Linux Polska

www.LinuxPolska.pl

Open Source Day 2017
Warsztaty WEBSSO

Andrzej Kardaś
Solution Architect
Linux Polska Sp. z o.o.

LinuxPolska SP. Z O.O.

OPEN SOURCE COMPANY

Linux Polska liderem otwartych technologii na rynku polskim

WDROŻENIA

SZKOLENIA

EDB POSTGRES

docker

ZABBIX

redhat.

puppet

SUSE

Agenda

- Single Sign On?
- Dostępne rozwiązania Open Source
- System Apereo CAS (Jas-Sig CAS)
- System KeyCloak (RedHat SSO)
- Środowisko Warsztatowe
- Ćwiczenia praktyczne
  - Integracja przykładowych aplikacji z CAS
  - Integracja przykładowych aplikacji z KeyCloak

Czym więc charakteryzuje SSO?

- Uwierzytelniasz się raz uzyskujesz dostęp do wielu zasobów i systemów
- Zapewnienia centralizację domen zarządzania użytkownikami i uprawnieniami
- Możliwość przekazywania różnych danych z systemów autoryzacji per system kliencki lub domena bezpieczeństwa (grupująca wiele aplikacji i systemów)
- Możliwość centralnego dynamicznego zarządzania uprawnieniami nie tylko użytkowników ale i systemów w naszym środowisku

Zalety Stosowania SSO

- Ułatwiona administracja – monitorujemy jeden centralny system, możemy zarządzać spójną bazą użytkowników
- Większa wydajność pracy użytkowników – przełączanie się między systemami (ich składnikami) może być transparentne dla użytkowników
- Wzrost wydajności pracy środowiska realizującego funkcje biznesowe – obsługa autoryzacji SSO (bilety, tokeny, asercje) powinien być lżejsza niż bezpośredni dostęp do baz i systemów autoryzacyjnych
- Brak ograniczeń w zakresie dekompozycji, rozdrobnienia funkcjonalności wykorzystywanych systemów informatycznych – wzrost skalowalności środowiska

Wady Stosowania SSO

- Teoretycznie tworzy jeden centralny punkt ataku na różne systemy Informatyczne – przechwycenie jednego zestawu danych dostępowych zapewnia dostęp do wielu zasobów i systemów
- Problemy integracyjne w środowiskach cechujących się dużą heterogenicznością, wsparcie dla różnych standardów, protokołów i rozwiązań po stronie aplikacji klienckich
- Praktyczna nie możność pełnej integracji wielu „wiekowych” aplikacji – szczególnie tych opartych na zamkniętym kodzie źródłowym

Systemy SSO Open Source

- Shibboleth – rozwiązanie SAML licencja Apache 2.0
  https://shibboleth.net/
- JOSSO – protokół SOAP over HTTP licencja LGPL
  http://www.josso.org/
- OpenSSO – oryginalnie stworzony przez Sun
  http://opensso.sourceforge.net/
- OpenAM – fork projektu OpenSSO na licencji CDDL tworzony przy wsparciu ForgeRock:
  https://github.com/ForgeRock/openam-community-edition
- CASINO – SSO z obsługą protokołu CAS w języku Ruby
  http://casino.rbcas.com/
- Apereo CAS – rozwiązanie stworzone dla środowisk akademickich
  https://apereo.github.io/cas/5.0.x/index.html
- KeyCloak – projekt JBOSS Community centralna część rozwiązania RedHat SSO

  http://www.keycloak.org

System Apereo CAS

- Stworzony z myślą o środowiskach akademickich (wiele wydziałów, wiele kierunków, wiele systemów)
- Rozwiązanie szyte na miarę – wymaga kompilacji aplikacji docelowej ze wsparciem dla wybranych funkcjonalności – wynikiem jest aplikacja WAR w technologii Spring Framwork 4.x
- Wsparcie dla szerokiej gamy serwerów aplikacji i kontenerów servletów
- Implementuje własny otwarty standard protokół CAS wykorzystujący pewne elementy specyfikacji SAML do przekazywania danych aplikacjom klienckim
- Szeroki zakres bibliotek klienckich
- Opcjonalne wsparcie innych protokołów w tym:
  - OpenIDC
  - SAML 2.0
- Rozbudowany interfejs REST
- Dostępny Interfejs do monitorowania i administracji pracy systemu
- Osobna Aplikacja do zarządzania serwisami (aplikacjami klienckimi)

System Apereo CAS cd.

- Szeroki wachlarz kompatybilności z systemami uwierzytelniania w tym:
  - Bazy danych: JDBC, MongoDB
  - Usługi katalogowe LDAP w tym AD
  - Biblioteki autoryzacyjne JAAS, Apache Shiro
  - Możliwość forwardowania autoryzacji do systemów wspierających standardy OpenID/Oauth (Facebook, Google itp..)
  - Autoryzacja certyfikatami X 509
  - I wiele innych
- Posiada wsparcie dla wielu standardów wielokrotnej (podwójnej) autoryzacji w tym:
  - Duo Security
  - Authy
  - YubiKey
  - Radius
  - Google Authenticator

System Apereo CAS cd.

- Konfiguracja elementów systemów i wkompilowanych funkcjonalności odbywa się poprzez centralny plik konfiguracyjny lub zdalne repozytorium konfiguracyjne czy bazę danych
- Obsługuje regularnie odświeżane repozytorium konfiguracji serwisów (aplikacji klienckich)
  - W postaci plików (JSON lub YAML)
  - Bazy danych
  - Usługi katalogowej
- Dostarcza dodatkowe mechanizmy bezpieczeństwa ograniczające ilość nieudanych prób logowania – wymaga dodania źródła danych
- Dostarcza podstawowe wsparcie dla obsługi mechanizmów zmiany i resetowania haseł użytkownika w oparciu o usługi pocztowe (funkcja dostępna od wersji 5.0 – status eksperymentalny)
- Prezentuje jedną domenę bezpieczeństwa z bardzo szeroką możliwością dostosowywania konfiguracji dla poszczególnego serwisu (aplikacji klienckiej)

System Apereo CAS konfiguracja serwisów

- Opcje dotyczące konfiguracji poszczególnych serwisów (aplikacji klienckich) dotyczą min:
  - Protokołów (CAS, SAML, OpenIDC)
  - Metod obsługi standardu Single Sing Out (Front czy Back Channel, Brak)
  - Obsługi poszczególnych źródeł autoryzacji z możliwością łączenia ich w łańcuchy
  - Uwalnianych i przekazywanych do serwisu ze źródła uwierzytelniania atrybutów
  - Ograniczeń autoryzacji ze względu na wartości atrybutów pobranych dla danego podmiotu autoryzacji ze źródła uwierzytelnienia
  - Obsługiwanych standardów wielokrotnego uwierzytelniania
  - Wyglądu okien logowania

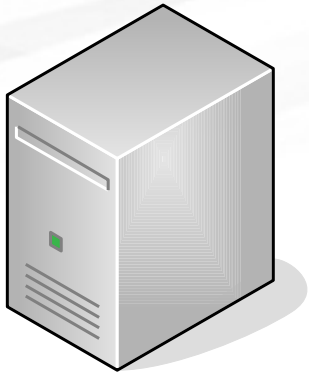
Środowisko Warsztatowe CAS

Serwer usługi katalogowej
LDAP 389DS

- Użytkownik: admin
- Hasło: admin
- Użytkownik: ssotest1
- Hasło: TrudneHaslo123$
- Użytkowik: ssotest2
- Hasło: TrudneHaslo123$

389ds.websso.linuxpolska.pl
ldap.websso.linuxpolska.pl

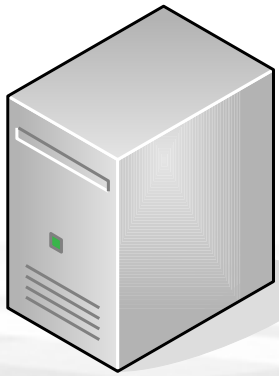
Serwer CAS



Kompilacja wspiera:
- Autoryzację LDAP
- Protokół CAS 3
- Interfejs LDAP
- Podstawowe monitorowanie
- Rejestr serwisów JSON
- aplikację WWW do zarządzania serwisami

cas.websso.linuxpolska.pl
- Aplikacja CAS:
  /auth
- Status:
  /auth/status
- Dashboard CAS
/auth/status/dashboard
- Konfiguracja Serwisów:
  /cas-management

Serwer aplikacji klienckich



appcas.websso.linuxpolska.pl
- Aplikacja Wordpress z wtyczką Cassify:
  /wordpress
- Aplikacja LifeRay:
- /liferay

Ćwiczenia CAS

- Jeśli nie zbudowałeś środowiska przed warsztatami wysłuchaj prowadzącego abyś mógł powtórzyć ćwiczenia samodzielnie (budowa środowiska od zera w warunkach warsztatów nie ma szansy się powieść ze względu na brak czasu)
- Zwróć uwagę na konieczność akceptacji certyfikatów bezpieczeństwa są one nieautoryzowane (Self Signed) – możesz zaimportować wygenerowane certyfikaty (pliki *.crt z katalogu tmp) do przeglądarki aby uniknąć odpowiadania na pytania o akceptację certyfikatów
- Prosimy o stosowanie się do nazewnictwa umieszczonego w instrukcji w innym wypadku prowadzący nie będzie mógł Ci pomóc w rozwiązaniu problemów
- Nie wylogowuj się z aplikacji, którą konfigurujesz z konta administratora dopóki nie sprawdzisz poprawności działania Twojej konfiguracji w innej przeglądarce lub na karcie w trybie incognito – inaczej w przypadku błędu lub literówki nie będziesz mógł się ponownie zalogować do systemu

System KeyCloak

- Stworzony jako projekt JBOSS Comunity – jeden z najaktywniejszych projektów tej społeczności
- Stanowi centralny punkt rozwiązania RedHat SSO (wsparcie, dokumentacja)
- Jest gotową aplikacją WAR ze wsparciem dla instalacji na serwerach aplikacji WildFly, JBOSS
- Wspiera dwa najbardziej uznane standardy w zakresie obsługi SSO:
  - OpenIDC
  - SAML 2.0
- Rozbudowany interfejs REST
- Szeroki zakres bibliotek klienckich
- Zintegrowane rozwiązanie, zarządzanie odbywa się poprzez intuicyjny interfejs WWW
- Udostępnia wbudowaną aplikację do zarządzania kontami użytkownika, ze wsparciem dla funkcji, resetowania haseł, edycji profilu – konfiguracji ustawień wielokrotnego uwierzytelniania w oparciu o Google Authenticator

System KeyCloak cd.

- Zapewnia funkcje federowania bazy użytkowników:
  - z usługi katalogowej LDAP w tym AD
  - źródła Kerberos
  - z możliwością kopiowania kont i ustawienia polityki synchronizacji danych pomiędzy KeyCloak a serwerem autoryzacji
  - pozwala na podpięcie wielu źródeł danych (LDAP, Kerberos) z określeniem priorytetów każdego z nich
- Pozwala na przekazywanie żądań uwierzytelnienia do systemów trzecich obsługujących protokoły SAML, OpenIDC z dodatkowo dostępnymi szablonami ułatwiającymi konfigurację dla popularnych usług społecznościowych min:
  - Facebook
  - Github
  - Twiiter
  - LinkedIn

System KeyCloak cd.

- Posiada wbudowane usługi podwyższające bezpieczeństwo pracy, np.: wykrywanie prób ataków BruteForce, które administrator może uaktywnić
- Posiada rozbudowane mechanizmy logowania zdarzeń – wraz z interfejsem do ich przeglądania, wyszukiwania
- Posiada intuicyjny interfejs zarządzanie otwartymi sesjami SSO
- Rozbudowane funkcje eksportu i importu danych wraz z możliwościami zdefiniowania własnych szablonów konfiguracyjnych (np. dla typowych konfiguracji aplikacji klienckich)
- Rozbudowany i w pełni konfigurowalny system uprawnień i ról jakie może przydzielać podmiotom logowania
- Prezentuje model wielu domen bezpieczeństwa (tzw. Realmów)

System KeyCloak Realmy i aplikacje klienckie

- Poszczególne relamy definiują:
  - mechanizmy federacji kont użytkowników
  - opcje bezpieczeństwa
  - funkcje udostępniane użytkownikom (rejestracja, przypomnienie hasła itp.)
  - ustawienia mechanizmów dodatkowej autoryzacji
  - ustawienia dotyczące wielokrotnego uwierzytelnienia (MFA)
  - ustawienia dotyczące wyglądu udostępniancych przez KeyKloak aplikacji i stron logowania
  - definicji poszczególnych aplikacji klienckie
- Definicje aplikacji klienckich obejmują:
  - Definicję protokołu (OpenIDC lub SAML 2.0)
  - Ustawienia dotyczące szczegółów pracy protokołu np. obsługi funkcji Single Sing Out
  - Mapowanie atrybutów podmiotu logowania przekazywanych aplikacji
  - Role i uprawnienia danego klienta

Środowisko Warsztatowe KeyCloak

Serwer KeyCloak

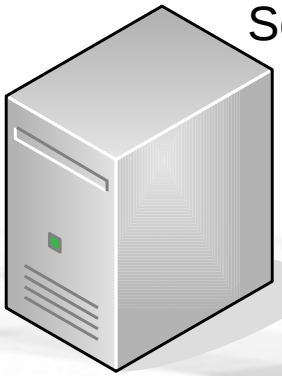
keycloak.websso.linuxpolska.pl
•Realm master:
/auth/realms/master

Serwer usługi katalogowej
LDAP 389DS

•Użytkownik: admin
•Hasło: admin
•Użytkownik: ssotest1
•Hasło: TrudneHaslo123$
•Użytkowik: ssotest2
•Hasło: TrudneHaslo123$

389ds.websso.linuxpolska.pl
ldap.websso.linuxpolska.pl

Serwer aplikacji klienckich



appkeycloak.websso.linuxpolska.pl
•Aplikacja Wordpress z wtyczką OneLogin SAML SSO:
/wordpress
•Aplikacja LifeRay z wtyczką OpenIDC:
•/liferay

Ćwiczenia Keycloak

- Jeśli nie zbudowałeś środowiska przed warsztatami wysłuchaj prowadzącego abyś mógł powtórzyć ćwiczenia samodzielnie (budowa środowiska od zera w warunkach warsztatów zajmie zbyt dużo czasu)
- Zwróć uwagę na konieczność akceptacji certyfikatów bezpieczeństwa są one nieautoryzowane (Self Signed) – możesz zaimportować wygenerowane certyfikaty (pliki *.crt z katalogu tmp) do przeglądarki aby uniknąć odpowiadania na pytania o akceptację certyfikatów
- Prosimy o stosowanie się do nazewnictwa umieszczonego w instrukcji w innym wypadku prowadzący nie będzie mógł Ci pomóc w rozwiązaniu problemów
- Nie wylogowuj się z aplikacji, którą konfigurujesz z konta administratora dopóki nie sprawdzisz poprawności działania Twojej konfiguracji w innej przeglądarce lub na karcie w trybie incognito – inaczej w przypadku błędu lub literówki nie będziesz mógł się ponownie zalogować do systemu.

Dziękujemy za uwagę

Andrzej Kardaś
Solution Architect
Linux Polska Sp. z o.o.