OPSWARE INC
Automating IT™

Opsware® System Data Center Intelligence 1.2 Administrator's Guide

Table of Contents

Chapter 3: Uninstalling, Moving, or Upgrading the DCI Report Server 28

Chapter 4: Writing Custom Reports 32

Chapter 5: DCI Report Server FAQ 37

Chapter 1: Opsware Data Center Intelligence Overview

IN THIS CHAPTER

This chapter provides an overview of the features and functions of the Opsware Data Center Intelligence Report Server (DCI), and includes the following topics:

- Access Information Across the Entire Data Center Environment

- Accurate Change History Information

- Comprehensive Patch Reports

- Easy Installation

- Rich Reporting

- Custom Report Integration

- Throughput and Performance

- Licensing

- Initial Deployment

- Processor Licensing

- Software and the Intelligent Software Module Development Kit

- Integration with the Opsware System

Welcome to the Opsware Data Center Intelligence (DCI) - an enterprise-class reporting system designed to integrate with Opsware System 4.7. The DCI provides real time intelligence and in depth reports that augment utilization of the Opsware System. This guide describes how to install and administer the DCI. It provides information about the architectural framework, installation methods and options, uninstalling, moving and upgrading the DCI, and customization instructions.

This guide is intended for system administrators who are responsible for installing and managing the DCI.

Access Information Across the Entire Data Center Environment

The DCI provides a comprehensive view of server and system across all hardware and software platforms and physical locations. Users can generate on-demand reports of any aspect their system from a single, high-quality data source. The pre-configured assets and change-history quick reports available on the DCI home page provide one-click access to real-time information for commonly required reporting functions. Ad-Hoc Reporting extends the reporting capability to generate a variety of highly focussed report types, which can be filtered by specific criteria and then displayed as a graphical view or

list. Placing your mouse over a specific report link or tab on the home page displays a snapshot of the report that will be generated. The following image shows a typical view of the DCI home page with a close up of a graphical report page.

Figure 1-1: The DCI Home Page and a Sample Report
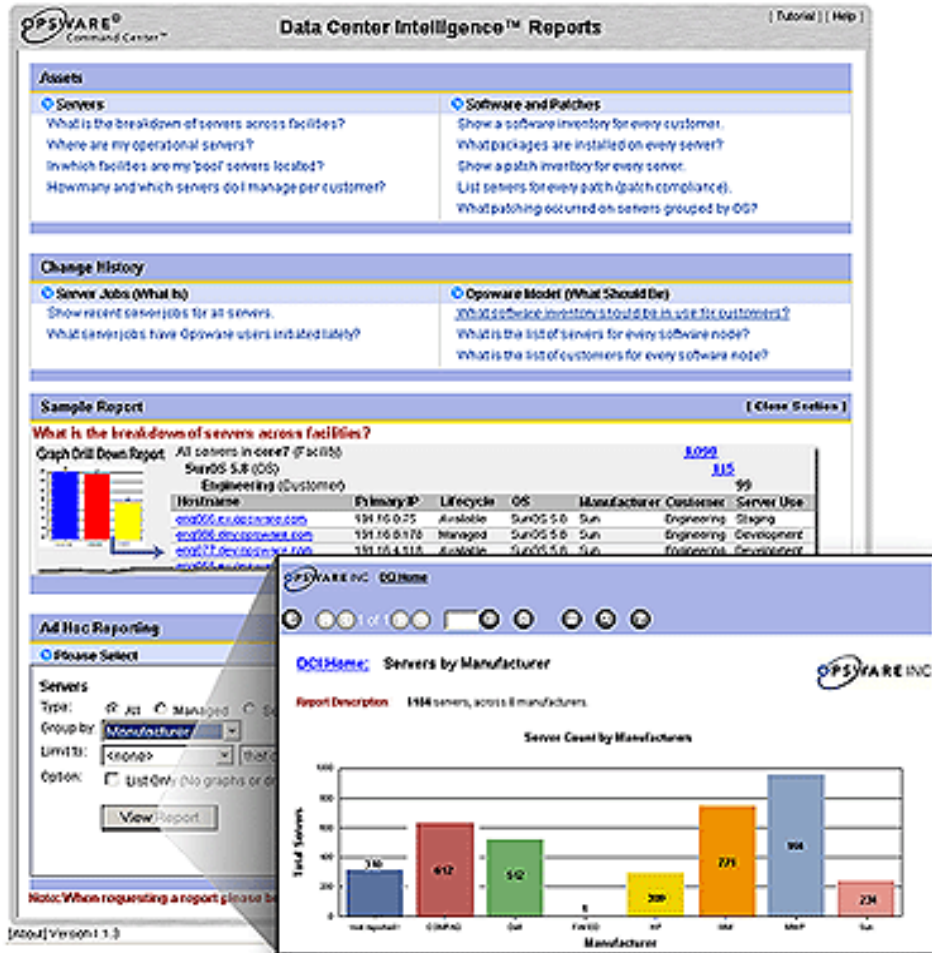
Accurate Change History Information

If a server's performance suddenly degrades, one of the best ways to diagnose the cause is to learn what changes have been recently introduced to the server, who made the changes, and when the changes occurred. This change history trail is usually difficult to obtain. In many cases, records are not accurately kept. The Opsware System

automatically maintains detailed records of each change: showing who, what, and when for every change on every server. These records are presented in a comprehensive series of server job reports that can significantly reduce the time and effort involved in debugging server and software problems.

Comprehensive Patch Reports

One of the most time-consuming aspects of installing patches is identifying which servers are vulnerable and in need of patching. Data collection for this task typically involves manually logging onto each server to find software versions and installed patches. The DCI helps administrators avoid this repetitive and time consuming task by offering a comprehensive set of patch management reports, including Windows patch update reporting. You can find these reports in the Software and Patches reports on the DCI home page. You can further customize your report results by using the Ad-Hoc Reporting tools.

Easy Installation

The DCI Report Server runs on Windows 2000 (IIS 5.0) with Service Pack 3 or higher or Windows 2003 (IIS 6.0) and integrates with the existing Opsware System 4.7. It installs onto a managed server seamlessly from the Opsware Command Center and is accessible from the Opsware Command Center Navigation panel.

Rich Reporting

The DCI consists of over 20 report (.rpt) files, many of which are flexible enough to generate 10 to 20 unique reports each, depending on the specific request. These files and the Web-based user interface can generate over 100 different reporting views. The reports are installed in the \Program Files\Opsware\DCI\Reports folder.

Custom Report Integration

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

crystalreports/default.asp). See Chapter 4, "Writing Custom Reports" for more information about creating customized reports. The database information used to create these reports is available to a report designer to create custom reports. See Appendix A, "Public Views" for a detailed view and description the database public views.

You can also contact Opsware Professional Services to help modify any shipped Opsware report or to create new customized reports for your particular needs. Custom reports can also be extended to integrate with other data sources (databases, spreadsheets, XML, and more) for more advanced data intelligence mining.

To create and integrate a custom report:

1   Create a new report (using Crystal Reports 9), or create a copy of an existing report.

2   Modify the report.

3   Place the completed report in the \Program Files\Opsware\DCI\Reports\Custom folder.

Reports in this folder are automatically added to the Reports home page. With the use of a properties file, custom reports can be further configured with a more descriptive label, section headings, and placed in a specific order on the home page. To write and incorporate custom reports, please see the detailed instructions in Chapter 4, "Writing Custom Reports" for more information.

Throughput and Performance

Report Application Server 10 (RAS) is a multi threaded report processing engine from Business Objects (http://www.businessobjects.com). It runs in an on-demand mode, meaning that it processes report requests as it receives them, and queues any requests that cannot be immediately processed.

RAS also includes server-side caching technology to speed the delivery of frequently requested content. After a port is processed, it is kept open on the server for a specific period of time so that subsequent report pages can be generated and other operations can be performed more rapidly.

The throughput of RAS can be extended with additional licensing from Opsware Inc.

Licensing

You may install a single instance of RAS. To run more than one Report Application Server, you must purchase additional copies of the Professional/Developer Edition from Business Objects or speak to your Opsware sales professional for special pricing. You cannot cluster multiple instances of RAS together through use of a Web farm to increase the scalability of a single application.

Initial Deployment

The RAS technology in the DCI product includes queuing technology and caching capabilities to provide a high level of production scalability for deployment of Web applications with variable user loads. The scalability of applications depends on many factors including the number, size, and complexity of reports, usage patterns, and data connectivity requirements. For Opsware System 4.7 customers, a bundled version of Crystal Decisions Advanced Edition is available which allows a single instance of RAS to be installed.

Processor Licensing

Opsware Inc., through agreement with Business Objects, offers additional processor licensing to unlock the full power of the server technology for unlimited access. A license is required only for the exact number of processors running RAS. Processor licensing of RAS allows you to cluster together multiple instances of RAS.

Software and the Intelligent Software Module Development Kit

The DCI software consists of the following components:

- Report Application Server (referred to as the Report Server)

- Web files (the ASP, JavaScript and image files as well as help documentation and the user training tutorial)

- Configuration files

- Reports

These components are installed onto an Opsware managed server using Opsware's Intelligent Software Module Development Kit (IDK), or by using the package upload process.

Your license includes broad support for major development platforms. The product includes Java, .NET, and COM APIs as well as a range of sample applications written in each of these languages, so you can extend the reporting capabilities of the Opsware System.

Your bundled version of Crystal Decisions Advanced Edition enables your developers to view reports and set data source and parameter information. A flexible set of report creation APIs are also included to aid developers in creating and modifying reports with a Web application. The Advanced Edition also includes more flexible data access with support for custom reports. The API documentation is installed on the DCI. It is available from the Start ➤ Programs ➤ Crystal Enterprise 9 ➤ Documentation menu.

Integration with the Opsware System

The Opsware System collects information from two sources: the Opsware Agent, which discovers hardware, software, and patches on each server, and the Opsware Model, which indicates what should be installed on each server. These reports provide a view of what is and "what should be to help users reconcile the differences between the two. The DCI always displays the most accurate and up-to-date information available, even during periods of frequent and substantial change. This accuracy of data reduces the risk of making the wrong decisions because of old information.

The DCI 1.2 is released with Opsware System 4.6. Older Opsware Systems such as 4.0, 4.0.1 and 4.0.2 must be upgraded to Opsware System 4.6 before upgrading The DCI to 1.2.

Figure 1.1illustrates how the DCI interacts with the Opsware System to retrieve information for a report.

Figure 1-1: DCI Integration with the Opsware System
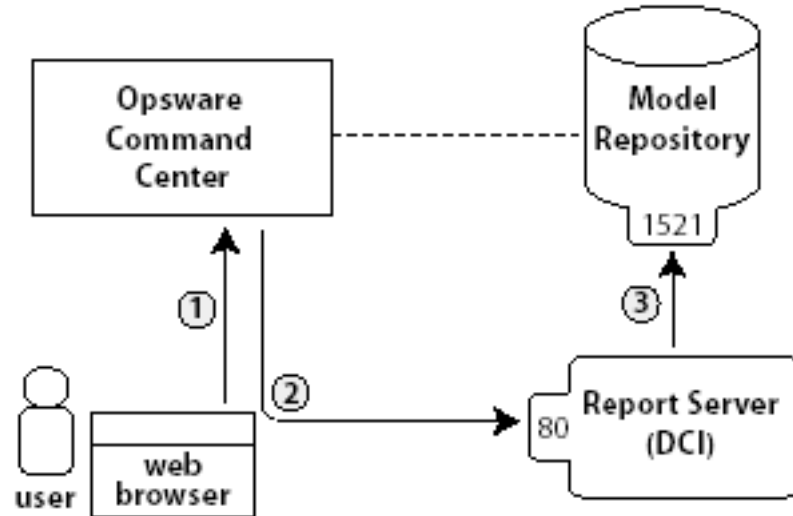
The DCI integrates seamlessly with the Opsware System and you can access it from the Opsware Command Center.

A typical report query involves the following steps:

1 A user logs into the Opsware Command Center and clicks the Reports link in the Navigation panel.

2 A screen loads in OCC with a direct connection to the report server (a server machine with RAS and IIS running) on port 80.

3 The report server generates a report by creating a database connection to the Model Repository on port 1521.

4 The DCI returns the report to the user's Web browser in a new window.

Chapter 2: Installing and Configuring the DCI Report Server

The DCI Report Server comes as a software package on the DCI Report Server disk of the Opsware Installation CDs. The DCI Report Server is compatible with Opsware System 4.7 only. DCI Report Server can be installed from a zip file or with the Integrated Software Management (ISM) Tool.

Internet Information Services (IIS) from Microsoft must be installed and running on the managed server where you install the DCI Report 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

You will need the following items to begin either a zip file installation or an installation with the ISMTool:

• Hardware

  • 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)

- Windows 2000, Service Pack 4 or higher, or Windows 2003, running the Internet Information Services 5.0 or 6.0

- Preparing the Server

  - Verify that the machine is available by logging in to the Opsware Command Center and making sure the named machine is available from the Servers ➤ Managed Servers page.

  - Verify that IIS is installed on this machine by clicking the name of the managed server, then selecting the Nodes tab. Make sure that IISADMIN and W3SVC are running.

  - Make sure you install IIS only after you add the server to the domain. If you already installed IIS but not yet added the server to the domain, then please perform the following task: "Setting DCI Report Server Default Domain in IIS" on page 26.

- The DCI CD-ROM must be loaded on your computer.

- The Oracle opsware_public views user password and name of the Oracle database the Opsware core (such as the SID) uses, which were configured when the Opsware System was installed. You might need to contact your Oracle administrator for this information.
  Opsware_public_views password: _____
  Oracle SID for Opsware: _____
  IP address of the OCC Server: _____
  IP address of the DCI Server: _____

- Check and make a note of what operating system is running on this server.

- If you are upgrading from the DCI 1.1 or earlier, you must completely uninstall the DCI Report Server and then follow all the steps in this chapter. See Chapter 3, "Uninstalling, Moving, or Upgrading the DCI Report Server" for more information about uninstalling the DCI Report Server.

The DCI 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.

Installing the DCI Report Server from a Zip File

Installing the DCI Report Server from a zip file requires the following six steps:

• Zip File Installation: Upload the DCI Package

• Zip File Installation: Creating the DCI Software Application Node

• Zip File Installation: Add Custom Attributes to the DCI Report Server

• Zip File Installation: Install the DCI Software

• Zip File Installation: Enable the DCI in the OCC

• Zip File Installation: Execute DCI Configuration Script

• ZIP File Installation: Modify the Apache Configuration

The following sections describe each of these processes in detail.

Zip File Installation: Upload the DCI Package

Perform the following steps to upload the DCI package:

1 From the Opsware Command Center, go to the Software ➤ Packages, and then click the Upload tab.

2 On the Upload Package page, select Customer Independent from the Customer drop-down menu, select Windows 2000 or 2003 from the Operating System drop-down menu, and select Windows Zip file from the Package Type drop-down menu.

3 Click Next.

4 Click the Browse button to locate the file `DCIPackage_en-1.2.zip` from the DCI Installation CD in your computer and click Open in the dialog box.

5 Click Upload. A progress bar appears while the package is uploading.

6 When the upload completes, the Packages: Edit Properties page displays. You can enter a description for the DCI package here.

Almost all installation errors and failures result from not entering the proper information in the following fields on the Packages: Edit Properties page. Double check that the following information is entered correctly into the proper fields.

7 In the **Post-Install Script Filename** field, enter `reports_install.bat`

8 Check the box next to "End this and subsequent installs if this script fails."

9 In the **Pre-Uninstall Script Filename** field, enter `reports_uninstall.bat`.

10 Check the box next to "End this and subsequent installs if this script fails."

11 In the **Post-Install Script** field, enter:
```
del /f /q "%SystemDrive%\Program Files\DCIPackage_en-
1.2\reports_install.bat".
```

12 In the **Post-Uninstall Script** field, enter:
```
rmdir /s /q "%SystemDrive%\Program Files\DCIPackage_en-1.2".
```

13 Click Save.

Zip File Installation: Creating the DCI Software Application Node

Perform the following steps to create the DCI software application node:

1 From the Opsware Command Center, navigate to Software ➤ Applications ➤ Other Applications.

2 Click the Add button to create an application node.

3 Enter

```
DCI
```

as the Name, and add a description such as "Opsware System 4.7 Data Center Intelligence Reporting Server for Windows 2000" and any notes you want to record.

4 Click Save.

5 The Edit Properties page for this node now displays. Scroll down and select Windows 2000 or Windows 2003 from the Change Operating Systems window.

6 Click Save.

7 Click the Add button to create a sub-node below the DCI Report Server node.

Enter

en

as the Name, and add a description such as

English language

and any notes you want to record.

8 Click Save, and click Save on the subsequent Edit Node Properties page.

9 Click the Add button to create a sub-node below the DCI Report Server language sub-node.

10 Enter 1.2 as the Name, and add a description such as "DCI version number" and any notes you want to record.

11 Click Save, and click Save on the subsequent Edit Node Properties page.

12 Click the Add button to create a sub-node below the DCI Report Server version number sub-node.

13 Enter

AllZip

as the Name, and add a description such as

Zip Package

and any notes you want to record.

14 Click Save, and click Save on the subsequent Edit Node Properties page.

15 Click the Packages tab.

16 Click Edit Packages.

17 Click Add Packages.

18 In the search window that appears, enter

DCIPackage

and choose Name and Windows zip file in the drop-down menus.

19 Click Find Software.

20 Click the check box for the DCIPackage_en-1.2.zip package and click Add to Node.

21 Click Cancel in the window that pops up. The main window now appears.

22 Click Save Edits.

You have now successfully created a software node and attached it to the DCI package that contains the software for the report server. See Chapter 6, Application Provisioning Setup in the Opsware System 4.7 User's Guide for more information about how to create nodes and attach packages.

Zip File Installation: Add Custom Attributes to the DCI Report Server

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 with your database administrator.

Perform the following steps to add essential custom attributes to the DCI Report Server

1 From the Opsware Command Center, go to the Servers ➤ Managed Servers page.

2 Find the server intended to install the DCI software, by name or IP address from Servers ➤ Managed Servers, or by Server Search.

3 Select the Custom Attributes tab.

4 Click the New Attribute button and enter

`ras_pwd`

(in lowercase) in the name field and enter the value for the database password for the public views user in the value field. The password is case sensitive. (If you do not know the password, you can find it in the Opsware installation response file. If you are not sure where to find this file, contact your Opsware administrator.)

5 Click Save.

6 Click the New Attribute button and enter to add a second attribute "`sid`" (in lowercase) and enter as its value the SID of the Oracle instance that contains the Model Repository. Make sure to use the correct case and spelling.

7 Click Save.

8 Add a third attribute with the New Attribute button named "`occ_ip`" (in lowercase) and enter as its value the address of the OCC server (for example, 192.168.8.144).

9 Click Save. You should now see the three new custom attributes on the Custom Attributes page for the DCI Report Server, as shown in Figure 2-1.

Figure 2-1: Custom Attributes Added to the DCI Report Server

CUSTOM ATTRIBUTE FOR Vivfake0000.opsware.com BELONGING TO UNKNOWN	
New Attribute	
Click attribute name to view or edit details.	
Name ▼	Value
☐ occ_ip	192.168.8.144
☐ ras_pwd	opsware_public_views
☐ sid	truth
Delete selected custom attributes	

Zip File Installation: Install the DCI Software

Perform the following steps to install the DCI Report Server software:

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

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

3 In the Install Software Wizard, click the Start button.

4 Click Other Applications, then navigate to the DCI ➤ en ➤ 1.2 ➤ AllZip. Select the check box in front of DCIPackage_en-1.2.zip and click Next.

5 On the Confirm Selections page, click Preview.

6 Wait for the Preview to complete and then click the View Details button. Verify that the status is Completed and that the Output tab shows that the DCI zip package will be installed. If you receive an error during this step, refer to Chapter 6, "Troubleshooting the DCI".

7 Click Close on the Reconcile Details window.

8 In the Schedule and Notify page of the Install Software wizard, Schedule section, choose Run Now. In the Notify section, choose if you want to send an email when the installation has finished.

9 Click Install and either wait for the installation to complete or click the Close button. Depending on the network, the installation can take about 8-20 minutes or more to complete.

10 To display the progress of the installation, click the name of the job from the My Jobs listing on the Opsware Command Center home page. The progress window displays.

You are now ready to enable the links on the Opsware Command Center so that other users of Opsware can access the report server.

Zip File Installation: Enable the DCI in the OCC

Perform the following steps to enable the DCI Report Server in the Opsware Command Center:

1 Log into the Opsware Command Center as administrator.

2 Go to Administration ➤ System Configuration.

3 From the Product list, click Opsware Command Center.

4 On the line owm.features.Reports.allow, select the Use value radio button and type:

`true`

5 On the line owm.features.Reports.URL, select the Use value radio button and type:

`/dci`

6 Scroll to the bottom of the page and click Save.

In a multimaster environment, each Opsware Command Center needs to have its configuration saved for the changes to take affect.

Zip File Installation: Execute DCI Configuration Script

In this task, you will run a script that will configure the DCI to enable communication between the DCI Server and the Reports function inside the OCC.

To perform this task, you need to log on to the OCC as administrator user that has distributed script execution permissions (DSE).

▌1▐ Log into the Opsware Command Center as administrator user that has distributed script execution permissions (DSE).

▌2▐ Click the Run Distributed Script link in the Tasks area of the Opsware Command Center home page to launch the Run Distributed Script Wizard.

▌3▐ On the Overview page of the Script Execution wizard, select Define Ad-Hoc, then click Next.

▌4▐ On the Define Script page, do the following:

   • Choose UNIX Shell as the type of script.

   • Upload Script option.

   • For the Encoding of Script, choose ASCII.

   • Click the Browse button and locate the script named "configDCI" on the DCI product CD. This script will be stored in the scripts folder on the CD.

▌5▐ Click Next.

▌6▐ On the Select Server page, select the OCC Server which your DCI Server is configured to run with, and then click Next.

▌7▐ On the Specify Options page, choose Run as root.

▌8▐ In the Command Line Parameters section enter:

▌9▐ For Windows 2000 DCI Report Server:

```
<OCC_ADMIN_USER> <OCC_ADMIN_PWD> <USER_DOMAIN> <DCI_SERVER_
IP>
```

For Windows 2003 DCI Report Server:

```
<OCC_ADMIN_USER> <OCC_ADMIN_PWD> <USER_DOMAIN> <DCI_SERVER_
IP> <REALM>
```

For example:

```
admin admin opsware.com 192.168.8.202 opsware.com
```

You can locate the `<USER_DOMAIN>` in the `/cust/owm/etc/psrvr.properties` file, in the `pref.domain.default` parameter.

▌10▐ Click Next.

11 Confirm the settings and select Next.

12 On the Confirm Setting page, check the script execution settings, and then click Next.

13 On the Schedule and Notify page, Schedule section, choose Run Now. In the Notify section, choose if you want to send an email when the installation has finished.

14 Click Run Script to run the script.

15 After script execution, summary details display for the total job and each server. An ID number at the top of the page identifies the job.

ZIP File Installation: Modify the Apache Configuration

In this section, you will configure the Apache server to be able to communicate with the OCC Server.

1 On the OCC Server, open the following Apache Proxy Server configuration file in a text editor:

```
/cust/apache/servers/https-Proxy/conf/httpd.conf
```

2 Uncomment the following two lines and replace `<IP>` with the IP address of DCI 1.2 Server:

– `RewriteRule ^/dci(.*) /com.loudcloud.ps.authproxy/`
`authproxy/http://<IP>/dci$1 [P,L]`

– `RewriteRule ^/crystalreportviewers10/(.*)/`
`com.loudcloud.ps.authproxy/authproxy/http://<IP>/`
`crystalreportviewers10$1 [P,L]`

3 Restart the Apache Proxy Server by executing the following command:

```
/etc/init.d/httpd restart
```

To access the DCI 1.2 inside the OCC, see "Accessing Reports in the OCC" on page 26.

Installing the DCI Report Server Using the ISMTool

If you are familiar with the ISMTool, this method for installing the DCI Report Server is recommended. You will 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.

The prerequisites for an ISMTool installation are the same as for zip file installation and are listed at the beginning of this chapter.

Installing the DCI Report Server using the ISMTool requires the following six steps:

- ISMTool Installation: Uninstall Older Version of the ISMTool

- ISMTool Installation: Install the ISMTool

- ISMTool Installation: Unpack the DCI Package

- ISMTool Installation: Add Custom Attributes to the DCI Report Server

- ISMTool Installation: Install the DCI Software

- ISMTool Installation: Enable the DCI in the OCC

- ISMTool Installation: Execute DCI Configuration Script

- ISMTool Installation: Modify the Apache Configuration

ISMTool Installation: Uninstall Older Version of the ISMTool

If you have an older version of the ISMtool installed on your computer (a version previous to 1.0.3), then you will need to uninstall that version before installing the newer version of the ISMTool (version 1.0.3 or later).

You only need to perform this step if you are running a version of the ISMTool previous to 1.0.3. If you already have a current version of the ISMTool, or do not have any version installed, then you can skip this task and move on to the next.

Perform the following steps to uninstall the older version of the ISMTool:

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-1.0.2) and remove the older version of the ISMTool application.

3   Log off and then back on to the computer, and then install the newer verison of the ISMTool (version 1.0.3 or later).

ISMTool Installation: Install the ISMTool

Perform the following steps to install the ISMTool:

1   Go to https://download.opsware.com/devtools/index.htm.

2 Select your operating system and download the latest version of the tool (version 1.0.3 or later) onto a server the Opsware Command Center manages where you want to perform the installation.

3 Double click the downloaded file to install the ISMTool. For Windows, the package installs into the directory Program Files\ismtool-1.0.3. The ISMTool cannot be installed over a network.

4 After a successful installation of the ISMTool, log off and log back onto the machine.

To use the ISMTool to upload the DCI package, the proper way script, version 2.6 or higher, must also be installed. If the proper version of the way script was not installed with your Opsware System software, contact Opsware Support.

ISMTool Installation: Unpack the DCI Package

Perform the following steps to unpack the DCI software package:

1 Copy the `DCIPackage_en-1.2.ism` package to an accessible location on the computer where the ISMTool is installed.

2 Open a command prompt interface.

3 Execute the following command:

```
ismtool --unpack DCIPackage_en-1.2.ism
```

4 Next, execute the following command:

```
ismtool --upload DCIPackage_en-1.2
```

The system confirms the Opsware core you are uploading the package to. Respond "Y" if this is the proper core.

5 At the Opsware user name and login prompt, enter the information for the default Opsware Administrator.

6 Enter

```
Customer Independent
```

for the Opsware customer prompt. The package takes roughly 15 minutes to upload.

ISMTool Installation: Add Custom Attributes to the DCI Report Server

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.

Perform the following steps to add essential custom attributes to the DCI Report Server

1 From the Opsware Command Center, go to the Servers ➤ Managed Servers page.

2 Find the server intended to install the DCI software, by name or IP address from Servers ➤ Managed Servers, or by Server Search.

3 Select the Custom Attributes tab.

4 Click the New Attribute button and enter

`ras_pwd`

(in lowercase) in the name field and enter the value for the database password for the public views user in the value field. The password is case sensitive. (If you do not know the password, you can find it in the Opsware installation response file. If you are not sure where to find this file, contact your Opsware administrator.)

5 Click Save.

6 Click the New Attribute button and enter to add a second attribute "`sid`" (in lowercase) and enter as its value the SID of the Oracle instance that contains the Model Repository. Make sure to use the correct case and spelling.

7 Click Save.

8 Add a third attribute with the New Attribute button named "`occ_ip`" (in lowercase) and enter as its value the address of the OCC server (for example, 192.168.8.144).

9 Click Save. You should now see the three new custom attributes on the Custom Attributes page for the DCI Report Server, as shown in Figure 2-1.

Figure 2-1: Custom Attributes Added to the DCI Report Server

ISMTool Installation: Install the DCI Software

Perform the following steps to install the DCI Software:

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

2 Check the box for the server, and from the Software menu choose Application. An Install Software Wizard window now launches.

3 In the Install Software Wizard, click the Start button.

4 Click Other Applications, then navigate to the DCI ➤ en ➤ 1.2 ➤ Windows 2000 (or Windows 2003). Select the check box in front of msi and click Next.

5 On the Confirm Selections page, click Preview.

6 Wait for the preview to complete and then click the View Details button. Verify that the status is completed and the Output tab shows that the DCI MSI packages will be installed. If you receive an error during this step, refer to Chapter 6, "Troubleshooting the DCI."

7 Click Close on the Reconcile Details window.

8 In the Schedule and Notify page of the Install Software wizard, Schedule section, choose Run Now. In the Notify section, choose if you want to send an email when the installation has finished.

9 Click Install and either wait for the installation to complete or click the Close button. Depending on the network, the installation can take about 8-20 minutes or more to complete.

10 To display the progress of the installation, click the name of the job from the My Jobs listing on the Opsware Command Center home page. The progress window displays.

When the installation has finished, you are now ready to enable the links on the Opsware Command Center so that other Opsware users can access the report server.

ISMTool Installation: Enable the DCI in the OCC

Perform the following steps to enable the DCI in the Opsware Command Center:

1 Log in to the Opsware Command Center as administrator.

2 Go to Administration ➤ System Configuration.

3 From the Product list, click Opsware Command Center.

4 On the line owm.features.Reports.allow, select the Use value radio button and type:

```
true
```

5 On the line owm.features.Reports.URL, select the Use value radio button and type"

```
/dci
```

6 Scroll to the bottom of the page and click Save.

In a multimaster environment, each Opsware Command Center needs to have its configuration saved for the changes to take affect.

ISMTool Installation: Execute DCI Configuration Script

In this task, you will run a script that will configure the DCI to enable communication between the DCI Server and the Reports function inside the OCC.

To perform this task, you need to log on to the OCC as administrator user that has distributed script execution permissions (DSE).

1 Log into the Opsware Command Center as administrator user that has distributed script execution permissions (DSE).

2 Click the Run Distributed Script link in the Tasks area of the Opsware Command Center home page to launch the Run Distributed Script Wizard.

3 On the Overview page of the Script Execution wizard, select Define Ad-Hoc, then click Next.

4 On the Define Script page, do the following:

- Choose UNIX Shell as the type of script.

- Upload Script option.

- For the Encoding of Script, choose ASCII.

- Click the Browse button and locate the script named "configDCI" on the DCI product CD. This script will be stored in the scripts folder on the CD.

5 Click Next.

6 On the Select Server page, select the OCC Server which your DCI Server is configured to run with, and then click Next.

7 On the Specify Options page, choose Run as root.

8 In the Command Line Parameters section enter:

9 For Windows 2000 DCI Report Server:

`<OCC_ADMIN_USER> <OCC_ADMIN_PWD> <USER_DOMAIN> <DCI_SERVER_ IP>`

For Windows 2003 DCI Report Server:

`<OCC_ADMIN_USER> <OCC_ADMIN_PWD> <USER_DOMAIN> <DCI_SERVER_ IP> <REALM>`

For example:

`admin admin opsware.com 192.168.8.202 opsware.com`

You can locate the `<USER_DOMAIN>` in the `/cust/owm/etc/psrvr.properties` file, in the `pref.domain.default` parameter.

---

10 Click Next.

11 Confirm the settings and select Next.

12 On the Confirm Setting page, check the script execution settings, and then click Next.

13 On the Schedule and Notify page, Schedule section, choose Run Now. In the Notify section, choose if you want to send an email when the installation has finished.

14 Click Run Script to run the script.

15 After script execution, summary details display for the total job and each server. An ID number at the top of the page identifies the job.

ISMTool Installation: Modify the Apache Configuration

In this section, you will configure the Apache server to be able to communicate with the OCC Server.

1 On the OCC Server, open the following Apache Proxy Server configuration file in a text editor:

```
/cust/apache/servers/https-Proxy/conf/httpd.conf
```

2 Uncomment the following two lines and replace `<IP>` with the IP address of DCI 1.2 Server:

- `RewriteRule ^/dci(.*) /com.loudcloud.ps.authproxy/`
  `authproxy/http://<IP>/dci$1 [P,L]`

- `RewriteRule ^/crystalreportviewers10/(.*)/`
  `com.loudcloud.ps.authproxy/authproxy/http://<IP>/`
  `crystalreportviewers10$1 [P,L]`

3 Restart the Apache Proxy Server by executing the following command:

```
/etc/init.d/httpd restart
```

Accessing Reports in the OCC

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

Figure 2-2: Reporting Links in the OCC
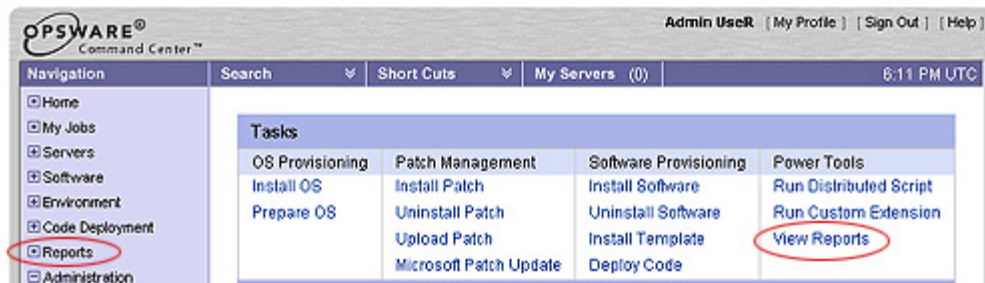
By default, only Advanced Users and Administrators have access to the DCI. However, you can give users access to the DCI by giving them DCI permissions. For information about setting and changing user permissions, please refer to the Opsware Administration Guide, Chapter 2, User Groups and Opsware System Permissions.

Setting DCI Report Server Default Domain in IIS

If you installed IIS on the server before you added the server to the domain, then you will need to edit the default domain for the DCI Report Server.

To set the DCI Report Server default domain in IIS:

1 Select Administrator Tools ➤ Internet Information Services.

2 Browse to the "Web Sites" folder under the local computer.

3 Right-click the "Web Sites" folder and choose Properties.

4 In the Properties dialog box, select the Directory Security tab.

5 Select the Edit button for Enable anonymous access and edit authentication methods for this resource.

6 Uncheck Enable anonymous access.

7 Check .NetPassport authentication.

8 In the Default domain field, choose the Select button to pick the correct default domain.

9 Select OK to set, then OK, and then OK again.

Chapter 3: Uninstalling, Moving, or Upgrading the DCI Report Server

This chapter provides the following information about changing, uninstalling, moving, and upgrading the DCI Report Server:

• Changing System Configurations

• Uninstalling the DCI Report Server

• Moving the Report Server to a Different Machine

• Upgrading the Report Server from a Zip File

• Upgrading the Report Server Using the ISMTool

To either move the report server to another machine or uninstall the DCI Report Server software, start by changing the Opsware Command Center system configurations as outlined below. Then any previous versions of theDCI Report Server must be uninstalled prior to upgrading or moving the DCI Report Server to prevent users from accessing the report server while the upgrade is in progress. Finally, the DCI Report Server can be upgraded or moved.

Custom reports are not deleted or damaged by upgrading or re-installing the DCI Report Server.

Changing System Configurations

Perform the following steps to change system configurations prior to moving or upgrading the DCI Report Server

1 Log in to the Opsware Command Center as administrator.

2 Choose Administration ➤ System Configuration from the Navigation panel and then click Opsware Command Center in the Product list.

3 If you are uninstalling the DCI software, scroll down and set owm.features.Reports.allow to False. Otherwise, skip to step 4.

4 If you are moving the report server, make sure the owm.features.Reports.URL parameter is blank or set to /dci.

5 Scroll down and click Save.

6 If you set owm.features.Reports.allow to False, reload the home page by selecting Home in the Navigation panel. The Reports link in the Navigation panel will be gone, and the View Reports link will deactivate. If you only changed the URL, you can test the changed URL from the links on the home page.

In a multimaster environment, each Opsware Command Center will need to have its configuration saved for the changes to take affect.

Uninstalling the DCI Report Server

You must first change your system configurations, as described in the previous section, to uninstall your server.

To uninstall the DCI Report Server:

1 Before uninstalling, you need to deactivate the DCI in the OCC. To do this, Log in to the Opsware Command Center as administrator.

2 Choose Administration ➤ System Configuration from the Navigation panel and then click Opsware Command Center in the Product list.

3 If you are uninstalling the DCI software, scroll down and set owm.features.Reports.allow to False.

4 Scroll to the bottom of the page and click Save.

5 Using Servers ➤ Managed Servers, find the report server (by name or IP address).

6 Select the check box for the report server, and from the Application menu, select Uninstall. The Uninstall Software Wizard launches.

7 Click Start in the Uninstall Software Wizard.

8 Select the DCI application and click Next.

9 Click Preview on the next screen.

10 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 node will be uninstalled. Click Close.

11 Click Uninstall in the Uninstall Software Wizard.

12 Check for status of Uninstall Software from the My Jobs listing on the Opsware Command Center's home page. Completion can take 10 minutes or longer.

If you want to verify uninstallation, log into the Opsware Command Center and go to the named machine from the Servers ➤ Managed Servers page. Go to the Services tab. You should *not* see an entry called "CrystalReportApplicationServer."

Moving the Report Server to a Different Machine

To upgrade to a new report server you will need to perform the following steps.

1 Disable the reports links from the Opsware Command Center (see steps 3 and 4 in "Changing System Configurations" in this chapter).

2 Uninstall the existing report server (see "To Uninstall" in this chapter).

3 Install the DCI Report Server on the new server (see Chapter 3).

4 Copy your custom reports from the original server to the %SystemDrive%\Program Files\Opsware\DCI\Reports\Custom folder on the new server.

5 Enable the Report link from the Opsware Command Center (see "Changing System Configurations" in this chapter).

Upgrading the Report Server from a Zip File

Perform the following steps to upgrade from the DCI 1.1 to 1.2 from a zip file. You must have already upgraded to Opsware System 4.1 to upgrade to the DCI 1.2. Skip to the next section for instructions on upgrading the DCI Report Server with the ISMTool.

1 Disable the Reports links from the Opsware Command Center (see "Changing System Configurations" in this chapter).

2 Uninstall the existing Reports server (see "Uninstalling" in this chapter).

3 In the Opsware Command Center, under Software ➤ Applications, navigate to the DCI node and click.

4 Click the Packages tab.

5 Click Edit Packages.

6 On the next screen, select the name of the old DCI package, and click Remove Packages.

7 Click Add Package.

8 A search window now appears. Search for DCI to find the new package, and then click Add to Node.

9 Click Save Edits.

10 Change the Report link from the Opsware Command Center (see "Changing System Configurations" at the beginning of this chapter).

11 Install the DCI application. Refer to the instructions in Chapter 3 for instructions about how to install the DCI Report Server.

12 Move any DCI custom reports if necessary. Refer to "Chapter 5: Writing Custom Reports" for details about how to install custom reports.

Upgrading the Report Server Using the ISMTool

Perform the following steps to upgrade from DCI 1.1 to 1.2 with the ISMTool. You must have already upgraded to Opsware System 4.1 to upgrade to DCI 1.2.

1 Disable the Reports links from the Opsware Command Center (see "Changing System Configurations" at the beginning of this chapter).

2 Uninstall the existing reports server (see "Uninstalling" in this chapter).

3 Install the ISMTool, if necessary, and unpack the DCI by using the ISMTool (see Chapter 3 for details).

4 Optional: Remove the old DCI node from the Opsware Command Center.

5 Change the Report link from the Opsware Command Center (see "Changing System Configurations" at the beginning of this chapter).

6 Install the DCI application.Refer to instructions in Chapter 3 for detailed instructions about how to install the DCI Report Server.

Chapter 4: Writing Custom Reports

IN THIS CHAPTER

This chapter introduces how to write custom reports for DCI and covers the following subjects:

• Understanding access to the public views

• Using a shipped report to create a custom report

• Extending reports with other data sources

• Installing a customized 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 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 \Program Files\Opsware\DCI\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 machine.

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 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 (any Crystal Report .rpt file) should be placed in the %SystemDrive%\Program Files\Opsware\DCI\Reports\Custom folder.

Figure 4-3: Adding a New Report to the Custom Reports Folder
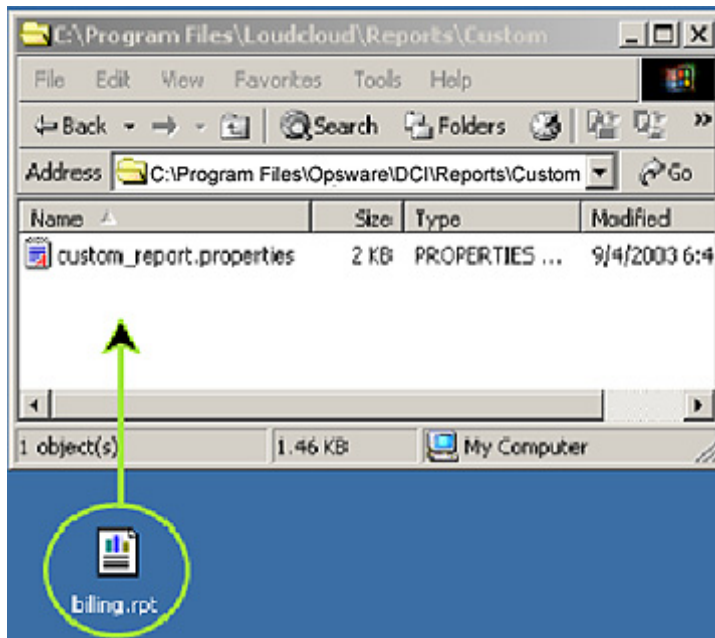
When a report is placed in the Custom folder (see Figure 5-2), the DCI home page shows the new report in the custom report section which appears as the first section of the home page (see Figure 5-3).

Figure 4-4: Home Page with the New Custom Report Visible

If no custom reports are stored in the Custom folder, then the message "No custom reports available" will be displayed.

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 configuration file customer_report.properties in the folder %SystemDrive%\Program Files\Opsware\DCI\wwwroot\Custom.

Figure 4-5: Home Page with Configured Custom Reports

See the detailed instructions inside the configuration file for more information. In Figure 5-4, the following information is set in the configuration file to make the home page display the custom reports as shown:

Section Title:: Custom Billing and Management

Left SubSection Title::Billing Services

Right SubSection Title::Management

R::Server Inventory by Manager::custominv.rpt

L::Customer Billing History for Premium Services::BillingPremium,l.rpt

The order in which the reports are listed in the properties file (for their respective left or right columns) 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 also appear on the home page. They will appear after any reports defined in the configuration file in the left column. If a report is removed from the Custom folder, you can choose to remove any corresponding entry in the configuration file. DCI checks to see if the file exists before enabling a link in the custom area of the DCI home page. If it does not see the file, it will not display the link. This checking process protects you from invalid links appearing on the DCI 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. Also, the Section titles are already formatted using the same style as the rest of the home page, but you can add any additional formatting that you choose.

36

Chapter 5: DCI Report Server FAQ

How Do I Restart or Stop the DCI Report Server?

The DCI Report Server is installed as a Windows service. From the Start ➤ Settings ➤ Control Panel ➤ Administrator Tools ➤ Services window, you can see an entry called Crystal Enterprise Report Application Server. It should be Started and Automatic, so that the DCI server will run when the host machine restarts. If you need to start or stop the service, click the service and choose the corresponding function from the menu (or click the item with the right mouse button).

How Does Updating the Opsware System Affect the DCI Report Server?

The DCI report Server does not affect Opsware's Command Center core installation and maintenance. The DCI report server is dependent on the same database as the main installation of the Opsware System core, and thus future upgrades to the Opsware System might require upgrades to the shipped reports. Installation of new reports on the home page does not affect existing custom reports. Installation of any DCI patches or upgrades does not affect the Opsware System.

Can I Use HTTPS with SSL to Secure the DCI Report Server?

You can use HTTPS and SSL to secure the DCI Report Server. The default setup of the Opsware Command Center links to reports that are not encrypted or secure. In fact, you can copy and paste any URL from the report server and share it with anyone who has access to the server through standard http. If this level of flexibility is too open, you can choose to setup security on the DCI Report Server using SSL.

Consult with your Windows administrator to establish your security policy and configure the report server accordingly. For more information about how to configure the Certificate Server and SSL, refer to the Microsoft Knowledge Base article #290625, "HOW TO: Configure SSL in a Windows 2000 IIS 5.0 Test Environment by Using Certificate Server 2.0."

After you set up and configure the DCI Report Server with SSL, you need to update the reporting address from http to https in the Opsware Command Center. You must have administrator privileges to change this value.

Perform the following steps to update the DCI Report Server address:

1 Log into the Opsware Command Center as administrator.

2 Click the Administration ➤ System Configuration link in the Navigation panel.

3 From the Product list, click the link for the Opsware Command Center.

4 Scroll down to the name for owm.features.Reports.URL, select the "Use value" radio button, and set the value to /dci.

How Do I Change the DCI Admin Password?

The DCI Report Server provides a batch script that allows you to change the password value of Public Views user stored on the DCI server. 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.

Changing the dciadmin password requires performing the following two tasks:

• Execute DCI Public Views Change Password Script

• Modify OCC Properties File

Execute DCI Public Views Change Password Script

1 Log in to the Opsware Command Center as administrator.

2 Click the Run Distributed Script link in the Tasks area of the Opsware Command Center home page to launch the Run Distributed Script wizard.

3 On the Overview page of the wizard, select Define Ad-Hoc Script and then click Start.

4 On the Define Script page of the wizard, from the Type drop-down list choose Windows.BAT as the type of script.

5 Select the Enter Script Contents option.

6 Enter the following text as the contents of the script:

```
@echo off
cd "%SystemDrive%\Program Files\DCIPackage_en-1.2"
cscript changeAdminPwd.vbs <enter new password here>
```

For example:

```
@echo off
cd "%SystemDrive%\Program Files\DCIPackage_en-1.2"
cscript changeAdminPwd.vbs mypassword
```

7 Click Next.

8 On the Select Server page of the wizard, choose the DCI Server, and then click Next.

9 On the Specify Options page, choose the Run As Local User option.

10 Leave all other options (Script Output and Script Timeout) with their default settings.

11 Click Next.

12 On the Confirm Settings page, review your script execution settings before proceeding. Click Next.

13 On the Schedule and Notify page of the wizard, you can choose to schedule this script at a later time, or choose to run the script now. You can also choose to be notified by email if when the scrip has finished executing.

14 Choose your scheduling and notification options and then click Run Script to execute the script and change the password.

Modify OCC Properties File

After the script completes executing, you need to perform the following task:

1 Log on the computer where the OCC is installed.

2 Open the following file in a text editor:

```
/cust/owm/wwwroot/com.loudcloud.ps.authproxy/WEB-INF/
properties.txt
```

3 Modify the following entry:

```
authproxy.partner_domain.<ip address of dci
server>.customer_domainpassword=<new password>
```

4 Restart the OCC Server by executing the following command:

```
/etc/init.d/owm.server restart
```

How Do I Change the 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 change the Oracle password, you will have to change the password stored on the DCI Report Server, which is described in a subsequent section of this chapter.

Perform the following steps to change the password in Oracle. For this example, we assume that the name of the server where the database is running is "`truth.opsware.com`", and the new password will be "`publicpassword`".

1 Log in to the server where Oracle is running.

2 Bring up a terminal window and press return after each of the following steps

3 Enter:
```
su - oracle
```

4 Enter
```
sqlplus
```

5 At the enter user-name prompt, enter
```
opsware_public_views
```

6 At the SQL> prompt enter
```
ALTER USER opsware_public_views
```

7 When "2" appears, enter
```
IDENTIFIED BY publicpassword;
```

8 Click Enter.
The message "User altered" appears.

The password is now changed. Make sure that the DCI Report Server will use this password to access the database (see "Changing the DCI Password" in this chapter). "Identified by" is the command that changes the password for a user.

How Do I Change the Oracle Public Views Password?

Normally the password for the Oracle "opsware_public_views" user is set at the time of the Opsware Command Center installation. This public password is set in a file on the report server so that all of the reports can be generated. Otherwise, users of all reports would have to know and enter this login and password for every report. If you change this Oracle password, you also need to change the password stored on the DCI report server.

In DCI 1.1, a batch script is provided so that you can change the public views password more conveniently. To use this script, first change the Oracle public views password in DCI, and then run the script.

Changing the DCI Password

Perform the following steps to change the DCI password:

1 Select the DCI report server in the Opsware Command Center, and click its name.

2 Click the Custom Attributes tab.

3 Click the attribute name ras_pwd.

4 Change the value to the new password and click Save.

Running the Change Password Script

Perform the following steps to run the change password script:

1 Go to the Managed Servers page in the Opsware Command Center.

2 Click the check box next to the DCI report server name, and choose Run Script from the Server drop-down menu to start the Run Distributed Script Wizard.

3 On the first page of the wizard, choose the radio button Define Ad-Hoc Script and click Start.

4 In the Type menu, choose Windows.bat.

5 In the Script Contents field, enter:
```
@echo off
cd "%SystemDrive%\Program Files\DCIPackage_en-1.1"
call changeRasPwd.bat
```

6 Enter your login, password, and confirmation password in the following screen.

7 Confirm all settings and click Run Script.

8 Verify that the script has run properly by running a report in DCI. If you are not prompted for the password, the script successfully executed.

How do I Change the Database Password on the DCI Report Server?

If the steps listed previously for changing the password do not work for any reason, the password can also be changed manually on the machine running the DCI Report Server. Log in to the DCI Report Server and open the file truthini.asp using a text editor (such as Notepad). The file is located in the folder `<system drive>\Program Files\Opsware\DCI\wwwroot\viewer`. The contents are shown below.

```
<%
    Dim truthViewId, truthViewPwd
    truthViewId="opsware_public_views"
    truthViewPwd="<password here>"
```

```
%>
```

Edit the existing password (after "truthViewPwd" in the code above) and save the file. The change is effective immediately.

How Do I Keep the Public Views Password Secure?

The password, when set up as a custom attribute in the Opsware Command Center, 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 only administrators with permission to view this server are able to see the value. You will need the password again if you upgrade the server or set up a new report server.

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.

Can I Use the DCI Report Server for Other Web content?

Yes, DCI 1.1 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 server.

Can I Install Multiple Network Cards on the DCI Report Server?

Yes, the DCI server can now have multiple network cards. Upgrading to DCI 1.1 or later resolves any issues with multiple network cards that would cause the server to shut down because of a licensing conflict.

Chapter 6: Troubleshooting the DCI

IN THIS CHAPTER

This chapter provides an overview and methodology to problem solving and troubleshooting for Opsware Data Center Intelligence (DCI):

• How to troubleshoot and diagnose errors and installation problems in the DCI Report Server

• How to contact Opsware Inc. Support

How to Troubleshoot Errors In the DCI

The following diagram shows a process chart to use for troubleshooting problems with DCI. This chart covers some of the major configuration problems and their resulting errors. Detailed instructions for each step are provided after the diagram.

Figure 6-6: DCI Troubleshooting
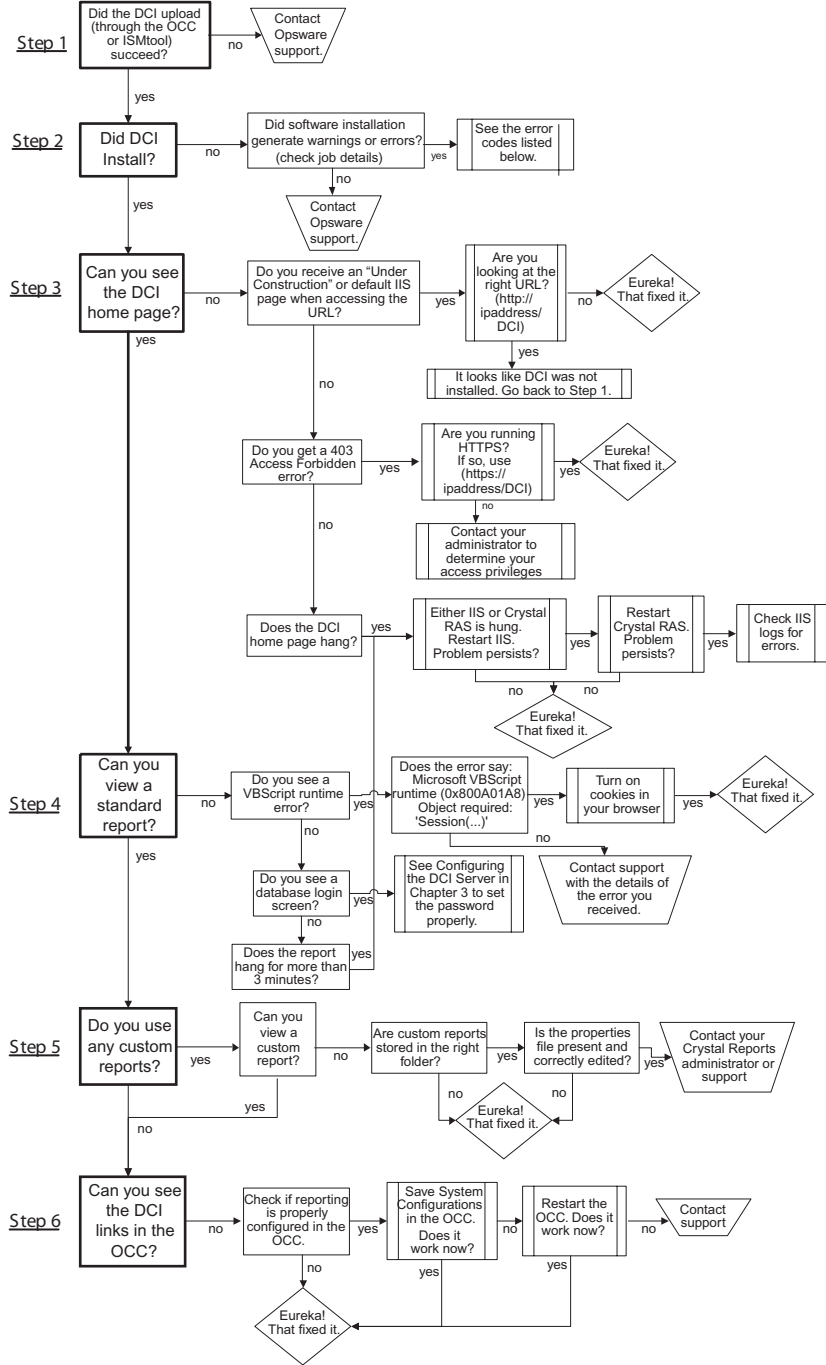
Step 1 - Did the DCI Package Upload?

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. Directions for contacting support are provided at the end of this chapter.

Step 2 - Did the DCI Report Server Install?

Verify that the DCI report server installed successfully by going to the server's URL from a Web browser (for example http://name of the machine/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-1.1\logs\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:

• Error 100. Insufficient disk space available. Installation halted.

• Error 101. IIS has not been installed or started. Please check the IIS prerequisites.

• Error 102. RAS installation failed. Please check the Event Viewer.

• Error 103. Failed to create the Virtual Directory DCI. Please check the Event Viewer.

• Error 104. Failed to make a connection to the Data Access Engine (the Spin), or the ras_pwd custom attribute does not exist.

• Error 105. Failed to parse the ras_pwd custom attribute.

• Error 106. Failed to make a connection to the Data Access Engine (the Spin), or the host name for the Data Repository, truth.host, does not exist.

• Error 107. Failed to retrieve the host name for the Data Repository, truth.host. It does not have a value.

• Error 108. Failed to make a connection to the Data Access Engine (the Spin), or truth.port does not exist.

• Error 109. Failed to retrieve truth.port. It does not have a value.

• Error 110. Failed to make a connection to the Data Access Engine (the Spin), or the sid custom attribute does not exist.

• Error 111. Failed to parse the sid custom attribute.

• Error 112. Failed to copy truthini.asp to Opsware\Inetpub-wwwroot\Viewer.

• Error 113. Failed to enable ASP Scripting in IIS 6.0.

• Error 114. DCI requires Service Pack Level 3 or higher for Windows 2000.

• Error 115. Failed to install DataDirect ODBC Drivers.

• Error 116. Failed to make a connection to the Data Access Engine (the Spin), or the occ_ip custom attribute does not exist.

• Error 117 - Failed to parse the occ_ip custom attribute.

• Error 18 - The syntax of the command is incorrect. Please supply a new password as parameter.

Step 3 - Can you see the DCI home page?

If you installed the DCI Report Server following the instructions in Chapter 3, but you cannot see the DCI home page, first check to see that you are looking at the right URL. Your DCI address should be http://ipaddress/DCI. If you are using HTTPS with SSL, then your address should be https://ipaddress/DCI.

If the DCI home page hangs or crashes, then the problem probably resides in IIS or the Crystal Report Application Server. Try restarting Crystal Report Application Server and then restarting IIS.

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 a database login screen, your public views password is not properly set. See the section "Configuring the DCI Server" in Chapter 3 to properly set your password.

If the report hangs or crashes, then the problem probably resides in IIS or the Crystal Report Application Server. Try restarting IIS and then restarting Crystal Report Application Server.

Another possible error:

• Custom reports section gives "you are not authorized" — It is possible that you do not have the authproxy or apache configured.

Step 5 - Do you use any custom reports and if so, 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 properties file. 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. Refer to Chapter 5 "Writing Custom Reports" for more information in custom report integration.

Step 6 - Does the Reports link show up on the OCC home page?

If the DCI works properly in a standalone browser, but the link does not show up on the Opsware Command Center home page, several problems could be occurring. First, check to see that reporting is configured properly in the OCC. This topic is covered under "Zip File Installation: Enable the DCI in the OCC" on page 16 or "ISMTool Installation: Enable the DCI in the OCC" on page 23 of this guide. You will need administrator privileges to perform this configuration.

If DCI is indeed properly configured in the Opsware Command Center, but the links are still not appearing on the home page, then it could be that old information is stuck in the Opsware Command Center memory. First try going to Administration ➤ System Configuration and click Save. If this does not work, try restarting the Opsware Command Center.

Miscellaneous DCI Troubleshooting

The following sections shows you how to solve various problems you might encounter with DCI.

What To Do If DCI Prompts for Username and Password

In some instances, users may encounter a login prompt asking for a username and password when attempting to access the DCI link inside the OCC. If this happens, then perform the following task:

1 On the DCI Server, select Administrator Tools ➤ Internet Information Services.

2 Browse to Default Web sites.

3 Right-click the "DCI" virtual directory and choose Properties.

4 Select the Directory Security tab.

5 Select the Edit button for Enable anonymous.

6 Enter your domain/realm in the "Realm" computer. (You can click the Select button to choose the domain/realm.

7 Click OK.

8 Repeat these exact same steps for the "crystalreportviewers10" virtual directory as well.

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

Appendix A: Public Views

Views of the Model Repository

Opsware System 4.0 and later uses Crystal Reports Designer 9 to give administrators direct access to the information recorded in the database repository. When accessing the Opsware database, the public views of interest are also referred to as the Truth. This appendix provides a visual overview of the database information available, a map of the relationships between tables in the public views, and a comprehensive list of definitions for each public view item. Users can write custom queries to retrieve customer, facility, server, network device, and software information from the database as described by these tables.

An Opsware public views user is created during installation of the Model Repository database. When the Opsware System was installed, a password was created for this "opsware_public_views" user. Use this password to access this view. Refer to Chapter 6 for information about how to change this password.

Opsware Public Views

The public views consist of a set of tables in the "Truth" schema, which is available from an ODBC or other connection to the Opsware database. This connection is read-only. The report server automatically connects to the opsware_public_user account. You need to know the password for this user to connect to the database.

If you are unfamiliar with the definitions of some of the field names in the public views, consult the Glossary in the <u>Opsware System 4.0 User's Guide</u>. All date and times are reported in UTC format.

Graphical Overview of Public Views

The next page shows a quick look at all public views. The table names and descriptions, as well as details for each of these table items, are provided in this appendix.

Figure 1-7: Public Views Overview

Graphical View of Public View Relationships

The next page shows a quick look at all the relationships between the public views tables. At each child end of a relationship on this chart, there can be one of three symbols, which indicate the nature of the relationship.

⚲ This symbol indicates there is no relationship from one table to the other.

┼ This symbol indicates there is one relationship.

⚵ This symbol indicates multiple relationships.

For example, a server can have multiple ⚮ services, interfaces, and so forth, but each service or interface corresponds to only one ⊦ server.
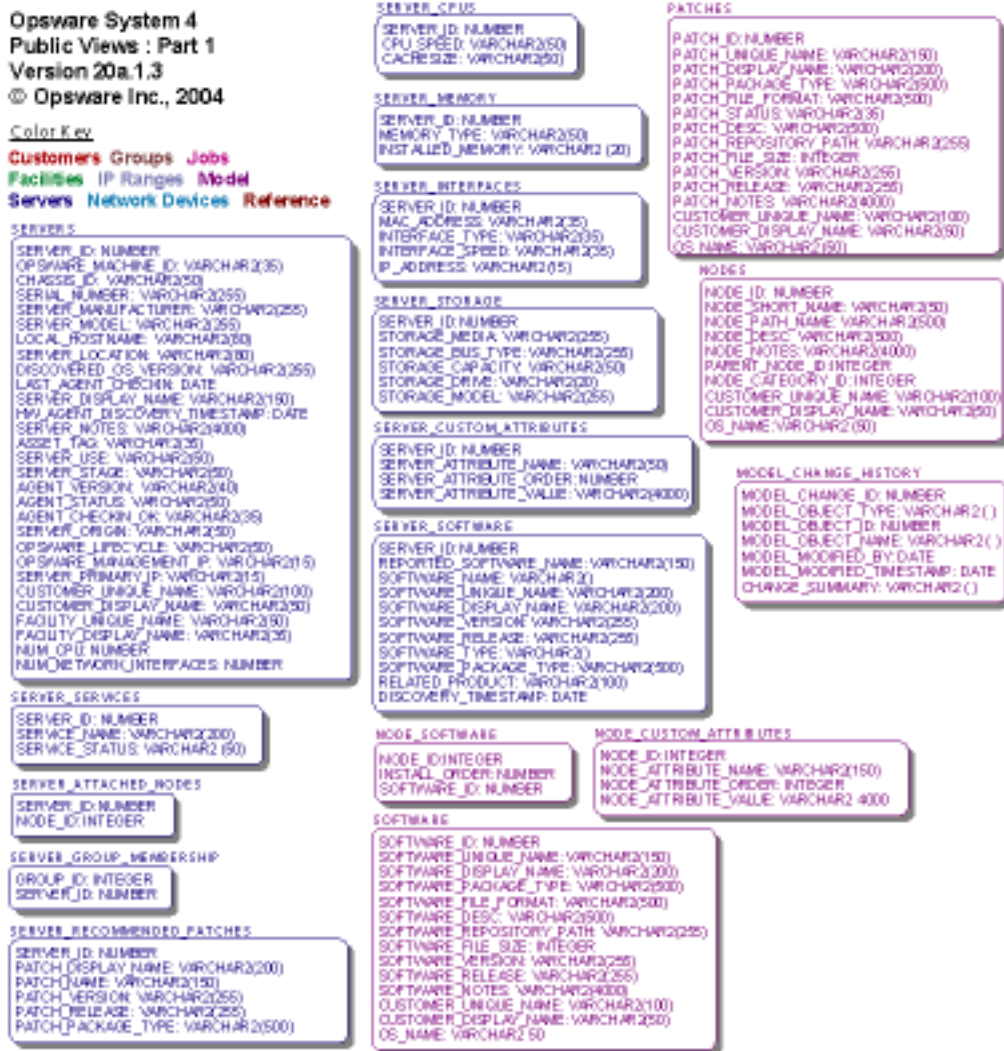
Figure 1-8: Public Views Relationships Chart – Part One†

Figure 1-9: Public Views Relationships Chart — Part Two

Table 1-1: View Name: SERVER_SERVICES

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server on which the service is installed
SERVICE_NAME	The name of the service on the server

Table 1-1: View Name: SERVER_SERVICES

COLUMN NAME	DESCRIPTION
SERVICE_STATUS	The status of the server as returned in a sentence, "This server is in <value> state". The value will most likely be Running, Stopped, or Paused. It can also be Paused Pending, Start Pending, Stop Pending, or Continue Pending.

Table 1-2: View Name: NODES

COLUMN NAME	DESCRIPTION
NODE_ID	The unique identifier for a node. This ID is generated automatically by the Opsware System.
NODE_SHORT_NAME	The name for a node
NODE_PATH_NAME	The full path to a node in the Opsware hierarchy
NODE_DESC	The description of a node
NODE_NOTES	When creating a node, the user can specify a description (which is limited to 255 characters), as well as notes, which can be longer than the description. For example, use this field to put temporary information on the node to note that an architect is still working on the node, or that changes should not be allowed and why.
PARENT_NODE_ID	The unique identifier of the node that is above a node in the model hierarchy

Table 1-2: View Name: NODES

COLUMN NAME	DESCRIPTION
NODE_CATEGORY_ID	The unique identifier for the node type that classifies a node. This is useful for filtering other node lists by category. 1. Customer 2. Data Center 3. Hardware 4. Service Level 5. Operating System 6. Opsware 7. System Utilities 8. Database Server 9. Application Server 10. Web Servers 11. Other Applications 12. OS Extras 13. <not used> 14. Templates 15. Patches
CUSTOMER_UNIQUE_NAME	The unique name of the customer who owns a node
CUSTOMER_DISPLAY_NAME	The display name of the customer who owns a node, or Customer_Independent for nodes that can span operating systems, or Not Assigned
OS_NAME	The operating system that applies to a node

Table 1-3: View Name: NODE_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
NODE_ID	The unique identifier for the node to which a custom attribute applies
NODE_ATTRIBUTE_NAME	The key name of a custom attribute

Table 1-3: View Name: NODE_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
NODE_ATTRIBUTE_ORDER	When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of NODE_ATTRIBUTE_VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.
NODE_ATTRIBUTE_VALUE	The value of the node custom attribute. When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of NODE_ATTRIBUTE_VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.

Table 1-4: View Name: MODEL_CHANGE_HISTORY

COLUMN NAME	DESCRIPTION
MODEL_CHANGE_ID	The unique identifier for an entry in the node change log. This ID is generated automatically by the Opsware System.
MODEL_OBJECT_TYPE	Indicates whether the model object that was changed is a node or a server
MODEL_OBJECT_ID	The unique identifier for the node or server to which a change applies
MODEL_OBJECT_NAME	The name of the model object. For nodes, this will be the node short name. For servers, this will be the server display name.
MODEL_MODIFIED_BY	The user who performed an operation
MODEL_MODIFIED_ TIMESTAMP	The date and time an operation occurred or started
CHANGE_SUMMARY	A summary of the changes that occurred during an operation

Table 1-5: View Name: SERVER_CPUS

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server in which a CPU is installed
CPU_SPEED	The speed of a CPU in megahertz
CACHESIZE	The size of the cache, in kilobytes, that a CPU uses

Table 1-6: View Name: SERVER_MEMORY

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server in which memory is installed
MEMORY_TYPE	The type of memory: RAM, SWAP, or SYSTEM MEMORY
INSTALLED_MEMORY	The amount of memory in kilobytes of the given type installed in a server

Table 1-7: View Name: SERVER_INTERFACES

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server in which a network interface is installed
MAC ADDRESS	The hardware address for a network interface card
INTERFACE_TYPE	The type of network interface: ETHERNET, SERIAL, FIBER CHANNEL, or VLAN
INTERFACE_SPEED	The speed of a network interface
IP_ADDRESS	The IP address for a network interface

Table 1-8: View Name: SERVER_STORAGE

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server in which a local storage device is installed
STORAGE_MEDIA	The media for a local storage device: DISK, FLOPPY, or CDROM
STORAGE_BUS_TYPE	The type of bus on which a storage device resides: IDE or SCSI
STORAGE_CAPACITY	The capacity of a storage device in kilobyes

Table 1-9: View Name: SERVER_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server to which a custom attribute applies
SERVER_ATTRIBUTE_NAME	The key name of a custom attribute
SERVER_ATTRIBUTE_ORDER	When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of SERVER_ATTRIBUTE_ VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.
SERVER_ATTRIBUTE_VALUE	The value of the server custom attribute. When a value has more than 4,000 characters, the value is broken into sections. The order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of SERVER_ATTRIBUTE_VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.

Table 1-10: View Name: SERVER_SOFTWARE

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier of the server on which software is installed
REPORTED_SOFTWARE_NAME	When the server registers its software, this field is generated. Depending on the SOFTWARE_TYPE, this name will vary.
SOFTWARE_NAME	The name of the software installed on a server as reported by the server
SOFTWARE_DISPLAY_NAME	The display name of the software
SOFTWARE_VERSION	The manufacturer's version number for the software
SOFTWARE_RELEASE	The manufacturer's release number for the software
SOFTWARE_TYPE	The type of software. See the SOFTWARE table: SOFTWARE_ PACKAGE_TYPE for the full list.
RELATED_PRODUCT	Defines the relationship between software

Table 1-10: View Name: SERVER_SOFTWARE

COLUMN NAME	DESCRIPTION
DISCOVERY_TIMESTAMP	The date and time at which the software was first discovered on a server

Table 1-11: View Name: SOFTWARE

COLUMN NAME	DESCRIPTION
SOFTWARE_ID	The unique identifier for some software. This ID is generated automatically by the Opsware System
SOFTWARE_UNIQUE_NAME	The unique name of a software application
SOFTWARE_DISPLAY_NAME	This display name of this software application
SOFTWARE_PACKAGE_TYPE	The type of software unit: AIX Base Fileset AIX Fileset AIX LPP AIX Update Fileset APAR APAR Fileset Application Configuration Backup File Application Configuration Backup Manifest File HP-UX Depot HP-UX Fileset HP-UX Patch Fileset HP-UX Patch Product HP-UX Product RPM Solaris Package Solaris Package Response File Solaris Patch Solaris Patch Cluster Unknown Windows GMI Windows Hotfix Windows MSI Windows Servicepack

Table 1-11: View Name: SOFTWARE

COLUMN NAME	DESCRIPTION
SOFTWARE_FILE_FORMAT	The file formats for this software: .bff, .exe, .gmi, .msi, .py, .rpm, .tar, .gz, .z, .tgz, .xml, .zip, Datastream file, and Text file. *Unknown* - Could not determine the file format of this software. *Virtual* - The software is a logical unit only. There is no corresponding physical file.
SOFTWARE_DESC	The description of a software application
SOFTWARE_REPOSITORY_ PATH	The full path to the physical location of a software package in the Software Repository in the Opsware System
SOFTWARE_FILE_SIZE	The size of a file in the package repository in bytes
SOFTWARE_VERSION	The manufacturer's version number for a software application
SOFTWARE_RELEASE	The manufacturer's release number for a software application
SOFTWARE_NOTES	The notes regarding a software application
CUSTOMER_UNIQUE_NAME	The unique name of the customer who owns a software application
CUSTOMER_DISPLAY_NAME	The display name of the customer who owns a software application
OS_NAME	The software platform on which a software application can be installed

Table 1-12: View Name: NODE_SOFTWARE

COLUMN NAME	DESCRIPTION
NODE_ID	The unique identifier of the node to which software is attached
INSTALL_ORDER	The order in which software is installed when reconciling a node onto a server
SOFTWARE_ID	The unique identifier of the software that is attached to this node

Table 1-13: View Name: MODEL_REPOSITORY_VERSION

COLUMN NAME	DESCRIPTION
MODEL_REPOSITORY_ VERSION	The version number for the current public views (for example, Version 20.0.3)

Table 1-14: View Name: CUSTOMERS

COLUMN NAME	DESCRIPTION
CUSTOMER_ID	The unique identifier for a customer. This ID is generated automatically by the Opsware System
CUSTOMER_UNIQUE_NAME	The unique name of a customer
CUSTOMER_DISPLAY_NAME	The display name of a customer. Display names are not necessarily unique across customers and can include spaces and special characters.
CUSTOMER_STATUS	*Active* - Indicates whether a customer is actively being used to classify servers.

Table 1-15: View Name: CUSTOMER_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
CUSTOMER_ID	The unique identifier for the customer to which a custom attribute applies
CUSTOMER_ATTRIBUTE_NAME	The key name of a custom attribute
CUSTOMER_ATTRIBUTE_ ORDER	When a value has more than 4,000 characters, the value is split into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of CUSTOMER_ATTRIBUTE_ VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.
CUSTOMER_ATTRIBUTE_VALUE	When a value has more than 4,000 characters, the value is split into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of CUSTOMER_ATTRIBUTE_ VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.

Table 1-16: View Name: FACILITIES

COLUMN NAME	DESCRIPTION
FACILITY_ID	The unique identifier for a facility. This ID is generated automatically by the Opsware System.
FACILITY_UNIQUE_NAME	The unique name of a facility
FACILITY_ DISPLAY_NAME	The display name of a facility. Display names are not necessarily unique across facilities and can include spaces and special characters.

Table 1-17: View Name: FACILITY_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
FACILITY_ID	The unique identifier for the facility to which a custom attribute applies
FACILITY_ATTRIBUTE_NAME	The key name of a custom attribute
FACILITY_ATTRIBUTE_ORDER	When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of FACILITY_ATTRIBUTE_ VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.
FACILITY_ATTTRIBUTE_VALUE	The value of a this attribute. When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of FACILITY_ATTRIBUTE_VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.

Table 1-18: View Name: IP_RANGE_GROUPS

COLUMN NAME	DESCRIPTION
IP_RANGE_GROUP_ID	The unique identifier for a group IP address range. This ID is generated automatically by the Opsware System.
IP_GROUP_NAME	The unique name for a group of IP address ranges

Table 1-18: View Name: IP_RANGE_GROUPS

COLUMN NAME	DESCRIPTION
CUSTOMER_UNIQUE_NAME	The unique name of the customer to which groups of IP address ranges belong
CUSTOMER_DISPLAY_NAME	The display name of the customer to which groups of IP address ranges belong
FACILITY_UNIQUE_NAME	The unique name of the facility in which groups of IP address ranges exist
FACILITY_DISPLAY_NAME	The display name of the facility in which groups of IP address ranges exist

Table 1-19: View Name: IP_RANGES

COLUMN NAME	DESCRIPTION
IP_RANGE_ID	The unique identifier for an IP address range. This ID is generated automatically by the Opsware system.
IP_RANGE_UNIQUE_NAME	The primary name for an IP address range
IP_RANGE_DISPLAY_NAME	Secondary name for an IP address range
IP_RANGE_DESC	The description of a range of IP addresses
IP_RANGE_TYPE	The use for this pool of IP addresses, such as core Opsware servers, public, and so forth.
IP_RANGE_SUBTYPE	Indicates whether an IP address range is used for production, development, staging, and so forth
SUBNET	The subnet mask for a range of IP addresses

Table 1-19: View Name: IP_RANGES

COLUMN NAME	DESCRIPTION
CIDR	Classless Inter-Domain Routing, also known as supernetting. The CIDR determines the number of hosts that can be used within that IP range, i.e., the size of the pool. CIDR is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes. CIDR Block Prefix # of Host Addresses /26 64 hosts /25 128 hosts /24 256 hosts /23 512 hosts /22 1,024 hosts /21 2,048 hosts /20 4,096 hosts /19 8,192 hosts /18 16,384 hosts /17 32,768 hosts /16 65,536 hosts /15 131,072 hosts /14 62,144 hosts /13 524,288 hosts
IP_RANGE_GROUP_ID	The unique identifier for the group to which an IP address range belongs

Table 1-20: View Name: JOBS

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier for the server against which this job was executed
JOB_ID	The unique identifier for a job. This ID is automatically generated by the Opsware System.

Table 1-20: View Name: JOBS

COLUMN NAME	DESCRIPTION
JOB_DESC	The purpose of a session
USERNAME	The user who initiated a session
JOB_STATUS	Indicates the disposition of a job: *Success* - The Opsware System completed this job without error. *Pending* - The Opsware System has not yet attempted this job. *Deleted* - The job was removed. *Warning* - The job returned some error condition, but completed. *Failure* - The job did not complete.
JOB_START_TIMESTAMP	The date and time at which a session was started
JOB_END_TIMESTAMP	The date and time at which a session completed

Table 1-21: View Name: JOB_EVENTS

COLUMN NAME	DESCRIPTION
JOB_ID	The unique identifier of a session for which an operation is a part
EVENT_ID	The unique identifier for an operation. This ID is automatically generated by the Opsware System.
EVENT_NAME	The operation that was performed

Table 1-21: View Name: JOB_EVENTS

COLUMN NAME	DESCRIPTION

EVENT_STATUS	The state of an operation. The most common possible states a user sees are:
	    ACTIVE - The command is running on the Opsware Agent.
	    FAILURE - The command failed.
	    SUCCESS - The command succeeded.
	    WAITING - The system is waiting for a pause to be resumed or for a child script to complete.
	
	Other infrequent messages:
	    INIT - The command has just been created. Transitions to LOCKED, LOCKFAIL, PROXY, PROXYFAIL, WAITING.
	    LOCKFAIL - The ServiceInstance the command needs to operate on is locked for another Session. Transitions to LOCKED.
	    LOCKED - The ServiceInstance the command needs to operate on was successfully locked for this Session. Transitions to POKED, POKEFAIL.
	    POKEFAIL - The ServiceInstance is not reachable on the network. At least one poke attempt has failed. Transitions to POKED.
	    POKED - The ServiceInstance is reachable on the network and a poke has been sent to it to notify it that a command is ready. The ServiceInstance is locked. Transitions to ACTIVE.
	    PROXYFAIL - The Command Engine is unable to contact the remote Command Engine that should manage the command. Transitions to PROXY.
	    PROXY - The command has been successfully delivered to the remote Command Engine that manages it. Transitions to SUCCESS, FAILURE, ABORTED.
	    ACTIVE - The ServiceInstance has fetched the command and is (presumably) executing it. The ServiceInstance is locked. Transitions to SUCCESS, FAILURE, ABORTED.
	    WAITING - The command is not a typical device interaction, but is pausing the session or running another script. Transitions to SUCCESS, FAILURE, ABORTED.
	    DENIED - Due to a permissions problem, the Command Engine refused to deliver a command to a ServiceInstance or a ServiceInstance refused to run a command that had been delivered. This is a terminal state.
	    SUCCESS - The ServiceInstance finished executing the command and returned results with a SUCCESS status, or restarted and registered after a previous command returned a CYCLING or BOOTING status. This is a terminal state.
	    FAILURE - The ServiceInstance finished executing the command and returned results with a FAILURE status. This is a terminal state.
	    ABORTED - The ServiceInstance could not execute the command, perhaps because the command name is unknown. This is a terminal state.
	
	Some background:
	    Most states are transitional. For example, the event starts out in INIT state, but stays there for just a second while it finishes creating the information needed to move onto the next state. The next state is usually LOCKED, which means it's locking the service instance so that it's the only one performing an operation. Two operations can't perform at the same time. Then it goes to POKED, usually for less than a second, where the system is contacting the Opsware Agent and is waiting for the Opsware Agent to fetch the command. Once the command is sent, it's in ACTIVE state. This is the state it stays in until completed. Once completed, it usually goes to SUCCESS or FAILURE, depending on the outcome.

Table 1-22: View Name: JOB_PARAMETERS

COLUMN NAME	DESCRIPTION
JOB_ID	The unique identifier of the session to which a parameter applies
PARAM_NAME	The key name of a parameter
PARAM_VALUE	The value of a parameter

Table 1-23: View Name: JOB_RESULTS

COLUMN NAME	DESCRIPTION
SERVER_ID	The unique identifier for the server for a job result
JOB_ID	The unique identifier for a job result
JOB_RESULTS_NAME	The name of the job results, such as "Installed Package"
JOB_RESULTS_ORDER	The order of job results. Ordering begins with 0.
JOB_RESULTS_TEXT	The details of the results of a job

Table 1-24: View Name: NETWORK_DEVICES

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier for a network device. This ID is generated automatically by the Opsware System.
OPSWARE_MACHINE_ID	The unique ID that the Opsware System use to identify a device
CHASSIS_ID	The serial number for a network device. If no serial number is available, the MAC address for a network device is used.
SERIAL_NUMBER	A user-defined column for storing chassis-related information such as the serial number
NETWORK_DEVICE_ MANUFACTURER	The manufacturer of a network device, as reported during hardware registration with the Opsware System
NETWORK_DEVICE_MODEL	The model of a network device as reported during hardware registration with the Opsware System
LOCAL_HOSTNAME	The hostname of a network device as reported by the Opsware Agent
NETWORK_DEVICE_LOCATION	A user-defined column for storing information about the location of a network device

Table 1-24: View Name: NETWORK_DEVICES

COLUMN NAME	DESCRIPTION
DISCOVERED_OS_VERSION	The version of the operating system of a network device as reported by the Opsware Agent
LAST_AGENT_CHECKIN	The date of the last successful Opsware Agent hardware registration for a network device
NETWORK_DEVICE_DISPLAY_ NAME	The display name of a network device as set by using the Opsware Command Center
HW_AGENT_DISCOVERY_ TIMESTAMP	The date and time (UTC) of the first successful Opsware Agent hardware registration for a network device
NETWORK_DEVICE_NOTES	The notes about a network device
ASSET_TAG	A user-defined column for storing asset related information such as the asset tag number
NETWORK_DEVICE_USE	The default values shipped are listed below. An administrator can use the Opsware Command Center (in Administration ‰ Server Attributes) to change and create new values. Predefined Values: - Development - Staging - Production - Not Specified
NETWORK_DEVICE_STAGE	The deployment stage of the network device. These values can be set by the user from the Opsware Command Center: *Not Specified* - The Opsware system is unable to determine the state of the network device. *In Deployment* - The network device has been provisioned, but has not yet had all software installed and configured. *Ops Ready* - All software has been installed and configured, and the network device is ready for final testing before being ready for live traffic. *Live* - The network device is ready for live traffic. *Offline* - The network device might be operating but has been removed from active management.
NETWORK_DEVICE_ORIGIN	Indicates whether or not the network device was provisioned by using the Opsware System

Table 1-24: View Name: NETWORK_DEVICES

COLUMN NAME	DESCRIPTION
OPSWARE_LIFECYCLE	How the Opsware System defines the state of a machine: *Available* - Seen by the Opsware System in the "Server Pool" and ready to deploy an Operating System. *Installing OS* - In the process of installing an operating system. *Build Failed* - Failed in its attempt to install an operating System. *Managed* - Working under the Opsware umbrella and available for all Opsware functions. *Deactivated* - This state is the result of choosing "Deactivate" from the Managed Server menu. The Opsware System will no longer manage this machine.
OPSWARE_MANAGEMENT_IP	The IP address that the Opsware Agent uses to manage a network device
NETWORK_DEVICE_PRIMARY_IP	The primary IP address of this network device
CUSTOMER_UNIQUE_NAME	The unique name of the customer using a network device
CUSTOMER_DISPLAY_NAME	The display name of the customer using a network device
FACILITY_UNIQUE_NAME	The unique name of the facility in which a network device exists
FACILITY_DISPLAY_NAME	The display name for the facility in which a network device exists
NUM_CPU	The number of CPUs installed in a network device
NUM_NETWORK_INTERFACES	The number of network interfaces installed in a network device

Table 1-25: View Name: NETWORK_DEVICE_CPUS

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device in which a CPU is installed
CPU_SPEED	The speed of a CPU in megahertz
CACHESIZE	The size of the cache, in kilobytes, that a CPU uses

70

Table 1-26: View Name: NETWORK_DEVICE_MEMORY

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device in which memory is installed
MEMORY_TYPE	The type of memory: RAM, SWAP, or SYSTEM MEMORY
INSTALLED_MEMORY	The amount of memory in kilobytes of the given type installed in a network device

Table 1-27: View Name: NETWORK_DEVICE_INTERFACES

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device in which memory is installed
MAC ADDRESS	The hardware address for a network interface card
INTERFACE_TYPE	The type of network interface: ETHERNET, SERIAL, FIBER CHANNEL, or VLAN
INTERFACE_SPEED	The speed of a network interface
IP_ADDRESS	The IP address for a network interface

Table 1-28: View Name: NETWORK_DEVICE_STORAGE

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device in which memory is installed
STORAGE_MEDIA	The media for a local storage device: DISK, FLOPPY, or CDROM
STORAGE_BUS_TYPE	The type of bus on which a storage device resides: IDE or SCSI
STORAGE_CAPACITY	The capacity of a storage device in kilobyes

Table 1-29: View Name: NET_DEVICE_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device to which a custom attribute applies
NETWORK_DEVICE_NAME	The key name of a custom attribute

Table 1-29: View Name: NET_DEVICE_CUSTOM_ATTRIBUTES

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ORDER	When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and is numbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of DEVICE_ATTRIBUTE_ VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.
NETWORK_DEVICE_VALUE	The value of the network device custom attribute. When a value has more than 4,000 characters, the value is broken into sections. The Order starts at 0 and isnumbered 0, 1, 2, and so forth. These should be concatenated to form the complete value from the corresponding series of DEVICE_ATTRIBUTE_VALUE. Thus, for a 11,000 character string, concatenate values from ORDER 0, 1 and 2 to get the complete value.

Table 1-30: View Name: NETWORK_DEVICE_ATTACHED_NODES

COLUMN NAME	DESCRIPTION
NETWORK_DEVICE_ID	The unique identifier of the network device that is associated with a node
NODE_ID	The unique identifier of the node that is associated with a network device

72

Index