OS2faktor

Windows Credential Providers

Version: 1.0.0
Date: 17.03.2019
Author: BSG

Indhold

1 Indledning

Dette dokument beskriver installation og konfiguration af Windows Crendetial Providers til hhv

- Login med OS2faktor
- Password Reset med OS2faktor

Målgruppen er it-teknikere i kommunen, der er ansvarlig for installation og opsætning af infrastruktur, samt udruldning af software til slutbrugerne.

1.1 Komponenter

Dokumentet dækker følgende 3 komponenter, der indgår i den samlede OS2faktor løsning til hhv Login og Password Reset.

OS2faktor Proxy

Dette er en infrastrukturkomponent der skal driftes på en Windows Server i kommunens egen netværk. Den skal installeres og konfigureres for at nedenstående 2 komponenter kan fungere.

OS2faktor Password Reset Credential Provider

Dette er en såkaldt Credential Provider, der installeres på udvalgte Windows Servere, hvor man på den måde beskytter serveren, så det kun er muligt at logge på serveren med OS2faktor.

OS2faktor Login Credential Provider

Dette er endnu en Credential Provider, der kan installeres på medarbejdernes PC'ere. Medarbejderne får så mulighed for at vælge et nyt kodeord vha NemID, hvis de har glemt deres normale kodeord.

2 Forudsætninger

Alt relevant software kan hentes her

https://www.os2faktor.dk/download.html

Man skal envidere bruge en Windows Server 2016 til at afvikle proxy komponenten, da denne leveres som en Docker container, der er fuldt understøttet af Windows Server 2016.

3 Installation og konfiguration af OS2faktor Proxy

OS2faktor Proxy komponenten er publiceret på Dockerhub

https://cloud.docker.com/u/os2faktor/repository/docker/os2faktor/proxy

Selve installationen af komponenten forudsætter at man har opsat en Windows Server 2016 til at kunne afvikle Docker containere. Dette gøres nemmest ved at følge denne vejledning

https://docs.docker.com/install/windows/docker-ee/

Efter at Container featuren er blevet enabled i Windows Server Management (jf ovenstående link), så skal Docker Compose installeres. Dette gøres ved at hente softwaren fra dette link

https://docs.docker.com/compose/install/

Den pakke med Proxy konfigurationen der kan hentes fra OS2faktor download websitet, indeholder følgende filer

- docker-compose.yml
- config/application.properties
- config/nemid.properties
- config/pid.properties

docker-compose.yml filen indeholder selve Docker konfigurationen for Proxy komponenten, og config folderen indeholder konfigurationen af Proxy softwaren.

For at starte/stoppe Proxy komponenten anvendes Docker Compose.

3.1 Konfiguration

docker-compose.yml filen er en nem måde at samle docker parametre i én konfigurationsfil, så man kan starte/stoppe Docker containeren uden at skulle huske en masse parametre (lidt som et smart powershell script).

Den fil der følger med softwaren indeholder alt hvad der skal bruges, og den eneste indstilling man løbende vil rette i, er versions-angivelsen af Proxy komponenten. Versionen er altid angivet som et dato-stempel (fx 2019-03-17), og tilrettes til den version man ønsker at afvikle.

På Dockerhub websitet (se link ovenfor) kan man se hvilke versioner der er frigivet.

De 3 konfigurationsfiler i config folderen, indeholder konfigurationen af selve Proxy applikationen. Der refereres til forskellige keystores i konfigurationen, og i alle tilfælde skal man blot lægge keystore filen in config folderen, så kan Proxy'en finde dem.

application.properties

Dette er styringsparametrene for Proxy komponenten, og filen er indelt i 4 afsnit.

1. afsnit - indstillinger der SKAL udfyldes

- ldap.url
  - Udfyldes med adressen på den domain controller som proxyen skal kommunikere med. Bemærk at det SKAL være over LDAPS (og ikke LDAP), dvs formatet skal være "ldaps://xxxx", eksempelt vis nedenfor
  - ldaps://dc.kommune.dk
- ldap.base
  - Udfyldes med den "rod" i Active Directory hvor der skal ledes efter brugere, fx
  - CN=Brugere,DC=Kommune,DC=dk
- ldap.username
  - Udfyldes med UPN på en systembruger der må lave opslag i Active Directory (og må ændre kodeord på brugere hvis Password Reset anvendes), fx
  - svproxy@kommune.dk
- ldap.password
  - Udfyldes med kodeordet på ovenstående bruger
- ldap.cert.trustall
  - Sættes til "true" hvis LDAPS endpointet er beskyttet med et SSL certifikat som slutbrugerenes PC'ere ikke stoler på

2. afsnit – indstillinger vedrørende Password Reset

- password.reset.enabled
  - Sættes til "true" hvis Password Reset skal bruges
- ldap.field.ssn
  - Sættes til den attribut i Active Directory hvor medarbejdernes personnummer står
- ldap.password.change.prevent.group
  - Sættes til værdien af den sikkerhedsgruppe i Active Directory, som man kan melde brugere ind i, hvis de IKKE må skifte kodeord vha NemID

3. afsnit – indstillinger vedrørende OS2faktor Login

- login.enabled
  - Sættes til "true" hvis man ønsker at gøre brug af OS2faktor som en login mekanisme til udvalgte Windows Servere
- login.backend.apikey
  - Udfyldes med en API nøgle man har fået til OS2faktor infrastrukturen (man kan med fordel få en ny nøgle til dette specifikke formål)
- login.keystore.location
  - Udfyldes med navnet på en pfx/p12 fil, som skal anvendes til at beskytte login forespørgsler (se detaljer længere nede). Navnet skal udfyldes med classpath: foran, fx
  - classpath:keystore.pfx
- login.keystore.password
  - Udfyldes med kodeordet til ovenstående keystore fil

4. afsnit – indstillinger vedrørende SSL certifikat

Dette afsnit anvendes kun hvis man ikke har mulighed for at sætte en Netscaler, WAP eller lignende op foran Proxy'en.

- server.ssl.key-store
  - Udfyldes med navnet på et pfx/p12 keystore, der har et SSL certifikat, som Proxy'en skal anvende, fx
  - classpath:ssl.pfx
- server.ssl.key-store-password
  - Udfyldes med kodeordet til keystore filen
- server.ssl.key-password
  - Udfyldes med samme kodeord som ovenfor
- server.ssl-key-store-type
  - Udfyldes med værdien "pkcs12"

nemid.properties

Denne fil er kun nødvendig at udfylde hvis man gør brug af Password Reset funktionaliteten. I så fald skal den udfyldes med konfigurationen for ens NemID tjenesteudbyderaftale.

De 4 indstillinger der skal tilrettes er:

- nemid.serviceprovider.logonto
  - Her indtastes navnet på ens NemID aftale (fx ”Min Kommune”)
- nemid.applet.parameter.signing.keystore
  - Her indtastet navnet på den pfx/p12 fil, som man skal bruge til at kalde NemID (i forbindelse med at man har indgået en aftale med NemID, har man også fået et tilhørende keystore). Der skal stå ”classpath:” foran filens navn, eksempel vises nedenfor
  - classpath:os2faktor.pfx
- nemid.applet.parameter.signing.keystore.password
  - Her indtastet kodeordet til keystore filen
- nemid.applet.parameter.signing.keystore.alias
  - Her indtastes navnet på certifikatet fra keystore filen

pid.properties

Denne fil er kun nødvendig at udfylde hvis man gør brug af Password Reset funktionaliteten. I så fald skal den udfyldes med konfigurationen for den ”PID til CPR” aftale man har indgået med Digitaliseringsstyrelsen

De 3 indstillinger der skal tilrettes er:

- pid.serviceproviderid
  - Her indtastet aftale-id’et fra ”PID til CPR” aftalen
- pid.keystore.location
  - Her indtastes same værdi som i ”nemid.applet.parameter.signing.keystore” fra nemid.properties filen
- pid.keystore.password
  - Her indtastes kodeordet til keystore filen (samme som for nemid.properties)

3.2 Keystore til signering

Hvis man anvender OS2faktor Login funktionaliteten, skal proxy komponenten være konfigureret med et keystore til at beskytte svaret på login forespørgslen. Dette sikrer mod angreb hvor en 3.part kan omgå 2.faktor login ved at route forespørgslen til en ondsindet proxy komponent.

Der skal anvendes et keystore med et certifikat. Der er ingen krav til at dette skal være et OCES certifikat, men man kan sagtens bruge et sådan hvis man ønsker.

Bemærk at den offentlige del af dette certifikat skal installeres på alle de servere hvor man skal kunne logge på med OS2faktor.

3.3 Start/stop af komponenten

Når komponenten er konfigureret, kan den startes og stoppes vha Docker Compose. Dette gøres med følgende kommandoer, der afvikles fra Powershell inde i folderen hvor docker-compose.yml filen ligger

```
$ docker-compose.exe up -d
```

Ovenstående kommando starter Proxy komponenten som et baggrundsjob. Hvis man gerne vil se outputtet fra kørslen, kan man bruge ”docker ps” til at finde ID’et på applikationen, og ”docker logs xxxx”, hvor xxxx er ID’et, til at se outputtet fra applikationen.

Man kan også starte applikationen uden ”-d”, så kommer loggen direkte i powershell konsollen.

```
$ docker-compose.exe down
```

Ovenstående kommando stopper applikationen igen.

3.4 Test af Proxy komponenten

Når man har installeret og startet Proxy’en, vil den lytte på port 9500. Man kan desværre ikke tilgå den fra samme maskine som Docker kører på, men fra en anden maskine på netværket, vil man kunne tilgå den via sin webbrowser på DNS navn + port 9500.

Man kan med fordel lade sin Netscaler, WAP eller lignende, mappe til port 443 (normal HTTPS).

3.5 Overvejelser omkring netværk

Det er vigtigt at Proxy’en kan nås fra de maskiner der skal anvende enten Login eller Password Reset funktionaliteten. Som udgangspunkt betyder det at man bør give Proxy’en et DNS navn, og referere til Proxy’en via denne, samt sikre at serveren kan nås fra de maskiner der skal tilgå den.

Hvis man ønsker at Password Reset funktionaliteten kan tilgås fra Internettet, bør man også konfigurere sin Netscaler, WAP eller anden firewall, så den tilllader trafik fra internettet.

Man kan med fordel håndtere SSL i sin firewall, så man ikke skal konfigurere det ude i Proxy’en.

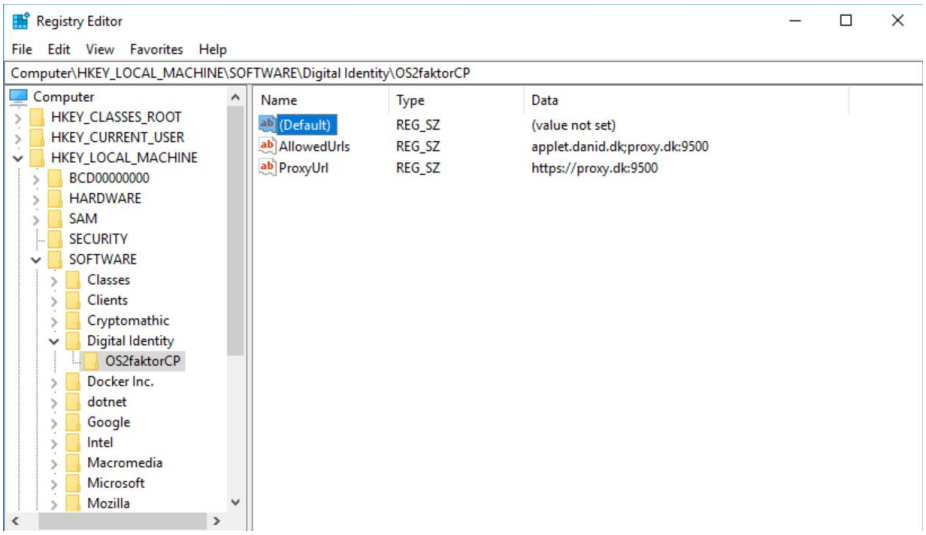
4 Installation og konfiguration af OS2faktor Password Reset

OS2faktor Password Reset komponenten distribueres som en MSI pakke, der kan installeres på de maskiner der skal gøre brug af Password Reset fra Windows loginskærmen.

MSI pakken kan hentes fra OS2faktor download sitet, og det anbefales at man bygger en ny MSI pakke, der indeholder tilpassede Windows Registry settings (eller at man ruller de fornødne Windows Registry settings på via anden kanal).

Der er 2 indstillinger til OS2faktor Password Reset, som gemmes i Windows Registry, under denne nøgle

HKLM -> Software -> Digital Identity -> OS2faktorCP



- **AllowedUrls**. Her indtastes domænenavnet på Proxy komponenten (inkl port hvis den ikke kører på 443), samt domænenavnet på NemID (applet.danid.dk), adskildt med semikolon.
- **ProxyUrl**. Her indtastes den fulde URL på Proxy komponenten (inkl port hvis den ikke kører på 443)

Password Reset komponenten anvender disse til at kommunikere med hhv NemID og Proxy komponenten.

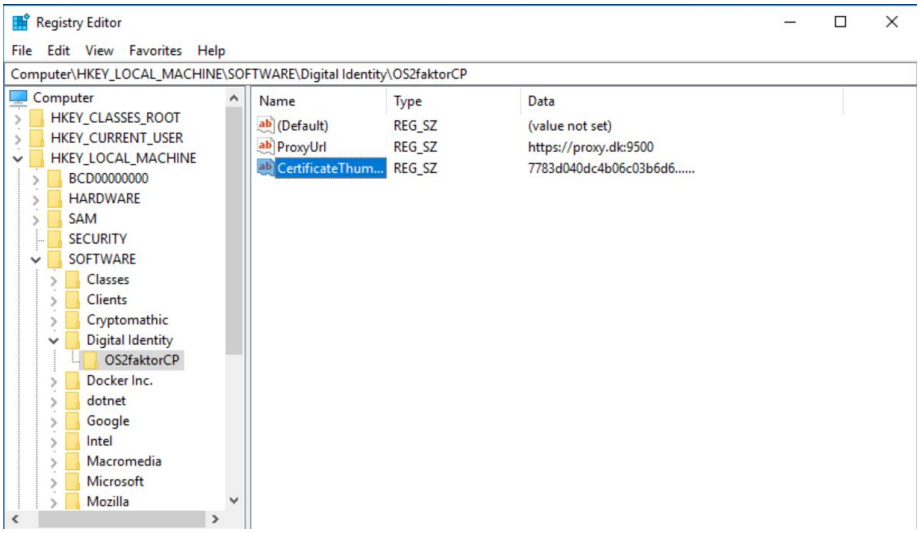
5 Installation og konfiguration af OS2faktor Login

OS2faktor Login komponenten distribueres som en MSI pakke, der kan installeres på de maskiner der skal gøre brug af OS2faktor til login.

MSI pakken kan hentes fra OS2faktor download sitet, og det anbefales at man bygger en ny MSI pakke, der indeholder tilpassede Windows Registry settings (eller at man ruller de fornødne Windows Registry settings på via anden kanal). Denne MSI pakke kan også samtidige installere det certifikat som Proxy komponenten anvender til at beskytte login forespørgsler (eller man kan distribuere certifikatet på anden vis).

Der er 2 indstillinger til OS2faktor Password Reset, som gemmes i Windows Registry, under denne nøgle

HKLM -> Software -> Digital Identity -> OS2faktorCP



- **CertificateThumbprint**. Her indtastes thumbprint på det certifikat som anvendes af Proxy komponenten til at beskytte login forespørgsler.
- **ProxyUrl**. Her indtastes den fulde URL på Proxy komponenten (inkl port hvis den ikke kører på 443)