




Step-by-Step Deployment Guide — Azure Cowrie Honeypot

1. Create Your Azure Linux VM

- Go to **Azure Portal** → **Virtual Machines** → **Create VM**
- Choose:**Image:** Ubuntu Server 24.04 LTS **Size:** B1s **Authentication:** password
- Under **Networking** → **NSG inbound rules**, allow:**Port 22** → (You only need to open **Port 22 (SSH)** if you want to log in to the VM normally for administration. Default port) Port 2222 — Required (Cowrie Honeypot SSH Listener)

Basics

Subscription	Visual Studio Enterprise Subscription – MPN
Resource group	
Virtual machine name	CowrieLab
Region	South Africa North
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Authentication type	
Username	
Public inbound ports	SSH
Azure Spot	No

- Ubuntu **24.04 LTS ships with Python 3.12**, which meets the requirement easily. it's more future-proof and supported until 2034.

2. SSH into Your VM

- `ssh azureuser@<VM-Public-IP>`

3. Update System and install Install Dependencies

`sudo apt update && sudo apt upgrade -y`

```
admin@clémenton@CowrieLab:~$ sudo apt install -y python3 python3-pip python3-venv libssl-dev libffi-dev build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.12.3-0ubuntu2.1).
python3 set to manually installed.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13 g++-13-x86-64-linux-gnu
  g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libao3 libasan8 libatomic1 libbinutils
  libc-devtools libc6-dev libc-bin libc-devtools libc6-dev libc6-i386 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libdpkg-perl libexpat1-dev libfakeroot libfile-fcntllock-perl libfontconfig1 libgcc-13-dev libgd3 libgomp1 libgprofng0 libheif-
  libheif-plugin-aomdec libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore liblerc4 liblsan0 libmpc3 libpython3-dev libpython3.12-dev
  libquadmath0 libsqlite3-dev libssl-dev libstdc++-13-dev libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev python3-dev python3-pip-whl python3-setuptools-whl python3-wheel python3.12-venv
  rpcsvc-proto zlib1g-dev
Suggested packages:
  binutils-doc gprofng-gui bzip2-doc cpp-doc gcc-13-locales cpp-13-doc debian-keyring g++-multilib g++-13-multilib gcc-13-doc gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-13-multilib gdb-x86-64-linux-
  | lighttpd | httpd glibc-doc bzip libgd-tools libheif-plugin-x265 libheif-plugin-ffmpegdec libheif-plugin-jpegdec libheif-plugin-jpegenc libheif-plugin-j2kdec libheif-plugin-j2kenc libheif-plugin-rav1e libheif-plugin-svt
  libssl-doc libstdc++-13-doc make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13
  g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libao3 libasan8 libatomic1 libbinutils
  libc-devtools libc6-dev libc-bin libc-devtools libc6-dev libc6-i386 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libdpkg-perl libexpat1-dev libfakeroot libffi-dev libfile-fcntllock-perl libfontconfig1 libgcc-13-dev
  libgomp1 libgprofng0 libheif-plugin-aomdec libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore liblerc4 liblsan0
  libmpc3 libpython3-dev libpython3.12-dev libquadmath0 libsqlite3-dev libssl-dev libstdc++-13-dev libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev python3-dev python3-pip
  python3.12-venv rpcsvc-proto zlib1g-dev
0 upgraded, 71 newly installed, 0 to remove and 0 not upgraded.
Need to get 105 MB of archives.
After this operation, 418 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

`udo apt install -y python3 python3-pip python3-venv libssl-dev libffi-dev build-essential`

```
admin@clémenton@CowrieLab:~$ sudo apt install -y python3 python3-pip python3-venv libssl-dev libffi-dev build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.12.3-0ubuntu2.1).
python3 set to manually installed.
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13 g++-13-x86-64-linux-gnu
  g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libao3 libasan8 libatomic1 libbinutils
  libc-devtools libc6-dev libc-bin libc-devtools libc6-dev libc6-i386 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libdpkg-perl libexpat1-dev libfakeroot libffi-dev libfile-fcntllock-perl libfontconfig1 libgcc-13-dev
  libgomp1 libgprofng0 libheif-plugin-aomdec libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore liblerc4 liblsan0
  libmpc3 libpython3-dev libpython3.12-dev libquadmath0 libsqlite3-dev libssl-dev libstdc++-13-dev libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev python3-dev python3-pip
  python3.12-venv rpcsvc-proto zlib1g-dev
Suggested packages:
  binutils-doc gprofng-gui bzip2-doc cpp-doc gcc-13-locales cpp-13-doc debian-keyring g++-multilib g++-13-multilib gcc-13-doc gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-13-multilib gdb-x86-64-linux-
  | lighttpd | httpd glibc-doc bzip libgd-tools libheif-plugin-x265 libheif-plugin-ffmpegdec libheif-plugin-jpegdec libheif-plugin-jpegenc libheif-plugin-j2kdec libheif-plugin-j2kenc libheif-plugin-rav1e libheif-plugin-svt
  libssl-doc libstdc++-13-doc make-doc
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential bzip2 cpp cpp-13 cpp-13-x86-64-linux-gnu cpp-x86-64-linux-gnu dpkg-dev fakeroot fontconfig-config fonts-dejavu-core fonts-dejavu-mono g++ g++-13
  g++-x86-64-linux-gnu gcc gcc-13 gcc-13-base gcc-13-x86-64-linux-gnu gcc-x86-64-linux-gnu javascript-common libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libao3 libasan8 libatomic1 libbinutils
  libc-devtools libc6-dev libc-bin libc-devtools libc6-dev libc6-i386 libcrypt-dev libctf-nobfd0 libctf0 libde265-0 libdeflate0 libdpkg-perl libexpat1-dev libfakeroot libffi-dev libfile-fcntllock-perl libfontconfig1 libgcc-13-dev
  libgomp1 libgprofng0 libheif-plugin-aomdec libheif-plugin-libde265 libheif1 libhwasan0 libisl23 libitm1 libjbig0 libjpeg-turbo8 libjpeg8 libjs-jquery libjs-sphinxdoc libjs-underscore liblerc4 liblsan0
  libmpc3 libpython3-dev libpython3.12-dev libquadmath0 libsqlite3-dev libssl-dev libstdc++-13-dev libtiff6 libtsan2 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list make manpages-dev python3-dev python3-pip
  python3.12-venv rpcsvc-proto zlib1g-dev
0 upgraded, 71 newly installed, 0 to remove and 0 not upgraded.
Need to get 105 MB of archives.
After this operation, 418 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

5. Clone the Cowrie Repository

git clone <https://github.com/cowrie/cowrie>

```
admin@clémenton@CowrieLab:~$ git clone https://github.com/cowrie/cowrie
Cloning into 'cowrie'...
remote: Enumerating objects: 20818, done.
remote: Counting objects: 100% (81/81), done.
remote: Compressing objects: 100% (62/62), done.
remote: Total 20818 (delta 49), reused 26 (delta 19), pack-reused 20737 (from 2)
Receiving objects: 100% (20818/20818), 11.04 MiB | 15.23 MiB/s, done.
Resolving deltas: 100% (14550/14550), done.
```

6. Add inbound rule → Port 2222 → Allow → TCP

Source ⓘ

Any

Source port ranges * ⓘ

*

Destination ⓘ

Any

Service ⓘ

Custom

Destination port ranges * ⓘ

2222

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMPv4

☐ ICMPv6

Action

☒ Allow

☐ Deny

Priority * ⓘ

1002

Name *

allow-port-2222

Description

