How to Create VPC Network

Creating a Virtual Private Cloud (VPC) network on DigitalOcean involves logging into your account, navigating to the Networking section, selecting a region, naming your VPC network, and creating it. VPCs provide isolated environments for deploying resources securely, ensuring that your infrastructure operates independently within its defined network.

How to Setup Firewall Rules

Configuring firewall rules on DigitalOcean is crucial for controlling inbound and outbound traffic to your resources. You can set up firewall rules by accessing the Firewall section, creating a new firewall with specific rules tailored to your security requirements, and activating it to protect your resources from unauthorized access.

How to Create Droplet

To create a droplet (virtual private server) on DigitalOcean, you need to choose a region, select an operating system, customize CPU and RAM specifications, configure SSH key authentication, specify a hostname, and create the droplet. Droplets are essential for deploying applications or services in a cloud environment, offering scalability and flexibility.

How to Add Droplet to Firewall Rules

After creating a droplet, associate it with existing firewall rules to ensure that it benefits from the security configurations you've defined. Access the Firewall section, select the appropriate firewall, and add the newly created droplet to its list of protected resources to safeguard it from unauthorized network access.

How to Set Up NMS (Network Management System)

Setting up a network management system on your DigitalOcean droplet involves SSH into the droplet, creating a new user, configuring sudo permissions, updating the system, installing necessary software like Git, and preparing the droplet for application deployment and efficient system management. This ensures that your infrastructure is well-maintained and ready for operational tasks.

how to Log onto the GCP Console

Log into GCP Console: Access your GCP account using credentials to reach the management interface where all cloud resources are administered.

Setup VPC for the NMS

Navigate to VPC Networks: Use the search bar in the GCP Console to find and select "VPC networks". This section allows you to create and manage Virtual Private Cloud (VPC) networks.

how to Create a VPC: Begin creating a new VPC by specifying a name (e.g., nms-vpc) and a description tailored to NMS (Network Management System) requirements.

Define Subnet Details: Enter subnet details such as IP ranges (e.g., 10.0.0.0/24) within the VPC to segment your network logically. Ensure these settings align with your network architecture needs.

how to Setup Firewall Policy

Access Firewall Policies: Search for "Firewall policies" and select the appropriate option to manage inbound and outbound traffic rules.

Create Firewall Policy: Initiate the creation of a new firewall policy (e.g., nms-node-firewall-policy) to control network access. Define rules specifying allowed protocols (e.g., SSH, RDP) and ports (e.g., tcp:22, tcp:3389).

Associate with VPC: Link the firewall policy to the previously created VPC (nms-vpc) to enforce security measures across your network environment effectively.

how Create VM Instance

Navigate to VM Instances: Proceed to the VM instances section within the GCP Console, where you can deploy and manage virtual machine instances.

Instance Creation: Start the creation process by specifying a unique name for the VM instance (e.g., nms-node-london). Choose a suitable region (e.g., europe-west2 (London)) and configure the machine type (e.g., CPU and memory allocation).

Select Boot Disk: Opt for an appropriate operating system and disk size (e.g., Ubuntu 20.04 LTS with a disk size of 320GB) to support your application requirements.

Networking Configuration: Configure networking settings by selecting the VPC (nms-vpc-network) and subnet (nms-nodes-subnet) previously set up. This ensures the VM instance operates within your defined network environment.

how to Deploy: Complete the setup by clicking "Create" to deploy the VM instance. Make note of the external IP address assigned to the instance for remote access.

Node Registration Procedure

SSH Access: Utilize SSH connectivity from the VM instances dashboard to establish a secure connection to the newly created VM instance. This step allows for further configuration and installation of the NMS software.

Summary

These steps provide a comprehensive guide to setting up a node on GCP, encompassing the creation of network infrastructure (VPC, subnet), enforcement of security policies (firewall rules), deployment of virtual resources (VM instance), and initial configuration via SSH. Each stage is crucial for establishing a robust and secure environment suitable for hosting network management applications and services.

Certainly! Here's the elaboration without bullet points:

explain the Vultr Node Setup Procedure:

Log onto your Vultr account: Begin by logging into your Vultr account via their web interface or API.

Step 1. Create Firewall Group:

Select Network and click on Firewall: Navigate to the Network section in the Vultr dashboard and select the Firewall option.

Click on Add Firewall Group: To create a new firewall group, click on the button labeled "Add Firewall Group."

Enter description and click on Add Firewall Group:** Provide a description for the firewall group you are creating, then finalize the creation by clicking on "Add Firewall Group."

Step 2. Add IPv4 Rules:

For Master node or Guardian node:** Depending on whether you're setting rules for a Master node or a Guardian node, configure the appropriate IPv4 rules. These rules typically involve specifying which IP addresses and ports are allowed or restricted for incoming connections.

Step 3. Create VPS (Virtual Private Server):**

Navigate to Compute:** Go to the Compute section in Vultr's dashboard.

Deploy Server:** Click on the option to deploy a new server instance.

Choose server settings:** Select AMD CPU and choose London as the server location.

Select Ubuntu 20.04 LTS x64:** Choose this specific operating system image for your server.

Select server size:** Opt for 350 GB storage, 8 CPUs, and 16 GB RAM.

Disable Auto Backups:** If prompted, disable automatic backups for this server.

Select firewall group:** Assign the previously created firewall group to this server.

Deploy Now:** Confirm and deploy the server instance with these settings.

Step 4. NMS Install Procedure (Vultr):**

Access the server:** Once the server is deployed, copy its IP address and use SSH to connect to it from your command line interface.

SSH connection:** Use the command `ssh root@<IPAddress>` and enter the password when prompted.

Configure server permissions:** Add a sudoers configuration and disable the firewall as per your setup requirements.

This process outlines the steps involved in setting up infrastructure on Vultr's cloud platform, including firewall configuration, server deployment, and initial setup of server permissions and access.

1.how to Setup Access Rules in AWS

To ensure consistency and proper resource management, it's crucial to select the appropriate AWS region for your resources. In this guide, we will use the eu-west-2 region, which corresponds to London. This will ensure all resources are created in the same geographic location, optimizing latency and compliance with regional data laws.

2. how to Create a VPC

A Virtual Private Cloud (VPC) allows you to provision a logically isolated section of the AWS cloud where you can launch AWS resources in a virtual network that you define.

Navigate to VPC Section: Open the AWS Management Console, type VPC in the search bar, and select "Your VPCs."

Create VPC: Click "Create VPC." Enter the IPv4 CIDR block 10.0.0.0/24, which defines a range of IP addresses for the VPC. Optionally, name your VPC for easier identification.

Complete VPC Creation: Click "Create VPC" to complete this step.

3.how to Create an Internet Gateway

An Internet Gateway (IGW) is a horizontally scaled, redundant, and highly available VPC component that allows communication between your VPC and the internet.

Navigate to Internet Gateway: In the AWS Console, search for Internet Gateway and click on it.

Create and Attach IGW: Click "Create Internet Gateway," enter a name, and click "Create Internet Gateway." After creation, attach it to your VPC by selecting the newly created VPC from the dropdown and clicking "Attach Internet Gateway."

4. Add the Internet Gateway to the Route Table

Route Tables contain a set of rules, called routes, that are used to determine where network traffic is directed.

Navigate to Route Tables: Go to the VPC section, select your VPC, and in the left navigation bar, click on "Route Tables."

Edit Routes: Find the Route Table ID associated with your VPC, click “Edit Routes,” and add a new route with the destination 0.0.0.0/0 (which means all IP addresses) and the target set to the Internet Gateway created earlier.

Save Changes: Save the changes to update the route table.

5. how to Create a Subnet

A Subnet is a range of IP addresses in your VPC where you can place groups of isolated resources.

Navigate to Subnet: Search for Subnet in the AWS Console and click on “Subnets - VPC Feature.”

Create Subnet: Create a new subnet by selecting your VPC and entering the IPv4 CIDR block 10.0.0.0/28. Optionally, name your subnet and select an Availability Zone.

Complete Subnet Creation: Click “Create Subnet” to finalize this step.

6.how to Create a Security Group

Security Groups act as a virtual firewall for your EC2 instances to control inbound and outbound traffic.

Navigate to Security Groups: In the AWS Console, search for Security Group and click on “Security Groups (EC2 Feature).”

Create Security Group: Enter a name, description, and select the VPC created earlier. Add inbound rules to allow traffic, such as a Custom TCP Rule with port range 8000-8001 and 9000, and set the source to Anywhere (0.0.0.0/0). Leave the outbound rules as default.

Complete Security Group Creation: Click “Create Security Group.”

7. Node Setup in AWS

Ensure that all resources, including EC2 instances, are created in the eu-west-2 region to maintain consistency and optimal performance.

8. Create a Key Pair

A Key Pair allows you to securely connect to your EC2 instances.

Navigate to Key Pairs: In the EC2 Dashboard, under “Network & Security,” click on “Key Pairs.”

Create Key Pair: Enter a name, select RSA, and choose the file format (.pem for Linux/Mac or .ppk for Windows). Click “Create Key Pair” and save the key file securely.

9. Create an EC2 Instance

EC2 (Elastic Compute Cloud) instances are virtual servers in AWS.

Launch EC2 Instance: In the AWS Console, type EC2 in the Services search box and click on EC2. Click “Launch Instance.”

Instance Configuration:

Name and AMI: Enter a name, select the Amazon Machine Image (AMI) Ubuntu Server 20.04 LTS (HVM), SSD Volume Type.

Instance Type: Choose an instance type such as t2.medium for 8 CPU and 16GB RAM.

Key Pair: Select the Key Pair created earlier.

Network Settings: Select the VPC and subnet created earlier and attach the Security Group created in step 6.

Storage: Set the storage size to 320 GB.

Launch Instance: Click “Launch Instance” and wait for the instance to be created.

10. Node Registration Procedure (AWS)

To connect to the EC2 instance:

Access EC2 Dashboard: Go to the EC2 Dashboard and click on “Instances (running).”

Connect to Instance: Select the instance ID and click on “Connect.” Use the provided connection details to access the EC2 instance command line.

Summary

This guide walks you through setting up a VPC, Internet Gateway, Route Table, Subnet, Security Group, and an EC2 instance in the AWS eu-west-2 region. This setup provides a secure and accessible environment for deploying your services or applications.