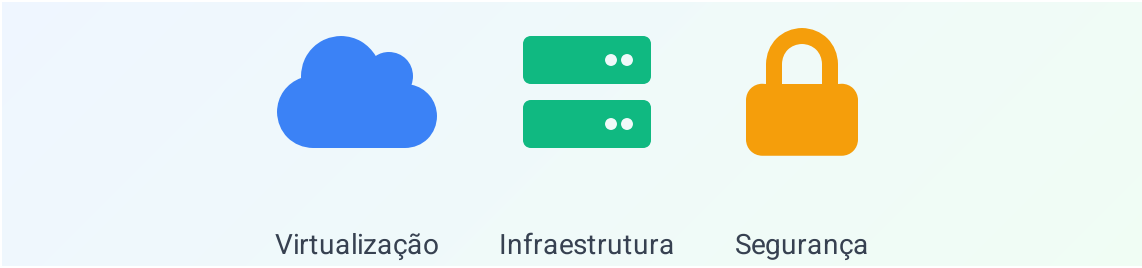
Configuração Básica de Máquina Virtual (VM) e Segurança Inicial

Aula 13 - Unidade Curricular 3

Aprenda a provisionar máquinas virtuais em ambientes cloud, configurar rede e implementar políticas de segurança essenciais para bancos de dados.



Como as empresas criam centenas de servidores rapidamente e de forma flexível?

A Resposta: Virtualização

Virtualização é a tecnologia que permite rodar múltiplos sistemas operacionais dentro de um único computador físico. Cada máquina virtual (VM) tem seu próprio hardware virtual (CPU, RAM, Disco), mas compartilha o hardware físico real.

Na nuvem (AWS, Azure, GCP), você não instala software de virtualização localmente. Em vez disso, você usa a **Web Console** dos provedores para provisionar VMs em segundos. Isso permite que empresas escalem sua infraestrutura de forma rápida e econômica.

Nesta aula, vamos aprender os **conceitos fundamentais** de VM, provisão de recursos, configuração de rede e segurança inicial.

Conceitos Fundamentais da Virtualização

Máquina Virtual (VM)

Uma **simulação de um computador físico** com seu próprio hardware virtual (CPU, RAM, Disco). Funciona como um computador real, mas é executada dentro de outro computador.

Hypervisor

O **software que gerencia as VMs**. Exemplos: VirtualBox, VMware, ou o sistema de gerenciamento de um provedor cloud (AWS, Azure, GCP).

Provisão de Recursos

O processo de **alocar recursos** (CPU, RAM, Disco) para uma VM. Você decide quanto de cada recurso a VM terá.

Atividade 1: Alocação de Recursos - Parte 1

Por que escolher um SO mínimo (Linux)?

Um SO mínimo como **Ubuntu Server** ou **Red Hat** não tem interface gráfica (GUI). Isso economiza recursos (CPU e RAM) que são críticos para um banco de dados. O servidor roda apenas via terminal, sendo leve e eficiente.

Processador (vCPUs)

2 vCPUs

Memória (RAM)

4 GB

Passo a Passo de Simulação

1. **Acessar a Console do Provedor Cloud**

   Abra a Web Console da AWS (EC2), Azure (Virtual Machines) ou GCP (Compute Engine).

2. **Escolher a Imagem do SO**

   Selecione **Ubuntu Server 22.04 LTS** (ou Red Hat Enterprise Linux). Esta é a imagem mínima sem GUI.

3. **Definir Tamanho da Instância**

   Selecione um tipo de instância com **2 vCPUs** e **4 GB de RAM**. Exemplos: AWS t3.medium, Azure Standard_B2s, GCP e2-medium.

Atividade 1: Alocação de Recursos - Parte 2

3 Definição de Tamanho (Allocation)

Simule a alocação de recursos: **"Vamos dar 2 vCPUs e 4GB de RAM para este servidor de banco de dados."**

- **2 vCPUs:** Duas unidades de processamento virtual (suficiente para um banco de dados pequeno a médio)
- **4GB RAM:** Memória para cache do banco de dados e operações em memória
- **Disco:** Escolha um tamanho apropriado (ex: 50GB para começar)

4 Criação da VM

Clique em **"Create"** ou **"Launch"** para iniciar o processo de provisão da VM.

- A nuvem começará a alocar os recursos que você especificou
- Isso pode levar alguns segundos a alguns minutos
- Você receberá uma confirmação quando a VM estiver pronta

5 Verificação e Confirmação

Confirme que a VM foi criada e está **rodando**.

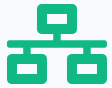
- Verifique o status da VM (deve estar como **"Running"** ou **"Active"**)
- Anote o **IP privado** atribuído à VM (você usará isso para conectar)
- Verifique se os recursos foram alocados corretamente (2 vCPUs, 4GB RAM)

Três Tipos de Rede para Máquinas Virtuais

Interna/NAT

- VM recebe IP **privado**
- Usa IP do host para acessar internet
- **Segura**, mas ruim para acesso externo

Exemplo: 192.168.1.100



Bridge

- VM se comporta como computador **real**
- Recebe seu próprio IP na rede
- **Flexível**, mas exige atenção à segurança

Exemplo: 192.168.0.50

VPC/VNet (Nuvem)

- VM obtém IP **privado** em sub-rede controlada
- Rede isolada e gerenciada
- **Padrão em nuvem** (AWS, Azure, GCP)

Exemplo: 10.0.1.25

Atividade 2: Configuração de Rede e Testes de Conectividade

ℹ️ As duplas devem trabalhar no terminal da VM criada no Bloco 1. Vocês testarão a conectividade de saída (acesso à internet) e descobrirão o IP privado da VM.

Tarefa 1: Testes de Conectividade

1. **Ping de Saída:** Teste se a VM pode acessar a internet

```
$ ping google.com
```

2. **Identificação do IP:** Descubra o IP privado (VPC) da VM

```
$ ip addr
ou
$ ifconfig
```

3. **Documentação:** Anote o IP privado (ex: 10.0.1.5) em um arquivo de texto

Tarefa 2: Conexão Remota SSH

1. **Entender SSH:** A conexão remota é feita via SSH na **porta 22** (padrão)
2. **Portas do SGBD:** O banco de dados rodará em uma porta específica:

```
PostgreSQL: porta 5432
MySQL: porta 3306
```

3. **Importância:** Essas portas precisam estar **abertas no firewall** para que aplicações externas possam se conectar

Instalação de SO Mínimo e Segurança Inicial

Login Pós-Instalação

Após instalar um SO Linux mínimo (como Ubuntu Server), o primeiro login é feito via **terminal**. Não há interface gráfica (GUI) - tudo é feito por linhas de comando.

Você receberá um prompt como este:

```
ubuntu@server:~$
```

Isto significa que você está logado como usuário **"ubuntu"** no servidor chamado **"server"**.

Scripts de Atualização

A primeira coisa a fazer é **atualizar o sistema**. Isso garante que você tenha as últimas correções de segurança.

1. Atualizar lista de pacotes:

```
$ sudo apt update
```

Baixa a lista de pacotes disponíveis

2. Atualizar pacotes instalados:

```
$ sudo apt upgrade -y
```

Instala atualizações de segurança (-y = sim automático)

> ⚠️ **Importante:** Sempre execute essas atualizações antes de instalar qualquer banco de dados!

Atividade 3: Configuração de Firewall e Segurança

Conceito: Security Groups e Network Security Groups

Na nuvem, o firewall não é instalado localmente. Em vez disso, você configura **Security Groups (AWS)** ou **Network Security Groups - NSGs (Azure/GCP)**. Esses são regras que controlam quem pode entrar e sair da VM.

Lógica: Por padrão, tudo é bloqueado. Você abre apenas as portas que precisa (SSH porta 22, SGBD porta 5432/3306, etc).

Simulação Prática: Configuração com UFW (Linux Firewall)

ℹ️ **Instrução:** As duplas devem usar o terminal da VM para configurar o firewall mínimo. Mesmo que o firewall da nuvem já esteja ativo, vamos configurar o firewall **dentro do servidor** para aprender a lógica.

1. **Permitir SSH (porta 22):** Essencial para administração remota. Faça isso ANTES de ativar o firewall!

```
$ sudo ufw allow 22/tcp
```

2. **Permitir Banco de Dados (porta 5432 para PostgreSQL):** Permite que aplicações se conectem ao BD

```
$ sudo ufw allow 5432/tcp
```

3. **Ativar o Firewall:** Bloqueia tudo que não foi explicitamente permitido

```
$ sudo ufw enable
```

Validação e Consolidação

Checklist de Validação

- ☐ VM foi criada com sucesso na nuvem
- ☐ SO mínimo (Linux) foi instalado
- ☐ Executou apt update e apt upgrade
- ☐ Testou conectividade com ping
- ☐ Recursos alocados: 2 vCPUs e 4GB RAM
- ☐ Conseguiu fazer login via terminal
- ☐ Identificou o IP privado da VM
- ☐ Configurou firewall básico (UFW)

Síntese: Por que Tudo Isso Importa

VM e rede são a fundação de qualquer projeto de banco de dados. Sem uma infraestrutura bem configurada, seu banco de dados não terá:

- **Isolamento:** Proteção contra outros serviços rodando no mesmo hardware
- **Escalabilidade:** Capacidade de aumentar recursos quando necessário
- **Segurança:** Firewall e controle de acesso para proteger dados
- **Disponibilidade:** Possibilidade de fazer backup e recuperação

Você agora está pronto para instalar um **SGBD (PostgreSQL ou MySQL)** nesta infraestrutura segura e bem configurada!

Conclusão: Próximos Passos

Você está pronto!

Você aprendeu os fundamentos essenciais de infraestrutura em nuvem. Agora você compreende como provisionar máquinas virtuais, configurar rede e implementar segurança básica. Esses conhecimentos são a base para qualquer profissional de dados que trabalha com bancos de dados em produção.

Próximos Passos Práticos

Instalar SGBD

Instale PostgreSQL ou MySQL na VM que você criou. Use apt install postgresql ou apt install mysql-server.

Configurar Segurança

Configure senhas fortes, crie usuários específicos para o BD e ajuste as permissões de acesso.

Monitorar e Otimizar

Monitore CPU, memória e disco. Otimize queries e índices para melhor performance.

Parabéns! Você completou a Aula 13. Agora você tem as habilidades para gerenciar infraestrutura de dados em ambientes profissionais. Continue aprendendo e praticando!