Windows Roaming Profiles with OpenAFS

Lars Schimmer

European OpenAFS Conference

August 10, 2010

Why at all?

- Central management
- Central backup
- Central templates
- No data on workstations
- Users get their own setup on every workstation they do login
- One filesystem for all means

Why not?

- Transfer of profile on every login
- Huge profile takes ages to load
- Not every software is profile aware
- Loss of token before logout
- Loss of network
- Possible loss of data on black out
- Users need to clean profiles on their own not to get them to big

How does it work?

- Workstations & Users in AD Domain
- Login against Domain (krb5-auth)
- Ticket/Token at login
- Windows fetches profile data from OpenAFS path (e.g. \\AFS\cgv.tugraz.at\home\user\winprofile.V2)
- User is logged in and works on local data
- No data is synced to OpenAFS yet!

How does it work? Pt. 2

- On logout all data is synced to OpenAFS path
- Local profile data on workstation may be removed while syncing or may be left on workstations harddrive
- In case of error, syncing will be stopped and logoff might break

Preparation of AD

- Given: working OpenAFS and AD setup, Users obtaining tickets/tokens from AD servers (or trusted krb5 servers)
- This for: single-DES enabled (STILL)
- For profiles enable "Do not check for user ownership of roaming profiles Folders“ Policy in Policies/Administrative/Templates/Sytem/Users Profiles – Windows does not know anything of ACLs!
- Set Policies on roaming profiles as you like (e.g. remove after logout)
- Install the UNIX extension to the AD, for setting home path and UID on users attributes. This enables your users to login to unix and windows with same account

Works in OpenAFS

- Create volumes for users home and win profile
- Create mountpoint winprofile.V2 for win profile
- Important: .V2 is added automatic for Windows Vista/7/8 profiles in AD
- Create users with IPs of AD servers
- Create a OpenAFS group which contains the AD IP users
- Set ACLs to lookup for the path into users winprofile.V2 for the OpenAFS-AD group
- Set ACL to read/write for user into profile path

AD User Settings

- In User Properties in profile tab
- Enter the UNC path to the profile directory, e.g.
- \\AFS\cgv.tugraz.at\home\schimmer\winprofile
- Take care: HERE do not enter the .V2, it will be appended automatic by Windows AD!
- In the UNIX attributes tab, enter the UID as OpenAFS user ID, the shell as wanted and the Home Directory as e.g. \\AFS\cgv.tugraz.at\home\schimmer

Ready to go

- Thats all!
- Now we are ready to test it:
- Go to a workstation and try to login as the prepared user
- After a Login/Logoff cycle, the OpenAFS directory should contain the usual windows profile content
- => it works!

Advanced

- Some more:
- Folder redirection
- Predefined skeleton profile on every login (clean system)