

Sizing Guide



Sizing SAP® BusinessObjects™ Access Control , Version 10.0

Released for SAP Customers and Partners

Document Version 1.0, November 2011

Please make sure that you are always using the most current version of the sizing guideline!



© Copyright 2011 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc. JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document

serves informational purposes only. National product specifications may vary.

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.

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 expressly prohibited, as is any decompilation of these components.

SAP Library document classification: CUSTOMERS & PARTNERS

Documentation in the SAP Service Marketplace

You can find this documentation at the following address: <http://service.sap.com/sizing>



TABLE OF CONTENTS

1.	Introduction	2
1.1.	Functions of SAP BusinessObjects Access Control	2
1.2.	Architecture of SAP BusinessObjects Access Control	3
1.3.	Factors that Influence Performance	4
2.	Sizing Fundamentals and Terminology	5
3.	Initial Sizing for SAP BusinessObjects Access Control	6
3.1.	Assumptions.....	6
3.2.	Sizing Overview	6
3.3.	Sizing Guidelines	6
3.3.1.	<i>User Synchronization</i>	<i>7</i>
3.3.2.	<i>Role Synchronization</i>	<i>7</i>
3.3.3.	<i>User Risk Analysis.....</i>	<i>8</i>
3.3.4.	<i>Role Risk Analysis.....</i>	<i>8</i>
3.3.5.	<i>Batch User Risk Analysis</i>	<i>8</i>
3.3.6.	<i>Batch Role Risk Analysis</i>	<i>9</i>
3.3.7.	<i>Access Request Creation.....</i>	<i>10</i>
3.3.8.	<i>Request Approval.....</i>	<i>10</i>
3.3.9.	<i>Role Import (Backend Synchronization).....</i>	<i>11</i>
3.3.10.	<i>Role Import (File Upload)</i>	<i>11</i>
3.3.11.	<i>Role Creation and Search</i>	<i>12</i>
3.3.12.	<i>Log Collection (Background Job)</i>	<i>12</i>
3.3.13.	<i>Log Report (Single User).....</i>	<i>13</i>
4.	Miscellaneous.....	14

1. INTRODUCTION

SAP BusinessObjects Access Control 10.0 (Access Control) delivers a comprehensive, cross-enterprise set of access controls that enables corporate compliance stakeholders -- including business managers, auditors, and IT security managers -- to collaboratively define and oversee proper Segregation of Duties (SoD) enforcement, enterprise role management, compliant provisioning, and super-user privilege management. SAP BusinessObjects Access Control addresses a complete range of control risks.

SAP solutions for governance, risk, and compliance are powered by the SAP NetWeaver® platform. SAP NetWeaver unifies technology components into a single platform, allowing organizations to reduce IT complexity and obtain more business value from their IT investments. It provides the best way to integrate all systems running SAP or non-SAP software. SAP NetWeaver also helps organizations align IT with their business. With SAP NetWeaver, organizations can compose and enhance business applications rapidly using enterprise services. As the foundation for enterprise service-oriented architecture (enterprise SOA), SAP NetWeaver allows organizations to evolve their current IT landscapes into a strategic environment that drives business change.

This guide provides guidelines and rules for sizing SAP BusinessObjects Access Control in your environment. Sizing is the process of translating business requirements into the overall hardware requirements (such as physical memory, CPU processing power, and network capacity) needed to implement SAP BusinessObjects Access Control. The guide describes the steps of this process and explains the factors that influence performance and hardware requirements.

Please note that this document only covers **general information about the initial sizing** of SAP BusinessObjects Access Control, and focuses on pure server sizing. Our experience from customer projects shows that every GRC Suite implementation is unique in scope and complexity. For this reason, we only provide general GRC recommendations and point out the most important factors that influence sizing. Complex scenarios are not covered in this document.

If your business requirement does not fit the standard T-shirt, we recommend performing an expert sizing, as every change in the infrastructure can have a significant impact on sizing and hardware requirements. Furthermore, the implementation of various SAP Business Packages or customer-specific content can have great impact on the sizing of the server and the related performance. Therefore, hardware requirements can vary dramatically.

1.1. Functions of SAP BusinessObjects Access Control

SAP BusinessObjects Access Control 10.0 provides several features including risk analysis and remediation, enterprise role management, superuser privilege management, and compliant user provisioning, among others. Specifically, Access Control 10.0 supports:

- Risk detection
Access Control 10.0 detects access and authorization risks across SAP and non-SAP applications, providing protection against a range of potential risk sources including segregation of duties and transaction monitoring.
- Risk remediation and mitigation
Access Control 10.0 enables fast, efficient remediation and mitigation of access and authorization risks by automating workflows and enabling collaboration among business and technical users.
- Reporting
Access Control 10.0 delivers the comprehensive reports and role-based dashboards businesses need to monitor the performance of compliance initiatives, and to take action as needed.
- Risk prevention
After access and authorization risks have been remediated, Access Control 10.0 prevents new risks from entering a production system. By empowering business users to check for risks in real time and automating user administration, Access Control 10.0 makes risk prevention a continuous, proactive process.

1.2. Architecture of SAP BusinessObjects Access Control

SAP GRC Access Control is an add-on (software component GRCFND_A) to SAP NetWeaver 7.02 (ABAP) that allows you to use all databases and operating systems supported by the SAP Web Application Server. Figure 1 illustrates the SAP BusinessObjects Access Control architecture.

Integrated scenarios, principally between GRC Access Control and GRC Process Control, require you to have both applications activated on the same SAP client (GRC Access Control resides in the same software component as the GRC Process Control and GRC Risk Management applications). Furthermore, GRC Plug-In Adapters are required for standard integration of SAP/non-SAP systems and GRC Access Control.



Note

Additional optional extensions (not considered in this initial sizing) are also available, including Identity Management Solutions integration, LDAP user repositories integration, non-SAP systems provisioning, and SAP NW Enterprise Portal provisioning integration, among others.

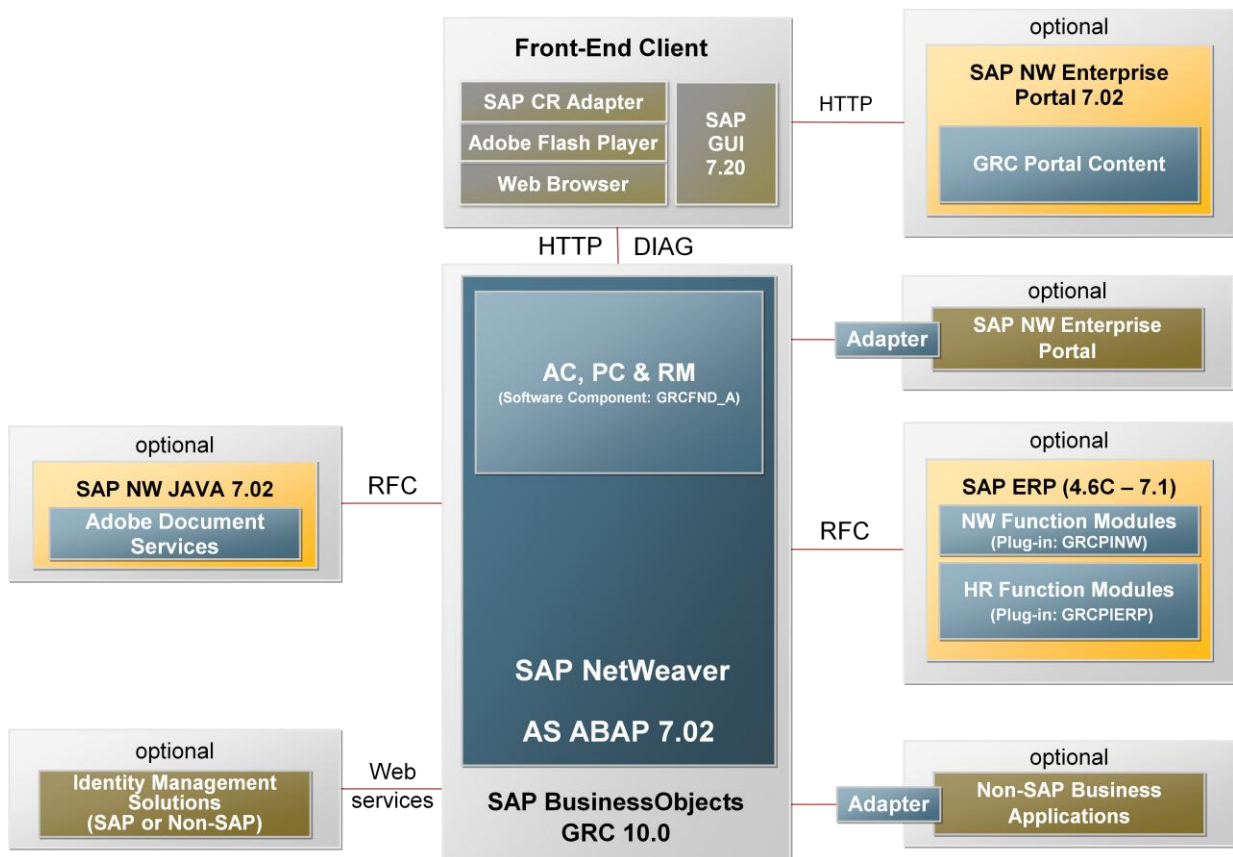


Figure 1: SAP BusinessObjects Access Control Architecture

1.3. Factors that Influence Performance

The performance-influencing factors in SAP BusinessObjects Access Control include the following:

- Master data volume
- Transaction data volume
- IMG configuration settings
- Number of concurrent users

In addition, the following factors influence performance when sizing SAP BusinessObjects Access Control:

- Landscape
 - Number and type of target/backend systems (including SAP, Non-SAP, IDM, and others) for access risk analysis, access provisioning, role generation and superuser privilege management
- Business Requirements
 - Total number of objects (users/roles/profiles) in each of the backend systems for access risk analysis
 - Total number of risks and rules defined for access risk analysis
 - Average number of permission level violations per object (user/role/profile) in access risk analysis
 - Number of average roles per request and number of average systems associated per request
 - Number of Firefighter IDs accessing the backend per hour during normal business hours and the average number of transactions per firefighter
 - Number of access requests per hour or per working day, and the number of maximum concurrent users to create or approve requests
 - Number of maximum concurrent real-time access risk analysis (ad-hoc) jobs and average number of objects (users/roles/profiles) in each real-time access risk analysis
 - Disk size (dependent on the number of violations, frequency of ad-hoc analysis, and the number of clients)
 - Complexity and configuration of the approval process definition (AC approval workflow settings)

2. SIZING FUNDAMENTALS AND TERMINOLOGY

SAP provides general sizing information on the SAP Service Marketplace. For the purpose of this guide, we assume that you are familiar with sizing fundamentals. You can find more information at <http://service.sap.com/sizing> → *Sizing Guidelines* → *General Sizing Procedures*.

This section explains the most important sizing terms, as these terms are used extensively in this document.

Sizing

Sizing means determining the hardware requirements of an SAP application, such as the network bandwidth, physical memory, CPU processing power, and I/O capacity. The size of the hardware and database is influenced by both business aspects and technological aspects. This means that the number of users using the various application components and the data load they put on the server must be taken into account.

Benchmarking

Sizing information can be determined using **SAP Standard Application Benchmarks** and scalability tests (www.sap.com/benchmark). Released for technology partners, benchmarks provide basic sizing recommendations to customers by placing a substantial load upon a system during the testing of new hardware, system software components, and relational database management systems (RDBMS). All performance data relevant to the system, user, and business applications are monitored during a benchmark run and can be used to compare platforms.

SAPS

The SAP Application Performance Standard (SAPS) is a hardware-independent unit that describes the performance of a system configuration in the SAP environment. It is derived from the Sales and Distribution (SD) Benchmark, where 100 SAPS is defined as the computing power to handle 2,000 fully business processed order line items per hour. (For more information about SAPS, see <http://www.sap.com/benchmark> → *Measuring in SAPS*).

Initial Sizing

Initial sizing refers to the sizing approach that provides statements about platform-independent requirements of the hardware resources necessary for representative, standard delivery SAP applications. The initial sizing guidelines assume optimal system parameter settings, standard business scenarios, and so on.

Expert Sizing

This term refers to a sizing exercise where customer-specific data is being analyzed and used to put more detail on the sizing result. The main objective is to determine the resource consumption of customized content and applications (not SAP standard delivery) by comprehensive measurements. For more information, see <http://service.sap.com/sizing> → *Sizing Guidelines* → *General Sizing Procedures* → *Expert Sizing*.

Configuration and System Landscaping

Hardware resource and optimal system configuration greatly depend on the requirements of the customer-specific project. This includes the implementation of distribution, security, and high availability solutions by different approaches using various third-party tools. In the case of high availability through redundant resources, for example, the final resource requirements must be adjusted accordingly. There are some "best practices" which may be valid for a specific combination of operating system and database. To provide guidance, SAP created the NetWeaver configuration guides (<http://service.sap.com/instguides> → *SAP NetWeaver*).

3. INITIAL SIZING FOR SAP BUSINESSOBJECTS ACCESS CONTROL

This section describes the procedure for sizing SAP BusinessObjects Access Control.

3.1. Assumptions

This section describes the assumptions used when sizing Access Control 10.0.

Initial sizing assumes the following:

- The standard, out-of-the-box access analysis rule set is used in all access risk analysis.
- The sizing relates to the Access Control 10.0 server only.
Plug-ins installed on backend systems can add overhead when Access Control 10.0 retrieves data. This overhead is not included.
- Initial sizing is completed using only select use cases, including full batch access risk analysis.
- Database sizing is included, but network sizing is not.

The following performance-influencing parameter in Access Control 10.0 have been turned off:

- Table logging

Also, this guide does not include sizing considerations for the following:

- NetWeaver Portal
- Report printing using Adobe Document Services (ADS)

3.2. Sizing Overview

Initial sizing involves a coordinated effort between SAP Basis and AC Functional experts to determine the expected number of users and transactional volume for the implemented features of Access Control.

With this user and transaction data, you can then use the sizing guidelines in the next section to determine the processing requirements, measured in SAPS. Finally, you can provide these results to your hardware partners to ensure that the appropriate processor, memory, and storage resources are available for your production environment.

3.3. Sizing Guidelines

The sizing results described in this section were obtained by measuring the following scenarios:

- User synchronization
- Role synchronization
- Batch user risk analysis
- Batch role risk analysis
- User risk analysis
- Role risk analysis
- Access request creation
- Request approval
- Role import (backend synchronization)
- Role import (file upload)
- Role creation and search

- Log collection (background job)
- Log report (single user)

3.3.1. User Synchronization

In this scenario, users perform user synchronization as a background job by running the SPRO transaction and executing *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Repository Object Synch.*

Procedure

1. Run the *SPRO* transaction.
2. Navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Repository Object Synch.*
3. In the *Select Sync Job* section, select the *User* check box.
4. Enter values in the required fields.
5. Choose the *Execute* pushbutton to run the user synchronization.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Synchronize 5000 users	4	327	2500
Medium	Synchronize 10,000 users	4	210	5000
Large	Synchronize 15,000 users	4	1,490	7500

3.3.2. Role Synchronization

In this scenario, users perform role synchronization as a background job by running the SPRO transaction and executing *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Repository Object Synch.*

Procedure

1. Run the *SPRO* transaction.
2. Navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Repository Object Synch.*
3. In the *Select Sync Job* section, select the *Role* check box.
4. Enter values in the required fields.
5. Choose the *Execute* pushbutton to run the role synchronization.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Synchronize 1000 roles*	8	2.67	1000
Medium	Synchronize 3000 roles*	8	6.24	3000
Large	Synchronize 5000 roles*	8	6.87	5000

* 5 languages.

3.3.3. User Risk Analysis

In this scenario, users perform user risk analysis using the *Access Management > Access Risk Analysis > User Level* application.

Procedure

1. Choose *Access Management > Access Risk Analysis > User Level*.
2. Enter values in the required fields.
3. Choose the *Run in Foreground* pushbutton to run the risk analysis.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1 user*	68	0.005	10
Medium	10 concurrent users*	68	0.045	100
Large	25 concurrent users*	68	0.110	250

* Performing 1 user risk analysis (4300 violations)

3.3.4. Role Risk Analysis

In this scenario, users perform role risk analysis using the *Access Management > Access Risk Analysis > Role Level* application.

Procedure

1. Choose *Access Management > Access Risk Analysis > Role Level*.
2. Enter values in the required fields.
3. Choose the *Run in Foreground* pushbutton to run the risk analysis.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1 user*	64	0.005	10
Medium	10 concurrent users*	64	0.045	100
Large	25 concurrent users*	64	0.110	250

* Performing 1 role risk analysis (4300 violations)

3.3.5. Batch User Risk Analysis

In this scenario, users perform batch user risk analysis by running the SPRO transaction and executing *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Access Risk Analysis > Batch Risk Analysis > Execute Batch Risk Analysis*.

Note the following assumptions for this scenario:

- 10% of the user community is violating
- Each violating user has 1000 violations and 5 profiles

Procedure

1. Run the *SPRO* transaction.
2. Navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Access Risk Analysis > Batch Risk Analysis > Execute Batch Risk Analysis*.
3. In the *System Selection* section, enter appropriate values in the *Job Name*, *System*, and *RuleSet* fields.
4. In the *Batch Processing Mode* field, choose *Full*.
5. In the *Object Selection* section, check the *User Analysis* check box and specify the *User* range for the batch risk analysis.
6. In the *Risk Analysis Type* section, check the *Permission/Critical Action/Critical Permission Level* check box.
7. Choose the *Execute* pushbutton to run the batch risk analysis.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1000 users	4	125	2000
Medium	5000 users	8	625	10,000
Large	10,000 users	8	1,250	20,000

Note: Each violating user with 1000 violations has a SAPS value of 20.

3.3.6. Batch Role Risk Analysis

In this scenario, users perform batch role risk analysis by running the *SPRO* transaction and executing *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Access Risk Analysis > Batch Risk Analysis > Execute Batch Risk Analysis*.

Procedure

1. Run the *SPRO* transaction.
2. Navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Access Risk Analysis > Batch Risk Analysis > Execute Batch Risk Analysis*.
3. In the *System Selection* section, enter appropriate values in the *Job Name*, *System*, and *RuleSet* fields.
4. In the *Batch Processing Mode* field, choose *Full*.
5. In the *Object Selection* section, check the *Role Analysis* check box and specify the *Role* range for the batch risk analysis.
6. In the *Risk Analysis Type* section, check the *Permission/Critical Action/Critical Permission Level* check box.
7. Choose the *Execute* pushbutton to run the batch risk analysis.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	100 roles*	8	98	400
Medium	1000 roles*	8	978	4000
Large	5000 roles*	20	4,892	20,000

* Each role has 1000 permission violations.

3.3.7. Access Request Creation

In this scenario, users create access requests using the *Access Management > Access Request Creation > Access Request* application.

Procedure

1. Choose *Access Management > Access Request Creation > Access Request*.
2. Enter values in the required fields.
3. Choose the *Submit* pushbutton.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1 user creating a request*	45	0.1	15
Medium	10 concurrent users each creating one request*	53	0.98	150
Large	25 concurrent users each creating one request*	53	2.45	375

* 1 user with 5 roles

3.3.8. Request Approval

In this scenario, users approve access requests using the *My Home > Work Inbox* application.

Procedure

1. Choose *My Home > Work Inbox*.
2. Search for the request created in section 3.2.7 (in this guide).
3. Choose the request hyperlink to open the request.
4. Choose the *Submit* pushbutton to approve the request.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1 user approves a request*	85	0.18	10
Medium	5 concurrent users approving requests*	87	0.86	50
Large	10 concurrent user approving requests*	87	1.7	100

* 1000 violations

3.3.9. Role Import (Backend Synchronization)

In this scenario, users import roles by performing backend synchronization using the *Access Management > Role Mass Maintenance > Role Import* application.

Procedure

1. Choose *Access Management > Role Mass Maintenance > Role Import*.
2. In the *Import Source* section, select *Backend System* as the *Role Authorization Source*.
3. In the *Definition Criteria* section, choose *Governance, Risk and Compliance* in the *Application Type* field.
4. Choose the appropriate *Landscape* and *Source System*, and choose the *Next* pushbutton.
5. In the *Select Role Data* step, complete the required fields and choose the *Next* pushbutton.
6. In the *Review* step, choose the *Next* pushbutton.
7. In the *Schedule* step, choose the *Submit* pushbutton.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Import 1000 roles	20	309	1000
Medium	Import 2000 roles	24	619	2000
Large	Import 5000 roles	32	1,547	5000

* Background execution

3.3.10. Role Import (File Upload)

In this scenario, users import roles through a file upload using the *Access Management > Role Mass Maintenance > Role Import* application.

Procedure

1. Choose *Access Management > Role Mass Maintenance > Role Import*.
2. In the *Import Source* section, select *File on Desktop* as the *Role Authorization Source*.
3. In the *Definition Criteria* section, choose *Governance, Risk and Compliance* in the *Application Type* field.
4. Choose the appropriate *Landscape*, and choose the *Next* pushbutton.
5. In the *Select Role Data* step, specify the file name in the *Role Authorization Source* section, and choose the *Next* pushbutton.
6. In the *Review* step, choose the *Next* pushbutton.
7. In the *Schedule* step, choose the *Submit* pushbutton.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Import 100 roles*	28	31	100
Medium	Import 200 roles*	555	62	200
Large	Import 500 roles*	1,363	155	500

* Background execution

3.3.11. Role Creation and Search

In this scenario, users create roles and then search for the role using the *Access Management > Role Management > Role Maintenance* application.

Procedure

1. Choose *Access Management > Role Management > Role Maintenance*.
2. Choose *Create > Single Role*.
3. Enter values in the required fields.
4. Choose the *Save & Continue* pushbutton.
5. Choose the appropriate authorization, and choose the *Save & Continue* pushbutton until the role generation is complete.
6. Choose the *Close* pushbutton.
7. Choose *Access Management > Role Management > Role Search*.
8. Type the name of the role you created above, and choose the *Search* pushbutton.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	1 user*	195	0.11	120
Medium	5 concurrent users**	203	0.54	600
Large	10 concurrent users**	200	1.1	1200

* Creating 1 role with 50 transactions and 20 auth objects, searching 1 role from among 10,000 roles

** Each user creating 1 role with 50 transactions and 20 auth objects, searching 1 role from among 10,000 roles

3.3.12. Log Collection (Background Job)

In this scenario, users perform log collection as a background job by running the SPRO transaction and executing *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Firefighter Log Synch*.

Procedure

1. Run the *SPRO* transaction.
2. Navigate to *SAP Reference IMG > Governance, Risk and Compliance > Access Control > Synchronization Jobs > Firefighter Log Synch*.
3. Enter an appropriate value in *Connector* field.
4. Choose the *Execute* pushbutton.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Log collection of 1 user executing 20 transactions	4	0.065	10
Medium	Log collection of 10 users executing 200 transactions	4	0.6	100
Large	Log collection of 50 users executing 1000 transactions	4	3.32	500

3.3.13. Log Report (Single User)

In this scenario, users create roles and then search for the role using the *Reports and Analytics > Super User Management Reports > Firefighter Log Summary Report* application.

Procedure

1. Choose *Reports and Analytics > Super User Management Reports > Firefighter Log Summary Report*.
2. Enter values in the required fields.
3. Choose the *Run in Foreground* pushbutton to run the report.

The following table shows the sizing guidelines according to the usage categories:

Category	Description	Peak Memory (MB)	Minimum Disk Space (MB)	Minimum SAPS
Small	Log report of 1 user executing 20 transactions	16	0	10
Medium	Log report of 10 users executing 200 transactions	20	0	100
Large	Log report of 50 users executing 1000 transactions	56	0	500

4. MISCELLANEOUS

This section describes the resources available related to sizing procedures and guidelines, as well as benchmark and installation guides.

General Sizing

<http://service.sap.com/sizing> > Sizing Guidelines > General Sizing Procedures

Expert Sizing

<http://service.sap.com/sizing> > Sizing Guidelines > General Sizing Procedures > Expert Sizing

Benchmarking

<http://www.sap.com/benchmark>

Business Process Experts

<https://www.sdn.sap.com/irj/sdn/bpx/grc>

Installation Guides

<http://service.sap.com/instguides> > SAP BusinessObjects > SAP BusinessObjects Governance, Risk, Compliance (GRC) > Access Control > SAP GRC Access Control 10.0