Details about Linux distribution templates in the Enterprise/Research Cloud

21.10.2025 01:15:43

FAQ-Artikel-Ausdruck

Kategorie:	Server-Dienste	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	en	**Letzte Aktualisierung:**	09:20:50 - 25.08.2025

Lösung (öffentlich)

The ZIH's Enterprise Cloud and Research Cloud services offer templates to enable faster work with a VM.
A new concept has been developed for the following distributions, which is explained in more detail in this FAQ article:

- Debian (from release 12 "Bookworm" onwards)
- Ubuntu (only as LTS version from Release 22.04 "Jammy Jellyfish" onwards)

Table of Contents

1. Access and user accounts

Each VM is provided with the user “service”. In the case of a new VM, the user's password has been generated automatically. It is strongly recommended that you reset this password. You should then remove the password from the VM overview in the SSP ([1]link to Enterprise Cloud VM overview or [2]link to Research Cloud VM overview).
The service user already has sudo rights. If desired, you can also use this to manage the root user of the VM.

A hardened configuration was installed for the SSH server on the VM:
- prohibit empty passwords
- disable compression
- prohibit HostKey-based login
- disable X11 forwarding
- disable AgentForwarding
- adjust permitted ciphers (see attached file sshd-ciphers.txt)

After logging in, the Message of the Day (hereinafter referred to as motd) appears before the first command prompt. This motd contains some important information about the new VM template concept. It can be expanded with additional files in the /etc/motd.d/ directory.

The umask 077 is used by default on the VMs, and existing files and directories in the home directory have been adjusted to this umask.
Please note that this umask does not correspond to the default for installations of currently common distributions. Umask 022 is still common there. Please note that this can lead to unexpected behavior in some situations.

The kernel command line parameter proc_hidepid=2 is set. This means that unprivileged users can only view their own processes. The proc group has been created for exceptions. Accounts belonging to this group still have the ability to retrieve information about all processes. This is intended in particular for admin or monitoring accounts.

2. Network and firewall

The VMs have a network interface with a routed IPv4 address. IPv6 routing does not take place, but IPv6 is not deactivated for compatibility reasons. The VMs therefore have at least one link-local fe80::[...] IPv6 address.

Each VM has a local firewall in the form of nftables. nftables is configured within the /etc/nftables/ directory.
In addition, nftables can be controlled using the nft command line tool.
Further information on nftables can be found here:

- [3]What is nftables? - wiki.nftables.org
- [4]Quick reference (nftables in 10 minutes) - wiki.nftables.org

It is recommended to configure nftables using the corresponding configuration files and the command line tool nft. However, if you still want to use ufw as your firewall frontend, additional configuration steps may be necessary when using nftables instead of iptables. Please also note that the iptables kernel module has been disabled. You may need to reactivate this kernel module for your firewall frontend.

Please note that there are also firewalls outside the VM. Campus-internal shares can be created or edited on the VM via the Enterprise Cloud menu item in the SSP. Global shares on the perimeter firewall are made in the form of requests from the SSP.

Furthermore, there is the fail2ban component. Fail2ban is preinstalled on every VM and equipped with an SSH profile. Depending on how additional software is installed on the VMs, additional profiles may be automatically

added and activated. It is also possible to manually enter new rules or profiles.

3. Partitioning und file systems The partition table looks like this:

Mount

Size

File system

LV

Comments

- 50 GiB - - Total size of the VHD and the VG main

/boot 512 MiB fat - EFI partition (Ubuntu 24.04 template only)

/ 20 GiB btrfs main-root automatic snapshots with snapper

/var 10 GiB btrfs main-var

<swap> 5 GiB swap main-swap

/tmp 4 GiB tmpfs -

- ~15 GiB - - free storage in the VG main

As can be seen in the partition table, there is a volume group (VG) with several logical volumes (LVs). These logical volumes do not use the entire storage space of the volume group. Depending on the needs of the VM, the remaining free storage space can be used to enlarge an existing LV or to create a new LV.
Please note that this method only provides a few GB of space, which can be used if the free storage space is just barely insufficient. If a lot of storage space is required, an additional data disk can be requested or a group drive can be connected.

Btrfs is used as the file system. Btrfs is a CoW file system and all VMs are equipped with a basic snapshotting configuration on the root partition. This can be used with the snapper command line tool.

Btrfs should be suitable for all use cases, but under certain circumstances, a faster journaling file system such as XFS may be more suitable for specific applications (e.g. very large database systems).

A swap partition has also been created. However, vm.swappiness is set to 0 so that swapping only occurs in emergencies.

4. Forwarding mails to root

Content coming soon...

5. Automatic updates and monitoring

Tools provided by distributions for performing automatic updates are disabled. These include unattended-updates.service and apt-daily-upgrade.timer. Instead, an additional package called zih-avd-vm-scripts is installed.

6. Additional installed software

Various software is preinstalled on the VMs. The software to be preinstalled is currently being reevaluated. Once this process is complete, the list will be updated here.

Older VMs may contain different preinstalled software.

7. Configuration of various software

Various default settings were made on the VMs for frequently used software:

bash The configuration of bash has been expanded to include various points, see:
- /etc/bash.bashrc
- /etc/bash.zih

chrony
- chrony is the ntp client
- configured to use the ZIH time server: time.zih.tu-dresden.de
- Configuration: /etc/chrony/chrony.conf

8. Ubuntu-specific aspects

Canonical's extended security program, known as Ubuntu ESM (Expanded Security Maintenance), is available for Ubuntu VMs in the Enterprise Cloud. With this program, Ubuntu distributions receive security updates for up to 10 years. ESM is part of Ubuntu Pro.

More information here (login required):
[5]Ubuntu ESM Paketsupport installieren

[1] https://selfservice.tu-dresden.de/services/enterprise-cloud/overview/
[2] https://selfservice.tu-dresden.de/services/research-cloud/overview/
[3] https://wiki.nftables.org/wiki-nftables/index.php/What_is_nftables%3F
[4] https://wiki.nftables.org/wiki-nftables/index.php/Quick_reference-nftables_in_10_minutes
[5] https://tickets.tu-dresden.de/otrs/customer.pl?Action=CustomerFAQZoom;ItemID=927