Self-Service, SSoT, Firewalls und OIDC

or How we learned to abuse oidc

Steffen Klemer

GWDG

19.03.2024

Wer?

Die GWDG

- Gesellschaft für Wissenschaftliche Datenverarbeitung Göttingen mbH
- Hochschul-RZ der Uni Göttingen
- Cloud-Provider, Hosting und Housing der Max-Planck-Gesellschaft in Deutschland
- Cloud-Provider generell für Bildung und Forschung
- www.gwdg.de

Wir

- **Netzwerk- und RZ-Gruppe der GWDG**
- Steffen Klemer –Technische Leitung Netze - steffen.klemer@gwdg.de

Wir suchen

- **Wir suchen Verstärkung**
- Hiwis, SHK, WHK, 540EUR-Jobs, Ferienarbeit
- Praktika, Abschlussarbeiten
- Stellen
- Leitung Arbeitsgruppe Netzwerk

Es war einmal

- Sicherheitsvorfall führt zur Abschaltung des Switch-Self-Service
  - System eng AD-gekoppelt, Vertrauen unklar
  - Neuaufbau aufwendig
  - Langfristige Strategie sah Ablöse vor
- Also: 2 Wochen konzentriertes Loshaxx0rn

SSo-was?

Single Source of Truth

- GWDG-Netzwerk auf Basis einer SSoT
  - Alle Änderungen mit Protokollierung dort
  - Reale Systeme werden daraus deployt
  - $\rightarrow$ Realität == Dokumentation
- $\rightarrow$ ITIL/ ISO 20001 und ISO 27001 Konformität

Nur Vorteile?

- SSoT besonders(!) schützenswert
- Self-Service bedingt aber einen Zugriff?!
- Was tun?

Self-Service bisher #1

- User haben direkten Zugriff auf “Ihre” Switches
  - Kein Changelog, keine IDM-Anbindung
  - Grob-Granulare Rechtevergabe
  - Rechteausweitung schwierig

Self-Service bisher #2

- User haben Zugriff auf ein Switch-Mgmt-System
  - Kein Changelog, kaum IDM-Anbindung
  - Fein-Granularere Rechtevergabe
  - Rechteausweitung mittelschwer

Self-Service und SSoT

0. Ansehen des aktuellen Zustands
1. Änderung der Doku
2. ggf. Berechnung von Seiteneffekten
3. Deploy der Änderung

Prior Art – Netzportal

- Python-Programmierte Website
- Auf Basis von Python-Bottle (wie Flask)
- Enthielt bereits User-Auth
  - Hinter Shib-SP
  - Anreicherung mit LDAP-Query

Prior Art – Nautobot als SSoT

- Python-Django basierte SSoT, DCIM, Automatisierungs-Plattform
- Switches und Switch-Topologie onboarded mit Ausleseskripten
- Zuordnung von Switchen/ Switchports zu Tenants

Prior Art – IDM-Rollen

- Tracking der Rolle ‘Fachverantwortlich für IT-Netze’ im IDM
- Darstellung über automagische Gruppenzugehörigkeit

```
- FvNetz [orgid]
```

Plan und Umsetzung

Der Plan

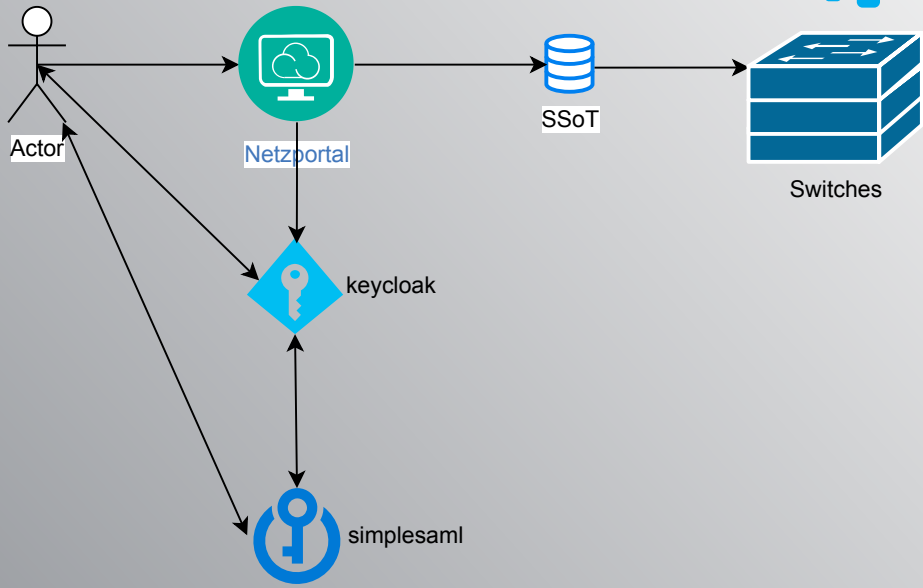


Figure 1: Aufbau

API-Konsum

- Wie greift das Netzportal auf die SSoT zu?
  - REST-API
- Wie autorisiert sich das Netzportal?
  - Mit Admin-Rechten
  - Mit Rechten des aktuellen Users

Vorteile der User Impersonation

- Kein Passwort/ Langzeit-Token auf dem Portalserver
- Selbst bei Programmierfehlern im Netzportal kaum Rechteausweitung möglich
  - maximal auf aktuell aktive User

Gekauft! Aber wie?

- Auth an der SSoT-API mittels Bearer Token
  - entsprechen letztlich den OIDC-Access-Token
  - dafür muss der audience-Claim zur SSoT passen
- `headers={"Authorization": f"Bearer keycloak {OIDC_access_token}}"`

Gekauft! Aber wie? #2

OIDC_CLAIM_sub:	"[redacted]"
OIDC_CLAIM_uid:	"sklemer"
OIDC_CLAIM_email_verified:	"1"
OIDC_CLAIM_goe_id:	"[redacted]"
OIDC_CLAIM_name:	"Steffen Klemer"
OIDC_CLAIM_groups:	"GWDG cloud-user-communications,FvNetz UNI,C
OIDC_CLAIM_preferred_username:	"[redacted]"
OIDC_CLAIM_given_name:	"Steffen"
OIDC_CLAIM_family_name:	"Klemer"
OIDC_CLAIM_email:	"steffen.klemer@gwdg.de"
OIDC_CLAIM_exp:	"1710661620"
OIDC_CLAIM_iat:	"1710661320"
OIDC_CLAIM_auth_time:	"1710661070"
OIDC_CLAIM_jti:	"[redacted]"
OIDC_CLAIM_iss:	"https://keycloak.sso.gwdg.de/auth/realms/ac
OIDC_CLAIM_aud:	"gwdg-netzportal-prod,nautobot"
OIDC_CLAIM_typ:	"ID"
OIDC_CLAIM_azp:	"gwdg-netzportal-prod"
OIDC_CLAIM_nonce:	[redacted]
OIDC_CLAIM_session_state:	
OIDC_CLAIM_at_hash:	
OIDC_CLAIM_sid:	
OIDC_access_token:	
OIDC_access_token_expires:	"1710661620"

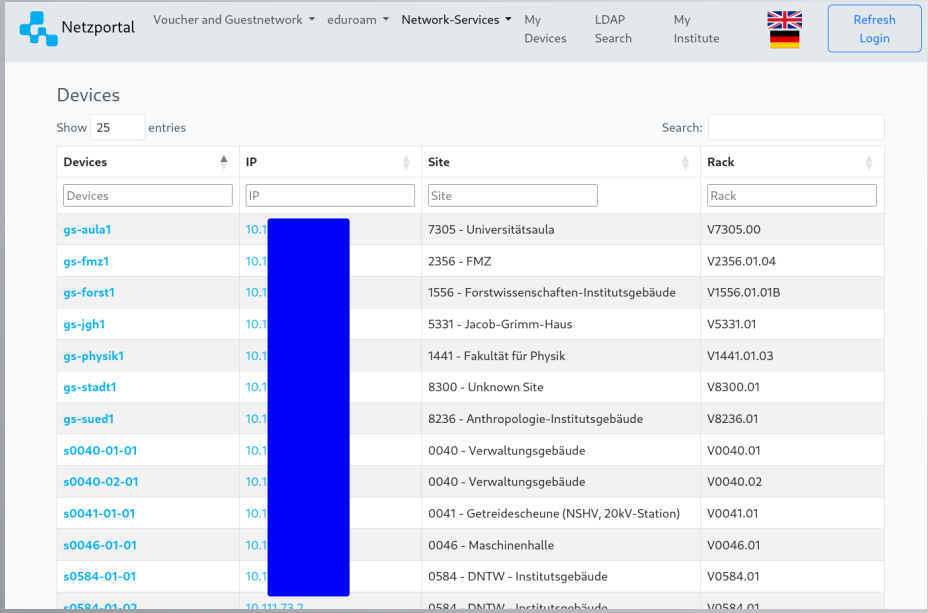
Figure 2: OIDC Claims

Alles Zusammen

1. User geht auf netzportal.gwdg.de/switches
2. User wird redirected zum SSO, meldet sich an, Redirect zurück
3. `mod_auth_openidc` verwendet den authcode, um ID-Token, Access-Token und Refresh-Token zu holen
   - der ausgestellte Access-Token enthält zusätzlich die SSoT im `aud`
4. Netzportal stellt API-Anfrage an die SSoT mit dem Access-Token als Bearer-Token
5. SSoT:
   - checkt den Token
   - Legt ggf. fehlende Tenants/ Gruppen an und setzt Rechte
   - Prüft, was der User tun darf; liefert Antwort
6. Netzportal stellt alles schick dar

In Bunt

Switchübersicht



Portübersicht

Device info

Name	**gs-aula1**
IP	10.[redacted]
Type	HP/Aruba 5406Rzl2 (J9850A)
Role	GÖNET-Switch
Site / Rack	[redacted]
Detailed Location	[redacted]

Live info

Device State	**Up**
Last Device Reboot	2022-10-12 at 16:47
Last Poll	2024-03-17 at 08:37
Last Discover	2024-03-17 at 08:05

change untagged VLANs

Show 53 entries Search:

S	Port	LAG	Type	Speed	Untagged VLAN	Tagged VLANs (mouse over VL for name)	Last State Change	Traffic Sum	Cable	Cable Peer
	Pc	L/	Ty	Spe	Untagge	Tagged VLANs	Last Stat	Traffi	Cat	Cable Pee
U	A1		Other	1G	**1** - default	168, 181, 300, 302, 306, 1111, 1734, 3128	2023-10-26 12:31	13.2 TiB	**Yes**	s6384-01-01 / Port 50
U	A2		Other	1G	**1** - default	48, 60, 162, 181, 300, 580, 1111, 1734, 1913, 2813, 2873	2023-10-06 09:22	9.1 TiB	**Yes**	s6368-01-01 / Port 48
U	A3		Other	1G	**1** - default	48, 60, 162, 181, 300, 302, 580, 667, 1111, 1734, 1913, 3126	2023-12-04 14:05	654.7 GiB	**Yes**	s6392-01-01 / Port 26
U	A4		Other	1G	**181** - aula	62, 168, 300, 302, 304, 1111, 1738, 1913, 2813, 3123, 3128	2022-10-12 16:49	20 TiB	**Yes**	s7307-01-01 / Port 48
U	A5		Other	1G	**168** - UVN	60, 162, 202, 302, 304, 306, 307, 480, 518, 519, 570, 1111, 1231, 1732, 1913, 2813	2022-10-12 16:49	45.2 TiB	**Yes**	s7384-01-01 / Port 52

VLAN-Form

☐	**D6**	*(Other)*	default (1) (not re-setable by you!)
☐	**D7**	*(Other)*	default (1) (not re-setable by you!)
☐	**D8**	*(Other)*	default (1) (not re-setable by you!)
☐	**or:** Bulk change checked ports to VLAN		

Why do you want to change this? *Changes without a good explanation might be rolled back!*
Die Begründung des Changes kann in Deutsch oder Englisch geschrieben werden.

Arbeitsplatz wird jetzt durch Gruppe Y genutzt
Outlet now used for a microscope
Ticket-ID 42 in our system
Nach Beschluss von X wird der Raum zu einem Labor umgebaut
...

Cancel | Save Changes

Nachfrage

Submit this change?

The following things will be changed

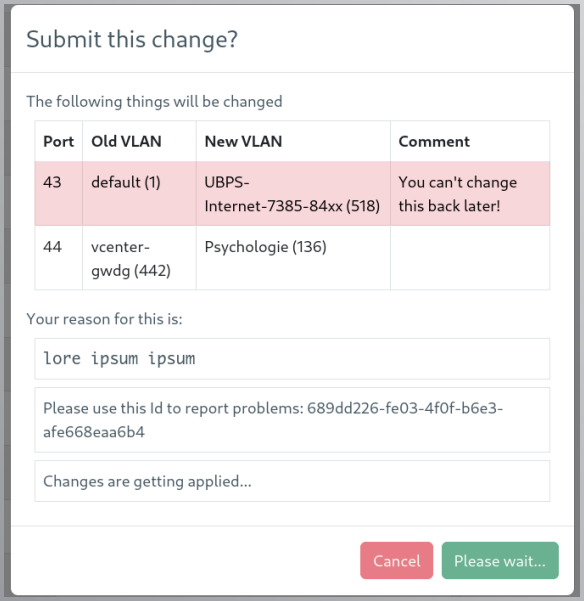
Port	Old VLAN	New VLAN	Comment
43	default (1)	UBPS-Internet-7385-84xx (518)	You can't change this back later!
44	vcenter-gwdg (442)	Psychologie (136)	

Your reason for this is:

```
lore ipsum ipsum
```

Cancel | Submit the request

Warten


Submit this change?
The following things will be changed
Port
Old VLAN
New VLAN
Comment
43
default (1)
UBPS-Internet-7385-84xx (518)
You can't change this back later!
44
vcenter-gwdg (442)
Psychologie (136)
Your reason for this is:
lore ipsum ipsum
Please use this Id to report problems: 689dd226-fe03-4f0f-b6e3-afe668eaa6b4
Changes are getting applied...
Cancel
Please wait...

VLAN geändert

Submit this change?

The following things will be changed

Port	Old VLAN	New VLAN	Comment
43	default (1)	UBPS-Internet-7385-84xx (518)	You can't change this back later!
44	vcenter-gwdg (442)	Psychologie (136)	

Your reason for this is:

```
lore ipsum ipsum
```

Please use this Id to report problems: 689dd226-fe03-4f0f-b6e3-afe668eaa6b4

VLAN successfully changed.

Cancel Close

too long; didn’t listen

tl;dl

- OIDC funktioniert
- OIDC ist einfacher, als man denkt
- Acces-Token für User-Impersonation bringen Sicherheit
- GWDG hat mit etwas Python, Nautobot und mehr Python VLAN-Service auf Procurve-Switches gebaut