SerNet

Samba and AFS

SambaXP 2004

Göttingen

7. April 2004

Volker Lendecke

SerNet - Service Network GmbH

Network Service in a Service Network

SerNet

Outline

- What is AFS
- Internal structure of AFS
- Samba/AFS Integrations Problems
- Samba solutions

Network Service in a Service Network

SerNet

What is AFS?

- Scalabale Network File System
- Origins at Carnegie Mellon University
- Andrew Carnegie, Andrew Mellon so Andrew FS
- At least 15 years old
- Many Servers
- 20000 clients with hardware of 15 years ago
- CMU->Transarc->IBM->Open Source

Network Service in a Service Network

SerNet

Scalability

- Kerberos as Authentication Protocol
- Logon once, access any number of servers
- User-based access controls, the server does not trust the client machine as in NFS
- Fileserver sees user identity through Kerberos ticket
- KDC is named *kaserver*

Network Service in a Service Network

SerNet

AFS file access semantics

- AFS doesn't lie
- NFS tells programs that it has Posix Semantics where it can't
- No byte range locks
- File changes only visible after a close
- Agressive persistent client caching

Network Service in a Service Network

SerNet

Volume Database

- Central file space under /afs
- Volume Location Database shows the physical location of abstract volumes
- Client Workstation asks dynamically
- Easy data replication
- Data relocatable while being accessed
- Server maintenance possible

Network Service in a Service Network

Protection Server

- Second AFS user database (besides kaserver)
- Tasks:
  - Map names and numeric AFS ids
  - Maintain groups and group memberships
  - Users can create groups of their own
  - Determine group id's of a user (create the NT token...)

Access Control

- User fetches a ticket via klog
- Client-Workstation gets the ticket pushed into the kernel
- Access to fileserver: Ticket is sent along with the request
- Fileserver decrypts ticket and finds the username
- Fileserver then asks ptserver for the numerid ids

AFS-ACLs

- Permissions only per directory, file access is regulated there
- Inheritance rules become a bit easier than under Windows....
- Directory permissions: (L)ookup, (I)nsert, (D)elete
- File permissions: (R)ead, (W)rite, (L)ock
- Special: (A)dminister

SerNet

Integration Problems:

- Klog needs plain text password
- Samba never sees the plain text password
- Pts-Database must be maintained
- AFS-ACLs are different from both NT and Unix
- More than one Samba exporting the same AFS space

Network Service in a Service Network

Fake-KAserver

- Kerberos Auth: Ticket encrypted with secret shared between server and kaserver
- First idea: AD is Kerberos-based, let's use those!
  - AD is Kerberos 5, AFS is still version 4
  - AD falls back to NTLM in really many cases
  - AD-Ticket is issued for Samba Server, not AFS
- Samba creates tickets on its own (AFS developer: „And you can still sleep?“)

ptproxy

- Integrating AFS into a Windows world means manually maintaining AFS group memberships
- Main task of ptserver: Username->List of numeric id's the user is able to use
- Ptserver replaced by ptproxy
- Ptproxy asks the locally running winbind

SerNet

AFS-ACLs

- Wish: Looking at and maintaining AFS-ACLs from Windows security editor
- Samba has a mapping to Posix ACLs
- AFS has system calls of its own
- Samba Posix ACL mapping is not usable
- Separate VFS module: afsacl

Network Service in a Service Network

SerNet

AFS-Locking

- AFS has no Byte Range Locking
- You can lock a complete file (L)-Permission
- SHARING_VIOLATION: Somebody else uses that file
- 'afs exclusive locks' enables multiple smbd's accessing the same file space
- Uses AFS caching over WAN links

Network Service in a Service Network

SerNet

Questions?

Volker Lendecke, VL@SerNet.DE

SerNet – Service Network GmbH
Bahnhofsallee 1b
37081 Göttingen

Tel: +49 551 370000 0
Fax: +49 551 370000 9
http://www.SerNet.DE

http://Samba.SerNet.DE

Network Service in a Service Network