No DC Around, Now What?

Protocols For Offline Support
Outline

- Introduction
  - About Myself
  - The Samba4 Story
- Offline Support
  - Scenarios
  - Data Needed
- Protocols used
  - Krb5
  - DRSUAPI
Introduction
About Myself

- Wine developer since 2005
- Samba Team member since 2007
The Samba4 Story

- Experimental branch
- Not intended for production
- Not going to be “the next Samba release”
Offline Support
Scenarios

Looking at files owned by others

- Want to translate SIDs used in ACLs
- Need to know user’s group memberships
Scenarios

Known user logs in

- Need to authenticate user
- Need to know user’s group memberships
Scenarios

Unknown user logs in

- Nothing we can do
Known, deleted user logs in

- Nothing we can do
Data Needed

- SID <=> Name mappings  ==> SAMdb
- Authentication ==> PAC/INFO_3
Getting SAMdb

- SID <=> name mappings visible to all members
- Group membership information
- Can be replicated with DRS
Getting the PAC

- Part of the user’s TGT
- Cached
- Needs timeout
Protocols Used
Kerberos 5

- Unix single sign-on
- Used in Active Directory
- In AD, contains PAC
- PAC contains group information
DRSUAPI

- DCE/RPC-based protocol
- Used by Directory Replication Service
Summary

- Support for common scenarios
- Caching also takes load off the DC
- Good for clusters
Thank you

Questions?