Configuring Oracle Enterprise Manager Grid Control 11g for Maximum Availability Architecture with Cisco Application Control Engine (ACE) Application Delivery Switch

Configuration Guide

October 2010

Scope

A step-by-step guide for configuring Oracle Enterprise Manager (OEM) Grid Control with Maximum Availability Architecture (MAA) behind a Cisco Application Control Engine (ACE) application delivery switch.

Executive Summary

This document shows how to properly configure OEM 11g with the Cisco ACE. This configuration is recommended by Oracle's Best Practices for load balancing Grid Control Oracle Management Service (OMS) Servers. Adding the Cisco ACE to your OEM deployment brings additional capabilities in the form of reliability, availability and scalability. This guide covers:

1. **Introduction to Oracle Enterprise Manager 11g**
2. **Enterprise Manager 11g Maximum Availability Architecture (MAA) with Server Load Balancing**
3. **Introduction to Cisco Application Control Engine (ACE)**
4. **OMS Configuration**
5. **Cisco ACE configuration**
6. **Oracle Enterprise Manager Agent configuration**

Audience

In general, the procedures in this document are intended for advanced users of OEM and Cisco ACE. It is intended for assisting OEM administrators and Cisco ACE users to quickly configure each component through a set of step-by-step configuration instructions aided with screen shots, making it easier to configure Cisco ACE as a critical component in the HA setup of Grid Control.

Introduction to Oracle Enterprise Manager 11g

Oracle Enterprise Manager 11*g* is the centerpiece of Oracle's integrated IT management strategy, which rejects the notion of management as an after-thought. At Oracle, we design manageability into each product from the start, enabling Oracle Enterprise Manager to then serve as the integrator of manageability across the entire stack encompassing Oracle and non-Oracle technologies. Fueled by this unique vision, Oracle Enterprise Manager 11*g* has introduced *business-driven IT management* to help IT deliver greater business value through three highly differentiated capabilities:

- Business-driven application management, which combines industry-leading capabilities in real user experience management, business transaction management and business service management to improve application users' productivity while enhancing business transaction availability
- Integrated application-to-disk management, which provides deep management across the entire Oracle stack to reduce IT management complexity and eliminate disparate point tools
- Integrated systems management and support, which utilizes industry-first technology bring support services into the IT management console; enabling proactive IT administration, increased application and system availability, and improved customer satisfaction

Enterprise Manager 11g Maximum Availability Architecture (MAA) with Server Load Balancing

Highly Available systems are critical to the success of virtually every business today. It is equally important that the management infrastructure monitoring these mission-critical systems is highly available. The Enterprise Manager Grid Control architecture is engineered to be scalable and available from the ground up. It is designed to ensure that you concentrate on managing the assets that support your business, while it takes care of meeting your business Service Level Agreements.

Best practices for Enterprise Manager 11g with Maximum Availability Architecture

When you configure Grid Control for high availability, your aim is to protect each component of the system, as well as the flow of management data in case of performance or availability problems, such as a failure of a host or a Management Service. Maximum Availability Architecture (MAA) provides a highly available Enterprise Manager implementation by guarding against failure at each component of Enterprise Manager.

One MAA best-practice is to install and configure OEM 11g behind a Server Load Balancer Router (SLB or LBR) such as Cisco Application Control Engine (ACE). Adding Cisco ACE to your OEM configuration brings additional capabilities in the form of reliability, availability and scalability. The following paper will detail the technical integration between Cisco ACE and Oracle Enterprise Manager.

Introduction to Cisco Application Control Engine (ACE)

The Cisco® ACE Application Control Engine is a family of application switches for maximizing the availability, acceleration, and security of data center applications. ACE allows enterprises to accomplish four primary IT objectives for application delivery:

- Maximize application availability
- Accelerate application performance
- Secure the data center and critical business applications
- Facilitate data center consolidation through the use of fewer servers, load balancers, and firewalls

ACE leverages the full range of Cisco application switching technology, including Layer 4 load balancing and Layer 7 content switching, server offload of SSL and smart TCP processing. These innovative application delivery features are offered on a unique virtualized architecture for significant CAPEX and OPEX savings by ACE customers.

Cisco ACE is offered in two form factors: (1) The ACE module for the Catalyst 6500 industry-leading enterprise class switch family and for the Cisco 7600 router family, and (2) The ACE 4710 standalone appliance. Each platform is enabled with a powerful software-based licensing mechanism that allows ACE customers to grow to higher levels of performance and scale without having to replace the current product.

OMS Configuration

Oracle Enterprise Manager 11g architecture is based on WebLogic Server (WLS). The key operations of OEM takes place in Oracle Management Services (OMS), this application is contained in a J2EE container EMGC_OMS, this application handles a number of operations including console User Interface (UI) access servlet, agent upload recievlet, repository loader servlet, job dispatchers and more. To access the client and agent services, an Oracle http server (OHS) web interface is integrated with each OMS. For more information please see the Oracle EM Concepts Guide:

http://download.oracle.com/docs/cd/E11857_01/em.111/e11982/toc.htm

The OMS application provides various services, each using its own protocol. Essentially, to maintain accessibility of OMS operation for its “clients” the following services must be available:

UI Access Services

- SSL
- Non-SSL

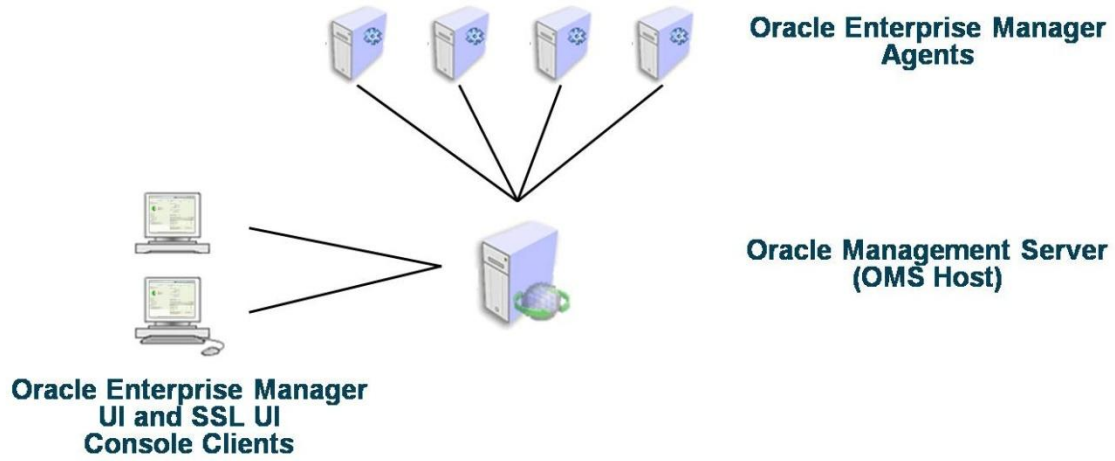
Note: Non-SSL UI access is not enabled by default. Oracle recommends that all UI communication should be over SSL. Non-SSL configuration steps are documented for those who still wish to use non-SSL.

Agent Upload Services

- SSL
- Non-SSL (Registration)

Figure 1 illustrates a single OMS deployment.

Figure 1: Single OMS Deployment

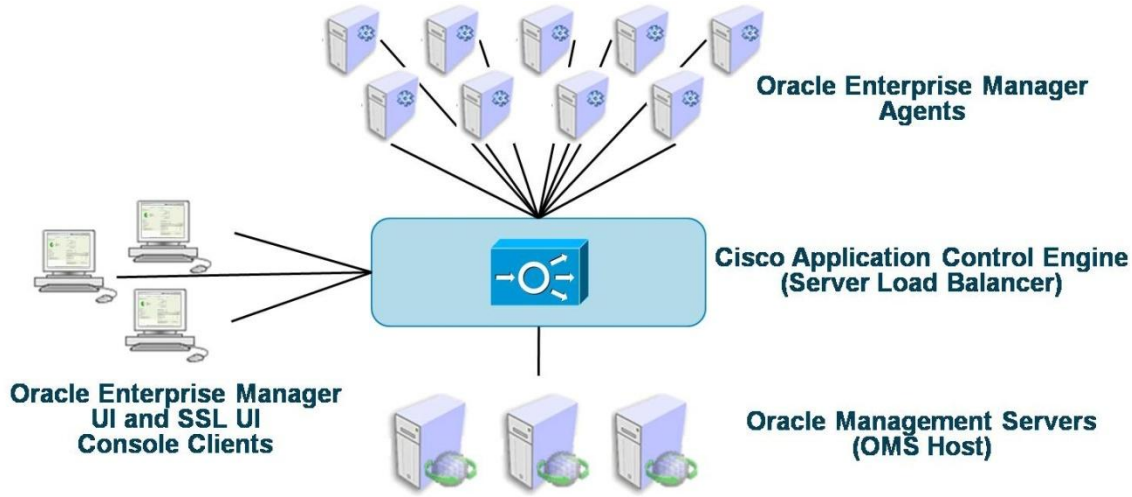


For high availability of Enterprise Manager, you would want to have **more than one** Oracle Management Services (OMSs) running in active/active mode.

To perform seamless load-balancing and routing of traffic to a "pool" of OMSs, a Server Load Balancer / Router should be used. Therefore, in order for Management Agents and Console UI's to utilize each OMS service simultaneously, **a common OMS name must be established**. This is where the Cisco ACE, acting as SLB, facilitates a single gate for entry.

Refer to Figure 2 for an illustration of multiple OMS servers and a Cisco ACE.

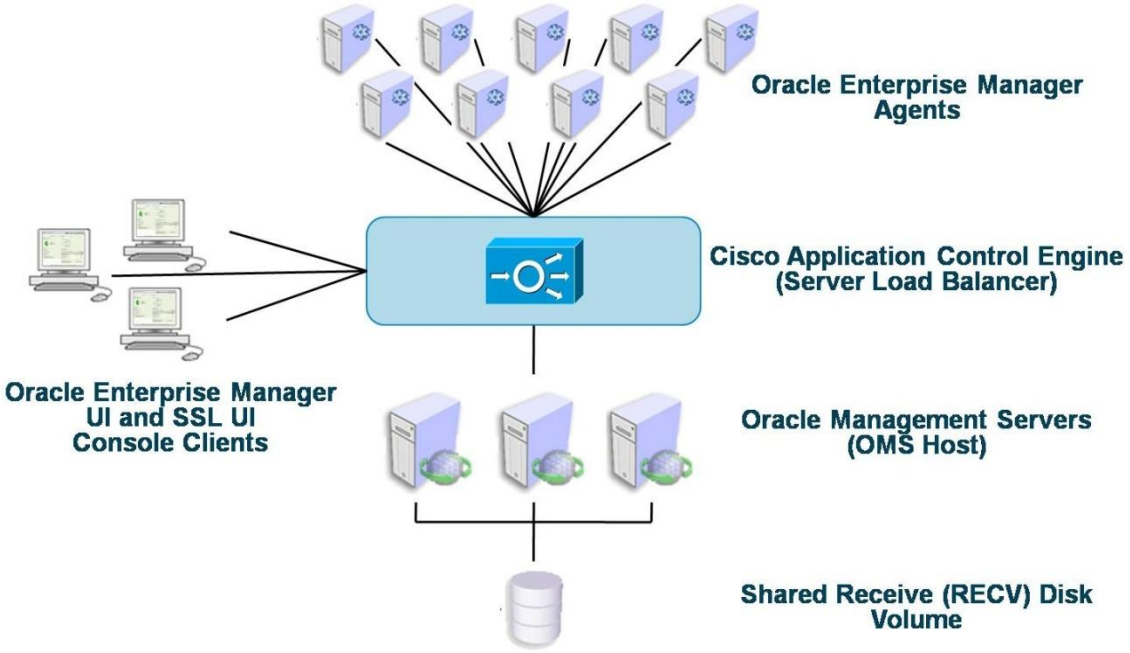
Figure 2: Multiple OMS Servers and a Cisco ACE



Additionally, each OMS service will use a temporary loader directory for receiving upload files from target agents. In a multi-OMS configuration, a shared receive (RECV) disk volume is necessary and must be used by all OMS servers in a Grid Control deployment.

Figure 3 illustrates the shared loader disk for OMS RECV directory.

Figure 3: OMS RECV Directory



For more information on Grid Control architecture, please see the online documentation on OTN:
http://download.oracle.com/docs/cd/E11857_01/em.111/e11982/toc.htm

Section 1 OMS Configuration

Configuring Shared Loader Directory

Step 1: Test Write permission to 'shared receive' directory
The first step in configuring multiple OMS servers requires that you setup a shared disk for access by all OMS servers. This 'shared receive' directory also ensures continuous data processing in the event of a single OMS failure by the surviving OMSs. Once you identify a suitable shared disk for both OMS servers, for example /Vol3/OMS/shared_recv, test write permissions by writing a file from one OMS host into this directory, then editing/deleting the same file from the other OMS host and vice versa.

Step 2: 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. The commands for achieving this:

1. Stop all OMS services
   emctl stop oms -all
2. Run the following command from the OMS_HOME/bin directory:
   emctl config oms loader –shared yes –dir /vol3/OMS/shared_recv

3. Run the same command from all other OMS servers.
4. Start the OMS from OMS_HOME/bin using:
   emctl start oms

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

Typically, the default ports used for Grid Control when using a Cisco ACE as SLB are:

Port 4889	Agent unsecure Upload HTTP service and Agent Registration port
Port 1159	Agent secure HTTPS service port
Port 7788	Console UI unsecure service port
Port 7799	Console UI secure HTTPS service port

Notice that UI service ports vs agent upload ports (HTTP and SSL enabled HTTP or HTTPS) are different. This helps to segregate UI traffic from Agent traffic.

To identify your specific OMS ports, execute the following command on each OMS host:

```
emctl status oms -details

Oracle Enterprise Manager 11g Release 1 Grid Control

Copyright (c) 1996, 2010 Oracle Corporation. All rights reserved.

Enter Enterprise Manager Root (SYSMAN) Password :

Console Server Host : lxclu1.acme.com

HTTP Console Port   : 7788

HTTPS Console Port  : 7799

HTTP Upload Port    : 4890

HTTPS Upload Port   : 4900

OMS is not configured with SLB or virtual hostname

Agent Upload is unlocked.

OMS Console is unlocked.

Active CA ID: 1
```

Configure Non-SSL UI

For HTTP UI access, traffic is routed directly to the Oracle HTTP Server. In 11g, there is no need to make any changes to access the UI via the SLB in non-SSL mode.

Configure SSL UI

For HTTPS UI access, traffic is routed to the SSL module loaded at the Oracle HTTP Server. Therefore, we need to "proxy-in" the hostname of the SLB virtual server. This is done automatically for you by running "emctl" using SLB arguments. Please perform the following tasks on each OMS:

Configure SSL UI

You can configure the OMS directly using emctl commands, without editing any of the .conf files. The following parameters can be used to configure the following ports:

[-secure_port] <<< SSL Upload (agent) Port at the OMS host

[-upload_http_port] <<< HTTP Upload (agent) Port at the OMS host

[-slb_port] <<< SSL Upload (agent) Port on the SLB

[-slb_console_port] <<< SSL Console Port on the SLB

The following examples provide different scenarios that explain how to map ports from the SLB (Cisco ACE) to the OMS, and the resulting URLs to use. If you choose to use the default OMS ports for each service on the SLB, then no customization is needed. However, if you choose to use a default HTTPS port on the SLB side, your resulting URL can be customized and simplified for the convenience of end-users.

Example 1

Configure the SLB virtual host to use the same ports as those on the OMS servers. Basically, you have a default installation and your new URLs that you will be using to access the console will only change hostnames, not ports.

Cd ~/oms10g/bin

./emctl secure oms -host myslb.acme.com

Resulting URLs:

Through SLB:

Console UI http://myslb.acme.com:7788/em

Console SSL UI: https://myslb.acme.com:7799/em

Agent upload (non-SSL) http://myslb.acme.com:4889/em/upload

Agent upload (SSL) https://myslb.acme.com:1159/em/upload

To bypass the SLB and go directly to a specific OMS host service, use the following URL examples:

Console UI : http://oms1.acme.com:7788/em/console/logon/logon

Console SSL UI: https://oms1.acme.com:7799/em/console/logon/logon

Agent upload (non-SSL) http://oms1.acme.com:4889/em/upload

Agent upload (SSL) https://oms1.acme.com:1159/em/upload

The above example is based on the following assumptions for OMS and SLB parameters:

	SSL Upload Port	SSL UI Port
SLB	1159	7799
OMS	1159	7799

Example 2
SLB virtual host will use different ports to build its virtual host services than the OMS servers. In other words, you will have to use new URLs to access the console, which not only use the SLB hostname, but also different ports than what you used before the access through SLB was configured.

cd ~/oms10g/bin

./emctl secure oms -host myslb.acme.com -secure_port 4888 -slb_port 1159 -slb_console_port 443

Resulting URLs:
Through SLB:

Console UI http://myslb.acme.com:7778/em

Console SSL UI: https://myslb.acme.com/em (443 is the default HTTPS port)

Agent upload (non-SSL) http://myslb.acme.com:4889/em/upload

Agent upload (SSL) https://myslb.acme.com:1159/em/upload

To bypass SLB (or before SLB configuration for Agent uploads):

Console UI : http://oms1.acme.com:7778/em/console/logon/logon

Console SSL UI: https://oms1.acme.com:4444/em/console/logon/logon

Agent upload (non-SSL) http://oms1.acme.com:4889/em/upload

Agent upload (SSL) https://oms1.acme.com:4888/em/upload

The above example is based on the following assumptions for OMS and SLB parameters:

	SSL Upload Port	SSL UI Port
SLB	1159	443
OMS	4888	4444

The slb_port parameter is only required if it is different from secure_port. By specifying slb_console_port, you don't have to manually modify the servername and port directives in ssl.conf. If you don't specify the slb_console_port, then you will have to manually change the servername and port directives in ssl.conf.

Finally, check the secure status of the OMS:

[omshost1]/refresh/gc111a/WLS/oms11g> emctl status oms -details

Oracle Enterprise Manager 11g Release 1 Grid Control

Copyright (c) 1996, 2010 Oracle Corporation. All rights reserved.

Enter Enterprise Manager Root (SYSMAN) Password :

Console Server Host : omshost1.acme.com

HTTP Console Port : 7788

HTTPS Console Port : 443

HTTP Upload Port : 4889

HTTPS Upload Port : 1159

SLB or virtual hostname: myslb.acme.com

Agent Upload is unlocked.

OMS Console is unlocked.

Active CA ID: 1

Note: Based on the selection done at install time, emctl secure unlock -console might be required to unlock Agent Upload and OMS Console non-SSL services.

Section 2 SLB Configuration

Your SLB vendor may have a GUI service for configuration operations. In this document the examples are shown using the embedded Device Manager for the a Cisco® ACE Application Control Engine (ACE) 4710 appliance as SLB. These examples are the same/similar to those for users of Cisco® Application Networking Manager for configuration, monitoring and operations management of multiple Cisco ACE 4710 appliances and/or Cisco® ACE Application Control Engine (ACE) Module for the Cisco Catalyst® 6500 Series Switches and Cisco 7600 Series Routers. Also, refer to Chapter 18 of the Grid Control Administrator's Guide on Load Balancer configurations.

The Cisco ACE Solution

The Cisco ACE is a network load balancing solution for highly available applications that need single point of access. This section demonstrates how to configure the required components of the Cisco ACE load balancer to provide access to OEM configured for high availability. The following table lists these common terms that will be used in the SLB configuration section.

Service	Description
Virtual Context	An ACE partition when multiple virtual devices or contexts exist. Each context contains its own set of policies, interfaces, resources, and administrators.
Probes	The process by which ACE determines that the service is up and running and can accept incoming requests.
Server Farms	A group of application servers hosts running an instance of the same Grid Control service (i.e. agent upload farm)
Stickiness	Stickiness (or session persistence) is a feature that allows the same client to maintain multiple simultaneous or subsequent TCP connections with the same real server for the duration of a session.
Virtual Server	A representation of a farm of services, accessible by one single / unique address
Grid Control Service	An instance of the specific service on the Grid Control server
VLAN	A VLAN is a network interface associated with a virtual context

The process of configuring your load balancer involves five steps:

1. Create Resource Class
2. Create Probes
3. Create Source Network Address Translation (SNAT) Pool(s)
4. Create Virtual Servers
5. Add Server Farms, Probes and custom properties to each Virtual Server

The goal is to create four Virtual Servers:

- SSL Console UI
- SSL Agent Upload
- Non-SSL Console UI
- Non-SSL Agent Upload

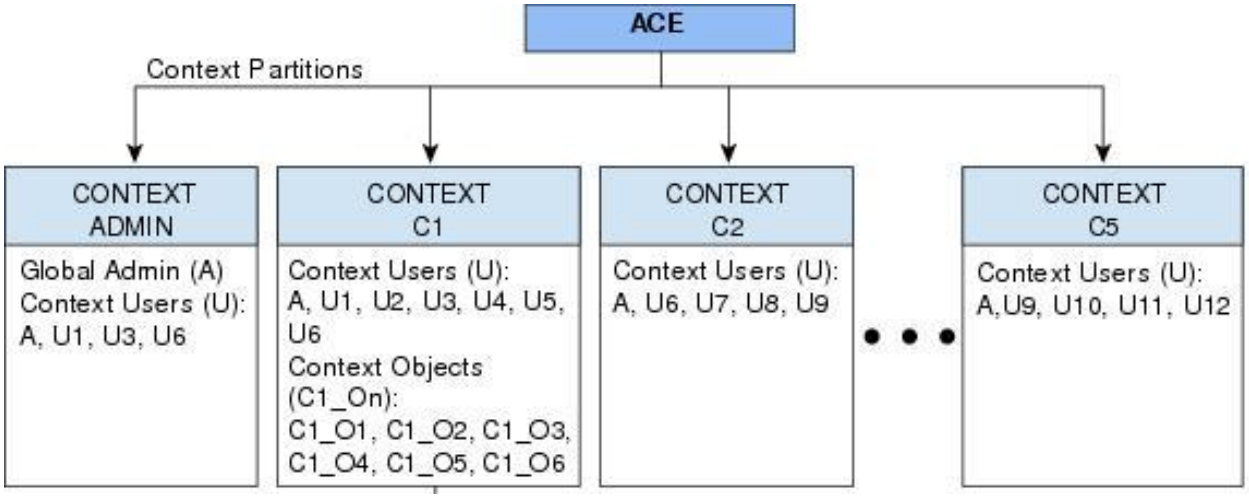
The following table lists the common / default ports used to configure each component on the Cisco ACE load balancer. Please refer to the two previous examples on using default ports vs. custom ports on the SLB.

Grid Control Service	OMS TCP Port	Probe	Stickiness	Farm	Virtual Server	Virtual Server Port
Secure Upload	1159	OracleGC_Upload_SSL	None	GC11g-SSL-Upload-Farm	vs_gcsu1159	1159
Agent Registration	4889	OracleGC_Upload_HTTP	Yes	GC11g-HTTP-Upload-Farm	vs_gcar4889	4889
Secure Console	7799	OracleGC_Upload_HTTP	Yes	GC11g-SSL-Upload-Farm	vs_gcsc7799	443
Unsecure Console	7788	OracleGC_Upload_SSL	Yes	GC11g-SSL-Upload-Farm	vs_ gcuc7788	7788

Before we begin to configure the Cisco ACE load balancer with specific Grid Control components, ensure that you are working with the Grid Control Context system. We will use the default "Admin" Virtual Context for the purpose of this paper, though you may wish to use a separately created Virtual Context to securely segment access and control, to assign resource allocations to the Virtual Context via Resource Class definitions, and simplify management by segmenting out the Grid Control load balancing services from other services being supported on the same Cisco ACE load balancer.

Create Resource Class

The virtualized environment is divided into objects called contexts. Each context behaves like an independent ACE appliance with its own policies, interfaces, domains, server farms, real servers, and administrators. Each context also has its own management VLAN that you can access using Telnet or Secure Shell (SSH). See illustration below.



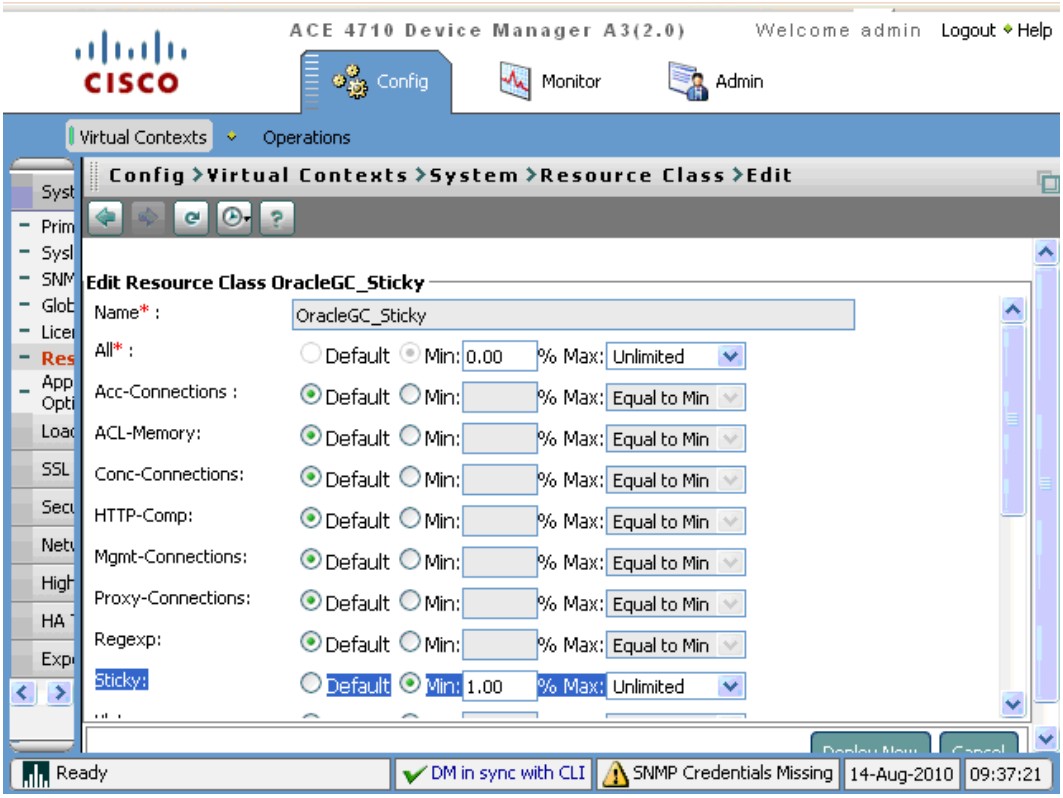
By default, when you create a context, the ACE associates the context with the default resource class. By means of resource class configuration it is possible to ensure that the services in each Virtual Context has the resources it needs while also ensuring it does not negatively impact other Virtual Contexts on the same physical ACE. The default resource class provides resources of a minimum of 0 and a maximum of unlimited for all resources except sticky entries. For stickiness to work properly, you must explicitly configure a minimum resource limit for sticky entries by using the **limit-resource** command. In this section, we will create this Resource Class from the UI. For more information on Cisco ACE virtualization, please see the Cisco online documentation:

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA3_1_0/configuration/virtualization/guide/config.html#wpmkr1053367

Navigate to the Virtual Contexts >> System >> Resource Class link and select Add. Name this Resource Class descriptively, i.e. OracleGC_Sticky.

Scroll down to “Sticky” field and select “Min” with value “1” then select Unlimited from the list of options for “Max” value.

Save this by clicking “Deploy” at the bottom of the screen.

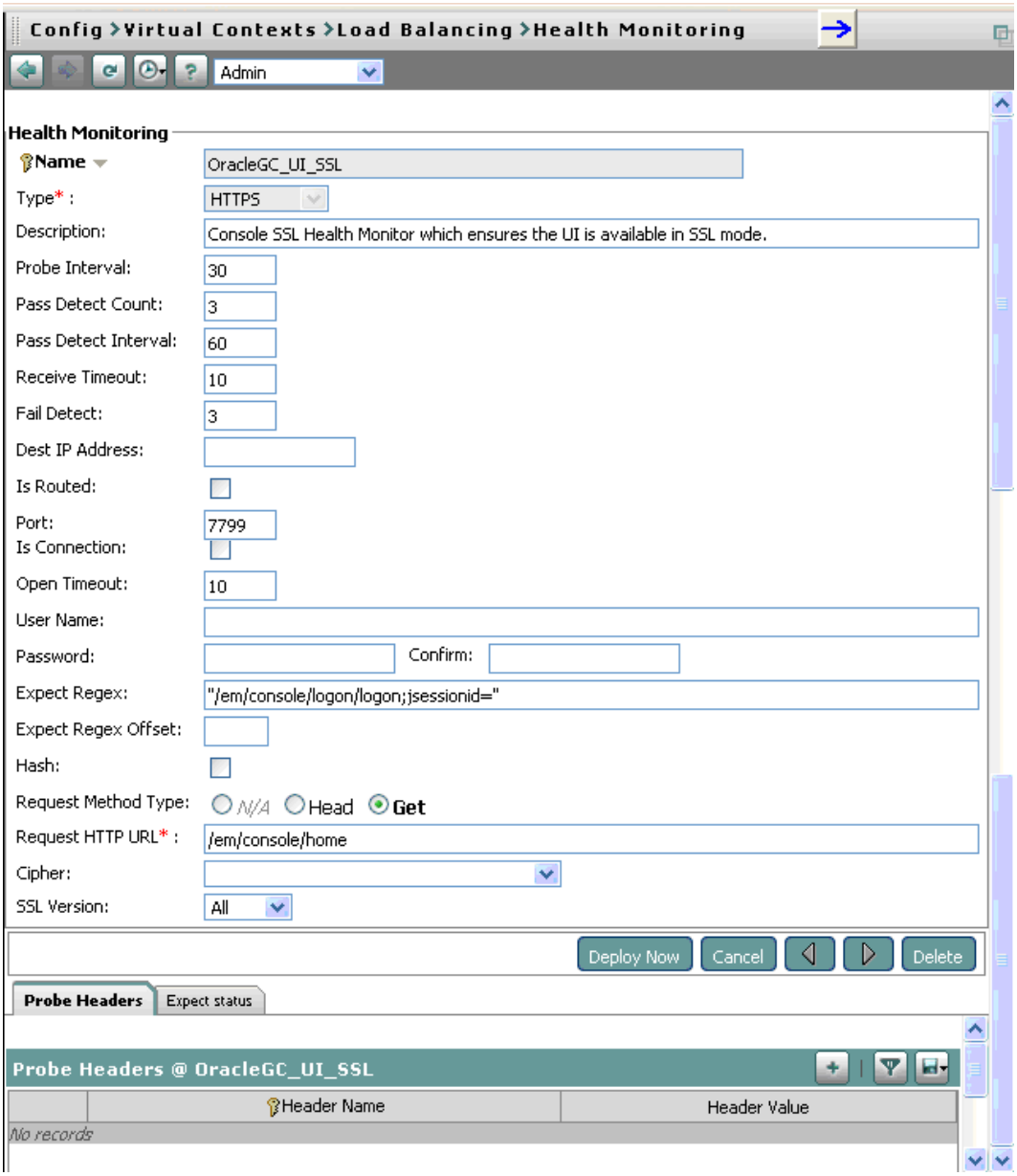


Create Probes

Probes are Health Monitors, which define tests that determine access and availability of each of back-end OMS service on each host periodically. A Probe is used by Virtual Servers to determine availability of Server Farm members for routing requests to available OMS’s. Probes in the ACE can be set to monitor all Server Farm members in the same way (set at the Server Farm level), or where necessary, to monitor individual Server Farm members (set at the individual Real Server level).

We need to “Probe” each service on each OMS host in the same way. Therefore, we need a total of four Probes which we will set at the Server Farm level. To do this we will first create the definition of these Probes and then configure them to apply to the appropriate Server Farm.

To create the first Probe, navigate to the Virtual Contexts >> Load Balancing >> Health Monitoring link and select Add. Name this Probe descriptively, i.e. OracleGC_UI_SSL.



Type >> **HTTPS**

Description: Describe the role of this Probe. For example “Console SSL Health Monitor which ensures the UI is available in SSL mode.”

Probe Interval: **30**. This is the interval that is used to check for this site’s availability. You want to make sure this meets your HA requirements for redirecting traffic away from an unavailable OMS.

Pass Detect Count: **3**

Pass Detect Interval: **60**

Receive Timeout: **10**

Fail Detect: **3**

Port: <enter your SSL UI port for your Grid Control servers>

Open Timeout: **10**

Expect Regex: **"/em/console/logon/logon;jsessionid="** This is the expected string the Probe is looking for in order to consider this OMS service "Available."

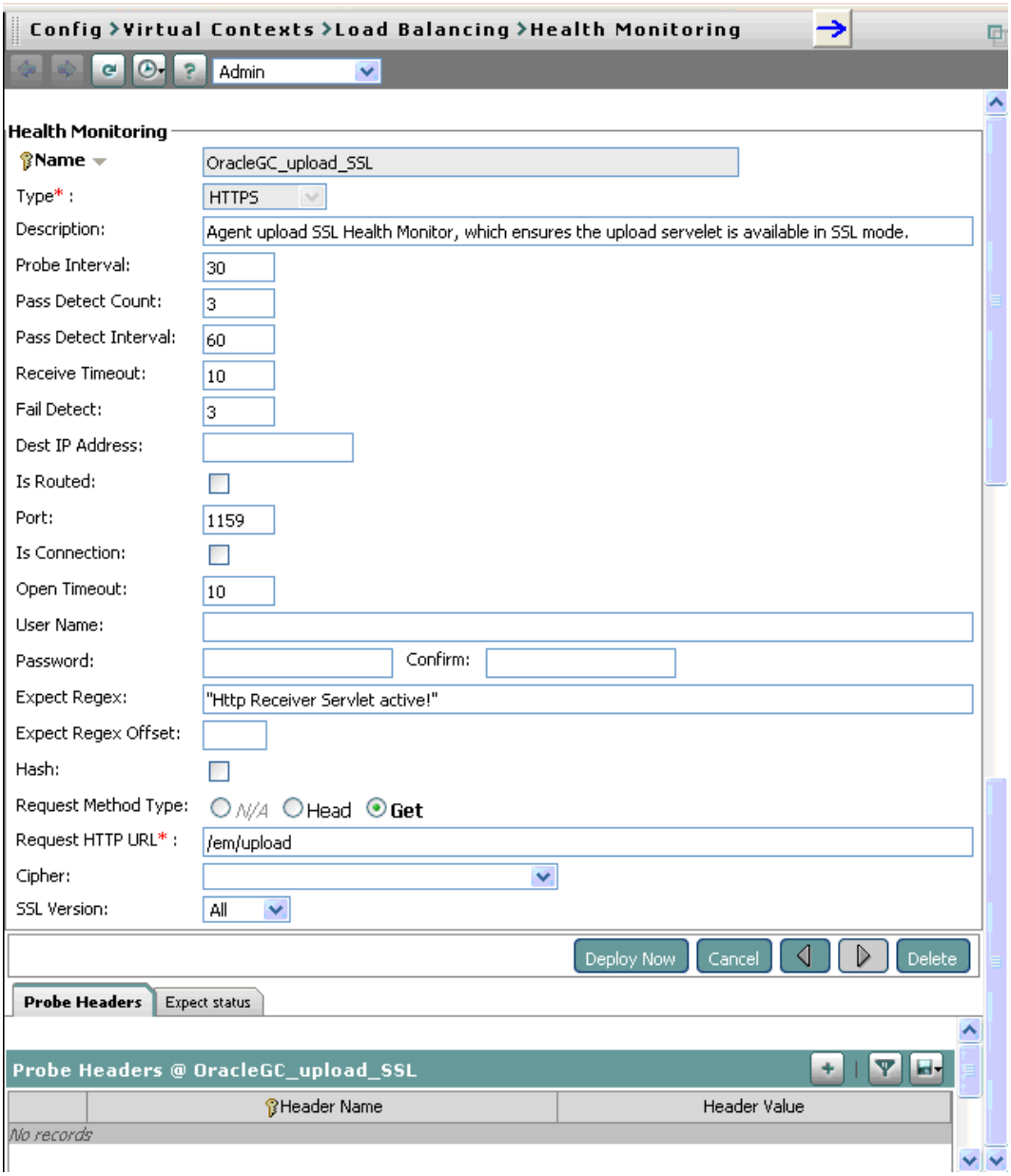
Request Method Type: **Get**

Request HTTP URL: "/em/console/home"

When finished, click "**Deploy Now**."

Next, we need to create a Probe for the agent upload HTTPS service.

While you're at the Health Monitoring summary screen, select Add again for the next Probe. Name this Probe descriptively, i.e. OracleGC_Upload_SSL.



Type >> **HTTPS**

Description: Describe the role of this Probe. For example “Agent upload SSL Health Monitor, which ensures the upload servlet is available in SSL mode.”

Probe Interval: **30** This is the interval that is used to check for this site’s availability. You want to make sure this meets your HA requirements for redirecting traffic away from an unavailable OMS.

Pass Detect Count: **3**

Pass Detect Interval: **60**

Receive Timeout: **10**

Fail Detect: **3**

Port: <enter your SSL UI port for your Grid Control servers>

Open Timeout: **10**.

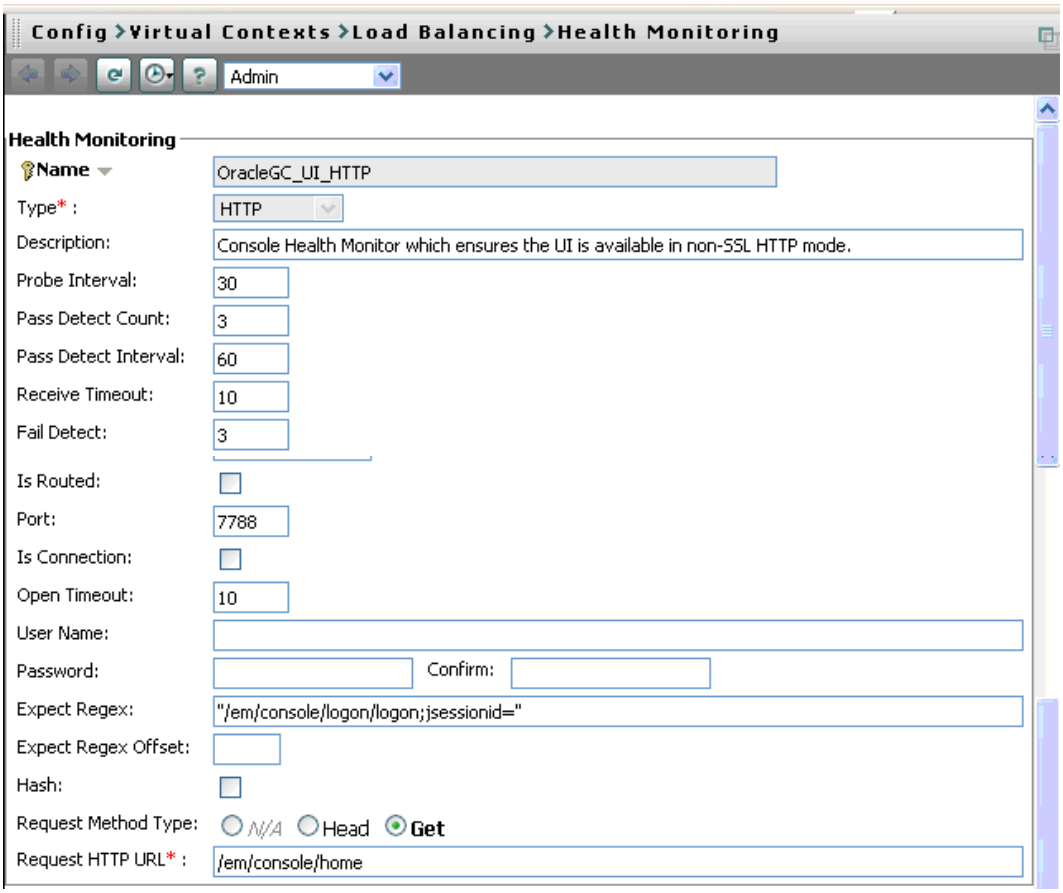
Expect Regex: **"Http Receiver Servlet active!"** This is the expected string the Probe is looking for in order to consider this OMS service “Available.”

Request Method Type: **Get**

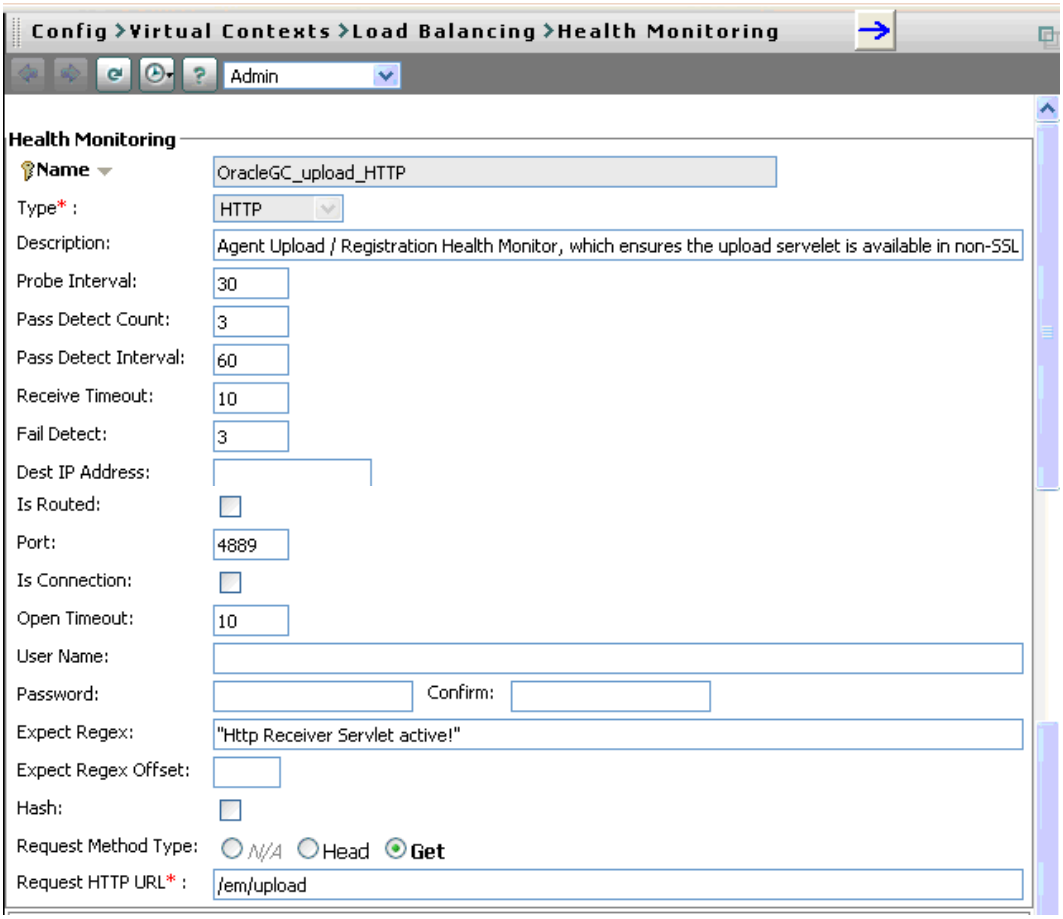
Request HTTP URL: **“/em/upload”**

When finished, click “**Deploy Now**.”

Repeat the same process above for HTTP UI Probe and agent HTTP Registration Probe.



The above screen shot shows the console HTTP Probe



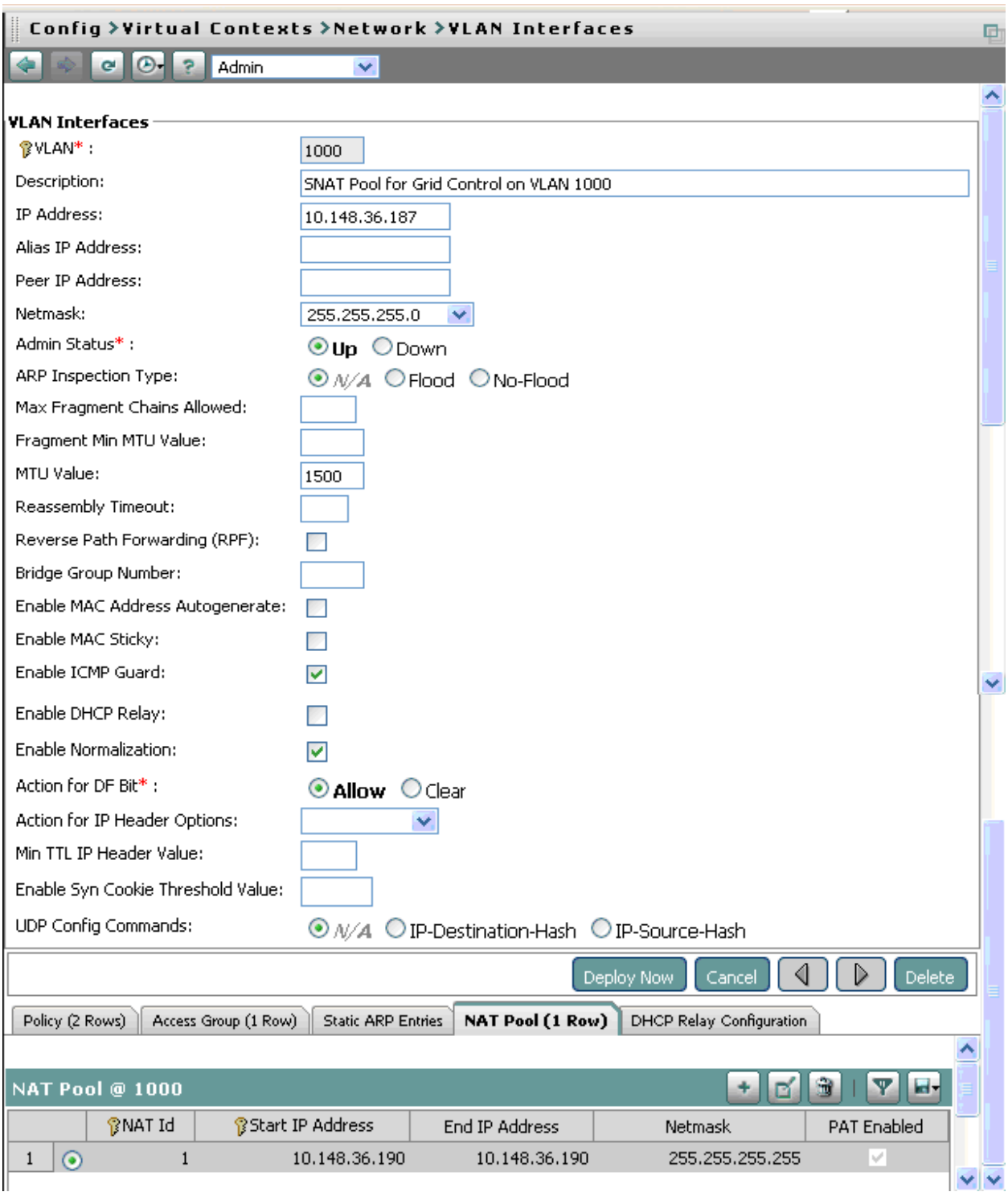
Your four Health Monitoring Probes are now defined and are available to be associated to Server Farms.

Configure SNAT Pool(s)

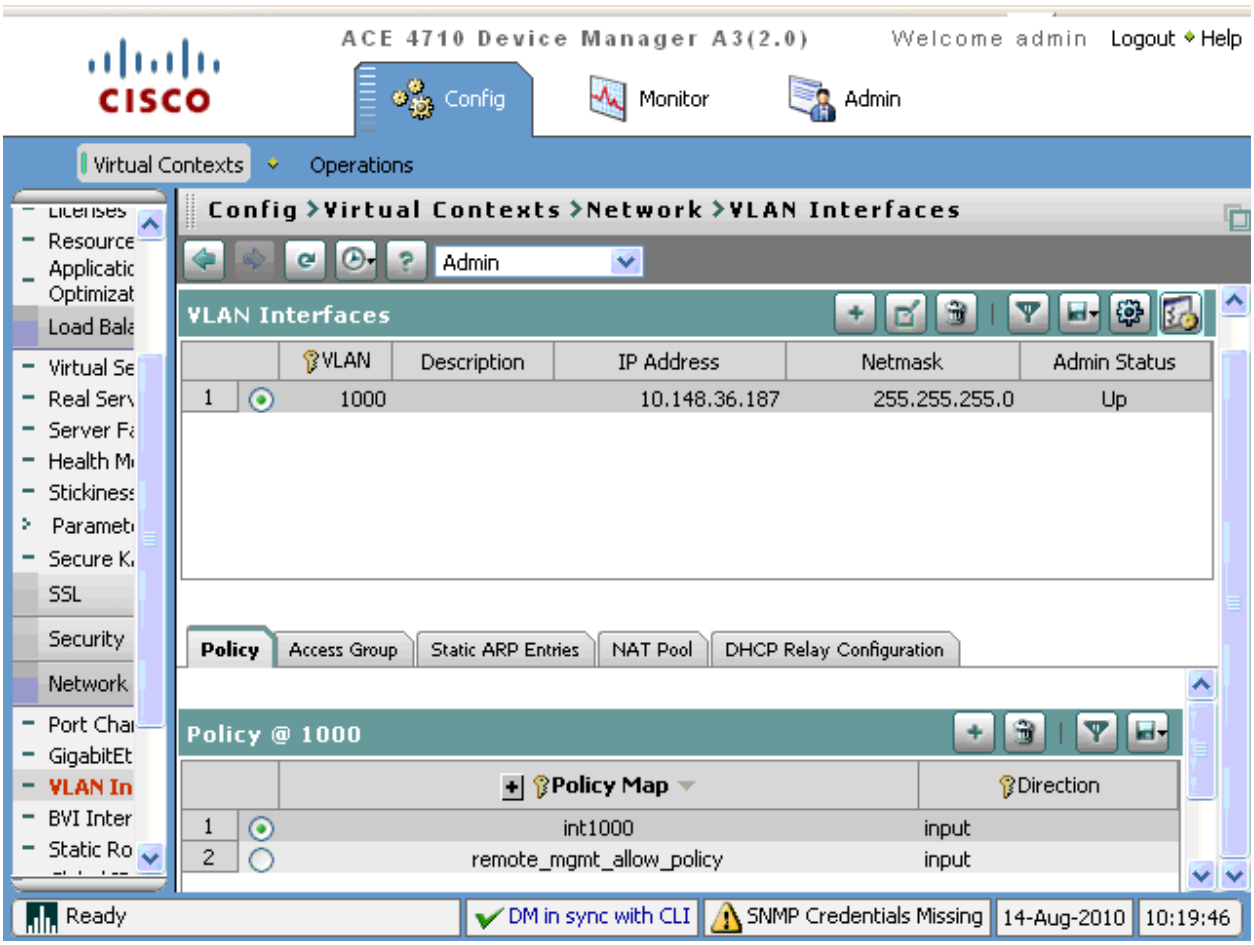
Support of Source Network Address Translation (SNAT) is a mandatory requirement for Grid Control setup through an SLB to prevent packet send/receive rejection by either end-points (source UI or agent vs. destination OMS host). It forces communications through the ACE from client to server in both directions. This is also known as One-Armed traffic routing. So before creation of the Virtual Servers, we need to ensure that we have a SNAT pool available. If this is not yet configured, you need an additional IP address on the ACE to configure this pool.

Navigate to the Virtual Contexts >> Network >> VLAN Interfaces >> and click Add. Provide the required fields as suggested by your Network team. Refer to the following example illustration for details. For additional guidance on this topic, please see the configuration examples in the document titled, *Basic Load Balancing Using One Arm Mode with Source NAT on the Cisco Application Control Engine Configuration Example* published on the docwiki for ACE at:

http://docwiki-dev.cisco.com/wiki/Basic_Load_Balancing_Using_One_Arm_Mode_with_Source_NAT_on_the_Cisco_Application_Control_Engine_Configuration_Example



When this is completed, you will see the (S)NAT Pool for VLAN 1000 listed as illustrated below.

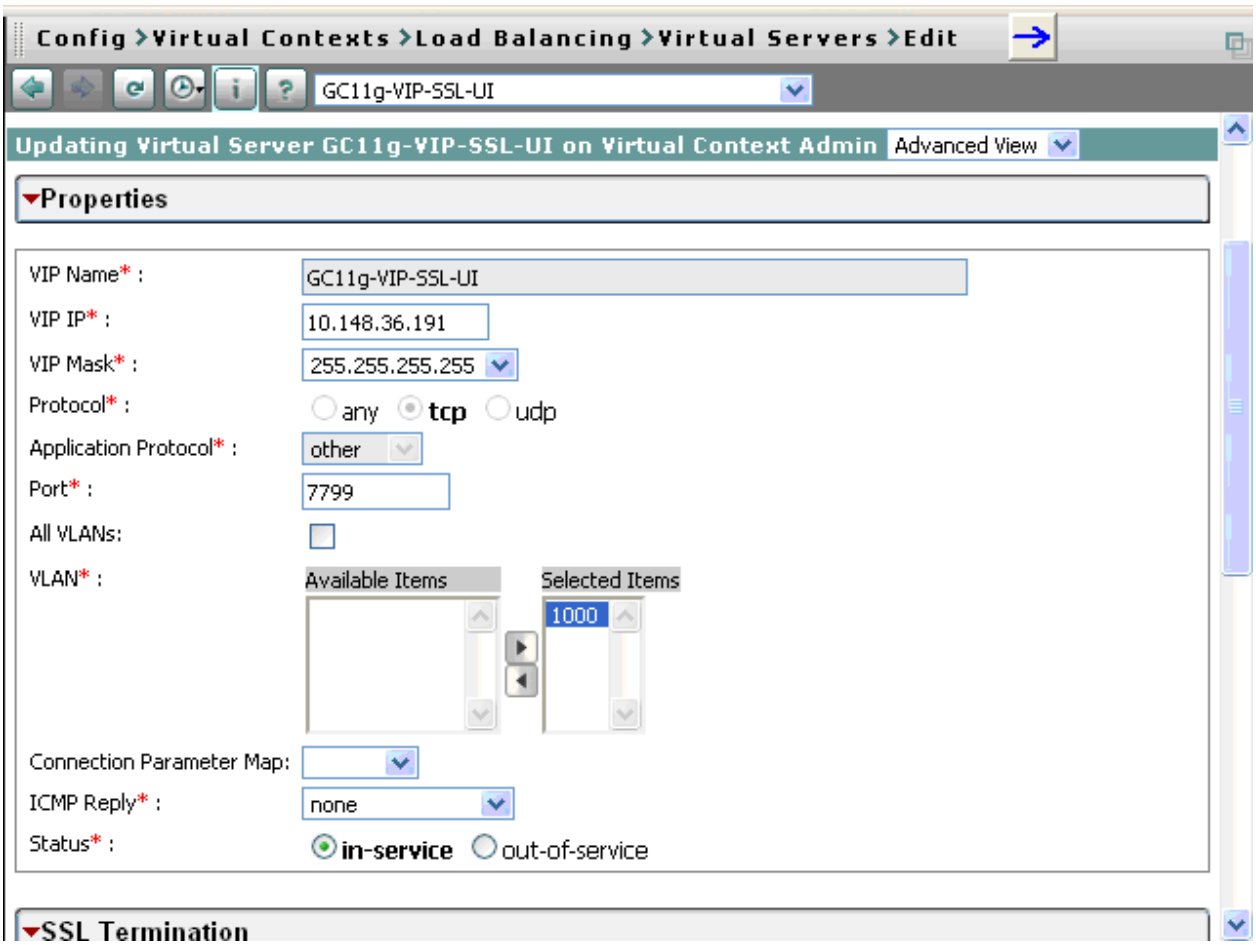


Now, we're ready for the final step in the SLB configuration.

Create Virtual Servers

Now, you are ready to create the four Virtual Servers (with their associated Virtual IP, or VIP addresses), which will represent your "OMS Alias" on the SLB.

Navigate to the Virtual Contexts >> Load Balancing >> Virtual Servers link and select Add. Select the Advanced view to see Advanced properties. Provide a name for this VIP, i.e. GC11g-VIP-SSL-UI.



VIP IP: <your VIP's IP address on the SLB>

VIP Mask: Select **255.255.255.255**. This will allow traffic on all subnets.

Protocol: **tcp**

Application Protocol: **Other**

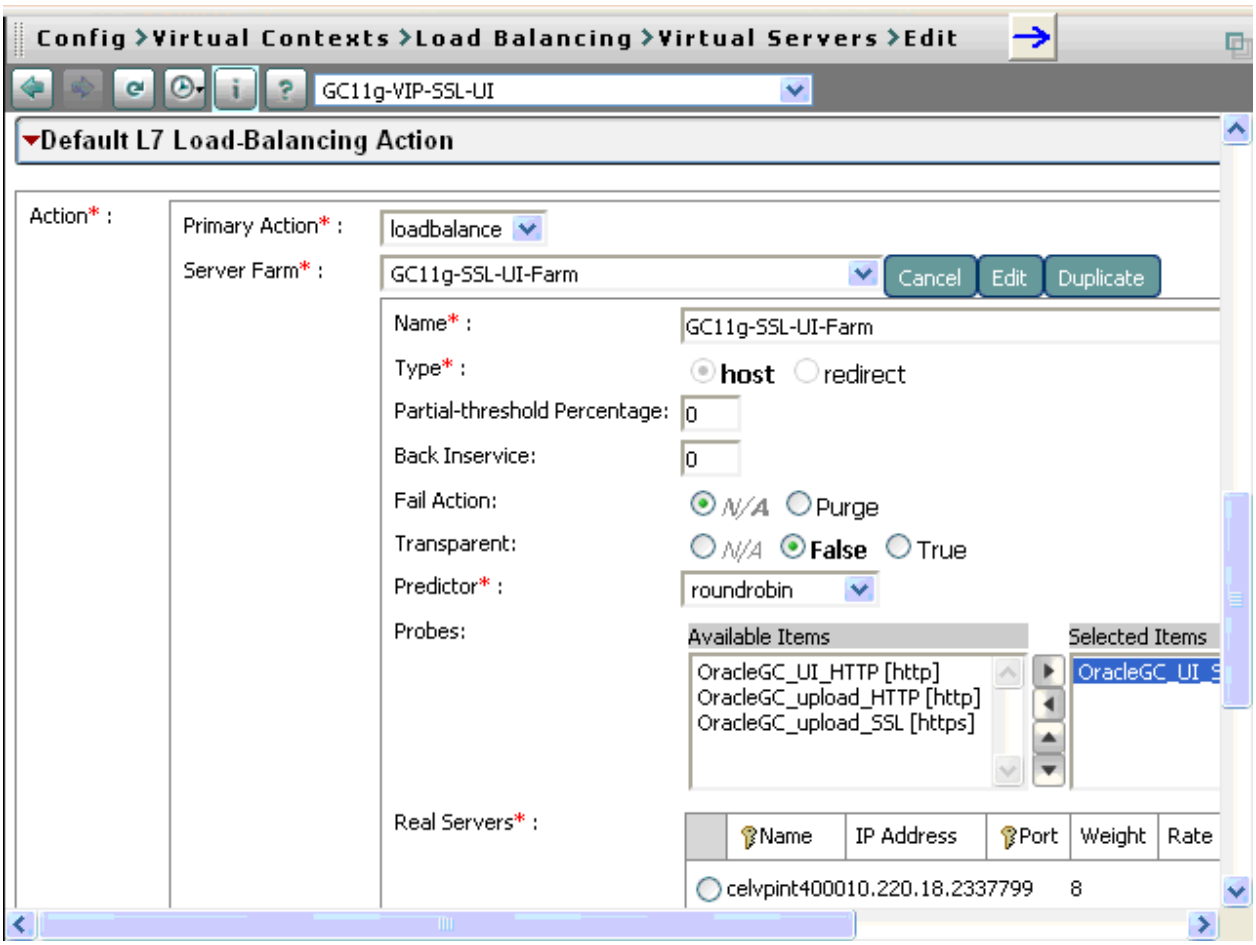
Port: <enter your SSL UI port you want to use in the browser UI>

VLAN: Select the VLAN you want to use for this VIP and move to the Selected Items list. In our example, our VLAN is **1000**

ICMP Reply: **none**

Status: **in-service**. This tells the ACE to activate this VIP for use once you apply the configuration.

In the next section of the Virtual Server screen - Default L7 Load-Balancing Action, define your Server Farm and other properties.



Click View then Add to enter each Server Farm member IP address and port etc., which are known of as Real Servers.

Primary Action: **loadbalance**

Server Farm: <the name of this server farm. i.e. GC11g-SSL-UI-Farm>.

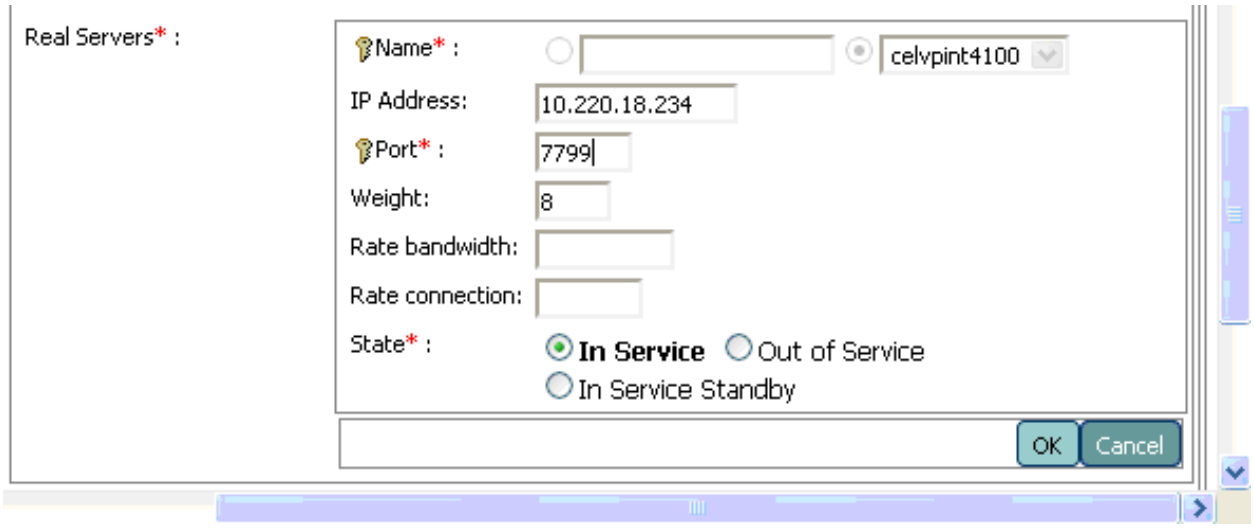
Type: **Host**.

Transparent: **False**.

Predictor: **roundrobin**

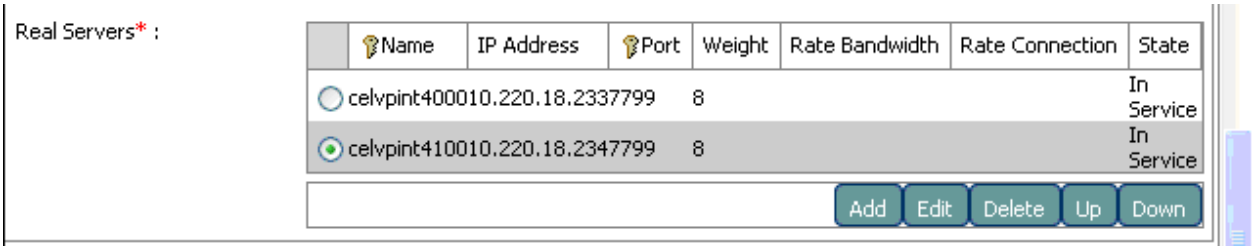
Probes: OracleGC_UI_SSL

Real Servers: add each OMS host IP address and Port and State:

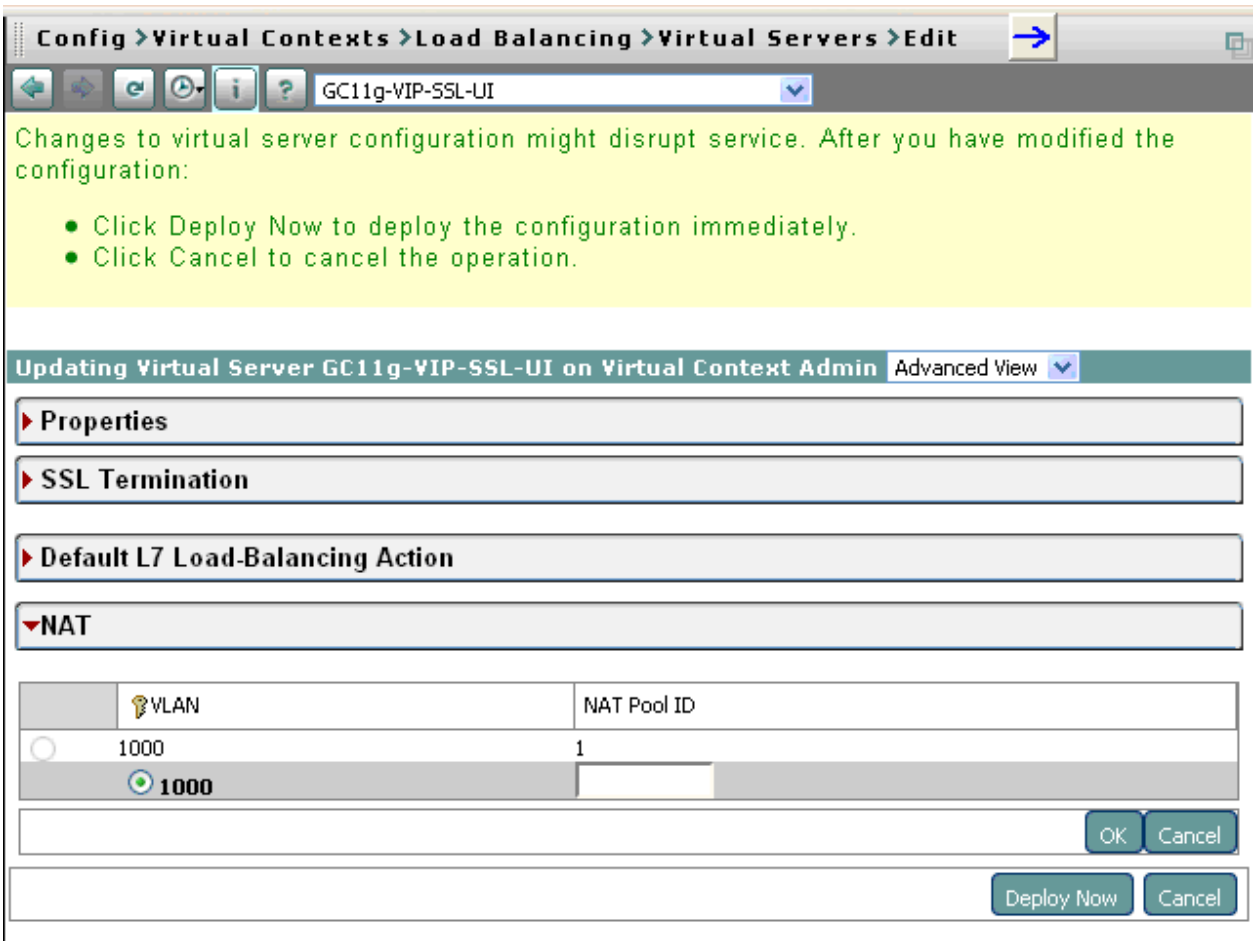


Click **OK** and add the next OMS the same way.

A list of all the Real Server members of the Server Farm will be shown at the bottom of this section.



Depending on how many NAT Pools are available to your specific VLAN on the ACE, you will need to specify an ID for NAT configuration to select the pool you have created for this service. Select an available VLAN and NAT Pool ID on the ACE device.



In this example, our VLAN name is 1000, with 4 NAT Pool ID's. Select any of the available four ID's.

Click "**Deploy Now"** when finished.

Create the next Virtual Server for Agent SSL Upload service the same way you did with this Virtual Server.

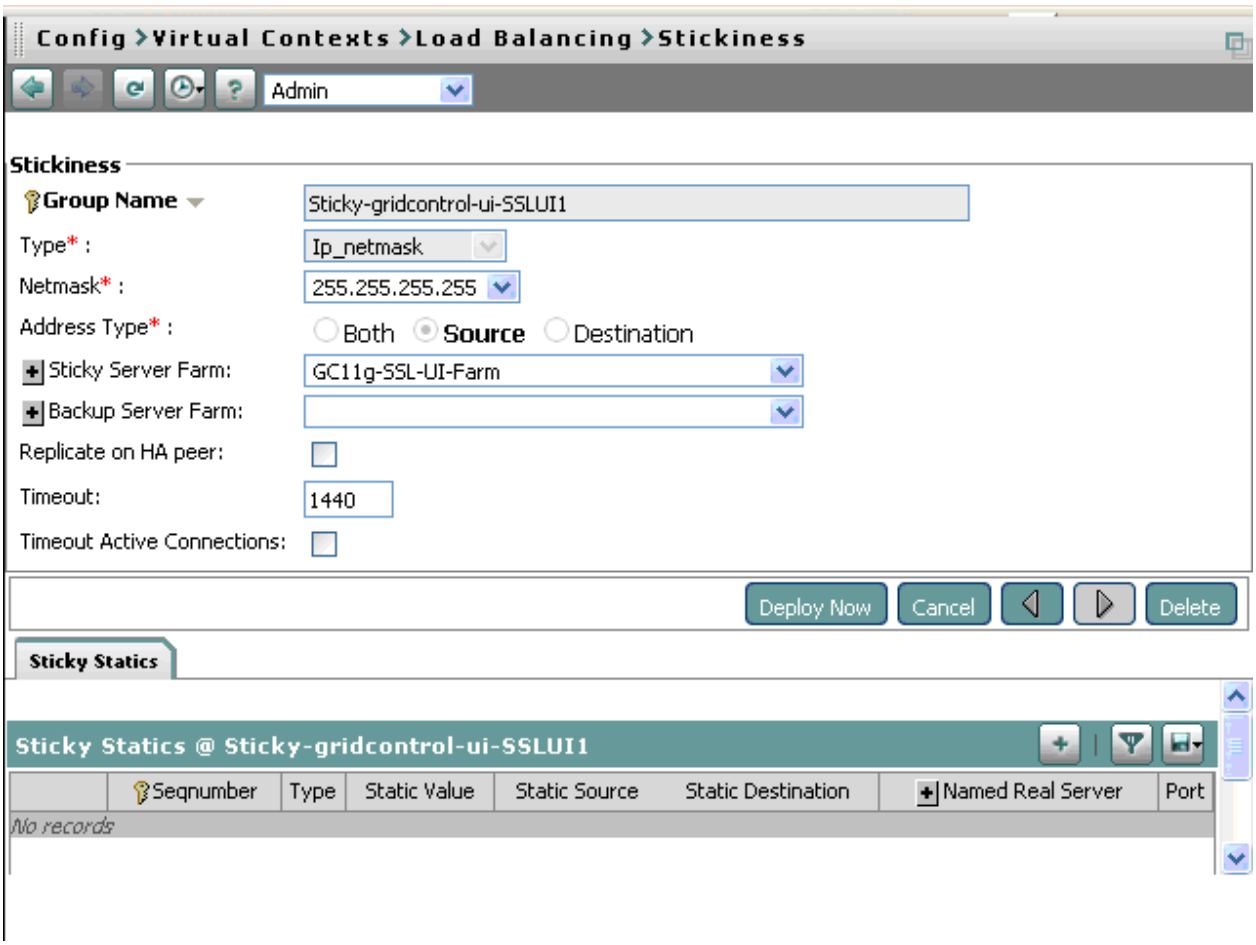
Enable Stickiness

At this time, we will enable Sticky rule for a couple of VIPs. Stickiness defines how the VIP will service incoming requests. Specifically, we need to keep a UI client connected to the same back-end Farm member to prevent a redirection to the login page every time the UI makes a subsequent request in the same session.

The agent upload services do not require Sticky rules since upload is performed in burst mode with no need for persistence. We will enable Stickiness for both UI Farms.

Navigate to Virtual Contexts >> Load Balancing >> Stickiness and click Add.

Fill in the required fields and select the Sticky Server Farm SSL UI.



Click "**Deploy Now"** to finish.

Repeat the same steps for the Sticky Server Farm non-SSL UI.

This completes the configuration of the ACE load balancer for the OMS services.

Section 3 Configuring Agents

One last step is needed to complete the implementation. To configure management agents (10.2.0.5 and higher) to point to the SLB instead of individual OMS hosts, simply run the following command and substitute your SLB service port for agent registration in URL:

emctl secure agent -emdWalletSrcUrl https://myslb.acme.com:4889/em

Conclusion

The steps documented in this white paper help you achieve the optimal high availability architecture for Oracle Enterprise Manager with Cisco ACE at the lowest cost and complexity. This allows you to concentrate more on managing the assets that support your critical business functions and at the same time meeting your business Service Level Agreements.

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

www.cisco.com

Tel: 408 526-4000

800 553-NETS (6387)

Fax: 408 527-0883

Oracle Corporation

500 Oracle Parkway

Redwood Shores, CA 94065

USA

www.oracle.com

General Inquiries: 1.800.ORACLE1

International: 1.650.506.7000