Biznet GIO Cloud
Menghubungkan VM via SSH

Pendahuluan

Menghubungkan Virtual Machine (VM) yang baru Anda buat melalui client SSH dapat dengan mudah tetapi Anda perlu untuk membuat beberapa perubahan konfigurasi di Portal pertama. Dokumen ini akan memandu Anda melalui proses yang diperlukan untuk mengkonfigurasi VM.

Setelah Anda membuat VM tidak akan dapat diakses melalui klien SSH. Hal ini karena Biznet Gio Cloud menyebarkan firewall antara VM dan Internet dengan menolak aturan sebagai default.

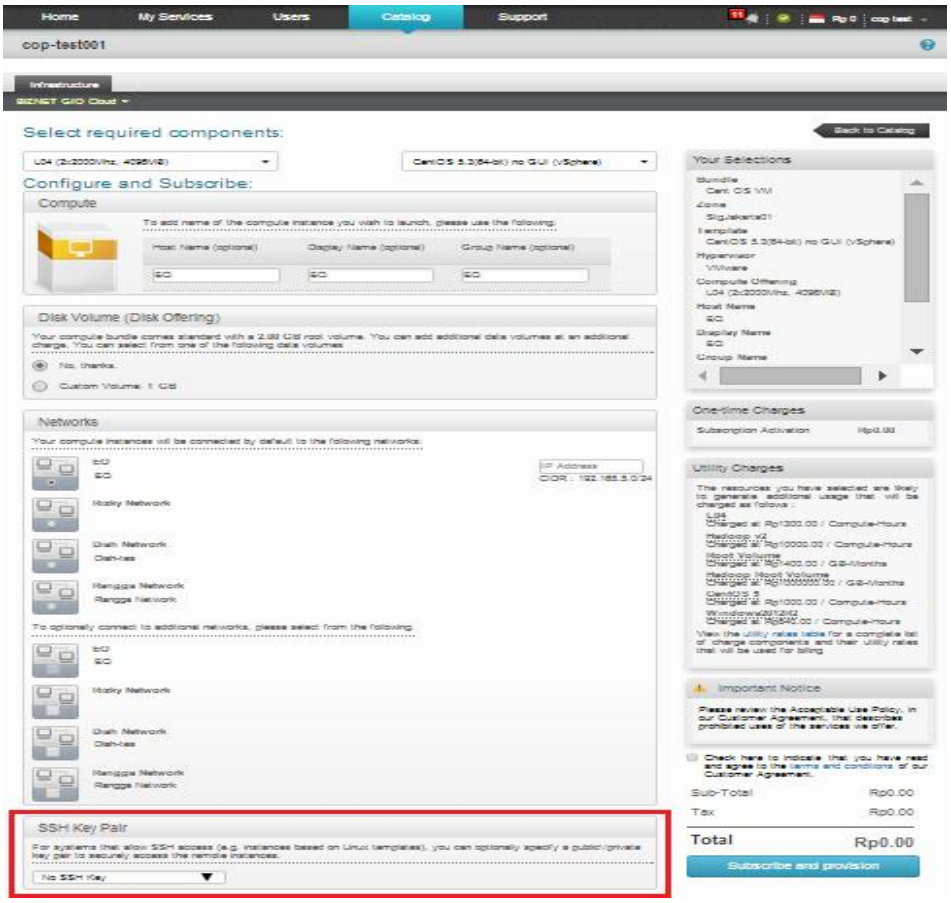
Prasyarat :

- VM Anda telah ditempatkan pada jaringan yang "terisolasi" (ini adalah jaringan standar yang ditetapkan secara auto).
- Jaringan Anda yang terisolasi memiliki IP Address eksternal (IP Address ini secara otomatis ditetapkan secara default di jaringan yang terisolasi). Setiap jaringan tambahan yang terisolasi tidak akan memiliki IP Address dan salah satu dapat diperoleh secara terpisah.
- VM anda yang sedang berjalan menggunakan system operasi Linux
- Anda menggunakan klien SSH yang sesuai seperti Putty. Untuk tujuan panduan ini kita akan menampilkan Putty tapi klien lain yang tersedia.

Menyiapkan SSH Key

Untuk mengakses Linux VM Anda menggunakan SSH Anda harus terlebih dahulu memilih / membuat atau menambah kunci SSH ke VM. Hal ini dicapai ketika Anda membuat VM Anda.

Setelah Anda memilih sistem ukuran VM, operasi dll Anda akan diminta untuk mengkonfigurasi dan berlangganan.



Pada "Configuration and Subsscribe" pada layar, di pojok kiri bawah Anda akan melihat bagian yang disebut "SSH Key Pair".

Dalam "SSH Key Pairs" ada sejumlah pilihan yang tersedia. Oleh karena itu Anda harus membuat pilihan sebelum Anda menyelesaikan pembuatan VM.

Pilihan yang berbeda dijelaskan pada halaman berikutnya dokumen ini.

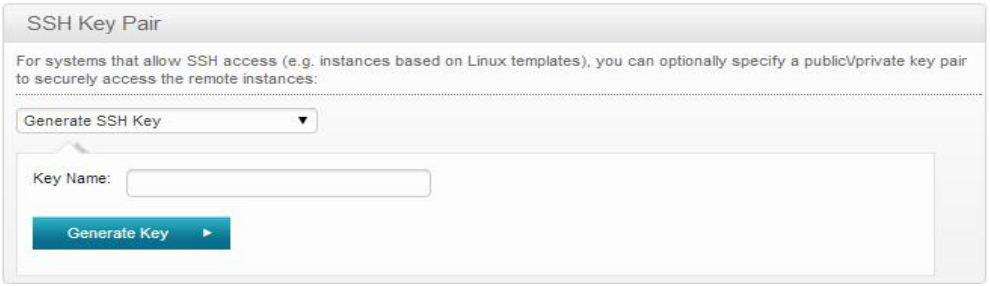
Ada dua pilihan untuk menghubungkan melalui SSH, menggunakan nama pengguna dan kombinasi password atau menggunakan kunci SSH.

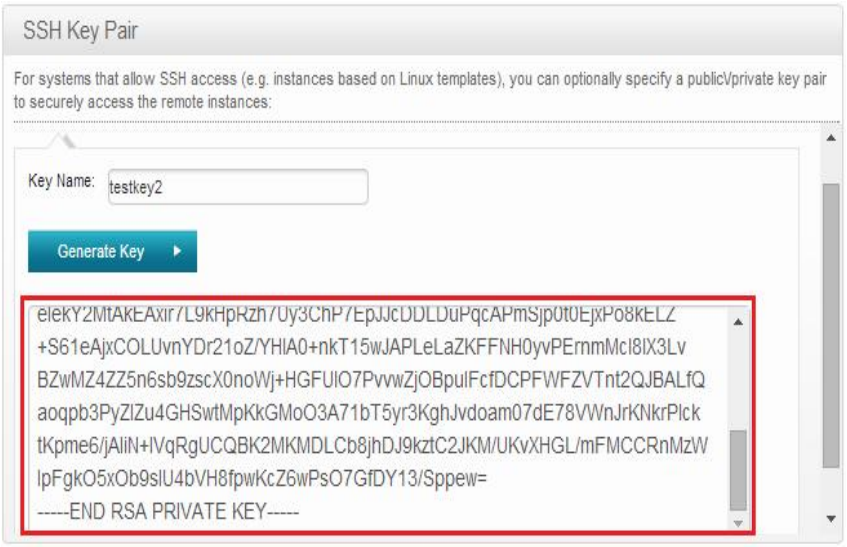
Jika Anda berniat untuk menggunakan kombinasi nama pengguna dan password pilih [No SSH Key]. Maka Anda dapat memilih [Subscribe and Provision] untuk membuat VM Anda.

Untuk menggunakan kunci SSH Anda dapat memiliki 2 cara yaitu dengan cara berikut : Generate a new SSH key, Upload a SSH key, setelah melakukan salah 1 cara tersebut anda dapat memilih Select SSH Key dari hasil Generate SSH key atau Upload SSH Key.

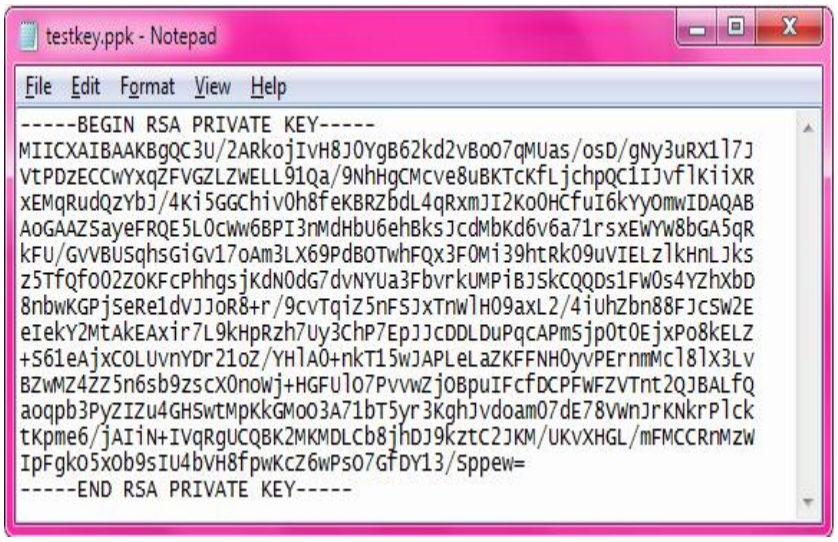
Generate SSH Key

Pilih [Generate SSH Key] akan menghasilkan kunci RSA. Teks kunci harus disalin ke notepad dan disimpan ke file lokal - ini akan digunakan kemudian untuk set-up klien SSH.

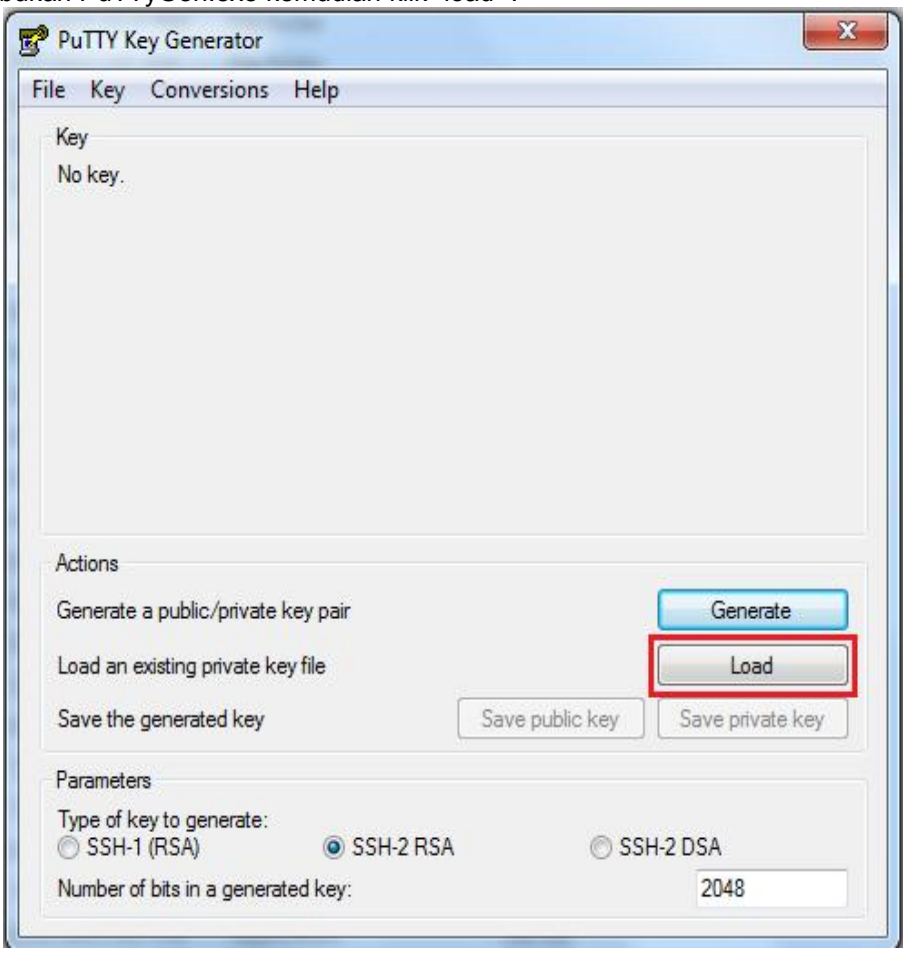




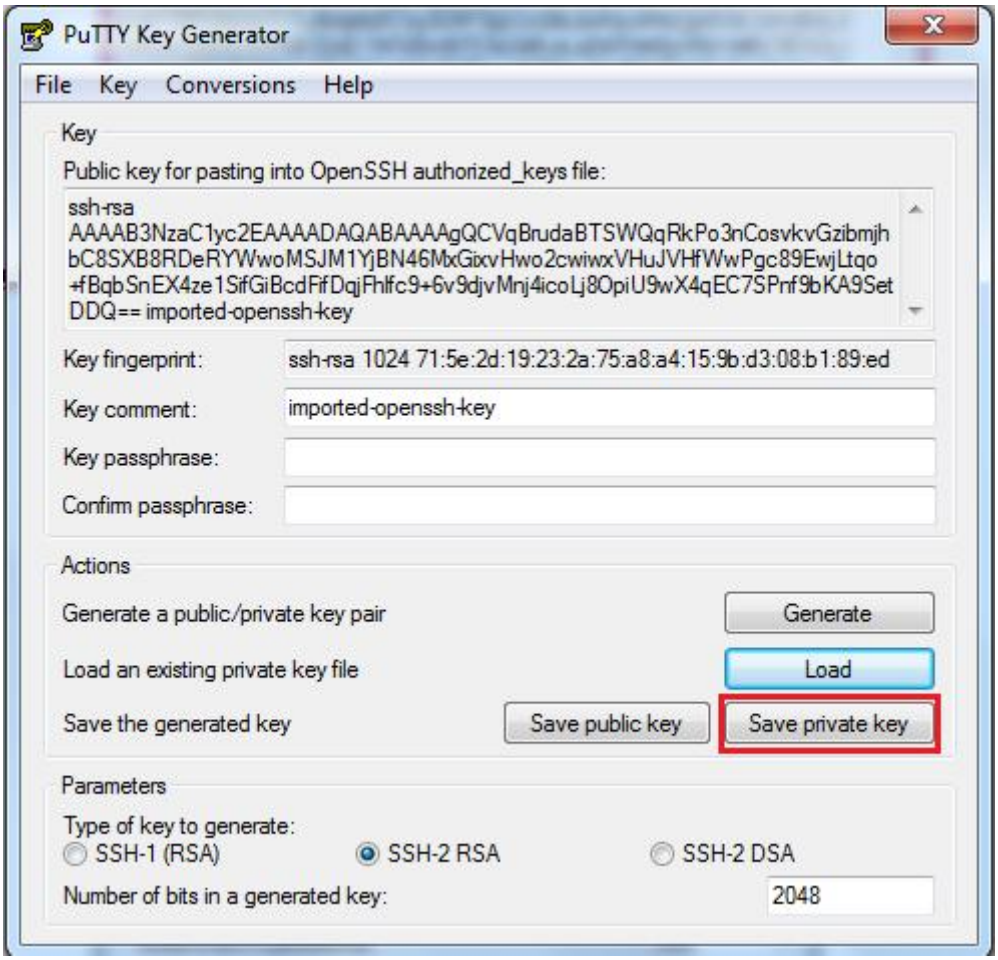
Program perangkat lunak lain dapat digunakan untuk menyimpan kunci. Dalam contoh ini kita telah menggunakan Microsoft Notepad



Setelah itu bukan PuTTyGen.exe kemudian klik “load” :



Kemudian pilih testkey.ppk / .txt yang sudah disimpan , kemudian save private key seperti berikut :



Setelah selesai harap simpan dengan baik privatekey tersebut, kemudian ikuti petunjuk penggunaannya di puttygen.exe pada panduan dibawah *Memilih SSH Key.*

Anda dapat mendownload pada link berikut *:*
http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe

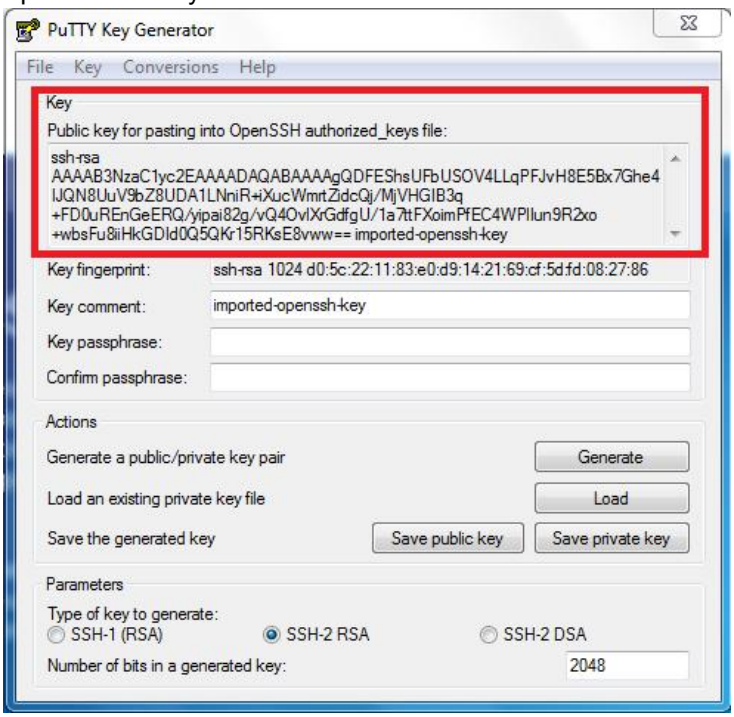
Upload Key

Tombol Upload memungkinkan Anda untuk meng-upload kunci yang sebelumnya telah dibuat di luar dari layanan Cloud Compute.
Untuk tujuan dokumen kita telah menggunakan Putty Key Generator.

NB Setiap kunci yang dihasilkan harus sesuai dengan data yang ada pada putty key generator.

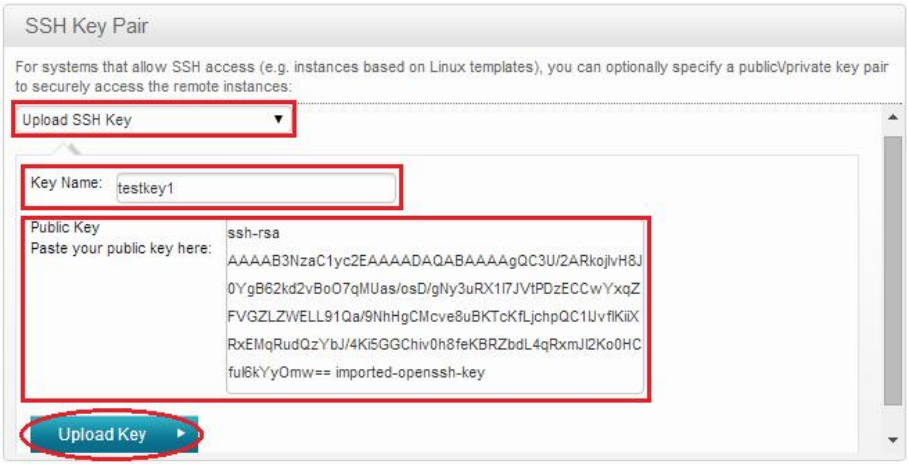
Anda dapat mendownload pada link berikut *:*
http://the.earth.li/~sgtatham/putty/latest/x86/puttygen.exe

Salin kunci publik dari key generator yang nantinya dapat dipaste ke portal public key Biznet Gio Portal pada menu Upload SSH Key.

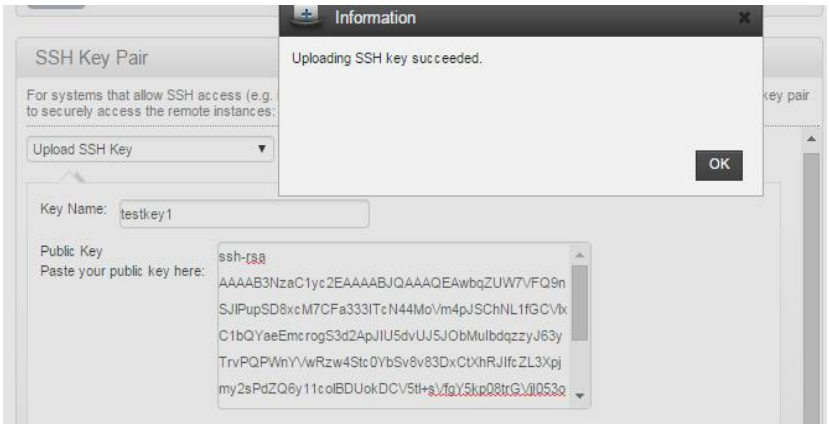


Di Biznet GIO Portal pilih [Upload SSH Key]. Lengkapi kunci Anda dengan nama kemudian paste kunci publik ke dalam kotak yang disediakan.

Lalu pilih [Upload Key].

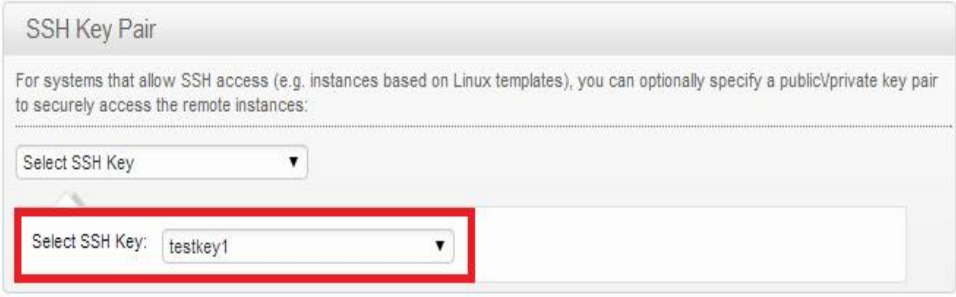


Anda kemudian akan melihat konfirmasi bahwa kunci telah dimuat.

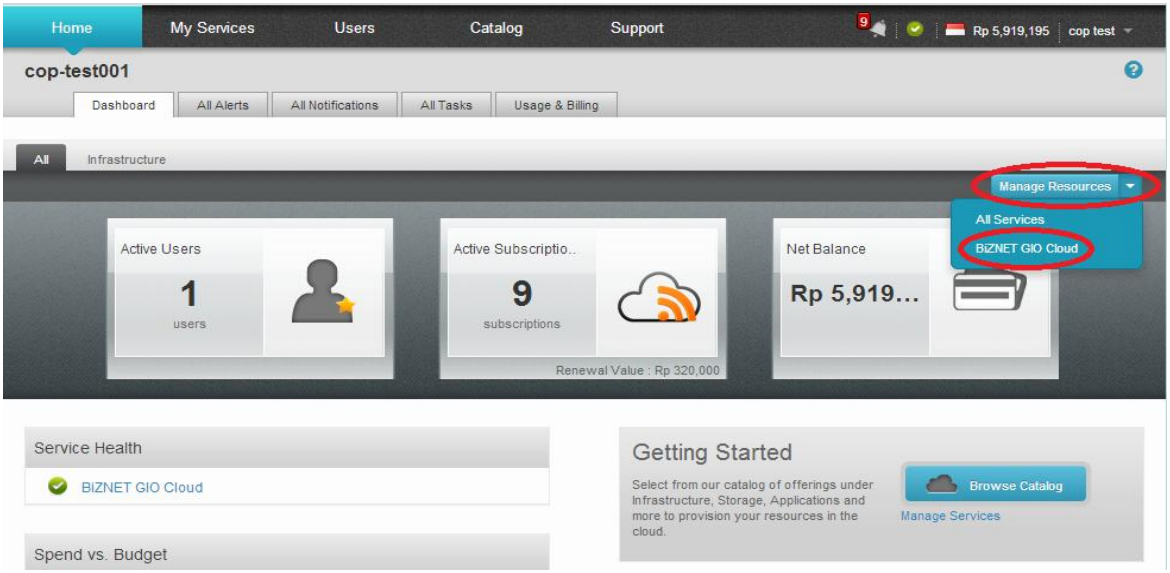


Memilih SSH Key

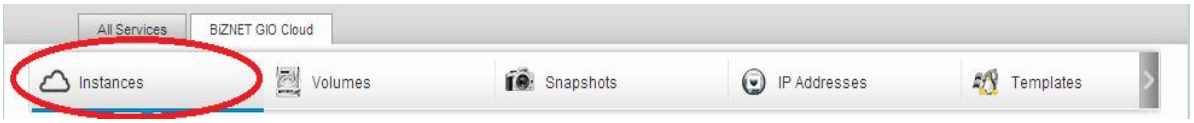
Jika langkah generated sebelumnya telah berhasil atau Anda telah menyimpah kunci ssh Anda dapat memilih kunci ini untuk digunakan pada VM baru.



Untuk mengakses VM yang telah dibuat menggunakan SSH silakan ikuti petunjuk di bawah ini. Dari layar Awal pilih [Manage Resources] diikuti oleh [Biznet GIO Cloud].



Dari jendela Biznet GIO Cloud pilih menu [Instances]



Dari menu sebelah kiri pilih VM yang ingin Anda terapkan aturan firewall. Dalam contoh ini kita telah memilih mesin kami sebelumnya yang disebut "BiznetGioCloud"

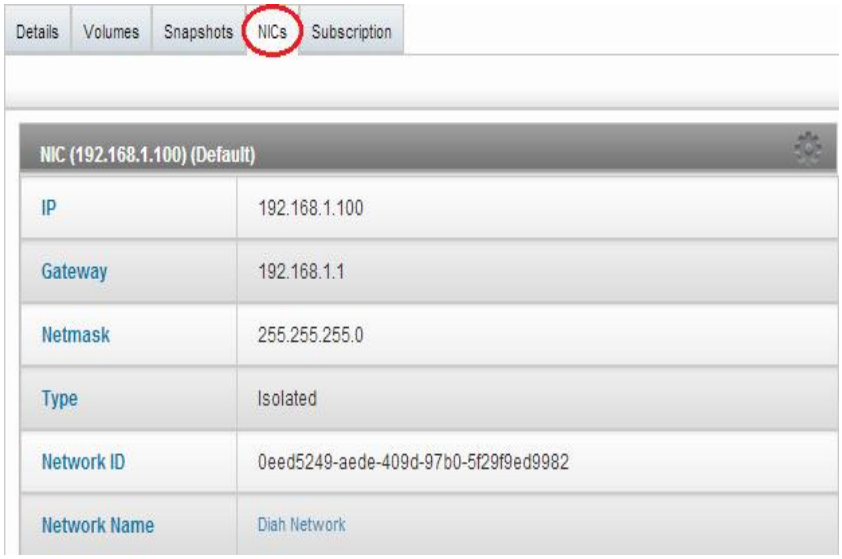
.

Untuk VM yang Anda pilih, pilih [NIC] tab.

Ini akan menunjukkan atribut jaringan VM Anda.

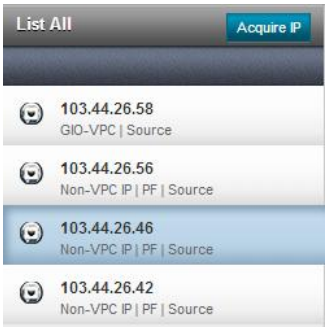
Dalam contoh ini kita bisa melihat VM terhubung ke jaringan terisolasi (dan karena itu bisa terhubung ke internet). Oleh karena itu kita perlu membuat catatan dari ID jaringan seperti yang kita akan memerlukan informasi ini dalam satu menit.

Ini adalah internal ID jaringan yang digunakan oleh VM Anda. Hal ini unik untuk setiap jaringan dan karena itu akan membantu kami mengidentifikasi jaringan yang kita perlu menerapkan aturan firewall

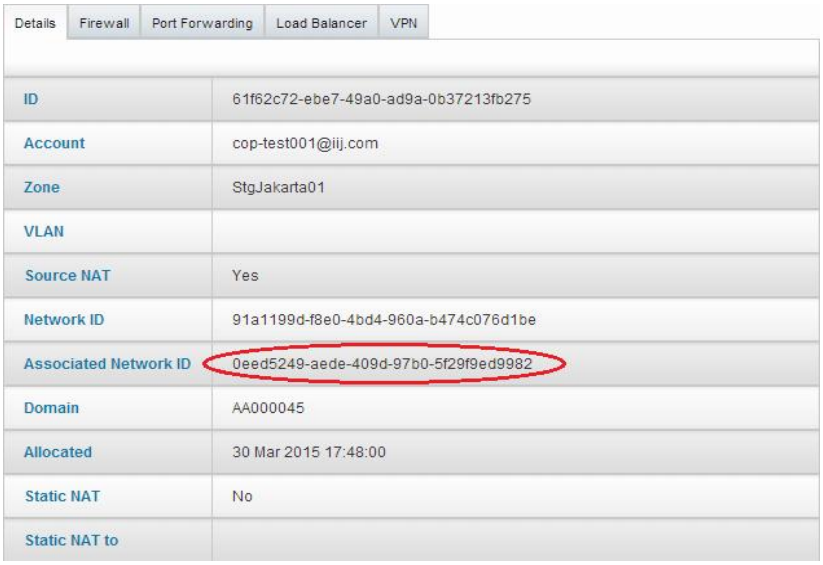


Kemudian pilih [IP Address] tab.

Ditampilkan pada navigasi sebelah kiri akan semua Alamat IP yang terkait dengan Akun Anda (Master User dan Power untuk semua pengguna terlihat). Ingat setiap Pengguna akan memiliki alamat IP dan setiap lokasi yang Anda telah dikerahkan VM juga akan memiliki alamat IP sehingga mungkin ada banyak yang ditampilkan.



Pilih melalui daftar Alamat IP sampai Anda menemukan satu dengan [Associated Network ID] yang cocok dengan [Network ID] yang sebelumnya Anda catat.



Sekarang bahwa Anda telah mengidentifikasi alamat IP yang terkait dengan jaringan VM Anda berada pada pilih [Firewall] tab.

Tab ini memungkinkan Anda untuk membuat aturan firewall yang terkait dengan jaringan Anda.

> Ini adalah aturan Ingress untuk jaringan Anda. Aturan jalan keluar dapat ditemukan pada bagian Network (bukan alamat IP tab) tetapi tidak diperlukan untuk mendirikan sebuah sesi SSH.

Untuk tujuan panduan ini kita akan menunjukkan cara membuat aturan standar untuk lalu lintas TCP / IP menggunakan port 22 (port default yang digunakan oleh SSH) - ini akan memungkinkan lalu lintas melalui remote desktop pada mesin virtual kami.

[Source CIDR]	Masukkan jaringan sumber perangkat Anda ingin memiliki akses ke mesin virtual Anda. Dalam contoh ini kita ingin tersedia untuk semua orang di Internet sehingga kita memasuki 124.195.113.0/24 untuk meningkatkan keamanan Anda dapat lebih spesifik dan menguncinya ke kantor jaringan Anda sendiri / home
[Protocol]	Menggunakan kotak dropdown pilih protokol yang diperlukan. Dalam hal ini kita ingin TCP standar
[Start Port]	Masukkan "22". Ini adalah port pertama dalam kisaran Anda ingin firewall untuk mengizinkan
[End Port]	Masukkan "22". Ini adalah port terakhir dalam kisaran Anda ingin firewall untuk mengizinkan

Jika ICMP dipilih sebagai Protokol masukkan "-1" di kedua [Type] dan [Code] kotak yang akan muncul. Hal ini akan memungkinkan Keamanan & Network Appliance untuk menanggapi permintaan ICMP.

Setelah aturan set firewall telah dimasukkan, klik pada "+" tombol untuk menambahkan aturan, setelah aturan telah ditambahkan, Anda melihatnya ditampilkan sebagai berikut:

Untuk menghapus aturan cukup pilih tombol terhadap aturan yang sesuai.

Pilih [Port Forwarding] tab. Ini akan memungkinkan anda untuk menentukan port mana pada VM yang ingin Anda gunakan.

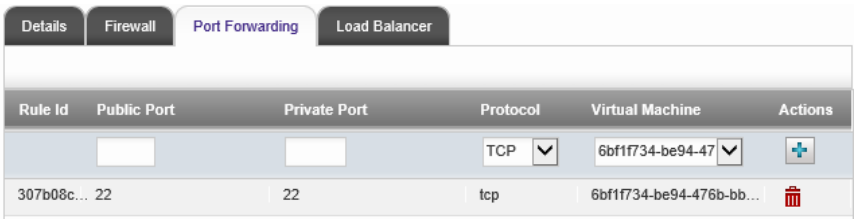
[Public Port] Masukkan port IP incoming traffic yang akan tiba. Ini harus berada dalam kisaran yang ditentukan dalam sebelumnya

[Private Port] Masukkan port IP yang akan digunakan oleh mesin virtual untuk lalu lintas ini. Ini bisa menjadi port yang berbeda dari yang ditentukan dalam kotak [Public Port], jika demikian port akan singkron

[Protocol] Tentukan protokol mana yang akan digunakan oleh target server untuk jenis trafik ini. Ini harus sesuai dengan pengaturan yang ditetapkan sebelumnya.

[Virtual Machine] Pilih target VM dari daftar yang ada

Setelah pengaturan pada port fowarding telah dimasukkan klik pada tombol “+” untuk menambahkan aturan, setelah aturan telah ditambahkan akan terlihat seperti dibawah ini.



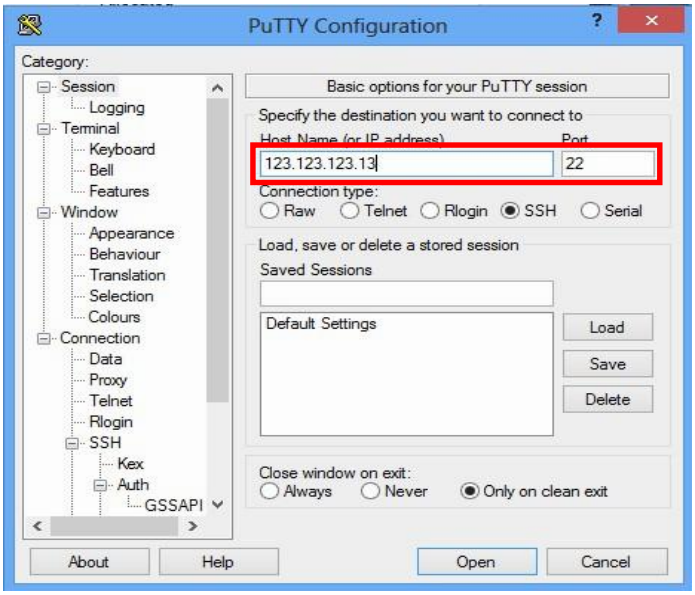
Untuk menghapus aturan cukup pilih tombol berikut

SSH (menggunakan PuTTY) ke VM Anda

Tetapkan alamat IP Address dari VM anda. Untuk tujuan panduan ini kita akan mengasumsikan IP Address adalah 123.123.123.13 .

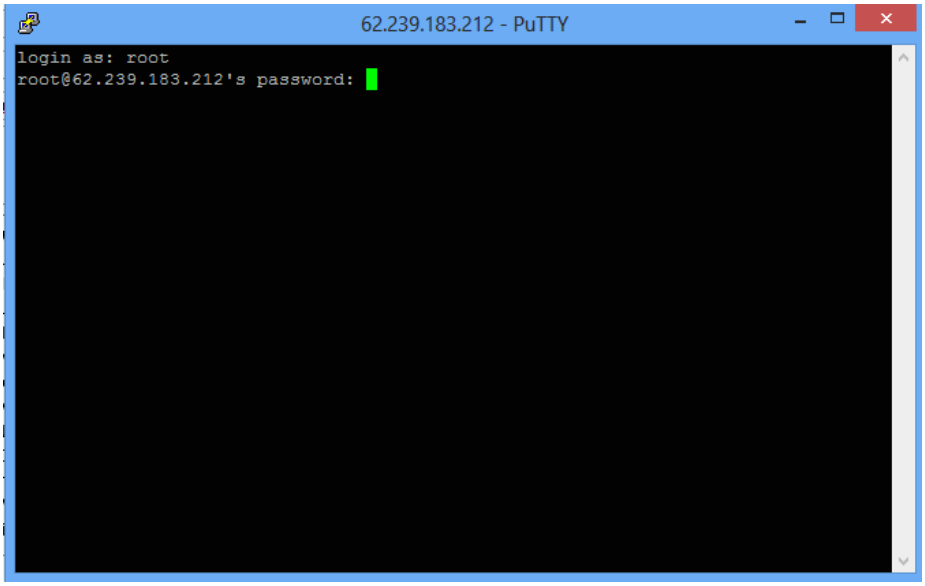
Buka aplikasi PuTTY.

Masukan alamat IP Address dan port ke dalam aplikasi putty.



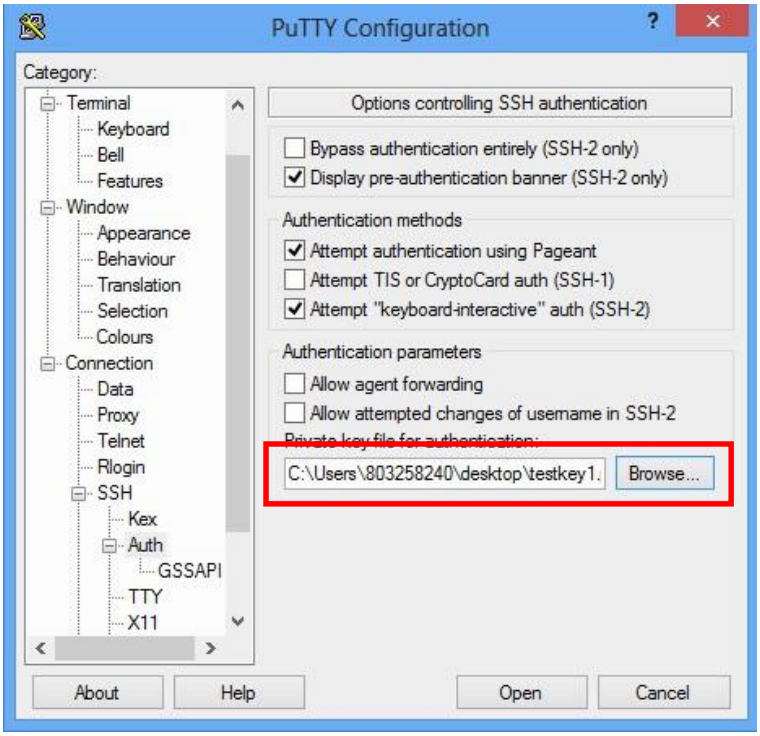
Masukan username dan passwordnya.

“Root” adalah default user administrator

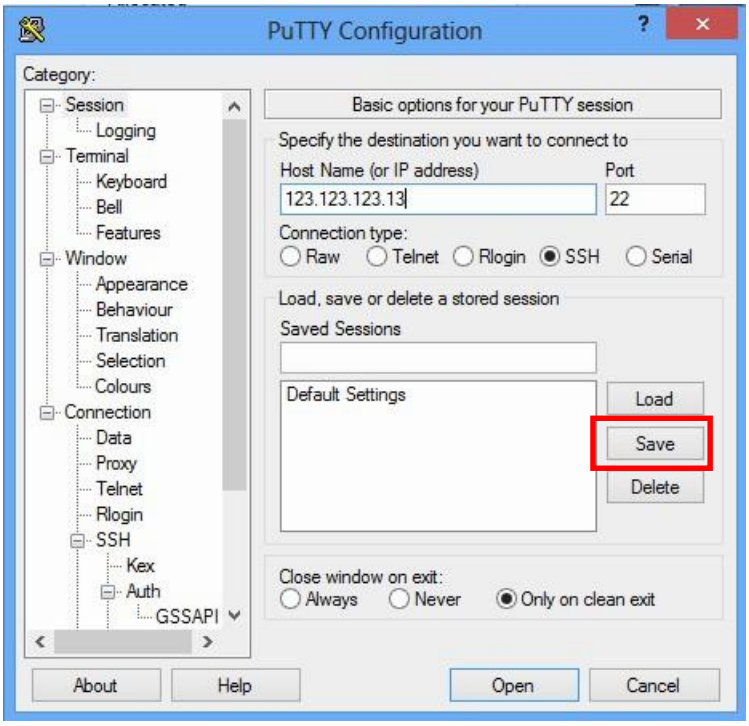


Menggunakan SSH Key

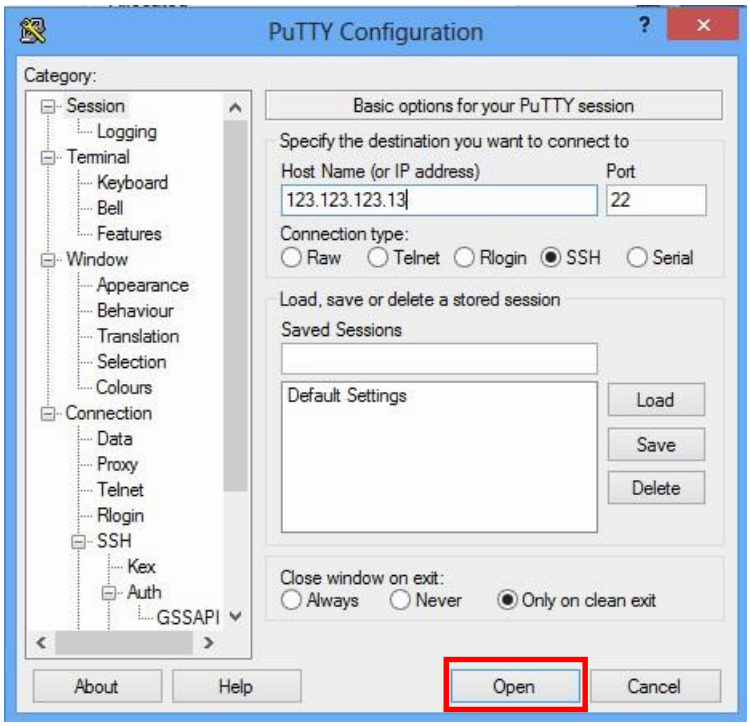
Pilih file dimana anda menyimpan SSH Key Private sebelumnya di menu [Auth].



Kemudian simpan profile.



Kemudian klik tombol Open di putty



Kemudian masukan username. “Root” adalah default user administrator.

Setelah memasukan username “Root” maka sesi ini akan dikonfirmasi dengan SSH Key di aplikasi PuTTY client dan anda sudah masuk ke user “Root” tanpa memasukan password.