How to Create a Scheduled Task to Automatically Rotate the Centrify Auditing Database

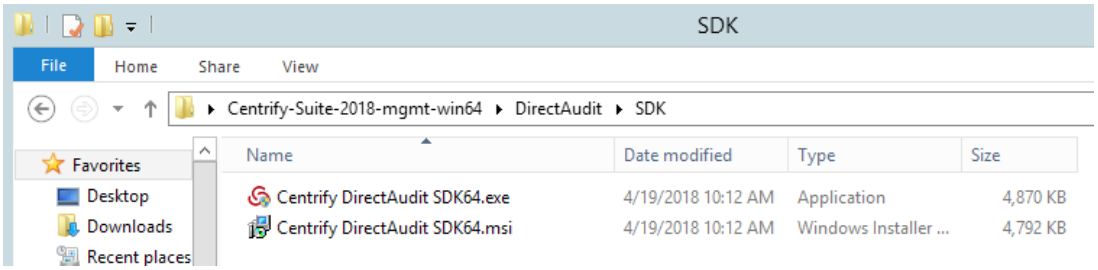
This document describes how to create a scheduled task that will automatically rotate the Centrify Auditing audit store database on the first day of each month. You can easily modify the command described below to suit your requirements.

Please refer to the following MSDN article for a complete list of Task Scheduler (Schtasks.exe) commands.

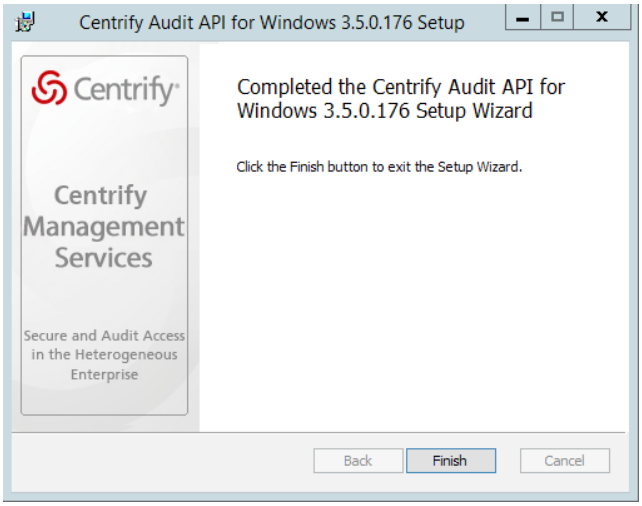
https://msdn.microsoft.com/en-us/library/windows/desktop/bb736357(v=vs.85).aspx

Installing the Centrify DirectAudit SDK

The DirectAudit SDK installer is included with the Centrify Suite download, within the ..**DirectAudit\SDK** directory. It is available in both .exe and .msi installer types.

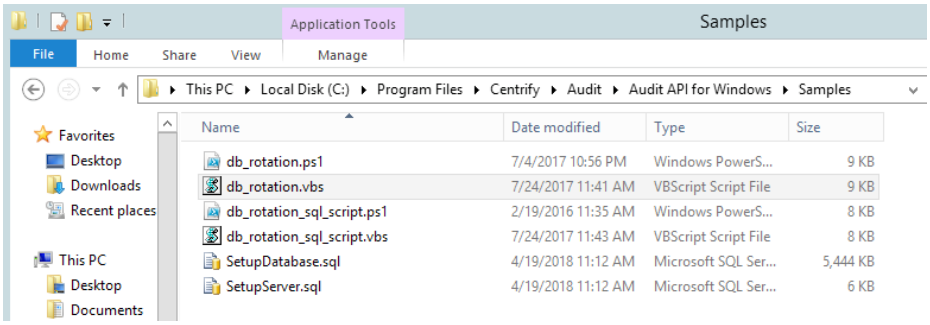


Run the **Centrify DirectAudit SDK64.exe** installer file, agree to the EULA, and next→finish through the installation.



The Auditing SDK includes four samples scripts that can be modified to suit your requirements. For our purposes, we will focus on the **db_rotation.vbs** script. For more information on all of the sample scripts, please refer to the **Database Management Guide**.

The sample scripts are located in **C:\Program Files\Centrify\Audit\Audit API for Windows\Samples**.



Creating the Scheduled Task

Open a PowerShell command prompt as Administrator, and change the directory to the location of the sample scripts.

```
cd 'C:\Program Files\Centrify\Audit\Audit API for Windows\Samples'
```

Next, we run a command that will add the `db_rotation.vbs` script as a scheduled task called '`rotate_database`'. It's a long command, but I will break it down so that you can easily modify it match your environment.

Here is an example of what the command should look like:

```
schtasks.exe /Create /TN "rotate_database" /TR "cscript.exe 'C:\Program Files\Centrify\Audit\Audit API
for Windows\Samples\db_rotation.vbs' DefaultInstallation Demo-Network@centrify.vms-AuditStore
member.centrify.vms\CENTRIFY_SUITE AuditStore" /RU domain\dbadmin /RP P4ssw0rd$ /RL Highest /SC Monthly
/MO 1
```

The command contains the following components:

```
 schtasks.exe /Create /TN <task_name> /TR <task_Command> /RU <run_as_user> /RP <run_as_user_password> /RL
<run_level> /SC <recurrence_rate> /MO <recurrence_increment>
```

Where

- ***task_name***: `rotate_database`
- ***task_command***: `cscript.exe 'C:\Program Files\Centrify\Audit\Audit API for Windows\Samples\db_rotation.vbs' DefaultInstallation Demo-Network@centrify.vms-AuditStore member.centrify.vms\CENTRIFY_SUITE AuditStore"`
- ***run_as_user***: `centrify\dbadmin`
  Note: I used a domain user (domain\user) for the run as user, but 'NT AUTHORITY\SYSTEM', or just 'SYSTEM' are also valid values.
- ***run_as_user_password***: `P4ssw0rd$`

Note: You must supply a password to enable the task to run even if the run as user is not logged in. If you choose to use 'NT AUTHORITY\SYSTEM' or 'SYSTEM', there is no password.

- ***run_level***: Highest
- ***recurrence_rate***: Monthly
- ***recurrence_increment***: 1

The task command consists of the following elements:

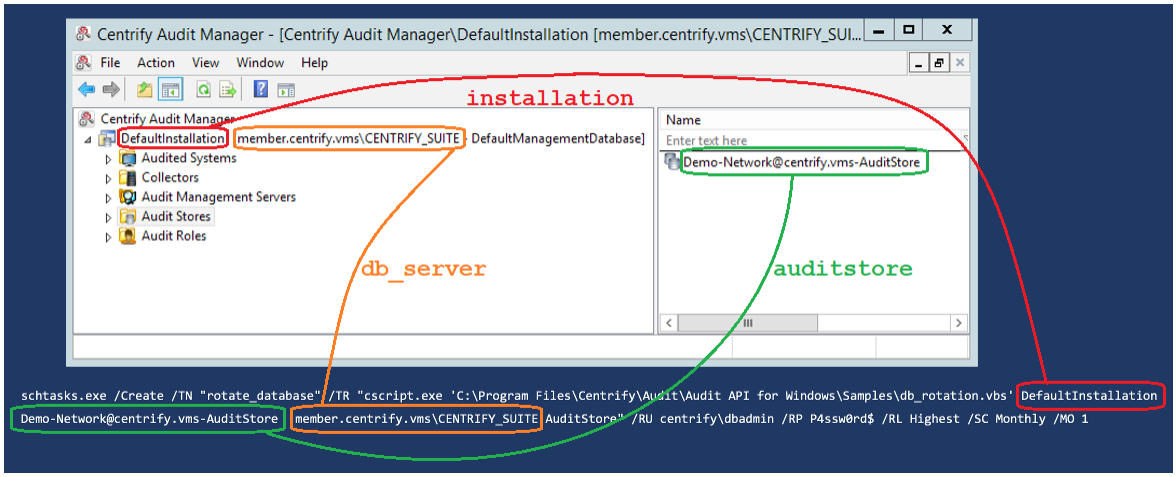
<parser> '<install_path>\<vbs_script>' <installation> <auditstore> <db_server> <db_prefix>

Where

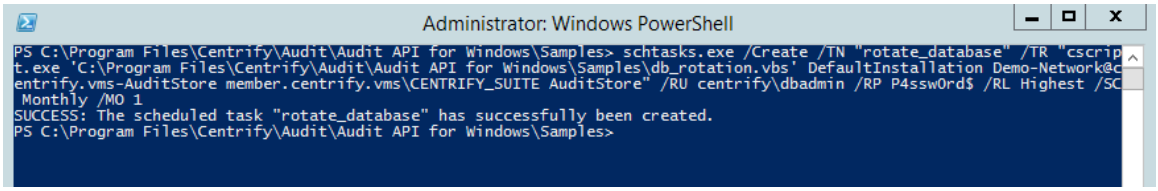
- ***parser***: cscript.exe
- ***install_path***: C:\Program Files\Centrify\Audit\Audit API for Windows\Samples
- ***vbs_script***: db_rotation.vbs
- ***installation***: DefaultInstallation
- ***auditstore***: Demo-Network@centrify.vms-AuditStore
- ***db_server***: member.centrify.vms\CENTRIFY_SUITE
- ***db_prefix***: AuditStore

  Note: The *db_prefix* value can be whatever you want to name the audit database. A date stamp will be attached to the *db_prefix* to compose the new database name.

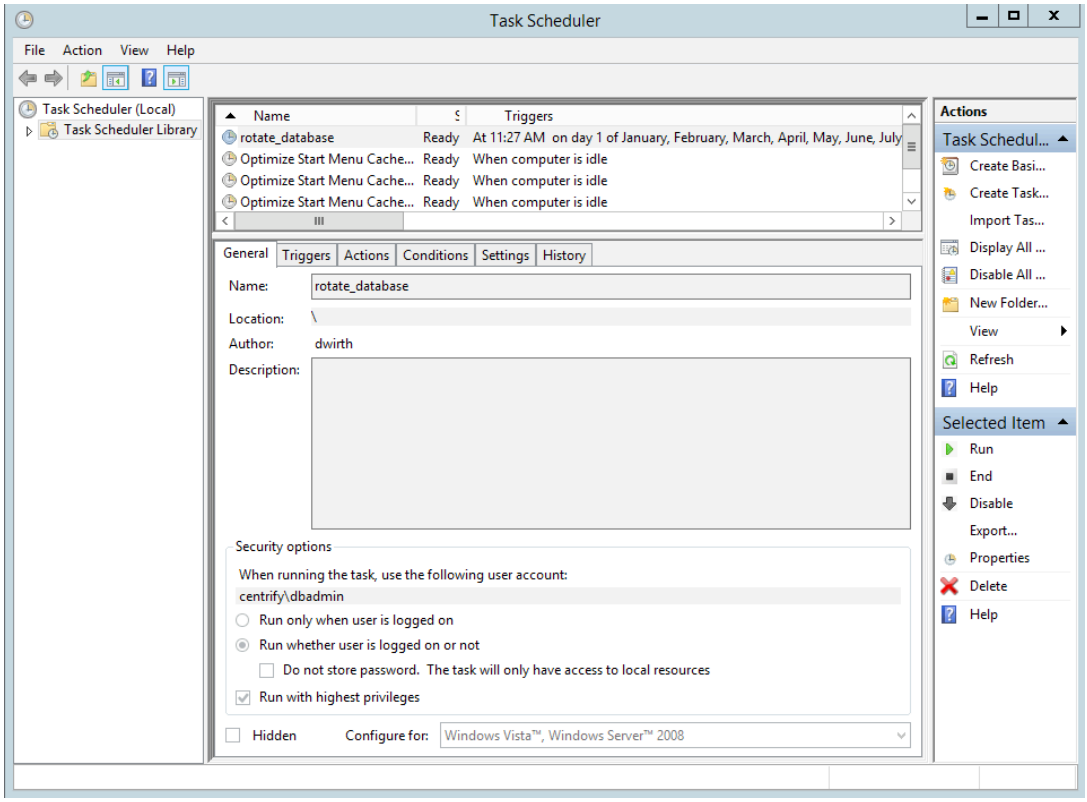
You can easily determine the *installation*, *auditstore*, and *db_server* values by viewing the **Centrify Audit Manager** console. See below.



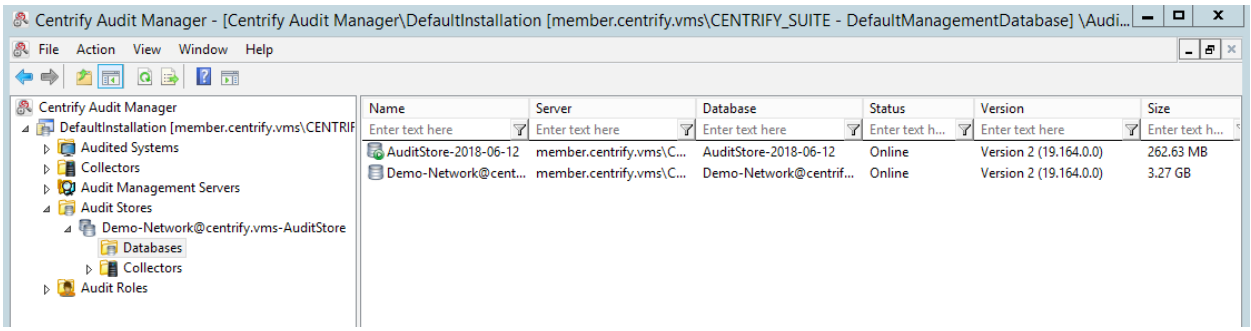
After running the command, you should receive a SUCCESS message.



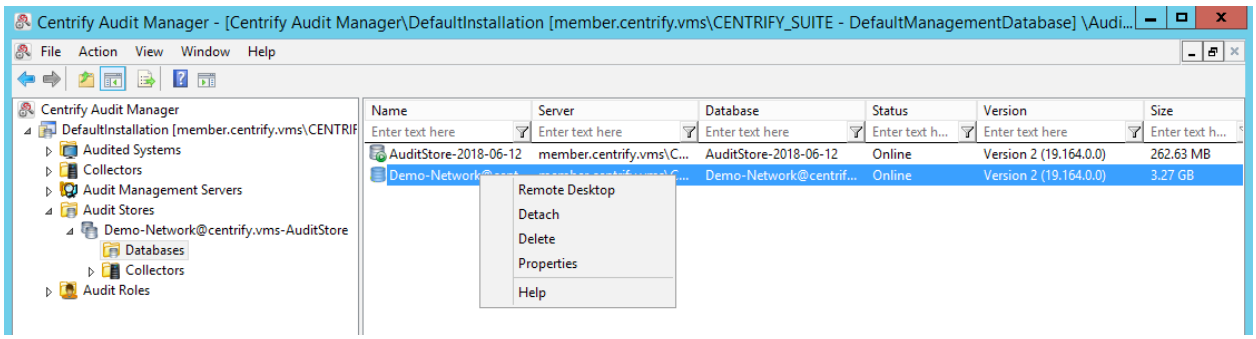
You should now be able to view the newly created task in **Task Scheduler**.



After the task runs, the newly created database is marked as active. The database that has been rotated out will remain attached. By default, the script is configured to detach rotated databases that are older than two years.



If you right-click on the rotated database within the **Centrify Audit Manager**, you can choose to detach or delete it.


Centrify Audit Manager - [Centrify Audit Manager\DefaultInstallation [member.centrify.vms\CENTRIFY_SUITE - DefaultManagementDatabase] \Audi...
File
Action
View
Window
Help
Centrify Audit Manager
DefaultInstallation [member.centrify.vms\CENTRIF
Audited Systems
Collectors
Audit Management Servers
Audit Stores
Demo-Network@centrify.vms-AuditStore
Databases
Collectors
Audit Roles
Name
Server
Database
Status
Version
Size
Enter text here
AuditStore-2018-06-12
member.centrify.vms\C...
AuditStore-2018-06-12
Online
Version 2 (19.164.0.0)
262.63 MB
Demo-Network@centrif...
Online
Version 2 (19.164.0.0)
3.27 GB
Remote Desktop
Detach
Delete
Properties
Help