

# ACL

## Access Control List

Marcel Münze - HTW Berlin - 2018

## Agenda

- Was sind ACLs?
- Anwendungsgebiete
  - UNIX Filesystem
  - Network Filesystem
  - Router

Marcel Münze - HTW Berlin - 2018

2

## Access Control Lists

*„A mechanism that implements access control for a system resource by enumerating the system entities that are permitted to access the resource and stating, either implicitly or explicitly, the access modes granted to each entity.“*

RFC 4949

Marcel Münze - HTW Berlin - 2018

5

## Access Control Lists

- Liste einem Objekt angehängt
- Mehrere Einträge (Access Control Entries)
- Eintrag aus Nutzer/Gruppe/Prozess und Operation
- Whitelist

Marcel Münze - HTW Berlin - 2018

6

## Unix FS ACL

- Normalerweise: Owner Group Others  
`-rw-r--r-- 1 marcel marcel [...] .bashrc`  
→ EIN Owner, EINE Gruppe
- ACL als Erweiterung (POSIX)
- ACL Obermenge von Dateirechten

Marcel Münze - HTW Berlin - 2018

7

## Unix FS ACL (POSIX)

- Entries: type:qualifier:permissions
- Types:
  - ACL\_USER\_OBJ
  - ACL\_USER + Qualifier
  - ACL\_GROUP\_OBJ
  - ACL\_GROUP + Qualifier
  - ACL\_MASK (USER, GROUP\_OBJ, GROUP)
  - ACL\_OTHER

Marcel Münze - HTW Berlin - 2018

8

## Unix FS ACL (POSIX)

- Entries: type:qualifier:permissions
- Qualifier: name / identifier
- Permissions: r, w, x

Marcel Münze - HTW Berlin - 2018

9

## Unix FS ACL (POSIX)

```
user::rw-
user:lisa:rw-  #effective:r--
group::r--
group:toolies:rw-  #effective:r--
mask::r--
other::r--
```

Marcel Münze - HTW Berlin - 2018

10

## NFS ACL

- Feiner als POSIX
- type:flags:principal:permissions
- Typen:  
Allow, Deny, Audit, Alarm
- Flags:  
Group (g), Inheritance (d, f, n, i), Administrative (S, F)
- Principal:  
Name@Domain (oder OWNER@, GROUP@, EVERYONE@, vgl. POSIX)

Marcel Münze - HTW Berlin - 2018

11

## NFS ACL

- Permissions:
  - r (read data, list directories)
  - w (write data, create files)
  - x (execute file, change directory)
  - a (append data, create subdirs)
  - d (delete)
  - D (delete-child)

Marcel Münze - HTW Berlin - 2018

12

## NFS ACL

- Permissions:
  - t / T (read / write attributes)
  - n / N (read / write named attributes)
  - c / C (read / write ACL)
  - o (write owner)
  - y (synchronize, use synchronous I/O)

Marcel Münze - HTW Berlin - 2018

13

## NFS ACL

```
A::OWNER@:rwatTnNcCy
A::alice@nfsdomain.org:rxtncy
A::bob@nfsdomain.org:rwadtTnNcCy
A:g:GROUP@:rtncy
D:g:GROUP@:waxTC
A::EVERYONE@:rtnyc
D::EVERYONE@:waxTC
```

Marcel Münze - HTW Berlin - 2018

14

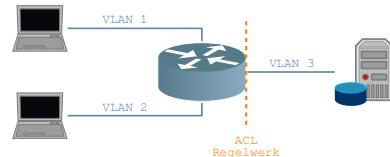
## Router ACL

- Als Firewall
- Pro Input / Output
- Pro Protokoll (IPv4, IPv6)
- Pro Richtung

Marcel Münze - HTW Berlin - 2018

15

## Router ACL



Marcel Münze - HTW Berlin - 2018

16

## Quellen

Manpage acl

Manpage nfs4\_acl

<https://tools.ietf.org/html/rfc4949>

<https://www.pluralsight.com/blog/it-ops/access-control-list-concepts>

Marcel Münze - HTW Berlin - 2018

17