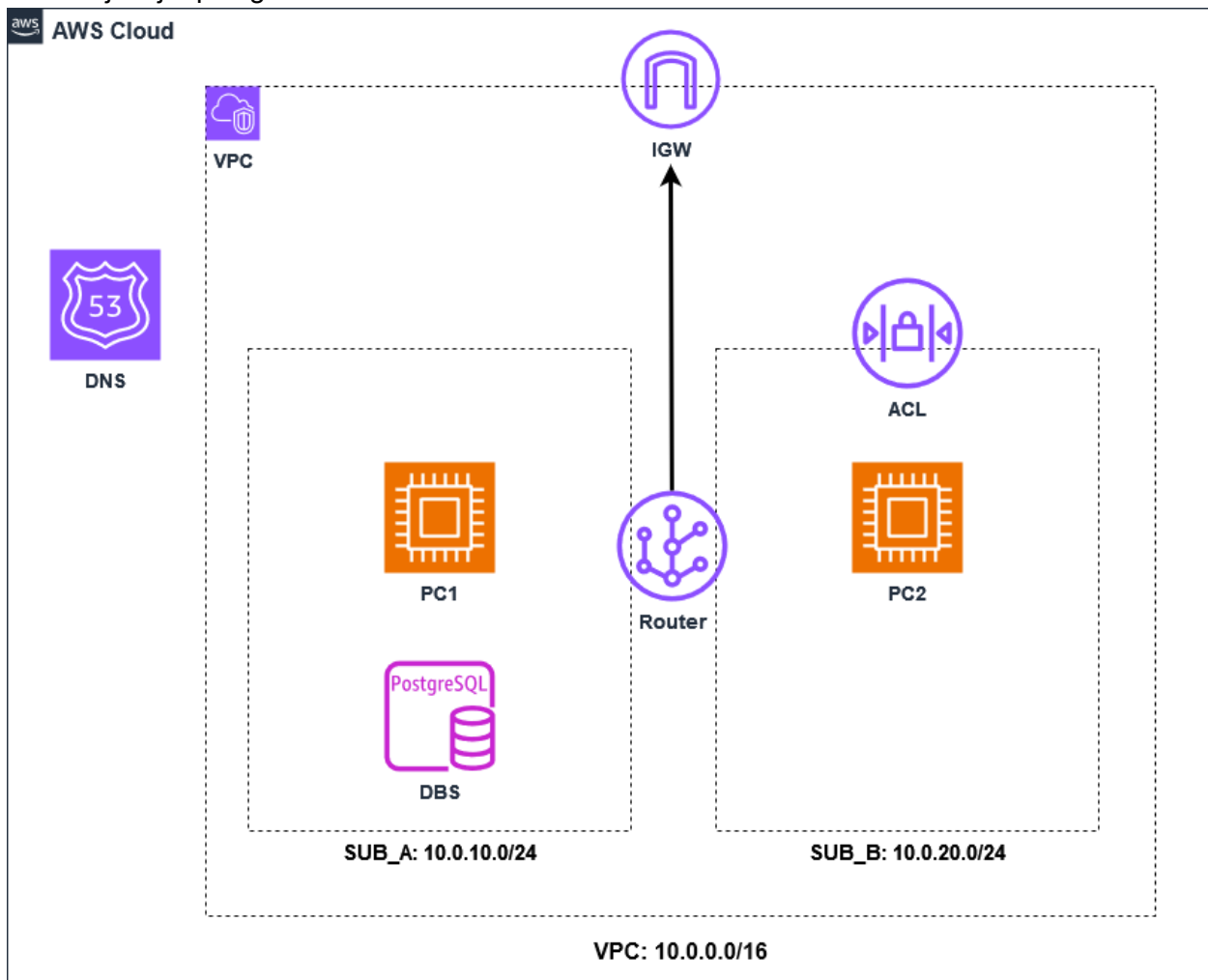


Tvorba sieťových prostredí v AWS cloud-e

Obsahom Lab manuálu je ukázať prácu so základnými službami v AWS cloud-e potrebnými pre prácu a vytváranie sieťových prostredí.

Topológia

Práca so základnými službami pre interakciu so sieťovým prostredím bude demonštrovaná na nasledujúcej topológii:

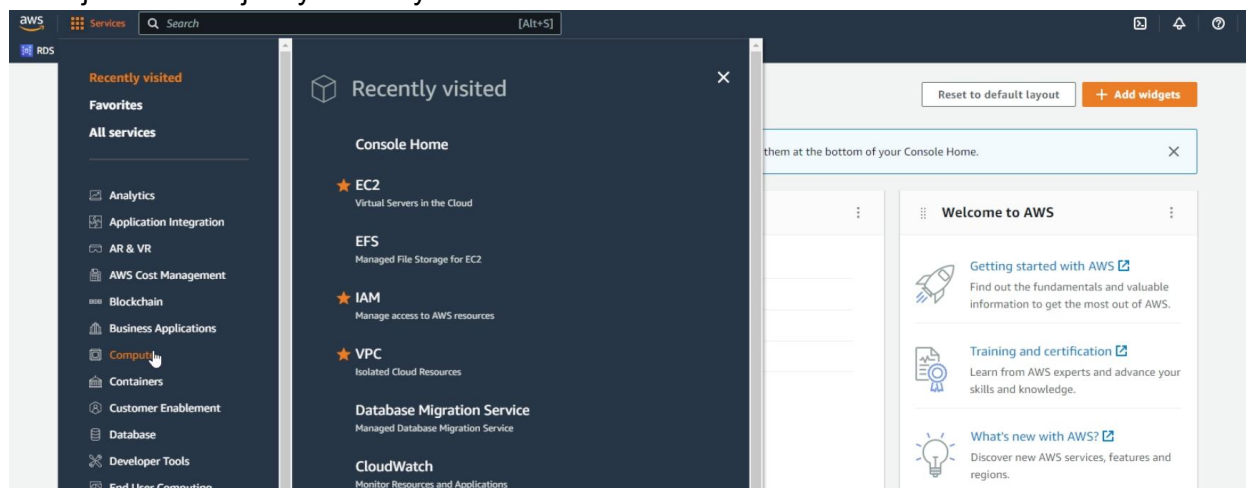


Úlohy

Nasledujúce úlohy ukážu, ako vytvoriť VPC sieť, ako túto sieť rozdeliť na menšie podsiete, ako pracovať so smerovaním, ako umožniť prístup zariadeniam vo VPC sieti do internetu, ako zabezpečiť prístup ku konkrétnym zdrojom, ako vytvoriť virtuálny server a pripojiť sa na neho využitím protokolov SSH a HTTP, ako povoliť komunikáciu medzi dvojicou vnútorných zdrojov, ako umožniť ich komunikáciu využitím doménových názvov, ako vytvoriť databázu a prepojiť ju s virtuálnym serverom a ako obmedziť komunikáciu medzi podsietami. Poslednou znázornenou úlohou je ukážka ako vybrané vyššie uvedené koncepty automatizovať využitím IaaS nástroja CloudFormation.

Pre prácu s AWS konzolou je potrebné mať vlastný účet. V tomto prípade je potrebné dať pozor na to, že niektoré AWS služby sú spoplatnené a ich použitie môže byť účtované. Druhou možnosťou je zakúpenie kurzu, napr. cez platformu acloudguru, v rámci ktorej sú k dispozícii 60 - 90 minútové cvičenia, ktorých súčasťou je prístup do AWS konzoly.

Všetky vyššie uvedené funkcionality sú v AWS cloude reprezentované na to určenou službou, ktorú je možné nájsť využitím vyhľadávacieho okna v AWS konzole.



Virtual Private Cloud (VPC)

Vytvorenie virtuálnej privátnej siete je možné využitím služby VPC, v rámci ktorej stačí zvoliť možnosť **Create VPC** a definovať nasledujúce parametre:

- Typ: **typ VPC siete**
- Tag: **označenie VPC siete**
- IPv4 CIDR block: **spôsob definovania adresného rozsahu**
- IPv4 CIDR: **10.0.0.0/16 (samotný adresný rozsah)**
- IPv6: **No IPv6 CIDR Block**
- Tenancy: **Default**

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

Creates a tag with a key of 'Name' and a value that you specify.

VPC

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

IPv6 CIDR block [Info](#)

☒ No IPv6 CIDR block

☐ IPAM-allocated IPv6 CIDR block

☐ Amazon-provided IPv6 CIDR block

☐ IPv6 CIDR owned by me

Tenancy [Info](#)

Default

Tenancy slúži na určenie toho, či zdroje v našej VPC sieti budú spustené na zdieľaných serveroch (default - lacnejšie riešenie), alebo na dedikovaných (dedicated - drahšie riešenie).

VPC dashboard

EC2 Global View [New](#)

Filter by VPC:

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

You successfully created vpc-09ec6b8b0693f97c2 / VPC

Your VPCs (1/1) [Info](#)

Filter VPCs

☒	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP option set
☒	VPC	vpc-09ec6b8b0693f97c2	Available	10.0.0.0/16	-	dopt-098b69014b4be

vpc-09ec6b8b0693f97c2 / VPC

Details Resource map CIDRs Flow logs Tags

Details

VPC ID vpc-09ec6b8b0693f97c2	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-098b69014b4be109	Main route table rtb-0ce19b67b94f9cd90	Main network A acl-0ea317d1d
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -	IPv6 CIDR (Netv -

Subnets

Definovanie podsiete vyžaduje nastavenie nasledujúcich parametrov:

- VPC ID: **id vytvorenej VPC, do ktorej bude podsiet' patriť**
- Subnet name: **meno podsiete**
- Availability Zone: **AZ, v ktorej sa bude podsiet' nachádzať**
- IPv4 CIDR block: **adresný rozsah danej podsiete**

Create subnet [Info](#)

VPC

VPC ID
Create subnets in this VPC.

vpc-09ec6b8b0693f97c2 (VPC) ▼

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

SUB_A

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

US East (N. Virginia) / us-east-1a ▼

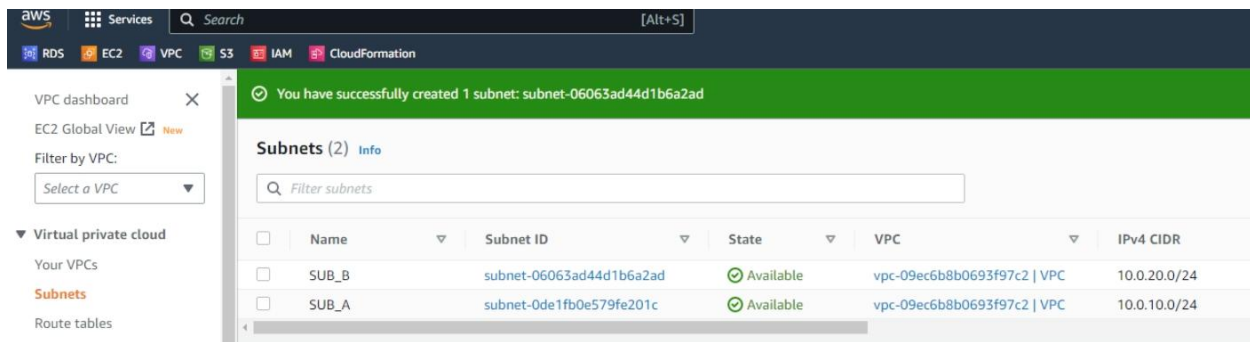
IPv4 CIDR block [Info](#)

10.0.10.0/24 X

10.0.10.0/24

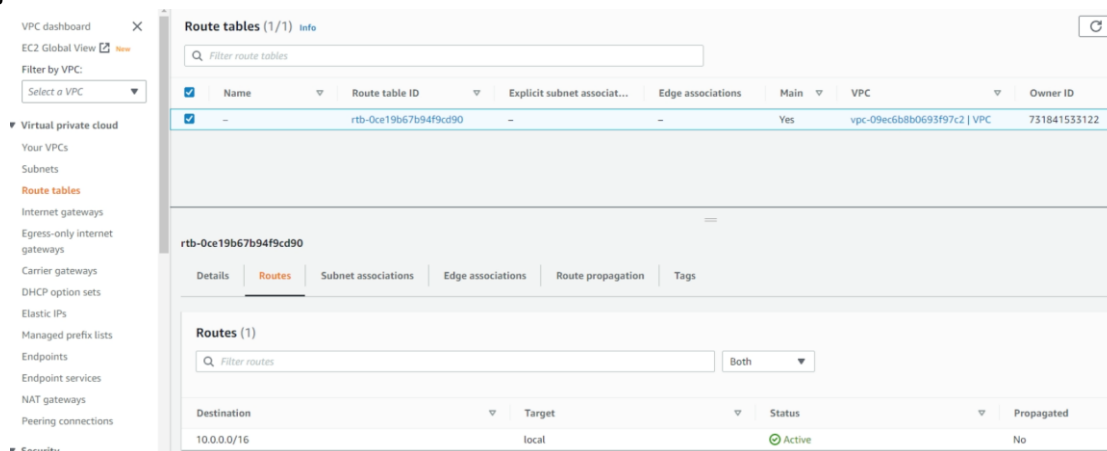
Key	Value - optional
Name X	SUB_A X

Rovnakým spôsobom vytvorte aj podsiet' SUB_B, ktorej pridelite adresný rozsah 10.0.20.0/24.



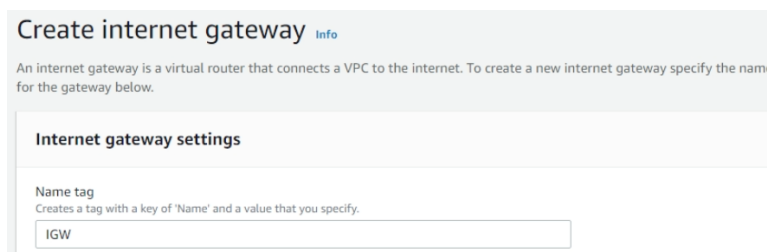
Routing table concepts

V AWS existuje globálna smerovacia tabuľka, v ktorej sa štandardne nachádzajú všetky podsiete a má súhrnný záznam na dosiahnutie celého adresného rozsahu celej VPC. Pre väčšiu granularitu je ale možné vytvoriť lokálne smerovacie tabuľky a v nich definovať, kam daná podsieť dokáže smerovať dáta. Podsieť, v ktorej sa nachádza default route sa označuje ako verejná.

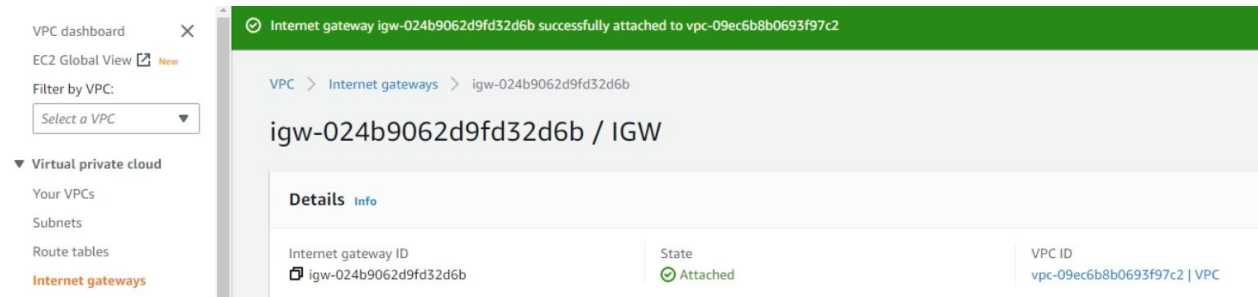


Internet Gateway

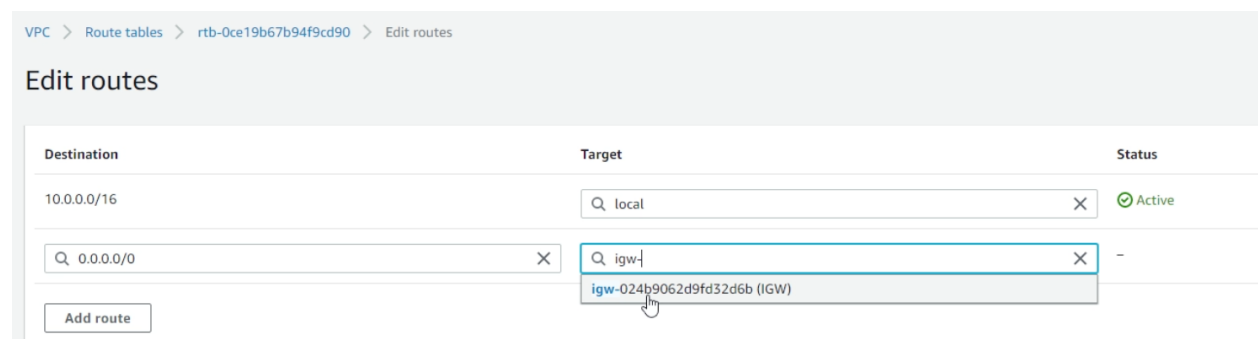
IGW je služba umožňujúca prístup k internetu. Táto služba môže byť označená ako smer pri definovaní default route. Pri vytváraní IGW stačí definovať jej názov.



Vytvorenú IGW je následne potrebné priradiť (Attach) k existujúcej VPC cez záložku Actions - Attach to VPC, kde stačí definovať cieľovú VPC sieť.



Do smerovacej tabuľky následne stačí pridať default route a ako cieľ nastaviť vytvorenú IGW.



Elastic Compute Cloud (EC2)

EC2 predstavuje inštanciu virtuálneho zariadenia. Pri jej vytváraní je potrebné definovať nasledujúce parametre:

- Priradiť do VPC a podsiete
- Zvoliť OS (AWS linux) a typ inštancie
- Vygenerovať SSH kľúč pre vzdialenú správu (.pem file)
- Nastaviť sieťové parametre a povoliť priradenie verejnej IP (potrebné pre umožnenie dostupnosti z internetu)
- Vytvoriť SG a povoliť v nej SSH (vzdialený prístup) a HTTP (prístup na webovú stránku)
- Vložiť script na inštaláciu Web servera

Konfigurácia vyššie uvedeného sa začína v záložke EC2 - Launch an instance:

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Quick Start



macOS



Ubuntu



Windows



Red Hat



S



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0aa7d40eeae50c9a9 (64-bit (x86)) / ami-084237e82d7842286 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

▼ Instance type [Info](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

[Compare instance types](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*



[Create new key pair](#)

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-09ec6b8b0693f97c2 (VPC)
10.0.0.0/16



Subnet [Info](#)

subnet-0de1fb0e579fe201c SUB_A
VPC: vpc-09ec6b8b0693f97c2 Owner: 731841533122 Availability Zone: us-east-1a
IP addresses available: 251 CIDR: 10.0.10.0/24



[Create new subnet](#)

Auto-assign public IP [Info](#)

Enable



Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - required

PC_SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and _-./()!@#%&*~:;[]\$*

Description - required [Info](#)

PC_SG

Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 85.159.104.185/32)

[Remove](#)

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

My IP

Name [Info](#)

[Add CIDR, prefix list or security](#)

85.159.104.185/32 ✕

Description - optional [Info](#)

e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0)

[Remove](#)

Type [Info](#)

HTTP

Protocol [Info](#)

TCP

Port range [Info](#)

80

Source type [Info](#)

Anywhere

Source [Info](#)

[Add CIDR, prefix list or security](#)

Description - optional [Info](#)

e.g. SSH for admin desktop

User data - optional [Info](#)

Enter custom user data into the field below

```
#!/bin/bash
yum update -y
yum install -y httpd
chkconfig httpd on
service httpd start
```

Zvyšok parametrov môže ostať v štandardnom nastavení.

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Instances (1/1) Info

Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
PC1	i-0a168d94605c569d5	Running	t2.micro	-	No alarms	us-east-1a	-

Instance: i-0a168d94605c569d5 (PC1)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Instance summary Info

Instance ID

i-0a168d94605c569d5 (PC1)

Public IPv4 address

34.235.88.120 | open address

Private IPv4 addresses

10.0.10.153

IPv6 address

-

Instance state

Running

Public IPv4 DNS

-

Hostname type

IP name: ip-10-0-10-153.ec2.internal

Private IP DNS name (IPv4 only)

ip-10-0-10-153.ec2.internal

Answer private resource DNS name

Instance type

Elastic IP addresses

Overiť úspešnosť riešenie je možné zobrazením webovej stránky dostupnej na verejnej adrese servera.

→

Nezabezpečené

34.235.88.120

Test Page

This page is used to test the proper operation of the Apache HTTP server after it has been installed. If you can read this page, it means that the Apache HTTP server installed at this site is working properly.

If you are a member of the general public:

The fact that you are seeing this page indicates that the website you just visited is either experiencing problems, or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

For example, if you experienced problems while visiting www.example.com, you should send e-mail to "webmaster@example.com".

If you are the website administrator:

You may now add content to the directory `/var/www/html/`. Note that until you do so, people will see this page instead of your content. To prevent this page from ever being used, follow the instructions in the file `README`.

You are free to use the image below on web sites powered by the Apache HTTP Server:

Overenie pripojenia na SSH daného servera je možné cez záložku **Connect**, kde je možné nájsť postupnosť krokov pre ssh pripojenie (vyžaduje existenciu `.pem` súboru definovaného pri vytváraní inštancie).

Connect to instance Info

Connect to your instance i-0a168d94605c569d5 (PC1) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0a168d94605c569d5 (PC1)

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is `key.pem`
- Run this command, if necessary, to ensure your key is not publicly viewable.

chmod 400 key.pem
- Connect to your instance using its Public IP:

34.235.88.120

Example:

ssh -i "key.pem" ec2-user@34.235.88.120

```
C:\Users\rp385yq\Desktop>ssh -i "key.pem" ec2-user@34.235.88.120
The authenticity of host '34.235.88.120 (34.235.88.120)' can't be established.
ECDSA key fingerprint is SHA256:KDSEkv22ImcndfwCK9NcxaZWPoqlWQigCjN86Coqzf0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.235.88.120' (ECDSA) to the list of known hosts.
```

```

_ |  ( _ | _ )
_ |  ( _ | _ )
_ |  ( _ | _ )

```

Amazon Linux 2 AMI

```
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-10-153 ~]$
```

Vytvorením súboru **/var/www/html/index.htm**, je možné upraviť obsah zobrazovanej webovej stránky.

```
<html>
Hello world from PC1
</html>
```

← → ↻ ⚠ Nezabezpečené | 34.235.88.120

Hello world from PC1

Rovnakým spôsobom je potrebné vytvoriť aj zariadenie PC2.

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Instances (1/2) Info

Find instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
☐	PC1	i-0a168d94605c569d5	Running	t2.micro	2/2 checks passed	No alarms	us-east-1a	-
☒	PC2	i-03d0d41a5c12dd88f	Running	t2.micro	-	No alarms	us-east-1b	-

Instance: i-03d0d41a5c12dd88f (PC2)

Details Security Networking Storage Status checks Monitoring Tags

▼ Instance summary Info

Instance ID	Public IPv4 address	Private IPv4 addresses
i-03d0d41a5c12dd88f (PC2)	18.212.137.53 open address	10.0.20.173
IPv6 address	Instance state	Public IPv4 DNS
-	Pending	-
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-10-0-20-173.ec2.internal	ip-10-0-20-173.ec2.internal	

Security Group (SG)

Bezpečnostné skupiny slúžia na ochranu konkrétnych sieťových kariet používaných zdrojov. Obsahujú len povolenia a môžu byť definované v smere do ale aj v smere z daného zdroja. Pravidlá majú stateful charakter a teda všetko čo je v jednom smere povolené SG, tak automaticky aj odpovede na túto komunikáciu sú povolené. Štandardne je všetka komunikácia smerom von povolená, avšak smerom dnu len to, čo sme definovali pri vytváraní EC2 inštalácie. Kvôli tomu, aktuálne nie je možná komunikácia protokolom ICMP z PC1 na PC2, pretože PC2 v smere in nepovoľuje ICMP správy. Opraviť tento nedostatok je možné pridaním ďalšieho záznamu do SG.

EC2 > Security Groups > sg-0d9db585059fb91c - PC_SG > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sg-03a4284eb776fb399	SSH	TCP	22	Custom	85.159.104.185/32
sg-0c9356fb5cb4bd10	HTTP	TCP	80	Custom	0.0.0.0/0
-	All ICMP - IPv4	ICMP	All	Anywhere-IPv4	0.0.0.0/0

[Add rule](#)

Route 53

Route 53 je služba pre mapovanie IP adries na doménové názvy. Je to AWS DNS služba. Štandardne v rámci AWS funguje lokálne DNS, ktoré umožňuje dosiahnuteľnosť zdrojov využitím ich **Private IP DNS name**. Pre definovanie vlastných doménových názvov je ale potrebné dodatočné nastavenie. V rámci služby Route 53 je potrebné vytvoriť **Private Hosted zone**. Existuje aj Public hosted zone, no tá by spravovala globálne dostupné DNS záznamy, avšak vyžaduje zakúpenie domény.

Vytvorenie Privátnej hosted zóny vyžaduje nastavenie jej typu, názvu domény a VPC siete.

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com subdomains.

Domain name [Info](#)

This is the name of the domain that you want to route traffic for.

test.com

Valid characters: a-z, 0-9, ! * # \$ % & ' () ^ + , - . / : ; < = > ? @ [\] ^ _ ` { | } . ~

Description - optional [Info](#)

This value lets you distinguish hosted zones that have the same name.

The hosted zone is used for...

The description can have up to 256 characters. 0/256

Type [Info](#)

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☐ Public hosted zone
A public hosted zone determines how traffic is routed on the internet.

☒ Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.

VPCs to associate with the hosted zone [Info](#)

To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.

[i](#) For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings [enableDnsHostnames](#) and [enableDnsSupport](#) to true.

Region [Info](#)

US East (N. Virginia) [us-east-1]

VPC ID [Info](#)

Q vpc-02b1730738f5627a4

Remove VPC

Add VPC

Po vytvorení hosted zóny sa vytvorí základná štruktúra DNS záznamu definujúca NS a SOA atribúty.

Route 53 > Hosted zones > test.com

Private test.com [Info](#) [Delete zone](#) [Test record](#) [Configure query logging](#)

► Hosted zone details [Edit hosted zone](#)

Records (2) Hosted zone tags (0)

Records (2) [Info](#)
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

[Refresh](#) [Delete record](#) [Import zone file](#) [Create record](#)

Filter records by property or value Type [▼](#) Routing policy [▼](#) Alias [▼](#) < 1 > [ⓘ](#)

☐	Record name	Type	Routin...	Differ...	Value/Route traffic to
☐	test.com	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
☐	test.com	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 9...

Teraz už len stačí definovať **A** záznam mapujúci požadovaný názov domény, napr. Pc2.test.com na IPv4 adresu daného zariadenia.

Quick create record [Switch to wizard](#)

▼ Record 1 [Delete](#)

Record name [Info](#) pc2 .test.com [Keep blank to create a record for the root domain.](#) Record type [Info](#) A – Routes traffic to an IPv4 address and some AWS resources

☒ Alias

Value [Info](#) 10.0.20.245

Enter multiple values on separate lines.

TTL (seconds) [Info](#) 300 1m 1h 1d Recommended values: 60 to 172800 (two days) Routing policy [Info](#) Simple routing

[Add another record](#)

[Cancel](#) [Create records](#)

Funkciou Route 53 je tvorba tzv. Alias záznamov, ktoré umožňujú efektívne mapovanie doménového názvu na doménový názov.

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name

Info

pc2a.test.com

Keep blank to create a record for the root domain.

Record type

Info

A – Routes traffic to an IPv4 address and some AWS resources

Alias

Route traffic to

Info

Alias to another record in this hosted zone

US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

pc2.test.com

Alias hosted zone ID: Z1300242ETY9K0XT61R

Routing policy

Info

Simple routing

Evaluate target health

Yes

Add another record

Cancel

Create records

Records (4) Info

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Filter records by property or value

Type

Routing policy

Alias

< 1 > ⚙

☐	Record name	Type	Routin...	Differ...	Value/Route traffic to
☐	test.com	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
☐	test.com	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 720...
☐	pc2.test.com	A	Simple	-	10.0.20.245
☐	pc2a.test.com	A	Simple	-	pc2.test.com.

```
[ec2-user@ip-10-0-10-84 ~]$ ping pc2a.test.com
PING pc2a.test.com (10.0.20.245) 56(84) bytes of data.
64 bytes from ip-10-0-20-245.ec2.internal (10.0.20.245): icmp_seq=1 ttl=255 time=0.666 ms
64 bytes from ip-10-0-20-245.ec2.internal (10.0.20.245): icmp_seq=2 ttl=255 time=0.735 ms
```

Rational Database Service (RDS)

RDS je službou pre vytváranie relačných databáz. Databázu je možné vytvoriť kliknutím na tlačidlo **Create database** a voľbou konkrétneho typu databázy.

Choose a database creation method [Info](#)

☒ Standard create

You set all of the configuration options, including ones for availability, security, backups, and maintenance.

☐ Easy create

Use recommended best-practice configurations. Some configuration options can be changed after the database is created.

Engine options

Engine type [Info](#)

☐ Amazon Aurora



☐ MySQL



☐ MariaDB



☒ PostgreSQL



☐ Oracle



☐ Microsoft SQL Server



Engine Version

PostgreSQL 13.7-R1

Ako template je potrebné zvoliť Free tier.

Templates

Choose a sample template to meet your use case.

☐ Production

Use defaults for high availability and fast, consistent performance.

☐ Dev/Test

This instance is intended for development use outside of a production environment.

☒ Free tier

Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

Ďalej je potrebné nastaviť **Meno databázy** a prihlasovacie údaje (**Master username** a **Master password**). Zvyšok parametrov je možné nechať bez zmeny. Jediným parametrom, ktorý je ešte potrebné nastaviť je **Initial database name**, ktorý je možné nájsť v časti Additional Configuration. Tiež je potrebné definovať v akej VPC sieti a AZ sa databáza bude nachádzať.

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ Credentials Settings

Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter.

- ☐ **Manage master credentials in AWS Secrets Manager - new**
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.
- ☐ **Auto generate a password**
Amazon RDS can generate a password for you, or you can specify your own password.

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), ' (single quote), " (double quote) and @ (at sign).

Confirm master password [Info](#)

▼ Additional configuration

Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)



Po dlhšej chvíli dôjde k vytvoreniu databázy.

Summary

DB identifier database-1	CPU 6.82%	Status Available	Class db.t3.micro
Role Instance	Current activity 0.00 sessions	Engine PostgreSQL	Region & AZ us-east-1a

Connectivity & security

Monitoring

Logs & events

Configuration

Maintenance & backups

Tags

Connectivity & security

Endpoint & port

Endpoint
database-1.cvzal0q2euwlus-east-1.rds.amazonaws.com

Port
5432

Networking

Availability Zone
us-east-1a

VPC
VPC (vpc-0b999025935ab20c7)

Subnet group
default-vpc-0b999025935ab20c7

Subnets
subnet-07b61283e0baea9c5
subnet-0d35e5bf29d3a9c43

Network type
IPv4

Security

VPC security groups
default (sg-0bae42fc740ee65f9)

Active

Publicly accessible
No

Certificate authority [info](#)
rds-ca-2019

Certificate authority date
August 22, 2024, 19:08 (UTC+02:00)

DB instance certificate expiration date
August 22, 2024, 19:08 (UTC+02:00)

RDS > Databases

Consider creating a Blue/Green Deployment to minimize downtime during upgrades

You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for cl

[Guide](#) [Aurora User Guide](#)

Databases

Group resources

Modify

Actions

Filter by databases

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions	CPU
database-1	Instance	PostgreSQL	us-east-1a	db.t3.micro	Available	-	-

Teraz je potrebné v časti vytvorenej databázy kliknúť na záložku **Actions** a zvoliť možnosť **Set up EC2 connection**. Tu stačí zvoliť EC2 inštanciu, s ktorou je potrebné vytvoriť spojenie.

Set up EC2 connection [Info](#)

Select EC2 instance

Database
database-1

EC2 instance
Choose the EC2 instance to connect to this database. Only EC2 instances in the same VPC as the database are shown. If no EC2 instances in the same VPC are available, you can create a new EC2 instance.

i-04362945db88e9ca8
Server us-east-1a

[Create EC2 instance](#)

Cancel

Continue

Vytvorené nastavenie automaticky vytvorí potrebné SG a priradí ich na inštanície EC2 a DB.

Connection summary [Info](#)

You are setting up a connection between RDS database [database-1](#) and EC2 instance [i-04362945db88e9ca8](#).

To set up a connection between the database and the EC2 instance, VPC security group *rds-ec2-1* is added to the database, and VPC security group *ec2-rds-1* is added to the EC2 instance.



Bold indicates an addition being made to set up a connection.

sg-03896f5a26b99a7 - ec2-rds-1

Details Inbound rules **Outbound rules** Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Outbound rules (1/1)

Filter security group rules

☒	Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
☒	-	sgr-03367c8741a061a...	-	PostgreSQL	TCP	5432	sg-0bf3b4aaaf726f4ac...	Rule to allow connecti...

sg-0bf3b4aaaf726f4ac - rds-ec2-1

Details **Inbound rules** Outbound rules Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (1/1)

Filter security group rules

☒	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
☒	-	sgr-0f441c8fbacff1e99	-	PostgreSQL	TCP	5432	sg-03896f5a26b99a...	Rule to allow connecti...

Na pripojenie sa z EC2 inštanície na databázu je potrebné spustiť nasledujúce príkazy z EC2 inštanície (inštalovanie db klienta a vykonanie prihlásenia):

```
sudo yum install postgresql15
```

```
psql -h <IP_Address> -p <port_no> -d <database_name> -U <DB_username> -W
```

```
psql -h database-1.cvza10q2euwl.us-east-1.rds.amazonaws.com -p 5432 -d myDB -U postgres -W
```

```
[ec2-user@ip-10-0-10-199 ~]$ psql -h database-1.cvzal0q2euw1.us-east-1.rds.amazonaws.com -p
5432 -d myDB -U postgres -W
Password for user postgres:
psql (9.2.24, server 13.7)
WARNING: psql version 9.2, server version 13.0.
Some psql features might not work.
SSL connection (cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256)
Type "help" for help.

myDB=>
```

Interakcia s Postgresql databázou je následne vykonateľná využitím bežných príkazov:

```
\l - zoznam databáz
CREATE TABLE students(
  user_id serial PRIMARY KEY,
  username VARCHAR(50),
  email VARCHAR(50)
);

\dt - zobrazenie vytvorených tabuliek

INSERT INTO students(username, email)
VALUES ('student1', 'student1@mail.com');

SELECT * from students;

\q
```

```
myDB=> \l
```

Name	Owner	Encoding	Collate	Ctype	Access privileges
myDB	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	
postgres	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	
rdsadmin	rdsadmin	UTF8	en_US.UTF-8	en_US.UTF-8	rdsadmin=CTc/rdsadmin+ rdstopmgr=Tc/rdsadmin
template0	rdsadmin	UTF8	en_US.UTF-8	en_US.UTF-8	=c/rdsadmin + rdsadmin=CTc/rdsadmin
template1	postgres	UTF8	en_US.UTF-8	en_US.UTF-8	=c/postgres + postgres=CTc/postgres

(5 rows)

```
myDB=> CREATE TABLE students(
myDB(> user_id serial PRIMARY KEY,
myDB(> username VARCHAR(50),
myDB(> email VARCHAR(50)
myDB(> );
CREATE TABLE
myDB=>
myDB=>
myDB=>
myDB=> \dt
```

Schema	Name	Type	Owner
public	students	table	postgres

(1 row)

```

myDB=> INSERT INTO students(username, email)
myDB-> VALUES ('student1', 'student1@mail.com');
INSERT 0 1
myDB=>
myDB=>
myDB=> INSERT INTO students(username, email)
myDB-> VALUES ('student2', 'student2@mail.com');
INSERT 0 1
myDB=>
myDB=>
myDB=> SELECT * from students;
 user_id | username | email
-----+-----+-----
        1 | student1 | student1@mail.com
        2 | student2 | student2@mail.com
(2 rows)

```

Network Access Control Lists (NACL)

NACL sú sieťové prístupové zoznamy, ktoré je možné používať na obmedzenie komunikácie medzi podsietami. NACL majú stateless správanie a teda pravidlo pridané do NACL automaticky nepovoľuje spätnú komunikáciu. Princíp je rovnaký ako pri ACL a teda sa jedná o číslovaný zoznam pravidiel, kde je možné mať **Allow** a **Deny** pravidiel. NACL sa vyhodnocuje zhora nadol, pričom na konci je implicitný záznam deny any. K ACL sa dá dostať cez záložku **VPC, Security** a **Network ACLs**, kde v rámci ACL je možné vidieť jeho základnú charakteristiku, vstupné a výstupné pravidla. Nakoniec je súčasťou ACL aj jeho asociácia s podsietami, na ktoré bude NACL aplikovaný.

Details

Inbound rules

Outbound rules

Subnet associations

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Outbound rules (2)

Edit outbound rules

Filter outbound rules

< 1 >

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow

Pri vytváraní nového ACL stačí kliknúť na **Create network ACL** a nastaviť jeho názov a VPC do ktorej bude patriť.

Network ACL settings

Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

VPC
VPC to use for this network ACL.

Select a VPC

V novo vytvorenom ACL je potrebné vložiť pravidlá podľa požiadaviek a následne stačí zvoliť z ponuky dostupných podsietí, do ktorých bude NACL patriť. Povolenie SSH pripojenia z akéhokoľvek zdroja znázorňuje nasledujúci obrázok:

Edit inbound rules [Info](#)
Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number	Type	Protocol	Port range	Source	Allow/Deny	
100	Custom TCP	TCP (6)	22	0.0.0.0/0	Allow	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

Subnet associations

[Details](#) [Inbound rules](#) [Outbound rules](#) [Subnet associations](#) [Tags](#)

[Edit subnet associations](#)

Name	Subnet ID	Associated with	Availability Zone	IPv4 CIDR	IP
------	-----------	-----------------	-------------------	-----------	----

CloudFormation

CloudFormation je služba na automatizované nasadzovanie zdrojov založenom na definovaní konfiguračného súboru v YAML alebo JSON formáte. Tento konfiguračný súbor stačí následne

vložiť v rámci vytvárania **Stack** objektu v kontexte CloudFormation služby. Pri vytváraní Stack-u je možné zvoliť použitie šablóny a miesto, kde sa nachádza (S3 alebo na lokálnom PC).

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template ☐ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL ☐ Upload a template file

Po vytvorení Stack objektu dôjde k vytvoreniu všetkých jeho zdrojov. Výhodou tohto spôsobu práce so zdrojmi je, že ich je možné priebežne aktualizovať a hlavne na konci, pri zmazení celého Stack objektu dôjde k vymazaniu všetkých zdrojov, vďaka čomu nedôjde k zabudnutiu spustenie niektorej zo služieb, ktorej nechcená prevádzka môže spôsobiť značné finančné dôsledky. Nasledujúci výpis znázorňuje základný konfiguračný súbor pre vytvorenie vybraných vyššie uvedených zdrojov (VPC, SUB_A, SUB_B, EC2, SG, IGW):

```
Resources:
  MyVPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: "10.0.0.0/16"
      EnableDnsSupport: 'true'
      EnableDnsHostnames: 'true'
      Tags:
        - Key: "Name"
          Value: "VPC"

  MySubnet1:
    Type: AWS::EC2::Subnet
    Properties:
      VpcId: !Ref MyVPC
      CidrBlock: "10.0.10.0/24"
      AvailabilityZone: us-east-1a
      Tags:
        - Key: "Name"
          Value: "SUB_A"
```

```
MySubnet2:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref MyVPC
    CidrBlock: "10.0.20.0/24"
    AvailabilityZone: us-east-1b
    Tags:
      - Key: "Name"
        Value: "SUB_B"

MySecurityGroup:
  Type: AWS::EC2::SecurityGroup
  Properties:
    VpcId: !Ref MyVPC
    GroupDescription: "Allow SSH and HTTP traffic"
    SecurityGroupIngress:
      - IpProtocol: tcp
        FromPort: 22
        ToPort: 22
        CidrIp: "0.0.0.0/0"
      - IpProtocol: tcp
        FromPort: 80
        ToPort: 80
        CidrIp: "0.0.0.0/0"
      - IpProtocol: icmp
        FromPort: -1
        ToPort: -1
        CidrIp: "0.0.0.0/0"
    Tags:
      - Key: "Name"
        Value: "SG"

MyEC2Instance1:
  Type: AWS::EC2::Instance
  Properties:
    InstanceType: t2.micro
    ImageId: ami-04cb4ca688797756f # Replace with a valid AMI ID
    KeyName: !Ref MyKeyPair
    NetworkInterfaces:
      - AssociatePublicIpAddress: "true"
        DeviceIndex: "0"
        GroupSet:
          - Ref: "MySecurityGroup"
        SubnetId:
          Ref: "MySubnet1"
    Tags:
      - Key: "Name"
        Value: "PC1"

MyKeyPair:
  Type: "AWS::EC2::KeyPair"
```

```
Properties:
  KeyName: "my-keypair"
```

```
MyInternetGateway:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: MyInternetGatewayName
```

```
AttachGateway:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    VpcId: !Ref MyVPC
    InternetGatewayId: !Ref MyInternetGateway
```