Chapter 20

Overview of Enterprise Service Portals

This chapter provides an overview of enterprise service portals and contains the following sections:

Function of Enterprise Service Portals

The SRC software enables service providers to use enterprise service portals to provision services to enterprise subscribers who connect to the SRC network by means of a JUNOSe router or a JUNOS routing platform. An enterprise service portal is a standalone Web application that runs in a Java 2 Platform, Enterprise Edition (J2EE)-compliant Web application server. An enterprise service portal must have a corresponding configuration in the directory. Typically, a service provider provisions the router and configures the initial directory structure.

IT managers in an enterprise log in to the SRC network through an enterprise service portal. The managers can then activate services and perform some administrative tasks associated with their enterprises. When an IT manager requests an action through an enterprise service portal, the enterprise service portal uses the SRC software's enterprise service portal application programming interface (API) to interact with the SAE and to update data in the directory.

More specifically, the enterprise service portal calls methods in this API to:

- Authenticate IT managers in an enterprise.
- Create, delete, and modify accounts for IT managers.
- Navigate among retailers, enterprises, sites, and accesses.
- Create, delete, activate, and deactivate subscriptions to services.
- Get feedback from the sessions that a subscription generates. This feedback, which comes directly from the SAE managing the session, indicates whether the session is active in the network and provides the values used for the service parameters.
- Get feedback about the use of resources, such as the number of bytes and packets the SAE has sent or received for a particular service.
- Configure values for service parameters.

Consistency of Data in the Directory

Enterprise service portals can monitor the consistency of data as you enter it through the portal; for example, an enterprise service portal can prevent you from deleting a subscription if that subscription depends on other data in the directory. Enterprise service portals do not constantly monitor the consistency of existing data in the directory for all subscribers, however, because doing so would consume significant network resources. Consequently, if you use an LDAP browser to modify data in the directory that was entered through a portal, you must be sure that the data in the directory is consistent.

Privileges of IT Managers

The enterprise service portal API controls the privileges that determine how IT managers can manipulate subscribers, subscriptions, and services associated with a retailer or enterprise. All IT managers in an enterprise share the same connections to the directory.

Developing and Customizing Enterprise Service Portals

You can customize enterprise service portals to provide customer-specific Web pages and supply specified services. By modifying JavaServer pages (JSP), which use a set of customized tags to call methods in the enterprise service portal API, you can customize an enterprise service portal to suit a customer's environment.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library in the SRC software distribution in the folder */SDK/doc/ent/tagDocs* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Identifying the SAE

An enterprise service portal handles a request from an IT manager by communicating with the SAE that manages the subscriber affected by the IT manager's request. You can use the following methods to allow the enterprise service portal to identify which SAE manages a subscriber:

- For SRC implementations that use more than five SAEs, configure a network information collector (NIC) that takes the distinguished name (DN) of an access as the key and returns the corresponding SAE as the value.

- For SRC implementations that use five or fewer SAEs, you can use directory eventing to identify the SAEs. If you configure this option, SAEs update the addresses of their external interfaces in the directory at a specified time interval. Each update triggers an event that is sent to the enterprise service portal to confirm that the corresponding SAE is available. If the enterprise service portal does not receive the update event within a certain time, the enterprise service portal assumes that the SAE is not available and subsequently does not send any service activation or feedback requests to that SAE. When the SAE becomes available and starts to manage subscribers again, the enterprise service portal sends new requests to that SAE.

Enterprise Service Portals Provided with the SRC Software

We provide several enterprise service portals in the SRC software distribution in the folder *webapp*. Some of the enterprise service portals we provide are intended for demonstration purposes or as a basis for developing a customized enterprise service portal for your SRC implementation. Other enterprise service portals are intended to serve a specific purpose and require little customization. The WAR files for the enterprise service portals contain all required libraries and Web contents.

The following enterprise service portals are available:

- Sample enterprise service portal

- Enterprise Manager Portal

- NAT Address Management Portal

Sample Enterprise Service Portal

The sample enterprise service portal incorporates many of the features that the enterprise service portal API offers. You can use the sample enterprise service portal to demonstrate the functionality available, and you can customize the sample enterprise service portal to create a portal for your own SRC implementation. The source code for the sample enterprise service portal is in its JSP pages; the code was created with the tags in the enterprise portal tag library.

For information about the JSP tags that you can use to customize an enterprise service portal, see the documentation for the enterprise tag library in the SRC software distribution in the folder */SDK/doc/ent/tagDocs* or on the Juniper Networks Web site at

http://www.juniper.net/techpubs/software/management/sdx/api-index.html

Enterprise Manager Portal

Service providers can deploy Enterprise Manager Portal to provision services for enterprise subscribers. IT managers can access the SRC network through this portal and select the services they require. Enterprise Manager Portal is a complete application for which you need to customize only style sheets and icons.

NAT Address Management Portal

Service providers can deploy this enterprise service portal to manage public IP addresses for use with NAT services on JUNOS routing platforms. IT managers make requests about public IP addresses through Enterprise Manager Portal. The service provider responds to these requests through NAT Address Management Portal. This enterprise service portal is a complete application for which you need to customize only style sheets and icons.

When an IT manager makes a request about public IP addresses through Enterprise Manager Portal, Enterprise Manager Portal sends an e-mail to a human administrator or a machine. For small installations or demonstration purposes, a human administrator can manage the public IP addresses; however, for large installations, public IP addresses are managed by machines. NAT Address Manager handles two operations: the supply of new IP addresses and the return of unwanted public IP addresses.

If a human administrator provides the IP addresses, the administrator can access the Address Manager portal by clicking the portal address that is included in the e-mail from Enterprise Manager Portal. The administrator can then use NAT Address Management Portal to make a change to the IT manager's public IP addresses in the directory. The IT manager can view the changes through Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

If you use a machine to manage public IP addresses, you must write an application that allows the machine to handle the e-mails that Enterprise Manager Portal sends. The e-mails contain XML code that NAT Address Management Portal and the machine must interpret. The following sequence of events describes how the machine interacts with the portals.

1. The IT manager requests one or more IP addresses through Enterprise Manager Portal.

2. Enterprise Manager Portal sends an e-mail to the machine that administers IP addresses.

   The subject line of the e-mail contains the URL of NAT Address Management Portal. The body of the e-mail contains an SDXNATStatusRequest message—XML code that contains a request for information about the status of a particular access.

3. The machine forwards the e-mail to the URL in the subject line of the e-mail.

4. The machine extracts the SDXNATStatusRequest message from the e-mail and sends it by means of HTTP to NAT Address Management Portal.

5. NAT Address Management Portal analyzes the SDXNATStatusRequest message and returns an SDXNATStatusResponse message to the machine.

6. The machine analyzes the response and determines the next action, such as providing an IP address for the enterprise.

7. The machine sends the appropriate information in an SDXNATOperationRequest message to NAT Address Management Portal.

8. NAT Address Management Portal updates the directory and returns an SDXNATOperationResponse message to the machine.

   When NAT Address Management Portal updates the directory, the IT manager can view the new status in Enterprise Manager Portal and can use the assigned IP addresses in subscriptions to NAT services.

The XML messages described above contain subordinate elements that depend on whether the IT manager's request is to obtain or return IP addresses. The document type definition (DTD) for the XML messages describes these subordinate elements. You can find the DTD in the SRC software distribution in the folder called *SDK/dtd*.

Enterprise Service Portal Audit Plug-In

The Enterprise Service Portal audit plug-in, also referred to as the enterprise service portal IT Manager audit plug-in or Enterprise Service audit plug-in, defines a callback interface, net.juniper.smgt.ent.plugin.AuditPluginEventListener, which receives events when IT managers complete specified operations, such as subscribing to a service or changing the parameter substitutions of a subscription. The events report the type of operation, the identity of the IT manager, and other attributes.

You can write audit plug-in event listeners by implementing the callback interface. A listener performs tasks such as processing received events and then publishing the events to one or more event handlers, such as a log file, system log, or database. Events are sent after the corresponding operations have been completed. The plug-in processes events, which are sent synchronously, and then returns control to the enterprise service portal. Future events are blocked from being processed until the listener returns the thread.

Network Information Collector with Enterprise Service Portals

You can improve the performance of service activation for an enterprise service portal by implementing the NIC in your network. In this case, the enterprise service portal uses the NIC to locate the SAE managing a particular session. If you do not configure a NIC for your network, the enterprise service portal locates the managing SAE by polling all the SAEs in the network. See *SRC-PE Network Guide, Chapter 9, Locating Subscriber Information with the NIC*.

Service Parameters

Subscribing to and activating services are only part of the functionality available through the enterprise service portal API. An enterprise service portal can also expose the power of service parameters.

An enterprise service is, at its core, a set of policies that affect network traffic when they are applied to the router interfaces associated with some subset of an enterprise's accesses. When these service policies are defined by the service provider, they can contain parameters. For example, a service that provides protection against denial-of-service attacks may limit the traffic on a specific port to a specific percentage of the bandwidth available on a router interface. Both the port and the percentage can be expressed as parameters in the service's network policies.

Service parameters allow for some very powerful functionality. For example, they allow the service provider to define a generic service that can be customized for specific enterprises or for specific sites or accesses within an enterprise. The enterprise customer can perform this customization at any time (even while the service is active) through an enterprise service portal. The enterprise service portal must invoke a method in the enterprise API to provide the value for each parameter.

For an enterprise service portal to detect service parameters configured for fragment services for an aggregate service, the parameters must be defined in the configuration for the aggregate service. See *Chapter 24, Managing Services with Enterprise Manager Portal*.

Substitutions and the Parameter Acquisition Path

Each parameter in a service policy requires that a value be obtained. In the example above, the denial-of-service protection policies have two parameters: port number and bandwidth percentage. Each of those parameters in a service's network policies results in the creation of a variable. Policy configuration specifies the name of a variable.

Each of these variables must have a value assigned to it (unless it already has a default value). The enterprise service portal can obtain that value from the enterprise customer. The enterprise service portal must then call a method in the API to assign that value to the variable. The API will record this value by writing a substitution into an LDAP entry. A substitution is an LDAP entry attribute that, at its simplest, just assigns a value to a variable.

More than one substitution can exist for a given variable. Substitutions for a given variable can exist in any LDAP entry on the acquisition path. The acquisition path is a path through a sequence of LDAP entries. It begins with a most specific entry and ends with a most general entry. When the value for a given variable is specified through substitution attributes in multiple LDAP entries on this path, only the most specific entry's substitution is actually used.

The ordering of the LDAP entries in the acquisition path is always the same. Starting from the most specific, they are the:

1. SSP subscription entry under the access entry (if one exists for the service in question)
2. Access entry
3. SSP subscription entry under the site entry (if one exists for the service in question)
4. Site entry
5. SSP subscription entry under the enterprise entry (if one exists for the service in question)
6. Enterprise entry
7. Relevant localized version of the SSP service entry (if one exists)
8. SSP service entry

The acquisition path allows values assigned to variables at a more general place in the acquisition path to be overridden by values assigned at a more specific place in the acquisition path. This method enables an enterprise to subscribe to a given service, to specify values for that service's parameters at a more general place in the acquisition path, and then to override those values at a more specific level according to the needs of local enterprise IT managers who control a given site or access.

NOTE: Each session of a subscription uses a different acquisition path (because each is associated with a different access). This means that each session of a subscription may end up with different values for a given service parameter. For each session, the enterprise API exposes detailed information about the actual values used for every service parameter.

Power of Substitutions

In addition to assigning values to the variables that are used as service parameters, a substitution can declare that the value it assigns is fixed. When a fixed value is declared, substitutions for the same variable that exist in more specific places in the acquisition path are ignored (that is, the fixed value cannot be overridden). More important, a substitution can specify the value for a variable as an expression that includes other variables. A substitution can also introduce new variables. The new variables are then available for use in other substitutions at any more specific point on the acquisition path. Enterprise service portals that expose these features allow enterprises to define their own way of presenting and managing service parameters. For more detail on service parameters, the acquisition path, and the uses of substitutions, see the see *SRC-PE Services and Policies Guide, Chapter 14, Defining and Acquiring Values for Parameters*.

Substituting Values for Policy Parameters

The value substitution feature of an enterprise service portal gives the enterprise IT manager the ability to customize subscribed services in his or her sphere of control. The enterprise IT manager can be required to provide a set of substitutions that define the values for the parameters of the underlying service policies everywhere the policies are applied. Sample parameter types that might require value substitution include:

- Network—Address/prefix length pairs that denote networks
- Interface—Router interface specifications
- Protocol—Eight-bit unsigned integers enumerating protocols such as IP, TCP, and UDP
- Rate—32-bit unsigned integers used for rate-limit and burst-size calculations

For example, the service provider could offer a service to the enterprise that applies a firewall policy. The firewall policy could screen ingress traffic from a source network and redirect the screened traffic to a specific destination. The enterprise IT manager might want to specify at the time of subscription or subscription activation which source networks are involved. The service provider establishes a general policy template, in this case configuring the destination. The enterprise IT manager modifies the template by means of value substitution for the particular needs of the enterprise, such as providing a range of IP addresses for one or more source networks.

A different service might have an egress rate-limit policy with policy rules to screen egress traffic from the source network, by protocol, or according to a traffic rate limit. Value substitution for the parameters defined in the generic policy template enables the manager to define the policy to match the needs of the enterprise.

Note that parameter names provided to one customer can be renamed by the service provider to suit the needs of another customer. For example, one customer might prefer a parameter named “department” to one named “network” because that name better fits the enterprise hierarchy.

The service provider can specify whether all parameters or only certain ones can be modified in the enterprise service portal by the enterprise IT manager by means of value substitution. Likewise, an IT manager can determine whether subordinate managers have the ability to modify a given service parameter. Parameters for which values cannot be substituted at a given level are said to be fixed at some higher level. For example, in the sample portal, the enterprise service portal populates drop-down lists from which the manager at that level can select values to substitute. If a parameter substitution is fixed at a higher management level, lower-level managers will not see options for substituting for that parameter in the drop-down lists on their instance of the enterprise service portal. See *SRC-PE Services and Policies Guide, Chapter 14, Defining and Acquiring Values for Parameters* for more information.

Managing Subscriptions to Aggregate Services

If an enterprise service portal manages subscriptions to aggregate services, ensure that each parameter defined for a fragment service is also defined in the aggregate service. For information about aggregate services, see *SRC-PE Services and Policies Guide, Chapter 1, Managing Services with the SRC CLI* or *SRC-PE Services and Policies Guide, Chapter 2, Managing Services on a Solaris Platform*.

To review parameter definitions and define parameters used by a fragment service for an aggregate service from SDX Admin:

1. Select the aggregate service to be managed by an enterprise service portal.
2. Click the **Aggregate** tab for the service, and review the parameters listed under Expression and Substitution for each service fragment.
3. Click the **Parameters** tab, and review the list of Substitutions. If a substitution is not listed for one of the parameters referenced on the Aggregate tab, add it.

   The value for each of the parameter substitutions should not be Fixed.

Configuring Your Web Browser to Use an Enterprise Service Portal

Before you can use an enterprise service portal, you must enable your Web browser to:

- Allow cookies from the enterprise service portal.
- (Enterprise Manager Portal and NAT Address Management Portal only) Use JavaScript.

Accessing Enterprise Service Portals

When viewing the enterprise service portals, take care to open only one browser window yourself. The portals automatically open pop-up windows for various operations. If you open more than one browser window yourself, the information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To access an enterprise service portal:

1. Enter the URL of the portal in your Web browser, and press Enter. For example, to access Enterprise Manager Portal, type:

   http://192.0.2.1:8080/entmgr

   The enterprise service portal displays the login page.

2. Select your service provider from the Retailer menu.

3. Enter your username in the Login ID field and your password in the Password field.

   The enterprise service portal displays your Welcome page. On the left of the page is a navigation pane for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation pane.