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 do system aplikację kliencką z Menu po lewej stronie wybierz: **Clients**
3. W otwartym oknie skorzystaj z przycisku **Create** (prawy róg ekranu)
4. 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.
7. Uzupełnimy adres serwisu w polu **Valid Redirect URIs**:
   https://**appkeycloak.websso.linuxpolska.pl**/liferay*
8. Zapisz zmiany wybierając przycisk Save
9. Konfiguracja logowania poprzez **OIDC** do portalu **liferay** dokonamy poprzez zmianę

   globalnych ustawień portalu w konsoli – wtyczka do autoryzacji nie posiada własnego gui konfiguracyjnego.
10. W celu konfiguracji przejdź do konsoli w której uruchomiłeś środowisko, upewnij się, że jesteś w katalogu ze sklonowanym repozytorium.
11. Połącz się z maszyną wirtualną wydając komendę:
    vagrant ssh appkeycloak.websso.linuxpolska.pl
12. Po połączeniu z maszyną przejmij uprawnienia roota wykonując komendę:
    su -
13. Wprowadź hasło roota: vagrant
14. 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
15. W pliku poddanym edycji odnajdź opcję dotyczące integracji portalu z openidc.

16. Zmień opcję: **openidconnect.enableOpenIDConnect** z false na true16. 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

20. systemctl restart liferay

21. 20. Wywołaj inną przeglądarkę lub okno incognito i wywołaj serwer aplikacji wpisując adres:

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

23. Z wyświetlonej listy aplikacji wybierz liferay

24. Poczekaj cierpliwie na załadowanie się portalu – przeładowałeś usługę to chwilę może potrwać

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

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

27. Jeśli uda ci się zalogować odniosłeś sukces.

28. Aby sprawdzić czy SSO działa w osobnej karcie przeglądarki otworzymy dodatkowo

29. 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

30. Jeśli się zalogowałaś automatycznie konfiguracja SSO prawidłowo działa

31. Po zakończeniu testu wyloguj się z aplikacji.

Zadanie 4

Konfiguracja aplikacji klienckiej na przykładzie Wordpress przy użyciu protokołu SAML.

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: wordpress-saml**
- **Client Protocol: saml**
- **Nie zmieniaj pozostałych opcji**

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

   Uzupełnimy adres serwisu w polu **Valid Redirect URIs:**
   https://appkeycloak.websso.linuxpolska.pl/wordpress*

7. Zapisz zmiany wybierając przycisk **Save**
8. Dodatkowo musimy określić mapowanie atrybutów naszego podmiotu logowania (czyli użytkownika), aby zarządzać mapowaniem atrybutów jakie przekazujemy do aplikacji musimy w oknie **Wordpress-saml** przejść do zakładani zatytułowanej **Mappers**
9. Rozpoczniemy od usunięcia bieżących wpisów tak aby nasza początkowa konfiguracja byłą jak najmniej skomplikowana (nie będziemy chcieli mapować ról) w tym celu wybieramy opcję **Delete** umieszczoną obok dostępnej na liście pozycji mapowania ról **role list.**
10. Kolejnym krokiem będzie dodanie mapowania atrybutów podmiotu logowania w tyn celu skorzystamy z opcji **Add Buildin** dodając automatycznie większość wbudowanych parametrów. Otworzy się okno wspomagające wybór parametrów.
11. Po zaznaczeniu opcji wybieramy **Add Selected**.
12. Pierwszym atrybutem jaki dodamy będzie nazwa użytkownika (będzie ona wymagana przez wtyczkę autoryzacji po stronie Wordpressa). W celu dodania mapowania nazwy użytkownika wybieramy przycisk **Create**
13. W oknie **Create Protocol Mapper** wypełniamy pola w następujący sposób:
    w polu **Name** wpisujemy username
    z list **Mapper** Type wybieramy **User Property**
    w polu **property** wpisujemy **username**
    w polu **Friendly Name** wpisujemy **username**
    w polu **SAML Atribute Name** wpisujemy **username**
    Na koniec wciskami przycisk **SAVE**

14. Drugim atrybutem jaki dodamy będzie email (będzie ona wymagana przez wtyczkę autoryzacji po stronie Wordpressa). W celu dodania mapowania nazwy użytkownika wybieramy przycisk **Create**

15. W oknie **Create Protocol Mapper** wypełniamy pola w następujący sposób:
    w polu **Name** wpisujemy email
    z list **Mapper** Type wybieramy **User Property**
    w polu **property** wpisujemy **email**
    w polu **Friendly Name** wpisujemy **email**
    w polu **SAML Atribute Name** wpisujemy **email**

16. Na koniec wciskami przycisk **Save**

17. Teraz przejdziemy do skonfigurowania protokołu SAML po stronie klienta w aplikacji Wordpress. Nie zamykaj okna konfiguracji Twojego realmu w aplikacji Keycloak, informacje takie jak klucze najprościej będzie przekopiować z jednego okna do drugiego.

18. W nowej karcie lub nowym oknie przeglądarki wywołaj serwer aplikacji wpisując adres: https://appkeycloak.websso.linuxpolska.pl

19. Z wyświetlonej listy aplikacji wybierz Wordpress

20. Po wyświetleniu okna logowania zaloguj się na konto administratora Wordpress podając dane:
    Username or Email Address: **admin**
    Password: **admin**

21. Po zalogowaniu rozpoczniemy od uaktywnienia wtyczki autoryzacyjnej w tym celu z menu po lewej stronie wybierz: **Plugins**

22. Po wyświetleniu listy wtyczek odnajdź wtyczkę **OneLogin SAML SSO** i wybierz odnośnik **Activate** umieszczony poniżej spowoduje to aktywację wtyczki autoryzacji poprzez protokół SAML.

23. Przejdziemy do konfiguracji wtyczki. Z menu po lewej stronie wybierz **Settings → SSO/SAML Settings**

24. W wyświetlonym oknie uzupełnij opcje konfiguracyjne zgodnie z poniższym wzorcem (opcji nie wymienionych poniżej nie zmieniaj – pamiętaj staramy się osiągnąć minimalną działającą konfigurację) :
    IdP Entity Id *: https://keycloak.websso.linuxpolska.pl/auth/realms/websso
    Single Sign On Service Url *:
    https://keycloak.websso.linuxpolska.pl/auth/realms/websso/protocol/saml
    (W razie wątpliwości skąd możemy pobrać te wartości są one dostępne w konfiguracji klienta SAML po stronie systemu KeyCloak. Informacje o poprawnych adresach znajdziesz wchodząc na zakładkę Installation i wybierając z listy **SAML Metadata IDPSSODescriptor –** wyświetlony tam dokument w formacie XML zawiera adresy endpointów protokołu SAML)

25. Najprostszą metodą uzupełnienia pola dotyczącego publicznego certyfiaktu idP, **X.509 Certificate** będzie jego skopiowanie z konfiguracji KeyCloak w tym celu powrócimy do zakładki/okna przeglądarki w której otwarta jest konfiguracja KeyCloak

26. W otwartym oknie KeyClaok upewnij się, że wybrałeś swój realm **websso** następnie z menu po lewej stronie wybierz **Realm Settings**

27. W otwartym oknie **Websso** przejdź do zakładki **Kyes**

28. W zakładce Keys Wybierz przycisk **Certificate** umieszczony obok wpisu zatytułowanego **RSA** wyświetli się okno z wartością certyfikatu.

29. Zaznacz całą wyświetloną wartość certyfikatu i skopiuj ją do schowka

30. Wróć do okna/karty przeglądarki z konfiguracją klienta SSO Wordpress.

31. Skopiowaną zawartość certyfikatu wklej w polu oznaczonym **X.509 Certificate –** upewnij się, że wklejasz właściwą wartość.

32. Z opcji wyświetlonych poniżej zaznacz
    Create user if not exists (utworzymy użytkownika jeśli nie istnieje w bazie użytkowników naszej instalacji Wordpressa)
    Update user data (pozwolimy na aktualizowanie danych użytkownika Wordpress ze źródła uwierzytelnienia)
    Force SAML login (w przypadku braku uwierzytelniania wymuszamy uwierzytelnienie źródle SAML)
    Upewnij się ,że w polu **Match Wordpress account** wybrano **Username**

33. W sekcji **ATTRIBUTE MAPPING** określimy mapowanie atrybutów podmiotu logowania zgodnie z ustawieniami jakie wprowadziliśmy w punktach **13 – 15**

34. Atrybut **Username *** określamy na **username**

35. Atrybut **Email *** określamy na **email**

36. Pozostałe atrybuty pozostawiamy na wstępnym etapie konfiguracji nie uzupełnione

37. Kolejną opcją jaką uzupełnimy jest opcja **Service Provider Entity Id** – jest to identyfikator naszego klienta SAML musi on być zgodny z wartością jaką wprowadziliśmy w punkcie **4** w związku z tym w polu obok opcji wpiszemy: **wordpress-saml**

38. Z pozostałych opcji uzupełnimy jeszcze opcje wymuszającą podpisywanie naszych żądań autoryzacyjnych – bez tego będą one odrzucane przez KeyCloaka w tym celu odnajdujemy opcję **Sign AuthnRequest** i zaznaczamy ją

39. Ostanie opcje jakie uzupełnimy to wartości kluczy podane w polach **Service Provider X.509 Certificate** oraz **Service Provider Private Key.** Wartości te skopiujemy z konfiguracji klienta wordpressa w KeyCloak. W tym celu wracamy do karty/okna przeglądarki w którym mamy otwartą konfiguracje keycloak.

40. W otwartym oknie KeyClaok upewnij się, że wybrałeś swój realm **websso** następnie z menu po lewej stronie wybierz **Clients**

41. W otwartym oknie **Clients** wchodzimy do zdefiniowanego przez klienta **wordpressa** o nazwie **wordpress-saml** wybierając jego nazwę umieszczoną w pierwszej kolumnie lub wybieraąc przycisk **Edit**
42. W otwartym oknie Wordpress-saml otwieramy zakładkę **SAML Keys.** Powinniśmy zobaczyć wygenerowane klucze służące do podpisywania żądań. Najpierw skopiujemy klucz certyfikatu.
43. W drugim polu zatytułowanym **Certificate** zaznacz całą zawartość i skopiuj ją do schowka.
44. Wróć do okna/karty przeglądarki z konfiguracją klienta SSO Wordpress.
45. Skopiowaną zawartość certyfikatu wklej w polu oznaczonym **Service Provider X.509 Certificate –** upewnij się, że wklejasz właściwą wartość.
46. Po wklejeniu zawartości klucza wracamy do okna z konfiguracją klienta wordpress w KeyCloak. Wracamy do miejsca konfiguracji certyfikatów.
47. W pierwszym polu zatytułowanym **Private Key** zaznacz całą zawartość i skopiuj ją do schowka.
48. Wróć do okna/karty przeglądarki z konfiguracją klienta SSO Wordpress.
49. Skopiowaną zawartość certyfikatu wklej w polu oznaczonym **Service Provider Private Key –** upewnij się, że wklejasz właściwą wartość.
50. Na koniec wybierz przycisk Save Changes
51. Nie wylogowuj się jeszcze z Wordpressa – na wypadek jakbyś popełnił drobny błąd będziesz mógł go poprawić!!!!
52. Otwórz inna przeglądarkę lub i ponownie połącz się ze stroną: https://appkeycloak.websso.linuxpolska.pl
53. Z wyświetlonej listy aplikacji wybierz **Wordpress**.
54. Powinieneś zostać przekierowany na stronę logowania systemu KeyCloak.
55. Zaloguj się wpisując dane:
    użytkownik: **ssotest1** hasło: **TrudneHaslo123$**
    użytkownik: **ssotest2** hasło: **TrudneHaslo123$**
56. W tym samym oknie przeglądarki, otwórz nową kartę przeglądarki i w nowej karcie wprowadź adres https://appkeycloak.websso.linuxpolska.pl
57. Z wyświetlonej listy aplikacji wybierz Liferay
58. Po wyświetleniu strony głównej **Liferay** wybierz opcję logowania **Sing In** (prawy górny róg ekranu) jeśli zostaniesz uwierzytelniony automatycznie oznacza to, że Single Sing On działa.