Criar conta no oracle

Instalar node-red na VM

Testar Mqtt

**Parte 1 — Criar Conta na Oracle Cloud**

1) Acesse https://www.oracle.com/cloud/free e clique em Start for Free.

2) Create your account: preencha First Name, Last Name, Email, Country e defina a Password.

3) Email verification: confirme pelo link recebido.

4) Payment information: informe credit card internacional físico. Cartão virtual geralmente falha. Sem cobranças se permanecer no Always Free (pode haver autorização de US$0–US$1).

5) Home Region: selecione (ex.: Brazil East (São Paulo) ou US East (Ashburn)).

6) Se PJ: Company Name e Tax ID (CNPJ). PF: dados pessoais (CPF).

7) Phone verification e Review & Accept → Create Account.

8) Acesse o console em <https://cloud.oracle.com>.

**Parte 2 — Criar a VM (Always Free)**

1) Console: Menu → Compute → Instances → Create Instance.

2) Basic information: Name = NodeRED-Server; Availability domain = AD-1; Capacity type = on-demand; Fault domain = Let Oracle choose the best fault domain.

3) Image and shape: Image → Change image → Canonical Ubuntu 22.04; Security → Shielded instance: default; Shape → Change shape → VM.Standard.E2.1.Micro (Always Free-eligible).

4) Networking: Create new virtual cloud network + Create new public subnet (CIDR 10.0.0.0/24). Public IPv4 address: Yes (em public subnet vem automático). Use network security groups: No.

5) SSH keys: Generate an SSH key pair → baixe a .pem (privada) e a public key.

6) Boot volume: default ≈46.6 GB (~50 GB), criptografia Oracle-managed. Sem block volumes.

7) Management / Availability configuration: default.

8) Create.

**Parte 3 — Abrir portas na Security List (subnet pública)**

Caminho: Menu → Networking → Virtual Cloud Networks → sua VCN → Security Lists → abra a lista da public subnet.

Adicione Ingress Rules (stateful): TCP 22, TCP 1880, TCP 1883 (todas de 0.0.0.0/0).

Garanta Egress Rule ampla: All protocols para 0.0.0.0/0.

Se criou nova Security List, associe em: VCN → Subnets → sua subnet → Security Lists → Add Security List.

Obs.: ICMP/ping pode não funcionar; teste pelas portas

**Parte 4 — Encontrar o IP público**

Menu → Compute → Instances → NodeRED-Server → Instance Information → Public IP Address.

**Parte 5 — SSH (cliente)**

Windows (PuTTY): converta .pem em .ppk (PuTTYgen); no PuTTY, Host: ubuntu@; selecione a .ppk em Connection → SSH → Auth.

**Instalação recomendada (via script oficial Node-RED)**

1. Atualize os pacotes:

sudo apt update && sudo apt upgrade -y

1. Instale o Node-RED com o script oficial (instala Node.js + Node-RED + npm):

bash <(curl -sL https://raw.githubusercontent.com/node-red/linux-installers/master/deb/update-nodejs-and-nodered)

1. Configure para iniciar automaticamente no boot:

sudo systemctl enable nodered.service

1. Inicie o serviço:

sudo systemctl start nodered.service

1. Verifique o status:

systemctl status nodered.service

1. Acesse pelo navegador:

http://144.33.16.207:1880

teste de porta

Test-NetConnection 144.33.16.207 -Port 22

Test-NetConnection 144.33.16.207 -Port 1880

Test-NetConnection 144.33.16.207 -Port 1883

Aí não conecta

Faz no VM do linux

# ver a ordem atual com números de linha

sudo iptables -L INPUT -n -v --line-numbers

# inserir ACCEPT para 1880 no topo (antes do REJECT)

sudo iptables -I INPUT -p tcp --dport 1880 -m state --state NEW -j ACCEPT

# (opcional) se usar MQTT 1883 também:

sudo iptables -I INPUT -p tcp --dport 1883 -m state --state NEW -j ACCEPT

# conferir que as novas regras ficaram ACIMA do REJECT:

sudo iptables -L INPUT -n -v --line-numbers

sudo nft insert rule ip filter INPUT tcp dport 1880 ct state new accept

# (e para 1883, se necessário)

sudo nft insert rule ip filter INPUT tcp dport 1883 ct state new accept

sudo nft list ruleset

sudo apt-get update

sudo apt-get install -y iptables-persistent

sudo iptables-save | sudo tee /etc/iptables/rules.v4 >/dev/null

sudo nft list ruleset | sudo tee /etc/iptables/rules.nft >/dev/null || true

instalando o Mosquitto

**e não tiver, duas formas de instalar**

**A) Bare-metal (rápido para teste)**

sudo apt update

sudo apt install -y mosquitto mosquitto-clients

# (opcional p/ teste simples — abre sem senha. Remova depois.)

echo -e "listener 1883\nallow\_anonymous true" | sudo tee /etc/mosquitto/conf.d/open.conf

sudo systemctl enable --now mosquitto

systemctl status mosquitto

ss -ltnp | grep :1883

Como seu host tem uma regra REJECT cedo no INPUT, garanta o ACCEPT **antes**:

sudo iptables -I INPUT -p tcp --dport 1883 -m state --state NEW -j ACCEPT

sudo iptables -L INPUT -n -v --line-numbers | sed -n '1,50p'

Teste local:

# em um terminal:

mosquitto\_sub -h 127.0.0.1 -t teste -v

# em outro:

mosquitto\_pub -h 127.0.0.1 -t teste -m "ping"

Teste externo (Windows):

Test-NetConnection 144.33.16.207 -Port 1883

Manutencao

sudo cp /etc/mosquitto/conf.d/open.conf /etc/mosquitto/conf.d/open.conf.bak && \

echo -e 'listener 1883 0.0.0.0\nallow\_anonymous true' | sudo tee /etc/mosquitto/conf.d/open.conf