください。

レポートパラメーターの変更

デフォルトパラメーターを変更して、特定のサーバーやカスタマー、ハードウェアモデルを含むレポートを実行できます。

デフォルトパラメーターを変更するには:

1 (サーバー、カスタマー、モデルなどの) ドロップダウンリスト で、[次の値を含む]、[次の値に等しい]、[次の値で始まる]、[次の値で終わる] を選択します。

2 (オプション) 省略記号ボタンを選択して、[値の選択] ウィンドウを開きます。

3 [値の選択] ウィンドウで [利用可能] または [選択済み] ペインの値を選択し、双方向ボタンを使って検索条件に値を含めたり、条件から除外したりします。

4 [**OK**] をクリックして変更内容を保存します。

5 [**実行**] をクリックしてレポートを実行します。レポート結果は、内容ペインに表示されます。レポート結果 (74ページ) を参照してください。

データが見つからずレポートを実行できない場合、"No records to display!" エラーが表示されます。詳細については、レポート結果の制限 (77ページ) も参照してください。

レポート結果

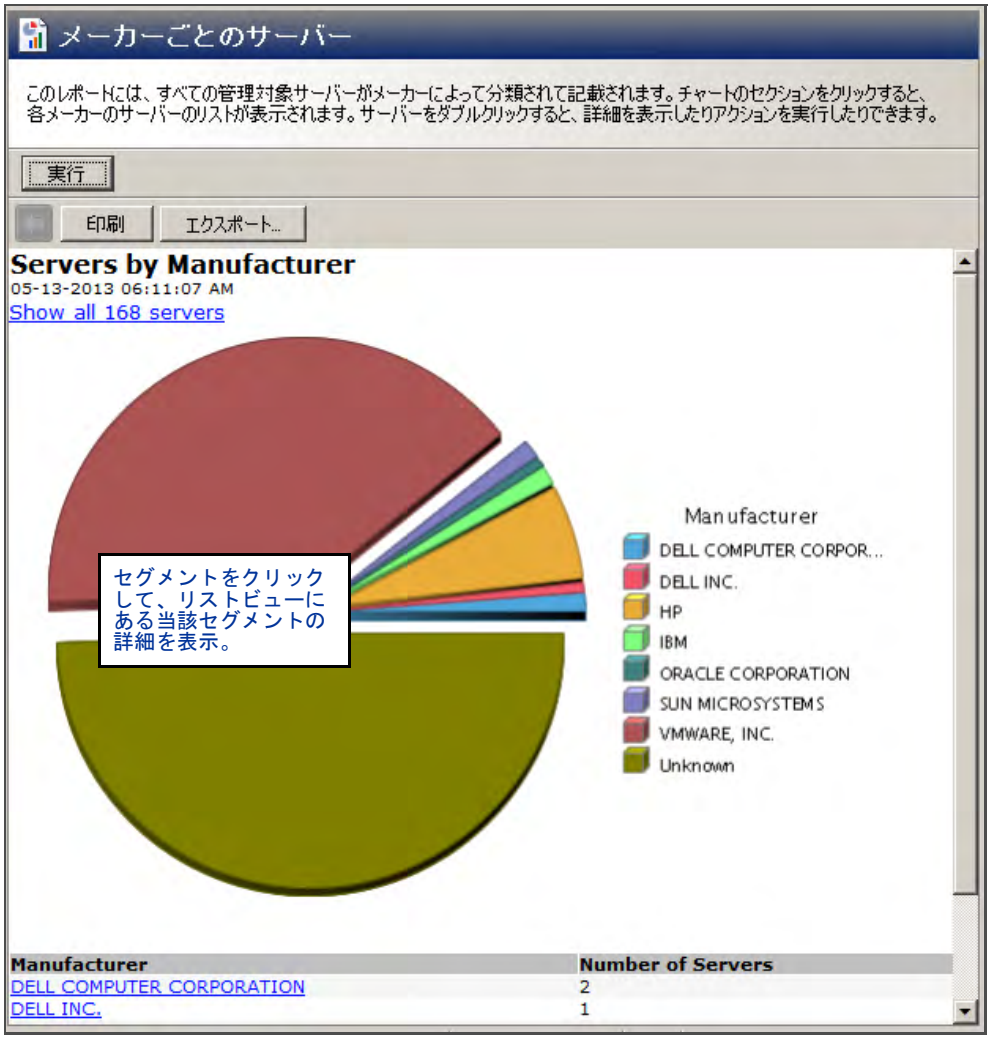
レポート結果はグラフィックまたはリストビューに最初に表示されます。グラフィックレポートはこのレポートに使用できるデータの概要を示すもので、円グラフまたは棒グラフで表示されます。グラフのいずれかの項目や棒をクリックして、詳細をドリルダウンできます。たとえば、レポートに表示される個別のサーバーについてドリルダウンし、サーバーの詳細情報を入手できます。

この項では、次の事項を説明します。

グラフィックレポートの表示

グラフィックレポートは円グラフで表示されます。

図 33　円グラフ

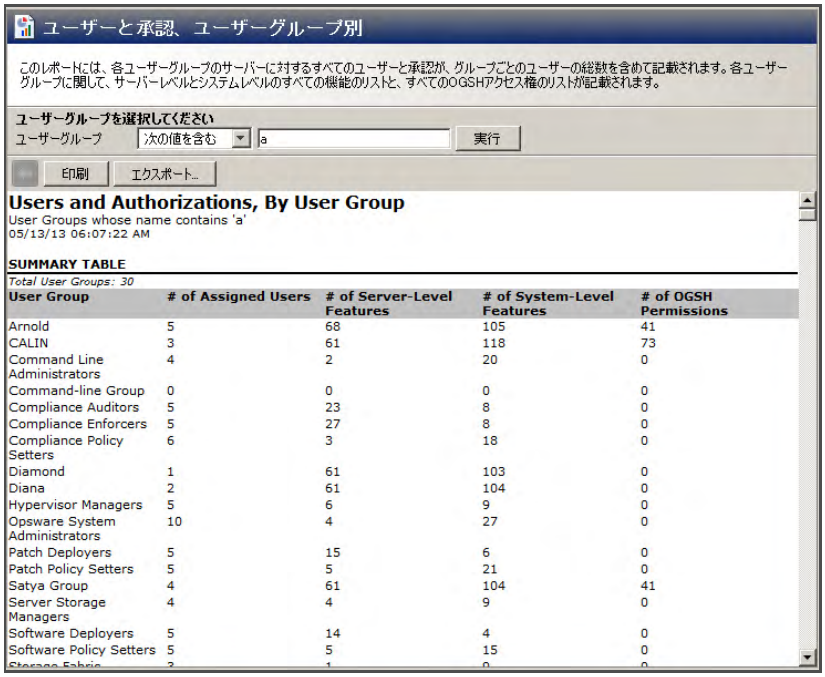


グラフの項目をクリックして詳細をドリルダウンしたり、アクションを実行したりします。また、「Show all <数値> servers」リンクをクリックして、サーバーの一覧を表示できます。

リストレポートの表示

リストレポートは、情報を表形式で表示したものです。サーバー、監査、ポリシーといったリストの行をダブルクリックして詳細を表示したり、アクションを実行したりします。図34の例を参照してください。

図 34　リストレポート



レポートのエクスポート

ローカルファイルシステムにレポートをエクスポートして他のアプリケーションで使用したり、電子メールに添付して配布したりできます。レポートのタイプにより、使用できるエクスポートファイルの形式が異なります。

- グラフィックレポート (円グラフや棒グラフ) は、.htmlまたは.pdf形式でエクスポート可能。
- リストレポートは、.html、.pdf、または.xls形式でエクスポート可能。

SA クライアントにレポートをエクスポートする場合、エクスポートしたレポートにマークされる時刻はレポートの作成時刻ではなく、レポートのエクスポート時刻になります。

レポートをエクスポートするには:

1. レポートで [**エクスポート**] をクリックし、[保存] ウィンドウを開きます。
2. フィールドの [保存] で、ファイルの保存先を入力するか、ドロップダウンリストから選択します。
3. ファイル名を入力します。
4. ファイルタイプを選択します。
5. [**保存**] をクリックします。

レポートの印刷

レポートを印刷するには:

1. レポートで [**印刷**] をクリックし、[印刷] ウィンドウを開きます。
2. デフォルトの印刷オプションを使うか、オプションを変更し、[**OK**] をクリックします。

レポート結果の制限

次のレポートは、結果表示できるアイテムが2000件に限られます。

- サーバーアクセス権、サーバー別
- サーバーアクセス権、ユーザー別
- OGFSアクセス権、サーバー別
- OGFSアクセス権、ユーザー別

これらのレポート結果が2000件に達した場合、レポートは停止します。これは、指定した検索パラメーターによっては結果が何千件にものぼることがあり、SAコアのパフォーマンスを低下させる恐れがあるためです。

たとえば [サーバーレポート、ユーザー別] は、検索パラメーターでユーザー 10人、サーバー 200台を指定した場合は問題なく実行されますが、ユーザー 10人、サーバー 201台を指定した場合には実行されません。

この問題を避けるには、検索パラメーターを変更して結果の件数を少なくするか、レポートクエリをより絞り込んだ検索に分割して、結果として必要なだけ絞り込んだレポートを複数回実行します。

索引

T

V

Z

こ