Commander, Pacific Fleet (COMPACFLT)
Secure Enterprise Access Control (SEAC)
Role Based Access Control (RBAC)

Point of Contact:
Richard Fernandez
(808) 474-9270

The information contained herein is considered U.S. Government Proprietary and may be related to one or more U.S. Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004
SSC San Diego
San Diego, CA 92152-5001
Approved for public release; distribution is unlimited.
The SEAC RBAC is available at:

References:
http://csrc.nist.gov/rbac/

For comments contact:
Richard Fernandez
(808) 474-9270
Richard.R.Fernandez@navy.mil

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Access Control Lists (ACL)

User name or unique identifier associates access to resources

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Groups

User associated to a group and group associated to resources

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Essentials for resource access

 Necessary requirement to access resources:

 • Not a user name
 • Not a unique identifier
 • Not a group association
 • List of user characteristics

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
What are user characteristics

User characteristics (user profile)

• Where client works: organization
• What security credentials: clearance
• What pay category: pay grade
• What branch: service
• What vocation: job function
• etc

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Examples of User Profiles

- User profile is a unique list of user characteristics.
- A client may have more than one user profile.
- User attributes should be compiled from an authoritative data source(s) on a real-time basis.

<table>
<thead>
<tr>
<th>Categories</th>
<th>COMPACFLT</th>
<th>USNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization:</td>
<td>CPF N65</td>
<td>Naval Intel</td>
</tr>
<tr>
<td>Clearance:</td>
<td>Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Paygrade:</td>
<td>DP3</td>
<td>02</td>
</tr>
<tr>
<td>Service:</td>
<td>DoD</td>
<td>DoNR</td>
</tr>
<tr>
<td>Function:</td>
<td>Program Manager</td>
<td>Intelligence</td>
</tr>
</tbody>
</table>

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Impact on resource access

The following can affect resource access:

• Transfer to another organization
• Loss of security clearance
• Change in job title
• Job promotion

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Problems with ACLs and Groups

Maintaining an updated ACL or group is time consuming.

Situation worsens when:

• Number of users increase
• Number of resources increase
Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) has declared RBAC an American National Standard - ANSI INCITS 359-2004 (approved 19 Feb 04)
Definitions:

**Users and Roles:** “…access decisions are based on the roles that individual users have as part of an organization.
"Access rights are grouped by role name…

**Role hierarchies:** "Under RBAC, roles can have overlapping responsibilities and privileges;

**Roles and Operations:** "Organizations can establish the rules for the association of operations with roles.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

<table>
<thead>
<tr>
<th>User Characteristics</th>
<th>Number of user characteristics evaluated</th>
<th>Hierarchal evaluation of user characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACLs</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Groups</td>
<td>1</td>
<td>Yes/No</td>
</tr>
<tr>
<td>NIST RBAC</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>SEAC RBAC</td>
<td>Unlimited</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note: A hierarchal structure offers inheritance capabilities.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
How the SEAC RBAC works

Step 1:
Resource manager establishes a set of conditions to access a resource.

These set of conditions represent a resource profile.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
How the SEAC RBAC works

Step 2:
An effective RBAC requires real-time creation of user profile(s) from authoritative data source(s).

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
How the SEAC RBAC works

Step 3:
The RBAC Rules Engine compares User and Resource Profiles to determine resource access.

User Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

Customer Resource Database
- Project Tracker (resource)
- HR Service (resource)
- Payroll Application (resource)

Access token for Project Tracker

RBAC Rules Engine

RBAC Resource Directory

Project Tracker Resource Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Reference directory standard specifications

- Customer meta-database
- LDAP v 3/DSML directory
- X500 class objects
  - organization
  - organizationalUnit
- Scalable
  - unlimited entries
  - modifications allowed
- Structure designation
  - domain
  - reference category
  - values
- Structure
  - flat
  - hierarchal
- Maintained
  - local commands
  - regional commands

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
# SEAC RBAC – Resource profiles

<table>
<thead>
<tr>
<th>Resource Roles for Project Tracker</th>
<th>Resource Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>CPF Guest</td>
</tr>
<tr>
<td></td>
<td>T ✓ COMPACFLT</td>
</tr>
<tr>
<td></td>
<td>✓ COMSUBPAC</td>
</tr>
<tr>
<td></td>
<td>✓ DoD</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>User</td>
<td>CPF N6 Users</td>
</tr>
<tr>
<td></td>
<td>T ✓ CPF N6</td>
</tr>
<tr>
<td></td>
<td>✓ GS12</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Administrator</td>
<td>CPF Admin</td>
</tr>
<tr>
<td></td>
<td>✓ CPF N65</td>
</tr>
<tr>
<td></td>
<td>T ✓ TS</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
SEAC RBAC – Security levels

During INFOCON B

- Pre-configure conditions under each security level.
- RBAC Rules Engine evaluates only conditions for prevailing security level.

During INFOCON C

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
(A) Directory Manager Interface: manages reference directory referrals.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
(B) Resource Manager Interface: manages a resource container used to store conditions.
(C) Security Level Interface: establishes prevailing security level.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
(E) User profile manager: user profile selection and DN formatting.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
SEAC RBAC - Model

(F) Rules Engines: evaluates user and resource profiles to determine resource access.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
(G) Condition deprecation: scans reference directories and compares resource profiles for any changes.
Pearl Harbor: resource profile created for local resource access.
**SEAC RBAC - Interoperability**

Pearl Harbor: local user profile is generated to access a local resource.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Pearl Harbor: user and resource profiles are evaluated by rules engine to determine local resource access.
Pearl Harbor: A resource profile to allow remote users access to local resources.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
San Diego: user profile generated.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
Pearl Harbor: San Diego user evaluated for Pearl Harbor resource access.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
San Diego: same user evaluated for San Diego resource access.

The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
The information contained herein is considered US Government Proprietary and may be related to one or more US Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.
The information contained herein is considered U.S. Government Proprietary and may be related to one or more U.S. Government owned inventions. Reference Navy Case No. 96,217. Please call (619) 553-3001 regarding licensing inquiries.

SD 541, June 2004
SSC San Diego
San Diego, CA 92152-5001
Approved for public release; distribution is unlimited.