Implementing element or cube based security for IBM Cognos TM1.

View more content in this series

Introduction

Purpose of document
This document will describe tips and techniques on how to setup element and/or cube based security for IBM Cognos TM1.

Applicability
IBM Cognos TM1 10.2 and IBM Cognos 10.2.2.

Exclusions and exceptions
There are no known exceptions and exclusions at the time this document is created.

Assumptions
The document tailors to IBM Cognos TM1 Systems Administrators and IBM Cognos TM1 Model Builders. The techniques stressed in this document are based on advanced knowledge of IBM Cognos TM1 as such may not be suitable for general IBM Cognos TM1 end-users.

IBM Cognos TM1 Security Overview

TM1 object level security
Users can assign object-level security for any non-administrative user group in IBM Cognos TM1. That means users cannot assign security rights for the ADMIN, DataAdmin or SecurityAdmin.
groups. The rights for these groups are predefined and appear disabled in the IBM Cognos TM1 Security Assignments dialog box. The object-level security rights for IBM Cognos TM1 groups are:

- **Admin**: Group has complete access to a cube, element, dimension, or other object.
- **Lock**: Group can view and edit a cube, element, dimension, or other object and can permanently lock objects to prevent other users from updating them.
- **Read**: Group can view a cube, element, dimension, process, or chore, but cannot perform operations on the object.
- **Reserve**: Group can view and edit a cube, element, dimension, or other object, and can temporarily reserve objects to prevent other users from updating them.
- **Write**: Group can view and update a cube, element, dimension, process, or chore.
- **None**: Group cannot see a cube, element, dimension, process, or chore, and cannot perform operations on the object.

As a refresher on what members of the security groups are allowed, users that belong to the ADMIN group have full Administrator rights on the IBM Cognos TM1 instance, users that belong to the DataAdmin group have full data-related administrative rights on the IBM Cognos TM1 instance but cannot make security related changes and users that belong to the SecurityAdmin group have Security Admin rights on the IBM Cognos TM1 Instance but cannot view any non-security related data in the instance. Security Admins also cannot change their own security credentials to include non-Security data.

When a user is assigned **Admin** rights, the following applies:

- **Cube**: Members of the group can read, write, reserve, lock, and delete the cube. They can save public cube views. They can also grant security rights to other users for this object.
- **Element**: Members of the group can access, update, reserve, lock, and delete the element. They can also grant security rights to other users for this object.
- **Dimension**: Members of the group can add, remove, and re-order elements in the dimension, and can reserve or lock the dimension. They can save public dimension subsets. They can also grant security rights to other users for this object.
- **Application**: Members of the group can see the application, use references within the application, and create both public and private references in the application. When a group has Admin privilege to an application, members of the group can set security privileges for all references and sub-applications within the application for other groups but not their own group.
- **Reference**: Members of the group can use the reference, as well as update or delete the reference. They can publish private references, and privatize public references.

When a user is assigned **Reserve** rights, the following applies. Note that a reservation expires automatically when the reserving user disconnects from the remote server or when the server shuts down.

- **Cube**: Members of the group have all privileges implied by Write permission, and can also reserve the cube to prevent other users from applying edits. The reservation can be removed either by the user who reserved the cube or by users who have Admin rights for the cube.
• **Element**: Members of the group have all privileges implied by Write permission, and can also reserve the element to prevent other users from updating cube cells identified by the element. The reservation can be removed either by the user who reserved the element or by users who have Admin rights for the element.

• **Dimension**: Members of the group have all privileges implied by Write permission, and can also reserve the dimension to prevent other users from redefining the dimension. The reservation can be removed either by the user who reserved the dimension or by users who have Admin rights for the dimension.

When a user is assigned **No** rights, the following applies:

• **Cube**: Members of the group cannot see the cube in the Server Explorer, and thus cannot browse the cube.

• **Cell**: Members of the group cannot see data for the cell.

• **Element**: Members of the group cannot see the element in the Subset Editor or Dimension Editor, and cannot see the cells identified by the element when browsing a cube.

• **Dimension**: Members of the group cannot see the dimension in the Server Explorer, and cannot browse a cube that contains the dimension.

• **Process**: Members of the group cannot see the process in the Server Explorer, and thus cannot execute the process. Privileges assigned to processes are ignored when a process is executed from within a chore.

• **Application**: Members of the group cannot see the application or its contents in the Server Explorer.

• **Chore**: Members of the group cannot see the chore in the Server Explorer, and thus cannot execute the chore.

• **Reference**: Members of the group cannot see the reference in the Server Explorer.

### IBM Cognos TM1 object level security options

In IBM Cognos TM1 there are options to apply security at the object, element and cell level. The following provides guidelines on security set up at the object, element and cell levels:

• **Object Security Cubes**: `{ObjectType}Security.cub

• **Element Security Cubes**: `{ElementSecurity_<DimensionName>.cub

• **Cell Security Cubes**: `{CellSecurity_<CubeName>.cub

### Interaction of different security rights

Rollup values remain unchanged by security - the value of a non-leaf member does not change if some or all of its descendants are inaccessible.

As mentioned above, if a user belongs to more than one group, user access credentials are determined by the intersection of the different group access credentials. If user is granted Read access to an element or cell via one group but Write access via another group, the user will be granted Write access. If user is not granted access to an element or cell via one group but Read access via another group, the user will be granted Read access.
Cube access credentials overrule cell security credentials in that cell security may not be less restrictive than cube security. If a user is granted Read access to a cube, Write access cannot be granted via cell security. Cell level security may be more restrictive than the corresponding cube access credentials.

Dimension and Element Access credentials may be overruled by cell security credentials in that cell security may be less restrictive than cube security. If a user is granted Read access to an element via element security or just via dimension security (no element security in place) but Write access to corresponding intersections in a cube via cell level security, then Write access is granted for this specific cube in accordance with the cell security configuration. Such a configuration is of particular use if for one and the same user group, Write access to an element is only to be granted in some cases (in some cubes) or if in certain cases the Write access is to be overruled with Read access only. Cell level security is typically driven by IBM Cognos TM1 Cube Rules that are applied in the cell security cube.

It is very important to be aware that while one might not be able to see an element, cell level security can be wrongfully configured such that access to the data elements is granted regardless. If cell level security grants Read access to an intersection BUT the corresponding element access is not granted (element security value of NONE or empty means no access), running a Perspectives query via DBRW formula and hard-coding the element into the DBRW formula will retrieve the desired value from the cube.

**Sample scenarios for object security configuration and interaction**

**Scenario 1**

Assign a user Read access to the P&L cube and Write access to the dimensions/elements used in the cube. In this scenario, the Read access of the P&L cube overrides the Write access of the elements. The user can view P&L cube data but cannot update the P&L cube data.

**Scenario 2**

The P&L What If Analysis cube contains the following dimensions - Account, Company, Cost Center, Geography, Version, Time Period and Currency. Suppose a user has Write access to the P&L What If Analysis cube, Read access to all of the elements in the Currency dimension, and Write access to all of the elements in the other dimensions. The elements in the Currency dimension identify every cell in the cube, and therefore – in the absence of cell security rules that could overrule the Read access restriction - the user cannot update any cube data.

**Scenario 3**

A user has Read access to all elements underneath Org hierarchy node A in dimension Cost Center/Org, Read access to Company 1 in dimension Company and Read access to Geography Ohio in dimension Geography. The P&L cube contains all the aforementioned dimensions. It follows that the user will only get access to intersections associated with Company 1 and Geography Ohio and Org node A. If Org node A contains data elements that are not associated with Company 1 and Geography Ohio, the user will not have access to the data.
Scenario 4

Several regional groups of users to read all data in the P&L What If Analysis cube. You also want each group to update data for their own Business Units (BU) and Product Ids (PID). To implement this security scheme, you could:

- Create groups that reflect Contributors by BU and PID, such as BU Contributors and PID Contributors, with Write access to the corresponding Customers and Products ElementSecurity.
- Grant each group Read access to the other BUs and PIDs, as these should be the ones that they should only be able to read, or create groups called All BUs READ and All PIDs READ that have Read access to all corresponding element security. Grant each group Write access to the P&L What If Analysis cube or create a separate group called P&L What If Analysis Contributor.
- Add users to the appropriate groups. Each user will get groups BU Contributor, P&L What If Analysis Contributor, All PIDs READ and All BUs READ.

Scenario 5

A user has access to customers from the San Francisco and the Oakland region, but not to Los Angeles. You want the user to be able to roll up data for San Francisco and Oakland. Your hierarchy contains a level called CA with children SF, Oakland and LA. It follows that if you give the user access to element CA, the user will be able to retrieve the Total CA number, which will include LA. TM1 hierarchy levels will always display the full value according to the hierarchical rollup - a consolidation is generally determined exclusively by the value of the immediate children/ descendants of the parent and the element weight of the children. The value of a non-leaf element does not change if a user does not have access to some or all of its descendants.

Do not give the user access to node CA. Instead, have the user create a custom, user based private hierarchy rollup for San Francisco and Oakland or create an additional rollup in the hierarchy for the SF and Oakland region.

Maintaining security metadata in TM1 security objects


If Turbo Integrator is used, a security metadata change – due to, for example, a hierarchy change with corresponding/resulting security changes for parent and/or child nodes or a new element being added to a hierarchy such as a new archived version for which Read access is now to be granted to all applicable groups – will always require running the SecurityRefresh() command in IBM Cognos TM1, effectively rendering all cached security settings invalid and hence renewing/refreshing all security credentials. A security refresh on large models will typically lead to a multi to many minute lock of all user activity due to IBM Cognos TM1 refreshing security access credentials for all active users and groups. If security is manually entered or processed via Turbo Integrator (and therefore directly stored in the corresponding security cube), a security refresh is
not necessary for such security changes. The security changes will propagate automatically and with only very short locks.

Securing cell-level data

Cell level security rules

IBM Cognos TM1 cell level security is applied individually per cube via the content of a cube-specific cell level security cube with values such as Read, Write and None for the security groups and cube cell intersections and subsections that are to be secured accordingly. The data content is typically also determined via rules in the cell security cube rather than written to the cell security cube using a Turbo Integrator (TI) process. Cell security cube rules are re-evaluated automatically once a user refreshes a query. This is contrary to cube, dimension and element security as a SecurityRefresh() is not required to refresh credentials established by cell security rules.

The reason for not using a TI process is the corresponding data volume would be very high if one were to process cell level security via TI. Also, because all or, at a minimum, a very large number of cells would have to be processed, the TI process would suffer from a very long runtime. More importantly, a security change at the element security level (which typically warrants corresponding changes at the cell security level) would require re-processing of the cell security credentials in each applicable cube, causing long processing times and corresponding user locks after only minor security changes.

When to apply cell security

If the security requirements can be just as easily be met using cube, dimension and element security only, then cell level security should be avoided. Particularly with very large cubes, cell level security can impose a query performance overhead depending on cell security requirements and cube size. With the release of IBM Cognos TM1 10.2 however, cell security performance has greatly improved due to the ability to customize a cell security cube such that it only contains the dimensions that are used in determining cell level security thereby allowing for significantly faster retrieval of cell security metadata. Prior to IBM Cognos TM1 10.2, cell level security cubes contained the same number of dimensions as the target cube plus the }Groups dimension. As a result, a comprehensive cell level security schema against very large cubes could have a significant effect on performance by slowing down queries due to the large cell level security metadata having to be evaluated. As of IBM Cognos TM1 10.2, cell level security can be defined against a subset – as in a select number of dimensions - of the target cube, potentially resulting in significantly faster cell level security processing time.

In a scenario where, for example, the cost center dimension is used to primarily define security, cell security rules would need to be implemented on only a small subset of each cube(s) dimensions. Read-only cubes will only need to be secured against their respective cost center dimension, meaning the Cell Security cube for Read-only cubes will only have two dimensions - <CostCenterDimension>.dim and }Groups.dim. Write-back cubes for what-if analysis need only to be secured against Cost Center, Time Period and Version resulting in a cell security
cube with four dimensions - <CostCenterDimension>.dim, <TimePeriodDimension>.dim, <VersionDimension>.dim and }Groups.dim.

**New feature for IBM Cognos TM1 10.2.2 – Enforce security on approval hierarchies**

In IBM Cognos TM1 version 10.2.2, users can use the **Enforce Element Security on Approval Hierarchies** parameter to turn element security on for approval hierarchies. This parameter is a property of all the **Approval** or **Responsibility** applications for a given TM1 server. For additional documentation on security, see the section titled *The interaction rights and access control in TM1 Applications* in the **TM1 Applications Guide 10.2.2**.
Resources

- IBM Cognos TM1 Web Security Configuration
- IBM Cognos TM1 Element Security Application for IBM Cognos TM1 10.2