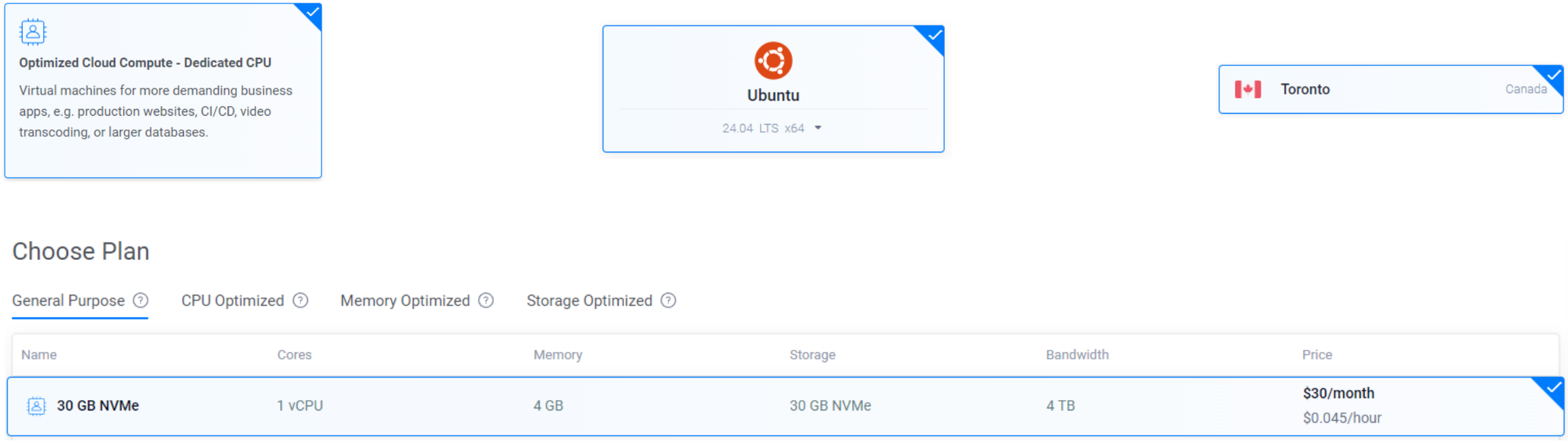
Day 12 - Ubuntu Server 24.02 Installation

Obiettivi

- **Setup di Server SSH**
- **Vedere Log di Autenticazione**

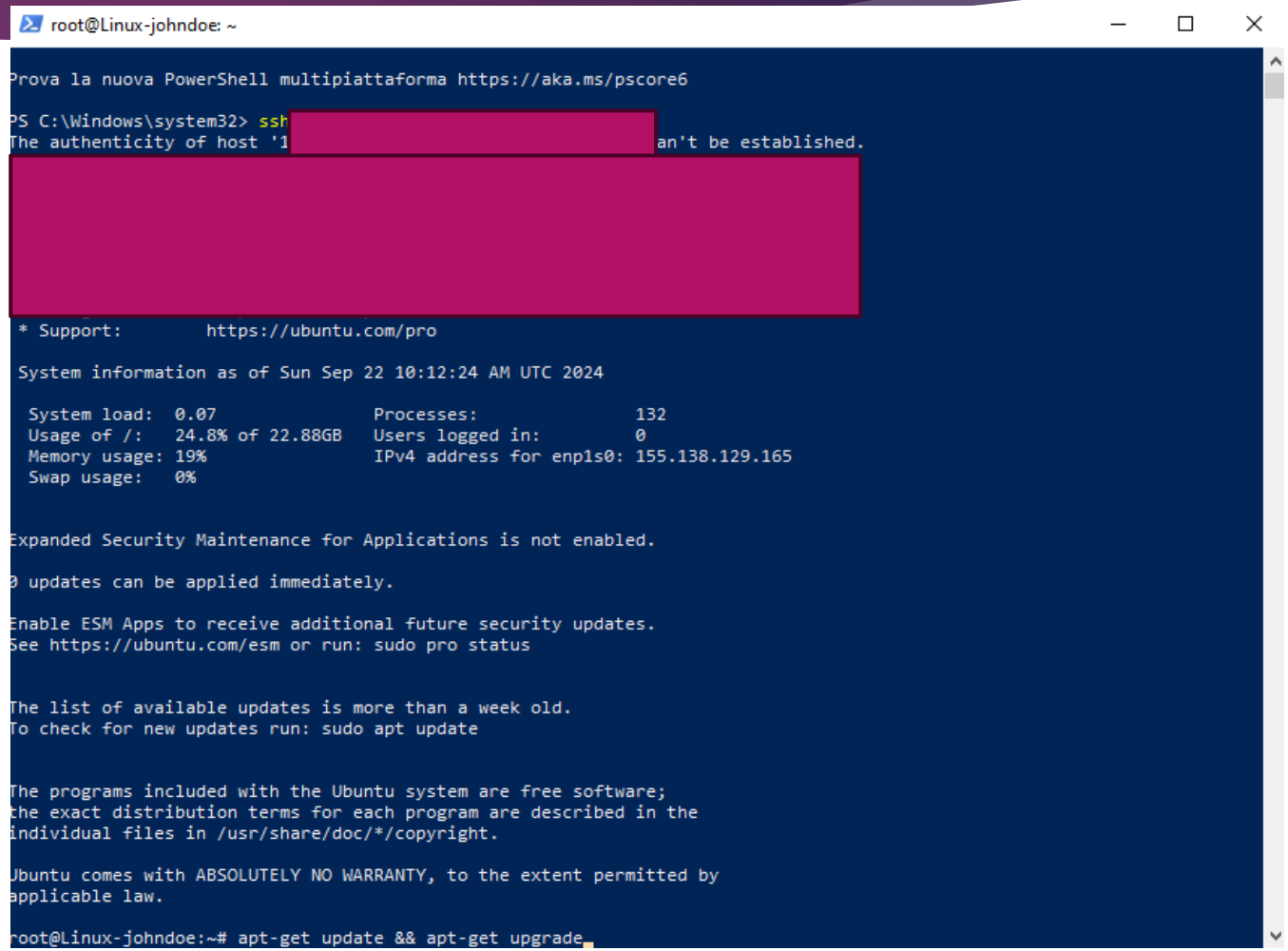
Ubuntu Server

Procediamo con il deployment di un **Ubuntu Server**, configurato con le seguenti specifiche:



Ubuntu Server

Anche in questo caso, mi collego all' **Ubuntu Server** tramite **SSH**, eseguo l'aggiornamento dei repository con i comandi `apt-get update` e `apt-get upgrade`.



Ubuntu Server

Ora accediamo alla cartella dei log, e puntiamo il file auth.log.
Qui possiamo osservare i tentativi di autenticazione.

Per simulare dei tentativi, ho aperto un'altra shell dove ho intenzionalmente inserito delle password errate.

Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multipiattaforma https://aka.ms/pscore6

PS C:\Users\royve> ssh root@155
root@155.: password:
ublickey,password).
PS C:\Users\royve>
```

root@Linux-johndoe: ~

```
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sun Sep 22 10:12:24 AM UTC 2024

  System load:  0.07               Processes:               132
  Usage of /:   24.8% of 22.88GB   Users logged in:         0
  Memory usage: 19%                IPv4 address for enp1s0: 155.138.129.165
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


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


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.

root@Linux-johndoe:~# apt-get update && apt-get upgrade
```

Ubuntu Server

Col comando ‘grep –i failed auth.log’ possiamo filtrare tutte le entries che contengono la parola ‘Failed’(-i ignora la ‘Case Sensitivity’).

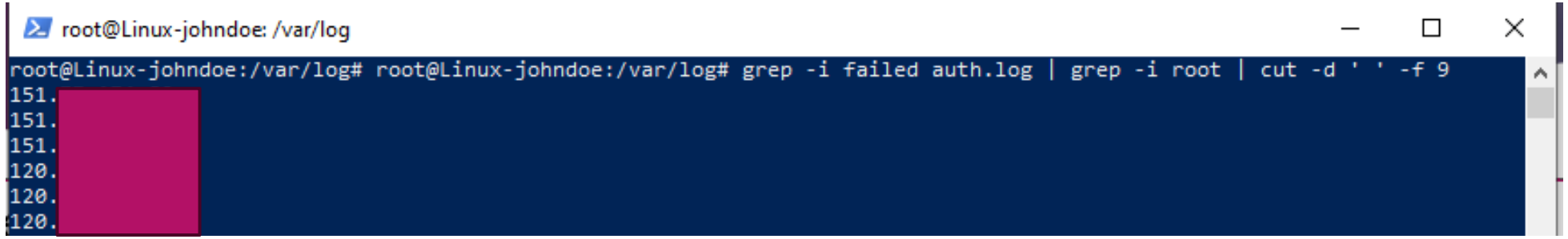
```
root@Linux-johndoe:/var/log# grep -i failed auth.log
2024-09-22T10:25:05.764976+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] port 57482 ssh2
2024-09-22T10:25:10.902327+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] port 57482 ssh2
2024-09-22T10:25:14.296620+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] port 57482 ssh2
```

Potrebbe non bastarci per cui andiamo oltre e tra i risultati che abbiamo ottenuto con failed filtriamo quelli per l’utente root col comando ‘grep –i failed auth.log | grep –i root’:

```
root@Linux-johndoe:/var/log# grep -i failed auth.log | grep -i root
2024-09-22T10:25:05.764976+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] rt 57482 ssh2
2024-09-22T10:25:10.902327+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] rt 57482 ssh2
2024-09-22T10:25:14.296620+00:00 Linux-johndoe sshd[9874]: Failed password for root from 151[redacted] rt 57482 ssh2
2024-09-22T10:39:20.386180+00:00 Linux-johndoe sshd[9947]: Failed password for root from 120[redacted] ort 50002 ssh2
2024-09-22T10:39:25.355017+00:00 Linux-johndoe sshd[9949]: Failed password for root from 120[redacted] ort 50003 ssh2
```

Ubuntu Server

Fatto ciò, potrebbe essere utile conoscere solo l'IP delle macchine attaccanti. Per farlo, filtriamo ulteriormente l'output dell'ultimo comando utilizzando il comando 'cut':



- Con -d ' ' indichiamo di separare i campi all'interno dei record utilizzando lo spazio (' ') come delimitatore.
- Con -f 9 specifichiamo di mostrare solo il nono campo a partire da sinistra, che corrisponde agli IP delle macchine che stanno tentando di accedere al server.