Documentação e instrução para configuração e execução da criação do RDS por meio do Terraform.

Fred Chardson Bezerra Lopes

1. Descrição e configuração

Inicialmente fora colocado dentro do arquivo main.tf as chaves para poder acessar a conta na AWS no entanto, como isso caracteriza quebra de segurança as chaves encontram-se nesse arquivo na sessão de passo a passo, posteriormente fora criado os blocos de códigos para a criação da VPC, grupo de segurança, bem como as subnets, contudo essas, estas e aquelas estão comentadas a fim de deixar a cargo de quem for utilizar o código para criação do RDS com subnet's e VPC'S descomentar ou seguir os passos descritos abaixo para a criação do RDS apenas.

Após as configurações destes pré-requisitos tem-se a criação do RDS propriamente dito com todos as configurações necessárias para o seu funcionamento assim como as especificidades que foram solicitas, a exemplo, senha, nome do banco, nome do usuário, monitoramento, snapshots, janela de backup, multi_az, proteção contra exclusão e demais. No que diz respeito ao cloudwatch o mesmo encontra-se comentado, pois está como variável a ser digitada as configurações ao rodar o comando de aplicação do código.

No arquivo de saída existem as saídas de configuração do RDS tais como: endpoint, porta, grupo de segurança, estas servem para obter e lançar as configurações supra mencionadas após a efetivação da criação do banco de dados.

Por fim, no arquivo de variáveis estão todas as variáveis a serem digitadas na criação do RDS: nome do banco, nome do usuário, senha, id da VPC, subnet, lista de Arns para notificação de CPU, armazenamento, memória, disco.

As métricas do PgBench estão dispostas entre os dois bancos criados, stone-cadastro e stone-faturamento, a fim de atender uma das exigências de comunicação entre duas contas e respectivamente o débito e o crédito entre as mesmas, resultante da operação de transferência. Fora utilizado para métrica um cliente realizando 1.000.000 de transações em ambos os bancos.

2. Passo a passo

Passo a Passo para a criação do RDS

Considerando que exista uma VPC e subnet já configuradas

1. Copiar a url do git.
2. Executar o git clone por meio do gibash no diretório o qual deseja extrair.
3. Inserir a secret key no arquivo main.
4. Abrir o terminal no vscode ou outro.
5. Executar o comando terraform init.
6. Executar o comando terraform plan.
7. Executar o comando terraform apply.
8. Fornecer um nome para a instância do RDS.
9. Fornecer nome para o banco de dados.
10. Fornecer uma senha para o banco de dados.
11. Fornecer um nome de usuário para o banco de dados.
12. Fornecer o id da VPC, no caso em tela já existe, adicionar a VPC existente ou se preferir criar nova.

VPC = vpc-00a2ececc433ef7c4

access_key = "AKIAZYGQ2EFVPXE5VJCP"

secret_key = "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"

Endereço git: https://github.com/FCLO/Desafio-DBA-Terraform.git

3. DUMP'S e configurações de restauração.

Por fim, como a Amazon cobra por tempo em que o RDS fica ligado, como também um valor extra pela disponibilidade de zona de AZ e este custo é considerável fora disponibilizado os DUMP's referentes aos bancos criados localmente atendendo à requisição de modelagem presente no desafio. Por meio do comando, psql -U -h -p -d -f onde U = usuário, h = host p = porta d = banco alvo, f = arquivo a ser carregado .sql. No terminal, prompt de comando, é possível a restauração do mesmo desde de haja um banco criado e com um esquema público os DUMP's foram criados utilizando a porta 5433. O usuário com permissão apenas de select fora criado com a denominação de db_user usando o comando grant do PostgresSQL. A tabela a qual contém 1.000.000 de linhas, contendo nome e e-mail, é a tabela tb_pessoa_fisica dentro do banco stone-cadastro no esquema public. Dentro do arquivo main.tf existem recursos para a criação tanto das subnets quanto de vpc's se por ventura seja do desejo criar.

Apêndice A

Script para atribuição de permissões a determinado grupo e restrições a outro (s). Usuário postgres possui permissão de super usuário, e, é membro do grupo all_group o qual possui privilégio de insert, delete, update, select, criar e excluir regras. Por outro lado, o usuário user_db possui apenas a permissão de select e, pertence ao grupo r_group, grupo o qual possui apenas permissão de leitura.

```
/*
   Name: abort_command(); Type: FUNCTION; Schema: public; Owner: postgres
   Função a qual bloqueia permissões não permitidas para o usuário

*/
drop function abort_command() cascade;

create function public.abort_command() returns event_trigger
    language plpgsql
    as $$
begin --fora usado o postgres, mas poderia ser usado algum outro padrão de nome de
--usuário.
      if current_user not similar to 'postgres%' then
      raise notice '[TIME] %',
current_timestamp;

raise notice '[EVENT-TRIGGERED] abort_command';

raise notice '[DESCRIPTION] COMANDO BLOQUEADO POR GATILHO - USUARIO ATUAL NAO
POSSUI AS PERMISSOES NECESSARIAS !';

raise notice '[EVENT] %',
tg_event;

raise notice '[COMMAND] %',
tg_tag;

raise exception '[!] % NAO POSSUI PERMISSOES PARA USAR O COMANDO %',
current_user,
tg_tag;
end if;
end;

$$;

alter function public.abort_command() owner to postgres;

/*
    Name: trg_create_set_owner(); Type: FUNCTION; Schema: public; Owner: postgres
   Função a qual ativa o gatilho de bloqueio
*/

drop function trg_create_set_owner() cascade;

create function public.trg_create_set_owner() returns event_trigger
    language plpgsql
    as $$
```

```
declare

  obj record;

begin

      if current_user = 'user_db' then

            execute execute 'REASSIGN OWNED BY user_db TO all_group';

raise notice '[TIME] %',
current_timestamp;

raise notice '[EVENT-TRIGGERED] trg_create_set_owner';

raise notice '[DESCRIPTION] DONO DO OBJETO ALTERADO PELO GATILHO';

raise notice '[EVENT] %',
tg_event;

raise notice '[COMMAND] %',
tg_tag;
end if;
end;

$$;

alter function public.trg_create_set_owner() owner to postgres;

/*

 Name: usp_alter_privileges(); Type: FUNCTION; Schema: public; Owner: all_group

 */

create function public.usp_alter_privileges() returns void
    language plpgsql
    as $$
declare
      dbname text;

begin

select
      CURRENT_DATABASE()
into
      dbname;

raise INFO '============================================================';

raise INFO '[...] ALTERANDO PRIVILÉGIOS NO BANCO DE DADOS: %',
dbname;

raise INFO '============================================================';

execute 'ALTER DATABASE ' || dbname || ' OWNER TO all_group;';

raise INFO '[OK] DONO DO DATABASE % ALTERADO PARA all_group',
dbname;

alter schema public owner to all_group;

raise INFO '[OK] DONO DO SCHEMA public ALTERADO PARA all_group';
```

```
revoke all privileges on
all tables in schema public
from
public;

raise INFO '[OK] TODOS PRIVILEGIOS REVOGADOS DE TODAS TABELAS DO SCHEMA public DO
PUBLICO';

revoke all privileges on
all sequences in schema public
from
public;

raise INFO '[OK] TODOS PRIVILEGIOS REVOGADOS DE SEQUENCIAS NO SCHEMA public DO
PUBLICO';

execute 'REVOKE ALL PRIVILEGES ON DATABASE ' || dbname || ' FROM public';

raise INFO '[OK] TODOS PRIVILEGIOS REVOGADOS DO DATABASE % DO PUBLICO',
dbname;

revoke all privileges on
schema public
from
public;

raise INFO '[OK] TODOS PRIVILEGIOS REVOGADOS DO SCHEMA public DO PUBLICO';

execute 'GRANT CONNECT ON DATABASE ' || dbname || ' TO r_group WITH GRANT OPTION';

raise INFO '[OK] CONEXAO GARANTIDA PARA r_group';

execute 'GRANT ALL PRIVILEGES ON DATABASE ' || dbname || ' TO all_group WITH GRANT
OPTION';

raise INFO '[OK] PRIVILEGIOS GARANTIDOS NO DATABASE PARA all_group';

grant usage on
schema public to r_group with grant option;

raise INFO '[OK] PRIVILEGIO USAGE GARANTIDO NO SCHEMA public PARA r_group';

grant all privileges on
schema public to all_group;

raise INFO '[OK] PRIVILEGIOS GARANTIDOS NO SCHEMA public PARA all_group';

grant
select
      on
      all tables in schema public to r_group with grant option;

raise INFO '[OK] PRIVILEGIO SELECT GARANTIDO EM TODAS TABELAS DO SCHEMA public
PARA r_group';

grant
select
      ,
      insert
      ,
      update
      ,
      delete
```

```
	on
	all tables in schema public to rw_group with grant option;

raise INFO '[OK] PRIVILEGIOS SELECT, INSERT, UPDATE, DELETE GARANTIDOS EM TODAS
TABELAS DO SCHEMA public PARA r_group';

grant all privileges on
all tables in schema public to all_group with grant option;

raise INFO '[OK] PRIVILEGIOS GARANTIDOS EM TODAS TABELAS DO SCHEMA public PARA
all_group';

grant usage,
select
	on
	all sequences in schema public to r_group with grant option;

grant all privileges on
all sequences in schema public to all_group with grant option;

raise INFO '============================================================';

raise INFO '[OK] PRIVILEGIOS ALTERADOS NO BANCO DE DADOS: %',
dbname;

raise INFO '============================================================';
end;

$$;

alter function public.usp_alter_privileges() owner to all_group;

revoke all on
schema public
from
user_db;

revoke all on
schema public
from
PUBLIC;

grant all on
schema public to PUBLIC;

/*
 Name: DEFAULT PRIVILEGES FOR TABLES; Type: DEFAULT ACL; Schema: -; Owner:
postgres
*/


alter default privileges for role user_db grant
select
	on
	tables to r_group;

alter default privileges for role postgres grant
select
	,
	insert
	,
	delete
	,
	update
```

```
      on
      tables to all_group;

/*

 Name: abort_command; Type: EVENT TRIGGER; Schema: -; Owner: all_group

*/


create event trigger abort_command on
ddl_command_start
when TAG in ('GRANT', 'REVOKE')
   execute function public.abort_command();

alter event trigger abort_command owner to all_group;

/*
 Name: trg_create_set_owner; Type: EVENT TRIGGER; Schema: -; Owner: postgres
*/

create event trigger trg_create_set_owner on
ddl_command_end
when TAG in ('CREATE TABLE', 'CREATE TYPE', 'CREATE SEQUENCE', 'CREATE DOMAIN')
   execute function public.trg_create_set_owner();

      alter event trigger trg_create_set_owner owner to postgres;
```

Comandos os quais concedem e revogam privilégios ao usuário (user_db), bem como garantem sua conexão com o banco de dados.

```
GRANT CONNECT ON DATABASE "stone-faturamento" to user_db;

ALTER DEFAULT PRIVILEGES IN SCHEMA public GRANT ALL ON TABLES TO user_db;

GRANT USAGE ON SCHEMA public to user_db;

GRANT SELECT ON ALL SEQUENCES IN SCHEMA public TO user_db;

GRANT SELECT ON ALL TABLES IN SCHEMA public TO user_db;

REVOKE ALL PRIVILEGES ON all tables in schema public FROM user_db;
```