

SOPHOS



sophos **nac**

ADVANCED

Operational Monitoring



Copyright 2007 Sophos Group. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

All other product and company names are trademarks or registered trademarks of their respective owners.

Document version 3.0
Published July 2007

Table of Contents

Operational Monitoring of Sophos NAC Advanced	4
Sophos Application Server	4
Sophos SQL Server.....	8

Operational Monitoring of Sophos NAC Advanced

Sophos NAC Advanced server components form an integral part of a NAC Advanced security infrastructure. Monitoring and management of the operation of security infrastructure is a proactive measure that improves the overall security posture of NAC Advanced. To achieve the highest level of operational security, Sophos NAC Advanced provides standardized operational monitoring events that can be integrated into the NAC Advanced Management System (EMS) framework. Operations staff who need to monitor the health of IT systems can use EMS tools, such as Microsoft® Operation Manager or HP OpenView, to track the status of the installed Sophos components. This document describes the Windows services, tasks, and events that Sophos components write to the Windows Server Event log. To verify the status and health of Sophos NAC Advanced, these services, tasks, and events can be monitored.

Sophos Application Server

The following services, scheduled tasks, and events can be monitored on the Sophos application server.

Services

The Sophos NAC Advanced application server requires four services to be started and running. The Sophos application installation sets these four services to start automatically. An operations monitor can monitor these services to verify that they are running.

Service Name	Startup	Path to Executable (under Program Files directory)
ENDFORCE Agent Report Service	Automatic	\agentreportservice\agentreportservice.exe
ENDFORCE Alert Service	Automatic	\alertservice>alertservice.exe
ENDFORCE Enforcer Report Service	Automatic	\authgateway\authgateway.exe
ENDFORCE Host Service	Automatic	\hostservice\efhostservice.exe

Scheduled Tasks

The Sophos NAC Advanced application installation sets up a scheduled task, the Sophos PatchLoader, that runs once per day at 2:00 A.M. local server time. Since this scheduled task does not run constantly, it cannot be monitored like other services. However, if the operations monitoring software supports it, a script can be written that interrogates this scheduled task to see when it was last run. Additionally, any failure of the PatchLoader task is recorded to the Sophos application server Event Log.

The Sophos NAC Advanced application installation also sets up a scheduled task for the CurrentDefsLoader that runs every hour (15 minutes after the hour). Since this task runs every hour, it is possible to monitor it as long as the monitoring software is able to run the query every hour at the same time that the task is running. It is also possible to use a script to interrogate this task to see when it was last run. Any errors of the application are recorded in the Event Log.

Events

The following events are written to the Event Log on the application server when and if they occur.

Event ID	Category	Severity	Description	Action
0	Middleware	Error	All errors generated by the Sophos NAC Advanced Web interface.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
1001	30	Error	Remote file download failed.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as trying to re-download the file. If not, escalate to Sophos.
1002	30	Error	Failure during file extraction.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as re-extracting the file. If not, escalate to Sophos.
1003	30	Error	Too many hash files in the directory. Unable to obtain hash of recently downloaded file.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as re-downloading the file. If not, escalate to Sophos.
1004	30	Error	Failure determining hash value of recently downloaded file.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as re-downloading the file. If not, escalate to Sophos.
1005	30	Error	Execution stopped as a result of previous failures.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
1006	30	Error	Unknown exception caught at execution. Cannot continue.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as re-trying previous operations. If not, escalate to Sophos.
1007	30	Error	Failure obtaining hash value for definition stored in database.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.

Event ID	Category	Severity	Description	Action
1008	30	Error	Failure to compress file contents for database storage.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
1009	30	Error	Failure to store new current definition data in database.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
1010	30	Error	Failure loading the downloaded XML document.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
1011	30	Error	Invalid application configuration.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as an application configuration. If not, escalate to Sophos.
2000	30	Warning	Unable to release sync record.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
2000	Policy Interface	Error	All errors generated by the Policy Interface.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
2001	30	Warning	Unable to clean up temporary file.	Try rebooting the machine to see if it fixes the problem. If not, escalate to Sophos.
2002	30	Warning	Failed updating the lastFetchDate on the current definition file row in the database.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
3000	Report Interface	Error	All errors generated by the Report Interface.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
3000	30	TraceL2	Remote file download beginning.	No action required.

Event ID	Category	Severity	Description	Action
3001	30	TraceL1	Remote file download completed.	No action required.
3002	30	TraceL2	Extracting files from compressed file.	No action required.
3003	30	TraceL1	Files extracted from compressed file.	No action required.
3004	30	TraceL1	The remote file is different than the current stored file. Database updated.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
3005	30	TraceL1	Remote file matches current definition hash value. No update needed.	No action required.
4001	Patch Loader	Error	All errors generated by the Patch Loader task.	Manually inspect the text of the error to see if it is something that can be corrected by the customer. This error is typically caused connectivity issues between the application server and the site from which the Patch Loader XML file is downloaded.
6000	Interface	Error	All errors generated by the Registration Interface.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
6003	Registration	Warning	Registration failed.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
7001	Policy Transfer Service	Error	Unknown exception.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
7002	Policy Transfer Service	Error	Unknown exception.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.

Event ID	Category	Severity	Description	Action
7033	Policy Transfer Service	Error	Unable to access the message queue.	Verify that the message queue is created and that the Sophos user has permissions to read and write to the queue. If this is not the problem, escalate to Sophos.
7035	Policy Transfer Service	Error	Bad dataset retrieved from the message queue.	This error signifies a problem. Report this problem to Sophos.
9000	RADIUS Extension	Error	This is the plug-in to Internet Authentication Service (IAS).	Inspect the error. Generally there are no errors from this component. A reboot of the server is required.
10000	Report Interface	Error	Sophos service that reads the reporting queue and writes to the reporting queue.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.
11000	ReportGroup Server	Error	COM+ Server Components.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.

Sophos SQL Server

The following services, scheduled tasks, and events can be monitored on the Sophos SQL server that contains the Sophos NAC Advanced databases.

Services

The Sophos SQL server requires the SQLSERVERAGENT service to be started and running. This service is installed with Microsoft SQL Server. An operations monitor can monitor this service to verify that it is running.

Service Name	Startup	Path to Executable (under Program Files directory)
SQLSERVERAGENT	Automatic	\Program Files\Microsoft\MSSQL\bin\sqlagent.exe

Scheduled SQL Server Agent Job

The Sophos SQL server installation sets up a scheduled SQL Agent job, Sophos NAC- LoadWH, that runs once per day at 2:30 A.M. local server time. Since this scheduled job does not run constantly, it cannot be monitored like other services. However, if the operations monitoring software supports it, a SQL server script can be written that interrogates this scheduled job to see when it was last run. Additionally, any failure of the Sophos NAC- LoadWH job, which executes a Sophos program called SQLTasks.exe, is recorded to the SQL server Event Log. See Event 12000 in the Event table in the next section.

Events

The following event is written to the Event Log on the SQL Server that contains the Sophos SQL databases and runs the Sophos SQL task.

Event ID	Category	Severity	Description	Action
12000	SQLTasks	Error	All errors generated by the SQLTasks process.	Manually inspect the text of the error to see if it is something that can be corrected by the customer, such as database connection failed. If not, escalate to Sophos.