

Oracle® Communications Converged Application Server

Release Notes

Release 4.0

August 2008

ORACLE®

Oracle Communications Converged Application Server Release Notes, Release 4.0

Copyright © 2007, 2008, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

1. Oracle Communications Converged Application Server Features and Changes

What's New in Oracle Communications Converged Application Server?	1-2
Based on Oracle WebLogic Server 10g Release 3	1-2
SIP Servlet 1.1 Specification (JSR 289)	1-2
Annotations and Resource Injection	1-3
Support for Unsolicited NOTIFY Messages	1-4
Updated Support for Globally-Routable User Agent URIs (GRUU)	1-4
SNMP Changes	1-4
Renamed Diagnostic Monitors and Actions	1-4
Examples Installation Changes	1-5
What's New in WebLogic SIP Server 3.x?	1-5
Integration with WebLogic Diagnostic Framework	1-5
Symmetric Response Routing (RFC 3581 rport parameter)	1-5
Domain Aliases	1-6
Additional Monitoring for SIP and Diameter Network Channels	1-6
Configurable Handling of Stale Session Data	1-6
List of SIP Headers and Parameters Added by WebLogic SIP Server	1-7
Geographically-Redundant Persistence	1-8
Diameter Base Protocol and IMS Ro, Rf Interface Support	1-8
Engine Tier Caching	1-9
RDBMS Storage for Long-Lived Call State Data	1-9

Minimal Transactional Latency with JRockit Deterministic Garbage Collection	1-9
Production Upgrade for Converged SIP/HTTP Applications.	1-9
SCTP Support for Diameter	1-10
DNS Support for Proxy Discovery and Response Routing	1-10
IPv6 Support.	1-10
Configurable Server Header	1-10
Configuration of SIP Message Header Formats	1-10
Extended API for Resolving TelURLs	1-11
SAR File Deployment	1-11
Extended Profile API.	1-12
Connection Pooling for Re-Use of TCP Connections	1-12
Support for Globally-Routable User Agent URIs (GRUU)	1-12

2. Resolved Problems in Oracle Communications Converged Application Server version 4.0

3. Oracle Communications Converged Application Server Known Issues

Oracle Communications Converged Application Server Features and

Changes

Welcome to Oracle Communications Converged Application Server Release 4.0! Oracle Communications Converged Application Server integrates SIP Servlet 1.1 technology with Java EE5 (JEE5) and other leading Internet standards to provide a reliable framework for developing highly available, scalable, and secure telecommunications applications. Oracle Communications Converged Application Server's seamless integration of disparate, heterogeneous platforms and applications enables your network to leverage existing software investments and share the enterprise-class services and data that are crucial to building next-generation telephony applications.

The following sections describe some of the new features and changes made in Oracle Communications Converged Application Server Release 4.0:

- [“What’s New in Oracle Communications Converged Application Server?”](#) on page 1-2
- [“What’s New in WebLogic SIP Server 3.x?”](#) on page 1-5

What's New in Oracle Communications Converged Application Server?

This section describes new features and functionality introduced in Oracle Communications Converged Application Server.

Based on Oracle WebLogic Server 10g Release 3

Oracle Communications Converged Application Server is deployed on the core Oracle WebLogic Server 10g Release 3 product, which introduces many key features such as an improved Administration Console, fast and flexible deployment model, new diagnostic capabilities, and EJB 3.0 support. See [What's New in WebLogic Server](#) in the Oracle WebLogic Server 10g Release 3 documentation.

Supporting files for Oracle Communications Converged Application Server are now stored in a *WLSS_HOME* directory within the BEA home directory (for example, `c:\bea\wlserver_10.3`). This is separate from the required Oracle WebLogic Server 10g Release 3 files, which are stored in the *WL_HOME* directory (for example, `c:\bea\wlserver_10.3`).

The revised documentation distinguishes between the *WLSS_HOME* and *WL_HOME* directories when appropriate.

SIP Servlet 1.1 Specification (JSR 289)

Oracle Communications Converged Application Server provides a robust SIP container that is compliant with the SIP Servlet 1.1 specification (JSR 289). The SIP Servlet 1.1 specification introduces many new features compared to the 1.0 specification, including:

- Improvements to the core SIP Servlet API
- Support for Back To Back User Agent (B2BUA) applications
- Formal application composition and application selection mechanisms
- Formal support for converged SIP and HTTP applications
- Support for SIP Servlet-related annotations.

See the [SIP Servlet v1.1 specification](#) for a complete guide to the new SIP Servlet API and container functionality. See [Porting Existing Applications to Oracle Communications Converged Application Server](#) in *Developing SIP Applications* for details about backward compatibility and porting existing v1.0 SIP Servlets.

Annotations and Resource Injection

In addition to the metadata annotations described in the SIP Servlet 1.1 specification, Oracle Communications Converged Application Server supports a subset of annotations from JSR 250 and JSR 154 for deployment and resource injection. The supported annotations are described in [Table 1-1](#) and [Table 1-2](#).

Table 1-1 Common Annotations

Annotation	Description
<code>@RunAs</code>	Declares the security role to use for executing the SIP Servlet. This annotation functions in the same manner as the <code>run-as</code> deployment descriptor element. See JSR 250 .
<code>@DeclareRoles</code>	Declares security roles used by the application. See JSR 250 .
<code>@PostConstruct</code>	Identifies a single initialization method to be called after a dependency injection. The specified method is called before the class is made available. See JSR 250 .
<code>@PreDestroy</code>	Identifies a method to be called when the container is removing the application. See JSR 250 .

Table 1-2 Common Resource Injections

Annotation	Description
<code>@Resource</code>	Declares a reference to a resource in a class, method, or field. This enables you to inject the <code>SipFactory</code> , <code>TimerService</code> , and <code>SipSessionUtil</code> objects. See JSR 250 .
<code>@Resources</code>	Declares multiple <code>@Resource</code> annotations. See JSR 250 .
<code>@EJB</code>	Declares a reference to an EJB component. This annotation functions in the same manner as the <code>ejb-ref</code> or <code>ejb-local-ref</code> deployment descriptor elements. See JSR 154 .
<code>@WebServiceRef</code>	Declares a reference to a Web Service. This annotation functions in the same manner as the <code>resource-reference</code> deployment descriptor element. See JSR 154 .

See also the [SIP Servlet 1.1 specification](#) for information about the new SIP Servlet-related annotations supported in this release, such as:

- `@SipServlet`

- @SipApplication
- @SipApplicationKey
- @SipListener (with associated listener-type specified in sip.xml)

Support for Unsolicited NOTIFY Messages

In order to improve compliance with RFC 3265, Oracle Communications Converged Application Server now permits applications to receive unsolicited NOTIFY messages and correlate them with a subscription. Prior to this release, Oracle Communications Converged Application Server would reject an unsolicited NOTIFY message with a 481 Subscription does not exist message.

Updated Support for Globally-Routable User Agent URIs (GRUU)

Oracle Communications Converged Application Server meets the requirements for obtaining and using Globally-Routable User Agent URIs (GRUU) as described in the latest [draft-ietf-sip-gruu-15: Obtaining and Using Globally Routable User Agent \(UA\) URIs \(GRUU\) in the Session Initiation Protocol \(SIP\)](#).

SNMP Changes

Oracle Communications Converged Application Server uses the new SNMP implementation provided by Oracle WebLogic Server 10g Release 3. In order to configure SNMP, you must create a dedicated Server SNMP agent for each engine and SIP data tier server (and optionally, the Administration Server) in your domain.

Oracle Communications Converged Application Server does not automatically increment the SNMP port number if the port is already in use. Instead, you must ensure that each agent is configured with a unique port number. In addition, the `-DWLSS.SNMPAgentPort` Java option cannot be used to override the SNMP agent configuration.

See [Configuring SNMP](#) in the *Operations Guide*.

Renamed Diagnostic Monitors and Actions

The diagnostic monitors and diagnostic actions provided in Oracle Communications Converged Application Server are now prefixed with `occas/`. For example, the WebLogic SIP Server 3.1 `Sip_Servlet_Before_Service` monitor is now named

`occas/Sip_Servlet_Before_Service`. You must update any existing diagnostic configuration files or applications that reference the non-prefixed names before they can work with Oracle Communications Converged Application Server.

See [Using the WebLogic Server Diagnostic Framework \(WLDF\)](#) in the *Operations Guide*.

Examples Installation Changes

Oracle Communications Converged Application Server example applications are no longer installed by default. To install the example applications, perform a custom installation and select the examples from the product component list.

When installed, Oracle Communications Converged Application Server examples are placed in the `WLSS_HOME/samples` directory (for example, `~/bea/wlcsrver_10.3/samples/sipserver/examples`).

A dedicated examples domain template is not included in this release. Instead, create a basic single-server domain using the `sipserverdomain.jar` template, then build and deploy individual example applications as needed.

See the [Installation Guide](#) for information about installing the examples and configuring a new domain. See the examples documentation installed at `WLSS_HOME/samples/sipserver/examples/src/index.html` for information about building and running the examples.

What's New in WebLogic SIP Server 3.x?

This section summarizes key new features and functionality that were introduced in the previous releases, WebLogic SIP Server 3.0 and 3.1.

Integration with WebLogic Diagnostic Framework

WebLogic SIP Server now integrates with the Weblogic Diagnostic Framework (WLDF) to provide improved data collection and logging, watches and notifications, diagnostic image capture, and code instrumentation. See [Using the WebLogic Diagnostic Framework \(WLDF\)](#) in the *Operations Guide*.

Symmetric Response Routing (RFC 3581 rport parameter)

WebLogic SIP Server 3.1 honors the `rport` parameter described in [RFC 3581](#) for symmetric response routing. When a message is received that has the `rport` parameter, the server responds

using the remote UDP port number from which the message was received, rather than the port number specified in the `via` header. You can also configure WebLogic SIP Server to automatically add the `rport` parameter to `via` headers when acting as a UAC. See [enable-rport](#) in the *Configuration Reference Manual*.

Domain Aliases

WebLogic SIP Server 3.1 now enables you to configure the exact domain(s) for which the server is responsible. Domain alias configuration avoids potential proxy problems and clarifies the domain handling support for a given server installation. See [domain-alias-name](#) in the *Configuration Reference Manual*.

Additional Monitoring for SIP and Diameter Network Channels

You can now monitor the behavior of WebLogic SIP Server network channels (`sip`, `sips`, `diameter`, `diameters`, and `diameter-sctp` channels) using the Administration Console. To monitor SIP and Diameter channels:

1. Access the Administration Console for your domain.
2. Select the Environment->Servers node.
3. Select the name of a server to monitor.
4. Select the Monitoring->Channels tab.

WebLogic SIP Server channels display statistics only for the Connections, Messages Received, Messages Sent, Bytes Received, and Bytes Sent attributes.

Configurable Handling of Stale Session Data

WebLogic SIP Server uses encoded URIs to identify the call states and application sessions associated with a message. When an application is undeployed or upgraded to a new version, incoming requests may have encoded URIs that specify “stale” or nonexistent call or session IDs. In WebLogic SIP Server 3.1, you can configure the action that the server takes when it encounters stale session data in a request. See [stale-session-handling](#) in the *Configuration Reference Manual*.

List of SIP Headers and Parameters Added by WebLogic SIP Server

WebLogic SIP Server may add one or more SIP headers and parameters to existing SIP messages in order to support various features. You must ensure that all network functions allow these headers and parameters to pass unchanged to SIP Server instances. Alternately, Session Border Control functions may archive and restore this information as necessary.

[Table 1-3](#) and [Table 1-4](#) describe the information that WebLogic SIP Server may add to SIP messages.

Table 1-3 WebLogic SIP Server Headers

Header Name	Description
X-BEA-Proxy-Policy	Determines the proxy policy used for sending certain requests.
X-Cluster-Info	Provides failover hints to the load balancer.
X-WLSS-Sdways-O-C	Used by the sideways forwarding mechanism to deliver messages to a compatible cluster during upgrade.
X-WLSS-Sdways-Req-Cert	Used by the sideways forwarding mechanism to deliver messages to a compatible cluster during upgrade.
X-WLSS-Sdways-Resp-Cert	Used by the sideways forwarding mechanism to deliver messages to a compatible cluster during upgrade.
X-WLSS-Sdways-R-C	Used by the sideways forwarding mechanism to deliver messages to a compatible cluster during upgrade.

Table 1-4 WebLogic SIP Server Parameters

Parameter Name	Description
apsessionid	Used with the <code>SipApplicationSession.encodeURI</code> method to store the session ID.
cluster	Provides failover hints to the load balancer.
wlsscid	Identifies the cluster ID of the cluster that originated the SIP message during a software upgrade. The sideways forwarding mechanism uses this attribute to ensure that messages are delivered to a compatible cluster.

Table 1-4 WebLogic SIP Server Parameters

Parameter Name	Description
wlssladdr	(New in Version 3.1.) Records the local address on which an incoming request was received by a stateless proxy. This header is required for handling the stateless proxy use case with rport support .
wlsslport	(New in Version 3.1.) Records the local port on which an incoming request was received by a stateless proxy. This header is required for handling the stateless proxy use case with rport support .
wlssrrd	Records the incoming and outgoing interfaces used in a multihomed configuration.

Geographically-Redundant Persistence

WebLogic SIP Server can be installed in a geographically-redundant configuration for customers who have multiple, regional data centers, and require continuing operation even after a catastrophic site failure. The geographically-redundant configuration enables multiple Weblogic SIP Server installations (complete with engine and SIP data tier clusters) to replicate call state transactions between one another. Administrators can then choose to redirect all network traffic to the secondary, replicated site to minimize lost calls if they determine that a regional site has failed. See [Configuring Geographically- Redundant Installations](#) in *Configuring and Managing WebLogic SIP Server*.

Diameter Base Protocol and IMS Ro, Rf Interface Support

In addition to the Diameter Sh protocol provider introduced in WebLogic SIP Server 2.2, version 3.0 includes new providers for the Ro and Rf protocols. The base Diameter protocol implementation is also now available for developers who want to implement additional Diameter applications. See the following links in *Developing Applications with WebLogic SIP Server* for more information:

- [Using the Diameter Base Protocol API](#)
- [Using the Diameter Rf Interface Application for Offline Charging](#)
- [Using the Diameter Ro Interface Application for Online Charging](#)

Engine Tier Caching

The engine tier now caches a portion of the SIP call state data available in SIP data tier replicas. When used in combination with a SIP-aware load balancer, the cache increases the performance of accessing call state data. See [Enabling the Engine Tier Cache in *Configuring and Managing WebLogic SIP Server*](#).

RDBMS Storage for Long-Lived Call State Data

WebLogic SIP Server 3.0 enables you to store long-lived call state data in an Oracle RDBMS in order to conserve RAM. The SIP data tier persists a call state's data to the RDBMS after the call dialog has been established, and retrieves or deletes the persisted call state data as necessary to modify or remove the call state. Oracle also provides an API for application designers to provide "hints" as to when the SIP data tier should persist call state data. See [Storing Call State Data in an RDBMS in *Configuring and Managing WebLogic SIP Server*](#).

Minimal Transactional Latency with JRockit Deterministic Garbage Collection

WebLogic SIP Server can be licensed in a "real time" configuration, which uses the JRockit deterministic garbage collector to greatly improve latency performance for SIP transactions. To enable this garbage collector, see [Using JRockit Deterministic Garbage Collection](#) in the *Configuration Guide*.

Production Upgrade for Converged SIP/HTTP Applications

WebLogic SIP Server 3.0 introduces application upgrade support for converged SIP/HTTP applications. Application upgrade support now closely models the upgrade support available in WebLogic Server 9.2, and provides for a SIP "administration channel" that can be used to securely testing applications in a production environment. See [Upgrading Deployed SIP Applications](#) in the *Operations Guide*.

Note: As part of the new upgrade functionality, `SipApplicationRuntimeMBean` is now deprecated for obtaining information about the application name and version string. Use `ApplicationRuntimeMBean` instead.

SCTP Support for Diameter

WebLogic SIP Server supports the SCTP transport protocol on certain operating systems for Diameter network traffic. See [Configuring Diameter Client Nodes and Relay Agents](#) in *Configuring Network Resources*.

DNS Support for Proxy Discovery and Response Routing

WebLogic SIP Server 3.0 now supports DNS for resolving the transport, IP address and port number of a proxy required to send a SIP message as described in [RFC 3263](#). DNS may also be used when routing responses in order to resolve the IP address and port number of a destination. Prior to version 3.0, DNS resolution had to be performed by the individual UA or proxy application.

See [Enabling DNS Support](#) in *Configuring Network Resources*.

IPv6 Support

WebLogic SIP Server supports IPv6 for external network interfaces as described in [RFC 2460: Internet Protocol, Version 6 \(IPv6\) Specification](#). To use IPv6, your underlying operating system must support the protocol, and you must configure IPv6 network channels on all engine tier server nodes. See [IPv4 and IPv6](#) in *Configuring Network Resources*.

Configurable Server Header

The Administrator can optionally configure the contents of the Server header that WebLogic SIP Server inserts into SIP message bodies. The entire header contents can be omitted to reduce the message size for wireless networks, or it can be set to an arbitrary string value. Prior to version 3.0, the header was always populated with the name and version of the WebLogic SIP Server instance. See [server-header](#) and [server-header-value](#) in the *Configuration Reference Manual*.

Configuration of SIP Message Header Formats

WebLogic SIP Server provides flexible configuration parameters and APIs for controlling whether generated SIP messages use compact or long header forms. Header form rules can be set at three different levels:

- Container-level configuration: Set the default rules for using compacting headers using elements in the `sipserver.xml` file. See [use-header-form](#) in the *Configuration Reference Manual*.

- **Message-level API:** The `WlssSipServletMessage` interface provides the `setUseHeaderForm` method to specify long or compact headers for a given SIP message. See [Using Compact and Long Header Formats for SIP Messages in *Developing Applications*](#).
- **Header-level API:** The JSR 116 `SipServletMessage` interface provides the `setHeader` method to set a given header name a specific value. See the JSR 116 JavaDoc for `SipServletMessage`.

`WlssSipServletResponse.setUseHeaderForm` can be used in combination with `SipServletMessage.setHeader` and the container-level configuration to customize header formats. See [Using Compact and Long Header Formats for SIP Messages in *Developing Applications*](#) for information about how the different settings interact with one another.

Extended API for Resolving TelURLs

WebLogic SIP Server extends the `javax.servlet.sip.TelURL` interface with the `com.bea.wcp.sip.WlssTelURI` interface. The extended interface enables applications to resolve Tel URLs present in the user portion of a SIP URI. The API parses a Tel URL into a domain name using the standard suffix, `e164.arpa`, as described in RFC 3761. It then performs a DNS NAPTR record lookup to produce an ENUM NAPTR record set.

For example, for a Tel URL domain name of `4.3.2.1.5.5.5.1.4.1.e164.arpa`, the API performs a DNS lookup to retrieve an ENUM NAPTR record set similar to:

```
$ORIGIN 4.3.2.1.5.5.5.1.4.1.e164.arpa
    IN NAPTR 100 10 "u" "E2U+sip"      "!^.*$!sip:user@example.com!"
    IN NAPTR 100 20 "u" "E2U+mailto"  "!^.*$!mailto:info@example.com!"
```

Methods in the `WlssTelURI` interface return either the full ENUM record set, an array of SIP URIs present in the record set, or only the highest-precedence SIP URI present in the record set. See `com.bea.wcp.sip.WlssTelURI` in the JavaDoc.

SAR File Deployment

WebLogic SIP Server 3.0 supports deployment of applications in SAR file format. The SAR file is similar in format to WAR files, and can contain deployment descriptor information for both HTTP and SIP Servlets. SAR files need not include a `weblogic.xml` deployment descriptor.

Extended Profile API

WebLogic SIP Server includes a public profile service API, `com.bea.wcp.sip.profile.API`, that you can use to create profile provider implementations. A profile provider performs the work of accessing XML documents from a data repository using a defined protocol. Deployed SIP Servlets and other applications need not understand the underlying protocol or the data repository in which the document is stored; they simply reference profile data using a custom URL using the provider API, and WebLogic SIP Server delegates the request processing to the correct provider. See [Developing Custom Profile Providers](#) in *Developing Applications with WebLogic SIP Server*.

Connection Pooling for Re-Use of TCP Connections

WebLogic SIP Server includes a new connection pooling mechanism to minimize unnecessary communication with a Session Border Control (SBC) function or Serving Call Session Control Function (S-CSCF). The server multiplexes a fixed pool of connections to a configured SBC or S-CSCF instead of repeatedly terminating and recreating connections during operation. See [connection-reuse-pool](#) in the *Configuration Reference Manual*.

Support for Globally-Routable User Agent URIs (GRUU)

WebLogic SIP Server meets the requirements for obtaining and using Globally-Routable User Agent URIs (GRUU) as described in [draft-ietf-sip-gruu-10: Obtaining and Using Globally Routable User Agent \(UA\) URIs \(GRUU\) in the Session Initiation Protocol \(SIP\)](#).

To specify a GRUU for WebLogic SIP Server to use when acting as a network element, see [globally-routable-uri](#) in the *Configuration Reference Manual*.

Resolved Problems in Oracle Communications Converged

Application Server version 4.0

[Table 2-1](#) below summarizes the issues in earlier releases (of the WebLogic SIP Server product) that have been resolved in Oracle Communications Converged Application Server version 4.0.

Table 2-1 Resolved Problems

Change Request Number	Description
CR239639	<p>When a SIP request was sent via application code, WebLogic SIP Server immediately started the transaction timer even though the actual message was queued for sending only after the application's service method ended. If the application code (or the system load) caused a delay in exiting the service method, retransmissions for the request could appear in a shorter amount of time than the configured SIP timers would indicate. (In extreme cases, the application request and its retransmission would appear on the wire at nearly the same time.)</p> <p>To address this problem, the code was modified to buffer the timer scheduling along with the request. This ensures more accurate timer behavior.</p>
CR290540	<p>In previous versions, <code>setCharacterEncoding()</code> did not throw an <code>UnsupportedEncodingException</code>. Existing Servlet code that called this method and used a catch clause for <code>UnsupportedEncodingException</code> had to be modified before recompiling for deployment to WebLogic SIP Server. This problem was addressed with a code fix.</p>
CR291406	<p>If you ran WebLogic SIP Server on a Windows platform with the JRockit JVM, you had to disable JRockit native IO in order to use SSL. If you did not disable native IO, an exception was generated similar to:</p> <pre>java.io.IOException: couldn't initialize IOPort: The parameter is incorrect.</pre> <p>This problem was addressed with a code fix.</p>

Table 2-1 Resolved Problems

Change Request Number	Description
CR297102	<p>While proxying an ACK message, if a <code>TooManyHopsException</code> was thrown WebLogic SIP Server would attempt to send a response to the ACK. This caused the exception:</p> <pre><Oct 17, 2006 1:50:18 PM PDT> <Error> <WLSS.Session> <BEA-331412> <Failed to respond 483 to too many hops request. java.lang.IllegalStateException: Cannot createResponse for ACK</pre> <p>The code was modified to drop the ACK after logging a message in this circumstance. The ACK can then be re-sent by the UAC when it receives a retransmission request.</p>
CR298765	<p>WebLogic SIP Server allowed you to deploy SIP applications with deployment descriptors that did not conform to their respective schemas. This could lead to exceptions or other unexpected behavior at runtime. The code was modified to reject application deployments when deployment descriptors do not conform to the schema.</p>
CR299384	<p>WebLogic SIP Server would log “unknown header” messages for the <code>WLSS-Default-Handler</code> header, even though this header is created and used by the server code itself. The header was registered and no longer generates error messages.</p>
CR300878	<p>When proxying a request over TCP, if an <code>IOException</code> was raised, WebLogic SIP Server logged the exception but did not send a final response upstream. Because of this, a UAC would not know whether an invite request was proxied successfully. The code was modified to detect transport errors while proxying, and create and send a 503 error response upstream in response to such errors.</p>

Table 2-1 Resolved Problems

Change Request Number	Description
CR301268	<p>If a Servlet used the <code>load-on-startup</code> deployment descriptor element to initialize the Servlet on startup (rather than on first request), and the <code>init</code> method created a new call state, WebLogic SIP Server would throw the following exception if any partition in the SIP data tier was not yet online:</p> <pre data-bbox="447 552 1053 760">Unexpected exception com.bea.wcp.sip.engine.server.SetupException : [WLSS.Engine:330027]Failed to initialize "proxy" servlet class test.ProxyServlet java.lang.IllegalStateException: PartitionClient offline</pre> <p>The code was modified to delay initialization a Servlet if all of the following conditions are met:</p> <ul data-bbox="447 852 1053 986" style="list-style-type: none"> • The Servlet uses <code>load-on-startup</code> • The Servlet overrides the <code>SipServlet.init</code> method • The Servlet is not deployed on the Administration Server • A configured partition is not yet online. <p>Note that the initialization delay is not applied to Administration Server deployments, because doing so could prevent replica servers from loading. Never deploy any applications to the Administration Server in a production system.</p>
CR301664	<p>WebLogic SIP Server used a fixed overload duration of 30 seconds. This could cause poor performance and continual overload situations with periodic spikes in <code>wlss.transport</code> work manager queue. The code was modified to set the initial overload duration to a much shorter 512 milliseconds, and then dynamically increase the duration if necessary in response to recurring overload conditions.</p>

Table 2-1 Resolved Problems

Change Request Number	Description
CR303194	<p>On Windows platforms, if you installed the WebLogic SIP Server product nested inside of other folders, the Administration Console extension could not load due to the length of the path being too long. To work around the problem, the following environment variable could be set before starting the Administration Server:</p> <pre>set JAVA_OPTIONS=-Dweblogic.j2ee.application.tmp Dir=d:/TEMP</pre> <p>This option is now automatically included in the server startup script, <code>commEnv.sh</code>.</p>
CR303219	<p>WebLogic SIP Server allowed SIP requests to access the retiring version of a deployed SIP application. This behavior was inconsistent with the base WebLogic Server application upgrade functionality, which disallows HTTP requests to a retiring application. For example, if you retired a converged SIP application, HTTP requests to the application would be rejected while SIP requests were permitted. The code was modified to be consistent with WebLogic Server behavior; the server now disallows SIP requests to a retiring application.</p>
CR303769	<p>Earlier WebLogic SIP Server versions ignored the encoding set through the <code>SipServletMessage.setCharacterEncoding()</code> method, and only honored the encoding if set using <code>contentType</code> argument of the <code>setContent()</code> method. This problem was addressed with a code fix.</p>
CR304389	<p>The server did not register SIP container runtime MBeans with the compatibility MBean server. This would lead to exceptions such as:</p> <pre>javax.servlet.ServletException: Unable to lookup type 'SipServletSnmpTrapRuntime'</pre> <p>The code was modified to address this problem.</p>

Table 2-1 Resolved Problems

Change Request Number	Description
CR305182	<p>When using WebLogic SIP Server with geographically-redundant installations, each write to a secondary site would log an error message similar to:</p> <pre><Dec 13, 2006 12:48:08 PM PST> <Error> <Security> <BEA-090513> <ServerIdentity failed validation, downgrading to anonymous.></pre> <p>This problem was addressed with a code fix.</p>
CR306926	<p>WebLogic SIP Server provided no way to configure the timeout duration for SCTP connections. The code was modified to honor a custom channel property, <code>SctpConnectTimeoutMillis</code>, to configure the property. See Configuring Custom Timeout, MTU, and Other Properties in <i>Configuring Network Resources</i>.</p>
CR308370	<p>WebLogic SIP Server could omit the tag parameter in the To header for PRACK messages. The code was modified to ensure that PRACK messages always include the To tag.</p>
CR309866	<p>WebLogic SIP Server exhibited poor scalability performance on Sun Sparc Enterprise T2000 servers when using the Sun JVM. These performance problems are addressed in Release 13 of the Sun JVM.</p>
CR310215	<p>WebLogic SIP Server would throw a <code>NullPointerException</code> if an application used <code>SipServletSnmpTrapRuntimeMBean</code> to generate an SNMP trap outside of a <code>doxxx</code> method. The code was modified to allow trap generation outside of a <code>doxxx</code> method. Note, however, that traps generate outside of a <code>doxxx</code> method use the string “Non Sip-Servlet Scope Application” instead of a Servlet name.</p>
CR310657	<p>The Diameter implementation used incorrect values (3 and 4) for the <code>CHECK_BALANCE</code> and <code>PRICE_ENQUIRY</code> values of the <code>Requested-Action</code> AVP. The code was modified to use the correct values of 2 and 3, respectively, as described in RFC4006.</p>

Table 2-1 Resolved Problems

Change Request Number	Description
CR310782	The Diameter implementation did not allow for a Diameter application to receive and process ASR requests. This meant that Diameter applications could not add AVPs to the termination CCR or be notified when a session was finished. The code was modified so that if a <code>SessionListener</code> is registered, the Diameter implementation passes ASR requests to the application listener for handling. In this case, it is the responsibility of the application to generate CCRs as well as send ASAs.
CR314296, CR315586	Oracle Communications Converged Application Server did not support monitoring network channels that used UDP via the Monitoring->Channels tab of the Administration Console. This problem was addressed with a code fix.
CR320065	When only the Ro application was configured, the Diameter CER was missing the <code>Supported-Vendor-Id</code> AVP. The code was modified to allow configuration of <code>Supported-Vendor-Id</code> values in the <code>diameter.xml</code> , in one or more <code>supported-vendor-id</code> elements.
CR328219	WebLogic SIP Server exhibited poor scalability performance on Sun Sparc Enterprise T2000 servers when using the JRockit JVM. These performance problems are addressed with a patch to JRockit R27.3.1 .

Table 2-1 Resolved Problems

Change Request Number	Description
CR367390	<p>In order to improve performance with non-replicated installations, local serialization is now performed whenever RDBMS persistence is enabled for Oracle Communications Converged Application Server. Because the RDBMS persistence feature is enabled by default for all installations, local serialization is also performed by default, even in replicated domains. Note, however, that local serialization is not used with, and does not interfere with, replicated domain functionality.</p>
CR374717	<p>To reduce the possibility of a buffer overflow attack, Oracle Communications Converged Application Server restricts the total size of UDP messages to 64K.</p> <p>TCP message headers are limited to 2048 bytes by default, as in previous releases. However, the TCP header size can now be increased as necessary by specifying the <code>-Dwls.header.maxSize=size</code> option at startup.</p>

Oracle Communications Converged Application Server Known Issues

The following table summarizes known issues and problems in Oracle Communications Converged Application Server.

Note: This section describes only those issues associated with the SIP Servlet container and data replication features of Oracle Communications Converged Application Server. See also the [WebLogic Server Known and Resolved Issues](#) for information about known problems with Oracle WebLogic Server 10g Release 3, which provides the underlying OA&M and Java EE5 capabilities of Oracle Communications Converged Application Server.

Table 3-1 Known Issues

Change Request Number	Description
n/a	By default, new Diameter network channels are created with a default Idle Connection Timeout value of 65 seconds. Change this attribute from the default in order to ensure that connections are not dropped and recreated every 65 seconds. See Creating Network Channels for the Diameter Protocol .
n/a	Oracle Communications Converged Application Server MIB objects are read-only. You cannot modify a Oracle Communications Converged Application Server configuration using SNMP.

Table 3-1 Known Issues

Change Request Number	Description
n/a	<p>This version of Oracle Communications Converged Application Server exhibits two behaviors that do not conform to the JSR 116 specification:</p> <ul style="list-style-type: none"> • MIME content is returned as a <code>String</code> object, rather than as a <code>javax.mail.Multipart</code> object as encouraged by the specification. • <code>isPersistent</code>, used for re-instantiating <code>ServletTimer</code> after server restarts, is not implemented. <p>Also, Oracle Communications Converged Application Server does not support dialog stateless proxies, an optional feature described in the API JavaDoc for the <code>Proxy</code> interface, <code>setStateful()</code> method:</p> <p>“This proxy parameter is a hint only. Implementations may choose to maintain transaction state regardless of the value of this flag, but if so the application will not be invoked again for this transaction.”</p>
n/a	<p>If you attempt to install Oracle Communications Converged Application Server 3.0 on Fedora Core 3 or 4 with <code>selinux</code> running, the installer throws a <code>java.lang.UnsatisfiedLinkError</code> exception. You cannot install Oracle Communications Converged Application Server while <code>selinux</code> is active.</p>
n/a	<p>If you configure two or more SIP data tier replicas using the default WebLogic Server Listen Address configuration (which specifies no listen address), multiple SIP data tier instances on the same machine cannot connect to one another. This problem occurs because, using the default Listen Address configuration, JNDI objects in the first booted server bind to all local IP addresses.</p> <p>To avoid this problem, always enter a valid IP address for each configured SIP data tier server instance.</p>
n/a	<p>In a Oracle Communications Converged Application Server installation with two engine tier nodes and two SIP data tier nodes in a partition (two replicas), if the connection to the SIP data tier becomes “split” such that each engine tier server can only reach a different SIP data tier node, one of the replicas is forced offline. To recover from this situation, always configure the Node Manager utility to restart SIP data tier replicas automatically when a replica fails. This enables the replica to rejoin its associated partition and update its copy of the call state data without having to manually restart the server.</p>

Table 3-1 Known Issues

Change Request Number	Description
CR294850	<p>The SIP Servlet v1.0 Specification states: “Containers may send the request asynchronously in which case sending may fail after the send method has returned successfully. In this type of situation, the container will generate its own final response. In this particular case, a 404 response would be appropriate.” Oracle Communications Converged Application Server sends requests asynchronously but does not deliver a 404 Not Found response to an application if a transport failure occurs. To work around this problem, applications should rely on the 408 Request Timeout response instead of 404.</p>
CR303216	<p>During an overload condition, Oracle Communications Converged Application Server may log messages similar to:</p> <pre><ACK received in state PROCEEDING:class=[ServerTransaction], objid=[25292416], key=[z9hg4bKc227250e04757a91cbdde388192e21f5], state=[3,PROCEEDING], method=[INVITE]></pre> <p>This occurs even if the ACK could be safely ignored (for example, if the ACK was generated by the server for a 503 response). There is no workaround to this problem, but it should occur only rarely (during overload conditions).</p>
CR267829	<p>When starting a replicated domain, if a partition has no running replicas and two replicas are started at the same time, the second replica shuts down if one or more engine tier servers are already running. To avoid this problem, always start all SIP data tier servers <i>before</i> starting any engine tier servers in a replicated domain.</p>

Table 3-1 Known Issues

Change Request Number	Description
CR272491, CR189353	<p>On Linux and UNIX systems, the default TCP connection timeout interval is usually very long and can cause Managed Servers to disconnect from the Administration Server under certain failure conditions.</p> <p>Specifically, if a single Managed Server in a domain fails abruptly or is disconnected from the network (for example, due to a removed network cable), the Administration Server tries to communicate to the failed server for the length of the TCP connection timeout value. During this time, the Administration Server does not send heartbeat messages to the remaining Managed Servers in the domain. Failing to send the heartbeat messages causes the remaining Managed Servers to consider the Administration Server as being offline, and they disconnect from the Administration Server. This finally causes the Administration Server to throw <code>PeerGoneExceptions</code> for the disconnected servers after the TCP timeout interval has been reached and the connection is closed.</p> <p>To work around this issue without changing the operating system TCP connection timeout value, use the</p> <pre>-Dweblogic.client.SocketConnectTimeoutInSecs</pre> <p>startup option when booting the Administration Server. BEA recommends using a value of 60 seconds to avoid numerous missed heartbeats</p> <pre>(-Dweblogic.client.SocketConnectTimeoutInSecs=60).</pre>
CR294126	<p>When an application in a replicated domain configuration is undeployed, Oracle Communications Converged Application Server uses timer processing to clean up the remaining call state data for the application. However, in a non-replicated configuration, the server attempts to invalidate remaining session data but does not destroy call states associated with the application; this may result in the server “leaking” call states that existed during application undeployment.</p>
CR300715	<p>Testing on Solaris platforms has shown that the following JVM arguments to improve performance with the Sun JVM for replica servers:</p> <pre>-server -Xms1024m -Xmx1024m -XX:+UseParNewGC -XX:+UseConcMarkSweepGC</pre> <p>For engine tier servers, these example arguments have shown to improve performance:</p> <pre>-server -Xms768m -Xmx768m -XX:+UseParallelGC -XX:MaxGCPauseMillis=400 -XX:+DisableExplicitGC</pre> <p>Note that these JVM settings have only been tested on Solaris platforms. For other platforms, begin with the example JVM arguments described in Tuning JVM Garbage Collection for Production Deployments.</p>

Table 3-1 Known Issues

Change Request Number	Description
CR302859	<p>In order to use SCTP with IPv4 on Solaris, you must set the <code>-Dsctp.preferIPv4Stack=true</code> Java option when starting the server. You can edit your startup script to include this option, or set the environment variable:</p> <pre>export JAVA_OPTIONS=-Dsctp.preferIPv4Stack=true</pre>
CR346262	<p>If you install the 64-bit version of Oracle Communications Converged Application Server installer package on Solaris, you must add the <code>-d64</code> option with the Sun JDK in order to specify 64-bit mode. If you omit the <code>-d64</code> option, the Sun JDK automatically defaults to 32-bit mode and the installer fails to install required 64-bit native libraries. This yields the following error on startup:</p> <pre><Oct 4, 2007 4:54:28 AM EDT> <Error> <Socket> <BEA-000438> <Unable to load performance pack. Using Java I/O instead. Please ensure that a native performance library is in: path></pre>

Oracle Communications Converged Application Server Known Issues