Deploying Oracle Identity Management with NetScaler

This guide focuses on defining the process for deploying Oracle Identity Management with Citrix NetScaler.
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 IDM deployments.

**Introduction**

This guide defines the process for deploying Oracle IDM/OAM Server 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 Identity Management (OIM) is a software suite from Oracle providing identity and access management (IAM) technologies. One of its key components is Oracle Access Manager, a strategic solution for access management and web single sign-on. Here, we will load balance Oracle IDM and the backend OID (Oracle Internet Directory) servers for enabling high availability for applications using the Oracle IDM suite for authentication and authorization.

**Configuration**
Recommended Product Versions

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle IDM Server</td>
<td>12.2</td>
</tr>
<tr>
<td>NetScaler VPX</td>
<td>11.0 Standard/Enterprise/Platinum</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 a minimum, 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 IDM 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 vserver. 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 IDM 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_idm_lb</td>
<td>IDM Load Balancer</td>
<td>1521</td>
<td>TCP</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_idm_ldap</td>
<td>IDM LDAP</td>
<td>3060</td>
<td>TCP</td>
<td>Source IP</td>
</tr>
<tr>
<td>vs_idm_ldaps</td>
<td>IDM LDAPS</td>
<td>3131</td>
<td>TCP</td>
<td>Source IP</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 TCP vservers defined here, only select the appropriate port and TCP as the protocol)
Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type, public IP address. If the application is accessible only from the local area network (LAN) address.

You can configure multiple virtual servers to receive client requests, thereby increasing...

Name*  
vs_idm_lb

Protocol*  
SSL

IP Address Type*  
IP Address

IP Address*  
10.105.157.199

Port*  
443

More

OK  Cancel

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

Load Balancing Virtual Server

Basic Settings

Name  vs_idm_lb
Protocol  SSL
State  @DOWN
IP Address  10.105.157.199
Port  443
Traffic Domain  0

Listen Priority  -
Redirect Expression  -
Redirection Mode  -
SSL State  -
AppFlow Logging  -
Redirect From Port  -
HTTPS Redirect URL  -

Services and Service Groups

2 Load Balancing Virtual Server Service Bindings

No Load Balancing Virtual Server ServiceGroup Binding
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 SSL Labs.com evaluation, refer to https://www.citrix.com/blogs/2016/06/09/scoring-an-a-at-ssl-labs-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 IDM server instance, the IP address (or choose from a list in the case of an existing server) for the IDM 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>srv_idm_lb</td>
<td>IDM Load Balancer</td>
<td>1521</td>
<td>TCP</td>
</tr>
<tr>
<td>srv_idm_ldap</td>
<td>IDM LDAP</td>
<td>3060</td>
<td>TCP</td>
</tr>
<tr>
<td>srv_idm_ldaps</td>
<td>IDM LDAPS</td>
<td>3131</td>
<td>TCP</td>
</tr>
</tbody>
</table>

Recommended Best Practices:

- Name your server instances as per their role, not with the IP address (for example, the Oracle IDM servers can be named IDM1 and IDM2)
- 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.
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 IDM Server servers to be load balanced and bind them to the load balancing virtual server.

<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 Service Group 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 Identity Management.
Verification

The functioning solution can be verified with a default IDM Server installation by navigating to https://<FQDN of LB vserver>:1521. This will show the Oracle Identity Management login screen.
Conclusion
NetScaler enables highly available Oracle Identity Management deployments with its load balancing capabilities, allowing all the various management services provided by IDM to be load balanced and monitored.

With NetScaler, enterprises can not only enable high availability for their Oracle Identity Management 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 Identity Management installations or address other application delivery requirements, please visit http://www.citrix.com.