

Rich ACLs in EOS

Rainer Töbicke - CERN - EOS Workshop 2019

Standard Linux ACLs

- Correspond to "Posix 1003.1e" standard
- Supported by several Linux file systems
- API, getfacl/setfacl, documentation
- Shortcomings:
 - Only registered users/groups allowed (numeric IDs), no CERN E-groups
 - Coarse permissions: only r, w, x
 - Do not match modern functionality of e.g. NFS V4 or Windows

EOS ACLs

- Directory-level ACLs, just like AFS
- Concise notation, appreciate `u:rtb:rx!w,g:c3:rw,x,z:rx`
- Stored in 2 extended attributes
 - -> unix mode bits -> `sys.acl` + `user.acl`
 - `user.acl` needs enabling
 - some "rights" are actually denials (e.g. "update")
 - E-groups support
- ACL handling: "eos attr", "eos acl", no API nor GUI

RichACLs

- Based on NFSv4 and Windows ACLs (very similar and in places bit-level identical)
- Roughly a superset of NFSv4 ACLs
- Modern, post-Posix, rich set of permissions
- Numeric IDs (system users) as well as textual "unmanaged" IDs (useful for E-groups)
- Developed by A.Grünbacher, Red Hat. User space API and management commands available in EPEL

Richacl-EOS

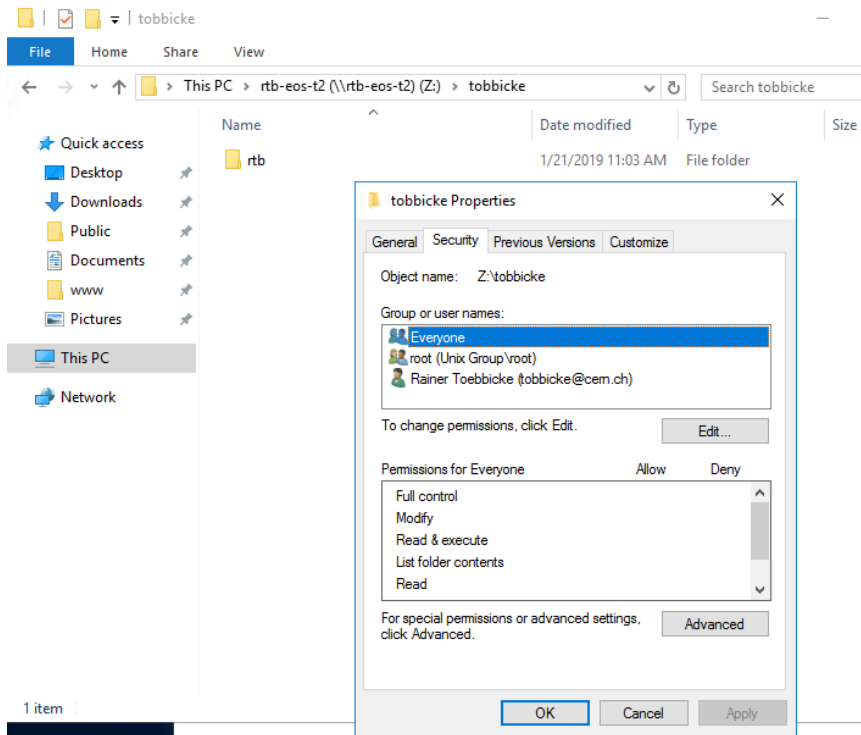
- Supported by the "fusex" interface (only)
- Reasonable set of permissions - not 100% compatible, but usable
- Textual and numeric subject IDs, textual group subject IDs treated as CERN E-groups
- Triggered EOS ACL enhancements
 - ACLs for plain files (in absence, directory ACL applies)
 - "Deny" type entries (denoted "!", with all the "use with caution" caveats)
- Spin-off: Samba VFS module, based on NFSv4 ACL module

ACL Examples

```
[rtb-eos-t4.cern.ch> pwd
/mnt/rtb-eos-t2/tobbbicke/rtb
[rtb-eos-t4.cern.ch> getrichacl .
.:
  user:rtb:rwpXd-A-WC----::allow
  owner@:rwpXd-----::allow
  everyone@:r--x-----::allow
  group@:-----D-----::allow

[rtb-eos-t4.cern.ch> mkdir dir1
[rtb-eos-t4.cern.ch> getrichacl dir1
dir1:
  owner@:rwpXdA-WC----::allow
  user:tobbbicke:rwpXd-----::allow
  everyone@:r--x-----::allow
  user:rtb:-----D-----::allow

[rtb-eos-t4.cern.ch> date > dir1/now
[rtb-eos-t4.cern.ch> getrichacl dir1/now
dir1/now:
  owner@:rwp--D-----::allow
  everyone@:r-----::allow
  user:tobbbicke:-----D-----::allow
```



ACL Examples 2

Permission Entry for rtb

Principal: Rainer Toebicke (rainer.toebicke@cern.ch) [Select a principal](#)

Type:


Applies to:

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input checked="" type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input checked="" type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input checked="" type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input checked="" type="checkbox"/> Create files / write data	<input checked="" type="checkbox"/> Change permissions
<input checked="" type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these permissions to objects and/or containers within this container [Clear all](#)

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

 Unable to contact Active Directory to access or verify claim types.

[Add a condition](#)

ACL Examples 3

The screenshot shows a Windows File Explorer window with the 'dir1 Properties' dialog box open. The dialog box has four tabs: 'General', 'Security', 'Previous Versions', and 'Customize'. The 'Security' tab is selected, showing the following information:

- Object name: Z:\tobbicke\rtb\dir1
- Group or user names:
 - Everyone (selected)
 - Rainer Toebbicke (rainer.toebbicke@cem.ch)
 - Rainer Toebbicke (tobbicke@cem.ch)
- To change permissions, click Edit. (Edit... button)
- Permissions for Everyone:

	Allow	Deny
Full control	<input type="checkbox"/>	<input type="checkbox"/>
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Read & execute	<input type="checkbox"/>	<input type="checkbox"/>
List folder contents	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
- For special permissions or advanced settings, click Advanced. (Advanced button)

At the bottom of the dialog box, there are three buttons: 'OK', 'Cancel', and 'Apply'. The 'OK' button is highlighted with a blue border.

ACL Examples 4

The screenshot shows a Windows File Explorer window with the address bar set to `rtb-eos-t2 (\rtb-eos-t2) (Z:) > toblicke > rtb > dir1`. A file named `now` is selected, and its properties dialog box is open. The `Security` tab is active, showing the following details:

- Object name: `Z:\toblicke\rtb\dir1\now`
- Group or user names:
 - Everyone (selected)
 - Rainer Toeblicke (rainer.toeblicke@cem.ch)
 - Rainer Toeblicke (toblicke@cem.ch)
- To change permissions, click Edit. (Edit... button)
- Permissions for Everyone:

	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		
- For special permissions or advanced settings, click Advanced. (Advanced button)

At the bottom of the dialog box, there are buttons for `OK`, `Cancel`, and `Apply`.

Alternatives considered

- Continue with "native" EOS-ACLs:
 - We do: EOS ACLs are simply translated back and forth to RichACLs, on-the-fly. They remain settable using the EOS shell
 - RichACLs are easier to use and more like traditional ACLs
- Support Standard Linux ACLs:
 - Doable, but limited and not lossless: EOS ACLs are richer than what Linux ACLs can express
 - Using the Windows ACL GUI on Linux ACLs would likely be confusing, for that same reason
 - Cannot express E-group subjects

RichACL Support - Summary

- EOS ACLs enhancements
 - Generalised "deny" type entries
 - Optional File-level ACLs
- RichACLs converted on-the-fly from/to EOS ACLs
 - CentOS 7, fusex only
- Samba VFS module for RichACL