

PROVA DISCURSIVA - RESPOSTAS TÉCNICAS

Candidato: Rodrigo Eloi

BLOCO 1 – FLUXO DE TRÁFEGO REAL

1. Fluxo Completo de Requisição

1. **Navegador:** O usuário digita a URL. A resolução DNS ocorre aqui, apontando o domínio para a Cloudflare (ou IP Público da EC2, dependendo da configuração final de DNS).
2. **Internet Gateway (IGW):** A requisição entra na VPC AWS através do IGW.
3. **EC2 Pública (Proxy):** O tráfego chega na porta 80/443. Aqui ocorre o **encerramento do TLS** (se configurado HTTPS no Nginx) e o Nginx atua como **Proxy Reverso**.
4. **Comunicação Interna:** O Nginx encaminha a requisição para a aplicação Node.js (via `localhost:3000` ou IP privado).
5. **Container da Aplicação:** O Node.js processa a lógica e precisa de dados.
6. **EC2 Privada (Banco):** A aplicação abre uma conexão TCP na porta 5432 para o IP Privado da EC2 de Banco (`10.0.x.x`). O Security Group da privada autoriza essa entrada.
7. **Retorno:** O banco responde para o App -> App responde para o Nginx -> Nginx responde para o Usuário.

2. Falha Parcial de Tráfego (Erro 504 Gateway Timeout) *Cenário: Proxy responde, mas App retorna 504. Ordem de Investigação:*

1. **Conectividade com o Banco (Security Group):** Verificar se a EC2 Privada está aceitando conexões na porta 5432 vindas da Pública. *Justificativa:* O erro 504 no Nginx geralmente significa que o Node.js travou esperando uma resposta (timeout) do banco, que é o bloqueio mais comum (firewall silencioso).
2. **Status do Container de Banco:** Verificar se o container Docker do PostgreSQL está rodando (`docker ps`). *Justificativa:* Se a rede está ok, o serviço pode ter caído.
3. **Recursos da EC2 Aplicação:** Verificar se a CPU/Memória da EC2 Pública está em 100%. *Justificativa:* Se a máquina travou, o Node.js não consegue processar a volta.

BLOCO 2 – REDE E ISOLAMENTO

3. **Subnet Privada na Prática** O que impede a EC2 privada de receber tráfego direto da internet é a **Route Table (Tabela de Rotas)** associada à Subnet Privada. Esta tabela **não possui uma rota apontando para o Internet Gateway (IGW)**. Mesmo que a instância

tivesse um IP público (o que não deve ter), o pacote não saberia como "voltar", pois o roteamento para `0.0.0.0/0` é inexistente ou aponta para um NAT local, nunca para o IGW direto.

4. NAT Gateway – Uso Real

- **Quem precisa:** A EC2 Privada (Banco de Dados).
- **Situação:** Necessário para baixar imagens Docker (`docker pull postgres`), instalar atualizações de segurança (`apt update`) ou instalar pacotes.
- **O que quebra:** Sem ele, o banco de dados fica isolado e não conseguimos instalar o Docker ou baixar a imagem do banco na primeira instalação. *(Nota: Nesta arquitetura, usamos a EC2 Pública como instância NAT via iptables para substituir o NAT Gateway pago).*

5. Security Groups vs Roteamento

- **Cenário:** As Tabelas de Rotas estão corretas, as máquinas se "pingam", mas a aplicação não conecta no banco.
- **Causa (Security Group):** O Security Group da **EC2 Privada** (`sgprovadb`) não tem uma regra de entrada (**Inbound Rule**) permitindo TCP na porta 5432 vindo da origem `10.0.0.0/16` (VPC CIDR).
- **Validação:** Executar `telnet IP_PRIVADO_BANCO 5432` ou `curl -v telnet://IP:5432` a partir da EC2 Pública. Se der "Timeout", é Security Group. Se der "No route to host", é Roteamento.

BLOCO 3 – PROXY E EXPOSIÇÃO

6. Nginx como Proxy Reverso Não basta apontar a Cloudflare direto para a aplicação (Node.js) porque:

- **Segurança:** O Nginx protege o servidor de aplicação contra ataques diretos, oculta headers de tecnologia (X-Powered-By) e gerencia melhor conexões lentas (Slowloris).
- **Manutenção:** Permite reiniciar a aplicação (Node.js) sem derrubar a conexão do usuário (o Nginx segura o pacote ou mostra uma página de manutenção amigável).
- **Observabilidade:** Os logs de acesso do Nginx são padronizados e mais fáceis de monitorar (status 200, 404, 500) do que logs brutos de console da aplicação.

7. HTTPS – Onde e Por Quê

- **Onde:** O HTTPS deve ser encerrado no **Nginx (EC2 Pública)** ou na **Cloudflare**.
- **Por que:** Para aliviar a carga de CPU da aplicação (Offloading SSL). O Node.js é *single-threaded*; gastar CPU descriptografando tráfego reduz a capacidade de processar regras de negócio.
- **Problema prático:** Encerrar TLS dentro do container da aplicação torna o gerenciamento de certificados complexo e consome recursos valiosos de processamento da aplicação.

BLOCO 4 – CONTAINERS EM EC2

8. Ordem de Subida dos Serviços

1. Inicialização das EC2 (Sistema Operacional).
2. Subida do Banco de Dados (Docker na Privada).
3. Subida da Aplicação (PM2/Node na Pública).
4. Liberação do Proxy (Nginx). *Se não respeitada*: Se a aplicação subir antes do banco, ela falhará na conexão inicial e poderá entrar em *loop* de reinicialização (CrashLoopBackOff) ou travar até que o banco esteja disponível.

9. Falha Após Reboot *Cenário: App não sobe, Banco OK.*

- **Verificar Primeiro**: Se o gerenciador de processos (PM2 ou Docker) foi configurado para iniciar no boot (`pm2 startup / docker update --restart always`).
- **Erro Comum**: Esquecer de rodar o comando `pm2 save` ou não habilitar o serviço do Docker no systemd (`systemctl enable docker`).
- **Como evitar**: Criar scripts de *User Data* ou garantir a configuração de persistência de serviço no setup inicial.

BLOCO 5 – OBSERVABILIDADE E DEBUG

10. Logs em Incidente Real *Usuários reclamam de lentidão.*

1. **Primeiro Log**: `access.log` do Nginx.
 - **O que procuro**: O tempo de resposta (`upstream_response_time`). Se for alto, a lentidão é na aplicação/banco. Se for baixo, a lentidão é na internet do usuário.
2. **Segundo Log**: Logs da Aplicação (`pm2 logs` ou `docker logs`). Procuro por *Slow Queries* ou erros de conexão com o banco.

11. Métricas Enganosas *CPU baixa, mas aplicação lenta.*

1. **I/O Wait**: O disco pode estar lento ou cheio, fazendo a CPU esperar (idle) enquanto grava logs ou dados.
2. **Latência de Rede/Banco**: A aplicação está parada esperando o banco de dados responder (Network Wait). Como o Node.js é assíncrono, ele não gasta CPU enquanto espera, mas para o usuário a requisição está parada.

BLOCO 6 – SEGURANÇA OPERACIONAL

12. Erro Comum de Security Group

- **Erro**: Liberar acesso SSH (Porta 22) para o "Meu IP" atual.
- **Por que quebra**: Provedores de internet mudam o IP (Dinâmico). No dia seguinte ("Produção"), o IP mudou e o administrador perde o acesso, bloqueando a manutenção.

13. Acesso Administrativo (Bastion vs SSM)

- **Risco do Bastion:** Exige expor a porta 22 para a internet e gerenciar chaves `.pem`. Se uma chave vazar (ex: dev subir no GitHub), a infraestrutura é comprometida.
- **Problema prático do SSM:** Exige instalação do Agente SSM e permissões de IAM corretas (`AmazonSSMManagedInstanceCore`). Se a instância estiver sem saída para internet (sem NAT) ou sem a Role correta, o acesso não funciona, dificultando o debug em emergências.

BLOCO 7 – DECISÕES E TRADE-OFFS

14. Banco em Container

- **Por que aceita:** Reduz custos (não paga RDS) e garante paridade entre ambiente de desenvolvimento local e produção na prova.
- **Inaceitável:** Em sistemas de missão crítica com grande volume de dados.
- **Risco:** Se o volume do Docker não for mapeado para o host (Bind Mount/Volume), ao recriar o container, **todos os dados são perdidos**. Além disso, o gerenciamento de backup e *failover* é manual.

15. Custo vs Segurança

- **Decisão:** Utilizar a EC2 Pública como instância NAT (via `iptables`) ao invés de um NAT Gateway Gerenciado.
- **Reduz Custo:** Economiza a taxa horária do NAT Gateway AWS (aprox. \$30/mês).
- **Aumenta Risco:** Cria um ponto único de falha. Se a EC2 Pública cair ou reiniciar, a EC2 Privada perde acesso à internet para atualizações.
- **Mitigação:** Scripts de monitoramento para reiniciar a rede ou, em produção real, migrar para NAT Gateway.

BLOCO 8 – INCIDENTE FINAL

16. Incidente Completo *Cenário: /health OK, mas erros intermitentes para usuários.*

- **Causa Provável:** Esgotamento do *Pool de Conexões* do Banco de Dados. O `/health` faz uma query simples (`SELECT 1`) e passa, mas quando muitos usuários acessam, o limite de `max_connections` do Postgres é atingido e novas conexões são rejeitadas.
- **Validação:** Monitorar a métrica de "Active Connections" no banco ou verificar logs de erro da aplicação por `FATAL: sorry, too many clients already`.
- **Ajuste:** Aumentar o `max_connections` no PostgreSQL ou configurar Pool de Conexões na aplicação (Ex: PgBouncer ou ajuste no driver do Node.js).

Informações

As regras de entrada controlam o tráfego de entrada que tem permissão para acessar a instância.

Regras de entrada

Informações

ID da regra do grupo de segurança

Tipo

Informações

Protocolo

Informações

Intervalo de portas

Informações

Origem

Informações

Descrição - opcional

Informações

sgr-08dc32cb9991319d9	<div>HTTP</div>	<div>TCP</div>	<div>80</div>	<div>Persona...</div>	<div>Q</div>	<div></div>	<div>Excluir</div>
sgr-0f60899858ff60e5f	<div>HTTPS</div>	<div>TCP</div>	<div>443</div>	<div>Persona...</div>	<div>Q</div>	<div></div>	<div>Excluir</div>
sgr-0751b706030bd4568	<div>SSH</div>	<div>TCP</div>	<div>22</div>	<div>Meu IP</div>	<div>Q</div>	<div></div>	<div>Excluir</div>

Adicionar regra

As regras com a origem 0.0.0.0/0 ou ::/0 permitem que todos os endereços IP acessem a instância. Recomendamos configurar as regras de grupo de segurança para permitir o acesso apenas de endereços IP conhecidos.

X

Cancelar

Visualizar alterações

Salvar regras

 |

Especificar detalhes do usuário

missões

tar

senha

Detalhes do usuário

Nome do usuário

validador-prova

O nome de usuário pode ter até 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , . @ _ - (href)

☒ Fornecer acesso para os usuários ao Console de Gerenciamento da AWS - opcional

Adm do acesso para os usuários não permissões SigninLocalDevelopmentAcessa podem usar as mesmas credenciais do console para acesso programático sem a necessidade de chaves de acesso.

Senha do console

☐ Senha gerada automaticamente

Você poderá visualizar a senha depois de criar o usuário.

☒ Senha personalizada

Insira uma senha personalizada para o usuário.

Prova@2026

• Deve ter pelo menos 8 caracteres

• Deve incluir pelo menos três dos seguintes tipos de combinação de caracteres: letras maiúsculas (A-Z), letras minúsculas (a-z), números (0-9) e os símbolos ! @ # \$ % ^ & * () _ + - (href) = {} |] ' "

☒ Mostrar senha

☒ Os usuários devem criar uma nova senha na próxima sessão (recomendado).

Os usuários obtêm automaticamente a política `IAMUserChangePassword` para permitir que eles alterem sua própria senha.

Se você estiver criando acesso programático por meio de chaves de acesso ou credenciais específicas de serviço para o AWS CodeCommit ou o Amazon Keyspaces, poderá gerá-las depois de criar esse usuário do IAM. [Saiba mais](#)

[Grupos de segurança](#) > sg-05347fd03a3485bd0 - sgprovaadb

sg-05347fd03a3485bd0 - sgprovadb

[illegible]

roundness

ações

<input type="text" value="Localizar instância por atributo ou tag (case-sensitive)"/> <input type="button" value="Todos os estados"/>										
<input type="button" value="Estado da instância = running"/> <input type="button" value="Limpar filtros"/>										
<input checked="" type="checkbox"/>	Name	ID da instância	Estado da inst...	Tipo de inst...	Verificação de sta	Status do alarm	Zona de dispon...	DNS IPv4 público	Endereço IP...	IP elástico
<input checked="" type="checkbox"/>	ec2-prova-app	i-05871b15b7d598116	Executando	t3.micro	3/3 verificações a	Exibir alarmes +	us-east-2a	-	18.118.220.236	18.118.220.236
<input type="checkbox"/>	ec2-prova-db	i-00307754ab9778848	Executando	t3.micro	3/3 verificações a	Exibir alarmes +	us-east-2a	-	-	-

Sub-redes (1/5)Informações

Encontrar sub-redes por atributo ou tag

Last updated about 2 hours ago

Ações

Criar sub-rede

	Name	ID da sub-rede	Estado	VPC	Bloquear acesso público	CIDR IPv4	CIDR IPv6
<input type="checkbox"/>	-	subnet-02f9e0a00fdb0df8a	Available	vpc-0311d3a93b1439059	Desativado	172.31.32.0/20	-
<input checked="" type="checkbox"/>	sub-prova-infra-pr	subnet-058b742b5861be618	Available	vpc-0e00e3411b1e8ff2 prove...	Desativado	10.0.2.0/24	-
<input type="checkbox"/>	-	subnet-02dd521bf9cfd30bc	Available	vpc-0311d3a93b1439059	Desativado	172.31.0.0/20	-
<input type="checkbox"/>	-	subnet-0b07e285e4a06d4c7	Available	vpc-0311d3a93b1439059	Desativado	172.31.16.0/20	-
<input type="checkbox"/>	sub-prova-infra-pu	subnet-0066f7e3959816271	Available	vpc-0e00e3411b1e8ff2 prove...	Desativado	10.0.0.0/24	-

Tabelas de rotas (1/3)Informações

Encontrar tabelas de rotas por atributo ou tag

Last updated about 2 hours ago

Ações

Criar tabela de rotas

	Name	ID da tabela de rotas	Associações explícitas...	Associações de ...	Princ...	VPC	ID do proprietário
<input checked="" type="checkbox"/>	rota-pu	rtb-0cddb391a3e6490ef	subnet-0066f7e3959816...	-	Não	vpc-0e00e3411b1e8ff2 prove-infra-rodrigo	125394634232
<input type="checkbox"/>	rota-pr	rtb-026f0b5cb5a4a417d	subnet-058b742b5861be...	-	Sim	vpc-0e00e3411b1e8ff2 prove-infra-rodrigo	125394634232
<input type="checkbox"/>	-	rtb-0841c66ce294b6cd5	-	-	Sim	vpc-0311d3a93b1439059	125394634232

rtb-0cddb391a3e6490ef

Ações

DetalhesInformações

ID da tabela de rotas

rtb-0cddb391a3e6490ef

VPC

vpc-0e00e3411b1e8ff2 | prove-infra-rodrigo

Principal

Não

ID do proprietário

125394634232

Associações explícitas de sub-rede

subnet-0066f7e3959816271 / sub-prova-infra-pu

Associações de borda

-

Rotas

Associações de sub-rede

Associações de borda

Propagação de rotas

Tags

Rotas (2)

Filterar rotas

Ambos

Editar rotas

Destino	Alvo	Status	Propagado	Origem da rota
0.0.0.0/0	igw-05bcf7fcbddcd4099	Ativo	Não	Criar rota
10.0.0.0/16	local	Ativo	Não	Criar tabela de rotas

rtb-026f0b5cb5a4a417d

Ações

DetalhesInformações

ID da tabela de rotas

rtb-026f0b5cb5a4a417d

VPC

vpc-0e00e3411b1e8ff2 | prove-infra-rodrigo

Principal

Sim

ID do proprietário

125394634232

Associações explícitas de sub-rede

subnet-058b742b5861be618 / sub-prova-infra-pr

Associações de borda

-

Rotas

Associações de sub-rede

Associações de borda

Propagação de rotas

Tags

Rotas (2)

Filterar rotas

Ambos

Editar rotas

Destino	Alvo	Status	Propagado	Origem da rota
0.0.0.0/0	eni-073847a7a7bcf4ec0	Ativo	Não	Criar rota
10.0.0.0/16	local	Ativo	Não	Criar tabela de rotas

Snapshot criado com êxito snap-03798cc60a8fa42a7.

Snapshots (1)Informações

De minha propriedade

Pesquisar

Last updated less than a minute ago

Lixeira

Ações

Criar snapshot

	Name	ID do snapshot	Tamanho comple...	Tamanho d...	Descrição	Nível de ...	Status do snapshot	Iniciado	Andamento
<input type="checkbox"/>	snap-03798cc60a8fa42a7	-	8 GiB	Backup Pre-Entrega Banco	Padrão	Pendente	2026/01/14 14:50 GMT-4	0%	

1a1a2a40000889e

Log de fluxo criado com êxito para o seguinte recurso:
vpc-0e00e3411b1e8fff2

fl-091a1a2a40000889e / Log-Prova

Ações

Detalhes

ID do log de fluxo
fl-091a1a2a40000889e

Nome
Log-Prova

Estado
Ativa

Horário de criação
quarta-feira, 14 de janeiro de 2026 às 14:55:42 AMT

Tipo de destino
cloud-watch-logs

Nome do destino
log

Função do IAM
arn:aws:iam::125394634232:role/aws-service-role/resource-explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer

Perfil do IAM entre contas
-

Tipo de tráfego
Rejeitar

Intervalo máximo de agregação
10 minutos

Formato de log
Padrão

Formato do arquivo
-

Partições compatíveis com Hive
-

Logs de partição
-

Tags

Integrações

Tags

Pesquisar etiquetas

Gerenciar tags

Chave

Valor

Name

Log-Prova

dash.cloudflare.com/7acaed463f9c171af610076b0f263b0f/cyberselva.com/dns/records

cyberselva.com

DNS

Registros

Configure registros DNS e revise o status do proxy dos seus nomes de host.

Documentação DNS

Etapas recomendadas para concluir a configuração da zona

Adicione um registro A, AAAA ou CNAME a www para que www.cyberselva.com seja resolvido.

Adicione um registro A, AAAA ou CNAME para seu domínio de raiz para que a cyberselva.com** seja resolvida.

Adicione um registro MX para seu domínio raiz para que o email possa acessar endereços @cyberselva.com ou configurar registros SPF, DKIM e DMARC restritivos para impedir a falsificação de emails.

Alguns de seus registros somente DNS estão expondo endereços IP com proxy da Cloudflare. Certifique-se de usar um proxy em todos os registros A, AAAA e CNAME apontando para registros com proxy para garantir que seu servidor de origem esteja totalmente protegido.

Gerenciamento de DNS para cyberselva.com

Revisar, adicionar e editar registros de DNS. As edições entrarão em vigor depois de salvas.

Configuração de DNS: Completo Importar e exportar Configurações de exibição do painel

Pesquisar registros de DNS

Adicionar filtro

Buscar

Adicionar registro

Tipo

Nome

Conteúdo

Status do proxy

TTL

Ações

A

prova

18.118.220.236

Com proxy

Auto

Editar