Bring on the replication

The year of Replication in Samba4
Sysadmin Miniconf – Linux.conf.au 2010

Andrew Bartlett <abartlet@samba.org>
Samba Team
Cisco Systems
abartlet

• A Samba developer for 9 years now
• One of the lead developers on Samba4
• I work for Cisco Systems
  – Full time on Samba4
  – But these are my views, not theirs
• Please ask questions during the talk
Samba4

- Provides AD-compatible Domain Controller
- Now also a replication Partner!
Replication

• Replication of user and group data
  – Data in the Directory
  – Not Group Policy data
  – Between Domain Controllers

• Replication of Passwords
Why Replication?

- Making Samba safe(er) to deploy
- Who wants a single point of failure?
Before

• Samba4 was suitable for:
  – Greenfield sites
  – Sites with only one domain controller
  – Sites willing to cut and run
The risks of cut and run

• Process:
  – Vampire AD domain
  – Shut down AD domain
  – Start up Samba4
  – Hope everything still works

• There was no way back
  – As soon as Samba starts, the DB may change
  – No way to replicate changes back
Now

- As of alpha11
- Benefits:
  - Samba4 is (more) suitable for sites with existing domains
  - Samba4 can be disabled, without loss of data
- Risks
  - Incorrect data written will be propagated across the enterprise
But didn't we already have replication?

- LDAP replication isn't really good enough
- We really need replication with Windows
  - And not just by using LDAP or DirSync
- The LDAP protocol does not have transactions
  - Nor do our current backend servers
  - We want both replication and transactions
DRS Replication

- The native replication with Windows
- Supported in both directions
- Supported from both initiators
  - Samba's provision
  - Windows 'dcpromo from scratch'
- NOT supported with the LDAP backend
Read Only Domain Controller

- Our next priority
- Allows safe incremental deployment
- Suitable for insecure branch offices
  - So a buggy Samba can't be any more malicious :-(
- This reduces the 'pollution' risk
  - No need to validate updates if there are none
Remaining risks

- **Access Control**
  - We have not fully locked down our LDB stack
  - Certain controls allow bypass of ACLs
- **Samba4 may mislead it's clients**
  - Group policy files not sync'ed yet
- **Disasters in the Samba4 code**
- **AD servers don't validate inbound replications**
Remaining tasks

- Admin tools
- Multi-domain forests
- Role management
- DNS
- And the DRS TODO list.
Interoperable DC versions

• Tested with
  – Windows 2008 R2
  – Windows 2008
  – Windows 2003
Production sites

- Secret Russian production site
- And a few others
  - Less intense use
  - Little feedback
Testing sites

- Little interest out of last year's Sysadmin Miniconf
- Have you eliminated all your windows clients?
- What are we not doing right?
Can I have version 1.0?

• No

• We will not 'release' Samba4 just to get the testing we need
  – Samba4 is unlikely to suit you if you can't pull from GIT to fix the problems you report
Demo Time!