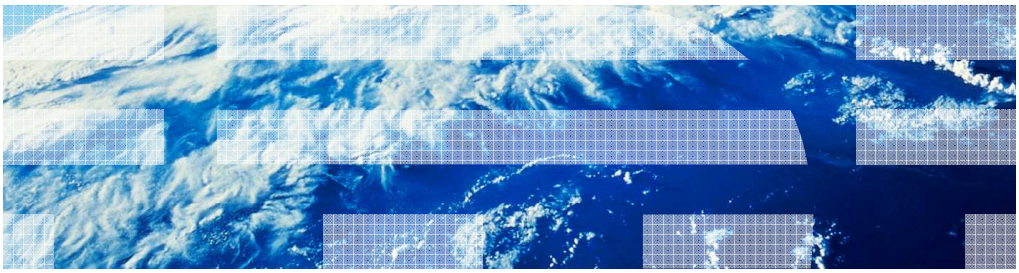
IBM Business Monitor

Fine Grained Security



WebSphere software

This presentation should give you an understanding of the use of fine grained security in IBM Business Monitor.

Goals

- Introduce fine grained security in IBM Business Monitor

This presentation will give you an understanding of fine grained security for filtering the display of monitored data in the dashboards.

Agenda

- Overview
- Security filters
- Object filters
- Examples
- Cube publishing

This is the agenda for this presentation. You will see a description of the purpose and usage of fine grained security, including the use of security filters and object filters. There are several slides that show some examples of the XML strings that configure the filters. You will review the commands that are used to control the security settings. Finally you will see how to publish the fine grained security to Cognos to see filtering in the reports.

Overview

- As an administrator, you can limit which monitoring context instance data each user or group has the authority to view
  - For example, users in group ‘Managers of Southwest’ are authorized to see only instances where metric Region is ‘Southwest’
- As an administrator, you can limit which metrics each user or group has the authority to view
  - For example, the administrator indicates that users in group “Worker” are not authorized to Loan Amount
- Fine grained security is configured once, but applied globally across widgets and Representational State Transfer (REST) services
- Secure data based on users, groups, Lightweight Directory Access Protocol (LDAP) user attributes, external entitlement system
- Use command line to import, export, delete
- Indicators on widgets to show that results are filtered
- Information center > Securing your environment > Configuring fine-grained security

Fine grained security allows you to restrict the display of monitoring context instances, for example showing only instances for a particular geograpical region. Also, you can restrict which metrics are displayed to a user, for example only showing loan amounts to authorized users.

Fine grained security is applied to all Monitor widgets and to any applications that are using Monitor REST services.

You can secure your data based on specific users or groups in the user registry. You can also apply security based on attributes assigned to the user in the LDAP user registry. You can also make use of an external entitlement system to determine which users are authorized.

For this release, only the command line is supported. You can import security rules, export rules and delete rules.

When displaying data with fine grain security applied, you will see an indicator on the widget that shows that the filters are active.

Security filters

- As a system administrator, you want to limit which monitoring context instance data each user or group has the authority to view
- For example considering these five instances, specify a condition such as:
  - Users in group 'Managers of Southwest' are authorized to see only Southwest loans (where metric Region = 'Southwest')
- This results in access only to the two highlighted rows

Loan Number	Date and Time of Loan Application	Loan Amount	Region	Loan Officer	Loan Status
10061	6/15/2010 10:0	$115 000 0	Northeas	Gerald Mande	Processor Validator an Underwritin
10061	6/16/2010 11:0	$275,000.0	Southwes	Robert Gum	Shippin
10070	7/7/2010 8:0	$500,000.0	Southwes	Gerald Mande	Shippin
10062	6/22/2010 14:0	$400,000.0	Centra	Gerald Mande	Processor Validator an Underwritin
10070	7/2/2010 8:0	$120,000.0	Northeas	Joan Smit	Post-Closin

You can apply security filters which affect the display of monitoring context instances. In this example the managers of the southwest region are allowed visibility to only loans that are assigned to the southwest region. Even though there are five instances in the database, only two of them are displayed to the southwest managers.

Object filters

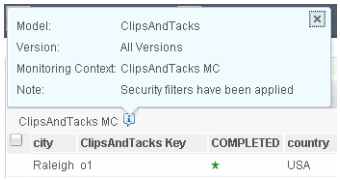
- As an administrator, you want to limit which metrics each user or group has the authority to view
- For example, the administrator indicates that users in group “Worker” are not authorized to Loan Amount

Loan Number	Date and Time of Loan Application	Loan Amount	Region	Loan Officer	Loan Status
10061	6/15/2010 10:0	$115,000.0	Northeas	Gerald Mande	Processor Validator an Underwritin
10061	6/16/2010 11:0	$275,000.0	Southwes	Robert Gum	Shippin
10070	7/7/2010 8:0	$500,000.0	Southwes	Gerald Mande	Shippin
10062	6/22/2010 14:0	$400,000.0	Centra	Gerald Mande	Processor Validator an Underwritin
10070	7/2/2010 8:0	$120,000.0	Northeas	Joan Smit	Post-Closin

You can apply object filters which affect the display of metric data. In this example the users in the worker group are restricted from seeing the metric for loan amount. After the filter is applied the worker sees the other five metrics in the dashboard but the loan amount is hidden from view.

Indicators

- Indicators on widgets to show that results are filtered
- Indicator usage is configured in the security filter definition
  - DisplayIndication parameter
- There is no indication for object security
- KPI target and ranges are suppressed



There are indicators on the widgets in the dashboard to show that the results are filtered. On the right you can see an icon on the instances and KPI's widgets that pops up more information about the filtering. If you prefer not to show the indicators, then you can set the parameter called DisplayIndication in the security filter definition. The indicators only apply to security filters not to object filters. For object filters, the metrics are hidden without an indication of the filtering.

For filtering in the KPI widget, the KPI target and ranges are not displayed. Since the aggregated values in the KPI are changed based on the filtering, the targets and ranges do not relate to the new aggregates.

Note that if you are the owner of a KPI or have 'KPI administrator' role, you are allowed to see KPI target/ranges, even if the KPI is filtered for you. Also, you are able to access and manage the KPI, even if object security is applied to the KPI. This also applies to KPI history and prediction and alerts.

Security filters example

- Security filters apply to instances, KPI's, KPI history/prediction, reports
- Static – fixed string
  - Loan_Officer = 'Joan Smith'
- Dynamic – logged in user
  - Loan_Officer equals $account.parameters.userID

```
{"SecurityFilterArray":[
{
      "ModelID":"ClipsAndTacks",
      "MCID":"ClipsAndTacks_MC",
      "User":"tw_admin",
      "FilterSet":{
            "FilterOperator":"AND",
            "FilterArray":[{
                  "FilterMetricID":"city",
                  "FilterOperator":"equals",
                  "FilterValue":"Raleigh",
                  "FilterOperatorCaseSensitive":false
                  }
            ]
      }
}]}
```


Security filters affect the display of monitoring information in the dashboard. They apply to the widgets for instances, KPI's, KPI history/prediction and reports. Use a text editor to create an XML file that contains the appropriate parameters for the filter that you are creating. You can specify the user as a fixed string or dynamically using the logged in user ID. In the example you see the parameters for the model ID, monitoring context ID, user and the filter set. The filter set will display only instances where the city metric has a value of "Raleigh". You can also apply a security filter to a user group rather than a specific list of users using the group parameter.

Object filters example

- Object filters apply to instance metrics, KPI's, alert templates, dimensions, measures, diagrams
- Diagrams
  - Metrics are hidden in instance diagrams, and KPIs are hidden in KPI diagrams
- Alerts - Security applied to source KPI triggering the alert
  - Dynamic public alerts – Security is evaluated based on alert owner not subscriber
  - Dynamic private alerts – Based on alert owner
  - Modeled alerts – Not supported
- Specify HiddenFrom and VisibleTo

```
{
    "ObjectSecurityArray": [
        {
            "ModelID": "ClipsAndTacks",
            "MetricRules": [
                {
                    "MCID": "ClipsAndTacks_MC",
                    "MCMetricRules": [
                        {
                            "MetricIDs": [
                              "country"
                            ],
                            "HiddenFrom": {
                              "Users":["tw_admin"]
                            }
                        }
                    ]
```

9 Monitor model versions

Object filters affect the display of monitoring information for instances, KPI's, alert templates, reports and diagrams. For diagrams, filtered metrics are hidden in instances diagrams. For KPI diagrams, KPI's are hidden that are based on the filtered metric.

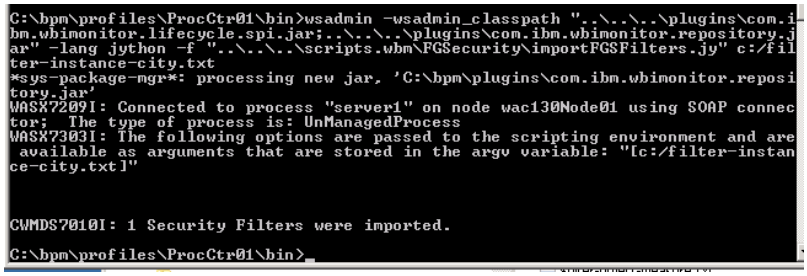
For alerts, object security can be applied to the KPI triggering the alert condition. Note that the security for dynamic alerts is applied based on the alert owner not the alert subscriber. For alerts defined in the model, object filters are not supported. To circumvent this, re-create the alerts in the dashboard using the alert manager, and then you can apply the filter.

Depending on your needs you can either set the HiddenFrom parameter or the VisibleTo filter or both.

In this example, an object filter hides the metric country from a user. You can just as easily apply the filter to a group of users rather than an individual list of users by using the group parameter.

Command

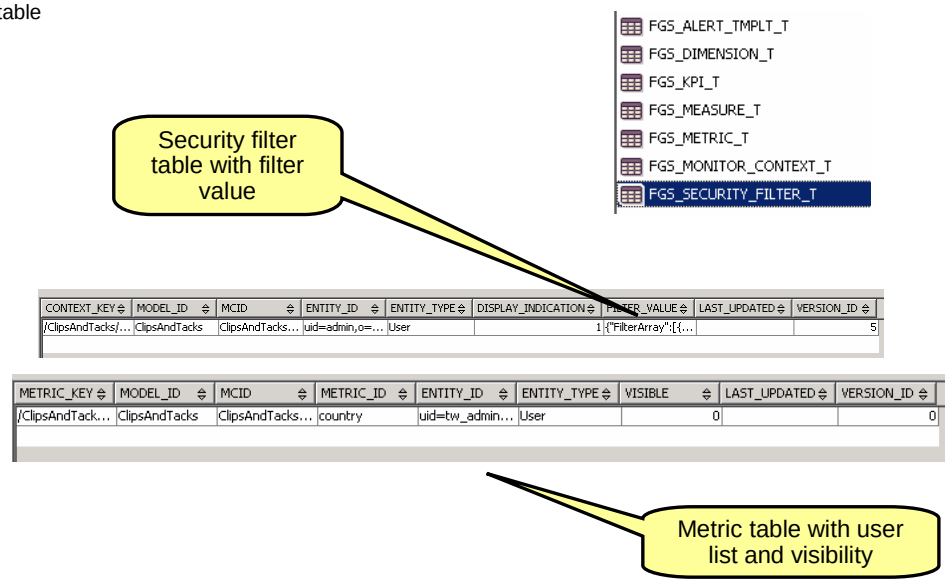
- Commands for import, export, delete
  - importFGSFilters, importFGSObjSecRules, deleteFGSFilters, deleteFGSObjSecRules, exportFGSFilters, exportFGSObjSecRules
- Example command
  - wsadmin -wsadmin_classpath "..\..\..\plugins\com.ibm.wbimonitor.lifecycle.spi.jar;..\..\..\plugins\com.ibm.wbimonitor.repository.jar" -lang jython -f "..\..\..\scripts.wbm\FGSecurity\importFGSFilters.jy" c:/filter-instance-city.txt
- For command details see the Monitor information center, topics 'Security filter file' and 'Object security rules file'



There are several commands that control importing, exporting, and deleting security and object filters. In the example, the command shows how to import a security filter. One of the parameters for the command is the file containing the security filter string. To see all the parameters for the commands and the filters, there are topics describing them in the Monitor information center.

Filter tables

- Tables fgs_* - one for each object type, also security filter table

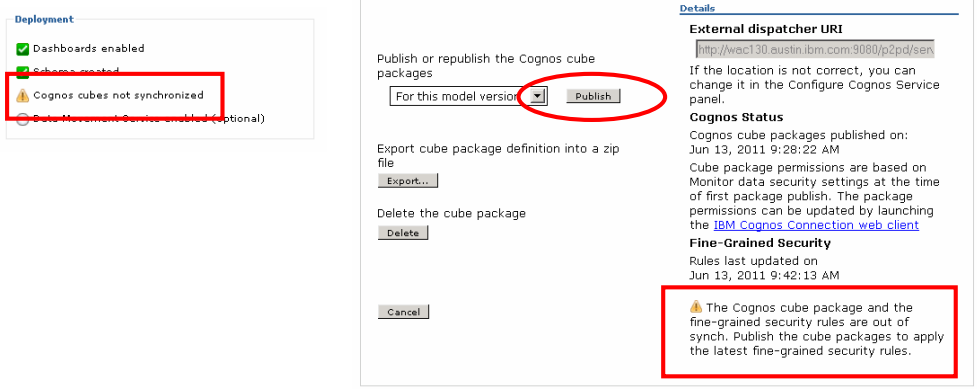


11 Monitor model versions

After importing several filters over time, you might be interested in determining all the filters that have been applied. You can see them in the database in the tables for fine grained security which have a prefix of ‘fgs_’. There is a single table for security filters with one row for each applied filter. For object filters there are separate tables for each object type. So you see tables for alert templates, dimensions, KPI’s, measures, metrics and monitoring contexts.

Publish cubes

- Manage Cognos cubes
- Indicators in the console to republish



12 Monitor model versions

When you run the commands to apply security filters, the Cognos cubes are not automatically updated. This means that the data shown in the reports widgets will not have the latest security filter updates. So you should remember to publish the Cognos cubes after you have made any changes to the security filters. In the administrative console you can find the page to manage the Cognos cubes for a model version. There are also convenient indicators to remind you that you should republish the cubes.

Summary

- Covered fine grained security in IBM Business Monitor

In summary, this presentation covered the use of fine grained security in IBM Business Monitor.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WBPM_Monitor_Model_Versions.ppt

This module is also available in PDF format at: ../WBPM_Monitor_Model_Versions.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information