

Karthik Pradeep Hegadi

2KE20CS032

Assignment 35

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

AWS

Assignment:3 VPN server configuration in AWS

1. Navigate EC2 -> Launch instance

The screenshot shows the 'Setting Started' section of the AWS EC2 'Launch Instance' wizard. In the 'Name and tags' step, the 'Name' field contains 'open-vpnserver'. Below it, there's a 'Search' bar with 'openvpnpi' typed in, and tabs for 'AMI from catalog', 'Recents', and 'Quick Start'. A 'Verified provider' badge is next to the search bar. On the right, there's a 'Browse more AMIs' button and a note about including AMIs from AWS, Marketplace, and the Community. At the bottom, a note states that launching the software without a subscription will result in being subscribed to the seller's End User License Agreement.

Name
open-vpnserver [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

Q openvpnpi X

AMI from catalog Recents Quick Start

Amazon Machine Image (AMI)
OpenVPN Access Server QA Image-
3b5882c4-551b-43fa-acfe-7f5cdb896ff1
ami-09d67c332a348e7ce Verified provider

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Catalog	Published	Architecture	Virtualization	Root device type	ENAv Enabled
AWS	2023-03-08T13:	x86_64	hvm	ebs	Yes
Marketplace	35:15.000Z				
AMIs					

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#).

2. In the AWS marketplace search text "openvpn" you will find the results. Select the first Image "OpenVPN Access Server"
3. In the Instance type select "2.micro" and click config instance details4 Select your VPC, select the Public subnet that you have created previously, Auto Assign ip -> enable, host name -> Use subnet setting (Ip name) and click Add storage
5. Storage settings can be default, click Add tags
6. Add tag key as "Name" and provide the value and click configure security group (Note: The default settings allows all traffic for ssh, you can change to "mv IP" to be more secure)
7. Click "Review & Launch" and then click "Launch option". Choose the existing keypair from the list that you generated and then click "Launch Instance"
8. Verify your Instance is running

▼ Network settings [Info](#)

VPC - required [Info](#)
 vpc-0e190ca43b317839f (my-vpc-01)
 10.0.0.0/16 G

Subnet [Info](#)
 subnet-0691fa12817842c2d private_01
 VPC: vpc-0e190ca43b317839f Owner: 405819896469
 Availability Zone: ap-south-1a IP addresses available: 249 CIDR: 10.0.3.0/24 C 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
 OpenVPN Access Server (5 Connected Devices)-2.11.3-AutogenByAWSMP--3

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](#)
 OpenVPN Access Server (5 Connected Devices)-2.11.3-AutogenByAWSMP--3 created

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) Remove

9. Login to the VPN server (Note : you can either ssh from windows/linux machine where you have copied the private key, or you can use putty as well)

You need to use username as openvpnas instead of root

```
|(base) kartikhegadi@Kartiks-MacBook-Air aws.02 % chmod 400 open_vpn.pem
|(base) kartikhegadi@Kartiks-MacBook-Air aws.02 % ssh -i "open_vpn.pem" openvpnas@65.0.93.148
The authenticity of host '65.0.93.148 (65.0.93.148)' can't be established.
ED25519 key fingerprint is SHA256:4oad0V3ufSCTGhS8JemoM4rYt7MNy9qzL7K+nrm/OIA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '65.0.93.148' (ED25519) to the list of known hosts.
Welcome to OpenVPN Access Server Appliance 2.11.3

System information as of Sat Jan 28 04:18:28 UTC 2023
```

10. Once you try gave your username it prompts for configurations .Follow the screenshots and make changes Will this be the primary Access server node ? - Enter for default : yes

Please specify the network interface - Press Enter for default :

Press Enter for default [9431 : "click enter"]

Press ENTER for the default[443] : "click enter"

Should client traffic be routed by default through VPN?

Press ENTER for default [no] : yes

Should client DNS traffic be routed by default through VPN? - "yes"

Use local authentication via internal DB? "Click enter"

Should private subnets be accessible to clients by default?

Press enter for EC2 default [yes]: "click enter"

```
[Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
[> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 10.0.1.48
Please enter the option number from the list above (1- 2).
[> Press Enter for default [1]: 1
```

```
Please specify the TCP port number for the OpenVPN Daemon  
[> Press ENTER for default [443]:  
  
Should client traffic be routed by default through the VPN?  
[> Press ENTER for default [no]: yes  
  
Should client DNS traffic be routed by default through the VPN?  
[> Press ENTER for default [no]: yes  
Admin user authentication will be local  
  
Private subnets detected: ['10.0.0.0/16']  
  
Should private subnets be accessible to clients by default?  
[> Press ENTER for EC2 default [yes]: yes
```

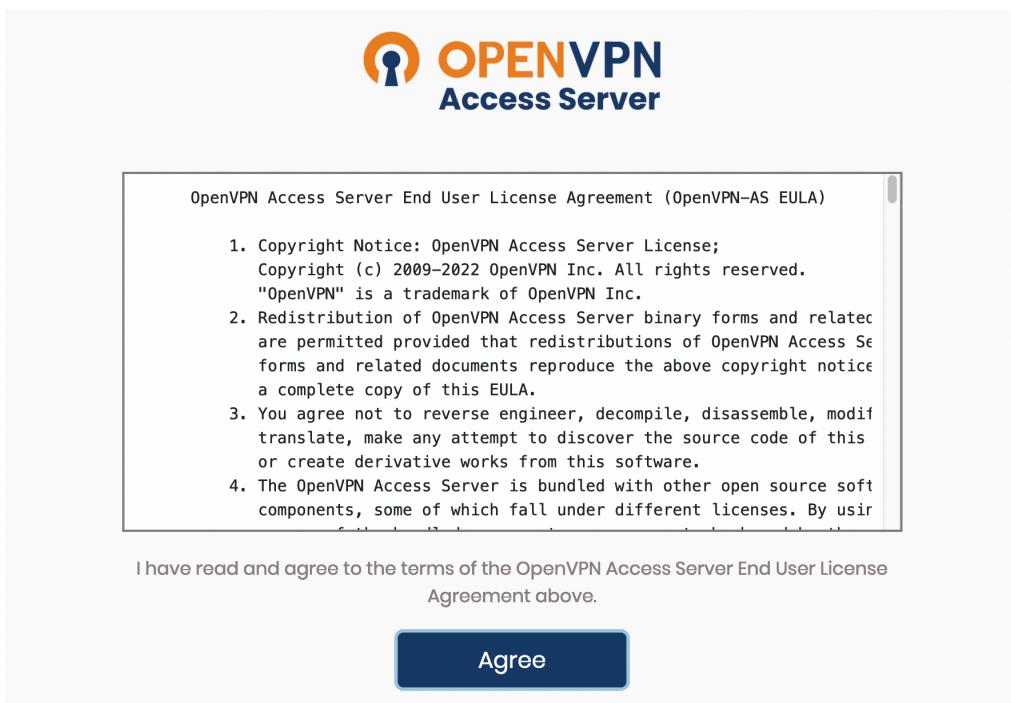
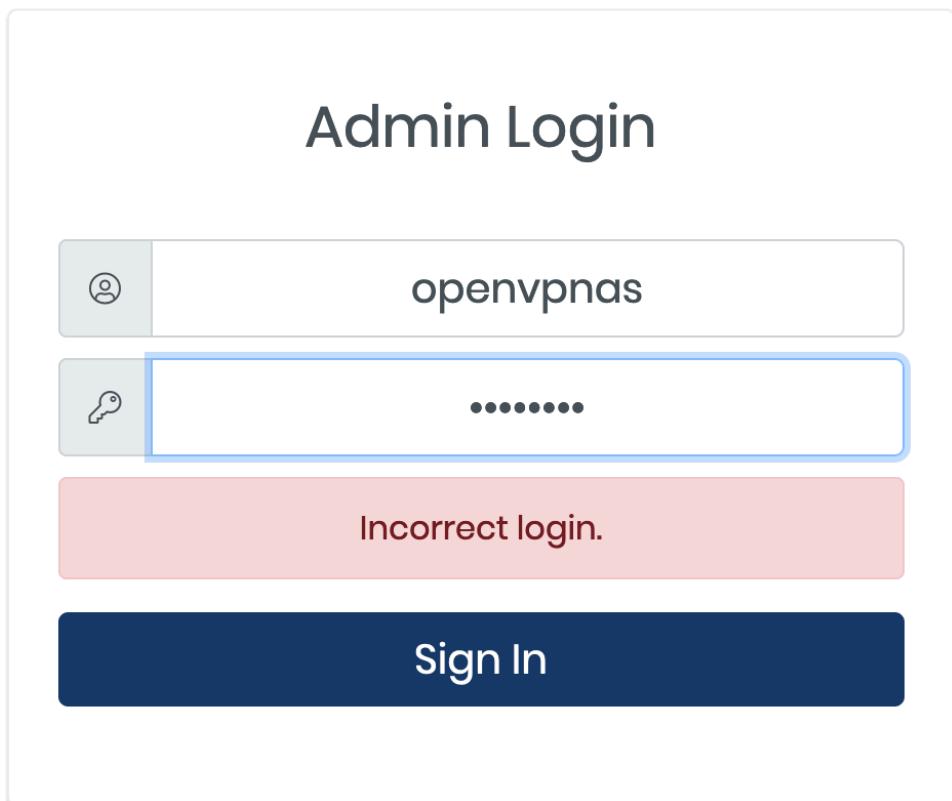
```
Created symlink /etc/systemd/system/multi-user.target.wants/openvpnas.service  
/lib/systemd/system/openvpnas.service.  
Starting openvpnas...  
  
NOTE: Your system clock must be correct for OpenVPN Access Server  
to perform correctly. Please ensure that your time and date  
are correct on this system.  
  
Initial Configuration Complete!  
  
You can now continue configuring OpenVPN Access Server by  
directing your Web browser to this URL:  
  
https://65.0.93.148:943/admin
```

```
During normal operation, OpenVPN AS can be accessed via these URLs:  
Admin UI: https://65.0.93.148:943/admin  
Client UI: https://65.0.93.148:943/  
To login please use the "openvpn" account with "SQHJbgbeRF3E" password.
```

```
See the Release Notes for this release at:  
https://openvpn.net/vpn-server-resources/release-notes/
```

```
openvpnas@ip-10-0-1-48:~$ sudo passwd openvpn  
passwd: user 'openvpn' does not exist  
openvpnas@ip-10-0-1-48:~$ sudo passwd openvpnas  
New password:  
Retype new password:      lusy@123  
passwd: password updated successfully  
openvpnas@ip-10-0-1-48:~$ |    lusy@123
```

11. Now you are logged in as "openvpnas" user



12. In order to login to the VPN server in GUI you need to login as user "openvpn".
Generate

the new password for openvpn user

Run the command "sudo passwd openvpn" and change the password

(note : give a strong password as it needs to be secured)

The screenshot shows the configuration interface with the following sections:

- Configuration** (Header)
- User Management** (Section)
 - User Permissions** (Selected tab)
 - User Profiles**
 - Group Permissions**
- capabilities. Learn More or dismiss** (Message bar)
- Active Configuration** (Section)
 - Access Server version:** [Redacted]
 - User Permissions Table:**

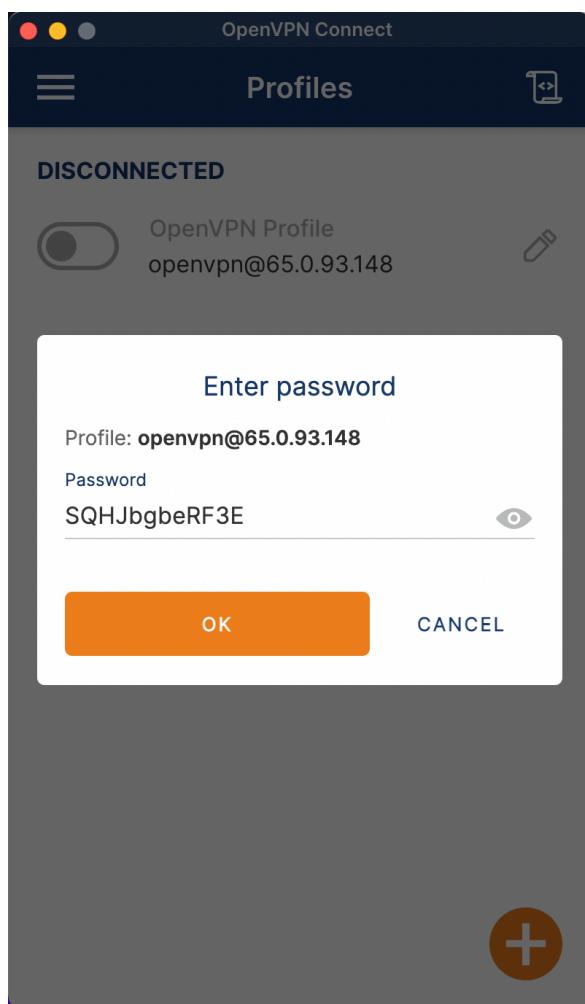
Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
lisy	No Default Group		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
 - Group Default IP Address Network (Optional):** 172.27.240.0/20
 - Routing:**
 - Should VPN clients have access to private subnets (non-public networks on the server side)?
Options: No, Yes, using NAT, Yes, using Routing
By default ccs aws give for free tire 10.0.0.0/16
 - Specify the private subnets to which all clients should be given access (one per line): 10.0.0.0/16
 - Should client Internet traffic be routed through the VPN?
Options: Yes

13. Now login to the web GUI using your public Ip <https://yourvpnip>, login using your openvpn username and password

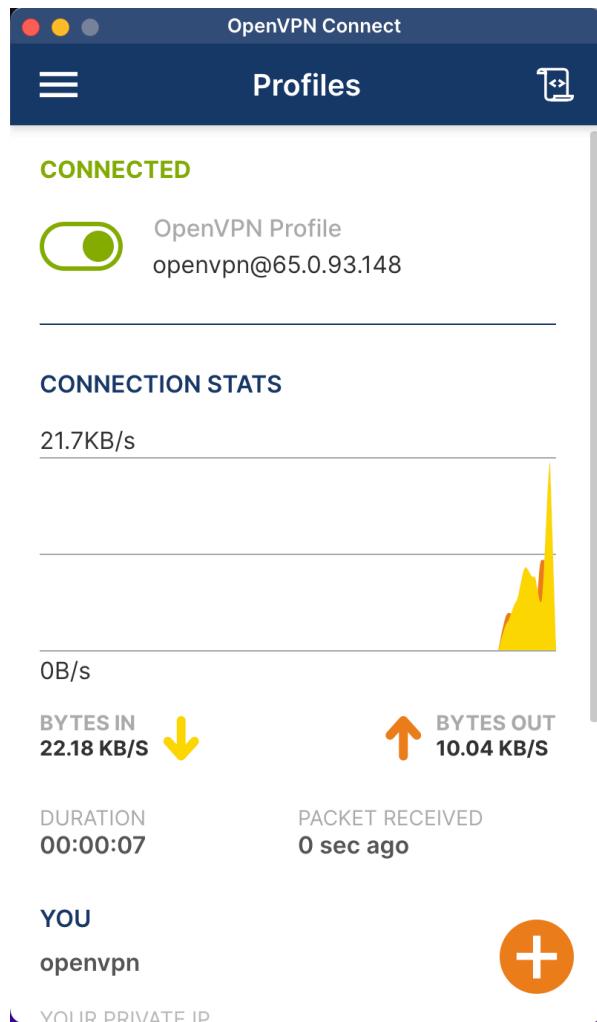
14. You can download openvpn connect for client if this prompt appears for you, if not You can download it separately(This is for windows)

Please refer end of the document if you want to configure OpenVpn client in your Linuxmachine

The screenshot shows the 'Server Network Settings' page of the OpenVPN Access Server. The left sidebar has 'Network Settings' selected. The main area shows a warning about changing hostnames or ports after deployment. The 'Hostname or IP Address' field contains '65.0.93.148'. A yellow warning box states: '⚠️ Changing the Hostname, Protocol or Port Number after VPN clients are deployed will cause the existing clients to be unusable (until a new client configuration or VPN installer is downloaded from the Client Web Server)'.



14. You can create customized users in this settings



The screenshot shows the homepage of WhatIsMyIPAddress.com. At the top, there is a search bar with the placeholder 'Enter Keywords or IP Address...' and a 'Search' button. To the right are links for 'ABOUT', 'PRESS', 'BLOG', and 'SUPPORT'. Below the header, it says 'My IP Address is:' followed by 'IPv4: 65.0.93.148' and 'IPv6: Not detected'. In the middle, it says 'My IP Information:' and lists: 'ISP: Amazon Data Services', 'India', 'City: Mumbai', 'Region: Maharashtra', and 'Country: India'. To the right, it says 'Your location may be exposed!' and shows a map of Mumbai with a red pin. A tooltip on the map says 'Click for more details about 65.0.93.148'. At the bottom, there is a red button with a shield icon that says 'HIDE MY IP ADDRESS NOW' and a link 'Show Complete IP Details'. On the right, it says 'Location not accurate?' and 'Update My IP Location'. The footer includes 'Leaflet | © OpenStreetMap Terms'.

15. Navigate to configuration -> VPN settings -> configure the routing

Specify the private subnets -> you can give your private subnet range in the field

(YES I CHANGED) (I forgot to take screenshot)

16. Click on save changes

Note : Everytime when your public ip got

17. Now you need to connect to the VPN network using VPN connect , launch "open vpn connect from your windows" . You need to import the profile using the VPN url. Once you did you can connect using your username password

The screenshot shows the AWS EC2 Instances page. A table lists four instances: 'private_02', 'test-instance-01', 'openvpn_server-01', and 'private_01'. The 'private_01' row is selected, indicated by a blue border. A context menu is open over this row, with 'Start instance' highlighted in blue. Other options in the menu include 'Stop instance', 'Reboot instance', 'Hibernate instance', and 'Terminate instance'. The 'Terminate instance' option has a note below it stating '2/2 checks passed'. The page also includes a search bar, a toolbar with various icons, and navigation links for Mumbai and the user's session.

The screenshot shows the 'Connect to instance' dialog for instance `i-0179f4b90df022f6a`. The 'EC2 Instance Connect' tab is selected. The 'Connection Type' section offers two options: 'Connect using EC2 Instance Connect' (disabled) and 'Connect using EC2 Instance Connect Endpoint' (selected). The 'Private IP address' field contains `10.0.3.42`. The 'User name' field contains `ec2-user`, with a note below it stating 'Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ec2-user.' A red arrow points from this note to the 'Select an endpoint' dropdown. The 'Max tunnel duration (seconds)' input field is set to `3600`, with a note below it stating 'The maximum allowed duration of the SSH connection. Must comply with the maxTunnelDuration condition (if specified) in the IAM policy.' The 'EC2 Instance Connect Endpoint' section notes that only completed endpoints can be selected. A note at the bottom states: 'In most cases, the default user name, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.'

PRIVATE INSTANCE-1

```
'  #  
 \_###_ Amazon Linux 2023  
 \###|  
 \#/ __ https://aws.amazon.com/linux/amazon-linux-2023  
 V~.'->  
 /  
 /_/  
 /m/  
 Last login: Thu Nov  2 16:14:05 2023 from 10.0.3.225  
 [ec2-user@ip-10-0-3-42 ~]$ ip a  
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
     inet 127.0.0.1/8 scope host lo  
       valid_lft forever preferred_lft forever  
       inet6 ::1/128 scope host noprefixroute  
         valid_lft forever preferred_lft forever  
 2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000  
     link/ether 02:27:b9:de:10:7c brd ff:ff:ff:ff:ff:ff  
     altname eni-0dd040d9b0241ec81  
     altname device-number-0  
     inet 10.0.3.42/24 metric 512 brd 10.0.3.255 scope global dynamic enX0  
       valid_lft 3137sec preferred_lft 3137sec  
       inet6 fe80::27:b9ff:fede:107c/64 scope link  
         valid_lft forever preferred_lft forever  
[ec2-user@ip-10-0-3-42 ~]$ ■  
  
accessed  
Firest machine
```

PRIVATE INSTANCE-2

```
'  #  
 \_###_ Amazon Linux 2023  
 \###|  
 \#/ __ https://aws.amazon.com/linux/amazon-linux-2023  
 V~.'->  
 /  
 /_/  
 /m/  
 [ec2-user@ip-10-0-4-113 ~]$ ip a  
 1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
     link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
     inet 127.0.0.1/8 scope host lo  
       valid_lft forever preferred_lft forever  
       inet6 ::1/128 scope host noprefixroute  
         valid_lft forever preferred_lft forever  
 2: enX0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000  
     link/ether 0a:a6:a8:5a:56:ae brd ff:ff:ff:ff:ff:ff  
     altname eni-0d0918dfd2079fb23  
     altname device-number-0  
     inet 10.0.4.113/24 metric 512 brd 10.0.4.255 scope global dynamic enX0  
       valid_lft 3582sec preferred_lft 3582sec  
       inet6 fe80::8a6:a8ff:fe5a:56ae/64 scope link  
         valid_lft forever preferred_lft forever  
[ec2-user@ip-10-0-4-113 ~]$ ■  
  
Second machine
```

we can see our **private IP range**

The screenshot shows the OpenVPN configuration interface. On the left, there's a sidebar with links for AUTHENTICATION, TOOLS, DOCUMENTATION, and SUPPORT, along with a Logout button and a Powered by OpenVPN logo. The main area has a "Routing" section where users can specify private subnets (e.g., 10.0.0.0/16). It also includes questions about routing client traffic through the VPN and allowing network access to the gateway. Below that is a "DNS Settings" section with options for pushing DNS servers to clients.

My VPC



Instance 1 (private)

```
~/Desktop/ssh-keys/aws.02 (3.126s)
ssh -i "private_02.pem" ec2-user@10.0.4.113
The authenticity of host '10.0.4.113 (10.0.4.113)' can't be established.
ED25519 key fingerprint is SHA256:E9H61UJC1mBPFbtUW050HrHjCqjEt12Q/Z1E102n9uQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.4.113' (ED25519) to the list of known hosts.

ec2-user@ip-10-0-4-113.ap-south-1.compute.internal ~
```

Instance 2 (private)

```
~/Desktop/ssh-keys/aws .02 (3.873s)
ssh -i "private_01.pem" ec2-user@10.0.3.42
The authenticity of host '10.0.3.42 (10.0.3.42)' can't be established.
ED25519 key fingerprint is SHA256:9xsDcrmMz4+GsYNUHCUyrQZEA1WhJWjH9f4Pfmhz3iY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.42' (ED25519) to the list of known hosts.

ec2-user@ip-10-0-3-42.ap-south-1.compute.internal ~
```