SAP GRC Access Control: Background jobs for risk analysis and remediation (formerly Virsa Compliance Calibrator)

Applies to:

SAP GRC Access Control, version 5.2

Summary

This document discusses the background jobs available in the context of using risk analysis and remediation in SAP GRC Access Control. Best practices on executing these jobs are given, e.g. the order in which background jobs should be executed, the difference between *full synch mode* and *incremental mode*.

Authors: Subrat Singh, Sirish Gullapali

Company: SAP

Created on: 13 July 2007

Author Bio

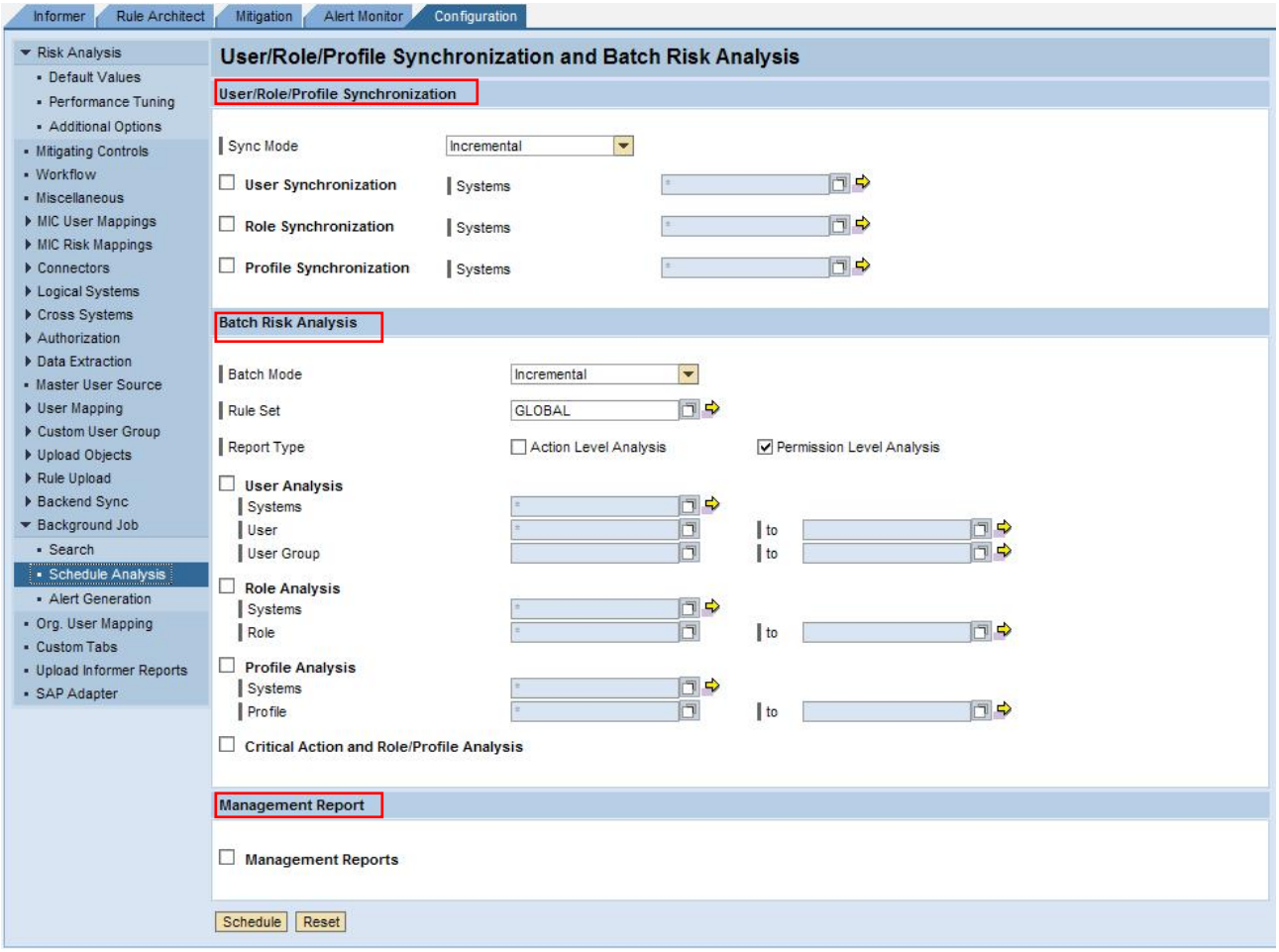
Subrat Singh is a Principal Consultant at Regional Implementation Group (RIG) SAP GRC. He is an expert in GRC Access Controls and was instrumental in many successful Access Control Ramp-up implementations. Prior to joining RIG he was part of the Access Control development team.

Sirish Gullapali is a Senior Consultant at RIG SAP GRC. He has gained extensive experience supporting SAP's customers in the implementation of SAP GRC Access Control.

Table of Contents

SAP GRC Access Control Background Jobs in risk analysis and remediation (formerly Virsa Compliance Calibrator)

One of the main tasks performed in risk analysis and remediation is running an organization-wide SOD risk analysis in regular intervals thus updating management reports to present the analysis results in a graphical and easy to read format. The system provides the facility to schedule background jobs for these activities. To navigate to the background job scheduler page, follow the path Configuration -> Background job -> Schedule Analysis.



This document looks at the capabilities of background jobs and outlines best practices around scheduling and running these background jobs. Following are the main topics discussed:

- Types of background jobs
- Modes of background jobs
- Order of executing background jobs
- Monitoring background jobs
- Ad hoc background jobs

Types of background jobs

Three different types of background jobs can be scheduled from the background job scheduler page.

- User/Role/Profile Synchronization
- Batch Risk Analysis
- Management Report

User/Role/Profile Synchronization background job pulls the users data (user ids and user names only), role and profile data (technical role/profile names only) from the selected backend systems and stores them. This is the first section in the background job scheduler page.

Batch Risk Analysis job performs SOD risk analysis on the users/roles/profiles stored with the system. During the execution of batch risk analysis for users, the application selects one user from the database, fetches the actions/authorizations of the user from the backend system and performs risk analysis using the rules stored in Access Control. The resulting SOD violations are stored. Access Control then selects the next user and performs the steps above for the new user. The batch risk analysis job for roles and profiles also follow similar steps.

Management Report job uses the results of batch risk analysis job to abstract the high level data to be presented in graphical formats in the informer tab. From the analysis results, the total no of violations, the distribution of violations with respect to business process and with respect to High, Medium and Low types of risks are calculated and stored during the execution of the management report job. One set of management report data is maintained in the application for each month. Every time a management report is run, the management report data is overwritten for the current month.

Modes of background jobs

Background jobs can be run in following two different modes.

- Incremental
- Full Synch

Incremental – When background job is run in Incremental mode, the application takes into account only those users/roles/profiles which are modified since the last background job run. For example; when a user synch job is run in the incremental mode, only the users added or modified in the selected backend ABAP system are pulled. Similarly when batch risk analysis job is run in incremental mode, SOD risk analysis job is performed for only those users who have been added or modified since last user analysis job was run.

Full Sync – When background job is run in a Full Sync mode, it takes into account all the users present in the system. For example, when the user synchronization job is run in Full Synch mode, data for all the users in the selected backend system is pulled into Access Control. Similarly when a batch risk analysis job is run in the full synch mode, SOD risk analysis is done for all the users present in Access Control regardless of whether any changes have happened to a user since the last run.

One important point to note about the Full synch mode is that when the background jobs are scheduled for the very first time, they need to be run in the full synch mode. Once the background jobs in full synch mode completes, incremental jobs can be scheduled to run in an ongoing basis to synchronize the Access Control database with changes made to Users/ Roles/Profiles in the backend and update risks incurred by the changes.

Order of executing background jobs

As discussed earlier there are three different types of background jobs namely: User/Role/Profile synch, Batch risk analysis and Management reports. For each of these job types, independent jobs can be scheduled from the background job scheduler page for users or roles or profiles. All these separate jobs

can also be scheduled to run together as one job. In this section it is described when to schedule individual jobs separately and when to schedule them together as one single job.

As one can imagine, there is a sequence in which the background jobs should be run for correct result. The following should be the order of execution:

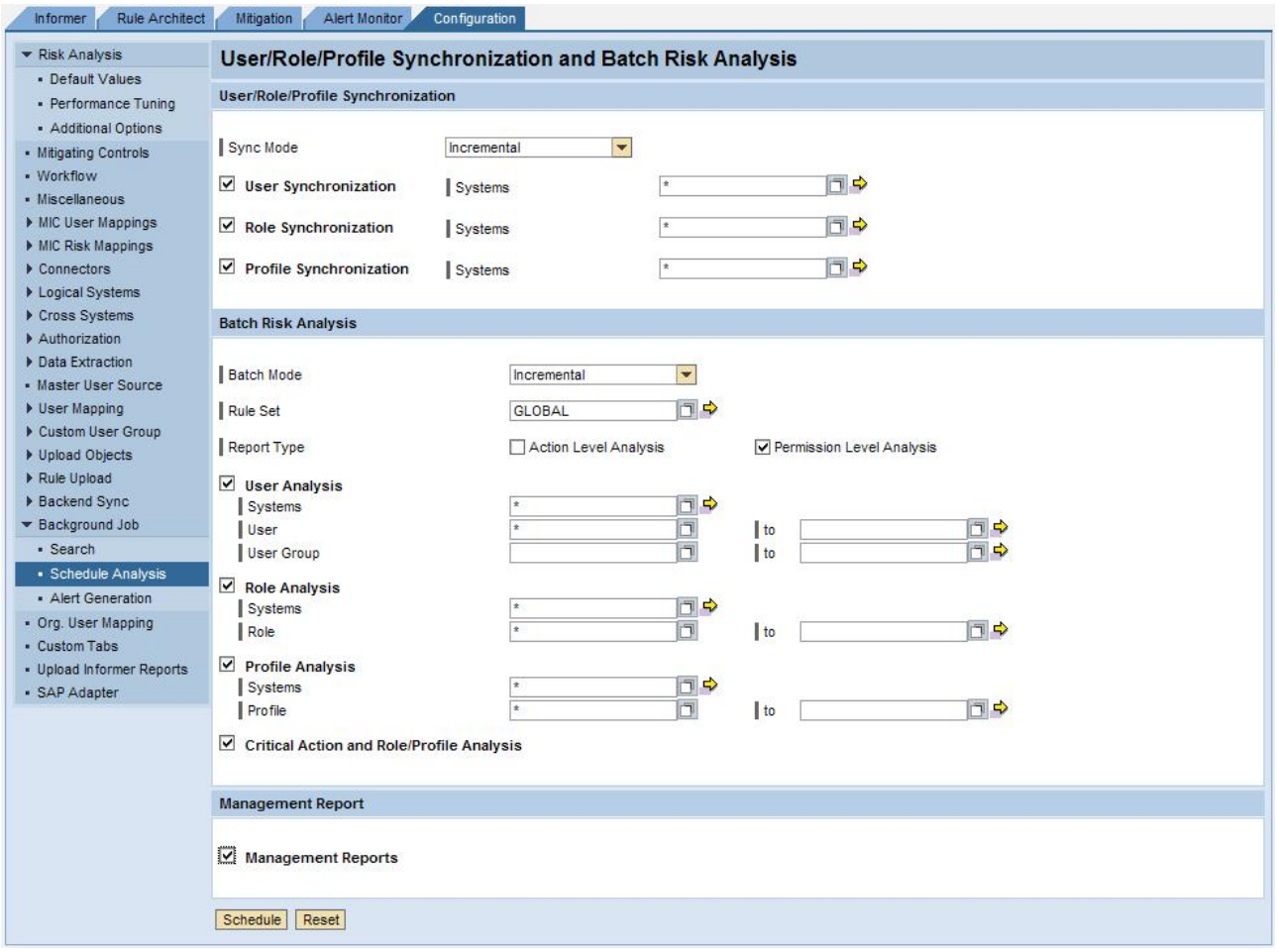
First: user/role/profile synchronization

Second: Batch Risk Analysis

Third: Management report

The user/role/profile synch job should be completed first before the batch risk analysis job can be started so that the risk analysis would occur on the most current data for users or roles or profiles. Management report should be run only after batch risk analysis job is completed successfully so that management report is based on the most current risk analysis result.

To ensure background jobs run in this sequence, all the jobs should be scheduled in one single job as depicted in the figure below. Access Control will start executing the individual tasks in the appropriate order. However it is recommended to schedule only the incremental jobs in this manner.

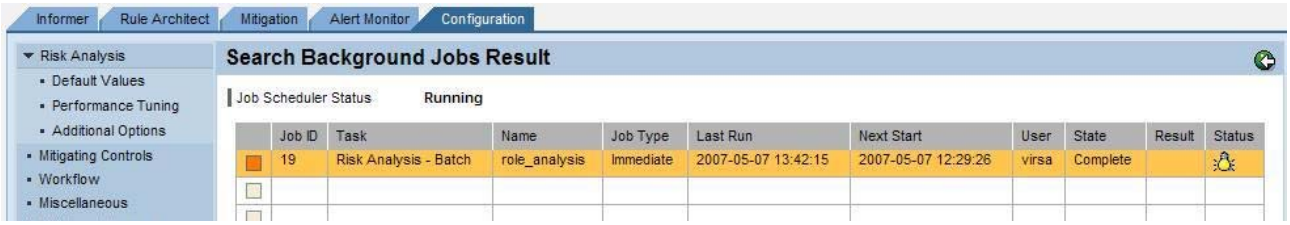


The full synch analysis jobs are not advisable to run in this fashion. This is because full synch jobs can be very heavy and time consuming jobs which might require manual monitoring to make sure that background jobs are progressing properly. The Full synch jobs can take hours to days to run depending upon the no of users/roles/profiles, the average no of authorizations and the no of SOD violations. Hence it is recommended that full synch jobs should be run separately in the sequence as mentioned above. The Batch Risk Analysis jobs are the most time consuming ones and it is better to monitor these jobs

during its execution. The following section describes how to monitor Access Control background jobs for risk analysis and remediation (formerly Virsa Compliance Calibrator).

Monitoring background jobs

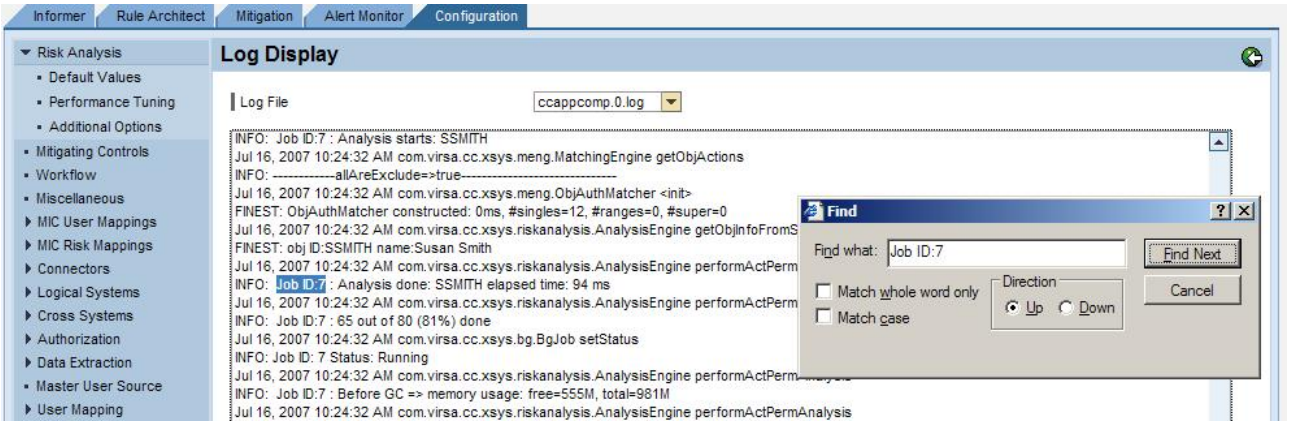
It is recommended to monitor Background Jobs that are taking long time or jobs that are scheduled during initial data load to make sure the data is loaded properly and completely. To monitor scheduled jobs, go to Configuration tab, click on Background Job and do search for the Background job. The resulting page displays the list of searched jobs as shown below.



The state of the job provides an initial status about the job. Following are the possible states of a background job.

- Ready: The job is scheduled and in the queue ready to be picked up by the scheduler.
- Running: The job is currently being executed.
- Complete: The job is completed successfully.
- Error: There was an error while executing the job.
- Aborted: An unexpected error happened and the job was aborted.

For those jobs which run for hours, you might want to get more insight into the progress of the job. Click on View Log button in the search result screen. The view log screen appears and the log details are displayed in a text area. Click inside the text area and search for the job id. The percentage complete; total no. of objects to be analyzed; no. of objects already analyzed; name of the object currently being analyzed etc. can be viewed in the log file. In the figure below, it shows - for the job id: 7, 81% analysis is complete. 65 out of 80 objects have been analyzed. The current user being analyzed is SSMITH. Since the latest status is at the bottom of the file, to get the latest status always scroll to the bottom and search for the job id in the upward direction.



Ad hoc background jobs

Ad hoc background jobs are risk analysis jobs scheduled from the Informer tab. The results of analysis are not stored in the Access Control database. The results are stored in flat files on the server. The results of these analyses do not contribute towards updating the management reports.

Related Content

- Quick reference guide on post-installation tasks
- SAP GRC Access Control pre-implementation guide
- Quick reference guide on periodic job processing

Copyright