Pushing users into the pit of success

War stories from the Samba 4.0 upgrade

Presented by Andrew Bartlett of Catalyst // 2015-01

catalyst

open source technologists

Please ask questions during the talk

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

Samba's AD DC

- A truly great success for the Samba project
- Windows desktops are still a reality
  - At least outside this room
  - And they need AD for management and authentication
- Samba's AD DC provides many complex services
  - Yet in a simple, seamless way
- Samba's first 'product' style feature

Samba AD DC Features

- LDAP
- Kerberos
- Windows Domain Controller
- Centralised Identity Management Server
  - Authentication
  - Authorisation
- SMB / SMB2 / CIFS
- Windows machines join AD natively

I think Samba's AD DC is a success

- Pushing users into the pit of success means:
  - Even if the software is complex
  - Even if the protocols are complex
  - Even if the needs of every site are different
  - That the initial install is a success

What is success: just working

- The initial install should just work
  - Answer some questions, and then add your first user
- Have all the details in the meantime taken care of
  - Generating any required configuration files
  - Scripting all the steps, leave no steps manual

What is success: security

- The initial install should be 'secure'
- Password policy should be on by default
  - Passwords should expire
  - Passwords should be complex
- The administrator shouldn't choose the machine keys (passwords)
  - These should be random gibberish
- Replication should be secure, encrypted

What is success: complexity

- Not shying away from complex protocols like Kerberos
- Hiding the details by making things 'just work'
- Making complex software simple to operate
  - Particularly when starting
- Not expecting the administrator to be an expert
  - Even if they are

This should not be revolutionary

- But too often, we assume the administrator:
  - Is an Identity and Security expert, and will add the security later
  - How many security bugs can you find below?

```
add: olcSyncRepl

olcSyncRepl: rid=0 provider=ldap://ldap01.example.com
bindmethod=simple binddn="cn=admin,dc=example,dc=com"
credentials=secret searchbase="dc=example,dc=com"
logbase="cn=accesslog"

logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"
schemachecking=on type=refreshAndPersist retry="60 +"
syncdata=accesslog
```

This should not be revolutionary

- But too often, we assume the administrator:
  - Is an Identity and Security expert, and will add the security later
  - How many security bugs can you find below?

```
add: olcSyncRepl

olcSyncRepl: rid=0 provider=ldap://ldap01.example.com

bindmethod=simple binddn="cn=admin,dc=example,dc=com"

credentials=secret searchbase="dc=example,dc=com"

logbase="cn=accesslog"

logfilter="(&(objectClass=auditWriteObject)(reqResult=0))"

schemachecking=on type=refreshAndPersist retry="60 +"

syncdata=accesslog
```

Are these not just motherhood statements?

- Because the alternatives are superficially easier
  - Yet dangerously simpler
  - With many guides leaving security as an afterthought
- Because asking the administrator to manually configure what we can script is a waste of everyone's time.

Impressive because of where we have come from

- I'll rag on the OpenLDAP / Samba pattern quite a bit
- A bit like arguing that PostgreSQL is wrong for not including the 'right' database schema
- OpenLDAP is **not** an Identity Management solution
  - But **no** commonly accepted IDM solution exists
  - And OpenLDAP / Samba **looks** like an IDM solution
- Many of the things I complain about **can** be done
  - But only by configuration of non-default modules

This may sound like a sales pitch

- I think Samba's AD DC has solved **some** of these problems very well
- This is at the expense of other things
  - Specifically performance
  - Also some flexibility
- I also have high praise for FreeIPA
  - Many of the same great patterns are there also
  - Very different products, but close communities

What have we done

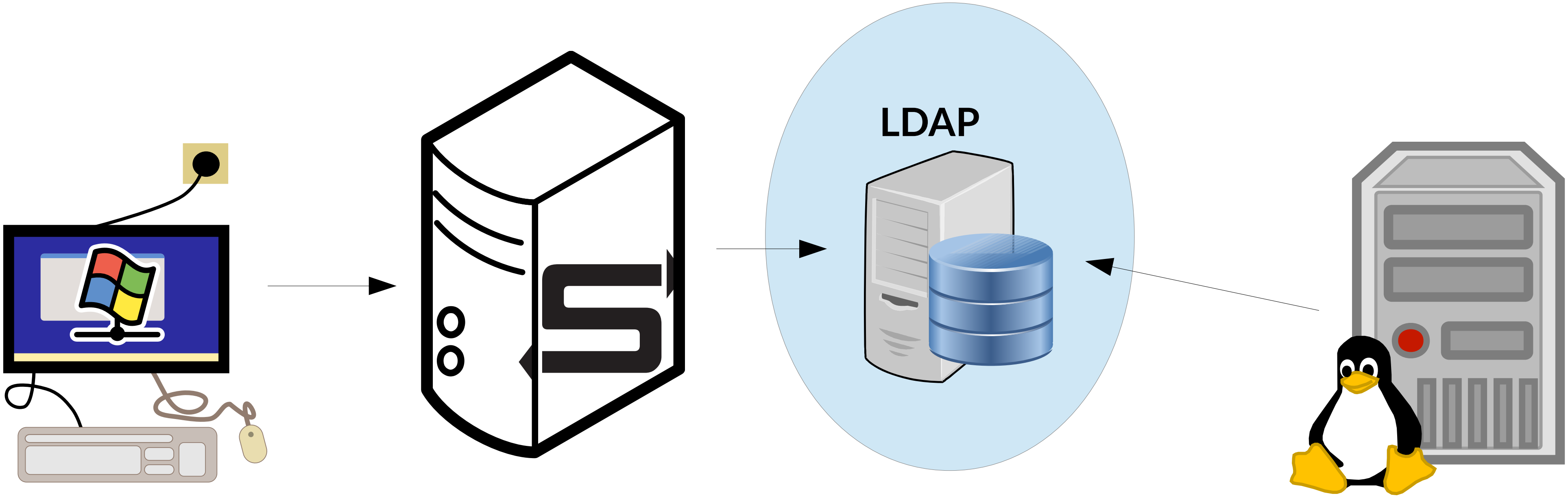
- We changed Samba's DC mode:
  - From a choose your own wiki adventure
  - Into a consistent reproducible pattern pattern
- We changed the constraints:
  - From allowing almost anything
  - To sensible and strictly defined constraints

What else we did

- We changed security:
  - From being optional and after the fact
  - To being on by default
- We changed replication from being
  - Hard to configure and easy to leave insecure
  - To being simple to configure
  - Sadly also really, really complex
    - OpenLDAP replication is much simpler under the hood

Samba 3.x and OpenLDAP

- A very common pattern
  - Samba stores users and groups in LDAP records
  - Essentially a NT4 Domain to LDAP translator



Samba 3.x / OpenLDAP Advantages

- LDAP backend provides replication 'for free'
- Solves key needs in heterogeneous networks
  - Windows workstations talk to Samba
  - Linux workstations and services talk to LDAP
- But only a loose pattern
  - Not a tool or script
  - No document of best practises
  - May not even provide a single password!

Integration

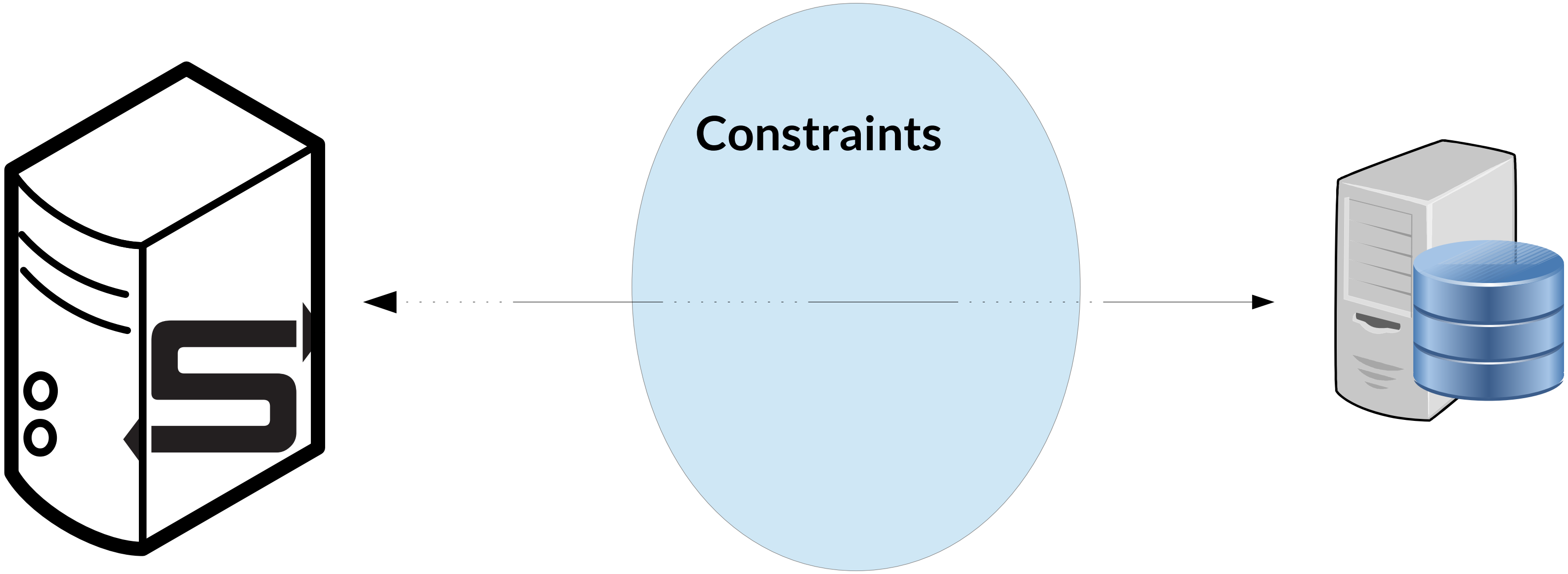
- Somebody Else's Problem?
- OpenLDAP is 'just' a data store
- Samba uses an externally managed LDAP store
- Lots of tools and modules you can use
  - But none installed or running by default
- Is the random wiki really in charge?
- Can we do better?

How bad is it really?

- Can't smart administrators
  - Collect the software
  - Follow internet guides
  - Customise for their own organisation?
- Succeed to:
  - Create a secure, reliable and fully featured IDM
  - Without great stress and inconvenience?
- Sadly NO

The missing Constraints

- Samba's AD DC enforces constraints
- In Samba / OpenLDAP constraints were typically 'somebody else's problem'



More than just constraints missing

- The typical wiki OpenLDAP Samba also misses:
  - Securing the LDAP directory
    - Default ACL is “to * by self write”
    - This allows you to update your own UID or SID!
    - Some guides often forget to secure the passwords!
  - Two-way password sync
    - Ensuring LDAP password changes change the Samba password too!
  - Password policy

Upgrading Samba 3 -> Samba 4

- Installing Samba 4.x is really easy
  - Install Samba
  - Samba-tool domain provision
  - Start Samba
- Upgrading Samba turns out to be much more difficult
  - It should have been 'samba-tool domain classicupgrade'
  - But our earlier flexibility came back to bite us

Given Infinite flexibility

- Our administrators used it all
- We had:
  - Duplicate SIDs
  - Mixed domains or Incorrect SIDs
  - Duplicate user names
  - Users with the same name as groups
  - Invalid account flags
  - Entries created by multiple, independent tools

Innovative Domains

- Other challenges included:
    - Administrator without the well-known SID
    - Invalid NetBIOS domains like myuni.edu
        - Not technically invalid, but highly discouraged
- Our admins used OpenLDAP well
    - Custom schema
    - Additional attributes

Classicupgrade becomes fsck

- With no previous 'check database for insanity' tool
- Administrators kept hitting strange errors
- We first have to tell them to clean up the source
- In the AD DC, we now have dbcheck

Not too bad in the end

- Some large domains took significant time to migrate
  - Some needed manual cleanup steps
  - Others needed 8 hours of CPU!
- We kept to our values:
  - Most of the fixes we automated
  - The upgrade process was script-able
  - The results were reproducible

Success for our users

- We strongly encouraged testing
  - On an independent network
- Many, many sites have migrated
  - Some quite large
- Very glad to be able to use modern windows out of the box
  - Eg Windows 7 and Windows 8

Things we could have done better

- Non-Samba data wasn't migrated
  - Initially no handling of POSIX attributes
    - Now we migrate some
- Other attributes have been left for the admin
  - Not even for compatible attributes
  - No schema migration
  - Had hoped users would have extended the script

We forgot that our most passionate users are POSIX-centric

- No distributed uid allocation (only RID allocation)
- No automatic provisioning of POSIX user attributes
- Winbindd on the DC
  - doesn't use LDAP uidNumber values by default
  - Doesn't use the LDAP unixHomeDirectory

Sysvol replication

- Still no SYSVOL replication in Samba AD DC
- Also no official workaround
- Development of the DFSR protocol
  - Difficult (needs new DCE RPC features)
  - Ongoing slowly

Simplicity: a development cost

- DNS kept on being the hardest part of the install
  - We forgot our rules, and asked the admin to manually configure
  - We gave the example config file, but it still caused trouble
- We wrote our own internal DNS server!
  - Simple
  - No caching
  - Reliably running without extra work

Lessons

- The key was the attitude change
- From kit of parts to product
- But admins still pushed off the cliff at the edge of support

Beyond Samba, Beyond Windows?

- See also FreeIPA
  - Based on 389 (ex Fedora DS, ex Netscape/Sun DS)
- OpenLDAP could still do the same
  - Great parts available for a non-AD solution
  - Needs to be scripted
  - Needs to be automated
  - Samba even has some of the code!

Samba Status update

- Samba 4.2 due soon
  - Finally End of life for Samba 3.6
- Improved security
  - DCERPC trailer signing, protecting key header info
  - Upgraded NETLOGON crypto
  - Winbind requires secure connections
    - Remove simple MITM attacks

File server

- SMB3 support a key feature
  - Leases (like oplocks)
- Snapper support
  - Previous file versions made easy
- Larger IO sizes in SMB2 reads and writes
- CTDB integrated into the tree
- vfs_fruit
  - Apple clients moving to SMB2

In the AD DC

- Bad Password Lockout
  - Writing this found a security hole in windows!
- Now uses the common winbindd
  - Deprecate the attempted rewrite
  - Now just re-uses the file server code with plugins
- Finished the smb.conf merge
  - No longer conflicting 'loadparm' tools

TODO on the AD DC

- Inter-forest trusts
  - Recent work on trusts to FreeIPA quite successful
- Subdomain support
- Performance
  - Our performance isn't great at massive scale
  - Experimental effort to (again) use OpenLDAP
    - But auto-configured this time
- POSIX Integration

Catalyst's Open Source Technologies

Interested in working for Catalyst on Samba? Catch me in the hallway track

Questions