

13: SSH - Tips and tricks

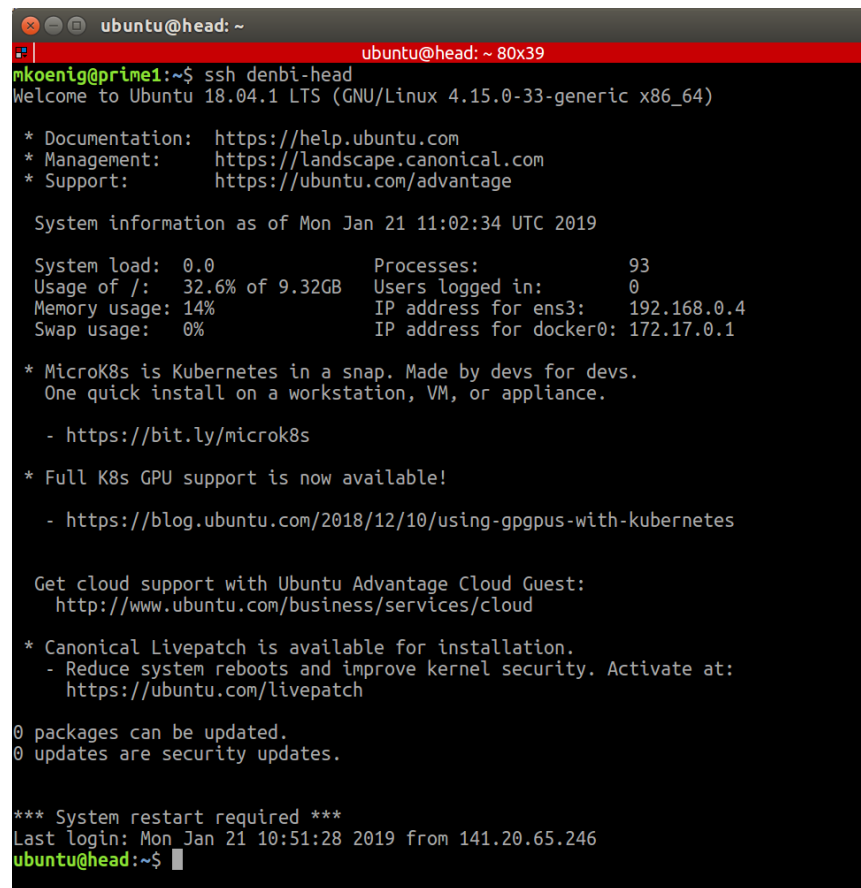
<https://github.com/matthiaskoenig/itbtechtalks>

Dr Matthias König
Humboldt University Berlin,
Institute for Theoretical Biology



What is SSH?

- **SSH, or Secure Shell, is a remote administration protocol** that allows users to control and modify their remote servers over the Internet.
- Provides mechanism for
 - authenticating a remote user
 - transferring inputs from the client to the host
 - relaying the output back to the client.
- Created as a **secure replacement for the unencrypted Telnet** and uses cryptographic techniques to ensure that all communication to and from the remote server happens in an encrypted manner.



```
ubuntu@head: ~  
mkoenig@prime1:~$ ssh denbi-head  
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-33-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Mon Jan 21 11:02:34 UTC 2019  
  
System load:  0.0           Processes:            93  
Usage of /:   32.6% of 9.32GB Users logged in:       0  
Memory usage: 14%          IP address for ens3:  192.168.0.4  
Swap usage:   0%           IP address for docker0: 172.17.0.1  
  
* MicroK8s is Kubernetes in a snap. Made by devs for devs.  
  One quick install on a workstation, VM, or appliance.  
  - https://bit.ly/microk8s  
  
* Full K8s GPU support is now available!  
  - https://blog.ubuntu.com/2018/12/10/using-gpgpus-with-kubernetes  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
  http://www.ubuntu.com/business/services/cloud  
  
* Canonical Livepatch is available for installation.  
  - Reduce system reboots and improve kernel security. Activate at:  
    https://ubuntu.com/livepatch  
  
0 packages can be updated.  
0 updates are security updates.  
  
*** System restart required ***  
Last login: Mon Jan 21 10:51:28 2019 from 141.20.65.246  
ubuntu@head:~$
```

Why use SSH?

- The most important reason why should use **OpenSSH** tools over ftp and telnet is that **all communications and user credentials using OpenSSH are encrypted**, they are also **protected from man in the middle attacks**.
- If a third party tries to intercept your connection, OpenSSH detects it and informs you about that.
- Access to remote computers, files and resources

Features

- Secure Communication
- Strong Encryption (3DES, Blowfish, AES, Arcfour)
- X11 Forwarding (encrypt X Window System traffic)
- Port Forwarding (encrypted channels for legacy protocols)
- Strong Authentication (Public Key, One-Time Password and Kerberos Authentication)
- Agent Forwarding (Single-Sign-On)
- Interoperability (Compliance with SSH 1.3, 1.5, and 2.0 protocol Standards)
- SFTP client and server support in both SSH1 and SSH2 protocols.
- Data Compression

References

- <https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work>
- <https://www.tecmint.com/install-openssh-server-in-linux/>
-