Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle’s products remains at the sole discretion of Oracle.
An introduction to Global Policies .................................................. 4
An introduction to Global Policies

In a given Policy, ‘Policy Shortcut Chain’ Filters allow us to delegate to one or more Policies to perform specific pieces of work, before continuing execution of the remaining Filters in the current Policy. Using this approach to encapsulate specific functionality in a given Policy allows modularity and reusability in designing the overall gateway circuitry, and this way the Policy designer can over time build up a Policy library of reusable routines.

Previously, each shortcut in a Policy Shortcut Chain needed to point to a specific Policy which gets called at each point in the execution chain. Consider however a Policy whose role is, say, to be called first in all message handling contexts before any context specific Policies are run. We’ll call this the ‘run-first’ role. To realize this previously you would have to create a Policy Shortcut Chain with a link to the ‘run-first’ Policy as its first entry, the context-specific Policy as its second link, and so on. One of the shortcomings of this approach was that if you had a large number of Policy Shortcut Chains set up, each calling the ‘run-first’ Policy, and you needed to change the ‘run-first’ Policy globally, you would need to update each Policy Shortcut Chain Filter individually to point to the newly designated ‘run-first’ Policy. Equally, if you wanted to ignore the ‘run-first’ Policy globally, you would need to remove the first entry in each Filter.

We have introduced the ability to label a given Policy, marking it in terms of its role, and can now delegate to the Policy via its label rather than via a specific link to a specific Policy. This indirection via a label makes it very easy to globally change which Policy gets delegated to, merely by moving the label from one Policy to another. Each Filter which refers to the Policy via its label now resolves the label to the new Policy without necessitating changing the configuration for the Filter. Equally, if the label is applied to no particular Policy, then nothing gets executed for this link.
There are 3 roles which have reserved labels and consequently specific meaning in the Policy configuration framework, namely:

<table>
<thead>
<tr>
<th>Role</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Request Policy</td>
<td>system.policy.request</td>
</tr>
<tr>
<td>Global Response Policy</td>
<td>system.policy.response</td>
</tr>
<tr>
<td>Global Fault Handler Policy</td>
<td>system.policy.faulthandler</td>
</tr>
</tbody>
</table>

The Policy designer can mark specific Policies with these roles from the Policy navigation tree, and references to these roles can be made when creating a Policy Shortcut Chain.

While the ‘Global Fault Handler Policy’ can be referred to in this way too, it has an additional meaning in that if any Policy throws an Abort during execution, or a top-level
Policy fails, and the user hasn’t specified a Fault Handler Filter, then this Policy will be
executed instead of the internal SOAP Fault Filter, should a Policy be so set in this role.

Any user-labelled Policies can be found from a right-click on the Policy root node:

As well as allowing the Policy designer to hand-roll Policy Shortcut Chains containing
role-based links, we have incorporated these global roles into the entry point handlers for
messages inbound to the Policy circuitry, namely the ‘Relative Path’ and ‘Web Service
Resolvers’. Here, instead of delegating to a single Policy on receiving a request as we did
in the past, we now allow the user to specify which Policies should be run in a hardcoded
sequence, namely:

1. Call the Global Request Policy
2. Call the specific handler for the resolver
3. Call the Global Response Policy
Oracle Enterprise Gateway

Resolve path to Policies

- Enable this path resolver

Policies

- Audit Settings

When a request arrives that matches the path: /

Call the following Policies:

- Global Request Policy

- Path Specific Policy: Return HTTP Error 403: Access Denied (Forbidden)

- Global Response Policy

OK  Cancel  Help