Diensten beschikbaar maken voor een beperkte groep gebruikers

Over deze problematiek verscheen in maart 2017 ook een blog.

Hoewel veel diensten die een instelling via SURFconext afneemt voor alle gebruikers van een IdP beschikbaar moeten zijn, kunnen er ook diensten worden gekoppeld die slechts voor een beperkte set gebruikers zijn bedoeld. Er kunnen verschillende redenen zijn om dit te doen, bijvoorbeeld:

- licentieoverwegingen; op deze manier kan een instelling een dienst afnemen voor een beperkte groep gebruikers (bijvoorbeeld alleen medewerkers, of alleen leden van een bepaalde faculteit);
- afscherming van gevoelige diensten; het koppelen van bijvoorbeeld beheerstools via SURFconext vermijdt het hergebruik van wachtwoorden en geeft het voordeel van single log-on; maar het is niet de bedoeling om alle gebruikers van een instelling toegang te geven;

Op deze pagina beschrijven we hoe een dienst die via SURFconext is gekoppeld, is af te schermen zodat gebruik van de dienst is beperkt tot een beperkte groep gebruikers van een instelling (bijvoorbeeld alleen studenten, of alleen medewerkers van een specifieke faculteit).

Er zijn verschillende mogelijkheden om een dergelijke afscherming te bereiken. Hieronder beschrijven we de drie meest gebruikte methodes.

Op basis van provisioning

Veel diensten hebben eigen voorzieningen voor het bepalen van toegang tot en rechten binnen de dienst. Typisch betekent dat dat de dienst, hoewel die via SURFconext is ontsloten, alleen gebruikers toelaat die vooraf in de dienst zijn aangemaakt (geprovisiond).

Het aanmaken van gebruikers in de dienst kan op diverse manieren gebeuren:

- handmatig in een userinterface in de dienst;
- door uploaden van een (CSV-)bestand met gebruikers naar de dienst;
- door het maken van een directe koppeling tussen de dienst en het IdM-systeem van de instelling. Afhankelijk van wat de dienst ondersteunt, kan zo'n koppeling worden geïmplementeerd op basis van AD/ldap (zoals bijvoorbeeld bij Office 365), via een dienst-specifieke API (zoals bijvoorbeeld bij Google Apps), of via een standaard provisioningsprotocol zoals SCIM. In de configuratie van de koppeling wordt dan bepaald welke groep gebruikers naar de dienst wordt gesynchroniseerd.

Uiteraard kan het zijn dat niet al deze mogelijkheden door de dienstverlener worden ondersteund.

Noot: identificatie van de gebruiker binnen de dienst

Een complicerende factor bij deze methode is dat bij het inloggen de identiteit van de gebruiker moet worden vastgesteld. Minimaal één van de attributen die de dienst bij logins via SURFconext binnenkrijgt, zal dus overeen moeten komen met de identiteit die de instelling in de dienst heeft aangemaakt. De gebruikelijke manieren van identificeren van SURFconextgebruikers vindt echter plaats met de NameId of met het eduPersonPrincipleName-attribuut; deze komen in dit geval typisch niet in aanmerking voor identificatie, omdat dit afgeleide attributen zijn die (meestal) niet aanwezig zijn in de IdM-systemen van de instelling. We raden daarom aan om voor dit scenario een medewerker- of studentnummer door te geven via het schacPersonalUniqueCode-attribuut. Identificatie op basis van het `uid`-attribuut raden wij af voor diensten van externe leveranciers, omdat dit attribuut bij de meeste instellingen de loginnaam van de gebruiker bevat, en het uit veiligheidsoverwegingen geen goed idee is om deze buiten de instelling te gebruiken

Op basis van attributen

Een andere veelgebruikte mogelijkheid is om vanuit de IdP van de instelling extra attributen mee te geven op basis waarvan toegang kan worden geregeld.

De volgende attributen komen in aanmerking:

- *eduPersonAffiliation*: dit attribuut geeft de rollen aan die een gebruiker heeft binnen de instelling. Op basis van dit attribuut is het dus mogelijk om alleen medewerkers, of juist alleen studenten, toegang te geven tot een bepaalde dienst.
- *eduPersonScopedAffiliation*: dit attribuut geeft de rollen aan die een gebruiker heeft binnen onderdelen van een instelling.
  Zo kan bijvoorbeeld worden aangegeven dat iemand een docent/onderzoeker is bij de faculteit wiskunde (`faculty@math.uniharderwijk.nl`), of een student bij de faculteit rechten (`student@law.uniharderwijk.nl`). Op basis hiervan kan dus zowel toegang worden verleend aan gebruikers van een specifiek onderdeel (bv., het instituut voor origamikunst `member@origami.uniharderwijk.nl`) van een instelling, of aan gebruikers met een specifieke rol binnen zo'n onderdeel (bv., docentent/onderzoekers van de sterrenkundeafdeling `faculty@astro.uniharderwijk.nl`).

- *eduPersonEntitlement* : dit attribuut kan waarden bevatten die een gebruiker specifiek toegang geven tot één (groep van) diensten. Om toegang te krijgen tot een data-opslagdienst, zou een gebruiker bijvoorbeeld de volgende entitlement-waarde moeten hebben: "`urn:x-surfnet:hippedienst.example.edu:access:true`".

De bovenstaande attributen worden van de instellings-IdP aan SURFconext doorgegeven. De daadwerkelijke afscherming kan op twee plaatsen worden uitgevoerd: in SURFconext, of in de dienst zelf.

Als SURFconext de afscherming regelt, kan deze workflow worden gebruikt zonder dat ondersteuning van de dienst nodig is. De afscherming vindt dan plaats via Autorisatieregels. Op het SURFconext Dashboard kunnen de SURFconext-contactpersonen van de instelling onder het tabblad "autorisatieregels" een filter toevoegen op basis van een (of meerdere) van de bovenstaande attributen. Daarmee kunnen de geselecteerde groepen worden toegelaten of juist worden geweigerd.

Als de dienst zelf de afscherming regelt, zal SURFconext de benodigde attributen, zoals hierboven beschreven, doorgeven aan de dienst. Alle gebruikers worden dus naar de dienst doorgelaten, en de dienst kan op basis van deze attributen toegang toestaan of weigeren. Uiteraard is het ook mogelijk dat de dienst op basis van deze attributen verschillende rechten toekent (bijvoorbeeld iedereen leesrechten, maar alleen medewerkers schrijfrechten). Dit is echter geheel afhankelijk van de ondersteuning en de mogelijkheden van de dienst.

Op basis van groepen

In plaats van in de IdP een attribuut toe te voegen voor bepaalde gebruikers, is het ook mogelijk om toegang te verlenen aan gebruikers in een specifieke groep. Daarvoor zijn twee mogelijkheden:

- De groepen worden met de hand beheerd via SURFconext Teams. Dit is met name zinvol als het een relatief kleine groep gebruikers betreft, of wanneer het beheer van de groep decentraal plaatsvindt (bijvoorbeeld binnen een onderzoeksgroep). Ook als er aan gebruikers van verschillende instellingen toegang moet worden verleend, of aan een combinatie van instellingsgebruikers en gasten uit de OneGini-IdP, is deze aanpak aan te raden.
  Via SURFconext kan een manager van een groep aangewezen worden die zelfstandig gebruikers aan een groep kan toevoegen en uit een groep kan verwijderen.
- De groepen worden beheerd binnen een groepsbeheersysteem van de instelling, en dit systeem wordt direct gekoppeld aan SURFconext . De groepen die binnen de instelling zijn gedefinieerd kunnen dan direct in SURFconext worden gebruikt. Afhankelijk van de implementatie binnen de instelling (of de groepen bijvoorbeeld in het IdM worden bijgehouden, of in decentrale systemen zoals een LMS of een SIS) vindt het beheer centraal plaats, of decentraal.

Ook in dit geval zijn er twee mogelijkheden om de daadwerkelijke afscherming te regelen: binnen SURFconext op basis van Autorisatieregels, of binnen de dienst:

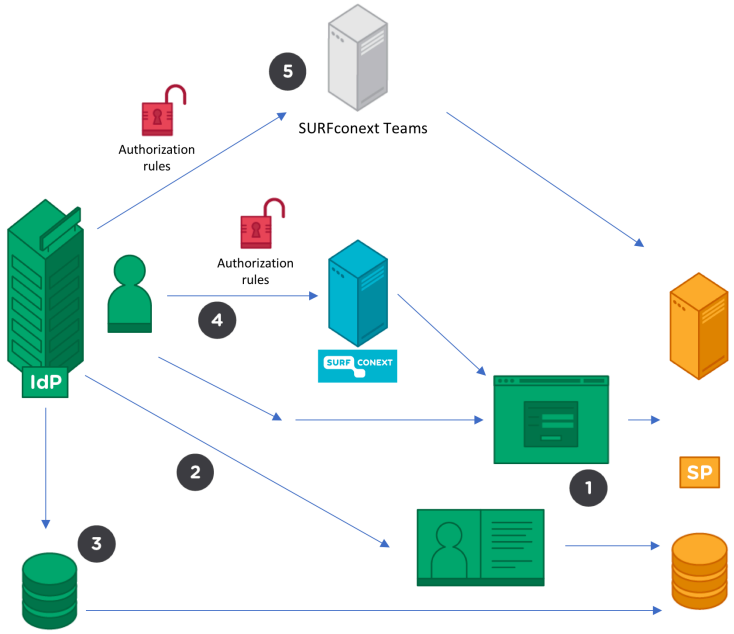
1. Als wordt gekozen voor afscherming door SURFconext, kan dit worden geregeld via Autorisatieregels. Deze kunnen op het SURFconext Dashboard worden aangepast. Daar kan dan worden gekozen voor een afscherming op basis van groepslidmaatschap. Deze workflow kan worden gebruikt zonder dat ondersteuning van de dienst nodig is.
2. Als de afscherming in de dienst moet worden geregeld, zal de dienst na elke login van een gebruiker in een aparte call ook diens groepen moeten opvragen bij SURFconext. Hoe dit in zijn werk gaat, wordt op een andere plek op deze wiki beschreven.

Overzicht

In onderstaande tabel worden de belangrijkste eigenschappen van de verschillende manieren van afscherming nogmaals met elkaar vergeleken.

type		beheer	afschermin g	ondersteuning SP
Provisioning		afhankelijk van SP instelling of decentraal	SP	vereist
Attributen		instelling: IAM-beheer	SURFconext	niet nodig
			SP	vereist
Groepen	instellingsgroepen	instelling: IAM-beheer of decentaal	SURFconext	niet nodig
			SP	vereist
	SURFconext Teams	decentraal	SURFconext	niet nodig
			SP	vereist

Schematisch



Ways to manage authorization

1. Manual manage within/at service/SP
2. Upload CSV to SP
3. Connect SP to IdM (AD, ldap, SCIM, API…)
4. Based on attributes:
    a) Via SURFconext authorization-rules
    b) At/in/by service/SP
5. Based on team membership
    a) Using SURFconext Teams
        a) Combine this with SC-auth-rules
        b) Use these in service/SP with VOOT
    b) Synching local AD-groups
        a) Combine this with SC-auth-rules
        b) Use these in service/SP with VOOT

Neem voor opmerkingen of vragen gerust contact op met het SURFconext Supportteam (support@surfconext.nl)