This guide focuses on defining the process for deploying Oracle Enterprise Manager with Citrix NetScaler.
Table of Contents

Introduction 3
Configuration 3
NetScaler features to be enabled 4
Steps for load balancing configuration 4
Solution Description 5
Quick Configuration Table 5
Configuring Load Balancing 7
Verification 11
Authentication 11
Configuring Optimization on NetScaler 12
HTTP Compression 12
Integrated Caching 14
Front End Optimization 18
Conclusion 20
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

For several years, Citrix has completed certifications and provided deployment guides for key enterprise applications. NetScaler’s rich application delivery capabilities significantly enhance the performance of these applications. With a comprehensive feature set, It provides availability, scalability, optimization and security for Oracle OEM deployments.

Introduction

This guide defines the process for deploying Oracle Enterprise Manager 12c with NetScaler. Citrix NetScaler is a world class application delivery controller, with the proven ability to load balance, accelerate, secure and optimize enterprise applications.

Oracle Enterprise Manager 12c is Oracle’s on-premises management platform, providing a single pane of glass for managing all of a customer’s Oracle deployments.

Configuration
Recommended Product Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Enterprise Manager</td>
<td>12c</td>
</tr>
<tr>
<td>NetScaler VPX</td>
<td>11.0 (Platinum License) – Load Balancing, Compression, Caching and FEO</td>
</tr>
<tr>
<td></td>
<td>11.0 (Standard License) – Only Load Balancing</td>
</tr>
</tbody>
</table>

NetScaler features

The following NetScaler features are discussed in this deployment guide.

- Load balancing
- SSL offload

Other considerations

- Make sure you have installed, at least one license on the NetScaler appliance.
- Set the time zone and a NTP (Network Time Protocol) server, and check the date and time on the NetScaler virtual appliance, as OEM Server server connections can be very sensitive to time differences.
- Configure your DNS settings properly: Note that for the purposes of certificate-based authentication, all addressable hosts that are part of the network setup should have resolvable domain names, not just IP addresses.
**Solution Description**

**Configuring Load Balancing**

A load balancing configuration consists of the definition of load balancing virtual servers (LB vServers), as well as services that are bound to the LB vservers. A service is simply a combination of a server and a protocol (e.g. HTTP, Port 80 or HTTPS, port 443).

**Step 1 - Define the load balancing virtual servers (LB vservers)**

Log into the NetScaler GUI. On the Configuration tab, navigate to Traffic Management>Load Balancing>Virtual Servers. For this deployment exercise, we are load balancing two Oracle OEM Server instances. The following load balancing virtual servers will be created as part of this configuration:

<table>
<thead>
<tr>
<th>Virtual Server Name</th>
<th>Details</th>
<th>Port</th>
<th>Protocol</th>
<th>Persistence</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_ccsc443</td>
<td>Secure Console</td>
<td>443</td>
<td>SSL</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_ccscbip5443</td>
<td>Secure BI Publisher</td>
<td>5443</td>
<td>SSL</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_ccuc80</td>
<td>Unsecure Console</td>
<td>80</td>
<td>HTTP</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_ccucbip8080</td>
<td>Unsecure BI Publisher</td>
<td>8080</td>
<td>HTTP</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_ccsu4900</td>
<td>Secure Upload</td>
<td>4900</td>
<td>SSL</td>
<td>NA</td>
</tr>
<tr>
<td>vs_ccar4889</td>
<td>Agent Registration</td>
<td>4889</td>
<td>HTTP</td>
<td>Cookie</td>
</tr>
<tr>
<td>vs_ccaom8081</td>
<td>Always-On Monitoring Secure Upload</td>
<td>8081</td>
<td>SSL</td>
<td>NA</td>
</tr>
</tbody>
</table>

When defining a new LB vserver, you will be presented with the settings screen.

(The steps shown here are for an SSL vserver. Follow the same steps to configure the HTTP vservers as well, only select port 80 as the port and HTTP as the protocol)
Load Balancing Virtual Server

After clicking OK, you will see the Basic Settings screen for the LB vserver. Here, you may change settings such as the session persistence method, authentication and load balancing methods. Set session persistence as per the table above and the load balancing method to LEASTCONNECTION for all virtual servers.

For more information on these features, please refer to https://docs.citrix.com/en-us/netscaler/11.html
To enable an SSL-based LB vserver, you should add an SSL certificate and key pair. For this, you may use either a self-signed certificate generated on the NetScaler appliance or a CA (Certificate Authority) signed one. The steps for generating a self-signed certificate on the NetScaler are as follows –

1. Login to your NetScaler appliance via the Configuration Utility.
2. Select Traffic Management > SSL
4. Here, the wizard will lead you through the series of steps for generating the self signed certificate –
   • Generate the private key
   • Generate the CSR (Certificate Signing Request)
   • Generate the Certificate (using the ns-root.cer NetScaler root certificate)
   • Save the Certificate and Key pair

Alternatively, if a certificate and key pair is already available, the same can be added by navigating to SSL>Certificates and clicking on the Add button. For more details refer to http://support.citrix.com/article/CTX109260

To improve site security and achieve an A/A+ rating on the SSLLabs.com evaluation, refer to https://www.citrix.com/blogs/2016/06/09/scoring-an-a-at-ssllabs-com-with-citrix-netscaler-2016-update/
Step 2 – Define LBVS server service group binding

Now click on the Load Balancing Virtual Server Service Binding tab in the Service and Service Groups section, or alternatively, click on Services in the Traffic Management>Load Balancing subsection and then, click on the Add button.

Every LB service is linked to a server; this can either be a new server or an existing server already defined in the Servers subsection under Load Balancing. Service groups extend this by allowing the creation of a group of services. An LB vserver can use a set of services or a service group.

Here, define the names for the services for each OEM server instance, the IP address (or choose from a list in the case of an existing server) for the OEM server instances and the protocol they operate on as per the table below:

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Details</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>vs_ccsc443</td>
<td>Secure Console</td>
<td>7802</td>
<td>SSL</td>
</tr>
<tr>
<td>vs_ccscbip5443</td>
<td>Secure BI Publisher</td>
<td>9803</td>
<td>SSL</td>
</tr>
<tr>
<td>vs_ccuc80</td>
<td>Unsecure Console</td>
<td>7788</td>
<td>HTTP</td>
</tr>
<tr>
<td>vs_ccucbip8080</td>
<td>Unsecure BI Publisher</td>
<td>9701</td>
<td>HTTP</td>
</tr>
<tr>
<td>vs_ccsu4900</td>
<td>Secure Upload</td>
<td>4903</td>
<td>SSL</td>
</tr>
<tr>
<td>vs_ccar4889</td>
<td>Agent Registration</td>
<td>3872</td>
<td>HTTP</td>
</tr>
<tr>
<td>vs_ccaom8081</td>
<td>Always-On Monitoring Secure Upload</td>
<td>8081</td>
<td>SSL</td>
</tr>
</tbody>
</table>

Recommended Best Practices:
- Name your server instances as per their role, not with the IP address (for example, the Oracle OEM servers can be named OEM1 and OEM2)
- As there will be multiple items linked to each application (LB vservers, services, policies among others), it is recommended that they be named appropriately for convenience. This will make using tools such as grep with the CLI a lot easier.
Step 3 – Define Monitors

After defining services, the following monitors should be defined and bound to the appropriate services –

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Details</th>
<th>Type</th>
<th>Interval</th>
<th>Timeout</th>
<th>Monitor Expression</th>
<th>Receive String</th>
</tr>
</thead>
</table>
| mon_ccsc     | Secure Console | https | 5        | 16      | GET /em/consoleStatus.jsp HTTP/1.1

Host:

Connection: Close

Enterprise Manager Console is UP |
| mon_ccscbip  | Secure BI Publisher | https | 5        | 15      | GET /empbs/genwallet

GenWallet Servlet activated |
| mon_ccuc     | Unsecure Console  | https | 5        | 16      | GET /em/consoleStatus.jsp HTTP/1.1

Host:

Connection: Close

And now... Some Services |
| mon_ccucbip  | Unsecure BI Publisher | http  | 5        | 16      | GET /em/consoleStatus.jsp HTTP/1.1

Host:

Connection: Close

Enterprise Manager Console is UP |
| mon_ccsu     | Secure Upload     | http  | 5        | 16      | GET /empbs/genwallet

GenWallet Servlet activated |
| mon_ccar     | Agent Registration| http  | 5        | 16      | GET /xmlpserver/services HTTP/1.1

Host:

Connection: Close

And now... Some Services |
| mon_ccaom    | Always-On Monitoring | Secure Upload | 60    | 181      | GET /empbs/upload

Http Receiver Servlet active!
You should enable Health Monitoring if you would like to have NetScaler poll the server periodically to verify its health – it is recommended that this setting should not be disabled except for diagnostic purposes. This and additional settings can be accessed by clicking on the More dropdown (as shown above). If Health Monitoring is disabled, the appliance shows the server UP at all times. Bind these service groups to the appropriate LB vservers and confirm that they have been bound correctly by checking the same in the LB vserver Basic Settings screen. Add all the OEM Server servers to be load balanced and bind them to the load balancing virtual server.

Load Balancing Virtual Server

<table>
<thead>
<tr>
<th>Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>State</td>
</tr>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Traffic Domain</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Services and Service Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 Load Balancing Virtual Server Service Bindings</td>
</tr>
<tr>
<td>No Load Balancing Virtual Server ServiceGroup Binding</td>
</tr>
</tbody>
</table>

Finally, the LB vservers created will be displayed on the configuration screen to the right in the same screen that is obtained by accessing Traffic Management>Load Balancing>Virtual Servers.

This completes the load balancing configuration for Oracle Enterprise Manager.
Verification

The functioning solution can be verified with a default OEM Server installation by navigating to https://<FQDN of LB vserver>:443. This will show the Oracle Enterprise Manager Secure Console login screen.
Conclusion
NetScaler enables highly available Oracle Enterprise Manager deployments with its load balancing capabilities, allowing all the various management services provided by OEM to be load balanced and monitored.

With NetScaler, enterprises can not only enable high availability for their Oracle Enterprise Manager environments, but also extend capabilities for security and optimized access. The policy engine used by NetScaler enables enterprises to deploy any specific use cases that they may require, making the NetScaler solution a flexible and robust one that can meet all enterprise requirements.

To learn more about how NetScaler can bring these benefits to Oracle Enterprise Manager installations or address other application delivery requirements, please visit http://www.citrix.com.