

# The Evolution of Samba Active Directory

---

Experiences in implementing and optimizing Active Directory features in Samba

Garming Sam – Catalyst IT



**What has been done in the last year?**

# Samba 4.9

---

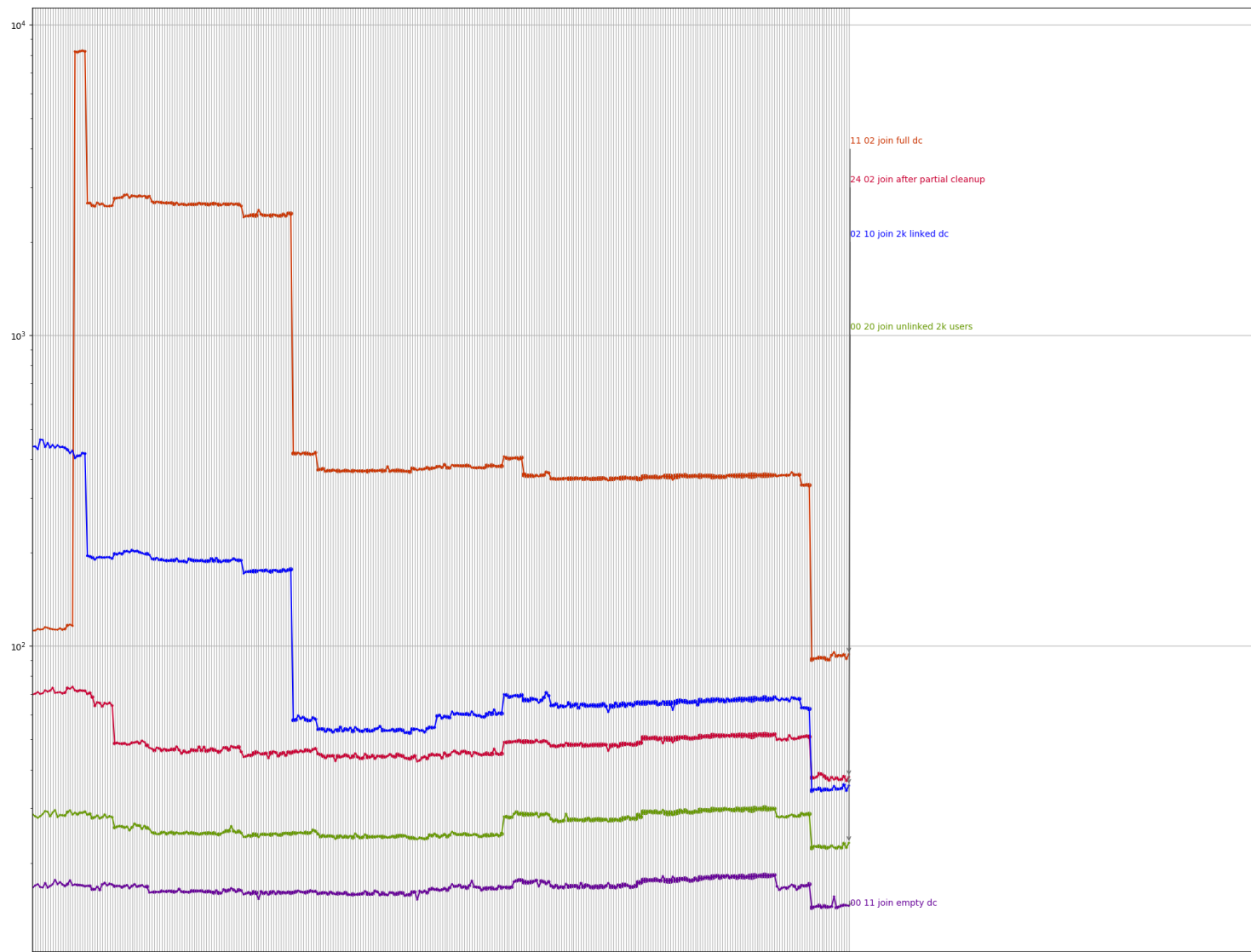
- Password and membership change auditing
- LMDB back-end (semi-experimental)\*
- Fine grained password policies
- Domain backup, restore and rename tools
- Better DRS partner visualization
- Automatic DNS site coverage\*
- DNS scavenging support\*
- Improved trust support and more...

# Samba 4.10

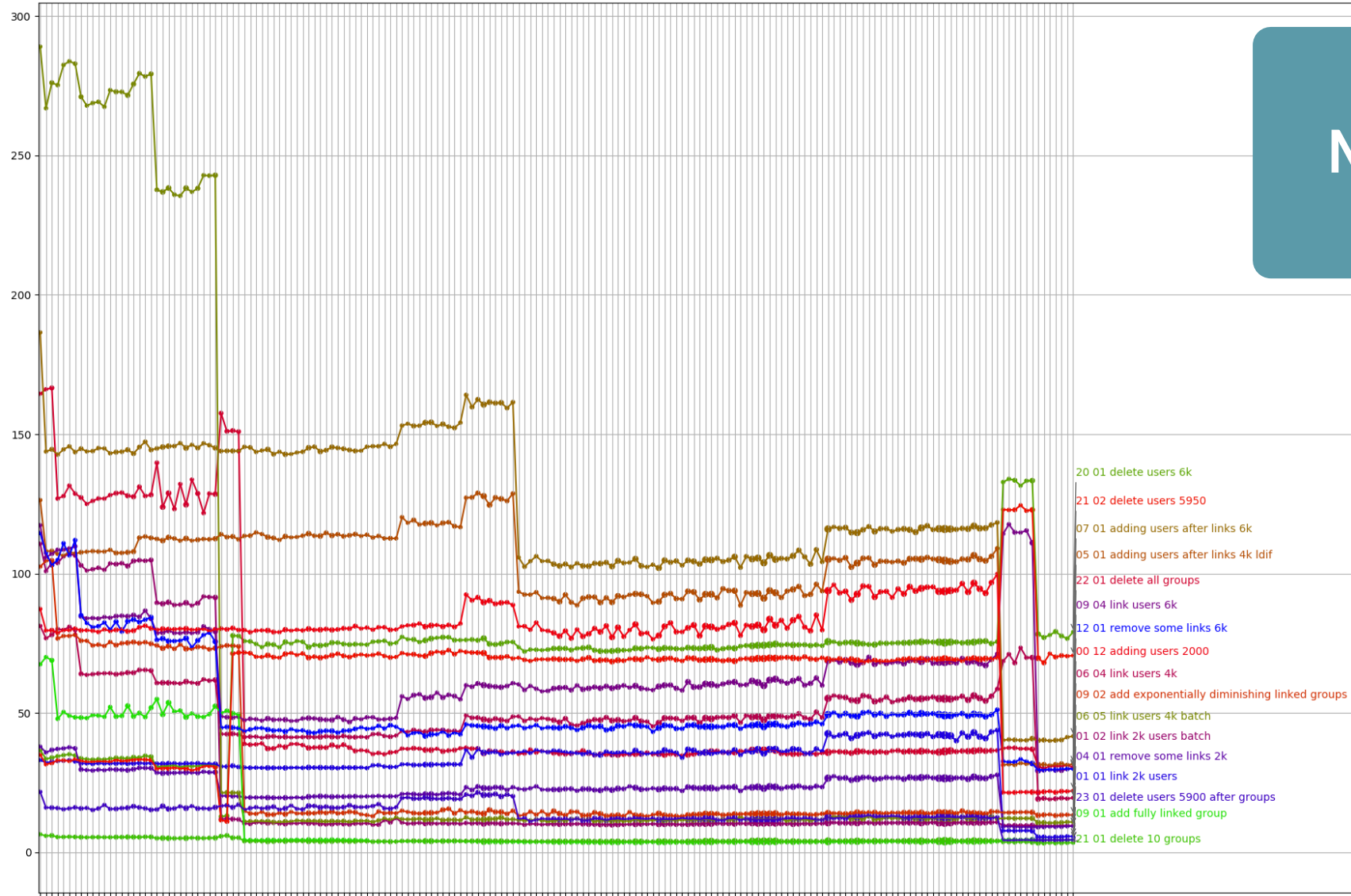
---

- GPO import and export\*
- KDC\* and NETLOGON prefork (default in 4.11)
- (Prefork) improvements for restarting services automatically
- Changes to LDAP paged results to save memory\*
- Offline domain backup
- Python 3 support
- Audit logging with MS event IDs and more...

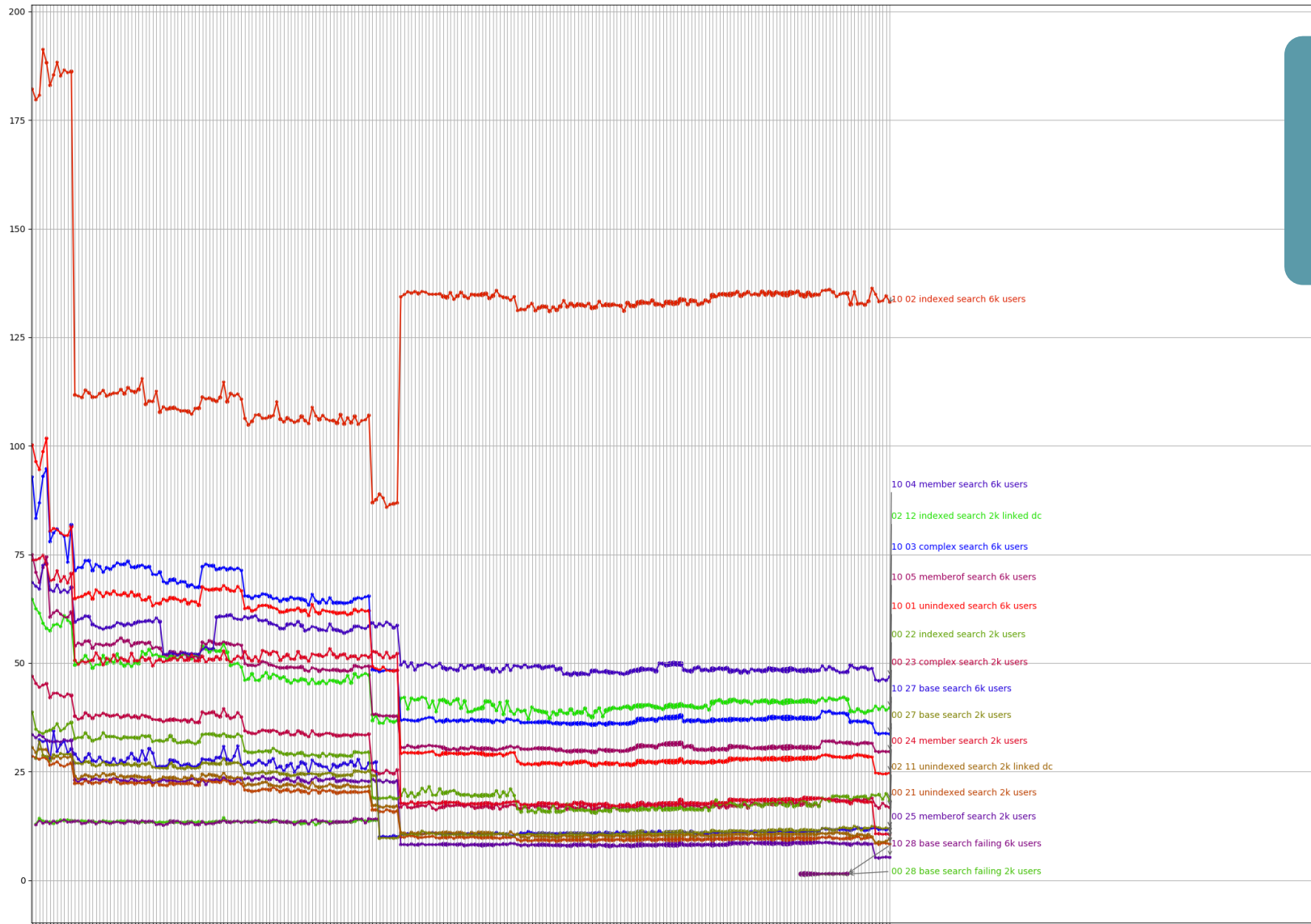
# Join



# Modify



# Search



# Performance, performance, performance

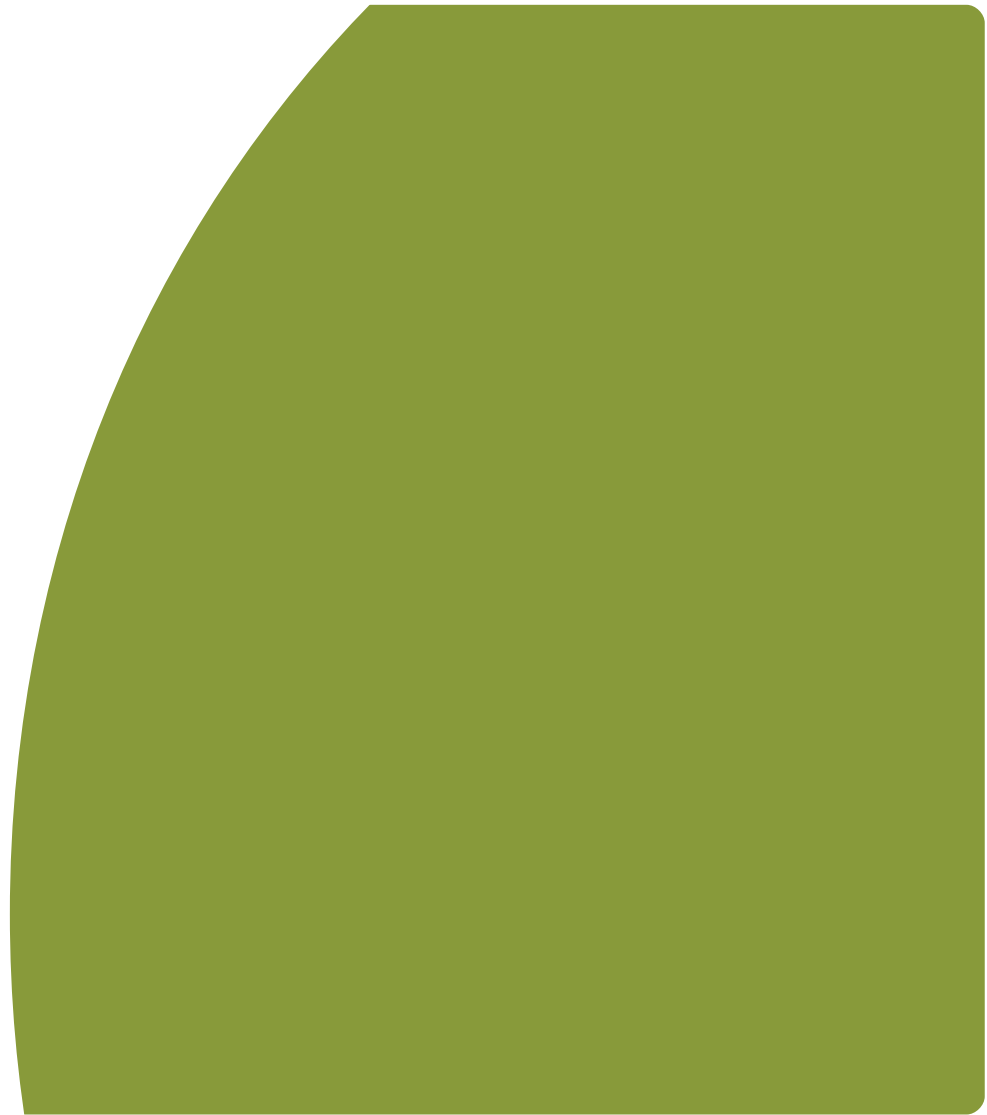
Replication improvements, linked attribute performance, rename performance, large scale improvements, ... as well as other things like schema updates



# Traffic replay runner

---

Recording real network traffic and playing it back at different speeds



## Naive traffic runner results (2 vCPU, 8GB RAM)

---

**v4.6** – 113 operations / second

**v4.7** – 94 operations / second (changes to LDAP multi-process)

**v4.8** – 154 operations / second (only in new prefork process mode)

**v4.9** – 157 operations / second (only in prefork mode)

**v4.10** – Same as 4.8 and 4.9

Git master (prefork is default) – about 165 operations / second

Traffic sample is largely DNS, name resolution, LDAP bind, NETLOGON (typical)

# Basic steps for replaying traffic

---



## Network trace

Run wireshark and get a pcap output



## Traffic summary

Anonymize the traffic and pick out important details to replay



## Traffic model (optional)

Create a statistical model for generating proportionally similar traffic

# Basic steps for replaying traffic

---



## Play traffic

Run either the summary or the model file



## Analyze the results

Successes or failures, median, mean, max, 95<sup>th</sup>

# Basic steps for replaying traffic

---



## Play traffic

Run either the summary or the model file



## Analyze the results

Successes or failures, median, mean, max, 95<sup>th</sup>

That's it!

We're fast, 100,000 users, no problems!

# The real difference between Samba 4.9 and the upcoming 4.11

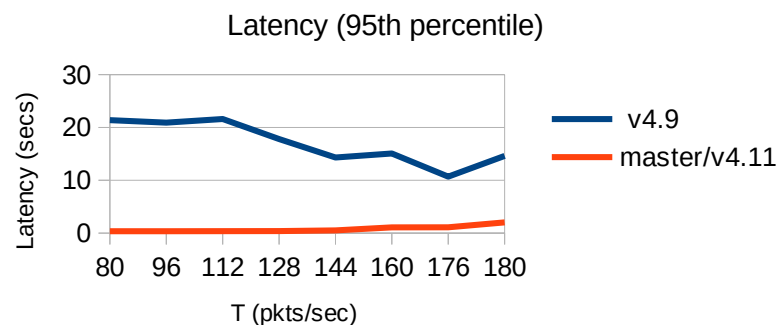
---

In particular environments, performance can degrade quickly based on database size:

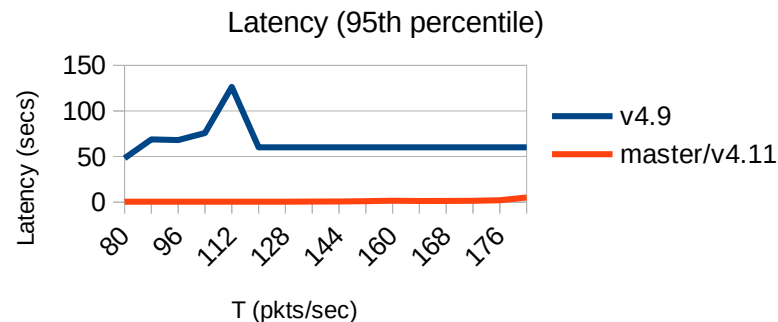
Build	Users	Machines	T (pkts/sec)	Ops/sec	Latency
Master/v4.11	4,400	4,400	240	~165	4.78s
v4.9	4,200	4,200	228	~157	3.24s
Master/v4.11	50,000	62,500	196	~135	4.58s
v4.9*	50,000	62,500	? < 80	? < 43	51.90s

# The real difference between Samba 4.9 and the upcoming 4.11

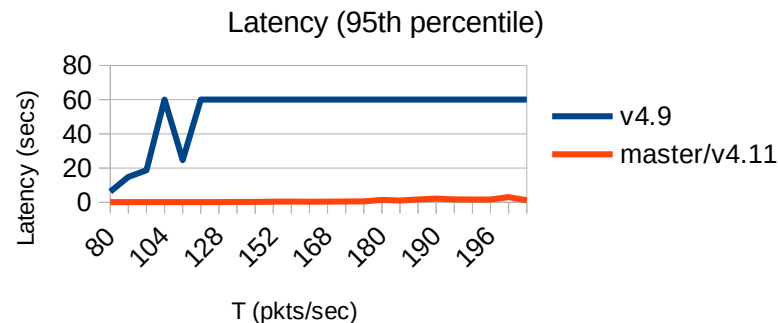
LDAP bindRequest



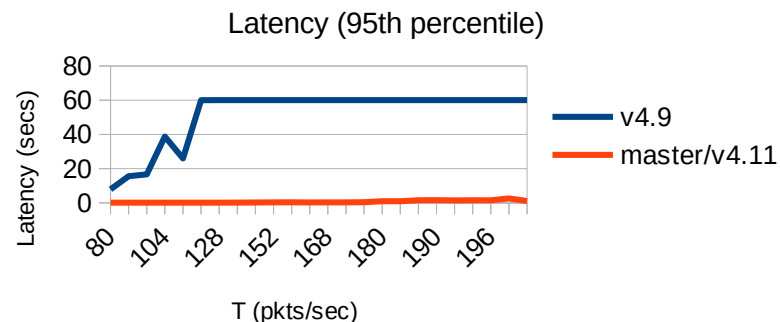
drsuapi DsBind



rpc\_netlogon NetrLogonGetDomainInfo

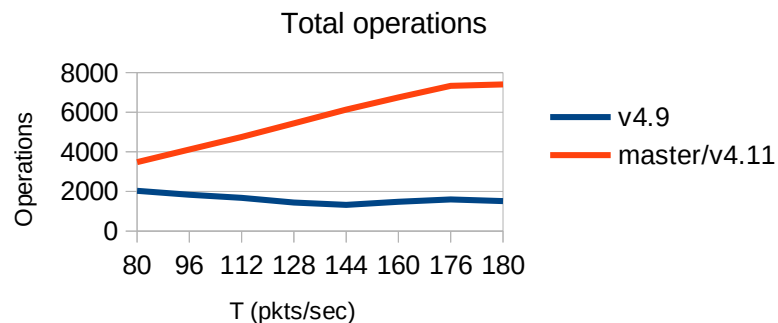


Isarpc Isa\_LookupNames4

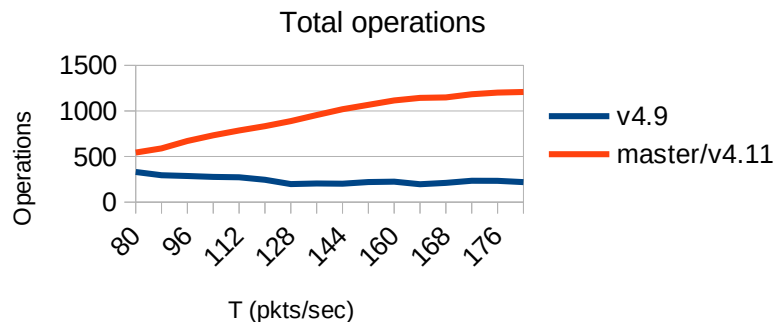


# The real difference between Samba 4.9 and the upcoming 4.11

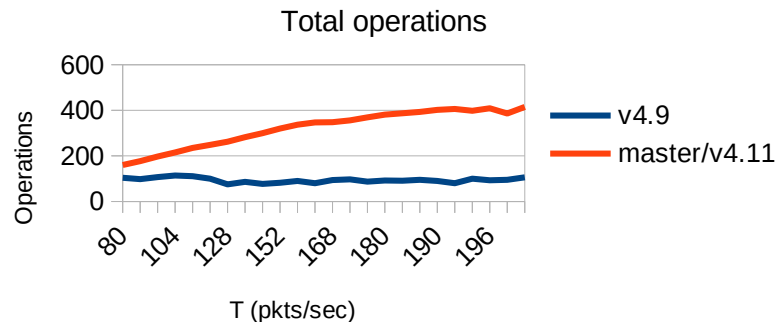
LDAP bindRequest



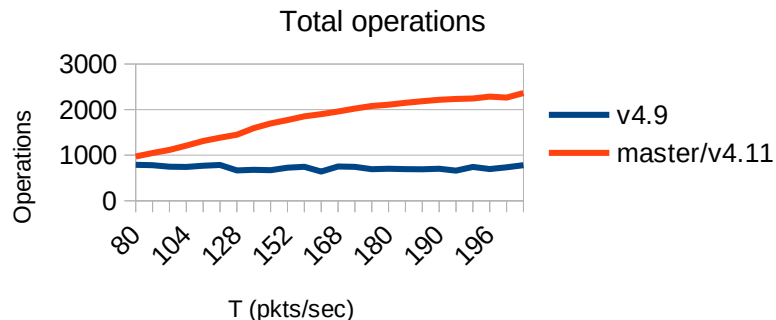
drsuapi DsBind



rpc\_netlogon NetrLogonGetDomainInfo



Isarpc Isa\_LookupNames4





## How did we do it?

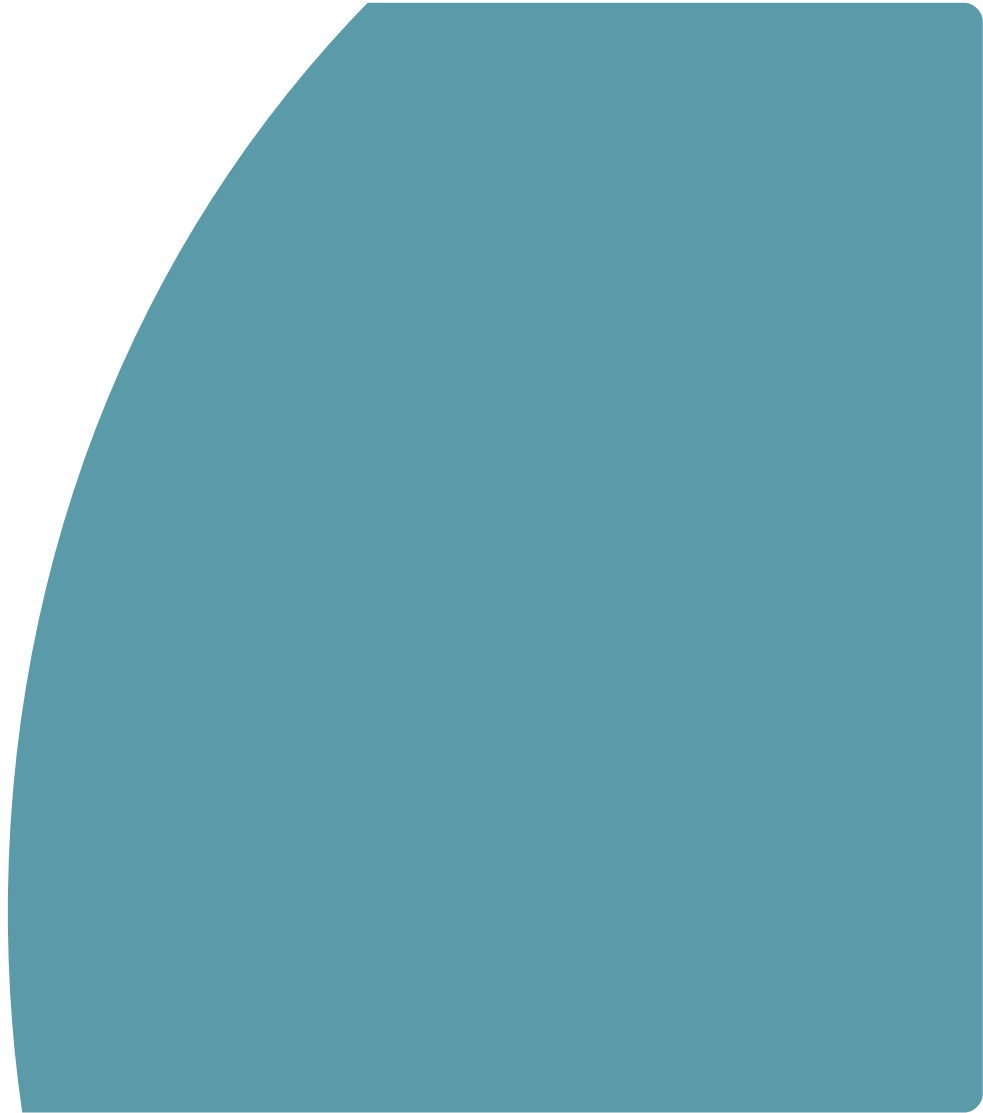
1. Created a new backup regime
2. Automated set-up of large domains
3. Periodic and targeted traffic replay

# Domain backup

---

A new method of backing up an AD  
Domain in Samba 4.9 + 4.10

Work done for a separate client

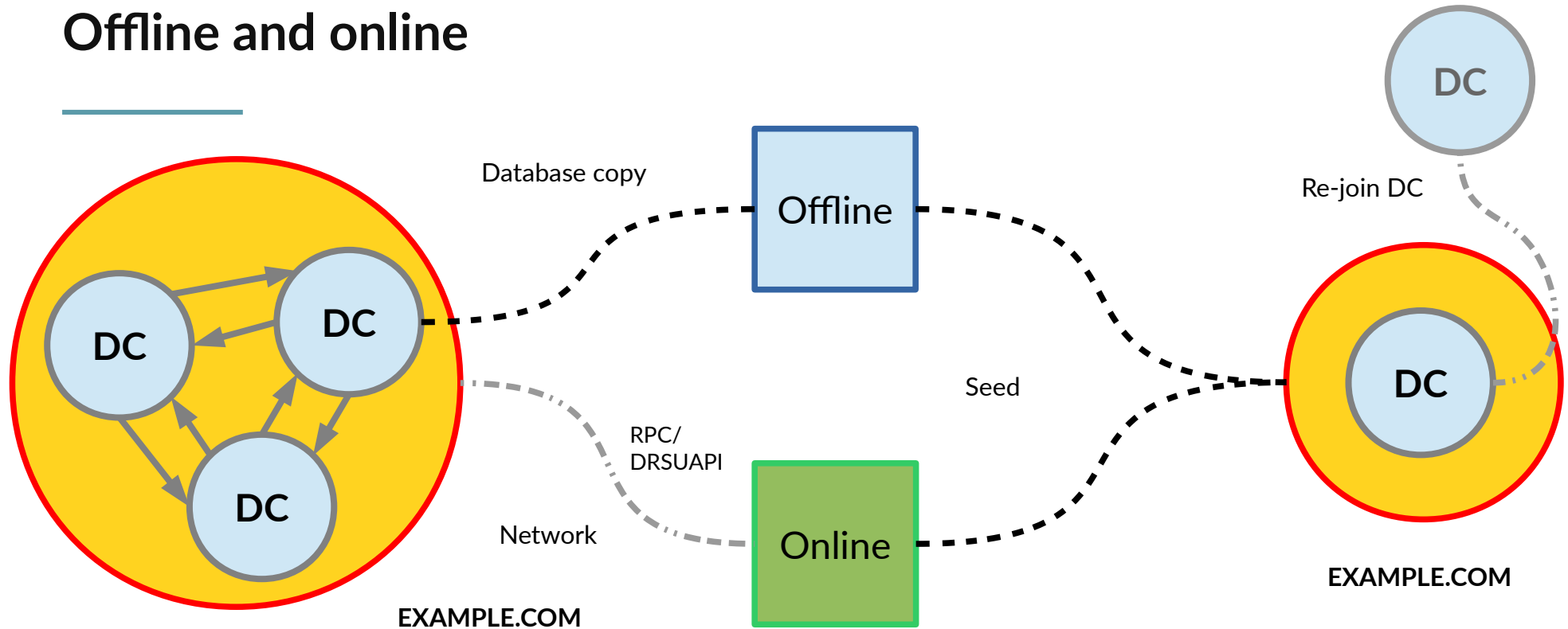


# Why?

---

- Existing samba\_backup script had a number of problems
  - With a running DC it wasn't certain to produce a valid copy
  - It was safer than a standard copy, but didn't respect lock ordering
  - Might have caused deadlocks, corrupt or inconsistent (secrets) data
- Single source of truth of the domain data (multi-master replication)
  - Forcing a pristine backup to override corrupt data elsewhere is non-trivial
  - Restoring into competing data, might look replicated due to old versioning
  - Avoid some database inconsistencies by creating a replication (online) backup

# Offline and online



samba-tool domain backup [online|offline]



Tar file



samba-tool domain backup restore

# Benefits

---

- Reproducible testing is easier, upgrade testing is easier
- Testing under different conditions is much easier
- For those who re-deploy in a certain way, it's the (almost) ideal tool
- Still has issues from a user-perspective but very useful as a developer tool
- Validating changes with large domains now becomes possible

# Automation

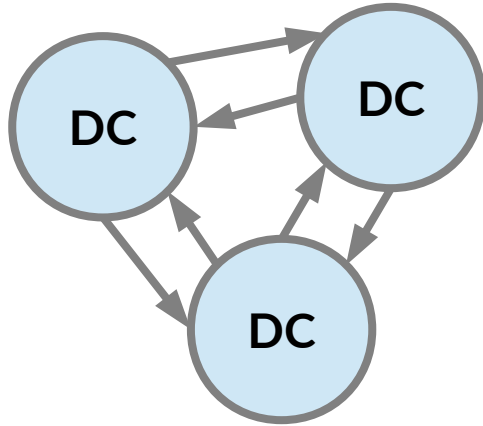
---

Actually running the traffic runner for real (making it reproducible and periodic)

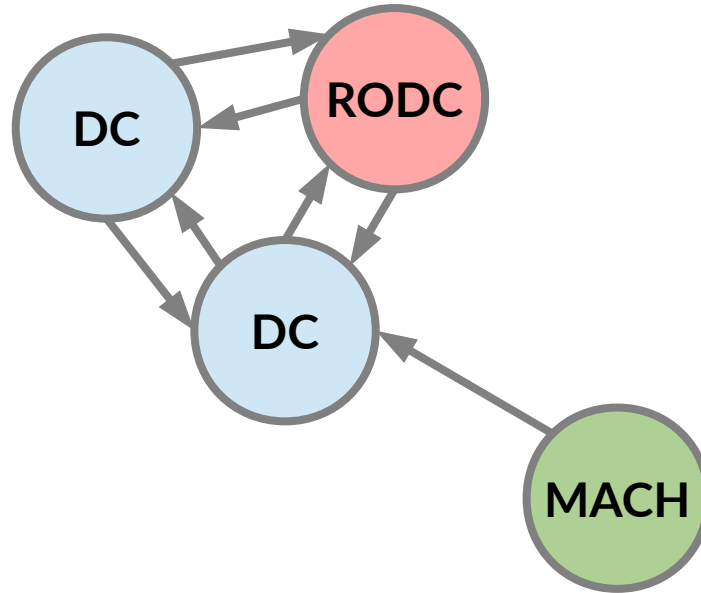


# Automation

---



Seed AD domain from a backup



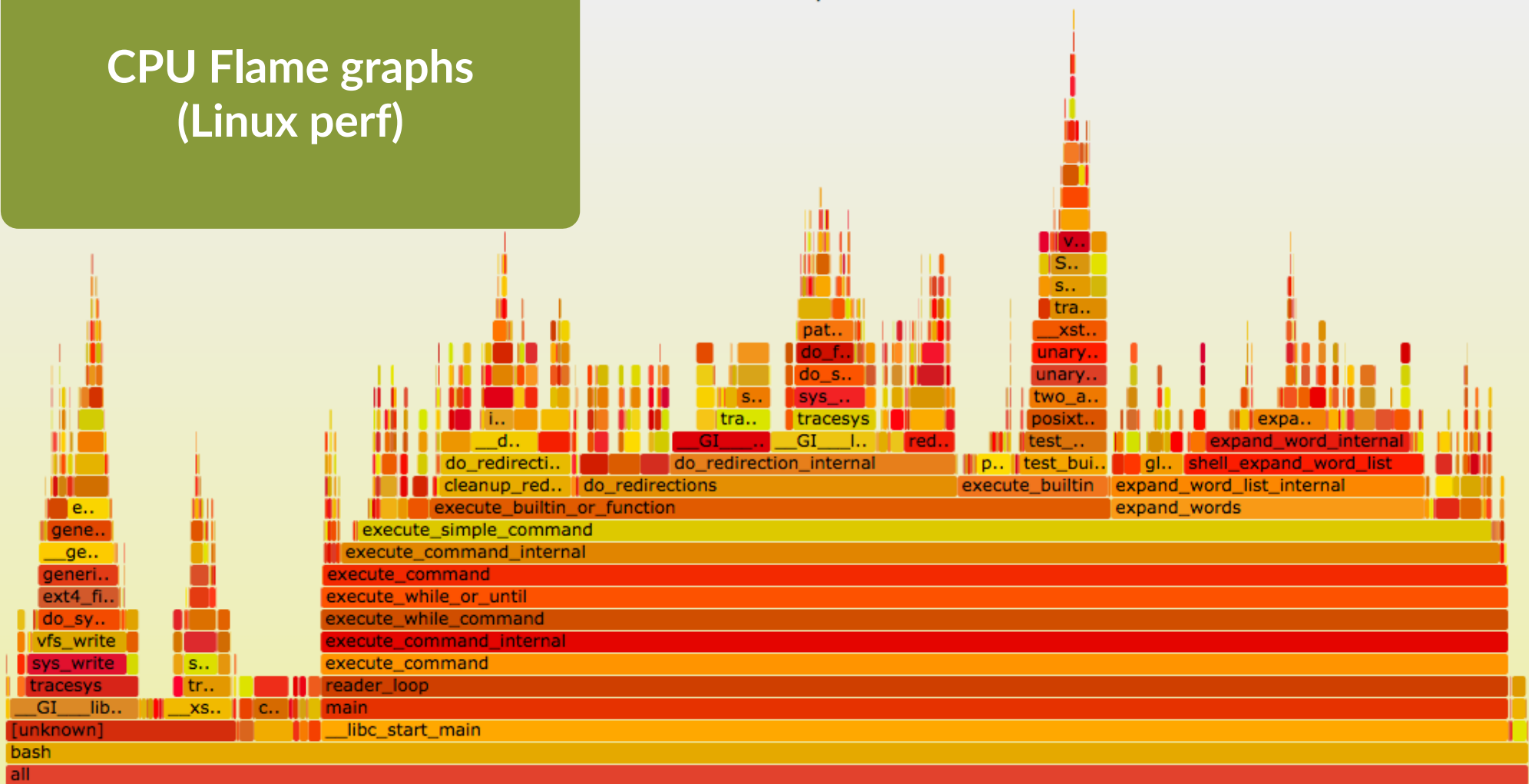
# Replicating... forever

After joining a new domain controller to a restored domain,  
ongoing replication would never end.

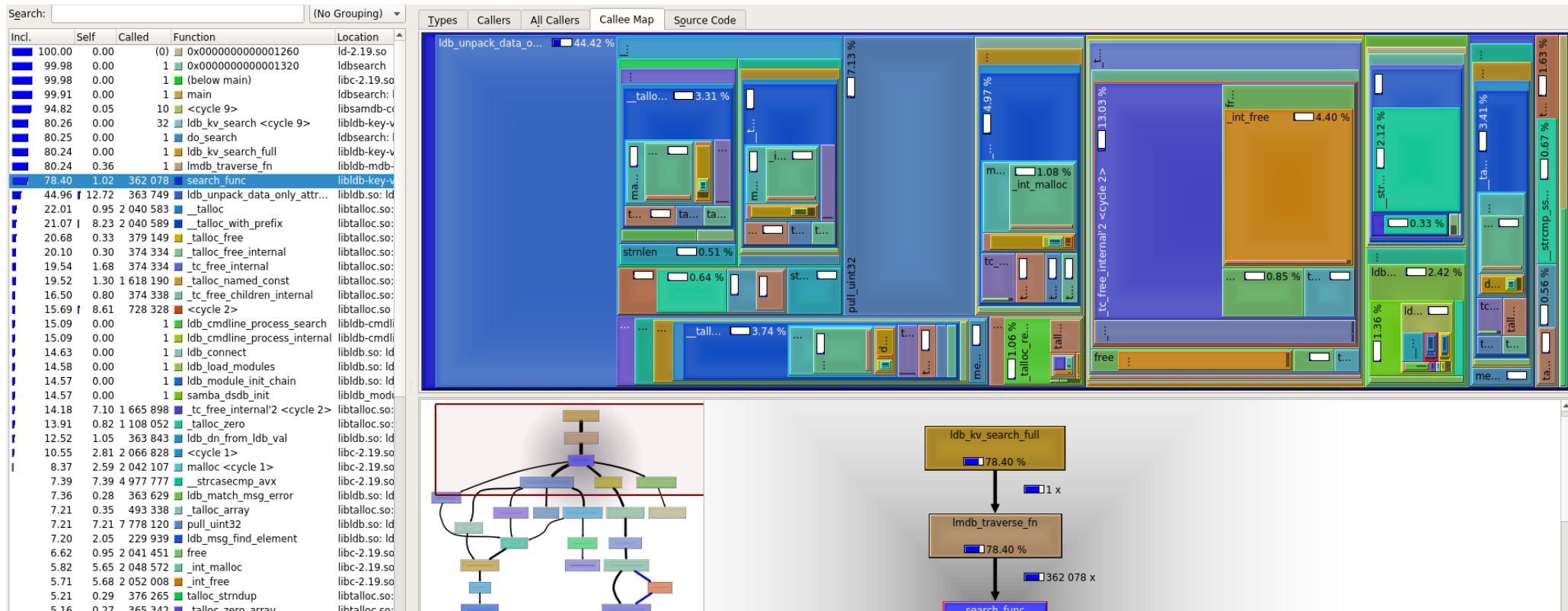
Why doesn't it only take as long as the join (30 minutes)?



# CPU Flame graphs (Linux perf)



# Callgrind



# Print debugging

**top (htop/iotop)**

**trial and error**

**basic arithmetic**

**gdb (attach to pid)**

**perf top**

**luck**

# Lessons

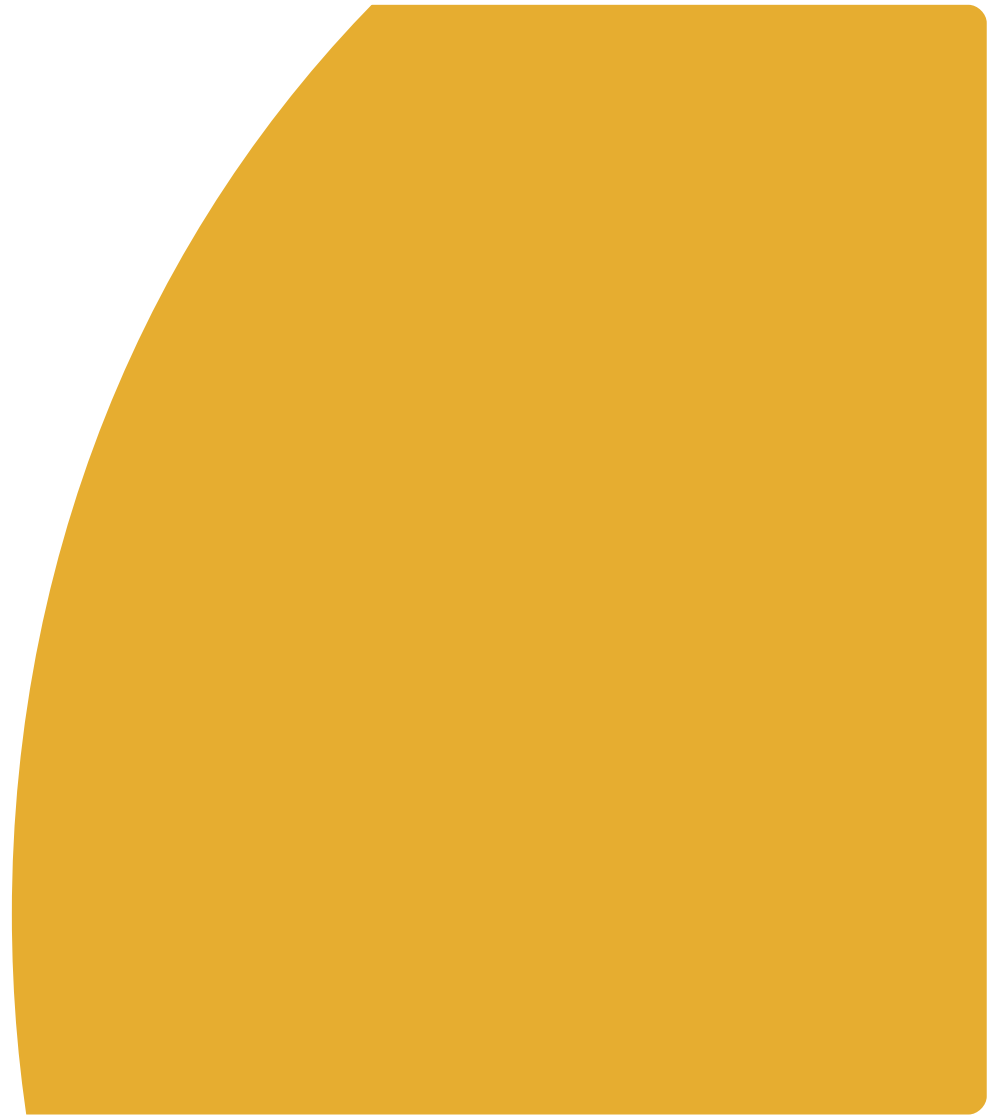
---

- It turns out there was a bug in the backup code, but it found real performance issues that we then fixed
- Accidentally doing the wrong thing means running out of memory quickly with a large database.
  - Piecemeal growth  $\neq$  dealing with everything at once
- Learning how LMDB behaves - completely different to our previous database backend (copy-on-write)

## Database changes motivated by our traffic statistics analysis

---

The effort required to improve figures to the degree shown in the upcoming 4.11 release



# Changes to our database and core database services

---

- Implemented indexing of  $\geq$  and  $\leq$  queries
- Indexing 300,000 records went from ~4 sec to ~0.2 sec
- Replication more responsive
  - Example testing: ~4 sec to ~1 sec for no data, ~6 sec to ~1 sec for 200 new records
- Paged results – Reducing required memory usage from GB to KB or MB
- LDAP efficiency improvements – Impossible operations can now be done (search)
- Subtree renames – Large renames from days to less than an hour

# Changes to the database record storage format

---

CN=test_user,CN=Users
2 elements
name   1 value   test_user
member   5 values
group_1, group_2
group_3
group_4, group_5



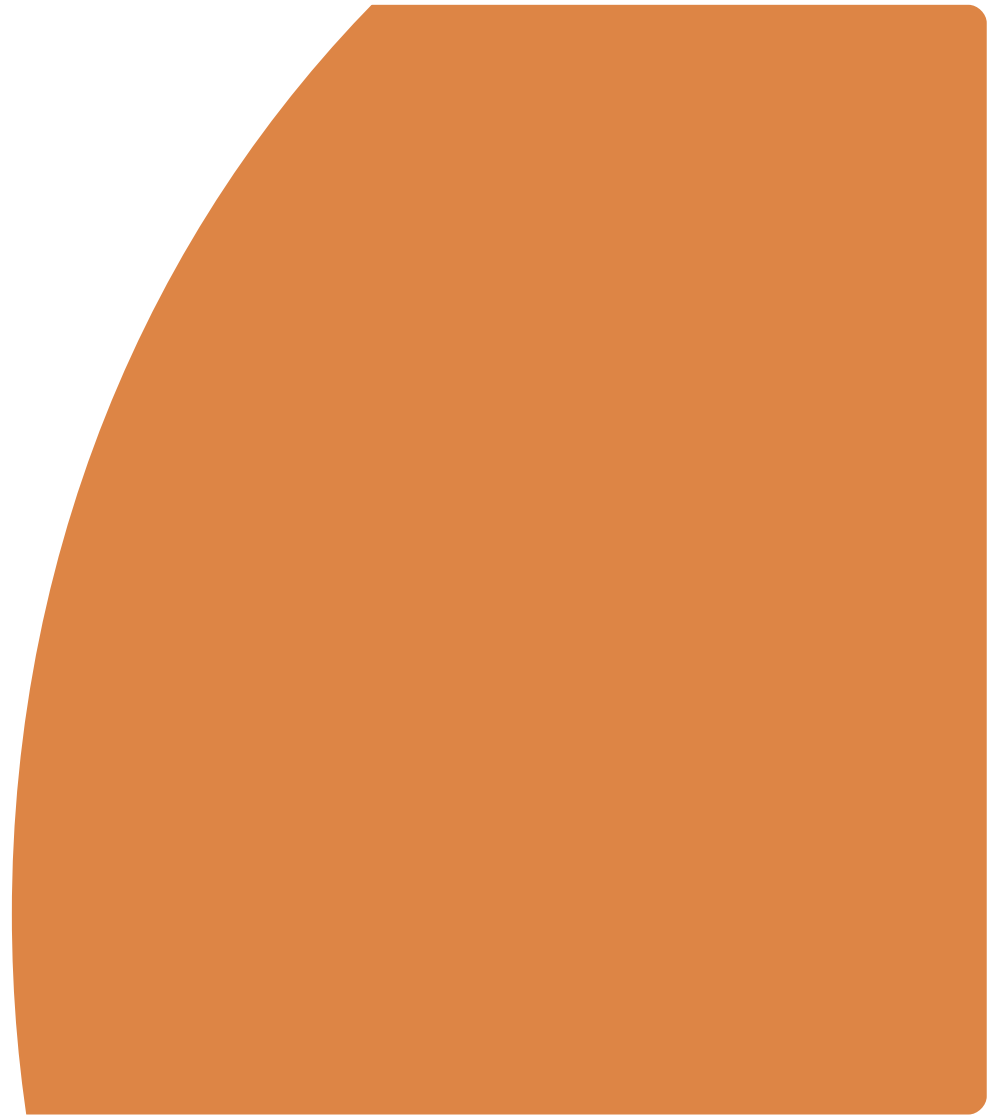
CN=test_user,CN=Users
2 elements
name   1   member   5
test_user
group_1, group_2
group_3
group_4, group_5

Only read data when necessary, offset data is stored at the beginning, massive size reduction.  
Applies to more than just storage of group membership but also big blobs of data (e.g. photos).

# 2012 R2 Schema Support

---

Pre-requisite for 2012 R2 functional level  
and newer AD (security) features





## 2012 R2 schema support

---

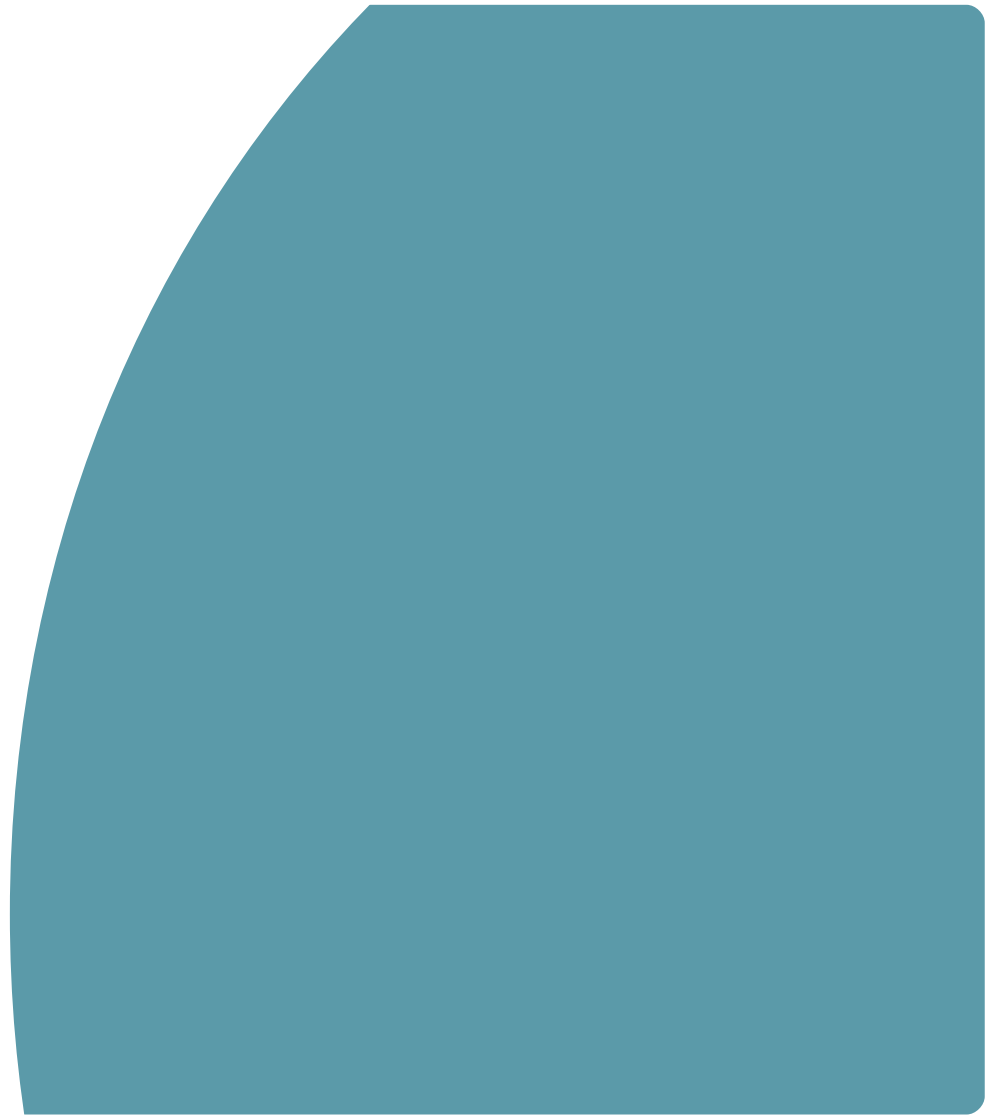
- First half (replication support) is already slated for 4.11
- Second half (default schema) is currently waiting final sign-off and tweaks
- Integration with newer Windows servers no longer causes ongoing replication problems and 2012 R2 servers can join Samba without issue now

# GPO import/export

---

A new way of copying over a SYSVOL that functions across domains

Exports to XML with XML entities



MS - GPOL

MS - GPNRPT

MS - GPFR

fdeploy1.ini

MS - GPWL

MS - GPSCR

User/Documents & Settings

.xml

MS - GPREG

registry.pol

MG - GPFAS

MS - GPOD

MS - GPAC

Machine/Microsoft/Windows NT/SecEdit

MS - GPSI

.aas

MS - GPDPC

audit.csv

MS - GPSB

GptTmpl.inf

MS - GPPREF

MS - GPIPSEC

MS - GPREF

# Using GPO Import/Export

---

```
samba-tool gpo backup  
samba-tool gpo restore
```

```
samba-tool gpo backup --generalize --entities=$OUT_PATH  
samba-tool gpo restore --entities=$IN_PATH
```

```
<!ENTITY SAMBA_____7b7bc2512ee1fedcd76bdc68926d4f7b__ "Guest">
```

[https://wiki.samba.org/index.php/GPO\\_Backup\\_and\\_Restore](https://wiki.samba.org/index.php/GPO_Backup_and_Restore)

# Re-indexing

---

Example of an operation where our tooling failed and discovered improvements to join time of 2-4x



## Re-indexing timings (mm:ss.ss)

---

100,000 users approx 230,000 records.

Hash size	re-index time
1,000	14:42.06
10,000	1:59.56
100,000	39.92
200,000	37.48
300,000	43.16

50,000 users approx 110,000 records.

Hash size	re-index time
1,000	3:46:93
10,000	37:29
100,000	18.95

20x improvement

Basically a one line  
change

# Domain rename

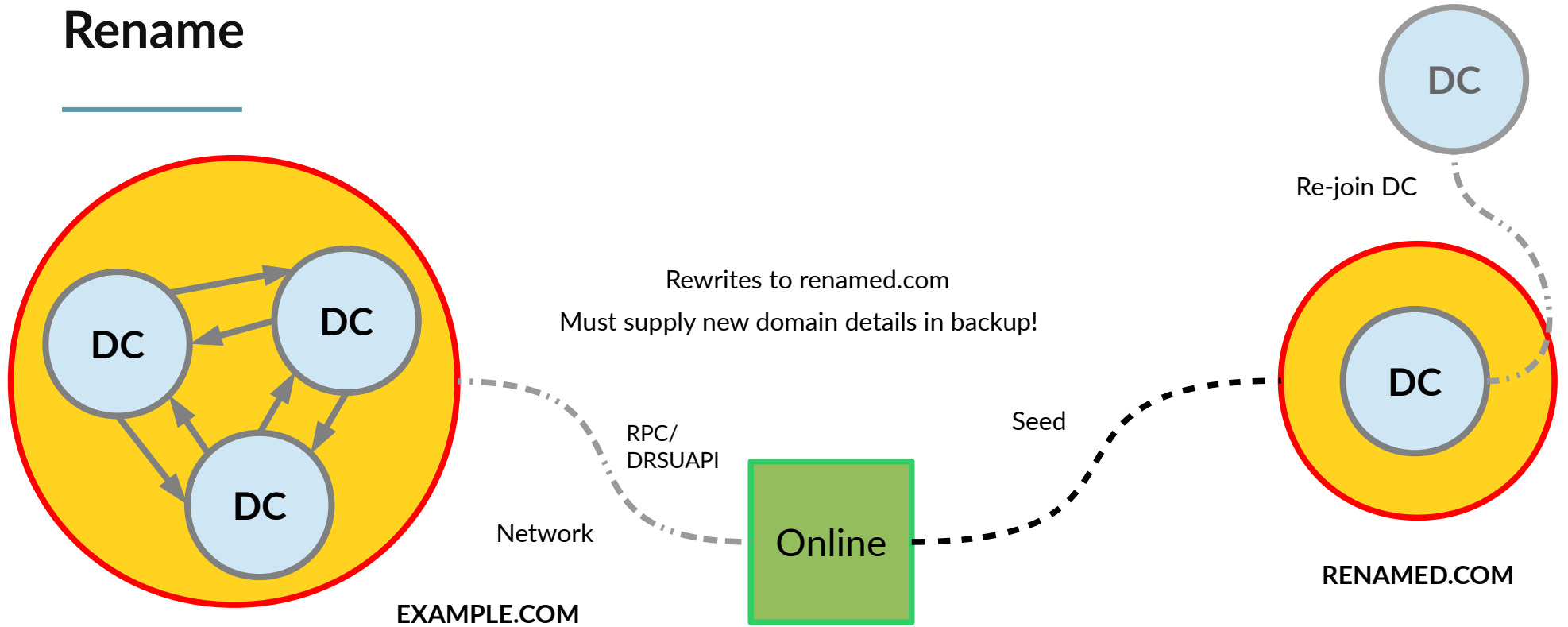
---

Create testing environments and lab domains (without passwords and secrets)

Good for load testing an isolated network



# Rename



`samba-tool domain backup rename`



Tar file



`samba-tool domain backup restore`



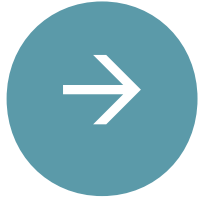
# Final takeaways

---

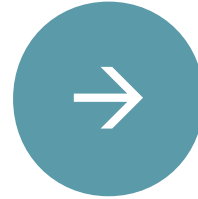
- 1) We've been investing significant amounts of effort into more realistic testing
- 2) Normal tools and rules do not apply (to understand high load and concurrency)
- 3) Identified new areas for improvement (increase responsiveness, robustness and avoid issues arising in the future)
- 4) Important pieces (backup) that helped deliver the scale and breadth of performance improvements for 4.11 were funded by someone else

# Thanks

...



[garmin@catalyst.net.nz](mailto:garmin@catalyst.net.nz)



[garmin@samba.org](mailto:garmin@samba.org)



[linkedin.com/in/garmin-sam](https://www.linkedin.com/in/garmin-sam)