

## Создание 2-х инстансов

### Бастион хост (лежит в публичной подсети и имеет Public IP)

Instance summary for i-0d95c068924b6889e (srv-bastion) Info

Updated less than a minute ago

Refresh

Connect

Instance state ▼

Actions ▼

Instance ID

🔗

 i-0d95c068924b6889e (srv-bastion)

IPv6 address

–

Hostname type

IP name: ip-10-1-2-17.eu-central-1.compute.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

🔗

 18.157.168.52 [Public IP]

IAM Role

–

Public IPv4 address

🔗

 18.157.168.52 | [open address](#)

Instance state

✔️

 Running

Private IP DNS name (IPv4 only)

🔗

 ip-10-1-2-17.eu-central-1.compute.internal

Instance type

t2.micro

VPC ID

🔗

 vpc-0c7484761af9c590a (vpc-for-task7) [🔗](#)

Subnet ID

🔗

 subnet-09858083f988612c5 (subnet-public-for-task7) [🔗](#)

Private IPv4 addresses

🔗

 10.1.2.17

Public IPv4 DNS

–

Elastic IP addresses

–

AWS Compute Optimizer finding

🔗

 Opt-in to AWS Compute Optimizer for recommendations.  
[| Learn more](#) [🔗](#)

Auto Scaling Group name

–

### srv-001 (лежит в приватной подсети без Public IP и имеет доступ в интернет через NAT)

Instance summary for i-0ee6fe41ad91ee54e (srv-001) [Info](#)

Updated less than a minute ago


Refresh

Connect

Instance state ▼

Actions ▼

Instance ID

 i-0ee6fe41ad91ee54e (srv-001)

IPv6 address

–

Hostname type

IP name: ip-10-1-1-125.eu-central-1.compute.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

–


IAM Role

–


Public IPv4 address

–

Instance state

 Running


Private IP DNS name (IPv4 only)

 ip-10-1-1-125.eu-central-1.compute.internal


Instance type

t2.micro


VPC ID

 vpc-0c7484761af9c590a (vpc-for-task7) [↗](#)

Subnet ID

 subnet-0413058d39f31628c (subnet-private-for-task7) [↗](#)

Private IPv4 addresses

 10.1.1.125


Public IPv4 DNS

–

Elastic IP addresses

–

AWS Compute Optimizer finding

 Opt-in to AWS Compute Optimizer for recommendations.  
[Learn more](#) [↗](#)

Auto Scaling Group name

–

## Проверяю подключение к srv-bastion по ssh

```
C:\Users\ADMIN>ssh -i Keys.pem ubuntu@18.157.168.52
The authenticity of host '18.157.168.52 (18.157.168.52)' can't be established.
ECDSA key fingerprint is SHA256:swAsqXN4swaQ40+QY9Beh+C0KKj pz2lykS7DEv0o3x4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.157.168.52' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Dec 16 10:19:42 UTC 2022

System load:  0.0               Processes:            99
Usage of /:   19.9% of 7.57GB   Users logged in:     1
Memory usage: 23%              IPv4 address for eth0: 10.1.2.17
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Fri Dec 16 10:10:20 2022 from 3.120.181.44
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-1-2-17:~$
```

## Копирую ключ на srv-bastion

```
C:\Users\ADMIN\scp -i Keys.pem Keys.pem ubuntu@10.157.168.52:/home/ubuntu
Keys.pem
100% 1674 29.7KB/s 00:00
C:\Users\ADMIN>
```

```
ubuntu@ip-10-1-2-17:~$ ll
total 40
drwxr-x--- 5 ubuntu ubuntu 4096 Dec 16 10:09 ./
drwxr-xr-x 3 root    root   4096 Dec 16 07:46 ../
-rw----- 1 ubuntu ubuntu  274 Dec 16 10:21 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Jan  6  2022 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Dec 16 07:59 .cache/
drwxrwxr-x 3 ubuntu ubuntu 4096 Dec 16 08:29 .local/
-rw-r--r-- 1 ubuntu ubuntu  807 Jan  6  2022 .profile
drwx----- 2 ubuntu ubuntu 4096 Dec 16 08:49 .ssh/
-rw----- 1 ubuntu ubuntu 1674 Dec 16 10:22 Keys.pem
ubuntu@ip-10-1-2-17:~$
```

## Забираю права с ключа

```
ubuntu@ip-10-1-2-17:~$ chmod 600 Keys.pem
ubuntu@ip-10-1-2-17:~$ ll
total 40
drwxr-x--- 5 ubuntu ubuntu 4096 Dec 16 10:09 ./
drwxr-xr-x 3 root    root   4096 Dec 16 07:46 ../
-rw----- 1 ubuntu ubuntu  274 Dec 16 10:21 .bash_history
-rw-r--r-- 1 ubuntu ubuntu  220 Jan  6  2022 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3771 Jan  6  2022 .bashrc
drwx----- 2 ubuntu ubuntu 4096 Dec 16 07:59 .cache/
drwxrwxr-x 3 ubuntu ubuntu 4096 Dec 16 08:29 .local/
-rw-r--r-- 1 ubuntu ubuntu  807 Jan  6  2022 .profile
drwx----- 2 ubuntu ubuntu 4096 Dec 16 08:49 .ssh/
-rw----- 1 ubuntu ubuntu 1674 Dec 16 10:22 Keys.pem
ubuntu@ip-10-1-2-17:~$
```

## Подключаюсь к srv-001 по ssh с srv-bastion

```
ubuntu@ip-10-1-2-17:~$ ssh -i Keys.pem ubuntu@10.1.1.125
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri Dec 16 10:26:21 UTC 2022

System load:  0.0               Processes:            98
Usage of /:   19.9% of 7.57GB   Users logged in:     1
Memory usage: 21%              IPv4 address for eth0: 10.1.1.125
Swap usage:   0%

0 updates can be applied immediately.

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Dec 16 10:10:41 2022 from 10.1.2.17
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-1-1-125:~$
```

## Удостоверяюсь в правильности настройки сети (хост должен иметь доступ в интернет)

```
ubuntu@ip-10-1-1-125:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=111 time=2.52 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=111 time=1.67 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=111 time=1.67 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=111 time=1.67 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.669/1.882/2.515/0.365 ms
ubuntu@ip-10-1-1-125:~$
```

Создаю скрипт aptUpdate.sh для подключения по ssh к srv-001 и выполнения команды

\$ sudo apt-get update

```
ubuntu@ip-10-1-2-17: ~  
GNU nano 6.2  
#!/bin/bash  
HOST="10.1.1.125"  
ssh -i /home/ubuntu/Keys.pem ubuntu@$HOST 'sudo apt-get update'
```

Выдаю права на исполнение скрипта

```
ubuntu@ip-10-1-2-17:~$ chmod ugo+x aptUpdate.sh  
ubuntu@ip-10-1-2-17:~$ ll  
total 44  
drwxr-x--- 5 ubuntu ubuntu 4096 Dec 16 10:55 ./  
drwxr-xr-x 3 root root 4096 Dec 16 07:46 ../  
-rw----- 1 ubuntu ubuntu 274 Dec 16 10:21 .bash_history  
-rw-r--r-- 1 ubuntu ubuntu 220 Jan 6 2022 .bash_logout  
-rw-r--r-- 1 ubuntu ubuntu 3771 Jan 6 2022 .bashrc  
drwx----- 2 ubuntu ubuntu 4096 Dec 16 07:59 .cache/  
drwxrwxr-x 3 ubuntu ubuntu 4096 Dec 16 08:29 .local/  
-rw-r--r-- 1 ubuntu ubuntu 807 Jan 6 2022 .profile  
drwx----- 2 ubuntu ubuntu 4096 Dec 16 08:49 .ssh/  
-rw-r--r-- 1 ubuntu ubuntu 0 Dec 16 10:55 .sudo_as_admin_successful  
-rw----- 1 ubuntu ubuntu 1674 Dec 16 10:22 Keys.pem  
-rwxr-xrwx 1 ubuntu ubuntu 95 Dec 16 10:54 aptUpdate.sh*  
ubuntu@ip-10-1-2-17:~$
```

Проверяю работоспособность скрипта

```
ubuntu@ip-10-1-2-17: ~  
ubuntu@ip-10-1-2-17:~$ ./aptUpdate.sh  
Hit:1 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:2 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:3 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Reading package lists...  
ubuntu@ip-10-1-2-17:~$
```

## Установил WireGuard

```
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
   Loaded: loaded (/lib/systemd/system/wg-quick@.service; enabled; vendor preset: enabled)
   Active: active (exited) since Fri 2022-12-16 12:46:29 UTC; 2min 47s ago
     Docs: man:wg-quick(8)
           man:wg(8)
           https://www.wireguard.com/
           https://www.wireguard.com/quickstart/
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
   Process: 4189 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/SUCCESS)
   Main PID: 4189 (code=exited, status=0/SUCCESS)
      CPU: 30ms

Dec 16 12:46:29 ip-10-1-2-17 systemd[1]: Starting WireGuard via wg-quick(8) for wg0...
Dec 16 12:46:29 ip-10-1-2-17 wg-quick[4189]: [#] ip link add wg0 type wireguard
Dec 16 12:46:29 ip-10-1-2-17 wg-quick[4189]: [#] wg setconf wg0 /dev/fd/63
Dec 16 12:46:29 ip-10-1-2-17 wg-quick[4189]: [#] ip -4 address add 10.10.10.1/24 dev wg0
Dec 16 12:46:29 ip-10-1-2-17 wg-quick[4189]: [#] ip link set mtu 8921 up dev wg0
Dec 16 12:46:29 ip-10-1-2-17 wg-quick[4189]: [#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
Dec 16 12:46:29 ip-10-1-2-17 systemd[1]: Finished WireGuard via wg-quick(8) for wg0.
```

## Сгенерировал пару ключей и изменил файл конфигурации для подключения пользователя

```
ubuntu@ip-10-1-2-17:~$ nano /etc/wireguard/wg0.conf
/etc/wireguard/wg0.conf
[Interface]
PrivateKey = 0CSJA19Du9s+9+WSnLnqA5gMCRJnqwlizlwAlkQno=
# Приватный ключ из файла /etc/wireguard/privatekey
Address = 10.10.10.1/24
# Адрес VPN-сервера в частной сети.
ListenPort = 50505
# Порт, который будет слушать VPN-сервер.
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# Команды, которые будут выполнять при поднятии сервера
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
# Команды, которые будут выполнять при выключении сервера

[Peer]
PublicKey = 250FNEysmxhIkIZ/Tyox6c6UkYP3fMPzN7Xymks/jWQ=
# Публичный ключ клиента /etc/wireguard/publickeyClient-001
AllowedIPs = 10.10.10.2/32
# IP-адрес в частной сети, который будет присвоен клиенту.
```

Открыл порт в security group для srv-bastion

sg-0e8621696ad040f67 - srv-bastion

Actions

Details

Security group name

srv-bastion

Security group ID

sg-0e8621696ad040f67

Description

srv-bastion created 2022-12-16T07:42:28.881Z

VPC ID

vpc-0c7484761af9c590a

Owner

684882578868

Inbound rules count

2 Permission entries

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (2)

Manage tags

Edit inbound rules

Filter security group rules

	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-01b4f7926b9a836...	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-0e0a6ded1e92d78fc	IPv4	Custom UDP	UDP	50505

Создал конфигурацию пользователя

Редактировать туннель

Название: client

Публичный ключ: 250FNEYswxhIkIZ/Tyox6c6UkYP3fMPzN7Xymks/jWQ=

[Interface]

PrivateKey = QIzEQ5hi2gE3BJQ5gDCWOJo9KBNrBn1J1RT45p2llUM=

Address = 10.10.210.2/32

DNS = 8.8.8.8, 1.1.1.1

[Peer]

PublicKey = ws0SA+ZnSiwNlhTCfBptVSsjteU57znsLwKr4hsF0Gg=

AllowedIPs = 10.10.10.1/24, 0.0.0.0/0

Endpoint = 18.157.168.52:50505

PersistentKeepalive = 25

☒ Блокировать нетуннелированный трафик

Сохранить

Отмена

Далее скачиваю WireGuard к себе на ПК и пробую подключиться по клиентскому конфигу

