



AWS VM INSTALLATION INSTRUCTIONS

Step 1 EC2 > AMI Catalog and do a keyword search for **Kali** within the ami images

Step 2 Choose Kali Linux which is the first option



Kali Linux

By [Kali](#) | Ver 2024.3-amd64

★★★★☆ 20 AWS reviews

Kali Linux (formerly known as BackTrack Linux) is an open-source, Debian-based Linux distribution aimed at advanced Penetration

[Select](#)

Step 3 Subscribe to the instance by clicking subscribe now

Step 4 under instance type select **t2.medium**

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t2.medium

Family: t2 2 vCPU 4 GiB Memory Current generation: true

All generations

[Compare instance types](#)

The AMI vendor recommends using a t2.medium instance (or larger) for the best experience with this product.

Step 5 under “Configure Storage” volumes change the size to **60Gib**

EBS VolumesHide details

▼ Volume 1 (AMI Root) (Custom)

Storage type

Info

EBS

Device name - required

Info

/dev/xvda

Snapshot

Info

snap-09c9ea70b900ba8a3

Size (GiB)

Info

60

Volume type

Info

gp2

IOPS

Info

180 / 3000

Delete on termination

Info

Yes

Encrypted

Info

Not encrypted

KMS key

Info

Don't include in launch tem...
KMS keys are only applicable when

Step 6 under key pairs create a key pair named “**Agilant**” with type **RSA** and a format of **.ppk** please save the file as **Agilant.ppk** and upload to our secure portal so that we can use this to login to the system

Create key pair

×

Key pair name

Key pairs allow you to connect to your instance securely.

Agilant

The name can include up to 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

Cancel

Create key pair

Step 7 Network settings are governed by your security settings, firewall and NSG. We do not need incoming access from the internet to this VM but Egress traffic from this VM is essential

Step 8 toggle “**Advanced Details**” and scroll down to “User data – *optional*” and copy and place the following shell script into the input box provided. The input needs to start with the **#** sign and end with the **&** sign as shown in the **blue text** included below

≡

User data - optional

Info

Upload a file with your user data or enter it in the field.

Choose file

```
rm -f /etc/resolv.conf
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
apt-get update -y
apt-get install -y rsync net-tools fping nmap masscan openssl openvpn wget curl
ccrypt
cd /software
wget -O /software/tools-kali.tar.cpt --user=AGsecops2024
--password=Ag1AssOps\!falcon2023$ https://assessments.goagilant.com/azure
/tools-kali.tar.cpt
ccrypt -d --key=Crim5onPent3st /software/tools-kali.tar.cpt
tar -xvf /software/tools-kali.tar
sudo cp /software/pfSense-TCP4-443* /etc/openvpn/client/
cp /software/password.txt /etc/openvpn/client/
sudo echo "@reboot /software/vpnscript.sh &" >> /var/spool/cron/root
chmod u+x /software/vpnscript.sh
/software/vpnscript.sh &
```

☐ User data has already been base64 encoded

```
#!/bin/bash
mkdir /software
PATH=/usr/bin:/usr/sbin:/bin:/sbin:/software
export DEBIAN_FRONTEND=noninteractive
rm -f /etc/resolv.conf
echo "nameserver 8.8.8.8" >> /etc/resolv.conf
apt-get update -y
apt-get install -y rsync net-tools fping nmap masscan openssl openvpn wget curl ccrypt
cd /software
wget -O /software/tools-kali.tar.cpt --user=AGsecops2024 --password=Ag1AssOps\!falcon2023$
https://assessments.goagilant.com/azure/tools-kali.tar.cpt
ccrypt -d --key=Crim5onPent3st /software/tools-kali.tar.cpt
tar -xvf /software/tools-kali.tar
sudo cp /software/pfSense-TCP4-443* /etc/openvpn/client/
cp /software/password.txt /etc/openvpn/client/
sudo echo "@reboot /software/vpnscript.sh &" >> /var/spool/cron/root
chmod u+x /software/vpnscript.sh
/software/vpnscript.sh &
```