Een non-web usecase: COmanage in combinatie met YODA

Amsterdam, december 2017
Versienummer: 1.0

Colofon

Een non-web usecase: COmanage in combinatie met YODA

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Auteurs
Harry Kodden - SURFsara

Reviewers
Ton Smeele - SURFsara
Gerben Venekamp – SURFsara
Michiel Schok – SURFnet (projectleider)

december 2017

Samenvatting

YODA (Your Data) is een data-opslag applicatie die binnen de Universiteit Utrecht gebruikt wordt om het samenwerken tussen onderzoekers te faciliteren. Authenticatie gebeurt primair tegen de Active Directory van de universiteit, voor gebruikers van buiten de instelling wordt een systeemaccount aangemaakt. In dit document is een mogelijke uitbreiding beschreven om YODA te ontsluiten op basis van federatieve accounts voor gebruikers van buiten de Universiteit Utrecht.

Case

Binnen de Universiteit Utrecht wordt een maatwerk toepassing (YODA) gebruikt waarmee gebruikers (primair onderzoekers) samenwerken en in staat zijn om alle bestanden en publicaties met elkaar te delen in een gecontroleerde omgeving. Hiervoor wordt gebruik gemaakt van Open Source iRODS software[1]. De hoofdonderzoeker is in staat om zijn team samen te stellen (organiseren van instroom en uitstroom van gebruikers).

De applicatie YODA is gerealiseerd 'on-top-off' de onderliggende iRODS systeem-architectuur. YODA bestaat uit een webgebaseerd portal en een WebDAV-voorziening. De eerste wordt met name gebruikt voor inrichting en beheer van de samenwerkingsstructuur en de catalogisering (metadatering) van de geproduceerde publicaties en onderzoekdata. De tweede is voor dagelijks gebruik waarbij de gebruikers een constante netwerkverbinding hebben met het YODA-samenwerkingsverband (deze verbinding is typisch een macOS Finder verbinding, danwel een Microsoft Internet Explorer verbinding). De gebruiker kan zodoende heel gemakkelijk bestanden gebruiken en delen binnen het samenwerkingsverband.

Bovenstaande functionaliteit werkt naar tevredenheid. Er is wel een 'maar'. Gebruikers zijn afhankelijk van de eis dat ze moeten kunnen 'inloggen' op de onderliggende iRODS toepassing.

Authenticeren ten behoeve van iRODS gebeurt door een Pluggable Authentication Module (PAM)[2] die draait op de iRODS-server.
De PAM-stack bestaat uit 2 succes-flows:

1. Gebruikers die via de PAM_LDAP route succesvol kunnen aanmelden tegen Universiteit Active Directory (hierin staan alle medewerkers van de UU met hun zogenaamde 'solos' account)
2. Gebruikers waarvoor op de iRODS-server een 'systeem account'(userid+password) is aangemaakt en die daarmee dus via de standaard PAM-auth module kunnen inloggen. Deze route wordt momenteel gebruikt voor alle externe gebruikers, dus gebruikers die niet beschikken over een 'solos' account van de UU)

Probleem

Hiermee is het probleem goed in beeld. Er is een groep van externe gebruikers, waarvoor het zeer arbeidsintensief is om systeem-accounts op de iRODS-server aan te maken en te beheren (retentie, wachtwoord management, deprovisioning etc). Om de verwachte verdere toename van externe gebruikers te kunnen accommoderen is het wenselijk om federatieve identiteiten te kunnen gebruiken. Voor webgebaseerde applicaties zou dit eenvoudig met SAML of OpenIDconnect kunnen, maar omdat

[1] https://irods.org , Open Source Data Management Software
[2] https://wiki.archlinux.org/index.php/PAM , Pluggable Authentication Modules, https://en.wikipedia.org/wiki/Pluggable_authentication_module

voor de functionaliteit van datatransfers binnen iRODS geen webprotocollen gebruikt worden (maar bijvoorbeeld WebDAV) is dat geen optie.

Uitdaging

De uitdaging bestaat uit het realiseren van de volgende functionaliteiten:

a) Mogelijkheid voor onderzoeker om een gebruiker uit te nodigen voor deelname aan een onderzoeksverband (“Enrollment”). Hierbij mag het niet uitmaken of de gebruiker intern (binnen de UU) of extern is;
b) Mogelijkheid voor die nieuwe gebruiker om in te loggen bij YODA (/iRODS) zonder dat daarvoor (handmatig) een systeem account moet worden aangemaakt. (“Authenticatie”);
c) Mogelijkheid voor onderzoeker om een (externe-) onderzoeker af te voeren van deelname (“Deprovisioning”);
d) Mogelijkheid voor gebruiker om zelfstandig beheer te voeren over zijn account (“self-service”).

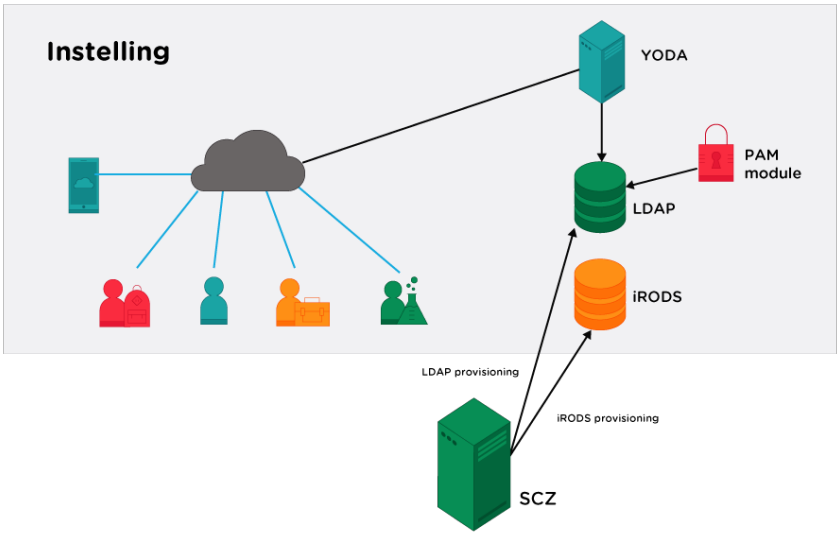
Resultaat – Proof of Concept

De uitwerking van bovenstaande uitdaging heeft geresulteerd in het volgende resultaat:

a) Het opzetten van een Collaborative Organization (CO) in de pilot-omgeving van de “Science Collaboration Zone” (SCZ[3]). De CO die is aangemaakt heeft de naam: “YODA University Utrecht”. Belangrijkste functionaliteit die de SCZ hier levert is een COmanage-omgeving waar gebruikersbeheer kan plaatsvinden.
b) Enrollment Flow binnen de CO waarmee een onderzoeker wordt uitgenodigd en waarbij hem wordt gevraagd om zich via een ‘vertrouwde Identity Provider’ (IdP) aan te melden. De SCZ kan er daarmee op vertrouwen dat deze persoon het ‘trustlevel’ bezit dat overeenkomt met het trustlevel dat SCZ aan de desbetreffende IdP heeft toegekend. Tijdens de enrollment flow wordt aan de nieuwe deelnemer via emailverificatie akkoord verklaring gevraagd voor de gebruiksvoorwaarden. Als laatste stap in de enrollment flow wordt aan de CO Admin de aanvraag voorgelegd. De CO Admin besluit nu of de nieuwe gebruiker al dan niet wordt geaccepteerd als deelnemer binnen de samenwerking. Om gedetailleerde auditing van alle processen mogelijk te maken worden alle stappen in het proces gelogd.
c) Provisioning Flows, waarmee elke wijziging van de CO (leden, groepen, rollen, lidmaatschap van leden in groepen, etc), worden ‘gepushed’ van de centrale SCZ-omgeving naar de decentrale YODA-omgeving (LDAP en iRODS catalogus). Hiervoor zijn in principe de standaard COmanage Provisioning Plugins gebruikt, echter aan de ontvangende UU-iRODS kant is een maatwerk REST-API gerealiseerd om de SCZ-pushberichten om te vormen naar iRODS-mutaties.
d) Aanmaken van een Service Token: Omdat bij federatieve authenticatie het wachtwoord uitsluitend bij de IdP wordt ingevoerd, beschikt COmanage niet over een wachtwoord van de gebruiker. Om applicaties op later moment toch de gebruiker te laten authenticeren maakt de gebruiker in COmanage een Service Token aan. Dat is een ‘shared secret’ dat wordt opgeslagen in de LDAP. In plaats van het gebruiken van dit 15-karakter-tekenreeks als wachtwoord, wordt dit in de vorm van een QR-code gepresenteerd aan de gebruiker zodat dit gebruikt kan worden in een authenticator app, zoals bijvoorbeeld Google Authenticator.
e) Verder is er een custom PAM-module gerealiseerd waarmee de externe gebruikers tegen de LDAP worden geauthenticeerd. Authenticatie gebeurt met een door COmanage toegekende ‘gebruikersnaam’ en een token (Timebased One Time Password) dat de gebruiker dient af te lezen vanaf zijn ‘authenticator app’ (Bijvoorbeeld Google Authenticator). Hiervoor wordt het totp-protocol[4] gebruikt.

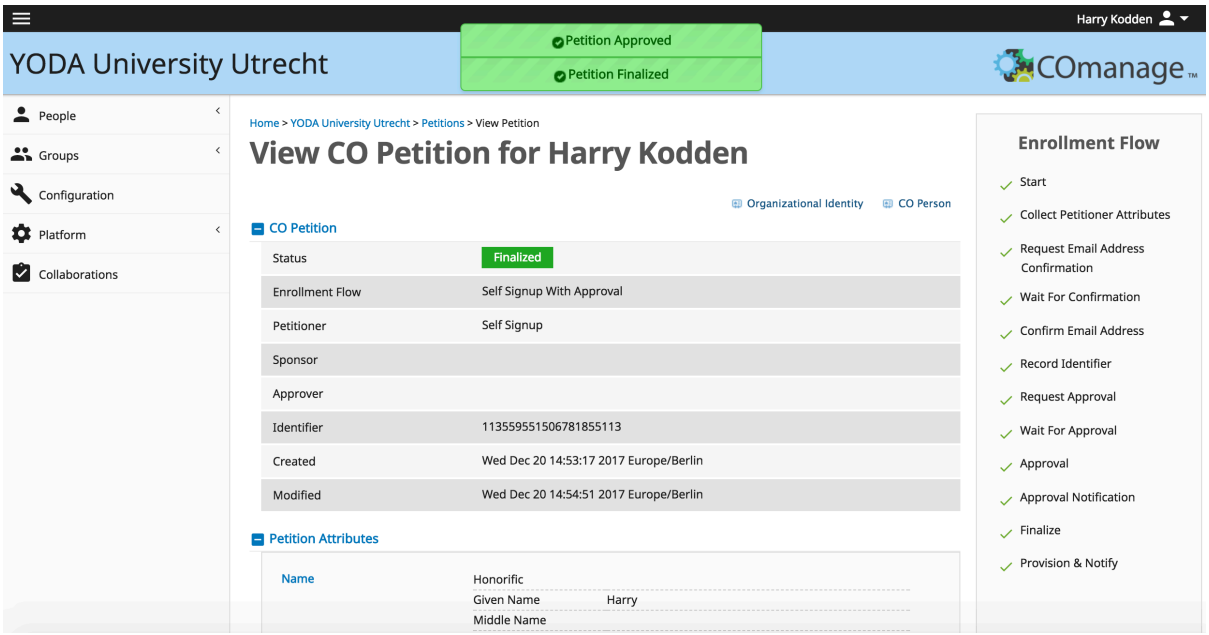
[3] https://wiki.surfnet.nl/display/SCZ/Science+Collaboration+Zone+Home
[4] https://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm

Het gehele plaatje ziet er daarmee als volgt uit:

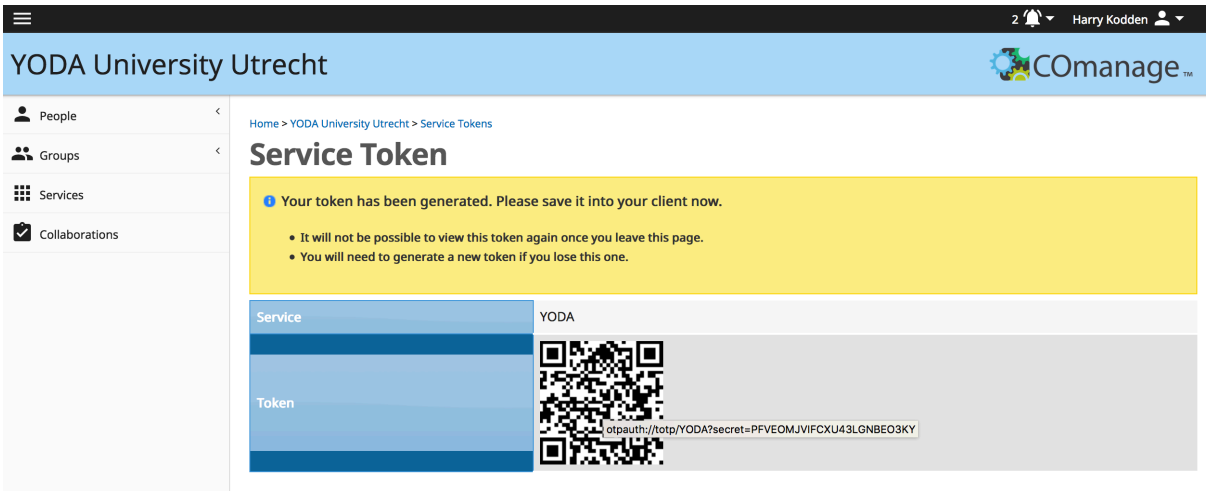


In bovenstaand schema is geschetst hoe vanuit SCZ de externe gebruikers bij de Instelling worden geprovisioned naar zowel de iRODS omgeving als ook naar de locale LDAP.

Voorbeeld van de Enrollment Flow

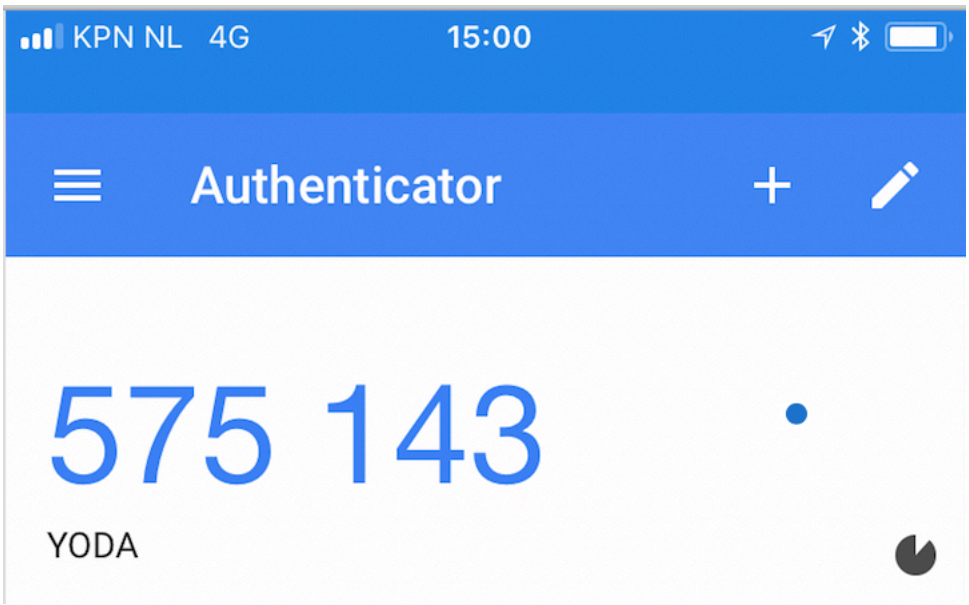


Aanmaken Service Token t.b.v. YODA, de zogenaamde “One-Time-Passwords”

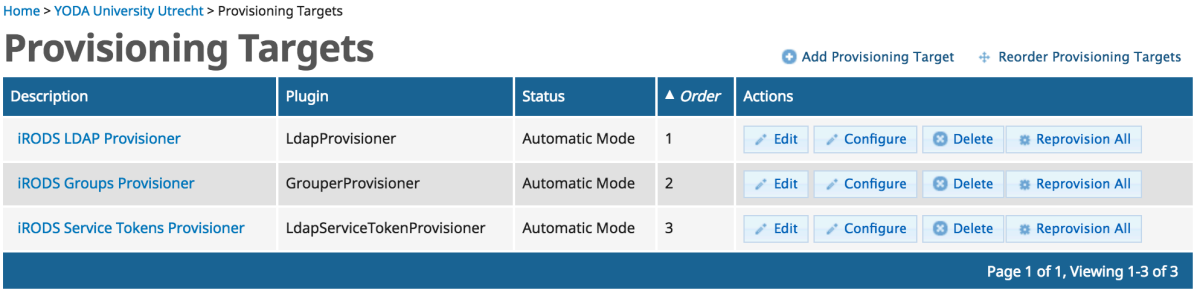


Voorbeeld van gebruik van de Google Authenticator

In dit voorbeeld is bovenstaande QR-code gescanned met de Google Authenticator. Deze app toont een 6-cijferig getal dat elke 30 seconden wijzigt. Op moment dat de gebruiker wenst in te loggen bij YODA dient hij als password de actuele code over te nemen. De PAM-module kan zelfstandig ook de code uitrekenen en vaststellen dat het aangeboden wachtwoord correct is of niet.



Provisioning Flows in COmanage t.b.v. YODA CO



Non-web inloggen op iRODS

Op de iRODS-omgeving hebben we een PAM-module geplaatst die de authenticatie van een gebruiker met een TOTP-code afhandelt.

```
[root@145 admincentos]# cat /etc/pam.d/irods
#%PAM-1.0
auth       sufficient     pam_unix.so
auth       sufficient     pam_soap.so uri=https://yoda.myvelocity.nl/api
```

Deze PAM-definitie beschrijft dat een iRODS-gebruiker succesvol is ingelogd met:

a) een geldige userid / wachtwoord combinatie;
b) een geldige response op afhandeling door een PAM_SOAP request. Deze PAM_SOAP request zal het aangeboden wachtwoord als TOTP-waarde verifiëren tegen de shared secret die voor deze gebruiker is opgeslagen in de LDAP.

Nu dat er vanuit COmanage de provisioning naar LDAP en iRODS is uitgevoerd, kunnen we inloggen op iRODS. iRODS voorziet in een command-line utility “irodsPamAuthCheck” om een authenticatie te controleren. Deze utility maakt gebruik van de eerder genoemde PAM-stack.

```
[admincentos@145 ~]$ irodsPamAuthCheck harry.kodden@yoda.uu
805199
Authenticated
```

Nu weten we dat iRODS kan authenticeren tegen onze PAM module. We kunnen dus nu daadwerkelijk gaan inloggen op iRODS

Hier een voorbeeld hoe we dat kunnen doen vanaf een willekeuring linux-systemaccount, bijvoorbeeld via dit bash-script:

```
#!/bin/bash

# Step 1. Make sure there is no previous session...
iexit full

# Step 2. Setup environment for this user...
export IRODS_ENVIRONMENT_FILE=`mktemp`
echo '{
    "irods_host":"localhost",
    "irods_port":1247,
    "irods_zone_name":"tempZone",
    "irods_user_name":"harry.kodden@yoda.uu",
    "irods_authentication_scheme":"PAM",
    "irods_home":"/tempZone/home",
    "irods_cwd":"/tempZone/home"
}' > $IRODS_ENVIRONMENT_FILE

# Step 3. Do the logon to iRODS...
iinit
```

De gebruiker wordt gevraagd om de TOTP-code in te geven die op dat moment verschijnt in de Google Authenticator. Bij correcte ingave is de gebruiker aangemeld bij iRODS

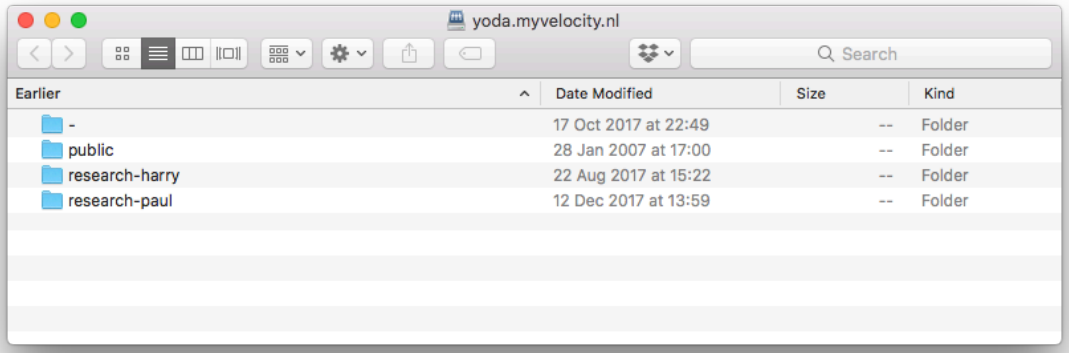
We kunnen nu iRODS commando's geven, bijvoorbeeld "ils":

```
[admincentos@145 ~]$ ils
/tempZone/home:
  C- /tempZone/home/-
  C- /tempZone/home/public
  C- /tempZone/home/research-harry
  C- /tempZone/home/research-paul
```

WebDAV

YODA is voorzien van een WebDAV-toegang waarbij de authenticatie eveneens wordt afgehandeld door de iRODS-authenticatie PAM-stack.
We kunnen dus nu eveneens inloggen op de YODA-WebDAV vanuit bijvoorbeeld de macOS Finder:

Bij succesvolle aanmelding hebben we een Finderwindow op onze iRODS-dataset.



Link naar Github : integratie van iRODS binnen de Science Collaboration Zone.
https://github.com/SURFscz/irods-integration

Vervolg

De Universiteit Utrecht ziet het opgeleverde werk als veelbelovend. Het belooft een duurzame oplossing te bieden voor het (toenemende-) externe gebruik. Op de SURFsara Super D[5] is door Ton Smeele ook een presentatie gegeven over deze en andere ontwikkelingen van YODA.

Omdat SCZ zich momenteel in een 'pilot-situatie' bevindt, betekent dit voor YODA dat er geen 24x7 productie afhankelijkheid met de SCZ kan bestaan. Om die reden overweegt de UU momenteel een eigen lokale COmanage implementatie op te zetten. Ze baseren zich hierbij op een 'standaard' COmanage installatie aangevuld met de eerder vermelde deliverables.
Op moment dat SCZ tot een volwaardige SURFdienst leidt, is het vervolgens mogelijk om daar naar over te schakelen. Een van de voorwaarden die de UU hier echter wel aan zal stellen is dat er een hoogwaardige security audit op de SCZ moet plaatsvinden vanwege de toegang die gebruikers gaan krijgen tot de privacygevoelige gegevens op diverse onderzoeksgebieden.

Binnen de SURFsara DMS group wordt gewerkt aan het beschikbaar stellen van iRODS als productiedienstverlening aan gebruikers. Met dit team zal in eerste instantie gewerkt worden aan het inzetten van deze technologie voor authenticatie van gebruikers, vervolgens zullen op basis van wensen van zowel productmanagement als gebruikers nieuwe functionaliteiten worden ontwikkeld en toegevoegd.

[5] 12 december 2017, https://super-d.surf.nl/speakers