Deployment Guide

Document version: 1.0

What's inside:

2 Prerequisites and configuration notes

2 Configuration example

3 Configuring the BIG-IP system for Oracle Enterprise Manager 12c

8 Configuring Enterprise Manager for Use with F5 BIG-IP LTM

10 Document Revision History

Deploying the BIG-IP LTM with Oracle Enterprise Manager 12c Cloud Control

Welcome to the F5 deployment guide for Oracle® Enterprise Manager 12c with the BIG-IP system. This guide shows administrators how to configure the BIG-IP Local Traffic Manager (LTM) for directing traffic, ensuring application availability, improving performance and providing a flexible layer of security for Oracle Enterprise Manager 12c deployments.

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line and provides the industry's first complete cloud lifecycle management solution. Oracle Enterprise Manager's Business-Driven IT Management capabilities allow you to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments from applications to disk.

This deployment guide has been jointly written by Oracle Corporation and F5 Networks and provides the detailed steps for implementation of an Oracle MAA solution for Oracle Enterprise Manager Cloud Control using BIG-IP from F5 Networks as the front end for the Cloud Control mid-tiers, known as the Oracle Management Service (OMS). The BIG-IP hardware platform can provide load balancing, high availability, service monitoring, TCP/IP enhancements, and application persistence for the Cloud Control environment as the front end for several Cloud Control services.

For more information on Oracle Enterprise Manager, see *http://www.oracle.com/us/products/enterprise-manager/index.html*

For more information on the F5 BIG-IP system, see *http://www.f5.com/products/big-ip/*

Products and versions

Product	Version
BIG-IP LTM	11.1, 11.2
Oracle Enterprise Manager Cloud Control	12.1.0.1.0

Important: *Make sure you are using the most recent version of this deployment guide, available at http://www.f5.com/pdf/deployment-guides/oracle-enterprise-manager-12c-dg.pdf.*

Prerequisites and configuration notes

The following are general prerequisites and configuration notes for this guide:

- You must have administrative access to the BIG-IP web-based Configuration utility.
- You must have administrative privileges on the Enterprise Manager system.
- You must have both the Oracle OMS systems and the LTM configured to use an NTP server for time synchronization.
- You must have both the Oracle OMS systems and LTM configured to use DNS for name resolution.

Configuration example

Cloud Control OMS Servers provide HTTP or HTTPS access to a set of Cloud Control services, listed below, to the Cloud Control clients, including the Cloud Control console and Management Agents. When more than one Cloud Control OMS Server is deployed, the F5 BIG-IP system can load balance requests for each service via virtual servers, with the Cloud Control clients making service requests using a virtual host name.

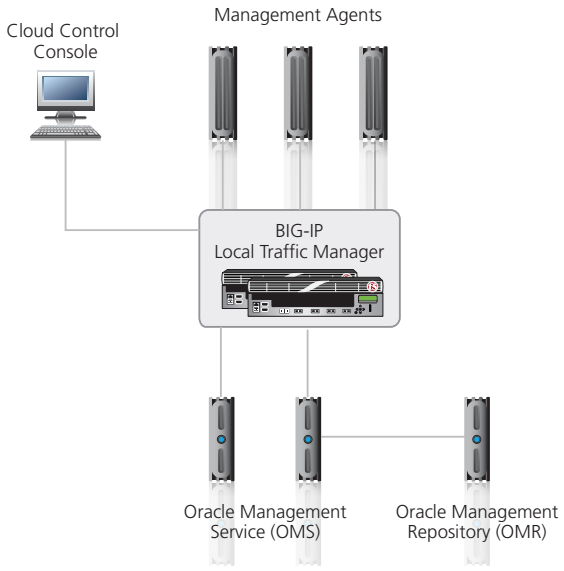

Figure 1: *Logical Configuration Example*

The Cloud Control services that can be served by the F5 BIG-IP in a multi-OMS setup are:

Cloud Control Service	Description
Secure Console	HTTPS access to Cloud Control Console
Unsecure Console	HTTP access to Cloud Control Console
Secure Upload	Secure Agent to OMS communication
Agent Registration	Unsecure Agent to OMS communication

Configuring the BIG-IP system for Oracle Enterprise Manager 12c

Use the following table for guidance on configuring the BIG-IP system for Oracle Enterprise Manager. This table contains any non-default setting you should configure as a part of this deployment. Settings not contained in the table can be configured as applicable. For specific instructions on configuring individual objects, see the online help or product manuals.

Health Monitors

Note: There are two entries for both the Secure Console and the Unsecure Console services. Configuration of these monitors differs depending on whether SSO has been configured for Enterprise Manager authentication. Only one monitor needs to be configured for each service, choose the relevant one for your environment.

To create a monitor, on the Main tab, expand **Local Traffic**, and then click **Monitors**. Click the **Create** button. After choosing the monitor type, from the **Configuration** list, select **Advanced**.

Cloud Control Service	Non-default settings/Notes	
Secure Console when not using SSO	***Name***	Give the monitor a unique name, such as *mon_ccsc7799*
	Type	**HTTPS**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /em/console/home HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n**
	Receive String	**/em/login.jsp**
	Alias Service Port	**7799**
Secure Console when using SSO	***Name***	Give the monitor a unique name, such as *mon_ccsc7799*
	Type	**HTTPS**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /empbs/genwallet \r\n**
	Receive String	**GenWallet Servlet activated**
	Alias Service Port	**7799**
Unsecure Console when not using SSO	***Name***	Give the monitor a unique name, such as *mon_ccuc7788*
	Type	**HTTP**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /em/console/home HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n**
	Receive String	**/em/login.jsp**
	Alias Service Port	**7788**
Unsecure Console when using SSO	***Name***	Give the monitor a unique name, such as *mon_ccuc7788*
	Type	**HTTP**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /empbs/genwallet \r\n**
	Receive String	**GenWallet Servlet activated**
	Alias Service Port	**7788**

Cloud Control Service	Non-default settings/Notes	
Secure Upload	***Name***	Give the monitor a unique name, such as *mon_ccsc7799*
	Type	**HTTPS**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /empbs/upload \r\n**
	Receive String	**Http Receiver Servlet active!**
	Alias Service Port	**4900**
Agent Registration	***Name***	Give the monitor a unique name, such as *mon_ccsc7799*
	Type	**HTTPS**
	Interval	**30**
	Timeout	**91**
	Send String	**GET /empbs/genwallet \r\n**
	Receive String	**GenWallet Servlet activated**
	Alias Service Port	**4889**

Pools

The next task is to create the load balancing pools. You must create a pool for each of the Cloud Control services as described in the following table.

To create a pool, on the Main tab, expand **Local Traffic**, and then click **Pools**. Click the **Create** button.

Cloud Control Service	Non-default settings/Notes	
Secure Console	***Name***	Give the pool a unique name, such as *pool_ccsc7799*
	Health Monitors	Activate the monitor you created for the Secure Console
	Load Balancing Method	**Least Connections (member)**
	New Members	In the **Address** box, type the IP address an OMS host. In the **Service Port** box, type **7799**. Repeat for each OMS host.
Unsecure Console	***Name***	Give the pool a unique name, such as *pool_ccuc7788*
	Health Monitors	Activate the monitor you created for the Unsecure Console
	Load Balancing Method	**Least Connections (member)**
	New Members	In the **Address** box, type the IP address an OMS host. In the **Service Port** box, type **7788**. Repeat for each OMS host.
Secure Upload	***Name***	Give the pool a unique name, such as *pool_ccsu4900*
	Health Monitors	Activate the monitor you created for Secure Upload
	Load Balancing Method	**Least Connections (member)**
	New Members	In the **Address** box, type the IP address an OMS host. In the **Service Port** box, type **4900**. Repeat for each OMS host.
Agent Registration	***Name***	Give the pool a unique name, such as *pool_ccar4889*
	Health Monitors	Activate the monitor you created for Agent Registration
	Load Balancing Method	**Least Connections (member)**
	New Members	In the **Address** box, type the IP address an OMS host. In the **Service Port** box, type **4889**. Repeat for each OMS host.

Profiles

The next task is to create Profiles on the BIG-IP system. You must create profiles for each of the Cloud Control services as described in the following table.

To create a Profile, on the Main tab, expand **Local Traffic**, and then click **Profiles**. On the Menu bar, click the appropriate profile type, and then click **Create**.

Cloud Control Service	Non-default settings/Notes	
Secure Console	***TCP Profile***	
	Name	Give the profile a unique name, such as *tcp_ccsc7799*
	Parent Profile	**tcp-lan-optimized**
	Idle Timeout	**3600 Seconds**
	Persistence Profile	
	Name	Give the profile a unique name, such as *sourceip_ccsc7799*
	Persistence Type	**Source Address Affinity**
	Timeout	Check the **Custom** box, and then in the **Seconds** box, type **3600**.
Unsecure Console	***TCP Profile***	
	Name	Give the profile a unique name, such as tcp_ccuc7788
	Parent Profile	**tcp-lan-optimized**
	Idle Timeout	**3600 Seconds**
	Persistence Profile	
	Name	Give the profile a unique name, such as *sourceip_ccuc7788*
	Persistence Type	**Source Address Affinity**
	Timeout	Check the **Custom** box, and then in the **Seconds** box, type **3600**.
Secure Upload	***TCP Profile***	
	Name	Give the profile a unique name, such as *tcp_ccsu4900*
	Parent Profile	**tcp-lan-optimized**
	Idle Timeout	**3600 Seconds**
	Persistence Profile	
	Name	Give the profile a unique name, such as *sourceip_ccsu4900*
	Persistence Type	**Source Address Affinity**
	Timeout	Check the **Custom** box, and then in the **Seconds** box, type **3600**.
Agent Registration	***TCP Profile***	
	Name	Give the profile a unique name, such as *tcp_ccar4889*
	Parent Profile	**tcp-lan-optimized**
	Idle Timeout	**3600 Seconds**
	Persistence Profile	
	Name	Give the profile a unique name, such as *sourceip_ccar4889*
	Persistence Type	**Source Address Affinity**
	Timeout	Check the **Custom** box, and then in the **Seconds** box, type **3600**.

Virtual Servers

The final task is to create the BIG-IP virtual servers. You must create a virtual server for each of the Cloud Control services as described in the table on the following page.

To create a Virtual Server, on the Main tab, expand **Local Traffic**, and then click **Virtual Servers**. Click **Create**.

Cloud Control Service	Non-default settings/Notes	
Secure Console	***Name***	Give the virtual server a unique name, such as *vs_ccsc443*
	Destination	Type the IP address you want to use for this virtual server
	Service Port	**443**
	Protocol Profile (Client)[1]	Select the TCP profile for Secure Console (tcp_ccsc7799 in our example)
	SNAT Pool	**Automap**
	Default Pool	Select the Pool for Secure Console (pool_ccsc7799 in our example)
	Default Persistence Profile	Select the Persistence Profile for Secure Console (_ccsc7799 in our example)
Unsecure Console	***Name***	Give the virtual server a unique name, such as *vs_ccuc7788*
	Destination	Type the IP address you want to use for this virtual server
	Service Port	**7788**
	Protocol Profile (Client)[1]	Select the TCP profile for Unsecure Console (tcp_ccuc7788 in our example)
	SNAT Pool	**Automap**
	Default Pool	Select the Pool for Unsecure Console (pool_ccuc7788 in our example)
	Default Persistence Profile	Select the Persistence Profile for Unsecure Console (sourceip_ccuc7788 in our example)
Secure Upload	***Name***	Give the virtual server a unique name, such as *vs_ccsu4900*
	Destination	Type the IP address you want to use for this virtual server
	Service Port	**4900**
	Protocol Profile (Client)[1]	Select the TCP profile for Secure Upload (tcp_ccsu4900 in our example)
	SNAT Pool	**Automap**
	Default Pool	Select the Pool for Secure Upload (pool_ccsu4900 in our example)
	Default Persistence Profile	Select the Persistence Profile for Secure Upload (sourceip_ccsu4900 in our example)
Agent Registration	***Name***	Give the virtual server a unique name, such as *vs_ccar4889*
	Destination	Type the IP address you want to use for this virtual server
	Service Port	**4889**
	Protocol Profile (Client)[1]	Select the TCP profile for Agent Registration (tcp_ccar4889 in our example)
	SNAT Pool	**Automap**
	Default Pool	Select the Pool for Agent Registration (pool_ccar4889 in our example)
	Default Persistence Profile	Select the Persistence Profile for Agent Registration (sourceip_ccar4889 in our example)

[1] You must select **Advanced** from the **Configuration** list for this option to appear

Configuring Enterprise Manager for Use with F5 BIG-IP LTM

Resecure Management Service

The management services must now be reconfigured so that the Management Service certificate uses the hostname associated with the F5 BIG-IP system. Steps 1 and 2 must be repeated for each configured OMS

1. **Resecure OMS**

   In our example we issued the following command:

```
$ emctl secure oms –sysman_pwd xxxxxx –reg_pwd xxxxxx –host slb.example.com –secure_
port 4900 –slb_port 4900 –slb_console_port 443 –console –lock –lock_console
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.1.0 Copyright (c) 1996, 2011
Oracle Corporation. All rights reserved. Securing OMS... Started.
Securing OMS... Successful
Restart OMS
```

2. **Restart the OMS**

```
$ ./emctl stop oms -all
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.1.0 Copyright (c) 1996, 2011
Oracle Corporation. All rights reserved. Stopping WebTier...
WebTier Successfully Stopped S
topping Oracle Management Server...
Oracle Management Server Successfully Stopped
AdminServer Successfully Stopped
Oracle Management Server is Down
$
$ ./emctl start oms
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.1.0 Copyright (c) 1996, 2011
Oracle Corporation. All rights reserved. Starting WebTier...
WebTier Successfully Started
Starting Oracle Management Server...
Oracle Management Server Successfully Started
Oracle Management Server is Up
```

3. **Resecure all Management Agents**

```
$ ./emctl secure agent -emdWalletSrcUrl https://slb.example.com:4900/em
Oracle Enterprise Manager 12c Release 1 12.1.0.1.0
Copyright (c) 1996, 2011 Oracle Corporation. All rights reserved.
Agent successfully stopped... Done.
Securing agent... Started.
Enter Agent Registration Password :
Agent successfully restarted... Done.
EMD gensudoprops completed successfully
Securing agent... Successful.
```

Verify Status of Management Service

The OMS configuration can be checked using the **emctl status oms –details** command. Following successful configuration this should show that the SLB or virtual hostname field has been set.

```
$ ./emctl status oms -details
Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.1.0
Copyright (c) 1996, 2011 Oracle Corporation. All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host : omsa.example.com
HTTP Console Port : 7788
HTTPS Console Port : 7799
HTTP Upload Port : 4889
HTTPS Upload Port : 4900
SLB or virtual hostname: slb.example.com
HTTPS SLB Upload Port : 4900
HTTPS SLB Console Port : 443
Agent Upload is locked.
OMS Console is unlocked.
Active CA ID: 1
Console URL: https://slb.example.com:443/em
Upload URL: https://slb.example.com:4900/empbs/upload

WLS Domain Information
Domain Name : GCDomain
Admin Server Host: omsa.xxx.xxx.xxx

Managed Server Information Managed Server Instance Name: EMGC_OMS1
Managed Server Instance Host: omsa.xxx.xxx.xxx
```

Document Revision History

Version	Description	Date
1.0	New document	05/01/2012

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com