ORACLE

API Gateway

Prasenjit Sarkar
Oracle Cloud Infrastructure
February 2020

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;

- Describe Oracle Cloud Infrastructure API Gateway service
- Configure and Create API Gateway Service

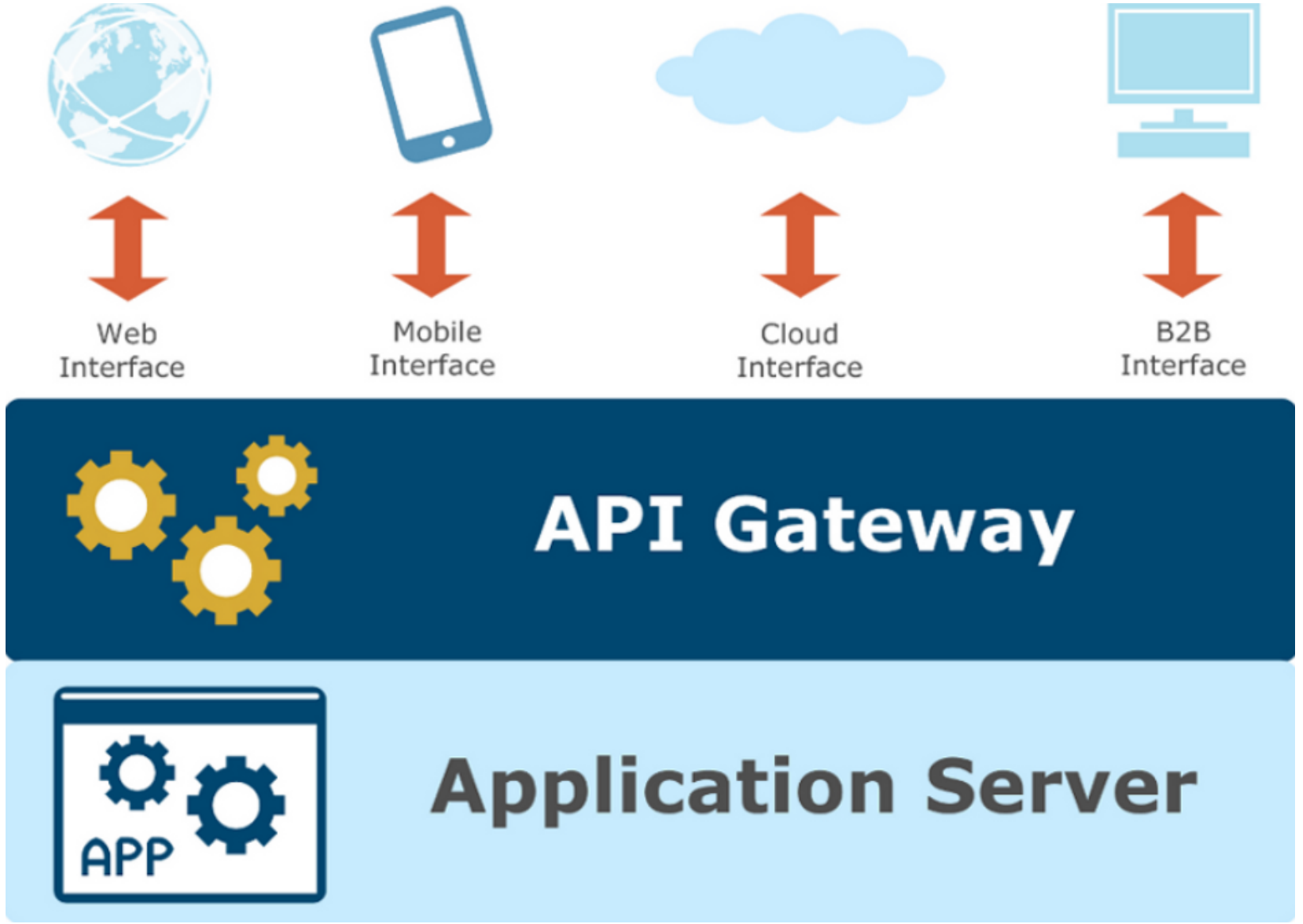
ORACLE

API Gateway Service

API Gateway Overview

- Microservices and Serverless deployment at scale can result in complex series of endpoints that need to be managed for front end and mobile applications
- APIs are common software interface that allows communication with these and other API enabled end points
- Can use a single API gateway to link multiple back-end services (such as load balancers, compute instances, and Oracle Functions) into a single consolidated API endpoint.
- API Gateway act as a "single point of entry" for all clients interacting with the end points, including:
  - Private endpoints that are accessible from within your network
  - Expose with public IP addresses if you want them to accept internet traffic
- API Gateways also give you the ability to easily implement (at Gateway level):
  - API validation
  - Request and response transformation
  - CORS (Cross-Origin Resource Sharing)
  - Authentication and authorization, and request limiting

API Gateway Overview

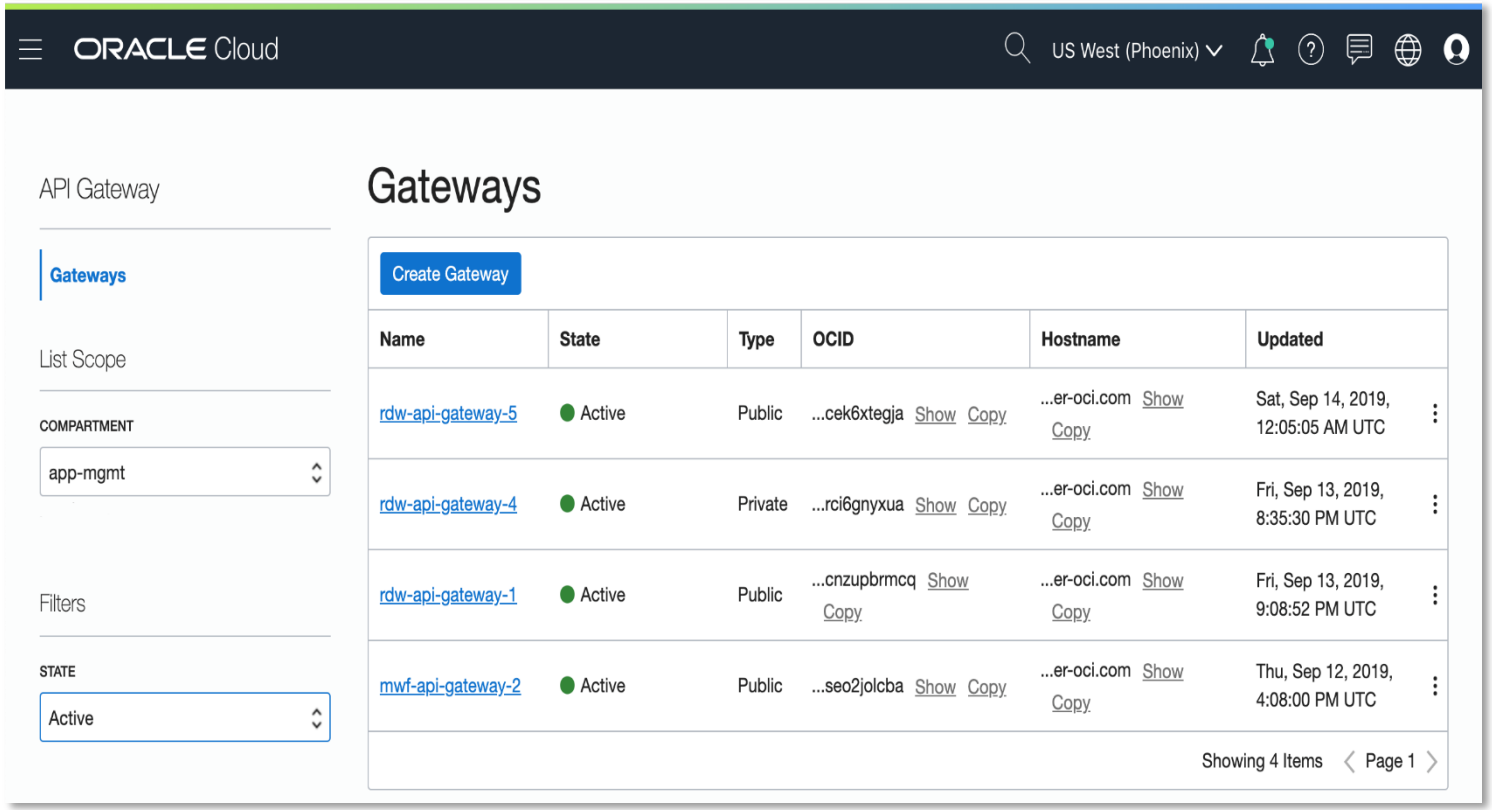


API Gateway Use Cases

- RESTful APIs for Functions
  - Extend applications
  - Manages security access
  - No SDK required
  - Manages security context
- APIs for custom development
  - Use with Oracle Kubernetes Engine
  - API interface for services on K8s
  - Use with services on Compute
- Protect SaaS Services
  - Rate-limit/protect access to SaaS RESTful services
  - Native service on OCI to support SaaS, and Autonomous Database

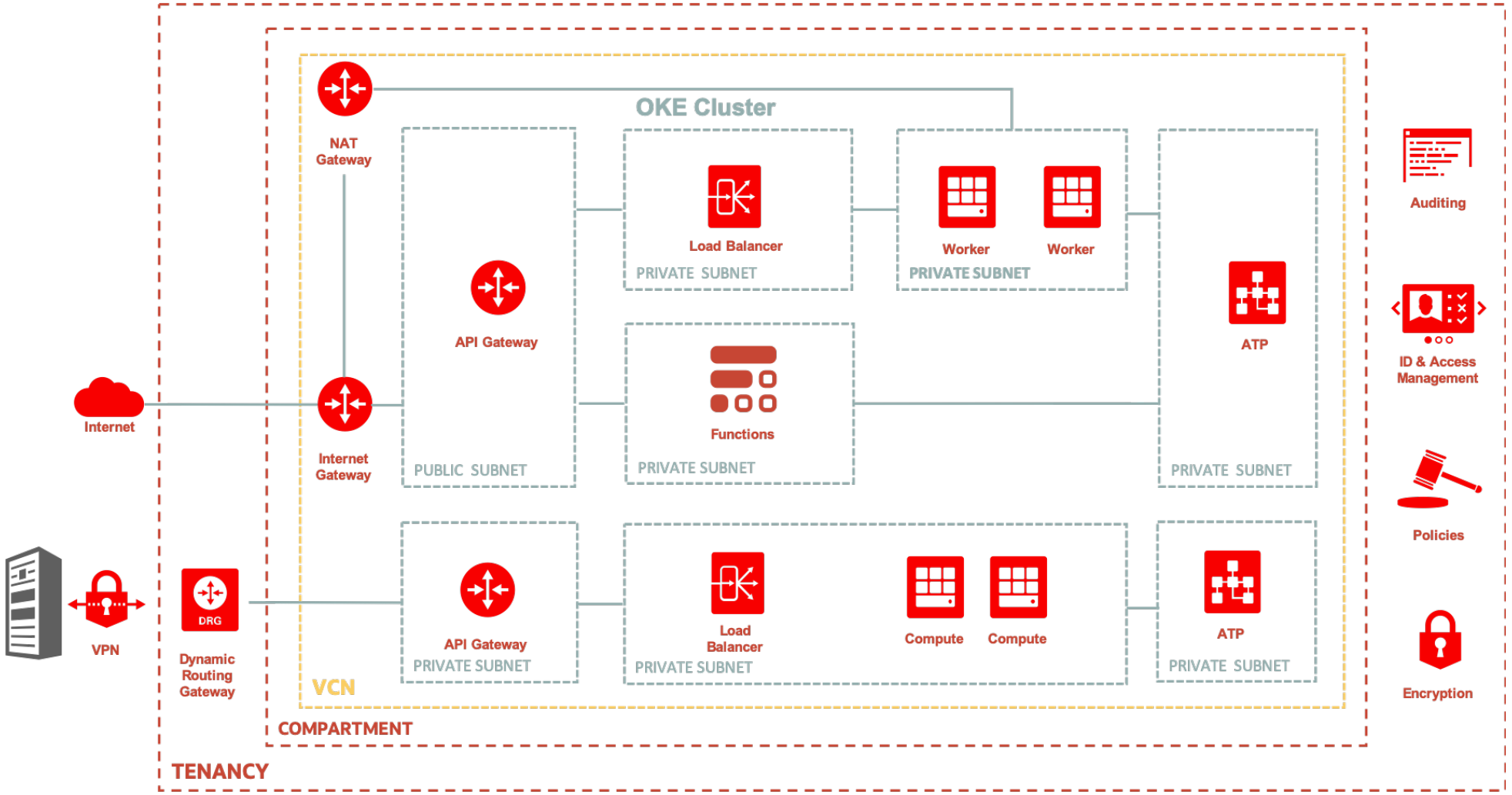
API Gateway Features

- REST APIs for OCI Services
  - Oracle Functions, K8S
  - HTTPS Back-ends
- Routing
- Rate-limiting
- Cross-origin Resource Sharing (CORS)
- Custom Authentication
- Metrics/Logging
- Fully Oracle Managed
- Terraform



Deployment scenario

- Example scenario of Using API Gateway for both Private and Public End point



API Gateway Concepts

APIs

- API is a set of resources, and methods (for example, GET, PUT) that can be performed on each resource in response to requests sent by a caller (a user or system)

API Deployments

- API deployment is the means by which you deploy API on API gateway
- When you create API deployment, you define properties for the API deployment
- Can deploy multiple APIs on the same API gateway

API Deployment Specifications

- Describes some aspects of API deployment:
  - Defines one or more back-end resources
  - Route to each back-end resource
  - Methods (for example, GET, PUT) that can be performed on each resource
  - How the API gateway integrates with the back end to execute those methods
  - Can also include request and response policies
- Can create using dialogs in the Console, or using JSON file

API Gateway Concepts

Front ends
- Means by which requests flow into an API gateway.
- Can have either a public front end or a private front end:
  - A public front end exposes the APIs deployed on an API gateway via a public IP address.
  - A private front end exposes the APIs deployed on an API gateway to a VCN via a private endpoint.

Back ends
- Means by which a gateway routes requests to the back-end services that implement APIs
  - Could be a private endpoint back end
  - Could be other services such as Oracle Functions

API Callers
- A person or system that calls an API by sending requests to the API gateway

API Gateway Developers
- A user responsible for creating API deployment specifications and deploying them to API gateways

API Gateway Administrators
- A person responsible for setting up the API Gateway service. For example, by setting up IAM policies

API Gateway Concepts

Routes

- Mapping between a path, one or more methods, and a back-end service.
- Routes are defined in API deployment specification

Policies

- Different than IAM polices
- Request policy describes actions to be performed on an incoming request from a caller before it is sent to a back end. Can be used to:
  - Limit the number of requests sent to back-end services
  - Enable CORS (Cross-Origin Resource Sharing) support
  - Provide authentication and authorization
- Can add request policies to an API deployment specification that apply globally to all routes

- Response policy describes actions to be performed on a response returned from a back end before it is sent to a caller

ORACLE

Create API Gateway and access Oracle Function

Configuration Tasks

- Below is a list of tasks needed. We will look at Policy tasks in more detail in the next slide

Task #	Tenancy Configuration Task
1	Create Groups and Users to Use API Gateway, if these don't exist already
2	Create Compartments to Own Network Resources and API Gateway Resources in the Tenancy, if they don't exist already
3	Create a VCN to Use with API Gateway, if one doesn't exist already
4	Create Policies to Control Access to Network and API Gateway-Related Resources, and more specifically: • Create a Policy to Give API Gateway Users Access to API Gateway-Related Resources • Create a Policy to Give API Gateway Users Access to Network Resources • Create a Policy to Give API Gateway Users Access to Functions • Create a Policy to Give a Dynamic Group of API Gateways Access to Functions

Required Policy

- Before using the API Gateway service to create API gateways and deploy APIs on them, number of policies are needed.
- In addition to granting access to user you can also grant API gateways access to functions (If a user specifies a serverless function defined in Oracle Functions as the API back end)

For User access;

- Give API Gateway Users Access to API Gateway-Related Resources

Allow group <group-name> to manage api-gateway-family in compartment <compartment-name>

- Give API Gateway Users Access to Network Resources

Allow group <group-name> to manage virtual-network-family in compartment <compartment-name>

- Give API Gateway Users Access to Functions

Allow group <group-name> to use functions-family in compartment <compartment-name>

Required Policy

For function as an API back end; (Grant API gateways access to functions defined in Oracle Functions)

- First create a dynamic group Before creating the API gateway (API Gateway service verifies that the new API gateway will have access to the specified function through its membership of a dynamic group to which a policy grants appropriate access).
- Enter a rule(For Dynamic group) that includes some or all of the API gateways in the compartment

ALL {resource.type = 'ApiGateway', resource.compartment.id = '<compartment-ocid>'}

- Create a IAM policy (Ensure the compartment_name is the compartment where function was created)

Allow dynamic-group <dynamic-group-name> to use functions-family in compartment <compartment-name>

- You also have to create a policy to give users access to Oracle Functions (As described previously)

Create API Gateway and access Oracle Function

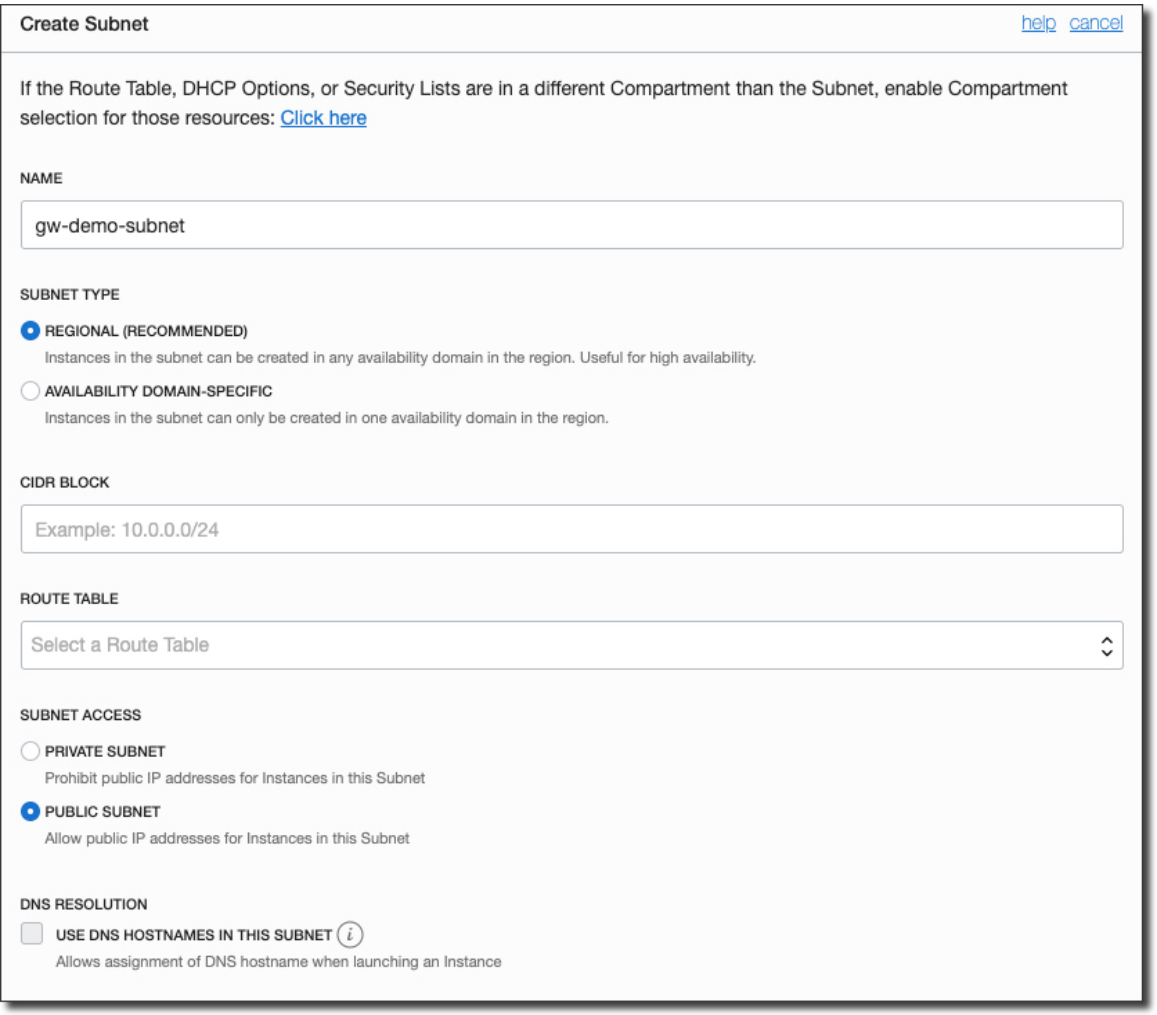
- Assuming user has already deployed an app called ‘Hello World’ using Oracle Fn
- We can invoke this Fn with the Fn CLI but not directly via HTTP(s) without signing the request or using the OCI SDK

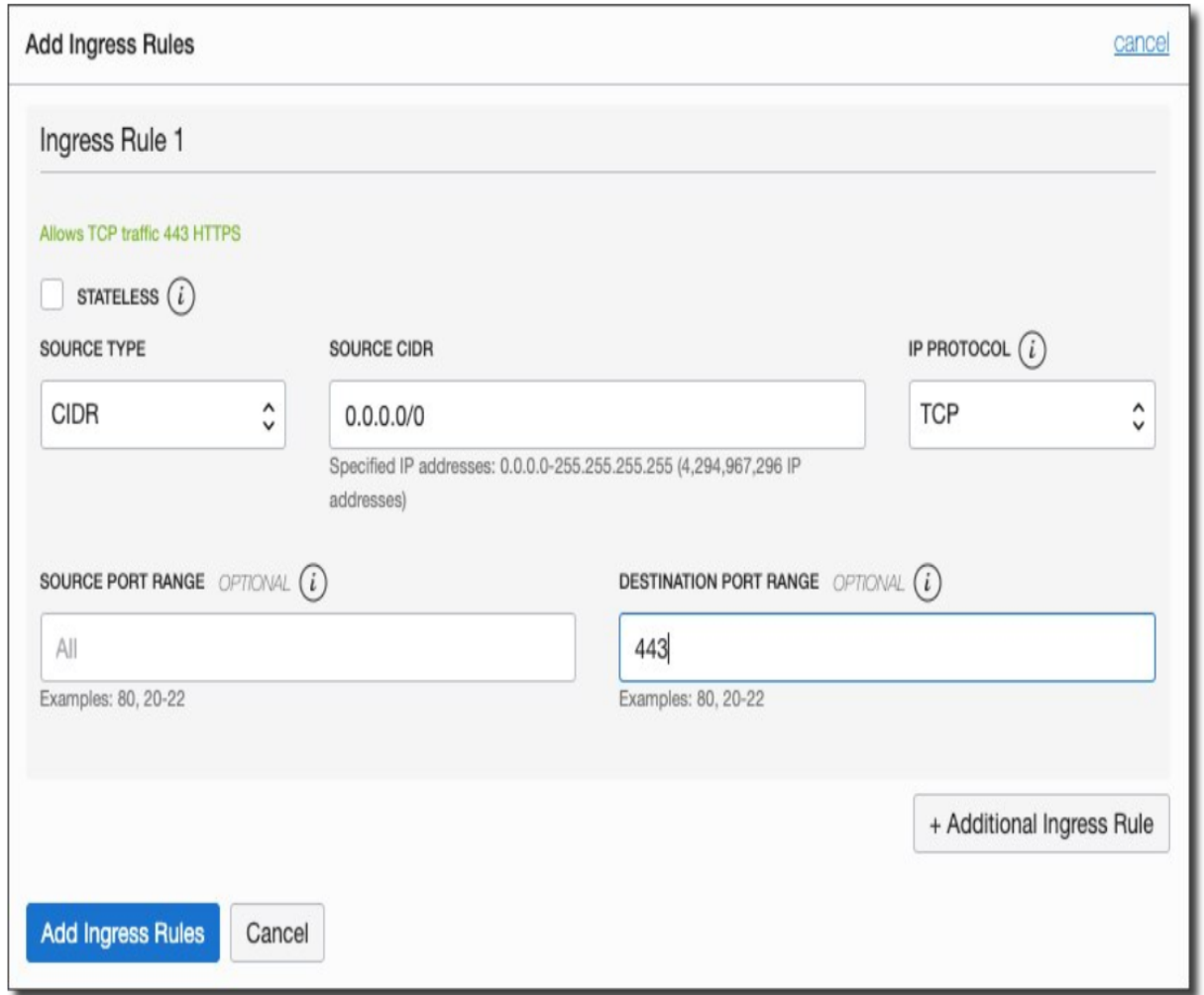
```
$ curl -i -X GET https://[redacted].us-phoenix-1.functions.oci.oraclecloud.com/20181201/functions/ocid1.fnfunc.oc1.phx..../actions/invoke
HTTP/1.1 401 Unauthorized
Date: Fri, 22 Nov 2019 14:24:33 GMT
Content-Type: application/json
Content-Length: 57
Connection: keep-alive
Opc-Request-Id: /01DT9R03K21BT1A2RZJ0005QSH/01DT9R03K21BT1A2RZJ0005QSJ
Www-Authenticate: Signature headers="date (request-target) host"

{"code":"NotAuthenticated","message":"Not authenticated"}
```

- Next, we will put this Fn behind API gateway and invoke it successfully.

Creating API Gateway

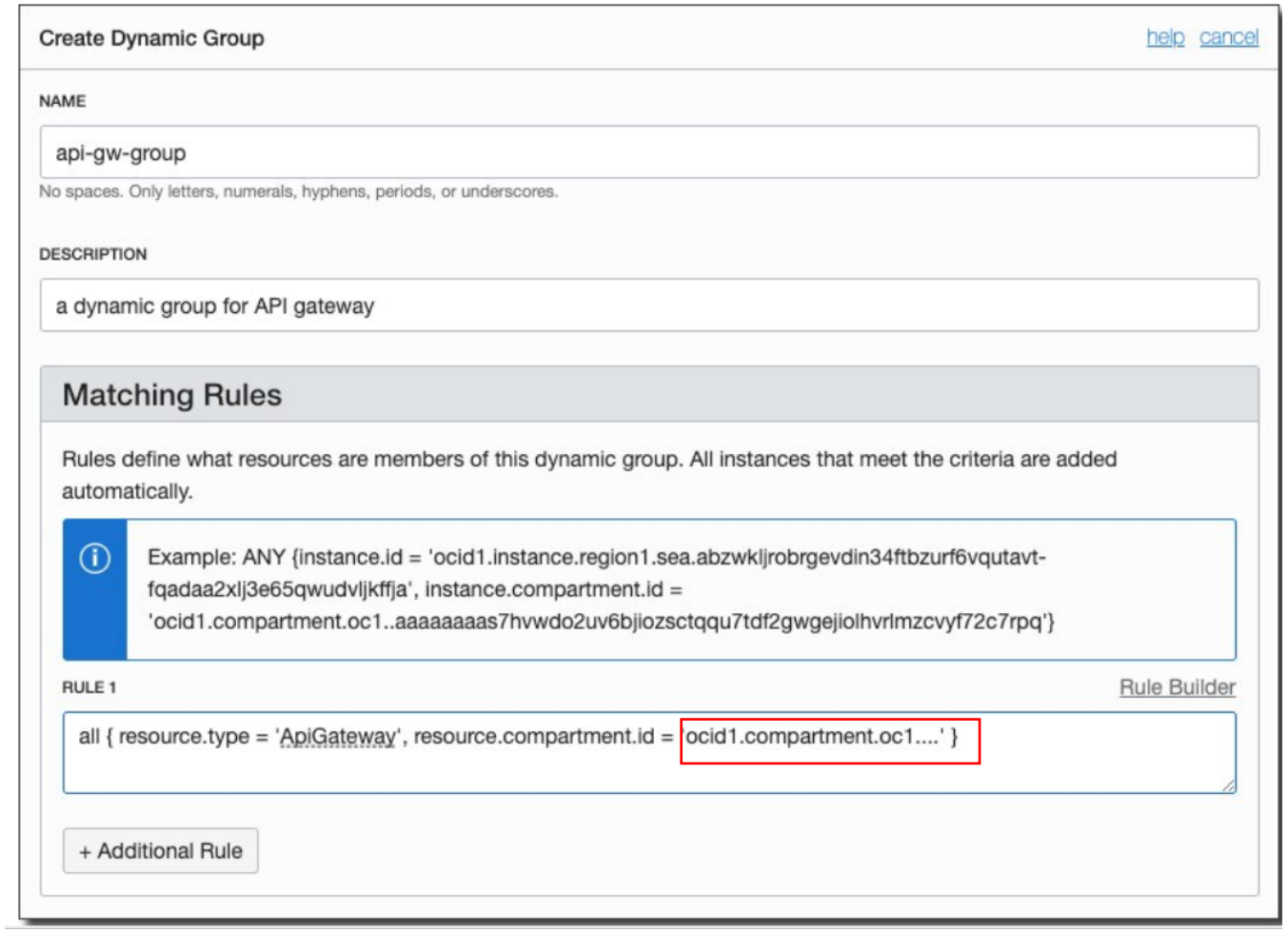
- Create a regional Public subnet that has an ingress rule for HTTPS traffic
  - ➢ Existing subnet can be used as well as long as HTTPS rule is added





Creating API Gateway

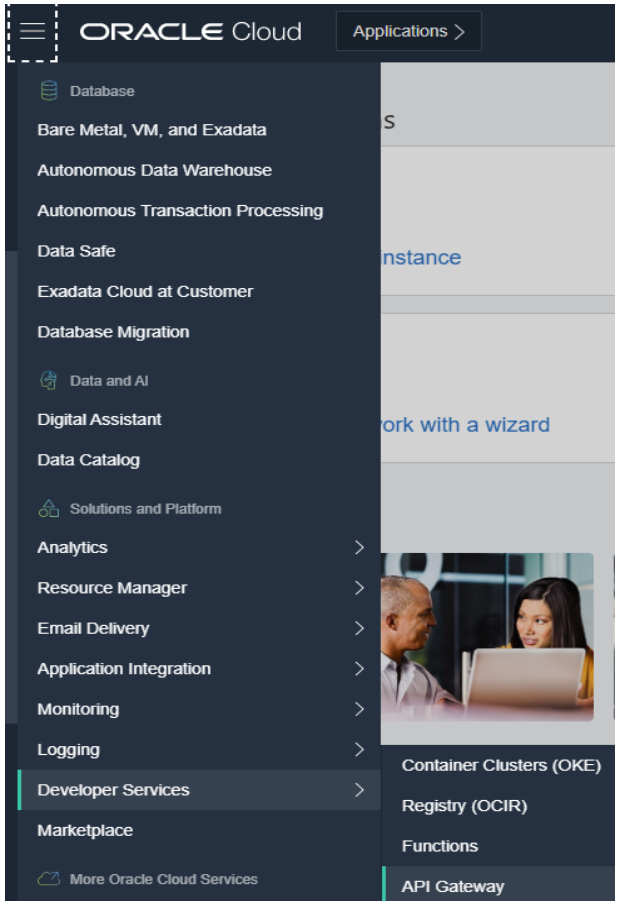
- Create dynamic group and Rules (Replacing OCID appropriately)



- **Also create IAM Policies as described earlier (Not covered in this Presentation)**

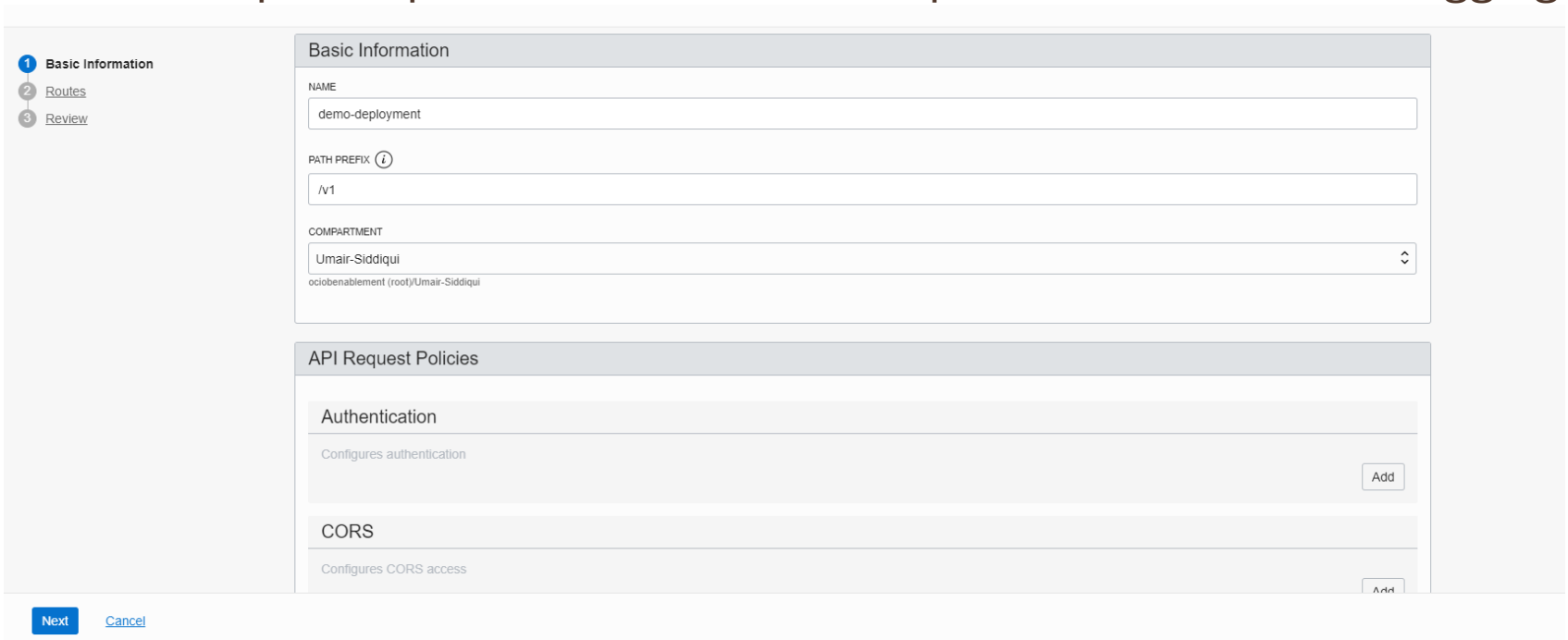
Creating API Gateway

- Can use Console, CLI or SDK
- From OCI console, navigate to ‘Developer Services’ and then ‘API Gateway’



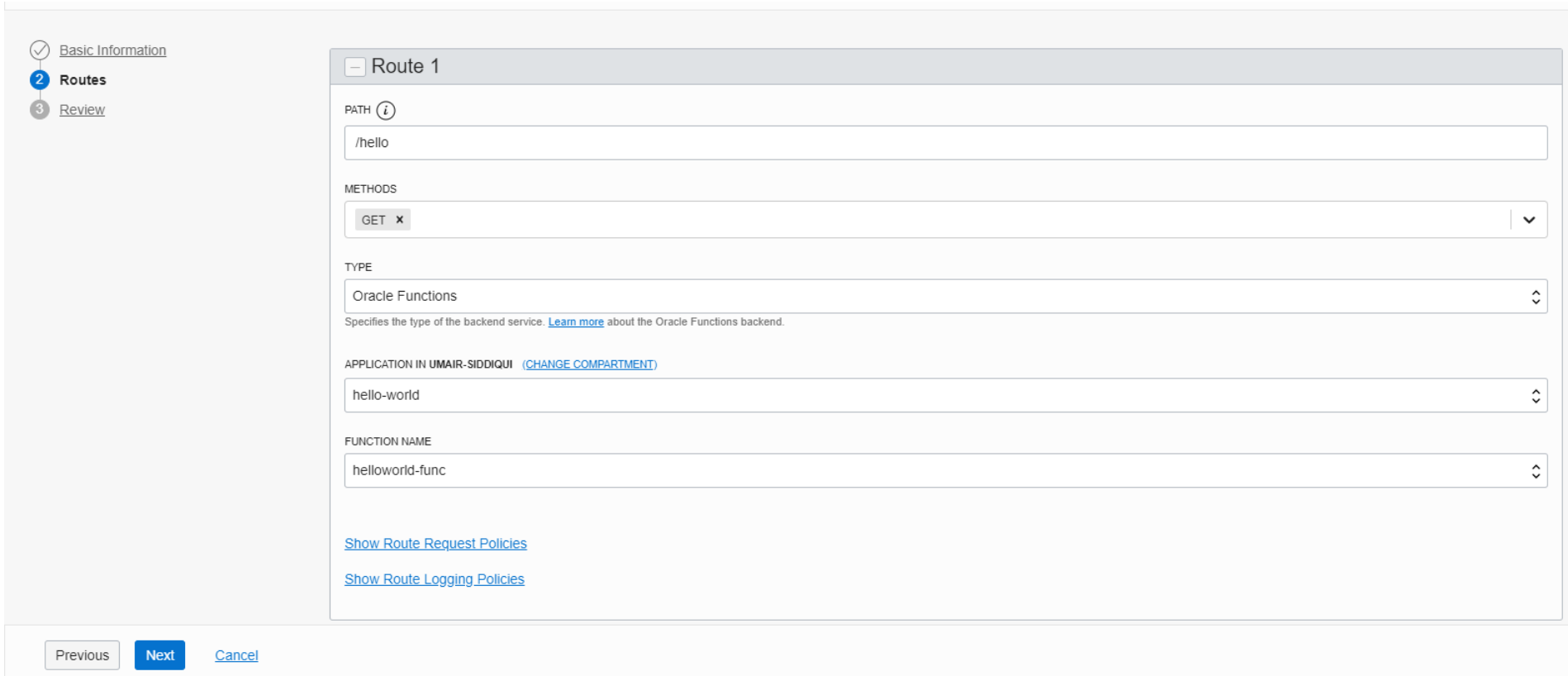
Creating API Gateway

- Once Gateway is available, Click ‘Deployments’ then ‘Create Deployment’
- You have option to create ‘From scratch’ or upload a JSON file. We will use ‘From Scratch’
  - Json Example file is shown later on
- Fill out the multi screen dialog box to configure your Gateway. Under ‘Basic Information’:
  - Provide a ‘Name’, ‘Path Prefix’ and ‘compartment’ (where Fn is deployed)
  - Can leave optional parameters under ‘API Request Policies’ and ‘API Logging policy’ to default



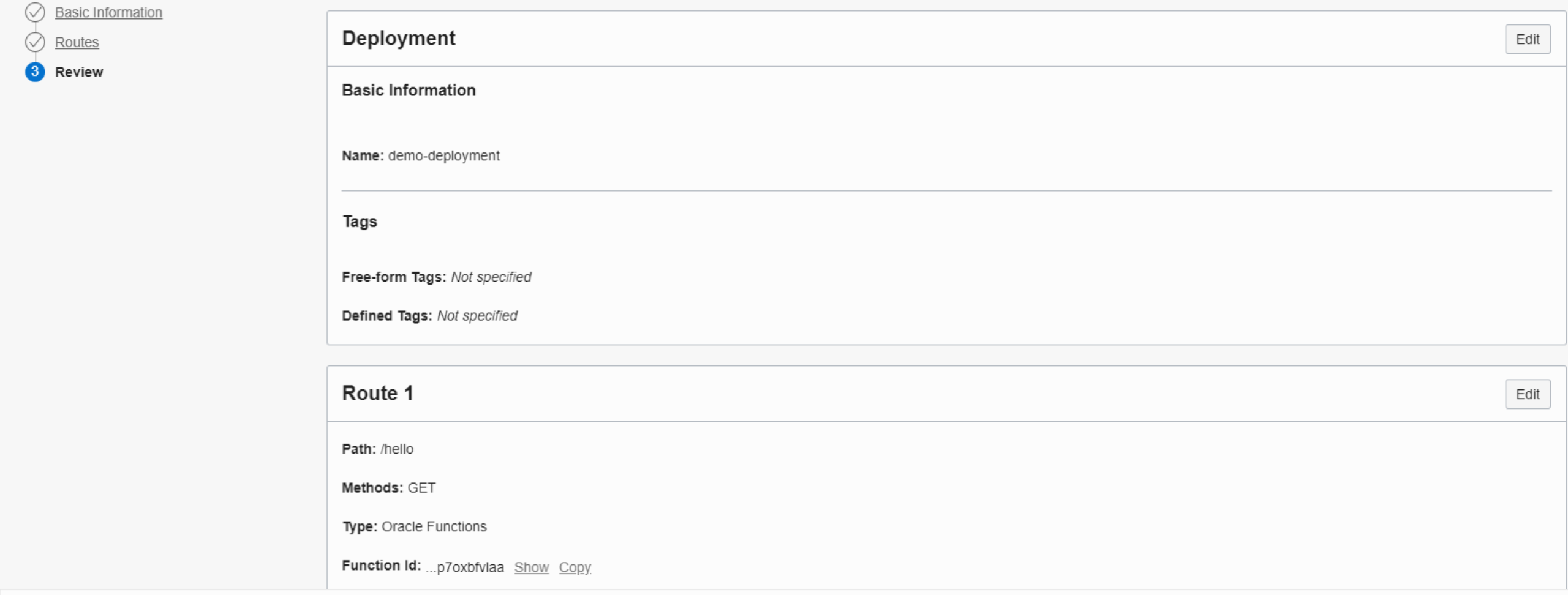
Creating API Gateway

- In ‘Routes’ screen, Under ‘Route 1’
  - ➢ Provide ‘Path’ (is relative to the deployment ‘path prefix’)
  - ➢ ‘Methods’ is GET, ‘Type’ is Oracle Functions
  - ➢ Choose the Application and Function Name using drop down



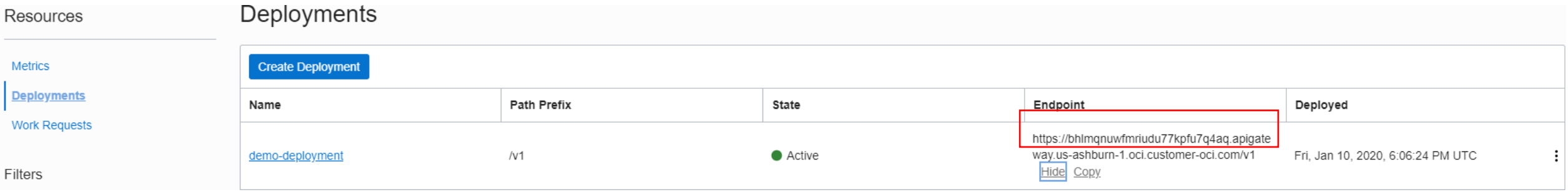
Creating API Gateway

- Review the information and click ‘Create’



Creating API Gateway

- Once Deployment is ‘Ready’, copy the ‘End Point’.



- Access the App again, replacing the end point and verifying Function was invoked

```
$ curl -i -X GET https://[redacted].apigateway.us-phoenix-1.oci.customer-oci.com/v1/hello
HTTP/1.1 200 OK
Date: Fri, 22 Nov 2019 15:04:11 GMT
Content-Type: application/json
Connection: keep-alive
Content-Length: 25
Server: Oracle API Gateway
Strict-Transport-Security: max-age=31536000
X-XSS-Protection: 1; mode=block
X-Frame-Options: sameorigin
X-Content-Type-Options: nosniff
opc-request-id: /429E9723BB6BED8DB8D237876894DDF6/3E4A5D8760D59242A98AB8A91E2B0107

{"message":"Hello World"}
```

Creating API Gateway

- Example JSON file

```
{
  "requestPolicies": {},
  "routes": [
    {
      "path": "<api-route-path>",
      "methods": ["<method-list>"],
      "backend": {
        "type": "<backend-type>",
        "<backend-target>": "<identifier>"
      },
      "requestPolicies": {}
    }
  ]
}
```

Trouble Shooting API Gateway

- Ensure your API Gateway is created in a VCN with at least 1 public subnet
- Ensure port 443 is open in Security list for the subnet
- Ensure ALL IAM policies are defined
- Ensure dynamic group is created

Additional Information

- For additional information on API Gateway, please refer to:

https://docs.cloud.oracle.com/iaas/Content/APIGateway/Concepts/apigatewayoverview.htm

ORACLE

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

OCI training and certification:
cloud.oracle.com/en_US/iaas/training
cloud.oracle.com/en_US/iaas/training/certification
education.oracle.com/oracle-certification-path/pFamily_647

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

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

Thank you