It's ALIVE!

Samba 4 with OpenLDAP Backend

Nadezhda Ivanova (nivanova@samba.org)

SambaXP 2014

About us

- Symas – www.symas.com

- And me
  - Involved on and off in Samba 4 since 2008
  - Currently developer at Symas

What happened to the OpenLDAP Backend

- OpenLDAP limitations
  - No transactions
  - Difficult to “break” the standard
- No resources or people

So, why now?

- Samba4 stable releases
- OpenLDAP – transactions, lmdb
- Renewed interest in the community
- Involvement from the OpenLDAP team

OpenLDAP

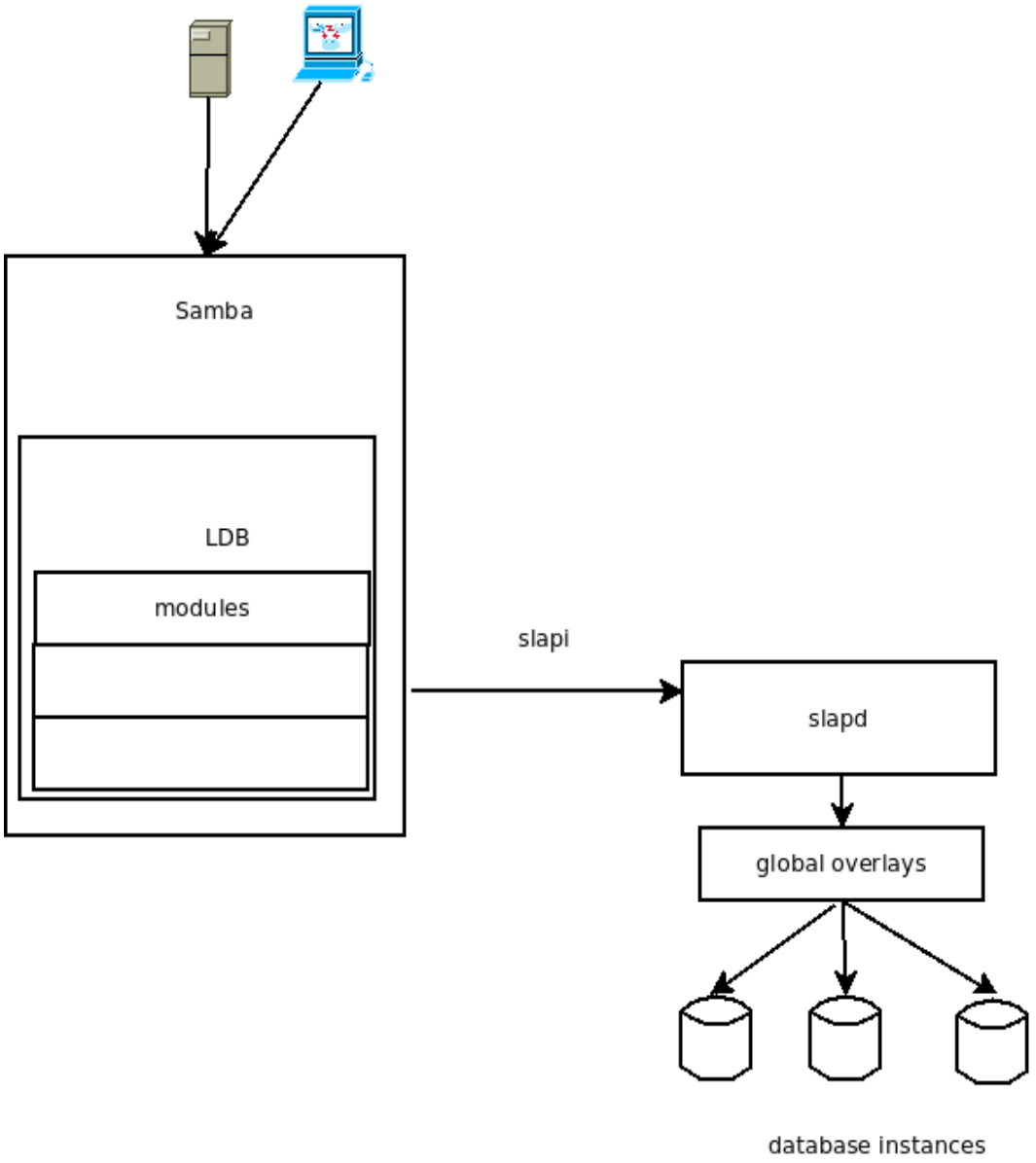
- Mdb is default backend since version 2.4
- Allows support for transactions
- OpenLDAP with mdb is much faster that OpenLDAP with hdb
- Flexibility of configuration – overlays, mixed db types, etc.

The art of necromancy

- Digging out the docs (https://wiki.samba.org/index.php/Samba4/LDAP_Backend/OpenLDAP)
- Restoring provision options

  (TEST_LDAP=yes samba-tool domain provision –realm=samba.example.org --domain=samba --host-name=myhost --adminpass=SecR3t --root=root --server-role="domain controller" --ldapadminpass=secret --ldap-backend-type=openldap --slapd-path=/usr/local/libexec/slapd)
- Bugfixing

Legacy OpenLDAP backend



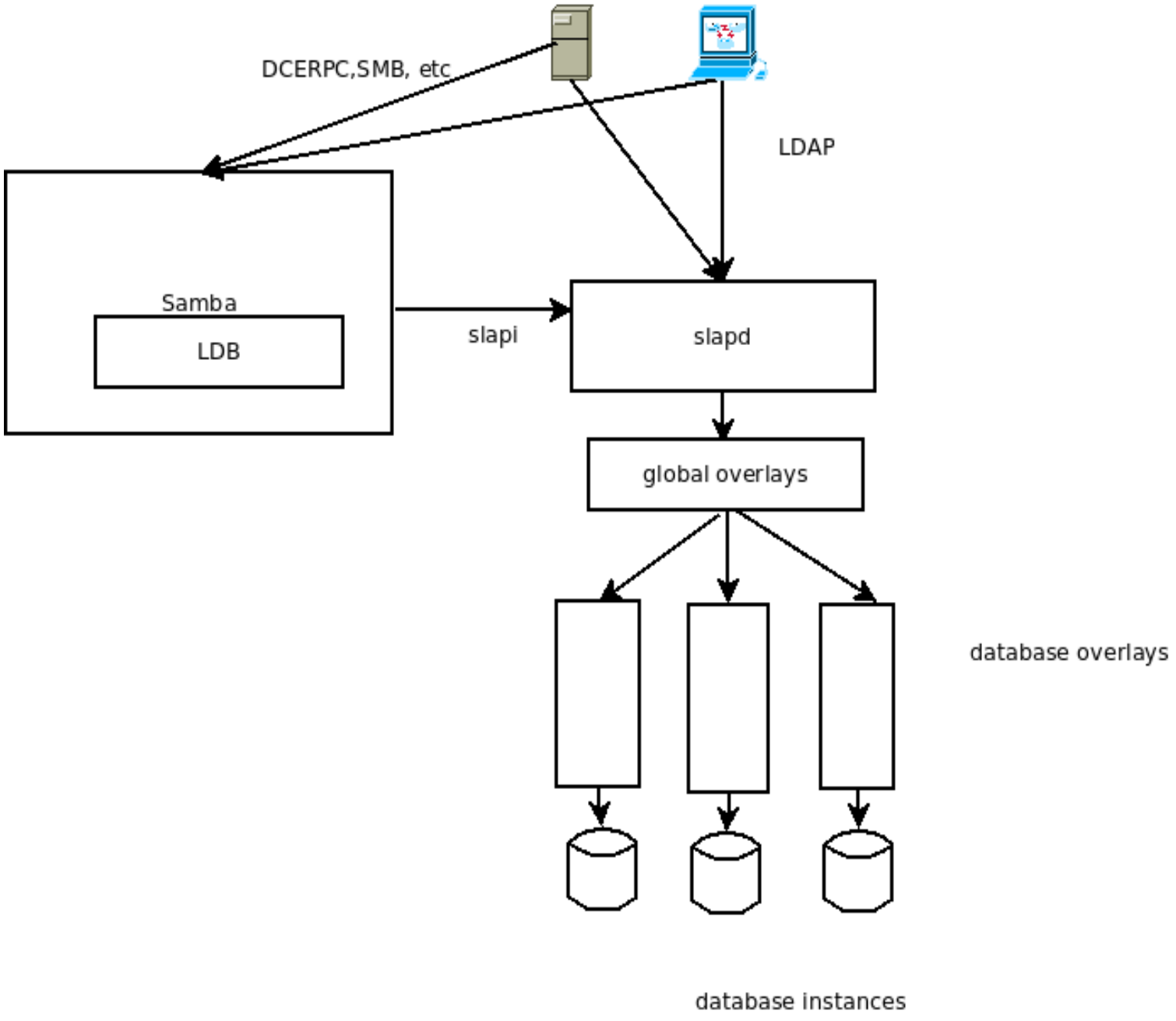
slapd.conf

```
##########################################
### cn=schema ###
database        hdb
suffix    ${SCHEMADN}
rootdn          cn=Manager,${SCHEMADN}
directory  ${LDAPDIR}/db/schema
${NOSYNC}
${INDEX_CONFIG}
maxsize 1073741824

#syncprov is stable in OpenLDAP 2.3, and available in 2.2.
#We need this for the contextCSN attribute and mmr.
overlay syncprov
syncprov-sessionlog 100
syncprov-checkpoint 100 10
overlay rdnval


### Multimaster-Replication of cn=schema Subcontext ###
${MMR_SYNCREPL_SCHEMA_CONFIG}
${MIRRORMODE}
```

The new monster

- We want the fastest AD compatible LDAP Server, to be achieved with symbiosis between OpenLDAP and Samba4
- Standard LDAP behavior will not be supported concurrently with AD compatibility on the same server
- This is not a work on the classic Samba3/OpenLDAP domain

Anatomy of the new monster



slapd.conf

```
#############################################
### cn=schema ###
database        mdb
suffix${SCHEMADN}
rootdn          cn=Manager,${SCHEMADN}
directory ${LDAPDIR}/db/schema
${NOSYNC}
${INDEX_CONFIG}
maxsize 1073741824
delay-checks on
#syncprov is stable in OpenLDAP 2.3, and available in 2.2.
#We need this for the contextCSN attribute and mmr.
overlay syncprov
syncprov-sessionlog 100
syncprov-checkpoint 100 10
overlay syntax_checks
overlay samba4_schema
samba4-initial-schema /usr/local/samba/share/setup/olschemadata.ldif
samba4-initial-prefixmap /usr/local/samba/share/setup/prmap_ol.ldif
samba4-schema-dn ${SCHEMADN}
overlay show_deleted
overlay rdnval
overlay secdescriptor
overlay instancetype
overlay operational
```

First steps

- Removing modules from LDB and reimplementing as overlays
- Dependencies and order preserved for the time being, but changes and restructuring may be needed in the future
- Samba Internal controls can me implemented in OpenLDAP amd restricted to the slapi connection type

Bits and pieces

- Libcli/security – for SD and access checks
- dsdb_schema – for pretty much everything
- misc

```
	get_parent_sd(op, rs, &(instance_attribute->a_vals[0]), &parent_sd);
	get_schema_sd_info(...);
	schema = get_samba_schema();
	dsdbclass = dsdb_class_by_lDAPDisplayName(schema,
objectclass_attribute->a_vals[objectclass_attribute->a_numvals-2].bv_val);
	secdesc_attribute = attr_find( op->ora_e->e_attrs, secdesc_descr);
	if ( secdesc_attribute != NULL) {
		if (secdesc_attribute->a_numvals !=1) {
			send_ldap_error( op, rs, LDAP_CONSTRAINT_VIOLATION,
					"Incorrect read of attribute nTSecurityDescriptor" );
			return rs->sr_err;
		}
		user_descriptor.data = (uint8_t *)secdesc_attribute->a_vals[0].bv_val;
		user_descriptor.length = secdesc_attribute->a_vals[0].bv_len;
		user_descriptor_ptr = &user_descriptor;
	}
	partition = get_partition_flag(op);
	DATA_BLOB *final_sd = security_descriptor_ds_create_as_blob(talloc_mem_ctx,
							sec_token,
							domain_sid,
							dsdbclass->defaultSecurityDescriptor,
							schemaIDGUID,
							parent_sd,
							user_descriptor_ptr,
							NULL,
							partition,
SD_SECINFO_OWNER|SD_SECINFO_GROUP|SD_SECINFO_SACL|SD_SECINFO_DACL,
							&as_sddl);
```

Future experiments

- Authentication – possibly making OpenLDAP use samba gensec and libcli/auth
- DSR replication and dirsync (repl_meta_data, dirsync)