Details zu Linux-Distributionsvorlagen in der Enterprise Cloud und Research Cloud

05.07.2025 04:33:55

FAQ-Artikel-Ausdruck

Kategorie:	Server-Dienste	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	15:29:53 - 30.06.2025

Lösung (öffentlich)

In den Diensten Enterprise Cloud und Research Cloud des ZIHs werden Templates angeboten um schneller mit einer VM arbeiten zu können.
Für folgende Distributionen wurde ein neues Konzept entwickelt, welches in diesem FAQ-Artikel näher erläutert wird:

- Debian (ab Release 12 "Bookworm")
- Ubuntu (nur als LTS-Version ab Release 22.04 "Jammy Jellyfish")

Inhaltsverzeichnis

1. Zugang und Benutzerkonten

Jede VM wird mit dem Nutzer "service" bereitgestellt. Im Falle einer neuen VM ist das Passwort des Nutzers automatisch generiert worden. Es wird dringend empfohlen, dieses Passwort neu zu setzen. Danach sollten Sie das Passwort von der VM-Übersicht im SSP entfernen ([1]Link zu Enterprise Cloud VM-Übersicht bzw. [2]Link zu Research Cloud VM-Übersicht).
Der service-Nutzer besitzt bereits sudo-Rechte. Falls gewünscht, können Sie damit auch den root-Nutzer der VM managen.

Für den SSH-Server auf der VM wurde eine gehärtete Konfiguration eingespielt:

- leere Passwörter verbieten
- Kompression abschalten
- HostKey-basierte Anmeldung verbieten
- X11-Forwarding abschalten
- AgentForwarding abschalten
- erlaubte Ciphers angepasst (siehe angehängte Datei sshd-ciphers.txt)

Nach Login erscheint noch vor der ersten Command Prompt die Message of the Day (fortan motd genannt). Diese motd enthält einige wichtige Hinweise zu dem neuen VM-Templates-Konzept. Es kann über zusätzliche Dateien im Verzeichnis /etc/motd.d/ erweitert werden.

Auf den VMs wird standardmäßig die umask 077 verwendet und bereits existierende Dateien und Verzeichnisse im Home-Verzeichnis wurden an diese umask angepasst.
Bitte beachten Sie, dass diese umask nicht dem default von Installationen aktuell üblicher Distributionen entspricht. Da ist noch umask 022 üblich.
Bitte beachten Sie, dass dies in der einen oder anderen Situation zu nicht erwartetem Verhalten führen kann.

Es wird der Kernel-Commandline-Parameter proc_hidepid=2 gesetzt. Damit haben unpriviligierte Nutzer nur noch Einsicht auf die eigenen Prozesse. Für Ausnahmen wurde die Gruppe proc angelegt. Accounts, die zu dieser Gruppe gehören, haben weiterhin die Möglichkeit, zu allen Prozessen Informationen abzurufen. Dies ist insbesondere für Admin- oder Monitoring-Konten vorgesehen.

2. Netzwerk und Firewall

Die VMs haben ein Netzwerkinterface mit einer gerouteten IPv4-Adresse. Ein IPv6-Routing findet nicht statt, aus Kompatibilitätsgründen wird IPv6 aber nicht deaktiviert. Die VMs haben damit zumindest eine link-lokale fe80::[...]-IPv6-Adresse.

Auf jeder VM ist eine lokale Firewall in Form von nftables vorhanden. nftables wird innerhalb des Verzeichnisses /etc/nftables/ konfiguriert.
Zusätzlich kann nftables über das Kommandozeilentool nft gesteuert werden.
Weitere Informationen zu nftables gibt es hier:

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

Es wird empfohlen, nftables über die entsprechenden Konfigurationsdateien und das Kommandozeilentool nft zu konfigurieren. Sollten Sie dennoch ufw als Firewall-Frontend verwenden wollen, können durch den Einsatz von nftables statt iptables weitere Konfigurationsschritte notwendig sein. Bitte bedenken Sie auch, dass das iptables-Kernelmodul deaktiviert wurde. Unter Umständen müssen Sie dieses Kernelmodul für Ihr Firewall-Frontend wieder aktivieren.

Bitte beachten Sie, dass es Firewalls auch außerhalb der VM gibt.
Campus-interne Freigaben können über den Menüpunkt Enterprise-Cloud im SSP jeweils an der VM erstellt bzw. bearbeitet werden. Weltweite Freigaben an der

Perimeterfirewall erfolgen in Form von Anträgen aus dem SSP heraus.

Desweiteren existiert die Komponente fail2ban. Auf jeder VM ist fail2ban vorinstalliert und mit einem SSH-Profil ausgestattet. Je nachdem wie zusätzliche Software auf den VMs installiert wird, kann es sein, dass zusätzliche Profile automatisch hinzugefügt und aktiviert werden. Das manuelle Eintragen von neuen Regeln bzw. Profilen ist auch möglich.

3. Partitionierung und Dateisysteme Die Partitionstabelle sieht folgendermaßen aus:

Mount

Größe

Dateisystem

LV

Bemerkungen

- 50 GiB - - Gesamtgröße der VHD und der VG main

/boot 512 MiB fat - EFI-Partition (nur Ubuntu 24.04-Template)

/ 20 GiB btrfs main-root automatische Snapshots mit snapper

/var 10 GiB btrfs main-var

<swap> 5 GiB swap main-swap

/tmp 4 GiB tmpfs -

- ~15 GiB - - freier Speicher in der VG main

Wie in der Partitionstabelle zu sehen, existiert eine volumegroup (VG) mit mehreren logical volumes (LVs). Diese logischen volumes nutzen nicht den gesamten Speicher der volumegroup aus. Je nach den Bedürfnissen der VM kann der ausstehende freie Speicher für eine Vergrößerung einer vorhandenen LV oder für das Anlegen eine neue LV genutzt werden.
Bitte bedenken Sie, dass über diesen Wege nur wenige GB zur Verfügung stehen, die dann verwendet werden können, wenn der freie Speicher nur knapp nicht ausreicht. Wenn viel Speicher notwendig ist, kann eine zusätzliche Datenplatte angefordert werden oder ein Gruppenlaufwerk angebunden werden.

Als Dateisystem wird btrfs eingesetzt. Btrfs ist ein CoW-Dateisystem und alle VMs sind mit einer grundlegenden Snapshotting-Konfiguration auf der root-Partition ausgestattet. Diese kann mit dem Kommandozeilentool snapper genutzt werden.

Btrfs sollte für alle Use Cases geeignet sein, aber unter Umständen kann ein schnelleres Journaling-Dateisystem wie XFS für bestimmte Anwendungen geeigneter sein (z. B. sehr große Datenbanksysteme).

Auch eine Swap-Partition wurde angelegt. Es wird aber vm.swappiness gleich 0 gesetzt, sodass nur im Notfall geswappt wird.

4. Weiterleitung von Mails an root

Inhalt folgt in Kürze...

5. Automatische Updates und Monitoring

Von Distributionen mitgebrachte Tools zur Durchführung automatischer Updates sind deaktiviert. Dazu gehören unattended-updates.service und apt-daily-upgrade.timer. Stattdessen wird ein zusätzliches Paket, genannt zih-avd-vm-scripts, installiert.

6. zusätzlich installierte Software

Auf den VMs wird diverse Software vorinstalliert. Gegenwärtig wird die zu vorinstallierende Software neu evaluiert. Sobald dieser Prozess abgeschlossen ist, wird die Liste hier ergänzt.

Ältere VMs können andere vorinstallierte Software enthalten.

7. Konfiguration diverser Software

Auf den VMs wurden diverse Voreinstellungen an häufig verwendeter Software vorgenommen:

bash Die Konfiguration von bash wurde um diverse Punkte erweitert, siehe:
- /etc/bash.bashrc
- /etc/bash.zih

chrony
- chrony ist der ntp-Client
- konfiguriert, den ZIH-Zeitserver zu verwenden: time.zih.tu-dresden.de
- Konfiguration: /etc/chrony/chrony.conf

8. Ubuntu-spezifische Aspekte

Für Ubuntu-VMs in der Enterprise Cloud steht das erweiterte Sicherheitsprogramm von Canonical bekannt als Ubuntu ESM (Expanded Security Maintenance) zur Verfügung. Mit diesem Programm erhalten Ubuntu-Distributionen Sicherheitsupdates für einen Zeitraum von bis zu 10 Jahren. ESM ist ein Bestandteil von Ubuntu Pro.

Mehr Informationen dazu hier (Login erforderlich):
[5]FAQ#: 4100927 — 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/public.pl?Action=PublicFAQZoom;ItemID=927