# HP BSA Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: SA 9.0 and BSA Essentials 2.0

# Reports

Document Release Date: June 2010
Software Release Date: June 2010

# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notices

## Trademark Notices

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Adobe® is a trademark of Adobe Systems Incorporated.

## Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

**http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

## Support

Visit the HP Software Support Online web site at:

**www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

To find more information about access levels, go to:

**http://h20230.www2.hp.com/new_access_levels.jsp**

# Contents

# 1 Server Automation Reports

This document describes the Server Automation (SA) 9.0 reports that are distributed through the BSA Essentials Network.

These reports are designed for BSA Essentials 2.0, and are viewable in the BSA Essentials Client.

SA provides the following two report types:

- **SA General Reports**

  General reports about various SA features, such as Windows Patching, Virtualization, Deployment Automation, and installed SA Server Agents. These reports can be downloaded from the BSA Essentials Network using the bsae_sa_reports stream.

- **SA Compliance Reports**

  Reports that display the compliance state of your data center, such as overall server compliance status, overall compliance by policy, and specific compliance categories for features such as Application Configuration, Windows Patching, Audits, and Software Management. These reports can be downloaded from the BSA Essentials Network using the sar78_reports stream.

## Windows Patching Reports

### ROI: Servers Affected by Windows Patch Policy Updates

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

For example, Microsoft Windows patches are made available on the second Tuesday of each month. SA Windows Patch Policies can be configured to automatically download new patches so they can be installed on specified servers.

SA automated patching provides return on investment by keeping all Windows Servers that are affected by new updates current and compliant with your Microsoft patch policy standards.

➤ This report does not support negative numbers for input.

#### Parameters

- **Date Range**: Allows you to filter the range of dates during which selected Windows Patch Policy were updated.
- **Policy Name**: Name of all policies that were modified with updates during the date range specified.

- **Per Server Cost**: The value that you apply to indicate the cost of bringing servers into compliance with respect to patch policies. This meaning of this unit can be any value you wish it to be, such as $, hours, and so on. (Negative numbers are not supported for this field.
- **Per Patch Cost**: The value that you apply to indicate the cost of installing one patch on a server. This meaning of this unit can be any value you wish it to be, such as $, hours, and so on. ( Negative numbers are not supported for this field.)

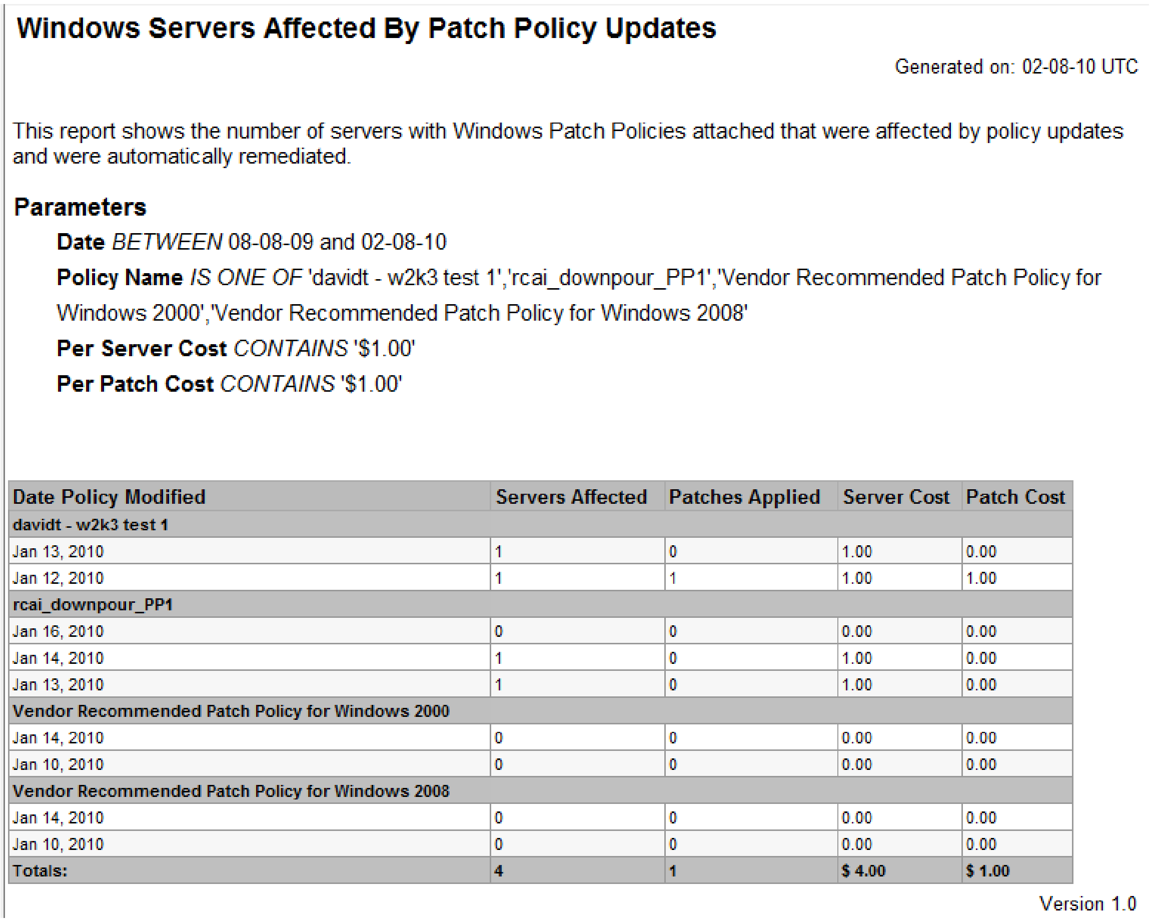
➤ The Per Server Cost and Per Patch Cost parameters use the “Contains” operator, but is considered equivalent (“equals”) to the value you enter in these fields.

## Table

- Results are grouped by policies.
- A row is shown for each date a policy is modified (within the specified date range).
- The counts and costs associated with each policy change date to reflect servers affected and patches applied due to the policy change.
- The per cost values can be any numeric value in units defined by the user such as dollars, hours, and so on.
- Total values for Servers Affected represents each time that a server is affected by a patch policy update (not unique servers). In some cases, you might see a total count of more than one server marked as being affected, when in fact a single servers is updated twice with a patch policy update. For example, if your report showed the following values for Servers Affected:
  - Mar. 10: Affected Servers = 1
  - Feb. 10: Affected Servers = 1
  - Total: Affected Servers = 2

  In this case it is possible the affected server in the Mar. 10 line item is the same server as the server that is counted in the Feb. 10 line item. In the total count 1 + 1 = 2, but the 2 servers are actually the same server counted twice. The reason the same server is affected by both Mar. 10 and Feb. 10 is because a patch applicable to the server was added to a policy in Feb. 10, and another applicable patch was added in on Mar. 10. So from an ROI perspective the server was affected twice, which is what the total count shows.

**Figure 1 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

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

When a change is made to a Windows patch policy (such as adding a patch), then the server or servers that the policy is attached to is considered non-compliant until the server is remediated to match the patch policy definition.

Using the date range parameters in this report, you can specify a time range and find out how long it takes for your windows servers to become compliant during any given time period after a Windows patch policy change is made.

> The server counts do not include servers that are in *scan needed* or *scan failed* states

### Parameters

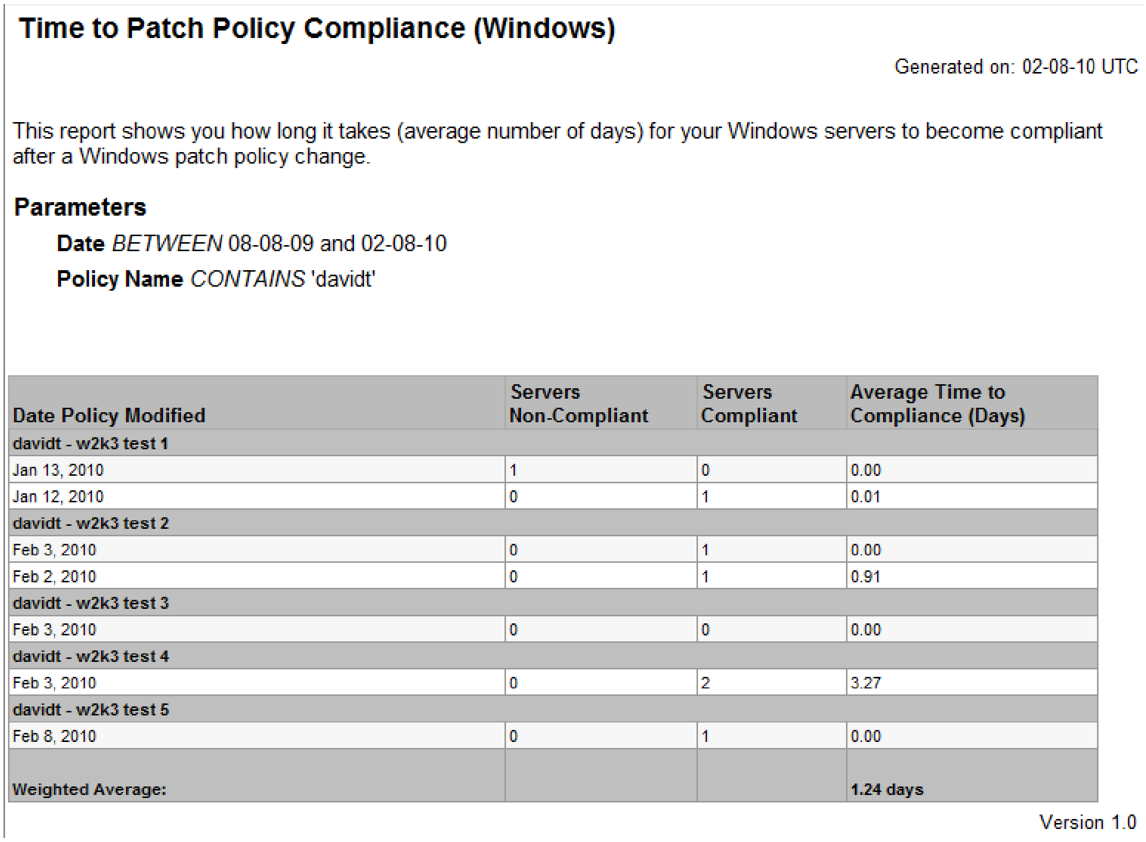
- **Date Range**: Allows you to specify a begin and end date criteria. This filter includes both the begin and end dates and determines the range of policy changes to show in the results.
- **Patch Policy**: Allows you to specify the Windows patch policies you want to return in the report results. Selection criteria can be: Equals, Contains, Begins With, or Ends With. If you select Equals [Any Value], this implies all Windows patch policies are selected.

All searches are case insensitive using the values specified.

## Table

- **Date Policy Modified**: Lists each patch policy select in the report parameters as well as each time the given policy was modified during the date range specified.
- **Servers Non-Compliant**: Indicates number of servers that were affected and made non-compliant after a patch policy change.
- **Servers Compliant**: Indicates number of servers that were affected and made compliant after a patch policy change.
- **Average Time to Compliance**: Average number of days (to 2 decimal places) between the time the policy was modified and when servers first became compliant.
- **Weighted Average**: Represents the average number of days to compliance for all servers that were affected patch policy changes for all selected policies in the report.

**Figure 2 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

# Virtual Server Reports

This section describes the reports about your virtual server environment.

## Virtualization Infrastructure Overview

This report compares managed virtual and physical servers, managed and unmanaged virtual servers and physical servers that are hypervisors and non-hypervisors.

### Graphs

These three charts show the type and degree of virtualization across your entire environment.

- Number of Managed Virtual vs. Managed Physical Servers compares all the managed virtual servers with all the managed physical servers and shows the degree of virtualization across your entire virtualized environment (VMware, Hyper-V, Solaris and so forth).
- Number of Managed vs. Unmanaged Virtual Servers compares all managed virtual servers with all unmanaged virtual servers.
- Number of Hypervisor vs. Non-Hypervisor Physical Servers compares all managed physical servers that are hypervisors with all managed physical servers that are not hypervisors.

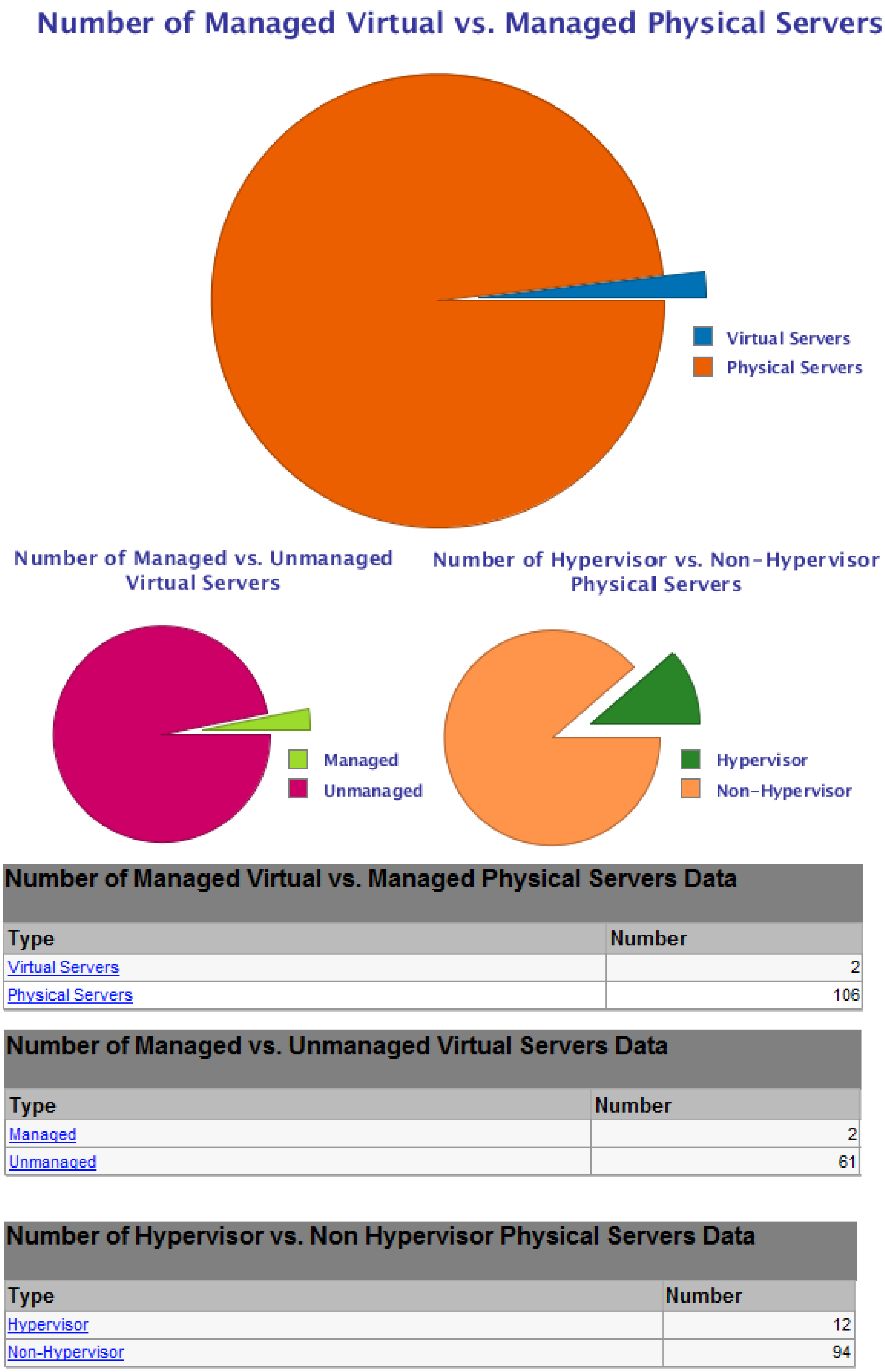
### Tables

- The tables show the corresponding data from the pie charts.

### Getting More Details

- Click on a section of any pie chart or on a link in any table to show a list of all the servers in that group.

**Figure 3 Pie Chart Showing Virtual and Physical Servers**


Number of Managed Virtual vs. Managed Physical Servers
🟦 Virtual Servers
🟧 Physical Servers
Number of Managed vs. Unmanaged Virtual Servers
🟩 Managed
🟥 Unmanaged
Number of Hypervisor vs. Non-Hypervisor Physical Servers
🟩 Hypervisor
🟧 Non-Hypervisor

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 |

# Managed Virtual vs. Physical Servers Trend Data

This report shows the percent of managed virtual servers versus managed physical servers over a time period. It shows how the percent of each type of server is changing over time.

## Graph

- The y axis is the percentage of each server type, virtual servers and physical servers.
- The x axis is the date.
- In Figure 4 below, approximately 10% of the managed servers are virtual servers and the remaining 90% are physical servers.

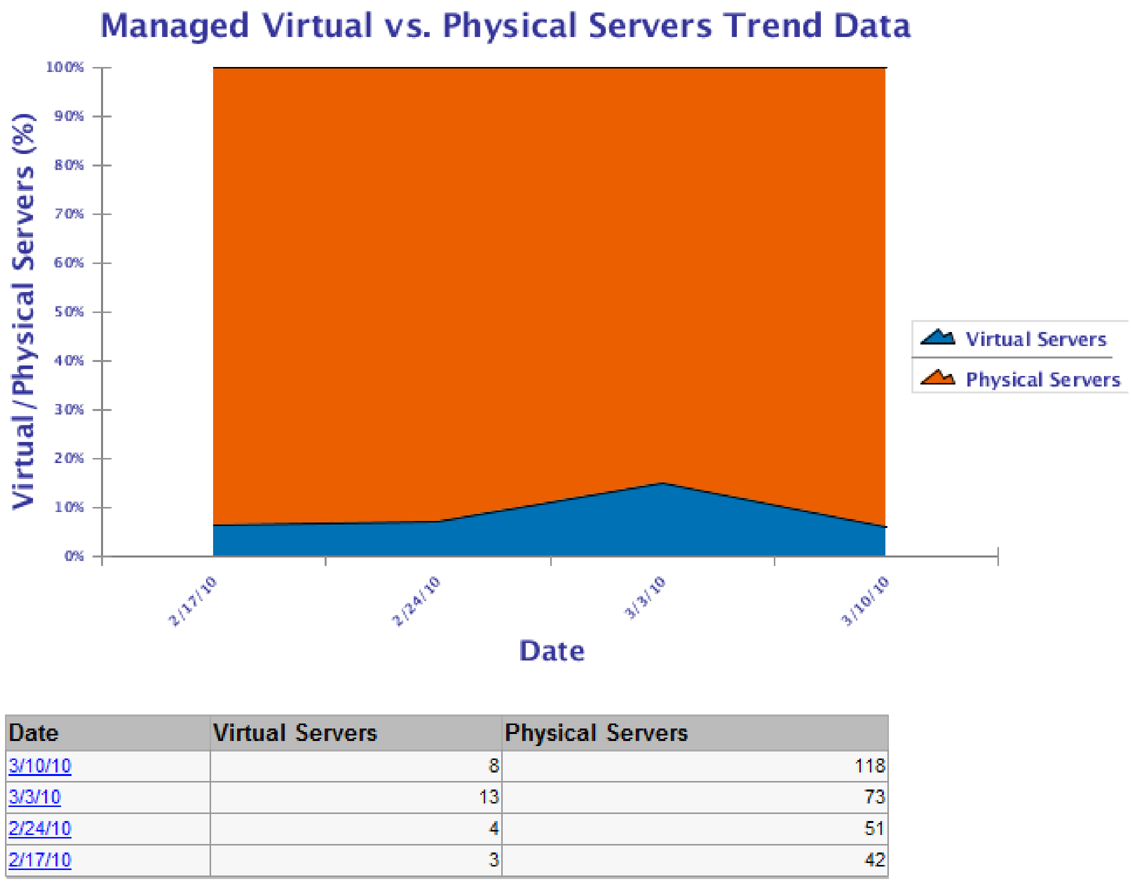
## Table

- The table gives the number of virtual and physical servers for each date in the specified date range and time interval.

## Getting More Details

- Click on a date in the table to display a list of all the servers on that date.

**Figure 4 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 and Not Running

This graph shows the number of virtual servers running and the number of virtual servers not running, over time. It is useful to determine which virtual servers are not being used and may be candidates for removal.

### Graph

- The y axis is the number of servers.
- The x axis is the date when the measurement was taken.

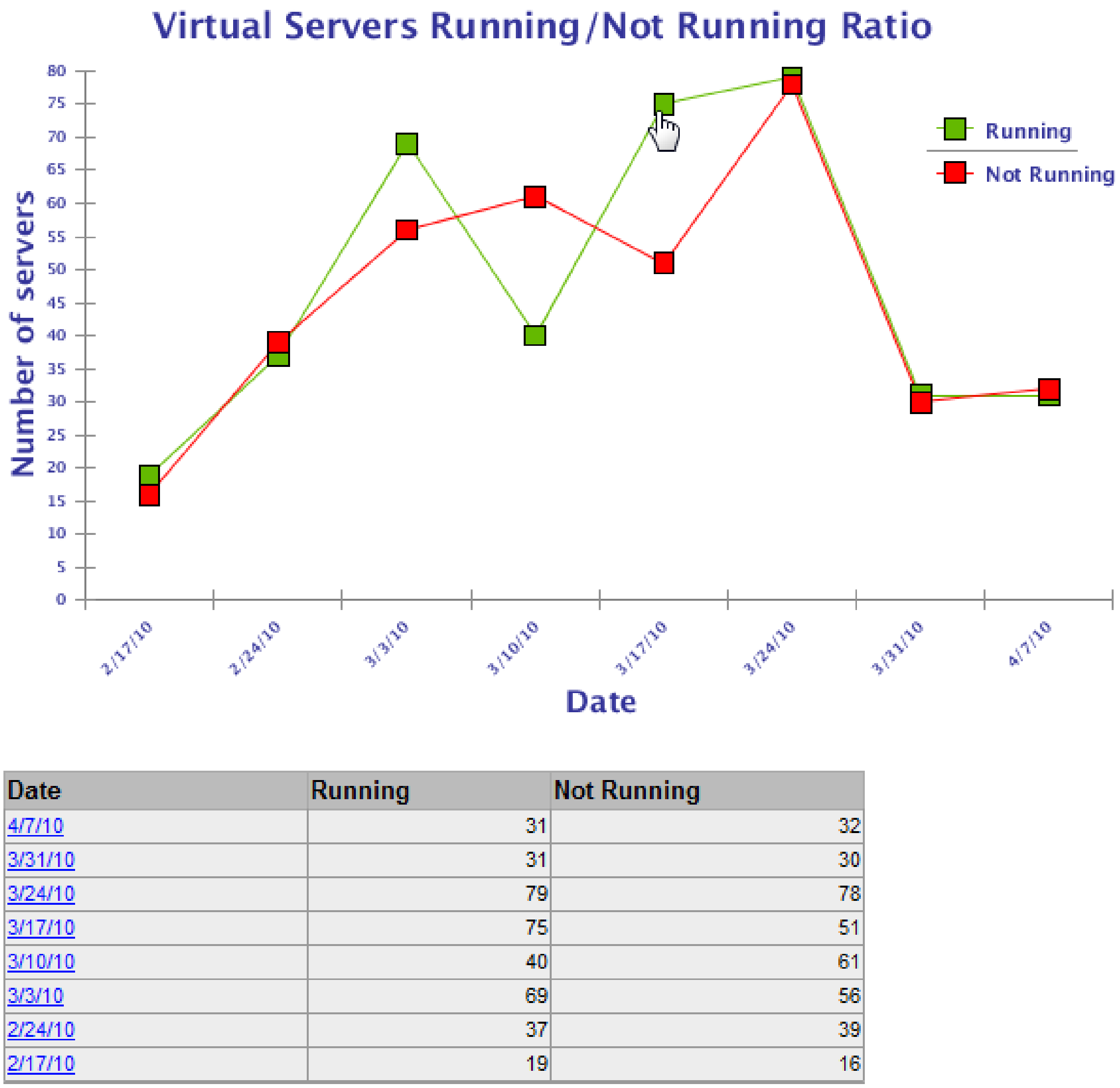
### Table

- The table lists the total number of servers in each category on each date in the specified interval.
- The total number of servers not running represents all the managed and unmanaged virtual servers that were powered off or not running on the specified date.
- The total number of running servers represents all the managed and unmanaged virtual servers that were powered on and running on the specified date.

### Getting More Details

- Click on a data point of the graph or on a date in the table to display a list of all the virtual servers in that category on that date.

**Figure 5 Virtual Servers Running and Not Running**

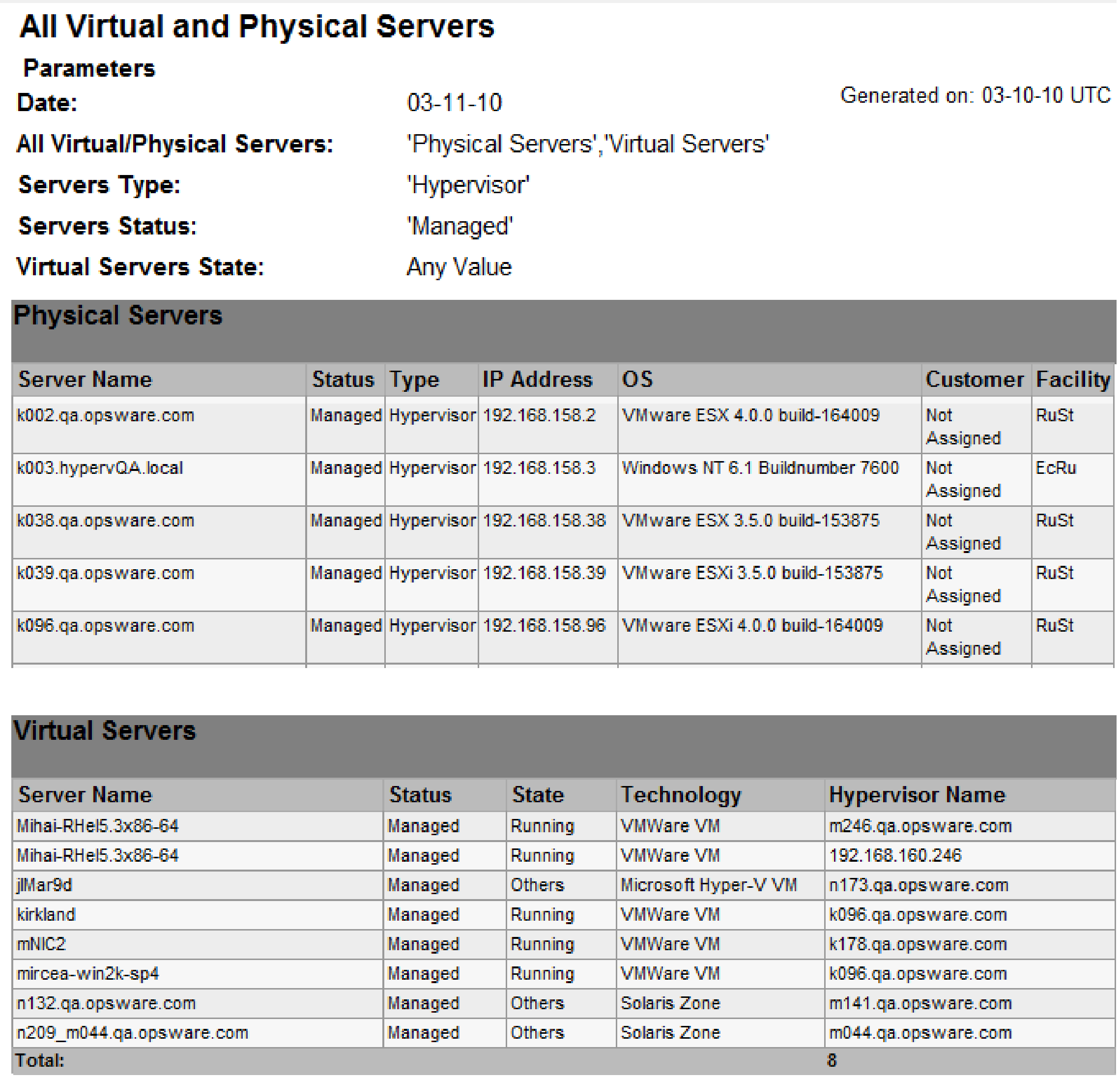


| Date | Running | Not Running |
|---|---|---|
| 4/7/10 | 31 | 32 |
| 3/31/10 | 31 | 30 |
| 3/24/10 | 79 | 78 |
| 3/17/10 | 75 | 51 |
| 3/10/10 | 40 | 61 |
| 3/3/10 | 69 | 56 |
| 2/24/10 | 37 | 39 |
| 2/17/10 | 19 | 16 |

## All Virtual and Physical Servers

This report displays details about all your virtual and physical servers on the specified date. It can also display the server type, hypervisor or non-hypervisor, whether the server is managed or unmanaged and whether the server is running or not. Figure 6 below shows a partial example of this table.

**Figure 6 Table Showing All Virtual and Physical Servers**



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 |

# Deployment Life Cycle Reports

This section describes the reports about your server deployments.

## Server Deployments by Operating System

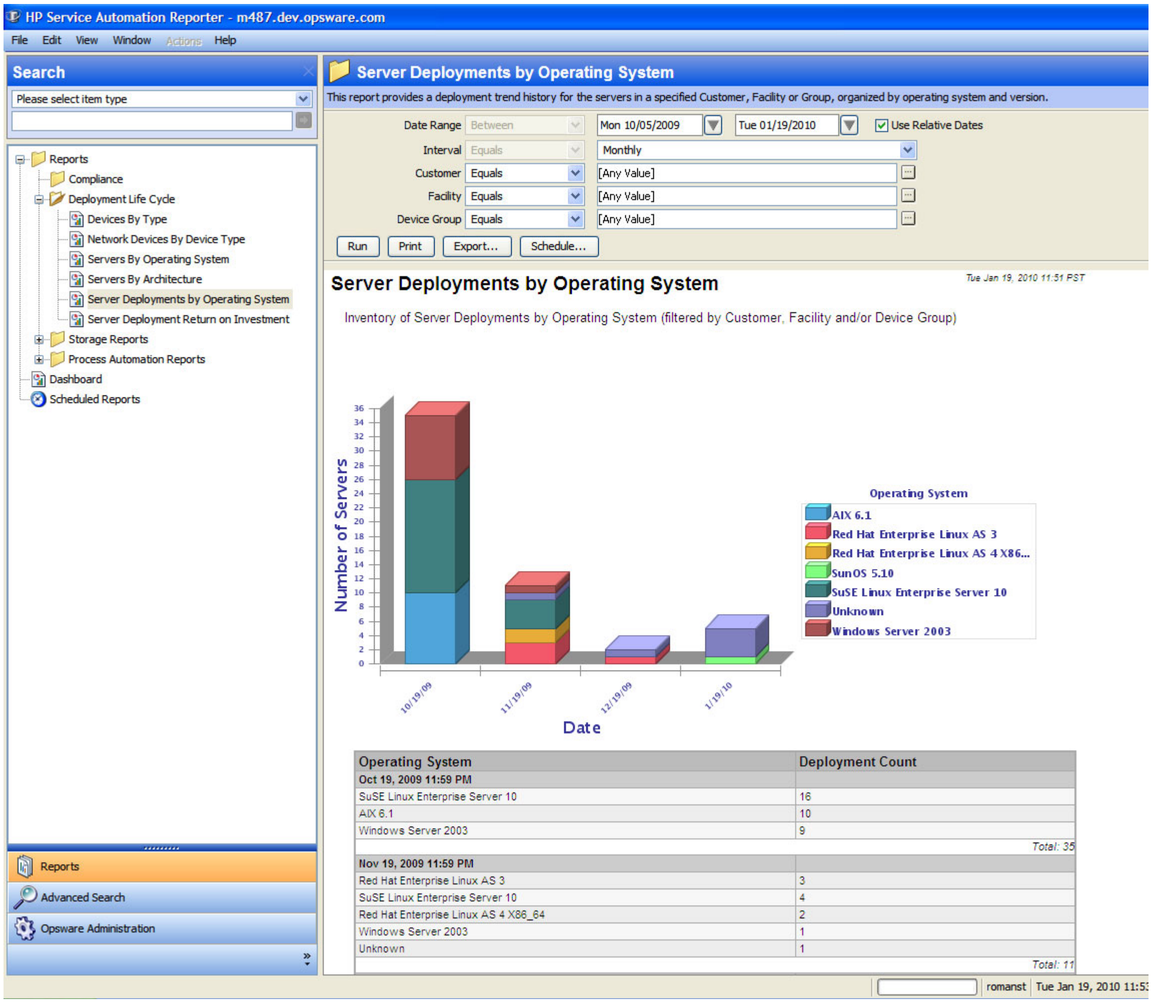
### Table

- Server deployment counts are grouped by operating system and time period.
- The Total number represents the total number of servers deployed during the specified time period.

### Graph

- The unit on the y-axis is the number of servers deployed during the specified time period.
- The counts are grouped by operating system.
- The x-axis is grouped by time period.

**Figure 7 Server Deployments by Operating System**



This report provides a deployment trend history for the servers in a specified Customer, Facility or Group, organized by operating system and version.

Date Range Between Mon 10/05/2009 Tue 01/19/2010 ☑ Use Relative Dates

Interval Equals Monthly

Customer Equals [Any Value]

Facility Equals [Any Value]

Device Group Equals [Any Value]

**Server Deployments by Operating System**

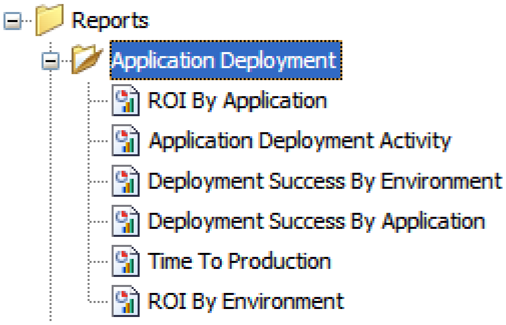
*Tue Jan 19, 2010 11:51 PST*

Inventory of Server Deployments by Operating System (filtered by Customer, Facility and/or Device Group)

| Operating System | Deployment Count |
|---|---|
| **Oct 19, 2009 11:59 PM** | |
| SuSE Linux Enterprise Server 10 | 16 |
| AIX 6.1 | 10 |
| Windows Server 2003 | 9 |
| | *Total: 35* |
| **Nov 19, 2009 11:59 PM** | |
| Red Hat Enterprise Linux AS 3 | 3 |
| SuSE Linux Enterprise Server 10 | 4 |
| Red Hat Enterprise Linux AS 4 X86_64 | 2 |
| Windows Server 2003 | 1 |
| Unknown | 1 |
| | *Total: 11* |

# Application Deployment Reports

This section describes the reports about Application Deployment activities performed in HP Server Automation. The following reports are available:



- Reports
  - Application Deployment
    - ROI By Application
    - Application Deployment Activity
    - Deployment Success By Environment
    - Deployment Success By Application
    - Time To Production
    - ROI By Environment

For more information about Application Deployment, refer to the *HP Server Automation Application Deployment User Guide*.

## Application Deployment Activity Reports

This report provides a list of all Application Deployment actions that are performed within a specified time range along with the details related to these actions.

### Parameters

You can filter an Application Deployment Activity using any combination of the following:

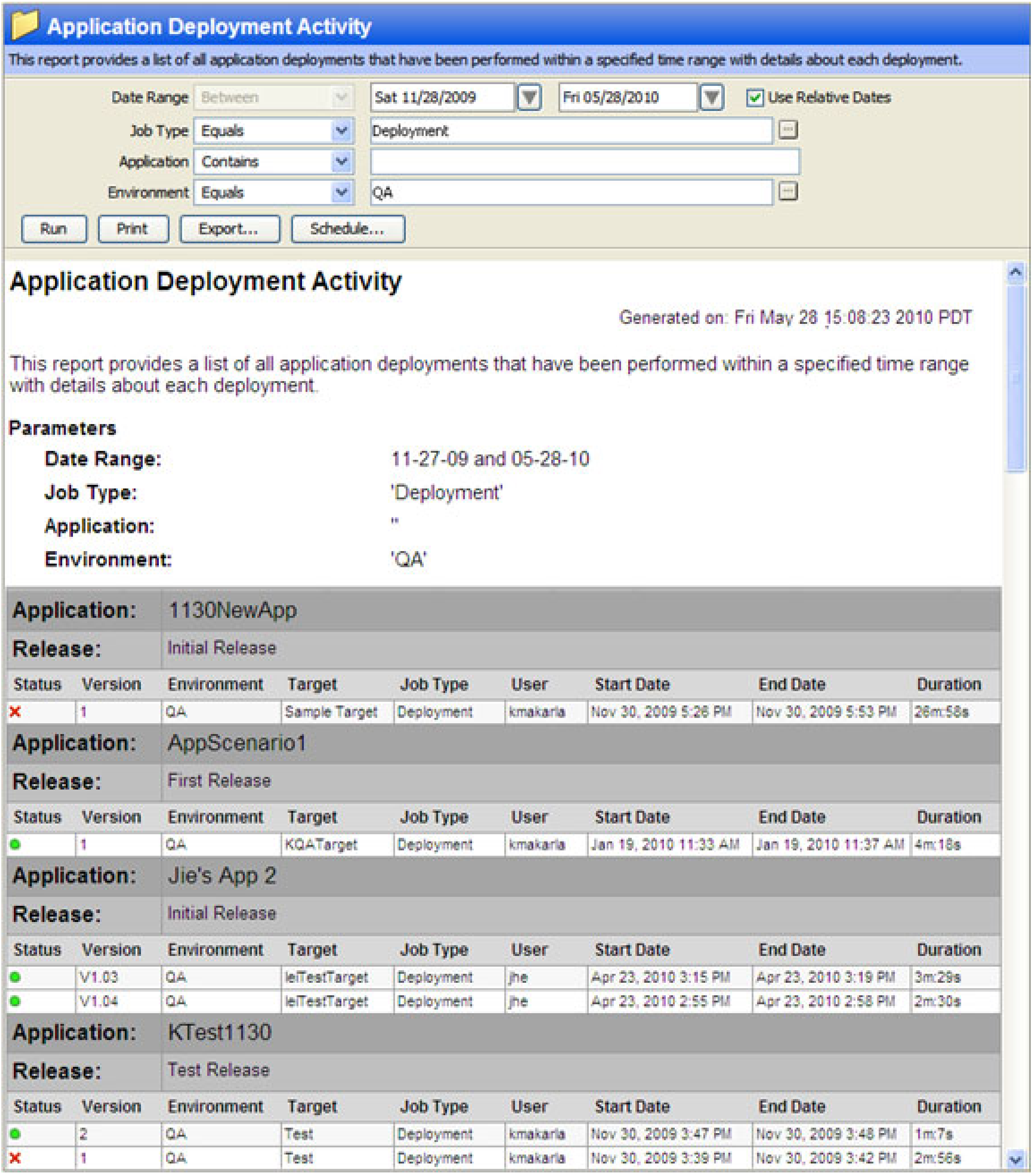
- **Date Range**: Range of dates during which the Application Deployment activities were performed.
- **Job Type**: Deployment, undeployment, or rollback.
- **Application**: Specific application (or applications) deployed.
- **Environment**: Application Deployment environment, such as QA or Production. The Application Deployment environments are mirrored as SA device groups.

### Table

- The report is grouped by Application and subgrouped by releases of that Application.
- Each row in the report describes an action, which can be a deployment, an undeployment, or a rollback.
- The Status column indicates whether the action succeeded or failed.
- The Version column shows the version of the application/release that was deployed, undeployed, or rolled back.
- The Environment column indicates which environment the application was deployed to, undeployed from, or rolled back from.
- The Target column shows the target of the action. A target is a group of one or more servers to which the application is deployed to, undeployed from, or rolled back from.
- The Job Type column indicates whether the action was a deployment, an undeployment, or a rollback.

- The User column shows the HP SA login ID of the user who initiated the operation.
- The Start Date and End Date columns show when the job started and when it completed.
- The Duration column gives the total elapsed time for the job.

**Figure 8 Application Deployment Activity Report**



This report provides a list of all application deployments that have been performed within a specified time range with details about each deployment.

| | | | |
|---|---|---|---|
| Date Range | Between | Sat 11/28/2009 | Fri 05/28/2010 ☑ Use Relative Dates |
| Job Type | Equals | Deployment | |
| Application | Contains | | |
| Environment | Equals | QA | |

Application Deployment Activity

Generated on: Fri May 28 15:08:23 2010 PDT

This report provides a list of all application deployments that have been performed within a specified time range with details about each deployment.

Parameters

| | |
|---|---|
| Date Range: | 11-27-09 and 05-28-10 |
| Job Type: | 'Deployment' |
| Application: | '' |
| Environment: | 'QA' |

Application: 1130NewApp

Release: Initial Release

| Status | Version | Environment | Target | Job Type | User | Start Date | End Date | Duration |
|---|---|---|---|---|---|---|---|---|
| ✗ | 1 | QA | Sample Target | Deployment | kmakarla | Nov 30, 2009 5:26 PM | Nov 30, 2009 5:53 PM | 26m:58s |

Application: AppScenario1

Release: First Release

| Status | Version | Environment | Target | Job Type | User | Start Date | End Date | Duration |
|---|---|---|---|---|---|---|---|---|
| ● | 1 | QA | KQATarget | Deployment | kmakarla | Jan 19, 2010 11:33 AM | Jan 19, 2010 11:37 AM | 4m:18s |

Application: Jie's App 2

Release: Initial Release

| Status | Version | Environment | Target | Job Type | User | Start Date | End Date | Duration |
|---|---|---|---|---|---|---|---|---|
| ● | V1.03 | QA | leTestTarget | Deployment | jhe | Apr 23, 2010 3:15 PM | Apr 23, 2010 3:19 PM | 3m:29s |
| ● | V1.04 | QA | leTestTarget | Deployment | jhe | Apr 23, 2010 2:55 PM | Apr 23, 2010 2:58 PM | 2m:30s |

Application: KTest1130

Release: Test Release

| Status | Version | Environment | Target | Job Type | User | Start Date | End Date | Duration |
|---|---|---|---|---|---|---|---|---|
| ● | 2 | QA | Test | Deployment | kmakarla | Nov 30, 2009 3:47 PM | Nov 30, 2009 3:48 PM | 1m:7s |
| ✗ | 1 | QA | Test | Deployment | kmakarla | Nov 30, 2009 3:39 PM | Nov 30, 2009 3:42 PM | 2m:56s |

## Getting More Details

Further drill-down is not available in this report.

# ROI Reports

The ROI reports enable you to see the Return On Investment (ROI) that you are realizing by using Application Deployment. You can generate a report grouped by Application or by Environment.

You can assign an ROI value (per target machine) to a release in the Application Deployment Manager. The ROI for an application is the sum of this ROI value for all targets to which any release of this application has been successfully deployed.

## Parameters for ROI by Application

You can filter an ROI by Application report using any combination of the following:

- **Date**: End-date for the 12-month period for which ROI is reported.
- **Application**: Specific application (or applications) deployed.

## Parameters for ROI by Environment

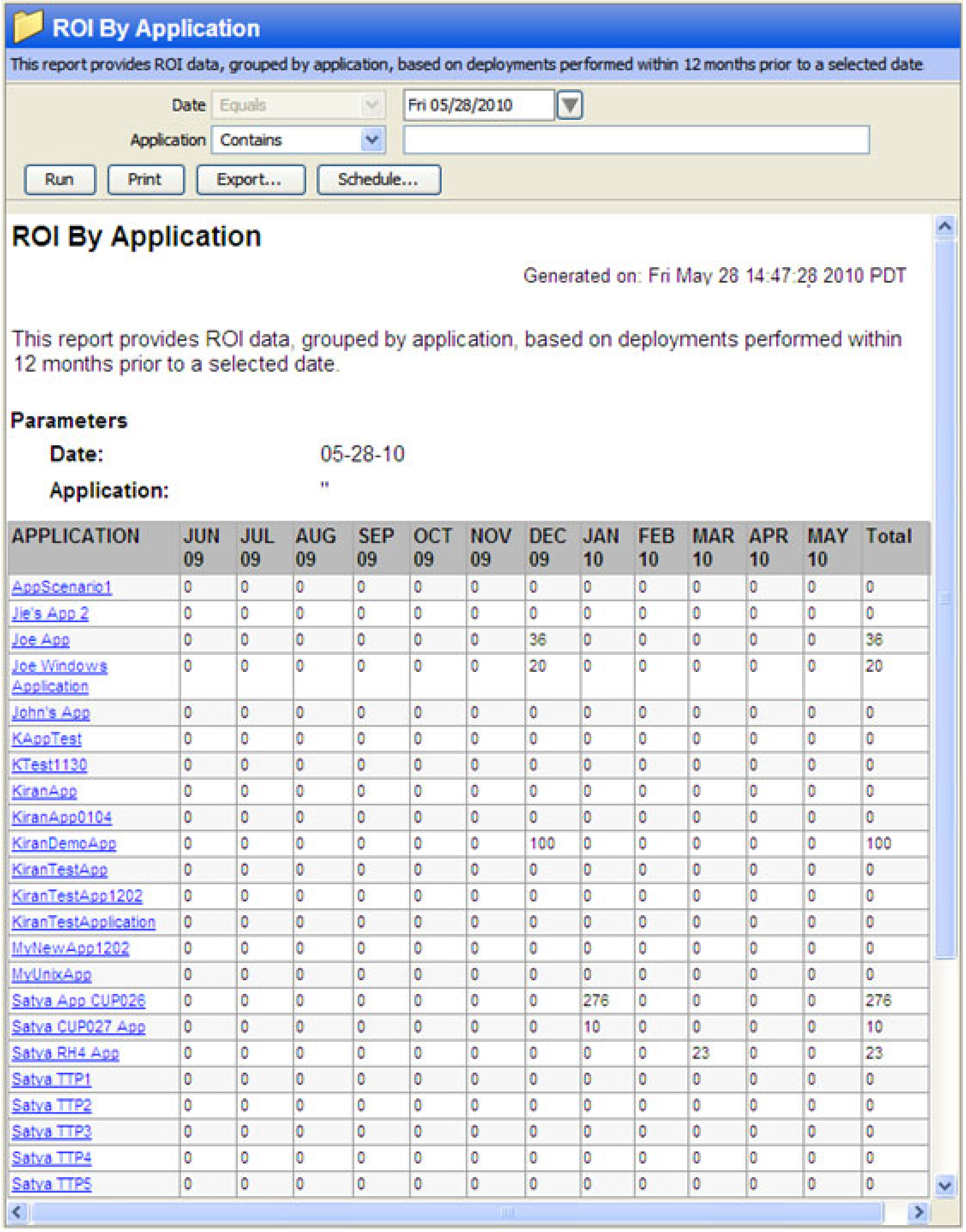
You can filter an ROI by Environment report using any combination of the following:

- **Date**: End-date for the 12-month period for which ROI is reported.
- **Environment**: Application Deployment environment, such as QA or Production. The Application Deployment environments are mirrored as SA device groups.

## Tables

Each row in the table describes the ROI realized during each month of the specified time period, and a total ROI for the entire period.

**Figure 9 Application Deployment ROI by Application Report**



This report provides ROI data, grouped by application, based on deployments performed within 12 months prior to a selected date

Date: Equals — Fri 05/28/2010

Application: Contains

## ROI By Application

Generated on: Fri May 28 14:47:28 2010 PDT

This report provides ROI data, grouped by application, based on deployments performed within 12 months prior to a selected date.

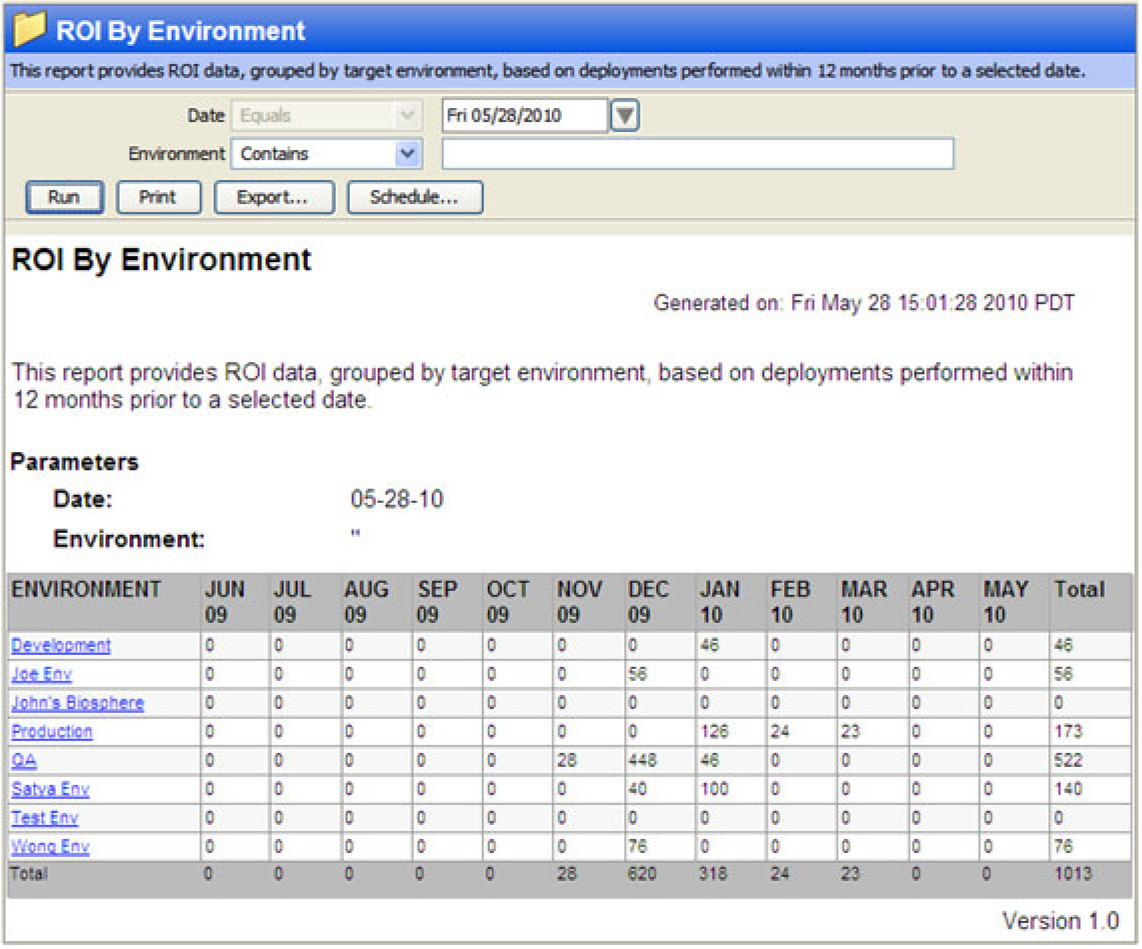
**Parameters**

**Date:** 05-28-10

**Application:** ''

| 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 |

**Figure 10 Application Deployment ROI by Environment Report**



ROI By Environment
This report provides ROI data, grouped by target environment, based on deployments performed within 12 months prior to a selected date.
Date
Equals
Fri 05/28/2010
Environment
Contains
Run
Print
Export...
Schedule...

ROI By Environment

Generated on: Fri May 28 15:01:28 2010 PDT

This report provides ROI data, grouped by target environment, based on deployments performed within 12 months prior to a selected date.

Parameters

Date: 05-28-10

Environment: ''

| 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 |

Version 1.0

## Getting More Details

- Click an Application name in the ROI by Application report to drill-down to the Application Deployment Activity report for that Application.
- Click an Environment name in the ROI by Environment report to drill-down to the Application Deployment Activity report for that Environment.

## Deployment Success Reports

These reports enable you to view data that describes how often Application Deployments succeed. For each month in the selected date range, the report shows you the number of deployment jobs that were attempted and the number that were successful. The report also represents this information as a percentage for each month in the selected date range. Undeployment and rollback jobs are not included in the calculations.

### Parameters for Deployment Success by Application

You can filter a Deployment Success by Application report using any combination of the following:

- **Date**: End-date for the 12-month period for which the data is reported.
- **Application**: Specific application (or applications) deployed.
- **Threshold (%)**: Success rate is shown in red if lower than this threshold.

### Parameters for Deployment Success by Environment

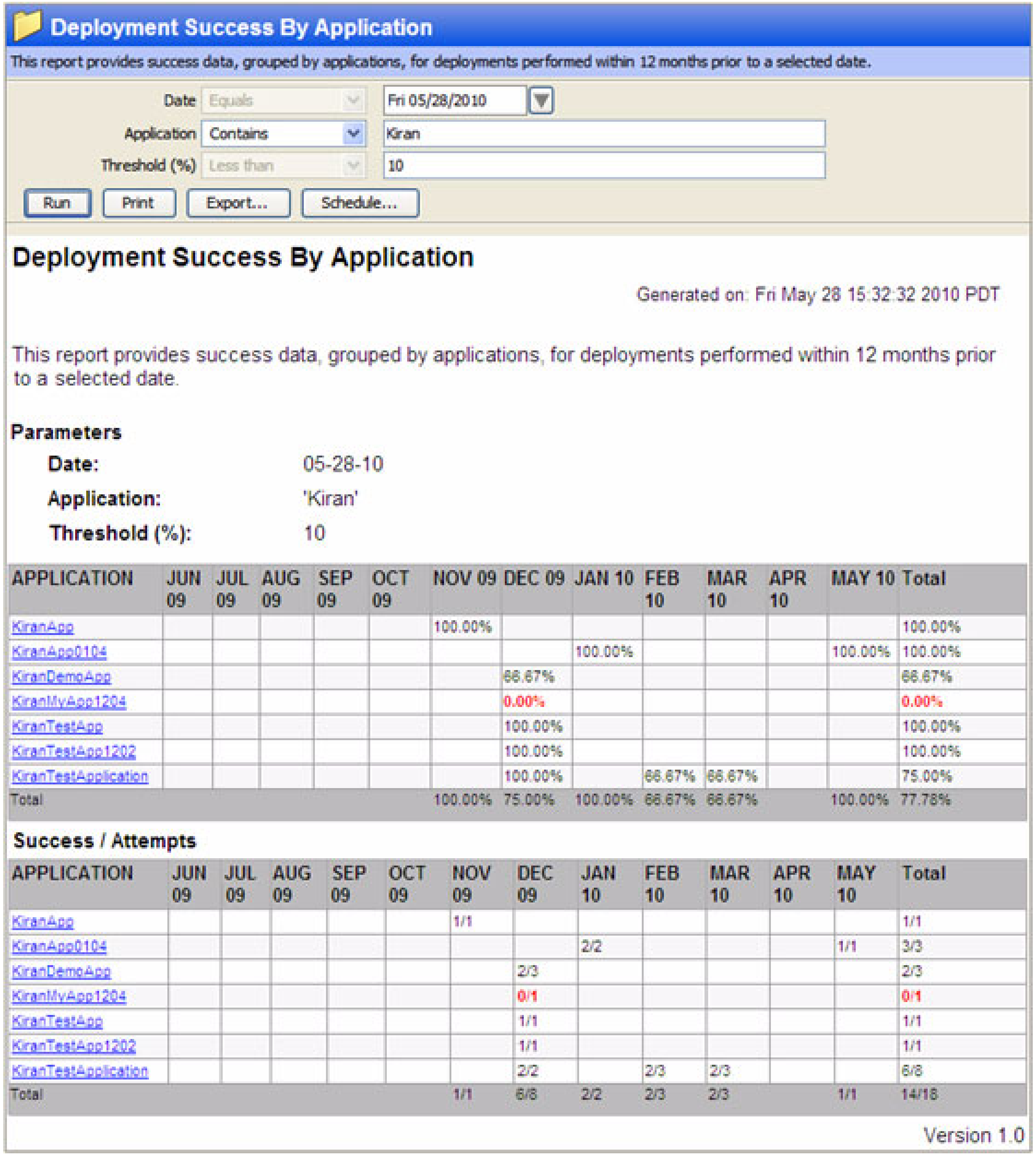
You can filter a Deployment Success by Environment report using any combination of the following:

- **Date**: End-date for the 12-month period for which the data is reported.
- **Environment**: Application Deployment environment, such as QA or Production. The Application Deployment environments are mirrored as SA device groups.
- **Threshold (%)**: Success rate is shown in red if lower than this threshold.

### Table

Each row in the table describes the success data for an Environment or an Application. The success data is reported for each month in the 12-month window prior to the Date specified and for the entire period

**Figure 11 Deployment Success by Application Report**



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

## 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 |

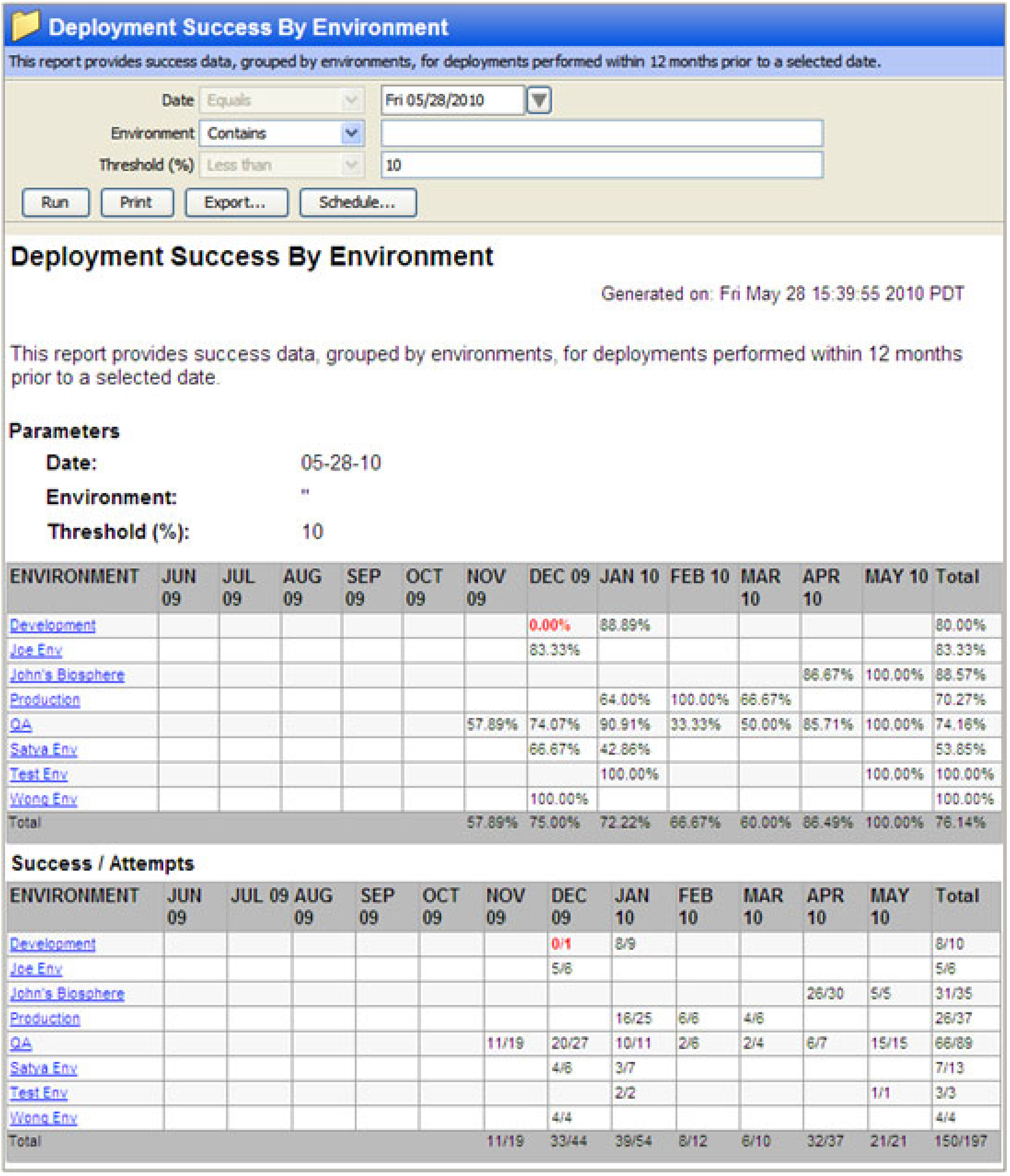
| APPLICATION | JUN 09 | JUL 09 | AUG 09 | SEP 09 | OCT 09 | NOV 09 | DEC 09 | JAN 10 | FEB 10 | MAR 10 | APR 10 | MAY 10 | Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| KiranApp | | | | | | 100.00% | | | | | | | 100.00% |
| KiranApp0104 | | | | | | | | 100.00% | | | | 100.00% | 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

**Figure 12 Deployment Success by Environment Report**



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 |

## 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 |

## Getting More Details

- Click an Application name in the Deployment Success by Application report to drill-down to the Application Deployment Activity report for that Application.
- Click an Environment name in the Deployment Success by Environment report to drill-down to the Application Deployment Activity report for that Environment.

## Time to Production Reports

The Time To Production reports enable you to see how long it takes for your applications to work their way through the application lifecycle. For each release of an application, the report shows how long it took for the application to reach the last stage in the application lifecycle (typically the Production environment).

The time to production for a given release is calculated as the time from the creation of the first version of a release to the time when the application is first deployed successfully into the final stage of the lifecycle. If the application is rolled back from the last lifecycle stage, then the application is not considered to have been successfully deployed.

### Parameters

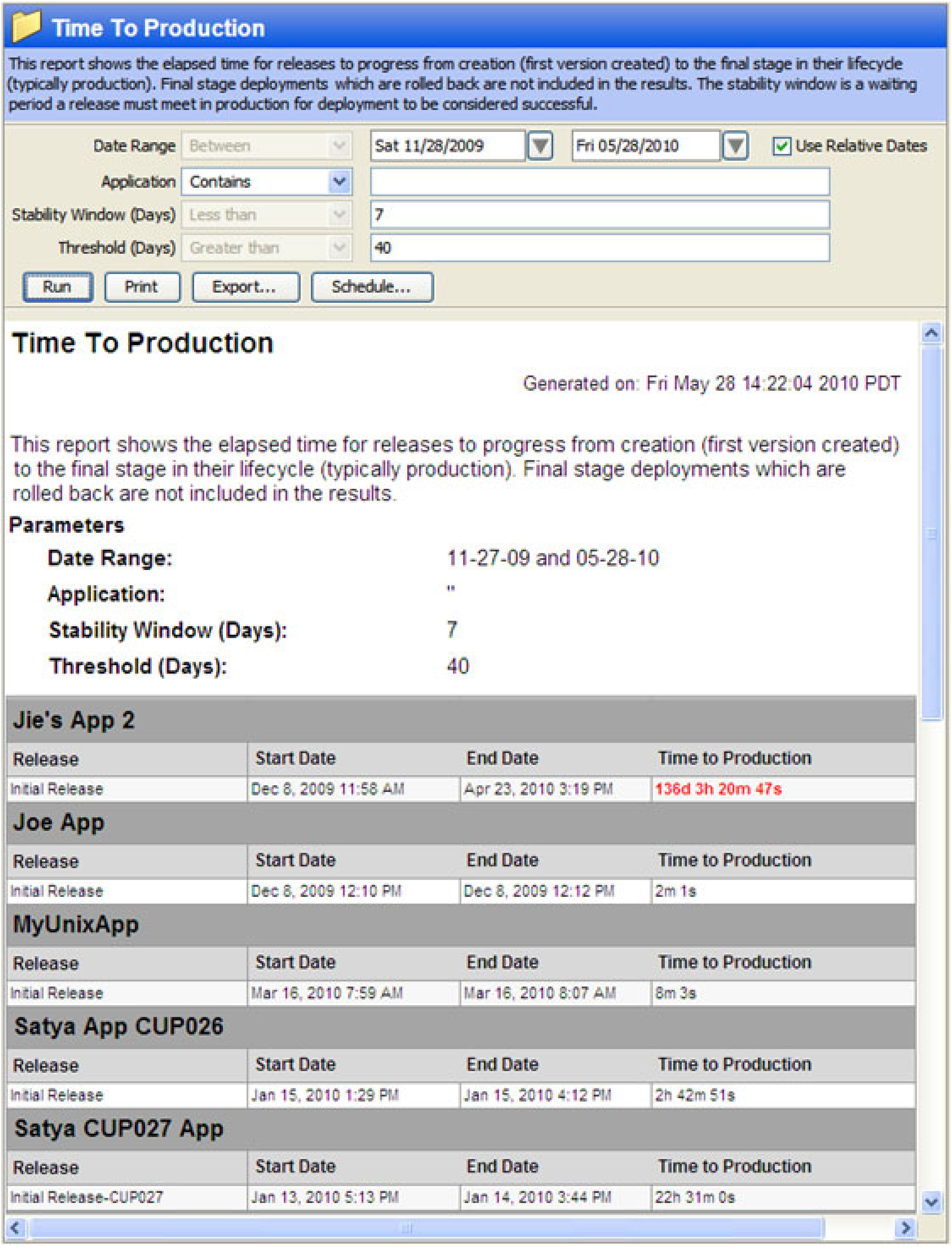
You can filter a Time to Production report by any combination of the following parameters:

- **Date Range**: Range of dates during which all applications that were successfully deployed to the Production environment will be counted.
- **Application**: Specific application (or applications) deployed.
- **Stability Window (Days)**: Number of days that the application must remain deployed in the final environment in the lifecycle (typically Production) in order to be considered a successful release. If the application is rolled back within this window, the release is not considered to be "in production."
- **Threshold (Days)**: Time to production is shown in red if greater than this threshold. In other words, applications that took longer than this number of days to reach Production are shown in red.

### Table

The report is grouped by Application and subgrouped by release.

**Figure 13 Time To Production Report**



This report shows the elapsed time for releases to progress from creation (first version created) to the final stage in their lifecycle (typically production). Final stage deployments which are rolled back are not included in the results. The stability window is a waiting period a release must meet in production for deployment to be considered successful.

Date Range: Between | Sat 11/28/2009 | Fri 05/28/2010 | ☑ Use Relative Dates

Application: Contains |

Stability Window (Days): Less than | 7

Threshold (Days): Greater than | 40

Time To Production

Generated on: Fri May 28 14:22:04 2010 PDT

This report shows the elapsed time for releases to progress from creation (first version created) to the final stage in their lifecycle (typically production). Final stage deployments which are rolled back are not included in the results.

Parameters

| | |
|---|---|
| Date Range: | 11-27-09 and 05-28-10 |
| Application: | '' |
| Stability Window (Days): | 7 |
| Threshold (Days): | 40 |

Jie's App 2

| Release | Start Date | End Date | Time to Production |
|---|---|---|---|
| Initial Release | Dec 8, 2009 11:58 AM | Apr 23, 2010 3:19 PM | 136d 3h 20m 47s |

Joe App

| Release | Start Date | End Date | Time to Production |
|---|---|---|---|
| Initial Release | Dec 8, 2009 12:10 PM | Dec 8, 2009 12:12 PM | 2m 1s |

MyUnixApp

| Release | Start Date | End Date | Time to Production |
|---|---|---|---|
| Initial Release | Mar 16, 2010 7:59 AM | Mar 16, 2010 8:07 AM | 8m 3s |

Satya App CUP026

| Release | Start Date | End Date | Time to Production |
|---|---|---|---|
| Initial Release | Jan 15, 2010 1:29 PM | Jan 15, 2010 4:12 PM | 2h 42m 51s |

Satya CUP027 App

| Release | Start Date | End Date | Time to Production |
|---|---|---|---|
| Initial Release-CUP027 | Jan 13, 2010 5:13 PM | Jan 14, 2010 3:44 PM | 22h 31m 0s |

## Getting More Details

There is no drill-down available in this report.

# 2 Server Automation Compliance Reports

This section described the current set of Server Automation (SA) compliance reports.

## Summary of Compliance by Policy

### Graph

- The unit on the y-axis is the sum of server compliance status counts with respect to policy/ policy instances attached for each policy type.
- The counts are not a count of unique servers attached across all policies. For example, a server could be attached to more than one policy and that server could be non-compliant for each of the policy and thus will be counted multiple times.
- The x-axis is categorized by policy type.

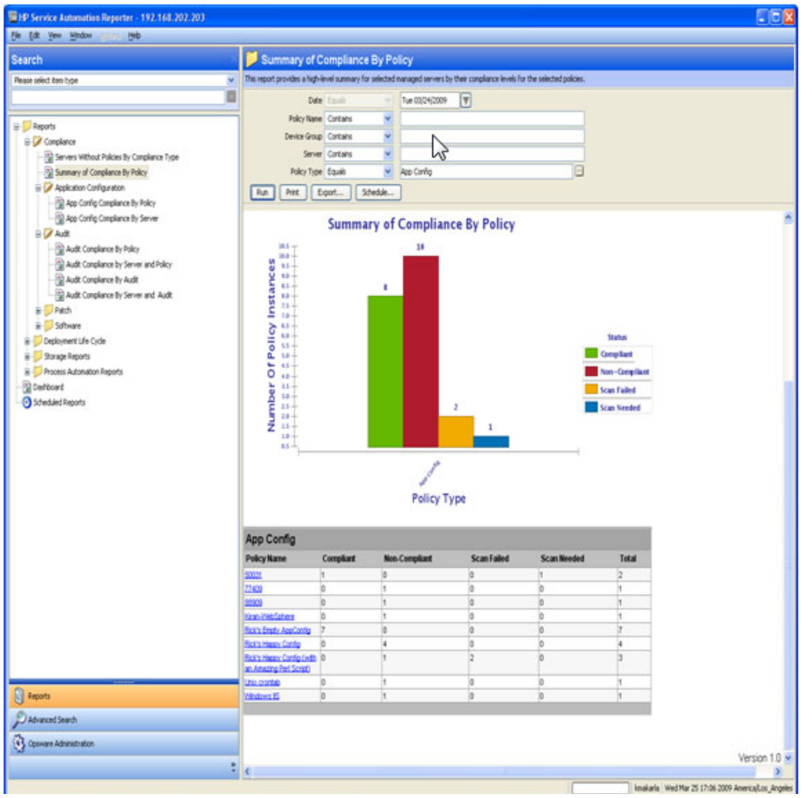
### Table

- Policies are grouped by policy type, with the name of each policy listed.
- A policy name can be a duplicate across policy types. For example, an audit policy can have the name 'P1' and similarly, a software policy can have the name 'P1'.
- A policy cannot have duplicate name within a policy type.
- The value in the 'Total' column represents total numbers of unique servers that are attached to individual policies with exception of 'Application Configuration' instance, where a single server can have multiple instances of same 'Application Configuration'.
- Counts reflect current managed/active servers only.

### Drill-Down

- Click the policy name in the report to drill-down to its full details report. This allows you to see a breakdown of selected policy and items with in by their compliance status, for each of the servers to which the policy is attached.
- Report parameter selection criteria's are maintained and would be propagated & applied to the drill-down report for the selected policy name.
- Drill-down report is displayed with-in the context and frame of the 'Summary Report', allowing user to navigate back.

## Figure 1    Summary of Compliance By Policy



HP Service Automation Reporter - 192.168.202.203
File Edit View Window Help
Search
Please select item type
Reports
Compliance
Servers Without Policies By Compliance Type
Summary of Compliance By Policy
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Audit Compliance By Policy
Audit Compliance by Server and Policy
Audit Compliance By Audit
Audit Compliance By Server and Audit
Patch
Software
Deployment Life Cycle
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Summary of Compliance By Policy

This report provides a high-level summary for selected managed servers by their compliance levels for the selected policies.

| | | |
|---|---|---|
| Date | Equals | Tue 03/24/2009 |
| Policy Name | Contains | |
| Device Group | Contains | |
| Server | Contains | |
| Policy Type | Equals | App Config |

Run
Print
Export...
Schedule...
Summary of Compliance By Policy
Number Of Policy Instances
10.5
10.0
9.5
9.0
8.5
8.0
7.5
7.0
6.5
6.0
5.5
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
8
10
2
1
App Config
Policy Type
Status
🟩 Compliant
🟥 Non-Compliant
🟨 Scan Failed
🟦 Scan Needed

App Config

| Policy Name | Compliant | Non-Compliant | Scan Failed | Scan Needed | Total |
|---|---|---|---|---|---|
| 50011 | 1 | 0 | 0 | 1 | 2 |
| 77400 | 0 | 1 | 0 | 0 | 1 |
| 99909 | 0 | 1 | 0 | 0 | 1 |
| Kiran-WebSphere | 0 | 1 | 0 | 0 | 1 |
| Rick's Empty AppConfig | 7 | 0 | 0 | 0 | 7 |
| Rick's Happy Config | 0 | 4 | 0 | 0 | 4 |
| Rick's Happy Config (with an Amazing Perl Script) | 0 | 1 | 2 | 0 | 3 |
| Unix crontab | 0 | 1 | 0 | 0 | 1 |
| Windows IIS | 0 | 1 | 0 | 0 | 1 |

# Summary of Compliance by Server

## Graph

- The unit on the y-axis is number of servers that a given policy is attached to. Count is the sum of policy compliance status for each of the policies that are attached to a server by their policy type.
- The counts are not a count of unique policy instances that are attached to the servers. For example, a policy could be attached to more than one server and that policy could be non-compliant for more than that one and thus will be counted multiple times.
- The x-axis is categorized by policy type.

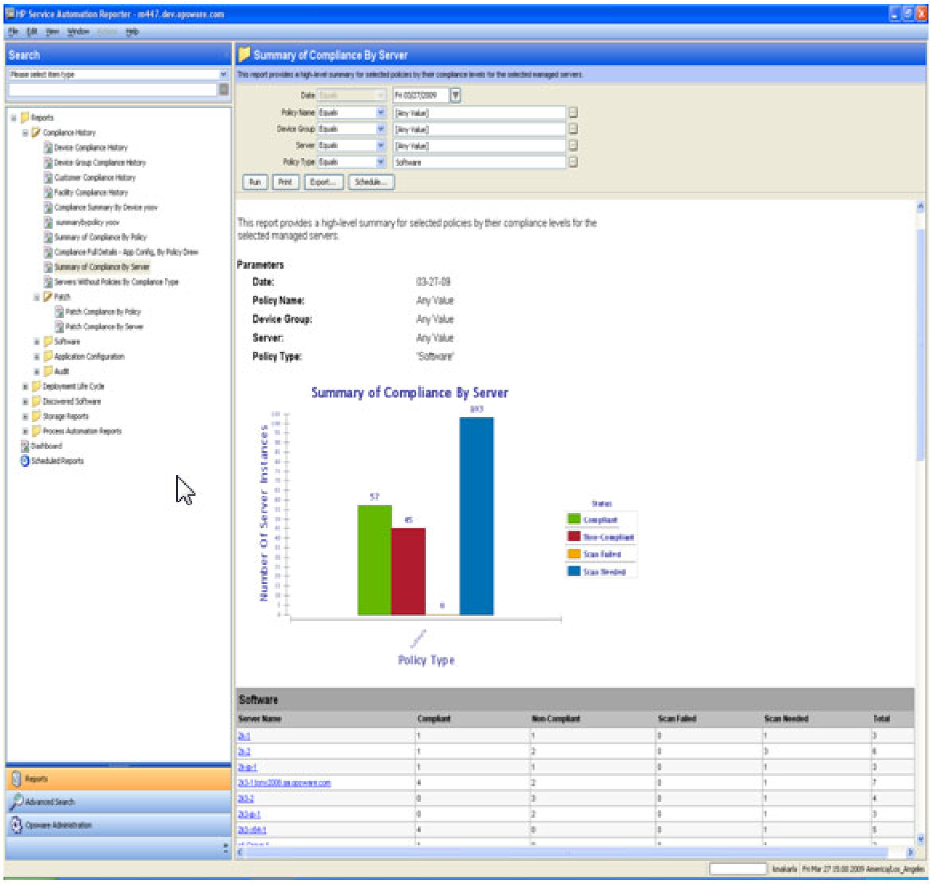
## Table

- The value in the 'Total' column represents total numbers of unique policies instances that are attached to a given server.
- Servers are grouped by the types of policies that are being attached i.e. policy type, with the name of each server listed.
- Server Name cannot be duplicate within a policy type.
- Server name can be repeated across policy types. For example, a server S1 can be attached to an audit Policy 'A1' and software policy 'SP1', S1 would be listed both under audit policy type as well as software policy type.
- Counts reflect current managed/active servers only.

## Drill-Down

- Click the server name in the report to drill-down to its full details report. This allows you to see a breakdown of selected server by its compliance status for each of the policies and items with in the policies that attached.
- Report parameter selection criteria's are maintained and would be propagated & applied to the drill-down report for the selected server name.
- Drill-down report is displayed with-in the context and frame of the 'Summary Report', allowing user to navigate back.

**Figure 2 Summary of Compliance By Server**


HP Service Automation Reporter - m447.dev.opsware.com
File Edit View Window Actions Help
Search
Please select item type
Reports
Compliance History
Device Compliance History
Device Group Compliance History
Customer Compliance History
Facility Compliance History
Compliance Summary By Device yoov
summaryBypolicy yoov
Summary of Compliance By Policy
Compliance Full Details - App Config, By Policy Drew
Summary of Compliance By Server
Servers Without Policies By Compliance Type
Patch
Patch Compliance By Policy
Patch Compliance By Server
Software
Application Configuration
Audit
Deployment Life Cycle
Discovered Software
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Summary of Compliance By Server
Run
Print
Export...
Schedule...
Summary of Compliance By Server
Number Of Server Instances
57
45
0
103
Software
Policy Type
Status
🟩 Compliant
🟥 Non-Compliant
🟧 Scan Failed
🟦 Scan Needed
lmakarla
Fri Mar 27 15:00 2009 America/Los_Angeles

This report provides a high-level summary for selected policies by their compliance levels for the selected managed servers.

Date: Equals Fri 03/27/2009
Policy Name: Equals [Any Value]
Device Group: Equals [Any Value]
Server: Equals [Any Value]
Policy Type: Equals Software

This report provides a high-level summary for selected policies by their compliance levels for the selected managed servers.

**Parameters**

| | |
|---|---|
| **Date:** | 03-27-09 |
| **Policy Name:** | Any Value |
| **Device Group:** | Any Value |
| **Server:** | Any Value |
| **Policy Type:** | 'Software' |

**Software**

| Server Name | Compliant | Non Compliant | Scan Failed | Scan Needed | Total |
|---|---|---|---|---|---|
| 2k-1 | 1 | 1 | 0 | 1 | 3 |
| 2k-2 | 1 | 2 | 0 | 3 | 6 |
| 2k-gs-1 | 1 | 1 | 0 | 1 | 3 |
| 2k3-1.bmo2008.qa.opsware.com | 4 | 2 | 0 | 1 | 7 |
| 2k3-2 | 0 | 3 | 0 | 1 | 4 |
| 2k3-gs-1 | 0 | 2 | 0 | 1 | 3 |
| 2k3-sfe-1 | 4 | 0 | 0 | 1 | 5 |

# Software Compliance by Policy

## Summary

- Compliant Policies: Count of compliant selected policies / Total number of selected policies that are attached to the servers.
- Compliant Items: Count of unique compliant items across all selected policies / Total number of unique items across all selected policies that are attached to the servers.
- Compliant Severs: Count of unique compliant servers / Total number of unique servers.
- Counts reflect current managed/active servers only.

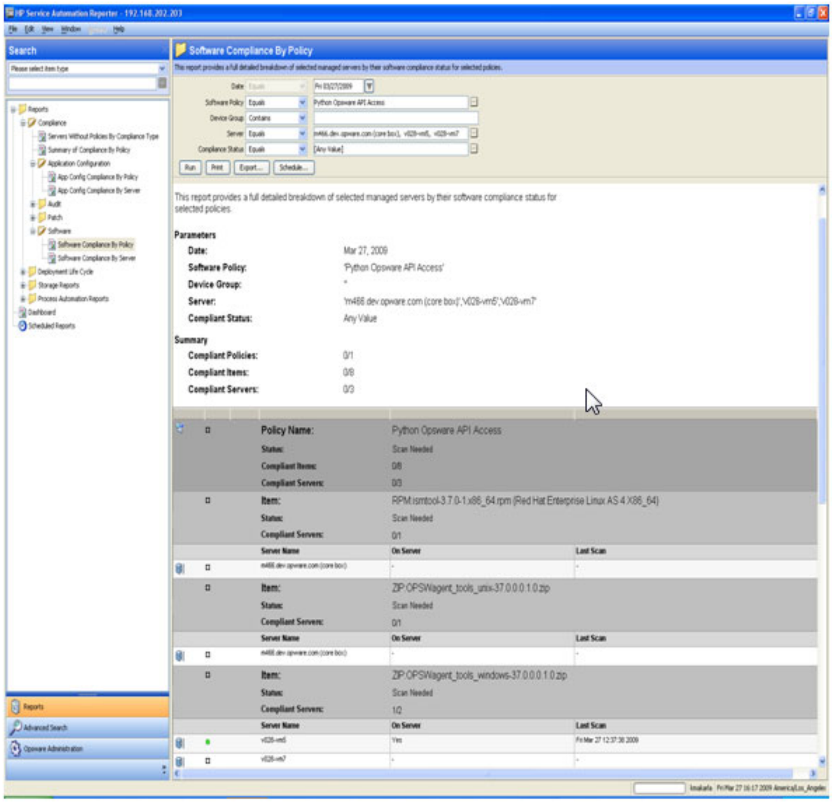
## Table

- A software policy can be attached to either a device group or directly to a server. When a policy is attached to device group, only servers with matching platform are reported
- Table is primarily grouped by policies. Each policy has compliance counts for each of its items and servers that are attached to it.
- Each Item is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Software Policy P1, has item, Item1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Item1 is non-compliant. Since Item1 is part of software policy P1, P1 is also non-compliant with respect to server.
- Software policies that have SMO (Server Module Objects) as items are not reported.
- Item Name will be displayed as a combination of concrete Item Type for unit, such as ZIP, MSI, RPM etc, and AppConfig_Instance for Application Configuration instances, along with their names.
- When a required / mandated software item exists on a server is considered to be compliant; however, a required item version may not exist on a server but is considered compliant, when a newer RPM version is installed on the server, and older version is listed in the model. This aberration is marked with '*' next to the server and a footnote for the same is provided in the report.
- A server is considered 'compliant' even if the policy that is attached to it is empty. However, no item information is displayed as there are no details to report on. Similarly, 'On Server' field is marked 'Unknown' for lack of details.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 3 Software Compliance By Policy**



HP Service Automation Reporter - 192.168.202.203
File Edit View Window Help
Search
Please select item type
Reports
Compliance
Servers Without Policies By Compliance Type
Summary of Compliance By Policy
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Patch
Software
Software Compliance By Policy
Software Compliance By Server
Deployment Life Cycle
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Software Compliance By Policy
Run
Print
Export...
Schedule...

This report provides a full detailed breakdown of selected managed servers by their software compliance status for selected policies.

| | | |
|---|---|---|
| Date | Equals | Fri 03/27/2009 |
| Software Policy | Equals | Python Opsware API Access |
| Device Group | Contains | |
| Server | Equals | m466.dev.opsware.com (core box), v028-vm6, v028-vm7 |
| Compliance Status | Equals | [Any Value] |

This report provides a full detailed breakdown of selected managed servers by their software compliance status for selected policies.

**Parameters**

| | |
|---|---|
| **Date:** | Mar 27, 2009 |
| **Software Policy:** | 'Python Opsware API Access' |
| **Device Group:** | * |
| **Server:** | 'm466.dev.opsware.com (core box)','V028-vm6','V028-vm7' |
| **Compliant Status:** | Any Value |

**Summary**

| | |
|---|---|
| **Compliant Policies:** | 0/1 |
| **Compliant Items:** | 0/8 |
| **Compliant Servers:** | 0/3 |

| | | | |
|---|---|---|---|
| □ | **Policy Name:** | Python Opsware API Access | |
| | **Status:** | Scan Needed | |
| | **Compliant Items:** | 0/8 | |
| | **Compliant Servers:** | 0/3 | |
| □ | **Item:** | RPM:ismtool-3.7.0-1.x86_64.rpm (Red Hat Enterprise Linux AS 4 X86_64) | |
| | **Status:** | Scan Needed | |
| | **Compliant Servers:** | 0/1 | |
| | **Server Name** | **On Server** | **Last Scan** |
| □ | m466.dev.opsware.com (core box) | - | - |
| □ | **Item:** | ZIP:OPSWagent_tools_unix-37.0.0.0.1.0.zip | |
| | **Status:** | Scan Needed | |
| | **Compliant Servers:** | 0/1 | |
| | **Server Name** | **On Server** | **Last Scan** |
| □ | m466.dev.opsware.com (core box) | - | - |
| □ | **Item:** | ZIP:OPSWagent_tools_windows-37.0.0.0.1.0.zip | |
| | **Status:** | Scan Needed | |
| | **Compliant Servers:** | 1/2 | |
| | **Server Name** | **On Server** | **Last Scan** |
| ● | v028-vm6 | Yes | Fri Mar 27 12:37:38 2009 |
| □ | v028-vm7 | - | - |

# Software Compliance by Server

## Summary

- Compliant: Total number of compliant servers.
- Non-Compliant: Total number of non-complaint servers. A server is considered to be non compliant when one or more of the policies or items with in those policies that are attached to are non-compliant.
- Scan Needed:  Total number of servers that are in need of scan. A server is in scan needed state when one of more of the policies that are attached to has been modified and in order to determine the server compliance, the server needs to be scanned.
- Counts reflect current managed/active servers only.

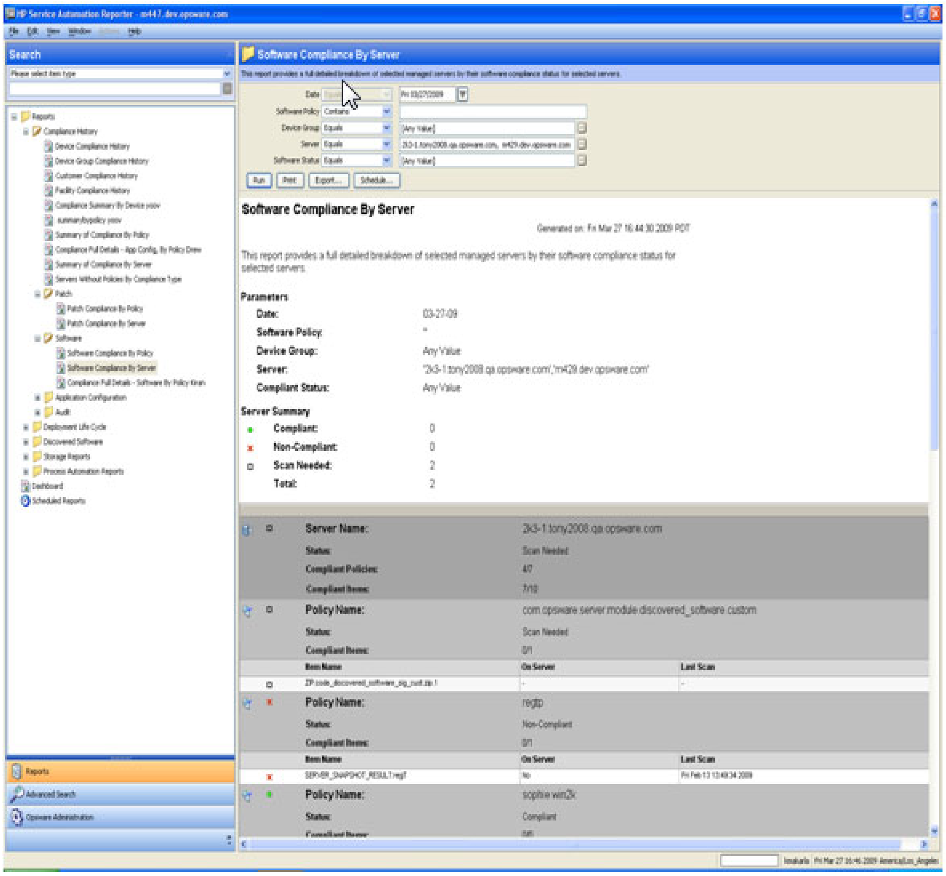
## Table

- A software policy can be attached to either a device group or directly to a server. When a policy is attached to device group, only servers with matching platform are reported.
- Table is primarily grouped by servers. Each server has compliance counts on each of the software policies that are attached.
- Each Item is further grouped with in a policy to give granular compliance details at this level. Server compliance status is rolled-up or bubbled up from this level. For example, Software Policy P1, has item, Item1 and is compliant for server S1, similarly another software policy P2, has item, Item2 and is non-compliant on server S1. Net server compliance status is non-compliant because Policy 1 is compliant, where as Policy 2 is non-compliant.
- Software policies that have SMO (Server Module Objects) as items are not reported.
- Item Name will be displayed as a combination of concrete Item Type for unit, such as ZIP, MSI, RPM etc, and AppConfig_Instance for Application Configuration instances, along with their names.
- When a required / mandated software item exists on a server is considered to be compliant; however, a required item version may not exist on a server but is considered compliant, when a newer RPM version is installed on the server, and older version is listed in the model. This aberration is marked with '*' next to the server and a footnote for the same is provided in the report.
- A server is considered 'compliant' even if the policy that is attached to it is empty. However, no item information is displayed as there are no details to report on. Similarly, 'On Server' field is marked 'Unknown' for lack of details.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 4 Software Compliance By Server**


HP Service Automation Reporter - m447.dev.opsware.com
File
Edit
View
Window
Actions
Help
Search
Please select item type
Reports
Compliance History
Device Compliance History
Device Group Compliance History
Customer Compliance History
Facility Compliance History
Compliance Summary By Device yoov
summarybypolicy yoov
Summary of Compliance By Policy
Compliance Full Details - App Config, By Policy Drew
Summary of Compliance By Server
Servers Without Policies By Compliance Type
Patch
Patch Compliance By Policy
Patch Compliance By Server
Software
Software Compliance By Policy
Software Compliance By Server
Compliance Full Details - Software By Policy Kiran
Application Configuration
Audit
Deployment Life Cycle
Discovered Software
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Software Compliance By Server
Run
Print
Export...
Schedule...
lesakarla
Fri Mar 27 16:46 2009 America/Los_Angeles

This report provides a full detailed breakdown of selected managed servers by their software compliance status for selected servers.

| | | |
|---|---|---|
| Date | Equals | Fri 03/27/2009 |
| Software Policy | Contains | |
| Device Group | Equals | [Any Value] |
| Server | Equals | 2k3-1.tony2008.qa.opsware.com, m429.dev.opsware.com |
| Software Status | Equals | [Any Value] |

## Software Compliance By Server

Generated on: Fri Mar 27 16:44:30 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their software compliance status for selected servers.

**Parameters**

| | |
|---|---|
| **Date:** | 03-27-09 |
| **Software Policy:** | * |
| **Device Group:** | Any Value |
| **Server:** | '2k3-1.tony2008.qa.opsware.com','m429.dev.opsware.com' |
| **Compliant Status:** | Any Value |

**Server Summary**

| | | |
|---|---|---|
| ● | **Compliant:** | 0 |
| ✗ | **Non-Compliant:** | 0 |
| □ | **Scan Needed:** | 2 |
| | **Total:** | 2 |

| | | |
|---|---|---|
| □ | **Server Name:** | 2k3-1.tony2008.qa.opsware.com |
| | **Status:** | Scan Needed |
| | **Compliant Policies:** | 4/7 |
| | **Compliant Items:** | 7/10 |
| □ | **Policy Name:** | com.opsware.server.module.discovered_software.custom |
| | **Status:** | Scan Needed |
| | **Compliant Items:** | 0/1 |

| | Item Name | On Server | Last Scan |
|---|---|---|---|
| □ | ZIP.code_discovered_software_zip_cust.zip.1 | - | - |

| | | |
|---|---|---|
| ✗ | **Policy Name:** | regtp |
| | **Status:** | Non-Compliant |
| | **Compliant Items:** | 0/1 |

| | Item Name | On Server | Last Scan |
|---|---|---|---|
| ✗ | SERVER_SNAPSHOT_RESULT.regf | No | Fri Feb 13 13:48:34 2009 |

| | | |
|---|---|---|
| ● | **Policy Name:** | sophie win2k |
| | **Status:** | Compliant |
| | **Compliant Items:** | 0/0 |

# App Config Compliance by Policy

## Summary

- Compliant Policies: Count of compliant selected policies / Total number of selected policies that are attached to the servers.
- Compliant Config Items: Count of unique compliant configuration items across all selected policies / Total number of unique configuration items across all selected policies that are attached to the servers.
- Compliant Severs: Count of unique compliant servers / Total number of unique servers.
- Counts reflect current managed/active servers only.

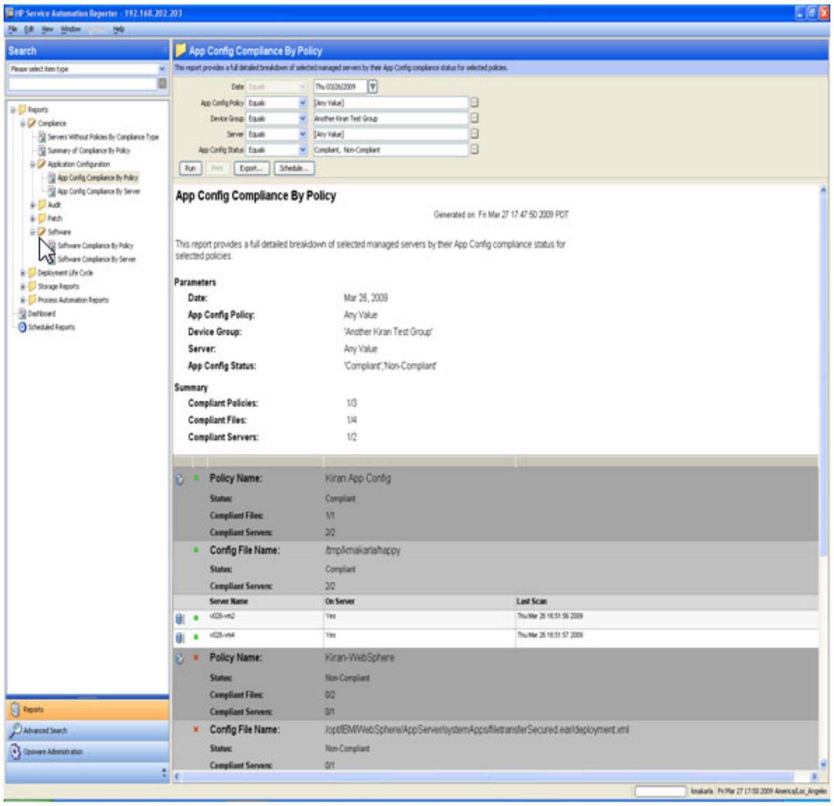
## Table

- An application configuration policy can be attached to either a device group or directly to a server. When a policy is attached to device group, a scan is needed in order for the system to recognize the server / policy attachment. Also, only servers with matching platform are reported
- Table is primarily grouped by policies. Each policy has compliance counts for each of its items and servers that are attached to it.
- Each Item is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, App Config Policy P1 is attached to Server S1 & Server 2. Policy P1 has item, Item1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Item1 is non-compliant. Since Item1 is part of policy P1, P1 is also non-compliant with respect to Server S1 & Server S2.
- Policy & Items with in a policy compliance details with respect to server will be reported only when a server scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- An application configuration can have multiple instances on a server i.e. for example, WebSphere 4.0 configuration files can be installed in /opt and /home directories of server. In this case, net server compliance is determined by the aggregate compliance status of each application instance.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 5 AppConfig Compliance By Policy**



HP Service Automation Reporter - 192.168.202.203
File
Edit
View
Window
Help
Search
Please select item type
Reports
Compliance
Servers Without Policies By Compliance Type
Summary of Compliance By Policy
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Patch
Software
Software Compliance By Policy
Software Compliance By Server
Deployment Life Cycle
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
App Config Compliance By Policy
Run
Print
Export...
Schedule...

This report provides a full detailed breakdown of selected managed servers by their App Config compliance status for selected policies.

Date: Equals — Thu 03/26/2009
App Config Policy: Equals — [Any Value]
Device Group: Equals — Another Kiran Test Group
Server: Equals — [Any Value]
App Config Status: Equals — Compliant, Non-Compliant

**App Config Compliance By Policy**

Generated on: Fri Mar 27 17:47:50 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their App Config compliance status for selected policies.

**Parameters**

| | |
|---|---|
| **Date:** | Mar 26, 2009 |
| **App Config Policy:** | Any Value |
| **Device Group:** | 'Another Kiran Test Group' |
| **Server:** | Any Value |
| **App Config Status:** | 'Compliant','Non-Compliant' |

**Summary**

| | |
|---|---|
| **Compliant Policies:** | 1/3 |
| **Compliant Files:** | 1/4 |
| **Compliant Servers:** | 1/2 |

| | |
|---|---|
| **Policy Name:** | Kiran App Config |
| **Status:** | Compliant |
| **Compliant Files:** | 1/1 |
| **Compliant Servers:** | 2/2 |
| **Config File Name:** | /tmp/kmakarla/happy |
| **Status:** | Compliant |
| **Compliant Servers:** | 2/2 |

| Server Name | On Server | Last Scan |
|---|---|---|
| v028-vm2 | Yes | Thu Mar 26 16:51:56 2009 |
| v028-vm4 | Yes | Thu Mar 26 16:51:57 2009 |

| | |
|---|---|
| **Policy Name:** | Kiran-WebSphere |
| **Status:** | Non-Compliant |
| **Compliant Files:** | 0/2 |
| **Compliant Servers:** | 0/1 |
| **Config File Name:** | /opt/IBM/WebSphere/AppServer/systemApps/filetransferSecured.ear/deployment.xml |
| **Status:** | Non-Compliant |
| **Compliant Servers:** | 0/1 |

kmakarla Fri Mar 27 17:50 2009 America/Los_Angeles

# App Config Compliance by Server

## Server Summary

- Compliant: Total number of compliant servers
- Non-Compliant: Total number of non-complaint servers. A server is considered to be non compliant when one or more of the policies or items with in those policies that are attached to are non-compliant.
- Scan Needed:  Total number of servers that are in need of scan. A server is in scan needed state when one of more of the policies that are attached to has been modified and in order to determine the server compliance, the server needs to be scanned.
- Scan Failed:  Total number of servers that failed to complete the job of scanning the server for its compliance.
- Counts reflect current managed/active servers only.

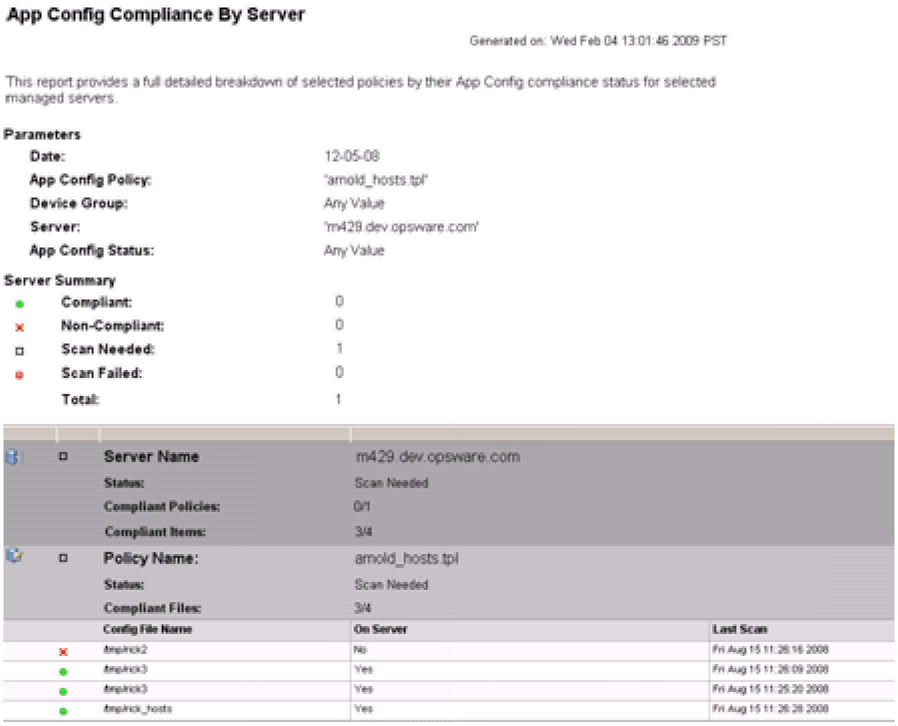
## Table

- An application configuration policy can be attached to either a device group or directly to a server. When a policy is attached to device group, a scan is needed in order for the system to recognize the server / policy attachment. Also, only servers with matching platform are reported.
- Table is primarily grouped by servers. Each server has compliance counts on each instance of the application configuration that are installed.
- Each configuration file is further grouped with in an application configuration instance to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Application Config P1, Application Config P2 is attached to Server S1 & Server 2. P1 has Config File F1, Config File F2 and it is compliant for S1 & non-compliant with S2. P2 is non-compliant for S1 & non-compliant with S2. Net compliance status for S1 & S2 is non-compliant.
- Config Files with in an App Config will be reported only when a server it is installed to is scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- An application configuration can have multiple instances on a server i.e. for example, Websphere 4.0 configuration files can be installed in /opt & /home directories of server. In this case, net compliance of server is determined by the combined compliance status of the each application instance.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

## Figure 6    AppConfig Compliance By Server



**App Config Compliance By Server**

Generated on: Wed Feb 04 13:01:46 2009 PST

This report provides a full detailed breakdown of selected policies by their App Config compliance status for selected managed servers.

**Parameters**

| | |
|---|---|
| **Date:** | 12-05-08 |
| **App Config Policy:** | 'arnold_hosts.tpl' |
| **Device Group:** | Any Value |
| **Server:** | 'm429.dev.opsware.com' |
| **App Config Status:** | Any Value |

**Server Summary**

| | | |
|---|---|---|
| ● | **Compliant:** | 0 |
| ✗ | **Non-Compliant:** | 0 |
| □ | **Scan Needed:** | 1 |
| ● | **Scan Failed:** | 0 |
| | **Total:** | 1 |

| | | | |
|---|---|---|---|
| | □ | **Server Name** | m429.dev.opsware.com |
| | | **Status:** | Scan Needed |
| | | **Compliant Policies:** | 0/1 |
| | | **Compliant Items:** | 3/4 |
| | □ | **Policy Name:** | arnold_hosts.tpl |
| | | **Status:** | Scan Needed |
| | | **Compliant Files:** | 3/4 |

| | Config File Name | On Server | Last Scan |
|---|---|---|---|
| ✗ | /tmp/rick2 | No | Fri Aug 15 11:26:16 2008 |
| ● | /tmp/rick3 | Yes | Fri Aug 15 11:26:09 2008 |
| ● | /tmp/rick3 | Yes | Fri Aug 15 11:25:20 2008 |
| ● | /tmp/rick_hosts | Yes | Fri Aug 15 11:26:28 2008 |

# Audit Compliance by Policy

## Summary

- Compliant Policies: Count of compliant selected policies / Total number of selected policies that are attached to the servers.
- Compliant Rules: Count of unique compliant Rules across all selected policies / Total number of unique Rules across all selected policies that are attached to the servers.
- Compliant Severs: Count of unique compliant servers / Total number of unique servers.
- Counts reflect current managed/active servers for recurring audits only.

## Table

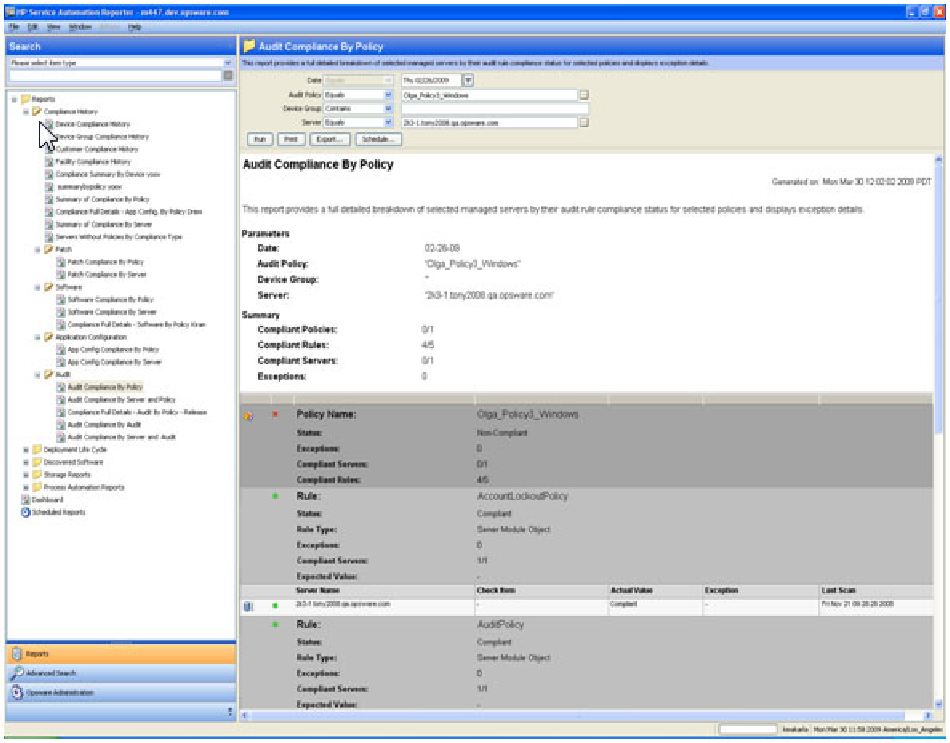
- Audit policy contains rules that are either defined within or extended from another policy. Multi level policy hierarchy is supported to create a composite policy.
- Table is primarily grouped by policies. Each policy has compliance counts for each of the rules and servers that are audit checked.
- Each rule is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Audit Policy P1 has Rule, Rule1 and is audit checked on Server S1 & Server 2. Rule1 is compliant for S1 & non-compliant for S2. Net compliance status for Rule1 is non-compliant. Since Rule1 is part of policy P1, P1 is also non-compliant with respect to S1 & S2.
- Rules with in a policy will be reported only when a server it is attached to is scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- Audit details that are captured for each of the target server vary depending on individual rule types and type of checks, that can be performed such as 'Value based' /'Comparison'.
- A 'Value Based' check verifies for a specific value on the target server, Example Min Password length = 8. "Actual Value" from the audit is reported, along with the "Expected Value" specified by the user.
- A 'Comparison Based' checks compares objects/files/directories etc on the source and target servers. Audit results could vary depending on existence of these objects on both source and target and their differences if exists.
- Audit reports for 'Comparison Based' checks, show only the differences between the source and target servers.
- An audit report consists of following columns:
  - Server Name
  - Check Item (depending on the rule type)
  - Actual Value or Differences (depending on the rule type)
  - Exception Details
  - Last Scan

## Value Based Checks

The following is a list of rule types on which 'Value Based' checks can be performed:

- Check Policy / Pluggable Check
- Application Configuration Policy
- Custom Script
- Network Duplex
- Server Module Object
- Storage Initiator

**Figure 7 Audit Compliance By Policy - Value-Based Checks**



Audit Compliance By Policy

Generated on: Mon Mar 30 12:02:02 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their audit rule compliance status for selected policies and displays exception details.

Parameters
Date: 02-26-09
Audit Policy: 'Olga_Policy3_Windows'
Device Group: -
Server: '2k3-1 tony2008.qa.opsware.com'

Summary
Compliant Policies: 0/1
Compliant Rules: 4/5
Compliant Servers: 0/1
Exceptions: 0

Policy Name: Olga_Policy3_Windows
Status: Non-Compliant
Exceptions: 0
Compliant Servers: 0/1
Compliant Rules: 4/5

Rule: AccountLockoutPolicy
Status: Compliant
Rule Type: Server Module Object
Exceptions: 0
Compliant Servers: 1/1
Expected Value: -

| Server Name | Check Item | Actual Value | Exception | Last Scan |
|---|---|---|---|---|
| 2k3-1 tony2008.qa.opsware.com | - | Compliant | - | Fri Nov 21 09:28:28 2008 |

Rule: AuditPolicy
Status: Compliant
Rule Type: Server Module Object
Exceptions: 0
Compliant Servers: 1/1
Expected Value: -

## Comparison Based Checks

The following is a list of rule types on which *Comparison Based* checks can be performed and reported:

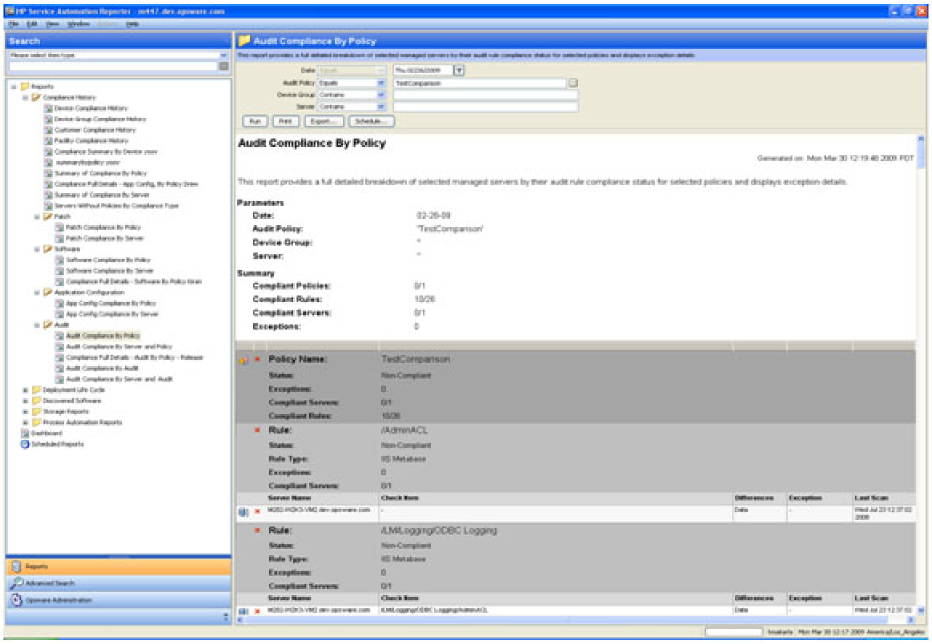
- Storage InitiatorCheck Policy / Pluggable Check
- Windows Services
- Registry
- COM+
- Custom Script
- Storage
- File System

- IIS Metabase
- Server Module Object
- Hardware
- An exception to an audit can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, for the specified target server, the server is considered 'Compliant'.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 8 Audit Compliance By Policy - Comparison-Based Checks**



Audit Compliance By Policy

Generated on: Mon Mar 30 12:19:48 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their audit rule compliance status for selected policies and displays exception details.

**Parameters**

| | |
|---|---|
| Date: | 02-26-09 |
| Audit Policy: | 'TestComparison' |
| Device Group: | * |
| Server: | * |

**Summary**

| | |
|---|---|
| Compliant Policies: | 0/1 |
| Compliant Rules: | 10/26 |
| Compliant Servers: | 0/1 |
| Exceptions: | 0 |

**Policy Name:** TestComparison

| | |
|---|---|
| Status: | Non Compliant |
| Exceptions: | 0 |
| Compliant Servers: | 0/1 |
| Compliant Rules: | 10/26 |

**Rule:** /AdminACL

| | |
|---|---|
| Status: | Non Compliant |
| Rule Type: | IIS Metabase |
| Exceptions: | 0 |
| Compliant Servers: | 0/1 |

| Server Name | Check Item | Differences | Exception | Last Scan |
|---|---|---|---|---|
| M0ID-HOK0-VM2.dev.opsware.com | - | Data | - | Wed Jul 23 12:37:02 2008 |

**Rule:** /LM/Logging/ODBC Logging

| | |
|---|---|
| Status: | Non Compliant |
| Rule Type: | IIS Metabase |
| Exceptions: | 0 |
| Compliant Servers: | 0/1 |

| Server Name | Check Item | Differences | Exception | Last Scan |
|---|---|---|---|---|
| M0ID-HOK0-VM2.dev.opsware.com | /LM/Logging/ODBC Logging/AdminACL | Data | - | Wed Jul 23 12:37:02 |

# Audit Compliance by Server and Policy

## Server Summary

- Compliant: Total number of compliant servers.
- Non-Compliant: Total number of non-complaint servers. A server is considered to be non compliant when one or more of the policies or rules with in those policies that are attached to are non-compliant.
- Scan Needed: Total number of servers that are in need of scan. A server is in scan needed state when one of more of the policies that are attached to has been modified and in order to determine the server compliance, the server needs to be scanned.
- Scan Failed: Total number of servers that failed to complete the job of scanning the server for its compliance.
- Counts reflect current managed/active servers for recurring audits only.

## Table

- Audit policy contains set of rules that are either defined within or extended from another policy. Multi level policy hierarchy is supported to create a composite policy.
- Table is primarily grouped by servers. Each server has compliance counts for each of the policy and rules within the policy that is audit checked.
- Each Rule is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Audit Policy P1 is audit checked on Server S1 & Server 2. Policy P1 has Rule, Rule1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Rule1 is non-compliant. Since Rule1 is part of policy P1, P1 is also non-compliant. Since P1 is attached to Server S1, S1 is non-compliant
- Rules with in a policy will be reported only when a server it is attached to is scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- Audit details that are captured for each of the target server vary depending on individual rule types and type of checks, which are be performed such as 'Value based' /'Comparison'.
- A 'Value Based' check is performed to verify for a specific value on the target server, Example Min Password length = 8. "Actual Value" from the audit is reported, along with the "Expected Value" specified by the user.
- A 'Comparison Based' checks are performed to compare objects/files/directories on the source and target servers. Audit results could vary depending on existence of these objects on both source and target and their differences if exists.
- Audit reports for 'Comparison Based' checks, show only the differences between the source and target servers.
- An audit report consists of the following columns:
  - Server Name
  - Check Item (depending on the rule type)
  - Actual Value or Differences (depending on the rule type)

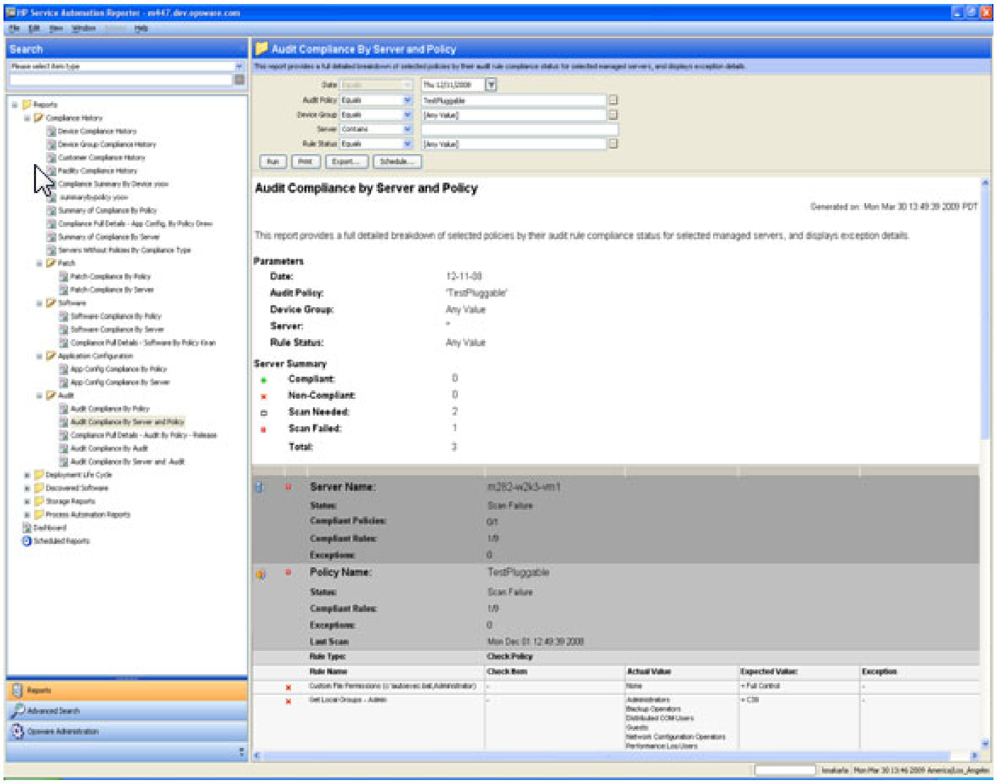
- — Exception Details
- — Last Scan

## Value Based Checks

The following is a list of rule types on which 'Value Based' checks can be performed:

- Check Policy / Pluggable Check
- Application Configuration Policy
- Custom Script
- Network Duplex
- Server Module Object
- Storage Initiator

**Figure 9 Audit Compliance By Server and Policy - Value-Based Checks**



Audit Compliance By Server and Policy

This report provides a full detailed breakdown of selected policies by their audit rule compliance status for selected managed servers, and displays exception details.

Date: Thu 12/11/2008
Audit Policy: Equals TestPluggable
Device Group: Equals [Any Value]
Server: Contains
Rule Status: Equals [Any Value]

Audit Compliance by Server and Policy

Generated on: Mon Mar 30 13:49:39 2009 PDT

This report provides a full detailed breakdown of selected policies by their audit rule compliance status for selected managed servers, and displays exception details.

Parameters
Date: 12-11-08
Audit Policy: 'TestPluggable'
Device Group: Any Value
Server: *
Rule Status: Any Value

Server Summary
Compliant: 0
Non-Compliant: 0
Scan Needed: 2
Scan Failed: 1
Total: 3

Server Name: m282-w2k3-vm1
Status: Scan Failure
Compliant Policies: 0/1
Compliant Rules: 1/9
Exceptions: 0

Policy Name: TestPluggable
Status: Scan Failure
Compliant Rules: 1/9
Exceptions: 0
Last Scan: Mon Dec 01 12:49:39 2008
Rule Type: Check Policy

| Rule Name | Check Item | Actual Value | Expected Value: | Exception |
|---|---|---|---|---|
| Custom File Permissions (c:\autoexec.bat,Administrator) | - | None | = Full Control | - |
| Get Local Groups - Admin | - | Administrators<br>Backup Operators<br>Distributed COM Users<br>Guests<br>Network Configuration Operators<br>Performance Log Users | = C39 | - |

localhost Mon Mar 30 13:46 2009 America/Los_Angeles

## Comparison Based Checks

The following is a list of rule types on which 'Comparison Based' checks can be performed and reported:

- Storage InitiatorCheck Policy / Pluggable Check
- Windows Services
- Registry
- COM+

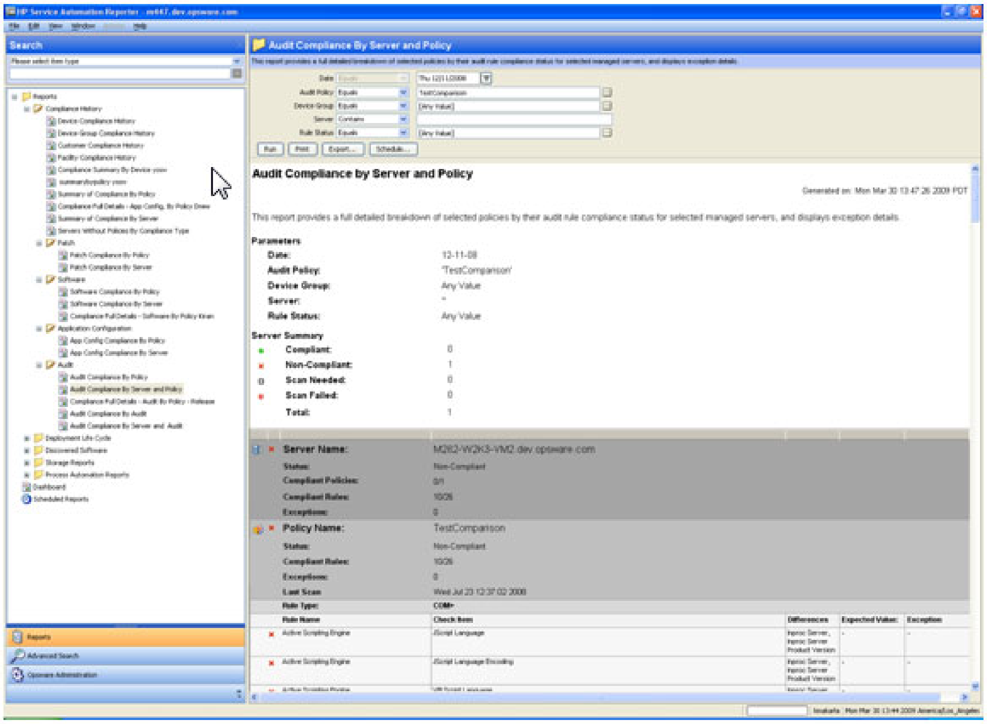
- Custom Script
- Storage
- File System
- IIS Metabase
- Server Module Object
- Hardware

An exception to an audit can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, for the specified target server, the server is considered 'Compliant'.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 10 Audit Compliance By Server and Policy - Comparison-Based Checks**



HP Service Automation Reporter
Search
Audit Compliance By Server and Policy
Run
Print
Export...
Schedule...
Reports
Advanced Search

This report provides a full detailed breakdown of selected policies by their audit rule compliance status for selected managed servers, and displays exception details.

Audit Compliance by Server and Policy

Generated on: Mon Mar 30 13:47:26 2009 PDT

This report provides a full detailed breakdown of selected policies by their audit rule compliance status for selected managed servers, and displays exception details.

Parameters
Date: 12-11-08
Audit Policy: 'TestComparison'
Device Group: Any Value
Server: *
Rule Status: Any Value

Server Summary
Compliant: 0
Non-Compliant: 1
Scan Needed: 0
Scan Failed: 0
Total: 1

Server Name: M282-W2K3-VM2.dev.opsware.com
Status: Non-Compliant
Compliant Policies: 0/1
Compliant Rules: 10/26
Exceptions: 0

Policy Name: TestComparison
Status: Non-Compliant
Compliant Rules: 10/26
Exceptions: 0
Last Scan: Wed Jul 23 12:37:02 2008
Rule Type: COM+

| Rule Name | Check Item | Differences | Expected Value | Exception |
|---|---|---|---|---|
| Active Scripting Engine | JScript Language | Inproc Server,<br>Inproc Server<br>Product Version | - | - |
| Active Scripting Engine | JScript Language Encoding | Inproc Server,<br>Inproc Server<br>Product Version | - | - |

# Audit Compliance by Audit

## Summary

- Compliant Audits: Count of compliant selected audits / Total number of selected audits that are performed on the servers.
- Compliant Rules: Count of unique compliant Rules across all selected audits / Total number of unique Rules across all selected audits that are performed on the servers.
- Compliant Severs: Count of unique compliant servers / Total number of unique servers.
- Counts reflect current managed/active servers for recurring/ recurring and non-recurring audits depending on the selection criteria.

## Table

- An audit consists of set of rules that are either derived from single or multiple audit policies. In addition audit can also have an implicit rules defined within to create a comprehensive audit.
- An audit snapshot specification can be created for set of servers using a policy that was pre configured with rules. The results for the specification can be used as a baseline for future audits.
- An audit can be created on set of target servers using either an audit snapshot specification result that was captured previously or on a recent snapshot specification result or as trivial as a single server as the source
- Table is primarily grouped by audits. Each audit has compliance counts for each of its Rules and servers that are audit checked.
- Each Rule is further grouped with in an audit to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Audit A1 is audit checked on Server S1 & Server 2. Audit A1 has Rule, Rule1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Rule1 is non-compliant. Since Rule1 is part of Audit A1, A1 is also non-compliant.
- Rules with in an Audit will be reported only when a server it is attached to is scanned In the event of scan failure or scan needed, only Audit - server attachment details are reported.
- Audit details that are captured for each of the target server vary depending on individual rule types and type of checks, which are be performed such as 'Value based' /'Comparison'.
- A 'Value Based' check is performed to verify for a specific value on the target server, Example Min Password length = 8. "Actual Value" from the audit is reported, along with the "Expected Value" specified by the user.
- A 'Comparison Based' checks are performed to compare objects/files/directories on the source and target servers. Audit results could vary depending on existence of these objects on both source and target and their differences if exists.
- Audit reports for 'Comparison Based' checks, show only the differences between the source and target servers.
- Audit report consists of following columns.
  - Server Name

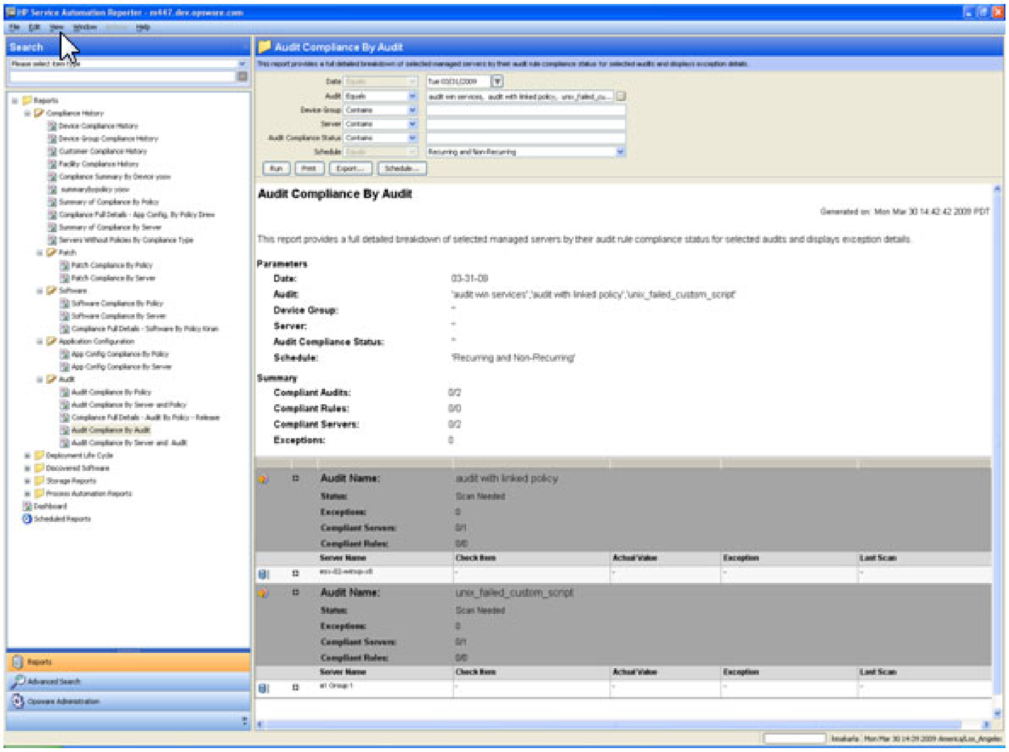
- — Check Item (depending on the rule type)
- — Actual Value or Differences (depending on the rule type)
- — Exception Details
- — Last Scan

## Value Based Checks

Following is a list of rule types on which 'Value Based' checks can be performed

- Check Policy / Pluggable Check
- Application Configuration Policy
- Custom Script
- Network Duplex
- Server Module Object
- Storage Initiator

**Figure 11 Audit Compliance By Audit - Value-Based Checks**



Date: Equals | Tue 03/31/2009
Audit: Equals | audit win services, audit with linked policy, unix_failed_cu...
Device Group: Contains
Server: Contains
Audit Compliance Status: Contains
Schedule: Equals | Recurring and Non-Recurring

**Audit Compliance By Audit**

Generated on: Mon Mar 30 14:42:42 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their audit rule compliance status for selected audits and displays exception details.

**Parameters**

**Date:** 03-31-09
**Audit:** 'audit win services','audit with linked policy','unix_failed_custom_script'
**Device Group:** *
**Server:** *
**Audit Compliance Status:** *
**Schedule:** 'Recurring and Non-Recurring'

**Summary**

**Compliant Audits:** 0/2
**Compliant Rules:** 0/0
**Compliant Servers:** 0/2
**Exceptions:** 0

**Audit Name:** audit with linked policy
**Status:** Scan Needed
**Exceptions:** 0
**Compliant Servers:** 0/1
**Compliant Rules:** 0/0

| Server Name | Check Item | Actual Value | Exception | Last Scan |
|---|---|---|---|---|
| [illegible] | - | - | - | - |

**Audit Name:** unix_failed_custom_script
**Status:** Scan Needed
**Exceptions:** 0
**Compliant Servers:** 0/1
**Compliant Rules:** 0/0

| Server Name | Check Item | Actual Value | Exception | Last Scan |
|---|---|---|---|---|
| #1 Group 1 | - | - | - | - |

## Comparison Based Checks

The following is a list of rule types on which 'Comparison Based' checks can be performed and reported:

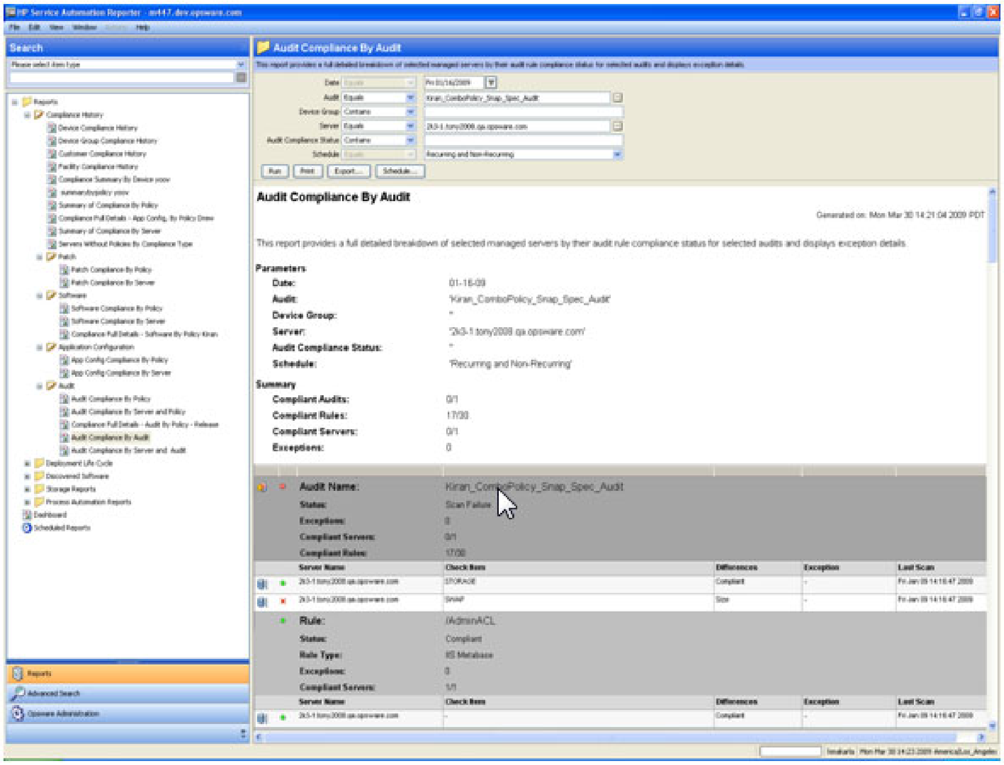
- Storage InitiatorCheck Policy / Pluggable Check
- Windows Services
- Registry

- COM+
- Custom Script
- Storage
- File System
- IIS Metabase
- Server Module Object
- Hardware
- An exception to an audit can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, for the specified target server, the server is considered 'Compliant'.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 12 Audit Compliance By Audit - Comparison-Based Checks**



Date: Equals — Fri 01/16/2009
Audit: Equals — Kiran_ComboPolicy_Snap_Spec_Audit
Device Group: Contains
Server: Equals — 2k3-1.tony2008.qa.opsware.com
Audit Compliance Status: Contains
Schedule: Equals — Recurring and Non-Recurring

Audit Compliance By Audit

Generated on: Mon Mar 30 14:21:04 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their audit rule compliance status for selected audits and displays exception details.

Parameters

| | |
|---|---|
| Date: | 01-16-09 |
| Audit: | 'Kiran_ComboPolicy_Snap_Spec_Audit' |
| Device Group: | * |
| Server: | '2k3-1.tony2008.qa.opsware.com' |
| Audit Compliance Status: | * |
| Schedule: | 'Recurring and Non-Recurring' |

Summary

| | |
|---|---|
| Compliant Audits: | 0/1 |
| Compliant Rules: | 17/30 |
| Compliant Servers: | 0/1 |
| Exceptions: | 0 |

| | |
|---|---|
| Audit Name: | Kiran_ComboPolicy_Snap_Spec_Audit |
| Status: | Scan Failure |
| Exceptions: | 0 |
| Compliant Servers: | 0/1 |
| Compliant Rules: | 17/30 |

| Server Name | Check Item | Differences | Exception | Last Scan |
|---|---|---|---|---|
| 2k3-1.tony2008.qa.opsware.com | STORAGE | Compliant | - | Fri Jan 09 14:16:47 2009 |
| 2k3-1.tony2008.qa.opsware.com | SNAP | Size | - | Fri Jan 09 14:16:47 2009 |

| | |
|---|---|
| Rule: | /AdminACL |
| Status: | Compliant |
| Rule Type: | IIS Metabase |
| Exceptions: | 0 |
| Compliant Servers: | 1/1 |

| Server Name | Check Item | Differences | Exception | Last Scan |
|---|---|---|---|---|
| 2k3-1.tony2008.qa.opsware.com | - | Compliant | - | Fri Jan 09 14:16:47 2009 |

# Audit Compliance by Server and Audit

## Server Summary

- Compliant: Total number of compliant servers
- Non-Compliant: Total number of non-complaint servers. A server is considered to be non compliant when one or more of the policies or rules with in those policies that are attached to are non-compliant
- Scan Needed: Total number of servers that are in need of scan. A server is in scan needed state when one of more of the policies that are attached to has been modified and in order to determine the server compliance, the server needs to be scanned.
- Scan Failed: Total number of servers that failed to complete the job of scanning the server for its compliance.
- Counts reflect current managed/active servers for recurring audits only

## Table

- An audit policy consists of set of rules that are either defined within or extended from another policy. Multi level policy inheritance is supported to create a composite policy.
- An audit snapshot specification can be created for set of target servers using a policy that was pre- configured with rules. The results for the specification can be used as a baseline for future audits.
- An audit can be created on set of target servers using either an audit snapshot specification result that was captured previously or on a recent snapshot specification result or as trivial as a single server as the source.
- Table is primarily grouped by servers. Each server has compliance counts for each of the policies and rules within the policy that are audit checked.
- Each Rule is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Audit Policy P1 is audit checked on Server S1 & Server 2. Policy P1 has Rule, Rule1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Rule1 is non-compliant. Since Rule1 is part of policy P1, P1 is also non-compliant. Since P1 is attached to Server S1, S1 is non-compliant.
- Rules with in a policy will be reported only when a server it is attached to is scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- Audit details that are captured for each of the target server vary depending on individual rule types and type of checks, which are be performed such as 'Value based' /'Comparison'.
- A 'Value Based' check is performed to verify for a specific value on the target server, Example Min Password length = 8. "Actual Value" from the audit is reported, along with the "Expected Value" specified by the user.
- A 'Comparison Based' checks are performed to compare objects/files/directories on the source and target servers. Audit results could vary depending on existence of these objects on both source and target and their differences if exists.
- Audit reports for 'Comparison Based' checks, show only the differences between the source and target servers

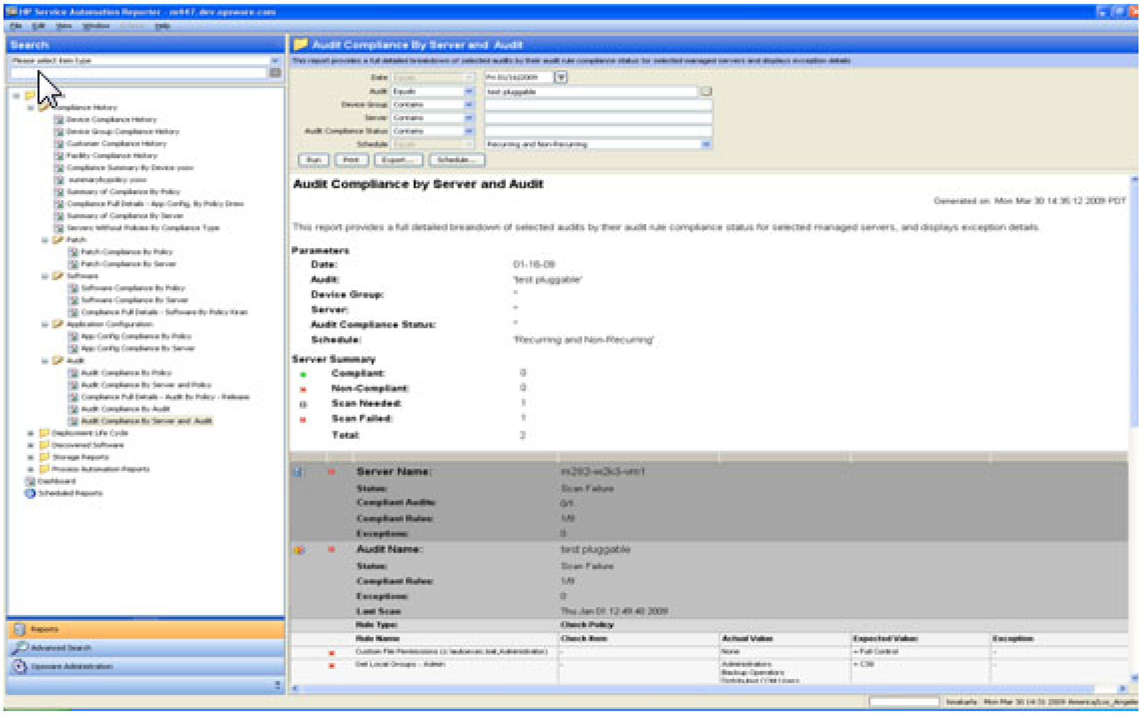
- Audit report consists of following columns
  - Server Name
  - Check Item (depending on the rule type)
  - Actual Value or Differences (depending on the rule type)
  - Exception Details
  - Last Scan

## Value Based Checks

The following is a list of rule types on which 'Value Based' checks can be performed:

- Check Policy / Pluggable Check
- Application Configuration Policy
- Custom Script
- Network Duplex
- Server Module Object
- Storage Initiator

**Figure 13 Audit Compliance By Server and Audit - Value-Based Checks**



Audit Compliance by Server and Audit

Generated on: Mon Mar 30 14:35:12 2009 PDT

This report provides a full detailed breakdown of selected audits by their audit rule compliance status for selected managed servers, and displays exception details.

Parameters

| | |
|---|---|
| Date: | 01-16-09 |
| Audit: | 'test pluggable' |
| Device Group: | * |
| Server: | * |
| Audit Compliance Status: | * |
| Schedule: | 'Recurring and Non-Recurring' |

Server Summary

| | | |
|---|---|---|
| 🟩 | Compliant: | 0 |
| 🟥 | Non-Compliant: | 0 |
| □ | Scan Needed: | 1 |
| 🟥 | Scan Failed: | 1 |
| | Total: | 2 |

| | |
|---|---|
| Server Name: | m283-w2k3-vm1 |
| Status: | Scan Failure |
| Compliant Audits: | 0/1 |
| Compliant Rules: | 1/9 |
| Exceptions: | 0 |
| Audit Name: | test pluggable |
| Status: | Scan Failure |
| Compliant Rules: | 1/9 |
| Exceptions: | 0 |
| Last Scan: | Thu Jan 01 12:49:40 2009 |
| Rule Type: | Check Policy |

| Rule Name | Check Item | Actual Value | Expected Value | Exception |
|---|---|---|---|---|
| Custom File Permissions (c:\autoexec.bat,Administrator) | - | None | + Full Control | - |
| Get Local Groups - Admin | - | Administrators<br>Backup Operators<br>Distributed COM Users | + C39 | - |

## Comparison Based Checks

The Following are list of rule types on which 'Comparison Based' checks can be performed and reported:

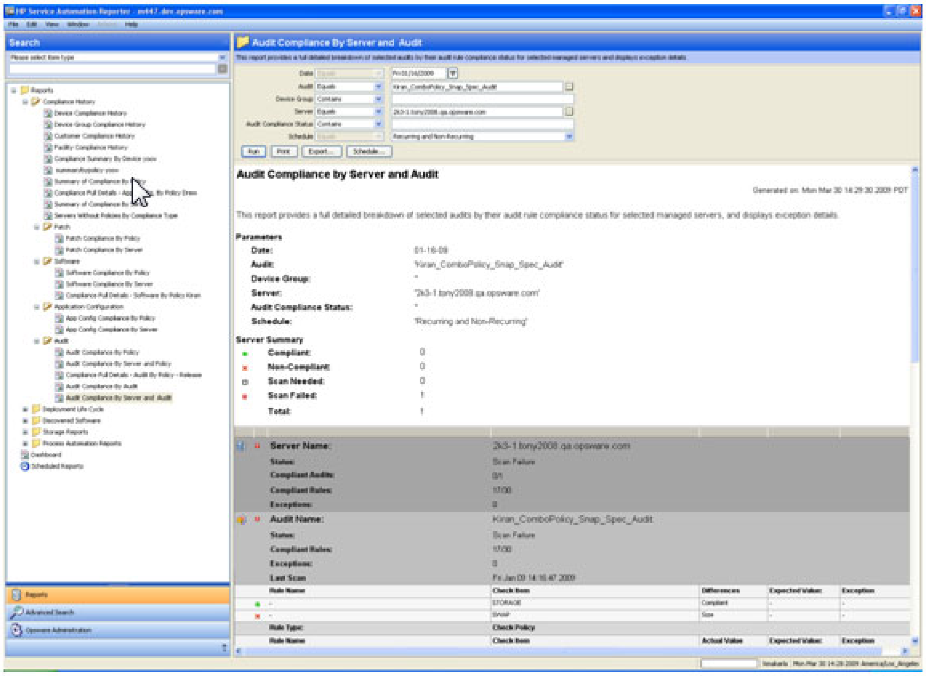
- Storage InitiatorCheck Policy / Pluggable Check

- Windows Services
- Registry
- COM+
- Custom Script
- Storage
- File System
- IIS Metabase
- Server Module Object
- Hardware
- An exception to an audit can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, for the specified target server, the server is considered 'Compliant'.

## Actionable

- Double Click / Right Click on an audit and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 14 Audit Compliance By Server and Audit - Comparison-Based Checks**


HP Service Automation Reporter - m447.dev.opsware.com
File
Edit
View
Window
Help
Search
Please select item type
Reports
Compliance History
Device Compliance History
Device Group Compliance History
Customer Compliance History
Facility Compliance History
Compliance Summary By Device yoov
summaryBypolicy yoov
Summary of Compliance By Policy
Compliance Full Details - App... By Policy Drew
Summary of Compliance By Server
Servers Without Policies By Compliance Type
Patch
Patch Compliance By Policy
Patch Compliance By Server
Software
Software Compliance By Policy
Software Compliance By Server
Compliance Full Details - Software By Policy Kiran
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Audit Compliance By Policy
Audit Compliance By Server and Policy
Compliance Full Details - Audit By Policy - Release
Audit Compliance By Audit
Audit Compliance By Server and Audit
Deployment Life Cycle
Discovered Software
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Audit Compliance By Server and Audit
Run
Print
Export...
Schedule...

This report provides a full detailed breakdown of selected audits by their audit rule compliance status for selected managed servers and displays exception details

Date: Equals: Fri 01/16/2009
Audit: Equals: Kiran_ComboPolicy_Snap_Spec_Audit
Device Group: Contains:
Server: Equals: 2k3-1.tony2008.qa.opsware.com
Audit Compliance Status: Contains:
Schedule: Equals: Recurring and Non-Recurring

Audit Compliance by Server and Audit

Generated on: Mon Mar 30 14:29:30 2009 PDT

This report provides a full detailed breakdown of selected audits by their audit rule compliance status for selected managed servers, and displays exception details.

**Parameters**

Date: 01-16-09
Audit: 'Kiran_ComboPolicy_Snap_Spec_Audit'
Device Group: *
Server: '2k3-1.tony2008.qa.opsware.com'
Audit Compliance Status: *
Schedule: 'Recurring and Non-Recurring'

**Server Summary**

Compliant: 0
Non-Compliant: 0
Scan Needed: 0
Scan Failed: 1
Total: 1

Server Name: 2k3-1.tony2008.qa.opsware.com
Status: Scan Failure
Compliant Audits: 0/1
Compliant Rules: 17/30
Exceptions: 0

Audit Name: Kiran_ComboPolicy_Snap_Spec_Audit
Status: Scan Failure
Compliant Rules: 17/30
Exceptions: 0
Last Scan: Fri Jan 09 14:16:47 2009

| Rule Name | Check Item | Differences | Expected Value: | Exception |
|---|---|---|---|---|
| - | STORAGE | Compliant | - | - |
| - | SNAP | Size | - | - |

Rule Type: Check Policy

| Rule Name | Check Item | Actual Value | Expected Value: | Exception |
|---|---|---|---|---|

# Patch Compliance By Policy

## Summary

- Compliant Policies: Count of compliant selected policies / Total number of selected policies that are attached to the servers.
- Compliant Patches: Count of unique compliant patches across all selected policies / Total number of unique patches across all selected policies that are attached to the servers.
- Compliant Severs: Count of unique compliant servers / Total number of unique servers.
- Counts reflect current managed/active servers only.

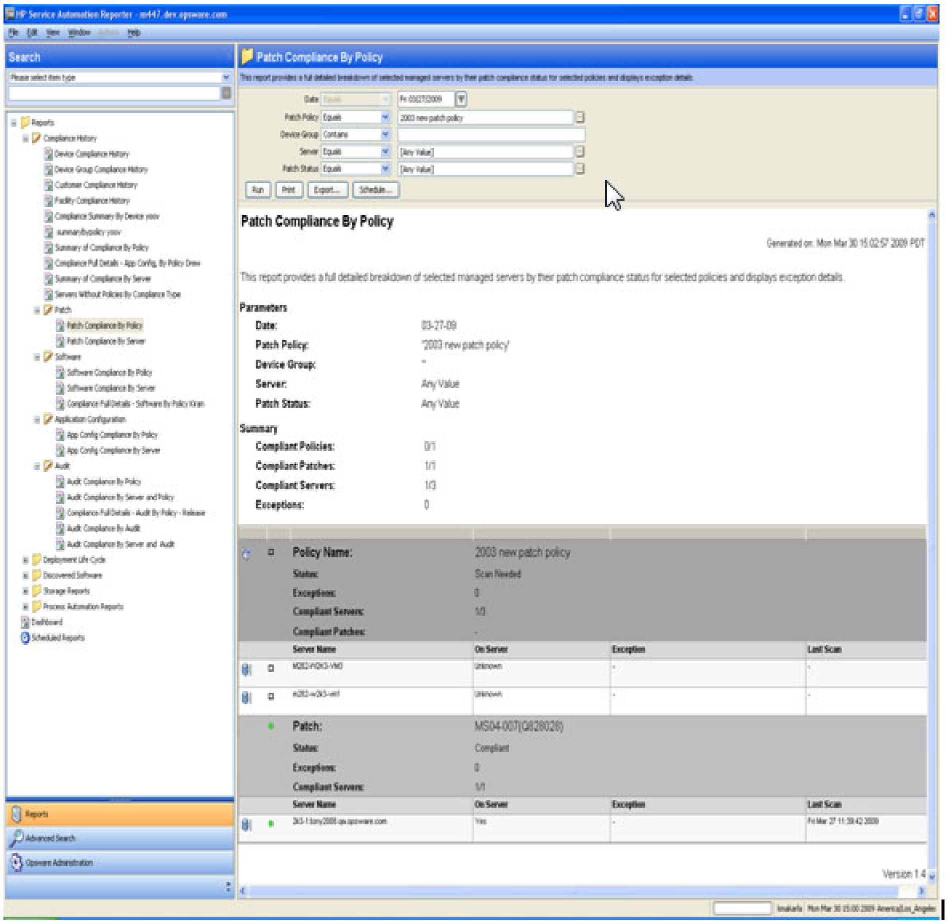
## Table

- A patch policy can be attached to either a device group or directly to a server. Only servers with matching platform are reported.
- A device group can have another device group i.e. nested device group. A patch policy can be attached to nested device group. By default only servers directly attached to parent device group are reported when parent device group is selected as part of user report criteria.
- To determine compliance details of nested device group, user has to select nested device group in the report criteria.
- Table is primarily grouped by policies. Each policy has compliance counts for each of its patches and servers that are attached to it.
- Each patch item is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Patch Policy P1 is attached to Server S1 & Server 2. Policy P1 has patch item, Item1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Item1 is non-compliant. Since Item1 is part of policy P1, P1 is also non-compliant.
- Compliance details of a patch item with in a policy will be reported only when a server it is attached to is scanned In the event of scan failure or scan needed, only policy - server attachment details are reported.
- A patch item that is 'Partially Complaint' would make the policy that is part of 'non-compliant'. However, the server would be in Partially-Compliant' status.
- An exception to a patch item can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, patch is compliant / partially-compliant depending on the patch compliance user setting in SA

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

## Figure 15 Patch Compliance By Policy


HP Service Automation Reporter - m447.dev.opsware.com
File Edit View Window Help
Search
Please select item type
Reports
Compliance History
Device Compliance History
Device Group Compliance History
Customer Compliance History
Facility Compliance History
Compliance Summary By Device yoov
summarybypolicy yoov
Summary of Compliance By Policy
Compliance Full Details - App Config, By Policy Drew
Summary of Compliance By Server
Servers Without Policies By Compliance Type
Patch
Patch Compliance By Policy
Patch Compliance By Server
Software
Software Compliance By Policy
Software Compliance By Server
Compliance Full Details - Software By Policy Kiran
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Audit Compliance By Policy
Audit Compliance By Server and Policy
Compliance Full Details - Audit By Policy - Release
Audit Compliance By Audit
Audit Compliance By Server and Audit
Deployment Life Cycle
Discovered Software
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Patch Compliance By Policy
Run
Print
Export...
Schedule...

This report provides a full detailed breakdown of selected managed servers by their patch compliance status for selected policies and displays exception details.

Date Equals Fri 03/27/2009
Patch Policy Equals 2003 new patch policy
Device Group Contains
Server Equals [Any Value]
Patch Status Equals [Any Value]

**Patch Compliance By Policy**

Generated on: Mon Mar 30 15:02:57 2009 PDT

This report provides a full detailed breakdown of selected managed servers by their patch compliance status for selected policies and displays exception details.

**Parameters**

| | |
|---|---|
| **Date:** | 03-27-09 |
| **Patch Policy:** | '2003 new patch policy' |
| **Device Group:** | " |
| **Server:** | Any Value |
| **Patch Status:** | Any Value |

**Summary**

| | |
|---|---|
| **Compliant Policies:** | 0/1 |
| **Compliant Patches:** | 1/1 |
| **Compliant Servers:** | 1/3 |
| **Exceptions:** | 0 |

| | | | | | |
|---|---|---|---|---|---|
| | □ | **Policy Name:** | 2003 new patch policy | | |
| | | **Status:** | Scan Needed | | |
| | | **Exceptions:** | 0 | | |
| | | **Compliant Servers:** | 1/3 | | |
| | | **Compliant Patches:** | - | | |
| | | **Server Name** | **On Server** | **Exception** | **Last Scan** |
| | □ | M2K3-W2K3-VM3 | Unknown | - | - |
| | □ | m2k3-w2k3-vm1 | Unknown | - | - |
| | ● | **Patch:** | MS04-007(Q828028) | | |
| | | **Status:** | Compliant | | |
| | | **Exceptions:** | 0 | | |
| | | **Compliant Servers:** | 1/1 | | |
| | | **Server Name** | **On Server** | **Exception** | **Last Scan** |
| | ● | 2k3-1-tony2008.qa.opsware.com | Yes | - | Fri Mar 27 11:38:42 2009 |

Version 1.4

kmakarla Mon Mar 30 15:00 2009 America/Los_Angeles

# Patch Compliance By Server

## Summary

- Total number of compliant servers.
- Non-Compliant: Total number of non-complaint servers. A server is considered to be non compliant when one or more of the policies or patches with in those policies that are attached to are non-compliant.
- Scan Needed: Total number of servers that are in need of scan. A server is in scan needed state when one of more of the policies that are attached to has been modified and in order to determine the server compliance, the server needs to be scanned.
- Scan Failed: Total number of servers that failed to complete the job of scanning the server for its compliance.
- Partially-Compliant: Total number of servers that failed to fully meet the patch compliance standards set by the administrators.
- Counts reflect current managed/active servers only.

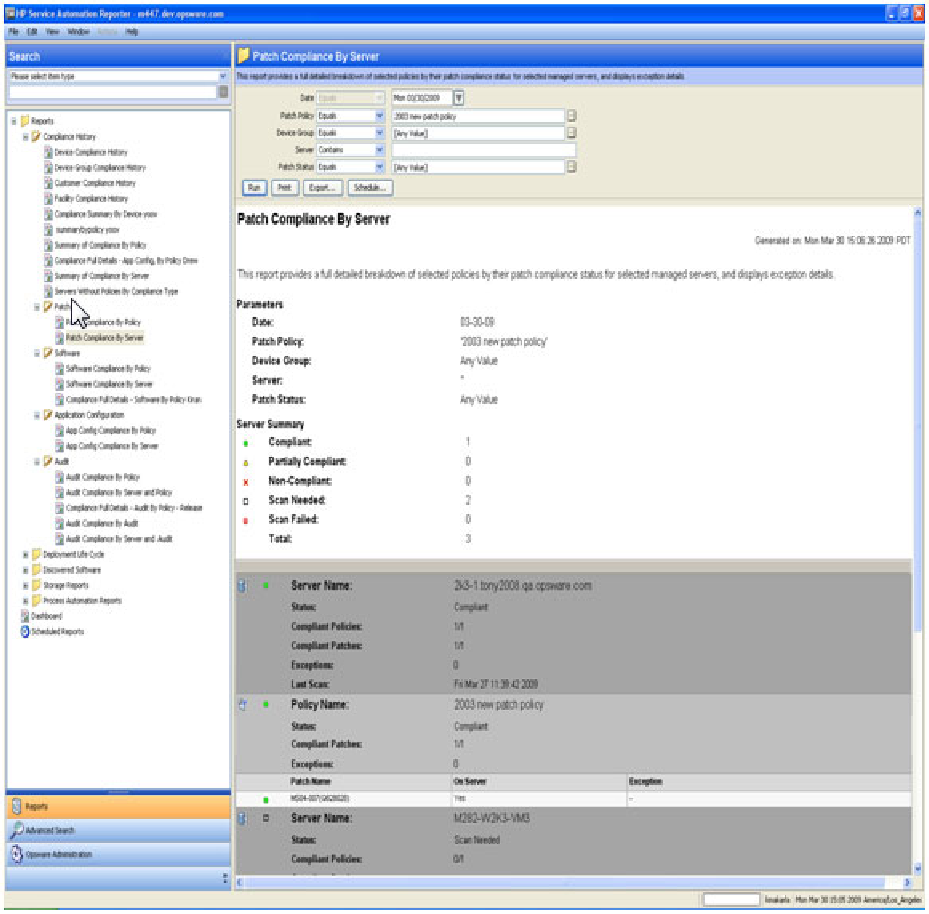
## Table

- A patch policy can be attached to either a device group or directly to a server. Only servers with matching platform are reported.
- A device group can have another device group i.e. nested device group. A patch policy can be attached to nested device group. By default only servers directly attached to parent device group are reported when parent device group is selected as part of user report criteria.
- To determine compliance details of nested device group, user has to select nested device group in the report criteria.
- Table is primarily grouped by servers. Each server has compliance counts for each of the policies that are attached and patches that are part of the policy.
- Each patch item is further grouped with in a policy to give granular compliance details at this level. Compliance status is rolled-up or bubbled up from this level. For example, Patch Policy P1 is attached to Server S1 & Server 2. Policy P1 has patch item, Item1 and it is compliant for server S1 & non-compliant with server S2. Net compliance status for Item1 is non-compliant. Since Item1 is part of policy P1, P1 is also non-compliant and so is the server S1.
- Compliance details of a patch item with in a policy will be reported only when a server it is attached to is scanned In the event of scan failure or scan needed, only policy - server attachment details are reported.
- A patch item that is 'Partially Complaint' would make the policy that is part of 'non-compliant'. However, the server would be in Partially-Compliant' status.
- An exception to a patch item can be created with or without 'Exception Details' / Exception Expiration Date. If exception criteria is met, patch is compliant / partially-compliant depending on the patch compliance user setting in SA.

## Actionable

- Double Click / Right Click on a policy and select 'Open' to launch SA Policy Browser. Various possible operations on the policy are subject to user permission.
- Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission.

**Figure 16 Patch Compliance By Server**


HP Service Automation Reporter - m447.dev.opsware.com
File Edit View Window Actions Help
Search
Please select item type
Reports
Compliance History
Device Compliance History
Device-Group Compliance History
Customer Compliance History
Facility Compliance History
Compliance Summary By Device yoov
summarybypolicy yoov
Summary of Compliance By Policy
Compliance Full Details - App Config, By Policy Drew
Summary of Compliance By Server
Servers Without Policies By Compliance Type
Patch
Patch Compliance By Policy
Patch Compliance By Server
Software
Software Compliance By Policy
Software Compliance By Server
Compliance Full Details - Software By Policy Kiran
Application Configuration
App Config Compliance By Policy
App Config Compliance By Server
Audit
Audit Compliance By Policy
Audit Compliance By Server and Policy
Compliance Full Details - Audit By Policy - Release
Audit Compliance By Audit
Audit Compliance By Server and Audit
Deployment Life Cycle
Discovered Software
Storage Reports
Process Automation Reports
Dashboard
Scheduled Reports
Reports
Advanced Search
Opsware Administration
Patch Compliance By Server
Run
Print
Export...
Schedule...

This report provides a full detailed breakdown of selected policies by their patch compliance status for selected managed servers, and displays exception details.

Date: Equals Mon 03/30/2009
Patch Policy: Equals 2003 new patch policy
Device Group: Equals [Any Value]
Server: Contains
Patch Status: Equals [Any Value]

**Patch Compliance By Server**

Generated on: Mon Mar 30 15:06:26 2009 PDT

This report provides a full detailed breakdown of selected policies by their patch compliance status for selected managed servers, and displays exception details.

**Parameters**

| | |
|---|---|
| **Date:** | 03-30-09 |
| **Patch Policy:** | '2003 new patch policy' |
| **Device Group:** | Any Value |
| **Server:** | * |
| **Patch Status:** | Any Value |

**Server Summary**

| | | |
|---|---|---|
| ● | **Compliant:** | 1 |
| ▲ | **Partially Compliant:** | 0 |
| ✕ | **Non-Compliant:** | 0 |
| □ | **Scan Needed:** | 2 |
| ● | **Scan Failed:** | 0 |
| | **Total:** | 3 |

| | |
|---|---|
| ● **Server Name:** | 2k3-1.tony2008.qa.opsware.com |
| **Status:** | Compliant |
| **Compliant Policies:** | 1/1 |
| **Compliant Patches:** | 1/1 |
| **Exceptions:** | 0 |
| **Last Scan:** | Fri Mar 27 11:39:42 2009 |
| ● **Policy Name:** | 2003 new patch policy |
| **Status:** | Compliant |
| **Compliant Patches:** | 1/1 |
| **Exceptions:** | 0 |

| | Patch Name | On Server | Exception |
|---|---|---|---|
| ● | MS04-007(KB828028) | Yes | - |

| | |
|---|---|
| □ **Server Name:** | M282-W2K3-VM3 |
| **Status:** | Scan Needed |
| **Compliant Policies:** | 0/1 |

kmakala Mon Mar 30 15:05 2009 America/Los_Angeles

# Servers Without Policies by Policy Type

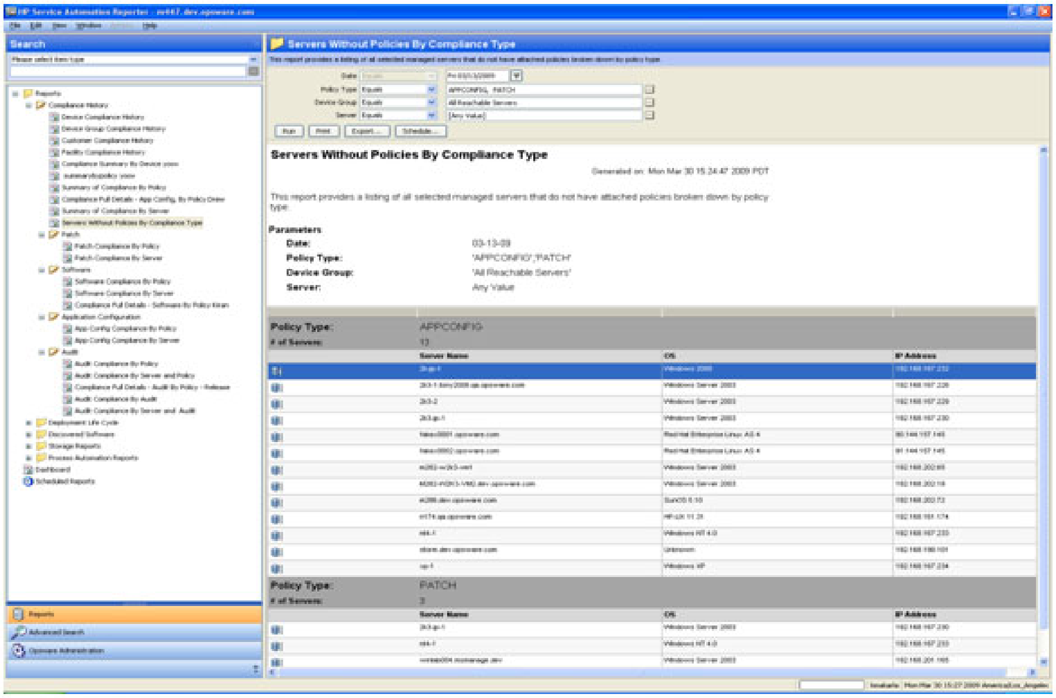
## Table

- Report lists servers that are do not have any policies attached to them.
- Servers are grouped by policy type, with the name of each server listed.
- A server can be listed under multiple policy type sections. For example server S1 can be listed in 'Audit Policy' type section and 'Software Policy' type section, if it is has only patch & App Config polices.
- Counts reflect current managed/active servers only.

## Actionable

Double Click / Right Click on a server and select 'Open' to launch SA Server browser window. Various possible operations on the server are subject to user permission

**Figure 17 Servers Without Policies By Compliance Type**



Servers Without Policies By Compliance Type

This report provides a listing of all selected managed servers that do not have attached policies broken down by policy type.

Date: Fri 03/13/2009

Policy Type: Equals APPCONFIG, PATCH

Device Group: Equals All Reachable Servers

Server: Equals [Any Value]

**Servers Without Policies By Compliance Type**

Generated on: Mon Mar 30 15:24:47 2009 PDT

This report provides a listing of all selected managed servers that do not have attached policies broken down by policy type.

**Parameters**

**Date:** 03-13-09

**Policy Type:** 'APPCONFIG','PATCH'

**Device Group:** 'All Reachable Servers'

**Server:** Any Value

**Policy Type:** APPCONFIG

**# of Servers:** 13

| Server Name | OS | IP Address |
|---|---|---|
| 2k-qa-1 | Windows 2000 | 192.168.197.232 |
| 2k3-1-bmy2008.qa.opsware.com | Windows Server 2003 | 192.168.197.228 |
| 2k3-2 | Windows Server 2003 | 192.168.197.229 |
| 2k3-qa-1 | Windows Server 2003 | 192.168.197.230 |
| hawx0001.opsware.com | Red Hat Enterprise Linux AS 4 | 90.144.157.145 |
| hawx0002.opsware.com | Red Hat Enterprise Linux AS 4 | 91.144.157.145 |
| m202-w2k3-vm1 | Windows Server 2003 | 192.168.202.65 |
| M202-W2K3-VM2.dev.opsware.com | Windows Server 2003 | 192.168.202.18 |
| m206.dev.opsware.com | SunOS 5.10 | 192.168.202.72 |
| m174.qa.opsware.com | HP-UX 11.31 | 192.168.191.174 |
| nt4-1 | Windows NT 4.0 | 192.168.197.233 |
| storm.dev.opsware.com | Unknown | 192.168.198.101 |
| xp-1 | Windows XP | 192.168.197.234 |

**Policy Type:** PATCH

**# of Servers:** 3

| Server Name | OS | IP Address |
|---|---|---|
| 2k3-qa-1 | Windows Server 2003 | 192.168.197.230 |
| nt4-1 | Windows NT 4.0 | 192.168.197.233 |
| wintab004.ncmanage.dev | Windows Server 2003 | 192.168.201.165 |

# 3 Glossary

## Generated On

Date the report is generated on with the data-time format as specified in the SA User Profile in SAS Web Client.

## Status

- Compliance Status of Server /Item: Status roll up is computed with worst case as cumulative status. Status bubbles up or rolls up from good to worst i.e. Compliance -> Partially Complaint (patch only) -> Non-Compliant -> Scan Needed -> Scan Failed.
- Compliance Status of Policy: Status roll up is computed with worst case being 'Scan Failure'. Status precedence from good to worst is Compliance -> Non-Compliant -> Scan Needed -> Scan Failed

## Last Scan

Date of last scan on which the compliance status is computed. Date format is same as that of user specified in the SA User Profile.

## Compliant Rules/Items/Files

Numerator specifies the number of compliant Rules/Items/Files with in a given policy, where as the denominator specifies total number of Rules/Items/Files with in a policy

## Compliant Servers

Numerator specifies the number of compliant servers for a given policy, where as the denominator specifies total number of server that are attached to a policy

## On Server

Determines if a particular version of patch item / software unit / App Config file exists on the server

## Exceptions

An exception can be created within a policy and can have details such as exception expiration date and details on exception itself.