

KATEDRA ZA OPERACIJSKE SUSTAVE

Autentikacijski sustavi i baze podataka

Projektni zadatak

REV 2.0

Uvod

AAA proces (Authentication, Autorization, Accounting) je dio našeg svakodnevnog IT života. Primjera radi, prijavom na vaše računalo započinju naše svakodnevne aktivnosti – dobivate mogućnost pokretanja aplikacija, prijave na poslovni sustav na poslu, prijave na web-stranice... Projekti koji slijede su logična ekstenzija tog načina razmišljanja. Tvrtke svih veličina koriste zajedničke autentifikacijske sustave bazirane na LDAP standardu kako bi olakšale administraciju svojih poslovnih informacijskih sustava.

Opis okoline – programski smjer

Tvrtka Authentication services d.o.o u svom poslovanju koristi okolinu baziranu na standardnim operacijskim sustavima i cloud rješenjima (Windows, Windows+Azure ili Linux). Potrebno je implementirati SSO sustav prema traženom zadatku.

Projekt za studente programskog inženjerstva

Ovaj projekt uključuje implementaciju mogućnosti jedinstvene prijave (SSO) za web aplikacije koje koriste Keycloak i FreeIPA, posebno se fokusirajući na integraciju OpenID-a i SAML autentifikacije. Keycloak je rješenje za upravljanje identitetom i pristupom otvorenog koda koje omogućuje federaciju korisnika iz različitih LDAP izvora, uključujući 389-Server, OpenLDAP i MS Active Directory. Također omogućuje prijavu bez lozinke pomoću Kerberos ticketa za klijente, dodajući praktičnost i sigurnost korisnicima unutar organizacije. Integracija se fokusira na poboljšanje sigurne autentifikacije u aplikacijama kao što je WordPress, omogućujući besprijekornu prijavu putem OpenID/SAML-a bez potrebe za lozinkama na uređajima koji podržavaju Kerberos.

Zahtjevi: Primarni zahtjevi za postavljanje ove integracije uključuju osnovnu instalaciju Red Hat Enterprise Linuxa (RHEL) 8 i potrebne pretplate za Red Hat SSO i JBoss EAP. Osim toga, za upravljanje identitetom i integraciju s Keycloakom preporučuje se konfigurirano FreeIPA ili Red Hat IdM okruženje, što omogućuje centraliziranu autentifikaciju korisnika. Projekt će također trebati web aplikaciju kao što je WordPress (ili bilo koja OpenID/SAML platforma s omogućenim OpenID-om) za testiranje postavki autentifikacije. Keycloak će služiti kao središnje SSO rješenje, objedinjavajući korisnike i nudeći fleksibilne mehanizme provjere autentičnosti za podršku prijavama temeljenim na lozinkama i bez lozinke (Kerberos).

Za postavljanje je potrebno najmanje 4 GB RAM-a i 50 GB prostora na disku, što je dovoljno za osnovnu konfiguraciju. Za uspješnu implementaciju projekta trebati će vam sljedeći paketi i repozitoriji: JBoss Enterprise Application Platform, Red Hat CodeReady Linux Builder i Single Sign-On paketi za RHEL 8.

Potrebne pretplate i alati

Studentima su potrebne aktivne pretplate za RHEL 8 i JBoss EAP za pristup Red Hatovim podržanim softverskim paketima. Za pristup pretplatama i licencama prijavite se na RedHat

stranicu i zatražite besplatni developer račun (<https://developers.redhat.com/>), nakon čega sa <https://access.redhat.com/downloads/content/rhel> preuzmite potrebne image datoteke. Također, to će vam omogućiti i pristup potrebnim repozitorijima za instalaciju potrebnih paketa (kao što su rh-ss0, httpd, mod_ssl i socat), kao i ACME shell skripte za rukovanje Let's Encrypt certifikatima. Konačno, studenti moraju konfigurirati Apache HTTP kao obrnuta proxy za sigurnu komunikaciju, omogućujući Keycloaku da učinkovito upravlja SSL certifikatima.

Napomena: Template za izradu projekta nalazi se na InfoEduci.

Opis okoline – sistemski smjer

Tvrtka Authentication services d.o.o u svom poslovanju koristi okolinu baziranu na standardnim operacijskim sustavima i rješenjima (Windows ili Linux). Potrebno je napraviti integraciju Active Directory i OpenLDAP rješenja na način da se konfigurira dvosmjerni *trust* (na vama je da odaberete da li ćete koristiti OpenLDAP ili FreeIPA rješenje).

Projektni zadatak za studente studenata smjera sistemskog inženjerstva

Prerequisite: Potrebno je instalirati jedan Windows Servera 2012, 2016, 2019 ili 2022, te jedan Linux server. Na Windows serveru potrebno je instalirati Active Directory Domain Services. Na Linux serveru potrebno je instalirati OpenLDAP, samba, SASL*, FreeIPA-u ili nešto slično uz pomoć čega ćete uspješno završiti projektni zadatak. Projektni zadatak je da spojite dotična dva servera ostvarite obostrano povjerenje. Način na koji ćete provjeriti *trust* je da pokušate u AD-u napraviti korisnika, koji mora biti vidljiv i na OpenLDAP/SAMBA/SASL*/FreeIPA serveru, i obrnuto.

Predaja projekta

Projekt se treba predati najkasnije do 11.1.2025. u 23:59:59. Svako kašnjenje znači gubitak jednog boda po ishodu po tjednu kašnjenja. Template za projekt nalazi se u folderu kolegija na InfoEduci. U projektnom dokumentu do detalja opisati sve što ste napravili – programski kod, screenshoti, procedure – da biste ostvarili cilj projekta. Također, na prvoj stranici projektnog dokumenta napisati vaše podatke i smjer.

Predaja izvan definiranog roka znači ponavljanje kolegija ako niste skupili dovoljni broj bodova. Konzultacije o radu su moguće mailom ili uživo u terminima vježbi.

Projekt predajete na InfoEduku pod seminarski rad iz predmeta ASBP – projekte predane mailom ne priznajemo.

Dodatna dokumentacija – programski smjer

1. <http://woshub.com/configuring-kerberos-authentication-on-iis-website/>
2. <https://www.codemag.com/Article/1312041/Using-Active-Directory-in-.NET>
3. <https://auth0.com/blog/using-ldap-with-c-sharp/>
4. https://www.freeipa.org/page/Web_App_Authentication
5. <https://blog.delouw.ch/2019/06/01/openid-and-saml-authentication-with-keycloak-and-freeipa/>
6. https://www.freeipa.org/page/Web_App_Authentication/Example_setup

Dodatna dokumentacija – sistemski smjer

1. <https://www.geeksforgeeks.org/directory-services-in-distributed-system/>
2. https://www.freeipa.org/page/Active_Directory_trust_setup
3. <https://www.freeipa.org/page/Trusts>
4. <https://learn.microsoft.com/en-us/entra/identity/domain-services/concepts-forest-trust>