

Підключення до віртуального сервера по SSH

SSH (Secure Shell або «безпечна оболонка» – **мережевий протокол** рівню застосунків) найчастіше використовується з метою віддаленого доступу до операційних систем (ОС) та безпечного пересилання файлів із шифруванням трафіку (включно з паролями). У якості зовнішньої «оболонки» для інших мережевих протоколів нижчого рівня, протокол SSH дозволяє організувати «тунелювання» – безпечну передачу шифрованих даних в незахищеному середовищі (Інтернет).

Під час роботи, SSH-сервер постійно «прослуховує» на порту 22 запити TCP-з'єднання від клієнтських комп'ютерів та у разі встановлення зв'язку проводить автентифікацію, починає обслуговування SSH-клієнта. Тому, у налаштуваннях групи безпеки «**default**» фаєрволу сервера встановіть **нове правило** – дозвольте вхідне (**Ingress**) з'єднання через **порт 22**.



Увага! З метою підвищення безпеки, рекомендується встановити правило виключно для однієї закріпленої за вами IP-адреси (визначеної вами для одноосібного віддаленого доступу до сервера):

The screenshot shows the GIGACLOUD interface for a Linux VM-1. A table lists security rules for the 'default' group. A blue arrow points to the rule with port 22.

Напрямок	Тип	Протокол	Діапазон портів	Віддалений	Дія
Ingress*	IPv4	TCP	443 - 443	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	TCP	22 - 22	185.168.128.165/32 (CIDR)	Видалити
Ingress*	IPv4	TCP	80 - 80	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	UDP	1 - 65535	0.0.0.0/0 (CIDR)	Видалити
Ingress*	IPv4	ICMP	8 -	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	1 - 45559	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	TCP	45561 - 65535	0.0.0.0/0 (CIDR)	Видалити
Egress*	IPv4	ICMP	-	0.0.0.0/0 (CIDR)	Видалити

*Ingress - вхідний трафік, Egress - вихідний трафік.

Більш детально про налаштування фаєрволу в хмарі S-Cloud наведено у [документі](#).

Якщо ви користуєтесь послугою IaaS у публічній хмарі E-Cloud, виконайте відповідні налаштування рішення **Edge Gateway** (розділ NAT) в [інтерфейсі vCloud Director](#):

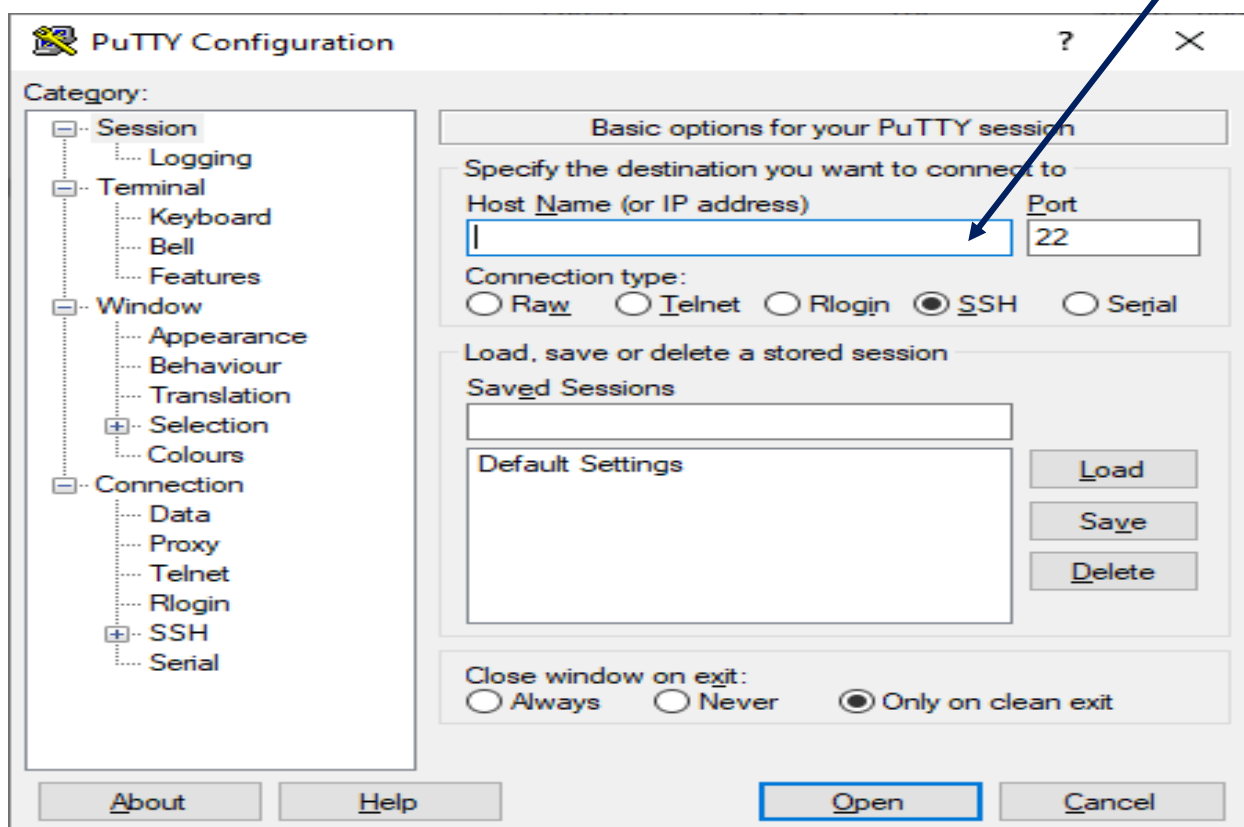
The screenshot shows the vCloud Director interface for an Edge Gateway. The NAT44 Rules table is visible, with a blue arrow pointing to the rule with port 22.

ID	Type	Action	Applied on	Original IP Address	Port	Translated IP Address	Port	Protocol	Enabled	Logging	Description
196609	User-defined	SNAT	External_demo_320	192.168.0.0/24	Any	94.131.243.122	Any	Any	✓	✗	
196610	User-defined	DNAT	External_demo_320	94.131.243.122	22022	192.168.0.3	22	tcp	✓	✗	Ubuntu19
196611	User-defined	DNAT	External_demo_320	94.131.243.122	5555	192.168.0.2	3389	tcp	✓	✗	

No NAT64 rules defined.

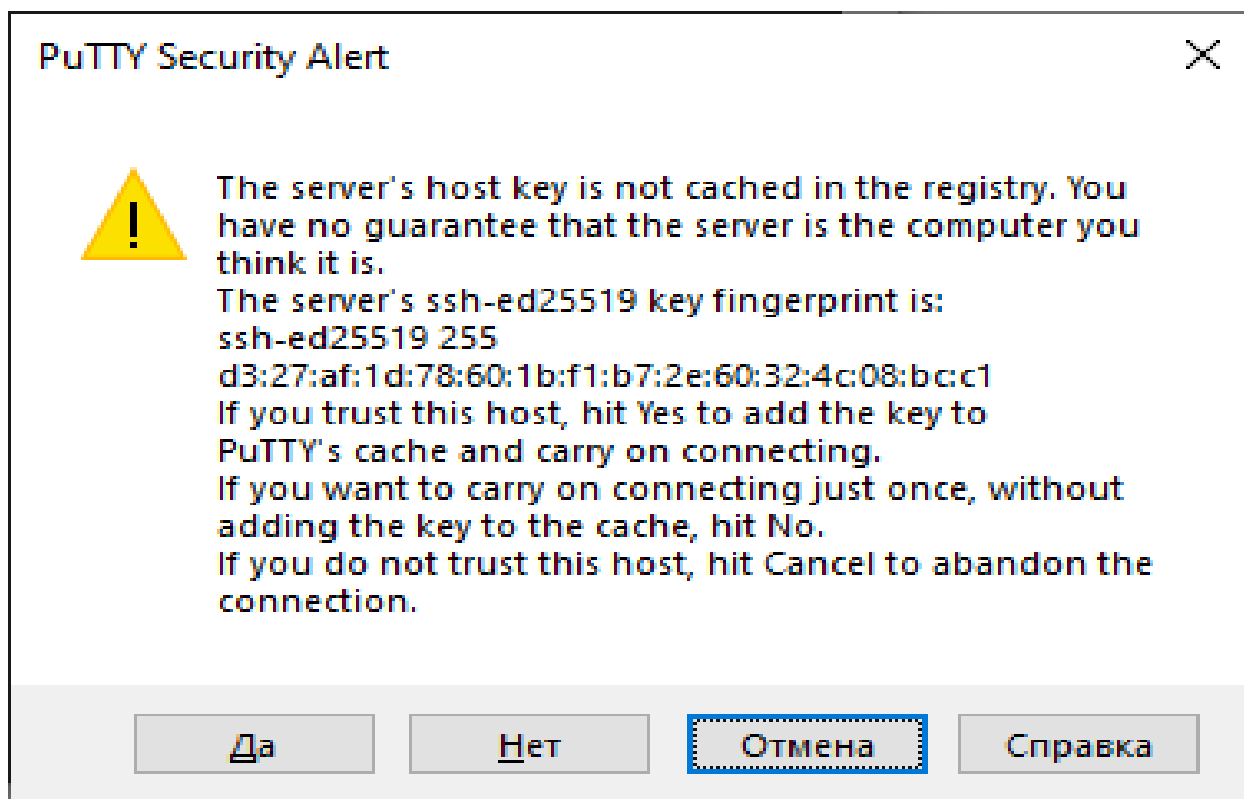
На клієнтському комп'ютері, з якого виконується доступ, потрібна відповідна програмна утіліта для з'єднання з сервером по SSH. Клієнтська частина **ssh** одразу міститься в ОС Linux, а для ОС Windows необхідно буде встановити програму **PuTTY**.

Після першого запуску **PuTTY** у полі «**Host Name**» введіть IP-адресу вашого серверу:

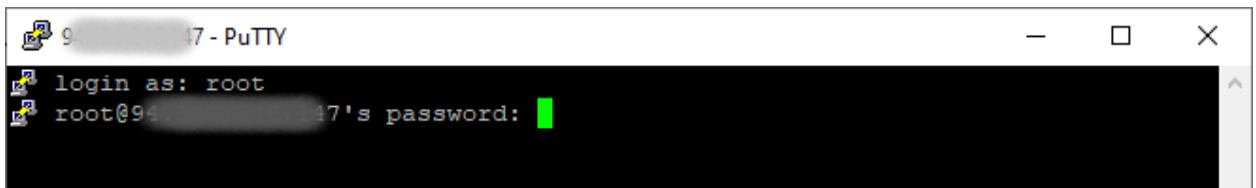


Натисніть екранну кнопку «**Open**».

Під час першого підключення до сервера, необхідно підтвердити використання ключа:



Після встановлення з'єднання з сервером, введіть логін (**root** для Linux або **Administrator** для Windows):

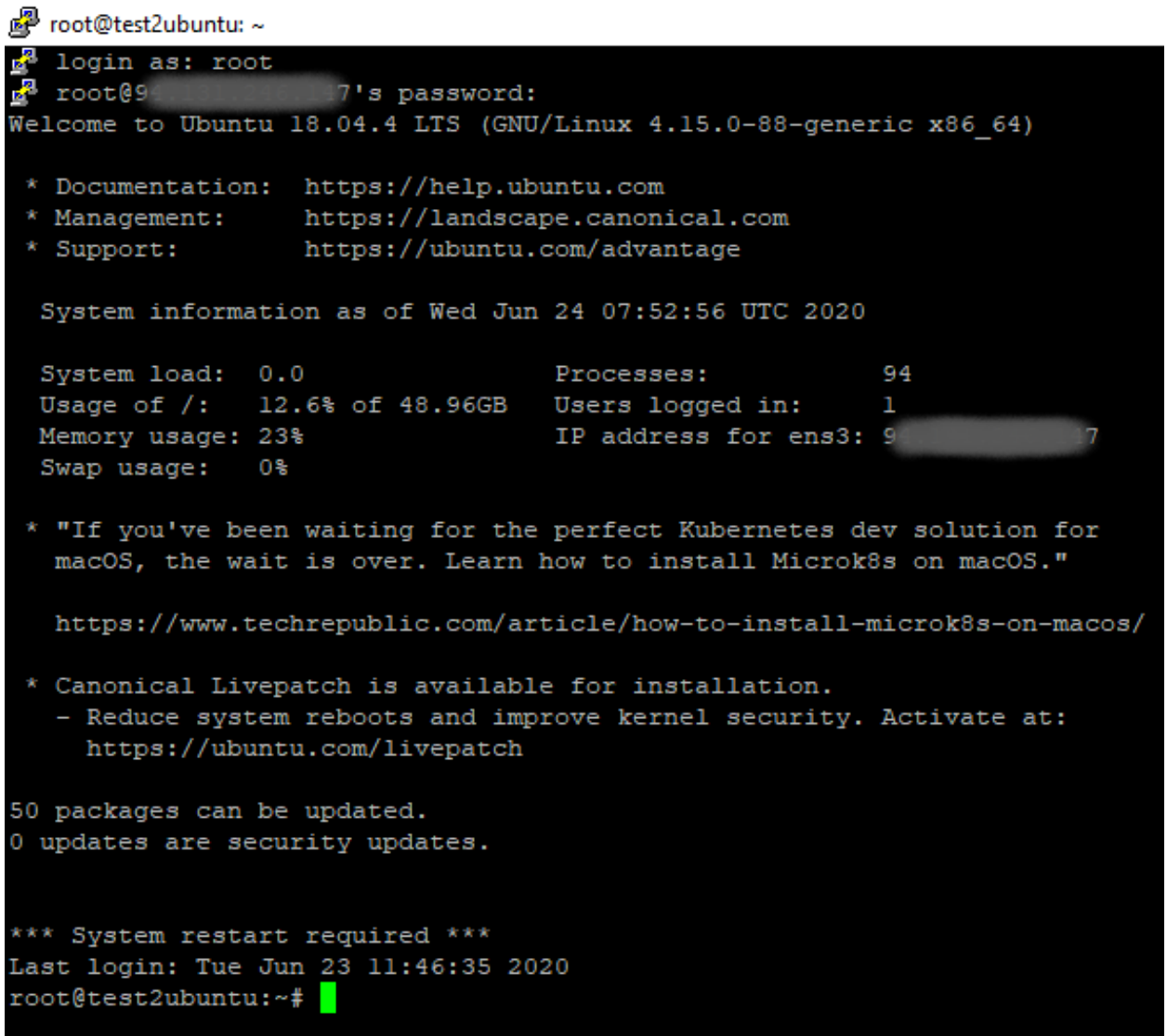


```
9[redacted]17 - PuTTY
login as: root
root@9[redacted]17's password: █
```

Введіть отриманий вами пароль для адміністративного доступу до віртуального сервера.



Увага! Під час введення пароль на екрані не відображається.



```
root@test2ubuntu: ~
login as: root
root@9[redacted]17's password: █
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-88-generic x86_64)

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

System information as of Wed Jun 24 07:52:56 UTC 2020

System load:  0.0          Processes:           94
Usage of /:   12.6% of 48.96GB  Users logged in:   1
Memory usage: 23%          IP address for ens3: 9[redacted]17
Swap usage:   0%

* "If you've been waiting for the perfect Kubernetes dev solution for
  macOS, the wait is over. Learn how to install Microk8s on macOS."

  https://www.techrepublic.com/article/how-to-install-microk8s-on-macos/

* Canonical Livepatch is available for installation.
  - Reduce system reboots and improve kernel security. Activate at:
    https://ubuntu.com/livepatch

50 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Tue Jun 23 11:46:35 2020
root@test2ubuntu:~# █
```