Group Provider koppelen aan SURFconext

Op deze pagina vind je technische informatie over hoe je een extra 'Group' koppeling maakt tussen jouw Identity Provider-systeem (bijvoorbeeld Active Directory) en SURFconext. Je zult deze extra koppeling moeten implementeren naast de bestaande koppeling voor individuele gebruikers. Een reden om deze koppeling te maken is b.v. zodat je groepen die je in je lokale systeem al hebt en beheert, ook kunt gebruiken in combinatie met SURFconext Teams, in SURFconext Autorisatieregels en andere applicaties die overweg kunnen met informatie over groepen /groepslidmaatschap. Avans Hogeschool gebruikt deze optie bijvoorbeeld.

Inleiding

Voor het uitwisselen van groepsinformatie tussen jouw Identity Provider-systeem en Service Providers maakt SURFconext gebruik van het VOOT-protocol, versie 2 (zie http://openvoot.org). VOOT staat voor Virtual Organization Orthogonal Technology. Dit protocol onderscheidt verschillende rollen:

- Group provider
- Client

Een *group provider* is een bron van groepsinformatie. Dit kan bijvoorbeeld jouw Identity Provider-systeem zijn, waarin staat *wie* in *welke groep* zit. Een *client* is een dienst (Service Provider) die gebruik maakt van deze groepsinformatie. Dit kan bijvoorbeeld een Wiki zijn, die bepaalde pagina's afschermt op basis van groepslidmaatschap (bijvoorbeeld alleen leden van de groep 'docenten' mogen een bepaalde pagina zien).

Beschrijving van het protocol

Als jouw organisatie in SURFconext groepen wil hergebruiken die je zelf definieert en beheert, dan word je gezien als een externe Group Provider. Je moet dan naast een koppeling voor individuele gebruikers ook een koppeling voor groepen maken met SURFconext. Dit doe je met behulp van het VOOT-protocol. VOOT staat voor Virtual Organization Orthogonal Technology.

Het protocol ondersteunt 2 manieren van authenticatie: Basic Authentication (RFC 2617) en OAuth 2.0 (RFC 6749). Wil je als externe Group Provider optreden in SURFconext, dan kun je alleen Basic Authentication gebruiken.

Je kunt het protocol zelf implementeren op jouw Identity Management-systeem of gebruik maken van een reeds bestaande implementatie. Bijvoorbeeld https://github.com/frkosurf/php-voot-provider.

Service Providers kunnen 2 verschillende typen verzoeken sturen naar jouw *group provider* via SURFconext:

Request	Resultaat
`"user/" + UID + "/groups"`	Geef alle groepen van gebruiker met UID*
`"user/" + UID + "/groups/" + GROUP_ID`	Geef groepsinformatie van groep GROUP_ID als gebruiker met UID lid is van deze groep.

* = Met UID wordt het attribuut `urn:mace:dir:attribute-def:uid` bedoeld. Deze wordt gebruikt om gebruikers binnen jouw Identity Provider uniek te herkennen. Zie de pagina over attributen voor meer informatie over dit attribuut.

Handleidingen

Om je op weg te helpen met het koppelen van jouw 'Group Provider' heeft SURFconext enkele handleidingen opgesteld:

- Eenvoudig via php-voot-provider
- Microsoft Active Directory als Group Provider
- Microsoft Active Directory als Group Provider (deprecated)
- Microsoft Sharepoint als Group Provider (deprecated)

Beveiliging interface

De VOOT-verzoeken die SURFconext stuurt zullen automatisch van de VOOT-omgeving komen. Om de gegevens te beschermen wordt altijd HTTPS gebruikt. De interface wordt afgeschermd met HTTP Basic Authentication met een door jullie aan SURFconext op te geven gebruikersnaam en (sterk) wachtwoord. Bij voorkeur stel je geen IP-adresrestricties op deze interface, omdat SURFconext op meerdere locaties gehost is en daarom vanaf verschillende ranges kan komen.