ORACLE ENTERPRISE MANAGER 13c

# Enterprise Manager 13c Cloud Control

## Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager

ORACLE WHITE PAPER | APRIL 2016

ORACLE

## Table of Contents


Introduction 1

Goals of this document 2

High Availability 2

F5 BIG-IP LTM and Oracle Enterprise Manager Cloud Control 3

Configuring an F5 BIG-IP LTM for Cloud Control Services 4

Detailed Configuration Instructions 5

- Prerequisites and Best Practice Recommendations 5
  - Use BIG-IP Administrative Partitions 5
  - Use the Configuration Table and Standard Naming Conventions 5
- Port Usage on the Individual Enterprise Manager Hosts 6
- Ports on the F5 BIG-IP LTM 6
- Methodology 7
  - Create the Health Monitors 8
  - Create the Cloud Control Pools 10
  - Create the TCP Profiles 12
  - Create the Persistence Profiles 13
  - Create a Redirect iRule for the Unsecure Console service 14
  - Create the Virtual Servers 15

Example Network Map for a Fully-Configured F5 BIG-IP LTM 18

Configuring Enterprise Manager for Use with the F5 BIG-IP LTM 19

- Resecure Management Services (OMS) 19
  - Resecure OMS in locked mode 19

Restart Enterprise Manager 19
Configure the Interface between the Oracle Management Service and BI Publisher 20
Resecure all Management Agents 20
Verify Status of Management Service 21
Configure Always-On Monitoring 22
Appendix A: F5 BIG-IP Local Traffic Manager Terms 23
Monitor 23
Pool 23
Member 23
Virtual Server 23
Profile 24
Persistence 24
Rule 24

## Introduction

Oracle Enterprise Manager Cloud Control is Oracle's integrated management platform that provides the industry's first complete cloud lifecycle management solution. Oracle Enterprise Manager's business-driven IT Management capabilities allow customers to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments.

Enterprise Manager allows customers to achieve:

- Best service levels for traditional, on premise applications, as well as for cloud-based applications, including Oracle Fusion Applications.
- Maximum return on IT management investment, through optimized management of the Oracle stack, as well as Oracle engineered systems.
- An unmatched customer support experience, using the real-time integration of Oracle's knowledge base in each customer's environment.

Oracle Maximum Availability Architecture (MAA) is the Oracle best practices blueprint for implementing Oracle high-availability technologies. Oracle Corporation and F5 Networks have jointly written this white paper. This white paper provides the detailed steps for implementation of an Oracle MAA solution for Oracle Enterprise Manager Cloud Control, using BIG-IP Local Traffic Manager from F5 Networks as the front end for the Cloud Control mid-tiers. The BIG-IP hardware platform can provide load balancing, high availability, service monitoring, TCP/IP enhancements, and application persistence for the Enterprise Manager Cloud Control environment.

Most of the procedures in this document are performed on the BIG-IP Local Traffic Manager (LTM). These procedures target different areas of the Enterprise Manager infrastructure. Additionally, these procedures provide high availability, to ensure continuous access for the mission critical Enterprise Manager components.

The Enterprise Manager components consist of the following applications:

- Oracle Management Service (OMS)
- Java Virtual Machine Diagnostics (JVMD)
- BI Publisher (BIP)
- Always-On Monitoring (AOM)

## Goals of this document

This paper introduces Cloud Control administrators to the high availability and load balancing features available with F5 solutions. Step-by-step configuration instructions and screen shots are provided to make it easier to understand and implement BIG-IP as a critical component of the Enterprise Manager Cloud Control architecture. The following software versions were used in the creation of this white paper:

» Enterprise Manager Cloud Control 13c Release 1
» BI Publisher 12.1.3, as shipped with Enterprise Manager 13c Release 1
» BIG-IP 11.6.0

*Note: This white paper assumes familiarity with BIG-IP from F5 Networks. See Appendix A for a summary of F5 BIG-IP Local Traffic Manager terminology. For detailed information, see the BIG-IP Solutions Guide and BIG-IP Configuration Guide and Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.*

## High Availability

In Enterprise Manager 13c Release 1, High Availability is supported for BI Publisher, Java Virtual Machine Diagnostics (JVMD), and Always-On Monitoring (AOM). BI Publisher is automatically installed and configured along with Enterprise Manager 13c Release 1.

*Note: Always-On Monitoring (AOM) is installed and configured separately from Enterprise Manager.*

In an Enterprise Manager 13c Release 1 High Availability environment, individual Enterprise Manager systems can run any of the below component configurations, and the F5 BIG-IP will properly manage traffic to the individual Enterprise Manager system component. For a given Enterprise Manager system **x**, the following configurations are supported.

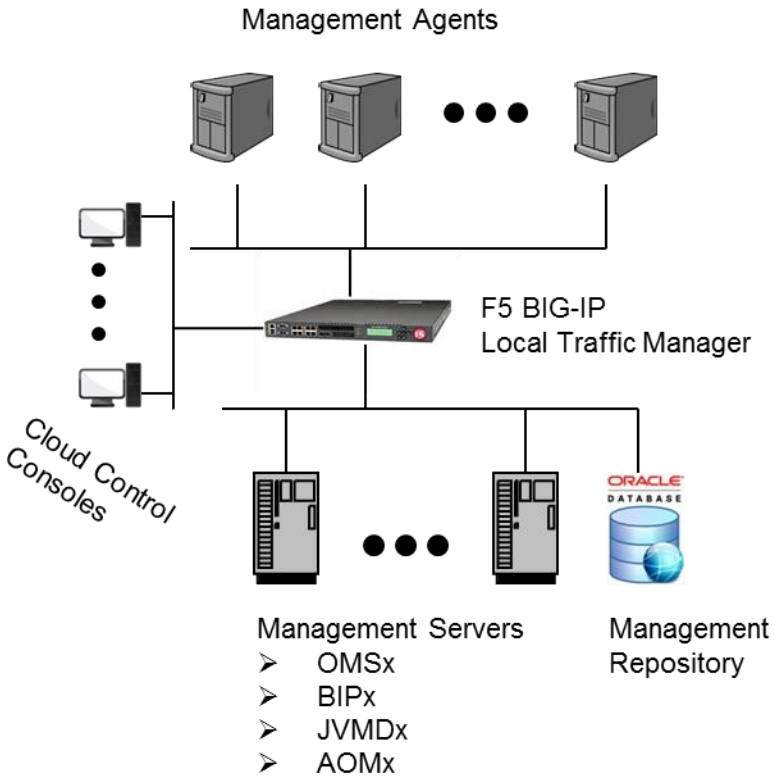
- OMS**x, JVMDx** and BIP**x** (standard configuration). Also, AOM**x** (if configured).
- OMS**x, JVMDx** and AOM**x** (if configured), (no BIP**x**).
- BIP**x** only (no OMS**x**, no JVMDx,no AOM**x**).
- None (An Enterprise Manager system is completely down).

*Note: The first BI Publisher server, running on the primary OMS system, is named 'BIP' and not 'BIP1'.*

## F5 BIG-IP LTM and Oracle Enterprise Manager Cloud Control

The diagram below shows how the F5 BIG-IP LTM is deployed within an Oracle Enterprise Manager environment.

Enterprise Manager 13c Cloud Control High Availability Architecture



## Configuring an F5 BIG-IP LTM for Cloud Control Services

Oracle Enterprise Manager components provide Cloud Control clients, including the Cloud Control console, BI Publisher console, and Management Agents, HTTP or HTTPS access, to the set of Cloud Control services listed below. When more than one Cloud Control OMS Server, BI Publisher server, and Always-On Monitoring server (if configured), are deployed, the F5 BIG-IP LTM can load balance requests for each service (OMS, BIP, and AOM). This load balancing is achieved via virtual servers, with the Cloud Control clients making service requests using a virtual hostname.

The table below shows the Cloud Control services that can be served by the F5 BIG-IP in an Enterprise Manager installation containing multiple Enterprise Manager systems. The items in italics are **not recommended**, as they are by definition, insecure.

| Cloud Control Service | Description | Conventional Port |
|---|---|---|
| Secure Console | HTTPS access to Cloud Control Console | 443 |
| *Unsecure Console* | HTTP access to Cloud Control Console (not recommended) | 80 |
| Secure BI Publisher | HTTPS access to Cloud Control BI Publisher | 5443 |
| *Unsecure BI Publisher* | HTTP access to Cloud Control BI Publisher (not recommended) | 8080 |
| Secure Upload | Secure Agent to OMS communication | 4900 |
| Agent Registration | Unsecure Agent to OMS communication | 4889 |
| Secure Always-On Monitoring Upload | Secure Agent to AOM communication | 8081 |
| Secure JVMD | Secure JVMD | 7301 |
| Unsecure JVMD | Unsecure JVMD | 7202 |

Each Cloud Control service that is managed by the F5 BIG-IP Local Traffic Manager requires configuration of the following F5 BIG-IP Local Traffic Manager objects:

- A health monitor for the service.

  The health monitor is the process by which the BIG-IP LTM determines whether the service is up and running and can take connections.

- A TCP profile for the service.

  The TCP profile is used to tune the TCP/IP stack from the BIG-IP LTM for optimum performance.

- A pool for the service.

  A pool is a group of two or more OMS Cloud Control servers that are load balanced, with each pool running an instance of the different Cloud Control services.

- A persistence profile for the service.

  The persistence profile is used to link a client to the proper Cloud Control pool member for the duration of a connection. This is required for all Cloud Control services except Secure Upload.

- A virtual server for the service.

  A virtual server is a unique IP address and port that represents a pool of servers.

The remainder of this paper provides detailed instructions for configuring the F5 BIG-IP LTM to manage Cloud Control services.

Each of the configuration discussions consists of:

- Operational best practices when using the F5 BIG-IP Web configuration utility to configure Oracle Enterprise Manager Cloud Control services.
- Screen shots of the BIG-IP Web interface that are based on BIG-IP Version 11.6.0 software.
- A Configuration Summary page naming all of the Cloud Control services and corresponding F5 configuration objects.

## Detailed Configuration Instructions

*For additional information about configuring BIG-IP, see the BIG-IP documentation at http://www.f5.com.*

The following section discusses how to configure Oracle Enterprise Manager Cloud Control to work with the F5 BIG-IP LTM.

### Prerequisites and Best Practice Recommendations

Use the following general guidelines when building the configuration.

#### Use BIG-IP Administrative Partitions

BIG-IP Administrative Partitions allow multiple administrators or operators to manage the configuration. The best practice recommendation is to create a dedicated Administrative Partition on the BIG-IP for configuration access and use by the Cloud Control administrators. All the necessary F5 BIG-IP configuration objects for the MAA Cloud Control environment are located in the Administrative Partition. Additions, deletions, and changes to these pools created in this partition would not interfere with any other services provided by the BIG-IP

For more information about configuring Administrative Partitions, see the BIG-IP documentation.

#### Use the Configuration Table and Standard Naming Conventions

For instructional consistency, this white paper uses a standard naming convention for the BIG-IP LTM configuration. Options include using an organization's existing naming standards (which a network operations team can provide if necessary), creating new naming conventions, or adopting the naming convention used in this white paper.

The following table shows the naming conventions used by the examples described in this white paper.

| BIG-IP Configuration Object | Convention |
|---|---|
| Health Monitors | mon_<service_label>[bip \| aom \| jvmd] |
| TCP Profiles | tcp_<service_label>[bip \| aom \| jvmd] |
| Pools | pool_<service_label>[bip \| aom \| jvmd] |
| Cookie Persistence Profile | cookie_<service_label> |
| Source IP Address Persistence Profile | sourceip_<service_label>[bip \| aom \| jvmd] |
| Virtual Server | vs_<service_label>[bip \| aom \| jvmd]<port> |

As an example, the Secure Console services (for both OMS and BIP) use "ccsc" as the service label. The Secure Console service for BIP uses "bip" as the suffix.

There are TCP/IP port numbers associated with Enterprise Manager services on the individual hosts. There are also TCP port numbers associated with the virtual servers on the F5 BIG-IP LTM itself.

## Port Usage on the Individual Enterprise Manager Hosts

Below are the ports used on the individual Enterprise Manager hosts, which can only be directly accessed by not providing the load balancer hostname. These ports can be, and often are, different than these default values.

| Port | Service Description |
|---|---|
| 7799 | Cloud Control Secure Console Port |
| 9851 | Cloud Control Secure BI Publisher Port (OHS HTTPS SSL Port) |
| 7788 | Cloud Control Unsecure Console Port |
| 9788 | Cloud Control Unsecure BI Publisher Port (OHS HTTP Port) |
| 4900 | Cloud Control Secure Upload Port. |
| 4889 | Cloud Control Agent Registration Port (Enterprise Manager Upload HTTP Port) |
| 8081 | Always-On Monitoring Secure Upload Port |
| 7301 | Cloud Control Secure JVMD Port (Managed Server HTTP SSL Port) |
| 7202 | Cloud Control Unsecure JVMD Port (Managed Server HTTP Port) |

## Ports on the F5 BIG-IP LTM

These are the ports that are accessible directly by Enterprise Manager administrators. When the F5 BIG-IP LTM is configured, any ports can be chosen for these:

| Port | Description |
|---|---|
| 443 | Cloud Control Secure Console (Note: 443 is the default SSL port, so it is not necessary to provide it in the URL) |
| 5443 | Cloud Control Secure BI Publisher Port (Note: Enterprise Manager administrators will typically not need to reference this port directly, since the list of BI Publisher reports that are shown in Enterprise Manager will automatically have this port embedded in them. |
| 4900 | Cloud Control Secure Upload |
| 8081 | Always-On Monitoring Secure Upload Port |
| 7301 | Cloud Control Secure JVMD |

*Note: A Virtual Server port can be different than the ports on the individual Enterprise Manager hosts, as is the case in this example.*

Configuring port 443 for the Secure Console Virtual Server port allows HTTPS console access without specifying a port number. So, for example, the virtual server name for the Enterprise Manager Secure Console would be vs_ccsc443, and the name for the Enterprise Manager Secure Console pool would be pool_ccsc.

This is true even though the Cloud Control Secure Console is running on port 7799. When the F5 BIG-IP LTM is configured using the following instructions, it forwards the request from the Virtual Server to the correct port on the OMS servers.

Additionally, if the iRule is defined, as shown in section VI, Enterprise Manager can be accessed directly by simply providing the hostname of the load balancer. This will default to unsecure access, on the default HTTP port, which is 80. The iRule will properly forward this to the load balancer on the default HTTPS port, which is 443.

The following table lists all F5 BIG-IP LTM configuration objects used throughout the rest of this white paper.

| Cloud Control Service | TCP Port | Monitor Name | TCP Profile Name | Persistence Profile | Pool name | Virtual Server Name | Virtual Server Port |
|---|---|---|---|---|---|---|---|
| Secure Console | 7799 | mon_ccsc | tcp_ccsc | sourceip_ccsc | pool_ccsc | vs_ccsc443 | 443 |
| Secure BI Publisher | 9851 | mon_ccscbip | tcp_ccscbip | sourceip_ccscbip | pool_ccscbip | vs_ccscbip5443 | 5443 |
| Unsecure Console | 7788 | mon_ccuc | tcp_ccuc | sourceip_ccuc | pool_ccuc | vs_ccuc80 | 80 |
| Unsecure BI Publisher | 9788 | mon_ccucbip | tcp_ccucbip | sourceip_ccucbip | pool_ccucbip | vs_ccucbip8080 | 8080 |
| Secure Upload | 4900 | mon_ccsu | tcp_ccsu | None | pool_ccsu | vs_ccsu4900 | 4900 |
| Agent Registration | 4889 | mon_ccar | tcp_ccar | cookie_ccar | pool_ccar | vs_ccar4889 | 4889 |
| Always-On Monitoring Secure Upload | 8081 | mon_ccaom | tcp_ccaom | None | pool_ccaom | vs_ccaom8081 | 8081 |
| Secure JVMD | 7301 | mon_ccsjvmd | tcp_ccsjvmd | sourceip_ccsjvmd | pool_ccsjvmd | vs_ccsjvmd7301 | 7301 |
| Unsecure JVMD | 7202 | mon_ccujvmd | tcp_ccujvmd | sourceip_ccujvmd | pool_ccujvmd | vs_ccujvmd7202 | 7202 |

## Methodology

To configure BIG-IP LTM for Cloud Control, it is necessary to create health monitors, load balancing pools, persistence profiles and virtual server configuration objects for the Cloud Control services listed in the above table. The following sections describe how to create and configure each of the configuration objects, providing a reference table with the required settings for each of the Cloud Control services, followed by a detailed example, including screenshots, using the Secure Console service as an example. The steps in each section should be repeated for each of the Cloud Control services.

### Create the Health Monitors

| Cloud Control Service | TCP Port | Monitor Name | Type | Interval | Timeout | Send String | Receive String |
|---|---|---|---|---|---|---|---|
| Secure Console (when **not** using SSO) | 7799 | mon_ccsc | HTTPS | 5 | 16 | `GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n` | `Enterprise Manager Console is UP` |
| Secure BI Publisher | 9851 | mon_ccscbip | HTTPS | 5 | 16 | `GET /xmlpserver/services HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n` | `And now... Some Services` |
| Unsecure Console (when **not** using SSO) | 7788 | mon_ccuc | HTTP | 5 | 16 | `GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n` | `Enterprise Manager Console is UP` |
| Unsecure BI Publisher | 9788 | mon_ccucbip | HTTP | 5 | 16 | `GET /xmlpserver/services HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n` | `And now... Some Services` |
| Secure Upload | 4900 | mon_ccsu | HTTPS | 60 | 181 | `GET /empbs/upload \r\n` | `Http Receiver Servlet active!` |
| Agent Registration | 4889 | mon_ccar | HTTP | 60 | 181 | `GET /empbs/genwallet \r\n` | `GenWallet Servlet activated` |
| Always-On Monitoring Secure Upload | 8081 | mon_ccaom | HTTPS | 60 | 181 | `GET /upload \r\n` | `Always On Monitoring is active` |
| Secure JVMD | 7301 | mon_ccsjvmd | HTTPS | 60 | 181 | `GET /jamservlet/comm\r\n` | `Reply to empty request` |
| Unsecure JVMD | 7202 | mon_ccujvmd | HTTP | 60 | 181 | `GET /jamservlet/comm\r\n` | `Reply to empty request` |

*The following steps should be followed for each health monitor that needs to be created:*

1. On the **Main** tab, expand **Local Traffic**, and then click **Monitors**.
2. On the **Monitors** screen, click **Create**.

   The New Monitor screen opens.
3. In the **Name** field, enter a unique name for the Monitor. For example: mon_ccsc
4. From the **Type** list, select the type for the Monitor. For example: HTTPS.
5. The Monitor configuration options display.From the **Configuration** list, select **Advanced**.
6. In the Configuration section, enter the appropriate values in Interval and Timeout fields:
   - **Interval** is the health monitor property that specifies the frequency at which the system issues the monitor check.
   - **Timeout** is the setting that allows the health monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * “Interval”) + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

   For example, set Interval to 5 and set Timeout to 16. Refer to the table above for the appropriate Interval and Timeout values for the monitor.
7. In the **Send String** field, add the Send String for the Monitor.

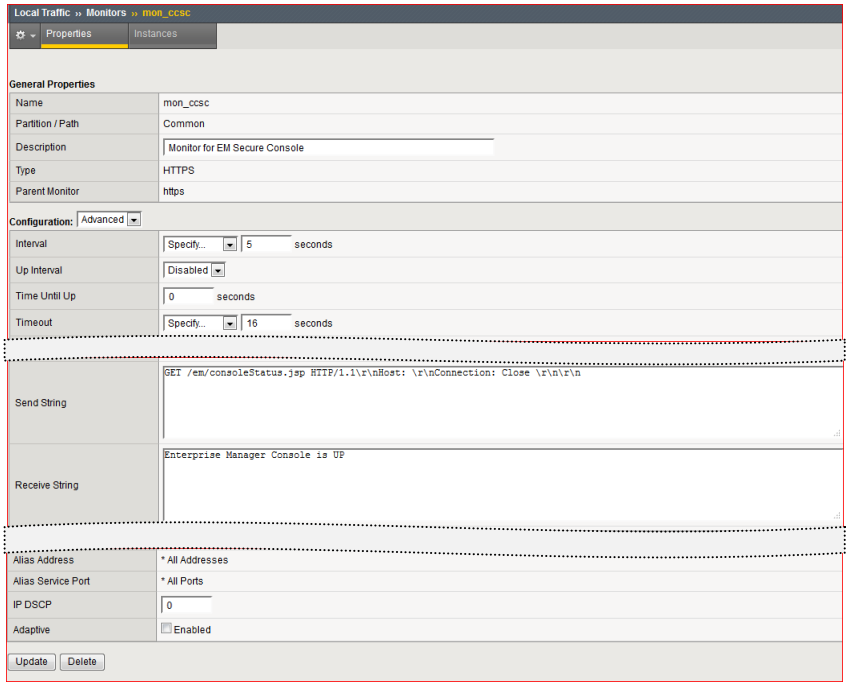
   For example:

   ```
   GET /em/consoleStatus.jps HTTP/1.1\r\nHost: \r\nConnection: Close \r\n\r\n
   ```
8. In the **Receive String** field, add the Receive String for the Monitor.

   For example:

   ```
   Enterprise Manager Console is UP
   ```

   All other configuration settings are optional.
9. Click Finished.




The finished definition of the monitor will look similar to this screen capture.

### Create the Cloud Control Pools

BIG-IP LTM pool is a set of servers grouped together to receive traffic according to a load balancing method. A pool needs to be created for each of the Cloud Control services as per the following table:

| Cloud Control Service | Pool Name | Associated Health Monitor | Load Balancing | Members |
|---|---|---|---|---|
| Secure Console | pool_ccsc | mon_ccsc | Least Connections (member) | OMS Host A:7799<br>OMS Host B:7799 |
| Secure BI Publisher | pool_ccscbip | mon_ccscbip | Least Connections (member) | OMS Host A:9851<br>OMS Host B:9851 |
| Unsecure Console | pool_ccuc | mon_ccuc | Least Connections (member) | OMS Host A:7788<br>OMS Host B:7788 |
| Unsecure BI Publisher | pool_ccucbip | mon_ccucbip | Least Connections (member) | OMS Host A:9788<br>OMS Host B:9788 |
| Secure Upload | pool_ccsu | mon_ccsu | Least Connections (member) | OMS Host A:4900<br>OMS Host B:4900 |
| Agent Registration | pool_ccar | mon_ccar | Least Connections (member) | OMS Host A:4889<br>OMS Host B:4889 |
| Always-On Monitoring Secure Upload | pool_ccaom | mon_ccaom | Least Connections (member) | OMS Host A:8081<br>OMS Host B:8081 |
| Secure JVMD | pool_ccsjvmd | mon_ccsjvmd | Least Connections (member) | OMS Host A:7301<br>OMS Host B:7301 |
| Unsecure JVMD | pool_ccujvmd | mon_ccujvmd | Least Connections (member) | OMS Host A:7202<br>OMS Host B:7202 |

*The following steps should be followed for each Pool that needs to be created:*

1. On the **Main** tab, expand **Local Traffic**, and then click **Pools**.
2. On the **Pools** screen, click **Create**.

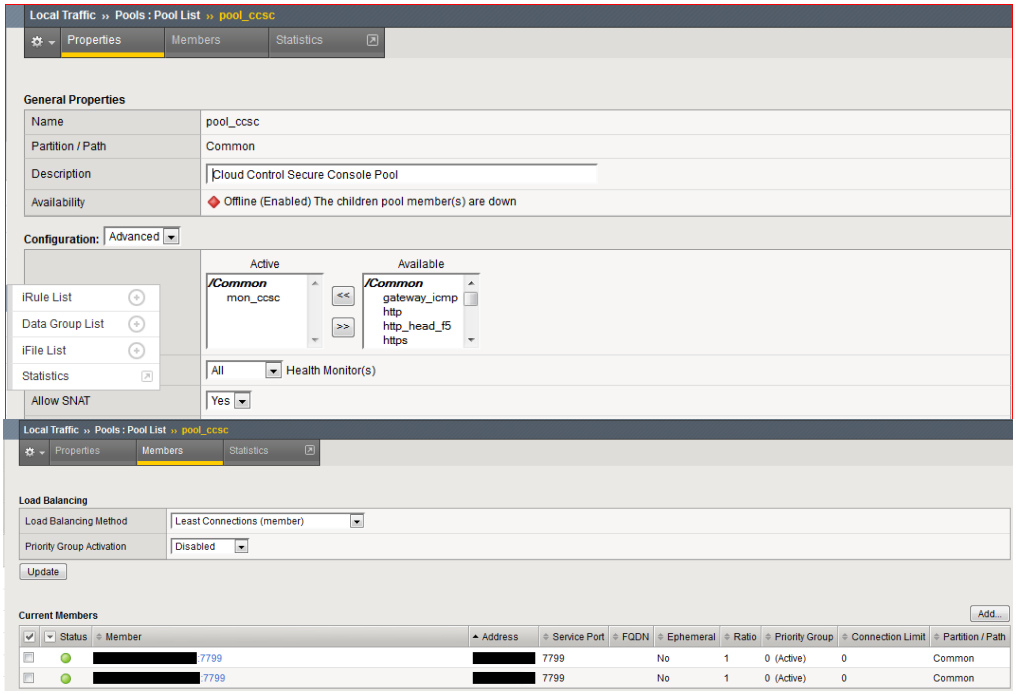
   The New Pool screen opens

   Note: For more (optional) pool configuration settings, from the Configuration list, select Advanced. Configure these settings, as applicable, for the network.
3. In the **Name** field, enter a unique name for the pool.

   For example, enter **pool_ccsc**.
4. In the **Health Monitors** section, select the name of the monitor for the service that the pool is being created for, and click the Add (**<<**) button.

   For example, select mon_ccsc.
5. From the **Load Balancing Method** list, choose the preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

   For example, select **Least Connections (member)**.
6. Keep the **Priority Group Activation** value as **Disabled**.
7. In the **New Members** section, add each OMS host as a member, one at a time, by entering the OMS hostname in the **Node Name** field, the OMS IP address in the **Address** field and the port for the service that the pool is being created for in the **Service Port** field, then clicking **Add**.
8. Click **Finished**.




The finished definition of the pool will look similar to this screen capture.

### Create the TCP Profiles

In this white paper, each TCP profile is based on the default TCP profile, and keeps all the options at their default settings. These options can be configured, as appropriate, for the network. A TCP profile needs to be created for each of the Cloud Control services as per the following table:

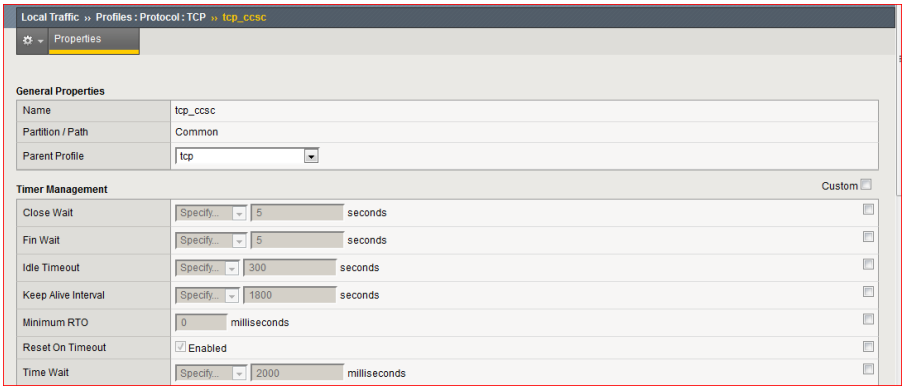
| Cloud Control Service | TCP Profile Name |
|---|---|
| Secure Console | tcp_ccsc |
| Secure BI Publisher | tcp_ccscbip |
| Unsecure Console | tcp_ccuc |
| Unsecure BI Publisher | tcp_ccucbip |
| Secure Upload | tcp_ccsu |
| Agent Registration | tcp_ccar |
| Always-On Monitoring Secure Upload | tcp_ccaom |
| Secure JVMD | tcp_ccsjvmd |
| Unsecure JVMD | tcp_ccujvmd |

*The steps below should be followed for each TCP profile that needs to be created:*

1. On the **Main** tab, expand **Local Traffic**.
2. Click **Profiles**.

   The HTTP Profiles screen opens.
3. On the Menu bar, from the **Protocol** menu, select **TCP**.
4. In the upper-right portion of the screen, click **Create**.

   The New TCP Profile screen opens.
5. In the **Name** field, enter a unique name for this profile. For example: **tcp_ccsc**.
6. If needed, modify as applicable for the network. See the F5 BIG-IP LTM online help for more information about the configuration options. Note that this example keeps the settings at their default levels.
7. Click **Finished**.




The finished definition of the TCP profile will look similar to this screen capture

### Create the Persistence Profiles

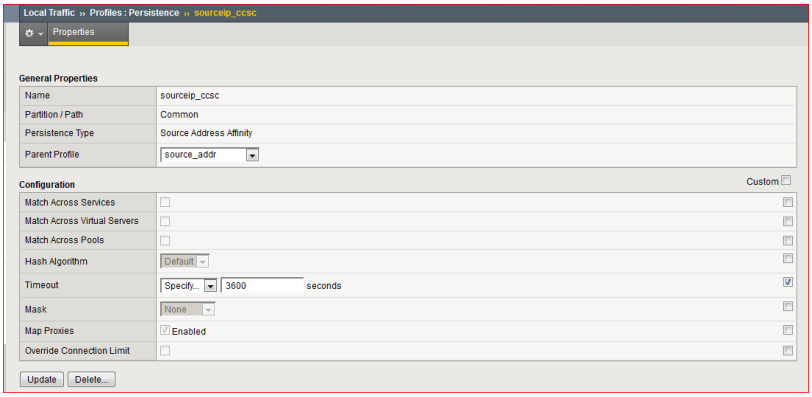
A persistence profile needs to be created for each of the Cloud Control services, except for the two secure upload services (Secure Upload, Always-On Monitoring Secure Upload), as per the following table:

| Cloud Control Service | F5 Persistence Profile Name | Type | Timeout | Expiration |
|---|---|---|---|---|
| Secure Console | sourceip_ccsc | Source Address Affinity | 3600 | Not Applicable |
| Secure BI Publisher | sourceip_ccscbip | Source Address Affinity | 3600 | Not Applicable |
| Unsecure Console | sourceip_ccuc | Source Address Affinity | 3600 | Not Applicable |
| Unsecure BI Publisher | sourceip_ccucbip | Source Address Affinity | 3600 | Not Applicable |
| Agent Registration | cookie_ccar | Cookie | Not Applicable | 3600 |
| Secure JVMD | sourceip_ccsjvmd | Source Address Affinity | 3600 | Not Applicable |
| Unsecure JVMD | sourceip_ccujvmd | Source Address Affinity | 3600 | Not Applicable |

*The steps below should be followed for each persistence profile that needs to be created:*

1. On the Main tab, expand **Local Traffic**, and then click **Profiles**.
   The HTTP Profiles screen opens.
2. On the Menu bar, click **Persistence**.
   The Persistence Profiles screen opens.
3. In the upper-right portion of the screen, click **Create**.
   The New Persistence Profile screen opens.
4. In the Name field, enter a unique name for this profile.
   For example, enter **sourceip_ccsc**.
5. If the persistence type for the service being created is 'Source Address Affinity':
   a. From the Persistence Type list select Source Address Affinity.
      The configuration options for SourceIP persistence display.
   b. Check the box next to the **Timeout** field to allow the Timeout value to be overridden
   c. Modify the **Timeout** value to **3600**.

   If the persistence type for the service being created is 'Cookie':
   a. From the Persistence Type list select **Cookie**
      The configuration options for Cookie persistence display.
   b. Check the box next to the **Expiration** field to allow the Expiration value to be overridden
   c. Clear the **Session Cookie** box.
      The **expiration** options appear.
   d. Provide the value **3600** in the Seconds field.
6. Click Finished.




The finished definition of the persistence profile will look similar to this screen capture

*For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation.*

### Create a Redirect iRule for the Unsecure Console service

*Create a Redirect iRule to provide access to Enterprise Manager without specifying https://*

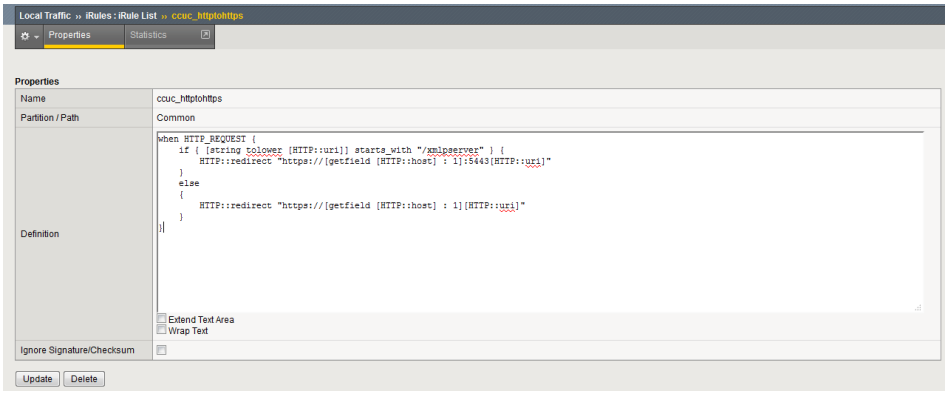
If unsecure access to Enterprise Manager and BI Publisher is not enabled (which is considered best practice), a Redirect iRule can be created to take incoming HTTP requests (non-secure) and redirect those requests to the correct HTTPS (secure) virtual server without user interaction. This will allow users to access Enterprise Manager using the following URL: *slb.example.com/em*, without regard to SSL or non-SSL. This Redirect iRule is used in the configuration of the Cloud Control unsecure console service virtual server, to redirect clients to the matching Cloud Control secure console service. This Redirect iRule will also allow users to access BI Publisher using the following URL: *slb.example.com/xmlpserver/*, without regard to SSL or non-SSL, as it will redirect to the correct HTTPS virtual server for BI Publisher on port 5443.

*The following steps should be followed to create the Redirect iRule*

1. On the Main tab, **expand Local Traffic** and click **iRules**.
2. In the upper right portion of the iRule screen, click **Create**.
3. In the **Name** field on the new iRule screen, enter a name for the iRule. For example, ccuc_**httptohttps**.
4. In the **Definition** section, copy and paste the following iRule:

```
when HTTP_REQUEST {
    if { [string tolower [HTTP::uri]] starts_with "/xmlpserver" } {
        HTTP::redirect "https://[getfield [HTTP::host] : 1]:5443[HTTP::uri]"
    }
    else
    {
        HTTP::redirect "https://[getfield [HTTP::host] : 1][HTTP::uri]"
    }
}
```

5. Click **Finished**.




The finished definition of the iRule will look similar to this screen capture.

### Create the Virtual Servers

The final step is to define virtual servers that reference the profiles and pools created for each Cloud Control service. A virtual server, with its virtual address and port number, is the client-addressable host name or IP address through which members of a load balancing pool are made available to a client. A virtual server needs to be created for each of the Cloud Control services as per the following table. The table below uses the default ports for HTTP (80) and HTTPS (443). Also, users will not usually access BI Publisher directly, but instead will be directed to the correct virtual server from the list of BI Publisher reports inside of Enterprise Manager. In the table below, VIP is the Virtual IP Address used on the F5 VLAN.

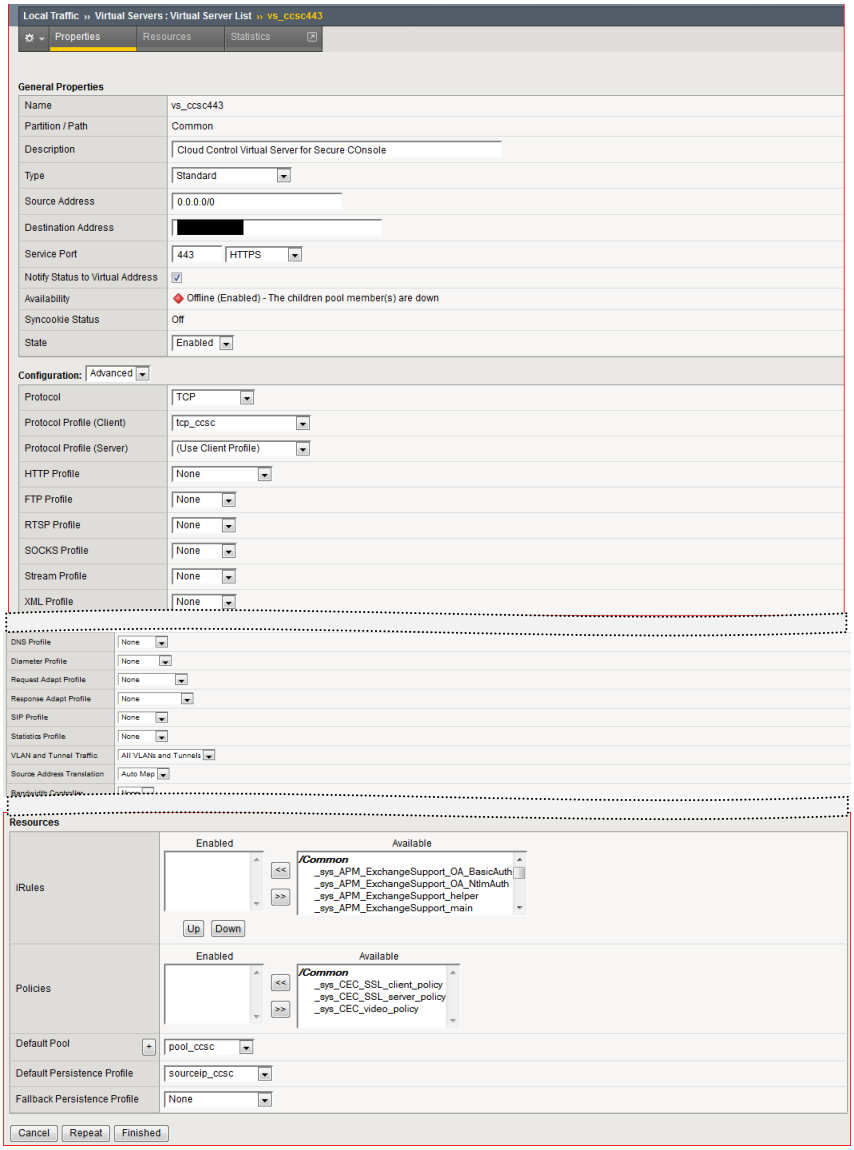
*Required Virtual Servers*

| Cloud Control Service | Virtual Server Name | Virtual IP and Port | Protocol Profile (Client) | HTTP Profile | Source Address Translation | iRule | Default Pool | Default Persistence Profile |
|---|---|---|---|---|---|---|---|---|
| Secure Console | vs_ccsc443 | VIP:443 | tcp_ccsc | None | Auto Map | None | pool_ccsc | sourceip_ccsc |
| Secure BI Publisher | vs_ccscbip5443 | VIP:5443 | tcp_ccscbip | None | Auto Map | None | pool_ccscbip | sourceip_ccscbip |
| Unsecure Console * | vs_ccuc80 | VIP:80 | tcp_ccuc | http | Auto Map | *ccuc_httptohttps* | pool_ccuc | sourceip_ccuc |
| Unsecure BI Publisher * | vs_ccucbip8080 | VIP:8080 | tcp_ccucbip | http | Auto Map | *ccuc_httptohttps* | pool_ccucbip | sourceip_ccucbip |
| Secure Upload | vs_ccsu4900 | VIP:4900 | tcp_ccsu | None | Auto Map | None | pool_ccsu | None |
| Agent Registration | vs_ccar4889 | VIP:4889 | tcp_ccar | http | Auto Map | None | pool_ccar | cookie_ccar |
| Always-On Monitoring Secure Upload | vs_ccaom8081 | VIP:8081 | tcp_ccaom | None | Auto Map | None | pool_ccaom | None |
| Secure JVMD | vs_ccsjvmd7301 | VIP:7301 | tcp_ccsjvmd | None | Auto Map | None | pool_ccsjvmd | sourceip_ccsjvmd |
| Unsecure JVMD | vs_ccujvmd7202 | VIP:7202 | tcp_ccujvmd | http | Auto Map | None | pool_ccujvmd | sourceip_ccujvmd |

* *Implementing unsecured and unencrypted access to Enterprise Manager is not considered best practice. These virtual servers can be configured with the iRule to redirect unsecure traffic to the secure virtual servers. Do not specify the iRule for these virtual servers if unsecure access is desired.*

*The following steps should be followed for each virtual server that needs to be created:*

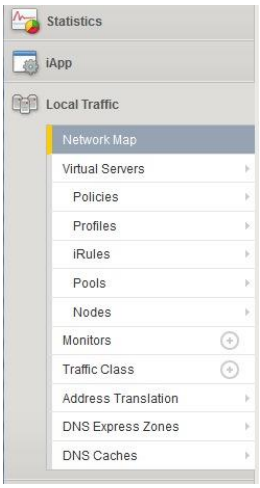
1. On the Main tab, expand **Local Traffic**, and then click **Virtual Servers**.
   The Virtual Servers screen opens.
2. In the upper-right portion of the screen, click the **Create** button.
   The New Virtual Server screen opens.
3. In the **Name** field, enter a unique name for this virtual server.
   For example, enter **vs_ccsc443**.
4. Keep the **Type** list at the default setting: **Standard**.
5. In the **Destination Address** field, enter the IP address of this virtual server.
6. In the **Service Port** field, enter the Virtual IP Port for the service being created.
   For example, port **443**.
7. From the Configuration list, select **Advanced**.
   The Advanced configuration options display.
8. From the **Protocol Profile (Client)** list select the name of the profile for the service being created.
   In this example, select **tcp_ccsc**.
9. Keep **the Protocol Profile (Server)** options at the default setting.
10. For the following virtual servers only, select **http** from the HTTP profile list:
    Agent Registration
    Unsecure Console service (if configured)
    Unsecure BI Publisher service (if configured)
    Unsecure JVMD service (if configured)
11. ***Important***: Change the **Source Address Translation** setting to **Auto Map**.
12. F5 iRule to allow access to Enterprise Manager without specifying https://
    *If not allowing unsecure access to Enterprise Manager an F5-specific iRule can be created to allow convenient access to Enterprise Manager without the need for the Enterprise Manager administrators to specify https:// in the browser address bar.*
    For the Unsecure Console and Unsecure BI Publisher services only, in the **iRules** section, add the iRule created earlier by selecting it in the **Available** list and clicking **<<** to add it to the **Enabled** list.
13. In the Resources section, from the **Default Pool** list, select the pool created for the service that the virtual server is being created for.
    In this example, select **pool_ccsc**.
14. From the **Default Persistence** Profile list, select the persistence profile created for the service that the virtual server is being created for.
    In this example, select **sourceip_ccsc**.
15. Click **Finished**.



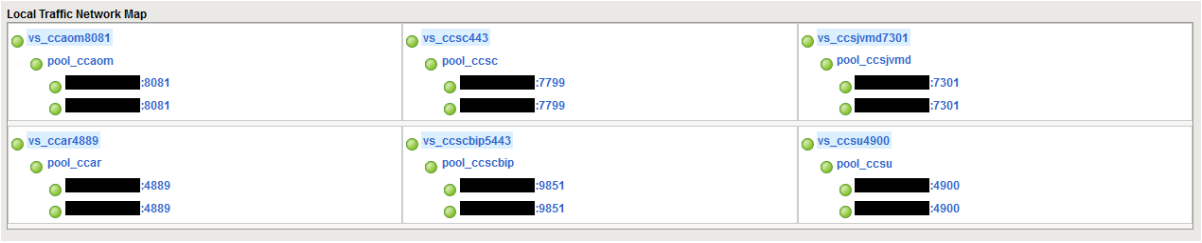

The finished definition of a completed virtual server will look similar to this screen capture.

## Example Network Map for a Fully-Configured F5 BIG-IP LTM

After all the above configurations have been done, click on the link (Network Map) in the BIG-IP Administration console to display the virtual servers created with associated pool of servers for each virtual server.




The screen capture below shows a network map (all the IP addresses in this example have been blurred out):



## Configuring Enterprise Manager for Use with the F5 BIG-IP LTM

### Resecure Management Services (OMS)

The OMS must now be reconfigured so that the Management Service certificate uses the hostname associated with the load balancer. The two steps below must be repeated for each configured OMS.

#### Resecure OMS in locked mode

In this configuration, Enterprise Manager only supports SSL access.

*This is the secure method to run Enterprise Manager, and it is highly recommended that all Enterprise Manager Installations run in SSL mode.*

***Important Note:*** *In order to properly support SLB configuration for JVMD in EM 13.1, patch 22920724 contained in EM 13.1 BP2 is required.*

```
emctl secure oms -host slb.example.com -slb_port 4900 -slb_console_port 443 -
slb_bip_http_port 8080 -slb_bip_https_port 5443 -slb_jvmd_https_port 7301 -
lock_console -lock_upload
Oracle Enterprise Manager Cloud Control 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Securing OMS... Started
Enter Enterprise Manager Root (SYSMAN) Password :
Enter Agent Registration Password :
(c) 1996, 2015 Oracle Corporation.  All rights reserved.
Securing OMS... Started.
Securing OMS... Successful
Restart OMS
```

*If running EM in unlocked mode (not secure), replace* ***-lock_console*** *with* ***-unlock_console*** *and* ***-lock_upload*** *with* ***-unlock_upload***

#### Restart Enterprise Manager

```
emctl stop oms -all
Oracle Enterprise Manager Cloud Control 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Stopping Oracle Management Server...
WebTier Successfully Stopped
Oracle Management Server Successfully Stopped
Oracle Management Server is Down
Stopping BI Publisher Server...
BI Publisher Server Successfully Stopped
AdminServer Successfully Stopped
BI Publisher Server is Down
emctl start oms
Oracle Enterprise Manager Cloud Control 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Starting Oracle Management Server...
WebTier Successfully Started
Oracle Management Server Successfully Started
Oracle Management Server is Up
Starting BI Publisher Server ...
BI Publisher Server Successfully Started
```

```
BI Publisher Server is Up
```

### Configure the Interface between the Oracle Management Service and BI Publisher

New for Enterprise Manager 13.1, access from the Oracle Management Service (OMS) to BI Publisher can go through the F5 BIG-IP LTM. This will ensure that all operations that require this communication will also be routed through F5 BIG-IP LTM URL.

Enable the configuration using the below command.

```
emcli login -username=sysman
Enter Password
emcli sync
emcli setup_bipublisher -force -nodeploy -proto=https -host=slb.example.com
-port=5443 -uri=xmlpserver
BI Publisher "https://slb.example.com:5443/xmlpserver" has been registered
for use with Enterprise Manager
```

*This new capability is supported both when custom third-party certificates are used, as well as when the demonstration (self-signed) certificates are used.*

### Resecure all Management Agents

```
emctl secure agent -emdWalletSrcUrl https://slb.example.com:4900/em
Oracle Enterprise Manager 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Agent successfully stopped...   Done.
Securing agent...   Started.
Enter Agent Registration Password :
Agent successfully restarted...   Done.
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
Enter Enterprise Manager Root (SYSMAN) Password :
Oracle Enterprise Manager Cloud Control 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Console Server Host        : emoms1.example.com
HTTP Console Port          : 7788
HTTPS Console Port         : 7799
HTTP Upload Port           : 4889
HTTPS Upload Port          : 4900
EM Instance Home           : /oracle/gc_inst/em/EMGC_OMS1
OMS Log Directory Location : /oracle/gc_inst/em/EMGC_OMS1/sysman/log
SLB or virtual hostname: slb.example.com
HTTPS SLB Upload Port : 4900
HTTPS SLB Console Port : 443
Agent Upload is locked.
OMS Console is locked.
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      : emoms1.example.com
Admin Server HTTPS Port: 7101
Admin Server is RUNNING

Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS1
Oracle Management Server Instance Host: emoms1.example.com
WebTier is Up
Oracle Management Server is Up

BI Publisher Server Information
BI Publisher Managed Server Name: BIP
BI Publisher Server is Up

BI Publisher HTTP Managed Server Port   : 9701
BI Publisher HTTPS Managed Server Port  : 9803
BI Publisher HTTP OHS Port              : 9788
BI Publisher HTTPS OHS Port             : 9851
BI Publisher HTTPS SLB Port             : 5443
BI Publisher HTTP SLB Port              : 8080
BI Publisher is locked.
BI Publisher Server named 'BIP' running at URL:
https://slb.example.com:5443/xmlpserver
BI Publisher Server Logs:
/oracle/gc_inst/user_projects/domains/GCDomain/servers/BIP/logs/
BI Publisher Log        :
/oracle/gc_inst/user_projects/domains/GCDomain/servers/BIP/logs/bipublish
er/bipublisher.log
```

## Configure Always-On Monitoring

The Always-On Monitoring application must be configured after the OMS has been secured, as it obtains the HTTPS settings from the partner OMS. Refer to the Enterprise Manager Cloud Control Administrator's Guide for details on configuring the Always-On Monitoring application using the emsca utility. The guide also includes specific instructions for reconfiguring existing Always-On Monitoring application instances if they were originally configured without an F5 BIG-IP LTM.

Once Always-On Monitoring has been configured on each server to make use of the F5 BIG-IP LTM, the below command must be run only once, and can be run from any OMS. No Enterprise Manager components must be restarted for this command to take effect.

```
emctl set property -name "oracle.sysman.core.events.emsURL"
-value "https://slb.example.com:8081/upload"
Enter Enterprise Manager Root (SYSMAN) Password :
Oracle Enterprise Manager Cloud Control 13c Release 1
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Property oracle.sysman.core.events.emsURL has been set to value
https://slb.example.com:8081/upload for all Management Servers
OMS restart is not required to reflect the new property value
```

## Appendix A: F5 BIG-IP Local Traffic Manager Terms

This document assumes familiarity with F5 Networks BIG-IP. This section discusses the basic terminology. For a detailed discussion of these terms, see the BIG-IP Solutions Guide and the BIG-IP Configuration Guide. These can be located at https://f5.com.

### Monitor

Monitors are used to verify the operational state of pool members. Monitors verify connections and services on nodes that are members of load-balancing pools. A monitor is designed to check the status of a service on an ongoing basis, at a set interval. If the service being checked does not respond within a specified timeout period, or the status of the service indicates that the performance has degraded, the BIG-IP system automatically takes it out of the pool and will choose the other members of the pool. When the node or service becomes available again, the monitor detects this and the member is automatically accessible to the pool and able to handle traffic. Monitors can be as simple as an ICMP ping to a server's IP address, to a TCP 3-way handshake to a service port, or as sophisticated as an HTTP Get Request with parameters, or SSL session negotiation. F5 monitors can also be custom programmed for specific needs.

### Pool

A pool is a set of servers grouped together to receive traffic on a specific TCP port using a load balancing method. Each pool can have its own unique characteristic for a persistence definition and the load-balancing algorithm used. The preferred setting of the load balance algorithm for all Cloud Control pools is Least Connections (Member). Pools are associated with specific virtual servers directly or by rules (see later). As a result, the traffic coming to a virtual server is directed to one of the associated pools, and ultimately to one of the pool members.

### Member

A member of the pool is defined as a node, as a destination for traffic, with an IP address and a port definition, expressed as a.b.c.d:nn, or 192.168.1.200:80 for a Web server with IP address 192.168.1.200 and listening on port 80. There must be at least two members in every pool to provide high availability. If one of the pool members is unavailable or offline, traffic is sent to the remaining member or members.

### Virtual Server

A virtual server with its virtual IP Address and port number is the client addressable hostname or IP address through which members of a load balancing pool are made available to a client. After a virtual server receives a request, it directs the request to a member of the pool based on a chosen load balancing method. After a virtual server receives traffic, either directly or through a rule, the virtual server can optionally perform a number of different operations, such as inserting or modifying a header into an HTTP request, setting a persistence record, or redirecting the request to another site or fallback destination. Before creating a virtual server, a load balancing pool must be created consisting of the actual physical devices (members) to which to forward the traffic. The virtual server can then be created, specifying that pool as the destination for any traffic coming from this virtual server. If some of the traffic from that virtual server should go to multiple pools based on a pre-determined criterion, then a rule can be created specifying the criteria, and BIG-IP would forward the traffic to a pool matching the rule's criteria. A virtual server is configured to a specific port or to accept "ANY" ports. A given F5 BIG-IP device may contain one or more virtual servers.

### Profile

A profile is an F5 object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as TCP or HTTP connections. BIG-IP version 9.0 and later uses profiles. Using profiles enhances control over managing network traffic, and makes traffic-management tasks easier and more efficient. It also allows for different characteristics to be matched to specific clients or applications. For example, one HTTP profile could be configured for Internet Explorer browsers, a different profile for Mozilla browsers, and yet another profile for hand held mobile browsers. This would provide complete control over all the HTTP options in each profile, to match the characteristics of these different Web browser types.

Although it is possible to use the default profiles, the best practice recommendation is to create new profiles based on the default parent profiles, even if any of the settings are not changed initially. Creating new profiles allows easy modification of the profile settings specific to this deployment, and ensures that the default profile is not accidentally overwritten.

### Persistence

Certain types of applications may require the same client returning to the same pool member, this is called persistence, or “stickiness”. It can be configured using a persistence profile, and applied to the virtual server. For Oracle Cloud Control services, persistence needs to be configured for every service, except for the two secure upload services (Secure Upload, Always-On Monitoring Secure Upload).

### Rule

A rule is a user-written script that uses criteria to choose among one or more pools. In the BIG-IP software, it is called an iRule and provides a powerful and more granular level of control over traffic management. For an incoming request to a virtual server, the iRule is evaluated and selects the pool to which a request will be sent. For more information about F5 iRules, see the F5 DevCentral Web site.

**Oracle Corporation, World Headquarters**
500 Oracle Parkway
Redwood Shores, CA 94065, USA

**Worldwide Inquiries**
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services



ENTERPRISE MANAGER 13C CLOUD CONTROL
Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager
April 2016
Authors: Abramson, Jerry (Oracle), Dhanarani, Angeline (Oracle), Dinkel, Curtis (Oracle), Viscusi, James (Oracle)