VHS NyA-webben

> Mål: Teknisk dokumentation hur ett lärosäte gör för att ge handläggare vid lärosätet tillgång till NyA-webben.
> För frågor kring dokumentationen nedan kontakta operations snabel-a SWAMID.SE

NyA-webben är ett nytt och enklare sätt att ta fram vissa uppgifter ur NyA. Den är ett komplement till den s k expertklienten, och vänder sig i första hand till personal vid institutioner (motsvarande) men kan även vara till nytta för andra användargrupper.

Funktionaliteten i den första versionen motsvarar till största del behörighetsnivån Institutionsanvändare 1 i expertklienten.

Viktiga fördelar med NyA-webben är:

- Till skillnad från expertklienten öppnas den i en vanlig webbläsare.
- Den ska vara lättillgänglig och enkel att använda även för mindre vana användare.
- Den kräver ingen särskild programinstallation eller Java-uppdatering.

Inloggning och rollhantering sker med hjälp av identitetsfederationen SWAMID mot den lokala identitetshanteraren för respektive lärosäte. Användare av expertklienten använder även i fortsättningen traditionellt användarkonto i NyA.

I den första versionen kommer NyA-webben ha två olika roller:

- Basanvändare: Kan titta på sökandes meriter, anmälningar och dokument.
- Institutionsanvändare – utdata: Kan skapa listor och statistik för sökande, antagna och reserver för en eller institutioner.

Dokument från VHS som beskriver rollhantering i NyA:

- NyA-webben - ett nytt gränssnitt för institutionsanvändare
- Tekniska anpassningar för inloggning till NyA-webben
- Överföringsformat för behörighetsinformation på NyA-webben

Förutsättningar

1. Lärosätet har en IdP uppsatt som är medlem i SWAMID (Om frågor - kontakta operations snabel-a SWAMID.SE), för mer information se HowTo Shibboleth 2.x IdP.
2. Attribut skickas till samtliga SP i Swamid enligt SWAMID HowTo (Shibboleth 2.x). Särskilt att tänka på är att attributen `eduPersonPrincipalName` (eppn) och `commonName` (cn) ska överföras till NyA-webben tillsammans med rollerna.
3. VHS SP för NyA-webben är medlem i SWAMID med (namnet) https://www.antagning.se/ecs-sp och testsystemen är medlemmar i testfederationen med namnen https://www.antagning.testa.antagning.se/ecs-sp och https://www.antagning.testb.antagning.se/ecs-sp.

Rekommenderad arbetsgång

1. Modifiera attribute-resolvern för din IdP så att den inkluderar rättighet att använda NyA-webben enligt nedan beskrivet format (`eduPersonEntitlement` (epe)), se sidan SWAMID HowTo (Shibboleth 2.x).
2. Modifiera attribute-release policy för din IdP enligt kod nedan. Syftet är att tillåta ivägskickande av behörighetsinformation till VHS **SAMT** för test sp.swamid.se
3. Verifiera mot sp.swamid.se att ni ser namn, e-postadress, rättighet (entitlement) och unik identitet (`eduPersonPrincipalName` (eppn)).
4. Kontakta VHS för att få sin IdP inlagd i NyA-webben - appldrift_saml *snabel-a* VHS.SE.
5. Verifiera att inloggning med behörigheter fungerar via aktuell inloggningslänk som VHS tillhandahåller.

Konfiguration för Shibboleth

> Konfigurationerna under detta avsnitt fungerar endast för Shibboleth 2 eller senare. För simpleSAMLphp och ADFS2 kan konfigurationsexemplen endast användas som inspiration.

Modifiera filen attribute-resolver.xml:

Alternativ 1: Särskilt attribut finns i LDAP för att visa att en användare har en eller flera roller i NyA-webben

Nedan finns ett skript som transformerar rollattributet swamiGmaiAssertion till rättighetsattributet eduPersonEntitlement inkl. namnbyte på applikationen (NyA -> nya-dw) och tillägg av organisationskod för lärosätet. Skriptet är inte heller begränsat till rollerna basanvändare och institutionsanvändare utan kan hantera alla framtida roller i NyA-webben så länge de följer samma attribututformning som dessa.

Förutsättningar:

- När detta skrivs finns två roller NyA-webben, basanvändare och institutionsanvändare.
- Basanvändare (titta på info, meriter, anmälningar och dokument för sökande) är inte kopplat till institution:
  - I LDAP finns attributet swamiGmaiAssertion med värdet "urn:mace:swami.se:gmai:NyA:base".

    - Till NyA-webben skickas attributet eduPersonEntitlement med värdet "urn:mace:swami.se:gmai:nya-dw:base:o=YY".
- Institutionsanvändare - utdata (skapa listor och statistik) är kopplad till institution:
    - I LDAP finns attributet swamiGmaiAssertion med värdet "urn:mace:swami.se:gmai:NyA:department:ladokInstitutionskod=ZZZZ".
    - Till NyA-webben skickas attributet eduPersonEntitlement med värdet "urn:mace:swami.se:gmai:nya-dw:department:o=YY:norEduOrgUnitUniqueNumber=ZZZZ".
- YY är lärosätes kod i NyA, t.ex. UU.
- ZZZZ är en institutionskod, t.ex. 4010, som användaren har rätt att företräda för aktuell roll i NyA-webben.

```
<resolver:AttributeDefinition xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="
NyAwebbenEntitlement" >
     <resolver:Dependency ref="swamiGmaiAssertion" />
     <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:mace:dir:attribute-def:eduPersonEntitlement" />
     <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
     <Script>
          <![CDATA[
               importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);
               NyAwebbenEntitlement = new BasicAttribute("NyAwebbenEntitlement");
               if (swamiGmaiAssertion) {
                    for (i=0; i < swamiGmaiAssertion.getValues().size(); i++) {
                         if (swamiGmaiAssertion.getValues().get(i).search("urn:mace:swami.se:gmai:NyA:") != -1)
{
                              if (swamiGmaiAssertion.getValues().get(i).search(":ladokInstitutionskod=") != -1)
{
                                   NyAwebbenEntitlement.getValues().add(swamiGmaiAssertion.getValues().get(i).
replace(":NyA:", ":nya-dw:").replace(":ladokInstitutionskod=", ":o=YY:norEduOrgUnitUniqueNumber="));
                              }
                              else {
                                   NyAwebbenEntitlement.getValues().add(swamiGmaiAssertion.getValues().get(i).
replace(":NyA:", ":nya-dw:") + ":o=YY");
                              }
                         }
                    }
               }
          ]]>
     </Script>
</resolver:AttributeDefinition>
```

Alternativ 2: Grupper i LDAP används för att visa att en användare har en eller flera roller i NyA-webben (fungerar med Actice Directory)

Förutsättningar:

- När detta skrivs finns två roller NyA-webben, basanvändare och institutionsanvändare.
- Basanvändare (titta på info, meriter, anmälningar och dokument för sökande) är inte kopplat till institution:
    - Medlemmar i gruppen "NyA-webben-Base" ska få rollen när de loggar in i NyA-webben.
    - Till NyA-webben skickas attributet eduPersonEntitlement med värdet "urn:mace:swami.se:gmai:nya-dw:base:o=YY".
- Institutionsanvändare - utdata (skapa listor och statistik) är kopplad till institution:
    - Medlemmar i gruppen "NyA-webben-Department-ZZZZ" för institution ZZZZ ska få rollen för angiven institutionskod när de loggar in i NyA-webben.
    - Till NyA-webben skickas attributet eduPersonEntitlement med värdet "urn:mace:swami.se:gmai:nya-dw:department:o=YY:norEduOrgUnitUniqueNumber=ZZZZ".
- YY är lärosätes kod i NyA, t.ex. UU.
- ZZZZ är en institutionskod, t.ex. 4010, som användaren har rätt att företräda för aktuell roll i NyA-webben.

Känd begränsning:

- Grupper i grupper fungerar inte.

```
<resolver:AttributeDefinition xsi:type="Simple" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="memberOf"
dependencyOnly="true">
     <resolver:Dependency ref="myLDAP" />
</resolver:AttributeDefinition>

<resolver:AttributeDefinition xsi:type="Script" xmlns="urn:mace:shibboleth:2.0:resolver:ad" id="
NyAwebbenEntitlement" >
     <resolver:Dependency ref="memberOf" />
     <resolver:AttributeEncoder xsi:type="SAML1String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:mace:dir:attribute-def:eduPersonEntitlement" />
     <resolver:AttributeEncoder xsi:type="SAML2String" xmlns="urn:mace:shibboleth:2.0:attribute:encoder" name="
urn:oid:1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
     <Script>
          <![CDATA[
               importPackage(Packages.edu.internet2.middleware.shibboleth.common.attribute.provider);

               // Definiera lärosäteskod i NyA
               larosatekod = new String("YY");

               // Definiera grupp för basanvändare
               baseGroup = new String("NyA-webben-Base");

               // Definiera grupprefix för de olika rollerna
               deparmentGroupPrefix = new String("NyA-webben-Department-");

               NyAwebbenEntitlement = new BasicAttribute("NyAwebbenEntitlement");
               if (memberOf) {
                    for (i=0; i < memberOf.getValues().size(); i++) {

                         // Basanvändare ej begränsad till enskild institution
                         if (memberOf.getValues().get(i).equals(baseGroup)) {
                              NyAwebbenEntitlement.getValues().add("urn:mace:swami.se:gmai:nya-dw:base:o=" +
larosatekod);
                         }

                         // Institutionsanvändare begränsat till enskild institution via gruppnamnet
                         else if (deparmentGroupPrefix.equals(memberOf.getValues().get(i).substring(0,
deparmentGroupPrefix.length()-1))) {
                              NyAwebbenEntitlement.getValues().add("urn:mace:swami.se:gmai:nya-dw:department:
o=" + larosatekod + ":norEduOrgUnitUniqueNumber=" + memberOf.getValues().get(i).substring(deparmentGroupPrefix.
length(),memberOf.getValues().get(i).length()));
                         }
                    }
               }
          ]]>
     </Script>
</resolver:AttributeDefinition>
```

Modifiera filen attribute-filter.xml enligt:

```
<AttributeFilterPolicy id="releaseNyAwebbenEntitlement">
     <PolicyRequirementRule xsi:type="basic:OR">
          <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://expert.antagning.se/ecs-sp" />
          <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://www.antagning.testa.antagning.se
/ecs-sp" />
          <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://www.antagning.testb.antagning.se
/ecs-sp" />
          <basic:Rule xsi:type="basic:AttributeRequesterString" value="https://sp.swamid.se/shibboleth" />
     </PolicyRequirementRule>
     <AttributeRule attributeID="NyAwebbenEntitlement">
          <PermitValueRule xsi:type="basic:ANY" />
     </AttributeRule>
</AttributeFilterPolicy>
```