WARSZTATY WEBSSO

Integracja systemów z KeyCloak

Prosimy o wysłuchanie komentarza prowadzącego przed przystąpieniem do realizacji ćwiczeń praktycznych.

Pamiętaj aby akceptować ostrzeżenia dotyczące nieautoryzowanych certyfikatów bezpieczeństwa w przeglądarkach. Alternatywnie możesz zaimportować certyfikaty z katalogu tmp – pliki *.crt do swojej przeglądarki. Po jej ponownym uruchomieniu nie powinieneś być pytane o akceptację certyfikatów.

Jeśli jeszcze tego nie zrobiłeś uruchom uprzednio zbudowane środowisko wchodząc do katalogu ze sklonowanym repozytorium i wydaj komendę:

Osoby posiadające 4GB pamięci w powinny wydać komendę uruchamiającą jedynie 3 maszyny wyłączając przed uruchomieniem poprzednio uruchomione maszyny systemu CAS:

vagrant halt *cas.websso.linuxpolska.pl appcas.websso.linuxpolska.pl*

vagrant up 389ds.websso.linuxpolska.pl keycloak.websso.linuxpolska.pl appkeycloak.websso.linuxpolska.pl

Jeśli posiadasz więcej niż 4GB ramu wydaj komendę:

vagrant up

Sprawdzenie środowiska przed wykonaniem zadań:

W przeglądarce wywołaj trzy adresy:

https://keycloak.websso.linuxpolska.pl/auth

https://appkeycloak.websso.linuxpolska.pl/wordpress/

https://appkeycloak.websso.linuxpolska.pl/liferay/

Jeśli wszystkie trzy strony pokazują się poprawnie – twoje 3 maszyny pracują poprawnie – ćwiczenia powinno udać się zrealizować.

Jeśli nie zbudowałeś środowiska warsztatowego przed warsztatami wysłuchaj prowadzącego, aby móc przeprowadzić ćwiczenia samodzielnie w późniejszym terminie – zbudowanie środowiska nie uda się na warsztatach (ograniczenie przepustowości sieci i czasu trwania ćwiczeń). Problemy z budową środowiska zgłoś prowadzącemu na zakończenie warsztatów na pewno coś doradzi – alternatywnie zgłoś problem poprzez repozytorium Github:
https://github.com/linuxpolska/WEBSSOOpenSourceDay2017

UWAGA!!!

Realizując zadania nie wylogowuj się z kont administracyjnych do momentu sprawdzenia poprawności wykonanej konfiguracji w innej przeglądarce lub oknie incognito tej samej przeglądarki – inaczej ewentualny drobny błąd lub literówka uniemożliwi ci ponowne zalogowanie się danej aplikacji.

Zadanie 1

Utworzenie nowego realmu w systemie KeyCloak

1. Wywołaj serwer aplikacji wpisując adres:
   https://keycloak.websso.linuxpolska.pl
2. Skorzystaj z odnośnika **Administration Console** aby połączyć się z interfejsem administracyjnym systemu KeyCloak
3. Zaloguj się na konto administratora wpisując dane:
   Username or email: **admin**
   password: **admin**
4. W celu dodania nowego realmu w lewym górnym rogu interfejsu **KeyCloak** wskaż nazwę **Realmu Master** i wybierz przycisk **Add Realm**
5. W oknie **Add realm** w polu **Name** wpisz nazwę Twojego realmu: **websso**
   Uwaga!!! do tej nazwy będą się odwoływały pozostałe ćwiczenia (jak określisz swoją nazwę – w przypadku wystąpienia problemów będziesz zdany na siebie)
6. Wybierz przycisk **Create**.
7. Twój realm zostanie dodany w polu display name możesz wpisać przyjazny opis jakie będą widzieli użytkownicy na stronie logowania np.: Warsztaty WEBSSO. Po wprowadzeniu opisu zapisz zmiany wybierając przycisk **Save**.
8. Przed przystąpieniem do wykonywania ćwiczeń warto jest odblokować zaawansowane logowanie zdarzeń w tym celu z Menu po lewej stronie wybierz: **Events**
9. Po otwarciu okna **Events Config** wybierz zakładkę **Config**
10. W sekcji **Login Events Settings** włącz opcję **Save Events**
11. W sekcji **Admin Events Settings** włącz opcję **Save Events**
12. Nie zmieniaj pozostałych ustawień
13. Zapisz zmiany wybierając przycisk **Save**
14. Twój realm jest wstępnie skonfigurowany i jest gotowy do uwierzytelniania – nie masz w nim jednak użytkowników

Zadanie 2

Dodanie zewnętrznego systemu uwierzytelniania (federacja użytkowników w oparciu o usługę katalogową LDAP)

1. Po zalogowaniu do interfejsu administracji systemu KeyCloak i wybraniu swojego realmu: websso
2. Aby dodać system uwierzytelniania Menu po lewej stronie wybierz: **User Fedration.**
3. W oknie **User Federation** z listy **Add provider** wybierz: **ldap**

- W otwartym oknie **add user storage provider** uzupełnij dane zgodnie z poniżej podanymi informacjami:
- **Wyłącz** opcję: **Import Users (Nie będziemy przenosić użytkowików)**
- Z listy **Edit Mode** wybierz **Read Only**
- **Wyłącz** opcję: **Sync Registration**
- Z listy **Vendor** wybierz: **Red Hat Directory Server (pozwoli to na uzupełnienie opcji domyślnych ułatwiając naszą konfigurację)** podstawą usługi RHDS jest baza 389ds z której my korzystamy – wybranie wzorca ułatwi konfigurację
- W polu **Connection URL** wpisz: ldap://ldap.websso.linuxpolska.pl
- Sprawdź możliwość połączenia przyciskiem **Test Connection –** w przypadku sukcesu przejdź dalej jeśli otrzymasz komunikatu błędu popraw adres, upewnij się, że maszyny 389ds.websso.linuxpolska.pl pracuje (vagrant status)
- W polu **Users DN** wpisz: **ou=users,dc=linuxpolska,dc=pl**
- W polu **Bind DN** wpisz: **uid=connectionagent,dc=linuxpolska,dc=pl**
- W polu **Bind Credential** wpisz**: SSO@g3nt**
- Sprawdź możliwość połączenia wybierając przycisk: **Test Authentication**
- W przypadku sukcesu przejdź dalej jeśli otrzymasz komunikatu błędu popraw dane autoryzacji (2 powyższe punkty)
- Zapisz zmiany w swojej konfiguracji wybierając przycisk **Save**.

  Federacja użytkowników w oparciu o bazę usługi katalogwej LDAP została skonfigurowana – KeyCloak będzie obsługiwał żądania uwierzytelnienia w oparciu o bazę LDAP.

Zadanie 3

Konfiguracja aplikacji klienckiej na przykładzie LifeRay przy użyciu protokołu OIDC.

1. Po zalogowaniu do interfejsu administracji systemu KeyCloak i wybraniu swojego realmu: websso
2. Aby dodać system aplikację kliencką z Menu po lewej stronie wybierz: **Clients**
3. W otwartym oknie skorzystaj z przycisku **Create** (prawy róg ekranu)
4. W otwartym oknie Add Client uzupełnij dane według poniższego wzroca:

- **Client ID: liferay-oidc**
- **Client Protocol: openid-connect**
- **Nie zmieniaj pozostałych opcji**

5. Zapisz zmiany wybierając przycisk **Save**
6. W otwartym oknie **Liferay-OIDC** uzupełnimy dane **dotyczące adresów przekierowania.**

   Uzupełnimy adres serwisu w polu **Valid Redirect URIs:**
   https://appkeycloak.websso.linuxpolska.pl/liferay*
7. Zapisz zmiany wybierając przycisk **Save**
8. Konfiguracja logowania poprzez OIDC do portalu liferay dokonamy poprzez zmianę globalnych ustawień portalu w konsoli – wtyczka do autoryzacji nie posiada własnego gui konfiguracyjnego.
9. W celu konfiguracji przejdź do konsoli w której uruchomiłeś środowisko, upewnij się, że jesteś w katalogu ze sklonowanym repozytorium.
10. Połącz się z maszyną wirtualną wydając komendę:
    vagrant ssh appkeycloak.websso.linuxpolska.pl
11. Po połączeniu z maszyną przejmij uprawnienia roota wykonując komendę:
    su -
12. Wprowadź hasło roota: **vagrant**
13. Przy użyciu ulubionego edytora tekstowego (vi, emacs, nano) dokonaj edycji pliku konfiguracyjnego portalu liferay (oczywiście wydaj komendę, która odpowiada twoim preferencjom edycyjnym)**:**
    vi /opt/liferay/tomcat-8.0.32/webapps/ROOT/WEB-INF/classes/portal-ext.properties
    lub
    nano /opt/liferay/tomcat-8.0.32/webapps/ROOT/WEB-INF/classes/portal-ext.properties
    lub
    emacs /opt/liferay/tomcat-8.0.32/webapps/ROOT/WEB-INF/classes/portal-ext.properties
14. W pliku poddanym edycji odnajdź opcję dotyczące integracji portalu z openidc.
15. Zmień opcję: **openidconnect.enableOpenIDConnect** z **false** na **true**

16. Upewnij się, że opcja: **openidconnect.client-id** odpowiada wpisanemu przez Ciebie w punkcie **4** identyfikatorowi klienta

17. Upewnij się, że w adresach wskazujących serwer keycloak znajduje się właściwa nazwa realmu (zgodnie z instrukcją websso)

18. Zapisz dokonane zmiany

19. Ustawienia portalu muszą zostać przeładowane w tym celu zrestartuj usługę systemową obsługującą portal wpisując w konsoli

    systemctl restart liferay

20. Wywołaj inną przeglądarkę lub okno incognito i wywołaj serwer aplikacji wpisując adres: https://appkeycloak.websso.linuxpolska.pl

21. Z wyświetlonej listy aplikacji wybierz liferay
    Poczekaj cierpliwie na załadowanie się portalu – przeładowałeś usługę to chwilę może potrwać

22. Po wyświetleniu okna strony głównej skorzystaj z opcji **Sign In** (Prawy górny róg)

23. Powinieneś zostać przekierowany do strony logowania KeyCloak twojego zdefiniowanego Realmu
    użytkownik: **ssotest1** hasło: **TrudneHaslo123$**
    użytkownik: **ssotest2** hasło: **TrudneHaslo123$**

24. Jeśli uda ci się zalogować odniosłeś sukces.

25. Aby sprawdzić czy SSO działa w osobnej karcie przeglądarki otworzymy dodatkowo aplikację do zarządzania kontem użytkownika udostępnianą przez system KeyCloak. W tym celu w nowej karcie przeglądarki wpisz adres:
    https://keycloak.websso.linuxpolska.pl/auth/realms/websso/account

26. Jeśli się zalogowałaś automatycznie konfiguracja SSO prawidłowo działa