bytecluster0002

bytecluster0002 ist ein Virtualisierungsserver, der Kommunikationsdienste für den Verein bereitstellt. Er löst bytecluster0001 ab.

Administratoren

- mape2k
- maddi
- suicider
- chaos

IPs /DNS

- bytecluster0002.bytespeicher.org
  - 138.201.246.25
  - 2a01:4f8:c17:cf64::1

Betrieb

Benutzer anlegen

1. Benutzer anlegen
   1. Normaler Benutzer ohne sudo-Rechte
      - **useradd --create-home --shell /bin/bash --comment "Max Mustermann" mustermann**
   2. Benutzer mit sudo-Rechten
      - **useradd --create-home --shell /bin/bash --comment "Max Mustermann" --groups sudo mustermann**
2. SSH-Key hinterlegen
   1. SSH-Verzeichnis anlegen
      - **mkdir /home/mustermann/.ssh**
   2. SSH-Schlüssel in Datei authorized_keys hinterlegen

      ```
      ssh-rsa AAAA... KOMMENTAR
      ```

   3. Berechtigungen und Rechte anpassen
      - **chown --recursive mustermann:mustermann /home/mustermann/.ssh**
      - **chmod 700 /home/mustermann/.ssh**
      - **chmod 644 /home/mustermann/.ssh/authorized_keys**
   4. Passwort setzen
      - Das Passwort ist für den Nutzung von sudo und für die Proxmox-Weboberfläche gültig und sollte vom Benutzer dann geändert werden!
      - **passwd mustermann**

Installation

Betriebssystem

- Debian 10 minimal (vorinstalliert)

Vorkonfiguration

1. Vorgeschlagene Pakete nicht mit installieren (bereits im Standard vom Provider vorhanden)

   ```
   APT::Install-Recommends "false";
   ```

Grundeinrichtung

1. System aktualisieren
   - **apt-get update**
   - **apt-get dist-upgrade**
2. Notwendige Standardsoftware installieren
   - vim (Editor)
   - mc (Dateimanager)
   - debian-goodies (Debian-Systemtools)
   - net-tools (Netzwerktools)
   - **apt-get install vim mc debian-goodies net-tools**
3. Suche in der Konsole mit Bild-ab/Bild-auf aktivieren

```
...
# alternate mappings for "page up" and "page down" to search the history
"\e[5~": history-search-backward
"\e[6~": history-search-forward
...
```

Absicherung

1. NFS / rpcbind deaktivieren (wird nicht benötigt, offene Ports schließen)
   - **systemctl stop rpcbind.socket**
   - **systemctl disable rpcbind.socket**
2. sudo installieren und konfigurieren
   - **apt-get install sudo**
   - Konfiguration prüfen, so dass sudo von Nutzern der Gruppe sudo genutzt werden kann

```
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
```

3. SSH - Login als root und mit Passwort deaktivieren
   - Vorher mindestens einen Benutzer einrichten, der einen SSH-Schlüssel hinterlegt hat!
   1. Konfiguration anpassen

```
...
PermitRootLogin no
...
PasswordAuthentication no
...
ChallengeResponseAuthentication no
...
```

   2. SSH-Daemon neustarten
      - **systemctl restart sshd**

Proxmox

- nach Anleitung: https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_Buster

Vorbereitung

1. Hosts-Datei anpassen
   - IP-Adresse des internen Netzes nutzen, so dass später ein Proxmox-Cluster möglich ist
   - Konfiguration

```
...
# 127.0.1.1 bytecluster0002 bytecluster0002
127.0.0.1 localhost
10.10.0.2 bytecluster0002 pvelocalhost
```

```
...
```

Installation

1. Installation nach Anleitung:
   https://pve.proxmox.com/wiki/Install_Proxmox_VE_on_Debian_Buster#Install_Proxmox_VE
   - bei **apt full-upgrade** mit „install the package maintainer's version“ die Konfiguration für grub-efi-amd64 übernehmen
   - für den Punkt „Install Proxmox VE packages“ nur **apt install proxmox-ve postfix** ausführen, da open-iscsi nicht benötigt wird
     - Modify smb.conf to use WINS settings from DHCP? **No**
     - Postfix
       - Postfix Configuration: **Local only**
       - System Name: **bytecluster0002**

2FA Grundeinrichtung

1. Skript anlegen

```
#!/bin/bash

clear

USERNAME=$USER
HOSTNAME=$(hostname --fqdn)
OATHKEY=$(oathkeygen)


qrencode -t ANSIUTF8 -o - "$(echo otpauth://totp/Proxmox $HOSTNAME?secret=$OATHKEY)"

read -p "Scan QR code in your application and press enter to activate. Otherwise press
Ctrl+C" -n1 -s
sudo pveum user modify $USER@pam -keys $OATHKEY
```

2. Berechtigungen anpassen und ausführbar machen
   - **chown root:root /usr/local/bin/pve_generate_oath**
   - **chmod 755 /usr/local/bin/pve_generate_oath**
3. 2FA für PAM-Anmeldungen verpflichtend machen
   - **pveum realm modify pam -tfa type=oath,digits=6 -default 1**

Admin-Gruppe und ersten Benutzer anlegen

1. Admin-Gruppe anlegen
   - **pveum group add admin -comment „Administrators“**
   - **pveum aclmod / -group admin -role Administrator**
2. ersten Benutzer zuweisen und root sperren
   - **pveum user add mustermann@pam -groups admin -enable 1 -firstname „Max“ -lastname „Mustermann“**
   - **pveum user modify root@pam -enable 0**
3. 2FA für ersten Benutzer aktivieren
   - **ALS BENUTZER AUSFÜHREN** - vorher also **su mustermann** (falls als root eingeloggt)
   - **pve_generate_oath**
     - QR-Code scannen und nach Enter ggf. Ausführung mit eigenem Passwort für sudo bestätigen

Dauerhafter Link zu diesem Dokument:
https://wiki.technikkultur-erfurt.de/dienste:bytecluster0002?rev=1594673056

Dokument zuletzt bearbeitet am: **13.07.2020 20:44**

Verein zur Förderung von Technikkultur in Erfurt e.V
https://wiki.technikkultur-erfurt.de/