VERITAS NetBackup™ 4.5
Global Data Manager

System Administrator's Guide

for UNIX and Windows

March 2002
30-000514-011

VERITAS

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.

Copyright

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

Contents

Using Global Data Manager 4.5 Documentation

This comprehensive manual provides detailed information and procedures for using Global Data Manager 4.5. Topics covered in this manual require the reader to have a working knowledge of the Windows NT/2000 and UNIX-based operating environments.

Understanding Documentation Conventions

The following documentation conventions are used throughout this manual.

Steps	Numbered steps are listed as 1., 2., ...etc.
Text that you type	Text that you are required to type on the keyboard is shown in a lowercase font similar to what you would see on your screen. The text to be typed is preceded by the word Type and followed by the key(s) to press: For example, Type: a:install and press <Enter>.
Keys	Keys appear in angle brackets (< >). For example, <Enter>, <Esc>, <Del>, etc. When two or more keys need to be pressed simultaneously to perform a function, they appear in angle brackets with a plus sign. For example, <Shift + F1>.
Hot keys or accelerator keys	If there is a shortcut key, it is shown in the application next to the menu choice. If there is a toolbar button or another shortcut, it will be noted in the documentation as a tip.

Understanding Manual Organization

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

Chapter 1	"Introducing Global Data Manager 4.5" contains general information about Global Data Manager, how Global Data Manager works, and what it can do for you.
Chapter 2	"Installation and Configuration" includes information about hardware and software requirements and instructions on performing the initial configuration of Global Data Manager.
Chapter 3	"Advanced Configuration"presents steps for making advanced configuration adjustments to Global Data Manager 4.5.
Chapter 4	"Using GDM" explains the GDM Dashboard interface. This chapter also explains how to use the Dashboard when monitoring your GDM domain.
Chapter 5	"Reports" includes information about the types of reports available through the GDM Dashboard.
Chapter 6	"Special Limitations" discusses changes to the GDM 4.5 product that have occurred since the previous release.
Chapter 7	"Troubleshooting FAQ" discusses solutions to issues that you may encounter using Global Data Manager 4.5.
Glossary	

Using Global Data Manager 4.5 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:

1. 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.

2. 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).

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

   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 4.5 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)**	Allows you to search the Help system for specific words and phrases.

Introducing Global Data Manager 4.5 1

This section provides an overview of the NetBackup Global Data Manager 4.5 and its features.

Introducing Global Data Manager 4.5 includes the following topics:

Section	Description
"Introducing Global Data Manager 4.5" on page 1	Describes a general overview of the Global Data Manager 4.5.
"Understanding GDM" on page 4	Describes how GDM works and its use of visual keys within the graphical user interface.

Introducing Global Data Manager 4.5

VERITAS Global Data Manager 4.5 is an advanced, high-performance monitoring application that works in conjunction with your installed base of NetBackup BusinesServer and DataCenter master servers, allowing you to quickly view in real time the operational status and health of your distributed data protection environment.

Using both icons and color, GDM allows you to quickly isolate NetBackup 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 NetBackup 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 VERITAS NetBackup BusinesServer™ and VERITAS NetBackup DataCenter™ are used to protect the data. As your investment in these two products grows, you may find the need to monitor multiple NetBackup 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 NetBackup 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 would have to be determined by physically being at each server.

Additional benefits include:

- *Monitoring of sparsely staffed remote sites*. At remote sites where staffing is an issue, GDM allows 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 sites can be continuously monitored on a 24 hour basis from GDM Dashboard installations world-wide. For example, assuming a company has NetBackup 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 NetBackup monitoring duties.
- *Advanced filtering options*. In environments where a high volume of data is being protected, GDM's advanced filtering options allow you to display only the type of information you want to see.

New In GDM 4.5

- *Improved graphical user interface*. GDM provides a completely redesigned, flexible Windows and Java-based interface called Dashboard, which features drill down ease of use and a single window consolidation of assembled information. Although a single window view may be sufficient, multiple views can also be configured when additional details of the information are required.
- *Architectural improvements*. Through architectural improvements in the both the GDM data collector and the Dashboard, GDM scalability, data throughput, and real-time monitoring performance are all enhanced.
- *Reports*. GDM's enhanced reporting engine provides improved *Snapshot-In-Time* reporting functionality. GDM also supports the optional NetBackup Advanced Reporter module, which features robust *historical* reporting capabilities.

Note Due to architectural improvements in Global Data Manager 4.5, the support for some features has been modified. For a list of modified feature support, see Appendix A, "Special Limitations" on page 83.

Usage Recommendations

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

However, if the number of master 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 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 masters. Switching between GDM Servers allows you to remain up-to-date with the entire NetBackup domain, in a much more efficient manner.

For more information on creating GDM domains, see “Creating GDM Server Domains” on page 13

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 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(s), and NetBackup 4.5 managed master 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 4.5 Master Servers.

GDM Servers are responsible for monitoring NetBackup 4.5 Master Servers for pre-defined data that is gathered from the master server and its media servers. When detected, the data is collected from each NetBackup 4.5 Master by the GDM Server and then stored locally in the GDM Server's database for future retrieval by a Dashboard client.

A GDM Server can be created from any existing NetBackup 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.

Managed Master Servers

Managed master servers are NetBackup 4.5 Master servers that are installed and licensed in your environment. Using GDM data collectors, NetBackup 4.5 Masters receive pertinent data about all backup and restore operations being conducted at each of NetBackup media server in the GDM domain. Received data is then stored in the master server's local database. A subset of the data, which indicates high level status and problems, is rolled up to the GDM Server's database.

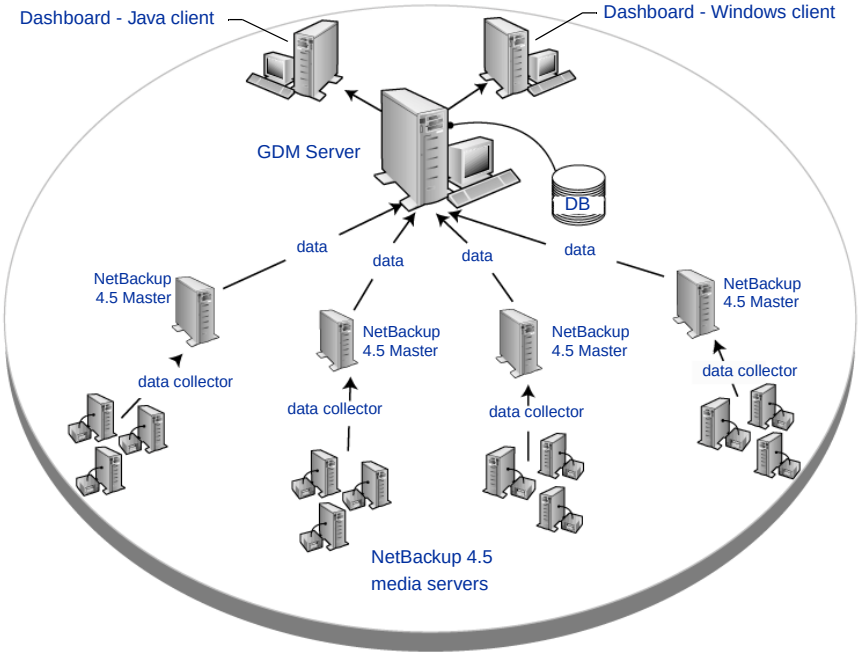
GDM Dashboard

To view the data collected from each NetBackup Master, GDM provides an easy-to-use GDM graphical user interface called the *GDM Dashboard* that runs on any computer that can run the NetBackup client. The Dashboard retrieves the data stored in the GDM Server database and then presents the information in an organized and efficient manner.

Note Because of the flexibility of the Dashboard, it can be installed and run at both the GDM Server or any managed master in the domain. It can also be installed and run remotely at any computer that can run the NetBackup interface.

The following diagram shows the flow of data from the NetBackup 4.5 media servers to the GDM Dashboard.

GDM Workflow Diagram



Data collected from media servers is forwarded to the NetBackup 4.5 Masters, which is then rolled up to the GDM Server database.

Visual Keys

To help you understand the information being presented, the GDM Dashboard makes liberal use of 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.

For more information, see “Color” on page 44.

Status Flags

Flag

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.

For more information, see “Status Flags” on page 44.

Icons

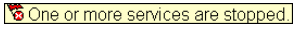
Icon

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.

For more information, see “Icons” on page 45.

ToolTips

ToolTip



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

For more information, see “ToolTips” on page 47.

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 master servers in the left pane. After clicking a managed master server name, the font face of the selected master changes, indicating which managed master server is currently being monitored.

For more information, see “Font Attribute Enhancements” on page 47.

Information Retrieval

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

Installation and Configuration 2

This section provides installation and configuration details about GDM.

Installation and Configuration includes the following topics:

Section	Description
"Installing Global Data Manager" on page 10	Describes detailed steps on installing GDM.
"Installing the GDM Components on UNIX-based Platforms" on page 10	Describes installing GDM on UNIX-based platforms.
"Installing the GDM Components on Windows NT or Windows 2000" on page 11	Describes installing GDM on Windows-based platforms.
"Configuring GDM" on page 13	Describes GDM configuration details.
"Creating GDM Server Domains" on page 13	Describes instructions for creating multiple GDM Domains
"Monitoring GDM Servers Located in Different GDM Domains" on page 17	Describes instructions for changing to a different GDM Server when using GDM Dashboard in a multi-GDM Domain environment.

GDM Installation Overview

GDM can be installed on either Windows NT/2000 computers or computers using the UNIX platform.

Installing Global Data Manager

This section guides you through the installation of GDM on both Windows NT/2000 and UNIX platforms. It also guides you through the configuration of GDM after installation is complete.

Note Before installing GDM, visit the VERITAS support web page at `www.support.veritas.com` for a list of the latest operating system and product patches and/or updates.

Caution Microsoft Internet Explorer 5.5 or higher is required on Windows NT/2000 systems in order to successfully install and use GDM. If IE 5.5 is not installed, please upgrade your version before installing GDM.

Installing the GDM Components on UNIX-based Platforms

Use the following steps to install GDM on the UNIX hosts that will either be used as a managed master server, or serve as the GDM Server.

▼ To install the GDM components on UNIX:

1. 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

2. Install NetBackup server software as explained in the *NetBackup 4.5 DataCenter Installation Guide for UNIX* (or *NetBackup 4.5 BusinesServer Getting Started Guide for UNIX*).

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
   ```

   Since other NetBackup products are included on the CD-ROM, a menu appears.

7. Select `NetBackup Add-On Product Software`.

8. Select the NetBackup Global Data Manager option.

9. Enter `q` to quit the menu.

10. When asked if the list is correct, answer `y`.

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.

Note The GDM Dashboard component (the graphical interface) is automatically installed as well.

Installing the GDM Components on Windows NT or Windows 2000

Use the following steps to install GDM on the Windows NT / 2000 hosts that will either be used as a managed master server, or serve as the GDM Server.

▼ To install the GDM components:

1. Log on as administrator.

2. Install NetBackup server software as explained in the *NetBackup DataCenter Installation Guide - Windows* (or *NetBackup BusinesServer Installation Guide - Windows*).

3. 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.

Note The GDM Dashboard component (the graphical interface) is automatically installed as well.

Installing the GDM Dashboard

The GDM Dashboard (the graphical interface) is automatically installed on all master servers and media servers. Any GDM domain can be remotely administered from those servers. In addition, the GDM Dashboard can be run from any client system that has the NetBackup administration interface programs installed.

The administration client has the software required to remotely administer GDM domains managed by either a UNIX GDM Server or a Windows NT/2000 GDM Server. There is no need to register GDM license keys on a remote system on which you intend to run only the GDM Dashboard component. License key registration is required only on the GDM Server and the GDM managed master servers.

Configuring GDM

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

After completing the Global Data Manager installation, a GDM domain, which is a set of managed NetBackup 4.5 master servers that GDM will be monitoring, must be created before GDM becomes fully operational.

In addition, the GDM domain you create will use, as its 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 if Dashboard performance issues arise.

Creating GDM Server Domains

A GDM domain is made up of a set of master servers that are being managed by a GDM Server. Although not a requirement, a GDM Server is typically an active master server and a member of the domain.

GDM can effectively monitor a GDM domain consisting of between 80 - 100 NetBackup master servers. If your installed base consists of more than 100 masters, it is recommended that you create multiple GDM domains, where each domain monitors up to 100 masters.

Note See Advanced Configuration section on data security for scenarios where one might want to designate a dormant master server as the GDM server.

▼ To create a GDM domain and add Managed Masters:

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

2. Start the GDM Dashboard.

Note Dashboard does not need to be run at the GDM Server. You may run the Dashboard remotely from a client system which has the NetBackup Administration Console installed.

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

4. Enter a GDM Server name, or enter its IP address.

5. Click OK.

Adding NetBackup Master Servers to the GDM Domain

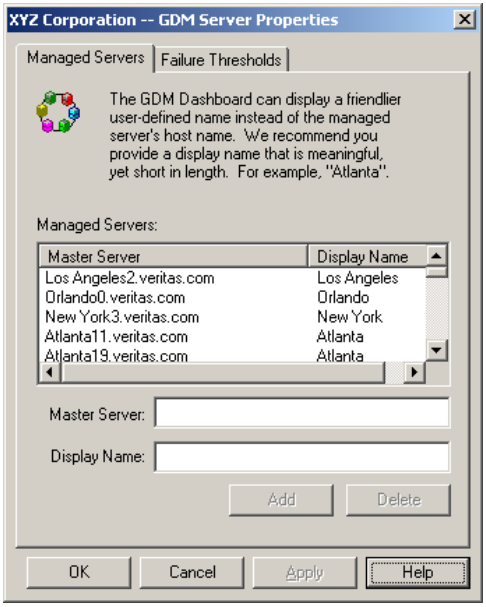
1. Choose Action from the menu bar.

2. Select Configure and then click General Properties.

   The GDM Server Properties dialog appears.

3. Click the Managed Servers tab.

GDM Server Properties Dialog Box



4. Add each managed master server's fully-qualified domain name (e.g., Madrid.XYZ.com) and a friendly display name such as *Atlanta*.

5. Click Add.

6. Click OK.

   The newly added master is added to the managed master server list. It can be viewed in the left pane of the Dashboard.

Modifying Master Server Properties in the GDM Domain

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

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

▼ **To make modifications:**

1. From the GDM menu bar, click Action.

2. Click Configure and the select General Properties.

3. In the Managed Servers tab, click a server to modify.

4. Make the adjustments and then click Change.

5. Click OK.

Removing NetBackup Master Servers from the GDM Domain

Use these steps to remove a managed master from the list of managed masters that appear in the left pane.

▼ **To remove a managed master server:**

1. Choose Action from the menu bar.

2. Select Configure and then click General Properties.

   The GDM Server Properties dialog appears.

3. Click the Managed Servers tab.

4. Click a managed master server to remove and then click Delete.

5. Click OK.

   The selected master is removed and no longer appears in the left pane of the Dashboard.

Monitoring GDM Servers Located in Different GDM Domains

If your environment is supporting multiple GDM Domains, at some point you may want to monitor the activity in those domains. To do so, you will need to point GDM Dashboard to the GDM Server in those domains in order to monitor the activity of the selected domain's NetBackup masters.

▼ To change GDM Servers:

1. From the GDM menu bar, choose Action and then select Change GDM Server.
2. Enter a GDM Server name, or enter its IP address.
3. Click OK.

   GDM Dashboard connects to the specified GDM Server.

Removing a Master Server from a GDM Domain

Use the following instructions to remove a master server from a list of servers to monitor.

▼ To remove a master server from a GDM domain:

1. Choose Action from the menu bar.
2. Select Configure and then click General Properties.

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

   The selected master server is removed.

Advanced Configuration 3

This section gives you the information necessary to make advanced configuration adjustments to Global Data Manager 4.5.

Advanced Configuration includes the following topics:

Section	Description
"Data Security" on page 19	Gives a general overview of the Global Data Manager 4.5.
"Adjusting Configuration Parameters" on page 20	Describes how GDM works and its use of visual keys within the graphical user interface.
"Using GDM with Firewalls" on page 28	Describes how Global Data Manager 4.5 can be used in environments that implement firewall protection.
"Enabling GDM Logging" on page 36	Describes how GDM logging is enabled on GDM Servers and / or GDM managed servers

Data Security

There may be situations where even the high level summary status about a master server cannot be trusted to be stored on a peer master server acting as the GDM Server. You may want a totally neutral system to serve as the GDM Server and as the central repository for all information culled from each master server in your domain.

In such a situation, you can create a dummy master server whose sole function is to act as a dedicated GDM Server. The setup procedures for a dedicated GDM server are the same as for a master server, except that there is no need to configure devices or policies. The one exception would be to back up the GDM Server's database in order to retain GDM threshold information in the event you have changed from the default thresholds.

Adjusting Configuration Parameters

You can adjust configuration parameters for both *failure threshold* and *data collection* properties for GDM Dashboard using the Configure selection found under the Action menu.

Adjusting Failure Thresholds

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

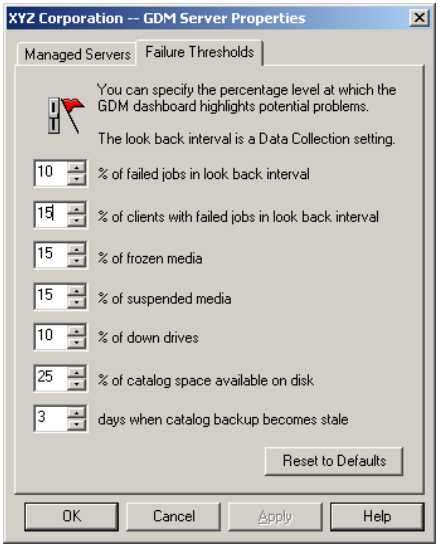
For example, you may deliberately down drives on media servers in order to keep the drives in reserve for emergency restores. For such situations, a downed drive does not represent a problem. However, if you have 10 drives and typically keep one down for emergency restores, then you can set a downed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

▼ To adjust the failure thresholds:

1. From the GDM Dashboard menu, click Action and then select Configure.
2. Click General Properties.

   The GDM Server Properties dialog box appears.
3. Click the tab, Failure Thresholds.

GDM Server Failure Thresholds



GDM Server Failure Threshold Options

Threshold	Definition
% of failed jobs in look back interval	Used for adjusting the 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. See “Adjusting the Look Back Interval” on page 22
% of clients with failed jobs in look back interval	Used for adjusting 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.
% of frozen media	Used for adjusting the point at which an alert flag is displayed for a high level of suspended media. The threshold specifies the number of tapes on a percentage basis that have been set to a frozen state.
% of suspended media	Used for adjusting the point at which an alert flag is displayed for a high level of suspended media. The threshold specifies the number of tapes on a percentage basis that are suspended.
% of down drives	Used for adjusting the point at which an alert flag is displayed for a high number of downed drives. The threshold specifies the number of drives on a percentage basis that are down.
% of catalog space available on disk	Used for adjusting 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 catalog's current size which should be available for future catalog growth.
days when catalog backup becomes stale	Used for adjusting 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.

4. Make adjustments to the threshold settings.

5. Click OK.

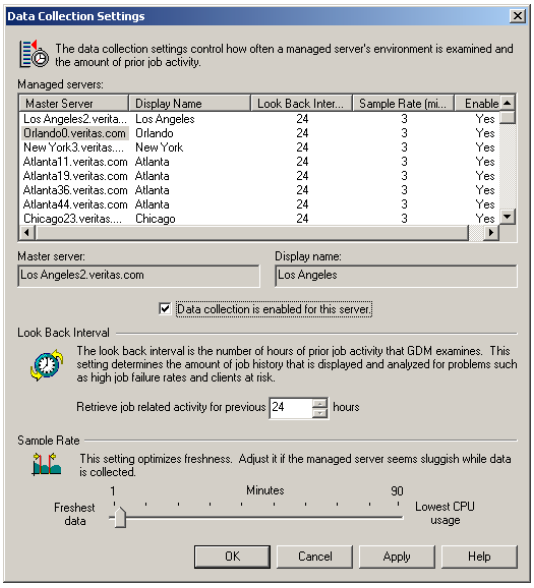
   Adjusted thresholds are then transferred to each master server, which are the applied during the next scheduled scan of the servers' environments.

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 a managed server's 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 the master server's performance.

Data Collection Settings Dialog Box



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 clients 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 Action.
2. Select Configure and then click Data Collection.

The Data Collection Settings dialog box appears.

3. In the list of managed servers, select a master 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 during the next scheduled scan of the managed server's environments

Adjusting the Sample Rate

The Sample Rate governs how often a managed server's 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 CPU usage cost to your master server when data is collected. For example, do you need to know about failed jobs within 2 minutes, or is 10 minutes sufficient?

Caution The Sample Rate adjustments are done on a per master 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 Action.

2. Select Configure and then click Data Collection.

   The Data Collection Settings dialog box appears.

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

4. Move the slider bar to the desired setting.

5. Click Apply.

6. Repeat these steps to adjust the sample rate on additional masters.

7. When finished, click OK.

Disabling and Enabling Data Collection

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

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

▼ To disable data collection:

1. From the GDM Dashboard menu bar, click Action.

2. Select Configure and then click Data Collection.

   The Data Collection Settings dialog box appears.

3. In the list of managed servers, select a master server on which to disable data collection.

4. Clear the Data collection is enabled for this server checkbox by clicking it.

5. Click Apply.

6. Repeat these steps to disable data collection on additional masters.

7. When finished, click OK.

▼ To enable data collection:

1. From the GDM Dashboard menu bar, click Action.

2. Select Configure and then click Data Collection.

   The Data Collection Settings dialog box appears.

3. In the list of managed servers, select a master server on which to enable data collection.

4. Enable data collection by clicking the Data collection is enabled for this server checkbox.

5. Click Apply.
6. Repeat these steps to enable data collection on additional masters.
7. When finished, click OK.

Controlling Configuration of the GDM Managed Server List

The GDM Dashboard contains dialog boxes that allow maintenance of the GDM configuration. One specific configuration parameter needs special mention - the list of managed servers.

Note The General Properties dialog box in the Dashboard interface controls this parameter. The tab can be found in the Action menu under Configure. Click General Properties and then click the tab, Managed Servers.

Caution It is possible that you will have multiple users viewing the GDM domain using multiple Dashboards in multiple locations over the course of the day. However, you, as the GDM administrator, should stress that users should not make changes to the managed server list unless the implications of the change are fully understood.

For example, if you as the administrator want to designate another master server as the GDM Server, connect to the first GDM Server and deleted all the managed servers. Then connect to the new GDM Server and add those managed servers.

Within a GDM domain there should be one machine designated as the GDM Server and all other servers should be listed as the managed servers.

Though theoretically possible, having a GDM domain monitored by more than one GDM Server is not recommended as the actions of multiple GDM Servers in a domain can create misleading results. If a user configures a different machine in the GDM domain to be the GDM Server (without clearing the original configuration) and then associates the first server's managed servers to be its managed servers, the results in the Dashboard could again be misleading.

Especially problematic is the case where a user creates a second GDM Server and then adds the original GDM Server to the second GDM Server's list of managed servers. If this is done without first clearing the original GDM Server's managed server list, the results can be unpredictable.

These problems can be mitigated by installing the proper license on each machine in the GDM domain. If only one machine has the *Global Data Manager* license, then other machines can't mistakenly be configured as the GDM Server. The other machines (managed servers) should only have the *GDM Managed Server* license installed.

Consider the following example:

Action: Host a, b, c are managed servers of GDM Server Host x.

Result: Host a, b, c will be continually reporting their changing status to Host x.

Action: Using the Dashboard, a user sets his GDM Server to Host a. He then adds host b and c to be managed servers of Host a.

Result: Host b, c will be continually reporting their changing status to both Host x and Host a. Performance degradation could result.

Now the GDM Domain has two GDM Servers, Host x and Host a.

Action: Using the Dashboard, another user sets his GDM Server to Host a. He then adds Host x as a managed server of Host a.

Result: Host a is reporting its changes to GDM Server Host x (because it is a managed server of Host x). But Host x is reporting its changes to GDM Server Host a (because it is a managed server of Host a.)

Due to the recursive nature of this configuration, performance problems may occur in the GDM application.

Using GDM with Firewalls

Global Data Manager 4.5 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 can be easily verified as correct. 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.

As such, GDM has been designed along 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.
- Ports opened on the GDM Server and the managed servers always have a well-known, active listener.
- 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.

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; they are determined using the Dashboard client computer's `DASHBOARD_PORT_WINDOW` entry found in the *bp.conf* file under UNIX, or the Dashboard Port Window registy entry under Windows NT/2000.

By default, the Dashboard client computer dynamically selects a port address to be used when dynamic assignment of addresses is required (see "GDM Dashboard Port").

GDM Server Port and GDM Managed Server Port (VISD)

The static port address assigned to port VISD 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, `/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 client 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 (see “Scenario 3 - Dual firewalls with Dashboard running on two terminals” on page 32).

By default, the GDM Dashboard client computer randomly selects a port address from an allowed range. The client computer can also be configured to select an address starting from the top of the range, picking the first one available.

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

Global Data Manager 4.5 can run multiple instances of the GDM Dashboard from one GDM Dashboard host in a firewall environment (see “Scenario 3 - Dual firewalls with Dashboard running on two terminals.” However, to run multiple Dashboard instances, firewall port assignments must first be modified at the GDM Dashboard host computer.

At the GDM Dashboard host, a range of reserved ports is specified, where the GDM Dashboard host can listen for connections. This address range is applied to the port on which the Dashboard host uses to listen.

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.

Note Use `DASHBOARD_PORT_WINDOW` in the UNIX `bp.conf` file or Dashboard Port Window in the Windows NT/2000 registry. For more information, see Available Port Addresses.

When the Dashboard hosts searches for an available port address, it randomly selects an address from those available in the allowed 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 4.5 interface.

Firewall Scenarios

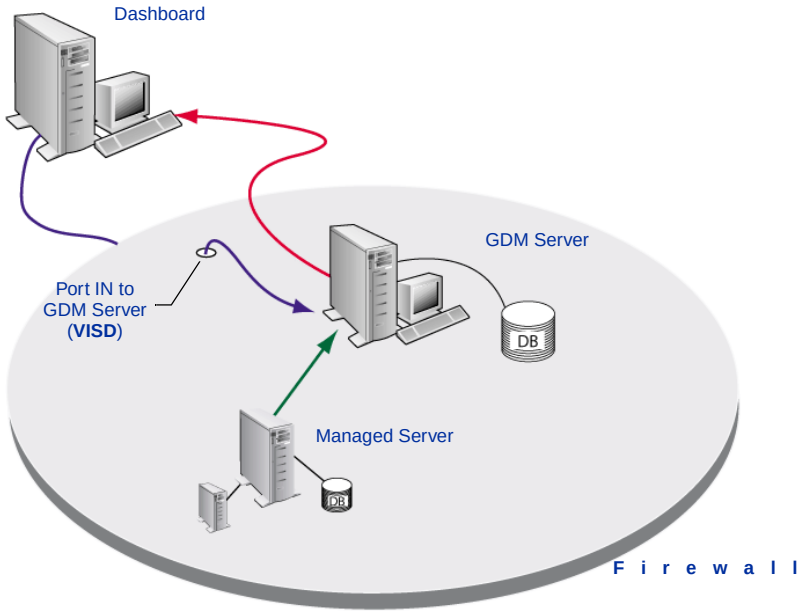
Three popular firewall environment scenarios are considered when GDM installation through a firewall is required. These include:

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

Scenario 1 - Single firewall environments

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

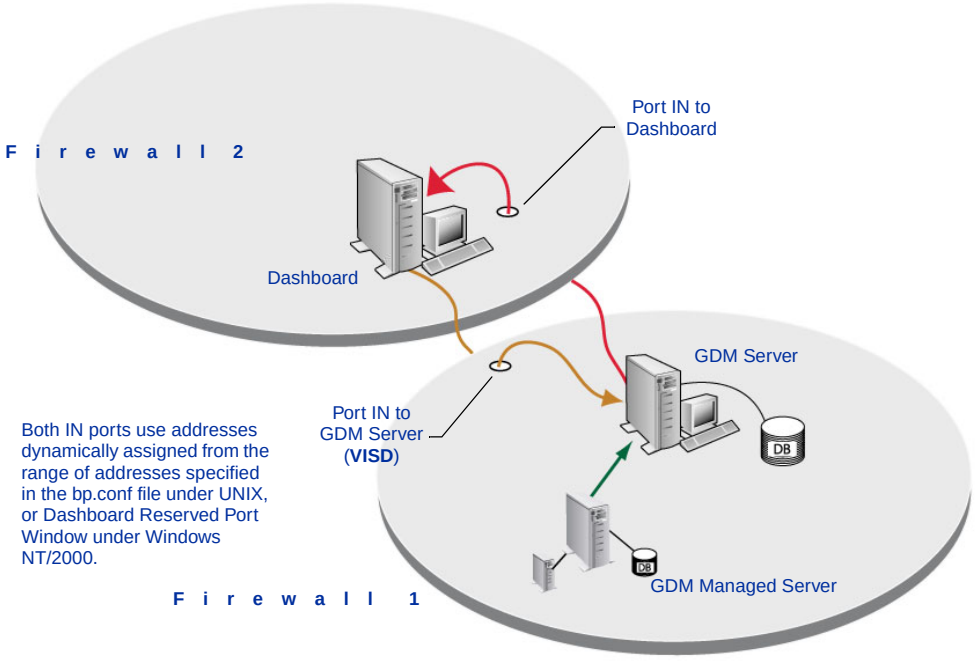
Single firewall configuration



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 Master servers, while the GDM Dashboard resides inside a second firewall-protected environment.

Dual Firewall - single Dashboard configuration

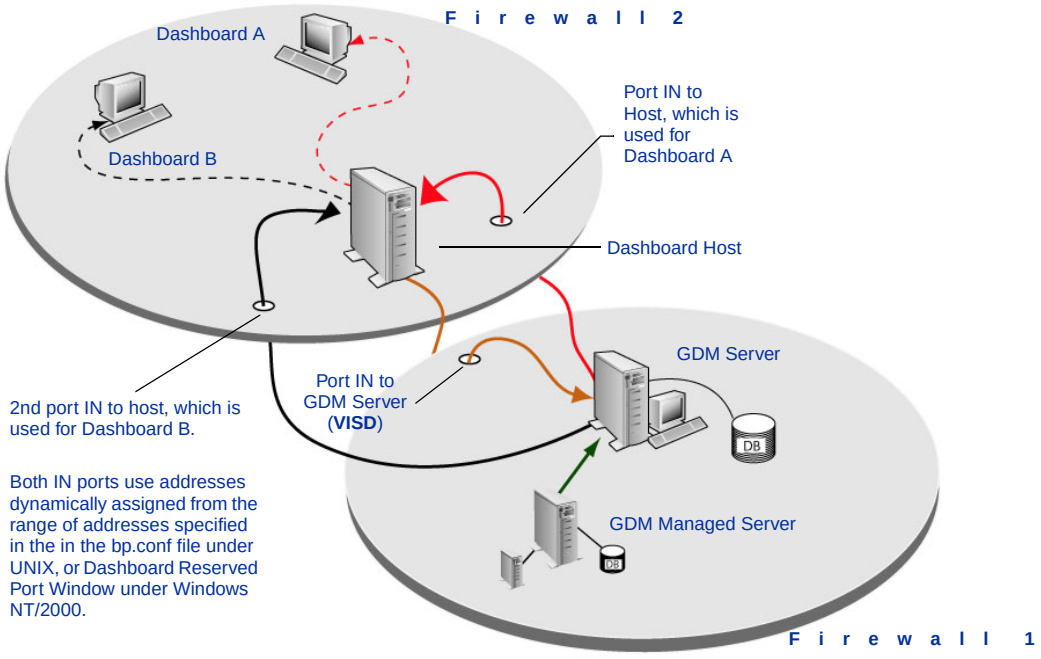


VISD port configuration in the `services` file under both UNIX and Windows NT/2000 is configured automatically during installation.

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 Master servers, while the GDM Dashboard runs on two terminals inside a second firewall-protected environment.

Dual firewalls with Dashboard running on two terminals inside the second firewall



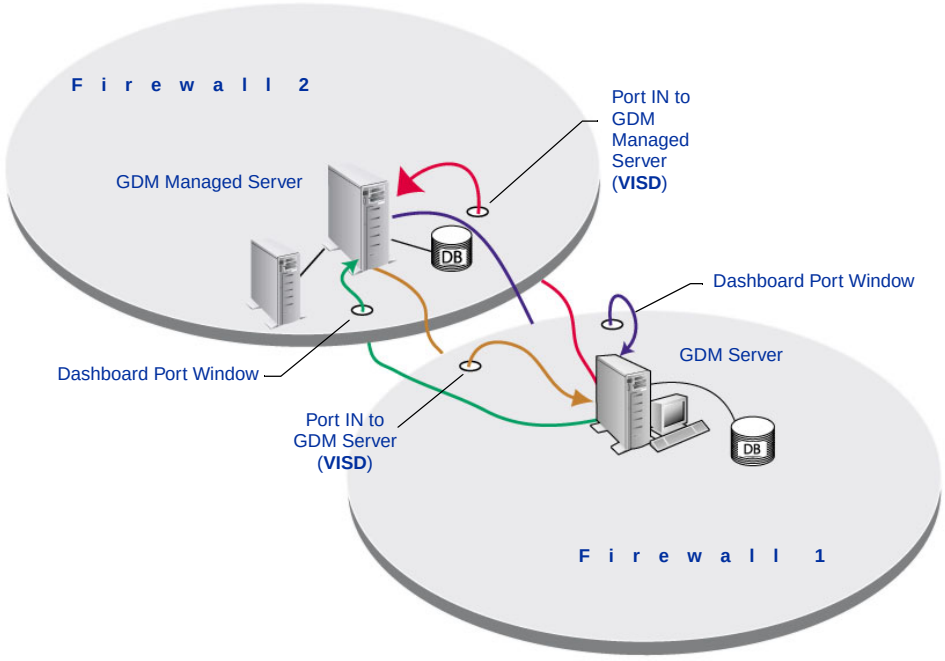
VISD port configuration in the `services` file under both UNIX and Windows NT/2000 is configured automatically during installation.

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.

Dual firewalls separating the GDM Server and a GDM Managed Server



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

Caution The range of port addresses specified for the Dashboard Port Window on the GDM Server must be equal to or greater than the number of managed servers outside the firewall enclosing the GDM Server.

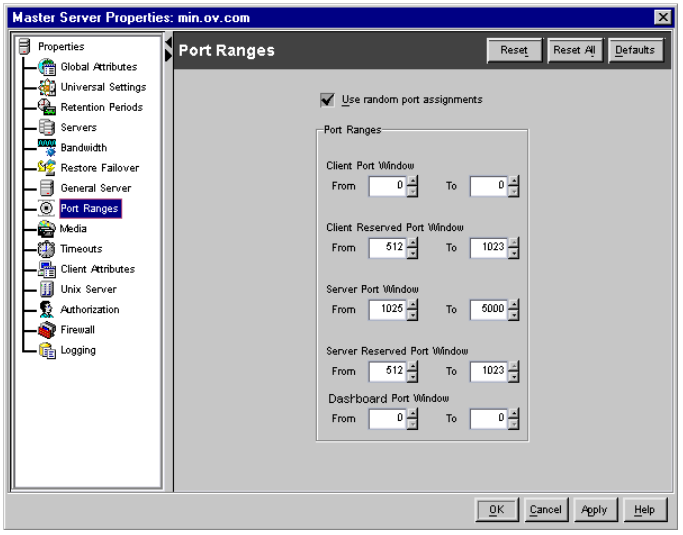
Modifying the Dashboard Port Address Range

Use the following steps to modify port addresses on the Dashboard host if you want to limit the range of ports used.

▼ To modify firewall port addresses:

1. For each Dashboard host, start NetBackup 4.5 on that 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 port modification is required and select Properties.
4. Click Port Ranges.
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



6. Click OK.
7. Close and restart all Dashboard interfaces running on the given system.

Enabling GDM Logging

GDM logging is enabled on GDM Servers or GDM managed servers by creating log file directories in `<install-directory>/netbackup/logs/`. The VISD needs to be stopped and restarted afterwards.

Keep in mind the following:

- Each GDM component has its own debug log directory.

  There are many GDM log file directories, with each correlating to a component within the GDM system. Although it may seem confusing to have multiple log files instead of one, in practice it makes diagnosing a problem a lot easier.

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

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

  log.<mmddyy>

  For example, *log.110891*

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

  Additional information on changing the keep logs x days parameter can be found in the *NetBackup 4.5 System Administrator's Guide*.

Caution Some of these logs can potentially become very large, and should only be enabled if unexplained problems exist.

Creating the following directories in a server's (GDM Server or GDM Managed Server) `netbackup/log` directory causes the corresponding GDM system component to output log information:

gdm_visd*	gdm_objcat
gdm_collector*	gdm_licenseblm
gdm_mastmon*	gdm_chgevt
gdm_psodbc*	gdm_heartbeat

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

Most of the GDM modules, except for exceptions such as the data collector module, support one level of debug logging. By simply creating the log files you get the complete 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 set the data collector's Parameters value.

Enabling Dashboard Logging

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.

Enabling logging for either the Dashboard Windows or Java clients using the following directions.

▼ To enable Dashboard logging on Windows NT/2000:

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

   For example, `c:\Program Files\VERITAS\netbackup\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, <drive letter>:\Program Files\VERITAS\NetBackup\Logs\gdmui

   When creating and naming the log file, GDM uses the format `gdm_yyyymmmdd_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.

Note 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 start Dashboard logging on UNIX:

1. Start the Dashboard Java client 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 based on a scale of 1 - 5, with 1 giving the least amount of detail and 5 giving 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"
  ```

▼ Setting the Parameters value on Windows NT/2000:

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:

- On UNIX, add the line `“Parameters”=”-sleep 60 -verbose 5”` beneath the heartbeat section in the `/usr/openv/var/visd.conf` file. 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 NT/2000:

1. On Windows NT/2000, edit the registry.
2. Find the chgevt key:

   HKEY_LOCAL_MACHINE]\[SOFTWARE]\[VERITAS]\[Infoserver\VTHost\Modules\chgevt].
3. In the chgevt key, add a new string value called Parameters.
4. Set the value of Parameters in the Value data field to -sleep 60 -verbose 5.
5. Next, find the heartbeat key:

   HKEY_LOCAL_MACHINE]\[SOFTWARE]\[VERITAS]\[Infoserver\VTHost\Modules\heartbeat]
6. In the heartbeat key, add a new string value called Parameters.
7. Set the value of Parameters in the Value data field to -stime 60 -verbose 5.
8. Close the registry.

Using GDM 4

This section provides information on using GDM.

Using GDM includes the following topics:

Section	Description
"Starting the GDM Dashboard" on page 41	Describes how to start Global Data Manager 4.5.
"Understanding the GDM Dashboard" on page 44	Describes how GDM works and its use of visual keys within the graphical user interface.
"Introducing the GDM Dashboard" on page 48	Describes the GDM Dashboard and the various components that comprise the interface.
"Viewing Modes" on page 50	Describes the Summary and Detail viewing modes available in GDM.
"Defining, Editing, and Deleting Filters" on page 64	Describes the use of filters in 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 and then click GDM Dashboard.

   The GDM Dashboard starts and a Connect to GDM Server dialog box appears.
3. Enter a GDM Server in which to connect.

Note During the initial initialization of the GDM Dashboard, a Connect to Server dialog box appears, asking you to select a GDM Server in which to connect. After making the initial connection, the GDM Dashboard will automatically find and connect to the GDM Server used in previous sessions, when subsequent sessions of the Dashboard are run.

The GDM Dashboard starts.

▼ **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/netbackup/bin/gdmSA &
   ```

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

Setting Up Your Window Manager

It is recommended that under UNIX, you always set your window manager so windows become active only when you click within the windows. Do not enable auto focus. Auto focus occurs when windows become active when the mouse pointer is moved over them. The GDM Dashboard Java client 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 Dashboard-Java client.

▼ **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.

   The Style Manager toolbar appears.

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

   The Style Manager - Window dialog box appears.

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

4. Click **OK**.

5. Click **OK** when asked 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 when they are encountered.

Understanding the GDM Visual Keys

To help you understand the information being presented, the GDM Dashboard makes liberal use of 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, where serious, data threatening issues exist. Critical conditions should be investigated as soon as possible.
- Yellow represents a warning condition, where possible data threatening issues exist. Warning conditions should be investigated as soon as possible.
- Blue indicates an activity condition exists, where some sort of activity is occurring at your Master 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 same conditions represented with the use of color. Status flag icons include:

Available Status Flags

Status Flag	Description
	*Critical Flags* - This status flag represents an error condition that must be investigated as soon as possible. Critical flags contain an X, which indicates serious data threatening issues at the managed master server. The color red is associated with this type of flag

Available Status Flags

Status Flag	Description
	*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
Services Detail Section	
 Running	This icon represents a running operation. Using the color green, indicates a running state. For example, under Services in the right pane, Run icons are used to indicate that services such as the NetBackup Client Service are running.
 Stop	This icon represents Stop. Using the color red, this icon indicates a stopped state. For example, under Services in the right pane, Stop icons are used to indicate that services such as the NetBackup Database Manager have been stopped.

Available GDM Icons

Icon	Description
Jobs Detail Section	These icons are typically found in the Jobs detail section.
 Finished Job - Successful	This icon 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.
 Queued Job	This icon represents a queued job, which indicates a job is queued and ready to be processed.
 Define Filter	This icon 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 64.
 Edit Filter	This icon 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 64.
 Delete Filter	This icon represents the Delete Filter feature. Using this feature allows you to delete user-defined filters. For more information, see “Defining, Editing, and Deleting Filters” on page 64.
Report Icons	
 Problems and Conditions Report	This icon presents the Problems and Conditions report, which is a report showing a list of managed servers with detected problems. For more information, see “Problem and Conditions Report” on page 80.
 Drive Status Summary Report	This icon represents the Drive Status Summary report, which is a report showing the status of drives on each of the managed master servers (and their media servers) being monitored by GDM. For more information, see “Drive Status Summary Report” on page 80.

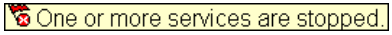
Available GDM Icons

Icon		Description
	General Status Report	This icon represents the General Status report, which is a report showing various totals and data points for each managed master server being monitored by GDM. For more information, see "General Status Report" on page 81.

ToolTips

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

Example of a ToolTip



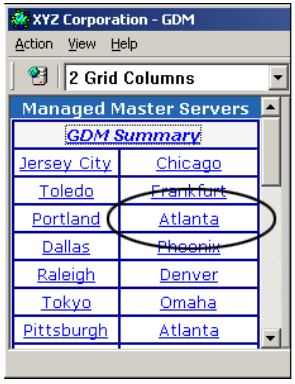
A ToolTip appears a second or two after resting the mouse over a managed master server name where a condition appears.

Note ToolTips are also available in the right pane, for each robot LED Drive Status graphic found in the Robot detail sections. For more information, see "Using GDM" on page 41.

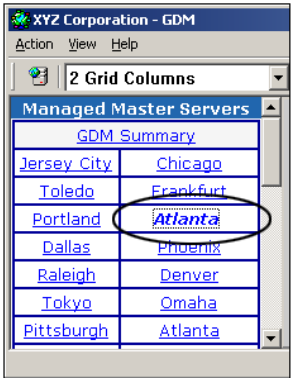
Font Attribute Enhancements

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

Text Enhancements - Windows Client



No managed server selected



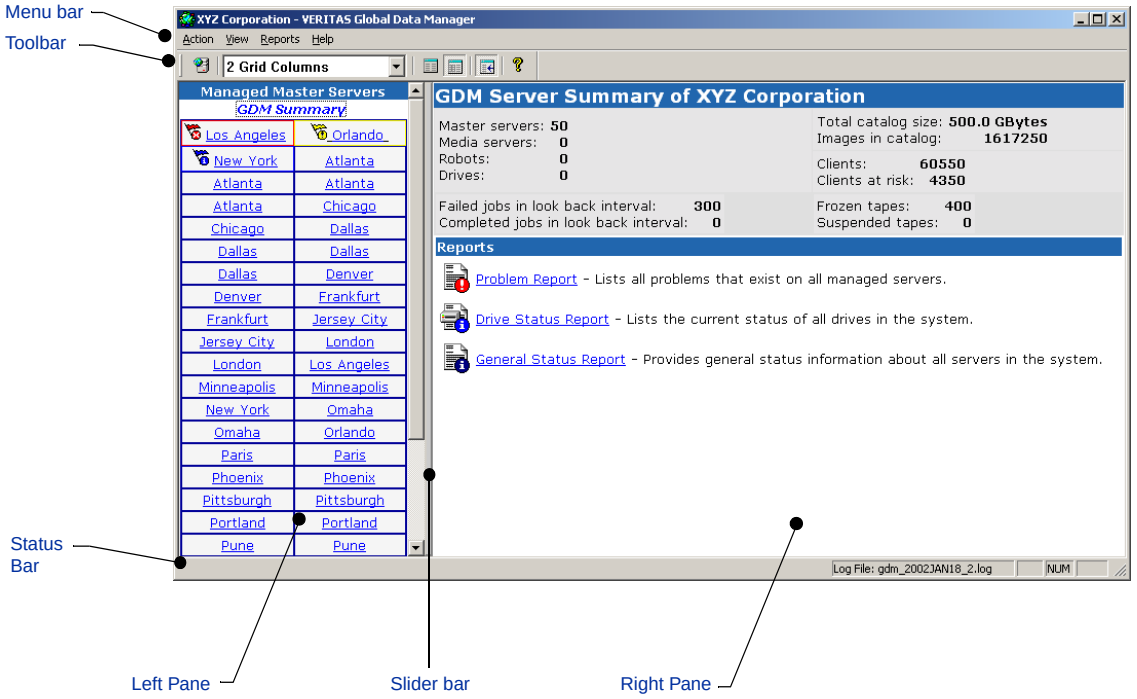
After managed server selected

Introducing the GDM Dashboard

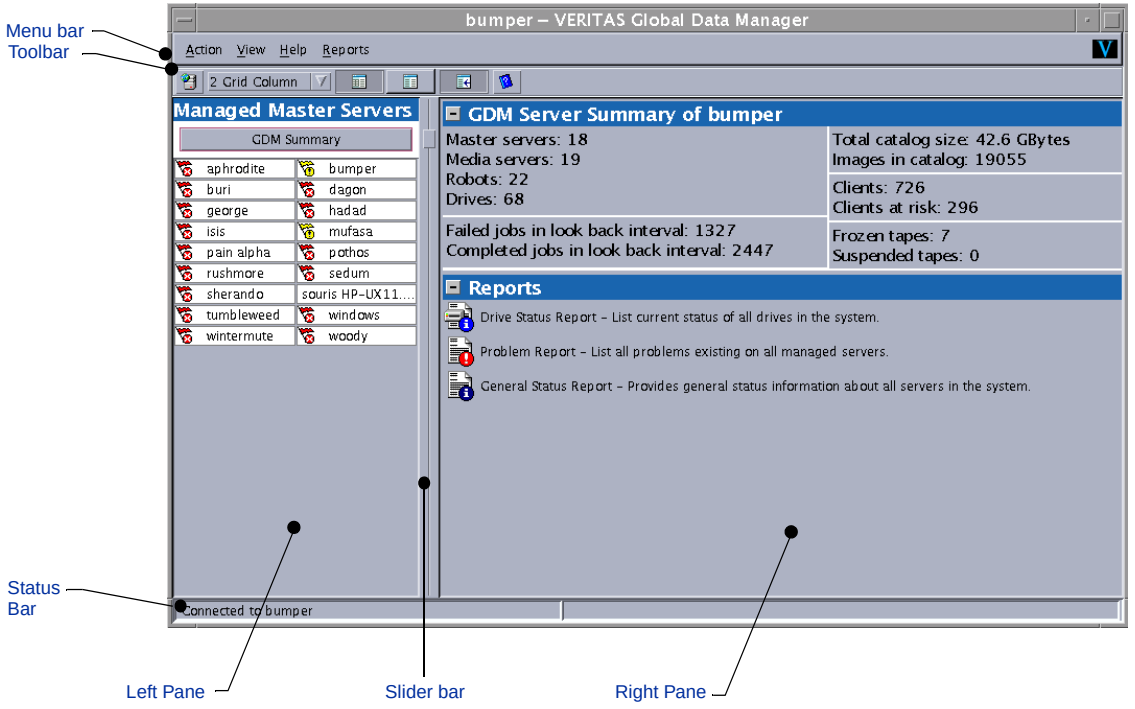
The GDM Dashboard consists of multiple interface components. These components include resizable *left* and *right* panes that are used to present the information gathered from each of the managed master servers being monitored. In between the left and right panes is a movable splitter bar, which can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

GDM Dashboard - Windows client



GDM Dashboard - Java client



Viewing Modes

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

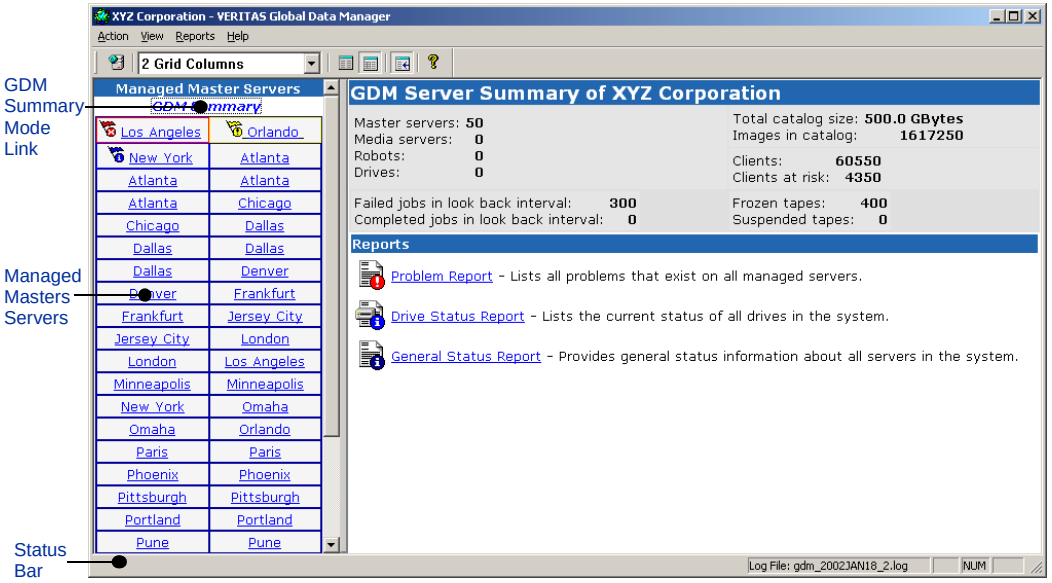
Summary Mode

The first type of viewing mode Dashboard offers is called *Summary mode*. Summary mode presents an overview of the entire GDM domain being monitored by the GDM Server to which you are connected. 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.

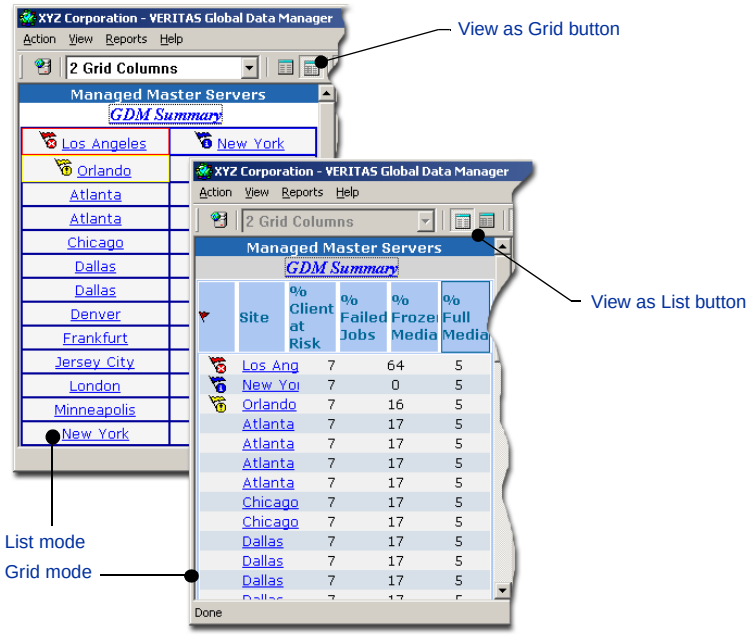
The *left pane* of GDM Summary mode displays all managed master servers that are being monitored by the GDM Server to which you are connected.

GDM Summary Mode - Windows client



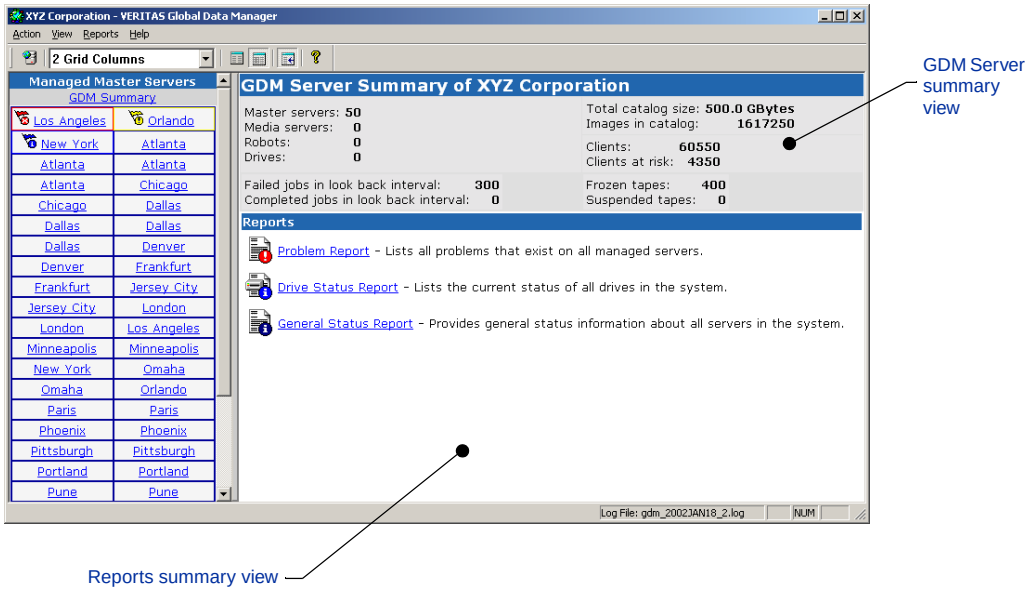
You can view these servers either in a list format or a grid format, depending on the toolbar button selected. For more information on the *View as List* and *View as Grid* buttons, see "GDM Toolbar" on page 72.

GDM Dashboard List mode and Grid mode - Windows client



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

Right Pane of the GDM Dashboard Summary View - Windows client



Summary Mode - Reports

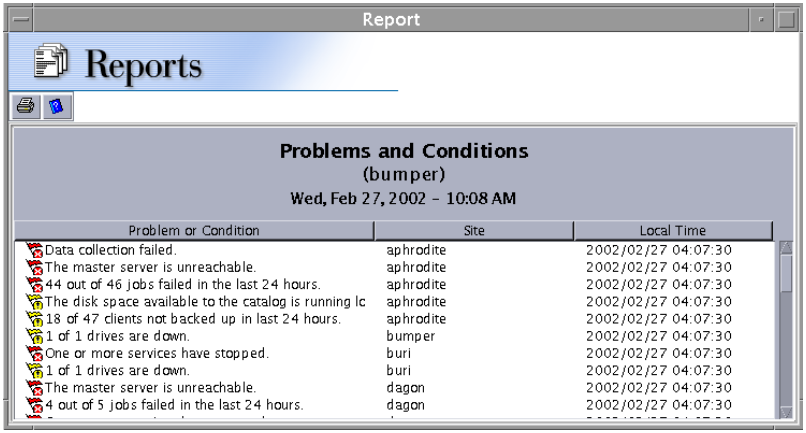
In Summary view, Dashboard's right pane also contains a Reports view. Located in the lower quadrant of the right pane, the Reports view offers you hypertext links to the following reports:

- *Problem Report* - This report lists problems that exist on all managed master 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 client)

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

GDM Report Example - Java client



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

For more about Dashboard reports, see “Reports” on page 77.

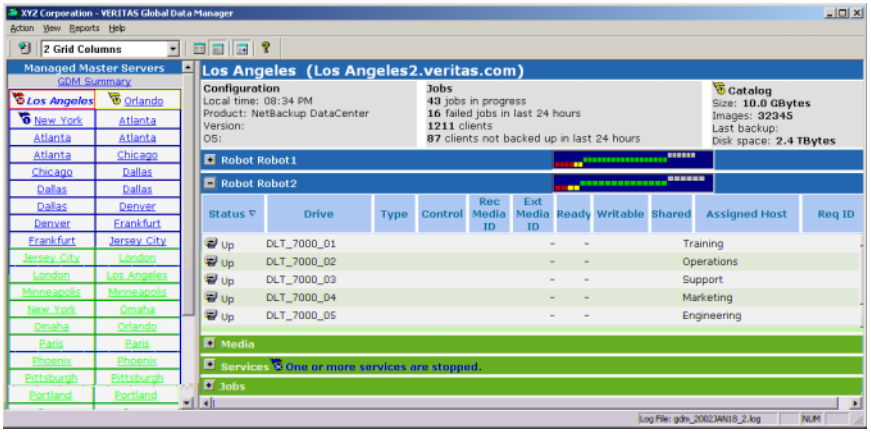
Detail Mode

The second type of viewing mode Dashboard offers is called *Detail mode*. Detail mode allows you to see detailed information for any of the individual master servers listed in the left pane.

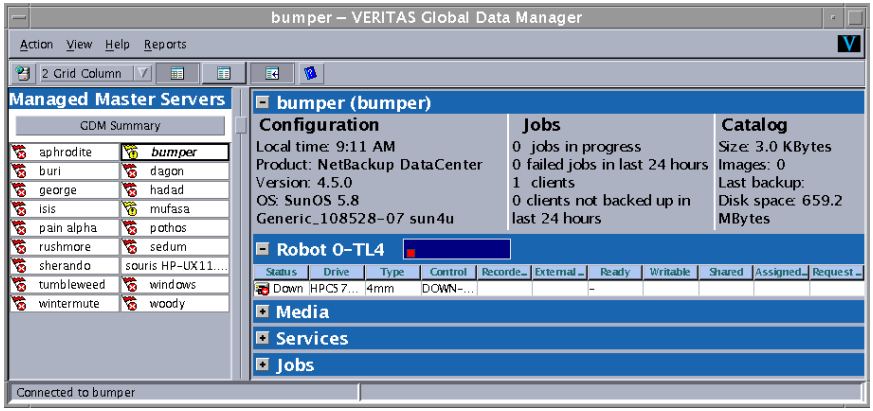
In Detail mode, the Dashboard's right pane reveals the following information:

- Summary details for the selected master server.
- Robot information for all robots installed at the master server.
- Services or daemon status information for NetBackup services on the master server and its media servers. For example, status of the Device Manager service.
- Job status information for all jobs being processed by the master server.
- Media status information for all media used by the master server and its associated media servers.

GDM Detail Mode - Windows client



GDM Detail Mode - Java client



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

After selecting a master server, the name of the selected server changes from a normal font face to italics, thus reflecting the currently selected master server (see “Font Attribute Enhancements” on page 47).

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

- Robots
- Services
- Jobs
- Media

Each detail section uses advanced drill-down technologies to reveal 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 temporarily 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 more suit your individual requirements.

For more information on organizing columns, see “Organizing Detail Section Columns” on page 66.

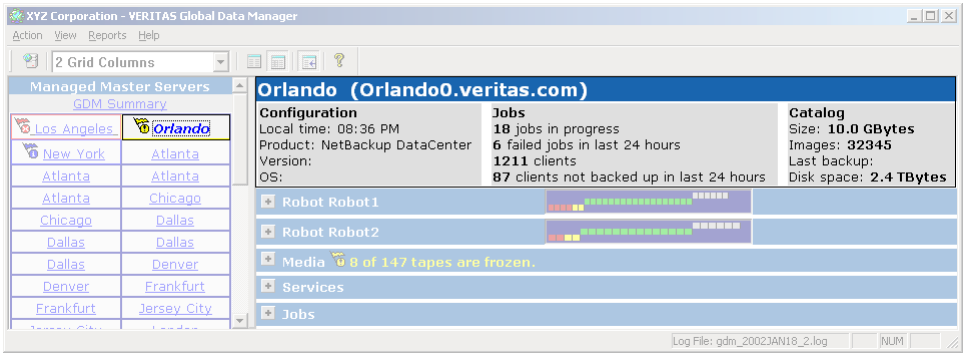
Detail Mode Sections

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 master server selected in the left pane. Summary information includes details about configuration, jobs, and catalogs.

Detail Mode - Summary detail section



Summary column details are defined in the following table.

Detail Mode - Summary details

Configuration	
Local Time	*Local Time* shows the current time in the NetBackup master server time zone.
Product	*Product* shows the type of VERITAS product installed at the master server.
Version	*Version* shows the version of the VERITAS product installed at the master server.
OS	*OS* shows the name of the operating system that is running on the master server.
Jobs	
Jobs in progress	*Jobs in progress* shows you the number of active jobs in progress that are being managed by the master server.
Failed jobs in last 24 hours	*Failed jobs in last 24 hours* shows the number of jobs that failed during the preceding 24 hours. The default interval of 24 hours can be configured to be an interval of your choosing. For more information, see "Adjusting the Look Back Interval" on page 22.
Clients	*Clients* shows the number of client computers that the Master server is protecting. The count is derived from the number of classes defined in active classes.
Clients not backed up in last 24 hours	*Clients not backed up in last 24 hours* shows 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 of your choosing. For more information, see "Adjusting the Look Back Interval" on page 22.
Catalogs	
Size	*Size* shows the total size of the current catalog being generated by NetBackup 4.5.
Image	*Image* shows the total number of images in the catalog.
Last Backup	*Last Backup* shows the date and time when catalog was last backed up.
Disk Space	*Disk Space* shows the amount of available disk space on the master server partition where the catalog resides. This value indicates how much space is available for future catalog growth.

Robot Details

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

Unique to the Robot section are 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.

Each square that appears in the graphic represents a physical drive. Based on the color and positioning of the squares, you can make a quick, visual determination of the general status of the robot's drives. RED squares indicate drives that are down and have serious issues, while GREEN squares indicate drives that are up and active. GRAY squares indicate drives that are up but are not presently active, while YELLOW squares indicate drives of unknown status due to the media servers to which they are attached being unreachable.

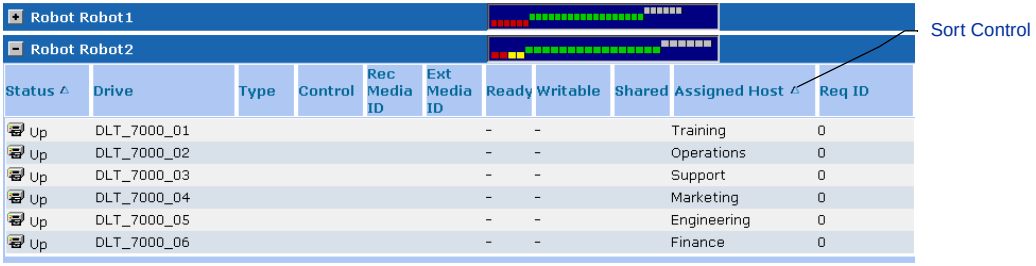
The positioning of an LED, along with its associated color, can indicate potential issues at a glance. All drives that are DOWN are positioned in the left portion of the graphic and are placed on a plane below the green LEDs, indicating a negative condition. Because the color green is associated with drives that are up and active, the green LEDS are considered normal conditions and are thus used as a base reference point. Gray LEDs appear above the green, showing an UP status.

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

Robot LED Graphic with ToolTip Example

Clicking the ⊞ control expands the Robot detail sections, revealing 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



Robot Detail columns are defined in the following table.

Robot Detail Section Column details

Status	Shows the situational status of the drive. The drive can be either up and active, up and idle, down, or unreachable (status unknown).
Drive	Drive name assigned to the drive during NetBackup configuration.
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.
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 statue 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 an administrator.
Recorded Media ID	Recorded media serial number 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.
External Media ID	External media ID serial number of the media mounted in the drive. Normally this identifier should match the Recorded Media ID. If a tape is not mounted, this field will be blank.
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.
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.
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.
Assigned Host	If this is a shared drive, this column shows the device host that has this drive assigned. If this is not a shared drive, this column contains a dash (-).
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.

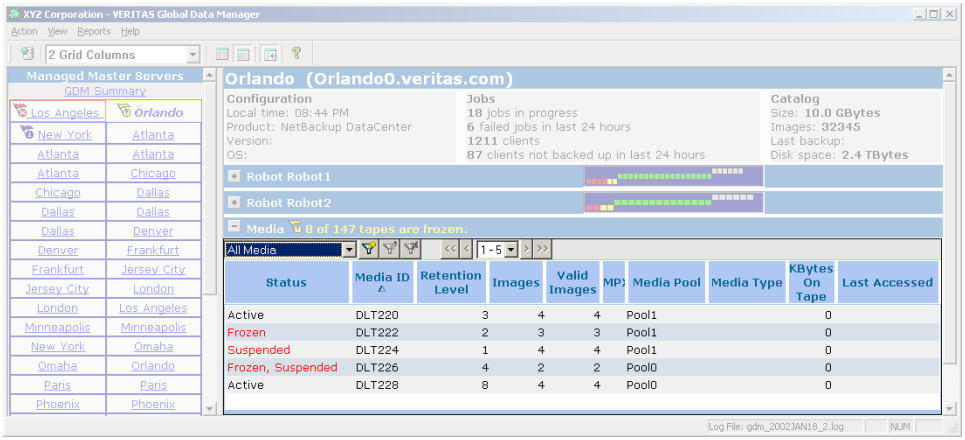
Media Details

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

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

For more information on job filtering, see “Defining, Editing, and Deleting Filters” on page 64.

Detail Mode - Media Detail Section



Media detail columns are defined in the following table.

Media Detail Section

Status	Displays the status of the media. Status conditions include: Suspended, frozen, full, imported and active.
Media ID	Displays the media identification number of each piece of media. Media IDs are assigned by NetBackup when you add media to a robot.
Retention Level	Displays the retention level assigned to a piece of media.
Images	Displays the number of images contained on a piece of media. An image is a collection of data that NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories, and catalog information associated with the backup or archive.
Valid Images	Displays the number of valid images contained on a piece of media. Note that on a multiplexed piece of media, this column may remain blank. A valid image is a collection of data (image) that has been verified.

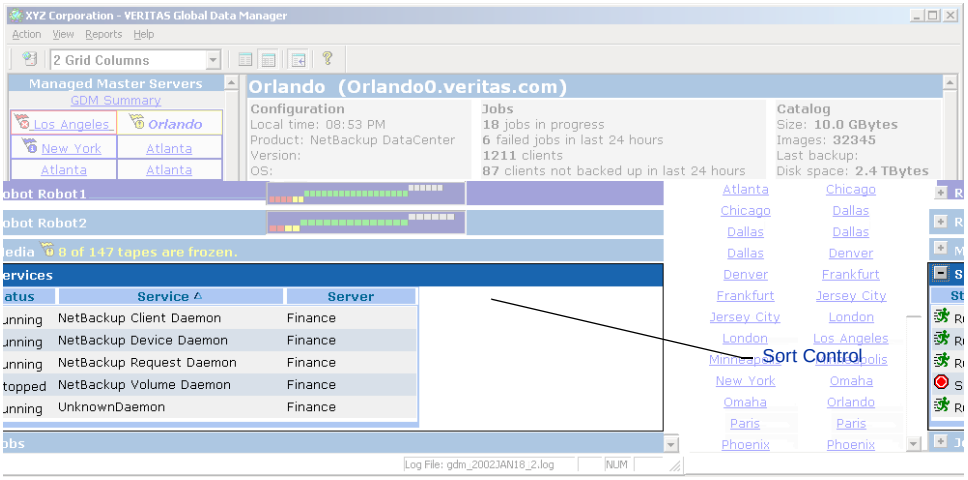
Media Detail Section

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.
Last Accessed	Displays the last date a piece of media was accessed by a storage device.
Media Type	Displays the type of media used. Types include: 4mm, 8mm, dlt, dlt2, dlt3, dtf, hcart, hcart2, hcart3, odiskwm, odiskwo, and qscis.
KBytes on Tape	Displays the amount of data on a piece of media, in Kilobytes.
MPX	Displays all multiplexed backup sets that are interleaved on storage media.

Services Details

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

Detail Mode - Services Detail Section



Service Detail section columns are defined in the following table.

Services Detail Section Column Titles

Status	Displays the operational status of the service or daemon. One of three status conditions can appear for each service / daemon listed: Stopped, Running, or Unreachable (if the media server could not be reached to detect the service status).
Service	Displays the name and type of service / daemon.
Server	Displays the name of the master server or media server where the service or daemon is running.

Available filters are defined in the following table:

Jobs Detail Section - Job Filters

All Jobs	Lists all jobs being managed by the master server.
All Active Jobs	Displays only active jobs being managed by the master server.
All Queued Jobs	Displays only pending jobs that are presently in the job queue.
All Done Jobs	Displays all jobs that have finished.
All Re-queued Jobs	Displays only jobs that have been re-queued by NetBackup at the master server.
All Failed Jobs	Displays all jobs that have failed.

Defining, Editing, and Deleting Filters

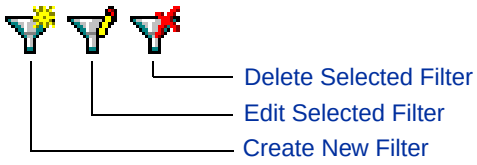
Both the Jobs and Media detail sections allow you to filter information using default filters provided by the GDM Dashboard. These filters allow you to filter on the following topics:

Media and Jobs Detail Section Filters

Media Filters	Jobs Filters
All Media	All Jobs
All Full Media	All Active Jobs
All Suspended Media	All Queued Jobs
All Active Media	All Done Jobs
All Unused Media	All Requeued Jobs
All Frozen Media	All Failed Jobs

In addition to these default filters, both the Job and Media detail sections allow you to create additional user-defined filters using the Create New Filter icon. After a user-defined filter is created, the Edit Selected Filter and Deleted Selected Filter icons can be used to either modify or delete the new filters.

Filter Icons



Note Both the Edit Selected Filter and the Delete Selected Filter icons only appear after user-defined filters have been created.

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 icon.

The Define Filter dialog box appears.

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 alpha 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 icon.

   The Define Filter dialog box appears, displaying the filter's defined definitions.
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 icon.

   A question box appears asking you to confirm the deletion operation.
4. Click Yes.

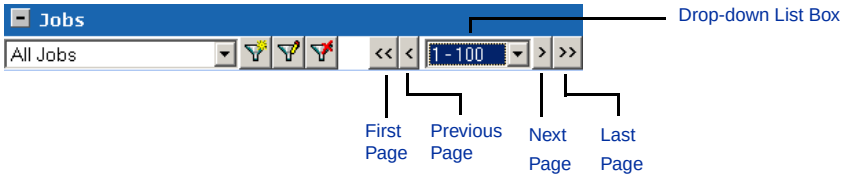
   The selected filter is deleted.

Managing the Amount of Data to Be Viewed

The amount of data 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 Dashboard Java-based client.

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.
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 information to you in a structured and organized manner. Within each table are column heads that specify the type of information that is displayed. You can customize the column heads by temporarily removing column heads containing information that may not be of interest to you.

For example, there may be instances where 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.

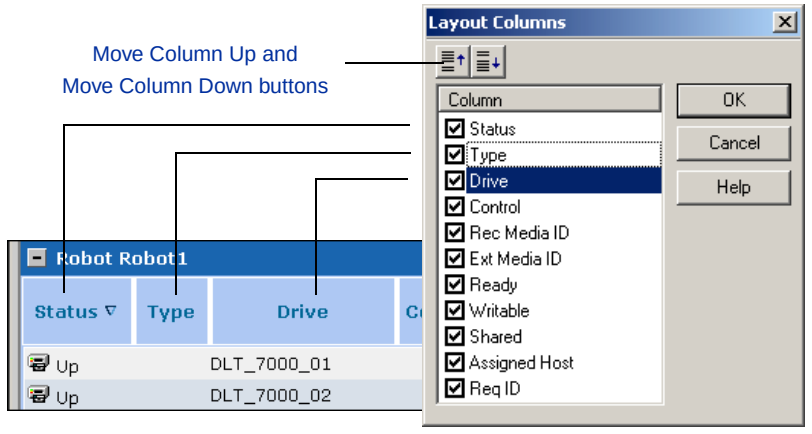
Note Changing detail section column head information is not a global operation. Each detail section is an independent entity. Any changes you make pertain only to the detail section you are viewing.

You can also specify the order in which the column heads appear, using the Move Column Down and Move Column Up icons. 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 Dashboard Java client, you can change the layout of the columns by clicking the column heads and then dragging them to a desired position.

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



▼ To hide column heads:

1. In a detail section you want to modify, right-click a column.
2. Click the Layout Columns popup that appears.
3. The Layout Columns dialog box appears.
4. Click the column titles you want to hide.
5. Click OK.

   The dialog box closes and the table's columns reset and now present only the information you want.

Viewing Modes

GDM Menu Bar

GDM Dashboard's Menu bar offers the following selections: Action, View, Reports, and Help.

GDM Menu bar

Action

The following commands can found under the Action menu.

Action Menu Commands

New Window	Allows you to open a new window, allowing you to simultaneously monitor multiple master servers, or configure additional views of a single master server's information.
Change GDM Server	Allows you to specify and connect to a different GDM Server.
<Previous GDM Servers>	Allows you to see a list of all previously viewed GDM Servers.
Configure	Allows you to configure or modify general properties and data collection properties for managed master servers. For more information, see "Advanced Configuration" on page 19.
Exit	Allows you to shut down the GDM Dashboard.

Action Menu Commands	
Data Collection Settings	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 clients at risk Sample Rate is the setting GDM uses to poll managed master 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.

View

The following commands are found under the View menu.

View Menu Commands	
Sort by Name	Allows you to sort the left pane by master server name.
Sort by Status	Allows you to sort the left pane according to the status of error conditions on the master server.
Sort Ascending	Allows you to sort the master server list in ascending, alphabetical order.
Sort Descending	Allows you to sort the master server list in descending order.
View Servers as Grid	Allows you to view the master server list using individual grid rows and columns.

View Menu Commands

View Servers as List	Allows you to view the master server list using as a list, rather than as a grid.
Grid Columns	Allows you to set the number of grids columns to use when viewing the master list as a grid. Grids can be divided using 1, 2, 3, or 4 columns, with 2 columns being the default.
Master Servers	Toggle switch used to display the master 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

Reports

The following reports can be launched from the Reports menu.

Reports Menu Reports

Problems and Conditions	Displays a report that lists all problems that exist on monitored managed servers in the system.
Drive Status Summary	Displays a report that shows the current status of all the drives in the system.
General Status Summary	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	Allows you to gain help through the GDM Help engine.
VERITAS web page	Allows you to access the VERITAS web site.
About GDM Dashboard	Shows version and copyright information about GDM.

GDM Toolbar

GDM Dashboard's Toolbar offers the following selections: Change GDM Server, Grid Column Adjustments (using both List Box and Button technologies), and About GDM.

GDM Toolbar

Change GDM Server Icon

Using the Change GDM Server icon quickly allows you to change GDM Servers.

▼ To change GDM Servers:

1. Click the GDM Server icon from the GDM Toolbar.

   The Change GDM Server dialog box appears.

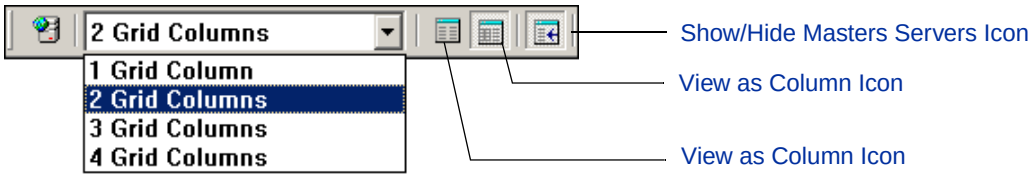
2. Enter a GDM Server name (or its IP address), or select from a list of GDM Servers that have been previously monitored using Dashboard.

3. Click OK.

Changing Grid Columns

You can change the number of grid columns that appear in the left pane by using the Grid Columns selection box. Dashboard left pane defaults to using a two column format.

Grid Column Selection Box



▼ To change the number of grid columns:

1. Click the Grid Columns selection box.
2. Click the number of columns you want to use.

View As List Icon

The View As List icon 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 icon.

The left pane changes from a column-based view to a list-based view.

View As Column Icon

The View As Column icon 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 Column icon.

The left pane changes from a list-based view to a column-based view.

Show/Hide Master Servers Icon

The Show / Hide Master Servers icon is a toggle button that either displays or hides Dashboard's left pane.

▼ To show/hide the left pane:

❖ Click the Show / Hide icon.

The left pane is either hidden from view or displayed.

About GDM

The About icon, in the form of a yellow question mark, displays information about GDM Dashboard.

▼ For GDM Dashboard information:

❖ Click the About icon.

GDM Usage Scenarios

This section offers insights on how GDM is typically used. The information is presented in a Frequently Asked Questions format.

I've just started GDM Dashboard. Where do I start?

Workflow for the GDM Dashboard normally starts in the left pane in GDM Summary mode. This mode 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 master server showing the indicator to gain more details about the issues that have been detected. These details are displayed in the right pane.

I'd 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 and Conditions entry.

I'd like to know how many failed jobs occurred at a managed master server. How do I do it?

In the left pane, click a managed master server name for which you'd like information about failed jobs. Details for that master 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 62.

I've noticed in the Robot detail sections of a particular managed master 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've configured multiple GDM Domains. How do I monitor the master servers in those other domains?

In order for GDM Dashboard to monitor master servers in your other domains, you must point Dashboard to the GDM Server of the other domain. Only then can GDM Dashboard successfully monitor master servers in other domains.

For details on changing GDM Servers, see "Monitoring GDM Servers Located in Different GDM Domains" on page 17.

Reports 5

This section provides information on GDM reports.

Reports includes the following topics:

Section	Description
"Generating and Viewing Reports" on page 77	Describes the GDM-generated reports that show detailed information about your managed master servers.
"Viewing Reports" on page 78	Describes how to view GDM reports.
"Printing Reports" on page 78	Describes how to print GDM reports.
"Problem and Conditions Report" on page 80	Describes the Problem and Conditions report.
"Drive Status Summary Report" on page 80	Describes the Drive Status Summary report.
"General Status Report" on page 81	Describes the GDM-generated reports that show detailed information about your managed master servers.

Generating and Viewing Reports

GDM Dashboard generates reports that show detailed information about your managed master 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.

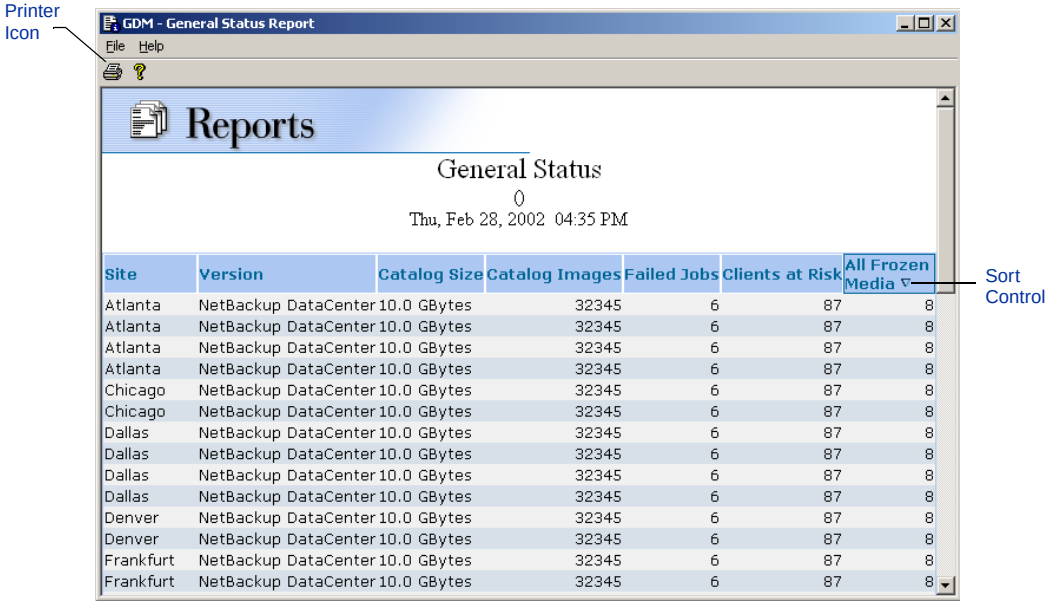
Viewing Reports

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 spawns 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



Printing Reports

In addition to viewing default Dashboard reports, you can also print them.

Note Depending on the Dashboard client you are using, a default printer for either the Windows and 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 and Conditions Report"
- "Drive Status Summary Report"
- "General Status Report"

Problem and Conditions Report

The Problem and Conditions 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 and Conditions Report Column Descriptions

Field	Description
Status	The operational status of the master server named in the Site column. Statuses include Critical, Warning, and Informational.
Site	The user-defined name given to the managed master server being monitored by Global Data Manager. For example, *Atlanta*.
Problem or Condition	The problem or condition that is affecting the managed master server.
Local Time	The local time where the managed master server is physically located.

Drive Status Summary Report

The Drive Status Summary 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 Summary Report Column Descriptions

Field	Description
Status	The status of drives at the master server (and its media servers) named in the Site 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 master server is unreachable), and Okay (no drives are down).
Site	The user-defined name given to the managed master server being monitored by Global Data Manager. For example, *Atlanta*.
Total Drives	The total number of drives being managed by the master server named in the Site column.

Drive Status Summary Report Column Descriptions

Field	Description
Downed Drives	The total number of drives being managed by the master server named in the Site column that are presently in a down state.
Active Drives	The total number of drives being managed by the master server named in the Site column that are presently in an active state.
Inactive Drives	The total number of drives being managed by the master server named in the Site column that are presently inactive.
Jobs in Progress	The total number of jobs that are in progress, that are being monitored by the master server named in the Site column.

General Status Report

The General Status report provides general status information about all managed master servers being monitored in the system.

General Status Report Column Descriptions

Status	Description
Site	The user-defined name given to the managed master server being monitored by Global Data Manager. For example, *Atlanta*.
Version	The version of NetBackup installed at the managed master 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.
Clients at Risk	The total number of clients that have not been backed up in a predetermined time.
All Frozen Media	The number of pieces of media that are considered to be frozen, or inaccessible.

Special Limitations 6

Because NetBackup 4.5 debuts both an updated look-and-feel and new architectural enhancements that are designed to increase scalability, all NetBackup GUI functions are now accessed through a single, consolidated application. Along with replacing the NetBackup 3.4 administrative GUI with an Explorer-like interface, the Global Data Manager interface has been removed and completely redesigned, implementing more robust scalability while at the same time offering *at-a-glance* health monitoring.

Due to these architectural improvements, the following apply for Global Data Manager 4.5:

- GDM 4.5 supports only NetBackup 4.5 managed servers. Support for NetBackup 3.4 and Backup Exec managed servers will be implemented in a future release.
- GDM 4.5 focuses on real-time monitoring of drives, jobs and configuration information, all of which can be viewed in a single, consolidated view. Information about policies, storage devices, and other NetBackup-related details can no longer be viewed in a single, consolidated view although this information can be viewed on a per-server basis using the NetBackup administration console.
- New historical reports are now available for GDM in the NetBackup add-on option, *VERITAS NetBackup 4.5 Advanced Reporter for UNIX and Windows*.

  Advanced Reporter extends the basic reporting feature of Global Data Manager by giving you the ability to customize detailed historical reports based on your GDM Server environment.
- The ability to view and change managed server configurations using GDM is now handled by opening the NetBackup administration console and selecting the desired managed server.

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.

Troubleshooting FAQ

Use this section for troubleshooting purposes.

I started GDM 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.

Common problems include

- not setting the correct display variable (solution: use the "-d hostname:0" option to gdmSA),
- exporting the GUI to a system different from the one you run the gdmSA start-up command.

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 Dashboard Windows client 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, GDM Dashboard 4.5's Windows client uses technical components of 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 (VERITAS Information Server Daemon).

Verify that the VISD is running on the GDM Server. The GUI retrieves GDM information from the GDM Server by connecting to the VISD. Run the `/usr/openv/netbackup/bin/bpps` command to see if visd is listed.

I have the GUI running, but there are no managed servers shown in the left pane. Why?

Did you configure the list of managed servers? Refer to "Configuring GDM" on page 13 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 - master 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 adding duplicate entries. Nonetheless, it is possible if more than one user is modifying the list at the same time, or if VISD is quickly shutdown 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 simply 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 is running on the managed server. The GDM Server's visd communicates with the managed server's visd to get information about the managed server.

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 managed server's fully-qualified domain name correct? That name appears in the horizontal bar next to the display name. For example, *Atlanta (master.server.com)*. Perhaps the master 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's grid. If you see some data, but not all, then you may have the data collection interval set too infrequently. Refer to the section, "Advanced Configuration" on page 19.

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. Refer to the section, "Enabling GDM Logging" on page 36.

After enabling logging and restarting 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's 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's 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 servers' 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 block waiting for space to become available, hence the unresponsiveness. The size of GDM's 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 job, image and media. In addition, GDM's database does not store historical data; therefore it will not grow over time like NetBackup Advanced Reporter's database.

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 the neither the NetBackup Database or the VISD service / 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 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.

Note Refer to “Enabling GDM Logging” on page 36 for additional GDM logging details

▼ **To start VISD manually on UNIX:**

- At a command prompt, enter:

```
$ /usr/openv/netbackup/bin/visd -console -debug
```

▼ **To start VISD manually on Windows NT/2000:**

1. Open a command prompt.
2. Enter the following:

```
c:\Program Files\VERITAS\NetBackup\bin> visd -console -debug
```

Additional VISD shutdown issues

VISD can also shut down prematurely if you have the VERITAS NetBackup Advanced Reporter option installed and running.

Problems occur in this scenario when the GDM data collector shuts down because it can't communicate with the GDM Server database. In this instance, the GDM Server database daemon (which communicates with the data collector) doesn't start because the default port it uses for communication is already in use by NetBackup Advanced Reporter's database daemon. Resolution is to either change NetBackup Advanced Reporter's database daemon port, or NetBackup's database daemon port.

For information on changing the NBAR database daemon port, see your VERITAS NetBackup Advanced Reporter documentation.

For information on changing the NetBackup database daemon port, see your VERITAS NetBackup System Administrator's Guide.

Glossary

access control list (ACL)

Security information associated with files on some file systems.

ACS

Automated Cartridge System. This robot type is supported only by NetBackup DataCenter servers.

active job

A job for which NetBackup is currently processing backup or restore data.

activity logs

See “debug logs.”

activity monitor

A NetBackup administration utility that displays information about NetBackup jobs and provides limited control over them.

administration client

See “remote administration console.”

administrator

A user that is granted special privileges to install, configure, and manage the operation of a system, network, or application

AIT

Sony Advanced Intelligent Tape, a type of tape drive or media type.

alternate-client restore

Restoring files to your client when they were originally backed up from a different client. The administrator using the interface on the master server can direct a restore to any client (this variation is called a server directed restore).

alternate-target restore

See “redirected restore (different target).”

alternate path restore

See “redirected restore (different path).”

archive

A special kind of backup where NetBackup backs up the selected files, and if the backup is successful, deletes the files from the local disk. In this manual, references to backups also apply to the backup portion of archive operations except where otherwise noted.

archive bit

A file-status bit that the Microsoft based operating system sets when it writes a file, thereby indicating that the file has changed.

attributes for a policy

Configuration parameters that control the behavior of NetBackup during operations involving this policy.

automatic backup

A scheduled backup by the master server.

back up

The act of copying and saving files and folders to storage media.

backup

Refers to the process of copying and saving files and directories to storage media. For example, *the backup is complete*. This term can also refer to the collection of data that NetBackup saves for a client during a backup or archive. For example, *duplicate the backup*.

Backup is two words when used as a verb. For example, *back up the file*.

backup, archive, and restore interface

The name of the NetBackup Microsoft Windows and Java based user interfaces for clients. On servers, these interfaces can be started through the NetBackup Administration Console.

backup window

The period of time during which backups can begin.

block size

The number of bytes in each block of data written on the media during a backup.

bp

A backup, archive, and restore utility for users on NetBackup UNIX clients. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bpadm

An administrator utility that runs on NetBackup UNIX servers. It has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

bp.conf file

A NetBackup configuration file on UNIX servers and also on UNIX, Macintosh, and OS/2 clients.

bp.ini file

NetBackup initialization file for Novell NetWare target clients.

bpcd

NetBackup Client service on Windows NT/2000 and the NetBackup Client daemon on UNIX.

bprd

NetBackup Request Manager service on Windows NT/2000 and NetBackup Request daemon on UNIX.

cancel a job

Terminating a job and removing it from the job queue.

catalogs

Internal NetBackup and Media Manager databases. These catalogs contain information about configuration, media, devices, status, errors, and the files and directories in the stored backup images.

CDF

Context-dependent file, which is a type of directory structure on a Hewlett-Packard system.

class

See “policy.”

client

The system with the files to back up, archive, or restore.

client-user interface

See “user interface.”

cluster

See master and media server cluster.

command lines

Commands that users can execute either from the system prompt or in scripts.

compression

The process of compacting data to enable more efficient transmission and storage.

configuration

The parameters that govern the behavior of an application. This term can also refer to the manner in which a network or system is laid out or connected (for example, a network configuration).

cpio

A UNIX command that can be used for copying files to or from a cpio archive on disk or tape.

ctime

The time that a UNIX inode was changed.

cumulative-incremental backup

A backup that is scheduled by the administrator on the master server and backs up files that have changed since the last successful full backup. All files are backed up if no prior backup has been done. Also see “differential-incremental backup.”

daemon

A program on a UNIX system that runs in the background and performs some task (for example, starting other programs when they are needed). Daemons are generally referred to as services or processes on Windows NT/2000 systems.

Dashboard

The name for the Global Data Manager graphical interface.

database-agent clients

Clients with additional NetBackup software that is designed to back up relational databases.

database-extension clients

See “Dashboard.”

debug logs

Logs that can be optionally enabled for specific NetBackup programs and processes and then used to investigate problems.

device delays

Delays caused by the device that are beyond the control of the storage application. An example is the time required to position tape under the read and write heads.

device host

A host (that has Media Manager installed) where a drive or robotic control is attached or is defined.

device monitor

A Media Manager administration utility that provides monitoring and manual control of Media Manager storage devices. For example, an administrator or computer room operator can use this utility to manually reset devices or set them to the UP or DOWN state.

DHCP

Dynamic host configuration protocol. This TCP/IP protocol automatically assigns temporary IP addresses to hosts when they connect to the network.

differential-incremental backup

Scheduled by the administrator on the master server and backs up files that have changed since the last successful incremental or full backup. All files are backed up if no prior backup has been done. Also see “cumulative-incremental backup.”

directory depth

The number of levels below the current directory level that the NetBackup interfaces show in their directory and file list displays.

directory tree

The hierarchical structure in which files are organized on a disk. Each directory lists the files and directories that are directly below it in the tree. On UNIX, the topmost directory is called the root directory.

disaster recovery

Recovering data from backups after a disk crash or other catastrophe.

disk

Magnetic or optical disk storage media.

disk-image backup

A bit-by-bit rather than a file system backup of a disk drive on Windows NT/2000.

DLT

Digital-linear tape or tape drive type.

Domain Name Service (DNS)

A program that handles name translation for network communications.

drive cleaning

The use of a special cleaning tape to clean the heads on a drive.

duplicate image

A copy of a backup image.

encryption

Provides additional security by encrypting backup data on the client. This capability is available only with the NetBackup Encryption option.

entry and exit ports

See “media access port.”

exclude list

A list that designates files or directories to exclude from automatic backups.

expiration (image)

The date and time when NetBackup stops tracking a backup image.

expiration (volume)

The date and time when the physical media (tape) is considered to be no longer usable.

external media ID

This is an identifier written on a media cartridge or canister to help the operator identify the volume before inserting it into a drive or robot. For labeled media, the external media ID should be the same as the media ID recorded on the media.

EVSN

See “external media ID.”

FastBackup

A special type of raw-partition backup that can be performed only on an Auspex client (this option is available only for NetBackup DataCenter).

FlashBackup

A special type of raw-partition backup that requires the NetBackup FlashBackup separately-priced option (this option is available only for NetBackup DataCenter).

flush level

Controls how often Netbackup clears its log files on a Novell NetWare or Microsoft Windows client platform.

fragment

A part of a backup or archive image. NetBackup can be configured to divide images into fragments when they exceed a certain size or span tapes.

frequency (backup)

How often NetBackup performs scheduled backups. For example, if the frequency is seven days then backups occur once a week.

FROZEN media state

If a volume is FROZEN, NetBackup keeps it indefinitely and can restore from it but not use it for further backups or archives.

full backup

A backup that copies, to a storage unit, all files and directories that are beneath a specified directory.

FULL media state

If this appears in a report or listing, it indicates the volume is FULL and cannot hold more data or be used for further backups.

global attributes

NetBackup configuration attributes that affect all policies.

GDM Dashboard

The name for the Global Data Manager interface. The Dashboard enables monitoring job and drive activity on multiple master servers, as well as providing alerts to problem conditions.

GDM Domain

A set of multiple master servers monitored and managed by a single server known as the GDM Server.

GDM Managed Server

A master server that has the GDM Managed Server license activated and has been configured as a member of a GDM domain.

gdmSA

The Java-based GDM Dashboard interface.

GDM Server

A NetBackup master server that has the Global Data Manager license activated. When logging into this host, the user can monitor the activity on multiple master servers using the GDM Dashboard interface. If the host has installed the Advanced Reporter option, the reports show information on multiple master servers.

Global Data Manager (GDM)

A separately-priced option that provides consolidated reporting in NetBackup Advanced Reporter and consolidated monitoring of backup activity on multiple master servers. There are two GDM licenses -- GDM Server (for the head of the GDM domain) and GDM Managed Server (for each master server in the GDM domain)

GNU tar

A public domain version of the UNIX tar program.

goodies directory

A directory containing programs, scripts, and other files that are not formally supported.

GUI

Graphical user interface.

hard link

On UNIX, a hard link is a pointer to the inode for the data. On Windows NT/2000 a hard link is a directory entry for a file. Every file can be considered to have at least one hard link. On NTFS volumes each file can have multiple hard links, and a single file can appear in many directories (or even in the same directory with different names).

heap level

A parameter for memory-heap debugging on a Novell NetWare or Windows NetBackup client.

hierarchical storage management

The process of automatically migrating selected files from a managed file system to specified migration levels on secondary storage, while maintaining transparent access to those files.

host

A computer that executes application programs.

host name

Name by which a host computer is identified by programs and other computers in the network.

HSM

See storage migrator.

image

The collection of data that NetBackup saves for an individual client during each backup or archive. The image contains all the files, directories, and catalog information associated with the backup or archive.

import

The process of recreating NetBackup records of images so the images can be restored.

include list

A list that designates files or directories to add back in from the exclude list.

incremental backup

See “cumulative-incremental backup” and “differential-incremental backup.”

inport

See “media access port.”

inode

A UNIX data structure that defines the existence of a single file.

install_path

Directory where NetBackup and Media Manager software is installed. The default on Windows NT/2000 is `C:\Program Files\VERITAS` and on UNIX it is `/usr/openv`.

jbpSA

The Java-based NetBackup interface for performing user backups, archives, and restores.

jnbSA

The Java-based NetBackup interface for administrators.

job

A parcel of work submitted to a computer. NetBackup jobs are backups, archives, or restores.

kernel

The nucleus of an operating system.

keyword phrase

A textual description of a backup.

kill a job

See “cancel a job.”

label

Identifier of a tape or optical disk volume. A recorded label includes a media ID.

A barcode label allows a barcode scanner to be used for media tracking.

library

See “robotic library.”

link

See “hard link” or “symbolic link.”

LMF - Library Management Facility

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

This robot type is supported only by NetBackup DataCenter servers.

load

(noun) Amount of work that is being performed by a system or the level of traffic on a network. For example, network load affects performance.

(verb) Copy data to internal memory. For example, load the installation program.

logs

Files where a computer or application records information about its activities.

mailslot

See “media access port.”

man pages

Online documentation provided with UNIX computer systems and applications.

Master and media server cluster

A NetBackup master server and the remote media servers that it is using for additional storage. It is possible to configure clusters only with NetBackup DataCenter servers. NetBackup BusinesServer supports only a single server, the master.

Master of Masters

A NetBackup host where Global Data Manager software is installed. When logging into this host, the interface has a tree view where the administrator can view and administer multiple master servers.

master server

The NetBackup server that provides administration and control for backups and restores for all clients and servers in a master and media server cluster. NetBackup BusinesServer supports only a single server and it is the master.

media

Physical magnetic tapes, optical disks, or magnetic disks where data are stored.

media access port

A slot or other opening in a robot where you can insert or remove a tape without having to access the interior of the robot. After inserting a tape, you move it to a slot by using an inject command. Prior to removing a tape, you move it to the port by using an eject command. The inject and eject commands are supported through the add and move screens in the Media Manager administration interface.

media host

NetBackup server to which the job (client) is sending the data.

media ID

An identifier that is written on a volume as part of the recorded label.

Media Manager

Software that is part of NetBackup and manages the storage devices and removable media.

Media Manager Host

See “device host.”

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.

media server

A NetBackup server that provides storage within a master and media server cluster. The master can also be a media server. A media server that is not the master is called a remote media server (or slave server). NetBackup BusinesServer does not support remote media servers.

menu interface

A character-based interface for use on terminals that do not have graphical capabilities.

MHD

See “Shared Storage Option (SSO).”

mount

Make a volume available for reading or writing.

mount point

The point where a file system on a disk logically connects to a system’s directory structure so the file system is available to users and applications.

MPX

See “multiplexing.”

mtime

The point in time when a UNIX or NTFS file is modified.

multiplexing

The process of sending concurrent-multiple backups from one or more clients to a single storage device and interleaving those images onto the media.

multiplexed group

A set of backups that were multiplexed together in a single multiplexing session.

NDMP

Network data management protocol. NetBackup requires the NetBackup for NDMP separately-priced option to support NDMP.

NetBackup Client service

NetBackup Windows NT/2000 service that runs on clients and servers and listens for connections from NetBackup servers and clients in the network. When a connection is made, this service starts the necessary programs.

NetBackup configuration options

On UNIX servers and on UNIX and Macintosh, clients, these settings are made in the `bp.conf` file. On NetWare target and OS/2 clients, they are in the `bp.ini` file. On Windows NT/2000 servers and Microsoft Windows clients, these settings are called properties and are made through the Backup, Archive, and Restore interface or the Host Properties dialog in the NetBackup Administration Console.

NetBackup databases

See catalogs.

NetBackup Database Manager service

NetBackup Windows NT/2000 service that runs on the master server and manages the NetBackup internal databases (called catalogs). This service must be running on the master server during all NetBackup administrative operations.

NetBackup Device Manager service

The NetBackup Windows NT/2000 service that runs on a NetBackup server and starts the robotic control processes and controls the reservation and assignment of volumes. This service runs only if the server has devices under Media Manager control. The process is `ltid`.

NetBackup properties

Same as NetBackup configuration options but are called NetBackup properties on Microsoft Windows platforms.

NetBackup Request Manager service

The NetBackup Windows NT/2000 service that runs on the master server and starts the scheduler and receives requests from clients.

NetBackup Volume Manager service

A NetBackup Windows NT/2000 service that runs on a NetBackup server, allows remote administration of Media Manager, and manages volume information. The process is `vmd`.

NIS

Network information service.

NLM

NetWare loadable module.

NFS

Network file system.

nonrobotic

See “standalone.”

ODL

Optical disk library. This robot type is supported only by NetBackup DataCenter servers.

outport

See “media access port.”

partitions

The logical partitions into which a magnetic disk is divided.

patch

A program that corrects a problem or adds a feature to an existing release of software.

path length

Number of characters in a pathname.

pathname

The list of directories in the path to a destination directory or file.

PC clients

NetBackup clients that have Microsoft Windows (NT/2000, 98, 95), Macintosh, or IBM OS/2 operating systems.

peername

The name by which a computer identifies itself when establishing connections to other systems.

policy

Defines the backup characteristics for a group of one or more clients that have similar backup requirements.

port

A location used for transferring data in or out of a computer.

Also see “media access port.”

primary copy

The copy of an image that NetBackup uses to satisfy restores. When NetBackup duplicates an image, the original is designated as the primary copy.

privileges

The tasks or functions that a user, system, or application is authorized to perform.

progress report

Log where NetBackup records events that occur during user operations.

proxy restore

A proxy restore allows the user to restore files that he has write access to, on a machine other than his desktop. The files must be in a backup of the machine to which they are being restored.

QIC

Quarter-inch-cartridge tape.

queued job

A job that has been added to the list of jobs to be performed.

raw-partition backup

Bit-by-bit backup of a partition of a disk drive on UNIX. On Windows NT/2000, this is called a disk-image backup.

rbak

The program that Apollo clients use to read data from tape during a restore.

recorded media ID

This is an identifier written as part of the label on a volume and used by Media Manager to ensure that the correct volume is mounted. The recorded media ID should match the external media ID.

redirected restore (different client)

Restoring files to your client when they were originally backed up from a different client. The administrator using the interface on the master server can direct a restore to any client (this variation is called a server directed restore).

redirected restore (different target)

On a Novell NetWare server platform running the NetBackup target version of client software, this operation restores files to a different target than the one from which they were backed up.

redirected restore (different path)

Restores files to a different directory than the one from which they were backed up.

registry

A Microsoft Windows 2000, NT, 98, and 95 database that has configuration information about hardware and user accounts.

remote administration console

A Windows NT/2000 NetBackup client that has the administration interface software installed and can be used to administer NetBackup servers.

remote media server

A media server that is not the master. Note that only NetBackup DataCenter supports remote media servers. NetBackup BusinesServer supports only a single server, the master.

residence

In Media Manager, information about the location of each volume is stored in a volume database. This residence entry contains information, such as robot number, robot host, robot type, and media type.

resource

A Novell NetWare term that refers to a data set on the target. For example, in DOS, resources are drives, directories, and files. Also see “target service.”

restore

(verb) The act of restoring selected files and directories from a previous backup or archive and returning them to their original directory locations (or to a different directory).

(noun) The process of restoring selected files and directories from a previous backup and returning them to their original directory locations (or to a different directory).

retention level

An index number that corresponds to a user-defined retention period. There are 10 levels from which to choose (0 though 9) and the retention period associated with each is configurable. Also see “retention period.”

retention period

The length of time that NetBackup keeps backup and archive images. The retention period is specified on the schedule.

robotic library

Refers to a robot and its accompanying software. A robotic library includes a collection of tapes or optical platters used for data storage and retrieval. For example, a Tape Library DLT (TLD) refers to a robot that has TLD robotic control.

root

The highest level directory in a hierarchical directory structure. In MS-DOS, the root directory on a drive is designated by a backslash (for example, the root on drive C is C:\). On UNIX, the root directory is designated by a slash (/).

Also, a UNIX user name having administration capability.

RS-232

An industry-standard interface for serial communications and sometimes used for communicating with storage peripherals.

RSM Interface

Application in Windows 2000 used to manage Removable Storage Manager (RSM) devices.

RSM - Removable Storage Manager

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

Also, a component of the Windows 2000 operating system that manages storage devices.

RVSN

See “recorded media ID.”

schedules

Controls when backups can occur in addition to other aspects of the backup, such as: the type of backup (full, incremental) and how long NetBackup retains the image.

SCSI

Small computer system interface. This is a type of parallel interface that is frequently used for communicating with storage peripherals.

server-directed restore

Using the user interface on the master server to restore files to any client. Only the administrator can perform this operation.

server independent restore

Restoring files by using a NetBackup server other than the one that was used to write the backup. This feature is available only with NetBackup DataCenter.

server list

The list of servers that a NetBackup client or server refers to when establishing or verifying connections to NetBackup servers. On a Windows NT/2000 server and Microsoft Windows clients, you update the list through a dialog box in the interface. On a UNIX server and UNIX and Macintosh clients, the list is in the `bp.conf` file. On NetWare target and OS/2 clients, the list is in the `bp.ini` file.

service

A program on a Windows NT/2000 system that runs in the background and performs some task (for example, starting other programs when they are needed). Services are generally referred to as daemons on UNIX systems.

session

An instance of NetBackup checking its schedules for backups that are due, adding them to its worklist, and attempting to complete all jobs in the worklist. For user backups and archives, a session usually consists of a single backup or archive.

shared drives

See “Shared Storage Option (SSO).”

Shared Storage Option (SSO)

A separately priced VERITAS software option that allows tape drives (standalone or in a robotic library) to be dynamically shared among multiple NetBackup and Storage Migrator servers.

This option is supported only on NetBackup DataCenter servers.

SMDR

Storage management data requestor, a Novell NetWare program that provides its services transparently to all SMS modules and lets remote and local modules communicate with one another.

SMS

Novell NetWare storage management services.

SSO

See “Shared Storage Option (SSO).”

standalone

A qualifier used with drives and media to indicate they are not associated with a robot. For example, a standalone tape drive is one where you must manually find and insert tapes before using them. A standalone volume is one that is located in a standalone drive or is stored outside of a drive and designated as standalone in the volume configuration.

status code

A numerical code, usually accompanied by a message, that indicates the outcome of an operation.

storage migrator

Refers to the VERITAS Storage Migrator line of hierarchical storage management products for UNIX and Windows NT/2000. These products make extra room on a disk by transparently moving data to other storage and then transparently retrieving the data when it is needed by a user or application.

Storage Migrator is available only for NetBackup DataCenter servers.

storage unit

Refers to a storage device where NetBackup or Storage Migrator stores files. It can be a set of drives in a robot or consist of one or more single tape drives that connect to the same host.

SUSPENDED media state

If a volume is SUSPENDED, NetBackup can restore from it but cannot use it for backups. NetBackup retains a record of the media ID until the last backup image on the volume expires.

symbolic link

On a UNIX system, this is a pointer to the name of the file that has the source data.

tape format

The format that an application uses to write data on a tape.

tape marks

A mark that is recorded between backup images on a tape.

tape overhead

The space required for data that is not part of the backup images. For example, tape marks and catalogs of what are on the tape are considered overhead.

tape spanning

Using more than one tape to store a single backup image.

tar

Tape Archive program that NetBackup uses to extract backup images during a restore.

target

See “target service.”

target service

A Novell NetWare service that needs storage management. The SMS views all services (for example, print services, communication services, workstations) as targets.

Target Service Agent

A Target-service agent is a Novell NetWare agent that prepares the target's data for SMS during a backup and for the target during a restore.

TLD - Tape Library DLT

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

TLH - Tape Library Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

This robot type is supported only by NetBackup DataCenter servers.

TLM - Tape Library Multimedia

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

This robot type is supported only by NetBackup DataCenter servers.

TL4 - Tape Library 4MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

TL8 - Tape Library 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

timeout period

The period of time that an application has allotted for an event to occur.

TIR

See “true image restore.”

tpconfig

A Media Manager administration utility for configuring devices, which is started from the command line. On UNIX, it has a character-based, menu interface that can be run from terminals that do not have X Windows capabilities.

transfer rate

The rate at which computer information is transferred between a source and a destination.

true image restore

Restores the contents of a directory to what it was at the time of any scheduled full or incremental backup. Previously deleted files are ignored.

TS8 - Tape Stacker 8MM

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

TSA

See “Target Service Agent.”

TSH - Tape Stacker Half-inch

A Media Manager designation for a category of robot. For the specific vendor types and models in this category, see the Supported Peripherals section of the NetBackup release notes.

This robot type is supported only by NetBackup DataCenter servers.

user interface

The program used to perform user backups, archives, and restores.

user operation

A backup, archive, or restore that is started by a person on a client system.

verbose flag

Configuration file entry that causes a higher level of detail to be written in the logs.

verify

An operation that compares the list of files that are actually on a volume with what NetBackup has recorded as being on it. The data that is on the media is not verified.

VISD

VISD (VERITAS Information Server Daemon) is a service that runs on any master server with GDM system components installed. For example, the GDM Server or a GDM managed server. VISD listens on a TCP port for requests from GDM clients. Clients include the GDM Dashboard user interface and Information Servers on NetBackup Master Servers.

vmadm

A Media Manager administrator utility for managing volumes. It runs on UNIX and has a character-based, menu interface that can be run from terminals.

vm.conf

A Media Manager configuration file with entries that include the servers that can manage local devices and default media ID prefixes for media that do not contain barcodes.

volume

Media Manager volumes are logical units of data storage or cleaning capability on media that have been assigned media IDs and other attributes, which are recorded in the Media Manager volume database.

volume configuration

Refers to configuration information that is stored in the Media Manager volume database.

volume database

An internal database where Media Manager keeps information about volumes. All hosts (where Media Manager is installed) have a volume database. However, the database is empty unless the host is designated as a volume database host.

volume database host

The host (where Media Manager is installed) that contains information about the volumes that Media Manager uses in a device. Because NetBackup BusinesServer supports only a single server, the volume database host is always on the same server.

volume group

A set of volumes that are configured within Media Manager to reside at the same physical location (for example, in a specific robot).

volume pool

A set of volumes that are configured within Media Manager to be used by a single application and are protected from access by other applications and users.

wakeup interval

The time interval at which NetBackup checks for backups that are due.

wildcard characters

A character that can be used to represent other characters in searches.

WORM media

Write-once, read-many media for optical disks. NetBackup BusinesServer does not support WORM media.

Windows Display Console

A NetBackup-Java interface program that runs on Windows 2000, NT, 98, and 95 computers. Users can start this interface on their local system, connect to a UNIX system that has the NetBackup-Java software installed, and then perform any user operations that their permissions allow.

xbp

The X Windows-based backup, archive, and restore program for users on NetBackup UNIX clients.

Index