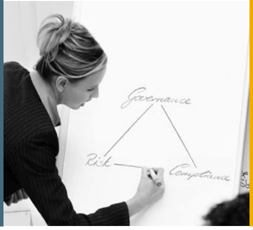
SAP SOLUTIONS FOR GOVERNANCE, RISK, AND COMPLIANCE

How-To Guide



How to Performance Optimize SAP GRC Access Control 5.3

SAP GRC Regional Implementation Group

Applicable Releases:

SAP Access Control 5.3

Version 1.1

February 2011

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

These materials are provided “as is” without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall not be liable for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials.

SAP does not warrant the accuracy or completeness of the information, text, graphics, links or other items contained within these materials. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third party web pages nor provide any warranty whatsoever relating to third party web pages.

SAP NetWeaver “How-to” Guides are intended to simplify the product implementation. While specific product features and procedures typically are explained in a practical business context, it is not implied that those features and procedures are the only approach in solving a specific business problem using SAP NetWeaver. Should you wish to receive additional information, clarification or support, please refer to SAP Consulting.

Any software coding and/or code lines / strings (“Code”) included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, except if such damages were caused by SAP intentionally or grossly negligent.

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP’s Support Services and may not be modified or altered in any way.

Document History

Document Version	Description
1.00	First official release of this guide
1.01	Wrong diagram replaced.
1.10	Limitations & Exclude Objects feature added, limitation of 5 server nodes per dispatcher removed.

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Icons

Icon	Description
⚠	Caution
💡	Note or Important
❖	Example
⬆	Recommendation or Tip

Table of Contents

1. Business Scenario

SAP GRC Access Control comes with the following four main product capabilities:

- **Risk Analysis and Remediation (RAR):** SAP GRC Access Control supports real-time compliance around the clock to detect, remove, and prevent access and authorization risk and stops security and controls violations before they occur. Using live data to assess risk, SAP GRC Access Control enables your organization to identify conflicts immediately, drill down into root causes, and achieve resolutions.
- **Superuser Access Management (SPM):** The application enables users to perform emergency activities outside their roles under a “privileged user,” but in a controlled and auditable environment.
- **Compliant User Provisioning (CUP):** As companies provision and de-provision access to enterprise systems, they often overlook how these changes can impact SoD requirements. SAP GRC Access Control can automate provisioning, test for SoD issues, streamline approvals, review and reaffirm access and reduce the workload for IT staff.
- **Enterprise Role Management (ERM):** This functionality standardizes and centralizes role creation, eliminating manual errors and making it easier to enforce best practices. The application prevents SoD violations by performing a real-time simulation of the data in a production system and testing the entire SAP software landscape.

Of these four capabilities it is in particular Risk Analysis and Remediation (RAR), which is very resource consumptive in terms of CPU and memory usage. It is clear why: It risk-analyzes the entire user population of a multitude of connected backend systems against a complex rule set identifying segregation of duty (SoD) and critical action and permission risks in a single and cross system analysis. Since this rule set is defined down to a granularity of authorization field values and is checked against every single authorization granted to very often thousands of backend users, it is easy to understand why RAR requires a considerable computational effort and why performance tuning is an important topic when operating SAP GRC Access Control.

This guide provides a structured approach to performance optimization of GRC Access Control 5.3. It starts with performance tuning on the technical platform being SAP NetWeaver Application Server Java 7.00, then focuses on performance aspects of the connectivity between the Access Control server and backend systems and finally resumes preferred practices in performance optimized setup and usage of the Access Control main product capabilities.

2. Background Information

2.1 Overview SAP NetWeaver AS Java 7.0

SAP GRC Access Control 5.3 is deployed on a SAP NetWeaver Application Server Java 7.0 SP12 or higher. For this reason it is crucial to understand how the Java server scales in order to understand how SAP GRC Access Control 5.3 scales.

2.1.1 Minimum Cluster Installation

The following figure shows the simplest installation of the usage type AS Java. The minimal AS Java installation consists of:

- The Java central instance with a dispatcher, a server process, and the Software Deployment Manager (SDM).
- The Central Services instance.
- The Database.

A Java Instance consists of (with the exception of Central Services):

- A Java Dispatcher
- One or several server processes

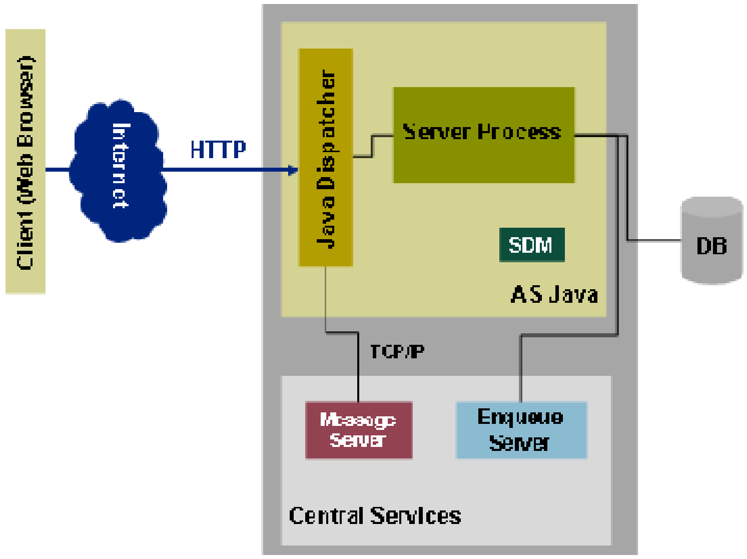


Figure: SAP NetWeaver Application Server Java: Minimal Cluster Installation

2.1.2 Scalability and Large Cluster Installation

The figure below shows a larger Java cluster installation. It consists of a central instance and two dialog instances, all of which have an instance number and each one can be started, stopped, and monitored separately.

> Note
>
> If you have a large Java cluster installation, the load is distributed between the available dialog instances by a load balancer. As load balancer you can either use SAP Web Dispatcher or a 3rd party hardware load balancer.

Each dialog instance can have an individual number of server nodes. In the figure below we have three J2EE instances; one with one server node, another one with two server nodes and the last one with three server nodes. Each server node hosts a number of threads where different requests can be processed in parallel.

For more information on NetWeaver architectural topics please refer to the *NetWeaver Architecure Manual*.

Field Code Changed

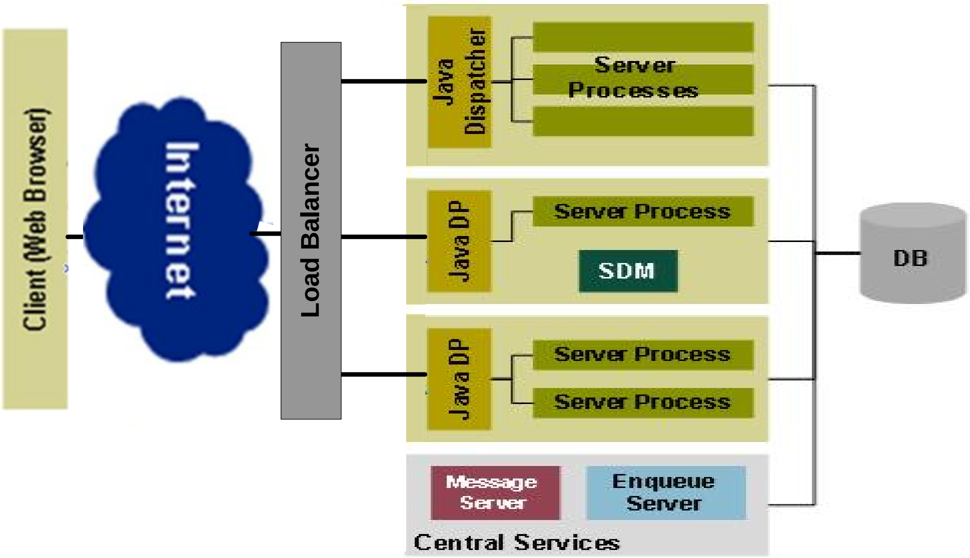


Figure: SAP NetWeaver Application Server Java: Large Cluster Installation

2.2 Access Control Technical Architecture

SAP GRC Access Control 5.3 leverages the technical infrastructure of SAP NetWeaver. Its user interface runs in any Browser supported by NetWeaver.

SAP GRC Access Control 5.3 is based on Web Dynpro Java (Risk Analysis and Remediation and Super User Privilege Management) and JSP (Compliant User Provisioning and Enterprise Role Management).

Each one of the four application components connects via System Connectors to a multitude of backend SAP and Non-SAP business applications. In the case of SAP backend systems all four application components can be configured to support integration with the system landscape directory for their system connectors. This allows for a central storage of connection data for each SAP backend system and for additional features like Secure Network Communication (SNC) and SAP Router strings.

In detail the four application components come with the following connectivity options:

- **Risk Analysis and Remediation:**
  - SAP Backend Systems with basis release levels 4.6C, 6.20, 6.40, 7.0 and 7.10
  - SAP NetWeaver Portal 7.0 SP12+
  - PEOPLESOFT Applications supported by Greenlight Adapters
  - JDE EnterpriseOne supported by Greenlight Adapters
  - ORACLE Applications supported by Greenlight Adapters
  - Legacy Application via flat file interface
- **Compliant User Provisioning:**
  - SAP Backend Systems with basis release levels 4.6C, 6.20, 6.40, 7.0 and 7.10
  - SAP NetWeaver Portal 7.0 SP12+
  - PEOPLESOFT Applications supported by Greenlight Adapters
  - JDE EnterpriseOne supported by Greenlight Adapters
  - ORACLE Applications supported by Greenlight Adapters
- **Enterprise Role Management:**
  - SAP Backend Systems with basis release levels 4.6C, 6.20, 6.40, 7.0 and 7.10
- **Superuser Privilege Management:**
  - SAP Backend Systems with basis release levels 4.6C, 6.20, 6.40, 7.0 and 7.10

For more detailed information on which versions of PEOPLESOFT, JDE and ORACLE applications are supported by Greenlight Adapters refer to SAP note 1076755.

For pie and bar chart generation SAP GRC Access Control 5.3 leverages the Internet Graphic Server (IGS) which is part of the NetWeaver technology platform.

Users within Access Control 5.3 are managed leveraging NetWeaver's User Management Engine (UME), which can to three different types of user repositories: local database, SAP backend system or to a supported LDAP directory.

To optimize user searches within the application context additional user persistence components can be added to the infrastructure:

- **Risk Analysis and Remediation:**
  - The *User Master Source* is the first system searched to obtain basic user data from. Any backend system connected via a system connector can be selected.
- **Compliant User Provisioning:**
  - The *User Source* is the primary source extracting basic user data during searches. UME or any backend system connected via a system connector can be selected.
  - The *User Details Source* is used to fetch additional information (attributes) about the user. UME or any backend system connected via a system connector or a combination of these (multiple data sources) can be selected.
  - The Authentication System verifies the requestor's identity from the selected system. UME or any backend system connected via a system connector can be selected.

Access Control 5.3 provides new web services for Identity Management (IDM) vendors, which enables seamless integration between IDM and GRC Access Control.

Access Control 5.3 is integrated with SAP Business Intelligence (BI 7.0.4). The BI content is packaged with the central BI content release.

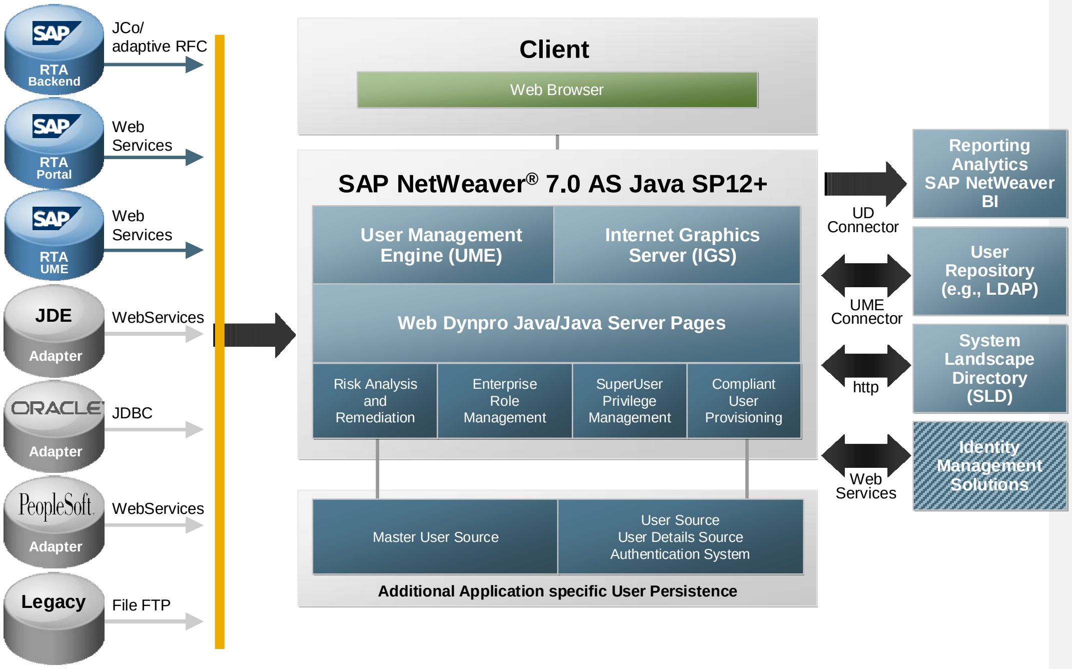

SAP
RTA
Backend
JCo/
adaptive RFC
SAP
RTA
Portal
Web
Services
SAP
RTA
UME
Web
Services
JDE
Adapter
WebServices
ORACLE
Adapter
JDBC
PeopleSoft
Adapter
WebServices
Legacy
File FTP
Client
Web Browser
SAP NetWeaver® 7.0 AS Java SP12+
User Management Engine (UME)
Internet Graphics Server (IGS)
Web Dynpro Java/Java Server Pages
Risk Analysis and Remediation
Enterprise Role Management
SuperUser Privilege Management
Compliant User Provisioning
Master User Source
User Source
User Details Source
Authentication System
Additional Application specific User Persistence
UD Connector
UME Connector
http
Web Services
Reporting Analytics SAP NetWeaver BI
User Repository (e.g., LDAP)
System Landscape Directory (SLD)
Identity Management Solutions

Figure: Access Control 5.3 – Technical Solution Architecture

3. Available Documentation

SAP Note 1243085 provides an overview of all existing documentation on SAP GRC Access Control and their locations. The following three subsections provide a summary and a list of SAP notes referenced in this guide.

3.1 GRC Access Control 5.3 Standard Documentation

SAP GRC Access Control 5.3 comes with the following documentation:

Title	Location
SAP GRC Access Control Configuration Guide	http://service.sap.com/instguides
SAP GRC Access Control Installation Guide	http://service.sap.com/instguides
SAP GRC Access Control Upgrade Guide	http://service.sap.com/instguides
SAP GRC Access Control Operations Guide	http://service.sap.com/instguides
SAP GRC Access Control User Guide	On SAP Help Portal at http://help.sap.com
SAP GRC Access Control Security Guide	http://service.sap.com/instguides
SAP GRC Access Control Release Notes	http://service.sap.com/releasenotes

3.2 Additional Useful Documentation

The table below contains references to additional useful documentation in the context of this guide

Content	Location
GRC HowTo Guides	www.sdn.sap.com/irj/sdn/bpx-grc
GRC Best Practices	www.sdn.sap.com/irj/sdn/bpx-grc
GRC Access Control - Access Risk Management Guide	https://www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/80c094de-90aa-2910-02b8-e31a6f5ff0c2
GRC eLearnings	https://www.sdn.sap.com/irj/sdn/grc-elearning
NetWeaver Architecure Manual	http://help.sap.com/saphelp_nw70/helpdata/en/e1/b5443e02a9ab4186a6e1240a9a2455/frameset.htm
Technical Operations Manual for SAP NetWeaver	http://service.sap.com/~form/sapnet?_SHORTKEY=01100035870000659947&_OBJECT=011000358700003985572006E
Sizing, calculation of hardware requirements such as CPU, disk and memory resource	http://service.sap.com/sizing
Released platforms and technology-related topics such as maintenance strategies and language support	http://service.sap.com/platforms To access the Platform Availability Matrix directly, enter service.sap.com/pam.

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Field Code Changed

Content	Location
Performance	http://service.sap.com/performance
Information about Support Package Stacks, latest software versions and patch level requirements	http://service.sap.com/sp-stacks

Field Code Changed

Field Code Changed

3.3 Important SAP Notes

The following SAP notes are referenced in this document:

SAP Note	Title	Content
1049638	System Data Maintenance for GRC Applications	Prerequisite for GRC support organization
723909	Java VM settings for J2EE 6.40/7.0	Prerequisite for performance optimization
871394	SAP NetWeaver04s:mandatory and optional J2EE Engine services	Deactivate non-mandatory J2EE engine services
927882	FAQ: MaxDB Update Statistics	FAQs. Important: Optimizer Statistics
1158625	Bad performance caused by Integer literals	MS SQL Server: J2EE Engine Patch
1044174	Recommendation for CC 5.x running on Oracle 10G Database	Creation of an index for table VIRSA_CC_PRMVL
830576	Parameter recommendations for Oracle 10g	General recommendation for Oracle 10g
823906	Oracle 9 database parameters tuning - EP in NW	To be applied accordingly for Access Control
124361	Oracle parameterization (R/3 >= 4.x, Oracle 8.x/9.x)	General recommendation for Oracle 8.x/9.x
1178370	Risk Analysis and Remediation - Table sizes	Suggested DB Administration tasks
1121978	Recommended settings to improve performance risk analysis	Datasource name & max. number of conncetions / JCo Pool Configuration / RAR Performance Tuning Parameters
1044173	Recomended NetWeaver Setting for Access Control 5.x	How to configure so as not to receive an out of memory exception.
1225111	CUP (AE)- Pool size limit (max connections) is 10 error	Increase max. number of JCo connection to 50.
1034117	Management Reports run too long, not updating, or inaccurate	Best Practice Recommendations on running RAR batch jobs
1179717	Risk Analysis and Remediation - Management Reports	Explanation of user / roles / profile synchronization process given
1126251	CC 5.x - Offline versus On-line Analysis	Explanations given on offline- and online analysis

SAP Note	Title	Content
1239588	Numbers of sync user / roles / profiles seem to be wrong	Detailed explanation of user / roles / profile synchronization process given
1249499	CC- Exceeds maximum number of WS threads allowed in Daemon	Background daemon troubleshooting
999785	Background Daemon will not Start	Background daemon troubleshooting
1176262	How to Start/Stop virsa/ccxsysbgear in Visual Admin	Background daemon troubleshooting
1176363	How to Start/Stop virsa/ccxsysbgear in Visual Admin	Background daemon troubleshooting
1129441	Monitoring Background Job Log Files for Archive or Delete	Avoid that Spool Files fill up your file system. Delete or archive them.
1178372	Risk Analysis and Remediation - Cross and Logical systems	Usage of Logical Systems & Cross Systems incl. limitations.
1039144	Superuser job is not completing or is not retrieving data	Performance optimization for retrieval of change logs.
1049512	Performance issues in running the Firefighter Background Job	Avoiding performance issues due to very large table CDHDR.

4. Step-by-Step Procedure

The following sections contain recommendations for performance optimization of SAP GRC Access Control 5.3 on the following layers:

- Java Virtual Machine
- J2EE Engine Services
- Adding Java Server Nodes
- Database Specific Recommendations
- System Connectors
- Risk Analysis and Remediation
- Superuser Privilege Management
- Compliant User Provisioning
- Enterprise Role Management

4.1 Optimize Java Virtual Machine (JVM)

After installation of the NetWeaver Application Java 7.0 make sure that you applied the recommended settings for Java Virtual Machine according to SAP Note 723909 and the SAP notes referenced in this note that apply to your specific platform. These settings are prerequisite for all further performance improvements.

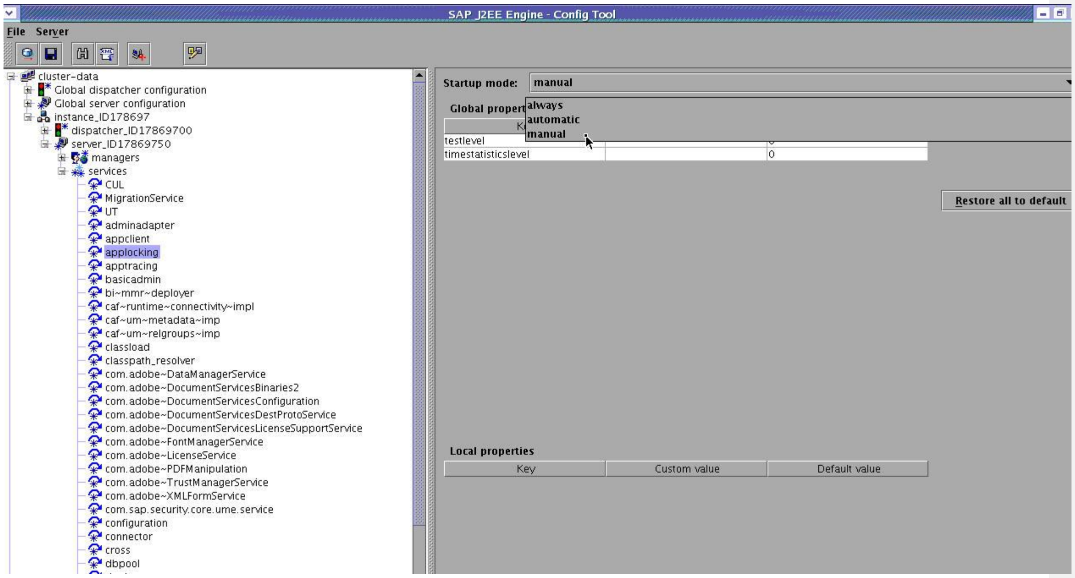
4.2 Deactivate Optional J2EE Engine Services

After a standard installation of the NetWeaver Application Java 7.0 many non-mandatory J2EE Engine services are activated and consume resources although they are not used. SAP Note 871394 lists mandatory and non-mandatory J2EE engine services. The following provides a list of services that can be deactivated without negative impact to the GRC Access Control application. Note that this list only applies, if you intend to use your Java application server to run SAP GRC Access Control only.

Name	**Technical name**
bi~mmr~deployer-provider	bi~mmr~deployer-provider
caf~runtime~connectivity~impl-provider	caf~runtime~connectivity~impl-provider
caf~um~metadata~imp-provider	caf~um~metadata~imp-provider
caf~um~relgroups~imp-provider	caf~um~relgroups~imp-provider
Document Services Data Manager	com.adobe~DataManagerService-provider
Document Services Binaries 2	com.adobe~DocumentServicesBinaries2-provider
Document Services Configuration	com.adobe~DocumentServicesConfiguration-provider
Document Adobe Destination Protocol Service	com.adobe~DocumentServicesDestProtoService-provider
Document Services Font Manager	com.adobe~FontManagerService-provider

Name	Technical name
Document Services License Support Service	com.adobe~LicenseSupportService-provider
PDF Manipulation Module - Low Encryption	com.adobe~PDFManipulation-provider
Document Services Trust Manager Service	com.adobe~TrustManagerService-provider
XML Form Module	com.adobe~XMLFormService-provider
IIOP Provider	iiop-provider
Leak Detector	leakdetector-provider
MigrationService-provider	MigrationService-provider
Log Viewer	tc.monitoring.logviewer-provider
eCATTPing - extended Computer Aided Test Tool Pinger	tc~eCATTPing~service-provider
Virus Scan Provider	tc~sec~vsi~service-provider
TREX Service	trex.service-provider

In order to deactivate a J2EE engine service logon to the Visual Administrator, select the service and change the startup mode to 'manual' as shown in the screenshot below:



```
cluster-data
  Global dispatcher configuration
  Global server configuration
  instance_ID178697
    dispatcher_ID17869700
    server_ID17869750
      managers
      services
        CUL
        MigrationService
        UT
        adminadapter
        appclient
        applocking
        apptracing
        basicadmin
        bi~mmr~deployer
        caf~runtime~connectivity~impl
        caf~um~metadata~imp
        caf~um~relgroups~imp
        classload
        classpath_resolver
        com.adobe~DataManagerService
        com.adobe~DocumentServicesBinaries2
        com.adobe~DocumentServicesConfiguration
        com.adobe~DocumentServicesDestProtoService
        com.adobe~DocumentServicesLicenseSupportService
        com.adobe~FontManagerService
        com.adobe~LicenseService
        com.adobe~PDFManipulation
        com.adobe~TrustManagerService
        com.adobe~XMLFormService
        com.sap.security.core.ume.service
        configuration
        connector
        cross
        dbpool
```

Startup mode: manual

always
automatic
manual

Global propert

K		
testlevel		
timestatisticslevel		0

Local properties

Key	Custom value	Default value

Figure: Changing the Startup Mode to deactivate a J2EE Engine Service

4.3 Set Severity Levels of J2EE Engine to ERROR

The Logs and Traces plug-in in the SAP NetWeaver Administrator allows you to view all list and text formatted logs and traces that are generated from the J2EE engine. You can access the Logs and Traces plug-in by choosing System Management → Monitoring → Logs and Traces.

You can configure logs and traces in the Log Configuration plug-in in the SAP NetWeaver Administrator. An important part of any log and trace message is its severity. This denotes the level of importance or relevance of a certain message. Log and traces can be limited to certain severity levels, that is, only data of a defined severity is collected. The order of the constants is, with increasing severity:

1. DEBUG – For debugging purpose, with extensive and low level information
2. PATH – For tracing the execution flow, for example, used in the context of entering and leaving a method, looping and branching operations
3. INFO – Informational text, mostly for echoing what has already been performed
4. WARNING – The application can recover from an anomaly and fulfill the required task, but needs attention from a developer/operator
5. ERROR – The application can recover from an error, but it cannot fulfill the required task due to the error
6. FATAL – The application cannot recover from an error, and the severe situation causes fatal termination

Categories and locations are associated with a severity. This acts as a filter where only those messages that are of equal or higher severity can pass.

Unless you are performing troubleshooting you should set severities to ERROR. Otherwise considerable system resources are used to write large amounts of logs and traces. For more information check the chapter on *Configuring Logs and Traces* in the *Technical Operations Manual for SAP NetWeaver*.

Field Code Changed

4.4 Add J2EE Server Nodes for Parallel Processing

In order to take advantage of parallel processing of batch risk analysis as explained in more detail in section 4.7.3 you should add server nodes to your Java instance. Note that it makes only sense to add server nodes to increase parallelization while CPU utilization during a batch risk analysis remains below 100% at least for some of your CPUs. Otherwise the server nodes are competing with each other for CPU time and the job wouldn't terminate much faster. As a first rough estimate on how many server nodes can be configured on your Java instance apply the following rules:

- Operation system and database will require approximately one CPU for itself.
- Each server node will require another CPU. For example you can configure 3 server nodes, if your hardware comes with 4 CPUs.
- Make sure that enough memory is available for your server nodes (refer to SAP note 723909).

Verify these recommendations for the initial configuration of your Java instance via diligent monitoring of CPU utilization and memory usage during batch risk analysis. Adapt the number of server nodes according to your observations.

4.5 Apply Database Specific SAP Notes

Depending on your database apply the following SAP notes:

Database	Note Number	Title
MS SQL Server	1158625	Bad performance caused by Integer literals

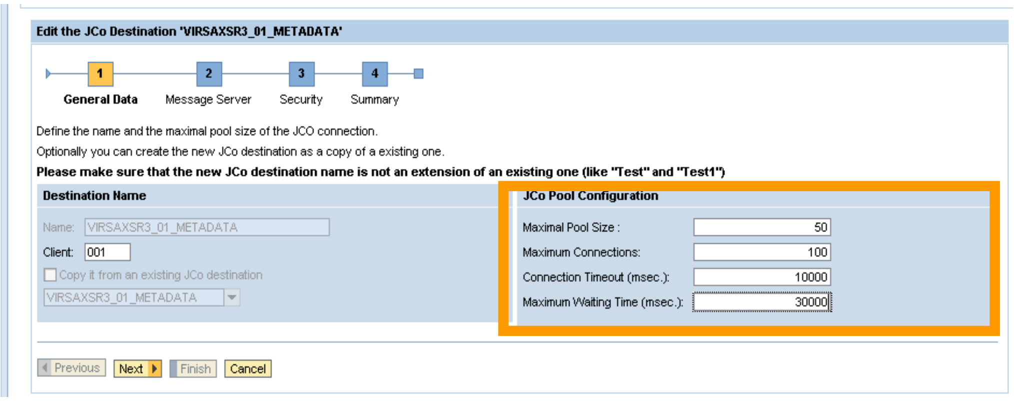
MaxDB	927882	FAQ: MaxDB Update Statistics
Oracle 10G	1044174	Recommendation for CC 5.x running on Oracle 10G Database
Oracle 10G	830576	Parameter recommendations for Oracle 10g
Oracle 8.x/9.x	124361	Oracle parameterization (R/3 >= 4.x, Oracle 8.x/9.x)
Oracle 9.x	823906	Oracle 9 database parameters tuning - EP in NW
All Databases	1178370	Risk Analysis and Remediation - Table sizes

Tip

If a batch risk analysis in Risk Analysis and Remediation doesn't complete after a long run time, before aborting check your database. In some databases you need to activate auto-extension of the database manually. During a synchronization or batch risk analysis temporary tables are filled and may hit your capacity limit.

4.6 Optimize System Connectors

Apply SAP Note 1121978 to tune Java Connector for Risk Analysis and Remediation in http://<server>:<port> → WebDynpro → Content Administrator.



Edit the JCo Destination 'VIRSAXSR3_01_METADATA'

Define the name and the maximal pool size of the JCO connection.

Optionally you can create the new JCo destination as a copy of a existing one.

Please make sure that the new JCo destination name is not an extension of an existing one (like "Test" and "Test1")

Destination Name

Name: VIRSAXSR3_01_METADATA

Client: 001

□ Copy it from an existing JCo destination

VIRSAXSR3_01_METADATA

JCo Pool Configuration

Maximal Pool Size : 50

Maximum Connections: 100

Connection Timeout (msec.): 10000

Maximum Waiting Time (msec.): 30000

Figure: Recommended JCo Pool Configuration

For Compliant User Provisioning apply SAP note 1225111 in order to increase pool size from 10 (default) to 50 JCo-connections

4.7 Optimize Risk Analysis and Remediation

The performance of Risk Analysis and Remediation can be improved by the following measures:

- Application of relevant SAP notes
- Usage of Logical Systems
- Parallelization of Synchronization and Batch Risk Analysis Background Jobs
- Application of Best Practices

The following subsections will provide more details on these measures.

4.7.1 Apply SAP Notes

Continue implementing SAP Note 1121978: In Risk Analysis and Remediation → Configuration → Performance Tuning set the following values:

- Batch size for users should be 1,000
- RFC Time out should be 1441
- Web Service worker: 5
- Job worker: 3

Make sure that your Sun JDE is on Compiler version 15 or higher (SAP note 1044173 – For Access Control 5.3 we recommend Sun JDK 1.4.2_15 or higher).

Schedule background jobs according to the recommendations given in SAP Note 1034117.

Refer to SAP Note 1179717, 1126251 and 1239588, if you want to learn more about synchronization and batch risk analysis.

For troubleshooting tips for the background job daemon refer to SAP notes 1249499, 999785, 1176262 and 1176363.

SAP Note 986997 provides additional information on how performance is impacted by various features of the application.

Finally make sure that spool files are regularly archived or deleted such that they cannot fill up your file system and cause a system stoppage. For details refer to SAP note 1129441.

4.7.2 Usage of Logical Systems

A logical system allows for a grouping of one or multiple physical system connectors in order to perform risk analysis against the same rules. Logical systems reduce the time and system resources required to load and maintain identical rule sets across multiple systems.

In SAP GRC Access Control risks are defined by one or multiple functions. Functions are defined by a set of actions and permissions each one referencing to one system. These system references in actions and permissions can be defined in two different ways:

- By references to physical system connectors
- By references to logical systems.

In the first case you need to include the same action / permission for each system connector individually into the function, which would multiply the number of actions and permissions contained in the function by the number of backend systems you want to use this function for.

For this reason it is strongly recommended using logical systems when uploading the SAP GRC rule set files during post-installation of Risk Analysis and Remediation or when defining functions manually in the rule architect. This approach allows sharing the same actions and permissions across multiple system connectors and keeps the number of rules to be loaded and checked against during a risk analysis smaller and reduces the time needed to complete a risk analysis considerably. It also facilitates the maintenance of your rule set, since a change of a function has to be implemented only once against the logical system rather than for each individual system connector individually. For more information on logical system refer to the *SAP GRC Access Control Configuration Guide*.

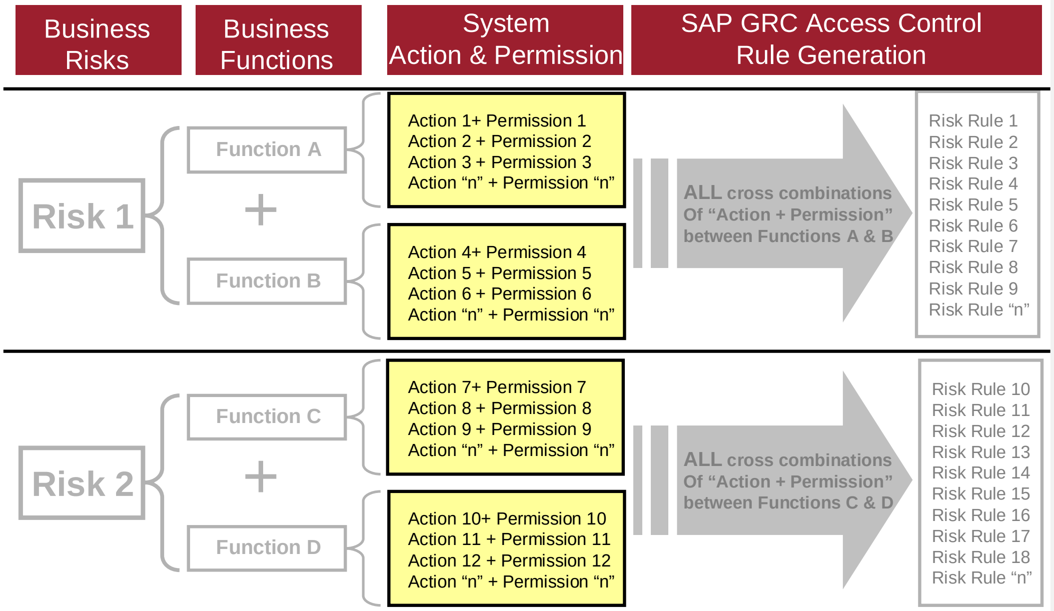


Figure: Definition of risks, functions and rules in SAP GRC Access Control

CAUTION

If you also plan to use the 'cross system' feature, please check SAP note 1178372 for limitations of the usage of logical systems in this context.

4.7.3 Parallelization of Background Jobs

SAP GRC Access Control 5.3 allows for foreground and background processing. All tasks are executed in threads running in the server nodes of the J2EE engine. Foreground processing takes place in so-called *web services worker* threads, whereas background jobs run in *background job worker* threads. The number of these threads can be configured (section 4.7.1). The threads are numbered in such a way that threads with IDs 0, 1 and 2 in each server node are used for background processing, if the recommendation in section 4.7.1 is followed. On each server node runs an Analysis Engine Daemon, which performs the dispatching of foreground tasks to web service worker threads and background jobs to background job worker threads. These daemons come with an ID, which is identical to the folder on the application server belonging to the server node the daemons runs in.

The Analysis Engine Daemon Manager allows monitoring these threads. It can be started with the URL http://<server>:<port>/sap/CCADStatus.jsp?debug=1.

Example

An example of a server with two server nodes is shown in the screenshot below. The threads are managed by two analysis engine daemons having the IDs D:\usr\sap\FGP\JC00\j2ee\cluster\server0\ and D:\usr\sap\FGP\JC00\j2ee\cluster\server1\, respectively. Each daemon manages three background job worker threads having the IDs 0,1 and 2 plus five web service worker threads having the IDs 3, 4, 5, 6 and 7. All threads are currently idle.

In GRC Access Control 5.3 the following two background jobs are executed in a parallelized fashion:

- User / Role / Profile Synchronization
- Batch Risk Analysis (scheduled in the Configuration → Background Jobs → Schedule Job)

Thread 0 on each server node is reserved for these two types of background jobs. A job of one of these two types is decomposed into subtasks and executed in parallel in the threads with ID 0 of each one of the available server nodes on the J2EE engine. Once all the subtasks are completed, the main job is marked as completed by the last server node which completes the last subtask.

Note

Only threads with ID 0 can execute user / role / profile synchronization and batch risk analysis background jobs. If there is already such a job running, other scheduled jobs of one of these two types have to wait until the running job completes and the threads with ID 0 become available again. Available background job worker threads with IDs different to 0 can't take over such jobs.

Note

None of the other background jobs like risk analysis started in the *Informer* tab, simulations, rule generation, organization user mapping, organization level reporting etc supports parallel processing. They are all processed in a single background job worker thread on one of the available server nodes.

If you have a large number of systems and users to include into your batch risk analysis, you should take advantage of the ability of parallel processing and configure multiple server nodes. If N is the number of server nodes, then the time required to complete the batch risk analysis should approximately depend by ~1/N on the number of available server nodes.

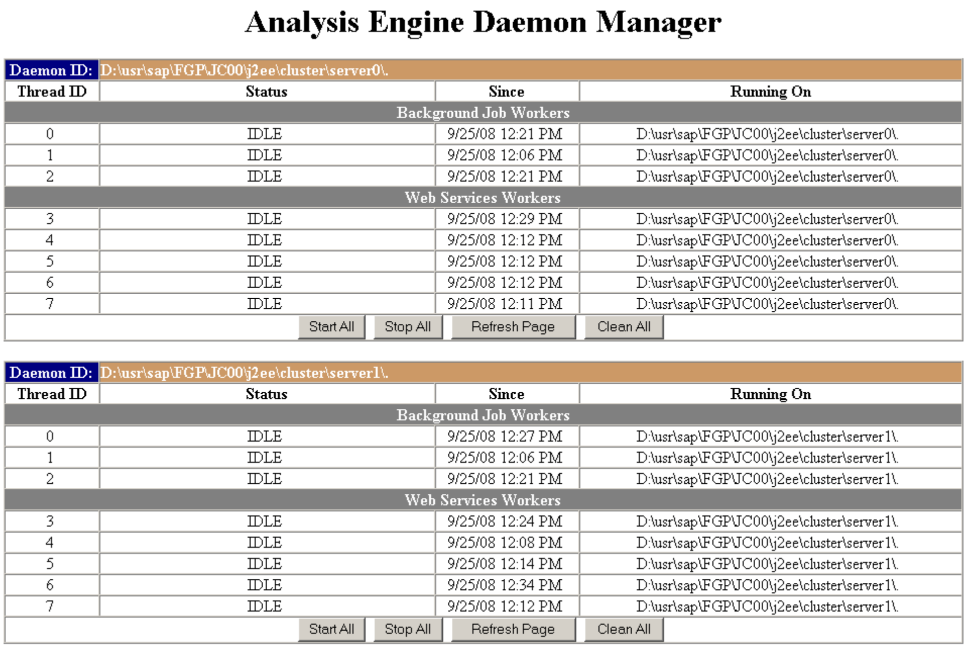
Example

Running a batch risk analysis on two server nodes should approximately take only half of the time than required for the same analysis on a single server node.

However, consider that adding server nodes requires more hardware resources (refer to section 4.3).

Note

Parallel processing is also supported across multiple Java dialog instances running on different hosts.



Analysis Engine Daemon Manager

Daemon ID:	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.		
Thread ID	Status	Since	Running On
Background Job Workers			
0	IDLE	9/25/08 12:21 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
1	IDLE	9/25/08 12:06 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
2	IDLE	9/25/08 12:21 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
Web Services Workers			
3	IDLE	9/25/08 12:29 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
4	IDLE	9/25/08 12:12 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
5	IDLE	9/25/08 12:12 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
6	IDLE	9/25/08 12:12 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.
7	IDLE	9/25/08 12:11 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server0\.

Daemon ID:	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.		
Thread ID	Status	Since	Running On
Background Job Workers			
0	IDLE	9/25/08 12:27 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
1	IDLE	9/25/08 12:06 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
2	IDLE	9/25/08 12:21 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
Web Services Workers			
3	IDLE	9/25/08 12:24 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
4	IDLE	9/25/08 12:08 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
5	IDLE	9/25/08 12:14 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
6	IDLE	9/25/08 12:34 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.
7	IDLE	9/25/08 12:12 PM	D:\usr\sap\FGP\JC00\j2ee\cluster\server1\.

Figure: Analysis Engine Daemon Manager on a server with two server nodes.

4.7.4 Best Practices for Batch Risk Analysis

4.7.4.1 Batch Risk Analysis – Selection Criteria

In Configuration → Background Jobs → Schedule Job in the Batch Risk Analysis frame you can select from one of the following options for the 'Analysis Mode':

- Incremental
- Full Sync.

The Full Sync mode will run over all users/roles/profiles in the selected systems and is only needed for initial risk analysis and each time when changes to the rule set incl. critical actions, critical roles, and critical profiles were applied. The Incremental mode will only analyze users/roles/profiles which have changed in your backend systems since the last batch risk analysis run and will complete much faster. It will not take front-end changes such as changes to the rule set into account. For this reason it is recommended that, in addition to the daily incremental batch risk analysis, a monthly full batch risk analysis is also scheduled. This will ensure that all changes made to the front-end are also appropriately reflected on the management reports.

The Batch Risk Analysis frame also allows for selection of the following objects to be included in the risk analysis:

- Users
- Roles
- Profiles
- Critical Action and Role/Profile Analysis

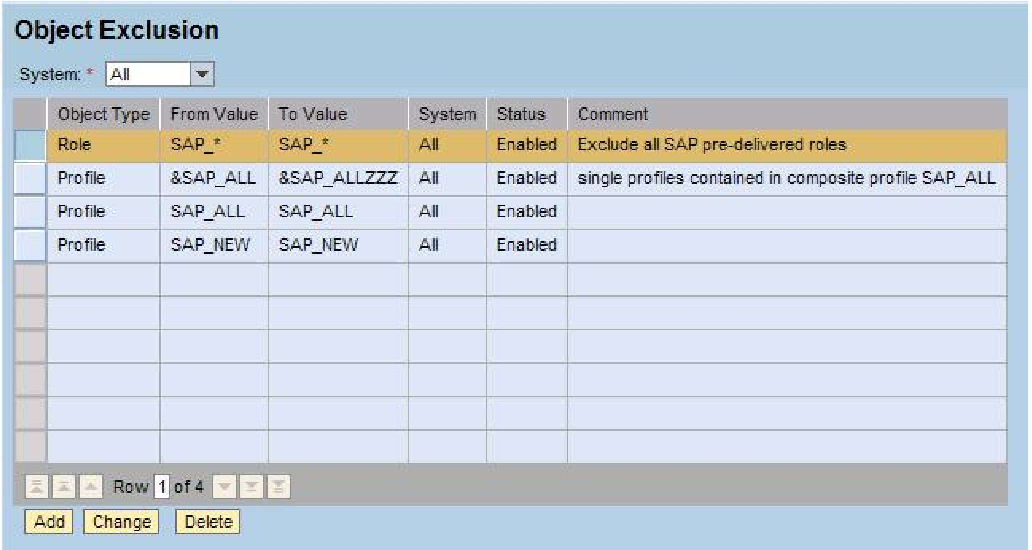
There is no need to include profiles, if you aren't assigning profiles to your users. Each SAP system comes with a considerable number of pre-delivered profiles; in addition, profile analysis will not only analyze old style SU02-profiles, but also all generated profiles that were already analyzed during the role analysis. If you have a large number of systems connected each one with rather small number of users, then the percentage of the total runtime spent for profile analysis may reach a two-digit percentage. For SAP_ALL and SAP_NEW and similar profiles refer to later section.

4.7.4.2 Batch Risk Analysis – Exclude Objects

With Support Package 05 the button 'Exclude Objects' was added in Configuration → Background Jobs → Schedule Job. It allows for exclusion of ranges of users, user groups (and the user included in the groups), roles and profiles from batch risk analysis and management reporting. Check whether you can exclude objects from risk analysis. This feature is most useful in combination with the Critical Roles and Critical Profiles features explained in the next section. You may exclude the following objects:

- Administrators or background users with SAP_ALL-like privileges: DDIC, SAP*, WFBATCH etc.
- Special user groups such as 'SUPER'
- SAP pre- delivered roles: 'SAP_*'
- Powerful roles you created for emergency access, administrators or system users.
- Special profiles such as all SAP_ALL and SAP_NEW profiles (including &SAP_ALL* and &SAP_NEW single profiles). Check SAP note 1034117 for more profiles to exclude.

SAP pre-delivered roles deserve particular attention. In ECC 6.0 SAP delivers more then 2500 roles in client 000. These roles are very often copied when setting up the business client xyz. Many customers don't use the pre-delivered roles and if they use them, then it is best practice to copy them into the customer name space first. Consequently, the originally pre-delivered roles are hardly used and may consume computation time during risk analysis, if their profiles were generated through mass generation at the time when the SAP system was installed. Note that these role occupy multiple name spaces: SAP_*, /IS*/* etc. If a high number of target systems is connected to your Access Control system with many of them having less than 1000 users, then percentage of the total runtime spent for the risk analysis on pre-delivered roles may become considerable. It is also possible to mass-delete these roles from your business client to keep it clean and simple. A mass deletion report is attached to SAP note 313587. Remember that you can always recover the deleted roles from client 000.



Object Exclusion

System: * All

Object Type	From Value	To Value	System	Status	Comment
Role	SAP_*	SAP_*	All	Enabled	Exclude all SAP pre-delivered roles
Profile	&SAP_ALL	&SAP_ALLZZZ	All	Enabled	single profiles contained in composite profile SAP_ALL
Profile	SAP_ALL	SAP_ALL	All	Enabled	
Profile	SAP_NEW	SAP_NEW	All	Enabled	

Row 1 of 4

Figure: List of Excluded Objects

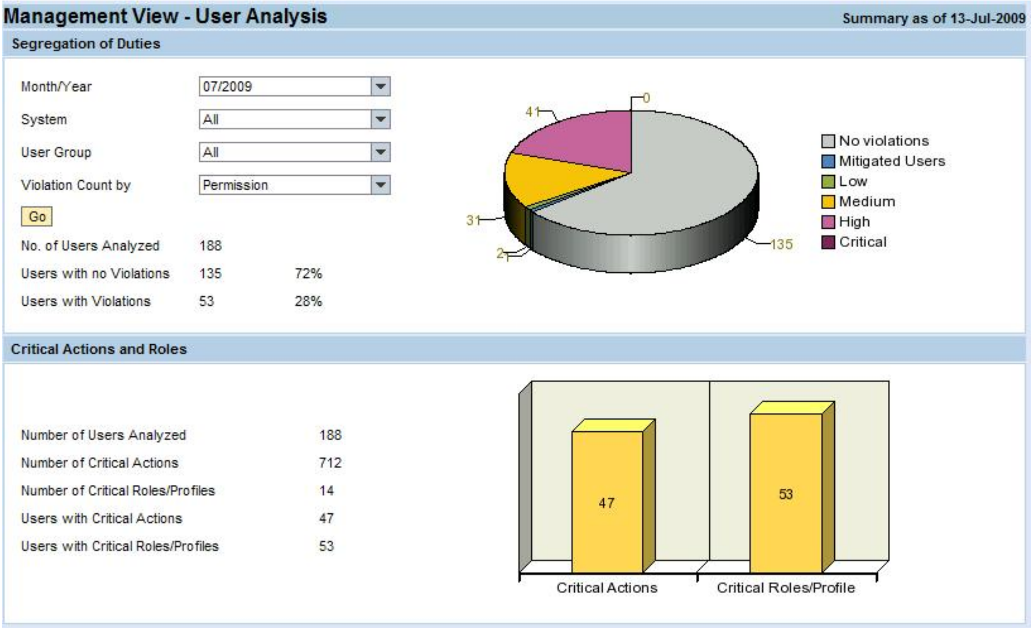
4.7.4.3 Critical Roles and Critical Profiles

There is little value in executing a time consuming risk analysis on roles or profiles such as SAP_ALL, which you already that they contain many critical risk violations. For this reason it is preferred practice to proceed as follows with such roles and profiles:

- Add critical roles to the Rule Architect → Critical Roles
- Add critical profiles to the Rule Architect → Critical Profiles
- During batch risk analysis mark the checkbox 'Critical Action and Role/Profile Analysis'
- Add the critical roles and profiles to the 'Object Exclusion' table
- Set the parameter 'Ignore Critical Roles & Profiles' in Configuration → Additional Options to 'Yes'. This ignores all the authorization objects that users are getting through critical roles / profiles when user level risk analysis is executed.

The users with critical roles and profiles are then reported in Informer → Management View → User Analysis and in Informer → Risk Analysis → User Level selecting 'Critical Role/Profile' as report type.

In addition, batch risk analysis for users with critical roles/profiles will focus on authorization from non-critical roles/profiles only that may have been assigned to the users as well. This helps drawing your attention on risk violations beyond the critical roles/profiles you may not have been aware of.



Management View - User Analysis — Summary as of 13-Jul-2009

Segregation of Duties

Month/Year	07/2009	
System	All	
User Group	All	
Violation Count by	Permission	
No. of Users Analyzed	188	
Users with no Violations	135	72%
Users with Violations	53	28%

Critical Actions and Roles

Number of Users Analyzed	188
Number of Critical Actions	712
Number of Critical Roles/Profiles	14
Users with Critical Actions	47
Users with Critical Roles/Profiles	53

4.7.4.4 Organizational Rules

Within Compliance Calibrator, SAP created organization rule functionality to eliminate these false positives based on organization level restrictions. It is important to understand that you should only use organization rules in those specific situations in which a company has made a conscious decision to segregate via organization levels. This functionality should not be used to try to group users into reports by organizational levels in order to distribute SoD reports to various management levels. Organization level rules should only be used for exception based reporting in order to remove false positive conflicts that result from organization level segregation. Because of the sizable performance impact that organization level rules can have, they should be used minimally for only those situations where the company has made a conscious decision to segregate via org levels. Companies should not institute organization rules until the remediation phase of their project. It is only after identifying a possible organization rule scenario that you should create the organization rules.

In conclusion, organizational rules should not be added as an additional organizational dimension on top of the corporate rule set, but are clearly a measure to be applied during the remediation phase on exceptional basis.

For more details refer to the *How-to-Guide SAP GRC Access Control: Organizational Rules and Organizational Level Reporting* available in BPX.

4.7.4.5 Default Values

Another powerful approach to speed up the time needed for batch risk analysis is focusing on only those users that are really relevant for your analysis. Therefore, in Configuration → Risk Analysis → Default Values we suggest excluding the following users:

- Locked users
- Expired users – users outside of their validity period can't logon
- Mitigated users – can be reported separately in Mitigation → Mitigated Users
- Default user type for risk analysis should be set to 'Dialog' to exclude all technical user types

4.7.4.6 Super User Privilege Management for Risk Remediation

The Super User Privilege Management capability is a powerful tool for risk remediation. It can help to shrink the number of risk violations with your user community drastically, which in turn reduces the runtime needed for risk analysis.

Start with identifying activities you need to perform in the backend systems, which

- are executed only once per month / quarter / year and
- add a considerable amount of risks to the users who have to perform them

Now, create in Superuser Privilege Management Firefighter IDs and grant the roles required for these activities to them. Then remove these privileges from your regular end users. As Firefighter IDs should be configured with user type 'communication' they can be excluded from risk analysis as well. This removes all risks related to these activities from your user community.

For more preferred practices on access risk remediation and mitigation refer to the GRC Access Control - Access Risk Management Guide.

4.8 Optimize Superuser Privilege Management

The performance of Superuser Privilege Management on application level can be improved by the following measures:

- Optimize retrieval of change logs

The following subsection will provide more details on this measure.

4.8.1 Performance optimization for retrieval of change logs

Superuser Privilege Management retrieves change logs from table CDHDR. In productive systems this table can become very large (several millions of data records). In order gain an acceptable performance in such environments it is strongly recommended to archive this table and follow the instructions given in SAP notes 1039144 and 1049512.

4.9 Optimize Compliant User Provisioning

The performance of Compliant User Provisioning on application level can be improved by the following measures:

- Reduce Log Level
- Avoid Risk Analysis for Critical Roles and Profiles

The following subsections will provide more details on these measures.

4.9.1 Reduce Log Level

Writing detailed logs is a resource consumptive operation. In Compliant User Provisioning in Configuration → Miscellaneous you can select from the following four log levels: DEBUG, INFO, WARN, ERROR. We recommend reducing the trace level down to ERROR.

4.9.2 Avoid Risk Analysis for Critical Roles & Profiles

In Compliant User Provisioning request approvers can perform a risk analysis the request approval screen before they approve the request. It is also possible to force approvers to run a risk analysis before they approve a request by a customizing setting in the stage definition. This is very useful feature for most requests. However, if the request contains profiles like SAP_ALL or very powerful roles designed for super-user or emergency access, an online risk analysis during request approval would take a very long time and have little benefit. Two alternative approaches help to avoid falling into this trap:

- Separate approvers for critical roles / profiles: Assigning a particular attribute to tag roles or profiles as critical can later be used to route requests to specific approvers responsible and trained for approving critical roles and profiles. They wouldn't start a risk analysis for such requests.
- If you run Superuser Privilege Management in the affected SAP backend systems, then the preferred approach would be to exclude critical roles and profiles from the role catalogue in Compliant User Provisioning and allow access to such roles and profiles only via a Firefighter ID in Superuser Privilege Management. End users can then request access to such a Firefighter ID in a particular SAP backend system via Compliant User Provisioning. As of Access Control 5.3 the new request type 'Super User Access' is available and allows for requesting and provisioning access to Firefighter IDs in Super User Privilege Management. For more information on this new feature refer to *SAP GRC Access Control Configuration Guide.*

4.10 Optimize Enterprise Role Management

The performance of Compliant User Provisioning on application level can be improved by the following measures:

- Reduce Log Level
- Avoid Risk Analysis for Critical Roles

The following subsections will provide more details on these measures.

4.10.1 Reduce Log Level

Writing detailed logs is a resource consumptive operation. In Enterprise Role Management in Configuration → Miscellaneous you can select from the following four log levels: DEBUG, INFO, WARN, ERROR. We recommend reducing the trace level down to ERROR.

4.10.2 Avoid Risk Analysis for Critical Roles

In Enterprise Role Management one or multiple methodology processes can be defined for role maintenance. A role methodology process is a sequence of the following available actions: Role Definition, Maintenance of Authorization Data, Role Derivation, Risk Analysis, Role Approval, Role Generation and Testing. Multiple role methodology processes can be created and used in parallel.

The first action in all role methodology processes is always Role Definition. During role definition role name, role attributes, description, role approvers etc. are defined. Each role methodology process is mapped against a set of values for the role attributes. According to the values of the role attributes assigned during role definition the role will be routed to the corresponding role methodology process. For more details on role methodology processes consult the *SAP GRC Access Control Configuration Guide.*

Similar to Compliant User Provisioning a risk analysis in Enterprise Role Management for a very powerful role designed for super-user or emergency access would be very time consumptive and have little benefit. For this reason it is recommended tagging such roles with a particular role attribute and routing it into a specific role methodology process for critical roles that doesn’t contain the Risk Analysis action. This avoids trapping with critical roles into a long-running risk analysis.

Appendix

A.1 Platform Details Used for Load Tests

Component	Details
Processor:	4 CPUs with 2,6 GHz Dual Core AMD Opteron Processor 2218
RAM	16 GB
OS	MS Server 2003
DB	SQL Server 2005
NetWeaver Application Server	Java 7.0 SP12
Server Nodes	2 GB heap space per server node 2 server nodes were used for: • RAR: Batch risk analysis tests • CUP: Tests
Access Control Version	Release: 5.3 Support Package 08: • RAR: Batch risk analysis (roles) • RAR: Batch risk analysis (profiles) • RAR: large rule set • RAR: Concurrent risk analysis • ERM: Single roles in composite roles Support Package 09: • RAR: Batch risk analysis (users) • ERM: Total number of roles • ERM: Number of authorizations in a role

A.2 Platform Details Used for SPM Load Tests

Component	Details
Processor:	32x AMD64 Level 16 (Mod 2 Step 3) 2200 MHz
RAM	24 GB
OS	MS Server 2003
DB	SQL Server 2005
NetWeaver Application Server	ABAP 7.01 SP3 (ECC 6.0)

Work Processes	49 Dialog Workprocesses
Access Control Version	**4.0** (VIRSA 400_700 Patch 10)