

# Guia de Laboratório: Infraestrutura como Serviço (IaaS)

## Laboratório 1: Provisionamento e Publicação Web com Nginx

Este guia detalha os comandos práticos executados na aula. Ele serve como referência para que você possa reproduzir o experimento em seu ambiente *Always Free* (usaremos o contexto de um provedor como o Oracle Cloud Infrastructure ou AWS/GCP Free Tier, onde o usuário padrão é tipicamente `ubuntu` ou `ec2-user`).

### Pré-requisitos:

1. Uma instância de VM Linux (ex: Ubuntu 22.04 LTS) provisionada.
2. Acesso ao **IP Público** da sua instância.
3. Sua **Chave Privada SSH** (`oci_key.pem`) com permissões corretas (`chmod 400`).
4. A **Porta 22 (SSH)** e a **Porta 80 (HTTP)** abertas no **Firewall da Nuvem** (Security Group/Security List).

---

## Passo 1: Configuração Inicial da Chave Privada

Antes de se conectar, garanta que sua chave privada tem as permissões mínimas de segurança exigidas pelo cliente SSH.

Comando	Função
<code>cd ~/keys</code>	Navega até o diretório onde sua chave está salva (ajuste o caminho).
<code>chmod 400 oci_key.pem</code>	Altera as permissões para que apenas o proprietário possa ler o arquivo.

Exportar para as Planilhas

**Output Esperado:** *Nenhum output de sucesso. O comando é silencioso.*

---

## Passo 2: Conexão Segura via SSH

Use o IP Público da sua VM e o nome de usuário padrão do sistema operacional (aqui, `ubuntu` para uma imagem Ubuntu).

Comando	Função
---------	--------

`ssh -i oci_key.pem ubuntu@150.230.123.456` Inicia a conexão: `-i` especifica a chave de identidade, seguido pelo usuário e IP da VM.

Exportar para as Planilhas

### Output Esperado (Primeira Conexão):

Bash

```
The authenticity of host '150.230.123.456 (150.230.123.456)' can't be established.  
ECDSA key fingerprint is SHA256:.....  
Are you sure you want to continue connecting (yes/no/[fingerprint])? **yes**  
Warning: Permanently added '150.230.123.456' (ECDSA) to the list of known hosts.  
Welcome to Ubuntu 22.04 LTS (...)  
ubuntu@instance-20251029:~$
```

### Comentários:

- Você deve digitar **yes** na primeira vez para aceitar a chave do host.
- O prompt muda para `ubuntu@instance-...:~$`, indicando que você está logado dentro da sua VM na Nuvem.

---

## Passo 3: Atualização do Sistema e Instalação do Nginx

Agora que estamos dentro da VM, vamos garantir que o sistema operacional esteja atualizado e instalar o servidor web.

Comando	Função
<code>sudo apt update</code>	Atualiza a lista de pacotes disponíveis do repositório (não instala nada, apenas o índice).
<code>sudo apt install -y nginx</code>	Instala o servidor web Nginx e a flag <code>-y</code> confirma automaticamente a instalação.

Exportar para as Planilhas

### Output Esperado (após a instalação do Nginx):

Bash

```
(...)  
Setting up nginx-common (1.18.0-6ubuntu14.4) ...  
Processing triggers for man-db (2.10.2-1) ...  
Processing triggers for ufw (0.36.1-4) ...  
Processing triggers for libc-bin (2.35-0ubuntu3.4) ...  
ubuntu@instance-20251029:~$
```

---

## Passo 4: Verificação do Serviço e Firewall Interno (UFW)

A instalação do Nginx geralmente o inicia automaticamente. Também vamos garantir que o firewall interno do SO (UFW) permita o tráfego web, embora muitas imagens de nuvem venham com ele desativado.

Comando	Função
<pre>sudo systemctl status nginx</pre>	Verifica o status do serviço Nginx.
<pre>sudo ufw allow 'Nginx HTTP'</pre>	(Opcional, mas boa prática) Adiciona uma regra no firewall interno UFW para a porta 80.
<pre>sudo ufw enable</pre>	(Opcional) Ativa o firewall interno UFW. <b>Cuidado:</b> Verifique se a porta 22 (SSH) também está permitida antes de ativar.

Exportar para as Planilhas

### Output Esperado (`systemctl status nginx`):

Bash

- nginx.service - A high performance web server and a reverse proxy server  
Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)  
Active: \*\*active (running)\*\* since Wed 2025-10-29 11:45:00 UTC; 1min 2s ago  
(...)

---

## Passo 5: Teste de Acesso Público

Com a VM ativa, Nginx rodando e as portas 80/22 abertas na nuvem (Security List) e no SO (UFW), o servidor deve estar acessível.

Ação	Resultado
Abrir Navegador Web	Navegue para: <code>http://[IP_PÚBLICO_DA_SUA_VM]</code>

Exportar para as Planilhas

### Resultado Esperado:

- Você verá a página padrão do Nginx que diz: **"Welcome to nginx! If you see this page, the nginx web server is successfully installed and working."**

## Diagnóstico Rápido:

- **Se a página carregar:** Parabéns! Você provisionou e configurou com sucesso sua primeira IaaS.
  - **Se a página não carregar (Time Out):** O problema está no **Firewall da Nuvem** (Security List/Group). Revise a regra da porta 80.
  - **Se você receber uma mensagem de erro do servidor:** O Nginx não está rodando. Revise o Passo 4.
- 

## Passo 6: Desafio de Expansão (Opcional)

Altere o conteúdo padrão para personalizar sua página.

### Editar o arquivo HTML padrão do Nginx:

Bash

```
$ sudo nano /var/www/html/index.nginx-debian.html
```

- 1.
2. **Alterar o Conteúdo:**
  - Use as setas para navegar no editor **nano**.
  - Substitua o conteúdo dentro da tag **<body>** pelo seguinte:

HTML

```
<body>
```

```
  <h1>Parabéns! Servidor IaaS do Professor [Seu Nome] Ativo!</h1>
```

```
  <p>Esta é a sua primeira aplicação hospedada em Infraestrutura como Serviço na Nuvem.</p>
```

```
</body>
```

- 3.
4. **Salvar e Sair do Nano:** Pressione **Ctrl+O** (para Salvar) e depois **Ctrl+X** (para Sair).
5. **Recarregar no Navegador:** Atualize a página no seu navegador.

**Resultado Esperado:** Sua mensagem personalizada será exibida!

---

## Comandos Finais (Desligamento)

Lembre-se de parar a instância para evitar custos, a menos que esteja usando um recurso **Always Free**:

Comando (Na VM)	Função
<code>exit</code>	Sai da conexão SSH.

Exportar para as Planilhas

Ação (No Console da Nuvem)	Função
----------------------------------	--------

<b>Stop Instance</b>	Para a VM, interrompendo a cobrança por CPU/RAM, mas mantendo o disco (necessário para o próximo laboratório).
----------------------	--