MTA SZTAKI

# Icinga SAML azonosítással

Szabó Gyula, MTA SZTAKI ITAK

2012. november 10.

# A feladat

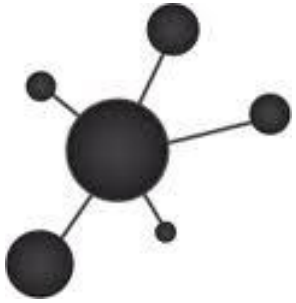
Negyedik projekt felügyelete

új nagios instance?

akkor már frissítsünk,
icinga
akkor már optimalizáljunk,
ne legyen x instance, legyen egy (mind felett);
azonosítsunk föderatív alapokon;
osszunk jogosultságokat központilag, sőt delegáltan.

# A megoldás

## Icinga



- icinga core
- classic ui
  - csoportkezelés shibboleth attribútum alapján
- icinga-web
  - "If you have new providers, please share them and let the auth database grow!"

# A megoldás

User story:

Ha egy felhasználó egy bizonyos csoport tagja, akkor bejelentkezés után csak a csoporthoz tartozó felügyelt objektumokat láthassa!

Ha több csoport tagja, akkor láthassa az összes felügyelt objektumot, amiket a csoporttagságai alapján láthat!

# A megoldás

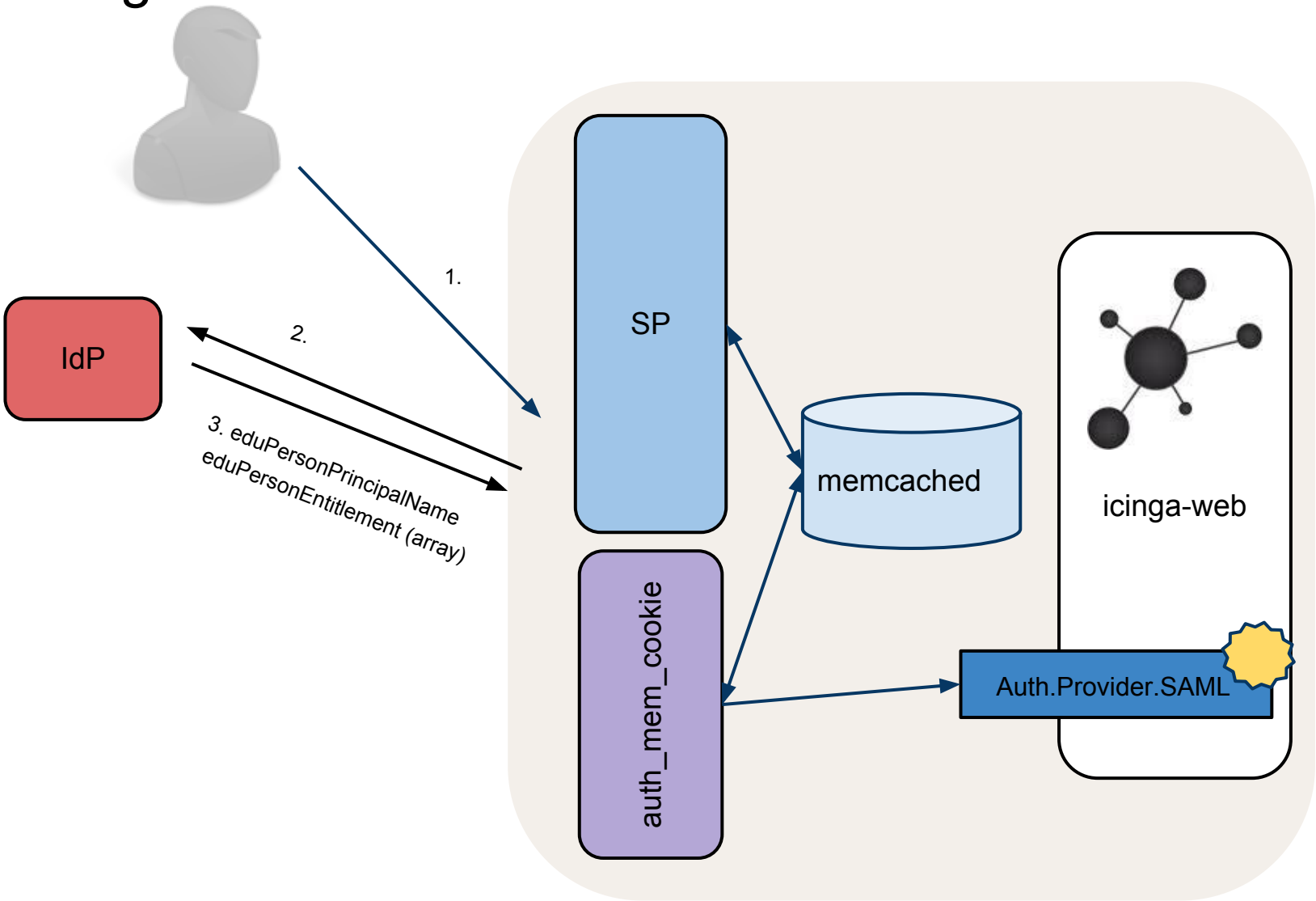
simpleSAMLphp + auth_mem_cookie kombó

icinga-web auth provider

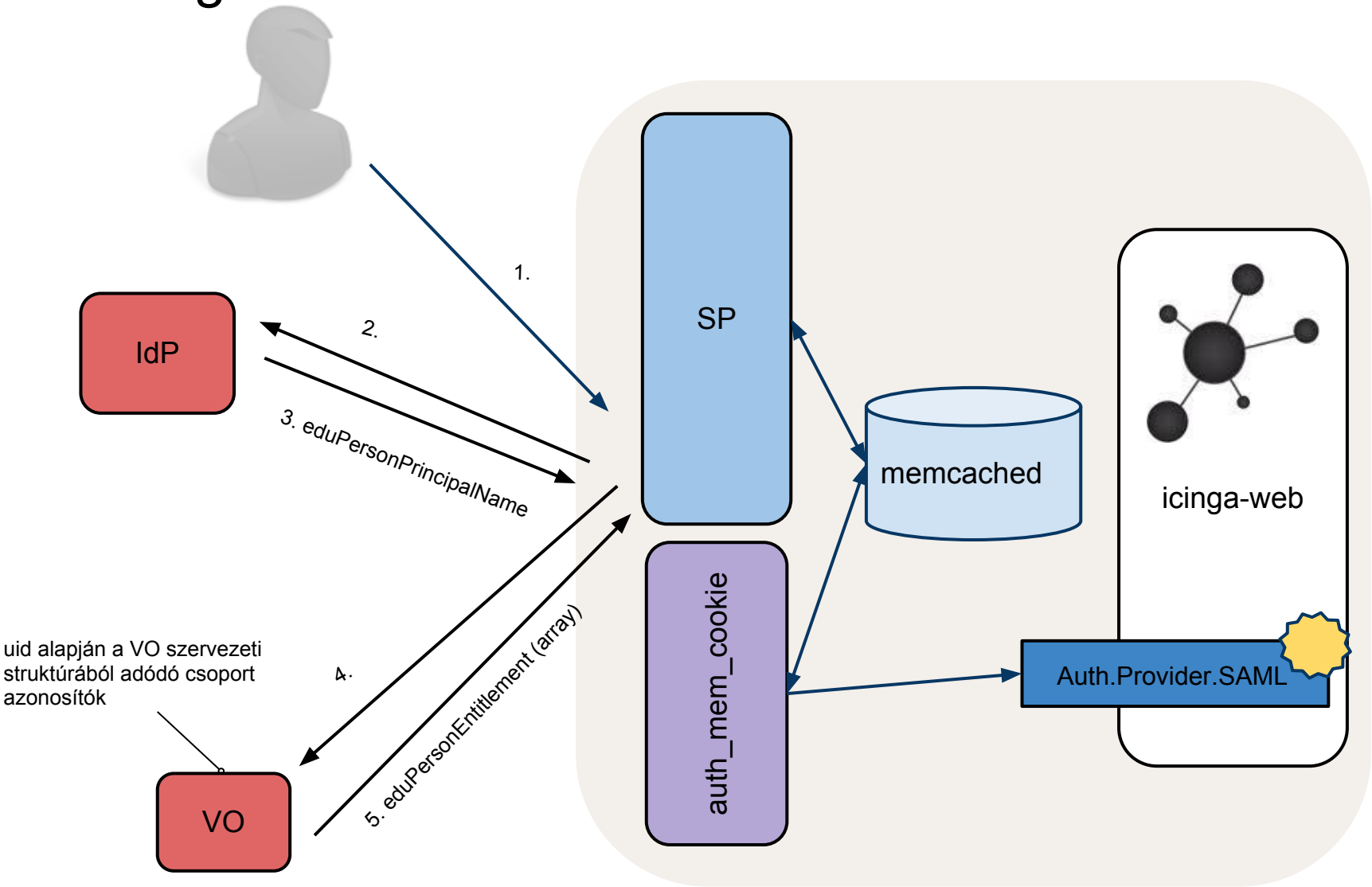
SAMLAuthProvider.php
- logika (create, update)

auth.site.xml
- attribútum mapping, $_SERVER tömb

# A megoldás


1.
2.
3. eduPersonPrincipalName
eduPersonEntitlement (array)
IdP
SP
memcached
auth_mem_cookie
icinga-web
Auth.Provider.SAML

# A megoldás


1.
2.
3. eduPersonPrincipalName
IdP
SP
memcached
icinga-web
auth_mem_cookie
Auth.Provider.SAML
uid alapján a VO szervezeti struktúrából adódó csoport azonosítók
4.
5. eduPersonEntitlement (array)
VO

# A telepítés

```
app/modules/AppKit/models/
Auth/Provider/SAMLModel.class.php
```

# A konfiguráció

`conf.d/auth.site.xml`

Három részre tagolódik

- alapvető beállítások
  - definiálás, bekapcsolás, viselkedés
- attribútum mappelés
  - user id, email cím, név
- csoport mappelés
  - jogosultságok

# A konfiguráció

```
<setting name="provider">
        <ae:parameter name="SAML_authentication">
          <ae:parameter name="auth_module">AppKit</ae:parameter>
          <ae:parameter name="auth_provider">Auth.Provider.SAML</ae:parameter>

          <ae:parameter name="auth_enable">true</ae:parameter>
          <ae:parameter name="auth_authoritative">true</ae:parameter>

          <ae:parameter name="auth_create">true</ae:parameter>
          <ae:parameter name="auth_update">true</ae:parameter>
```

# A konfiguráció

```
.....
    <ae:parameter name="auth_map">
        <ae:parameter name="user_firstname">MCAC_ATTR_givenName
                </ae:parameter>
        <ae:parameter name="user_lastname">MCAC_ATTR_sn
                </ae:parameter>
        <ae:parameter name="user_email">MCAC_ATTR_mail
                </ae:parameter>
        <ae:parameter name="user_name">MCAC_ATTR_eduPersonPrincipalName
                </ae:parameter>
        <ae:parameter name="user_authid">MCAC_ATTR_eduPersonPrincipalName
                </ae:parameter>
        <ae:parameter name="auth_name">MCAC_ATTR_eduPersonPrincipalName
                </ae:parameter>
    </ae:parameter>
...
```

# A konfiguráció

```
.....
        <ae:parameter name="role_attribute">MCAC_ATTR_eduPersonEntitlement
              </ae:parameter>
        <ae:parameter name="role_prefix">urn:geant:niif.hu:sztaki:icinga:
              </ae:parameter>

        <ae:parameter name="role_guest">4</ae:parameter>
        <ae:parameter name="role_admin">admin</ae:parameter>

        <ae:parameter name="role_map">
          <ae:parameter name="admin">
              <ae:parameter>2</ae:parameter>
              <ae:parameter>3</ae:parameter>
          </ae:parameter>
          <ae:parameter name="itak">
              <ae:parameter>6</ae:parameter>
          </ae:parameter>
        </ae:parameter>

      .....
    </setting>
```

eduPersonEntitlement

group_id@icinga-web

# Eredmény

Egy felügyeleti rendszer az összes projektnek;

föderatív azonosítás (SSO, SAML);

alkalmazástól leválasztott (pl. VO) jogosultságkezelés.

# Eredmény

Valódi ereje a VO-sítás után látszik, a szolgáltatáshoz történő hozzáférést a projekt menedzserei szabályozzák.

Az icinga gazdájának a felügyelt objektumok konfigurációján kívül nem kell foglalkoznia felhasználókkal.

Kérdések?

Köszönöm a figyelmet!