Integrating OpenLDAP and Samba Active Directory in Univention Corporate Server

LDAPCon 2017

Arvid Requate

Univention GmbH

univention

Agenda

1. Introduction: Whom I work for
2. OpenLDAP and Active Directory in Univention Corporate Server (UCS)
3. LDAP Synchronization
4. Solved Challenges
5. Future direction

Univention GmbH

- Producer of the enterprise Linux distribution Univention Corporate Server (UCS)
- Identity and Access Management
- Founded in 2002, offices in Bremen, Berlin and Seattle
- 45 employees

Installation Footprints

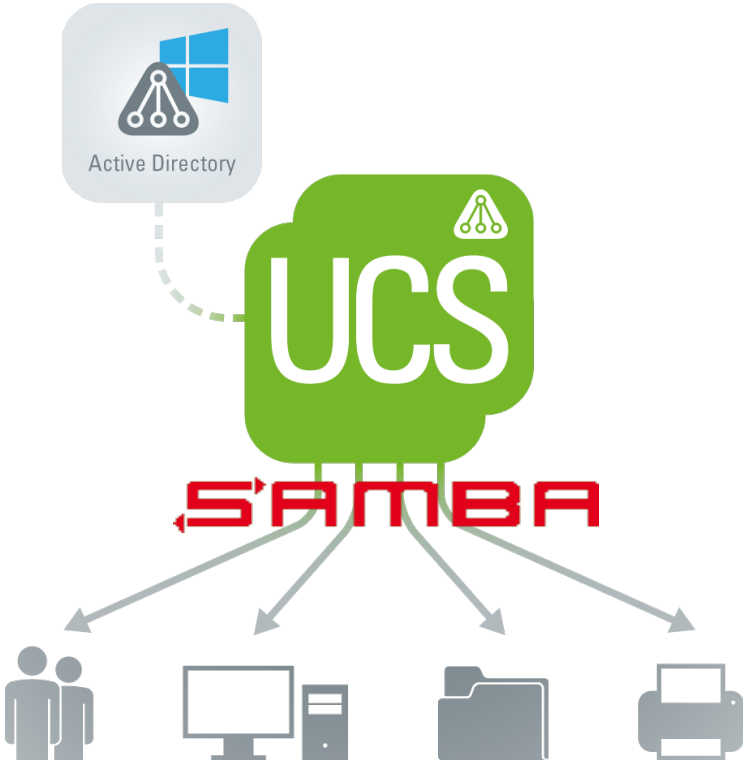
- One customer with 30M authentication / email accounts
- One customer with 70k Samba / Active Directory accounts,
  not all users in generic groups like *Domain Users*
- Another with 30k Samba / Active Directory accounts
- Down to small to medium size business customers

Univention Corporate Server (UCS)

- Debian based Linux distribution with Microsoft-like domain concept, 100% open source (AGPL v3)
- Web-based management interface
- HTTP- and Python-API
- Main backend: OpenLDAP
- Samba Active Directory Services for Microsoft Windows Clients & Servers
- A lot of third party services

UCS & Active Directory Services

- Active Directory Domain Control and Services for Windows Clients
- LDAP Service with AD semantics on port 389
- Obstacle I: Differing LDAP Schemata OpenLDAP vs Active Directory
- Obstacle II: Differing LDAP server implementations, metadata etc.



OpenLDAP Replication in UCS

- **Single-master** configuration
- Replication via custom “listener/notifier” mechanism (C + Python modules)
- Custom “translog” OpenLDAP overlay a bit like the accesslog overlay
- **Selective replication** via ACLs
- Port 7389 / 7636 only if Samba/AD is present

Samba 4 / Microsoft Active Directory Replication (DRS)

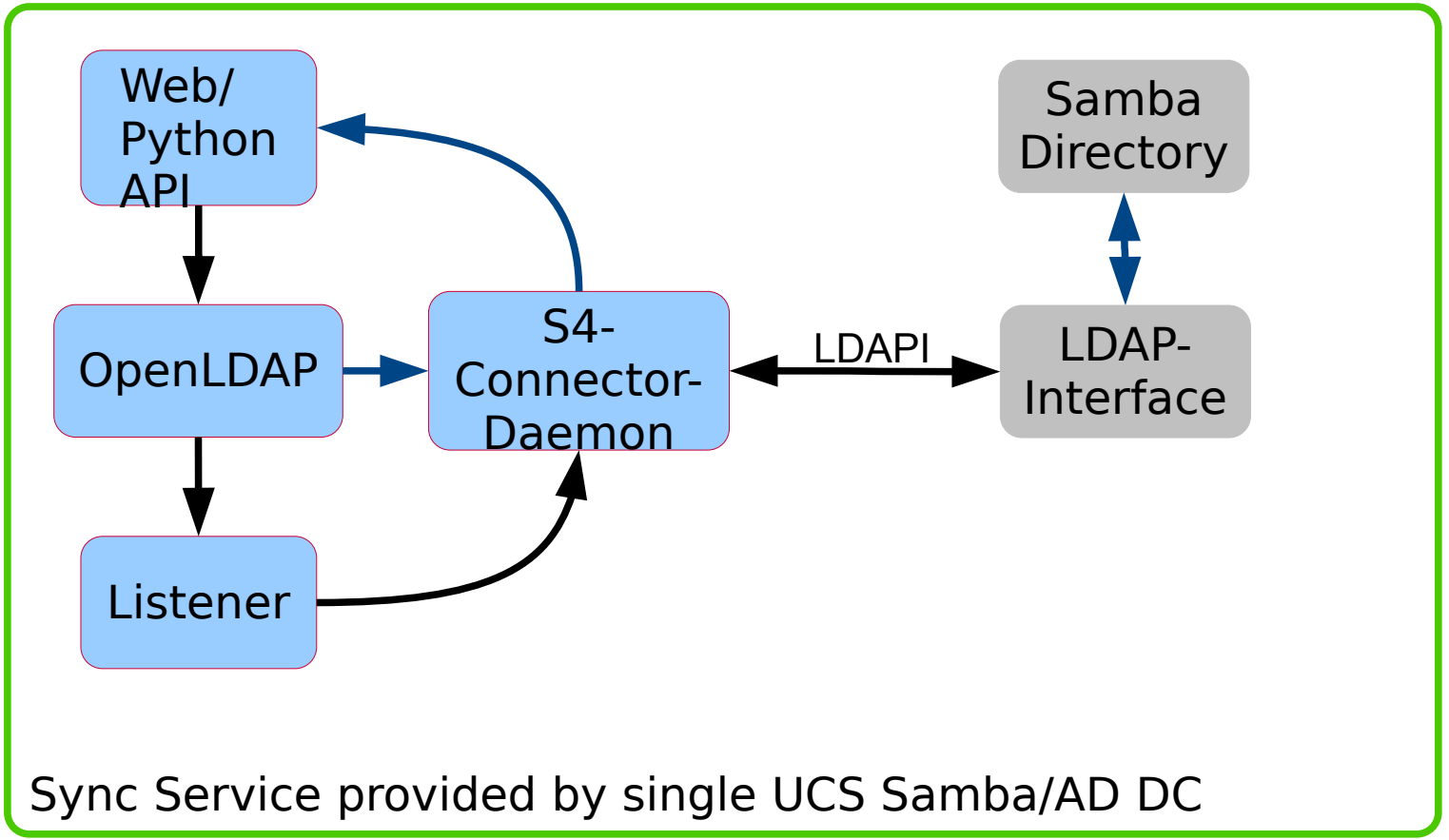
- **Multi-master** operation
- Replication between Domain Controllers via Microsoft DRS protocol
- Full mesh or structured into “sites“

- **F**lexible **S**ingle **M**aster **O**peration roles:
  - Master for Account-IDs (RID pools)
  - Schema master
  - ...
- Not much support for selective replication

Bridging the worlds: Univention S4 Connector

- Originally implemented to replicate user and group objects between pre-existing native Microsoft Active Directory (AD) Domains and UCS / OpenLDAP
- Re-invented to synchronize Samba/AD with OpenLDAP inside of a UCS domain controller (including Kerberos hashes)

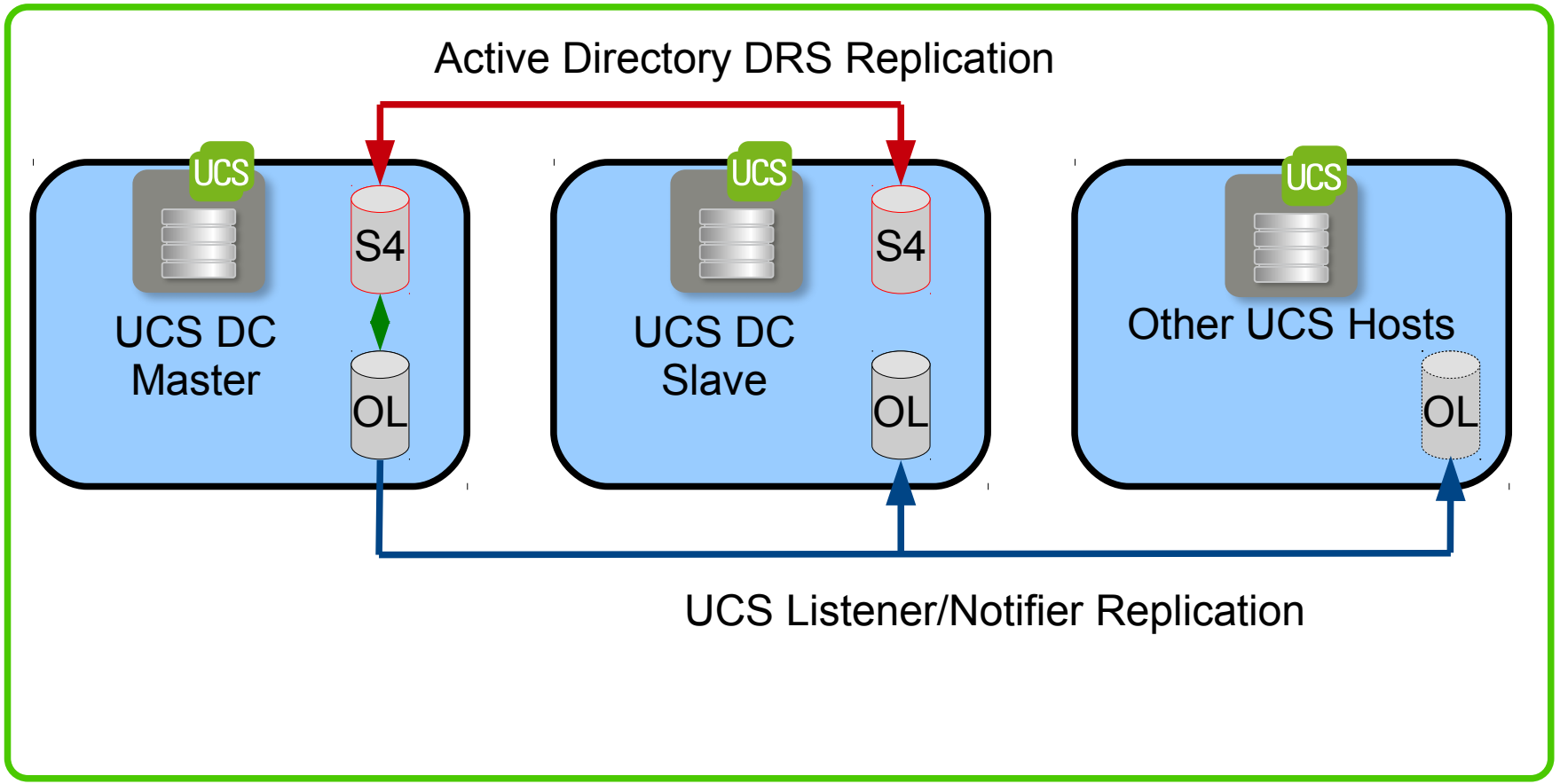
Bridging the worlds: Univention S4 Connector



Bridging the worlds: Univention S4 Connector

- Single point of transition between single-master OpenLDAP and multi-master Samba / Active Directory
- In specialized products (UCS@school) we use OpenLDAP as information bus between separate Active Directory Controllers, using OpenLDAP ACLs to implement selective replication

Bridging the worlds: Univention S4 Connector



Update tracking: Active Directory

- Active Directory:
  - State based replication, not diff based
  - Each Domain Controller maintains

    per change *uSNChanged* attribute (update sequence number)
  - per **attribute version numbers**, timestamps and USNs in *replPropertyMetadata*

- plus Linked Value Replication (LVR), e.g. for member/memberOf:
  - *msDS-ReplValueMetaData*

Update tracking: OpenLDAP

- OpenLDAP:
  - **per object** *entryCSN*
  - Optional: accesslog **diffs** (e.g. for delta-syncrepl)
  - No attribute level metadata

- Some applications using OpenLDAP implement their own attribute timestamps
  - *shadowLastChange*
  - *sambaPwdLastSet*
  - *krb5KeyVersionNumber*

UCS LDAP Replication

- Univention specific addon: Translog overlay for OpenLDAP:
  - Logging **per change** Notifier-ID (like *uSNChanged*)

- Listener process reacts on changes, calls Python modules for replication
- Listener cache (LMDB, hurray!) - passes cached and current LDAP object state
  - attribute level diff

- One of the consumer modules: “S4-Connector“
- S4-Connector translates schema differences, values, positions, ...
- Diffs Samba/AD object against changed OpenLDAP attributes → ldapmodify Samba/AD

S4-Connector replication: ping pong

- Bidirectional synchronization: Asynchronous polling of both sides
  - Notifier-IDs change → Sync to Samba/AD
  - *highestCommittedUSN* change → Sync to OpenLDAP
- Eventual convergence
- Ok: Several “trivial” issues and corner cases to work around, like schema mapping, value marshalling, group membership replication, Deleted Objects

Example: S4-Connector replication concurrency conflict

1) Windows Admin running GUI tool working on Samba/AD

2) Click → Write to Samba/AD

3) S4-Connector sync to OpenLDAP

4) Race condition:
   - S4-Connector detects change in OpenLDAP
     → Sync back to Samba/AD
   - User clicks again → Write to Samba/AD

Fixing S4-Connector replication concurrency

- Active Directory Replication (DRS) avoids this by *Propagation Dampening*
  - Each LDAP server maintains an “Up-to-dateness-vector” of *uSNChanged* values to avoid sending obsolete updates (attribute level filtering)

- Workaround: The S4-Connector can track the *entryCSN* of own writes to OpenLDAP
  So we can ignore them on the way back to Samba/AD LDAP
  - Using Post-Read LDAP Control (RFC 4527) to avoid TOCTTOU issues

- We use this and it helps a lot, but: OpenLDAP only

Directions: How to improve from here?

- Two complementary options:

1) Implement Post-Read LDAP Control (RFC 4527) for Samba/AD LDAP
   - Probably we need to do this first

2) More metadata detail → finer change granularity
   - Object level → attribute level
   - reduced conflict surface
   - decidability

OpenLDAP Metadata

» Object level:

```
dn: uid=user1,cn=users,dc=ar41i1,dc=qa
entryUUID: ee0bf7d6-1d33-1037-9e97-3bb60a8becb2
createTimestamp: 20170824162046Z
modifyTimestamp: 20170824162332Z
creatorsName: cn=admin,dc=ar41i1,dc=qa
modifiersName: cn=admin,dc=ar41i1,dc=qa
entryCSN: 20170824162332.083696Z#000000#000#000000
```

Active Directory Metadata

» Object level →

```
dn: CN=user1,CN=Users,DC=ar41i1,DC=qa

objectGUID: 7f82f70c-1247-4846-bf49-a72447c704c1

whenCreated: 20170824162050.0Z

whenChanged: 20170824162332.0Z

uSNCreated: 3996

uSNChanged: 4002
```

» Attribute level →

```
replPropertyMetaData::
AQAAAAAAAAAaAAAAAAAAAAAAAAAABAAAA4o2vDwMAAADsNYL/lTN+QK2
LYeclOEzgnA8AAAAAAACcDwAAAAAAAMAAAACAAAAhI6vDwMAAADsNY
L/lTN+QK2LYeclOEzgoA8AAACcDwAAAAAAA==
```

Active Directory Attribute Metadata

Attribute level →

```
dn: CN=user1,CN=Users,DC=ar41i1,DC=qa
replPropertyMetaData: array: ARRAY(26)
  element(1): struct replPropertyMetaData1
    Attid                    : DRSUAPI_ATTID_objectClass
    Version                  : 0x00000001 (1)
    originating_change_time  : Thu Aug 24 18:20:50 2017
    originating_invocation_id: ff8235ec-3395-407e-ad8b-61e725384ce0
    originating_usn          : 0x0000000000000f9c (3996)
    local_usn                : 0x0000000000000a3f (2623)
```

Attribute level versioning in OpenLDAP?

- Pro: enables attribute level state comparison between Samba/AD and OpenLDAP
- Pro: provide basis for attribute level conflict resolution in multi-master syncrepl setups
- *replPropertyMetaData* attribute would be a precondition for DRS replication between OpenLDAP and Samba/AD LDAP
- Example: `contrib/slapd-modules/samba4/vernum.c` for *msDS-KeyVersionNumber*

Questions? Feedback?

Thank you!

Thanks to the
OpenLDAP maintainers!

Univention is hiring!

:-)

Contact information

Univention GmbH
Bremen Germany
+49 421 222 32-20

Arvid Requate
requate@univention.de
+49 421 222 32-52
www.univention.com

Univention North America
Boston, MA, USA
+1 781 968-5492