

NB: Een vertrouwelijke versie van dit document is op aanvraag beschikbaar. Deze bevat meer informatie over beveiliging bevindingen.

Test Connectivity Yoda vanuit SURF ResearchCloud

Use-case:

Vanuit een workspace van SURF ResearchCloud willen we persistente data kunnen benaderen die opgeslagen wordt in Yoda, zodat deze data in SRC geanalyseerd kan worden.

Development activiteiten uitgevoerd in kader van DCC-2020 project:

De Yoda software is aangepast om voor WebDAV connectiviteit een token-based access te ondersteunen. Deze feature is opgenomen in pre-alpha versies van Yoda 1.8. Wij hebben in onze testen van deze pre-release gebruik gemaakt.

TEST 1: Algemene connectiviteit SRC -Yoda

We configureren onze WebDav koppeling met Yoda alsof het ResearchDrive betreft.

Voor configuratie volgen we de documentatie op de SURF wiki:

<https://servicedesk.surfsara.nl/wiki/display/WIKI/Connect+Research+Drive>

Als CO gebruiken we “rdms-innovation t Experiment” waar nog geen drive aan gekoppeld is.

- a) “Use SURF’s Researchdrive” uitvinken
- b) URL = “<https://145.100.59.141.surf-hosted.nl:8080/>” (Yoda disk adres van test omgeving)
- c) Username = “researcher1”
- d) Password = (wachtwoord dat user researcher1 gebruikt voor inloggen in Yoda portal)

We controleren door met een browser naar de disk te navigeren of de Yoda disk bereikbaar is: er blijkt een self-signed certificaat op geïnstalleerd te zijn, wat zorgt voor een waarschuwing door de browser. We moeten handmatig een security risico accepteren alvorens toegang te krijgen. Daarna laat onze browser de Yoda folders/bestanden goed zien.

Vervolgens maken we in SRC portal een “iCommands” applicatie workspace aan van onze CO.

Met ssh verbinden we met deze workspace. In de folder “~/researchdrive” verwachten we Yoda folders te zien maar het mounten is mislukt.

In de file `/var/log/research_drive.log` van de workspace staat:

```
*** Mon Oct 18 06:56:36 2021
*** Mon Oct 18 06:56:36 2021
*** Mon Oct 18 07:00:33 2021
*** Mon Oct 18 07:00:33 2021
*** Mon Oct 18 07:00:33 2021
*** Mon Oct 18 07:00:33 2021
*** Mon Oct 18 07:01:34 2021
*** Mon Oct 18 07:01:34 2021
*** Mon Oct 18 07:04:32 2021
researcher1 https://145.100.59.141.surf-hosted.nl:8080/
*** Mon Oct 18 07:04:32 2021
/sbin/mount.davfs: Mounting failed.
Server certificate verification failed: issuer is not trusted
*** Mon Oct 18 07:08:01 2021
*** Mon Oct 18 07:08:01 2021
```

Bevindingen:

- verbinding lijkt gemaakt te worden maar self-signed certificaat wordt afgewezen

Actie: Het public server certificaat van Yoda geplaatst in de workspace in file `/etc/davfs2/certs/yoda.pem` en in de configuratie file `etcdavfs2/davfs2.conf` een regel toegevoegd: `"trust_server_cert /etc/davfs2/certs/yoda.pem"`.

De workspace een reboot gegeven (via in pauze zetten en resumen). Nu wordt certificaat wel geaccepteerd en zijn de Yoda folders beschikbaar onder de home dir van de user.

TEST2: Yoda webdav token gebaseerde connectie

In de Yoda portal genereren we als ingelogde user "researcher1" een data access password (drop-down box met gebruikersnaam rechtsboven openen, kiezen voor "data access password"). Dit token heeft een geldigheidsduur van 72 uur wordt ons gemeld.

Updaten van het password in SRC portal blijkt niet mogelijk. Daarom verwijderen we de ingestelde drive link en stellen deze opnieuw in, nu met het gegeneerde token als password.

We herstarten de workspace om zeker te zijn dat de nieuwe credentials gebruikt zullen gaan worden. Resultaat is dat de Yoda folders zichtbaar zijn onder de home dir van de workspace gebruiker.

Algemene bevinding

De WebDav koppeling tussen SURF Research Cloud en SURF ResearchDrive heeft kwetsbaarheden die we separaat aan SURF gemeld hebben. Oplossen van kwetsbaarheden zal nodig zijn voordat de koppeling door UU in productie kan worden genomen.

Conclusies

1) Het is in principe mogelijk om een workspace te laten verbinden met Yoda in plaats van Researchdrive. Daarbij kan ook een Yoda data access password gebruikt worden.

De koppeling wordt per gebruiker ingesteld per CO. Het aantal te linken drives is beperkt tot een.

2) De features in SRC zijn nog onvoldoende uitgewerkt voor productie doeleinden:

- er zijn kwetsbaarheden geconstateerd in de beveiliging
- er ontbreekt een voorziening om tokens gemakkelijk te kunnen updaten
- er ontbreekt een voorziening om meerdere drives te kunnen linken en de naam van een link te kunnen instellen (nu ontstaat er altijd een folder 'researchdrive' in de homedir van de gebruiker).
- wanneer mounten van de disk in een workspace mislukt is dat voor de gebruiker niet te duiden, anders dan dat de 'researchdrive' folder in de home directory leeg blijft. Het zou goed zijn (ook voor het kunnen ondersteunen van de gebruiker) als er in de home directory van de gebruiker een logfile ontstaat met daarin een kopie van de relevante logregels in `/var/log/research-drive.log`.

3) De geldigheidsduur van het data access password in Yoda is erg kort voor praktische toepassing. De geldigheid is momenteel 72 uur. Dit betekent dat analyse jobs in een workspace die langer dan 72 uur duren hun connectiviteit kunnen gaan verliezen. Advies is de geldigheidsduur van het token tenminste een maand te laten zijn.

Getest: 18-oct-2021 door Ton Smeele.