Overview

Manual server management

➟ Hetzner cloud administration GUI

Create and publish a Hetzner account

- Sign up at https://accounts.hetzner.com/signUp.

  > **Note**
  >
  > ID card may be required, but no payment.

- **Activate 2-factor authentication!**
- Confirm your newly created account at your Moodle course.
- Upon confirmation by your lecturer a Hetzner project space e.g. »g01« corresponding to your Moodle group number should be visible after login.

Your cloud project

- After login select »cloud« at the upper right menu or go to projects.
- Select your project e.g. »g01« and click on `Security` --> `Members`

You should see yourself and your Moodle course project partner having »`Admin`« role assigned.

Server creation prerequisite: A Firewall

Creating a server requires a firewall.

- Select `Firewalls` --> `Create Firewall`.
- Adapt settings and hit »`Create Firewall`«

Inbound rules

Just leave the two inbound rules port 22 and ICMP untouched.

Name

Either accept default or set to e.g. »`basicFirewall`«

Your first server

Image:

Debian 12

Type

Shared vCpu x86 (Intel/AMD) / **CX22 or cheapest**

Name

An identifier of your choice e.g. **`myfirstserver`**.

Firewalls

Your previously created firewall.

Upon hitting »Create and buy« you'll receive an E-Mail containing your **server's IP** and **root password**. You may reset root's password in the GUI's `rescue` tab.

Server access by ssh

```
$ ssh root@95.216.187.60
The authenticity of host '95.216.187.60 (95.216.187.60)' can't be established.
ED25519 key fingerprint is SHA256:vpV7B+l9RLQ+SwTMqtkk7YbICBhyhi2OP780+WVEFMY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '95.216.187.60' (ED25519) to the list of known hosts.
root@95.216.187.60's password:
You are required to change your password immediately (administrator enforced).
   ...
The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Changing password for root.
Current password:
New password:
Retype new password:
```

Server access by web gui

- In your cloud project select your server
- Hit the **>_** symbol in the upper right left of the **actions** button.
- Login using your emailed credentials.

> ## Tip
>
> You may copy text into the console by disabling **GUI-mode** and re-enabling it subsequently.

Followup exercises

288. Server creation

289. Server re-creation

Overview

- Manual server management
  - Using ssh
    - Public / private key pair

Current server security flaws

1. Password based logins being notoriously prone to attacks.
   Solution: Use public/private key based ssh login.
2. No updates: Software state of a most likely outdated installation image.

An elliptic ssh public / private key pair

`id_ed25519`

(private key)

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDZrjJrxfC/gCHcAhu6CROIxAps/tP8hNsNgM1RgyTL0wAAAKiPQ5vcj0Ob
3AAAAAtzc2gtZWQyNTUxOQAAACDZrjJrxfC/gCHcAhu6CROIxAps/tP8hNsNgM1RgyTL0w
AAAECjW290zPFjh2srRIloZdaO49cs7hgQ7A7lmG8Z+SVDjdmuMmvF8L+AIdwCG7oJE4jE
Cmz+0/yE2w2AzVGDJMvTAAAAImdvaWtAbWFydGluLXBjLWRhY2hib2Rlbi5mcml0ei5ib3
gBAgM=
-----END OPENSSH PRIVATE KEY-----
```

`id_ed25519.pub`

(public key)

```
ssh-ed25519 AAAAC3NzaC1 ... Cmz+0/yE2w2AzVGDJMvT goik@hdm-stuttgart.de
```

Safety considerations

Private key

- Keep it private!
- Define a **good passphrase** on key pair creation.
- Cannot be derived / re-engineered from corresponding public key.

Public key

May be given to anybody.

`https://www.ssh.com/academy/ssh/passphrase`:

A **good passphrase** should have at least 15, preferably 20 characters and be difficult to guess. It should contain upper case letters, lower case letters, digits, and preferably at least one punctuation character. No part of it should be derivable from personal information about the user or his/her family.

ssh-keygen for elliptic key creation

```
$ ssh-keygen  -a 256 -t ed25519 (1) -C "$(hostname)-$(date +'%d-%m-%Y')"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/foo/.ssh/id_ed25519):
Created directory '/home/foo/.ssh'.
Enter passphrase (empty for no passphrase): (2)
Enter same passphrase again:
Your identification has been saved in /home/foo/.ssh/id_ed25519 (3)
Your public key has been saved in /home/foo/.ssh/id_ed25519.pub (4)
...
```

Result of ssh-keygen execution (client side)

```
~/.ssh$ cd ~/.ssh
/home/foo/.ssh cat id_ed25519.pub >> authorized_keys (1)
mistudent@w10m:~/.ssh$ ls -al

drwxr-xr-x  2 student mi    0 Okt 17 17:45 .
drwxr-xr-x 32 student mi    0 Okt 17 17:44 ..
-rw-r--r--  1 student mi  396 Okt 17 17:45 authorized_keys (2)
-rw-------  1 student mi 1675 Okt 17 17:38 id_ed25519 (3)
-rw-r--r--  1 student mi  396 Okt 17 17:38 id_ed25519.pub (4)
```

(1) Append public key to list of authorized keys.

---

(2) The **authorized_keys** file may contain multiple lines containing public keys having access.

---

(3) Private key.

---

(4) Corresponding public key.

Transfer public key from client to server

```
goik@martin-hdm-desktop:~$ scp .ssh/id_ed25519.pub root@37.27.32.138:/tmp (1)
root@37.27.32.138's password:
id_ed25519.pub                                100%  103     3.7KB/s   00:00
goik@martin-hdm-desktop:~$ ssh root@37.27.32.138 (2)
root@37.27.32.138's password:
      ...
root@debian-4gb-hel1-2:~# cat  /tmp/id_ed25519.pub >> ~/.ssh/authorized_keys (3)
root@debian-4gb-hel1-2:~# exit (4)
goik@martin-hdm-desktop:~$ ssh root@37.27.32.138 (5)
     ...
Last login: Tue Apr  8 13:38:42 2025 from 141.62.31.244
```

Followup exercise

290. Improve your server's security!

Cleaning up!

Caution

This is about

$$\$MONEY$$

$

- Delete your server including the IPv4 address and its volume: **All three are being billed on a per hour basis.**
- You may optionally delete your firewall.

Overview

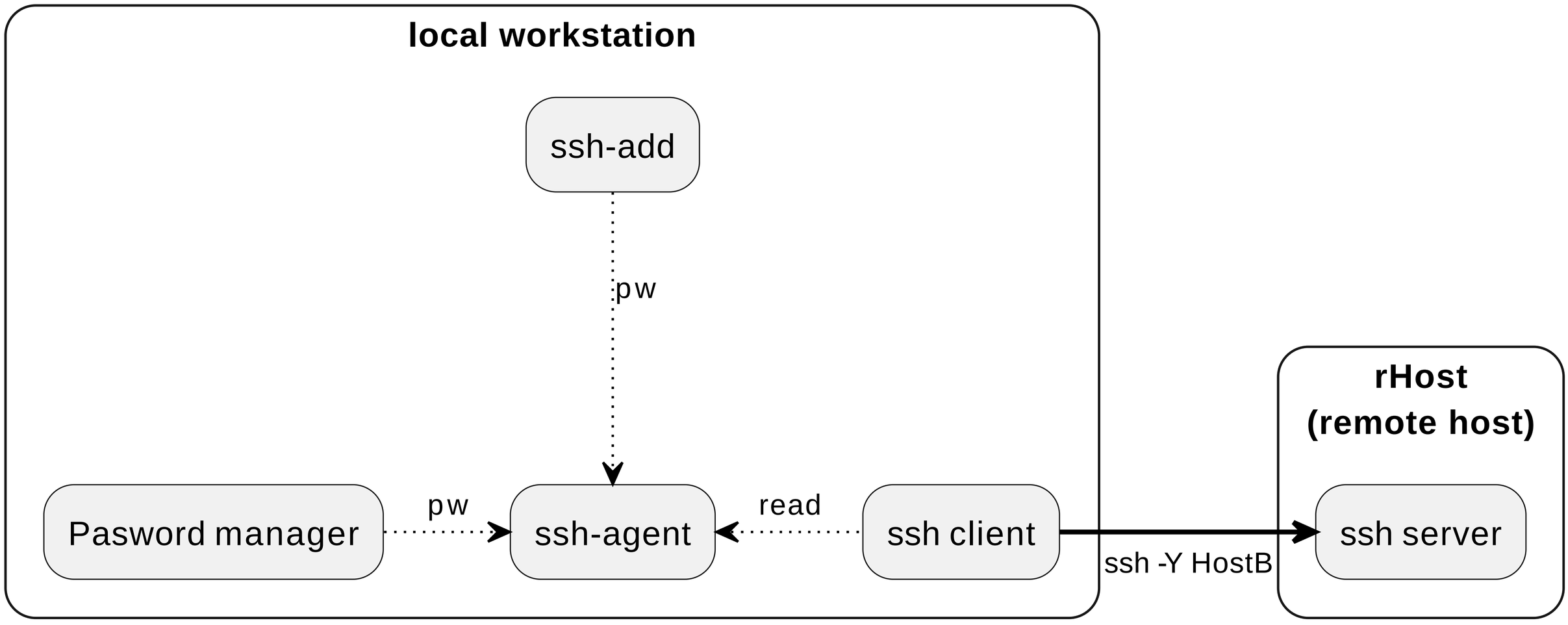
Manual server management

- Using ssh
  - Passphrases and ssh agent

Tedious: Passphrase required for each remote login

```
>ssh root@learn.mi.hdm-stuttgart.de
Enter passphrase for key '/home/goik/.ssh/id_ed25519':
root@learn:~# exit
logout
Connection to learn.mi.hdm-stuttgart.de closed.
>ssh root@klausur.mi.hdm-stuttgart.de
Enter passphrase for key '/home/goik/.ssh/id_ed25519':
root@klausur:~# exit
logout
Connection to klausur.mi.hdm-stuttgart.de closed.
```

Solving the passphrase issue



- Install **ssh-agent** or related on your system: Passphrase will be cached per session.
- Optional: Connect your password manager to the agent.

  Example: KeepassXC SSH Agent integration.

Behind the scenes: How does it work?

```
>printenv |grep SSH_AUTH_SOCK
SSH_AUTH_SOCK=/run/user/21100/keyring/ssh
>ps aux|grep ssh-agent
goik        6671  ... /usr/bin/ssh-agent -D -a /run/user/21100/keyring/.ssh
>ls -al /run/user/21100/keyring/ssh
srwxr-xr-x. 1 goik goik 0 Apr 12 09:58 /run/user/21100/keyring/ssh
```

Note: The “**s**” in **s**rwxr-xr-x indicates a domain socket.

Followup exercises

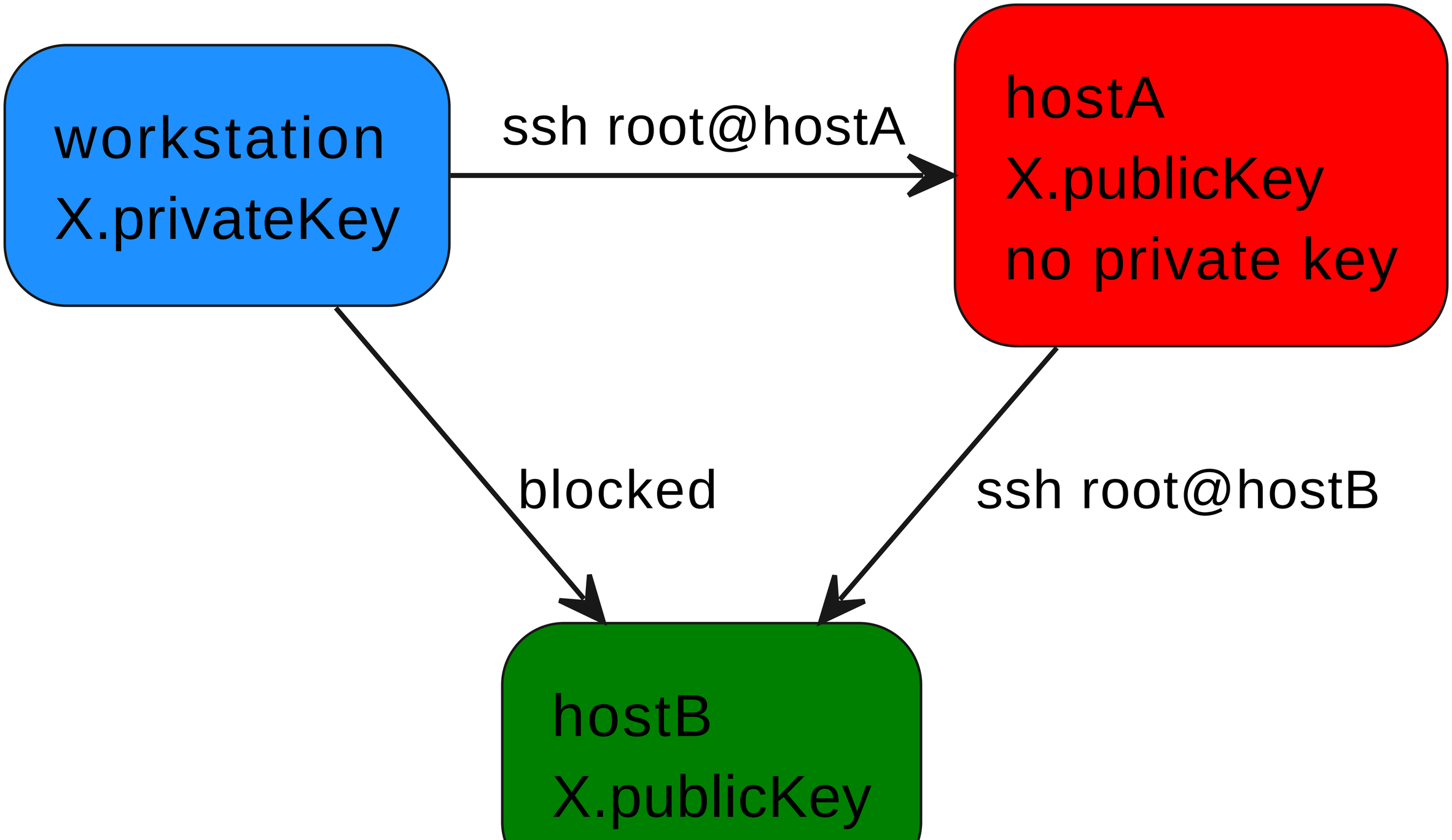
291. **ssh-agent** installation

292. MI Gitlab access by ssh

Overview

- Manual server management
  - Using ssh
    - Agent forwarding

Intermediate host hopping



Intermediate host hopping fails

```
goik@local> ssh root@learn.mi.hdm-stuttgart.de
Linux learn 6.5.13-1-pve #1 SMP PREEMPT_DYNAMIC PMX 6.5.13-1 (2024-02-05T13:50Z) x86_64
...
root@learn:~# ssh klausur.mi.hdm-stuttgart.de
root@klausur.mi.hdm-stuttgart.de: Permission denied (publickey).
```

Intermediate host hopping options

1. Copy private key `~/.ssh/id_ed25519` to intermediate host (and re-enter passphrase there).
2. Enable agent forwarding.

> **Note**
>
> Agent authentication socket on originating client host required.

Enable ssh agent forwarding

```
# File ~/.ssh/config goik@local
...
Host learn.mi.hdm-stuttgart.de
  ForwardAgent yes # Forward ssh agent
                   # to remote host.
...
```

```
goik@local> ssh root@learn.mi.hdm-stuttgart.de
Linux learn 6.5.13-1-pve #1 SMP ...
   ...
root@learn:~#
root@learn:~# ssh klausur.mi.hdm-stuttgart.de
Linux klausur 6.8.8-4-pve #1 SMP ...
   ...
root@klausur:~#
```

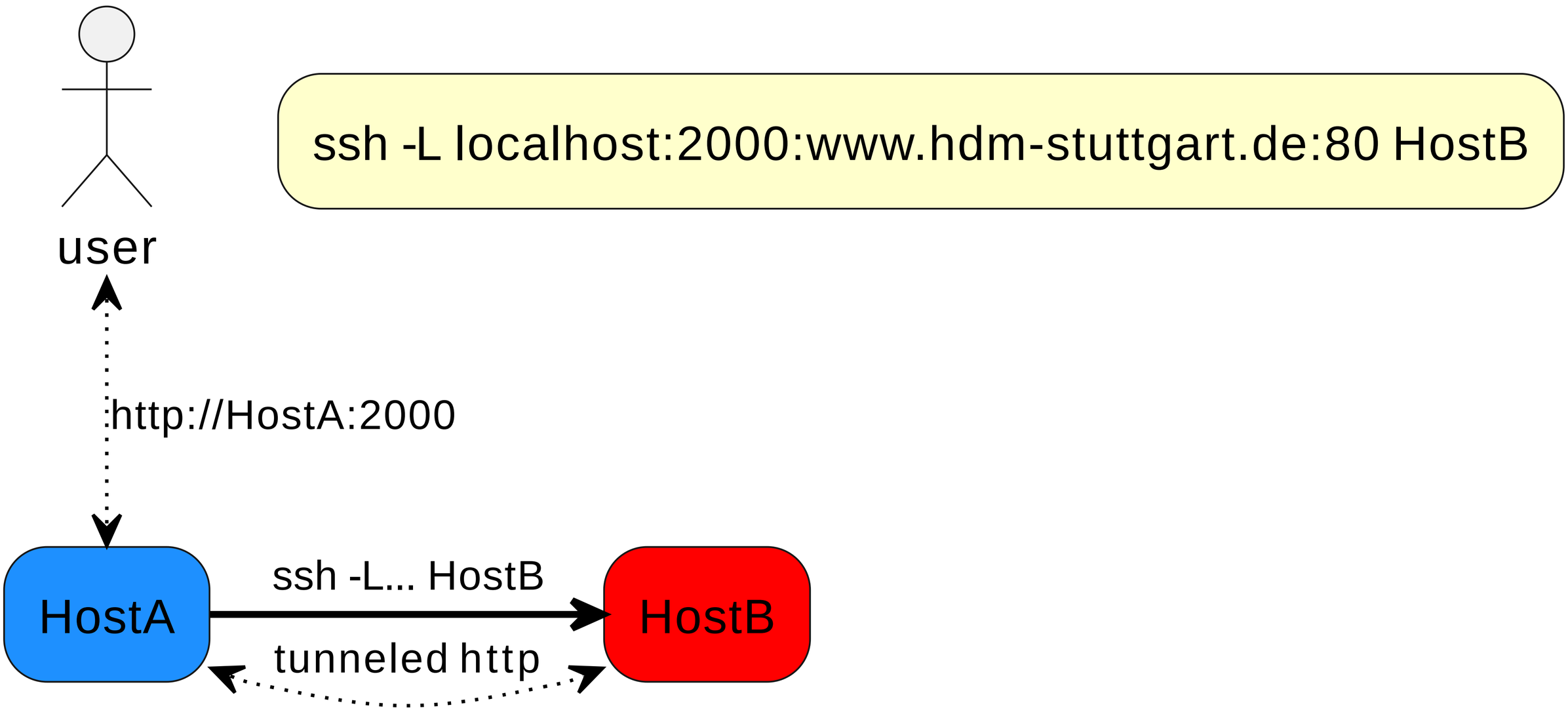
Followup exercise

293. ssh host hopping

Overview

- Manual server management
  - Using ssh
    - Port forwarding

Forwarding port 80 to 2000 at localhost



Frequent use e.g. connecting to remote database server

```
# Implicit for ssh-L localhost:2000:localhost:3306 ...
#
ssh -L 2000:localhost:3306 HostB # Mysql DB Server
```

```
# Originating host
#
$ telnet localhost:2000
Trying ::1...
Connected to localhost.
Escape character is '^]'.
DHost '127.0.0.1' is not allowed
to connect to this MariaDB server
```

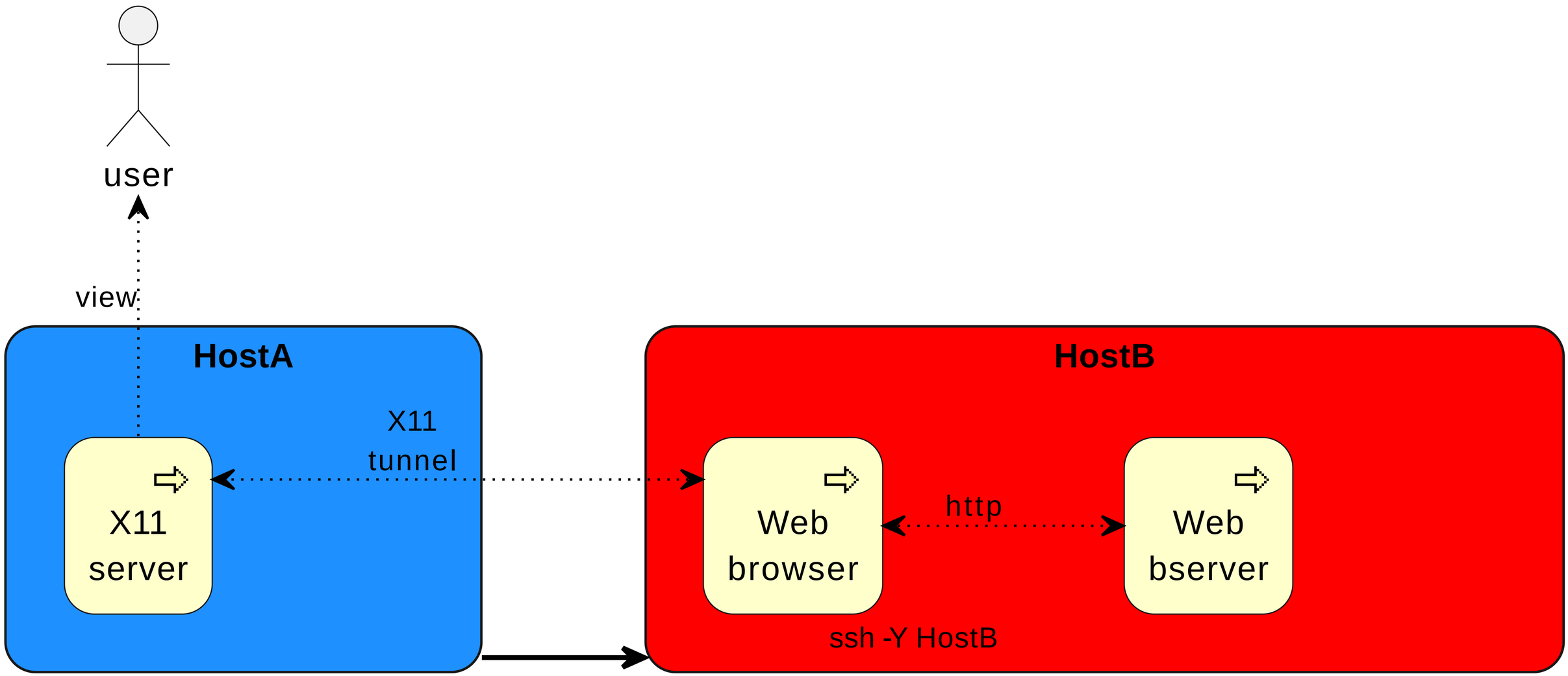
Followup exercise

294. ssh port forwarding

Overview

- Manual server management
  - Using ssh
    - X11 forwarding

X11 browser application forwarding



Followup exercise

Overview

Manual server management

➟ Prerequisites

Shell / Bash

Bash Guide for Beginners

Choosing a text editor

- Vim Introduction and Tutorial
- How to Use Nano

Secure Shell

The definitive guide, also available at SafariOnline

- Public/private keys, pass phrases
- Trusted hosts
- Port forwarding
- X11 forwarding
- **ssh** agent

Working with files

- **rm**, **rmdir**
- **ls**, **file**
- **find** / **locate**
- **touch**
- **chmod** / **chown**
- **head**, **tail**
- **grep**

Network

- **ip**
- **dig / nslookup**
- **ping**
- **route**
- **traceroute**

Processes handling

- **ps**
- **kill**
- **top** / **htop**
- **nice**

Followup exercises

296. Enabling index based file search
297. Using the **tail** -f command

Overview

Manual server management

- Ubuntu / Debian Package management
  - Prerequisites

Suggested readings:

- Debian package management introduction and reference.
- 15 Practical Examples of “dpkg commands” for Debian Based Distros
- Using PPA in Ubuntu Linux

`.deb` packages

- Sample: `firefox_75.0-2_amd64.deb`
- Archive containing:
  - Files
  - Pre- and post installation scripts
  - trigger

The dpkg command

- Query installed, install / update from file system and purge packages, i.e.:

```
> dpkg -i skypeforlinux-64.deb
```

```
> dpkg -l apt*
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Inst/Conf-files/Unpacked/halF-conf/...
+++-====================-====================...
ii  apt                  2.0.2                amd64...
ii  apt-config-icons     0.12.10-2            all
un  apt-config-icons-hidpi <none>             <none>
un  apt-doc              <none>               <none>
un  apt-listbugs         <none>               <none> ...
```

- Low level package management
- Dependency unaware

The apt command

- Network based
- Dependency aware
- Automated system updates

```
#> apt update (1)
Hit:1 http://security.debian.org buster/updates InRelease
...
4 packages can be upgraded

#> apt upgrade (2)
... The following packages will be upgraded:
  libldap-2.4-2 libldap-common libssl1.1 openssl
...
Get:1 http://security.debian.org buster/updates/main ...
Get:2 http://security.debian.org buster/updates/main ...
```

Rationale using PPA's

Problems:

- "Not available here"
- Version outdated
- Needing "bleeding edge" version