

Using and Archiving Network Manager's Database

Dell™ OpenManage™ Network Manager

By Joe Farrell

Engineering Manager
PowerConnect™ Engineering



November 17, 2003

Contents

Section 1	4
Introduction.....	4
Section 2	5
Why Do I Need a Database Aging Policy (DAP)?	5
Section 3	6
Configuring Database Aging Policies.....	6
Alarm Policy Set Up.....	7
Audit Trail Log Policy Set Up	9
Job Status Record Policy Set Up	12
Log Record Policy Set Up	12
Section 4	14
Sizing the Network Manager Database.....	14
Estimating Database Size	14
Adding Volumes	15
Recovering From Database Full Errors.....	16
Section 5	18
Conclusion.....	18

Figures

- Figure 1. Database Aging Policy Main Screen..... 6
- Figure 2. Selecting a DAP type. 7
- Figure 3. Setting up a DAP for alarms. 8
- Figure 4. Alarm DAP parameters. 9
- Figure 5. Audit Trail DAP parameters. 9
- Figure 6. Job Status DAP parameters..... 12
- Figure 7. Log Record DAP parameters..... 13

Introduction

Dell's OpenManage Network Manager uses an object oriented database from Versant to store information on equipment, configuration, services objects and alarm data. The number of objects can be quite large, and will grow over time as information accumulates and/or as the size of the managed network grows. This document tells you how to create policies for automatically archiving information in the database to increase the amount of available free space and also provides some technical information that allows you to resize the database appropriately for your installation.

Why Do I Need a Database Aging Policy (DAP)?

When you install Network Manager, automatic archiving of database content is not enabled so, over time, your database will fill up if no action is taken. This is a potential problem since the Network Manager application will not continue to function if the database runs out of space. The errors that will be seen are arbitrary since they depend on the specific component in use at the time the database fills.

To ensure that you are aware that your database is nearing capacity, Network Manager will issue a warning event when the database reaches a pre-set threshold of 85% full. This event will be visible in the event monitor screen when it is issued and will remain persistently in the event history database. A warning is also written into the Network Manager Application Server's log which can be accessed by right-clicking on the application server icon in your server's system tray. If you ignore the warning and exceed the physical limit of the database, the application will cease functioning as noted above and the database must be recovered using a procedure described later in this document.

Generally your system administrator will monitor Network Manager and take steps to resolve database-full issues before they occur. Network Manager provides you with a tool that helps simplify this process. That tool, the Database Aging Policy (DAP) Manager allows you to configure separate archiving policies for alarms/events, audit trail logs, job status records and log records. For each, you can specify the threshold at which the policy will be invoked (number of items in the database), the number of days worth of data to retain in the database once the policy is executed and the disposition of the data once it is removed (either archived or deleted).

The policies defined within the DAP Manager can be run explicitly by using the "Execute" button within the manager or can be scheduled to run at appropriate times. Multiple policies can be defined for each of the data types, so for example you could have one alarm policy that is scheduled to run once a day and another that does a major clean-up and is scheduled to run once a month.

Configuring Database Aging Policies

In order to configure your database aging policies, select the DAP Manager from the Navigation Pane (Callout 1 in Figure 1). This will open the Database Policy Manager main screen as shown in Figure 1. The first time you open the manager, there will be no policies defined so none are listed. As with other managers, once you have policies defined, you can filter them so specific subsets are shown on this screen.

In order to define a new policy, click the **New** button (Callout 2 in Figure 1). The resulting screen, shown in Figure 2 allows you to select the type of database aging policy you want to set up. Once you've selected a DAP type, click on the **OK** button to move to the configuration screen for that particular policy.

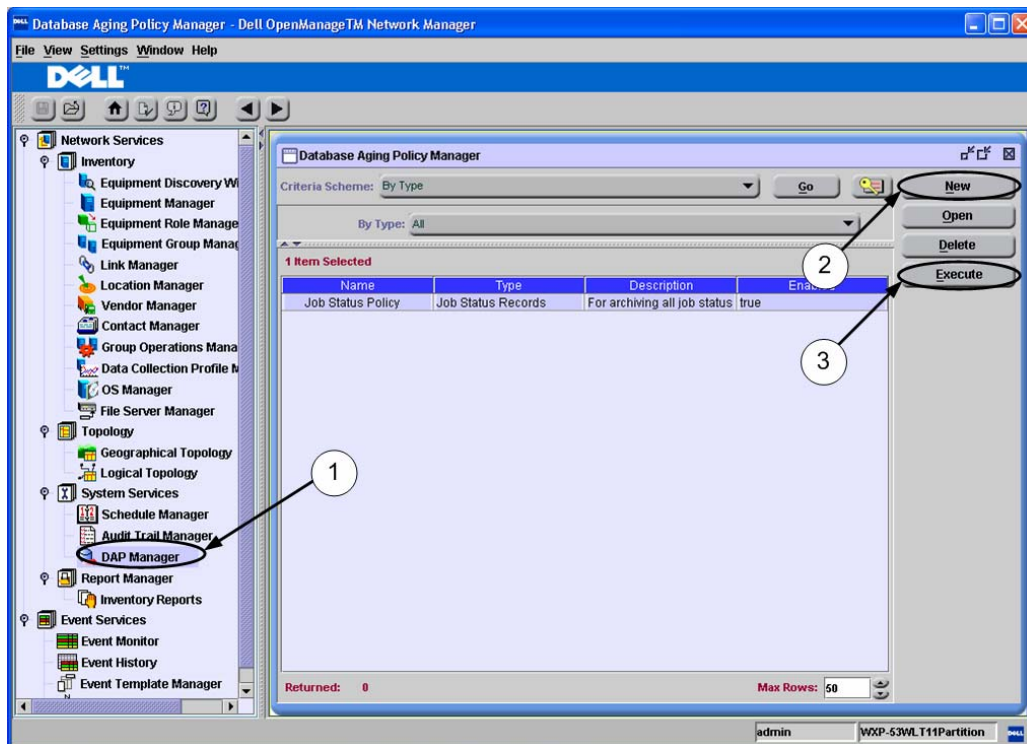


Figure 1. Database Aging Policy Main Screen.



Note: Database Aging Policies do not run automatically, even if you enable them on the policy set-up screen. You must explicitly execute the policy using the **Execute** button (Callout 3 in Figure 1) or by scheduling the policy for execution using the **Schedule Manager**.

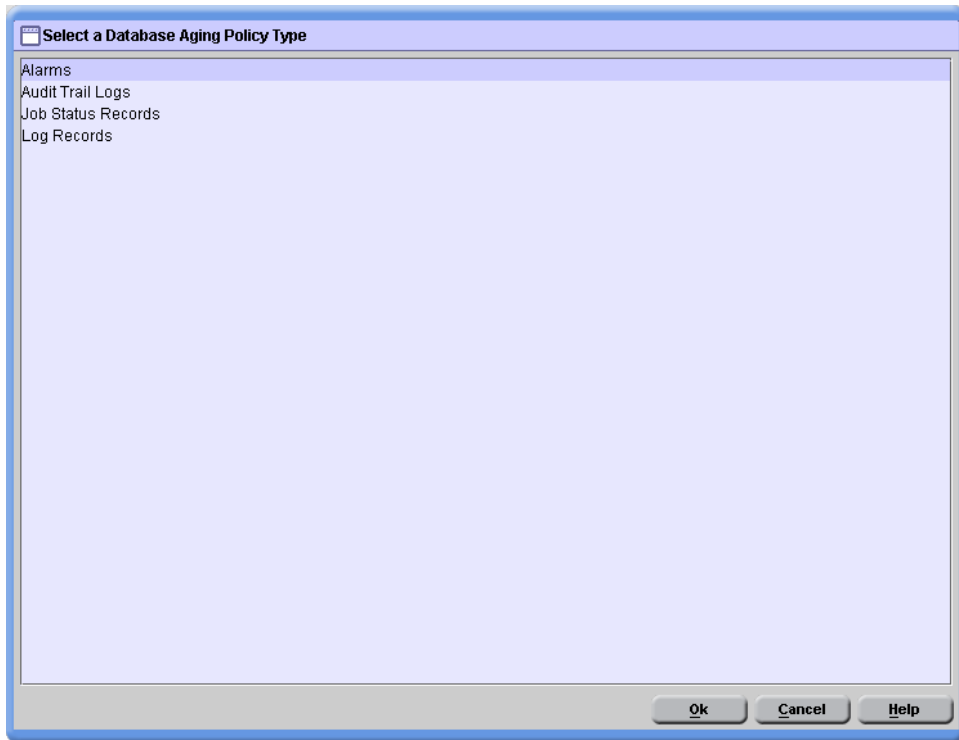


Figure 2. Selecting a DAP type.

Alarm Policy Set Up

Figure 3 shows the configuration screen for setting up an alarm DAP. There are two configuration panes available, “General Info” and “Alarm DAP Parameters”. Note that the layout for the “General Info” screen is the same for all DAP types and contains the following selections:

- **Name** — A unique identifier for this policy
- **Description** — A text description
- **Record Threshold** — The number of records that must exist before archiving begins. If the policy is run, either by using the “Execute” button or as a scheduled event, archiving will take place if the number of objects in the database exceeds this amount.
- **Primary Archive Location** — A disk location for archiving.
- **Secondary Archive Location** — A disk location for archiving if the primary location fails.
- **Base Archive Name** — The base name for the archive (part of the filename).
- **Compress Archive** — A checkbox that enables compression of the archive.
- **Enabled** — Determines whether the policy is enabled/disabled. Check to enable. If the policy is not enabled, there will be no effect even if it is run using the “Execute” button or as a scheduled event.

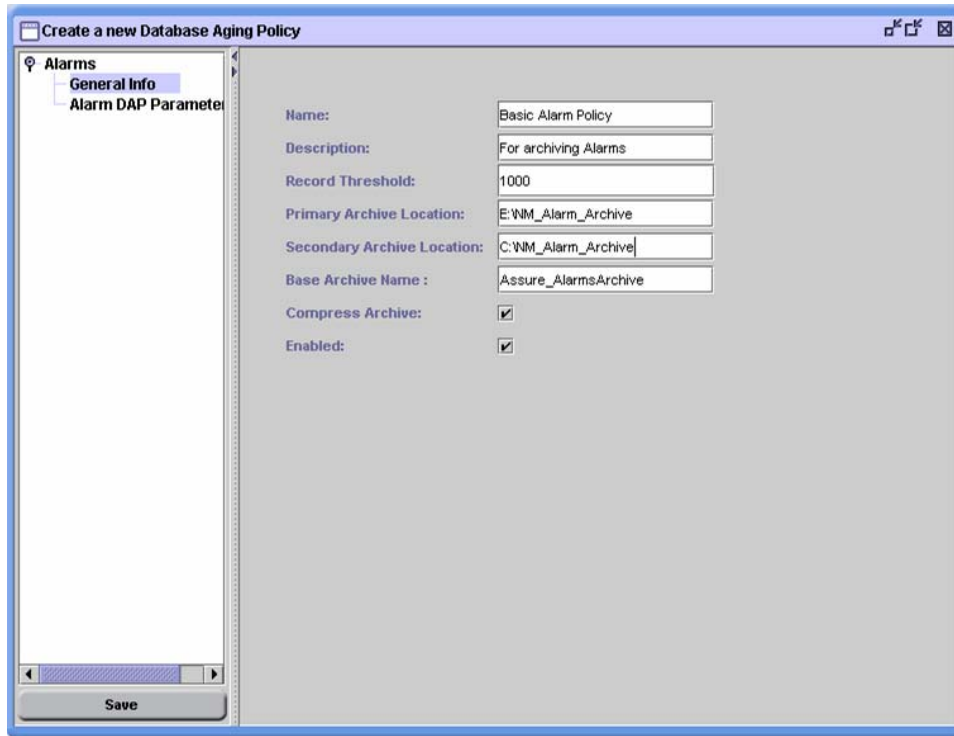


Figure 3. Setting up a DAP for alarms.

Note that the archive location can be on either a local or a remotely mounted disk. If the primary archive location is on a remote disk, it would be prudent to make the secondary archive location a locally mounted disk in case there were network problems at the time the archive action occurred.

The Alarm DAP Parameters set-up screen is shown in Figure 4. There are three parameters that can be changed on this screen:

- **Include Open Alarms** — If selected, the archive includes any alarms that were open at the time the archive was created.
- **Days to Retain** — Allows you to enter the number of days worth of alarms that will be retained in the database once the archiving operation is complete.
- **Archive** — If selected, the information is archived to a file at the location specified on the “General” screen of the Alarm DAP. If not selected, the information is simply deleted from the database.

Once you have set the parameters, click **Add** to create the policy. You can modify and delete already created policies by selecting them and clicking the appropriate button at the right hand side of the screen. It is possible to create multiple policies by selecting a different set of parameters and clicking **Add**. The capability is not useful for alarms but as you will see, makes sense for other DAP types.

Once you have created your Alarm DAP, click **Save** at the bottom of the selection panel to save the policy.

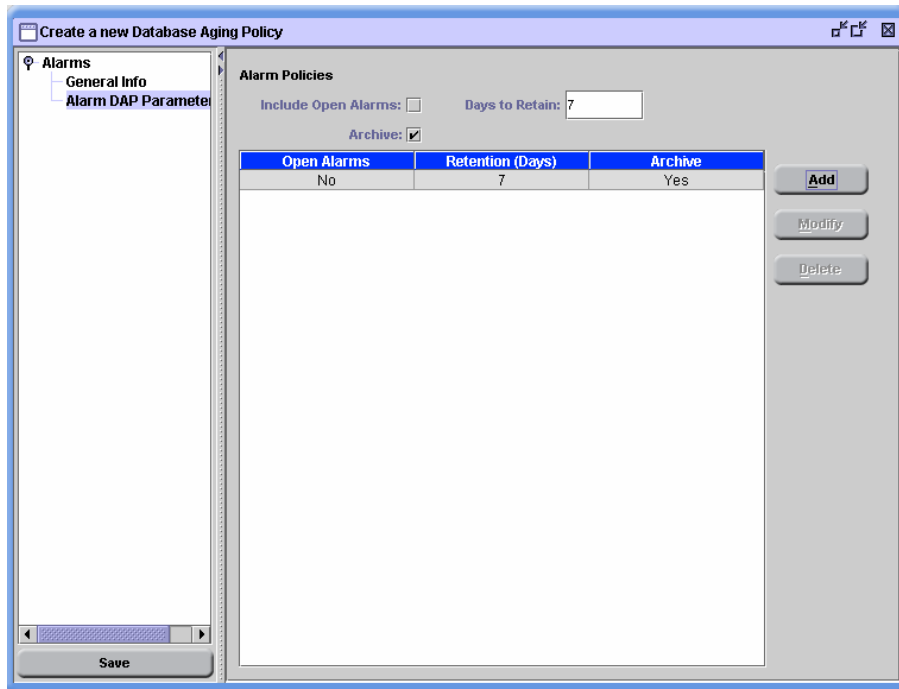


Figure 4. Alarm DAP parameters.

Audit Trail Log Policy Set Up

Audit trails provide a record of the actions performed by (and on) your Network Manager server. They are useful in troubleshooting problems and for tracking potential security violations so they are logged to the database and periodically need to be archived. Discussion here will be limited to “Audit” specific items. The “Audit” set up screen is shown in Figure 5.

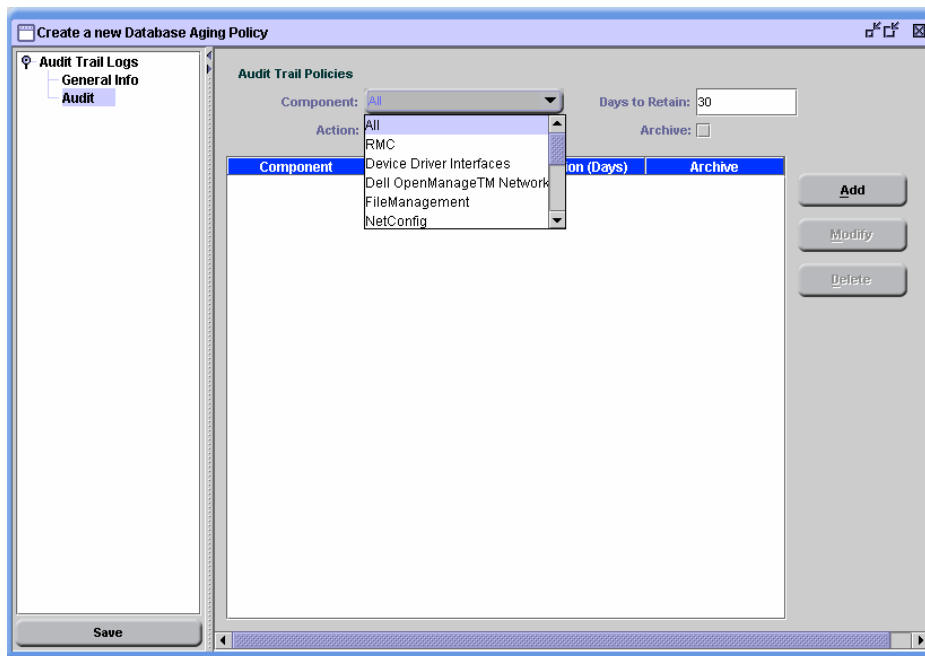


Figure 5. Audit Trail DAP parameters.

The screen is very similar to the Alarm DAP set up screen, but has the additional capability of selecting individual components and actions for archiving. Component selection is done using the drop-down menu as shown in Figure 5, and action selection is done using the drop-down menu concealed underneath the component drop down in the Figure.

For Network Manager, the available components and actions are:

Component	Action
All	All
RMC	All
	Discrete Configurations
NetConfig	NetConfig Restore
	NetConfig Backup
	Global Deploy
	Global Backup
	Batch Deploy
	Batch Backup
	NetConfig Deploy
Common Services	All
	DAP executed
	Configuration Accessed
	Security Policy Change
	User Disabled
	User Login
	User Logoff
	App Policy Change
	Account Reset
	Invalid Login
	User Created
	Client Termination
	User Locked Out
	Password Change
	Password Reset
	User Changed
	Schedule Item Added
	Schedule Item Deleted
Schedule Item Updated	

Component	Action
Assure	All
	Alarms Resync with Topology
	Event Template Updated
	Event Template Deleted
	Event Template Added
	Northbound Filter Updated
	Northbound Filter Deleted
	Northbound Filter Added
	Northbound System Started
	Northbound System Updated
	Northbound System Stopped
	Northbound System Deleted
	Northbound System Added
Performance Monitor	Data Collection Profile Deleted
	Data Collection Profile Disabled
	Data Collection Profile Enabled
	Data Collection Profile Updated
	Data Collection Profile Created
FileXferAPI	All
	Test TFTP Put Activated
	Test TFTP Get Activated
	FTP Get Activated
	FTP Put Activated
	Test FTP Get Activated
	Test FTP Put Activated
Group Operations	All
	Group Configuration Audit
	Group Operation Audit

As with the Alarm DAP screen, you can select the number of days of information to retain following the archive operation, and by selecting the "Archive" checkbox you can elect to archive the data rather than just deleting it from the database.

In the case of Audit Trail Policies, creating multiple policies is a useful option since so many components and actions can be selected. In order to have a comprehensive backup and maximize your database space recovery, simply select "All" components and "All" actions in the drop-down menus.

Job Status Record Policy Set Up

The DAP screen specific to the Job Status profile is shown in Figure 6. You can elect to archive all job status records or choose to archive only those for jobs that had a final status of Cancelled, Failed, Successful or Unknown. The **Days to Retain** and **Archive** fields function the same way for all DAP screens.

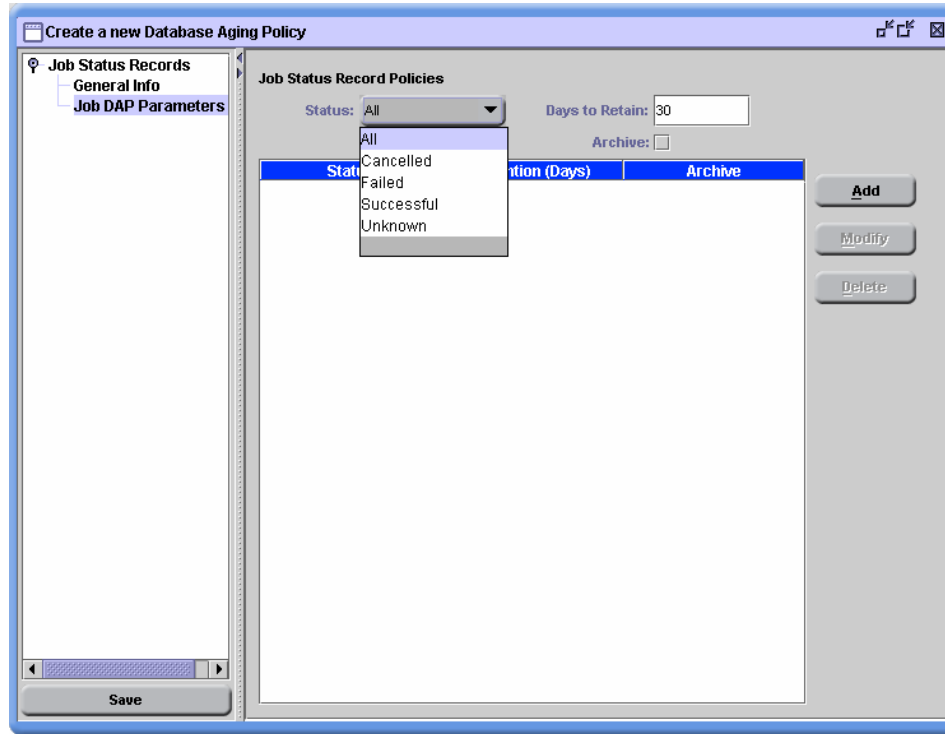


Figure 6. Job Status DAP parameters.

Log Record Policy Set Up

The DAP screen specific to the Log Records profile is shown in Figure 7. You can elect to archive all job status records or choose to archive only those logs that have an Unassigned category, those resulting from the execution of a scheduled item, those generated by Network Manger's rules engine or exception logs. The **Days to Retain** and **Archive** fields, although hidden in by the drop down menu in Figure 7, function the same way as in other DAP screens.

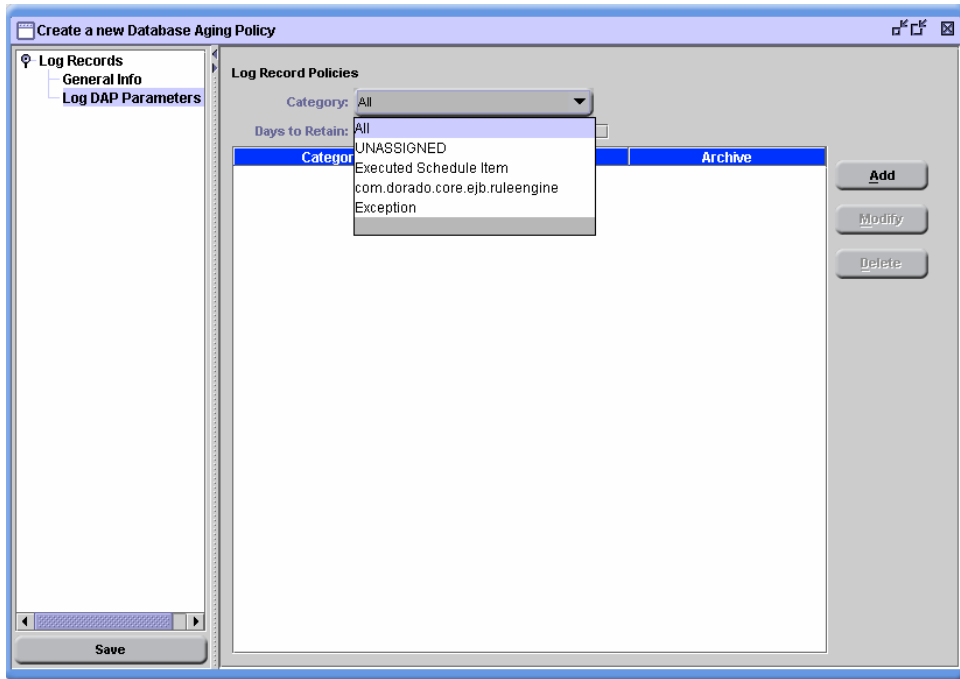


Figure 7. Log Record DAP parameters.

Sizing the Network Manager Database

Within Network Manager, all equipment, configuration, and services objects, and all alarm data are stored within a Versant database. The number of objects can be quite large and will grow over time as the size of the managed network increases and/or alarm data accumulates. This Section describes the procedure for estimating the size of the database and allocating additional space for the database as it grows.

In a standard Network Manager installation, the location of the binary files containing database information (volumes) is:

C:\Program Files\Dell\OpenManage\Network Manager\oware3rd\versant\db\busdb

The original volume is in a file named “system”.

When Network Manager is installed, the maximum database size defaults to 512 Megabytes (M). This means that the “system” file mentioned above will not exceed 512M in size



It is important that the maximum size of the database is not exceeded since Network Manager will not function properly if the database runs out of space. The errors that will be seen are arbitrary since they depend on the specific component in use at the time the database fails. Ideally, the Network Manager system administrator will monitor the Network Manager application and take necessary steps to keep the database from exceeding its volume size.

Estimating Database Size

There are two approaches that can be used in order to size the database. The first is to watch the size of the database file, and, as it approaches its maximum, add a new volume. This can be continued until the database stabilizes in size.



To monitor the free space remaining in your database, use the command **dbtool -F busdb** in a Windows command shell (where busdb is the name of your database). You will need to enter the **oware** command in your command shell to properly set the environment before using the **dbtool** command. To enter the **oware** command environment, simply type **oware** in the Windows command shell.

The second approach is to estimate the total amount of database space that will be required and pre-allocate enough space to accommodate all expected growth.

In order to estimate the amount of disk space that will be required for the database, use the following formula:

Approximate Database Size =

$$\begin{aligned} & 1.800M \\ + & .1125M * (\text{Number of Managed Switches}) \\ + & .0525M * (\text{Number of SNMP Traps to be Stored in Server}) \end{aligned}$$

+ .0525M * (Number of Audit Records to be Stored in Server)

This formula can be used to estimate in advance how large the database will grow and allows the network administrator to plan for additional database volume needs. To determine how large an additional volume size you may need, subtract 512M (the default volume size) from the "Approximate Database Size" calculated.

These numbers are very approximate and after calculating the database size needed for your installation, you should continue to monitor your database closely through several archive cycles to ensure that the overall maximum size has stabilized. You should also ensure that there is enough excess capacity to handle situations where

- A network event (or series of events) causes many traps to arrive in a short period of time
- Or to handle the increased number of audit records that might be generated during a period of network reconfiguration.

Adding Volumes

As the database grows, it may be necessary to add volumes and this Subsection provides you with details on carrying out that operation. Note that in most cases volumes can be added while Network Manager is running.

New volumes are added using the **addvol** command from the Windows command shell.

Usage: addvol [parameters] [options] <dbname>

parameters:

-n volName logical name for volume
-p volPath path of volume device/file

options:

-s volSize volume size, defaults to 4M
-e extSize extent size, defaults to use backend profile
-i pre-allocate and initialize volume
-noprint suppress display messages

dbname: database name

The following command adds a new volume named 'newsystem' with a filename of 'system2' and a size of 1 Gb to the database busdb:

** For this and the following examples, PATH has been defined as:*

\\Program Files\Dell\OpenManage\Network Manager\loware3rd\versant\db\busdb

If your copy of Network Manager was installed to a different location, substitute the path to that location in your command. The database will be in the "loware3rd\versant\db\busdb" subdirectory under your installation directory.

addvol -n newsystem -p PATH\system2 -s 1024M busdb

* 'M' is used to denote Megabytes; 'G' (for Gigabytes) is not supported.

Recovering From Database Full Errors

If the allocated space for the database is exceeded during a transaction, the database will shut down. As noted previously, this will cause unexpected results in Network Manager and the application will not function properly. Before attempting to add capacity to the database once a volume error has been encountered, stop the Network Manager application server first.

Normally, you would restart the database using the **startdb** command and then immediately add additional space using the **addvol** command as described above. Sometimes, the attempt to restart the database fails because the logical.log file is storing the transaction that caused the initial failure. In this case, issue the following commands in a Windows shell (comments appear in parenthesis):

```
oware (set the environment)
stopdb busdb (stop the database)
cp -p
PATH\logical.log
PATH\logical.log.back (copy log file to a backup)
dbtool -E busdb (do an "Emergency" restart)
addvol -n volname -p PATH\volnameFile busdb
(add a default 4M partition to
busdb)
stopdb -f busdb (immediately and forcibly stop
the database)
cp -p
PATH\logical.log.back
PATH\logical.log (restore the backed up log file)
startdb busdb (restart the database)
```

It is possible that the <dbtool -E> command might fail with a 7070 error code. If this is the case (and only if, this will not work if the error does not occur), use the following method:

```
oware (set the environment)
stopdb busdb (stop the database)
cp -p
PATH\logical.log
PATH\logical.log.back (copy log file to a backup)
makedb -g newDB (create a new database-step 1)
createdb newDB (create a new database-step 2)
cp -p
/dorado/oware/versant/db/newDB/logical.log
PATH\logical.log (copy log file from new database
to the busdb directory)
removedb newDB (delete the new database)
startdb busdb (start busdb using the new log)
```

```
file)
addvol -n volname -p PATH\volnameFile busdb      (add a default 4M partition to
                                                    busdb)
stopdb -f busdb                                  (stop the database)
cp -p
PATH\logical.log.back
PATH\logical.log                                 (restore the original log file)
Startdb                                          (restart the database)
```

Because the volume file will not expand if pre-allocated, and because there are obvious issues if the database becomes full, it is recommended that you not use the '-i' tag when creating a new database with **createdb**, and instead let the volume file grow automatically. This will allow the user to monitor the file size so it can be expanded before reaching the maximum. It is currently not possible to determine what percentage of a pre-allocated volume on a given database is being utilized.

Conclusion

After reading this How-To Guide, you should have enough information to begin using Database Aging Policies appropriately, know how to monitor your database usage to avoid disruptions in Network Manager operations and know what to do in the event that your database becomes full. Many more details on configuring Database Aging Policies can be found in your Network Manager User's Guide. Information on administering the Versant database can be found in the Network Manager Administration Guide as well.

THIS HOW-TO GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, IT MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Dell, OpenManage is a trademark of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

©Copyright 2003 Dell Inc. All rights reserved. Reproduction in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Information in this document is subject to change without notice.