Enable access to a remote host

In most cases you will not need to add your own SSH public key to other CNCA remote hosts as there are other processes to do so, namelly:

- To get access to the CNCA login hosts you will be required to send your SSH public key to the CNCA administrators that will install it where needed and will report back to you.
- When using the CNCA cloud services you may need to add your SSH key to a VM managed by yourself. Usually this is done through the Openstack command line interface or through the Openstack Horizon dashboard when the machine is first created and does not require other manual intervention. See the CNCA cloud documentation **here**.

- However if you need to add a key manually to a remote host account the required steps are:
  1. login into the remote host account or access its home directory through the root account
  2. check if the account directory `~user/.ssh` exists in the home directory of the remote user, if not create it with `mkdir ~user/.ssh; chmod u=rwx ~user/.ssh`
  3. check if the file `~user/.ssh/authorized_keys` exists under `~user/.ssh`, if not create the file with `touch ~user/.ssh/authorized_keys; chmod u=rw ~user/.ssh/authorized_keys`
  4. copy the public key to the remote host and append it to the file `~user/.ssh/authorized_keys` make sure not to overwrite other keys that may already exist.
  5. If you did the above steps from the root account make sure the files ownership are correct and if not change them to the correct uid and gid with `chown -R user.group ~user/.ssh`

Revision #5
Created 2021-01-11 20:37:10 UTC by Jorge Gomes
Updated 2026-07-10 14:56:25 UTC by Jorge Gomes