Identity Provider Migratie

Een migratie van een identity provider is heel gebruikelijk als er een upgrade aan je identity provider wordt uitgevoerd. Zo kan het zijn dat je je oude Microsoft ADFS omgeving upgrade naar een nieuwe omgeving zoals Azure. Dan zijn er wijzigingen in de end-points, de single sign-on locaties en het entityID van je IdP. Het entityID van de IdP wordt door SURFconext gebruikt voor het uniek identificeren van de IdP en kan maar één keer voorkomen in de beheersystemen van SURFconext. Bij een dergelijke migratie wordt er van uit gegaan dat de nieuwe IdP een nieuw EntityID krijgt. Als de nieuwe IdP eenzelfde entityID houdt zal een ander pad gevolgd moeten worden. Hoe je deze nieuwe IdP inricht is te vinden op onze pagina met handleidingen en richtlijnen. Zorg dat je dat hebt afgerond voordat je ons bericht over de migratie.

Voor de migratie van de IdP moeten de volgende stappen doorlopen worden.

Voorbereiden Migratie

We beginnen met de voorbereidende werkzaamheden als je je IdP hebt geconfigureerd zoals aangegeven in onze handleidingen.

1. We hebben een akkoord nodig van de SURFconext verantwoordelijke van jouw instelling voor het overzetten van de oude IdP naar de nieuwe IdP. Een mail naar support@surfconext.nl van de SURFconextverantwoordelijke volstaat hiervoor.
2. We gaan de nieuwe IdP opvoeren in onze testomgeving of in onze productieomgeving, afhankelijk van hoe je wilt testen. Hiervoor hebben we de metadata van de IdP nodig.
3. Daarna gaan we controleren of de attributen van de oude IdP gelijk zijn aan de attributen van de nieuwe IdP. Dit is met name van belang voor de **uid**, **schacHomeOrganization**. Deze zijn essentieel zijn voor de identificatie van de gebruiker op de aangesloten diensten. Als een je hier toch iets verandert zal het er toe leiden dat SURFconext een nieuw **NameID** en **eduPersonTargetedID** gaat genereren. Dit kan tot gevolg hebben dat gebruikers geen toegang meer hebben tot hun profielen bij diensten. Als deze attributen gelijk blijven zullen de gebruikersprofielen bij diensten bewaard blijven. Zie ook onze attributen pagina. Stuur ons de attributen van een zelfde gebruikersaccount van de **nieuwe én** de **oude IdP** door aan te melden in een private sessie van je browser op **https://engine.surfconext.nl/authentication/sp/debug** en ons de attributen sturen door te klikken, onderaan de pagina, op de knop "Mail naar SURFconext-Beheer". Als je Identity Provider op onze testomgeving is gedefinieerd kun je ons de attributen daarvan sturen door te navigeren naar **https://engine.test.surfconext.nl/authentication/sp/debug**.
4. Zorg dat je de end-points, de SingleSignOnService-locaties, op je IdP een minimale score 'B' heeft op SSL-Labs. Het zal doorgaans zo zijn dat je bij een upgrade minimaal 'A' scoort omdat je systeem weer bij de tijd is. Als je hier niet aan voldoet sluiten we de IdP niet aan op productieomgeving van SURFconext. Je hebt nog tot aan de dag van de migratie om dit op te lossen.
5. Voordat de migratie ingezet wordt gaan we er van uit dat alles grondig is getest in de test-omgeving van SURFconext. **Test met alle browsers: Chrome, Safari, Firefox, Opera, Edge, Internet Explorer, ...**
6. Wij zullen ruim voor de dag van migratie diensten met een eigen WAYF (Where Are You From) inlichten dat het entityID van jullie IdP gaat veranderen. Deze diensten blijven tot nader orde op beide IdPs aangesloten, dus ook nadat je nieuwe IdP in bedrijf is. Het bijwerken van de WAYF gaat bij de ene dienst sneller dan de andere dus hier beginnen we op tijd mee. Hoewel diensten van Topdesk geen WAYF tonen moeten ook voor instanties van Topdesk de nieuwe IdP ingesteld worden. Dit is aan de instelling om te configureren dan wel aan te geven bij Topdesk met een mail naar premiumsupport@topdesk.com. SURFnet kan je de informatie geven die je nodig hebt voor de migratie. Je ontvangt een lijst met diensten die hun eigen WAYF hebben.
7. **Tot slot: geef bij ons aan wanneer je de migratie gaat uitvoeren.**

De dag van migratie

Op de dag van migratie doorlopen we de volgende stappen:

1. We gaan de nieuwe IdP naar de productie omgeving van SURFconext verplaatsen. Zorg dat jouw IdP ook naar de productieomgeving van SURFconext verwijst.
2. De instelling zal gaan testen of de nieuwe IdP goed werkt op de gekoppelde diensten en zal SURFnet informeren als er problemen zijn.
3. Bij problemen gaan we kijken wat we er aan kunnen doen. Als de problemen niet opgelost kunnen worden zal op het niveau van SURFconext de oude configuratie terug gezet worden. Je kunt tot nader orde de oude IdP gebruiken.
4. Als alles goed is gegaan zal de oude IdP offline gehaald worden dan wel verplaatsen naar de test omgeving van SURFconext waardoor deze onzichtbaar wordt in de WAYF van de aangesloten diensten. De oude IdP zal pas offline gehaald worden als alle diensten over zijn, dus ook diensten met hun eigen WAYF. Dat laatste duurt soms wel even.

Omdat een dienst zelf kan bepalen of deze gebruik maakt van de WAYF die SURFconext aanbied of zelf een lokale WAYF heeft, hebben wij geen volledig inzicht in de diensten die een eigen WAYF implementeren en waarvan de metadata niet dynamisch wordt bijgewerkt. Zelfs bij diensten waarbij de metadata wel automatisch wordt bijgewerkt is een kortstondige uitval (de tijd tussen de updates welke tussen de 5 minuten en 24 uur kan liggen) onvermijdelijk.

Als we bovenstaande stappen hebben doorlopen ben je gemigreerd naar je nieuwe IdP. Als wij ons werk goed hebben gedaan hebben gebruikers er niets van gemerkt en hebben ze gebruik kunnen maken van de op SURFconext aangesloten diensten via jouw IdP tijdens de migratie.