

The Samba logo is displayed in a bold, white, sans-serif font. The letter 'S' is stylized with a white arrow pointing to the left, and the letter 'A' has a white arrow pointing to the right. The logo is set against a dark grey rectangular background.

SAMBA

opening windows to a wider world

The Samba 4.0 AD Domain Controller

Linux.conf.au 2013 SysAdmin mini-conf

Me – Andrew Bartlett

- Samba developer since 2001
 - Working on the AD DC since soon after the start of the 4.0 branch
 - Samba4 started as a new file server back in 2005
 - Moved on to take on the challenge of the AD DC
 - These views are my own, and not that of any of my employer or clients.
 - That said, I thank NETGEAR for their support
-

Samba 4.0

- Released in December
 - A major release for the Samba Team:
 - SMB3 File server
 - New unified build system (smaller binaries)
 - Python client libraries
 - AD Domain Controller
 - Supports external projects such as OpenChange, FreeIPA
-

Integration – there is only one Samba 4.0

- The theme of the last year of development
 - Removing much of the split-track development
 - Moving towards 'use any code, anywhere'
 - Regardless of the original historical development codebase
 - Using our primary SMB3 file server for all server roles
 - Samba 4.0 is the agreed future of the Samba project
-

Upgrading file servers

- Maintaining most existing features and behaviors
 - The binaries we shipped in Samba 3.6 still work the same
 - Some features deprecated and removed
 - security=share
 - security=server
 - **Not** a large change for file server users
 - SMB3 support is additional and optional
 - Continuous integration has kept the tree quite stable
-

Upgrading to Samba 4.0 AD DC

- Upgrades of classic passdb backends into the AD DC
 - samba-tool domain classicupgrade
 - Will upgrade all of
 - tdbsam
 - smbpasswd
 - Ldap
 - Migration from windows
 - samba-tool domain join
 - **No** need to rejoin client workstations
-

LDAP Backend

- Samba 4.0 as an AD DC **can not** use a OpenLDAP backend
 - Must use Samba's Internal LDAP server
 - To use the AD DC may require migration of other LDAP users
 - Migration is still 'samba-tool domain classicupgrade', but expect manual work after that
 - May be difficult to load additional schema
 - Expected to work, but there have been issues here
-

KDC – Embedded Heimdal KDC

- No way to use a different KDC
 - We have to match AD features exactly
 - Import from MIT KDC is a manual process
 - Upgrade from Heimdal/Samba3 is via the classicupgrade
 - Plus manual fixup
-

Trusts

- We don't have trusted domain support
 - Exceptions:
 - Some inter-realm trust stuff happens to work
 - Being trusted by a Samba classic domain works
 - That means no parent-child domains
 - One domain == One Forest
-

Replication

- Replication works
 - Not fully supported
 - Dense mesh replication
 - No site optimization
 - Schema changes particularly unreliable
 - Still best option for redundancy
 - Do NOT use CTDB or DRDB with the AD DC
-

Packaging

- NO proper packages of the AD DC
 - For any major distribution
 - Except packages in /opt
 - Issues:
 - Red Hat / Fedora Packages
 - Disable the AD DC
 - Debian / Ubuntu Packages
 - Disable the smbd/s3fs file server
-

Other major TODO items

- Sysvol replication
 - Currently needs to be manually provided
 - Replication topology
 - We need to use a more efficient algorithm for larger networks
 - Improve performance in very large (> 10,000) user domains
-

Folks already using 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!



AD DC Summery

- We now use the same file server in all default server roles
 - We force the use of the `acl_xattr` module
 - AD DC can co-exist with standard file server tasks
 - However we recommend larger sites split the roles
 - Still a different winbind however
 - This impacts idmap handling primarily
 - This is a task for 4.1
-

Questions?

