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

This whitepaper applies to Enterprise Manager Release 13.5 with 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 13.5.

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>2</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>2</td>
</tr>
<tr>
<td>Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling).</td>
<td>3</td>
</tr>
<tr>
<td>SSL Proxying (formerly known as 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>Ciphers Rules and Cipher Groups</td>
<td>6</td>
</tr>
<tr>
<td>SSL profiles, on the F5</td>
<td>6</td>
</tr>
<tr>
<td>health monitors</td>
<td>6</td>
</tr>
<tr>
<td>TCP profiles</td>
<td>6</td>
</tr>
<tr>
<td>Nodes</td>
<td>6</td>
</tr>
<tr>
<td>Pools</td>
<td>6</td>
</tr>
<tr>
<td>Persistence Profiles</td>
<td>6</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>6</td>
</tr>
<tr>
<td>Detailed Configuration Instructions</td>
<td>8</td>
</tr>
<tr>
<td>Prerequisites and Best Practice Recommendations</td>
<td>8</td>
</tr>
<tr>
<td>Use BIG-IP Administrative Partitions</td>
<td>8</td>
</tr>
<tr>
<td>Use the Configuration Table and Standard Naming Conventions</td>
<td>9</td>
</tr>
<tr>
<td>Determining the Port Usage on the Enterprise Manager Hosts</td>
<td>10</td>
</tr>
<tr>
<td>Example TCP/IP ports used throughout this guide</td>
<td>10</td>
</tr>
<tr>
<td>Ports on the F5 BIG-IP LTM</td>
<td>11</td>
</tr>
<tr>
<td>Mapping between F5 Ports to Ports on EM Host(s)</td>
<td>11</td>
</tr>
<tr>
<td>F5 BIG-IP LTM configuration objects for this white paper</td>
<td>12</td>
</tr>
<tr>
<td>Methodology</td>
<td>13</td>
</tr>
<tr>
<td>Create the Cloud Control Cipher Rule</td>
<td>13</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control Cipher Rule</td>
<td>13</td>
</tr>
<tr>
<td>Create the Cloud Control Cipher Group</td>
<td>14</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control Cipher Group</td>
<td>14</td>
</tr>
<tr>
<td>SSL Client Certificate</td>
<td>15</td>
</tr>
<tr>
<td>Create the Cloud Control SSL Server Profile</td>
<td>16</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control SSL Server Profile</td>
<td>16</td>
</tr>
<tr>
<td>Create the Cloud Control SSL Client Profile</td>
<td>17</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control SSL Client Profile</td>
<td>17</td>
</tr>
<tr>
<td>Create the Health Monitors</td>
<td>18</td>
</tr>
<tr>
<td>Base Cloud Control Health Monitor Settings</td>
<td>19</td>
</tr>
<tr>
<td>Health Monitor Send/Receive Strings</td>
<td>19</td>
</tr>
<tr>
<td>Same text formatted for easy Copy/Paste</td>
<td>20</td>
</tr>
<tr>
<td>Comments Regarding the values used above</td>
<td>20</td>
</tr>
<tr>
<td>Detailed steps to create the Cloud Control Health Monitors</td>
<td>21</td>
</tr>
<tr>
<td>Completed Health Monitors</td>
<td>23</td>
</tr>
<tr>
<td>F5 Node DEFINITIONS</td>
<td>24</td>
</tr>
<tr>
<td>Best Practice Health Monitoring Synopsis</td>
<td>24</td>
</tr>
</tbody>
</table>
LIST OF FIGURES
Figure 1: Enterprise Manager 13c Cloud Control High Availability Architecture – Layer 3 Load Balancing ................................................................. 3
Figure 2. Enterprise Manager 13c Cloud Control High Availability Architecture: SSL Proxying ................................................................. 4
Figure 3. Example Output for ports from emgc.properties ................................................................. 10
Figure 4. Mapping between F5 Ports and EM Host Ports ..................................................................... 11
Figure 5. Example of finished definition of Cipher Rule ................................................................. 13
Figure 6. Example of finished definition of the Cipher Group .......................................................... 14
Figure 7. Example of a finished definition of the Server SSL Profile .................................................. 16
Figure 8. Example of a finished definition of the Client SSL Profile .................................................. 17
Figure 9. Example of finished definition of a health monitor ............................................................. 22
Figure 10. Screenshot of all required health monitors ....................................................................... 23
Figure 11. Example node definitions.................................................................................................. 24
Figure 12. Example of finished definition of a F5 pool ...................................................................... 26
Figure 13. Screenshot of all required pools ....................................................................................... 27
Figure 14. Example of a finished definition of a TCP profile .............................................................. 28
Figure 15. Screenshot of completed TCP Profiles ................................................................................ 28
Figure 16. Example of a finished definition of a Persistence Profile utilizing Source Address Affinity .............................................................................. 31
Figure 17. Example of a finished definition of a Persistence Profile utilizing Cookie Persistence with Secured Cookies .................................................. 32
Figure 18. Screenshot of completed persistence profiles – SSL Proxying – secured cookies ..................................................................................... 33
Figure 19. Unsecure Console Redirect Rule ........................................................................................ 34
Figure 20. Definition of redirect iRule ................................................................................................ 34
Figure 21. Screen shot of the finished definition of a completed virtual server .................................... 38
Figure 22. Screenshot of completed Virtual Servers – Secured HTTPS ................................................ 39
Figure 23. Example Network Map after completed configuration ........................................................ 39
Figure 24. TCP half_open monitor .................................................................................................... 43

LIST OF TABLES
Table 1. Conventional TCP/IP Port Numbers on the BIG-IP F5 LTM .................................................. 5
Table 2. Example of Browser Access to Enterprise Manager, via the BIG-IP F5 LTM .................................... 5
Table 3. Naming Convention for BIG-IP Configuration Objects .......................................................... 9
Table 4. Port cross-reference ........................................................................................................... 10
Table 5. Ports on the F5 BIG-IP LTM ................................................................................................. 11
Table 6. Summary of all F5 BIG-IP LTM Configuration Objects ......................................................... 12
Table 7. Health Monitors to utilize for Enterprise Manager 13.5 ......................................................... 19
Table 8. Detailed Health Monitor Send/Receive Strings .................................................................... 19
Table 9. Cloud Control Pools ............................................................................................................ 25
Table 10. List of Cloud Control TCP Profiles .................................................................................... 27
Table 11. List of Cloud Control TCP Profiles .................................................................................... 29
Table 12. Persistence Profile Options .................................................................................................. 30
Table 13. Full set of valid URLs ....................................................................................................... 34
Table 14. BIG-IP F5 LTM Virtual Servers (Layer-3 Load Balancing) ................................................... 35
Table 15. BIG-IP F5 LTM Virtual Servers (SSL Proxying) ................................................................ 36
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. 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)
- 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 5
- 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 5, High Availability is supported for the Oracle Management Server, Java Virtual Machine Diagnostics (JVMD), and optionally Always-On Monitoring (AOM).

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

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. **Layer-3 Load Balancing** - formerly named Standard TCP/IP tunneling:
   a) This approach lends itself to limiting the resource requirements on the F5 device.
   b) This is also a possible approach to take when migrating a single OMS system to be behind the F5 device.
   c) In this scenario, the single OMS system would already be configured appropriately.
   d) 3rd Party SSL certificate management is performed on each EM host.

2. **SSL Proxying** - formerly named SSL end-to-end with iRules.
   a) Most resource intensive solution, as well as most secure.
   b) Some reliance on proprietary F5 TCL-based iRules.
   c) Enterprise Manager Console is accessed using the default TCP/IP port 443.
   d) There are two slight variations in this architectural option.
      i) Third party (e.g. Verisign) trusted SSL certificate(s) installed throughout the environment.
         1) 3rd Party SSL Certificate Management needs to be performed both on the F5 and on each EM system.
         2) Valid SSL certificates on each EM system, for each OMS component (OHS, WLS Servers):
      ii) 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 two detailed diagrams depict 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: Layer 3 Load Balancing (formerly known as SSL Tunneling).

Figure 1: Enterprise Manager 13c Cloud Control High Availability Architecture – Layer 3 Load Balancing
SSL Proxying (formerly known as SSL end-to-end with iRules)

Figure 2. Enterprise Manager 13c Cloud Control High Availability Architecture: SSL Proxying
CONFIGURING AN F5 BIG-IP LTM FOR CLOUD CONTROL SERVICES

Oracle Enterprise Manager Components provide Cloud Control clients, including the Cloud Control console and Management Agents, HTTP or HTTPS access, to the set of Cloud Control services listed below. The F5 BIG-IP LTM can load balance requests for each service (OMS, AOM, and Management Agent). The table below demonstrates a best practice configuration for a Load Balancing front-end.

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

The list of Cloud Control services to be managed by the F5 BIG-IP is shown in table 1.

<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 (default https port)</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</td>
<td>Secure Agent to AOM communication</td>
<td>8081</td>
</tr>
<tr>
<td>Upload</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 combination of the Ports above, and the constant server-side TCP/IP address, form the destination of the TCP/IP connection 4-tuple.

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

1. Source address
2. Source Port #
3. Destination Address (for example, slb.example.com).
4. Destination Port Number (examples shown in table below).

The Conventional Ports shown above are the TCP/IP ports on which the F5 BIG-IP LTM will service requests, for the given virtual address.

For example, if the Server Load Balancer’s Virtual Server address is slb.example.com, the website address of the Enterprise Manager Console is shown below (port 443 is the default for https).

<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>

*Table 2. Example of Browser Access to Enterprise Manager, via the BIG-IP F5 LTM*
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.

Refer to Appendix B: F5 BIG-IP Local Traffic Manager Terms for more details on the below objects.

Ciphers Rules and Cipher Groups

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.

SSL profiles, on the F5

F5 LTM supports two distinct types of SSL profiles.

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.

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.

Health Monitors

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

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.

TCP profiles

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

Nodes

F5 BIG-IP LTM supports the creation of node definitions. This can help manage the creation of pools.

Pools

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.

Persistence Profiles

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.

Virtual Server

A virtual server is a unique IP address and port that represents a pool of servers. If utilizing ‘SSL Proxying’, each virtual server must also specify the specific Client 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:

- 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 13.1 software.
- A Configuration Summary page naming all the Cloud Control services and corresponding F5 configuration objects.

Refer to Appendix A: optimization of pool monitoring for a possible optimization of Cloud Control pool health monitoring.
DETAILED CONFIGURATION INSTRUCTIONS

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

This 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 in the Partition named **EM_135**.

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.

For a specific implementation, 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>Internal Host Name for EM Virtual Server. Recommended to be forward and reverse DNS resolvable. Samples use ‘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;[aom</td>
</tr>
<tr>
<td>TCP Profiles</td>
<td>tcp_&lt;service_label&gt;[aom</td>
</tr>
<tr>
<td>Nodes</td>
<td>Internal IT Conventions Samples provided as emomsX.example.com</td>
</tr>
<tr>
<td>Pools</td>
<td>pool_&lt;service_label&gt;[aom</td>
</tr>
<tr>
<td>Cookie Persistence Profile</td>
<td>cookie_&lt;service_label&gt;</td>
</tr>
<tr>
<td>Source IP Address Persistence Profile</td>
<td>sourceip_&lt;service_label&gt;[aom</td>
</tr>
<tr>
<td>Virtual Server</td>
<td>vs_&lt;service_label&gt;[aom</td>
</tr>
</tbody>
</table>

Table 3. Naming Convention for BIG-IP Configuration Objects

- As an example, the Secure Console services uses “ccsc” as the service label.
- The optional Insecure Console Services for the OMS uses “ccuc” as the service label.
Determining the 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_UPLOAD_HTTPS_PORT=4903
EM_CONSOLE_HTTPS_PORT=7802
MS_HTTPS_PORT=7301
```

Figure 3. Example Output for ports from emgc.properties

Example TCP/IP ports used throughout this guide

The specific port values listed below are used in all example commands throughout this document.

<table>
<thead>
<tr>
<th>PORT</th>
<th>CLOUD CONTROL SERVICE</th>
<th>DESCRIPTION</th>
<th>CROSS REFERENCE FROM EMGC.PROPERTIES</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>4903</td>
<td>Secure Upload Port</td>
<td>HTTPS EM Agent access to Cloud Control Uploads</td>
<td>EM_UPLOAD_HTTPS_PORT</td>
</tr>
<tr>
<td>4889</td>
<td>Cloud Control Agent Registration Port</td>
<td>HTTP EM Agents, for Agent Registration, to Cloud Control.</td>
<td>EM_UPLOAD_HTTP_PORT</td>
</tr>
<tr>
<td>8081</td>
<td>Secure Always-On Monitoring</td>
<td>HTTPS EM Agent access to AOM uploads.</td>
<td>Refer to Configure Always-On Monitoring</td>
</tr>
<tr>
<td>7301</td>
<td>Cloud Control Secure JVMD Port (Managed Server HTTP SSL Port)</td>
<td>HTTPS Access for JVMD.</td>
<td>MS_HTTPS_PORT</td>
</tr>
</tbody>
</table>

Table 4. Port cross-reference

THE PORT NUMBERS FOR YOUR PARTICULAR INSTALLATION MAY BE DIFFERENT THAN SHOWN ABOVE.
Ports on the F5 BIG-IP LTM

To review from ‘Table 1. Conventional TCP/IP Port Numbers on the BIG-IP F5 LTM’, the ports that are accessible directly by Enterprise Manager Administrators and Management Agents, via the F5 BIG-IP LTM are:

<table>
<thead>
<tr>
<th>PORT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
</tr>
<tr>
<td>4903</td>
<td>Cloud Control Secure Upload</td>
</tr>
<tr>
<td>4889</td>
<td>Cloud Control Agent Registration Port</td>
</tr>
<tr>
<td>8081</td>
<td>Always-On Monitoring Secure Upload Port (if configured)</td>
</tr>
<tr>
<td>7301</td>
<td>Cloud Control Secure JVMD</td>
</tr>
<tr>
<td>80</td>
<td>Redirect iRule for Cloud Control Secure Console</td>
</tr>
</tbody>
</table>

Table 5. Ports on the F5 BIG-IP LTM

PORTS ON THE F5 BIG-IP ARE OFTEN DIFFERENT THAN THE PORTS USED BY ENTERPRISE MANAGER.

Mapping between F5 Ports to Ports on EM Host(s)

This diagram outlines the ports used throughout this paper.

- Port 443 on the F5 BIG-IP LTM handles traffic from Enterprise Manager Administrators.
  - This traffic will be redirected, using secure https, to port 7802 on the Enterprise Manager hosts.
- Ports 4903, 4889, and 8081 handle incoming traffic from Enterprise Management Agents.
  - This traffic will be redirected to the respective ports of the Enterprise Manager Management Servers (OMSs).

Figure 4. Mapping between F5 Ports and EM Host Ports
### F5 BIG-IP LTM configuration objects for this white paper

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>TCP PORT ON EM HOSTS</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 or cookie_ccsc</td>
<td>pool_ccsc</td>
<td>vs_ccsc443</td>
<td>443</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional Redirects to Secure Console using F5 BIG-IP LTM iRules</td>
<td>N/A</td>
<td>N/A</td>
<td>tcp_ccuc</td>
<td>N/A</td>
<td>N/A</td>
<td>vs_ccuc80</td>
<td>80</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>4903</td>
<td></td>
<td>tcp_ccsu</td>
<td>Optional: mon_cc_halfopen</td>
<td>pool_ccsu</td>
<td>vs_ccsu4903</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 Secure Upload (If configured)</td>
<td>8081</td>
<td>mon_ccaom</td>
<td>tcp_ccaom</td>
<td>None</td>
<td>pool_ccaom</td>
<td>vs_ccaom8081</td>
<td>8081</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>7301</td>
<td>mon_ccsjvmd</td>
<td>tcp_ccsjvmd</td>
<td>sourceip_ccsjvmd or cookie_ccsjvmd</td>
<td>pool_ccsjvmd</td>
<td>vs_ccsjvmd7301</td>
<td>7301</td>
</tr>
<tr>
<td>Unsecure JVMD (Not Recommended) *</td>
<td>7202</td>
<td>mon_ccujvmd</td>
<td>tcp_ccujvmd</td>
<td>sourceip_ccujvmd or cookie_ccujvmd</td>
<td>pool_ccujvmd</td>
<td>vs_ccujvmd7202</td>
<td>7202</td>
</tr>
</tbody>
</table>

* The unsecure JVMD should not be opened on the F5 BIG-IP LTM under any normal circumstance. No specific documentation steps are provided for this deprecated item.

---

Table 6. Summary of all F5 BIG-IP LTM Configuration Objects
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 Table 4. Port cross-reference. 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 architectural approaches, 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 or greater, and not support insecure ciphers, such as MD5.

Detailed steps to create the Cloud Control Cipher Rule
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. For the Cipher String, enter a value appropriate for your Enterprise Manager Security Configuration.
9. For example, enter the following cipher string:
10. Possibly requires an F5 specific version of ECDHE
12. Choose Finished.

![Figure 5. Example of finished definition of Cipher Rule](image-url)
**CREATE THE CLOUD CONTROL CIPHER GROUP**

For the ‘SSL Proxying’ approach, an F5 LTM Cipher group, referencing the Cipher Rule above, must be created.

**Detailed steps to create the Cloud Control Cipher Group**

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 **Groups**.
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**.

![Figure 6. Example of finished definition of the Cipher Group](image)
SSL CLIENT CERTIFICATE

When utilizing architectural option 2 ‘SSL Proxying (formerly known as SSL end-to-end with iRules)’, 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 file containing a certificate chain, for which the root of the chain, was issued by a 3rd party certificate authority (CA).
- All modern Web Browsers, and all Fusion Middleware components, will automatically trust this third party certificate Authority (CA).

**slb-chain**
- This certificate chain is required when utilizing ‘SSL Proxying, variation ii’. 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.
- This certificate chain is necessary to form the required trust relationship between the F5 and the EM components.
CREATE THE CLOUD CONTROL SSL SERVER PROFILE

For approach 2 ‘SSL Proxying’, an F5 LTM SSL Server Profile should be created specific to the SSL configuration used by Enterprise Manager.

Detailed 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. Select the checkboxes on the right-hand side for Certificate, Key, Pass Phrase, optionally for Chain, and Ciphers.
12. Ensure that the checkboxes for Certificate and Key are selected, and then choose the appropriate SSL Certificate and Key, for example slb.example.com
13. Optionally, ensure that the checkbox for Chain is selected, and then choose the appropriate Chain, for example slb-chain
14. Midway down the screen, you will see an entry for Ciphers.
15. Ensure that the checkbox for Cipher Group is selected, and then in the drop down, choose the cipher_ccsc cipher group.

Figure 7. Example of a finished definition of the Server SSL Profile
CREATE THE CLOUD CONTROL SSL CLIENT PROFILE

If utilizing architectural option 2 SSL Proxying (formerly known as SSL end-to-end with iRules), an F5 LTM SSL Client Profile should be created specific to the SSL configuration used by Enterprise Manager.

Detailed 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 checkbox for Enabled.
12. Select the check boxes on the right hand-side for Certificate Key Chain, and Ciphers.
13. Ensure that the checkbox for Certificate Key Chain is selected, and choose the appropriate SSL Certificate and Key, if installed on the F5 BIG-IP LTM.
14. Midway down the screen, you will see an entry for Ciphers.
15. Ensure that the Cipher Group checkbox is selected.
16. In the drop down, choose the cipher_ccsc cipher group.
17. Choose Finished.

Figure 8. Example of a finished definition of the Client SSL Profile
CREATE THE HEALTH MONITORS

There are two components when creating valid health monitors, for use with Enterprise Manager 13.5.

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.
Base Cloud Control Health Monitor Settings

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>MONITOR NAME</th>
<th>TYPE</th>
<th>SSL PROFILE</th>
<th>INTERVAL</th>
<th>TIMEOUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>mon_ccsc</td>
<td>HTTPS</td>
<td>sslserver_ccsc</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Unsecure Console (not recommended)</td>
<td>mon_ccuc</td>
<td>HTTP</td>
<td>N/A</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>mon_ccsu</td>
<td>HTTPS</td>
<td>Optional</td>
<td>60 (See Above)</td>
<td>181</td>
</tr>
<tr>
<td>Optional:</td>
<td>mon_cc_halfopen</td>
<td>TCP Half Open</td>
<td>N/A</td>
<td>5</td>
<td>16</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>mon_ccar</td>
<td>HTTP</td>
<td>N/A</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Always-On Monitoring (if configured)</td>
<td>mon_ccaom</td>
<td>HTTPS</td>
<td>Optional</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>mon_ccsjvmd</td>
<td>HTTPS</td>
<td>Optional</td>
<td>60</td>
<td>181</td>
</tr>
<tr>
<td>Unsecure JVMD (not recommended)</td>
<td>mon_ccujvmd</td>
<td>HTTP</td>
<td>N/A</td>
<td>60</td>
<td>181</td>
</tr>
</tbody>
</table>

Table 7. Health Monitors to utilize for Enterprise Manager 13.5

Health Monitor Send/Receive Strings

<table>
<thead>
<tr>
<th>MONITOR NAME</th>
<th>SEND STRING</th>
<th>RECEIVE STRING</th>
</tr>
</thead>
<tbody>
<tr>
<td>mon_ccsc</td>
<td>GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Enterprise Manager Console is UP</td>
</tr>
<tr>
<td>mon_ccuc (Optional)</td>
<td>GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Enterprise Manager Console is UP</td>
</tr>
<tr>
<td>mon_ccsu</td>
<td>GET /empbs/upload HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Http Receiver Servlet active!</td>
</tr>
<tr>
<td>mon_ccar</td>
<td>GET /empbs/genwallet HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>GenWallet Servlet activated</td>
</tr>
<tr>
<td>mon_ccaom (If configured)</td>
<td>GET /upload HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Always On Monitoring is active</td>
</tr>
<tr>
<td>mon_ccsjvmd</td>
<td>GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Reply to empty request</td>
</tr>
<tr>
<td>Optional: on_cc_half_open</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>mon_ccujvmd : Not recommended</td>
<td>GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close</td>
<td>Reply to empty request</td>
</tr>
</tbody>
</table>

Table 8. Detailed Health Monitor Send/Receive Strings
Same text formatted for easy Copy/Paste

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

In order to avoid errors when copying the text in the above table, it is repeated below, in a plain-text format:

**mon_ccsc** and **mon_ccuc**

GET /em/consoleStatus.jsp HTTP/1.1
r
nHost: slb.example.com
r
nConnection: Close

Enterprise Manager Console is UP

**mon_ccsu**

GET /empbs/upload HTTP/1.1
r
nHost: slb.example.com
r
nConnection: Close

Http Receiver Servlet active!

**mon_ccar**

GET /empbs/genwallet HTTP/1.1
r
nHost: slb.example.com
r
nConnection: Close

GenWallet Servlet activated

**mon_ccaom**

GET /upload HTTP/1.1
r
nHost: slb.example.com
r
nConnection: Close

Always On Monitoring is active

**mon_ccsjvmd** and **mon_ccujvmd**

GET /jamservlet/comm HTTP/1.1
r
nHost: slb.example.com
r
nConnection: Close

Reply to empty request

**Comments Regarding the values used above**

1. For EM 13.5, there is a hard requirement on case sensitivity (i.e. **HTTP/1.1** instead of **http/1.1**)
2. The value for the **Host:** header needs to be set to the fully DNS resolvable hostname associated with the virtual IP address for the appropriate Virtual Server. In the examples above: Host: slb.example.com

The reasoning for this is related to the requirement on the use of **HTTP Version 1.1** with Enterprise Manager 13.5.

» The value specified of the **Host:** header shall be a resolvable hostname.

» The associated IP address for the given hostname shall match the destination server to which the request is sent.

» If the value of **Host:** header does not meet these requirements, the server is to return an error code of 400.

» The implications for a given health monitor is that an incorrect value for the **Host:** header would result in a failure condition, marking the pool member as down.

» Although alternative values for the **Host:** header may work, there is no guarantee that sometime in the future this would stop working.

» There is no way to predict when any possible failure would occur, so the Best Practice for these health monitors is to provide a valid value in the **Host:** header.
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:
   9. **Interval** is the health monitor property that specifies the frequency at which the system issues the monitor check.
   10. **Timeout** is the setting that allows the health monitor to mark a member as down.
   11. The recommendation from F5 is to set the BIG-IP LTM Health Monitor Timeout setting as \((3 \times \text{Interval}) + 1\)
   12. For example, set **Interval** to 5 and set **Timeout** to 16.
   13. Refer to the table above for the specific Interval and Timeout values for the monitor being configured.
   14. In the **Send String** field, insert the appropriate string for the Monitor being configured.
   15. The HTTP header **Host** must reference the hostname of the Virtual Server.
   16. This **hostname** must match the SSL certificate being presented by EM.
   17. It is also required that the hostname is **DNS resolvable**.
   18. The HTTP request and headers are case-sensitive for Enterprise Manager 13.5.
   19. Please copy/paste above strings exactly as shown.
   20. In the **Receive String** field, insert the appropriate string for the Monitor being configured.

21. For approach 2 'SSL Proxying (formerly known as SSL end-to-end with iRules)' in the **SSL Profile** drop down, choose our Server SSL Profile named sslserver_ccsc

22. **IMPORTANT**: For approach 1 'Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling),' the **SSL Profile** drop-down must show **no entries**.
23. For the Agent Secure Upload Health Monitor, specifying the **SSL Profile** is optional.
24. **IMPORTANT**: Ensure to leave the **Username** and **Password** fields blank.
25. **Some browsers will incorrectly auto-fill** the **Username** and **Password** field with any possibly saved passwords for the F5 BIG-IP LTM.
26. For simplicity, leave the **Alias Address** field and the **Alias Port** fields at their default values:
27. **Alias Address**: * All Addresses
28. **Alias Port**: * All Ports
29. 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.

![Health Monitor Configuration](image)

**Figure 9. Example of finished definition of a health monitor**
Completed Health Monitors

Below is an example showing the required health monitors, (as well as the optional half open monitor).

![Screenshot of all required health monitors](image)

*Figure 10. Screenshot of all required health monitors*
F5 NODE DEFINITIONS

A node is a logical object on the BIG-IP® the BIG-IP system system that identifies the IP address of a physical resource on the network. You can explicitly create a node, or you can instruct the BIG-IP system to automatically create one when you add a pool member to a load balancing pool.

The difference between a node and a pool member is that a node is designated by the device’s IP address only (192.168.1.10), while designation of a pool member includes an IP address and a service (such as 192.168.1.10:443).

A primary feature of nodes is their association with health monitors. Like pool members, nodes can be associated with health monitors as a way to determine server status. However, a health monitor for a pool member reports the status of a service running on the device, whereas a health monitor associated with a node reports status of the device itself.

Nodes are the basis for creating a load balancing pool. For any server that you want to be part of a load balancing pool, you must first create a node, that is, designate that server as a node. After designating the server as node, you can add the node to a pool as a pool member. You can also associate a health monitor with the node, to report the status of that server.

Utilizing the F5 node definition, each pool member for each pool utilized in this white paper effectively provides an additional health monitor, based on an extremely lightweight, and fast, ICMP ping request/response.

The following screen shot shows an example of the set of nodes for a 2 node Enterprise Manager High Availability installation. The backend Enterprise Manager hosts are on the IP addresses 192.168.1.10 and 192.168.1.11.

![Node Definitions Screen Shot](image)

**Figure 11. Example node definitions**

Best Practice Health Monitoring Synopsis

For a given pool member to be marked up, the given host must be up and reachable [and optionally respond to an incoming TCP/IP connection (half-open)] and respond with an indication of health from a specific application.
CREATE THE CLOUD CONTROL POOLS

A BIG-IP LTM pool is a set of servers grouped together to receive traffic according to a load balancing method. Create a pool for each of the Cloud Control services using the following table. Work with your respective networking team(s) when considering the **Load Balancing** Option to utilize.

<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 Upload</td>
<td>pool_ccsu</td>
<td>mon_ccsu Optional: mon_cc_halfopen</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 Secure Upload</td>
<td>pool_ccaom</td>
<td>mon_ccaom</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 (Not recommended)</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>

Table 9. Cloud Control Pools

**Detailed steps to create each Cloud Control Pool**

1. On the **Main** tab, expand **Local Traffic**, and then click **Pools**.
2. On the **Pools** screen, click **Create**.
4. Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**.
5. Configure these settings, as applicable, for the network.
6. In the **Name** field, enter a unique name for the pool.
7. For example, enter `pool_ccsc`.
8. 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.
9. For example, select `mon_ccsc`.
10. From the **Load Balancing Method** list, choose the preferred load balancing method (different load balancing methods may yield optimal results for a particular network).
11. For example, select Least Connections (member).
12. Keep the Priority Group Activation value as **Disabled**.
13. In the **New Members** section, add each OMS node, using the available node definitions.
14. Enter the OMS hostname in the **Node Name** field.
15. Enter the OMS IP address in the **Address** field.
16. Enter the OMS port number, for the service that the pool is being created for, in the **Service Port** field.
17. Click **Add**.
18. Click **Finished**.
In this example, the health monitor for the Cloud Control Secure Console is shown.

Figure 12. Example of finished definition of a F5 pool
**Completed Pools**

Below is an example showing all the required pools.

![Pool List](image)

---

**CREATE THE TCP PROFILES**

In this guide, 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, per internal networking requirements.

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>Unsecure Console</td>
<td>tcp_ccuc</td>
</tr>
<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 Secure Upload</td>
<td>tcp_ccaom</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>tcp_ccsjvmd</td>
</tr>
<tr>
<td>Unsecure JVMD (not recommended)</td>
<td>tcp_ccujvmd</td>
</tr>
</tbody>
</table>

*Table 10. List of Cloud Control TCP Profiles*
Detailed steps for each TCP profile to be created:

1. On the Main tab, expand Local Traffic.
2. Click Profiles.
3. The HTTP Profiles screen opens.
4. On the Menu bar, from the Protocol menu, select TCP.
5. In the upper-right portion of the screen, click Create.
6. The New TCP Profile screen opens.
7. In the Name field, enter a unique name for this profile. For example: tcp_ccsc.
8. For the Parent Profile, the default option of tcp is utilized in this guide.
9. If needed, modify as applicable. Consult F5 BIG-IP LTM online documentation, and internal networking standards, to choose any options that may differ from the defaults.
10. Click Finished.

---

**Figure 14. Example of a finished definition of a TCP profile**

**Completed TCP Profile**

Below is an example showing all of the required TCP Profiles:

---

**Figure 15. Screenshot of completed TCP Profiles**
PERSISTENCE PROFILE TYPES
Persistence profiles may be required to ensure that a given client continues to communicate with a single back-end OMS system, for example, after a successful login to Enterprise Manager.

The informal term for this is ‘session stickiness’.

There are three options for persistence profile types that can be utilized for any given virtual server.

Types of persistence profiles
A brief outline of three of the most common persistence profiles are shown in the table below.

<table>
<thead>
<tr>
<th>PERSISTENCE PROFILE TYPE</th>
<th>TIMEOUT</th>
<th>EXPIRATION</th>
<th>SHORT HAND</th>
<th>COMMENTS</th>
</tr>
</thead>
</table>
| Source Address Affinity   | 3660    | saf        |            | • Simplest persistence profile type.  
|                          |         |            |            | • Secure https (ie. SSL/TLS) Virtual Servers:  
|                          |         |            |            | • Required when using ‘Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling)’.  
|                          |         |            |            | • Not appropriate if the client IP address can change dynamically. |
| Cookie Persistence        | 3600    | cookie     |            | • Does not rely on a static client IP Address for browsers and/or agents.  
|                          |         |            |            | • Secure https (ie. SSL/TLS) Virtual Servers.  
|                          |         |            |            | • Requires ‘SSL Proxying (formerly known as SSL end-to-end with iRules)’  
|                          |         |            |            | ⊳ NOTE: Must be utilized carefully to meet any possible security compliance requirements. |
| No Persistence Profile    | none    | none       |            | • Only usable if ‘session stickiness’ is not required. |

Table 1. List of Cloud Control TCP Profiles
Options for the persistent profiles for each Cloud Control Service

With the above three persistence profile options, the Virtual Server for a given cloud control service may have options for the persistence profile to utilize.

<table>
<thead>
<tr>
<th>CLOUD CONTROL SERVICE</th>
<th>STANDARD CONFIGURATION: LAYER 3 LOAD BALANCING (FORMERLY KNOWN AS SSL TUNNELING).</th>
<th>SSL PROXYING (FORMERLY KNOWN AS SSL END-TO-END WITH IRULES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Console</td>
<td>saf: Naming convention: sourceip_ccsc</td>
<td>saf: Naming convention: sourceip_ccsc</td>
</tr>
<tr>
<td></td>
<td>cookie: Naming convention: cookie_ccsc</td>
<td>cookie: Naming convention: cookie_ccsc</td>
</tr>
<tr>
<td>Unsecure Console</td>
<td>saf: Naming convention: sourceip_ccuc</td>
<td>saf: Naming convention: sourceip_ccuc</td>
</tr>
<tr>
<td></td>
<td>cookie: Naming convention: cookie_ccuc</td>
<td>cookie: Naming convention: cookie_ccuc</td>
</tr>
<tr>
<td>Secure Upload</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Agent Registration</td>
<td>cookie: Naming convention: cookie_ccar</td>
<td>cookie: Naming convention: cookie_ccar</td>
</tr>
<tr>
<td>Always-On Monitoring</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Secure JVMD</td>
<td>saf: Naming convention: sourceip_ccsjvmd</td>
<td>saf: Naming convention: sourceip_ccsjvmd</td>
</tr>
<tr>
<td></td>
<td>cookie: Naming convention: cookie_ccsjvmd</td>
<td>cookie: Naming convention: cookie_ccsjvmd</td>
</tr>
<tr>
<td>Unsecure JVMD</td>
<td>saf: Naming convention: sourceip_ccujvmd</td>
<td>saf: Naming convention: sourceip_ccujvmd</td>
</tr>
<tr>
<td></td>
<td>cookie: Naming convention: cookie_ccujvmd</td>
<td>cookie: Naming convention: cookie_ccujvmd</td>
</tr>
</tbody>
</table>

Table 12. Persistence Profile Options

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

CREATE THE PERSISTENCE PROFILES

Detailed steps for each persistence profile to be created:

1. On the Main tab, expand Local Traffic, and then click Profiles.
2. The Persistence Profiles screen opens.
3. On the Menu bar, click Persistence.
4. The Persistence Profiles 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.
8. For example, enter sourceip_ccsc
9. For each Persistence Profile being configured, follow one of the next two set of steps:
10. For Persistence Profiles utilizing Source Address Affinity, follow just the first set of steps below.
11. For Persistence Profiles utilizing Cookie Persistence, follow just the second set of steps.
Detailed steps to create Persistence Profile: Source Address Affinity

1. From the Persistence Type list select Source Address Affinity.
2. The configuration options for SourceIP persistence display.
3. Check the box next to the Timeout field to allow the Timeout value to be overridden.
4. Modify the Timeout value to 3600.
5. Click Finished.

Figure 16. Example of a finished definition of a Persistence Profile utilizing Source Address Affinity
**Detailed steps to create Persistence Profile: Cookie**

An important consideration when configuring **Cookie Persistence** is the likely security requirement to mask or hide the back-end OMS host that is servicing a given request.

1. From the Persistence Type list select **Cookie**.
2. The configuration options for Cookie persistence display.
3. In the **Name** field, enter a unique name for the profile.
4. For example: `cookie_ccsc`.
5. For each of options in the Configuration section:
6. Check the box next to the **Cookie Method** field to allow the Cookie Method value to be specified.
7. Choose the option **HTTP Cookie Insert**.
8. Check the box next to the **HTTPOnlyAttribute** to allow the **HTTPOnlyAttribute** to be specified.
9. Choose the option **Enabled**.
10. Check the box next to the **Expiration** field to allow the Expiration value to be overridden.
11. Clear the **Session Cookie** box.
12. The expiration options appear.
13. Provide the value 3600 in the Seconds field.
14. Based on internal security requirements, check the box next to the **Secure Attribute** to allow the Secure Attribute value to be specified.

   » **Set the Secure Attribute to the option Enabled or Disabled.**
15. Based on internal security requirements, select the check box next to **Default Cookie Encrypt Pool-Name** to allow the Default Cookie Encrypt Pool-Name to be specified.

   » **Set the Default Cookie Encrypt Pool-Name to the option Enabled or Disabled.**
16. Based on internal security requirements, select the check box next to **Cookie Encryption Use Policy** to allow the Cookie Encryption Use Policy to be specified.

   » **Set the Cookie Encryption Use Policy.**
17. Select the check box next to **Encryption Passphrase** to allow the Encryption Passphrase to be specified.
18. Choose a value for the **Encryption Passphrase**.
19. Click **Finished**.

---

*Figure 17. Example of a finished definition of a Persistence Profile utilizing Cookie Persistence with Secured Cookies*
Completed Persistence Profiles

The following screenshot shows the completed set of persistence profiles, when utilizing approach 2 ‘SSL Proxying (formerly known as SSL end-to-end with iRules)’, with secured cookie persistence.

<table>
<thead>
<tr>
<th>Name</th>
<th>Application</th>
<th>Type</th>
<th>Parent Profile</th>
<th>Partition / Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookie_ccar</td>
<td>Cookie</td>
<td>cookie</td>
<td></td>
<td>EM135</td>
</tr>
<tr>
<td>cookie_ccsjmd</td>
<td>Cookie</td>
<td>cookie</td>
<td></td>
<td>EM135</td>
</tr>
<tr>
<td>cookie_ccsc</td>
<td>Cookie</td>
<td>cookie</td>
<td></td>
<td>EM135</td>
</tr>
</tbody>
</table>

Figure 18. Screenshot of completed persistence profiles – SSL Proxying – secured cookies
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.

Unsecure Console service Redirect iRule

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

Figure 19. Unsecure Console Redirect Rule

Detailed steps 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_httptolistps.
4. Copy the appropriate iRule text from the section above and paste it in the Definition section.
5. Click Finished.

Figure 20. Definition of redirect iRule

Full set of valid URLs after iRule creation

<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>Invalid URL - /em is required for EM 13.5</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>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>
</tbody>
</table>

Table 13. Full set of valid URLs
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 the appropriate table for the approach being utilized:

» Approach 1: Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling).

» Approach 2: SSL Proxying (formerly known as SSL end-to-end with iRules)

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.

Layer-3 Load Balancing

<table>
<thead>
<tr>
<th>VIRTUAL SERVER NAME</th>
<th>SECURE CONSOLE</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_ccaom8081</td>
<td></td>
<td>vs_ccsjvmd7301</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>None</td>
<td>http</td>
<td>None</td>
<td>http</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL CLIENT PROFILE</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL SERVER PROFILE</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>iRULE</td>
<td>None</td>
<td>ccuc_httptohttps</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>DEFAULT POOL</td>
<td>pool_ccsc</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>None</td>
<td>None</td>
<td>cookie_ccar</td>
<td>None</td>
<td>sourceip_ccsjvmd</td>
</tr>
</tbody>
</table>

Table 14. BIG-IP F5 LTM Virtual Servers (Layer-3 Load Balancing)
### SSL Proxying

Reference the table below for information to configure the virtual servers for the SSL Proxying approach.

<table>
<thead>
<tr>
<th>VIRTUAL SERVER</th>
<th>SECURE CONSOLE</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>VIRTUAL SERVER NAME</td>
<td>vs_ccsc443</td>
<td>vs_ccuc80</td>
<td>vs_ccsu4903</td>
<td>vs_ccar4889</td>
<td>vs_ccaom8081</td>
<td>vs_ccsjvmd7301</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>saf</td>
<td>None</td>
<td>http</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>SSL CLIENT PROFILE</td>
<td>sslclient_ccsc</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>sslclient_ccsc</td>
</tr>
<tr>
<td>SSL SERVER PROFILE</td>
<td>sslserver_ccsc</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>sslserver_ccsc</td>
<td></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>IRULE</td>
<td>None</td>
<td>ccuc_httptohttps</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>DEFAULT POOL</td>
<td>pool_ccsc</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>saf</td>
<td>sourceip_ccsc</td>
<td>None</td>
<td>None</td>
<td>cookie_ccar</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>cookie</td>
<td>cookie_ccsc</td>
<td></td>
<td></td>
<td></td>
<td>cookie</td>
</tr>
</tbody>
</table>

*Table 15. BIG-IP F5 LTM Virtual Servers (SSL Proxying)*
Detailed steps to create each Virtual Server

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

1. On the Main tab, expand Local Traffic, and then click Virtual Servers.
2. The Virtual Servers screen opens.
3. In the upper-right portion of the screen, click the Create button.
5. In the Name field, enter a unique name for this virtual server.
6. For example, enter vs_ccsc443.
7. Keep the Type list at the default setting: Standard.
8. In the Destination Address field, enter the IP address of this virtual server, for example 10.10.10.10.
9. In the Service Port field, enter the Virtual IP Port for the service being created, for example port 443.
10. From the Configuration list, select Advanced.
11. The Advanced configuration options display.
12. From the Protocol Profile (Client) list select the name of the profile for the service being created.
13. In this example, select tcp_ccsc.
14. Keep the Protocol Profile (Server) options as the defaults.
15. For the following virtual servers only, select http from the HTTP profile list.
16. Agent Registration
17. Unsecure Console service (if configured)
18. Unsecure JVMD service (if configured)
19. Important: Change the Source Address Translation setting to Auto Map.
20. In the Resources section, from the Default Pool list, select the pool created for the service that the virtual server is being created for.
21. In this example, select pool_ccsc.
22. Note that the
23. From the Default Persistence Profile list, select the persistence profile created for the service that the virtual server is being created for.
24. In this example, select sourceip_ccsc.
25. Alternatively, when utilizing approach 2 ‘SSL Proxying (formerly known as SSL end-to-end with iRules)’:
    • The cookie_ccsc persistence profile can be referenced.
26. Click Finished.
In this example, the Virtual Server for the Cloud Control Secure Console is shown.

Figure 21. Screen shot of the finished definition of a completed virtual server
Completed Virtual Servers

The following screenshot shows the completed set of Virtual Servers, when utilizing approach 2 ‘SSL Proxying (formerly known as SSL end-to-end with iRules)’, with secured cookie persistence.

![Completed Virtual Servers](image)

**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.

![Example Network Map](image)

The screen capture below shows a network map (all the IP addresses in this example have been anonymized).

![Example Network Map](image)
CONFIGURE THE ENTERPRISE MANAGER MANAGEMENT SERVERS

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 the OMS

Approach 1: Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling).

```
$ emctl secure oms -host slb.example.com \   
   -slb_port 4903 -slb_console_port 443 \   
   -slb_jvmd_https_port 7301 \   
   -lock_console -lock_upload

Oracle Enterprise Manager Cloud Control 13c Release 5
Copyright (c) ...
Securing OMS... Started
Enter Enterprise Manager Root (SYSMAN) Password :
Enter Agent Registration Password :
Copyright (c) ...
Securing OMS... Started.
Securing OMS... Successful
Restart OMS
```

Approach 2: SSL Proxying (formerly known as SSL end-to-end with iRules)

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

Stop Enterprise Manager

```
emctl stop oms -all
Oracle Enterprise Manager Cloud Control 13c Release 5
Copyright (c) ... Stopping Oracle Management Server...
WebTier Successfully Stopped
Oracle Management Server Successfully Stopped
Oracle Management Server is Down
AdminServer Successfully Stopped
```

Start Enterprise Manager

```
emctl start oms
Oracle Enterprise Manager Cloud Control 13c Release 5
Copyright (c) ... Starting Oracle Management Server...
WebTier Successfully Started
Oracle Management Server Successfully Started
Oracle Management Server is Up
```
CONFIGURE THE ENTERPRISE MANAGER AGENTS

Resecure all Management Agents

```
emctl secure agent -emdWalletSrcUrl https://slb.example.com:4903/em
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 5
Copyright (c)...
Console Server Host : emoms1.example.com
HTTP Console Port  : 7788
HTTPS Console Port : 7799
HTTP Upload Port   : 4889
HTTPS Upload Port  : 4903
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 : 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
```
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 5
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

CONFIGURE EMCLI CLIENT

Configure the EMCLI client installations to use the SLB hostname and port for the EM console. This reconfiguration can be expected to run for approximately 15-20 minutes.

```
emcli setup -url="https://slb.example.com:443/em" -username=sysman -trustall
```

Oracle Enterprise Manager 13c Release 5
Copyright (c) 1996, 2020 Oracle Corporation and/or its affiliates. All rights reserved.
Enter password:
Emcli setup successful
APPENDIX A: OPTIMIZATION OF POOL MONITORING

The F5 BIG-IP LTM provides a robust load balancing solution with various levels of sophistication. An example of this is the ‘TCP Half Open Monitor’.

Trade Off of Response Time Versus System Load

» A critical aspect of any health monitor is the tradeoff between the frequency of a health check, and any possible adverse impact to the service being monitored. An alternative health monitor solution utilizes two (or more) health checks.

» For example:
  » A Standard health check, with an interval of 60 seconds.
  » An additional TCP Half-Open health check with a shorter interval of 5 seconds.
  » For demonstration purposes, this white paper includes an example monitor named mon_cc_halfopen.

The tcp_half_open monitor sends a SYN packet to the pool member, and if a SYN-ACK is received from the server in response, the pool member is marked UP.

```
| SYN sent |  |
| SYN/ACK rec'd? |  |
| no | yes |  |
| DOWN** | UP |  |
| RST sent |  |
```

Figure 24. TCP half_open monitor

An important component of the above handshake is that in both instances, whether a SYN/ACK is received or not, the connection is first reset (if it was up), and then closed.

```
TCP/IP SYN Packet sent
  From F5 BIG-IP LTM -----+
                | SYN/ACK rec'd? |
                | no | yes |
                | DOWN | UP |
                | RST sent |

-----------> F5 BIG-IP LTM resets and closes connection = hence half-open
```

Please consult the F5 documentation and internal F5 support channels for further details.

The Oracle MAA team has instrumented the above health monitor, and has determined that if just the OMS is brought down, the additional health monitor provides little benefit.

The additional health monitor will be beneficial if the entire OMS stack (including Webtier) is brought down (or if the host itself were to unexpectedly crash).

In order to optimize the utilization of the additional health monitor, the following procedural changes are recommended.

- For planned outages of an Oracle Management Server, ensure to use the command below:

```
emctl stop oms -all
```
APPENDIX B: 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.

Node

In the context of the F5 BIG-IP LTM, a node is a definition that maps a specific Fully Qualified Domain Name to a specific IP Address. The default health monitor for a newly defined node is typically a simple ICMP (ie. ping).
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.
CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

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

Copyright © 2021, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Authors: Abramson, Jerry (Oracle), Bradshaw, Earl (Oracle), ...

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120

Configuring OMS High Availability with F5 BIG-IP Local Traffic Manager
October, 2021