Le modèle M.V.C. de Spring 2/2

1 Utiliser des données en session

Il existe trois solutions pour travailler facilement avec des données stockées en session.

1.1 Gérer facilement les données en session

Voila un exemple de contrôleur qui travaille sur un compteur stocké en session et récupéré via les paramètres des méthodes :

```
package mybootapp.web;

import javax.servlet.http.HttpSession;

import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.ResponseBody;
import org.springframework.web.bind.annotation.SessionAttribute;

@Controller
@RequestMapping("/counter")
public class CounterController {

    class CounterBean {
        int value = 0;
    }

    @RequestMapping(value = "/init")
    @ResponseBody
    public String init(HttpSession session) {
        var counter = new CounterBean();
        session.setAttribute("counter", counter);
        return String.format("int␣counter␣=␣%d\n", counter.value);
    }

    @RequestMapping(value = "/show")
    @ResponseBody
    public String show(@SessionAttribute(required = false) CounterBean counter) {
        if (counter == null) {
            return ("counter␣is␣null\n");
        }
        return String.format("counter␣=␣%d\n", counter.value);
    }

    @RequestMapping(value = "/inc")
    @ResponseBody
    public String incCounter(@SessionAttribute CounterBean counter) {
        counter.value++;
        return (show(counter));
    }

}
```

1.2 Utiliser la portée dans Spring

Il est facile de récupérer des données placées en session, mais Spring nous offre le moyen d'injecter directement dans nos contrôleurs des données de portée session.

Étape 1 : définissez un nouveau bean pour représenter l'utilisateur courant :

```
package mybootapp.web;

import org.springframework.stereotype.Component;
import org.springframework.web.context.annotation.SessionScope;

import lombok.Data;

@Component
@SessionScope
@Data
public class User {

    private String name;

}
```

L'annotation `Component` indique que c'est un composant géré par Spring. L'annotation `SessionScope` donne la portée des instances (une par session). Les portées `RequestScope` et `ApplicationScope` sont également disponibles. Ce n'est pas directement une instance qui va être injectée, mais un proxy qui va sélectionner la bonne instance (dans la bonne session) en fonction du contexte.

Étape 2 : définissez un contrôleur qui utilise l'injection du bean `User` :

```java
package mybootapp.web;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.ModelAttribute;
import org.springframework.web.bind.annotation.RequestMapping;

@Controller()
@RequestMapping("/user")
public class UserController {

    protected final Log logger = LogFactory.getLog(getClass());

    @Autowired()
    User user;

    @ModelAttribute("user")
    public User newUser() {
        return user;
    }

    @RequestMapping(value = "/show")
    public String show() {
        logger.info("show␣user␣" + user);
        return "user";
    }

    @RequestMapping(value = "/login")
    public String login() {
        logger.info("login␣user␣" + user);
        user.setName("It's␣me");
        return "user";
    }

    @RequestMapping(value = "/logout")
    public String logout() {
        logger.info("logout␣user␣" + user);
        user.setName("Anonymous");
        return "user";
    }
}
```

Étape 3 : La vue :

```
<%@ include file="/WEB-INF/jsp/header.jsp"%>

<c:url var="login" value="/user/login" />
<c:url var="logout" value="/user/logout" />
<c:url var="show" value="/user/show" />

<div class="container">
    <h1>User</h1>

    <p>
    name : <c:out value="${user.name}" default="no name"/> |
    <a href="${show}">Show</a> | <a href="${login}">Login</a> |
    <a href="${logout}">Logout</a>
    </p>
</div>

<%@ include file="/WEB-INF/jsp/footer.jsp"%>
```

Moralité : Le contrôleur (qui est un singleton exécuté par plusieurs `threads`) utilise le `proxy` pour sélectionner **automatiquement** l'instance du bean `User` qui correspond à la requête courante et à la session courante.

La liaison se fait par le `thread`. C'est le même `thread` qui traite toute la requête (`Dispatcher`, contrôleur, vue). Le `thread` courant est donc utilisé comme une sorte de variable globale qui permet de faire des liaisons implicites.

1.3 Placer des données en session

Une deuxième solution consiste à indiquer, dans le contrôleur, les instances du modèle que Spring devra placer dans la session. Reprenons le même exemple mais avec un utilisateur simple (pas annoté) :

```
package mybootapp.web;

import lombok.Data;

@Data
public class SimpleUser {

    private String name;

}
```

Nous pouvons maintenant définir un nouveau contrôleur :

```java
package mybootapp.web;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.ModelAttribute;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.SessionAttributes;
import org.springframework.web.servlet.mvc.support.RedirectAttributes;

@Controller()
@RequestMapping("/simple-user")
@SessionAttributes("simpleUser")
public class SimpleUserController {

    protected final Log logger = LogFactory.getLog(getClass());

    @ModelAttribute("simpleUser")
    public SimpleUser newUser() {
        var user = new SimpleUser();
        logger.info("new␣user␣" + user);
        return user;
    }

    @RequestMapping(value = "/show")
    public String show(@ModelAttribute("simpleUser") SimpleUser user) {
        logger.info("show␣user␣" + user);
        return "simple-user";
    }

    @RequestMapping(value = "/login")
    public String login(//
            @ModelAttribute("simpleUser") SimpleUser user, //
            RedirectAttributes attributes) {
        logger.info("login␣user␣" + user);
        user.setName("It's␣me");
        attributes.addFlashAttribute("message", "Bienvenue␣!");
        return "redirect:show";
    }

    @RequestMapping(value = "/logout")
    public String logout(//
            @ModelAttribute("simpleUser") SimpleUser user, //
            RedirectAttributes attributes) {
        logger.info("logout␣user␣" + user);
        user.setName("Anonymous");
        attributes.addFlashAttribute("message", "Au␣revoir.");
        return "redirect:show";
    }
}
```

Commentaire 1 : L'annotation `@SessionAttributes` permet d'indiquer quelles sont les instances du modèle qui doivent être placées en session. L'instance en question (`simpleUser`) est produite par la méthode `newUser` . Les méthodes traitants les requêtes peuvent récupérer cette instance pour la modifier.

Commentaire 2 : Je profite de cet exemple pour introduire les données flash qui sont destinées à être utilisées dans la requête suivante. C'est précisément le cas car, contrairement à la première version, les actions de `/login` et `/logout` renvoient une redirection vers `/show` .

Il ne reste plus qu'à définir la vue :

Fichier WEB-INF/jsp/simple-user.jsp

```
<%@ include file="/WEB-INF/jsp/header.jsp"%>

<c:url var="login" value="/simple-user/login" />
<c:url var="logout" value="/simple-user/logout" />
<c:url var="show" value="/simple-user/show" />

<div class="container">
    <h1>Simple User</h1>

    <c:if test="${message != null}">
        <div class="alert alert-success" role="alert">
            <c:out value="${message}" />
        </div>
    </c:if>

    <p>
        name :
        <c:out value="${simpleUser.name}" default="no name" />
        | <a href="${show}">Show</a> | <a href="${login}">Login</a> |
        <a href="${logout}">Logout</a>
    </p>
</div>

<%@ include file="/WEB-INF/jsp/footer.jsp"%>
```

Travail à faire : testez le bon fonctionnement de cet exemple.

2 Tester vos contrôleurs

Voila un exemple simple de test unitaire basé `MockMvc` qui permet de vérifier le bon fonctionnement des contrôleurs :

- Créez dans le répertoire `test` le package `mybootapp.web`.
- Créez la classe de test unitaire ci-dessous :

```java
package mybootapp.web;

import static org.springframework.test.web.servlet.request.MockMvcRequestBuilders.get;
import static org.springframework.test.web.servlet.result.MockMvcResultHandlers.print;
import static org.springframework.test.web.servlet.result.MockMvcResultMatchers.model;
import static org.springframework.test.web.servlet.result.MockMvcResultMatchers.status;
import static org.springframework.test.web.servlet.result.MockMvcResultMatchers.view;
import static org.springframework.test.web.servlet.result.MockMvcResultMatchers.content;

import org.junit.jupiter.api.Test;
import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.boot.test.autoconfigure.web.servlet.AutoConfigureMockMvc;
import org.springframework.boot.test.context.SpringBootTest;
import org.springframework.test.context.ContextConfiguration;
import org.springframework.test.web.servlet.MockMvc;

import mybootapp.web.Starter;

@SpringBootTest
@ContextConfiguration(classes = Starter.class)
@AutoConfigureMockMvc
public class TestWebApp {

    @Autowired
    private MockMvc mvc;

    @Test
    public void testCourseList() throws Exception {
        mvc.perform(get("/course/list"))//
                // afficher
                .andDo(print())//
                // vérifier le statut
                .andExpect(status().isOk())//
                // vérifier le nom de la vue
                .andExpect(view().name("course"))//
                // vérifier le modèle
                .andExpect(model().attributeExists("courses"));
    }

}
```

Travail à faire : Tester quelques possibilités des instances renvoyées par les méthodes statiques `status()`, `view()` et `model()`.

3 Utiliser des intercepteurs

Vous pouvez très facilement installer des classes d'interception afin d'ajouter des opérations avant et après le traitement des requêtes. Définissez la classe suivante (elle vérifie l'adresse du client) :

```java
package mybootapp.web;

import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.springframework.web.servlet.HandlerInterceptor;
import org.springframework.web.servlet.ModelAndView;

public class LoggerInterceptor implements HandlerInterceptor {

    private static Log log = LogFactory.getLog(LoggerInterceptor.class);

    @Override
    public boolean preHandle(HttpServletRequest request, //
            HttpServletResponse response, Object handler) throws Exception {
        var client = request.getRemoteAddr();
        log.info("Inside␣pre␣handle␣from␣" + client);
        switch (client) {
        case "127.0.0.1":
        case "0:0:0:0:0:0:0:1":
            return true;
        }
        response.getWriter().printf("Only␣127.0.0.1");
        return false;
    }

    @Override
    public void postHandle(HttpServletRequest request, //
            HttpServletResponse response, //
            Object handler, //
            ModelAndView modelAndView) throws Exception {
        log.info("Inside␣post␣handle");
    }

    @Override
    public void afterCompletion(HttpServletRequest request, //
            HttpServletResponse response, Object handler, //
            Exception exception) throws Exception {
        log.info("Inside␣after␣completion");
    }
}
```

Pour installer cet intercepteur (il peut y avoir plusieurs), ajoutez la méthode ci-dessous à votre classe `Starter` :

```java
@Override
public void addInterceptors(InterceptorRegistry registry) {
    registry.addInterceptor(new LoggerInterceptor());
}
```

Travail à faire : Vérifiez que l'application n'est plus accessible à partir de l'adresse publique.

4 Gestion des erreurs

La récupération des erreurs est simplement réalisée par l'ajout d'un contrôleur spécifique dans lequel nous sommes capable de traiter plusieurs causes d'exception :

```java
package mybootapp.web;

import org.springframework.boot.web.servlet.error.ErrorController;
import org.springframework.web.bind.annotation.ControllerAdvice;
import org.springframework.web.bind.annotation.ExceptionHandler;
import org.springframework.web.bind.annotation.ResponseBody;

@ControllerAdvice
public class ErrorControler implements ErrorController {

    @ResponseBody
    @ExceptionHandler({NullPointerException.class})
    public String handleNullPointerException(Exception e) {
        System.err.println("--␣NullPointerException:");
        e.printStackTrace(System.err);
        return "Null␣Pointer␣Error";
    }

    @ResponseBody
    @ExceptionHandler
    public String handleOtherException(Exception e) {
        System.err.println("--␣Other␣Exception:");
        e.printStackTrace(System.err);
        return "Other␣Error";
    }

}
```

Je ne rentre pas dans plus de détails, vous trouverez plus de détails sur cette page [1].

5 Très légère introduction aux API RESTfull

L'idée est simple :

- Proposer une API WEB pour récupérer et agir sur les données d'un serveur.
- Utiliser les méthodes HTTP (`GET`, `POST`, `DELETE`, etc) pour coder les actions sur les données.
- Utiliser des langages normalisés pour la description des données (XML et surtout Json).
- Offrir ainsi un service complet accessible aux clients (des applications WEB, des téléphones portables, des dispositifs nomades, etc.)

5.1 Mise en place d'un controleur REST

Commencez par ajouter les dépendances pour Jackson (outils pour transformer une instance Java en Json et vice-versa) :

```xml
...
<dependency>
    <groupId>com.fasterxml.jackson.core</groupId>
    <artifactId>jackson-databind</artifactId>
    <!-- <version>2.9.8</version> NOUVEAU -->
</dependency>
...
```

Créez ensuite une contrôleur REST (une calculatrice à pile) :

1. https://www.baeldung.com/spring-boot-custom-error-page

```java
package mybootapp.web;

import java.util.Stack;

import javax.annotation.PostConstruct;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.springframework.http.HttpStatus;
import org.springframework.web.bind.annotation.GetMapping;
import org.springframework.web.bind.annotation.PostMapping;
import org.springframework.web.bind.annotation.RequestBody;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.ResponseStatus;
import org.springframework.web.bind.annotation.RestController;

@RestController
@RequestMapping("/calculator")
public class RestCalculator {

    protected final Log logger = LogFactory.getLog(getClass());
    private Stack<Integer> numbers = new Stack<>();

    @PostConstruct
    public void init() {
        numbers.push(100);
        numbers.push(200);
        numbers.push(300);
    }

    @GetMapping("/show")
    public Stack<Integer> show() {
        return numbers;
    }

    @GetMapping("/add")
    @ResponseStatus(HttpStatus.OK)
    public void add() {
        Integer val1 = numbers.pop();
        Integer val2 = numbers.pop();
        numbers.push(val1 + val2);
    }

    @PostMapping(value = "/put", consumes = "application/json")
    @ResponseStatus(HttpStatus.CREATED)
    public String put(@RequestBody() Integer id) {
        numbers.push(id);
        logger.info(String.format("put␣%d", id));
        return "Ok";
    }

}
```

Testez l'API Rest avec des requêtes directes :

```
http://localhost:8081/calculator/show
http://localhost:8081/calculator/add
http://localhost:8081/calculator/show
```

La première donne les trois éléments de la pile. La second remplace les deux éléments de la tête de pile par leur addition. etc.

Vous pouvez ensuite déposer des données dans la pile en lancant une requete `POST` à l'aide de l'outil en ligne de commande `curl` :

Commandes à taper dans un shell

```
URL="http://localhost:8081/calculator/put"
curl -X POST -H "Content-Type: application/json" --data '222' $URL
curl -X POST -H "Content-Type: application/json" --data '333' $URL
curl http://localhost:8081/calculator/show
```

5.2 Une petite application REST

Nous allons maintenant créer un code javaScript coté client qui va interagir avec cette API REST. Commencez par le fichier javaScript suivant :

Fichier src/main/webapp/functions.js

```
function showStack() {
    var base = ($('<a␣href=".">')[0].href);
    $.ajax({
        type : 'GET',
        url : (base + "calculator/show"),
        data : '200',
        timeout : 3000,
        success : function(data) {
            $('#numbers').hide();
            $('#numbers').html("Stack:␣");
            jQuery.each(data, function(i, val) {
                $("#numbers").append("␣-␣");
                $("#numbers").append(document.createTextNode(val));
            });
            $('#numbers').show();
        }
    });
}

function show() {
    showStack();
    $('#message').html("");
}

function add() {
    var base = ($('<a␣href=".">')[0].href);
    $.ajax({
        type : 'GET',
        url : (base + "calculator/add"),
        timeout : 3000,
        error : function() {
            $('#message').html('Addition␣impossible');
            showStack();
        },
        success : function(data) {
            $('#message').html('Addition␣réalisée');
            showStack();
        }
    });
}

function put() {
    var base = ($('<a␣href=".">')[0].href);
    var value = ($('#input').val());
    $.ajax({
        type : 'POST',
        url : (base + "calculator/put"),
        data : value,
        timeout : 3000,
        dataType : "json",
        contentType : "application/json",
        success : function(data) {
            showStack();
            $('#input').html("");
        },
        error : function() {
            showStack();
            $('#input').html("");
        }
    });
}
```

Ces fonctions JavaScript vont utiliser la méthode `ajax` de `JQuery` pour envoyer des requêtes asynchrones vers l'API REST.

Nous pouvons maintenant préparer une page JSP qui va produire une page HTML à destination d'un navigateur. La page chargée va utiliser `JQuery` et proposer une interface minimale pour lister les éléments de la pile, ajouter un nombre et calculer une addition.

Fichier `src/main/webapp/rest-app.jsp`

```
<%@ include file="/WEB-INF/jsp/header.jsp"%>

<c:url var="function" value="/functions.js" />

<div class="container">
    <script src="${function}"></script>
    <h1>Simple stack calculator (rest application)</h1>
    <p>
        <button onclick="show();">Show</button>
        <input id="input" size="10" />
        <button onclick="put();">put</button>
        <span> | </span>
        <button onclick="add();">+</button>
        <span> </span> <span style="color: blue;" id="message"></span>
    </p>
    <p id="numbers"></p>
</div>

<%@ include file="/WEB-INF/jsp/footer.jsp"%>
```

Travail à faire : prévoir l'opération de soustraction (fonction JavaScript, bouton html et requête `/calculator/sub` sur l'API REST.

6 Introduction à Spring security

6.1 Mise en place

Nous pouvons maintenant ajouter Spring Security [2] : une couche des gestion de la sécurité. Pour ce faire, suivez les étapes ci-dessous :

- Ajoutez au fichier `pom.xml` les dépendances de Spring Security.

```
<dependency>
    <groupId>org.springframework.boot</groupId>
    <artifactId>spring-boot-starter-security</artifactId>
</dependency>
<dependency>
    <groupId>org.springframework.security</groupId>
    <artifactId>spring-security-test</artifactId>
    <scope>test</scope>
</dependency>
<dependency>
    <groupId>org.springframework.security</groupId>
    <artifactId>spring-security-taglibs</artifactId>
</dependency>
```

- Créez le package `mybootapp.web.security`.
- Ajoutez ensuite une classe de configuration :

2. https://spring.io/guides/topicals/spring-security-architecture

```java
package mybootapp.web.security;

import org.springframework.context.annotation.Bean;
import org.springframework.security.config.annotation.authentication.builders.
    AuthenticationManagerBuilder;
import org.springframework.security.config.annotation.method.configuration.
    EnableGlobalMethodSecurity;
import org.springframework.security.config.annotation.web.builders.HttpSecurity;
import org.springframework.security.config.annotation.web.configuration.EnableWebSecurity;
import org.springframework.security.config.annotation.web.configuration.
    WebSecurityConfigurerAdapter;
import org.springframework.security.crypto.bcrypt.BCryptPasswordEncoder;
import org.springframework.security.crypto.password.PasswordEncoder;
import org.springframework.stereotype.Component;

@Component
@EnableWebSecurity
@EnableGlobalMethodSecurity(prePostEnabled = true, securedEnabled = true, jsr250Enabled = true)
public class SpringSecurity extends WebSecurityConfigurerAdapter {

    @Override
    protected void configure(HttpSecurity http) throws Exception {
        http
                // -- ne pas activer la protection CSRF
                .csrf().disable()
                // -- URL sans authentification
                .authorizeRequests()//
                .antMatchers("/", "/webjars/**", //
                        "/home", "/login", //
                        "/calculator/**")//
                .permitAll()//
                // -- Les autres URL nécessitent une authentification
                .anyRequest().authenticated()
                // -- Nous autorisons un formulaire de login
                .and().formLogin().permitAll()
                // -- Nous autorisons un formulaire de logout
                .and().logout().permitAll();
    }

    /* Définir la base de l'authentification. */
    @Override
    protected void configure(final AuthenticationManagerBuilder auth) throws Exception {
        var encoder = passwordEncoder();
        auth.inMemoryAuthentication()//
                .withUser("user1").password(encoder.encode("user1")).authorities("USER")//
                .and()//
                .withUser("user2").password(encoder.encode("user2")).authorities("USER")//
                .and()//
                .withUser("admin").password(encoder.encode("admin")).authorities("ADMIN");
    }

    @Bean
    public PasswordEncoder passwordEncoder() {
        return new BCryptPasswordEncoder();
    }
}
```

- **Commentaire** : Cette classe va définir les règles de sécurité et la base de l'authentification. Nous nous contenterons de définir, en mémoire, la liste des utilisateurs.

Travail à faire :

- Redémarrez votre application et vérifiez que les règles sont bien respectées. Réalisez plusieurs phases de

login/logout.

- Limitez l'accès à `/simple-user` aux administrateurs :

```
.antMatchers("/simple-user/**")//
.hasAnyAuthority("ADMIN") /// ****** NOUVEAU
```

- Vous pouvez écrire un test unitaire pour valider cette limitation et utiliser l'annotation ci-dessous (sur la méthode de test) pour vous mettre dans le bon contexte :

```
@WithMockUser(username = "user1",  authorities = { "ADMIN" })
```

6.2 Les tag de Spring Security

- Utilisez cette documentation [3] pour faire varier le contenu des pages JSP en fonction de l'authentification : par exemple, faites apparaître sur certaines pages un lien vers `/logout` seulement si l'utilisateur est connecté.

Protection CSRF :

- Activez maintenant la protection CSRF en commentant la ligne en question :

```
// -- ACTIVER la protection CSRF
//.csrf().disable()
```

  À ce stade, votre formulaire de rechercher des UE ne doit plus fonctionner. En effet, Spring Security va vérifier la présence d'un jeton CSRF pour s'assurer de la validité d'une requête `POST` avant de la traiter. Par contre, le formulaire d'édition des produits (géré par une balise Spring) fonctionne car il intègre maintenant un jeton CSRF. Vérifiez la présence de ce jeton dans le code source de la page HTML.

- En utilisant la balise ci-dessous (déjà vu dans la librairie de balises Spring Security), faites en sorte que le formulaire de recherche des UE fonctione à nouveau.

```
<sec:csrfInput />
```

6.3 Utiliser les données en BD

Objectif : utiliser notre BD pour représenter les utilisateurs authentifiés sur l'application.

- Commencez par créer une entité pour représenter un utilisateur :

3. https://www.baeldung.com/spring-security-taglibs

```java
package mybootapp.model;

import java.util.Set;

import javax.persistence.Basic;
import javax.persistence.ElementCollection;
import javax.persistence.Entity;
import javax.persistence.FetchType;
import javax.persistence.Id;

import lombok.AllArgsConstructor;
import lombok.Data;
import lombok.NoArgsConstructor;

@Entity
@Data
@NoArgsConstructor
@AllArgsConstructor
public class XUser {

    @Id
    String userName;

    @Basic
    String password;

    @ElementCollection(fetch = FetchType.EAGER)
    Set<String> roles;

}
```

- Continuez avec la couche DAO :

```java
package mybootapp.repo;

import org.springframework.data.jpa.repository.JpaRepository;
import org.springframework.stereotype.Repository;
import org.springframework.transaction.annotation.Transactional;

import mybootapp.model.XUser;

@Repository
@Transactional
public interface XUserRepository extends JpaRepository<XUser, String> {

}
```

- Ajoutez maintenant une classe qui représente un utilisateur authentifié (un `UserDetails`) de Spring Security et qui est basée sur le classe `XUser`. Vous remarquerez que toutes les possibilités ne sont pas exploitées (compte verrouillé, expiré, désactivé). Il faurdait, pour cela, enrichir notre classe `XUser`.

```java
package mybootapp.web.security;

import java.util.Collection;
import java.util.LinkedList;

import org.springframework.security.core.GrantedAuthority;
import org.springframework.security.core.authority.SimpleGrantedAuthority;
import org.springframework.security.core.userdetails.UserDetails;

import mybootapp.model.XUser;

public class MyUserPrincipal implements UserDetails {

    private static final long serialVersionUID = 1L;

    private XUser user;

    public MyUserPrincipal(XUser user) {
        this.user = user;
    }

    @Override
    public Collection<? extends GrantedAuthority> getAuthorities() {
        var authorites = new LinkedList<GrantedAuthority>();
        user.getRoles().forEach((role) -> {
            authorites.add(new SimpleGrantedAuthority(role));
        });
        return authorites;
    }

    @Override
    public String getPassword() {
        return user.getPassword();
    }

    @Override
    public String getUsername() {
        return user.getUserName();
    }

    @Override
    public boolean isAccountNonExpired() {
        return true;
    }

    @Override
    public boolean isAccountNonLocked() {
        return true;
    }

    @Override
    public boolean isCredentialsNonExpired() {
        return true;
    }

    @Override
    public boolean isEnabled() {
        return true;
    }
}
```

- Nous devons maintenant créer le service qui permet de trouver un `UserDetails` :

```java
package mybootapp.web.security;

import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.security.core.userdetails.UserDetails;
import org.springframework.security.core.userdetails.UserDetailsService;
import org.springframework.security.core.userdetails.UsernameNotFoundException;
import org.springframework.stereotype.Service;

import mybootapp.repo.XUserRepository;

@Service
public class MyUserDetails implements UserDetailsService {

    @Autowired
    private XUserRepository userRepository;

    @Override
    public UserDetails loadUserByUsername(String username) {
        var user = userRepository.findById(username);
        if (user.isEmpty()) {
            throw new UsernameNotFoundException(username);
        }
        return new MyUserPrincipal(user.get());
    }
}
```

- Ajoutez à votre couche `SpringSecurity` une méthode d'initialisation et de création de deux utilisateurs :

```java
...

    @Autowired
    XUserRepository userRepo;

    @PostConstruct
    public void init() {
        var encoder = passwordEncoder();
        var aa = new XUser("aaa", encoder.encode("aaa"), Set.of("ADMIN", "USER"));
        var bb = new XUser("bbb", encoder.encode("bbb"), Set.of("USER"));
        userRepo.save(aa);
        userRepo.save(bb);
        System.out.println("---␣INIT␣SPRING␣SECURITY");
    }

...
```

- Et finalement, toujours dans `SpringSecurity`, changez la méthode d'authentification :

```
...

    @Autowired
    UserDetailsService myUserDetailsService;

    @Bean
    public DaoAuthenticationProvider authProvider() {
        DaoAuthenticationProvider authProvider = new DaoAuthenticationProvider();
        authProvider.setUserDetailsService(myUserDetailsService);
        authProvider.setPasswordEncoder(passwordEncoder());
        return authProvider;
    }

    @Override
    protected void configure(AuthenticationManagerBuilder auth) throws Exception {
        auth.authenticationProvider(authProvider());
    }

...
```

- **Moralité** : Nous créons des utilisateurs par JPA et la couche `UserDetails` est utilisée par Spring Security pour récupérer les informations d'authentification. Vous pouvez même créer une entrée pour récupérer les données de l'utilisateur connecté :

```
package mybootapp.web;

import java.security.Principal;

import org.apache.commons.logging.Log;
import org.apache.commons.logging.LogFactory;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.ResponseBody;

@Controller()
@RequestMapping("/principal")
public class ShowPrincipal {

    protected final Log logger = LogFactory.getLog(getClass());

    @ResponseBody
    @RequestMapping("")
    public String show(Principal p) {
        logger.info("show␣user␣" + p);
        return p.toString();
    }

}
```

6.4 Contrôler les méthodes

Spring Security n'est pas seulement utile pour les contrôleurs Il est également capable de contrôler l'accès aux méthodes d'un service.

- Voila un service Spring qui est sécurisé par Spring Security. La méthode `helloAdmin` est réservée aux administrateur et la méthode `helloForUser` n'est accessible qui si le paramètre `userName` correspond à l'utilisateur courant.

```java
package mybootapp.web.security;

import org.springframework.security.access.prepost.PreAuthorize;
import org.springframework.stereotype.Service;

@Service
public class SecureService {

    @PreAuthorize("hasAuthority('ADMIN')")
    public String helloAdmin() {
        return "Hello";
    }

    @PreAuthorize("#userName␣==␣principal.username")
    public String helloForUser(String userName) {
        return "Hello␣" + userName;
    }

}
```

- Préparez un contrôleur pour tester cette sécurisation :

```java
package mybootapp.web.security;

import org.springframework.beans.factory.annotation.Autowired;
import org.springframework.stereotype.Controller;
import org.springframework.web.bind.annotation.RequestMapping;
import org.springframework.web.bind.annotation.ResponseBody;

@Controller()
@RequestMapping("/secure")
public class SecureController {

    @Autowired
    SecureService ss;

    @ResponseBody
    @RequestMapping("/hello")
    public String hello() {
        return ss.helloAdmin();
    }

    @ResponseBody
    @RequestMapping("/aaa")
    public String helloForUser() {
        return ss.helloForUser("aaa");
    }

}
```

- Pour aller plus loin [4].

6.5 Définir ses conditions

Nous avons quelquefois besoin d'écrire le code de vérification d'un droit (par exemple pour savoir si un utilisateur a le droit d'agir sur une donnée précise). Nous devons, dans ce cas, définir un service de vérification :

4. https://www.baeldung.com/spring-security-method-security

```java
package mybootapp.web.security;

import org.springframework.stereotype.Service;

@Service("securityChecker")
public class SecurityChecker {

    public boolean isOk(String userName) {
        return "aaa".equals(userName);
    }

}
```

Remarque : Ce service est trivial, mais nous pourrions faire des accès BD et des vérifications plus compliquées.

Travail à faire :

- Nous pouvons maintenant définir une nouvelle méthode du service sécurisé qui utilise cette vérification :

```java
...

@Service
public class SecureService {

    ...

    @PreAuthorize("@securityChecker.isOk(principal.username)")
    public String helloSecuredByCode() {
        return "helloSecuredByCode␣is␣OK␣";
    }

}
```

- Ajoutez une entrée à votre contrôleur pour tester cette vérification.
- Pour aller plus loin [5].

5. https://docs.spring.io/spring-security/site/docs/5.0.7.RELEASE/reference/html/el-access.html