**MS SQL SERVER**

**Standard Operating Procedures**

**(SOP)**

**Access management for SSAS**

**SQL Server Analysis Services**

Submitted to

****

**By**



CIS, Wipro Limited

Document Details

|  |  |
| --- | --- |
| Project Name | Innogy SE |
| Account | CIS |
| IT Component/Application Title | Access management for SSAS |
| Current Version | 1.2 |
| List of Contributors | Pradipkumar Kansara, Kiran Bhalekar, Ayushi Gautam, Sivakumar Goud, Pramod Patil |
| Customer Contact Information |  |

Version History

(All revisions made to this document must be listed in chronological order. All revisions must be approved. Review and Approval can be done by an internal source or by the customer)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Date of Revision | Description | Author | Reviewed By | Approved By |
| 1.0 | 08-12-2017 | Initial Draft | Kiran Bhalekar | Pradipkumar Kansara | Santosh Badiger |
| 1.1 | **13-12-2017** | **Document Completed** | **Kiran Bhalekar** | **Pradipkumar Kansara** | **Santosh Badiger** |
| 1.2 | **10-12-2018** | **Updated the content** | **Pramod Patil** | **Pradipkumar Kansara** | **Santosh Badiger** |

Document Distribution List

|  |  |  |
| --- | --- | --- |
| **Sr.No** | **Name and Company** | **Purpose** |
| **1** | RWEIT-SQLDBA | **This document is useful to understand access management for SSAS** |
| **2** |  |  |

**TABLE OF CONTENT**

[1. Purpose 4](#_Toc215826375)

[2. Scope 4](#_Toc215826376)

[3. Administor configuration during installation 4](#_Toc215826377)

[4. Reference 15](#_Toc215826378)

# 

# Purpose

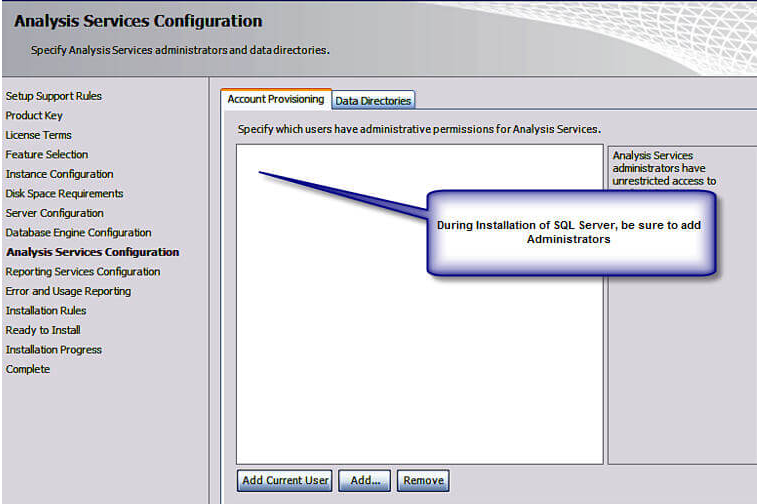
This document is to cover access management for SSAS i.e. SQL Server Analysis Server. This will help you in understanding the steps involved in giving access to SSAS.

# Scope

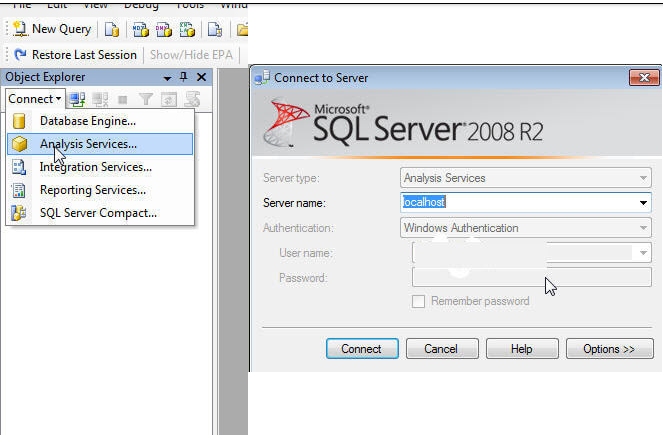
This document is prepared for GSMC Wipro sustenance team and provides the concepts of access management for SSAS.

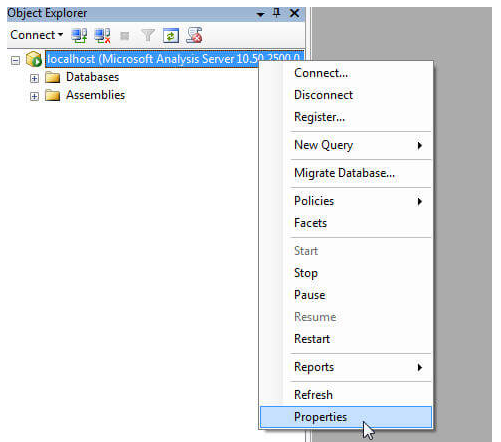
# Administrator configuration during SQL server installation:

During the SQL Server installation, first time DBAs and DWAs are tempted to just click next.. next ... next. However, many of the installation screens contain vitally important selections that impact your department for the life of your installation. It is of the utmost importance to plan your installation well and ultimately test your installation results. One such planning item is determining who the SSAS Administrators will be. Once that decision is made, adding the appropriate users on the SSAS Account provision screen is as easy as adding the appropriate users as noted in the below screen print. These users will have full rights to ALL SSAS databases, cubes, and dimensions, and more importantly, the ability to add other users as full administrators to the instance or individually to single SSAS databases.

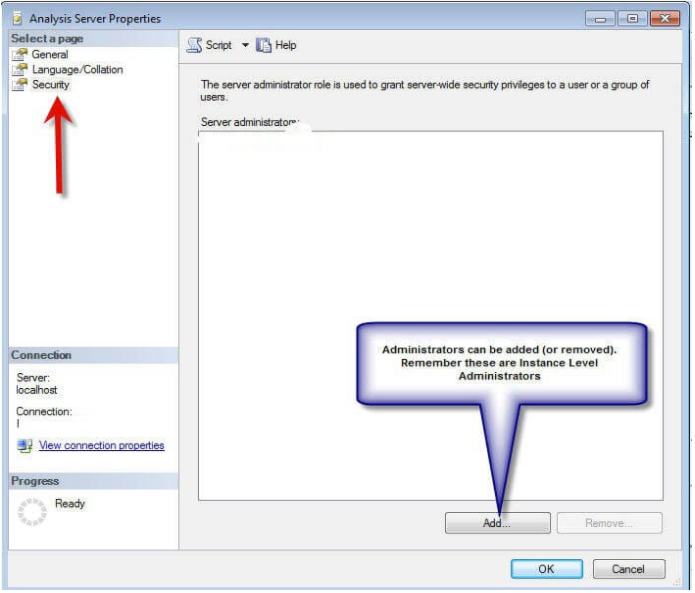


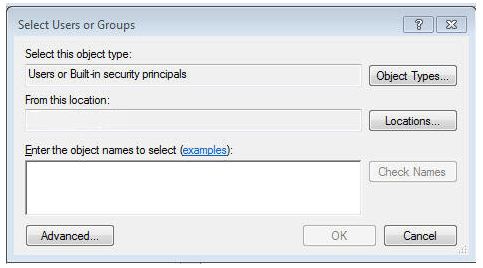
If additional administrators need to be added after the Installation, they can be added in Management Studio (SSMS). Depending on your level of experience, you may not realize that you can connect to Analysis Services (and Reporting Services for that matter) in Management Studio. First Open SSMS and then click Connect > Analysis Services



Once the connection is successful, right click on the Instance and Select Properties

As noted below, within the SSAS Instance Properties, select security. On this window, new instance level administrators (including groups) can be added (or old ones can be removed). The normal Windows user selection box appears which allows you to search for and validate users. Now that the instance level security is setup, database and cube level security can be created.

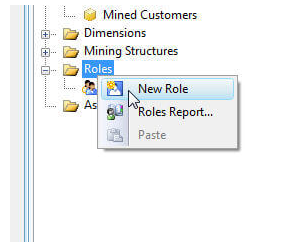




### Database and Cube Level Security

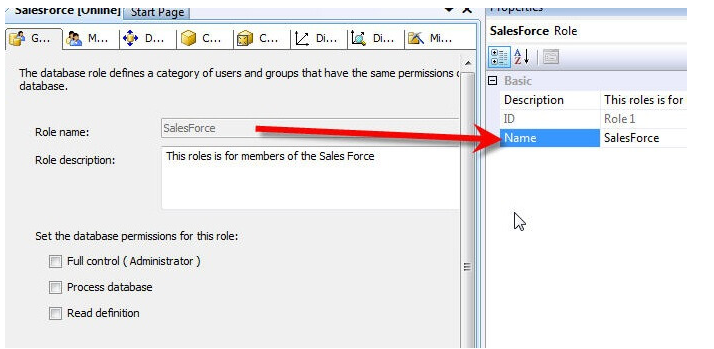
Database and cube level security can be maintained in either BIDS or Management Studio (if you are using a SSAS Project, which helps with deployment and version control, remember each deployment will overwrite the current security unless you use the deployment wizard

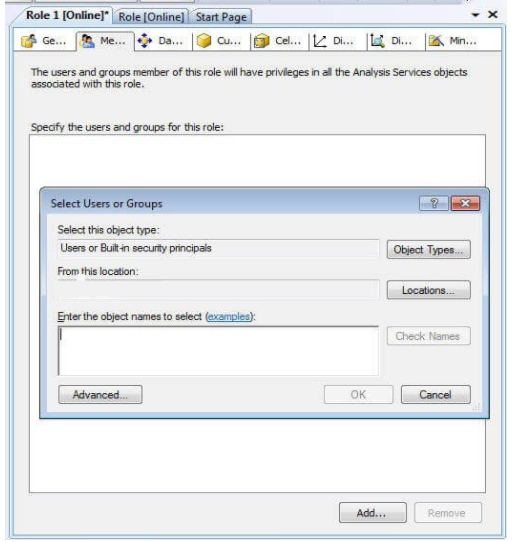
My preference is to use BIDS, although the screens are very similar in either Management Studio or BIDS. In order to create a new role, simply right click on Roles and Select New Roles.



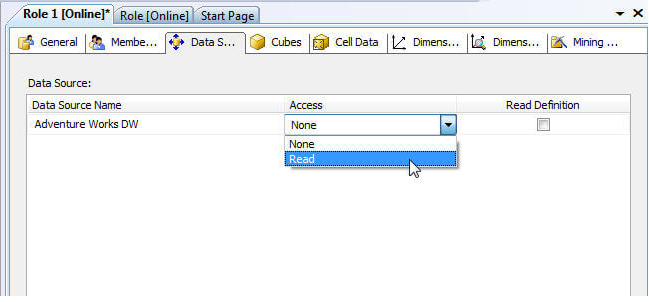
As shown on the below screen print, step 1 is to define the Role Name in the properties windows; use a name which is both descriptive and meaningful. If the properties window is not visible, select View > Properties (or hit F4). Next, fill in the Role Description as needed. As important as the name is, the three other check boxes below the role description play a vital role in defining database level access to the members of this role.  Each check box is described next:

* Full control: This permission grants full access to this particular SSAS database. Members with this permission have similar access rights as the server role noted above. However, these permissions apply to this database only, and not to all the databases within the SSAS instance. Full control grants members access to add other users and to process and maintain databases, cubes, and dimensions.
* Process database: This permission allows a member to process this database and its related cubes and dimensions.
* Read definitions: This permission allows role members to read the database metadata. Granting this access, though, does not provide access to read the metadata of other objects within the database such as cube meta data or dimension metadata. This lower level meta data access will be discussed later in the article.

Often, none of these check boxes are checked for regular users of the cube.Switching to the members tab allows the administrator to add specific users to the role. Membership can be added either by typing the individual users or by using the windows Advanced > Find option. Again, you can add active directory groups, local windows groups, domain users, or local users; however, SQL users cannot be used! The Add members processes is illustrated in the following screen print. Of course for manageability, using groups is recommended.



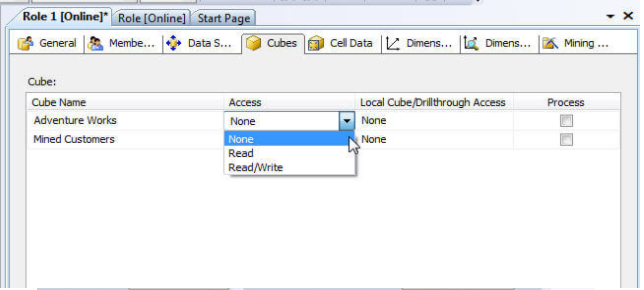
Moving on to the Data Source tab, intuitively, it would seem that a user would need access to the data source. However, granting access to the data source actually grants permissions to the underlying data sources of the SSAS project or database. Generally, this option should be set to None, unless users are utilizing data mining structures or links to external datasets.

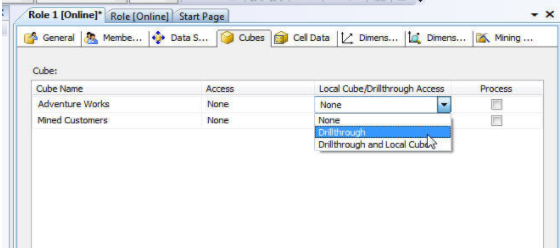


Switching to the Cubes tab finally provides methods which will grant read data access to role members. If a SSAS database has multiple cubes, access is given on a cube by cube basis and is broken into the following three categories as described below and illustrated subsequently:

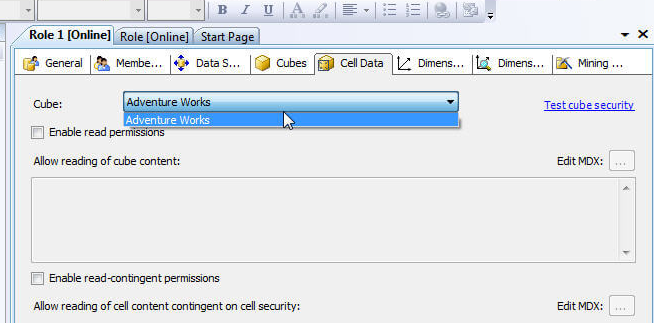
* Access
  + None: Role members are not able to access this particular cube
  + Read: Users can read data from the cube, but not write data back to the cube. This option is most commonly selected
  + Read/Write: Users can read data from cube and write data back to the cube
* Local Cube/Drillthrough Access
  + None: No Drillthough or local cube creation
  + Drill through: Drillthrough is permitted for this cube (see Cube > Actions tab)
  + Drill through and Local Cube: Drillthrough is permitted as is the creation of local cubes from the Server cube.
* Process:
  + Role members are able to process this particular cube.

Remember, if access is not specifically granted to the cube, end users will not even see the cube from their client applications.

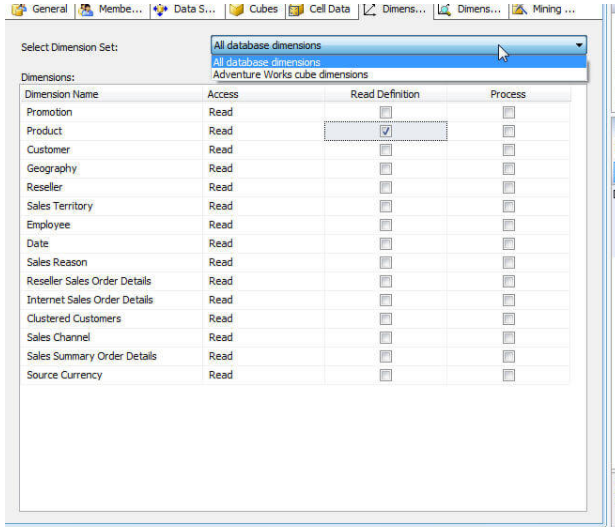


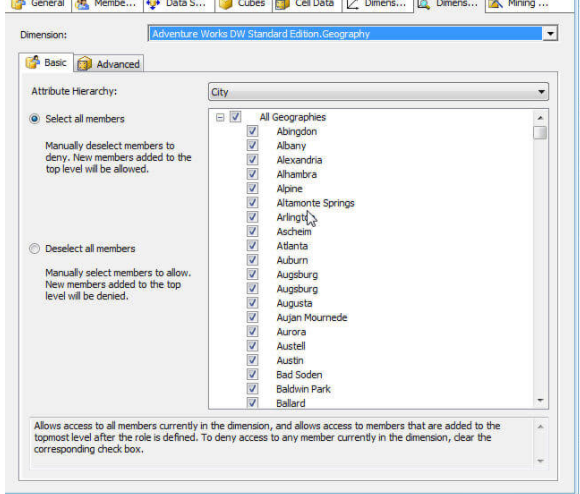


The Cell Data tab affords administrators the ability to granularly set read, read-contingent, and read/write permissions to role members. Once any of these options are enabled by selecting the appropriate check box, the administrator must enter a MDX expression which defines the cells which are available or restricted for the role members. Although, Cell Data permission restrict access to certain cells or cell ranges, these restrictions work hand and hand with the dimension permissions which will be subsequently discussed. Additionally, if certain cells are restricted, but other non-restricted calculated cells are derived from that restricted values, users may be able to make a determination of a particular value.

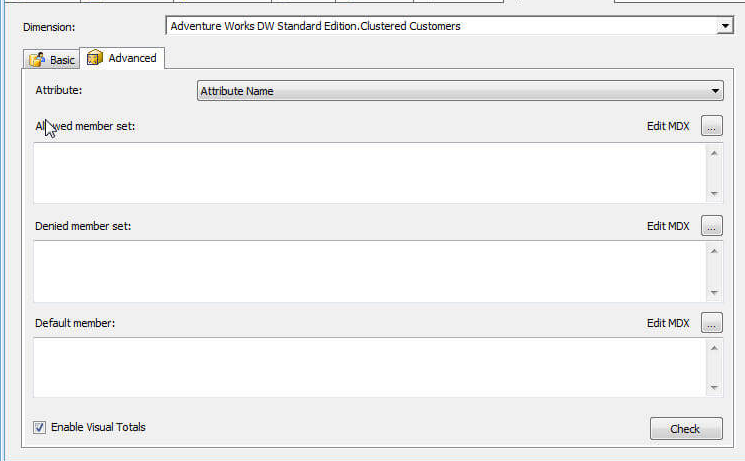


The Dimension tab assigns privileges to role members at the dimension level. First, two options exists at the dimensions level, either Read or Read and Write. Roles whose access is set to none will not even see the dimension marked as such. Furthermore, roles can be granted Read Definition access which allows for the role members to read the metadata concerning the dimension. Similar to the Cubes Access Rights, granting Process rights to a role, allows the members to process that particular dimension. The next tab to the right of the dimension tab is the Dimensions data tab; moving from dimension security at the dimension level, the dimension data tab allows the administrator to restrict or deny access to certain attribute values. For example, if a sales group only should have access to sales data in their state geographic territory, then a role could be designed to only allow access the sales person's assigned states. As seen in the next illustration, two options for entering the dimension restrictions: the basic option which allows the selection of specific values to display or restrict. The advanced option relies on the entry of MDX queries for generating the list of available or restrict access points.





One caveat in the use of Dimension Data security; total rows will display the total for all values in the dimension even those that restricted which in turn could allow end users to determine the value of the restricted attributes. To have the end client reporting tools only rollup the unrestricted values, check the enable Visual Totals check box, displayed at the bottom of the following illustration, which will then only rollup the unrestricted values. Please note, this feature can cause slower performance.



### Conclusion-Security

Implementing SSAS Security is as important as every other methods of restricting organizational data.  AS a DBA/ DWA, we are ultimately responsible for providing not only the correct and appropriate data (all very quickly), but we also must provide such data using a method and path which appropriately protects access to a SSAS database with such data. Therefore, SSAS allows us to setup the following security points:

* who administers the database
* who processes the databases, cubes, and dimensions
* who can access the meta data about the cubes and dimensions
* who can read data from the SSAS database
  + including drill through
  + dimension level and dimension data security

# References:

<https://www.mssqltips.com/sqlservertip/2776/configuring-permissions-for-sql-server-analysis-services/>