Configuring Maximum Availability Architecture for Oracle Enterprise Manager with F5 BIG-IP Local Traffic Manager

Oracle Maximum Availability Architecture White Paper February 2010

Maximum Availability Architecture

Oracle Best Practices For High Availability



Executive Overview	2
About F5 BIG-IP and Oracle Enterprise Manager Grid Control	3
Configuring an F5 BIG-IP LTM for Grid Control Services	4
Prerequisites and Best Practice Recommendations	4
Configure BIG-IP for Secure Upload (Port 1159)	7
Configure BIG-IP for Agent Registration (Port 4889)	14
Configure BIG-IP for Secure Console (Port 4444)	22
Configure BIG-IP for Unsecure Console (Port 7777)	30
Configure BIG-IP for WebCache Secure (Port 4443)	39
Configure BIG-IP for WebCache Unsecure (Port 7779)	47
Configuring Enterprise Manager for Use with F5 BIG-IP LTM	55
Oracle Enterprise Manager Architecture Overview	55
Configuring Shared Loader Directory	56
Configuring OHS	57
Configure SSL UI (10.2.0.5 and later versions)	60
Appendix A: F5 BIG-IP Local Traffic Manager Terms	61
Appendix B: Summary and Examples	63
F5 Configuration Summary	63
References	68
Oracle	68
F5	68

Executive Overview

Oracle Maximum Availability Architecture (MAA) [1] is the Oracle best practices blueprint for implementing Oracle high-availability technologies. Oracle Enterprise Manager is the management platform for Oracle solutions. This white paper has been jointly written by Oracle Corporation and F5 Networks and provides the detailed steps for implementation of an Oracle MAA solution for Oracle Enterprise Manager Grid Control using BIG-IP from F5 Networks as the front end for the Grid Control mid-tiers, known as the Oracle Managements Service (OMS).

The BIG-IP hardware platform can provide load balancing, high availability, service monitoring, TCP/IP enhancements, and application persistence for the Grid Control environment as the front end for several Grid Control services, including Secure Upload, Agent Registration, Secure Console, Unsecure Console and if required, WebCache Secure, and WebCache Unsecure.

Most of the procedures in this document are performed on the BIG-IP Local Traffic Manager (LTM), targeting different areas of the infrastructure where high availability is required to provide continuous access to the Grid Control OMS application that has been deemed mission critical.

This paper is designed to provide the Grid Control Administrator with an introduction 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 Grid Control architecture.

In general, assume that the following software versions are used in this white paper:

- BIG-IP Version 10.0.1, Build 283
- Grid Control Release 10.2

Any distinction in release numbers is noted within the relevant discussions of this paper.

Note: This white paper assumes that you are familiar with BIG-IP from F5 Networks. See <u>Appendix A</u> for a quick terminology reference. For detailed information, see the <u>BIG-</u> <u>IP Solutions Guide</u> and <u>BIG-IP Configuration Guide</u>, and Chapter 17 in the <u>Oracle</u> <u>Enterprise Manager Installation and Configuration Guide</u>.

About F5 BIG-IP and Oracle Enterprise Manager Grid Control

Figure 1 shows F5 and Oracle Enterprise Manager Elements in a Grid Control environment.





Each Grid Control service that is managed by F5 BIG-IP requires that you configure the following F5 BIG-IP Local Traffic Manager objects:

• A <u>health monitor</u> for the service.

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

• A <u>TCP profile</u> for the service.

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

• A <u>Pool</u> for the service.

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

• A <u>Persistence profile</u> for the service.

The Persistence profile is used to link an OMS agent to the proper Grid Control pool member for the duration of a connection. This is required for all Grid Control services except Secure Upload (See Table 1).

• A <u>Virtual Server</u> for the service.

A Virtual Server is a unique IP address and port that represents a pool of servers.

The remainder of this paper provides detailed instructions for configuring Grid Control services. Each of the configuration discussions imparts:

- Operational best practices when using the F5 BIG-IP Web configuration utility to configure Oracle Enterprise Manager Grid Control services.
- Screen shots of the BIG-IP Web interface that are based on BIG-IP Version 10.0.1 software. You can also use Version 9.*n* BIG-IP software because the configuration steps are identical.
- A Configuration Summary page naming all of the Grid Control services and matching F5 configuration elements.

For additional information about configuring BIG-IP Version 10.*n* and Version 9.*n*, see the BIG-IP documentation at <u>http://www.f5.com</u>.

Configuring an F5 BIG-IP LTM for Grid Control Services

Use the instructions that follow to configure Oracle Enterprise Manager to work with the F5 BIG-IP LTM. These procedures are provided for your convenience. For more detailed information and instructions, see the Oracle and F5 documentation resources that are listed in the <u>References</u> section at the end of this white paper.

4

Prerequisites and Best Practice Recommendations

Use the following general guidelines when building your configuration.

Use BIG-IP Administrative Partitions

A feature of the BIG-IP software is the ability to use *Administrative Partitions* to 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 for access and use by the Grid Control administrators. All the necessary F5 configuration elements for the MAA Grid Control environment are located in the Administrative Partition. Additions, deletions, and changes to these pools created in this partition would not interfere with any other services provided by the BIG-IP. For more information about <u>Configuring Administrative Partitions</u>, see the <u>BIG-IP documentation</u>.

Use the Configuration Table and Standard Naming Conventions

To make the configuration consistent, easy to read, and easy to administer, this white paper uses a standard naming convention for the F5 configuration. Your organization may already use naming standards (which your Network Operations team can provide if necessary), or you can create naming conventions or adopt the ones used in this white paper.

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

SERVICE	PREFIX
Health monitors	mon_
TCP Profiles	tcp_
Pools	pool_
Cookie persistence profile	cookie_
Source IP Address persistence profile	sourceip_
Virtual server	VS_
Grid control services	gc_

Using the "Grid Control Secure Console" as an example, we derived the prefix "gcsc" and terminated each name with the TCP port number as a suffix. In the following list of names, the TCP port number 4444 is used for the servers, and 443 is used for the virtual server:

- mon_gcsc4444
- tcp_gcsc4444
- sourceip_gcsc4444

• pool_gcsc4444

• vs_gcsc443

Pool port numbers are referenced by the Grid Control servers. Virtual Server port numbers are referenced by the Grid Control clients.

These values are shown in Table 1, which provides a reference for all of the F5 configuration objects in this document. All of the names used in this white paper follow this convention, which is considered to be a best practice.

TABLE 1: F5 CONFIGURATION SUMMARY FOR GRID CONTROL SERVICES

GRID CONTROL SERVICE	TCP PORT	F5 MONITOR NAME	F5 TCP PROFILE NAME	F5 PERSIST PROFILE	F5 POOL NAME	F5 VIRTUAL SERVER NAME	F5 VIRTUAL SERVER PORT
Secure Upload	1159	mon_gcsu1159	tcp_gcsu1159	None	pool_gcsu1159	vs_gcsu1159	1159
Agent Registration	4889	mon_gcar4889	tcp_gcar4889	cookie_gcar4889	pool_gcar4889	vs_gcar4889	4889
Secure Console	4444	mon_gcsc4444	tcp_gcsc4444	sourceip_gcsc4444	pool_gcsc4444	vs_gcsc4444	443
Unsecure Console ¹	7777	mon_ gcuc7777	tcp_ gcuc7777	sourceip_ gcuc7777	pool_gcuc7777	vs_ gcuc7777	7777
WebCache ²	4443	mon_gcws4443	tcp_gcws4443	sourceip_gcws4443	pool_gcws4443	vs_gcws4443	4443
WebCache Unsecure	7779	mon_gcwu7779	tcp_gcwu7779	sourceip_gcwu7779	pool_gcwu7779	vs_gcwu7779	7779

Tip: Print Table 1 for easy reference during the configuration process.

6

¹ For information about configuring this pool, see the 'Create the Grid Control Unsecure Console Redirect iRule' topic in the F5 iRules at the F5 DevCentral Web site: <u>http://devcentral.f5.com/Default.aspx?tabid=75</u>.

² Configuration of the WebCache component is required only when WebCache is used. WebCache is optional unless it is specifically required by an Oracle Enterprise Manager Pack or feature.

Configure BIG-IP for Secure Upload (Port 1159)

Use the following step-by-step procedure as a template for configuring F5 BIG-IP to support the Secure Upload Service for the OMS system.

Step 1: Configure a health monitor for the Secure Upload service

On the Main tab, expand Local Traffic, and then click Monitors.

1. On the **Monitors** screen, click **Create**.

The New Monitor screen opens.

- 2. In the Name field, enter a unique name for the Monitor. For example: mon_gcsu1159
- 3. From the **Type** list, select **HTTPS**.

The Monitor configuration options display.

- 4. From the Configuration list, select Advanced.
- 5. In the Configuration section, enter values in Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 60 and Timeout to 181.

6. In the Send String field, add a Send String, as follows:

GET /em/upload HTTP/1.0

7. In the **Receive String** field, add a Receive String, as follows:

Http Receiver Servlet active!

- 8. In the Alias Service Port field, enter **1159**. All other configuration settings are optional.
- 9. Click Finished.

Main	Help About	Local Traffic » Monitors	s >> New Monitor	
	Overview Access statistics, performance	General Properties		
	graphs, and links to helpful tools.	Name	mon_gcsu1159	
a	Templates and Wizards	Туре	HTTPS 🔽	
	Templates	Import Settings	https	
	Device Wizards	Configuration: Advanced	·	
0	Global Traffic	Interval	60 seconds	
D	Control the delivery of application traffic for a wide area network.	Timeout	181 seconds	
2	Local Traffic	Manual Resume	◯ Yes ⊙ No	
	Network Map	Check Until Up	🔿 Yes 💿 No	
	Virtual Servers		GET /em/upload HTTP/1.0	
	Profiles	Send String		
	iRules			
	Pools		Http Receiver Servlet active!	
	Nodes	Receive String		
	Monitors			
	Rate Shaping			
		Alias Address	* All Addresses	
		Alias Service Port	1159 Other: 💌	

Step 2: Create a new TCP profile for the Secure Upload service

In the following example, the TCP profile is based on the default TCP profile, and keeps all of the options at the default settings. You can configure these options, as appropriate, for your network.

8

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

The HTTP Profiles screen opens.

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

5. In the Name field, enter a unique name for this profile. For example: tcp_gcsu1159.

If needed, modify the name, as applicable, for your network. See the F5 online help for more information about the configuration options. In the MAA example the settings remain at the default levels.

6. Click Finished.

Hostnar IP Addre	me: Biglp6800.oracle.com Da ess: 192.168.1.245 Ti	ate: Jun 9, me: 5:00 P	2009 User:admi VI(PDT) Role:Admi	n nistrator			
Main	Unit 1 State: ACTIVE	In	cal Traffic ა, Profiles	• Protocol • TCP აა	New TCP Profile		
	Overview Access statistics, performance	Ger	eral Properties				
	graphs, and links to helpful tools.	N	ame	tcp_gcsu1	1159		
Ê	Templates and Wizards	Pa	arent Profile	tcp	~		
	Templates	Set	Settings				
	Device Wizards	R	eset On Timeout	🗹 Enab	led		
0	Global Traffic	Ti	me Wait Recycle	🗹 Enab	iled		
0	Control the delivery of application traffic for a wide area network.	D	elayed Acks	🗹 Enab	led		
0-0	Local Traffic	Pr	oxy M <mark>ax</mark> imum Segmen	t 🗆			
	Network Map	Pr	oxy Options				
	Virtual Servers) Pr	oxy Buffer Low	4096	bytes		
	Profiles	Pr	oxy Buffer High	16384	bytes		

Step 3: Create the Secure Upload pool

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing methodology. In this configuration example, one pool is created for the Grid Control Secure Upload devices:

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

The Pool screen opens. In the upper right portion of the screen, click Create.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, select **Advanced** from the Configuration list. Configure these settings as applicable for your network.

- 2. In the **Name** field, enter a unique name for your pool. In the MAA example, we entered **pool_gcsu1159**.
- In the Health Monitors section, select the name of the monitor you created in the "Configure the Secure Upload health monitor step", and click Add (<<). In the MAA example, we select mon_gcsu1159.
- From the Load Balancing Method list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In the MAA example, we select Least Connections (member).
- 5. For this pool, keep the Priority Group Activation at **Disabled**.
- 6. In the New Members section, make sure the New Address option is selected.
- In the Address field, add the first server to the pool. The MAA example uses 10.10.10.151.
- In the Service Port field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list. The MAA example uses 1159.
- 9. Click Add to add the member to the list.
- 10. Repeat steps 8 through 10 for each server that you want to add to the pool.
- 11. In the MAA example, we repeated these steps three times for the remaining servers: 10.10.10.152, 10.10.10.153, and 10.10.10.154.
- 12. Click Finished.

Hostnam IP Addre	ne: Biglp6800.oracle.com ess: 192.168.1.245	Date: . Time:	Jun 9, 2009 5:37 PM (PDT)	User: admin Role: Administrato			
Main	Unit 1 State: ACTIVE Help Abou	ıt	Local Traffi	c » Pools » New	Pool		
	Overview Access statistics, performa	nce	Configuration	n: Basic 💌			
	graphs, and links to helpful t	ools.	Name		pool_gcsu	1159	
Ê	Templates and Wizards Templates Device Wizards		Health Mon	itors	Ac mon_gcs	tive u1159 << >>	Available mon_gcar4889 ^ mon_gcsc4444 mon_gcwu7779 v
\bigcirc	Global Traffic Control the delivery of applic traffic for a wide area netw	ation ork.	Resources	cing Method	Least Conne	ctions (member)	~
~	Local Traffic		Priority Grou	up Activation	Disabled	~	
	Network Map					New Address	O Node List
	Virtual Servers	×.			Address:	10.10.10.154	
	Profiles	E.			Service Port	t 1159 Sele	ct 💌
	iRules	×.	New Memb	ers	Add	0 10 151 -1150	
	Pools	÷.			R:1 P:1 10.1 B:1 P:1 10.1 B:1 P:1 10.1	0.10.152 :1159	
	Nodes	÷.			R:1 P:1 10.1	0.10.154 :1159	
	Monitors	÷			Edit	Delete	1
	Rate Shaping	F	(Canaal) (R	anost Disished			
	Traffic Class	E.					

Step 4: Create the virtual server

Perform the following steps to configure a Secure Upload virtual server that references the monitor, profiles, and pool you created in the preceding steps:

- On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.
- In the upper right portion of the screen, click Create. The New Virtual Server screen opens.
- In the Name field, enter a unique name for this virtual server. In the MAA example, we entered vs_gcsu1159.
- 4. In the **Destination** section, select the **Host** option.
- 5. In the Address field, enter the IP address of this virtual server.

In the MAA example, we used **10.10.101**.

- 6. In the Service Port field, enter 1159.
- From the Configuration list, select Advanced. The Advanced configuration options display.
- 8. Keep the **Type** list at the default setting: **Standard**.
- From the Protocol Profile (Client) list, select the name of the profile you created in the "<u>Create a TCP profile for Secure Upload</u>" section. In the MAA example, we selected tcp_gcsu1159.
- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the SNAT Pool setting to Automap.
- 12. In the Resources section, from the **Default Pool** list, select the pool you created in the "<u>Create the pool for Secure Upload</u>" section.

In the MAA example, we selected **pool_gcsu1159**.

Name	vs_gcsu1159
Destination	Type: Host Network Address: 10.10.101
Service Port	1159 Other: 💌
State	Enabled 💌
onfiguration: Advanced 💌	
Гуре	Standard 🗸
Protocol	TCP V
Protocol Profile (Client)	tcp_gcsu1159
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	Nonel V
HTTP Profile	None
TP Profile	None 💽
SSL Profile (Client)	None
SSL Profile (Server)	None
SNAT Pool	Auto Map 🗸
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None 🛩 Context: server 💌
lesources	
iRules	Enabled Available Sys_auth_ktbdelegate sys_auth_ssl_cc_idap Up Down
HTTP Class Profiles	Enabled Available
Default Pool	pool_gcsu1159
Default Persistence Profile	None
Fallback Persistence Profile	None

Configure BIG-IP for Agent Registration (Port 4889)

Use the following procedure as a template for configuring F5 to support the Agent Registration Service for the OMS system. This procedure uses entries from the Monitor Port (Monitor Type) column in Table 1.

Step 1: Configure a health monitor for the Agent Registration service

- On the Main tab, expand Local Traffic, and then click Monitors. The Monitors screen opens.
- On the Monitors screen, click Create.
 The New Monitor screen opens.
- 3. In the Name field, enter a unique name for this Monitor. For example: mon_gcar4889.
- From the Type list, select the monitor type found in the Monitor Port (Monitor Type) column in parenthesis. Select HTTP. The Monitor configuration options display.
- 5. From the **Configuration** list, select **Advanced**.
- 6. In the Configuration section, enter values in the Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 60 and Timeout to 181.

7. In the Send String field, add a Send String, as follows:

GET /em/genwallet HTTP/1.0

8. In the Receive String field, add a Receive String, as follows:

GenWallet Servlet activated

- In the Alias Service Port field, enter 4889.
 All other configuration settings are optional.
- 10. Click Finished.

Overview Access statistics, p	erformance	General Properties		
graphs, and links to	helpful tools.	Name	mon_gcar4889	
Templates and V	lizards	Туре	HTTP	
Templates		Import Settings	http 😪	
Device Wizard	5	Configuration: Advanced		
Global Traffic		Interval	60 seconds	
Control the delivery traffic for a wide an	of application ea network.	Timeout	181 seconds	
Local Traffic		Manual Resume	🔿 Yes 💿 No	
Network Map		Check Until Up	O Yes 💿 No	
Virtual Servers	F.		GET /em/genwallet HTTP/1.0	
Profiles	Þ	Send String		
iRules	E			
Pools	R	-	GenWallet Servlet activated	
Nodes	E:	Receive String		
Monitors	Þ.	-		
Rate Shaping	E.	Liner Nome		
Traffic Class	÷.	User Marrie	1	
SNATs	E:	Password		
SSL Certificate	is 🕨 🕨	Reverse	O Yes 💿 No	
Manual		Transparent	🔿 Yes 💿 No	
	elements for	Alias Address	* All Addresses	

Step 2: Create the TCP profile for the Agent Registration service

In our MAA example, we base the TCP profile on the default TCP profile, and keep all the options at their default settings. You can configure these options, as appropriate, for your network.

To create a new TCP profile for the Agent Registration service:

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

The HTTP Profiles screen opens.

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

The New TCP Profile screen opens.

- 5. In the **Name** field, enter a unique name for this profile. For example: tcp_gcar4889.
- 6. If needed, modify as applicable for your network. See the F5 online help for more information about the configuration options. Note that the MAA example keeps the settings at their default levels.
- 7. Click Finished.



Step 3: Create a cookie persistence profile

When creating a Cookie Persistence profile, the best practice recommendation is to use the default cookie method for this profile (**HTTP cookie insert**).

To create a new cookie persistence profile based on the default profile:

- On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
- On the Menu bar, click Persistence.
 The Persistence Profiles screen opens.
- In the upper right portion of the screen, click Create. The New Persistence Profile screen opens.
- In the Name field, enter a name for this profile.
 In the MAA example, we entered cookie_gcar4889.
- From the Persistence Type list, select Cookie.
 The configuration options for cookie persistence display.
- 6. Modify the cookie timeout value to **3600**.
- 7. Click Finished.

Name	cookie_	gcar4889		
Persistence Type	Cookie			
Parent Profile	cookie	*		
onfiguration				
Cookie Method	HTTP Co	okie Insert	~	
Cookie Name				
	Days	Hours	Minutes	Seconds
Expiration	0	0	0	3600
	Ses	sion Cookie		
Quarrida Connection Limit	1000			

For more information about creating or modifying profiles or applying profiles in general, see the BIG-IP documentation listed in the <u>References</u> section.

Step 4: Create the pool for the Agent Registration

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In the MAA configuration, we created one pool for the Grid Control Agent Registration devices.

To create the Agent Registration pool:

1. On the Main tab, expand Local Traffic, and then click Pools.

The Pool screen opens.

2. In the upper right portion of the screen, click Create.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings, as applicable, for your network.

3. In the Name field, enter a unique name for your pool.

In the MAA example, we entered **pool_gcar4889**.

 In the Health Monitors section, select the name of the monitor you created in the <u>"Creating the Agent Registration health monitor step</u>", and click the Add (<<) button. In the MAA example, we selected mon_gcar4889.

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

In the MAA example, we selected **Least Connections (member)**.

- 6. For this pool, keep the Priority Group Activation at Disabled.
- 7. In the New Members section, make sure the New Address option button is selected.
- 8. In the **Address** field, add the first server to the pool.

In the MAA example, we entered **10.10.10.15**.

9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

In the MAA example, we entered 4889.

- 10. Click **Add** to add the member to the list.
- 11. Repeat steps 8 through 10 for each server you want to add to the pool.

In the MAA example, we repeated these steps three times for the remaining servers, 10.10.10.152, **10.10.10.153**, and **10.10.10.154**.

Hostnam IP Addre	e: Biglp6800.oracle.com ss: 192.168.1.245	Date: J Time: 5	lun 9, 2009 5:41 PM (PDT)	User: admin Role: Administrato		
6	Unit 1					
Main	Help Abou	ıt	Local Traffic	: » Pools » New	Pool	
	Overview Access statistics, performar	ice	Configuration	: Basic 💌		
	graphs, and links to helpful to	ools.	Name		pool_gcar4889	
Ê	Templates and Wizards				Active mon_gcar4889	Available
	Device Wizards		Health Moni	tors		→ mon_gcsc4444 mon_gcws4443 mon_gcwu7779 tcp
•	Global Traffic Control the delivery of applic	ation	Resources			
	traffic for a wide area netwo	ork.	Load Baland	cing Method	Least Connections (membe	er) 💌
	Local Traffic		Priority Grou	p Activation	Disabled 💉	
	Network Map				New A	ddress 🔘 Node List
	Virtual Servers	- F			Address: 10.10.10.1	54
	Profiles	3E			Service Port: 4889	Select
	iRules		New Membe	ers	Add	
	Pools				R:1 P:1 10.10.10.151 488 R:1 P:1 10.10.10.152 488 P:1 P:1 10.10.10.152 488	9
	Nodes				R:1 P:1 10.10.10.154 :488	19
	Monitors	19			Edit Delete	
	Rate Shaping					
	Traffic Class	() ()		epeat Finished		

Step 5: Create the Agent Registration virtual server

To configure an Agent Registration virtual server that references the monitor, profiles, persistence, and pool you created in the preceding procedures, perform the following steps:

1. On the Main tab, expand Local Traffic, and then click Virtual Servers.

The Virtual Servers screen opens.

- In the upper right portion of the screen, click Create. The New Virtual Server screen opens.
- 3. In the **Name** field, enter a unique name for this virtual server.

In the MAA example, we entered vs_gcar4889.

- 4. In the **Destination** section, select the **Host** option.
- In the Address field, enter the IP address of this virtual server. In the MAA example, we used 10.10.101.
- 6. In the Service Port field, enter 4889.

- From the Configuration list, select Advanced.
 The Advanced configuration options display.
- 8. Keep the **Type** list at the default setting: **Standard**.
- 9. From the **Protocol Profile (Client)** list select the name of the profile you created in the *Creating a TCP profile* section.

In the MAA example, we selected tcp_gcar4889.

- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the HTTP Profile to **HTTP**.
- 12. Change the SNAT Pool setting to Automap.
- 13. In the Resources section, from the **Default Pool** list, select the pool you created in the "<u>Creating the pool for the Agent Registration</u>" step.

In the MAA example, we selected pool_gcar4889.

14. From the **Default Persistence Profile** list, select the persistence profile you created in the "<u>Creating a cookie persistence profile for the Agent Registration</u>" step.

In the MAA example, we selected cookie_gcar4889.

Name	vs_gcar4889			
Destination	Type: 💿 Host 🔿 Netw	vork		
beamaion	Address: 10.10.10.101			
Service Port	4889 Other:	•		
State	Enabled 💌			
onfiguration: Advanced 💉				
Туре	Standard			
Protocol	TCP			
Protocol Profile (Client)	tcp_gcar4889			
Protocol Profile (Server)	(Use Client Profile)			
OneConnect Profile	None			
NTLM Conn Pool	None V			
HTTP Profile	http	~		
FTP Profile	None ~			
SSL Profile (Client)	None			
SSL Profile (Server)	None			
SNAT Pool	Auto Map 💌			
Clone Pool (Client)	None			
Clone Pool (Server)	None			
Last Hop Pool	None			
iSession Profile	None 💟 Context: server 💌	•		
esources				
	Enabled	Available		
(Dulas		_sys_auth_krbdelegate _sys_auth_ssl_cc_ldap		
IKUIES	>>>			
	Up Down	•		
	Enabled	Available		
	<	httpclass		
HTTP Class Profiles	>>			
	Up Down	1		
Default Pool +	pool_gcar4889 💌			
Default Persistence Profile	cookie_gcar4889 💌			
Fallback Persistence Profile	None			

Configure BIG-IP for Secure Console (Port 4444)

Use the step-by-step procedure in this section as a template for configuring the F5 BIG-IP to support the Secure Console Service for the OMS system.

Step 1: Configure a health monitor for the Secure Console service

- On the Main tab, expand Local Traffic, and then click Monitors. The Monitors screen opens.
- Click Create. The New Monitor screen opens.
- 3. In the **Name** field, enter a unique name for this Monitor. For example, enter **mon_gcsc4444**.
- 4. From the **Type** list, select **HTTPS**.

The Monitor configuration options display.

- 5. From the **Configuration** list, select **Advanced**.
- 6. In the Configuration section, enter values in Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 60 and Timeout to 181.

7. In the **Send String** field, add a Send String as follows:

GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)

8. In the **Receive String** field, add a Receive String as follows:

/em/console/logon/logon;jsessionid=

9. In the Alias Service Port field, enter 4444.

All other configuration settings are optional.

😭 🏟	GBIG-IP® - BigIp6800.oracle.com	(192.168.1.24	5)					
Main	Help About	Local Tra	affic » Monitors » t	New Monitor				
	Overview Access statistics performance	General P	roperties					
100 Marcal	graphs, and links to helpful tools.			mon_gcsc4444				
(÷	Templates and Wizards Templates			HTTPS 💌				
			ettings	https 🔽				
	Device Wizards	Configuration: Advanced						
-	Global Traffic	Interval 30 seconds						
0	Control the delivery of application traffic for a wide area network.			91 s	91 seconds			
00	Local Traffic		Resume	O Yes 💿 No				
	Network Map	Check Until Up Send String		O Yes 💿 N	○ Yes ⊙ No			
	Virtual Servers			GET /em/cons	GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0			
	Profiles			3 ¹⁵ 70				
	iRules							
	Pools	<u>21</u>		/em/console/logon/logon;jsessionid=				
	Nodes	Receive	String					
	Monitors	1 COOMO	oung					
	Rate Shaping	Olahari.						
	Traffic Class	Cipner L	IST	UEFAULT:+SH	SHA:+3DES:-kEDH			
84	System		Reverse		○ Yes ④ No			
	Configure system access, availability, reporting, and n	high nore.	nigh Iore. Transparent		◯ Yes ④ No			
			Alias Address	s	* All Addresses			
			Alias Service	Port	4444 Other: 💌			
			Cancel Rep	peat Finished]			

Step 2: Create the TCP profile for the Secure Console service

In the following example, the TCP profile is based on the default TCP profile, and keeps all of the options at the default settings. You can configure these options, as appropriate, for your network.

To create a new TCP profile for the Secure Console service:

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

The HTTP Profiles screen opens.

3. On the Menu bar, from the **Protocol** menu, select **TCP**.

4. In the upper right portion of the screen, click **Create**.

The New TCP Profile screen opens.

- 5. In the Name field, enter a unique name for this profile. For example: tcp_gcsc4444.
- 6. If needed, modify any of the settings as applicable for your network. See the F5 online help for more information on the configuration options. In the MAA example, we kept the settings at the default levels.
- 7. Click Finished.

Hostna IP Addr	me: Biglp6800.oracle.com Date ess: 192.168.1.245 Time	Jun 9, 2009 User: admin 5:05 PM (PDT) Role: Administra	itor		
ſ	Unit 1 State: ACTIVE				
Main	Help About	Local Traffic » Profiles : Pro	otocol : TCP » New TCP Profile		
	Overview Access statistics, performance	General Properties			
	graphs, and links to helpful tools.	Name	tcp_gcsc4444		
Ê	Templates and Wizards	Parent Profile	tcp 💌		
	Templates	Settings			
	Device Wizards	Reset On Timeout	Enabled		
0	Global Traffic	Time Wait Recycle	🗹 Enabled		
0	Control the delivery of application traffic for a wide area network.	Delayed Acks	Enabled		
	Local Traffic	Proxy Maximum Segment			
	Network Map	Proxy Options			
	Virtual Servers	Proxy Buffer Low	4096 bytes		
	Profiles >	Proxy Buffer High	bytes		
	iRules	Idle Timeout	Spector V 300		

Step 3: Create a ClientIP persistence profile for the Secure Console service

When creating the ClientIP Persistence profile, the best practice is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default profile:

1. On the Main tab, expand Local Traffic, and then click Profiles.

The HTTP Profiles screen opens.

2. On the Menu bar, click **Persistence**.

The Persistence Profiles screen opens.

- 3. In the upper right portion of the screen, click Create.
- 4. The New Persistence Profile screen opens.

- 5. In the Name field, enter a unique name for this profile. For example, enter **sourceip_gcsc4444**.
- From the Persistence Type list, select Source Address Affinity. The configuration options for SourceIP persistence display.
- 7. Modify the persistence timeout value to **3600**.
- 8. Click Finished.

Namo		_		
Name	j sourceip_gcsc4444			
Persistence Type	Source Address Affinity			
Parent Profile	source_addr 💌			
onfiguration				
Mirror Persistence				
Match Across Services				
Match Across Virtual Servers				
Match Across Pools				
Timeout	Specify 😒 3600 secon	nd		
Mask	None			
Map Proxies	Enabled			
Override Connection Limit				

For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation, which is listed in the <u>References</u> section.

Step 4: Create the pool for the Secure Console service

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control Secure Console devices.

To create the Secure Console pool

1. On the Main tab, expand Local Traffic, and then click Pools.

The Pool screen opens.

2. In the upper right portion of the screen, click Create.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings, as applicable, for your network.

3. In the **Name** field, enter a unique name for your pool.

In the MAA example, we entered pool_gcsc4444.

4. In the **Health Monitors** section, select the name of the monitor you created in the "<u>Creating the Secure Console health monitor</u>" step, and click **Add (<<)**.

In the MAA example, we selected mon_gcsc4444.

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

In the MAA example, we selected Least Connections (member).

- 6. For this pool, we kept the Priority Group Activation Disabled.
- 7. In the New Members section, make sure the New Address option button is selected.
- In the Address field, add the first server to the pool.
 In the MAA example, we entered 10.10.10.151
- 9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

In the MAA example, we entered 4444.

- 10. Click Add to add the member to the list.
- 11. Repeat steps 8 through 10 for each server that you want to add to the pool.

In the MAA example, we repeated these steps three times for the remaining servers, **10.10.10.152, 10.10.10.153, and 10.10.10.154**.

Hostnar IP Addre	me: Biglp6800.oracle.com E ess: 192.168.1.245 T)ate: Jun 9, 2009 Time: 5:45 PM (PDT)	User. admin Role: Administri	ator	
ß	Unit 1 State: ACTIVE				
Main	Help About	Local Traffi	c » Pools » Ne	w Pool	
	Overview	Configuratio	n: Basic 💌		
	graphs, and links to helpful tools.	Name		pool_gcsc4444	
Ê	Templates and Wizards			Active mon_gcsc4444	Available
_	Device Wizards	Health Mon	itors	×	inband mon_gcsu1159 I mon_gcws4443 mon_gcwu7779 V
S	Global Traffic Control the delivery of application	Resources			
	traffic for a wide area network.	Load Balar	icing Method	Least Connections (member)	~
0-0	Local Traffic	Priority Gro	up Activation	Disabled	
	Network Map			New Addres	s 🔿 Node List
	Virtual Servers	×		Address: 10.10.10.154	
	Profiles	8		Service Port. 4444 Sel	ect 💌
	iRules	New Memb	ers	Add	
	Pools	ъ		R:1 P:1 10.10.10.151:4444 R:1 P:1 10.10.10.152:4444 D:1 D:1 10.10.10.152:4444	
	Nodes	×		R:1 P:1 10.10.10.153 :4444 R:1 P:1 10.10.10.154 :4444	
	Monitors	- E		Edit Delete	
	Rate Shaping				
	Traffic Class	Cancel	Cancel Repeat Finished		

Step 5: Create the Secure Console virtual server

This step configures a Secure Console virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

To create the virtual server

- On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.
- In the upper right portion of the screen, click the Create button. The New Virtual Server screen opens.
- 3. In the **Name** field, enter a unique name for this virtual server. In the MAA example, we entered **vs_gcsc4444**.
- 4. In the **Destination** section, select the **Host** option button.

5. In the Address field, enter the IP address of this virtual server.

In the MAA example, we used **10.10.101**.

6. In the Service Port field, enter 443.

Note: The virtual server is listening on port 443, but the Secure Console service is running on port 4444 on the OMS servers. You may need to change this virtual server port number, depending on the installation.

7. From the Configuration list, select Advanced.

The Advanced configuration options display.

- 8. Keep the **Type** list at the default setting: **Standard**.
- From the Protocol Profile (Client) list select the name of the profile you created in the "Creating a TCP profile" step.

In the MAA example, we selected tcp_gcsc4444.

- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the SNAT Pool setting to Automap.
- 12. In the Resources section, from the **Default Pool** list, select the pool you created in the "<u>Creating the pool</u>" step.

In the MAA example, we selected pool_gcsc4444.

 From the Default Persistence Profile list, select the persistence profile you created in the "Creating a ClientIP persistence profile" step.

In the MAA example, we selected sourceip_gcsc4444.

Name	vs_gcsc4444
Destination	Type: Host Network Address: 10.10.101
Service Port	443 HTTPS
State	Enabled 💌
onfiguration: Advanced 💌	
Гуре	Standard
Protocol	TCP 💌
Protocol Profile (Client)	tcp_gcsc4444
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None v
HTTP Profile	None
FTP Profile	None 💌
SSL Profile (Client)	None
SSL Profile (Server)	None
SNAT Pool	Auto Map 💌
Clone Pool (Client)	None
Clone Pool (Server)	None
Last Hop Pool	None
iSession Profile	None Context: server V
lesources	
iRules	Enabled Available CC Sys_auth_krbdelegate Sys_auth_ssl_cc_ldap Up Down
HTTP Class Profiles	Enabled Available
Default Pool +	pool_gcsc4444 💌
Default Persistence Profile	sourceip_gcsc4444 💌
Fallback Persistence Profile	None

Configure BIG-IP for Unsecure Console (Port 7777)

Use the step-by-step procedure in this section as a template for configuring the F5 BIG-IP to support the Unsecure Console Service for the OMS system.

Note: The procedure to configure the Unsecure Console pool is for informational purposes only. The best practice is to route all traffic to and from Oracle Enterprise Manager in a secure fashion. Instead of configuring the Unsecure Console, Oracle recommends configuring the iRule (as described in the "Create Grid Control Unsecure Console Redirect <u>iRule"</u> step) to redirect all traffic to the secure port that was inadvertently sent to the unsecure pool.

Step 1: Create the Unsecure Console health monitor

The following procedure uses entries from the **Monitor Port (Monitor Type)** column shown in Table 1.

To configure a health monitor for the Unsecure Console service:

- On the Main tab, expand Local Traffic, and then click Monitors. The Monitors screen opens.
- 2. Click Create.

The New Monitor screen opens.

- 3. In the **Name** field, enter a unique name for this Monitor. For example: mon_gcuc7777.
- 4. From the **Type** list, select **HTTP**.

The Monitor configuration options display.

- 5. From the Configuration list, select Advanced.
- 6. In the Configuration section, enter values in the Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 30 and Timeout to 91.

7. In the **Send String** field, add a Send String, as follows:

GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0) 8. In the Receive String field, add a Receive String, as follows:

/em/console/logon/logon;jsessionid=

9. In the Alias Service Port field, enter 7777.

All other configuration settings are optional.

10. Click Finished.

	Overview Access statistics, performance	General Properties				
	graphs, and links to helpful tools.	Name	mon_gcuc7777			
Ê	Templates and Wizards	Туре	HTTP			
	Templates	Import Settings	http 👻			
	Device Wizards	Configuration: Advanced				
0	Global Traffic	Interval	30 seconds			
0	Control the delivery of application traffic for a wide area network.	Timeout	91 seconds			
0-0	Local Traffic	Manual Resume	○ Yes ④ No			
	Network Map	Check Until Up Send String	O Yes 💿 No			
	Virtual Servers		GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)			
	Profiles +					
	iRules					
	Pools +	Receive String	/em/console/logon/logon;jsessionid=			
	Nodes					
	Monitors +					
	Rate Shaping	LassName				
	Traffic Class	User Name				
	SNATs -	Password				
	SSL Certificates	Reverse	○ Yes ④ No			
		Transparent	🔿 Yes 💿 No			
	Network Configure network elements for	Alias Address	* All Addresses			
	routing and switching.	Alias Service Port	7777 Other: 💌			
8 ¢	System Configure system access, high	Cancel Repeat Finish	ned			

Step 2: Create a new TCP profile for the Unsecure Console service

In the MAA example, the TCP profile is based on the default TCP profile, and keeps all of the options set to their default values. You can configure these options, as appropriate, for your network.

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

The HTTP Profiles screen opens.

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

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. For example: tcp_gcuc7777.

If needed, modify the name appropriately for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at their default levels.

6. Click Finished.

Hostnar IP Addr	ne: Biglp6800.oracle.com Date: ess: 192.168.1.245 Time:	Jun 9, 2009 User: admin 5:07 PM (PDT) Role: Administra	
ſ	Unit 1 State: ACTIVE		
Main	Help About	Local Traffic » Profiles : Pro	tocol : TCP » New TCP Profile
Overview		General Properties	
	graphs, and links to helpful tools.	Name	tcp_gcuc7777
हि	Templates and Wizards	Parent Profile	tcp 🖌
	Templates	Settings	
	Device Wizards	Reset On Timeout	Enabled
0	Global Traffic	Time Wait Recycle	Enabled
0	Control the delivery of application traffic for a wide area network.	Delayed Acks	Enabled
~~	Local Traffic	Proxy Maximum Segment	
	Network Map	Proxy Options	
	Virtual Servers	Proxy Buffer Low	d096 bytes
	Profiles	Proxy Buffer High	16384 bytes
	iRules	Idle Timeout	Specific III v 200

Step 3: Create a ClientIP persistence profile for the Unsecure Console

When creating a ClientIP Persistence profile, the best practice is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default profile:

- On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
- 2. On the Menu bar, click **Persistence**.

The Persistence Profiles screen opens.

- In the upper right portion of the screen, click Create. The New Persistence Profile screen opens.
- 4. In the **Name** field, enter a unique name for this profile. In the MAA example, we entered **sourceip_gcuc7777**.
- 5. From the **Persistence Type** list, select **Source Address Affinity**.

The configuration options for persistence display.

- 6. Click **custom** (not shown) to activate the timeout column; Modify the persistence timeout value to **3600**.
- 7. Click Finished.

Name	sourceip_gcuc7777		
Persistence Type	Source Address Affinity		
Parent Profile	source_addr		
onfiguration			
Mirror Persistence			
Match Across Services			
Match Across Virtual Servers			
Match Across Pools			
Timeout	Specify 😪 3600 seconds		
Mask	None 🗸 🗸		
Map Proxies	Enabled		
Override Connection Limit			

For more information about creating or modifying profiles, or applying profiles in general, see the F5 BIG-IP documentation listed in the <u>R eferences</u> section.

Step 4: Create the Grid Control Unsecure Console Redirect iRule

The Redirect iRule takes incoming HTTP requests (non-secure) and redirects them to the correct HTTPS (secure) virtual server, without user interaction. This Redirect iRule will be used on the Grid Control Unsecure Console virtual server, to redirect clients to the matching SSL Secured Console Service.

To create the Redirect iRule:

- On the Main tab, expand Local Traffic, and then click iRules. The iRule screen opens.
- In the upper right portion of the screen, click Create. The New iRule screen opens.
- 3. In the **Name** field, enter a name for your iRule.

In the MAA example, we used gcuc_httptohttps.

4. In the **Definition** section, copy and paste the following iRule:

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host]/
}
```

5. Click Finished.

lame	gcuc_httptohttps
Definition	<pre>when HITP_REQUEST { HITP::redirect https://[HITP::host]/ }</pre>
	Extend Text Area

Step 5: Create the Unsecure Console pool

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control Unsecure Console devices.

To create the Unsecure Console pool:

1. On the Main tab, expand Local Traffic, and then click Pools.

The Pool screen opens.

2. In the upper right portion of the screen, click the Create button.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure the advanced settings appropriately for your network.

3. In the Name field, enter a unique name for your pool.

In the MAA example, we entered **pool_gcuc7777**.

In the Health Monitors section, select the name of the monitor you created in the "Creating the Unsecure Console health monitor" step, and click Add (<<).

In the MAA example, we selected $\mathbf{mon_gcuc7777}.$

 From the Load Balancing Method list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network).

In the MAA example, we selected Least Connections (member).

- 6. For this pool, we kept the Priority Group Activation at Disabled.
- 7. In the New Members section, make sure New Address option is selected.
- In the Address field, add the first server to the pool. In the MAA example, we entered 10.10.10.151.
- 9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

In the MAA example, we entered 7777.

- 10. Click Add to add the member to the list.
- 11. Repeat steps 8 through 10 for each server you want to add to the pool.

In the MAA example, we repeated these steps three times for the remaining servers, **10.10.10.152**, **10.10.10.153**, and **10.10.10154**.

Hostnam IP Addre	ne: Biglp6800.oracle.com ess: 192.168.1.245	Date: Time:	Jun 9, 2009 User: admin 5:51 PM (PDT) Role: Admin	istrator
ß	Unit 1 State: ACTIVE			
Main	Help Abou	it 🖉	Local Traffic » Pools »	New Pool
	Overview Access statistics, performance graphs, and links to helpful tools.		Configuration: Basic	v
			Name	pool_gcuc7777
Ż	Templates and Wizards		2	Active Available
	Templates		Health Monitors	mon_gcuc7777 mon_gcar4889 A
	Device Wizards			mon_gcsu1159 ₪ mon_gcws4443 mon_gcwu7779 ♥
9	Global Traffic		Resources	
0	traffic for a wide area netwo	ation prk.	Load Balancing Method	Least Connections (member)
2-0	Local Traffic		Priority Group Activation	Disabled
	Network Map		1.	New Address O Node List
	Virtual Servers	- 963 -		Address: 10.10.10.154
	Profiles			Service Port: 7777 Select
	iRules	Эk	New Members	Add
	Pools			R:1 P:1 10.10.10.152 :7777 P:1 P:1 10.10.10.152 :7777
	Nodes	96) -		R:1 P:1 10.10.10.154 :7777
	Monitors			Edit Delete
	Rate Shaping	ЭĿ		
	Troffic Close	100	Cancel Repeat Finish	led

Step 6: Create the Unsecure Console virtual server

To configure an Unsecure Console virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

- On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.
- In the upper right portion of the screen, click Create. The New Virtual Server screen opens.
- In the Name field, enter a unique name for this virtual server. In the MAA example, we entered vs_gcuc7777.
- 4. In the **Destination** section, select **Host**.
- In the Address field, enter the IP address of this virtual server. In the MAA example, we used 10.10.101.
- 6. In the Service Port field, enter 7777.

7. From the Configuration list, select **Advanced**.

The Advanced configuration options display.

- 8. Keep the **Type** list at the default setting: **Standard**.
- 9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the "<u>Creating a TCP profile</u>" step. In the MAA example, we selected **tcp_gcuc7777**.
- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the HTTP Profile to http.
- 12. Change the SNAT Pool setting to Automap.
- 13. In the Resources section, in the iRules **Available** list, select the iRule you created in the "<u>Creating the iRule</u>" step, and click << to move it to the **Enabled** list.

In the MAA example, we selected gcuc_httptohttps.

14. In the Resources section, from the **Default Pool** list, select the pool you created in the "<u>Creating the pool</u>" step.

In the MAA example, we selected pool_gcuc7777.

15. From the **Default Persistence Profile** list, select the persistence profile you created in the "<u>Creating a ClientIP persistence profile</u>" step.

In the MAA example, we selected **sourceip_gcuc7777**.

Name	vs_gcuc7777
Destination	Type: Host Network Address: 10.10.101
Service Port	7777 Other: 💉
State	Enabled 💟
onfiguration: Advanced 💌	
Гуре	Standard
Protocol	TCP 👻
Protocol Profile (Client)	tcp_gcuc7777
Protocol Profile (Server)	(Use Client Profile)
DneConnect Profile	None
NTLM Conn Pool	Nonel ~
HTTP Profile	http
TP Profile	Noriel V
SSL Profile (Client)	None
SSL Profile (Server)	None
NAT Pool	Auto Map 💌
lone Pool (Client)	None
lone Pool (Server)	None
ast Hop Pool	None
Session Profile	None Context: server V
sources	
Rules	Enabled Available gcuc_httptohttps Comparison Compa
ITTP Class Profiles	Enabled Available
Default Pool 두	pool_gcuc7777 V
efault Persistence Profile	sourceip_gcuc7777
allback Percistance Profile	None

Configure BIG-IP for WebCache Secure (Port 4443)

Use the following step-by-step procedure as a template for configuring the F5 BIG-IP to support the WebCache Secure Service for the OMS system.

Step 1: Create the WebCache Secure health monitor

- On the Main tab, expand Local Traffic, and then click Monitors. The Monitors screen opens.
- 2. Click Create.

The New Monitor screen opens.

- 3. In the **Name** field, enter a unique name for this Monitor. For example: mon_gcws4443.
- 4. From the **Type** list, select **HTTPS**.

The Monitor configuration options display.

- 5. From the Configuration list, select Advanced.
- 6. In the Configuration section, enter values in Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 30 and Timeout to 91.

7. In the Send String field, add a Send String, as follows:

GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)

8. In the **Receive String** field, add a Receive String, as follows:

/em/console/logon/logon;jsessionid=

9. In the Alias Service Port field, enter in 4443.

All other configuration settings are optional.

🚖 🏟	Image: Start					
IP Add	ame: Biglp6800.oracle.com D ress: 192.168.1.245 Ti	ate: J ime: 4	un 9, 2009 User: admin :43 PM (PDT) Role: Admini	istrator		
C	Unit 1 State: ACTIVE					
Mair	n Help About		Local Traffic » Monitors	» New Mo	onitor	
	Overview		General Properties			
	Access statistics, performance graphs, and links to helpful tools.		Name	5	non ocwe4443	
-	Templates and Wizards		Type		ITTPS	
Ľ	Templates		Import Settings	latting w		
	Device Wizards		mport detangs		upa 💽	
	Global Traffic		Configuration: Advanced	<i>.</i>		
0			Interval	30	D seconds	
V	Control the delivery of application traffic for a wide area network.		Timeout	9	1 seconds	
00	Local Traffic Network Map		Manual Resume	0	Yes 💿 No	
			Check Until Up	0	Yes 💿 No	
	Virtual Servers	Ē.		GE	T /em/console/home HTTP/1.0\nUser-Agent: Mo	
	Profiles	F.	Send String			
	iRules	÷.				
	Pools	P.			/em/console/logon/logon;jsessionid=	
	Nodes	÷.	Receive String			
	Monitors	×.				
	Rate Shaping Monitors	E F		1		
	Rate Shaping	×	1			
	Traffic Class	×	Cipher List		DEFAULT:+SHA:+3DES:+kEDH	
	SNATS	×	User Name			
	SSL Certificates	¥	Password			
	latuark		Compatibility		Enabled 💌	
	Configure network elements for		Client Certificate		None	
n	outing and switching.		Client Key		None	
¢ S	system		Reverse		🔿 Yes 💿 No	
a	configure system access, high vailability, reporting, and more.		Transparent		🔿 Yes 💿 No	
			Alias Address		* All Addresses	
			Alias Service Port		4443 Other:	
			Alias Service Port Cancel Repeat Fi	nished	4443 Other	

Step 2: Create the TCP profile for WebCache Secure service

The following procedure bases the TCP profile on the default TCP profile, and keeps all of the options at their default settings. You can configure these options as appropriate for your network.

To create a new TCP profile for the WebCache Secure service:

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

The HTTP Profiles screen opens.

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

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile. For example: tcp_gcws4443.

If needed, modify the name as applicable for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at the default levels.

6. Click Finished.

Hostnar IP Addre	ne: Biglp6800.oracle.com Date: ess: 192.168.1.245 Time;	Jun 9, 2009 User: admin 5:09 PM (PDT) Role: Administra	tor	
ß	Unit 1 State: ACTIVE			
Main	Help About	Local Traffic » Profiles : Pro	tocol:TCP » New TCP Profile	
	Overview Access statistics, performance	General Properties		
	graphs, and links to helpful tools.	Name	tcp_gcws4443	
Ê	Templates and Wizards	Parent Profile	tcp	
	Templates	Settings		
	Device Wizards	Reset On Timeout	Enabled	
	Global Traffic	Time Wait Recycle	Enabled	
0	Control the delivery of application traffic for a wide area network.	Delayed Acks	Enabled	
~~	Local Traffic	Proxy Maximum Segment		
	Network Map	Proxy Options		
	Virtual Servers	Proxy Buffer Low	4096 bytes	
	Profiles	Proxy Buffer High	16384 bytes	
	iRules F	Idle Timeout	Spectral N 300	

Step 3: Create a ClientIP persistence profile for the WebCache Secure service

When creating a ClientIP Persistence profile, the recommendation is to use the default SourceIP method for this profile, as follows:

1. On the Main tab, expand Local Traffic, and then click Profiles.

The HTTP Profiles screen opens.

- On the Menu bar, click Persistence.
 The Persistence Profiles screen opens.
- In the upper right portion of the screen, click Create. The New Persistence Profile screen opens.
- In the Name field, enter a unique name for this profile. In the MAA example, we entered sourceip_gcws4443.
- From the Persistence Type list, select Source Address Affinity. The configuration options for SourceIP persistence display.
- 6. Modify the persistence timeout value to **3600**.
- 7. Click Finished.

Name	sourceip_gcws4443	
Persistence Type	Source Address Affinity	
Parent Profile	source_addr 💌	
onfiguration		
Mirror Persistence		
Match Across Services		
Match Across Virtual Servers		
Match Across Pools		
Timeout	Specify 💉 3600	seconds
Mask	None 🗸 🗸	
Map Proxies	Enabled	
Override Connection Limit		

For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation resources listed in the <u>References</u> section.

Step 4: Create the pool for the WebCache Secure service

A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control WebCache Secure devices.

To create the WebCache Secure pool:

- On the Main tab, expand Local Traffic, and then click Pools. The Pool screen opens.
- 2. In the upper right portion of the screen, click **Create**.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings appropriately for your network.

3. In the Name field, enter a unique name for your pool.

In the MAA example, we entered pool_gcws4443.

4. In the Health Monitors section, select the name of the monitor you created in the "Create the WebCache Secure health monitor" step, and click Add (<<).

In the MAA example, we selected **mon_gcws4443**.

- From the Load Balancing Method list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In the MAA example, we selected Least Connections (member).
- 6. For this pool, we keep the Priority Group Activation at **Disabled**.
- 7. In the New Members section, make sure the New Address option button is selected.
- In the Address field, add the first server to the pool. In the MAA example, we entered 10.10.10.151.
- 9. In the **Service Port** field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

In the MAA example, we entered 4443.

- 10. Click Add to add the member to the list.
- 11. Repeat steps 8 through 10 for each server you want to add to the pool.

In the MAA example, we repeated these steps three times for the remaining servers: **10.10.10.152, 10.10.10.153, and 10.10.10154**.

Hostnan IP Addre	ne: Biglp6800.oracle.com ess: 192.168.1.245	Date: Time:	Jun 9, 2009 5:54 PM (PDT)	User: admin Role: Administrato			
Main	Unit 1 State: ACTIVE Help Abou	t	Local Traffi	c » Pools » New	Pool		
	Overview Access statistics, performan	ice	Configuration	n: Basic 💌			
	graphs, and links to helpful to	ols.	Name		pool_gcws4443	1	
Ê	Templates and Wizards		18		Active		Available
	Templates Device Wizards		Health Monitors		mon_gcws444	3 <<	mon_gcsc4444 🔺 mon_gcsu1159
						>>	mon_gcwu7779 tcp tcp_half_open
63	Global Traffic	ation	Resources				
	traffic for a wide area netwo	ark.	Load Balan	cing Method	Least Connections	(member)	~
R - R	Local Traffic		Priority Grou	up Activation	Disabled		
	Network Map				۲	New Address	O Node List
	Virtual Servers				Address: 10.	10.10.154	
	Profiles	- P			Service Port: 44	43 Selec	t 💌
	iRules		New Memb	ers	Add	151 4440	
	Pools				R:1 P:1 10.10.10. R:1 P:1 10.10.10.	151 :4443 152 :4443	
	Nodes				R:1 P:1 10.10.10.	154 :4443	
	Monitors	26			Edit Delet	e	
	Rate Shaping						
	Traffic Class		Cancel	epeat Finished			

Step 5: Create the WebCache Secure virtual server

This step configures a WebCache Secure virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures.

To create the virtual server:

- On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.
- In the upper right portion of the screen, click Create. The New Virtual Server screen opens.
- 3. In the **Name** field, enter a unique name for this virtual server.

In the MAA example, we entered vs_gcws4443.

- 4. In the **Destination** section, select the **Host** option.
- In the Address field, enter the IP address of this virtual server. In the MAA example, we used 10.10.101.
- 6. In the Service Port field, enter 4443.
- From the Configuration list, select Advanced. The Advanced configuration options display.
- 8. Keep the **Type** list at the default setting: **Standard**.
- 9. From the **Protocol Profile (Client)** list, select the name of the profile you created in the "<u>Create a TCP profile</u>" step.

In the MAA example, we selected tcp_gcws4443.

- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the SNAT Pool setting to Automap.
- 12. In the Resources section, from the **Default Pool** list, select the pool you created in the "<u>Creating the pool</u>" step.

In the MAA example, we selected pool_gcws4443.

13. From the **Default Persistence Profile** list, select the persistence profile you created in the "<u>Creating a ClientIP persistence profile</u>" step.

In the MAA example, we selected sourceip_gcws4443.

Name	vs_gcws4443
	Type: Host Network
Destination	Address: 10.10.10.101
Service Port	4443 Other: 💌
State	Enabled 💌
onfiguration: Advanced 💌	
Гуре	Standard
Protocol	TCP 💌
Protocol Profile (Client)	tcp_gcws4443
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	Nonel 🛩
HTTP Profile	None
FTP Profile	None 💌
SSL Profile (Client)	None
SSL Profile (Server)	None
SNAT Pool	Auto Map 💌
Clone Pool (Cli <mark>e</mark> nt)	None
Clone Pool (Server)	None
Last Hop Pool	None
Session Profile	None Context: server 💌
esources	
	Enabled Available
Pulse	
Rules	
	Up Down
	Enabled Available
	<< http://www.httpclass
HTTP Class Profiles	>>
	Up Down
Default Pool +	pool_gcws4443 💌
Default Persistence Profile	sourceip_gcws4443
Fallback Persistence Profile	None

Configure BIG-IP for WebCache Unsecure (Port 7779)

Use the following procedures as a template for configuring the F5 BIG-IP to support the WebCache Unsecure Service for the OMS system.

Step 1: Create the WebCache Unsecure health monitor

This procedure uses entries from the Monitor Port (Monitor Type) column in the Table 1.

- On the Main tab, expand Local Traffic, and then click Monitors. The Monitors screen opens.
- 2. Click Create.

The New Monitor screen opens.

- 3. In the **Name** field, enter a unique name for this Monitor. For example: mon_gcwu7779.
- 4. From the **Type** list, select **HTTP**.

The Monitor configuration options display.

- 5. From the Configuration list, select Advanced.
- 6. In the Configuration section, enter values in Interval and Timeout fields:
 - **Interval** is the Health Monitor property that specifies the frequency at which the system issues the monitor check.
 - **Timeout** is the setting that allows the monitor to fail three times before marking a pool member as down. The recommendation is to set the BIG-IP LTM Health Monitor Timeout setting as (3 * "Interval") + 1, allowing at least a 1:3 +1 ratio between the interval and the timeout.

The MAA example sets Interval to 30 and Timeout to 91.

7. In the Send String field, add a Send String, as follows:

GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)

8. In the **Receive String** field, add a Receive String, as follows:

/em/console/logon/logon;jsessionid=

9. In the Alias Service Port field, enter 7779.

All other configuration settings are optional.

Main	Help About	Local Traffic » Monitors	s » New Monitor			
	Overview Access statistics, performance	General Properties				
100 000000	graphs, and links to helpful tools.	Name	mon_gcwu7779			
Ê	Templates and Wizards	Туре	HTTP			
	Templates	Import Settings	http 💌			
	Device Wizards	Configuration: Advanced				
0	Global Traffic	Interval	30 seconds			
0	Control the delivery of application traffic for a wide area network.	Timeout	91 seconds			
	Local Traffic	Manual Resume	◯ Yes ⊛ No			
	Network Map	Check Until Up	○ Yes ⊙ No			
	Virtual Servers	Send String	GET /em/console/home HITP/1.0\nUser-Agent: Mozilla/4.0(compatible; MSIE 6.0; Windows NT 5.0)			
	Profiles +					
	iRules					
	Pools +		/em/console/logon/logon;jsessionid=			
	Nodes >	Receive String				
	Monitors +					
	Rate Shaping	Lloor Name				
	Traffic Class	Osermanie				
	SNATs >	Password				
	SSL Certificates	Reverse	O Yes 💿 No			
_	Network	Transparent	○ Yes ⊙ No			
	Configure network elements for	Alias Address	*All Addresses			
	routing and switching.	Alias Service Port	7779 Other: 💌			

Step 2: Create the TCP profile for the WebCache Unsecure service

The following procedure bases the TCP profile on the default TCP profile, and keeps all of the options at their default settings. You can configure these options as appropriate for your network.

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

The HTTP Profiles screen opens.

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

The New TCP Profile screen opens.

5. In the Name field, enter a unique name for this profile, For example: tcp_gcwu7779.

If needed, modify the name, as applicable for your network. See the F5 BIG-IP online help for more information about the configuration options. In the MAA example, we kept the settings at their default levels.

6. Click Finished.

Hostnan IP Addre	ne: Biglp6800.oracle.com ss: 192.168.1.245	Date: . Time: :	Jun 9, 2009 User: admin 5:11 PM (PDT) Role: Adminis	strator			
Main	Unit 1 State: ACTIVE Help About		Local Traffic » Profiles : F	Protocol : TCP » New TCP Profile			
Overview		B	General Properties				
	graphs, and links to helpful too	ls.	Name	tcp_gcwu7779			
Ê	Templates and Wizards Templates		Parent Profile	tcp			
			Settings				
Device Wizards		63	Reset On Timeout	Enabled			
Global Traffic			Time Wait Recycle	Enabled			
0	Control the delivery of applicat traffic for a wide area network	on c.	Delayed Acks	C Enabled			
~~	Local Traffic		Proxy Maximum Segment				
	Network Map		Proxy Options				
	Virtual Servers		Proxy Buffer Low	4096 bytes			
	Profiles	E	Proxy Buffer High	16384. bytes			
	iRules	•	Idle Timeout	Specify V 200			

Step 3: Creating a ClientIP persistence profile for the WebCache Unsecure service

When creating a ClientIP Persistence profile, the recommendation is to use the default SourceIP method for this profile.

To create a new ClientIP persistence profile based on the default profile

- On the Main tab, expand Local Traffic, and then click Profiles. The HTTP Profiles screen opens.
- 2. On the Menu bar, click **Persistence**.

The Persistence Profiles screen opens.

- In the upper right portion of the screen, click Create. The New Persistence Profile screen opens.
- In the Name field, enter a unique name for this profile. In the MAA example, we used sourceip_gcwu7779.

5. From the **Persistence Type** list, select **SourceIP**.

The configuration options for SourceIP persistence display.

- 6. Modify the persistence timeout value to **3600**.
- 7. Click Finished.

Name	sourceip_gcwu7779
Persistence Type	Source Address Affinity
Parent Profile	source_addr
onfiguration	
Mirror Persistence	
Match Across Services	
Match Across Virtual Servers	
Match Across Pools	
Timeout	Specify 💉 3600 seconds
Mask	None
Map Proxies	Enabled
Override Connection Limit	

For more information about creating or modifying profiles, or applying profiles in general, see the BIG-IP documentation that you can access by means of the <u>References</u> section.

Step 4: Creating the pool for the WebCache Unsecure service

The next step in this configuration is to create a pool on the BIG-IP system. A BIG-IP pool is a set of devices grouped together to receive traffic according to a load balancing method. In this configuration, we create one pool for the Grid Control WebCache Unsecure devices.

To create the WebCache Unsecure pool

- On the Main tab, expand Local Traffic, and then click Pools. The Pool screen opens.
- 2. In the upper right portion of the screen, click Create.

The New Pool screen opens.

Note: For more (optional) pool configuration settings, from the Configuration list, select **Advanced**. Configure these settings as applicable for your network.

- 3. In the **Name** field, enter a unique name for your pool. In the MAA example, we entered **pool_gcwu7779**.
- In the Health Monitors section, select the name of the monitor you created in the "Creating the WebCache Unsecure health monitor" step, and click Add (<<).
 In the MAA example, we selected mon_gcwu7779.
- From the Load Balancing Method list, choose your preferred load balancing method (different load balancing methods may yield optimal results for a particular network). In the MAA example, we selected Least Connections (member).
- 6. For this pool, we kept the Priority Group Activation as **Disabled**.
- 7. In the New Members section, make sure the New Address option is selected.
- In the Address field, add the first server to the pool. In the MAA example, we used 10.10.151.
- In the Service Port field, enter the service number you want to use for this device, or specify a service by choosing a service name from the list.

In the MAA example, we entered 7779.

- 10. Click Add to add the member to the list.
- 11. Repeat steps 8 through 10 for each server you want to add to the pool.

In the MAA example, we repeated these steps three times for the remaining servers: **10.10.10.152, 10.10.10.153, and 10.10.10.154**.

Hostnar IP Addre	ne: Biglp6800.oracle.com D ess: 192.168.1.245 Ti	ate: Jun 9, 2009 me: 5:57 PM (PDT)	User: admin Role: Administrat		
Main	Unit 1 State: ACTIVE	Local Traffi	c » Pools » New	r Pool	
	Overview Access statistics, performance	Configuratio	n: Basic 💌		
	graphs, and links to helpful tools.	Name		pool_gcwu7779	
(÷	Templates and Wizards			Active	Available
	Templates	Health Mon	itors	mon_gcwu7779	<pre>mon_gcar4889 mon_gcsc4444</pre>
	Device Wizards				>>> mon_gcsu1159 mon_gcuc7777 tcp
5	Global Traffic Control the delivery of application	Resources			
	traffic for a wide area network.	Load Balan	cing Method	Least Connections (member)	*
	Local Traffic	Priority Gro	up Activation	Disabled 💌	
	Network Map			New Add	fress 🔿 Node List
	Virtual Servers	(F)		Address: 10.10.10.154	
	Profiles			Service Port: 7779	Select 💌
	iRules	New Memb	ers	Add	1
	Pools	() (E		R:1 P:1 10.10.10.151:7779 R:1 P:1 10.10.10.152:7779 B:1 P:1 10 10 10 153:7779	
	Nodes	×		R:1 P:1 10.10.10.154 :7779	
	Monitors			Edit Delete]
	Rate Shaping				
	Traffia Class	Cancel	epeat Hinished		

Step 5: Create the WebCache Unsecure virtual server

This step configures a WebCache Unsecure virtual server that references the monitor, profiles, persistence and pool you created in the preceding procedures

To create the virtual server:

- On the Main tab, expand Local Traffic, and then click Virtual Servers. The Virtual Servers screen opens.
- In the upper right portion of the screen, click the Create button. The New Virtual Server screen opens.
- In the Name field, enter a unique name for this virtual server. In the MAA example, we entered vs_gcwu7779.
- 4. In the **Destination** section, select the **Host** option.
- 5. In the **Address** field, enter the IP address of this virtual server. In the MAA example, we used **10.10.101**.

- 6. In the Service Port field, enter 7779.
- From the Configuration list, select Advanced. The Advanced configuration options display.
- 8. Keep the Type list at the default setting: Standard.
- 9. From the **Protocol Profile (Client)** list select the name of the profile you created in the "Creating a TCP profile" step.

In the MAA example, we selected tcp_gcwu7779.

- 10. Keep the Protocol Profile (Server) option at the default setting.
- 11. Change the SNAT Pool setting to Automap.
- 12. In the **Resources** section, from the **Default Pool** list, select the pool you created in the "<u>Creating the pool</u>" step.

In the MAA example, we selected pool_gcwu7779.

13. From the **Default Persistence Profile** list, select the persistence profile you created in the "<u>Create a ClientIP persistence profile</u>" step.

In the MAA example, we selected sourceip_gcwu7779.

eneral Properties	
Name	vs_gcwu7779
Destination	Type: Host Network Address: 10.10.101
Service Port	7779 Other: 💌
State	Enabled 💌
onfiguration: Advanced 💌	
Туре	Standard 💌
Protocol	TCP 💌
Protocol Profile (Client)	tcp_gcwu7779
Protocol Profile (Server)	(Use Client Profile)
OneConnect Profile	None
NTLM Conn Pool	None 🗸
HTTP Profile	None
FTP Profile	None 😽
SSL Profile (Client)	None
SSL Profile (Server)	None
SNAT Pool	Auto Map 💌
Clone Pool (Client)	None
Clone Pool (Server)	None
ast Hop Pool	None
Session Profile	None 🔽 Context: server 🔽
sources	
	Enabled Available
Rules	
	Up Down
	Enabled Available
	< http://www.inter-statestatestatestatestatestatestatestat
HTTP Class Profiles	
Default Pool	
efault Persistence Profile	sourceip acwu7779
allback Pornictance Drafile	

Configuring Enterprise Manager for Use with F5 BIG-IP LTM

Oracle Enterprise Manager Architecture Overview

Oracle Enterprise Manager Middle tier framework is based on the Oracle Application Server 10g architecture and is comprised of the following components:

- Oracle HTTP Server (OHS)
- OC4J_EM
- OC4J_EMPROV
- WebCache
- dcm-daemon

The Oracle Management Service (OMS) application is contained in an OC4J container OC4J_EM, which handles a number of operations including console UI access servlet, agent upload receivelet, repository loader servlet, job dispatchers. The OMS application provides various services, each using its own protocol. To access the client and agent services, an OHS Web interface is integrated with each OMS.

For the OMS to maintain service availability for its "clients" (the console UI and Management Agents), the following services minimally must be available:

- UI Access Services
 - SSL
 - Non-SSL
- Agent Upload Services
 - SSL
 - Non-SSL

In configurations with more than one OMS installed, a common OMS name must be established for Enterprise Manager Agents and Console UI. The F5 BIG-IP LTM will act as a single point of contact for these components, distributing the load to any available OMS. For more details about configuring Multiple OMS environments, see Chapter 17 in the <u>Oracle Enterprise Manager</u>. <u>Grid Control Installation and Configuration Guide</u> at

http://download.oracle.com/docs/cd/B16240_01/doc/install.102/e10953/toc.htm

In Figure 2 multiple OMS servers and an F5 Load Balancer are configured to manage traffic from Management Agents and Console UIs.



Figure 2 : Multiple OMS Servers and F5 Load Balancer Configuration

Note: The Virtual IP address used by the F5 BIG-IP must be in the same subnet as the one of the Self-IPs of the load balancer. The Self-IP is configured using the network configuration tab on the BIG-IP management interface. The OMS machines that will be used in this configuration should also be in the same subnet.

Configuring Shared Loader Directory

The first step to configure multiple OMS servers behind an SLB requires that you setup a shared disk for access by all OMS servers. Then, configure each OMS to use the same directory on this shared disk for receiving and staging uploaded files from monitored agents. This way, each OMS can share the load of processing and loading these files into the repository database. This *shared receive* directory also ensure continuous data processing in the event of a single OMS failure by the surviving OMSs.

Use the following steps to configure the OMS to use a shared receive directory.

- 1. Stop all OMS services for each OMS (cd to OMS_HOME/opmn/bin):
 - ./opmnctl stopall

- 2. Run the following command from the OMS_HOME/bin directory: ./emctl config oms loader -shared yes -dir /vol3/OMS/shared_recv
- 3. Repeat these commands for all other OMS servers.
- 4. Start the OMS from OMS_HOME/bin directory using the following command:

./emctl start oms

Configuring OHS

At this point, you are ready to configure each OMS to enable the use of the common OMS name on the SLB for client UI traffic.

The following table shows the default ports that are typically used for Grid Control when using an SLB:

```
TABLE 2: DEFAULT PORTS USED FOR GRID CONTROL WITH SLB
```

PORT	DESCRIPTION
4889	Agent unsecure Upload HTTP service and Agent Registration port
1159	Agent secure HTTPS service port
7777	Console UI unsecure service port
4444	Console UI secure HTTPS service port

Configure Non-SSL UI

For HTTP UI access, perform the following tasks on each OMS:

1. Stop the OHS:

~/omsl0g/opmn/bin \$./opmnctl stopproc ias-component=HTTP_Server
opmnctl: stopping opmn managed processes...
~/omsl0g/opmn/bin \$

Note: Backup the httpd.conf file before editing it in step 2

2. Add VirtualHost section with SLB alias in httpd.conf.

Note: This should match the F5 Virtual server port. In this case, both are set to 7777.

```
cd ~/oms10g/Apache/Apache/conf
vi httpd.conf
<VirtualHost *:7777>
DocumentRoot "absolute path to
your/oms10g/Apache/Apache/htdocs"
ServerName myslb.acme.com
Port 7777
</VirtualHost>
```

- 3. Save the httpd.conf file and exit.
- 4. Start the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

Configure SSL UI (10.2.0.4 and earlier versions)

For SSL UI access, perform the following tasks on each OMS (versions < 10.2.0.5):

1. Stop the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl stopproc ias-component=HTTP_Server
opmnctl: stopping opmn managed processes...
~/oms10g/opmn/bin $
```

Note: Backup the ssl.conf file before editing it in step 2.

2. Change the following section in ~/omsl0g/Apache/Apache/conf/ssl.conf files, as shown in the following table:

ORIGINAL SECTION	NEW SECTION
Listen 4444	Listen 4444
<virtualhost _default_:4444=""></virtualhost>	<virtualhost _default_:4444=""></virtualhost>
# General setup for the virtual host	# General setup for the virtual host
DocumentRoot	DocumentRoot
"/app/oracle/Grid2/oms10g/Apache/Apache/htdocs"	"/app/oracle/Grid2/oms10g/Apache/Apache/htdocs"
ServerName omshost.acme.com <<<	ServerName myslb.acme.com <<< change
current OMS hostname	to your SLB alias
ServerAdmin you@your.address	ServerAdmin you@your.address
ErrorLog	ErrorLog
TransferLog	TransferLog
Port 8250	Port 443

- 3. Save the ssl.conf file and exit.
- 4. Start the OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

5. Update dcm with the new configuration:

```
cd ~/oms10g/dcm/bin
./dcmctl updateconfig -ct ohs
```

6. Start OHS:

```
~/oms10g/opmn/bin $ ./opmnctl startproc ias-component=HTTP_Server
opmnctl: starting opmn managed processes...
~/oms10g/opmn/bin $
```

7. Secure each OMS using the common SLB virtual hostname:

```
cd ~/oms10g/bin
./emctl secure oms -host myslb.acme.com -secure_port 1159
```

```
Oracle Enterprise Manager 10g Release 4 Grid Control
Copyright (c) 1996, 2007 Oracle Corporation. All rights reserved.
Enter Enterprise Manager Root Password :
Enter Agent Registration password :
OPMN processes successfully stopped... Done.
Securing central oms... Started.
Checking Repository... Done.
```

```
Checking Em Key...
                     Done.
Checking Repository for an existing Enterprise Manager Root Key...
Done.
Fetching Root Certificate from the Repository...
                                                   Done.
Generating Registration Password Verifier in the Repository...
Done.
Generating Oracle Wallet Password for Enterprise Manager OMS...
Done.
Generating Oracle Wallet for Enterprise Manager OMS...
                                                          Done.
Generating Oracle Wallet for iAS HTTP Server...
                                                  Done.
Updating HTTPS port in emoms.properties file...
                                                  Done.
Generating HTTPS Virtual Host for Enterprise Manager OMS...
Done.
Securing central oms...
                          Ended.
OPMN processes successfully restarted...
                                           Done.
```

Configure SSL UI (10.2.0.5 and later versions)

If the OMS is running release 10.2.0.5 or higher, you can skip editing the ssl.conf file and specify the SECURE_PORT, SLB_PORT and SLB_CONSOLE_PORT parameters when you secure the OMS:

```
cd ~/oms10g/bin
./emctl secure oms -host myslb.acme.com -secure_port 4888 -slb_port 1159
-slb_console_port 443
```

The preceding example is based on assumptions for the OMS and SLB parameters that are shown in the following table:

	HOSTNAME	SSL UPLOAD PORT	SSL UI PORT
SLB	myslb.acme.com	1159	443
OMS	omshost.acme.com	4889	4444

Note the following:

- The SLB_PORT parameter is required only if it is different from the SECURE_PORT parameter.
- By specifying the SLB_CONSOLE_PORT parameter, you do not need to manually modify the servername and port directives in the ssl.conf file.
- If you do not specify the SLB_CONSOLE_PORT parameter, then you will have to manually change the servername and port directives in the ssl.conf file.

Finally, check the secure status of the OMS by issuing the following command:

./emctl status oms -secure

Oracle Enterprise Manager 10g Release 4 Grid Control Copyright (c) 1996, 2007 Oracle Corporation. All rights reserved. Checking the security status of the OMS at location set in /app/oracle/Grid2/oms10g/sysman/config/emoms.properties... Done. OMS is secure on HTTPS Port 1159

Appendix A: F5 BIG-IP Local Traffic Manager Terms

This document assumes that you are familiar with F5 Networks <u>BIG-IP</u>. This section discusses the basic terminology. For a detailed discussion of these terms, see the <u>BIG-IP Solutions Guide</u> and the <u>BIG-IP Configuration Guide</u>.

The version of BIG-IP software used in this white paper is BIG-IP Version 10.0.1, Build 283. Terminology is identical between Version 9 and 10 of the BIG-IP software, but specific commands may have slightly different syntax.

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 Grid 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, you must configure a load balancing pool of the actual physical devices (members) you wish to forward the traffic to. You can then create the virtual server, specifying that pool as the destination for any traffic coming from this virtual server. Also, if you want some of the traffic from that virtual server to go to multiple pools based on a predetermined criterion, then you can create a rule specifying the criteria, and BIG-IP would forward the traffic to a pool matching the rule's criteria. A virtual server is configured to a specific port or to accept "ANY" ports.

A given F5 BIG-IP device may contain one or more virtual servers.

Profile

A **profile** is an F5 object that contains user-configurable settings for controlling the behavior of a particular type of network traffic, such as TCP or HTTP connections. BIG-IP version 9.0 and later uses profiles.

Using profiles enhances your control over managing network traffic, and makes trafficmanagement tasks easier and more efficient. It also allows for different characteristics to be matched to specific clients or applications. For example, one HTTP profile could be configured for Internet Explorer browsers, a different profile for Mozilla browsers, and yet another profile for hand held mobile browsers. You would have 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 you do not change any of the settings initially. Creating new profiles allows you to easily modify the profile settings specific to this deployment, and ensures that you do not accidentally overwrite the default profile.

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 Grid Control services, persistence needs to be configured for every service, except for the Secure Upload service.

Rule

A rule is a user-written script that uses criteria to choose among one or more pools. In the BIG-IP software, it is called an iRule and provides a powerful and more granular level of control over traffic management. For an incoming request to a virtual server, the iRule is evaluated and selects the pool to which a request will be sent. For more information about F5 iRules, see the F5 DevCentral Web site at http://devcentral.f5.com/Default.aspx?tabid=75

Appendix B: Summary and Examples

F5 Configuration Summary

Based on the configuration example used throughout this document, you should finish the F5 configuration and have a working environment. The finished configuration should look similar to the screen shots shown here of a BIG-IP LTM configured for all six of the Grid Control Services.

Hostnai IP Addr	me: Biglp6800.oracle.com ess: 192.168.1.245	Date: Ju Time: 3:	in 10, 2 44 PM (2009 (PDT)	User: admin Role: Admir	istrator	
ß	Unit 1 State: ACTIVE						
Main	Help Abo	out	Loca	al Traffic >	» Monitors		
	Overview		# -	Monitor	List		
	Access statistics, perform graphs, and links to helpful	ance tools.	r			Search	
स्ति	Templates and Wizard	s		 Name 			
	Create common application	traffic	🖾 gateway_icmp				
	and system corrigerations		12	http			
Global Traffic			🖾 https				
U	control the delivery of appl traffic for a wide area netw	ication vork.	C	https_443	3		
R -0	Local Traffic			icmp			
	Network Map	F		mon acc	r4000	1	
	Virtual Servers	<u>.</u>		mon_gca	14009		
	Profiles	(b)		mon_gcs	c4444		
	iRules	<u>.</u>		mon_gcs	u1159		
	Pools			mon_gcu	ic7777		
	Nodes	ം		mon_gcv	vs4443		
	Monitors			mon_gcv	vu7779		
	Pate Shaning		322	real con	ior.	1	

These are the Health Monitors for the Grid Control services.

Main	Help	About	Loca	al Traffic » Profil	es : Protocol : TCP				
	Overview Access statistics, p graphs, and links to	erformance helpful tools.	*						
Ê	Templates and Wizards Create common application traffic and system configurations.			✓ Name ☐ tcp					
5	Global Traffic Control the delivery traffic for a wide an	of application ea network.		tcp-lan-optimized					
	Local Traffic Network Map Virtual Servers			tcp_gcar4889					
				tcp_gcsc4444					
	Profiles			tcp_gcuc7777					
	iRules Pools Nodes Monitors			tcn_ncws4443					
				top_gen/34443					
				tcp_gcwu7779					
				wom-tcp-lan-optimized					
	Rate Shaping			wom-tcp-wan-optimized					
	Traffic Class		Dele	Delete					

These are the TCP profiles created for the Grid Control services.

Hostname IP Addres	a: Biglp6800.oracle.com ss: 192.168.1.245	Date: Time:	Jun 10, 20 3:48 PM (F	009 L PDT) F	Jser, admin Role: Admin	istrator		
6	Unit 1 State: ACTIVE							
Main	Help About		Local	Traffic »	Profiles :	Persistence		
	Overview		⇔ -	Services		 Persistence 		
	Access statistics, performance graphs, and links to helpful tools	s.	۲			Search		
Ren 1	Templates and Wizards Create common application traffic			 Name 				
			0	cookie				
	Global Traffic Control the delivery of application traffic for a wide area network.			cookie_gc	ar4889			
53			D	dest_addr				
t				hash				
R-0 1	Local Traffic			msrdp				
	Network Map		E sip_info					
	Virtual Servers			source_a	ddr			
	Profiles	R		sourceip_	gcsc4444			
	iRules	- E		sourceip_	gcuc7777			
	Pools			sourceip_	gcws4443			
				sourceip_	gcwu7779			
	Monitors	ĸ	0	ssl				
	Rate Shaping	×.		universal				
	Traffic Class	ĸ	Delete					

Persistence Profiles for the Grid Control services.

Hostnar IP Addre	ne: Bigip6800.oraci ess: 192.168.1.245	le.com	Date: Time:	Jun 10, 20 3:51 PM (F	109 L PDT) F	Jser: adn Role: Adr	nin ninistrator	
ß	Unit 1 State: ACTI	VE						
Main	Help	About		Local	Traffic »	Pools		
	Overview			# -	Pool Lis	ti	Statistics	
	Access statistics, performance graphs, and links to helpful tools.			•			Search)
Ê	Templates and V	Vizards		 Image: A start of the start of	Status	A Nan	ne	
	Create common application traffic and system configurations.				٠	pool_g		
	Global Traffic Control the delivery of application traffic for a wide area network.				•	pool_g		
5					٠	pool_c		
						pool_g		
	Local Traffic Network Map				•	pool_g	cws4443	
					D 000 gcwu7779			
	Virtual Servers			Dalat				
	Profiles		×.	Delet				

Pools for the Grid Control services.

Local	Traffic »	Virtual Servers					
# -	Virtual Se	rver List Virtual Address List Statis	tics				
L.		Create	_				Consta
	✓ Status	▲ Name	Partition	Destination	Service Port	Type	Resources
	•	vs_gcar4889	Common	10.10.10.101	<mark>4</mark> 889	Standard	Edit
	•	vs_gcsc4444	Common	10.10.10.101	443 (HTTPS)	Standard	Edit
	•	vs_gcsu1159	Common	10.10.10.101	1159	Standard	Edit
	•	vs_gcuc7777	Common	10.10.10.101	7777	Standard	Edit
	•	vs_gcws4443	Common	10.10.10.101	4443	Standard	Edit
	•	vs_gcwu7779	Common	10.10.10.101	7779	Standard	Edit
Enable	Disable	Delete					

Virtual Servers for the Grid Control services.

References

Oracle

- 1. Oracle Maximum Availability Architecture Web site http://www.otn.oracle.com/goto/maa
- 2. Oracle Database High Availability Overview (Part #B14210) http://otn.oracle.com/pls/db111/db111.to_toc?partno=b28281
- 3. Oracle Database High Availability Best Practices (Part B25159) http://otn.oracle.com/pls/db111/db111.to_toc?partno=b28282

F5

- 1. F5 Networks Home Page http://www.f5.com
- 2. F5 and Oracle Solutions Home Page http://www.f5.com/solutions/applications/oracle/
- 3. F5 Oracle Grid Control Configuration Guide http://www.f5.com/pdf/deployment-guides/oracle-grid-control-big-ip-dg.pdf
- 4. F5 BIG-IP Product Documentation http://www.f5.com/products/big-ip/
- F5 Version 10 Software Configuration Guide <u>https://support.f5.com/kb/en-us/products/big-</u> ip ltm/manuals/product/ltm configuration guide 10 0 0.html
- 6. F5 Technical Support Knowledge Base https://support.f5.com/kb/en-us.html
- F5 and Oracle Cooperative Support Agreement http://www.f5.com/news-press-events/press/archive/20050725b.html
- 8. F5 Training and Support http://www.f5.com/training-support/
- F5 DevCentral Web site http://devcentral.f5.com/Default.aspx?tabid=75



Configuring Maximum Availability Architecture for Oracle Enterprise Manager with F5 BIG-IP Local Traffic Manager February 2010 Authors: Farouk Abushaban, Oracle Corporation Chris Akker, F5 Networks James Viscusi, Oracle Corporation

Oracle Corporation World Headquarters 500 Oracle Parkway Redwood Shores, CA 94065 U.S.A.

Worldwide Inquiries: Phone: +1.650.506.7000 Fax: +1.650.506.7200 oracle.com

D

Oracle is committed to developing practices and products that help protect the environment

Copyright © 2010, 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 and conditions 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.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

0109