VERITAS™

VERITAS Global Data Manager™ 5.1

System Administrator’s Guide

for UNIX and Windows

N12344C

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual. 50504.

VERITAS Legal Notice

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2908
www.veritas.com

Third-Party Copyrights

Contents

Preface

This comprehensive manual provides detailed information and procedures for using Global Data Manager 5.1. Topics covered in this manual require the reader to have a working knowledge of the Windows or UNIX operating environments.

What Is In This Manual?

This manual is for network administrators responsible for protecting data on the network. The following is an organizational overview of this manual:

Revision History	"Revision History" discusses changes to the GDM product that have occurred since the previous release.
Chapter 1	"Introducing Global Data Manager" contains general information about Global Data Manager, how Global Data Manager works, and what it can do for you.
Chapter 2	"GDM Installation" includes information about hardware and software requirements and instructions on performing the initial configuration of Global Data Manager.
Chapter 3	"GDM Configuration" includes configuration details about GDM.
Chapter 4	"GDM Advanced Configuration"presents steps for making advanced configuration adjustments to GDM.
Chapter 5	"Using GDM" explains the GDM Dashboard interface. This chapter also explains how to use the Dashboard when monitoring your GDM domain.
Chapter 6	"GDM Reports" includes information about the types of reports available through the GDM Dashboard.

Chapter 7	"Troubleshooting GDM" discusses solutions to issues that you may encounter using Global Data Manager.
Appendix A	"Common Terminology" describes the NetBackup and Backup Exec terms that are used interchangeably in GDM.

Getting Help

Accessing the VERITAS Technical Support Web Site

The VERITAS Technical Support Web site allows you to:

- obtain updated information about Global Data Manager, including system requirements, supported platforms, and supported peripherals
- contact the VERITAS Technical Support staff and post questions to them
- get the latest patches, upgrades, and utilities
- view the Global Data Manager Frequently Asked Questions (FAQ) page
- search the knowledge base for answers to technical support questions
- receive automatic notice of product updates
- find out about Global Data Manager training
- read current white papers related to Global Data Manager

The address for the VERITAS Technical Support Web site is:

- `http://support.veritas.com`

Using VERITAS Telephone and Email Support

Telephone support for Global Data Manager is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

▼ To locate the telephone support directory on the VERITAS web site

1. Open `http://www.support.veritas.com/` in your web browser.

2. Click **Phone Support**.

3. Select a phone number from the list that appears.

▼ To contact Technical Support via email

- ❖ Send an e-mail to the following e-mail address:

  support@veritas.com

Using Global Data Manager Online Documentation (CD-ROM)

Online documentation is included on the Global Data Manager installation CD. These documents can be displayed with the Adobe Acrobat™ Reader for Windows NT and the Adobe Acrobat Reader for UNIX.

▼ To view an online document

4. Insert the CD-ROM containing the NetBackup Global Data Manager software into the drive.

   a. If you are running Windows, the manual files are located in the `\Doc` directory on the CD.

   b. If you are running UNIX, the manual files are located in the `/Doc` directory on the CD.

5. If you do not already have the Adobe Acrobat reader installed on your system, you can download the latest version of the program from Adobe's web site (www.adobe.com).

   a. If you are running on the Windows platform, you can open the manual you want to view by double-clicking the manual's icon.

   b. If you are running on the UNIX platform, or you want to open the manual files from within Adobe Acrobat, use Acrobat's **File > Open** menu.

Note To find the information you need, use Adobe Acrobat's powerful search tools, or the manual's hypertext Table of Contents and Index.

Using Global Data Manager Online Help

When you click **Help** on the Global Data Manager menu bar, the following options are displayed:

- *Help Topics.* Displays the Help window for Microsoft Management Console.
- *About GDM Dashboard.* Lists information about this version of Global Data Manager Dashboard.

Help is also available in most windows and all menus. For menu items help, click the item and press <F1>. For help on a particular dialog box, display the dialog box and press <F1>, or click the Help button.

Every Help window includes a Help Menu Bar and a Help Selection Bar.

The Help dialog contains the following items:

Option	Description
Contents tab	Lists information organized by category.
Index tab	Lists the Help index. Type a topic you want to find or scroll through the list to search for Help topics.
Find tab (Windows) **Search tab (UNIX)**	Enables you to search the Help system for specific words and phrases.

Accessibility Features

Global Data Manager contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the NetBackup *System Administrator's Guide* and the *Backup Exec System Administrator's Guide*.

Conventions

The following section explains typographical and other conventions used in this guide.

Product-Specific Conventions

The following term is used in VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

- Microsoft Windows, Windows

  Terms used to describe a specific product or operating system developed by Microsoft, Inc. Some examples are, Windows 2000, Windows Server 2003, Windows servers, Windows clients, Windows platforms, or Windows GUI. For more information on the Windows operating systems that NetBackup supports, refer to the *VERITAS NetBackup Release Notes for UNIX and Windows* or go to the VERITAS support web site at `http://www.support.veritas.com`.

Note When a specific Windows product is identified in the documentation, only that particular product is valid in that instance.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.

Conventions (continued)

Convention	Description
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces.
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

```
command arg1|arg2
```

In this example, the user can use either the *arg1* or *arg2* variable.

Navigating Multiple Menu Levels

When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action.

The following example shows how the > is used to condense a series of menu selections into one step:

❖ Select **Start** > **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**.

The corresponding actions could be described in more steps as follows:

1. Click **Start** in the task bar.

2. Move your cursor to **Programs**.

3. Move your cursor to the right and highlight **VERITAS NetBackup**.

Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.

Introducing Global Data Manager 1

This section provides an overview of the NetBackup Global Data Manager and its features.

Introducing Global Data Manager includes the following topics:

Section	Description
"Introducing Global Data Manager" on page 1	Describes a general overview of the Global Data Manager.
"Understanding GDM" on page 4	Describes how GDM works and its use of visual keys within the graphical user interface.

Introducing Global Data Manager

VERITAS Global Data Manager is an advanced, high-performance monitoring application that works in conjunction with your installed base of VERITAS NetBackup Server and VERITAS NetBackup Enterprise master servers, and VERITAS Backup Exec for Windows NT/2000 and VERITAS Backup Exec for Windows Servers media servers. It allows you to quickly view the operational status and health of your distributed data protection environment in real-time.

Using both icons and color, GDM enables you to quickly isolate NetBackup and Backup Exec system issues by displaying visual keys in a single display window. And because the intuitive and easy-to-use GDM client interface (GDM Dashboard) runs on both Windows and UNIX platforms, you can monitor both NetBackup and Backup Exec operations from a centralized computer on either platform.

Why Use GDM?

As the proliferation of data continues in today's computing environment, effective data management and analysis tools are required to manage and protect this valuable resource. In many cases NetBackup and Backup Exec are used to protect the data. As your investment in these products grows, you may find the need to monitor multiple NetBackup master servers and Backup Exec media servers, at many locations.

GDM offers you the ability to quickly gain, at a glance, a real-time understanding of the health of your entire environment. Using GDM, you can diagnose problems, identify potential issues, or just review the operational status of one or more computers -- all from a centralized location. Without GDM, the operational status of each NetBackup master server or Backup Exec media server would have to be determined by attaching to each computer individually.

Additional benefits include:

- *Monitoring of sparsely staffed remote sites*. At remote sites where staffing is an issue, GDM enables you to use available resources in a more efficient manner.
- *More efficient monitoring capabilities*. GDM consolidates all pertinent information and presents it in a convenient, easy-to-use, single window graphical interface.
- *24 hour monitoring of global NetBackup sites*. Global NetBackup and Backup Exec sites can be continuously monitored on a 24 hour basis from GDM Dashboard installations world-wide. For example, assuming a company has NetBackup and Backup Exec sites in San Francisco, Paris, and Tokyo, a Tokyo-based administrator can monitor all locations during Japanese business hours. At the end of the Japanese work day, world-wide monitoring responsibilities can be assumed by the Paris-based administrator. At the end of the French work day, a San Francisco-based administrator can assume monitoring duties.
- *Advanced filtering options*. In environments where a high volume of data is being protected, GDM uses advanced filtering options that enable you to display only the type of information you want to see.

New In GDM

- *NetBackup Cluster support*. GDM includes support for monitoring and management of NetBackup 5.0 and 5.1 master servers that are configured in a clustered environment.

Supported Operating Systems and Hardware

For a list of GDM-compatible operating systems, see **Compatibility Lists** at http://support.veritas.com. For additional information, refer to the GDM 5.1 Release Notes.

Common Terminology

Because GDM supports two platforms (NetBackup and Backup Exec), a list of terminology common between the two products is available.

See also:

"Common Terminology" on page 147.

Managing NetBackup and Backup Exec Installations

In many cases, heterogeneous network environments are in place, running both UNIX and Windows servers. In such a network, both NetBackup master servers and Backup Exec for Windows Servers media servers may be protecting valuable data. Using the flexibility offered by GDM, you can easily administer both data protection platforms using a single Java-based or Windows-based GDM Dashboard.

See also:

"Administering the Managed Servers" on page 109.

Limitations

- Although Backup Exec media servers are supported in the GDM domain, they can be configured only as managed servers. Unlike NetBackup master servers, a Backup Exec media server cannot be configured as a GDM Server.
- Backup Exec alerts displayed in GDM are read-only. However, launching Backup Exec's Remote Administrator client though GDM's Action menu enables you to actively manage any alerts that are generated by the Backup Exec managed server.
- Only Backup Exec for Windows NT/2000 8.6 and Backup Exec for Windows Servers 9.x products are supported. No licenses are required to monitor either Backup Exec platform. Backup Exec for NetWare is not supported.
- If Backup Exec and NetBackup are installed on the same computer, GDM will monitor the computer only as a NetBackup master server while completely ignoring it as a Backup Exec managed server. For GDM to monitor the computer solely as a Backup Exec managed server, Backup Exec and NetBackup must not reside on the same machine.
- Upgrading from Backup Exec to NetBackup requires you to uninstall the GDM version used with Backup Exec and then re-installing GDM for use with NetBackup.

Using GDM with Backup Exec Alerts

As a feature of Backup Exec, alerts are generated when an event occurs that requires a response from the user. These alerts originate from system, job, media, or devices sources, and each category may contain one or more events that can generate the alert.

GDM displays all Backup Exec-generated alerts in read-only mode, which means they cannot be addressed directly using GDM. They can however, be addressed by launching Backup Exec's administration console from within GDM, and you can, of course, physically move to the Backup Exec managed server and reply to them locally.

See also:

"Icons" on page 73.

GDM Usage Recommendations

Depending on the size of your data protection environment, a GDM Server can be configured to monitor a small number of NetBackup and Backup Exec computers, or it can monitor hundreds of them - all within the single window view of the GDM Dashboard.

However, if the number of managed servers being monitored is expected to grow substantially, you may find that monitoring them as a whole may become inefficient, due to the sheer number of servers being displayed.

In this case, it is recommended that you logically subdivide a single large NetBackup or Backup Exec domain into multiple, small GDM domains where each domain contains a GDM Server. Each GDM Server can then be configured to monitor a small number of NetBackup and Backup Exec configurations. Switching between GDM Servers enables you to remain up-to-date with the entire domain, in a much more efficient manner.

See also:

"Using GDM with Backup Exec Media Servers" on page 34.

Understanding GDM

This section explains the components of GDM and how data is gathered and presented. It also explains the visual keys used in the Dashboard interface that help you understand the operational status of your NetBackup and Backup Exec domain.

The GDM Architecture

GDM works in a user defined environment called a GDM domain. A GDM domain consists of a GDM Server, GDM Dashboard or Dashboards, NetBackup and Backup Exec managed servers.

The GDM Server

The NetBackup master server where GDM is installed and licensed is known as the GDM Server. GDM Server components include a database and software called data collectors. Data collectors are GDM components that gather pre-defined data from NetBackup 5.1 master servers or Backup Exec media servers. Under UNIX, the data collector is a component of a VERITAS-supplied GDM daemon called *visd*; under Windows, the data collector is a component of a VERITAS-supplied GDM service called the *VERITAS GDM Information Server service*.

GDM Servers store summary information for the GDM domain allowing for a quick high level view of the domain's operational status. The GDM Servers are responsible for monitoring both NetBackup master servers and Backup Exec media servers for pre-defined data that is gathered from these servers. When detected, the data is collected from each NetBackup and Backup Exec computer by the GDM Server and then stored locally in the GDM Server's database for future retrieval by a Dashboard client.

A GDM 5.1 Server can be created from any existing NetBackup 5.1 master server in the NetBackup domain. Installing the GDM Server license on more than one computer in a domain results in the creation of multiple GDM Servers.

Note Creating multiple GDM Servers is only necessary when creating multiple GDM domains.

GDM Managed Servers

GDM managed servers consist of NetBackup master servers and Backup Exec media servers that are installed and licensed in your environment.

Using GDM data collectors, GDM managed servers gather pertinent data about all backup and restore operations being conducted at NetBackup and Backup Exec media servers in the GDM domain.

Data received from a GDM data collector is stored in the managed server's local database. A subset of the data is then rolled up to the GDM Server's database.

GDM managed servers can be members of multiple GDM domains.

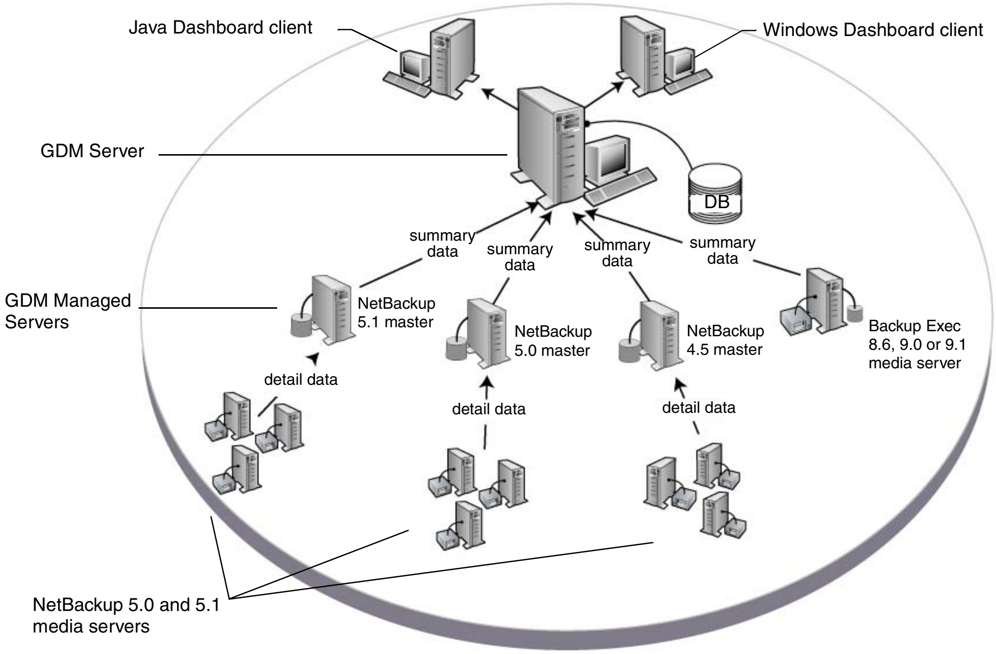
GDM Dashboard

To view the status of the domain, GDM provides an easy-to-use, Windows or Java-based graphical user interface called the *GDM Dashboard* that runs on any computer. The Dashboard connects to a GDM Server and retrieves the data stored in the GDM Server database and then presents the information in an organized and efficient manner.

Note Typically the GDM Dashboard is installed and used on a GDM Server or on a managed server in the domain. However, it can also be installed on any computer inside or outside the GDM domain, as a stand-alone application.

The following diagram shows the flow of data from the media servers to the GDM Dashboard.

GDM Workflow Diagram



Summary data collected by the GDM managed servers is rolled up to the GDM Server database at user defined intervals.

GDM Server........ NetBackup 5.1 master server running Unix or Windows

GDM Managed Servers............. NetBackup 5.1/5.0/4.5 master servers, or Backup Exec 8.6/9.0/9.1 media servers

Note: Terminology-wise, Backup Exec media servers are the equivalent of NetBackup master servers in the GDM domain.

Visual Keys

To help you understand the information being presented, the GDM Dashboard uses visual keys. These keys include color, status flags, icons, tool tips, and font styles.

Color

The colors red and yellow are used when conditions exist that should be investigated. Blue is used when general information conditions exist.

See also:

"Color" on page 72.

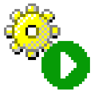
Status Flags

Status flags icons are also used in conjunction with the GDM color scheme. Each flag represents critical, warning, or informational conditions that mirror the same conditions represented with the use of color.

See also:

"Status Flags" on page 72.

Icons



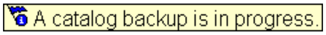
Icons are used in the detail sections of the Dashboard's right pane to help you quickly determine the status of a particular area of interest in your GDM domain.

See also:

"Icons" on page 73.

ToolTips

ToolTip



A catalog backup is in progress.

ToolTips provide brief descriptions of the visual keys that appear in the left pane when GDM detects a condition at a managed server. A ToolTip appears a second or two after resting the mouse over a managed server name where a condition appears.

Note ToolTips are also available in the right pane, for each robot LCD Drive Status graphic found in the Robot detail sections.

Font Enhancements

GDM also makes use of italicized and bold fonts when selecting managed servers in the left pane. After clicking a managed server name, the font of the selected server changes from plain font to a bold, italicized font, indicating which managed server is currently being monitored.

See also:

"Font Attribute Enhancements" on page 79.

Information Retrieval

GDM Dashboard uses drill-down technologies to retrieve information from the GDM Managed Server database. Using this technology, GDM presents a maximum amount of information in a minimum amount of screen space.

GDM Installation 2

This section provides installation, upgrade and uninstall information about GDM.

GDM Installation includes the following topics:

Section	**Description**
"Installing Global Data Manager" on page 15	Provides detailed steps for installing GDM.
"Installing GDM on UNIX for the First Time" on page 15	Provides the steps required to install GDM software for the first time on the UNIX hosts that will serve as the GDM Server or a GDM managed server.
"Installing GDM on Windows for the First Time" on page 17	Provides the steps required to install GDM software for the first time on supported Windows systems that will serve as the GDM Server or a GDM managed server.
"Installing GDM in a Cluster" on page 20	Provides the steps required to install GDM software in a clustered environment.
"Installing the GDM Dashboard as a Stand-alone Option" on page 22	Provides the steps required to install both the Windows-based and Java-based Dashboard on supported Windows systems.
"Modifying the GDM Windows Installation" on page 25	Provides the steps required to modify the GDM installation on supported Windows systems.
"Repairing the GDM Windows Installation" on page 26	Provides steps to run the repair feature of the GDM installation wizard. This option can fix missing or corrupt files, shortcuts, and registry entries.
"Upgrading to GDM 5.1" on page 27	Provides the steps necessary to upgrade GDM.

Section	Description
"Uninstalling GDM 5.1 from UNIX Systems" on page 30	Provides steps for uninstalling GDM on UNIX systems running Solaris, HP-UX, Alpha, Linux, and AIX.
"Uninstalling GDM 5.1 From Windows Systems" on page 31	Provides steps for uninstalling GDM from Windows systems.

GDM Installation Overview

GDM 5.1 can be installed on the following systems:

- UNIX NetBackup master server systems
- Windows NT, Windows 2000, and Windows Server 2003 NetBackup master server systems.
- (Dashboard only) Windows NT, Windows 2000, and Windows Server 2003 workstations that do not have NetBackup or Backup Exec installed.

GDM 5.1 is supported in NetBackup VERITAS Cluster Server and Microsoft Cluster Server environments. Refer to the compatibility matrices on the support.veritas.com website for details on which platforms and cluster solutions are supported. Before installing GDM 5.1 in a supported cluster environment, ensure that NetBackup 5.1 is installed on all nodes, and that the nodes have been fully configured as a cluster.

Note GDM 5.1 cannot be installed on Backup Exec servers. GDM 5.1 can monitor Backup Exec servers on which GDM 5.0 is installed. For more information, see the *VERITAS Global Data Manager 5.1 Release Notes.*

General GDM Considerations

GDM consists of the following software components:

- GDM Server software for both UNIX and Windows
- GDM Java-based Dashboard software for both UNIX and Windows
- GDM Windows-based Dashboard software for Windows only

GDM Server software

The Global Data Manager Server component of this software package can be installed on any supported UNIXor Windows computer running NetBackup that you want to configure as a GDM Server or a GDM managed server.

It can also be used to upgrade any supported UNIX or Windows GDM Server running any GDM 4.5 or 5.0 revision, provided that these computers are first upgraded to NetBackup 5.1.

GDM Java-based Dashboard

- The GDM Java version of the Dashboard software for UNIX and Windows is provided on the CD. The GDM Java Dashboard for UNIX is installed automatically on any UNIX system on which NetBackup master server software is installed.
- The GDM Java Dashboard for Windows can be installed on computers that are running a supported Windows system on which NetBackup master server software is installed.

Caution The NetBackup Java Administration Console must be installed on systems running a supported Windows system *before* you can install the GDM Java Dashboard for Windows. Refer to the *NetBackup Installation Guide for Windows* for more information.

Note The GDM Java Dashboard for UNIX is automatically installed on all UNIX platforms when the GDM Server for UNIX software is installed. It is not a separate installation.

GDM Windows-based Dashboard

- The GDM Windows-based Dashboard can be installed on any suported Windows system, regardless of whether NetBackup or Backup Exec software is installed.

Note The GDM Windows-based Dashboard is included in the GDM Windows installation. It can also be optionally installed on any supported Windows system, and it does not require NetBackup server software to be installed.

Requirements

- IE 5.5 or later

Installing Global Data Manager

This section guides you through the installation of GDM on both UNIX and Windows platforms.

Topics include:

- "Installing GDM on UNIX for the First Time" on page 15
- "Installing GDM on Windows for the First Time" on page 17
- "Installing the GDM Dashboard as a Stand-alone Option" on page 22
- "Modifying the GDM Windows Installation" on page 25
- "Repairing the GDM Windows Installation" on page 26

Before installing GDM, visit the VERITAS support web page at http://www.support.veritas.com for a list of the latest operating system and hardware platforms, and product patches and updates.

Caution Microsoft Internet Explorer 5.5 or higher is required on Windows systems in order to successfully install and use GDM. If IE 5.5 is not installed, upgrade your Internet Explorer version before installing GDM.

Installing GDM on UNIX for the First Time

Use the following steps to install GDM software on UNIX host systems that will serve as the GDM Server or a GDM managed server.

Note GDM is supported in NetBackup VERITAS Cluster Server and Microsoft Cluster Server environments. Refer to the compatibility matrices on the support.veritas.com website for details on what platforms and cluster solutions are supported.

Before installing GDM 5.1 in these environments, ensure that NetBackup 5.1 is installed on all nodes, and that the nodes have been fully configured as a cluster.

For more information, see the *VERITAS NetBackup 5.1 High Availability System Administrators' Guide*.

Requirements

- The target UNIX system must have the NetBackup 5.1 installed *before* beginning the installation of GDM.

Note GDM 5.1 cannot be installed on UNIX systems running any revision of NetBackup 4.5 GA or NetBackup 3.4.

Installing the GDM Server Component on UNIX

▼ To install the GDM Server component on UNIX

1. If you are installing GDM in a clustered environment, freeze the active node so that migrations do not occur while the inactive nodes are being upgraded. Install GDM on the active node last. Refer to the clustering section in the *NetBackup High Availability System Administrator's Guide* that pertains to the type of cluster software you are running for more information on freezing a service group.

2. Log in as root on the server.

   If you are already logged in, but are not the root user, execute the following command:

   ```
   su - root
   ```

3. Make sure a valid GDM license key (either GDM Server or GDM Managed Server) has been registered by entering the following command to list and add keys:

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

   For each GDM domain you are creating, make sure you specify only one host in that domain to have the GDM Server key. All other hosts should have the GDM Managed Server key.

4. Insert the CD-ROM containing the NetBackup Global Data Manager software in the drive.

5. Change your working directory to the CD-ROM directory:

   ```
   cd /<cd_rom_directory>
   ```

   where `cd_rom_directory` is the path to the directory where you can access the CD-ROM. On some platforms, it may be necessary to mount this directory.

6. To install NetBackup Global Data Manager, execute the following:

   ```
   ./install
   ```

   The install script begins the installation process.

   When finished, the GDM Server 5.1 software and the GDM Java Dashboard are installed and ready for use.

The server that acts as the GDM Server can itself be managed using the GDM Server key; you do not need to additionally register the GDM Managed Server key as well.

Note In a clustered environment, the above steps must be done on each node in the cluster.

7. If you installed GDM in a clustered environment, unfreeze the active node after installing GDM 5.1 on all nodes of the cluster. Again, refer to the appropriate clustering section in the *NetBackup High Availability System Administrator's Guide* for more information on unfreezing a service group.

Installing GDM on Windows for the First Time

Use the following steps to install GDM on a supported Windows system that will serve as the GDM Server.

GDM 5.1 is supported in VERITAS Cluster Server and Microsoft Cluster Server environments for NetBackup master servers. Refer to the compatibility matrices on the VERITAS technical support website (http://support.veritas.com) for details on what platforms and cluster solutions are supported. Before installing GDM 5.1 in these environments, ensure that NetBackup 5.1 is installed on all nodes, and that the nodes have been fully configured as a cluster. For more information, see the *VERITAS NetBackup 5.1 High Availability System Administrators' Guide*.

Caution Installing GDM 5.1 in a VERITAS Cluster Server or Microsoft Cluster Server environment is only supported when the clustering environment is configured using NetBackup-based Master Servers. Installing GDM 5.1 into VERITAS Cluster Server or Microsoft Cluster Server environments based on systems running Backup Exec is not supported.

Requirements

◆ To install the GDM Server component, you must have NetBackup 5.1 master server software installed on the computer where you are installing GDM 5.1.

Installing the GDM Server Component on Windows Systems

▼ **To install GDM server component on Windows**

1. Move to the Windows computer where you want to install GDM.

2. Log on as administrator.

3. If you haven’t already done so, install the NetBackup 5.1 server software as explained in the *NetBackup Installation Guide for Windows*.

4. Make sure a valid GDM license key (either GDM Server or GDM Managed Server) has been registered by doing the following:

   a. From the NetBackup Administration Console window, choose **Help**.

   b. From the Help menu, select **License Keys**.

      The NetBackup License Keys window appears. Existing keys are listed in the lower part of the window.

   c. To register a new key, type your license key in the New license key field and click **Add**.

      The new license key appears in the lower part of the dialog box.

5. Insert the CD-ROM containing the NetBackup Global Data Manager software in the drive.

6. From the Windows taskbar, click **Start** >**Run** and enter the following:

   ```
   <drive_letter>:\setup.exe
   ```

   where `drive_letter` is the letter of the CD-ROM drive where you can access the CD-ROM.

7. When the Installation wizard’s **Welcome** screen appears, click **Next**.

8. Read and accept the license terms and then click **Next**.

9. Enter the pertinent information on the **Customer Information** screen and then click **Next**.

10. Select **Complete** and then click **Next**.

11. Click **Install** to begin the installation.

12. When the **InstallShield Wizard Completed** screen appears, click **Finished**.

    When the installation finishes, the GDM Server software, along with the VERITAS GDM Information Server service and the Windows Dashboard are installed on your system, and are ready to use.

Note After installing GDM on a Windows platform, ensure that the Information Server service has been set to automatic start up. In some cases, the install process leaves the Information Server service to manual start-up. Do not set visd to *Automatic* if GDM is installed in a NetBackup VERITAS Cluster Server or Microsoft Cluster Server cluster.

Note In a clustered environment, the above steps must be done on each node in the cluster.

Installing GDM in a Cluster

GDM 5.1 (GDM Server and GDM managed servers) is supported in VERITAS Cluster Server and Microsoft Cluster Server environments for NetBackup Master Servers.

When GDM is installed in a cluster, the installer automatically configures GDM to use the virtual name, not the local host name, on each clustered machine it is installed on. On Windows platforms, the installer sets the EndPoints registry setting to the virtual name. On UNIX, platforms, it sets the EndPoints parameter in the visd.conf configuration file to the virtual name.

Refer to the compatibility matrices on the support.veritas.com website for details on what platforms and cluster solutions are supported.

Before installing GDM 5.1 in these environments, ensure that NetBackup 5.1 is installed on all nodes, and that the nodes have been fully configured as a cluster. For more information, see the *VERITAS NetBackup 5.1 High Availability System Administrators' Guide*.

▼ To install GDM into a cluster

1. Install and configure NetBackup into a cluster, setting up both active and inactive nodes. For more information, see the *VERITAS NetBackup 5.1 High Availability System Administrators' Guide*.

2. Do *not* freeze the active node.

3. Install GDM on all inactive nodes in the cluster. For more information on installing GDM, see “Installing Global Data Manager” on page 15.

4. After installing GDM on all inactive nodes, install GDM on the active node in the cluster. For more information on installing GDM, see “Installing Global Data Manager” on page 15.

Note If GDM installs successfully on all nodes of the cluster but does not appear to be configured correctly in the cluster or if GDM was installed while the NetBackup group was frozen, run the following bpclusterutil command (after the group is unfrozen) to configure GDM correctly in the cluster:

```
install_path\NetBackup\bin\bpclusterutil -a GDM
```

Note GDM does not cause failover. If NetBackup fails over, GDM will fail over with NetBackup. However, if there is a problem with the GDM application, a failover will not be triggered in NetBackup.

Note When installing into a Microsoft cluster, do not change the GDM services to affect the NetBackup group.

Installing the GDM Dashboard as a Stand-alone Option

The GDM 5.1 Dashboard is available in two versions for the Windows platform: A Windows-based version and a Java-based version for the Windows platform. For remote monitoring purposes, either or both of these two versions can be installed as a stand-alone GDM 5.1 option on any supported Windows system. For example, you may want to monitor the operations of your managed servers remotely using a Windows-based laptop computer.

Rather than installing the entire GDM 5.1 package, you can use the following section to install the version of the GDM Dashboard you want.

Installing the Windows GDM Dashboard as a Standalone Option

▼ **To install the Windows version of the GDM Dashboard**

Note To be able to administer your managed servers from the Windows Dashboard, install the NetBackup Administration Console and/or the applicable Backup Exec Remote Administrator Console *before* continuing with these installation instructions.

The NetBackup Administration Console is required to manage NetBackup master servers, while the Backup Exec remote administration console is required to manage Backup Exec media servers from the Windows version of the GDM Dashboard. For more information, see your NetBackup or Backup Exec documentation.

1. Move to the Windows computer where you want to install the GDM 5.1 Windows-based Dashboard.

2. Log on as administrator.

3. Insert the CD-ROM containing the NetBackup Global Data Manager 5.1 software in the drive.

4. From the Windows taskbar, click **Start** >**Run** and enter the following:

   ```
   <drive_letter>:\setup.exe
   ```

   where `drive_letter` is the letter of the CD-ROM drive where you can access the CD-ROM.

5. When the Installation wizard's **Welcome** screen appears, click **Next**.

6. Read and accept the license terms and then click **Next**.

7. Enter the pertinent information on the **Customer Information** screen and then click **Next**.

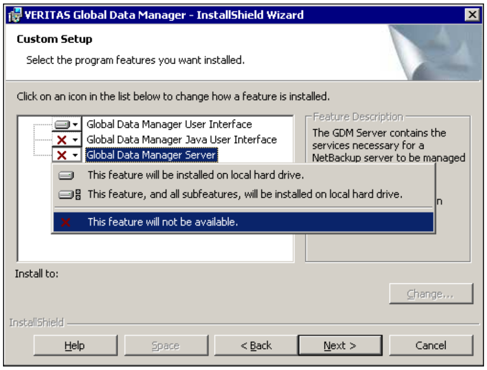
8. Select **Custom** and then click **Next**.

9. In the **Custom Setup** screen, select the **Global Data Manager User Interface** and then click **This feature will be installed on the local hard drive**.

10. If they are available, select the following options and then click **This feature will not be available** for each option. An X appears before each option after you make the selection.

    - **Global Data Manager User Java Interface**
    - **Global Data Manager Server**

Note While installing the Global Data Manager User Interface option, you can also install the Global Data Manager User Java Interface at the same time. However, if the GDM User Java Interface is already installed, selecting **This feature will not be available** will *uninstall* it.



VERITAS Global Data Manager - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

Global Data Manager User Interface
☒ Global Data Manager Java User Interface
☒ Global Data Manager Server

This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
☒ This feature will not be available.

Feature Description
The GDM Server contains the services necessary for a NetBackup server to be managed

Install to:

Note The Global Data Manager Java User Interface option is only available when the NetBackup 5.1 Java Administration Console is installed on this computer.

The Global Data Manager Server option is only available if NetBackup 5.1 master server software or Backup Exec 8.6, 9.0, or 9.1 media server software is installed on this computer.

11. Click **Next**.

12. Click **Install** to begin the installation.

13. When the **InstallShield Wizard Completed** screen appears, click **Finished**.

    The GDM 5.1 Windows Dashboard is now installed.

Installing the Java-based GDM Dashboard

▼ To install the Java-based GDM Dashboard on Windows

Note To be able to manage your managed servers from the Java Dashboard, install the NetBackup Java Administration Console *before* continuing with these installation instructions.

The NetBackup Java Administration Console is required to manage NetBackup master servers from the GDM Java Dashboard. Backup Exec managed servers cannot be administered from the GDM Java Dashboard.

1. Move to the Windows computer where you want to install the GDM 5.1 Java-based Dashboard.

2. Log on as administrator.

3. Insert the CD-ROM containing the NetBackup Global Data Manager 5.1 software in the drive.

4. From the Windows taskbar, click **Start** >**Run** and enter the following:

   ```
   <drive_letter>:\setup.exe
   ```

   where `drive_letter` is the letter of the CD-ROM drive where you can access the CD-ROM.

5. When the Installation wizard's **Welcome** screen appears, click **Next**.

6. Read and accept the license terms and then click **Next**.

7. Enter the pertinent information on the **Customer Information** screen and then click **Next**.

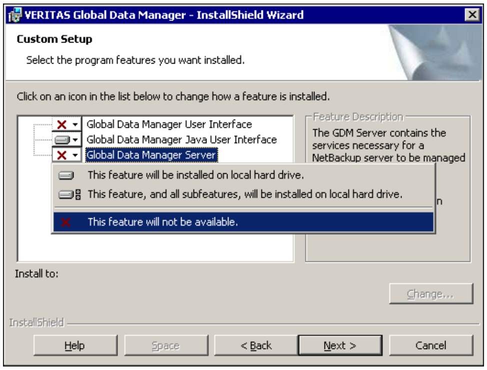
8. Select **Custom** and then click **Next**.

9. In the **Custom Setup** screen, select the **Global Data Manager Java User Interface** and then click **This feature will be installed on the local hard drive**.

10. Select the following options and then click **This feature will not be available** for each option. An X appears before each option after you make the selection.

- **Global Data Manager User Interface**
- **Global Data Manager Server**

Note While installing the Global Data Manager Java User Interface option, you can also install the Global Data Manager User Interface at the same time. However, if the GDM User Interface is already installed, selecting **This feature will not be available** will *uninstall* it.



VERITAS Global Data Manager - InstallShield Wizard

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

☒ Global Data Manager User Interface
Global Data Manager Java User Interface
☒ Global Data Manager Server

This feature will be installed on local hard drive.
This feature, and all subfeatures, will be installed on local hard drive.
This feature will not be available.

Feature Description
The GDM Server contains the services necessary for a NetBackup server to be managed

Install to:

11. Click **Next**.

12. Click **Install** to begin the installation.

13. At the **InstallShield Wizard Completed** screen, click **Finished**.

    The GDM 5.1 Java-based Dashboard installation is now complete.

Modifying the GDM Windows Installation

This section guides you through the steps required to enable you to change the GDM features that are installed.

▼ To change the GDM features that are installed

1. Click **Start>Settings>Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Select **VERITAS Global Data Manager** and then click **Change**.

4. On the **Welcome** screen, click **Next**.

5. On the **Program Maintenance** screen, select **Modify**.

6. Click **Next**.

7. On the **Custom Setup** screen, make your feature modifications and then click **Next**.

8. Follow the directions provided by the Windows install program.

Repairing the GDM Windows Installation

This section guides you through the steps required to run the repair feature of the GDM installation wizard. This option can fix missing or corrupt files, shortcuts, and registry entries.

▼ To repair the GDM installation

1. Click **Start**>**Settings**>**Control Panel**.

2. Double-click **Add/Remove Programs**.

3. Select **VERITAS Global Data Manager** and then click **Change**.

4. On the **Welcome** screen, click **Next**.

5. On the **Program Maintenance** screen, select **Repair**.

6. Click **Next.**

7. In the **Ready to Repair the Program** screen, click **Install**.

8. Follow the directions provided by the Windows install program.

Upgrading Existing Global Data Manager Installations

This section guides you through the steps necessary to upgrade prior versions of GDM to GDM 5.1.

Caution If GDM 4.5 for NetBackup 3.4 Servers is installed on NetBackup 3.4 master servers, you must first upgrade NetBackup 3.4 to NetBackup 5.1 before upgrading GDM. See the NetBackup 5.1 installation guides for more information.

Topics include:

"Upgrading to GDM 5.1" on page 27

"Upgrading to GDM 5.1 on UNIX" on page 27

"Upgrading to GDM 5.1 on Windows" on page 29

Upgrading to GDM 5.1

This section provides information on upgrading from any GDM 4.5 or 5.0 revision to GDM 5.1 on both the UNIX and Windows platforms.

Topics include:

"Upgrading to GDM 5.1 on UNIX" on page 27

"Upgrading to GDM 5.1 on Windows" on page 29

Upgrading to GDM 5.1 on UNIX

This section guides you through the steps required to successfully upgrade existing GDM 4.5 or 5.0 installations on NetBackup to GDM 5.1 on UNIX systems.

Requirements

- Before upgrading GDM, you must first upgrade your existing NetBackup system to NetBackup 5.1. Only after upgrading NetBackup to the 5.1 version can you upgrade to GDM 5.1.
- On Solaris systems, you must first do a `pkgrm` command to remove the GDM Solaris package. Answer `Y` when prompted, `Are you doing this pkgram as a step in an upgrade process?` *before* beginning the GDM 5.1 upgrade process.

▼ To upgrade to GDM 5.1 on UNIX systems

1. Log in as root on the server, where you want to upgrade to GDM 5.1.

   If you are already logged in, but are not the root user, execute the following command:

   ```
   su - root
   ```

2. On Solaris systems, execute the following:

   ```
   pkgrm VRTSnbgdm
   ```

   When prompted, answer Yes (`Y`) to the question, `Are you doing this pkgrm as a step in an upgrade process?`

3. Make sure a valid GDM license key (either GDM Server or GDM Managed Server) has been registered by entering the following command to list and add keys:

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

   For each GDM domain you are creating, make sure you specify only one host in that domain to have the GDM Server key. All other hosts should have the GDM Managed Server key.

4. Insert the CD-ROM containing the NetBackup Global Data Manager software in the drive.

5. Change your working directory to the CD-ROM directory:

   ```
   cd /<cd_rom_directory>
   ```

   where `cd_rom_directory` is the path to the directory where you can access the CD-ROM. On some platforms, it may be necessary to mount this directory.

6. To install NetBackup Global Data Manager, execute the following:

   ```
   ./install
   ```

   The install script begins.

   When finished, the GDM server software and the Java Dashboard software upgrade is complete.

Note The master server which acts as the GDM Server can itself be managed using the GDM Server key; you do not need to additionally register the GDM Managed Server key as well.

Upgrading to GDM 5.1 on Windows

Requirements

❖ Before upgrading GDM on NetBackup systems, you must first upgrade your existing NetBackup 4.5 or 5.0 system to NetBackup 5.1.

▼ Upgrading to GDM 5.1 on Windows systems

1. Move to the Windows computer where you want to upgrade to GDM 5.1.

2. Log on as administrator.

3. Insert the CD-ROM containing the NetBackup Global Data Manager 5.1 software in the drive.

4. From the Windows, click **Start** >**Run** and enter the following:

   ```
   <drive_letter>:\setup.exe
   ```

   where `drive_letter` is the letter of the CD-ROM drive where you can access the CD-ROM.

5. When the Installation wizard's **Welcome** screen appears, click **Next**.

6. Read and accept the license terms and then click **Next**.

7. Enter the pertinent information on the **Customer Information** screen and then click **Next**.

8. Select **Complete** and then click **Next**.

9. Click **Install** to begin the upgrade.

10. When the **InstallShield Wizard Completed** screen appears, click **Finished**.

    The GDM Server and the Windows Dashboard software upgrade is complete.

Uninstalling GDM from both UNIX and Windows

This section provides information for uninstalling GDM from UNIX and Windows systems.

See also:

"Uninstalling GDM 5.1 from UNIX Systems" on page 30

"Uninstalling GDM 5.1 From Windows Systems" on page 31

Uninstalling GDM 5.1 from UNIX Systems

▼ To uninstall Global Data Manager from a UNIX server

Note If you are uninstalling in a cluster environment, you must first freeze the active node so that migrations do not occur during the uninstall. For information about freezing a service group, see the clustering section in the *NetBackup High Availability System Administrator's Guide* for the cluster software you are running.

1. Log in as the root user on the master server.

   If you are already logged in, but are not the root user, execute the following command:

   ```
   su - root
   ```

2. Execute the uninstall command or script:

   On a Solaris server, type:

   ```
   pkgrm VRTSnbgdm
   ```

   When prompted, answer No (`N`) to the question, `Are you doing this pkgrm as a step in an upgrade process?`.

   On non-Solaris servers, type:

   ```
   <install_path>/netbackup/bin/install_gdm -deinstall
   ```

   where `<install_path>` is the directory in which NetBackup resides.

3. When the uninstall command or script finishes, the following temporary file may be created.

   ```
   <tmpdir>/VERITASgdm-db.tar.Z
   ```

   where `<tmpdir>` is the value of the TMPDIR environment variable at the time the install script is executed.

   If you are completely uninstalling GDM, delete this file.

If you are upgrading or reinstalling GDM, do not delete this file until *after* the installation has completed.

Note If you are uninstalling in a cluster environment, unfreeze the active node after the uninstall operation has been completed on all nodes. For information about unfreezing a service group, see the clustering section in the *NetBackup High Availability System Administrator's Guide* for the cluster software you are running.

Uninstalling GDM 5.1 From Windows Systems

To uninstall GDM 5.1 from Windows systems, use the following steps.

Caution If the NetBackup Java Administration Console and the GDM Java Dashboard are installed, and you want to uninstall the NetBackup Java Administration Console, you should uninstall the Java Dashboard first. Otherwise, the only way to uninstall the Java Dashboard will be to uninstall all of GDM using the **Remove** button in the Windows **Add/Remove Programs** applet.

If NetBackup or Backup Exec is installed, and later you want to uninstall, the GDM Server component should be uninstalled first. Otherwise, the only way to uninstall the GDM Server component will be to uninstall all of GDM using the **Remove** button in the Windows **Add/Remove Programs** applet.

▼ To remove GDM on Windows systems

1. If you are uninstalling GDM in a clustered environment, freeze the active node so that migrations do not occur while the inactive nodes are being modified. Uninstall GDM on the active node last. Refer to the clustering section in the *NetBackup High Availability System Administrator's Guide* that pertains to the type of cluster software you are running for more information on freezing a service group.

2. Log on as administrator.

3. Click **Start**>**Settings**>**Control Panel**>**Add/Remove Programs**.

4. Click **VERITAS Global Data Manager**.

5. Click **Remove**.

6. Click **Yes** when prompted.

   The Windows Installer begins the GDM uninstall process.

7. When finished, close **Add/Remove Programs**.

GDM Configuration 3

This section provides configuration details about GDM.

GDM Configuration includes the following topics:

Section	Description
"GDM Configuration Overview" on page 33	Provides GDM configuration details.
"Using GDM with Backup Exec Media Servers" on page 34	Provides a general overview on how to use GDM with Backup Exec media servers.
"Using GDM with Backup Exec Media Servers" on page 34	Provides steps for creating multiple GDM domains.
"Monitoring Other GDM Domains" on page 38	Provides steps for changing to a different GDM Server when using GDM Dashboard in a multi-GDM domain environment.

GDM Configuration Overview

This section guides you through the creation of a GDM domain. It also provides general information about GDM configuration parameters.

After completing the Global Data Manager installation, a GDM domain must be created before GDM becomes fully operational.

In addition, the GDM domain you create will use as the default, pre-defined configuration settings. The parameters that comprise this default configuration govern the sensitivity at which problems are flagged in the GDM Dashboard. It is recommended that the default be used; however they can be adjusted to meet your needs, or if Dashboard performance issues arise.

See also:

"Creating GDM Server Domains" on page 34

"Using GDM with Backup Exec Media Servers" on page 34

"Monitoring Other GDM Domains" on page 38

Using GDM with Backup Exec Media Servers

Administrators managing computing environments running both NetBackup and Backup Exec-based systems, can use GDM 5.1 to monitor, as GDM managed servers, Backup Exec media servers running Backup Exec versions 8.6, 9.0 and 9.1. In order to monitor these media servers, a NetBackup master server running the GDM 5.1 Server software must be present.

As an administrator overseeing a fully configured GDM Domain consisting of a licensed GDM Server running on a NetBackup 5.1 master computer, use the GDM CD-ROM to install the GDM software on each Backup Exec media server to be monitored. For more information see, "Installing the GDM Server Component on Windows Systems" on page 17.

After the installation completes, add the desired Backup Exec media server or servers to the GDM Domain using the GDM Managed Servers tab in the GDM Dashboard. For more information see, "Adding Servers to the GDM Domain" on page 35.

Note Installing the GDM software on Backup Exec media servers does not require a license key.

After you have added the Backup Exec media servers, they appear as managed servers in the GDM Dashboard.

Creating GDM Server Domains

A GDM domain is made up of a set of NetBackup master servers and Backup Exec media servers that are being managed by a GDM Server. After being added to the GDM domain, they are collectively known as managed servers.

Note The GDM Server by default is added to the GDM domain as a managed server when you initially create the domain.

GDM can effectively monitor a GDM domain consisting of an unlimited number of managed servers. The response of the system depends on network activity, concurrent backup activity, and the number of active Dashboards. If the performance of the system becomes an issue due to any of the above mentioned factors, it is recommended that you create multiple GDM domains, where each domain monitors up to 100 managed servers.

Use the following steps to create one or more GDM domains.

▼ To create a GDM domain and add managed servers

1. Ensure the visd daemon (UNIX) or the VERITAS GDM Information Server service (Windows) is running on the GDM Server. The visd daemon/VERITAS GDM Information Server service must be active in order to save configuration settings.

2. Start the GDM Windows Dashboard.

3. Connect to the GDM Server. If you are running GDM for the first time, choose **File** from the GDM menu bar and then select **Change GDM Server**.

4. Enter a GDM Server name, or enter its IP address. Use the default port number that appears in the **Port number** field.

5. Click **OK**.

See also:

"Adding Servers to the GDM Domain" on page 35

"Modifying Managed Server Properties in the GDM Domain" on page 36

"Removing a Managed Server from a GDM Domain" on page 37

Adding Servers to the GDM Domain

Use the following steps to add NetBackup master servers and Backup Exec media servers to the GDM domain.

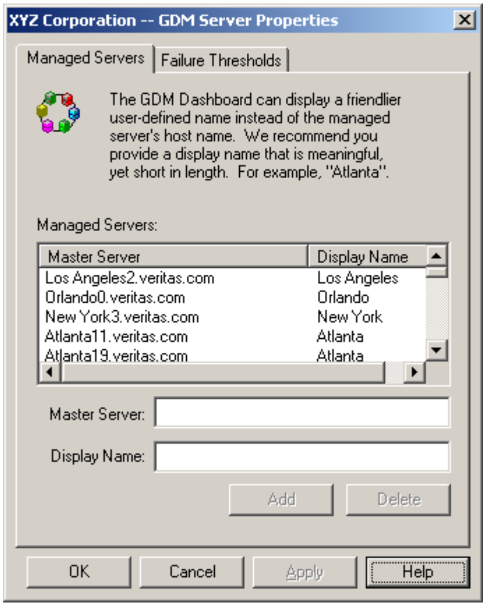
▼ To add servers

1. Choose **Edit** from the menu bar.

2. Click **General Properties**.

3. Click the **Managed Servers** tab.

GDM Server Properties Dialog Box



XYZ Corporation -- GDM Server Properties

The GDM Dashboard can display a friendlier user-defined name instead of the managed server's host name. We recommend you provide a display name that is meaningful, yet short in length. For example, "Atlanta".

Managed Servers:

Master Server	Display Name
Los Angeles2.veritas.com	Los Angeles
Orlando0.veritas.com	Orlando
New York3.veritas.com	New York
Atlanta11.veritas.com	Atlanta
Atlanta19.veritas.com	Atlanta

Master Server:

Display Name:

4. Add the fully-qualified domain name for each server such as Madrid.XYZ.com, and a friendly display name such as *Atlanta*.

5. Click **Add**.

6. Click **OK**.

   The newly added server now becomes a managed server and is added to the managed server list. It can be viewed in the left pane of the Dashboard.

See also:

"Modifying Managed Server Properties in the GDM Domain" on page 36

"Removing a Managed Server from a GDM Domain" on page 37

Modifying Managed Server Properties in the GDM Domain

You can make minor adjustments to the general properties of your managed servers in the GDM Server Properties dialog box.

For example, you can change the display name to something more useful to your administrators. The default display name for a managed server is the managed server's name.

▼ To make modifications

1. From the GDM menu bar, click **Edit**.
2. Click **General Properties**.
3. In the **Managed Servers** tab, click a server to modify.
4. Make the adjustments and then click **Change**.
5. Click **OK**.

See also:

"Adding Servers to the GDM Domain" on page 35

"Removing a Managed Server from a GDM Domain" on page 37

Removing a Managed Server from a GDM Domain

Use the following instructions to remove a managed server from the GDM domain.

▼ To remove a managed server from a GDM domain

1. From the GDM menu bar, choose **Edit**.
2. Click **General Properties**.

   The GDM Server Properties dialog appears.
3. Click the **Managed Servers** tab.
4. Click a managed server to remove and then click **Delete**.
5. Click **OK**.

   The selected managed server is removed from the GDM domain. It is also removed from the GDM Managed Servers pane.

See also:

"Adding Servers to the GDM Domain" on page 35

"Modifying Managed Server Properties in the GDM Domain" on page 36

Monitoring Other GDM Domains

If your environment is supporting multiple GDM domains, you may want to monitor the activity in any one of those domains. To do so, you will need to point the GDM Dashboard to the GDM Server in whose domain you want to monitor the activity of its NetBackup and Backup Exec managed servers.

▼ To change GDM Servers using the Windows Dashboard

1. From the menu bar, choose **File** and then select **Change GDM Server**.

Note If you want to change to a previously used GDM Server, click the list box on the **Change GDM Server** dialog box and then make a selection. Continue with step 4.

2. Enter a target GDM Server name, or its IP address.

3. In the **Port number** field, use the default port number provided, unless you changed the port number used by the GDM Server.

4. Click **OK**.

   GDM Dashboard connects to the specified GDM Server.

▼ To change GDM Servers using the Java Dashboard

1. From the menu bar, choose **File** and then select **Change GDM Server**.

Note If you want to change to a previously used GDM Server, click the name of an existing GDM Server that appears in the dialog box and continue with step 4.

2. Click **New** to add the name of the target managed server.

3. In the **Define a GDM Server** dialog box, enter the managed server name and IP address or DNS name. Use the default port address unless you changed the port number used by the GDM Server.

Note The managed server name you enter is for display only. As such, it can be any name that you want.

4. Click **OK**.

See also:

"Adding Servers to the GDM Domain" on page 35

“Modifying Managed Server Properties in the GDM Domain” on page 36

“Removing a Managed Server from a GDM Domain” on page 37

GDM Advanced Configuration 4

This section provides the information necessary to make advanced configuration adjustments to Global Data Manager.

Advanced Configuration includes the following topics:

Adjusting Configuration Parameters

This section provides information on adjusting configuration parameters for both *failure threshold* and *data collection* properties for GDM Dashboard.

Access to the Dashboard's configuration settings is unrestricted. Users with the remote administration client installed on their workstations can start the GDM Dashboard and connect remotely to a GDM Server. From there, the user can adjust configuration settings such as threshold levels, the list of managed servers, and data collection rates. Administrators should stress to all users having access to the NetBackup graphical interfaces on their systems that the GDM configuration settings apply globally, not just to their view.

See also:

"Adjusting Failure Thresholds" on page 42

"Adjusting GDM Data Collection Settings" on page 46

Adjusting Failure Thresholds

Problems within a GDM domain are flagged when conditions surpass threshold levels. Threshold levels exist in order to reduce the *noise* you might see if every potential problem was highlighted.

For example, you may deliberately down drives on media servers in order to keep the drives in reserve for emergency restores. For such situations, a downed drive does not represent a problem. However, if you have 10 drives and typically keep one down for emergency restores, then you can set a downed drive threshold level of 15% (in the **Value** field) in order to be alerted to unusual conditions .

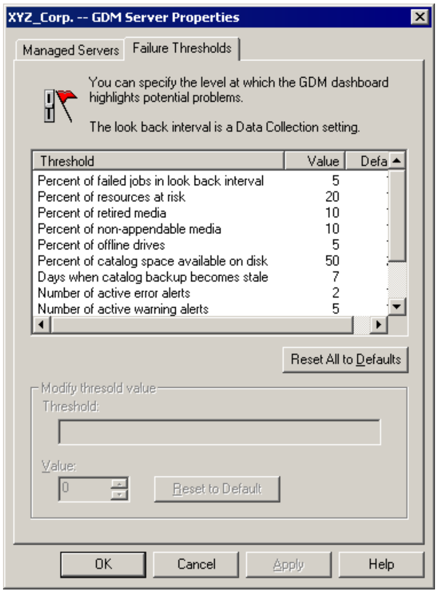
Some terms used in the failure threshold descriptions may be unfamiliar to you. For definitions of these terms, see the appendix, "Common Terminology" on page 147.

▼ To adjust the failure thresholds

1. From the GDM Dashboard menu, click **Edit** and then select **General Properties**.

2. Click the tab, **Failure Thresholds.**

GDM Server Failure Thresholds



XYZ_Corp. -- GDM Server Properties

You can specify the level at which the GDM dashboard highlights potential problems.

The look back interval is a Data Collection setting.

Threshold	Value	Defa
Percent of failed jobs in look back interval	5	
Percent of resources at risk	20	
Percent of retired media	10	
Percent of non-appendable media	10	
Percent of offline drives	5	
Percent of catalog space available on disk	50	
Days when catalog backup becomes stale	7	
Number of active error alerts	2	
Number of active warning alerts	5	

Modify thresold value

Threshold:

Value: 0

GDM Server Failure Threshold Options

Threshold	Definition
Percent of failed jobs in look back interval	Specifies point at which an alert flag is displayed for job failure. The threshold specifies the number of failed jobs, as a percentage, in the look back interval. If a threshold is reached, a red critical flag appears. Refer to “Adjusting the Look Back Interval” on page 47.
Percent of resources at risk	Specifies the point at which an alert flag is displayed for clients at risk for not being backed up. The threshold specifies the number of clients that failed on a percentage basis during the look back interval. If a threshold is reached, a yellow warning flag appears. **Note** This threshold applies only to NetBackup managed servers.
Percent of retired media	Specifies the point at which an alert flag is displayed for retired media. The threshold specifies the number of media on a percentage basis that have been set to a retired state. If a threshold is reached, a yellow warning flag appears.
Percent of Non-appendable media	Specifies the point at which an alert flag is displayed for non-appendable media. The threshold specifies the number of media on a percentage basis that are non-appendable. If a threshold is reached, a yellow warning flag appears.
Percent of offline drives	Specifies the point at which an alert flag is displayed for offline drives. The threshold specifies the number of drives on a percentage basis that are offline. If a threshold is reached, a yellow warning flag appears.
Percent of catalog space available on disk	Specifies the point at which an alert flag is displayed when a shortage of disk space occurs on the disk upon which the catalog resides. The threshold specifies the percentage of the current size of the catalog which should be available for future catalog growth. If a threshold is reached, a yellow warning flag appears. **Note** This threshold applies only to NetBackup managed servers.
Days when catalog backup becomes stale	Specifies the point at which an alert flag is displayed when a stale catalog backup is detected. The threshold specifies the number of days that have passed without the catalog having been backed up. If a threshold is reached, a yellow warning flag appears. **Note** This threshold applies only to NetBackup managed servers.

GDM Server Failure Threshold Options

Threshold	Definition
Number of active error alerts	Specifies the point at which an alert flag is displayed when active error alerts exceed a pre-determined number. **Number of active error alerts** does not have a maximum value that you can configure, but it does have a minimum of 0. Unlike the other failure threshold options, the value you set for this option is an absolute number, not a percentage. If a threshold is reached, a red critical flag appears.
Number of active warning alerts	Specifies the point at which an alert flag is displayed when warning error alerts exceed a pre-determined number. **Number of active warning alerts** does not have a maximum value that you can configure, but it does have a minimum of 0. Unlike the other failure threshold options, the value you set for this option is an absolute number, not a percentage. If a threshold is reached, a red critical flag appears.
Number of active attention alerts	Specifies the point at which an alert flag is displayed when attention error alerts exceed a pre-determined number. **Number of active attention alerts** does not have a maximum value that you can configure, but it does have a minimum of 0. Unlike the other failure threshold options, the value you set are for this option is an absolute number, not a percentage. If a threshold is reached, a red critical flag appears.
Number of active informational alerts	Specifies the point at which an alert flag is displayed when informational error alerts exceed a pre-determined number. **Number of active informational alerts** does not have a maximum value that you can configure, but it does have a minimum of 0. Unlike the other failure threshold options, the value you set are for this option is an absolute number, not a percentage. If a threshold is reached, a blue informational flag appears.

Note The event, **Required service has stopped or failed**, does not have an associated failure threshold. However, if a required service does stop or fail, a red critical flag appears.

3. Select a threshold to adjust and adjust the value in the **Value** field.

   Failure threshold values range from 0 to 100, with 0 representing the minimum and 100 representing the maximum. Setting a 0 value for a failure threshold will *always* cause a red flag condition to appear.

Note The maximum value that can be set for the failure threshold, **Days when catalog backup becomes stale**, is 60.

4. Click **Apply**.

5. Make adjustments to other threshold settings, if desired.

6. Click **OK**.

   Adjusted thresholds are then transferred to each managed server, which are then applied during the next scheduled scan of the server environments.

See also:

"Adjusting GDM Data Collection Settings" on page 46

Adjusting GDM Data Collection Settings

For the majority of GDM settings, the default values set during initial install will suffice for most environments. There may be situations however, where you want to alter how often the managed server environment is examined for backup activity.

Caution Changing data collection settings should be done with caution, as over adjustment of the monitoring settings can affect managed server performance.

See also:

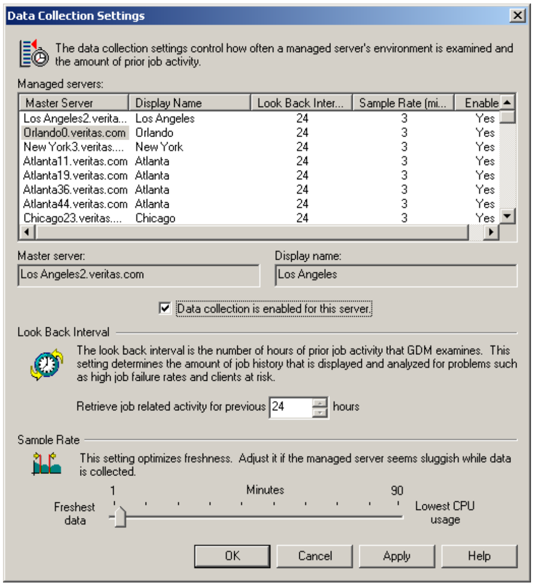
"Adjusting the Look Back Interval" on page 47

"Adjusting the Sample Rate" on page 48

"Disabling and Enabling Data Collection" on page 48

"Adjusting Configuration Parameters" on page 42

Data Collection Settings Dialog Box



Data Collection Settings

The data collection settings control how often a managed server's environment is examined and the amount of prior job activity.

Managed servers:

Master Server	Display Name	Look Back Inter...	Sample Rate (mi...	Enable
Los Angeles2.verita...	Los Angeles	24	3	Yes
Orlando0.veritas.com	Orlando	24	3	Yes
New York3.veritas....	New York	24	3	Yes
Atlanta11.veritas.com	Atlanta	24	3	Yes
Atlanta19.veritas.com	Atlanta	24	3	Yes
Atlanta36.veritas.com	Atlanta	24	3	Yes
Atlanta44.veritas.com	Atlanta	24	3	Yes
Chicago23.veritas....	Chicago	24	3	Yes

Master server: Los Angeles2.veritas.com

Display name: Los Angeles

☑ Data collection is enabled for this server.

Look Back Interval

The look back interval is the number of hours of prior job activity that GDM examines. This setting determines the amount of job history that is displayed and analyzed for problems such as high job failure rates and clients at risk.

Retrieve job related activity for previous 24 hours

Sample Rate

This setting optimizes freshness. Adjust it if the managed server seems sluggish while data is collected.

Adjusting the Look Back Interval

The number of hours of prior job activity that GDM examines is called the look back interval. By default, the look back interval is 24 hours.

When you run the GDM Dashboard for the first time, the previous 24 hours of job activity is displayed. In addition, problems such as high job failure rates or number of resources at risk due to failed backups are determined by examining the previous 24 hours worth of job activity.

▼ To change the look back interval

1. From the GDM Dashboard menu bar, click **Edit**.

2. Click **Data Collection**.

3. In the list of managed servers, select a managed server on which to adjust the look back interval.

4. Modify the look back interval by changing the hourly values in the **Retrieve job related activity for previous xx hours** field.

5. Click **Apply.**

6. Click **OK**.

Note The adjusted look back interval will be applied when the next scheduled scan of the managed server data is scanned.

Adjusting the Sample Rate

The sample rate governs how often a managed server backup environment is examined. It is the time between when data collection finishes and the next data collection cycle starts. By default, the sample rate is 3 minutes. Increasing the rate at which data is collected will result in fresher data, although there is an associated cost of more CPU processing power required to gather the data. You should select a rate that balances how soon you need to be alerted to problems with the amount of CPU being used by the managed server when data is collected. For example, you may need to know about failed jobs within 2 minutes, or you may decide 10 minutes is sufficient.

Caution Sample rate adjustments are done on a per managed server basis. It is not a global setting and does not apply to the entire GDM domain.

▼ To change the sample rate

1. From the GDM Dashboard menu bar, click **Edit**.

2. Select **Data Collection**.

3. In the list of managed servers, select a managed server on which to adjust the sample rate.

4. Move the slider bar to the setting you want.

5. Click **Apply**.

6. Repeat these steps to adjust the sample rate on additional managed servers, if necessary.

7. When finished, click **OK**.

Disabling and Enabling Data Collection

At some point, you may want to take a managed server offline temporarily. You can disable and then re-enable data collection efforts from a selected managed server using the **Data Collection Settings** dialog box.

Note By default, data collection is enabled for all newly configured managed servers.

▼ To disable data collection

1. From the GDM Dashboard menu bar, click **Edit**.
2. Click **Data Collection**.
3. In the list of managed servers, select a managed server on which to disable data collection.
4. Click the **Data collection is enabled for this server** check box.
5. Click **Apply**.
6. Repeat these steps to disable data collection on additional managed servers.
7. When you are finished, click **OK**.

▼ To enable data collection

1. From the GDM Dashboard menu bar, click **Edit**.
2. Click **Data Collection**.
3. In the list of managed servers, select a server on which to enable data collection.
4. Click the **Data collection is enabled for this server** check box.
5. Click **Apply**.
6. Repeat these steps to enable data collection on additional managed servers.
7. When you are finished, click **OK**.

Adjusting the Dashboard Port Window

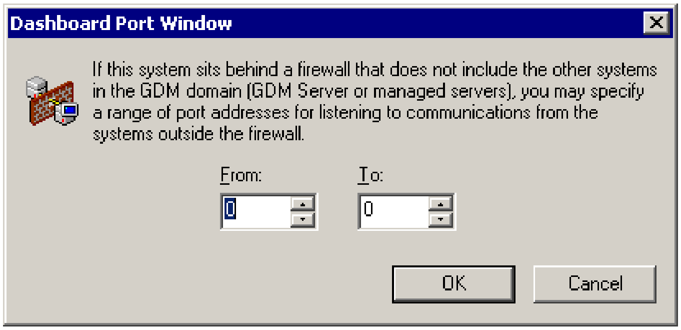
If your GDM Server resides behind a firewall, and the firewall does not include other GDM Servers or managed servers in the GDM domain, you can specify a range of port or Dashboard addresses for listening to communications from GDM Servers, or managed servers that reside outside the firewall.

Note The option **Dashboard Port** appears if you are using the GDM Dashboard on a computer that does not have NetBackup installed. If NetBackup is installed, the port addresses are modified in the NetBackup Administration Console.

▼ To adjust the Dashboard port addresses

1. From the **Edit** menu, click **Dashboard Port**.

Dashboard Port Window - Windows Dashboard



Dashboard Port Window

If this system sits behind a firewall that does not include the other systems in the GDM domain (GDM Server or managed servers), you may specify a range of port addresses for listening to communications from the systems outside the firewall.

From: 0

To: 0

2. Enter the port address ranges in the **From** and **To** fields.

3. Click **OK**.

4. Close and restart the Dashboard.

See also:

"Using GDM with Firewalls" on page 52

"Modifying Dashboard Host Port Assignments for Firewall Operations" on page 54

"Adjusting Configuration Parameters" on page 42

Managing a GDM Domain

GDM is most effective when it is used for monitoring a large number of backup servers from a single NetBackup master server. This is called a GDM domain. A GDM domain consists of one GDM Server and a number of managed servers. Any computer running NetBackup can be configured as a GDM Server. NetBackup master servers, Backup Exec 8.6 media servers, or Backup Exec 9.0/9.1 media servers can be added to the GDM Domain as managed servers.

The version of NetBackup on the GDM server must be the most recent version of all versions of NetBackup servers running on managed servers in that domain.

The GDM Dashboard contains a GDM Server Properties dialog box for configuring a list of managed servers on a GDM Server. The list of managed servers is stored on the GDM Server for the GDM domain.

From the GDM Dashboard click **Edit** > **General Properties** and select the **Managed Servers** tab. Managed servers can be added, deleted or changed using this dialog.

Note Any GDM Dashboard user can change the managed server list. If two users change the same list simultaneously it is likely that changes made by one user will be lost or overwritten. It is recommended that only one user change the managed server list.

A GDM managed server may be used in the managed server list of one or more GDM server but a GDM Server cannot be used as a managed server under another GDM Server.

When splitting one large GDM domain into two or more domains you may have to promote a managed server into a GDM Server. Before doing this remove the GDM managed server that you want to promote from the managed server list of all GDM Servers. Then use the Dashboard to add managed servers to its managed server list by using the **GDM Server Properties** dialog box.

See also:

"Using GDM with Backup Exec Media Servers" on page 34

"Adding Servers to the GDM Domain" on page 35

"Modifying Managed Server Properties in the GDM Domain" on page 36

"Removing a Managed Server from a GDM Domain" on page 37

"Using GDM with Firewalls" on page 52

"Enabling GDM Logging" on page 62

Using GDM with Firewalls

Global Data Manager can be used in environments that implement firewall protection. However, because firewalls affect system communications between a GDM Server computer and any GDM Dashboard computers that reside outside the firewall environment, special port requirements must be considered when configuring GDM for use with firewalls.

Firewall security is best maintained by ensuring that the configuration of the firewall server. To achieve this, the configuration must be as simple as possible. For example, the more packet-filtering rules that are defined, the harder it is to ensure a safe configuration.

GDM has been designed using the following guidelines in order to be used in a firewall environment.

- The number of different ports used for receiving incoming connections has been kept to a minimum. This reduces the number of ports that must be opened in a packet filter or the number of *plugs* that must be configured.
- The use of *ad-hoc* ports for receiving incoming connections is not supported. GDM selects a port for use from a range of ports specified by the firewall administrator in order to support multiple numbers of active, listening Dashboard-specific connections.
- The ports that are opened on the GDM Server and the managed servers always have a well-known, active listener.

See also:

"Firewall Scenarios" on page 58

"Scenario 1 - Single firewall environments" on page 58

"Scenario 2 - Dual firewall environments separating the Dashboard and GDM Server" on page 59

"Scenario 3 - Dual firewalls with Dashboard running on two terminals" on page 60

"Scenario 4 - Dual firewalls separating the GDM Server and a GDM Managed Server" on page 61

GDM Ports

The GDM Dashboard, GDM Server, and GDM managed servers communicate using ports on the Dashboard system and on the server systems.

The GDM Server and the GDM managed servers use a static port address known as the VERITAS Information Server Daemon (visd).

The GDM Dashboard's port addresses are dynamically assigned.

See also:

"GDM Server Port and GDM Managed Server Port (visd)" on page 53

"GDM Dashboard Port" on page 53

"Modifying Dashboard Host Port Assignments for Firewall Operations" on page 54

"Modifying Port Addresses On NetBackup Hosts" on page 55

"Modifying Port Addresses on Non-NetBackup Hosts" on page 56

GDM Server Port and GDM Managed Server Port (visd)

The static port address assigned to the *visd* port is: 9284; visd is the port on which the GDM Server and GDM managed servers listen for incoming communication. This port is specified in a system configuration file that is located in `/etc/services` under UNIX and `%systemroot%\system32\drivers\etc\services` under Windows NT and Windows 2000.

Note *visd* port configuration in the `services` file under both UNIX and Windows NT/2000 is configured automatically during installation.

GDM Dashboard Port

The GDM Dashboard computers require a port on which to listen for communications from the GDM Server.

Dynamically-assigned ports are assigned, as needed, from a range of port addresses that are specified on the Dashboard host. The range of addresses is used to support instances of the Dashboard running on multiple terminals from a single Dashboard host computer within a firewall.

Available Port Addresses

Determining an acceptable range of firewall port addresses is determined by you, the firewall administrator, based on your firewall environment. Keep in mind that the range of addresses specified must at least equal the number of Dashboard instances you want to run. This requirement ensures that each Dashboard instance finds an available firewall port address to use when connecting to a GDM Server.

Modifying Dashboard Host Port Assignments for Firewall Operations

If you must enable outgoing ports in a firewall, you should increase your port address ranges to support outgoing communications from the GDM Server to the Dashboard client computer.

When the Dashboard hosts searches for an available port address, it randomly selects an address from those available in a specified range.

Note If you decide to run multiple instances of the Dashboard, the range of addresses specified must at least equal the number of Dashboard instances you want to run. This requirement ensures that each Dashboard instance finds an available firewall port address to use when connecting to a GDM Server.

Dashboard host port assignments are modified using the NetBackup 5.1 interface when the Dashboard host is also a NetBackup master server. When the Dashboard host is not a NetBackup master server, the Dashboards provide a mechanism for configuring the range of ports.

See also:

"Modifying Dashboard Port Address Ranges" on page 54.

"Modifying Port Addresses On NetBackup Hosts" on page 55

"Modifying Port Addresses on Non-NetBackup Hosts" on page 56

Modifying Dashboard Port Address Ranges

This section provides information on modifying the GDM port address ranges for host computers running NetBackup. It also provides information on port address modification for those hosts not running NetBackup.

See also:

"GDM Dashboard Port"

"Modifying Port Addresses On NetBackup Hosts"

"Modifying Port Addresses on Non-NetBackup Hosts"

Modifying Port Addresses On NetBackup Hosts

If NetBackup is installed on the host computer, use the following steps to modify the port address ranges.

▼ To modify the port address range on hosts running NetBackup

1. For each Dashboard host, start NetBackup 5.1 on the host's master server.

2. In the left pane, double-click **Host Properties**.

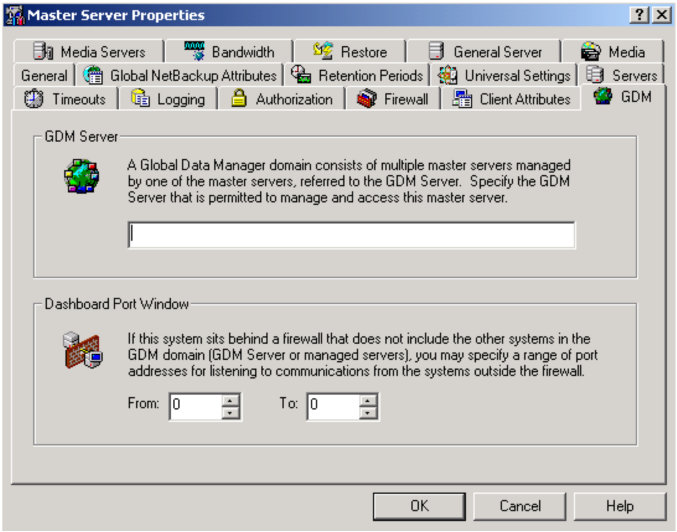
   - If the Dashboard host being modified is a master server, double-click **master Servers**.
   - If the Dashboard host being modified is a media server, double-click **Media Servers**.
   - If the Dashboard host being modified is a client computer, double-click **Clients**.

3. In the right pane, right-click the computer for which you want to modify the port and select **Properties**.

4. Click **GDM**.

5. Under **Dashboard Port Window**, enter a range of port addresses in the **From** and **To** fields.

Port Range Modification Dialog Box - Dashboard Port Window



A Global Data Manager domain consists of multiple master servers managed by one of the master servers, referred to the GDM Server. Specify the GDM Server that is permitted to manage and access this master server.

If this system sits behind a firewall that does not include the other systems in the GDM domain (GDM Server or managed servers), you may specify a range of port addresses for listening to communications from the systems outside the firewall.

From: 0 To: 0

Note The Port Range Modification screen is available in the Windows or Java versions of the NetBackup Administration Console.

6. Click **OK**.

   Close and restart all Dashboard interfaces running on the system.

Modifying Port Addresses on Non-NetBackup Hosts

Note If NetBackup is not installed on the host computer, the NetBackup Administration Console cannot be used to modify host's port address configuration.

If NetBackup is not installed on the Dashboard host computer, use the following steps to modify the port address ranges.

▼ If you are using the Java version of the Dashboard on Windows

Note To make port address modifications, you must manually edit the file, gdm.conf, which is found in the `C:\Program Files\VERITAS\java` directory.

1. Open the file, `gdm.conf`.

2. Edit the entry, `DASHBOARD_PORT_WINDOW=`
   If the entry does not exist, create the entry.

3. Add the desired port ranges using the following format:

   `DASHBOARD_PORT_WINDOW= n m`, where `n` is the first port range and `m` is the last.

Caution `DASHBOARD_PORT_WINDOW= 0 0` creates an unrestricted port window.

4. Save the gdm.conf file and then close and restart all Dashboard interfaces running on the host computer.

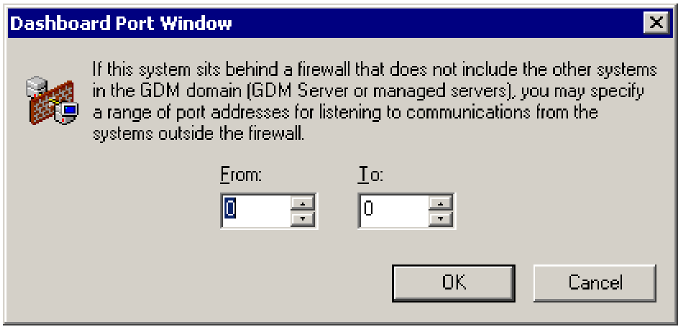
▼ If you are using the Windows version of the Dashboard

1. Start the Dashboard.

2. From the **Edit** menu, click **Dashboard Port Window**.

Note The option, **Dashboard Port Window**, is not available on Dashboard interfaces running on hosts where NetBackup is installed.

Dashboard Port Window Dialog Box - Windows Dashboard



Dashboard Port Window

If this system sits behind a firewall that does not include the other systems in the GDM domain (GDM Server or managed servers), you may specify a range of port addresses for listening to communications from the systems outside the firewall.

From: 0

To: 0

3. Enter a range of port addresses in the **From** and **To** fields.

Caution Entering a range of **0 0** creates an unrestricted port window.

4. Click **OK**.

5. Close and restart all Dashboard interfaces running on the host computer.

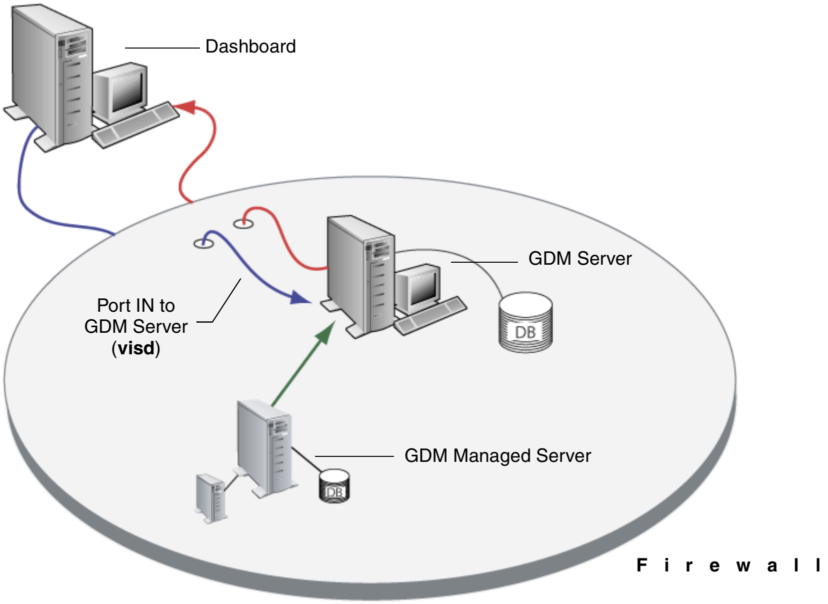
Firewall Scenarios

Four popular firewall environment scenarios are considered when GDM installation through a firewall is required. These include:

- "Scenario 1 - Single firewall environments" on page 58
- "Scenario 2 - Dual firewall environments separating the Dashboard and GDM Server" on page 59
- "Scenario 3 - Dual firewalls with Dashboard running on two terminals" on page 60
- "Scenario 4 - Dual firewalls separating the GDM Server and a GDM Managed Server" on page 61

Scenario 1 - Single firewall environments

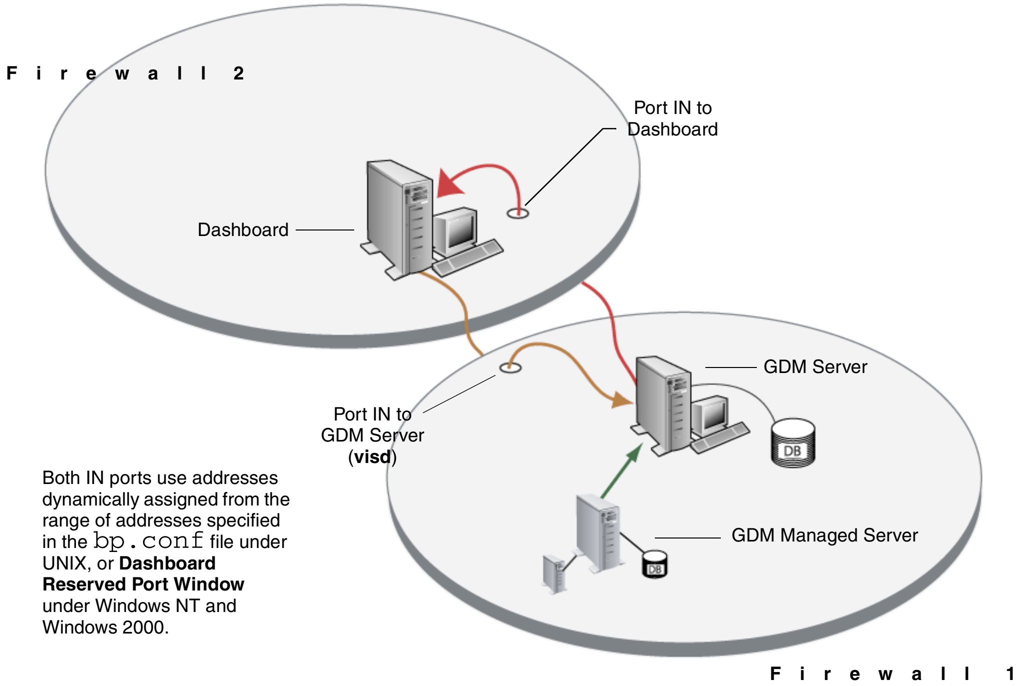
This scenario reflects an environment where a single firewall is used to enclose the GDM Server and all managed servers, while the GDM Dashboard resides outside the firewall-protected environment.



Note Only the visd port must be opened. The Dashboard port range can be unrestricted.

Scenario 2 - Dual firewall environments separating the Dashboard and GDM Server

This scenario reflects an environment where one firewall is used to enclose the GDM Server and all managed servers, while the GDM Dashboard resides inside a second firewall-protected environment.



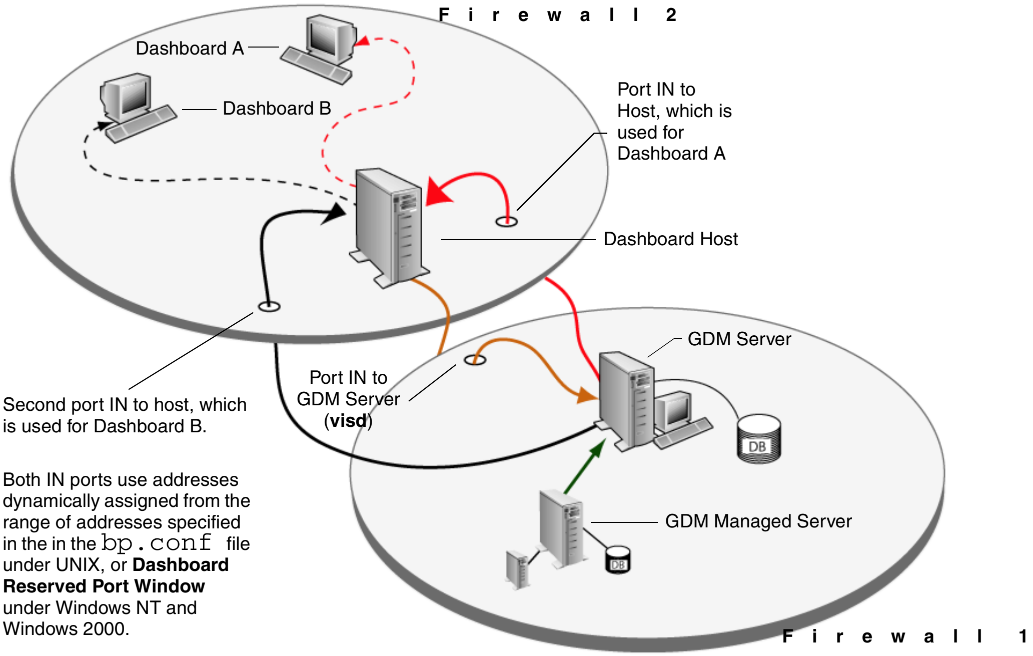
Both IN ports use addresses dynamically assigned from the range of addresses specified in the `bp.conf` file under UNIX, or **Dashboard Reserved Port Window** under Windows NT and Windows 2000.

visd port configuration in the `services` file under both UNIX, and Windows NT and Windows 2000 is configured automatically during installation.

Note The visd port must be opened in Firewall 1 and the Dashboard port in Firewall 2.

Scenario 3 - Dual firewalls with Dashboard running on two terminals

This scenario reflects an environment where two firewalls are is used to enclose the GDM Server and all managed servers, while the GDM Dashboard runs on two terminals inside a second firewall-protected environment.

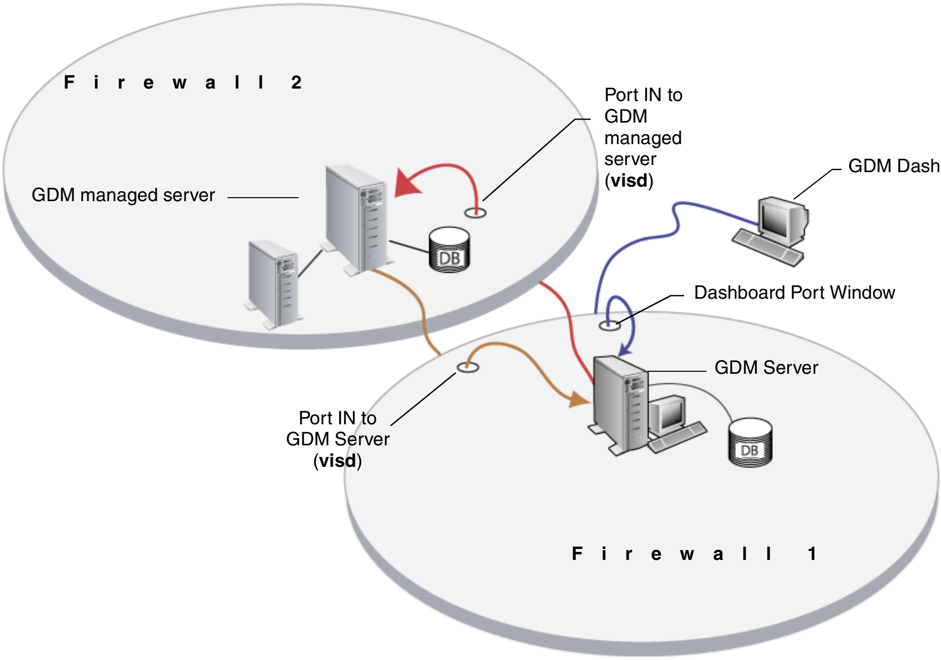

Firewall 2
Dashboard A
Dashboard B
Port IN to Host, which is used for Dashboard A
Dashboard Host
GDM Server
DB
Port IN to GDM Server (visd)
Second port IN to host, which is used for Dashboard B.
Both IN ports use addresses dynamically assigned from the range of addresses specified in the in the bp.conf file under UNIX, or **Dashboard Reserved Port Window** under Windows NT and Windows 2000.
GDM Managed Server
DB
Firewall 1

`visd` port configuration in the services file under both UNIX, and Windows NT and Windows 2000 is configured automatically during installation.

Note If you decide to run multiple instances of the Dashboard, the range of specified firewall port addresses must at least equal the number of Dashboard instances you want to run. This ensures that each Dashboard instance finds an available firewall port address to use when connecting to a GDM Server.

Scenario 4 - Dual firewalls separating the GDM Server and a GDM Managed Server

This scenario reflects an environment where the GDM Server and a GDM managed server reside behind separate firewalls.



visd port configuration in the `services` file under both UNIX, and Windows NT and Windows 2000 is configured automatically during installation.

Caution The range of port addresses specified for the Dashboard Port Window must be equal to or greater than the number of Dashboard instances running on the Dashboard host.

Enabling GDM Logging

You can enable GDM logging on GDM Servers or GDM managed servers by creating log file directories as follows:

On a NetBackup managed server:

```
<install-directory>/netbackup/logs/..
```

On a Backup Exec managed server:

```
<install-directory>\GDM\logs\
```

The visd daemon or the VERITAS GDM Information Server service needs to be stopped and restarted afterwards creating the directories.

See also:

"Creating the GDM Log Directories" on page 63

"Enabling Dashboard Logs" on page 64

"Adjusting the Amount of Detail in the Data Collector Log File" on page 66

"Adjusting the Amount of Detail in other GDM Log Files" on page 67

GDM Log Notes

- Each GDM component has its own debug log directory.

  There are many GDM log file directories, and each correlates to a component within the GDM system. Having multiple log files makes it easier for you to diagnose a problem.

- Debug logging is only in affect for a component if the debug log directory for the component is defined.

  One debug log file is created per component per day. The file names created are of the form:

  log.<mmddyy>

  For example, *log.110891*

- The log files in these directories are automatically pruned by the NetBackup request daemon, `bprd`. The administrative parameter keep logs x days determines how long the log files exist.

Note When GDM runs on hosts that are not running NetBackup, automatic log pruning does not occur.

Additional information on changing the **keep logs x days** parameter can be found in the *NetBackup 5.1 System Administrator's Guide*.

Caution Some of these logs can become very large and can use up large amounts of hard drive space. They should be enabled only if problems exist.

Creating the GDM Log Directories

▼ To create the log directories

1. Create the following directories under the appropriate log directory as described in "Enabling GDM Logging":

   Note Log directories with asterisks (*) are more likely to contain answers to common problems. Those log files are the ones you should view first.

```
gdm_visd*
gdm_collector*
gdm_mastmon*
gdm_psodbc*
gdm_gdmblm
gdm_objcat
gdm_licenseblm
gdm_chgevt
gdm_heartbeat
gdm_becollector
```

2. After creating the previous directories, create another set under the `gdm_gdmblm` directory with the following names:

```
RobotSummary
JobManager
ServiceManager
MonitoredServer
Configuration
LicenseBO
DriveManager
MediaManager
MasterServerSummary
HeartbeatBO
ProblemThreshold
alerts
```

3. Stop and restart the visd daemon or the VERITAS GDM Information Server service after creating the directories.

   Most of the GDM modules, except for the data collector module, support one level of debug logging. By creating the log files, you get the detailed logging of messages. Varying the verbosity levels of logging for modules like the data collector requires changing the module's Parameters value. To get a more verbose level of logging for data collection, you can adjust the the **Parameters** value for the data collector.

See also:

"Adjusting the Amount of Detail in the Data Collector Log File" on page 66.

"Adjusting the Amount of Detail in other GDM Log Files" on page 67

Enabling Dashboard Logs

In addition to capturing log output on the GDM Server systems, you can also enable logging on the GDM client systems - the machines where you run the Dashboard interface.

▼ To enable the Windows Dashboard logging on Windows

1. Open a command prompt and change directories to the directory where GDM is installed.

   For example, `c:\Program Files\VERITAS\GDM\bin`

2. At the prompt start GDM with the log option.

   ```
   gdm -log
   ```

   Debug output is directed to log files in the **gdmui** directory.

   For example, all log file output can be found in
   <drive letter>:\Program Files\VERITAS\GDM\Logs\gdmui

   When creating and naming the log file, GDM uses the format `gdm_yyyymmdd_x.log`. where `x` indicates a sequential number for that day starting with 1.

   For example, `gdm_2001OCT23_2.log` reflects that GDM has run twice on Oct. 23, 2001.

Message A unique log file is created for each secondary Dashboard window that you open. For example, if you open 5 additional windows, Dashboard creates 5 log files.

```
gdm_2001OCT23_1.log
gdm_2001OCT23_2.log
gdm_2001OCT23_3.log
gdm_2001OCT23_4.log
gdm_2001OCT23_5.log
```

If you close and then reopen multiple secondary Dashboard windows again on the same day, GDM increments the numbering of additional logs by one.

```
gdm_2001OCT23_6.log
gdm_2001OCT23_7.log
gdm_2001OCT23_8.log
gdm_2001OCT23_9.log
gdm_2001OCT23_10.log
```

▼ To enable more verbose Dashboard logging on UNIX

❖ Start the Java version of the Dashboard by starting the GDM start-up script with the logging option.

```
$ gdmSA --debug
```

Debug output is directed to the file displayed in initial lines of the output.

For example:

```
The log file for this execution instance is
/usr/openv/java/logs/root.gdmSA.15953.log
```

Adjusting the Amount of Detail in the Data Collector Log File

Unlike other GDM-produced log files, you can adjust the parameters that are used to set the amount of detail (verbosity) you can see in the log file produced for the data collector (gdm_collector). The level of detail that can be seen is adjustable. It is based on a scale of 1 - 5, with 1 being the least amount of detail and 5 being the most.

Caution Because of the potentially large amount of disk space required, full verbosity for logging (- verbose 5) should only be activated for debugging purposes. After debug efforts are complete, disable logging or reconfigure the verbosity level to provide less detail.

Use the following steps to adjust the detail level.

▼ Adjusting the Parameters value on UNIX

❖ On UNIX, add the line “Parameters”=”-verbose 5” beneath the data collector section in the `/usr/openv/var/visd.conf` file.

The following example shows you where to insert the line and how it should look. Five levels of verbosity are available. The example shows a value of 5, which is the most verbose setting providing full details. Other values are 1, 2, 3, and 4, each providing less detail.

[Infoserver\VTHost\Modules\collector]

```
”FileName”=”/usr/openv/lib/libcollector.so”
“Parameters”=”-verbose 5”
```

▼ Adjusting the Parameters value on Windows

1. On Windows NT/2000, edit the registry.

2. Find the key:

   [HKEY_LOCAL_MACHINE]\[SOFTWARE]\[VERITAS]\[Infoserver\VTHost\Modules\collector]\Parameters

3. Set the value of Parameters to **-verbose 1** to get basic output. Use **-verbose 2** to get more detail, and so on. Finally, use **-verbose 5** to get full details.

Adjusting the Amount of Detail in other GDM Log Files

As with the Data Collector, you can adjust the level of details that appear in the log files of other GDM modules.

Use the following steps to adjust the detail level.

▼ Adjusting the parameters on UNIX

1. On UNIX, add the line `“Parameters”=”-stime 60 -verbose 5”` beneath the heartbeat section in the `/usr/openv/var/visd.conf` file.

2. Add the line `“Parameters”=”-verbose 5”` beneath the chgevt section.

   The following example shows you where to insert the lines and how they should look.

```
[Infoserver\VTHost\Modules\chgevt]
“FileName”=”/usr/openv/lib/libchgevt”
“Parameters”=”-verbose 5”

[Infoserver\VTHost\Modules\heartbeat]
“Filename”=”/usr/openv/lib/libheartbeat”
“Parameters”=”-stime 60 -verbose 5”
```

▼ Setting the Parameters value on Windows

1. On Windows NT/2000, find the chgevt key:

   HKEY_LOCAL_MACHINE]\[SOFTWARE]\[VERITAS]\[Infoserver\VTHost\Modules\chgevt]

2. Add a new string value called **Parameters** and then set the value of Parameters in the Value data field to -sleep 60 -verbose 5**.**

3. Find the heartbeat key:

   HKEY_LOCAL_MACHINE]\[SOFTWARE]\[VERITAS]\[Infoserver\VTHost\Modules\heartbeat]

4. Add a new string value called Parameters and then set the value of Parameters in the Value data field to -stime 60 -verbose 5.

5. Close the registry.

Using GDM on a Windows Server with Multiple Network Interfaces

A NetBackup server with more than one network interface defined may not work properly with GDM when using the default configuration.

A GDM Server or a GDM managed server can have more than one network interface, although they must be forced to use the same network interface to communicate with each other. The hostnames of the servers are used to set up the default GDM configuration.

The configuration parameter `EndPoints` specifies the network interface for the GDM Server to use.

On Windows NT/2000 computers it is defined as a registry entry:

```
HKEY_LOCAL_MACHINE|SOFTWARE|VERITAS|InfoServer|VTHost|Profiles|Def
ault
```

For example, suppose *hosta* is a UNIX GDM server with one network interface and *hostb* is a GDM managed server on a Windows NT/2000 computer. *Hostb* has two network interfaces, *hostb* for GDM communication and *hostb_other* for other communications.

Knowing that network interfaces can be assigned different IP addresses, assume *hostb* is assigned IP address 10.20.30.40 and *hostb_other* is assigned IP address 190.186.32.10.

To force the GDM managed server to use *hostb* (or its equivalent IP address 10.20.30.40) to communicate with the GDM server, specify 10.20.30.40 as the value for the `EndPoints` configuration parameter in the registry entry on your Windows NT/2000 computer.

Using GDM 5

This section provides information on using GDM.

Using GDM includes the following topics:

Section	Description
"Starting the GDM Dashboard" on page 70	Describes how to start Global Data Manager.
"Understanding the GDM Dashboard" on page 72	Describes how GDM works and its use of visual keys within the graphical user interface.
"Introducing the GDM Dashboard" on page 81	Describes the GDM Dashboard and the various components that comprise the interface.
"Viewing Modes" on page 82	Describes the Summary and Detail viewing modes available in GDM.
"Defining, Editing, and Deleting Filters" on page 102	Describes the use of creating, modifying and deleting customized filters in GDM.
"Administering the Managed Servers" on page 109	Describes how to start the both the NetBackup and Backup Exec administration consoles from within GDM.

Starting the GDM Dashboard

Use the following steps to start the GDM Dashboard on Windows-based or UNIX-based platforms.

▼ On Windows-based platforms

1. From the Windows Taskbar, click **Start**.

2. Point to **Programs** > **VERITAS Global Data Manager** and then click **VERITAS Global Data Manager** or **VERITAS Global Data Manager - Java** if you installed the Java version of the Windows Dashboard.

   The GDM Dashboard starts and the **Connect to GDM Server** dialog box appears.

3. Enter a GDM Server in which to connect.

   The first time you initialize the GDM Dashboard, a **Connect to Server** dialog box appears; you must select a GDM Server in which to connect. After making the initial connection, the GDM Dashboard will automatically find and connect to the selected GDM Server when subsequent sessions of the Dashboard are run.

▼ On UNIX-based platforms

1. Log in as root on the NetBackup system where you are going to start the GDM Dashboard.

2. Start the Dashboard by executing the following:

```
/usr/openv/java/gdmSA &
```

Note The GDM Java Dashboard supports remote X Windows display only between Solaris systems. For example, assume you are on a Solaris system named tiger and the Java Dashboard is on a Solaris system named shark. On tiger, you can display the interface by performing an `rlogin` to shark and executing `gdmSA -d tiger`. However, if shark were an HP system, you could only display `jnbSA` only directly on shark.

Setting Up The Window Manager

Under UNIX, it is recommended that you set your window manager to activate windows only when you click within the windows. It is also recommended that you do not enable auto focus; auto focus occurs when windows become active after the mouse pointer is moved over them. The GDM Java Dashboard does not run properly with auto focus enabled. The following are general instructions for correctly configuring the focus on a CDE (Common Desktop Environment) window manager, which is the preferred window manager for the Java Dashboard.

▼ To prepare a CDE (Common Desktop Environment) for the Administration Console

1. On the front panel in the CDE window, click the **Style Manager** control icon.

2. On the Style Manager toolbar, click the **Window** control icon.

3. In the Style Manager-Window dialog box, click the **Click In Window To Make Active** button.

4. Click **OK**.

5. Click **OK** when prompted to **Restart the Workspace Manager**.

Understanding the GDM Dashboard

This section explains the GDM Dashboard and the various components that comprise the interface.

Note Because GDM Dashboard is designed for use on both UNIX-based and Windows-based platforms, slight discrepancies in the look-and-feel of the Dashboard interface may exist. These variations will be noted in the manual when they are encountered.

Understanding the GDM Visual Keys

To help you understand the information being presented, the GDM Dashboard uses visual keys. These keys include color, status flags, icons, tool tips, and font styles.

Color

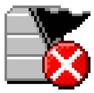
The colors red, yellow, and blue are used when conditions exist that should be investigated.

- Red represents a critical condition, in which data threatening issues exist. Critical conditions should be investigated as soon as possible.
- Yellow represents a warning condition, in which possible data threatening issues exist. Warning conditions should be investigated as soon as possible.
- Blue indicates an activity condition exists, in which some sort of activity is occurring at your managed servers. Blue conditions can be examined at your discretion.

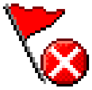
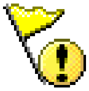
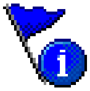
Status Flags

Status flags icons are also used in conjunction with the GDM color scheme. Each flag represents critical, warning, or informational conditions that mirror the conditions represented with the use of color. Status flag icons include:

Available Status Flags

Status Flag	Description
	*Server Unreachable* - This icon represents a NetBackup or Backup Exec managed server that GDM is unable to communicate with. Server Unreachable icons indicate a severe status condition has occurred and should be given your highest priority when they appear.

Available Status Flags (continued)

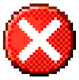
Status Flag	Description
	*Critical Flags* - This status flag represents an error condition or conditions that must be investigated as soon as possible. Critical flags contain an X, which indicates serious data threatening issues at the managed server. The color red is associated with this type of flag.
	*Warning Flags* - This status flag represents a condition that is deemed a problem, yet is not considered to be critical. Warning flags contain an exclamation mark and are usually associated with the color yellow.
	*Informational Flags* - This status flag represents events that are of interest but are not necessarily problems. Information flags contain a lower case "i" and are associated with the color blue.

Icons

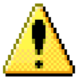
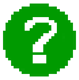
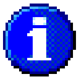
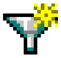
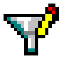
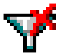
Along with status flags, icons are used throughout the Dashboard interface to help you quickly determine the status of a particular area of interest in your GDM domain.

Dashboard icons include:

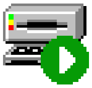
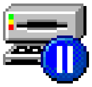
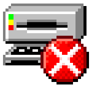
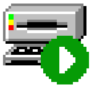
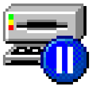
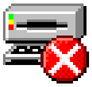
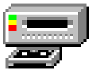
Available GDM Icons

Icon	Description
Alerts Detail Section (Backup Exec only)	If alerts are generated by Backup Exec, they appear in the GDM Alerts detail section. The Alerts detail section only appears in the right pane after you select a Backup Exec managed server in the left pane.
 Error Alert	For Backup Exec managed servers only. Error alerts are generated when system, job, media and device error occur. Error alerts are severe and require prompt user intervention. *Job Cancellation* is an example of an error alert.

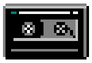
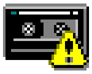
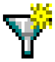
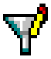
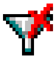
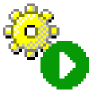
Available GDM Icons (continued)

Icon	Description
 Warning Alert	(Backup Exec managed servers only) Warning alerts are generated when system, job, media and warning alerts occur. Warning alerts should be addressed in a timely manner. *Job Completed with Exceptions* is an example of a warning alert.
 Attention Alert	For Backup Exec managed servers only. Attention alerts are generated when system, job, media and device attention messages occur. *Media Insert* is an example of an attention alert.
 Informational Alert	For Backup Exec managed servers only. Informational alerts are generated when system, job, media and device informational messages occurs. *Service Start* is an example of an informational alert.
 Define Filter	Represents the Define Filter feature. Filters can be defined, allowing you a view GDM data based on your preferences. For more information, see "Defining, Editing, and Deleting Filters" on page 102.
 Edit Filter	Represents the Edit Filter feature. After defining a filter, you can use this feature to modify the parameters of your user-defined filter. For more information, see "Defining, Editing, and Deleting Filters" on page 102.
 Delete Filter	Represents the Delete Filter feature. Using this feature enables you to delete user-defined filters. For more information, see "Defining, Editing, and Deleting Filters" on page 102.

Available GDM Icons (continued)

Icon		Description
Robot Detail Section		
	Drive Active	Represents a robot drive that is actively processing jobs.
	Drive Paused	Represents a robot drive that been placed in a paused state.
	Drive Offline	Represents a robot drive that is offline.
Standalone Drives Detail Section		
	Drive Active	Represents a standalone drive that is actively processing jobs.
	Drive Paused	Represents a standalone drive that has been placed in a paused state.
	Drive Down	Represents a standalone drive that is down and not functioning properly.
	Drive is Available	Represents a standalone drive that is available and is ready to process jobs.

Available GDM Icons (continued)

Icon	Description
Media Detail Section	
 Catalog Conditions	Represents media where conditions exist. This icon appears when the following media conditions exist: ◆ The media has been imported. ◆ The media contains catalog data. ◆ A catalog error has occurred.
 Media Warning	Represents media where the following conditions exist: ◆ The media is full. ◆ The media has been retired. ◆ The media is full.
 Define Filter	Represents the Define Filter feature. Filters can be defined, allowing you a view GDM data based on your preferences. For more information, see “Defining, Editing, and Deleting Filters” on page 102.
 Edit Filter	Represents the Edit Filter feature. After defining a filter, you can use this feature to modify the parameters of your user-defined filter. For more information, see “Defining, Editing, and Deleting Filters” on page 102.
 Delete Filter	Represents the Delete Filter feature. Using this feature enables you to delete user-defined filters. For more information, see “Defining, Editing, and Deleting Filters” on page 102.
Services Detail Section	
 Active	Represents a service that is active. The color green is used to indicate an active state. For example, under Services in the right pane, Active icons are used to indicate that services such as the NetBackup Client Service are running.

Available GDM Icons (continued)

Icon	Description
⚙⏸ Inactive	Represents an inactive service. A service is considered inactive if it is not running, and it is not required to be running. For example, if a NetBackup master server has a storage device attached, the Device Daemon service normally should be running. However, if a storage device is not attached, the service is normally inactive.
⚙✖ Failed	Represents a failed service. A service is considered failed if it normally should be running, but is not.
⚙? Unknown	Represents a service with an unknown status due to the managed server being unreachable.
Jobs Detail Section	These icons are typically found in the Jobs detail section.
▶ Active Job	Represents a job that is being actively processed.
■ Cancelled Job	Represents a job that has been cancelled.
✓ Finished Job - Successful	Represents a job that has finished successfully. Using the color blue, this icon represents a job that has had no failures.
! Finished Job - Partially Successful	Using the color yellow, this icon represents a job that has finished but for some reason, not all files could be backed up.
✖ Finished Job - Failed	Using the color red, this icon indicates a job that has finished but has failed.

Available GDM Icons (continued)

Icon	Description
⛔ Incomplete Job	Represents a job that is incomplete.
⏸ On Hold Job	Represents a job that has been placed on hold.
⏭ Queued or Requeued Job	Represents a queued or requeued job, which indicates a job is queued and ready to be processed.
Scheduled Job	Represents a scheduled job, which indicates a job has been scheduled for processing sometime in the future.
⏸ Suspended Job	Represents a suspended job.
Define Filter	Represents the Define Filter feature. Filters can be defined, allowing you a view GDM data based on your preferences. For more information, see “Defining, Editing, and Deleting Filters” on page 102.
Edit Filter	Represents the Edit Filter feature. After defining a filter, you can use this feature to modify the parameters of your user-defined filter. For more information, see “Defining, Editing, and Deleting Filters” on page 102.
Delete Filter	Represents the Delete Filter feature. Using this feature enables you to delete user-defined filters. For more information, see “Defining, Editing, and Deleting Filters” on page 102.

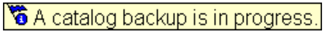
Available GDM Icons (continued)

Icon	Description
Report Icons	
Problem Report	This icon presents the Problems report, which shows a list of managed servers, on which problems are detected. For more information, see "Problem Report" on page 136.
Drive Status Report	This icon represents the Drive Status report, which shows the status of drives on each of the managed servers (and their media servers) being monitored by GDM. For more information, see "Drive Status Report" on page 137.
General Status Report	This icon represents the General Status report, which shows various totals and data points for each managed server being monitored by GDM. For more information, see "General Status Report" on page 138.

ToolTips

ToolTips provide brief descriptions of the visual keys that appear in the left pane when GDM detects a condition at a managed server.

Example of a ToolTip



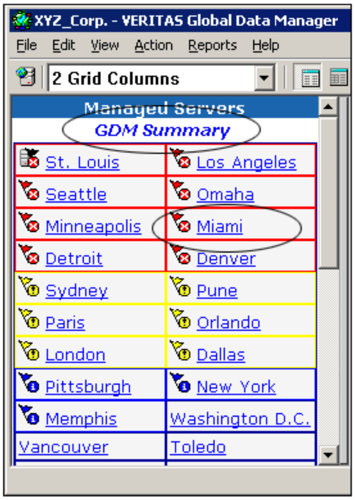
A catalog backup is in progress.

A ToolTip appears a second or so after stopping the mouse over a managed server name where a condition appears. They are also available in the right pane, for each robot LED Drive Status graphic found in the Robot detail sections.

Font Attribute Enhancements

GDM also makes use of italicized and bold font faces when the selection of managed servers is made in the left pane. After clicking a managed server name, the font of the selected managed server changes to a bold and italicized face, showing you the managed server actively being monitored.

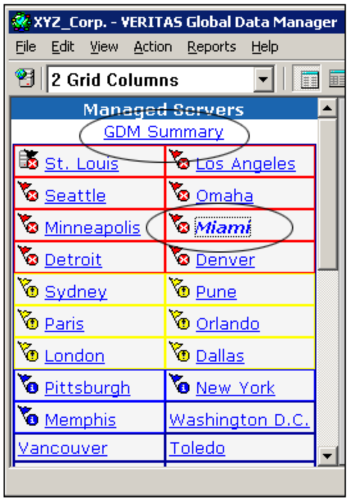
Text Enhancements


XYZ_Corp. - VERITAS Global Data Manager
File Edit View Action Reports Help
2 Grid Columns
Managed Servers

GDM Summary

St. Louis	Los Angeles
Seattle	Omaha
Minneapolis	Miami
Detroit	Denver
Sydney	Pune
Paris	Orlando
London	Dallas
Pittsburgh	New York
Memphis	Washington D.C.
Vancouver	Toledo

Before a managed server is selected


XYZ_Corp. - VERITAS Global Data Manager
File Edit View Action Reports Help
2 Grid Columns
Managed Servers

GDM Summary

St. Louis	Los Angeles
Seattle	Omaha
Minneapolis	Miami
Detroit	Denver
Sydney	Pune
Paris	Orlando
London	Dallas
Pittsburgh	New York
Memphis	Washington D.C.
Vancouver	Toledo

After a managed server is selected

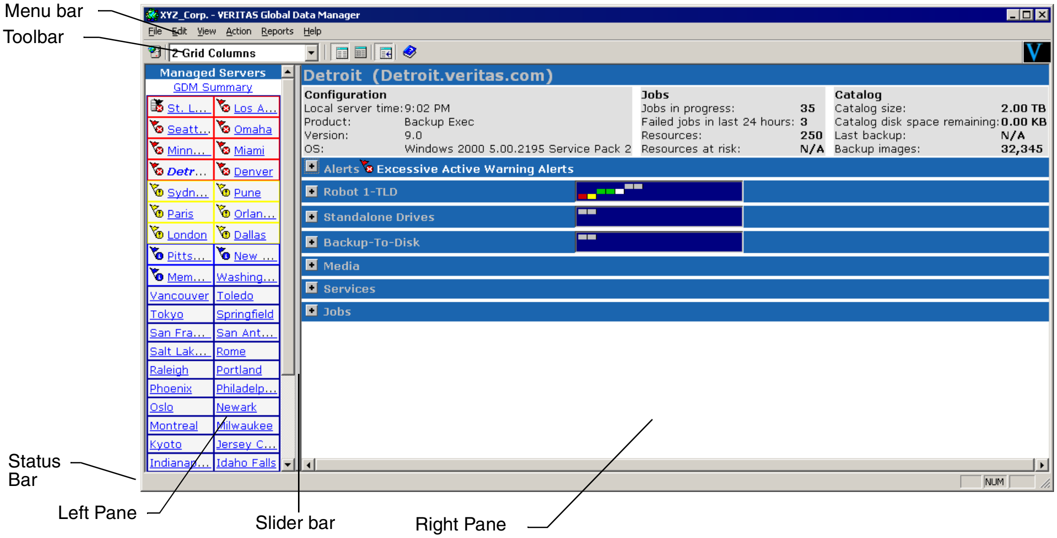
Introducing the GDM Dashboard

The GDM Dashboard consists of multiple interface components. These components include resizable *left* and *right* panes that are used to present the information gathered from each of the managed servers being monitored. In between the left and right panes is a movable splitter bar, which can be used to resize the individual panes.

In addition, GDM Dashboard also uses a *Menu bar* and a *Toolbar*, which allow you to make modifications to the way information is presented.

At the bottom of the GDM interface is a *status bar*, which displays the name of a managed server when you mouse over one in the left pane. It also displays general operational messages pertaining to your GDM managed servers.

GDM Dashboard - Windows version



St. L...	Los A...
Seatt...	Omaha
Minn...	Miami
Detr...	Denver
Sydn...	Pune
Paris	Orlan...
London	Dallas
Pitts...	New ...
Mem...	Washing...
Vancouver	Toledo
Tokyo	Springfield
San Fra...	San Ant...
Salt Lak...	Rome
Raleigh	Portland
Phoenix	Philadelp...
Oslo	Newark
Montreal	Milwaukee
Kyoto	Jersey C...
Indianap...	Idaho Falls

Detroit (Detroit.veritas.com)

Configuration		Jobs		Catalog	
Local server time:	9:02 PM	Jobs in progress:	35	Catalog size:	2.00 TB
Product:	Backup Exec	Failed jobs in last 24 hours:	3	Catalog disk space remaining:	0.00 KB
Version:	9.0	Resources:	250	Last backup:	N/A
OS:	Windows 2000 5.00.2195 Service Pack 2	Resources at risk:	N/A	Backup images:	32,345

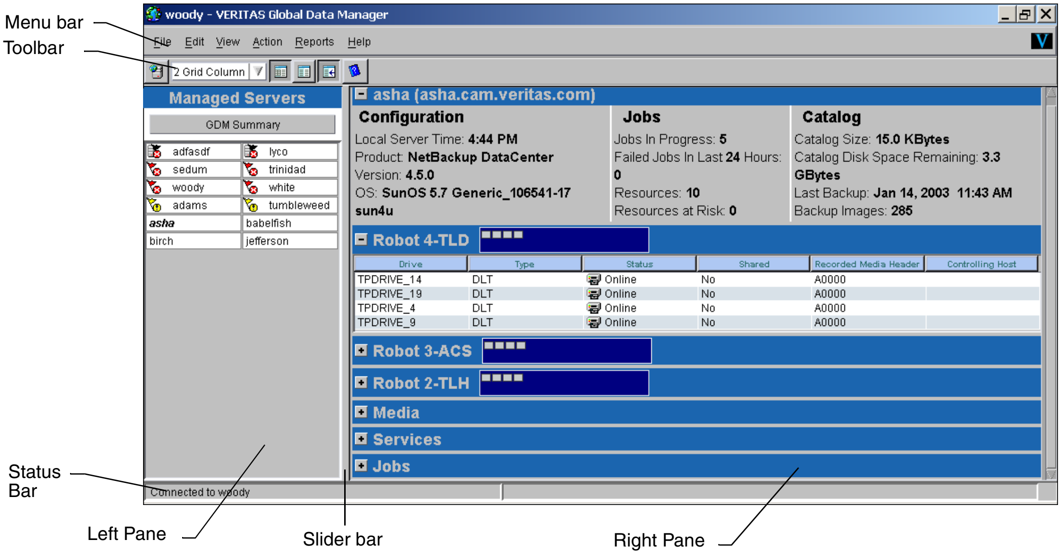
Alerts Excessive Active Warning Alerts

See also:

"GDM Menu Bar" on page 124

"GDM Toolbar" on page 129

GDM Dashboard - Java version



asha (asha.cam.veritas.com)

Configuration
Local Server Time: **4:44 PM**
Product: **NetBackup DataCenter**
Version: **4.5.0**
OS: **SunOS 5.7 Generic_106541-17 sun4u**

Jobs
Jobs In Progress: **5**
Failed Jobs In Last **24** Hours: **0**
Resources: **10**
Resources at Risk: **0**

Catalog
Catalog Size: **15.0 KBytes**
Catalog Disk Space Remaining: **3.3 GBytes**
Last Backup: **Jan 14, 2003 11:43 AM**
Backup Images: **285**

Robot 4-TLD

Drive	Type	Status	Shared	Recorded Media Header	Controlling Host
TPDRIVE_14	DLT	Online	No	A0000	
TPDRIVE_19	DLT	Online	No	A0000	
TPDRIVE_4	DLT	Online	No	A0000	
TPDRIVE_9	DLT	Online	No	A0000	

Viewing Modes

GDM Dashboard presents information in two viewing modes: *Summary* and *Detail*.

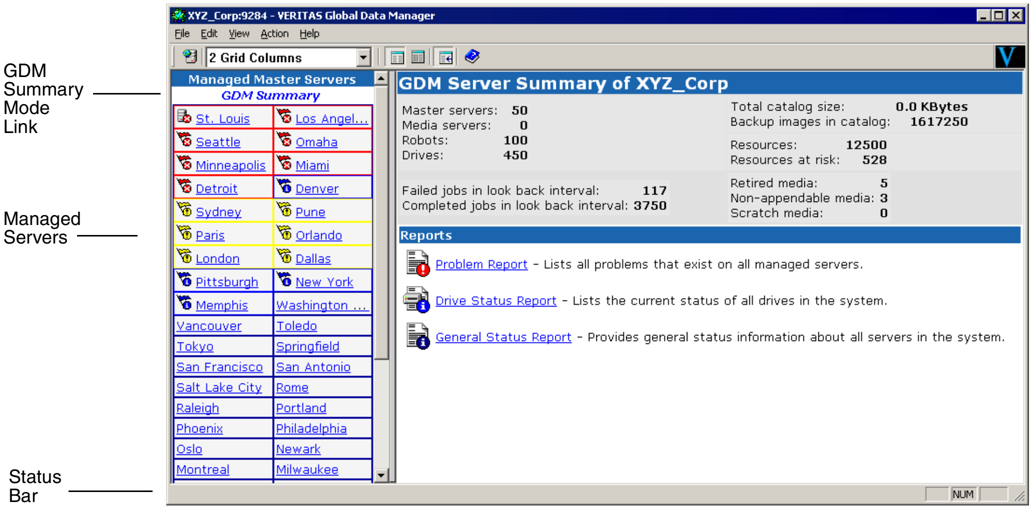
Summary Mode

The first type of viewing mode the Dashboard provides is called *Summary mode*. Summary mode provides an overview of the entire GDM domain the GDM Server to which you are connected is monitoring. In Summary mode, you can quickly determine the overall status of your operation using a single window.

Summary mode appears as the default mode when the GDM Dashboard first starts. After moving around the interface during a GDM session, you can use the *GDM Summary* link to quickly return to GDM’s Summary mode from any location in the Dashboard.

The *left pane* of GDM Summary mode contains the M*anaged Server* list. This list displays all managed servers that are being monitored by the GDM Server to which you are connected. Managed servers with issues display an event status flag to the left of the server name. In the Windows Dashboard only, a colored border is used to highlight the managed server where events are identified.

GDM Summary Mode - Windows Dashboard



St. Louis	Los Angel...
Seattle	Omaha
Minneapolis	Miami
Detroit	Denver
Sydney	Pune
Paris	Orlando
London	Dallas
Pittsburgh	New York
Memphis	Washington ...
Vancouver	Toledo
Tokyo	Springfield
San Francisco	San Antonio
Salt Lake City	Rome
Raleigh	Portland
Phoenix	Philadelphia
Oslo	Newark
Montreal	Milwaukee

GDM Server Summary of XYZ_Corp

Master servers:	50	Total catalog size:	0.0 KBytes
Media servers:	0	Backup images in catalog:	1617250
Robots:	100	Resources:	12500
Drives:	450	Resources at risk:	528
Failed jobs in look back interval:	117	Retired media:	5
Completed jobs in look back interval:	3750	Non-appendable media:	3
		Scratch media:	0

Reports

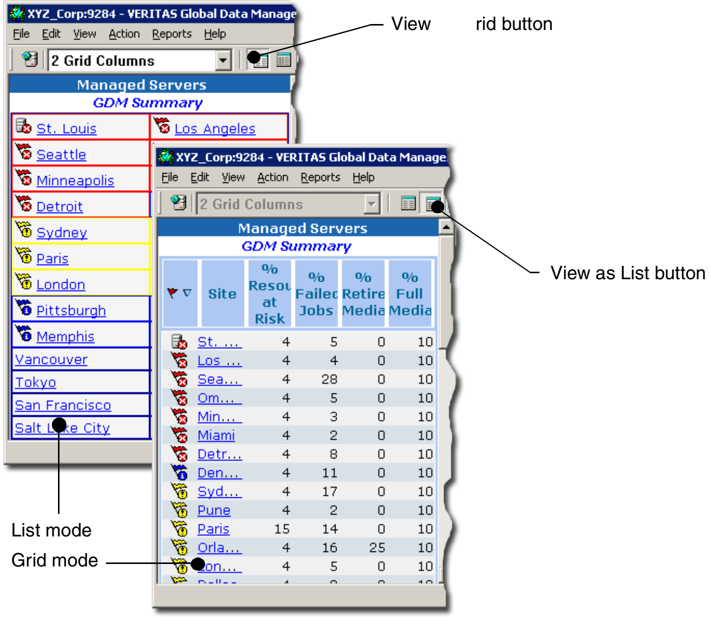
Problem Report - Lists all problems that exist on all managed servers.

Drive Status Report - Lists the current status of all drives in the system.

General Status Report - Provides general status information about all servers in the system.

You can view these servers either in a list format or a grid format, depending on the toolbar button selected.

GDM Dashboard List mode and Grid mode - Windows Dashboard



St. Louis
Seattle
Minneapolis
Detroit
Sydney
Paris
London
Pittsburgh
Memphis
Vancouver
Tokyo
San Francisco
Salt Lake City

Los Angeles

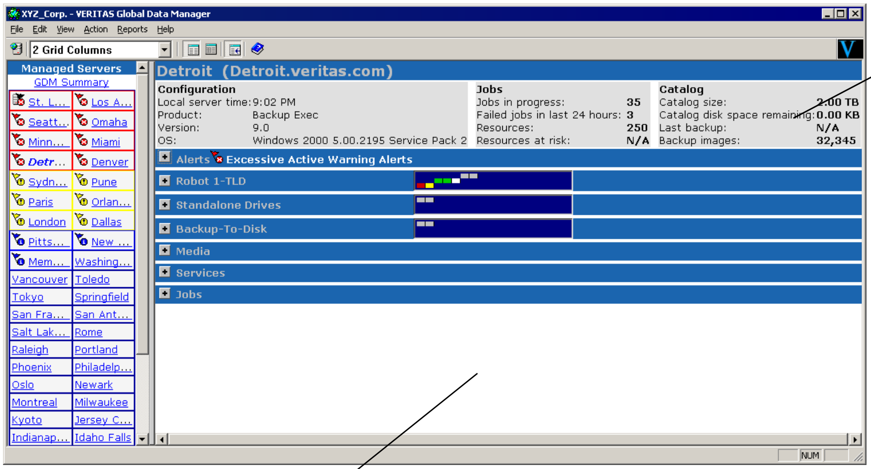
	Site	% Resou at Risk	% Failec Jobs	% Retire Media	% Full Media
	St. ...	4	5	0	10
	Los ...	4	4	0	10
	Sea...	4	28	0	10
	Om...	4	5	0	10
	Min...	4	3	0	10
	Miami	4	2	0	10
	Detr...	4	8	0	10
	Den...	4	11	0	10
	Syd...	4	17	0	10
	Pune	4	2	0	10
	Paris	15	14	0	10
	Orla...	4	16	25	10
	Lon...	4	5	0	10

The *right pane* of GDM Summary mode displays a complete, state-of-health view of the managed server environment being monitoring.

See also:

"GDM Toolbar" on page 129

Right Pane of the GDM Dashboard Summary View - Windows Dashboard



Managed Servers	
St. L...	Los A...
Seatt...	Omaha
Minn...	Miami
Detr...	Denver
Sydn...	Pune
Paris	Orlan...
London	Dallas
Pitts...	New ...
Mem...	Washing...
Vancouver	Toledo
Tokyo	Springfield
San Fra...	San Ant...
Salt Lak...	Rome
Raleigh	Portland
Phoenix	Philadelp...
Oslo	Newark
Montreal	Milwaukee
Kyoto	Jersey C...
Indianap...	Idaho Falls

Detroit (Detroit.veritas.com)

Configuration
Local server time: 9:02 PM
Product: Backup Exec
Version: 9.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: N/A

Catalog
Catalog size: 2.00 TB
Catalog disk space remaining: 0.00 KB
Last backup: N/A
Backup images: 32,345

Alerts Excessive Active Warning Alerts

GDM Server summary view

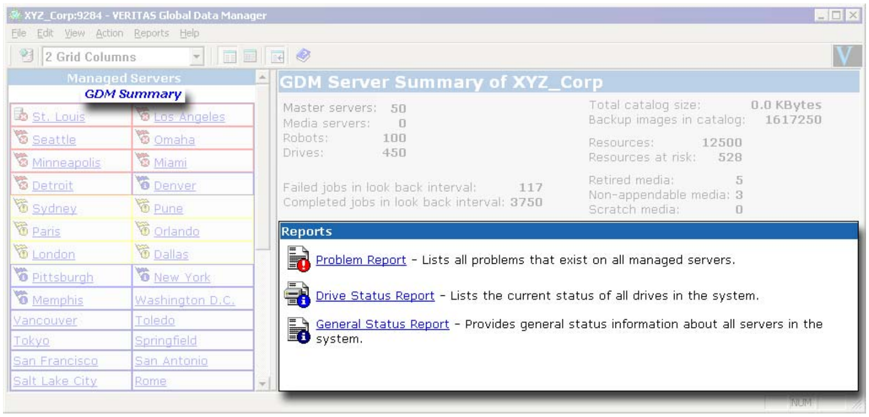
Reports summary view

Summary Mode - Reports

In Summary view, Dashboard's right pane also contains a Reports view. Located in the lower quadrant of the right pane, the Reports view offers you hypertext links to the following reports:

- *Problem Report* - This report lists problems that exist on all managed servers.
- *Drive Status Report* - This report lists the current status of all drives in the system.
- *General Status Report* - This report provides general status information about all servers in the system.

GDM Summary Mode - Reports - Windows Dashboard



GDM Server Summary of XYZ_Corp

Master servers:	50	Total catalog size:	0.0 KBytes
Media servers:	0	Backup images in catalog:	1617250
Robots:	100	Resources:	12500
Drives:	450	Resources at risk:	528
Failed jobs in look back interval:	117	Retired media:	5
Completed jobs in look back interval:	3750	Non-appendable media:	3
		Scratch media:	0

Reports

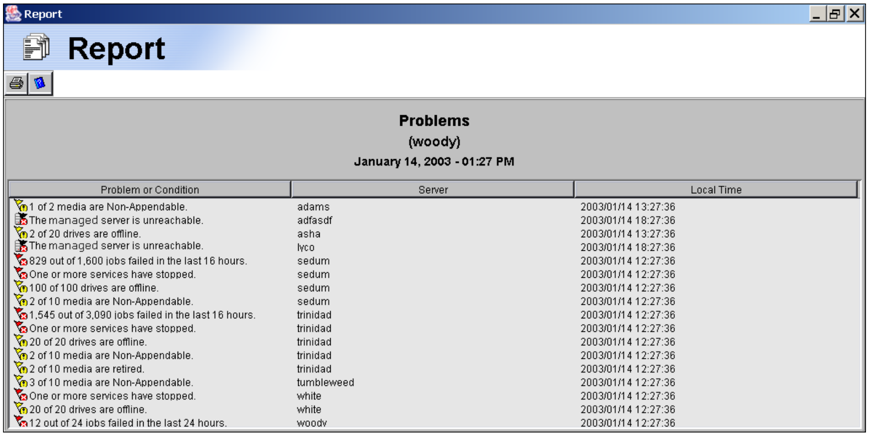
Problem Report - Lists all problems that exist on all managed servers.

Drive Status Report - Lists the current status of all drives in the system.

General Status Report - Provides general status information about all servers in the system.

Clicking a report link launches a secondary window that displays the selected report.

GDM Report Example - Java Dashboard



Problems
(woody)
January 14, 2003 - 01:27 PM

Problem or Condition	Server	Local Time
1 of 2 media are Non-Appendable.	adams	2003/01/14 13:27:36
The managed server is unreachable.	adfasdf	2003/01/14 18:27:36
2 of 20 drives are offline.	asha	2003/01/14 13:27:36
The managed server is unreachable.	lyco	2003/01/14 18:27:36
829 out of 1,600 jobs failed in the last 16 hours.	sedum	2003/01/14 12:27:36
One or more services have stopped.	sedum	2003/01/14 12:27:36
100 of 100 drives are offline.	sedum	2003/01/14 12:27:36
2 of 10 media are Non-Appendable.	sedum	2003/01/14 12:27:36
1,545 out of 3,090 jobs failed in the last 16 hours.	trinidad	2003/01/14 12:27:36
One or more services have stopped.	trinidad	2003/01/14 12:27:36
20 of 20 drives are offline.	trinidad	2003/01/14 12:27:36
2 of 10 media are Non-Appendable.	trinidad	2003/01/14 12:27:36
2 of 10 media are retired.	trinidad	2003/01/14 12:27:36
3 of 10 media are Non-Appendable.	tumbleweed	2003/01/14 12:27:36
One or more services have stopped.	white	2003/01/14 12:27:36
20 of 20 drives are offline.	white	2003/01/14 12:27:36
12 out of 24 jobs failed in the last 24 hours.	woody	2003/01/14 12:27:36

Dashboard reports can also be accessed using the Dashboard menu bar under **Reports**.

See also:

"GDM Reports" on page 133.

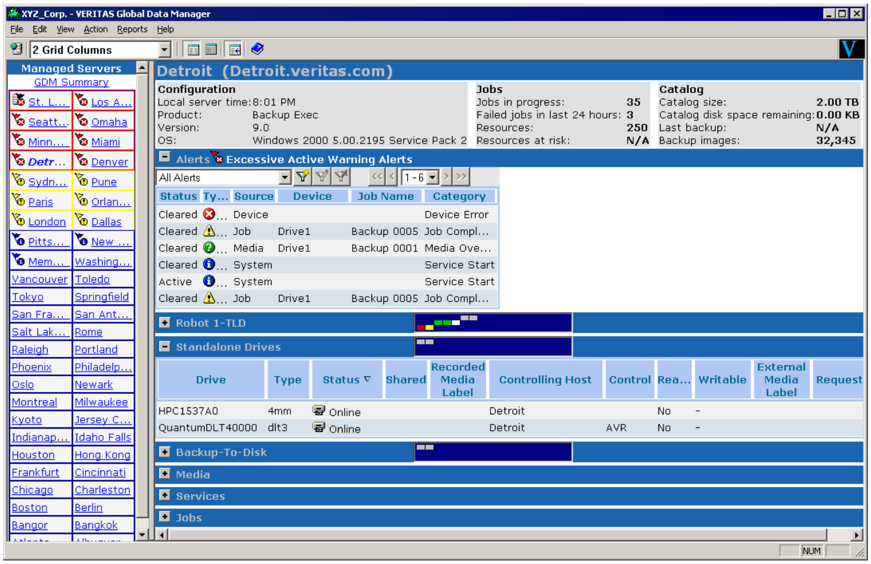
Detail Mode

The Dashboard provides a second type of viewing mode called the *Detail mode*. Detail mode enables you to see detailed information for any of the individual managed servers listed in the left pane.

In Detail mode, the Dashboard's right pane shows the following information:

- Summary details for the selected managed server.
- Alerts information for all Backup Exec media servers being monitored. (Backup Exec managed servers only)
- Robot information for all robots installed at the managed server.
- Daemon or services status information for NetBackup or Backup Exec managed servers.
- Job status information for all jobs being processed by the managed server.
- Media status information for all media used by the managed server.

GDM Detail Mode - Windows Dashboard



Detroit (Detroit.veritas.com)

Configuration
Local server time: 8:01 PM
Product: Backup Exec
Version: 9.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: N/A

Catalog
Catalog size: 2.00 TB
Catalog disk space remaining: 0.00 KB
Last backup: N/A
Backup images: 32,345

Alerts Excessive Active Warning Alerts

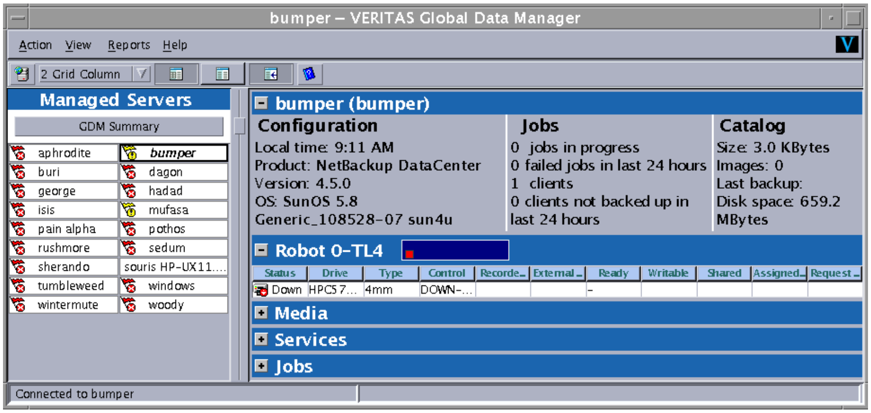
All Alerts 1 - 6

Status	Ty...	Source	Device	Job Name	Category
Cleared	...	Device			Device Error
Cleared	...	Job	Drive1	Backup 0005	Job Compl...
Cleared	...	Media	Drive1	Backup 0001	Media Ove...
Cleared	...	System			Service Start
Active	...	System			Service Start
Cleared	...	Job	Drive1	Backup 0005	Job Compl...

Standalone Drives

Drive	Type	Status	Shared	Recorded Media Label	Controlling Host	Control	Rea...	Writable	External Media Label	Request
HPC1537A0	4mm	Online			Detroit		No	-		
QuantumDLT40000	dlt3	Online			Detroit	AVR	No	-		

GDM Detail Mode - Java Dashboard



Managed Servers

GDM Summary

aphrodite	*bumper*
buri	dagon
george	hadad
isis	mufasa
pain alpha	pothos
rushmore	sedum
sherando	souris HP-UX11....
tumbleweed	windows
wintermute	woody

bumper (bumper)

Configuration	Jobs	Catalog
Local time: 9:11 AM Product: NetBackup DataCenter Version: 4.5.0 OS: SunOS 5.8 Generic_108528-07 sun4u	0 jobs in progress 0 failed jobs in last 24 hours 1 clients 0 clients not backed up in last 24 hours	Size: 3.0 KBytes Images: 0 Last backup: Disk space: 659.2 MBytes

Robot 0-TL4

Status	Drive	Type	Control	Recorde...	External ...	Ready	Writable	Shared	Assigned...	Request ...
Down	HPC57...	4mm	DOWN-...			–				

Media

Services

Jobs

Connected to bumper

To select Detail mode, click a managed server in the left pane.

After selecting a managed server, the name of the selected server changes from a normal font to an italicized font, reflecting the currently selected managed server.

At the same time, the right pane changes to reflect a complete summary of the currently selected managed server. In addition to the summary section at the top of the pane, the following detail categories are available for each managed server being monitored by GDM:

- Alerts (Backup Exec managed servers only)
- Robots
- Standalone Drives
- Backup-To-Disk (Backup Exec managed servers only)
- Media
- Services
- Jobs

Each detail section uses advanced drill-down technologies to show information about a section.

For example, clicking the ⊞ control opens a section, allowing you to see additional details. Clicking the ⊟ control closes the section.

Dashboard’s detail sections also use tables to present information to you in a structured and organized manner. Within each table are column headers that specify the type of information that is displayed. You can customize the column heads that appear in the detail sections by hiding column heads containing information that may not be of interest to you. You can also re-arrange the order of the column heads to suit your individual requirements.

See also:

"Font Attribute Enhancements" on page 79

"Organizing Detail Section Columns" on page 105.

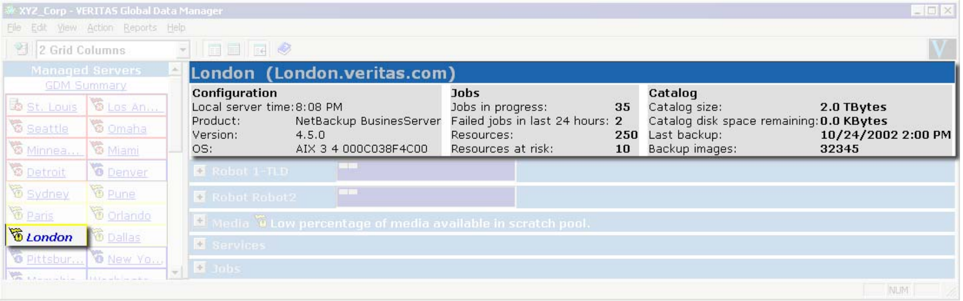
Detail Mode Sections

This section provides information for each of the detail sections found in the right pane of the GDM Dashboard.

Summary Section

The Summary detail section presents a summary overview of the managed server selected in the left pane. Summary information includes details about configuration, jobs, and catalogs.

Detail Mode - Summary Detail Section



London (London.veritas.com)

Configuration		Jobs		Catalog	
Local server time:	8:08 PM	Jobs in progress:	35	Catalog size:	2.0 TBytes
Product:	NetBackup BusinesServer	Failed jobs in last 24 hours:	2	Catalog disk space remaining:	0.0 KBytes
Version:	4.5.0	Resources:	250	Last backup:	10/24/2002 2:00 PM
OS:	AIX 3 4 000C038F4C00	Resources at risk:	10	Backup images:	32345

Media Low percentage of media available in scratch pool.

Summary column details are defined in the following table.

Detail Mode - Summary details

Configuration	Description
Local Server Time	The current time in the NetBackup managed server time zone. It is derived by using the local time and time zone of the Dashboard host computer and then applying a Greenwich Mean Time (GMT) offset to the GDM managed servers.
Product	The type of VERITAS product installed at the managed server.
Version	The version of the VERITAS product installed at the managed server.

Detail Mode - Summary details

OS	The name of the operating system that is running on the managed server.
Jobs	
Jobs in progress	The number of active jobs in progress that are being managed by the managed server.
Failed jobs in last 24 hours	The number of jobs that failed during the preceding 24 hours. The default interval of 24 hours can be configured to be an interval you choose. For more information, see "Adjusting the Look Back Interval" on page 47.
Resources	The number of client computers that the managed server is protecting. The count is derived from the number of classes defined in active classes. Under Backup Exec, resources include partitions, shares, databases, volumes, and so on.
Resources at Risk	The number of clients with failed backups in the preceding 24 hours. The default interval of 24 hours can be configured to be an interval you choose. **Note** Under Backup Exec managed servers, this category is listed as N/A, as this information is not available in Backup Exec. For more information, see "Adjusting the Look Back Interval" on page 47.
Catalogs	
Catalog Size	The total size of the current catalog being generated by NetBackup 5.1, NetBackup 4.5, NetBackup 3.4, and Backup Exec 8.6, 9.0 and 9.1 media servers.
Catalog Disk Space Remaining	The amount of available disk space on the managed server partition where the catalog resides. This value indicates how much space is available for future catalog growth.
Last Backup	The date and time when the catalog or catalogs was last backed up. **Note** Under Backup Exec managed servers, this category is listed as N/A, as this information is not available in Backup Exec.

Detail Mode - Summary details

Backup Images	The total number of backup images in the catalog.

Alert Details (Backup Exec managed servers only)

The Alert detail section shows alert details that are generated from Backup Exec managed servers in the GDM domain. All Backup Exec-generated alerts are displayed in read-only mode, which means you cannot respond to them directly using GDM. You can, however, respond to them by launching Backup Exec's Administration Console from within GDM. You can also move to the Backup Exec managed server and reply to the alerts locally.

Alert Detail Section - Column Details

Alert Time	Displays the date and time the alert occurred.
Category	Displays the alert category from which an alert was generated.
Device	Displays the name of the device on which the alert occurred.
Job Log File	The name of the job log file that contains details about the alert.
Job Name	Displays the name of the job associated with the alert.
Message	Describes the event that caused the alert.
Responder	Displays the user ID that responded to the alert.
Response Machine	Name of the computer from which the user responded.
Server	Displays the name of the Backup Exec managed server on which the alert occurred.
Source	Displays the cause of the alert. Alerts can originate from one of the following sources: ◆ System ◆ Job ◆ Media ◆ Device

Alert Detail Section - Column Details (continued)

Status	Displays the operational status of the alert, which is either Active or Cleared. Alerts remain active in the Backup Exec system until you enter a response, or you can configure the alert category property to automatically clear the alert after a specified length of time. Depending on the alert type, it may not be necessary to respond to the alert to continue with operations. After you respond to an alert, it is moved to the alert history, where the alert remains for the length of time you choose to keep it in the Backup Exec database or until you delete it. For more information, see your Backup Exec Administrator's Guide.
Time of Response	The time at which a user responded to the alert.
Type	Displays the severity of the alert. The type helps you determine how quickly you want to respond. Alert types include: ◆ Errors ◆ Warnings ◆ Information ◆ Attention Required
User Response	The response the user entered for the alert.

Because the Alerts detail section can potentially list large numbers of alerts, alert status filtering is available, which can be used to limit the number or types of alerts that appear.

See also:

"Organizing Detail Section Columns" on page 105

"Defining, Editing, and Deleting Filters" on page 102.

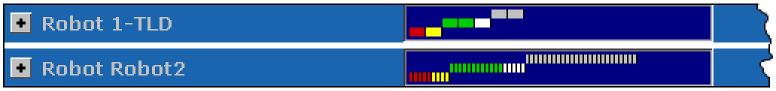
Robot Details

The Robot detail section shows details for each of the robotic drives that are being managed by the selected managed server or one of its media servers. Standalone drives are displayed in a separate detail section labeled *Standalone Drives*.

The Robot section contains unique LED-style graphics that allow you to quickly see the status of the drives in your robots, without having to open the Robot detail section. Depending on the number of drives within the robot, and because computer monitor screen space can be limited, each LED can represent either a single drive, or multiple drives in the same operational state. The more drives that are connected to a robot, the thinner the LEDs become, in order to accommodate the actual number of drives being represented within the LED-style graphic.

LED Examples

Robot with a small number of drives attached



Robot with many drives attached

Based on the color and positioning of the LEDs, you can make a quick, visual determination of the general status of the robot's drives.

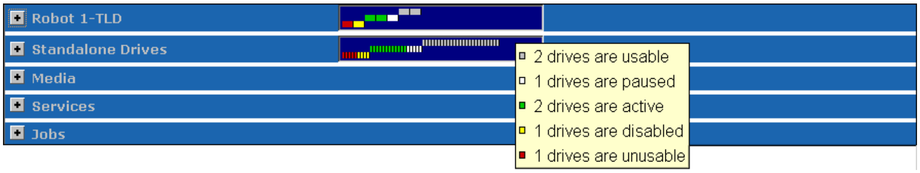
lED Color Definitions

LED Color	What it means
Red	Drives that are down and have serious issues.
Green	Drives that are up and active.
Gray	Drives that are up but are idle.
Yellow	Drives statuses are unknown because the media servers to which they are attached cannot be reached.
White	Drives that have been paused.

The positioning of an LED, along with its associated color, enables you to quickly determine if there are potential issues. All drives that are DOWN are positioned in the left portion of the graphic and are placed on a plane below the green LEDs, indicating a negative condition. Because the color green is associated with drives that are online and active, the green LEDS are considered normal conditions and are used as a base reference point. Gray LEDs appear above the green, showing an UP status.

Along with colors, ToolTips are used to help you interpret the information contained in the LED graphic.

Robot LED Graphic with ToolTip Example



⊞ Robot 1-TLD

⊞ Standalone Drives

⊞ Media

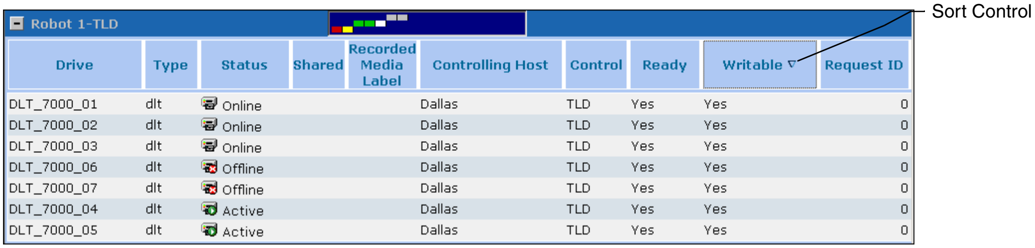
⊞ Services

⊞ Jobs

- □ 2 drives are usable
- □ 1 drives are paused
- 🟩 2 drives are active
- 🟨 1 drives are disabled
- 🟥 1 drives are unusable

Clicking the ⊞ control expands the Robot detail sections, displaying information about individual drives. Clicking a column head activates a Sort control, allowing you to sort column information in ascending and descending order.

Expanded Robot Detail Section



Sort Control

⊟ Robot 1-TLD

Drive	Type	Status	Shared	Recorded Media Label	Controlling Host	Control	Ready	Writable ▿	Request ID
DLT_7000_01	dlt	Online			Dallas	TLD	Yes	Yes	0
DLT_7000_02	dlt	Online			Dallas	TLD	Yes	Yes	0
DLT_7000_03	dlt	Online			Dallas	TLD	Yes	Yes	0
DLT_7000_06	dlt	Offline			Dallas	TLD	Yes	Yes	0
DLT_7000_07	dlt	Offline			Dallas	TLD	Yes	Yes	0
DLT_7000_04	dlt	Active			Dallas	TLD	Yes	Yes	0
DLT_7000_05	dlt	Active			Dallas	TLD	Yes	Yes	0

Robot Detail columns are defined in the following table.

Robot Detail Section - Column Details

Control

Drive control mode. If the drive is in a robot, a designation of the robot such as TS8 or TS8-DOWN appears in this column.

If the robotic drive is in a DOWN state, this column shows the selected mode as follows:

AVR (UP in Automatic Volume Recognition mode). This is the normal operating mode.

OPR (UP in Operator Control mode). You can set the drive to this state with the **UP Drive**, **Operator Control** command on the **Drives** menu in NetBackup.

DOWN. In this state, the drive is not available to Media Manager. A drive can be in the DOWN state because of problems, or because it was deliberately taken down by an administrator.

Controlling Host

If this drive is shared, the device host where the drive is assigned appears in this column.

If this drive is not shared, this column contains a dash (-). If you are using the Java-based Dashboard under Windows NT/2000, the column is blank.

Robot Detail Section - Column Details (continued)

Description *(Backup Exec only)* Displays the identifier used to determine the type of drive used by the robot.

Drive Drive name assigned to the drive during NetBackup configuration.

External Media ID External media ID serial number of the media mounted in the drive. Normally this identifier should match the Recorded Media Label. If a tape is not mounted, this field will be blank.

Path *(Backup Exec only)* Displays the path used by the Backup Exec feature, Backup-to-Disk. For more information, see your Backup Exec documentation.

Ready Status of the drive, indicating if it is ready to perform an operation on the loaded media. **Yes** means ready; **No** means not ready. A **dash** means the status is unknown.

Recorded Media Label Recorded media label of the media mounted in the drive. This identifier is the same as the media ID and should match the external media ID. If a tape is not mounted, this field will be blank.

Request ID Identification number for the request or action. This is a NetBackup system-assigned number that identifies the request. A pending action is indicated by an asterisk to the left of the request ID.

Shared Shows if the drive is shared by more than one host (Shared Storage Option). **Yes** means the drive is shared; **No** means the drive is not shared. A **dash** means the status is unknown.

Status Shows the situational status of the drive. The drive can be either up and active, up and idle, down, or unreachable, which means the status is unknown.

Type Drive type. Types include: 4mm, 8mm, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, and qscis. For more information, see your NetBackup documentation.

Writable Shows whether the volume currently mounted on this drive is write-enabled. **Yes** means the drive is write-enabled; **No** means it is write-protected. A **dash** means the status is unknown.

Standalone Drives Details

The Standalone Drives detail section shows details for non robotic, standalone storage drives that are attached to media servers being monitored by the NetBackup and/or Backup Exec managed servers in a GDM domain.

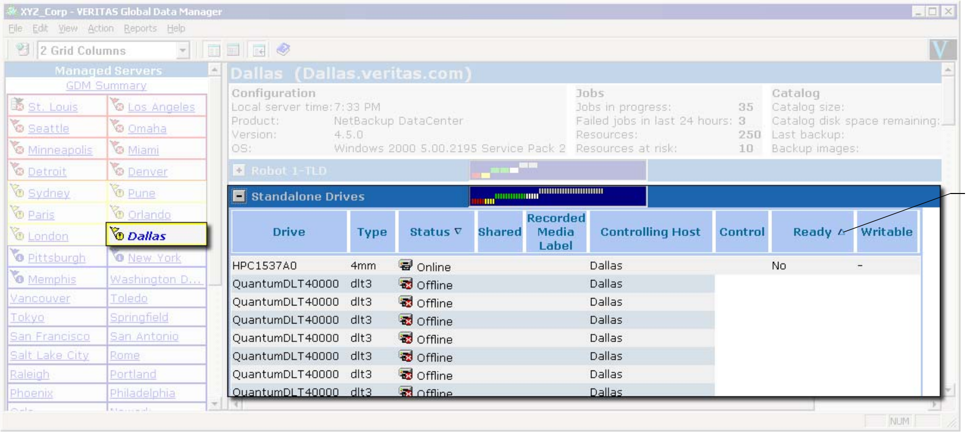
Like the Robot detail section, LED-style graphics are used to quickly determine standalone drive status.

The Standalone Drives detail section uses the same column head information found in the Robot detail section.

See also:

"Organizing Detail Section Columns" on page 105

Standalone Drives Detail Section



Configuration
Local server time: 7:33 PM
Product: NetBackup DataCenter
Version: 4.5.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: 10

Catalog
Catalog size:
Catalog disk space remaining:
Last backup:
Backup images:

Drive	Type	Status ▽	Shared	Recorded Media Label	Controlling Host	Control	Ready △	Writable
HPC1537A0	4mm	Online			Dallas		No	-
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			
QuantumDLT40000	dlt3	Offline			Dallas			

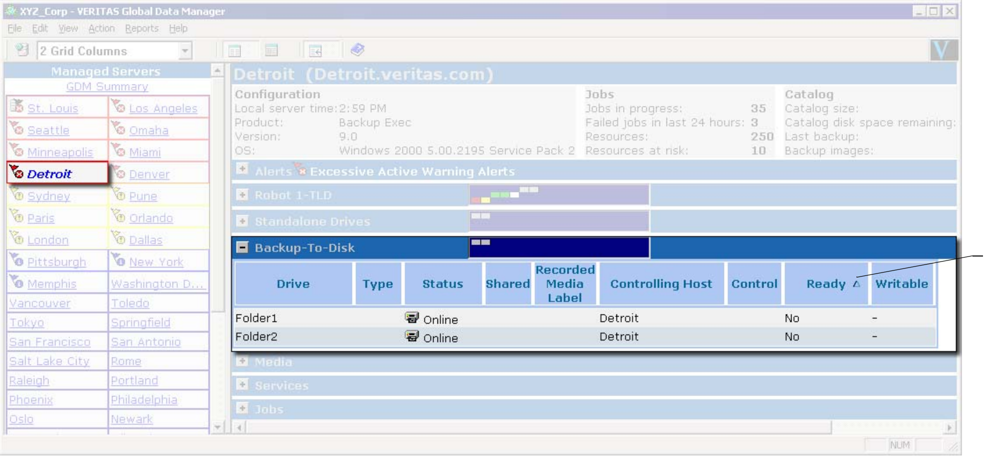
Sort Control

Backup-to-Disk Details (Backup Exec managed servers only)

The Backup-to-Disk details section shows details for each of the hard drive-based backup folders.

Backup Exec includes a feature called Backup-to-Disk, which allows you to back up data to a folder on a hard drive instead of to a storage device. Backup-to-Disk provides a faster method of backing up and restoring files, which is useful when you have a short amount of time to back up or restore data. You can use it as part of a two-stage backup process where you back up data to disk first and then transfer the data to media when more time is available. For more information on Backup-to-Disk, see your Backup Exec documentation.

Backup-to-Disk Detail Section



Detroit (Detroit.veritas.com)

Configuration
Local server time: 2:59 PM
Product: Backup Exec
Version: 9.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: 10

Catalog
Catalog size:
Catalog disk space remaining:
Last backup:
Backup images:

Alerts Excessive Active Warning Alerts

Robot 1-TLD

Standalone Drives

Backup-To-Disk

Drive	Type	Status	Shared	Recorded Media Label	Controlling Host	Control	Ready ▵	Writable
Folder1		Online			Detroit		No	-
Folder2		Online			Detroit		No	-

Media

Services

Jobs

Sort Control

Backup Exec recognizes Backup-to-Disk folders as robotic devices. As such, the GDM column head information used in the Robots detail section is also used in the Backup-to-Disk details section.

See also:

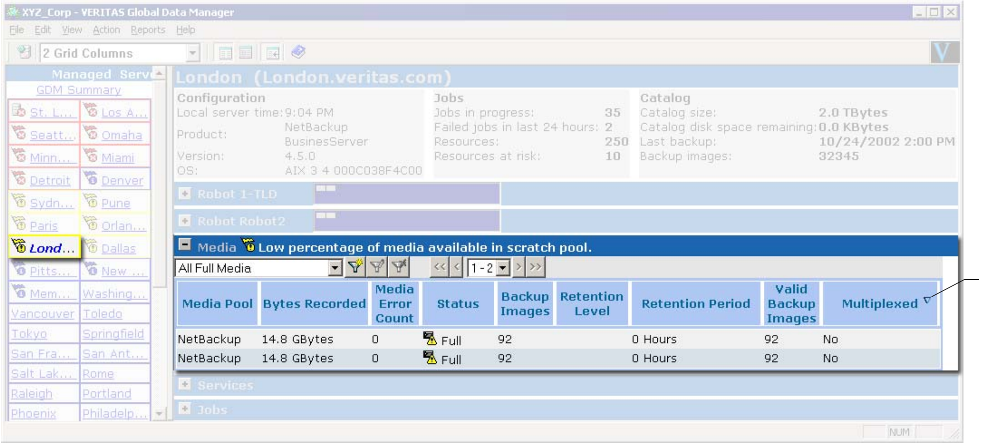
"Organizing Detail Section Columns" on page 105.

Media Details

The Media detail section shows details for each media being managed by the managed server selected in the left pane.

Because the Media detail section can potentially list large numbers of media, media status filtering is available, to limit the number or types of media that appear.

Detail Mode - Media Detail Section



London (London.veritas.com)

Configuration
Local server time: 9:04 PM
Product: NetBackup BusinesServer
Version: 4.5.0
OS: AIX 3 4 000C038F4C00

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 2
Resources: 250
Resources at risk: 10

Catalog
Catalog size: 2.0 TBytes
Catalog disk space remaining: 0.0 KBytes
Last backup: 10/24/2002 2:00 PM
Backup images: 32345

Media Low percentage of media available in scratch pool.

All Full Media

1 - 2

Media Pool	Bytes Recorded	Media Error Count	Status	Backup Images	Retention Level	Retention Period	Valid Backup Images	Multiplexed
NetBackup	14.8 GBytes	0	Full	92		0 Hours	92	No
NetBackup	14.8 GBytes	0	Full	92		0 Hours	92	No

Sort Control

Media detail columns are defined in the following table.

Media Detail Section - Column Details

Backup Images	Displays the number of backup images contained on media. A backup image is a collection of data that is saved for an individual client during each backup or archive. The backup image contains all the files, directories, and catalog information associated with the backup or archive.
Bytes Recorded	Displays the amount of data on media, in gigabytes, megabytes, or kilobytes, depending on the amount actually recorded.
Last Accessed	Displays the last date media was accessed by a storage device.
Media Error Count	Displays the number of hard or soft errors detected on the physical media during the processing of a job.
Media Pool	Formerly known as a volume pool, the media pool identifies a logical set of volumes by usage. Associating volumes with a volume [media] pool protects them from access by unauthorized users, groups, or applications.
Multiplexed	Displays all multiplexed backup sets that are interleaved on storage media.
Recorded Media Label	Recorded label of the media mounted in the drive. This identifier is the same as the media ID and should match the external media ID. If media is not mounted, this field will be blank.
Type	Displays the type of media used. Types include: 4mm, 8mm, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, and qscis.

Media Detail Section - Column Details (continued)

Recyclable On	Displays the date at which time the media can be reused.
Retention Level	Displays the retention level assigned to media.
Retention Period	Displays the period of time the data on the media is to be retained.
Retire On	Displays the date at which time the media should be retired due to media age considerations.
Status	Displays the status of the media. Status conditions include: Non appendable, Imported, Full, Retired, Catalog Data, and Catalog Error. For more information, see "Available Media Statuses" on page 98.
Valid Backup Images	Displays the number of valid backup images contained on a piece of media. Note that on multiplexed media, this column may remain blank. A valid backup image is a collection of data (backup image) that has been verified.

The following table describes the media statuses that can appear in the **Status** column.

Available Media Statuses

Available Media Statuses

Status	Description
Non Appendable	Media that cannot be appended to, either by policy or user action.
Imported	Media is imported.
Full	Media is full.
Retired	Media is no longer available for use.
Catalog Data	Media contains catalog data, which is required to restore data.
Catalog Error	Information that NetBackup and the MediaManager have about media is inconsistent. For example, the MediaManager may have media flagged as assigned to NetBackup, but NetBackup does not know anything about it.

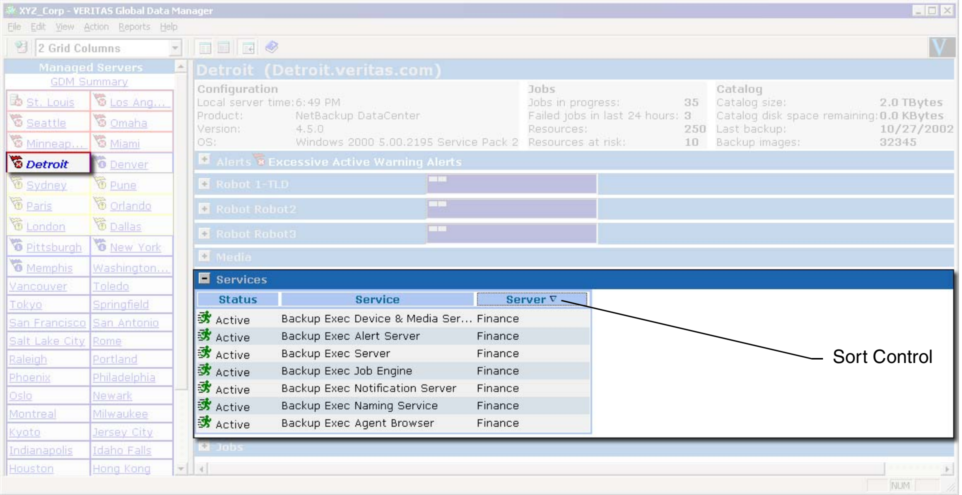
See also:

“Organizing Detail Section Columns” on page 105

Services Details

The Services detail section shows status details for each of the services or daemons that are installed on the managed server (or its media servers) selected in the left pane.

Detail Mode - Services Detail Section



Detroit (Detroit.veritas.com)

Configuration
Local server time: 6:49 PM
Product: NetBackup DataCenter
Version: 4.5.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: 10

Catalog
Catalog size: 2.0 TBytes
Catalog disk space remaining: 0.0 KBytes
Last backup: 10/27/2002
Backup images: 32345

Status	Service	Server ▽
Active	Backup Exec Device & Media Ser...	Finance
Active	Backup Exec Alert Server	Finance
Active	Backup Exec Server	Finance
Active	Backup Exec Job Engine	Finance
Active	Backup Exec Notification Server	Finance
Active	Backup Exec Naming Service	Finance
Active	Backup Exec Agent Browser	Finance

Sort Control

Service Detail section columns are defined in the following table.

Services Detail Section - Column Details

Status	Displays the operational status of the service or daemon. One of three status conditions can appear for each service or daemon listed: Active, Inactive, Failed, or Unreachable (if a media server cannot be reached to detect the service status). **Note** **Inactive** and **Failed** services are marked as **Inactive** on pre-Feature Pack 3 versions of NetBackup.
Service	Displays the name and type of service or daemon.
Server	Displays the name of the NetBackup master server or the Backup Exec media server where the service or daemon is running.

See also:

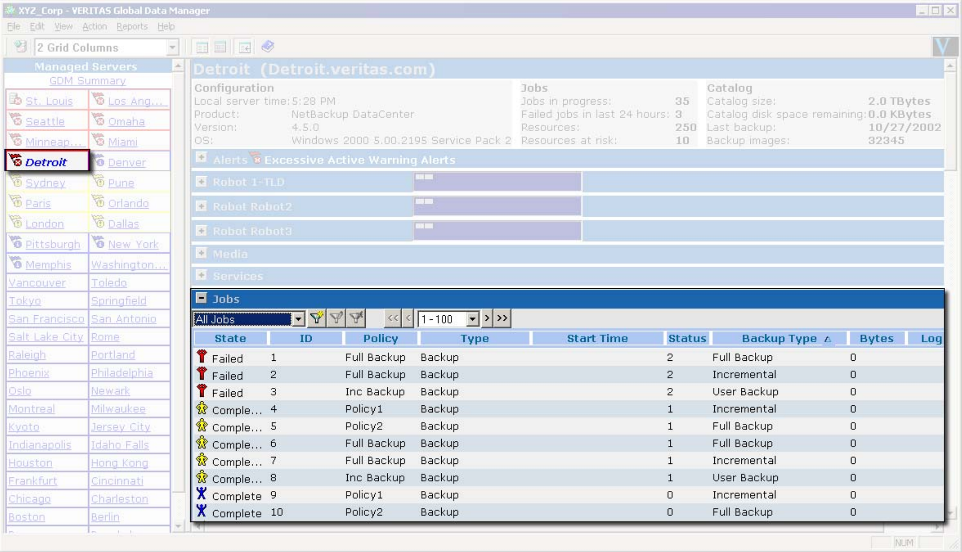
“Organizing Detail Section Columns” on page 105

Jobs Details

The Jobs detail section shows details for each of the jobs being managed by the managed server selected in the left pane.

Because the Jobs detail section can potentially list a large number of jobs, job filtering is available, to limit the number or types of jobs that appear.

Detail Mode - Jobs Detail Section



Detroit (Detroit.veritas.com)

Configuration
Local server time: 5:28 PM
Product: NetBackup DataCenter
Version: 4.5.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: 10

Catalog
Catalog size: 2.0 TBytes
Catalog disk space remaining: 0.0 KBytes
Last backup: 10/27/2002
Backup images: 32345

State	ID	Policy	Type	Start Time	Status	Backup Type ▵	Bytes	Log
Failed	1	Full Backup	Backup		2	Full Backup	0	
Failed	2	Full Backup	Backup		2	Incremental	0	
Failed	3	Inc Backup	Backup		2	User Backup	0	
Comple...	4	Policy1	Backup		1	Incremental	0	
Comple...	5	Policy2	Backup		1	Full Backup	0	
Comple...	6	Full Backup	Backup		1	Full Backup	0	
Comple...	7	Full Backup	Backup		1	Incremental	0	
Comple...	8	Inc Backup	Backup		1	User Backup	0	
Complete	9	Policy1	Backup		0	Incremental	0	
Complete	10	Policy2	Backup		0	Full Backup	0	

Jobs detail columns are defined in the following table.

Jobs Detail Section - Column Details

Backup Type Displays the type of backup job being processed. For example, full, incremental, differential and user backup.

Bytes Displays the number of bytes backed up.

Elapsed Time Displays the amount of time that has elapsed since the job started.

End Time Displays the time the job ended.

ID Displays the identifying number that NetBackup has assigned to the job.

Log File Displays the name and location of the log file generated for the job.

NBU Job ID Displays the job ID generated by NetBackup.

Jobs Detail Section - Column Details

Media Server	Displays the name of the media server that is, or will be, processing the job.
Percent Complete	Displays the completion percentage of the job as it is being processed.
Policy	Displays the backup policy associated with the backup job.
Resource	Displays the client name of the computer at which the job originates.
Schedule	Displays the type of job scheduled to be executed. For example, full backup, incremental/differential, user backup.
Start Time	Displays the time the job started.
State	Displays the state of the job. For example, Queued, Active, Requeued, Done. For more information on job states, see your NetBackup documentation.
Status	Displays a numerical code, usually accompanied by a message, that indicates the status or outcome of an operation.
Type	Displays the type of operation for the selected job. For example, Backup, Archive, Restore, Verify and Duplicate. for more information, see your Backup Exec documentation.

See also:

"Organizing Detail Section Columns" on page 105

"Defining, Editing, and Deleting Filters" on page 102.

Defining, Editing, and Deleting Filters

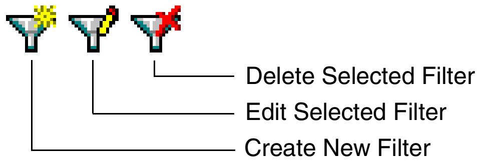
The Alerts, Media and Jobs detail sections enable you to use default filters provided by the GDM Dashboard. These filters enable you to filter on the following topics:

Alerts, Media and Jobs Detail Section Filters

Alerts Filters	Media Filters	Jobs Filters
All Alerts	All Media	All Jobs
Active Alerts	All Full Media	All Active Jobs
Historical Alerts	All Non appendable Media	All Queued Jobs
System Alerts	All Unused Media	All Done Jobs
Media Alerts	All Retired Media	All Requeued Jobs
Device Alerts		All Failed Jobs
Job Alerts		
Error Alerts		
Warning Alerts		
Informational Alerts		
Attention Required Alerts		

In addition to these default filters, you can also create your own filters using the **Create New Filter** button. After a user-defined filter is created, the **Edit Selected Filter** and **Deleted Selected Filter** buttons can be used to either modify or delete the new filters.

Filter Icons



Note Both the **Edit Selected Filter** and the **Delete Selected Filter** buttons are enabled only when a user-defined filter is selected.

Default GDM filters cannot be modified or deleted.

▼ To define a filter

1. Open the **Jobs** or **Media** detail section.
2. Click the **Create New Filter** button.
3. Enter a name for the new filter.
4. Select a filter type in the **Field** box.
5. Select a comparison type in the **Comparison** box.
6. Enter a value in the **Value** box.

Note Values can be alphabetical labels, numerics, or conditions such as Active, Suspended, Frozen, or Imported.

7. When finished, click **OK**.

   After defining a filter, it appears in the drop-down list box.

▼ To modify/edit a filter

1. Open the **Jobs** or **Media** detail section.
2. Click the drop-down filter list box and select a filter to edit.
3. Click the **Edit Selected Filter** button.
4. Make your changes and click **OK**.

▼ To delete a filter

1. Open the **Jobs** or **Media** detail section.

2. Click the drop-down list box and select a filter to delete.

3. Click **Delete Selected Filter** button.

   You are prompted to confirm the deletion operation.

4. Click **Yes**.

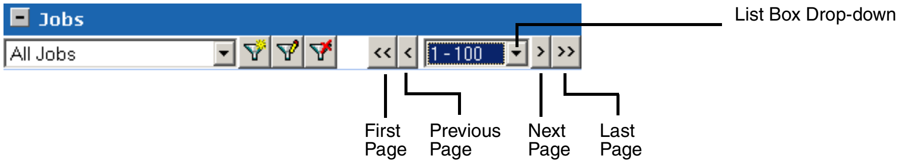
   The selected filter is deleted.

Managing the Amount of Data to Be Viewed

The amount of data that GDM monitors can quickly multiply. To effectively manage the data, both the Media and Jobs detail sections provide a drop-down list box where you can make selections to limit the number of media or jobs that appear in each section.

Note This feature is not supported in the GDM Java Dashboard.

Example of managing the number of jobs to be viewed



Each detail section's list box uses four buttons for navigational purposes. These include the following:

List Box Action Buttons

Button	Action
First Page	Displays the first page in a sequence of pages of monitored data.
Previous Page	Displays the previous page of monitored data.
Next Page	Displays the next page in a sequence of pages of monitored data.

List Box Action Buttons

Button	Action
Last Page	Displays the last page in a sequence of pages of monitored data.

Organizing Detail Section Columns

Each Dashboard detail section uses tables to present structured information. Within each table are column heads that specify the type of information that is displayed. You can customize the column heads by removing column heads containing information that may not be of interest to you.

For example, there may be instances when you want to limit the type of information that is presented in a detail section, or you may want to present the information in a different order.

Note Changing detail section column head information is not a global operation. Because each detail section is an independent entity, any changes you make pertain only to the detail section you are viewing.

You can also specify the order in which the column heads appear, using the **Move Column Down** and **Move Column Up** buttons. These buttons are located in the upper left corner of the Column Layout dialog box. Highlighting a column head name in the Layout Columns selection box and then clicking the **Move Column Up** button once causes the column name to move one column to the left in the detail section. Clicking the **Move Column Down** button once moves the selected column name one column to the right.

The position of the column names in the Layout Columns selection box dictates the column's positioning within the detail section. For instance, column names appearing at the top of the list are positioned left in the detail section.

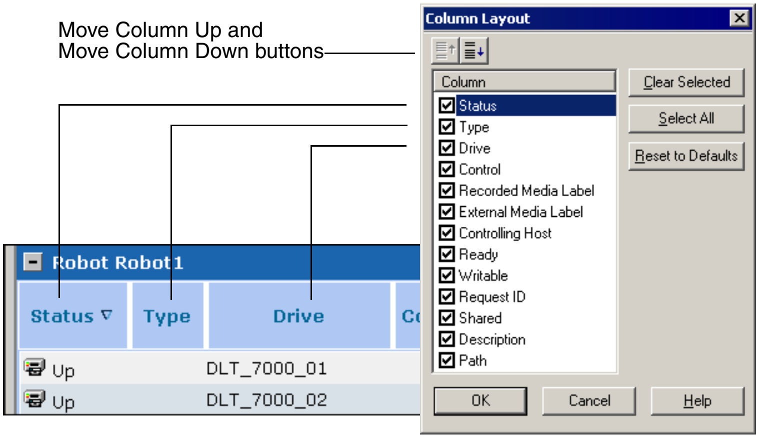
Note In the GDM Java Dashboard, you can change the layout of the columns by selecting a column head with your mouse, and then dragging it to a position.

Changes to a column layout for a table are retained between dashboard sessions, and are shared by all managed servers in the GDM domain. Because there may be a variable number of Robot detail sections per server, changes to a column layout for a Robot table for a managed server are applied to that robot section only and are shared by other servers in the domain that have a robot section in the same ordinal position. Robot sections are numbered top to bottom, with the topmost section starting with 1.

Note In the GDM Java Dashboard, changes to a column layout for a Robot table are applied to that robot section only and are shared by other servers in the domain that have the same Robot number, regardless of the ordinal position of the section.

Also, column layouts are not retained between the Windows-based version of the Dashboard and the Java-based version of the Dashboard. As such, changing the configuration in the Java Dashboard has no impact on the Windows Dashboard.

Layout Column Selection Box and Column Layout Positions - Windows Dashboard only



☑ Status
☑ Type
☑ Drive
☑ Control
☑ Recorded Media Label
☑ External Media Label
☑ Controlling Host
☑ Ready
☑ Writable
☑ Request ID
☑ Shared
☑ Description
☑ Path

Status	Type	Drive
Up		DLT_7000_01
Up		DLT_7000_02

▼ To hide column heads

1. In a detail section you want to modify, right-click a column.

2. Click **Column Layout** on the shortcut or context menu that appears.

3. Click the column titles that you want to hide.

Note To quickly hide previously selected column heads, click the **Clear Selected** button on the right side of the selection box.

4. Click **OK**.

   The table columns are reset and now display the information you want to see.

   To reset the default view, click the **Reset to Defaults** button on the right side of the selection box.

▼ To show column heads

1. In a detail section you want to modify, right-click a column.

    a. In the Windows Dashboard, click **Column Layout** on the shortcut or context menu that appears.

    b. In the Java Dashboard, click **Add/Remove** on the context menu that appears.

2. Click the column titles you want to see.

Note To quickly add all column heads, click the **Select All** button on the right side of the selection box.

3. Click **OK**.

    The table columns are reset and now display the information you want to see.

    To reset the default view, click the **Reset to Defaults** button on the right side of the selection box.

▼ To re-arrange column head order

If you are using the Windows Dashboard

1. In a detail section you want to modify, right-click any column.

2. Click **Column Layout** on the shortcut or context menu that appears.

3. Click a column you want to re-arrange.

4. In the **Layout Columns** selection box toolbar, click either the Move Column Down icon or the **Move Column Up** icon, depending on where you want the column to appear in the detail section.

Note Clicking the **Move Column Down** icon results in the column being moved to the right in the detail section; clicking the **Move Column Up** icon results in the column being moved to the left in the detail section.

5. Click **OK**.

    The column information is now re-arranged in the order you want.

    To reset the column layout to the default view, click the **Reset to Defaults** button on the right side of the selection box.

If you are using the Java Dashboard

1. Click a column head.
2. Drag it to the new position.

Administering the Managed Servers

At some point, you may want to actively manage the issues that appear in GDM while GDM monitors your managed servers. Although the GDM does not directly allow you to manage NetBackup or Backup Exec servers, you can run administration functions on these computers by using the administration consoles provided in both NetBackup and Backup Exec. Through its user interface, GDM makes it easy to launch and run either the NetBackup *Administration Console* or the Backup Exec *Administration Console.*

The following chart shows the administration console launch compatibilities on the Windows and UNIX platforms.

Administration Consoles That Can Be Launched From GDM

Operating System Platform	GDM Dashboard Version	NetBackup AC (Windows)	NetBackup AC (Java)	Backup Exec AC
Windows	Windows	X		X
Windows	Java		X	
UNIX	Java		X	

Configuration Requirements for Managing Servers Using GDM

◆ *Windows Dashboard* - With the Windows version of the GDM Dashboard, you can manage NetBackup managed servers running on supported UNIX or Windows systems. You can also manage Backup Exec 8.6, 9.0, and 9.1.

To manage either the UNIX or Windows version of NetBackup, you must install the administration console for NetBackup on the computer where the GDM Dashboard is running.

Note The NetBackup Administration Console and the GDM Dashboard must be both running the same version.

You must also configure the NetBackup server configuration in such a way that the user of the GDM Dashboard can independently use the NetBackup Administration Console interface from the Dashboard computer to manage both the UNIX and Windows-based NetBackup managed servers.

● To manage Backup Exec, you must install the Backup Exec Remote Administrator console on the computer where the GDM Dashboard is installed. In addition, the Dashboard user must have Backup Exec administration privileges in order to manage Backup Exec managed servers. For more information, see your *Backup Exec for Windows NT/2000 Administrator's Guide* or your *Backup Exec for Windows Servers Administrator's Guide*.

- *Java Dashboard* - With the Java version of the GDM Dashboard, you can manage NetBackup managed servers. However, the Java version of the NetBackup Administration Console must be installed on the computer where the GDM Dashboard is running.

  Additionally:

  - The Java Dashboard user must have administrative privileges on the GDM Server.
  - There must be a trusted relationship established between the GDM Server and the NetBackup managed servers you want to manage.

  For more information, see your *NetBackup 5.1 System Administrator's Guide*.

  Note The Java version of the GDM Dashboard can be installed on supported Windows or UNIX systems. It can then be used to manage NetBackup servers using GDM.

Limitations

Although GDM can launch the NetBackup and Backup Exec administration consoles that enable you to actively address issues at the managed servers, there are limitations. These limitations include the following:

- The GDM Dashboard *does not support* the GDM-based launching of the NetBackup 3.4 master Server Administration Console. To actively manage a NetBackup 3.4 managed server, you must run the NetBackup 3.4 Administration Console in a separate window, outside the GDM application.
- The GDM Dashboard supports the GDM-based launching of both the Windows and Java-based versions of the NetBackup 4.5 Administration Console. Consider the following:

  ❖ If you are using the Java-based Dashboard:

  - The *Java-based* version of the GDM Dashboard launches only the *Java-based* version of the NetBackup Administration Console. Pre 4.5 FP 3 versions of NetBackup Administration Consoles are not supported. Launching the *Windows-based* version of NetBackup Administration Console is not supported from the Java-based version of the Dashboard.
  - The *Java-based* version of the GDM Dashboard does not support launching Backup Exec Administration Consoles.

  - To manage a server in a GDM domain using the launch of the NetBackup Administration Console, the managed server must have a trusted relationship established with the GDM Server using NetBackup's authentication model, as described in the *NetBackupSystem Administrator's Guide*.

    When the NetBackup Administration Console is executed directly from the command line, by default you are prompted for the user name and password of the local machine. However, when the administration console is launched from Dashboard, the server you are logging into is forced to log into the GDM Server. From this point, the NetBackup authentication model is used.

    Because of the forced logon to the GDM Server, only those NetBackup servers that you want to manage through GDM using the administration console must be configured as a trusted server to the GDM Server.

❖ If you are using the Windows-based Dashboard:

  - The *Windows-based* version of the GDM Dashboard launches the respective administration consoles for managed servers running NetBackup or Backup Exec, depending on the administration console it finds installed on the managed servers.

    For example, if the target managed server is running Backup Exec 8.6, GDM will launch Backup Exec's Administration Console. If the target managed server is running NetBackup, GDM will launch the Windows-based NetBackup Administration Console.

  - The Dashboard host computer must be configured as a trusted server in the Managed Server List (both UNIX and Windows).

- Firewall support is not available.

Security

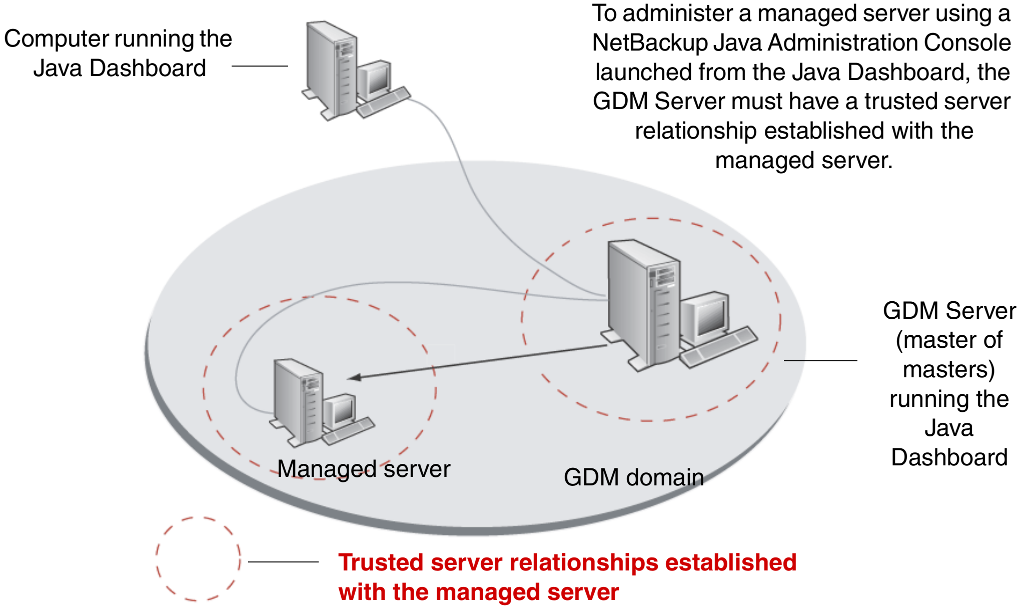
This section provides you with information concerning the required GDM security model when working with the NetBackup Java Administration Console.

GDM Java Dashboard and the NetBackup Java Administration Console

Launching the NetBackup Java-based administration console from the GDM Java-based Dashboard does not override or compromise existing NetBackup security that is in place.

To launch the NetBackup Java administration console for administration of a managed server, the GDM Server must be a *trusted server* to the managed server, and the username used to log into the GDM Server must have the applicable privileges on the managed server. Follow the NetBackup security models (Java authentication model for root and non-root users, or the advanced security model) to authenticate the GDM Server and username. This authentication model applies to GDM Servers on Windows as well as UNIX platforms.

Required Trusted Server Relationships


Computer running the Java Dashboard
To administer a managed server using a NetBackup Java Administration Console launched from the Java Dashboard, the GDM Server must have a trusted server relationship established with the managed server.
GDM Server (master of masters) running the Java Dashboard
Managed server
GDM domain
Trusted server relationships established with the managed server

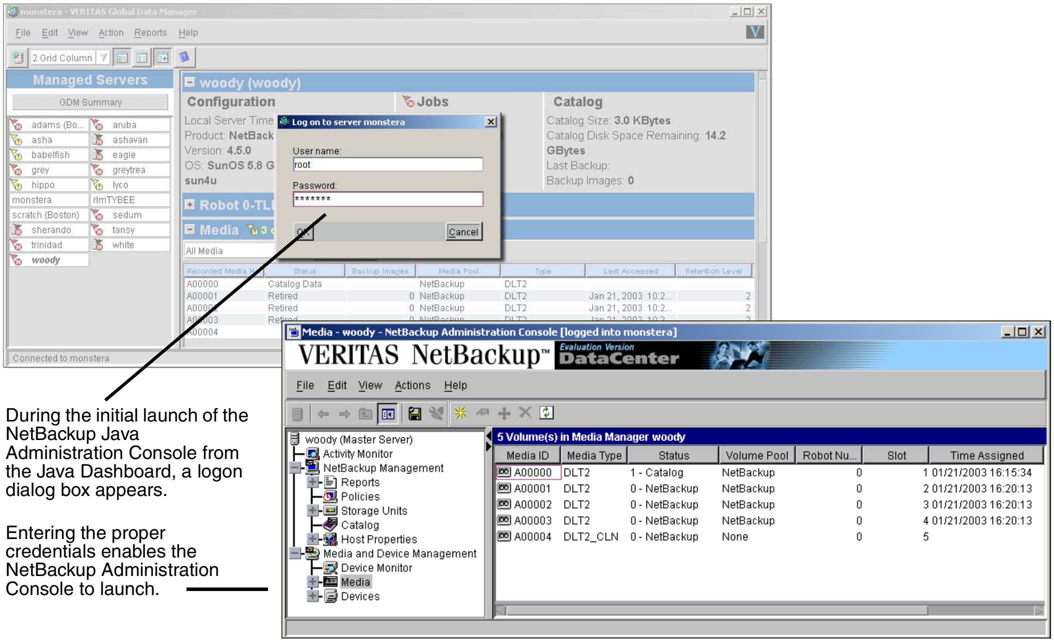
For more information, see the following:

- *Running the Java-based Windows Display Console* in the *NetBackup System Administrator's Guide for UNIX, Volume I*
- *Enhanced Authentication and Authorization* in the *NetBackup System Administrator's Guide for UNIX, Volume II*

Upon the initial launch of the NetBackup Java-based Administration Console, a login dialog box appears, prompting you for the username and password to use to log in to the GDM Server (also known as the master of masters). This is the equivalent of starting the NetBackup Java Administration Console directly and logging in to the GDM Server as the initial master server where you want to manage NetBackup.

The following example shows the NetBackup Java Administration Console being launched from the GDM Java Dashboard.

Launching the NetBackup Java Administration Console from the GDM Java Dashboard



Log on to server monstera

User name: root

Password: *******

Media - woody - NetBackup Administration Console [logged into monstera]

5 Volume(s) in Media Manager woody

Media ID	Media Type	Status	Volume Pool	Robot Nu...	Slot	Time Assigned
A00000	DLT2	1 - Catalog	NetBackup	0	1	01/21/2003 16:15:34
A00001	DLT2	0 - NetBackup	NetBackup	0	2	01/21/2003 16:20:13
A00002	DLT2	0 - NetBackup	NetBackup	0	3	01/21/2003 16:20:13
A00003	DLT2	0 - NetBackup	NetBackup	0	4	01/21/2003 16:20:13
A00004	DLT2_CLN	0 - NetBackup	None	0	5	

During the initial launch of the NetBackup Java Administration Console from the Java Dashboard, a logon dialog box appears.

Entering the proper credentials enables the NetBackup Administration Console to launch.

Caution Attempting to launch the NetBackup Administration Console with a username that does not have administrator rights will generate an error and the launch of the NetBackup Administration Console will fail.

For more information, see the following sections in your *NetBackup 5.1 System Administration Guide for UNIX, Volume I*:

- *NetBackup Administration Console Setup*
- *Introduction to NetBackup*
- *Administering Remote Servers*
- *Running the Java-based Windows Display Console*

Launching an Administration Console

This section guides you through steps necessary to launch either the NetBackup or Backup Exec Administration Consoles from:

- The Java version of Dashboard, when connecting to a managed server running:
  - NetBackup on a UNIX or Windows-based computer
- The Windows version of Dashboard when connecting to a managed server running:
  - NetBackup on a UNIX or Windows-based computer
  - Backup Exec

Launching from the Java Version of the Dashboard

▼ To launch from NetBackup on a UNIX or Windows-based managed server

1. To launch the NetBackup Administration Console, select a UNIX or Windows-based managed server running NetBackup in the Managed Servers pane on the left side of the Dashboard interface.

2. From the **Action** menu at the top of the Dashboard interface, click **Action** > **Administer**.

Note You can also launch the NetBackup Administration Console by right-clicking the UNIX or Windows-based managed server in the Managed Servers pane and then selecting **Administer** from the shortcut menu that appears.

The NetBackup Administration Console appears in a separate window and can now be used to administer the managed NetBackup server.

Launching from the Windows Version of the Dashboard

▼ To launch from NetBackup on a UNIX or a Windows-based managed server

1. To launch the NetBackup Administration Console, select a UNIX or Windows-based managed server running NetBackup in the Managed Servers pane on the left side of the Dashboard interface.

2. From the **Action** menu at the top of the Dashboard interface, click **Action** > **Administer**.

   Note You can also launch the NetBackup Administration Console by right-clicking on the UNIX or Windows-based managed server name in the Managed Servers pane on the left side of the Dashboard, and then selecting **Administer** from the shortcut menu that appears.

   The NetBackup Administration Console appears in a separate window and can now be used to administer the managed NetBackup server.

▼ To launch from Backup Exec on a Windows-based managed server

1. To launch the Backup Exec Administration Console, select a managed Backup Exec media server listed in the Managed Servers pane on the left side of the Dashboard interface.

2. From the **Action** menu, click **Administer**.

   The Backup Exec Administration Console appears in a separate window and can now be used to administer the managed Backup Exec media server.

   Note You can also launch the Backup Exec Administration Console by right-clicking on the Backup Exec managed server name in the Managed Servers pane on the left side of the Dashboard, and then selecting **Administer** from the shortcut menu that appears.

Window Management in GDM

This section provides information for the various window management methods GDM uses after you launch an administration console from within the GDM Dashboard interfaces.

Maintaining Context

In GDM, administration consoles are typically launched through the Dashboard's **Action** menu (**Action** > **Administer**), or a shortcut or context menu.

When launching an administration console from a Dashboard detail section, the context of your location in the Dashboard is matched to its corresponding location in the administration console.

For example, if you launch the Backup Exec Administration Console from the Alerts detail section of the Dashboard, Dashboard brings you directly to the Alerts view in the Backup Exec Administration Console.

Note Launching the Backup Exec 8.6 Administration Console from the Dashboard *Services* detail section of a Backup Exec 8.6 managed server is not supported.

Administration Console Launch Contexts

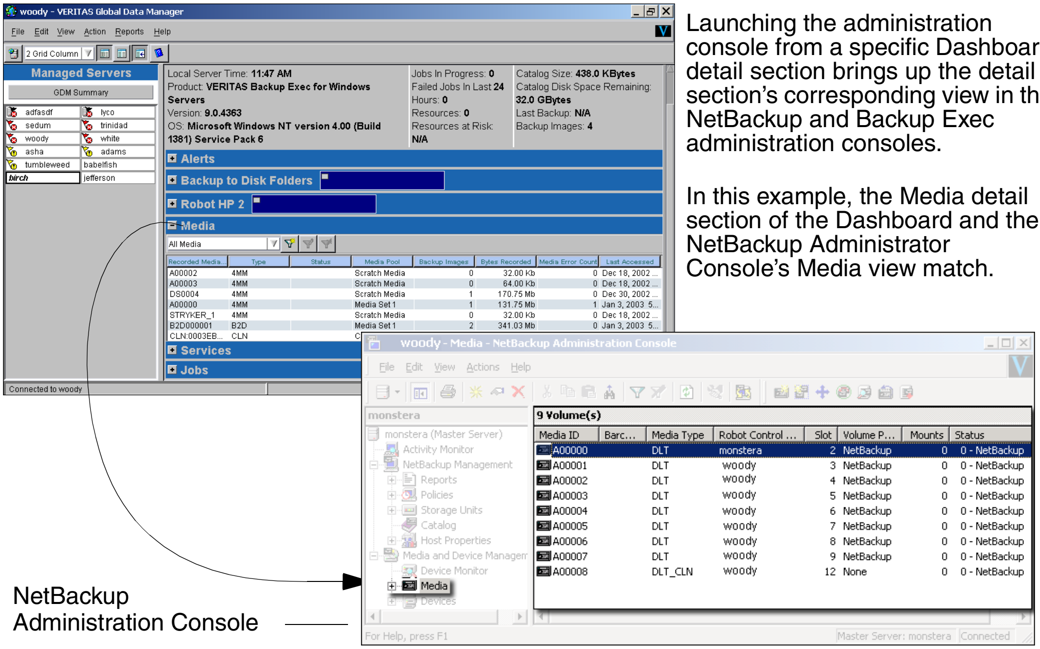
Administration Console Contexts When Launched From Within the GDM Dashboard

Administration Console Platform	NetBackup Admin Console (Windows)	NetBackup Admin Console (Java)	Backup Exec 8.6 Admin Console	Backup Exec 9.*x* Admin Console
Launching an administration console from the GDM...				
...Managed Servers pane takes you to:	**Master Server node**	**Master Server node**	**Backup Selections tab (default)**	**Overview panel (default panel)**
...Robot Detail Section takes you to:	**Device Monitor node**	**Device Monitor node**	**Devices tab**	**Devices panel**
...Standalone Drive Detail Section takes you to:	**Device Monitor node**	**Device Monitor node**	**Devices tab**	**Devices panel**
...Backup-to-Disk Detail Section takes you to:	**n/a**	**n/a**	**Devices tab**	**Devices panel**
...Alerts Detail Section takes you to:	**n/a**	**n/a**	**Alerts tab**	**Alerts panel**
...Media Detail Section takes you to:	**Media node**	**Media node**	**Media tab**	**Media panel**

Administration Console Launch Contexts (continued)

Administration Console Contexts When Launched From Within the GDM Dashboard				
Administration Console Platform	**NetBackup Admin Console (Windows)**	**NetBackup Admin Console (Java)**	**Backup Exec 8.6 Admin Console**	**Backup Exec 9.*x* Admin Console**
...Services Detail Section takes you to:	**Activity Monitor node with Daemons tab selected**	**Activity Monitor node with Daemons tab selected**	**n/a**	**Previous context used**
...Jobs Detail Section takes you to:	**Activity Monitor node with Jobs tab selected**	**Activity Monitor node with Jobs tab selected**	**Activity Monitor tab**	**Job Monitor panel**

Example of Context Launching



Local Server Time: **11:47 AM**
Product: **VERITAS Backup Exec for Windows Servers**
Version: **9.0.4363**
OS: **Microsoft Windows NT version 4.00 (Build 1381) Service Pack 6**

Jobs In Progress: **0**
Failed Jobs In Last **24** Hours: **0**
Resources: **0**
Resources at Risk: **N/A**

Catalog Size: **438.0 KBytes**
Catalog Disk Space Remaining: **32.0 GBytes**
Last Backup: **N/A**
Backup Images: **4**

Recorded Media...	Type	Status	Media Pool	Backup Images	Bytes Recorded	Media Error Count	Last Accessed
A00002	4MM		Scratch Media	0	32.00 Kb	0	Dec 18, 2002 ...
A00003	4MM		Scratch Media	0	64.00 Kb	0	Dec 18, 2002 ...
DS0004	4MM		Scratch Media	1	170.75 Mb	0	Dec 30, 2002 ...
A00000	4MM		Media Set 1	1	131.75 Mb	1	Jan 3, 2003 5...
STRYKER_1	4MM		Scratch Media	0	32.00 Kb	0	Dec 18, 2002 ...
B2D000001	B2D		Media Set 1	2	341.03 Mb	0	Jan 3, 2003 5...
CLN:0003EB...	CLN		C				

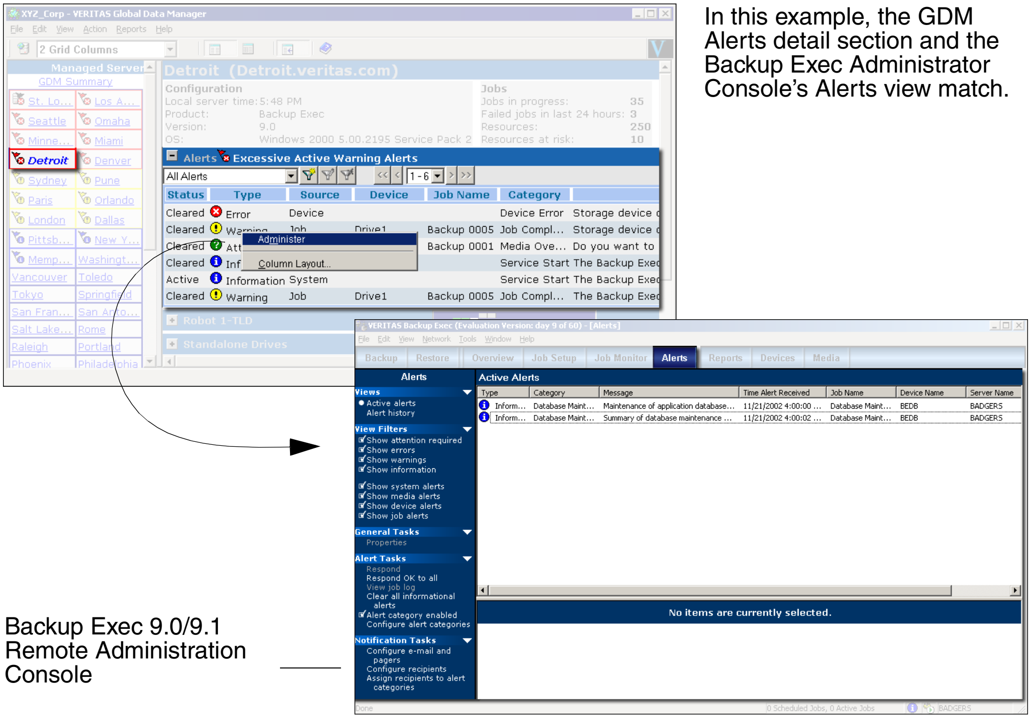
9 Volume(s)

Media ID	Barc...	Media Type	Robot Control ...	Slot	Volume P...	Mounts	Status
A00000		DLT	monstera	2	NetBackup	0	0 - NetBackup
A00001		DLT	woody	3	NetBackup	0	0 - NetBackup
A00002		DLT	woody	4	NetBackup	0	0 - NetBackup
A00003		DLT	woody	5	NetBackup	0	0 - NetBackup
A00004		DLT	woody	6	NetBackup	0	0 - NetBackup
A00005		DLT	woody	7	NetBackup	0	0 - NetBackup
A00006		DLT	woody	8	NetBackup	0	0 - NetBackup
A00007		DLT	woody	9	NetBackup	0	0 - NetBackup
A00008		DLT_CLN	woody	12	None	0	0 - NetBackup

NetBackup Administration Console

Launching the administration console from a specific Dashboard detail section brings up the detail section's corresponding view in the NetBackup and Backup Exec administration consoles.

In this example, the Media detail section of the Dashboard and the NetBackup Administrator Console's Media view match.



Configuration
Local server time: 5:48 PM
Product: Backup Exec
Version: 9.0
OS: Windows 2000 5.00.2195 Service Pack 2

Jobs
Jobs in progress: 35
Failed jobs in last 24 hours: 3
Resources: 250
Resources at risk: 10

Status	Type	Source	Device	Job Name	Category	
Cleared	Error	Device			Device Error	Storage device c
Cleared	Warning	Job	Drive1	Backup 0005	Job Compl...	Storage device c
Cleared	Att			Backup 0001	Media Ove...	Do you want to
Cleared	Inf				Service Start	The Backup Exec
Active	Information	System			Service Start	The Backup Exec
Cleared	Warning	Job	Drive1	Backup 0005	Job Compl...	The Backup Exec

Active Alerts

Type	Category	Message	Time Alert Received	Job Name	Device Name	Server Name
Inform...	Database Maint...	Maintenance of application database...	11/21/2002 4:00:00 ...	Database Maint...	BEDB	BADGERS
Inform...	Database Maint...	Summary of database maintenance ...	11/21/2002 4:00:02 ...	Database Maint...	BEDB	BADGERS

No items are currently selected.

In this example, the GDM Alerts detail section and the Backup Exec Administrator Console's Alerts view match.

Backup Exec 9.0/9.1 Remote Administration Console

Exit Coordination

When selecting the **Close** option on an active secondary GDM window, only the active window closes. All other secondary windows, along with the original instance of GDM, remain open.

When you close a secondary window using the **Exit** option, *all* Dashboard windows are closed, and the instance of GDM Dashboard is shut down.

Windows Dashboard and Administration Consoles

Administration consoles that are launched through the Windows version of Dashboard are independent applications, separate from the GDM Dashboard. They are not considered secondary Dashboard windows. As such, when you use the Exit option to shut down all secondary Windows Dashboard windows, and the Dashboard itself, the administration console remains running, and is *not* closed.

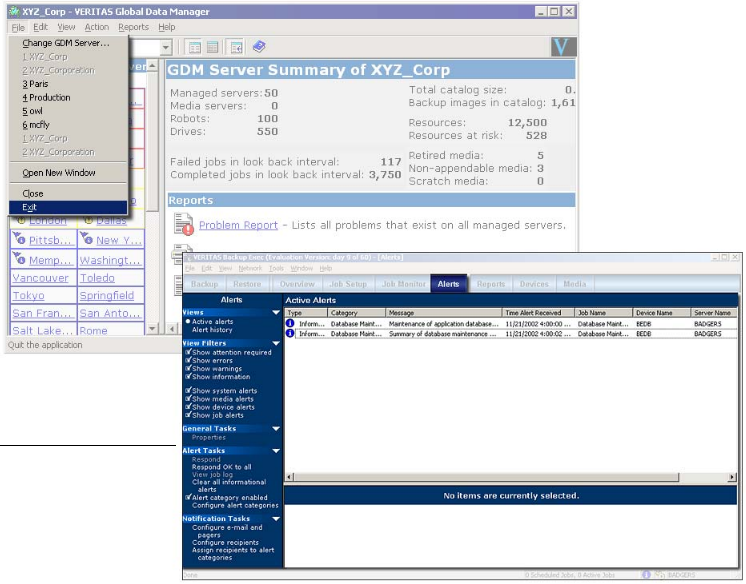
Windows Dashboard and Administration Console Exit Behavior

Windows-based GDM Dashboard

Selecting **Exit** here closes the Windows version of the GDM Dashboard and all secondary GDM Dashboard windows...

... but it does NOT close the Backup Exec 9.0/9.1 Remote Administrator console.

The console remains running, as it is an independent application



GDM Server Summary of XYZ_Corp

Managed servers: 50
Media servers: 0
Robots: 100
Drives: 550
Total catalog size: 0.
Backup images in catalog: 1,61
Resources: 12,500
Resources at risk: 528
Failed jobs in look back interval: 117
Completed jobs in look back interval: 3,750
Retired media: 5
Non-appendable media: 3
Scratch media: 0

Reports

Problem Report - Lists all problems that exist on all managed servers.

Active Alerts

Type	Category	Message	Time Alert Received	Job Name	Device Name	Server Name
Inform...	Database Maint...	Maintenance of application database...	11/21/2002 4:00:00 ...	Database Maint...	BEDB	BADGERS
Inform...	Database Maint...	Summary of database maintenance ...	11/21/2002 4:00:02 ...	Database Maint...	BEDB	BADGERS

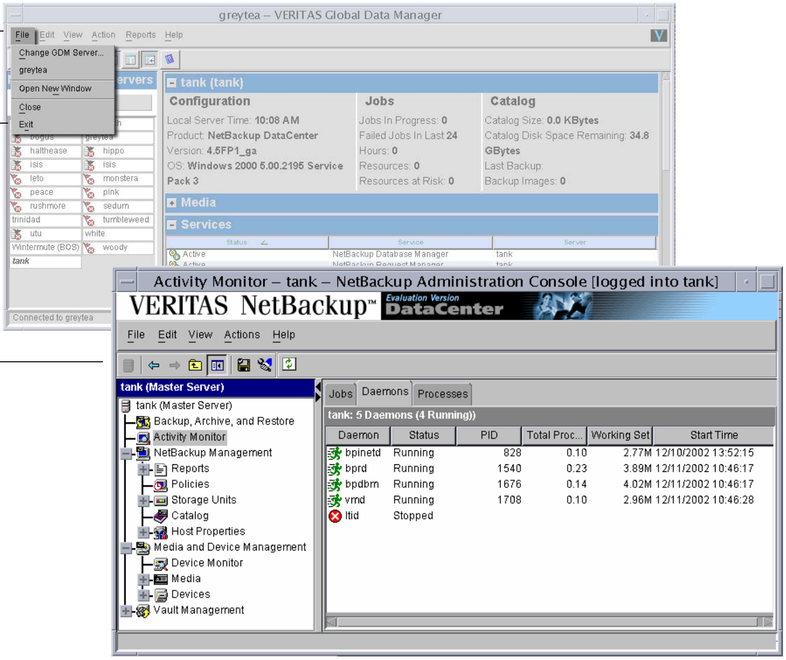
Backup Exec 9.0/9.1 Remote Administration Console

Note With the Windows-based version of GDM Dashboard, you are limited to launching a single instance of the Dashboard using the Windows **Start** button. To open multiple instances, you must use the **Open New Window** option on the GDM menu bar (**File** > **Open New Window**).

Java Dashboard and the NetBackup Administration Console

Unlike the Windows Dashboard, launching an administration console *through* the Java version of the Dashboard opens a NetBackup Administration Console as a *dependent* application to the Java Dashboard. In other words, when launched from the Java Dashboard, the NetBackup Administration Console becomes a part of the overall Java Dashboard process. As such, the NetBackup Administration Console's exit behavior falls under the control of the Java Dashboard. When you use the **Exit** option to shut down all secondary Java Dashboard windows, and the Java Dashboard itself, the NetBackup Administration Console *is also* shutdown.

Java Dashboard and the NetBackup Administration Console Exit Behavior



Java-based GDM Dashboard

Selecting **Exit** here closes the Java version of the GDM Dashboard and all secondary GDM Dashboard windows...

... while also closing the Netbackup Administrator Console.

If the NetBackup Administration Console is launched from within the Java Dashboard, it becomes part of the Java Dashboard process and falls under the control of the Dashboard's **Exit** option.

greytea – VERITAS Global Data Manager

tank (tank)

Configuration
Local Server Time: **10:08 AM**
Product: **NetBackup DataCenter**
Version: **4.5FP1_ga**
OS: **Windows 2000 5.00.2195 Service Pack 3**

Jobs
Jobs In Progress: **0**
Failed Jobs In Last **24** Hours: **0**
Resources: **0**
Resources at Risk: **0**

Catalog
Catalog Size: **0.0 KBytes**
Catalog Disk Space Remaining: **34.8 GBytes**
Last Backup:
Backup Images: **0**

Status	Service	Server
Active	NetBackup Database Manager	tank
Active	NetBackup Request Manager	tank

Connected to greytea

Activity Monitor – tank – NetBackup Administration Console [logged into tank]

tank: 5 Daemons (4 Running))

Daemon	Status	PID	Total Proc...	Working Set	Start Time
bpinetd	Running	828	0.10	2.77M	12/10/2002 13:52:15
bprd	Running	1540	0.23	3.89M	12/11/2002 10:46:17
bpdbm	Running	1676	0.14	4.02M	12/11/2002 10:46:17
vmd	Running	1708	0.10	2.96M	12/11/2002 10:46:28
ltid	Stopped				

Window Reuse

After launching an administration console, GDM manages the open NetBackup or Backup Exec Administration Console windows in different ways. Wherever possible, GDM re-uses the existing administration console window after the administration console has been launched, in order to minimize window proliferation and memory consumption.

Use the information in the following table as a guide.

Administration Console Window Reuse Properties

Administration Console Window Reuse Properties

Dashboard Version	Administration Console	Reuse Properties
Windows Dashboard	**Backup Exec 8.6 Administration Console**	◆ Only one instance of the Backup Exec 8.6 Administration Console can be open at one time. If the Backup Exec 8.6 Administration Console is running, launching additional instances will simply make the existing administration console window the active window. Additional instances will not be launched. You must close the administration console before you can launch it again, or change the desired context in the Backup Exec Administration Console itself. ◆ If the Backup Exec 8.6 Administration Console is *not* running, launching the administration console from the Dashboard will open an administration console window for the target managed server, in the corresponding context. Refer to the table, "Administration Console Launch Contexts" on page 117
Windows Dashboard	**Backup Exec 9.*x* Administration Console**	◆ Multiple Backup Exec 9.*x* Administration Console windows can be opened at one time. ◆ Each launch of the Backup Exec 9.*x* Administration Console opens a new administration console window for the target managed server in the corresponding context. Refer to the table, "Administration Console Launch Contexts" on page 117. ◆ An existing Backup Exec 9.*x* Administration Console window is never re-used for during subsequent launches of additional instances of the Backup Exec Administration Console.

Administration Console Window Reuse Properties

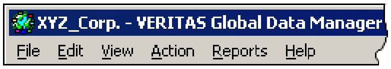
Administration Console Window Reuse Properties

Dashboard Version	Administration Console	Reuse Properties
Windows Dashboard	**NetBackup Administration Console**	◆ Multiple NetBackup Administration Console windows can be opened at one time. ◆ If a NetBackup Administration Console window is already open for the target managed server in any context within the same Java Dashboard process, another launch of the administration console will re-use the existing window without opening a new one. If the context is different, the context in the existing administration console window changes accordingly. **Note** If the existing window is blocked, such as with a dialog box waiting for user input, a new window will be created.
Java Dashboard	**NetBackup Administration Console**	◆ Multiple NetBackup Administration Console windows can be opened at one time. ◆ If a NetBackup Administration Console window is already open for the target managed server in any context within the same Java Dashboard process, another launch of the administration console will re-use the existing window without opening a new one. If the context is different, the context in the existing administration console window changes accordingly. **Note** If the existing window is blocked, such as with a dialog box waiting for user input, a new window will be created.

GDM Menu Bar

GDM Dashboard's Menu bar offers the following selections: File, Edit, View, Action, Reports, and Help.

GDM Menu bar



File

The following commands are found under the File menu.

File Menu Commands

Change GDM Server	Enables you to specify and connect to a different GDM Server.
<Previous GDM Servers>	Displays a list of the last four previously monitored GDM Servers.
Open New Window	Enables you to open a new window, allowing you to simultaneously monitor multiple managed servers, or configure additional views of a single managed server's information.
Close	The GDM Dashboard interface is designed to enable you to open additional GDM Dashboard windows, allowing you to monitor multiple managed servers simultaneously. Although new windows are separate entities when viewed on-screen, they are not separate applications. All secondary windows opened from the original instance of the Dashboard remain under the control of the Dashboard, specifically the File options, **Close** and **Exit**. The Close option enables you to close secondary GDM Dashboard windows without exiting GDM. When selecting the Close option on an active secondary GDM window, only the active window closes. All other secondary windows, along with the original instance of GDM, remain open.
Exit	The Exit option enables you to shut down the GDM Dashboard, simultaneously closing all secondary windows and shutting down GDM Dashboard simultaneously.

Edit

The following commands are found under the Edit menu.

Edit Menu Commands

General Properties

Enables you to configure or modify managed server and failure threshold properties for managed servers. For more information, see "GDM Advanced Configuration" on page 41.

Data Collection (includes Look Back Interval and Sample Rate)

Data collection settings control how often a managed server's environment is examined. These settings also govern the amount of prior job activity displayed and analyzed for problem conditions.

Data collection settings that can be adjusted include Look Back Interval and Sample Rate.

Look Back Interval is the number of hours of prior job activity that GDM examines. This setting determines the amount of job history that is displayed and analyzed for problems such as high job failure rates and resources at risk

Sample Rate is the setting GDM uses to poll managed servers for data. A scale between 1 and 90 minutes is used, where 1 represents the highest data refresh rate and high CPU usage, and 90 represents the lowest data refresh rate and the lowest CPU usage. The Sample Rate should be adjusted if the managed server seems sluggish while data collection is occurring.

Dashboard Port Settings

(Windows platforms only)

Used in firewall environments. If the GDM Server sits behind a firewall that does not include other GDM servers or managed servers in the GDM domain, you can specify a range of port addresses for listening to communications from the systems outside the firewall.

Note This option only appears if NetBackup is *not installed* on the computer where the Dashboard is installed. If NetBackup is installed, the port settings are configured using the NetBackup Administration Console.

View

The following commands are found under the View menu.

View Menu Commands

Sort by Name	Enables you to sort the left pane by managed server name.
Sort by Status	Enables you to sort the left pane according to the status of error conditions on the managed server.
Ascending	Enables you to sort the managed server list in ascending, alphabetical order.
Descending	Enables you to sort the managed server list in descending order.
View as Grid	Enables you to view the managed server list using individual grid rows and columns.
View as List	Enables you to view the managed server list using as a list, rather than as a grid.
Grid Columns	Enables you to set the number of grids columns to use when viewing the managed list as a grid. Grids can be divided using 1, 2, 3, or 4 columns, with 2 columns being the default.
Managed Servers	Toggle switch used to display the managed server list in the left pane.
Toolbar	Toggle switch used to display the GDM Toolbar.
Status Bar	Toggle switch used to display the GDM Status bar
Refresh **(Windows Dashboard only)**	Used to refresh the GDM interface.
Transpose **(Server Summary grid only)**	**Note** Transpose can only be activated from the shortcut menu launched from the Server Summary grid. Used to organize the order of the sort operation selected under the View menu. For example, the sort order can be organized vertically from the top of the GDM Summary pane to the bottom. Or the sort order can be organized horizontally, from the left to the right. To activate the Transpose feature, mouse over the Server Summary pane on the left side of the GDM Dashboard and then select **Transpose** from the shortcut menu that appears.

View Menu Commands (continued)

Open in New Window (Server Summary grid only)	**Note** **Open in New Window** can only be activated from the shortcut menu launched from the Server Summary grid. Used to view a specific managed server in a secondary GDM Dashboard window. To activate the Open in New Window feature, mouse over a specific managed server for which you want details on in the Server Summary pane on the left side of the GDM Dashboard. Then right-click and select **Open in New Window** from the shortcut menu that appears. **Note** **Open in New Window** can only be activated from the shortcut menu launched from the Server Summary grid.

Action

The Action menu contains the following commands:.

Action Menu Commands

Administer	Enables you to launch the NetBackup Administration Console or the Backup Exec Administration Console from within GDM.

Reports

Launch the following reports from the Reports menu:.

Available Reports

Problems Report	Displays a report that lists all problems that exist on monitored managed servers in the system.
Drive Status Report	Displays a report that shows the current status of all the drives in the system.
General Status Report	Displays a report that lists general status of all managed servers in the GDM domain.

Help

The following Help topics can be found under the Help menu.

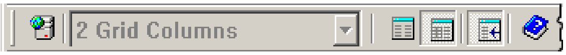
Help Menu Topics

Help topics	Access help through the GDM Help engine.
VERITAS Web Page (GDM Windows Dashboard only)	Access the VERITAS web site at http://www.veritas.com.
About GDM Dashboard	Displays version and copyright information about GDM.

GDM Toolbar

GDM Dashboard's Toolbar contains the following selections: **Change GDM Server**, **Grid Column Adjustments** (using both list box and button technologies), and **About GDM**.

GDM Toolbar



Change GDM Server Button

Use the **Change GDM Server** button to quickly change GDM Servers.

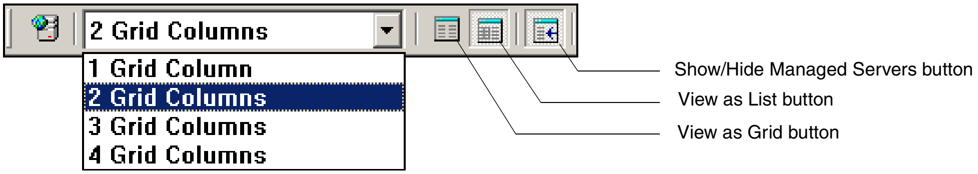
▼ **To change GDM Servers**

1. Click the **GDM Server** button from the GDM Toolbar.
2. Enter a GDM Server name (or its IP address), or select from a list of GDM Servers that have been previously monitored using Dashboard.
3. Click **OK**.

Changing Grid Columns

Although the Dashboard's left pane defaults to using a two column format, you can change the number of grid columns that appear by using the **Grid Columns** list box.

Grid Column Selection Box



▼ **To change the number of grid columns**

1. Click the **Grid Columns** list box.
2. Click the number of columns you want to use.

View As List Icon

The **View As List** button changes the left pane from a column-based view to a list-based view.

▼ To view the left pane in a list format

- ❖ Click the **View as List** button.

  The left pane changes from a column-based view to a list-based view.

View As Grid Icon

The **View As Grid** button changes the left pane from a list-based view to a column-based view.

▼ To view the left pane in a column format

- ❖ Click the **View as Grid** button.

  The left pane changes from a list-based view to a grid-based view.

Show/Hide Managed Servers Icon

The **Show/Hide Managed Servers** button is a toggle button that either displays or hides Dashboard's left pane.

▼ To show/hide the left pane

- ❖ Click the **Show/Hide** button.

  The left pane is either hidden from view or displayed.

About GDM

The **About** button, in the form of a blue book, displays information about GDM Dashboard.

▼ For GDM Dashboard information

- ❖ Click the **About** button.

GDM Usage Scenarios

This section offers insights on how GDM is typically used. The information is presented in a Frequently Asked Questions format.

I have just started GDM Dashboard. Where do I start?

Workflow for the GDM Dashboard normally starts in the left side of the application, in the Managed Servers pane. This pane presents a quick visual overview of the immediate status of your GDM domain. If there are visual indicators present (color/flags), you can click a managed server showing the indicator to gain more details about the issues that have been detected. These summary details are displayed in the right pane.

I would like to see a consolidated list of all the problems shown in the ToolTips that appear when I hover the cursor over the managed server in the left pane. Where do I do this?

GDM has a report that displays all the problems shown in the Tooltip. Go to the **Reports** menu and select the **Problems** report.

I would like to know how many failed jobs occurred at a managed server. How do I do it?

In the left pane, click a managed server name for which you'd like information about failed jobs. Details for that managed server appear in the right pane. At the top of the pane, under the Jobs column, the number of failed jobs appears as part of the overall job information presented. For additional details, expand the Jobs detail section in the right pane. You can filter the section for all failed jobs to gain additional information.

For more information, see "Jobs Details" on page 100.

I have noticed in the Robot detail sections of a particular managed server, the LED graphic indicates two drives are down. How do I find out more details?

Expand the **Robot** details section and then click the sort control in the **Status** column to quickly find the drives that are down.

I have configured multiple GDM domains. How do I monitor the managed servers in those other domains?

In order for GDM Dashboard to monitor managed servers in your other domains, you must point Dashboard to the GDM Server of the other domain. Only then can GDM Dashboard successfully monitor managed servers in other domains.

For details on changing GDM Servers, see "Monitoring Other GDM Domains" on page 38.

GDM Reports 6

This section provides information on GDM reports.

Reports includes the following topics:

Section	Description
"Generating and Viewing Reports" on page 134	Describes the GDM-generated reports that show detailed information about your managed servers.
"Printing Reports" on page 134	Describes how to print GDM reports.
"Problem Report" on page 136	Describes the Problem report.
"Drive Status Report" on page 137	Describes the Drive Status report.
"General Status Report" on page 138	Describes the General Status report.

Generating and Viewing Reports

GDM Dashboard generates reports that show detailed information about your managed servers. Data appearing in each report is dynamically culled from the GDM Server database at the time the report is requested, thus presenting you with a "snapshot in time" view of your enterprise.

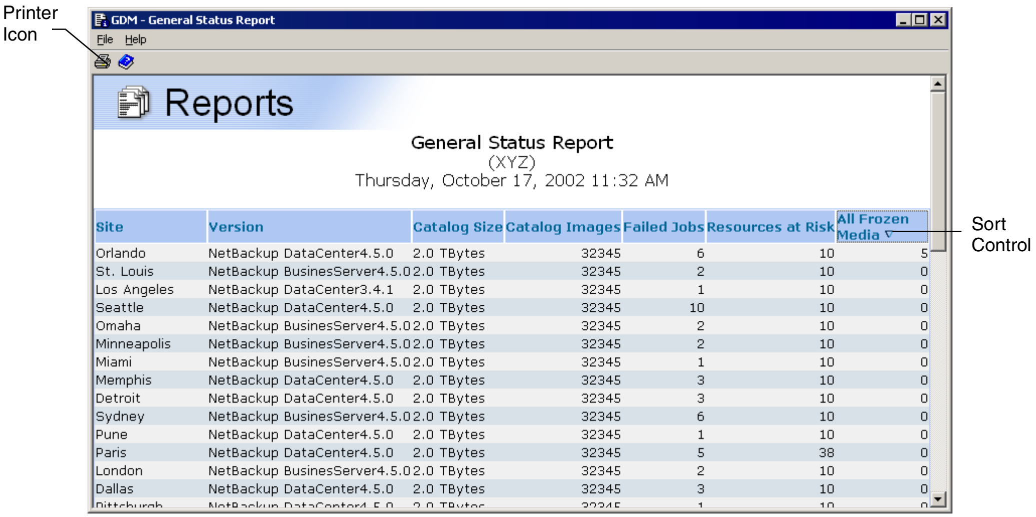
For environments that require additional reporting capabilities, including the generation of historical reports, the NetBackup Advanced Reporter option is recommended.

You can view Dashboard reports by launching them from either the GDM Server Summary page in the right pane, or from the Reports selection on the menu bar.

After launching a report, Dashboard creates a secondary window that contains the report.

Note Clicking a report's column head activates a **Sort** control, allowing you to sort column information in ascending and descending order.

Secondary Dashboard Sample Report Window



General Status Report
(XYZ)
Thursday, October 17, 2002 11:32 AM

Site	Version	Catalog Size	Catalog Images	Failed Jobs	Resources at Risk	All Frozen Media ▿
Orlando	NetBackup DataCenter4.5.0	2.0 TBytes	32345	6	10	5
St. Louis	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	2	10	0
Los Angeles	NetBackup DataCenter3.4.1	2.0 TBytes	32345	1	10	0
Seattle	NetBackup DataCenter4.5.0	2.0 TBytes	32345	10	10	0
Omaha	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	2	10	0
Minneapolis	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	2	10	0
Miami	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	1	10	0
Memphis	NetBackup DataCenter4.5.0	2.0 TBytes	32345	3	10	0
Detroit	NetBackup DataCenter4.5.0	2.0 TBytes	32345	3	10	0
Sydney	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	6	10	0
Pune	NetBackup DataCenter4.5.0	2.0 TBytes	32345	1	10	0
Paris	NetBackup DataCenter4.5.0	2.0 TBytes	32345	5	38	0
London	NetBackup BusinesServer4.5.0	2.0 TBytes	32345	2	10	0
Dallas	NetBackup DataCenter4.5.0	2.0 TBytes	32345	3	10	0
Pittsburgh	NetBackup DataCenter4.5.0	2.0 TBytes	32345	1	10	0

Printing Reports

In addition to viewing default Dashboard reports, you can also print them.

Note Depending on the version of the Dashboard that you are using, a default printer for either the Windows or UNIX operating systems must be configured to properly print the integrated GDM Dashboard reports.

▼ To print a report

1. Launch a report.

2. In the report window, click the printer icon on the report window tool bar.

3. Select a printer and then click **OK**.

Default Reports

The following reports are generated by GDM Dashboard:

- Problem Report
- Drive Status Report
- General Status Report

Problem Report

The Problem report lists all problems and conditions that exist on all managed servers. Along with the following columns, the report also displays the date and time the report is generated.

Problem Report Column Descriptions

Field	Description
Status (Windows Dashboard only)	The operational status of the managed server named in the **Server** column. Statuses include Critical, Warning, and Informational.
Server	The user-defined name given to the managed server being monitored by Global Data Manager. For example, *Atlanta*.
Problem or Condition	The problem or condition that is affecting the managed server.
Local Time	The local time where the managed server is physically located.

Drive Status Report

The Drive Status report lists the current status of all drives in the system. Along with the following columns, the report also displays the date and time the report is generated.

Drive Status Report Column Descriptions

Field	Description
Status	The status of drives at the managed server named in the Server column. Statuses include: ◆ Warning (a high percentage of drives are down) ◆ Informational (more than one drive is down, but not more than the error threshold) ◆ Unknown (the managed server is unreachable), and Okay (no drives are down).
Server	The user-defined name given to the managed server being monitored by Global Data Manager. For example, *Atlanta*.
Total Drives	The total number of drives being managed by the managed server named in the Server column.
Offline Drives	The total number of drives being managed by the managed server named in the Server column that are presently offline.
Active Drives	The total number of drives being managed by the managed server named in the Server column that are presently in an active state.
Inactive Drives	The total number of drives being managed by the managed server named in the Server column that are presently inactive.
Jobs in Progress	The total number of jobs that are in progress and that are being monitored by the managed server named in the Server column.

General Status Report

The General Status report provides general status information about all managed servers being monitored in the system.

General Status Report Column Descriptions

Status	Description
Server	The user-defined name given to the managed server being monitored by Global Data Manager. For example, *Atlanta*.
Version	The version of NetBackup or Backup Exec installed at the managed server. The version information includes the product name and the version number.
Catalog Size	The total size of the catalogs being stored, in megabytes (MB).
Catalog Images	The number of images inside the catalogs.
Failed Jobs	The number of jobs that failed during the past 24 hours.
Resources at Risk	The total number of resources that have not been backed up in a predetermined time.
Retired Media	The number of media that are considered to be retired.

Troubleshooting GDM 7

This section provides the information you need to:

- Find answers to frequently asked questions about Global Data Manager.
- Troubleshoot and solve errors that you may encounter.

I started GDM Java Dashboard but the GUI doesn't display. What's the problem?

If you are running the Java-based Dashboard, the output from the gdmSA startup script will give the full pathname to the log file. Peruse the contents of the log file.

A common problems can include not setting the correct display variable (solution: use the "-d hostname:0" option to gdmSA),

To get more verbose output, turn on logging for the Java GUI: "gdmSA --debug" and it will put verbose debugging output to the log file name displayed in first lines of output.

I try to start the GDM Windows Dashboard but it fails with an error message stating that Microsoft Internet Explorer 5.5 is not installed. Why do I need IE 5.5?

To display its graphical user interface, the GDM Windows Dashboard uses technical components introduced in Internet Explorer 5.5. Upgrade to Internet Explorer 5.5 and then try restarting GDM Dashboard.

The GDM Dashboard starts, but an error message appears stating that the Dashboard is unable to connect to the GDM Server. Why?

Verify that you are not having network connection problems. Can the console system reach the GDM server using ping?

Verify that the system you are connecting to is really the GDM Server. Does it have the GDM Server license installed? Go to that system and ensure that you have installed/activated the GDM Server license. Then restart the visd daemon on UNIX or the VERITAS GDM Information Server service under Windows.

Verify that the visd daemon or the VERITAS GDM Information Server service is running on the GDM Server. The GUI retrieves GDM information from the GDM Server by connecting to the visd daemon or the GDM Information Server service.

- On UNIX, run the `/usr/openv/netbackup/bin/bpps` command to see if the visd daemon is listed (NetBackup only).
- On Windows NT and Windows 2000, use the Service Control Manager to verify the VERITAS GDM Information Server service is running.

I have the GUI running, but there are no managed servers shown in the left pane. Why?

Make sure you configured the list of managed servers. Refer to "GDM Configuration Overview" on page 33 for instructions on how to create and modify the list.

Also make sure that you selected the GDM server and not one of the managed servers. The GDM domain list is maintained on the GDM Server, not any of the managed servers.

Note It is important that you do not configure a GDM domain on a managed server as this will create cross-membership managed servers belonging to more than one GDM domain and therefore being monitored by more than one GDM Server. It is highly recommended that you ensure that only one server, the GDM Server, is configured to have a list of managed servers. To do otherwise will introduce inefficiencies in your system and lead to CPU and memory waste.

When I look at the GUI, the list of managed servers shows the same server twice. What happened?

When you modify the list of managed servers, GDM will prevent the addition of duplicate entries. Nonetheless, it is possible if more than one user is modifying the list at the same time, or if visd is quickly shut down and restarted, that the list is not properly synchronized in the database and in the registry (or bp.conf on Unix systems) where it is mirrored. To correct the situation, delete both duplicate server entries and re-add one entry again. It is important to completely remove all duplicate entries instead of deleting all but one. One of the entries will have important unique identifying information that the other entries will not. Since you will be unable to determine which is the true and complete entry, it is best to delete all and let the system re-initialize that information when you add a fresh entry for the server.

One of the managed servers has a red flag and the error message saying that it is unreachable. Why?

- Verify that you are not having network connection problems. Using a utility like ping, verify that the GDM Server can reach the managed server.
- Verify that the managed server has the GDM managed server license installed.
- Verify that the visd daemon or the VERITAS GDM Information Server service is running on the managed server. The GDM Server visd communicates with the managed servers visd to get information about the managed server.

- On UNIX, run the `/usr/openv/netbackup/bin/bpps` command to see if the visd daemon is listed.
- On Windows NT and Windows 2000, use the Service Control Manager to verify the VERITAS GDM Information Server service is running.

When I look at a managed server view, there is no data. I do not see information about the jobs, media, services, etc. Why?

Is the fully qualified domain name for the managed server correct? That name appears in the horizontal bar next to the display name. For example, *Atlanta (master.server.com)*. Perhaps the managed server name is incorrect.

Verify that the data collector is running on the managed server. If data collection is inactive on the managed server, then you should see an error flag next to the managed server name in the grid. If you see some data, but not all, then you may have the data collection interval set too infrequently.

For more information, refer to "GDM Advanced Configuration" on page 41.

If none of the above troubleshooting tips results in data appearing for the server, the next step is to turn on logging on the GDM Server. If the problem pertains to a managed server, then you also need to turn logging on at the managed server.

For more information, refer to "Enabling GDM Logging" on page 62.

After you enable logging and restart visd, the first log file you should view is the `gdm_visd` log file.

The following list describes some of the problems you can detect by examining the `gdm_visd` log:

- A module failed to load.

  GDM components are contained within loadable modules. When the visd starts, it loads key modules. If a module fails to load, the `gdm_visd` log file will report the error and identify the module. From there you go to the log file corresponding to the module. Critical errors during module loading will also be recorded in the event log on NT and the syslog on Unix.

- Unable to connect to a managed server.

  If you can run the Dashboard and see a managed server, but no data exists for the managed server, then the `gdm_mastmon` log file will disclose errors with data rollup from the managed server to the GDM Server.

- No data appears.

  First, determine if you are missing data from only one server or from more than one server. If no data at all appears, it is likely a problem on the GDM server with the data rollup procedure. Look at the `gdm_visd` and `gdm_mastmon` log files.

If data is missing for a subset of servers, then it is more likely that the rollup is working since data from other managed servers is visible. The problem probably exists on the managed servers. Go to those particular server log files, specifically the `gdm_visd` and `gdm_collector` directories. The `gdm_mastmon` log file is not applicable on a managed server.

Data does not appear to be updating on the screen and the Dashboard interface appears unresponsive. What could be happening?

Verify that you have not run low on disk space or memory. If you have turned on logging and are not pruning the log files, it is easy to run out of space fairly quickly. Make sure you have logging turned on only for a short time to diagnose a specific problem, and then turn it off. Also, make sure there is enough space on the disk. If GDM is unable to write to its database because there is not enough space to grow then it may become unresponsive. The size of the GDM database is largely governed by the amount of data in the look back interval. In other words, how you set the Data Collection setting for the time period in which to analyze backup activity. For example, the previous 24 hours versus the previous 48 hours determines how much job activity to save and analyze. However, the data GDM saves is minimal in relation to the data that NetBackup stores about jobs, images and media. In addition, the GDM database does not store historical data; therefore it will not grow over time like the NetBackup Advanced Reporter database.

The Local Server Time for a remote server shown in the GDM Dashboard is off by several minutes from the local time on that server. Why?

The time setting on the remote server may be off by a few minutes from the wall clock time. Local Server Time is derived by using the local time and time zone of the Dashboard host computer and then applying a Greenwich Mean Time (GMT) offset to the GDM managed servers.

The GDM Dashboard shows the wrong Local Server Time for all managed servers in my GDM domain. Why?

Either the time or the time zone setting on the dashboard host is wrong. In that case, the Local Server Time will be incorrect for all managed servers, and the Local Server Time for managed servers that are in the same time zone as the dashboard host will appear to have the same time as the dashboard host. The reason for this is because Local Server Time is derived by using the local time and time zone of the Dashboard host computer and then applying a Greenwich Mean Time (GMT) offset to the GDM managed servers. To resolve, ensure the time and time zone setting on the dashboard host machine is correct.

The GDM Dashboard shows the same Local Server Time for one or more managed servers, which does not match the actual time on those managed servers. Why?

Either the time or the time zone setting on the dashboard host is wrong. In that case, the Local Server Time will be incorrect for all managed servers, and the Local Server Time for managed servers that are in the same time zone as the dashboard host will appear to have the same time as the dashboard host. The reason for this is because Local Server Time is derived by using the local time and time zone of the Dashboard host computer and then applying a Greenwich Mean Time (GMT) offset to the GDM managed servers. To resolve, ensure the time and time zone setting on the dashboard host machine is correct.

The error, "Cannot connect to the database server" appears in the visd Syslog or the Windows event log. What is happening?

The Information Server (`visd`) requires the Persistent Store (`nbdbd`) daemon/service to be active. If the `nbdbd` daemon is unavailable, then the GDM collector will shut down because it is unable to store collected data. The message you will see in the `visd` syslog or event log output is: NetBackup Data Collector: Maximum number or restarts exceeded, shutting down…

On Windows systems, the Information Server will also generate an event (Event ID of 100 in source NetBackup GDM PSODBC) in the Event Log. The description will contain the sentence **Cannot connect to the database server**. When verifying the availability `nbdbd`, also check that `nbdbd`'s port number is not in use by another application.

My Java Dashboard performance seems sluggish. Why?

Java Dashboard performance depends upon the console system's environment. The default configuration, specifically the INITIAL_MEMORY and MAX_MEMORY options within the gdm.conf file, assumes sufficient memory resources on the machine you execute the `gdmSA` command. To ensure satisfactory performance, run `gdmSA` on a 512 MB machine that has at least 128 MB of RAM available to the application.

I would like to use the Java Dashboard in a remote environment. Are there any things I should be aware of?

On many Unix systems, cross-platform display fails for graphical interface applications. Therefore, VERITAS does not recommend displaying the Java Dashboard remotely back to a different platform type from the one where the application was started. For example, if you execute `gdmSA` on an HP 11.0 computer, you should not use the DISPLAY environment variable (or `gdmSA`'s `-d` display option) to display back to a Solaris computer.

Does the Java Dashboard track events in a log file?

To better facilitate getting support information for problems you may experience with the Java Dashboard interface, the application startup script (`gdmSA`) writes a log file by default to `/usr/openv/java/logs`. There is one log file for every instance of the Java Dashboard. Normally these log files are not large (less than 2 KB). However, periodic pruning of the files in this directory is recommended.

On my Tru64 system, text does not appear correctly in the Java Dashboard. Why?

On Tru64 systems, text in the Java Dashboard interface may appear irregularly sized causing parts of the words or letters to be slightly cropped. This is due to font sizing problems on the Alpha platform.

visd-related Questions

This section focuses on visd questions only.

When I start GDM Dashboard, I receive a message stating that GDM cannot connect to the GDM Server. Why?

It's possible that neither the NetBackup Database or the VERITAS GDM Information Server service or visd daemon has started on the GDM Server. If one or the other fails to start, a connection to the GDM Server will not be successful.

I want to stop the visd daemon on my UNIX platforms. What is the best method for stopping it?

On UNIX platforms use `kill -9` command to stop `visd`. `visd` does not always stop when the `kill` command with `-INT`, `-TERM`, or `-HUP` option is used. Make sure that only one `visd` process is running at one time.

I start visd but it terminates soon afterwards. Why?

Verify that a GDM license key is installed; visd shuts down if it does not see a GDM Server or GDM Managed Server license key. Before shutting down, a message will be logged. A quick way to determine if licensing is the problem is to start visd manually with verbose logging output.

For more information, refer to "Enabling GDM Logging" on page 62.

▼ To start visd manually on UNIX

❖ At a command prompt, enter:

```
$ /usr/openv/netbackup/bin/initvisd -console -debug
```

▼ To start visd manually on Windows

1. Open a command prompt.

2. Enter the following:

```
c:\Program Files\VERITAS\GDM\bin\visd -console -debug
```

Common Terminology A

The following NetBackup and Backup Exec terms are used interchangeably in GDM.

Common Term	As used in NetBackup	As used in Backup Exec	Term Description
Appendable	Active media	Appendable media	Media state representing media on which data can be appended.
Automatic Media Recognition	Automatic Volume Recognition (AVR)	Inventory	The process of determining the type of media being used in a storage device, and what type of formatting the media uses when data is written to it.
Backup Images	Images	Backups	A process where files on a server or workstation drive are copied and stored on a reliable form of media.
Cancel	Cancel, Kill	Abort	Action taken to prematurely halt a job or procedure.
Device	Device, Robot, Drive	Device, changer, Drive	Robotic library or drive hardware.
Disabled	Down	Disabled	Object state where the object is not used.

Common Term	As used in NetBackup	As used in Backup Exec	Term Description
Drive	Drive	Drive	Device capable of data storage, optionally allowing removable media.
Drive Pool	Storage unit	Drive pool	A user-defined logical grouping of devices used as a target for assigning jobs.
External Media Label	Media ID, EVSN	Cartridge label	Visually-based identifier used for differentiating between physical media.
Import/Export	Inject/Eject	Import/Export	Action where media is moved into or out of a robotic library through a media access port.
Library Type	Robot Type	Changer Type	Identifier for a class of robotic libraries, for example.
Media	Media, Media ID, Volume	Media, Cartridge	Physical media used for data storage, which includes tape, optical disks, and hard disks.
Media Access Port	Entry Port, Exit Port, Import, Outport, Mailslot	Portal Slot, Media Import/Export Mailslot	Physical mechanism or library slot range used for moving media into or out of a robotic library.
Media and Device Management	Media and Device Manager	ADAMM (Advanced Device and Media Management)	A component of both NetBackup and Backup Exec responsible for media management.
Media Description	Volume Description	Alternate Label	User-defined text for identifying media or media-specific attributes or contents.

Common Term	As used in NetBackup	As used in Backup Exec	Term Description
Media Pool	Volume Pool	Media Pool, Media Set	Groups of media sharing common attributes.
Media Server	Media Server, Device Host	Media server	A machine, or host computer used for data storage or management of data storage.
Media Type	Media Type, Density	Cartridge Type, Media Type	Identifier for a class of media. For example, DLT or AIT.
Non-appendable Media	Suspended	Not Appendable	Media on which data cannot be appended. In Backup Exec, the term non-appendable means that data cannot be appended to a tape due to reasons such as the tape being full or the expiration of the time allocated to appending data to tape.
Offline	DOWN	Offline	The object is not functioning normally and is not available.
Online	Up, AVR, OPR	Online	The object is functioning normally and can be used.
Paused	Paused	Paused	The object is functional but its use has been suspended by an operator.
Recorded Media Label	Volume Label, Volume Header, Media ID, RVSN	Media Label	An identification label written to the media by NetBackup and Backup Exec, which is used to track media usage.

Common Term	As used in NetBackup	As used in Backup Exec	Term Description
Recyclable	Expired	Recyclable	Media whose retention periods have expired and are now eligible for reuse.
Remote Administration clients	Remote Administration Console	Remote Administrator	The Backup Exec or NetBackup user interface (administration console) that runs on remote Windows computers.
Remote media server	media server	media server	A media server that is not the NetBackup master. **Note** Only NetBackup Enterprise Server supports remote media servers. NetBackup Server supports only a single server, which is the NetBackup master.
Resource	Client	Resource	An entity that is backed up. It can be a client, a disk, a database and so on.
Retired (media)	Frozen (media)	Retired (media)	A piece of media that has been removed from active use due to age issues.

50304

Index