UHR 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.

Förnärvarande finns fem olika roller i NyA-webben:

- Basanvändare: Kan titta på sökandes meriter, anmälningar och dokument.
- Institutionsanvändare – Utdata: Kan skapa listor och statistik för sökande, antagna och reserver för en eller flera institutioner.
- Institutionsanvändare – Bedömning: Kan besluta om särskild behörighet samt registrera och titta på värden för alternativa meriter.
- Sen anmälan och efterantagning. Kan uppdatera efterantagningstal och stänga för sen anmälan för anmälningsalternativ som hör till den egna institutionen.
- Sen anmälan och efterantagning - tittbehörighet. Kan se uppgifter om efterantagningstal samt när anmälningsalternativ stänger för anmälan, för den egna institutionen.

För att en användare med rollen "Institutionsanvändare – Bedömning" ska kunna se information om personer bör den även ha rollen "Basanvändare".

Dokument från UHR som beskriver rollhantering i NyA:

- Överforingsformat för behorighetsinformation på NyA-webben uppdaterat inför leverans 2015_05.doc

Förutsättningar

1. Lärosätet har en Identity Provider uppsatt som är medlem i SWAMID (Om frågor - kontakta operations snabel-a SWAMID.SE.
2. Attribut skickas till Service Providers i Swamid enligt avsnittet attribute-filter.xml på wikisidan Konfigurera metadata för att använda SWAMID. Särskilt att tänka på är att attributen `eduPersonPrincipalName` (EPPN) och `commonName` (CN) ska överföras till NyA-webben tillsammans med rollerna.
3. UHR:s SP för NyA-webben är medlem i SWAMID med entityId **https://expert.antagning.se/ecs-sp** (Produktion) respektive **https://expert.test.antagning.se/ecs-sp** (Test)

Rekommenderad arbetsgång

1. Modifiera attribute-resolvern för din Identity Provider så att den inkluderar rättighet att använda NyA-webben enligt nedan beskrivet format (`eduPersonEntitlement` (EPE)), se sidan Konfigurera metadata för att använda SWAMID.
2. Modifiera attribute-release policy för din Identity Provider 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 UHR för att få sin IdP inlagd i NyA-webben - appldrift_saml *snabel-a* UHR.SE.
5. Verifiera att inloggning med behörigheter fungerar via aktuell inloggningslänk som UHR 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 tre roller basanvändare, institutionsanvändare - utdata och institutionsanvändare - bedömning.
- Basanvändare (titta på info, meriter, anmälningar och dokument för sökande) är inte kopplad 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".
- Institutionsanvändare – Bedömning (registrera och titta på värden för alternativa meriter) är kopplad till institution:
  - I LDAP finns attributet swamiGmaiAssertion med värdet "urn:mace:swami.se:gmai:NyA:department_assessment:ladokInstitutionskod=ZZZZ".
  - Till NyA-webben skickas attributet eduPersonEntitlement med värdet "urn:mace:swami.se:gmai:nya-dw:department_assessment: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.
- LDAP-attribut för gruppmedlemskapet är memberOf med gruppnamnet som värde.

```
<resolver:AttributeDefinition xsi:type="Script" id="NyAwebbenEntitlement" >
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:
attribute-def:eduPersonEntitlement" />
     <resolver:AttributeEncoder xsi:type="SAML2String" name="urn:oid:
1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
     <Script>
          <![CDATA[
               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 tre roller basanvändare, institutionsanvändare - utdata och institutionsanvändare - bedömning.
- Basanvändare (titta på info, meriter, anmälningar och dokument för sökande) är inte kopplad 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".
- Institutionsanvändare – Bedömning (registrera och titta på värden för alternativa meriter) är kopplad till institution:
  - Medlemmar i gruppen "NyA-webben-DepartmentAssessment-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_assessment: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="Script" id="NyAwebbenEntitlement" >
     <resolver:Dependency ref="myLDAP" />
     <resolver:AttributeEncoder xsi:type="SAML1String" name="urn:mace:dir:
attribute-def:eduPersonEntitlement" />
     <resolver:AttributeEncoder xsi:type="SAML2String" name="urn:oid:
1.3.6.1.4.1.5923.1.1.1.7" friendlyName="eduPersonEntitlement" />
     <Script>
          <![CDATA[
               // 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-");
               deparmentAssessmentGroupPrefix = new String("NyA-webben-
DepartmentAssessment-");
               deparmentLateAdmissionGroupPrefix = new String("NyA-webben-
DepartmentLateAdmission-");
               deparmentReserveAdmissionGroupPrefix = new String("NyA-
webben-DepartmentReserveAdmission-");

               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 - utdata 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()));
                        }

                        // Institutionsanvändare - bedömning begränsat
till enskild institution via gruppnamnet
                        else if (deparmentAssessmentGroupPrefix.equals
(memberOf.getValues().get(i).substring(0,deparmentAssessmentGroupPrefix.
length()-1))) {
                            NyAwebbenEntitlement.getValues().add("urn:
mace:swami.se:gmai:nya-dw:department_assessment:o=" + larosatekod + ":
norEduOrgUnitUniqueNumber=" + memberOf.getValues().get(i).substring
(deparmentAssessmentGroupPrefix.length(),memberOf.getValues().get(i).
length()));
                        }

                        // Institutionsanvändare - sen antagning
begränsat till enskild institution via gruppnamnet
                        else if (deparmentLateAdmissionGroupPrefix.equals
(memberOf.getValues().get(i).substring(0,deparmentLateAdmissionGroupPrefix.
length()-1))) {
                            NyAwebbenEntitlement.getValues().add("urn:
mace:swami.se:gmai:nya-dw:department_late_admission:o=" + larosatekod + ":
norEduOrgUnitUniqueNumber=" + memberOf.getValues().get(i).substring
(deparmentLateAdmissionGroupPrefix.length(),memberOf.getValues().get(i).
length()));
                        }

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

Modifiera filen attribute-filter.xml enligt:

I Example of a standard attribute filter for Shibboleth IdP finns användningen filter NyA-webben definierad men bortkommenterad.