ORACLE

Load Balancer

Level 200

Changbin Gong
Oracle Cloud Infrastructure
September, 2019

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Objectives

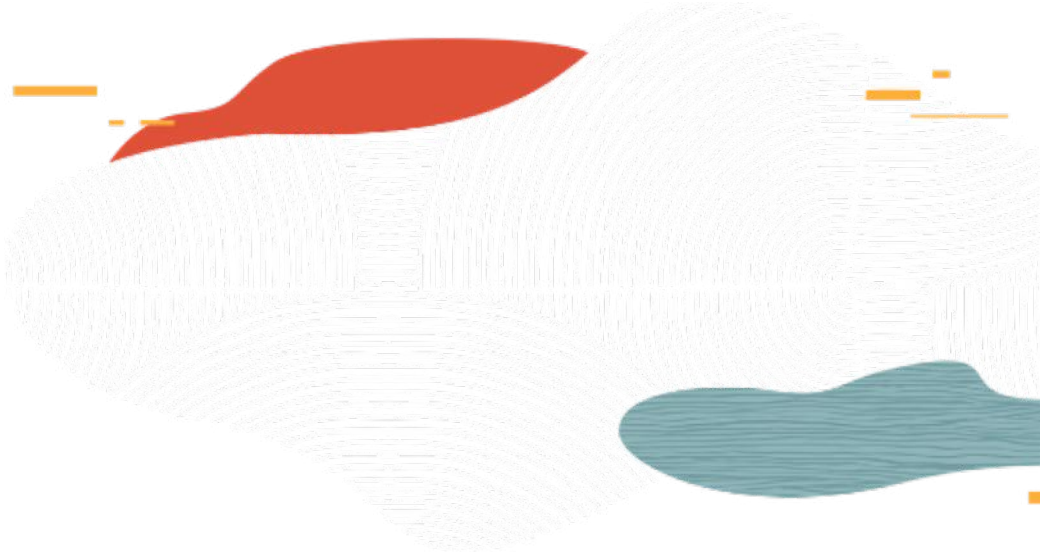
After completing this lesson, you should be able to:

- Learn more about OCI LB SSL Support
- Discuss advanced topics, including Session Persistence and Path Based Routing
- Monitoring Metrics
- Troubleshooting Guidelines

Recap: OCI Load Balancing Service

- Load Balancer as-a-service, provides scale and HA
- Public and Private Load Balancer options
- Public Load Balancer service is regional in scope and requires 2 Availability Domains
- Supported Protocols – TCP, HTTP/1.0, HTTP/1.1, HTTP/2, WebSocket
- Supports SSL Termination, End-to-End SSL, SSL Tunneling
- Supports advanced features such as session persistence and content based routing
- Key differentiators
  - Private or Public Load Balancer (with Public IP address)
  - Provisioned bandwidth – 100 Mbps, 400 Mbps, 8 Gbps
  - Single load balancer for TCP (layer 4) and HTTP (layer 7) traffic

ORACLE



Part I: Session Persistence

Session Persistence

Session persistence – set of strategies that direct any number of requests, originating from a single logical client, to a single backend web server

If your backend servers perform significant caching to enable some features (e.g. login sessions, shopping carts), or to improve performance by not overloading backing systems, LBs might need or benefit from session persistence

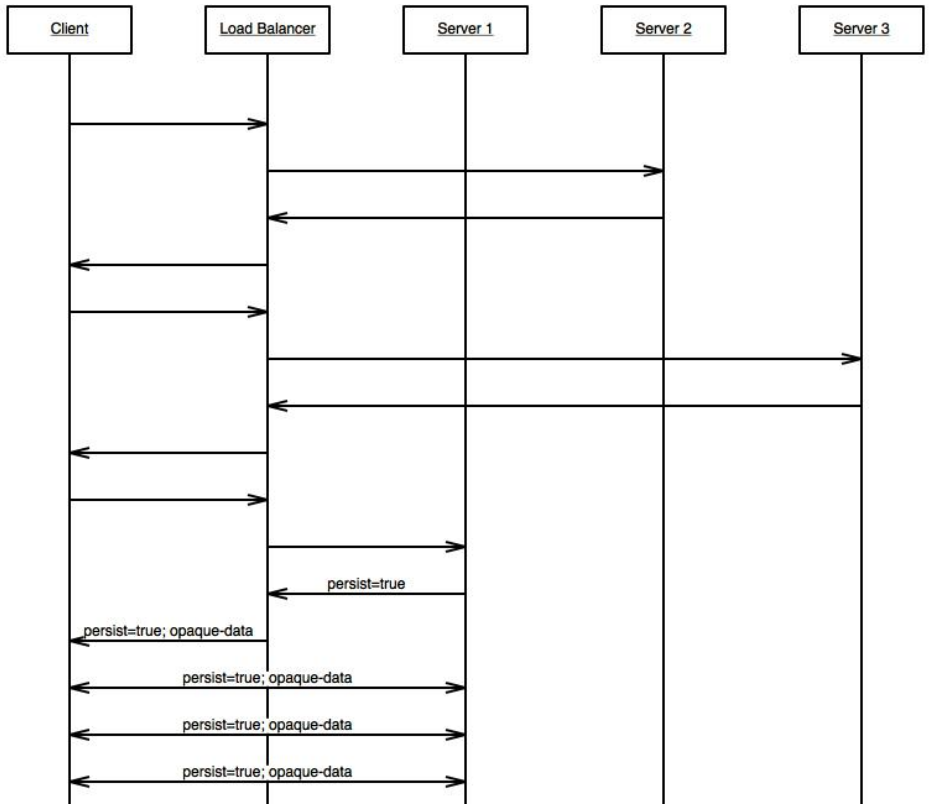
OCI LB Service supports session persistence, specifically **server side, cookie driven** session persistence (LB must be in HTTP mode)

Session persistence is not enabled for clients that do not accept cookies

Session Persistence

Session persistence is a feature that can be configured and enabled on the level of a backend set. For each backend set, two parameters are set to control it:

- Cookie name: the name of a cookie, or a match-all pattern, that will be set in the response from the backend server to request session persistence
- Fallback: a boolean value that controls how OCI LB handles session persisted requests in case the original backing server isn't available



- Activated when a server sends a Set-Cookie response header with the cookie name matching the one in the Cookie name parameter, or if the server sends any cookie (match-all pattern)
- In both cases, OCI LB will create a new cookie that is sent to the client. This is used in the future requests to correctly route the request to the session persisted backend server
- Until one of the backend servers activates session persistence, OCI LB uses the already configured load balancing mechanism (round-robin, least open connections, etc...)

Session Persistence

- What happens when my backend server becomes unavailable?
  - The fallback parameter controls whether OCI LB is permitted to redirect the session to a different server in case the original backend server becomes unavailable
  - If its value is set to true, OCI LB picks a different server from the backend set, and redirects the session to it. If the value is set to false, the LB will fail the request with an HTTP code 502
- How do I stop persisting a session?
  - Your backend server needs to delete the cookie configured by Cookie name parameter, or all cookies if you used the match-all pattern
  - The typical approach for deleting cookies is to resend them (by sending a Set-Cookie response header), with an expiration date in the past
  - The next request received by the OCI LB will follow the load balancing mechanism configured (round-robin, least open connections, etc...)

ORACLE

Part II: Request Routing

Request Routing (Virtual Hostnames & Path Routing)

Request routing feature allows users to route traffic based on certain request parameters

- Hostname (HTTP requests) – **Virtual Hostnames**
- The HTTP(s) request's path – **Path Routing**

The virtual hostnames feature supports HTTP and HTTPS listeners only, but does not support TCP listeners.

Virtual Hostnames

You can assign virtual hostnames to any ***OCI LB Listener***. Each hostname can correspond to an application served from your backend.

Enterprises use a single LB to host multiple apps, each app identified by hostname. Advantages include

- Single associated IP address - this makes the process of network-ACL configuration simpler
- Single bandwidth/shape - Multiplexing many apps in a single shape/size provides customers with the flexibility of better managing the aggregate bandwidth demands. Also improves overall utilization
- Shared backend set definition - administrative simplification of managing the set of backends under a single resource
- Without virtual hostnames, customers have to instantiate different LBs for each application. This would lead to administrative pain points related to IP address management, Network/ACL configuration

Virtual Hostnames

- LB service supports 3 matching variants for virtual hosts hostname in order:
  - exact matching (e.g. app.example.com)
  - longest wildcard starting with asterisk (*.example.com)
  - longest wildcard ending with asterisk (app.example.*)
- The virtual hostnames feature supports HTTP & HTTPS listeners, but not TCP listeners
- If a listener has no virtual hostname specified, that listener is the default for the assigned port
- Don't support regular expression matching

Path Routing

- Various apps have multiple end-points or content-types reflected by distinct path (for e.g. "/admin", "/data" or "/video", or "/cgi"), and requests for each of these endpoints need to be routed to different backend sets
- W/o path based routing, different end-points would need to be represented by different port numbers. If customer wants to differentiate traffic between two backend sets, their options :
  - different listeners for each backend set -- which requires a different port for each listener or
  - different load balancers for each set of traffic
  - Neither of these workarounds are suitable as they require clients to hit different endpoints: either a different port or a different load balancer altogether
- A path route is a string that the LB matches against an incoming URI to determine the appropriate destination backend set

Path Routing

- A *path route rule* consists of a path route string and a pattern match type.
- Pattern match types include:
  - **EXACT MATCH** – Looks for a path string that exactly matches the incoming URI path.

    ^<path_string>$
  - **FORCE_LONGEST_PREFIX_MATCH** – Looks for the path string with the best, longest match of the beginning portion of the incoming URI path.

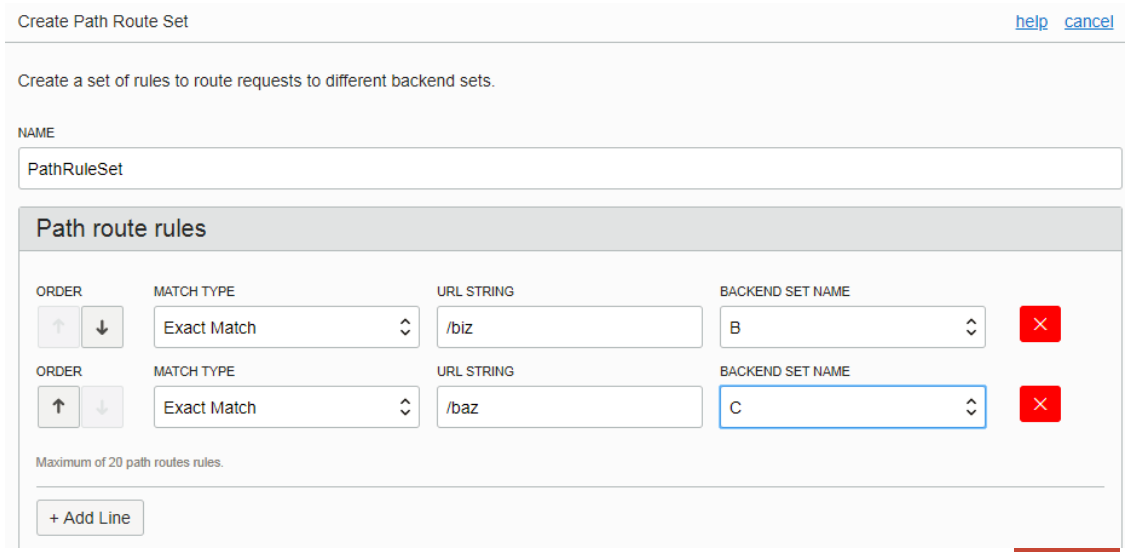
    <path_string>.*
  - **PREFIX_MATCH** – Looks for a path string that matches the beginning portion of the incoming URI path.

    ^<path_string>.*
  - **SUFFIX_MATCH** – Looks for a path string that matches the ending portion of the incoming URI path.

    .*<path_string>$
- Path route rules apply only to HTTP and HTTPS requests and have no effect on TCP requests.
- You can specify up to 20 path route rules per path route set.
- You can have one path route set per listener.

Path Routing

- Path based routing priority
  - EXACT_MATCH
  - FORCE_LONGEST_PREFIX_MATCH
  - PREFIX_MATCH or SUFFIX_MATCH
- The ***order*** of the rules within the path route set does not matter for EXACT_MATCH and FORCE_LONGEST_PREFIX_MATCH.
- If matching cascades down to prefix or suffix matching, the ***order*** of the rules within the path route set DOES matter.



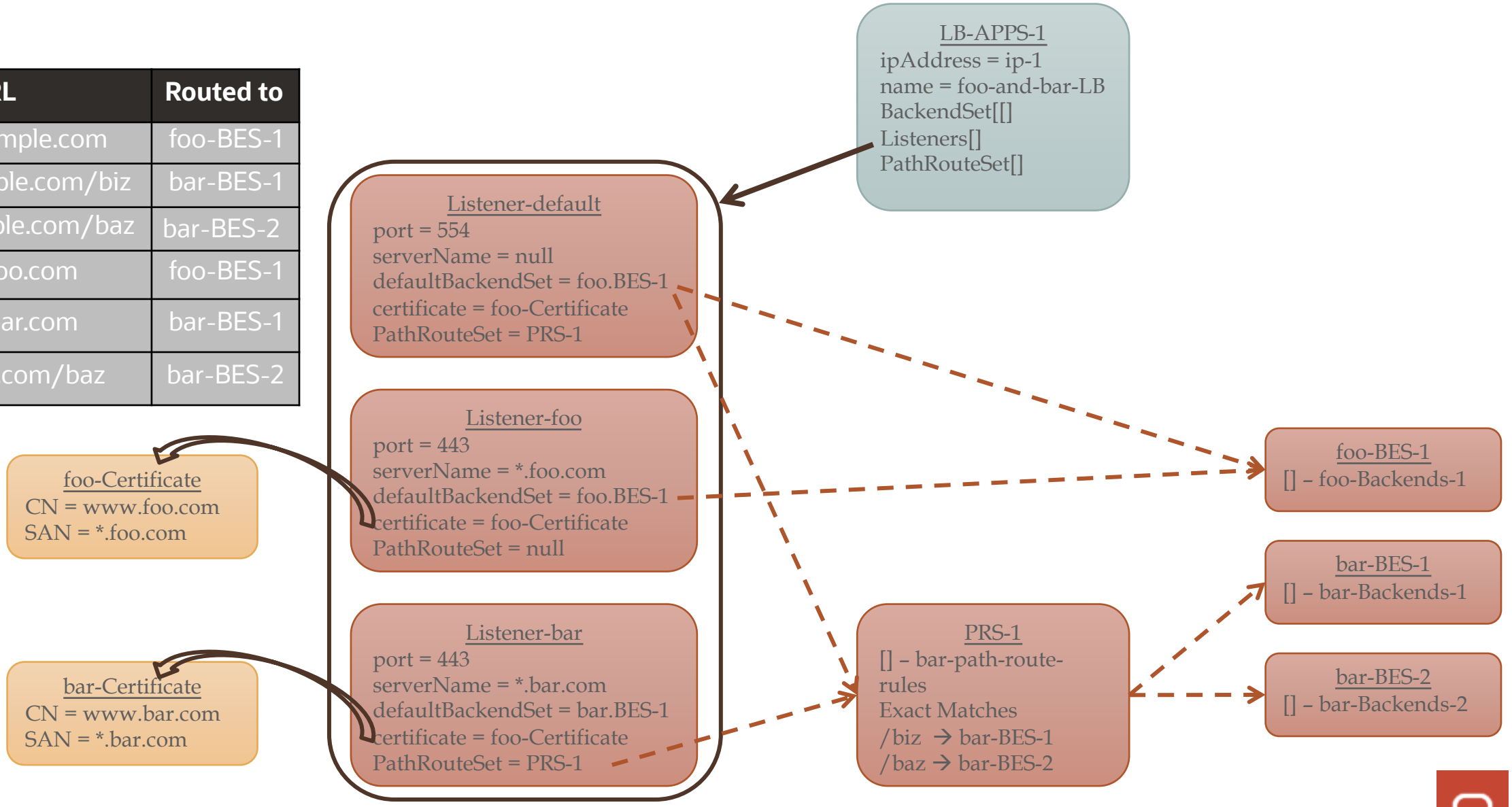
Virtual Hostname and Path Routing

- Both of these features route requests to backend sets. Hostname/DNS based virtual hosts has higher priority than URI based route.
- LB supports per-virtual host URI routes. Assume a single listener and three backend sets, A, B, and C. Default backend set is A.
- Virtual host rules:
  - foo.com -> backend set B
  - bar.com -> backend set C
- URI routes:
  - /biz -> backend set B (exact match)
  - /baz -> backend set C (exact match)

URL	Routed to
http://example.com	A
http://example.com/biz	B
http://example.com/baz	C
http://foo.com	B
http://foo.com/biz	B
http://foo.com/baz	C
http://bar.com	C
http://bar.com/biz	B
http://bar.com/baz	C

Virtual Hostnames and Path Routes

URL	Routed to
http://example.com	foo-BES-1
http://example.com/biz	bar-BES-1
http://example.com/baz	bar-BES-2
http://foo.com	foo-BES-1
http://bar.com	bar-BES-1
http://bar.com/baz	bar-BES-2



ORACLE

Part III: SSL Handling

SSL Handling

SSL Termination – SSL is terminate at LB. LB can accept encrypted traffic from a client; no encryption of traffic between LB and backend servers

SSL Tunneling – SSL implemented between LB and backend servers

End to end SSL – LB can accept SSL encrypted traffic from clients and encrypts traffic to the backend servers

To use SSL with your load balancer, you must add one or more certificate bundles to your system.

The certificate bundle you upload includes the public certificate, the corresponding private key, and any associated Certificate Authority (CA) certificates.

Oracle Cloud Infrastructure accepts x.509 type certificates in PEM format only.

Concepts

In cryptography, X.509 is a standard that defines the format of public key certificates

X.509 certificates are used in many protocols, including TLS/SSL, which is the basis for HTTPS

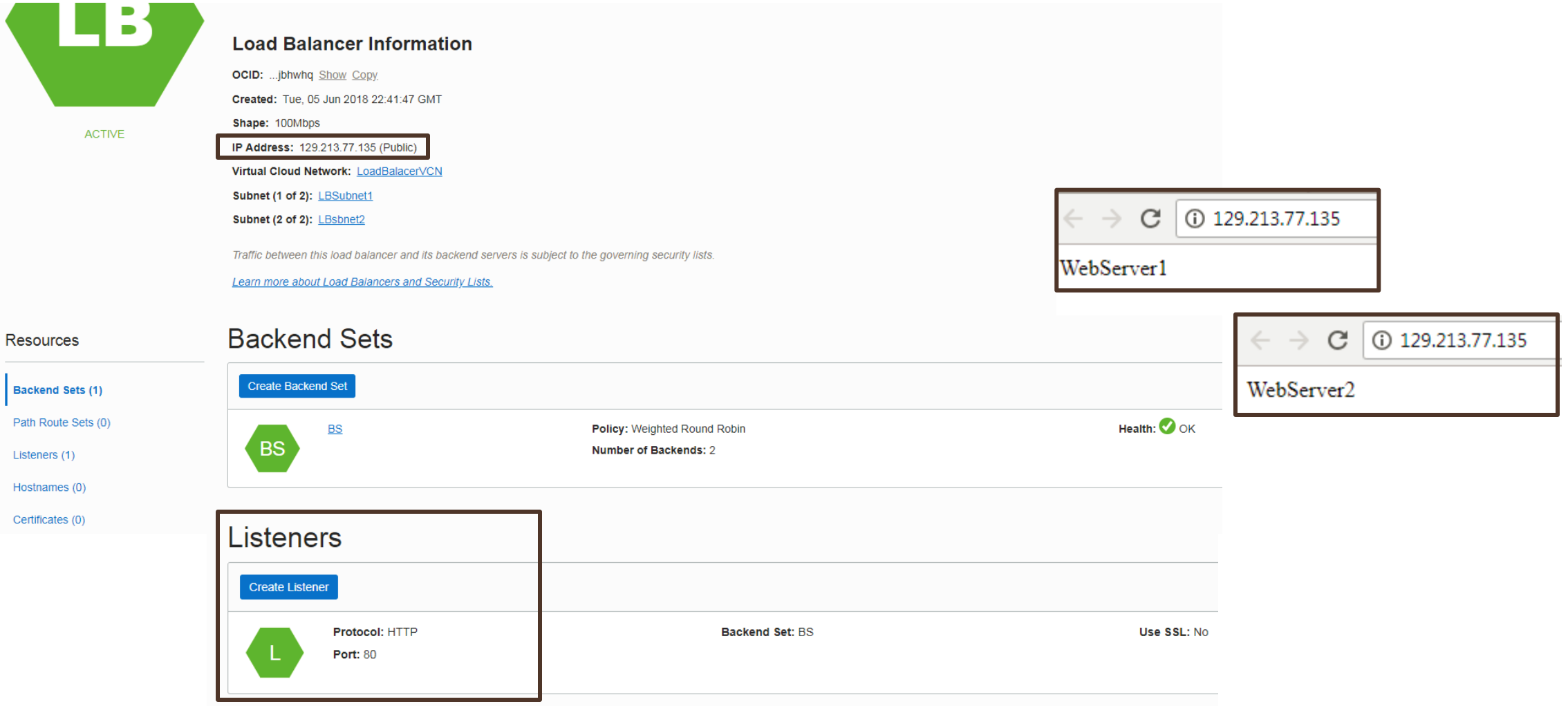
A X.509 v3 digital certificate has this structure:

Certificate
- Version
- Serial Number
- Algorithm ID
- Issuer
- Validity
  - Not Before
  - Not After
- Subject
- Subject public key info
- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Extensions (optional)
  - ...

- Certificate Signature Algorithm
- Certificate Signature

Openssl is a toolkit that can be used to generate X.509 certificates

LB with SSL not enabled



1. Generate private key and CSR

Generate a RSA key

```
$ openssl genrsa -out MyKey.key 2048
Generating RSA private key, 2048 bit long modulus
.........................+++
.......................+++
e is 65537 (0x10001)
```

Create a certificate signing request (CSR)

```
$ openssl req -new -key MyKey.key -out MyCSR.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:WA
Locality Name (eg, city) []:Redmond
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Oracle
Organizational Unit Name (eg, section) []:OCI
Common Name (e.g. server FQDN or YOUR name) []:*.example.org
Email Address []:rohit.rahi@oracle.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

2. Generate a self-signed certificate

Generate a self-signed certificate

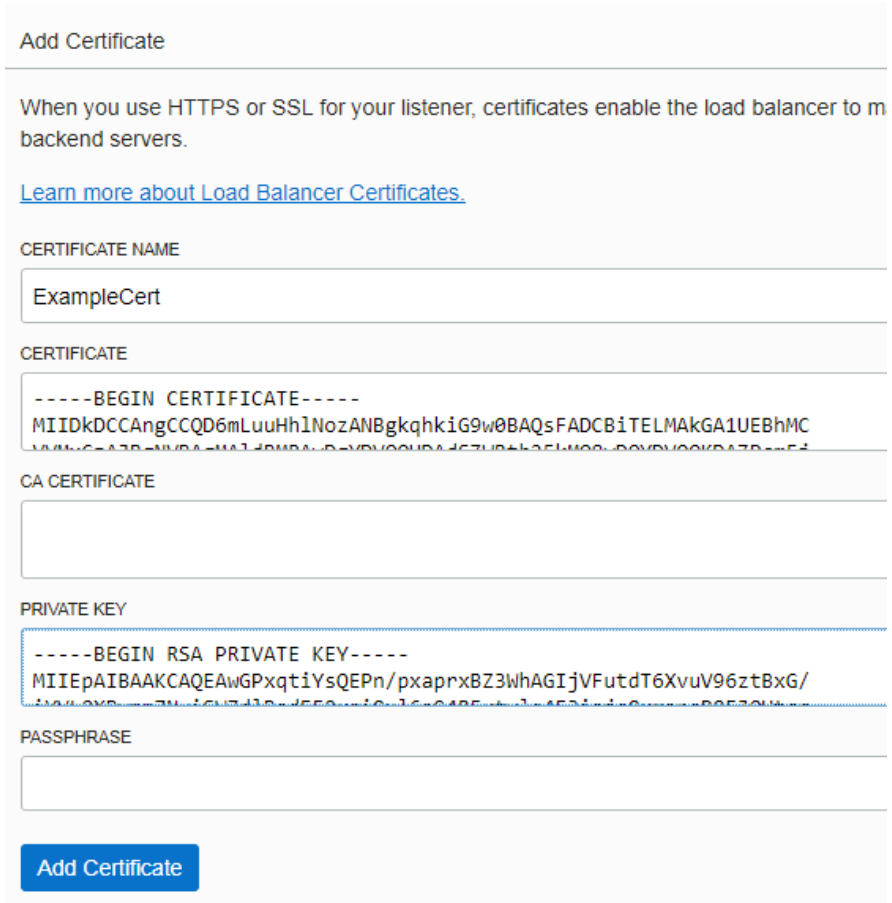
```
$ openssl x509 -req -days 365 -in MyCSR.csr -signkey MyKey.key -out ExampleCert.crt
Signature ok
subject=/C=US/ST=WA/L=Redmond/O=Oracle/OU=OCI/CN=*.example.org/emailAddress=rohit.rahi@oracle.com
Getting Private key
```

```
$ openssl x509 -in exampleCert.crt -noout -text
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            fa:98:bb:ae:1e:19:4d:a3
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=WA, L=Redmond, O=Oracle, OU=OCI, CN=*.example.org/emailAddress=rohit.rahi@oracle.com
        Validity
            Not Before: Jun  6 18:34:41 2018 GMT
            Not After : Jun  6 18:34:41 2019 GMT
        Subject: C=US, ST=WA, L=Redmond, O=Oracle, OU=OCI, CN=*.example.org/emailAddress=rohit.rahi@oracle.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c0:63:f1:aa:d8:98:b1:01:0f:9f:fa:71:6a:9a:
                    f1:05:9d:d6:84:01:88:8d:51:6e:b5:d4:fa:5e:fb:
                    95:f7:ac:ed:07:11:bf:89:85:4b:39:70:71:9e:7e:
                    cd:ba:24:96:65:d9:41:69:d1:05:f7:1a:a2:43:29:
                    7a:6b:de:11:e7:2b:6f:95:ee:04:de:2b:23:b1:0b:
                    a6:a2:76:8f:40:42:50:1e:d8:2a:16:2c:d5:97:2b:
…
```

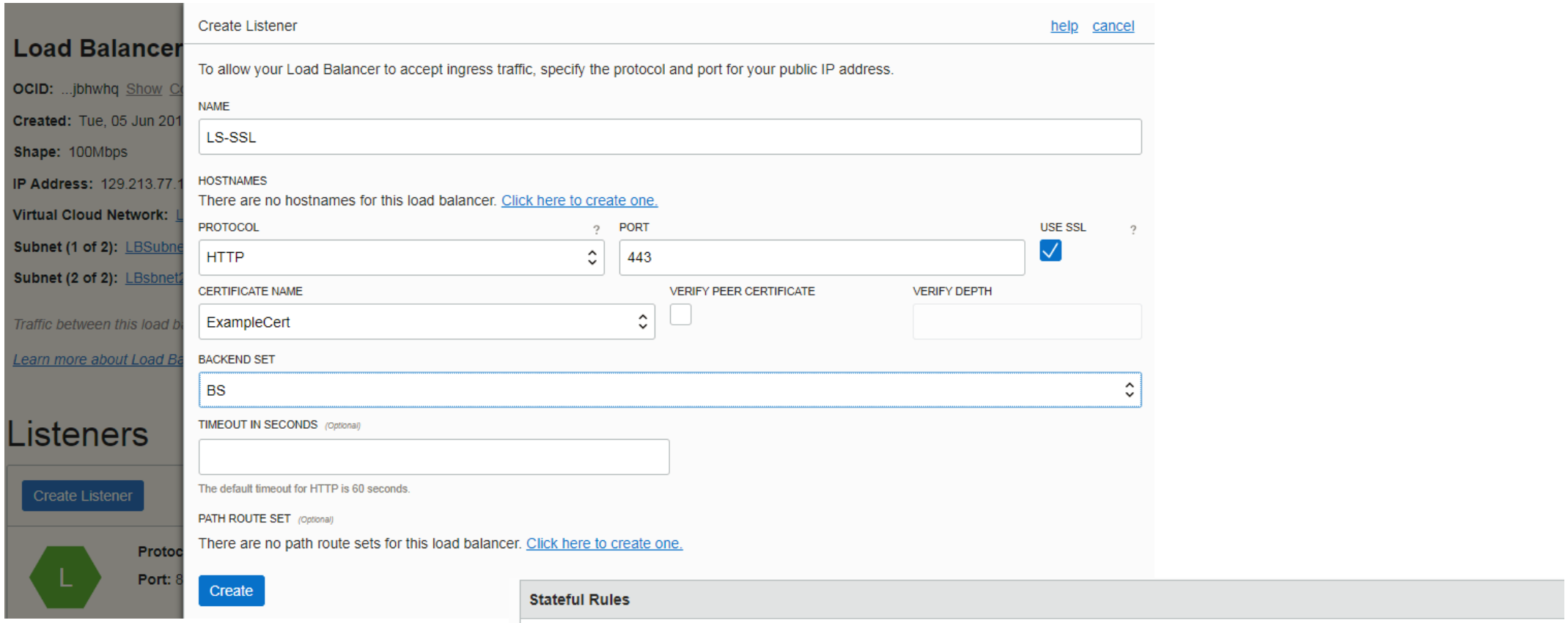
3. Add certificate to the LB

Convert the certificate to a PEM format

```
$ openssl x509 -in ExampleCert.crt -out ExampleCert.pem -outform PEM
```

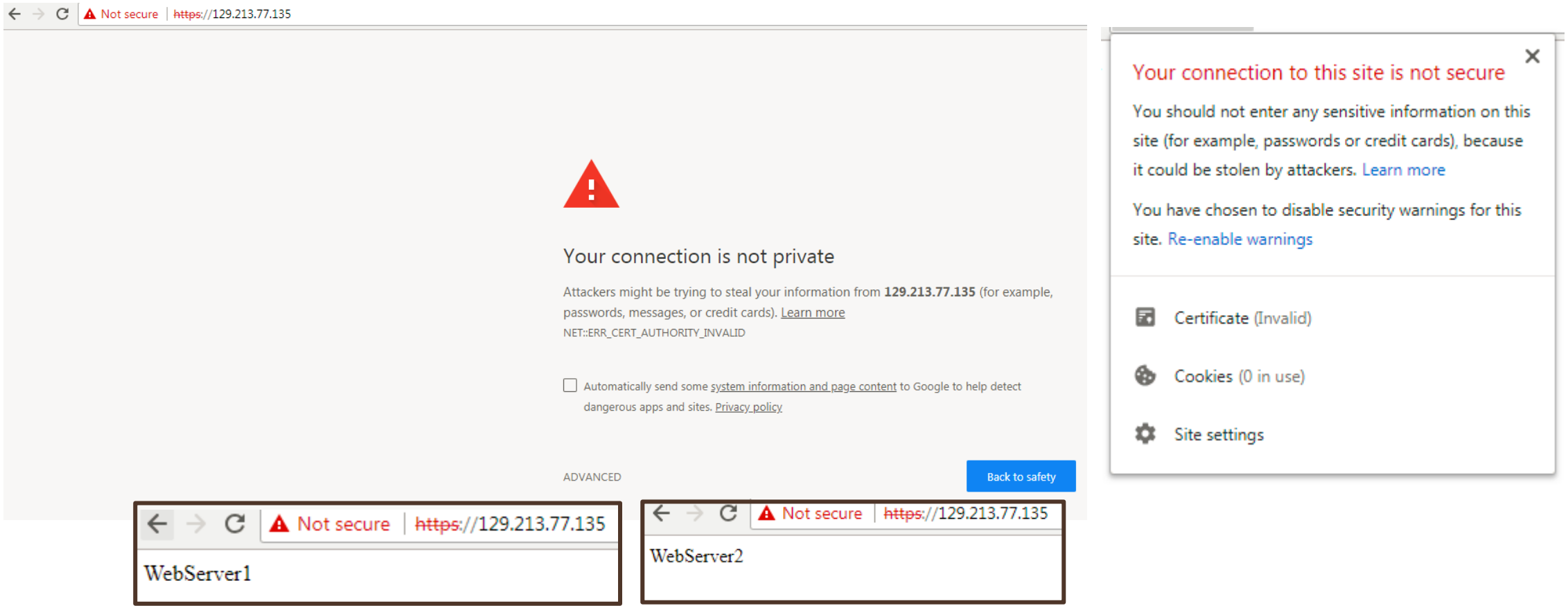


3. Create a listener to listen on port 443



Stateful Rules			
Source: 0.0.0.0/0	**IP Protocol:** TCP	**Source Port Range:** All	**Destination Port Range:** 80
Source: 0.0.0.0/0	**IP Protocol:** TCP	**Source Port Range:** All	**Destination Port Range:** 443

SSL Termination enabled for LB



A self-signed certificate implements full encryption but will cause most browsers to present a warning or error when visitors try to access a public site

ORACLE

Part IV: Troubleshooting Guidelines and Load Balancer Metrics

Troubleshooting Guidelines

- Load balancer health reflects the health of its components. The health status indicators provide information you might need to drill down and investigate an existing issue.

- Configure your health check protocol to match your application or service.

- Common issues and troubleshooting guidelines:
  - A health check is misconfigured.
  - A listener is misconfigured.
    - Listen on the wrong port.
    - Use the wrong protocol.
    - Use the wrong policy.
  - A security list is misconfigured.
    - VCN security lists or network security groups block traffic.
  - Compute instances have misconfigured route tables.
  - Check the corresponding error code listed in the **status** field on the backend server's *Details* page.

- Health status is updated every three minutes. No finer granularity is available.

Load Balancer Metrics - Dimensions

- **AVAILABILITYDOMAIN**
  - The availability domain in which the load balancer resides.
- **BACKENDSETNAME**
  - The name of the backend set to which the metrics apply.
- **LBCOMPONENT**
  - The load balancer component to which the metrics apply.
  - Valid metrics for the three **lbComponent** dimension values:
    - Backendset
    - Listener
    - Loadbalancer
- **LBHOSTID**
  - A unique ID that represents the current load balancer host. This ID is subject to change.
- **LISTENERNAME**
  - The name of the listener to which the metrics apply.
- **REGION**
  - The region in which the load balancer resides.
- **RESOURCEID**
  - The OCID of the resource to which the metrics apply.

Metrics details for the lbComponent Dimension value"Loadbalancer"

Metric	Metric Display Name	Unit	Description
AcceptedConnections	**Accepted Connections**	count	The number of connections accepted by the load balancer.
AcceptedSSLHandshake	**Accepted SSL Handshakes**	count	The number of accepted SSL handshakes.
ActiveConnections	**Active Connections**	count	The number of active connections from clients to the load balancer.
ActiveSSLConnections	**Active SSL Connections**	count	The number of active SSL connections.
BytesReceived	**Bytes Received**	bytes	The number of bytes received by the load balancer.
BytesSent	**Bytes Sent**	bytes	The number of bytes sent by the load balancer.
FailedSSLClientCertVerify	**Failed Client SSL Cert Verifications**	count	The number of failed client SSL certificate verifications.
FailedSSLHandshake	**Failed SSL Handshakes**	count	The number of failed SSL handshakes.
HandledConnections	**Handled Connections**	count	The number of connections handled by the load balancer.
HttpRequests	**Inbound Requests**	count	The number of incoming client requests to the load balancer.

Summary

- Session Persistence
- Virtual Hostnames
- Path based routing
- SSL Handling by OCI LB
- Metrics
- Troubleshooting guidelines

ORACLE

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
oracle.com/cloud/iaas/training
oracle.com/cloud/iaas/training/certification
education.oracle.com/oracle-certification-path

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning