

## How to run VM in MetaCentrum cloud and set access from Windows using Putty

[https://wiki.metacentrum.cz/wiki/MetaCloud\\_testbed\\_registration](https://wiki.metacentrum.cz/wiki/MetaCloud_testbed_registration)

[https://wiki.metacentrum.cz/wiki/MetaCloud\\_testbed\\_%E2%80%93\\_quick\\_guide](https://wiki.metacentrum.cz/wiki/MetaCloud_testbed_%E2%80%93_quick_guide)

1. registration to MetaCentrum cloud
  - generate private SSH key
    - login to, e.g., skirit (skirit.ics.muni.cz) using SSH
    - run command 'ssh-keygen' and enter file name for the key and set passphrase to access it – this password is optional, it is not a MetaCentrum password
    - there are two new files in the folder ~/.ssh/
    - open the file with the suffix \*.pub (public key), e.g., using 'less name.pub'
    - copy the entire content of the file to clipboard, i.e., select with a mouse and ctrl+A
  - fill the application for the metacloud group
    - <https://perun.metacentrum.cz/fed/registrar/?vo=meta&group=metacloud>
    - login with CAS password
    - paste public key from the clipboard (ctrl+V)
2. run VM in MetaCloud
  - login to <https://cloud.metacentrum.cz/> using MetaCentrum credentials
  - click on the green icon with '+'
  - select a desired image, e.g., CERIT-SC CentOS7
  - set parameters (RAM, CPU, VCPU, disk, network)
  - click on *Create*
  - VM is starting and information about IP address are shown, copy public IP (starts with 147) to the clipboard
3. conversion of the private key (for using with Putty)
  - copy private key from MetaCentrum to the local computer (i.e., the file without \*.pub suffix)
  - open puttygen.exe (downloaded from <http://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>)
  - *Conversions* -> *Import key* (select file with the private key)
  - click on *Save private key* and save the key in Putty format with the suffix \*.ppk
4. set access with Putty
  - open Putty
  - under Category 'Session' paste IP address of VM to *Host Name IP* (from clipboard)
  - under Category 'Connection – SSH – Auth' select *Private key* generated in the step 3
  - under Category 'Connection – SSH – Auth – GSSAPI' deselect 'Attempt GSSAPI authentication'
  - under Category 'Session' name this connection in 'Saved Sessions' and click on Save
  - connect by clicking on Open
  - for next time login just click on the name of the connection, Load and Open
  - login as: root
  - passphrase for key: *passphrase from the step 1*