INSTITUCINIO SSO NAUDOTOJO VADOVAS

REIKALAVIMAI SISTEMAI

Sistema testuota Linux Debian ir Ubuntu distribucijose. Pagrindiniai reikalavimai:

- Python3 palaikymas
- Docker palaikymas
- Python paketų valdymo įrankio (pip) palaikymas
- Nginx palaikymas

SISTEMOS DIEGIMO ŽINGSNIAI

1. Sudiegiamos docker bibliotekos python kalbai:
   (ln -s /usr/bin/pip3 /usr/bin/pip)
   pip install docker
2. Nukopijuojamas simpleContainers scenarijus į darbinį katalogą.
   git clone https://github.com/litnet/simpleContainers
3. Sukuriamas konteineris:
   cd simpleContainers/
   ./simpleContainers --action=create -n [konteinerio_pavadinimas] -p 127.0.0.1:8080:80 -v /etc/simplesamlphp -i litnet/simplesamlphp-idp:latest
   (šiame žingsnyje parsiunčiamas ir paleidžiamas konteineris, kurio konfigūracija patalpinama į pastovų diską, pasiekiamą iš docker serverio. Sukūrus konteinerį atspausdinamas konteinerio ID.)
4. Atliekama pradinė konfigūracija sukuriant sertifikatus ir administratoriaus slaptažodžius:
   docker exec -it [konteinerio_id] /root/first_run.sh
   (serveryje esančių docker konteinerių ID galima gauti naudojant komandą „docker ps“)
5. SimpleSAMLphp konfigūracijos vietą galima gauti naudojant komandą:
   docker volume inspect [konteinerio_pavadinimas]
   Pagal nutylėjimą ji talpinama kataloge /var/lib/docker/volumes
6. Byloje „authsources.php“ yra paruošta pradinė konfigūracija naudojant LDAP arba ActiveDirectory tarnybas. Pasirinktinai nuo sistemos, kurioje yra naudotojų duomenys, atkomentuojama viena arba kita konfigūracija ir papildoma prisijungimo duomenimis.
7. Norint naudotis LitNET FEDI „discovery“ paslauga reikėtų papildomai paleisti komandą įgalinančią FEDI metaduomenų sinchronizavimo galimybę:
   docker exec -it [konteinerio_id] /root/enable_FEDI.sh
8. Norint naudotis LitNET FEDI ir eduGAIN „discovery“ paslauga reikėtų papildomai paleisti komandą įgalinančią FEDI ir eduGAIN metaduomenų sinchronizavimo galimybę:
   docker exec -it [konteinerio_id] /root/enable_FEDI-eduGAIN.sh
9. Jeigu reikia išjungti FEDI arba FEDI ir eduGAIN metaduomenų sinchronizavimą bei išvalyti metaduomenis, tuomet reikėtų paleisti šią komandą:
   docker exec -it [konteinerio_id] /root/clean_metadata_config.sh
10. Simplesamlphp vartotojo „admin“ (reikalingo prisijungti prie administravimo svetainės) slaptažodis sugeneruojamas automatiškai ir randasi byloje „secrets.inc.php“.

11. Kad konteineryje veikiantis SSO būtų pasiekiamas naudotojams, nginx „/etc/nginx/sites-available/default“ konfigūracijos byloje pakeičiama „proxy_pass“ reikšmė į konteinerio sukūrimo metu naudoto adreso ir prievado reikšmes bei užkomentuojama eilutė „try_files $uri $uri/ =404;“:

```
location / {
        proxy_pass http://127.0.0.1:8080;
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        # try_files $uri $uri/ =404;
        proxy_set_header Host $host;
}
```

    Galiausiai perkraunamas nginx servisas įvykdant „service nginx reload“ arba „/etc/init.d/nginx reload“ komandą.

12. Administravimo puslapis pasiekiamas adresu „http://[serverio_adresas]/simplesamlphp“.

SISTEMOS ATNAUJINIMAS

Kadangi naudojama centrinė repozitorija, sistema atnaujinama viena komanda:

./simpleContainers --single --action=upgrade --name=[konteinerio_pavadinimas]

Ją įvykdžius naujausia versija bus atsiųsta ir įdiegta, išsaugant konfigūraciją, padarytą diegimo metu.

SISTEMOS NAUDOJIMAS

Tam, kad vyktų autentifikavimas institucinio SSO pagalba, naudotojo informacinėje sistemoje turi būti įdiegta biblioteka, įskiepis, papildinys ar modulis skirtas duomenų apsikeitimui tarp informacinės sistemos ir SimpleSAMLphp. Naudotojas pateikia sugeneruotą XML bylą SSO prižiūrinčiam administratoriui. Administratorius bylos turinį įkelia simplesamlphp formatu į SSO konfigūracijos bylą „/var/lib/docker/volumes/[konteinerio_pavadinimas]/_data/metadata/saml20-sp-remote.php“. XML bylos konvertavimui į simplesamlphp formatą naudojamas konverteris „XML to SimpleSAMLphp metadata converter“ esantis adresu „http://[serverio_adresas]/simplesamlphp/admin/metadata-converter.php“.

Patikrinti ar veikia metaduomenų sinchronizavimas su LiteNET FEDI ar eduGAIN galima įsitikinti užėjus adresu „https://[serverio_adresas]/simplesamlphp/module.php/core/frontpage_federation.php“. Šiame puslapyje turi atsirasti sąrašas patikimų paslaugų tiekėjų metaduomenų.

SISTEMOS REZERVINIS KOPIJAVIMAS IR ATSTATYMAS

Centralizuotai prižiūrimų SSO paslaugų sistemos rezervinis kopijavimas.

Centralizuotai prižiūrimų SSO esančio VU duomenų centre sistemos rezervinis kopijavimas vykdomas VU turimomis vidinėmis priemonėmis. T. y. Backup Exec programinės įrangos pagalba nukopijuojamas visas virtualus serveris kuriame veikia SSO paslauga.

Incidento atveju kuomet reikia atstatyti sistemą atstatomas visas virtualus serveris į hypervizorių. Startavus serveriui jame automatiškai pasileidžia Docker konteineriai su juose sukonfigūruotomis SSO paslaugomis.

Institucijų infrastruktūroje veikiančių SSO paslaugų rezervinis kopijavimas

Institucijų infrastruktūroje veikiančių SSO paslaugų rezervinis kopijavimas gali būti atliekamas kopijuojant visas konfigūracijos bylas esančias kataloge „/var/lib/docker/volumes/[konteinerio_pavadinimas]/_data“ į atskirą rezervinėms kopijoms skirtą diską.

Incidento atveju sistema atstatoma naujai įdiegiant serverį ir jį parengiant pagal institucinio SSO diegimo instrukcijas. Vėliau į jau paleisto konteinerio „/var/lib/docker/volumes/[konteinerio_pavadinimas]/_data“ katalogą įkopijuojamos vėliausio rezervinio kopijavimo metu nukopijuotos konfigūracijos bylos.