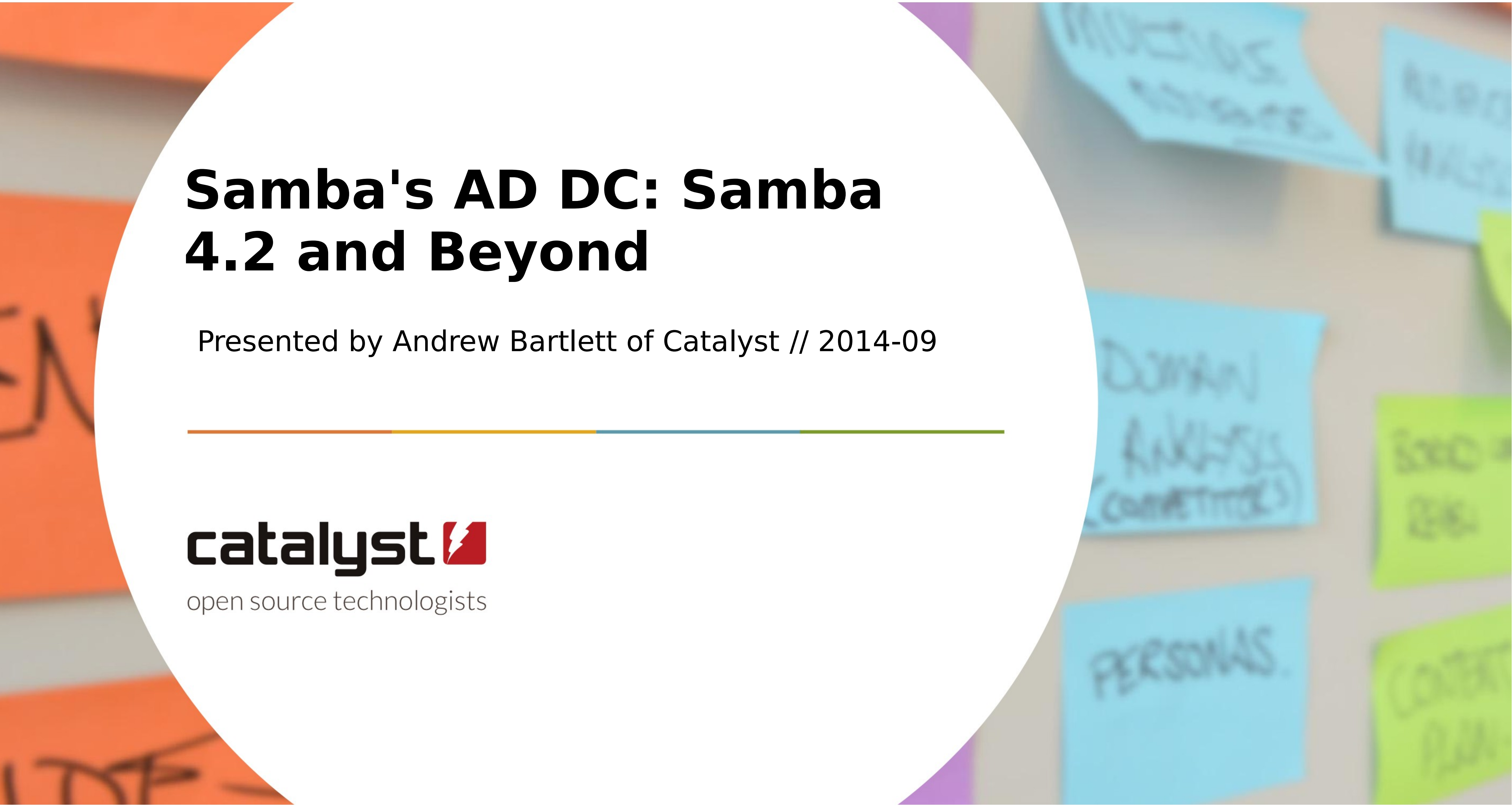


# Samba's AD DC: Samba 4.2 and Beyond

Presented by Andrew Bartlett of Catalyst // 2014-09

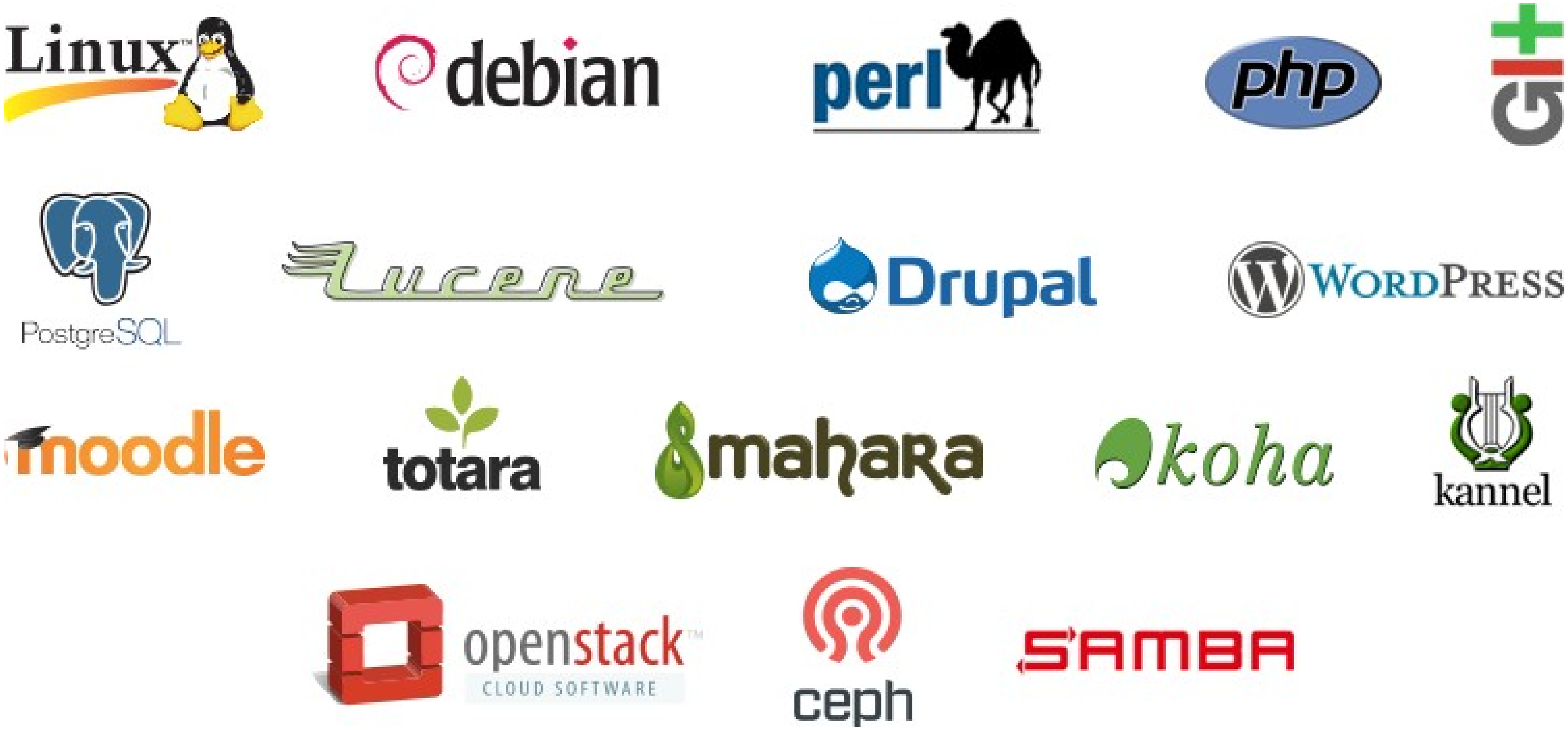
catalyst

open source technologists

# 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
  - My fellow Samba Team members

# Open Source Technologies



# Samba's AD DC

- The combination of many years work
  - File server
  - Print server
  - Active Directory Domain controller
  - (and many other features)
- First Release Dec 2012
- Now on the road to Samba 4.2
  - Due for RC1 on Monday Sep 22

# 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?

# 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

# 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 provisoin
  - 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

# Group Policy

- Fully supported on the AD client
  - Not yet supported on Linux clients or Samba servers
  - Google Summer of Code project last year
    - Still needs to be cleaned up
- 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!

# 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

# Status of the Samba AD DC

- What is new  in Samba 4.2
- Where are we headed beyond Samba 4.2

# What is new in Samba 4.2?

- Finally a single winbindd
- Domain trusts (in progress)
- Improved DRS replication stability
- Improved DNS behaviour

# Improved, single winbind

- Making it easier to build a single 'everything' box.
- Support winbindd features
  - 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

# Domain Trusts and multi-domain forests

- Active effort to finish the work here
  - Developers working at the plugfest to find the low-hanging fruit
  - Merged winbindd a key step in this process
  - Samba can now join Windows as a subdomain
- Stalled to allow us room to release Samba 4.0 and 4.1
- Support for both NTLM and Kerberos cross-trust authentication

# Improved stability of DRS replication

- From the experience of production deployments
- Dbcheck tools and runtime checks to detect partial record replication
- Improvements back-ported to later Samba 4.1 releases

# Improved DNS behaviour

- Ensuring we delete records for interfaces that go away
- Avoiding the 100,000 record DB issue
  - A 4.1 regression in the internal DNS server
- Added unit tests for bind9 DLZ module

# 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

# Improved KCC

- Written before 4.0, not yet enabled
- Python
  - Easier to modify than C
  - Implements a proper (non-dense) replication graph
  - Still needs some work

# Sysvol replication

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

# 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

# Using Samba's AD DC

- Many existing, production users
- As a product
- As a platform
- In the cloud

# Users of the Samba 4.x 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 AD DC as a product

- Use Samba out of the box as an AD DC
- Bundle it with our file server for a small business server
- Find it in better Linux distributions
  - Debian backports
  - Ubuntu 14.04
  - Not RHEL or Fedora yet
- Download it from enterprisesamba.org
- Buid it yourself

# Samba AD DC as a platform

- The platform for these products:
  - Zentyal combines it with OpenChange for an MS Exchange replacement
  - Univention combines it with OpenLDAP and a web UI for Univention Corporate Server
- Build your own product or service on Samba's AD DC
  - NAS
    - Small Buisness Server device
  - Cluster
    - Fast, local RODC for reliable directory access

# Samba in the Cloud Platform

- Not just in the cloud, part of the cloud platform
- Samba already part of Manila (file server as a service)
  - The 'Generic' driver is Samba and NFS on Linux
- Samba's AD DC should be the same
  - Perhaps in Murano
  - Perhaps as something more specialised

# The opportunity of the cloud

- In the cloud, the questions of brand go away
  - Clients trust the provider to provide a service
  - Already Azure AD is a different implementation
- Flexible service offerings
  - Choose trade-offs you can't do in general
  - Perhaps fast LDAP instead of DRS replication?
  - Link or sync to another identity system

# Use cases for Samba in the cloud

- The ideal cloud identity provider for:
  - Windows servers
  - Windows Desktop as a service
  - Sync back to the corporate domain with our RODC
- The ideal file server for:
  - Image hosting
  - export ceph, GlusterFS to clients
- The ideal partner to OpenStack
  - Integrate Samba 4.x as the cloud IDM?

# What could you do with Samba?

- Are you a cloud provider based on OpenStack?
- Do you or your customers use a lot of Windows?
- Would you like an integrated directory with LDAP and Kerberos?

# 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

# Conclusion

- Samba 4.x 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? / Catalyst Services

- Catalyst is a consulting business  based in Wellington, NZ
- Providing Samba / SMB / windows interop services
  - Samba feature development
  - 3rd and 4th level support for Samba using OEMs
  - Support of Samba installations
  - Protocol questions
- We are only 3 or 5 hours away by time-zone
- Local phone call access: 650 479 3022
- www.catalyst.net.nz