HP 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 9.10 and BSA Essentials 2.0

Reports Guide

Document Release Date: June 2011
Software Release Date: June 2011

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

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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) reports. There are two venues for SA reports, SA Client reports that are available in the SA Client, and BSA Essentials (BSAE) reports that are distributed through the HP Live Network.

For the BSA Essentials reports with streamed content, you can get the latest version of documentation from the HP Live Network at http://www.hp.com/go/livenetwork. See BSAE Reporting Prerequisites on page 8 for additional details.

In this section:

SA Client Reports

SA Client reports provide real-time information about managed servers, virtual servers, network devices, and user and security permissions in your environment. They are parameterized and actionable—which means that you can perform appropriate actions on objects, such as a policy or an audit, within the report. These reports are also exportable to your local file system (as .html, .pdf, or .xls files) to facilitate use within your organization.

See SA Client Reports on page 61.

BSA Essentials Reports for SA

BSA Essentials (BSAE) provides both high level and detailed historical reporting on your data center's automation processes for Server Automation (SA). BSAE gives you insight through rich reporting on the cost effectiveness and return on investments (ROI) for the automated processes in your data center. BSAE also provides a window into the compliance state of your servers, devices, and business applications.

The following two SA report types are viewable in the BSA Essentials Java Client:

- **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 HP Live Network using the bsae_sa_reports stream.

SA General Reports via BSAE on page 11 describes these reports.

- **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 HP Live Network using the sar78_reports stream.

  SA Compliance Reports via BSAE on page 33 describes these reports.

- **BSAE Custom Reports**

  See the BSAE Client Help for instructions on creating custom reports.

To get started with BSAE reports, see BSAE Reporting Prerequisites on page 8.

BSAE Reporting Prerequisites

To run the BSAE reports for SA, you must meet the following requirements:

- Have a BSA Essentials account.
  - — You can request a BSA Essentials account from the HP Live Network.
- Have the BSA Essentials Java Client installed.
- Have the HP Live Network connector (LNc), installed and configured on your core server. This is the client for the HP Live Network, which automates content updates, downloads, and imports into the product (SAS, BSAE, SAR).

  The LNc is installed with Server Automation. Refer to the LNc documentation for configuration instructions.

IMPORTANT: LNc will not list, download, preview, or import content if you do not have the proper products specified! See the *Live Network connector Users Guide* on the HP Live Network for instructions on enabling products.

- Subscribe to the relevant reports streams for your version of SA and the reports you wish to run. To download the report streams:
  - — Go to the HP Live Network and click the Live Network connector link.
  - — Download the LNc Users guide for instructions on using the HP Live Network and information about the correct report streams.
  - — Once the LNc has been configured for your specific product(s), you can also see a list of available streams via:

    ```
    live-network-connector list-streams
    ```

Additional information may be available on the individual streams by using the "`describe`" command. This information may provide a long text description and a URL for where to locate additional information on the specified Stream/content.

URLs:

- HP Live Network URL = http://www.hp.com/go/livenetwork.
- The HP documentation portal URL = http://h20230.www2.hp.com/selfsolve/manuals

For additional information about how to access and run these reports, see the online help in the respective BSAE Client.

2 SA General Reports via BSAE

This section describes the set of Server Automation (SA) general reports available through the BSAE Client. These reports can be downloaded from the BSA Essentials Network using the sar_reports stream.

In this section:

For additional information about how to access and run these reports, see the online help in the BSAE Client. For information about installing the BSAE Client that is available with the SA Client, see BSA Essentials Reports for SA on page 7.

Windows Patching Reports

This section describes the reports about your Windows patch policy compliance.

In this section:

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.)

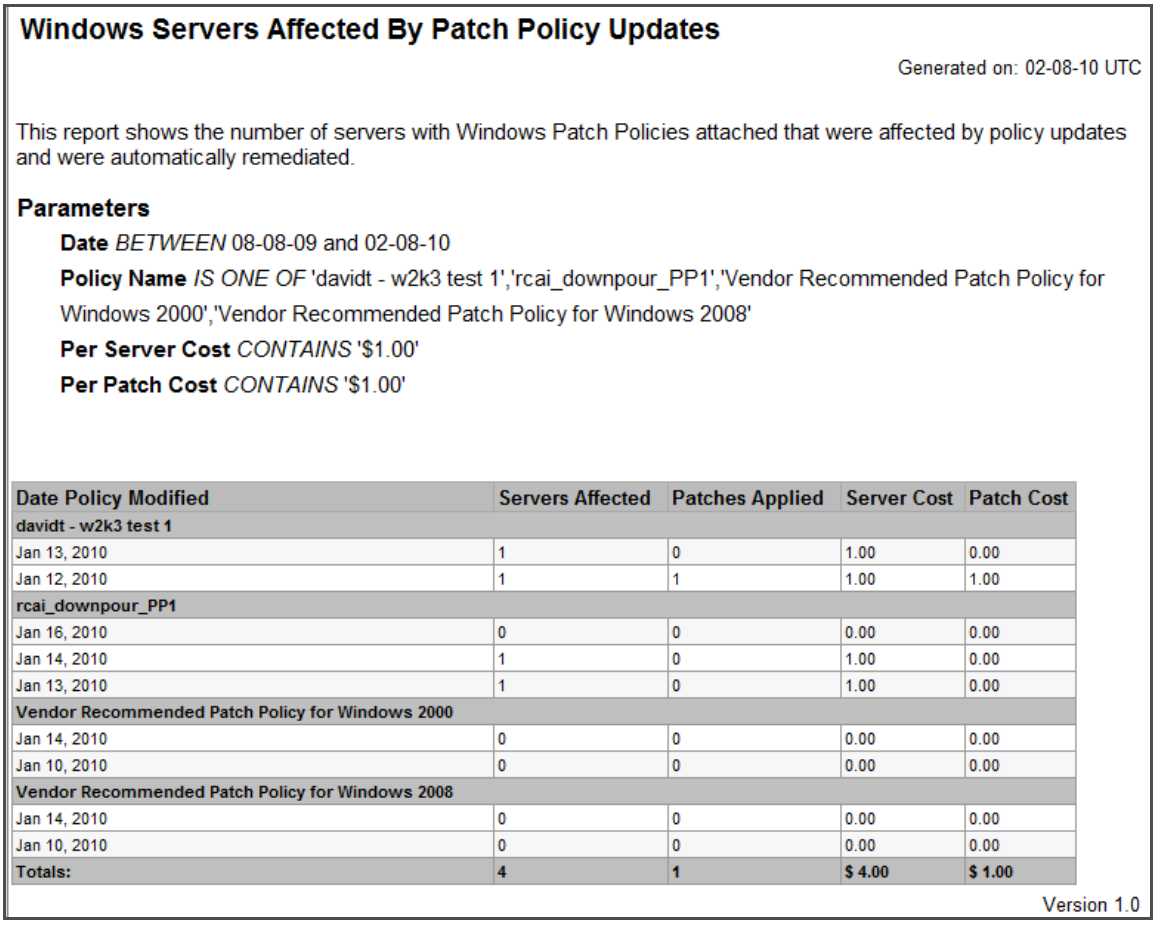
The Per Server Cost and Per Patch Cost parameters use the “Contains” operator, but is considered equivalent (“equals”) to the value you enter in these fields.

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.

In this section:

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.

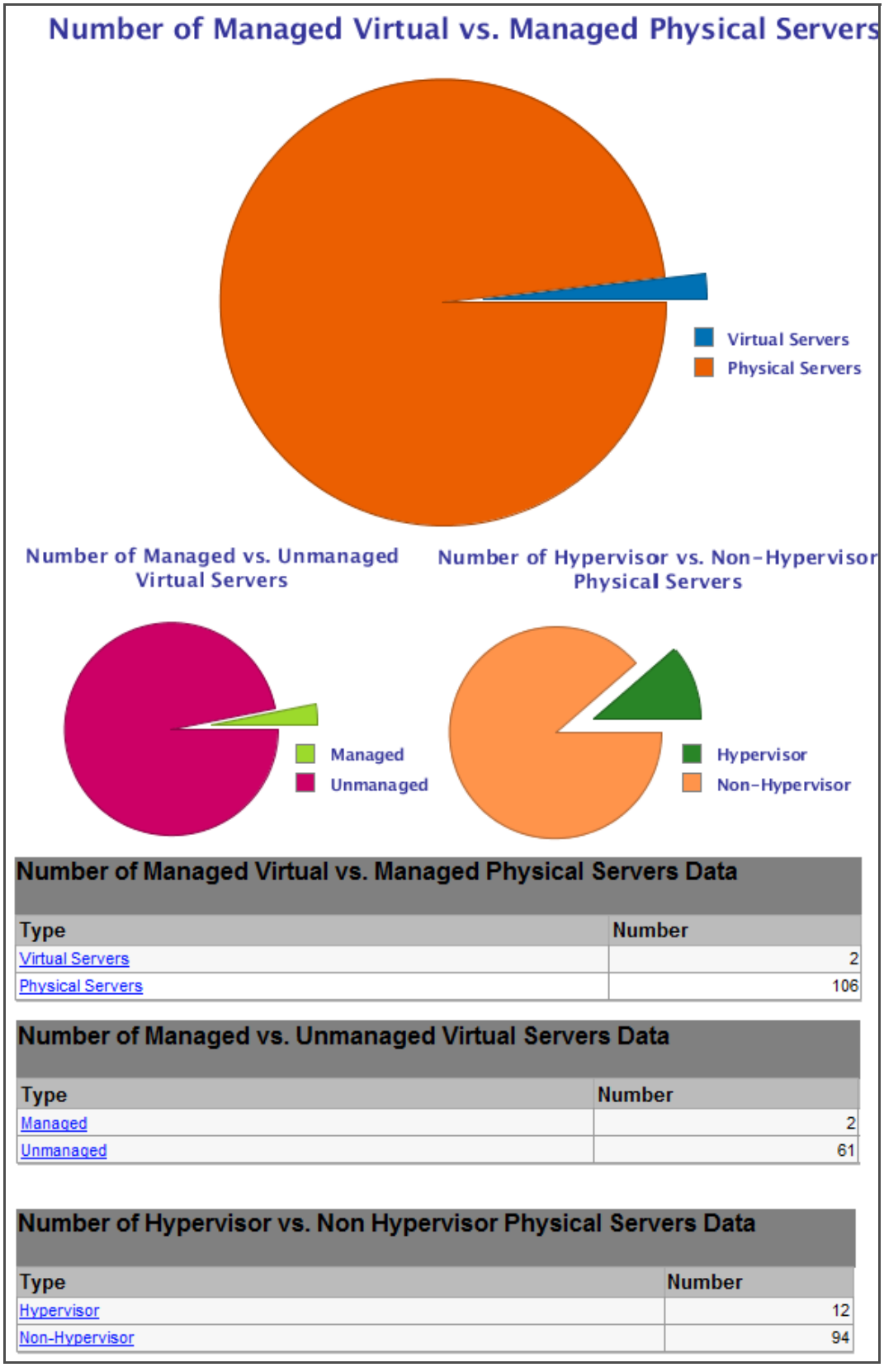
Tables

- 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 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.

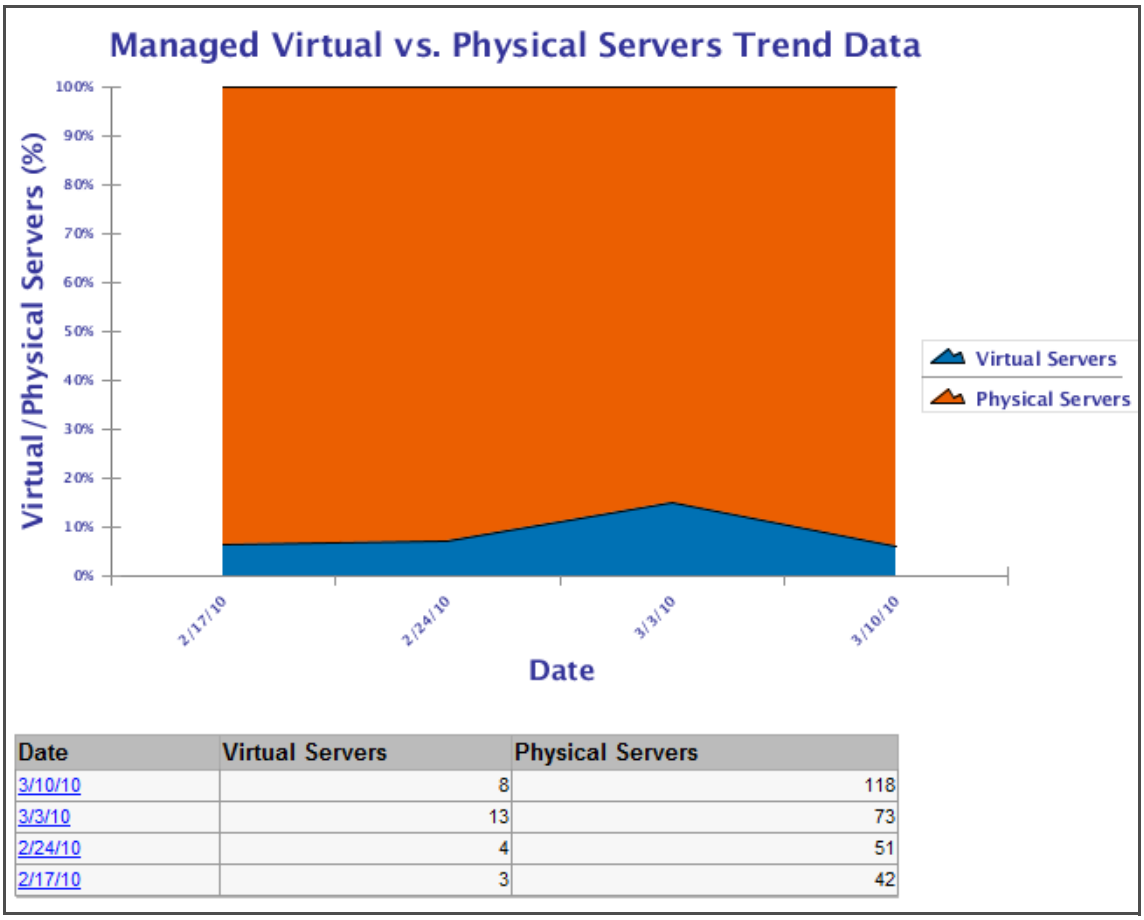
Table

- 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.

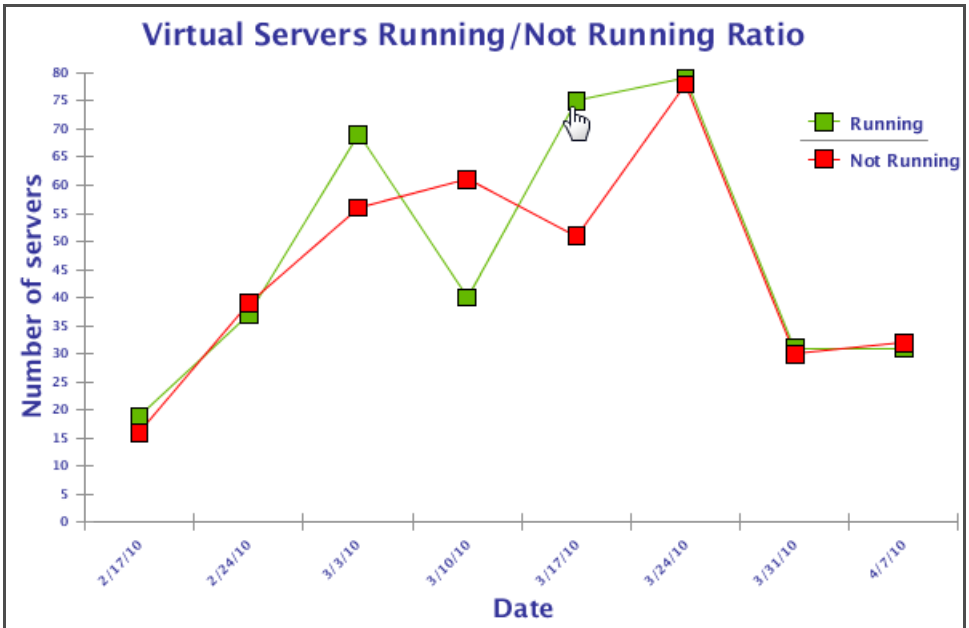
Table

- 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

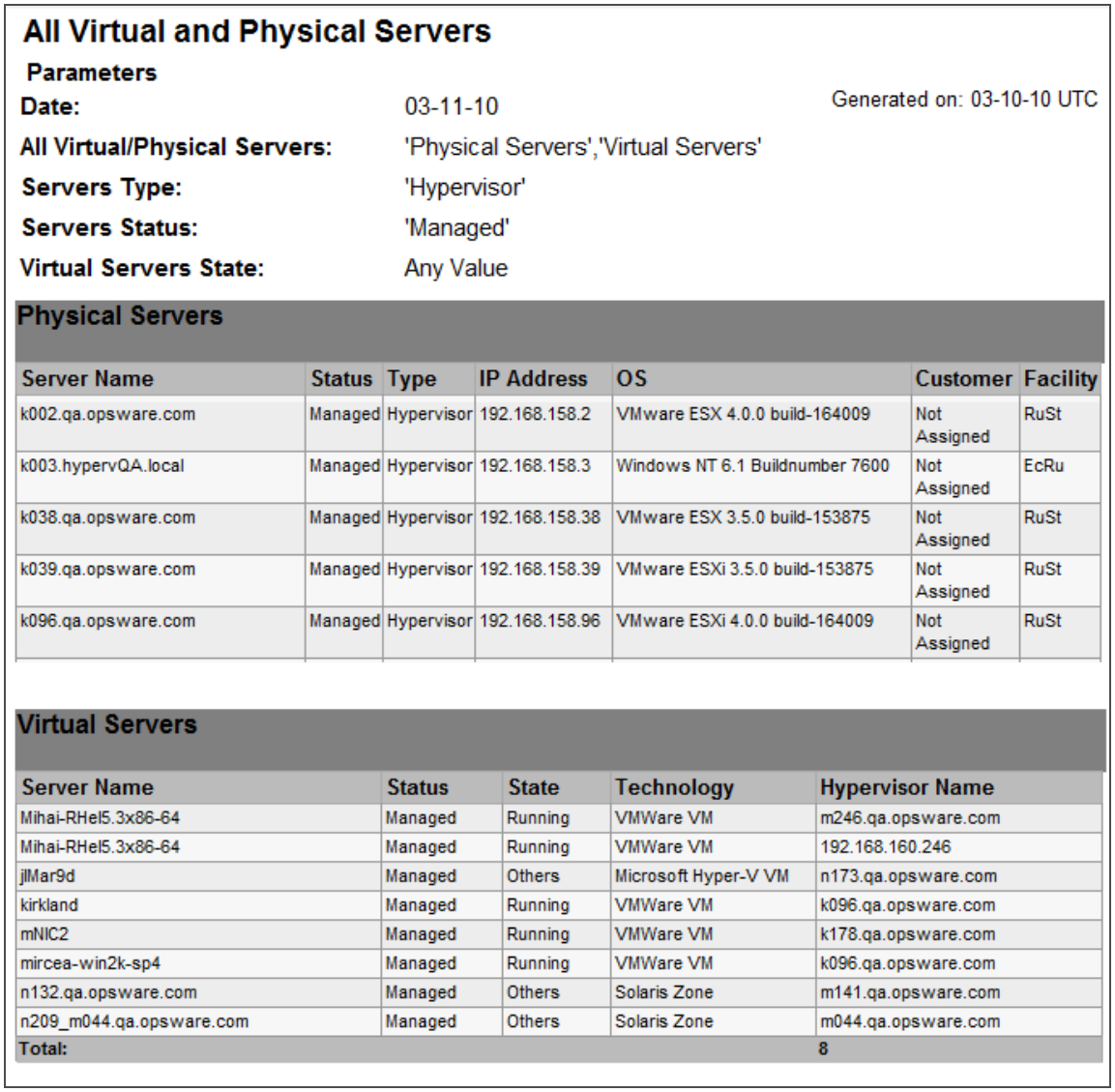


Date	Running	Not Running
4/7/10	31	32
3/31/10	31	30
3/24/10	79	78
3/17/10	75	51
3/10/10	40	61
3/3/10	69	56
2/24/10	37	39
2/17/10	19	16

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 report about your server deployments.

Server Deployments by Operating System

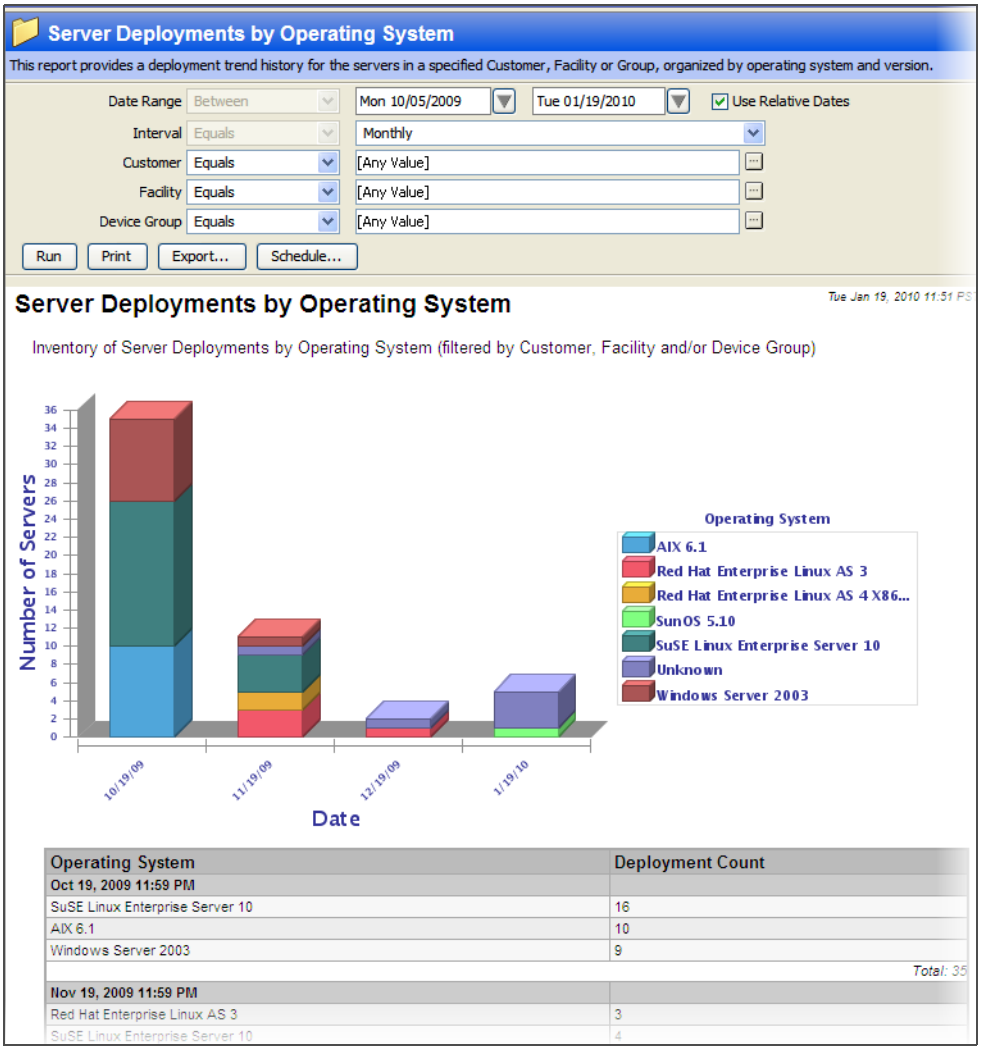
Table

- 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



Application Deployment Reports

This section describes the reports about Application Deployment activities performed in HP Server Automation.

In this section:

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

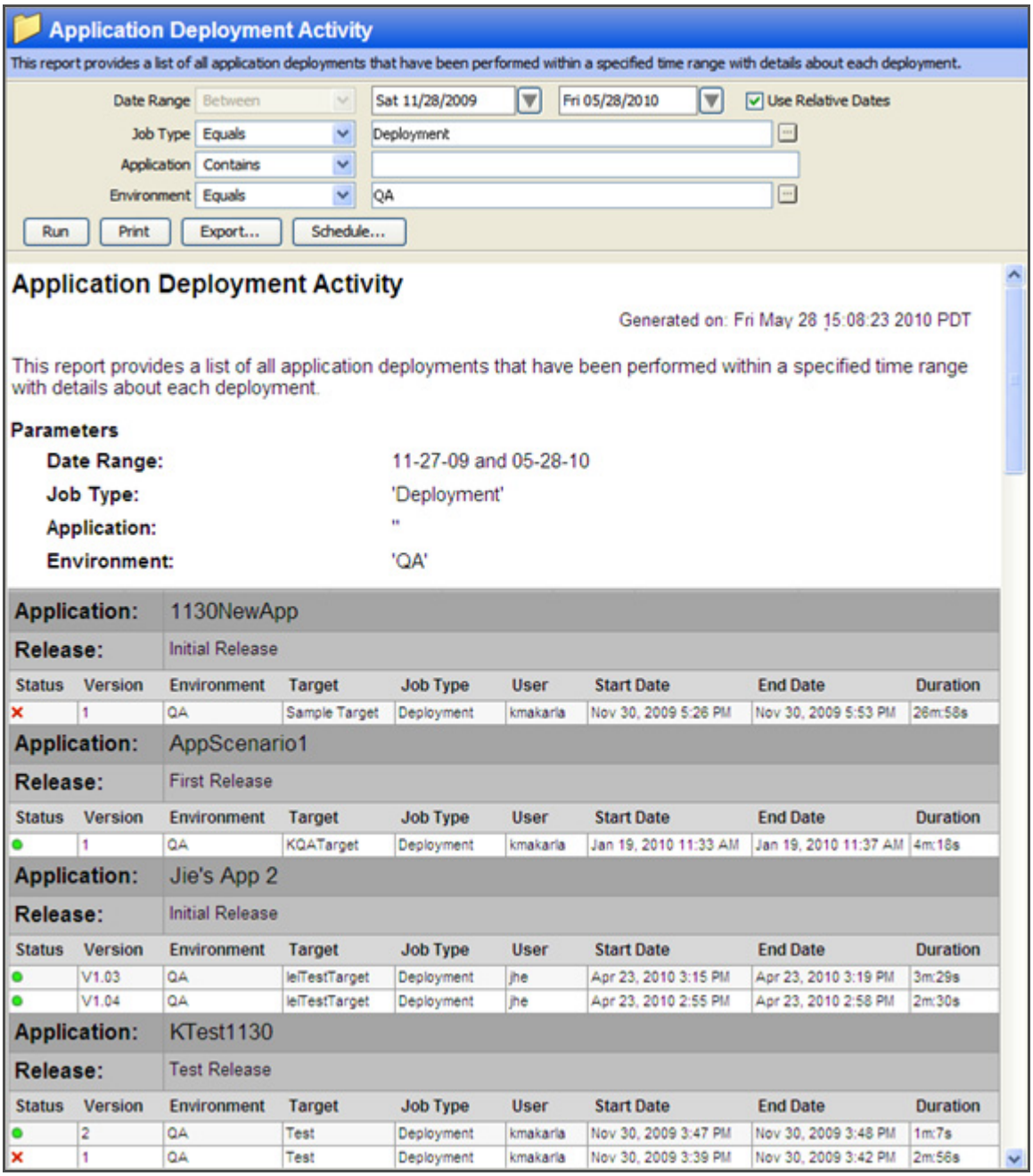
You can filter an Application Deployment Activity using any combination of the following:

- **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



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.

ROI values are intentionally provided without units. You can think of them in terms of currency, hours spent, or whatever units make sense for your organization.

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

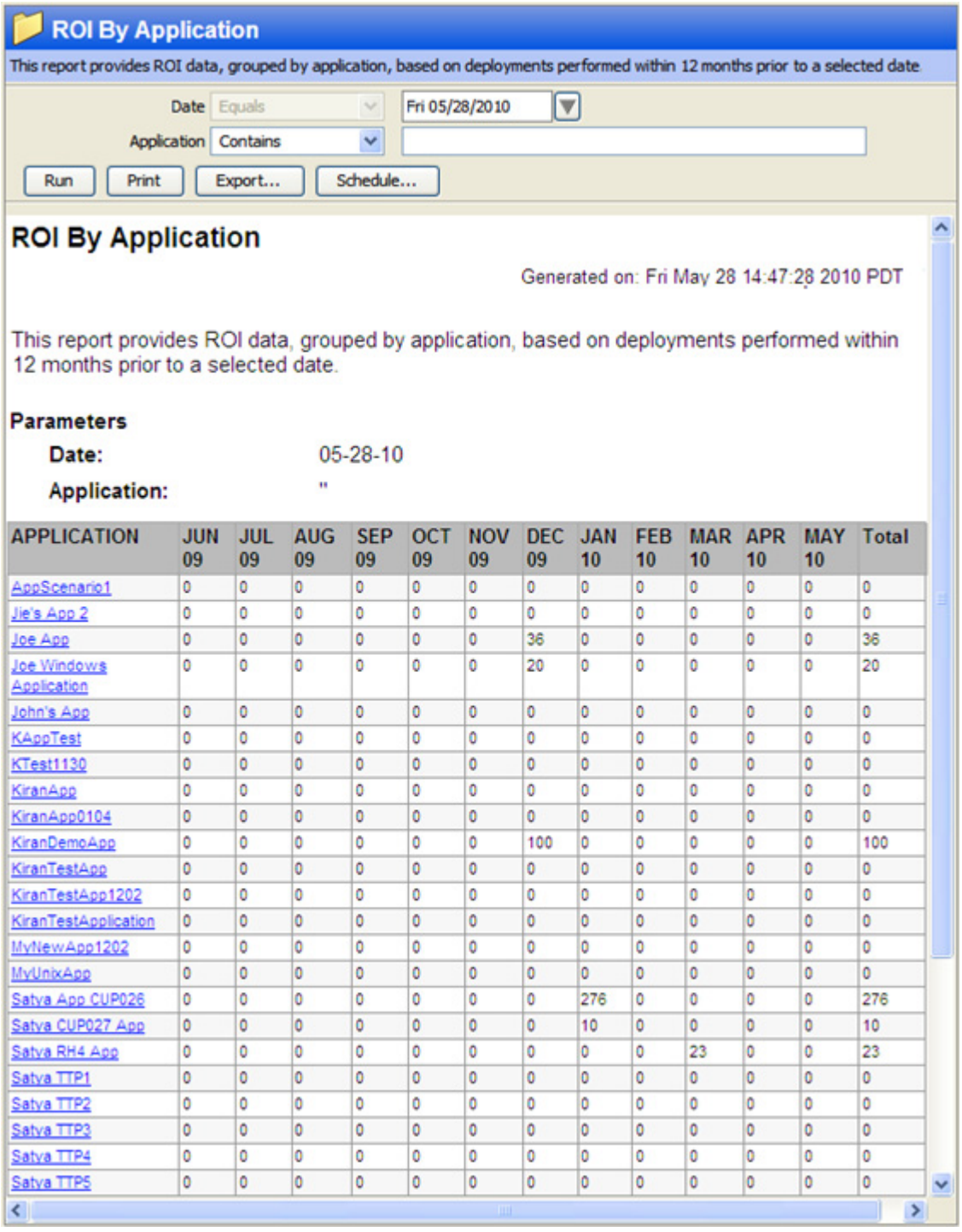
You can filter an ROI by Environment report using any combination of the following:

- **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



ROI By Application

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

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

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.

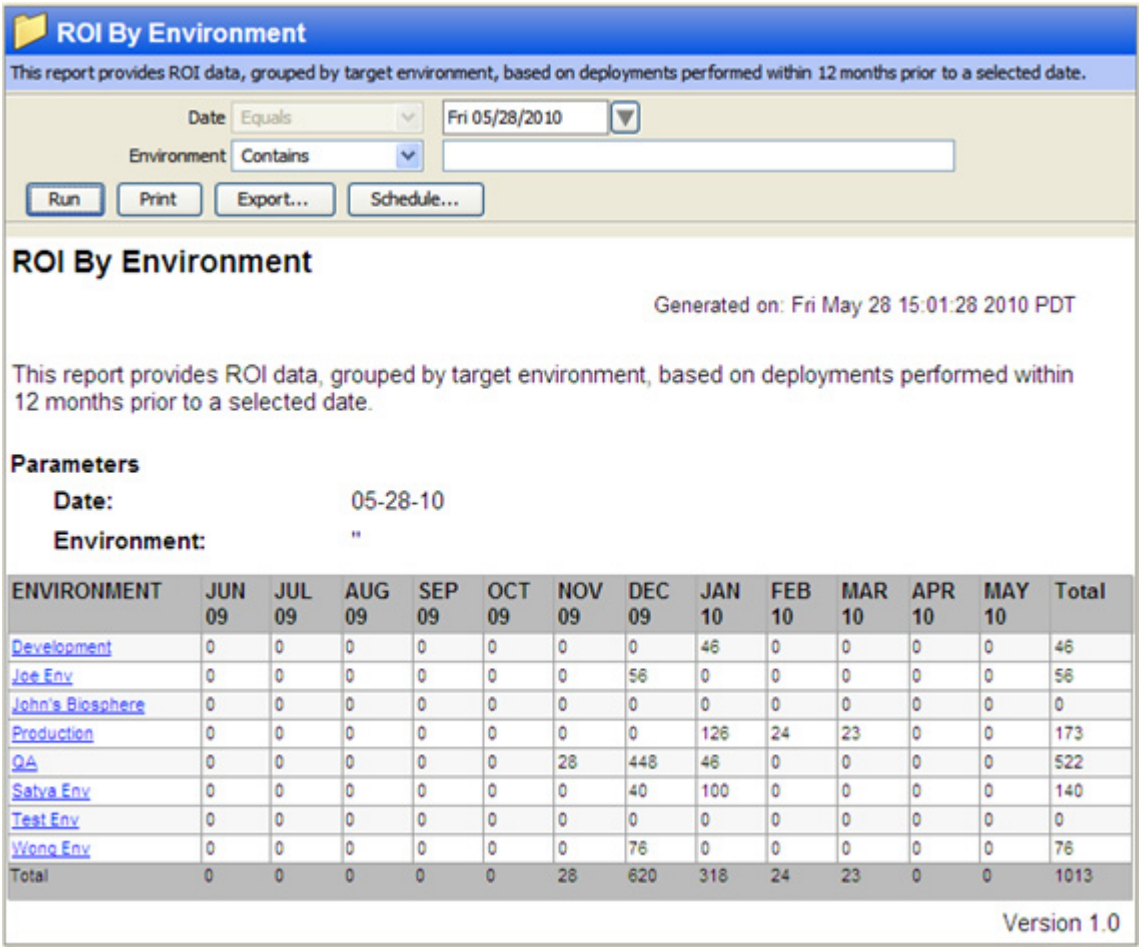
Parameters

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



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

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

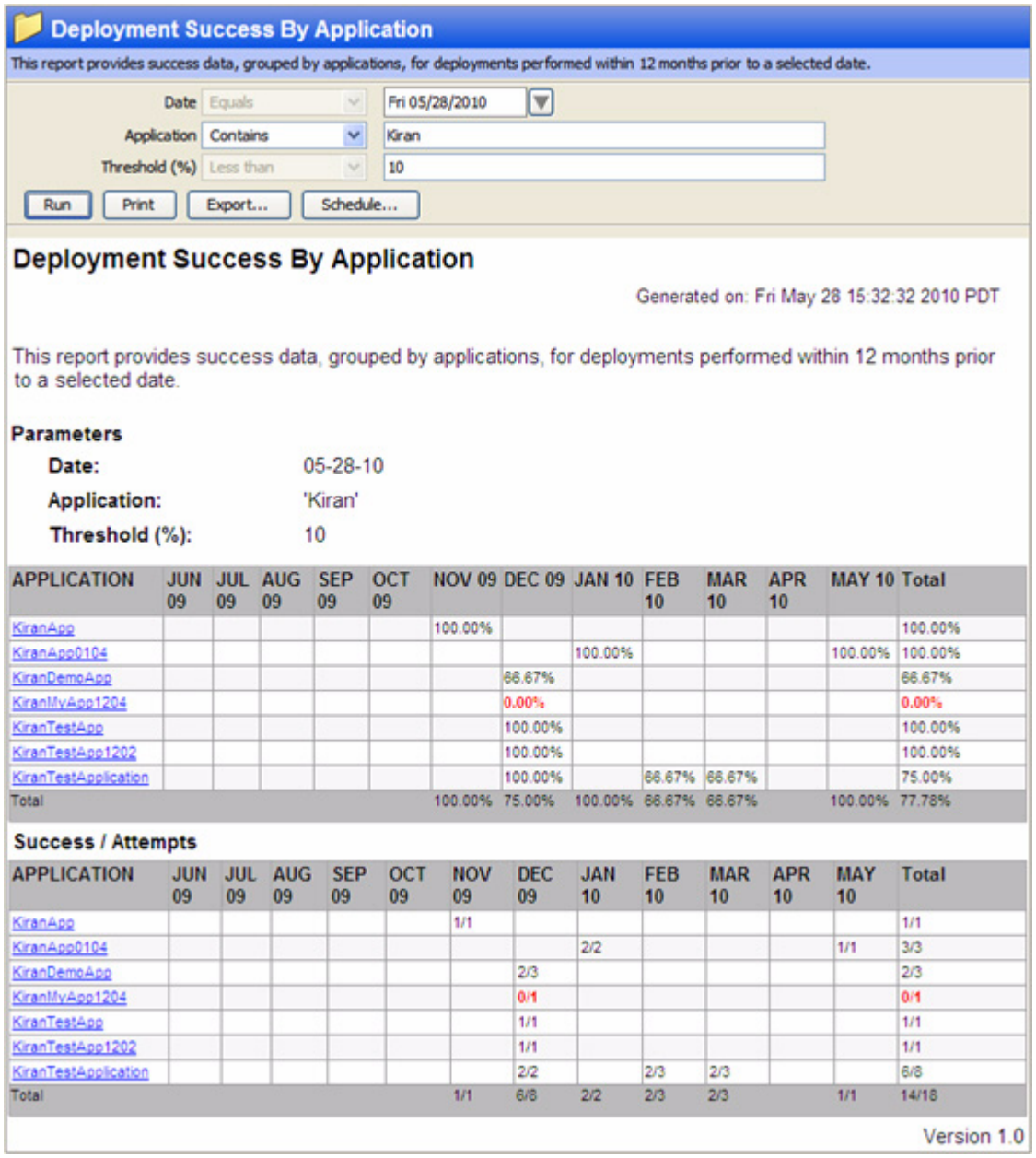
You can filter a Deployment Success by Environment report using any combination of the following:

- **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

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

Deployment Success By Application

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

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

Parameters

Date: 05-28-10

Application: 'Kiran'

Threshold (%): 10

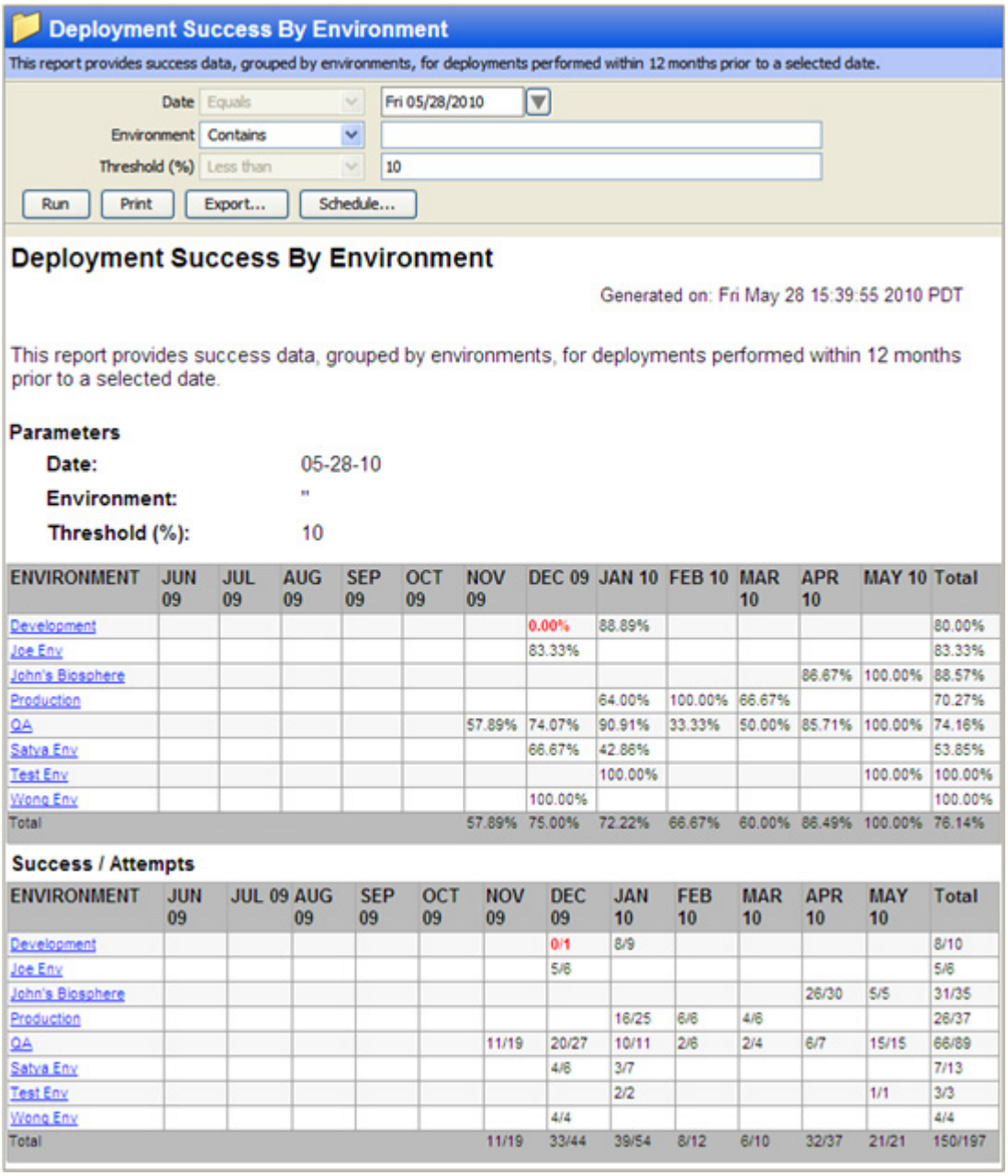
APPLICATION	JUN 09	JUL 09	AUG 09	SEP 09	OCT 09	NOV 09	DEC 09	JAN 10	FEB 10	MAR 10	APR 10	MAY 10	Total
KiranApp						100.00%							100.00%
KiranApp0104								100.00%				100.00%	100.00%
KiranDemoApp							66.67%						66.67%
KiranMyApp1204							0.00%						0.00%
KiranTestApp							100.00%						100.00%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

Success / Attempts

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

Version 1.0

Figure 12 Deployment Success by Environment Report



Deployment Success By Environment

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

Date: Equals Fri 05/28/2010

Environment: Contains

Threshold (%): Less than 10

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

Deployment Success By Environment

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

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

Parameters

Date: 05-28-10

Environment: ''

Threshold (%): 10

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

Success / Attempts

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

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

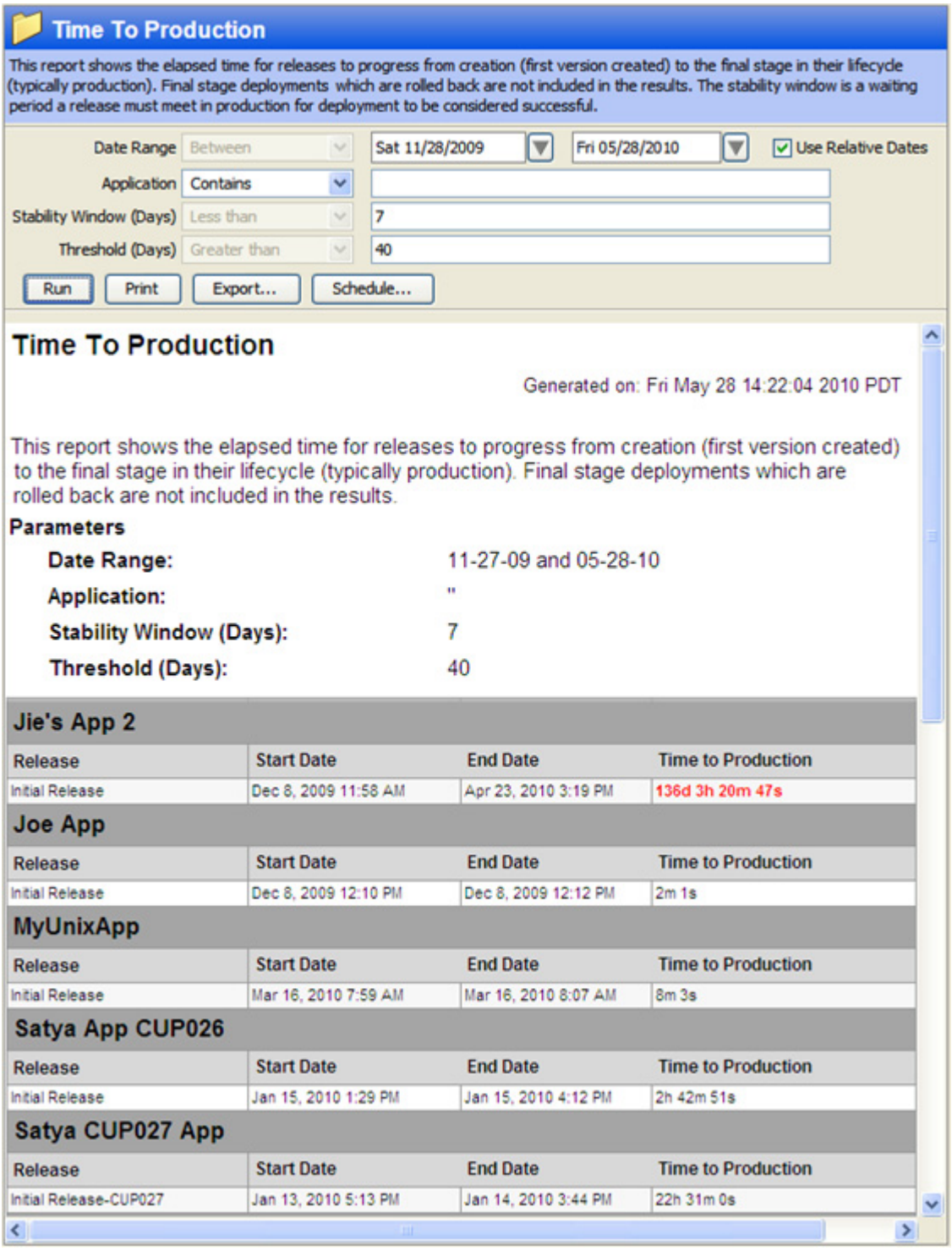
You can filter a Time to Production report by any combination of the following parameters:

- **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



Getting More Details

There is no drill-down available in this report.

3 SA Compliance Reports via BSAE

This section describes the current set of Server Automation (SA) compliance reports available through the BSAE Client. These reports can be downloaded from the BSA Essentials Network using the sar78_reports stream.

In this section:

The BSAE Client is available with the SA Client. For information about setting up the BSAE Client to run these SA Reports, see BSA Essentials Reports for SA on page 7. For additional information about how to access and run these reports, see the online help in the BSAE Client.

Terms Used in Compliance Reports

Term	Description
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.

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.

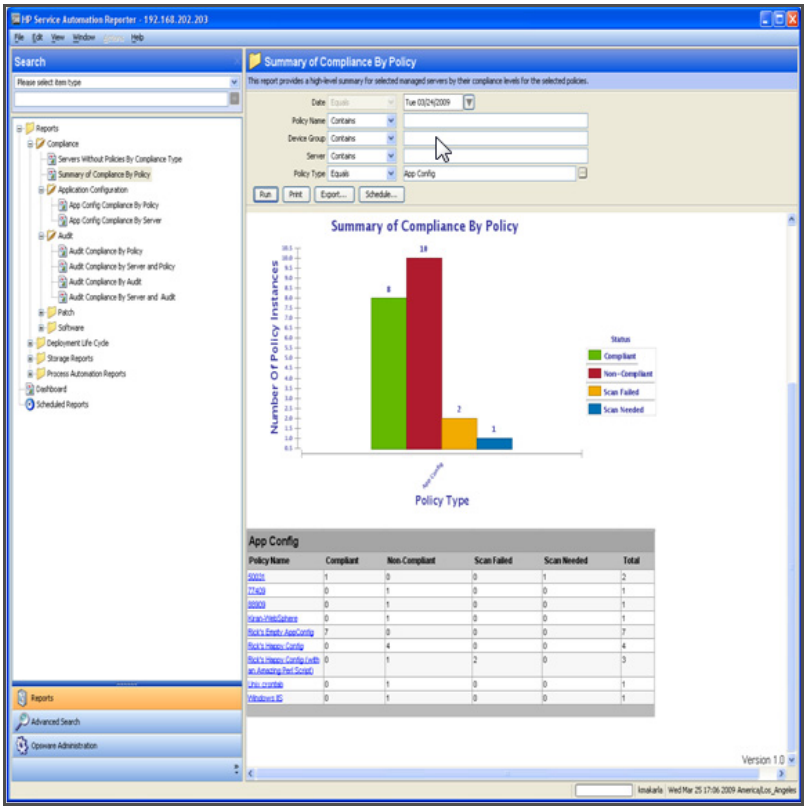
Table

- 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.

Getting More Details

- 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 14 Summary of Compliance By Policy



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.

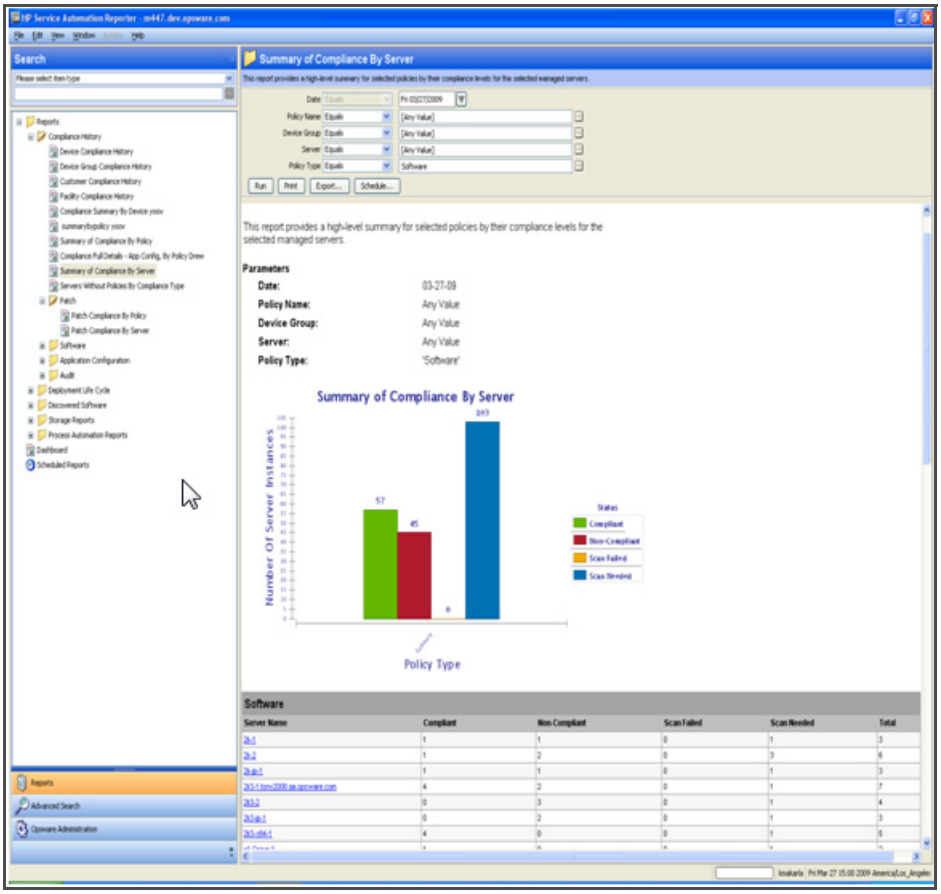
Table

- 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.

Getting More Details

- 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 15 Summary of Compliance By Server



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

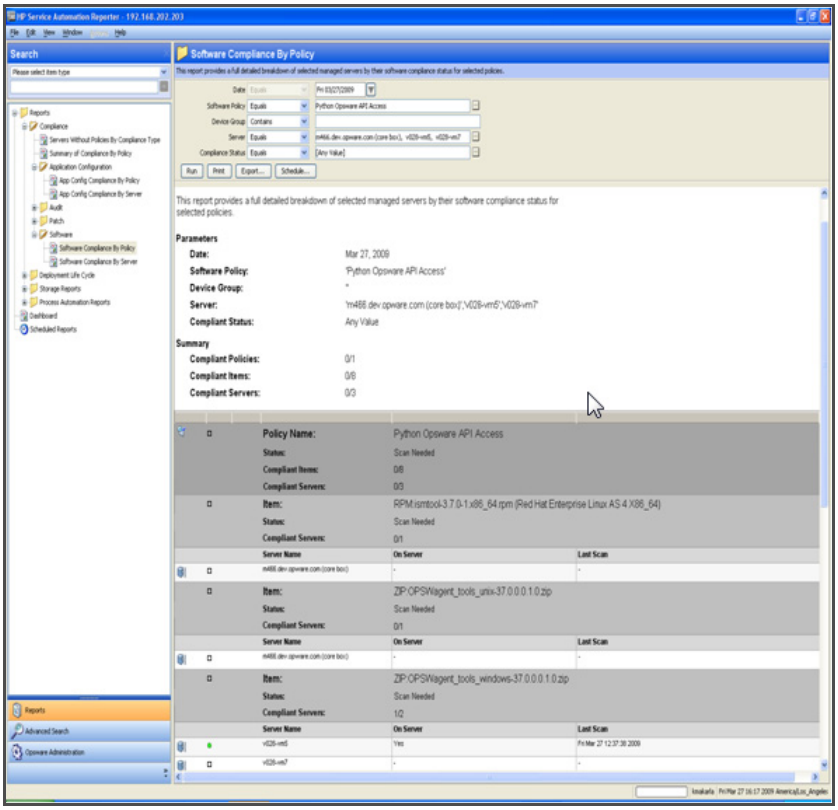
- A software policy can be attached to either a device group or directly to a server. When a policy is attached to device group, only servers with matching platform are reported
- Table is primarily grouped by policies. Each policy has compliance counts for each of its items and servers that are attached 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), 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.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 16 Software Compliance By Policy



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.

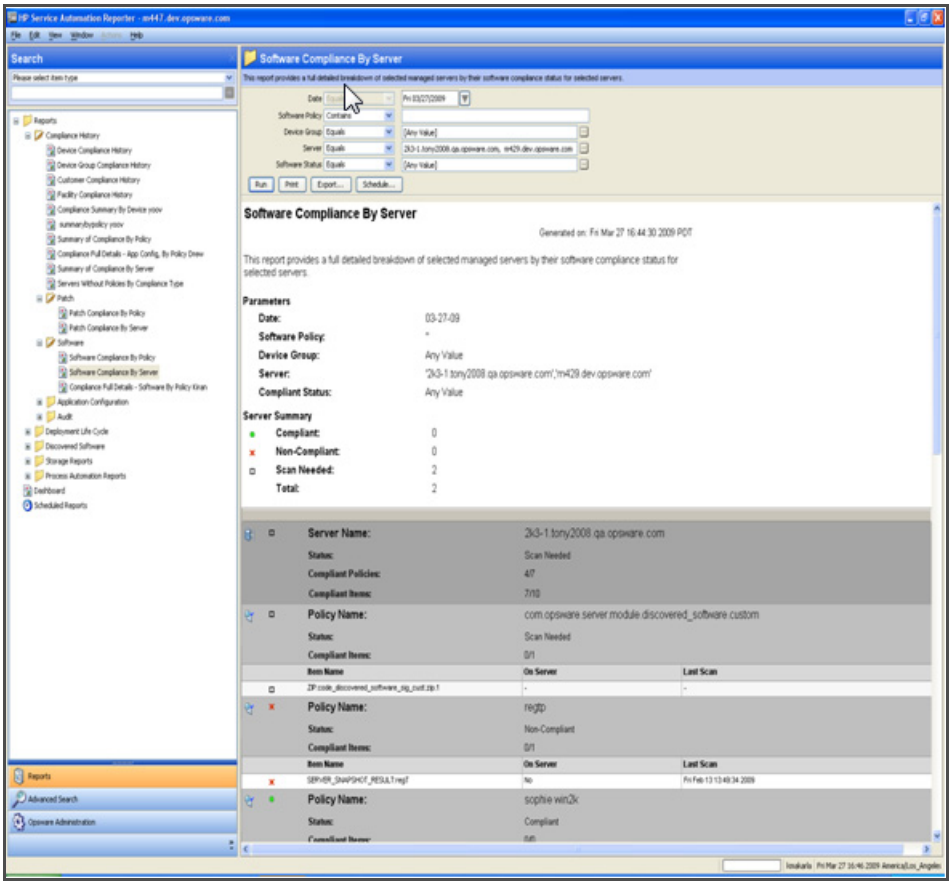
Table

- 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), 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.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 17 Software Compliance By Server



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

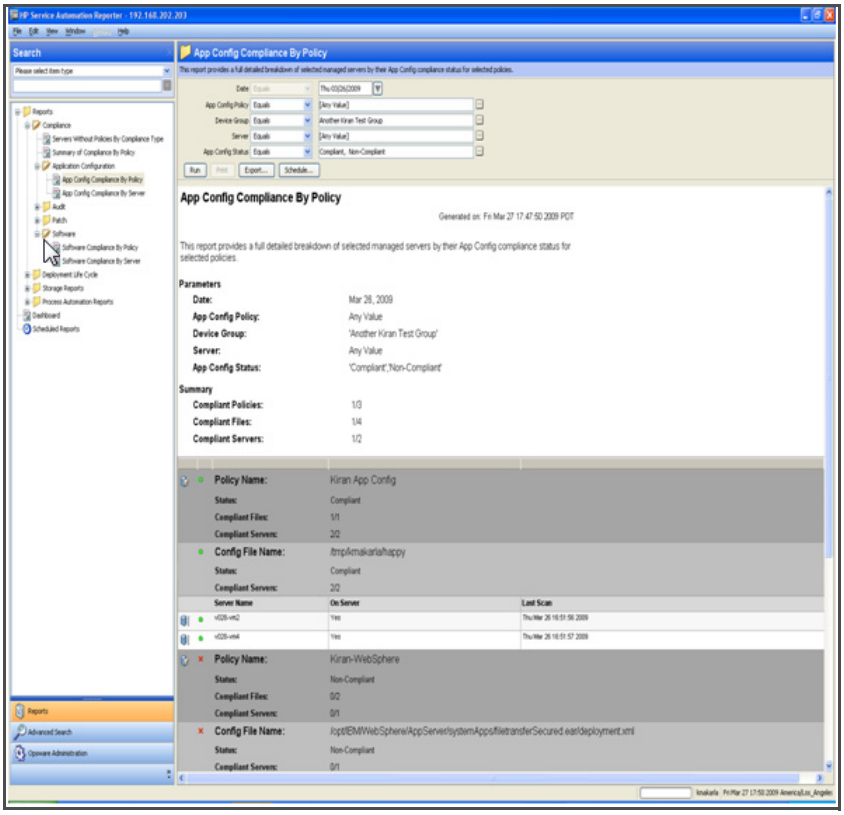
- An application configuration policy can be attached to either a device group or directly to a server. When a policy is attached to device group, a scan is needed in order for the system to recognize the server / policy attachment. Also, only servers with matching platform are reported
- Table is primarily 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.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 18 AppConfig Compliance By Policy



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.

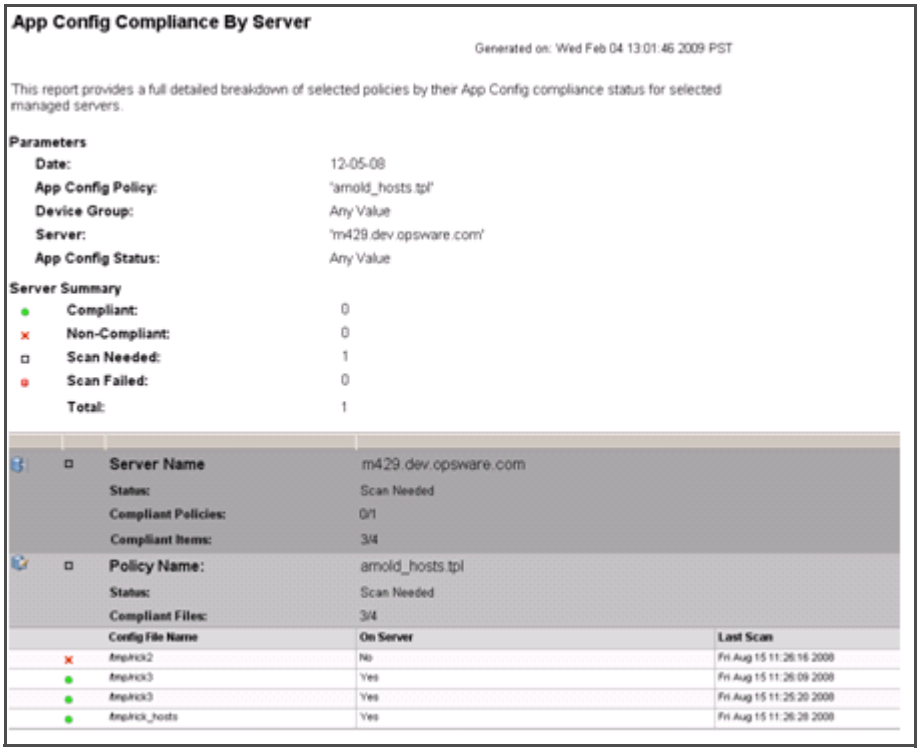
Table

- 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.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 19 AppConfig Compliance By Server



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.

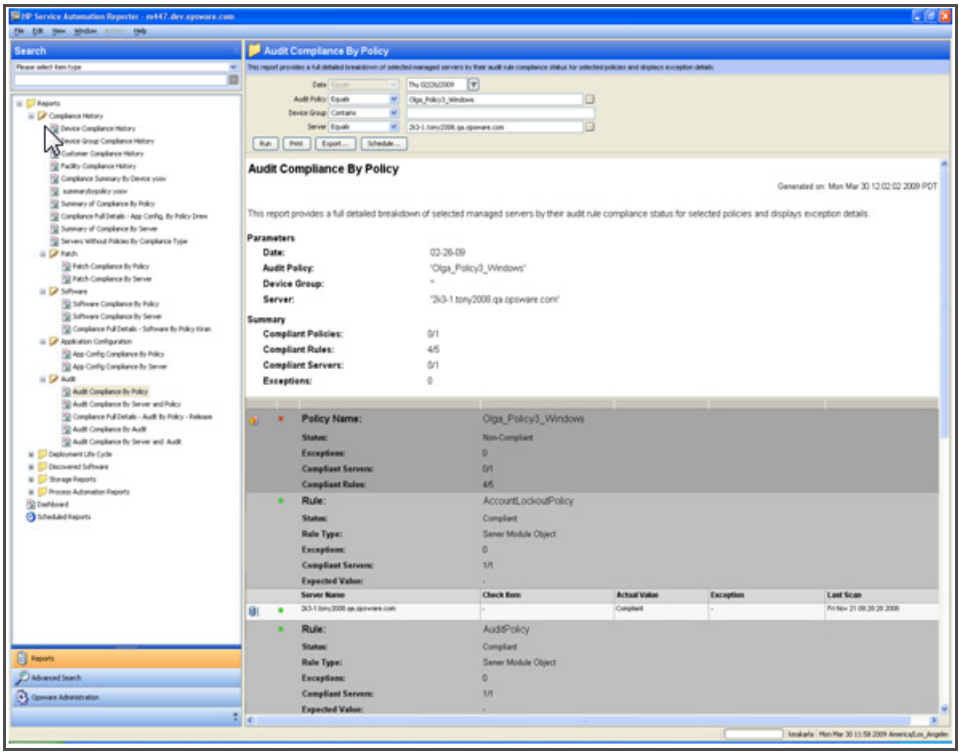
- Rules with in a policy will be reported only when a server it is attached to is scanned. In the event of scan failure or scan needed, only policy - server attachment details are reported.
- Audit details that are captured for each of the target server vary depending on individual rule types and type 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' check compares objects, files, and 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 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 20 Audit Compliance By Policy - Value-Based Checks



Comparison Based Checks

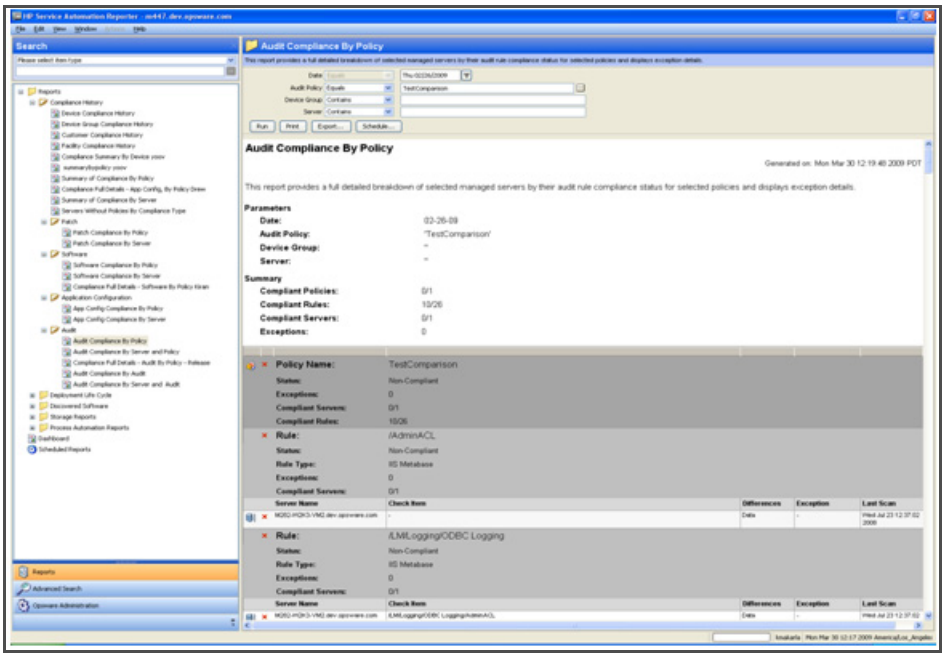
The following is a list of rule types on which *Comparison Based* checks can be performed and reported:

- Storage Initiator
- Check 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'.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 21 Audit Compliance By Policy - Comparison-Based Checks



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

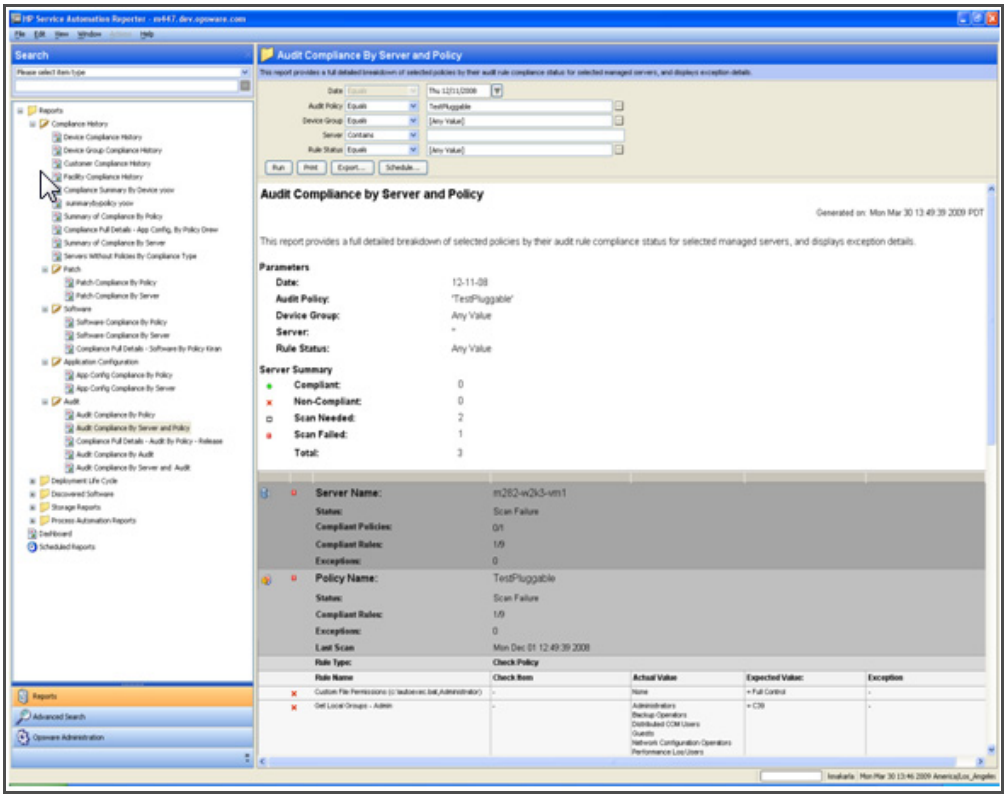
- Audit policy contains set of rules that are either defined within or extended from another policy. Multi level policy hierarchy is supported to create a composite policy.
- Table is primarily grouped by servers. Each server has compliance counts for each of the policy and rules within the policy that 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 22 Audit Compliance By Server and Policy - Value-Based Checks



Comparison Based Checks

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

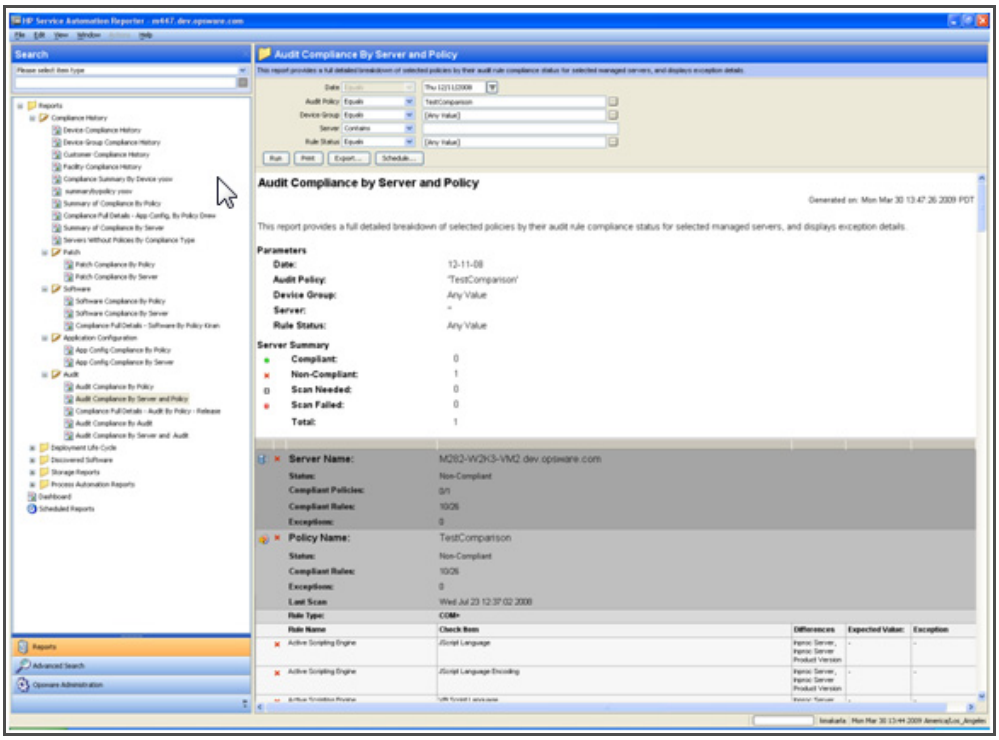
- Storage Initiator
- Check Policy / Pluggable Check
- Windows Services
- Registry
- COM+
- Custom Script
- Storage
- File System
- IIS Metabase
- Server Module Object
- Hardware

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'.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 23 Audit Compliance By Server and Policy - Comparison-Based Checks



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

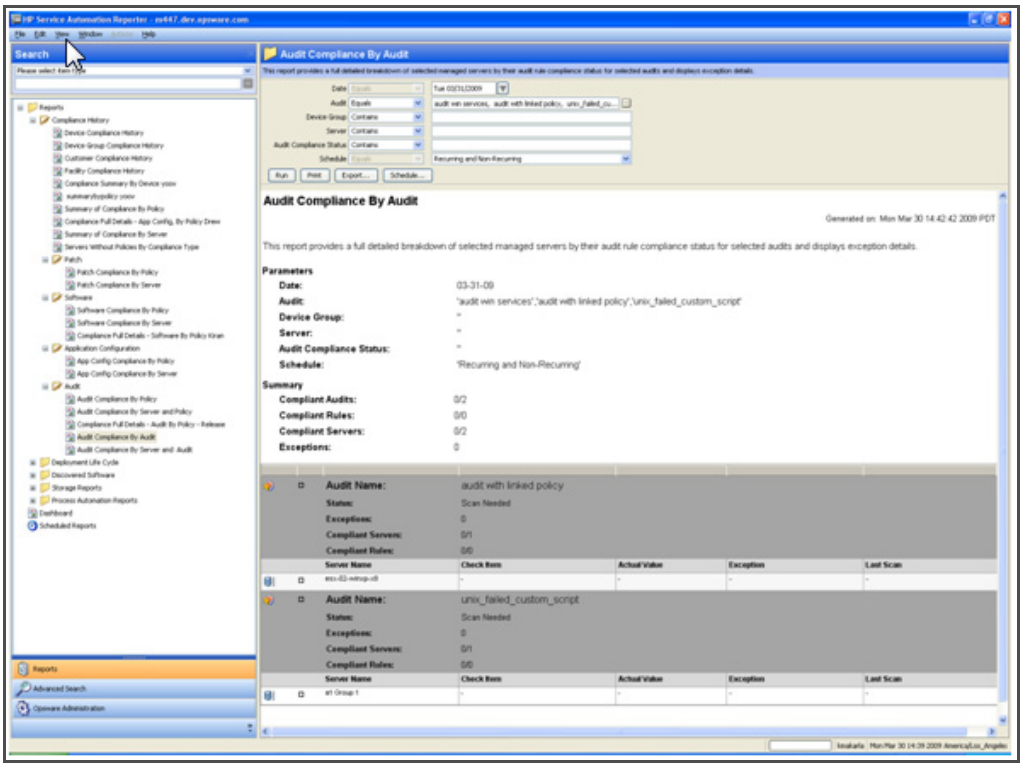
Value Based Checks

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 24 Audit Compliance By Audit - Value-Based Checks



Comparison Based Checks

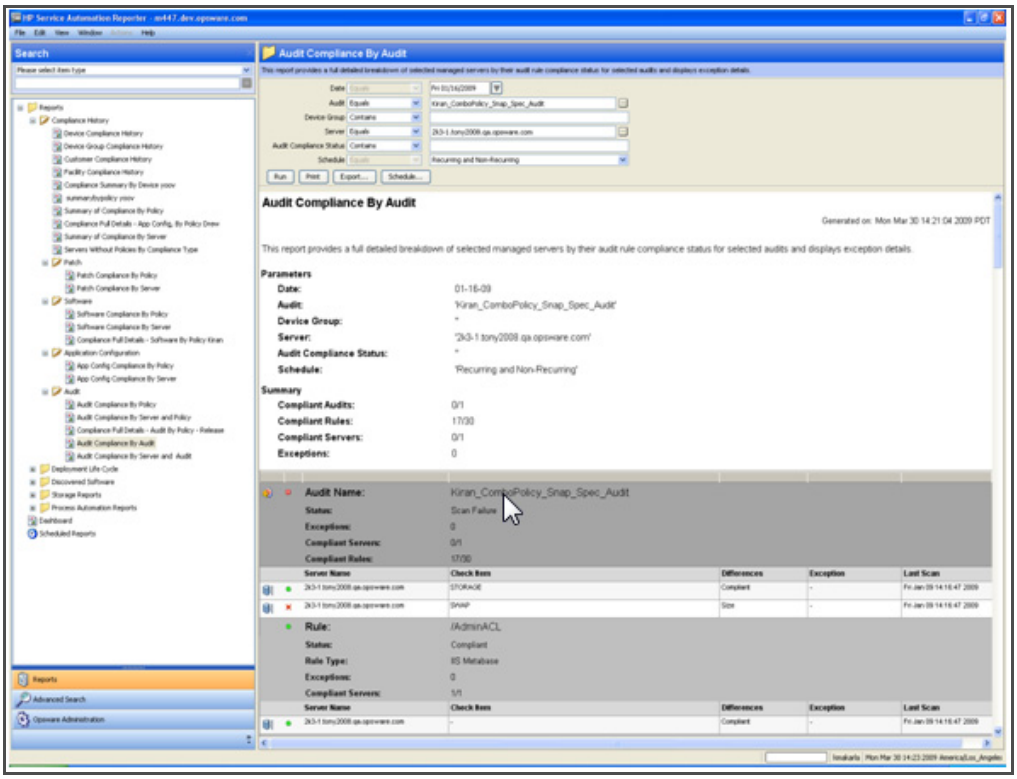
The following is a list of rule types on which 'Comparison Based' checks can be performed and reported:

- Storage Initiator
- Check 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'.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 25 Audit Compliance By Audit - Comparison-Based Checks



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

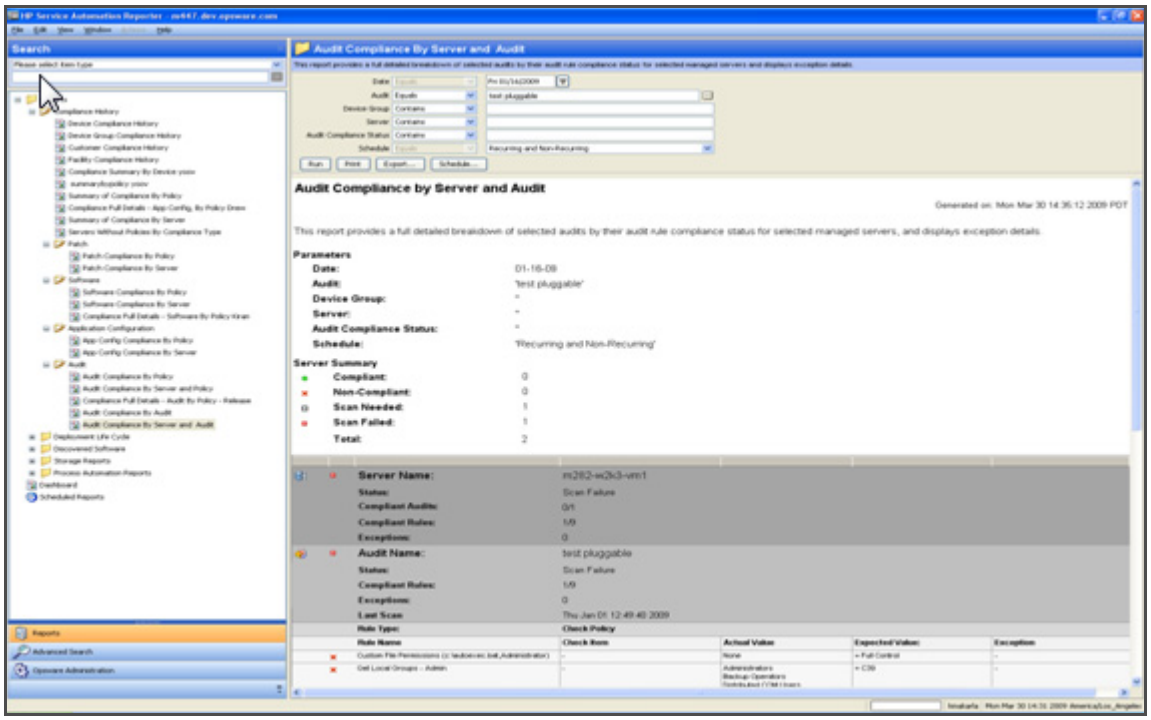
Value Based Checks

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 26 Audit Compliance By Server and Audit - Value-Based Checks



Comparison Based Checks

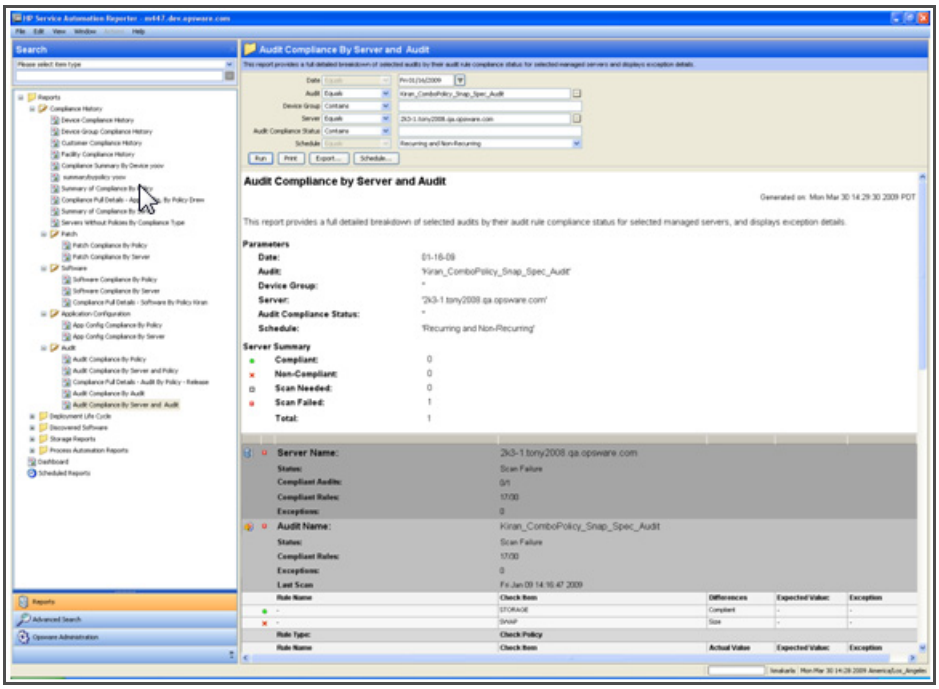
The Following are list of rule types on which 'Comparison Based' checks can be performed and reported:

- Storage Initiator
- Check 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'.

Acting on Details

- Double-click / Right-click on an audit and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 27 Audit Compliance By Server and Audit - Comparison-Based Checks



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

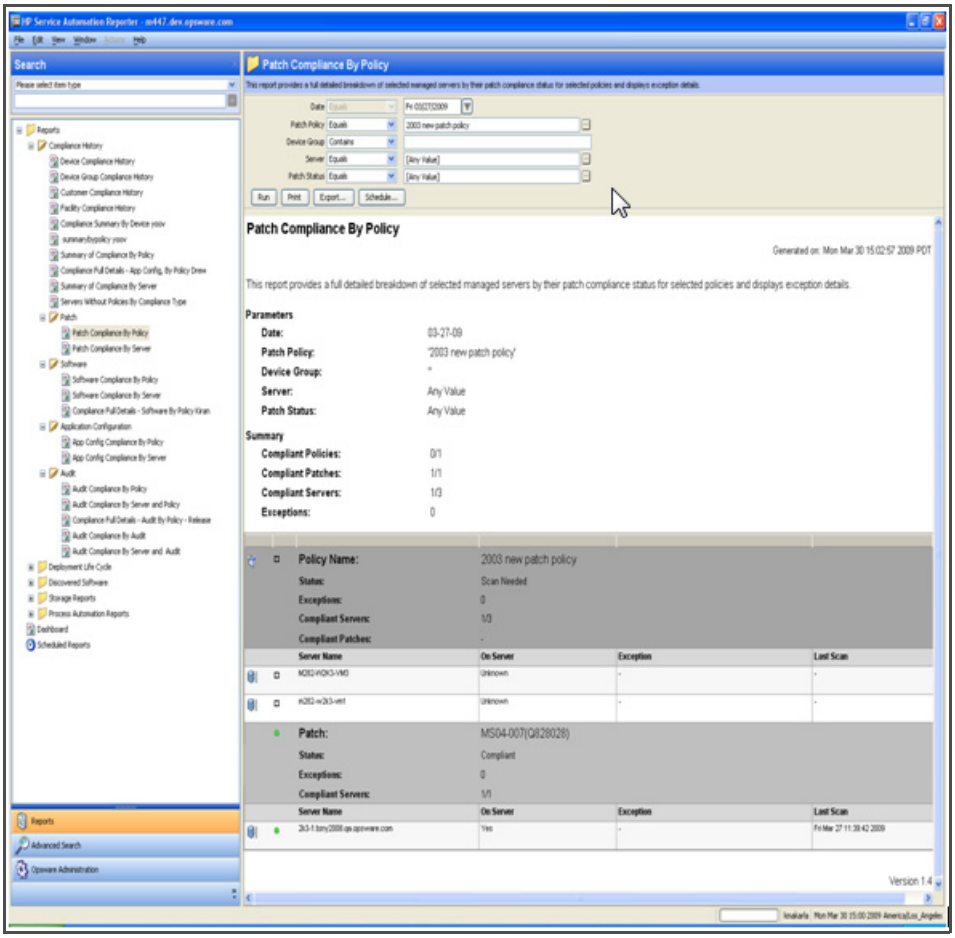
- A patch policy can be attached to either a device group or directly to a server. Only servers with matching platform are reported.
- A device group can have another device group i.e. nested device group. A patch policy can be attached to nested device group. By default only servers directly attached 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

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 28 Patch Compliance By Policy



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.

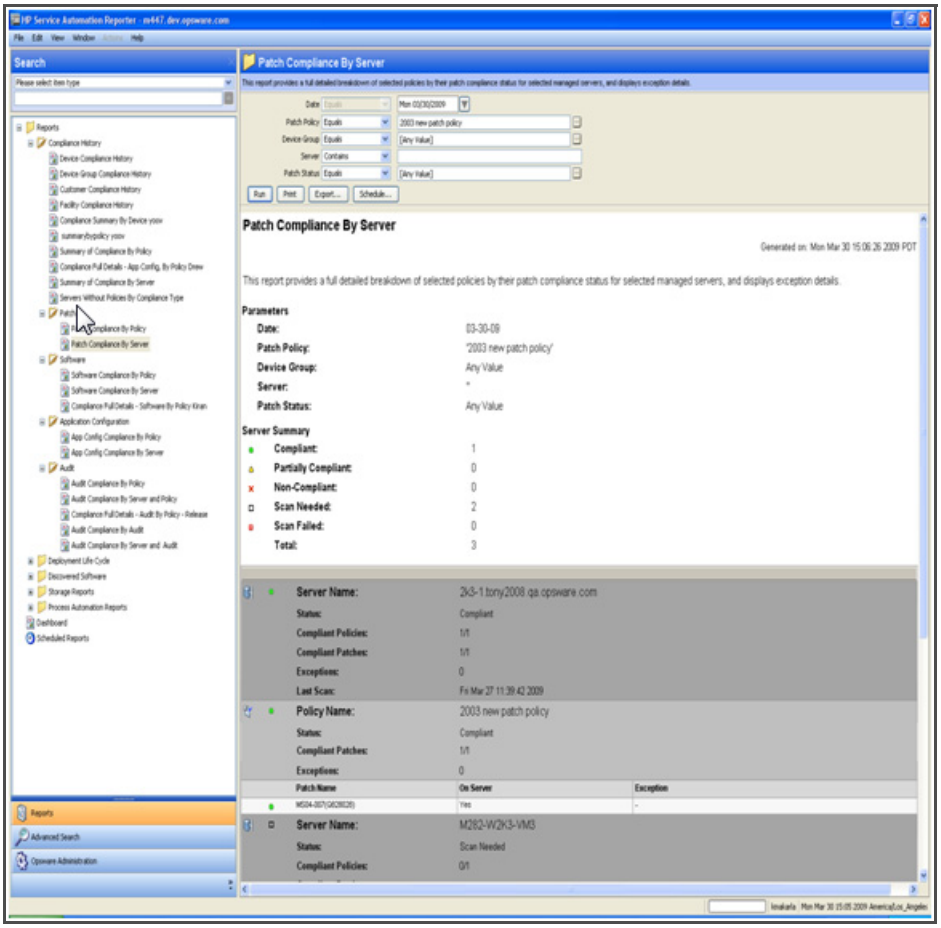
Table

- 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.

Acting on Details

- Double-click / Right-click on a policy and select Open to launch SA Policy Browser. 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. Operations on the server are subject to user permission.

Figure 29 Patch Compliance By Server



Servers Without Policies by Compliance Type

Table

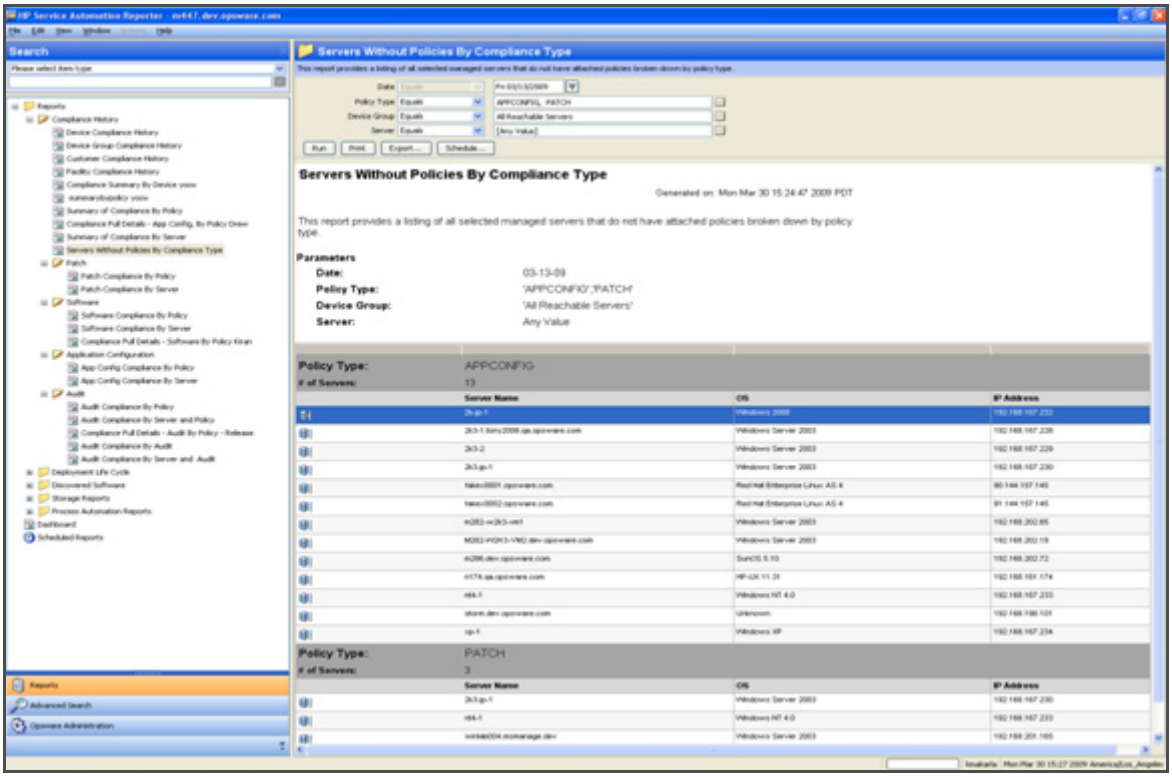
- Report lists servers that do not have any policies attached to them.
- Servers are grouped by compliance type, with the name of each server listed.
- A server can be listed under multiple compliance type sections.
- Counts reflect current managed/active servers only.

Servers with application configuration policies that have been attached but not yet pushed will not appear in this report.

Acting on Details

Double-click / Right-click on a server and select Open to launch SA Server browser window. Operations on the server are subject to user permission

Figure 30 Servers Without Policies by Compliance Type



4 SA Client Reports

SA Client reports provide comprehensive, real-time information about managed servers, virtual servers, network devices, and user and security permissions in your environment. These parameterized reports are presented in graphical and tabular format, and are actionable—which means that you can perform appropriate actions on objects, such as a policy or an audit, within the report. These reports are also exportable to your local file system (as .html, .pdf, or .xls files) to facilitate use within your organization.

This section contains information about the types of SA Client reports, how to modify report parameters, how to run the reports, and how to perform actions in the report results.

Additional reporting for SA Client features is available in the BSA Essentials Client. For additional information, see BSA Essentials Reports for SA on page 7.

In this section:

Reports Features

SA Client Reports enable you to perform enterprise health assessments by providing the following features:

- Actionable reports that enable you to take the appropriate action on objects within the reports. For example, in the list view of a compliance report, you can select a server and open a Remote Terminal or Server Explorer to browse it, perform an audit, create a snapshot, create a package, and so on.
- A single entry point in the SA Client Dashboard for all reports.
- Reports that are data-secured—controlled by the user's permissions. You can view all objects that you have read permissions for. You can perform actions on objects that you have write permissions for.
- Reports that are exportable to .html, .pdf, and .xls formats. You can export reports to your local file system for use within your organization.

HP Server Automation Client Reports

The following table lists the SA Client Reports by report folders.

Table 1 SA Client Reports

Report Folder	Report Title
Server Reports	• Servers by Customer • Servers by Facility • Servers by Manufacturer • Servers by Model • Servers by Operating System • Servers by Use
Virtualization Reports	• Virtualization by Virtual Technology • All Virtual Servers • Solaris 10 — Virtual Servers by Hypervisors (zones only) — Resource Allocation by Hypervisors (zones only) • VMware ESX 3 — Virtual Servers by Hypervisors (VMs only) — Resource Allocation by Hypervisors (VMS only)
User and Security Reports	• Client and Feature Permissions • Customer/Facility Permissions and Device Group Permission Overrides • User Groups Memberships • User Login • Administrator Actions • Users and Authorizations, By User Group • Users and Authorizations, By Individual User Group • Administrator Customer Groups • Server Permissions, By User • Server Permissions, By Server • OGFS Permissions, By User • OGFS Permissions, By Server

Table 1 SA Client Reports (cont'd)

Report Folder	Report Title
Network Reports	• Connections by Network Device • Connections by Server • Duplex Compliance (All Servers) • Duplex Compliance by Customer • Duplex Compliance by Facility

The following documentation describes the SA Client features that support information in these reports.

- "Network Reports" in the *SA Integration Guide*
- "Virtual Server Management" in the*SA Users Guide: Server Automation*

Additional reporting for SA Client features is available in the BSA Essentials Client. For additional information, see BSA Essentials Reports for SA on page 7.

User Permissions for Reports

Reports are controlled by the user's permissions. You can view all objects that you have read permissions for, and you can perform actions on objects that you have write permissions for.

To view or run a network report, SA/NA integration must be configured. See the *SA Integration Guide*.

To view or run a user and security report, system administrator permissions are required.

Launching the Reports Feature

To launch the Reports feature, perform one of the following steps:

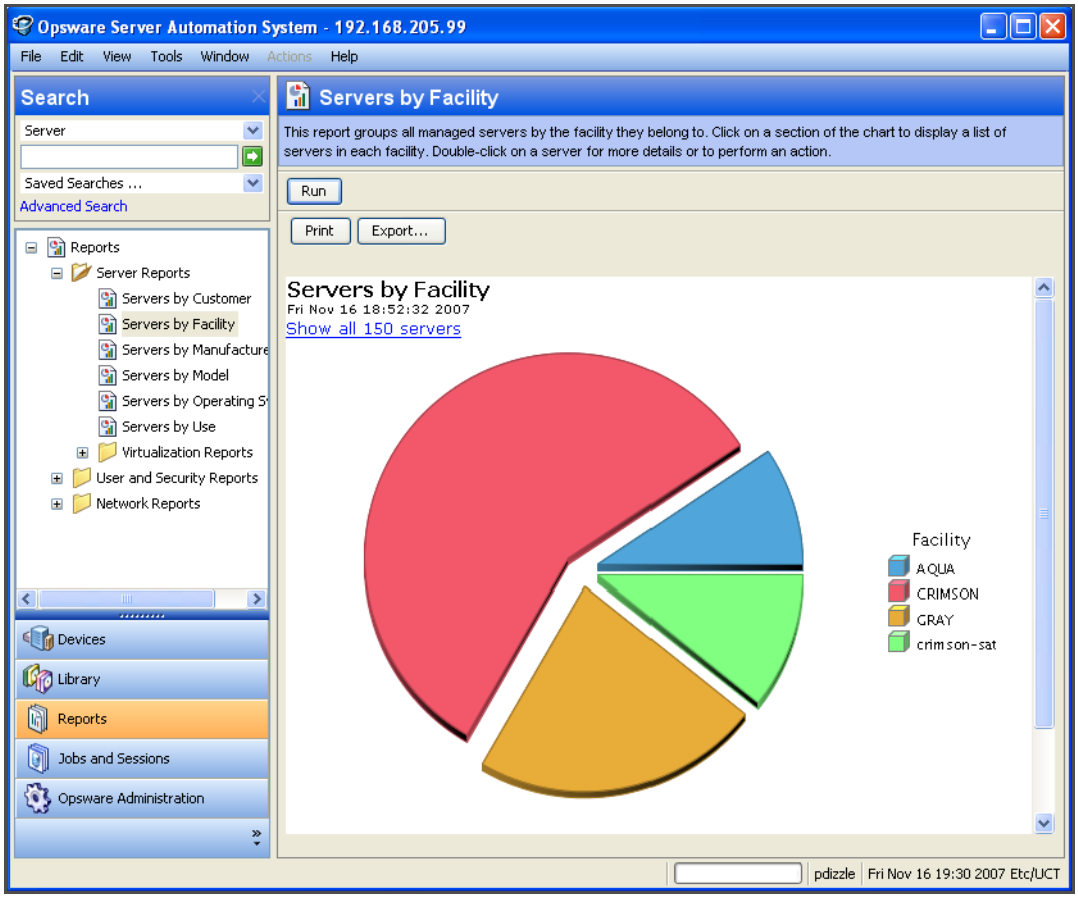
- From the **View** menu, select **Reports ➤ Dashboard**.
- From the **View** menu, select **Reports ➤ Reports**.
- From the navigation pane, select Reports.

Reports Display

In the SA Client reports window consists of a search pane, report parameters, report folders, and other filtering tools.

In this section:

Figure 31 The Reports Feature Display



Search Pane

All tab views have a search pane that allow you to search for information in the SA Client by selecting a component category and entering a keyword in the search text field. The results appear in a configurable list in the contents pane with an option to specify additional filter criteria. For more information, see the *SA Users Guide: Server Automation*

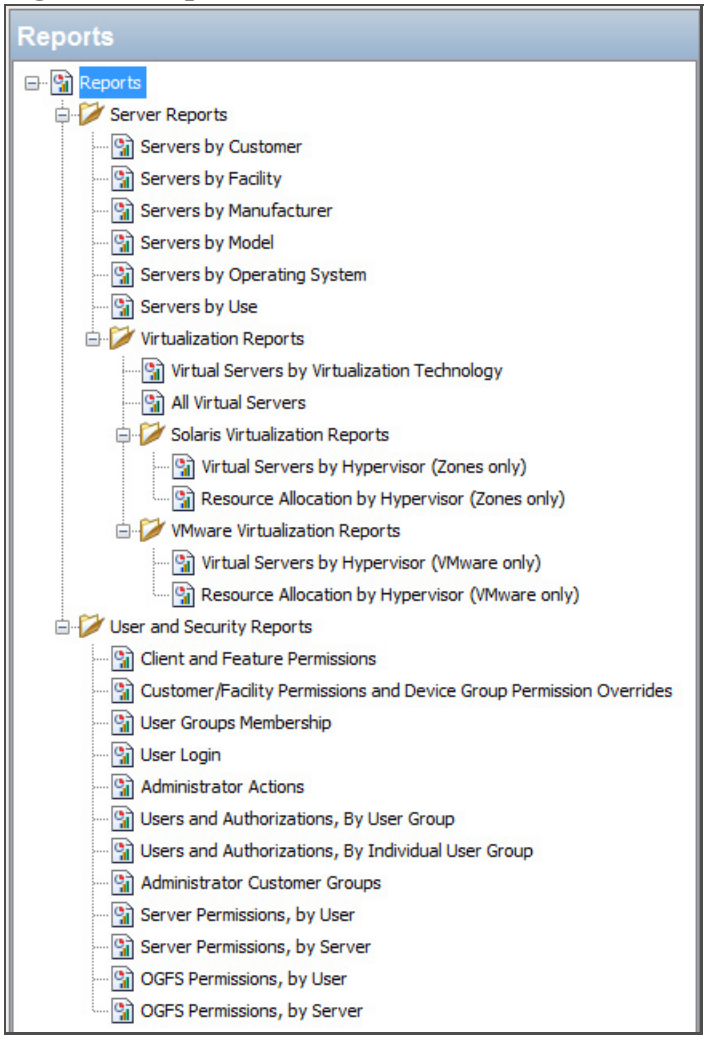
Report Folders

Reports are organized into folders according to regulatory or IT best practice standards.

- **Server Reports**: This folder contains reports about servers by customer, facility, manufacturer, model, operating system, and server usage.
- **Virtualization Reports**: This subfolder contains reports about virtual servers and resource allocation by technology and by hypervisor.
- **Network Reports**: This folder contains reports about connections and duplex compliance for network devices and servers. You must have NA installed to see this folder.
- **User and Security Reports**: This folder contains reports about client and feature permissions; customer, facility, and device group permissions; and user group memberships. You must have system administrator permissions to see this folder.

The following figure illustrates how the Report folders appear in the navigation pane, including the reports listed in each folder.

Figure 32 Report Folders



Report Parameters

Many reports require input parameters in order to be run. For these reports, you can run the report with its default parameter values or modify the parameter values. If you want to run a report that includes or excludes certain servers, customers, or hardware models, you need to specify this criteria in the report parameters. See Running a Report on page 66.

Running and Modifying Reports

In this section:

Running a Report

To run a report, perform the following steps:

1. From the navigation pane, select **Reports**.
2. Expand the Reports folder and then expand the Server Reports and Virtualization Reports.
3. Select one of the virtualization report listed in the folder.
4. If there are no report parameters in the Content pane, click **Run**.
5. If there are report parameters in the Content pane, you can either use the default parameters or change them:
   - To use the default report parameters, click **Run** to run the report. The report results appear in the contents pane. See Report Results on page 67.
   - To change the report parameters, see Modifying Report Parameters on page 66.

Modifying Report Parameters

You can modify the default parameters and run a report that includes certain servers, customers, or hardware models.

To modify the default parameters:

1. In the drop-down list for (the Server, Customer, Model, and so on), select Contains, Equals, Begins With, or Ends With.
2. (Optional) Select the ellipsis button to open the Select Values window.
3. In the Select Values window, select a value in the Available or Selected pane and then use the directional buttons to include it in or exclude it from your search criteria.
4. Click **OK** to save your changes.
5. Click **Run** to run the report. The report results appear in the contents pane. See Report Results on page 67.

If data cannot be found to run the report, a “No records to display!” error displays. See also Report Results Restrictions on page 69.

Report Results

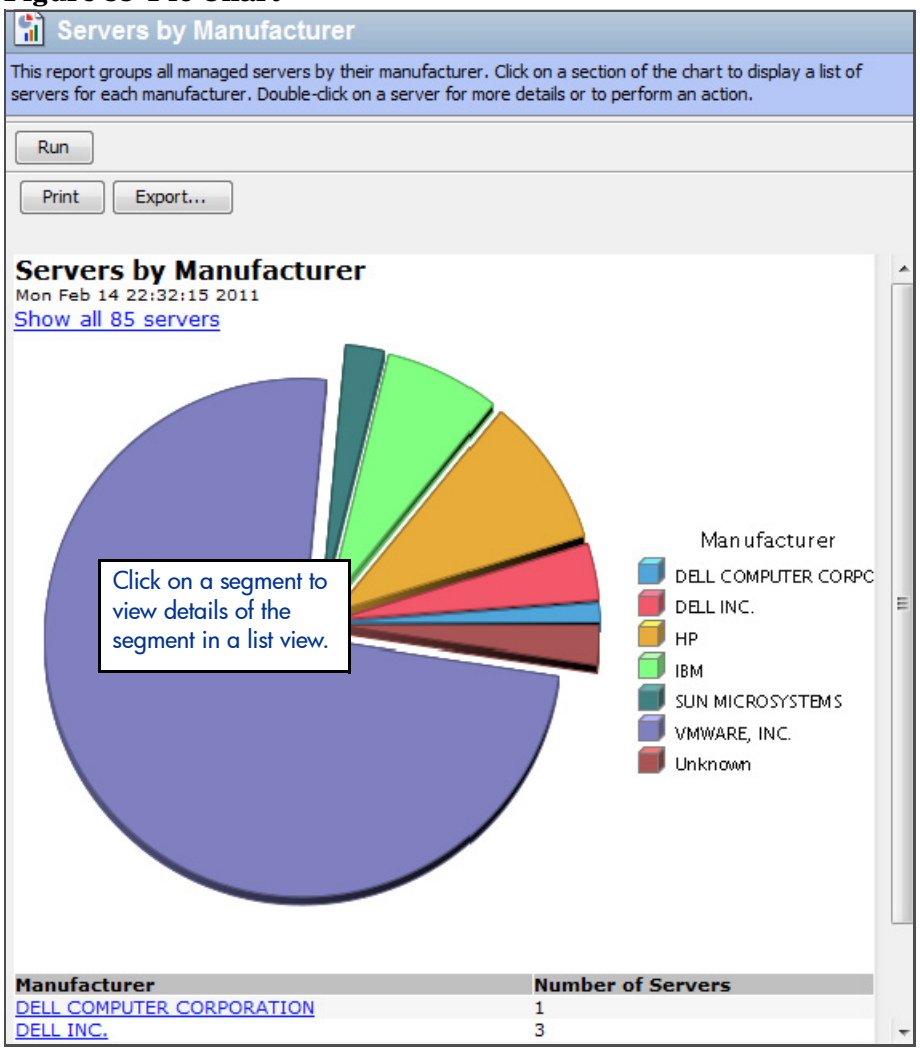
Report results initially appear in a graphical or list view. The graphical report is an overview of available data for this report displayed in a pie chart or in a bar graph. You can drill down for more detail in the chart or graph by clicking on any of the sections or bars. For example, you can drill down to individual servers that appear in a report and get detailed information about them.

In this section:

Viewing a Graphical Report

A graphical report is a pie chart.

Figure 33 Pie Chart

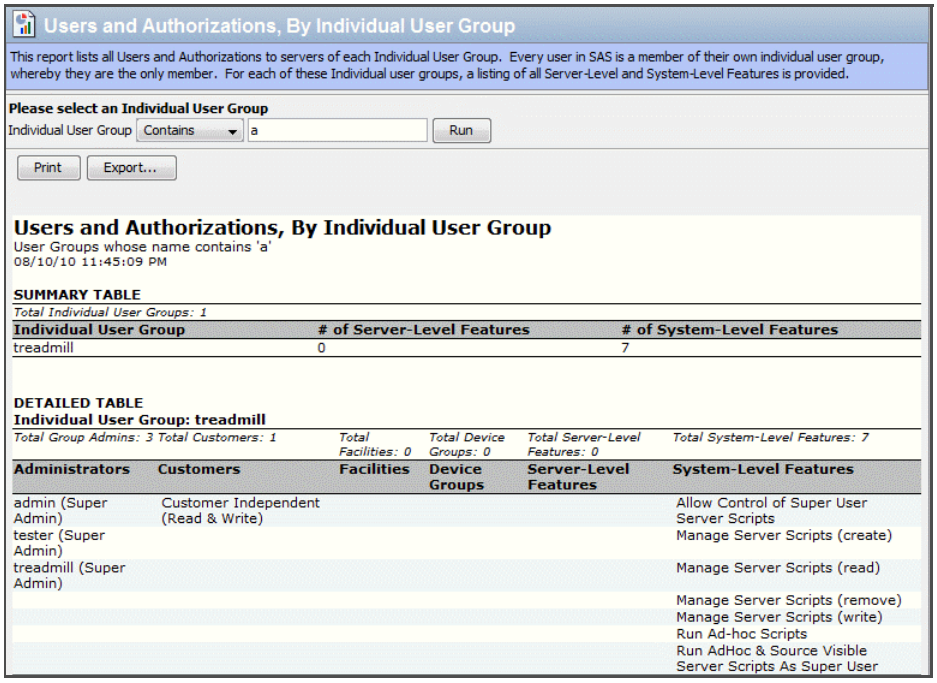


Click on a section of the chart to drill down for more details or to perform an action. You can also click on the “Show all <number> servers” link to display a list of servers.

Viewing a List Report

A list report is a tabular display of information. Double-click on a row in the list, such as a server, audit, or policy, for more detail or to perform an action. See Figure 34 for an example.

Figure 34 List Report



Exporting a Report

You can export a report to your local file system for use in other applications or to distribute as an attachment in an email. The type of report determines which export file formats are available:

- Graphical reports (pie or bar charts) can be exported to .html or .pdf format.
- List reports can be exported to .html, .pdf, or .xls format.

When you export a report in the SA Client, the time that you will see marked on the exported report will be the time when the report was exported, not the time when the report was generated.

To export a report:

1. From the report, click **Export** to open the Save window.
2. In the Save in field, enter a location that identifies where you want to save the file to, or select from the drop-down list.
3. Enter a file name.
4. Select the file type.
5. Click **Save**.

Printing a Report

To print a report:

1. From the report, click **Print** to open the Print window.
2. Use the default print options or modify them, and then click **OK**.

Report Results Restrictions

The following reports have a limit of 2000 “items” that can be displayed in their results:

- Server Permissions By Server
- Server Permissions By User
- OGFS Permissions By Server
- OGFS Permissions By User

In these reports, if the results reach 2000, the report will stop, because depending on the specified search parameters, they can yield thousands of results and slow performance of the SA core.

For example, the Server Report by User will run successfully if you specify 10 users and 200 servers in the search parameters, but will not run if you specify 10 users and 201 servers.

To avoid this problem, either modify your search parameters to yield less results, or break the report query into smaller searches and run as many smaller reports as you need to achieve your results.