Setup ADchangeTracker instructions

Installation and configuration of ADchangeTracker service.

Please see [Active-Directory-change-tracking](http://www.codeproject.com/Articles/1002714/Active-Directory-change-tracking) for more information.

Table of Contents

[1 Configure Event Logging in Active Directory 1](#_Toc423003981)

[2 Create a service user in Active Directory 1](#_Toc423003982)

[3 Grant service user permission to read Security Log on all DC‘s 2](#_Toc423003983)

[4 Create security group for AD reports 3](#_Toc423003984)

[5 Create a database in SQL server 3](#_Toc423003985)

[6 Create logins and grant permissions in SQL server 3](#_Toc423003986)

[7 Install ADchangeTracker service on all writable DC‘s 3](#_Toc423003987)

[8 Install and configure reports in SSRS 4](#_Toc423003988)

In the downloaded ZIP file you will find the following files:

|  |  |  |
| --- | --- | --- |
| Filename | What is it | To Do |
| Setup ADchangeTracker instructions.PDF | This document | Read it |
| Active Directory change auditing screenshots.PDF | AD event logging help |  |
| Setup.exe | The ADchangeTracker service | Run on Domain Controllers |
| CreateAD\_DWdatabase.sql | Create DB T-SQL script | Run on SQL server |
| CreateLogins.sql | Create logins T-SQL script | Run on SQL server |
| AD\_Events.rdl | SSRS report | Upload to SSRS server |
| EventXml.rdl | SSRS report | Upload to SSRS server |

# Configure Event Logging in Active Directory

**You will need Domain Admin permissions to perform this task.**

This is by far the most time consuming task – also the most technical.

Use **Group Policy Management** tool and **Active Directory Users and Computers** tool to perform the tasks required in this step.

*Note – you can continue and complete the remaining steps of the ADchangeTracker setup process even if you have not successfully completed this one. But you will not see much data flowing into the SQL DB unless AD change events are generated into the Security Log.*

This web page provides very good information on how to do this:

[How to enable Active Directory Change Events](http://www.morgantechspace.com/2013/08/how-to-enable-active-directory-change.html)

Please see also the included document “Active Directory change auditing screenshots.PDF”.

After you have completed this step – you should verify that AD change events are generated when an object in AD is changed. See this reference: [Active Directory Change and Security Event IDs](http://www.morgantechspace.com/2013/08/active-directory-change-audit-events.html)

Here are a few other websites for reference:

[Who Moved the AD Cheese?](http://blogs.technet.com/b/askpfeplat/archive/2012/04/22/who-moved-the-ad-cheese.aspx)

[AD DS Auditing Step-by-Step Guide](https://technet.microsoft.com/en-us/library/cc731607(WS.10).aspx)

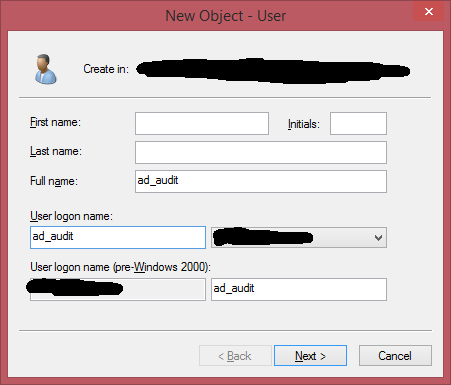
[Active Directory Services Audit - Document references](http://social.technet.microsoft.com/wiki/contents/articles/15232.active-directory-services-audit-document-references.aspx)

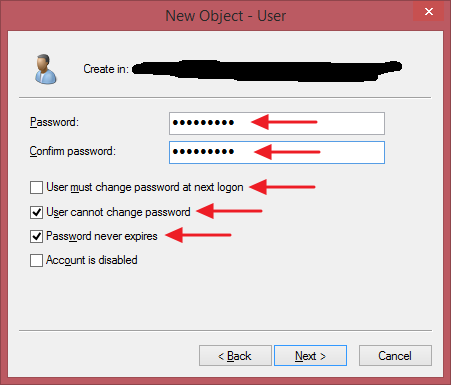
# Create a service user in Active Directory

**You will need Domain Admin permissions to perform this task.**

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Create a user named “**ad\_audit**” in an OU where you normally keep service users (you can change the name of course).





This user will run the **ADchangeTracker** service on all writable domain controllers. The user needs permissions to read the **Security Log** on the domain controllers (Step 3) and will also need permissions to execute stored procedures in the **AD\_DW** SQL database (Step 6).

# Grant the service user permission to read Security Log on all DC‘s

**You will need Domain Admin permissions to perform this task.**

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Click on “**Builtin**” OU, double click “**Event Log Readers**” group. Add “**ad\_audit**” user to the group.

This will grant the user permission to read the **Security Log** on all Domain Controllers.

# Create security group for SSRS reports

**You will need Domain Admin permissions to perform this task.**

Use **Active Directory Users and Computers** tool to perform the task required in this step.

Create a security group named “**SG-ADreports**” in an OU where you normally keep such groups. Add all the users you want to have access to the reports (you can change the group name of course).

*Note – the users you added to the group will need to log out and then in again on their workstations before group membership is updated.*

This security group will be used both in SQL server and in SQL Server Reporting Services.

# Create a database in SQL server

**You will need SysAdmin permissions in SQL server to perform this task.**

Use **SQL Management Studio** tool to perform the task required in this step.

Connect to the SQL server where the database will reside, open the included **CreateAD\_DWdatabase.sql** file and run it.

This T-SQL script will create the **AD\_DW** database, tables, indices, views and stored procedures.

# Create logins and grant permissions in SQL server

**You will need SysAdmin permissions in SQL server to perform this task.**

Use **SQL Mangement Studio** tool to perform the task required in this step.

Connect to the SQL server where the **AD\_DW** database is found, open the included **CreateLogins.sql** file.

Now do a find/replace on “DOMAIN” replace with your domain name in the script.

Now run the script.

This T-SQL script will grant read, execute permissions to the **SG-ADreports** security group and execute to the **ad\_audit** user on the **AD\_DW** database.

# Install ADchangeTracker service on all writable DC‘s

**You will need Domain Admin permissions to perform this task.**

Do the following on **all writable domain controllers** in your domain.

* Log on to a domain controller.
* Run the included **Setup.exe**.

*After setup completes you will find a new service “****Active Directory change tracker****” in the list of services. This service is not running yet, you need to configure a few things before it can run.*

* Run **Notepad** as Administrator.
* Open the **C:\Program Files (x86)\ADchangeTracker\ADchangeTracker.cfg** file.
* Edit the “*# SqlConnString etc*“ line, remove the “# “ (hashtag space) from the beginning of the line and change *‘SQLserverName’* to the name of the SQL server where the **AD\_DW** database is found.
* You don’t need to change the other settings in the file.
* Save the file and close Notepad.
* Open **Services** tool.
* Right click on the **Active Directory change tracker** service, select **Properties**.
* Click on **Log On** tab.
* Select **This account**, click **Browse** button, type “**ad\_audit**” in the textbox. Click **Locations** button, select “**Entire Directory**” and click **OK** button. Click **Check Names** button and if no error; click **OK** button.
* Type the password for user **ad\_audit** in the textboxes for password and click **OK** button.
* Click on **General** tab.
* Change **Startup type** to **Automatic.**
* Click **Apply** button.
* Click **Start** button.
* Click **OK** button.

Open **File Explorer** and go to **C:\ProgramData\ADchangeTracker** (note – **ProgramData** is a hidden folder).

Open the log file in **Notepad** that was created when the service started. Check for any errors.

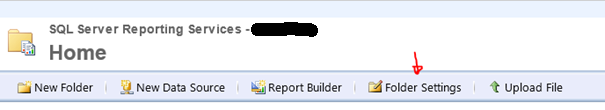
Log files are named like this: ***ADchangeTracker\_YYYY-MM-DD\_HH-MM-SS.log***

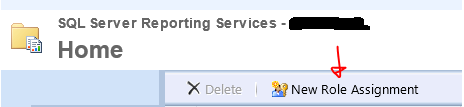
# Install and configure reports in SSRS

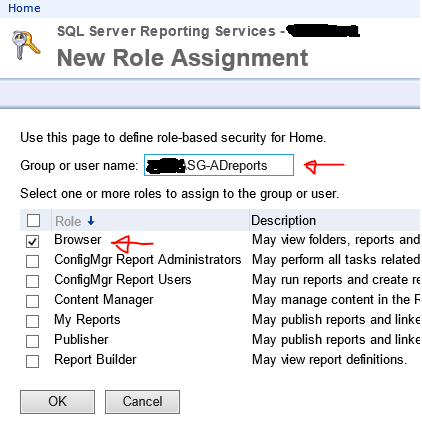
**You will need System Administrator permissions on SSRS to perform this task.**

Open **Internet Explorer** and browse to the **Home** page of the **SQL Server Reporting Services** server.

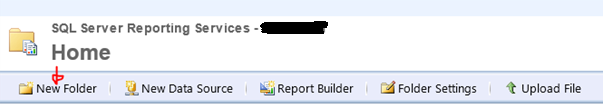
|  |
| --- |
| Grant the SG-ADreports security group Browser permission on the Home folder. |

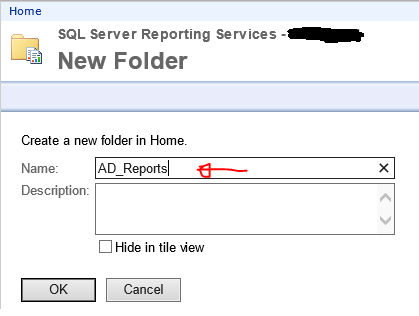




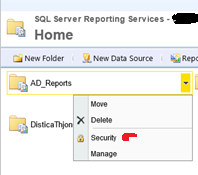


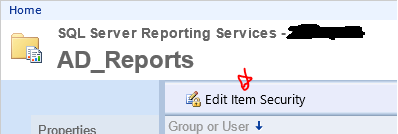
|  |
| --- |
| Create a new folder “AD\_Reports” (you can change the name of course). |

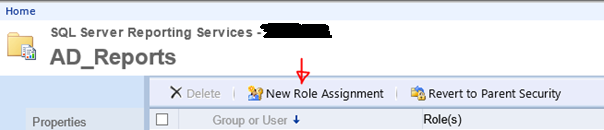


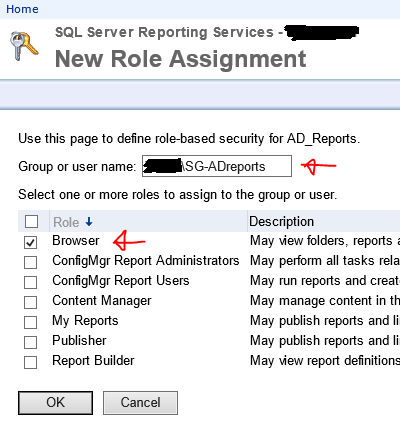


|  |
| --- |
| Grant SG-ADreports security group Browser permission on the folder. |

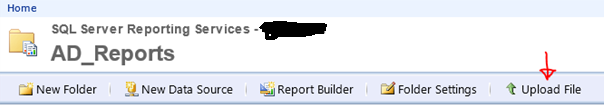


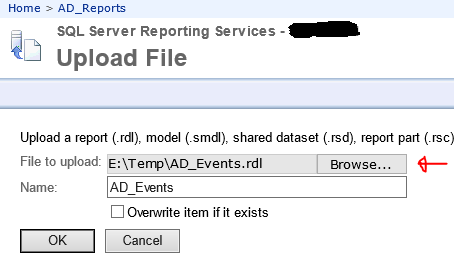


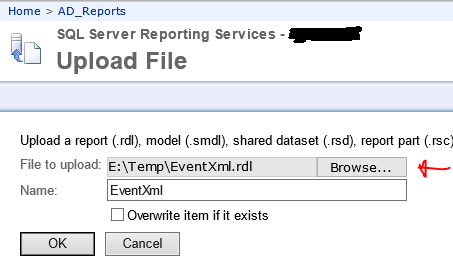




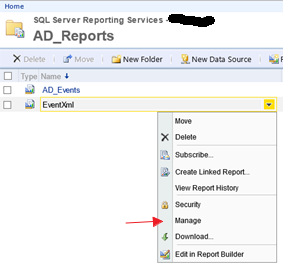
|  |
| --- |
| Upload the supplied two report files - AD\_Events.rdl and EventXml.rdl. |

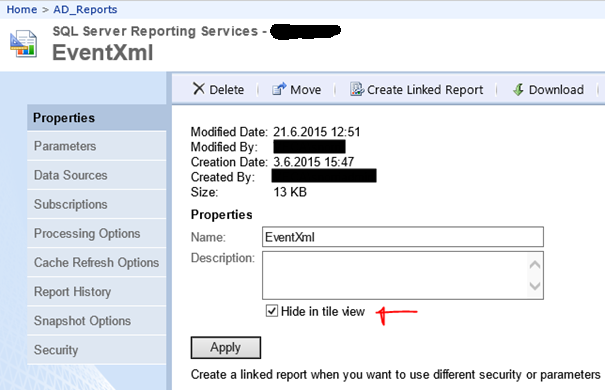






|  |
| --- |
| Set the EventXml report as hidden (because it’s a subreport). |





|  |
| --- |
| Change the connection string for the reports – set the name of your SQL server. |

