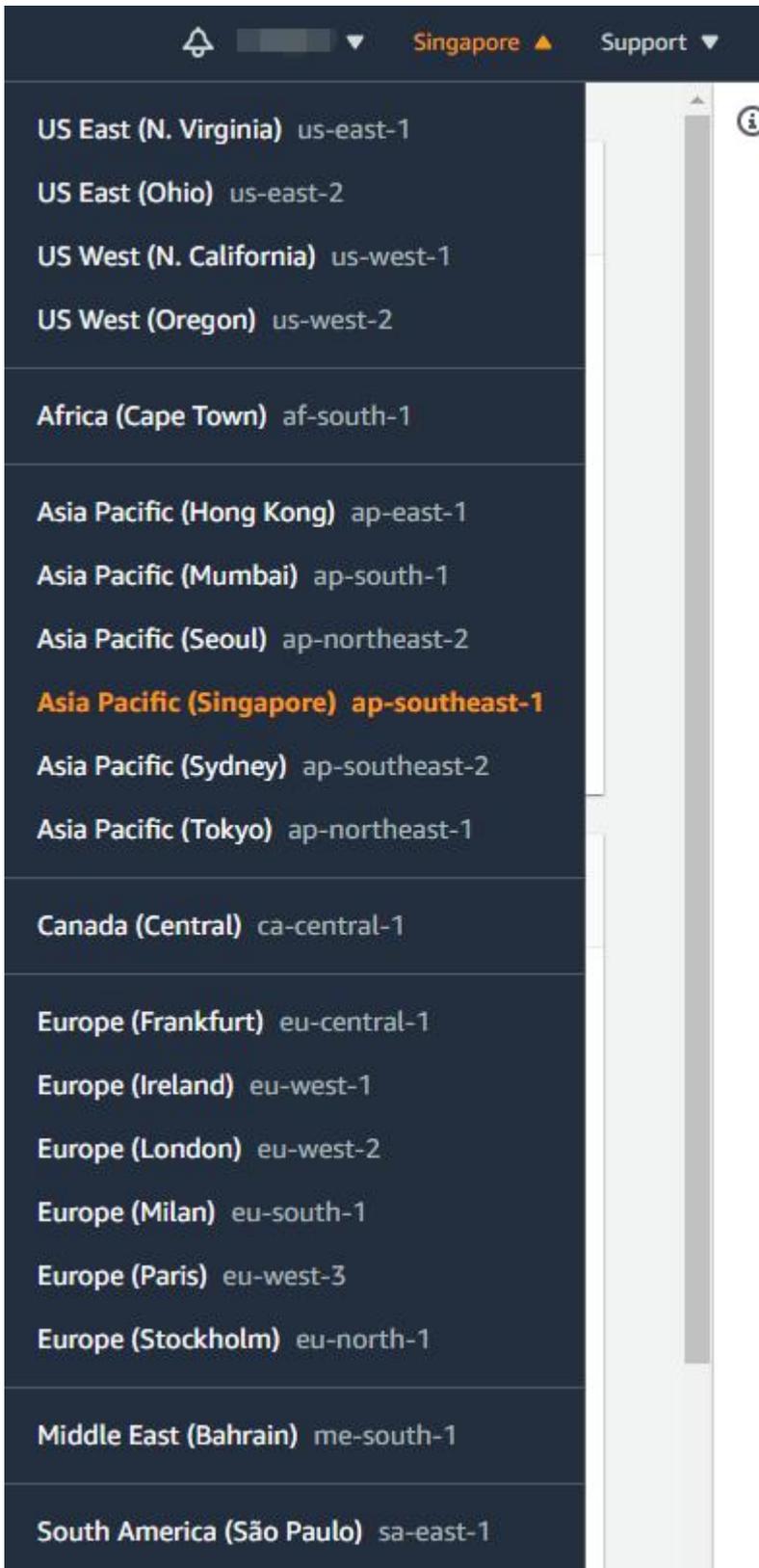


How to Build C3 Bonding Server by AWS EC2 For Ubuntu 18.04

V1.0, Nov 2, 2023

1. Visit <https://aws.amazon.com>, register and complete your account verification.
 - a. Choose the **region** that suits you best.



d. Click on "Browse more AMIs", type "ubuntu-bionic-18.04-amd64-server" & search, then select the correct one,

[EC2](#) > [Instances](#) > 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

[My AMIs](#) | [Quick Start](#)

						<div style="border: 2px solid red; padding: 5px;"> Browse more AMIs Including AMIs from AWS, Marketplace and the Community</div>
---	---	---	---	--	---	---

Q:

Quickstart AMIs (0) | My AMIs (3) | AWS Marketplace AMIs (2) | **Community AMIs (101)**

Refine results

Clear all filters

Operating system

Linux/Unix

- All Linux/Unix
- Amazon Linux
- CentOS
- Debian
- Fedora
- Gentoo

ubuntu-bionic-18.04-amd64-server (101 filtered, 101 unfiltered)

Community AMIs
Community AMIs contain all AMIs that are public, therefore anyone can publish an AMI and it will show in this catalog. This catalog can also contain paid products. When using community AMIs it is best practice to ensure you know and trust the publisher before launching an AMI.

ubuntu Verified provider
ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server-20220104
ami-0788ed331c80d7f13
Canonical, Ubuntu, 18.04 LTS, amd64 bionic image build on 2022-01-04
OwnerAlias: amazon Platform: Ubuntu Architecture: x86_64 Owner: 099720109477 Publish date: 2022-01-04
Root device type: ebs Virtualization: hvm ENA enabled: Yes

Select

e. Select the exist Key pair or **Create new key pair** – Private key file format based on your demand, you can choose .pem or .ppk then click Create key pair and save it. For Windows OS – select the ppk would be better (Connect with PuTTY).

▼ **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 key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

C3-SG

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

RSA
RSA encrypted private and public key pair

ED25519
ED25519 encrypted private and public key pair

Private key file format

.pem
For use with OpenSSH

.ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) [↗](#)

Cancel
Create key pair

f. **Network settings** – Click “Edit” to set Inbound rules. You can open the ports as per your requirements. It is suggested to open port 22 for SSH, port 54321 for the bonding server admin panel, and port 54322 for aggregating traffic.

▼ **Network settings** [Info](#)
Edit

▼ Network settings [Info](#)

VPC - *required* [Info](#)

vpc-604d1004 (default) ▼

172.31.0.0/16

Subnet [Info](#)

No preference ▼

[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*

launch-wizard-1

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](#)

launch-wizard-1 created 2023-11-02T03:09:31.663Z

Inbound Security Group Rules

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

[Remove](#)

Type [Info](#)

ssh ▼

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere ▼

Source [Info](#)

Add CIDR, prefix list or security

Description - *optional* [Info](#)

e.g. SSH for admin desktop

0.0.0.0/0

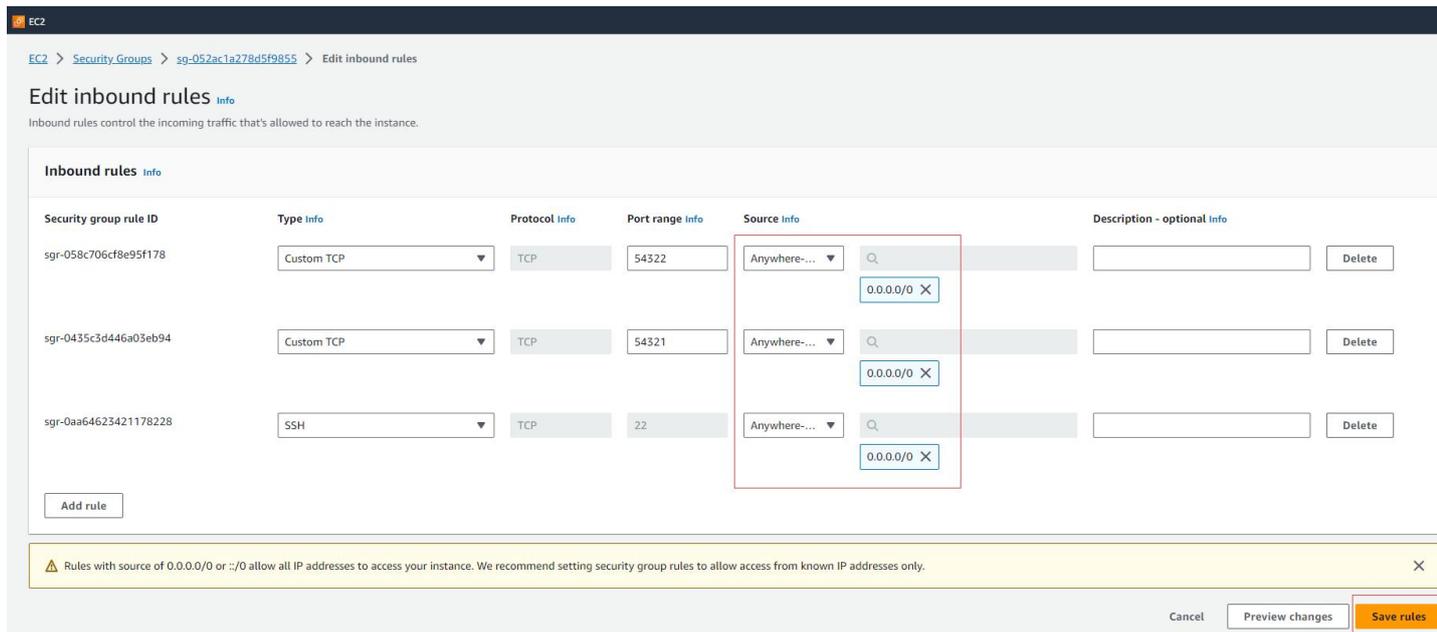
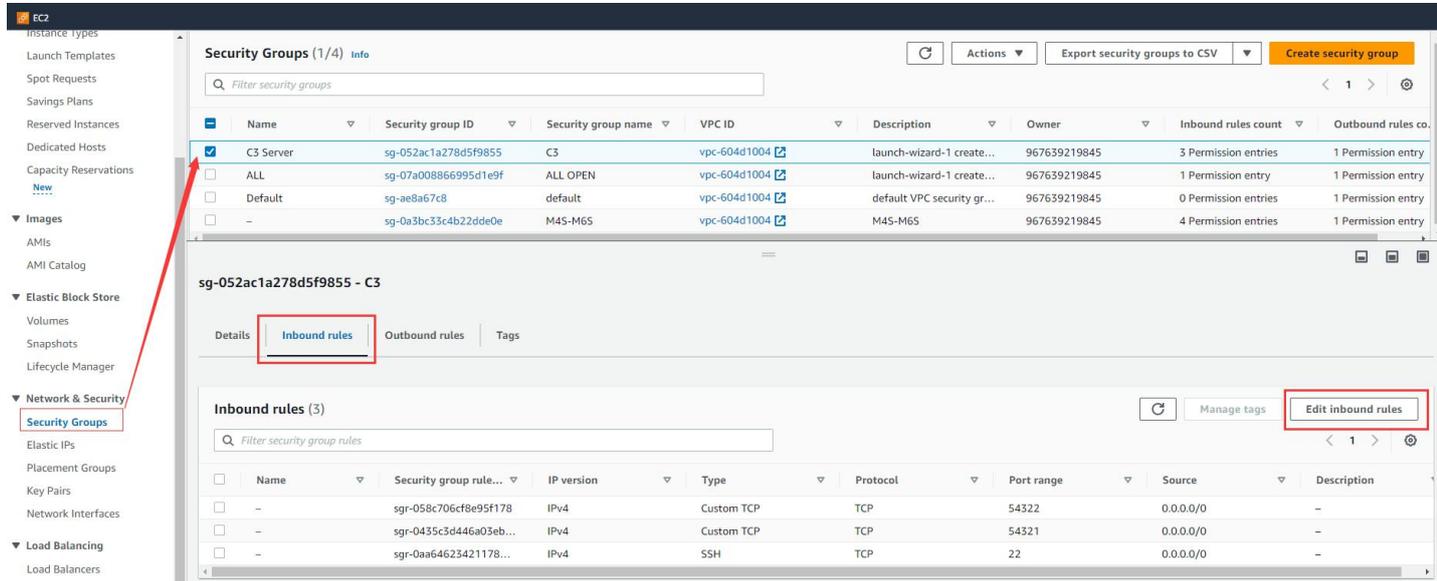
for the "Inbound Security Group Rules", once an EC2 instance is created, you can modify its associated security groups at any time.

Here are the steps to modify the inbound rules for a security group:

1. In the navigation pane, choose 'Security Groups'.
2. Select the security group that's associated with the EC2 instance.

3. Choose the 'Inbound rules' tab, and then choose 'Edit inbound rules'.
4. In the dialog box, you can add, remove, or modify rules.
5. When you're done, choose 'Save rules'.

Please note that these changes will take effect immediately, and traffic that's not allowed by the rules is automatically dropped. Also, remember to follow best practices for security group rules to ensure your resources are protected.



- g. Launch Instance – click the launched instance,

Description - required [Info](#)

unch-wizard-2 created 2023-05-26T01:20:21.740Z

Bound security groups rules

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

[Remove](#)

[Info](#)

h

[Info](#)

TCP

[Info](#)

22

[Info](#)

anywhere

[Info](#)

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

[Info](#)

e.g. SSH for admin desktop

0.0.0.0/0 [X](#)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#)

[Launch instance](#)

[Review commands](#)

[EC2](#) > [Instances](#) > [Launch an instance](#)

Success

Successfully initiated launch of instance **(i-0c08ed16f275795ff)**

h. Start & Stop Terminate EC2

If you're not using the server all the time, you can stop the instance to save costs. When you need to use the instance again, you can start it. However, please note that once restarted, the server's public IPv4 will change. If you want your C3 server IP to remain consistent with your EC2 instance's IP, you might need to consider using Elastic IP. Elastic IP is a static IPv4 address provided by AWS that can be bound to any instance. Even if the instance is stopped and restarted, the Elastic IP remains unchanged. This way, you can ensure that the IP address remains the same no matter when the EC2 instance is started or stopped. But please note that while each AWS account has one free Elastic IP, AWS will charge a certain fee if the Elastic IP is not bound to a running instance. Therefore, it's best to release the Elastic IP when not using the EC2 instance to avoid additional fees.

Instances (1/1) Info							
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/> C3 Bonding Se...	i-0c08ed16f275795ff	Running	t2.micro	2/2 checks passed	No alarms	ap-southeast-1a	ec2

[Instance state](#) ▲

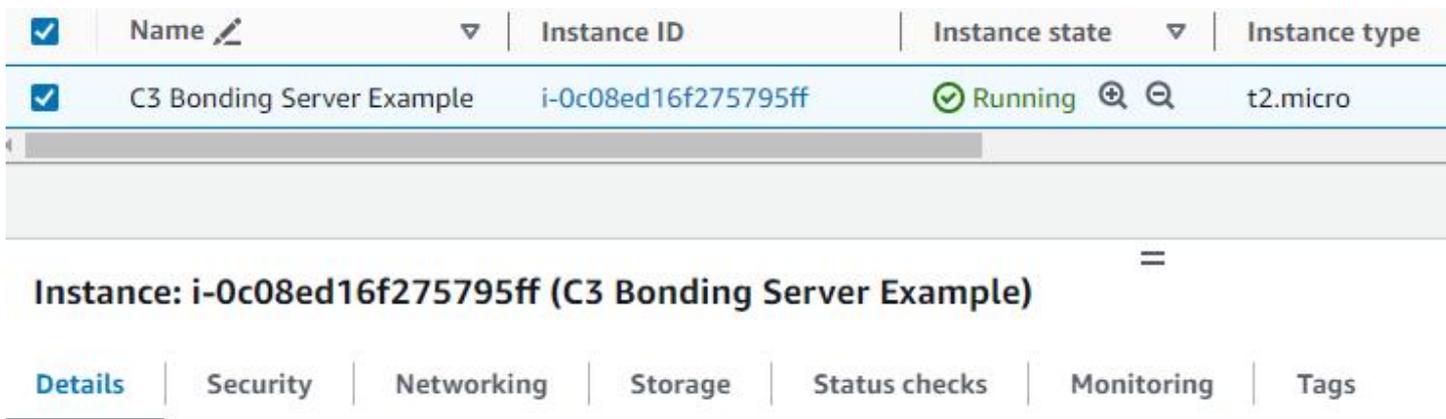
- [Stop instance](#)
- [Start instance](#)
- [Reboot instance](#)
- [Hibernate instance](#)
- [Terminate instance](#)

2. Connect to Amazon EC2 Instance & install the bonding software on it.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html>

Here from Windows OS with PuTTY , you can download the PuTTY here,

<https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

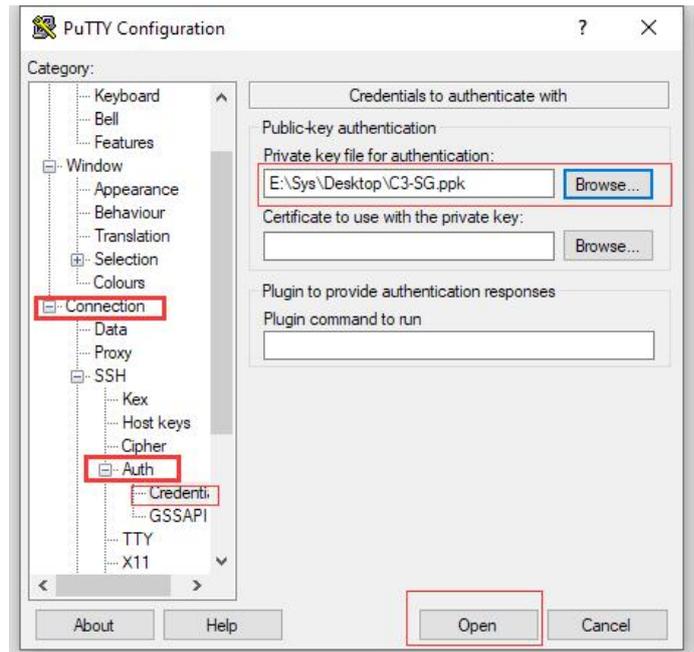
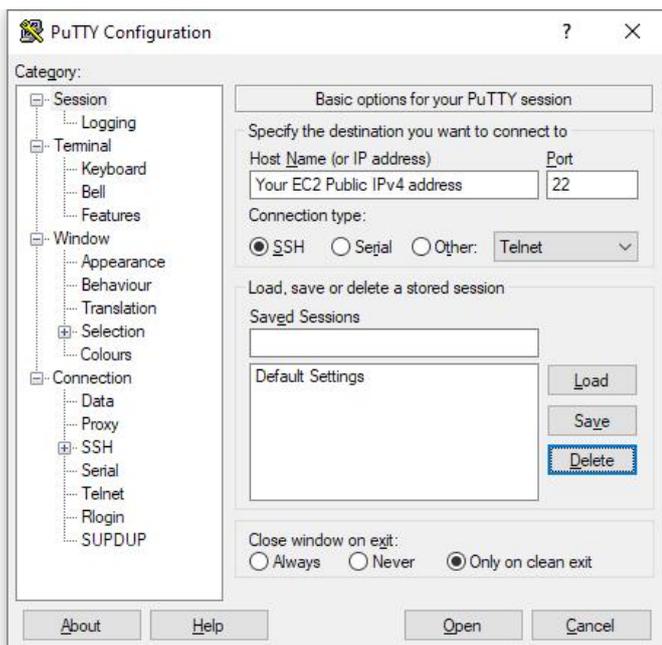


▼ Instance summary **Info**

Instance ID
 i-0c08ed16f275795ff (C3 Bonding Server Example) Public IPv4 address
54. [redacted] | open address

1. Launch PuTTY.
2. In the 'Host Name (or IP address)' field, paste the EC2 Public IPv4 address.
3. Ensure that the 'Port' is set to 22 and 'Connection type' is set to SSH.
4. In the 'Category' pane on the left, expand 'Connection', expand 'SSH', then 'Auth', select the Credentials,
5. Click 'Browse' and select the .ppk file that you saved earlier.
6. Click 'Open' to start the PuTTY session.

If a security alert about the host key is not cached for this server, choose 'Accept' to add the key to PuTTY's cache and connect to your instance.



login as **ubuntu**, type **sudo -s** switch to root, by below commands (this commands may update, please contact with the seller or our tech support to get the latest) to install the bonding software,

wget https://gitee.com/link4all_admin/vps/raw/master/debian_ubuntu_install.sh -O debian_ubuntu_install.sh && sh debian_ubuntu_install.sh

```

root@ip-172-31-17-189: ~
login as: ubuntu
Authenticating with public key "C3-SG"
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1061-aws x86_64)

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

System information as of Thu Nov  2 03:34:39 UTC 2023

System load:  0.0          Processes:            93
Usage of /:   15.0% of 7.69GB Users logged in:     0
Memory usage: 20%         IP address for eth0: 172.31.17.189
Swap usage:   0%

0 updates can be applied immediately.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-17-189:~$ sudo -s
root@ip-172-31-17-189:~# wget https://gitee.com/link4all_admin/vps/raw/master/debian_ubuntu_install.sh -O debian_ubuntu_install.sh && sh debian_ubuntu_install.sh

```

when in installing, if any promotion, type Y and click Enter to continue

```

iptables-persistent netfilter-persistent
0 upgraded, 2 newly installed, 0 to remove and 3 not upgraded.
Need to get 13.8 kB of archives.
After this operation, 89.1 kB of additional disk space will be used.
Do you want to continue? [Y/n] y

```

Reboot the EC2 server by **reboot** command after the bonding software installed.

```

install.sh: 99: echo Success, please allow TCP ports 59999, 60011 (for network bondin
root@ip-172-31-12-224:/home/ubuntu# reboot

```

To check your server port open status by <http://adminkit.net/telnet.aspx>

Connection Status : **Connection to 54.234.21.12 on port 54321 was successful**