WHITE PAPER: DATA PROTECTION

symantec.
Confidence in the connected world.

NetBackup Operations Manager: Monitoring, Alerting and Reporting for Veritas NetBackup

Erica Antony and Tim Burlowski | January 2008

White Paper: NetBackup Operations Manager: Monitoring, Alerting and Reporting for Veritas NetBackup

Content

Introduction

NetBackup Operations Manager (NOM) was introduced with Veritas NetBackup 6.0. It is a core component of the product providing advanced operational monitoring, alerting, troubleshooting and reporting. Designed to support NetBackup administrators and the operations team, NOM is focused on real-time, centralized monitoring across the NetBackup environment.

Some of the highlights covered in this document include:

- Advanced Operational Management Capabilities in NOM – Key Features and Benefits
- NOM and Veritas Backup Reporter – The Complete Management & Reporting Solution

Advanced Operational Management

Monitoring

NOM provides monitoring and management across multiple NetBackup servers. Communication between the NOM server and NetBackup managed servers is continuous, providing a real-time view of operations. A select subset of servers can be monitored using advanced data filtering options. Custom or ready-to-use filters allow only information satisfying the defined conditions to be presented. For instance, a filter may be applied to display only jobs for a specific client or policy, or to include/exclude certain exit status codes. These views might be critical in quickly communicating backup health of a particular customer's environment or identifying issues with a set of mission critical systems.

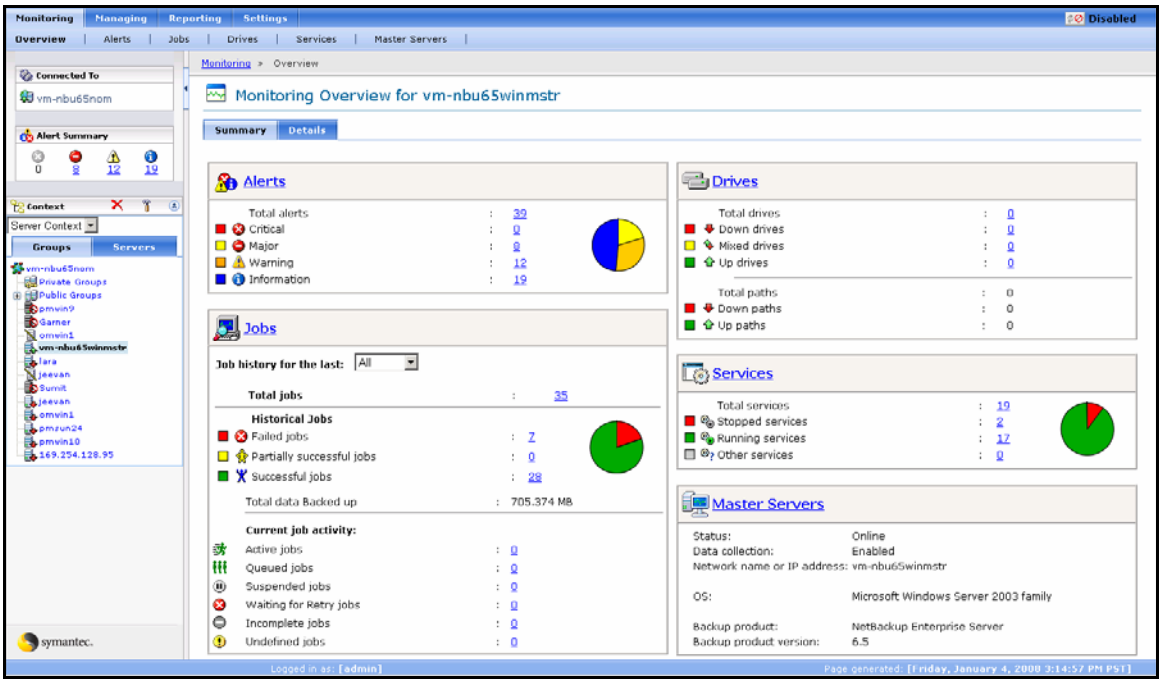

Figure 1: Example of the NOM Monitoring page

Web-based administration

Often the greatest challenge with globally distributed, complex enterprise data centers is remote administration. Issues range from slow connections that require significantly increased administration time to installations with large system footprints that consume 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. There is little system resource impact as there are no local installation requirements beyond the browser platform.

Real-time View of Operations

NetBackup and NOM communication is designed to be real-time, leveraging more of a “push” style of data collection instead of a “pull” or polling type method, which is generally leveraged by standalone data protection reporting offerings. NOM uses the NetBackup Service Layer infrastructure to subscribe to events from NetBackup. Once events are received by NOM, NOM then stores and aggregates this data in a relational database for later use in monitoring and reporting.

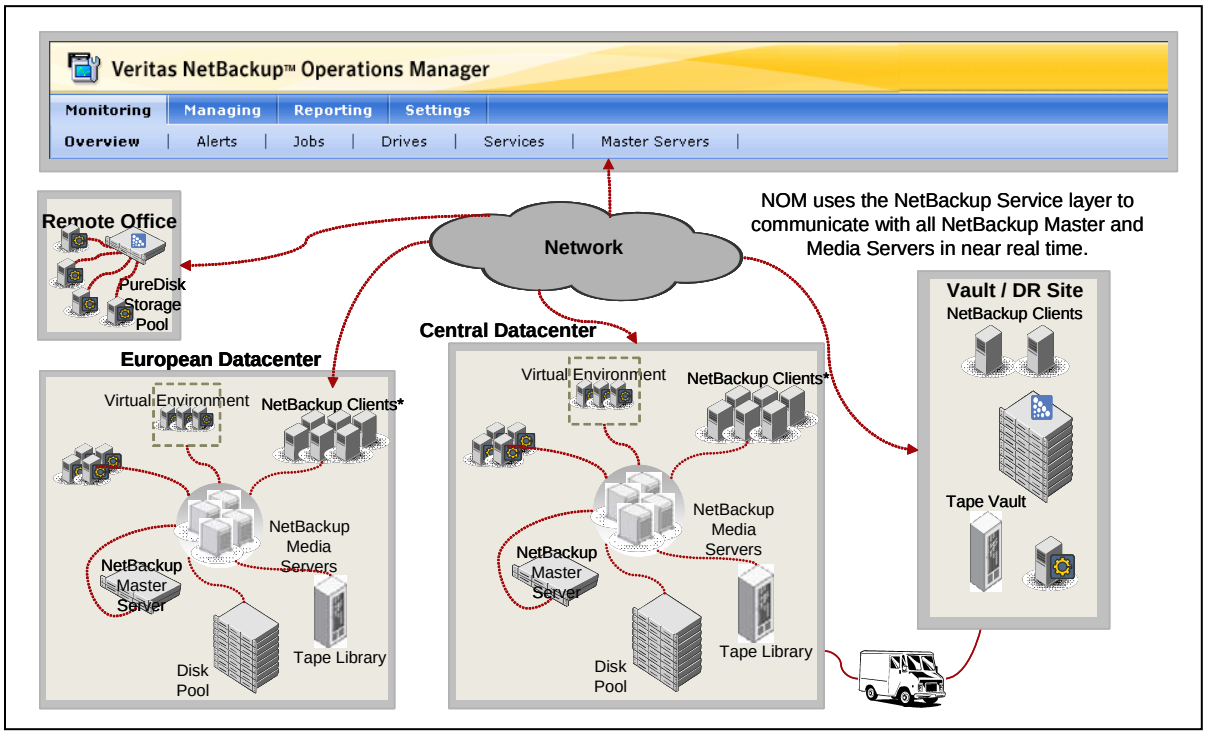

Figure 2: NOM Architectural Diagram showing the management of many NBU Servers

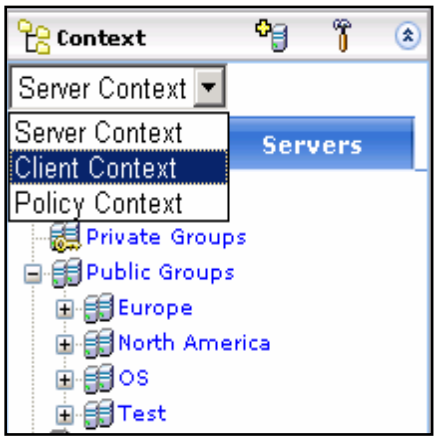

Figure 3: Contextual Grouping

Server & Policy Grouping

NOM was designed to support monitoring and managing many master servers. Our grouping capability enables context-specific monitoring and alerting. It was introduced at a master server level with NetBackup 6.0. If two master servers are configured in a group, only jobs, policies, services, etc., that are specific to those backup domains are presented when that group context is selected. The grouping functionality was extended in NetBackup 6.5 to include client and policy grouping which enables a more granular view of the environment. This is especially beneficial for application monitoring where specific clients make up the application, or a certain subset of backup polices represent the entire protection policy.

Alerting

NOM offers real-time, policy-based alerting, including a set of predefined alert definitions that cover typical problem scenarios. Alert policies have configurable parameters to allow flexibility for unique conditions or distinguishing severity. They can be set up for notification through email or SNMP.

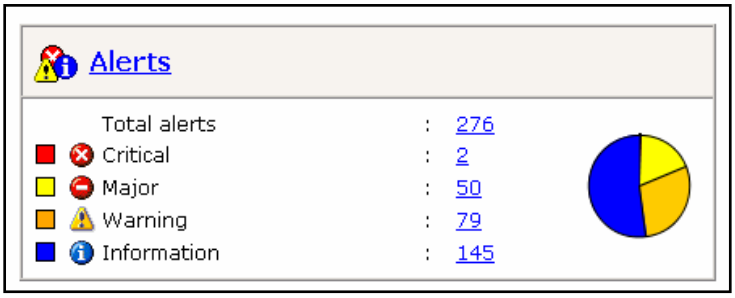

Figure 4: Alerts can be created with different severities.

Alert Conditions

All alert policies have user-configurable attributes and thresholds or parameters. Each alert can be assigned a name, description, severity level, recipient and status (active/inactive). While most alerts can be configured for activation with default parameters, each has unique conditions to accommodate specific alerting needs for the various recipients.

Table 1 Available Alert Conditions (Version indicates the earliest release when the alert condition was available)

Name	Conditions	Version
Catalog Backup Disabled	N/A	6.0
Catalog not Backed Up	Time period in days, hours, minutes	6.0
Catalog Space Low	Threshold % or Size (MB, GB, etc.)	6.0
Drive is Down	Media server, robot	6.0
High Down Drives	Threshold %	6.0

Name	Conditions	Version
High Frozen Media	Threshold %	6.0
High Job Failure Rate	Threshold %, time period in days/hours/minutes, exit status (all, include, exclude)	6.0
High Suspended Media	Threshold %	6.0
Hung Job	Time period in days/hours/minutes, policies, clients	6.0
Job Finalized	Job type, exit status (all, include, exclude), policies, clients	6.0
Lost Contact with Media Server	N/A	6.0
Low Available Media	Threshold %	6.0
Master Server Unreachable	N/A	6.0
Mount Request	N/A	6.0
No Cleaning Tape	N/A	6.0
Service Stopped	Service Name	6.0
Zero Cleaning Left	N/A	6.0
Disk Volume Down	Disk Volume	6.5
Disk Volume Full	Disk Volume	6.5
Exceeded Maximum Mounts	Number of mounts, media server, individual media	6.5
Frozen Media	Media server, individual media	6.5
Low Disk Volume Capacity	Threshold %	6.5
Media Required for Restore	Policies, clients	6.5
Job Policy Change	Policies	6.5
Suspended Media	Media server, individual media	6.5

Integration with 3rd Party Event Management Frameworks

A common way to integrate with 3rd party event management frameworks – like Microsoft Operations Manager (MOM), HP Openview or CA Unicenter – is through SNMP traps. NOM alerts can be configured for delivery through SNMP trap forwarding. Some configuration in the 3rd party event management console may be required to receive and "translate" the alert as a notification from NetBackup. Additional details on NOM alerts (MIB definitions, etc.) are available in the product documentation as well as in online technotes.

Sort & Filter

Advanced filtering provides a facility to monitor NetBackup objects based on specific criteria. Filters can be configured for each of the monitoring areas including policies, drives, media, alerts, jobs and services. There are default filters for standard conditions like policy enabled/disabled, job status (partial, success, incomplete, success, etc.), and frozen/suspended media. Filters are completely customizable and saved on a per-user basis for unique monitoring requirements.

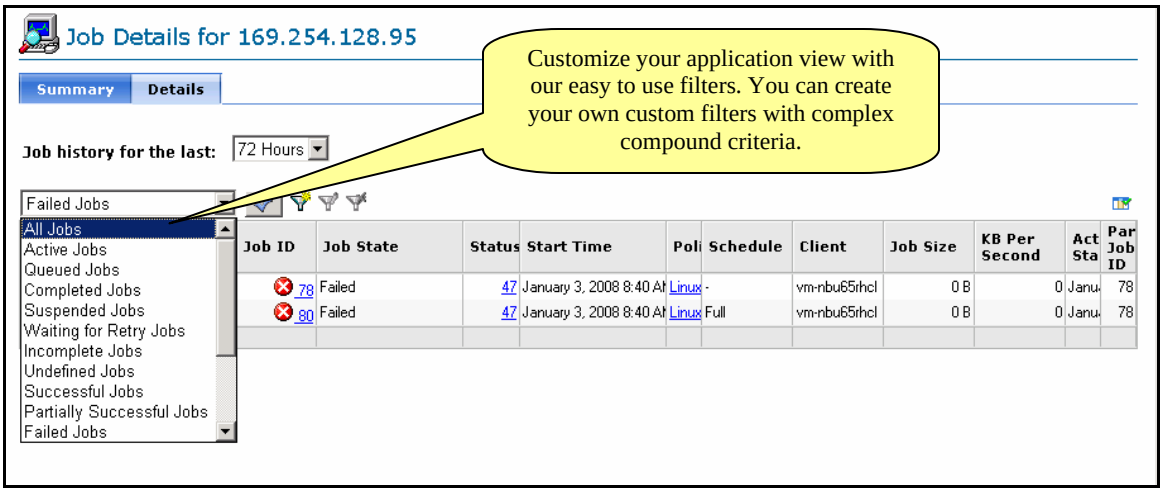

Figure 5: Filter Customization

Troubleshooting

Troubleshooting remains one of the most time consuming responsibilities for administrators. NOM reduces time to resolution by way of job and server drill-down, advanced data filters and sorting methods, and job-context log viewing.

Logging

Centralized viewing and management of NetBackup job and debug logs is provided through the NOM interface. Using NOM, a failed job can be traced to the problem source with a push-button operation to collect and export all logs related to a particular job.

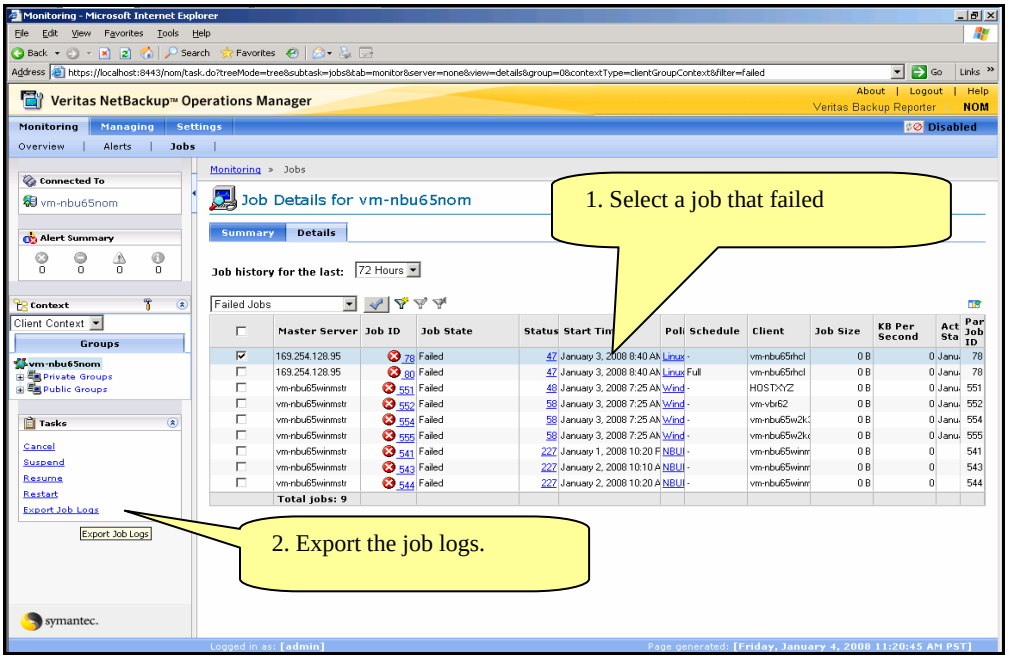

Figure 6: Log export

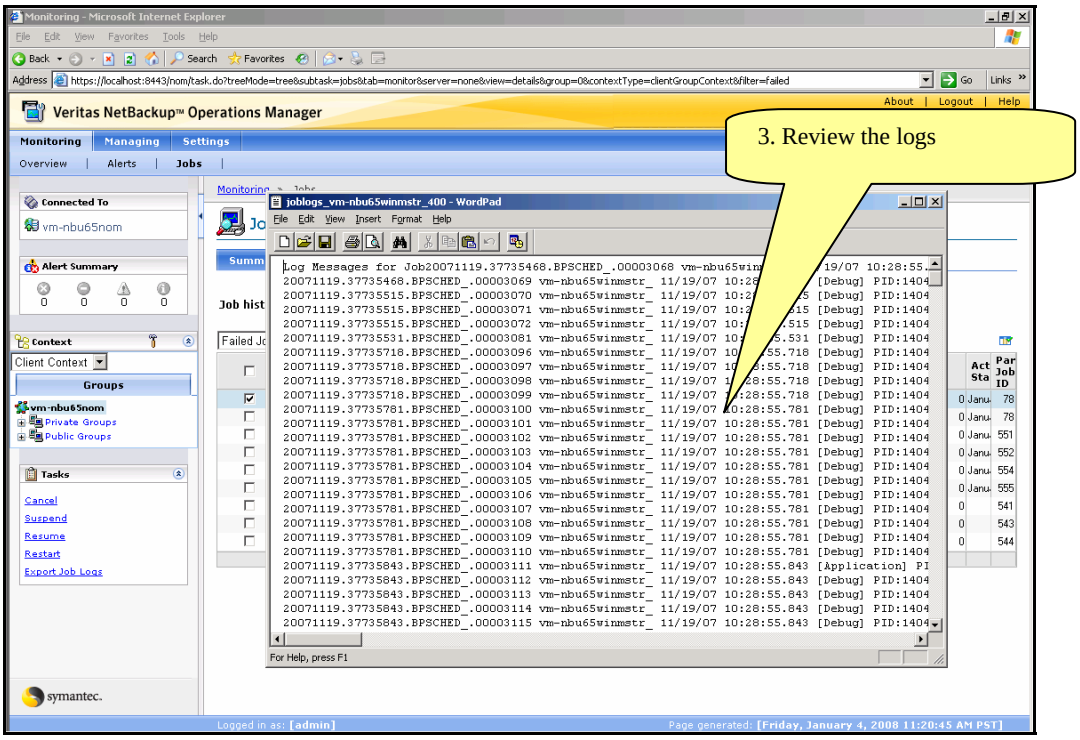

Figure 7: Log Review

Error Code Analysis

Job exit status codes are linked to related troubleshooting guide information for streamlined problem resolution. Additionally, operational reports are available to analyze error code distributions and focused troubleshooting efforts.

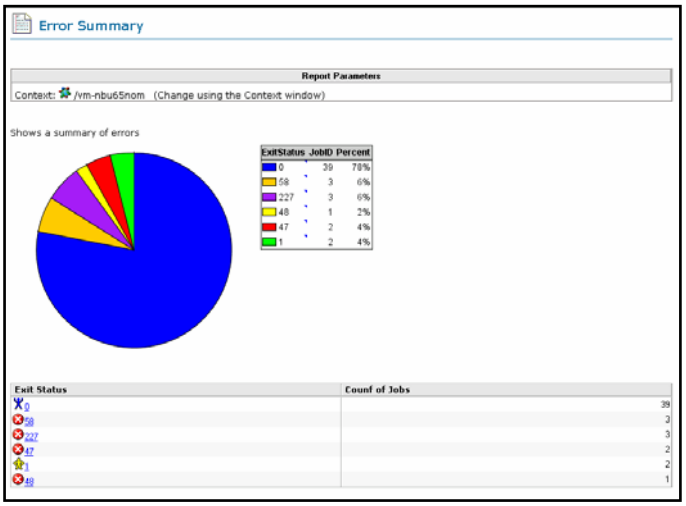

Figure 8: Report Showing Distribution of Job Exit Status

Operational Management

In addition to multi-site roll-up and visibility, NOM enhances operations with active management features. Examples of operational management tasks within NOM include media freeze/unfreeze, job start/stop/suspend/restart, drive up/down/reset and NetBackup service up/down. All of the active management functions are

available for each NetBackup domain monitored by NOM.

Policy Change History

Changes to individual backup policies are captured in NOM. From the time a NetBackup domain is added to a NOM server for monitoring, each policy change is recorded and the history preserved for analysis of one version to the next. The "what" and "when" detail for policy changes is available at a single policy level, or a standard report can be executed to show the count of policy changes over a given time period by an individual NetBackup domain or backup policy. Looking forward, the change history will be extended to include other NetBackup objects and actions, as well as to add the "who" component of the audit record.

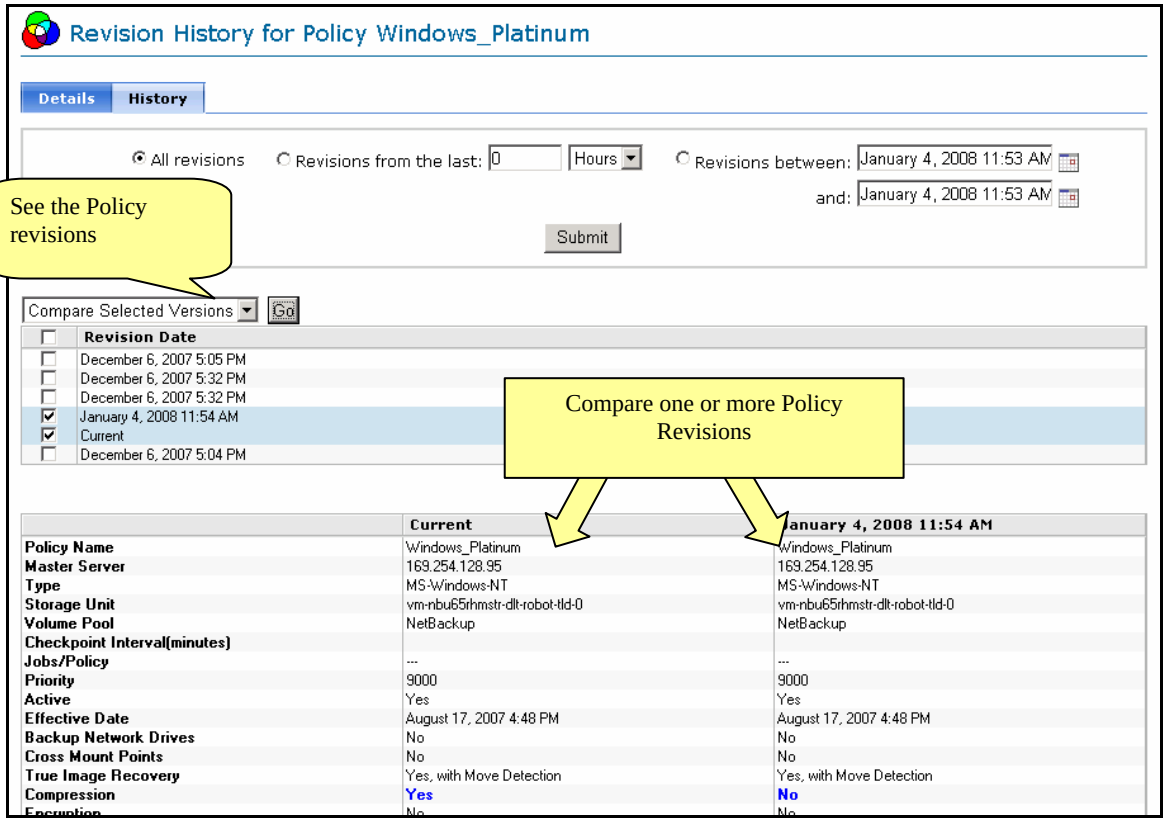

Figure 9: Revision History for Policies

In NetBackup 6.5, the policy change tracking was enhanced with an alert policy for real-time notification of policy updates.

Reporting

Immediately assess the status of operations through standard, point-and-click style reports on jobs, catalog backups, media and devices, policies, clients and performance. Reports can be configured to display in a traditional tabular format or optionally through a graphical representation.

The standard report set is designed for the operations team, focusing on data needed for effective day-to-day monitoring and management of the NetBackup environment.

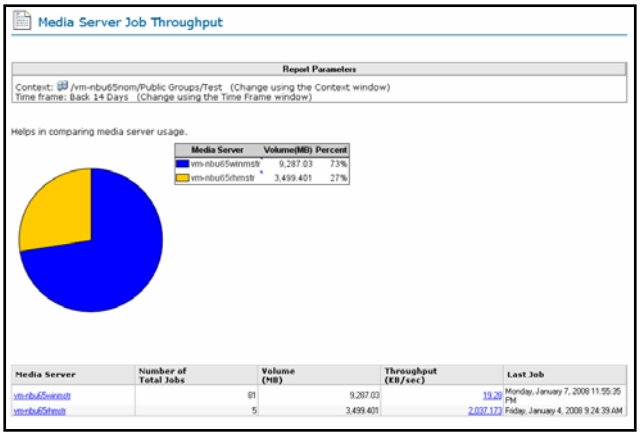

Figure 10: Example report showing Media Server aggregate throughput

Table 2: Standard Reports

Report Name	Description	Version
Available Media Report	Lists all the available media.	6.0
Client Restore	Lists all the restore jobs of the given client.	6.0
Cold Catalog Backup	Shows the count of NetBackup cold catalog backups and information of media used.	6.0
File Count Variance	Gives percentage difference in backup file count as compared to average backup file count of past jobs with same policy, schedule and client. Useful in detecting abnormal changes in backup file count.	6.0
Full Media Capacity	Useful to find out average size of full media for each media type in your backup environment.	6.0
Job Details	This report shows the jobs details for selected job types, policy types and schedule types.	6.0
Job Exit Status Detail	Provides a count of jobs with a particular exit status per date.	6.0
Job Success Rate by Policy Type	Displays the success rate per client, server, and policy type.	6.0
Job Summary	Graphical summary of volume of data processed and number of files processed per day filterable by policy type and schedule type.	6.0
Job Summary by Client	This report shows the Job Summary by Client.	6.5
Job summary by status	This report shows the successful, partial and failed jobs summary for selected job types, policy types and schedule types.	6.0

Report Name	Description	Version
Jobs by Application	Summarizes total data backed up and total files by policy type, per client and server.	6.0
Media State	Lists number of media in each media status per media type and per media server.	6.0
Partially Successful Job Details	Lists partially successful jobs for the selected timeframe.	6.0
Policy Change	Provides a count of the changes made to each job policy per master server.	6.0
Restore Job Details	Lists all the completed restore jobs for selected timeframe.	6.0
Restore Job Summary	Graphical summary of volume of data restored and number of restore jobs per day.	6.0
Backup Job Size Variance	Gives percentage difference in backup size as compared to average backup size of past jobs with same policy, schedule and client. Useful in detecting abnormal changes in backup size.	6.5
Backup Duration Variance	Gives percentage difference in backup duration as compared to average backup duration of past jobs with same policy, schedule and client. Useful in detecting abnormal changes in backup duration.	6.5
Backup Window Failures	Lists jobs failing because backup window was closed.	6.5
BMR Client Configuration Backup Failures	Shows the list of all jobs that failed to back up BMR client configuration, but the client data backup was partially or fully successful.	6.5
Client Summary Dashboard	Summarizes jobs data on various parameters per client.	6.5
Clients Not Backed Up	Lists all the clients not backed up within a given time frame.	6.5
Current Disk Usage	Current disk usage.	6.5
Cycle Dashboard	This report shows jobs summary for the selected cycle and week of the reporting day.	6.5
Cycle Dashboard by Job Type	This report shows jobs summary by job type for the selected cycle and week of the reporting day.	6.5
Cycle Dashboard by Media Server	This report shows jobs summary for the selected cycle, media server and week of the reporting day.	6.5
Disk Usage	This report shows the disk usage for selected server for the selected timeframe.	6.5
Drive Usage	This report shows the drive usage for selected server for the selected timeframe.	6.5
Drives in Use	Report gives details of drives that are currently in use.	6.5
Job Success by Client	This report provide job summary along with the success rate by client.	6.5

Report Name	Description	Version
Job Success Rate by Policy Type	Displays the success rate per client, server, and policy type.	6.5
Jobs Scheduled to Run	This report shows a list of jobs to be executed.	6.5
License Capacity	This report shows all the capacity-based licenses and the actual usage per disk type.	6.5
Master Server Job Throughput	Useful in comparing master server usage and performance.	6.5
Media Expiration Schedule	Stacked bars representing number of media getting expired on a particular reporting day.	6.5
Media Server Job Throughput	Helps in comparing media server usage.	6.5
Media Summary by Media Server	Media summary by media server.	6.5
Media Utilization	Plots graphical summary and lists tabular details of media count by media status and media type.	6.5
Policy Summary Dashboard	Summarizes jobs on various parameters per policy.	6.5
Rolling 8 Day Summary	This report shows the Rolling 8 day Summary. Jobs are represented using icons (mapping to job type and status) and colors (mapping to schedule Type).	6.5
Rolling 8 Day Summary by Media Server	This report shows the Rolling 8 day Summary by Media server. Jobs are represented using icons (mapping to job type and status) and colors (mapping to schedule Type).	6.5
Running vs. Queued	This report shows comparison between running and queued jobs.	6.5
SAN Client Jobs	This report shows the jobs for given client and media server. This also displays whether a job is a FT job or not.	6.5
Skipped Files Summary	Gives breakdown of skipped files by policy and client and allows drilling down to details.	6.5
Storage unit usage	This report shows the storage unit usage for selected server for the selected timeframe.	6.5
Throughput Variance	Gives percentage difference in job throughput duration as compared to average job throughput of past jobs with same policy, schedule and client. Useful in detecting abnormal changes in job throughput.	6.5
Top 10 Policies Using most Server Space	Lists the top 10 policies backing up most data.	6.5
Vault Media Usage	Report shows offsite media trend for selected vaults and current offsite media count.	6.5

Report Name	Description	Version
Week at a glance	This report shows weekly job summary for selected clients.	6.5
Window Utilization by Policy	This report shows the window utilization by policy for a particular day.	6.5

Report Operations

All reports can be scheduled for execution and also configured for communication through email. Regular status updates can be sent to management, customers, application owners and other interested parties in an automated fashion with frequency-based report scheduling.

While the predefined report set is designed to meet the most common requirements for NetBackup reporting, customers often require a very specific set of data based on unique reporting needs. Most standard reports can be copied and modified if the definition simply needs to be fine-tuned to meet the requirement. For a more customized representation, roughly 30 database views are provided – based on the views defined for each report in the standard set - for which any data set can be created and filtered for a completely unique presentation.

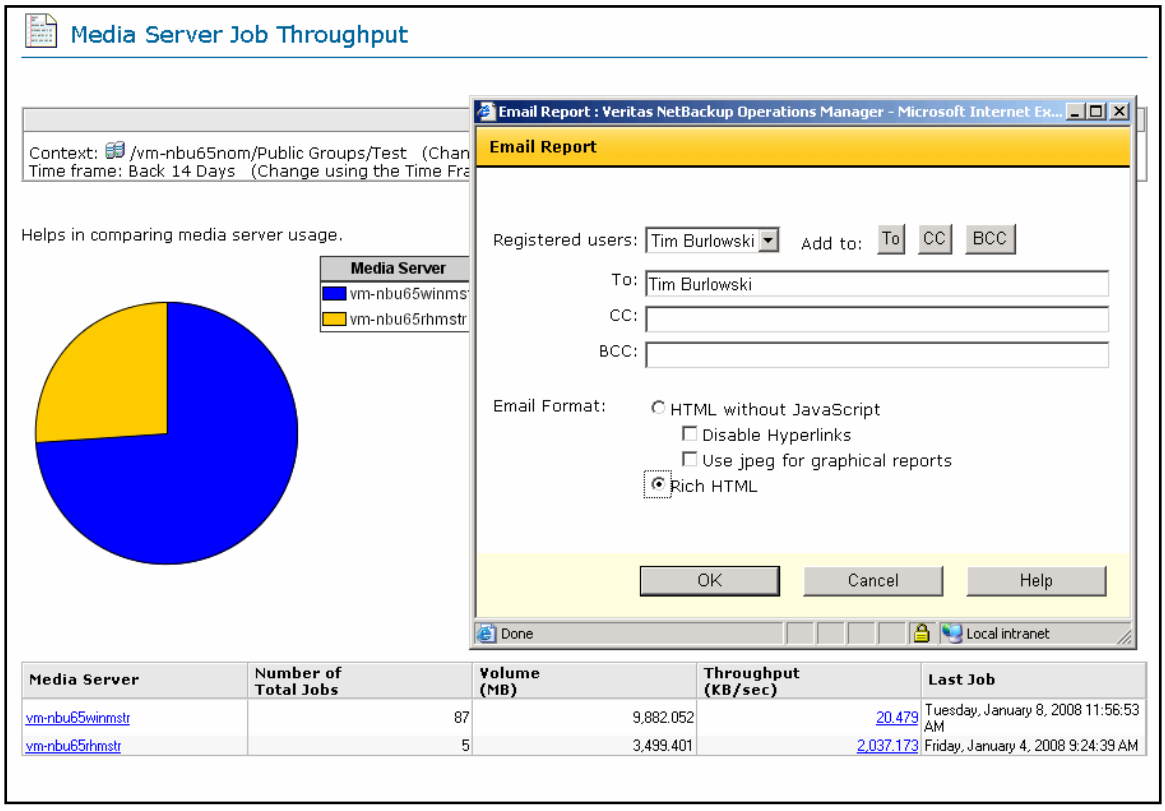

Figure 11: Emailing a Report

NOM and Veritas Backup Reporter

Do I need Veritas Backup Reporter?

Both NOM and Veritas Backup Reporter (VBR) can be categorized as data protection management offerings. However, the key features and focus areas of each offering are unique, making them complementary and a complete, end-to-end data protection management solution for NetBackup.

Historical Reporting

VBR was designed to support comprehensive reporting. Data collection and retention is fully configurable to support analysis of data over time, showing trends and enabling forecasting. On the other hand, with recommended 30-days data retention, NOM is designed for real-time monitoring across NetBackup domains. A push mechanism is built into NetBackup to send updates to NOM as changes are made in the environment. This provides a real-time view of the jobs that are running, drives that are spinning, etc. NOM is optimized for this real-time data collection and the monitoring, alerting and management functions enabled only through immediate data access.

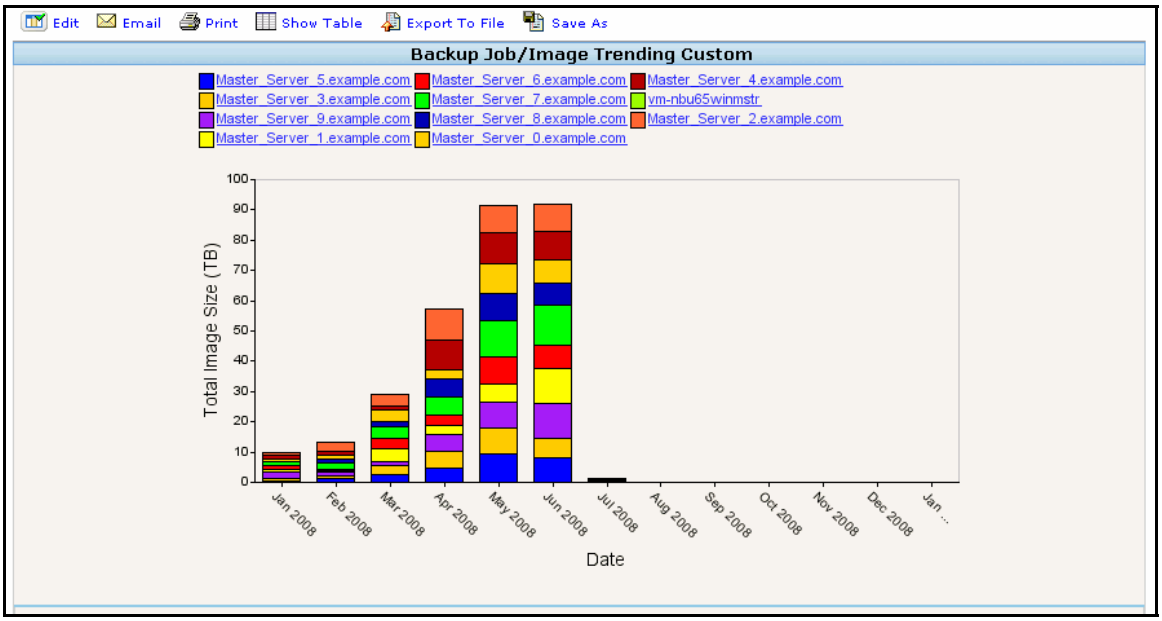

Figure 12: Example Image trending report from Veritas Backup Reporter

Customization

VBR has three primary methods of customization. First, the report wizard through the product interface is a common way to select the report style, data set and analysis criteria. Next, there is a query management component within the product to store and execute SQL statements as any other standard report. This is a great way to take advantage of the advanced custom reporting available with direct database queries in a supportable and maintainable fashion. Finally, direct access to the VBR database is provided – and the schema published – for users who prefer this level of interaction with the product.

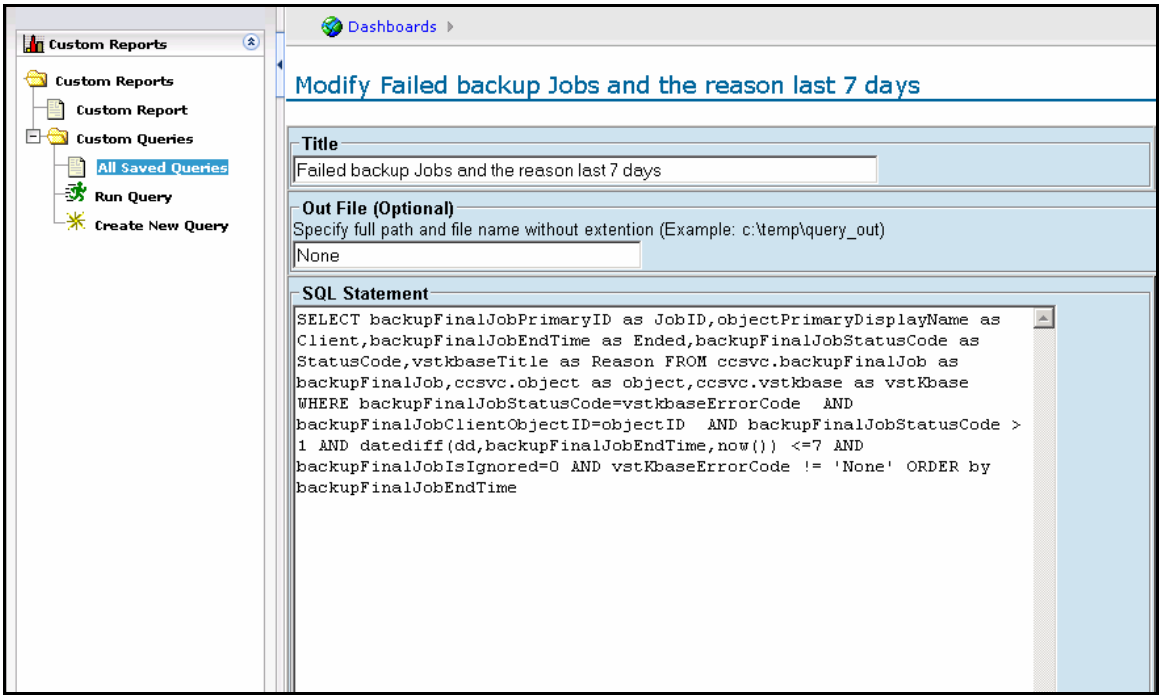

Figure 13: Custom SQL Report in Veritas Backup Reporter

NOM has point-and-click style reporting with customization only within the parameters of the existing reports. While the 30+ standard reports cover a breadth of operational reporting needs, the focus of this core-NetBackup component is on real-time monitoring, alerting and administration.

Figure 14: Example View

Views – Business Context

One of the most advanced functions in VBR is business Views for context-specific reporting. Any report can be run in context of a View, for example, application, geography, business unit, customer or data center. This helps to provide insight into trends, failures or performance metrics for that particular entity. Views will be unique from one environment to the next, so there are multiple options for defining and generating business Views. They are user-defined and can be manually created through a drag-and-drop capability or automated through rules or definition import.

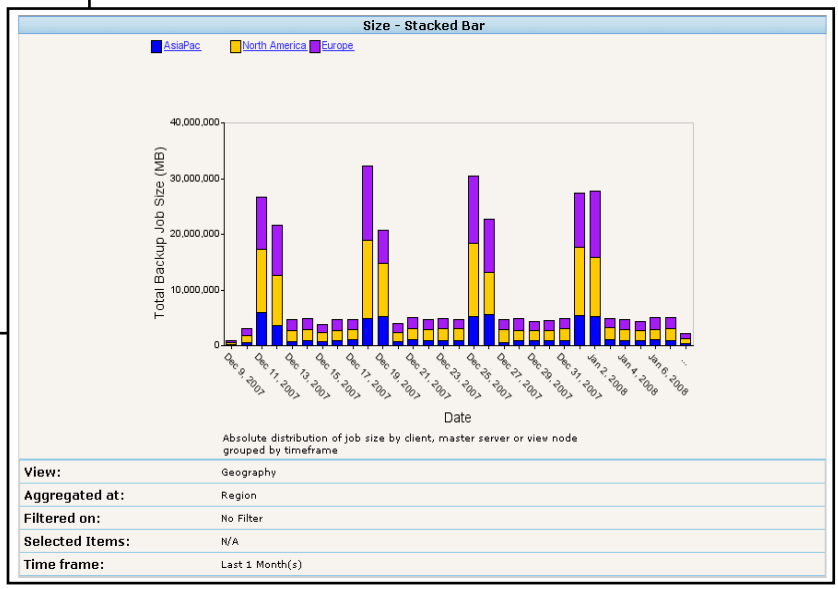

Figure 15: Example report created in the context of a view

Heterogeneous Product Support

VBR supports NetBackup, NetBackup PureDisk as well as Backup Exec. Several third-party data protection applications are also supported, e.g., IBM Tivoli Storage Manager, EMC NetWorker and CommVault Galaxy.

As a part of core NetBackup, NOM monitors only NetBackup. This component was introduced in version 6.0 of the product and can roll up from 6.0 and later versions of the product.

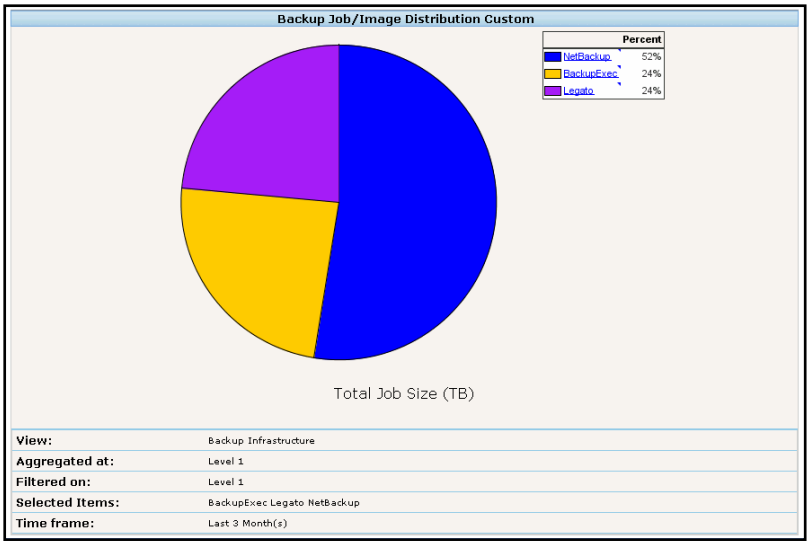

Figure 16: Example report summarizing Job Size by backup product, NetBackup, Backup Exec and EMC NetWorker (Legato).

Cost Analysis and Chargeback

VBR provides modeling tools to help assess the costs associated with data protection. With detailed information about the data protection environment, VBR can analyze user-provided operating costs against a variety of variables to help report the true cost of data protection. For example, variables could include, the amount of data protected on disk or tape, the number of restores executed each month, the backup methods used by client or application, etc. The data can also be used to justify investment in additional resources and also drive rational decisions in defining protection policies.

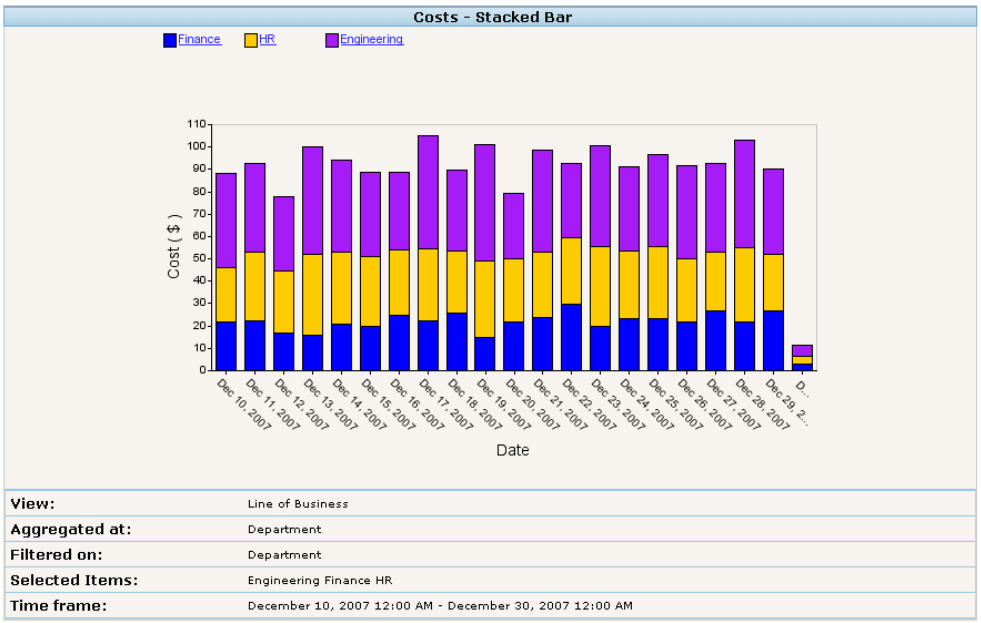

Figure 17: Example Cost trends report

NOM & VBR Focus Areas

The following chart highlights some of the key features and focus areas of NetBackup Operations Manager and Veritas Backup Reporter.

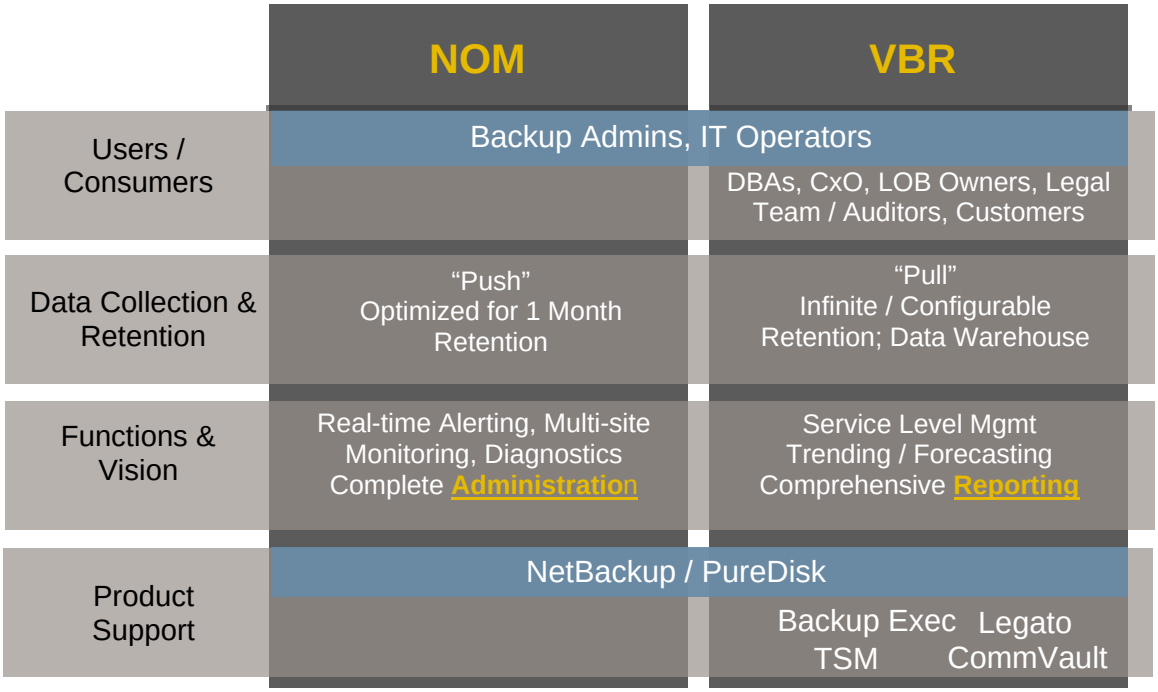

Figure 18: NOM & VBR Focus Areas

Summary

Netbackup Operations Manager allows for simplified Monitoring and Centralized administration. It allows users to create a "single pane of glass" for many day to day NetBackup operational needs.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

1/08 13603529