Oracle® Communication and Mobility Server

Release Notes

Release 10.1.3.3.2

E10517-01

September 2007

This document contains information about the Release 10.1.3.3.2 patchset. It augments information in the existing books in the Oracle Communication and Mobility Server (OCMS) library (Installation Guide, Administrator's Guide, Developer's Guide, and Release Notes).

1 New in this Release

Beginning with this patchset release, Oracle Communication and Mobility Server supports a deployment topology in which an F5 BigIP Load balancer can assume the role of the Edge Proxy node and achieve a Highly Available Cluster configuration.

For information on this topology, see Section 4, "F5 BigIP Load Balancer with SIP Application Session Persistence". All other topologies described in the documentation remain supported.

2 Bugs Fixed in this Release

This cumulative patchset includes bug fixes. Bugs fixed by this, and the previous patchset are listed.

Table 1 Bugs fixed in this release

Bug Number	Description	Available in Patchset 1?
5958103	CREATECANCEL() DOES NOT COPY ROUTE HEADERS FROM INVITE	Y
6040227	SPINNING ON ABROGATED SESSION	Y
6059635	CORE SIPCONTAINER IN OCMS 10.1.3.3 FAILED TO WORK WITH OC4J 10.1.3.1	Y
6065641	THE EDGE PROXY DOESN'T IMPLEMENT 16.4 OF RFC3261 IN THE CORRECT WAY	Y
6065646	THE EDGE PROXY CONVERTS FROM TCP TO UDP - NOT ALLOWED AS STATELESS PROXY	Y
6065650	INCORRECT DETECTION OF STRICT ROUTERS FOR INCOMING REQUEST (HOSTNAME MATCHING)	Y
6071277	MODIFICATION OF CONTACT HEADER NOT ALLOWED	Y
6111989	HA OCMS SERVICE HANG - VERY SERIOUS IMPACT	Y
6115309	HA LOCKS REPLICATION MANAGER ("BRICKS") THREAD	Y

Table 1 (Cont.) Bugs fixed in this release

Bug Number	Description	Available in Patchset 1?
6122007	X-RESOLVED-ADDR NOT SET ON SUBSEQUENT REQUESTS	Y
6137833	SPECIFIC APP SESS ID PARAMETER MISSING FOR ENCODEURI	Y
6137860	SIP CONTAINER MAPS INITIAL REQUESTS TO EXISTING APPLICATION SESSION	Y
6137935	CONTAINER ADDS APP SESS ID ON ALL CONTACT HEADERS	Y
6124785	PROXY 503 AS 500 MISSING HEADERS, E.G. RETRY-AFTER	N
6140611	OCMS HANGS AFTER SEVERAL 4XX RESPONSES FROM PSTN GW	N
6145767	PORT BUG 6143849 FROM 10.1.3.4	N
6162739	LOG CONTAINS UNCLEAR MESSAGES	N
6195318	UDPMESSAGETOOBIGEXCEPTION	N
6238385	UNABLE TO CREATE PRACK	N
6270642	PARLAY X: SHOULD USE SOAP HEADER TO IDENTIFY USER INSTEAD OF HTTP HDR	N

3 Limitations

The following limitations exist in this release.

3.1 SCE Java Settings

In the documentation, you are directed to set JAVA_HOME to point to the JRE directory. That works in most situations, but it is not adequate when you are creating a web-converged application (such as the Message Sender application), in which case you would not be able to deploy it properly. In that case, your settings should be:

```
JAVA_HOME= java/jdk
PATH= java/jdk/bin
Eclipse JDK / JRE is set to java/jdk
```

3.2 Recommended TCP Window Size on HPUX

In the HPUX OCMS version, an adjustment in configuration may need to be made.

If you are expecting more than 50 simultaneous TCP connections to the server, use a 32Kb TCP window size. Here is the command:

```
ndd -set /dev/tcp tcp_recv_hiwater_def 32768
```

If you are expecting less than 50 simultaneous TCP connections to the server, set a large TCP Window size. Here is the command:

```
ndd -set /dev/tcp tcp_recv_hiwater_def 4194304
```

The HPUX JVM allocates a buffer for each concurrent TCP connection the size of the TCP Window size.

Note that the setting may vary between the SIP Container (usually requires a higher setting) and the Edge Proxy (usually requires a lower setting).

3.3 Verify Spelling in Attribute Names

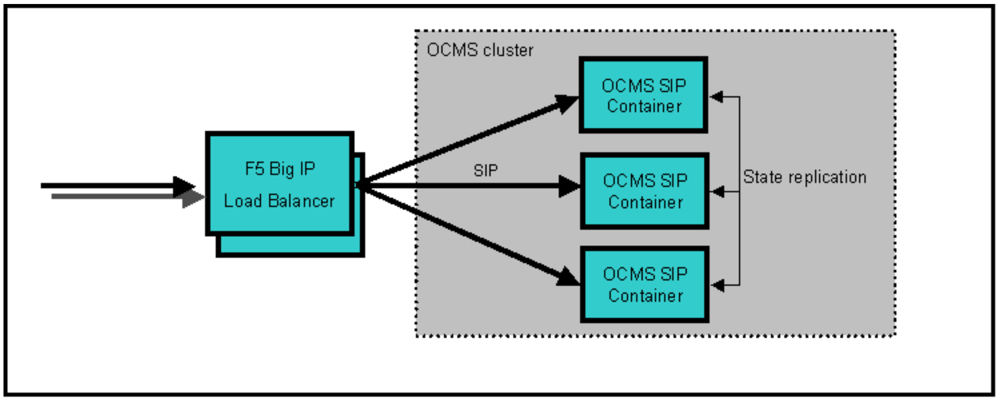
When an attribute name is misspelled in `opmn.xml`, the corresponding process will not start, and you will receive an error message in the logs stating that the misspelled attribute name is not found. In `orion-application.xml`, however, you will not receive such an error message if the name of an attribute is misspelled. So if you misspell an attribute name in the cluster configuration section, replication will appear to have started, but session replication will not work. Be very careful to spell attribute names correctly in `orion-application.xml`.

4 F5 BigIP Load Balancer with SIP Application Session Persistence

This section details the requirements and procedures needed to use an F5 BigIP Load Balancer in an OCMS cluster for high availability and scalability without Edge Proxy nodes. The following topics are included:

- Requirements
- Installation
- Verify the Configuration
- Post-Installation Steps
- OPTIONS Handling
- Load Balancing Limitation

Figure 1 F5 BigIP Load Balancer without Edge Proxy



This section is only for advanced users setting up an F5 BigIP Load Balancer.

4.1 Requirements

To set up an OCMS cluster as described in this document the following components are required:

- You are familiar with OCMS and BigIP.
- Two or more SIP Application Server nodes with OCMS 10.1.3.3.2 installed.

- One F5 BigIP load balancer version 9.4.1 or higher.
- The iRule scripts
  - `ocms-persist-udp-inbound.tcl`
  - `ocms-persist-udp-outbound.tcl`
  - `ocms-persist-tcp-inbound.tcl`
  - `ocms-persist-tcp-outbound.tcl`
  - `ocms-persist-parameters.tcl`

4.2 Installation

Complete the following steps to install and configure BigIP.

> **Note:** This configuration will not work with an Edge Proxy.

Begin by setting up your network:

1. Define one Virtual Server IP address (must be routable from external SIP entities).
2. Set up the network and the different nodes so that the SIP Application Server nodes all use the BigIP as router for all outgoing SIP traffic. This involves creating SelfIPs and VLANs on the BigIP and configuring the networking on the SIP Application Server machines (and possibly reconfiguring other routers in the network). See your F5 documentation for more information.

   Install OCMS:

3. Follow the OCMS 10.1.3.3 Installation Guide to install the SIP Application Server nodes. Apply the OCMS 10.1.3.3.2 patchset; it is required for the HA topology without EdgeProxy nodes.

   Configure BigIP Monitors:

4. On the BigIP administration web interface, create a new monitor of type `ICMP` with the name *ocms_icmp*; set the Interval to 1 second and the Timeout to 3 seconds.
5. Create another monitor of type `SIP` with the name *ocms_sip*; set the Interval to 1 second and the Timeout to 3 seconds. If the ProxyRegistrar application is to be deployed in this cluster, then add 400 as additional response code for this monitor.

   Configure BigIP iRules:

6. Add a new iRule with the name *ocms-persist-udp-inbound* and paste the contents of the file `ocms-persist-udp-inbound.tcl` into the Definition text area.
7. Add a new iRule with the name *ocms-persist-udp-outbound* and paste the contents of the file `ocms-persist-udp-outbound.tcl` into the Definition text area.
8. Add a new iRule with the name *ocms-persist-tcp-inbound* and paste the contents of the file `ocms-persist-tcp-inbound.tcl` into the Definition text area.
9. Add a new iRule with the name *ocms-persist-tcp-outbound* and paste the contents of the file `ocms-persist-tcp-outbound.tcl` into the Definition text area.
10. Add a new iRule with the name *ocms-persist-parameters* and paste the contents of the file `ocms-persist-parameters.tcl` into the Definition text area.

Configure BigIP (Inbound):

11. Create a new Node for each SIP Application Server node in the cluster and assign them the health monitor `ocms_icmp`.

12. Create a new Pool with the name *ocms_pool* and assign it the health monitor `ocms_sip`.

13. Add all the SIP Application Server Nodes as members of this pool on port `5060`.

14. Create a new Profile of type UDP with the name *ocms_udp* and set the Idle Timeout to Immediate, and enable Datagram LB.

15. Create a Virtual Server of type Standard, with the IP address defined in Step 1. Set the Service Port to `5060` and the Protocol to `UDP`. Set the Protocol Profile to `ocms_udp`, and enable it on the VLAN to which external SIP entities are connected (the external network).

16. Set the default pool to `ocms_pool` and add the iRules `ocms-persist-udp-inbound.tcl` and `ocms-persist-parameters.tcl` to the Virtual Server.

17. Create another Virtual Server of type Standard, with the same IP address and Service Port, but with the Protocol set to TCP. Enable it in the VLAN to which external SIP entities are connected (the external network).

18. Set the default pool to `ocms_pool` and add the iRules `ocms-persist-tcp-inbound.tcl`, and `ocms-persist-parameters.tcl` to the Virtual Server.

Configure BigIP (Outbound):

19. Create a new SNAT pool with the name *ocms_outbound_snat* containing one IP address, the same IP address that was defined in Step 1 (the Virtual Server IP).

20. Create a new Pool with the name *ocms_outbound_pool*, containing as its only member, an unused IP address on the external VLAN (and any port). This pool will only be used as a "dummy" pool as a workaround for a bug in the BigIP software. Therefore, the choice of IP address is not important, and will not be used in the routing decision. Still, the BigIP will only allow you to add a valid IP address on one of the connected subnets.

21. Create a new Virtual Server of Destination Type Network with the name sip_outbound_udp. Set the Destination Address to `0.0.0.0` and the Mask to `0.0.0.0`. Set the port to `* All Ports`, the Protocol to `UDP` and the Protocol Profile to `ocms_udp`. Enable the Virtual Server on the VLAN to which the SIP Application Servers are connected, and select `ocms_outbound_snat` as the SNAT Pool.

22. Disable Address Translation for this Virtual Server, and set the default pool to `ocms_outbound_pool`.

23. Add the iRules `ocms-persist-udp-outbound.tcl` and `ocms-persist-parameter.tcl` to this Virtual Server.

24. Create a new Virtual Server of Destination Type `Network` with the name *sip_outbound_tcp*. Set the Destination Address to `0.0.0.0` and the Mask to `0.0.0.0`. Set the port to `* All Ports`, and the Protocol to `TCP`. Enable the Virtual Server on the VLAN to which the SIP Application Servers are connected, and select `ocms_outbound_snat` as SNAT Pool.

25. Disable Address Translation for this Virtual Server, and set the default pool to `ocms_outbound_pool`.

26. Add the iRules `ocms-persist-tcp-outbound.tcl` and `ocms-persist-parameters.tcl` to this Virtual Server.

    Configure OCMS:

27. Configure the `DistributableRecordRoute`, `DistributableContact`, and `Via` parameters in the SipServletContainer so that these URIs point to the Virtual Server of the BigIP load balancer, either using the IP address or a hostname that resolves to the same.

28. Make sure that the EdgeProxy parameter is empty!

4.3 Verify the Configuration

To verify the configuration, go to the BigIP administration web interface and select the `ocms-pool`. Ensure that the Availability of the pool is green. Click the **Members** tab and make sure that all pool members have a green status.

4.4 Post-Installation Steps

The four iRule scripts store information about SIP sessions in memory in order to perform the correct load balancing. To avoid filling the BigIP's memory each such persisted connection has a timeout value that defines how long the information will be kept in memory before it is removed, as long as no traffic associated with the connection is processed. Each SIP Servlet Application running on the SIP Application Server have a similar timeout value that defines how long the SIP Servlet Container will keep a session in memory. For the system to work these two timers must match, otherwise load balancing may be incorrect which can lead to broken sessions.

The session timer in each application can be configured in the `sip.xml` for the SIP Servlet, but it can also be set programmatically. It may be different for different applications deployed on the same server. The default value for the timer in the SIP Servlet Container is 15 minutes.

The timeout used by the BigIP for SIP sessions is defined in the iRule `ocms-persist-parameters`. To change the session timeout, update the `sessionTimeout` parameter to the desired value in seconds. The default value is 900s (15min).

4.5 OPTIONS Handling

The BigIP configuration described in this document relies on sending a `SIP OPTIONS` request to the OCMS nodes in the cluster as a monitoring mechanism, expecting a `200 OK` response back from healthy nodes. These OPTIONS requests include a request URI with an empty user part, and the host part being the IP address of the OCMS node. The OCMS SIP Container has a default behavior to respond to such OPTIONS requests with a 200 OK. However, any SIP Servlet application can override this behavior by having a servlet-mapping that matches this type of OPTIONS request. In order to preserve the functionality of the cluster, caution must be taken to ensure that any application deployed on the system that overrides this default behavior responds to this type of OPTIONS requests with a 200 OK. If it responds with a response code other than 200 OK, then that response code should be added as an additional response code for the monitor.

4.6 Load Balancing Limitation

In this release, the F5 BigIP solution (version 9.4.1) has a limitation in that multiple calls/dialogs on a single incoming TCP connection will always end up in a single cluster node. The selection of cluster node is based on the first inspected message on the TCP stream. Initial requests on this same TCP stream will follow the same path and end up in the same cluster node. The result is that no load balancing nor stickiness is applied for calls/dialogs that are multiplexed on the same TCP stream.

Nodes connecting to the OCMS cluster using this solution must use either UDP or a single TCP stream for each SIP dialog or transaction.

5 Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Oracle® Communication and Mobility Server, Release 10.1.3.3.2
E10517-01

licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.