univention

univention GmbH
Mary-Somerville-Str. 1
28359 Bremen
Fon: +49 421 22232-0
Fax: +49 421 22232-99
info@univention.de

Managing File- and Directory Access Rights with POSIX-ACLs

SambaXP 2007

Andreas Büsching (buesching@univention.de)

univention

Agenda

- About us
- Motivation
- Scenarios
  - Examples
  - Problems & Features
  - POSIX (Default) ACLs
- Questions?

univention

Univention GmbH

- Producer of the Linux distribution Univention Corporate Server (UCS)
- An Enterprise Distribution based on Debian GNU/Linux with a unique Management System based on Directory Services
- Founded 2001
- Customer References: Public Authorities, Financial Services, Medium-Sized Businesses, ...

Andreas Büsching

- Studies of Computer Science
- Technical Assistant for Computer Science at University of Bremen: Research & Teaching
- System Develeper at Univention
- Assistant Technical Direktor of Univention

univention

Motivation I

- File-Services
  - Most import service in computer networks
  - Sharing files within a trusted network
  - Among different operating systems (servers as well as clients)
  - Setup: High Availibility, Backup Strategies, Access Rights, ...
- Access Control
  - Restrications for files and/or complete subtrees
  - Access granted by Authentication
  - Different Access Control Models in UNIX and Windows

univention

Motivation II

- Linux servers shall provide file services for (at least)
  - Linux Clients (NFS)
  - Windows clients (SMB/CIFS)
- The following must apply independ of the client's OS:
  - Restrictions for users must have effect
  - Manipulating Permissions must be possible
  - Creating new files/directories should result in the same permissions

univention

Scenarios

- Schools of the Federal State Bremen
  - Every School has a Market Place
  - Teachers may read, write and delete every file
  - Pupils may read every file and delete their own files
  - Others should have no access
  - Problems
- Federal Office for Radiation Protection
  - One giant share
  - For almost each diretory different access rights
  - Before: for each directory two groups: to separat read and write access
  - Problems

Problems & Features I

- UNIX vs Microsoft Windows
  - Restricted possibilities compared to other operating systems like Windows
  - Three Categories: owner, one group and the rest
  - Three rights: read, write and execute
  - POSIX ACLs: extends number of categories, but not the types of access rights
  - Experience: More types of access rights not really required
  - Samba maps Windows ACLs to POSIX ACLs

univention

Problems & Features II

- Move vs 'Copy & Delete'
  - Move: files keeps acess rights
  - Copy & Delete: files inherits access rights from new location
  - NetWare environment might act differently (can be customized)
- Inheritance of Access rights
  - Windows: serveral possibilities to control the inheritance of access rights
  - UNIX: by default no inheritance
    - With POSIX Default ACLs possible

Problems & Features III

- Summary
  - Shares usable from Linux and Windows
  - Same Access Control Model
  - Complex Access Rights (more than default UNIX rights)

univention

POSIX (Default) ACLs

- An extension to UNIX rights management
- Usable on common filesystems (e.g. EXT3, XFS)
  - Configurable via mount option
- Features
  - Set rights for serveral groups and users
  - Define umask
  - Define rights inherited by child objects (Default ACLs)
- Command line tools: setfacl/getfacl
- Standard UNIX tools:
  - `ls` shows '+' after UNIX rights if ACLs are exist
  - IMPORTANT: `chmod g+???` -> modifies ACL umask and not group rights

Samba and POSIX ACLs

- Samba supports POSIX (Default) ACLs
  - Several options define the behaviour for the access control model
- Map Windows ACLs: `nt acl support = yes`
  - Activates Support for mapping Windows ACLs to UNIX rights and POSIX ACLs
- POSIX Default ACLs: `inherit acls = yes`
  - When creating objects the Default ACLs are checked
- Inheritance Behaviour: `map acl inherit = yes`
  - Uses extended attributes to store 'inherit' and 'protected' access control flags
- Changing permissions: `acl group control = yes`
  - By default only the owner (and root) may change permissions, with this flag the primary group owner too

Setting POSIX (Default) ACLs

- Linux Client: Konqueror and Nautilus
- Windows Client: Security Tab
- `setfacl` - modifies permissions
  - for single files or directories
  - for complete subtrees (-R)
- `getfacl` - display permissions
  - Of files, directory or subtrees
  - Calculates effective rights (umask)
- Examples
  - `setfacl -m user::rwx share1/file1`
  - `setfacl -R -m group:Domain Admins:rwx share1`

univention

Approach: Schools of the Federal State Bremen

- Market Place
  - Define POSIX Default ACLs
  - Full access for the owner
  - Force owner group (any but pupils or teachers)
  - No access rights for owner group
  - Rights for specific groups:

    Pupils: read and execute

    Teacher: read, write and execute

univention

Thank you for the attention

Questions?