Opsware® System Data Center Intelligence 1.5 Administrator's Guide

Corporate Headquarters

599 North Mathilda Avenue Sunnyvale, California 94085 U.S.A.
T + 1 408.744.7300 F +1 408.744.7383 www.opsware.com

Table of Contents

Chapter 1: Data Center Intelligence (DCI) Reporting

IN THIS CHAPTER

This section covers the following topics:

- About DCI Reporting
- Accessing DCI Reports in the OCC
- Report Parameters
- Report Results
- DCI Reports

About DCI Reporting

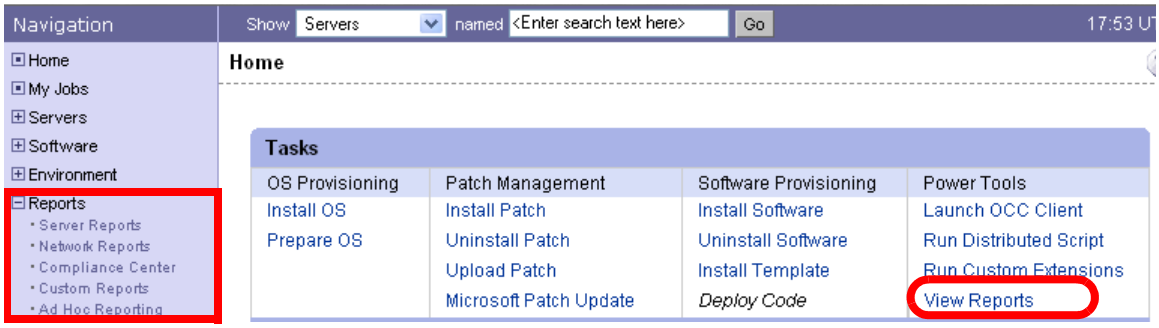
Welcome to Opsware's DCI Reporting. DCI reports provide real-time comprehensive information about an organizations servers, software, customers, operating systems, patches, compliance policies and what changes have occurred and should occur. After an action completes in the Opsware Command Center, it is available in the DCI reports.

This help provides an overview of how to use the DCI Report Server, introduces DCI concepts, and explains how the software functions, so you can be effective using Opsware's DCI Reports.

Accessing DCI Reports in the OCC

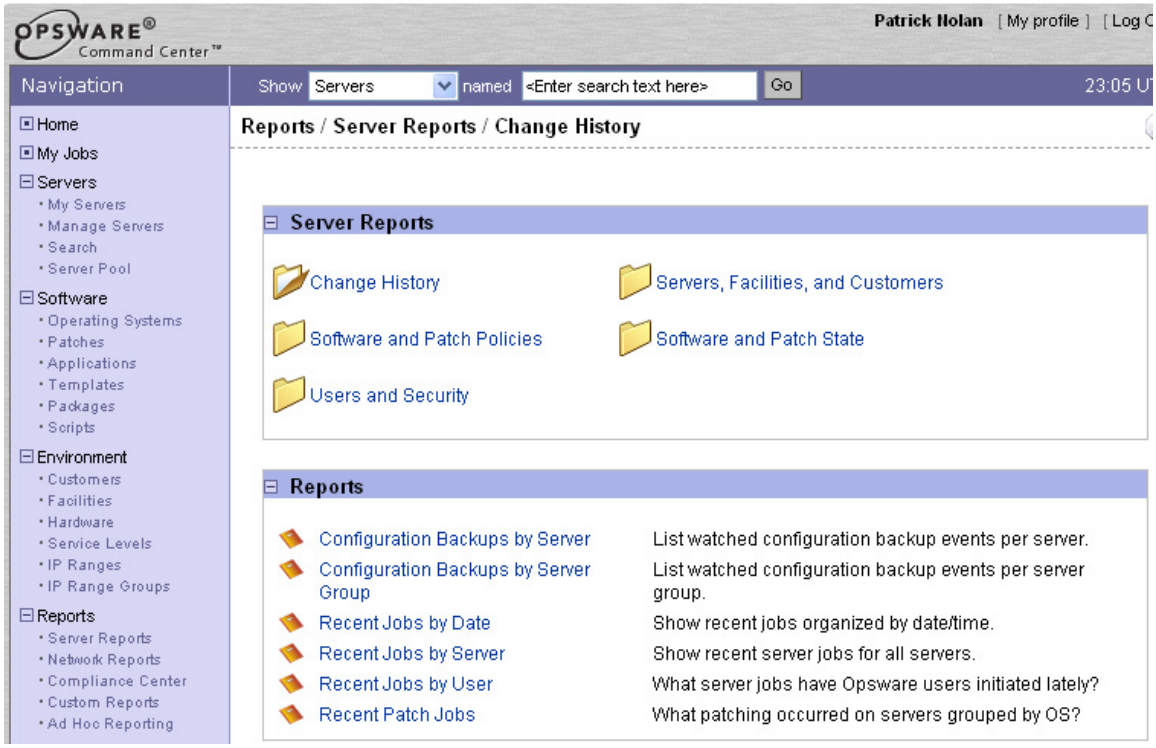
The home page is divided into five main sections: Server Reports, Network Reports, Compliance Center, Custom Reports, and Ad Hoc Reporting.

Figure 1-1: The DCI Home Page — Server Reports Page



If you click a Reports link from the Navigation bar, the screen displays a page of available reports for each reporting category. From each report page, clicking on the name of any report folder will generate a list of associated reports in the lower pane of the DCI window. For example, clicking the Server Reports link will display the following page shown in Figure 1-2

Figure 1-2: Server Reports Page - Change History Reports

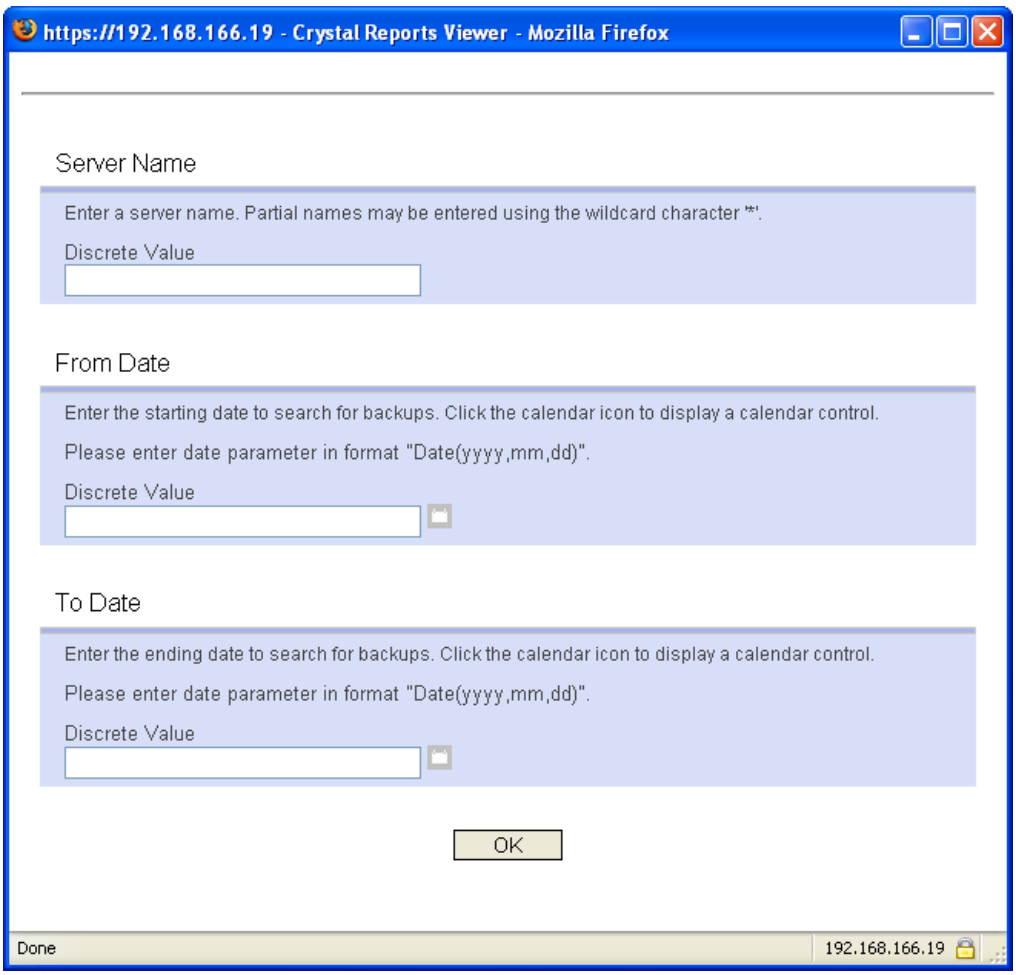


Clicking on the name of a report will launch either the report itself or a new window to set the parameters for the report.

Report Parameters

Some reports require input parameters in order to be run. In most cases for such reports, these parameters include a server or server group name, a "from date" and a "to date." The following example in Figure 1-3 shows an input page for running a report.

Figure 1-3: Sample Set Parameters Page for Running a Report



To set report parameters, enter the following information:

- **Server Name**: Use the full name for servers (not IP addresses) and server groups or use a name plus an asterisk ("*") to search by name. For example: "Develop*".
- **From Date**: Enter dates in the required format (or use the calendar pop-up).
- **To Date**: Enter time values in days (or use the calendar pop-up).

Not all reports will require entering parameters, and some reports will require only a single parameter, such as server name or date.

Report Results

Report results initially appear in a graphical or list view. The graphical view provides a quick overview of the available data for this report in a chart. Clicking on any of the bars in the chart will drill down to more detail on the selected item only.

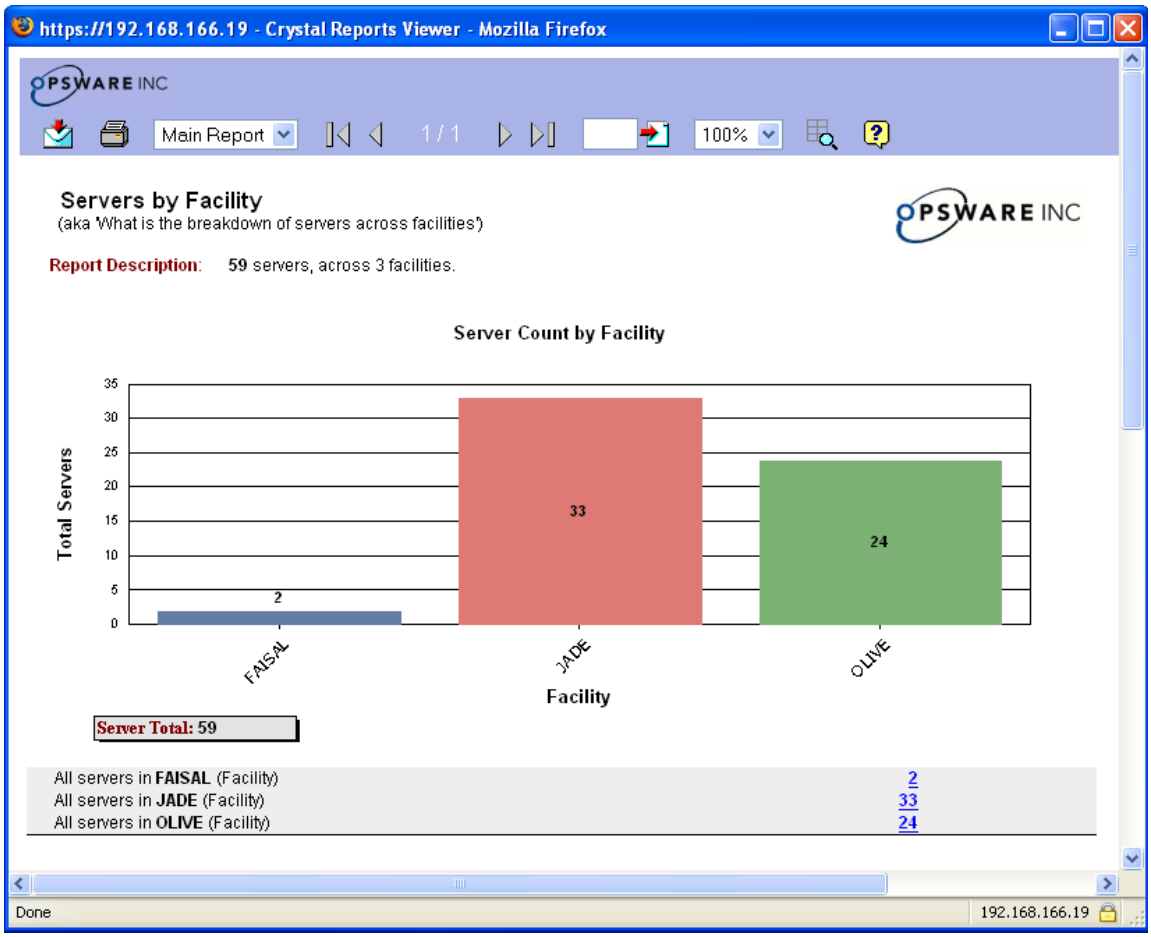
This section discusses the types of DCI report results and contains the following topics:

- Graphical View Report Results
- List View Report Results
- Individual Server Results View
- Report Results Icons

Graphical View Report Results

Figure 1-4 shows the server report named "All Servers By Facility" in a graphical view.

Figure 1-4: Graphical View of Report All Servers By Facility



Many of the elements inside the report are clickable, enabling you to drill down and display more detailed information about specific information on the results. For example, if you click the center bar for the Jade facility, a more detailed view of the servers in this facility is displayed, as shown in Figure 1-5.

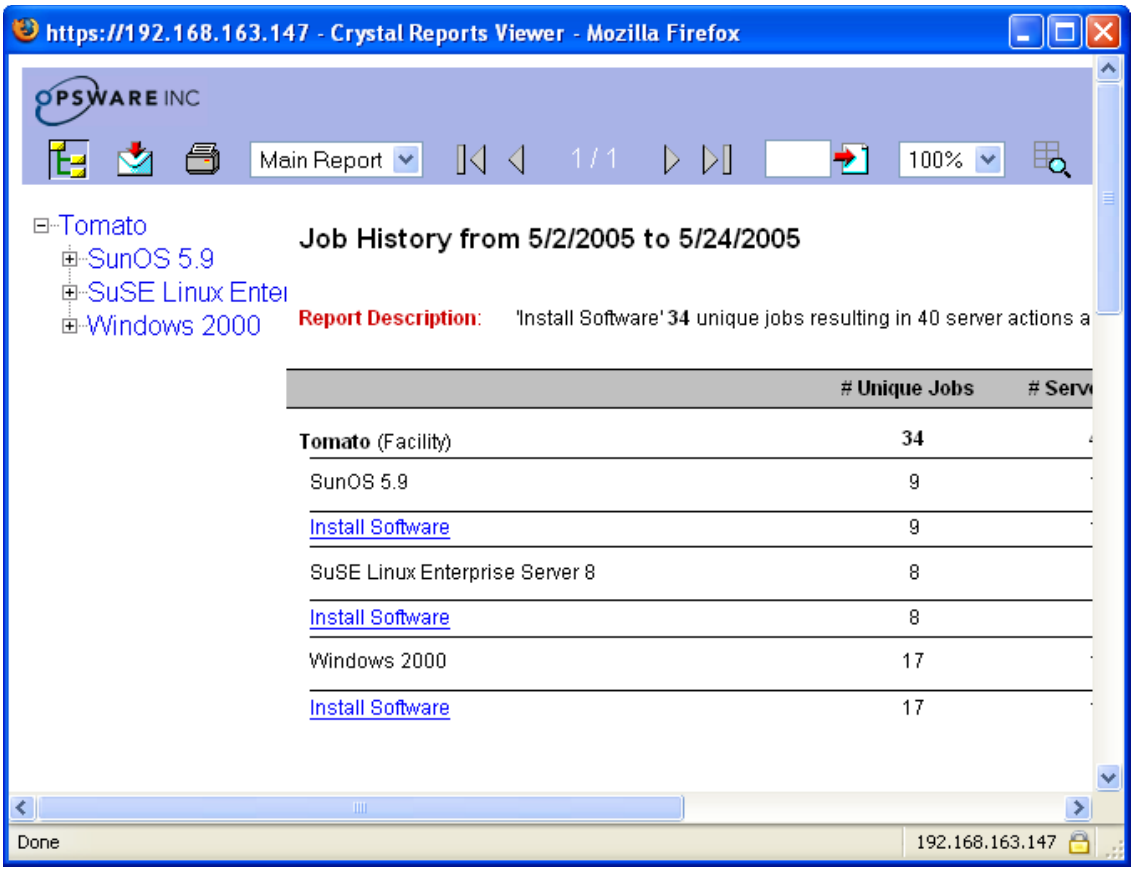
Figure 1-5: Servers By Facility – Detailed View

This more detailed view lists all servers in this facility distinguished by operating system (OS). You can keep drilling down to individual servers by clicking any live links.

List View Report Results

Some reports appear in a table format with an expandable tree view on the left. The tree view allows you to easily navigate levels of your report. Clicking the links in a report will drill down to the specific data for the link you selected. Many reports have multiple levels of information to fine tune your reporting results. This type of report result is illustrated in Figure 1-6.

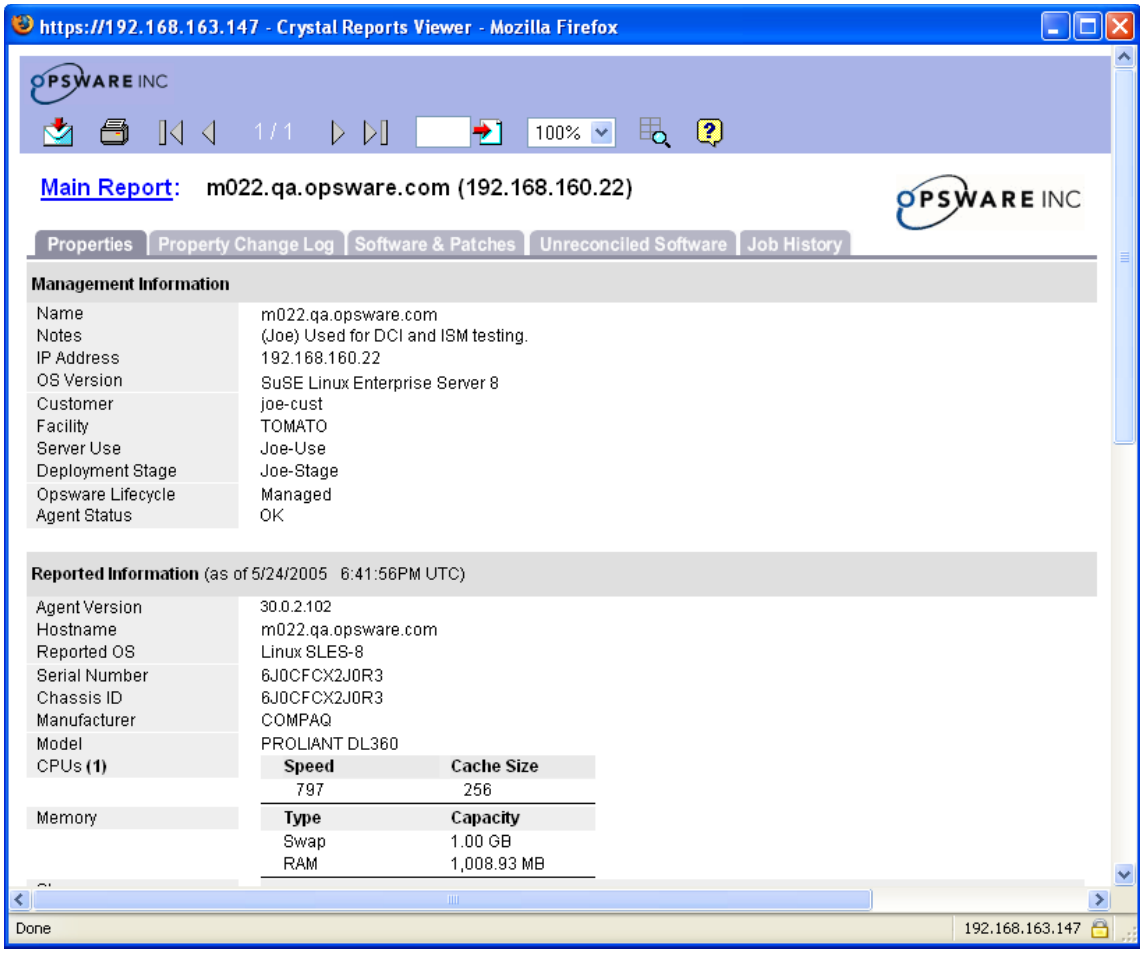
Figure 1-6: List View Report Result for Job History Report



Individual Server Results View

Drilling down to a specific server will result in a tabbed window showing detailed reporting information for that computer, as shown in Figure 1-7.

Figure 1-7: Detailed View of Individual Server



Report Results Icons

Each report generated appears on a page with a set of icons at the top. These icons can be used to click through the pages of the report, search for a particular page, print the report, export the report in various formats, and get help. Reports can be exported in

Excel, Word, Acrobat, Crystal Reports and rich text format. Reports do not tally the number of pages in advance. Therefore, 1-1+ will display initially, with this display changing as you click through the pages of a report. Table 1-8 illustrates the report results icons.

Figure 1-8: Report Results Icons

DCI Reports

DCI Reports are available to users who have been granted the appropriate permissions. Five reporting types are available from the OCC navigation panel. Each area links to a set of related reports organized into folders. Some of these reports are repeated in different areas to provide complete sets of compliance standards reports.

DCI provides the following categories of reports:

- **Server Reports**: Reports about Opsware Server Automation System (SAS), such as server changes, server facilities and customers, software and patches, and users and security.
- **Network Reports**: If the Opsware Network Automation System (NAS) is installed, reports about the network environment, status, and health will display here.
- **Compliance Center**: Reports for compliance standards including COBIT, COSO, ITIL and Sarbanes Oxley.
- **Custom Reports**: Specific reports created for particular needs in your operational environment.
- **Ad-hoc Reports**: Configurable report interface to create reports about specific software, servers, patches and the Opsware model, grouped and filtered according to your needs.

Server Reports

The following Opsware Server Automation System (SAS) pre-built reports are available in the Server Reports and Compliance links of the Reports section in the OCC navigation bar. Some reports are repeated among the various compliance standards.

Note that all reports involving Server Groups will show results for the servers in a dynamic server group as of the last time the group was reconciled.

In some cases, you might experience a delay between the time a modification is made in Opsware and when it appears in your reports depending upon the way your Crystal Reports server has been configured. For information on how to troubleshoot this issue, see See Chapter 6, “Troubleshooting the DCI Report Server” on page 59of this guide for more information.

- **All Servers by Facility**: This report defines what servers are located in each managed Facility. Click on a Facility to show the list of servers by OS in that facility, and then click the name of an OS to show the selected servers by Customer.
- **Compliance Summary**: This report quickly summarizes and visually presents an overview of what servers and/or server groups are in compliance with their policies according to user defined thresholds. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.

  First choose whether to list servers, server groups, or both and optionally enter a server group name. Then, choose a percentage for server group compliance to appear in a warning state (such as 1), which is shown as yellow, and a percentage to show in a non-compliant state (such as 5, which is shown as red). Do not use the % symbol. Server groups that are “in compliance” and have less than the Yellow Threshold value show as green. Use the drop-down menu to display only red, yellow or green server groups, or choose All to see a complete compliance report. Finally, set a time range for the report.

  Note that the “From Date” does not apply to software and patches. Audits for software and patches are based on what is currently installed. For Compliance, Configuration, and Watched Configuration Audits, the From Date can be specified to limit how far back audits are to be performed.

  The report results are calculated according to the following formula:

  – A = installed software count + installed patch count + matching application configuration count + audits with no discrepancies
  – B = modeled software count + modeled patch count + configuration objects checked count + total audit jobs performed

  - Overall Non-Compliance = ((B-A)/B) * 100

- **Configuration Audits by Server**: This report displays detailed application configuration audit results by server within a user defined time period.
- **Configuration Audits by Server Group:** This report displays detailed application configuration audit results by server group within a user defined time period.
- **Configuration Backups by Server**: This report shows the results of Configuration Audits run on a particular server during a defined time period. This report only includes triggered incremental and full backups; manual backups are excluded. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.
- **Configuration Backups by Server Group**: This report lists the configurations that have been backed up for a particular server group in a defined time range.This report only includes triggered incremental and full backups; manual backups are excluded. This report is the same as Backed Up Configurations by Server, except that the servers are displayed by server group. The configurations, however, are performed based on the policies defined at the server level, not the server group level. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.
- **Difference Audits by Server**: This report presents the results of compliance audits run on a particular server during a defined time period.
- **Difference Audits by Server Group**: This report presents the results of compliance audits run on a particular server group during a defined time period. This report is the same as Compliance Audits by Server, except that the servers are displayed by server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.
- **Managed Servers by Facility**: This report shows all managed servers in the operational environment organized by Customer. Clicking on a Customer name shows servers for that Customer organized by OS. Clicking on an OS shows a list of the actual servers by name.
- **Nodes by Customer**: This report lists all software a customer has installed. Click a Customer name, then click the name of a software package to see what servers have

it installed. Software Nodes are listed alphabetically in the report and also in the navigation tree on the left.

- **Package Catalog**: This report lists the packages installed on each server limited by OS. All known software is grouped alphabetically (to speed report processing). Drill down by the first letter of the software package name and then see a list of servers that have that software installed.
- **Patch Catalog**: This report lists the patches installed on each server limited by OS. All known patches are grouped alphabetically (to speed report processing). Drill down by the first letter of the patch name and then see a list of servers with the software installed.
- **Patch Inventory**: This report lists all servers and the patches installed on each server. Click a server name to see the list of patches on that server.
- **Patching Audits by Server**: This report displays a summary of the patches expected on a server versus what is actually there. Enter a server name to see expected patches and installed patches for that server. Software is not listed.
- **Patching Audits by Server Group:** This report displays a summary of the patches expected on a server group versus what is actually there. Enter a server group name to see expected patches and installed patches for that server. Software is not listed. This report is the same as Patching Audits by Server, except that the servers are displayed by server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.
- **Patching on Servers Grouped by OS**: This reports shows the patches installed on servers grouped by operating system. Click a Job name to view patch details.
- **Recent Jobs by Date:** This report lists all server jobs chronologically by date. Clicking on the name of a server job will show details for that job. User selects the desired job type which may be "All Jobs."
- **Recent Jobs by Server**: This report lists all server jobs alphabetically by server name. Clicking on the name of a server job will show details for that job.
- **Recent Jobs by User**: This report lists all server jobs alphabetically by user name. Clicking on the name of a server job will show details for that job and clicking the name of a server will show server details.
- **Recent Patch Jobs**: This report displays the patches installed on servers grouped by OS.

- **Server Attachments by Node**: This report lists all servers attached to each node in the Software Tree.
- **Server Groups without Application Configuration Policies:** This report alphabetically lists all server groups without Application Configuration policies. Clicking the number in the Server Count column will display the individual servers in a group.
- **Server Groups without Compliance Audit Policies:** This report alphabetically lists all server groups without Compliance Audit policies. Clicking the number in the Server Count column will display the individual servers in a group.
- **Server Groups without Configuration Tracking Policies**: This report alphabetically lists all server groups without Configuration Tracking policies. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.
- **Server Groups without Patch Policies:** This report alphabetically lists all server groups without Patch policies. Clicking the number in the Server Count column will display the individual servers in a group.
- **Server Groups without Software Policies:** This report alphabetically lists all server groups without Software policies. Clicking the number in the Server Count column will display the individual servers in a group.
- **Server Pool:** This report lists servers in the server pool (unprovisioned servers without an operating system installed) by Facility.
- **Servers by Customer**: This report lists how many servers are assigned to each Customer. Click on a Customer name to show servers for that Customer organized by OS. Then click on an OS to show a list of the actual servers by name.
- **Servers without Application Configuration Policies**: This report alphabetically lists all servers without Application Configuration policies.
- **Servers without Compliance Audit Policies**: This report alphabetically lists all servers without Compliance Audit policies.
- **Servers without Configuration Tracking Policies**: This report alphabetically lists all servers without Configuration Tracking policies. Tracked configuration applies to the policies that are directly attached to a server or via a node, regardless of whether or not the policies have been reconciled onto a server.

- **Servers without Patch Policies**: This report alphabetically lists all servers without patch policies.
- **Servers without Software Policies**: This report alphabetically lists all servers without Software policies.
- **Software Audits by Server**: This report displays a summary of software expected on a server versus the software actually installed. Only software is listed, not patches.
- **Software Audits by Server Group**: This report shows a summary of software expected on a server group versus the software actually installed. Only software is listed, not patches. This report is the same as Software Audits by Server, except that the servers are displayed by server group. The audits, however, are performed based on the policies defined at the server level, not the server group level.
- **Software by Customer**: This report shows the software each customer should have according to the Model. Click a Customer name to view a software list for that Customer, then click a software name to see servers with software installed.
- **Software Inventory**: This report lists a software inventory for a customer. Choose a customer name to display all known software on a customer's servers.
- **User Groups**: This report lists the Members, Features and the Permissions associated with a specified User Group.
- **User Logins**: This report shows what users are active, in a warning or in an expired state, based on specified values. Enter desired threshold values in days.
- **User Permissions**: This report describes what permissions are assigned to a particular user. Enter a user name to view a complete list of their designated permissions.

Network Reports

The following networking reports are available when the Opsware Network Automation System (NAS) is also installed:

- **ACLs in Use**: This report shows all Access Control Lists (ACLs) that are in use in specified devices.
- **ACL Changes**: This report lists all ACL changes in the last seven days and the specific devices the changes occurred on.
- **All ACLs**: This report lists the details of all the ACLs in the inventory including host name, ACL ID, Handle, type, and date last modified.

- **Active Configurations**: This report displays all active Device configurations in the network environment.
- **Approved Changes**: This report lists all tasks approved within a user defined time range.
- **Changes Pending Approval**: This report lists the changes pending approval as well as who scheduled the change and the host or group affected.
- **Configuration Changes**: This report shows the configuration changes that have occurred in a user defined time range.
- **Configuration Policies**: This report displays all configuration policies and status in place in the network environment.
- **Configuration Policy Events**: This report lists all configuration policy non-compliance events within a user defined time range.
- **Device List**: This report presents a complete list of all devices available in the network inventory.
- **Device Password Rules**: This report lists all password rules in place in the network environment.
- **Device Software Report**: This report lists what devices are in software compliance.
- **Devices without Driver Assigned**: This report lists all devices without any driver assigned.
- **Devices with Driver Assigned but no Configuration Stored**: This report lists all devices with a driver assigned but no configuration stored.
- **Devices with Different Startup and Running Configurations**: This report lists devices with different start up and running configurations.
- **Diagnostics**: This report shows what diagnostics have been run in a user defined time range.
- **Failed, Skipped, and Duplicate Tasks**: This report shows what tasks have failed, been skipped, or duplicated within a user defined time period. The results are listed by the date and time stamp.
- **Inaccessible Devices**: This report displays a list of devices with access failures.
- **Inactive Devices**: This report lists all inactive devices in the network inventory.

- **Modules**: This report lists the modules available in the network device inventory as well as slot info and descriptions for each module.
- **Network Status Report**: This report shows the status of devices in the network including policy rule violations, start up versus running configuration mismatches, software compliance violations, device access failures and configuration changes within the past 24 hours.
- **Past Tasks**: This report displays all device change tasks performed within a user defined time range.
- **Pending Deployments**: This report displays the software deployments scheduled in a user defined time range.
- **Pending Tasks**: This report lists all device change tasks scheduled for a user defined time range.
- **Port Availability**: This report lists what devices have port availability of less than 10%.
- **Sessions Created**: This report lists what telnet/ssh proxy sessions have been created within a user specified time range.
- **Task that Require Approval**: This report lists all tasks that require approval within a user defined time range.
- **Unapproved Changes:** This report shows what unapproved changes have taken place in the network environment within a user specified time range.
- **Users List**: This report presents a list of all users in the network environment.

Compliance Center

Several compliance standards have become commonplace in the IT industry. DCI supports reporting for these specific standards. Some background for each of these four compliance standards is provided in the following sections.

COBIT

Control Objectives for Information and related Technology (COBIT), published by the IT Governance Institute, is an internal control framework that helps meet the multiple needs of management by bridging the gaps among business risks, control needs, and technical issues and balancing risk versus return over IT and its processes. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT has been implemented by a number of companies to provide additional details about their system of IT controls.

Note that COBIT provides controls that address operational and compliance objectives in addition to those related directly to financial reporting.

COSO

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a landmark report on internal control. Internal Control – Integrated Framework provides a sound basis for establishing internal control systems and determining their effectiveness.

According to COSO, the three primary objectives of an internal control system are to ensure (1) efficient and effective operations, (2) accurate financial reporting, and (3) compliance with laws and regulations. The report outlines five essential components of an effective internal control system.

- **Control Environment**: This establishes the foundation for the internal control system by providing fundamental discipline and structure.
- **Risk Assessment**: This involves the identification and analysis by management - not the internal auditor – of relevant risks to achieving predetermined objectives.
- **Control Activities**: The policies, procedures, and practices that ensure management objectives are achieved and risk mitigation strategies are carried out.
- **Information And Communication**: This supports all other control components by communicating control responsibilities to employees and by providing information in a form and time frame that allows people to carry out their duties.
- **Monitoring**: This covers the external oversight of internal controls by management or other parties outside the process or the application of independent methodologies such as customized procedures or standard checklists by employees within a process.

ITIL

IT Infrastructure Library (ITIL) was developed for the British government by the CCTA (now the OGC: Office of Government Commerce) and has been rapidly adopted across the world as the standard for best practice in the provision of IT services. Three major areas of ITIL are Service Support, Service Delivery, and Security Management. Service Support and Service Delivery are the disciplines that comprise IT Service Management (ITSM), which embraces provisioning and management of effective IT services.

- **Service Support**

  Service Support is the practice of those disciplines that enable IT Services to be provided effectively. Service Support consists of six (6) disciplines:

  – Configuration Management

  – Incident Management

  – Problem Management

  – Change Management

  – Service/Help Desk

  – Release Management

- **Service Delivery**

  Service Delivery is the management of the IT services themselves, and involves a number of management practices to ensure that IT services are provided as agreed between the Service Provider and the Customer. Service Delivery consists of five (5) disciplines:

  – Service Level Management

  – Capacity Management

  – Continuity Management

  – Availability Management

  – IT Financial Management

- **Security Management**

  Using security management, data and infrastructures are to be protected so that:

  – Confidentiality is appropriately preserved

  – Integrity of information is ensured.

  – Availability is ensured.

  – Conducting a transaction is not denied.

  – Obligations imposed by law, contractual agreement, and supervisory bodies can be fulfilled.

Sarbanes Oxley (Section 404)

The Regulatory Compliance Center provides reports detailing the current compliance status of your network infrastructure with respect to Sarbanes-Oxley (Section 404) and supporting internal control frameworks. Sarbanes-Oxley (Section 404) itself provides no

specific control requirements that can be used for IT-related compliance efforts. Organizations must instead choose an internal control framework, such as COSO, COBIT, or ITIL, and enforce and report against that framework.

Overview

The Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as Sarbanes-Oxley, is designed to improve the accuracy and reliability of corporate disclosures to investors.

Sarbanes-Oxley generally applies to all U.S. companies registered with or required to file reports with the SEC (Securities and Exchange Commission). The regulation requires the CEO and CFO of reporting companies to certify their companies' SEC reports (with possible criminal and civil liability for false statements).

A key provision of Sarbanes-Oxley is Section 404, which specifically addresses internal control over financial reporting. Section 404 requires that reporting companies include an internal controls report and assessment as part of their financial reporting. Under the new compliance schedule released by the SEC on February 24, 2004, a company that is an "accelerated filer" as defined in Exchange Act Rule 12b-2 (generally, a U.S. company that has equity market capitalization over $75 million and has filed at least one annual report with the Commission), must begin to comply with these amendments for its first fiscal year ending on or after Nov. 15, 2004 (originally June 15, 2004). A non-accelerated filer must begin to comply with these requirements for its first fiscal year ending on or after July 15, 2005 (originally April 15, 2005). (Refer to SEC Release No. 33-8392 for more detailed information.)

The consensus among auditors such as Deloitte & Touche, Ernst & Young, and PriceWaterhouseCoopers is that internal control over financial reporting includes controls over the safeguarding of assets and controls related to the prevention or timely detection of unauthorized acquisition, use, or disposition of an entity's assets (including network assets) that could have a material effect on the financial statements. IT support systems, including networks, are involved in the financial reporting process, and, as a result, should be considered in any design and evaluation of internal controls. Without adequate internal control over the network infrastructure, the reliability of the resulting financial reports cannot be assured.

Ensuring Compliance Using Opsware

Sarbanes-Oxley Section 404 does not specify the means by which internal controls over the corporate IT infrastructure are to be established and verified. However, the SEC in its final rules regarding Sarbanes-Oxley made specific reference to the recommendations of

the Committee of the Sponsoring Organizations of the Treadway Commission (COSO). COSO issued a landmark report on internal control, Internal Control - Integrated Framework, which provides a sound basis for establishing internal control systems and determining their effectiveness.

The U.S. Public Company Accounting Oversight Board (PCAOB) is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports. The PCAOB emphasizes the importance of IT controls. Both the PCAOB and the SEC approved PCAOB Auditing Standard No. 2, titled An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. PCAOB Auditing Standard No. 2 states: Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures to develop the framework. In the United States, the Committee of Sponsoring Organizations (COSO of the Treadway Commission has published Internal Control - Integrated Framework. COSO publication (also referred to simply as COSO) provides a suitable framework for purposes of management's assessment.

Often, SEC registrants and others have found that additional details regarding IT control considerations are needed beyond those provided in COSO. COBIT and ITIL have been implemented by a number of companies to provide additional details about their system of IT controls.

Custom Reports

Custom reports can be created and added depending on the specific needs of an operational environment. Using a Crystal Reports expert is recommended to create custom reports. See the DCI Administrator’s Guide for more information.

Ad-hoc Reports

Ad Hoc Reporting enables searching for specific software, servers, and so on, grouped and filtered according to your needs. For example, the Servers folder allows for choosing the types of servers to include in the report and how the servers will be grouped.

To query a specific set of servers, limit the results to generate a smaller report of just the information you requested. First a report appears that contains summary graphs organized so that you can gather group information. Drill down to more detailed group information by clicking columns in the graph or links in the table until the actual server

information that makes up the summary is displayed. However, to display just a list of servers, select **List Only** and the report will suppress the graphs and show all the results in one long report. This format is best for printing or exporting an inventory list.

Chapter 2: Installing and Configuring the DCI Report Server

IN THIS CHAPTER

This chapter discusses the following topics:

- Prerequisites
- Installing the DCI Report Server
- Configuring DCI Report Servers in a Multimaster Mesh
- Accessing Reports in the OCC

The DCI Report Server 1.5 is a software package on the DCI Report Server disk of the Opsware System 5.1 Installation DVDs. The DCI Report Server must be installed using the Integrated Software Management (ISM) Tool.

Before you install the DCI Report Server, Microsoft Internet Information Services (IIS) must be installed and running on your managed server. The installation process creates a virtual directory, DCI (the alias for this web site), under the IIS web site default directory that points to a real directory on the server. The path of the directory where the content will reside is `%SystemDrive%\Program Files\Opsware\DCI\wwwroot`.

Prerequisites

To install the DCI Report Server, you need the following hardware, server setup, and user privileges.

Hardware

You need the following items to begin installing the DCI Report Server:

- A Pentium III CPU or higher (Pentium 4 at 2 GHz or more recommended)
- 256 MB RAM or higher (512 MB recommended, more for heavy usage)

- 800 MB of free disk space to download and install the DCI package. Installed software is approximately 320 MB
- An Opsware managed server (a server with an Opsware Agent that is managed through the Opsware Command Center)
- On Windows 2000, Service Pack 4 or higher, running the Internet Information Services 5.0 or 6.0
- On Windows 2003, Internet Information Services 6.0
- If you plan to run the DCI server with an Opsware Network Automation System (NAS) server, the NAS server must be running with an Oracle database. Consult your NAS system administrator for more information.

Software

DCI Report Server 1.5 is only compatible with Opsware System 5.1 and Opsware Network Automation 4.0.

Preparing the Server

To install the DCI Report Server, your server must meet the following conditions:

- The machine is available to Opsware users and the named machine is accessible in the Opsware Command Center from the Servers ➤ Manage Servers page.
- IIS is installed on your machine. To verify this, the following programs should be present on the computer:

  Programs ➤ Administrative Tools ➤ Internet Services Manager

  Or

  Programs ➤ Administrative Tools ➤ Services ➤ IIS Admin Service

  Or

  Programs ➤ Administrative Tools ➤ Internet Information Services (IIS) Manager
- The DCI Report Server DVD-ROM is loaded on your computer.
- The DCI server can resolve the hostname "truth" to the desired Opsware database server.
- The database can accept connections on default port 1521.
- The following information is related to your Opsware System configuration. These values will be required to configure custom attributes for the DCI Report Server once it

has been installed. All NAS information is optional and only required if you plan to use DCI with a NAS server.

  - DCI administrator's user name: _____
  - DCI administrator's password: _____
    (This password needs to meet security requirements on the DCI Server.)
  - Hostname or IP address of the NAS server (optional): _____
  - Port number for the NAS server (optional): _____
  - Password for the NAS Oracle database (optional): _____
  - SID for the NAS Oracle database (optional): _____
    (Make sure that you use the database SID, not the database service name.)
  - User name for the NAS Oracle database (optional): _____
  - IP address of the OCC Server: _____
  - Opsware_public_views password: _____
  - SID for the Model Repository database: _____
    (Make sure that you use the database SID, not the database service name.)

- Before you install the DCI Report Server, perform the following steps:
  - If you plan to run the DCI Report Server with a NAS server, you need the Oracle SID for your NAS server. (DCI is only compatible with NAS servers that use an Oracle database.)
  - Check and make a note of the operating system running on this server.
  - If you are upgrading from the a previous version of the DCI Report Server, you must completely uninstall the DCI Report Server and then follow all the steps in this chapter. See Chapter 3, "Uninstalling, Moving, or Upgrading DCI Report Server" for more information.

The DCI Report Server installation file is about 320 megabytes and can take a while to upload, depending on your network connection. You must have the appropriate permissions to manage software packages in the Opsware Command Center to perform this upload.

Getting Proper User Privileges

Before you can begin installing and configuring DCI, ensure that you are an administrator user that belongs to the Advanced Users group in the Opsware Command Center.

If the Advanced Users group is customized and has lost some of the necessary permissions required for installing and configuring DCI, ensure that the user performing the installation and configuration of DCI belongs to a group that has the following permissions:

- Wizard: Install Software
- Wizard: Uninstall Software
- Data Center Intelligence Reports
- Read permissions on the Other Applications and System Utilities stacks.
- Write permission to the facility and customer of the server

To add a user to Administrator and Advanced User groups, perform the following steps:

1. Log in to the Opsware Command Center as an administrator user.
2. From the navigation panel, click Administration ➤ Users & Groups. The Manage Users: View Users page appears. By default, the Users tab page displays.
3. Click the Administrators tab. The View Administrators page shows current Opsware administrators.
4. Click the **New Administrator** button. The Users & Groups: Add Administrators page appears.
5. Select a user from the list.
6. Click the **Save** button. The Opsware Command Center displays a confirmation message.
7. Click the **Continue** button.
8. The Opsware Command Center adds the user to the current list of Opsware administrators and displays an updated Users & Groups: View Administrators page.
9. To add this user to the Advanced Users group, on the Users & Groups: View Administrators page, click the Groups tab. The Users & Groups: View Groups page appears showing a list of all groups.

10 Click the Advanced Users link name. The Users & Groups: Edit Group - Advanced Users page appears with the User tab selected showing a list of users that you can choose from.

11 In the Unassigned Members box, highlight the names of the members you want to add to the Advanced Users group, and click the left-pointing arrow to move the names into the Assigned Members box.

12 When you finish selecting members, click **Save**. A confirmation page appears.

13 Click **Continue** to return to the Assign Users page. The user now has the proper user privileges to install and configure DCI.

Installing the DCI Report Server

To install the DCI Report Server, you need the Opsware ISMTool. You will also need an Opsware System login and password to download the ISMTool. Contact support@opsware.com if you do not already have a login and password.

To install the DCI Report Server using the ISMTool, perform the following steps:

- Uninstall the Older Version of ISMTool
- Install the ISMTool
- Unpack and Upload the DCI Report Server Package
- Set Custom Attributes Values on DCI Report Server Software Node
- Install the DCI Report Server Software

Uninstall the Older Version of ISMTool

DCI will only work with ISMTool version 2.0.4. So, if you have a previous version of the ISMTool installed, you will need to uninstall it.

To uninstall the older version of the ISMTool, perform the following steps:

1 Log on to the computer where the older version of the ISMTool is installed.

2 From the Control Panel ➤ Add Remove Programs, locate the ISMTool application (for example, ismtool-1.0.6) and remove the older version of the ISMTool application.

3 Log off and then back on to the computer, and then install the newer version of the ISMTool (version 2.0.4).

Install the ISMTool

To install the ISMTool on any Windows 2000 or 2003 managed server, perform the following steps:

1. From the Opsware Command Center, go to the Servers ➤ Manage Servers page.
2. Find the Windows server to install the DCI Report Server software on, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
3. Check the box for the server, and from the **Software** menu choose **Tasks ➤ Install ➤ Application**. The Install Software Wizard window launches.
4. In the Select software page, navigate to System Utilities ➤ Opsware Tools ➤ ISMTool.
5. You will see a list of operating systems that the ISMTool supports. Scroll down to either Windows 2000 or 2003 and check the box next to it to select the ISMTool for installation.
6. Click **Next**.
7. In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.
8. After the preview has finished, click **Next**.
9. In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:
   - If you want to install immediately, click **Install**.
   - If you would like to schedule the installation, in the Schedule section, choose Run Now. In the Notify section, choose if you want to send an e-mail when the installation has finished. When you have finished setting a scheduled time for installation, click **Schedule**.
10. When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page after it has installed.
11. Click **Close** to exit the installation.

Unpack and Upload the DCI Report Server Package

To unpack and upload the DCI Report Server software package, perform the following steps:

1. Copy the `DCIPackage_en-1.5.ism` package to an accessible location on the computer where the ISMTool is installed.
2. Open a command prompt and go to the directory where the ISM has been copied to.
3. Execute the following command:

   ```
   ismtool --unpack DCIPackage_en-1.5.ism
   ```

4. Next, execute the following command:

   ```
   ismtool --upload DCIPackage_en-1.5
   ```

5. You will be prompted to respond to the following confirmation

   ```
   Using an agent gateway to reach an Opsware Core

   Is this correct? [y/n]:
   ```

6. Type `Y` for yes and press ENTER.
7. At the Opsware user name and login prompt, enter the Opsware Administrator user name and password.
8. At the Opsware customer prompt, enter:

   ```
   Customer Independent
   ```

   After successfully uploading, you will see a message stating “Update complete.”

Set Custom Attributes Values on DCI Report Server Software Node

The following steps are critical for the report server to correctly connect to the database. If an attempt to access a report from the Report home page fails after installation, review this information.

To set custom attributes to the DCI Report Server software node, perform the following steps:

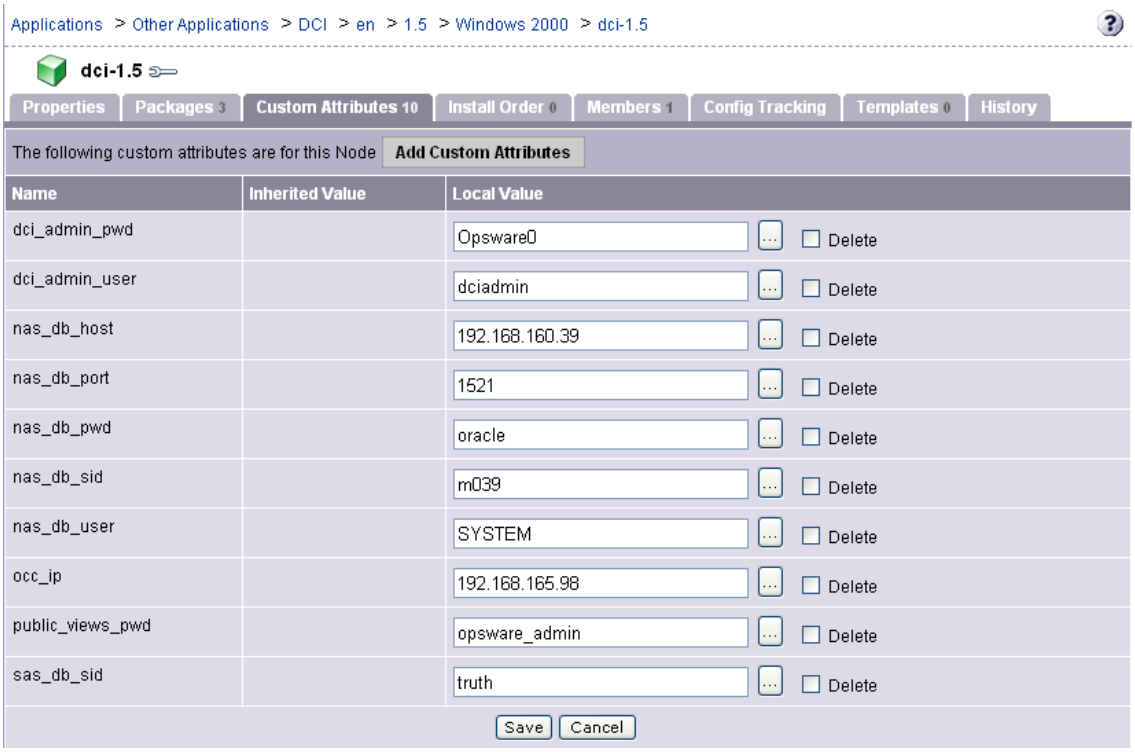
1. From the Opsware Command Center, from the Software link in the navigation bar, click Applications ➤ Other Applications, then navigate to the DCI ➤ en ➤ 1.5 ➤ Windows 200<?> ➤ DCI 1.5.
2. Select the Custom Attributes tab.
3. Click **Edit**.
4. In the Custom Attributes page DCI server, enter the custom attribute values. These attributes are required, and the installation will fail if any of them are missing or incorrect.

Table 2-1: DCI Software Node Custom Attribute Configuration – Required Attributes

CUSTOM ATTRIBUTE	DESCRIPTION
dci_admin_user	The user name for the admin user to be created on the DCI server.
dci_admin_pwd	The password for the DCI admin user. By default, this password is `Opsware0`, but this can be changed.
occ_ip	The IP address of the Opsware Command Center (OCC) to be configured for reporting access.
public_views_pwd	The password for the Opsware_public_views user.
sas_db_sid	The SID of the Opsware Data Repository database. (Make sure that you use the database SID, not the database service name.)

Figure 2-9 illustrates the DCI software node custom attribute fields.

Figure 2-9: DCI Software Node Custom Attribute Fields



5 If you plan to run the DCI server with a NAS server, then you will also need to enter values for the following attributes. These additional attributes are only needed to enable reporting from the Opsware Network Automation System. They must either all be blank, or all have appropriate values.

Table 2-2: DCI Software Node Custom Attribute Configuration – NAS Server Option

CUSTOM ATTRIBUTE	DESCRIPTION
nas_db_host	The hostname or IP address of the NAS database.
nas_db_port	The port on which the NAS database accepts connections.
nas_db_sid	The SID of the NAS database. (Make sure that you use the database SID, not the database service name.)
nas_db_user	The user name of the NAS database.

Table 2-2: DCI Software Node Custom Attribute Configuration — NAS Server Option

CUSTOM ATTRIBUTE	DESCRIPTION
nas_db_pwd	The password for the NAS database.

You can run the DCI server with the OCC alone, with the OCC and NAS, but not with NAS alone. If you do plan to run DCI Report Server with a NAS server, then you will need to fill out all NAS attributes.

6 Click **Save**.

Install the DCI Report Server Software

To install the DCI Report Server software, perform the following steps:

1 Find the server intended to host the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.

2 Check the box for the server, and from the **Software** menu choose **Tasks ➤ Install ➤ Application**. The Install Software Wizard window launches.

3 Click Other Applications, then navigate to the DCI ➤ en ➤ 1.5 ➤ Windows 200<?>.

4 Select the check box in front of dci-1.5 and click **Next**.

5 In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.

6 After the preview has finished, click **Next**.

7 In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:

- If you want to install immediately, click **Install**.
- If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and enter the e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.

8. When the installation has finished, click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.
9. Click **Close** to exit the installation. You are now ready to enable the Opsware Command Center so that other Opsware users can access the report server.
10. Next, from the navigation bar click the Configuration link to go to the System Configuration page.
11. On this page, click the Opsware Command Center link.
12. Scroll down the page and double-check the parameter named owm.features.Reports.allow. Ensure that the value is set to `true`. True means that the installation was successful. If the value is set to false, there was a problem with the installation and you will need to troubleshoot the error. If you see a true value, click **Save** at the bottom of the page. You should now see the Reports link in the navigation panel.

Configuring DCI Report Servers in a Multimaster Mesh

In a very basic deployment, a single core would run a single DCI Report Server. Depending upon your environment, however, you could be running a multimaster mesh (multiple cores) with several cores pointing at a single DCI Report Server.

As your mesh becomes more complex, you might want to add more DCI servers to your multimaster mesh. For example, you multimaster mesh might have one DCI Report Server designated to run reports for a certain group of cores, and a second DCI Report Server designated for a different set of cores.

In these situations, you will need to make modifications to custom attributes on the DCI Report Server and use the DCI reconfigure control to configure the mesh properly.

Remember that when you first installed the DCI Report Server software node, the custom attribute occ_ip was set at the node level to point to the core that you installed the DCI Report Server on. In order to enable additional cores in the mesh to be able to view reports from a single DCI Report Server, you need to add or modify the occ_ip custom attribute on the DCI Report Server itself. When you set a custom attribute at the server level, that value will override that attribute for any nodes attached to that server (in this case, the DCI Server software node).

This section applies to multiple DCI Report Servers that are running on the same operating system – Windows 2000 or Windows 2003. If you introduce a new DCI Report Server that runs on a different operating system than the DCI Report Server already installed in your core, then you need to set the proper custom attributes on the DCI software node following the instructions found at "Set Custom Attributes Values on DCI Report Server Software Node" on page 30. Then, install the new DCI Report Server following the regular DCI Report Server instructions, found at "Install the DCI Report Server Software" on page 32.

The following section shows you how to configure the following two DCI Report Server configuration scenarios:

- Configuring a Single DCI Server in a Multimaster Mesh
- Configuring Multiple DCI Servers in a Multimaster Mesh

Configuring a Single DCI Server in a Multimaster Mesh

If you are using a single DCI Report Server in a multimaster mesh and would like to have more than one core to view reports from that DCI Report Server, you need to add or change the custom attribute named `occ_ip` on the DCI Report Server so that it points to another core in the multimaster mesh. The DCI reconfigure control enables you to set this attribute on the DCI Report Server.

To configure additional cores in a multimaster mesh to view a DCI Report Server, perform the following steps:

1. Find the server that hosts the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. Click the server name link.
3. On the server property page, select the Custom Attributes tab.
4. Click the **Edit** button.
5. Edit the value of the custom attribute named `occ_ip` and enter the IP of the new core you would like to point to the DCI Report Server.
6. Click **Save**.
7. Find the DCI Report Server again, by name or IP address from Servers ➤ Manage Servers, or by Server Search.

8 Select the check mark next to the server.

9 From the **Tasks** menu, choose **Run ➤ Control**.

10 In the DCI Control dialog box, from the Application drop down list, make sure you choose dci-1.5 (Server) and that the Action drop down list is set to Reconfigure.

11 Click **Run**.

12 After the reconfigure control has finished running, from the navigation bar click the Configuration link to go to the System Configuration page.

13 On this page, click the Opsware Command Center link.

14 Click **Save** at the bottom of the page. Even if you make no changes, click **Save** to ensure the proper configuration.

When you run the DCI reconfigure control, the Apache server will be restarted and any users logged into the OCC at the time will be logged off.

Configuring Multiple DCI Servers in a Multimaster Mesh

If you would like to run more than one DCI Report Server in a multimaster mesh, you will need to install each additional DCI Report Server and reconfigure the custom attribute occ_ip for that server to point to specific cores in the mesh.

To introduce a second DCI Report Server into the mesh, you first need to add a new custom attribute named `occ_ip` on the new DCI Report Server, set the `occ_ip` attribute value to the IP address of a new core, and then install the new DCI Report Server software node on the new server.

The reason that you need to create and set a new `occ_ip` custom attribute value on the second DCI Report Server is that you cannot have two DCI Report Servers pointing to the same core. Thus for the second DCI Report Server, you will override the `occ_ip` value that was originally set on the DCI Report Server software node. Remember that when you set a custom attribute at the server level, that value will override the same attribute for any nodes attached to that server (in this case, the DCI Report Server software node).

To configure multiple DCI Servers in a multimaster mesh, perform the following tasks:

- Install the DCI Report Server Software with New Custom Attribute
- Run the DCI Reconfigure Control

Install the DCI Report Server Software with New Custom Attribute

To install a new DCI Report Server in a multimaster mesh, perform the following steps:

1. Find the server intended to host the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. Select the server link (the server's name).
3. In the server's property page, select the Custom Attributes tab.
4. In the Custom Attributes page for the server, click **New**. New attribute fields appear at the bottom of the attribute list.
5. From the Name column, enter

   `occ_ip`

   as the new attribute name.
6. In the Value column, enter the IP address of the core you want to point to the new DCI Report Server.
7. Click **Save**.
8. Click the Return to Manage Servers link.
9. To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ➤ Manage Servers, or by Server Search.
10. Check the box for the server, and from the **Software** menu choose **Tasks ➤ Install ➤ Application**. The Install Software Wizard window launches.
11. Click Other Applications, then navigate to the DCI ➤ en ➤ 1.5 ➤ Windows 200<?>.
12. Select the check box in front of dci-1.5 and click **Next**.
13. In the Confirm Selection page, double-check all the parameters of your selections, and then click **Preview**.
14. After the preview has finished, click **Next**.
15. In the Schedule and Notify page, you have the option of scheduling the ISMTool installation, or installing it immediately:
    - If you want to install immediately, click **Install**.
    - If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and

enter e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.

16 When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.

17 From the navigation bar, click the Configuration link to go to the System Configuration page.

18 On this page, click the Opsware Command Center link.

19 Scroll down the page and double check the parameter named owm.features.Reports.allow. Make sure the value is set to true. True means the installation was successful. If the value is set to false, there was a problem with the installation and you will need to troubleshoot the error. If you see a true value, click **Save** at the bottom of the page.

20 You should now see the Reports link in the navigation panel.

Run the DCI Reconfigure Control

Once you have installed a second DCI Report Server in your multimaster mesh, use the DCI reconfigure control to configure a core to point to the DCI Report Server.

This task is only necessary if additional cores need to be configured.

To run the DCI reconfigure control, perform the following steps:

1 Find the server that hosts the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.

2 Select the check box next to the server (do not click the server name link).

3 From the **Tasks** menu, choose **Run ➤ Control**.

4 In the DCI Control dialog box, from the Application drop down list, make sure you choose dci-1.5 (Server) and that the Action drop down list is set to Reconfigure.

5 Click **Run**.

When you run the DCI reconfigure control, the Apache server will be restarted and any users logged into the OCC at the time will be logged off.

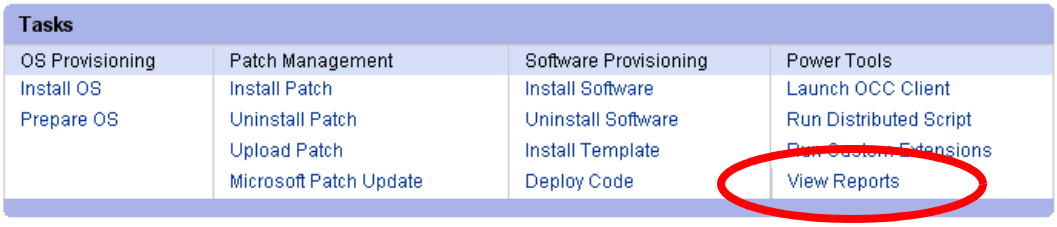
6. After the reconfigure control has run, from the navigation bar, click the Configuration link to go to the System Configuration page.
7. On this page, click the Opsware Command Center link.
8. Scroll down the page and click **Save**. Even if you make no changes, click **Save** to ensure the proper configuration.
9. You should now see the Reports link in the navigation panel.

Accessing Reports in the OCC

You should now see the View Reports link in the Navigation panel and under Power Tools. Figure 2-10 shows how the reporting links appear in the Opsware Command Center.

Figure 2-10: Reporting Links in the OCC Navigation Bar

Figure 2-11: Reporting Links in the OCC – Power Tools



By default, only Advanced Users and Administrators have access to the DCI Report Server. However, you can give users access to the DCI Report Server by giving them DCI permissions. For information about setting and changing user permissions, please refer to the *Opsware System 5.1 Administration Guide*.

Chapter 3: Uninstalling, Moving, Upgrading DCI

IN THIS CHAPTER

This chapter contains the following topics:

- About Uninstalling, Moving, Upgrading DCI Report Server
- Uninstalling the DCI Report Server
- Moving DCI Report Server
- Upgrading the DCI Report Server

About Uninstalling, Moving, Upgrading DCI Report Server

This chapter shows you how to uninstall, move, and upgrade the DCI Report Server. These instructions assume that you are working with a single DCI Report Server in a core. Special considerations regarding multiple DCI Report Servers in a multimaster mesh are discussed where relevant.

Uninstalling the DCI Report Server

To uninstall the DCI Report Server, perform the following steps:

1. Find the server you want to uninstall the DCI Report Server from, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. Check the box for the server, and from the **Software** menu choose **Tasks ➤ Uninstall ➤ Application**. The Uninstall Software Wizard window launches.
3. Select the DCI application and click **Next**.
4. In the Confirm selections page, verify that you have selected the correct software (DCI) and the correct server, and then click **Preview**.

5. Wait for the Preview to complete, and then from the **View Details** button, verify the status is Completed and the Output tab shows that the DCI software node will be uninstalled. Click **Close**.
6. Click **Next**.
7. In the Schedule and Notify page, you have the option of scheduling the DCI uninstallation, or uninstalling it immediately:
   - If you want to install immediately, click **Uninstall**.
   - If you would like to schedule the installation, in the Schedule section, choose Specify Time and select a time from the drop-down list. If you want to send e-mail when the installation has finished, in the Notify section, choose Condition and enter e-mail addresses. When you have finished setting a scheduled time for installation, click **Schedule**.
8. When the installation has finished, you can click **View Details** for more information. If you have scheduled the installation to run later, you can check the Job details from the OCC home page.
9. Once the uninstall software wizard completes, from the navigation bar click the Configuration link to go to the System Configuration page.
10. On this page, click the Opsware Command Center link.
11. Scroll down the page and double check the parameter named owm.features.Reports.allow. Ensure that the value is set to `false`. False means the uninstallation was successful. If the value is set to `true`, there was a problem with the installation and you will need to troubleshoot the error. If you see a false value, click **Save** at the bottom of the page – even if you do not make any changes to the page. The Reports link in the navigation panel will be removed.

On the server where DCI was installed, make sure that the DCI virtual directory on IIS (DCI under default web site) has been fully removed and that the \Program Files\Opsware\DCI\wwwroot directory is absent or contains only a logs directory.

Moving DCI Report Server

In order to move the DCI Report Server, you need to first uninstall the DCI Report Server then reinstall it in its new location. For information on how to uninstall and install, see the following tasks:

- Uninstalling the DCI Report Server on page 41
- Installing the DCI Report Server on page 27

Updating DCI Report Server in Multimaster Mesh

If the DCI Report Server being moved to a multimaster mesh (with multiple OCCs), see the Configuring DCI Report Servers in a Multimaster Mesh on page 33 or more information.

Upgrading the DCI Report Server

In order to upgrade the DCI Report Server, you need to first uninstall the DCI Report Server then reinstall the new version. For information on how to uninstall and install, see the following tasks:

- Uninstalling the DCI Report Server on page 41
- Installing the DCI Report Server on page 27

When you upgrade the DCI Report Server, any existing custom reports will be backed up during uninstallation, so you will not need to reinstall them. After the new version of DCI is installed, the custom reports will be restored to the appropriate structure (prior to the uninstallation).

Chapter 4: Writing Custom Reports

IN THIS CHAPTER

This chapter discusses the following topics:

- Understanding Access to Public Views
- Using a Shipped Report to Create a Custom Report
- Extending Reports with other Data Sources
- Installing a Customized Report
- Sample def.xml for a Custom Report

Understanding Access to Public Views

The Opsware System keeps records of many events and items. Much of this data is available to create your own reports, or to integrate this information with other systems. The primary view of this information is called the Opsware Public Views. It is a set of tables stored in a database. With the right information, you can establish a connection to the database and view this read-only information. Please refer to Appendix A: Public Views of this guide for detailed information about these tables.

You might want to create custom versions of our shipped reports, create your own reports, or create database connections to other systems. This chapter gives you an overview of the data in the public views and shows you how to understand and use it to create your own reports.

Using a Shipped Report to Create a Custom Report

The reports are created and processed with Crystal Reports, Report Application Server 10 (RAS). This software is not included with the DCI Report Server and much be purchased separately from Business Objects (http://www.businessobjects.com/products/reporting/

crystalreports/default.asp). This software allows you to edit .rpt files. You can copy any existing report from the report server located in the %SystemDrive%\Program Files\Opsware\DCI\wwroot\Reports folder as your starting point.

If you are unfamiliar with Crystal Reports, ask Opsware Professional Services for assistance.

The reports take advantage of an Open Database Connectivity (ODBC) connection to the Opsware Oracle database, which can be seen on the System DSN tab, in the Start Menu ➤ Settings ➤ Control Panel ➤ Administrative Tools ➤ Data Sources (ODBC) on a Windows 2000 computer.

The database is accessed through the Public Views of the Model Repository. The Model Repository contains the tables listed in Appendix A of this guide. These tables can be used to generate new reports. The existing reports take advantage of the RAS Server for dynamically generating the correct report based on the input from the forms on the report server home page. Use of the report server API is not necessary to create reports but it does create a cleaner user interface. Consult the RAS documentation installed on the report server for more information about how to use the API (see the Start ➤ Programs ➤ Crystal Enterprise 9 ➤ Documentation menu).

Editing any of the reports that are shipped with the report server is not recommended. Doing so will result in losing these reports when you upgrade. To enhance an existing report, make a copy of the report, edit it, and place the finished file in the Custom folder. All existing reports contain special functions and parameters that the DCI home page uses. These functions and parameters should be removed from any customized reports to streamline custom reporting.

Extending Reports with other Data Sources

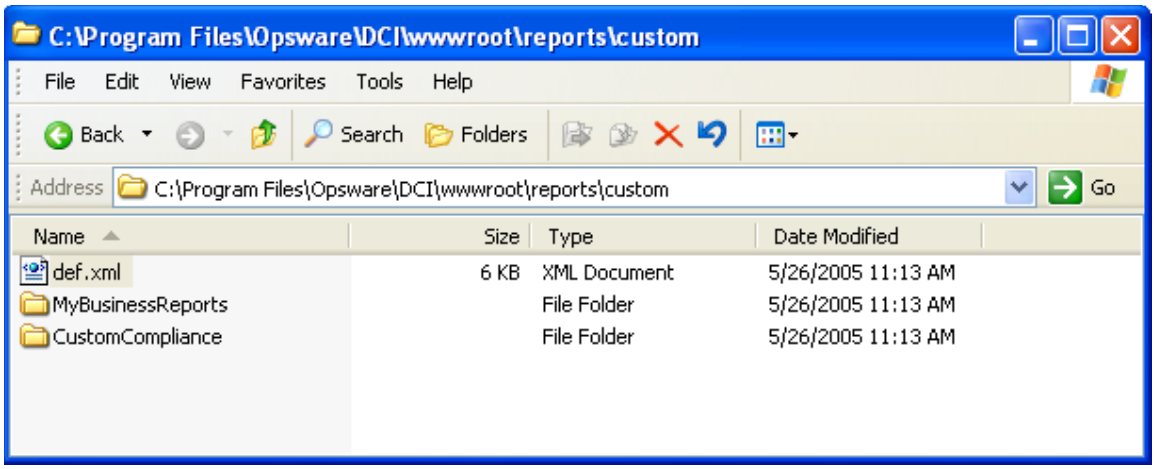
Crystal Reports allows one report to connect and relate to more than one data source. With the correct key fields, a report developer can create reports that combine the Opsware data source with other data sources that might contain more detailed server information, cost or depreciation information, or application tracking information.

Installing a Customized Report

Custom reports should be placed put in either the custom folder or in a sub folder directly under custom folder. For example, %SystemDrive%\Program Files\Opsware\DCI\wwwroot\reports\custom.

If report filenames are suitable for display in DCI then no extra step is needed outside of placing the file in the folder. However, to have DCI display different names for the reports or folders, the def.xml file must be configured in the folder with the reports. (See the def.xml sample file for details)

Figure 4-1: Adding a New Report to the Custom Reports Folder



In addition to having the file name automatically appear on the home page, the Custom Report section can be configured to show a more descriptive name for a report, subsection names (for the left and right columns), a title for the section, and reorder the reports in the left and right columns. To make any of these configurations, edit the def.xml in the folder %SystemDrive%\Program Files\Opsware\DCI\wwwroot\reports\custom. Also, each subfolder in Custom Report may have its own def.xml as well.

See the detailed instructions inside the sample def.xml file for more information.

Alphabetical order is the order they will appear on the home page. Reports in the Custom folder that do *not* have an entry in the configuration file will *not* appear on the home page.

You can use HTML tags in the configuration file to change the appearance of the labels for the reports, but make sure you use valid HTML tags, or it might affect the rest of the home page.

Sample def.xml for a Custom Report

The following example illustrates how the def.xml can be marked up for a custom report.

```
<!--sample def.xml for custom reports category

The def xml file is used to display DCI reports in the OCC.

The root element is the <sections> tag.

Inside the <sections> tag are three types of sections:

<text_section>
This is an optional section that can be used to display textual
information on the page. Multiple text sections may be defined
for a page.

<folder_section>
This section is used solely in reporting category definitions to
define subfolders within the category.

<report_section>
This section is used to define report sections with report links
and descriptions. Multiple text sections may be defined for a
page.

When sections are displayed in the OCC, they are shown in the
order in which they are defined in the def.xml file.

Note:

Sometimes you need to include data in this file that might
contain XML-like tags and other data that you don't want XML to
interpret. XML has a special section called CDATA that you can
use to eclose text data. A CDATA section starts with '<![CDATA['
and ends with ']]>'. You might, for example, want to include
HTML text in the description for a text_section. You don't want
the XML parser to interpret the HTML tags.

Here is an example:

<description>
<![CDATA[
<b>This text is not parsed by XML parser</b>
]]>
</description>
-->
```

```
<sections>
    <!-- title is displayed by the DCI UI Navigation Display at
top of the page. This is not used if within
         a subfolder of a category that has already defined the
subfolder's displayname. -->

    <title>Custom Reports</title>
    <!-- The text section is an optional section used to display
textual information.  -->
    <text_section>
        <!-- The title of the section -->
        <title>Overview</title>
        <!-- The descriptive content of the section. May include
HTML if enclosed in CDATA tags.  -->
        <description>
            The custom category is where the customer can add
their own folders and reports
        </description>
    </text_section>
    <!-- The folder section is used to display subfolders within
a reporting category. This section should only
         be defined in the def.xml of a reporting category. It
does not have any purpose in the def.xml of a
         category subfolder. -->
    <folder_section>
        <!-- title of section -->
        <title>My Folders</title>
        <!-- The folder section has a folder element for each
subfolder within the category. Folders are displayed
             in alphabetical order. -->
        <folder>
            <!-- The name of the physical subdirectory to which
the subfolder applies (required).
                 In this example, the subdirectory referenced by
'folder1' would be
                  DCI\wwwroot\reports\custom\folder1 -->
            <name>folder1</name>
            <!-- The name to display in place of physical folder
name (if this element is not
                 defined then the name value will be used for
displayname) -->
            <displayname>
                Sample Folder 1
            </displayname>
        </folder>
        <folder>
            <name>folder2</name>
```

```
            <displayname>
                Sample Folder 2
            </displayname>
        </folder>
    </folder_section>
    <!-- The report section is used to define links to reports.
Multiple report sections may be defined
        to group reports within the same page.  -->
    <report_section>
        <!-- The displayed title of the section -->
        <title>My Reports</title>
        <!-- One or more report elements should be defined for
each report section. Reports within the
             same report section are listed in alphabetical
order. -->
        <report>
           <!-- The report file name (required). If displayname
is not defined, this value will be
                used with the extension stripped off.-->
            <name>sample_report_1.rpt</name>
            <!-- The displayed report name (optional). If this
element is not defined then the name
                 value will be used for display. -->
            <displayname>Sample Report 1</displayname>
           <!-- The description is displayed beside the report
name (optional) -->
            <description>... Description for report 1 ...</
description>
            <!-- The location of the report relative to DCI/
wwwroot/reports if not in the current
                 folder (optional, if in current folder) -->
            <path>shared\server</path>
           <!-- An optional URL to the ASP used to display the
report. The URL may contain a
                query string. The parameter 'ReportName' is
always appended to the end of this
               URL as in '&ReportName=sample_report_1.rpt'. The
URL string should always be enclosed
                in CDATA tags.  -->
            <url>
                <![CDATA[
                viewer/
MyDCIViewer.asp?serverType=managed&FilterBy=Hostname
                ]]>
            </url>
        </report>
        <report>
```



```
            <name>sample_report_2.rpt</name>
            <displayname>Sample Report 2</displayname>
            <description>... Description for report 2 ...</
description>
        </report>
    </report_section>
</sections>
```


Chapter 5: DCI Report Server FAQ

IN THIS CHAPTER

This chapter discusses the following topics:

- How Do I Restart or Stop the DCI Report Server?
- How Do I Change the DCI Username and/or Password?
- How Do I Change the Public Views Password in Oracle?
- How Do I Change the Public Views Password In DCI?
- How Do I Keep the Public Views Password Secure?
- What Time Zone is Used in Reporting?
- Can I Share the DCI Report Server With Other Web Applications?

How Do I Restart or Stop the DCI Report Server?

In order to start and stop the DCI Report Server, perform the following steps:

1. On the DCI server, open the Crystal Configuration Manager from Programs ➤ Crystal Enterprise 10.
2. Right-click the Crystal Report Application Server (RAS) and select **Stop** to stop the RAS service.
3. Right-click the Crystal Report Application Server (RAS) and select **Start**.

How Do I Change the DCI Username and/or Password?

If you want to change the DCI user name and/or password, modify the following custom attribute values the server, and then use the DCI reconfigure control to implement the changes:

- `dci_admin_user`
- `dci_admin_pwd`

1. Find the server that hosts the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. Select the server link (the server's name).
3. In the server's property page, select the Custom Attributes tab.
4. In the custom attribute list, scroll down and modify the values of the following attributes to create a new DCI user name and password:

   `dci_admin_user`

   `dci_admin_pwd`
5. Click **Save**.
6. To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ➤ Manage Servers, or by Server Search
7. Select the check box next to the server (do not click the server name link).
8. From the **Tasks** menu, choose **Run ➤ Control**.
9. In the DCI Control dialog box, click the View Parameters link.
10. From the Application drop down list, make sure you choose dci-1.5 (Server) and that the Action drop down list is set to Reconfigure.
11. After you have make the appropriate changes to the attributes, click **Run**.

When you run the DCI reconfigure control, Apache server will be restarted and any users logged into the OCC at the time will be logged off.

How Do I Change the Public Views Password in Oracle?

If you have access permissions to the Oracle installation for the Opsware System, you can use SQL to change the Opsware public views password (you must know the current password). After you have changed the Oracle password, you will have to change the password stored on the DCI Report Server. For information on changing the DCI Report Server password, see "How Do I Change the Public Views Password In DCI?" on page 55.

Perform the following steps to change the password in Oracle. For this example, we assume that the name of the new password will be "`publicpassword`".

1. Log in as root to the server where Oracle is running.
2. Bring up a terminal window and press return after each of the following steps
3. At the Unix command line type:

   ```
   su - oracle
   ```

   and press ENTER.
4. Connect to Oracle through SQL*Plus by running:

   ```
   sqlplus "/ as sysdba"
   ```
5. At the SQL> command-prompt type:

   ```
   ALTER USER opsware_public_views IDENTIFIED BY
   publicpassword;
   ```

   and press ENTER.
6. You should see the message “User altered” which indicates the command ran successfully.
7. Exit SQL*plus by entering `exit` at the command line.

How Do I Change the Public Views Password In DCI?

The Public Views user ID is created on the DCI Report Server during installation and is used for authentication between the OCC and the DCI Report Server. To change the password value of Public Views password, modify the server custom attribute named `public_views_pwd` and then use the DCI reconfigure control to implement the changes.

1. Find the server that hosts the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. In the server's property page, select the Custom Attributes tab.
3. In the custom attribute list, scroll down and modify the values of the following attributes to create a new DCI user name and password:

   `public_views_pwd`
4. Click **Save**.
5. To find the DCI Report Server you just added the new custom attribute to, search by name or IP address from Servers ➤ Manage Servers, or by Server Search

6. Select the check box next to the server (do not click the server name link).
7. From the **Tasks** menu, choose **Run ➤ Control**.
8. In the DCI Control dialog box, click the View Parameters link.
9. From the Application drop down list, make sure you choose dci-1.5 (Server) and that the Action drop down list is set to Reconfigure.
10. Click **Run**.

How Do I Keep the Public Views Password Secure?

The DCI Report Server public views password is a custom attribute in the Opsware Command Center. It is saved in plain text so the report server installer will configure the correct files to access the database for gathering report data. If keeping the password in this field in the Opsware Command Center is a security issue, you can remove the value after you complete the installation. The opsware_public_views user is a read-only account, and administrators with permission to view this server are able to see the value. You will need to set the password custom attribute again if you upgrade the server or set up a new DCI Report Server.

To make the DCI Report Server public views password secure, modify the DCI custom attribute named `public_views_pwd` so that its value is blank and then save the change. Do not reconfigure the DCI Report Server. (This assumes that you have already set the public views password at least once.)

To keep the DCI Report Server public views password secure, perform the following steps:

1. From the Opsware Command Center, click Other Applications, then navigate to the DCI ➤ en ➤ 1.5 ➤ Windows 200<?> ➤ DCI 1.5.
2. Select the Custom Attributes tab.
3. Click the **Edit** button.
4. In the Custom Attributes page DCI server, locate the custom attribute named `public_views_pwd` and delete the value.
5. Click **Save**.

What Time Zone is Used in Reporting?

The core for the Opsware System installation depends on UTC (Greenwich mean time). Thus, all reports display date and time information in UTC. This setting is not configurable. However, reports will show a time stamp from the DCI Server where IIS is installed.

Can I Share the DCI Report Server With Other Web Applications?

Yes, DCI Report Server is installed into its own work area within IIS on the server and should not interfere with other Web services that are running on the same servers.

Chapter 6: Troubleshooting the DCI Report Server

IN THIS CHAPTER

This chapter discusses the following topics:

- Troubleshooting General Errors In the DCI Report Server
- Miscellaneous DCI Report Server Troubleshooting
- Contacting Opsware Support

Troubleshooting General Errors In the DCI Report Server

This section describes how to troubleshoot common DCI Report Server issues. If you are experiencing problems with your DCI Report Server, browse through these steps and determine if any apply to your situation.

- Step 1 - Did the DCI Package Upload?
- Step 2 - Did the DCI Report Server Install?
- Step 3 - Can You Access DCI in the OCC?
- Step 4 - Can You View a Standard Report?
- Step 5 - Do You See Any Custom Reports, And Are They Working?

Step 1 - Did the DCI Package Upload?

Check to make sure that the DCI package properly uploaded into the Opsware Command Center. If you experience problems with the upload process, contact Opsware Support. For more information on how to contact Opsware Support, see “Contacting Opsware Support” on page 68.

Step 2 - Did the DCI Report Server Install?

Verify that the DCI report server installed successfully by pointing to the server's URL from a Web browser (for example http://<server_name>/dci).

If DCI did not install properly, check the log files to see what error message was recorded. Errors that occur during installation are recorded in the Program Files\DCIPackage_en-1.5logs\dci_install.log file. You can also access this log file from the My Jobs details in the Opsware Command Center. In addition to the log file, DCI also reports the following error codes to the Install Software Wizard, as shown in Table 6-1.

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
Error 100 Insufficient disk space available. Installation halted.	The amount of space required for unpacking and installing the application components is not available. To solve this problem, uninstall the DCI Report Server software, ensure the documented space requirements are met, and begin installation again.
Error 101 IIS has not been installed or started.	Check IIS prerequisites. This means that the IIS service is not running. Ensure that IIS is installed and running, then uninstall the DCI Report Server and begin installation again.
Error 102 RAS installation failed.	Check the Event Viewer. The Report Application Server installation failed. Check the Event Viewer for any relevant errors. Uninstall and begin installation again.
Error 103 Failed to create the Virtual Directory DCI.	Check the Event Viewer. The installation could not create the IIS virtual directory, possibly due to inappropriate custom attribute settings. Check the log for explanatory messages, resolve any issues, and run the dci-1.5 reconfigure control (Managed Servers ➤ Tasks ➤ Control).
Error 113 Failed to enable ASP Scripting in IIS 6.0.	IIS could not be configured to allow ASP scripting. Check the log for explanatory messages, resolve the issue, uninstall and begin installation again.
Error 114 DCI requires Service Pack Level 3 or higher for Windows 2000.	Windows 2000 appears to be at an unsupported Service Pack level. Ensure that Service Pack 3 or later is installed, uninstall and begin installation again.

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
Error 115 Failed to install ODBC Drivers (`%errorlevel%`).	The ODBC Driver installation failed. Uninstall and begin installation again.
Error 118 DCI currently installed.	Please follow upgrade procedures. Then Check IIS prerequisites. The DCI Report Server application appears to already exist on the server. Ensure that this is not the case. This is triggered by the presence of the directory `%Program Files%\Opsware\DCI\wwwroot\common`. If this directory has been left behind after an uninstall, remove it, uninstall, and begin installation again.
Error 119 Failed to contact (ping) the Data Repository, truth.host (`%truthhost%`).	The hostname “truth” must be accessible from the DCI server. Verify connectivity and name resolution, uninstall, and begin installation again.
Error 122 Failed to contact (ping) the NAS Database Host, (`%nas_db_host%`).	The IP address/hostname provided could not be accessed from the DCI server. Verify the address or hostname, and connectivity, then uninstall and begin installation again.
Error 131 Incomplete NAS configuration.	You must supply all parameters or none. The five custom attributes for NAS reporting must either all be blank, or contain all values. Uninstall the package, set the appropriate values as described in the documentation and begin the installation again.
Error 132 Failed to contact (ping) the OCC host (`%occ_ip%`).	The IP address provided could not be accessed from the DCI Report Server. Verify the address and connectivity, uninstall and begin installation again.
Error 139 Invalid argument: '`%1`'.	Must be either install or reconfig. The installation/ reconfiguration was not started through the OCC's install/ control interface. Contact Opsware Customer Support.

Table 6-1: DCI Report Server Installation Errors and Solutions

DCI INSTALLATION ERROR NUMBER/ DESCRIPTION	EXPLANATION/SOLUTION
Error 140 Failed to retrieve custom attributes from ISM parameters interface.	The ISM could not access the custom attributes. Contact Opsware Customer Support.
Error 141 Missing one or more required Custom Attributes.	All five of the custom attributes related to SAS reporting are required. Uninstall the package, set the appropriate values as described in the documentation and begin installation again.
Error 138 Failed to configure OCC for DCI access. Configuration of the OCC failed.	Possibly due to inappropriate custom attributes. Correct the custom attribute values, and run the dci-1.5 reconfigure control (Managed Servers ➤ Tasks ➤ Control).
Error 255 Failed to create DCI Admin User. Could not create the DCI Admin User account.	Possibly due to inappropriate custom attribute settings. Check the log for explanatory messages, resolve any issues, and run the dci-1.5 reconfigure control (Managed Servers ➤ Tasks ➤ Control).

Step 3 - Can You Access DCI in the OCC?

If your DCI Report Server was installed and configured correctly, you should be able to access it from the OCC. You will know if the installation and configuration was successful if you can see the following DCI links in the OCC:

- The View Reports in the Power Tools section of the OCC home page.
- The View Reports link in the navigation panel
- A list of links below the Report links in the navigation panel: Server Reports, Compliance Center, Network (if you have NAS configured), Custom Reports, and Ad Hoc Reporting

If you do not see the DCI Report Server links in the OCC, try the following steps:

1. Inside the OCC where your DCI Report Server is installed, from the navigation bar click the Configuration link to go to the System Configuration page.

2. On this page, click the Opsware Command Center link.

3. Scroll down the page and double check the parameter named `owm.features.Reports.allow` has its value set to `true`. True means the installation was successful. If the value is set to false, there was a problem with the installation and you will need to troubleshoot the error. If you see a `true` value, click **Save** at the bottom of the page. Even if you make no changes, click **Save** to ensure the proper configuration. You should now see the Reports link in the navigation panel.

If you are viewing a DCI Report Server in a multimaster mesh where there might be more than one DCI Report Server, make sure that you modify the correct DCI Server in the mesh.

Step 4 - Can You View a Standard Report?

If you can view the DCI home page but can not click on a report name to view an actual report, several problems might be occurring. The following error is caused by having cookies in your browser turned off.

```
* Error Type:
     Microsoft VBScript runtime (0x800A01A8)
     Object required: 'Session(...)'
```

To fix this problem in Internet Explorer 5.x and 6.x, go to Tools ➤ Internet Options ➤ Privacy and move the security slider for cookies to medium or lower. If you are receiving a different VBScript runtime error, if might be caused by insufficient memory on the report server. Try increasing the server's memory. If the runtime error still persists, send the error details to Opsware support for assistance.

If you see an ODBC login screen, it is possible that your database connection is not properly configured. Check to make sure that:

- For SAS reports, the following custom attributes must be configured correctly:

  `public_views_pwd`

  `sas_db_sid`

- For NAS reports, all custom attributes must be configured correctly.

To set custom attributes to the DCI Report Server software node, perform the following steps:

1. Find the server that hosts the DCI Report Server, by name or IP address from Servers ➤ Manage Servers, or by Server Search.
2. Select the check box next to the server (do not click the server name link).
3. From the **Tasks** menu, choose **Run ➤ Control**.
4. In the DCI Control dialog box, click the View Parameters link.
5. In the custom attribute list, scroll down and modify the values of the appropriate custom attributes.
6. After you have make the appropriate changes to the attributes, click **Run**.

Step 5 - Do You See Any Custom Reports, And Are They Working?

If you can view a standard report, but not a custom report, the problem lies within either your custom report itself or the custom configuration definition file (def.xml).

First, check to make sure your custom reports reside in the proper folder. Then, check to make sure the custom configuration properties file has been properly written. See Chapter 5, "DCI Report Server FAQ" on page 53 of this guide for more information.

Miscellaneous DCI Report Server Troubleshooting

This section shows you how to solve various problems you might encounter with DCI Report Server and contains the following topics:

- Delay Occurs While Generating Some Server Reports
- Prompt for User Name/Password When Accessing DCI Home Page
- Database Login is Displayed When Running a Report
- Microsoft VBScript Runtime Error
- Running a Report Returns a Page Full of "unspecified errors"
- Images and Graphs Missing on a Report
- A Report "hangs" for Longer Than Five Minutes
- Troubleshooting Windows Permissions for DCI

- DCI User Not Created on Windows
- Error Seen on All Links in a Report

Delay Occurs While Generating Some Server Reports

If you experience a delay in the generation of some server reports, there are two factors that could produce this delay: one is a delay in database updates as result of reconcile processes; the other is related to the caching of report data by Crystal RAS.

Crystal RAS has a configuration setting for the maximum time that previously queried data is allowed to be displayed in a report before refreshing the data. The default setting is one hour. Reports will display faster as long as cached data is used. Increasing this value causes data to be cached longer. Once the cache expires, the report has to requery the data, which will slow the report by the amount of query time. Reducing the setting causes the data to be cached for a shorter period of time and allows changes in the Opsware system to be seen in reports sooner.

To modify the RAS data caching, perform the following steps:

1. On the DCI server, open the Crystal Configuration Manager from Programs/Crystal Enterprise 10.
2. Right click the Crystal Report Application Server (RAS) and select **Stop**.
3. Right-click again and choose **Properties** to display the Properties page.
4. Select the Parameters tab to display the RAS parameter settings.
5. Change the Data Refresh setting to the maximum allowable age of cached report data in minutes. This value may be set to zero to always retrieve the most recent data.
6. Right-click the Crystal Report Application Server (RAS) and select **Start** to start the RAS service.

Prompt for User Name/Password When Accessing DCI Home Page

If you attempt to access the DCI Report Server and you are prompted with a pop up dialog asking for a user name and password, it is possible that the dci_admin_user and dci_admin_pwd are not properly configured. For information on how to set these custom attribute values, see the instructions for changing DCI Report Server custom attributes in the troubleshooting step named “Step 4 - Can You View a Standard Report?” on page 63.

Database Login is Displayed When Running a Report

This probably means that the Crystal Reports Application server in the DCI Report Server is unable to connect to the database. There are several possible solutions:

- Check that the Opsware DCI ODBC configuration is valid.
- Check that the host, port, and SID settings are correct. For more information, see the troubleshooting step named "Step 4 - Can You View a Standard Report?" on page 63.
- Verify that the host is accessible from the DCI Server. For SAS reports, the hostname "truth" should be assessable. For NAS reporting, the custom attribute named nas_db_host must be correct.
- Verify that the database and its listener are started.

Microsoft VBScript Runtime Error

If you run a report and get the following error:

```
Microsoft VBScript runtime error '800a01a8' Object required:
'Session(…)'
```

This means that the ASP within the DCI Web application redirects the request to another URL and the browser is unable to obtain the session cookie for the current ASP session. Ensure that the browser is configured to accept cookies.

Running a Report Returns a Page Full of "unspecified errors"

In some cases, running a report may result in a page full of errors beginning with:

```
Unspecified error; Error code 0x80004500; Source:
webReporting.dll.
```

Error messages will also include:

```
renderPage failed
```

and

```
RenderContent failed
```

Typically this error is seen when either the dciadmin user or the IUSR_<machinename> user on the DCI server do not have appropriate permissions to the system TEMP directory. Grant full access to the system TEMP directory and its subdirectories. If this does not correct the problem, see"Troubleshooting Windows Permissions for DCI" on page 67.

Images and Graphs Missing on a Report

Typically this error is seen when the IUSR_<machinename> user on the DCI server does not have appropriate permissions to the system TEMP directory. Grant full access to the system TEMP directory and its subdirectories. If this does not correct the problem, see "Troubleshooting Windows Permissions for DCI" on page 67.

A Report "hangs" for Longer Than Five Minutes

A report can appear to be hanging for the following reasons:

- The report is running, yet it is either very complex or has to process a large amount of data or both. Some reports can run for hours in an environment with a large amount of data.
- The report is running, yet there are problems with database optimization.
- The number of available Crystal Report sessions has been exceeded and the current report is waiting for one to become free. The default number of session licenses is three. This becomes a problem when the number of reports being run exceeds the number of session licenses. Licenses should be increased if report usage warrants it.
- There may be a problem with either IIS or the Crystal Reports Application Server. Restart IIS and then restart the Crystal Report Application Server service.

Troubleshooting Windows Permissions for DCI

In general, when there are potential permission problems in Windows, use the following procedure to pinpoint the issues:

- Use the Windows Local Security Policy tool to set the local Audit Policy to audit failed object access attempts.
- Go to Properties of the C: root directory, click the Advanced button on the Security tab, then set Auditing on the Users group to Full Control for Failed access. After clicking OK, it may take a while to propagate the settings to all subdirectories. You could set up Auditing on more specific directories, but this approach ensures that we catch all access problems on C:. Of course, these settings should all be temporary until the problem is resolved.
- Reproduce the permissions-related error and check the Security event log for failed access events. Events of type 560 should specify the user, the object being accessed, and the requested permissions.

DCI User Not Created on Windows

If the password that you specify in dci_admin_pwd does not meet the security requirements for the DCI Report Server, then the DCI user will not get created. If this is the case, you will see installation error 255. For more information on this installation report error, see "Step 2 - Did the DCI Report Server Install?" on page 59.

To fix this problem, you will need to reset the dci_admin_pwd with a value that meets the security requirement of your facility. For information on how to change this password, see the instructions for changing DCI Report Server custom attributes in the troubleshooting step named "Step 4 - Can You View a Standard Report?" on page 63.

Error Seen on All Links in a Report

The DCI home page loads but all links have the following error

```
* Error Type:
  clientdoc.dll (0x80041015)
  Failed to connect to server "<servername>". Error
  returned from Windows Sockets API : 0.
  /DCI/viewer/customReportViewer.asp, line 29
```

To solve this problem, restart Crystal Reports.

Contacting Opsware Support

When you contact Opsware Support, have the following information available to help you with your support call:

- Be at your computer and have network access to the servers running the Opsware core.
- Have your Opsware guides available.
- Write down the steps followed prior to the problem occurring.
- Write down the exact text of the error appearing on your screen or print out the page on which the error appears.
- Be able to describe the problem in detail.

Contact Opsware Technical Support:

Phone: +1 877 677-9273 (1-877-Opsware), in the United States
International Phone: 1 408-212-5300
E-Mail: support@opsware.com

Index

