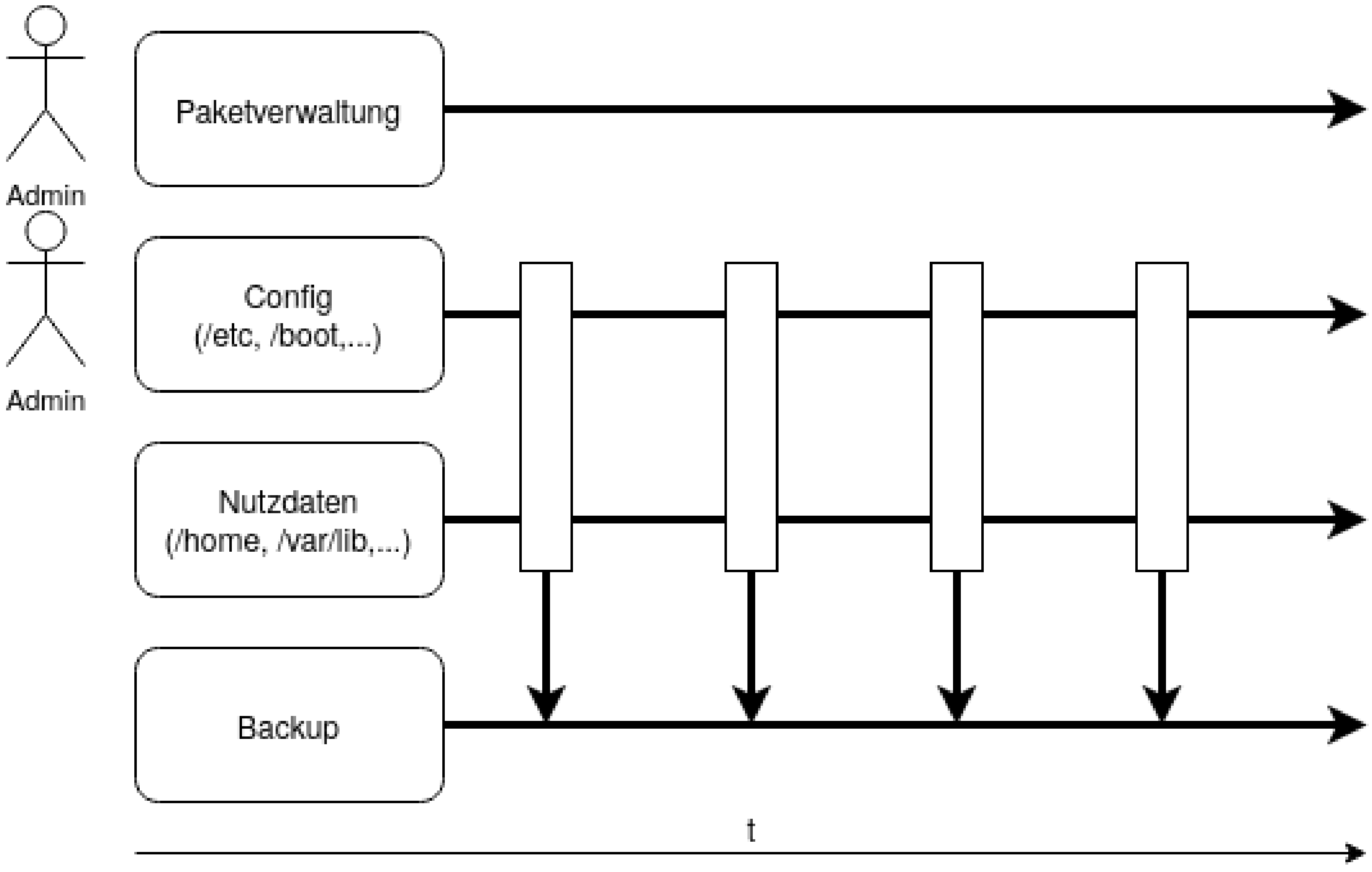
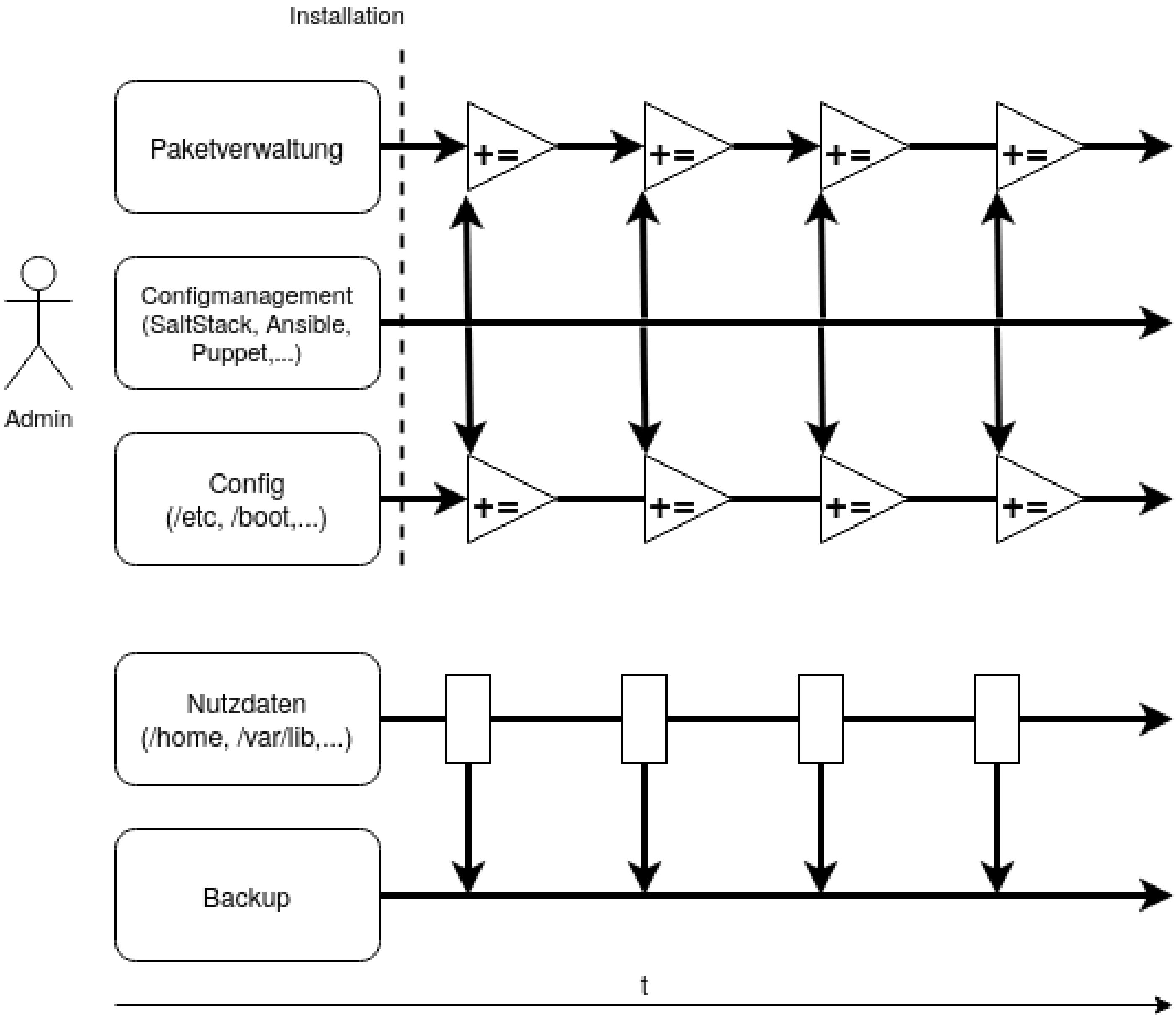
Sysadmin mit NixOS

Matrix: @hax404:hax404.de
Mastodon: @hax404@chaos.social
EPVPN: HAX4 (4294)

Lebenslauf eines Systems



Lebenslauf eines Systems

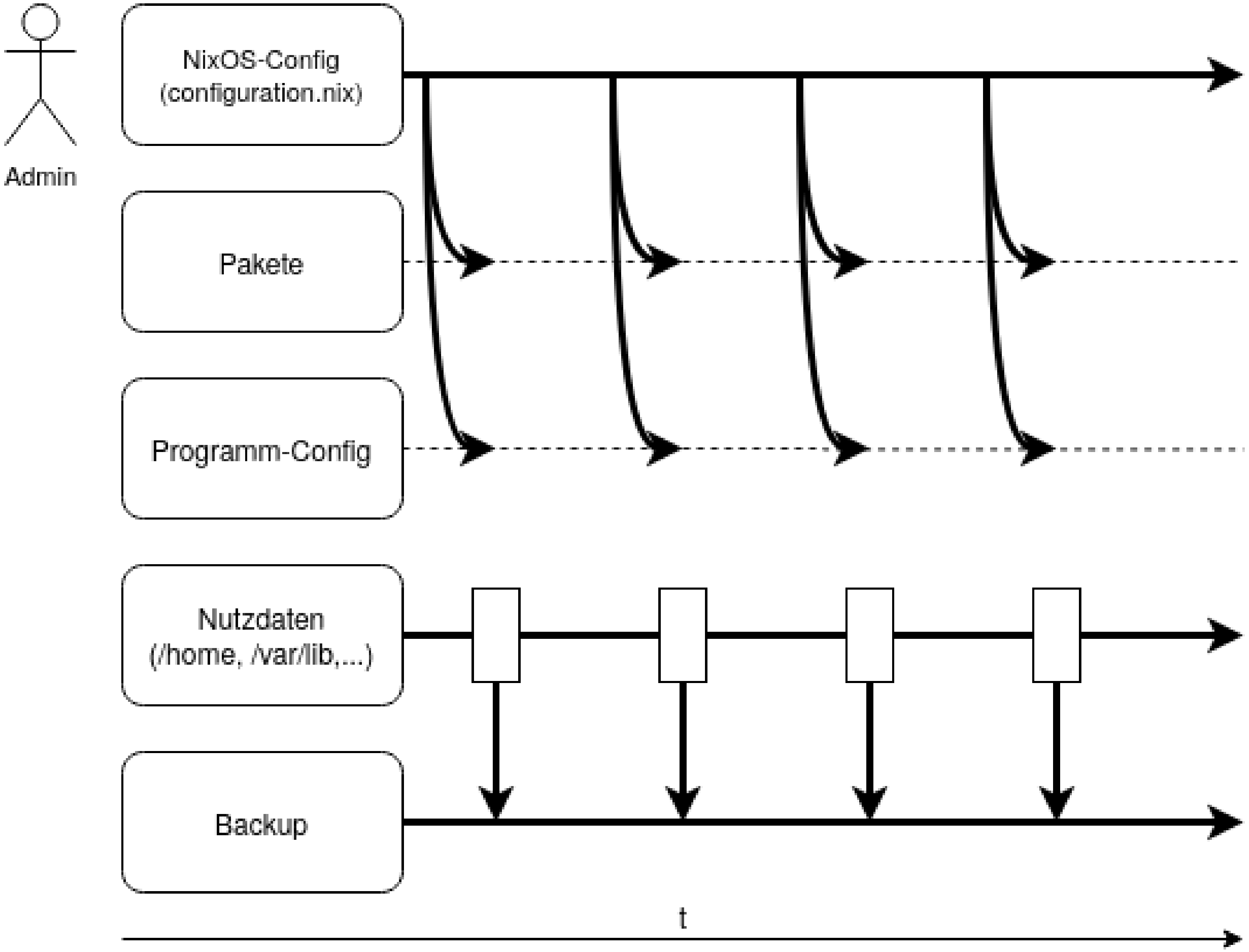

Installation
Paketverwaltung
Admin
Configmanagement (SaltStack, Ansible, Puppet,...)
Config (/etc, /boot,...)
+=
+=
+=
+=
+=
+=
+=
+=
Nutzdaten (/home, /var/lib,...)
Backup
t

SaltStack

```
/etc/cron.d/icvpn-dns:
  file.absent

/etc/systemd/system/icvpn-dns.service
  file.managed:
    - source: salt://icvpn/files/icvpn-dns.service
    - user: root
    - group: root
    - mode: '0644'
    - require:
      - file: /usr/local/sbin/icvpn-mkdns

/etc/systemd/system/icvpn-dns.timer
  file.managed:
    - source: salt://icvpn/files/icvpn-dns.timer
    - user: root
    - group: root
    - mode: '0644'
    - require:
      - file: /usr/local/sbin/icvpn-mkdns

icvpn-dns.timer:
  service.running:
    - enable: True
    - require:
      - file: /etc/systemd/system/icvpn-dns.service
```

Aus: https://git.darmstadt.ccc.de/ffda/infra/salt/-/blob/master/icvpn/init.sls

Lebenslauf eines Systems



NixOS Pakete, Module

- https://github.com/NixOS/nixpkgs
- Letzten Monat >3000 gemergte Pull Requests
- Doku:
  - https://search.nixos.org/options
  - configuration.nix(5)
  - https://nixos.org/nixos/manual/options (laden dauert!)

Prinzipien

- Trennung von

Programmen	`/nix/store`
Nutzdaten	`/var/lib, /home`
Configs	`/etc/nixos`

Secrets	`/run/secrets, /etc/secrets,`
	`/var/lib/secrets`

Installation NixOS

- Installationsmedium
  - Live-ISO
  - Network-Boot (netboot.xyz)
  - ein anderes Live-Linux (z.B. grml)
- manuelle Partitionierung und Formatierung
  - künftiges / nach /mnt einhängen
- `# nixos-generate-config --root /mnt`
  - erzeugt `hardware-configuration.nix`
- `configuration.nix` anpassen
- `# nixos-install`
  - Abfrage vom Root-Passwort
- reboot

hardware-configuration.nix

```
# Do not modify this file!  It was generated by ‘nixos-generate-config’
# and may be overwritten by future invocations.  Please make changes
# to /etc/nixos/configuration.nix instead.
{ config, lib, pkgs, modulesPath, ... }:

{
  imports =
    [ (modulesPath + "/profiles/qemu-guest.nix")
    ];

  boot.initrd.availableKernelModules = [ "ahci" "sym53c8xx" "xhci_pci" "sd_mod" "sr_mod" ];
  boot.initrd.kernelModules = [ ];
  boot.kernelModules = [ ];
  boot.extraModulePackages = [ ];

  fileSystems."/" =
    { device = "/dev/disk/by-uuid/cfc564d9-5ffb-457a-950a-1e6227c46b76";
      fsType = "ext4";
    };

  swapDevices =
    [ { device = "/dev/disk/by-uuid/d9870704-854c-4703-a42e-94082d5fa47e"; }
    ];

}
```

SSH public keys

```
{
  services.openssh.enable = true;
  services.openssh.passwordAuthentication = false;
  users.users.root.openssh.authorizedKeys.keys = [
    "ssh-ed25519 [...] georg@rick"
    "ssh-ed25519 [...] georg@spock"
  ];
}
```

Webserver mit Letsencrypt

```
{
  networking.firewall.allowedTCPPorts = [ 80 443 ];
  services.nginx = {
    enable = true;
    recommendedTlsSettings = true;
    recommendedOptimisation = true;
    recommendedGzipSettings = true;
    recommendedProxySettings = true;

    virtualHosts.“summer.hax404.de“ = {
      forceSSL = true;
      enableACME = true;
      default = true;

      locations."/".return = "301 https://www.hax404.de\$request_uri";

      locations."= /.well-known/matrix/server".extraConfig = ''
        add_header Content-Type application/json;
        return 200 '{ "m.server": "matrix.hax404.de:443" }\n';
      '';
    };
  };
  security.acme.acceptTerms = true;
}
```

Webserver mit Webseite

```
{
  services.nginx = {
    virtualHosts."ip.hax404.de" = {
      serverAliases = [ "ip4.hax404.de" "ip6.hax404.de" ];
      forceSSL = true;
      enableACME = true;

      locations."/" = {
        extraConfig = ''
          ssi on;
          ssi_types text/plain;
        '';
        return = ''
          200 '<!--#echo var="REMOTE_ADDR" -->\n'
        '';
      };
    };
  };
}
```

Webserver mit Webseite

```
{ pkgs, ... }:
{
  services.nginx = {
    virtualHosts."clock.hax404.de" = let
      segment_Clock = pkgs.fetchFromGitHub {
        owner = "fl0rp";
        repo = "7segment";
        rev = "6dd837497f919e25c98c8aa1f684965d278368c1";
        sha256 = "1np7hm84hlgyl861yczsld65n5rmf5fslzsrz0kpcs4h3g0c6czv";
      };
    in
    {
      forceSSL = true;
      enableACME = true;

      locations."/".root = "${segment_Clock}";
    };
  };
}
```

Backups – Quelle

```
{
  services.borgbackup.jobs = {
    summer-borg = {
      paths = [
        "/etc/nixos"
        "/var/lib/knot"
        "/var/lib/murmur"
        "/var/lib/vmail"
      ];
      repo = "borg@jerry.hax404.de:/var/lib/borgbackup/summer-borg";
      compression = "auto,zstd";
      StartAt = "*-*-* 00,06,12,18:46:00";
      encryption = {
        mode = "repokey";
        passCommand = "cat /var/lib/secrets/borgbackup-summer.key";
      };
      extraCreateArgs = "--stats -v";
    };
  };
}
```

Backups – Ziel

```
{
  services.borgbackup.repos = {
    summer-borg = {
      authorizedKeysAppendOnly = [
        "ssh-ed25519 [...] root@summer”
      ];
      path = "/var/lib/borgbackup/summer-borg”;
    };
  };
}
```

Wireguard

```
{
  systemd.network = {
    enable = true;

    netdevs.int_beth = {
      netdevConfig = {
        Kind = "wireguard";
        Name = "int_beth";
      };
      wireguardConfig = {
        PrivateKeyFile = "/var/lib/secrets/int_beth_wg.key";
        ListenPort = 42012;
      };
      wireguardPeers = [
        {
          wireguardPeerConfig = {
            PublicKey = "1TPr0Pz/mcNLF4eIfiuD7cfe9mDfTtQIQvf+8+uHWRU=";
            AllowedIPs = [ "0.0.0.0/0" "::/0" ];
          };
        }
      ];
    };
    networks.int_beth = {
      name = "int_beth";
      addresses = [
        { addressConfig = { Address = "172.23.136.34/32"; Peer = "172.23.137.194/32"; }; }
        { addressConfig = { Address = "fe80::1/64"; }; }
      ];
    };
  };
}
```

sqlite in postfix

```
{
  nixpkgs.overlays = [
    (self: super: {

      # Enable sqlite in postfix
      postfix = super.postfix.override (oldAttrs: {
        withSQLite = true;
      });

    })
  ];
}
```

SSH patchen

```
{ pkgs, ... }:
{
  programs.ssh.package = let
    sctpPatch = pkgs.fetchurl {
      url = "https://dev.gentoo.org/~chutzpah/dist/openssh/openssh-$
{pkgs.openssh.version}-sctp-1.2.patch.xz";
      sha256 = "1l7qyljcxz5lpv4mv8d9kmbg4sd0rm63nb4v16mb1ak5i4rn9r86";
    };
  in
  pkgs.openssh.overrideAttrs ( oldAttrs: {
    configureFlags = oldAttrs.configureFlags ++ [ "--with-sctp=yes" ];
    buildInputs = oldAttrs.buildInputs ++ [ pkgs.lksctp-tools ];
    nativeBuildInputs = oldAttrs.nativeBuildInputs ++ [ pkgs.autoreconfHook ];
    patches = oldAttrs.patches ++ [ sctpPatch ];
  });
  services.openssh.extraConfig = ''
    Transport all
  '';
}
```

/etc/nixos

```
/etc/nixos
├── config
│   ├── acme.nix                        zentralisierte ACME-Config mit DNS01-Challenge
│   ├── boot.nix
│   ├── borgbackup.nix                  Backups
│   ├── container                       NixOS Container
│   │   ├── alfred
│   │   │   └── default.nix             tmux-Weechat stack
│   │   ├── dn42                        dn42-Presenz
│   │   │   ├── bird.nix                bird2-config (BGP, babel)
│   │   │   ├── default.nix
│   │   │   ├── firewall.nix            nftables
│   │   │   ├── prometheus.nix
│   │   │   ├── socat-helper.nix        Hilfsservices für legacy IPv4-Gegenstellen
│   │   │   └── vpn.nix                 wireguard, OpenVPN
│   │   └── mpd
│   │       └── default.nix             remote Musikplayer (Anbindung ans dn42 und EPVPN)
│   ├── default.nix
│   ├── distributed-builds.nix          Freigabe als remote-Builder
│   ├── firewall.nix                    nftables
│   ├── gopher.nix                      gopher-Presenz
│   ├── knot.nix                        Master und Slave, sowie DNS-Server für DNS01-Challenge
│   ├── localization.nix                defaultLocale=en_DK.UTF-8; timeZone="Europe/Berlin"; keyMap="neo";
│   ├── mail.nix                        postfix, dovecot, rspamd, fetchmail
│   ├── matrix.nix                      synapse homeserver
│   ├── murmur.nix                      mumble.hax404.de
│   ├── networking.nix                  Netzwerk-Config, NDP-Proxy
│   ├── nginx.nix                       Webserver, reverse-Proxy
│   ├── programs.nix                    Standardprogramme, u.A. vim, tmux, mtr, tcpdump, ncdu
│   ├── prometheus.nix                  node-exporter
│   ├── radicale.nix                    Kalender
│   ├── ssh.nix
│   ├── syncthing.nix                   Ordnersynchronisierung
│   └── upterm.nix                      Terminalsharing über SSH
├── configuration.nix
└── hardware-configuration.nix
```

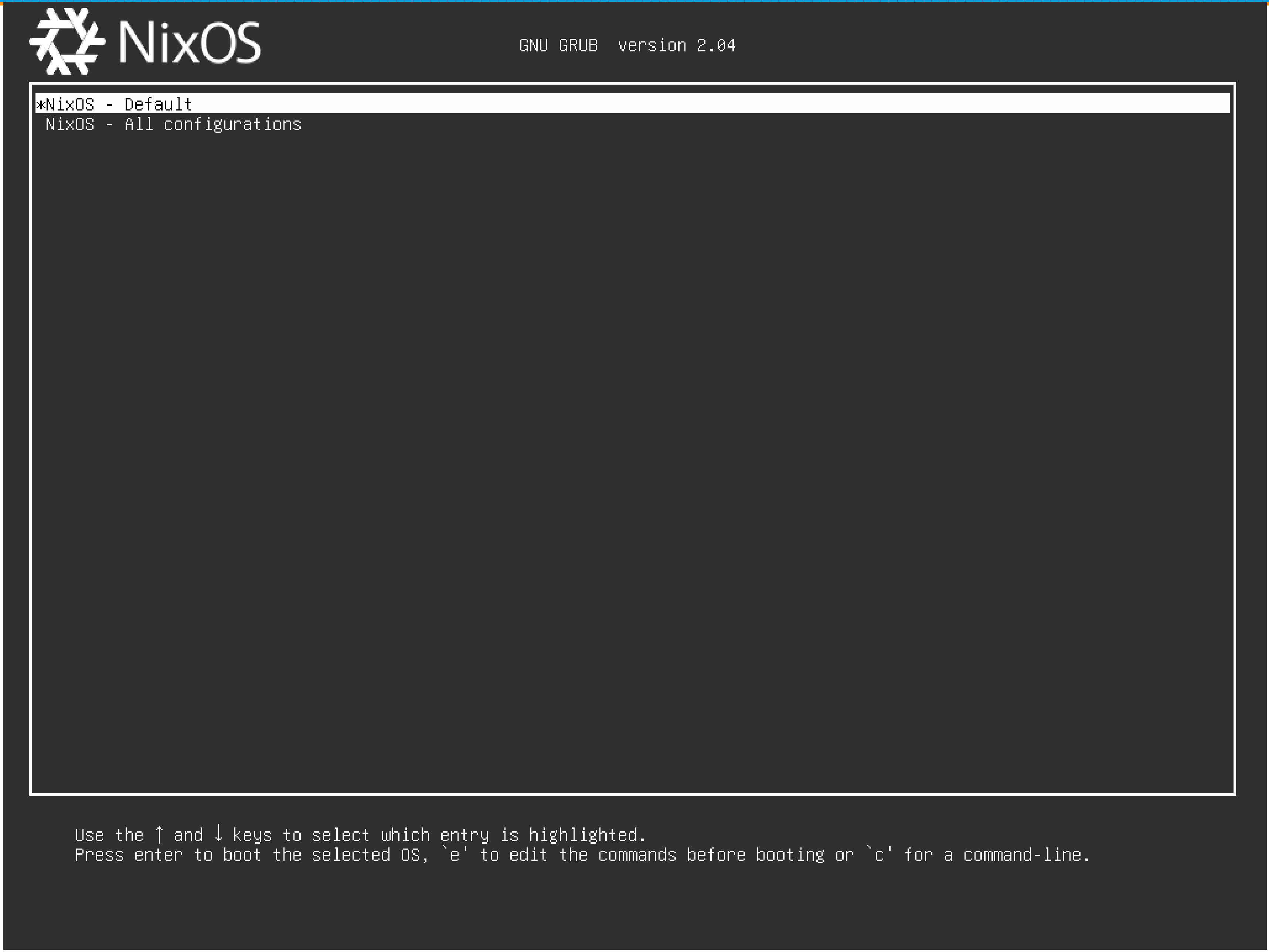
Änderungen anwenden

```
# nixos-rebuild ...
```

	build	test	switch	boot
Config bauen	✔	✔	✔	✔
Config direkt anwenden		✔	✔	
Config in Bootloader eintragen			✔	✔

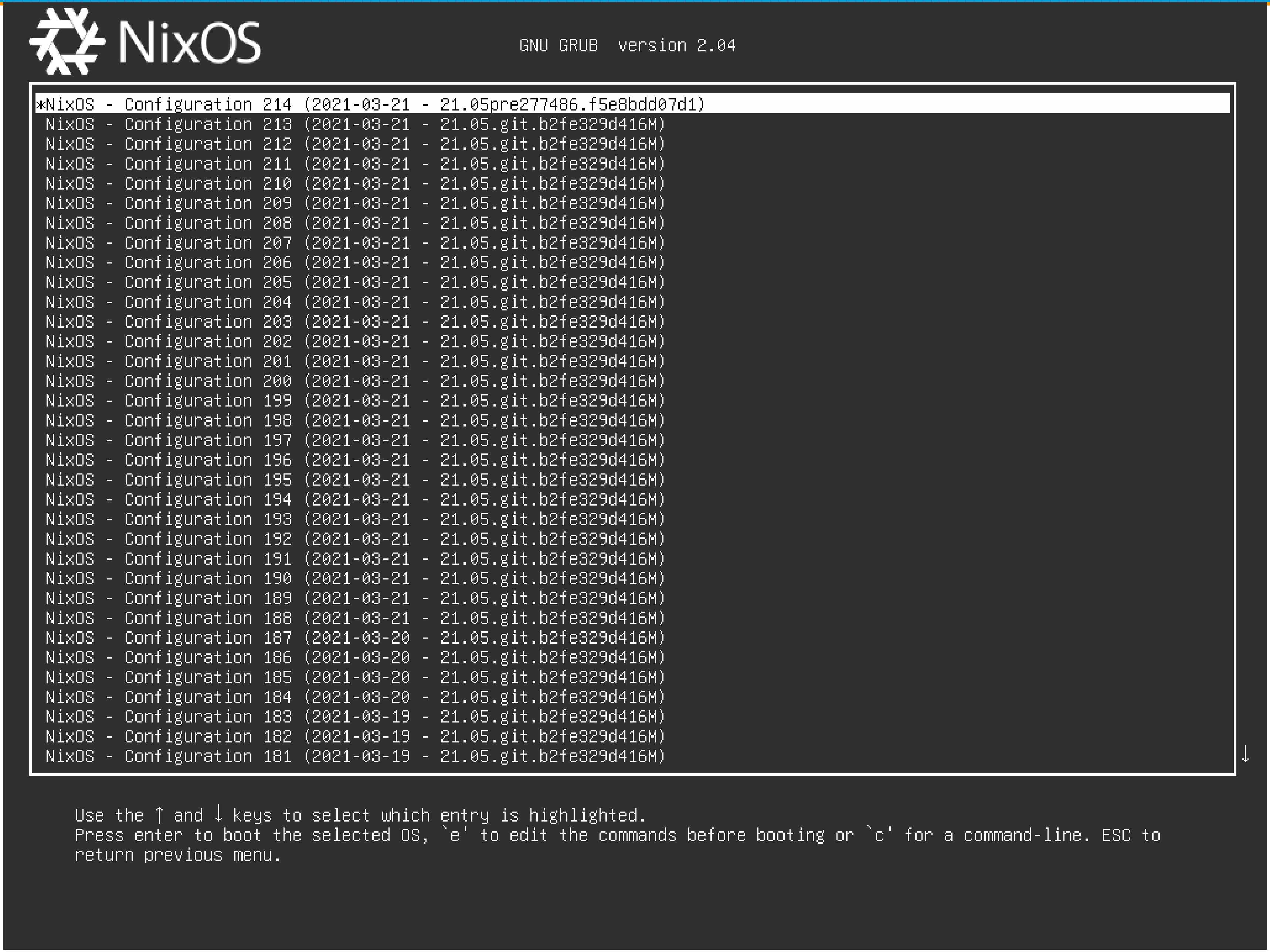
```
# nixos-rebuild switch --upgrade

# nixos-rebuild test   # sleep 300 && reboot

# nixos-rebuild -I nixpkgs=git/nixpkgs switch
```

Rollback über Bootloader



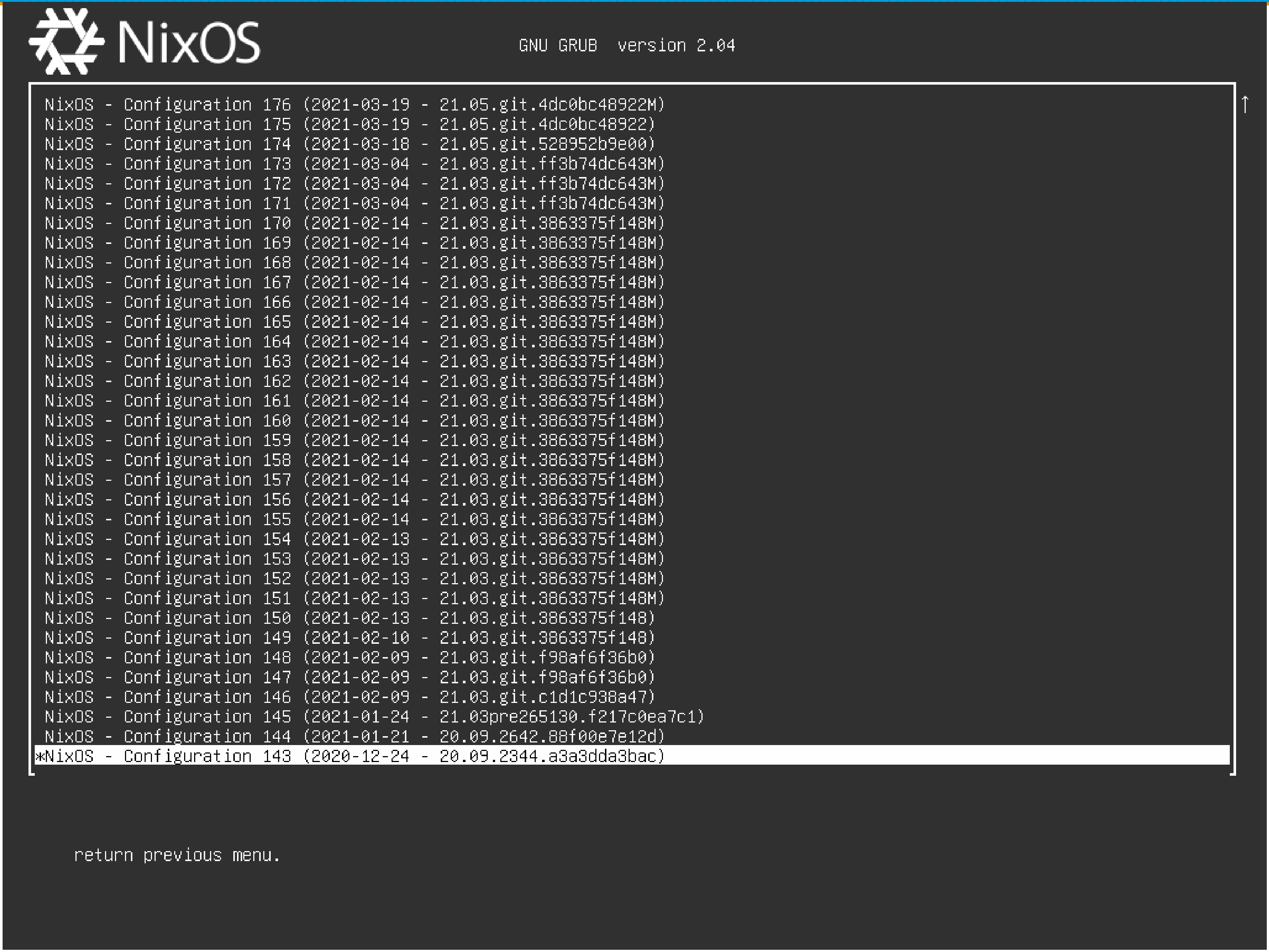
```
NixOS                                GNU GRUB  version 2.04

*NixOS - Default
 NixOS - All configurations


    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
```

Rollback über Bootloader



```
GNU GRUB  version 2.04

*NixOS - Configuration 214 (2021-03-21 - 21.05pre277486.f5e8bdd07d1)
 NixOS - Configuration 213 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 212 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 211 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 210 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 209 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 208 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 207 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 206 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 205 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 204 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 203 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 202 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 201 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 200 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 199 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 198 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 197 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 196 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 195 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 194 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 193 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 192 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 191 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 190 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 189 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 188 (2021-03-21 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 187 (2021-03-20 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 186 (2021-03-20 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 185 (2021-03-20 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 184 (2021-03-20 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 183 (2021-03-19 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 182 (2021-03-19 - 21.05.git.b2fe329d416M)
 NixOS - Configuration 181 (2021-03-19 - 21.05.git.b2fe329d416M)      ↓

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line. ESC to
    return previous menu.
```

Rollback über Bootloader



```
NixOS                                   GNU GRUB  version 2.04

 NixOS - Configuration 176 (2021-03-19 - 21.05.git.4dc0bc48922M)                ↑
 NixOS - Configuration 175 (2021-03-19 - 21.05.git.4dc0bc48922)
 NixOS - Configuration 174 (2021-03-18 - 21.05.git.528952b9e00)
 NixOS - Configuration 173 (2021-03-04 - 21.03.git.ff3b74dc643M)
 NixOS - Configuration 172 (2021-03-04 - 21.03.git.ff3b74dc643M)
 NixOS - Configuration 171 (2021-03-04 - 21.03.git.ff3b74dc643M)
 NixOS - Configuration 170 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 169 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 168 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 167 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 166 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 165 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 164 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 163 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 162 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 161 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 160 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 159 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 158 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 157 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 156 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 155 (2021-02-14 - 21.03.git.3863375f148M)
 NixOS - Configuration 154 (2021-02-13 - 21.03.git.3863375f148M)
 NixOS - Configuration 153 (2021-02-13 - 21.03.git.3863375f148M)
 NixOS - Configuration 152 (2021-02-13 - 21.03.git.3863375f148M)
 NixOS - Configuration 151 (2021-02-13 - 21.03.git.3863375f148M)
 NixOS - Configuration 150 (2021-02-13 - 21.03.git.3863375f148)
 NixOS - Configuration 149 (2021-02-10 - 21.03.git.3863375f148)
 NixOS - Configuration 148 (2021-02-09 - 21.03.git.f98af6f36b0)
 NixOS - Configuration 147 (2021-02-09 - 21.03.git.f98af6f36b0)
 NixOS - Configuration 146 (2021-02-09 - 21.03.git.c1d1c938a47)
 NixOS - Configuration 145 (2021-01-24 - 21.03pre265130.f217c0ea7c1)
 NixOS - Configuration 144 (2021-01-21 - 20.09.2642.88f00e7e12d)
*NixOS - Configuration 143 (2020-12-24 - 20.09.2344.a3a3dda3bac)

    return previous menu.
```