Collecting Security Events Using Audit Collection Services in Operations Manager

Updated: May 13, 2016

Applies To: System Center 2012 R2 Operations Manager, System Center 2012 - Operations Manager, System Center 2012 SP1 - Operations Manager

In System Center 2012 – Operations Manager, Audit Collection Services (ACS) provides a means to collect records generated by an audit policy and store them in a centralized database. By default, when an audit policy is implemented on a Windows computer, that computer automatically saves all events generated by the audit policy to its local Security log. This is true for Windows workstations as well as servers. In organizations that have strict security requirements, audit policies can quickly generate large volumes of events.

Using ACS, organizations can consolidate individual Security logs into a centrally managed database and can filter and analyze events using the data analysis and reporting tools provided by Microsoft SQL Server. With ACS, only a user who has specifically been given the right to access the ACS database can run queries and create reports on the collected data.

ACS requires the following components:

- ACS Forwarders
- ACS Collector
- ACS Database

Auditing is supported on UNIX and Linux computers. For more information, see ACS on UNIX and Linux in this topic.

(See list of Collecting Security Events Using Audit Collection Services topics.)

ACS Forwarders

The service that runs on ACS forwarders is included in the Operations Manager agent. By default, this service is installed but not enabled when the Operations Manager agent is installed. You can enable this service for multiple agent computers at the same time using the **Enable Audit Collection** task. After you enable this service, all security events are sent to the ACS collector in addition to the local Security log.

ACS Collector

The ACS collector receives and processes events from ACS forwarders and then sends this data to the ACS database. This processing includes disassembling the data so that it can be spread across several tables within the ACS database, minimizing data redundancy, and applying filters so that unnecessary events are not added to the ACS database.

The number of ACS forwarders that can be supported by a single ACS collector and ACS database can vary, depending on the following factors:

- The number of events that your audit policy generates.
- The role of the computers that the ACS forwarders monitor (such as domain controller versus member server).
- The level of activities on the computer.
- The hardware on which the ACS collector and ACS database run.

If your environment contains too many ACS forwarders for a single ACS collector, you can install more than one ACS collector. Each ACS collector must have its own ACS database.

The requirements for an ACS collector are as follows:

- An Operations Manager management server
- A member of an Active Directory domain
- A minimum of 1 gigabyte (GB) of RAM, with 2 GB recommended
- At least a 1.8 gigahertz (GHz) processor, with a 2.8 GHz processor recommended
- 10 GB of hard disk space available, at a minimum, with 50 GB recommended

On each computer on which you plan to install the ACS collector, you must download and install the latest version of the Microsoft Data Access Components (MDAC) from the Microsoft Web site. To learn more about MDAC, see at Learning Microsoft Data Access Components (MDAC).

ACS Database

The ACS database is the central repository for events that are generated by an audit policy within an ACS deployment. The ACS database can be located on the same computer as the ACS collector, but for best performance, each should be installed on a dedicated server.

The requirements for an ACS database are as follows:

- For System Center 2012 – Operations Manager: SQL Server 2005 or SQL Server 2008. You can choose an existing or new installation of SQL Server. The Enterprise edition of SQL Server is recommended because of the stress of daily ACS database maintenance.
- For System Center 2012 Service Pack 1 (SP1), Operations Manager: SQL Server SQL 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1. The Enterprise edition of SQL Server is recommended because of the stress of daily ACS database maintenance.
- A minimum of 1 GB of RAM, with 2 GB recommended

Note

If you are using SQL Server 2008 R2 or earlier and your server has more than 2 GB of memory some additional configuration steps are needed. For more information and the steps needed, see How to configure SQL Server to use more than 2 GB of physical memory. For a list of the minimum hardware and software requirements to install and run SQL Server 2012, see Hardware and Software Requirements for Installing SQL Server 2012.

- At least a 1.8 GHz processor, with a 2.8 GHz processor recommended
- 20 GB of hard disk space available, at a minimum, with 100 GB recommended

If you use SQL Server standard edition, the database must pause during daily maintenance operations. This may cause the ACS collector queue to fill with requests from ACS forwarders. A full ACS collector queue then causes ACS forwarders to be disconnected from the ACS collector. Disconnected ACS forwarders reconnect after the database maintenance is complete and the queue backlog is then processed. To ensure no audit events are lost, allocate a sufficient amount of hard disk space for the local security log on all ACS forwarder.

SQL Server enterprise edition can continue to service ACS forwarder requests, although at a lower performance level, during daily maintenance operations. For more information on the ACS collector queue and ACS forwarder disconnection see Audit Collection Services Capacity Planning and Monitoring Audit Collection Services Performance.