

O que é Single Sign On

O logon único (SSO) é um método de autenticação que permite que os usuários se autentiquem com segurança em vários aplicativos e sites usando apenas um conjunto de credenciais.

Como funciona o SSO?

O SSO funciona com base em uma relação de confiança estabelecida entre um sistema, conhecido como provedor de serviços, e um provedor de identidade. Essa relação de confiança geralmente é baseada em um certificado que é trocado entre o provedor de identidade e o provedor de serviços. Este certificado pode ser usado para assinar informações de identidade que estão sendo enviadas do provedor de identidade para o provedor de serviços para que o provedor de serviços saiba que estão vindo de uma fonte confiável. No SSO, esses dados de identidade assumem a forma de tokens que contêm bits de identificação de informações sobre o usuário, como o endereço de e-mail ou nome de usuário de um usuário etc.

O que é OAuth 2.0?

OAuth 2.0 é um protocolo de autorização e não um protocolo de autenticação. Como tal, ele é projetado principalmente como um meio de conceder acesso a um conjunto de recursos, por exemplo, APIs remotas ou dados do usuário. OAuth 2.0 usa tokens de acesso. Um token de acesso é um dado que representa a autorização para acessar recursos em nome do usuário final. OAuth 2.0 não define um formato específico para tokens de acesso. No entanto, em alguns contextos, o formato JSON Web Token (JWT) é frequentemente usado. Isso permite que os emissores de token incluam dados no próprio token. Além disso, por motivos de segurança, os tokens de acesso podem ter uma data de expiração.

O que é OpenID Connect (OIDC)?

OIDC é um protocolo para verificar as identidades do usuário e obter informações do perfil do usuário. O OpenID Connect é baseado no OAuth 2.0, que especifica uma API RESTful HTTP e usa JSON como formato de dados. Ele possui um conjunto especializado de tipos de dados predefinidos e terminais para a troca de informações do usuário entre o provedor de identidade e o aplicativo, desta forma, permite que os dispositivos verifiquem identidades com base na autenticação feita por um servidor de autenticação. O OpenID Connect é executado pela OpenID Foundation. O OAuth, no qual é construído, também é um padrão aberto, mantido pelo Grupo de Trabalho OAuth da Força-Tarefa de Engenharia da Internet.

O que é um token SSO?

Um token SSO é uma coleção de dados ou informações que são passados ​​de um sistema para outro durante o processo de SSO. Os dados podem ser matrícula do usuário, endereço de e-mail e informações sobre qual sistema está enviando o token. Os tokens devem ser assinados digitalmente para que o receptor do token verifique se o token está vindo de uma fonte confiável. O certificado usado para esta assinatura digital é trocado durante o processo de configuração inicial.

O que é Keycloak

Keycloak é um programa de código aberto que permite configurar um provedor de logon único seguro - SSO. Ele oferece suporte a vários protocolos, como SAML 2.0 e OpenID Connect. Ele também pode armazenar credenciais de usuário localmente ou por meio de um back-end LDAP ou Kerberos. Esses recursos permitem que o Keycloak seja altamente configurável, mas também bastante fácil de instalar e configurar.

Benefícios do SSO

1.A localização central para autenticação permite auditoria e segurança mais fáceis.

2.Local central para configuração de autorização.

3.A autenticação para serviços externos, como um pacote de CRM hospedado, é possível sem o envio de solicitações LDAP pela Internet.

4.Os tokens são agrupados em SSL / TLS como parte da conexão HTTPS, mas também podem ser assinados e/ou criptografados usando chaves conhecidas apenas entre o provedor de identidade e o serviço para maior segurança.

Fluxo de Autenticação

- Perspectiva do Usuário

Diagrama

Descrição gerada automaticamente

1. O usuário acessa o endereço da Web de uma aplicação protegido por SSO (conhecido como provedor de serviços).
2. O serviço direciona o usuário para o provedor de identidade (Keycloaker) configurado através de uma página de login que será apresentada no browser.
3. O usuário efetua login com as credenciais fornecidas. O Provedor de identidade compara a credenciais armazenadas no seu sistema ou a um back-end LDAP ou Kerberos.
4. Caso o login no provedor de identidade tenha sucesso, o browser do usuário recepciona a aplicação para ser utilizada.

- Perspectiva aplicação Java/Quarkus - Microserviço

Uma imagem contendo Diagrama

Descrição gerada automaticamente

1. O usuário acessa o endereço Web de uma aplicação protegido por SSO. A Aplicação FrontEnd redireciona para página de login do servidor de autorização para usuário inserir suas credenciais.
2. Aplicação FrontEnd recebe refresh token após usuário logado.
3. Aplicação FrontEnd envia endpoint do serviço com refresh token para Aplicação BackEnd
4. Aplicação BackEnd consulta servidor de Autorização se o token refresh é valido, caso sim, servidor de autorização disponibiliza Access token com informações do usuário e seu permissionamento.
5. Aplicação BackEnd disponibiliza em formato json os dados e regra de negócio disponibilizados através do serviço REST requisitado.
6. Usuário recepciona a informação tratada de forma amigável pela Aplicação FrontEnd.

O que precisa para configurar em aplicações JAVA/Quarkus

Criação de cli-web conforme ....

Configuração de amnienmte xxxxxx