

SOPHOS



sophos **nac**

ADVANCED

SQL Server Database
Administrator's Guide



Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.2
Published January 2011

Table of Contents

About This Document.....	4
Sophos Compliance Databases Descriptions	4
Sophos - LoadWH SQL Server Task Description.....	5
Database Deployment Considerations	5
Database Sizes	5
Database Properties.....	7
Database Location	7
Disaster Recovery	9
Maintenance Recommendations.....	10
Database Best Practices	10
Backup and Recovery Best Practices	11
SQL Server Maintenance Plan Best Practices.....	12

About This Document

This document describes how Sophos NAC Advanced uses SQL server databases in its operation. The document's purpose is to provide information to the database administrator who will maintain corporate SQL servers, but who may not necessarily have the responsibility for administering NAC Advanced. This document includes the following:

- Sophos Compliance Databases descriptions
- Sophos - LoadWH SQL server task description
- Database deployment considerations
- Maintenance recommendations

Sophos Compliance Databases Descriptions

Sophos SQL server database components (or Sophos Compliance Databases) contain all databases used by NAC Advanced, which include the following:

- **AlertStore:** This database store holds the information used to send alerts when user defined criteria is met. One such example would be an alert that is set up to send the administrator an email when the CEO's computer is non-compliant.
- **AuditStore:** This database contains the audit data which tracks what users make changes in the Sophos Compliance Manager. NAC Advanced maintains full audit information of every update made through the Compliance Manager. This audit information is kept in this database.
- **GeneralStore:** This database holds general data such as user home page preferences (the graphs the user sees when they log in), behavior categories, system objects, and metadata related to PolicyStore schema structures.
- **PolicyStore:** This database holds the application, policy, network access, and registration data, required by the software to determine security policy compliance and network access. The Sophos Compliance Application Server executes a PatchLoader job daily, which updates patch definitions in this database. Aside from this job, the contents of the application and policy portion of the database typically change only as the administrator updates these definitions. However, the registration, network access, and alerting information are updated as the Sophos Compliance Agents assess endpoints. The CurrentDefsLoader (scheduled task that imports current virus/application definitions) is also run as a scheduled task against this database.
- **ReportStore:** This data store holds the data reported by the Compliance Agents that can be viewed in the Compliance Manager Reports area. The ReportStore also contains staging tables that are used by the warehouse load process. Data is constantly being added to this database as endpoints report assessment results. Data is also archived daily as the report data migrates to the report store warehouse.
- **ReportStoreWH:** This database contains archived warehouse report information that is displayed in the Compliance Manager Reports area. Each night (by default), data is copied from the ReportStore to the ReportStoreWH and data that has aged past the retention period is purged from the ReportStoreWH. This data store is primarily read as archived reports are displayed online or the SQL views are used to generate reports. The update of this database occurs once per day when the job runs.
- **ReportStoreCache:** This database is a work database that does not hold any permanent data. It contains data from archived reports run throughout the day to facilitate performance.
- **SecurityStore:** This database contains the account login information for Compliance Manager users.

Sophos - LoadWH SQL Server Task Description

Sophos – LoadWH: The warehouse load task (ETL process) is responsible for moving report data to the warehouse (ReportStoreWH). When the task runs, it pulls report data from the current report tables, archives it in the report warehouse, and deletes the data from the report store. It also removes data from the warehouse that is older than the defined retention period. When it runs, the warehouse load task moves an entire day's worth of data from the report database to the warehouse and also purges an entire day's data from the archive.

The default retention period for the archived report data is 30 days. This value can be changed by following the procedure described in the *Sophos NAC Advanced Installation Guide*. Reducing the retention days results in a smaller report warehouse store, but does not reduce the amount of data that is moved when the Sophos – LoadWH task runs.

This task is scheduled to run once every 24 hours. By default, it runs at 2:30 AM local server time. The administrator can change the task schedule so that it runs at a different time. The administrator can also manually run the scheduled task using the SQL task scheduler. This job moves a significant amount of enterprise report data between two different databases, so it is recommended that you do not run or schedule the job to run during a busy time of day or while performing server backups.

Database Deployment Considerations

When you install the Compliance Databases, eight databases are created (if they do not already exist) in the default location for that SQL server (typically “\Program Files\Microsoft SQL Server\MSSQL”).

Note: Once NAC Advanced operations have begun, your policies are defined, and Compliance Agents are deployed, it is very difficult to make changes to the databases because the Sophos services have to be shut down during the maintenance. Though it is not required, we recommend establishing the database settings before NAC Advanced is deployed. Set the database size, location, and properties immediately after installation so that normal operations do not have to be interrupted.

Database Sizes

During the Compliance Databases installation, the databases are created with a small fixed size. All enterprises should resize the databases for production purposes. Even though SQL server databases can grow in size, the entire database is locked when it expands. Therefore, improve the overall performance by specifying a database at a large enough size so that it does not expand frequently. Many different factors affect the size of these databases, so precise formulas are difficult to obtain. However, estimates can be made to provide a size calculation that is adequate.

AlertStore

The amount of data in the AlertStore depends on many variables including number of alerts that are configured. In most cases this database should be set to auto grow by 25 MB increments.

AuditStore

The AuditStore will grow based upon how many updates are made in the Compliance Manager. If there are many users logging in and making changes to the Compliance Manager then this database can grow significantly. In most cases this database should be set to grow in 100 MB increments.

GeneralStore

The size of the GeneralStore will grow dependent on how many additions/customizations are made to user home pages (the graphs the user sees when they log in to the Compliance Manager), as well as application behavior categories, and other system objects. This database should remain constant in size and, in most cases, setting this to auto grow in 25 MB increments is sufficient.

PolicyStore

The amount of data in the PolicyStore depends on many variables including number and size of policies, number of registered endpoints, and number of alerts. The PolicyStore for a large enterprise (thousands of users) with a policy size of less than 100 applications will approach 500 MB. Each 1000 registered endpoints also require an additional 2 MB of space.

ReportStore

The ReportStore size depends on the number of endpoints that report assessments each day. This database should be set to a Fixed Growth Size of 500MB and will grow based on the following calculation:

.4 KB x [number of profiles in policy] x [number of endpoints].

Policies with more applications result in a larger growth rate.

ReportStoreWH

The ReportStoreWH size corresponds with the number endpoints that have archived reports in this database. This database should be set to a Fixed Growth Size of 500MB and will grow based on the following calculation:

.4 KB x [number of profiles in policy] x [number of endpoints] x [purge data value in days].

ReportStoreCache

This database does not hold any permanent data. It contains cached data from viewing archived reports and is purged daily. A database size of 250 MB set to auto grow by 25 MB increments is sufficient in most cases.

SecurityStore

This database holds data corresponding to the number of accounts that have been created and includes encrypted credentials for any accounts that are configured to use the internal user store. In most cases, this database should be set to auto grow in 25 MB increments.

Transaction Logs

No formula can be used to determine the appropriate transaction log size. Microsoft suggests monitoring the transaction log size over time and making it large enough so that it does not frequently expand.

Tempdb

Sophos uses tempdb during normal operations by using cursors and created temp tables. For this reason, tempdb must be set to automatically grow at a fixed value. Assuming the SQL server is dedicated to the NAC Advanced installation and applications, an allocated size of 1 GB should be sufficient. If tempdb requires more space, it expands to accommodate these needs.

When the SQL server restarts, tempdb is rebuilt with a default size. This size can potentially cause performance issues after restarting, because tempdb occasionally expands again while normal operations proceed. To avoid this, set the size of tempdb so that it rarely has to expand. Unfortunately, there are no metrics that can be used to

predict the required size of tempdb. Microsoft suggests monitoring the tempdb size over time and making it large enough so that it does not frequently expand.

Database Properties

Databases are created by default to allow auto grow, prevent auto shrink, and automatically update statistics. Use these default settings for all Compliance Databases.

Auto Grow Database by Fixed Size

Set the Compliance Databases to automatically grow by a fixed size rather than a percentage. Even if appropriately sized from the beginning, some event may cause a database to require more space. Set databases to grow automatically to ensure that if more space is needed, it is available. Verify that there is enough room on the disk so that the databases will grow and continue normal operations. After all Compliance Agents are deployed and NAC Advanced has been running for a time period equal to the retention days of the report archive, the databases will have reached a stable size and they will not expand frequently.

Note: Altering the NAC Advanced environment, such as changing the report interval or adding many new users, causes the databases to expand.

Prevent Auto Shrink Database

Set the Compliance Databases to prevent them from automatically shrinking. This is the default setting. Compliance Databases do get to a relatively static point over the course of operations. This means the databases do not appreciably grow or shrink, unless some change takes place, such as changing the report archive retention days. Once the databases reach a stable size, they more than likely will never shrink.

Auto Update Statistics

By default, the Compliance Databases are created with Auto create statistics and Auto update statistics enabled. The value of these database properties can be specified in the database Properties dialog in SQL Server Enterprise Manager or SQL Server Management Studio (depending on SQL server version). Enable these properties for each database so that queries are optimized based on the current index statistics.

Recovery Mode

There are three recovery modes available for each database: simple, bulk-logged, and full. Full is the default setting and offers the best protection against failure by allowing databases to be restored from full or differential backups. Bulk-logged recovery mode does not log such operations as SELECT INTO and bulk load.

Database Location

Moving all or part of the Compliance Databases to separate drives can improve performance of the application. The following section describes how to move databases, log files, and indexes to separate devices.

Database

It is possible to locate one or more of the Compliance Databases in another location. This option can help improve performance if databases with different update profiles are placed on different physical drives managed by separate controllers. For instance, placing the PolicyStore and ReportStore on separate physical drives will eliminate the I/O contention between the databases during the normal operations of retrieving policy and reporting compliance.

The easiest way to relocate databases to another location is to first install the Compliance Databases using the installation package, then detach the newly created databases, then move them (with their corresponding transaction logs) to the new location, and then re-attach them. If NAC Advanced is already installed and running,

then put the Compliance Application Server into maintenance mode, detach the databases, move the data and log files, re-attach the databases, and restart the services.

Note: Putting the Compliance Application Server (not the Compliance Database Server) into maintenance mode does not prevent the report warehouse load task from running, since this is a SQL job and not a service. Put the Compliance Application Server into maintenance mode, move the databases, and then stop maintenance mode to allow the NAC services to reconnect. These are the commands to put the Compliance Application Server into maintenance mode and move it out of maintenance mode from a command prompt:

```
“%programfiles%\Sophos\NAC\Support Tools\”maintmode.exe /start  
“%programfiles%\Sophos\NAC\Support Tools\”maintmode.exe /stop
```

The following procedure uses the ReportStore database to show how to move one of the databases to a different location.

1. Start the maintenance mode using the start command.
2. On the Compliance Database Server, detach the database.
sp_detach_db 'ReportStore'.
3. Move the files **ReportStore_Data.MDF** and **ReportStore_Log.LDF** from their location to a new location on a different drive. For example, move the database to D:\Sophos.
4. Re-attach the database.
**EXEC sp_attach_db @dbname = 'ReportStore',
@filename1 = 'D:\Sophos\ReportStore_Data.MDF',
@filename2 = 'D:\Sophos\ReportStore_Log.LDF'**
5. Stop the maintenance mode using the stop command.

Log File Location

The log files of the Compliance Databases can be moved to different locations as well. This option can improve performance by allowing log file I/O to be separate from data file I/O. The following procedure uses the PolicyStore database to show how to move a log file to a different disk drive.

1. Start the maintenance mode using the start command.
2. On the Compliance Database Server, detach the database.
sp_detach_db 'PolicyStore'
3. Move the file **PolicyStore_Log.LDF** from its location to a new location on a different drive. For example, move the log file to D:\Sophos.
4. Re-attach the database.
**EXEC sp_attach_db @dbname = 'PolicyStore',
@filename1 = 'C:\Program Files\Microsoft SQL Server\MSSQL',
@filename2 = 'D:\Sophos\ReportStore_Log.LDF'.**
5. Stop the maintenance mode using the stop command.

Index Location

Placing non-clustered indexes on a drive separate from the data can improve performance. Compliance Databases are deployed with indexes that have been designed and tested for NAC Advanced. Since indexes are already in place, moving them to another location involves scripting the DROP and CREATE statements indexes and altering the ON Primary parameter of the CREATE statement to use a filegroup that is on a different drive. The SQL Server Enterprise Manager or SQL Server Management Studio (depending on SQL server version) can be used to create and edit these scripts to change the filegroup. The Query Analyzer can then be used to run the scripts.

RAID

RAID storage is natively supported by SQL Server and Windows Server 2003/2008. Since the three primary Compliance Databases have the potential for significant write activity at various times throughout the day, care must be taken to choose the RAID level that offers the best combination of economy and performance. RAID 0 or disk striping improves performance by spreading read/write operations across disks, but does not offer fault tolerance. RAID 1, or mirroring, keeps identical copies of the selected disk. It provides good fault tolerance, but may degrade write performance. Many RAID controllers offer a hybrid solution known as RAID 0+1. RAID 5 is called striping with parity and offers data redundancy with the parity information. RAID 1 and RAID 0+1 offer better data protection and performance than RAID 5, but at higher cost in terms of the number of disks required. For more information on RAID, see the SQL Server Books Online.

Disaster Recovery

Log shipping

SQL Server Enterprise Edition provides log shipping. Log shipping creates warm standby servers that offer backup of the primary production server. To set up log shipping between the primary and backup servers, follow the instructions for implementing log shipping in the SQL Server documentation.

Note: If the primary server runs into problems, the secondary server can be promoted to primary.

1. Start the maintenance mode using the [start](#) command.
2. Follow the instructions in SQL Server documentation for changing the primary role of a SQL server.
3. From the Compliance Application Server, use Add or Remove Programs Control Panel to uninstall the Compliance Application Server.
4. From the Compliance Application Server, reinstall the Compliance Application Server. When prompted for the SQL server name, specify the new primary SQL server.
5. Stop the maintenance mode using the [stop](#) command.

Failover Clustering

Failover clustering provides a high availability solution because a SQL server will immediately fail over to the second node. Since Active/Passive clustering is designed to be transparent to the end user, no special considerations need to be made for the Compliance Databases. The key to using an Active/Passive cluster transparently is to ensure that NAC Advanced is installed to the "clustered" instance from both the Active and the Passive server (cluster will need to be failed over to the secondary node to install NAC Advanced on the secondary server). Once this is in place, the cluster can move back and forth between the active and passive nodes with no impact. If NAC Advanced is only installed on the primary node and not on the secondary node, then when the cluster fails over to the secondary node, the LoadWH job (ETL process) will not be able to run as it will not have been created on the secondary node (since NAC Advanced wasn't installed on this server).

Note: NAC Advanced does not currently support Active/Active clustering.

Maintenance Recommendations

Database Best Practices

The following database best practices ensure that the Compliance Databases run without errors and that the report database archives and purges data without errors. NAC Advanced reports are enterprise data-driven and are built with large enterprises in mind. The reports are comprehensive, robust, and produce large amounts of reporting information.

Best Practices	Description
Monitor your SQL server log and SQL server event log to verify that no server or SQL errors or warnings are causing problems with the NAC report data archiving and purging processes.	The server log and the event log provide details around warnings or errors that occur on the SQL server. By proactively monitoring these logs, Compliance Databases remain operational and fully functional.
Verify that the NAC report warehouse task is moving report data from the current reports to the archive reports on a daily basis according to the specified schedule.	Access the Compliance Manager and view an Archive report. The date and time to the right of the report title indicates the time/date of the most recent warehouse load. If this process does not run daily, report data may be lost and can cause database performance issues on the Report Store.
We recommend that no processes or backups run when the NAC report warehouse is moving report data from the current reports to the archive reports. The task runs at 2:30 AM daily by default.	The NAC report warehouse task can be SQL server intensive and will complete faster when other processes and backups are not running at the same time. Other processes and backups can cause resource contention, and this contention will affect the timeliness of the warehouse task.
On a weekly basis, verify that ample disk space is available on the SQL server for the Compliance Databases.	The size of the Compliance Databases will grow substantially if the NAC report warehouse and/or report purge processes have not been successfully running. Additional changes to NAC Advanced, such as adding users, will also increase the amount of space required.
Verify that the SQL Agent is turned on and is running. The SQL Agent must be running for the Sophos report data archiving and purge processes to run as scheduled.	If the SQL Agent is not running, these processes will not run and the report databases will grow substantially.

Backup and Recovery Best Practices

The following backup and recovery recommendations constitute best practices for the backup and recovery of the Sophos AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreWH, ReportStoreCache, and the SecurityStore databases:

Best Practice	Description
Create backup schedules for the AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreWH, ReportStoreCache, and the SecurityStore databases based on size, tolerance for data loss, and the time available for backup and recovery.	Database backup schedules ensure that data is backed up. Failure to back up the Compliance Databases could result in unrecoverable policy and report data.
For the PolicyStore database, use a combination of database, differential, and log backups. For example, back up the entire database nightly, perform a differential backup hourly, and back up the transaction log every 20 minutes.	The combination of database, differential, and log backups for the PolicyStore database provides comprehensive policy backup coverage. This combination ensures that no policies or policy changes are lost.
Create a step-by-step recovery plan for the PolicyStore, ReportStore, ReportStoreWH, and ReportStoreCache databases. Test the recovery plan using real backups.	The step-by-step recovery plan and test guarantees that policy and report information are recoverable in the event of database corruption or hardware failure.
Store database backups in a secure off-site location.	Store all database backups at an off-site location to guarantee data integrity when and if the need to use the backups occurs. If database backups are unavailable, all policy and report data will be lost and unrecoverable.
Create a process to notify the person or persons responsible for enterprise disaster recovery.	When database recovery is required, contact all individuals responsible for recovering databases. This process ensures that policy and report data are restored both efficiently and timely with minimal errors and data loss.

SQL Server Maintenance Plan Best Practices

The Microsoft SQL Server Maintenance Plan Wizard provides the easiest way to create a maintenance plan that protects your NAC data. Using the wizard automates essential maintenance tasks. Performing these tasks, which include integrity checks, backups, and database optimization, keeps the Compliance Databases running efficiently. Once you complete the maintenance wizard, you should test it and verify that it performs as expected.

Microsoft SQL Server Maintenance Plan Wizard Settings

The following table provides the Sophos recommended settings for the SQL Server Maintenance Wizard. Remember to not schedule these maintenance tasks at the same time that the data warehouse load task is running.

Setting Name	Setting
Data Optimization Information	
Important: Manually initiate the data optimization process only during a maintenance window.	
Reorganize data and index pages	Select
Free space per page percentage	10
Schedule	<i>Determined by DBA</i>
Duration	No End Date
Enable Schedule	Yes
Database Integrity Check	
Check database integrity	Select
Include indexes	Select
Attempt to repair any minor problems	Select
Perform these checks before doing backups	Select
Schedule	<i>Determined by DBA</i>
Duration	No End Date
Enable Schedule	Yes
Specify Database Backup Plan	
Back up the database as part of the maintenance plan	Select
Verify the integrity of the backup when complete	Select
Location to store the backup file	Disk

Setting Name	Setting
Schedule	<i>Determined by DBA</i>
Duration	No End Date
Enable Schedule	Yes
Specify Backup Disk Directory	
Use the default backup directory	Select
Remove files older than	<i>Determined by DBA</i>
Backup file extension	BAK
Specify the Transaction Log Backup Plan	
Back up the database as part of the maintenance plan	Select
Verify the integrity of the backup when complete	Select
Location to store the backup file	Disk
Schedule	<i>Determined by DBA</i>
Duration	No End Date
Enable Schedule	Yes
Specify Transaction Log Backup Disk Directory	
Use the default backup directory	Select
Remove files older than	<i>Depends on log file size (2 weeks to 3 days)</i>
Backup file extension	TRN
Reports to Generate	
Write report to a text file in directory	Select
Maintenance Plan History (local server)	
Write history to the msdb.dbo.maintplan_history table on this server	Select
Limit the rows in the table to	1000 rows for this plan
Database Maintenance Plan Wizard	
Assign name to the maintenance plan	Yes