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

This whitepaper applies to Enterprise Manager Release 13.4 and F5 BIG-IP Local Traffic Manager 13.1
PURPOSE STATEMENT
This document has been created to serve as an example for the configuration of a server load balancer for use with Oracle Enterprise Manager. This document provides an overview of the requirements for configuring F5 BIG-IP Local Traffic Manager version 13.1 to serve as a server load balancer for Enterprise Manager 13.4.

DISCLAIMER
This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose Statement</td>
<td>1</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Goals of this document</td>
<td>1</td>
</tr>
<tr>
<td>High Availability</td>
<td>1</td>
</tr>
<tr>
<td>F5 BIG-IP LTM and Oracle Enterprise Manager Cloud Control</td>
<td>2</td>
</tr>
<tr>
<td>Architectural Options for Network Configuration</td>
<td>2</td>
</tr>
<tr>
<td>Detailed Diagrams of the Two Architectural Approaches</td>
<td>3</td>
</tr>
<tr>
<td>Standard Configuration: TCP/IP Tunneling</td>
<td>3</td>
</tr>
<tr>
<td>SSL end-to-end with iRules</td>
<td>4</td>
</tr>
<tr>
<td>Configuring an F5 BIG-IP LTM for Cloud Control Services</td>
<td>5</td>
</tr>
<tr>
<td>Outline of required F5 LTM Configuration Objects</td>
<td>6</td>
</tr>
<tr>
<td>Detailed Configuration Instructions</td>
<td>7</td>
</tr>
<tr>
<td>Prerequisites and Best Practice Recommendations</td>
<td>7</td>
</tr>
<tr>
<td>Use BIG-IP Administrative Partitions</td>
<td>7</td>
</tr>
<tr>
<td>Use the Configuration Table and Standard Naming Conventions</td>
<td>7</td>
</tr>
<tr>
<td>Secured Port Usage on the Enterprise Manager Hosts</td>
<td>8</td>
</tr>
<tr>
<td>Ports on the F5 BIG-IP LTM</td>
<td>9</td>
</tr>
<tr>
<td>Methodology</td>
<td>11</td>
</tr>
<tr>
<td>Create the Cloud Control Cipher Rule</td>
<td>11</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control Cipher Group</td>
<td>12</td>
</tr>
<tr>
<td>SSL Client Certificate</td>
<td>13</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control SSL Server Profile</td>
<td>13</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control SSL Client Profile</td>
<td>14</td>
</tr>
<tr>
<td>Create the Health Monitors</td>
<td>15</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control Health Monitors</td>
<td>17</td>
</tr>
<tr>
<td>Create the Cloud Control Pools</td>
<td>19</td>
</tr>
<tr>
<td>Create the TCP Profiles</td>
<td>20</td>
</tr>
<tr>
<td>Create the Persistence Profiles</td>
<td>21</td>
</tr>
<tr>
<td>Create a Redirect iRule for the Unsecure Console service</td>
<td>23</td>
</tr>
<tr>
<td>Create a Redirect iRule to provide access to Enterprise Manager without specifying the https port number</td>
<td>24</td>
</tr>
<tr>
<td>iRule for ‘SSL end-to-end with iRules’ approach</td>
<td>24</td>
</tr>
<tr>
<td>Create the Virtual Servers</td>
<td>25</td>
</tr>
<tr>
<td>Example Network Map for a Fully Configured F5 BIG-IP LTM</td>
<td>29</td>
</tr>
<tr>
<td>Configuring Enterprise Manager Management Servers for the F5 BIG-IP LTM</td>
<td>31</td>
</tr>
<tr>
<td>Secure OMS in locked mode :</td>
<td>31</td>
</tr>
<tr>
<td>Secure OMS in locked mode : ‘SSL end-to-end with iRules’</td>
<td>31</td>
</tr>
<tr>
<td>Stop Enterprise Manager</td>
<td>31</td>
</tr>
<tr>
<td>Start Enterprise Manager</td>
<td>31</td>
</tr>
<tr>
<td>Configure Internal Communication between the OMSs and BI Publisher</td>
<td>32</td>
</tr>
<tr>
<td>SSL end-to-end with iRules</td>
<td>32</td>
</tr>
<tr>
<td>Configure the Enterprise Manager Agents</td>
<td>32</td>
</tr>
<tr>
<td>Resecure all Management Agents</td>
<td>32</td>
</tr>
<tr>
<td>Verify Status of Management Service</td>
<td>32</td>
</tr>
<tr>
<td>Configure Always-On Monitoring</td>
<td>33</td>
</tr>
<tr>
<td>Appendix A: F5 BIG-IP Local Traffic Manager Terms</td>
<td>35</td>
</tr>
<tr>
<td>Monitor</td>
<td>35</td>
</tr>
<tr>
<td>Pool</td>
<td>35</td>
</tr>
<tr>
<td>Member</td>
<td>35</td>
</tr>
</tbody>
</table>

---

Copyright © 2020, Oracle and/or its affiliates | Confidential - Public/Oracle Internal/Oracle Restricted/Oracle Highly Restricted
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 4
- BI Publisher 12.2.1.3, as shipped with Enterprise Manager 13c Release 4
- BIG-IP 13.1

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 4, 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 4.

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

In an Enterprise Manager 13c Release 4 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.

1. OMS\( x \), JVMD\( x \) and BIP\( x \) (standard configuration). Also, AOM\( x \) (if configured).
2. OMS\( x \), JVMD\( x \) and AOM\( x \) (if configured), (no BIP\( x \)).
3. BIP\( x \) only (no OMS\( x \), no JVMD\( x \), no AOM\( x \)).
4. 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 following set of diagrams show two typical approaches to utilize with the BIG-IP.

Each approach has various advantages and disadvantages.

**Architectural Options for Network Configuration**

1. Standard TCP/IP tunneling:
2. This approach lends itself to limiting the resource requirements on the F5 device.
3. This is also a possible approach to take when migrating a single OMS system to be behind the F5 device.
4. In this scenario, the single OMS system would already be configured appropriately.
5. Utilizing this approach requires a separate TCP/IP port for BI Publisher, distinct from the OMS. For example, BI Publisher is accessed over port 9851, and the OMS console using port 443.
6. 3rd Party SSL certificate management is performed on each EM host.
7. SSL end-to-end with iRules:
8. Most resource intensive solution, on both the F5 and the EM systems.
9. 3rd Party SSL Certificate Management needs to be performed both on the F5 and on each EM system.
10. Reliance on proprietary F5 TCL-based iRules.
11. Both the Enterprise Manager Console and BI Publisher are accessed using the default TCP/IP port 443.
12. There are two slight variations in this architectural option.
13. Third party (i.e. Verisign) trusted SSL certificate(s) installed through the environment:
14. Valid SSL certificates on each EM system, for each OMS component:
15. OHS
16. WebLogic Managed Server
17. A valid third-party SSL certificate installed and configured on the F5 BIG-IP LTM.
18. Valid third-party SSL certificates installed on the F5 BIG-IP LTM, and self-signed SSL certificates installed on each EM system, for each OMS component.
Detailed Diagrams of the Two Architectural Approaches

The following detailed diagrams depicting the two approaches described above.

It is important to pay particular attention the often-differing port numbers incoming to the F5 BIG-IP LTM, as opposed to the port numbers on the Enterprise Manager hosts.

Standard Configuration: TCP/IP Tunneling

Figure 1: Enterprise Manager 13c Cloud Control High Availability Architecture – TCP/IP Tunneling
SSL end-to-end with iRules

Figure 2. Enterprise Manager 13c Cloud Control High Availability Architecture: SSL end-to-end with iRules
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). The table below demonstrates a best practice configuration for a Load Balancing front-end.

The Cloud Control clients make service requests using a virtual hostname, such as slb.example.com

In the table below, the list of Cloud Control services, to be managed by the F5 BIG-IP, is shown. The Conventional Ports shown below are the TCP/IP ports on which the F5 BIG-IP LTM will service requests, for the given virtual hostname.

The combination of the single virtual hostname, and the conventional Ports listed, form the server-side components of the TCP/IP connection 4-tuple.

For reference, a TCP/IP 4-tuple is composed of the following:

1. Source address, Source Port #, Destination Address, Destination Port #
2. In the list below, the Destination Address is constant, and is resolved via the DNS hostname: slb.example.com
3. Each Cloud Control Service runs on an independent TCP/IP Port.

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>DESCRIPTION</th>
<th>CONVENTIONAL PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>HTTPS access to Cloud Control Console</td>
<td>443</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>HTTPS access to Cloud Control BI Publisher</td>
<td>5443</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>Secure Agent to OMS communication</td>
<td>4903</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>Unsecure Agent to OMS communication</td>
<td>4889</td>
</tr>
<tr>
<td>Secure Always-On Monitoring Upload</td>
<td>Secure Agent to AOM communication</td>
<td>8081</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>Secure JVMD</td>
<td>7301</td>
</tr>
</tbody>
</table>

Table 1. Conventional TCP/IP Port Numbers on the BIG-IP F5 LTM

The conventional ports listed above are the TCP/IP ports as accessed from the F5 BIG-IP LTM's Virtual Server.

For example, if the Server Load Balancer’s Virtual Server hostname is slb.example.com:

<table>
<thead>
<tr>
<th>BROWSER ACCESS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://slb.example.com/em">https://slb.example.com/em</a></td>
<td>Cloud Control Console</td>
</tr>
</tbody>
</table>
OUTLINE OF REQUIRED F5 LTM CONFIGURATION OBJECTS

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:

1. Ciphers Rules
   a. F5 LTM allows for consistent use of SSL cipher suites using Cipher Rules. These Cipher Rules are in turn referenced from one or more Server SSL Profiles. This is an important consideration when configuring appropriate health monitors for EM components.

2. SSL profiles on the F5: F5 LTM supports two distinct types of SSL profiles.
   a. Client SSL Profiles: These profiles specify the 3rd party SSL certificates to use, as well as the specific details on the supported SSL Ciphers. These profiles are utilized by the F5 system in presenting certificates to client-side browsers.
   b. Server SSL Profiles: These profiles specify any possible client certificates (not often utilized), as well as details on the supported SSL Ciphers between the F5 system, and the Enterprise Manager components.

3. A health monitor for the service.
   a. The health monitor is the process by which the BIG-IP LTM determines whether the service is up and running and can take connections.
   b. New for LTM 13, HTTPS health monitors can reference a specific Server SSL Profile, which in turn can reference a specific Cipher Group, and corresponding Cipher Rule. In this manner, specific restrictions can be specified for communications between the F5 and the Enterprise Manager components.

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

5. A pool for the service.
   a. 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.

6. A persistence profile for the service.
   a. 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.

7. A virtual server for the service.
   a. A virtual server is a unique IP address and port that represents a pool of servers.
   b. If utilizing ‘SSL end-to-end with iRules’, each virtual server must also specify the specific Client SSL Profile.
   c. If utilizing ‘SSL end-to-end with iRules’, each virtual server must also specify the specific Server SSL Profile.

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:

1. Operational best practices when using the F5 BIG-IP Web configuration utility to configure Oracle Enterprise Manager Cloud Control services.
2. Screen shots of the BIG-IP Web interface that are based on BIG-IP Version 13.1 software.
3. A Configuration Summary page naming all 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. Throughout this white paper, all the necessary F5 BIG-IP configuration objects for the Cloud Control environment are located in the Partition named EM_134. Additions, deletions, and changes to the object’s pools created in this partition would not interfere with any other services provided by the BIG-IP LTM.

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.

<table>
<thead>
<tr>
<th>BIG-IP CONFIGURATION OBJECT</th>
<th>CONVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Certificate</td>
<td>slb.example.com</td>
</tr>
<tr>
<td>Cipher Rules</td>
<td>cipher_ccsc</td>
</tr>
<tr>
<td>Cipher Group</td>
<td>cipher_ccsc</td>
</tr>
<tr>
<td>SSL Client Profile</td>
<td>sslclient_ccsc</td>
</tr>
<tr>
<td>SSL Server Profile</td>
<td>sslserver_ccsc</td>
</tr>
<tr>
<td>Health Monitors</td>
<td>mon_&lt;service_label&gt;[bip</td>
</tr>
<tr>
<td>TCP Profiles</td>
<td>tcp_&lt;service_label&gt;[bip</td>
</tr>
<tr>
<td>Pools</td>
<td>pool_&lt;service_label&gt;[bip</td>
</tr>
</tbody>
</table>
Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager 13.1

### Naming Convention for BIG-IP Configuration Objects

<table>
<thead>
<tr>
<th>Cookie Persistence Profile</th>
<th>cookie_&lt;service_label&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address Persistence Profile</td>
<td>sourceip_&lt;service_label&gt;[bip</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>vs_&lt;service_label&gt;[bip</td>
</tr>
</tbody>
</table>

Table 3. Naming Convention for BIG-IP Configuration Objects

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.

The Insecure Console Services (for both OMS and BIP) use “ccuc” as the service label. The Insecure Console service for BIP uses “bip” as the suffix.

### Secured Port Usage on the Enterprise Manager Hosts

In addition to the port numbers shown above, there are TCP/IP port numbers associated with Enterprise Manager services on the individual hosts. These should not be confused with the TCP port numbers associated with the virtual servers on the F5 BIG-IP LTM itself.

Determine the port numbers for your specific configuration by executing the following command, and cross reference the output of the command to the fourth column in the tables below.

**NOTE:** The crossed-out ports would never be open between the SLB and any of the EM hosts.

```
$ emctl status oms -details > /tmp/em_ports.txt
$ grep 'EM Instance Home' /tmp/em_ports.txt
EM Instance Home : /oracle/gc_inst/em/EMGC_OMS1
$ cd /oracle/gc_inst/em/EMGC_OMS1/
$ grep PORT= emgc.properties
EM_UPLOAD_HTTP_PORT=4889
MSPORT=7202
EM_CONSOLE_HTTP_PORT=7788
EM_UPLOADHTTPS_PORT=4903
EM_CONSOLEHTTPS_PORT=7802
MS_HTTPS_PORT=7301
$ grep PORT= embip.properties
BIP_HTTPS_OHS_PORT=9851
BIP_HTTPS_OHS_PORT=9851
```

**Error! Reference source not found.** shows example port numbers for an EM configuration that features secured connections to the various Cloud Control services and would be used for the ‘Standard Configuration: TCP/IP Tunneling’ and ‘SSL end-to-end with iRules’ approaches. The ports listed in **Error! Reference source not found.** will be used in example commands throughout this document.

<table>
<thead>
<tr>
<th>PORT</th>
<th>CLOUD CONTROL SERVICE</th>
<th>DESCRIPTION</th>
<th>CROSS REFERENCE FROM OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>7802</td>
<td>Secure Console</td>
<td>HTTPS browser access to Cloud Control</td>
<td>EM_CONSOLE_HTTPS_PORT</td>
</tr>
<tr>
<td>PORT</td>
<td>DESCRIPTION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Cloud Control Secure Console (Note: 443 is the default SSL port, so it is not necessary to provide it in the URL).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5443 *</td>
<td>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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4903</td>
<td>Cloud Control Secure Upload</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8081</td>
<td>Always-On Monitoring Secure Upload Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7301</td>
<td>Cloud Control Secure JVMD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>Cloud Control Secure Console (Note: 443 is the default SSL port, so it is not necessary to provide it in the URL).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Port cross-reference

Ports on the F5 BIG-IP LTM

To review from ‘Error! Reference source not found.’, below are the ports that are accessible directly by Enterprise Manager administrators, via the F5 BIG-IP LTM Virtual Server.

If approach 2 ‘SSL end-to-end with iRules’ is utilized, along with the associated iRule for ‘SSL end-to-end with iRules’ approach’, then the virtual server on port 5443 is not needed.

A Virtual Server port is often different than the ports on the individual Enterprise Manager hosts.

Detailed examples extrapolated from the above table:

- In the table above, port 443 on the F5 BIG-IP LTM will be redirected to port 7802 on the Enterprise Manager hosts.
- If approach 2 ‘SSL end-to-end with iRules’ is utilized, along with the associated iRule for “SSL end-to-end with iRules’ approach:
- Enterprise Manager administrators will be properly redirected to the correct port (port 7802 for the OMS, or port 9851 for BIP).

  - Similarly, port 5443 on the F5 BIG-IP LTM will be redirected to port 9851 on the Enterprise Manager hosts.
  - Port 4903 on the F5 BIG-IP LTM will be redirected to port 4903 on the Enterprise Manager hosts (the same port is coincidental, and not required).
  - Port 8081 on the F5 BIG-IP LTM will be redirected to port 4903 on the Enterprise Manager hosts.
  - Port 7301 on the F5 BIG-IP LTM will be redirected to port 7301 on the Enterprise Manager hosts (the same port is coincidental, and not required).

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 7802. 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 iRule 1. Unsecure Console Redirect iRule, 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.

F5 BIG-IP LTM configuration objects used throughout the rest of this white paper:

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>TCP PORT [EM HOST]</th>
<th>MONITOR NAME</th>
<th>TCP PROFILE NAME</th>
<th>PERSISTENCE PROFILE</th>
<th>POOL NAME</th>
<th>VIRTUAL SERVER NAME</th>
<th>VIRTUAL SERVER PORT [SLB]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>7802</td>
<td>mon_ccsc</td>
<td>tcp_ccsc</td>
<td>sourceip_ccsc</td>
<td>pool_ccsc</td>
<td>vs_ccsc443</td>
<td>443</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>9851</td>
<td>mon_ccscbiip</td>
<td>tcp_ccscbip</td>
<td>sourceip_ccscbip</td>
<td>pool_ccscbip</td>
<td>vs_ccscbip9851</td>
<td>5443</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>7788</td>
<td>mon_ccuc</td>
<td>tcp_ccuc</td>
<td>sourceip_ccuc</td>
<td>pool_ccuc</td>
<td>vs_ccuc80</td>
<td>80</td>
</tr>
<tr>
<td>Unsecure BI Publisher</td>
<td>9788</td>
<td>mon_ccucbiip</td>
<td>tcp_ccucbip</td>
<td>sourceip_ccucbip</td>
<td>pool_ccucbip</td>
<td>vs_ccucbip8080</td>
<td>8080</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>4903</td>
<td>mon_ccsu</td>
<td>tcp_ccsu</td>
<td>None</td>
<td>pool_ccsu</td>
<td>vs_ccsu4900</td>
<td>4903</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>4889</td>
<td>mon_ccar</td>
<td>tcp_ccar</td>
<td>cookie_ccar</td>
<td>pool_ccar</td>
<td>vs_ccar4889</td>
<td>4889</td>
</tr>
<tr>
<td>Always-On Monitoring</td>
<td>Secure Upload</td>
<td>Secure JVMD</td>
<td>Unsecure JVMD *</td>
<td>8081</td>
<td>7301</td>
<td>7202</td>
<td>8081</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>-------------</td>
<td>----------------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td></td>
<td>mon_ccaom</td>
<td>tcp_ccaom</td>
<td>None</td>
<td>pool_ccaom</td>
<td>vs_ccaom</td>
<td>8081</td>
<td>8081</td>
</tr>
<tr>
<td></td>
<td>tcp_ccsjvmd</td>
<td>sourceip_ccsjvmd</td>
<td>pool_ccsjvmd</td>
<td>vs_ccsjvmd7301</td>
<td>7301</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>mon_ccujvmd</td>
<td>tcp_ccujvmd</td>
<td>sourceip_ccujvmd</td>
<td>pool_ccujvmd</td>
<td>vs_ccujvmd7202</td>
<td>7202</td>
<td></td>
</tr>
</tbody>
</table>

Table 6. Summary of all F5 BIG-IP LTM Configuration Objects

* The insecure BI Publisher and Unsecure JVMD should not be opened up on the F5 BIG-IP LTM under any normal circumstance. No specific documentation steps are provided for these two deprecated items.

**Methodology**

To configure BIG-IP LTM for Cloud Control, you must create health monitors, load balancing pools, persistence profiles and virtual server configuration objects for the Cloud Control services listed in **Error! Reference source not found.** The following sections describe how to create and configure each of the configuration objects, provide reference tables with the required settings for each of the Cloud Control services, and include detailed examples, 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 Cloud Control Cipher Rule**

For both approaches ‘**Error! Reference source not found.**’ and ‘SSL end-to-end with iRules’, create an F5 LTM Cipher specific to the SSL configuration used by Enterprise Manager.

For example, any modern Webserver would limit traffic to TLS1.2, and not support insecure ciphers, such as MD5.

**Complete the following steps to create the Cloud Control Cipher Rule**

1. On the **Main** tab, expand **Local Traffic**.
2. Click Ciphers
3. The Ciphers screen opens.
4. On the Menu bar, from the **Ciphers: Rules** menu, select **Rules**.
5. In the upper-right portion of the screen, click **Create**.
7. In the **Name** field, enter a unique name for this profile. For example: **cipher_ccsc**
8. For the Cipher String, enter a value appropriate for your Enterprise Manager Security Configuration.
9. For example, enter the following cipher string:
10. **!NULL:!MD5:!CAMELLIA:ECDHE:RSA:!SSLV3:!RC4:!EXP:!DES:!3DES:ECDHE_ECDSA**
11. Choose Finished
Detailed steps to create the Cloud Control Cipher Group

For the Error! Reference source not found. ‘SSL end-to-end with iRules’ approach, an F5 LTM Cipher group, referencing the Cipher Rule above, must be created.

**The following steps should be followed to create the Cloud Control Cipher Group**

1. On the Main tab, expand Local Traffic.
2. Click Ciphers
3. The Ciphers screen opens.
5. In the upper-right portion of the screen, click Create.
7. In the Name field, enter a unique name for this profile. For example: `cipher_ccsc`
8. In the Cipher Creation group details section, select the `cipher_ccsc` check box, and then press the << button to move the rule into the list of allowed rules.
9. After the Cipher Rule is moved over, the Cipher Audit section will automatically be updated with the complete list of Cipher Strings.
10. Choose Finished
SSL Client Certificate

If utilizing the ‘SSL end-to-end with iRules’ approach, the BIG-IP F5 LTM will be presenting SSL certificates to clients, such as Web Browsers.

Certificate file management on a BIG-IP F5 LTM device is beyond the scope of this document.

However, for consistency, throughout this document, the following two generic SSL certificate filenames will be utilized:

- **slb.example.com** – A third party certificate, in which all required certificates in the certificate chain, lead up to a root certificate, issued by a trusted, third party, certificate authority (CA). By default, all modern Web Browsers and all Fusion Middleware components, will trust any legitimate certificate Authority.

- **slb-chain** – When utilizing variation ‘18 Third party Certificates install on the F5, and self-signed certificates installed on EM hosts’. It is necessary to install the certificate chain from the individual Enterprise Manager Hosts.

Detailed steps to create the Cloud Control SSL Server Profile

For approach 2 ‘SSL end-to-end with iRules’ approaches, an F5 LTM SSL Server Profile should be created specific to the SSL configuration used by Enterprise Manager.
Complete the following steps to create the Cloud Control SSL Server Profile

1. On the **Main** tab, expand **Local Traffic**.
2. Click **Profiles**
3. The Profile screen opens.
4. On the list of tabs, select the **SSL** tab.
5. In the drop-down menu, select the **Server** option.
6. In the upper-right portion of the screen, click **Create**.
7. The New Server SSL Profile screen opens.
8. In the **Name** field, enter a unique name for this profile. For example: `sslserver_ccsc`
9. Use the default parent profile of `serverssl`
10. In the **Configuration** drop down, choose **Advanced**
11. Choose the appropriate SSL Certificate and Key, for example `slb.example.com`
12. If needed, choose the appropriate **Chain**, for example `slb-chain`
13. Midway down the screen, you will see an entry for **Ciphers**
14. In order to change the default **Cipher Group**, click the check box on the far right, representing a **custom** choice
15. Select the **Cipher Group** radio button.
16. In the drop down, choose the `cipher_ccsc` cipher group.
17. Choose **Finished**

![Figure 5. Example of a finished definition of the Server SSL Profile](image)

Detailed steps to create the Cloud Control SSL Client Profile

If utilizing the 'SSL end-to-end with iRules' approach, an F5 LTM SSL Client Profile should be created specific to the SSL configuration used by Enterprise Manager.
Complete the following steps to create the Cloud Control SSL Client Profile

1. On the Main tab, expand Local Traffic.
2. Click Profiles.
3. The Profile screen opens.
4. On the list of tabs, select the SSL tab.
5. In the drop-down menu, select the Client option.
6. In the upper-right portion of the screen, click Create.
7. The New Client SSL Profile screen opens.
8. In the Name field, enter a unique name for this profile. For example: sslclient_ccsc
9. Use the default parent profile of clientssl
10. In the Configuration drop down, choose Advanced.
11. On the Mode entry, click the check box for Enabled.
12. In order to select Certificate Key Chain, click the check box on the far right, representing a custom choice.
13. Choose the appropriate SSL Certificate and Key if installed onto the F5 BIG-IP LTM.
14. Midway down the screen, you will see an entry for Ciphers
15. In order to change the default Cipher Group, click the check box on the far right, representing a custom choice.
16. Select the Cipher Group radio button.
17. In the drop down, choose the cipher_ccsc cipher group.
18. Choose Finished

Create the Health Monitors

There are two critical components when creating valid health monitors for Enterprise Manager 13.4, with the BIG-IP LTM:

1. The first component involves creating the health monitors using the appropriate type (HTTPS or HTTP), and the correct interval/timeout values.
2. The second component involves setting the exact health monitor strings to use for send/receive health checks.

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>MONITOR NAME</th>
<th>TYPE</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>mon_ccsc</td>
<td>HTTPS</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>mon_ccscbip</td>
<td>HTTPS</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>mon_ccuc</td>
<td>HTTP</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Unsecure BI Publisher</td>
<td>mon_ccucbip</td>
<td>HTTP</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>mon_ccsu</td>
<td>HTTPS</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>mon_ccar</td>
<td>HTTP</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Always-On Monitoring</td>
<td>mon_ccaom</td>
<td>HTTPS</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>mon_ccsjvmd</td>
<td>HTTPS</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Unsecure JVMD</td>
<td>mon_ccujvmd</td>
<td>HTTP</td>
<td>60</td>
<td>181</td>
</tr>
</tbody>
</table>

Table 7. Health Monitors to utilize for Enterprise Manager 13.4

It is critical to exactly copy/paste the health monitor Send String and Receive String values

NOTE: For EM 13.4, case is critical (e.g. HTTP/1.1 instead of http/1.1)
### Detailed steps to create the Cloud Control Health Monitors

1. On the **Main** tab, expand **Local Traffic**, and then click **Monitors**.
2. On the **Monitors** screen, click **Create**.
3. The New Monitor screen opens.
4. In the **Name** field, enter a unique name for the Monitor. For example: mon_ccsc
5. From the **Type** list, select the type for the Monitor. For example: HTTPS.
6. The Monitor configuration options display.
7. From the **Configuration** list, select **Advanced**.
8. 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 mark a member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as \((5 \times \text{"Interval"}) + 1\).
9. For example, set **Interval** to 5 and set **Timeout** to 16.
10. Refer to the table above for the specific **Interval** and **Timeout** values for the monitor.
11. In the **Send String** field, insert the appropriate string for the Monitor being configured.
12. The HTTP header 'Host:' must reference the hostname of the Virtual Server.
13. This hostname must match the SSL certificate being presented by EM.
14. It may also be required that the hostname is DNS resolvable.
15. The HTTP request and headers appear to be case-sensitive for Enterprise Manager 13.4. Please copy/paste above strings exactly as shown.
16. In the **Receive String** field, insert the appropriate string for the Monitor being configured.
17. For approach 2 'SSL end-to-end with iRules' in the **SSL Profile** drop down, choose our Server SSL Profile named **sslserver_ccsc**
18. **IMPORTANT**: For approach 1 'Standard Configuration: TCP/IP Tunneling' the **SSL Profile** drop-down **must show no entries**.
19. **IMPORTANT**: Insure to leave the **Username** and **Password** fields blank.
20. Some browsers will incorrectly auto-fill the **Username** and **Password** field with any possibly saved passwords for the F5 BIG-IP LTM.
21. For simplicity, leave the **Alias Address** field and the **Alias Port** fields at their default values:
   - **Alias Address**: * All Addresses
   - **Alias Port**: * All Ports
22. Click **Update**
The screen shot on the next page provides an example of what a correctly configured health monitor would look like.

In this example, the health monitor for the Cloud Control Secure Console is shown.

![Example of finished definition of a health monitor](image-url)

Figure 7. Example of finished definition of a health monitor
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. Create a for each of the Cloud Control services using the following table:

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>POOL NAME</th>
<th>ASSOCIATED HEALTH MONITOR</th>
<th>LOAD BALANCING</th>
<th>MEMBERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>pool_ccsc</td>
<td>mon_ccsc</td>
<td>Least Connections (member)</td>
<td>OMS Host A:7802 OMS Host B:7802</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>pool_ccsbip</td>
<td>mon_ccscbip</td>
<td>Least Connections (member)</td>
<td>OMS Host A:9851 OMS Host B:9851</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>pool_ccuc</td>
<td>mon_ccuc</td>
<td>Least Connections (member)</td>
<td>OMS Host A:7788 OMS Host B:7788</td>
</tr>
<tr>
<td>Unsecure BI Publisher</td>
<td>pool_ccucbip</td>
<td>mon_ccucbip</td>
<td>Least Connections (member)</td>
<td>OMS Host A:9788 OMS Host B:9788</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>pool_ccsu</td>
<td>mon_ccsu</td>
<td>Least Connections (member)</td>
<td>OMS Host A:4903 OMS Host B:4903</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>pool_ccar</td>
<td>mon_ccar</td>
<td>Least Connections (member)</td>
<td>OMS Host A:4889 OMS Host B:4889</td>
</tr>
<tr>
<td>Always-On Monitoring</td>
<td>pool_ccao</td>
<td>mon_ccao</td>
<td>Least Connections (member)</td>
<td>OMS Host A:8081 OMS Host B:8081</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>pool_ccsjvmd</td>
<td>mon_ccsjvmd</td>
<td>Least Connections (member)</td>
<td>OMS Host A:7301 OMS Host B:7301</td>
</tr>
<tr>
<td>Unsecure JVMD</td>
<td>pool_ccujvmd</td>
<td>mon_ccujvmd</td>
<td>Least Connections (member)</td>
<td>OMS Host A:7202 OMS Host B:7202</td>
</tr>
</tbody>
</table>

Complete the following steps to create each Cloud Control Pool to be configured:

1. On the Main tab, expand Local Traffic, and then click Pools.
2. On the Pools screen, click Create.
3. The New Pool screen opens
4. Note: For more (optional) pool configuration settings, from the Configuration list, select Advanced. Configure these settings, as applicable, for the network.
5. In the Name field, enter a unique name for the pool.
6. For example, enter pool_ccsc.
7. 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.
8. For example, select mon_ccsc.
9. From the Load Balancing Method list, choose the preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
10. For example, select Least Connections (member).
11. Keep the Priority Group Activation value as Disabled.
12. 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.
13. Click Finished.

![Figure 8. Example of finished definition of a F5 pool](image)

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 must be created for each of the Cloud Control services using the following table:

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>TCP PROFILE NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>tcp_ccsc</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>tcp_ccscbip</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>tcp_ccuc</td>
</tr>
<tr>
<td>Unsecure BI Publisher</td>
<td>tcp_ccucbip</td>
</tr>
</tbody>
</table>
Table 9. List of Cloud Control TCP Profiles

<table>
<thead>
<tr>
<th>Service</th>
<th>Profile Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Upload</td>
<td>tcp_ccsu</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>tcp_ccar</td>
</tr>
<tr>
<td>Always-On Monitoring</td>
<td>tcp_ccaom</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>tcp_ccsvm</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>tcp_ccsvjmd</td>
</tr>
<tr>
<td>Unsecure JVMD</td>
<td>tcp_ccujvmd</td>
</tr>
</tbody>
</table>

Complete the following steps for each TCP profile to be created:

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

![Figure 9. Example of a finished definition of a TCP profile](image)

Create the Persistence Profiles

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

<table>
<thead>
<tr>
<th>Cloud Control Service</th>
<th>F5 Persistence Profile Name</th>
<th>Type</th>
<th>Timeout</th>
<th>Expiration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>sourceip_ccsc</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Secure BI Publisher</td>
<td>sourceip_ccscbip</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
<td>------</td>
<td>----------------</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>sourceip_ccuc</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Unsecure BI Publisher</td>
<td>sourceip_ccucbip</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>cookie_ccar</td>
<td>Cookie</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>sourceip_ccsjvmd</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Unsecure JVMD</td>
<td>sourceip_ccujvmd</td>
<td>Source Address Affinity</td>
<td>3600</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

Table 10. List of Cloud Control Persistence Profiles

**Complete the following steps for each persistence profile to be created:**

1. On the Main tab, expand Local Traffic, and then click Profiles.
   a. The HTTP Profiles screen opens.
2. On the Menu bar, click Persistence.
   a. The Persistence Profiles screen opens.
3. In the upper-right portion of the screen, click Create.
   a. The New Persistence Profile screen opens.
4. In the Name field, enter a unique name for this profile.
   a. 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.
   b. The configuration options for SourceIP persistence display.
   c. Check the box next to the Timeout field to allow the Timeout value to be overridden
   d. Modify the Timeout value to **3600**.
6. If the persistence type for the service being created is ‘Cookie’:
   a. From the Persistence Type list select Cookie
   b. The configuration options for Cookie persistence display.
   c. Check the box next to the Expiration field to allow the Expiration value to be overridden
   d. Clear the Session Cookie box.
   i. The expiration options appear.
   e. Provide the value **3600** in the Seconds field.
7. 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 rule to provide access to Enterprise Manager without specifying https:// in the URL. This iRule accepts incoming HTTP requests (non-secure) and redirects 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.

There are slight variations in this iRule, depending on the approach being utilized:

Unsecure Console service Redirect iRule for ‘Standard Configuration: TCP/IP Tunneling’

```bash
when HTTP_REQUEST {
    if { [string tolower [HTTP::uri]] starts_with "/xmlpserver" } {
        HTTP::redirect "https://[getfield [HTTP::host] : 1]:9051[HTTP::uri]"
    }
    else {
        HTTP::redirect "https://[getfield [HTTP::host] : 1][HTTP::uri]"
    }
}
```

iRule 1. Unsecure Console Redirect iRule – TCP/IP Tunneling

Unsecure Console service Redirect iRule for ‘SSL end-to-end with iRules’

```bash
when HTTP_REQUEST {
    HTTP::redirect "https://[getfield [HTTP::host] : 1][HTTP::uri]"
}
```

iRule 2. Unsecure Console Redirect Rule - SSL end-to-end with iRules

1. Redirect iRule Creation Procedures
2. On the Main tab, expand Local Traffic and click iRules.
3. In the upper right portion of the iRule screen, click Create.
4. In the Name field on the new iRule screen, enter a name for the iRule. For example, ccuc_httpstohttps.
5. Copy the appropriate iRule text from the section above and paste it in the Definition section
6. Click Finished.
Create a Redirect iRule to provide access to Enterprise Manager without specifying the https port number

Create a Redirect iRule to accept incoming HTTPS requests (port 443) and redirect those requests to the correct HTTPS (secure) virtual server without user interaction. This will allow users to access Enterprise Manager as well as BI Publisher using the following URLs, respectively: https://slb.example.com/em and https://slb.example.com/xmlpserver

NOTE: F5 requires explicit pool designation, including F5 partition. Even if an iRule is in a partition, for example “EM134”, if a pool is referenced without an explicit partition, a pool in some random partition, with the same matching name, can be chosen. For the purposes of this white paper, all F5 objects are defined in the F5 partition named ‘EM134’.

We have found the italicized blue portions of the below iRule beneficial during debugging. You should remove these debug messages once functionality is confirmed.

**iRule for “SSL end-to-end with iRules’ approach**

```plaintext
when HTTP_REQUEST {
  if { [string tolower [HTTP::uri]] starts_with ”/xmlpserver” } {
    pool /EM134/pool_ccscbip
  } else {
    if { [HTTP::uri] == ”/” } {
      HTTP::redirect "https://[getfield [HTTP::host] : 1]/em"
    } else {
      pool /EM134/pool_ccsc
    }
  }
}

when LB_FAILED {
  log “Selected server [LB::server] did not respond.”
}
```

iRule 3. iRule for SSL end-to-end with iRules
When the iRule above is combined with the prior iRules, the full set of valid URLs will be:

<table>
<thead>
<tr>
<th>URL</th>
<th>CLOUD CONTROL COMPONENT</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://slb.example.com">https://slb.example.com</a></td>
<td>Enterprise Manager Cloud Control Secure Console</td>
</tr>
<tr>
<td><a href="https://slb.example.com/em">https://slb.example.com/em</a></td>
<td>Enterprise Manager Cloud Control Secure Console</td>
</tr>
<tr>
<td><a href="https://slb.example.com/xmlpserver">https://slb.example.com/xmlpserver</a></td>
<td>Enterprise Manager Cloud Control Secure BI Publisher</td>
</tr>
<tr>
<td>slb.example.com</td>
<td>Enterprise Manager Cloud Control Secure (via redirect) Console</td>
</tr>
<tr>
<td>slb.example.com/em</td>
<td>Enterprise Manager Cloud Control Secure (via redirect) Console</td>
</tr>
<tr>
<td>slb.example.com/xmlpserver</td>
<td>Enterprise Manager Cloud Control Secure (via redirect) BI Publisher</td>
</tr>
</tbody>
</table>

**Table 11. Full set of valid URLs**

**Complete the following steps to create the iRule.**

7. On the Main tab, expand Local Traffic and click iRules.
8. In the upper right portion of the iRule screen, click Create.
9. In the Name field on the new iRule screen, enter a name for the iRule. For example, ccsc_emandbip
10. Copy the text in the iRule provided above and paste it into the Definition section.
11. Click Finished.

**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.

Create a virtual server for each of the Cloud Control services using to the appropriate table for your particular approach.

When defining your virtual servers, use the default ports for HTTP (80) and HTTPS (443). For the Virtual Server IP, the term “VIP” refers to the Virtual IP Address used on the F5 VLAN.

*Each Virtual Servers needs to reference either a default pool or an iRule. Ensure that no Virtual Server references both an iRule and a default pool. Error! Reference source not found.*

Reference Table 12 for information to configure the virtual servers for the TCP/IP Tunneling approach. Procedural steps for Virtual Server configuration are in the Section "Virtual Server"
Table 13. BIG-IP F5 LTM Virtual Servers (SSL End-To-End With iRules)

**Virtual Server Creation Procedures**

<table>
<thead>
<tr>
<th>Virtual Server Name</th>
<th>Secure Console and BI Publisher</th>
<th>Unsecure Console</th>
<th>Secure Upload</th>
<th>Agent Registration</th>
<th>Always-On Monitoring</th>
<th>Secure JVMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_ccsc44</td>
<td>vs_ccuc80</td>
<td>vs_ccsu4903</td>
<td>vs_ccar4889</td>
<td>vs_ccaom80</td>
<td>vs_ccsjvmd7301</td>
<td></td>
</tr>
<tr>
<td>Protocol Profile (Client)</td>
<td>tcp_ccsc</td>
<td>tcp_ccuc</td>
<td>tcp_ccsu</td>
<td>tcp_ccar</td>
<td>tcp_ccaom</td>
<td>tcp_ccsjvmd</td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>ssliclient_c</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Client Profile</td>
<td>serverssl-insecure-compatible</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Server Profile</td>
<td>vs_ccsc44</td>
<td>vs_ccuc80</td>
<td>vs_ccsu4903</td>
<td>vs_ccar4889</td>
<td>vs_ccaom80</td>
<td>vs_ccsjvmd7301</td>
</tr>
<tr>
<td>Source Address Translation</td>
<td>Auto Map</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>http</td>
<td>http</td>
<td>None</td>
<td>http</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>iRule</td>
<td>ccsc_emandbip</td>
<td>ccuc_httpthttps</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Default Pool</td>
<td>None</td>
<td>None</td>
<td>pool_ccsu</td>
<td>pool_ccar</td>
<td>pool_ccaom</td>
<td>pool_ccsjvmd</td>
</tr>
<tr>
<td>Default Persistence Profile</td>
<td>sourceip_ccsc</td>
<td>sourceip_ccuc</td>
<td>None</td>
<td>cookie_ccar</td>
<td>sourceip_ccsjvmd</td>
<td></td>
</tr>
</tbody>
</table>

**VIRTUAL SERVER**

<table>
<thead>
<tr>
<th>Secure Console</th>
<th>Secure BI Publisher</th>
<th>Unsecure Console</th>
<th>Secure Upload</th>
<th>Agent Registration</th>
<th>Always-On Monitoring</th>
<th>Secure JVMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsCcsc44</td>
<td>vs_CccsBip98</td>
<td>vs_Ccuc80</td>
<td>vs_CcSu4903</td>
<td>vs_CcAr4889</td>
<td>vs_Ccaom80</td>
<td>vs_Ccsjvmd7301</td>
</tr>
</tbody>
</table>

26 ENTERPRISE MANAGER 13C RELEASE 13.4 CLOUD CONTROL Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager 13.1
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol Profile (Client)</td>
<td>tcp_ccsc</td>
<td>tcp_ccscbip</td>
<td>tcp_ccuc</td>
<td>tcp_ccsu</td>
<td>tcp_ccar</td>
<td>tcp_ccaom</td>
<td>Tcp_ccsjvmd</td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>None</td>
<td>None</td>
<td>http</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Client Profile</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Server Profile</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Source Address Translation</td>
<td>Auto Map</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>iRule</td>
<td>None</td>
<td>None</td>
<td>ccuc_httpthttps¹</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Default Pool</td>
<td>pool_ccsc</td>
<td>pool_ccscbip</td>
<td>None</td>
<td>pool_ccsu</td>
<td>pool_ccar</td>
<td>pool_ccaom</td>
<td>pool_ccsjvmd</td>
</tr>
<tr>
<td>Default Persistence Profile</td>
<td>sourceip_ccsc</td>
<td>sourceip_ccscbip</td>
<td>sourceip_ccuc</td>
<td>None</td>
<td>cookie_ccar</td>
<td>None</td>
<td>Sourceip_ccsjvmd</td>
</tr>
</tbody>
</table>

¹ iRule 1. Unsecure Console Redirect Rule

Table 12. BIG-IP F5 LTM Virtual Servers (TCP/IP Tunneling)
SSL End-to-end Configuration

Reference Table 13 for information to configure the virtual servers for the SSL End-to-End With iRules approach. Procedural steps for Virtual Server configuration are in the Section “

Table 13. BIG-IP F5 LTM Virtual Servers (SSL End-To-End With iRules)

Virtual Server Creation Procedures”
<table>
<thead>
<tr>
<th>Virtual Server Name</th>
<th>Secure Console and BI Publisher</th>
<th>Unsecure Console</th>
<th>Secure Upload</th>
<th>Agent Registration</th>
<th>Always-On Monitoring</th>
<th>Secure JVMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_ccsc443</td>
<td>vs_ccuc80</td>
<td>vs_ccsu4903</td>
<td>vs_ccar4889</td>
<td>vs_ccaom80</td>
<td>vs_ccsjvmd7301</td>
<td></td>
</tr>
<tr>
<td>Protocol Profile (Client)</td>
<td>tcp_ccsc</td>
<td>tcp_ccuc</td>
<td>tcp_ccsu</td>
<td>tcp_ccar</td>
<td>tcp_ccaom</td>
<td>tcp_ccsjvmd</td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>sslclient_c</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Client Profile</td>
<td>serverssl-insecure-compatible</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL Server Profile</td>
<td>vs_ccsc443</td>
<td>vs_ccuc80</td>
<td>vs_ccsu4903</td>
<td>vs_ccar4889</td>
<td>vs_ccaom80</td>
<td>vs_ccsjvmd7301</td>
</tr>
<tr>
<td>Source Address Translation</td>
<td>Auto Map</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTP Profile</td>
<td>http</td>
<td>http</td>
<td>None</td>
<td>http</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>iRule</td>
<td>ccsc_ema ndbip</td>
<td>ccuc_httpsthpps</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Default Pool</td>
<td>None</td>
<td>None</td>
<td>pool_ccsu</td>
<td>pool_ccar</td>
<td>pool_ccaom</td>
<td>pool_ccsjvmd</td>
</tr>
<tr>
<td>Default Persistence Profile</td>
<td>sourceip_csc</td>
<td>sourceip_ccuc</td>
<td>None</td>
<td>cookie_ccar</td>
<td>None</td>
<td>sourceip_ccsjvmd</td>
</tr>
</tbody>
</table>

Table 13. BIG-IP F5 LTM Virtual Servers (SSL End-To-End With iRules)

Virtual Server Creation Procedures

Complete the following steps for each virtual server to be created:

1. On the Main tab, expand Local Traffic, and then click Virtual Servers.
   a. The Virtual Servers screen opens.
2. In the upper-right portion of the screen, click the Create button.
3. In the Name field, enter a unique name for this virtual server.
   a. 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**.
   a. The Advanced configuration options display.
8. From the **Protocol Profile (Client)** list select the name of the profile for the service being created.
   a. 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:
    a. Agent Registration
    b. Unsecure Console service (if configured)
    c. Unsecure BI Publisher service (if configured)
    d. Unsecure JVMD service (if configured)
11. **Important**: Change the Source Address Translation setting to Auto Map.
12. For the Unsecure Console and Unsecure BI Publisher services only:
    a. In the **iRules** section, add the iRule created earlier in ‘Create a Redirect iRule for the Unsecure Console service’ by selecting it in the **Available** list and clicking `<<` to add it to the **Enabled** list.
13. **For the Secure Console**, when utilizing approach 2 ‘SSL end-to-end with iRules’:
    a. In the **iRules** section, add the iRule created earlier in ‘SSL end-to-end with iRules’ approach” by selecting it in the **Available** list and clicking `<<` to add it to the **Enabled** list.
14. In the Resources section, from the **Default Pool** list, select the pool created for the service that the virtual server is being created for.
    a. In this example, select `pool_ccsc`.
15. From the **Default Persistence** Profile list, select the persistence profile created for the service that the virtual server is being created for.
    a. In this example, select `sourceip_ccsc`.
16. 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).

In this particular screenshot, the F5 BIG-IP partition named EM134 is used to isolate all of the specific Enterprise Manager configuration objects.

Additionally, this screenshot demonstrates that the 2nd host is down.

**NOTE:** This screen grab is from a configuration of approach 2 ‘SSL end-to-end with iRules’.
Figure 11. Example Network Map after completed configuration

CONFIGURING ENTERPRISE MANAGER MANAGEMENT SERVERS FOR THE F5 BIG-IP LTM

Reconfigure OMS 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.

Secure OMS in locked mode:

```
emctl secure oms -host slb.example.com -slb_port 4903 -slb_console_port 443 -slb_bip_http_port 9851 -slb_jvmd_http_port 7301 -lock_console -lock_upload
```

Oracle Enterprise Manager Cloud Control 13c Release 4
Copyright (c) ...
Securing OMS... Started

Enter Enterprise Manager Root (SYSMAN) Password:

Copyright (c) ...
Securing OMS... Started.
Securing OMS... Successful

Restart OMS

Secure OMS in locked mode: ‘SSL end-to-end with iRules’

```
emctl secure oms -host slb.example.com -slb_port 4903 -slb_console_port 443 -slb_bip_http_port 443 -slb_jvmd_http_port 7301 -lock_console -lock_upload
-wallet ...
-trust_certs_loc ...
```

Stop Enterprise Manager
emctl stop oms -all
Oracle Enterprise Manager Cloud Control 13c Release 4
Copyright (c) ...  
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

Start Enterprise Manager
emctl start oms
Oracle Enterprise Manager Cloud Control 13c Release 4
Copyright (c) ...  
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 INTERNAL COMMUNICATION BETWEEN THE OMSS AND BI PUBLISHER

Error! Reference source not found.
emcli login -username=sysman
Enter Password
emcli sync
emcli setup_bipublisher -force -nodeploy -proto=https -host=slb.example.com -port=9851 -uri=xmlpserver
BI Publisher "https://slb.example.com:9851/xmlpserver" has been registered for use with Enterprise Manager

SSL end-to-end with iRules
emcli login -username=sysman
Enter Password
emcli sync
emcli setup_bipublisher -force -nodeploy -proto=https -host=slb.example.com -port=443 -uri=xmlpserver
BI Publisher "https://slb.example.com:443/xmlpserver" has been registered for use with Enterprise Manager

CONFIGURE THE ENTERPRISE MANAGER AGENTS

Resecure all Management Agents
emctl secure agent -emdWalletSrcUrl https://slb.example.com:4903/en
Oracle Enterprise Manager 13c Release 4
Copyright (c) ...  
Agent successfully stopped...  Done.
Securing agent...  Started.
Enter Agent Registration Password :
Agent successfully restarted...  Done.
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.

eemctl status oms -details

Enter Enterprise Manager Root (SYSMAN) Password :

Oracle Enterprise Manager Cloud Control 13c Release 4
Copyright (c) ...

Console Server Host : emoms1.example.com
HTTP Console Port   : 7788
HTTPS Console Port  : 7799
HTTP Upload Port    : 4889
HTTPS Upload Port   : 4903
OMS Log Directory Location : /oracle/gc_inst/em/EMGC_OMS1
SLB or virtual hostname: slb.example.com
HTTPS SLB Upload Port : 4903
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:4903/empbs/upload

WLS Domain Information
Domain Name          : GCDomain
Admin Server Host    : emoms1.example.com
Admin Server HTTPS Port: 7102
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 : 9851
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/bipublisher/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 4
Copyright (c) ...

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 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 handheld 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).

iRule
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.

Cipher
A Cipher is a specific encryption algorithm utilized during Transport Layer Security processing of HTTPS requests.

Cipher Suite
A Cipher Suite is a set of Ciphers that secure communication between network clients utilizing Transport Layer Security (TLS) for HTTPS requests.

Transport Layer Security
Transport Layer Security (TLS), and the deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over TCP/IP network connections.

There are several versions of TLS, such as TLS1.0, TLS1.1, etc.

Each subsequent TLS version is considered more secure than its predecessors.

Cipher Group
A Cipher Group is an F5 object that is references a particular Cipher Suite.

Cipher Rule
A Cipher Rule is an F5 object that references both a Cipher Group, and specific TLS protocol requirements.
Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager

July 2020