ORACLE

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

October 2021 | Version 3.01

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

Purpose Statement 1

Disclaimer 1

Introduction 1

Goals of this document 1

High Availability 2

F5 BIG-IP LTM and Oracle Enterprise Manager Cloud Control 2

- Architectural Options for Network Configuration 2
- Detailed Diagrams of the Two Architectural Approaches 2
  - Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling). 3
  - SSL Proxying (formerly known as SSL end-to-end with iRules) 4

Configuring an F5 BIG-IP LTM for Cloud Control Services 5

Outline of required F5 LTM Configuration Objects 6

- Ciphers Rules and Cipher Groups 6
- SSL profiles, on the F5 6
- health monitors 6
- TCP profiles 6
- Nodes 6
- Pools 6
- Persistence Profiles 6
- Virtual Server 6

Detailed Configuration Instructions 8

- Prerequisites and Best Practice Recommendations 8
- Use BIG-IP Administrative Partitions 8
- Use the Configuration Table and Standard Naming Conventions 9
- Determining the Port Usage on the Enterprise Manager Hosts 10
- Example TCP/IP ports used throughout this guide 10
- Ports on the F5 BIG-IP LTM 11
- Mapping between F5 Ports to Ports on EM Host(s) 11
- F5 BIG-IP LTM configuration objects for this white paper 12

Methodology 13

Create the Cloud Control Cipher Rule 13

- Detailed steps to create the Cloud Control Cipher Rule 13

Create the Cloud Control Cipher Group 14

- Detailed steps to create the Cloud Control Cipher Group 14

SSL Client Certificate 15

Create the Cloud Control SSL Server Profile 16

- Detailed steps to create the Cloud Control SSL Server Profile 16

Create the Cloud Control SSL Client Profile 17

- Detailed steps to create the Cloud Control SSL Client Profile 17

Create the Health Monitors 18

- Base Cloud Control Health Monitor Settings 19
- Health Monitor Send/Receive Strings 19
- Same text formatted for easy Copy/Paste 20
  - Comments Regarding the values used above 20
- Detailed steps to create the Cloud Control Health Monitors 21
- Completed Health Monitors 23

F5 Node DEFINITIONS 24

- Best Practice Health Monitoring Synoposis 24

Create the Cloud Control Pools 25
- Detailed steps to create each Cloud Control Pool 25
- Completed Pools 27

Create the TCP Profiles 27
- Detailed steps for each TCP profile to be created: 28
- Completed TCP Profile 28

Persistence Profile Types 29
- Types of persistence profiles 29
- Options for the persistent profiles for each Cloud Control Service 30

Create the Persistence Profiles 30
- Detailed steps for each persistence profile to be created: 30
  - Detailed steps to create Persistence Profile: Source Address Affinity 31
  - Detailed steps to create Persistence Profile: Cookie 32
- Completed Persistence Profiles 33

Create a Redirect iRule for the Unsecure Console service 34
- Unsecure Console service Redirect iRule 34
- Detailed steps to create the Redirect iRule 34
- Full set of valid URLs after iRule creation 34

Create the Virtual Servers 35
- Layer-3 Load Balancing 35
- SSL Proxying 36
  - Detailed steps to create each Virtual Server 37
- Completed Virtual Servers 39

Example Network Map for a Fully Configured F5 BIG-IP LTM 39

ConfiguRE the Enterprise Manager Management Servers 40
- Secure the OMS 40
  - Approach 1: Standard Configuration: Layer 3 Load Balancing (formerly known as SSL Tunneling). 40
  - Approach 2: SSL Proxying (formerly known as SSL end-to-end with iRules) 40
- Stop Enterprise Manager 40
- Start Enterprise Manager 40

Configure the Enterprise Manager Agents 41
- Resecure all Management Agents 41

Verify Status of Management Service 41

Configure Always-On Monitoring 42

Configure EMCLI CLIENT 42

Appendix A: optimization of pool monitoring 43
- Trade Off of Response Time Versus System Load 43

Appendix B: F5 BIG-IP Local Traffic Manager Terms 44
- Monitor 44
- Pool 44
- Member 44
- Virtual Server 44
- Node 44
- Profile 45
- Persistence 45
- iRule 45
- Cipher 45
- Cipher Suite 45
  - Transport Layer Security 45
- Cipher Group 45
- Cipher Rule 45

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. Screnshot 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).

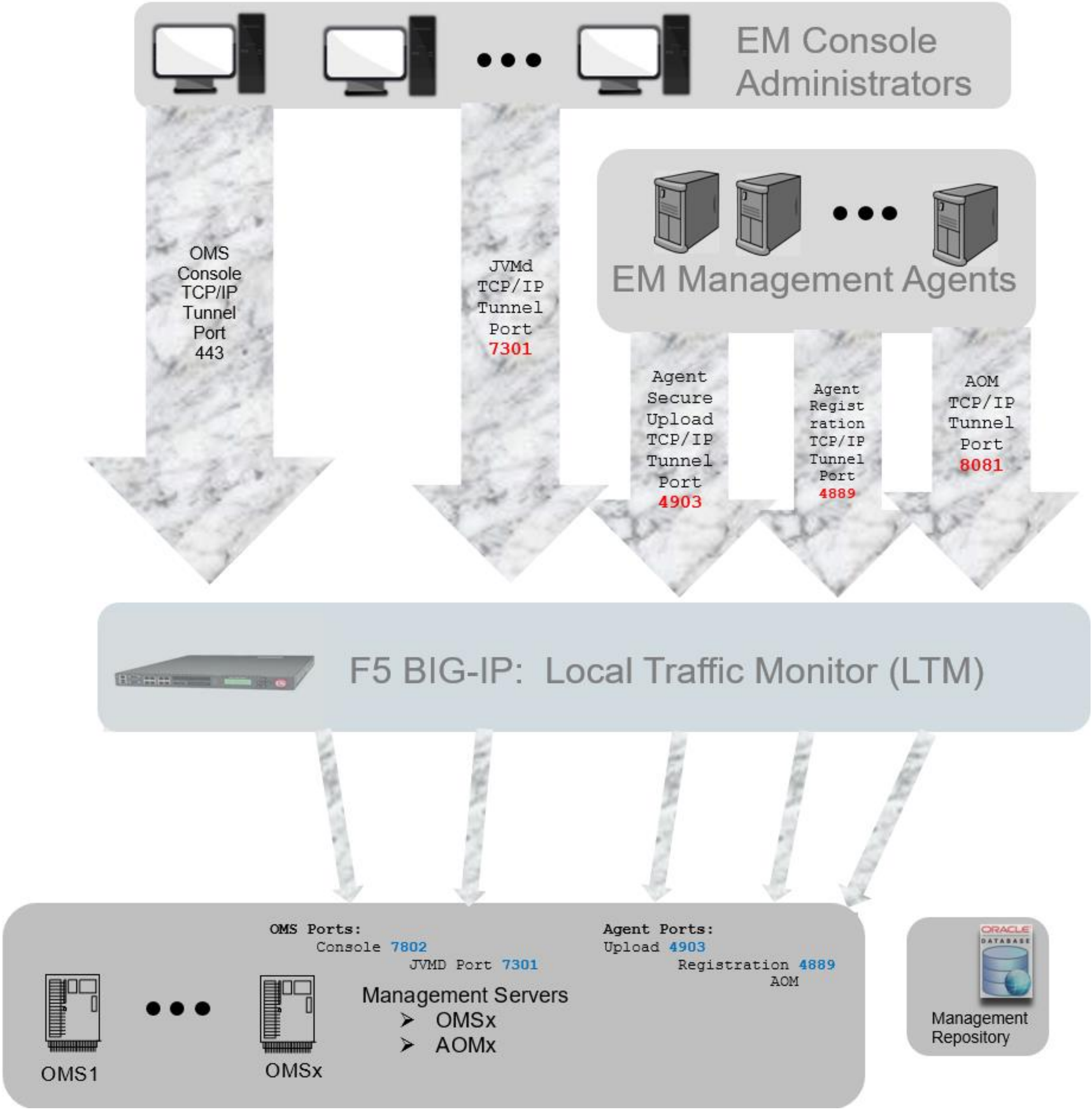

EM Console Administrators
OMS Console TCP/IP Tunnel Port 443
JVMd TCP/IP Tunnel Port 7301
EM Management Agents
Agent Secure Upload TCP/IP Tunnel Port 4903
Agent Registration TCP/IP Tunnel Port 4889
AOM TCP/IP Tunnel Port 8081
F5 BIG-IP: Local Traffic Monitor (LTM)
OMS Ports:
Console 7802
JVMD Port 7301
Agent Ports:
Upload 4903
Registration 4889
AOM
Management Servers
OMSx
AOMx
OMS1
OMSx
ORACLE DATABASE
Management Repository

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)

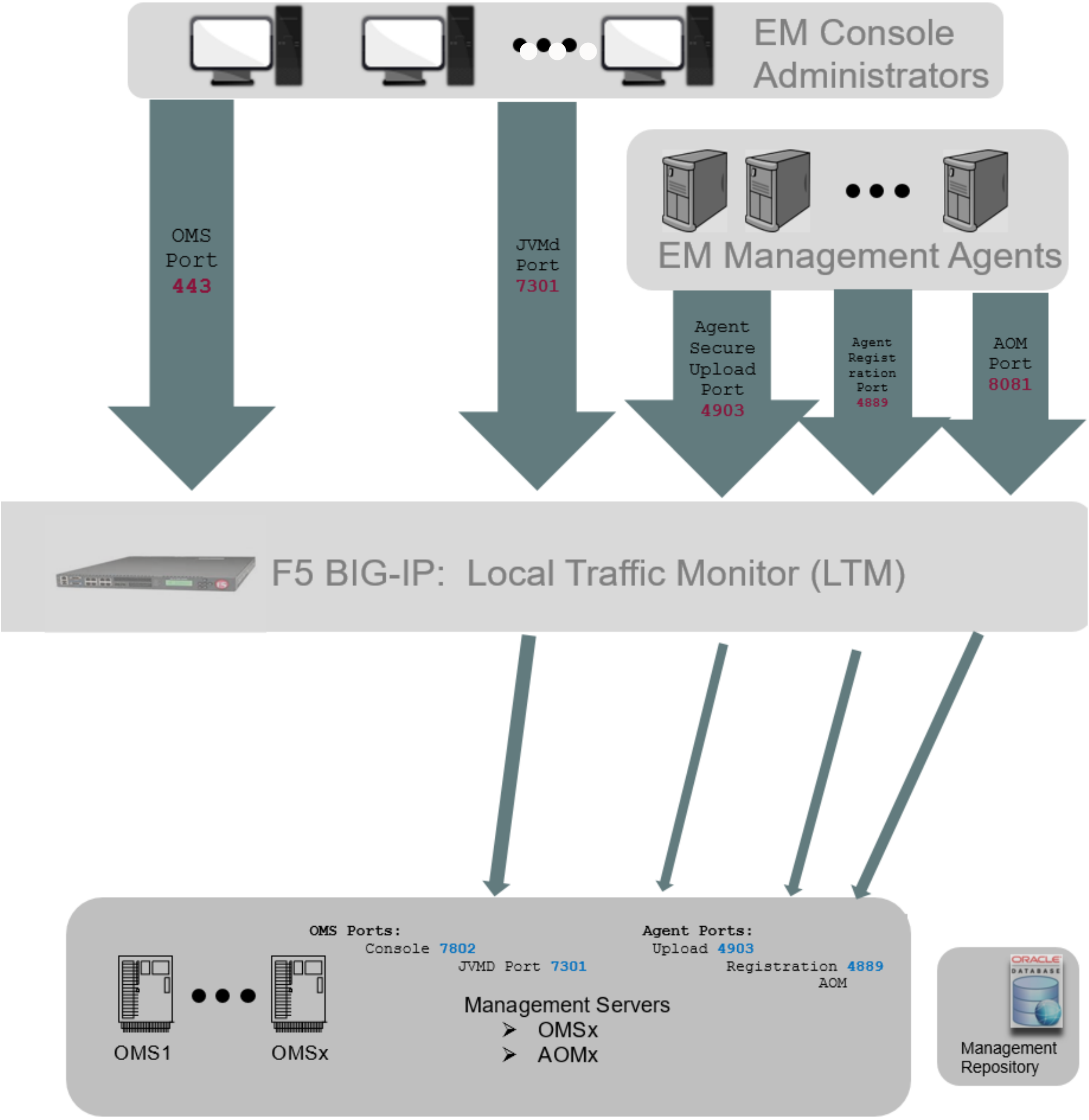


Figure 2. Enterprise Manager 13c Cloud Control High Availability Architecture: SSL Proxying

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.

CLOUD CONTROL SERVICE	DESCRIPTION	CONVENTIONAL PORT
Secure Console	HTTPS access to Cloud Control Console	443 (default https port)
Secure Upload	Secure Agent to OMS communication	4903
Agent Registration	Unsecure Agent to OMS communication	4889
Secure Always-On Monitoring Upload	Secure Agent to AOM communication	8081
Secure JVMD	Secure JVMD	7301

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 Port**s 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).

BROWSER ACCESS	DESCRIPTION
https://slb.example.com/em	Cloud Control Console

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.

BIG-IP CONFIGURATION OBJECT	CONVENTION
SSL Certificate	Internal Host Name for EM Virtual Server. Recommended to be forward and reverse DNS resolvable. Samples use 'slb.example.com'
Cipher Rules	cipher_ccsc
Cipher Group	cipher_ccsc
SSL Client Profile	sslclient_ccsc
SSL Server Profile	sslserver_ccsc
Health Monitors	mon_<service_label>[aom | jvmd]
TCP Profiles	tcp_<service_label>[aom | jvmd]
Nodes	Internal IT Conventions Samples provided as emomsX.example.com
Pools	pool_<service_label>[aom | jvmd]
Cookie Persistence Profile	cookie_<service_label>
Source IP Address Persistence Profile	sourceip_<service_label>[aom | jvmd]
Virtual Server	vs_<service_label>[aom | jvmd]<port>

Table 3. Naming Convention for BIG-IP Configuration Objects

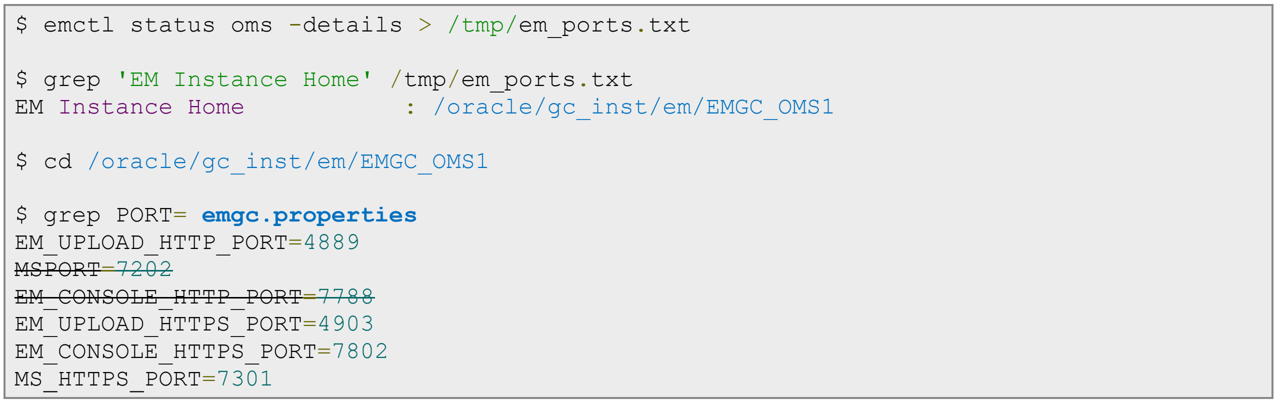
- As an example, the Secure Console services uses "**ccsc**" as the service label.
- The optional Insecure Console Services for the OMS uses "**ccuc**" as the service label.

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.

PORT	CLOUD CONTROL SERVICE	DESCRIPTION	CROSS REFERENCE FROM EMGC.PROPERTIES
7802	Secure Console	HTTPS browser access to Cloud Control	EM_CONSOLE_HTTPS_PORT
4903	Secure Upload Port	HTTPS EM Agent access to Cloud Control Uploads	EM_UPLOAD_HTTPS_PORT
4889	Cloud Control Agent Registration Port	HTTP EM Agents, for Agent Registration, to Cloud Control.	EM_UPLOAD_HTTP_PORT
8081	Secure Always-On Monitoring (If configured)	HTTPS EM Agent access to AOM uploads.	Refer to Configure Always-On Monitoring
7301	Cloud Control Secure JVMD Port (Managed Server HTTP SSL Port)	HTTPS Access for JVMD	MS_HTTPS_PORT

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 the ports that are accessible directly by Enterprise Manager Administrators and Management Agents, via the F5 BIG-IP LTM are:

PORT	DESCRIPTION
443	Cloud Control Secure Console (Note: 443 is the default SSL port, so it is not necessary to provide it in the URL).
4903	Cloud Control Secure Upload
4889	Cloud Control Agent Registration Port
8081	Always-On Monitoring Secure Upload Port (If configured)
7301	Cloud Control Secure JVMD
80	Redirect iRule for Cloud Control Secure Console

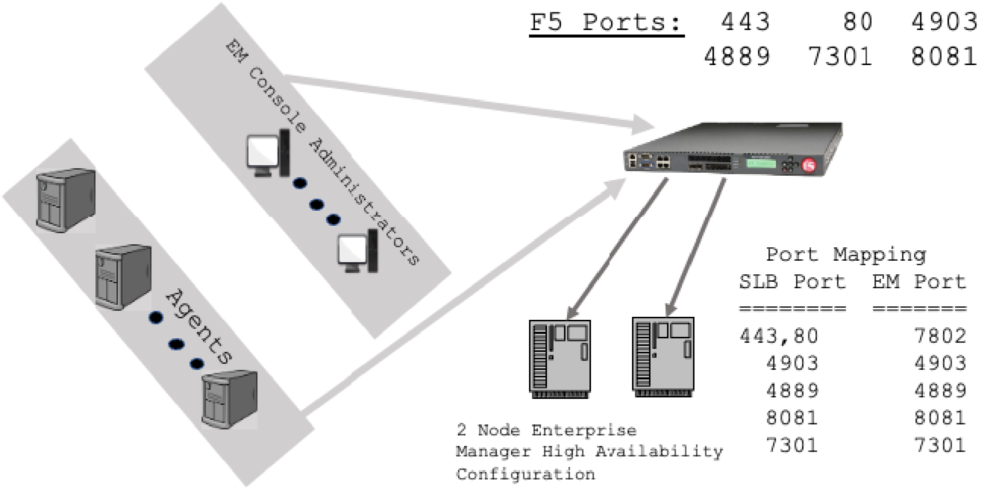
Table 5. Ports on the F5 BIG-IP LTM

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.
  - o 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.
  - o This traffic will be redirected to the respective ports of the Enterprise Manager Management Servers (OMSs).


F5 Ports: 443 80 4903
4889 7301 8081
EM Console Administrators
Agents
2 Node Enterprise Manager High Availability Configuration

Port Mapping

SLB Port	EM Port
========	=======
443,80	7802
4903	4903
4889	4889
8081	8081
7301	7301

Figure 4. Mapping between F5 Ports and EM Host Ports

F5 BIG-IP LTM configuration objects for this white paper

CLOUD CONTROL SERVICE	TCP PORT ON EM HOSTS	MONITOR NAME	TCP PROFILE NAME	PERSISTENCE PROFILE	POOL NAME	VIRTUAL SERVER NAME	VIRTUAL SERVER PORT SLB
Secure Console	7802	mon_ccsc	tcp_ccsc	sourceip_ccsc or cookie_ccsc	pool_ccsc	vs_ccsc443	443
Unsecure Console Optional Redirects to Secure Console using F5 BIG-IP LTM iRules	N/A	N/A	tcp_ccuc	N/A	N/A	vs_ccuc80	80
Secure Upload	4903	mon_ccsu Optional: mon_cc_halfopen Appendix A: optimization of pool monitoring	tcp_ccsu	None	pool_ccsu	vs_ccsu4903	4903
Agent Registration	4889	mon_ccar	tcp_ccar	cookie_ccar	pool_ccar	vs_ccar4889	4889
Always-On Monitoring Secure Upload (If configured)	8081	mon_ccaom	tcp_ccaom	None	pool_ccaom	vs_ccaom8081	8081
Secure JVMD	7301	mon_ccsjvmd	tcp_ccsjvmd	sourceip_ccsjvmd or cookie_ccsjvmd	pool_ccsjvmd	vs_ccsjvmd7301	7301
Unsecure JVMD (Not Recommended) *	**7202**	**mon_ccujvmd**	**tcp_ccujvmd**	**sourceip_ccujvmd** **or** **cookie_ccujvmd**	**pool_ccujvmd**	**vs_ccujvmd7202**	**7202**

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

***** *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.*

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.

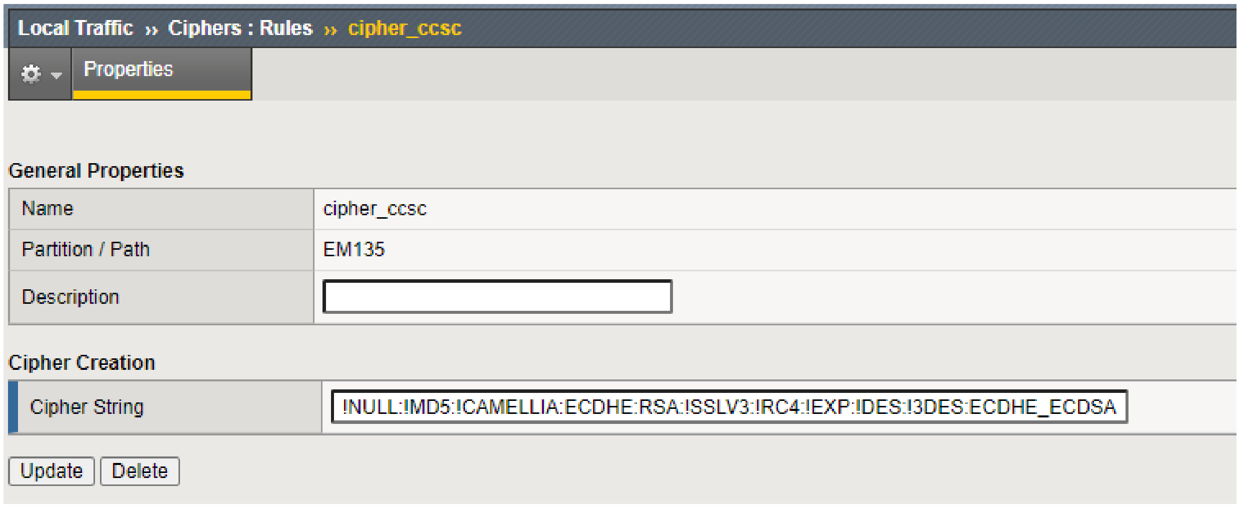
For example, any modern Webserver would limit traffic to TLS1.2 or greater, and not support insecure ciphers, such as MD5.

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.
4. On the Menu bar, from the **Ciphers: Rules** menu, select **Rules.**
5. In the upper-right portion of the screen, click **Create**.
6. The New Cipher Rule screen opens.
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. New Perspective List:

```
!NULL:!MD5:!CAMELLIA:ECDHE:RSA:!SSLV3:!RC4:!EXP:!DES:!3DES:ECDHE_ECDSA
```

11. Possibly requires an F5 specific version of `:!SEED`
12. Old List: !NULL:!MD5:!CAMELLIA:ECDHE:RSA:!SSLV3:!RC4:!EXP:!DES:!3DES:ECDHE_ECDSA
13. Choose **Finished**.



General Properties

Name	cipher_ccsc
Partition / Path	EM135
Description	

Cipher Creation

Cipher String	!NULL:!MD5:!CAMELLIA:ECDHE:RSA:!SSLV3:!RC4:!EXP:!DES:!3DES:ECDHE_ECDSA

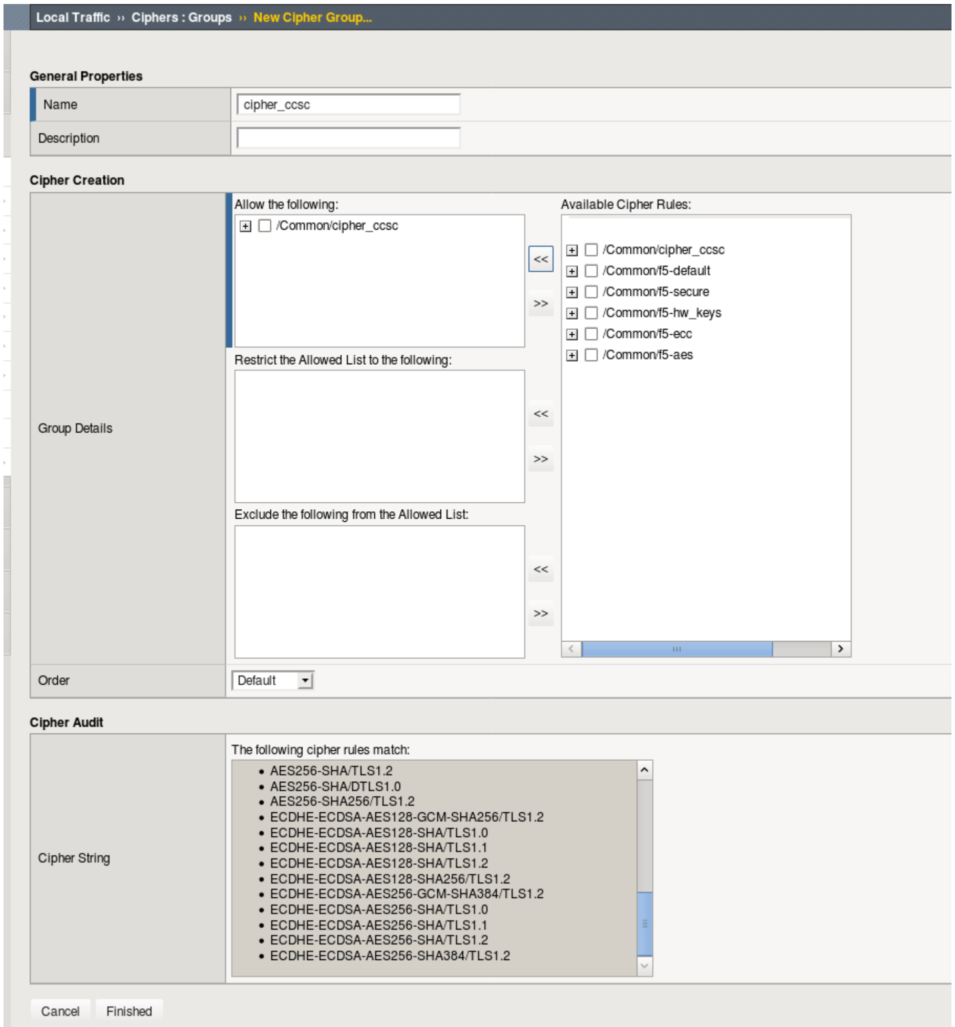
Figure 5. Example of finished definition of Cipher Rule

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**.
6. The New Cipher Rule screen opens.
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 String**s.
10. Choose **Finished**.



General Properties

Name: cipher_ccsc

Description:

Cipher Creation

Group Details

Allow the following:
- ⊞ □ /Common/cipher_ccsc

Restrict the Allowed List to the following:

Exclude the following from the Allowed List:

Available Cipher Rules:
- ⊞ □ /Common/cipher_ccsc
- ⊞ □ /Common/f5-default
- ⊞ □ /Common/f5-secure
- ⊞ □ /Common/f5-hw_keys
- ⊞ □ /Common/f5-ecc
- ⊞ □ /Common/f5-aes

Order: Default

Cipher Audit

Cipher String

The following cipher rules match:
- AES256-SHA/TLS1.2
- AES256-SHA/DTLS1.0
- AES256-SHA256/TLS1.2
- ECDHE-ECDSA-AES128-GCM-SHA256/TLS1.2
- ECDHE-ECDSA-AES128-SHA/TLS1.0
- ECDHE-ECDSA-AES128-SHA/TLS1.1
- ECDHE-ECDSA-AES128-SHA/TLS1.2
- ECDHE-ECDSA-AES128-SHA256/TLS1.2
- ECDHE-ECDSA-AES256-GCM-SHA384/TLS1.2
- ECDHE-ECDSA-AES256-SHA/TLS1.0
- ECDHE-ECDSA-AES256-SHA/TLS1.1
- ECDHE-ECDSA-AES256-SHA/TLS1.2
- ECDHE-ECDSA-AES256-SHA384/TLS1.2

Figure 6. Example of finished definition of the Cipher Group

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`

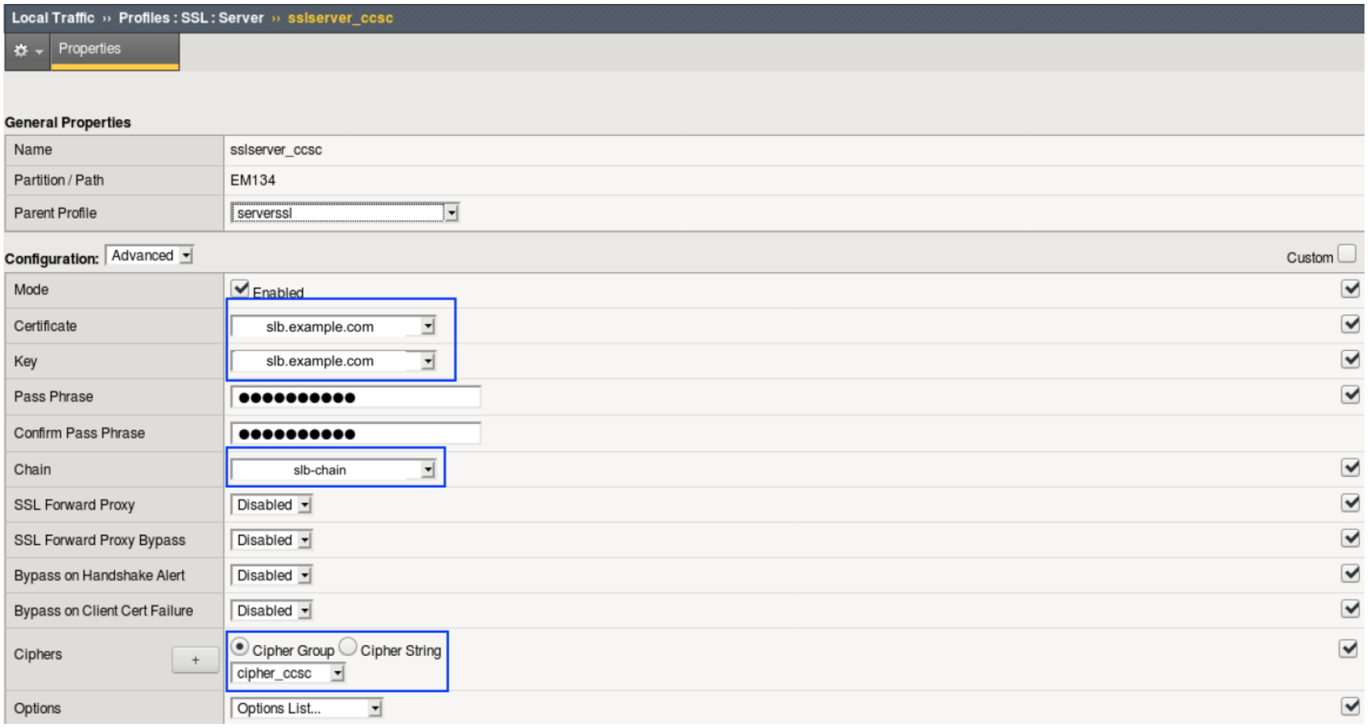
- This certificate chain is required when utilizing ‘SSL Proxying***, variation ii***. Valid third-party SSL certificates installed on the F5 BIG-IP LTM, and self-signed SSL certificates installed on each EM system, for each OMS component.
- This certificate chain is necessary to form the required *trust 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.
16. Choose **Finished**.



Local Traffic ›› Profiles : SSL : Server ›› sslserver_ccsc

Properties

General Properties

Name	sslserver_ccsc
Partition / Path	EM134
Parent Profile	serverssl

Configuration: Advanced — Custom □

Mode	☑ Enabled	☑
Certificate	slb.example.com	☑
Key	slb.example.com	☑
Pass Phrase	●●●●●●●●●●●	☑
Confirm Pass Phrase	●●●●●●●●●●●	
Chain	slb-chain	☑
SSL Forward Proxy	Disabled	☑
SSL Forward Proxy Bypass	Disabled	☑
Bypass on Handshake Alert	Disabled	☑
Bypass on Client Cert Failure	Disabled	☑
Ciphers +	● Cipher Group ○ Cipher String cipher_ccsc	☑
Options	Options List...	☑

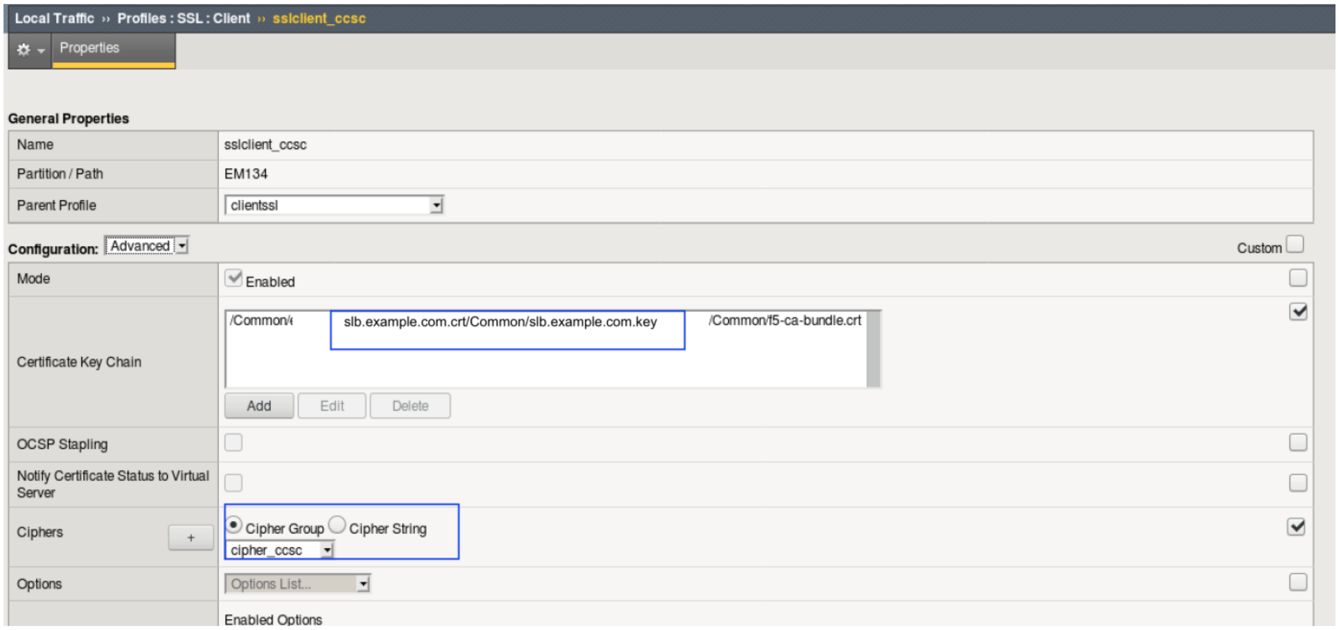
Figure 7. Example of a finished definition of the Server SSL Profile

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**.



Local Traffic ›› Profiles : SSL : Client ›› sslclient_ccsc

Properties

General Properties

Name	sslclient_ccsc
Partition / Path	EM134
Parent Profile	clientssl

Configuration: Advanced — Custom ☐

Mode	☑ Enabled	☐
Certificate Key Chain	/Common/(slb.example.com.crt/Common/slb.example.com.key /Common/f5-ca-bundle.crt Add Edit Delete	☑
OCSP Stapling	☐	☐
Notify Certificate Status to Virtual Server	☐	☐
Ciphers +	● Cipher Group ○ Cipher String cipher_ccsc	☑
Options	Options List...	☐
	Enabled Options	

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

CLOUD CONTROL SERVICE	MONITOR NAME	TYPE	SSL PROFILE	INTERVAL	TIMEOUT
Secure Console	mon_ccsc	HTTPS	sslserver_ccsc	5	16
Unsecure Console (not recommended)	mon_ccuc	HTTP	N/A	5	16
Secure Upload	mon_ccsu	HTTPS	Optional	60 (See Above)	181
Optional: mon_cc_halfopen (Appendix A: optimization of pool monitoring)	mon_cc_halfopen	TCP Half Open	N/A	5	16
Agent Registration	mon_ccar	HTTP	N/A	60	181
Always-On Monitoring (If configured)	mon_ccaom	HTTPS	Optional	60	181
Secure JVMD	mon_ccsjvmd	HTTPS	Optional	60	181
Unsecure JVMD (not recommended)	mon_ccujvmd	HTTP	N/A	60	181

Table 7. Health Monitors to utilize for Enterprise Manager 13.5

Health Monitor Send/Receive Strings

MONITOR NAME	SEND STRING	RECEIVE STRING
mon_ccsc	`GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Enterprise Manager Console is UP`
mon_ccuc (Optional)	`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 (If configured)	`GET /upload HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Always On Monitoring is active`
mon_ccsjvmd	`GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Reply to empty request`
Optional: on_cc_half_open	`N/A`	`N/A`
mon_ccujvmd : Not recommended	`GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Reply to empty request`

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 (ie. `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.

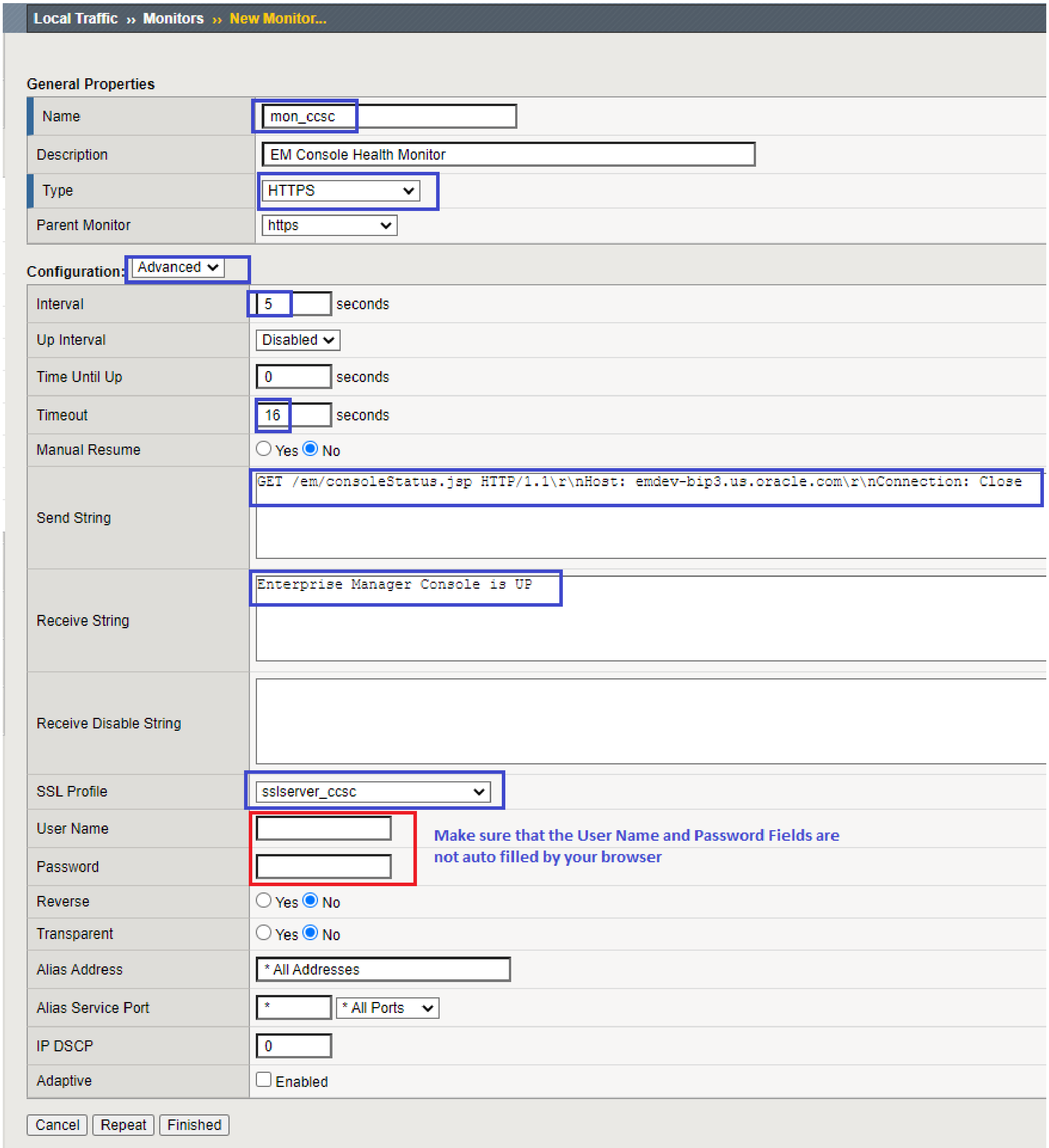
- The value specified of the **`Host:`** header shall be a resolvable hostname.
  - The associated IP address for the given hostname shall match the destination server to which the request is sent.
  - If the value of Host: header does not meet these requirements, the server is to return an error code 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 * "**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.



Local Traffic ›› Monitors ›› New Monitor...

General Properties

Name	mon_ccsc
Description	EM Console Health Monitor
Type	HTTPS
Parent Monitor	https

Configuration: Advanced

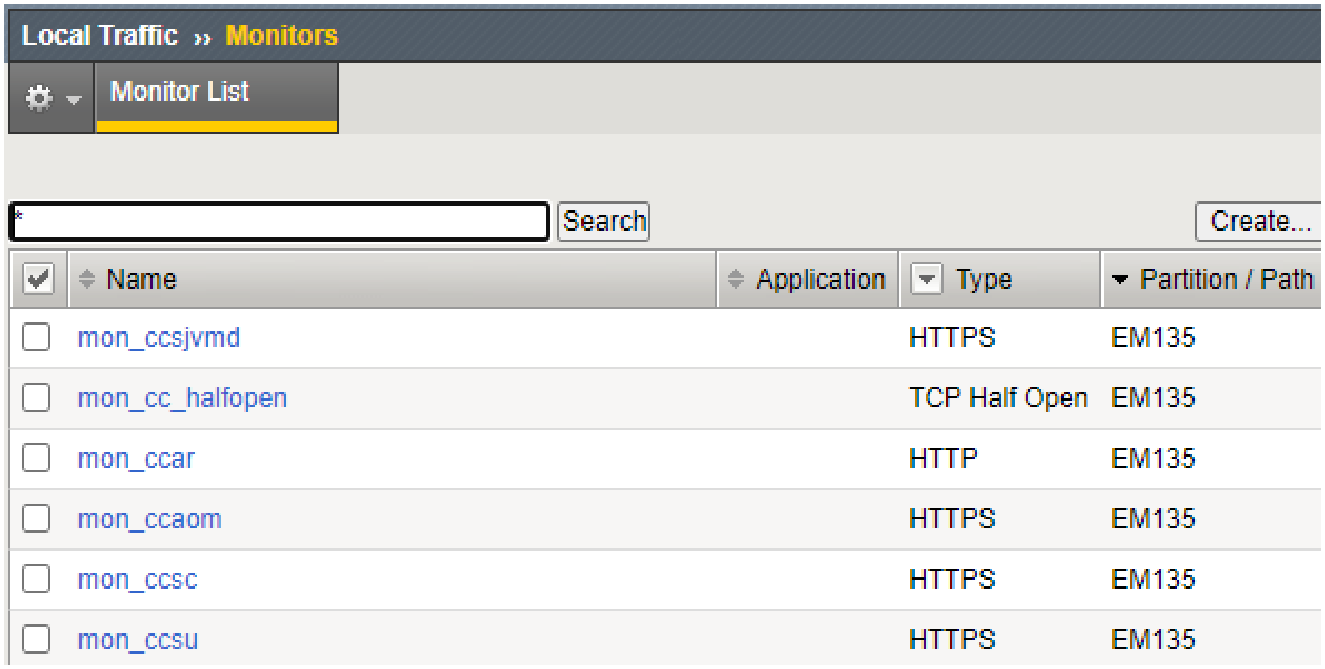
Interval	5 seconds
Up Interval	Disabled
Time Until Up	0 seconds
Timeout	16 seconds
Manual Resume	○ Yes ● No
Send String	`GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: emdev-bip3.us.oracle.com\r\nConnection: Close`
Receive String	`Enterprise Manager Console is UP`
Receive Disable String	
SSL Profile	sslserver_ccsc
User Name	
Password	
Reverse	○ Yes ● No
Transparent	○ Yes ● No
Alias Address	* All Addresses
Alias Service Port	* * All Ports
IP DSCP	0
Adaptive	□ Enabled

Make sure that the User Name and Password Fields are not auto filled by your browser

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).



☑	Name	Application	Type	Partition / Path
□	mon_ccsjvmd		HTTPS	EM135
□	mon_cc_halfopen		TCP Half Open	EM135
□	mon_ccar		HTTP	EM135
□	mon_ccaom		HTTPS	EM135
□	mon_ccsc		HTTPS	EM135
□	mon_ccsu		HTTPS	EM135

Figure 10. Screenshot of all required health monitors

F5 NODE DEFINITIONS

FROM F5 - ASKF5

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.

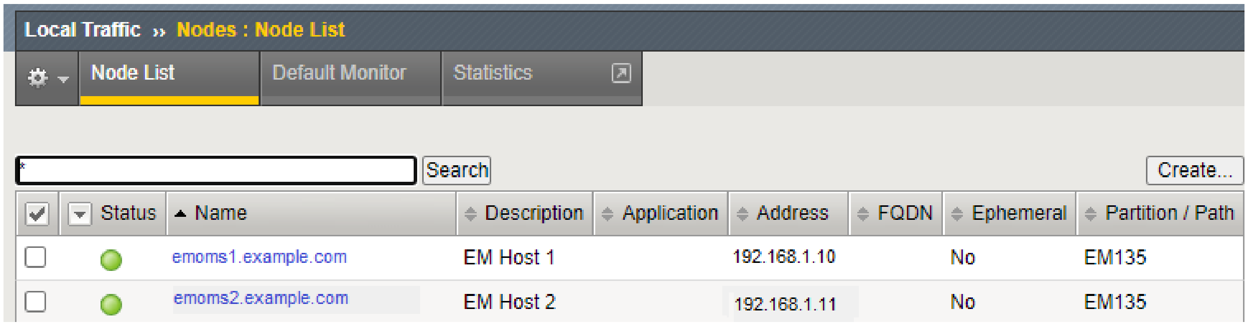
The difference between a node and a pool member is that a node is designated by the device's IP address only (192.168.1.10), while designation of a pool member includes an IP address and a service (such as 192.168.1.10:443.

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.



☑	Status	Name	Description	Application	Address	FQDN	Ephemeral	Partition / Path
□	●	emoms1.example.com	EM Host 1		192.168.1.10		No	EM135
□	●	emoms2.example.com	EM Host 2		192.168.1.11		No	EM135

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.

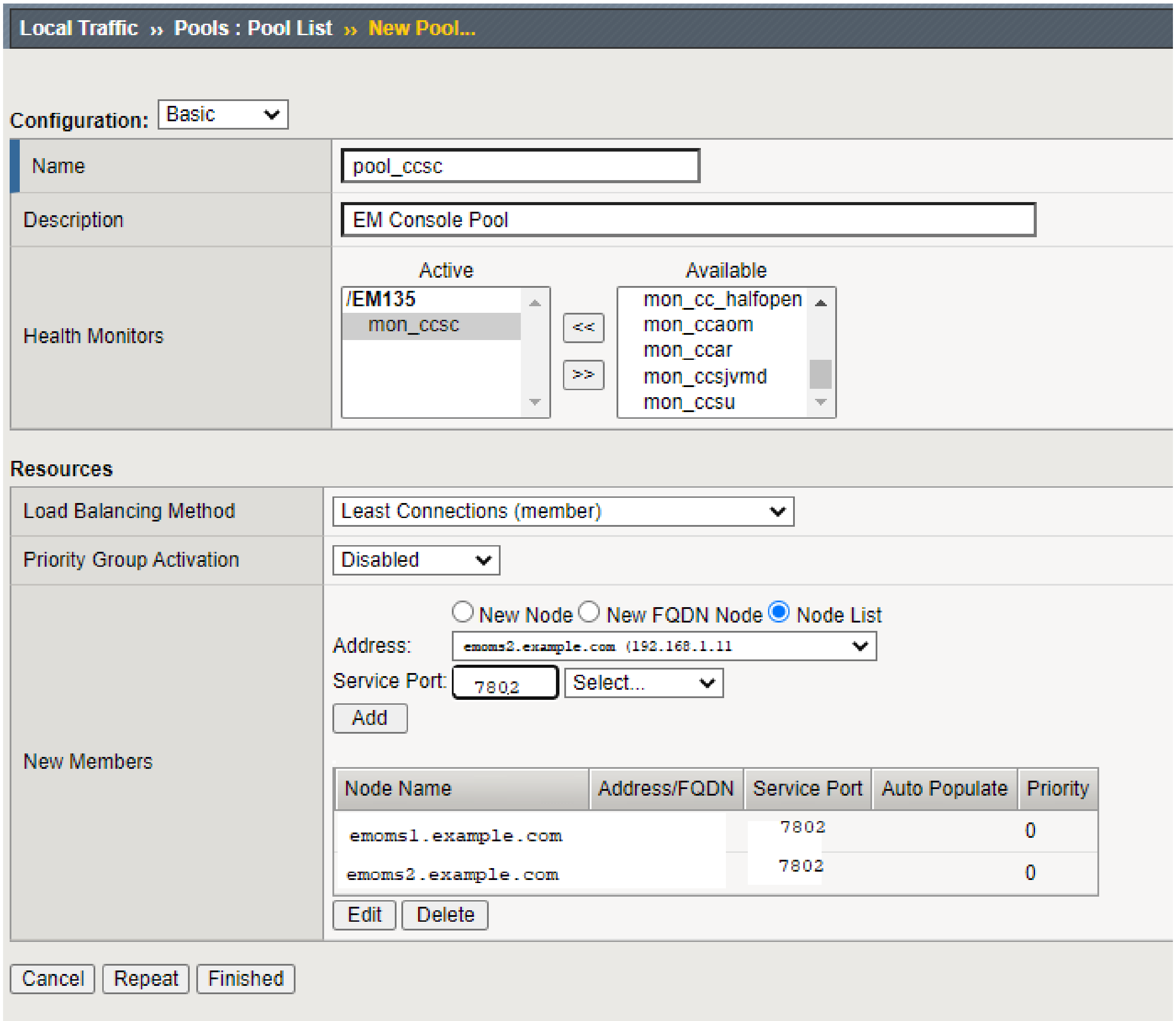
CLOUD CONTROL SERVICE	POOL NAME	ASSOCIATED HEALTH MONITOR	LOAD BALANCING	MEMBERS
Secure Console	pool_ccsc	mon_ccsc	Least Connections (member)	OMS Host A:7802 OMS Host B:7802
Secure Upload	pool_ccsu	mon_ccsu Optional: mon_cc_halfopen Appendix A: optimization of pool monitoring	Least Connections (member)	OMS Host A:4903 OMS Host B:4903
Agent Registration	pool_ccar	mon_ccar	Least Connections (member)	OMS Host A:4889 OMS Host B:4889
Always-On Monitoring Secure Upload	pool_ccaom	mon_ccaom	Least Connections (member)	OMS Host A:8081 OMS Host B:8081
Secure JVMD	pool_ccsjvmd	mon_ccsjvmd	Least Connections (member)	OMS Host A:7301 OMS Host B:7301
Unsecure JVMD (Not recommended)	pool_ccujvmd	mon_ccujvmd	Least Connections (member)	OMS Host A:7202 OMS Host B:7202

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**.
3. The New Pool screen opens.
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.



Local Traffic » Pools : Pool List » New Pool...

Configuration: Basic

Name	pool_ccsc
Description	EM Console Pool
Health Monitors	Active: /EM135 mon_ccsc Available: mon_cc_halfopen, mon_ccaom, mon_ccar, mon_ccsjvmd, mon_ccsu

Resources

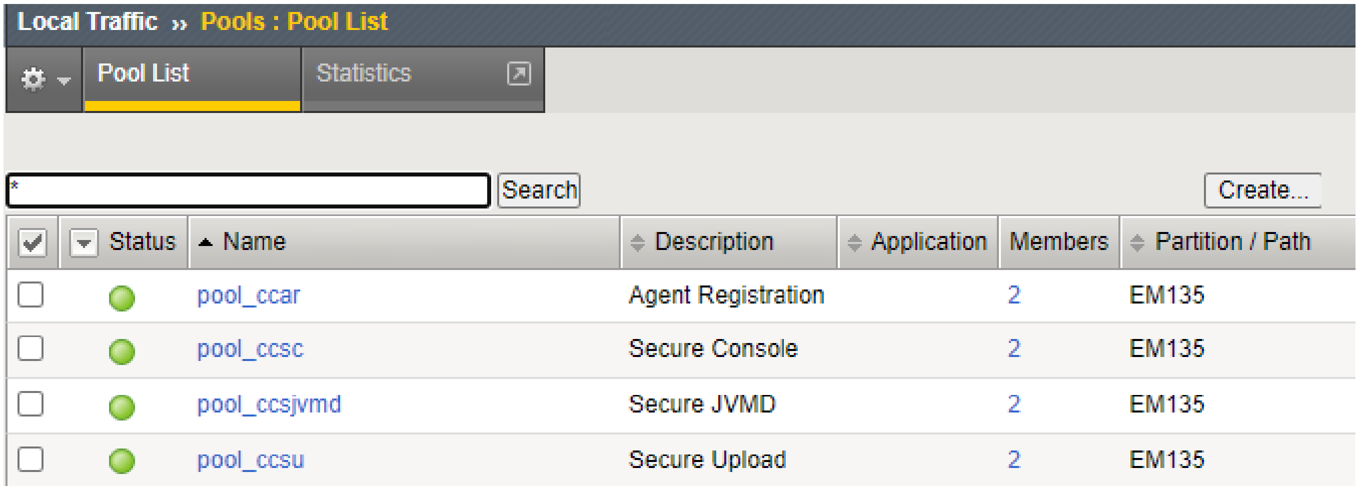
Load Balancing Method	Least Connections (member)
Priority Group Activation	Disabled
New Members	○ New Node ○ New FQDN Node ● Node List Address: emoms2.example.com (192.168.1.11 Service Port: 7802 Select...

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
emoms1.example.com		7802		0
emoms2.example.com		7802		0

Figure 12. Example of finished definition of a F5 pool

Completed Pools

Below is an example showing all the required pools.



☑	Status	Name	Description	Application	Members	Partition / Path
□	●	pool_ccar	Agent Registration		2	EM135
□	●	pool_ccsc	Secure Console		2	EM135
□	●	pool_ccsjvmd	Secure JVMD		2	EM135
□	●	pool_ccsu	Secure Upload		2	EM135

Figure 13. Screenshot of all required pools

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.

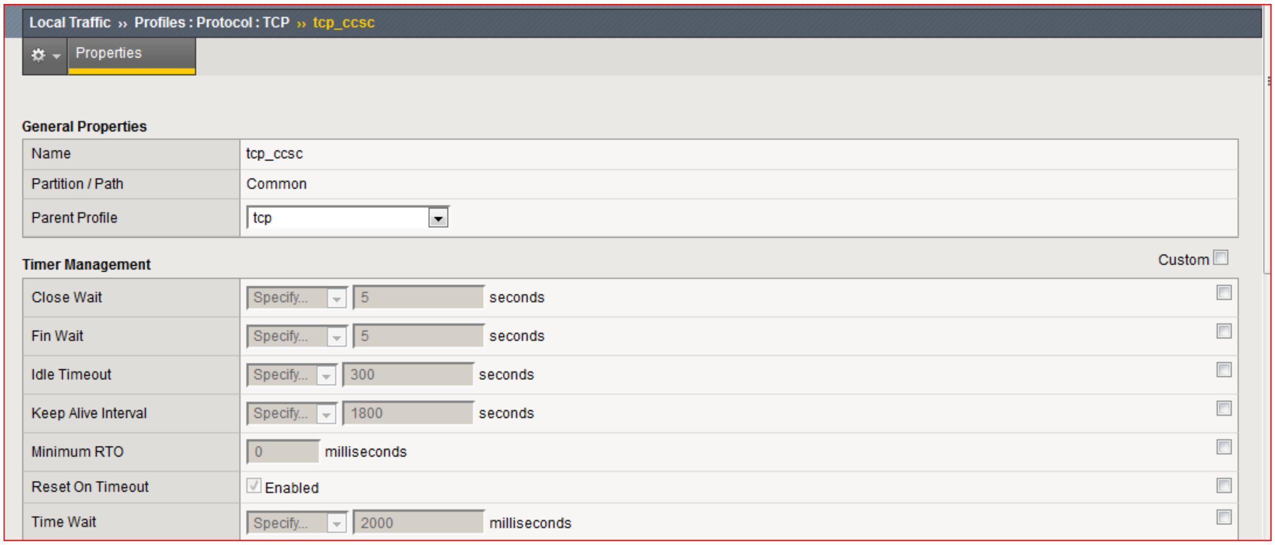
A TCP profile must be created for each of the Cloud Control services using the following table:

CLOUD CONTROL SERVICE	TCP PROFILE NAME
Secure Console	tcp_ccsc
Unsecure Console	tcp_ccuc
Secure Upload	tcp_ccsu
Agent Registration	tcp_ccar
Always-On Monitoring Secure Upload	tcp_ccaom
Secure JVMD	tcp_ccsjvmd
Unsecure JVMD (not recommended)	tcp_ccujvmd

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.



General Properties

Name	tcp_ccsc
Partition / Path	Common
Parent Profile	tcp

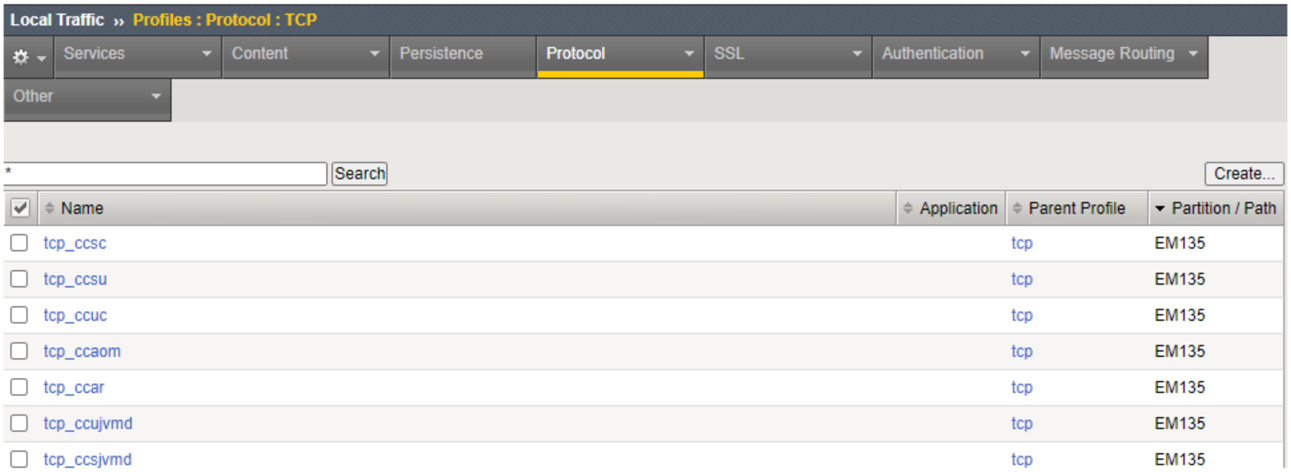
Timer Management — Custom □

Close Wait	Specify... 5 seconds	□
Fin Wait	Specify... 5 seconds	□
Idle Timeout	Specify... 300 seconds	□
Keep Alive Interval	Specify... 1800 seconds	□
Minimum RTO	0 milliseconds	□
Reset On Timeout	☑ Enabled	□
Time Wait	Specify... 2000 milliseconds	□

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:



☑	Name	Application	Parent Profile	Partition / Path
□	tcp_ccsc		tcp	EM135
□	tcp_ccsu		tcp	EM135
□	tcp_ccuc		tcp	EM135
□	tcp_ccaom		tcp	EM135
□	tcp_ccar		tcp	EM135
□	tcp_ccujvmd		tcp	EM135
□	tcp_ccsjvmd		tcp	EM135

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.

PERSISTENCE PROFILE TYPE	TIMEOUT	EXPIRATION	SHORT HAND	COMMENTS
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 Persistience		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	• Only usable if '*session 'stickiness'* is not required.

Table 11. 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.

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

Table 12. Persistence Profile Options

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

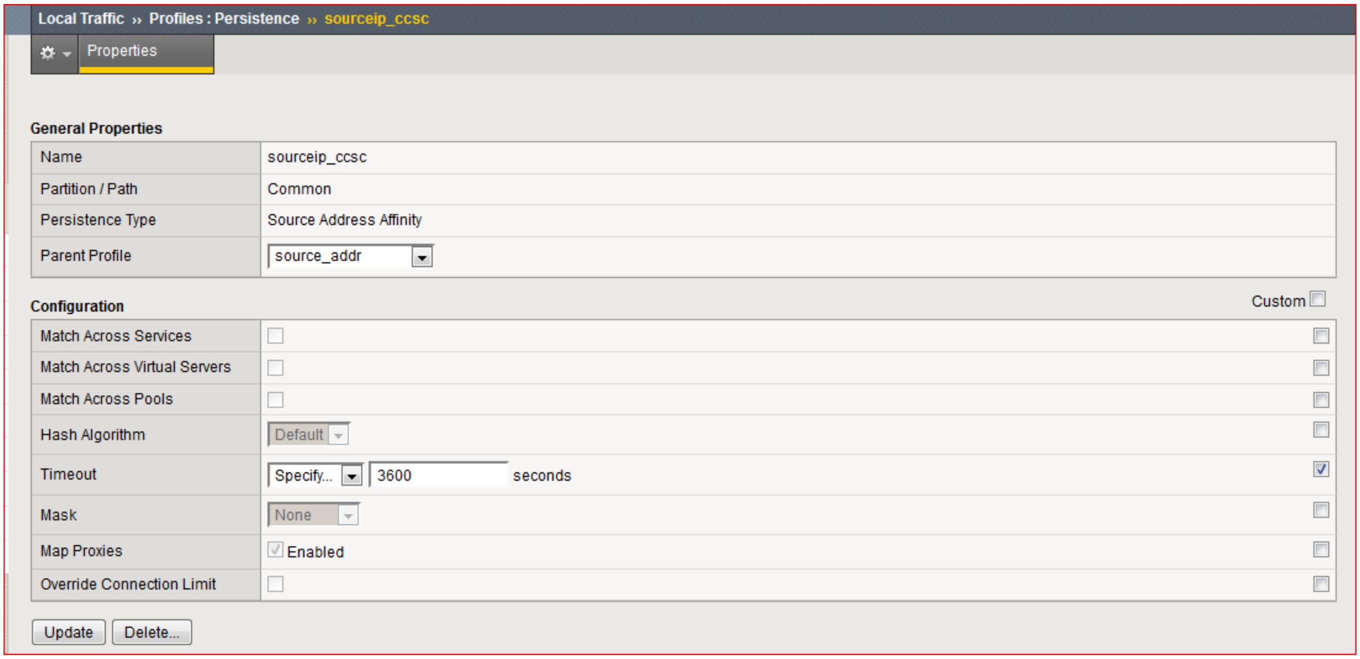
CREATE THE PERSISTENCE PROFILES

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**.
6. The New Persistence Profile screen opens.
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 Afinity, follow just the first set of steps below.
11. For Persistence Profiles utilizing Cookie Persisitence, 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.



Local Traffic ›› Profiles : Persistence ›› sourceip_ccsc

General Properties

Name	sourceip_ccsc
Partition / Path	Common
Persistence Type	Source Address Affinity
Parent Profile	source_addr

Configuration

		Custom □
Match Across Services	□	□
Match Across Virtual Servers	□	□
Match Across Pools	□	□
Hash Algorithm	Default	□
Timeout	Specify... 3600 seconds	☑
Mask	None	□
Map Proxies	☑ Enabled	□
Override Connection Limit	□	□

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**.

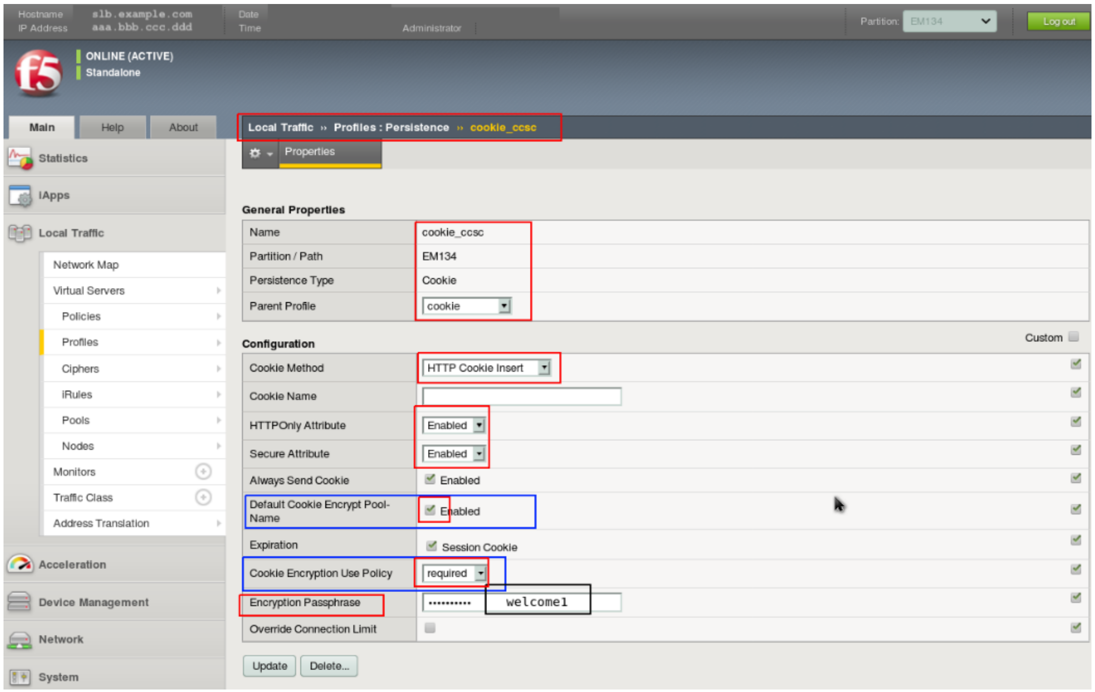
15. Based on internal security requirements, select the check box next to **Default Cookie Encrypt Pool-Name** to allow the Default Cookie Encrypt Pool-Name to be specified.

    » 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.



General Properties

Name	cookie_ccsc
Partition / Path	EM134
Persistence Type	Cookie
Parent Profile	cookie

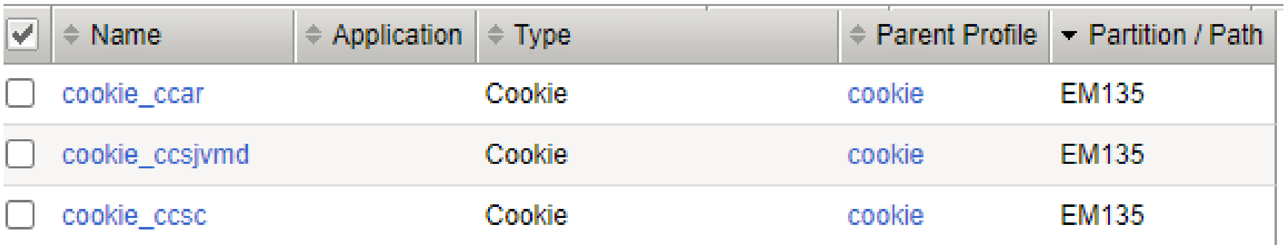
Configuration

		Custom □
Cookie Method	HTTP Cookie Insert	☑
Cookie Name		☑
HTTPOnly Attribute	Enabled	☑
Secure Attribute	Enabled	☑
Always Send Cookie	☑ Enabled	☑
Default Cookie Encrypt Pool-Name	☑ Enabled	☑
Expiration	☑ Session Cookie	☑
Cookie Encryption Use Policy	required	☑
Encryption Passphrase	•••••••••• welcome1	☑
Override Connection Limit	□	☑

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.



☑	Name	Application	Type	Parent Profile	Partition / Path
□	cookie_ccar		Cookie	cookie	EM135
□	cookie_ccsjvmd		Cookie	cookie	EM135
□	cookie_ccsc		Cookie	cookie	EM135

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.

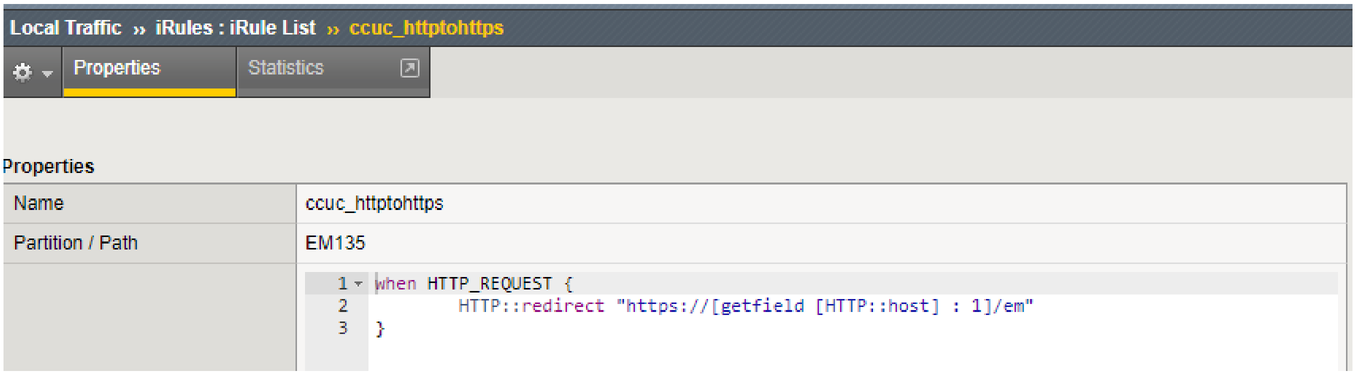
Unsecure Console service Redirect iRule

```
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_**httptohttps**.
4. Copy the appropriate iRule text from the section above and paste it in the **Definition** section
5. Click Finished.



Properties

Name	ccuc_httptohttps
Partition / Path	EM135

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

Figure 20. Definition of redirect iRule

Full set of valid URLs after iRule creation

URL	CLOUD CONTROL COMPONENT
https://slb.example.com	Invalid URL - /em is required for EM 13.5
https://slb.example.com/em	Enterprise Manager Cloud Control Secure Console
slb.example.com	Enterprise Manager Cloud Control Secure (via redirect) Console
slb.example.com/em	Enterprise Manager Cloud Control Secure (via redirect) Console

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

	VIRTUAL SERVER					
	SECURE CONSOLE	UNSECURE CONSOLE	SECURE UPLOAD	AGENT REGISTRATION	ALWAYS-ON MONITORING	SECURE JVMD
VIRTUAL SERVER NAME	vs_ccsc443	vs_ccuc80	vs_ccsu4903	vs_ccar4889	vs_ccaom8081	vs_ccsjvmd7301
VIRTUAL IP:PORT	VIP:443	VIP:80	VIP:4903	VIP:4889	VIP:8081	VIP:7301
PROTOCOL PROFILE (CLIENT)	tcp_ccsc	tcp_ccuc	tcp_ccsu	tcp_ccar	tcp_ccaom	tcp_ccsjvmd
HTTP PROFILE	None	http	None	http	None	None
SSL CLIENT PROFILE	None					
SSL SERVER PROFILE	None					
SOURCE ADDRESS TRANSLATION	Auto Map					
IRULE	None	ccuc_httptohttps	None	None	None	None
DEFAULT POOL	pool_ccsc	None	pool_ccsu	pool_ccar	pool_ccaom	pool_ccsjvmd
DEFAULT PERSISTENCE PROFILE	sourceip_ccsc	None	None	cookie_ccar	None	sourceip_ccsjvmd

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.

	VIRTUAL SERVER					
	SECURE CONSOLE	UNSECURE CONSOLE	SECURE UPLOAD	AGENT REGISTRATION	ALWAYS ON MONITORING	SECURE JVMD
VIRTUAL SERVER NAME	vs_ccsc443	vs_ccuc80	vs_ccsu4903	vs_ccar4889	vs_ccaom8081	vs_ccsjvmd7301
VIRTUAL IP:PORT	VIP:443	VIP:80	VIP:4903	VIP:4889	VIP:8081	VIP:7301
PROTOCOL PROFILE (CLIENT)	tcp_ccsc	tcp_ccuc	tcp_ccsu	tcp_ccar	tcp_ccaom	tcp_ccsjvmd
HTTP PROFILE	**saf** None **cookie** http	http	None	None	None	**saf** None **cookie** http
SSL CLIENT PROFILE	sslclient_ccsc	None	None	None	None	sslclient_ccsc
SSL SERVER PROFILE	sslserver_ccsc	None	None	None	sslserver_ccsc	sslserver_ccsc
SOURCE ADDRESS TRANSLATION	Auto Map					
IRULE	None	ccuc_httptohttps	None	None	None	None
DEFAULT POOL	pool_ccsc	None	pool_ccsu	pool_ccar	pool_ccaom	pool_ccsjvmd
DEFAULT PERSISTENCE PROFILE	**saf** sourceip_ccsc **cookie** cookie_ccsc	None	None	cookie_ccar	None	**saf** sourceip_ccsjvmd **cookie** cookie_ccsvmd

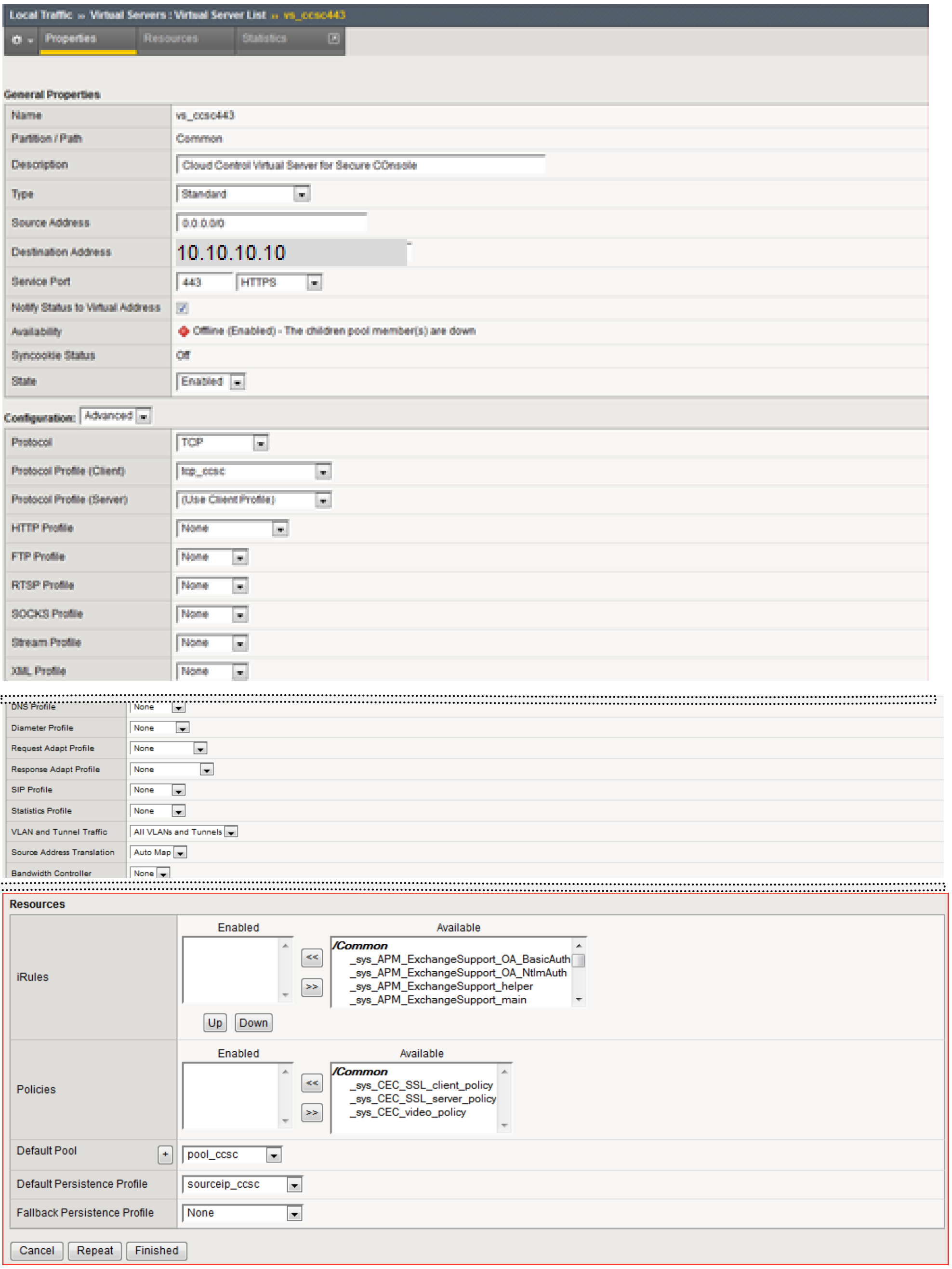
Table 15. BIG-IP F5 LTM Virtual Servers (SSL Proxying)

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.
4. The New Virtual Server screen opens.
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.



Local Traffic » Virtual Servers : Virtual Server List » vs_ccsc443

General Properties

Name	vs_ccsc443
Partition / Path	Common
Description	Cloud Control Virtual Server for Secure COnsole
Type	Standard
Source Address	0.0.0.0/0
Destination Address	10.10.10.10
Service Port	443 HTTPS
Notify Status to Virtual Address	☑
Availability	● Offline (Enabled) - The children pool member(s) are down
Syncookie Status	Off
State	Enabled

Configuration: Advanced

Protocol	TCP
Protocol Profile (Client)	tcp_ccsc
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	None
FTP Profile	None
RTSP Profile	None
SOCKS Profile	None
Stream Profile	None
XML Profile	None
DNS Profile	None
Diameter Profile	None
Request Adapt Profile	None
Response Adapt Profile	None
SIP Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map
Bandwidth Controller	None

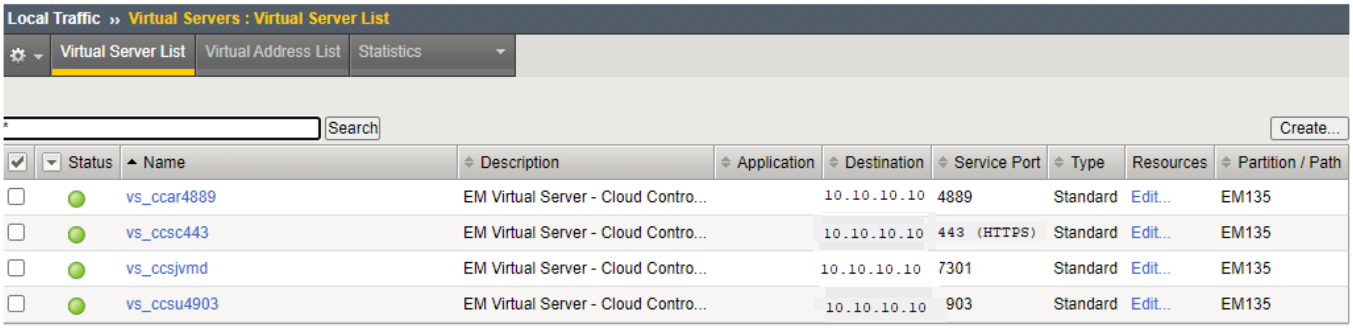
Resources

iRules	Enabled	Available /Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtlmAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main
Policies	Enabled	Available /Common _sys_CEC_SSL_client_policy _sys_CEC_SSL_server_policy _sys_CEC_video_policy
Default Pool	pool_ccsc	
Default Persistence Profile	sourceip_ccsc	
Fallback Persistence Profile	None	

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.

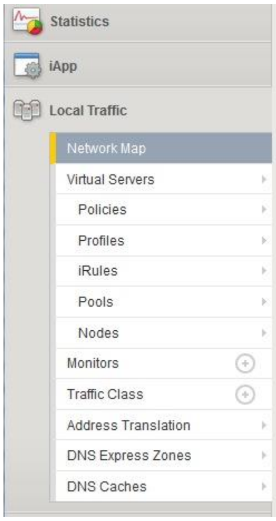


☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	vs_ccar4889	EM Virtual Server - Cloud Contro...		10.10.10.10	4889	Standard	Edit...	EM135
□	●	vs_ccsc443	EM Virtual Server - Cloud Contro...		10.10.10.10	443 (HTTPS)	Standard	Edit...	EM135
□	●	vs_ccsjvmd	EM Virtual Server - Cloud Contro...		10.10.10.10	7301	Standard	Edit...	EM135
□	●	vs_ccsu4903	EM Virtual Server - Cloud Contro...		10.10.10.10	903	Standard	Edit...	EM135

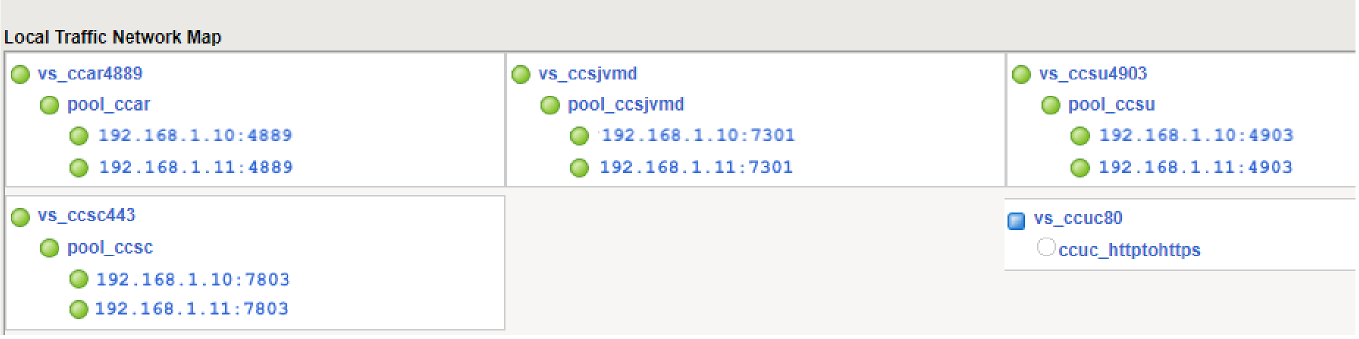
Figure 22. Screnshot of completed Virtual Servers – Secured HTTPS

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 anonymized).



Local Traffic Network Map

- ● vs_ccar4889
  - ● pool_ccar
    - ● 192.168.1.10:4889
    - ● 192.168.1.11:4889
- ● vs_ccsjvmd
  - ● pool_ccsjvmd
    - ● 192.168.1.10:7301
    - ● 192.168.1.11:7301
- ● vs_ccsu4903
  - ● pool_ccsu
    - ● 192.168.1.10:4903
    - ● 192.168.1.11:4903
- ● vs_ccsc443
  - ● pool_ccsc
    - ● 192.168.1.10:7803
    - ● 192.168.1.11:7803
- ■ vs_ccuc80
  - ○ ccuc_httptohttps

Figure 23. Example Network Map after completed configuration

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
Oracle Enterprise Manager Cloud Control 13c Release 5
Copyright (c) 1996, 2021 Oracle Corporation.  All rights reserved.
Agent successfully stopped...   Done.
Securing agent...   Started.
Enter Agent Registration Password :
Agent successfully restarted...   Done.
Securing agent...   Successful.
```

VERIFY STATUS OF MANAGEMENT SERVICE

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

```
emctl status oms -details
Enter Enterprise Manager Root (SYSMAN) Password :
Oracle Enterprise Manager Cloud Control 13c Release 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 a an interval of 60 seconds.
  - An additional TCP Half-Open health check with a shorter interval of5 seconds.
  - For demonstration purposes, this white paper includes an example monitor named **mon_cc_halfopen**

FROM F5 DEV CENTRAL

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

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.

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