

Veritas NetBackup Operations Manager[™] Guide

Windows and Solaris

Release 6.5

Veritas NetBackup Operations Manager Guide

Copyright © 2005 - 2007 Symantec Corporation. All rights reserved.

NetBackup Operations Manager 6.5

Symantec, the Symantec Logo, and NetBackup Operations Manager are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID, SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be “commercial computer software” and “commercial computer software documentation” as defined in FAR Sections 12.212 and DFARS Section 227.7202.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
www.symantec.com

Printed in the United States of America.

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder. All third-party copyrights that are associated with this product are listed in the accompanying release notes.

Solaris is a trademark of Sun Microsystems, Inc.

Windows is a registered trademark of Microsoft Corporation.

Licensing and registration

Veritas NetBackup is a licensed product. See the *NetBackup Installation Guide* for license installation instructions.

Technical support

For technical assistance, visit <http://entsupport.symantec.com> and select phone or email support. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service

Contents

Chapter 1	NetBackup Operations Manager overview	
	What is NetBackup Operations Manager?	12
	Why use NetBackup Operations Manager?	12
	NetBackup Operations Manager components	16
	The NOM console	18
	NOM deployment	18
	Managed NetBackup master servers	20
	Where to go in this guide for specific NetBackup Operations Manager information	20
Chapter 2	Installing NetBackup Operations Manager	
	Planning a NetBackup Operations Manager installation	24
	Shared and unshared software components that NOM uses	24
	Choosing a server where NOM is installed	25
	Web browser considerations	26
	Global Data Manager and NetBackup Advanced Reporter considerations	28
	Managed NetBackup master server considerations	28
	NetBackup Enterprise Server media kit (CDs)	31
	NetBackup Enterprise Server media kit (DVDs)	32
	Installation of NOM and required components	
	on a Windows server	34
	Before starting the installation	34
	Installing NetBackup client software on the NOM server	36
	Installing Symantec Product Authentication Service on the NOM server	36
	Installing NOM software	41
	Installing the Symantec Product Authentication Service before the NetBackup client	44
	Installation behavior on upgrading to NOM 6.5	47
	Installation of NOM and required components	
	on a Solaris server	47
	Before starting the installation	48
	Installing NetBackup client software on the NOM server	49
	Installing Symantec Private Branch Exchange and Symantec Product Authentication Service software on the NOM server	49

Installing NOM software	53
Installing the Symantec Product Authentication Service before Symantec Private Branch Exchange	56
Installation behavior on upgrading to NOM 6.5	57
After NetBackup Operations Manager is installed	58
Starting to use NOM	59
Start-up tasks that NOM performs	59
Tuning NOM for more performance	60
Troubleshooting NOM	61

Chapter 3 Administering NetBackup Operations Manager

NOM services and processes used by NOM	64
Services used by NOM on Windows	64
Processes used by NOM on Solaris	65
NOM server scripts on Solaris	66
Controlling NOM services and processes	67
Dependency of services	69
NOM database administration	69
Database maintenance utilities (NOMAdmin)	69
Moving the NOM database to a non-default location	75
Database troubleshooting	76
Back up and restore of NOM	77
Creating snapshots of the NOM and VxAM databases	78
Saving the NOM user profiles managed by Symantec Product Authentication Service	84
Using NetBackup to save the database snapshots and user profiles ...	84
Restoring NOM	85
NOM security topics	87
Configuring security for managed servers	87
Multiple security models	88
NOM users	92
Communication and firewall considerations	93
Support script in NOM	96
NOM and VBR single sign-on	97
Considerations for NOM and VBR	97
NOM and VBR single sign-on	98
NOM log files	102
VxUL log files	102
NOM log files on Windows servers	103
NOM log files on Solaris servers	105

Chapter 4 Getting started using the NOM console

Before you use the NOM console	110
Starting the NOM console	110
Accessing the NOM console	111
Logging on to the NOM console	112
Logging out of the NOM console	114
Possible issues when using the NOM console	114
NOM console components	116
Using the links on the title bar	117
Using tabs and subtabs	118
Using the refresh mode control	119
The connected to pane	119
Using the alert summary pane	120
Understanding the context pane	120
Using the task pane	123
Using the content pane	123
The NOM status bar	124
Visual keys in the console	124
Using tables	125
Using help to understand NOM views and tasks	130
A quick start for performing common tasks in NOM	131
Using NOM context groups	132
Configuring server groups or servers (using the context pane)	133
Configuring client or policy groups (using the context pane)	137
Selecting server, client, or policy groups to manage	139
Using Web browser bookmarks	141

Chapter 5

Understanding NOM alert policies and alerts

NOM alert policies	144
Creating alert policies	144
Managing your alert policies	148
Setting up the recipients to receive alerts	149
Administering NOM alerts	149
How NOM displays alerts in the console	149
How alerts are removed from the NOM database	150
Configuring NOM alert parameters	150
Viewing NOM alerts	151
Responding to NOM alerts	152
Using SNMP with NOM	153
About SNMP	153
SNMP versions	153
SNMP version supported in NOM	154
The Management Information Base (MIB) and NOM support	154
Process of generating SNMP traps in NOM using VxAM	154

	Frequently asked SNMP questions	155
Chapter 6	Troubleshooting NetBackup issues using NOM	
	NetBackup master and media server log files	158
	NetBackup jobs	160
	NetBackup services	162
Chapter 7	NOM monitoring, managing, and configuration topics	
	Understanding monitoring and managing group component summaries	166
	Overview summary and overview detail tabs	166
	Summary views for NetBackup and NOM categories	167
	Understanding NBSL monitors and the Partially Online server status	170
	NBSL (NetBackup Service Layer) monitors	170
	Partially Online managed server status in the context pane	172
	Configuring user preferences and system settings	172
	Setting preferences for NOM users	173
	Setting system preferences for the NOM server	177
Chapter 8	NOM reporting topics	
	Understanding NOM report capabilities	179
	Why use NOM reports?	180
	Quickly view the reports you need	180
	Accessing all NOM reports	181
	Scheduling reports to run when you need them	185
	Managing the schedule for a report	185
	Creating the reports you need	186
	Managing reports	186
	Using online help to obtain more information about reporting	186
	Running a report	187
	Running a report with run time parameters	188
	Performing tasks to manage your reports	191
	Emailing NOM reports	192
	Using the report builder wizard	194
	Required wizard screens for a custom report	196
	Optional wizard screens for additional report customization	201
	SQL grammar used by the wizard	207
	Building a sample report	211
	Using the composite report builder wizard	220
	Using the composite report builder screens	221
	Using the report scheduler wizard	223
	Using the report scheduler screens	223
	Upgrading reports from 6.0 or 6.0MPx to 6.5	226

	Migrating to the new reports	228
Chapter 9	Understanding NOM online help	
	Online help components	232
	Accessing online help	232
	Locating the topics you need	233
	Using the related topics in help	234
	Viewing graphics in thumbnails	234
	Using the quick-links page for help	234
	Using the options icons in help	235
Index		237

NetBackup Operations Manager overview

This guide contains getting started topics for using NetBackup Operations Manager (NOM) to manage and monitor key areas of your NetBackup™ Enterprise Server environment.

This guide assumes you are familiar with key backup concepts of NetBackup, Symantec Product Authentication Service, and the operating system of the server where NOM software is installed.

See the NetBackup Release Notes or the Welcome topic in the NOM online help for information about available NetBackup documentation and how to access the Symantec support site.

Topic	Description
“What is NetBackup Operations Manager?” on page 12	Provides an overview of NOM and its capabilities
“Why use NetBackup Operations Manager?” on page 12	Provides a list of benefits in using NOM in your NetBackup environment
“NetBackup Operations Manager components” on page 16	Provides an overview of the key components of NOM
“Where to go in this guide for specific NetBackup Operations Manager information” on page 20	Provides you with information to help you locate NOM information in this guide

What is NetBackup Operations Manager?

- NOM is an advanced, easy-to-use Web based application used for managing and monitoring NetBackup master and media servers, clients, and policies. NOM console can be used to monitor world-wide NetBackup sites in real-time on a 24-hour basis. NOM is included with NetBackup server products for no additional cost.
- NOM lets you view the operational status and health of your distributed data protection environment. NOM can manage and monitor dozens of NetBackup installations spread across multiple locations from a single point.
NOM does not require you to separately log on to each NetBackup master or media server.
- NOM provides a consistent interface to simplify the complex tasks necessary to effectively manage the data protection environment of a large enterprise effectively. NOM can monitor and manage NetBackup job activity, job policies, media, devices, and services. NOM also provides policy-based alert and notifications.
- NOM focuses on how to maintain your backup environment after you complete the NetBackup configuration.
You need to use the NetBackup Administration console and command line interfaces for core NetBackup administrative functions such as configuring media, storage units, and policies.
- NOM contains built-in standard reports that you can use immediately. You can modify these reports to meet your specific needs. You can also create your own reports using the custom report wizard.
These reports are designed for operational management and real-time monitoring. For optimal performance and scalability, you should manage approximately a month of historical data.

Why use NetBackup Operations Manager?

The management challenge

As the proliferation of data continues in today's computer environments, effective data management and analysis tools are required to manage and protect this valuable resource. As datacenters quickly grow and become more complex, it increases the difficulty of management. Remote management can be cumbersome and inefficient.

Management and reporting methods are critical functions in these complex enterprise environments. The ability to monitor, capture, and respond quickly to datacenter events is essential. When each of these requires multiple tools and areas of expertise, it presents challenges.

To determine each server's operational status without NOM, you need to log on to multiple servers and use the NetBackup Administration Console on each to view the server and its logs.

How NetBackup Operations Manager can help

NOM provides advanced management, as well as operational reports and alert functions that simplify administration of NetBackup environments. NOM offers you the ability to gain a real-time understanding of the health of your entire NetBackup server environment quickly.

NOM provides the ability to monitor and manage across multiple NetBackup master servers. The NOM server component is in continuous communication with NetBackup servers to provide a real-time view of operations. You can monitor selected subsets of servers, policies, or clients by using groupings and advanced data filter options.

Using NOM, you can diagnose problems, identify potential issues, or review the operational status of multiple NetBackup servers and clients at many locations. With NOM, you perform all these tasks from a centralized location.

Additional benefits of NetBackup Operations Manager include the following:

- *Managing and monitoring of global NetBackup servers*
You can monitor world-wide NetBackup sites in real-time on a 24-hour basis using NOM consoles. At remote sites where limited staff may be an issue, NOM enables you to use available resources in a more efficient manner. NOM provides "at-a-glance views" of the domain and the ability to drill down to monitor an individual NetBackup server for more detail. Built-in context groups of master servers, policies, or clients let you define groups and easily manage diverse geographical sites.
- *Single point of control*
Often the greatest challenge with globally distributed, complex enterprise datacenters is remote administration. Issues can range from a slow connection that requires increased administration time to installations with a large system footprint that consumes valuable space and resources. The NOM interface is Web based and provides efficient remote administration across multiple NetBackup servers from a single, centralized console. Administration can be done from any Web-enabled system. The system resource impact of NOM is minimal since it has few local installation requirements.

Network environments with multiple UNIX, Linux, or Windows NetBackup servers are commonly used to protect valuable data. Using the flexibility that NOM offers, you can easily administer heterogeneous systems from any Web-enabled system.

- *NOM alert monitor capability, notification, and management*

Management across many NetBackup servers can be complicated in enterprise environments, which makes management by exception desirable. In large, distributed environments, proactive management is necessary to head off potentially critical issues and problems.

NOM provides a policy-based alert system, which monitors and notifies you before serious problems happen to your NetBackup systems. The policy-based alert system in NOM can also be integrated with common event management frameworks or consoles.

You can use predefined alert conditions to create alert policies to monitor typical issues or thresholds within NetBackup. You can specify email or SNMP notification in response to an actual alert, which lets administrators focus on other job responsibilities. They no longer need to be logged in to a terminal to monitor systems continuously.

NOM lets you track all policy updates over time by displaying a side-by-side comparison of one version with the next.

- *Standard and custom reporting capabilities*

Many NetBackup sites use custom scripts to meet their reporting needs and often get too much or too little information in these reports. Also, many administrators expect immediate access to specific information, for example, server status, job status, restorability of data, and so on.

NOM provides operational report capabilities to support your backup operations team. The NOM reports contain the data that the NOM server collects from your NetBackup master servers. You can use reports on backup performance, media utilization, and success rates of jobs and policies to assess your NetBackup environment.

NOM comes with built-in reports, which you can use immediately to access commonly requested data or customize the reports to fit your special needs. In addition to the built-in reports, you can create custom reports for tracking the performance of your NetBackup environment. Custom reports can be created using the custom report wizard.

When you create custom reports, NOM provides several database views that you can use as a starting point for your report. The advanced options in the wizard allow you to group data by certain entities like client, policy, and so on. You can tailor these reports by specifying runtime parameters, and you can email, print, or copy these reports. The customization of the reports is within the parameters of the existing reports and database views.

- *NetBackup troubleshooting assistance*

Troubleshooting remains one of the most time consuming responsibilities for NetBackup administrators. NOM reduces the time that is needed to resolve NetBackup issues by providing capabilities to troubleshoot NetBackup.

NOM provides visual indicators to monitor the health of your servers and NOM alert notifications. NOM also provides in-context links to NetBackup job status codes.

NOM provides log views within the context of a job, and advanced data filters and sort methods. NOM also lets you export and filter multiple job or service logs.

- *Advanced data filtering options to view only data (policies, clients, media, jobs, etc.) of interest*

In environments where multiple NetBackup master and media servers protect a high volume of data, NOM allows filter options and server, policy, or client groupings. These options and groupings let you display and report on only the type of information from the components that you want. NOM consolidates and displays the data views needed to make important decisions.

Custom or easy-to-use filters allow only the information that satisfies the defined condition to be presented. For instance, you can apply a filter to display only the jobs for a specific NetBackup client or policy.

The grouping of related master servers can be used to manage sets of NetBackup servers. Master server groups can be used in the monitoring of NetBackup environments, as well as reporting and active management functions throughout NOM.

- *Intuitive and easy-to-use*

Icons and the use of color provide visual keys to the health of your systems and enable you to isolate possible NetBackup system issues quickly.

- *NetBackup job monitoring and management*

With consolidated job and job policy views per server, policy, or client grouping, you can filter and sort job activity.

Available tasks in NOM allow you to activate or deactivate job policies, or start a job using an existing NetBackup policy. You can also pause, restart, or cancel a job. NOM also provides help for all NetBackup job status codes. NOM also lets you view policy change history to track all policy updates over time, including a side-by-side comparison of one version to the next.

- *NetBackup log file management*

NOM improves and consolidates NetBackup log management features. NOM features allow a user to list, export, and filter logs to help debug issues, all from a single location.

Available log views and tasks allow you to trace the progress of a single job as it runs on NetBackup master and media servers. You can view all applicable debug and error logs, export log files, configure log settings, search for a specific log message, or filter logs using regular expression conditions.

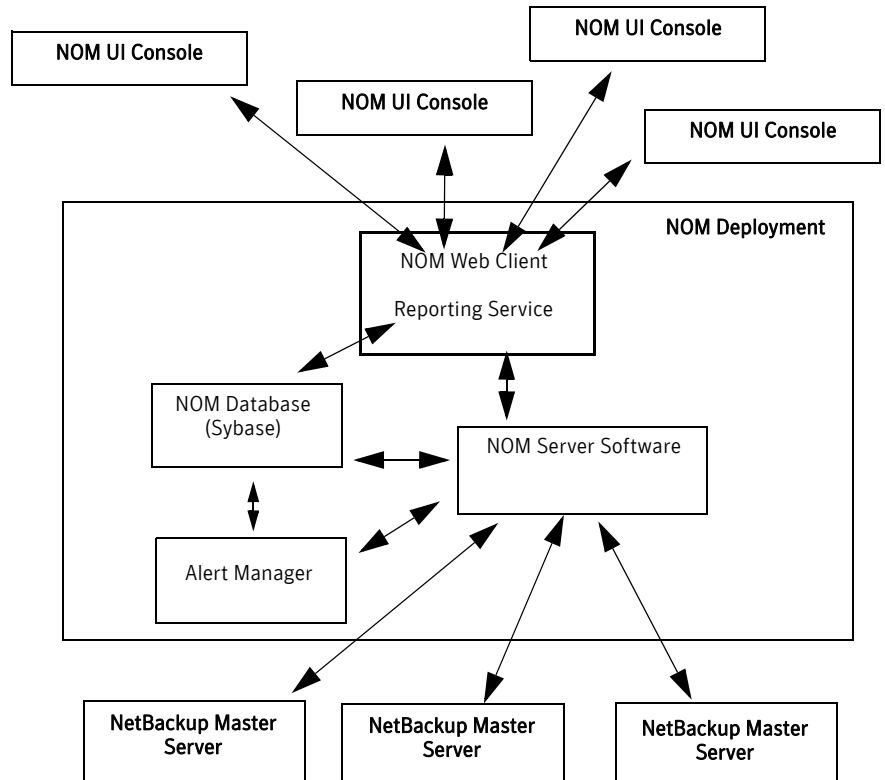
Other tasks allow you to enable or disable selected logs. You can also set retention levels and the verbose levels for most NetBackup log files.

- *NetBackup device, media, and storage unit monitoring and management*
Consolidated NOM views provide an overview of the health of the robots, drives, media, and storage units in your NetBackup environment. For example, associated drive tasks allow you to control drives and also the paths to drives.
- *NetBackup service monitoring and management*
You can use consolidated status views in NOM for all NetBackup services on all master servers to troubleshoot or prevent issues with your jobs. Associated tasks let you control (stop, start, and restart) most services.
- *NOM security*
NOM uses the Symantec Product Authentication Service for user logon authentication and for NOM operations. It is also used for secure communication with NetBackup if the NetBackup server has NBAC (NetBackup Access Control) enabled.
To log into the NOM console, users must have access rights (provided by the NOM administrator).

NetBackup Operations Manager components

NetBackup Operations Manager is comprised of associated components which collect job, configuration, and performance data from NetBackup master and media servers and clients.

The following diagram shows the typical flow of data from multiple NetBackup master servers to the NOM server. NOM formats the data and displays it on one or more Web-based NOM UI consoles.



The NOM console provides a single user interface to the NOM server. All requests from the console are sent to the NOM Web client.

The NOM server software is the centralized focal point that monitors and manages the NetBackup servers in your environment. The NOM server software gathers data and information from NetBackup master servers and stores it in the NOM database. The NOM server software also handles any user-requested monitoring and maintenance tasks for the NetBackup master servers.

See the following topics for more information about key NOM components:

Topic	Description
“The NOM console” on page 18	Provides an overview about the Web-based user interface.

Topic	Description
“NOM deployment” on page 18	Provides an overview about the main NOM components.
“Managed NetBackup master servers” on page 20	Provides an overview about how NOM obtains information about NetBackup jobs and resources, and so on from the master servers.

The NOM console

The NOM console is a Web-based user interface that displays data and handles the associated management tasks for your backup master servers. You can use many standard Web browsers to display the NOM console.

The console connects to and communicates with the NOM Web client (see [“NOM Web client”](#) on page 19). The console is a central point from where you can monitor and manage NetBackup resources. In addition, you can create and modify alert policies, administer user access control, and view reports by using the NOM console.

The console displays multi-level (summary, detail, and object) monitoring and managing views of key NetBackup resources and objects. From the console, you can monitor the status of NetBackup servers, and manage jobs, resources, and troubleshoot log files. The NOM console also contains tools for creating groups of servers, policies, or clients. These tools help you to manage large numbers of master servers easily and simplify the displayed data .

The NOM console also provides quick access to online help for all console views, task dialogs, and wizard task screens.

NOM deployment

The server where NetBackup Operations Manager software is installed is known as the NOM server. You should install NOM software on a dedicated server. The NOM server requires that the NetBackup Service Layer (NBSL) is present and in operation on all managed NetBackup master servers.

For information, recommendations, and requirements for the server where you install NOM, see [“Choosing a server where NOM is installed”](#) on page 25.

The NOM server provides the core functional logic, including the following:

- User access control
- User preferences and NOM server system preferences
- Master server, policy, or client grouping functions
- Monitoring and managing functions

- Reporting functions
- NOM database management tools

NOM deployment comprises of the following main components. All of these are installed as part of the NOM software installation.

NOM Web client

The NOM Web client services HTTP and HTTPS requests and handles user logon requests. It communicates with the NOM server software that monitors and manages NetBackup objects and generates HTML pages for display in the console.

The NOM Web client has a component known as Reporting service. The Reporting service creates and manages reports. These reports consist of the data that the NOM server software collects and are formatted as standard reports or as defined by users. You can customize most reports by selecting groups of NetBackup servers, jobs, or policies to report on. You can also email, export, print, copy, or import these reports.

NOM server software

The NOM server software communicates with NetBackup master servers and the NOM Web client to satisfy requests for NetBackup backup data.

For example, the NOM server software interfaces with the NetBackup media and device components to monitor media and devices and display the information in the NOM console.

See “[Managed NetBackup master servers](#)” on page 20.

Alert manager

A NOM alert policy associates particular sets of conditions with NetBackup resources or object limits. If any of those conditions are met, an alert is raised in the console.

The alert manager communicates with the NOM server software and the NOM database to handle alerts. This component manages alert policies to let users define policies, view active policies, modify policies, and respond to any actual alerts.

NOM database

The NOM server software, alert manager, and reporting system components use a Sybase database management system (DBMS and DB).

See “[NOM server software](#)” on page 19.

This database stores and retrieve all data that is related to NetBackup managed servers, NOM alerts, and NOM reports.

This database is not shared with NetBackup. The database contains the VxAM and NOM database schemas, and database views that NOM reports use.

NOM provides utility to purge data and to manage passwords. Some utilities allow you to view and manage the database.

Managed NetBackup master servers

The NetBackup data collection and management logic that NOM uses is built into NetBackup master servers. This logic is included in the NetBackup Service Layer (NBSL). NBSL is automatically included with NetBackup release 6.0 and greater.

NBSL provides a single point of access to key NetBackup data, objects, and change events. The NetBackup UI also uses NBSL. NBSL runs as a service or daemon and has local configuration information, but no local database.

Each NetBackup master server that NOM manages must have NBSL present and in operation. NBSL is also included on media servers, but NOM does not use it.

NetBackup master servers with NBSL that NOM manages are referred to as managed NetBackup servers. These managed NetBackup servers harvest pertinent NetBackup data and store it in the NOM database.

See [“NOM database”](#) on page 19.

When the NOM server first connects to a NetBackup master server, it collects any changes that occurred since it last connected with the server. After it collects changes, the master server pushes NetBackup event changes to the NOM server.

Where to go in this guide for specific NetBackup Operations Manager information

- For information about the required software components that NOM uses and must be installed, see [“Installing NetBackup Operations Manager”](#) on page 23 and [“Shared and unshared software components that NOM uses”](#) on page 24.
- For more detailed information about the NOM database, security, log files, and services and processes, see [“Administering NetBackup Operations Manager”](#) on page 63.
- For information about using the NOM console and available console features, refer to [“Getting started using the NOM console”](#) on page 109.

Where to go in this guide for specific NetBackup Operations Manager information

- For detailed information and instructions on using NOM to monitor and manage your NetBackup server environment, use the NOM online help that is available in the console.
See [“Using help to understand NOM views and tasks”](#) on page 130.
- For a list of typical NOM management tasks, refer to [“A quick start for performing common tasks in NOM”](#) on page 131.
- For an overview of NOM alert policies and alerts, see [“Understanding NOM alert policies and alerts”](#) on page 143.
- For information about using NOM to troubleshoot your NetBackup environment, see [“Troubleshooting NetBackup issues using NOM”](#) on page 157.
- For information about NOM management groups, NBSL monitors, and configuration of user preferences and system settings, see [“NOM monitoring, managing, and configuration topics”](#) on page 165.
- For information on using the NOM report builder and report scheduler wizards, see [“NOM reporting topics”](#) on page 179.
- For information about using NOM online help (including Quick-Help Links and the Search function), refer to [“Understanding NOM online help”](#) on page 231.

Where to go in this guide for specific NetBackup Operations Manager information

Installing NetBackup Operations Manager

This chapter covers the planning and implementation of your installation of NetBackup Operations Manager software.

The process includes choosing the server where you will install NOM software, installing NOM, and other required components. Also included are topic references to get you started using NOM and tune NOM server performance.

This chapter contains the following installation topics:

Topic	Description
“Planning a NetBackup Operations Manager installation” on page 24	Describes how to plan your NOM installation. Included are NOM sever, NetBackup master server, and Web browser considerations.
“Installation of NOM and required components on a Windows server” on page 34	Describes how to install NOM software and shared Symantec components on a Windows server.
“Installation of NOM and required components on a Solaris server” on page 47	Describes how to install NOM software and shared Symantec components on a Solaris SPARC server.
“After NetBackup Operations Manager is installed” on page 58	Provides a list of the start-up tasks that NOM performs, document references to get you started using the NOM console, and NOM performance tuning.

Planning a NetBackup Operations Manager installation

Review the following sections before you decide on a server where you install NetBackup Operations Manager.

Shared and unshared software components that NOM uses

NOM uses some common Symantec components that are shared and also uses some components that are not shared.

Components shared with other Symantec applications

NOM uses the following shared Symantec components:

- **Symantec Private Branch Exchange (VxPBX)**
VxPBX lets Symantec applications share a common TCP/IP port, which reduces the number of ports in the firewalls that must be open to operate products. VxPBX also integrates with the Symantec Product Authentication Service to allow for authenticated connections in addition to nonauthenticated connections.
See the pdf files in the `docs` directory of the ICS CD/DVD (“[Infrastructure Core Services \(ICS\) CD](#)” on page 31 and “[NetBackup and ICS DVD](#)” on page 32) for information about VxPBX.

Note: Since it is an independent component, the VxPBX port number can be changed using VxPBX configuration files. Changing the VxPBX port number on the server where NOM is installed may cause NOM to fail.

- **Symantec Product Authentication Service**
This service is primarily used for user login authentication and is required for secure communication between NOM client and NOM server software. It is also used for secure communication with NetBackup if the NetBackup server has NBAC (NetBackup Access Control) enabled. See “[Configuring security for managed servers](#)” on page 87 for information about using Symantec Product Authentication Service with NOM and your managed NetBackup master servers.
Symantec Product Authentication Service must be installed on the NOM server. The authentication service can be installed as a client + server or only as a client.
When installing the authentication service as a client + server, it must be installed in Root + Authentication Broker (Root + AB) mode on the server where NOM is installed.

When installing the authentication service as a client, you must install the client APIs locally on the NOM server and the server component can be installed on a remote computer in the network.

Note: There is no requirement for Symantec Product Authorization Service to be installed. Also, there is no requirement for NBAC to be configured on your managed NetBackup master servers.

See the pdf files in the `docs` directory of the ICS CD/DVD (“[Infrastructure Core Services \(ICS\) CD](#)” on page 31 and “[NetBackup and ICS DVD](#)” on page 32) for information about Symantec Product Authentication Service.

- VERITAS Web Server (VRTSweb)
The NOM Web client and the reporting service run under VRTSweb. See the *Veritas Cluster Server Administrator’s Guide for Windows* or the *Veritas Cluster Server User’s Guide for Solaris* for more information about VRTSweb.
- VRTSjre (Java Run Time Environment)
The VRTSweb and the NOM application require this component.
- Veritas Unified Logging (VxUL)
This logging component is installed with the NetBackup 6.0 (or later) client and is used to configure and view NetBackup and NOM logs. See the *NetBackup Troubleshooting Guide* for more information about VxUL logs.

Components not shared with other Symantec applications

The following components are used only by NetBackup Operations Manager:

- NOM Sybase database (NOM uses a Sybase database installation that is separate from the NetBackup database).
See <http://www.sybase.com/support/manuals> for more information about this component.
- Alert manager (VRTSamnom).

Choosing a server where NOM is installed

Consider the following recommendations and requirements when you choose a server system to install NOM software.

Caution: Always refer to the NetBackup Operations Manager sections of the NetBackup release notes for any last-minute changes to the information presented in this document. The release notes for your release of NOM also include any restrictions or limits for NOM.

- Installation of NOM software on the same server as NetBackup server software is *not* recommended. This can lead to performance issues.
- NetBackup 6.0 (or later) client must be installed on the NOM server. NOM uses the NetBackup client software to configure and view VxUL logs written by NOM and NetBackup. You also can use the client software when you back up and restore NOM.
See “[Back up and restore of NOM](#)” on page 77 and “[VxUL log files](#)” on page 102.

Platforms supported for NOM

NetBackup Operations Manager software can be installed on the following operating system platforms.

Operating System	Supported Versions	Notes
Windows 2000	2000 SP4	No 64-bit support
Windows Server 2003	2003 SP1	No 64-bit support
Solaris	8	Sun SPARC No 64-bit support
Solaris	9	Sun SPARC No 64-bit support
Solaris	10	Sun SPARC No 64-bit support

NOM server guidelines and sizing

Please refer to the *NetBackup 6.0 Backup Planning and Performance Tuning Guide* for specific sizing guidelines for the NOM server. This guide is available on the Symantec support Web site.

Web browser considerations

Consider the following recommendations and requirements for the Web browser to use to access the NOM console.

Caution: Always refer to the NetBackup Operations Manager sections of the NetBackup release notes for any last-minute changes to the information presented in this document.

The release notes for your release of NOM also include any restrictions or limits for NOM.

- The NOM console uses pop-up menus in some cases. If you are using pop-up blockers with your Web browser some of these menus may not display properly. You should disable pop-up blocking or add the NOM Web address to the list of acceptable sites in your browser.
- The Web browser should have active scripting (ActiveX and JavaScript) enabled.

Web browsers supported by NOM

The NetBackup Operations Manager user interface (the NOM console) is supported with the following Web browsers. Other Web browsers like Mozilla Firefox may work, but have not been tested.

Web Browser	Supported Versions	Notes
Microsoft Internet Explorer	6.0	
Netscape	7.1 or greater	
Mozilla Firefox	1.0 or greater	Microsoft Windows only.

Email client considerations

NetBackup Operations Manager email uses SMTP protocol for sending email (JavaEmail API). It conforms to specification RFC 822 (Standard for the Format of ARPA Internet Text Messages) and RFC 2045 (Multipurpose Internet Mail Extensions). All email clients conforming to these standards should work with NOM.

Some of the HTML email viewers, like Yahoo, strip off the HTML header and attach their own header when displaying emails. This corrupts the NOM emailed reports.

NOM has been tested with the following email clients:

Email Client	Client Level
Lotus Notes	7

Email Client	Client Level
Microsoft Outlook	2000 and 2003
Mozilla Thunderbird	1.5

Note: SMTP server password authentication is not supported by NOM.

Global Data Manager and NetBackup Advanced Reporter considerations

NOM is based on new architecture and is not an incremental update to any existing Symantec products. You cannot upgrade current GDM and NBAR installations to NOM installations.

NBAR is not supported with NetBackup 6.0 and later releases. NBAR can no longer be used for reporting after the master server is upgraded to NetBackup 6.0 (or later). Only NOM may be used for reporting after upgrading the server.

You cannot install GDM or NBAR on a server where NetBackup 6.0 (or later) software is installed.

Due to differences in architecture, design, implementation, and the data model, the data from NBAR installations is not applicable and cannot be migrated to NOM. Before you use NetBackup 6.0 (or later) and NOM, you may want to run NBAR or GDM in parallel on earlier NetBackup systems during the transition period.

If you upgrade NetBackup software from a previous version to NetBackup 6.0 (or later), first uninstall GDM or NBAR if they are installed on the server.

The NBAR database should be preserved if NOM software is to be installed on that server.

Managed NetBackup master server considerations

Consider the following recommendations and requirements for your managed NetBackup master servers.

Caution: Always refer to the NetBackup Operations Manager sections of the NetBackup release notes for any last-minute changes to the information presented in this document.

The release notes for your release of NOM also include any restrictions or limits for NOM.

- NOM does not collect data from the managed servers that are configured within a Network Address Translation (NAT) network.
- Symantec recommends that any NetBackup master server be monitored by only one NOM server.
- Installation of NOM software on the same server as NetBackup master or media server software is *not* recommended.

See “[Configuring server groups or servers \(using the context pane\)](#)” on page 133 for information on adding managed NetBackup servers in NOM.

Platforms supported for NetBackup servers

NetBackup Operations Manager software supports management and monitoring of NetBackup master servers on the following operating systems:

Note: Refer to NetBackup version compatibility matrix for the latest information on supported platforms. This document is available on the Symantec support Web site.

Table 2-1 Supported Platforms for NetBackup servers

Operating System	Supported Versions	Vendor/Platform
Windows 2000	2000 SP4	Intel IA-32 32-bit Windows 2000 on AMD64 and EM64T hardware
Windows Server 2003	Server 2003, Server 2003 SP1, SP2 Standard Enterprise, Datacenter, and Web editions. Server 2003 R2 Standard, Enterprise, and Datacenter	Intel IA-32
Windows Server 2003	Server 2003, Server 2003 SP1, SP2 Standard Enterprise, Datacenter, and Web editions. Server 2003 R2 Standard, Enterprise, and Datacenter	Supported with 32-bit Netbackup binaries. 32-bit Windows server 2003 on AMD64 and EM64T platforms.

Table 2-1 Supported Platforms for NetBackup servers

Operating System	Supported Versions	Vendor/Platform
Solaris	8	Sun SPARC Fujitsu PRIMEPOWER
Solaris	9	Sun SPARC Fujitsu PRIMEPOWER
Solaris	10	Sun SPARC Fujitsu PRIMEPOWER
HP-UX	11.0 (32/64 bit)	HP 9000
HP-UX	11i v1 (11.11) (32/64 bit)	HP 9000
HP-UX	11i v2 (11.23) (32/64 bit)	HP 9000
HP-UX	11i v2 (11.23)	HP Integrity (IA-64)
AIX	5.1 (32/64 bit)	IBM Power 3, Power 4, Power 5
AIX	5.2 (32/64 bit)	IBM Power 3, Power 4, Power 5
AIX	5.3 (32/64 bit)	IBM Power 3, Power 4, Power 5
Redhat Enterprise Linux	2.1 Intel x86	Intel IA-32
Redhat Enterprise Linux	3.0 Intel x86	Intel IA-32
Redhat Enterprise Linux	4.0 Intel x86	Intel IA-32
SuSE Linux Desktop	9.0	Intel IA-32

NOM can be used to monitor a NetBackup cluster. NOM supports NetBackup clusters on the platforms listed in [Table 2-1](#) on page 29.

See *NetBackup Installation Guide* for more details on setting up a NetBackup cluster environment. Also review the NetBackup Operations Manager sections of the NetBackup release notes before using NOM for monitoring NetBackup clusters.

NBSL and NetBackup Event Manager

Starting with the 6.0 release of NetBackup, NetBackup Service Layer (NBSL) components are included as a part of NetBackup on master and media servers.

NBSL and NBEvtMgr (NetBackup Event Manager) are required and are used by NOM for all NetBackup monitoring, managing, and control functions. There is an impact if either service stops running on a managed NetBackup server.

If NBEvtMgr stops, any management changes are lost. If NBSL stops, NOM may not capture any changes that were made to the NetBackup configuration. When NBSL restarts, NOM correctly recaptures the latest state.

See “[Understanding NBSL monitors and the Partially Online server status](#)” on page 170.

See the *NetBackup Administrator’s Guide, Volume II* for more information about NBSL.

NetBackup Enterprise Server media kit (CDs)

The NetBackup Enterprise Server media kit includes the following software CDs (along with other CDs). Use these CDs to install NetBackup Operations Manager and required components.

Note that the media kit organizes the CDs by operating system platform. See the *NetBackup Installation Guide* for more details about the contents of this media kit.

NetBackup CDs

You must install NetBackup client software on the NOM server. NOM uses the client software to configure and view VxUL logs. You can also use the client when you back up and restore the NOM database.

See “[Installing NetBackup client software on the NOM server](#)” on page 36 for Windows and “[Installing NetBackup client software on the NOM server](#)” on page 49 for Solaris.

Infrastructure Core Services (ICS) CD

NOM requires NetBackup compatible versions of the following software components. These components can be installed on Windows or Solaris SPARC NOM servers.

- Symantec Private Branch Exchange
This component is available only with ICS CDs for Solaris SPARC platform and must be installed only for Solaris SPARC installations.
This component does not need to be separately installed on Windows servers as it gets installed with NetBackup client 6.5 for Windows.
- Symantec Product Authentication Service
This component must be installed for both Windows and Solaris SPARC installations.

The `docs` directory on the CD contains pdf files for the installation and administration of these ICS components.

Before you install NOM on a server, you must first install and configure these components on the server.

See [“Installing Symantec Product Authentication Service on the NOM server”](#) on page 36 for Windows installations and [“Installing Symantec Private Branch Exchange and Symantec Product Authentication Service software on the NOM server”](#) on page 49 for Solaris installations.

NetBackup Operations Manager CD

The NOM CD is included in the NetBackup Enterprise Server media kit at no additional charge. No license keys are required to use NOM. With an enterprise license you can use NOM to monitor and manage other installations including NetBackup server.

The CD includes the following software components that are associated with NOM. These components are installed at the completion of NOM installation on Windows or Solaris SPARC servers.

- NetBackup Operations Manager Server software
- NetBackup Operations Manager Alert Manager (VxAM)
- NetBackup Operations Manager Database Server
- NetBackup Operations Manager Web Console
- VERITAS Web Server (VRTSweb)
- Symantec Private Branch Exchange (VxPBX)
- Java Run Time Environment (VRTSjre)

NetBackup Enterprise Server media kit (DVDs)

The NetBackup Enterprise Server media kit includes the following software DVDs for installing NetBackup Operations Manager. Use these DVDs to install NetBackup Operations Manager and its required components.

Note that the media kit organizes the DVDs by operating system platform. See the *NetBackup Installation Guide* for more details about the contents of this media kit.

NetBackup and ICS DVD

Before you install NOM on a server, you must first install NetBackup client software on the NOM server.

After installing NetBackup client, you must install and configure the ICS components on the NOM server. These components are included on the DVD and can be installed on Windows or Solaris SPARC NOM servers.

- Symantec Private Branch Exchange
This component is available only with ICS DVDs for Solaris SPARC platform and must be installed only for Solaris SPARC installations.
This component does not need to be separately installed on Windows servers as it gets installed with NetBackup client 6.5 for Windows.
- Symantec Product Authentication Service
This component must be installed for both Windows and Solaris SPARC installations. The `docs` directory on the DVD contains pdf files for the installation and administration of these ICS components.

See [“Installing Symantec Product Authentication Service on the NOM server”](#) on page 36 for Windows installations and [“Installing Symantec Private Branch Exchange and Symantec Product Authentication Service software on the NOM server”](#) on page 49 for Solaris installations.

NetBackup Operations Manager DVD

The NOM DVD is included in the NetBackup Enterprise Server media kit at no additional charge. No license keys are required to use NOM. With an enterprise license you can use NOM to monitor and manage other installations including NetBackup server.

The DVD includes the following software components that are associated with NOM. These components are installed at the completion of NOM installation on Windows or Solaris SPARC servers.

- NetBackup Operations Manager Server software
- NetBackup Operations Manager Alert Manager (VxAM)
- NetBackup Operations Manager Database Server
- NetBackup Operations Manager Web Console
- VERITAS Web Server (VRTSweb)
- Symantec Private Branch Exchange (VxPBX)
- Java Run Time Environment (VRTSjre)

Installation of NOM and required components on a Windows server

Use the following installation steps.

Table 2-2 Installation Sequence on a Windows server

Step	Description	See this Topic
1	Perform preinstallation checks	“Before starting the installation” on page 34
2	Install the NetBackup client	“Installing NetBackup client software on the NOM server” on page 36
3	Install ICS software components	“Installing Symantec Product Authentication Service on the NOM server” on page 36
4	Install NetBackup Operations Manager software	“Installing NOM software” on page 41
5	Handling an out-of-sequence installation	“Installing the Symantec Product Authentication Service before the NetBackup client” on page 44
6	Describes the installer behavior on upgrading from NOM 6.0 or 6.0 MPx to NOM 6.5.	“Installation behavior on upgrading to NOM 6.5” on page 47

Before starting the installation

Review the topics in [“Choosing a server where NOM is installed”](#) on page 25 before starting the installation.

Also review the following topics that may cause installation problems or issues when starting the NOM server.

Considerations for the NOM server

- The NOM server should be configured as a fixed host with a static IP address.
- NOM is not tested on servers hardened for security. If you install NOM on a hardened server you should open any necessary ports. See [“Communication and firewall considerations”](#) on page 93 for port information.
- NOM will not install if the following registry key has two backslashes. This can occur if NOM has been uninstalled.

```
[HKLM\software\VERITAS\Security\Authentication]\InstallDir
```

The entry should look similar to this:

```
INSTALL_PATH\Security\Authentication\
```

and not like this:

```
INSTALL_PATH\Security\Authentication\
```

Note: *INSTALL_PATH* refers to the directory where you have installed NetBackup Operations Manager. By default, the *INSTALL_PATH* for NOM is C:\Program Files\VERITAS.

- NOM will not install and start correctly if a file called `program` resides in the C:\ folder on the NOM server. In this case, an error message similar to the following is displayed and the NOM services do not start.
Error 1920: Service NetBackup Operations Manager Server (VRTSnomSrvr) failed to start
You must delete or rename the file and retry the install.
- NOM installer might hang if you try to install NOM in a folder whose name contains special characters like %, ~, !, @, \$, &, >, # etc. For example, NOM installer might not respond if you are installing NOM in D:\ab%c.

NOM server name length limit

The installation of NOM software requires that the FQDN (fully qualified domain name) of the NOM server should have 44 or fewer characters.

NOM uses a set of domains that start with strings like `NOM_TRUSTED_CLIENTS`, `NOM_Builtin`, and so on. The longest string NOM uses while preparing a domain in the Symantec Product Authentication Service is `NOM_TRUSTED_CLIENTS` which is 19 characters long.

NOM appends the @ character and the FQDN of the server to these strings. For example, `NOM_Builtin@FQDN\FQDN`.

So NOM may add an additional 20 characters to the FQDN of the server to prepare a domain in the authentication service. The server FQDN must be restricted to 44 characters or less.

Note: If the name of the server where NOM is installed is greater than 64 characters, NOM will not start.

Installing NetBackup client software on the NOM server

The NetBackup 6.0 (or later) client must be installed on the server where you plan to install NOM software. You can skip this installation step if any 6.0 (or later) client software is currently installed on the server. See [“Choosing a server where NOM is installed”](#) on page 25.

See the appropriate client sections of the *NetBackup Installation Guide for Windows* for instructions.

Installing Symantec Product Authentication Service on the NOM server

The Symantec Product Authentication Service is an ICS software component used by NOM.

While security authentication is optional for NetBackup master servers, it is required for NOM operation and must be present in your server configuration. The authentication service can be installed on the NOM server or on another server.

NOM uses the authentication service to authenticate NOM users, mutually authenticate NOM client and server communication, and establish secure communication with managed NetBackup master servers.

You need to install the Symantec Product Authentication Service version shipped with the ICS CD/DVD before installing NOM 6.5.

Note: The NOM installer does not check whether the authentication service has been installed or not. You will not be able to log on to NOM 6.5 if the service has not been installed or if the version of the service is not the latest shipped version.

NOM uses client APIs to communicate with the Root Broker of the authentication service. NOM requires additional configuration information to establish this connection. See [“To install NetBackup Operations Manager”](#) on page 42 for details.

NOM can manage NetBackup master servers with or without NBAC configured on master servers. If you configure the NetBackup Access Control (NBAC) feature for NetBackup servers, it also uses Symantec Product Authentication Service components.

Supported Symantec Product Authentication Service installation types

The Symantec Product Authentication Service can be installed as a client + server (**Complete** installation) or only as a client (**Typical** installation).

For NOM 6.5 (or later), NOM supports using a remote authentication service configuration for security.

When installing the service as client + server, you must install it in Root + Authentication Broker (Root + AB) mode on the NOM server.

Note: NOM does *not* support the authentication service running in only ROOT or only AB mode. This restriction applies to both remote (or local) servers.

When installing the service as a client, you install the client component locally on the NOM server and server component on a remote computer in the network. See [“Installing Symantec Product Authentication Service on the NOM server”](#) on page 37 for more information on installing the authentication service.

Installing Symantec Product Authentication Service on the NOM server

At a minimum, NOM requires that you always install the client APIs for the authentication service on the NOM server. These APIs are used to connect to the Server component.

Note: You must install the latest shipped version of the Symantec Product Authentication Service with NOM 6.5. NOM 6.5 does not support any other version of the authentication service.

The following two sets of instructions describe the common authentication service installation cases:

- [“Case 1: Installing the authentication service as client + server”](#) on page 37
- [“Case 2: Installing the authentication service as a client”](#) on page 40

Case 1: Installing the authentication service as client + server

In this case, the complete Symantec Product Authentication Service is installed on the NOM server.

To install the authentication service server and the client APIs on the NOM server

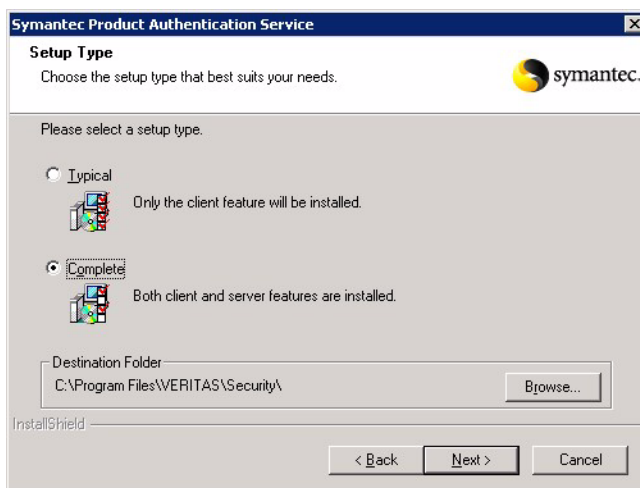
- 1 Insert the ICS CD/DVD.

Note: Use the Authentication/VxSSVRTSatSetup.exe file and not one of the msi (silent installation) files.

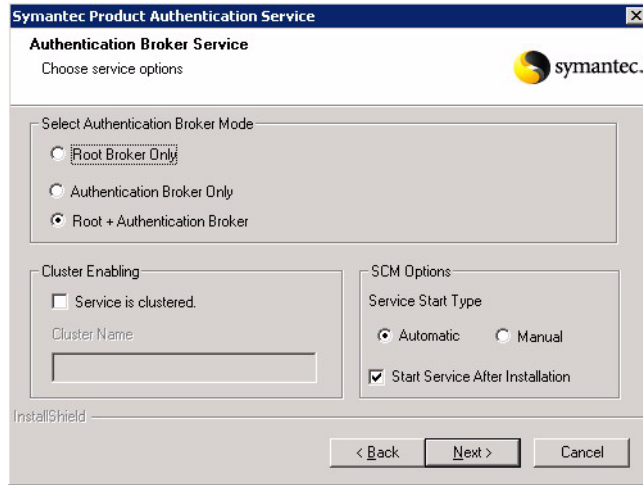
- 2 Run the InstallShield wizard.

Note: There is no requirement for the Symantec Product Authorization Service to be installed.

- 3 Accept the default installation settings.
From the **Setup Type** screen, select **Complete** to install the server component and the client APIs on the NOM server.

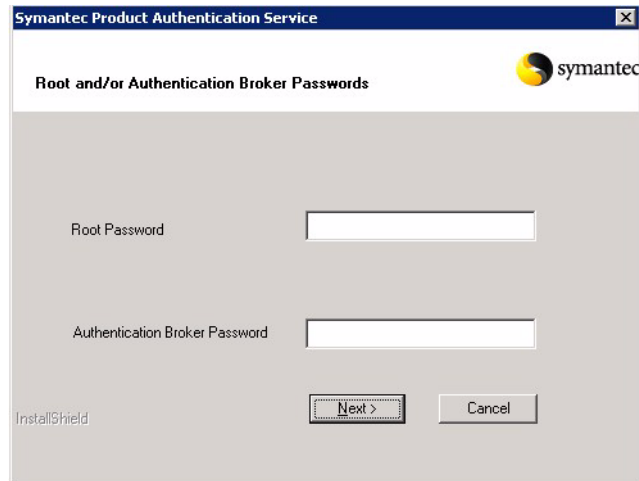


- 4 From the **Authentication Broker Service Options** screen, select **Root + Authentication Broker**.



Accept the default options for this screen.

- 5 In the **Symantec Product Authentication Service** screen, you can choose to specify the Root Password and Authentication Broker Password or leave the fields blank. If you choose to leave the fields blank, the authentication service is installed with the default password (Vxadmin). Accept the warning messages for keeping the default password. In case you enter a custom password, you must also enter the same in the **Authentication Service Password** field of the **Security Options** screen during NOM installation. See [step 3](#) on page 42 for the **Security Options** screen.



Accept the remaining installation options. A root and AB broker are configured on the NOM server.

- 6 You can have managed servers *using* the authentication service and NBAC and servers *not using* the service and NBAC in your NetBackup server environment.
Make sure you configure the servers that are *not using* the authentication service and NBAC to allow server access and data collection by NOM. You must add the name of the NOM server to the trusted SERVER list on each of these servers. From the NetBackup administration console of each managed server, use the **Host Properties** node of **NetBackup Management** to add the name of the NOM server.
See [“Managed NetBackup servers with and without NBAC configured and authentication service locally installed on the NOM server”](#) on page 89 for an example of this security model.

Case 2: Installing the authentication service as a client

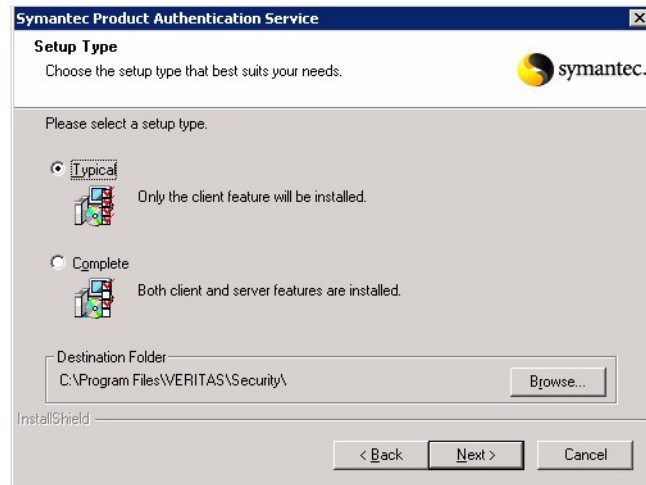
In this case, you install the client locally on the NOM server and the server component is installed on a remote computer. NOM uses the client APIs to communicate with and use the authentication service (Root + AB broker) installed on the managed NetBackup servers.

To install the authentication service client APIs on the NOM server

- 1 Insert the ICS CD/DVD.

Note: Use the `Authentication/VxSSVRTSatSetup.exe` file and not one of the msi (silent installation) files.

- 2 Run the InstallShield wizard.
- 3 From the **Setup Type** screen, select **Typical** to install only the client APIs on the NOM server.



Note: When you perform the NOM installation (“[Installing NOM software](#)” on page 41), you also need to supply the details of the remote server component in the security options screen. This information is required to complete the authentication service installation. See [step 3](#) on page 42 for the security options screen.

- 4 You can have managed servers *using* the authentication service and NBAC and servers *not using* the service and NBAC in your NetBackup server environment.
 Make sure you configure the servers that are *not using* the authentication service and NBAC to allow server access and data collection by NOM. You must add the name of the NOM server to the trusted SERVER list on each of these servers. From the NetBackup administration console of the managed server, use the **Host Properties** node of **NetBackup Management** to add the name of the NOM server.
 See “[Managed NetBackup servers with and without NBAC configured and authentication service on the remote computer](#)” on page 90 for an example of this security model.

Installing NOM software

The NetBackup 6.0 (or later) client must be installed on the server where you plan to install NOM software. You can install the client software from the clients CD/DVD.

To install NetBackup Operations Manager

The default location for the installation is: C:\Program Files\VERITAS\NetBackup Operations Manager.

An option to specify an alternate path for the installation appears during the installation.

Log files are created during the installation to trace any install issues.

See “[NOM log files on Windows servers](#)” on page 103.

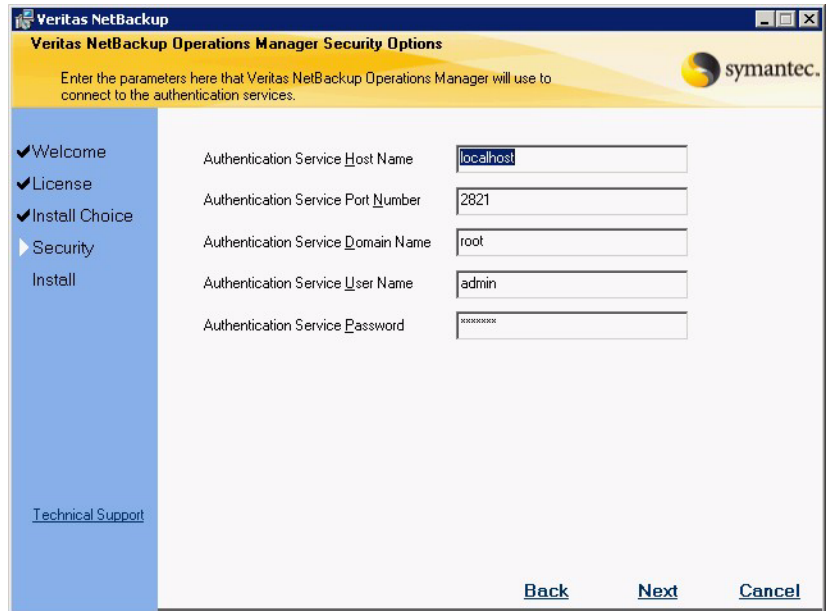
- 1 Insert the NOM CD/DVD.
Navigate to the NB_OM directory in the DVD to run the NOM installation.
- 2 Run setup.exe.
The installation checks for the presence and the minimum version required for the following software components.
 - VRTSjre and VRTSweb. The installation installs or upgrades these components (using merge modules).
 - VxPBX (Symantec Private Branch Exchange). The NetBackup client 6.5 installation installs or upgrades VxPBX if it is not installed or is out-of-date.
VxPBX does not appear in the **Add/Remove Programs** list of the Windows **Control Panel** when it is installed with NetBackup Client.

Note: You do not need to install a separate version of VxPBX for installing NOM 6.5.

Note: The NOM installer does not check whether the Symantec Product Authentication Service has been installed or not. You will not be able to log on to NOM 6.5 if the service has not been installed or if the version is not the latest shipped version.

- 3 Symantec Product Authentication Service can be completely installed on the NOM server or you can install the client APIs locally on the NOM server and the server component on a remote computer.
If you did a **Typical** installation of the service and installed only the client APIs, you need to provide the configuration parameters that are used by

NOM to connect to the server component in the **Veritas Netbackup Operations Manager Security Options** screen.



Note: In case you chose a custom password while installing the authentication service as client+server (Root+AB mode) in [step 5](#) on page 39, you must enter the same password in the **Authentication Service Password** field.

The following table describes the authentication service fields that are listed in the **Security Options** screen.

Table 2-3 Authentication service fields

Field	Value to enter
Authentication Service Host Name	The fully qualified host name (FQHN) of the server on which the authentication service server component is running. The default value is localhost if the authentication service is installed on the NOM server.

Table 2-3 Authentication service fields

Field	Value to enter
Authentication Service Port Number	The port number of the server on which the authentication service server component is running. The default value is 2821.
Authentication Service Domain Name	The domain name of the root. The default value is root.
Authentication Service User Name	The name of the root user used for initial authentication. The default value is admin.
Authentication Service Password	The password of the root user used for initial authentication. The default value is Vxadmin

If you have not specified the details associated with the remote authentication server component during NOM installation, you can add these details using the `NOMAdmin` utility. See [“Configuring Authentication Server Parameters”](#) on page 75 for details.

Note: In case you installed authentication service as client + server (**Complete** installation) with the default values on the NOM server, you do not need to modify the default values listed on the screen or use the `NOMAdmin` utility.

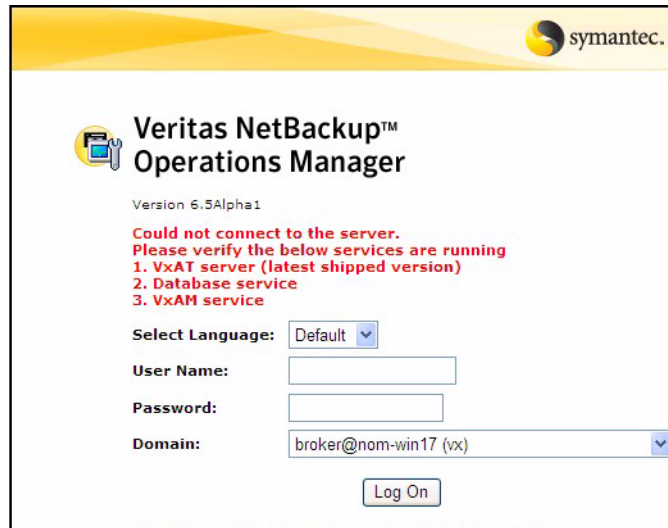
- 4 A menu item for **Veritas NetBackup > NetBackup Operations Manager** is added to the Windows Start menu at the completion of the installation.

Installing the Symantec Product Authentication Service before the NetBackup client

You should follow the installation sequence mentioned in [Table 2-2](#) on page 34 to install NOM. The NetBackup client installation installs or upgrades Symantec Private Branch Exchange if it is not installed or is out-of-date. This installation sequence also connects the authentication service and private branch exchange components.

If you installed the authentication service before installing NetBackup client software, you are likely to see the following issues.

- You are unable to log on to NOM server and get the error message as depicted in the following figure:



- The NOM_Builtin@hostname domain may not be present in the list of domains.

NOM requires that you need to connect the authentication service and VxPBX components. This can be done by verifying whether `pbxexchflag` of the authentication service is set or not. When `pbxexchflag` is set, its value is equal to 1. Before setting the value of `pbxexchflag`, you must stop all NOM services, Symantec Product Authentication Service and Symantec Private Branch Exchange. After setting the value of `pbxexchflag` to 1, you must restart these services.

To connect Symantec Product Authentication Service and Symantec Private Branch Exchange

- 1 Open the command prompt and navigate to `INSTALL_PATH\Security\Authentication\bin` directory. Enter the following command:

```
vssat.exe showispbxexchflag
```

This command gives the value of `pbxexchflag`. If the value of `pbxexchflag` is 0, you need to set it to 1.

Note: In case the value of `pbxexchflag` is 1, you do not need to follow the remaining steps. You should be able to log on to NOM.

- 2 Navigate to `INSTALL_PATH\NetBackup Operations Manager\bin\admincmd` directory. Stop all the NOM services by executing the following command:

```
NOMAdmin.bat -stop_service
```
- 3 Stop Symantec Product Authentication Service by performing either of the following steps:
 - Use the stop option in the Windows Service pane, or
 - Execute the following command in a command console:

```
net stop vrtsat
```
- 4 Stop Symantec Private Branch Exchange by performing either of the following steps:
 - Use the stop option in the Windows Service pane, or
 - Execute the following command in a command console:

```
net stop vrtspbx
```
- 5 Navigate to `INSTALL_PATH\Security\Authentication\bin` directory. Enter the following command at the bin directory to set the value of `pbxexchflag`:

```
vssat.exe setispbxexchflag --enable
```

The value of `pbxexchflag` is set to 1. Follow [step 1](#) of this procedure to verify if the value of `pbxexchflag` is 1.
- 6 Restart Symantec Private Branch Exchange by performing either of the following steps:
 - Use the start option in the Windows Service pane, or
 - Execute the following command in a command console:

```
net start vrtspbx
```
- 7 Restart Symantec Product Authentication Service by performing either of the following steps:
 - Use the start option in the Windows Service pane, or
 - Execute the following command in a command console:

```
net start vrtsat
```
- 8 Restart all the NOM services by performing the following steps:
 - Navigate to `INSTALL_PATH\NetBackup Operations Manager\bin\admincmd` directory.
 - Restart all the NOM services by executing the following command:

```
NOMAdmin.bat -start_service
```
- 9 You should now be able to log on to NOM.

Installation behavior on upgrading to NOM 6.5

You will find the following things when you upgrade from NOM 6.0 or 6.0 MPx to NOM 6.5:

- The data in the NOM database is retained when you upgrade to NOM 6.5. Only schema changes are applied on the NOM database during the upgrade process.
- If your database port number is not 13729, then the installer retains the same database port number during an upgrade to NOM 6.5. If your database port number is 13729, then 13786 is set as the default database port number for NOM 6.5.
- The Database administrator password for NOM 6.0 or NOM 6.0 MPx remains the same when you upgrade to NOM 6.5.
- The symbolic link is retained in an upgrade to NOM 6.5. For example, you might have created a symbolic link to data present in `INSTALL_PATH\NetBackup Operations Manager\db` directory. This link is retained in an upgrade to NOM 6.5.

Note: Some standard reports have been deprecated and replaced with new standard reports in NOM 6.5. To migrate to the new 6.5 reports, see [“Upgrading reports from 6.0 or 6.0MPx to 6.5”](#) on page 226.

Note: The default location for the NOM database can be changed. This location can be changed after NOM has been installed or before upgrading to NOM 6.5 from NOM 6.0 or 6.0MPx. See [“Moving the NOM database to a non-default location”](#) on page 75 for specific instructions.

Installation of NOM and required components on a Solaris server

Note: The term Solaris in the following section refers specifically to Solaris SPARC.

Use the following installation steps.

Table 2-4 Installation Sequence on a Solaris server

Step	Description	See this Topic
1	Perform preinstallation checks	“Before starting the installation” on page 48
2	Install the NetBackup client	“Installing NetBackup client software on the NOM server” on page 49
3	Install ICS software components	“Installing Symantec Private Branch Exchange and Symantec Product Authentication Service software on the NOM server” on page 49
4	Install NetBackup Operations Manager software	“Installing NOM software” on page 53
5	Handling an out-of-sequence installation	“Installing the Symantec Product Authentication Service before Symantec Private Branch Exchange” on page 56
6	Describes the installer behavior on upgrading from NOM 6.0 or 6.0 MPx to NOM 6.5.	“Installation behavior on upgrading to NOM 6.5” on page 57

Before starting the installation

Review the topics in [“Choosing a server where NOM is installed”](#) on page 25 before starting the installation.

Also review the following topics that may cause installation problems or issues when starting NOM.

Considerations for the NOM server

- The NOM server should be configured as a fixed host with a static IP address.
- NOM is not tested on servers hardened for security. If you install NOM on a hardened server you should open any necessary ports. See [“Communication and firewall considerations”](#) on page 93 for port information.

VRTSweb installer issues

NOM installation issues occur if the server has a symbolic link to the /opt directory. The VRTSweb installer unlinks /opt and creates a new /opt directory.

This unlink happens after the VxAM and the NOM client packages have successfully been installed into the `/opt` symbolic link. As a result, NOM database initialization does not happen and the NOM server software does not start.

Using a symbolic link to the `/opt` directory is not recommended.

Installing NetBackup client software on the NOM server

The NetBackup 6.0 (or later) client must be installed on the server where you plan to install NOM software. You can skip this installation step if any 6.0 (or later) client software is currently installed on the server. See [“Choosing a server where NOM is installed”](#) on page 25.

See the appropriate server or client sections of the *NetBackup Installation Guide for UNIX and Linux* for instructions.

Installing Symantec Private Branch Exchange and Symantec Product Authentication Service software on the NOM server

Symantec Private Branch Exchange and Symantec Product Authentication Service software are ICS software components used by NOM.

While security authentication is optional for NetBackup master servers, it is required for NOM operation and must be present in your server configuration. Symantec Product Authentication Service can be installed on the NOM server or on another server.

NOM uses Symantec Product Authentication Service to authenticate NOM users, mutually authenticate NOM client and server communication, and establish secure communication with managed NetBackup master servers.

Note: You must install the Symantec Product Authentication Service version shipped with the ICS CD/DVD before installing NOM 6.5. You will not be able to log on to NOM 6.5 if the service has not been installed or if the version of the service is not the latest shipped version.

NOM uses client APIs to communicate with the authentication service Root Broker. NOM requires additional configuration information to establish this connection. See [“To install NetBackup Operations Manager”](#) on page 53 for details.

NOM can manage NetBackup master servers with or without NBAC configured on master servers. If you configure the NetBackup Access Control (NBAC) feature for NetBackup servers, it also uses Symantec Product Authentication Service components.

Supported Symantec Product Authentication Service installation types

The Symantec Product Authentication Service can be installed as a client + server or only as a client.

For NOM 6.5 (or later), NOM supports using a remote authentication service configuration for security.

When installing the service as client + server, you must install it in Root + Authentication Broker (Root + AB) mode on the NOM server.

Note: NOM does *not* support the authentication service running in only ROOT or only AB mode. This restriction applies to both remote (or local) servers.

When installing the service as a client, you install the client component locally on the NOM server and server component on a remote computer in the network. See “[Installing Symantec Private Branch Exchange and Symantec Product Authentication Service on the NOM server](#)” on page 50 for more information on installing the authentication service.

Installing Symantec Private Branch Exchange and Symantec Product Authentication Service on the NOM server

At a minimum, NOM requires that you always install the client APIs for the authentication service on the NOM server. These APIs are used to connect to the server component.

Note: You must install the latest shipped version of the Symantec Product Authentication Service with NOM 6.5. NOM 6.5 does not support any other version of the authentication service.

The following two sets of instructions describe the common authentication service installation cases:

- “[Case 1: Installing the authentication service as client + server](#)” on page 50
- “[Case 2: Installing the authentication service as a client](#)” on page 52

Case 1: Installing the authentication service as client + server

In this case, the complete Symantec Product Authentication Service is installed on the NOM server.

Note: There is no requirement for Symantec Product Authorization Service to be installed for NOM.

To install Symantec Private Branch Exchange, authentication server and client APIs on the NOM server

- 1 Insert the ICS CD/DVD.
You must run the `installics` script for each software component that you want to install.
- 2 Run the `installics` script.
The script displays the versions of all software components currently installed on the NOM server.
Select **(I)** to install or update a software component.
Select **(1)** to install Symantec Private Branch Exchange.
Accept the default options for the remaining steps of the installation.
When prompted for the system name, enter the name of the NOM server.
- 3 Run the `installics` script.
Select **(I)** to install or update a software component.
Select **(2)** to install Symantec Product Authentication Service.
Select **y** to install the authentication server software.
The client APIs are automatically installed.
Select **(1) Root + AB Mode** to install and configure a root and AB broker for NOM.

Note: NOM *does not* support authentication service running in only ROOT or only AB mode.

When prompted for the system name on which to install the authentication service, enter the name of the NOM server.
Accept the default options for the remaining steps of the installation.

- 4 Configure the authentication server software.

Note: It is optional to configure authentication server. If you choose to do this later, you can do it manually or run the `installat -configure` command from the `/opt/VRTS/install` directory.

Enter a password for the Root Broker administrator for the Root Broker on the NOM server. You can either use Vxadmin (default password) or create a custom password.

Enter a password for the Authentication Broker administrator for the Authentication Broker on the NOM server. You can either use Vxadmin (default password) or create a custom password.

Note: You can change the default password (Vxadmin) and use a custom password for configuring Root Broker and Authentication Broker. In case you are using a custom password, the same must be entered during NOM installation in the Authentication Service Password field. Refer to [step 3](#) on page 54 for more information.

You must enable VxPBX support for the Authentication Broker server. Answer **y** to enable Private Branch Exchange (PBX) support in Authentication Broker server.

Answer **y** to start the Symantec Product Authentication Server process. Enter a password encryption name to continue.

- 5 You can have managed servers *using* the authentication service and NBAC and servers *not using* the service and NBAC in your NetBackup server environment.
Make sure you configure the servers that are *not using* the authentication service and NBAC to allow server access and data collection by NOM. You must add the name of the NOM server to the trusted SERVER list on each of these servers. From the NetBackup administration console of each managed server, use the **Host Properties** node of **NetBackup Management** to add the name of the NOM server.
See “[Managed NetBackup servers with and without NBAC configured and authentication service locally installed on the NOM server](#)” on page 89 for an example of this security model.

Case 2: Installing the authentication service as a client

In this case, you install the client locally on the NOM server and the server component is installed on a remote computer. NOM uses the client APIs to communicate with and use the authentication service (Root + AB broker) installed on the managed NetBackup servers.

To install Symantec Private Branch Exchange and authentication service client APIs on the NOM server

- 1 Insert the ICS CD/DVD.
You must run the `installics` script for each software component that you want to install.
- 2 Run the `installics` script.
The script displays the versions of all software components currently installed on the NOM server.
Select **(I)** to install or update a software component.
Select **(1)** to install Symantec Private Branch Exchange.
- 3 Run the `installics` script.

Select **(1)** to install or update a software component.

Select **(2)** to install Symantec Product Authentication Service.

Answer **n** to installation of the authentication service server software.

When installing the client APIs and prompted for the system name, enter the name of the NOM server.

Accept the default options for the remaining steps of the installation.

- 4 You can have managed servers *using* the authentication service and NBAC and servers *not using* the service and NBAC in your NetBackup server environment.

Make sure you configure the servers that are *not using* the authentication service and NBAC to allow server access and data collection by NOM. You must add the name of the NOM server to the trusted SERVER list on each of these servers. From the NetBackup administration console of the managed server, use the **Host Properties** node of **NetBackup Management** to add the name of the NOM server.

See “[Managed NetBackup servers with and without NBAC configured and authentication service on the remote computer](#)” on page 90 for an example of this security model.

Installing NOM software

The NetBackup 6.0 (or later) client must be installed on the server where you plan to install NOM software. You can install the client software from the clients CD/DVD.

To install NetBackup Operations Manager

Use the installation defaults when you install NOM. The default location for the installation is `/opt`.

NOM creates a log file with the name of `installnom_trace.nnnn` in `/opt/tmp` to trace any install issues. `nnnn` is the process id of this installation.

See “[NOM log files on Solaris servers](#)” on page 105.

- 1 Insert the NOM CD/DVD.
Navigate to the `NB_OM` directory in the DVD to run the NOM installation.
- 2 Run the `install` script.

Note: The install script should not be executed from the CD/DVD location.

You must run the install script from the root (`/`) directory and execute the full pathname to this script. For example, if the install script is located in `/mnt/cdrom` directory, enter the following commands to run the install script:

```
cd /  
/mnt/cdrom/install
```

The install script starts.

Accept the default options.

The script stops if the NetBackup client is not present on the server. In addition, the script checks for the presence of the following software components. The installation of NOM requires a specific minimum version of each.

- Symantec Private Branch Exchange and Symantec Product Authentication Service. The script stops if these ICS components are not installed or are out-of-date.

Note: The installation will proceed if either client APIs or authentication service server component has been installed. The script stops if both client APIs and authentication service server component have not been installed.

Note: You must install the Symantec Product Authentication Service version shipped with the ICS CD/DVD before installing NOM 6.5.

- VxAM, VRTSjre, and VRTSweb. The script installs these components from the NOM CD/DVD if they are not present. It offers to remove and upgrade them if they are out-of-date or partially installed. You can select **no** to this removal and the installation stops, which leaves your system unchanged.
- 3 Symantec Product Authentication Service can be completely installed on the NOM server or you can install only the client APIs on the NOM server and authentication server component on a remote computer.

If only the client APIs have been installed locally on the NOM server, you need to provide the configuration parameters that are used by NOM to connect to the remote authentication service server component.

The installer prompts you to provide the values for the following parameters to configure authentication server parameters. The current values for authentication server parameters are specified in brackets. You must enter the new values next to the respective parameter to configure authentication server.

```
Authentication Service Host Name[<current_parameter  
value>]:  
Authentication Service Port number[<current_parameter  
value>]:  
Authentication Service Domain Name[<current_parameter  
value>]:
```

```
Authentication Service User Name[<current_parameter  
value>]:  
Authentication Service Password[<current_parameter  
value>]:
```

Note: In case you chose a custom password while installing the authentication server and client APIs (Root+AB mode) in [step 4](#) on page 51, you must enter the same password in the **Authentication Service Password** field. If you installed authentication server and client APIs with the default values for the passwords, you do not need to configure these parameters during NOM installation or use the `NOMAdmin` utility.

See [Table 2-4](#) on page 55 for a description of these parameters.

NOM services must be restarted in case you have specified any new values for authentication service parameters.

Answer **y** to restart these services.

The following table describes the authentication service parameters.

Table 2-5 Authentication service parameters

Field	Value to enter
Authentication Service Host Name	The fully qualified host name (FQHN) of the server on which the authentication server is running. The default value is localhost if the authentication service is installed on the NOM server.
Authentication Service Port Number	The port number of the server on which authentication server is running. The default value is 2821.
Authentication Service Domain Name	The domain name of the root. The default value is root or root@FQHN.
Authentication Service User Name	The name of the root user used for initial authentication. The default value is admin.
Authentication Service Password	The password of the root user used for initial authentication. The default value is Vxadmin.

If you have not specified the details associated with the remote authentication server component during NOM installation, you can add

these details using the `NOMAdmin` utility. See “[Configuring Authentication Server Parameters](#)” on page 75 for details.

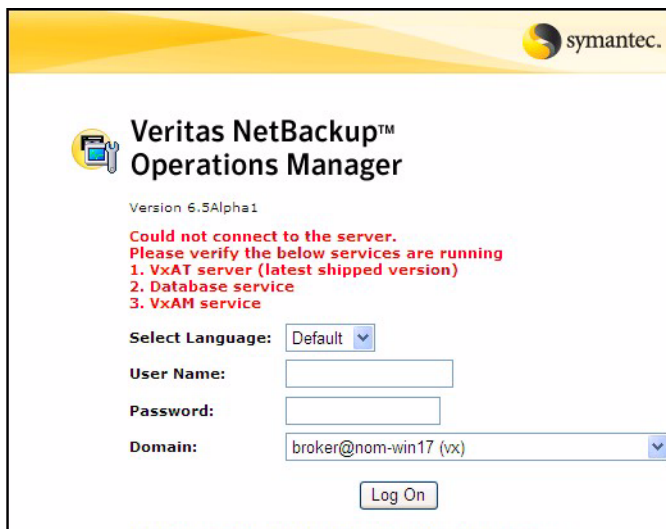
- 4 The `/opt/VRTSnom` directory is created at the completion of the installation.

Installing the Symantec Product Authentication Service before Symantec Private Branch Exchange

You should follow the installation sequence mentioned in [Table 2-4](#) on page 48 to install NOM on a Solaris server. The NetBackup client installation installs or upgrades Symantec Private Branch Exchange if it is not installed or is out-of-date. This installation sequence also connects the authentication service and private branch exchange components.

If you installed the authentication service before you installed Symantec Private Branch Exchange, you are likely to see the following issues.

- You are unable to log on to NOM server. You get the following error message as depicted in the figure:



- `NOM_Builtin@hostname` domain may not be present in the list of domains. NOM requires that you need to connect authentication service and private branch exchange components. This can be done by verifying whether `pbxexchflag` of the authentication service is set or not. When `pbxexchflag` is set, its value is equal to 1. Before setting the value of `pbxexchflag` to 1, you must stop all NOM services, Symantec Product Authentication Service and

Symantec Private Branch Exchange. After setting the value of `pbxexchflag` to 1, you must restart these services.

To connect Symantec Product Authentication Service and Symantec Private Branch Exchange:

- 1 Open the command console and enter the following command:

```
/opt/VRTSat/bin/vssat showispbxexchflag
```

This command gives the value of `pbxexchflag`. If the value of `pbxexchflag` is 0, you need to set it to 1.

Note: In case the value of `pbxexchflag` is 1, you do not need to follow the remaining steps. You should be able to log on to NOM.

- 2 Stop all the NOM services by entering the following command:

```
/opt/VRTSnom/bin/NOMAdmin -stop_service
```

- 3 Stop Symantec Product Authentication Service by issuing `kill` command on the process id of the `vxatd` service. For example, if the process id of `vxatd` service is 203, run the following command:

```
kill 203
```

- 4 Run the following command to stop Symantec Private Branch Exchange:

```
/opt/VRTSspb/bin/vxpbx_exchanged stop
```

- 5 Enter the following command at the bin directory to set the value of `pbxexchflag`:

```
/opt/VRTSat/bin/vssat setispbxexchflag --enable
```

The value of `pbxexchflag` is set to 1. Follow [step 1](#) of this procedure to verify if the value of `pbxexchflag` is 1.

- 6 Run the following command to restart Symantec Private Branch Exchange:

```
/opt/VRTSspb/bin/vxpbx_exchanged start
```

- 7 Run the following command to restart Symantec Product Authentication Service:

```
/opt/VRTSat/bin/vxatd
```

- 8 Run the following command to restart all the NOM services:

```
/opt/VRTSnom/bin/NOMAdmin -start_service
```

- 9 You will be able to log on to NOM.

Installation behavior on upgrading to NOM 6.5

You will find the following things when you upgrade from NOM 6.0 or 6.0 MPx to NOM 6.5 on Solaris:

- The data in the NOM database is retained when you upgrade to NOM 6.5. Only schema changes are applied on the NOM database during the upgrade process.
- Before upgrading to NOM 6.5, the installer queries the following:
Do you wish to upgrade?
The installer quits in case of a negative response.
- If your database port number is not 13729, then the installer retains the same database port number during an upgrade to NOM 6.5. If your database port number is 13729, then 13786 is set as the default database port number for NOM 6.5.
- The Database administrator password for NOM 6.0 or NOM 6.0 MPx remains the same when you upgrade to NOM 6.5.
- The symbolic link is retained in an upgrade to NOM 6.5. For example, you might have created a symbolic link to data present in `/opt/VRTSnom/db` directory. This link is retained in an upgrade to NOM 6.5.

Note: Some reports have been deprecated and replaced with new reports in NOM 6.5. To upgrade to the new 6.5 reports, see [“Upgrading reports from 6.0 or 6.0MPx to 6.5”](#) on page 226.

Note: The default location for the NOM database can be changed. This location can be changed after NOM has been installed or before upgrading to NOM 6.5 from NOM 6.0 or 6.0MPx. See [“Moving the NOM database to a non-default location”](#) on page 75 for specific instructions.

After NetBackup Operations Manager is installed

The following sections explain how to start using NOM and includes some performance tuning tips for NOM.

- [“Starting to use NOM”](#) on page 59
- [“Start-up tasks that NOM performs”](#) on page 59
- [“Tuning NOM for more performance”](#) on page 60
- [“Troubleshooting NOM”](#) on page 61

Starting to use NOM

After you complete the NOM installation, you are ready to start using the NOM console.

To access and log on to the NOM console

This topic provides instructions on how to access the console and log on, and provides solutions to possible issues.

- ◆ See [“Starting the NOM console”](#) on page 110.

To change the password for the administrator logon

For administrator initial logon, the user name is admin and the password is Vxadmin if you have chosen to keep the default password during installation. After initial logon, it is recommended that you change the user name and password.

To change passwords you must use the NOM authentication client application. Administrator logon passwords are not changed using the NOM console.

- ◆ See [“Changing the NOM admin password”](#) on page 88.

To learn about the NOM console components

This topic provides an overview of the console components that you will use.

- ◆ See [“NOM console components”](#) on page 116.

To learn more about using the NOM console

For instructions on understanding and using the various NOM monitoring, managing, and reporting views and related tasks, use the NOM online help.

- ◆ See [“Using help to understand NOM views and tasks”](#) on page 130.
- ◆ See [“Understanding NOM online help”](#) on page 231.

To learn about typical tasks in the NOM console

To get you started using NOM, instructions on accessing some typical monitoring, managing, and reporting tasks in NOM are provided.

- ◆ See [“A quick start for performing common tasks in NOM”](#) on page 131.

Start-up tasks that NOM performs

The first time NetBackup Operations Manager starts, the following tasks are performed.

- 1 Creates and initializes the security domain that the authentication broker requires. If this security domain is present, NOM uses it.

- 2 Creates the NOM admin user.
- 3 Starts the Sybase database server and creates and initializes the NOM database.
- 4 Starts the NOM alert manager.
- 5 Starts the NOM server.
The NOM server service depends on the NOM Alert Manager (VRTSamnom) and NOM Database Server (Sybase). If either of these services fail to start, the NOM server also fails.
The NOM server process depends on the NOM alert manager and database server. If either of these services fail to start, the NOM server also fails.
See “[Services used by NOM on Windows](#)” on page 64 for a list of services that are normally running after the NOM server is started.
See “[Processes used by NOM on Solaris](#)” on page 65 for a list of processes that are normally running after the NOM server is started.
- 6 Starts the NOM Web client (the NOM console).

Tuning NOM for more performance

The following settings can be tuned to improve NOM performance.

Default heap size for the NOM server

The NOM server default heap size can be increased from 512 MB up to 2048 MB.

On Windows servers

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VRTSnomSrvr\Parameters]
```

```
"JVM Option Number 0"="-Xmx512"
```

On Solaris SPARC servers

- 1 Open and edit the following file. This can be done using the vi editor:

```
vi /opt/VRTSnom/bin/nomsrvctl
```

- 2 Change the value of the following parameter and save the file:

```
MAX_HEAP=-Xmx512m
```

Default heap size for NOM Web server

The NOM Web server default heap size can be increased from 256 MB to 2048 MB.

Note: If you start seeing poor performance in the NOM console every few days and restarting the NOM Web service fixes the problem, you should increase the Web server default. The recommended value in this case is 512 MB.

On Windows servers

```
"INSTALL_PATH\VRTSweb\bin\webgui" maxheap 512 MB
```

On Solaris SPARC servers

```
/opt/VRTSweb/bin/maxheap 512 MB
```

Troubleshooting NOM

NOM provides a support script to collect system information about your system environment and NOM configuration. This information can be sent to the support team to analyze your system environment and provide a solution to your problem.

See “[Support script in NOM](#)” on page 96 for more information.

Administering NetBackup Operations Manager

This chapter provides information on managing the NOM database, security issues, NOM logging, SNMP use in NOM, and the NOM services and scripts that are installed.

These topics assume you already installed NOM on a server. If not, please see [“Installing NetBackup Operations Manager”](#) on page 23.

Note: The term Solaris in the following sections refers specifically to Solaris SPARC.

See the following administration and reference topics:

Topic	Description
“NOM services and processes used by NOM” on page 64	Provides the information about controlling the NOM services and processes.
“NOM database administration” on page 69	Provides the information on using the various NOM database utilities and database troubleshooting. Also provides information on how to move NOM database to a non-default location.
“Back up and restore of NOM” on page 77	Provides the detailed steps needed to back up and restore your NOM server.
“NOM security topics” on page 87	Provides the information about authentication service, the NOM Admin user, normal NOM users, and firewall issues in NOM.
“Support script in NOM” on page 96	Provides the information about using the support script for troubleshooting NOM issues.

Topic	Description
“NOM and VBR single sign-on” on page 97	Provides information on how to configure Symantec Product Authentication Service to enable the single sign-on to work between NOM and VBR.
“NOM log files” on page 102	Provides information on using NOM log files to troubleshoot NOM issues.

NOM services and processes used by NOM

This section includes the following topics about the NOM services and processes:

- [“Services used by NOM on Windows”](#) on page 64
- [“Processes used by NOM on Solaris”](#) on page 65
- [“Controlling NOM services and processes”](#) on page 67
- [“Dependency of services”](#) on page 69

Services used by NOM on Windows

After installing NetBackup Operations Manager on Windows, the following services should be active. NOM depends on these services. If any of these services fail to start, NOM will fail to start.

Service Name	Service	Description
NetBackup Operations Manager Server	javasvc.exe	The NOM server interacts with the NOM client and provides the data requested by the client from the NOM database. It also interacts with NetBackup through NBSL to get data regularly.
NetBackup Operations Manager Database Server	vrtsnomdsrv.exe	This service manages the NOM databases. This process must be running on the NOM server during all normal operations like viewing reports, running reports and so on.
NetBackup Operations Manager Alert Manager	vxamd.exe	NOM uses this service to generate alerts based on events from NetBackup and existing data in the NOM database.

Service Name	Service	Description
NetBackup Operations Manager Web Console Service	webappsvc.exe	This service is the NOM Console (client) component.
VERITAS Web Server	VRTSweb.exe	This is not a NOM service, but it is used by NOM to host the NOM Console. This component is shared by various Symantec Web consoles.
Symantec Private Branch Exchange	pbx_exchange.exe	This is not a NOM service, but it is a component used by NOM. VxPBX allows all socket communication to take place through a single port.
Symantec Product Authentication Service	vxatd.exe	This is not a NOM service, but it is used by NOM to authenticate users of NOM.

To verify that these services are running

- 1 Use **Start > Control Panel > Administrative Tools > Services**.
- 2 Check the **Status** column for each service.

The **Services** panel can also be used to stop, start, and restart the NOM services and Symantec shared services.

Processes used by NOM on Solaris

After installing NetBackup Operations Manager on Solaris, the following processes should be active.:

Process Description	Process	Detailed Description
NetBackup Operations Manager Server	/opt/VRTSnom/bin/VRTSnomd	The NOM server interacts with the NOM client and provides the data requested by the client from the NOM database. It also interacts with NetBackup to get data regularly.

Process Description	Process	Detailed Description
NetBackup Operations Manager Database Server	/opt/VRTSnom/db/bin/NOM_dbsrv	This process manages the NOM databases. This process must be running on the NOM server during all normal operations like viewing reports, running reports and so on.
NetBackup Operations Manager Alert Manager	/opt/VRTSamnom/bin/vxamd	NOM uses this process to generate alerts based on events from NetBackup and existing data in the NOM database.
VERITAS Web Server	/opt/VRTSweb/bin/webgui	This is not a NOM process, but it is used by NOM to host the NOM Console. This component is shared by various Symantec Web consoles.
Symantec Private Branch Exchange	/opt/VRTSspb/bin/pbx_exchange	This is not a NOM process, but it is a component used by NOM. VxPBX allows all socket communication to take place through a single port.
Symantec Product Authentication Service	/opt/VRTSat/bin/vxatd	This is not a NOM process, but it is used by NOM to authenticate users of NOM.

NOM server scripts on Solaris

The following scripts are used within NOM. Many of these scripts can also be used by the NOM administrator. Use the -h option for help about these scripts

Script	Location	Function	Invokes or Is Invoked by
vxnomd	/etc/init.d	Controls the start up/shut down of NOM_dbsrv, vxam, and VRTSnomd.	dbspawn, dbstop, and nomsrvctl.

Script	Location	Function	Invokes or Is Invoked by
vxnomweb	/etc/init.d	Controls the start up/shut down of the Web client under /var/VRTSnomweb.	/opt/VRTSweb/bin/startApp and /opt/VRTSweb/bin/topApp.
nomsvctl	/opt/VRTSnom/bin	Controls start or stop of VRTSnomd.	vxnomd and nom_server.
VRTSnomd	/opt/VRTSnom/bin	A symbolic link to java to give the NOM java server application its name.	vxnomd and nom_server.
nom_server	/opt/VRTSnom/bin	Starts, stops, or restarts all VRTSnom applications. Similar to running both vxnomd and vxnomweb.	The NOM administrator or custom site scripts.
nomdbms_Create ServerDB	/opt/VRTSnom/bin	Configures and initializes the database engines for NOM and VxAM.	pkgadd post-install. Also may be invoked by the NOM Administrator to complete installation manually, when the prerequisite packages were not available at pkgadd time. It is only run once.
nomps	/opt/VRTSnom/bin	Displays the status of the required NOM processes.	pkgadd post-install, vxnomd status, vxnomweb status, or the NOM administrator.

Controlling NOM services and processes

This section includes the following topics about the NOM services and processes:

- [“Controlling the NOM Database Server service on Windows servers”](#) on page 68
- [“Controlling the NOM Server service on Windows servers”](#) on page 68

- [“Controlling the NOM Database Server process on Solaris servers”](#) on page 68
- [“Controlling the NOM Server process on Solaris servers”](#) on page 68

Controlling the NOM Database Server service on Windows servers

To start or stop the NOM database server service

- ◆ Select **Control Panel > Administrative Tools > Services** and start or stop the **NetBackup Operations Manager Database Server** service.

Controlling the NOM Server service on Windows servers

To start or stop the NOM service

- ◆ Select **Control Panel > Administrative Tools > Services** and start or stop the **NetBackup Operations Manager Server** service.

Controlling the NOM Database Server process on Solaris servers

To start the database server

- ◆ Enter the following:
`/opt/VRTSnom/bin/NOMAdmin -start`

To stop the database server

- ◆ Enter the following:
`/opt/VRTSnom/bin/NOMAdmin -stop`

Controlling the NOM Server process on Solaris servers

To start the NOM server

- ◆ Enter the following:
`/opt/VRTSnom/bin/nomsrvctl -s`

To stop the NOM server

- ◆ Enter the following:
`/opt/VRTSnom/bin/nomsrvctl -k`

Dependency of services

The NOM server service is dependent on the following services (processes) running. If you stop any of these services, then the NOM server will also stop.

- NOM database server
- NOM alert manager
- Symantec Product Authentication Service
- Symantec Private Branch Exchange

NOM database administration

The Sybase databases used by NOM and VxAM are similar to that used by NetBackup and are installed as part of the NOM installation. These databases are located on the NOM server.

Visit <http://www.sybase.com/support/manuals> for information about Sybase databases.

This section contains the following database topics:

- “[Database maintenance utilities \(NOMAdmin\)](#)” on page 69
- “[Moving the NOM database to a non-default location](#)” on page 75
- “[Database troubleshooting](#)” on page 76

Database maintenance utilities (NOMAdmin)

NOM provides some useful utilities to help manage the NOM database. These utilities are available from the NOMAdmin utility. If required, NOMAdmin starts and stops the NOM server and database server. NOMAdmin also lets you change authentication server parameters and provides user help.

To run NOMAdmin on Windows

- ◆ Enter the following command:

```
INSTALL_PATH\NetBackup Operations Manager\bin\admincmd\NOMAdmin
```

To run NOMAdmin on Solaris

- ◆ Enter the following command:

```
/opt/VRTSnom/bin/NOMAdmin
```

The following sections list the individual options that are available when you use NOMAdmin utility.

NOMAdmin Option	Reference
-changePW	“Changing the NOM Database administrator password” on page 70
-changeGuest	“Changing the NOM database administrator password for guest users” on page 71
-changePort	“Changing the NOM database port number” on page 71
-export -import	“Exporting, importing and defragmenting the NOM Databases” on page 72
-version	“Displaying NOM version information” on page 72
-deleteAlerts	“Purging NOM alerts” on page 72
-purge_and_save	“Purging jobs and alerts data and saving NOM jobs data” on page 73
-purge	“Purging NOM alerts and job data” on page 74
-change_NOM_AT_p arameters	“Configuring Authentication Server Parameters” on page 75

Changing the NOM Database administrator password

This option lets you change the database administrator password used for the NOM database.

Note: This option is not used to change the logon password for NOM. To change the existing logon password you must use the NOM authentication services client application (see [“Changing the NOM admin password”](#) on page 88).

The database administrator user ID is DBA and the initial password is SQL (password is case-sensitive).

To change the database administrator password

- 1 Enter the following:
`NOMAdmin -changePW`
- 2 You are prompted for the old database administrator password.
- 3 You are prompted for a new database administrator password. New passwords cannot

- Exceed 30 characters.
- Contain consecutive black slash characters.
- Contain any bracket [] characters.
- Contain any of the following characters. These characters have special meaning in Windows or in shell scripts.
` ! \$ % & . ; > | < > , { } \$ " ~ [] \ \
- Contain any ASCII characters < 32 or > 127.
- Begin with White space and a single quote character.
- End with White space.

Changing the NOM database administrator password for guest users

NOM allows guest users to view the NOM database (read-only view of some tables and views). This option lets the administrator change the database administrator password used by guest users.

The database administrator guest user ID is `NOM_GUEST` and the initial password is `welcome` (password is case sensitive).

This database password should not be confused with the logon password for NOM. The guest password is specific to the NOM database.

To change administrator passwords you must use the NOM authentication service client application (see “[Changing the NOM admin password](#)” on page 88).

To change the database administrator guest password

- 1 Enter the following:
`NOMAdmin -changeGuest`
- 2 You are prompted for the current database administrator password (see “[Changing the NOM Database administrator password](#)” on page 70).
- 3 You are prompted for a new database guest password. See “[To change the database administrator password](#)” on page 70 for the rules for new passwords.

Changing the NOM database port number

This option lets the administrator change the default server port number used by the NOM database engine.

To change the database port

- ◆ Enter the following:
`NOMAdmin -changePort new_port_number`

Exporting, importing and defragmenting the NOM Databases

The export option creates SQL that you can use to export a snapshot of the current NOM and VxAM databases.

The import option can be used to reload this snapshot (created by exporting the database) to form the database.

The snapshots can be used to recreate your database and data.

You can also defragment the NOM databases using the export and the import options. Defragmentation helps to increase data access and retrieval speed.

To export the NOM primary database and alerts databases

- ◆ Enter the following:

```
NOMAdmin -export directory_name
```

To import the NOM primary database and alerts databases

Use this command to restore the primary NOM databases captured by the export command.

- ◆ Enter the following:

```
NOMAdmin -import directory_name
```

To defragment the NOM primary and alerts databases

To defragment the NOM database, you must first export and then import the database. You must run these commands consecutively (without any time gap) to avoid any kind of data loss.

- ◆ Enter the following commands:

```
NOMAdmin -export directory_name  
NOMAdmin -import directory_name
```

The directory location (*directory_name*) must be the same in both the commands.

Displaying NOM version information

This option displays the NOM package version and the NOM database schema version.

To display NOM versions

- ◆ Enter the following:

```
NOMAdmin -version
```

Purging NOM alerts

This option can be used to delete all alerts in the NOM database whose modification date is older than a specified date.

This option is useful if you see NOM performance degrade when there is a high number of alerts in the NOM database.

To delete old NOM alerts

- 1 Enter the following:
`NOMAdmin -deleteAlerts`
- 2 You are prompted for an alert modification date. Enter a date in `yyyy-mm-dd` format.
The utility displays the number of alerts that are deleted.

Purging jobs and alerts data and saving NOM jobs data

These options allow you to purge data collected for NetBackup jobs and alert data based on a retention period that you specify.

Any purged data is *not available* for use in NOM (monitoring, managing, or reporting).

Purged job data is saved in the NOM database for other use, while alert data is deleted permanently.

To purge and save data

- 1 Enter the following:
`NOMAdmin -purge_and_save`
- 2 You are prompted for a number of days for data to be retained. Alert data older than this number is purged from the NOM database. Job data is purged and also saved.

To automatically purge and save data

The `auto` parameter specifies that the purge and save operation will be run automatically.

If automatic purging is configured and you later run `NOMAdmin -purge`, data is purged without affecting the automatic purge configuration.

If automatic purging was configured and you later use `-purge auto`, then `-purge auto` is used for the new automatic purge configuration.

- 1 Enter the following:
`NOMAdmin -purge_and_save auto`
- 2 You are prompted for a number of days for data to be retained. Alert data older than this number is purged from the NOM database. Job data is purged and also saved.

Purging NOM alerts and job data

These options allow you to purge data collected for NetBackup jobs and alert data. Any purged data is *not available* for use in NOM (monitoring, managing, or reporting).

Any purged data is not saved.

To purge data

- 1 Enter the following:

```
NOMAdmin -purge
```
- 2 You are prompted for a number of days for data to be retained. Data older than this number is purged from the NOM database.

To automatically purge data

The `auto` parameter specifies that the purge operation is to be run automatically.

If automatic purging is configured and you later run `NOMAdmin -purge`, data is purged without affecting the automatic purge configuration.

If automatic purging is configured and you later use `-purge_and_save auto`, then `-purge_and_save auto` is used as the new automatic purge configuration.

- 1 Enter the following:

```
NOMAdmin -purge auto
```
- 2 You are prompted for a number of days for data to be retained. Data older than this number is purged from the NOM database.

To disable automatic data purging

The `auto_off` parameter disables any automatic purging.

- ◆ Enter the following:

```
NOMAdmin -purge auto_off
```

To delete saved data

Specifying this parameter deletes any data previously saved by a `save` option. See “[Purging jobs and alerts data and saving NOM jobs data](#)” on page 73.

- ◆ Enter the following:

```
NOMAdmin -purge delete_saved
```

To view your purge settings

This parameter is useful to determine the status of your automatic purge configuration (auto enabled or disabled is displayed).

If auto purging is enabled, the option also displays how old the data being purged is.

- ◆ Enter the following:

```
NOMAdmin -purge status
```

Configuring Authentication Server Parameters

Authentication server parameters can be configured during NOM installation in the security options screen in [step 3](#) on page 42 for Windows platform. Similarly, authentication server parameters can be configured during NOM installation using the instructions given in [step 3](#) on page 54 for Solaris platform.

The authentication server parameters can also be configured after the NOM installation by using the `NOMAdmin` utility.

To configure authentication server parameters using `NOMAdmin` utility

- 1 Enter the following:

```
NOMAdmin -change_NOM_AT_parameters
```

The authentication server parameters appear one by one. The current values of the parameters are specified in brackets. See [Table 2-2](#) on page 43 for a description of these parameters.

- 2 Enter the new values next to the respective parameter. If you do not enter a new value for a parameter, the value of the parameter will not change.
- 3 You must restart the NOM services for these changes to be effective. Answer **y** to restart the NOM services.

Moving the NOM database to a non-default location

The default location for the NOM database can be changed. This location can be changed after NOM has been installed or before upgrading to NOM 6.5 from NOM 6.0 or 6.0MPx. In case you modify the default location of the database before upgrading to NOM 6.5, your database will be installed in the custom location that you specify.

The following procedure describes the sequence of steps to be followed for changing the default database location on Windows and Solaris:

To move the NOM database to a non-default location on Windows:

- 1 Stop all NOM services. Enter the following command:

```
INSTALL_PATH\NetBackup Operations Manager\bin\admincmd\NOMAdmin  
-stop_service
```

- 2 Open the `database.conf` file with a text editor like notepad from the following directory:

`INSTALL_PATH\NetBackup Operations Manager\db\conf`

This file will have the following contents:

```
"INSTALL_PATH\NetBackup Operations  
Manager\db\data\vxpmdb.db" "INSTALL_PATH\NetBackup  
Operations Manager\db\data\vxam.db"
```

These paths specify the default location of the NOM primary database and the alerts database respectively.

- 3 To move the database to a custom location like `E:\Database`, replace the contents of the file with the following:

```
"E:\Database\vxpmdb.db" "E:\Database\vxam.db"
```

Make sure that you specify the path in double quotes. Also the directories in the specified path should not contain any special characters like `%`, `~`, `!`, `@`, `$`, `&`, `>`, `#` etc. For example, do not specify a path like `E:\Database%`.

- 4 Save this file and restart all NOM services.

To restart all NOM services, enter the following command:

```
INSTALL_PATH\NetBackup Operations Manager\bin\admincmd\NOMAdmin  
-start_service
```

To move the NOM database to a non-default location on Solaris:

- 1 Stop all NOM services. Enter the following command:

```
/opt/VRTSnom/bin/NOMAdmin -stop_service
```

- 2 The default location of the NOM database in Solaris is

`/opt/VRTSnom/db/data`. To move the database to a custom location like `/usr/mydata`, enter the following command:

```
mv /opt/VRTSnom/db/data /usr/mydata
```

- 3 Create a symbolic link to `/usr/mydata` in `/opt/VRTSnom/db`. To do this, enter the following command:

```
ln -s /usr/mydata /opt/VRTSnom/db/data
```

- 4 Restart all NOM services by entering the following command:

```
/opt/VRTSnom/bin/NOMAdmin -start_service
```

Database troubleshooting

See [“NOM Web client/NOM server to Sybase database communication”](#) on page 96 for security information.

See [“NOM log files on Windows servers”](#) on page 103 or [“NOM log files on Solaris servers”](#) on page 105 for NOM log files information.

Back up and restore of NOM

The procedures in this section explain about the backup of NOM and recovery in case of a disaster.

Back up and restore overview

The following sequence of steps show an overview of the backup steps to follow for NOM:

- 1 There are two separate NOM databases that need to be configured for automatic snapshots. These are the `vxpmdb` and `vxam` databases. It is necessary to configure each database, one at a time, to get proper snapshots. These snapshots are written to a specified directory. See [“Creating snapshots of the NOM and VxAM databases”](#) on page 78.
- 2 The user information managed by Symantec Product Authentication Service also must be saved in a directory or by using a NetBackup backup policy. See [“Saving the NOM user profiles managed by Symantec Product Authentication Service”](#) on page 84.
- 3 NetBackup policies can be created and used to back up the NOM database snapshots and the authentication service user configuration files. See [“Using NetBackup to save the database snapshots and user profiles”](#) on page 84.

The following sequence of steps show an overview of the recover steps to follow for NOM:

- 1 Restore the NOM database snapshot files and authentication service user profiles from the NetBackup backup image.
- 2 Install NOM on a server with the same name as the server where problems happened.
- 3 Stop the NOM services.
- 4 Copy the NOM database snapshot files and authentication service user profiles from the backup image. See [“To restore NOM on Windows servers”](#) on page 85 and [“To restore NOM on Solaris servers”](#) on page 86
- 5 If you saved a copy of the NOM database password file, see [“To restore the NOM database password file”](#) on page 86.
- 6 If you need to change the port number for the NOM database, see [“To restore NOM with a changed database Port”](#) on page 87.
- 7 Restart the NOM services.

Creating snapshots of the NOM and VxAM databases

The NOM `NightlyBackup.sql` script creates a Sybase database event that does a hot snapshot of the two NOM databases to a directory that you specify. The script also copies the database log files to this directory.

The Sybase `dbisqlc` command is used to log into the NOM databases and configure the frequency and location to use for the NOM database snapshots.

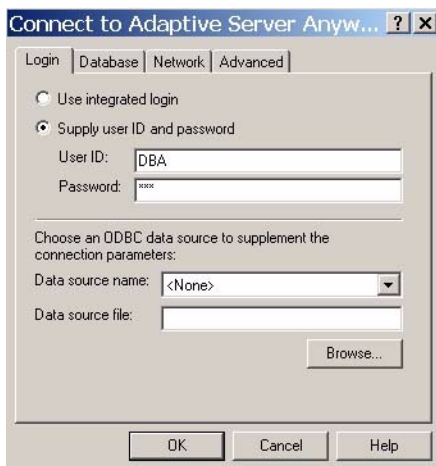
Caution: This command modifies the NOM database and should only be used to make the changes described in this document.

The VxPMDB and VxAM databases are saved every day using the time and directory specified. The script creates a subdirectory for each day of the week. Each directory contains copies of the VxPMDB and VxAM database and log files. `dbisqlc` can also be used to change the frequency or location of snapshots after they have been configured. The process to change the snapshot settings is the same, except the first line of the `NightlyBackup.sql` file must be changed to `ALTER` to change the configuration. See [step 5](#) on page 80 or [step 6](#) on page 83. The following steps only create a snapshot of the NOM databases. It is still necessary to back up these files on a daily basis using NetBackup.

To create snapshots of the databases on Windows servers

- 1 Before configuring the snapshots of the NOM databases, stop the NOM database service as follows:
Select **Control Panel > Administrative Tools > Services** and stop the **NetBackup Operations Manager Database Server** service.
- 2 When the NOM database stops, use the Windows explorer to open the `INSTALL_PATH\NetBackup Operations manager\db\WIN32` folder. Double-click the `dbisqlc` command to launch the database utility.
- 3 Enter the following information in the **Login** tab:
User ID: DBA

Password: SQL (this is the default password unless it has been changed by the administrator using the NOMAdmin option, see “[Changing the NOM Database administrator password](#)” on page 70)

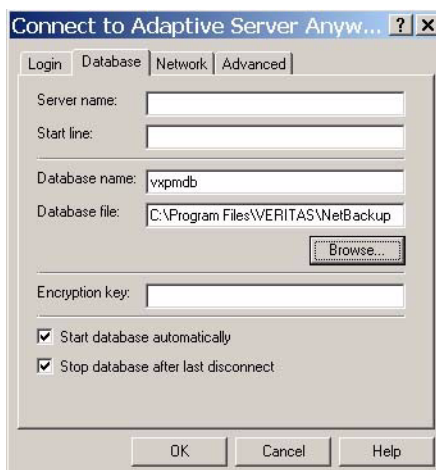


- 4 Select the **Database** tab and enter the database information. To log into the VxPMDB database use the following information.

Database name: vxpmdb

To set the database file location click **Browse** and select the *INSTALL_PATH\Netbackup Operations Manager\db\data\vxpmdb.db* file.

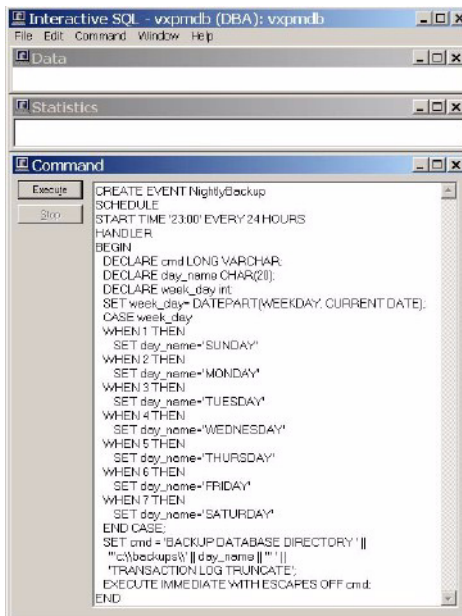
Make sure the boxes for **Start database automatically** and **Stop database after last disconnect** are checked.



After the information for the database is entered, select **OK** to start the `dbisqlc` utility as the DBA user.

- 5 A backup script (`NightlyBackup.sql`) is provided in the `admincmd` directory. Use the Windows explorer to locate the `INSTALL_PATH\NetBackup Operations Manager\bin\admincmd` folder.
Open the `NightlyBackup.sql` file using notepad or another text editor and edit the file so it reflects when and where the snapshot should occur. The following entries need to be configured.
 - a It is necessary to CREATE or ALTER the `NightlyBackup` event in the NOM database.
The first time snapshots are configured it is necessary to create the event. This is the default setting in the file: `CREATE EVENT NightlyBackup`
If the configuration ever needs to be changed, this entry needs to be changed to alter the event: `ALTER EVENT NightlyBackup`
 - b Change the START TIME to reflect the time you want to schedule the NOM database snapshot. This time uses a 24 hour clock.
For example, if the snapshot should start at 19:00 every night, then change:
`START TIME '23:00' EVERY 24 HOURS`
To
`START TIME '19:00' EVERY 24 HOURS`
 - c Change the default directory location to the directory the snapshot should be written to. It is necessary to create the directory to be used for snapshots prior to the first snapshot running.
For example, if the snapshot should be written to `d:\NOMbackups` then change:
`''c:\\backups\\' || day_name || ' ' ||`
To
`''d:\\NOMbackups\\' || day_name || ' ' ||`

- 6 Cut and paste the edited `NightlyBackup.sql` file into the **Command** section of the `dbisqlc` utility.



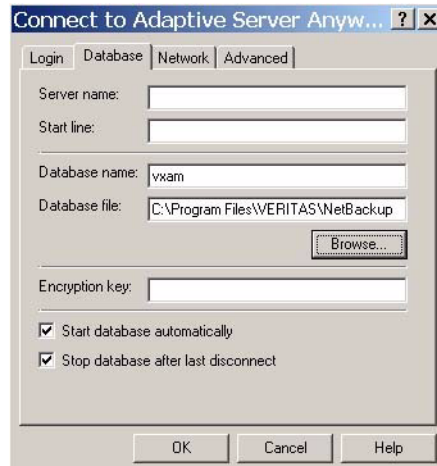
Click **Execute**. The utility makes a backup of the `vxpmdb.db` and `vxpmdb.log` files.

- 7 After executing the script, select **Command > Disconnect** from the menu to disconnect from NOM database.
Then select **File > Exit** to exit the utility.
- 8 Repeat [step 3](#) on page 78 through [step 7](#) on page 81, this time connecting to the VxAM database. To log into the VxAM Database use the following information.

Database name: vxam

To set the database file location click **Browse** and select the `INSTALL_PATH\Netbackup Operations Manager\db\data\vxam.db` file.

Make sure the boxes for **Start database automatically** and **Stop database after last disconnect** are checked.



- 9 After the VxPMD and VxAM database scripts have been updated it is necessary to restart the NOM services.
Select **Control Panel > Administrative Tools > Services** and start the **NetBackup Operations Manager Database Server** service.
Select **Control Panel > Administrative Tools > Services** and start the **NetBackup Operations Manager Server** service.

To create snapshots of the databases on Solaris servers

- 1 Log in to the NOM server as root.
- 2 Switch to the NOM database directory.
`cd /opt/VRTSnom/db/bin`
- 3 Set up the root user environment so that the `dbisqlc` database utility can be run.

If you are using the C shell use `setenv` to set the following parameters.

```
setenv LD_LIBRARY_PATH "/opt/VRTSnom/db/lib/"
setenv PATH
"/bin:/usr/sbin:/usr/bin:/usr/ucb/bin:/opt/VRTSnom/db/bin"
```

If you are using the Bourne or Korn shell then use `export` to set the following parameters.

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/VRTSnom/db/lib
export PATH=$PATH:/opt/VRTSnom/db/bin
```

- 4 Create a directory where the NOM database snapshot files are to be written
`mkdir /NOMbackups`

- 5 Change the permissions on the `NightlyBackup.sql` so it can be edited.

```
chmod 700 /opt/VRTSnom/bin/NightlyBackup.sql
```

- 6 Edit the script using `vi` or another text editor so it reflects when and where the snapshot should occur.

```
vi /opt/VRTSnom/bin/NightlyBackup.sql
```

The following entries need to be configured:

- a It is necessary to `CREATE` or `ALTER` the `NightlyBackup` event in the NOM database.

The first time snapshots are configured it is necessary to create the event. This is the default setting in the file: `CREATE EVENT NightlyBackup`

If the configuration ever needs to be changed, this entry needs to be changed to alter the event: `ALTER EVENT NightlyBackup`

- b Change the `START TIME` to reflect the time you want to schedule the NOM database snapshot. This time uses a 24 hour clock.

For example, if the snapshot should start at 19:00 every night, then change:

```
START TIME '23:00' EVERY 24 HOURS
```

To

```
START TIME '19:00' EVERY 24 HOURS
```

- c Change the default directory location in the file to the actual directory the snapshot should be written to. It is necessary to create the directory to be used for snapshots prior to the first snapshot running.

If the backup should be written to `/drive2/NOM/backups` then change:

```
'''/NOMbackups/' || day_name || ' ' ||
```

to

```
'''/drive2/NOM/backups/' || day_name || ' ' ||
```

- 7 After all changes have been made save the `NightlyBackup.sql` file.

- 8 Use the following `dbisqlc` commands to configure the NOM databases. Execute the following command to configure the `NightlyBackup` event in the `VxPMDB` database:

```
dbisqlc -c
```

```
"CS=utf8;UID=DBA;PWD=SQL;DBN=vxpmdb;LINKS=shmem,tcPIP{HS  
T=localhost;PORT=13786}"
```

```
/opt/VRTSnom/bin/NightlyBackup.sql
```

Execute the following command to configure the `NightlyBackup` event in the `VxAM` database:

```
dbisqlc -c  
"CS=utf8;UID=DBA;PWD=SQL;DBN=vxam;LINKS=shmem,tcip{HOS=localho  
st;PORT=13786}" /opt/VRTSnom/bin/NightlyBackup.sql
```

- 9 After the NightlyBackup schedule has been added to both databases exit the terminal session and restart the NOM services.

```
/opt/VRTSnom/bin/nom_server restart
```

Saving the NOM user profiles managed by Symantec Product Authentication Service

To save authentication service profiles on Windows servers

- ◆ Do one of the following to save the user profiles:
 - Copy the folder `INSTALL_PATH\Security\Authentication\systemprofile` to another folder.
 - Create a NetBackup job policy to back up the authentication service systemprofile folder.

To save authentication service profiles on Solaris servers

- ◆ Do one of the following to save the user profiles:
 - Copy the folder `/var/VRTSat/.VRTSat/profile` to another folder.
 - Create a NetBackup job policy to back up the authentication service profile folder.

Using NetBackup to save the database snapshots and user profiles

The previous procedures create snapshots of the NOM database files and the authentication service user profiles in specified directories. If these directories are not already backed up on a daily basis then it is necessary to create a NetBackup policy to back up these directories.

Backing up the NOM database password file

If you want to change the NOM database password you also need to back up the following password file (along with the backup of the NOM database files and authentication service profile folders mentioned previously):

On Windows: `INSTALL_PATH/conf/server_config.xml`

On Solaris: `/opt/VRTSnom/server_config.xml`

Using a NetBackup policy

Create a NetBackup backup policy and schedule to back up the saved directories or the files within the directories.

Note: NetBackup client software is available on the NOM server.

See the *NetBackup Administrator's Guide, Volume I* for more information on how to configure a policy and schedule.

Restoring NOM

Restore operations can be used to restore the database files and NOM in case of a disaster.

To restore NOM and the NOM databases it is necessary to configure the NightlyBackup event to generate snapshot files. These files then need to be saved using a NetBackup policy. See “[Back up and restore overview](#)” on page 77. A restore of NOM requires that the new NOM server has the same host name and IP address of the old server that crashed. This limitation involves authentication service credentials (host name and IP address) which are stored on the server.

To restore NOM on Windows servers

This procedure assumes that you have NOM database snapshots and the authentication service user profiles saved in folders.

- 1 Stop the NOM database service as follows:
Select **Control Panel > Administrative Tools > Services** and stop the **NetBackup Operations Manager Database Server** service.
- 2 If still available, move or remove the corrupted NOM database files from the NOM server.

```
cd INSTALL_PATH\NetBackup Operations Manager\db\data
move vxam.db vxamdb.old
move vxam.log vxamlog.old
move vxpmdb.db vxpmdbdb.old
move vxpmdb.log vxpmdblog.old
```

- 3 Copy or overwrite the following database snapshot files to
`INSTALL_PATH\NetBackup Operations Manager\db\data`
 - vxam.db
 - vxam.log
 - vxpmdb.db
 - vxpmdb.log

- 4 Copy or overwrite the folder containing the authentication service user profiles to
`INSTALL_PATH\Security\Authentication\systemprofile.`
- 5 Restart the NOM services.
Select **Control Panel > Administrative Tools > Services** and start the **NetBackup Operations Manager Database Server** service.
Select **Control Panel > Administrative Tools > Services** and start the **NetBackup Operations Manager Server** service.

To restore NOM on Solaris servers

This procedure assumes that you have NOM database snapshots and the authentication service user profiles saved in folders.

- 1 Stop the NOM services:
`/opt/VRTSnom/bin/NOMAdmin -stop_service`
- 2 If still available, move or remove the corrupted NOM database files from the NOM server.
`cd /opt/VRTSnom/db/data
mv vxam.db vxamdb.old
mv vxam.log vxamlog.old
mv vxpmdb.db vxpmdbdb.old
mv vxpmdb.log vxpmdblog.old`
- 3 Copy or overwrite the following database snapshot files to
`/opt/VRTSnom/db/data`
 - vxam.db
 - vxam.log
 - vxpmdb.db
 - vxpmdb.log
- 4 Copy or overwrite the folder containing the authentication service user profiles to `/var/VRTSat/.VRTSat`
- 5 Start the NOM services.
`/opt/VRTSnom/bin/NOMAdmin -start_service`

To restore the NOM database password file

If you have saved the NOM database password file, copy the file to the corresponding location on the newly installed NOM server.

- 1 For example on Windows, restore the `server_config.xml` file from the backup image.
- 2 Copy the file to `INSTALL_PATH/conf` on the newly installed NOM server.

To restore NOM with a changed database Port

- 1 If you previously changed the port of the NOM database and need to restore NOM, restore NOM as described previously (see [“Restoring NOM”](#) on page 85).
- 2 NOM is configured with the default port during the installation (13786). After NOM services are started, you can use the NOMAdmin option to change the port back to the previous port number (see [“Changing the NOM database port number”](#) on page 71).

NOM security topics

This section contains the following NOM security topics:

- [“Configuring security for managed servers”](#) on page 87.
- [“Multiple security models”](#) on page 88.
- [“NOM users”](#) on page 92.
- [“Communication and firewall considerations”](#) on page 93.

Configuring security for managed servers

You should be familiar with Symantec Product Authentication Service before you design and configure your security environment. Review [“Symantec Product Authentication Service”](#) on page 24 before deciding on your security configuration.

Symantec Product Authentication Service provides low, medium, and high levels of security. For a highly secure environment, install the authentication service root broker on a secure server. Do not install it on the NOM server, which is open to the World Wide Web.

Many different and complex security configuration options are available to you. See [“Multiple security models”](#) on page 88 for information on some common security models.

Before you set up your security environment by installing the authentication service for NOM, carefully review the Symantec Product Authentication Service and NOM documentation.

See the files in the `docs` directory of ICS CD/DVD ([“Infrastructure Core Services \(ICS\) CD”](#) on page 31 and [“NetBackup and ICS DVD”](#) on page 32) for information on how to install and configure authentication services.

Also refer to the Access Management chapter in the *NetBackup Administrator’s Guide, Volume II* for information about NBAC.

Changing the NOM admin password

NOM uses the authentication services subsystem to control access to the NOM Console. This requires using the Symantec Product Authentication Services GUI or the command line to change passwords. There is no option in the NOM Console to change the admin password.

To change the admin password from the Symantec Product Authentication Services GUI

- 1 Launch the Administration Console.
For Solaris run: `/opt/VRTSat/bin/run/runvssatgui.sh`
For Windows run: **Start > Programs > Symantec > Symantec Product Authentication Services.**
- 2 Click **Domains** and select `NOM_BuiltIn@hostname` from the list of domains.
- 3 Click **admin** from the **Principals of Selected Domain**.
- 4 Select **Authentication > Principal > Change Password**.
- 5 Enter the old admin password and the new password.
- 6 Click **Change Password** to change the password.

To change the admin password from the command line

- 1 Use the `vssat` command to change the default password for the NOM Console admin user.

```
cd /opt/VRTSat/bin
vssat changepasswd --pdrtype ab --domain NOM_BuiltIn@hostname
--prplname admin
```
- 2 Enter current password: *old-password*
Enter new password: *new-password*
Reenter new password: *new-password*

Multiple security models

The way you install, configure, and use Symantec Product Authentication Service depends on your security requirements and the deployment model.

This section describes the following two common security deployment models for managed NetBackup servers.

- [“Managed NetBackup servers with and without NBAC configured and authentication service locally installed on the NOM server”](#) on page 89.
- [“Managed NetBackup servers with and without NBAC configured and authentication service on the remote computer”](#) on page 90.

You also can mix portions of these models in your security architecture. You can use many different security deployment models with NOM, NetBackup, and other Symantec applications. Consult the Symantec Product Authentication Service documentation when you use other models of security.

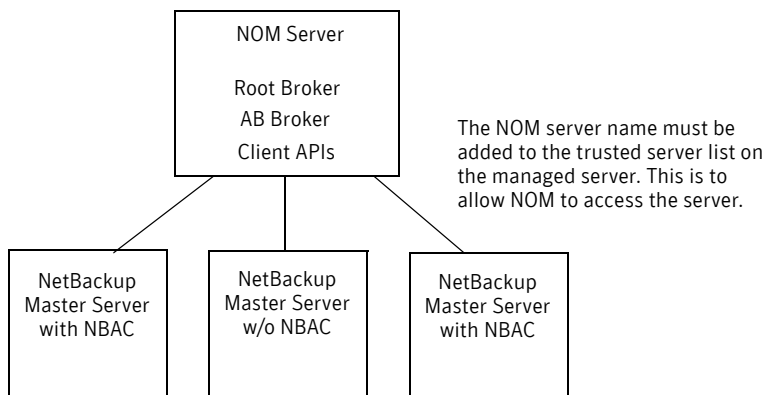
See the following topics for detailed installation instructions for these two typical models. They describe installing the required authentication service components on NOM Windows and Solaris servers:

- [“Installing Symantec Product Authentication Service on the NOM server”](#) on page 37
- [“Installing Symantec Private Branch Exchange and Symantec Product Authentication Service on the NOM server”](#) on page 50

Managed NetBackup servers with and without NBAC configured and authentication service locally installed on the NOM server

In this model, authentication service is installed locally on the NOM server in the Root + Authentication Broker (Root + AB) mode. The authentication service client APIs are also installed on the NOM server.

This model has multiple NetBackup servers. Some of these servers have NBAC configured while some do not have NBAC configured. Symantec Product Authentication Service must be installed on all the NBAC enabled servers in Root+AB mode.



The following cases are possible in this setup:

Case 1: [“Managed NetBackup servers with NBAC configured”](#) on page 90

Case 2: [“Managed NetBackup servers without NBAC configured”](#) on page 90

Managed NetBackup servers with NBAC configured

A trust relationship must be established between root broker of NOM server and the root broker of each managed NetBackup server. To set up these trust relationships, use the `vssat` command in Symantec Product Authentication Service. NOM cannot monitor NetBackup servers if the trust relationship has not been set up between NOM and NetBackup server.

See the files in the `docs` directory of the ICS CD/DVD (“[Infrastructure Core Services \(ICS\) CD](#)” on page 31 and “[NetBackup and ICS DVD](#)” on page 32) for information on how to install and configure authentication services.

Also refer to the Access Management chapter in the *NetBackup Administrator's Guide, Volume II* for information about NBAC.

Managed NetBackup servers without NBAC configured

These servers do not have Symantec Product Authentication Service and NBAC installed or configured (no root + AB brokers are installed).

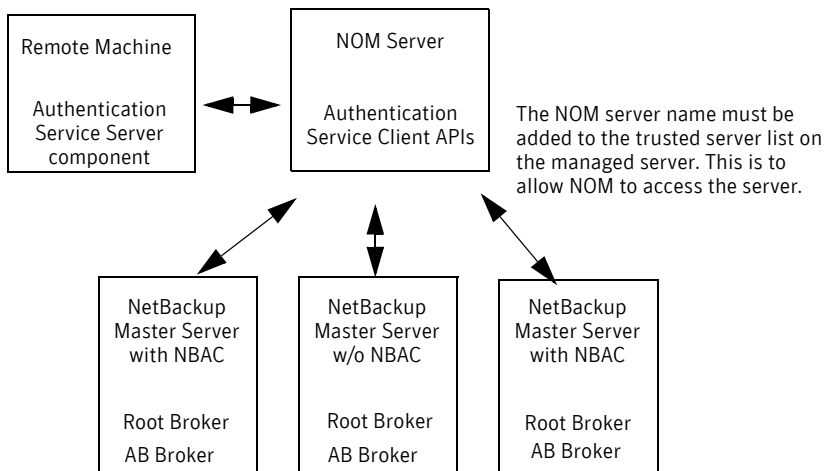
Make sure you configure these managed servers to allow server access and data collection by NOM. The NOM server name must be added to the trusted server list on the managed server. Use the **Host Properties** node of NetBackup Management on the managed server to add the name of the NOM server.

See *NetBackup Administrator's Guide, Volume II* for more details.

Managed NetBackup servers with and without NBAC configured and authentication service on the remote computer

In this model, only the client APIs for authentication service are installed on the NOM server. The authentication service server component is installed on a remote computer.

This model has multiple NetBackup servers. Some of these servers have NBAC configured while some do not have NBAC configured. The authentication service (Root + AB brokers) must be installed and configured on all NBAC-enabled managed master servers.



The following cases are possible in this setup:

Case 1: “[Managed NetBackup servers with NBAC configured](#)” on page 90

Case 2: “[Managed NetBackup servers without NBAC configured](#)” on page 90

Managed NetBackup servers with NBAC configured

A trust relationship must be established between the root broker of the NOM server and the root broker of each managed NetBackup server. To set up these trust relationships, use the `vssat` command in Symantec Product Authentication Service.

NOM cannot monitor NetBackup servers if the trust relationship has not been set up between NOM and NetBackup server.

See the files in the `docs` directory of the ICS CD/DVD (“[Infrastructure Core Services \(ICS\) CD](#)” on page 31 and “[NetBackup and ICS DVD](#)” on page 32) for information on how to install and configure authentication services.

Also refer to the Access Management chapter in the *NetBackup Administrator’s Guide, Volume II* for information about NBAC.

Managed NetBackup servers without NBAC configured

These servers do not have Symantec Product Authentication Service and NBAC installed or configured (no root + AB brokers are installed).

Make sure you configure these managed servers to allow server access and data collection by NOM. The NOM server name must be added to the trusted server list on the managed server. Use the **Host Properties** node of NetBackup Management on the managed server to add the name of the NOM server.

See *NetBackup Administrator's Guide, Volume II* for more details.

NOM users

Only NOM users can log on to NOM. NOM, as opposed to NBU, does not support role-based access.

NOM has two kinds of users namely the NOM admin user and a normal NOM user. The only difference between the NOM admin user and a normal user is that the admin user can add other NOM users. See “[The NOM Admin user](#)” on page 92 and “[Normal NOM users](#)” on page 92.

The NOM Admin user

NOM creates a private domain (`NOM_Builtin@FQDN`) and an admin user when the NOM server is first started. *FQDN* is the fully qualified domain name of the server on which the NOM server and Web client software are running.

User authentication is performed by the NOM Web client using the authentication service (authentication broker).

The admin user has the following properties:

- Is automatically granted administrative and normal user rights to the NOM server. These rights cannot be revoked.
Only the admin user has administrative rights and these rights cannot be granted to other users.
- Can add or remove other NOM users using the NOM console, and can perform all UI functions of normal users.
Settings > Access Control in the NOM console provides a list of the currently configured users of NOM (including the admin user) and provides tasks to manage NOM users.
- Has a default initial user name and password. The password can be changed at the time of NOM installation or after the NOM server is first started. This can be done by using the `vssat` command line (`changepasswd`) or the authentication GUI.
See “[Changing the NOM Database administrator password](#)” on page 70 and “[Changing the NOM admin password](#)” on page 88.
For initial logon by an administrator, see “[Logging on to the NOM console](#)” on page 112.

Normal NOM users

Any other user of NOM except the admin can be categorized as a normal NOM user. Normal users of NOM can perform all functions (for example, NetBackup

monitoring, management, and reporting), except the management of other NOM users.

A NOM admin user can add or delete NOM users. Any user that can be authenticated by the local authentication service can be added.

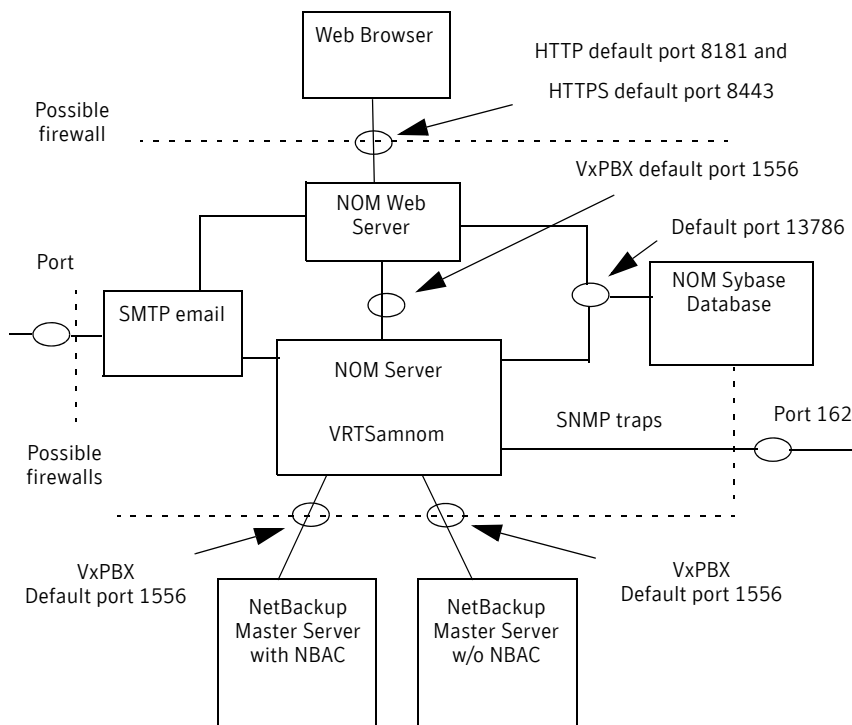
Active Directory or Network Information Service (NIS) users can be made NOM users. (A local to remote authentication trust relationship may be needed).

LDAP (Lightweight Directory Access Protocol) is also supported.

See the *Symantec Product Authentication Service Administrator's Guide* located in the docs directory on the ICS CD/DVD for a list of naming services that are supported by authentication service.

Communication and firewall considerations

The following figure shows the key NOM components and the communication ports that are used.



The following table shows the default port settings for NOM.

SMTP recipient ports can be configured from the NOM console (using **Settings > System**). SNMP trap recipient ports can be configured from the NOM console (using **Settings > Recipients**).

The Sybase database server port can be configured using the Admin utility (see “[Changing the NOM database port number](#)”). If these ports are changed then the appropriate hardware ports have to be opened.

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
NOM Server	Mail Server	25	SMTP	Allow from source to destination.
NOM Server	SNMP Server	162	SNMP trap recipient	Allow from source to destination.
NOM Server	NetBackup Master Server(s)	1556	VxPBX (pbx_exchange)	Allow between source and destination (bi-directional). VxPBX port number configuration is not supported. See “ NOM Web client to NOM server software communication ” on page 95.
NOM Client	NOM Server	1556	VxPBX (pbx_exchange)	Allow between source and destination. Some hardened servers and firewall configurations may block this port. VxPBX port number configuration is not supported. See “ NOM Web client to NOM server software communication ” on page 95.
Web Browser	NOM Server	8181	HTTP (vrtsweb)	Allow from all hosts on network.
Web Browser	NOM Server	8443	HTTPS (vrtsweb)	Allow from all hosts on network.

Source Host	Destination Host	Port Number	Usage (Process Name)	Port Configuration
NOM Server	NOM Server	13786	Sybase database (vrtsnomdbsrv)	Allow between source and destination. Some hardened servers and firewall configurations may block this port.
NOM Server	NetBackup Master Server(s)	2821	Symantec Product Authentication Service (vxatd)	Allow between source and destination in case NBAC is enabled on NetBackup master server.

Web browser to NOM Web client connection

Web browsers use Insecure Hyper Text Transfer Protocol (HTTP) and Secure Hyper Text Transfer Protocol (HTTPS) to communicate with the NOM Web client. These protocols use TCP/IP.

The default port initially used by NOM is 8181 for HTTP and is then switched to 8443 for HTTPS. These ports are opened only for input and are configurable using the VRTSweb console or command lines.

See the administering Veritas Web appendix of the *Veritas Cluster Server Administrator's Guide for Windows* or the *Veritas Cluster Server User's Guide for Solaris* for instructions on using VRTSweb to configure these ports.

NOM Web client to NOM server software communication

The NOM Web client uses VxPBX to communicate with the NOM server software. The default port is 1556. The VxPBX port is opened for input and output traffic.

Since it is an independent component, the VxPBX port number can be changed through VxPBX configuration files. Changing the VxPBX port number on the server where NOM is installed may cause NOM to fail.

See the PDF files in the `docs` directory of the ICS CD/DVD ("[Infrastructure Core Services \(ICS\) CD](#)") on page 31 and "[NetBackup and ICS DVD](#)" on page 32) for information about VxPBX.

NOM server to NetBackup master server (NBSL) communication

NOM requires the NetBackup Service Layer (NBSL) and NetBackup Event Manager (NBEvtMgr) to be present on all managed master servers.

See the *NetBackup Administrator's Guide, Volume II* for information on how to configure NBSL.

Symantec Private Branch Exchange is used for communication and requires a port opened for input and output. The default VxPBX port used is 1556. The VxPBX port range is not configurable.

NOM cannot communicate with different master servers for which Symantec Private Branch Exchange is running on different ports.

See the PDF files in the `docs` directory of the ICS CD/DVD (“[Infrastructure Core Services \(ICS\) CD](#)” on page 31 and “[NetBackup and ICS DVD](#)” on page 32) for information about VxPBX. Also see “[NOM Web client to NOM server software communication](#)” on page 95 for information on VxPBX.

Also see “[Configuring security for managed servers](#)” on page 87 for information on how to use NBAC with NetBackup servers.

SNMP traps

SNMP trap protocol is used for outbound UDP traffic and requires a port that opens for output. The port number is 162.

NOM Web client/NOM server to Sybase database communication

The NOM Web client communicates with the NOM Sybase ASA database server by using the default port 13786.

The Sybase database server port is closed to all inbound connections. The database is available only to resident NOM components on the NOM server.

NOM Web client/NOM server email communication

SMTP email server protocol is used for outgoing mail. The port number is defined when the SMTP server port is specified by the user (see **Settings > System** in the NOM UI console to specify this port). The port is opened for output only.

Support script in NOM

NOM provides a support script to collect data about your system environment and NOM configuration. This can serve as a first-level information for the support team in case of an issue with NOM.

To run the support script

- 1 Run the following commands to execute the support script. These commands must be executed on the NOM server.
For Solaris run: `/opt/VRTSnom/bin/nomsupport`
For Windows run: `INSTALL_PATH\NetBackup Operations Manager\bin\admincmd\nomsupport.bat`
- 2 This script stops all the NOM services and then collects system information and NOM configuration information. It then zips all this information in a file called `Support.zip`. You can also choose to add log files, NOM database files etc to this zip file.
Adding log files and NOM database files can increase the file size of `Support.zip`.
- 3 This zip file is stored in the following directories:
On Solaris: `/opt/VRTSnom/temp/Support.zip`
On Windows: `INSTALL_PATH\NetBackup Operations Manager\temp\Support.zip`
- 4 After the zip file is created, the script starts all the NOM services.

NOM and VBR single sign-on

A single sign-on is sufficient for migrating between NOM and VBR (Veritas Backup Reporter). To enable cross-navigation between NOM and VBR using a single sign-on, you must configure Symantec Product Authentication Service on the NOM machine to allow the authentication brokers to exchange information. Configuring these authentication broker trusts allows cross-product linking without additional user logons. The following sections specify how you can cross-navigate between NOM and VBR.

Considerations for NOM and VBR

The following things should be kept in mind before setting up the single sign-on between VBR and NOM:

- NOM and VBR should be installed on separate computers.
- Symantec Product Authentication Service should be installed in Root+AB mode on both NOM and VBR computers.

NOM and VBR single sign-on

You must perform the following steps to enable the single sign-on to work between NOM and VBR:

Step	Description	See this Topic
1	Create a VBR trusted user on the NOM server	“Creating a VBR trusted user on the NOM server” on page 98
2	Create a valid NOM user who can log on to NOM using VBR credentials.	“Creating a NOM user who can access VBR” on page 100
3	Connect NOM and VBR	“Connecting NOM and VBR” on page 101

Creating a VBR trusted user on the NOM server

This involves using the credentials of a VBR user to create a VBR trusted user on the NOM server. The trusted user should have a valid user name, password, domain name, and domain type.

- 1 Create a VBR user. If a VBR user has already been created, you will have the following credentials:

Credentials in Veritas Backup Reporter	Value
User name	A valid user name with which to connect to VBR. The default user name in VBR is admin.
Password	The password for the specified user name used to connect to VBR. The default value of password is password
Domain name	The name of the network domain of which the specified user name is a member. The default is the private domain name <code>cc_users@<machine name></code> For example: <code>cc_users@nom-win14</code>
Domain type	The type of network domain specified: NIS, NT, or a private domain. Valid entries are: nis, nt, or vx. The default domain type in VBR is vx.

Credentials in Veritas Backup Reporter	Value
Broker	<machine name> where VBR has been installed. For example: nom-win14
Port number	The registered port number for Symantec Product Authentication Service is 2821.

These credentials will be used in the subsequent steps.

See *Veritas Backup Reporter Administrator's Guide* for information on how to create a VBR user.

- 2 Access the Symantec Product Authentication Services command line interface on the NOM server. To access the command line interface, navigate to the following directory:

On Windows: `INSTALL_PATH\security\authentication\bin`

On Solaris: `/opt/VRTSat/bin`

- 3 Create the domain-broker mapping in Symantec Product Authentication Service application on the NOM server.

- a Add the domain-broker mapping by running the following command:

```
vssat addbrokerdomain --broker host:port --domain type:name
--broker host:port refers to the host and port of the broker. The
registered port for Authentication is 2821.
```

```
--domain type:name is the domain information of the domain for
which broker name needs to be configured.
```

You must specify the broker and domain credentials for the VBR user as parameters in this command. These credentials have been defined in [step 1](#) on page 98.

This command can be used as shown in the following example:

```
vssat addbrokerdomain --broker nom-win14:2821 --domain
vx:cc_users@nom-win14
```

After running this command, a domain-broker mapping is created in the local registry. Such a mapping indicates which broker should be approached when trying to authenticate to a particular domain.

- b View all the mappings that are present in the local registry by running the following command:

```
vssat showallbrokerdomains
```

- 4 Establish trust relationship between NOM and VBR machine. To establish a trust relationship between NOM and the VBR machine, run the following command on the NOM server:

```
vssat setuptrust --broker remotehost:port --securitylevel high
```

where `<remotehost>` is either a host name, qualified domain host name, or host IP address of the remote VBR host with which you are establishing the trust.

`<port>` is the port number of the broker to be trusted. 2821 is the registered port number for Symantec Product Authentication Service.

This command can be used as shown in the following example:

```
vssat setuptrust --broker nom-win14:2821 --securitylevel high
```

Answer **y** to the next prompt for establishing trust between NOM and VBR machines.

- 5 Create the user certificate on the NOM server. To create a user certificate, run the following command:

```
vssat authenticate --domain type:name --prplname prpl name  
--password password --broker host:port
```

`--domain <type:name>` is the name and type of the domain that holds the principal.

`--prplname <prpl name>` is the name of the principal that is to be authenticated.

`--password <password>` is the password of the principal that is to be authenticated.

`--broker <host:port>` is the hostname and port number of the broker.

You must use the credentials for the VBR user as parameters in this command. This command can be used as shown in the following example:

```
vssat authenticate --domain vx:cc_users@nom-win14 --prplname  
admin --password password --broker nom-win14:2821
```

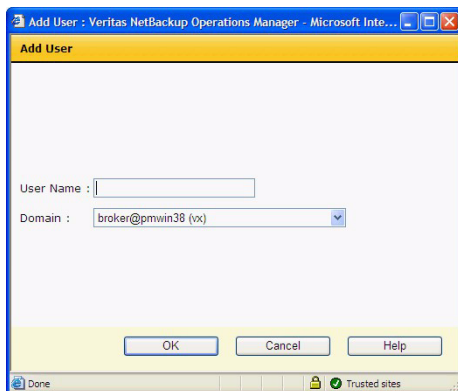
You can also verify if this user certificate has been created. You can find the user certificate listed in the output when you run the following command:

```
vssat showcred
```

Creating a NOM user who can access VBR

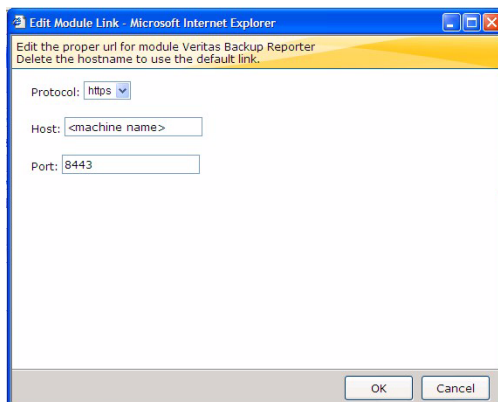
- 1 Log on to the NOM console using Administrator credentials. The default credentials are admin/Vxadmin.
The same NOM host must be used that has been configured for single sign-on.

- 2 Click **Settings > Access Control** and then click **Add User** from the **Tasks** pane. Specify the same user name and domain as your VBR credentials and click **OK**.



Connecting NOM and VBR

- 1 Log on to NOM with the newly created user that has the VBR credentials. The same NOM host must be used that has been configured for the single sign-on.
- 2 Click **Veritas Backup Reporter** and add the corresponding entries as shown in the following figure:



The protocol used must be https and the port number must be 8443. The value of the host field is the same as *<machine name>* where VBR is installed.

- 3 Click **OK**. Click **Veritas Backup Reporter** again and the VBR home page appears.

The configuration information required for [step 2](#) in this procedure is only needed once. Subsequent navigation to VBR is allowed without providing this information again.

NOM log files

NetBackup Operations Manager creates log files that you can use to troubleshoot installation, performance, and other issues. NOM writes log files using VERITAS Unified Logging (VxUL), legacy, and other log file formats.

See “[NOM log files on Windows servers](#)” on page 103 and “[NOM log files on Solaris servers](#)” on page 105.

VxUL log files

The VxUL log file creates log file names and messages in a format that is standardized across all Symantec components. These messages use VxUL IDs (a product ID and an originator ID) that identify the component that wrote the log message.

NOM components create most log messages in VxUL format. The following table shows the originator IDs used by NOM and key shared components:

VxUL originator ID	Originator name
103	Symantec Private Branch Exchange service (PBX)
132	NetBackup Service Layer (NBSL)
146	NetBackup Operations Manager Reporting Service
147	NetBackup Operations Manager Client
148	NetBackup Operations Manager Server

In Windows, NOM writes VxUL logs to the following directory:

`INSTALL_PATH\NetBackup Operations Manager\logs`

In Solaris, NOM writes VxUL logs to the following directory:

`/usr/opensv/logs`

The settings in the following log configuration file determine how NOM writes log files:

On Windows: `INSTALL_PATH\NetBackup\nblog.conf`

On Solaris: `/usr/opensv/netbackup/nblog.conf`

See the *NetBackup Troubleshooting Guide* for more information about VxUL logs and how to use the following configuration file and commands:

- `nblog.conf`
- The `vxlogview` command to view logs
- The `vxlogmgr` command to manage log files
- The `vxlogcfg` command to configure log settings

NOM log files on Windows servers

NOM writes the following log files using VxUL and legacy formats.

NOM log files

Log file directory	Log file	Troubleshooting purpose
<i>INSTALL_PATH</i> \NetBackup Operations Manager\logs\	convertdb_err.txt	These files contain redirected stdout and stderr output from the commands that run during the installation of NOM.
	convertdb_out.txt	
	ulconfig_err.txt	
	ulconfig_out.txt	
	NOMSrvr_err.txt NOMSrvr_out.txt	These log files for system.err and system.out pass to javasvc when you install the NOM server service.
	vxam.txt	NOM VxAM activity.

Log files for the components that NOM uses

Log file directory	Log file	Troubleshooting purpose
<i>INSTALL_PATH</i> \Security\Authentication\bin	vxatd.log vssconfig.log	VxSSAT activity.

NOM database log files

Log file directory	Log file	Troubleshooting purpose
<i>INSTALL_PATH</i> \NetBackup Operations Manager\logs\	nomdbsrv.log	NOM Sybase database activity.
<i>INSTALL_PATH</i> \NetBackup Operations Manager\db\log\	server.log	VxDBMS activity.
<i>INSTALL_PATH</i> \NetBackup Operations Manager\db\data\	vxam.log vxpmdb.log	NOM Sybase database transaction files. NOTE: Do not change these two log files.

NOM Web client log files

Log file directory	Log file	Troubleshooting purpose
<i>INSTALL_PATH</i> \VRTSweb\log\	_vrtswb0.0.log	Web client application activity (stdout).
	_err0.0.log	Web client errors (stderr).

Log file directory	Log file	Troubleshooting purpose
	nom0.0.log	Web client start up and shut down activity.

VxUL log files for NOM and the components that NOM uses

Log file directory	Log file	Troubleshooting purpose
<i>INSTALL_PATH</i> \VxPBX\bin\	50936-103*.log	VxPBX activity.
<i>INSTALL_PATH</i> \NetBackup\logs\ 51216-132*.log	51216-111*.log	NetBackup activity.
<i>INSTALL_PATH</i> \NetBackup Operations Manager\logs\ 51216-146*.log	51216-132*.log	NBSL activity.
<i>INSTALL_PATH</i> \NetBackup Operations Manager\logs\ 51216-147*.log	51216-146*.log	NOM Web client (reporting service) activity.
	51216-148*.log	NOM Web client activity.
		NOM server activity.

NOM log files on Solaris servers

NOM creates the following log files by using VxUL and legacy formats.

NOM log files

NOM log file	Troubleshooting purpose
/opt/VRTSnom/logs/VRTSnom.log	stdout and stderr for the VRTSnomd daemon.
/tmp/installnom_trace.nnnn	Provides a trace for any installation issues.
/opt/VRTSnom/logs/vxam.txt	NOM VxAM activity.

Log files for the components that NOM uses

Log file	Troubleshooting purpose
/var/VRTSsat/vxatd.log	VxSSAT activity.

NOM database log files

NOM log file	Troubleshooting purpose
/opt/VRTSnom/logs/nomdbsrv.log	NOM Sybase database activity.
/opt/VRTSnom/db/data/vxam.log	NOM Sybase database transaction files.
/opt/VRTSnom/db/data/vxpmdb.log	Note: Do not touch these log files.

NOM Web client log files

NOM log file	Troubleshooting purpose
/var/VRTSweb/log/_vrtsweb0.0.log	Web client application activity (stdout).
/var/VRTSweb/log/_err0.0.log	Web client errors (stderr).
/var/VRTSweb/log/_nom0.0.log	Web client start up and shut down activity.

VxUL log files for NOM and the components that NOM uses

NOM log file	Troubleshooting purpose
/opt/VRTSspb/log/50936-103*.log	VxPBX activity.
/opt/openssl/logs/51216-111*.log	NetBackup activity.
/opt/openssl/logs/51216-132*.log	NBSL activity.

NOM log file	Troubleshooting purpose
/var/VRTSnomweb/webgui/logs/51216-146*.log	NOM Web client (reporting service) activity.
/var/VRTSnomweb/log/51216-147*.log	NOM Web client activity.
/opt/VRTSnom/logs/51216-148*.log	NOM server activity.

Getting started using the NOM console

This section covers the basics of how to access and use NetBackup Operations Manager. It includes how to log on and log off, how to set up managed master servers or server groups, and how the NOM console works.

The following topics are included:

Topic	Description
“Before you use the NOM console” on page 110	Describes how to use the extensive online help to learn more about NOM capabilities and tasks.
“Starting the NOM console” on page 110	Describes how to start the NOM console to manage your NetBackup servers. Potential start-up issues are also covered.
“NOM console components” on page 116	Provides the detailed information on the navigation features, panes, links, and table components available in the NOM console.
“Using help to understand NOM views and tasks” on page 130	Provides a table of typical NOM tasks and how to locate information about them in the NOM online help.
“Using NOM context groups” on page 132	Provides an overview about predefined and user-defined master server groups.
“Using Web browser bookmarks” on page 141	Describes how to use bookmarks to mark key views and tasks in NOM that you use frequently.

Before you use the NOM console

For information on how to understand and use the various NOM views and related tasks, refer to the NOM online help. Context-sensitive help is available for all console views, task dialog boxes, and wizard task screens.

The NOM online documentation assumes that the user has a good working knowledge of NetBackup and its concepts and components.

Portions of the online help may refer the user to other NetBackup documentation for descriptions of NetBackup fields and components.

The following NetBackup documents are referenced in the NOM online help.

- *NetBackup Administrator's Guide for Windows, Volume I*
- *NetBackup Administrator's Guide for UNIX and Linux, Volume I*
- *NetBackup Shared Storage Guide for UNIX, Windows, and Linux*
- *NetBackup Troubleshooting Guide for UNIX, Windows, and Linux*

See [“Using help to understand NOM views and tasks”](#) on page 130 and [“Understanding NOM online help”](#) on page 231 for more information.

Starting the NOM console

The NOM server is the focal point for centralized management of the NetBackup servers (release 6.0 MP5 and greater) in your backup environment.

When you install NetBackup Operations Manager, you select the computer that serves as the NOM server. When you start the NOM console to manage and monitor your NetBackup environment, you open a connection to the NOM Web client.

Topic	Description
“Accessing the NOM console” on page 111	Describes how to access the NOM console
“Logging on to the NOM console” on page 112	Describes how to supply logon credentials for NOM
“Logging out of the NOM console” on page 114	Describes how to log off from NOM
“Possible issues when using the NOM console” on page 114	Provides the troubleshooting information for other NOM issues that may occur during operations

Accessing the NOM console

On a system that has a network connection to the NOM server, start the system's Web browser.

From the browser, type the following address to start the NOM console.

host.domain is the name of the NOM server and can also be an IP number.

```
http://host.domain:8181/nom
```

Possible NOM console access issues

You may see the following issues when you access the console.

Issue

You cannot connect to the Web client. Your Web browser displays the following messages: “page cannot be displayed” or “connection was refused.”

Cause

The Veritas Web client (the NOM console) is not running or is inaccessible on the network.

Solution

- 1 Verify that the VERITAS Web server service (VRTSweb) is running.
- 2 Verify that a Web browser on the NOM server can connect to the NOM console by using the following address:

```
http://localhost:8181/nom
```

Issue

The Veritas Web client is running, but the NOM console is not available. Your Web browser displays an “HTTP STATUS 404” error.

Cause

The NOM console application is not loaded.

Solution on Windows

- 1 Locate the `nom.war` file in the following directory to verify that the NOM application is installed:
`INSTALL_PATH\VRTSweb\VERITAS`
- 2 Verify that the NOM application is running by using the `monitorApp` command line utility. This utility is located in the `VRTSweb\bin` directory. Enter `monitorApp nom`.

- 3 If the NOM application is not running, start it by using the `startApp` utility in the `VRTSweb\bin` directory.
If the application is running, a `nom` directory exists in the same directory as `nom.war` file.

Solution on Solaris

- 1 Locate the `nom.war` file in the following directory to verify that the NOM application is installed:
`/opt/VRTSnom/webgui`
- 2 Verify that the NOM application is running by using the following command. Any required NOM process that is not running appears with NOT RUNNING in its entry.
`/opt/VRTSnom/bin/nom_server status`
- 3 If any processes appear as NOT RUNNING, restart the NOM software by running the following command:
`/opt/VRTSnom/bin/nom_server restart`

Logging on to the NOM console

You must supply logon credentials on the NOM login screen.

To log on to NetBackup Operations Manager console

- 1 Choose a display language for the console by using the drop-down list. The first time you log on, NOM uses the default language of the Web browser. If NOM does not support this language, it uses English. After initial logon, you can specify a default language by using **Settings > Preferences** and then select **Default**. If you do not set a default, NOM uses the Web browser language (or English).
- 2 Enter a user name and password, and select a domain from the **Domain** drop-down list. `NOM_Builtin@FQDN` domain is used for logging on. `FQDN` is the fully qualified domain name of the server on which the NOM server and web client software are running.
For administrator initial logon, the user name is `admin` and the password is `Vxadmin` or any custom password that you chose during the installation.
For a Solaris NOM server also, the administrator initial logon is through `NOM_Builtin@FQDN` domain. The user name is `admin` and the password is `Vxadmin` or any custom password that you chose during the installation.
After you create recipients in NOM, select `hostname (unixpwd)` as the domain setting.
After the initial log on, you should change the user name and password. To change existing passwords use the Symantec Product Authentication

Service. Administrator logon passwords are not changed using the NOM console.

See “[Changing the NOM Database administrator password](#)” on page 70. NOM can use any password added to the security environment.

3 Click **Log On.**

Initially, a monitoring overview of the NetBackup master servers under NOM management appears. When you log off from the console, NOM saves your settings and preferences and uses these settings when you restart the console again.

Possible NOM console logon issues

You may see the following issues when you log on to the console.

Issue

You have a user authentication error. The login screen displays the message “User authentication failed. The user name/password are invalid for the selected domain.”

Cause

The Symantec Product Authentication Service cannot validate the user name and password for the entered domain.

Solution

Enter a valid user name, password, and domain.

Issue

The entered user name is not a registered NOM user. The login screen displays the message “User *user_name* is not a registered NetBackup Operations Manager user.”

Cause

The user name and domain are valid, but the user was not added to the list of users for NOM.

Solution

Log on as the NOM admin user and add the user to the list of NOM users.

Issue

You cannot connect to the NOM server. The login screen displays the message “Unable to connect to server *server_name*.”

Cause

The NOM server is not running.

Solution

Start the NOM server and verify that it is running properly.

Logging out of the NOM console

When you log out from the console, NOM saves all settings and changes you make in a NOM session.

To log out from NetBackup Operations Manager

- ◆ Click **Logout** located on the right side of the title bar.

Possible issues when using the NOM console

You may see the following issues while running the console.

Issue

The connection to the NOM server is lost. The message “*NOM_server* - Not Responding” appears in the **Connected To** pane (see “[The connected to pane](#)” on page 119).

Solution

Restart the NOM server and verify that it is running properly. Then refresh the GUI from your browser. The GUI automatically reconnects to the NOM server.

Issue

Your NOM console session times out. The login screen appears when you try to change views or refresh the current view.

Cause

After 30 minutes of inactivity, the NOM user automatically logs out of the console. Any attempt to use NOM, displays the NOM login screen.

Solution

Log on again. After successful logon, you then return to the NOM view that you last visited.

Issue

An internal error occurs in the NOM console. An exception error message appears in the NOM console.

Cause

This error results from an internal issue in the NOM console application.

Solution

Use one of the following solutions:

- Close the browser and open a new browser session.
- Restart the NOM console.

Issue

You receive the message “Application initialization failed. The database credentials could not be retrieved from the NOM server.”

Cause

The NOM Web application was not able to get the database credentials from the NOM server.

Solution

Ensure that the NOM server and database are running.

Issue

You receive the message “Application initialization failed. The reporting service is not running.”

Cause

The NOM reporting service was not started successfully.

Solution

Restart the NOM database, server, and Web server.

Issue

You receive the message “Active scripting is required to use this application. Enable active scripting in the browser.”

Cause

Active scripting is disabled in the Web browser.

Solution

Enable active scripting in the Web browser. You must enable it to use NOM.

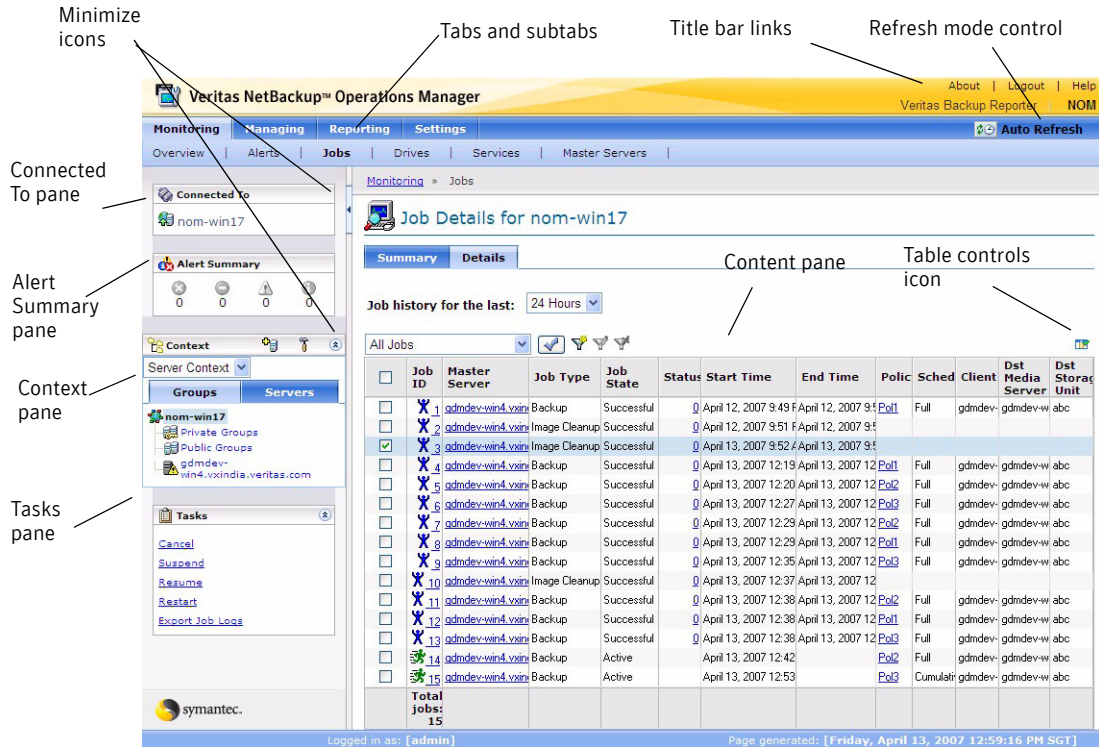
NOM console components

This section provides information on the panes and navigation features available in the NOM console. You view the console by using a Web browser.

When you log on initially, the **Summary** view of the monitoring overview appears (**Monitoring > Overview**). See “[Summary and details views](#)” on page 123. The following is an example view that shows the NOM console components.

When you change the settings and preferences they are saved and if you log out and log on again these settings will be used.

The following figure shows the NOM console components.



The following topics describe the main elements of the console in greater detail.

Topic	Description
“Using the links on the title bar” on page 117	Describes how to use the links (for example, Logout and Help) available from the title bar
“Using tabs and subtabs” on page 118	Provides an overview about the main and subtabs available in the console
“Using the refresh mode control” on page 119	Describes how to control the frequency that the NOM console refreshes to reflect changes in your backup environment
“The connected to pane” on page 119	Describes the pane that contains the NOM server connection and its status
“Using the alert summary pane” on page 120	Describes how to use the pane that displays a quick visual summary of any current alerts
“Understanding the context pane” on page 120	Describes how to use the pane that serves as a key navigation tool in NOM
“Using the task pane” on page 123	Provides an overview about task panes
“Using the content pane” on page 123	Describes how to use the main data display pane that NOM uses
“The NOM status bar” on page 124	Describes how to use the status bar at the bottom of the NOM console
“Visual keys in the console” on page 124	Describes how to use the visual keys that NOM uses to help you understand displayed information
“Using tables” on page 125	Describes how to use tables, which includes how to customize tables, select rows, and use filters.

Using the links on the title bar

Use the NOM links available in the title bar at the top of the console for the following tasks:

- To know NetBackup Operations Manager product version and copyright information (click **About**).
- Disconnect from the NOM server to end your session (click **Logout**). See [“Logging out of the NOM console”](#) on page 114.
- Access NetBackup Operations Manager help (click **Help**). Context-sensitive help for all views, wizards, and dialog boxes is also available. See [“Understanding NOM online help”](#) on page 231 for more information.

- Switch between using NOM and VBR (Veritas Backup Reporter). A single user sign-on allows cross navigation between these two products. Click **Veritas Backup Reporter** to access Veritas Backup Reporter from the NOM console.

If you want to use VBR, see “[NOM and VBR single sign-on](#)” on page 97 for information on how to set up a single sign-on.

When you click **Veritas Backup Reporter** for the first time, you need to provide the protocol, host and port number. The protocol used must be https and the port number must be 8443. The value of the host field is the same as *<machine name>* where VBR is installed. This configuration information is only required once. Subsequent navigation to VBR is allowed without providing this information again.

Using tabs and subtabs

The following main tabs provide access to the major areas of the NetBackup Operations Manager console.

Tab	Description
Monitoring	Monitor the status of NetBackup jobs, drives, services, and master servers; and display and respond to any NOM alerts.
Managing	Manage NOM alert policies, NetBackup job policies, storage units, devices and media.
Reporting	View standard NOM reports, create and run custom reports, and schedule reports. The Reporting tab is not available when a Policy context or a Client context group is selected in the Context pane.
Settings	Customize the NOM server, add NOM users, define user preferences, add context groups, configure job cycles, and set up email and SNMP recipients.

Under each main tab is a series of subtabs. The contents of these subtabs vary depending on the current view and represent the views accessible from each main tab. For example, under the **Reporting** tab are subtabs for **My Portal**, **All Reports**, and **Scheduled Reports**.

Also, not all tabs or subtabs are available when a Policy context or a Client context group is selected in the Context pane. NOM views depend on context groups that you select in the Context pane.

See “[Understanding the context pane](#)” on page 120 and “[Using NOM context groups](#)” on page 132 to know more about context groups.




Using the refresh mode control

As you use NetBackup Operations Manager, the status of your backup environment is likely to change. Devices go online and offline, NOM generates alerts, media usage fluctuates, and so on. You can control when the information in the console refreshes to reflect the changes in your backup environment.

To change the refresh setting

In the upper right-hand corner of the console window, a refresh icon indicates the current refresh setting and allows you to change the refresh settings.

- 1 Click the refresh icon.
- 2 Select one of the setting choices from the first column of the following table. The refresh icon changes to reflect your choice as shown in the third column.

Dialog box setting	Description	Icon shown
Disabled	Disables the update notification. This setting does not provide notification of data changes. You must use your browser refresh button periodically to update your view.	
Notify Only	Informs you when data is available that is more current than the displayed information. To display current data, manually refresh by clicking the refresh icon that appears in place of the notify icon or click your browser's refresh button. Notify Only is the default setting.	
Auto Refresh	Automatically updates the console display every 60 seconds or when the displayed data is no longer current.	

The connected to pane

The **Connected To** pane shows the NOM server that you logged on to and also the state of your connection to the server. If you lose your connection to the NOM server, the server connection icon changes from green to red.

This pane is available in all NOM console views.

Related topics

[“Visual keys in the console”](#) on page 124

Using the alert summary pane

The **Alert Summary** pane provides a visual summary of the critical, error, warning, and informational alerts for the NetBackup master servers to which you are connected. This pane is available in all console views.

If no outstanding system alerts exist, all icons appear as gray.

To view outstanding alerts quickly

- ◆ Click any of the four available colored icons for alerts.
A filtered detail view for that alert category appears (this view is a shortcut to **Monitoring > Alerts > Details**).

Related topics

[“Visual keys in the console”](#) on page 124

Understanding the context pane

The **Context** pane is a key navigation and configuration tool in NetBackup Operations Manager. This pane lets you select and also manage the group context to control the scope of your views.

NOM provides three types of context groups used to monitor and manage your backup environment: server context, client context, and policy context.

Using NOM context groups you can view NetBackup information for your whole management domain, a context group, or an individual server (in the case of **Server Context**).

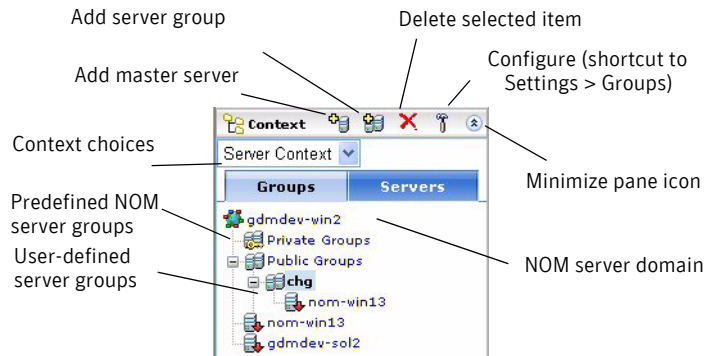
The **Context** pane

- Is available in any NOM view where you can change the group context.
- Uses unique icons and colors to convey operational states.
For example, a managed server that is online is shown with a green arrow icon. This means that all of the NBSL monitors are currently connected to the managed server.
- Allows you to access and change the context groups that you monitor or manage.
As you navigate within the NOM console, your context selection applies for any subsequent views until you select a different context.
Using this pane is one of the methods you can use to determine the scope of information that you view.

- Allows you to add and manage context groups.
Icons are available to add a context group, or only an individual server. These icons are present in the respective **Context** pane only where that particular task is allowed.
You also can use the **Configure** icon to add and manage context groups. Using this icon is a shortcut to the configuration tasks available in the **Settings > Groups** view.

The following figure shows a sample context pane for **Server Context**.

The context pane for **Client Context** and **Policy Context** are similar, but only contain context groups.



To minimize the context pane

- ◆ Click the minimize icon in the **Context** pane. Click the icon again to view the pane.

Understanding the groups and servers tabs

The NOM server name (the NOM domain) appears as the top level in the context tree.

If you select another group context or a group, all data views in the content pane on the right change. You can also select the entire NOM domain.

The groups tab

Context groups appear alphabetically in a hierarchical (tree) structure. This tab includes all configured context groups that NOM manages. It may contain all of your NetBackup servers, job policies, or clients; or subgroups.

The groups tab shows you at a glance where you are in your NOM environment and makes it easy to move to another level. To navigate within the tree, expand

(+) or collapse (-) the groups in the tree. The group that is currently selected is highlighted.

The groups tab contains two predefined groups: **Private Groups** and **Public Groups**. You cannot edit predefined groups, but you can add user-defined subgroups under these predefined groups.

Private groups (predefined)

Any NOM user can add groups under private groups. New groups in the private group are only visible to the creator of the groups. Users can edit and delete only the private groups that they create. Private groups are displayed with an icon that contains a lock symbol.

Public groups (predefined)

The NOM administrator can add groups under public groups. New groups in the public group are visible to all users. Only the NOM administrator can edit or delete public server groups.

User-defined groups

A user-defined group can either be a part of a private group or a public group. You cannot move user-defined groups between the NOM predefined groups.

User-defined groups can contain other subgroups. If the selected context is **Server Context**, groups can contain individual master servers in addition to subgroups containing servers.

The servers tab (available in server context only)

When the selected group context is **Server Context**, this tab contains an alphabetical list of all NetBackup servers that NOM manages. The server that is currently selected is highlighted in the list.

This tab may be useful if you manage a small number of servers and do not want to create and use managed server groups.

Related topics

[“Visual keys in the console”](#) on page 124

[“Using NOM context groups”](#) on page 132

[“Configuring server groups or servers \(using the context pane\)”](#) on page 133

[“Configuring client or policy groups \(using the context pane\)”](#) on page 137

[“Selecting server, client, or policy groups to manage”](#) on page 139

Using the task pane

In many views in the console, a task pane is available. This pane provides access to tasks that are related to that specific tab and view. A task usually requires a selection in the **Content** pane, and until a selection is made, a task may be unavailable.

To minimize the tasks pane

- ◆ Click the minimize icon in the **Tasks** pane. Click the icon again to view the pane.

Using the content pane

When you initially log on to NetBackup Operations Manager, the content pane displays a summary of information for all master servers in the NOM server domain. Initially, a monitoring overview appears (**Monitoring > Overview > Summary**).

Information in the content pane varies and is context sensitive to current selections in the **Context** pane, the tabs and subtabs, and the **Task** pane.

Summary and details views

The NOM monitoring and managing tabs present information in two main viewing modes: **Summary** and **Details**. You can view information about your NetBackup environment in the summary view or use the details view. To switch between these views, use the **Summary** tab or the **Details** tab.

For example, you can view a summary of completed NetBackup jobs for a master server by using the **Monitoring > Jobs > Summary** tabs. If you click the **Details** tab, detailed job activity appears for that server.

After you use the console to drill down and view details, use the **Summary** tab to return to a NOM summary from any view.

Summary views can provide an overview of the entire domain of the NOM server to which you are connected. By using summary views, you can quickly determine the overall status of your operation in a single content pane.

The **Details** tab views contain information in a variety of tabular and graphical formats.

To enlarge the content pane

To provide a larger view of the content pane, use the minimize icon to hide all NOM console panes that normally appear on the left.

- ◆ Click the icon between the **Context** pane and the content pane. This icon is called Collapse Task Panel. Click the icon again to show all panes.

The NOM status bar

At the bottom of the console, the **Logged in as** value shows the user name that is logged onto the NOM server.

The **Page generated** value shows the date and time of the NOM server you are logged on to (adjusted to match your time zone). This value updates when the view changes or refreshes.

Visual keys in the console

To help you understand the information it presents, NetBackup Operations Manager uses several visual keys. These keys include color, status icons, and tool tips.

Color coding

The following colors are used along with status icons:

- Red indicates a critical condition that may cause the system to be unable to perform an important function. Investigate critical conditions immediately. An icon with a red arrow pointing downwards (offline) means that a connection to the managed server is lost. A reattempt to connect happens after 2 minutes. An icon with a red dashed-circle means that data collection for the managed server was disabled by the user.
- Yellow (or orange) indicates a warning condition that may cause the system to perform in a way that you do not want. Investigate warning conditions as soon as possible. A server that is partially online is shown with a yellow caution icon. One or more NBSL monitors are down. NOM tries to reconnect the monitor.
- Green indicates a normal condition, result, or operation. A managed server that is online is shown with a green arrow icon which points upwards. This means that all of the NBSL monitors are currently connected to the server.
- Blue indicates informational-only conditions.
- Blue-gray and gray often indicate enabled and disabled, or assigned and unassigned conditions respectively.

Status icons

Status icons are also used with color coding. When NOM detects a condition (for example, up or down) for a managed NetBackup server, job, drive, or drive path, the icon contains color coding.

These icon colors represent critical, warning, or informational conditions and let you quickly determine the status of a particular area in your NetBackup environment. For example, the detail view for monitoring jobs contains green icons for running and idle jobs.

Unique icons also appear in the drive details view for shared drives (the NetBackup SSO option). These icons represent the shared drives that are up on all servers that share the drive. Icons also appear for shared drives where the drive status is mixed (up on some servers and down on other servers that share the drive).

The following icons are used for managed NetBackup master servers in the **Context** pane:

- An icon with a green arrow pointing upwards (online) means that all of the NBSL monitors are currently connected to the managed server.
- An icon with a red arrow pointing downwards (offline) means that a connection to the managed server is lost. A reattempt to connect happens after 2 minutes.
- An icon with a red dashed-circle means that data collection for the managed server was disabled by the user.
- A server that is partially online is shown with a yellow caution icon. One or more NBSL monitors are down. NOM tries to reconnect to the monitor.
- A managed server icon with a line through it denotes that the server is not a valid managed NetBackup server. This may happen when you uninstall and reinstall NOM on a managed server.

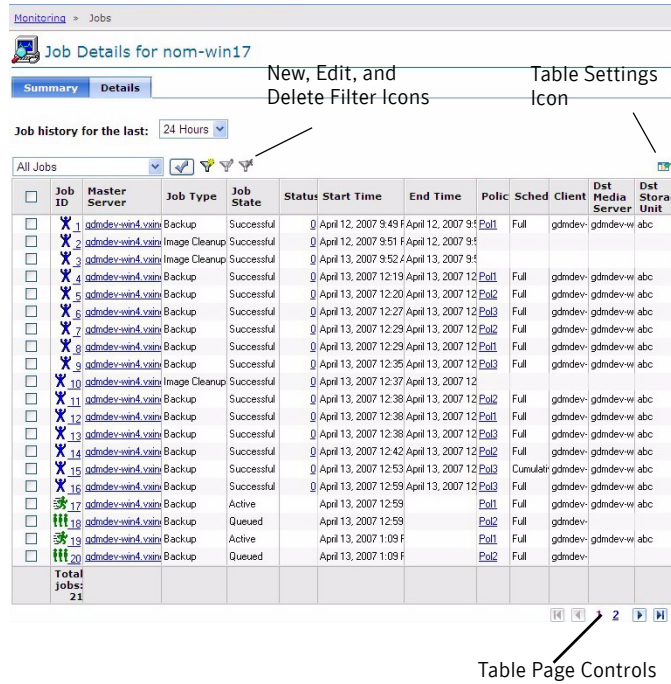
Tool tips

Tool tips provide brief descriptions of the tool and the status icons that appear in NOM views. A tool tip appears when you place the mouse over an icon.

Using tables

NOM collects information about aspects of your NetBackup environment and presents much of this information in tables. This section describes how to change the tables to display the information you want to see. The following is a sample table showing task icons.

The following figure shows the task buttons for tables.



The following topics describe these tasks in greater detail.

Topic	Description
“Customizing tables for your needs” on page 126	Describes how to customize tables, including how to view normally hidden columns and how to move columns.
“Accessing multiple pages of data in tables” on page 128	Describes how to view tables with multiple pages of data.
“Selecting rows in tables” on page 128	Describes how to select single or multiple table rows.
“Using filters to customize your views” on page 129	Describes how to use table filters, including how to create and use custom filters.

Customizing tables for your needs

You can perform the following operations to a table. The table refreshes after the operation and shows the changes you made.

- Add or remove columns.
- Re-arrange the order of the columns for your individual requirements.
- Choose the number of rows and which columns to display.
- Sort columns in ascending or descending order.
- Change the widths of columns.

For these operations, NOM saves and reloads your customized settings when you log on to the NOM server again. Each user can have different customized table settings.

To specify which columns appear in a table

Initially, some NOM tables do not show all available columns. To view any of these columns, you may first have to remove one or more columns from the table and then add the missing columns.

- 1 Click the **Table Settings** icon at the top of the table.
- 2 Remove columns you do not want to appear by selecting the column in **Selected Columns**. Then click **Remove**.
Add any columns that currently do not appear by selecting the column in the **Available Columns** list. Then click **Add**. Added columns appear as the last column in the table.

To move a column

- 1 Click the **Table Settings** icon at the top of the table.
- 2 Select the name of the column in **Selected Columns**. Click **Move Up** to move the column to the left in the table. Click **Move Down** to move the column to the right in the table.

To choose a sort order for a column or a multiple columns

You can group columns together to provide a multi-column sort. See [“To sort the contents of a column or multiple columns”](#) on page 128 for instructions on how to sort columns.

- 1 Click the **Table Settings** icon at the top of the table.
- 2 Use the **Sort** drop-down list box that is available for each column.
- 3 Select **Up** to sort the largest values for that column at the bottom of the table. Select **Down** to sort the largest values for that column at the top of the table.

To choose the number of rows that appear per page for a table

- 1 Click the **Table Settings** icon at the top of the table.

- 2 Select a number from the **Rows Per Page** drop-down list box.
- 3 Select **Apply To All Tables** if you want the **Rows Per Page** setting to apply to all tables in NOM (includes reports).

To sort the contents of a column or multiple columns

See “[To choose a sort order for a column or a multiple columns](#)” on page 127 for sort order instructions for columns.

- ◆ In a table, click the column name. The column sorts in ascending order by default.
To sort in descending order, click the column name again.

To change the width of a column

- 1 Select the edge of the column heading and hold down the left mouse button.
- 2 Drag the edge of the column heading to the right or left.

Accessing multiple pages of data in tables

Much of the monitoring information appears in a table format. NOM tables display 10 rows at one time by default. You can also change the number of rows to be displayed in the table from the Table Settings icon.

When you have more data to display than can fit in a table, the table contains multiple pages. Use the table page controls (located below the table) to help you navigate the pages.

To display the next 10 rows or to return to a previous set of rows in large tables, use the table page controls.

To go to a specific page

- ◆ Click the page number.

To go to the previous or the next page

- ◆ Click the left arrow or the right arrow.

To go to the first or the last page

- ◆ Click the double left arrow or the double right arrow.

Selecting rows in tables

For many tables in NOM, you must select a row or rows to enable the tasks in the **Tasks** pane.

To select a row in a table

- ◆ Click the check box for that row. Click the check box again to deselect the selected row.

To select all rows on the current page of the table

- ◆ Click the check box in the header row of the table. Click the check box again to deselect all selected rows.

Using filters to customize your views

Many tables in NOM let you display a subset of the information available by creating and using custom filters, or by using the predefined (ready-to-use) filters. A filter screens information that is based on a set of conditions that you define. Once you create a filter, you can save it, edit it, or remove it.

In the views that allow filtering, filtering icons appear above the table.

Creating custom filters

After you create a custom filter, it appears in the filter drop-down list.

To create a custom filter

- 1 Select the **New filter** icon.
- 2 Type a name for the filter in **Filter name**.
- 3 For **Column**, select the column name that you want to filter on from the drop-down list.
For **Operator**, select an operator. Use **!=** if you do not want to match a specific value.
For **Value**, enter or select a value.
If you select **Start Time** or **End Time** for **Column**, a calendar icon appears for **Value**. Click the calendar icon to choose a date and time and then click **OK**.
- 4 Click **>>** to build the filter query.
The **Filter Definition** on the right shows the resulting filter queries. You can use the drop-down lists to add or remove open and closed parentheses to refine a query further. You can also use parentheses to nest your queries. If the query is not what you want, click the **Delete** icon to remove the query.
- 5 To continue building the filter, select another column. Repeat [step 3](#) and [step 4](#).
- 6 Click **OK** when you finish building the filter. Your new filter is available in the filter drop-down list.

Applying filters

NOM filters the table according to the criteria you specify. The view remains in effect until you change it by selecting another filter.

Picking a filter to use

To pick a filter

- 1 From the drop-down list, select a custom filter or a NOM built-in filter.
- 2 Click the check mark icon.

Editing Custom filters

You cannot modify the ready-to-use NOM filters. You can only modify custom filters.

To edit a custom filter

- 1 From the drop-down list, select a custom filter.
- 2 Click the **Edit filter** icon.
- 3 See “[Creating custom filters](#)” on page 129 for instructions for using the dialog to edit a filter.
Make your changes.

Deleting custom filters

You cannot delete the ready-to-use filters.

To remove a custom filter

- 1 From the drop-down list, select a custom filter.
- 2 Click the **Delete filter** icon.
- 3 Click **OK** to remove the filter.

Using help to understand NOM views and tasks

The NOM context-sensitive online help for a view is the best place to start understanding the capabilities and tasks in the console.

The NOM help for the various console views provides the following:

- A description of the view
- How to navigate within the view
- How to start the tasks that are related to the view

In many cases, links to helpful, related topics are at the end of each help topic.

To access the online help, use the help buttons in most dialog boxes and wizard screens. You also can use the help button on the title bar of NOM views (see “[NOM console components](#)” on page 116).

See “[Understanding NOM online help](#)” on page 231 for more information on the help components and how to use help.

The following table contains common starting tasks in the console and how to locate them in the NOM console.

A quick start for performing common tasks in NOM

The following table lists some tasks you may be interested in and how to locate information about them.

To learn how to	Use the Help button in this console view
Add authorized NOM users	Settings > Access Control
Set up user preferences	Settings > Preferences
Configure the SMTP server and NOM alert retention settings	Settings > System
Set up recipients for alert and report notification	Settings > Recipients
Configure NOM server groups and master servers	Settings > Server Groups
Create NOM alert policies for your site	Managing > Alert Policies > Summary and Managing > Alert Policies > Details
View and respond to NOM alerts	Monitoring > Alerts > Details
View the details for a NetBackup job	Monitoring > Jobs > Details
View a NetBackup job policy	Managing > Job Policies > Details
Control NetBackup job policies	Managing > Job Policies > Details

To learn how to	Use the Help button in this console view
Configure log settings for NetBackup master servers	Select a master server first and then see the following views: Monitoring > Master Servers > List Log Files > Configure Log Settings Setting > Groups > List Log Files > Configure Log Settings Monitoring > jobs > Details (click the drill down link from the Master Server column) > List Log Files > Configure Log Settings Managing > Job Policies > Details (click the drill down link from the Master Server column) > List Log Files > Configure Log Settings
Export NetBackup job log files	Monitoring > Jobs > Details
Control NetBackup services	Monitoring > Services > Details
Use the NOM standard reports	Reports > All Reports > Standard Reports
Create custom reports for your needs	Reports > All Reports > New Report
Schedule when you want a report to run	Reports > All Reports > Schedule

Using NOM context groups

NOM provides three types of context groups that can be used to monitor and manage your backup environment:

- Server context
- Client context
- Policy context

Using context groups you can view NetBackup information for your whole management domain, a context group, or just an individual server (in the case of server context).

Server context view shows all the four tabs namely **Monitoring**, **Managing**, **Reporting** and **Settings** while client and policy context views do not show the **Reporting** tab.

The following topics describe configuring and using context groups in greater detail.

Topic	Description
“Configuring server groups or servers (using the context pane)” on page 133	Describes how to configure servers or server context groups.
“Configuring client or policy groups (using the context pane)” on page 137	Describes how to configure client or policy context groups.
“Selecting server, client, or policy groups to manage” on page 139	Describes how to select a context group (or single server) to manage your NetBackup environment.

Configuring server groups or servers (using the context pane)

Based on your needs, you can organize NetBackup master servers into groups of servers for ease of management. Server groups can contain individual master servers or subgroups of servers.

You can add, edit, or remove a group of managed servers, or an individual server. Note the following points:

- Any NetBackup master servers that you add to the NOM domain of managed servers appear in the **Groups** tab *and* in the **Servers** tab.
- The NOM server name (the NOM domain) appears as the top level in the groups or server tree.
If you select the NOM domain in the **Context** pane, you can *only* add individual servers. The **Add master server** icon is available.
- You can create a server group without adding any servers, but you cannot add servers to the groups until you add individual servers in NOM. You can create a server group only under the Private or Public groups.
- You can add a single, master server in multiple server groups, but you can add it only once in any server group. You also can add a server in a server group and in subgroups of that server group.

For example, you can include server named `West` in server group-23 and in server group-24, but you cannot include it twice in server group-23. You can define the server named `West` in server group-23 and in a subgroup of server group-23.

If you include a managed server in a server group multiple times, the server group displays contain only one set of data for that server.

- If you select one of the predefined NOM server groups (**Private Groups** or **Public Groups**) in the **Context** pane, you can *only* add server groups. Only the **Add server group** icon is available.
- If you select a user-defined server group in the **Context** pane, you can add servers or server groups. The **Add master server** and **Add server group** icons are available.
- If you select a server in the **Context** pane, you cannot add servers or server groups. The **Add master server** and **Add server group** icons are *not* available.
- When you click the **Configure** icon for edit tasks, you are directed to the NOM **Settings > Groups** view with your server or server group selection highlighted.
- If you delete a master server it is also deleted from all server groups of which it is a member.

The following topics describe these tasks in greater detail.

Topic	Description
“Adding a master server” on page 134	Describes how to add a NetBackup master server to your NOM domain
“Editing a master server” on page 135	Describes how to change the configuration information for a NetBackup master server
“Removing a master server” on page 136	Describes how to remove a server from your NOM domain
“Adding a server group” on page 136	Describes how to add a group of NetBackup master servers to the NOM domain
“Editing a server group” on page 136	Describes how to change the configuration information for a master server group
“Removing a server group” on page 137	Describes how to remove a server group from the NOM domain

Adding a master server

To allow the NOM server to communicate with a managed NetBackup server and collect data requires some security configuration.

If you use NetBackup Access Control (NBAC) on the managed NetBackup server, you must configure Symantec Product Authentication Service security.

If you do not use NBAC, add the name of the NOM server to the trusted SERVER list on the managed server. Use the **Host Properties** node of **NetBackup Management** on the managed server to add the name of the NOM server.

For more information, see “[NOM security topics](#)” on page 87.

To add a managed NetBackup server

- 1 In the **Context** pane, select the server group level where you want to add the server.
- 2 Click the **Add master server** icon.
- 3 In the **Network name or IP address** field, enter a host name, a fully qualified server name (*server.domain*), or an IP address. This field is required. Any IP address is accepted, but unresolved network names are not accepted. Optionally, you can use **Locate** to determine if the NOM server can connect to and talk to the NetBackup master server. Master servers must be running NetBackup release 6.0 MP5 (or greater) to communicate with NOM 6.5.
- 4 In **Display name** enter a name for the server. You can use duplicate display names (you can change the display name later). You can use special characters. The server name is optional and if left blank, NOM uses the network name.
- 5 Click **OK** when you finish.

Tip: You can click **Add** to add multiple servers without closing the dialog box.

An error appears if the NOM server cannot connect to the NetBackup master server on the network.

Editing a master server

To edit the information for a managed NetBackup server

- 1 In the **Context** pane, select the server you want to change.
- 2 Click the **Configure** icon.
- 3 From the **Context Groups Tasks** pane, select **Edit**.

Note: The edit server dialog box is also available from other views in the NOM console.

- 4 Supply the information that the dialog box requests. You can change the name of the server (or its IP address) or the display name for the server. Optionally, you can use **Locate** to determine if the NOM server can connect to and talk to the NetBackup master server. Master servers must be running NetBackup release 6.0 MP5 (or greater) to communicate with NOM 6.5.
- 5 Click **OK**.

You receive a message if the server successfully updates.

Removing a master server

To remove a managed NetBackup server

- 1 In the **Context** pane, select the server you want to remove.
- 2 Click the **Delete selected item** icon.
- 3 Click **OK** to remove the selected item.

Adding a server group

To add a server group

- 1 In the **Context** pane, select the server group where you want to add the server group.
- 2 Click the **Add server group** icon.
- 3 In the **Group name** field, type a descriptive name for the server group. This name is required. You can use special characters. You cannot use duplicate or blank group names.
- 4 Select the check box next to each NetBackup master server you want to include in this server group.
Click the forward arrows (>>) to add the servers to the server group.
Click the back arrows (<<) to remove the servers from the server group.
- 5 Click **OK** when done.

Tip: You can click **Add** to add multiple server groups without closing the dialog box.

Editing a server group

To edit the information for a server group

- 1 In the **Context** pane select the server group you want to change.
- 2 Click the **Configure** icon.
- 3 From the **Context Group Tasks** pane, select **Edit**.
- 4 You can change the **Group name** field.
- 5 Select the check box next to each NetBackup master server you want to include in this server group.

Click the forward arrows (>>) to add the servers to the server group.

Click the back arrows (<<) to remove the servers from the server group.

6 Click **OK**.

Removing a server group

To remove a server group

- 1 In the **Context** pane select the server group you want to remove.
- 2 Click the **Delete selected item** icon.
- 3 Click **OK** to remove the selected group.

Related topics

[“Configuring client or policy groups \(using the context pane\)”](#) on page 137

[“Selecting server, client, or policy groups to manage”](#) on page 139

Configuring client or policy groups (using the context pane)

If you have a number of NetBackup clients that are backed up or job policies, you can organize them into logical groups for ease of management.

You can create and manage groups of clients or groups policies from the available list of NetBackup clients or policies.

NetBackup clients or policies are available to NOM when a master server is initially added as a managed server in NOM. If other clients or policies are later added to the managed server they also are available to NOM.

You can add, edit, or remove a group. Note the following points:

- The NOM server name (the NOM domain) appears as the top level in the groups tree.
- You can *only* add new client or policy groups to existing groups. You cannot add an existing group to a group.
- You can not create a group that contains clients *and* policies.
- When you click the **Configure** icon for edit tasks, you are directed to the NOM **Settings > Groups** view with your group selection highlighted.

The following topics describe these tasks in greater detail.

Topic	Description
“Adding a client or policy group” on page 138	Describes how to add a group of NetBackup clients or policies to the NOM management domain.

Topic	Description
“Editing a client or policy group” on page 138	Describes how to change a group of NetBackup clients or policies.
“Removing a client or policy group” on page 139	Describes how to delete a group of NetBackup clients or policies.

Adding a client or policy group

To add a group

- 1 In the **Context** pane, select the group where you want to add the new group.
- 2 Click the **Add client group** or **Add policy group** icon.
- 3 In the **Group name** field, type a descriptive name for the group. This name is required. You can use special characters. You cannot use duplicate or blank group names.
- 4 Select the check box next to each NetBackup client or policy that you want to include in this group. Click the forward arrows (>>) to add clients or policies to the group. Click the back arrows (<<) to remove clients or policies from the group.
- 5 Click **OK** when done.

Tip: You can click **Add** to add multiple groups without closing the dialog box.

Editing a client or policy group

To edit the information for a group

- 1 In the **Context** pane select the group you want to change.
- 2 Click the **Configure** icon.
- 3 From the **Context Group Tasks** pane, select **Edit**.
- 4 You can change the **Group name** field.
- 5 Select the check box next to each NetBackup client or policy that you want to include in this group. Click the forward arrows (>>) to add clients or policies to the group. Click the back arrows (<<) to remove clients or policies from the group.
- 6 Click **OK**.

Removing a client or policy group

To remove a group

- 1 In the **Context** pane select the group you want to remove.
- 2 Click the **Delete selected item** icon.
- 3 Click **OK** to remove the selected group.

Related topics

[“Understanding the context pane”](#) on page 120

[“Configuring server groups or servers \(using the context pane\)”](#) on page 133

[“Selecting server, client, or policy groups to manage”](#) on page 139

Selecting server, client, or policy groups to manage

As you navigate within NOM, your current group selection in the **Context** pane determines the scope of your view. If the group context is **Server Context**, you can select a single master server.

Using groups, you can broaden your view to see an overview of NetBackup information for all client or policy groups. Or you can focus your attention on a particular group of servers or a single managed master server.

To select the group (or an individual server) that you want to view and manage, you can do either of the following actions:

Action	Reference topic
Use the Context pane	“Selecting a group using the context pane” on page 140.
Drill down in a group table	“Selecting a group by drilling down in a group component table” on page 140.

Keep the following points in mind:

- The selected context can be **Server Context**, **Client Context**, or **Policy Context**.
- You can set the default context using the **Settings > Preferences** tab. If a default is not set, server context is used as the default.
- When you select a group, an overview appears that shows the groups in the selected group.

If the context is **Server Context**, a summary view appears that shows the servers (and any server groups) in that selected group. If you select a single server, a view appears for only that server.

- You can change context while in a subtab to a new context where the subtab is not applicable. In this case, you are presented an overview of the parent tab.
For example, your context is **Server Context** and you are in the **Managing > Devices** subtab. You then change the context to **Client Context** where this subtab is not applicable. You are then directed to the **Managing > Overview** view.
- Your group (or managed master server) selection applies for any subsequent views in NOM (until you select a different context or group).

Selecting a group using the context pane

In the **Groups** tab, context groups appear in a tree (hierarchical) structure. This tree tells you at a glance where you are in your group environment and makes it easy to move to another group.

If the context is **Server Context**, the **Servers** tab contains a list of all added NetBackup master servers.

To navigate within the tree, expand or collapse the branches of the tree. The group (or server) that is currently selected is highlighted.

To select a group

If you want your view or actions to affect all managed context groups, select the NOM domain. If you select a group (or a server) lower in the context tree, only the views for that selection appears.

- 1 In the **Context** pane, select a context.
- 2 In the **Groups** tab, navigate the tree and select a group.

To select a master server (available only for server context)

- 1 In the **Context** pane, select **Server Context** and the **Servers** tab.

Tip: You also can select a master server from the **Groups** tab.

- 2 Select a master server.

Selecting a group by drilling down in a group component table

From a group component summary table, you can drill down and select a group.

To drill down to a group

- ◆ Click a group link. These links appear in the **Name** column.

If the context is **Server Context**, you can also select a master server from the table.

Related topics

[“Understanding the context pane”](#) on page 120

[“Configuring server groups or servers \(using the context pane\)”](#) on page 133

[“Configuring client or policy groups \(using the context pane\)”](#) on page 137

Using Web browser bookmarks

By using your Web browser, you can add a bookmark for any view in the NOM console and return to it as needed.

If you log out of the NOM console, you can use the bookmark to return to the same view after you log onto the console.

Understanding NOM alert policies and alerts

NetBackup Operations Manager provides tools to create and manage alert policies and handle any resulting alerts that the policies generate. Alert policies help you manage your NetBackup environment by providing constant monitoring of your NetBackup systems.

You can create alert policies to detect when something goes wrong with NetBackup and troubleshoot it. Alert policies help you anticipate and handle problems before they occur. For example, you can monitor for frozen media and email the operator when the number of frozen media exceeds a threshold value. You then can take corrective action.

When a NetBackup system event triggers a NOM alert (based on your alert policies), the following occurs:

- NOM sends email or SNMP notices to any recipients that are configured in the policy.
- The NOM console displays views to help you track and manage these alerts.

Some examples of alert events that can be monitored are as follows:

- A job fails with an error.
- Lost contact with a media server.
- A service stops.
- Catalog space is low, or a catalog is not backed up.

This chapter contains the following topics on NOM alert policies and alerts.

Topic	Description
“NOM alert policies” on page 144	Describes the alert policies that you can create, use, and manage.

Topic	Description
“Administering NOM alerts” on page 149	Describes how to handle any generated alerts. These alerts are created and distributed based on alert policies that you define.
“Using SNMP with NOM” on page 153	Provides information about SNMP and how it is used by NOM.

NOM alert policies

NOM provides a policy-based alert mechanism and alert notification that lets you proactively identify issues before problems occur in your NetBackup systems.

You use the alert policy wizard to create alert policies using predefined alert conditions to monitor typical issues or thresholds within NetBackup.

You can create an alert policy for a master server, a policy group, or a client group depending on your **Context** pane selection. For example, you can create a policy to alert you when a job fails on a specific NetBackup master server.

You can specify email or SNMP notification in response to an alert, which lets administrators focus on other job responsibilities. Administrators do not need to monitor a terminal continuously.

Alert policies are defined as informational, warning, major, or critical.

Creating alert policies

Review the following notes for specific alert conditions:

- The following alert conditions that pertain to NetBackup catalogs are available to help you identify NetBackup catalog-related issues. The context setting must be **Server Context** to use these conditions. You can specify any of these conditions when you create a NOM alert policy.

NOM alert condition	Description
Catalog Space Low	Alerts you if the space available for catalogs is below the percentage threshold value or size.
Catalog not Backed Up	Alerts you if a catalog backup does not take place during the predefined time period.
Catalog Backup Disabled	Alerts you if the catalog backup is disabled.

You need to provide the required threshold values (if applicable) while creating an alert policy. For Catalog Space low condition, you can specify the threshold value for a particular policy in percentage, bytes, kilobytes (KB), megabytes (MB), gigabytes (GB), terabytes (TB) or petabytes (PB) and generate alerts. The generated alert also shows available catalog space using these units.

You can also specify email and SNMP recipients to receive these alerts.

- The **Job Policy Change** condition raises an alert when a policy attribute for a job policy is changed.

If you select a particular job policy, only the selected job policy is monitored for change. If you do not select any job policy, all the job policies will be monitored for changes.

Only the following policy attributes are monitored for job policies:

Policy name	Policy client type	Storage unit	Volume pool
Checkpoint interval	Check point	Jobs/Policy	Priority
Effective date	Backup network drives	Cross mount points	True image recovery
Compression	Encryption	Allow multiple data streams	Keyword Phrase
Block level incrementals	Offhost	Alternate client	Data mover
Snapshot method	Snapshot arguments	Individual file restore from raw	Status
Master server	Client name	Block increment	Backup copy
Collect bmr info	Collect true image restore info	Data mover type	Disaster recovery
Fail on error	Ext sec info	File list	Follows nfs mounts
Frozen image	Keyword phrase	Max fragmentation size	Max jobs per policy
Number of copies	Off host backup	Pfi enabled	Proxy client
Residence	Catalog	Data classification name	Share group
Schedules	Clients	Policy active	

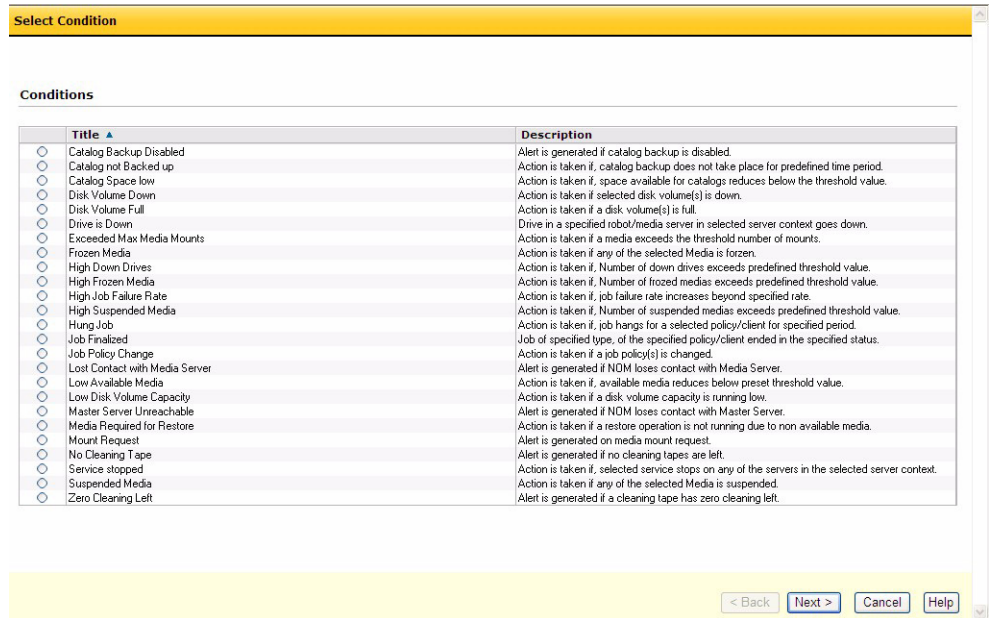
- The **Master Server Unreachable** condition means that the connection between NOM and the managed NetBackup master server is lost. It does not necessarily mean that NetBackup backups are not working.
- The alert policy based on **Disk Volume Full** condition generates an alert only when the used capacity of the disk volume becomes 100%.
An alert policy based on **Disk Volume Full** condition might not generate an alert when a disk group reaches the **High water mark**. This is because the disk volume is not 100% full. The disk group may consist of single disk volume or multiple disk volumes.
- The **Hung Job** condition is checked every 15 minutes. Depending upon when a job starts within a check cycle, an alert *may not* occur.
For example, suppose a policy is created with a job threshold of 25 minutes. A job starts 10 minutes after a first check cycle and ends 13 minutes after a third check cycle is done. This is a total execution of 33 (5 + 15 + 13) minutes, but an alert is not raised.
In this case, the policy is checked four times. The job was not yet started during the first check, was running less than the threshold during the second (job duration = 5 minutes) and third checks (job duration = 20 minutes), and the job completes (job duration = 33) before the fourth check. If a job starts at 4 minutes after a first check, an alert *is* raised at the third check, since the job has executed for 26 minutes (11 + 15 minutes).
- Due to performance and data accuracy reasons, the **Job State Changed** alert policy has been removed from NOM. Alerts are not raised for existing alert policies of this type and do not appear in the console.

To create an alert policy

To create an alert policy, follow the screens of the alert policy wizard.

- 1 From the **Context** pane select a context.
- 2 Select **Managing > Alert Policies > Summary** or **Managing > Alert Policies > Details**.
- 3 From the **Tasks** pane, click **New Alert Policy**.
The first screen of the policy wizard displays the available alert conditions you can select to create an alert policy. You can only select one alert condition for an alert policy.

The set of alert conditions that you can select varies and is dependant upon your current context selection. All alert conditions are available when the context is **Server Context**.



- 4 Select an alert condition for this policy.
 The required information and the required number of screens vary depending on the alert condition your choose. For some alert conditions, you can skip the optional screens.
 For many alert conditions (for example, for the **Job Finalized** condition) you may need to enter threshold parameters and other required or optional parameters. These parameters define and limit the alert.
- 5 Enter a name and description for the alert policy. The name must be unique. Select an alert category from the **Alert severity** drop-down list. (If this alert occurs, the alert is displayed in this alert category in the **Monitoring** view and in the **Alert Summary** pane.)
 Select **Activate the policy** if you want the policy active immediately. You can activate or deactivate the policy later by using the **Activate** tasks or **Deactivate** tasks.
- 6 Click **Save and Next** to continue and view the optional wizard screens. Click **Save and Finish** to skip the optional screens and exit the wizard.

When you select either save option, the alert policy is created. To add email or SNMP recipients later you can select the policy and change it.

- 7 Optionally, you can select email or SNMP recipients (or both) to receive the alert.

The list of registered users (recipients) also contains inactive users, since they might change to active before the alert is generated. If a user is still inactive when the alert is generated, the recipient is removed from the mailing list.

For an active email group the alert notice is emailed to all members of the group. If a user is inactive but is included in an active group, the user receives the alert in the form of email or an SNMP trap.

If you create an alert policy and do not define any recipients, the alert still is displayed in the **Monitoring > Alerts** view.

- 8 Click **Finish** at the end of any optional screens.

Managing your alert policies

You can use the NOM console to browse and display alert policies and also filter policies against various attributes. You can also activate or deactivate alert policies.

See the available online help when managing alert policies for more information about each of these tasks.

To manage an alert policy

- 1 Select **Managing > Alert Policies > Details**.
- 2 Select an alert policy from the table of policies.
- 3 From the **Tasks** pane, click **Copy, Change, Delete, Activate, or Deactivate**.
You can also view any alerts that are currently associated with a particular alert policy.

To add recipients for an alert policy

- 1 Select **Managing > Alert Policies > Details**.
- 2 Click the alert policy link in the **Name** column of the table.
- 3 From the **Tasks** pane, click **Edit Email Recipient** or **Edit Trap Recipient**.
- 4 Select a recipient from the table of recipients.

To remove recipients for an alert policy

- 1 Select **Managing > Alert Policies > Details**.
- 2 Click the alert policy link in the **Name** column of the table.

- 3 From the **Tasks** pane, click **Edit Email Recipient** or **Edit Trap Recipient**.
- 4 Unselect a recipient from the table of recipients.

Setting up the recipients to receive alerts

You can specify the email or SNMP recipients that receive NOM alerts. This feature lets you generate SNMP traps or send emails to inform key personnel of the issue instantly.

An alert notification email contains the following information:

- The alert ID and description
- The time of the alert
- The NetBackup server name and process name
- The NOM alert policy name
- The NOM server name
- The severity level of the alert

To create email or SNMP recipients

- 1 Select **Settings > Recipients > Email** or **Settings > Recipients > SNMP**.
- 2 Click **Create Recipient**.
- 3 Use the dialog box to define the recipient.
See the available online help for more information.

Administering NOM alerts

The **Monitoring** tab of the NOM console provides tools to view and filter alerts, and to track user responses to alerts.

How NOM displays alerts in the console

NOM only displays active alerts (these are alerts that have not been cleared). Some alerts (for example, **Drive is Down**) are cleared automatically when the condition is resolved.

NOM does not normally display any cleared alerts, but you can view cleared alerts from **Monitoring > Alerts > Details** using the **Cleared** filter.

How alerts are removed from the NOM database

You can use the NOMAdmin utility to purge cleared alerts and data collected for jobs from the database. Purged data is *not available* for use in NOM (monitoring, managing, or reporting). Purged job data can also be saved in the NOM database for other usage.

See “[Database maintenance utilities \(NOMAdmin\)](#)” on page 69 for information about the available purge options.

You can also purge active alerts if the modification time for the alert is older than the data retention you specified for the NOMAdmin purge. The modification time is set by an **Acknowledge**, **Add Comment**, or **Assign** task.

See “[Responding to NOM alerts](#)” on page 152.

This means that an active alert with a comment added could be removed before it is cleared. But if another comment is added to the same alert the modification date is changed. The date the alert is removed is now based on a new modification date.

See “[Configuring NOM alert parameters](#)” on page 150.

Configuring NOM alert parameters

You can change the following parameters related to alerts:

System setting	Description
SMTP Server Name	The name of the SMTP server that is used to email reports and alert notifications.
SMTP Server Port	The TCP/IP port number for the SMTP server that is used to email reports and alert notifications.
Sender Email ID	The identifier that is used in the From: field of emailed reports and alert notifications. For example, sender@domain.com. Often the @domain.com portion can be skipped. However depending on your SMTP server configuration, the server may reject emails if the sender ID does not include a valid domain name.

To change an alert parameter

See “[Setting system preferences for the NOM server](#)” on page 177 for more details about these settings.

- 1 Select **Settings > System**.
- 2 Enter new values for any of the system settings in the text boxes.
- 3 Click **Update**.

Viewing NOM alerts

Active alerts appear in the monitoring views for alerts. You can track and manage all user responses to alerts.

To monitor all alerts

- ◆ Select **Monitoring > Alerts > Summary**.

Note: The **License Capacity Alert** is an informational alert. It is internal to NOM and cannot be modified. It appears only in server context and occurs if your storage service capacity has been exceeded. This alert is not generated for the capacity based licenses for OpenStorage Disk option, PureDisk Storage option, and Virtual Tape option.

All capacity values for this alert are calculated based on the definition that 1 terabyte=1,099,511,627,776 bytes.

Understanding alert counts in the monitoring summary views

Alerts apply only to the context where the corresponding alert policy is created. When alerts are raised for that policy they are raised on the selected context view.

For example, you create an alert policy for a selected server group that contains two master servers. For the policy you select an alert of type of **Job State Finalized**. Since a job is related with a master server in the group, the alert is also related with the master server. This master server is present in the group so the alert is listed in the summary for the server as well as the group summary.

But some types of alerts, for example **High Job Failure Rate**, apply across groups. In this case, the alert is raised if the job failure rate for the servers in the selected context is more than a user-defined threshold. Jobs from all of the master servers in the selected group are used to calculate the job failure rate. The alert does not apply to a single master server in the group but applies to the server group on which the alert policy was created. Therefore, the alert is listed only when you select the server group on which alert policy is created (or a parent group of that group).

If you create this type of alert policy for a single managed server, the alert is raised on the server since the server is the selected context. The alert also applies to all the groups that contain the master server.

Following are the NOM alert policy conditions that apply to the selected server context:

- High Down Drives
- High Frozen Media

- High Job Failure Rate
- High Suspended Media
- Low Disk Volume Capacity
- Low Available Media

Note: High Job Failure Rate alert policy condition also applies to client and policy context views.

Also see “[Summary views for NetBackup and NOM categories](#)” on page 167 for more information about viewing the **Group Component Summary** tables.

To obtain a detail view of all alerts

In this view, you can filter on various severity levels or status settings that let you focus on the alerts of interest to you.

- ◆ Select **Monitoring > Alerts > Details**.

Responding to NOM alerts

You can sort and filter the alerts detail view to focus on the specific alerts that are of interest to you.

You can clear or acknowledge an alert, assign it to an individual, or add comments to it. This allows multiple users to process or take action on an alert. Under certain circumstances there may be issues among multiple NOM users. For instance, a NOM user comments on an alert while another NOM user tries to clear the same alert.

You can also edit the related policy for an alert.

To handle an alert

The NOM console displays active alerts. When you acknowledge an alert, you inform other users who see the alert that action on the alert occurred.

If you clear an alert, you cannot perform any further activity on the alert (for example, assign or acknowledge). Cleared alerts no longer appear in the NOM alert views. You can also remove cleared alerts from the database based on your NOMAdmin purge data retention setting.

- 1 Select **Monitoring > Alerts > Details**.
- 2 Select an alert from the table.
- 3 From the **Tasks** pane, click **Acknowledge**, **Clear**, **Add Comment**, **Edit Policy**, or **Assign**.

See the available online help when monitoring alert details for more information about each of these tasks.

Using SNMP with NOM

This section contains the following SNMP topics:

- [“About SNMP”](#) on page 153.
- [“SNMP versions”](#) on page 153.
- [“SNMP version supported in NOM”](#) on page 154.
- [“The Management Information Base \(MIB\) and NOM support”](#) on page 154.
- [“Process of generating SNMP traps in NOM using VxAM”](#) on page 154.
- [“Frequently asked SNMP questions”](#) on page 155.

About SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP is based on the manager and agent model consisting of a manager, an agent, a database of management information, managed objects, and the network protocol.

The manager provides the interface between the human network manager and the management system. The agent provides the interface between the manager and the physical devices being managed.

The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. The MIB is organized in a tree structure with individual variables, such as point status or description, being represented as leaves on the branches. A numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

SNMP versions

The versions of SNMP protocol are as follows:

- SNMPv1

This is the first and standard version of the protocol and is defined by RFC 1157. This document replaces the earlier versions that were published as RFC 1067 and RFC 1098. Security is based on community strings.

- **SNMPv2**

It was created as an update of SNMPv1 adding several features. The key enhancements to SNMPv2 are focused on the SMI, manager-to-manager capability and protocol operations.

SNMPv2c combines the community-based approach of SNMPv1 with the protocol operation of SNMPv2 and omits all SNMPv2 security features.

There are four different SNMPv2 variants:

- The original SNMPv2 (SNMPv2p)
- Community-based SNMPv2 (SNMPv2c)
- User-based SNMPv2 (SNMPv2u)
- SNMPv2 star (SNMPv2*).

- **SNMPv3**

This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p, and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*. It is defined by RFC 1905, RFC 1906, RFC 2261, RFC 2262, RFC 2263, RFC 2264, and RFC 2265.

SNMP version supported in NOM

The default version of SNMP supported in NOM is SNMPv2c. NOM users cannot configure this default version of SNMP.

The Management Information Base (MIB) and NOM support

Each SNMP element manages specific objects with each object having specific characteristics. Each object and characteristic has a unique object identifier (OID) consisting of numbers separated by decimal points (for example, 1.3.6.1.4.1.2682.1).

These OIDs form a tree. The MIB associates each OID with a readable label and various other parameters related to the object. The MIB then serves as a data dictionary that is used to assemble and interpret SNMP messages.

Process of generating SNMP traps in NOM using VxAM

The NOM server can create alert policies and generate alerts based on alert conditions. NOM uses VxAM component to send notifications for the generated alerts in the form of SMTP and SNMP traps.

The SNMP configuration is provided by NOM and it is stored in the VxAM database table. On the startup of the NOM server, the MIB supported by NOM is loaded by VxAM in its own database.

When defining an alert policy, NOM associates an SNMP configuration with alert policy. Whenever an alert policy is created in NOM a corresponding policy is also created in VxAM. The VxAM policy understands different notification actions (traps, Email, and so on) associated with the policy. When an alert is generated the corresponding notification action is automatically executed by VxAM.

Note: The community name string defined for NOM in VxAM is NOM. Currently this string cannot be edited.

Frequently asked SNMP questions

What is the default version of SNMP that is supported in NOM?

SNMPv2c.

Can the version be configured by the user?

No, you cannot configure the SNMP version.

What is SNMPv2c? How it is different from SNMPv2?

See “[SNMP versions](#)” on page 153.

Is the NOM SNMP community name configurable?

No, but there are plans to make it configurable in a future release.

How is the NOM community related to the public community?

Is the default community name of “NOM” just a name for the community, but still considered public because of certain attributes?

Generally, the “default read community string” for the public community is “public”. Public community means read-only access to SNMP traps.

The “NOM” community used by NOM is public, but the community name is maintained as “NOM”.

How do I find information on creating and using SNMP alert policies in NOM?

Start the NOM console and click the **Help** link. Use the TOC on the left to view the topic **Understanding NOM alert policies and alerts**, or use the **Creating alert polices** or **Managing your alert policies** quick links displayed on the right.

Troubleshooting NetBackup issues using NOM

NetBackup Operations Manager provides several features and capabilities to help troubleshoot NetBackup system issues. Some of these features are:

- Log file management, which includes the following tasks:
 - Export and filter log files from jobs, services, and master servers.
 - Enable and disable log files from the NOM console.
 - Trace the progress of a job.
 - Filter logs based on a single failure in NetBackup.
- NOM alert policies to detect when something is not normal in your backup environment, and to anticipate and handle problems before they occur. See [“Understanding NOM alert policies and alerts”](#) on page 143 for overview information on how to set up alert policies and how to respond to any resulting alerts.
- NetBackup reports and alert conditions that you can use. See NOM online help for more details about running reports and alert conditions.

This section contains the following NetBackup troubleshooting topics:

Topic	Description
“NetBackup master and media server log files” on page 158	Describes how to export and manage server log messages to troubleshoot NetBackup.

Topic	Description
“NetBackup jobs” on page 160	Describes how to use NOM to troubleshoot jobs, which includes how to control jobs and view job policy information.
“NetBackup services” on page 162	Describes how to control services.

NetBackup master and media server log files

NetBackup log files exist in many formats and in many locations. You can disable or enable these logs and set the retention period and verbosity to any level that NetBackup allows. You can export and filter master server or media server logs.

All these tasks are available from the following views when a master server is selected:

- **Monitoring > Master Servers > List Log Files**
- **Settings > Groups > List Log Files**
- **Monitoring > Jobs > Details** (Click the drilldown link from **Master Server** column) > **List Log Files**
- **Managing > Job Policies > Details** (Click the drilldown link from **Master Server** column) > **List Log Files**.

Exporting and filtering log messages for a master server

You can select process, job, and service or daemon debug log files from different servers and export them in an Excel format. You can also filter these log messages before exporting them.

To export and filter NetBackup log file

- 1 From the **Context** pane select **Server Context**.
- 2 Select **Monitoring > Master Servers > Details**.
- 3 Select a master server from the table.
- 4 From the **Master Server Tasks** pane, click **List Log Files**.
- 5 Select **Master Server Logs** or **Media Server Logs**.
- 6 Select a log file from the table. You can export only one log source at a time.
- 7 From the **Select a Task** drop-down list, select **Export Log Messages**. A dialog box appears where you can specify the filter criteria.

- 8 Select one of the following to filter the number of log messages to be displayed:
 - **Messages from the last** and select a number of hours or days.
 - **Messages between** and use the calendar icons to select a date and time for the message pane.
 You cannot give a time range which is greater than 3 days or 72 hours in the dialog box. This is because at a given point in time, log messages can be collected for a maximum period of 3 days.
 - You can also enter an expression in the **Regular Expression (Perl Compatible)** field to search for specific text and limit the number of messages. The expression must be a Perl Compatible Regular Expression (PCRE) and not a simple search string.
- 9 Click **Export Log Messages**. Click **Open** or **Save** from the dialog box that appears to open or save the log messages in an Excel format.

Note: You can also export the NetBackup `error_log` file using the same procedure. This file is present in the **Master Server Logs** tab.

Controlling NetBackup log file creation

You can control the creation of individual NetBackup, volume manager, or VxUL log files. Any log file settings you make from this view are local and override the global settings for the server.

You can set retention levels and the verbosity levels for most NetBackup logs.

To control the creation of selected NetBackup log messages

- 1 From the **Context** pane select **Server Context**.
- 2 Select **Monitoring > Master Servers > Details**.
- 3 Select a master server from the table.
- 4 From the **Master Server Tasks** pane, click **List Log Files**.
- 5 Select **Master Server Logs** or **Media Server Logs**.
- 6 Select a log source(s) from the table.
- 7 From the **Select a Task** drop-down list, select **Enable Logs** or **Disable Logs**.
- 8 Accept the warning messages to enable or disable the log files. You need to restart all Netbackup services on the server after enabling or disabling the log files.

Configuring log file verbosity settings and retention period

You can set the retention period or verbosity levels for NetBackup, volume manager, or VxUL log file categories for the server you select. These levels apply to all log files for this selection. You can apply these settings to all log sources by selecting **Apply Verbosity Settings to all log sources** from the Configure Log Settings dialog box.

The verbosity setting for NetBackup volume manager logs is either Minimal or Maximal (these logs do not support multiple verbosity levels like NetBackup and VxUL logs).

- 1 From the **Context** pane select **Server Context**.
- 2 Select **Monitoring > Master Servers > Details**.
- 3 Select a master server from the table.
- 4 From the **Master Server Tasks** pane, click **List Log Files**.
- 5 Select **Master Server Logs** or **Media Server Logs**.
- 6 From the **Tasks** pane, select **Configure Log Settings**.
- 7 From the **NetBackup Default Verbosity Level** drop-down list, select a verbosity level.
From the **Volume Manager Default Verbosity Level** drop-down list, select a verbosity level.
From the **Vxul Default Verbosity Level** drop-down list, select a verbosity level.
- 8 Select **Apply Verbosity Settings to all log sources** to apply your settings to all log files of a particular type.

Note: If you do not select this checkbox and change verbosity level and retention period settings from the Configure Log Settings dialog box, then only log files with default settings for verbosity level and retention period will change.

- 9 Specify a retention period for all logs in days.
- 10 Click **OK** to configure the selected log settings.

NetBackup jobs

NOM provides centralized viewing and management of NetBackup jobs.

Controlling jobs

To control a job

- 1 Select **Monitoring > Jobs > Details**.
- 2 Select a job(s) from the table.
- 3 Click **Cancel**, **Suspend**, **Resume**, or **Restart** from the **Tasks** pane.

To export job logs

Note: Log files for all job types are not available. Before exporting a log file, ensure that the NetBackup master server is online and the selected job logs are enabled.

- 1 Select **Monitoring > Jobs > Details**.
- 2 Select a job from the table.
- 3 Click **Export Job Logs** from the **Tasks** pane.
- 4 Click **Open** or **Save** from the dialog box to open or save the log messages in an Excel format.

Handling job failures

To identify failed jobs

You can locate failed jobs by applying filters to the table of jobs. You can also create custom filters to locate a more specific failed job. For example, a particular job type that failed.

- 1 Select **Monitoring > Jobs > Details**.
- 2 From the filter drop-down list, select **Failed Jobs** (or use a custom filter).
- 3 Click the check mark icon to filter the view.

To view troubleshooting information for the completion status of a particular job

This view provides descriptions of all NetBackup job status codes and helpful recommended actions to resolve any issues. These topics are from the NetBackup Troubleshooting Guide. Some of the status codes contain links to support tech notes that contain more information.

- 1 Select **Monitoring > Jobs > Details**.
- 2 Click the status code (link) for the job in the **Status** column of the table.

Viewing job policy information for a job

To view policy information for a particular job

- 1 Select **Monitoring > Jobs > Details**.
- 2 Click the policy name (link) for the job in the **Policy** column of the table.

To view and compare any revisions to a job policy

- 1 Select **Monitoring > Jobs > Details**.
- 2 Click the policy name (link) for the job in the **Policy** column of the table.
- 3 Select the **History** tab.
- 4 Using the time parameters, select the revisions to this policy that you want to view.
- 5 Select **Compare Selected Versions** to list all changes to the policy.
Select **Diff Selected Versions** to list only the differences in the policies.
- 6 Click **Go** to display a table that shows the changes to the policy.

Viewing master server information for a job

From these views you can configure a master server and also view information for associated media servers and clients.

To view master server information for a job

- 1 Select **Monitoring > Jobs > Details**.
- 2 Click the server name (drilldown link) for the job in the **Master Server** column of the table.

NetBackup services

NOM provides tools to control NetBackup services.

Controlling NetBackup services

If you start or stop a service that has a dependency on another service, NetBackup ensures that any dependent services are also started or stopped.

You cannot control the following services from NOM:

- NetBackup service layer (nbsl)
- NetBackup Event Manager (NBEvtMgr)
- Enterprise media manager (nbemm)

- NetBackup service monitor (nbsvcmon)
- NetBackup client service (bpinetd)
- Adaptive Server Anywhere - VERITAS_NB (dbsrv9)

To control a service

- 1 Select **Monitoring > Services > Details**.
- 2 Select a service(s) from the table.
- 3 Click **Start, Stop, or Restart**.
Starting, Stopping, or Restarting appear in the **Status** column until the action completes.

To export service logs

Before exporting the log file, ensure that the NetBackup master server is online and the selected service logs are enabled.

- 1 Select **Monitoring > Services > Details**.
- 2 Select a service from the table.
- 3 Click **Export Service Logs**. Click **Open** or **Save** from the dialog box to open or save the log messages in an Excel format.

NOM monitoring, managing, and configuration topics

For information on understanding and using the various NOM monitoring, managing, and reporting views and their related tasks, refer to the online help when using NOM.

The online help provided for the various NOM console views provides a description of the view, instructions for navigating within the view and starting the tasks related to the view. In many cases, links are provided at the end of the help topic to helpful related topics.

Context-sensitive help is available for all console views, task dialogs, and wizard task screens. The online help also provides information about each standard reports.

See [“Using help to understand NOM views and tasks”](#) on page 130 for a list of common tasks you may be interested in.

This chapter contains information about key NOM console topics.

Topic	Description
“Understanding monitoring and managing group component summaries” on page 166	This topic clarifies some anomalies in the group components displayed for NOM monitoring and managing views.
“Understanding NBSL monitors and the Partially Online server status” on page 170.	This topic describes the NBSL monitors used by NOM and the partially online status for managed servers.
“Configuring user preferences and system settings” on page 172	This topic describes the user and system preferences that can be changed for NOM.

Understanding monitoring and managing group component summaries

This section clarifies some anomalies that you may see when group components are displayed for NOM monitoring and managing views. This section contains the following topics:

- [“Overview summary and overview detail tabs”](#) on page 166
- [“Summary views for NetBackup and NOM categories”](#) on page 167

Overview summary and overview detail tabs

NOM provides overview summaries and overview detail views for the monitoring and managing tabs. These views are available for **Sever Context**, **Client Context**, or **Policy Context**.

For example, see **Monitoring > Overview > Summary** or **Managing > Overview > Details**.

Understanding the table in the overview details tab

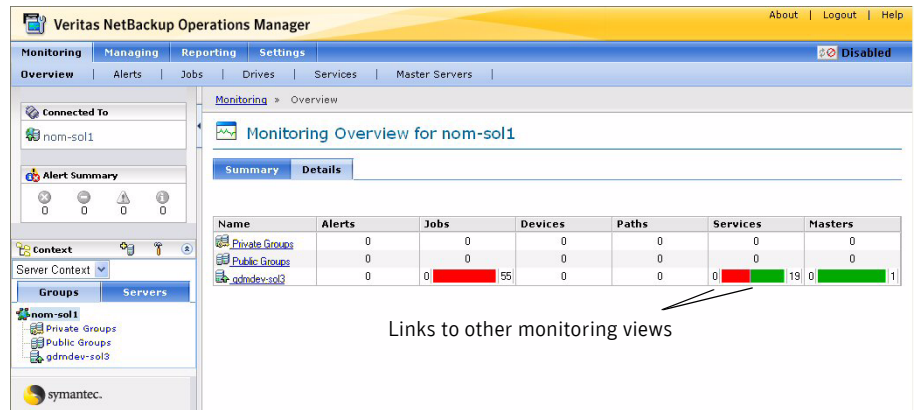
The object categories (such as NOM alerts and NetBackup jobs for the **Monitoring** tab) shown in these views are the same categories as those in the overview **Summary** tab. The difference in using the **Details** tab is that NOM organizes the data by the context group selected.

To view monitoring or managing overview details

- ◆ Select **Monitoring > Overview > Details** or **Managing > Overview > Details**.

Note: The **Details** tab is not available for **Client Context** or **Policy Context** when the bottommost group within a parent client or policy group is selected.

The following figure shows a sample monitoring overview details view (using **Server Context**). The views displayed for the **Managing** tab are similar.



The table in this view contains a row for each server group or server that is included in the current selection in the **Context** pane.

The table shown is empty when the selected group contains no subgroups or individual servers.

Summary views for NetBackup and NOM categories

The monitoring and managing summary views are always based on the context that you select in the **Context** pane. The summary views also include links to filtered detail views.

Note: The examples in this section refer to the **Monitoring > Alerts > Summary** view. Other summary views are similar when viewing other monitoring categories (such as, jobs, drives, or master servers) and also when viewing other categories using the **Managing** tab.

To display the summary views for a category in monitoring or managing

- ◆ Select a monitoring or managing subtab.
 For example, select **Monitoring > Alerts > Summary** or **Managing > Job Policies > Summary**.

The summary view for an empty group component or a single server

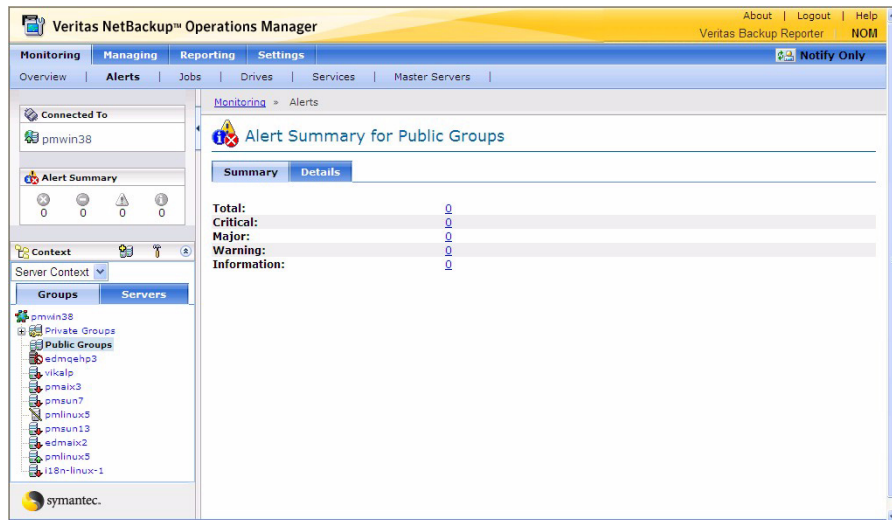
The following figure shows an example of the summary view for monitoring NOM alerts when you select any of the following:

- A component of a group that does not contain any subgroups.
- A component of a server group that does not contain any managed servers.
- A single managed server.

Note: The view for a single managed server may or may not show data. This depends on whether alert policies have been created for the server or not.

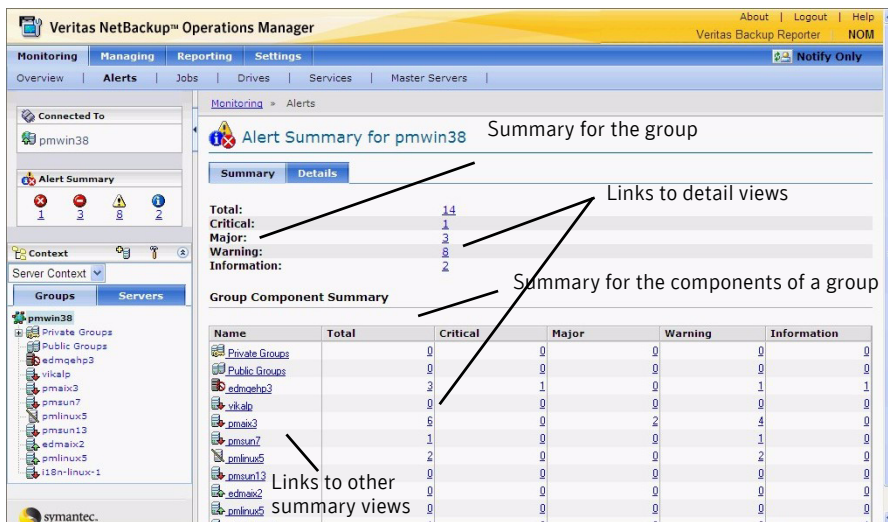
The top of this view includes summary information for the item selected in the **Context** pane.

In this case, the **Group Component Summary** table is not shown.



The summary view for a group containing components

The following figure is an example of the summary view when you select a group that contains components.



The top of this view includes summary information for the group selected in the **Context** pane. The view also includes a **Group Component Summary** table that shows information for the components included in the group.

Understanding the group component summary table

A group can contain two subgroups that have same set of members. In this case there are rows in the **Group Component Summary** for each subgroup. The summaries shown in the two rows are identical since the groups are identical.

Summing the rows in the **Group Component Summary** may not match the counts in the summary information for the group. This case occurs if the group contains subgroups with common members.

Summing the rows in the **Group Component Summary** *does* match the summary information if subgroups do not contain any common members and there are no context-level alerts for the selected context.

Also see “[Understanding alert counts in the monitoring summary views](#)” on page 151 for information regarding the special cases when monitoring NOM alerts.

Understanding NBSL monitors and the Partially Online server status

This section includes the following NBSL and partially online server topics:

- “[NBSL \(NetBackup Service Layer\) monitors](#)” on page 170
- “[Partially Online managed server status in the context pane](#)” on page 172

NBSL (NetBackup Service Layer) monitors

NOM uses 15 NBSL monitors. These monitors are communication channels between your managed NetBackup masters and NOM and function independently of one another.

Note: These monitors do not represent corresponding monitors in NetBackup.

For most operations and changes in NetBackup, the NBSL monitors send events to NOM. For changes such as job, policy, services, and devices the event also contains the changed data. This data is stored in the NOM database.

If all of the NBSL monitors are up, the server is in the **Online** state. If all are down, the state is **Offline**.

If some monitors are up and some are down, the state is **Partially Online**. This status usually means that one of them may currently be down and is considered normal.

A monitor can get disconnected and then reconnected after some time. This is also normal behavior. If a monitor gets disconnected, it should be automatically connected again within 10 minutes. All the functionality other than the functionality of the disconnected monitor can be used normally while a monitor is disconnected.

NOM uses the following NBSL monitors:

Disk	Drive	Job	Log
Media	Policy	Robot	Service
StorageUnit Group	Storage Unit	Volume Group	Volume Pool
FT	Storage Service	Licensing	

To view the details for a master server and view NBSL monitor status

- 1 Select **Monitoring > Master Servers**.
- 2 Select a master server from the **Context** pane.

Note: The master server view is also available when you select a master server from the **Context** pane and then click the hammer icon. This view is also available from the **Managing** and **Settings** tabs.

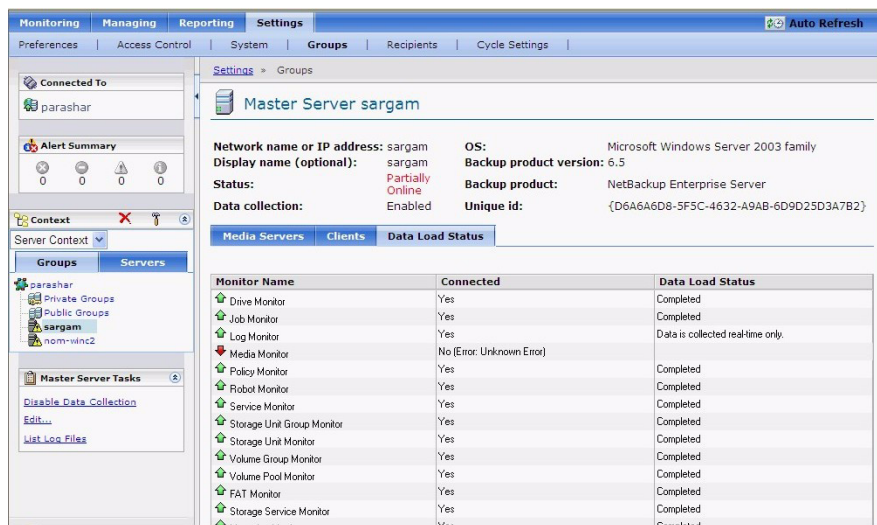
Configuration information that was entered when the master server was added to NOM appears at the top of this view. The **Status** field for the server may contain **Partially Online**.

Also included in this view are subtabs for the **Media Servers**, **Clients**, and **Data Load Status** that are associated with this master server.

To view information for the NOM server connections to NBSL for this master server

- 1 Select **Monitoring > Master Servers**.
- 2 Select a master server from the **Context** pane.
- 3 Select the **Data Load Status** tab.

This view provides the connection and the data load status for each of the NBSL monitors used by NOM. The following figure shows a sample data load view for a master server.



The following table describes the contents of this view:

Column	Description
Monitor name	The name of a monitor used by NOM. A red or green icon provides status of the monitor connection at a glance.
Connected	This column provides the connection status for each monitor. If the connection status is not yes, information about the error is provided.
Data Load Status	This column provides the status of each data load activity requested by NOM.

Partially Online managed server status in the context pane

The NOM console **Context** pane can also indicate a partially online server status. In this case, a NetBackup master server that is partially online is shown with a yellow caution icon. This status means that one or more of the NBSL monitors are down. NOM tries to reconnect to the disconnected monitor.

Configuring user preferences and system settings

This section includes the following configuration topics:

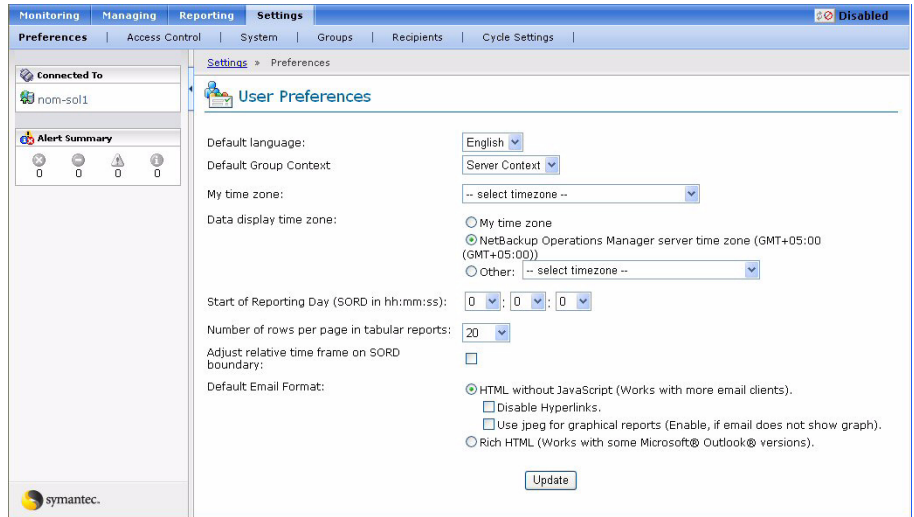
- [“Setting preferences for NOM users”](#) on page 173
- [“Setting system preferences for the NOM server”](#) on page 177

The **Settings** tab in the console also contains these additional configuration tasks. See the online help available for these views for more information.

- Managing access control for users
- Managing context groups
- Managing Email and SNMP recipients
- Managing reporting cycles for NOM standard reports

Setting preferences for NOM users

When you select **Settings > Preferences**, the following view appears. These preferences are valid only for the user who is currently logged into NOM. Each NOM user can have unique preferences.



The following user preferences can be changed:

Preference Setting	Description
Default language	The default display language that the NOM console uses. If a default is not set, the language of the Web browser (or English) is used.
Default group context	The default group context that the NOM console uses. The new default is used when you next log into the console. The default context is applicable until changed again. If a default is not set, server context is used.
My time zone	The time zone where the NOM Web application (the NOM console) is running. So if you are using a laptop computer and travelling, you can set the time zone to that location or set it to your home time zone.
Data display time zone	The time zone that is used to generate and display NOM data views and reports.

Preference Setting	Description
Start of Reporting Day (SORD)	The start time that is used to display the date and time in graphical reports. For example, a job runs Jan 1st at 07:00:00 and the SORD is set to 8:00:00. The run date for the job displays Dec. 31st since the reporting day has not started. The default start time for a reporting day is 00:00:00.
Number of rows per page in tabular reports	You can set the default page size for table reports.
Adjust relative time frame on SORD boundary	If this checkbox is selected, the relative time frame is adjusted on the SORD boundary and the end time of the time frame is set to the future SORD time. The default setting is not selected.
Default Email format	The default HTML format for NOM reports that are to be emailed.

To specify a default language setting for the NOM console

- 1 Select a language from the drop-down list.
- 2 Click **Update**.

To specify a default context setting for the NOM console

- 1 Select a context from the drop-down list.
Contexts can be **Server Context**, **Client Context**, or **Policy Context**.
- 2 Click **Update**.

To specify the time zone where you are running the NOM console

This setting lets you specify the time zone of the location where you are running the NOM console (from a Web browser).

See [“How does NOM handle different time zones when it generates reports?”](#) on page 189 for more information.

- 1 Select a value from the drop-down list.
- 2 Click **Update**.

To specify the time zone for the data that the NOM console displays

The **Data display time zone** setting is used to specify the time zone used when you display NOM data views and reports.

The **Master server time zone** option is removed from the **Data display time zone** preferences. As a result, if your managed master servers are located in different

time zones, then you can no longer view the data for both managed servers in their respective time zone at one time. You still can view the data in the specified display time zone.

- 1 Select a time zone option.
- 2 If you select **Other**, select a time zone from the drop-down list.
- 3 Click **Update**.

How is the start of the reporting day (SORD) used in NOM?

A NOM reporting day is defined as 24 hours. The start of the reporting day setting lets you specify the time when a NOM reporting day starts and therefore define your reporting day boundaries.

NOM uses the SORD to determine what day a job ran and is used only for reports. For example, the SORD is set to 09:00:00 and the current date is February 10. The reporting day starts February 10 at 9:00 A.M. and ends February 11 at 9:00 A.M. NOM considers all NetBackup data that is collected between February 10 at 9:00 A.M. and February 11 at 9:00 A.M. to be data for February 10.

Also see [“How is the Adjust relative time frame on SORD boundary setting used?”](#) on page 175.

To specify the start of your reporting day

Each user of NOM can have a different SORD. You can set this time to be different from the default start time of 00:00:00.

- 1 Select a start time (hh:mm:ss) from the drop-down list boxes.
- 2 Click **Update**.

To specify the default number of rows to display per page

This setting only applies to table format reports.

- 1 Select a number from the drop-down list.
- 2 Click **Update**.

How is the Adjust relative time frame on SORD boundary setting used?

If the **Adjust relative time frame on SORD boundary** checkbox is selected, the relative time frame is adjusted on the SORD boundary and the end time of the time frame is set to the future SORD time.

For example, it is 10:00 PM on 10 Jan and you run a report specifying a relative time frame of back 24 hours and the SORD is set to 8:00AM. Selecting this

checkbox sets the end time to 11 Jan 8:00AM to align with the SORD and sets the start time to 24 hours back from the end time or 10 Jan 8:00AM.

If the checkbox is not selected, the relative time frame is relative to the current time. So in the example, the current time is 10:00 PM on 10 Jan and the time frame is set 24 hours back. The resulting time frame is 9 Jan 10:00 PM to 10 Jan 10:00 PM.

The scheduled report saves this setting when the schedule is defined and instead of using the current time it uses the schedule time to calculate the time frame.

By default this checkbox is not selected. NOM releases before the 6.0 MP4 release adjust the time frame on the SORD boundary. So any report schedules created before the 6.0 MP4 release adjust the time frame on the SORD boundary. If you want the time frame for your report schedules not to be adjusted on the SORD boundary, select the checkbox, edit, and save the schedule.

Also see “[How is the start of the reporting day \(SORD\) used in NOM?](#)” on page 175.

To adjust the relative time frame for reports and use the SORD setting

- 1 Select the **Adjust relative time frame on SORD boundary** checkbox. By default this checkbox is not selected.
- 2 Click **Update**.

To specify the default HTML format for emailed reports

This setting lets you specify the default format for NOM reports that are emailed. Format options can also be changed before emailing a report using the schedule wizard or the email report screen.

If you select **HTML without JavaScript**, reports are emailed without embedded JavaScript. This format avoids some error messages if the email client does not support JavaScript. The Lotus Notes client and Mozilla based clients require this format. This is the default format.

This format also allows the following additional options. Selecting either of these additional options is not required.

- **Disable hyperlinks**
Hides all hyperlinks in a report. This option can be used if you want to email a report only for presentation.
- **Use jpeg for graphical reports**
Graphical reports are emailed in jpeg email format. This option must be selected if you want to use Lotus notes or Mozilla based email clients. If you do not select this option, graphical reports are generated in png image format. png format is not suitable for Lotus Notes.

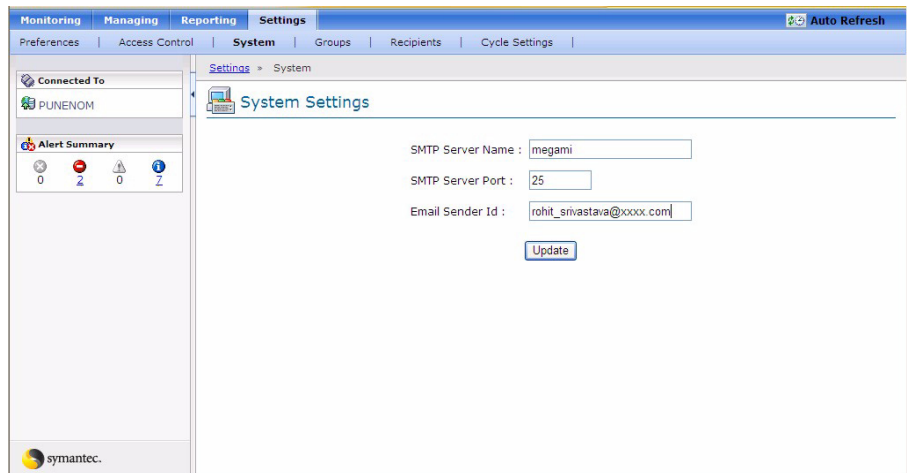
Microsoft Outlook users should not select this option for higher image quality.

If you select **Rich HTML**, reports are emailed with JavaScript embedded. This preserves tooltips in the reports. Note that tool tips only work on some versions of Microsoft Outlook.

- 1 Select one of the default formats.
 If you select **HTML without JavaScript** you can also select additional options. Selecting either of these additional options is not required.
- 2 Click **Update**.

Setting system preferences for the NOM server

When you select **Settings > System**, the following view appears, which shows the currently configured system settings for the NOM server.



The following settings can be changed.:

System Setting	Description
SMTP Server Name	The name of the SMTP server that is used to email reports and alert notifications.
SMTP Server Port	The TCP/IP port number for the SMTP server that is used to email reports and alert notifications.

System Setting	Description
Sender Email ID	The identifier that is used in the From: field of emailed reports and alert notifications. For example, sender@domain.com. Often the @domain.com portion can be skipped. However depending on your SMTP server configuration, the server may reject emails if the sender ID does not include a valid domain name.

To change a system setting

- 1 Enter new values for any of the system settings in the text boxes.
- 2 Click **Update**.

NOM reporting topics

This chapter contains additional information about understanding and using NOM reports and the report wizards.

Topic	Description
“Understanding NOM report capabilities” on page 179	This topic provides an overview of NOM reporting.
“Running a report” on page 187	This topic describes running NOM reports with and without runtime parameters.
“Performing tasks to manage your reports” on page 191	This topic contains a table that explains when the various NOM report tasks can be used. Also explained is email formatting options for NOM reports.
“Using the report builder wizard” on page 194	This topic describes the wizard screens, SQL basics, and shows how to build some sample custom reports.
“Using the composite report builder wizard” on page 220	This topic describes the wizard screens used to create composite custom reports.
“Using the report scheduler wizard” on page 223.	This topic describes the required and optional wizard screens used to schedule custom or standard reports.
“Upgrading reports from 6.0 or 6.0MPx to 6.5” on page 226	This topic lists the standard reports that have been deprecated and replaced with new reports in NOM 6.5. It also explains how you can migrate the old deprecated reports to the new NOM 6.5 reports.

Understanding NOM report capabilities

You can use NOM to generate detailed reports for your backup environment.

From the **Reporting** tab and its subtabs, you can access a variety of reports that contain detailed information about your backup environment. This information includes NetBackup jobs, devices, and policies. Many tasks are also available for managing reports. For example, you can schedule, customize, print, or email these reports.

Why use NOM reports?

With NOM reports, you do not have to search through the numerous text files that make up NetBackup job logs. NOM reports present the data you want to see in intuitive formats.

NOM standard reports are designed to simplify how you monitor and report on your NetBackup servers. You can diagnose the status of NetBackup operations by using reports on jobs, media and devices, policies, and clients.

Standard reports let you identify problems and potential problem areas quickly. They also provide a data summary and a way to analyze that data to get an overview of the health of your NetBackup environment.

Since NOM builds reports dynamically at the time you request a report, your report presents a current view of your environment. NOM collects data and produces reports from any NetBackup master servers (or server groups) that you are currently managing. These reports provide a global perspective on your backup environments.

Using NOM reports lets you gain perspective on the health of multiple NetBackup servers and to answer important questions like the following:

- Which master server has the most problems with its backup jobs?
- Which master servers back up the most data?
- Which storage units are likely to need to recycle their media soon?

Quickly view the reports you need

You can access the reports you want quickly by using the **Reporting > My Portal** view. You can customize this view and choose your favorite reports as a starting point. You can include private reports, public reports, or standard reports. See [“Accessing all NOM reports”](#) on page 181 to know about private reports, public reports, and standard reports.

Each NOM user can create a unique portal view that provides current, at-a-glance health assessment of NetBackup operations.

The maximum number of reports that can be added to the **My Portal** reporting tab is five. This report limit is required because some browsers have performance issues (for example, Netscape and Firefox).

Accessing all NOM reports

You can access all available NOM reports easily by using the **Reporting > All Reports** view. The subtabs in this view provide quick access to private, public, and standard reports.

You also use the all reports view for most report tasks, such as copying a report. See [“Performing tasks to manage your reports”](#) on page 191.

Also see [“Using help to understand NOM views and tasks”](#) on page 130 for a list of common reporting tasks you may be interested in.

Private Reports

The **Private Reports** subtab contains any custom reports that you create or any report that you copy here. When you create a new custom report, it is placed in **Private Reports** by default. Only the creator (owner) of these reports can use and manage them.

Public Reports

The **Public Reports** tab contains any custom reports that can be shared with all NOM users.

To place a report in **Public Reports** do either of the following:

- Copy any report, private, public or standard, and select **Public** as the destination folder.
- Create a shortcut for any private report (the shortcut is placed in **Public Reports** by default).

A public report can only be modified by the user who copied it to the public folder. If you do not own a public report and you want to edit it you can copy it to your private area or public area.

A private report can be copied to **Public Reports**. It is then available to all users.

Standard Reports

You can easily integrate NOM built-in standard reports into your business practices. Standard reports are predefined reports and cannot be modified. However, you can copy most standard reports to **Public Reports** or **Private Reports** area and then make changes. Some standard reports cannot be copied.

Standard reports help you analyze and improve your NetBackup environment by presenting NetBackup data as follows:

- They provide detailed operational views. Reports show whether daily backups perform successfully and where the problems are with unsuccessful backups.

- You can review NetBackup activities quickly without the need to cull information from error logs, which makes you more effective and responsive to users' needs.
- They provide valid performance indicators, such as data throughput.
- They provide useful, auditable data (the same data that appears in the NetBackup console).

The online help in the NOM console provides information, such as report format, run time parameters, default reporting period, and notes for each NOM standard report.

To learn more about each standard report

- ◆ Click **Reporting > All Reports > Standard Reports > Help**.
From the table shown in the help, click on the report you are interested in.

Icons used in job related standard reports













The following table contains a list of icons used to describe the various job types and the job status. These icons are used in the following standard reports:











- Rolling 8 day Summary
- Rolling 8 day Summary by Media Server
- Week at a glance
- Job Summary by Client
- Job Summary by Client for master server
- Job Summary by Client for media server

The remaining job related standard reports use the icons for Backup job type only.

Note: If your managed servers are on NetBackup 6.5, both custom and standard reports will only show jobs whose job state is Done in NetBackup. This applies to all reports which show job-related data.

Job Types	Job Status	Icon shown
Backup	Successful	
	Partially Successful	
	Failed	
Archive	Successful	
	Partially Successful	
	Failed	
Verify	Successful	
	Partially Successful	
	Failed	
Restore	Successful	
	Partially Successful	
	Failed	

Job Types	Job Status	Icon shown
Duplicate	Successful	
	Partially Successful	
	Failed	
DBBackup	Successful	
	Partially Successful	
	Failed	
Vault	Successful	
	Partially Successful	
	Failed	
Erase	Successful	
	Partially Successful	
	Failed	

Job Types	Job Status	Icon shown
Import	Successful	
	Partially Successful	
	Failed	
Image cleanup, Live Update, DB Recover, Generic, Tape formatting, Media contents, Cleaning, Tape request, Inventory, DQTS, Undefined	Successful	
	Partially Successful	
	Failed	
Label	Successful	
	Partially Successful	
	Failed	
None of the above job types		

Scheduling reports to run when you need them

You can schedule when you want custom or standard reports to run. You can schedule reports in a variety of ways.

Report schedules follow user access control. This means that a schedule will only be visible to the user who created it. Other users cannot see this schedule.

See [“Using the report scheduler wizard”](#) on page 223.

Managing the schedule for a report

To manage any reports that you have scheduled, use the **Reporting > Scheduled Reports** view. The tasks in this view allow you to edit or delete a schedule. You

can also select a schedule to view the details of this schedule and the scheduled report that it is associated with.

Creating the reports you need

NOM provides a number of preconfigured standard NetBackup reports. This standard set meets common requirements for NetBackup reporting, however you may require a more specific view of the data based on your unique reporting needs.

When you create custom reports, NOM provides several database views that you can use as a starting point for your report. You can also use run time parameters to create and filter the data for unique reports.

To create a custom report

- 1 Select **Reporting > All Reports**.
- 2 From the **Tasks** pane, click **New Report**.
See “[Using the report builder wizard](#)” on page 194 for more details.

To create a composite report from existing reports

- 1 Select **Reporting > All Reports**.
- 2 From the **Tasks** pane, click **New Composite Report**.
See “[Using the composite report builder wizard](#)” on page 220 for more details.

Managing reports

You also use the all reports view (**Reporting > All Reports**) for most report tasks such as copying a report.

See “[Performing tasks to manage your reports](#)” on page 191.

Also see “[Using help to understand NOM views and tasks](#)” on page 130 for a list of common reporting tasks you may be interested in.

Using online help to obtain more information about reporting

For detailed information on understanding and using the NOM reporting views and reporting tasks, always refer to the NOM online help.

The online help provided for the various NOM console views provides a description of the view, instructions for navigating within the view and starting the tasks related to the view.

Context-sensitive help is available for all console views, task dialogs, and wizard task screens. The online help also provides information about each standard report.

Running a report

If you define a report with any run time parameters, before you run the report you must supply these parameters.

If the report definition includes	Then
A server	The Context pane is available.
A time filter	The Time Frame pane and its functions are available.
A filter for a NetBackup object	Parameter selection drop-down list boxes are available in the report.

To run and view a report

Each report in the **Reporting** views contains a link to report. Click the link to run and view the report.

Some reports require that you specify run time filters first before they are run. See [“Running a report with run time parameters”](#) on page 188.

Reports can be rerun after modifying the run time parameters. This allows flexibility and lets you see the reports you need.

The following figure shows a sample report and the report tasks that are available after you run the report.

Master Server	Feature Name	Licensed Capacity (TB)	Used Capacity (TB)	In Compliance
gdndev-sol3	Advanced Disk Storage Unit	10.00	0	YES
gdndev-sol3	Advanced Virtual Tape Storage Unit	10.00	0	YES
gdndev-sol3	NAS SnapVault	10.00	0	YES
gdndev-sol3	NetApp Disk Storage Unit	10.00	0	YES
gdndev-sol3	OpenStorage Disk Storage Unit	10.00	0	YES
gdndev-sol3	PureDisk MS Exchange Agent	10.00	0	YES
gdndev-sol3	PureDisk MS SQL Server Agent	10.00	0	YES
gdndev-sol3	PureDisk Remote Office	10.00	0	YES
gdndev-sol3	PureDisk Storage Unit	10.00	0	YES

- 1 Click the link to a report (the link is the same as the report title).
- 2 Supply the required run time parameters for the report.

Running a report with run time parameters

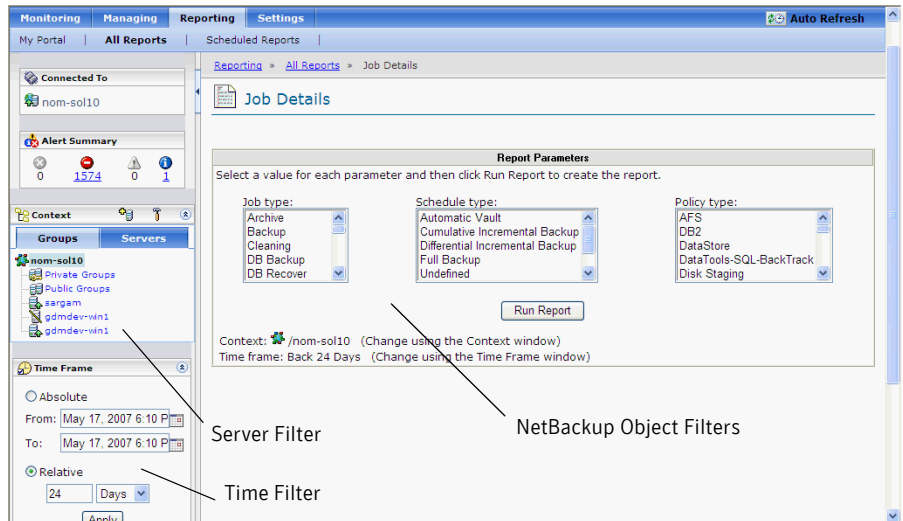
A report (custom or standard) can contain run time parameters. You define these parameters when you create the report. A report can contain any of the following types of run time parameters. A report can include more than one parameter in a report.

- A filter for date or time. The report runs using the values in the **Time Frame** pane. You can use this pane to change the values.
See [“Running a report with date or time run time parameters”](#) on page 189.
- A filter for server (or server group). The report runs using the currently selected server in the **Context** pane. You can use this pane to change the selection.
See [“Running a report with server \(or server group\) run time parameters”](#) on page 191.
- A filter for a NetBackup object that the report requires such as, schedule type, job type, or policy type. Parameter selection drop-down list boxes and/or text boxes are available. NOM does not run the report until you specify all required parameters.
See [“Running a report with NetBackup object run time parameters”](#) on page 191.

Reports can be rerun after modifying the run time parameters.

The following figure shows an example of a report containing time, server, and NetBackup object filters. After you specify all the parameters, the report is run.

See [“Filtering options for the report”](#) on page 203 for information about using filters when you create a report.



Running a report with date or time run time parameters

The following topics explain how to run a report with date or time parameters.

How does NOM handle different time zones when it generates reports?

NOM uses the following event sequence for time zones:

- 1 NOM stores all data that it collects from your managed NetBackup servers in the NOM database with a time stamp. This time stamp is of a time zone specified for NOM server.
- 2 NOM uses the time frame you specify in the **Time Frame** pane and determines the range of data you want to see.
 See [“Specifying the time frame for a report”](#) on page 190.
- 3 NOM uses your Data display time zone preference, converts the data to that time zone, and displays the data.
Settings > Preferences > Data display time zone lets you specify the time zone that is used to display data for all generated views and reports in NOM.
- 4 If **Adjust relative time frame on the SORD boundary** option from the **Settings > Preferences** tab is selected, the specified SORD value is used to

calculate start time and end time of relative timeframe or reporting day. See [“To filter the report by using a reporting day”](#) on page 204 for more details.

Settings > Preferences > Start of Reporting Day lets you specify your reporting day.

See [“Setting preferences for NOM users”](#) on page 173 for information about the SORD setting.

Specifying the time frame for a report

NOM runs reports with date or time parameters by using the default time frame specified for that report. You can specify a different time frame and the report is run again by using your new selection. This selected timeframe is applicable to the specified report only for the current user session.

You can specify an absolute or a relative time frame (or reporting day) for a report. The time frame specifies the range of data that you want to include in the report.

Caution: Use caution when you specify a time frame for a report. A long time frame may lead to large amounts of data and may cause NOM database issues.

To specify an absolute time frame for a report

- 1 Click the report name to run the report.
- 2 Select **Absolute** in the **Time Frame** pane.
- 3 In the **From** box, use the calendar icon to specify the start date.
In the **To** box, use the calendar icon to specify the end date.
- 4 Click **Apply**. NOM runs the report with the new selection.

To specify a relative time frame for a report

The start time and end time specify the time frame that NOM uses when it generates the report.

- 1 Click the report name to run the report.
- 2 Select **Relative** in the **Time Frame** pane.
- 3 Use the text box and the drop-down list box to specify the time (duration of the report). You can specify hours or days. The time you specify is the start time for the report.
- 4 Click **Apply**. NOM runs the report with the new selection.

Running a report with server (or server group) run time parameters

These types of reports run using the currently selected server in the **Context** pane. You can specify a different server (or server group) and NOM runs the report again by using the new server.

To specify the server for a report

- 1 Click the report name to run the report.
- 2 Select a server (or server group) in the **Context** pane.

Running a report with NetBackup object run time parameters

These types of reports do not run until you specify all required object run time parameters. These parameters narrow the focus of the report by specifying NetBackup criteria such as a particular job type or backup policy before the report is run.

To specify the object criteria for a report

- 1 Click the report name to run the report.
- 2 Use the drop-down list boxes (for example, **Job type**) to select the object criteria this report requires.
 You can use Ctrl + Shift to select some or all of the values. You also can use click and drag to select all values.
- 3 Click **Run Report**.

Performing tasks to manage your reports

The tasks that are available to manage your reports vary depending on the composition of the report and your current report view.

Some tasks are always available. Some are available only after selecting a report or a report schedule. Others are available only after you run a report. Refer to the task availability column of the following table for each task.

For detailed information on understanding and using the reporting tasks, refer to the NOM online help that is available for most task dialogs.

Task	Task availability
Customize Portal	Always available from the My Portal view
New Report	Always available from the All Reports views

Task	Task availability
New Composite Report	Always available from the All Reports views
Create Copy	After you select a report in Private Reports, Public Reports or Standard Reports (you cannot copy some standard reports)
Create Shortcut	After you select a report in Private Reports
Edit	After you select a report in Private Reports or Public Reports After you select a report schedule in Scheduled Reports
Delete	After you select a report in Private Reports or Public Reports, After you select a report schedule in Scheduled Reports
Schedule	After you select a report After a report runs
Import	Always available from the All Reports views
Export	After you select a report or reports in Private Reports or Public Reports
Email Report	After a report runs. Also see “ Emailing NOM reports ” on page 192.
Export Data	After a report runs
Printer Friendly	After a report runs

To manage your reports

- 1 From a table that contains the available reports or report schedules, select the check box to choose a report or a schedule.

Note: For some report tasks, you must first run the report by clicking the link to the report.

- 2 From the **Tasks** pane, select an applicable task.

Emailing NOM reports

You can email a report in HTML format from the report screen after running a report. The **Email Report** task reruns the report in the background and emails it to the specified recipients. Since the report is re-run, if you sort or change a report while viewing the report in the console any changes are not preserved in

the emailed report. The emailed report uses the sort order as specified in the report definition.

You can also schedule a report so that it is run and emailed at the scheduled time using the scheduler wizard (see [“Using the report scheduler wizard”](#) on page 223).

Available HTML formats for emailed reports

In NOM you can email reports in the following two report formats. You choose a format from the email report screen after running a report or from the scheduler wizard (see [“Specifying email addresses and HTML format for the report”](#) on page 224).

The default email report format can be specified in the **Settings > Preferences** tab. See [“Setting preferences for NOM users”](#) on page 173.

Format options can always be changed before emailing a report using the schedule wizard or the email report screen.

HTML without JavaScript

Reports are emailed without JavaScript embedded. This avoids some error messages if the email client does not support JavaScript. The Lotus Notes client and Mozilla based clients require this format. This is the default format.

This format also allows the following additional options. Selecting either of these options is not required.

- **Disable hyperlinks**
Hides all hyperlinks in a report. This option can be used if you want to email a report only for presentation.
- **Use jpeg for graphical reports**
Graphical reports are emailed in jpeg email format. This option must be selected if you want to use Lotus notes or Mozilla based email clients. If you do not select this option, graphical reports are generated in png format. png image format is not suitable for Lotus Notes.
Microsoft Outlook users should not select this email format option for higher image quality.

Rich HTML

Reports are emailed with JavaScript embedded. This preserves tooltips in the reports. Note that tool tips only work on some versions of Microsoft Outlook.

Using the report builder wizard

The report builder wizard lets you create new custom reports or change existing reports. You can create reports to display in a traditional table format or through a graphical representation. Also, the report builder wizard allows creating a hierarchy of related reports.

The report builder wizard has a navigation pane on the left hand side. As you build a report, the navigation pane reflects the selections you make.

The report definition process consists of the basic report design and report options you can use to specify the report data and how it should be displayed.

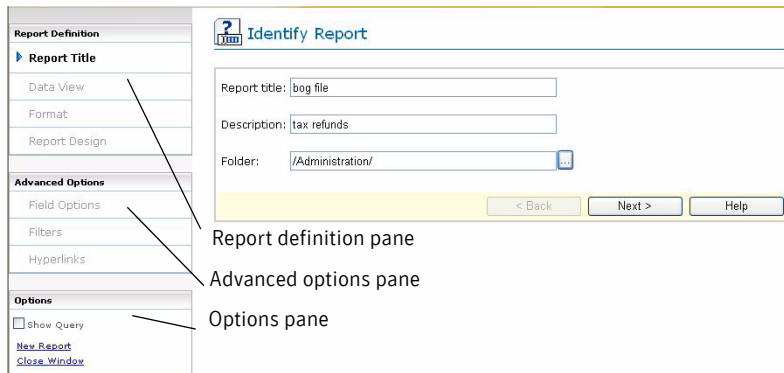
To best use the report functions, you should understand basic SQL.

The wizard lets you:

- Define the basic presentation of your report.
NOM uses SQL to specify the data. The report builder wizard has a query builder that helps you select data for the report.
You can choose the type of report, for example a table or bar chart. You can also specify the title of each column, tool tips and so on for the report.
- Further customize your report by using advanced options.
The advanced options allow you to group data by certain entities like client, policy and so on. They also allow you to select parameters when running a report and allow you to link multiple related reports together to enable management by exception.

To start the report builder

- 1 Select **Reporting > All Reports**.
- 2 In the **Tasks** pane, click **New Report**.



- 3 After you finish defining a report, click **Finish**. A preview of the report appears. The completed report is available in the **Private Reports** section.
- 4 You can view the report and return to make changes to the report if needed.

To go back and change your report definition

- ◆ In the Report Definition pane, click a screen and follow the instructions.

To view the SQL query that is generated for your report

- ◆ In the **Options** pane, select **Show Query**.

To customize your report definition

- ◆ Click **Advanced** on the last required screen to use the advanced option screens to customize your report further.

To create another report without exiting the report builder

- ◆ In the **Options** pane, select **New Report**.

To exit the report builder and not create a report

- ◆ In the **Options** pane, select **Close Window**.

The following sections contain these report builder wizard topics.

- [“Required wizard screens for a custom report”](#) on page 196
 This section explains the screens and tasks that are required to build a report. If your report requires no advanced features, you can consider the report finished.
- [“Optional wizard screens for additional report customization”](#) on page 201
 This section explains the screens that are optional when you build a report.
- [“SQL grammar used by the wizard”](#) on page 207
 To best use the report builder, you should understand basic SQL (Structured Query Language). Refer to this section for basic information about SQL queries and NOM.
- [“Building a sample report”](#) on page 211
 This section explains how to create a sample report, enhance the report, and finally create linked reports. Also shown are the relevant SQL queries.

Required wizard screens for a custom report

The following sections explain the screens and tasks that NOM requires to build a report. If your report requires no advanced features, you can consider the report finished.

Note: Each step of the process may involve multiple sub steps and the sequence of steps taken by report builder wizard may not match the following example sequences.

- [“Identifying the report”](#) on page 196
- [“Selecting the data for the report”](#) on page 197
- [“Picking a display format for the report”](#) on page 198
- [“Selecting the data fields to display in your report”](#) on page 198

Identifying the report

To identify the report

- 1 Type a title and description for the report.
The report title and description appear in the **Private Reports** view when the report is completed. The report description also appears with the report results.
- 2 Type a folder name to use to organize your reports.
You also can click ... to use the **Pick Report Folder** dialog box. This dialog box lets you browse and select an existing folder, or create a new report folder.

Using the pick report folder dialog box

The folder structure provides a catalog of all custom reports that you created and is a convenient way to organize your reports. This folder structure is internal to NOM and does not map to a file system.

Do one of the following:

- ◆ Select an existing folder from the current folder tree.
- ◆ Type a path name for a new folder in **Folder name**. Use / (forward slash) to separate folders and subfolders.

Selecting the data for the report

To select the data for the report

- ◆ Select one of the types of data that is listed.
You can expand (click +) to view the complete contents of the data view that you select.

Reports based on Volume data view

If a report is based on **Volume** data view and the report uses Mounts, MaxMounts, or CleaningsRemaining columns, then the value of these columns may be -1. This is because of the following reasons:

- The value of the Mounts or MaxMounts column is -1 if the media is a cleaning media.
- The value of the CleaningsRemaining column is -1 if the media is not cleaning media.

Data Views Dependent on Catalog Image Data Disabled

The following data views have been disabled in the NOM custom report builder. You can not create any new custom reports using these data views.

- Hot Catalog Backup (Hot Catalog Backup Information)
- Catalog (Catalog metadata)
- Image (Current Image information)
- Combined Job and Image (Combined Image and Job information)
- Client Media (Summarizes media usage by client)

All standard or custom reports that use any of these data views may not show up-to-date information. This applies to reports in the **My Portal**, **All Reports**, and **Scheduled Reports** tabs.

All standard reports that are based on these data views have a red asterisk next to the report name in the **Standard Reports** display. At the bottom of the view a warning message for these reports is displayed.

Any custom reports previously created using these data views can still be executed. But the reports will likely display inaccurate data and the usage of any custom report using these data views is not recommended.

When a report based on catalog image views is run, the following warning message is displayed in the run report screen: **Note: This report is based on Catalog data. It will not show up-to-date information.**

If any component reports of a composite report are defined based on any of these data views, the message is also displayed.

If you have any schedules for reports created from these data views, the reports will be run and any emailed reports also have the warning message.

Picking a display format for the report

Select the display format you want to use for the report. The display format you select determines the report builder wizard screens that are required.

To select a format for the report

- ◆ Select one of the available report output formats.

Selecting the data fields to display in your report

The report builder wizard screens used to select data fields vary slightly depending on the display format you select, as follows.

To select the data fields for a table

- 1 Click **Add Column** to add columns to the table.
- 2 Select from the drop-down list to choose the NetBackup data to include in each column of the table.
You can select duplicate data fields to display, but you must specify unique names for them in the title column.
You can change the display title for each column of the table. The default title for the column is the NetBackup field name from the data view.
In addition if you include **Exit Status field** in your report design, the status displayed in the report automatically is linked to help topics for the selected NetBackup status code. The **Exit Status** field is present only for some views. These topics are from the *NetBackup Troubleshooting Guide*.
- 3 For some data fields, you can convert the unit of display. In fields where you cannot change the display unit, N/A appears under **Units**.
- 4 You can use optional title tool tips and data tool tips, to identify and explain the report and its data.
For title tool tips, your text appears as mouseovers in the column titles when you generate the report. For a title tool tip, specify the text in the **Title Tooltip** section of the field.
If you do not specify a title tool tip, the display title that you specified in [step](#) is used.
- 5 For data tooltips, your explanatory text appears as mouseovers in each data column of the report. For tool tips, you can specify descriptive text and a link to report fields or hidden fields. Hidden fields are not directly displayed in a report. However they can be used in a tooltip, or in a filter.

To specify a link to a field, use this format: *optional text %data-field%*. *data-field* must match a report field title or hidden field title.

For example, for the job ID field of a report, the **Data Tooltip** entry might contain the following entry: *The policy name for this job = %PolicyName%*. In the job ID column of the actual report, the resulting tool tip displays the text *The policy name for this job =* and the policy name for each job.

To use tool tips with a hidden field, first specify the associated data in the **Hidden Fields** section. This data only appears in the tool tip and not in the actual report. Click **Add Field** to add hidden fields.

Hidden fields can also be passed to linked destination reports.

- 6 Use the arrows to move the columns to change the order that the columns appear. The top row in **Table Definition** area appears as the leftmost column in the table.
Use the delete icon to remove any data column that you do not want in the report.

To select the data fields for a pie chart

For this report type, a pie chart and a legend explaining the chart are displayed. The colors used in a pie chart are selected automatically by NOM.

- 1 Select from the **Field** drop-down list box to select the NetBackup data to include as slices of the pie chart. The field used for the slice must be numeric. A nonnumeric field can be used with a function that returns a number for the slice.
- 2 Add a title for the slice. This title is displayed in the legend.
- 3 For some data fields, you can convert the unit of display. For fields where you cannot change the display unit, N/A (does not apply) appears under **Units**.
- 4 You can add an optional tool tip, which is useful to identify the report data further. Your explanatory text appears as mouseovers in each slice of the generated pie. For tool tips, you can specify descriptive text and a link to report fields or use hidden fields.

If you do not specify a tool tip, a tooltip with the relative percents of 100 percent is automatically created for each slice.

To specify a link to a field, use this format: *optional text %data-field%*. *data-field* must match a report or hidden field.

For example, for the job ID field of a report, the **Tooltip** entry might contain the following entry: *The policy name for this job = %PolicyName%*. In the job ID field of the actual report, the resulting tool tip displays the text *The policy name for this job =* and the policy name for each job.

To use tool tips with a hidden field, first specify the associated data in the **Hidden Fields** section. This data only appears in the tool tip and not in the actual report. Click **Add Field** to add hidden fields. Use the delete icon to remove any field that you do not want.

- 5 Select from the **Field** drop-down list to select the data to compare against the data specified in [step 1](#).
Add a title for the data. This title is displayed in the legend.
For example you selected the attempted number of jobs data field in [step 1](#). For this field you could select a time range (**StartTime**). The pie chart result then shows the number of jobs for each day in the time range.

To select the data fields for a bar, stacked bar, line, or area chart

In a bar chart, each added field appears as a bar. In a stacked bar chart, all the added fields appear as one stacked bar.

It is not valid to define a stack bar chart using all data views. For example you can define a stack bar chart using the **Media Summary** view, but you cannot use the **Jobs** view. The other three reports can be based on any view.

Bar, stacked bar, line, or area reports share some common characteristics as follows:

- In the **Report Design** screen, the field used for the Y axis must be numeric. A nonnumeric field can be used with a function that returns a number for the Y axis. For example in the **Field Options** screen, the **count** aggregate function is applied to the **PolicyName** field.
 - If the X axis field uses a date (for example, **StartTime**), then you can specify a time interval.
- 1 Click **Add Bar**, **Add Line**, or **Add Area** to add fields to the report.
 - 2 Select from the drop-down list to choose the NetBackup data to include in the chart. Select only numeric data fields for the fields you add.
You can select duplicate data fields to display, but you must specify unique names for them in the title column.
 - 3 You can change the title to display for each field. The default title is the data field name.
For some data fields, you can convert the unit of display. In fields where you cannot change the display unit, N/A appears (does not apply).
 - 4 You can add optional tooltips, which are useful to identify the report data further. Your explanatory text appears as mouseovers in each data field of the generated report. For tool tips, you can specify descriptive text and a link to report fields or hidden fields.

If you do not specify a tool tip, a tool tip with a format of *field-title:field-name* is automatically created by NOM.

To specify a link to a field, use this format: *optional text %data-field%. data-field* must match a report or hidden field.

For example, for the job ID field of a report, the **Data Tooltip** entry might contain the following entry: *The policy name for this job = %PolicyName%*. In the job ID field of the actual report, the resulting tool tip displays the text *The policy name for this job =* and the policy name for each job.

To use tool tips with a hidden field, first add the associated data view fields in the **Hidden Fields** section. This field only appears in the tool tip and not in the actual report. Click **Add Field** to add hidden fields.

- 5 NOM uses default fill colors for the report fields. The default fill colors are shown in the **Fill Color** field for each report field. You can click on the default color and pick a new color. The new color is then shown in the **Fill Color** field.
- 6 For multiple display fields, you can use the arrows to change the order that the fields appear in the chart or delete a field.
Use the delete icon to remove any field that you do not want.
- 7 Select from the **Field** drop-down list to choose the data to compare against the other data fields you specified in [step 2](#) on page 200.
If you use the **StartTime** or **EndTime** fields in your report design, you also can specify a time interval in days, hours, minutes, or seconds in **Interval**.
You can add descriptive labels for the x and y axis of the chart.

Optional wizard screens for additional report customization

As you add options to a report, the navigation frame reflects the selections you make (the **Advanced Options** pane on the left). You can return to any of these screens and add options.

Note: Each step of the process may involve multiple sub steps and the sequence of steps taken by report builder wizard may not match the following example sequences.

The following sections explain the screens that are optional when you create a report:

- [“Field options for the report”](#) on page 202
- [“Filtering options for the report”](#) on page 203
- [“Linking reports together”](#) on page 205
- [“Building a sample report”](#) on page 206

Field options for the report

This screen lets you select any group option or sort option for each field of the report.

To select the fields to group in the report

If you select the group option for any fields of the report, you must assign an aggregate function to each non-grouped field in the report.

For example, if a report has ten rows where the value for the **Control Host** data field is the same and you group by **Control Host**, then these ten rows are grouped and appear as one row.

- ◆ Select the **Group By** checkbox for the data fields you want to group in the report.

To select the group fields order

If you select the group option for any fields of a report, you need to specify the order for the fields. This does not affect the order in which the data appears in the report.

- ◆ Select a value for the sequence in the **Group By Order** drop-down list for each grouped field.

To perform a summary function on non-grouped fields

If you use the group option for any fields of a report, for each non-grouped field you must assign a summary (or aggregate) function to it. NOM reporting supports the following aggregate functions: **min**, **max**, **count**, and **avg, sum**.

For example, for the number of jobs field (**AttemptNumber**), the **count** function is available.

- ◆ Select a function in the **Aggregate Function** drop-down list for each non-grouped field.

To perform a conversion of the data in a field

For time-related fields, functions like **cyc_formatYear** and **reporting_day** are available. The **reporting_day** function returns a single day for a report.

NOM reporting supports the following scalar functions: **cyc_formatDay**, **cyc_formatMonth**, **cyc_formatYear**, and **reporting_day**.

- ◆ Select a function in the **Scalar Function** drop-down list for each field.

To select the sort order for fields

- ◆ In the **Sort Direction** drop-down list, select **Ascending** or **Descending** order for each field in the report.

To use graphical images in your report (table format reports only)

If you include **Exit Status**, **Drive Status**, or **Media Status** fields in your report design, you can choose to display an image for these fields to improve report readability.

Only one graphical image can be shown per report and it always appears in the first column of the report.

- ◆ In the **Select Column** drop-down list, select **Exit Status**, **Drive Status**, or **Media Status** image for the report. The box has applicable options depending on the view and columns that you selected earlier.

Filtering options for the report

These options allow you to define filters for the data that is included when a report runs. If you do not specify any filtering criteria, all data in the report is displayed.

You can define the following types of filters. You can filter the report using any or all of the following filters.

- Use a master server filter.
See [“To filter the report by using a master server selection”](#) on page 203.
- Use a time window filter.
You cannot define a filter based on both a time frame and a reporting day. Select **No Filter** if you do not want to use a time filter.
See [“To filter the report by using a time frame”](#) on page 203 or [“To filter the report by using a reporting day”](#) on page 204.
- An SQL expression filter.
See [“To filter the report by using a SQL expression for the filter”](#) on page 204.

Values for run time filters can be specified when you run the report or when you schedule a report.

To filter the report by using a master server selection

The generated report uses the currently selected master server (or server group) in the **Context** pane when the report runs. If needed, the context can be changed each time the report is run.

- ◆ Select the **Filter the data on servers and server groups** checkbox.

To filter the report by using a time frame

The generated report is filtered using the time frame you choose. Using the **Time Frame** pane the time span can be specified as absolute or relative when the report is run and can be changed when the report is rerun. This option is

available only if the selected view has any date type column like Start time, end time etc.

- 1 Select **Time Frame**.
- 2 Select any type of time column to apply the time frame to by using the drop-down list.
If you choose **StartTime** for start time and end time fields, the report runs using the following SQL filter:
StartTime BETWEEN Start_time_chosen_when_running_the_report AND End_time_chosen_when_running_the_report
- 3 Specify a default relative time span for the report in **Time Span**.
The report runs using the default time span.
It is good practice to have a longer time span for summary reports and a shorter time span for detailed reports. For example, a report with job summary information by client could have a default time span of 7 days or a month. A report with job details for last 24 hours should have a default time span of 24 hours.

To filter the report by using a reporting day

The generated report is filtered using a **ReportingDay** run time parameter. You must specify a reporting day before the report is run.

ReportingDay is available only if you have applied the **reporting_day** function in the Report Design page of the report builder.

See “[Selecting the data fields to display in your report](#)” on page 198.

- 1 Select **Reporting Day**.
- 2 Select a data field by using the drop-down list.
Select a date type of column to apply the reporting day filter to. If you applied the **reporting_day** function to any column in the Report Design page, then all of those columns appear in the drop-down list.

To filter the report by using a SQL expression for the filter

The generated report uses the filter when the report runs. SQL query is used to specify the expression.

- 1 In the **Define Filter** section, select a field, a SQL operator for the field, and a value to compare against when NOM generates the report.
The operators available are based on the data type of the field you select. If the field you select involves a time value, use the calendar icon (**Pick date and time**) to choose a date for the report.

- 2 If you specify a field in the filter that can also be a run time parameter (for example, **JobType** or **ClientName**), you can select **Specify value when report is run**. This option is shown for the fields which can be run time parameters. If you specify a run time parameter and do not use **Specify value when report is run**, you must enter a value for the parameter when defining this filter.
- 3 Ensure that you use the arrow (>>) button to add this expression to the **Filter Definition** section. This section shows the resulting SQL expressions. As you build the expression, you can use **and** or **or** operators in the expression. Use the delete icon to remove any unwanted expression.
- 4 You can create multiple filter expressions by repeating the previous steps.

To limit the results of filter operations

- ◆ Select **Number of results to show** and enter a value.

Linking reports together

You can link a report to another existing report. When the source report runs and you click a hyperlink in the report, NOM passes values from the report to the destination report. NOM then displays the destination report using the passed values.

You can do any of the following types of linking:

- Link to any report from the source report. The destination report does not have any run time parameter.
- Pass field values from the source to a destination report.
- Pass values of run time parameters from the source to a destination report.

This powerful linking feature lets you link and drill down to view other related reports. See [“Linking a source report to a destination report”](#) on page 218 for a linking example.

To link to an existing report

You must assign some (or all) of the fields of your source report to run time parameters in an existing destination report.

Fields corresponding to all run time parameters in the destination report should also be present in your source report for the report to run correctly. These fields in your source report can be regular fields, hidden fields, or run time parameters.

- 1 For each field in your report, you can select a destination report to link to by using the **Linked To** drop-down list boxes. The reports available in **Linked To**

are based on the fields and run time parameters that are present in your source report. and run time parameters in destination reports.

If the source report has all information required to pass to a destination report then the report is included in **Linked To**.

For example, if a destination report uses the **ClientName** runtime parameter then the destination report is included if the source report also uses client name in a field or as a runtime parameter.

Note: Destination reports where server context is used appear in the **Linked To** section if the source report contains **HostGUID** as a data field or the source report uses server or server group context as a filter.

See “[To filter the report by using a master server selection](#)” on page 203.

- 2 If the destination report you select contains any run time parameters, they appear in the **Linked Report Parameters** section. The available parameters shown are based on the fields present in your source report and the run time parameters in your destination report.
If you select a field value (for example, **ClientName**), the client name is passed on to the destination report. The field can be a displayed or hidden field in the source report.

Building a sample report

Some examples on how to design a sample report using the custom report builder wizard are given below:

Pie chart report example

You could design a pie chart report as follows:

- 1 In the **Data View** screen, select **Job**.
- 2 In the **Report Design** screen, select **AttemptNumber** as the attempted number of jobs field for the Y axis (*no of jobs* is used for the title).
Select **StartTime** as the time field for the X axis (*day* is used for the title).
- 3 In the **Field Options** screen, apply the **reporting_day** scalar function to *day* and also group the *day* field.
Apply the **count** aggregate function to *no of jobs*.
Using the **Field Options** screen, the result could also be sorted by *no of jobs* or *day*, if needed.

You then run the report to include ten days of data. The report result is a pie chart with ten slices.

Bar, line, or area chart report example

You could design a report for one of these report types as follows. This sample report generates a chart with the amount of data displayed on the Y axis and the day on the X axis.

- 1 In the **Data View** screen, select **Job**.
- 2 In the **Report Design** screen, select **Kbytes** for the Y axis (*size* is used for the title).
Select **StartTime** for the X axis (*start* is used for the title).
- 3 In the **Field Options** screen, apply the **reporting_day** scalar function to *start* and also group the *start* field.
Apply the **sum** aggregate function to *size*.

You could also use the **Filters** screen, to filter the report by context or a time frame.

SQL grammar used by the wizard

This section explains the SQL grammar that is supported by NOM and shows the mapping between the report builder wizard screens and SQL clauses. Some example SQL queries are also shown. Use this section to help you prepare a SQL query before you launch the NOM report builder wizard.

If you have a knowledge of SQL, this section explains which screens in the report builder wizard accepts which SQL details. For example, the hidden fields that you can specify in **Report Design** wizard screen are used in the SELECT clause of the SQL query. See [“Selecting the data fields to display in your report”](#) on page 198.

The grammar of the SQL supported by NOM follows:

```
SELECT [ TOP n ] selected-fields [, hidden-fields]
```

```
FROM data-view
```

```
[ WHERE filters ]
```

```
[ GROUP BY group-by-list ] [ HAVING filters ]
```

```
[ ORDER BY { field-name | title } [ ASC | DESC ], ... ] (Note: ASC is the default)
```

```
selected-fields::
```

```
{ field-name } AS title | { aggregate_function (field-name) |  
Scalar_function (field-name) } AS title, ...
```

```
group-by-list:
```

```
{ field-name | title }, ...
```

```
hidden-fields::
```

```
{field-name } AS title |{ aggregate_function (field-name) |  
Scalar_function (field-name)} AS title, ...
```

FROM clause

This clause lets you specify the database view used to select the report data. For the applicable wizard screens, see [“Selecting the data for the report”](#) on page 197.

Note: NOM does not support joins of multiple tables. It makes available only a select views to define reports on.

Top n clause

You can retrieve only a limited number of rows returned by a query. For the applicable wizard screen, see [“To limit the results of filter operations”](#) on page 205.

This clause combined with the ORDER BY clause can be very useful. It is recommended to always combine this clause with the ORDER BY clause to ensure that if the data in the database hasn't changed, the report shows the same data each time it is run.

If you want to get a list of the top 10 NetBackup clients processing maximum data, you could write a SQL query like the following sample:

```
SELECT TOP 10 ClientName as "Client Name", sum (kBytes) as "Data  
Processed"  
FROM Job  
GROUP BY "Client Name"  
ORDER BY "Data Processed" DESC
```

This query sorts the result in descending order of "Data Processed". So only the top 10 clients with maximum amount of data processed are included in the resulting report.

Grammar of selected-fields and hidden-fields clauses

Selected and hidden fields for columns in tables and for a bar in a graphical report are used in the SELECT clause of the query.

For the applicable wizard screens to select data and hidden fields, see [“To select the data fields for a table”](#) on page 198, [“To select the data fields for a pie chart”](#) on page 199, and [“To select the data fields for a bar, stacked bar, line, or area chart”](#) on page 200.

Hidden fields are not directly displayed in a report. However they can be used in a tooltip, or in a filter. For example, in a bar graph that shows the number of successful jobs on Y axis and the corresponding client on X axis, you may want

to include details like, the number of files processed, the amount of data processed, duration and so on in the tool tip of each bar representing successful jobs of each client.

The selected field allows you applying some functions on the columns or bars. If the column or bar is grouped, then it can use a scalar function. And all the non-grouped columns or bars must have aggregate function applied to them.

The following scalar function is supported by NOM: **reporting_day**. This function is defined by NOM and it converts a time stamp into a reporting day as defined by the Start of Reporting Day (SORD) value defined in user preferences. The specified SORD value is used only if **Adjust relative time frame on SORD boundary** is selected from the **Settings > Preferences** tab.

See "[How is the start of the reporting day \(SORD\) used in NOM?](#)" on page 175 for information about the SORD setting.

For example if the SORD value is set to 8:00AM, for a time stamp of 10 Jan 2006 7:00AM the function returns 9 Jan 2006 and for a time stamp of 10 Jan 2006 9:00AM the function returns 10 Jan 2006.

The reporting day function is handy for example, when you want to plot a graph that shows the number of jobs running every day with the number of jobs displayed on the Y axis and the day on X axis. You also want the data to show the last 10 days. The following SQL query using aggregate and scalar functions could be used:

```
SELECT TOP 10 reporting_day (startTime) as "day", count (JobID) as "No of Jobs" from Job group by "day" order by "day" DESC.
```

You would put the "No of Jobs" column on the Y axis and the "day" column on X axis when defining this report in the report builder.

Filter clauses

Filters can be defined on selected fields, hidden fields or directly on fields in the data view. If title of a selected or hidden field and a data view field are the same, the filter is applied on the respective selected or hidden field. Nested filters with multiple AND and OR operators are supported by NOM.

For the applicable wizard screen for filters, see "[Filtering options for the report](#)" on page 203. This is the screen used to make a report server context sensitive or time frame sensitive. You can also use a filter with a run time parameter.

All filters defined in the wizard are used in the WHERE or HAVING clause of the query depending on if it is defined on a selected or a hidden column with a scalar or aggregate function respectively. Please refer to any SQL tutorial or manual for more details about using the HAVING or WHERE clauses.

For example to define a report that gives a list of all jobs for a given time frame and for a client selected at run time, the query would be similar to the following:

```
SELECT JobID as "JobID", ClientName as "ClientName", FileCount as  
"FileCount",  
FROM Job  
WHERE "StartTime" >= $TimeFrame.startTime$ AND "StartTime" <=  
$TimeFrame.endTime$ AND "ClientName" = $ClientName.ClientName$
```

In this filter, all values enclosed by \$ signs are accepted from the user when the report is run. You are asked to enter a client and time frame, since the query has ClientName and time frame parameters. The filter clauses using StartTime are the result of selecting the **Time Frame** option in the **Filters** screen of the wizard. The StartTime fields are used for the query since they were both specified in the **Start time field** and **End time field** in the wizard. Generally, both of these fields should be set to StartTime, unless you know what you want to achieve. Refer to [“Filtering options for the report”](#) on page 203 to see how a time frame filter is defined.

Group By clause

The **Field Options** wizard screen lets you select the fields to group by (see [“Field options for the report”](#) on page 202). You can group on selected fields or on hidden fields. You can achieve grouping by adding fields in the hidden columns list and then grouping on the hidden columns.

This clause is useful when you want to summarize data. For example, you may want to count the number of jobs per client, in such cases you need to group by client. If you want to calculate the number of jobs per policy and per client, then you should group on policy and on client. The order of the grouping is important. The **Field Options** screen lets you specify the grouping order.

For example, a query to count the number of jobs per policy per client would be similar to the following:

```
SELECT PolicyName as "Policy", ClientName as "Client", count (JobID) as  
"No of Jobs"  
FROM Job  
Where "Policy" IS NOT NULL  
GROUP BY "Policy", "Client"  
ORDER BY "Policy", "Client"
```

Order By clause

This clause lets you sort the data in ascending (the default) or descending order by one or more columns. It is recommended that all tabular reports use this clause. Using this clause ensures that when retrieving a page of data, the report consistently returns the same data if the data in database has not changed, after the report is run.

For example given these two queries:

- Query 1: select jobid from Job
- Query 2: select jobid from Job order by jobid

Each time the first query is run it can return job information in any order. So if you are seeing jobid 1 as the first row when you first run the query, you may see jobid 2 in first row when you next run the query. However, using the second query always returns the results in same order, that is, sorted by jobid.

In a tabular report it is important that the results are fetched in a certain order since the query is used again and again to fetch the next page.

For more details please refer to any SQL reference.

Building a sample report

Creating a report consists of the following basic steps:

- 1 Identify the data required for a report.
- 2 Decide on the report presentation.
- 3 Write a SQL query to help design the report.
- 4 Launch the report builder wizard and define the report.

This section shows how to

- Create a sample report (“[Designing a sample report](#)” on page 211).
- Enhance the sample report (“[Enhancing the sample report](#)” on page 217).
- Create a linked report from the sample report (“[Linking a source report to a destination report](#)” on page 218).

Note: Each step of the report creation process may involve multiple sub steps and the sequence of steps taken by report builder wizard may not match the following example sequences.

The queries specified in the example are pseudo queries. For example, nom_nbJob is the database view name and Job is the logical name that is used in the report builder. Real report queries may look somewhat different.

Designing a sample report

Suppose we want to generate a historical report for the data backed up per client. Also, we want it to be a graphical report of data backed up on the Y axis

and the corresponding clients on the X axis. Sample input data for this report looks like this:

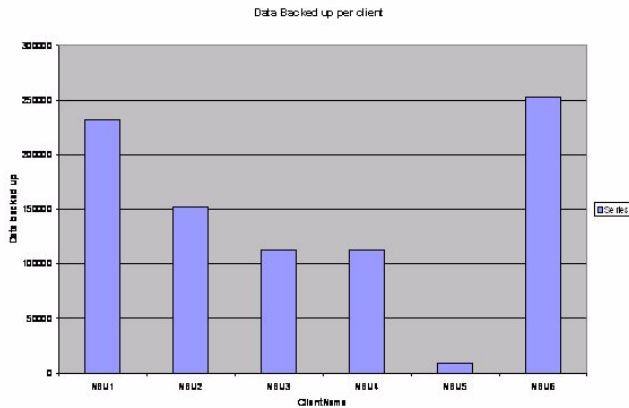
Client Name	kBytes
NBU1	232416
NBU2	152416
NBU3	112416
NBU4	512790
NBU5	9160
NBU6	352416

The SQL query for this report would be:

```
SELECT ClientName as "Client Name", sum (kBytes) as "kBytes"  
FROM Job  
GROUP BY "Client Name"
```

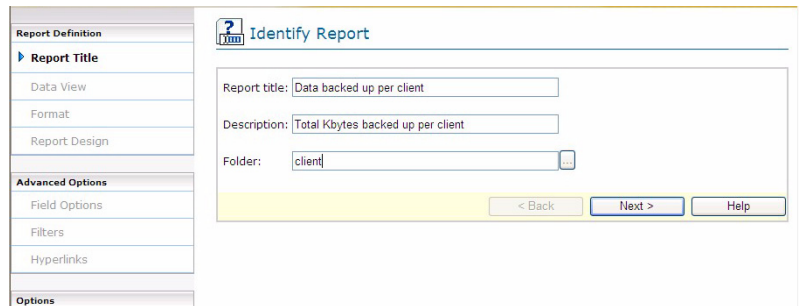
We will use the **Job** data view. This NOM builder data view contains a client name column and a kBytes column. The **Job Attempt** view could also have been used. The difference between the two views is that **Job Attempt** has the information for each attempt of the job while the **Job** view has information only for the final job state. Since we are not concerned about job attempts, **Job** view can be used.

We want the report to look similar to the following bar chart (graphical):

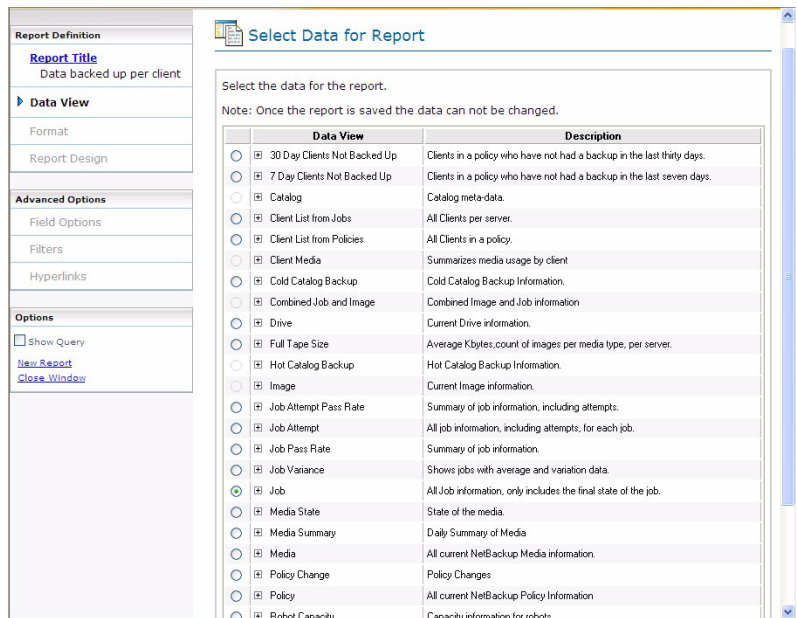


In the query the selected field, Client Name will become the X axis and Kbytes will become the Y axis of the report.

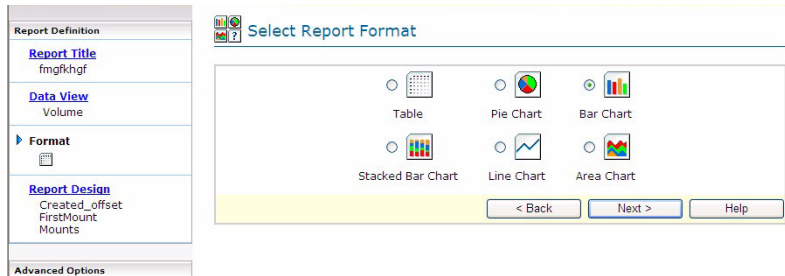
- 1 Start the report builder (see “[To start the report builder](#)” on page 194). In the first wizard screen (see “[To identify the report](#)” on page 196), type the following:
 - *Data backed up per client* as the report title.
 - *Total KBytes backed up per client* for a description for the report. The report description is displayed in the Private Reports view when the report is completed.
 - *client* as the folder name that will be used to organize your reports.



- 2 Select **Job** as the data view (see “[To select the data for the report](#)” on page 197).



- 3 Select the **Bar Chart** format (see “[To select a format for the report](#)” on page 198).



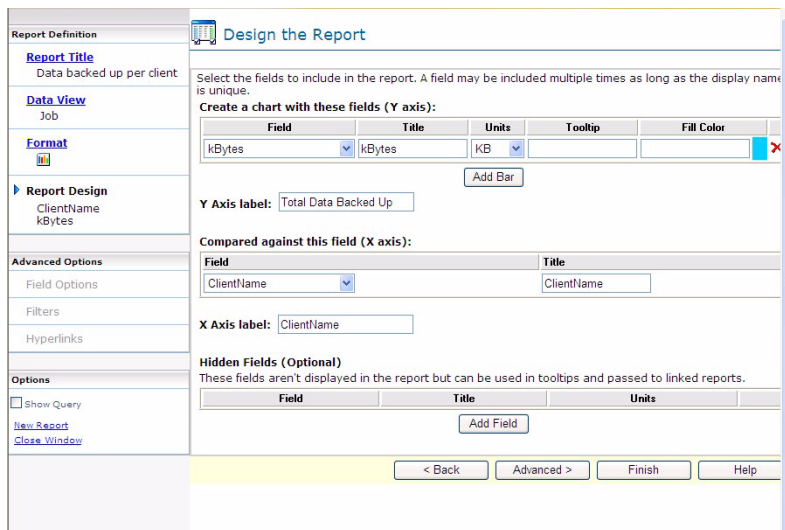
- 4 We need to define the X axis and Y axis for the data fields for the report. To add the Y axis field click on **add bar** and select the kBytes option from the drop-down list (see “[To select the data fields for a bar, stacked bar, line, or area chart](#)” on page 200).

Add *Total Data backed up* as the label for the Y axis.

To define the X axis field, select **ClientName** from the drop-down list.

Add *ClientName* as the label for the X axis.

You can also specify the fill color for the report fields. NOM uses default fill colors for the report fields. The default fill colors are shown in the **Fill Color** field for each report field. You can click on the default color and pick a new color. The new color is then shown in the **Fill Color** field.



- The next step is to apply grouping and aggregate functions. To accomplish this we need to use the **Advanced Options** of the report builder (see “[Field options for the report](#)” on page 202).

We want to calculate the total kBytes backed up for each client, so we need to group the input data based on **ClientName** and sum kBytes for each client.

Select the **Group By** option for **ClientName** and the **Aggregate Function** to be **sum** for **kBytes**.

The screenshot shows the 'Field Options' dialog box with the following configuration:

Field	Group By	Group By Order	Aggregate Function	Scalar Function	Sort Direction
ClientName	<input checked="" type="checkbox"/>	1	None	None	None
kBytes	<input type="checkbox"/>	1	sum	None	None

Buttons: < Back, Next >, Finish, Help

Click **Finish** to preview the report.

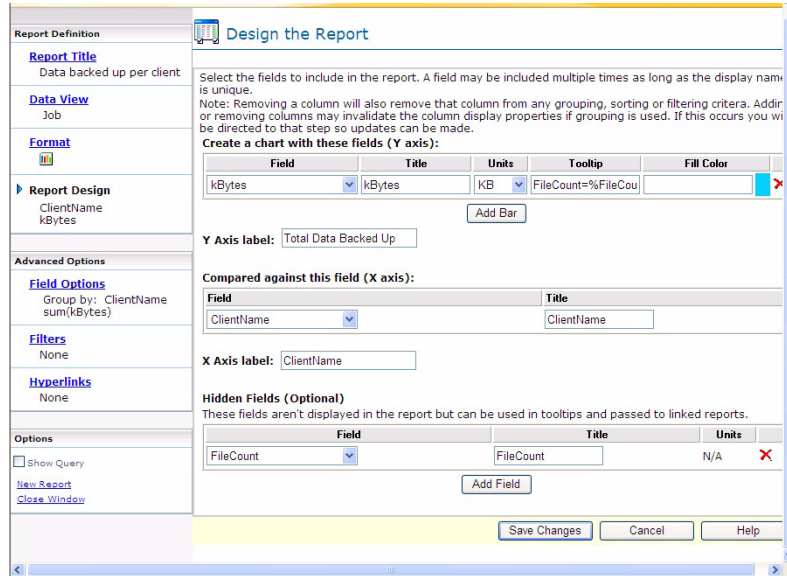
- Additionally, assume there is a requirement to display File Count in a tool tip of each bar corresponding to a client. We want to display the total files backed up as the value of **FileCount**. **FileCount** is currently not in our query, so we need to modify the query:

```
SELECT ClientName AS "Client Name", SUM (kBytes) AS "kBytes", SUM (FileCount) AS "FileCount "
FROM Job GROUP BY "Client Name"
```

Return to the **Report Design** screen and add a tool tip for the Y axis. To specify a tool tip, use this format *optional text %data-field%*.

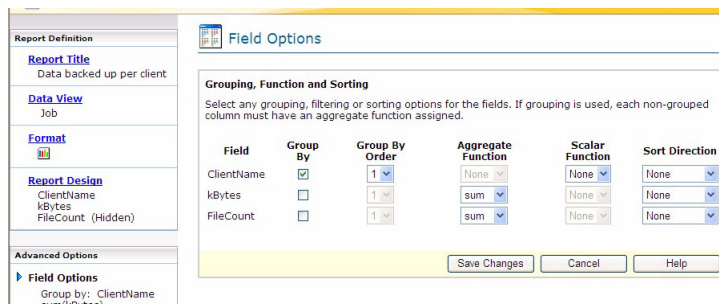
We do not want to display **FileCount** in the report, but want to use it in a tool tip. Hidden fields can be used in such cases.

Select **FileCount** as a hidden field. This adds **FileCount** to the selection query. In the **Tooltip** column specify *FileCount= %FileCount%*.



Click **Save Changes**.

- 7 Because we added **FileCount** as a hidden field in the previous step, the wizard displays the **Field Options** screen page. This happens because we need to apply a function on the **FileCount** column. Apply the **Aggregate Function of sum** on **FileCount** and save the changes.



We have not specified any ordering of the data in the query. So we will see the report data in the same order as is available in the NOM database.

We need to sort the data according to **kBytes** in ascending order. The new query would look like the following:

```
SELECT ClientName AS "Client Name", sum (kBytes) AS "kBytes", sum (FileCount) AS "FileCount"
```



```
FROM Job GROUP BY "Client Name"
ORDER BY "kBytes" ASC
```

This sort ordering can be specified in the report builder using the **Sort Direction** column. Specify **Ascending** for the **kBytes** field.

Click **Finish** to complete the report and preview the report output.

Enhancing the sample report

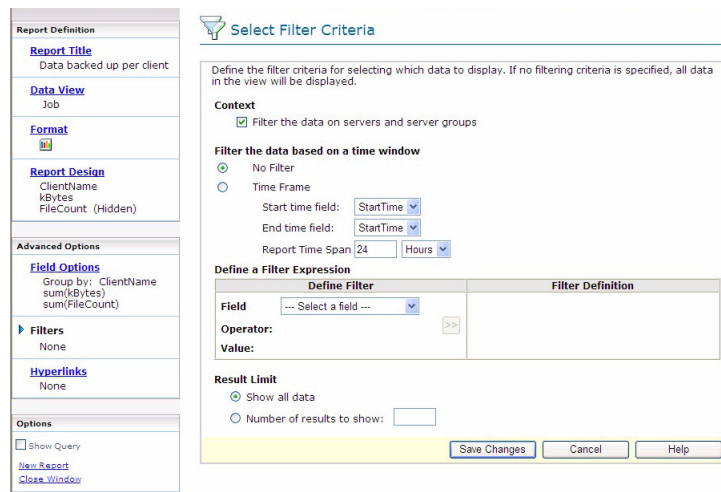
Next we want to modify the sample report definition to filter the data and see only the data for a specific master server.

- 1 Modify the SQL query to add the master server constraints. We add a WHERE clause to the earlier query:

```
SELECT ClientName AS "Client Name", SUM (kBytes) AS "kBytes", SUM (FileCount) AS "FileCount"
FROM Job WHERE
isMember($GroupGUIDName.GroupGUIDName$, "HostGUID")
GROUP BY ClientName
ORDER BY kBytes ASC
```

- 2 To change the report, select the report and click the **Edit** task. We can filter the input data for a specific master server using the **Filters** screen in the report builder (see “[Filtering options for the report](#)” on page 203).

Select the **Filter the data on servers or server groups** option. This filter is available only if the data view selected contains a master server. Only the data for the server or sever group selected when the report is run will be retrieved by NOM.



- 3 Click **Save Changes** to save the changes to the report. A preview of the report is shown in the report builder.

Linking a source report to a destination report

We also want to link this sample bar chart report to another report which provides detailed information about backups for a specified client.

- 1 Create a simple table report using the report builder to provide detailed backup information for a specified client of the selected master server. Use *Job Details for Client* as the report title and use **ClientName** as a run time parameter.

The table would look similar to the following:

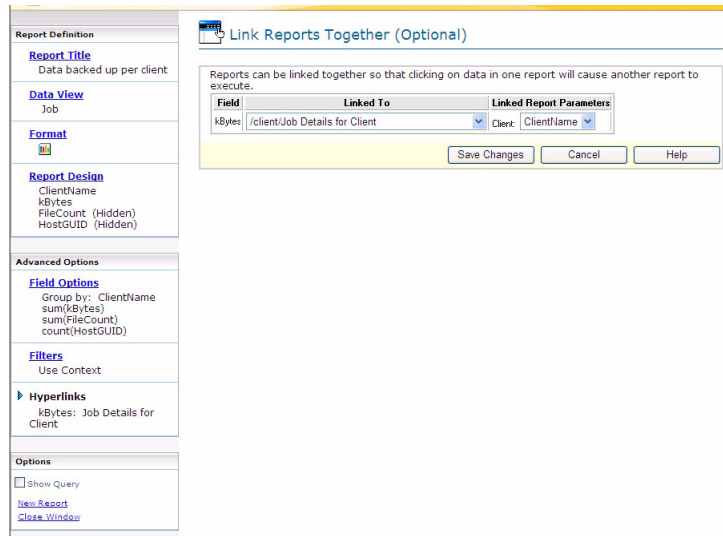
Job ID	Exit Status	Job Type	Client Name	Start time	KBytes	File Count
2,359	129	Backup	NBU1	8/30/06 3:56	1,203,200	2,500
2,400	129	Backup	NBU1	8/30/06 4:30	1,203,200	2,500
2,668	129	Backup	NBU1	8/30/06 9:05	1,143,040	2,500
2,699	129	Backup	NBU1	8/30/06 9:35	1,193,216	2,500
3,026	129	Backup	NBU1	9/2/06 4:19	1,082,880	2,000
3,041	129	Backup	NBU1	8/30/06 16:18	1,143,040	2,500
3,056	129	Backup	NBU1	8/30/06 16:33	1,143,040	2,500
3,274	129	Backup	NBU1	8/30/06 21:09	1,143,040	2,500
3,613	129	Backup	NBU1	9/2/06 4:37	1,082,880	2,000

- 2 Prepare the SQL query as follows:

```
SELECT JobId AS "JobId", ExitStatus AS "Exit Status", JobType AS "Job Type",
ClientName AS "Client Name", StartTime AS "Start Time", kBytes AS
"KBytes",
FileCount AS "FileCount"
FROM Job
WHERE isMember($GroupGUIDName.GroupGUIDName$, "HostGUID")
AND clientname='$clientname.clientname$'
```

 Using the report builder wizard and this query, create and save the report.

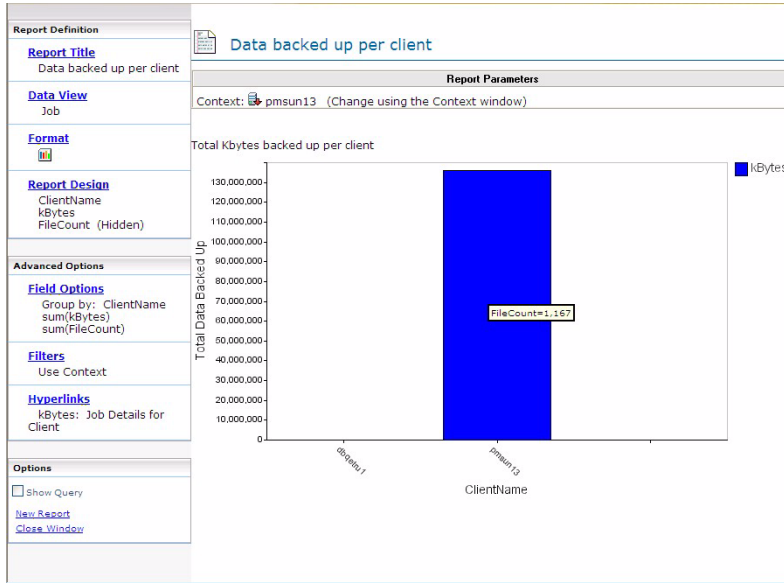
- 3 Link the bar chart report to the table report. The report where the link is created is called the source report and the report that is linked to is called the destination report.
 The destination report has **HostGUID** and **ClientName** defined as run time parameters. So these parameters need to be passed from the source report. We have **ClientName** in the selection of the source report, and **HostGUID** will come from the filter on server or servergroup we have applied on source report.
- 4 Select the **Hyperlinks** screen to define the link with the destination report. The **Linked To** column shows the reports to which this report can be linked. Select *Job Details for Client* from the list for the **kBytes** field.
 The **Linked Report Parameters** column displays the run time parameters of destination report and the data fields of the source report which are of the same type as the run time parameter.
 Since we want to pass the value of **ClientName** to the destination report, select **ClientName**. HostGUID is passed internally so we do not have to specify it explicitly.



Click **Save Changes** to save and preview the report.

- 5 As a result, clicking on any bar of the *Data Backed up per client* report displays the destination report (*Job Details for Client*). This report is run

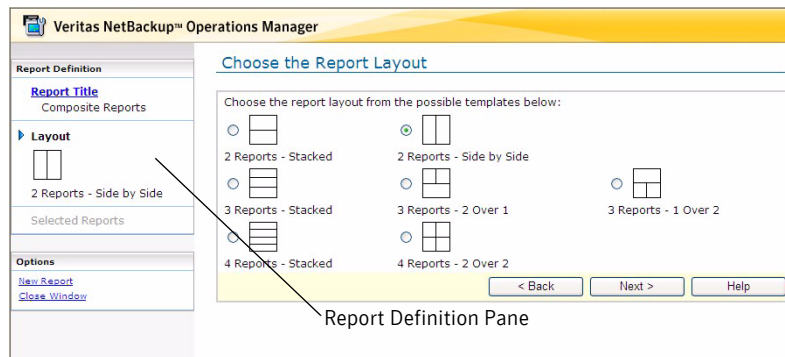
without the need of specifying the run time parameters since they are passed from the *Data Backed up per client* report.



Using the composite report builder wizard

The composite report builder wizard lets you create new reports from other existing reports. This feature lets you use existing key reports and generate a new report quickly.

The following figure shows a sample view of the composite report builder wizard.



The composite report builder wizard has a navigation frame on the left hand side. As you build a report, the navigation frame reflects the selections you make (the **Report Definition** pane on the left). You can return to any of these screens and edit them after you click **Finish**.

The following figure shows a sample composite report. The report contains two component table reports that appear side by side.

Attempt	ClientN	Elapse	JobID	JobTyp	JobDef
1	pmsun13	20.4	4	Backup	full
1	pmsun13	37.5	5	Backup	shard_full
1	pmsun13	18.6	6	Backup	shard_full
1	pmsun13	3,329.7	7	Backup	shard_full
1	pmsun13	416.8	8	Backup	shard_full
1		4.9		Image	Cleanup
1	pmsun13	50.10		Backup	shard_full
1	pmsun13	37.11		Backup	shard_full
1		5.12		Image	Cleanup

JobID	ExitSt	JobTy	Client	Start1	kByte	FileCc
56	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1
57	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1
58	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1
59	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1
60	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1
61	0	Backup	pmsun1:2007	Friday, May 11, 12:00:00 AM	32,768	1

To create a composite report

- 1 In the **Tasks** pane, click **New Composite Report**.
- 2 Follow the wizard instructions.

Using the composite report builder screens

To go back and change your report

- ◆ In the **Report Definition** pane, click a screen and follow the instructions for that screen.

To create another report without exiting the builder

- ◆ From the **Options** pane, select **New Report**.

To exit the report builder and not create a report

- ◆ From the **Options** pane, select **Close Window**.

The following sections explain the screens and tasks that NOM uses to build a composite report:

Identifying the report

To identify the report

- 1 Type a title and description for the report.
The report description appears in the **All Reports** view.
- 2 Type an existing folder name where you want to store the report. You also can click ... to use the **Pick Report Folder** dialog box. This dialog box lets you browse and select an existing folder, or create a new report folder.

Using the pick report folder dialog box

Do one of the following:

- ◆ Select an existing folder from the current folder tree.
- ◆ Type a path name for the new folder in **Folder name**. Use / to separate folders and subfolders.

Picking a format for the report

Select the display format you want for the new report. The available report formats depend on the number of component reports that comprise the new composite report.

To select a format for the report

- ◆ Select one of the available output formats in the wizard.

Selecting the reports that comprise your composite report

To select the data for the report

- ◆ Using the drop-down lists, select an existing report to include for each section of the new composite report.

When you click **Finish**, a preview of the new report appears.

Using the report scheduler wizard

You can schedule the run time for all reports - custom, or standard. You can select a one-time event or a recurring schedule for any report by using the report scheduler wizard. A recurring schedule can be one of the following types: an interval, a weekly schedule, or a monthly schedule.

You also can use the report scheduler to change an existing report schedule.

Any configured scheduled reports appear in the **Scheduled Reports** tab.

To schedule a report

- 1 Select **Reporting**.
- 2 From the tables of available reports in **Private Reports**, **Public Reports**, or **Standard Reports** select a report you want to schedule. You can also schedule a report after running a report.
- 3 From the **Tasks** pane, click **Schedule** to start the schedule builder wizard.

Using the report scheduler screens

The type of schedule you choose determines the wizard screens you use to schedule a report (not all of the screens are used for all schedules).

Note: The scheduler wizard uses the **My time zone** setting of the **Settings > Preferences** tab. If you see an unusual time in any schedule wizard screen, you should make sure that this setting is correct.

Selecting a schedule type (one-time or recurring)

To choose a schedule type for a report

Enter a name for the schedule and do one of the following:

- ◆ Select **Create a one-time event** for a report to run only once.
- ◆ Select **Create a recurring schedule** for a report to run periodically.

Specifying a date for a one-time report

To choose a date for the scheduled report

- ◆ Select the month (use << and >>), day, and time when you want the report to run.

Selecting a recurring report type (time, weekly, or monthly)

To choose a recurring schedule type

Do one of the following to choose a recurring report type:

- ◆ Select **Specify an Interval**.
- ◆ Select **Choose the days of the week**.
- ◆ Select **Choose the days of the month**.

Specifying a time for a recurring report

To specify how often to run the report

- 1 Specify a time interval for the report. Select the number of hours or days for the interval.

Specifying a schedule for a weekly recurring report

To choose the days of the week to run the report

- ◆ Select a day(s) of the week and the time for the report.

Specifying a schedule for a monthly recurring report

To choose the days of the month to run the report

- ◆ Select a day(s) of the month and the time for the report. Select **Last Day of Month** if you want to run the report on the last day of each month.

Specifying an activation date and time for a recurring report

After specifying a schedule for a weekly or monthly recurring report, you specify an activation date and time for your schedule. This should be done if you want to run the report on the last day of each month.

The scheduled report is not run until after this activation date and time occurs.

To specify when to activate the schedule

- ◆ Using the calendar, select a date and time to activate the report schedule.

Specifying email addresses and HTML format for the report

The list of registered users (recipients) also contains inactive users, since they may change to active before you generate the scheduled report. If a user is still

inactive when you generate the report, NOM removes the recipient from the mailing list.

For an active email group, the report is emailed to all members of the group. If a user is inactive but is included in an active group, the user receives the email. If your SMTP server is not configured, you first must configure the server. You can email reports in HTML without JavaScript or in Rich HTML formats.

To specify email addresses for recipients of this report

Do one of the following:

- ◆ Select an email address from the list of registered users and click **To**, **CC**, or **BCC** to add the address to the lists of recipients.
- ◆ Enter email addresses for recipients of this report in the **To**, **CC**, or **BCC** fields. Use semicolons (;) to separate multiple addresses.

To specify the HTML format for this report

See “[Available HTML formats for emailed reports](#)” on page 193 for more information about each of these formats.

- 1 Select **HTML without JavaScript** or **Rich HTML** format.
- 2 For **HTML without JavaScript** you can also select other options.

Specifying run time parameters for the scheduled report

Depending on the report you schedule, some report definitions may require that you specify run time parameters for the report before the report is run.

To specify an absolute time frame for the collected report data

- 1 Select **Absolute**.
- 2 In the **From** box, use the calendar icon to specify the start date.
- 3 In the **To** box, use the calendar icon to specify the end date.

To specify a relative time frame for the collected report data

While calculating relative time, SORD is considered if **Adjust relative time frame on SORD boundary** is selected at the time of schedule creation. See “[Setting preferences for NOM users](#)” on page 173 for information about the SORD.

For example, suppose the current time is 7 Sept 11:34 AM and the SORD is set as 8:00 AM. Also **Adjust relative time frame on SORD boundary** option in **Settings > Preferences** is selected. You select the time frame as 1 day relative, then the duration for the collected report data is from 7 Sept 8:00AM to 8 Sept 8:00AM.

- 1 Select **Relative**.
- 2 Specify the time (duration of the report) by using the text box and the drop-down list box. You can specify this time in hours or days. This time is the start time for the report.

To specify the NetBackup objects for this report

- ◆ Use the drop-down list boxes (for example, **Job type** or **Policy type**) to select the object criteria this report requires. Use the calendar to specify the **Reporting Day** parameter.

Specifying the server context for the report

Depending on the report you schedule, some report definitions may require that you specify a master server (or server group).

To specify the server context for this report

- ◆ Navigate the tree and select a master server or server group.

Using the report confirmation screen

Review and confirm that the schedule for this report is configured the way you want.

If the schedule is correct, click **Finish**. The new scheduled report appears in the **Scheduled Reports** tab.

Click **Back** to change the schedule.

Upgrading reports from 6.0 or 6.0MPx to 6.5

Some of the standard reports from the earlier 6.0 or 6.0 MPx releases have been deprecated and replaced with the new standard reports in NOM 6.5 to make them more usable. The following 6.0 and 6.0MPx standard reports have been deprecated:

Standard reports in NOM 6.0 and 6.0 MPx	Equivalent Reports in NOM 6.5	How the report has been changed in NOM 6.5
Catalog Files	Not Available	Report does not exist.
Catalog Size	Not Available	Report does not exist.
Hot Catalog Backup	Not Available	Report does not exist.

Standard reports in NOM 6.0 and 6.0 MPx	Equivalent Reports in NOM 6.5	How the report has been changed in NOM 6.5
Throughput Variance	Throughput Variance	Throughput variance, volume variance and file count variance reports have been modified from composite report to simple report in NOM 6.5.
Volume Variance	Backup Job Size Variance	
File Count Variance	File Count Variance	
Server Job Count	Master Server Job Throughput	Report has been renamed and modified.
Full Job Summary	Job Summary	The following 6.0 reports have been merged into a single report called Job Summary in NOM 6.5: <ul style="list-style-type: none"> ■ Full Job Summary ■ All Job Summary ■ Differential Incremental Job Summary, and ■ Cumulative Incremental Job Summary
All Job Summary		
Differential Incremental Job Summary		
Cumulative Incremental Job Summary		
Restore Job Summary	Restore Job Summary	Modified from a simple report to composite report.
Media Usage by Client	Not Available	Report does not exist
Job Success Rate by Policy Type	Job Success Rate by Policy Type	Modified from a simple report to composite report.

The following 6.0 and 6.0MPx standard reports have only been renamed in NOM 6.5:

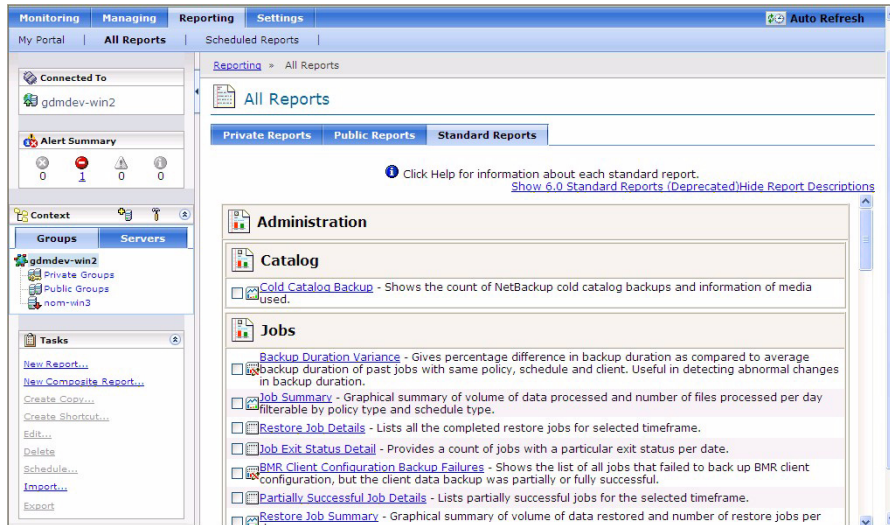
Standard reports in NOM 6.0 and 6.0 MPx	Equivalent Reports in NOM 6.5	How the report has been changed in NOM 6.5
Volume Utilization	Media Utilization	Report has been renamed.

Standard reports in NOM 6.0 and 6.0MPx	Equivalent Reports in NOM 6.5	How the report has been changed in NOM 6.5
Job Summary by Client	Job Success by Client	Report has been renamed.

On upgrading to NOM 6.5, the installer will not delete the deprecated 6.0 or 6.0MPx standard reports from the **All Reports** tab.

On upgrading to NOM 6.5, all deprecated 6.0 or 6.0MPx standard reports will be shown on a separate screen under the **Standard Reports** tab.

On upgrading to NOM 6.5, the **Standard Reports** tab will look like the following:



Click **Show 6.0 Standard Reports (Deprecated)** to see the deprecated standard reports in NOM 6.5.

Migrating to the new reports

You should perform the following steps to migrate these reports to the new NOM 6.5 reports.

- 1 Migrate all schedules to use new standard reports. If there are schedules built for the deprecated 6.0 reports, then you must recreate these schedules for the equivalent 6.5 reports.

You might find that some older schedules will have a "*" after the schedule

name like `schedule1*`. This is because some report runtime parameters might be missing for these schedules in NOM 6.5. Schedules marked with "*" will not work in NOM 6.5. These schedules must be edited to make them work.

- 2 It is recommended to move all the hyperlinks created on the deprecated 6.0 reports to the equivalent 6.5 reports.
 See "[To link to an existing report](#)" on page 205 to create hyperlinks on reports.
- 3 If any of the deprecated 6.0 Reports are present in **My Portal**, then it is recommended to remove those reports from **My Portal**. You can then add the equivalent set of 6.5 reports to **My Portal**.
- 4 After performing these steps, you can delete the old deprecated standard reports from NOM 6.5. To delete these reports, perform the following steps:
 - Add a property called "reports.deleteOldReports=true" in `nom_config.properties` file and then save this file.
 This file is present at the following location:
 On Windows:
`INSTALL_PATH\VRTSweb\VERITAS\nom_config.properties`
 On Solaris: `/opt/VRTSnom/webgui/nom_config.properties`
 - Restart NOM for these changes to take effect.

Note: It is recommended that you should delete the old deprecated standard reports. This should be done to avoid confusion due to a similar set of the new NOM 6.5 reports.

Upgrading reports from 6.0 or 6.0MPx to 6.5

Understanding NOM online help

Using the NetBackup Operations Manager online help is the best place to start to understand the capabilities and tasks in the console. Online help provides you with information to help you navigate to the NOM views you need and to use task dialog boxes and task wizards.

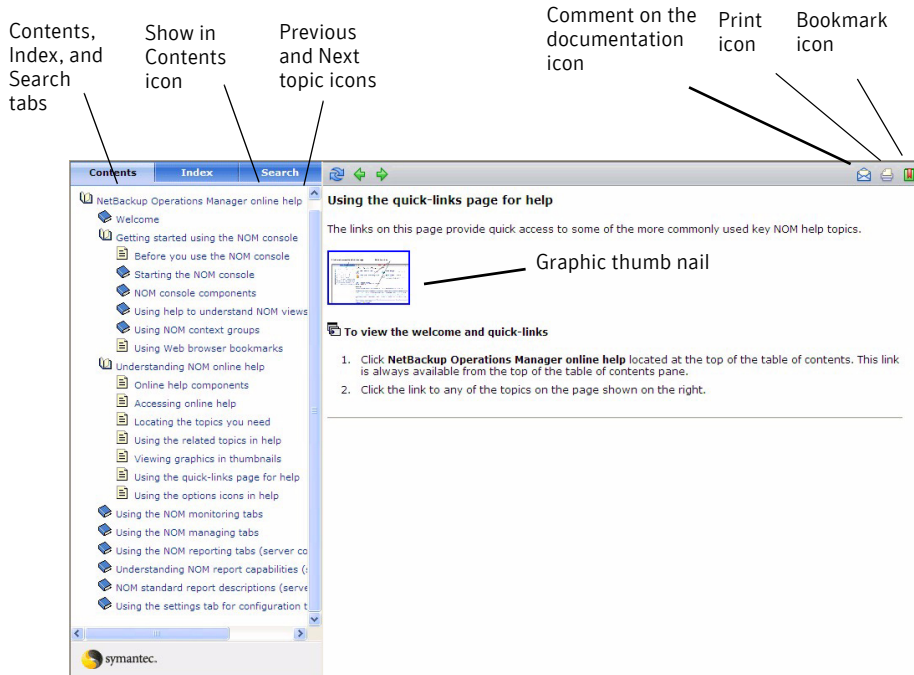
NOM has online help for most console views, tasks, and wizard screens.

The following topics describe online help usage in greater detail.

Topic	Description
“Online help components” on page 232	Provides an overview of the online help interface used, which includes the contents and search tabs, and the print icon
“Accessing online help” on page 232	Describes how to get help for views, dialog boxes, and wizard screens
“Locating the topics you need” on page 233	Describes how to find information you need, which includes how to use the table of contents, index, and search tools
“Using the related topics in help” on page 234	Describes the related help topics that are available
“Viewing graphics in thumbnails” on page 234	Describes how to expand the graphics that appear as thumbnails in some help topics
“Using the quick-links page for help” on page 234	Describes how to access some of the more commonly used NOM help topics quickly
“Using the options icons in help” on page 235	Describes how to send a comment on the help, print a topic, or bookmark a topic

Online help components

The following figure shows the help control and access components.



Accessing online help

Online help is available for most views, dialog boxes, and wizard screens in NetBackup Operations Manager.

To access help for the current NOM view

See "[NOM console components](#)" on page 116 for the location of the **Help** option.

- ◆ Click **Help** in the upper-right corner of the console header.
The help page appears, based on your currently selected view in NOM.

To access help for a dialog box or wizard

- ◆ Click **Help** from the task dialog box or wizard screen.
The help page appears, based on the current dialog box or wizard screen.

Locating the topics you need

You can navigate and locate the help you want by using any of the following methods. See “[Online help components](#)” on page 232 for the location of these help icons.

To view the table of contents for the help

This view presents the table of contents for all the NOM help topics that are available.

- ◆ If the table of contents is hidden, click the closed book icon which is located in the **Contents** tab.

To use the table of contents

- ◆ Click any closed books to open them and drill down to expand the view of available help topics.

To locate the current help topic in the table of contents

This help feature shows you the location of the topic currently on display within the table of contents.

- ◆ Click the **Show in Contents** icon.
In the table of contents, the book icons expand to show the location of the current topic.

To use the index of topics

- 1 Click **Index**.
- 2 Click a letter to view the indexed terms for that letter.

To use the key word search

If you enter multiple key words, the resulting topic links contain each of the key words, but not necessarily together as a phrase.

- 1 Click **Search**.
- 2 Enter a key word(s) for the search and click **Go!**
The resulting topic links are weighted based on the number of key word matches in the topic. The first topic in the list has the maximum rank and is the most likely match for the search.

To navigate from the current help topic to the next or the previous topic

You can navigate from the help topic currently on display to other related topics. The order in which the topics appear is based on their order in the table of contents.

- ◆ Click the **Previous** or the **Next** icons that appear at the top of all help topics.

Using the related topics in help

Many NOM help topics include **Related Topics** sections at the end. Use these related links to access more information on concepts or topics.

Viewing graphics in thumbnails

Many help topics include a graphic image that initially appears in a compressed thumbnail form. You can open and view the graphic when needed.

To view the expanded graphic

- ◆ Click the graphic image.

To return to the help topic

- ◆ Click the back button of your browser.

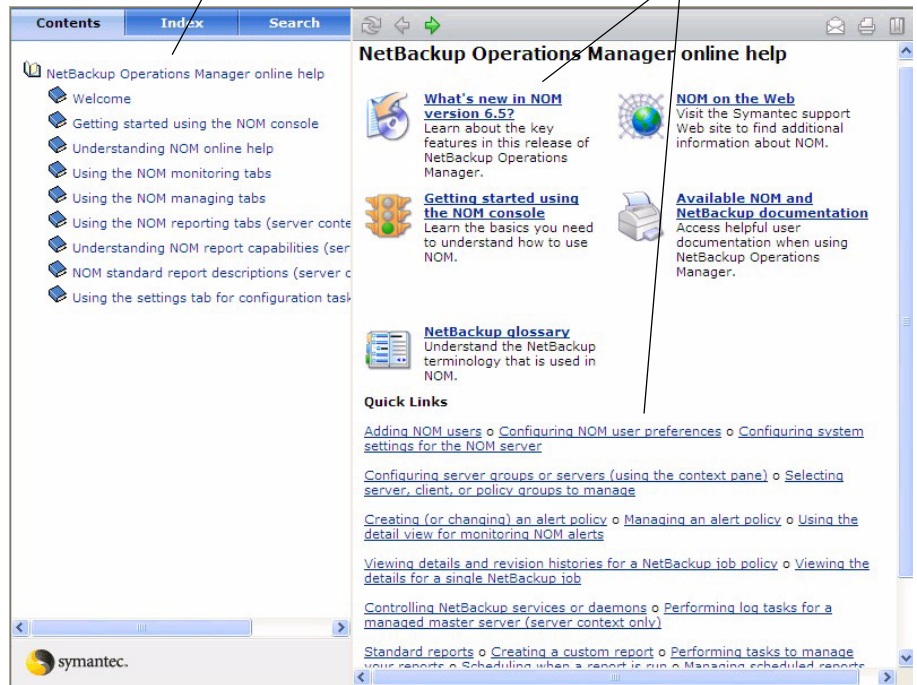
Using the quick-links page for help

The links on this page provide quick access to some of the more commonly used key NOM help topics.

The following figure shows the welcome and quick-links help page.

Click here to access the quick-links page

Quick help links



To view the welcome and quick-links

- 1 Click **NetBackup Operations Manager online help** located at the top of the table of contents. This link is always available from the top of the table of contents pane.
- 2 Click the link to any of the topics on the page which is shown on the right.

Using the options icons in help

See “[Online help components](#)” on page 232 for the location of these help icons.

To send an email about help issues

You can send email with any comments, questions, or suggestions regarding the online help to the NOM documentation team. NOM uses the URL of the last help topic that you opened as the default feedback subject for the email.

- 1 Click the **Comment on the documentation** icon.

- 2 Enter your comment or suggestion.
- 3 Click **Send**.

To print the current help topic

You can print the current topic by using your Web browser.

- 1 Click the **Print** icon.
- 2 In the print dialog box for your operating system, select a printer and adjust the printer settings as required.
- 3 Click **Print**.

To bookmark the current help topic

You can add the current topic to your Web browser's favorites list.

- 1 Click the **Bookmark** icon.
- 2 Follow the instructions in the dialog box.
- 3 Complete your Web browser's bookmark dialog box.

Index

A

- activation date, for a recurring scheduled report 224
- Active Directory 93
- ActiveX 27
- adding
 - client groups 138
 - policy groups 138
 - server groups 136
 - servers 134
- adjust relative time frame on SORD boundary 174, 175
- alert manager (VRTSamnom) 19, 25
- alert policies
 - creating 144
 - managing 148
 - understanding 144
- alert policy wizard 144
- Alert Summary pane, using 120
- alerts
 - displaying 149
 - modification time 150
 - notification email contents 149
 - removing from database 150
 - responding to 152
 - setting up recipients 149
 - viewing 151
- authentication service fields 54
- Authentication service GUI 92
- authentication service wizard, Windows server 38
- authentication service, Windows server 40

B

- bookmarks, using with NOM 141

C

- changepasswd, vssat command 92
- changing administrator passwords 59, 112
- changing NOM administrator passwords 88, 92
- changing the NOM admin password 88

- client groups
 - changing 138
 - NOM predefined private groups 122
 - NOM predefined public groups 122
 - removing 139
 - understanding 121
 - user-defined groups 122
 - viewing by drilling down 140
 - viewing using the Context pane 140
- color coding, in NOM 124
- composite report
 - creating 220
 - using the report builder 221
- configuring
 - data display time zone 174
 - default email format 176
 - start of your reporting day (SORD) 175
- Connected To pane, using 119
- Content pane
 - enlarging 123
 - Summary and Details tabs 123
 - using 123
- Context pane
 - configuring client groups 137
 - configuring policy groups 137
 - configuring servers and server groups 133
 - groups and server tabs 121
 - minimizing 121
 - using with alert policies 144
- controlling jobs 161
- controlling NOM services and processes 67
- copying a private report 181, 192
- creating alert policies 144
- cross navigation 118
- custom reports
 - filtering options 203
 - linking reports 205
 - optional screens 201
 - required screens 196

D

data display time zone 173, 189
 data load status, for NBSL connections 171
 database, see (NOM database) 69
 default Email format 174
 default group context 173
 default language 173
 deleteAlerts 70
 dependency of NOM services 69
 documentation
 for Sybase 69
 NBSL 30
 NetBackup 110
 NOM 20
 VRTSweb 25, 95
 VxUL 25

E

email client support 27
 email formatting options for reports 192
 emailing NOM reports 176, 192
 example SQL queries 207

F

finding
 more information about NOM 20
 online help topics 233
 firewall considerations 93

G

getting started with typical NOM tasks 131
 group component summaries 166
 Groups tab 133, 140

H

hardened servers 34, 48
 help
 accessing the online help 232
 online help overview 231
 tools for locating information 233
 using the graphic thumbnails 234
 using the help icons 235
 using the quick-links page 234
 using the Search tool 233
 using the Show in Contents icon 233
 HTML formats for reports 193

HTML without JavaScript, email format 176, 193,
 225
 HTTP 95
 HTTPS 95

I

icons for managed server status 124
 ICS CD, software components 31
 initial login by an administrator 59, 92, 112
 install script, Solaris SPARC 53
 installing
 NetBackup on the NOM server 36, 49
 NOM software 41, 53
 NOM, planning 24
 Symantec Private Branch Exchange on the
 NOM server 49
 Symantec Product Authentication Service on
 the NOM server 49
 the authentication service on the NOM
 server 36

J

JavaScript 27, 176, 177, 193
 Job State Changed, alert policy 146
 jobs
 controlling 161
 tracing 157

K

Korn shell 82

L

LDAP (Lightweight Directory Access Protocol) 93
 License Capacity Alert 151
 linking reports 205
 log files
 on Solaris SPARC servers 105
 on Windows servers 103
 retention period 159
 verbosity settings 160
 viewing and filtering 157
 logging
 into NOM 92, 112
 out of NOM 114
 Lotus Notes 27, 193

M

- managed NetBackup servers 20
- managed server icons 124
- Management Information Base (MIB) 154
- Master Server Unreachable condition 146
- master server, time zone option 174
- McAfee Antivirus considerations 35
- media kit 31
- Microsoft Internet Explorer 27
- Microsoft Outlook 27
- Mozilla Firefox 27
- Mozilla Thunderbird 27
- my portal tab, limit 180
- my time zone 173, 223

N

- NetBackup DVD, software components 32
- NetBackup servers not using NBAC for security 56
- NetBackup Service Layer (NBSL) 30, 95, 170
- NetBackup services, (see services) 162
- NetBIOS considerations 34
- Netscape 27
- Network Address Translation (NAT) network considerations 29
- Network Information Service (NIS) 93
- NightlyBackup database script 78
- NOM
 - color keys 124
 - log files 100
 - software components on NOM CD 32
 - software components on NOM DVD 33
 - status bar 124
 - status icons 124
 - Sybase database used 19, 25
 - tasks performed on startup 59
 - understanding the basic components 16
 - web client 18, 19
 - what is it? 12
- NOM admin password, changing 88
- NOM admin user 92
- NOM back up and restore procedures 77
- NOM client groups, (see client groups) 132
- NOM cross navigation link 118
- NOM database
 - back up using NetBackup and NightlyBackup script 77
- NOM database password file 84
- NOM database utilities

- change database administrator password 70
- change database administrator password for guest users 71
- change port number 71
- controlling NOM services 68
- controlling the database server 68
- display version information 72
- export NOM databases 72
- import NOM databases 72
- purge and save NOM alerts and job data 73
- purge old NOM alerts 72
- starting NOMAdmin 69
- NOM installation
 - before starting
 - on Microsoft Windows 34
 - on Solaris SPARC 48
 - choosing a server for NOM 25
 - GDM and NBAR considerations 28
 - NetBackup media kit contents 31
 - on Microsoft Windows 34
 - on Solaris SPARC 47
 - web browser considerations 26
- NOM policy groups, (see policy groups) 132
- NOM post-installation
 - starting to use NOM 59
- NOM processes, on Solaris SPARC 65
- NOM server
 - guidelines and sizing recommendations 26
 - name length limit (Windows) 35
 - platform support 26
- NOM server scripts, Solaris SPARC 66
- NOM services, on Microsoft Windows 64
- NOM start-up tasks 59
- NOM title bar link 118
- NOM user profiles 84
- NOM users 92
- NOMAdmin (see NOM database utilities) 69
- number of rows per page in tabular reports 174

O

- offline, server status 170
- online help, (see help) 231
- online, server status 170
- originator ID 102

P

- partially online, server status 170, 172
- performance tuning 60

- pick report folder dialog 196, 222
- policy groups
 - changing 138
 - NOM predefined private groups 122
 - NOM predefined public groups 122
 - removing 139
 - understanding 121
 - user-defined groups 122
 - viewing by drilling down 140
 - viewing using the Context pane 140
- pre-installation checks 34, 48
- private groups 122
- private report, copying 181
- private reports 181
- product ID 102
- public groups 122
- public reports 181
- purge 70
- purging old NOM alerts 72, 73

Q

- quick start for NOM tasks 131

R

- read-only database view for guest user 71
- refresh mode control, using 119
- registry key considerations 34
- regular expression (PCRE) search 159
- related NetBackup documentation, locating 110
- remote APIs 36, 49
- reports
 - Advanced Options pane 201
 - configuring reporting cycles 172
 - create reports from existing reports 220
 - creating custom reports 186
 - optional tasks 201
 - required tasks 196
 - data tooltips 198
 - emailing formats 192, 224
 - linking reports 205
 - my portal limit 180
 - rerunning 189
 - running 187
 - sample report 211
 - sample report linking 218
 - scheduling 223
 - shortcuts to 181
 - SQL grammar 207

- standard descriptions 182
- title tooltips 198
- restoring NOM 85
- Rich HTML, email format 177, 193, 225
- Root + Authentication Broker (Root + AB) mode 38, 50
- run time parameters 187, 188

S

- samples, creating a custom report 211
- scheduled reports
 - creating a one-time report 223
 - creating a recurring report 224
 - managing the schedule 185
 - specifying the activation date 224
- security options page 54, 55
- security, deployment models 88
- Sender Email ID 178
- server groups
 - adding 136
 - changing 136
 - NOM predefined private groups 122
 - NOM predefined public groups 122
 - removing 137
 - user-defined groups 122
 - viewing by drilling down 140
 - viewing using the Context pane 140
- server name length limit 35
- server scripts for NOM, Solaris SPARC 66
- servers
 - adding 134
 - changing 135
 - removing 136
 - viewing by drilling down 140
 - viewing using the Context pane 140
- servers hardened for security 34, 48
- Servers tab 133
- services
 - controlling 162
- shortcut for private reports 181
- Show Query, for generated SQL 195
- Simple Network Management Protocol (SNMP) 153
- SMTP Server Name 177
- SMTP Server Port 177
- SNMP in NOM 96
- SNMP traps 96
- software components used by NOM 24
- SORD (start of reporting day) 175
- SQL grammar supported by NOM 207

- SQL sample queries 207
- standard reports 181
- start of reporting day (SORD) 174, 175, 225
- start-up tasks, NOM server 59
- status icons in NOM 124
- supported
 - email clients 27
 - managed NetBackup server platforms 29
 - NOM server platforms 26
- Symantec Firewall (Client Security)
 - considerations 35
- Symantec Private Branch Exchange
 - port number configuration 24
- Symantec Private Branch Exchange (VxPBX) 24
 - installing 42, 50
 - port number configuration 95
- Symantec Product Authentication Service
 - considerations 36, 87
 - installation 36, 49
 - shared component 24

T

- tables in NOM
 - applying filters 130
 - creating custom filters 129
 - customizing 126
 - editing custom filters 130
 - selecting rows 128
 - sorting 127
 - using filters 129
 - viewing hidden columns 126
 - viewing multiple pages 128
- Tasks pane, minimizing 123
- time zone options 174
- tool tips 125
- troubleshooting
 - accessing NOM 111
 - logging into NOM 113
 - NetBackup using NOM 157
 - NOM server issues 100, 114
 - support script in NOM 96
- tuning NOM for performance 60

U

- unified logging (VxUL) 102
- upgrading, GDM or NBAR installations 28
- user-defined context groups 122

V

- VBR cross navigation link 118
- VBR title bar link 118
- verbosity settings 160
- Veritas Backup Reporter (VBR) 118
- Veritas Unified Logging (VxUL)
 - log files 102
 - originator IDs used by NOM 102
 - shared component 25
- Veritas Web Server (VRTSweb) 25, 42
- visual keys, in the NOM console 124
- VRTSjre (Java Run Time Environment) 25
- VRTSweb installer issues 48
- vssat command 92

W

- web browser
 - book marks 141
 - default language 173
 - pop-up blockers 27
 - support 27

