

Procedimento para setup de Ambiente Seguro contendo mTLS + OCI LB + OCI WAF + OCI API Gateway com autenticação JWT e OCI Functions

Parte 2 de 3

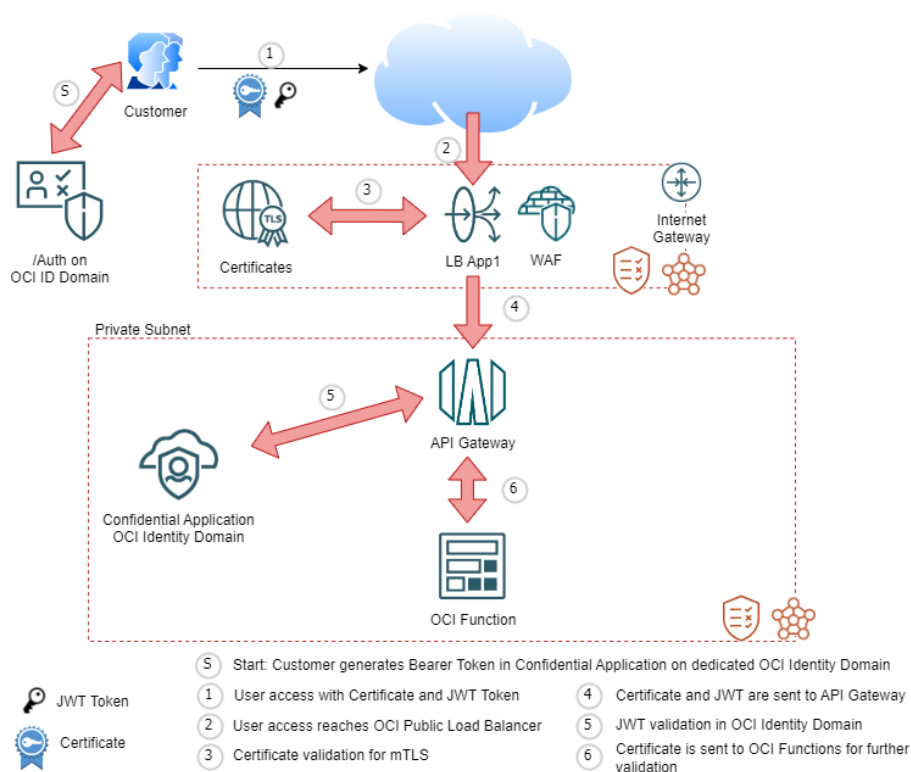
Sumário

1 – Prefácio	2
1.1 – Safe Harbor	3
2 – Criação e Configuração de Master Encryption Key da CA	3
2.1 – Geração de Chave Privada da CA	3
2.2 – Importação da Chave Privada da CA no OCI Vault	4
2.2.1 – Criação do OCI Vault	4
2.2.2 – Copiar a Public Wrapping Key do OCI Vault	6
2.2.3 – Realizando o Wrapping da Private Key da CA	8
2.2.4 – Criação da Master Encryption Key (MEK) da CA no OCI Vault	10
3 – Criação e Configuração da Certificate Authority (CA)	12
3.1 – Criação da CA no OCI Certificates	12
3.2 – Criação dos Certificados SSL	18
3.2.1 – Criação dos Certificados SSL Client	18
4 – Integração entre OCI Certificates e OCI Load Balancer	24
4.1 – Importar os certificados SSL no OCI Load Balancer	24
4.2 – Habilitar SSL no OCI Load Balancer	28
4.3 – Teste de conectividade HTTPS e mTLS no OCI Load Balancer	30
4.4 – Encaminhamento de certificado SSL para o backend do OCI Load Balancer	30
5 – Referências	33

1 – Prefácio

Este procedimento demonstra como configurar um ambiente altamente protegido utilizando conectividade mTLS em um OCI Load Balancer em conjunto com a proteção do OCI Regional WAF. Somado a isso, a solução demonstrará a implantação de um OCI API Gateway validando a autorização de acesso via token JWT e o processamento do certificado mTLS enviado pelo cliente por uma OCI Function.

O ambiente necessário para a configuração desta solução demandará uma VCN contendo uma subnet pública onde o OCI Load Balancer será instalado e uma subnet privada, onde serão instalados o OCI API Gateway e o OCI Functions.



Neste procedimento será necessário utilizar os seguintes serviços OCI:

- OCI Load Balancer
- OCI Certificates
- OCI WAF
- OCI Identity Domains (Confidential Application)
- OCI API Gateway

- OCI Functions
- OCI Vault

Importante:

- Antes do uso deste material, recomendamos a leitura dos links de referência e documentações oficiais para administração de ambientes Oracle cloud.
- Todo código apresentado neste procedimento, bem como os ambientes OCI necessários para o seu funcionamento ou suporte não são responsabilidade dos times técnicos da Oracle.

Nesta parte 2 do procedimento iremos criar toda a infraestrutura necessária para o fechamento do túnel mTLS gerenciado por uma Certificate Authority privada. Faremos a criação manual e importação de chaves privadas utilizando o OCI Vault para uso no OCI Certificates. Em seguida, criaremos uma CA Privativa no OCI Certificates.

Esta CA será utilizada para assinar os certificados utilizados pelo OCI Load Balancer e pelo cliente remoto para a conexão utilizando o mTLS. Após isso, faremos a configuração do mTLS no OCI Load Balancer e testaremos a conectividade do ambiente dentro do túnel criptografado. Por fim será configurado o forward do certificado SSL do cliente para o API Gateway.

1.1 – Safe Harbor

O conteúdo a seguir destina-se a delinear a direção geral de uso de produto. Destina-se apenas a fins informativos e não pode ser incorporado a nenhum contrato. Não é um compromisso entregar qualquer material, código ou funcionalidade e não deve ser considerado na tomada de decisões de compra. O desenvolvimento, lançamento, tempo e preços de quaisquer recursos ou funcionalidades descritos para os produtos da Oracle podem mudar e permanecem a critério exclusivo da Oracle Corporation.

2 – Criação e Configuração de Master Encryption Key da CA

Para podermos criar a CA privativa que será utilizada para a assinatura dos certificados utilizados no mTLS, precisaremos gerar uma chave privada utilizando o OpenSSL. Esta chave privada será utilizada na criação da Certificate Authority que, por sua vez, assinará os certificados a serem utilizados no ambiente deste tutorial.

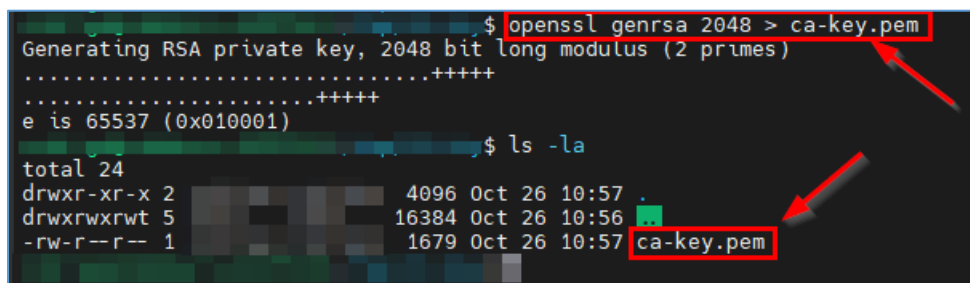
2.1 – Geração de Chave Privada da CA

Antes de efetuar a criação da Certificate Authority dentro do serviço OCI Certificates, será necessário criar a chave privada da CA (Certificate Authority) e importá-la como uma Master Encryption Key dentro do OCI Vault.

Isso se faz necessário pois o processo de criação da CA (Certificate Authority) dentro do serviço OCI Certificates requisita que a chave privada da CA esteja obrigatoriamente armazenada no serviço OCI Vault como uma Master Encryption Key e em um HSM (Hardware Security Module).

Desta forma, para criar a chave privada e armazená-la dentro do OCI Vault como uma MEK (Master Encryption Key), execute o seguinte comando em um terminal Linux que tenha o OpenSSL instalado:

```
$ openssl genrsa 2048 > ca-key.pem
```



```
$ openssl genrsa 2048 > ca-key.pem
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
$ ls -la
total 24
drwxr-xr-x 2 4096 Oct 26 10:57 .
drwxrwxrwt 5 16384 Oct 26 10:56 ..
-rw-r--r-- 1 1679 Oct 26 10:57 ca-key.pem
```

Uma vez criada a chave privada da CA, deve-se importá-la no OCI Vault para que esta chave privada possa, então, ser utilizada para a criação do certificado da Certificate Authority do ambiente.

2.2 – Importação da Chave Privada da CA no OCI Vault

Para poder realizar a criação de uma Certificate Authority será preciso fazer a criação de uma nova Master Encryption Key (MEK) no OCI Vault. Para isso a chave privada da CA criada no item 2.1 será utilizada.

Para importar a chave privada da CA no serviço OCI Vault é necessário seguir os passos abaixo:

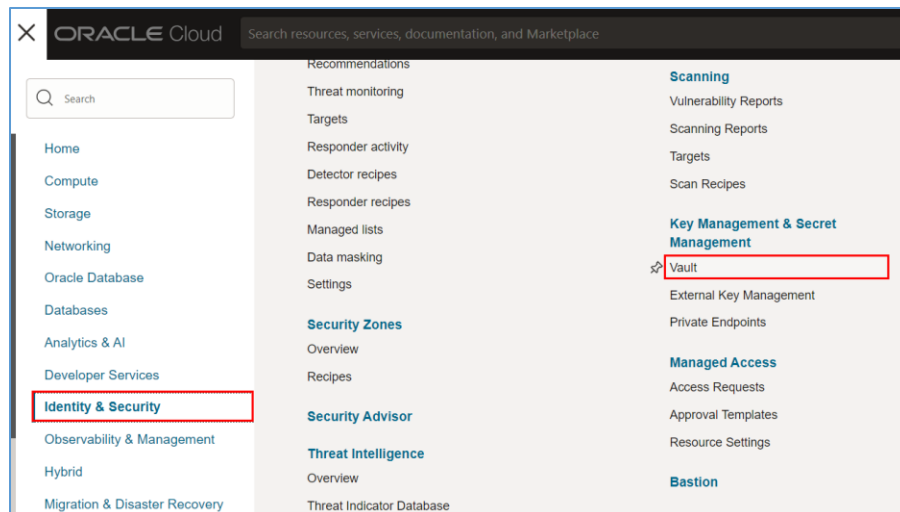
1. Copiar a Public Wrapping Key do OCI Vault que armazenará a chave privada da CA
2. Empacotar a chave privada da CA utilizando a Public Wrapping Key do seu OCI Vault
3. Importar o Key Material como uma External Key no OCI Vault

Vamos detalhar cada um destes pontos.

2.2.1 – Criação do OCI Vault

Para poder copiar a Public Wrapping Key você precisará de uma instância de OCI Vault criada.

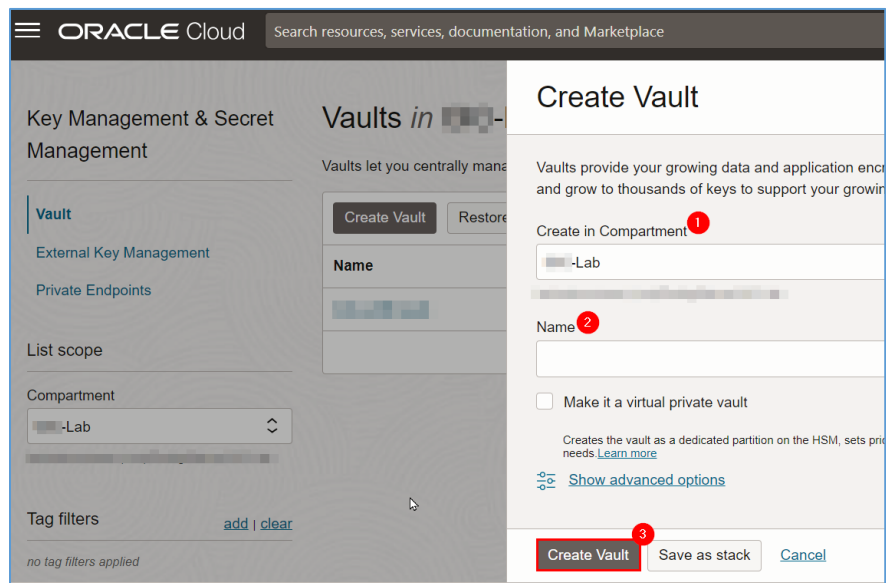
Para criar uma instância do OCI Vault, clique no menu principal da sua console OCI e vá em “Identity & Security -> Vault”:



Uma vez dentro da página de serviço do OCI Vault, selecione o seu compartment e clique em “Create Vault”:



Então selecione o compartment onde o seu OCI Vault será criado, digite o nome do seu Vault e clique no botão “Create Vault”:



Após a criação, o seu OCI Vault ficará com o estado “Active”. Clique no link do seu OCI Vault para acessar as suas configurações.

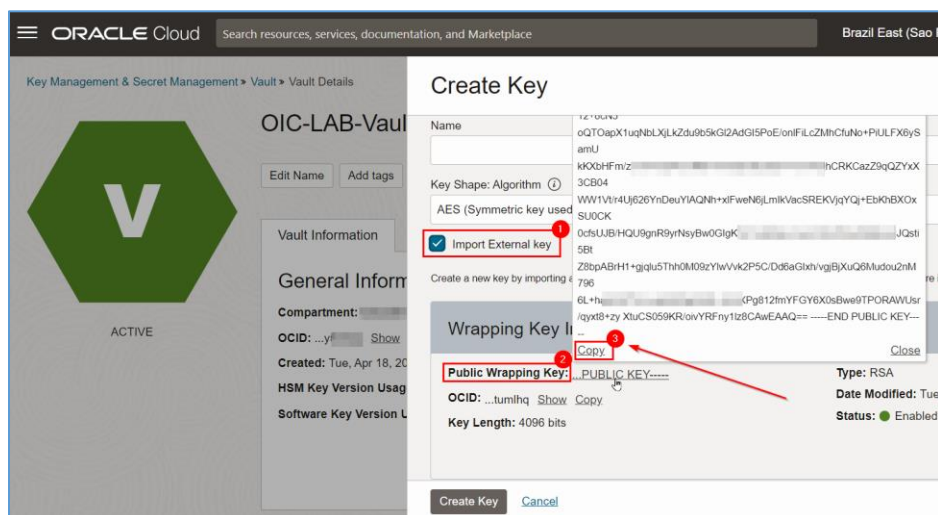


2.2.2 – Copiar a Public Wrapping Key do OCI Vault

Uma vez dentro do seu OCI Vault, clique em “Master Encryption Keys” no menu “Resources” e, após isso, clique no botão “Create Key”:



Após clicar no botão “Create Key”, a janela de configuração da sua Master Encryption Key será aberta. Nela selecione o box “Import External key”. Isso abrirá a seção de “Wrapping Key Information”. Nela, passe o mouse sobre o item “Public Wrapping Key” e clique no link “Copy” conforme mostra a image:



Feito isso, grave o valor da Public Wrapping Key em um arquivo de texto para poder utilizá-la durante o processo de import da Master Encryption Key (MEK) da Certificate Authority (CA) que será criada.

2.2.3 – Realizando o Wrapping da Private Key da CA

Uma vez que já temos a instância do OCI Vault criado e já obtivemos a Public Wrapping Key, podemos proceder com o empacotamento da Private Key da CA para efetuar o seu import no OCI Vault.

Este empacotamento servirá para podermos criar uma nova MEK que será utilizada para a criação da CA a ser utilizada no ambiente.

Para empacotar a Chave Privada da CA que foi gerada o item 2.1 acima, execute os seguintes passos abaixo.

Nota: A execução destes passos do procedimento foi feita em um servidor Linux com o OpenSSL instalado.

Passo 1: Crie uma chave AES temporária para ser utilizada durante o processo

```
$ openssl rand -out temporary-AES.key 32
```

Onde:

- **temporary-AES.key:** Chave de criptografia temporária a ser utilizada no processo de empacotamento da chave primária da CA.

Passo 2: Empacote a chave AES temporária com a chave pública extraída do seu OCI Vault usando RSA-OAEP com SHA-256:

```
$ openssl pkeyutl -encrypt -in temporary-AES.key -inkey vault-public-wrapping.key -pubin -out temporary-AES-file.key -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256
```

Onde:

- **vault-public-wrapping.key:** Arquivo de texto contendo a Public Wrapping Key copiada do Vault no passo anterior
- **temporary-AES-file.key:** Arquivo que será gerado após a execução do comando e conterá a chave ca-key.pem empacotada utilizando a Wrapping Key Pública do Vault

Passo 3: Gere um código hexadecimal do arquivo da chave privada da CA:

```
$ temporary_AES_key_hexdump=$(hexdump -v -e '/1 "%02x"' < temporary-AES.key)
```

Onde:

- **temporary_AES_key_hexdump:** Variável de ambiente do Linux contendo o código hexadecimal gerado a partir da chave privada ca-key.pem.

Passo 4: Agora precisaremos converter a chave ca-key.pem do formato PEM para o formato DER:

```
$ openssl pkcs8 -topk8 -nocrypt -inform PEM -outform DER -in ca-key.pem -out ca-key.der
```

Onde:

- **ca-key.der:** Chave primária criada no item 2.1 convertida para o formato DER.

Passo 5: Neste passo empacote a chave privada no formato DER utilizando a variável de ambiente criada no passo 2:

```
$ openssl enc -id-aes256-wrap-pad -iv A65959A6 -K $temporary_AES_key_hexdump -in ca-key.der -out wrapped-target-key.der
```

Onde:

- **\$temporary_AES_key_hexdump:** Código hexadecimal gerado no passo 2 acima
- **wrapped-target-key.der:** Chave primária empacotada utilizando a Public Wrapping Key copiada do Vault

Passo 6: Por fim, crie o material final a ser importado no OCI Vault concatenando os itens gerados nos passos 2 e 5 da seguinte forma:

```
$ cat temporary-AES-file.key wrapped-target-key.der > final-wrapped-material.key
```

Onde:

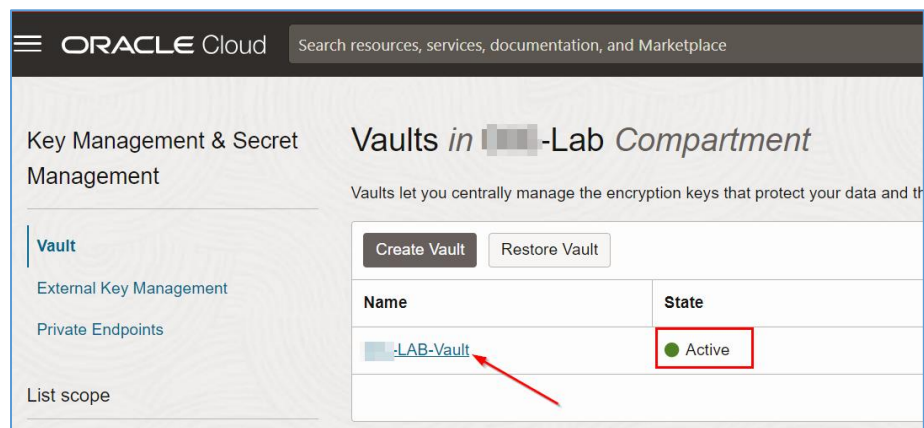
- **final-wrapped-material.key:** Arquivo final a ser importado dentro do OCI Vault para criação da Master Encryption Key.

Importante: Normalmente as instalações do OpenSSL não possuem a opção de criptografia utilizada no passo 5 (**SA_OAEP_AES_SHA256**). Caso isso ocorra durante a sua execução, será necessário que você execute um patch no OpenSSL para corrigir este item. Para obter o passo a

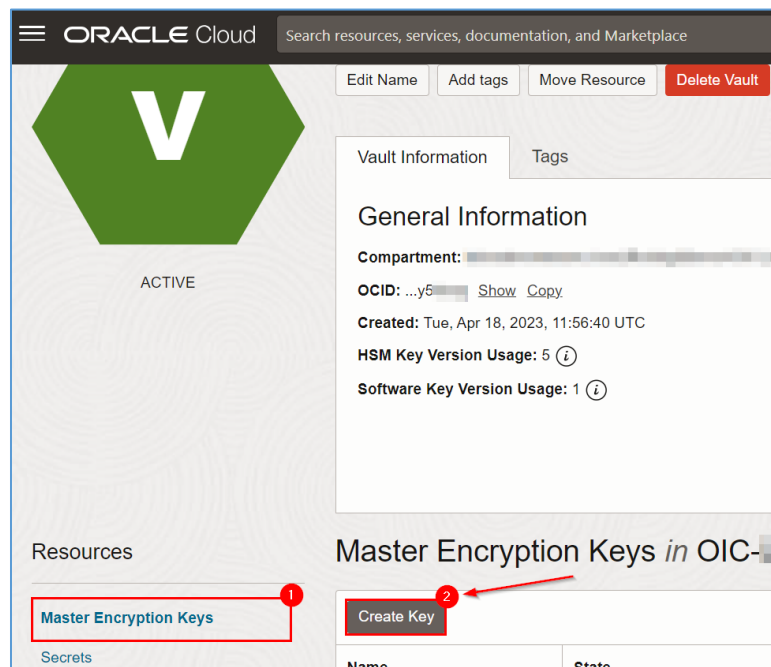
passo de aplicação do patch no OpenSSL, por favor, leia a documentação “Configuring OpenSSL Patch to Wrap Key Material” neste [link](#).

2.2.4 – Criação da Master Encryption Key (MEK) da CA no OCI Vault

Uma vez gerado o material dos passos acima, volte à console Web OCI. Volte ao serviço do OCI Vault e clique novamente no Vault criado:



Então, clique em “Master Encryption Keys” no menu “Resources” e, após isso, clique no botão “Create Key”:



Uma nova página surgirá e nela preencha as informações necessárias para a criação de uma nova MEK:

ORACLE Cloud Search resources, services, documentation, and Marketplace Brazil East (Sao Paulo)

Key Management & Secret Management > Vault > Vault Details

OIC-LAB

ACTIVE

Create Key

Create in Compartment 1

Protection Mode 2

Name 3

Key Shape: Algorithm 4

Key Shape: Length

Import External key 5

Create a new key by importing a wrapped file containing key data that matches the specified key shape. For more information, see [Importing Keys](#).

Create Key Cancel

Onde:

1. **Create in Compartment:** Selecione o compartment onde a sua chave será criada
2. **Protection Mode:** Selecione HSM
3. **Name:** Digite um nome para identificar a sua Master Encryption Key
4. **Key Shape:** Selecione “RSA (Asymmetric key user for Encrypt, Decrypt, Sign and Verify)”
5. **Import External Key:** Selecione este item

Ao selecionar o item “Import External key”, uma continuação da página de configuração da MEK será aberta. Nesta continuação selecione o “Wrapping Key Algorithm” e faça o upload da sua chave (final-wrapped-material.key gerada no passo 6 do item anterior) e clique no botão “Create key”:

ORACLE Cloud Search resources, services, documentation, and Marketplace Brazil East (Sao Paulo)

Key Management & Secret Management > Vault > Vault Details

OIC-LAB-Vault

ACTIVE

Create Key

Import External key 1

Wrapping Key Information

Public Wrapping Key: PUBLIC KEY

Type: RSA

OCID: tumh9g Show Copy

Date Modified: Tue, Apr 18, 2023, 11:56:57 UTC

Key Length: 4096 bits

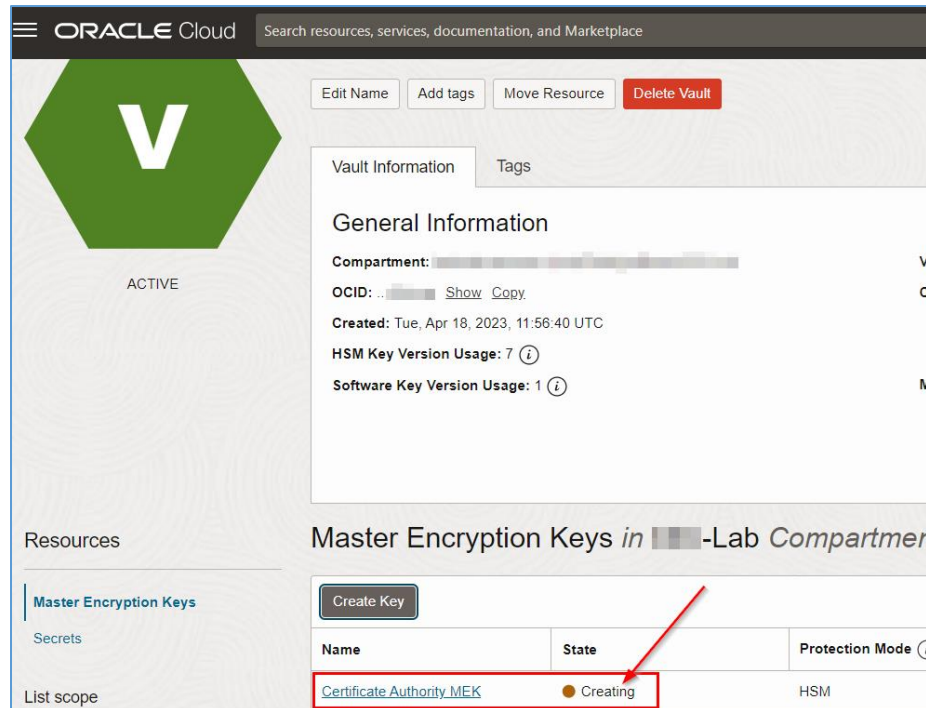
Status: Enabled

Wrapping Algorithm 2

External Key Data Source 3

Create Key Cancel

Aguarde até que a chave tenha sido criada e seu status mude de “Creating” para “Enabled”



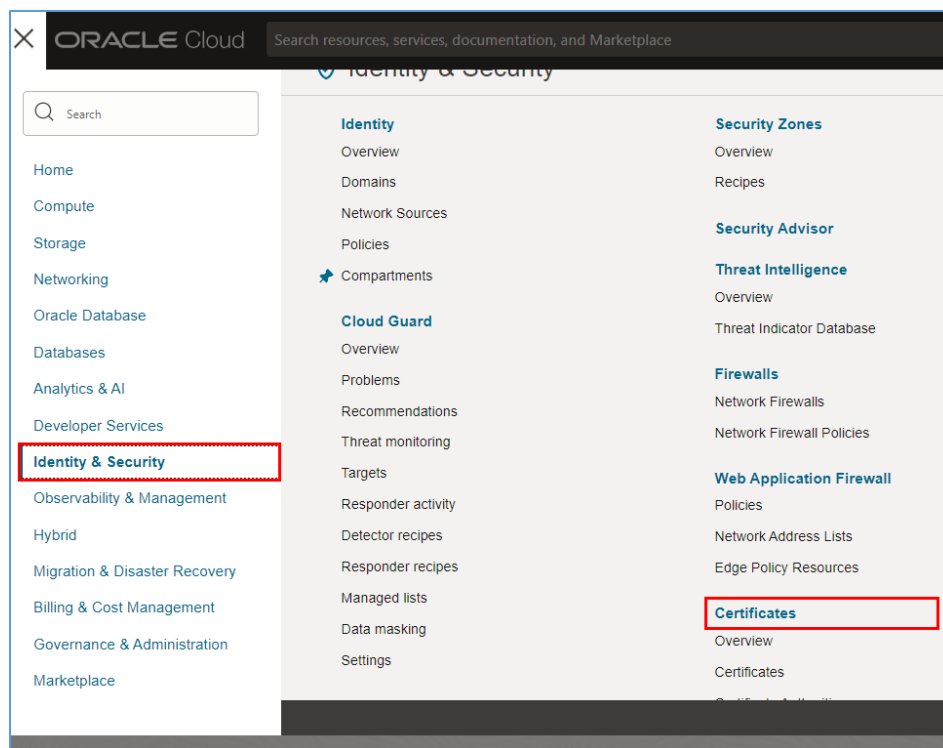
Pronto. Agora já temos a Master Encryption Key que será utilizada para a criação da Certificate Authority do ambiente.

Importante: Note que o Protection Mode da sua Master Encryption Key deve ser “HSM”.

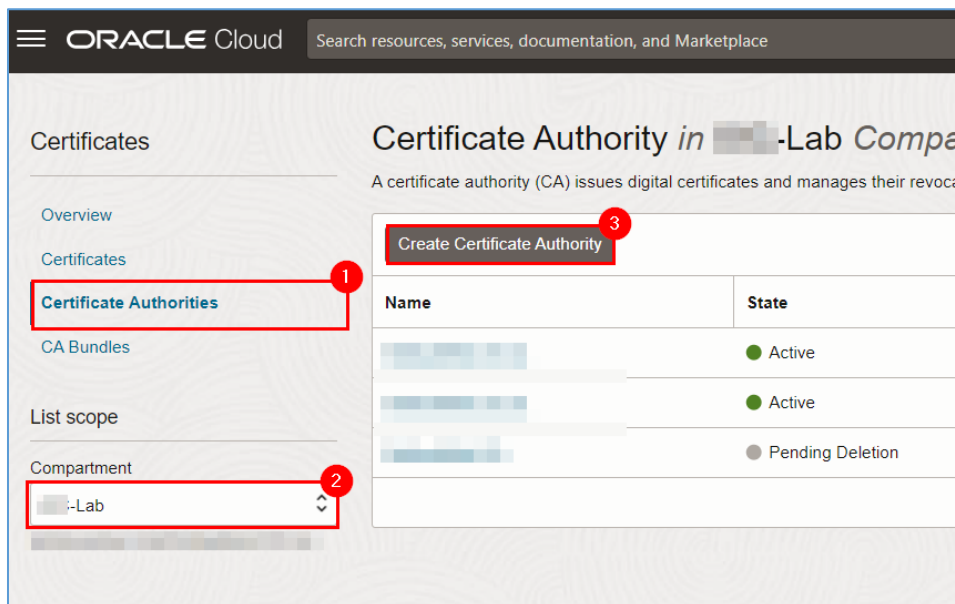
3 – Criação e Configuração da Certificate Authority (CA)

3.1 – Criação da CA no OCI Certificates

Para efetuar a criação da Certificate Authority clique no menu principal da sua console OCI e vá em “Identity & Security -> Certificates”:



Assim que a tela de serviço do OCI Certificates abrir, clique no item “Certificate Authorities” para iniciar a criação da sua CA e, então, selecione o compartment onde a CA será criada e clique no botão “Create Certificate Authority”:



Ao clicar no botão “Create Certificate Authority” o workflow de criação será aberto. Preencha as informações requisitadas:

Onde:

1. **Compartment:** Selecione o compartment onde a sua Certificate Authority será criada
2. **Certificate Authority Type:** Selecione “Root Certificate Authority”
3. **Name:** Digite o nome da sua CA
4. **Description:** Digite uma descrição para a sua CA

Por fim, ao terminar de preencher as informações, clique no botão “Next”.

Ao clicar no botão “Next”, será o momento de preencher as “Subject Informations”. Preencha o campo “Common Name” da sua Certificate Authority.

O **Common Name (CN)** representa o FQDN (Fully Qualified Domain Name) protegido pelo certificado SSL. O certificado será válido somente se o nome do host da solicitação corresponder ao nome comum do certificado.

Neste laboratório é possível definir qualquer CN, uma vez que o certificado gerado não será válido.

Importante: Neste tutorial utilizaremos um certificado auto assinado, ou seja, ele não será gerado por uma Certificate Authority pública.

ORACLE Cloud Search resources, services, documentation, and Marketplace Brazil East

Create Certificate Authority

- 1 Basic Information
- 2 Subject Information**
- 3 Authority Configuration
- 4 Rules
- 5 Revocation Configuration
- 6 Summary

Subject Information

Common Name

[Show Additional Fields](#)

Previous **Next** Cancel

Após preencher os dados do Subject, clique em “Next”.

Neste próximo passo preencha os dados do “Authority Configuration”:

ORACLE Cloud Search resources, services, documentation, and Marketplace Brazil East

Create Certificate Authority

- 1 Basic Information
- 2 Subject Information
- 3 Authority Configuration**
- 4 Rules
- 5 Revocation Configuration
- 6 Summary

Authority Configuration

Not Valid Before

Not Valid After

Vault in **LAB** (Change Compartment)

Key in **LAB** (Change Compartment)

Signing Algorithm

Previous **Next** Cancel

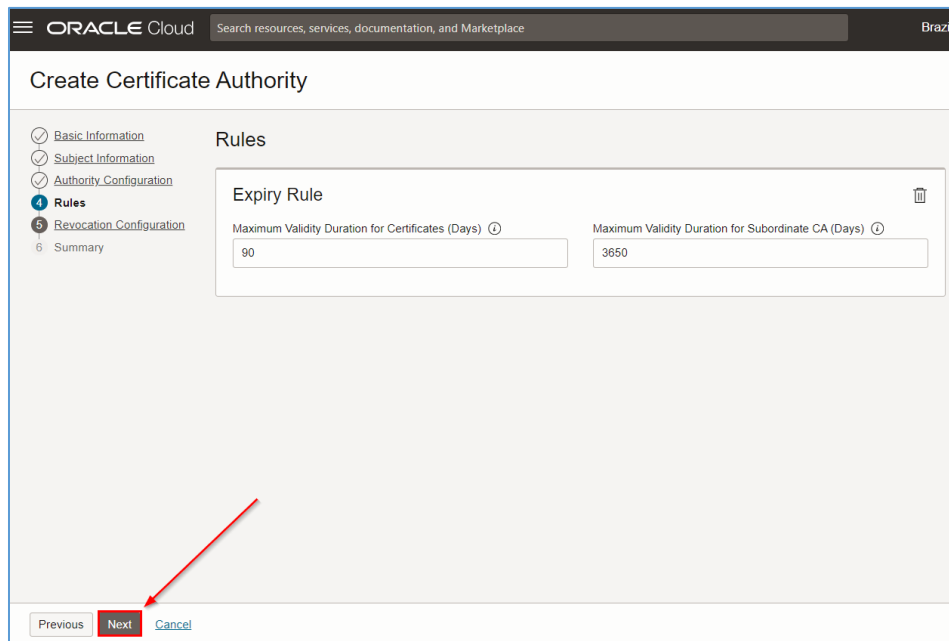
Nesta tela você precisará preencher:

1. **Not Valid After:** Defina a data de expiração da sua CA. O item “Not Valid Before” é opcional.

2. **Vault in <Compartment>**: Selecione seu OCI Vault criado no item acima, no início deste procedimento
3. **Key in <Compartment>**: Selecione a Master Encryption Key (MEK) que foi importada nos passos acima
4. **Signing Algorithm**: Mantenha SHA256_WITH_RSA

Após preencher os valores corretamente, clique no botão “Next”.

O próximo passo, na página “Rules”, mantenha os valores autopreenchidos:



Clique novamente no botão “Next”.

Em seguida, na página “Revocation Configuration”, não é necessário preencher as configurações de Revocation dado que neste laboratório não faremos uso destas configurações. Assim, clique em “Skip Revocation” para poder pular esta configuração:

The screenshot shows the 'Create Certificate Authority' wizard in the Oracle Cloud console, specifically the 'Revocation Configuration' step. On the left, a sidebar lists the steps: Basic Information, Subject Information, Authority Configuration, Rules, Revocation Configuration (selected), and Summary. The main area is titled 'Revocation Configuration' and contains a checkbox labeled 'Skip Revocation' which is checked and highlighted with a red rectangle. Below this, there are fields for 'Object Storage Bucket in' (set to 'WafLab-Lab'), 'Object Name Format', and 'Custom Formatted URLs'. At the bottom, there are three buttons: 'Previous', 'Next' (highlighted with a red rectangle and a red arrow pointing to it), and 'Cancel'.

Clique novamente no botão “Next”.

Por fim, ao chegar na página de “Summary”, as informações preenchidas para a criação da Certificate Authority serão mostradas. Para finalizar a sua criação, clique no botão “Create Certificate Authority”:

The screenshot shows the 'Create Certificate Authority' wizard in the Oracle Cloud console, specifically the 'Summary' step. On the left, the sidebar lists the steps: Basic Information, Subject Information, Authority Configuration, Rules, Revocation Configuration, and Summary (selected). The main area is titled 'Summary' and displays the configuration details for the Certificate Authority. It includes sections for 'Basic Information' (Compartment: WafLab-Lab, Name: WafLabMtls-CA-v3, Certificate Authority Type: Root Certificate Authority), 'Subject Information' (Common Name: *.r...com.br), 'Authority Configuration' (Signing Algorithm: SHA256_WITH_RSA, Not Valid After: Tue, Oct 25, 2033, 00:00:00 UTC, Vault: y6... Show Copy, Key: ... Show Copy), and 'Rules' (Maximum Validity Duration for Certificates (Days): 90, Maximum Validity Duration for Subordinate CA (Days): 3650). At the bottom, there are four buttons: 'Previous', 'Create Certificate Authority' (highlighted with a red rectangle and a red arrow pointing to it), 'Save as stack', and 'Cancel'.

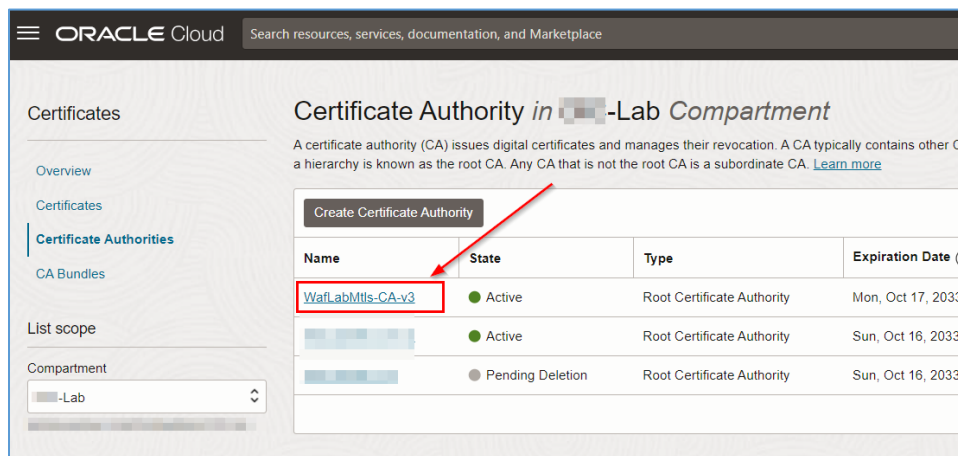
Aguarde alguns instantes para que a sua Certificate Authority seja criada.

Esta CA privada que foi criada será a responsável pela emissão dos Certificados a serem utilizados para a conexão mTLS a ser fechada entre o cliente e o OCI Load Balancer.

3.2 – Criação dos Certificados SSL

Uma vez que já temos a CA (Certificate Authority) criada, podemos então iniciar a criação dos certificados SSL que serão utilizados na conectividade mTLS a ser fechada entre o cliente e o OCI Load Balancer.

Os certificados a serem utilizados poderão ser criados somente após a sua CA entrar no estado “Active”. Para criar os seus certificados, acesse a sua CA clicando no seu link:



Para este laboratório precisaremos criar 2 certificados, sendo eles:

- **WAFServerCertificate:** Este será o certificado a ser utilizado no Listener do Load Balancer a ser configurado.
- **ClientCertificateWAFLab:** Este será o certificado a ser utilizado pelo cliente que irá acessar o ambiente protegido pela infraestrutura que estamos montando.

Antes de efetuar a criação dos certificados, precisaremos criar a private key para os certificados e os arquivos CSR (Certified Signing Request) e CERT (Certificate) tanto para o Load Balancer (Server) quanto para o Cliente. Estes arquivos serão importados dentro do OCI Certificates para que eles sejam assinados pela CA e, assim, possam ser utilizados no acesso mTLS.

Nota: Para podermos fechar a sessão mTLS será necessário termos em mãos o arquivo da chave privada do certificado digital do Cliente (gerado no passo 3.2.1). Desta forma, para simplificar o procedimento, geraremos ambas as chaves (Cliente e Server) da mesma maneira.

3.2.1 – Criação dos Certificados SSL Client

Para criar o certificado SSL que será utilizado no Cliente, precisaremos executar alguns comandos OpenSSL para gerar:

- Chave Privada do Cliente
- Requisição de Assinatura de Certificado para o Cliente (a ser realizado pela CA que foi criada no passo anterior)

Para criar a Chave Privada do **Cliente**, execute os seguintes comandos:

```
$ openssl req -newkey rsa:2048 -nodes -days 365000 -keyout client-key.pem -out client-req.pem
```

Onde:

- **client-key.pem**: Arquivo da chave privada do Cliente
- **client-req.pem**: Arquivo CSR (Certified Signing Request) do Cliente

Para criar a Chave Privada do **Server**, execute os seguintes comandos:

```
$ openssl req -newkey rsa:2048 -nodes -days 365000 -keyout server-key.pem -out server-req.pem
```

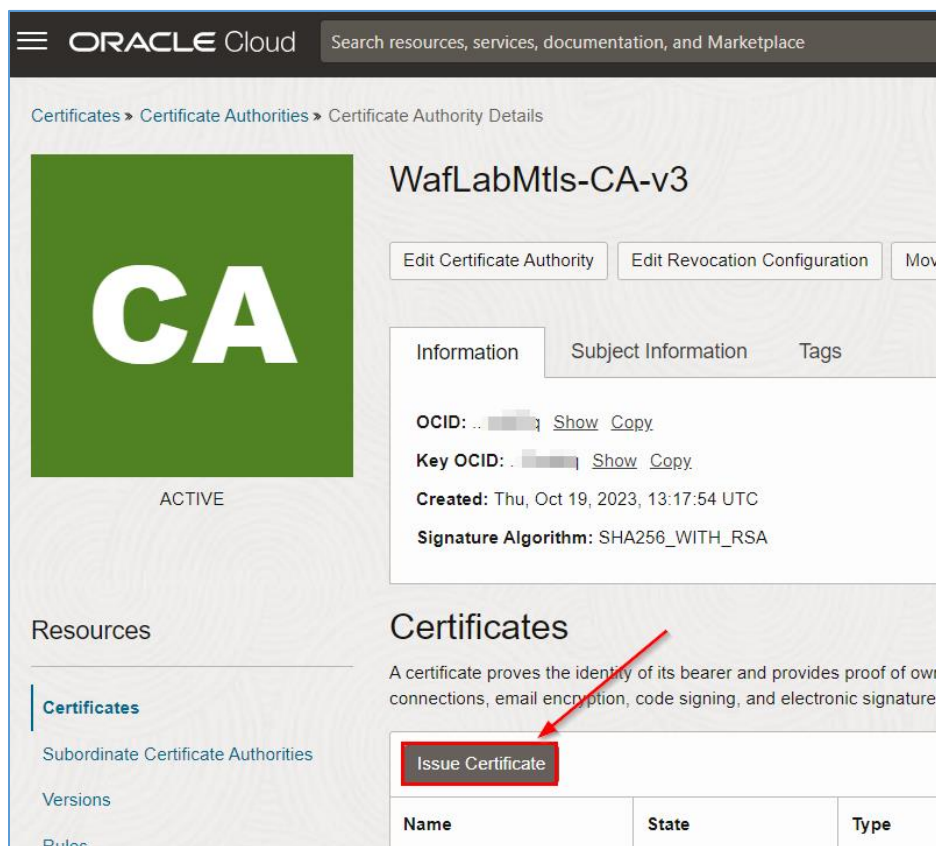
Onde:

- **server-key.pem**: Arquivo da chave privada do Server
- **server-req.pem**: Arquivo CSR (Certified Signing Request) do Server

Após gerar os arquivos, será necessário importá-los no OCI Certificate durante a importação dos certificados digitais na CA do nosso ambiente.

Nota: A criação dos arquivos precisa ser feita de forma manual pois é necessário utilizar a chave privada do cliente para a criação da sessão mTLS entre o Cliente e o Server. Como informado antes, realizamos os processos para os certificados do Cliente e Server de maneira igual para simplificar o procedimento.

Após criar os arquivos de chave privada e de CSR (Certificate Signing Request) do Cliente e do Server conforme indicado anteriormente, volte à Console Web OCI e dentro da página de serviços da CA criada clique no botão “Issue Certificate”:



Ao clicar no botão “Issue Certificate” uma nova janela se abrirá com o workflow de criação do certificado.

Para este laboratório criaremos, conforme mostrado acima, utilizaremos os arquivos gerados via OpenSSL para criar os 2 certificados, sendo eles:

- **WAFServerCertificate:** Este será o certificado a ser utilizado no Listener do Load Balancer a ser configurado.
- **ClientCertificateWAFLab:** Este será o certificado a ser utilizado pelo cliente que irá acessar o ambiente protegido pela infraestrutura que estamos montando.

Assim, na primeira tela do workflow de criação do certificado, preencha as informações requisitadas:

ORACLE Cloud Search resources, services, documentation, and Marketplace

Create Certificate

- 1 Basic Information
- 2 Subject Information
- 3 Certificate Configuration
- 4 Rules
- 5 Summary

Basic Information

Compartment **1**

Certificate Type **2**

- Issued by internal CA
A certificate issued and managed by a Certificates service private certificate authority (CA)
- Issued by internal CA, managed externally**
A certificate issued by a Certificates service private certificate authority (CA) that you intend to manage outside the service ✓
- Imported
A certificate issued by a third-party public or private certificate authority (CA) that you intend to manage by using the Certificates service

Name **3**

Description **4**

[Show Tagging Options](#)

5 Next Cancel

Onde:

1. **Compartment:** Selecione o compartment onde o certificado será criado
2. **Certificate Type:** Selecione a opção “Issued by internal CA, managed externally” selecionada
3. **Name:** Digite o nome do certificado
4. **Description:** Digite uma descrição para o certificado gerado

Após preencher todas as informações clique no botão “Next” para seguir para o próximo passo do Workflow.

Na janela seguinte denominada “Subject Information”, não é necessário preencher informações:

ORACLE Cloud Search resources, services, documentation, and Marketplace

Create Certificate

- 1 Basic Information
- 2 Subject Information**
- 3 Certificate Configuration
- 4 Rules
- 5 Summary

Subject Information

1 You only need to provide subject information for certificates issued by a Certificates service private certificate authority (CA).

Previous **Next** Cancel

Apenas clique novamente no botão “Next”.

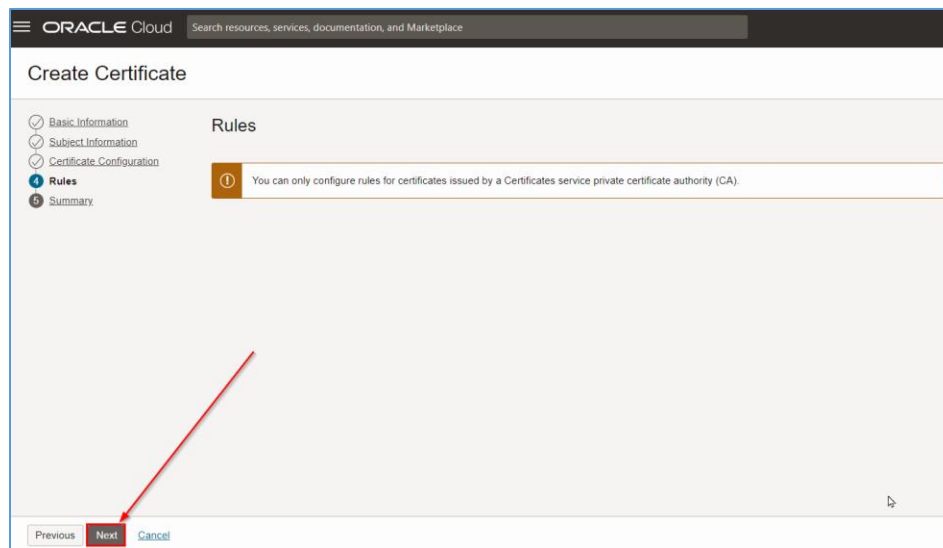
Na janela seguinte denominada “Certificate Configuration”, preencha as informações requisitadas:

Onde:

1. **Issuer Certificate Authority in <Compartment>:** Informe em qual compartment está configurada a CA a ser utilizada para a geração dos certificados
2. **Not Valid After:** Informe a data de validade final dos certificados gerados. Não é necessário preencher data no item “Not Valid Before” para este laboratório
3. **Certificate Signing Request:** Fazer o upload do arquivo CSR ou copie e cole o conteúdo do arquivo CSR nesta tela

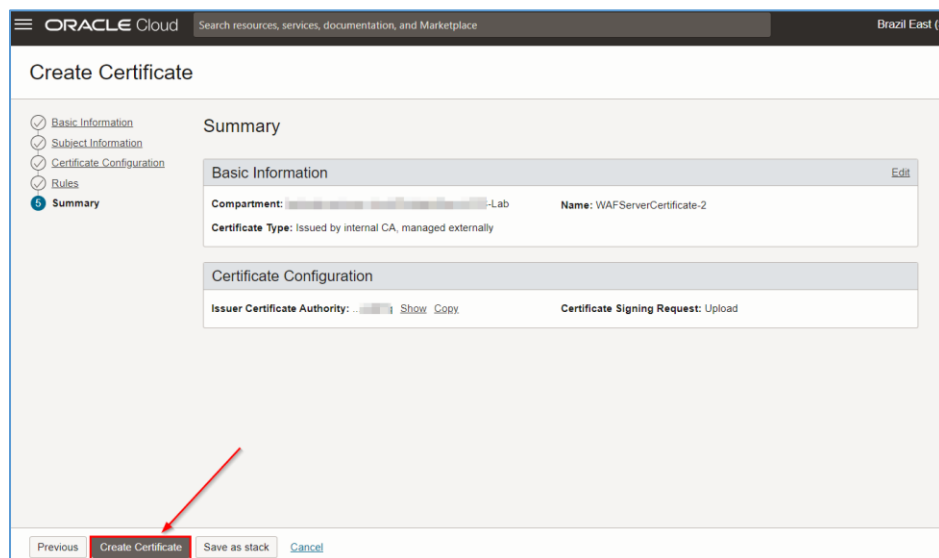
Após preencher os dados, clique novamente no botão “Next”.

Na tela “Rules”, apenas clique no botão “Next”:



Ao clicar no botão “Next”, a tela de “Summary” será apresentada contendo as informações passadas para a criação do certificado.

Valide as informações e clique no botão “Create Certificate” para finalizar a criação do certificado.



Importante: Este processo de criação de certificados precisará ser executado 2 vezes tendo em vista que serão necessários 2 certificados (um para o OCI Load Balancer e o outro para o cliente). Portanto, repita os passos acima e faça a criação do Certificado a ser utilizado pelo Load Balancer.

Depois de criar os dois certificados necessários, eles devem estar listados dentro do menu de serviços “Certificates” da CA que foi criada:

4 – Integração entre OCI Certificates e OCI Load Balancer

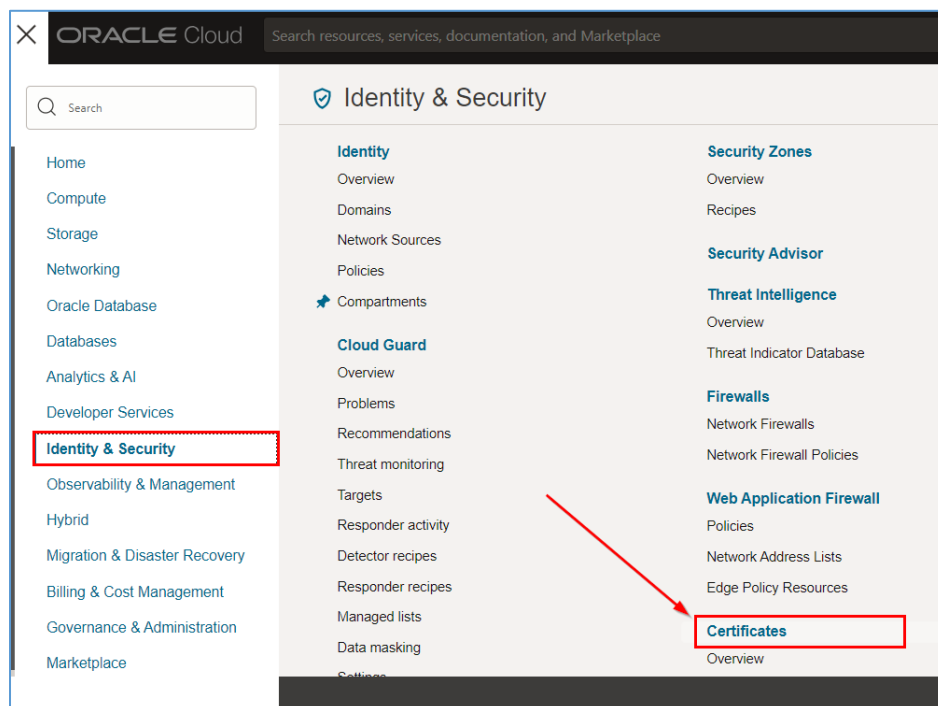
Uma vez configurada a CA e os certificados SSL do Servidor, é possível configurar o SSL no OCI Load Balancer. Esta configuração é simples e rápida.

4.1 – Importar os certificados SSL no OCI Load Balancer

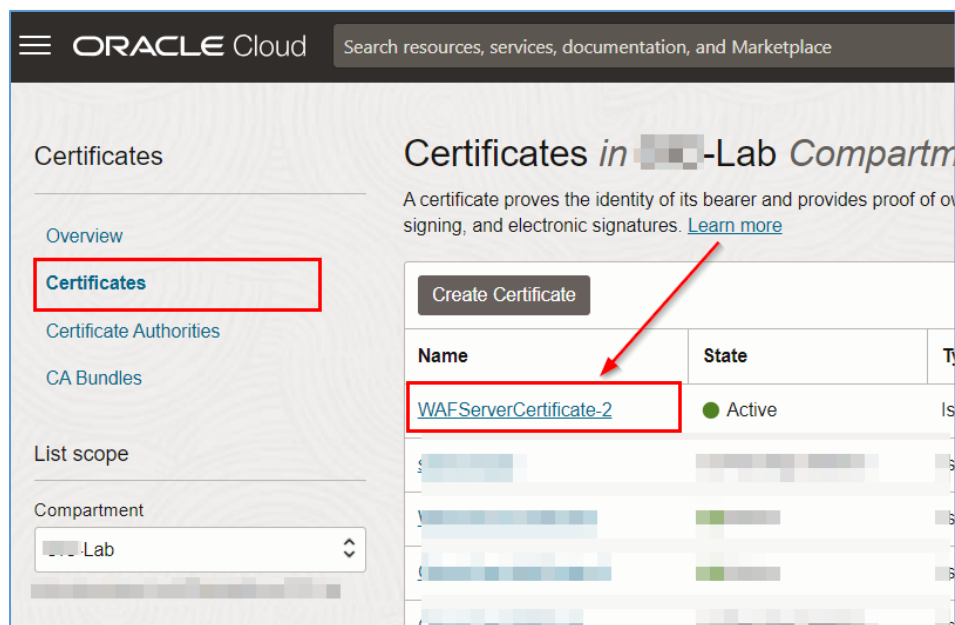
Para podermos configurar o SSL e o mTLS é necessário importar o certificado do Servidor criado nos passos anteriores no OCI Load Balancer.

Antes de importar o certificado no OCI Load Balancer é necessário copiar a sua chave pública. Esta chave pública está disponível no OCI Certificate, de acordo com o que foi executado nos passos anteriores.

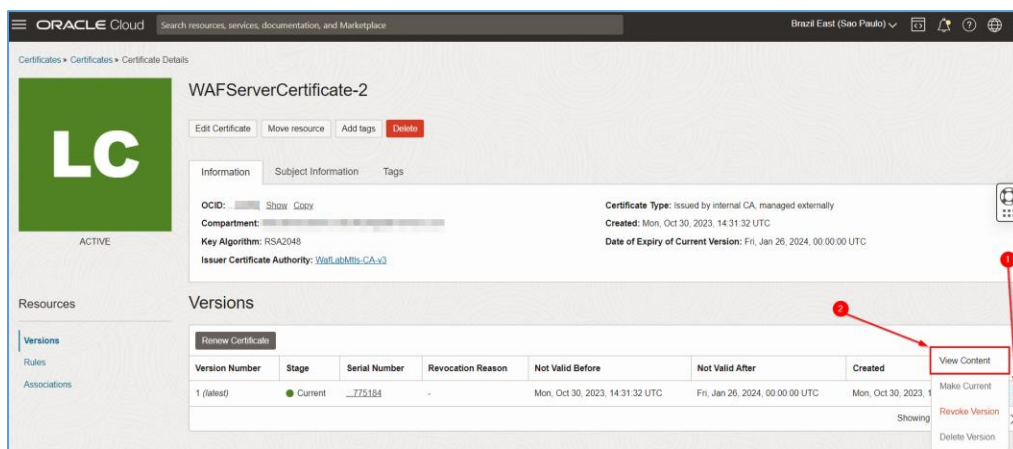
Para capturar a chave pública do certificado do Servidor, acesse o serviço OCI Certificates:



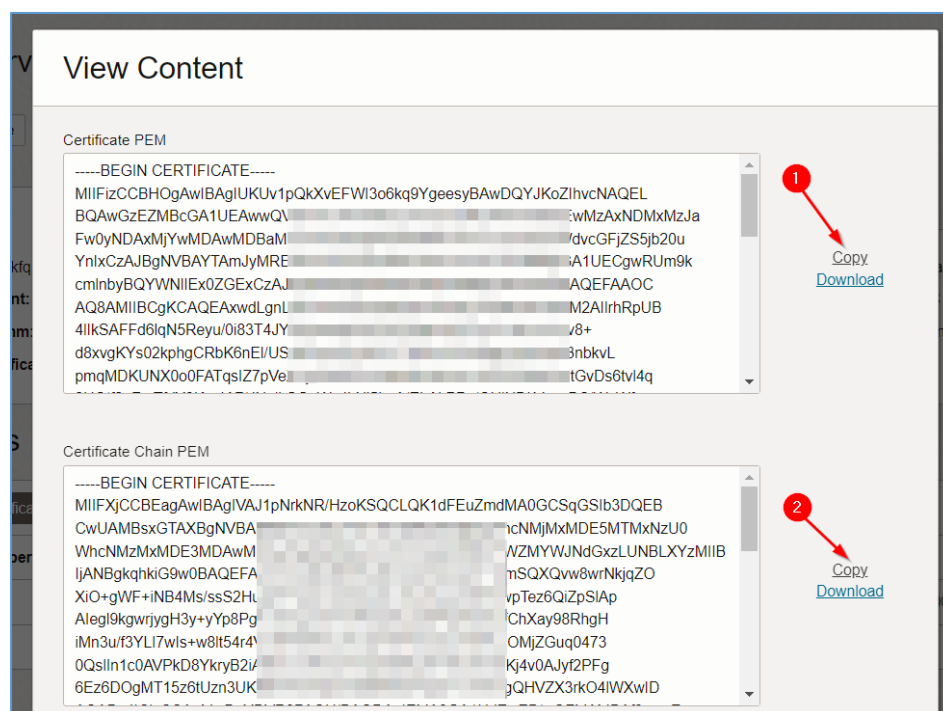
E em seguida, clique no nome do certificado do Servidor criado anteriormente:



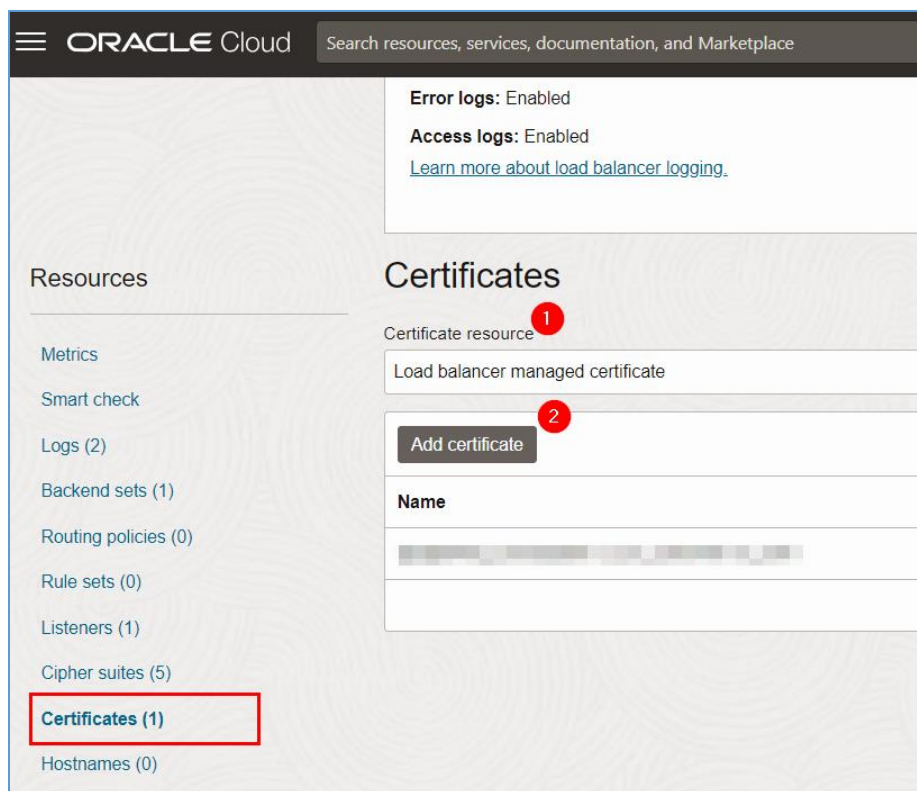
Ao clicar no nome do certificado, clique no menu da direita e em “View Content”:



Uma vez carregada a página dos dados do certificado copie e armazene as informações do “Certificate PEM” e “Certificate Chain PEM”:



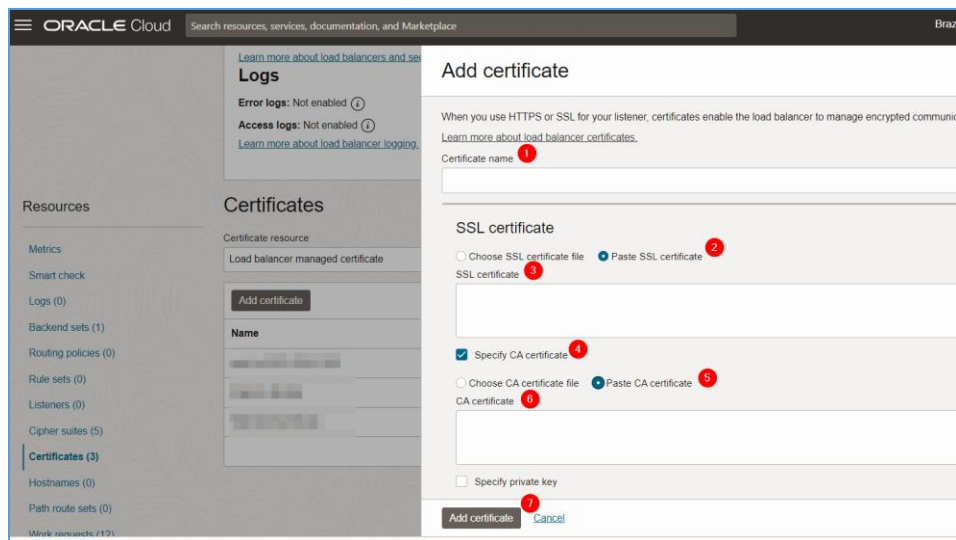
Agora que as informações do certificado foram armazenadas para inserção no Load Balancer, volte à página do OCI Load Balancer. Para inserir o certificado SSL no OCI Load Balancer, no menu “Resources” clique em “Certificates”:



Onde:

1. **Certificate resource:** Selecione “Load balancer managed certificate”;

Ao selecionar, clique no botão “Add certificate” para poder adicionar o certificado do Servidor no Load Balancer. Ao clicar, a tela de inserção do certificado será carregada:



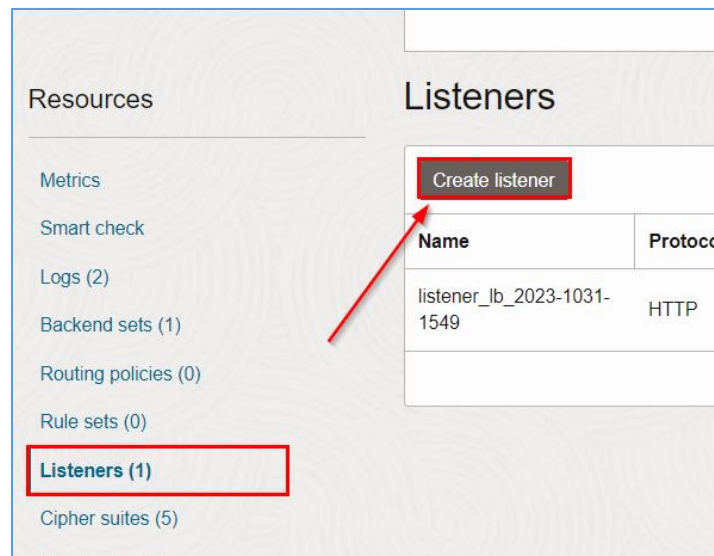
Onde:

1. **Certificate name:** Digite o nome do certificado do Servidor a ser importado;
2. **Paste SSL Certificate:** Em “SSL Certificate”, selecione “Paste SSL Certificate” para poder habilitar a possibilidade de colar o conteúdo registrado de “Certificate PEM” no passo anterior;
3. **SSL certificate:** Cole o conteúdo de “Certificate PEM” no campo;
4. **Specify CA certificate:** Selecione essa caixa para habilitar a possibilidade de colar o conteúdo registrado de “Certificate Chain PEM”;
5. **CA certificate:** Cole o conteúdo de “Certificate Chain PEM” no campo.

Após preencher os campos, clique no botão “Add certificate” para adicionar o certificado do Servidor no Load Balancer.

4.2 – Habilitar SSL no OCI Load Balancer

Após inserir o certificado do Servidor no Load Balancer, inicie a configuração do SSL no OCI Load Balancer. Para isso, clique no menu “Listeners”. A página com o listener criado será mostrada. Nela, clique no botão “Create listener”:



Ao clicar, a página de criação do listener será carregada. Preencha as informações requeridas para criar o listener HTTPS no Load Balancer e ativar a configuração do mTLS:

Edit listener

To allow your load balancer to accept ingress traffic, specify the protocol and port for your public IP address.

Name ¹ *Read-only*
listener_https

Protocol ²
HTTPS

Port ³
443

Use SSL ⁴
☒

Certificate resource ⁵
Load balancer managed certificate

Certificate name ⁶
WAFServerCertificate-2

Verify peer certificate ⁷
☒

Verify depth *Optional*
1

There are no hostnames for this load balancer. [Create a hostname.](#)

Backend set ⁸
backendset_ssl_intermediate

Ensure your backend health check protocol matches the listener protocol.

[Save changes](#) [Cancel](#)

Onde:

6. **Name:** Informe um nome para o listener a ser criado;
7. **Protocol:** Selecione HTTPS;
8. **Port:** O valor 443 será autopreenchido;
9. **Use SSL:** Selecione esta caixa para habilitar o HTTPS no listener do seu Load Balancer;
10. **Certificate resource:** Selecione “Load balancer managed certificate”;
11. **Certificate name:** Procure pelo certificado do Servidor e selecione-o;
12. **Verify peer certificate:** Selecione esta caixa para habilitar o mTLS no seu Load Balancer;
13. **Backend set:** Selecione o backend set criado para o API Gateway conforme feito anteriormente

Após preencher todos os dados corretamente, clique no botão “Save changes”.

Uma vez feito este processo, o OCI Load Balancer possuirá um listener em HTTPS e que utiliza mTLS para validar a autenticidade das conexões que chegam até ele.

Feito isso já podemos testar a conectividade HTTPS do Listener do OCI Load Balancer e, também, testar o mTLS.

4.3 – Teste de conectividade HTTPS e mTLS no OCI Load Balancer

O teste de conectividade HTTPS e mTLS pode ser feito via Curl. Para isso, execute o seguinte comando abaixo:

```
$ curl --cacert ca-cert.pem --key client-key.pem --cert client-cert.pem -k --location 'https://<IP_Load_Balancer>/v1/hello'
```

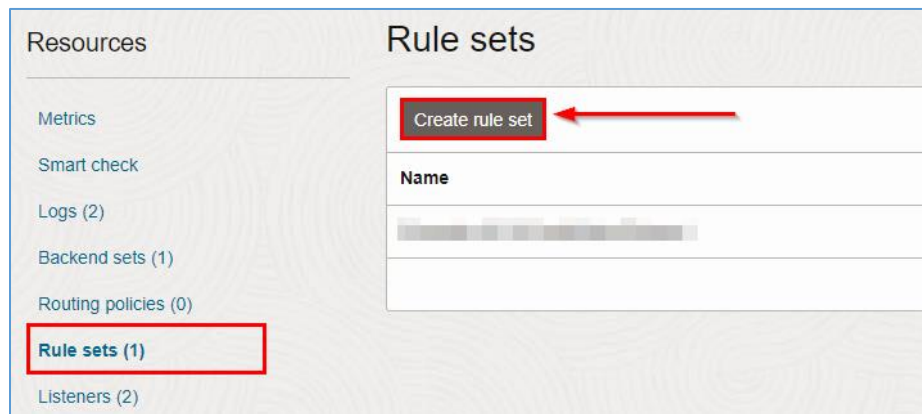
Ao executar este comando, o comando Curl deverá ter sucesso em se conectar ao Load Balancer utilizando HTTPS e mTLS e, por fim, fazer acesso à OCI Function que está configurada como backend do OCI API Gateway.

Nota: Caso o comando Curl não funcione corretamente, habilite os logs do Deployment do API Gateway e do Load Balancer para realizar o troubleshooting do ambiente.

4.4 – Encaminhamento de certificado SSL para o backend do OCI Load Balancer

É possível realizar o encaminhamento para o backend do Load Balancer do certificado utilizado pelo cliente para fechar a sessão mTLS. Para isso, é preciso configurar uma Rule Set no Load Balancer e aplica-la ao Listener ativo na porta 443.

Para configurar a Rule Set, no link “Rule sets” do menu “Resources” do seu OCI Load Balancer, clique no botão “Create rule set”:



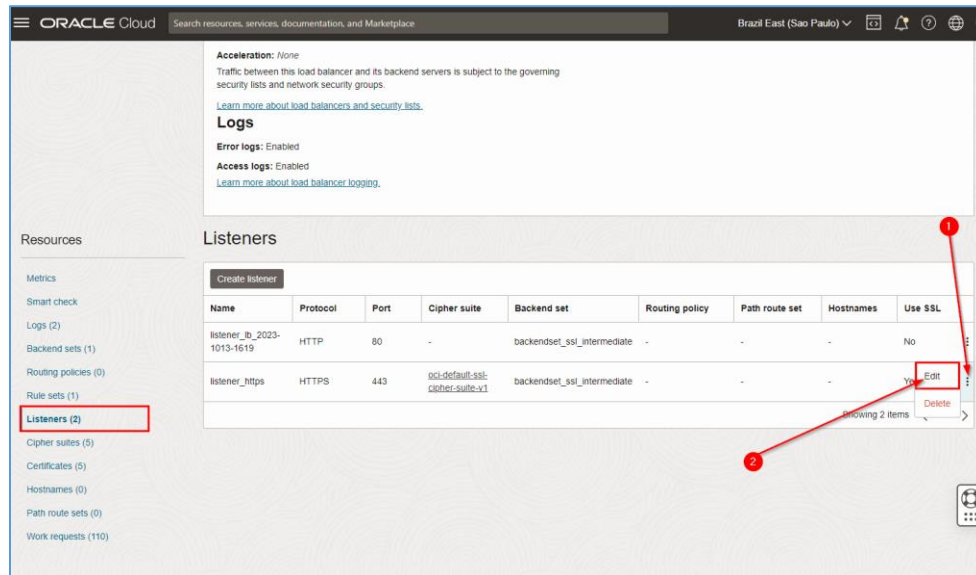
Ao clicar no botão, preencha as informações conforme requisitado:

Onde:

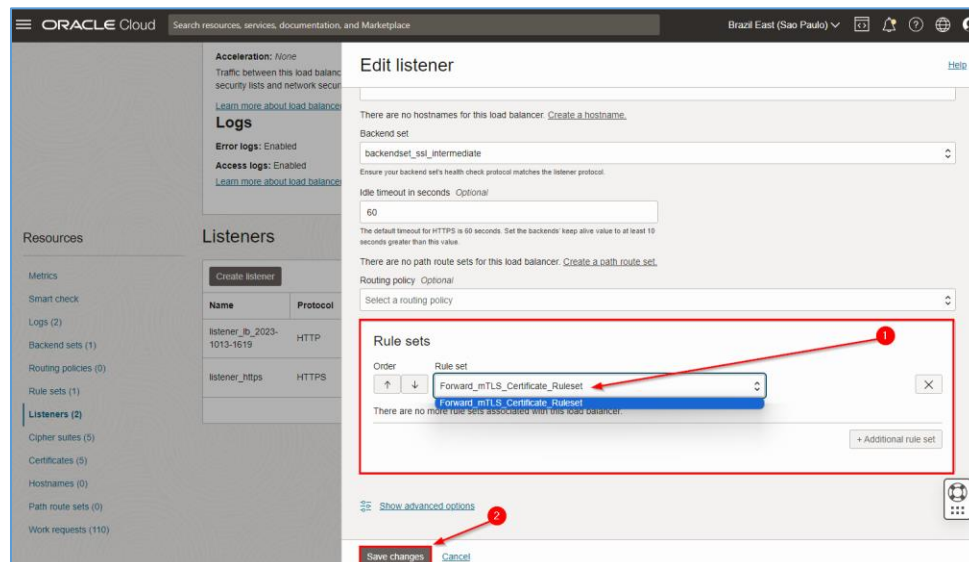
1. **Name:** Digite o nome da rule set a ser criada,
2. **Specify request header rule:** Selecione este campo para que seja possível criar uma regra de processamento de request headers,
3. **Header:** Informe o nome do header a ser inserido no cabeçalho da requisição HTTPS. Este request header conterá o certificado SSL utilizado pelo cliente para conectividade mTLS e este cabeçalho será enviado para o backend do OCI Load Balancer, ou seja, para o OCI API Gateway,
4. **Value:** Preencha o valor “`{oci_lb_client_cert_url_encoded}`”. Mais detalhes sobre esta variável do OCI Load Balancer podem ser encontrados neste [link](#) de documentação.

Uma vez preenchidos os valores, clique no botão “Create”.

Ao finalizar a criação da Rule Set, será necessário implementá-la no Listener ativo na porta 443/TCP do seu Load Balancer. Para isso clique em “Listeners” e edite as configurações do seu listener ativo na porta 443:



Ao editar, uma tela contendo os detalhes do Listener será aberta:



Nesta tela, em “Rule sets”, selecione a rule set recém criada e clique no botão “Save changes”. A partir de agora o certificado do cliente será sempre enviado via request header para o OCI API Gateway.

5 – Referências

Antes do uso deste material, recomendamos a leitura dos links de referência e documentações oficiais para administração de ambientes Oracle cloud.

OCI Logging:

<https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm>

OCI Custom Logs

https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/custom_logs.htm

OCI Dynamic Groups

<https://docs.oracle.com/en-us/iaas/data-science/using/create-dynamic-groups.htm>

OCI Logs and Logging Groups

<https://docs.oracle.com/en-us/iaas/Content/Logging/Task/managinglogs.htm>

OCI Functions

<https://docs.oracle.com/pt-br/iaas/Content/Functions/Concepts/functionsshowitworks.htm>

OCI Service Connector

<https://docs.oracle.com/pt-br/iaas/Content/service-connector-hub/overview.htm>

OCI Auth Token

<https://docs.oracle.com/pt-br/iaas/Content/Registry/Tasks/registrygettingauthtoken.htm>

Using Microsoft Azure Sentinel SIEM tools with OCI Logging service

<https://blogs.oracle.com/cloud-infrastructure/post/using-microsoft-azure-sentinel-siem-tools-with-oci-logging-service>

