univention

univention
linux for your business

Experiences of 1.5 Years of Samba 4 in the Field

SAMBA

Göttingen, May 16th 2013

Arvid Requate <requate@univention.de>

Agenda

- Introduction: Whom I work for.. What we do..
- Milestones of Samba4 integration into our products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SAMBA

UCS Univention Corporate Server

Agenda

- Introduction: Whom I work for.. What we do..
- Milestones of Samba4 integration into out products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SAMBA

UCS Univention Corporate Server

About Univention

- Main product: Univention Corporate Server

  Linux distribution with a domain concept and management
- Specialized solutions like UCS@school
- Selling product licenses and service (customizations etc.)
- 40 employees
- based in Bremen, Germany

univention

Univention Corporate Server

- Debian based Linux Distribution, 100% OpenSource / AGPL3, offering a Microsoft-like domain concept
  - Samba 3/NT and Samba 4/AD Windows Domain Control
  - Backed by OpenLDAP Directory Services
  - Identity Management via Web interface and Python/CLI API
  - Domain Services – DNS, DHCP, NTP, PKI, Proxy, Mail, Virtualization, etc.

univention

debian GNU/Linux

UCS Univention Corporate Server

UCS@school

- Specialized solution for distributed branch site requirements of school departments:
- selective replication to the branch sites.

univention

debian GNU/Linux

UCS » @school

Agenda

- Introduction
- Milestones of Samba4 integration into our products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SAMBA

UCS Univention Corporate Server

Milestones

- Initial Product Release UCS 3 feat. Samba4/AD Domain Contol
  Dec, 2011
- Integration into UCS@school (feat. selective replication)
  June, 2012
- C't Computer Magazine Edition (AD/SBS Takeover Solution)
  Dec, 2012
- Release of UCS 3.1 with Samba4 ~rc6 one day before official 4.0 release
  same month
- Update to official Samba 4.0.3
  Feb, 2013

univention

UCS Univention Corporate Server

First Enterprise Linux Distribution integrating Samba4

- UCS 3.0 released on Dec, 12th 2011 one year before 4.0
- Based on Samba 4 Alpha17 + upstream git patches
- OpenLDAP as primary management backend
- Bidirectional Sync with Samba4 (Univention S4 Connector)
- Fruitful collaboration with Stefan Metzmacher @ SerNet for Password-Hash and Kerberos-Ticket Sync and file+print integration.
- „Franky“ style approach for file+print: samba + smbd & nmbd

univention

UCS Univention Corporate Server

Features of First Release

- Managing Samba Accounts and DNS records via Univention Directory Manager (Web Interface / python) as well as with AD Users and Computers
- Multi-DC operation (DC function level 2008R2)
- rsync/Cron-based sysvol replication
- GPO administration as Administrator only
- DDNS updates against Bind9 backend
- No SNTP time sync
- Schema updates disabled by default

univention

UCS Univention Corporate Server

First Productive UCS3/Samba4 Site

- Landtag Brandenburg (as early as Feb. 2012) with a couple of Samba 4 DCs and Samba 3 fileservers.
- Customer-Experience Presentation at CeBIT 2012, March
- Generally positive feedback, despite some issues, e.g.
  - One single machine account lost all objectclasses, probably due to some replication collision → ntp_signed segfault
  - Segfault in the Directory-ACL code due to missing „dnsdomain“
  - Excessive memory consumption of drepl and rpc_server
  - Samba-tool drs showrepl quite flakey

univention

Selective Replication for UCS@school

- UCS@school 3.0 released on June, 5th 2012
- Still based on Samba 4 Alpha17 + even more patches
- Emphasis on OpenLDAP replication as primary „bus“
- Allowing selective replication filtering via LDAP-ACLs
- Not possible with DRS
- Concept of so called „Slave PDCs“ ported from UCS 2.x/Samba3 to the new world of UCS 3.x/Samba4

UCS c't-Edition: Samba4 AD Takeover

- Dec, 3th 2012: Issue 26/2012 of the german computer magazine c't, large audience.
- Targeted at conversions of Microsoft Small Business Server installations.
- Scripted takeover + magazine howto.

univention

UCS Univention Corporate Server

„Minor“ Updates

- UCS 3.1 released on Dec, 12th 2012,
  one day after the official Samba4 4.0 release.
- Still based on Samba4 RC6 + upstream patches (freeze a couple of days before the official Samba 4.0)
- Incident based support by Andrew Bartlett.

- UCS 3.1-1, released March, 2013:
  Update to official Samba 4.0.3 + patches

univention

UCS Univention Corporate Server

Latest Samba3 → Samba4 Migration

- Last Thursday.
- 8 Samba4 DCs distributed across Germany.
- Some interesting initial replication problem on one of the DCs, solvable with one manual intervention.
- High load after joining a DC for about 10-20 minutes
- Probably due to increased replication with each additional DC

univention

Agenda

- Introduction
- Milestones of Samba4 integration into our products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SAMBA

UCS Univention Corporate Server

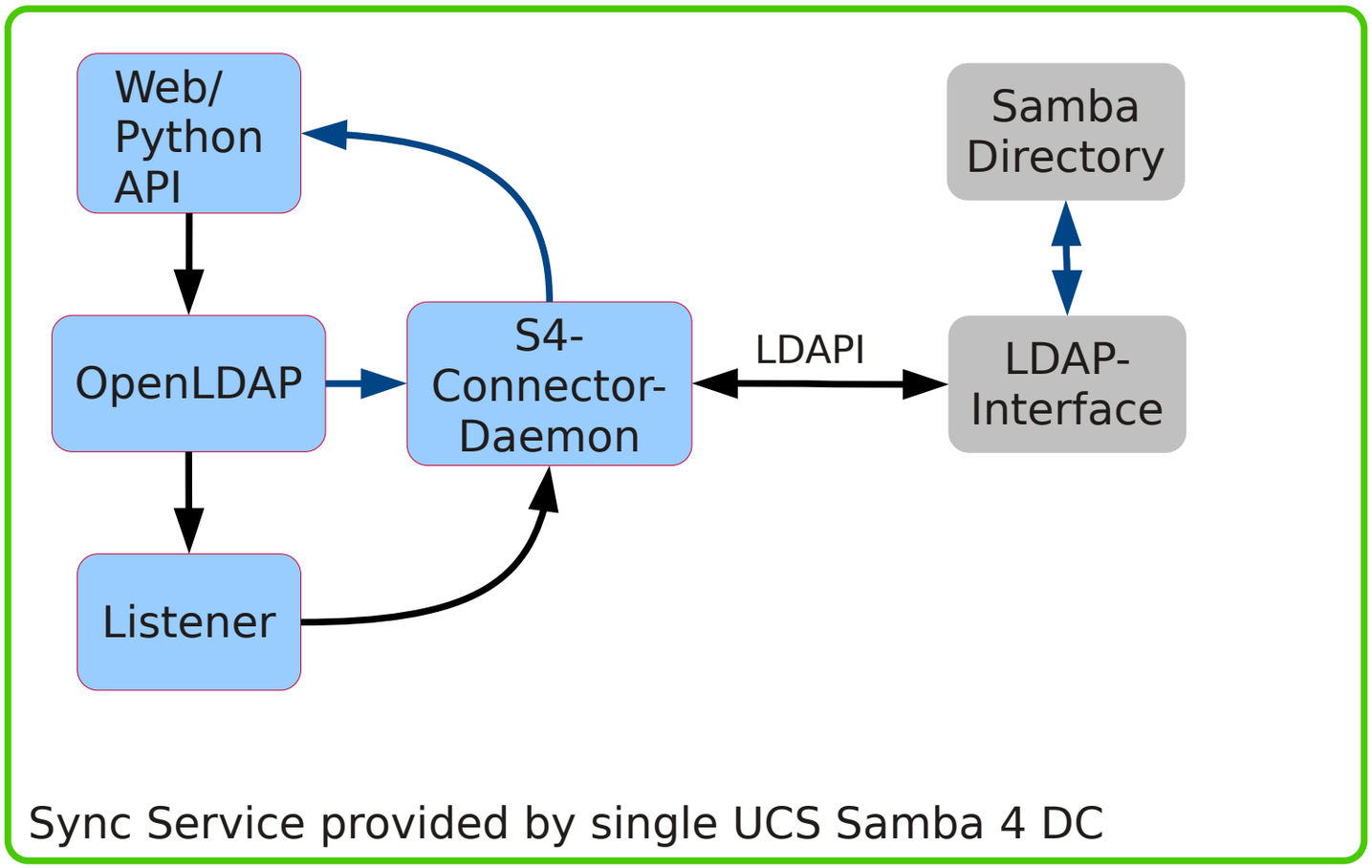
Univention S4 Connector

bidirectional, selective Synchronisation

- User, Group and Machine Accounts
- Password hashes
- DNS Records
- GPOs & gPLinks
- CN/OU Objects
- Running only on the first provisioned UCS Samba 4 DC

univention

Univention S4 Connector



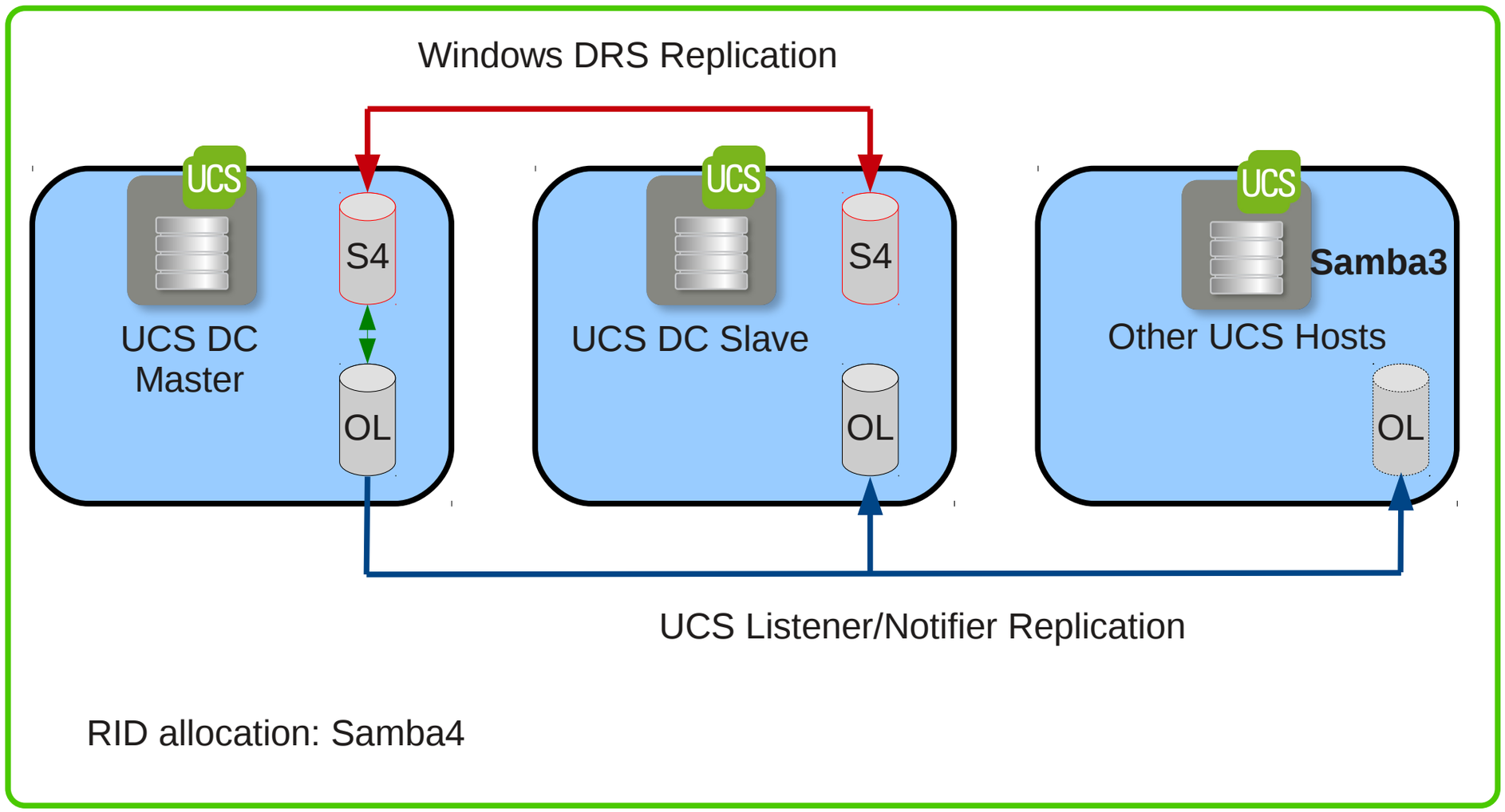
Single UCS/Samba 4 Domain

univention

UCS with Samba 4 and OpenLDAP

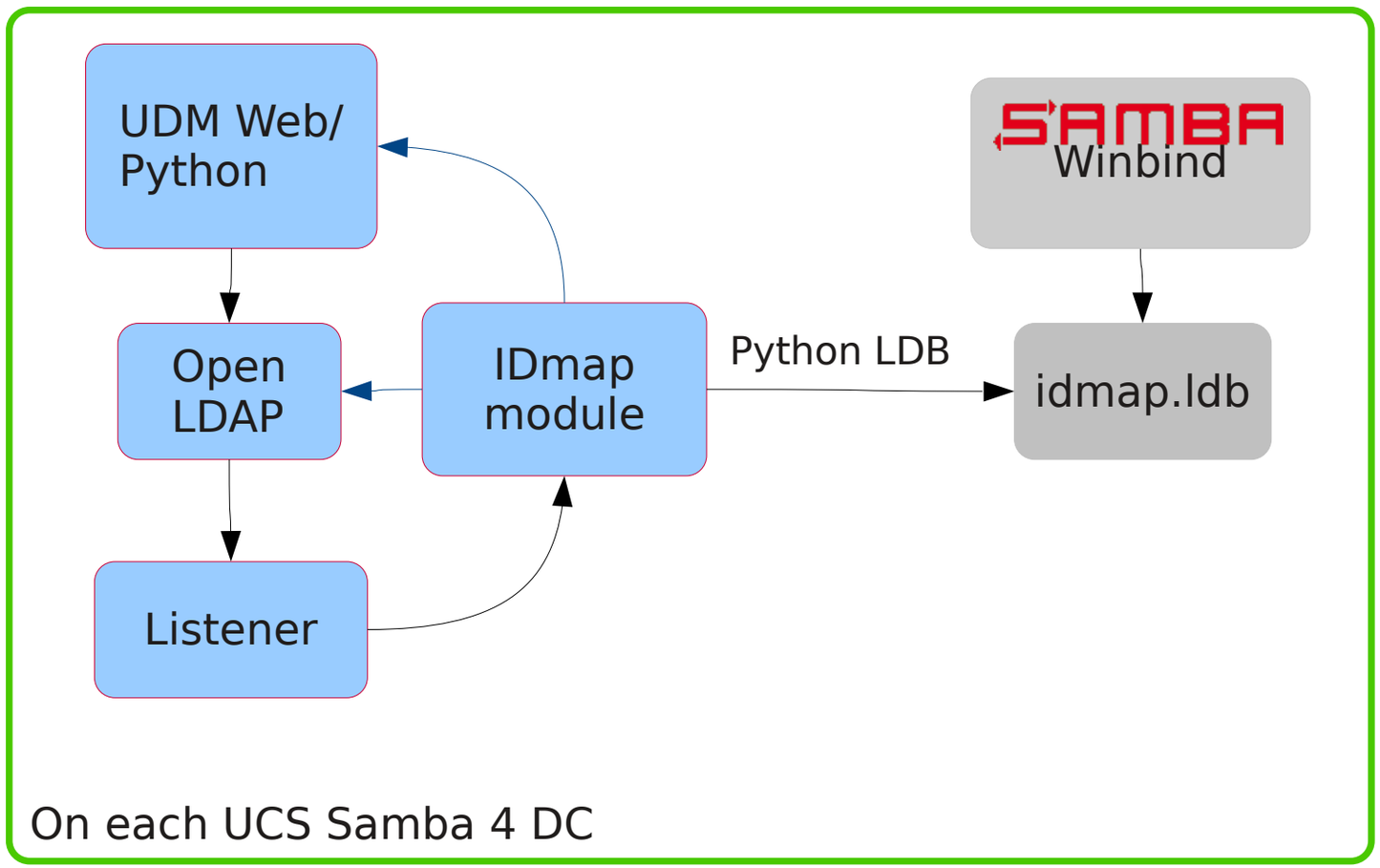
- Univention Directory Manager (Web GUI / Python API)
  - POSIX UIDs allocation
  - Conflict management (e.g. object naming)
  - OpenLDAP on non-standard ports (7389 / 7636)
- Samba 4
  - Allocation of RIDs (RID master), synced back to OpenLDAP

Regular UCS 3 / Samba4 Domain Replication Scheme



univention

Integrated Identity Mapping



univention

UCS Univention Corporate Server

Identity Mapping

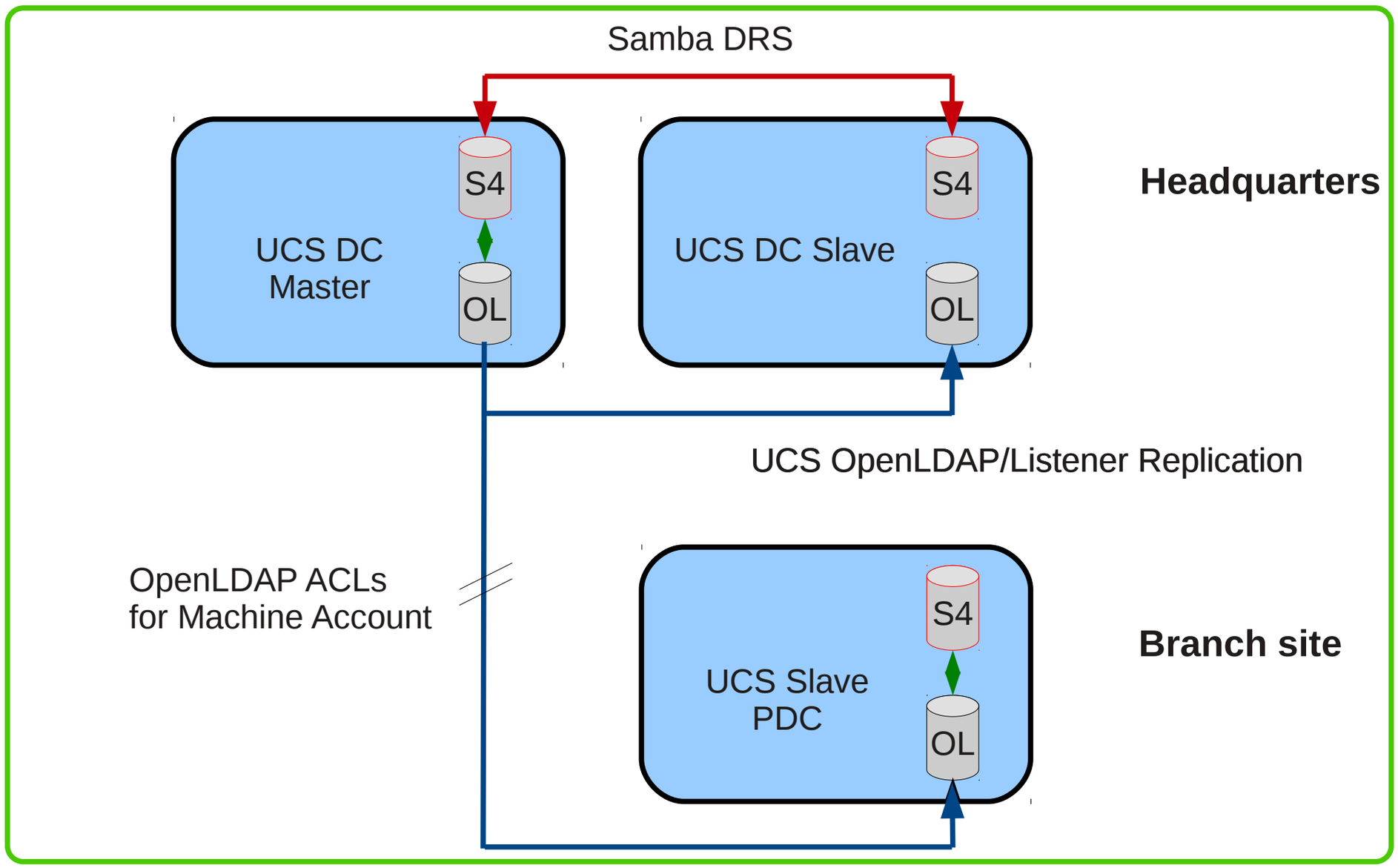
- Idmap.ldb contains records like this:

```
# record 4
dn: CN=S-1-5-21-309148026-423043480-4103072415-500

objectClass: sidMap

type: ID_TYPE_UID

objectSid: S-1-5-21-309148026-423043480-4103072415-500

xidNumber: 2002
```

- xid type UID/GID is important! With ID_TYPE_BOTH user/group mixup occurs if user and group Posix IDs are not distinct.

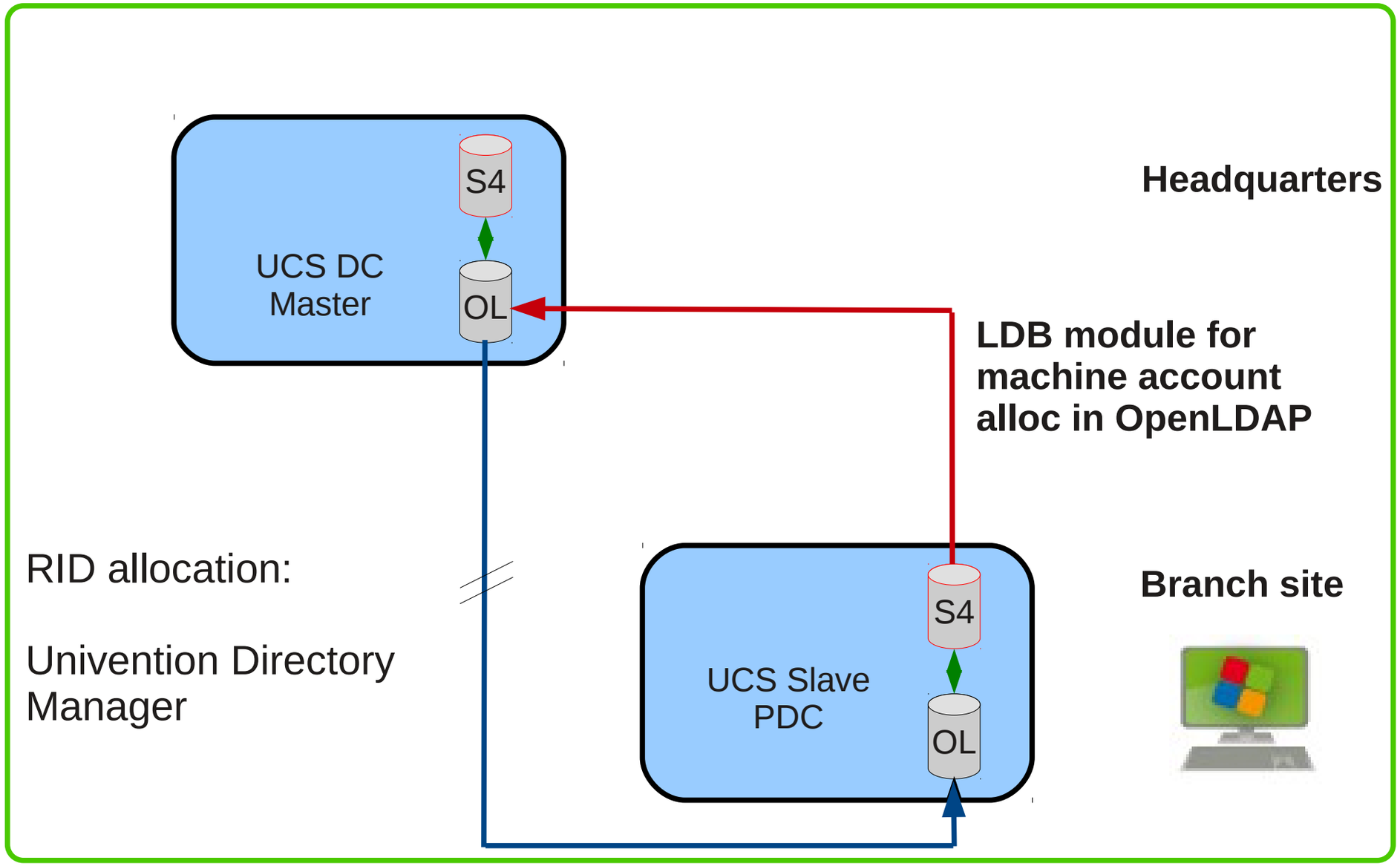
univention

UCS@school / Samba4 „Slave PDC“ Selective Replication Scheme



univention

UCS@school Samba4 Slave PDC: external RID allocation



univention

Running dlz_bind9

- Minor adjustements were necessary
- Data stored in CN=MicrosoftDNS in Samba4
- application partitions („DC=DomainDnsZones“) not used currently
- Kerberized DDNS updates working transparently

univention

Agenda

- Introduction
- Milestones of Samba4 integration into our products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SNTP peculiarities

- Matthieu Patou on samba-technical about MS-SNTP:

  "I used to have the same haircut as Stallman before dealing with (s)ntp and now I look more like Bruce Willis." - Apr. 2011

- „Please be aware that windows won't accept the answer from the time server even if it has the signature if the server says that it's not completely synchronized with a upper time server.“

univention

SNTP peculiarities

- Similar experience in UCS 3.0: w32tm /query /peers /status

```
Peer: ucs310samba4.foo.bar          ## ntpd on DC with    local stratum 10
State: Active
Time Remaining: 618.4000000s
Mode: 3 (Client)
Stratum: 0 (unspecified)            ## should be 11  for the Windows7 client
PeerPoll Interval: 0 (unspecified)
HostPoll Interval: 10 (1024s)
Last Successful Sync Time: (null)
LastSyncError: 0x800705B4 (This operation returned [...] timeout period expired. )
LastSyncErrorMsgId: 0x00000000 (Succesful)
AuthTypeMsgId: 0x0000005B (NtDigest )
Resolve Attempts: 0
ValidDataCounter: 1
Reachability: 2
```

SNTP peculiarities resolved

- It turns out that Windows 7 doesn't accept NTP servers with local stratum >9. With lowered DC stratum:

```
Peer: ucs311samba4.foo.bar          ## ntpd on DC with stratum lowered to 5
State: Active
Time Remaining: 861.6196000s
Mode: 3 (Client)
Stratum: 6 (secondary reference - syncd by (S)NTP)
PeerPoll Interval: 0 (unspecified)
HostPoll Interval: 10 (1024s)
```

- Shipped adjusted ntpd. conf in current UCS 3.1-1 → fixed
  Avoiding a lot of AD-issues (DDNS update, GPO evaluation, ...)

univention

Rosswell Incident

- Customer with a hand full of Samba4/AD-Sites across the USA
- No RID Set generated by RID Master at SiteA after join of DC3 into SiteB
- Inconsistent sam.ldb on RID Master
- Cleaned things up with sambatool dbcheck –fix
- Joined again into SiteB, still no RID Set, no local account creation possible.
- Other replication problems
- Initially looked like timeouts due to low network bandwidth

univention

Samba-tool drs showrepl

```
root@dc1:~# samba-tool drs showrepl    ## on 4.0.0~rc6
Site1\DC1
DSA Options: 0x00000001
DSA object GUID: 058f8b5e-1236-4efd-92a5-6c00849c24dd
DSA invocationId: 091ea78b-bd85-4d6b-b65b-6a796da6b377

==== INBOUND NEIGHBORS ====

DC=foo,DC=bar
        Site1\DC2 via RPC
                DSA object GUID: c8167f37-dab0-4dd7-9895-efe4d921f27d
                Last attempt @ Tue Mar 26 09:08:57 2013 MDT failed, result 58 (WERR_BAD_NET_RESP)
                1458 consecutive failure(s).
                Last success @ Sun Mar 17 04:41:14 2013 MDT

DC=foo,DC=bar
        Site2\DC3 via RPC
                DSA object GUID: 393be633-d0a0-46aa-9d0a-e4106fbc2da9
                Last attempt @ Tue Mar 26 09:11:59 2013 MDT failed, result 121 (WERR_SEM_TIMEOUT)
                2059 consecutive failure(s).
                Last success @ NTTIME(0)

DC=foo,DC=bar
        Site3\DC5 via RPC
                DSA object GUID: 5fbe2f02-895d-400c-af5a-2cc1c3da5fbf
                Last attempt @ Tue Mar 26 09:11:59 2013 MDT failed, result 2 (WERR_BADFILE)
                158 consecutive failure(s).
                Last success @ NTTIME(0)
```

univention

Rosswell Incident

- Replication issues could be tracked down in this case to some Riverbed WAN accelerators joined into the domain...

- We saw at least one entirely different case where RID Pool allocation failed as well..

- Manual triggering of RID Pool creation works nicely, running the „getncchanges“ script with exop FSMO_RID_ALLOC.

univention

Samba-tool drs showrepl flakeyness

```
root@DC1:~# samba-tool drs showrepl
Site1\DC1
DSA Options: 0x00000001
DSA object GUID: 058f8b5e-1236-4efd-92a5-6c00849c24dd
DSA invocationId: 091ea78b-bd85-4d6b-b65b-6a796da6b377

==== INBOUND NEIGHBORS ====

ERROR(runtime): DsReplicaGetInfo of type 0 failed - (8442,
'WERR_DS_DRA_INTERNAL_ERROR')
```

- Sometimes samba-tool drs kcc helps in this case
- Transient, maybe related to samba replication load

univention

Last Thursday: Conflict resolution oddities

- One DC showed WERR_GENERAL_FAILURE für Replication of the Domain partition to another DC. log.samba shows:

```
 [2013/04/09] repl_meta_data.c:3583: Resolving conflict record  via existing rename
'CN=BCKUPKEY_PREFERRED Secret,CN=System,DC=foo,DC=bar' ->
'CN=BCKUPKEY_PREFERRED        Secret\0ACNF:613a86cd-3570-442c-9d7e-
ac7333da10c1,CN=System,DC=foo,DC=bar'

 [2013/04/09] replicated_objects.c:618 (dsdb_replicated_objects_commit)
      Failed to apply records: subtree_rename: Cannot move/rename
CN=BCKUPKEY_PREFERRED Secret,CN=System,   DC=foo,DC=bar. It's an LSA-specific
object!: Entry already exists

 [2013/05/09] drepl_out_helpers.c:718 (dreplsrv_op_pull_source_apply_changes_trigger)
     Failed to commit objects:
WERR_GENERAL_FAILURE/NT_STATUS_INVALID_NETWORK_RESPONSE
```

- Replication continued OK after manual removal of the object

univention

Agenda

- Introduction
- Milestones of Samba4 integration into our products
- Overview of the Integration
- Issues and Cases
- Outlook

univention

SAMBA

UCS Univention Corporate Server

Outlook

- Did we open a can of worms? Don't think so.

  Certainly after 1.5 years it does not look and feel bad.

  (about 20 samba bugs filed by Univention, more than 10 fixed today)

- Problems are localized well
- tracking them down was more or less straight forward once we learned the basic structures.
- Happy to not depend 100% on DRS replication.
- Looking forward to exciting new possibilities.

univention

Special Credits from my Side

- Special thanks to Metze and Andrew Bartlett for all the insight and advice!

univention

Thank you!

Thanks to the

SAMBA -Team!

SambaXP 2013

Arvid Requate, requate@univention.de

univention

Contact

- Dr. Arvid Requate
- +49 421 22232-40 (Tel.)
- +49 421 22232-99 (Fax)
- requate@univention.de

univention