


Day 5 – Windows Server

Windows Server


Procediamo col deploy di un nuovo server **Windows** su **Vultr** con le seguenti caratteristiche:

 **Toronto** Canada




Cloud Compute - Shared CPU

Virtual machines for apps with bursty performance, e.g. low traffic websites, blogs, CMS, dev/test environments, and small databases.



Windows Standard


2022 x64 **\$14.00/mo**



Auto Backups \$2.00/mo

Highly recommend for mission-critical systems. Backups enable easy recovery from a disaster by spinning up a new...

[Learn More](#)



IPv6 Free

If checked, an IPv6 address will be assigned to the instance.


Choose Plan

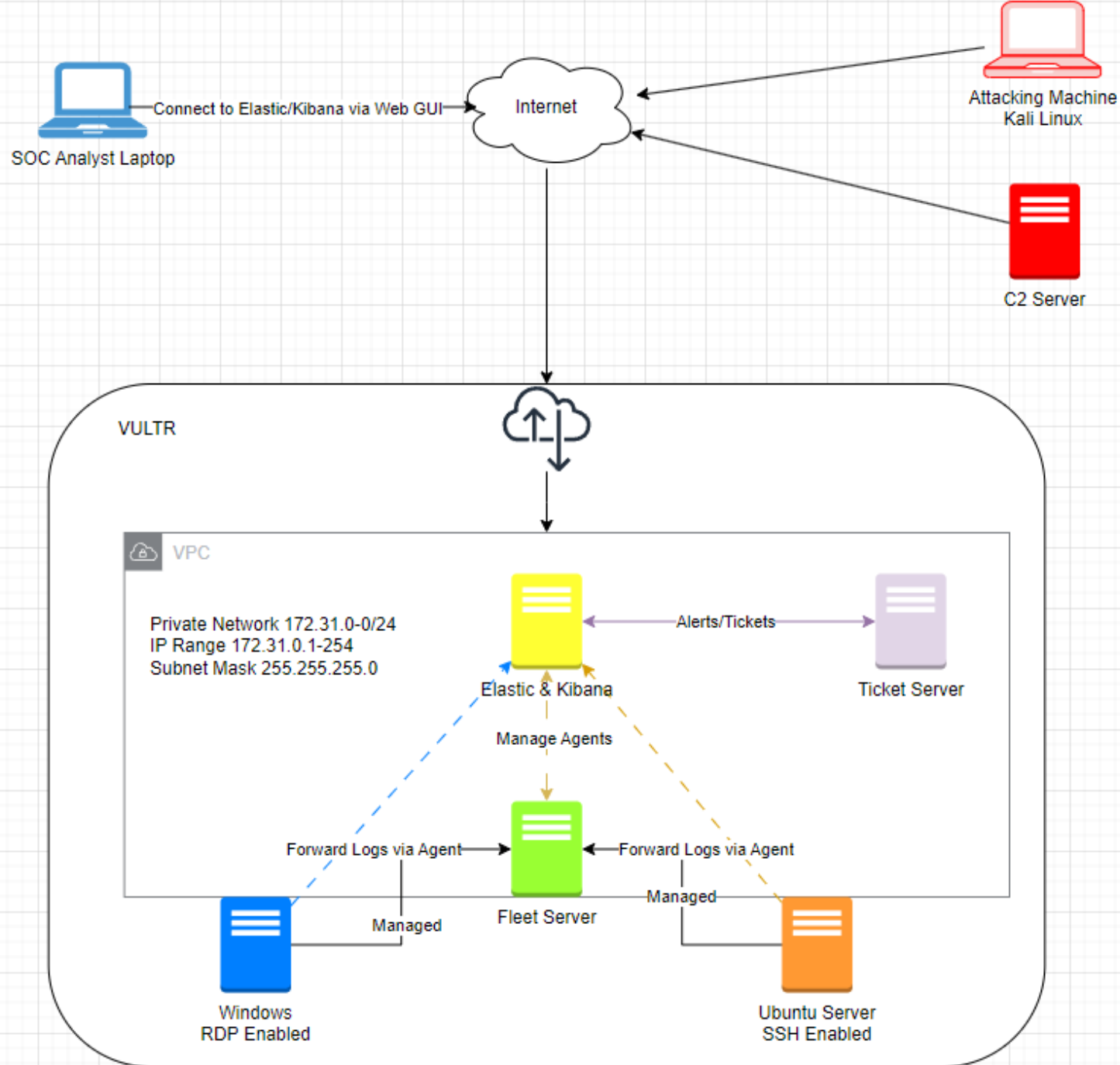
AMD High Performance ?

Intel High Performance ?

High Frequency ?

Regular Cloud Compute ?

Name	Cores	Memory	Storage	Bandwidth	Price
 55 GB SSD	1 vCPU	2 GB	55 GB SSD	2 TB	\$24/month \$0.036/hour



In questo caso non includiamo il server nella **VPC**. Aggiungeremo anche lo schema dell'architettura del nostro laboratorio. Questa scelta è motivata dal fatto che, se **il server Windows** venisse compromesso, l'attaccante potrebbe avere accesso al resto della rete. Pertanto, è necessario aggiornare il diagramma per riflettere questa modifica.

Windows Server







Ora sono attive due macchine sul cloud provider: oltre al server **ELK** (Kibana, Elastic), è in esecuzione anche il **server Windows**.

Cloud Compute

☰ Location ▼

🔍 Search

+ Deploy

<input type="checkbox"/>	Name	OS	Location	Charges	Status	
<input type="checkbox"/>	WIN-johndoe 2048.00 MB Regular Cloud Compute - 155. [REDACTED]		 Toronto	\$0.02	 Running	...
<input type="checkbox"/>	ELK 16384.00 MB Optimized Cloud - 155. [REDACTED]		 Toronto	\$13.75	 Running	...

Windows Server

Una volta disponibile, procediamo con l'accesso utilizzando la password indicata dal cloud provider.

The screenshot shows the Vultr control panel for a Windows Server instance named "WIN-johndoe". The instance is located in Toronto and was created 53 seconds ago. The interface includes tabs for Overview, Usage Graphs, Settings, Snapshots, Backups, User-Data, Tags, and DDOS. The Overview tab is selected, showing metrics for Bandwidth Usage (0GB), vCPU Usage (1 vCPU), and Current Charges (\$0.02). Below these metrics, the instance details are listed: Location (Toronto), ID Address (redacted), Username (Administrator), Password (redacted), vCPU/s (1 vCPU), RAM (2048.00 MB), Storage (55 GB SSD), Bandwidth (0 GB), Label (WIN-johndoe), OS (Windows 2022 Standard), and a "Add Tag +" button.

WIN-johndoe
Toronto Created 53 seconds ago

Overview Usage Graphs Settings Snapshots Backups User-Data Tags DDOS

Bandwidth Usage
0GB

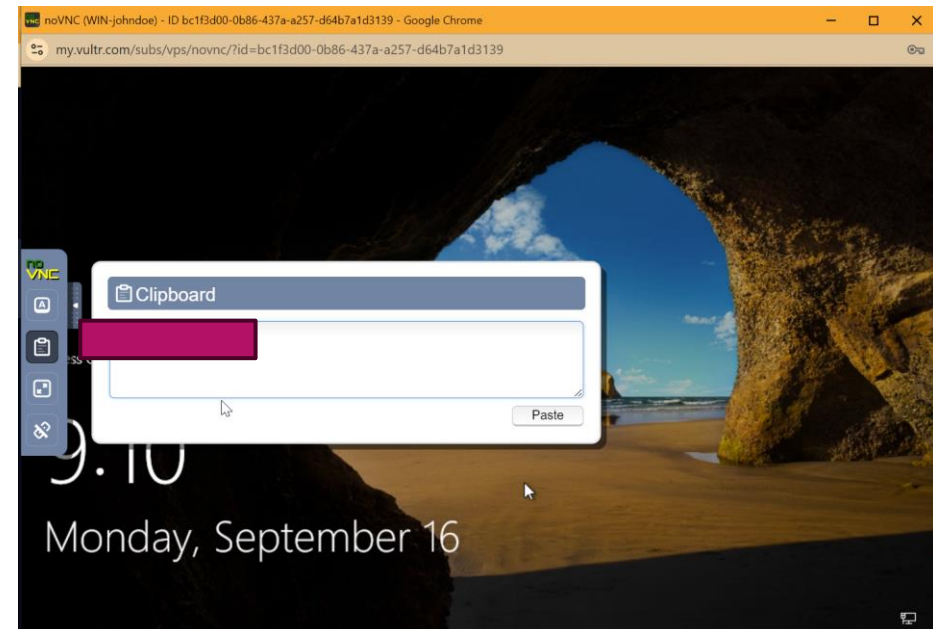
vCPU Usage
1 vCPU

Current Charges
\$0.02

Location: Toronto
ID Address: [redacted]
Username: Administrator
Password: [redacted]

vCPU/s: 1 vCPU
RAM: 2048.00 MB
Storage: 55 GB SSD
Bandwidth: 0 GB

Label: WIN-johndoe
OS: Windows 2022 Standard



Windows Server

Infine, mi assicuro che l'IP della macchina sia esposto pubblicamente provando ad accedere tramite **RDC** (Remote Desktop Connection) dal mio PC.

