Microsoft Active Directory als Group Provider

Introductie

Deze pagina beschrijft hoe je Microsoft Active Directory (AD) als 'Group Provider' kunt inrichten. Hierdoor kan groepsinformatie rechtstreeks vanuit de AD via SURFconext naar bepaalde Service Providers worden doorgestuurd.

Een 'Group Provider' is een REST-service die op basis van *basic authentication* informatie verstrekt middels het VOOT-protocol.

⚠ Deze pagina beschrijft hoe een Microsoft Active Directory gebruikt kan worden als 'Group Provider', maar bevat geen compleet voorbeeld. Kennis van Visual Studio en C# is vereist om de benoemde stappen volledig door te lopen.

Een simpele manier om een 'Group Provider' op te zetten is:

1. Installeer een server met IIS (Internet Information Service)
2. Maak een .NET project op basis van het WCF Service Application, met daarin een REST Service
3. Zorgt dat het .NET project antwoordt nav. 2 typen REST calls
4. Deploy het .NET project in IIS
5. Beveilig ISS oa. dmv. Basic Authentication

De calls gestuurd naar uw 'Group Provider' komen van de SURFconext groeps-omgeving voot.surfconext.nl en zijn:

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

Stap 1: Installeer IIS

Bij het installeren van IIS voor de 'Group Provider' kan gebruik gemaakt worden van de standaard IIS installatie/rol.

Aandachtspunten zijn:

- De IIS server zal via LDAP (vanuit het .NET project) contact moeten kunnen leggen met de Active Directory omgeving (Zonder SSL via poort 389, met SSL - LDAPS, poort 636).
- De IIS server zal benaderd moeten kunnen worden vanaf de SURFconext groeps-omgeving (voot.surfconext.nl; `145.100.191.192/26` & `2001:610:188:426::/64`).

Stap 2: Maken .NET project

Creëer een nieuw .NET project met daarin een RESTfull Service. Een voorbeeld is te vinden op: http://www.topwcftutorials.net/2013/09/simple-steps-for-restful-service.html.

Stap 3: Pas .NET project aan voor VOOT2/Group Provider

De call die door de groepenomgeving van SURFconext naar uw 'Group Provider' wordt gestuurd is: `/groups/{groupid}/{userid}`.

Hierbij is `{groupid}` de volledige identifier van de groep zoals bijvoorbeeld: `urn:collab:group:example.org:nl:surfnet:diensten:groupname1`

`{userid}` is de UID van de gebruiker, zoals: `urn:collab:person:example.org:user1`

Door het OperationContract in het .NET project aan te passen is het mogelijk de waarden van uit de call (in de URI/URL) te gebruiken binnen het project:

```
[OperationContract]
[WebInvoke(Method = "GET", ResponseFormat = WebMessageFormat.Xml,
BodyStyle = WebMessageBodyStyle.Bare,
UriTemplate = "user/{userid}/group/{groupid}")]
```

Door middel van LDAP is het nu mogelijk om te kijken om gebruiker met `{userid}` lid is van een groep met de naam `{groupid}`. Om verbinding te maken met de LDAP-server heb je de component LDAP library for C#.NET nodig.

Er kan gebruik gemaakt worden van de volgende code om in Active Directory to zoeken of een gebruiker lid is van een bepaalde groep. Let op dat deze code niet compleet is en aanpassingen behoeft mbt. AD-domein en groups-locatie in de AD.

```
public static List<string> GetUserGroupDetails(string userName)
        {
                        DirectoryEntry entry = new DirectoryEntry("LDAP://CN=users,DC=fabrikam,DC=com");
            DirectorySearcher search = new DirectorySearcher(entry);
            List<string> groupsList = new List<string>();
            search.Filter = String.Format("(cn={0})", userName);
            search.PropertiesToLoad.Add("memberOf");

            SearchResult result = search.FindOne();
            if (result != null)
            {
                int groupCount = result.Properties["memberOf"].Count;

                for (int counter = 0; counter < groupCount; counter++)
                {
                    string s = (string)result.Properties["memberOf"][counter];
                    groupsList.Add(s);
                    // _log.DebugFormat("found group for user {0} : {1}", userName, s);

                }
            }
            else
            {
                _log.Warn("no groups found for user " + userName);
            }
            return groupsList;
        }
```

Voorbeelden van de VOOT2-JSON uitvoer zien er zo uit:

- Geen groep gevonden = lege JSON:

```
[]
```

- 1 groep gevonden:

```
{
  "id": "id1",
```

```
  "displayName": "display name 1",
  "membership": {
    "basic": "member"
  },
  "description": "description...1"
}
```

- Meerdere groepen gevonden:

```
[
  {
    "id": "id1",
    "displayName": "display name 1",
    "membership": {
      "basic": "member"
    },
    "description": "description...1"
  },
  {
    "id": "id2",
    "displayName": "display name 2",
    "membership": {
      "basic": "member"
    },
    "description": "description...2"
  }
]
```

Stap 4: Toevoegen .NET project aan IIS

Na het maken van het .NET project kan deze worden toegevoegd aan de IIS-webserver. Zie hiervoor de stappen zoals beschreven in: http://www.iis.net/learn/application-frameworks/scenario-build-an-aspnet-website-on-iis/configuring-step-1-install-iis-and-asp-net-modules#12.

Stap 5: Configuratie Basic Authentication + beperking toegang op basis van IP-adressen

De nieuwe 'Group Provider' dient te worden geconfigureerd in de SURFconext groepenomgeving. Om te zorgen dat alleen SURFconext met deze dienst kan communiceren (eventuele Service Providers communiceren altijd via het SURFconext-platform) wordt gebruik gemaakt van Basic Authentication in IIS en een restrictie van de servers die contact mogen leggen vanaf bepaalde IP-adressen.

Basic Authentication

Voer de volgende stappen uit om Basic Authentication aan te zetten op de web site van de 'Group Provider':

1. Open IIS manager en ga naar de web site.
2. Open de '**Features View**' en dubbelklik op **Authentication**.
3. Op de **Authentication** pagina selecteer **'Basic Authentication'**.
4. In het **Actions** paneel selecteer **Enable** om de Basic Authentication te gebruiken met de standaard instellingen.
5. Disable alle andere authenticatiemethoden.
6. Klik met **rechts** op **Basic Authentication** en selecteer **Edit**.
7. Geeft het standaard Active Directory domein aan in het veld **Domein**. Er hoeft geen **realm** geconfigureerd te worden.
8. Klik op **OK**.
9. Pas de **permissies** aan voor de website, zodat alleen een gespecificeerde gebruiker toegang heeft tot de website.
10. Geef de naam en het wachtwoord van deze gebruiker door aan SURFconext (via support@surfconext.nl)

Basic Authentication wordt niet standaard mee 'geïnstalleerd' in de Server Rol 'Webserver (IIS)'. Deze feature dient eerst aan de rol toegevoegd worden

Pas de rol 'Web Server (IIS)' aan en enable de feature: Web Server - Security - **Basic Authentication**.

IP-adres restrictie

Om te zorgen dat alleen de SURFconext groepenomgeving verbinding mag maken met de website voer de volgende stappen uit:

1. Open IIS manager en ga naar de Website.
2. Open de '**Features View**' en dubbelklik op **IP Address and Domain Restrictions**.
3. Klik bij **Actions** op **'Add Allow Entry'**.
4. Selecteer '**IP address range'.**
5. IP adres: **145.100.191.192**.
6. Mask: **255.255.255.192**.
7. Klik **OK**.
8. Klik bij **Actions** op **'Add Allow Entry'**.
9. Selecteer '**IP address range'.**
10. IP adres: **2001:610:188:426::**
11. Mask: **64**.
12. Klik **OK**.

'IP and Domain Restrictions' wordt niet standaard mee 'geinstalleerd' in de Server Rol 'Webserver (IIS)'. Deze feature dient eerst aan de rol toegevoegd worden

Pas de rol 'Web Server (IIS)' aan en enable de feature: Web Server - Security - **IP and Domain Restrictions**.