News from the IT department, how (not?) to move a server room and IT security

PI IT Team

Oliver Freyermuth, Frank Frommberger, *Michael Hübner*, Ernst-Michail Limbach-Gorny, Andreas Wißkirchen, Markus Gruber from FTD IT & more helping hands in projects and from the HISKP IT Team

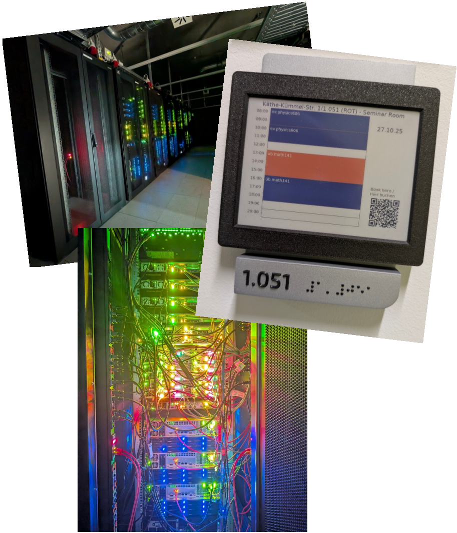
it-support@physik.uni-bonn.de

6th November, 2025

Physikalisches Institut
UNIVERSITÄT BONN

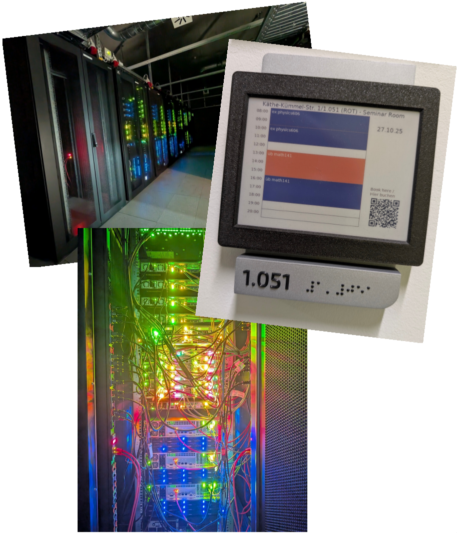
Outline

1. News, Highlights and Numbers of the year
2. Funded IT R&D projects on Research Data Infrastructures
3. How (not?) to move a server room — and all the other rooms and infrastructure
4. IT Security: A deep-dive with Recollections and Recommendations



Outline

1. News, Highlights and Numbers of the year
2. ~~Funded IT R&D projects on Research Data Infrastructures~~
3. How (not?) to move a server room — and all the other rooms and infrastructure
4. IT Security: A deep-dive with Recollections and Recommendations



Personnel Changes

- FTD IT position finally filled: Welcome, Markus Gruber! ☺

- Daniel Jonas (IT specialist system integration) back with HRZ, best IHK trainee 2025!

Project-specific helpers

- Development for web and database projects: Oliver But
- Research data infrastructure projects: Florian Kirfel
- IT specialist trainees: 3 months every year in cooperation with HRZ

(several personnel changes in the past years also in these projects)

Personnel Changes

- FTD IT position finally filled: Welcome, Markus Gruber! ☺

- Daniel Jonas (IT specialist system integration) back with HRZ, best IHK trainee 2025!

PI Web team

Barbara Valeriani-Kaminski, Florian Kirfel
(coordinating also with FTD, HISKP and department web teams)

Flexible project developers

Antonio Figueiredo

Highlight Projects

Selection of projects

- still ongoing
  - Web development team: ongoing **development of HR system and userportal**
  - Joint project of PI & HISKP IT teams, secretaries, HRZ: **Indico**
  - Development of **common firewall** (HISKP, PI, FTD)
- new in 2025
  - Indico succesfully used for ROT, also in other faculties
  - Autodesk licences: Support for network licenses to be dropped early 2026, solution compatible with data protection being investigated
  - Debian 12 rollout ongoing — sadly, many machines still off after the move, no information from groups about machine locations / status
  - Group mailing lists: Most migrated to `listen.uni-bonn.de` with automated management, groups which did not respond to multiple queries will lose their lists (in next months)
  - New institute member list (rollout to other institutes / 'Fachgruppe' planned) ⇒ Thanks, Markus Gruber!

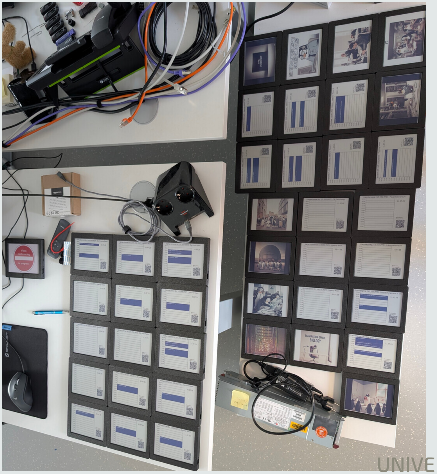
Highlight Projects (continued)

Selection of projects (continued)

- upcoming
  - Migration of subdomain mail addresses `@physik.uni-bonn.de` to new mail system (merge with `@uni-bonn.de`)
    Warning: You have to migrate calendars and or contacts manually!
  - Two-factor authentication with hardware YubiKeys for staff members (TOTP for students)

Highlight Projects: Signage

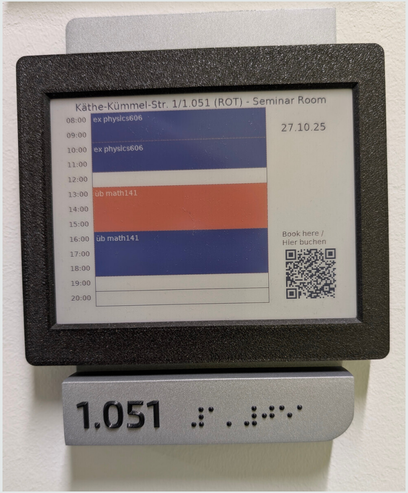
Indico signage



Initial work done by D. Jonas

Highlight Projects: Signage

Indico signage

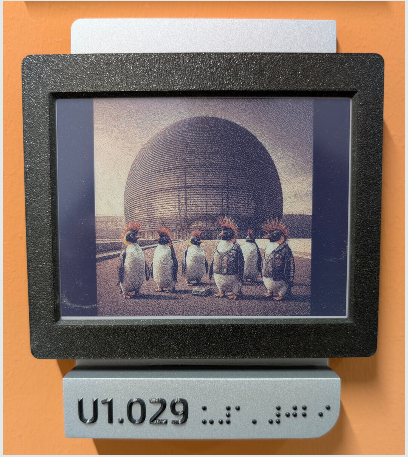


- ePaper refreshing automatically based on room booking data from Indico
- QR code leads to booking page
- Students can use rooms in between courses and tutorials

Initial work done by D. Jonas

Highlight Projects: Signage

Indico signage



- Self-managed content possible for special applications
  - Labs
  - Opening hours of examination office
  - ...

Initial work done by D. Jonas

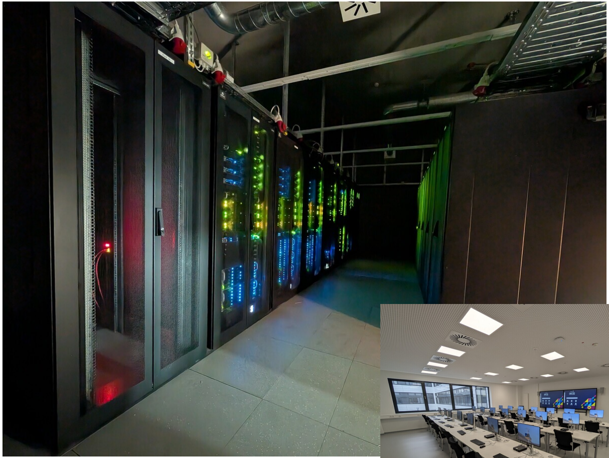
Highlight Projects: Move to ROT, A Room with a View

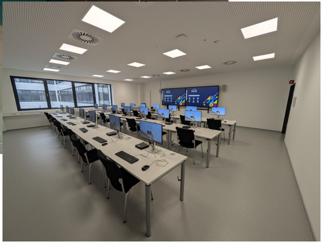
Before. . .

Highlight Projects: Move to ROT, A Room with a View

After. . .

Highlight Projects: Move to ROT





- Server room: New cooling & network technology
- Dedicated printer rooms
- New CIP pool (QV budget), old PCs used for lab classes
- Rooms bookable via Indico (across faculties)
- Largest number of network outlets of all buildings of University of Bonn ($\mathcal{O}(4000)$)

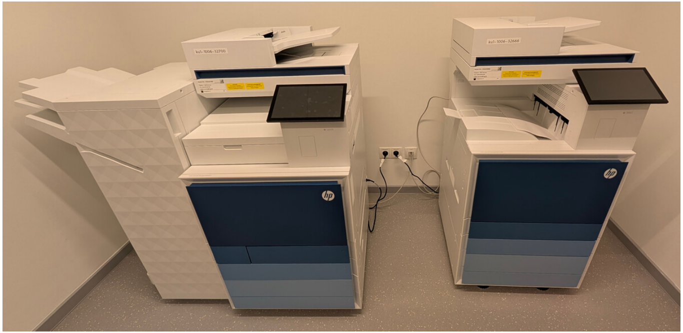
Highlight Projects: New Multi-function Printers

- New contract chosen by central procurement and external company
- Over 40 Xerox printers in total needed to be replaced
- Integration with IAP ⇒ HISKP, FTD, PI, IAP with common printer setup
- Needed to make new HP models work with all OSs in our setup (printers in isolated network, common print server) in a few days
  Printers should have been delivered beforehand, but that seems to have only happened for central administration with homogeneous Windows infrastructure
- Configure scan to mail, fax functionality, security options,. . .
- 3 common models via leasing:
  - smallest models (A4 only) found in secretariats, at one end of the FTD office corridors
  - medium models are the most common models
  - largest models don't look very different, but print much faster (e. g. one in ROT printer room on 1st floor)

Highlight Projects: New Multi-function Printers

Some news

- Printers with finisher can not only perform stapling, but also hole punching!
- New devices are in general faster, and more silent
- Don't try to change toner yourself — compartments are locked.
- Preview of scanned pages right on the device.



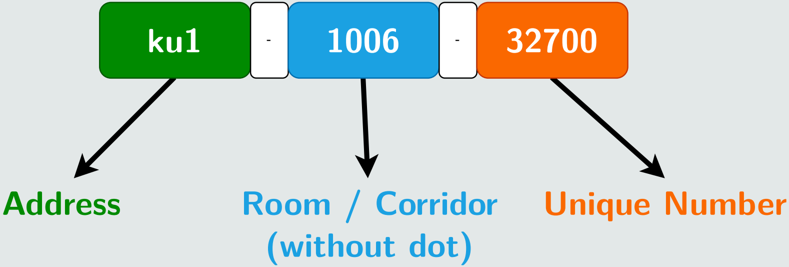
Highlight Projects: New Multi-function Printers

Biggest hurdles

- Windows drivers are not designed for network isolation (always want to contact printer directly)
  Needed to fight our way through wrong documentation until a working approach was found
- Reporting of printed pages and ordering of new toner still not automated yet
  Waiting for replies from new partner company
- In addition to leasing models, some models bought via new contract: Smaller devices in old PI library, FTD secretariat

Highlight Projects: New Multi-function Printers

Unchanged Features



ku1 - 1006 - 32700

Address

Room / Corridor (without dot)

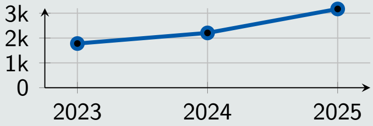
Unique Number

- Printer naming scheme is common and was kept, only last numbers changed
- For managed Linux system: Closest printer is set by default automatically
  Please keep us updated if desktops are moved!
- Documentation on Confluence:
  https://confluence.team.uni-bonn.de/x/LQRY

Some numbers from the past year. . .

- > 70 ↗ 95 procurement requests via IT (with hardware, software and license counseling), in many cases consisting of several orders
- > 408 reinstalled machines (laptops for masterclasses, upgraded servers etc.)
- > 540 ↗ 578 managed Linux systems in total
- > 40 ↗ 79 managed Windows systems in total
- > 48 non-trivial hardware issues (includes 14 broken hard disks in servers)
- newly created tickets (most contain dozens of back-and-forth mails):

1779	from October 2022 to October 2023
2206	from October 2023 to October 2024
3170	from October 2024 to October 2025



(includes about 10 % automatic, but actionable issues per year, excludes merged tickets, excludes most ‘do-you-have-a-minute?’ customers)

Move to ROT: How (not?) to move a server room

Some numbers. . .

- 127 physical servers
  between 10 kg and 40 kg each
- 384 Ethernet ports, i. e. 768 plugs
  Labels on machines and switches (colour scheme), reassignment of switch ports
- 72 Infiniband cables, i. e. 144 plugs
- 16 switch fibre uplinks, i. e. 32 (Q)SFP(+) plugs
- 32 PDUs with monitoring of all phases and residual currents, including alerting
- 4 existing + 1 new UPS, new power adapters required (‘St. Anton distributors’)
- 8 active cool doors with modbus interface, 3 temperature sensors each
- 5 room temperature sensors and below-floor leak sensor

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues?

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)?

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)? ✗
  - Contacting IT transport companies (Germany)?

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)? ✗
  - Contacting IT transport companies (Germany)? ✗
    two said 'yes', and never responded to further queries after receiving more information
  - Contacting local (larger) server retailers?

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)? ✗
  - Contacting IT transport companies (Germany)? ✗
    two said ‘yes’, and never responded to further queries after receiving more information
  - Contacting local (larger) server retailers? ✗
  - Contacting our usual server vendors?

Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)? ✗
  - Contacting IT transport companies (Germany)? ✗
    two said ‘yes’, and never responded to further queries after receiving more information
  - Contacting local (larger) server retailers? ✗
  - Contacting our usual server vendors? ✓
    Two positive responses! Timeframe works for one of them, got direct contact to their partner for setting up new server rooms!
    We usually don’t advertise, but: **TechCare Solutions GmbH**
  - Flexible enough to follow ‘the usual delays’?

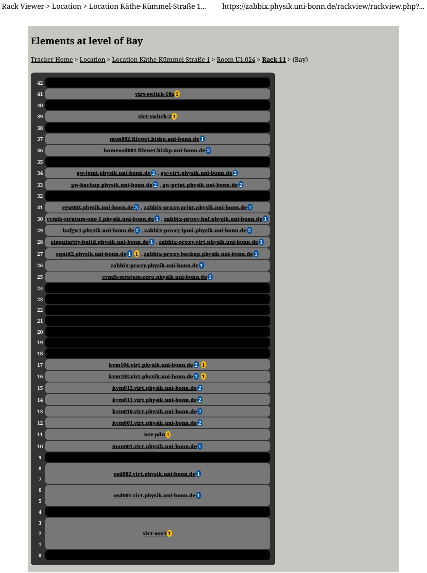
Move to ROT: How (not?) to move a server room

Problem 1

How to move 127 servers in a few days? ⇒ Not alone — would take us weeks. . .

- Search for companies:
  - Asking colleagues? ✗
  - Contacting IT transport companies (locally)? ✗
  - Contacting IT transport companies (Germany)? ✗
    two said 'yes', and never responded to further queries after receiving more information
  - Contacting local (larger) server retailers? ✗
  - Contacting our usual server vendors? ✓
    Two positive responses! Timeframe works for one of them, got direct contact to their partner for setting up new server rooms!
    We usually don't advertise, but: **TechCare Solutions GmbH**
  - Flexible enough to follow 'the usual delays'? ✓
    Initial plan: November 2024, shifted two times, to March 2025!

Move to ROT: Preparations (Rack Plan)



Rack Viewer > Location > Location Käthe-Kümmel-Straße 1... https://zabbix.physik.uni-bonn.de/rackview/rackview.php?...

Elements at level of Bay

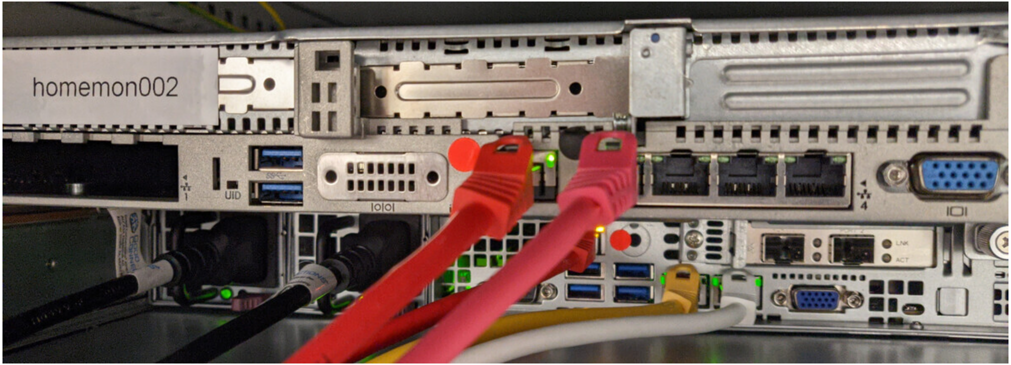
Tracker Home > Location > Location Käthe-Kümmel-Straße 1 > Room U1.024 > **Rack 11** > (Bay)

42	
41	virt-switch-10g 1
40	
39	virt-switch-2 1
38	
37	mon002.filenet.hiskp.uni-bonn.de 1
36	homeosd002.filenet.hiskp.uni-bonn.de 2
35	
34	gw-ipmi.physik.uni-bonn.de 2 , gw-virt.physik.uni-bonn.de 2
33	gw-backup.physik.uni-bonn.de 2 , gw-print.physik.uni-bonn.de 2
32	
31	rgw002.physik.uni-bonn.de 2 , zabbix-proxy.print.physik.uni-bonn.de 1
30	cvmfs-stratum-one-1.physik.uni-bonn.de 1 , zabbix-proxy.baf.physik.uni-bonn.de 1
29	bafgw1.physik.uni-bonn.de 2 , zabbix-proxy-ipmi.physik.uni-bonn.de 2
28	singularity-build.physik.uni-bonn.de 1 , zabbix-proxy.virt.physik.uni-bonn.de 1
27	squid2.physik.uni-bonn.de 1 1 , zabbix-proxy.backup.physik.uni-bonn.de 1
26	zabbix-proxy.physik.uni-bonn.de 1
25	cvmfs-stratum-zero.physik.uni-bonn.de 1
24	
23	
22	
21	
20	
19	
18	
17	kvm104.virt.physik.uni-bonn.de 2 1
16	kvm103.virt.physik.uni-bonn.de 2 1
15	kvm012.virt.physik.uni-bonn.de 2
14	kvm011.virt.physik.uni-bonn.de 2
13	kvm010.virt.physik.uni-bonn.de 2
12	kvm001.virt.physik.uni-bonn.de 2
11	usv-pdu 1
10	mon001.virt.physik.uni-bonn.de 1
9	
8	osd002.virt.physik.uni-bonn.de 1
7	
6	osd001.virt.physik.uni-bonn.de 1
5	
4	
3	virt-usv1 1
2	
1	
0	

Machine distribution over new racks

- Including distribution of switches, speed of ports
- UPS distribution
- Optimized total power / heat by rack

Move to ROT: Preparations (LAN port labelling)



Labelling of LAN ports

- All servers are connected to multiple networks
- Example: Management network (red cables)
- Ports labelled with coloured dots

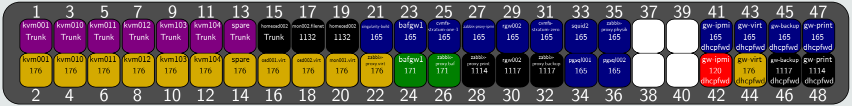
Move to ROT: Preparations (Switch Ports and more)

Rack 11, virt-switch-10g, kuemmel1-1ug-sv-11 (neuer Switch)

● IPMI
● VLAN 176 (Virt)
● VLAN 165 (GPN PI)
● VLAN 171 (BAF2)
● Trunk / other

"kvm"-Trunk: 117, 120, 160, 165, 171, 172, 174, 176, 1102, 1111, 1112, 1113, 1114, 1117, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1128, 1129, 1130, 1131, 1132, 1133, 1144

"Filenet"-Trunk: 174, 1111, 1112



1	kvm001	Trunk	2	kvm001	176
3	kvm010	Trunk	4	kvm010	176
5	kvm011	Trunk	6	kvm011	176
7	kvm012	Trunk	8	kvm012	176
9	kvm103	Trunk	10	kvm103	176
11	kvm104	Trunk	12	kvm104	176
13	spare	Trunk	14	spare	176
15	homeosd002	Trunk	16	osd001.virt	176
17	mon002.filenet	1132	18	osd002.virt	176
19	homeosd002	1132	20	mon001.virt	176
21	singularity-build	165	22	zabbix-proxy.virt	176
23	bafgw1	165	24	bafgw1	171
25	cvmfs-stratum-one-1	165	26	zabbix-proxy.baf	171
27	zabbix-proxy-ipmi	165	28	zabbix-proxy.print	1114
29	rgw002	165	30	rgw002	1117
31	cvmfs-stratum-zero	165	32	zabbix-proxy.backup	1117
33	squid2	165	34	pgsql001	165
35	zabbix-proxy.physik	165	36	pgsql002	165
37			38		
39			40		
41	gw-ipmi	165 dhcpfwd	42	gw-ipmi	120 dhcpfwd
43	gw-virt	165 dhcpfwd	44	gw-virt	176 dhcpfwd
45	gw-backup	165 dhcpfwd	46	gw-backup	1117 dhcpfwd
47	gw-print	165 dhcpfwd	48	gw-print	1114 dhcpfwd

- 'Graphical' (colour coding) and of course taking port speeds into account
- Prepare data tables for switch configuration
- Prepared as A3 paper printouts for the move helpers

Other preparations

- Move all VMs and most storage to FTD and HISKP before the move
  ⇒ minimize downtime for web services, print service etc.
- Reduce unused ports, e. g. old virtualization infrastructure

Move to ROT: No RCDs in new server room

- No residual current devices in new server room ('Fehlerstromschutzschalter')
- Safety instructions needed: Danger of electric shock
- GLT monitoring & monitoring by PDUs
- Before our office move to ROT, we found the room unlocked almost every second day, even when servers were inside...

Missing in 'completed' building

- Signaling of residual current
- Working cooling
- Temperature-driven shutdowns
- Emergency switches not connected

Move to ROT: (Not so) short timeline

March 10th

- First TÜV check of new server room, some complaints found, but can be operated
- Most network switches moved and cabled — some unexpected changes. . .
  Great support by computing centre in taking switches online quickly!
- Gateways for internal networks (Backup, virtualization etc.) moved and back online

March 11th

- Half of the firewall system moved over, failover done, all internet traffic now via ROT!
  User-facing: Short interruption of internet traffic.
- Basic monitoring operational again.
- Debugging of networking issues (partially due to more modern switches / switch updates).

Move to ROT: (Not so) short timeline

March 12th & 13th

- Old virtualization infrastructure moved (for monitoring)
- Accompanied by some defects, e. g. empty CMOS battery, broken RAID 1 disk
- Second firewall machine moved over (still off)
- Took network cables from old server room (different lengths needed than anticipated when move was planned in 2024)
- New UPS: Cable attached by ELSA electricians, **many thanks!**

March 14th

- Critical servers now connected to UPS power.
- Extracted InfiniBand cables from old server room.
- Sealed all new racks (air pressure difference needed for cooling).
- All servers now physically in ROT!

Move to ROT: How (not?) to move a server room

Move to ROT: All servers physically in ROT!

Move to ROT: (Not so) short timeline

March 15th & 16th (the weekend)

Took monitoring of active cooldoors via Modbus into operation (monitor fans, air pressure and temperatures, allow to change settings).

March 17th

- Network debugging: Solved issues with internal network gateways, firewall redundant again (special configurations in new switches required).
- In principle, finally ready to start turning on less critical systems. . .

Move to ROT: (Not so) short timeline

March 15th & 16th (the weekend)

Took monitoring of active cooldoors via Modbus into operation (monitor fans, air pressure and temperatures, allow to change settings).

March 17th

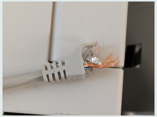
- Network debugging: Solved issues with internal network gateways, firewall redundant again (special configurations in new switches required).
- In principle, finally ready to start turning on less critical systems. . .
- Past 6 PM: Received information that Electricians (company responsible for ROT) plans to fix all issues on March 20th, which will require almost complete shutdown. Accepted the time slot to prevent another shutdown right after all would have been turned on. . .

Move to ROT: Colour Concept at Night

Move to ROT: (Not so) short timeline

March 18th & 19th

- Planning for electrical intervention: Shutdown expected to exceed UPS runtime!
- Work through huge backlog of tickets, some highlights:
  - Several printers with empty toner (unusually high page count these weeks)
  - SSH does not work when machines are off! (several tickets, first when move started)
  - Printer offline. . . maybe due to move, try restart or reconnect cable? I can't. . . ↓
  - Do you have `3.5"` floppy disks for us?
  - Plan reconstruction work for old PI (IT-related)
  - Which AV equipment would be best for our seminar room?
  - I bought a 3D printer. Chose model without LAN. How to connect it?



- Analyze strange behaviour of new UPS (sudden switch to bypass / AC power). ⇒ Great support by vendor, actual issue was a temporary short (broken PSU), led to overload of the UPS, broken PSU (central firewall) replaced.

Move to ROT: (Not so) short timeline

March 20th

- Electricians arrived before the agreed-upon time and turned off all power in the server room:
  - All of IT was in their cars and on the road.
  - While 5 UPSs were frantically beeping and dozens of servers made a constant whining audible alarm, they continued their carnage.
  - When we arrived, all UPS batteries were empty and all servers off...
  - Power was on again and all electricians gone, hiding in other parts of the building.
  - Our preparations were for naught...
- Day was spent:
  - turning everything on again & checking for damages
  - reactivating some non-critical base services (which people asked for)
  - organizing the 2nd TÜV check (which will require short shutdowns coverably with UPSs)
  - fixing printer issues

Move to ROT: The effects of unlocked doors and electricians. . .

Move to ROT: (Not so) short timeline

March 21st

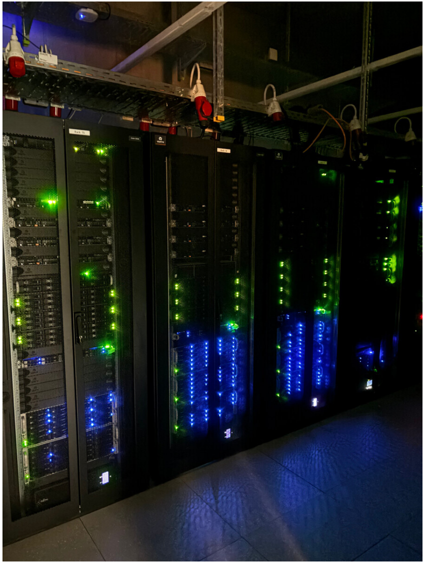
- Produce heat with servers to test cooling infrastructure
- Fix some wrongly connected network cables (company had well over 95 % correct)
- Exchange broken HDD in Backup system
- Digestion of motivational ticket by a group leader:
  Can you please bring back the cluster anytime soon? TÜV checks and other such events should be predictable, why does the cluster need to remain offline?

Move to ROT: (Not so) short timeline

March 24th

- 2nd TÜV check: Successful, several full (short) shutdowns needed as expected.
- Finally turning on most base services
- Fully reactivated Backup system
- BAF: Filesystem problems
  - Ceph needs a quorum of ‘mon’ machines, 2 of 3 had hardware issues, worked around both
  - NVMe drive in one of BAFs file servers temporarily not detected anymore
  - Newly bought active InfiniBand cables do not work with our older hardware. . . Required for worker nodes and file servers!

Move to ROT: BAF2 Ceph trying to deal with half a server ‘gone’



- One NVMe is used for 18 HDDs as DB device for the blocks stored on them ⇒ Bottom left server ‘half-gone’
- If no other disk fails, sufficient redundancy to recover from that (with capacity loss and time)

Move to ROT: (Not so) short timeline

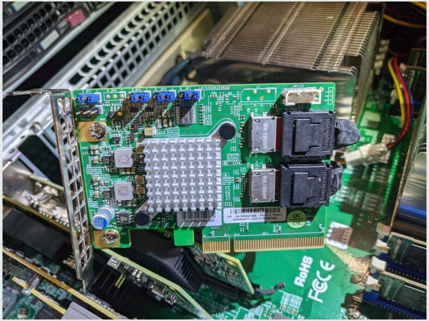
March 25th

- Attempts to get InfiniBand cables to work with firmware updates, no success
- Salvage all old InfiniBand cables from old server room and adapt cabling in ROT
- Turn on most systems apart from desktop login nodes
- BAF: Filesystem problems
  - HDD failure
  - in parallel, NVMe again not detected in one file server (i. e. half server is offline)
  - Critical Situation!

Move to ROT: (Not so) short timeline

March 26th

- Disassembled file server, found one NVMe-cable was mounted in a slightly bent way Assumption: This only became an issue during the physical server move.



- ‘Un-bent’ the cable, ordered a spare. NVMe detected again! ⇒ File system can heal hard disk failure safely!

Move to ROT: (Not so) short timeline

March 26th (continued)

- RAM failure in one worker node → DIMM removed, boots again

March 27th

- BAF file system recovered, replaced defective disk now that everything is stable
- Login desktops reactivated
- BAF opened up for users again

Move to ROT: (Not so) short timeline

April 3rd

- Manufacturer of the racks sends a service technician to investigate some smaller issues and fans making strange noises
- Noises vanished when the technician arrived...

June 2nd

- One of the active fans failed. Monitoring caught it, rack automatically increased airflow via other fans.
- Informed BLB about defect.

Move to ROT: (Not so) short timeline

July 11th

- Technician confirmed: Fan is dead, replacement needed.
- We ordered a spare fan (for quicker replacements in the future) and triggered warranty repair. . .

November 24th

- Technician should come to replace fan. . .

In the meantime, a PDU locked up — the story continues. . .

Move to ROT: We still have to clean out most of the old room. . .

IT Security: Introduction

- Phishing & Spam
- Supply Chain Attacks
- Hosting of Web Applications
- Why to use privilege separation
- Keeping Credentials safe
- 'There's something strange on my machine (or in the neighbourhood)!' — how to act

Phishing & Spam: Sometimes, University-focussed

Still one of the most common and most successful, ‘cheap’ attacks!

Example

```
Von:     Real Professor <realprofessor.b@gmail.com>
Betreff: DRINGEND
Datum:   Di, 23.Jan 2024 07:45:00
An:      <UNIID@uni-bonn.de>

Hallo Vorname!  Bist du verfügbar?

Prof. Dr. Real Professor
Vorsitzender der Fakultät für Physik und Astronomie
Experimentelle Teilchenphysik
#real room number
Nussallee 12
53115 Bonn
```

Phishing & Spam

How is this spam?

- In many cases, no personal data (i. e. no real names), but *was present here!*
- Sender mail address (not name!) was external (`gmail.com` in this case)
  Note: Many mail clients don't show this to you right away!
- Call to action: If you responded, the other end communicated in your language of choice, and finally asked you to buy a gift card...

How to act?

- Stop and think!
- If in doubt, contact the sender via a known official address (or other technology)
- If still in doubt, contact us

E-Mails: Some basics

- The ‘name’ in the `From` field is completely free to choose
- The `From` address is ‘usually’ free to choose (in some cases leads to flagging as spam)
  Problem: Mailing lists usually send mail ‘for you’ and may keep your mail address!
- When accepting mail, a mail server can only check the basic information (no content!) to decide whether to accept it
- Afterwards, further checks can only change whether it is moved to Junk
- The full ‘source code’ shows the path (‘stamps by postmen’) the mail took
  Note: ‘Earlier’ stamps can be faked!

⇒ **E-Mail is in many regards the same as snail mail!**

Phishing & Spam: Sextortion

Example

```
From: My Name <myuniid@uni-bonn.de>
Consider this message as your last warning.
We hacked your system!
We have copied all the data from your device to our own servers.
Curious videos were recorded from your camera and your actions while watching
↪  porn.
Your device was infected with our virus when you visited the porn site.
The Trojan virus gives us full access, allows us to control your device.
...
This information can destroy your reputation once and for all in a matter of
↪  minutes.
You have an opportunity to prevent irreversible consequences.
To do this:
Transfer 1300 $ USD (US dollars) to our bitcoin wallet.
...
```

Phishing & Spam

How is this spam?

- Technically, not impossible, but. . . what do you do in your offices at night? 😉
- Mails sometimes contain ‘proof’, e. g.
  - sent ‘from your own mail address’ (see our mail basics. . .)
  - leaked passwords linked to your mail address which may be real
    Usually old passwords which may not be in use anymore.

How to act?

- Stop and think!
- Keep your passwords unique by use case, and complex (password manager).
- Password managers also allow to reversely search for passwords.
- Change passwords on a ‘safe’ device when leaks become known!

Phishing & Spam: Special Cases

Mailinglist Spam

- Some scammers add a set of ‘related mail contacts’ of companies and customers to a Google Groups mailing list
  sadly, works without you agreeing to this, even though GDPR mandates that. . .
- Inject some mail, e. g. a payment reminder, into the list and watch what happens. . .
- Are any payment details, credit card data etc. leaked? Are the addresses active?
- Only way to get rid of this: Unsubscribe. Some mail clients offer a button, safe way: Check mail source code, which contains an unsubscribe address.
- If in doubt, contact us.

Common ‘calls to action’ with dangerous links

- Quota exceeded, click here to fix!
- Your webmail is disabled, click here to update!
- Please confirm your account is still valid.

Phishing & Spam: Dangerous Links

Usage of ‘twisted’ domain names

What about the URL:

`https://mail.uni-boon.de/login.php?id=c29tZXVzZXIK`

Would you click it? Would you log in?

How to detect dangerous URLs?

- Ideally, never click, but visit the known page and then find your way.
- Hovering over URLs / buttons shows the real link target.
- Common malicious targets:
  - Twisted domains (see above)
  - Cloud storage (e. g. Google Drive etc.)
  - Direct IP address
  - Hacked web page which redirects the request

Many other ways to send spam, continuously evolving!

Supply Chain Attacks

```
pip install my-analysis-software
```

Pop Quiz

What happens?

Ideas

Supply Chain Attacks

```
pip install my-analysis-software
```

Pop Quiz

What happens?

Ideas

- This installs the software I need for my analysis!
- Wait! It also installs the dependencies that software has.
- I can do this again tomorrow and it will lead to the same result — right?
- Please?

Supply Chain Attacks

```
pip install my-analysis-software
```

Pop Quiz

What happens?

Answer?

$\Rightarrow$ **Yes, but. . .**

Supply Chain Attacks

```
pip install my-analysis-software
```

Pop Quiz

What happens?

Real answer

- Usually, `pip` always selects the 'latest and greatest'.
  This can lead to a different result every day!
- 'Python's Cheese Shop': Packages contributed by developers.
- If a developer account is hijacked...
- A single infected package can have huge impact!

UNIVERSITÄT BONN

Supply Chain Attacks

```
pip install my-analysis-software
```

Pop Quiz

What happens?

Recommendations

- Carefully check packages and dependencies!
- Keep dependencies minimal when developing your own code, prefer well-maintained dependencies.
- Fix versions for scientific work, update in a controlled way.
- Check whether results change when upgrading.

Supply Chain Attacks

Can affect any 'package management system' or 'app store' / 'extension store', i. e. may also happen with VSCode extensions, browser extensions, your phone apps, `npm`, Julia packages, Conda packages, Docker containers / layers, Windows or Apple App Store, GitHub. . .

Countermeasures

- Careful choice of packages.
- Don't allow developers to 'push' updates directly to your machine. Use packages vetted by a trusted party, e. g. browser addons from Linux distribution repo.
- Validation by the app store:
  - Technical checks (e. g. automated code scanning).
  - Enforcing external assessments, e. g. annual security assessment.
  - Vetting of developers (e. g. identity check, 2FA, paid accounts. . .).
  - Ensure reproducible builds from public source code.
  - Enforcing signatures of build products.

⇒ Some of these checks disagree with FOSS / independent devs!

Web Applications

Web Applications

- We observe a rising request to deploy self-written web applications
- These are usually developed without contacting us beforehand
- They provide some user interface triggering code execution
- Running this self-developed code on a public page essentially allows remote code execution

Some examples on how this can go wrong...

- Text box which allows to choose a value:
  Browser sends a string containing SQL commands instead ⇒ SQL injection
- Persistent storage allowed e. g. for session data, text:
  Can easily be exploited for file sharing purposes
- Input fields which are effectively evaluated:
  Effective remote code execution possible

Web Applications

Problems with Remote Code Execution

- Attackers gain full control of a machine in University network
- Can easily access (and attack!) internal resources
- Can use system to send spam, attack other sites with Uni Bonn as source, mine Bitcoins etc.
- May also be used to steal credentials or deploy silent, dormant malware

⇒ This is a sad reality: All of this has happened at Universities in the past years!

Some alternatives. . .

- Static pages with dynamic elements (e. g. institute member list: search, filters. . .)
  For example, can use GitLab pages for static content with dynamic Javascript.
- Web assembly (code runs in web browser, full power of programming language)
  Extremely powerful, just recently, Linux kernel ported to web assembly!

Privilege Separation

- Self-managed / lab machines require admin privileges ‘every now and then’
- In many cases, operating systems set up things in an ‘admin-by-default’ way, e. g.
  - Windows account with admin privileges
  - Passwordless `sudo` on Linux
  - macOS user with admin privileges
- Convenient for the user — and an attacker who can directly elevate to admin privileges from your user session.

Recommendations

- Always use a separate admin account with password
- Conscious decision whenever admin permissions are required
- Allows to split responsibilities: Only experienced group admin has password
- Allows to ‘hand over’ machines to next Bachelor generation: Purge user account and data, create new user.

Privilege Separation

Centrally managed machines (i. e. by us)

- Users get no admin privileges whatsoever
- They still do not miss anything:
    - If a software is required, contact us, in most cases, it is already installed
    - We install printers for you
    - We take care of updates etc.
- Already caught many slip-ups this way, e. g. installing ownCloud / NextCloud / CERNBox / Sciebo clients in parallel, software which is only free for private use etc.
- If we install something, it is present on all machines — we don't use admin accounts on individual machines usually.

Privilege Separation

For group admins and developers. . .

- Don’t neglect additional protection mechanisms such as SELinux
  They may be more cumbersome to set up, but offer a significant layer of protection
- Use unprivileged accounts whenever possible, this also works for services, containers etc.
- For shared storage spaces, have one responsible to keep things cleaned up, not everybody needs write access
- For development (e. g. GitLab) think about a merge request / approval workflow

Credential Safety

Pop Quiz

What makes a good password?

Ideas

Credential Safety

Pop Quiz

What makes a good password?

Ideas

- It's long!
- Different character classes.
- One for each service / website.

Credential Safety

Pop Quiz

What makes a good password?

Answer?

⇒ **All of this! And. . .**

Credential Safety

Pop Quiz

What makes a good password?

Recommendations

- Think: ‘How would I brute-force my password?’
  - No dictionary words, no common passwords, also not as parts
  - Long, different character classes
  - ‘Common password’ with extension not ideal: One leak, then part of all passwords known. . .

Credential Safety: Recommendations

- No need to memorize all passwords: Use password managers!
  - Graphical: e. g. Keepass, KeepassXC (installed on machines managed by us)
  - Commandline: e. g. `pass`

  Choose them wisely (don't let the cloud have your passwords!), set a safe encryption password, use 2FA if possible!
- If you need to memorize: Use e. g. first letters of a long, memorable sentence.
- Mail account passwords especially critical, usually allows to reset other passwords!

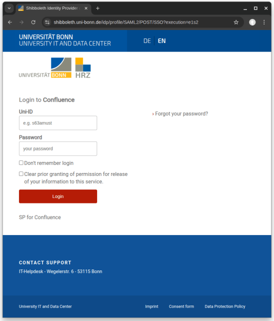
Common Misconceptions

- Regular password changes? ⇒ No gain — especially if need to memorize!
- Long and complex passwords are always safe?
  No, there can be bugs, faulty service setup by admins etc..
- Passwords are stored on all systems I log in to?
  No, passwords are (usually) hashed. Nobody (including yourself) should store your clear-text password (only encrypted in a password manager).

Credential Safety: Recommendations

Where to enter my password

- At Uni Bonn, almost all web services use Shibboleth ⇒
- Most large centres do this, e. g. CERN, DESY
- Some exceptions in our environment exist
- Check URLs and encryption carefully — can you trust the website operator?
- Don't follow links from mails, visit known page directly.



Shibboleth Identity Provider

shibboleth.uni-bonn.de/idp/profile/SAML2/POST/SSO?execution=e1s2

UNIVERSITÄT BONN
UNIVERSITY IT AND DATA CENTER

DE EN

UNIVERSITÄT BONN HRZ

Login to **Confluence**

Uni-ID

e.g. s63amust

Password

your password

› Forgot your password?

□ Don't remember login

□ Clear prior granting of permission for release of your information to this service.

Login

SP for Confluence

CONTACT SUPPORT

IT-Helpdesk - Wegelerstr. 6 - 53115 Bonn

University IT and Data Center

Imprint Consent form Data Protection Policy

Passwordless Approaches

These can help to reduce the impact if your machine is compromised.

- SSH keys? No, please still encrypt them with a passphrase (at least at rest).
- 'Passkeys', i. e. device-specific long-time passwords.
- App passwords, i. e. app-specific passwords (for example for Sciebo).

Incident Response

Something bad has happened. . .

I have installed random software XY from the interwebz and my machine is acting strange. . . what do I (not) do?

What not to do. . .

- Do not ignore the problem.
- Do not continue to use the machine.
- Do not shut it down, reboot, or start a virus scanner.
  This makes forensics harder / impossible!
- Do not contact us from the affected system.

Incident Response

Something bad has happened. . .

I have installed random software XY from the interwebz and my machine is acting strange. . . what do I (not) do?

Actions to take as a user

- **Don't panic!**
- Stop using the machine immediately. Contact us via another system or personally.
- Await further advice — you should assume all credentials entered on an affected system as compromised, so you will need to change your passwords from an unaffected system.
- Watch out for your identity / accounts being misused.
- Check our Confluence page 'Security Incidents' (before the incident, or on another machine).

Example Cases (1): Somewhere in a lab, admin account. . .

'Let me install this helpful Windows taskbar customization tool I always use at home from my USB pendrive. . . '
'License and usage terms? Just click yes, I work with the admin account. . . 😇'

A few weeks later. . .

- DFN contacts HRZ who contact us: Abuse report by other sites: Tons of spam mail sent by a lab machine
- Machine collected and forensics started: Found this started when the app was installed.
- App checked in sandbox: Usage terms stated 'internet access will be shared with others'. . .

Note: Not all apps will state clearly that they do turn your machine into a puppet, but choose your apps wisely!

Example Cases (2): Somewhere in another lab, admin account. . .

‘I have a problem — let’s find an app to solve it. . . ’

App installed from the Windows store

‘It does not work, let’s click help. . . ’

Many pages pop up, they claim the machine is infected!

‘Let me install an antivirus software and scan the full machine, just take the first Google hit, I work with the admin account. . . 😇’

A few minutes later. . .

- Our monitoring picks up unexpected network activity
- We contact the group admin, since we have no updated information about the location of the machine
- Hours later, we are put in contact with the user — who continues working and replies from his mailbox on the potentially compromised machine. . .

Summary

- Move to ROT (server room, CIP pool, offices,. . .) had a huge impact on IT
  We are still not finished, for example labclass moves, upcoming move by theory. . .
- Construction projects are still absorbing a significant fraction of time and energy
- Continuous rise in user requests
- IT security is ever present, and new possibilities mean you must take even more care
  Hopefully, some of our advice will help you out!

Thank you

for your attention!

☕

Funded Projects

Particles, Universe, NuClei and Hadrons for the NFDI

Activities in Bonn:

- JupyterHub frontend for federated Compute infrastructure ('Single Point of Entry')
- Including resources in Bonn in the Compute infrastructure
- Federated storage for 'small' experiments

⇒ half-time for project, handed in midterm report a few weeks ago

FIDIUM

- Federated Digital Infrastructures for Research on Universe and Matter
- Entered new funding phase, preparing for new project call beginning of next year
- Will focus efforts in Bonn on sustainability and checkpointing