Configuring Audit Collection Services in Operations Manager 2007 SP1

Step-by-step guidance for configuring redundant ACS Collectors for a single Audit Database

Authors:

Anders Bengtsson and Pete Zerger,
MS MVPs - System Center Operations Manager 2007

Version: 1.0
March 16th, 2008

Contents

Introduction

Audit Collection Services (ACS) is a feature introduced in Operations Manager 2007 designed for medium and large enterprises requiring collection and analysis of a high volume of Security Event Log data for internal and external regulatory compliance auditing purposes.

The RTM release of ACS in Operations Manager 2007 required a 1-to-1 relationship between the ACS collector and Audit database it reported to – meaning multiple collectors could not report to a single Audit database. This was in large part due to the fact that the bottleneck in the ACS architecture is actually the SQL 2005 limitation of database inserts per second, as explained by the product team around the time Operations Manager 2007 was released. While the Audit database can be part of an MSCS cluster, this left an obvious gap in the high availability story for the ACS feature.

New in SP1, Microsoft will now allow 2 ACS collectors to point to the same ACS database, but with only one active at a time. One acts as the primary collector, the other acts as the failover/secondary collector, which can only be enabled when the primary one failed or is disabled.

The focus of this document is to provide step-by-step instructions for implementing redundant ACS Collectors for a single Audit database in Operations Manager 2007 SP1. A brief architectural overview of Audit Collection Services has been provided for those not familiar with ACS.

This is a living document and will be updated as additional details become available.

ACS Architecture – A Brief Overview

This section is designed as a brief overview for those not completely familiar with the roles within the Audit Collection architecture. If you're already well-grounded in this area, proceed directly to the section titled "Implementing Redundant ACS Collectors for a Single Audit Database"

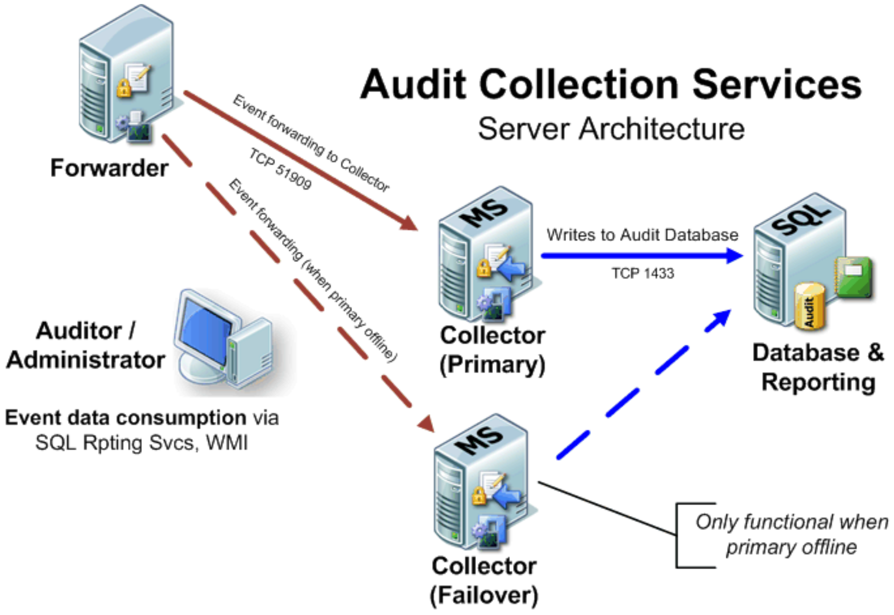
Audit Collection Services (ACS) is a component of Operations Manager 2007 that delivers centralized archival and reporting of Windows Security Event Logs. By consolidating security data to a central repository, this also serves to separate the role of local Administrator and Security Administrator

This data can be analyzed and presented through the Audit Collection Reports, which are delivered through SQL 2005 Reporting Services or via any tool with ODBC connectivity.

The ACS architecture consists of following roles:

- Collector
- Database
- Forwarder
- Reporting

The following sections contain a brief overview of these roles and their function in the ACS architecture.



Collector

The ACS collector role can be installed on any Management Server. The ACS collector inserts events received from ACS forwarders into the ACS database.

To ensure best performance and scalability, the ACS database should be located on a separate server from the ACS collector in large environments. See the Operations Manager 2007 Performance and Scalability Guide for additional details on sizing ACS server roles.

Database

The ACS Audit database is the central repository for events that are collected from ACS-enabled agents. The ACS database can be located on the same computer as the ACS collector, but for optimal performance, each should be installed on a dedicated server.

The ACS database stores events forwarded to the Collector by Agent Forwarders. Data is retained according to a user-defined retention schedule (14 days by default). Like other Operations Manager 2007 databases, the ACS database is partitioned to reduce grooming overhead. The partitioning interval is 1 day by default.

As previously mentioned, the RTM release of Operations Manager 2007 required a 1-to-1 relationship between ACS Collectors and Audit databases. This was in large part due to the fact that the bottleneck in the ACS architecture is the SQL limitation of database inserts per second, as explained by the product team around the time Operations Manager 2007 was released.

This was rectified in SP1 for Operations Manager, which introduced the capability to add a failover/secondary collector to that can be enabled when the primary collector fails.

TIP

Deploying the ACS database on SQL 2005 Standard Edition means that online database maintenance will not be possible, forcing the collector role to pause event insertion during the nightly maintenance window. Such a backlog of event data may be unacceptable in busy environments.

SQL 2005 Enterprise Edition allows online indexing and maintenance, allowing inserts to continue, although at a substantially reduced rate.

Forwarder

The ACS forwarder is integrated into the Operations Manager Agent. The ACS forwarder sends events to the collector in real time. The ACS Forwarding Service is installed automatically during the Operations Manager Agent installation, but is disabled by default. When Audit Collection Services is enabled for an agent-managed computer, the service is enabled, set to startup type Automatic, and the service started, making the agent an ACS forwarder. Shortly after, the ACS Forwarding Service on the forwarder contacts the ACS collector Service on the collector and downloads the event schema and associated job instructions.

The ACS architecture is based on principals contained in the '10 Immutable Laws of Security.' In particular, the 6th immutable law of security states "The computer is only as secure as the administrator is trustworthy". In that respect, every forwarder resides in an environment that is less than 100% trustworthy. Any actions or changes on the forwarder are under the control of the local administrator, as he/she is in a position to manipulate the state of the forwarder. By forwarding events in real time, this limits a local administrator's ability to interfere with security event analysis through evasive actions such as clearing the Security Event Log.

FAQ

Where is the queue on the ACS Forwarder?

The answer is that the Security Log itself is essentially the ACS Forwarder Queue. The ACS Collector keeps a watermark/checkpoint in a file for each forwarder where in the log was the last event sent. When connection resumes, the collector informs the forwarder where to start sending event again. (I won't list the details here…there is no reason it should be tampered with.)

This calls attention to the fact the Security Event Log size is important. Make sure to increase this from the Windows 2003 default of 16 MB, especially on AD domain controllers.

Reporting

ACS Reports will be uploaded via a command-line using the ReportingConfig utility in batch command. There are approximately 18 reports available out-of-the-box covering a number of common auditing scenarios, including:

- Active Directory administration events, such as account creation and deletion
- Changes to sensitive groups and password changes
- Object access and usage tracking

As of Opsmgr 2007 SP1, Audit Collection Services Reporting can be installed in a separate SQL Reporting Services from the primary Opsmgr 2007 reports, or installed into the existing Opsmgr SQL Reporting Services instance, allowing integration of ACS reports into the Reporting space in the Operations console.

Implementing Redundant ACS Collectors for a Single Audit Database

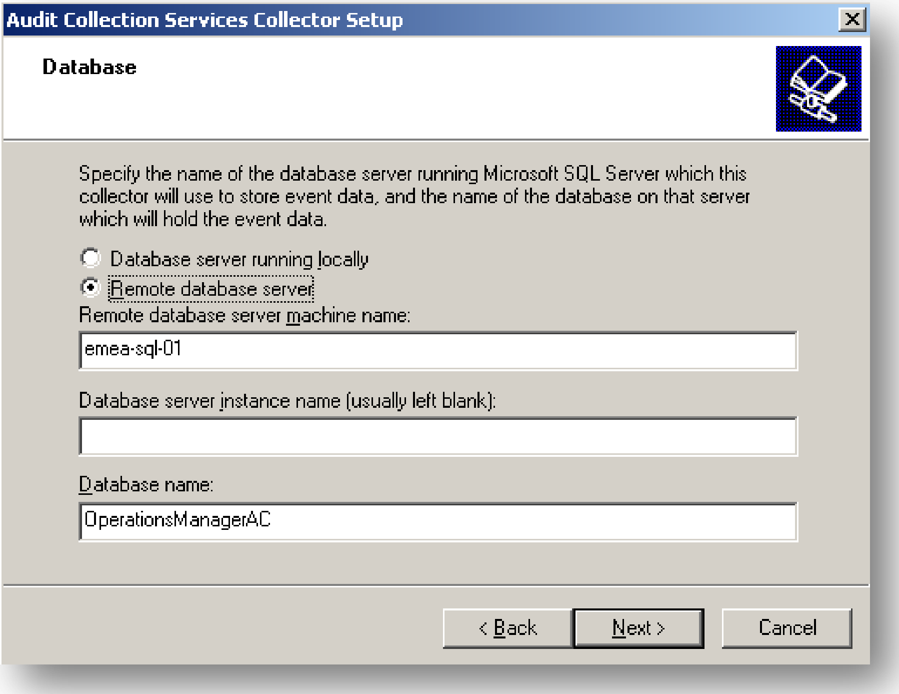
In this example we have two management servers and one SQL server. EMEA-OPSMGR-RMS is our root management server. EMEA-OPSMGR-MS2 is our second management server and EMEA-SQL-01 is our database machine. The two management servers will be installed as ACS collectors and the SQL server will host the Audit database.

Deploy the first ACS Collector

When the first collector is installed, the database should be created on the remote SQL server from the same wizard.

1. Double-click the **setupOM.exe** from the installation source files.
2. On the **System Center Operations Manager 2007 Setup** screen, select **Install Audit Collection Server**.
3. On the **Welcome** screen, click **Next.**
4. On the **License Agreement** screen, Read the agreement and then select the checkbox by **I accept the agreement** and click **Next.**
5. On the **Database Installation Options** screen, **Select Create a new database** and click **Next**
6. On the **Data Source screen**, input a **name** for the ODBC Data Source and click Next, or accept the default name, OpsMgrAC, click **Next**

7. On the **Database** screen: Input the **name** of the **SQL server** and **instance**. Also input a **database** name, the default name is OperationsManagerAC. Click **Next**



Audit Collection Services Collector Setup

Database

Specify the name of the database server running Microsoft SQL Server which this collector will use to store event data, and the name of the database on that server which will hold the event data.

○ Database server running locally
● Remote database server

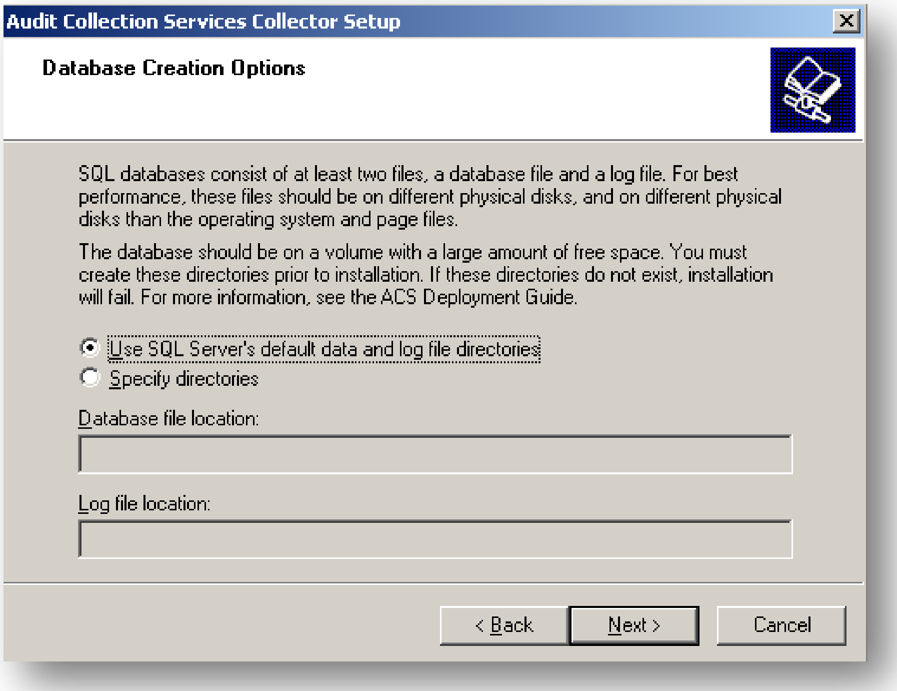
Remote database server machine name: emea-sql-01

Database server instance name (usually left blank):

Database name: OperationsManagerAC

8. On the **Database Authentication screen,** select **SQL authentication**. Click **Next**
9. On the **Database Credentials** screen, input a **SQL login name** and a **SQL password** for the new SQL user. For example ACSCollector as login name. Make sure you input a password that fulfills your organization password policy. Click **Next**

10. On the **Database Creation Options** screen, select to use SQL **default data and log file directories** or input a new path. Click **Next**



Audit Collection Services Collector Setup

Database Creation Options

SQL databases consist of at least two files, a database file and a log file. For best performance, these files should be on different physical disks, and on different physical disks than the operating system and page files.

The database should be on a volume with a large amount of free space. You must create these directories prior to installation. If these directories do not exist, installation will fail. For more information, see the ACS Deployment Guide.

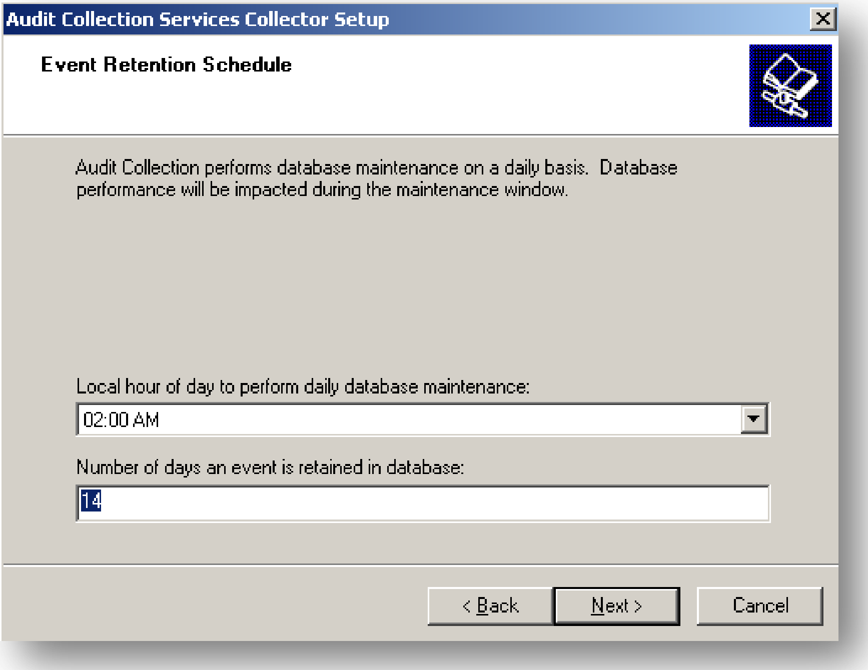
● Use SQL Server's default data and log file directories

○ Specify directories

Database file location:

Log file location:

11. On the **Event Retention Schedule screen,** select **hour** to perform database maintenance and also **number of days** to store in the database. Make sure your selection fulfills your organization policies. Click **Next**



Audit Collection Services Collector Setup

Event Retention Schedule

Audit Collection performs database maintenance on a daily basis. Database performance will be impacted during the maintenance window.

Local hour of day to perform daily database maintenance: 02:00 AM

Number of days an event is retained in database: 14

12. On the **ACS Stored Timestamp Format** screen, select if you want ACS to use local time or UTC time for **timestamps** in the database. Click **Next**
13. On the **Summary** screen, **review** all your options and then click **Next** to begin the setup
14. If you receive a **SQL Server Logon** popup window, simple select **use a trusted connection** and then click **OK**
15. Om the **Audit Collection Services** screen verify that ACS has been successfully installed, **review** that all components have been successfully installed then click **Finish**

Prepare for the second collector

Before you can deploy the second ACS Collector you must shutdown the first ACS Collector. You can do this by stopping the AdtServer service.

On your first ACS Collector

1. Click **start** and choose **run**
2. Input **services.msc** and click **OK**
3. In the Services console, **select** and **right-click** the **Operations Manager Audit Collection Service** service, select **stop** from the context menu.
4. **Verify** that the services has stopped
5. **Close** the services **console**

Deploy the second ACS Collector

1. Start the **setupOM.exe** from your installation source
2. In the **System Center Operations Manager 2007 Setup screen**, select **Install Audit Collection Server**
3. In the **Welcome** screen, click **Next**
4. On the **License Agreement** screen, **read** the agreement and then select **I accept the agreement** and click **Next**
5. On the **Database Installation Options** screen, select **Use an existing database,** click **Next**
6. On the **Data Source** screen, input the same **name** as you did on the first collector. Click **Next**
7. On the **Database** screen, input the name of the **SQL server and instance**. Also input the **database name**, the default name is OperationsManagerAC. Note that these settings should be the **same** as you imputed when deploying the first ACS Collector. Click **Next**
8. On the **Database Authentication** screen, select **SQL authentication**. Click **Next**
9. On the **Database Credentials** screen, input the **SQL login name** and the **SQL password** that you specified for the new SQL user. Click **Next**
10. On the **Summary** screen, **review** all your options and then click **Next** to begin the setup
11. Om the **Audit Collection Services** screen verify that ACS has been successfully installed, **review** that all components have been successfully installed then click **Finish**

We should now turn of the ACS collector service on the second ACS Collector and start it up on the first collector.

On your second ACS Collector

1. Click **start** and choose **run**
2. Input **services.msc** and click **OK**
3. In the Services console, **select** and **right-click** the **Operations Manager Audit Collection Service** service, select **stop** from the context menu.
4. **Verify** that the services has stopped
5. **Close** the services **console**

Enable ACS forwarding and enable failover

1. Start the **System Center Operations Manager 2007 console**
2. Select a state view showing **data related to agent**
3. **Select** a agent and select **Enable Audit Collection** from the action pane
4. On the **Enable Audit Collection** screen, click **Override**
5. On the **Override Task Parameters** screen, input your **two ACS Collectors FQDN** as new value, for example "emea-opsmgr-rms, emea-opsmgr-ms2" , click **Override**
6. On the **Enable Audit Collection** screen, input **task credentials** and then click **Run**
7. On the **Enable Audit Collection** screen, **verify** that the task was successful. Click **Close**

Now you have enable ACS forwarding from one of your agents. The agent will fail over to the second ACS Collector that you specified in the override field, if it can't communicate with the first ACS collector.

How to test ACS collector failover

If you disconnect the first ACS collector, in our example emea-opsmgr-rms, from the network you will get an event (ID 4369) in the Operations Manager Event Log on the ACS forwarder. This event tells you that the agent cannot connect to any ACS collector, but a couple of seconds later you will see a event (ID 4368) telling you that the ACS forwarder is now connected to the other ACS collector, emea-opsmgr-ms2. If you then stop the collector service on the second ACS collector and start the service on the first ACS collector you will see that the ACS forwarder will connect to the first ACS collector again.

To redirect audit traffic to the Secondary Collector (in the event that the Primary Collector is having problem), one must first ensure AdtServer is NOT running on the Primary Collector, and then turn on AdtServer on the Secondary Collector.

1. **Configure** your ACS forwarder with **multiple ACS collectors**
2. **Disconnect** the first **ACS collector** from the network
3. **Start** the **AdtServer service** on the **second ACS collector**
4. **Verify** that the ACS forwarder **failover**
5. **Verify** in the Audit **reports** that you have data for the **failover timeframe**
6. **Stop** the **AdtServer service** on the **second ACS collector**
7. **Start** the **AdtServer service** on the **first ACS collector**
8. **Verify** on the **ACS forwarder** that it have connected to **the first ACS collector** again

Automating ACS Collector Failover and Failback Processes

To automate the process of ACS failover and failback, you could create a TCP port monitor to check port 51909 on your ACS collector, if it does not respond, start the ACS collector service on the other ACS collector as a response. You can also setup a monitor to verify that the ACS collector service is running; else start the service on the other ACS collector machine.

This is just an example, not an official recommendation. Any such automation of the collector failover / failback process should be carefully tested, as no official guidance has been published in this regard. Your Microsoft Technical Account Manager (TAM) or other representative may also be of assistance in obtaining some official recommendation from the product team.

Conclusion

We hope you have found this article helpful. Your feedback is always welcome at

http://www.systemcenterforum.org/contact

Additional Reading

You may receive a "Not associated with a trusted SQL Server connection" error message when you try to connect to SQL Server 2000 or SQL Server 2005

http://support.microsoft.com/kb/889615

Operations Manager 2007 SP1 Supported Configurations
http://technet.microsoft.com/en-us/library/bb309428.aspx