An OpenLDAP backend for Samba

The road so far, and a new way forward

Nadezhda Ivanova
Software Engineer @ Symas

symas

About Samba4

- Combines the file sharing service of Samba with a fully AD compatible Domain controller
- Can be a standalone Domain Controller
- Can join an existing Windows Active Directory domain as a member server, or an RODC
- Supports all FSMO roles
- Domain member machines running Windows work with Samba4 transparently
- Management can be done both with samba-tool and by installing Microsoft's RSAT (Remote Server Administration Tools) on a Windows machine.

symas

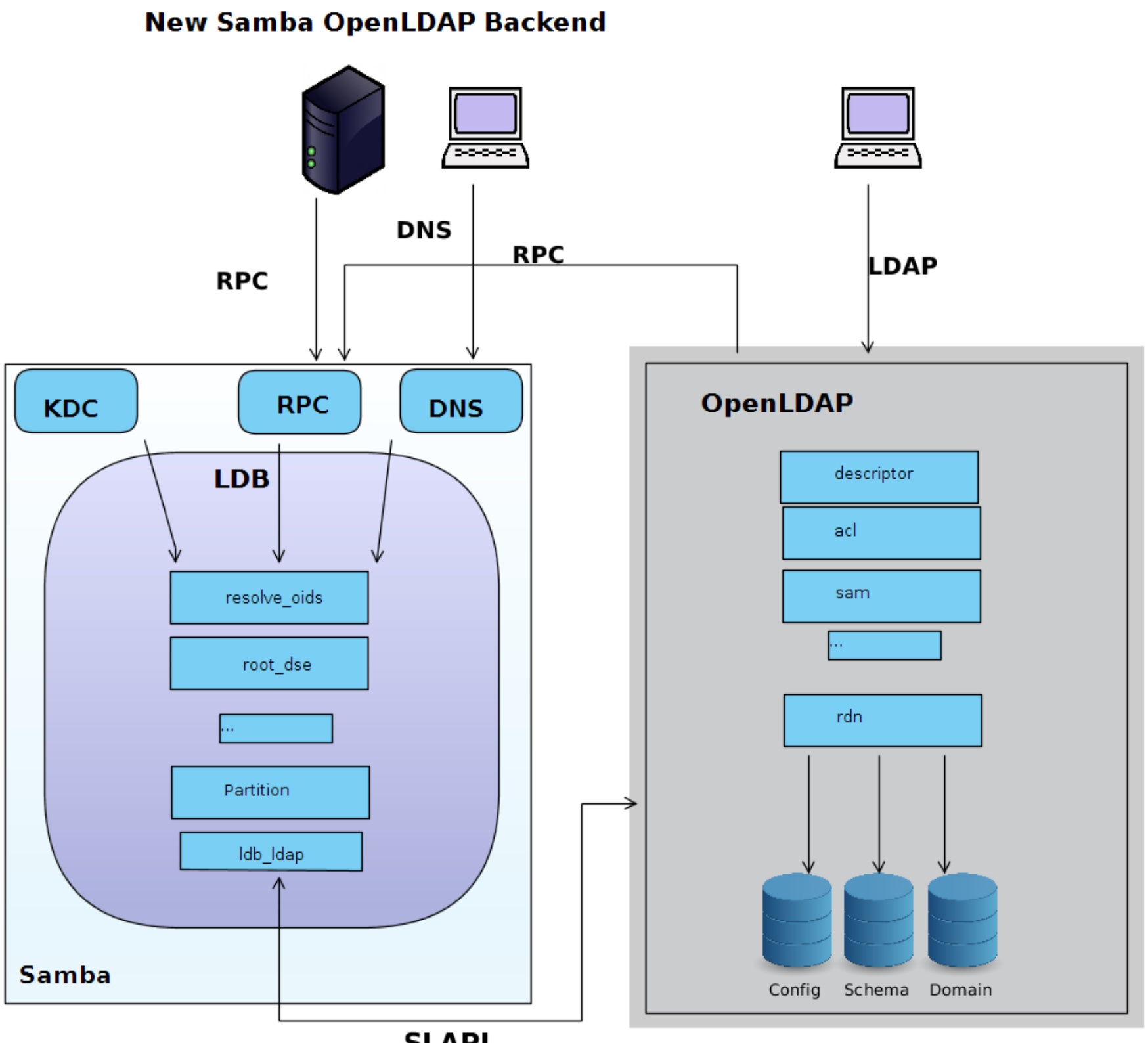
About Samba4

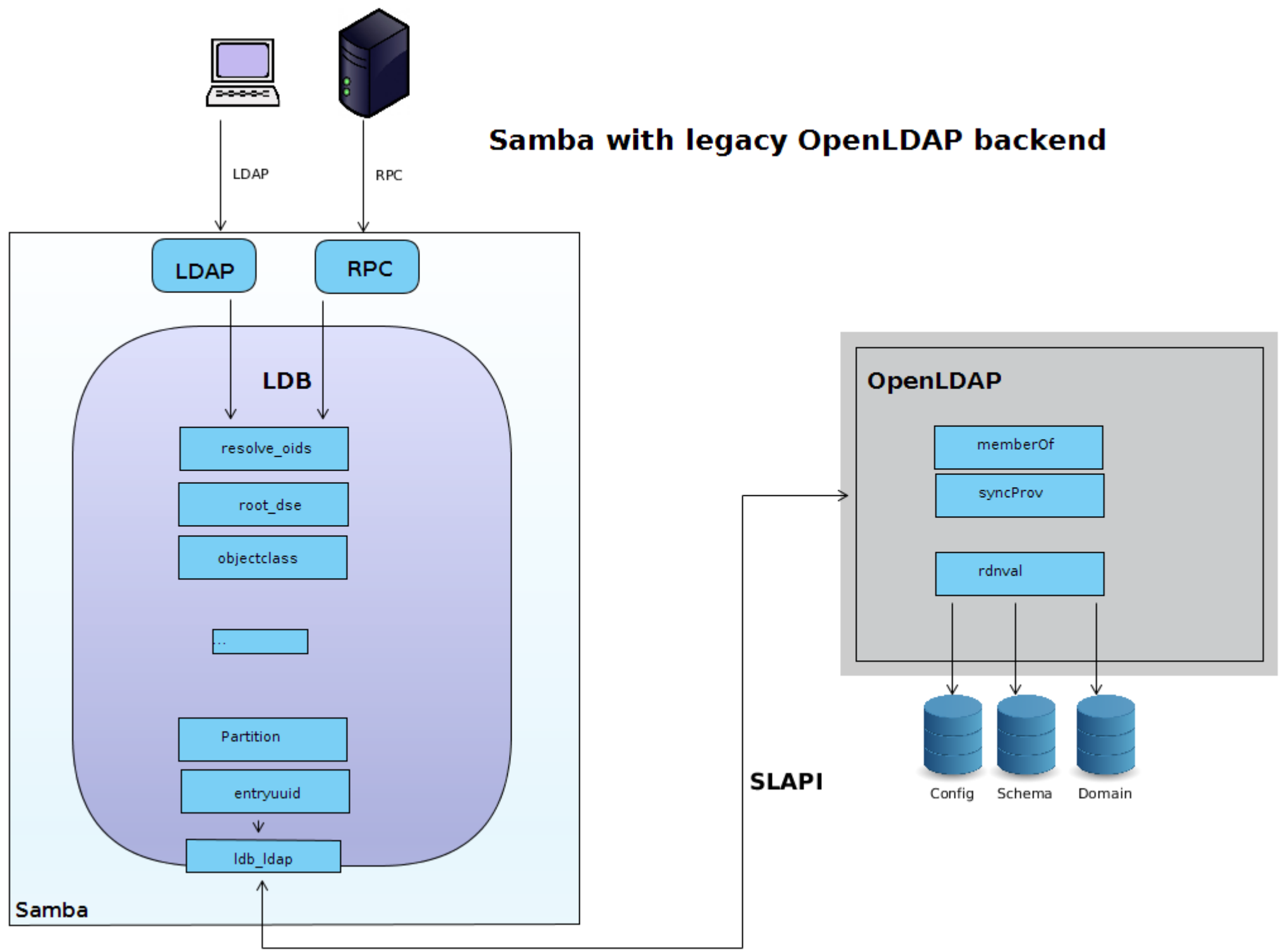
- Released in 2013 after more than 10 years in development
- New releases added every 6-9 months
- Successfully deployed by small to mid-sized companies
- Functionality is developed as separate LDB modules, similar in structure to OpenLDAP overlays
- Has its own internal DNS server, or can work with BIND9 using a BIND_DLZ module.
- Has its own Kerberos KDC
- Used to have an OpenLDAP back-end, which got retired due to lack of resources and technical difficulties

symas

A new back-end for Samba 4

- Integrate Samba 4's AD implementation with the speed and scalability of OpenLDAP
- Samba 4 (used to) have a built-in size limitation due to use of TDB
- Samba 4 (used to) have a slow LDAP service.
- An attempt was made to implement an OpenLDAP backend


New Samba OpenLDAP Backend
DNS
RPC
RPC
LDAP
KDC
RPC
DNS
LDB
resolve_oids
root_dse
...
Partition
ldb_ldap
Samba
OpenLDAP
descriptor
acl
sam
...
rdn
Config
Schema
Domain
SLAPI


Samba with legacy OpenLDAP backend
LDAP
RPC
LDAP
RPC
LDB
resolve_oids
root_dse
objectclass
...
Partition
entryuuid
ldb_ldap
Samba
SLAPI
OpenLDAP
memberOf
syncProv
rdnval
Config
Schema
Domain

symas

Implementation approach

- We started by using the legacy back-end and replacing individual modules
- But:
  - Samba modules are interconnected and often communicate with each other via internal controls
  - They rely on being executed in a specific order, and not all of them can be removed
  - Sometimes RPC traffic is initiated from inside a module, e.g samldb and replmetadata

symas

Where did we get?

- Secdescriptor overlay
  - Collects the necessary data – parent SD, default security descriptor.
  - Calculates the new descriptor using some Samba library functions and adds it to the new entry.
  - Recalculates the SD's of the modified object and all of its children.
  - Handles the sDFlags control

symas

A new back-end for Samba 4 - Reloaded

- Switch to separate implementation of functionality within OpenLDAP, with manual testing via OpenLDAP directly, until LDAP behavior is as desired
- Use Samba's provisioning script to populate a database, than rely on that to gradually add functionality to OpenLDAP
- Determine how and if to remove or modify Samba modules later, after RPC tests

symas

But...

- Samba does not stand still, and it is hard to keep up
- Samba switched to a multi-process model
- Samba implemented (and made default) an LMDB back-end
- Changes to LDB broke the ability to provision the legacy OpenLDAP back-end

symas

Where did we get?

- ad_schema overlay - registers the attributeSchema and classSchema attributes in OpenLDAP schema
  - Maps the AD style syntax to LDAP syntax
  - creates schema definition for the class or attribute that is registered in OpenLDAP schema
  - Adds the additional schema data to the expanded AttributeType and objectClass data
  - If the attribute is indexed, creates an index value for it in cn=config
  - If the attribute is linked, creates a memberOf configuration entry
- Objectguid overlay - constructs and adds the objects':
  - GUID – a randomly generated unique identifier got the object
  - SID – Security Identifier of a security principal.
  - InstanceType
  - WhenCreated, whenChanged

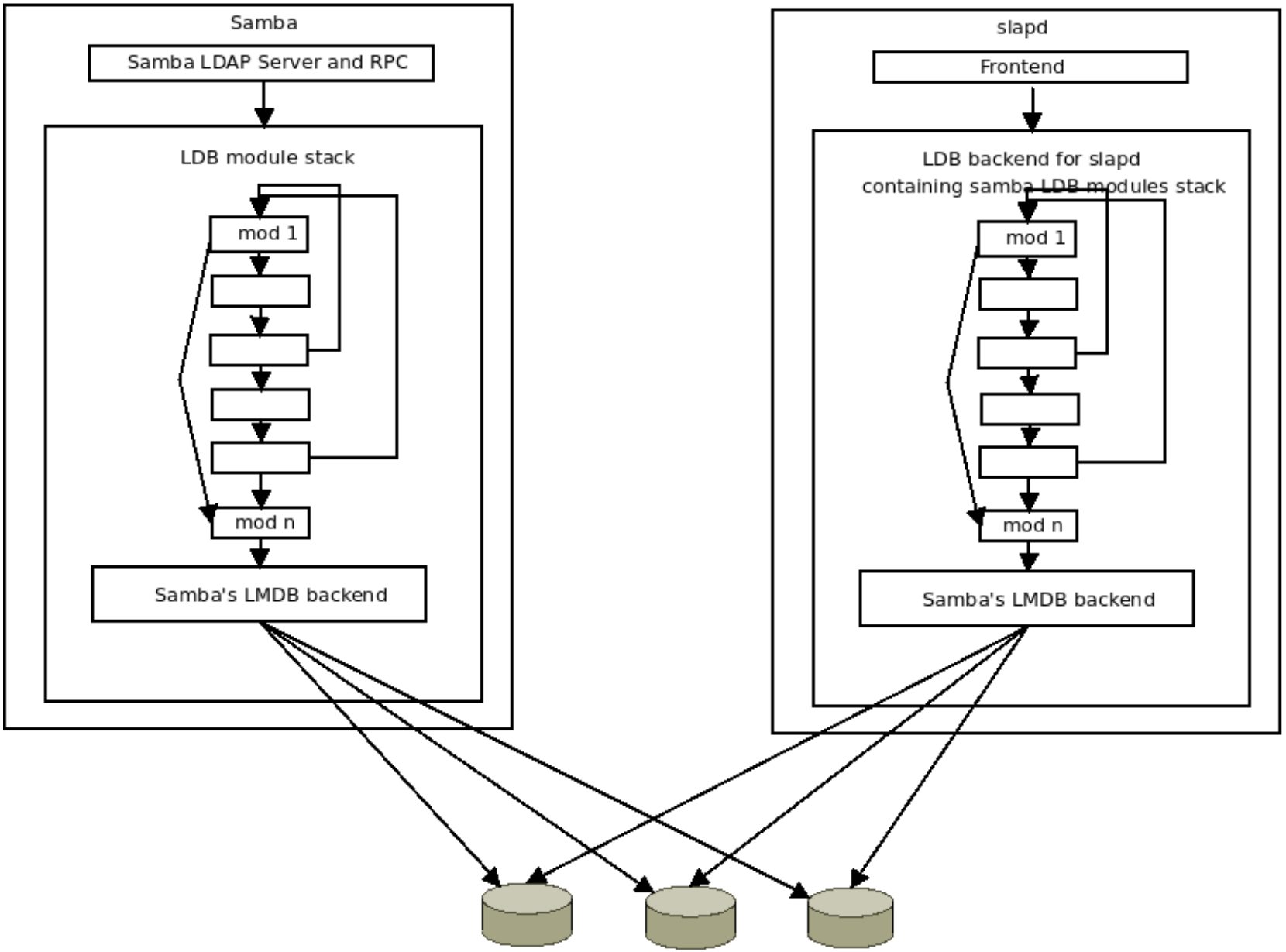
symas

A new back-end for Samba 4 - Revolutions

- Integrate the LDB module stack as an OpenLDAP backend
- Re-factor the LDB stack so that modules become truly independent
- Develop he ability to wrap LDB modules inside overlays, tuning the LDB stack into an overlay stack, while still using Samba code

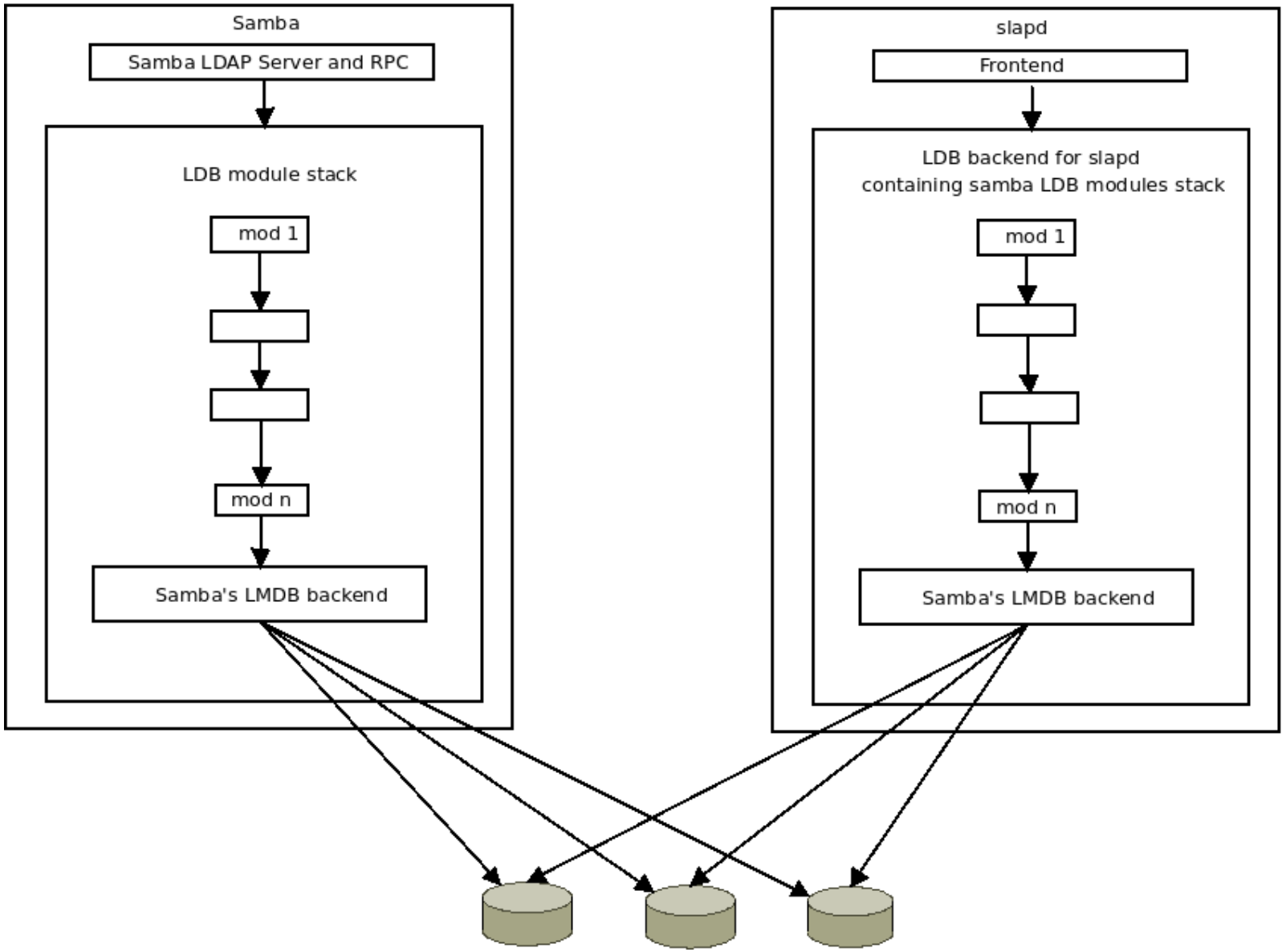
symas

Step 1


Samba
Samba LDAP Server and RPC
LDB module stack
mod 1
mod n
Samba's LMDB backend
slapd
Frontend
LDB backend for slapd
containing samba LDB modules stack
mod 1
mod n
Samba's LMDB backend

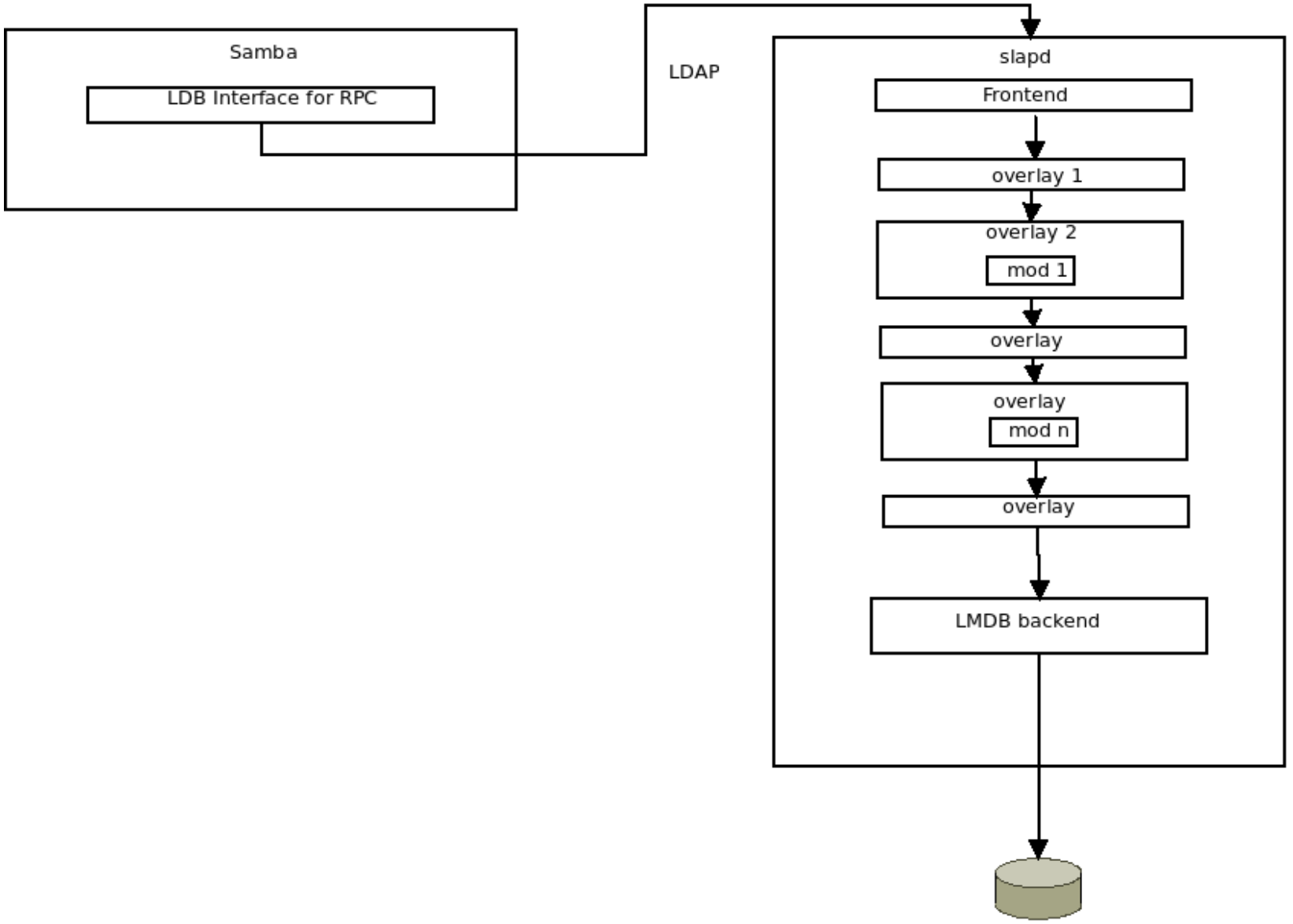
symas

Step 2


Samba
Samba LDAP Server and RPC
LDB module stack
mod 1
mod n
Samba's LMDB backend
slapd
Frontend
LDB backend for slapd
containing samba LDB modules stack
mod 1
mod n
Samba's LMDB backend

symas

Step 3


Samba
LDB Interface for RPC
LDAP
slapd
Frontend
overlay 1
overlay 2
mod 1
overlay
overlay
mod n
overlay
LMDB backend

symas

Why now?

- Samba has an LMDB backend
- Some serious performance improvements in Samba
- Work on Samba is an a stage where there is a will and some resources to assist us with refactoring

symas

Why at all?

- It will lead to a much better integration of OpenLDAP and Samba
- Until we move on to rewriting the LDB modules as overlays, we will be able to collaborate with the Samba Team in the support of the code
- We will be able to deliver a use-able solution faster
- Users will be able to use new Samba features faster
- But...

symas

symas

The agents Brown, Smith and Jones

- LDB is not (and was never meant to be) thread-safe
- Incorporating and linking all this code will be a challenge
- Extensive work will be necessary to re-factor the LDB modules
- Surprises…

symas

We will do it anyway

symas