Oracle® Communications Converged Application Server

Developing Diameter Applications

Release 4.0

August 2008

ORACLE

Oracle Communications Converged Application Server Developing Diameter Applications, Release 4.0

Contents

3. Using the Diameter Rf Interface Application for Offline Charging

4. Using the Diameter Ro Interface Application for Online Charging

CHAPTER 1

Using the Diameter Base Protocol API

The following sections provide an overview of using the Oracle Communications Converged Application Server Diameter Base protocol implementation to create your own Diameter applications:

Overview of Diameter Protocol Support

Diameter is a peer-to-peer protocol that involves delivering attribute-value pairs (AVPs). A Diameter message includes a header and one or more AVPs. The collection of AVPs in each message is determined by the type of Diameter application, and the Diameter protocol also allows for extension by adding new commands and AVPs. Diameter enables multiple peers to negotiate their capabilities with one another, and defines rules for session handling and accounting functions.

Oracle Communications Converged Application Server includes an implementation of the base Diameter protocol that supports the core functionality and accounting features described in RFC 3588. Oracle Communications Converged Application Server uses the base Diameter functionality to implement multiple Diameter applications, including the Sh, Rf, and Ro applications described later in this document.

You can also use the base Diameter protocol to implement additional client and server-side Diameter applications. The base Diameter API provides a simple, Servlet-like programming model that enables you to combine Diameter functionality with SIP or HTTP functionality in a converged application.

The sections that follow provide an overview of the base Diameter protocol packages, classes, and programming model used for developing client and server-side Diameter applications. See also the following sections for information about using the provided Diameter protocol applications in your SIP Servlets:

- "Using the Diameter Sh Interface Application" on page 2-1 describes how to access and manage subscriber profile data using the Diameter Sh application.
- "Using the Diameter Rf Interface Application for Offline Charging" on page 3-1 describes how to issue offline charging requests using the Diameter Rf application.
- "Using the Diameter Ro Interface Application for Online Charging" on page 4-1 describes how to perform online charging using the Diameter Ro application.

Overview of the Diameter API

All classes in the Diameter base protocol API reside in the root `com.bea.wcp.diameter` package. Table 1-1 describes the key classes, interfaces, and exceptions in this package.

Table 1-1 Key Elements of the Diameter Base Protocol API

Category	Element	Description
Diameter Node	Node	A class that represents a Diameter node implementation. A diameter node can represent a client- or server-based Diameter application, as well as a Diameter relay agent.

Table 1-1 Key Elements of the Diameter Base Protocol API

Diameter Applications	Application, ClientApplication	A class that represents a basic Diameter application. ClientApplication extends Application for client-specific features such as specifying destination hosts and realms. All Diameter applications must extend one of these classes to return an application identifier. The classes can also be used directly to create new Diameter sessions.
	ApplicationId	A class that represents the Diameter application ID. This ID is used by the Diameter protocol for routing messages to the appropriate application. The `ApplicationId` corresponds to one of the Auth-Application-Id, Acct-Application-Id, or Vendor-Specific-Application-Id AVPs contained in a Diameter message.
	Session	A class that represents a Diameter session. Applications that perform session-based handling must extend this class to provide application-specific behavior for managing requests and answering messages.
Message Processing	Message, Request, Answer	The Message class is a base class used to represent request and answer message types. Request and Answer extend the base class.
	Command	A class that represents a Diameter command code.
	RAR, RAA	These classes extend the `Request` and `Answer` classes to represent re-authorization messages.
	ResultCode	A class that represents a Diameter result code, and provides constant values for the base Diameter protocol result codes.
AVP Handling	Attribute	A class that provides Diameter attribute information.
	Avp, AvpList	Classes that represent one or more attribute-value pairs in a message. AvpList is also used to represent AVPs contained in a grouped AVP.
	Type	A class that defines the supported AVP datatypes.
Error Handling	DiameterException	The base exception class for Diameter exceptions.
	MessageException	An exception that is raised when an invalid Diameter message is discovered.
	AvpException	An exception that is raised when an invalid AVP is discovered.

Table 1-1 Key Elements of the Diameter Base Protocol API

Supporting Interfaces	Enumerated	An enum value that implements this interface can be used as the value of an AVP of type INTEGER32, INTEGER64, or ENUMERATED.
	SessionListener	An interface that applications can implement to subscribe to messages delivered to a Diameter session.
	MessageFactory	An interface that allows applications to override the default message decoder for received messages, and create new types of `Request` and `Answer` objects. The default decoding process begins by decoding the message header from the message bytes using an instance of `MessageFactory`. This is done so that an early error message can be generated if the message header is invalid. The actual message AVPs are decoded in a separate step by calling `decodeAvps`. AVP values are fully decoded and validated by calling `validate`, which in turn calls `validateAvp` for each partially-decoded AVP in the message.

In addition to these base Diameter classes, accounting-related classes are stored in the `com.bea.wcp.diameter.accounting` package, and credit-control-related classes are stored in `com.bea.wcp.diameter.cc`. See "Using the Diameter Ro Interface Application for Online Charging" on page 4-1 and "Using the Diameter Rf Interface Application for Offline Charging" on page 3-1 for more information about classes in these packages.

Working with Diameter Nodes

A diameter node is represented by the `com.bea.wcp.diameter.Node` class. A Diameter node may host one or more Diameter applications, as configured in the `diameter.xml` file. In order to access a Diameter application, a deployed application (such as a SIP Servlet) must obtain the diameter Node instance and request the application. Listing 1-1 shows the sample code used to access the Rf application.

Listing 1-1 Accessing a Diameter Node and Application

```
ServletContext sc = getServletConfig().getServletContext();
Node node = sc.getAttribute("com.bea.wcp.diameter.Node");
```

```
RfApplication rfApp = (RfApplication)
node.getApplication(Charging.RF_APPLICATION_ID);
```

Diameter Nodes are generally configured and started as part of a Oracle Communications Converged Application Server instance. However, for development and testing purposes, you can also run a Diameter node as a standalone process. To do so:

1. Set the environment for your domain:

   ```
   cd ~/bea/user_projects/domains/diameter/bin
   . ./setDomainEnv.sh
   ```

2. Locate the `diameter.xml` configuration file for the Node you want to start:

   ```
   cd ../config/custom
   ```

3. Start the Diameter node, specifying the `diameter.xml` configuration file to use:

   ```
   java com.bea.wcp.diameter.Node diameter.xml
   ```

Implementing a Diameter Application

All Diameter applications must extend either the base `Application` class or, for client applications, the `ClientApplication` class. The model for creating a Diameter application is similar to that for implementing Servlets in the following ways:

- Diameter applications override the `init()` method for initialization tasks.
- Initialization parameters configured for the application in `diameter.xml` are made available to the application.
- A session factory is used to generate new application sessions.

Diameter applications must also implement the `getId()` method to return the proper application ID. This ID is used to deliver Diameter messages to the correct application.

Applications can optionally implement `rcvRequest()` or `rcvAnswer()` as needed. By default, `rcvRequest()` answers with UNABLE_TO_COMPLY, and `rcvRequest()` drops the Diameter message.

Listing 1-2 shows a simple Diameter client application that does not use sessions.

Listing 1-2 Simple Diameter Application

```
public class TestApplication extends ClientApplication {
```

```
  protected void init() {
    log("Test application initialized.");
  }
  public ApplicationId getId() {
    return ApplicationId.BASE_ACCOUNTING;
  }
  public void rcvRequest(Request req) throws IOException {
    log("Got request: " + req.getHopByHopId());
    req.createAnswer(ResultCode.SUCCESS).send();
  }
}
```

Working with Diameter Sessions

The base Session class represents a Diameter session. If you extend the base Session class, you must implement either `rcvRequest()` or `rcvAnswer()`, and may implement both methods.

The base Application class is used to generate new Session objects. After a session is created, all session-related messages are delivered directly to the session object. The Oracle Communications Converged Application Server container automatically generates the session ID and encodes the ID in each message. Session attributes are supported much in the same fashion as attributes in `SipApplicationSession`.

Listing 1-3 shows a simple Diameter session implementation.

Listing 1-3 Simple Diameter Session

```
public class TestSession extends Session {
  public TestSession(TestApplication app) {
    super(app);
  }
  public void rcvRequest(Request req) throws IOException {
    getApplication().log("rcvReuest: " + req.getHopByHopId());
```

```
    req.createAnswer(ResultCode.SUCCESS).send();
  }
}
```

To use the sample session class, the `TestApplication` in `Listing 1-2` would need to add a factory method:

```
public class TestApplication extends Application {
  ...
  public TestSession createSession() {
    return new TestSession(this);
  }
}
```

`TestSession` could then be used to create new requests as follows:

```
TestSession session = testApp.createSession();
Request req = session.creatRequest();
req.sent();
```

The answer is delivered directly to the Session object.

Working with Diameter Messages

The base `Message` class is used for both Request and Answer message types. A Message always includes an application ID, and optionally includes a session ID. By default, messages are handled in the following manner:

1. The message bytes are parsed.
2. The application and session ID values are determined.
3. The message is delivered to a matching session or application using the following rules:
   a. If the Session-Id AVP is present, the associated Session is located and the session's `rcvMessage()` method is called.
   b. If there is no Session-Id AVP present, or if the session cannot be located, the Diameter application's `rcvMessage()` method is called

c. If the application cannot be located, an UNABLE_TO_DELIVER response is generated.

The message type is determined from the Diameter command code. Certain special message types, such as RAR, RAA, ACR, ACA, CCR, and CCA, have getter and setter methods in the `Message` object for convenience.

Sending Request Messages

Either a `Session` or `Application` can originate and receive request messages. Requests are generated using the `createRequest()` method. You must supply a command code for the new request message. For routing purposes, the destination host or destination realm AVPs are also generally set by the originating session or application.

Requests can be sent asynchronously using the `send()` method, or synchronously using the blocking `sendAndWait()` method. Answers for requests that were sent asynchronously are delivered to the originating session or application. You can specify a request timeout value when sending the message, or can use the global `request-timeout` configuration element in `diameter.xml`. An UNABLE_TO_DELIVER result code is generated if the timeout value is reached before an answer is delivered. `getResultCode()` on the resulting Answer returns the result code.

Sending Answer Messages

New answer messages are generated from the `Request` object, using `createAnswer()`. All generated answers should specify a ResultCode and an optional Error-Message AVP value. The `ResultCode` class contains pre-defined result codes that can be used.

Answers are delivered using the `send()` method, which is always asynchronous (non-blocking).

Received answers can be obtained using `Request.getAnswer()`. After receiving an answer, you can use `getSession()` to obtain the relevant session ID and `getResultCode()` to determine the result. You can also use `Answer.getRequest()` to obtain the original request message.

Creating New Command Codes

The `Command` class represents pre-defined commands codes for the Diameter base protocol, and can be used to create new command codes. Command codes share a common name space based on the code itself.

The `define()` method enables you to define codes, as in:

```
static final Command TCA = Command.define(1234, “Test-Request”, true, true);
```

The `define()` method registers a new Command, or returns a previous command definition if one was already defined. Commands can be compared using the reference equality operator (==).

Working with AVPs

The `Avp` class represents a Diameter attribute-value pair. You can create new AVPs with an attribute value in the following way:

```
Avp avp = new Avp(Attribute.ERROR_MESSAGE, “Bad request”);
```

You can also specify the attribute name directly, as in:

```
Avp avp = new Avp(“Error-Message”, “Bad request”);
```

The value that you specify must be valid for the specified attribute type.

To create a grouped AVP, use the `AvpList` class, as in:

```
AvpList avps = new AvpList();
avps.add(new Avp(“Event-Timestamp”, 1234));
avps.add(new Avp(“Vendor-Id”, 1111));
```

Creating New Attributes

The Attribute class represents an AVP attribute, and includes the AVP code, name, flags, optional vendor ID, and type of attribute. The class also maintains a registry of defined attributes. All attributes share a common namespace based on the attribute code and vendor ID.

The `define()` method enables you to define new attributes, as in:

```
static final Attribute TEST = Attribute.define(1234, “Test-Attribute”, 0,
Attribute.FLAG_MANDATORY, Type.INTEGER32);
```

Table 1-2 lists the available attribute types and describes how they are mapped to Java types.

The `define()` method registers a new attribute, or returns a previous definition if one was already defined. Attributes can be compared using the reference equality operator (==).

Table 1-2 Attribute Types

Diameter Type	Type Constant	Java Type
Integer32	Type.INTEGER32	Integer
Integer64	Type.INTEGER64	Long

Table 1-2 Attribute Types

Diameter Type	Type Constant	Java Type
Float32	Type.FLOAT32	Float
OctetString	Type.BYTES	ByteBuffer (read-only)
UTF8String	Type.STRING	String
Address	Type.ADDRESS	InetAddress
Grouped	Type.GROUPED	AvpList

Creating Converged Diameter and SIP Applications

The Diameter API enables you to create converged applications that utilize both SIP and Diameter functionality. A SIP Servlet can access an available Diameter application via the Diameter Node, as shown in Listing 1-4.

Listing 1-4 Accessing the Rf Application from a SIP Servlet

```
ServletContext sc = getServletConfig().getServletContext();

Node node = (Node) sc.getAttribute("com.bea.wcp.diameter.Node");

RfApplication rfApp = (RfApplication)
node.getApplication(Charging.RF_APPLICATION_ID);
```

Oracle Communications Converged Application Server automatically links the Diameter session to the currently-active call state by encoding the Call-id into the Diameter session ID. When a Diameter message is received, the container automatically retrieves the associated call state and locates the Diameter session. A Diameter session is are serializable, so you can store the session as an attribute in a the `SipApplicationSession` object, or vice versa.

Converged applications can use the Diameter `SessionListener` interface to receive notification when a Diameter message is received by the session. The `SessionListener` interface defines a single method, `rcvMessage()`. `Listing 1-5` shows an example of how to implement the method.

Listing 1-5 Implementing SessionListener

```
Session session = app.createSession();
session.setListener(new SessionListener() {
  public void rcvMessage(Message msg) {
    if (msg.isRequest()) System.out.println(“Got request!”);
  }
});
```

Note: The `SessionListener` implementation must be serializable for distributed applications.

CHAPTER 2

Using the Diameter Sh Interface Application

The following sections describe how to use the Diameter Sh interface application, based on the Oracle Communications Converged Application Server Diameter protocol implementation, in your own applications:

Overview of Profile Service API and Sh Interface Support

The IMS specification defines the Sh interface as the method of communication between the Application Server (AS) function and the Home Subscriber Server (HSS), or between multiple IMS Application Servers. The AS uses the Sh interface in two basic ways:

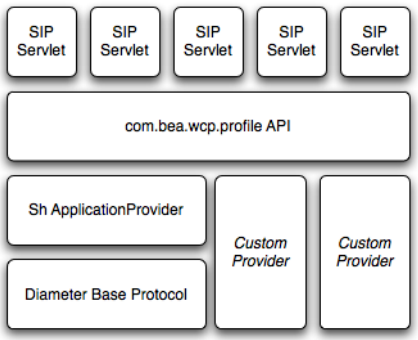
- To query or update a user's data stored on the HSS
- To subscribe to and receive notifications when a user's data changes on the HSS

The user data available to an AS may be defined by a service running on the AS (*repository data*), or it may be a subset of the user's IMS profile data hosted on the HSS. The Sh interface

specification, 3GPP TS 29.328, defines the IMS profile data that can be queried and updated via Sh. All user data accessible via the Sh interface is presented as an XML document with the schema defined in 3GPP TS 29.328.

The IMS Sh interface is implemented as a provider to the base Diameter protocol support in Oracle Communications Converged Application Server. The provider transparently generates and responds to the Diameter command codes defined in the Sh application specification. A higher-level Profile Service API enables SIP Servlets to manage user profile data as an XML document using XML Document Object Model (DOM). Subscriptions and notifications for changed profile data are managed by implementing a profile listener interface in a SIP Servlet.

Figure 2-1 Profile Service API and Sh Provider Implementation



Oracle Communications Converged Application Server includes a provider for the Diameter Sh interface. Providers to support additional interfaces defined in the IMS specification may be provided in future releases. Applications using the profile service API will be able to use additional providers as they are made available.

Enabling the Sh Interface Provider

See Configuring Diameter Sh Client Nodes and Relay Agents in *Configuring Network Resources* for full instructions on setting up Diameter support.

Overview of the Profile Service API

Oracle Communications Converged Application Server provides a simple profile service API that SIP Servlets can use to query or modify subscriber profile data, or to manage subscriptions for receiving notifications about changed profile data. Using the API, a SIP Servlet explicitly requests user profile documents via the Sh provider application. The provider returns an XML document, and the Servlet can then use standard DOM techniques to read or modify profile data in the local document. Updates to the local document are applied to the HSS after a "put" operation.

Creating a Document Key for Application-Managed Profile Data

Servlets that manage profile data can explicitly obtain an Sh XML document from a factory using a key, and then work with the document using DOM.

The document selector key identifies the XML document to be retrieved by a Diameter interface, and uses the format `protocol://uri/reference_type[/access_key]`.

The `protocol` portion of the selector identifies the Diameter interface provider to use for retrieving the document. Sh XML documents require the `sh://` protocol designation.

With Sh document selectors, the next element, `uri`, generally corresponds to the User-Identity or Public-Identity of the user whose profile data is being retrieved. If you are requesting an Sh data reference of type LocationInformation or UserState, the URI value can be the User-Identity or MSISDN for the user.

Table 2-1 summarizes the possible URI values that can be supplied depending on the Sh data reference you are requesting. 3GPP TS 29.328 describes the possible data references and associated reference types in more detail.

Table 2-1 Possible URI Values for Sh Data References

Sh Data Reference Number	Data Reference Type	Possible URI Value in Document Selector
0	RepositoryData	User-Identity or Public-Identity
10	IMSPublicIdentity	
11	IMSUserState	
12	S-CSCFName	
13	InitialFilterCriteria	
14	LocationInformation	User-Identity or MSISDN
15	UserState	
17	Charging information	User-Identity or Public-Identity
17	MSISDN	

The final element of the document selector, *`reference_type`*, specifies the data reference type being requested. For some data reference requests, only the *`uri`* and *`reference_type`* are required. Other Sh requests use an access key, which requires a third element in the document selector corresponding to the value of the Attribute-Value Pair (AVP) defined in the key.

Table 2-2 summarizes the required document selector elements for each type of Sh data reference request.

Table 2-2 Summary of Document Selector Elements for Sh Data Reference Requests

Data Reference Type	Required Document Selector Elements	Example Document Selector
RepositoryData	sh://uri/reference_type/Service-Indication	sh://sip:user@oracle.com/RepositoryData/Call Screening/
IMSPublicIdentity	sh://uri/reference_type/[*Identity-Set*] where *Identity-Set* is one of: • All-Identities • Registered-Identities • Implicit-Identities	sh://sip:user@oracle.com/IMSPublicIdentity/Registered-Identities
IMSUserState	sh://uri/reference_type	sh://sip:user@oracle.com/IMSUserState/
S-CSCFName	sh://uri/reference_type	sh://sip:user@oracle.com/S-CSCFName/
InitialFilterCriteria	sh://uri/reference_type/Server-Name	sh://sip:user@oracle.com/InitialFilterCriteria/www.oracle.com/
LocationInformation	sh://uri/reference_type/(CS-Domain | PS-Domain)	sh://sip:user@oracle.com/LocationInformation/CS-Domain/
UserState	sh://uri/reference_type/(CS-Domain | PS-Domain)	sh://sip:user@oracle.com/UserState/PS-Domain/
Charging information	sh://uri/reference_type	sh://sip:user@oracle.com/Charging information/
MSISDN	sh://uri/reference_type	sh://sip:user@oracle.com/MSISDN/

Using a Constructed Document Key to Manage Profile Data

Oracle Communications Converged Application Server provides a helper class, `com.bea.wcp.profile.ProfileService`, to help you easily retrieve a profile data document. The `getDocument()` method takes a constructed document key, and returns a read-only

`org.w3c.dom.Document` object. To modify the document, you make and edit a copy, then send the modified document and key as arguments to the `putDocument()` method.

Note: If Diameter Sh client node services are not available on the Oracle Communications Converged Application Server instance when `getDocument()` the profile service throws a "No registered provider for protocol" exception.

Oracle Communications Converged Application Server caches the documents returned from the profile service for the duration of the service method invocation (for example, when a `doRequest()` method is invoked). If the service method requests the same profile document multiple times, the subsequent requests are served from the cache rather than by re-querying the HSS.

Listing 2-1 shows a sample SIP Servlet that obtains and modifies profile data.

Listing 2-1 Sample Servlet Using ProfileService to Retrieve and Write User Profile Data

```
package demo;
import com.bea.wcp.profile.*;
import javax.servlet.sip.SipServletRequest;
import javax.servlet.sip.SipServlet;
import org.w3c.dom.Document;
import java.io.IOException;
public class MyServlet extends SipServlet {
      private ProfileService psvc;
      public void init() {
        psvc = (ProfileService)
getServletContext().getAttribute(ProfileService.PROFILE_SERVICE);
      }
      protected void doInvite(SipServletRequest req) throws IOException {
        String docSel = "sh://" + req.getTo() + "/IMSUserState/";
        // Obtain and change a profile document.
        Document doc = psvc.getDocument(docSel); // Document is read only.
```

```
        Document docCopy = (Document) doc.cloneNode(true);
        // Modify the copy using DOM.
        psvc.putDocument(docSel, docCopy); // Apply the changes.
      }
}
```

Monitoring Profile Data with ProfileListener

The IMS Sh interface enables applications to receive automatic notifications when a subscriber's profile data changes. Oracle Communications Converged Application Server provides an easy-to-use API for managing profile data subscriptions. A SIP Servlet registers to receive notifications by implementing the `com.bea.wcp.profile.ProfileListener` interface, which consists of a single `update` method that is automatically invoked when a change occurs to profile to which the Servlet is subscribed. Notifications are not sent if that same Servlet modifies the profile information (for example, if a user modifies their own profile data).

Note: In a replicated environment, Diameter relay nodes always attempt to push notifications directly to the engine tier server that subscribed for profile updates. If that engine tier server is unavailable, another server in the engine tier cluster is chosen to receive the notification. This model succeeds because session information is stored in the SIP data tier, rather than the engine tier.

Prerequisites for Listener Implementations

In order to receive a call back for subscribed profile data, a SIP Servlet must do the following:

- Implement `com.bea.wcp.profile.ProfileListener`.
- Create one or more subscriptions using the `subscribe` method in the `com.bea.wcp.profile.ProfileService` helper class.
- Register itself as a listener using the `listener` element in `sip.xml`.

"Implementing ProfileListener" on page 2-8 describes how to implement `ProfileListener` and use the `susbscribe` method. In addition to having a valid listener implementation, the Servlet must declare itself as a listener in the `sip.xml` deployment descriptor file. For example, it must add a `listener` element declaration similar to:

```
<listener>
   <lisener-class>com.mycompany.MyLisenerServlet</listener-class>
```

```
</listener>
```

Implementing ProfileListener

Actual subscriptions are managed using the `subscribe` method of the `com.bea.wcp.profile.ProfileService` helper class. The subscribe method requires that you supply the current `SipApplicationSession` and the key for the profile data document you want to monitor. See "Creating a Document Key for Application-Managed Profile Data" on page 2-3.

Applications can cancel subscriptions by calling `ProfileSubscription.cancel()`. Also, pending subscriptions for an application are automatically cancelled if the application session is terminated.

Listing 2-2 shows sample code for a Servlet that implements the `ProfileListener` interface.

Listing 2-2 Sample Servlet Implementing ProfileListener Interface

```
package demo;
    import com.bea.wcp.profile.*;
    import javax.servlet.sip.SipServletRequest;
    import javax.servlet.sip.SipServlet;
    import org.w3c.dom.Document;
    import java.io.IOException;
    public class MyServlet extends SipServlet implements ProfileListener {
      private ProfileService psvc;
      public void init() {
        psvc = (ProfileService)
getServletContext().getAttribute(ProfileService.PROFILE_SERVICE);
      }
      protected void doInvite(SipServletRequest req) throws IOException {
        String docSel = "sh://" + req.getTo() + "/IMSUserState/";
        // Subscribe to profile data.
        psvc.subscribe(req.getApplicationSession(), docSel, null);
```

```
}
      public void update(ProfileSubscription ps, Document document) {
        System.out.println("IMSUserState updated: " +
ps.getDocumentSelector());
      }
    }
```

CHAPTER 3

Using the Diameter Rf Interface Application for Offline Charging

The following sections describe how to use the Diameter Rf interface application, based on the Oracle Communications Converged Application Server Diameter protocol implementation, in your own applications:

Overview of Rf Interface Support

Offline charging is used for network services that are paid for periodically. For example, a user may have a subscription for voice calls that is paid monthly. The Rf protocol allows an IMS Charging Trigger Function (CTF) to issue offline charging events to a Charging Data Function (CDF). The charging events can either be one-time events or may be session-based.

Oracle Communications Converged Application Server provides a Diameter Offline Charging Application that can be used by deployment application to generate charging events based on the Rf protocol. The offline charging application uses the base Diameter protocol implementation, and allows any application deployed on Oracle Communications Converged Application Server to act as CTF to a configured CDF.

For basic information about offline charging, see RFC 3588: Diameter Base Protocol. For more information about the Rf protocol, see 3GPP TS 32.299.

Understanding Offline Charging Events

For both event and session based charging, the CTF implements the accounting state machine described in RFC 3588. The server (CDF) implements the accounting state machine “SERVER, STATELESS ACCOUNTING” as specified in RFC 3588.

The reporting of offline charging events to the CDF is managed through the Diameter Accounting Request (ACR) message. Rf supports the ACR event types described in Table 3-1.

Table 3-1 Rf ACR Event Types

Request	Description
START	Starts an accounting session.
INTERIM	Updates an accounting session.
STOP	Stops an accounting session
EVENT	Indicates a one-time accounting event.

The START, INTERIM, and STOP event types are used for session-based accounting. The EVENT type is used for event based accounting, or to indicate a failed attempt to establish a session.

Event-Based Charging ¶

Event-based charging events are reported through the ACR EVENT message. Listing 3-1 shows the basic message flow.

Listing 3-1 Message Flow for Event-Based Charging

```
CTF (WLSS)           CDF (Server)
    |                     |
    | --- ACR (EVENT) --> |
    |                     |
    |                (Process accounting request)
    |                     |
    | <-- ACA (EVENT) --- |
```

```
    |                    |
```

Session-Based Charging ¶

Session-based charging uses the ACR START, INTERIM, and STOP requests to report usage to the CDF. During a session, the CTF may report multiple ACR INTERIM requests depending on the session lifecycle. Listing 3-2 shows the basic message flow

Listing 3-2 Message Flow for Session-Based Charging

```
CTF (WLSS)            CDF (Server)
    |                      |
    | --- ACR (START) ----> |
    |                      |
    |                 (Open CDR)
    |                      |
    | <-- ACA (START) ----- |
    |                      |
   ...                    ...
    | --- ACR (INTERIM) --> |
    |                      |
    |                 (Update CDR)
    |                      |
    | <-- ACA (INTERIM) --- |
   ...                    ...
    | --- ACR (STOP) -----> |
    |                      |
    |                 (Close CDR)
    |                      |
```

```
              | <-- ACA (STOP) ------ |
              |                       |
```

Here, ACA START is sent a receipt of a service request by Oracle Communications Converged Application Server. ACA INTERIM is typically sent upon expiration of the AII timer. ACA STOP is issued upon request for service termination by Oracle Communications Converged Application Server.

Configuring the Rf Application

The `RfApplication` is packaged as a Diameter application similar to the Sh application used for managing profile data. The Rf Diameter application can be configured and enabled by editing the Diameter configuration file located in *`DOMAIN_ROOT`*`/config/custom/diameter.xml`, or by using the Diameter console extension. Additionally, configuration of both the CDF realm and host can be specified using the cdf.realm and cdf.host initialization parameters to the Diameter Rf application.

Listing 3-3 shows a sample excerpt from `diameter.xml` that enables Rf with a CDF realm of "oracle.com" and host "cdf.oracle.com:"

Listing 3-3 Sample Rf Application Configuration (diameter.xml)

```
<application>
  <application-id>3</application-id>
  <accounting>true</accounting>
  <class-name>com.bea.wcp.diameter.charging.RfApplication</class-name>
  <param>
    <name>cdf.realm</name>
    <value>oracle.com</value>
  </param>
  <param>
    <name>cdf.host</name>
    <value>cdf.oracle.com</value>
  </param>
```

```
</application>
```

Because the `RfApplication` uses the Diameter base accounting messages, its Diameter application id is 3 and there is no vendor ID.

Using the Offline Charging API

Oracle Communications Converged Application Server provides an offline charging API to enable any deployed application to act as a CTF and issue offline charging events. This API supports both event-based and session-based charging events.

The classes in package `com.bea.wcp.diameter.accounting` provide general support for Diameter accounting messages and sessions. Table 3-1 summarizes the classes.

Table 3-2 Diameter Accounting Classes

Class	Description
ACR	An Accounting-Request message.
ACA	An Accounting-Answer message.
ClientSession	A Client-based accounting session.
RecordType	Accounting record type constants.

In addition, classes in package `com.bea.wcp.diameter.charging` support the Rf application specifically. Table 3-1 summarizes the classes.

Table 3-3 Diameter Rf Application Support Classes

Charging	Common definitions for 3GPP charging functions
RfApplication	Offline charging application
RfSession	Offline charging session

The `RfApplication` class can be used to directly send ACR requests for event-based charging. The application also has the option of directly modifying the ACR request before it is sent out. This is necessary in order for an application to add any custom AVPs to the request.

In particular, an application should set the Service-Information AVP it carries the service-specific parameters for the CDF. The Service-Information AVP of the ACR request is used to send the application-specific charging service information from the CTF (WLSS) to the CDF (Charging

Server). This is a grouped AVP whose value will depend on the application and its charging function. The Offline Charging API allows the application to set this information on the request before it is sent out.

For session-based accounting, the `RfApplication` class can also be used to create new accounting sessions for generating session-based charging events. Each accounting session is represented by an instance of `RfSession`, which encapsulates the accounting state machine for the session.

Accessing the Rf Application

If the Rf application is deployed, then applications deployed on Oracle Communications Converged Application Server can obtain an instance of the application from the Diameter node (`com.bea.wcp.diameter.Node` class). Listing 3-4 shows the sample Servlet code used to obtain the Diameter `Node` and access the Rf application.

Listing 3-4 Accessing the Rf Application

```
ServletContext sc = getServletConfig().getServletContext();

Node node = sc.getAttribute("com.bea.wcp.diameter.Node");

RfApplication rfApp = (RfApplication)
node.getApplication(Charging.RF_APPLICATION_ID);
```

Applications can safely use a single instance of `RfApplication` to issue offline charging requests concurrently, in multiple threads. Each instance of `RfSession` actually holds the per-session state unique to each call.

Implementing Session-Based Charging

For session-based charging requests, an application first uses the `RfApplication` to create an instance of `RfSession`. The application can then use the session object to create one or more charging requests.

The first charging request must be an ACR START request, followed by zero or more ACR INTERIM requests. The session ends with an ACR STOP request. Upon receipt of the corresponding ACA STOP message, the `RfApplication` automatically terminates the `RfSession`.

Listing 3-5 shows the sample code used to start a new session-based accounting session.

Listing 3-5 Starting a Session-Based Account Session

```
RfSession session = rfApp.createSession();
sipRequest.getApplicationSession().setAttribute("RfSession", session);
ACR acr = session.createACR(RecordType.START);
acr.addAvp(Charging.SERVICE_INFORMATION, ...);
ACA aca = acr.sendAndWait(1000);
if (!aca.getResultCode().isSuccess()) {
  ... error ...
}
```

In Listing 3-5, the `RfSession` is stored as a SIP application session attribute so that it can be used to send additional accounting requests as the call progresses. Listing 3-6 shows how to send an INTERIM request.

Listing 3-6 Sending an INTERIM request

```
RfSession session = (RfSession)
req.getApplicationSession().getAttribute("RfSession");
ACR acr = session.createACR(RecordType.INTERIM);
ACA aca = acr.sendAndWait(1000);
if (!aca.getResultCode().isSuccess()) {
  ... error ...
}
```

An application may want to send one or more ACR INTERIM requests while a call is in progress. The frequency of ACR INTERIM requests is usually based on the Acct-Interim-Interval AVP value in the ACA START message sent by the CDF. For this reason, an application timer should be used to send ACR INTERIM requests at the requested interval. See 3GPP TS 32.299 for more details about interim requests.

Sending Asynchronous Requests

Applications will generally use the synchronous `sendAndWait()` method. However, if latency is critical, an asynchronous API is provided wherein the application Servlet is asynchronously notified when an answer message is received from the CDF. To use the asynchronous API, an application first registers an instance of `SessionListener` in order to asynchronously receive messages delivered to the session, as shown in Listing 3-7

Listing 3-7 Registering a SessionListener

```
RfSession session = rfApp.createSession();
session.setAttribute("SAS", sipReq.getApplicationSession());
session.setListener(this);
```

Attributes can be stored in an `RfSession` instance similar to the way SIP application session attributes are stored. In the above example, the associated SIP application was stored as an `RfSession` so that it is available to the listener callback.

When a Diameter request or answer message is received from the CDF, the application Servlet is notified by calling the `rcvMessage(Message msg)` method. The associated SIP application session can then be retrieved from the `RfSession` if it was stored as a session attribute, as shown in Listing 3-8.

Listing 3-8 Retrieving the RfSession after a Notification

```
public void rcvMessage(Message msg) {
  if (msg.getCommand() != Command.ACA) {
    if (msg.isRequest()) {
      ((Request) msg).createAnswer(ResultCode.UNABLE_TO_COMPLY,
"Unexpected request").send();
    }
    return;
  }
  ACA aca = (ACA) msg;
```

```
    RfSession session = (RfSession) aca.getSession();
    SipApplicationSession appSession = (SipApplicationSession)
session.getAttribute("SAS");
    ...
  }
```

Specifying the Session Expiration

The Acct-Interim-Interval (AII) timer value is used to indicate the expiration time of an Rf accounting session. It is specified when ACR START is sent to the CDF to initiate the accounting session. The CDF responds with its own AII value, which must be used by the CTF to start a timer upon whose expiration an ACR INTERIM message must be sent. This INTERIM message informs the CDF that the session is still in use. Otherwise, the CDF terminates the session automatically.

It is the application's responsibility to send ACR INTERIM messages, because these are used to send updated Service-Information data to the CDF. Oracle recommends creating a ServletTimer that is set to expire according to the AII value. When the timer expires, the application should send an ACR INTERIM message with the updated service information data.

Implementing Event-Based Charging

For an event-based charging request, the charging request is a one-time event and the session is automatically terminated upon receipt of the corresponding EVENT ACA message. The `sendAndWait(long timeout)` method can be used to synchronously send the EVENT request and block the thread until a response has been received from the CDF. Listing 3-9 shows an example that uses an `RfSession` for sending an event-based charging request.

Listing 3-9 Event-Based Charging Using RfSession

```
RfSession session = rfApp.createSession();
ACR acr = session.createACR(RecordType.EVENT);
acr.addAvp(Charging.SERVICE_INFORMATION, ...);
ACA aca = acr.sendAndWait(1000);
if (!aca.getResultCode().isSuccess()) {
  ... send error response ...
```

```
}
```

For convenience, it is also possible send event-based charging requests using the `RfApplication` directly, as shown in Listing 3-10.

Listing 3-10 Event-Based Charging Using RfApplication

```
ACR acr = rfApp.createEventACR();
acr.addAvp(Charging.SERVICE_INFORMATION, ...);
ACA aca = acr.sendAndWait(1000);
```

Internally, the `RfApplication` creates an instance of `RfSession` associated with the ACR request, so this method is equivalent to creating the session explicitly.

For both session and event based accounting, the `RfSession` class automatically handles creating session IDs, as well as updating the Accounting-Record-Number AVP used to sequence messages within the same accounting session.

In the above cases the applications waits for up to 1000 ms to receive an answer from the CDF. If no answer is received within that time, the Diameter core delivers an UNABLE_TO_COMPLY error response to the application, and cancels the request. If no timeout is specified with `sendAndWait()`, then the default request timeout of 30 seconds is used. This default value can be configured using the Diameter console extension.

Using the Accounting Session State ¶

The accounting session state for offline charging is serializable, so it can be stored as a SIP application session attribute. Because the client APIs are synchronous, it is not necessary to maintain any state for the accounting session once the Servlet has finished handling the call.

For event-based charging events it is not necessary for the application to maintain any accounting session state because it is only used internally, and is disposed once the ACA response has been received.

CHAPTER 4

Using the Diameter Ro Interface Application for Online Charging

The following sections describe how to use the Diameter Rf interface application, based on the Oracle Communications Converged Application Server Diameter protocol implementation, in your own applications:

Overview of Ro Interface Support

Online charging, also known as credit-based charging, is used to charge prepaid services. A typical example of a prepaid service is a calling card purchased for voice or video. The Ro protocol allows a Charging Trigger Function (CTF) to issue charging events to an Online Charging Function (OCF). The charging events can be immediate, event-based, or session-based.

Oracle Communications Converged Application Server provides a Diameter Online Charging Application that deployed applications can use to generate charging events based on the Ro protocol. This enables deployed applications to act as CTF to a configured OCF. The Diameter Online Charging Application uses the base Diameter protocol that underpins both the Rf and Sh applications.

The Diameter Online Charging Application is based on IETF RFC 4006: Diameter Credit Control Application. However, the application supports only a subset of the RFC 4006 required for compliance with 3GPP TS 32.299: Telecommunication management; Charging management; Diameter charging applications. Specifically, the Oracle Communications Converged Application Server Diameter Online Charging Application provides no direct support for service-specific Attribute-Value Pairs (AVPs), but the API that is provided is flexible enough to allow applications to include custom service-specific AVPs in any credit control request.

Understanding Credit Authorization Models

RFC 4006 defines two basic types of credit authorization models:

- Credit authorization with unit reservation, and
- Credit authorization with direct debiting.

Credit authorization with unit reservation can be performed with either event-based or session-based charging events. Credit authorization with direct debiting uses immediate charging events. In both models, the CTF requests credit authorization from the OCF prior to delivering services to the end user. In both models

The sections that follow describe each model in more detail.

Credit Authorization with Unit Determination

RFC 4006 defines both Event Charging with Unit Reservation (ECUR) and Session Charging with Unit Reservation (SCUR). Both charging events are session-based, and require multiple transactions between the CTF and OCF. ECUR begins with an interrogation to reserve units before delivering services, followed by an additional interrogation to report the actual used units to the OCF upon service termination. With SCUR, it is also possible to include one or more intermediate interrogations for the CTF in order to report currently-used units, and to reserve additional units if required. In both cases, the session state is maintained in both the CTF and OCF.

For both ECUR and SCUR, the online charging client implements the “CLIENT, SESSION BASED” state machine described in RFC 4006.

Credit Authorization with Direct Debiting

For direct debiting, Immediate Event Charging (IEC) is used. With IEC, a single transaction is created where the OCF deducts a specific amount from the user's account immediately after completing the credit authorization. After receiving the authorization, the CTF delivers services. This form of credit authorization is a one-time event in which no session state is maintained.

With IEC, the online charging client implements the “CLIENT, EVENT BASED” state machine described in IETF RFC 4006.

Determining Units and Rating

Unit determination refers to calculating the number of non-monetary units (service units, time, events) that can be assigned prior to delivering services. Unit rating refers to determining a price based on the non-monetary units calculated by the unit determination function.

It is possible for either the OCF or the CTF to handle unit determination and unit rating. The decision lies with the client application, which controls the selection of AVPs in the credit control request sent to the OCF.

Configuring the Ro Application

The `RoApplication` is packaged as a Diameter application similar to the Sh application used for managing profile data. The Ro Diameter application can be configured and enabled by editing the Diameter configuration file located in *`DOMAIN_ROOT`*`/config/custom/diameter.xml`, or by using the Diameter console extension.

The application init parameter `ocs.host` specifies the host identity of the OCF. The OCF host must also be configured in the peer table as part of the global Diameter configuration. Alternately, the init parameter `ocs.realm` can be used to specify more than one OCF host using realm-based routing. The corresponding realm definition must also exist in the global Diameter configuration.

Listing 4-1 shows a sample excerpt from `diameter.xml` that enables Ro with an OCF host name of “myocs.oracle.com.”

Listing 4-1 Sample Ro Application Configuration (diameter.xml)

```
<application>
  <application-id>4</application-id>
  <class-name>com.bea.wcp.diameter.charging.RoApplication</class-name>
  <param>
    <name>ocs.host</name>
    <value>myocs.oracle.com</value>
  </param>
</application>
```

Because the `RoApplication` is based on the Diameter Credit Control Application, its Diameter application id is 4.

Overview of the Online Charging API

Oracle Communications Converged Application Server provides an online charging API to enable any deployed application to act as a CTF and issue online charging events to an OCS via the Ro protocol. All online charging requests use the Diameter Credit-Control-Request (CCR) message. The CC-Request-Type AVP is used to indicate the type of charging used. In the charging API, the CC-Request-Type is represented by the `RequestType` class in package `com.bea.wcp.diameter.cc`. Table 4-1 shows the request types associated with different credit authorization models.

Table 4-1 Credit Control Request Types

Type	Description	RequestType Field in com.bea.wcp.diameter.cc.RequestType
IEC	Immediate Event Charging	`EVENT_REQUEST`
ECUR	Event Charging with Unit Reservation	`INITIAL` or `TERMINATION_REQUEST`
SCUR	Session Charging with Unit Reservation	`INITIAL`, `UPDATE`, or `TERMINATION_REQUEST`

For ECUR and SCUR, units are reserved prior to service delivery and committed upon service completion. Units are reserved with `INITIAL_REQUEST` and committed with a `TERMINATION_REQUEST`. For SCUR, units can also be updated with `UPDATE_REQUEST`.

The base diameter package, `com.bea.wcp.diameter`, contains classes to support the re-authorization requests used in Ro. The `com.bea.wcp.diameter.cc` package contains classes to support credit-control applications, including Ro applications. `com.bea.wcp.diameter.charging` directly supports the Ro credit-control application. Listing 4-2 summarizes the classes of interest to Ro credit-control.

Table 4-2 Summary of Ro Classes

Class	Description	Package
`Charging`	Constant definitions	`com.bea.wcp.diameter.charging`
`RoApplication`	Online charging application	`com.bea.wcp.diameter.charging`
`RoSession`	Online charging session	`com.bea.wcp.diameter.charging`
`CCR`	Credit Control Request	`com.bea.wcp.diameter.cc`
`CCA`	Credit Control Answer	`com.bea.wcp.diameter.cc`
`ClientSession`	Credit control client session	`com.bea.wcp.diameter.cc`
`RequestType`	Credit-control request type	`com.bea.wcp.diameter.cc`
`RAR`	Re-Auth-Request message	`com.bea.wcp.diameter`
`RAA`	Re-Auth-Answer message	`com.bea.wcp.diameter`

Accessing the Ro Application

If the Ro application is deployed, then applications deployed on Oracle Communications Converged Application Server can obtain an instance of the application from the Diameter node (`com.bea.wcp.diameter.Node` class). Listing 4-2 shows the sample Servlet code used to obtain the Diameter `Node` and access the Ro application.

Listing 4-2 Accessing the Ro Application

```
private RoApplication roApp;
```

```
void init(ServletConfig conf) {
    ServletContext ctx = conf.getServletContext();
    Node node = (Node) ctx.getParameter("com.bea.wcp.diameter.Node");
    roApp = node.getApplication(Charging.RO_APPLICATION_ID);
  }
```

This code example would make `RoApplication` available to the Servlet as an instance variable. The instance of `RoApplication` is safe for use by multiple concurrent threads.

Implementing Session-Based Charging

The `RoApplication` can be used to create new sessions for session-based credit authorization. The `RoSession` class implements the appropriate state machine depending on the credit control type, either ECUR (Event-Based Charging with Unit Reservation) or SCUR (Session-based Charging with Unit Reservation). The `RoSession` class is also serializable, so it can be stored as a SIP session attribute. This allows the session to be restored when necessary to terminate the session or update credit authorization.

The example in Listing 4-3 creates a new `RoSession` for event-based charging, and sends a CCR request to start the first interrogation. The `RoSession` instance is saved so that it can be terminated later, after the service has finished.

Note that the `RoSession` class automatically handles creating session IDs; the application is not required to set the session ID.

Listing 4-3 Creating and Using a RoSession

```
RoSession session = roApp.createSession();
CCR ccr = session.createCCR(RequestType.INITIAL);
CCA cca = ccr.sendAndWait();
sipAppSession.setAttribute("RoSession", session);
...
```

Handling Re-Auth-Request Messages

The OCS may initiate credit re-authorization by issuing a Re-Auth-Request (RAR) to the CTF. The application can register a session listener for handling this type of request. Upon receiving a RAR, the Diameter subsystem invoke the session listener on the applications corresponding `RoSession` object. The application should then respond to the OCS with an appropriate RAA message and initiate credit re-authorization to the CTF by sending a CCR with the CC-Request-Type AVP set to the value UPDATE_REQUEST, as described in section 5.5 of RFC 4006.

A session listener must implement the `SessionListener` interface and be serializable, or it must be an instance of `SipServlet`. A Servlet can register a listener as follows:

```
RoSession session = roApp.createSession();
session.addListener(new SessionListener() {
  public void rcvMessage(Message msg) {
    System.out.println("Got message: id = " msg.getSession().getId());
  }
});
```

Listing 4-4 shows sample `rcvMessage()` code for processing a Re-Auth-Request.

Listing 4-4 Managing a Re-Auth-Request

```
RoSession session = roApp.createSession();
session.addListener(new SessionListener() {
public void rcvMessage(Message msg) {
  if (req.getCommand() != Command.RE_AUTH_REQUEST) return;
  RoSession session = (RoSession) req.getSession();
  Answer ans = req.createAnswer();
  ans.setResultCode(ResultCode.LIMITED_SUCCESS); // Per RFC 4006 5.5
  ans.send();
  CCR ccr = session.createCCR(Ro.UPDATE_REQUEST);
  ... // Set CCR AVPs according to requested credit re-authorization
```

```
    ccr.send();
    CCA cca = (CCA) ccr.waitForAnswer();
  }
```

In Listing 4-4, upon receiving the Re-Auth-Request the application sends an RAA with the result code DIAMETER_LIMITED_SUCCESS to indicate to the OCS that an additional CCR request is required in order to complete the procedure. The CCR is then sent to initiate credit re-authorization.

Note: Because the Diameter subsystem locks the call state before delivering the request to the corresponding `RoSession`, the call state remains locked while the handler processes the request.

Sending Credit-Control-Request Messages

The CCR class represents a Diameter Credit-Control-Request message, and can be used to send credit control requests to the OCF. For both ECUR (Event-Based Charging with Unit Reservation) and SCUR (Session-Based Charging with Unit Reservation), an instance of `RoSession` is used to create new CCR requests. You can also use `RoApplication` directly to create CCR messages for IEC (Immediate Event Charging). Listing 4-5 shows an example of how to create and send a CCR.

Listing 4-5 Creating and Sending a CCR

```
CCR ccr = session.createCCR(RequestType.INITIAL);
ccr.setServiceContextId("sample_id");
CCA cca = ccr.sendAndWait();
```

Once a CCR request is created, you can set whatever application- or service-specific AVPs that are required before sending the request using the `addAvp()` method. Because some of the same AVPs will need to be included in each new request for the session, it is also possible to set these AVPs on the session itself. Listing 4-6 shows a sample that sets:

- Subscription-Id to identify the user for the session
- Service-Identifier to indicate the service requested, and
- Requested-Service-Unit to specify the units requested.

A custom AVP is also added directly to the CCR request.

Listing 4-6 Setting AVPs in the CCR

```
session.setSubscriptionId(...);
session.setServiceIdentifier(...);
CCR ccr = session.createCCR(RequestType.INITIAL);
ccr.setRequestedServiceUnit(...);
ccr.addAvp(CUSTOM_MESSAGE, "This is a test");
ccr.send();
```

In this case, the same Subscription-Id and Service-Identifier are added to every new request for the session. The custom AVP “Custom-Message” is added to the message before it is sent out.

Handling Failures

Applications can examine the Result-Code AVP in CCA error responses from the OCF to detect the cause of a failure and take an appropriate action. Locally-generated errors, such as an unavailable peer or invalid route specification, cause the request send method to throw an `IOException` to with a detailed message indicating the nature of the failure.

Applications can also use the Diameter Timer Tx value for determining when the OCF fails to respond to a credit authorization request. Timer Tx has a default value of 10 seconds, but can be overridden using the `tx.timer` init parameter in the `RoApplication` configuration. Timer Tx starts when a CCR is sent to the OCF. The timer resets after the corresponding CCA is received.

If Tx expires before a corresponding CCA arrives, any call to `waitForAnswer` immediately returns null to indicate that the request has timed out. An application can then take action according to the value of the Credit-Control-Failure-Handling (CCFH) AVP in the request. See section 5.7, “Failure Procedures” in RFC 4006 for more details.

Listing 4-7 terminates the credit control session if timer Tx expires before receiving the CCA. If the CCA is received later by the Diameter subsystem, the message is ignored because the session longer exists.

Listing 4-7 Checking for Timer Tx Expiry

```
CCR ccr = session.createCCR(RequestType.INITIAL);
ccr.setCreditControlFailureHandling(RequestType.TERMINATION);
ccr.send();
CCA cca = ccr.waitForAnswer();
if (cca == null) {
  session.terminate();
}
```