DirectManage Audit 3.x Databases Migration - Step by step

Centrify Corporation

Abstract

How to migrate databases associated with a Centrify DirectManage Audit 3.x installation from one database server to another

Centrify Corporation
785 N. Mary Avenue, Suite 200
Sunnyvale, CA 94085

TEL (408) 542-7500
FAX (408) 542-7575
URL www.centrify.com

Contents

1 Introduction

A Centrify DirectManage Audit 3.x installation consists of various distributed components such as Audited Systems, Collectors, Audit Manager/Audit Analyzer Consoles and databases which store all the audited data and other settings related to the DirectManage Audit system. It's expected that the database server(s) hosting these databases remain available and unchanged for the DirectManage Audit system to work properly. However, in certain cases, a user may need to migrate these databases from one physical/virtual server to another. The reason behind such move could be upgrading to a newer hardware or upgrading to a newer version of Microsoft SQL server or anything else.

Current version of Centrify DirectManage Audit does not have a built in support for database migration i.e. once a DirectManage Audit 3.x installation is setup, it's expected that the database server's hostname and instance name does not change. This document explains in details what steps should be taken in case if database migration is inevitable in order to keep the impact on the DirectManage Audit system as minimal as possible.

1.1 Audience

This document is intended for system administrators overseeing a Centrify DirectManage Audit 3.x installation in an enterprise. User must have a basic knowledge of Microsoft SQL server database and Active Directory in order to perform tasks mentioned in this document.

Expected time to finish this task is 20-30 minutes. During the migration process, the audited systems will not be able to connect to the collectors and hence will spool the audited data locally. No data during the migration time frame will be lost once the collectors come back online.

2 Things to know before starting the migration

2.1 Types of databases

A DirectManage Audit 3.x installation typically creates and deals with two types of databases i.e. an Audit Server database (also known as the Management database) and Audit Store database. The Audit Server database stores DirectManage Audit 3.x application specific settings whereas the Audit Store database is used to store the actual

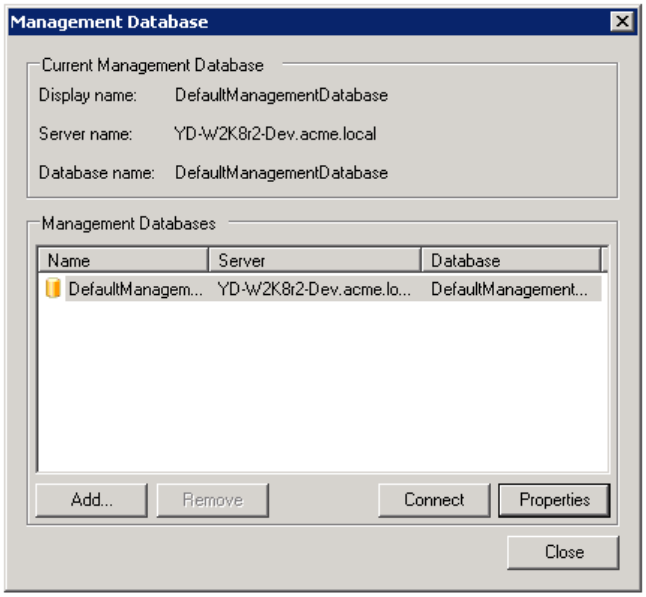
audited user sessions. A typical DirectManage Audit 3.x installation consists of one Audit Server database and one or more Audit Store database(s).

2.2 Note the outgoing account

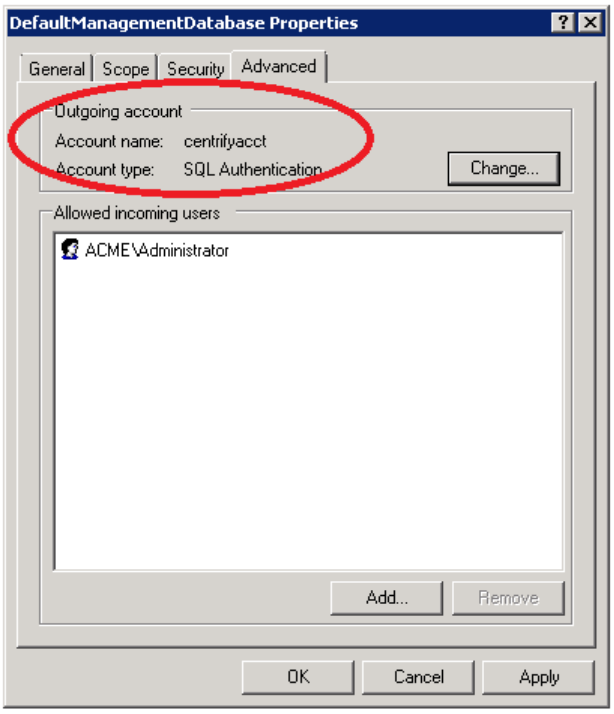
An outgoing account is a Windows authentication or SQL authentication account that is used by the Audit Server database to communicate with the Audit Store database. Before proceeding with the migration, you must note down the Outgoing account name, especially if it's a SQL authentication account.

To find the outgoing account name,

1. Open the Centrify Audit Manager console.
2. Right click on the DirectManage Audit installation name and select **Management Databases**.
3. On the Management Database dialog box, highlight the database and click on **Properties**.



4. On the **Properties** page, go to the **Advanced** tab and check the setting for **Account type**. If the **Account type** is **Windows Authentication**, it indicates that the Audit Server database is currently using its machine account to talk to the Audit Store databases and the authentication mechanism being used is Windows authentication. If the **Account type** is **SQL Authentication**, note down the **Account name**. For the remainder of this document, this account will be called as centrifyacct.



2.3 Where DA stores database information

Typically, the whereabouts of databases associated with a DirectManage Audit 3.x installation are stored in three different data sources.

1. **Active Directory** – Information related to each DirectManage Audit 3.x installation is stored in a Service Connection Point object in the Active Directory. This information includes data points such as installation name, name of the Audit Server database and details of the SQL server hosting this database, license key etc. If a DirectManage Audit 3.x Audit Server database is getting migrated, this information must be updated in Active Directory for a successful migration.

2. **Registry** – Registry may contain some information related to the Audit Server database that belongs to a DirectManage Audit 3.x installation. Typically, this information is stored on machines where DirectManage Audit Manager/Audit Analyzer consoles are installed. This information does not need to be updated when migrating databases associated with a DirectManage Audit 3.x database.

3. **Audit Server database** – The Audit Server database itself stores whereabouts of one or more Audit Store databases associated with the DirectManage Audit 3.x installation and hence this information (typically stored in one or more tables) must be updated when migrating the databases.

3 Use case

In order to explain how to migrate databases from one database server to another, this document will assume a simple use case.

3.1 Assumptions

1. This use case assumes that a DirectManage Audit 3.x installation has been created using Centrify DirectManage Audit 3.0.0 release; the same steps should also work for an installation created using DirectManage Audit 3.0.1 or 3.0.2 release.

2. This use case assumes that the DirectManage Audit 3.x installation consists of one Audit Server database and one Audit Store database. For simplicity, it's also assumed that both the Audit Server database and Audit Store database are being hosted on the same database server\instance.

3. The use case assumes that the databases are being hosted on a database server\instance identified as **DBSERVER\SOURCE** where DBSERVER is the machine name of the database server and SOURCE is the database instance name.

4. The use case assumes that the user wants to move the databases associated with the DirectManage Audit 3.x database to a new database server\instance identified as **NEWDBSERVER\DESTINATION** where NEWDBSERVER is the machine name of the new database server and DESTINATION is the database instance name that is going to host the migrated databases.

5. The use case assumes that the name of the Audit Server database is **DefaultAuditServer** and name of the Audit Store database is **DefaultAuditStoreDatabase**. The name of the Audit Store is **DefaultAuditStore**.

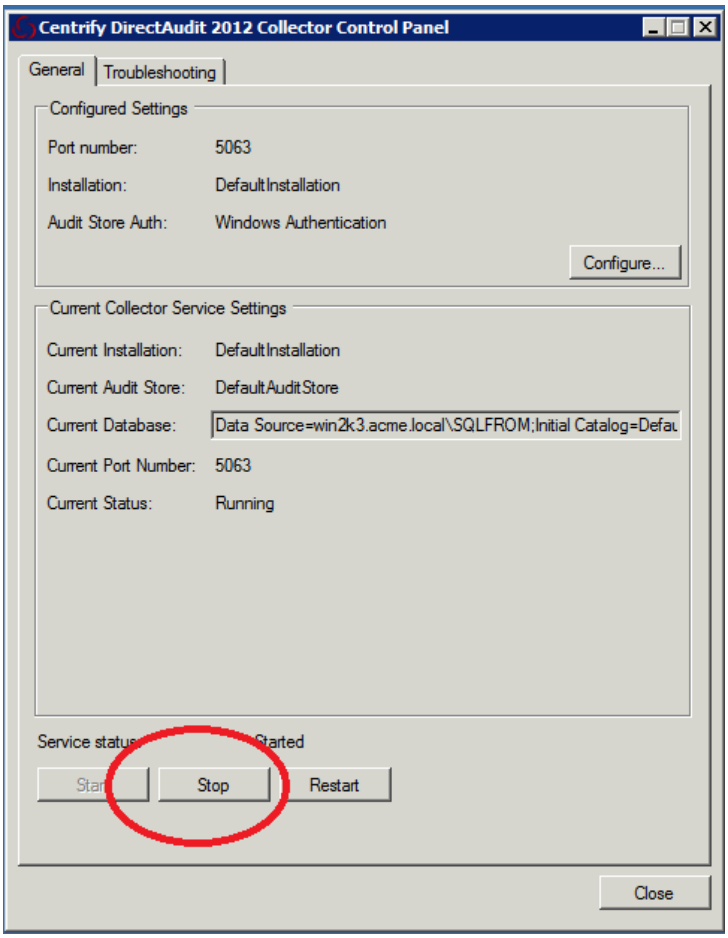
6. The use case assumes that the name of the DirectManage Audit 3.x installation is **DefaultInstallation**

4 Migration – Step by step

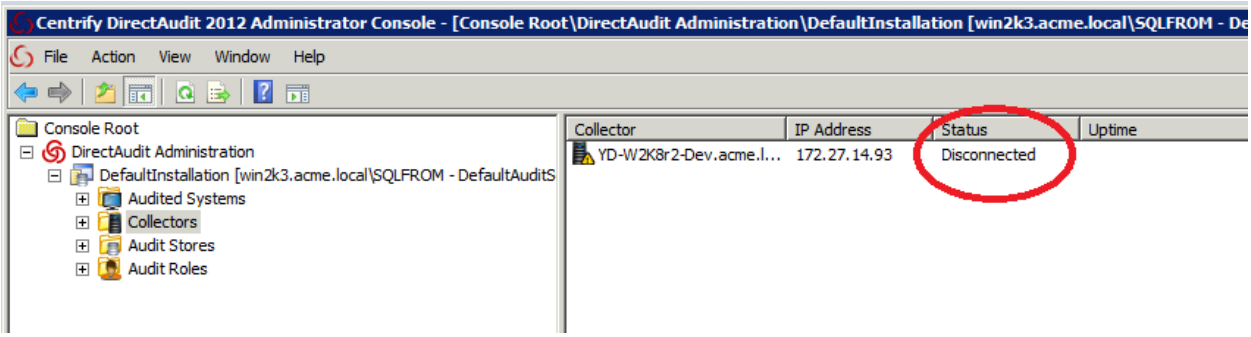
4.1 Step 1 – Stop all the collectors

Permission required *– Local administrator on each of the machines where DirectManage Audit 3.x Collector component is installed and running.*

The databases associated with the DirectManage Audit 3.x installation should not receive any new data while the migration is under way. In order to achieve that, logon to each machine where Centrify DirectManage Audit 3.x Collector component is running and stop the Collector service using the Centrify DirectManage Audit Collector Control Panel. Please refer to the screenshot below,



Ensure that all the collectors are stopped by looking at their connection status in the DirectManage Audit Manager console.



4.2 Step 2 – Take backup of existing databases (optional but recommended)

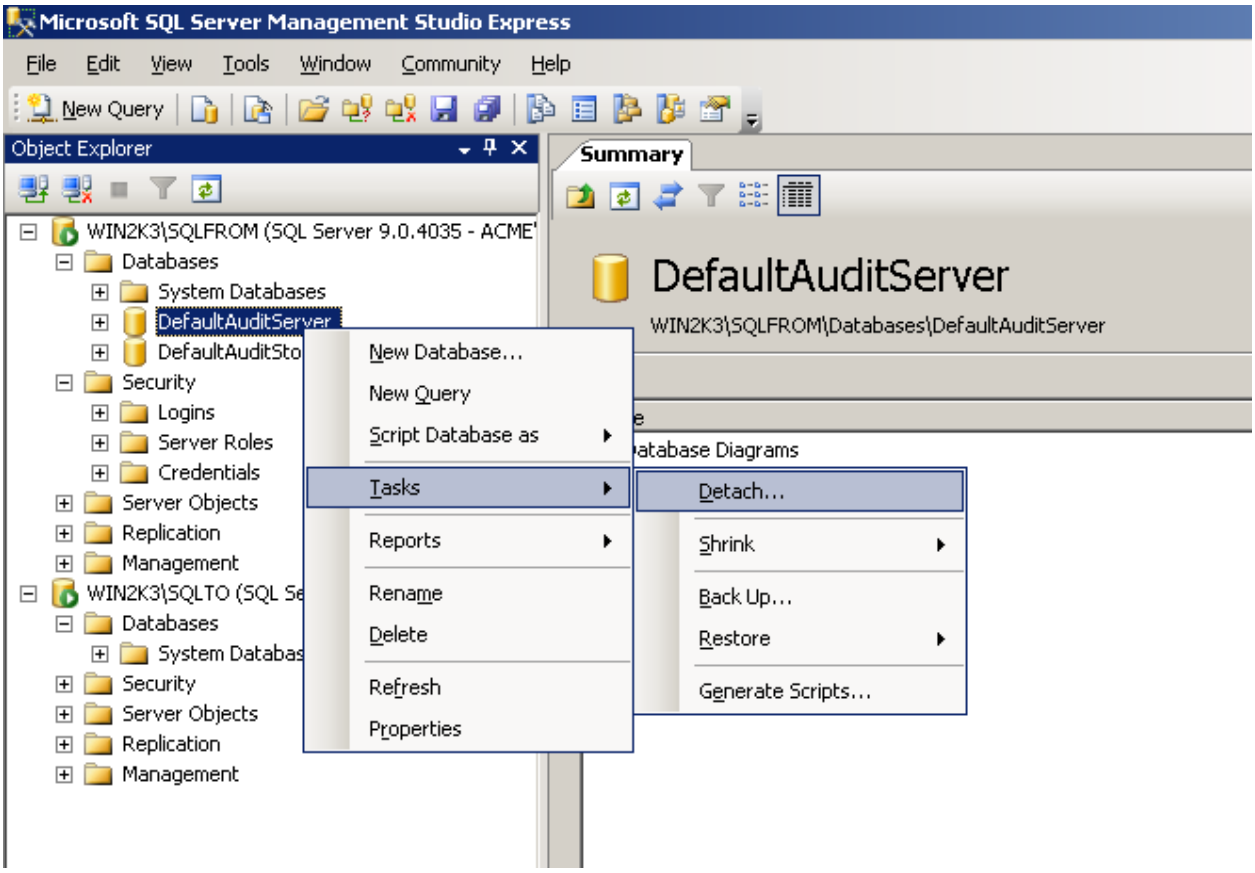
Permission required – DBA on the existing database server

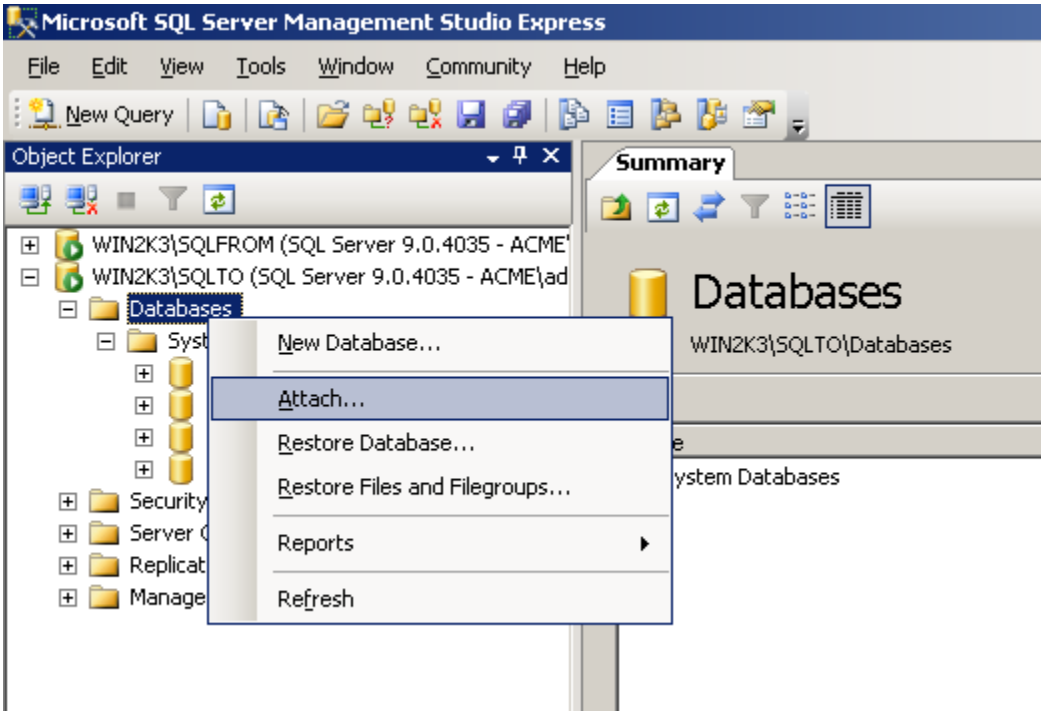
Take a backup of existing Audit Server database and Audit Store database in case if databases need to be restored in future. For this use case, user needs to take full backup of two databases viz. DefaultAuditServer and DefaultAuditStoreDatabase

4.3 Step 3 – Detach the existing databases and attach them to the new database server

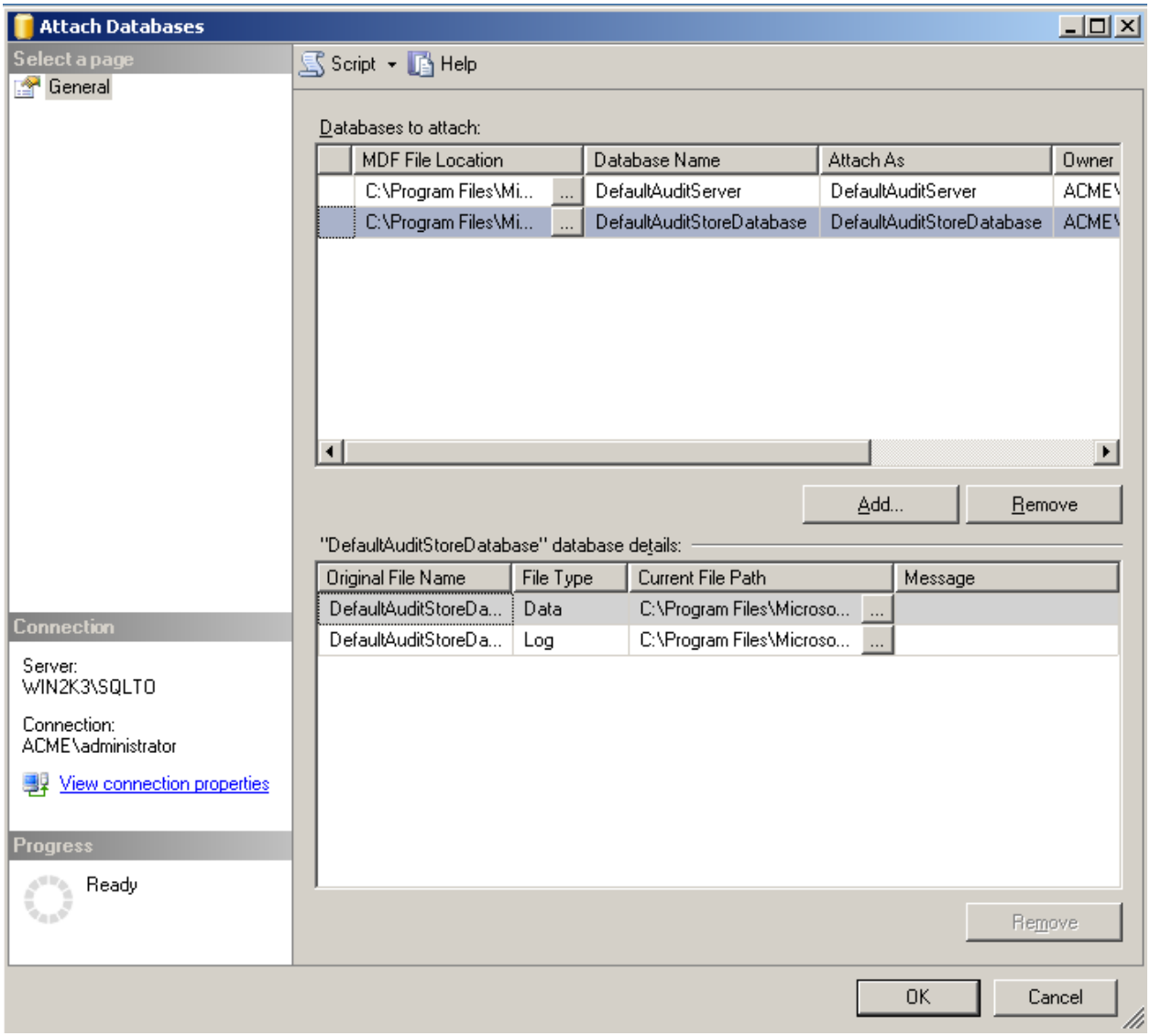
Permission required – DBA on the existing database server and DBA on the new database server

Using SQL Management Studio, detach both the Audit Server database and Audit Store database from DBSERVER\SOURCE and attach the same to the new database viz. DBSERVER\DESTINATION. In order to attach the database files to the new database server, you'll need to physically copy the .mdf and .LDF files of the detached databases to a folder on the new database server.





Once you are ready to attach the database files to the new database server, select **sa** as the Owner of the new databases by selecting **sa** from the Owner dropdown list for both the databases and then click OK.



External links –

How to detach a database using SQL Management Studio

http://msdn.microsoft.com/en-us/library/ms191491(v=sql.90).aspx

How to attach a database using SQL Management Studio

http://msdn.microsoft.com/en-us/library/ms190209(v=sql.90).aspx

4.4 Step 4 – Ensure that CLR integration is enabled on the new database server and login for NT AUTHORITY\SYSTEM exists on the server

Permission required – DBA on the new database server

The CLR integration must be enabled on the database server for DirectManage Audit 3.x system to function properly. In this use case, you must ensure that the new

database server\instance viz. NEWDBSERVER\DESTINATION has the CLR integration enabled. Use the SQL Management Studio and run the following SQL queries on the new database server\instance in order to enable the CLR integration

```
sp_configure 'clr enabled', 1;

GO

RECONFIGURE;

GO
```

External link –

How to enable CLR integration

http://msdn.microsoft.com/en-us/library/ms131048(v=sql.105).aspx

Ensure that the Local System account of SQL Server (NT AUTHORITY\SYSTEM) has a login on the SQL Server instance and it's a member of sysadmin fixed server role. If the required login is missing, run following SQL command to create the same and assign necessary permissions to the same,

```
CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS WITH
DEFAULT_DATABASE=[master]

ALTER SERVER ROLE [sysadmin] ADD MEMBER [NT AUTHORITY\SYSTEM]
```

4.5 Step 5 – Restore the TRUSTWORTHY flag and owner of the database

Permission required – DBA on the new database server

When you detach and attach a database using Microsoft SQL's detach/attach functionality, the value of TRUSTOWRTHY flag is lost when a database is detached and attached back. Use the SQL Management Studio and run the following SQL queries on the new database server\instance viz. NEWDBSERVER\DESTINATION to restore the flag value correctly,

```
ALTER DATABASE [DefaultAuditServer] SET TRUSTWORTHY ON

ALTER DATABASE [DefaultAuditStoreDatabase] SET TRUSTWORTHY ON
```

Tip – If you have moved more than one Audit Store databases from old database server to the new database server, you'll need to set the TRUSTWORTHY flag ON for each of the Audit Store databases.

Once the database is attached, set sa as the owner of the database by running following SQL command,

```
ALTER AUTHORIZATION ON DATABASE::<DB_NAME> TO [sa]
```

```
e.g. ALTER AUTHORIZATION ON DATABASE::DefaultAuditServer TO [sa]
```

4.6 Step 6 – Modify the newly attached Audit Server database

Permission required – DBA on the new database server

As explained previously, the Audit Server database itself stores whereabouts of Audit Store database in a couple of database tables. These entries must be manually modified for the migration to be successful.

1. Using SQL Management Studio, open a database connection to the new database server\instance viz. NEWDBSERVER\DESTINATION and open the Audit Server database viz. DefaultAuditServer database.

2. Open the **AuditStoreDatabase** table and rename all references of DBSERVER\SOURCE to NEWDBSERVER\DESTINATION. In most cases, you'll only need to modify the contents of Server column of the AuditStoreDatabase table.

3. Open the **ManagementDatabase** table and rename all references of DBSERVER\SOURCE to NEWDBSERVER\DESTINATION. In most cases, you'll only need to modify the contents of the Server column of the ManagementDatabase table.

4.7 Step 7 – Restoring connection between Audit Server database and Audit Store database

Permission required – DBA on the new database server

Important – Please skip to the next section (Special Case) if the Outgoing account discovered in Step 2.2 was a SQL Authentication account.

In most cases, the Audit Server database talks to the Audit Store database using the machine account of the SQL server that is hosting the Audit Server database. When you move (detach-attach) the Audit Server database from one physical/virtual server to another, this connection is lost. In order to restore this link, run following SQL queries on each of the Audit Store databases hosted on the new database server\instance.

```
CREATE USER [DOMAIN\MACHINENAME$] FOR LOGIN [DOMAIN\MACHINENAME$] WITH DEFAULT_SCHEMA=[dbo]
```

Where,

DOMAIN **–**NetBIOS name of the domain to which the new database server is joined

MACHINENAME$ - Machine name of the new database server hosting the Audit Server database (The machine name must have the $ suffix)

e.g. For this use, the SQL query would be,

```
CREATE USER [DOMAIN\NEWDBSERVER$] FOR LOGIN [DOMAIN\NEWDBSERVER$] WITH DEFAULT_SCHEMA=[dbo]
```

Once the login is created for the Audit Server database account, make this new login a member of ***managementdb*** database role by running following SQL query,

```
EXEC sp_addrolemember 'managementdb', [DOMAIN\MACHINENAME$]
```

Where,

DOMAIN\MACHINENAME$ - The new login created by the previous SQL query

e.g. For this use case, the SQL query would be,

```
EXEC sp_addrolemember 'managementdb', [DOMAIN\NEWDBSERVER$]
```

Special case – Using SQL Authentication for communication between databases

In some cases (e.g. one way trust), the Audit Server database cannot talk to the Audit Store database using the machine account of the SQL server that is hosting the Audit Server database. In such cases, a SQL account is used for communication between the two databases. In DirectManage Audit terminology such account is known as Outgoing account. When you move (detach-attach) the Audit Server database from one physical/virtual server to another, this Outgoing account must be created on the new SQL server in order to restore the connection between the two databases. Use the SQL management studio to connect to the new SQL server and manually create this Outgoing account. When you create the account, make sure that,

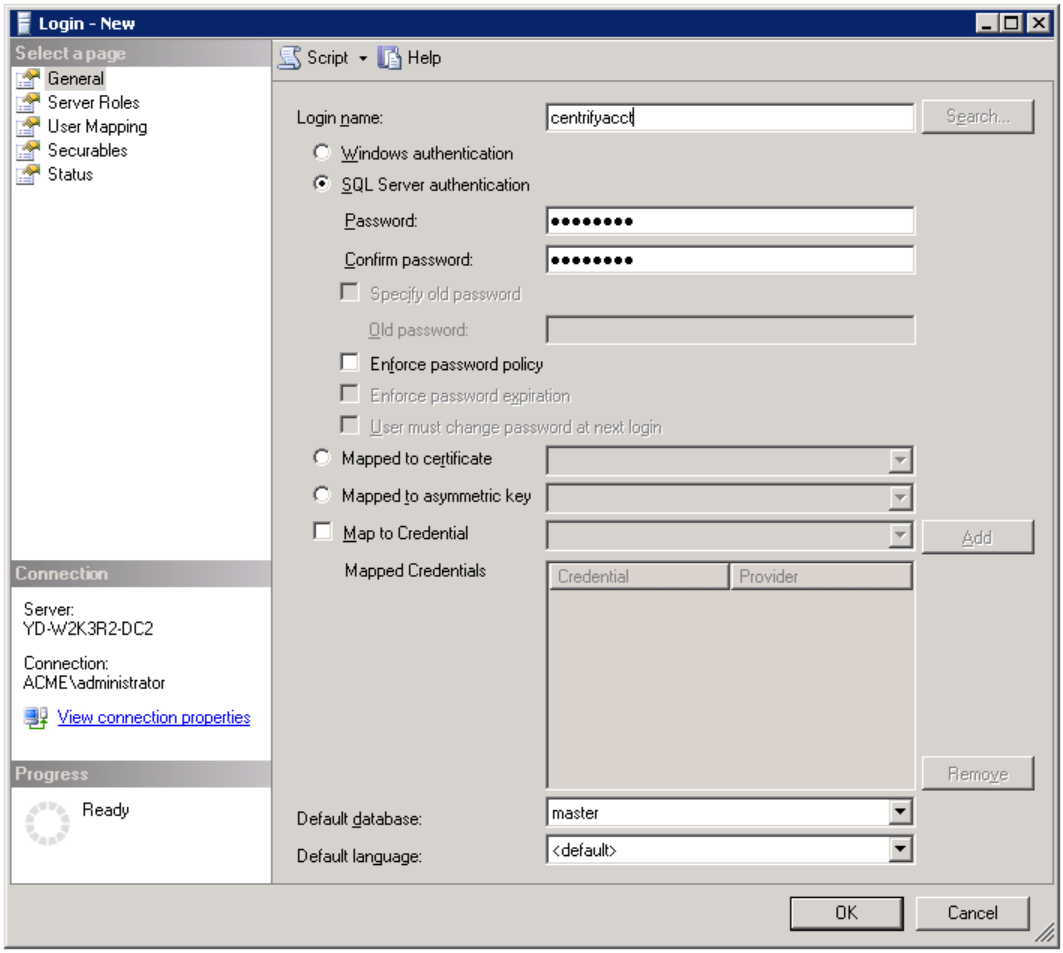
a) The account's login name is same as the Outgoing account name discovered in step 2.2. In this example use case, the Outgoing account name is centrifyacct.

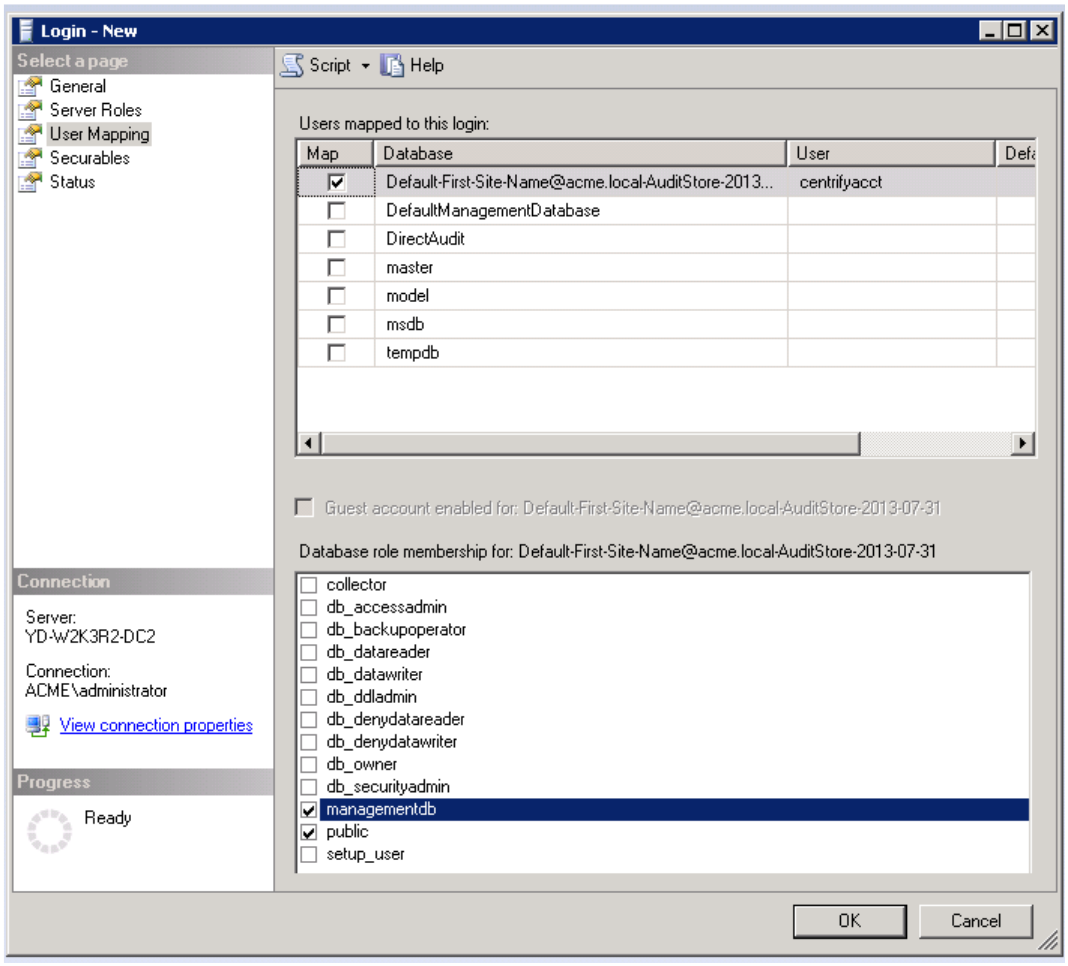
b) The account's login type is SQL Server authentication

c) The account password is same as that on the older SQL server

d) Under **User Mapping**, this new account is mapped to the newly attached Audit Store database and is a member of **managementdb** role on this database.

Please refer to the screenshots below for additional information,





4.8 Step 8 – Update the database entries in Active Directory

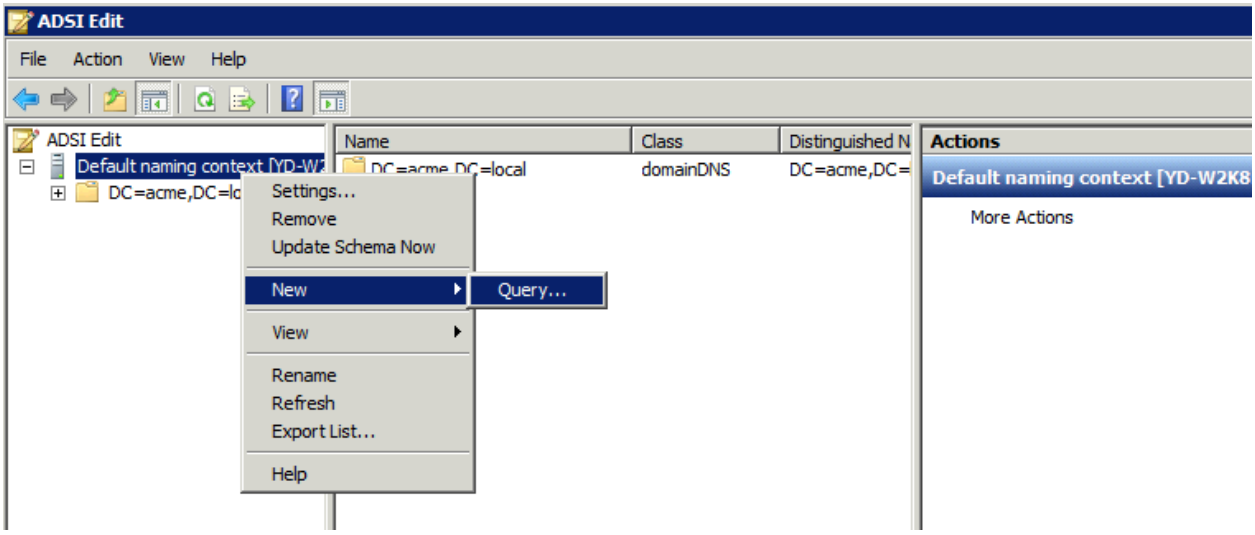
Permission required – Active Directory administrator

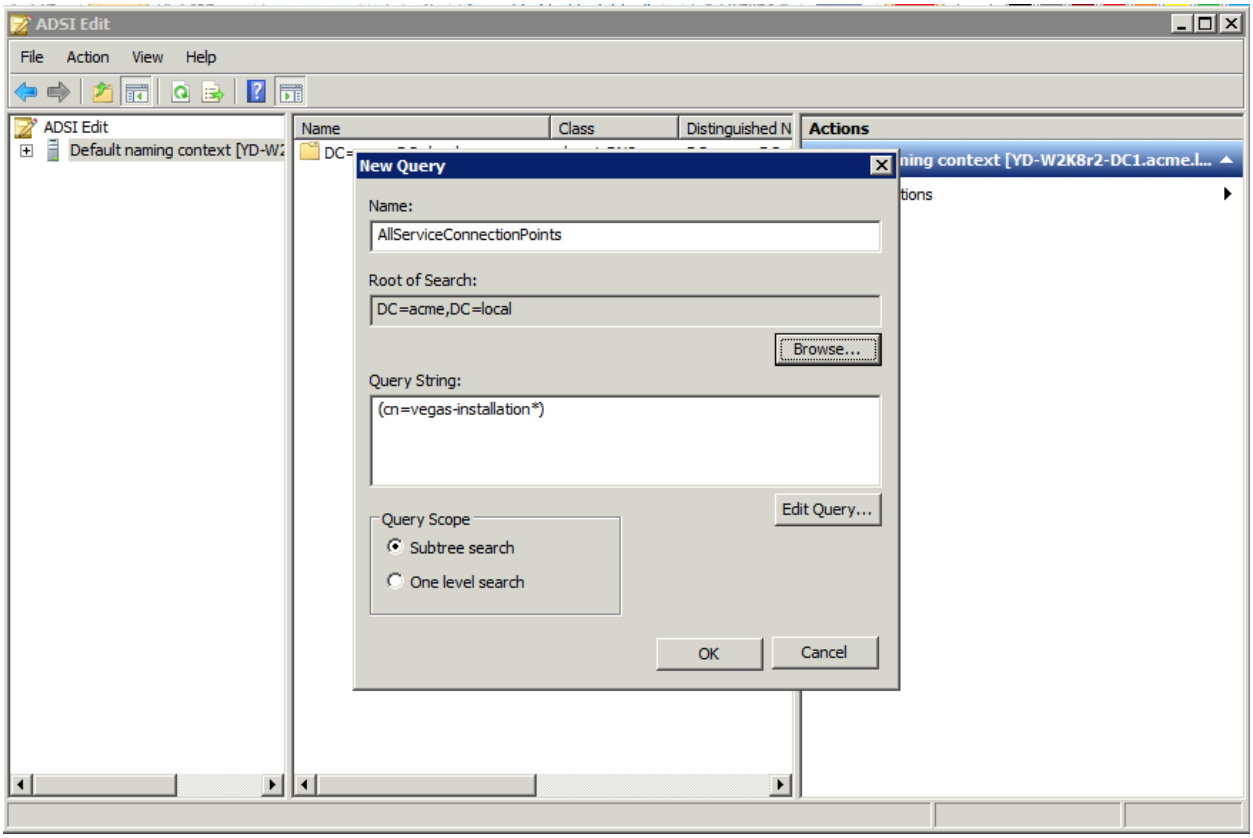
In this step, you'll update the information of DirectManage Audit 3.x database that is stored in the Active Directory. DirectManage Audit stores this information in a Service Connection Point object and hence first step to update the entries is to locate this Service Connection Point in Active Directory.

1. Using an Active Directory management tool such as **ADSIEdit.msc**, find the Service Connection Point object corresponding to the DirectManage Audit 3.x installation. The Service Connection Point object starts with the prefix ***Vegas-Installation*** and hence following LDAP query should return all the Service Connection Point objects in the Active Directory

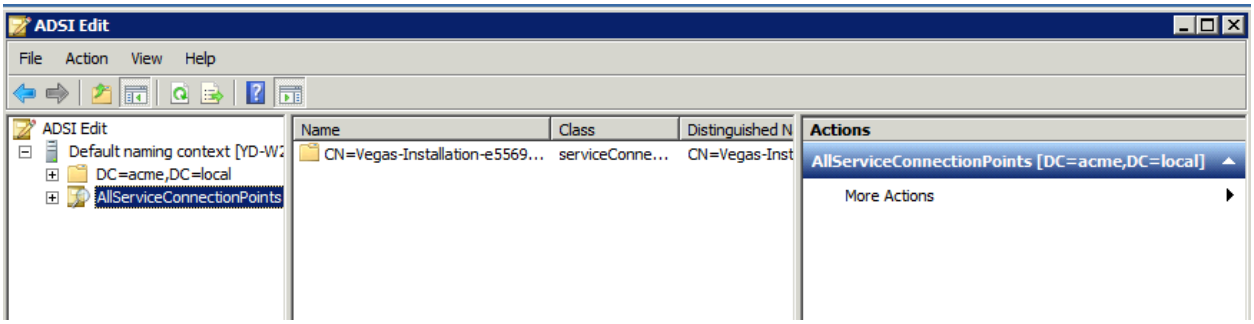
   (cn=Vegas-Installation*)

   Screenshots below show how to create a new LDAP query using the ADSIEDIT.msc tool,

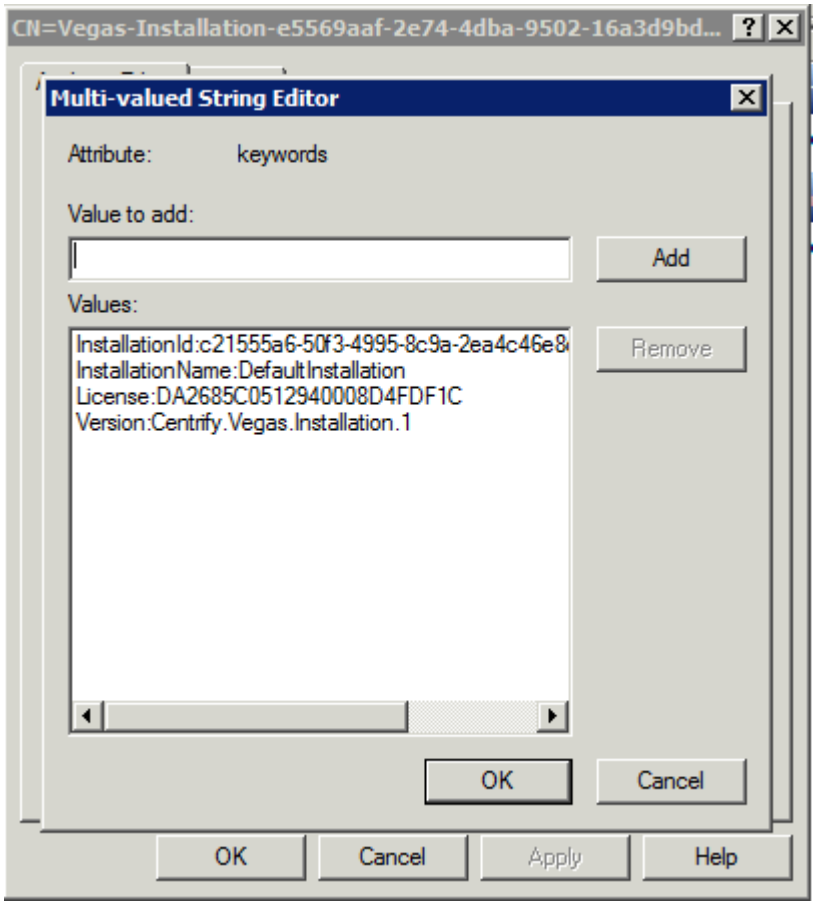




Run the newly created LDAP query and it should show the Service Connection Point object associated with the installation in the right pane.

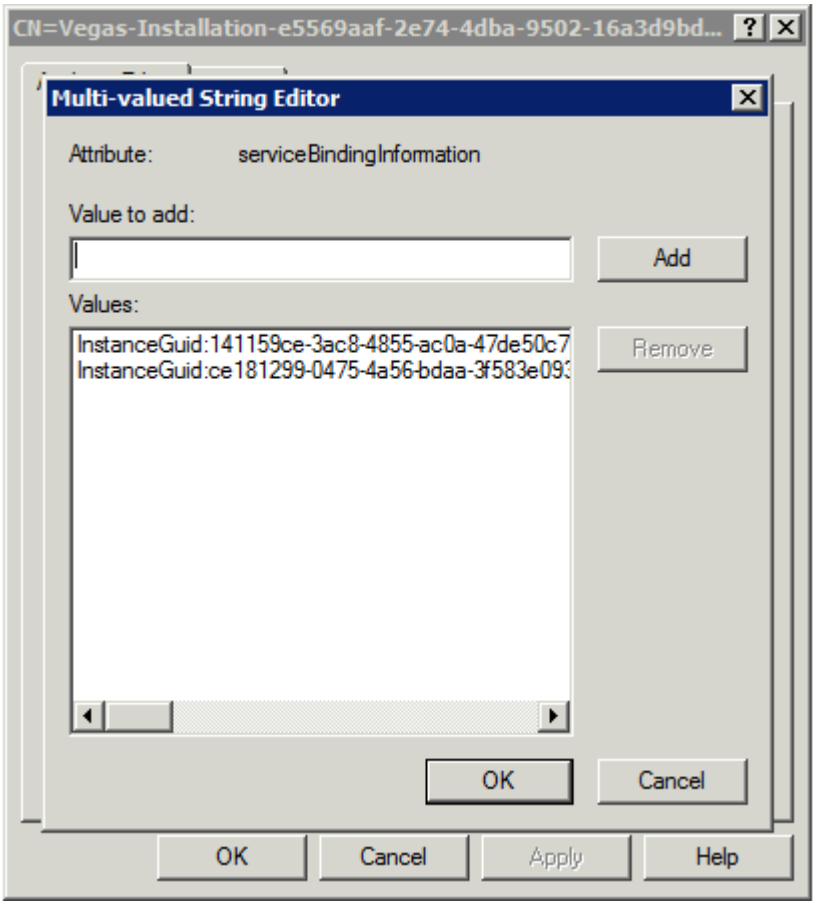


If the search returns more than one Service Connection Points, it indicates that more than one installation is available in the Active Directory. In such case, simply open each of the Service Connection Points in the search result (Right Click > Properties) and look at the value of attribute named **Keywords**. This attribute stores the name of the DirectManage Audit 3.x installation associated with this Service Connection Point e.g. For DirectManage Audit 3.x installation named DefaultInstallation, the keywords attribute must contain a value InstallationName:DefaultInstallation. Please refer to the screenshot below,



2. Once you locate the Service Connection Point object, open the Properties window (Right Click > Properties) and locate the **serviceBindingInformation** attribute.

3. Rename all the references of DBSERVER\SOURCE to NEWDBSERVER\DESTINATION in all the values assigned to the serviceBindingInformation attribute. Since this is a multi value attribute, there would be more than one value containing reference to the old database server\instance viz. DBSERVER\SOURCE.



4.9 Step 9 – Start all the collectors

Permission required *– Local administrator on each of the machines where DirectManage Audit 3.x Collector component was previously stopped.*

Since the migration process is complete, logon to each machine where Centrify DirectManage Audit 3.x Collector component was previously stopped and start the Collector service using the Centrify DirectManage Audit Collector Control Panel.

