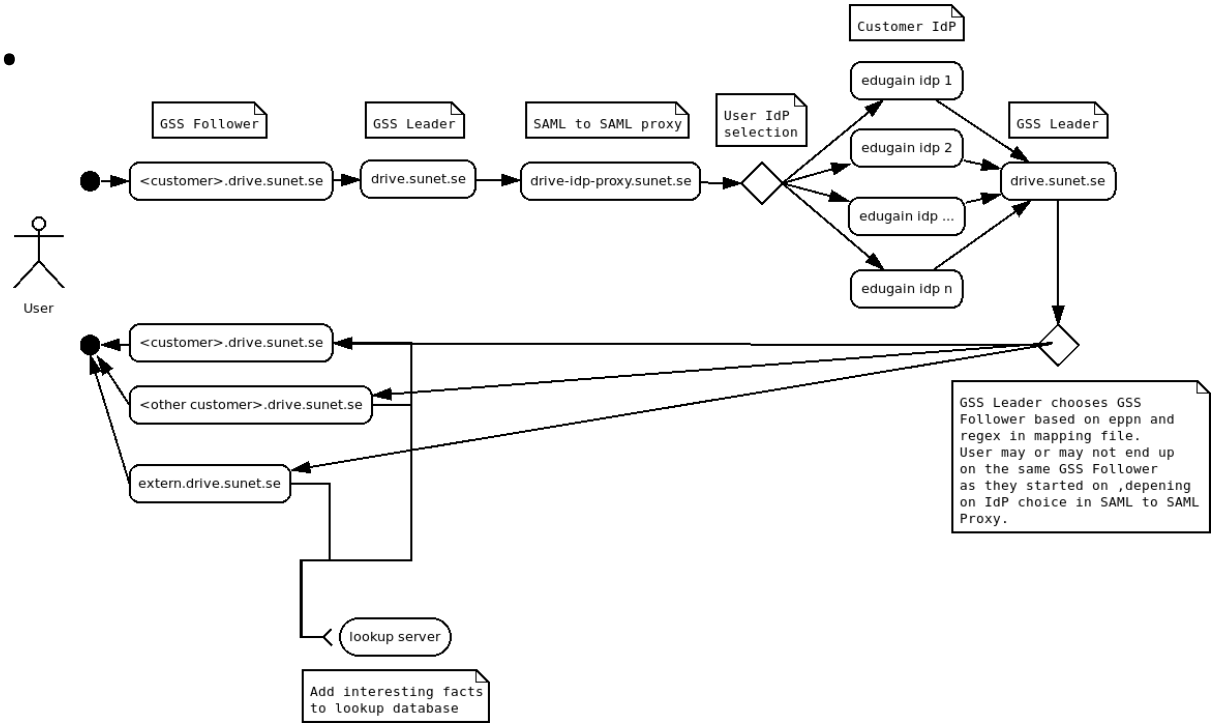
Sunet dagarna 2024

Sunet Drive - MFA på djupet

Micke Nordin kano@sunet.se
Richard Freitag freitag@sunet.se
Magnus Andersson mandersson@sunet.se

Sunet Drive - MFA på djupet

MFA är ett enkelt problem med en svår lösning.



SUNET

Historik

Sedan starten har det varit möjligt att använda Drive med MFA:

- ✔️ Via Nextcloud med lokala konton
- ✔️ Via IdP med SSO-konton

SUNET

Historik

Sedan starten har det varit möjligt att använda Drive med MFA:

- ✔️ Via Nextcloud med lokala konton
- ✔️ Via IdP med SSO-konton
- ❌ Via Nextcloud med SSO-konton

SUNET

Historik

Vår äldsta användarfeedback:

❌ Via Nextcloud med SSO-konton

✔️ Via Nextcloud med SSO-

#	TITLE	CUSTOMER	GROUP	OWNER	CREATED AT
9616455	Step-up MFA with Saml/sso	Richard Freitag	Support	Julius Härtl	15.12.2020

SUNET

Problemet

Nextcloud menar att SSO betyder att IdP:n ska hantera allt som har med inloggning att göra.

Ingen vill slå på MFA i sin IdP...

SUNET

Problemet

Varför vill ingen ha MFA i IdP:n?

Gäller ofta alla användare, på alla siter, som använder SSO.

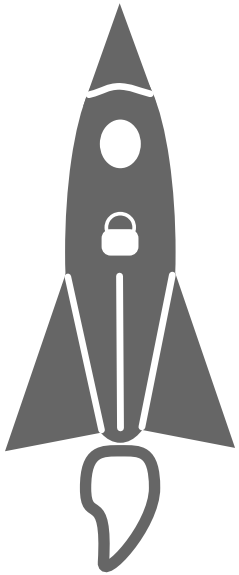
Kan vara knepigt att implementera.

SUNET

Lösningen

En ny Nextcloud app utvecklad av Sunet.

https://github.com/SUNET/nextcloud-stepup-auth/



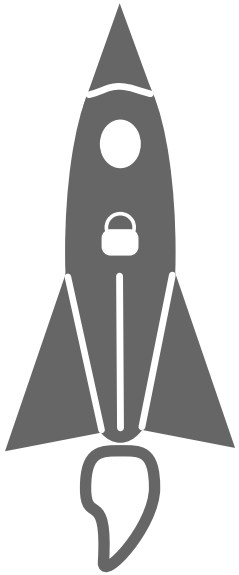
SUNET

Step up auth

✔️ Använder bara publika API:er.

✔️ Bygger på enkla, stabila, mekanismer.

✔️ Återanvänder Nextclouds inbyggda funktionalitet.

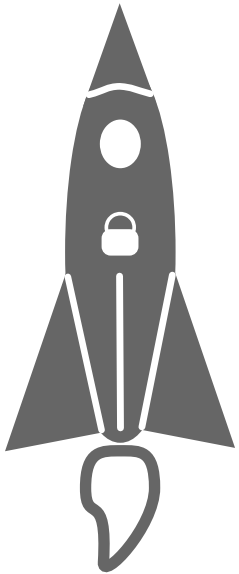


SUNET

Step up auth

Kan göras tvingande för:

- alla
- grupper
- enskilda användare



Möjligör alltså att vissa användare kan avkrävas MFA, medan andra slipper.

SUNET

Vidareutveckling

Ytterligare en app från Sunet:

https://github.com/SUNET/nextcloud-mfazones/

SUNET

MFA Zoner

✔️ Använder bara publika API:er.

✔️ Bygger på enkla, stabila, mekanismer.

🌟 Lägger till ny funktionalitet genom
ramverket för filaccess.

SUNET

MFA Zoner

Har beroenden på:
- files access control
- files automated tagging
- (step up auth – endast för SSO)

Fungerar inte med:
- global site selector*

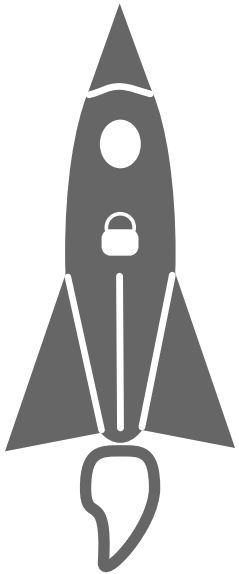
* ännu: https://github.com/nextcloud/globalsiteselector/pull/150

SUNET

Helheten

1. Användaren loggar in
 – Event listener i Step up auth säkerställer att en andra faktor anges.

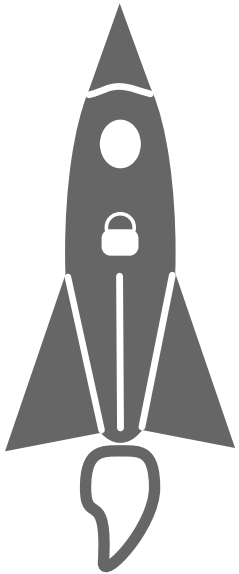
2. Användaren accessar en katalog
 – Event listner i mfazones kör en check, work flow engine garanterar att katalogen inte kan accessas om inte checken har gått igenom.



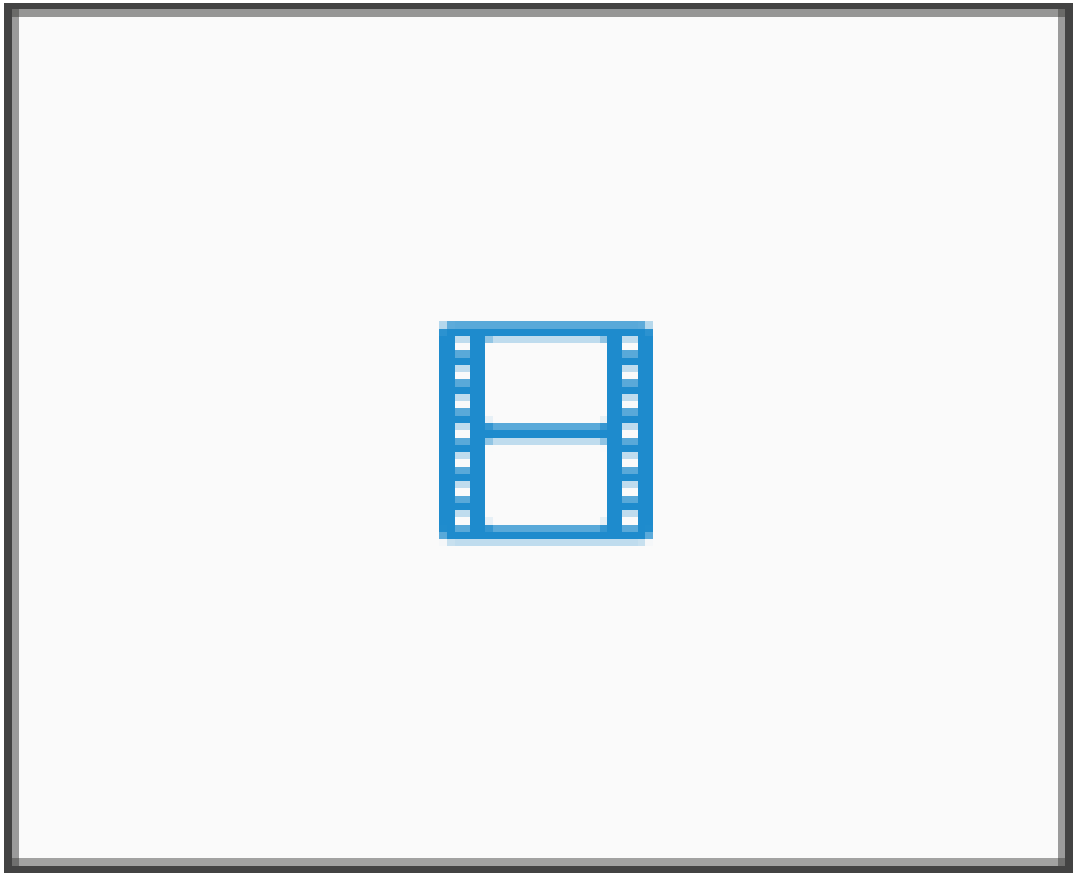
SUNET

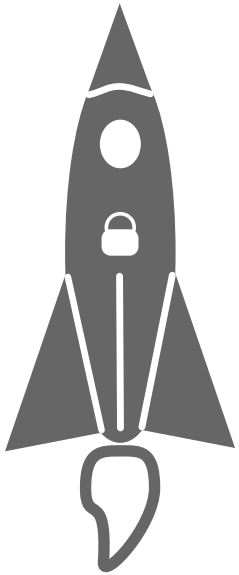
Helheten

3. Användaren markerar en mfazon – Systemtaggar i Nextcloud används för att markera en katalog som mfazon.



Demo





SUNET

Säkerhetsgranskning

Inledningsvis togs konsulthjälp in för att ta fram lösningen.

Lösningen har säkerhetsgranskats i två omgångar.

Första granskningen hittade två sårbarheter rankade medium och en rankad låg och appen har sedan dessa till stora delar skrivits om av Sunets egen personal. Vid senaste säkerhetsgranskningen har inget framkommit som ger anledning till oro och lösningen kan därför slås på i Sunet Drive, efter beställning.

SUNET

Säkerhetsgranskning

”The auditors tried to bypass MFA and Step-up authentication but failed. So, even though the efforts were made, our conclusion is that the quality is outstanding regarding the main target of the audit”

triop

SUNET

Frågor?

Micke Nordin kano@sunet.se
Richard Freitag freitag@sunet.se
Magnus Andersson mandersson@sunet.se