



Samba 4.0 released

What next for the Active Directory DC?



About me

- Andrew Bartlett
- Samba Team member since 2001
- Working on the AD DC since 2006
- These views are my own, but I do with to thank:
 - My employer: Catalyst IT
 - Our client NETGEAR Inc for their support of this work
 - My fellow Samba Team members

Samba 4.0 released!

- The combination of many years work
 - File server
 - Print server
 - Active Directory Domain controller
 - (and many other features)
- Now on the road to Samba 4.1
 - Due for release on Friday Sep 27
 - Consolidating on the 4.0 release
 - Improved client library handling for SMB3
 - Keeping to our fixed release schedule

Re-opening the heart of the network

- Samba's AD DC brings open source to the heart of the network again
- Samba has long provided a Domain Controller
 - But without support for Group Policy and other AD features like Kerberos
- Organizations again have a practical choice other than Microsoft Windows

The flexibility to innovate

- Open Source lets you do more
- Just as Samba is in many NAS devices, including NETGEAR's ReadyNAS
- Samba inside Catalyst's print server
 - No CALs, multi-device access
- Imagine
 - What if was also an AD DC?
 - Instant branch office solution
 - Perhaps managed from the cloud?



A private DC for your NAS?

- Isolate your NAS from the shared customer DC
- Keep user data close to the NAS that needs it
- Informed on change, not cache timeout

Innovative Directory Solutions

- Samba 4.0 as an AD DC firstly works just like Windows AD
 - LDAP / Kerberos / NTLM all integrated into a 'just works' package
- But being open source, some have taken it further
 - Univention Corporate Server installs modules into Samba 4.0 for to sync passwords with OpenLDAP
- Samba provides access to the previously unreadable password hashes
 - I've seen integration tools both read and write these

Breaking vendor lock in

- Samba can migrate to and from Microsoft Windows based AD domains
 - Without loss of data
 - Without password resets or domain joins
- Samba 4.0 can upgrade existing Samba 3.x domains to AD
 - And you can even migrate that to a Microsoft Windows AD if you want to
 - We won't hold you against your will!

Uses Native Microsoft Admin tools

- Microsoft Management Console snap-ins
 - In general, fully supported by Samba 4.0 AD DC
 - Are the recommended GUI tool
 - Down-loadable from Microsoft for running on Windows desktops joined to the domain

Group Policy

- Fully supported on the AD client
 - Not yet supported on Linux clients or Samba servers
 - Google Summer of Code project in progress on this point
- Single most requested feature for Samba domains
- Group Policy administration is done on a windows client

Read Only Domain Controller

- We support both being and hosting RODCs
- Ideal for remote offices
 - Don't store all the passwords for the company everywhere
- Ideal way to start with Samba as an AD DC
 - As we can't break what we can't change!

Or our command line tools

- Samba-tool
 - Our primary commandline tool for the AD DC
- LDB tools
 - Directly access the underlying database using LDAP-like syntax
- Python bindings
 - Create powerful scripts calling our python API

Easy to set up

- samba-tool domain provision
 - Follow the prompts
- Then just run:
 - samba
- And then join a Windows client to the domain!
 - Ensure it is using the Samba server for DNS

Users of the Samba 4.0 AD DC

- Schools, NGOs, Companies, Cities
 - I've seen admins from all of these using Samba 4.0 AD DC even pre-beta!
- Incredibly enthusiastic user base
 - We know folks are trying it all the time, as if we make a mistake, we hear about it fast!

Samba 4.0 and the Cloud

- Cloud computing is largely Open Source
 - Spin-up, spin-down
 - Not chasing licensing when scaling is a big cost advantage
- Integrate Samba 4.0 into or as the cloud IDM?
- Use our Read Only DC code for user cloud sync?

Replication – multiple DCs

- Replication between multiple Samba and Windows Domain Controllers works
 - With some limitations
 - Dense mesh replication in 4.0 and 4.1
 - No site optimization
 - Schema changes not recommended
- Still best option for redundancy
- Let Samba do it's own replication
 - Don't use an OS level replication service under our databases

Direction: Where to for the Open Source DC?

- Samba 4.1
 - Consolidation of the DC code
 - Most fixes backported to 4.0
- Samba 4.2
 - Current development series

Domain Trusts and multi-domain forests

- Active effort to finish the work here
 - Developers working at the plugfest to find the low-hanging fruit
- Much of the work already done!
 - Stalled to allow us room to release Samba 4.0 and 4.1
 - KDC (Heimdal) always supported trusts
 - FreeIPA developed the RPC code and tests
 - Inter-forest trusts in particular

Improved KCC

- Written before 4.0, but only enabled in 4.2
- Python
 - Easier to modify than C
 - Implements a proper (non-dense) replication graph

Sysvol replication

- An area of continued interest
- Two replication protocols:
 - FRS
 - DFS-R

Improved, single winbind

- Making it easier to build a single 'everything' box.
- Support winbindd features
 - 'winbind use default domain'
 - Caching
 - Consistent behaviour on template parameters
 - RFC2307 support for homeDirectory and posixShell
- Still started from 'samba'
 - All AD DC features, regardless of code origin start the same way

Group Policy application on the DC

- Password policy in particular
 - Allowing use of Microsoft tools to set password policy
- Google 'Summer of Code' project

OpenLDAP backend

- A great example of Samba's flexibility
 - First attempted during early AD DC development
 - Put aside while we worked on to get our 4.0 release
- Now being revived!
 - NOT connecting to existing LDAP servers
 - A new effort to build a combined OL/Samba DC with AD semantics

Conclusion

- Samba 4.0 brings the world's first Open Source AD Domain Controller
- Already deployed in production in a variety of settings
- Provides equal-footing inter-operability with Windows DCs.
- A key project to watch as the ID Management space changes, particularly with the cloud
- Development continuing on new features.

Questions?
